Diss. ETH No. 29663

A Composable Treatment of Anonymous Communication

A thesis submitted to attain the degree of

Doctor of Sciences of ETH Zurich
(Dr. sc. ETH Zurich)

presented by

Fabio Matteo Banfi
MSc ETH in Computer Science, ETH Zurich

born on June 21, 1990
citizen of Lugano TI, Switzerland

accepted on the recommendation of

Prof. Dr. Ueli Maurer, examiner
Prof. Dr. Dennis Hofheinz, co-examiner
Prof. Dr. Daniele Venturi, co-examiner

2023

Acknowledgements

First and foremost, I would like to express my deep gratitude to my advisor Ueli Maurer for granting me the opportunity to further explore my passion for cryptography by pursuing a PhD in his group. His constant striving for abstraction and minimality heavily influenced my way of thinking and working. Through the innumerable interesting and insightful discussions we had, both scientific and not, and thanks to his constant encouragement and support, I have acquired a plethora of knowledge that I can apply both at work and in my personal life.

Sincere thanks go to Dennis Hofheinz and Daniele Venturi for co-refereeing this thesis. The final version greatly benefited their careful review and valuable feedback.

I would also like to address special thanks to Stefan Wolf, Willi Meier, Sandro Coretti, and Christian Badertscher, who helped steering my professional journey towards cryptography before my doctoral studies.

For all the fruitful and on-going collaborations, both inside and outside the scope of this thesis, I thank Christian Badertscher, Jesus Diaz Vico, Konstantin Gegier, Martin Hirt, Ueli Maurer, Christopher Portmann, Guilherme Rito, and Jiamin Zhu, as well as all the students I had the pleasure of supervising, Ganyuan Cao, Sina Ghaseminejad, Silvia Ritsch, and Frederik Semmel.

I also want to thank Claudia Günthart, Bernadette Gianesi, and Denise Spicher for their administrative support.

For all the interesting discussions, both about research and life, all the passionate foosball matches, exciting summer retreats in Magliaso, conferences and workshops, and all the other good times we had together, I thank all the current and former members of the Information Security and Cryptography Research Group: Christian Badertscher, Gianluca Brian,

Giovanni Deligios, Konstantin Gegier, Yijun He, Martin Hirt, Daniel Jost, David Lanzenberger, Chen Da Liu-Zhang, Christian Matt, Ueli Maurer, Eleanor McMurtry, Marta Mularczyk, Hai Hoang Nguyen, Christopher Portmann, Guilherme Rito, Daniel Tschudi, and Jiamin Zhu.

I want to further extend my thanks to several members of the other Cryptography and Distributed Systems groups at ETH, who contributed to making my journey even more enjoyable. For all the hikes, dinners, game nights, partying, foosball, tennis, table-tennis matches, and innumerable interesting lunch discussions, I thank Matilda Backendal, Cecilia Boschini, Nicholas Brandt, Suvradip Chakraborty, Andrei Constantinescu, Sebastian Faller, Francesca Falzon, Mia Filić, Diana Ghinea, Sofia Giampietro, Laura Hetz, Kristina Hostáková, Julia Kastner, Karen Klein, Roman Langrehr, Varun Maram, Lenka Mareková, Matteo Scarlatta, Jakub Sliwinski, Kien Tuong Truong, Anupama Unnikrishnan, Bogdan Ursu, Akin Ünal, Yann Vonlanthen, and Shannon Veitch.

Besides my colleagues at ETH, I would also like to thank all the wonderful people who made my life in Zurich all these years so enjoyable. While it is impossible to list them all, sincere gratitude goes to Alessio, Ana, Anna, Adrian, Carina, Daniele, Eleonora, Gianluca, Guido, Katja, Larissa, Leilah, Linus, Lisa, Luca d. T., Luca R., Matteo, Paolo, Sasha, Sofia, Susi, and Svenja.

Last but not least, I would like to express my deepest gratitude to my family. For their continuous love, encouragement, and support, heartfelt thanks go to my parents Sandra (with Sebastiano) and Giovanni (with Fernanda), as well as my sisters Joyce, Melanie, and Lia. To Melanie special thanks for being a fantastic flatmate for all these years.

Abstract

The goal of this thesis is complete the composable study of anonymity in the framework of Constructive Cryptography (CC) of Maurer and Renner. In CC, anonymity is modeled by considering a channel resource that does not leak the identity of senders/receivers to the adversary (but in the case of multiple senders, still might reveal their identities to the receiver(s)). In the literature, this problem has been already partially solved: For example, Kohlweiss et al. considered the setting where one sender and multiple receivers want to communicate over an insecure and anonymous channel, in a way that achieves confidentiality, but crucially while preserving anonymity.

They showed that public-key encryption schemes that are ciphertext-indistinguishable, key-indistingushability, and weakly-robust under a chosen-ciphertext attack enable the construction of a confidential and anonymous channel from one that is insecure but otherwise anonymous. In a follow-up work by Alwen et al., the dual setting of multiple senders and one receiver was analyzed. There, the authors showed that message authentication code schemes that are unforgeable and key-indistinguishable under a chosen-message attack enable the construction of an authenticated and anonymous channel from one that is insecure but otherwise anonymous. The analysis of similar guarantees achieved by symmetric-key encryption and signatures was left open.

In this thesis we complete the picture by filling the above mentioned gaps in the study of anonymity preservation, and also considering the additional but related problem of anonymity creation. We do so by first putting forth a new abstract framework which casts conventional (both game-based and composable) security definitions as *substitutions* of systems. This framework allows for clean syntactic proofs of security and

potentially enables automated verification. We see this framework as an additional contribution by itself, and we use it consistently throughout this thesis.

Armed with this new framework, in the first part we begin by showing that in the setting of multiple senders and one receiver, (probabilistic) symmetric-key encryption schemes that are ciphertext-indistinguishable and key-indistingushability under a chosen-plaintext attack enable the construction of a secure and anonymous channel from one that is authenticated but otherwise anonymous. Moreover, we also show that (probabilistic) authenticated encryption schemes that are ciphertext-indistinguishable, ciphertext-unforgeable, and key-indistingushability under a chosen-ciphertext attack enable the construction of a secure and anonymous channel from one that is insecure but otherwise anonymous.

In the second part, we consider again the setting of multiple senders and one receiver, but move our attention to the problem of enabling the construction of an authenticated and anonymous channel from one that is insecure but otherwise anonymous using public-key cryptography. Intuitively, some form of anonymous signatures should be employed, but we begin by showing that this exact construction is impossible in the intuitive public-key setting required by regular signatures (that is, if in addition to the insecure and anonymous channel, only a one-time authenticated channel from the senders to the receiver is assumed). We therefore provide three alternative constructions which provide some trade-offs between authenticity and anonymity (of the senders), by considering bilateral signatures (a new type of scheme that we introduce), partial signatures, and ring signatures. The first construction, using bilateral signatures, assumes an additional one-time authenticated channel from the receiver to the senders; the second construction, using partial signatures, enables the construction of a weaker version of the authenticated and anonymous channel, that is, a channel that can be interpreted as being selectively anonymous towards the eavesdropping adversary and the receiver; the third construction, using ring signatures, enables the construction of an authenticated channel that is not only anonymous towards the adversary, but towards the receiver as well, that is, the identity of the senders will also not be leaked to the receiver.

Finally, we consider the challenging problem of constructing a secure and anonymous channel from channels that are only authenticated, but crucially not anonymous. We begin by reconsidering game-based notions

of security for universal re-encryption (URE) recently introduced by Young and Yung, and pointing out that they do not minimally capture the essence of URE, which we identify as being unlinkability. We finally show how URE in principle enables the construction of a secure and anonymous channel from channels that are only authenticated, by first obtaining a channel that is unlinkable.

Riassunto

L'obiettivo di questa tesi è quello di completare lo studio composizionale dell'anonimato nel contesto della crittografia costruttiva (CC) di Maurer e Renner. In CC, l'anonimato è modellato considerando una risorsa di canale che non rivela l'identità dei mittenti/destinatari all'avversario (ma che, nel caso di mittenti multipli, potrebbe comunque rivelare la loro identità ai destinatari). Nella letteratura, questo problema è già stato parzialmente risolto: Ad esempio, Kohlweiss et al. hanno considerato il caso in cui un mittente e molteplici destinatari vogliano comunicare su un canale insicuro e anonimo, in modo da ottenere la confidenzialità, ma soprattutto preservando l'anonimato.

Hanno dimostrato che i cifrari a chiave pubblica che hanno indistinguibilità dei crittotesti, indistinguibilità delle chiavi, e sono debolmente robusti sotto un attacco a crittotesto scelto, consentono di costruire un canale confidenziale e anonimo da uno che è insicuro ma altrimenti anonimo. In un lavoro successivo di Alwen et al., è stato analizzato lo scenario duale di molteplici mittenti e un destinatario. Gli autori hanno dimostrato che gli schemi di codici autenticatori di messaggio che sono inforgiabile e hanno indistinguibilità delle chiavi sotto un attacco a messaggio scelto consentono di costruire un canale autenticato e anonimo da uno che è insicuro ma altrimenti anonimo. L'analisi di garanzie simili ottenute dai cifrari a chiave simmetrica e dalle firme digitali è rimasta aperta.

In questa tesi completiamo il quadro colmando le lacune sopra menzionate nello studio della conservazione dell'anonimato e considerando anche il problema aggiuntivo, ma correlato, della creazione dell'anonimato. Lo facciamo proponendo prima di tutto un nuovo modello astratto che presenta le definizioni di sicurezza convenzionali (sia basate su giochi che componibili) come *sostituzioni* di sistemi. Questo modello permette di

ottenere dimostrazioni sintattiche della sicurezza e potenzialmente consente una verifica automatizzata. Consideriamo questo modello come un contributo aggiuntivo di per sé, e lo utilizziamo coerentemente in tutta la tesi.

Armati di questo nuovo modello, nella prima parte mostriamo che, nello scenario con molteplici mittenti e un ricevitore, i cifrari (probabilistici) a chiave simmetrica che hanno indistinguibilità dei crittotesti e indistinguibilità dalla chiave sotto un attacco a messagio scelto consentono di costruire un canale sicuro e anonimo da uno che è autenticato ma altrimenti anonimo. Inoltre, dimostriamo anche che i cifrari autenticati (probabilistici) che hanno indistinguibilità dei crittotesti, sono inforgiabili, e hanno indistinguibilità dalla chiave sotto un attacco a crittotesto scelto permettono di costruire un canale sicuro e anonimo da uno che è insicuro ma altrimenti anonimo.

Nella seconda parte, consideriamo ancora una volta lo scenario con molteplici mittenti e un ricevitore, ma spostiamo la nostra attenzione sul problema di consentire la costruzione di un canale autenticato e anonimo da uno insicuro ma altrimenti anonimo utilizzando la crittografia a chiave pubblica. Intuitivamente, si dovrebbe utilizzare una qualche forma di firma digitale anonima, ma iniziamo mostrando che questa costruzione esatta è impossibile nello scenario a chiave pubblica intuitivamente richiesto dalle regolari firme digitali (cioè, se oltre al canale insicuro e anonimo, si assume solo un canale autenticato una tantum dal mittente al destinatario). Forniamo quindi tre costruzioni alternative che offrono un compromesso tra autenticità e anonimato (dei mittenti), considerando le firme digitali bilaterali (un nuovo tipo di schema che introduciamo), le firme digitali parziali e le firme digitali ad anello. La prima costruzione, che utilizza firme digitali bilaterali, presuppone un ulteriore canale autenticato una tantum dal destinatario ai mittenti; la seconda costruzione, che utilizza firme digitali parziali, consente di costruire una versione più debole del canale autenticato e anonimo, cioè un canale che può essere interpretato come selettivamente anonimo nei confronti dell'avversario che intercetta e del destinatario; la terza costruzione, che utilizza le firme digitali ad anello, consente di costruire un canale autenticato che non è anonimo solo nei confronti dell'avversario, ma anche nei confronti del destinatario, cioè l'identità dei mittenti non viene rivelata al destinatario.

Infine, consideriamo il difficile problema di costruire un canale sicuro e anonimo a partire da canali solo autenticati, ma in modo cruciale non

anonimi. Iniziamo riconsiderando le nozioni di sicurezza basate su giochi per la ri-cifratura universale (URE) recentemente introdotte da Young e Yung, e sottolineando che esse non catturano minimamente l'essenza dell'URE, che noi identifichiamo come la non-associabilità. Mostriamo infine come URE consenta in linea di principio di costruire un canale sicuro e anonimo a partire da canali solo autenticati, ottenendo prima un canale non-associabile.

Contents

Chapter 1

Introduction

1.1 Motivation

Secure communication is often associated with the two fundamental cryptographic properties of confidentiality and authenticity. Confidentiality captures the guarantee that no information about the content of the communication can leak to an eavesdropping adversary, whereas authenticity captures the guarantee that no adversary capable of injecting messages in the communication channel, can convince the receiver that such messages are from the original sender. By encouraging open communication and fostering trust, both these properties are indispensable for establishing a secure digital infrastructure for communication.

However, in today's highly digitized world, it is apparent that a third crucial property must also be considered, when communicating online: *anonymity*. In a complex digital system such as the internet, where multiple senders and receivers communicate, a fundamental extension of the meaning of privacy is the ability to conceal the identities of the communicating parties.

1.1.1 Anonymity

In the cryptographic literature, the term privacy has been originally associated with confidentiality. Only later its meaning has been expanded to incorporate other important security guarantees, such as anonymity.

Considering for example public-key encryption (PKE), notions for confidentiality have crystallized by the late eighties and early nineties. The seminal work of Goldwasser and Micali [GM84] introduced the concept of *semantic security* and showed its equivalence to *indistinguishability under chosen-plaintext attacks* (IND-CPA). Privacy was therefore associated with the inability of an attacker to distinguish between ciphertexts encrypting different messages under the same public key. A few years later, this notion was further strengthened as indistinguishability under chosen-*ciphertext* attacks (IND-CCA) by Naor and Yung [NY90] and Rackoff and Simon [RS92], where the adversary was given the additional power of having access to a decryption oracle.

On the other hand, almost a decade passed before a notion akin to anonymity was introduced. While the term indistinguishability had long been associated with the hardness of distinguishing encryptions of potentially different messages under the *same* key, the new term *key-privacy* introduced by Bellare et al. [BBDP01] extended its meaning to capture the infeasibility of distinguishing between encryptions of messages *under different keys*. Such notion has been formalized as *indistinguishability of keys* (IK), under both chosen-plaintext and chosen-ciphertext attacks, resulting in IK-CPA and IK-CCA security.

Anonymity Preservation. The property of key-indistinguishability introduced in [BBDP01] for PKE has also been considered for the case of symmetric encryption by Fischlin [Fis99], Desai [Des00], and Abadi and Rogaway [AR02]. Furthermore, IK notions have been formulated for various variants of signature schemes, including *ring signatures*, by Rivest et al. [RST01], *anonymous signatures*, by Yang et al. [YWDW06], Fischlin [Fis07], and Zhang and Imai [ZI09], and *partial signatures* by Bellare and Duan [BD09] and Saraswat and Yun [SY09]. Moreover, Alwen et al. [AHM+14] also introduced IK notions for the symmetric-key counterpart of signatures, message authentication codes (MAC).

Still, as pointed out by Kohlweiss et al. [KMO+13], when employing IK-secure schemes in the regular way, usually rather than "generating" anonymity, they merely guarantee its *preservation*. More precisely, considering for example an IK-secure PKE scheme, it would be wrong to assume that its use is sufficient to hide the identity of the receiver. Crucially, the channel used to transmit the ciphertexts *must already provide anonymity*, in order for this to be true. The importance of employing an IK-secure

PKE scheme in this case, is to guarantee that any anonymity already provided by such communication channel, is not *destroyed* by the use of the scheme. Importantly, such considerations are harder to gain from the classical game-based definitions of the various IK notions, and it is therefore imperative to also understand them from an *application point of view*, using for example a composable security framework.

Anonymity Creation. On the other hand, schemes that in principle do produce anonymity, if used in the intended way, do exist. An example of such a scheme is universal re-encryption (URE), introduced by Golle et al. [GJJS04]. Even though its use is not as straightforward as the use of a regular PKE scheme, through the careful design of a protocol based on URE, it is possible to realize an unlinkable communication channel, which lends itself naturally to provide anonymity, under the right conditions.

More precisely, a URE scheme allows anyone to re-encrypt a ciphertext without the need for the public-key originally used to produce it, in such a way that it will still decrypt to the underlying message when using the original secret key. This enables the design of a so-called mix-network, or *mixnet* for short, where senders post ciphertexts on a bulletin board, mixers periodically re-encrypt the posted ciphertexts, and receivers fetch the messages addressed to them by trial-decryption.

Rather than unlinkability, URE has been equipped with the game-based notions of IND-CPA and IK-CPA in [GJJS04]. Several years later, Young and Yung [YY18] pointed out some subtleties in the original definitions, but they still did not phrase security of URE in terms of unlinkability. Again, this emphasizes how understanding the creation of anonymity from an application point of view is of fundamental importance, since it uncovers that the intended application of URE is indeed unlinkability.

1.1.2 Constructive Cryptography

As we have outlined above, game-based definitions have significant shortcomings when it comes to understanding their application semantics. Having been a recurrent issue in the cryptographic literature, this motivated the creation of several composable security frameworks. Rather than defining security by excluding certain attacks, such frameworks generally aim at providing a security statement for a scheme in terms of its suit-

ability in realizing a certain *application*. Examples of composable security frameworks are universal composability (UC) by Canetti [Can01], reactive simulatability by Backes, Pfitzmann, and Waidner [PW01, BPW07], constructive cryptography (CC) by Maurer and Renner [MR11, Mau12], and the inexhaustible interactive Turing machines (IITM) model by Küsters, Tuengerthal, and Rausch [KTR13].

While these frameworks have distinct focuses and vary on a technical level, they all share a common high-level approach for defining security, known as the real-world ideal-world paradigm. For example in CC, the framework used in this thesis, the security of a certain scheme is assessed by comparing two different scenarios. In the first one, the real world, a protocol making use of the scheme is given access to so-called *assumed resources*, such as various communication channels and shared secret keys. Such resources have *interfaces* for both honest and dishonest users, and in the real world the protocol is connected to the honest ones. In the second one, the ideal world, one considers a so-called *ideal resource* (such as a communication channel with better guarantees than an assumed one), whose goal is to capture the intended application of the scheme, together with a simulator that is connected to the dishonest interfaces. Assessing the scheme as secure can then be seen as the protocol safely *constructing* the ideal resource from the assumed one. More concretely, security is captured by asserting the indistinguishability of the two worlds, which implies that any attack in the real world can be translated (by the simulator) into an attack in the ideal world. Turned around, this means that any attack excluded *by definition* by the ideal resource, cannot happen in the real world, thus implying that the real world is not worse (for the honest users) than the ideal world.

An essential consequence of this, is that whenever the ideal resource is needed, it can be safely replaced by the protocol with the assumed resources, *independently of the context*. This is naturally captured by the composition theorem, a central element of CC and the similar frameworks. A significant advantage of defining security in a composable manner, is that it promotes modularity and abstraction, which are essential for designing and analyzing complex systems, extending beyond cryptography. By defining clear abstraction boundaries and abstracting away the construction details, composition allows higher-level protocols to utilize an idealized model of a lower-level protocol, sparing the designer from the need to consider specific details of the latter.

1.2 Overview and Contributions

The development of a library of construction statements is of paramount importance within the framework of constructive cryptography. In this thesis, we enrich such library by including new statements considering resources that capture anonymity. We next summarize our main contributions, and give pointers to the publications they are based on.

1.2.1 The Substitutions Framework

As part of the preliminaries in Chapter 2, we introduce a new framework to define and relate security notions that enables an almost entirely algebraic technique for proving cryptographic statements. We call it the *substitutions framework*, and we will use it consistently throughout this thesis to capture and relate both game-based notions as well as composable ones, using an adaptation of constructive cryptography. As a toy example to get familiar with the framework, in Chapter 2 we also give a very simple proof of the fact that the authenticated encryption notion obtained by combining indistinguishability under a chosen-*plaintext* attack with integrity of *ciphertexts* is equivalent to the one obtained by combining indistinguishability under a chosen-*ciphertext* attack with integrity of *plaintexts*. This framework has evolved and has been refined throughout the three publications on which the main three parts (Chapters 3 to 5) of this thesis are based.

1.2.2 Secret-Key Anonymity Preservation

In the first part of the thesis, presented in Chapter 3, we consider the problem of anonymity preservation in a setting where multiple senders and one receiver use secret-key cryptography. Since the composable analysis of this setting was already carried out in [AHM+15] for the case of anonymous probabilistic message authentication codes (MAC) schemes, we focus on the remaining open problem of studying the composable semantics of anonymous probabilistic encryption (pE) and authenticated encryption (pAE) schemes.

We begin by introducing game-based notions, capturing both confidentiality and anonymity for pE and pAE, as substitutions. More precisely, for pE we cast as a substitution the conventional real-or-random formulation of

indistinguishability under a chosen-plaintext attack (IND-CPA), as well as other notions from the literature of key-indistinguishability under a chosen-plaintext attack (IK-CPA), whereas for pE we first cast as a substitution the all-in-one formulation capturing confidentiality and unforgeability at one, and introduce a new notion of IK under a chosen-ciphertext attack (IK-CCA), also as a substitution. We also define combined notions, capturing all notions at once for each primitive, and we then show the relevant relations among them. Next, we show that for both pE and pAE, their respective stronger confidentiality notions demanding pseudorandom ciphertexts (IND$), indeed imply anonymity. Moreover, we show that the Encrypt-then-MAC paradigm, not only preserves security, but anonymity as well.

We then move to the composable treatment of anonymity preservation for pE and pAE, by showing that in this setting, the introduced game-based notions are sufficient to construct a secure and anonymous channel from an authenticated and anonymous channel. Our analysis makes it explicit that in this setting, key-indistinguishability must be understood as a property that *preserves* anonymity, rather than creating it.

These results in that chapter are based on the publication [BM20].

1.2.3 Public-Key Anonymity Preservation

In the second part of the thesis, presented in Chapter 4, we consider the problem of anonymity preservation in a setting where multiple senders and one receiver use public-key cryptography. Since the composable analysis of this setting was already carried out in [KMO+13] for the case of anonymous public-key encryption (PKE) schemes, we focus on the remaining open problem of studying the composable semantics of anonymous variants of digital signature schemes.

In this scenario, intuitively we should construct an authenticated and anonymous channel from an insecure and anonymous channel. We begin by showing that this exact construction is impossible in the intuitive public-key setting required by regular signatures, that is, if in addition to the insecure and anonymous channel, only a one-time authenticated channel from the senders to the receiver is assumed. We therefore provide three alternative constructions which provide some sort of trade-off between authenticity and anonymity (of the senders), by considering three variants of digital signatures that capture some forms of anonymity.

The first uses a new type of scheme that we introduce, bilateral signatures (BS), which are closely related to designated verifier signatures (DVS). We provide game-based notions for BS, cast as substitutions, and then show that they are sufficient for the construction of an anonymous authenticated channel from an insecure and anonymous channel, a one-time authenticated channel from the senders to the receiver, and an additional one-time authenticated channel from the receiver to the senders.

The second uses partial signatures (PS), introduced independently by Saraswat and Yun [SY09] and Bellare and Duan [BD09]. We cast game-based notions for PS to substitutions, also proposing new combined notions, and then show that they are sufficient to construct, from an insecure and anonymous channel and a one-time authenticated channel from the senders to the receiver, a weaker version of the authenticated and anonymous channel: a *de-anonymizable* authenticated channel, that is, a channel that allows a sender to send a value anonymously (thus, not authentically) to the receiver, but also allows the sender to later give up anonymity and authenticate the value. On a technical level, in this construction we encounter the challenging commitment problem, which we are able to circumvent by using a recent extension of constructive cryptography by Jost and Maurer [JM20].

Finally, the third uses ring signatures (RS), introduced by [RST01] and refined by [BKM06]. We cast game-based notions for RS to substitutions, also proposing new combined notions, and then show that they are sufficient to construct, from an insecure and anonymous channel and a one-time authenticated channel from the senders to all other senders and the receiver, a stronger version of the authenticated and anonymous channel: a *receiver-side* anonymous authenticated channel, that is, a channel that allows a sender to send a value anonymously not only towards the eavesdropper, but towards the receiver as well.

These results in that chapter are based on the publication [BM22].

1.2.4 Anonymity Creation

In the third part of the thesis, presented in Chapter 5, we consider the challenging problem of constructing a secure and anonymous channel from channels that are only authenticated, but crucially *not* already anonymous. In practice, a common approach to this problem is the design of a mix network, or *mixnet* for short. In the cryptographic literature, there are

several schemes that can in princible be used to realize a mixnet. Here we focus on universal re-encryption (URE), introduced by Golle et al. [GJJS04].

We begin by casting as substitutions game-based notions of security for URE recently introduced by Young and Yung [YY18], and pointing out that they do not minimally capture the essence of URE, which we identify as being unlinkability. We do so by introducing new notions, combinations thereof, and showing both relations and separations among them, using our substitutions framework.

We then study the composable semantics of URE by modeling a simple mixnet with an honest mixer in constructive cryptography. We consider an authenticated and not anonymous channel from a set of senders to a mixer, as well as one from the mixer to a set of receivers, but in both directions. We then show that a natural protocol modeling a mixer operating on a bulletin board, constructs an unlinkable channel from the senders to the receivers. This channel allows senders to input messages for receivers and receivers to retrieve messages meant for them, but in such a way that the adversary cannot link these actions together. We also discuss how under the right circumstances, this channel provides anonymity.

Finally, we model the decisional Diffie-Hellman (DDH) problem also as a substitution, and show how the original ElGamal-based scheme from [GJJS04] satisfies our game-based notions, and therefore enables the construction of the unlinkable channel.

The results in that chapter are based on the preprint [BMR23]. In the same work, the final form of the substitution framework has been introduced.

1.3 Related Work

The thesis studies the problem of defining anonymity within a composable framework from thee different angles. We therefore provide the relevant related work for each topic in the respective chapters. The bibliography is found at the end of the thesis.

Chapter 2

Preliminaries

2.1 Notation

For a list of variables $x_1, x_2, \ldots$, we write $x_1, x_2, \ldots \leftarrow y$ to assign the same value y to each variable and $x_1, x_2, \ldots \leftarrow \mathcal{D}$ to assign independently and identically distributed values to each variable according to distribution $\mathcal{D}$, where we usually describe $\mathcal{D}$ as a probabilistic function. For a binary operation $\star$, $y \xleftarrow{\star} x$ means $y \leftarrow y \star x$. A map M is initialized by $M \leftarrow [\,]$ and accessed by $M[\cdot]$. $\varnothing$ denotes the empty set, $\mathbb{N} \doteq \{0, 1, 2, \ldots\}$ denotes the set of natural numbers, and for $n \in \mathbb{N}$, we use the convention $[n] \doteq \{1, \ldots, n\}$. For $n \in \mathbb{N}$, $\{0,1\}^n$ denotes the set of bitstrings of length n, $\{0,1\}^* \doteq \bigcup_{i>0}\{0,1\}^i$ denotes the set of all finite length bitstrings, for $s \in \{0,1\}^*$, $|s|$ denotes the length of s (in bits), and $\$^n$ represent a uniformly sampled random bitstring of length n. For tuples we sometimes abuse notation in the following way: $(x, (y, z)) = (x, y, z)$. For a random variable X over a set $\mathcal{X}$, we define $\operatorname{supp} X \doteq \{x \in \mathcal{X} \mid \Pr[X = x] > 0\}$. For a logical statement S, $\mathbb{1}\{S\}$ is 1 if S is true, and 0 otherwise. We treat sets as multisets.

2.2 Cryptographic Systems

In this thesis we follow [Mau02, MPR07] in making security statements about cryptographic schemes using *random systems* (just *systems* for

brevity). Such a system takes inputs $X_1, X_2, \ldots$ from some input set $\mathcal{X}$ and generates, for each new input X_i, an output Y_i from some output set $\mathcal{Y}$, which depends (possibly probabilistically) on the current input X_i and on the internal state. A system is described exactly by the conditional probability distributions of the i-th output Y_i, given $X_i \doteq (X_1, \ldots, X_i)$ and $Y^{i-1} \doteq (Y_1, \ldots, Y_{i-1})$, for all $i \geq 1$.

Definition 2.2.1 (System)**.** An $(\mathcal{X}, \mathcal{Y})$-*system* $\mathbf{S}$, for input set $\mathcal{X}$ and output set $\mathcal{Y}$, is a sequence of conditional probability distributions $\mathsf{p}^{\mathbf{S}}_{Y_i|Y^{i-1}X^i}$, for $i \geq 1$. Two systems are *compatible* if they have the same input and output sets, and two compatible systems $\mathbf{S}$ and $\mathbf{T}$ are *equivalent*, denoted $\mathbf{S} \equiv \mathbf{T}$, if they have the same input-output behavior, that is, $\mathsf{p}^{\mathbf{S}}_{Y_i|Y^{i-1}X^i} = \mathsf{p}^{\mathbf{T}}_{Y_i|Y^{i-1}X^i}$ for all $i \geq 1$.

Throughout this thesis, we will describe systems informally or with intuitive pseudocode, rather than by the conditional probabilities characterizing them.

2.2.1 Basic System Relations

A useful relation on systems is their *information theoretic distance*, which is denoted $\mathbf{S} \approx_p \mathbf{T}$. In this thesis, we only use such distance for part of an exemplification of our substitution framework, so we only define it informally here; the statement essentially means that *any* distinguisher has probability at most p in distinguishing between an interaction with system $\mathbf{S}$ or system $\mathbf{T}$. Another useful relation in this context, is that of two systems behaving identically only until a certain (bad) event $\mathcal{A}$ is provoked in $\mathbf{S}$, denoted $\mathbf{S}|\mathcal{A} \equiv \mathbf{T}$, but differently afterwards. Clearly, an adversary successfully causing such an event, will be able to distinguish between the two systems. A standard result in cryptography, states that the opposite is also true: A successful distinguisher for the two systems, can be transformed into a successful adversary provoking the event. Again, since our framework of substitution mostly allows us to phrase notions as distinguishing problems, rather than provoking conditions in games, we only present this result from the literature in a form tailored to our needs.

Lemma 2.2.2 ([Sho01, Mau02, BR06, MPR07])**.** *For any compatible systems* $\mathbf{S}$ *and* $\mathbf{T}$*, and event* $\mathcal{A}$ *defined in at least one of* $\mathbf{S}$ *or* $\mathbf{T}$*,*

$$\mathbf{S}|\mathcal{A} \equiv \mathbf{T} \quad \Longrightarrow \quad \mathbf{S} \approx_{\Pr[\neg\mathcal{A}]} \mathbf{T}.$$

This result had been shown specifically for systems in [Mau02, MPR07]. It was proven even more generally in [Sho01], and is usually referred to as the *fundamental lemma of game-playing* from [BR06], where it was shown for code-based games.

2.2.2 System (Black-Box) Transformations

Systems can be transformed into other systems by means of black-box *transformations*, which in this thesis we abstract away as functions from systems to systems. For example, given some system $\mathbf{S}$ and a transformation ρ, we denote by $\rho(\mathbf{S})$ the resulting new system. Concretely, since we consider them to always be black-box, transformations are implemented by systems themselves, that is, ρ is associated with a system $\mathbf{C}^\rho$ which is connected in such a way to system $\mathbf{S}$ that allows it to modify the latter's behavior by processing its inputs and outputs. More precisely, $\mathbf{C}^\rho$ obtains the input given to $\rho(\mathbf{S})$, can then interact for a bounded number of times with $\mathbf{S}$, and finally returns the output of $\rho(\mathbf{S})$. We give more examples and details of transformations in the next subsection.

2.2.3 Basic System Operations

We next define two fundamental operations on systems. First, given some systems $\mathbf{S}_1, \ldots, \mathbf{S}_\ell$, for some $\ell \in \mathbb{N}$, we define $[\mathbf{S}_1, \ldots, \mathbf{S}_\ell]$ as a $(\bigcup_{i=1}^{\ell}(\{i\} \times \mathcal{X}_i), \bigcup_{i=1}^{\ell} \mathcal{Y}_i)$-system that on input (i, x), inputs x to $\mathbf{S}_i$, obtains y, and then outputs y. We call this operation *parallel composition*, and rather than saying "input (i, x) to $[\mathbf{S}_1, \ldots, \mathbf{S}_\ell]$", we say "input x to sub-system $\mathbf{S}_i$". If two or more of the systems $\mathbf{S}_1, \ldots, \mathbf{S}_\ell$ depend on some shared parameter, or if they share state, then we use the notation $[\![\mathbf{S}_1, \ldots, \mathbf{S}_\ell]\!]$ to denote their *correlated* parallel composition, and make any common parameter explicit. An intuitive description of such composition is depicted in Figure 2.1.

For the case of a shared parameter, consider for example a system $\mathbf{S}_p$, whose behavior depends on some parameter p, from some (finite) space $\mathcal{P}$. Let now a, b be values sampled *independently* over $\mathcal{P}$, possibly according to some specified distribution. We can think of a and b as (independent) *random variables* over $\mathcal{P}$. Then, we might for example consider the composed system $[\mathbf{S}_a, \mathbf{S}_b]$, where the two systems are independent, but also the composed system $[\![\mathbf{S}_a, \mathbf{S}_a]\!]$, where now the two systems are *correlated*.

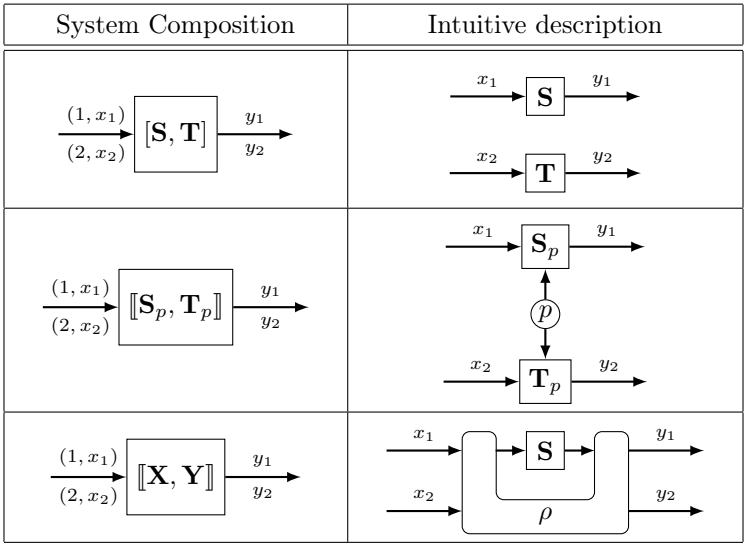


Figure 2.1: Schematic representation of parallel composition of two systems, independent and correlated through a shared parameter or state.

In the context of anonymity, this is useful for modeling pairs of oracles which might be implementing for example encryption either under the same key, or under two independent key.

For the case of shared state, consider for example a system $\mathbf{S}$ and a transformation ρ as per Section 2.2.2. The resulting system $\rho(\mathbf{S})$ might be compatible with $\mathbf{S}$, but more in general ρ might transform $\mathbf{S}$ into a system that is compatible with two or more arbitrary systems composed in parallel, which share some state kept by ρ. Considering the simple case of two, we indicate this by writing $\rho(\mathbf{S}) \equiv [\![\mathbf{X}, \mathbf{Y}]\!]$, where $\mathbf{X}$ and $\mathbf{Y}$ are names given to the two *correlated* systems composed in parallel that ρ emulates. Note that $\mathbf{S}$ might be itself a system composed in parallel.

2.3 The Substitutions Framework

Most security proofs are based on the idea of transforming an adversary for a problem into another adversary for a different problem via a reduc-

tion. Usually security notions and hardness assumptions are phrased as distinguishing problems, so in this case an adversary is called a distinguisher. Here we take a more abstract view, and rather than relating notions and hardness assumptions by transforming distinguishers, we transform the distinguishing problems themselves, modeled as Maurer's random systems [Mau02]. To do so, we introduce the notion of *substitution* for two such systems, an abstraction of indistinguishability that does not require to reason about distinguishers. Our security statements can then be compactly described as substitutions, and relating notions boils down to algebraically showing connections between substitutions, which potentially enables automated verifiability.

We formulate all of the above mentioned security definitions in a systematic and concise language. We see the framework we put forth as an independent contribution of this thesis, since it allows for compact formulations of security definitions, and enables easy and short (*reduction*-based) proofs of security, which in principle could be formally verified in a rather direct way (we leave this task open). Our proposed framework is based on the earlier work on *cryptographic systems* of Maurer, Pietrzak, and Renner [Mau02, MPR07] and can be seen as a specialization of the recent work of Brzuska, Delignat-Lavaud, Fournet, Kohbrok, and Kohlweiss [BDF+18], where security notions are defined as *packages* representing collections of oracles. Their motivation is similar to ours, as they also claim that their method facilitates computer-aided proofs by allowing to delegate perfect reductions steps to proof assistants. It is inspired by the approach taken by Rosulek in [Ros21], as well as by the earlier work of Abadi and Rogaway [AR02].

Definition 2.3.1 (Substitution)**.** For two compatible systems $\mathbf{S}$ and $\mathbf{T}$, we denote by $\mathbf{S} \eqsim \mathbf{T}$ that $\mathbf{S}$ *substitutes* $\mathbf{T}$, where $\eqsim$ is a relation on systems satisfying the following three properties, for a third compatible system $\mathbf{U}$ and a transformation ρ:

Symmetry: $\mathbf{S} \eqsim \mathbf{T} \iff \mathbf{T} \eqsim \mathbf{S}$.

Transitivity: $\mathbf{S} \eqsim \mathbf{T} \wedge \mathbf{T} \eqsim \mathbf{U} \implies \mathbf{S} \eqsim \mathbf{U}$.

Preservation: $\mathbf{S} \eqsim \mathbf{T} \implies \rho(\mathbf{S}) \eqsim \rho(\mathbf{T})$.

The notion of a substitution is exclusively used to make *conditional statements*, that is, statements of the form *"if we can substitute* $\mathbf{S}$ *by* $\mathbf{T}$

($\mathbf{S} \eqsim \mathbf{T}$), *then we can also substitute system* $\mathbf{S}'$ *by system* $\mathbf{T}'$ ($\mathbf{S}' \eqsim \mathbf{T}'$)*"*, which we denote (and formalize below) as $\mathbf{S} \eqsim \mathbf{T} \implies \mathbf{S}' \eqsim \mathbf{T}'$. In order to show such an implication, we usually find systems $\mathbf{S}''$ and $\mathbf{T}''$ such that $\mathbf{S}' \equiv \mathbf{S}''$ and $\mathbf{S}' \equiv \mathbf{T}''$ (that is, $\mathbf{S}''$ and $\mathbf{T}''$ are more convenient descriptions of a system with the same behavior as $\mathbf{S}'$ and $\mathbf{T}'$, respectively), as well as transformation ρ such that $\rho(\mathbf{S}) = \mathbf{S}''$ and $\rho(\mathbf{T}) = \mathbf{T}''$. Now, since $\{\mathbf{S}', \mathbf{T}'\} \equiv \{\mathbf{S}'', \mathbf{T}''\} = \{\rho(\mathbf{S}), \rho(\mathbf{T})\}$ means $\mathbf{S}' \eqsim \mathbf{T}' \iff \rho(\mathbf{S}) \eqsim \rho(\mathbf{T})$, and since $\mathbf{S} \eqsim \mathbf{T} \implies \rho(\mathbf{S}) \eqsim \rho(\mathbf{T})$ (we can substitute $\mathbf{S}$ and $\mathbf{T}$ in any context, see discussion at the end of this section for more details), we proved the original implication.

2.3.1 Modeling Security Notions as Substitutions

We can now describe how to use substitutions in order to capture security statements. Consider some cryptographic scheme Π. A security notion X^{Π} for Π is defined by a substitution $\mathbf{X}_0 \eqsim \mathbf{X}_1$, for two systems $\mathbf{X}_0$ and $\mathbf{X}_1$ depending (implicitly) on Π. The expression *"*X^{Π} *holds unconditionally"*, means that $\mathbf{X}_0 \equiv \mathbf{X}_1$, and *"*$\mathsf{X}^{\Pi}$ *holds unconditionally except with probability* p*"*, means that the behaviors of $\mathbf{X}_0$ and $\mathbf{X}_1$ differs with probability p, denoted $\mathbf{X}_0 \approx_p \mathbf{X}_1$. If the scheme Π is clear from the context, we just write X rather than X^{Π}.

Let us now explain how we can *relate* security notions defined as substitutions. Let $\mathsf{x}_1, \ldots, \mathsf{x}_\ell, \mathsf{y}$ be some security notions (possibly relative to different schemes), for some $\ell \in \mathbb{N}$, defined as substitutions $\mathsf{x}_i :\iff \mathbf{X}_{i,0} \eqsim \mathbf{X}_{i,1}$, for $i \in [\ell]$, and $\mathsf{y} :\iff \mathbf{Y}_0 \eqsim \mathbf{Y}_1$. We say that $\mathsf{x}_1, \ldots, \mathsf{x}_\ell$ *imply* y, denoted

$$(\mathsf{x}_1, \ldots, \mathsf{x}_\ell) \xrightarrow{t_1, \ldots, t_\ell} \mathsf{y},$$

if there exist $n \in \mathbb{N}$, $\rho_1, \ldots, \rho_n$, $i_1, \ldots, i_n \in [\ell]$, and $b_1, \ldots, b_n \in \{0, 1\}$, such that

- $\mathbf{Y}_0 \equiv \rho_1(\mathbf{X}_{i_1, b_1})$,
- $\rho_j(\mathbf{X}_{i_j, 1-b_j}) \equiv \rho_{j+1}(\mathbf{X}_{i_{j+1}, b_{j+1}})$, for any $j \in [n-1]$, and
- $\mathbf{Y}_1 \equiv \rho_n(\mathbf{X}_{i_n, 1-b_n})$,

and where $t_j \doteq |\{k \,|\, i_k = j, k \in [n]\}|$, for any $j \in [n]$, represents the number of times each substitution x_j is used. Concretely, we explicitly

show the implication by the following sequence of steps:

$$\begin{aligned}
\mathbf{Y}_0 &\equiv \rho_1(\mathbf{X}_{i_1,b_1}) \\
&\eqsim \rho_1(\mathbf{X}_{i_1,1-b_1}) && (\mathsf{x}_{i_1}) \\
&\equiv \rho_2(\mathbf{X}_{i_2,b_2}) \\
&\eqsim \rho_2(\mathbf{X}_{i_2,1-b_2}) && (\mathsf{x}_{i_2}) \\
&\equiv \cdots \\
&\equiv \rho_n(\mathbf{X}_{i_n,b_n}) \\
&\eqsim \rho_n(\mathbf{X}_{i_n,1-b_n}) && (\mathsf{x}_{i_n}) \\
&\equiv \mathbf{Y}_1.
\end{aligned}$$

For a more informal statement making the values $t_1, \ldots, t_n$ implicit, we use the alternative notation $(\mathsf{x}_1, \ldots, \mathsf{x}_\ell) \implies \mathsf{y}$, and by $(\mathsf{x}_1, \ldots, \mathsf{x}_\ell) \iff \mathsf{y}$, we mean that, additionally, $\mathsf{y} \implies \mathsf{x}_i$, for each $i \in [\ell]$. Moreover, in case some of the steps can be justifies by $\rho_i(\mathbf{X}_{i,b_i}) \approx_{p_i} \rho_i(\mathbf{X}_{i,1-b_i})$ (for some probability p_i), rather than a substitution $\mathbf{X}_{i,0} \eqsim \mathbf{X}_{i,1}$, we then collect the sum of such p_i's into a value ε, and write $(\mathsf{x}_1, \ldots, \mathsf{x}_\ell) \xrightarrow{t_1,\ldots,t_\ell;\, \varepsilon} \mathsf{y}$ instead.

Finally, let us explain how we can *separate* security notions defined as substitutions. Let x and y be some security notions defined as substitutions $\mathsf{x} :\iff \mathbf{X}_0 \eqsim \mathbf{X}_1$ and $\mathsf{y} :\iff \mathbf{Y}_0 \eqsim \mathbf{Y}_1$. We say that y *is strictly stronger than* x, denoted

$$\mathsf{x} \not\longrightarrow \mathsf{y},$$

if there exists a concrete scheme Π' such that $\mathbf{X}_0^{\Pi'} \eqsim \mathbf{X}_1^{\Pi'}$, but $\mathbf{Y}_0^{\Pi'} \not\eqsim \mathbf{Y}_1^{\Pi'}$, where by $\not\eqsim$ we mean that the systems $\mathbf{Y}_0^{\Pi'}$ and $\mathbf{Y}_1^{\Pi'}$ are *trivially distinguishable*, and thus not substitutable (for example, $\mathbf{Y}_0^{\Pi'}$ outputs 1 if a certain value is input, and 0 otherwise, whereas $\mathbf{Y}_1^{\Pi'}$ always outputs a random bit, for a large enough set of possible value). Nevertheless, this is instead always shown by constructing the scheme Π' from a generic scheme Π, and then proving that $\mathsf{X}^{\Pi} \implies \mathsf{X}^{\Pi'}$, but $\mathbf{Y}_0^{\Pi'} \not\eqsim \mathbf{Y}_1^{\Pi'}$. We use the natural shorthand notation $\mathsf{x} \not\longleftrightarrow \mathsf{y}$ to mean $\mathsf{x} \not\longrightarrow \mathsf{y}$ *and* $\mathsf{y} \not\longrightarrow \mathsf{x}$.

2.3.2 Abstracting the Hybrid Argument

Another standard result from the cryptographic literature, appearing in many different ways, is the *hybrid argument*. Within our framework of

substitutions, we can capture the *essence* of what the hybrid argument really is: A way to show that the two extremes of a sequence of systems (the *hybrids*) can be substituted, if they can all be pairwise substituted. This is essentially the same as the generic way to relate security notions we showed in Section 2.3.1. In fact, the difference seems to be that cryptographers usually refer to the hybrid argument only when the *same* substitution is used multiple times. Still, for convenience, we next formalize the hybrid argument in what we believe to be its most abstract form as substitutions.

Lemma 2.3.2. *For any $n \in \mathbb{N}$, consider independent systems $\mathbf{S}_1, \ldots, \mathbf{S}_n$, $\mathbf{T}_1, \ldots, \mathbf{T}_n$ and transformations $\rho_1, \ldots, \rho_n$. If $\mathbf{S}_i \eqsim \mathbf{T}_i$, for any $i \in [n]$, and $\rho_i(\mathbf{T}_i) \equiv \rho_{i+1}(\mathbf{S}_{i+1})$, for any $i \in [n-1]$, then $\rho_1(\mathbf{S}_1) \eqsim \rho_n(\mathbf{T}_n)$.*

Proof. $\rho_1(\mathbf{S}_1) \eqsim \rho_1(\mathbf{T}_1) \equiv \rho_2(\mathbf{S}_2) \eqsim \rho_2(\mathbf{T}_2) \equiv \cdots \equiv \rho_n(\mathbf{S}_n) \eqsim \rho_n(\mathbf{T}_n)$. □

Note that often in the literature only the less generic version of Lemma 2.3.2 with $\mathbf{S}_1 = \cdots = \mathbf{S}_n$ and $\mathbf{T}_1 = \cdots = \mathbf{T}_n$ is referred to as hybrid argument.

2.3.3 Relating Substitutions to Concrete Security

For two systems $\mathbf{S}$ and $\mathbf{T}$, we mentioned above that if $\mathbf{S} \eqsim \mathbf{T}$ is a valid substitution, then so is $\rho(\mathbf{S}) \eqsim \rho(\mathbf{T})$. To see this, assume for example that we instantiate systems as some kind of poly-time programs, in some security parameter $\kappa \in \mathbb{N}$, and define $\mathbf{S}_\kappa \eqsim \mathbf{T}_\kappa$ to mean

$$\Delta^{\mathbf{D}_\kappa}(\mathbf{S}_\kappa, \mathbf{T}_\kappa) \doteq |\Pr[\mathbf{D}_\kappa(\mathbf{S}_\kappa) = 0] - \Pr[\mathbf{D}_\kappa(\mathbf{T}_\kappa) = 0]| \leq \varepsilon(\mathbf{D}_\kappa),$$

for all poly-time (distinguishing) programs $\mathbf{D}_\kappa$ and some function ε negligible in κ. Now, we might want to show that if this is the case, then

$$\Delta^{\mathbf{D}_\kappa}(\mathbf{S}'_\kappa, \mathbf{T}'_\kappa) \leq \varepsilon'(\mathbf{D}_\kappa),$$

for all $\mathbf{D}_\kappa$ and some other negligible function ε'. In this case, the way to show this is to simply observe that, since composing $\mathbf{D}_\kappa$ with (black-box) transformation ρ, denoted $\mathbf{D}_\kappa\rho$, still results in a poly-time program in κ, then

$$\Delta^{\mathbf{D}_\kappa}(\mathbf{S}'_\kappa, \mathbf{T}'_\kappa) = \Delta^{\mathbf{D}_\kappa}(\mathbf{S}''_\kappa, \mathbf{T}''_\kappa) = \Delta^{\mathbf{D}_\kappa}(\rho(\mathbf{S}_\kappa), \rho(\mathbf{T}_\kappa)) = \Delta^{\mathbf{D}_\kappa\rho}(\mathbf{S}_\kappa, \mathbf{T}_\kappa).$$

Therefore, with $\varepsilon'(\mathbf{D}_\kappa) \doteq \varepsilon(\mathbf{D}_\kappa\rho)$ being still negligible in κ, we proved the implication.

2.3.4 An Example: Authenticated Encryption

In this section we exemplify the substitution framework by giving a very simple proof of the fact that authenticated encryption (AE) can be equivalently formulated as ciphertext-indistinguishability under a chosen-*plaintext* attack plus *ciphertext*-integrity ($\mathsf{ind\text{-}cpa} \wedge \mathsf{int\text{-}ctxt}$, as defined for example in [BN00]) and ciphertext-indistinguishability under a chosen-*ciphertext* attack plus *plaintext*-integrity ($\mathsf{ind\text{-}cca} \wedge \mathsf{int\text{-}ptxt}$, as defined for example in [KL20]). We do so by showing that both combinations are equivalent to an all-in-one formulation of AE, denoted[1] ae, which in turn implies all four notions. In [BN00], where the notions of $\mathsf{int\text{-}ptxt}$ and $\mathsf{int\text{-}ctxt}$ were originally introduced, it was shown that $\mathsf{ind\text{-}cpa} \wedge \mathsf{int\text{-}ctxt}$ implies $\mathsf{ind\text{-}cca}$, but that $\mathsf{ind\text{-}cca} \wedge \mathsf{int\text{-}ptxt}$ implies $\mathsf{int\text{-}ctxt}$ was only shown much later in [JBB18]. Provided these two implications, the result trivially follows since $\mathsf{ind\text{-}cca}$ implies $\mathsf{ind\text{-}cpa}$ and $\mathsf{int\text{-}ctxt}$ implies $\mathsf{int\text{-}ptxt}$. Whereas the proof given in [JBB18] is code-based, generalized to stateful encryption, and rather involved, ours takes advantage of substitutions, and is therefore much simpler, concise, and intuitive.

In order to show all implications, we first need to rephrase the two notions of plaintext-integrity and ciphertext-integrity as substitutions. In [BN00], they are defined as games where an adversary is given access to encryption and decryption oracles, and wins if upon a decryption query, a certain condition is met; for plaintext-integrity, the queried ciphertext needs to be valid (that is, *not* decrypt to the special symbol $\perp$) and decrypt to a plaintext that was not previously *queried* to the encryption oracle, whereas for ciphertext-integrity, the queried ciphertext needs to be valid and not have been previously *output* by the encryption oracle.

Any such game can in principle be turned into a distinguishing problem (hence, a substitution) between a real system and an ideal one where the winning condition of the original game is used to make the latter systems behave identically unless the condition itself is provoked (for example, this approach is extensively used in [Ros21]). Because of this, it is easy to see that (1) if the condition is provoked in the game, then the systems are trivially distinguishable, and (2) if the two systems behave identically unless the condition is provoked, then distinguishing them reduces to provoking the condition in the corresponding game, as per Lemma 2.2.2.

[1] This notion has been introduced in [Shr04] under the name of IND-CCA3, but our notion is closer to a re-formulation of IND-CCA3 from [AGM18].

We now define symmetric-key encryption, and the systems needed to capture the above security notion. Note that we will reuse these later in Chapter 3.

Definition 2.3.3. A *Symmetric-Key Encryption Scheme* for key space $\mathcal{K}$, supported message lengths $\mathcal{L} \subseteq \mathbb{N}$, message space $\mathcal{M} = \bigcup_{\ell \in \mathcal{L}} \{0,1\}^\ell$, expansion factor $\tau \in \mathbb{N}$, and ciphertext space $\mathcal{C} = \bigcup_{\ell \in \mathcal{L}} \{0,1\}^{\ell+\tau}$, is a triple $\Pi = (\mathtt{Gen}, \mathtt{Enc}, \mathtt{Dec})$ where:

- $\mathtt{Gen}$ is an (efficiently samplable) distribution over $\mathcal{K}$;
- $\mathtt{Enc} : \mathcal{K} \times \mathcal{M} \to \mathcal{C}$ is a (efficiently computable) probabilistic function;
- $\mathtt{Dec} : \mathcal{K} \times \mathcal{C} \to \mathcal{M} \cup \{\perp\}$ is an (efficiently computable) deterministic function.

For $k \in \mathcal{K}$, we write $\mathtt{Enc}_k(\cdot)$ for $\mathtt{Enc}(k, \cdot)$ and $\mathtt{Dec}_k(\cdot)$ for $\mathtt{Dec}(k, \cdot)$.

In the following, all notions are relative to some fixed symmetric-key scheme $\Pi = (\mathtt{Gen}, \mathtt{Enc}, \mathtt{Dec})$, for which we define the following systems, parameterized by some key $k \in \mathcal{K}$:

- $\mathbf{E}_k$: On input $m \in \mathcal{M}$, get $c \leftarrow \mathtt{Enc}_k(m)$ and output c.
- $\mathbf{D}_k$: On input $c \in \mathcal{C}$, get $m := \mathtt{Dec}_k(c)$ and output m.

A natural combination of the above systems, is the correlated parallel compositon $[\![\mathbf{E}_k, \mathbf{D}_k]\!]$, that provides access to both encryption and decryption oracles. Moreover, we also define the following transformations, for some arbitrary systems $\mathbf{X}$ and $\mathbf{Y}$:

- $\rho^{\mathsf{cpa}}(\mathbf{X})$: On input m, for $m \in \mathcal{M}$, get $\tilde{m} \xleftarrow{\$} \{0,1\}^{|m|}$, forward $\tilde{m}$ to $\mathbf{X}$, obtain $c \in \mathcal{C}$, and output c.
- $\rho^{\mathsf{cca}}([\![\mathbf{X}, \mathbf{Y}]\!]) \equiv [\![\mathbf{X}', \mathbf{Y}']\!]$, for some correlated systems $\mathbf{X}'$ and $\mathbf{Y}'$ that behave as follows: Initially set $\mathcal{Q} \subseteq \mathcal{M} \times \mathcal{C}$ to $\varnothing$, and then:
  - On input $m \in \mathcal{M}$ to $\mathbf{X}'$, get $\tilde{m} \xleftarrow{\$} \{0,1\}^{|m|}$, forward $\tilde{m}$ to $\mathbf{X}$, obtain $c \in \mathcal{C}$, set $\mathcal{Q}$ to $\mathcal{Q} \cup \{(m, c)\}$, and output c.
  - On input $c \in \mathcal{C}$ to $\mathbf{Y}'$, if there exists[2] an $m \in \mathcal{M}$ such that $(m, c) \in \mathcal{Q}$, then output m, otherwise forward c to $\mathbf{Y}$, obtain $m' \in \mathcal{M} \cup \{\perp\}$, and output m'.

[2] Here and in all subsequent similar transformations, if multiple such values exist we always tacitly assume that the *first* corresponding element inserted in $\mathcal{Q}$ is taken.

- $\rho^{\mathsf{ptxt}}([\![\mathbf{X}, \mathbf{Y}]\!]) \equiv [\![\mathbf{X}', \mathbf{Y}']\!]$, for some correlated systems $\mathbf{X}'$ and $\mathbf{Y}'$ that behave as follows: Initially set $\mathcal{Q} \subseteq \mathcal{M}$ to $\varnothing$, and then:
  - On input $m \in \mathcal{M}$ to $\mathbf{X}'$, set $\mathcal{Q}$ to $\mathcal{Q} \cup \{m\}$, forward m to $\mathbf{X}$, obtain $c \in \mathcal{C}$, and output c.
  - On input $c \in \mathcal{C}$ to $\mathbf{Y}'$, forward c to $\mathbf{Y}$, obtain $m \in \mathcal{M} \cup \{\perp\}$, and if $m \in \mathcal{Q}$ then output m, otherwise output $\perp$.
- $\rho^{\mathsf{ctxt}}(\mathbf{X}) \equiv [\![\mathbf{X}', \mathbf{Y}']\!]$, for some correlated systems $\mathbf{X}'$ and $\mathbf{Y}'$ that behave as follows: Initially set $\mathcal{Q} \subseteq \mathcal{M} \times \mathcal{C}$ to $\varnothing$, and then:
  - On input $m \in \mathcal{M}$ to $\mathbf{X}'$, forward m to $\mathbf{X}$, obtain $c \in \mathcal{C}$, set $\mathcal{Q}$ to $\mathcal{Q} \cup \{(m, c)\}$, and output c.
  - On input $c \in \mathcal{C}$ to $\mathbf{Y}'$, if there exists an $m \in \mathcal{M}$ such that $(m, c) \in \mathcal{Q}$, then output m, otherwise output $\perp$.
- $\rho^{\mathsf{ae}}(\mathbf{X}) \doteq \rho^{\mathsf{ctxt}} \circ \rho^{\mathsf{cpa}}(\mathbf{X}) \equiv [\![\mathbf{X}', \mathbf{Y}']\!]$, for some correlated systems $\mathbf{X}'$ and $\mathbf{Y}'$ that behave as follows: Initially set $\mathcal{Q} \subseteq \mathcal{M} \times \mathcal{C}$ to $\varnothing$, and then:
  - On input $m \in \mathcal{M}$ to $\mathbf{X}'$, get $\tilde{m} \xleftarrow{\$} \{0,1\}^{|m|}$, forward $\tilde{m}$ to $\mathbf{X}$, obtain $c \in \mathcal{C}$, set $\mathcal{Q}$ to $\mathcal{Q} \cup \{(m, c)\}$, and output c.
  - On input $c \in \mathcal{C}$ to $\mathbf{Y}'$, if there exists an $m \in \mathcal{M}$ such that $(m, c) \in \mathcal{Q}$, then output m, otherwise output $\perp$.

In certain contexts, one might with to give explicit names to two oracles emulated by a transformation, and in this case we suggest the following notations:

- $\mathbf{E}_k^{\$} \doteq \rho^{\mathsf{cpa}}(\mathbf{E}_k)$;
- $[\![\mathbf{E}_k, \hat{\mathbf{D}}_k]\!] \doteq \rho^{\mathsf{cca}}([\![\mathbf{E}_k, \mathbf{D}_k]\!])$;
- $[\![\mathbf{E}_k, \mathbf{D}_k^{\perp}]\!] \doteq \rho^{\mathsf{ptxt}}([\![\mathbf{E}_k, \mathbf{D}_k]\!])$;
- $[\![\mathbf{E}_k, \mathbf{D}^{\perp}]\!] \doteq \rho^{\mathsf{ctxt}}(\mathbf{E}_k)$;
- $[\![\mathbf{E}_k^{\$}, \mathbf{D}^{\perp}]\!] \doteq \rho^{\mathsf{ae}}(\mathbf{E}_k)$.

We can now define security notions for AE as substitutions.

Following [BDJR97], we first define the game-based security notion of confidentiality under a chosen-plaintext attack in the *real-or-random* fashion, where the adversary must distinguish between a true encryption oracle and one which ignores inputs and encrypts random messages of the same length instead. The following definition is essentially the abstraction of the one named ROR-CPA in [BDJR97], which is linearly equivalent (in the number of queries) to the one dubbed FTG-CPA (for "find-then-guess") therein, which is usually what IND-CPA refers to in the literature.

Definition 2.3.4 (ind-cpa)**.** $\mathbf{E}_k \doteq \rho^{\mathsf{cpa}}(\mathbf{E}_k)$, for $k \leftarrow \mathtt{Gen}$.

Again following [BDJR97], we then define the game-based security notion of confidentiality under a chosen-ciphertext attack also in the real-or-random fashion, where the adversary must distinguish between a pair of (true) encryption *and* decryption oracles and a pair of (fake) oracles where the first ignores inputs and encrypts random messages of the same length instead, and the second only decrypts ciphertexts not previously output by the first. More precisely, the fake decryption oracle returns the originally input message, in case a previously output ciphertext is queried. We therefore deviate slightly from [BDJR97], where it was instead mandated that the adversary does not query such a ciphertext in the first place.

Definition 2.3.5 (ind-cca)**.** $[\![\mathbf{E}_k, \mathbf{D}_k]\!] \doteq \rho^{\mathsf{cca}}([\![\mathbf{E}_k, \mathbf{D}_k]\!])$, for $k \leftarrow \mathtt{Gen}$.

Recall our discussion above on how a notion phrased as a game with a winning condition can be phrased as a distinguishing problem. With that in mind, consider the conventional notion of plaintext integrity from [BN00], where an adversary has access to two oracles: one for encryption, that remembers the queried messages, and one for verification, that only returns a bit indicating whether the input ciphertext decrypts to a valid message or not, and sets the winning flag to true in case such message is indeed valid and was not previously queried to the encryption oracle. First of all, following [MRT12], we use a stronger notion where the verification oracle returns the decrypted message or the special symbol $\perp$ instead of just a bit, since the original notion cannot guarantee composability. We therefore, refer to the *decryption* oracle, rather than the verification oracle. Moreover, we do not hard-code a condition to be won inside

the decryption oracle, but rather model the notion as the problem of distinguishing between two pairs of oracles: The first models regular encryption and decryption, whereas the second pair is composed of an oracle for encryption that stores the queried messages and an oracle for (fake) decryption, that only returns the decryption of the input massage if it corresponds to one of those queried to the encryption oracle.

Definition 2.3.6 (int-ptxt)**.** $[\![\mathbf{E}_k, \mathbf{D}_k]\!] \eqsim \rho^{\mathsf{ptxt}}([\![\mathbf{E}_k, \mathbf{D}_k]\!])$, for $k \leftarrow \mathtt{Gen}$.

The stronger notion of ciphertext integrity is similar to the previous notion of plaintext integrity, except that now the fake decryption oracle will not first decrypt the input ciphertext and then check whether the resulting message is new or not, but rather only output a message, if such message was the query to the encryption oracle that produced the queried ciphertext. For this, the encryption oracle will now not only keep track of the queried messages, but rather of the resulting message-ciphertext pairs.

Definition 2.3.7 (int-ctxt)**.** $[\![\mathbf{E}_k, \mathbf{D}_k]\!] \eqsim \rho^{\mathsf{ctxt}}(\mathbf{E}_k)$, for $k \leftarrow \mathtt{Gen}$.

For the *all-in-one* security notion ae capturing both confidentiality and authenticity, we follow the one originally introduced by Shrimpton in [Shr04] and dubbed IND-CCA3 therein. There, an adversary must again distinguish between a pair of (true) encryption and decryption oracles and a pair of (fake) oracles where the first ignores inputs and encrypts random messages of the same length instead, and the second always return $\perp$, except if the provided ciphertext was previously output upon (fake) encryption, in which case the original message is returned. Note that we are again deviating slightly from the original IND-CCA3 notion, since we don't put any restriction on the adversary. This variant of the notion was first put forth in [AGM18] and shown to be equivalent to IND-CCA3, and it was for example of fundamental importance in the formulation of composable notions for *quantum* authenticated encryption in CC [BMPZ19], where the so-called *no-cloning theorem* directly contradicts the IND-CCA3 definition. Moreover, note that given how we modeled IND-CPA and INT-CTXT, it is exactly the composition of those two notions *by definition*.

Definition 2.3.8 (ae)**.** $[\![\mathbf{E}_k, \mathbf{D}_k]\!] \eqsim \rho^{\mathsf{ae}}(\mathbf{E}_k)$, for $k \leftarrow \mathtt{Gen}$.

In order to prove the main result, we need to additionally define the following transformations (for arbitrary systems $\mathbf{X}$ and $\mathbf{Y}$), systems, and a lemma.

- $\rho^{\mathsf{enc}}(\llbracket \mathbf{X}, \mathbf{Y} \rrbracket)$: On input $m \in \mathcal{M}$, forward m to $\mathbf{X}$, obtain $c \in \mathcal{C}$, and output c. Note that this means $\rho^{\mathsf{enc}}(\llbracket \mathbf{X}, \mathbf{Y} \rrbracket) \equiv \mathbf{X}$.
- $\rho^{\mathsf{cca\text{-}wor}}(\llbracket \mathbf{X}, \mathbf{Y} \rrbracket) \equiv \llbracket \mathbf{X}', \mathbf{Y}' \rrbracket$, for some correlated systems $\mathbf{X}'$ and $\mathbf{Y}'$ that behave as follows: Initially set $\mathcal{Q} \subseteq \mathcal{M} \times \mathcal{C}$ and $\mathcal{Q}' \subseteq \mathcal{M}$ to $\varnothing$, and then:
  - On input $m \in \mathcal{M}$ to $\mathbf{X}'$, set $\mathcal{Q}'$ to $\mathcal{Q}' \cup \{m\}$, get $\tilde{m} \xleftarrow{\$} \{0,1\}^{|m|} \setminus \mathcal{Q}'$, forward $\tilde{m}$ to $\mathbf{X}$, obtain $c \in \mathcal{C}$, set $\mathcal{Q}$ to $\mathcal{Q} \cup \{(m, c)\}$, and output c.
  - On input $c \in \mathcal{C}$ to $\mathbf{Y}'$, if there exists an $m \in \mathcal{M}$ such that $(m, c) \in \mathcal{Q}$, then output m, otherwise forward c to $\mathbf{Y}$, obtain $m' \in \mathcal{M} \cup \{\bot\}$, and output m'.
- $\mathbf{M}^{\mathsf{wr}}$: On input $m \in \mathcal{M}$, get $\tilde{m} \xleftarrow{\$} \{0,1\}^{|m|}$, and output $\tilde{m}$.
- $\mathbf{M}^{\mathsf{wor}}$: Initially set $\mathcal{Q} \subseteq \mathcal{M}$ to $\varnothing$, and then on input $m \in \mathcal{M}$, set $\mathcal{Q}$ to $\mathcal{Q} \cup \{m\}$, get $\tilde{m} \xleftarrow{\$} \{0,1\}^{|m|} \setminus \mathcal{Q}$, and output $\tilde{m}$.

Lemma 2.3.9. *Let q be the maximum number of queries and $\ell_{\mathsf{min}} \doteq \min \mathcal{L}$. Then:*

$$\mathbf{M}^{\mathsf{wr}} \approx_{q^2/2^{\ell_{\mathsf{min}}}} \mathbf{M}^{\mathsf{wor}}.$$

Proof. Towards the worst-case analysis, assume all messages $m_1, \ldots, m_q$ queried to $\mathbf{M}^{\mathsf{wr}}$ have length ℓ_{min}. Let $\tilde{m}_1, \ldots, \tilde{m}_q$ be the messages sampled by $\mathbf{M}^{\mathsf{wr}}$. Let $\mathcal{A}$ be the event that in $\mathbf{M}^{\mathsf{wr}}$, for any $i \in [q]$ and any $j \in [i]$, $\tilde{m}_i \neq m_j$. Then clearly $\mathbf{M}^{\mathsf{wr}} | \mathcal{A} \equiv \mathbf{M}^{\mathsf{wor}}$. Therefore, by Lemma 2.2.2,

$$\mathbf{M}^{\mathsf{wr}} \approx_{\Pr[\neg\mathcal{A}]} \mathbf{M}^{\mathsf{wor}},$$

where

$$\begin{aligned}
\Pr[\neg\mathcal{A}] &= \Pr[\exists i \in [q] \colon \exists j \in [i] \colon \tilde{m}_i = m_j] \\
&\leq \sum_{i=1}^{q} \sum_{j=1}^{i} \frac{1}{2^{\ell_{\mathsf{min}}}} \\
&\leq \frac{q^2}{2^{\ell_{\mathsf{min}}}}.
\end{aligned}$$

□

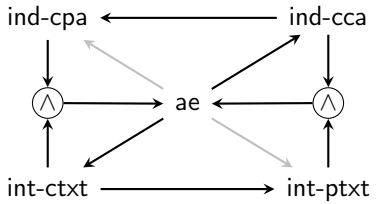


Figure 2.2: Relations among notions: the six black arrows represent the implications we concretely show in Theorem 2.3.10, the two gray ones follow from them.

We can now state and prove the main result.

Theorem 2.3.10. $(\mathsf{ind\text{-}cpa}, \mathsf{int\text{-}ctxt}) \iff (\mathsf{ind\text{-}cca}, \mathsf{int\text{-}ptxt}) \iff \mathsf{ae}$.

Proof. Let $k \leftarrow \mathtt{Gen}$. To show the two equivalences, it is sufficient to prove the following six implications (see Figure 2.2).

1. $\mathsf{ind\text{-}cca} \xrightarrow{1} \mathsf{ind\text{-}cpa}$:

$$\begin{aligned} \mathbf{E}_k &\equiv \rho^{\mathsf{enc}}([\![\mathbf{E}_k, \mathbf{D}_k]\!]) && (2.1)\\ &\eqsim \rho^{\mathsf{enc}} \circ \rho^{\mathsf{cca}}([\![\mathbf{E}_k, \mathbf{D}_k]\!]) && (\mathsf{ind\text{-}cca})\\ &\equiv \rho^{\mathsf{cpa}}(\mathbf{E}_k), && (2.2) \end{aligned}$$

   where equations (2.1) and (2.2) hold because ρ^{enc} only accepts and forwards queries over $\mathcal{M}$.

2. $\mathsf{int\text{-}ctxt} \xrightarrow{2} \mathsf{int\text{-}ptxt}$:

$$\begin{aligned} [\![\mathbf{E}_k, \mathbf{D}_k]\!] &\eqsim \rho^{\mathsf{ctxt}}(\mathbf{E}_k) && (\mathsf{int\text{-}ctxt})\\ &\equiv \rho^{\mathsf{ptxt}} \circ \rho^{\mathsf{ctxt}}(\mathbf{E}_k) && (2.3)\\ &\eqsim \rho^{\mathsf{ptxt}}([\![\mathbf{E}_k, \mathbf{D}_k]\!]), && (\mathsf{int\text{-}ctxt}) \end{aligned}$$

   where equation (2.3) holds because in the composed transformation $\rho^{\mathsf{ptxt}} \circ \rho^{\mathsf{ctxt}}$, where ρ^{ptxt} keeps the set $\mathcal{Q}$ and ρ^{ctxt} keeps the set $\mathcal{Q}'$, if there exists an $m \in \mathcal{M}$ such that $(m, c) \in \mathcal{Q}'$, then $m \in \mathcal{Q}$.

3. $(\mathsf{ind\text{-}cpa}, \mathsf{int\text{-}ctxt}) \xrightarrow{1,1} \mathsf{ae}$:

$$\begin{aligned}
[\![\mathbf{E}_k, \mathbf{D}_k]\!] &\doteq \rho^{\mathsf{ctxt}}(\mathbf{E}_k) && (\mathsf{int\text{-}ctxt})\\
&\doteq \rho^{\mathsf{ctxt}} \circ \rho^{\mathsf{cpa}}(\mathbf{E}_k) && (\mathsf{ind\text{-}cpa})\\
&= \rho^{\mathsf{ae}}(\mathbf{E}_k). && (\text{Def.})
\end{aligned}$$

4. $(\mathsf{ind\text{-}cca}, \mathsf{int\text{-}ptxt}) \xrightarrow{1,2;\, q_e^2/2^{\ell_{\mathsf{min}}}} \mathsf{ae}$: Consider $\rho(\mathbf{X}) \equiv [\![\mathbf{X}', \mathbf{Y}']\!]$, for some correlated systems $\mathbf{X}'$ and $\mathbf{Y}'$, that behave as follows: Initially get $k' \leftarrow \mathtt{Gen}$, set $\mathcal{Q}, \mathcal{Q}'' \subseteq \mathcal{M}$ and $\mathcal{Q}' \subseteq \mathcal{M} \times \mathcal{C}$ to $\varnothing$, and then:

   - On input $m \in \mathcal{M}$ to $\mathbf{X}'$, set $\mathcal{Q}$ to $\mathcal{Q} \cup \{m\}$, forward m to $\mathbf{X}$, obtain $\tilde{m}$, set $\mathcal{Q}''$ to $\mathcal{Q}'' \cup \{\tilde{m}\}$, get $c \leftarrow \mathtt{Enc}_{k'}(m)$, set $\mathcal{Q}'$ to $\mathcal{Q}' \cup \{(\tilde{m}, c)\}$, and output c.
   - On input $c \in \mathcal{C}$ to $\mathbf{Y}'$:
     - If there exists an $m \in \mathcal{M}$ such that $(m, c) \in \mathcal{Q}'$: If $m \in \mathcal{Q}$, output m, otherwise output $\perp$.
     - Otherwise, get $m' := \mathtt{Dec}'_{k_i}(c) \in \mathcal{M} \cup \{\perp\}$, and if $m' \in \mathcal{Q}$, output m, otherwise output $\perp$.

   Then:

$$\begin{aligned}
[\![\mathbf{E}_k, \mathbf{D}_k]\!] &\doteq \rho^{\mathsf{ptxt}}([\![\mathbf{E}_k, \mathbf{D}_k]\!]) && (\mathsf{int\text{-}ptxt})\\
&\doteq \rho^{\mathsf{ptxt}} \circ \rho^{\mathsf{cca}}([\![\mathbf{E}_k, \mathbf{D}_k]\!]) && (\mathsf{ind\text{-}cca})\\
&\doteq \rho^{\mathsf{ptxt}} \circ \rho^{\mathsf{cca}} \circ \rho^{\mathsf{ptxt}}([\![\mathbf{E}_k, \mathbf{D}_k]\!]) && (\mathsf{int\text{-}ptxt})\\
&\equiv \rho(\mathbf{M}^{\mathsf{wr}})\\
&\approx_{q_e^2/2^{\ell_{\mathsf{min}}}} \rho(\mathbf{M}^{\mathsf{wor}}) && (\text{Lemma 2.3.9})\\
&\equiv \rho^{\mathsf{ptxt}} \circ \rho^{\mathsf{cca\text{-}wor}} \circ \rho^{\mathsf{ptxt}}([\![\mathbf{E}_k, \mathbf{D}_k]\!])\\
&\equiv \rho^{\mathsf{ae}}(\mathbf{E}_k), && (2.4)
\end{aligned}$$

   where the only non-trivial step is equation (2.4), which we now justify. Let define systems $\mathbf{S} \doteq \rho^{\mathsf{ptxt}} \circ \rho^{\mathsf{cca\text{-}wor}} \circ \rho^{\mathsf{ptxt}}([\![\mathbf{E}_k, \mathbf{D}_k]\!])$. Without loss of generality, assume that a message $m \in \mathcal{M}$ has been input to $\mathbf{S}$ (respectively $\rho^{\mathsf{ae}}(\mathbf{E}_k)$), and internally $\mathbf{S}$ (respectively $\rho^{\mathsf{ae}}(\mathbf{E}_k)$) has sampled $\tilde{m} \in \mathcal{M}$ with $|\tilde{m}| = |m|$ (and $\tilde{m} \neq m$, for $\mathbf{S}$), computed $c \leftarrow \mathtt{Enc}_k(\tilde{m})$, and then output c. We can distinguish four cases for a further input $c' \in \mathcal{C}$ to $\mathbf{S}$ (respectively $\rho^{\mathsf{ae}}(\mathbf{E}_k)$):

(i) $c' = c$;

(ii) $c' \neq c$, $\mathtt{Dec}_k(c') = m$;

(iii) $c' \neq c$, $\mathtt{Dec}_k(c') = \tilde{m}$;

(iv) $c' \neq c$, $\mathtt{Dec}_k(c') \neq m$, $\mathtt{Dec}_k(c') \neq \tilde{m}$.

Since $\tilde{m} \neq m$ in $\mathbf{S}$, these four cases are disjoint and cover all possible outcomes. We now show that only for case (i) the output of both $\mathbf{S}$ and $\rho^{\mathsf{ae}}(\mathbf{E}_k)$ will be m, whereas for all other cases, both systems will consistently output $\perp$. For $\mathbf{S}$, consider the set $\mathcal{Q} \subseteq \mathcal{M}$ kept by the leftmost ρ^{ptxt}, the set $\mathcal{Q}' \subseteq \mathcal{M} \times \mathcal{C}$ kept by ρ^{cca}, and the set $\mathcal{Q}'' \subseteq \mathcal{M}$ kept by the rightmost ρ^{ptxt}. Then $\mathcal{Q} = \{m\}$, $\mathcal{Q}' = \{(m, c)\}$, and $\mathcal{Q}'' = \{\tilde{m}\}$. Therefore:

(i) If $c' = c$, then $(m, c') \in \mathcal{Q}'$, and since $m \in \mathcal{Q}$, $\mathbf{S}$ outputs m;

(ii) If $c' \neq c$ and $\mathtt{Dec}_k(c') = m$, then since there is no $m \in \mathcal{M}$ such that $(m, c') \in \mathcal{Q}'$, $\mathbf{S}$ computes $m \leftarrow \mathtt{Dec}_k(c')$. But since $m \notin \mathcal{Q}''$ (and $\perp \notin \mathcal{Q}$), $\mathbf{S}$ outputs $\perp$;

(iii) If $c' \neq c$ and $\mathtt{Dec}_k(c') = \tilde{m}$, then since there is no $m \in \mathcal{M}$ such that $(m, c') \in \mathcal{Q}'$, $\mathbf{S}$ computes $\tilde{m} \leftarrow \mathtt{Dec}_k(c')$, so $\tilde{m} \in \mathcal{Q}''$. But since $\tilde{m} \notin \mathcal{Q}$, $\mathbf{S}$ outputs $\perp$;

(iv) If $c' \neq c$, $\mathtt{Dec}_k(c') \neq m$, and $\mathtt{Dec}_k(c') \neq \tilde{m}$, then since there is no $m \in \mathcal{M}$ such that $(m, c') \in \mathcal{Q}'$, $\mathbf{S}$ computes $m' \leftarrow \mathtt{Dec}_k(c')$. But since $m' \notin \mathcal{Q}''$ (and $\perp \notin \mathcal{Q}$), $\mathbf{S}$ outputs $\perp$.

For $\rho^{\mathsf{ae}}(\mathbf{E}_k)$, consider the set $\mathcal{Q}$ kept by ρ^{ae}. Then $\mathcal{Q} = \{(m, c)\}$. Therefore, if $c' = c$, then $(m, c') \in \mathcal{Q}$, thus $\rho^{\mathsf{ae}}(\mathbf{E}_k)$ outputs m. Moreover, cases (ii)–(iv) collapse to the same case: since $c' \neq c$, there is no $m \in \mathcal{M}$ such that $(m, c') \in \mathcal{Q}$, thus $\rho^{\mathsf{ae}}(\mathbf{E}_k)$ always outputs $\perp$.

5. $\mathsf{ae} \xrightarrow{2} \mathsf{ind\text{-}cca}$:

$$\begin{aligned} [\![\mathbf{E}_k, \mathbf{D}_k]\!] &\eqsim \rho^{\mathsf{ae}}(\mathbf{E}_k) && (\mathsf{ae}) \\ &\equiv \rho^{\mathsf{cca}} \circ \rho^{\mathsf{ae}}(\mathbf{E}_k) && (2.5) \\ &\eqsim \rho^{\mathsf{cca}}([\![\mathbf{E}_k, \mathbf{D}_k]\!]), && (\mathsf{ae}) \end{aligned}$$

where equation (2.5) holds because in the composed transformation $\rho^{\mathsf{cca}} \circ \rho^{\mathsf{ae}}$, where ρ^{cca} keeps the set $\mathcal{Q}$ and ρ^{ae} keeps the set $\mathcal{Q}'$, there exists an $m \in \mathcal{M}$ such that $(m, c) \in \mathcal{Q}$ if and only if there exists an $\tilde{m} \in \mathcal{M}$ such that $(\tilde{m}, c) \in \mathcal{Q}'$.

6. $\mathsf{ae} \xrightarrow{3} \mathsf{int\text{-}ctxt}$:

$$\begin{aligned}
[\![\mathbf{E}_k, \mathbf{D}_k]\!] &\eqsim \rho^{\mathsf{ae}}(\mathbf{E}_k) && (\mathsf{ae}) \\
&= \rho^{\mathsf{ctxt}} \circ \rho^{\mathsf{cpa}}(\mathbf{E}_k) && (\text{Def.}) \\
&\equiv \rho^{\mathsf{ctxt}} \circ \rho^{\mathsf{cca}}([\![\mathbf{E}_k, \mathbf{D}_k]\!]) && (2.6) \\
&\eqsim \rho^{\mathsf{ctxt}}([\![\mathbf{E}_k, \mathbf{D}_k]\!]), && (\mathsf{ind\text{-}cca})
\end{aligned}$$

where equation (2.6) holds because ρ^{ctxt} never forwards queries over $\mathcal{C}$, and for the last step, since we just proved that $\mathsf{ae} \xrightarrow{2} \mathsf{ind\text{-}cca}$, we used $\mathsf{ind\text{-}cca}$ (hence ae twice). □

Remark. Sometimes indistinguishability is phrased in the stronger sense of *indistinguishability from random bitstrings* (cf. Definition 3.2.15). It is possible to show Theorem 2.3.10 where all notions of confidentiality are strengthened in this way, which would result in even shorter proofs. In particular, the proof of $(\mathsf{ind\text{-}cca}, \mathsf{int\text{-}ptxt}) \implies \mathsf{ae}$ would require (a weakened version of) the $\mathsf{int\text{-}ptxt}$ substitution to be invoked only once, and it would not incur any additional term $q_{\mathsf{e}}^2/2^{\ell_{\mathsf{min}}}$ [Bel22].

2.4 Constructive Cryptography

We now turn our attention to composable security, as opposed to game-based security. For this, we make use of the constructive cryptography (CC) framework by Maurer [Mau12], which is a specialization of the abstract cryptography theory by Maurer and Renner [MR11]. In essence, CC allows to define security of cryptographic protocols as statements about constructions of resources from other resources, which we model as cryptographic systems from Section 2.2, enhanced with *interfaces*. For such systems, we use suggestive words typed in sans-serif rather than bold-faced letters.

Definition 2.4.1 ($\mathcal{P}$-Resource)**.** For a party set $\mathcal{P}$, a *$\mathcal{P}$-resource* RES for (implicit) input-output set $\mathcal{X}$, is a $(\mathcal{P} \times \mathcal{X}, \mathcal{P} \times \mathcal{X})$-system. For $P \in \mathcal{P}$ and $x \in \mathcal{X}$, to *"input x at interface P of RES"* means inputting (P, x) to RES, and to *"obtain x from interface P of RES"*, means getting an output (P, x) from RES.

The various interfaces of a resource should be thought of as being assigned to parties. In both Chapters 3 and 4, we focus on a more specific set of resources which are parameterized only by an integer $n \geq 2$ (the case $n = 1$ would be pointless for anonymity), defining $n + 2$ interfaces: n for the *senders*, denoted $S_1, \ldots, S_n$, one for the *adversary*, denoted E, and one for the *receiver*, denoted R. Therefore, in those two chapters we use the expression n-resource to indicate $\mathcal{P}$-resources with $\mathcal{P} = \{S_1, \ldots, S_n, R, E\}$.

Another crucial ingredient of CC are *converters*, also formally modeled as systems (labeled by lower-case sans-serif suggestive words), which when applied to individual interfaces of $\mathcal{P}$-resources, give raise to a new $\mathcal{P}$-resource.

Definition 2.4.2 (Local Converter)**.** A local converter cnv is a system with in and out interfaces (as per Definition 2.4.1), which can be applied to an interface $P \in \mathcal{P}$ of a $\mathcal{P}$-resource RES, denoted $\mathsf{cnv}^P\,\mathsf{RES}$, which is in turn a $\mathcal{P}$-resource. $\mathsf{cnv}^P\,\mathsf{RES}$ behaves as RES, except that:

- Inputs to interface P are first input to interface out of cnv, which then produces an output at its interface in, which is in turn input to interface P of RES.
- Outputs at interface P of RES are first input to interface in of cnv, which then produces an output at its interface out, which is in turn output at interface P of $\mathsf{cnv}^P\,\mathsf{RES}$.

For another local converter $\widehat{\mathsf{cnv}}$, $(\widehat{\mathsf{cnv}}\,\mathsf{cnv})^P\,\mathsf{RES}$ is the resource resulting from connecting interface in of $\widehat{\mathsf{cnv}}$ to interface out of cnv and interface in of cnv to interface P of RES.

In order to make security statements within CC, we model protocols as lists of converters attached to the *honest* interfaces of a resource, defined by a set $\mathcal{H} \subseteq \mathcal{P}$. More precisely, an $\mathcal{H}$-protocol $\boldsymbol{\pi}$ is a list of $h \doteq |\mathcal{H}|$ converters $\boldsymbol{\pi} \doteq (\mathsf{cnv}_1, \ldots, \mathsf{cnv}_h)$, where without loss of generality, $\mathcal{H} = \{P_1, \ldots, P_h\}$, and cnv_i is attached to honest party interface P_i, for

$i \in [h]$. For the special case of n-resources, we call $\boldsymbol{\pi}$ an n-protocol. Assuming all senders and receivers to be honest, we use the convention that with $\boldsymbol{\pi} \doteq (\mathsf{cnv}_1, \ldots, \mathsf{cnv}_{n+1})$, cnv_i is attached to S_i, for $i \in [n]$, and cnv_{n+1} is attached to R.

Throughout this thesis, we will use the short-hand notation $\boldsymbol{\pi}\,\mathsf{RES}$ for the $\mathcal{P}$-resource $\mathsf{cnv}_1^{P_1} \cdots \mathsf{cnv}_h^{P_h}\,\mathsf{RES}$. Moreover, for a second $\mathcal{H}$-protocol $\hat{\boldsymbol{\pi}} \doteq (\widehat{\mathsf{cnv}}_1, \ldots, \widehat{\mathsf{cnv}}_h)$, we define the *composition* of $\hat{\boldsymbol{\pi}}$ and $\boldsymbol{\pi}$ as $\hat{\boldsymbol{\pi}}\boldsymbol{\pi} \doteq (\widehat{\mathsf{cnv}}_1\,\mathsf{cnv}_1, \ldots, \widehat{\mathsf{cnv}}_h\,\mathsf{cnv}_h)$, and therefore $\hat{\boldsymbol{\pi}}\boldsymbol{\pi}\,\mathsf{RES}$ is the $\mathcal{P}$-resource

$$(\widehat{\mathsf{cnv}}_1\,\mathsf{cnv}_1)^{P_1} \cdots (\widehat{\mathsf{cnv}}_h\,\mathsf{cnv}_h)^{P_h}\,\mathsf{RES}.$$

The last ingredient we need is that of a simulator $\boldsymbol{\sigma}$, which is modeled as a converter to be attached to the adversarial interface E, simply denoted $\boldsymbol{\sigma}\,\mathsf{RES}$ (rather than the more pedantic $\boldsymbol{\sigma}^E\,\mathsf{RES}$, since throughout this thesis the adversarial interface will always be denoted E). With this, we can now express composable security of an $\mathcal{H}$-protocol $\boldsymbol{\pi}$ in terms of substitutions as follows.

Definition 2.4.3 (Construction)**.** For $\mathcal{P}$-resources REAL and IDEAL, and a list of substitutions $\mathsf{s}_1, \mathsf{s}_2, \ldots$, we say that an $\mathcal{H}$-protocol $\boldsymbol{\pi}$, for $\overline{\mathcal{H}} = \{E\}$, *constructs* IDEAL *from* REAL *assuming* $\mathsf{s}_1, \mathsf{s}_2, \ldots$, denoted

$$\mathsf{REAL} \overset{\boldsymbol{\pi};\mathsf{s}_1,\mathsf{s}_2,\ldots}{\longmapsto} \mathsf{IDEAL},$$

if there exists a simulator $\boldsymbol{\sigma}$ such that,

$$(\mathsf{s}_1, \mathsf{s}_2, \ldots) \implies \boldsymbol{\pi}\,\mathsf{REAL} \eqsim \boldsymbol{\sigma}\,\mathsf{IDEAL}.$$

The intuition behind Definition 2.4.3 is that if $\mathcal{S}$ is a reasonable set of substitutions, then in any context where IDEAL is needed, $\boldsymbol{\pi}\,\mathsf{REAL}$ can be safely used instead. Recall that the advantage of composable security notions, as opposed to simple substitutions capturing conventional game-based security notions, is that they naturally compose. This is the central point of composable security definitions, and is formalized by the following theorem, following directly from [MR11] (we nevertheless provide a short proof of this special formulation using substitutions).

Theorem 2.4.4 (Composition)**.** *For any $\mathcal{P}$-resources $\mathsf{R}, \mathsf{S}, \mathsf{T}$, $\mathcal{H}$-protocols $\boldsymbol{\pi}_1, \boldsymbol{\pi}_2$, for $\overline{\mathcal{H}} = \{E\}$, and lists of substitutions $\mathsf{s}_{1,1}, \mathsf{s}_{1,2}, \ldots$, $\mathsf{s}_{2,1}, \mathsf{s}_{2,2}, \ldots$, if*

$$\mathsf{R} \overset{\boldsymbol{\pi}_1;\mathsf{s}_{1,1},\mathsf{s}_{1,2},\ldots}{\longmapsto} \mathsf{S} \quad \textit{and} \quad \mathsf{S} \overset{\boldsymbol{\pi}_2;\mathsf{s}_{2,1},\mathsf{s}_{2,2},\ldots}{\longmapsto} \mathsf{T}$$

then

$$\mathsf{R} \overset{\boldsymbol{\pi}_2\boldsymbol{\pi}_1;\mathsf{s}_{1,1},\mathsf{s}_{1,2},\ldots,\mathsf{s}_{2,1},\mathsf{s}_{2,2},\ldots}{\Longrightarrow} \mathsf{T}.$$

Proof. From the assumption, we have that there exist simulators $\boldsymbol{\sigma}_1, \boldsymbol{\sigma}_2$ such that:

- $\mathsf{s}_{1,1}, \mathsf{s}_{1,2}, \ldots \implies \boldsymbol{\pi}_1\,\mathsf{R} \eqsim \boldsymbol{\sigma}_1\,\mathsf{S}$, and
- $\mathsf{s}_{2,1}, \mathsf{s}_{2,2}, \ldots \implies \boldsymbol{\pi}_2\,\mathsf{S} \eqsim \boldsymbol{\sigma}_2\,\mathsf{T}$.

Therefore,

$$\begin{aligned}
\boldsymbol{\pi}_2\boldsymbol{\pi}_1\,\mathsf{R} &\equiv \boldsymbol{\pi}_2(\boldsymbol{\pi}_1\,\mathsf{R}) \\
&\eqsim \boldsymbol{\pi}_2(\boldsymbol{\sigma}_1\,\mathsf{S}) && (\mathsf{s}_{1,1}, \mathsf{s}_{1,2}, \ldots) \\
&\equiv \boldsymbol{\sigma}_1(\boldsymbol{\pi}_2\,\mathsf{S}) \\
&\eqsim \boldsymbol{\sigma}_1(\boldsymbol{\sigma}_2\,\mathsf{T}) && (\mathsf{s}_{2,1}, \mathsf{s}_{2,2}, \ldots) \\
&\equiv (\boldsymbol{\sigma}_1\boldsymbol{\sigma}_2)\,\mathsf{T},
\end{aligned}$$

which means that there exists a simulator $\boldsymbol{\sigma}$ (that is, $\boldsymbol{\sigma}_1\boldsymbol{\sigma}_2$), such that

$$\mathsf{s}_{1,1}, \mathsf{s}_{1,2}, \ldots \mathsf{s}_{2,1}, \mathsf{s}_{2,2}, \ldots \implies \boldsymbol{\pi}_2\boldsymbol{\pi}_1\,\mathsf{R} \eqsim \boldsymbol{\sigma}\,\mathsf{T}. \qquad \square$$

Chapter 3

Anonymity Preservation: Secret-Key Primitives

3.1 Introduction

When transmitting messages in the symmetric-key setting, where communicating parties share secret keys a priori, traditionally *confidentiality* and *authenticity* are the security properties that are mostly considered. Confidentiality guarantees exclusivity of the receiving party (no one but the receiver should be able to gain any partial information about the transmitted message, possibly other than its length), while authenticity guarantees exclusivity of the sending party (no one except the sender should be able to convince the receiver that it indeed originated the message). But in a scenario where there are more than just two communicating parties using the same protocol, e.g., many senders and one receiver (as considered in this work), another important security property must be taken into account, namely *anonymity*.

For the mentioned setting, we are more specifically interested in *external sender anonymity*, that is, the property that guarantees that no one but the receiver can learn from which sender a message originated. The main focus of our work is on security definitions which capture exactly this guarantee (in particular, note that we are not addressing other common forms of anonymity usually found in the literature, arising

for instance from traffic-flow analysis).

3.1.1 Motivation

Anonymity, as opposed to confidentiality and authenticity, in most settings (as is the case for the one considered here) cannot be "created out of the blue"; rather, an intrinsic property of anonymity is that it can be *preserved*. In the game-based spirit of security definitions, this is reflected by the fact that conventional anonymity notions are captured by the concept of *key-indistinguishability* of a scheme originally intended to provide other forms of security, as confidentiality or authenticity. More specifically, in the symmetric-key setting this means that anonymity is a property that needs to be provided in conjunction with confidentiality for encryption schemes and with authenticity for MAC schemes.

But when considered from a composable standpoint, the fact that anonymity can merely be preserved becomes even more evident: consider for example a protocol employing a MAC scheme and shared secret keys between the senders and the receiver, which is executed on top of an insecure channel to obtain an authenticated channel; if one wishes for the constructed channel to additionally be also anonymous, it must be the case that the insecure channel is anonymous as well, and this construction is still possible precisely if the employed MAC scheme not only is unforgeable, but is also key-indistinguishable.

The latter considerations were made explicit by Alwen, Hirt, Maurer, Patra, and Raykov in [AHM+15], and our work can be seen as a continuation and refinement of this line of research: Here we consider the construction of an anonymous *secure* (confidential *and* authenticated) channel from an anonymous authenticated one, and show that this is possible precisely if the employed encryption scheme not only has indistinguishable ciphertexts, but also indistinguishable keys. Moreover, we show that only if a secure authenticated encryption scheme which is key-indistinguishable is employed, one can construct the anonymous secure channel directly from the anonymous insecure one.

3.1.2 Contributions

We consider the following setting: n parties, the senders, wish to securely and anonymously transmit messages to the same party, the re-

ceiver, and we assume that the receiver a priori shares a (different) secret key with each of the n senders. Since all of our treatment is in the *symmetric-key* setting, and the considered protocols employ *probabilistic* (as opposed to nonce-based) schemes, we often tacitly assume these two facts throughout this chapter. Moreover, since the meaning of security usually depends on the context, we adopt the convention that for a cryptographic scheme by *anonymous security* we mean anonymity (in form of key-indistinguishability) in conjunction with its conventionally associated security notion, that is, confidentiality for encryption, authenticity for MAC, and confidentiality plus authenticity (usually simply referred to as just security) for authenticated encryption.

Game-Based Security Definitions. We start by providing game-based security definitions capturing anonymity for both *probabilistic encryption* (pE) and *probabilistic authenticated encryption* (pAE) using the substitution framework introduced in Section 2.3. For the former, we revisit the notion of *key-indistinguishability*, originally put forth by Fischlin [Fis99], and subsequently treated in [Des00] by Desai and in [AR02] by Abadi and Rogaway. In all three works this notion has been expressed for $n = 2$ senders; here we generalize it to an arbitrary number of senders. For *nonce-based* authenticated encryption (nAE), the analogous notion of key-indistinguishability has been recently put forth by Chan and Rogaway [CR19]. Here we propose a concise definition for the case of pAE instead.

For both pE and pAE we show the relevant implications among the introduced security definitions, exposing the concrete security losses surfacing from the reductions. Furthermore, we formally show that indeed the strong security notion of *indistinguishability from random ciphertexts* (dubbed ind$, and valid for both schemes) implies key-indistinguishability. Finally, we prove that the Encrypt-then-MAC (EtM) paradigm, applied on secure and anonymous pE and probabilistic MAC (pMAC), yields pAE which is not only secure, but crucially also anonymous, thus confirming that EtM is *anonymity-preserving*.

Composable Security Definitions. We next move to the focal point of our work, the composable treatment of anonymity. Here we introduce alternative security definitions within the *constructive cryptography* (CC) framework of Maurer and Renner [MR11, Mau12] introduced in Section 2.4, which enjoy composability and allow to make explicit security goals from an application point of view.

First we phrase the desired security properties of (symmetric-key) protocols as specific constructions of cryptographic communication channels. More concretely, we start by defining the following resources which expose n interfaces to send messages and one to receive them: the *insecure anonymous channel* (A-INS), the *authenticated anonymous channel* (A-AUT), and the *secure anonymous channel* (A-SEC). Then we state that a protocol (executed by the senders and the receiver, which share secret keys a priori) provides *authenticity in conjunction with anonymity* if it constructs A-AUT from A-INS, provides *confidentiality in conjunction with anonymity* if it constructs A-SEC from A-AUT, and provides *security (i.e., confidentiality and authenticity) in conjunction with anonymity* if it constructs A-SEC directly from A-INS.

Secondly, we establish relations between the previously introduced game-based security definitions and their composable counterparts, that is, we show sufficiency conditions in terms of game-based definitions for the above mentioned constructions. As already mentioned earlier, in [AHM+15] it was shown that key-indistinguishable pMAC schemes enable the construction of A-AUT from A-INS. Here we show that anonymous secure pE enables the next logical step, namely the construction of A-SEC from A-AUT. In terms of time-complexity, this significantly improves upon the MAC-based solution proposed in [AHM+15] for the same construction. Furthermore, we show that these two steps can be performed in one shot using authenticated encryption instead, that is, we show that anonymous secure pAE constructs a A-SEC directly from A-INS. Again, this significantly improves upon the MAC-based solution proposed in [AHM+15] for the same construction. Moreover, this provides further evidence of the anonymity preservation of EtM.

Preferring Probabilistic Schemes for Anonymity. We observe that our constructive treatment strengthens the role of probabilistic authenticated encryption in contrast to its nonce-based counterpart when it comes to anonymity. According to Rogaway [Rog04], a main advantage provided by nonces is that

> *"encryption schemes constructed to be secure under nonce-based security notions may be less prone to misuse".*

Nevertheless, this raises concerns about attacks in the multi-user (mu) setting, where crucially anonymity lives. For this reason in TLS 1.3 a *randomized nonces* mechanism has been proposed for the employed

nAE scheme, AES with GCM (Galois/Counter Mode). This recently spawned work by Bellare and Tackmann [BT16] and Hoang, Tessaro, and Thiruvengadam [HTT18], which initiated and refined the study of mu security of nAE in order to rigorously formalize security under such randomized nonces mechanism (but they did not address anonymity, in the form of key-indistinguishability).

But quoting again Rogaway [Rog11, I.8 (page 22)],

> "[if] *an IV-based encryption scheme* [...] *is good in the nonce-based framework* [...] *then it is also good in the probabilistic setting",*

which implies that an ind$-secure nAE scheme is an ind$-secure pAE scheme, when the nonce is randomized (if one ignores the concept of *associated data*). Therefore, in view of our previously mentioned result attesting that ind$-secure pAE implies anonymity, our work can be considered as a confirmation that the random nonce mechanism, if used with an ind$-secure nAE scheme and under the assumption that the nonces are indeed truly uniformly random, also provides anonymity. Note that our consideration here is rather informal, and a more thorough study should be carried out to also incorporate the issue of nonce repetition and related birthday paradox security bounds (in our discussion, we are assuming a setting where not too many messages are exchanged).

This is to be compared to a recent work by Chan and Rogaway [CR19], which studies the anonymity of nAE: the authors observe that because of the session-related nature of the nonces, nAE actually fails to generally provide anonymity. For this reason, they introduce a transformation (dubbed NonceWrap) which converts an nAE scheme into a (syntactically different) new scheme, *anonymous* nAE (anAE), which they show does achieve anonymity (i.e., key-indistinguishability).

3.1.3 Related Work

The concept of key-indistinguishability has been first introduced under the name of *"key-hiding private-key encryption"* by Fischlin in [Fis99] (captured by our notion of 2-ik-cpa, according to Definition 3.2.1). Subsequently, in [Des00], Desai also studied the problem introducing the concept of *"non-separability of keys"*, but specifically for encryption schemes based on block ciphers. Later, in [AR02], Abadi and Rogaway presented a security notion called *"which-key concealing"*, that is basically

identical to Fischlin's, but they defined security as a combination of key-indistinguishability and ciphertext-indistinguishability (captured by our notion of 2-ik-ind-cpa according to Definition 3.2.3). They also claimed that popular modes of operation for symmetric encryption yield key-private encryption schemes. We will prove this formally in Section 3.2.2. The concept of key-indistinguishability has been translated to the public-key setting by Bellare, Boldyreva, Desai, and Pointcheval in [BBDP01], where the terms *key-privacy* and *indistinguishability of keys* were originally suggested.

As previously mentioned, regarding key-indistinguishability of ae, in a recent work Chan and Rogaway [CR19] introduce the nonce-based counterpart of our notion for pAE, Definition 3.2.4, which is crucially *not* directly applicable to nAE, but rather to anAE, a syntactically different scheme which can be obtained from nAE through the transformation NonceWrap that they introduce.

3.2 Game-Based Security of pE and pAE

For the conventional security notions capturing confidentiality and authenticity for probabilistic encryption (pE) and probabilistic authenticated encryption (pAE), as well as for the systems used to define notions of security for pE and pAE, we refer to Section 2.3.4.

Regarding the game-based definitions of anonymity for pE and pAE, we adopt what in the literature is usually termed *key-indistinguishability*. We begin by providing a game-based security definition capturing exclusively the notion of anonymity (in terms of key-indistinguishability) of pE and pAE. Roughly speaking, the notion guarantees that an adversary cannot distinguish between n distinct and independent copies of system $\mathbf{E}_{k_i}$, each of which is parameterized by a different, freshly and independently sampled key k_i, from n copies of the same system $\mathbf{E}_{k_1}$, each of which is parameterized by the same key k_1 (previously freshly sampled).

Definition 3.2.1 (n-ik-cpa)**.**

$$[\mathbf{E}_{k_1}, \ldots, \mathbf{E}_{k_n}] \eqcirc [\![\underbrace{\mathbf{E}_{k_1}, \ldots, \mathbf{E}_{k_1}}_{n \text{ times}}]\!],$$

for independent $k_1, \ldots, k_n \leftarrow \mathsf{Gen}$.

Definition 3.2.2 (n-ik-cca)**.**

$$[[\mathbf{E}_{k_1}, \mathbf{D}_{k_1}]], \ldots, [[\mathbf{E}_{k_n}, \mathbf{D}_{k_n}]] \backsimeq [[\underbrace{\rho^{\mathsf{ctxt}}(\mathbf{E}_{k_1}), \ldots, \rho^{\mathsf{ctxt}}(\mathbf{E}_{k_1})}_{n \text{ times}}]],$$

for independent $k_1, \ldots, k_n \leftarrow \mathtt{Gen}$.

Next, we define the coupling of the traditional security goal of pE/pAE with anonymity. For both notions, we use the term *anonymous security*; specifically, by anonymous and secure pE we mean key-indistinguishable and confidential encryption, whereas by anonymous and secure pAE we mean key-indistinguishable, confidential, and authenticated encryption.

Definition 3.2.3 (n-ik-ind-cpa)**.**

$$[\mathbf{E}_{k_1}, \ldots, \mathbf{E}_{k_n}] \backsimeq [[\underbrace{\rho^{\mathsf{cpa}}(\mathbf{E}_{k_1}), \ldots, \rho^{\mathsf{cpa}}(\mathbf{E}_{k_1})}_{n \text{ times}}]],$$

for independent $k_1, \ldots, k_n \leftarrow \mathtt{Gen}$.

Definition 3.2.4 (n-ik-ae)**.**

$$[[\mathbf{E}_{k_1}, \mathbf{D}_{k_1}]], \ldots, [[\mathbf{E}_{k_n}, \mathbf{D}_{k_n}]] \backsimeq [[\underbrace{\rho^{\mathsf{ae}}(\mathbf{E}_{k_1}), \ldots, \rho^{\mathsf{ae}}(\mathbf{E}_{k_1})}_{n \text{ times}}]],$$

for independent $k_1, \ldots, k_n \leftarrow \mathtt{Gen}$.

3.2.1 Relations Among Notions

We now show that the combinations of ciphertext-indistinguishability and key-indistinguishability, ind-cpa + ik-cpa for pE and ae + ik-ae for pAE, are equivalent to the respective game-based notions capturing both goals simultaneously, ik-ind-cpa for pE and ik-ae for pAE, regardless of the number of users.

We start by showing that key-indistinguishability is preserved up to constant increase when the number of users is incremented.

Lemma 3.2.5. 2-ik-cpa $\xrightarrow{n-1}$ n-ik-cpa*, for any* $n \in \mathbb{N}$.

Proof. Let $k_1, \ldots, k_n \leftarrow \mathtt{Gen}$, and consider

$$\rho_i([[\mathbf{X}, \mathbf{Y}]]) \doteq [[\underbrace{\mathbf{X}, \ldots, \mathbf{X}}_{i \text{ times}}, \mathbf{Y}, \mathbf{E}_{k_{i+2}}, \ldots, \mathbf{E}_{k_n}]],$$

for $i \in [n-1]$. Note that:

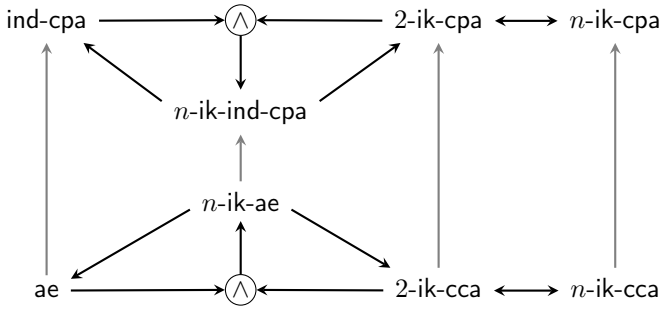


Figure 3.1: Relations among ciphertext-indistinguishability and key-indistinguishability notions. The gray arrows indicate trivial implications.

- $\rho_1([\mathbf{E}_{k_1}, \mathbf{E}_{k_2}]) \equiv [\mathbf{E}_{k_1}, \ldots, \mathbf{E}_{k_n}]$,
- $\rho_{n-1}([\![\mathbf{E}_{k_1}, \mathbf{E}_{k_1}]\!]) \equiv [\![\underbrace{\mathbf{E}_{k_1}, \ldots, \mathbf{E}_{k_1}}_{n \text{ times}}]\!]$, and
- $\rho_i([\![\mathbf{E}_{k_1}, \mathbf{E}_{k_1}]\!]) \equiv \rho_{i+1}([\mathbf{E}_{k_1}, \mathbf{E}_{k_{i+2}}])$, for any $i \in [n-2]$.

Then, since by 2-ik-cpa we have

$$[\mathbf{E}_{k_1}, \mathbf{E}_{k_{i+1}}] \backsimeq [\![\mathbf{E}_{k_1}, \mathbf{E}_{k_1}]\!],$$

for any $i \in [n-1]$, by Lemma 2.3.2 it follows that

$$\rho_1([\mathbf{E}_{k_1}, \mathbf{E}_{k_2}]) \backsimeq \rho_{n-1}([\![\mathbf{E}_{k_1}, \mathbf{E}_{k_1}]\!]).$$

Therefore,

$$[\mathbf{E}_{k_1}, \ldots, \mathbf{E}_{k_n}] \backsimeq [\![\underbrace{\mathbf{E}_{k_1}, \ldots, \mathbf{E}_{k_1}}_{n \text{ times}}]\!]. \qquad \square$$

Lemma 3.2.6. 2-ik-cca $\xrightarrow{n-1}$ n-ik-cca*, for any* $n \in \mathbb{N}$.

Proof. Let $k_1, \ldots, k_n \leftarrow \mathtt{Gen}$, and consider

- $\rho_1([\![[\![\mathbf{X}_1, \mathbf{Y}_1]\!], [\![\mathbf{X}_2, \mathbf{Y}_2]\!]]\!])$
  $\doteq [\![[\![\mathbf{X}_1, \mathbf{Y}_1]\!], [\![\mathbf{X}_2, \mathbf{Y}_2]\!], [\![\mathbf{E}_{k_3}, \mathbf{D}_{k_3}]\!], \ldots, [\![\mathbf{E}_{k_n}, \mathbf{D}_{k_n}]\!]]\!]$,

  and

- $\rho_i([\![[\![\mathbf{X}_1, \mathbf{Y}_1]\!], [\![\mathbf{X}_2, \mathbf{Y}_2]\!]]\!] \doteq [\![\underbrace{\rho^{\mathsf{ctxt}}(\mathbf{X}_1), \ldots, \rho^{\mathsf{ctxt}}(\mathbf{X}_1)}_{i \text{ times}},$
  $[\![\mathbf{X}_2, \mathbf{Y}_2]\!], [\![\mathbf{E}_{k_{i+2}}, \mathbf{D}_{k_{i+2}}]\!], \ldots, [\![\mathbf{E}_{k_n}, \mathbf{D}_{k_n}]\!]]\!]$,
  for $i = 2, \ldots, n-1$.

Note that:

- $\rho_1([[\![\mathbf{E}_{k_1}, \mathbf{D}_{k_1}]\!], [\![\mathbf{E}_{k_2}, \mathbf{D}_{k_2}]\!]]) \equiv [[\![\mathbf{E}_{k_1}, \mathbf{D}_{k_1}]\!], \ldots, [\![\mathbf{E}_{k_n}, \mathbf{D}_{k_n}]\!]]$,
- $\rho_{n-1}([\![\rho^{\mathsf{ctxt}}(\mathbf{E}_{k_1}), \rho^{\mathsf{ctxt}}(\mathbf{E}_{k_1})]\!]) \equiv [\![\underbrace{\rho^{\mathsf{ctxt}}(\mathbf{E}_{k_1}), \ldots, \rho^{\mathsf{ctxt}}(\mathbf{E}_{k_1})}_{n \text{ times}}]\!]$, and
- $\rho_i([\![\rho^{\mathsf{ctxt}}(\mathbf{E}_{k_1}), \rho^{\mathsf{ctxt}}(\mathbf{E}_{k_1})]\!]) \equiv \rho_{i+1}([[\![\mathbf{E}_{k_1}, \mathbf{D}_{k_1}]\!], [\![\mathbf{E}_{k_{i+2}}, \mathbf{D}_{k_{i+2}}]\!]])$, for any $i \in [n-2]$.

Then, since by 2-ik-cca we have

$$[[\![\mathbf{E}_{k_1}, \mathbf{D}_{k_1}]\!], [\![\mathbf{E}_{k_{i+1}}, \mathbf{D}_{k_{i+1}}]\!]] \backsimeq [\![\rho^{\mathsf{ctxt}}(\mathbf{E}_{k_1}), \rho^{\mathsf{ctxt}}(\mathbf{E}_{k_1})]\!],$$

for any $i \in [n-1]$, by Lemma 2.3.2 it follows that

$$\rho_1([[\![\mathbf{E}_{k_1}, \mathbf{D}_{k_1}]\!], [\![\mathbf{E}_{k_2}, \mathbf{D}_{k_2}]\!]]) \backsimeq \rho_{n-1}([\![\rho^{\mathsf{ctxt}}(\mathbf{E}_{k_1}), \rho^{\mathsf{ctxt}}(\mathbf{E}_{k_1})]\!]).$$

Therefore,

$$[[\![\mathbf{E}_{k_1}, \mathbf{D}_{k_1}]\!], \ldots, [\![\mathbf{E}_{k_n}, \mathbf{D}_{k_n}]\!]] \backsimeq [\![\underbrace{\rho^{\mathsf{ctxt}}(\mathbf{E}_{k_1}), \ldots, \rho^{\mathsf{ctxt}}(\mathbf{E}_{k_1})}_{n \text{ times}}]\!]. \qquad \square$$

Next, we confirm the natural intuition that ciphertext-indistinguishability is also preserved when coupled with key-indistinguishability.

Lemma 3.2.7. $(2\text{-ik-cpa}, \mathsf{ind\text{-}cpa}) \xrightarrow{n-1,1} n\text{-ik-ind-cpa}$.

Proof. Let $k_1, \ldots, k_n \leftarrow \mathtt{Gen}$, and consider

$$\rho(\mathbf{X}) \doteq [\![\underbrace{\mathbf{X}, \ldots, \mathbf{X}}_{n \text{ times}}]\!].$$

Then, using Lemma 3.2.5:

$$\begin{aligned}
[\mathbf{E}_{k_1}, \ldots, \mathbf{E}_{k_n}] &\eqsim \underbrace{[\![\mathbf{E}_{k_1}, \ldots, \mathbf{E}_{k_1}]\!]}_{n \text{ times}} && (n\text{-ik-cpa}) \\
&= \rho(\mathbf{E}_{k_1}) \\
&\eqsim \rho \circ \rho^{\mathsf{cpa}}(\mathbf{E}_{k_1}) && (\text{ind-cpa}) \\
&= \underbrace{[\![\rho^{\mathsf{cpa}}(\mathbf{E}_{k_1}), \ldots, \rho^{\mathsf{cpa}}(\mathbf{E}_{k_1})]\!]}_{n \text{ times}}. && \square
\end{aligned}$$

Lemma 3.2.8. $(2\text{-ik-cca}, \mathsf{ae}) \xrightarrow{n-1,1} n\text{-ik-ae}$.

Proof. Let $k_1, \ldots, k_n \leftarrow \mathtt{Gen}$, and consider

$$\rho([\![\mathbf{X}, \mathbf{Y}]\!]) \doteq \underbrace{[\![\rho^{\mathsf{ctxt}}(\mathbf{X}), \ldots, \rho^{\mathsf{ctxt}}(\mathbf{X})]\!]}_{n \text{ times}}.$$

Moreover, note that $\rho^{\mathsf{ae}} \circ \rho^{\mathsf{ctxt}} \equiv \rho^{\mathsf{ae}}$. Then, using Lemma 3.2.6:

$$\begin{aligned}
[[\![\mathbf{E}_{k_1}, \mathbf{D}_{k_1}]\!], \ldots, [\![\mathbf{E}_{k_n}, \mathbf{D}_{k_n}]\!]] &\eqsim \underbrace{[\![\rho^{\mathsf{ctxt}}(\mathbf{E}_{k_1}), \ldots, \rho^{\mathsf{ctxt}}(\mathbf{E}_{k_1})]\!]}_{n \text{ times}} && (n\text{-ik-cca}) \\
&= \rho([\![\mathbf{E}_{k_1}, \mathbf{D}_{k_1}]\!]) \\
&\eqsim \rho \circ \rho^{\mathsf{ae}}(\mathbf{E}_{k_1}) && (\mathsf{ae}) \\
&= \underbrace{[\![\rho^{\mathsf{ae}} \circ \rho^{\mathsf{ctxt}}(\mathbf{E}_{k_1}) \ldots, \rho^{\mathsf{ae}} \circ \rho^{\mathsf{ctxt}}(\mathbf{E}_{k_1})]\!]}_{n \text{ times}} \\
&\equiv \underbrace{[\![\rho^{\mathsf{ae}}(\mathbf{E}_{k_1}), \ldots, \rho^{\mathsf{ae}}(\mathbf{E}_{k_1})]\!]}_{n \text{ times}}. && \square
\end{aligned}$$

Note that similarly to Lemma 3.2.7, also n-ik-cpa security coupled with ind-cpa security implies n-ik-ind-cpa security, and similarly to Lemma 3.2.8, also n-ik-cca security coupled with ae security implies n-ik-ae security. We now turn to the necessary conditions; first we show that indeed the combined notions of ciphertext-indistinguishability and key-indistinguishability imply key-indistinguishability.

Lemma 3.2.9. $n\text{-ik-ind-cpa} \xrightarrow{2} 2\text{-ik-cpa}$.

Proof. Let $k_1, \ldots, k_n \leftarrow \mathsf{Gen}$, and consider $\rho_1(\llbracket \mathbf{X}_1, \ldots, \mathbf{X}_n \rrbracket) \doteq \llbracket \mathbf{X}_1, \mathbf{X}_2 \rrbracket$ and $\rho_2(\llbracket \mathbf{X}_1, \ldots, \mathbf{X}_n \rrbracket) \doteq \llbracket \mathbf{X}_1, \mathbf{X}_1 \rrbracket$. Then:

$$\begin{aligned}
[\mathbf{E}_{k_1}, \mathbf{E}_{k_2}] &= \rho_1([\mathbf{E}_{k_1}, \ldots, \mathbf{E}_{k_n}]) \\
&\doteqdot \rho_1(\underbrace{\llbracket \rho^{\mathsf{cpa}}(\mathbf{E}_{k_1}), \ldots, \rho^{\mathsf{cpa}}(\mathbf{E}_{k_1}) \rrbracket}_{n \text{ times}}) && (n\text{-ik-ind-cpa}) \\
&= \llbracket \rho^{\mathsf{cpa}}(\mathbf{E}_{k_1}), \rho^{\mathsf{cpa}}(\mathbf{E}_{k_1}) \rrbracket \\
&= \rho_2(\underbrace{\llbracket \rho^{\mathsf{cpa}}(\mathbf{E}_{k_1}), \ldots, \rho^{\mathsf{cpa}}(\mathbf{E}_{k_1}) \rrbracket}_{n \text{ times}}) \\
&\doteqdot \rho_2([\mathbf{E}_{k_1}, \ldots, \mathbf{E}_{k_n}]) && (n\text{-ik-ind-cpa}) \\
&= \llbracket \mathbf{E}_{k_1}, \mathbf{E}_{k_1} \rrbracket. && \square
\end{aligned}$$

Lemma 3.2.10. n-ik-ae $\xrightarrow{2}$ 2-ik-cca.

Proof. Let $k_1, \ldots, k_n \leftarrow \mathsf{Gen}$, and consider $\rho_1(\llbracket \mathbf{X}_1, \ldots, \mathbf{X}_n \rrbracket) \doteq \llbracket \mathbf{X}_1, \mathbf{X}_2 \rrbracket$ and $\rho_2(\llbracket \mathbf{X}_1, \ldots, \mathbf{X}_n \rrbracket) \doteq \llbracket \rho^{\mathsf{ctxt}}(\mathbf{X}_1), \rho^{\mathsf{ctxt}}(\mathbf{X}_1) \rrbracket$. Moreover, note that $\rho^{\mathsf{ctxt}} \circ \rho^{\mathsf{ae}} = \rho^{\mathsf{ctxt}} \circ \rho^{\mathsf{ctxt}} \circ \rho^{\mathsf{cpa}} \equiv \rho^{\mathsf{ctxt}} \circ \rho^{\mathsf{cpa}} = \rho^{\mathsf{ae}}$. Then:

$$\begin{aligned}
[\llbracket \mathbf{E}_{k_1}, \mathbf{D}_{k_1} \rrbracket, \llbracket \mathbf{E}_{k_2}, \mathbf{D}_{k_2} \rrbracket] &= \rho_1([\llbracket \mathbf{E}_{k_1}, \mathbf{D}_{k_1} \rrbracket, \ldots, \llbracket \mathbf{E}_{k_n}, \mathbf{D}_{k_n} \rrbracket]) \\
&\doteqdot \rho_1(\underbrace{\llbracket \rho^{\mathsf{ae}}(\mathbf{E}_{k_1}), \ldots, \rho^{\mathsf{ae}}(\mathbf{E}_{k_1}) \rrbracket}_{n \text{ times}}) && (n\text{-ik-ae}) \\
&= \llbracket \rho^{\mathsf{ae}}(\mathbf{E}_{k_1}), \rho^{\mathsf{ae}}(\mathbf{E}_{k_1}) \rrbracket \\
&\equiv \llbracket \rho^{\mathsf{ctxt}} \circ \rho^{\mathsf{ae}}(\mathbf{E}_{k_1}), \rho^{\mathsf{ctxt}} \circ \rho^{\mathsf{ae}}(\mathbf{E}_{k_1}) \rrbracket \\
&= \rho_2(\underbrace{\llbracket \rho^{\mathsf{ae}}(\mathbf{E}_{k_1}), \ldots, \rho^{\mathsf{ae}}(\mathbf{E}_{k_1}) \rrbracket}_{n \text{ times}}) \\
&\doteqdot \rho_2([\llbracket \mathbf{E}_{k_1}, \mathbf{D}_{k_1} \rrbracket, \ldots, \llbracket \mathbf{E}_{k_n}, \mathbf{D}_{k_n} \rrbracket]) && (n\text{-ik-ae}) \\
&= \llbracket \rho^{\mathsf{ctxt}}(\llbracket \mathbf{E}_{k_1}, \mathbf{D}_{k_1} \rrbracket), \rho^{\mathsf{ctxt}}(\llbracket \mathbf{E}_{k_1}, \mathbf{D}_{k_1} \rrbracket) \rrbracket \\
&\equiv \llbracket \rho^{\mathsf{ctxt}}(\mathbf{E}_{k_1}), \rho^{\mathsf{ctxt}}(\mathbf{E}_{k_1}) \rrbracket. && \square
\end{aligned}$$

Note that similarly to Lemma 3.2.9, n-ik-ind-cpa security also implies n-ik-cpa security, and similarly to Lemma 3.2.10, n-ik-ae security also implies n-ik-cca security. For the last necessary condition, we show that indeed the combined notions of ciphertext-indistinguishability and key-indistinguishability imply ciphertext-indistinguishability.

Lemma 3.2.11. n-ik-ind-cpa $\xrightarrow{1}$ ind-cpa.

Proof. Let $k_1, \ldots, k_n \leftarrow \mathtt{Gen}$, and consider $\rho(\llbracket \mathbf{X}_1, \ldots, \mathbf{X}_n \rrbracket) \doteq \mathbf{X}_1$. Then:

$$\begin{aligned}\mathbf{E}_{k_1} &= \rho([\mathbf{E}_{k_1}, \ldots, \mathbf{E}_{k_n}]) \\ &\widehat{=} \rho(\llbracket \underbrace{\rho^{\mathsf{cpa}}(\mathbf{E}_{k_1}), \ldots, \rho^{\mathsf{cpa}}(\mathbf{E}_{k_1})}_{n \text{ times}} \rrbracket) && (n\text{-ik-ind-cpa}) \\ &= \rho^{\mathsf{cpa}}(\mathbf{E}_{k_1}).\end{aligned}$$ □

Lemma 3.2.12. n-ik-ae $\xrightarrow{1}$ ae.

Proof. Let $k_1, \ldots, k_n \leftarrow \mathtt{Gen}$, and consider $\rho(\llbracket \mathbf{X}_1, \ldots, \mathbf{X}_n \rrbracket) \doteq \mathbf{X}_1$. Then:

$$\begin{aligned}\llbracket \mathbf{E}_{k_1}, \mathbf{D}_{k_1} \rrbracket &= \rho([\llbracket \mathbf{E}_{k_1}, \mathbf{D}_{k_1} \rrbracket, \ldots, \llbracket \mathbf{E}_{k_n}, \mathbf{D}_{k_n} \rrbracket]) \\ &\widehat{=} \rho(\llbracket \underbrace{\rho^{\mathsf{ae}}(\mathbf{E}_{k_1}), \ldots, \rho^{\mathsf{ae}}(\mathbf{E}_{k_1})}_{n \text{ times}} \rrbracket) && (n\text{-ik-ae}) \\ &= \rho^{\mathsf{ae}}(\mathbf{E}_{k_1}).\end{aligned}$$ □

Therefore, we showed that an encryption scheme is n-ik-ind-cpa secure if and only if it is both n-ik-cpa and ind-cpa secure, and that an authenticated encryption scheme is n-ik-ae secure if and only if it is both n-ik-cca and ae secure. Clearly both results can be cast down to the case of 2 users, in line with the security definitions of [Fis99, AR02].

Corollary 3.2.13. (ind-cpa, 2-ik-cpa) $\iff$ 2-ik-ind-cpa.

Corollary 3.2.14. (ae, 2-ik-cca) $\iff$ 2-ik-ae.

3.2.2 Uniform Ciphertexts Imply Anonymity

In this section we revisit a stronger security notion for symmetric encryption, which we call *indistinguishability from uniform ciphertexts*. It can be defined for both pE, dubbed ind$-cpa-security, and for pAE, dubbed ae$-security. We show a simple folklore result that was stated in [AR02] (of which, to the best of our knowledge, there is no formal proof yet). This definition intuitively should capture indistinguishability of plaintexts, but it actually overshoots this goal, and it is stronger in the sense that it also implies indistinguishability of keys. Recall that ind-cpa and ae security *do not* imply indistinguishability of keys, but it turns out to be easier to prove that schemes meet the stronger notion, which is also

conceptually simpler. Essentially, instead of choosing a random message to be encrypted in the ideal world, a random ciphertext is output (thus neglecting encryption altogether).

This stronger security notion appears to have been originally introduced by Rogaway, Bellare, Black, and Krovetz in [RBBK01] for proving the security of the so-called offset codebook (OCB) mode of operation for symmetric encryption.[1] A number of other important results, such as the security of counter (CTR) or cipher block chaining (CBC) modes, first carried out in [BDJR97], have been later adapted by Rogaway [Rog04] to show that such schemes actually satisfy this stronger definition.[2] In fact, as argued in [AR02] (where this security notion—targeted to encryption rather than authenticated encryption—is dubbed *type-1 security*), by the above mentioned folklore result which we prove here, such modes indeed yield key indistinguishable schemes. We remark that subsequently, this definition was also used in the field of *provable secure steganography* (for both symmetric-key and asymmetric-key schemes) [HLv02, vH04, Möl04, BC05]. In the literature, this definition is alternatively called *indistinguishability from random bits/bitstrings* or simply *pseudorandom ciphertexts* security.

In order to formalize this notion, we need to introduce the system **\$** (with implicit dependency on a fixed encryption scheme Π) which on input any message $m \in \mathcal{M}$ simply outputs a uniformly sampled ciphertext of appropriate length, that is, according to our Definition 2.3.3, a uniform random bitstring of length $|m| + \tau$, where $\tau \in \mathbb{N}$ is the expansion factor defined by Π (thus, in particular, **\$** does not make use of the underlying encryption function defined by Π). Then for the case of pE we can increase the security requirement as follows.

Definition 3.2.15 (ind\$-cpa)**.** $\mathbf{E}_k \doteq \mathbf{\$}$, for $k \leftarrow \mathtt{Gen}$.

The analogous notion for pAE was introduced by Rogaway and Shrimpton in [RS06], and is adapted within our framework as follows.

Definition 3.2.16 (ae\$)**.** $[\![\mathbf{E}_k, \mathbf{D}_k]\!] \doteq \rho^{\mathsf{ctxt}}(\mathbf{\$})$, for $k \leftarrow \mathtt{Gen}$.

[1] Note that OCB actually yields more than a secure encryption scheme: in [RBBK01] it is actually shown that OCB is *confidential* according to the mentioned stronger notion, but also *authentic*, thus making it a *secure authenticated encryption* scheme.

[2] All of those results are actually geared towards *nonce-based symmetric encryption*, but they also apply to our setting.

Next, starting with the case of pE, we show that the stronger notion of ind$-cpa indeed implies ik-ind-cpa (and thus also both ik-cpa and ind-cpa), as originally pointed out in [AR02]. This is captured formally by the following statement, shown for 2 users for cleaner presentation, but easily generalized to n users.

Theorem 3.2.17. ind$-cpa $\xrightarrow{3}$ ik-ind-cpa.

Proof. Let $k_1, k_2 \leftarrow \mathtt{Gen}$, and consider

- $\rho_1(\mathbf{X}) \doteq [\mathbf{X}, \mathbf{E}_{k_2}]$,
- $\rho_2(\mathbf{X}) \doteq [\$, \mathbf{X}]$, and
- $\rho_3(\mathbf{X}) \doteq [\![\mathbf{X}', \mathbf{Y}']\!]$, for some systems $\mathbf{X}'$ and $\mathbf{Y}'$ that behave as follows:
  - On input $m \in \mathcal{M}$ to $\mathbf{X}'$, forward m to $\mathbf{X}$, obtain $c \in \mathcal{C}$, and output c.
  - On input $m \in \mathcal{M}$ to $\mathbf{Y}'$, forward m to $\mathbf{X}$, obtain $c \in \mathcal{C}$, and output c.

Note that ρ_3 essentially *duplicates* the system $\mathbf{X}$, and therefore we have $\rho_3(\$) \equiv [\$, \$]$ and $\rho_3 \circ \rho^{\mathsf{cpa}}(\mathbf{E}_{k_1}) \equiv [\![\rho^{\mathsf{cpa}}(\mathbf{E}_{k_1}), \rho^{\mathsf{cpa}}(\mathbf{E}_{k_1})]\!]$. To see this, observe that both $\$$ and $\rho^{\mathsf{cpa}}(\mathbf{E}_{k_1})$ are stateless and internally sample fresh and independent randomness on each new input. Moreover, note that $\rho^{\mathsf{cpa}}(\$) \equiv \$$, since first sampling a uniformly random message $\tilde{m} \xleftarrow{\$} \{0,1\}^{|m|}$, on input message m, and subsequently sampling a uniformly random ciphertext $c \xleftarrow{\$} \{0,1\}^{|\tilde{m}|}$, is the same as directly sampling a

uniformly random ciphertext $c \xleftarrow{\$} \{0,1\}^{|m|}$, on input message m. Then:

$$\begin{aligned}
[\mathbf{E}_{k_1}, \mathbf{E}_{k_2}] &= \rho_1(\mathbf{E}_{k_1}) \\
&\eqsim \rho_1(\$) && (\mathsf{ind\$\text{-}cpa}) \\
&= [\$, \mathbf{E}_{k_2}] \\
&= \rho_2(\mathbf{E}_{k_2}) \\
&\eqsim \rho_2(\$) && (\mathsf{ind\$\text{-}cpa}) \\
&= [\$, \$] \\
&\equiv \rho_3(\$) \\
&\equiv \rho_3 \circ \rho^{\mathsf{cpa}}(\$) \\
&\eqsim \rho_3 \circ \rho^{\mathsf{cpa}}(\mathbf{E}_{k_1}) && (\mathsf{ind\$\text{-}cpa}) \\
&\equiv [\![\rho^{\mathsf{cpa}}(\mathbf{E}_{k_1}), \rho^{\mathsf{cpa}}(\mathbf{E}_{k_1})]\!]. && \square
\end{aligned}$$

Finally, the analogous statement for the case of pAE follows as a natural lifting of Theorem 3.2.17, that is, we next show that the stronger notion of ae\$ indeed implies ik-ae (and thus also both ik-cca and ae). We remark that this fact was informally pointed out by Rogaway [Rog13].

Theorem 3.2.18. $\mathsf{ae\$} \xrightarrow{3} \mathsf{ik\text{-}ae}$.

Proof. Let $k_1, k_2 \leftarrow \mathtt{Gen}$, and consider

- $\rho_1([\![\mathbf{X}, \mathbf{Y}]\!]) \doteq [[\![\mathbf{X}, \mathbf{Y}]\!], [\![\mathbf{E}_{k_2}, \mathbf{D}_{k_2}]\!]]$,
- $\rho_2([\![\mathbf{X}, \mathbf{Y}]\!]) \doteq [\rho^{\mathsf{ctxt}}(\$), [\![\mathbf{X}, \mathbf{Y}]\!]]$, and
- $\rho_3([\![\mathbf{X}, \mathbf{Y}]\!]) \equiv [\![[\![\mathbf{X}'_1, \mathbf{Y}'_1]\!], [\![\mathbf{X}'_2, \mathbf{Y}'_2]\!]]\!]$, for some correlated systems $\mathbf{X}'_1$, $\mathbf{Y}'_1$, $\mathbf{X}'_2$, and $\mathbf{Y}'_2$ that behave as follows: Initially set $\mathcal{Q}_1, \mathcal{Q}_2 \subseteq \mathcal{M} \times \mathcal{C}$ to $\varnothing$, and then:
  - On input $m \in \mathcal{M}$ to $\mathbf{X}'_1$, forward m to $\mathbf{X}$, obtain $c \in \mathcal{C}$, set $\mathcal{Q}_1$ to $\mathcal{Q}_1 \cup \{(m, c)\}$, and output c.
  - On input $c \in \mathcal{C}$ to $\mathbf{Y}'_1$, if there exists an $m \in \mathcal{M}$ such that $(m, c) \in \mathcal{Q}_1$, then output m, otherwise output $\perp$.
  - On input $m \in \mathcal{M}$ to $\mathbf{X}'_2$, forward m to $\mathbf{X}$, obtain $c \in \mathcal{C}$, set $\mathcal{Q}_2$ to $\mathcal{Q}_2 \cup \{(m, c)\}$, and output c.

– On input $c \in \mathcal{C}$ to $\mathbf{Y}'_2$, if there exists an $m \in \mathcal{M}$ such that $(m, c) \in \mathcal{Q}_2$, then output m, otherwise output $\perp$.

Also recall the transformation ρ^{enc} from Section 2.3.4, which is such that $\rho^{\mathsf{enc}}([\![\mathbf{X}, \mathbf{Y}]\!]) \equiv \mathbf{X}$. Note that ρ_3 ignores system $\mathbf{Y}$, and therefore, since both $\rho^{\mathsf{ctxt}}(\$)$ and $\rho^{\mathsf{ae}}(\mathbf{E}_{k_1})$ are stateless and internally sample fresh and independent randomness on each new input, we have $\rho_3 \circ \rho^{\mathsf{ctxt}}(\$) \equiv [\rho^{\mathsf{ctxt}}(\$), \rho^{\mathsf{ctxt}}(\$)]$ and $\rho_3 \circ \rho^{\mathsf{ae}}(\mathbf{E}_{k_1}) \equiv [\![\rho^{\mathsf{ae}}(\mathbf{E}_{k_1}), \rho^{\mathsf{ae}}(\mathbf{E}_{k_1})]\!]$. Thus, ρ_3 essentially *duplicates* systems $\rho^{\mathsf{ctxt}}(\$)$ and $\rho^{\mathsf{ae}}(\mathbf{E}_{k_1})$. Moreover, note that $\rho^{\mathsf{ae}} \circ \rho^{\mathsf{enc}} \circ \rho^{\mathsf{ctxt}}(\$) \equiv \rho^{\mathsf{ctxt}}(\$)$, since the decryption oracle of ρ^{ctxt} is ignored, and since first sampling a uniformly random message $\tilde{m} \xleftarrow{\$} \{0,1\}^{|m|}$, on input message m, and subsequently sampling a uniformly random ciphertext $c \xleftarrow{\$} \{0,1\}^{|\tilde{m}|}$, is the same as directly sampling a uniformly random ciphertext $c \xleftarrow{\$} \{0,1\}^{|m|}$, on input message m. Then:

$$
\begin{aligned}
[[\![\mathbf{E}_{k_1}, \mathbf{D}_{k_1}]\!], [\![\mathbf{E}_{k_2}, \mathbf{D}_{k_2}]\!]] &= \rho_1([\![\mathbf{E}_{k_1}, \mathbf{D}_{k_1}]\!]) \\
&\eqsim \rho_1 \circ \rho^{\mathsf{ctxt}}(\$) && (\mathsf{ae}\$) \\
&= [\rho^{\mathsf{ctxt}}(\$), [\![\mathbf{E}_{k_2}, \mathbf{D}_{k_2}]\!]] \\
&= \rho_2([\![\mathbf{E}_{k_2}, \mathbf{D}_{k_2}]\!]) \\
&\eqsim \rho_2 \circ \rho^{\mathsf{ctxt}}(\$) && (\mathsf{ae}\$) \\
&= [\rho^{\mathsf{ctxt}}(\$), \rho^{\mathsf{ctxt}}(\$)] \\
&\equiv \rho_3 \circ \rho^{\mathsf{ctxt}}(\$) \\
&\equiv \rho_3 \circ \rho^{\mathsf{ae}} \circ \rho^{\mathsf{enc}} \circ \rho^{\mathsf{ctxt}}(\$) \\
&\eqsim \rho_3 \circ \rho^{\mathsf{ae}} \circ \rho^{\mathsf{enc}}([\![\mathbf{E}_{k_1}, \mathbf{D}_{k_1}]\!]) && (\mathsf{ae}\$) \\
&= \rho_3 \circ \rho^{\mathsf{ae}}(\mathbf{E}_{k_1}) \\
&\equiv [\![\rho^{\mathsf{ae}}(\mathbf{E}_{k_1}), \rho^{\mathsf{ae}}(\mathbf{E}_{k_1})]\!]. && \square
\end{aligned}
$$

3.2.3 Anonymity Preservation of Encrypt-then-MAC

After having related the various game-based notions for pE and for pAE separately, we finally show how the anonymity enhanced security definitions for pE relate with those of pAE. For this, we need to introduce the concept of *message authentication code (MAC)* and its security and anonymity notions. We introduce a very specific syntax for *Message Authentication Codes (MAC)* which will turn out to be very useful in order to analyze the Encrypt-then-MAC paradigm. More precisely, we

consider MAC schemes which take as messages ciphertexts arising from some encryption scheme, and which provide an interface optimized for being coupled with such scheme. In this section we revisit the security and anonymity notions of MAC, the latter having being originally introduced in [AHM+14] (as a form of *key-indistinguishability*), and used in [AHM+15] to construct an authenticated and anonymous channel. Note that since we are interested in anonymity in this thesis, it is imperative that we only consider probabilistic MAC (pMAC), as pointed out in [AHM+14, AHM+15].

Definition 3.2.19 (MAC Scheme)**.** A *(probabilistic) message authentication code (MAC) scheme* $\Sigma \doteq (\mathtt{Gen}, \mathtt{Tag}, \mathtt{Vrf})$ over key-space $\mathcal{K}$, message-space $\mathcal{C}$, and tag-space $\mathcal{T}$ (with $\perp \notin \mathcal{K} \cup \mathcal{C} \cup \mathcal{T}$), is such that

- $\mathtt{Gen}$ is a distribution (often the uniform one) over $\mathcal{K}$;
- $\mathtt{Tag} : \mathcal{K} \times \mathcal{C} \to \mathcal{C} \times \mathcal{T}$ is a *probabilistic* function;
- $\mathtt{Vrf} : \mathcal{K} \times \mathcal{C} \times \mathcal{T} \to \mathcal{C} \cup \{\perp\}$ is a *deterministic* function.

As customary, for $k \in \mathcal{K}$ we use the short-hand notation $\mathtt{Tag}_k(\cdot)$ for $\mathtt{Tag}(k, \cdot)$ and $\mathtt{Vrf}_k(\cdot, \cdot)$ for $\mathtt{Vrf}(k, \cdot, \cdot)$. Moreover, we assume *correctness* of Σ, that is, for all keys k distributed according to $\mathtt{Gen}$, and all ciphertext-tag pairs $(c, \tau) \in \mathcal{C} \times \mathcal{T}$,

$$\mathtt{Vrf}_k(c, \tau) = \begin{cases} c & \text{if } (c, \tau) \in \operatorname{supp}(\mathtt{Tag}_k(c)), \\ \perp & \text{otherwise.} \end{cases}$$

As for pE and pAE, in order to define the security and anonymity of a fixed MAC scheme Σ, we need to define the following single and double interface systems (where the dependency on Σ is implicit), parameterized by some key $k \in \mathcal{K}$:

- $[\![\mathbf{T}_k, \mathbf{V}_k]\!]$:
  - On input a ciphertext $c \in \mathcal{C}$, return $\mathtt{Tag}_k(c) \in \mathcal{C} \times \mathcal{T}$.
  - On input a ciphertext-tag pair $(c, \tau) \in \mathcal{C} \times \mathcal{T}$, return $\mathtt{Vrf}_k(c, \tau) \in \mathcal{C} \cup \{\perp\}$.
- $\rho^{\mathsf{uf}}(\mathbf{X}) \equiv [\![\mathbf{X}', \mathbf{Y}']\!]$, for some correlated systems $\mathbf{X}'$ and $\mathbf{Y}'$ that behave as follows: Initially set $\mathcal{Q} \subseteq \mathcal{C} \times \mathcal{T}$ to $\varnothing$, and then:

- On input $c \in \mathcal{C}$ to $\mathbf{X}'$, forward c to $\mathbf{X}$, obtain $(c, \tau) \in \mathcal{C} \times \mathcal{T}$, set $\mathcal{Q}$ to $\mathcal{Q} \cup \{(c, \tau)\}$, and output (c, τ).
- On input $(c, \tau) \in \mathcal{C} \times \mathcal{T}$ to $\mathbf{Y}'$, if $(c, \tau) \in \mathcal{Q}$ then output c, otherwise output $\perp$.

For convenience we define $[\![\mathbf{T}_k, \mathbf{V}^{\perp}]\!] \doteq \rho^{\mathsf{uf}}(\mathbf{T}_k)$.

The classical security notion of MAC is *existential unforgeability under chosen messages attack*. This kind of game-based definition is often formulated as a game which an adversary is supposed to win. In this thesis we take the dual view that such a definition can be equivalently phrased as a distinguishing problem, hence a substitution (see for example [Mau02, MPR07, Ros21]).

Definition 3.2.20 (uf-cma)**.** $[\![\mathbf{T}_k, \mathbf{V}_k]\!] \eqsim \rho^{\mathsf{uf}}(\mathbf{T}_k)$, for $k \leftarrow \mathtt{Gen}$.

The concept of anonymous MAC schemes was crystallized by Alwen et al., which in [AHM+14] introduced the notion of key-indistinguishable pMAC. In the following definition, we introduce a new all-in-one definition for pMAC, which captures both unforgeability and anonymity.

Definition 3.2.21 (n-ik-uf-cma)**.**

$$[[\![\mathbf{T}_{k_1}, \mathbf{V}_{k_1}]\!], \ldots, [\![\mathbf{T}_{k_n}, \mathbf{V}_{k_n}]\!]] \eqsim [\![\underbrace{\rho^{\mathsf{uf}}(\mathbf{T}_{k_1}), \ldots, \rho^{\mathsf{uf}}(\mathbf{T}_{k_1})}_{n \text{ times}}]\!],$$

for independent $k_1, \ldots, k_n \leftarrow \mathtt{Gen}$.

Recall that Bellare and Namprempre [BN00] and Krawczyk [Kra01] have shown that the combination of a strongly unforgeable (uf-cma) MAC and a secure (ind-cpa) encryption scheme, performed according to the *Encrypt-then-MAC* (EtM) paradigm, yields an encryption scheme which is both secure (ind-cpa) and unforgeable (int-ctxt, the equivalent notion of uf-cma for encryption). Later, Shrimpton [Shr04] showed that a nice *all-in-one* security definition for secure authenticated encryption, ae, is equivalent to the combination ind-cpa and int-ctxt, thus attesting that EtM performed on a uf-cma-secure MAC scheme and an ind-cpa-secure encryption scheme, yields a ae-secure authenticated encryption scheme. Using our notation from Section 2.3.4 and above, the encryption scheme $\mathtt{EtM}(\Pi, \Sigma) \doteq (\widehat{\mathtt{Gen}}, \widehat{\mathtt{Tag}}, \widehat{\mathtt{Vrf}})$, resulting from this specific composition of an

encryption scheme $\Pi \doteq (\mathtt{Gen}_\Pi, \mathtt{Enc}, \mathtt{Dec})$ (with key-space $\mathcal{K}_\Pi$) and a MAC scheme $\Sigma \doteq (\mathtt{Gen}_\Sigma, \mathtt{Tag}, \mathtt{Vrf})$ (with key-space $\mathcal{K}_\Sigma$) is defined as follows:[3]

- $\widehat{\mathtt{Gen}}$ is the product distribution of $\mathtt{Gen}_\Pi$ and $\mathtt{Gen}_\Sigma$ over $\mathcal{K}_\Pi \times \mathcal{K}_\Sigma$;
- $\widehat{\mathtt{Enc}}_{k^{\mathsf{e}},k^{\mathsf{a}}} \doteq \mathtt{Tag}_{k^{\mathsf{a}}} \circ \mathtt{Enc}_{k^{\mathsf{e}}}$;
- $\widehat{\mathtt{Vrf}}_{k^{\mathsf{e}},k^{\mathsf{a}}} \doteq \mathtt{Dec}_{k^{\mathsf{e}}} \circ \mathtt{Vrf}_{k^{\mathsf{a}}}$.

Note that in order for correctness to hold, we further need to assume that $\perp \in \mathcal{M}$, and that $\mathtt{Enc}_k(\perp) = \perp$ for any $k \in \mathcal{K}_\Pi$.

If we now want to define security of the composed scheme $\widehat{\Pi} \doteq \mathtt{EtM}(\Pi, \Sigma)$, we need to introduce a simple operator between (single-interface) systems, namely *cascading*: Informally, given systems $\mathbf{X}$ and $\mathbf{Y}$, we define the new system $\mathbf{X} \triangleright \mathbf{Y}$ as the system[4] that on input x computes $y \doteq \mathbf{X}(x)$, and returns $z \doteq \mathbf{Y}(y)$ (where we are assuming matching domains). As we did for Π, we can define systems $\mathbf{T}_k$ and $\mathbf{V}_k$ relative to Σ. Then $\widehat{\mathtt{Enc}}_{k^{\mathsf{e}},k^{\mathsf{a}}}$ is modeled by $\widehat{\mathbf{E}}_{k^{\mathsf{e}},k^{\mathsf{a}}} \doteq \mathbf{E}_{k^{\mathsf{e}}} \triangleright \mathbf{T}_{k^{\mathsf{a}}}$, and $\widehat{\mathtt{Dec}}_{k^{\mathsf{e}},k^{\mathsf{a}}}$ by $\widehat{\mathbf{D}}_{k^{\mathsf{e}},k^{\mathsf{a}}} \doteq \mathbf{V}_{k^{\mathsf{a}}} \triangleright \mathbf{D}_{k^{\mathsf{e}}}$. Recalling the security definitions from Section 2.3.4 and above, the statement that $\widehat{\Pi}$ is secure follows.

Theorem 3.2.22. $(\mathsf{ind\text{-}cpa}(\Pi), \mathsf{uf\text{-}cma}(\Sigma)) \xrightarrow{1,1} \mathsf{ae}(\mathtt{EtM}(\Pi, \Sigma))$.

Proof. Let $k^{\mathsf{e}} \leftarrow \mathtt{Gen}_\Pi$, $k^{\mathsf{a}} \leftarrow \mathtt{Gen}_\Sigma$, and consider

- $\rho_1(\llbracket \mathbf{X}, \mathbf{Y} \rrbracket) \doteq \llbracket \mathbf{E}_{k^{\mathsf{e}}} \triangleright \mathbf{X}, \mathbf{Y} \triangleright \mathbf{D}_{k^{\mathsf{e}}} \rrbracket$ and
- $\rho_2(\mathbf{X}) \doteq \rho^{\mathsf{ctxt}}(\mathbf{X} \triangleright \mathbf{T}_{k^{\mathsf{a}}})$.

[3] Recall that the symbol $\circ$ in this context represents *function composition*.
[4] This operator is also formally defined later in Definition 5.2.2.

Then:

$$\begin{aligned}
[\![\widehat{\mathbf{E}}_{k^{\mathsf{e}},k^{\mathsf{a}}}, \widehat{\mathbf{D}}_{k^{\mathsf{e}},k^{\mathsf{a}}}]\!] &= [\![\mathbf{E}_{k^{\mathsf{e}}} \triangleright \mathbf{T}_{k^{\mathsf{a}}}, \mathbf{V}_{k^{\mathsf{a}}} \triangleright \mathbf{D}_{k^{\mathsf{e}}}]\!] \\
&= \rho_1([\![\mathbf{T}_{k^{\mathsf{a}}}, \mathbf{V}_{k^{\mathsf{a}}}]\!]) \\
&\eqsim \rho_1([\![\mathbf{T}_{k^{\mathsf{a}}}, \mathbf{V}^{\perp}]\!]) && (\mathsf{uf\text{-}cma}) \\
&= [\![\mathbf{E}_{k^{\mathsf{e}}} \triangleright \mathbf{T}_{k^{\mathsf{a}}}, \mathbf{V}^{\perp} \triangleright \mathbf{D}_{k^{\mathsf{e}}}]\!] \\
&\equiv \rho^{\mathsf{ctxt}}(\mathbf{E}_{k^{\mathsf{e}}} \triangleright \mathbf{T}_{k^{\mathsf{a}}}) \\
&= \rho_2(\mathbf{E}_{k^{\mathsf{e}}}) \\
&\eqsim \rho_2 \circ \rho^{\mathsf{cpa}}(\mathbf{E}_{k^{\mathsf{e}}}) && (\mathsf{ind\text{-}cpa}) \\
&= \rho^{\mathsf{ctxt}}(\rho^{\mathsf{cpa}}(\mathbf{E}_{k^{\mathsf{e}}}) \triangleright \mathbf{T}_{k^{\mathsf{a}}}) \\
&\equiv \rho^{\mathsf{ctxt}} \circ \rho^{\mathsf{cpa}}(\mathbf{E}_{k^{\mathsf{e}}} \triangleright \mathbf{T}_{k^{\mathsf{a}}}) \\
&= \rho^{\mathsf{ae}}(\widehat{\mathbf{E}}_{k^{\mathsf{e}},k^{\mathsf{a}}}). && \square
\end{aligned}$$

We finally show the important fact that EtM is *anonymity-preserving*, in the sense that if an encryption scheme Π is both $\mathsf{ind\text{-}cpa}$-secure and $\mathsf{ik\text{-}cpa}$-secure (that is, $\mathsf{ik\text{-}ind\text{-}cpa}$-secure) and a MAC scheme Σ is both $\mathsf{uf\text{-}cma}$-secure and $\mathsf{ik\text{-}cma}$-secure (that is, $\mathsf{ik\text{-}uf\text{-}cma}$-secure), then $\mathtt{EtM}(\Pi, \Sigma)$ not only is ae-secure, but also $\mathsf{ik\text{-}cca}$-secure (that is, $\mathsf{ik\text{-}ae}$-secure). This is captured formally by the following statement, shown for 2 users for cleaner presentation, but easily generalized to n users.

Theorem 3.2.23.

$$(2\text{-}\mathsf{ik\text{-}ind\text{-}cpa}(\Pi), 2\text{-}\mathsf{ik\text{-}uf\text{-}cma}(\Sigma)) \xrightarrow{1,1} 2\text{-}\mathsf{ik\text{-}ae}(\mathtt{EtM}(\Pi, \Sigma)).$$

Proof. Let $k_1^{\mathsf{e}}, k_2^{\mathsf{e}} \leftarrow \mathtt{Gen}_{\Pi}$, $k_1^{\mathsf{a}}, k_2^{\mathsf{a}} \leftarrow \mathtt{Gen}_{\Sigma}$, and consider

- $\rho_1([\![[\![\mathbf{X}_1, \mathbf{Y}_1]\!], [\![\mathbf{X}_2, \mathbf{Y}_2]\!]]\!]) \doteq [[\![\mathbf{E}_{k_1^{\mathsf{e}}} \triangleright \mathbf{X}_1, \mathbf{Y}_1 \triangleright \mathbf{D}_{k_1^{\mathsf{e}}}]\!], [\![\mathbf{E}_{k_2^{\mathsf{e}}} \triangleright \mathbf{X}_2, \mathbf{Y}_2 \triangleright \mathbf{D}_{k_2^{\mathsf{e}}}]\!]]$ and

- $\rho_2([\![\mathbf{X}, \mathbf{Y}]\!]) \doteq [\![\rho^{\mathsf{ctxt}}(\mathbf{X} \triangleright \mathbf{T}_{k_1^{\mathsf{a}}}), \rho^{\mathsf{ctxt}}(\mathbf{Y} \triangleright \mathbf{T}_{k_1^{\mathsf{a}}})]\!]$.

Then:

$$
\begin{aligned}
&[[\![\widehat{\mathbf{E}}_{k_1^{\mathsf{e}},k_1^{\mathsf{a}}}, \widehat{\mathbf{D}}_{k_1^{\mathsf{e}},k_1^{\mathsf{a}}}]\!], [\![\widehat{\mathbf{E}}_{k_2^{\mathsf{e}},k_2^{\mathsf{a}}}, \widehat{\mathbf{D}}_{k_2^{\mathsf{e}},k_2^{\mathsf{a}}}]\!]] \\
&\quad = [[\![\mathbf{E}_{k_1^{\mathsf{e}}} \triangleright \mathbf{T}_{k_1^{\mathsf{a}}}, \mathbf{V}_{k_1^{\mathsf{a}}} \triangleright \mathbf{D}_{k_1^{\mathsf{e}}}]\!], [\![\mathbf{E}_{k_2^{\mathsf{e}}} \triangleright \mathbf{T}_{k_2^{\mathsf{a}}}, \mathbf{V}_{k_2^{\mathsf{a}}} \triangleright \mathbf{D}_{k_2^{\mathsf{e}}}]\!]] \\
&\quad = \rho_1([[\![\mathbf{T}_{k_1^{\mathsf{a}}}, \mathbf{V}_{k_1^{\mathsf{a}}}]\!], [\![\mathbf{T}_{k_2^{\mathsf{a}}}, \mathbf{V}_{k_2^{\mathsf{a}}}]\!]]) \\
&\quad \eqsim \rho_1([[\![\mathbf{T}_{k_1^{\mathsf{a}}}, \mathbf{V}^{\perp}]\!], [\![\mathbf{T}_{k_1^{\mathsf{a}}}, \mathbf{V}^{\perp}]\!]]) \qquad \text{(2-ik-uf-cma)} \\
&\quad = [[\![\mathbf{E}_{k_1^{\mathsf{e}}} \triangleright \mathbf{T}_{k_1^{\mathsf{a}}}, \mathbf{V}^{\perp} \triangleright \mathbf{D}_{k_1^{\mathsf{e}}}]\!], [\![\mathbf{E}_{k_2^{\mathsf{e}}} \triangleright \mathbf{T}_{k_1^{\mathsf{a}}}, \mathbf{V}^{\perp} \triangleright \mathbf{D}_{k_2^{\mathsf{e}}}]\!]] \\
&\quad \equiv [\![\rho^{\mathsf{ctxt}}(\mathbf{E}_{k_1^{\mathsf{e}}} \triangleright \mathbf{T}_{k_1^{\mathsf{a}}}), \rho^{\mathsf{ctxt}}(\mathbf{E}_{k_2^{\mathsf{e}}} \triangleright \mathbf{T}_{k_1^{\mathsf{a}}})]\!] \\
&\quad = \rho_2([\mathbf{E}_{k_1^{\mathsf{e}}}, \mathbf{E}_{k_2^{\mathsf{e}}}]) \\
&\quad \eqsim \rho_2([\![\rho^{\mathsf{cpa}}(\mathbf{E}_{k_1^{\mathsf{e}}}), \rho^{\mathsf{cpa}}(\mathbf{E}_{k_1^{\mathsf{e}}})]\!]) \qquad \text{(2-ik-ind-cpa)} \\
&\quad = [\![\rho^{\mathsf{ctxt}}(\rho^{\mathsf{cpa}}(\mathbf{E}_{k_1^{\mathsf{e}}}) \triangleright \mathbf{T}_{k_1^{\mathsf{a}}}), \rho^{\mathsf{ctxt}}(\rho^{\mathsf{cpa}}(\mathbf{E}_{k_1^{\mathsf{e}}}) \triangleright \mathbf{T}_{k_1^{\mathsf{a}}})]\!] \\
&\quad \equiv [\![\rho^{\mathsf{ctxt}} \circ \rho^{\mathsf{cpa}}(\mathbf{E}_{k_1^{\mathsf{e}}} \triangleright \mathbf{T}_{k_1^{\mathsf{a}}}), \rho^{\mathsf{ctxt}} \circ \rho^{\mathsf{cpa}}(\mathbf{E}_{k_1^{\mathsf{e}}} \triangleright \mathbf{T}_{k_1^{\mathsf{a}}})]\!] \\
&\quad = [\![\rho^{\mathsf{ae}}(\widehat{\mathbf{E}}_{k_1^{\mathsf{e}},k_1^{\mathsf{a}}}), \rho^{\mathsf{ae}}(\widehat{\mathbf{E}}_{k_1^{\mathsf{e}},k_1^{\mathsf{a}}})]\!]. \qquad \square
\end{aligned}
$$

We will confirm Theorem 3.2.23 with a composable approach in the next section.

3.3 Composable Security of pE and pAE

In this section we turn our attention to *composable security*, as opposed to game-based security. For this, we make use of the *constructive cryptography* (CC) framework by Maurer and Renner [MR11, Mau12] as introduced in Section 2.4.

3.3.1 Anonymous Channels

There are four n-resources that we consider in this chapter. The first, $\mathsf{KEY}^{\mathcal{K}}_{n\leftrightarrow 1}$, models the initial symmetric-key setup: it generates n independent keys $k_1, \ldots, k_n \in \mathcal{K}$ according to an implicitly defined distribution $\mathtt{Gen}$ over $\mathcal{K}$, and for $i \in [n]$ it outputs k_i at interface S_i; at interface R it outputs the list $(k_1, \ldots, k_n)$ of all generated keys, while it outputs nothing at interface E. The remaining three n-resources model the anonymous channels for n senders and one receiver mentioned above (for messages over some set $\mathcal{X}$), where we assume a central adversary that is in full control

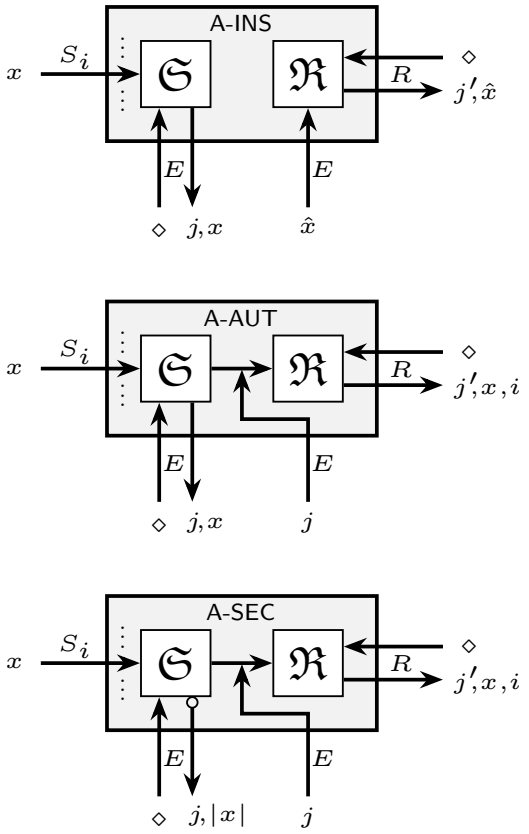


Figure 3.2: Sketches of the anonymous channel resources.

$\mathsf{A\text{-}INS}^{\mathcal{X}}_{n\to 1}$

$\mathfrak{S}, \mathfrak{R} \subseteq \mathbb{N} \times \mathcal{X}$
$c_S, c_R, t_S, t_R \in \mathbb{N}$
Initialize:
  $\mathfrak{S}, \mathfrak{R} \leftarrow \varnothing$
  $c_S, c_R \leftarrow 1$
  $t_S, t_R \leftarrow 0$
Interface $S_i(x \in \mathcal{X})$: // $i \in [n]$
  $t_S \leftarrow t_S + 1$
  $\mathfrak{S} \leftarrow \mathfrak{S} \cup \{(t_S, x)\}$
Interface $E(\diamond)$:
  $\mathfrak{O} \leftarrow \{(j, x) \in \mathfrak{S} \mid c_S \leq j \leq t_S\}$
  $c_S \leftarrow t_S + 1$
  return $\mathfrak{O}$
Interface $E(x \in \mathcal{X})$:
  $t_R \leftarrow t_R + 1$
  $\mathfrak{R} \leftarrow \mathfrak{R} \cup \{(t_R, x)\}$
Interface $R(\diamond)$:
  $\mathfrak{O} \leftarrow \{(j, x) \in \mathfrak{R} \mid c_R \leq j \leq t_R\}$
  $c_R \leftarrow t_R + 1$
  return $\mathfrak{O}$

Figure 3.3: Formal description of the *insecure anonymous channel* $\mathsf{A\text{-}INS}^{\mathcal{X}}_{n\to 1}$.

$\mathsf{A\text{-}AUT}^{\mathcal{X}}_{n\to 1}$

$\mathfrak{S}, \mathfrak{R} \subseteq (\mathbb{N} \times \mathcal{X} \times \mathbb{N}) \cup (\mathbb{N} \times \{\bot\}^2)$
$c_S, c_R, t_S, t_R \in \mathbb{N}$
Initialize:
  $\mathfrak{S}, \mathfrak{R} \leftarrow \varnothing$
  $c_S, c_R \leftarrow 1$
  $t_S, t_R \leftarrow 0$
Interface $S_i(x \in \mathcal{X})$: // $i \in [n]$
  $t_S \leftarrow t_S + 1$
  $\mathfrak{S} \leftarrow \mathfrak{S} \cup \{(t_S, x, i)\}$
Interface $E(\diamond)$:
  $\mathfrak{O} \leftarrow \{(j, x) \in \mathbb{N} \times \mathcal{X} \mid \exists i \in [n] \colon (j, x, i) \in \mathfrak{S}, c_S \le j \le t_S\}$
  $c_S \leftarrow t_S + 1$
  return $\mathfrak{O}$
Interface $E(j \in \mathbb{N} \cup \{-1\})$:
  if $\exists x \in \mathcal{X}, i \in [n] \colon (j, x, i) \in \mathfrak{S}$ **then**
    $t_R \leftarrow t_R + 1$
    $\mathfrak{R} \leftarrow \mathfrak{R} \cup \{(t_R, x, i)\}$
  else if $j = -1$ **then**
    $t_R \leftarrow t_R + 1$
    $\mathfrak{R} \leftarrow \mathfrak{R} \cup \{(t_R, \bot, \bot)\}$
Interface $R(\diamond)$:
  $\mathfrak{O} \leftarrow \{(j, x, i) \in \mathfrak{R} \mid c_R \le j \le t_R\}$
  $c_R \leftarrow t_R + 1$
  return $\mathfrak{O}$

Figure 3.4: Formal description of the *authenticated anonymous channels* $\mathsf{A\text{-}AUT}^{\mathcal{X}}_{n\to 1}$, with the differences from $\mathsf{A\text{-}INS}^{\mathcal{X}}_{n\to 1}$ highlighted in dark gray.

$\mathsf{A\text{-}SEC}^{\mathcal{X}}_{n\to 1}$

$\mathfrak{S}, \mathfrak{R} \subseteq (\mathbb{N} \times \mathcal{X} \times \mathbb{N}) \cup (\mathbb{N} \times \{\bot\}^2)$
$c_S, c_R, t_S, t_R \in \mathbb{N}$
Initialize:
  $\mathfrak{S}, \mathfrak{R} \leftarrow \varnothing$
  $c_S, c_R \leftarrow 1$
  $t_S, t_R \leftarrow 0$
Interface $S_i(x \in \mathcal{X})$: // $i \in [n]$
  $t_S \leftarrow t_S + 1$
  $\mathfrak{S} \leftarrow \mathfrak{S} \cup \{(t_S, x, i)\}$
Interface $E(\diamond)$:
  $\mathfrak{O} \leftarrow \{(j, |x|) \in \mathbb{N} \times \mathbb{N} \mid \exists i \in [n] \colon (j, x, i) \in \mathfrak{S},\ c_S \le j \le t_S\}$
  $c_S \leftarrow t_S + 1$
  return $\mathfrak{O}$
Interface $E(j \in \mathbb{N} \cup \{-1\})$:
  if $\exists x \in \mathcal{X}, i \in [n] \colon (j, x, i) \in \mathfrak{S}$ **then**
    $t_R \leftarrow t_R + 1$
    $\mathfrak{R} \leftarrow \mathfrak{R} \cup \{(t_R, x, i)\}$
  else if $j = -1$ **then**
    $t_R \leftarrow t_R + 1$
    $\mathfrak{R} \leftarrow \mathfrak{R} \cup \{(t_R, \bot, \bot)\}$
Interface $R(\diamond)$:
  $\mathfrak{O} \leftarrow \{(j, x, i) \in \mathfrak{R} \mid c_R \le j \le t_R\}$
  $c_R \leftarrow t_R + 1$
  return $\mathfrak{O}$

Figure 3.5: Formal description of the *secure anonymous channels* $\mathsf{A\text{-}SEC}^{\mathcal{X}}_{n\to 1}$, with the differences from $\mathsf{A\text{-}AUT}^{\mathcal{X}}_{n\to 1}$ highlighted in dark gray.

of the physical communication between the senders and the receiver, that is, an adversary that can *delete*, *repeat*, and *reorder* messages.[5] $\mathsf{A\text{-}INS}^{\mathcal{X}}_{n\to 1}$ models the channel which leaks every message input by any sender (but not their identities) directly to the adversary. Note that in particular this means that the receiver does not directly receive the messages sent by the senders. Moreover, $\mathsf{A\text{-}INS}^{\mathcal{X}}_{n\to 1}$ allows the adversary to inject any message to the receiver (thus, in particular, also the ones originally sent by the senders). Note that this channel, while providing anonymity, is per se pretty useless, since the receiver has also no information about the identity of the sender of any message. Instead, $\mathsf{A\text{-}AUT}^{\mathcal{X}}_{n\to 1}$, while still leaking all the messages sent by the senders directly to the adversary, does not allow the latter to inject any message; instead, the adversary can now *select* messages that it wants to be forwarded to the receiver. Moreover, the forwarded messages also carry the identity of the original sender, still hidden to the adversary. Finally, $\mathsf{A\text{-}SEC}^{\mathcal{X}}_{n\to 1}$ essentially works as $\mathsf{A\text{-}AUT}^{\mathcal{X}}_{n\to 1}$, except that now only the *lengths* of the messages sent by the senders are leaked directly to the adversary. We sketch the three anonymous channels in Figure 3.2 and provide a formal description of the behavior of the systems implementing such n-resources in Figures 3.3 to 3.5.

3.3.2 Overview of the Results

In [AHM+15] it was already shown[6] that n-ik-uf-cma-secure (as defined in Section 3.2.3) pMAC constructs $\mathsf{A\text{-}AUT}^{\mathcal{M}}_{n\to 1}$ from $\mathsf{A\text{-}INS}^{\mathcal{M}\times\mathcal{T}}_{n\to 1}$ and $\mathsf{KEY}^{\mathcal{K}}_{n\leftrightarrow 1}$; within our model, this result is captured by the following statement:

$$[\mathsf{KEY}^{\mathcal{K}}_{n\leftrightarrow 1}, \mathsf{A\text{-}INS}^{\mathcal{M}\times\mathcal{T}}_{n\to 1}] \xrightarrow{\boldsymbol{\pi}_{\mathsf{pMAC}};\, n\text{-ik-uf-cma}} \mathsf{A\text{-}AUT}^{\mathcal{M}}_{n\to 1},$$

(for appropriate n-protocol $\boldsymbol{\pi}_{\mathsf{pMAC}}$ implementing pMAC). Here we instead focus on the following further constructions:

[5] Note that while deletion is a physical phenomenon, and can thus not be prevented using cryptography, it is in principle possible to prevent repetition and reordering, concretely by means of *sequence numbers*. But we do not cover this aspect of security in this thesis.

[6] For a slightly different modeling of the game-based notions and anonymous channel resources.

- n-ik-ind-cpa-secure pE constructs $\mathsf{A\text{-}SEC}^{\mathcal{M}}_{n\to 1}$ from $\mathsf{A\text{-}AUT}^{\mathcal{C}}_{n\to 1}$ and $\mathsf{KEY}^{\mathcal{K}}_{n\leftrightarrow 1}$ (cf. Theorem 3.3.1):

$$[\mathsf{KEY}^{\mathcal{K}}_{n\leftrightarrow 1}, \mathsf{A\text{-}AUT}^{\mathcal{C}}_{n\to 1}] \xrightarrow{\boldsymbol{\pi}_{\mathsf{pE}};\, n\text{-ik-ind-cpa}} \mathsf{A\text{-}SEC}^{\mathcal{M}}_{n\to 1},$$

  (for appropriate n-protocol $\boldsymbol{\pi}_{\mathsf{pE}}$).

- ik-ae-secure pAE constructs $\mathsf{A\text{-}SEC}^{\mathcal{M}}_{n\to 1}$ from $\mathsf{A\text{-}INS}^{\mathcal{C}}_{n\to 1}$ and $\mathsf{KEY}^{\mathcal{K}}_{n\leftrightarrow 1}$ (cf. Theorem 3.3.2):

$$[\mathsf{KEY}^{\mathcal{K}}_{n\leftrightarrow 1}, \mathsf{A\text{-}INS}^{\mathcal{C}}_{n\to 1}] \xrightarrow{\boldsymbol{\pi}_{\mathsf{pAE}};\, n\text{-ik-ae}} \mathsf{A\text{-}SEC}^{\mathcal{M}}_{n\to 1},$$

  (for appropriate n-protocol $\boldsymbol{\pi}_{\mathsf{pAE}}$).

Note that by the composition theorem (Theorem 2.4.4), the first two statements imply the third for the (composed) protocol $\hat{\boldsymbol{\pi}}_{\mathsf{pAE}} = \boldsymbol{\pi}_{\mathsf{pE}}\, \boldsymbol{\pi}_{\mathsf{pMAC}}$, namely

$$[\mathsf{KEY}^{\mathcal{K}}_{n\leftrightarrow 1}, \mathsf{KEY}^{\mathcal{K}}_{n\leftrightarrow 1}, \mathsf{A\text{-}INS}^{\mathcal{C}}_{n\to 1}] \xrightarrow{\hat{\boldsymbol{\pi}}_{\mathsf{pAE}};\, n\text{-ik-uf-cma}, n\text{-ik-ind-cpa}} \mathsf{A\text{-}SEC}^{\mathcal{M}}_{n\to 1}.$$

In particular, note that this corresponds to the EtM paradigm, and therefore is a (composable) confirmation of Theorem 3.2.23.

3.3.3 Composable Anonymous Security of pE

In this section we first introduce a composable definition of anonymous security for pE, and then we show that the previously introduced game-based notion of ik-ind-cpa-security implies the former. The composable definition can be interpreted as providing *composable semantics* to ik-ind-cpa-security for pE, in the sense that the result we show here attests that if an encryption scheme is ik-ind-cpa-secure, then it can be safely used to construct a secure channel from an authenticated one, *while preserving anonymity*.

In the following, for a fixed encryption scheme Π let the converter enc (where the dependency on Π is implicit) behave as follows when connected to interface S_i of $\mathsf{KEY}^{\mathcal{K}}_{n\leftrightarrow 1}$ and interface S_i of $\mathsf{A\text{-}AUT}^{\mathcal{C}}_{n\to 1}$, for $i \in [n]$: on input a message $m \in \mathcal{M}$ from the outside, if not already done so before, output $\diamond$ to $\mathsf{KEY}^{\mathcal{K}}_{n\leftrightarrow 1}$ in order to fetch key k_i, then compute

$c \leftarrow \mathtt{Enc}_{k_i}(m) \in \mathcal{C}$ and output c to $\mathsf{A\text{-}AUT}^{\mathcal{C}}_{n\to 1}$. Also let the converter dec (where again the dependency on Π is implicit) behave as follows when connected to interface R of $\mathsf{KEY}^{\mathcal{K}}_{n\leftrightarrow 1}$ and interface R of $\mathsf{A\text{-}AUT}^{\mathcal{C}}_{n\to 1}$: on input $\diamond$ from the outside, if not already done so before, output $\diamond$ to $\mathsf{KEY}^{\mathcal{K}}_{n\leftrightarrow 1}$ in order to fetch keys $k_1, \ldots, k_n$, and then output $\diamond$ to $\mathsf{A\text{-}AUT}^{\mathcal{C}}_{n\to 1}$; for each obtained tuple (j, c, i), compute $m \leftarrow \mathtt{Dec}_{k_i}(c)$, and output the collection of all such resulting tuples (j, m, i) to the outside. Finally, we define the n-protocol $\boldsymbol{\pi}_{\mathsf{pE}} \doteq (\mathsf{enc}, \ldots, \mathsf{enc}, \mathsf{dec})$.

Theorem 3.3.1. $[\mathsf{KEY}^{\mathcal{K}}_{n\leftrightarrow 1}, \mathsf{A\text{-}AUT}^{\mathcal{C}}_{n\to 1}] \overset{\boldsymbol{\pi}_{\mathsf{pE}};\, n\text{-}\mathsf{ik\text{-}ind\text{-}cpa}}{\Longrightarrow} \mathsf{A\text{-}SEC}^{\mathcal{M}}_{n\to 1}$.

Proof. Define[7] transformation ρ as in Figure 3.6, system $\mathbf{H}_0$ as in Figure 3.7, and simulator $\boldsymbol{\sigma}$ attached to interface E of $\mathsf{A\text{-}SEC}^{\mathcal{M}}_{n\to 1}$ that behaves as follows: Initially, sample a key k_1 according to $\mathtt{Gen}$. Then:

- On input $\diamond$ from the outside, output $\diamond$ on the inside, obtain a set $\mathfrak{O} \subseteq \mathbb{N} \times \mathbb{N}$, and initialize another set $\mathfrak{O}' \subseteq \mathbb{N} \times \mathcal{M}$ to $\varnothing$; Then for each $(j, \ell) \in \mathfrak{O}$, add $(j, \mathtt{Enc}_{k_1}(\tilde{m}))$ to $\mathfrak{O}'$, for freshly and uniformly sampled $\tilde{m} \in \mathcal{M}$ with $|\tilde{m}| = |m|$. Finally, output $\mathfrak{O}'$.
- On input $j \in \mathbb{N}$ from the outside, simply forward j to the inside.

Let $k_1, \ldots, k_n \leftarrow \mathtt{Gen}$. Then,

$$\begin{aligned}
\boldsymbol{\pi}_{\mathsf{pE}}\,[\mathsf{KEY}^{\mathcal{K}}_{n\leftrightarrow 1}, \mathsf{A\text{-}AUT}^{\mathcal{C}}_{n\to 1}] &\equiv \mathbf{H}_0 && \text{(monolithic representation)}\\
&\equiv \rho([\mathbf{E}_{k_1}, \ldots, \mathbf{E}_{k_n}]) && \text{(correctness)}\\
&\eqsim \rho([\![\rho^{\mathsf{cpa}}(\mathbf{E}_{k_1}), \ldots, \rho^{\mathsf{cpa}}(\mathbf{E}_{k_1})]\!]) && (n\text{-}\mathsf{ik\text{-}ind\text{-}cpa})\\
&\equiv \boldsymbol{\sigma}\,\mathsf{A\text{-}SEC}^{\mathcal{M}}_{n\to 1}. && \text{(monolithic representation)}
\end{aligned}$$

□

Note that by combining Theorem 3.3.1 with Theorem 3.2.17, we also have

$$[\mathsf{KEY}^{\mathcal{K}}_{n\leftrightarrow 1}, \mathsf{A\text{-}AUT}^{\mathcal{C}}_{n\to 1}] \overset{\boldsymbol{\pi}_{\mathsf{pE}};\, \mathsf{ind\$\text{-}cpa}}{\Longrightarrow} \mathsf{A\text{-}SEC}^{\mathcal{M}}_{n\to 1}.$$

[7] For simplicity, here we consider the slightly different channel resources which on input -1 at interface E do nothing (instead of adding the tuple $(k, \bot, \bot)$, for some $k \in \mathbb{N}$, to the set $\mathfrak{R}$), since they would behave identically also otherwise.

$\rho([\![\mathbf{X}_1, \ldots, \mathbf{X}_n]\!])$

$\mathfrak{S}, \mathfrak{R} \subseteq \mathbb{N} \times \mathcal{M} \times \mathbb{N}$
$c_S, c_R, t_S, t_R \in \mathbb{N}$
Initialize:
  $\mathfrak{S}, \mathfrak{R} \leftarrow \varnothing$
  $c_S, c_R \leftarrow 1$
  $t_S, t_R \leftarrow 0$
Interface $S_i(m)$: // $i \in [n]$
  $t_S \leftarrow t_S + 1$
  $\mathfrak{S} \leftarrow \mathfrak{S} \cup \{(t_S, m, i)\}$
Interface $E(\diamond)$:
  $\mathfrak{O} \leftarrow \{(j, \mathbf{X}_i(m)) \in \mathbb{N} \times \mathcal{C} \mid (j, m, i) \in \mathfrak{S}, c_S \leq j \leq t_S\}$
  $c_S \leftarrow t_S + 1$
  return $\mathfrak{O}$
Interface $E(j)$:
  if $\exists m \in \mathcal{M}, i \in [n] : (j, m, i) \in \mathfrak{S}$ **then**
    $t_R \leftarrow t_R + 1$
    $\mathfrak{R} \leftarrow \mathfrak{R} \cup \{(t_R, m, i)\}$
Interface $R(\diamond)$:
  $\mathfrak{O} \leftarrow \{(j, m, i) \in \mathfrak{R} \mid c_R \leq j \leq t_R\}$
  $c_R \leftarrow t_R + 1$
  return $\mathfrak{O}$

Figure 3.6: Transformation ρ for Theorem 3.3.1.

$\mathbf{H}_0$

$\mathfrak{S}, \mathfrak{R} \subseteq \mathbb{N} \times \mathcal{C} \times \mathbb{N}$
$c_S, c_R, t_S, t_R \in \mathbb{N}$
$k_1, \ldots, k_n \in \mathcal{K}$
Initialize:
  $\mathfrak{S}, \mathfrak{R} \leftarrow \varnothing$
  $c_S, c_R \leftarrow 1$
  $t_S, t_R \leftarrow 0$
  $k_1, \ldots, k_n \leftarrow \mathtt{Gen}$
Interface $S_i(m)$: // $i \in [n]$
  $t_S \leftarrow t_S + 1$
  $\mathfrak{S} \leftarrow \mathfrak{S} \cup \{(t_S, \mathtt{Enc}_{k_i}(m), i)\}$
Interface $E(\diamond)$:
  $\mathfrak{O} \leftarrow \{(j, c) \in \mathbb{N} \times \mathcal{C} \mid \exists i \in [n] : (j, c, i) \in \mathfrak{S}, c_S \leq j \leq t_S\}$
  $c_S \leftarrow t_S + 1$
  return $\mathfrak{O}$
Interface $E(j)$:
  if $\exists c \in \mathcal{C}, i \in [n] : (j, c, i) \in \mathfrak{S}$ **then**
    $t_R \leftarrow t_R + 1$
    $\mathfrak{R} \leftarrow \mathfrak{R} \cup \{(t_R, c, i)\}$
Interface $R(\diamond)$:
  $\mathfrak{O} \leftarrow \{(j, \mathtt{Dec}_{k_i}(c), i) \in \mathbb{N} \times \mathcal{M} \times [n] \mid (j, c, i) \in \mathfrak{R}, c_R \leq j \leq t_R\}$
  $c_R \leftarrow t_R + 1$
  return $\mathfrak{O}$

Figure 3.7: Hybrid system $\mathbf{H}_0$ for Theorem 3.3.1.

Comparison With Alwen et al. Note that in [AHM+15] this construction step was already presented, but for a much less efficient (but statistically secure) protocol: the idea is to double the number of sender interfaces (two interfaces per user), and transmit messages bit-by-bit. More concretely, assuming $\mathcal{M} = \{0,1\}^\ell$, for some $\ell \in \mathbb{N}$, this protocol constructs $\mathsf{A\text{-}SEC}^{\mathcal{M}}_{n\to 1}$ from $\mathsf{A\text{-}AUT}^{\mathcal{R}\times[\ell]}_{2n\to 1}$ (and, crucially, *no* $\mathsf{KEY}^{\mathcal{K}}_{n\leftrightarrow 1}$ resource). It works by assigning to each outside interface S_i, for $i \in [n]$, two interfaces $S_{i,b}$ of $\mathsf{A\text{-}AUT}^{\mathcal{R}\times[\ell]}_{2n\to 1}$, with $b \in \{0,1\}$, and transmits each message $m = (m_1, \ldots, m_\ell) \in \mathcal{M}$ as follows: First, sample some fresh uniform randomness $r \in \mathcal{R}$, for some randomness space $\mathcal{R}$, and then, for each $j \in [\ell]$, input (r, j) at interface S_{i,m_j} of $\mathsf{A\text{-}AUT}^{\mathcal{R}\times[\ell]}_{2n\to 1}$. Then at the receiver interface R, each message is reconstructed in the obvious way: upon obtaining *all* of the ℓ triplets $(\cdot, (r, j), (i, m_j))$, output the triplet $(\cdot, (m_1, \ldots, m_\ell), i)$ (where we are ignoring the counters, i.e., the first arguments of the triplets). This protocol is intuitively secure because for the adversary sitting at interface E, its view is independent of each message m, and moreover it can only provoke the protocol to output an invalid message at R if one of the senders reuses the same randomness value r for two different messages, which can be avoided by introducing *state* by the senders. Otherwise, assuming uniform distribution over $\mathcal{R}$, this anyway happens with very small probability, that is, by a standard approximation for the birthday paradox bound, at most $q^2/|\mathcal{R}|$, where q is the total of transmitted messages.

The above protocol is nevertheless clearly inefficient: Considering the construction of $\mathsf{A\text{-}AUT}^{\mathcal{C}}_{n\to 1}$ using a MAC scheme, for each message of size ℓ, the underlying MAC must be invoked ℓ times. Here we propose a much more efficient construction by employing symmetric-key encryption, only at the cost of doubling the size of the shared secret keys. The new protocol is more efficient because now for every message only a single invocation of both the MAC and the encryption scheme are required, independently of its size.

3.3.4 Composable Anonymous Security of pAE

In this section we first introduce a composable definition of anonymous security for pAE, and then we show that the previously introduced game-based notion of ik-ae-security implies the former. The composable defini-

tion can be interpreted as providing *composable semantics* to ik-ae-security for pAE, in the sense that the result we show here attests that if an (authenticated) encryption scheme is ik-ae-secure, then it can be safely used to construct a secure channel from an insecure one, *while preserving anonymity*.

In the following, for a fixed (authenticated) encryption scheme Π let the converter aenc (where the dependency on Π is implicit) behave as follows when connected to interface S_i of $\mathsf{KEY}^{\mathcal{K}}_{n\leftrightarrow 1}$ and interface S_i of $\mathsf{A\text{-}INS}^{\mathcal{C}}_{n\to 1}$, for $i \in [n]$: on input a message $m \in \mathcal{M}$ from the outside, if not already done so before, output $\diamond$ to $\mathsf{KEY}^{\mathcal{K}}_{n\leftrightarrow 1}$ in order to fetch key k_i, then compute $c \leftarrow \mathtt{Enc}_{k_i}(m) \in \mathcal{C}$ and output c to $\mathsf{A\text{-}INS}^{\mathcal{C}}_{n\to 1}$. Also let the converter adec (where again the dependency on Π is implicit) behave as follows when connected to interface R of $\mathsf{KEY}^{\mathcal{K}}_{n\leftrightarrow 1}$ and interface R of $\mathsf{A\text{-}INS}^{\mathcal{C}}_{n\to 1}$: on input $\diamond$ from the outside, if not already done so before, output $\diamond$ to $\mathsf{KEY}^{\mathcal{K}}_{n\leftrightarrow 1}$ in order to fetch keys $k_1, \ldots, k_n$, and then output $\diamond$ to $\mathsf{A\text{-}INS}^{\mathcal{C}}_{n\to 1}$; for each obtained tuple (j, c), find the index $i \in [n]$ such that $m \neq \bot$, for $m \leftarrow \mathtt{Dec}_{k_i}(c)$, and output the collection of all such resulting tuples (j, m, i) to the outside. Finally, we define the n-protocol $\boldsymbol{\pi}_{\mathsf{pAE}} \doteq (\mathsf{aenc}, \ldots, \mathsf{aenc}, \mathsf{adec})$.

Note that the scheme Π must satisfy a weak form of robustness, that is: an honestly generated ciphertext c, for some message m and key k_i, when decrypted using k_j, for $j \neq i$, will result in $\bot$. As shown in [FOR17], ae\$ security guarantees this property. In Appendix A.1 we will show how our weaker 2-ik-ae also implies such notion of robustness.

Theorem 3.3.2. $[\mathsf{KEY}^{\mathcal{K}}_{n\leftrightarrow 1}, \mathsf{A\text{-}INS}^{\mathcal{C}}_{n\to 1}] \overset{\boldsymbol{\pi}_{\mathsf{pAE}};\, n\text{-ik-ae}}{\Longrightarrow} \mathsf{A\text{-}SEC}^{\mathcal{M}}_{n\to 1}$.

Proof. Define transformation ρ as in Figure 3.8, system $\mathbf{H}_0$ as in Figure 3.9, system $\mathbf{H}_1$ as in Figure 3.10, and simulator $\boldsymbol{\sigma}$ attached to interface E of $\mathsf{A\text{-}SEC}^{\mathcal{M}}_{n\to 1}$ that behaves as follows: Initially, sample a key k_1 according to Gen. Then:

- On input $\diamond$ from the outside, output $\diamond$ on the inside, obtain a set $\mathfrak{O} \subseteq \mathbb{N} \times \mathbb{N}$, and initialize another set $\mathfrak{O}' \subseteq \mathbb{N} \times \mathcal{M}$ to $\varnothing$; Then for each $(j, \ell) \in \mathfrak{O}$, add $(j, \mathtt{Enc}_{k_1}(\tilde{m}))$ to both $\mathfrak{O}'$ and $\mathcal{T}$, for freshly and uniformly sampled $\tilde{m} \in \mathcal{M}$ with $|\tilde{m}| = |m|$. Finally, output $\mathfrak{O}'$.
- On input $c \in \mathcal{C}$ from the outside, if there exists a $j \in \mathbb{N}$ such that $(j, c) \in \mathcal{T}$, then forward j to the inside.

$\rho([\![[\![\mathbf{X}_1, \mathbf{Y}_1]\!], \ldots, [\![\mathbf{X}_n, \mathbf{Y}_n]\!]]\!])$

$\mathfrak{S}, \mathfrak{R} \subseteq (\mathbb{N} \times \mathcal{M} \times \mathbb{N}) \cup (\mathbb{N} \times \{\bot\}^2)$
$c_S, c_R, t_S, t_R \in \mathbb{N}$
Initialize:
  $\mathfrak{S}, \mathfrak{R} \leftarrow \varnothing$
  $c_S, c_R \leftarrow 1$
  $t_S, t_R \leftarrow 0$
Interface $S_i(m)$: // $i \in [n]$
  $t_S \leftarrow t_S + 1$
  $\mathfrak{S} \leftarrow \mathfrak{S} \cup \{(t_S, m, i)\}$
Interface $E(\diamond)$:
  $\mathfrak{O} \leftarrow \{(j, \mathbf{X}_i(m)) \in \mathbb{N} \times \mathcal{C} \mid (j, m, i) \in \mathfrak{S}, c_S \leq j \leq t_S\}$
  $c_S \leftarrow t_S + 1$
  return $\mathfrak{O}$
Interface $E(c)$:
  $t_R \leftarrow t_R + 1$
  if $\exists i \in [n] : \mathbf{Y}_i(c) \neq \bot$ **then**
    $\mathfrak{R} \leftarrow \mathfrak{R} \cup \{(t_R, \mathbf{Y}_i(c), i)\}$
  else
    $\mathfrak{R} \leftarrow \mathfrak{R} \cup \{(t_R, \bot, \bot)\}$
Interface $R(\diamond)$:
  $\mathfrak{O} \leftarrow \{(j, m, i) \in \mathfrak{R} \mid c_R \leq j \leq t_R\}$
  $c_R \leftarrow t_R + 1$
  return $\mathfrak{O}$

Figure 3.8: Transformation ρ for Theorem 3.3.2.

$\mathbf{H}_0$

$\mathfrak{S}, \mathfrak{R} \subseteq \mathbb{N} \times \mathcal{C}$
$c_S, c_R, t_S, t_R \in \mathbb{N}$
$k_1, \ldots, k_n \in \mathcal{K}$
Initialize:
  $\mathfrak{S}, \mathfrak{R} \leftarrow \varnothing$
  $c_S, c_R \leftarrow 1$
  $t_S, t_R \leftarrow 0$
  $k_1, \ldots, k_n \leftarrow \mathtt{Gen}$
Interface $S_i(m)$: // $i \in [n]$
  $t_S \leftarrow t_S + 1$
  $\mathfrak{S} \leftarrow \mathfrak{S} \cup \{(t_S, \mathtt{Enc}_{k_i}(m))\}$
Interface $E(\diamond)$:
  $\mathfrak{O} \leftarrow \{(j, c) \in \mathfrak{S} \mid c_S \leq j \leq t_S\}$
  $c_S \leftarrow t_S + 1$
  return $\mathfrak{O}$
Interface $E(c)$:
  $t_R \leftarrow t_R + 1$
  $\mathfrak{R} \leftarrow \mathfrak{R} \cup \{(t_R, c)\}$
Interface $R(\diamond)$:
  $\mathfrak{O} \leftarrow \{(j, \mathtt{Dec}_{k_i}(c), i) \in \mathbb{N} \times \mathcal{M} \times [n] \mid (j, c) \in \mathfrak{R}, c_R \leq j \leq t_R,$
    $\mathtt{Dec}_{k_i}(c) \neq \perp\} \cup \{(j, \perp, \perp) \mid \exists c \in \mathcal{C} : (j, c) \in \mathfrak{R}, c_R \leq j \leq t_R,$
    $\forall i \in [n] : \mathtt{Dec}_{k_i}(c) = \perp\}$
  $c_R \leftarrow t_R + 1$
  return $\mathfrak{O}$

Figure 3.9: Hybrid system $\mathbf{H}_0$ for Theorem 3.3.2.

$\mathbf{H}_1$

$\mathfrak{S}, \mathfrak{R} \subseteq (\mathbb{N} \times \mathcal{M} \times \mathbb{N}) \cup (\mathbb{N} \times \{\bot\}^2)$
$\mathfrak{T} \subseteq \mathbb{N} \times \mathcal{C}$
$c_S, c_R, t_S, t_R \in \mathbb{N}$
$k_1 \in \mathcal{K}$
Initialize:
  $\mathfrak{S}, \mathfrak{R}, \mathfrak{T} \leftarrow \varnothing$
  $c_S, c_R \leftarrow 1$
  $t_S, t_R \leftarrow 0$
  $k_1 \leftarrow \texttt{Gen}$
Interface $S_i(m)$: // $i \in [n]$
  $t_S \leftarrow t_S + 1$
  $\mathfrak{S} \leftarrow \mathfrak{S} \cup \{(t_S, m, i)\}$
Interface $E(\diamond)$:
  $\tilde{m} \leftarrow \{0,1\}^{|m|}$
  $\mathfrak{O} \leftarrow \{(j, \texttt{Enc}_{k_1}(\tilde{m})) \in \mathbb{N} \times \mathcal{C} \mid \exists i \in [n] : (j, m, i) \in \mathfrak{S}, c_S \leq j \leq t_S\}$
  $\mathfrak{T} \leftarrow \mathfrak{T} \cup \mathfrak{O}$
  $c_S \leftarrow t_S + 1$
  return $\mathfrak{O}$
Interface $E(c)$:
  $t_R \leftarrow t_R + 1$
  if $\exists j \in \mathbb{N} : (j, c) \in \mathfrak{T}$ **then**
    $\mathfrak{R} \leftarrow \mathfrak{R} \cup \{(t_R, m, i) \in \mathbb{N} \times \mathcal{M} \times \mathbb{N} \mid (j, m, i) \in \mathfrak{S}\}$
  else
    $\mathfrak{R} \leftarrow \mathfrak{R} \cup \{(t_R, \bot, \bot)\}$
Interface $R(\diamond)$:
  $\mathfrak{O} \leftarrow \{(j, m, i) \in \mathfrak{R} \mid c_R \leq j \leq t_R\}$
  $c_R \leftarrow t_R + 1$
  return $\mathfrak{O}$

Figure 3.10: Hybrid system $\mathbf{H}_1$ for Theorem 3.3.2.

Let $k_1, \ldots, k_n \leftarrow \mathtt{Gen}$. Then,

$$\begin{aligned}
&\boldsymbol{\pi}_{\mathsf{pAE}}\,[\mathsf{KEY}^{\mathcal{K}}_{n\leftrightarrow 1}, \mathsf{A\text{-}INS}^{\mathcal{C}}_{n\to 1}] \\
&\quad \equiv \mathbf{H}_0 && \text{(monolithic representation)} \\
&\quad \equiv \rho([\![\mathbf{E}_{k_1}, \mathbf{D}_{k_1}]\!], \ldots, [\![\mathbf{E}_{k_n}, \mathbf{D}_{k_n}]\!]) && \text{(by inspection)} \\
&\quad \eqsim \rho([\![\rho^{\mathsf{ae}}(\mathbf{E}_{k_1}), \ldots, \rho^{\mathsf{ae}}(\mathbf{E}_{k_1})]\!]) && (n\text{-}\mathsf{ik\text{-}ae}) \\
&\quad \equiv \mathbf{H}_1 && \text{(correctness)} \\
&\quad \equiv \boldsymbol{\sigma}\,\mathsf{A\text{-}SEC}^{\mathcal{M}}_{n\to 1}. && \text{(monolithic representation)}
\end{aligned}$$

□

Note that, analogously as for pE, by combining Theorem 3.3.2 with Theorem 3.2.18, we also have

$$[\mathsf{KEY}^{\mathcal{K}}_{n\leftrightarrow 1}, \mathsf{A\text{-}INS}^{\mathcal{C}}_{n\to 1}] \xrightarrow{\boldsymbol{\pi}_{\mathsf{pAE}};\, \mathsf{ae\$}} \mathsf{A\text{-}SEC}^{\mathcal{M}}_{n\to 1}.$$

Comparison With Alwen et al. Again, note that in [AHM+15, Theorem 2] this direct construction step was already presented but the suggested protocol is again much less efficient than ours. The idea improves upon the previous one used to construct $\mathsf{A\text{-}SEC}^{\mathcal{M}}_{n\to 1}$ from $\mathsf{A\text{-}AUT}^{\mathcal{R}\times[\ell]}_{n\to 1}$, by using the randomness $r \in \mathcal{R}$ only once per message, and reducing the domain of the underlying MAC scheme to $|\mathcal{R}| + \log \ell$ bits (where again we are assuming $\mathcal{M} = \{0,1\}^{\ell}$). Detailedly, given a MAC with message space $\mathcal{M}' \doteq \mathcal{R} \times \{0,1\}^{\log \ell}$ and tag space $\mathcal{T}$, the protocol uses $[\mathsf{KEY}^{\mathcal{K}}_{n\leftrightarrow 1}, \mathsf{KEY}^{\mathcal{K}}_{n\leftrightarrow 1}, \mathsf{A\text{-}INS}^{\mathcal{R}\times\mathcal{T}^{\ell}}_{n\to 1}]$ in the following way: on input a message $m = (m_1, \ldots, m_\ell) \in \mathcal{M}$ at the outside interface assigned to sender S_i, compute $c \doteq (r, \mathtt{Tag}_{k_{i,m_1}}(r,1), \ldots, \mathtt{Tag}_{k_{i,m_\ell}}(r,\ell))$, where r is sampled uniformly at random over $\mathcal{R}$, $k_{i,0}$ is the key shared by S_i and R through the first $\mathsf{KEY}^{\mathcal{K}}_{n\leftrightarrow 1}$ resource, and $k_{i,1}$ is the key shared by S_i and R through the second $\mathsf{KEY}^{\mathcal{K}}_{n\leftrightarrow 1}$ resource. Then at the receiver interface R, each message is reconstructed by testing the value $(r, \tau_1, \ldots, \tau_\ell)$ obtained by $\mathsf{A\text{-}INS}^{\mathcal{R}\times\mathcal{T}^{\ell}}_{n\to 1}$ against each possible key-pair $(k_{i,0}, k_{i,1})$, for $i \in [n]$, and message $(m_1, \ldots, m_\ell) \in \{0,1\}^{\ell}$: if for each $j \in [\ell]$ the tag τ_j is valid for the (MAC) message $(r, j) \in \mathcal{R} \times \{0,1\}^{\log \ell}$ under key k_{i,m_j}, then output $(\cdot, (m_1, \ldots, m_\ell), i)$

Note that the major drawbacks of this construction are (1) the fact that even if the message space of the MAC has been reduced, this must be invoked ℓ times for each message (as opposed to 1 time), and (2) the fact that the time complexity of the receiver is $\mathcal{O}(n\ell)$ for each message (as opposed to $\mathcal{O}(n)$). Here we improve the efficiency of this construction by employing authenticated encryption instead; therefore, this can be seen as improving upon both the amount of invocations to the underlying primitive (once per message—once MAC and once encryption, if the scheme arises from the Encrypt-then-MAC paradigm—instead of ℓ), and the time complexity associated to the receiving of each message: we only need to test the received ciphertext against each possible of the n keys. Moreover, our construction statement arguably feels more "natural" than the one of [AHM+15].

Chapter 4

Anonymity Preservation: Public-Key Primitives

4.1 Introduction

4.1.1 Motivation

When studying the security of public-key encryption (PKE) it is natural to consider a setting with one sender and many receivers, each generating its own key-pair and authentically transmitting the public key to the sender. Then a reasonable concern is whether ciphertexts subsequently generated by the sender for distinct receivers are (computationally) indistinguishable. This captures the intuitive notion of receiver anonymity from the standpoint of an eavesdropper, and is formalized by the security definition of *key-indistinguishability*, first proposed by Bellare et al. [BBDP01]. Almost a decade later, Abdalla et al. [ABN10] introduced another related notion for PKE, *robustness*, which intuitively captures the fact that ciphertexts can only be meaningfully decrypted using the correct corresponding private key, meaning that trying to decrypt with a wrong key results in an error.

It turns out that this further property is crucially needed in conjunction with key-indistinguishability in order to provide a "usable" form of anonymous PKE, and this has been highlighted by Kohlweiss et al.

[KMO+13] by showing that both properties, together with IND-CCA security, are needed in order for a PKE scheme to enhance an anonymous insecure broadcast channel into an anonymous confidential broadcast channel. Importantly, their work also highlights how key-indistinguishability is a security notion that exclusively *preserves* anonymity, rather than "creating" it, whereas IND-CCA *lifts* insecurity to confidentiality, thus "creating" more security along the secrecy axis.

On the other hand, for the security of digital signature schemes (DSS) the natural setting to consider is the dual of the above: Many senders, each authentically publishing their public verification key, send messages to the same party, the receiver. Here too it is reasonable to consider anonymity (preservation), of the sender in this case, from the standpoint of an eavesdropper. But in this setting it is additionally also meaningful to study the stronger notion of anonymity from the standpoint of the receiver, that is, we might want the senders to remain anonymous not only towards an external attacker (the eavesdropper), but towards the receiver as well. We distinguish those two separate notions of anonymity in this setting as *external* and *internal*, respectively, where clearly the latter implies the former (but not vice versa). However, unlike for PKE, the situation is arguably more intricate for DSS; in fact, providing external anonymity alone already appears paradoxical: How can we guarantee (computational) indistinguishability of signatures, when in the usual application of DSS it is assumed that an eavesdropper has access to the corresponding message as well as all possible verification keys, and could therefore easily distinguish signatures generated with different keys by simply verifying the signature on the message against all keys?

A direct consequence of this apparent dilemma is that for the setting discussed above, the standard syntactic definition of a DSS cannot possibly achieve any meaningful form of anonymity, as we prove later within our framework. This is in fact the reason why in the cryptographic literature there exist a multitude of different security notions capturing various forms of anonymity in relation to syntactic modifications of the usual DSS definition. A non-exhaustive list of examples includes: group signatures [Cv91], ring signatures [RST01], anonymous signatures [YWDW06, Fis07, ZI09], and partial signatures [BD09, SY09].

In this chapter we take an alternative approach in order to treat the apparently oxymoronic problem of achieving anonymous authenticity: Instead of creating new syntactic modifications of DSS and ad-hoc game-

based security definitions thereof, we begin from a more abstract point of view and identify possible applications where those two goals simultaneously come into play, and directly define security in a composable fashion, using the framework of constructive cryptography of Maurer and Renner [MR11, Mau12] introduced in Section 2.4, requiring that a protocol realizes such an application relying on the public-key infrastructure (PKI). More precisely, we introduce three novel composable security notions for generic protocols, and then present concrete protocols satisfying each of those. The first protocol makes use of a novel cryptographic scheme, dubbed *bilateral signatures*, while the other two employ *partial signatures* and *ring signatures*, respectively.

4.1.2 Related Work

The goal of this chapter is to finish filling the blanks in the composable treatment of anonymity preservation. To better understand what is missing in this line of research, let us summarize the state of affairs. Recall some typical resources used in constructive cryptography: the *insecure channel* INS (which leaks everything the sender inputs to the adversary, and allows the latter to send values to the receiver), the *authenticated channel* AUT, the *confidential channel* CNF, and the secure (i.e., authentic and confidential) channel SEC, all allowing to send multiple values. In order to capture anonymity, we are interested in a setting where there are multiple parties. More concretely, we consider resources with n senders $S_1, \ldots, S_n$ and one receiver R (for which we use the intuitive notation ${}_{n\to 1}$), and resources with one sender and n receivers (for which we use the intuitive notation ${}_{1\to n}$). If one considers the above channels, a natural approach to extend them to this setting would be to simply compose them in parallel, but this would imply that the leakage now includes the identities of the sender S_i or the receiver R_i, since the individual channels are distinguishable by definition by the adversary. In the following table we summarize the guarantees provided by resources combining such channels (which we also denote as channels) in terms of what is leaked to the adversary relative to a value $x \in \mathcal{X}$, for some set $\mathcal{X}$, input by a sender and whether the adversary can inject values (such that the receiver can not distinguish whether the value was sent by the sender S or the adversary E).

Channel	Leaked	Inject	Channel	Leaked	Inject
$\mathsf{INS}^{\mathcal{X}}_{n\to 1}$	S_i, x	yes	$\mathsf{INS}^{\mathcal{X}}_{1\to n}$	R_i, x	yes
$\mathsf{AUT}^{\mathcal{X}}_{n\to 1}$	S_i, x	no	$\mathsf{AUT}^{\mathcal{X}}_{1\to n}$	R_i, x	no
$\mathsf{CNF}^{\mathcal{X}}_{n\to 1}$	$S_i, \lvert x\rvert$	yes	$\mathsf{CNF}^{\mathcal{X}}_{1\to n}$	$R_i, \lvert x\rvert$	yes
$\mathsf{SEC}^{\mathcal{X}}_{n\to 1}$	$S_i, \lvert x\rvert$	no	$\mathsf{SEC}^{\mathcal{X}}_{1\to n}$	$R_i, \lvert x\rvert$	no

It seems natural that truly *anonymous* versions of these channels, that is, channels capturing sender and receiver anonymity, must *not* leak such identities to the adversary. Therefore we enhance the above channels with these guarantees (adding the prefix A- for *anonymous*), and summarize the new channels in the following table (note that in $\mathsf{A\text{-}AUT}^{\mathcal{M}}_{n\to 1}$, $\mathsf{A\text{-}CNF}^{\mathcal{M}}_{n\to 1}$, and $\mathsf{A\text{-}SEC}^{\mathcal{M}}_{n\to 1}$, the receiver also obtains the identity S_i of the sender, along with the message $m \in \mathcal{M}$).

Channel		Leaked	Inject
Sender anon.	Receiver anon.		
$\mathsf{A\text{-}INS}^{\mathcal{X}}_{n\to 1}$	$\mathsf{A\text{-}INS}^{\mathcal{X}}_{1\to n}$	x	yes
$\mathsf{A\text{-}AUT}^{\mathcal{X}}_{n\to 1}$	$\mathsf{A\text{-}AUT}^{\mathcal{X}}_{1\to n}$	x	no
$\mathsf{A\text{-}CNF}^{\mathcal{X}}_{n\to 1}$	$\mathsf{A\text{-}CNF}^{\mathcal{X}}_{1\to n}$	$\lvert x\rvert$	yes
$\mathsf{A\text{-}SEC}^{\mathcal{X}}_{n\to 1}$	$\mathsf{A\text{-}SEC}^{\mathcal{X}}_{1\to n}$	$\lvert x\rvert$	no

Other (non-anonymous) resources that we need in this setting are: $\mathsf{KEY}^{\mathcal{K}}_{n\leftrightarrow 1}$, for some set of keys $\mathcal{K}$, which provides each sender with a (different) *shared secret-key* with the receiver; $\mathsf{KEY}^{\mathcal{K}}_{1\leftrightarrow n}$, which provides each receiver with a shared secret-key with the sender (in both resources, the adversary's interface is inactive); $\mathsf{1\text{-}AUT}^{\mathcal{PK}}_{n\to 1}$, for some set of public keys $\mathcal{PK}$, which provides each sender with a (different) *single-use authenticated channel* to the receiver; $\mathsf{1\text{-}AUT}^{\mathcal{PK}}_{1\leftarrow n}$, which provides the receiver with n (different) *single-use authenticated channels*, one to each of the senders.

We stress again that we are considering anonymity *preservation*, therefore in the following we summarize the previous results from the literature in terms of constructions among the anonymous channels mentioned above (plus shared secret keys and one-time authenticated channels). This means that both real and ideal core resources are anonymous, and hence the enhancement of security provided by a construction happens along a different axis (namely confidentiality, authenticity, or both).

- In the symmetric-key setting, two works provide sender anonymous constructions, for messages set $\mathcal{M}$, ciphertexts set $\mathcal{C}$, and MAC tags set $\mathcal{T}$:

  – In [AHM+15], Alwen et al. show that for a simple protocol $\boldsymbol{\pi}_{\mathsf{pMAC}}$ based on key-indistinguishable and unforgeable *probabilistic MAC* schemes,

  $$[\mathsf{KEY}^{\mathcal{K}}_{n\leftrightarrow 1}, \mathsf{A\text{-}INS}^{\mathcal{M}\times\mathcal{T}}_{n\to 1}] \overset{\boldsymbol{\pi}_{\mathsf{pMAC}}}{\Longrightarrow} \mathsf{A\text{-}AUT}^{\mathcal{M}}_{n\to 1}.$$

  – As presented in Chapter 3, in [BM20] Banfi and Maurer show that for a simple protocol $\boldsymbol{\pi}_{\mathsf{pE}}$ based on key-indistinguishable and IND-CPA *probabilistic encryption* schemes,

  $$[\mathsf{KEY}^{\mathcal{K}}_{n\leftrightarrow 1}, \mathsf{A\text{-}AUT}^{\mathcal{C}}_{n\to 1}] \overset{\boldsymbol{\pi}_{\mathsf{pE}}}{\Longrightarrow} \mathsf{A\text{-}SEC}^{\mathcal{M}}_{n\to 1},$$

  and for a simple protocol $\boldsymbol{\pi}_{\mathsf{pAE}}$ based on key-indistinguishable and IND-CCA3 *probabilistic authenticated encryption* schemes,

  $$[\mathsf{KEY}^{\mathcal{K}}_{n\leftrightarrow 1}, \mathsf{A\text{-}INS}^{\mathcal{C}}_{n\to 1}] \overset{\boldsymbol{\pi}_{\mathsf{pAE}}}{\Longrightarrow} \mathsf{A\text{-}SEC}^{\mathcal{M}}_{n\to 1}.$$

- In the public-key setting, Kohlweiss et al. [KMO+13] show that for a simple protocol $\boldsymbol{\pi}_{\mathsf{PKE}}$ based on key-indistinguishable and robust IND-CCA *public-key encryption* schemes,

  $$[\mathsf{1\text{-}AUT}^{\mathcal{PK}}_{1\leftarrow n}, \mathsf{A\text{-}INS}^{\mathcal{C}}_{1\to n}] \overset{\boldsymbol{\pi}_{\mathsf{PKE}}}{\Longrightarrow} \mathsf{A\text{-}CNF}^{\mathcal{M}}_{1\to n}.$$

So far, no public-key constructions achieving sender anonymity were given, and we fill precisely this gap here, stated as an open problem in [KMO+13].

4.1.3 Contributions

Referring to the above discussion, it is natural to ask whether it is possible to construct $\mathsf{A\text{-}AUT}^{\mathcal{M}}_{n\to 1}$ from $\mathsf{1\text{-}AUT}^{\mathcal{PK}}_{n\to 1}$ and $\mathsf{A\text{-}INS}^{\mathcal{M}\times\mathcal{S}}_{n\to 1}$, for some set of signatures $\mathcal{S}$, using a protocol based on signature schemes achieving some form of anonymity. But it is rather easy to see that for regular signature

schemes, this is impossible. Using an intuitive notation, the first result that we show is in fact that for any such protocol $\boldsymbol{\pi}$,

$$[\mathsf{1\text{-}AUT}^{\mathcal{PK}}_{n\to 1}, \mathsf{A\text{-}INS}^{\mathcal{M}\times\mathcal{S}}_{n\to 1}] \overset{\boldsymbol{\pi}}{\not\Longrightarrow} \mathsf{A\text{-}AUT}^{\mathcal{M}}_{n\to 1}, \tag{4.1}$$

that is, no protocol that is attached *exclusively* to the resources $\mathsf{1\text{-}AUT}^{\mathcal{PK}}_{n\to 1}$ and $\mathsf{A\text{-}INS}^{\mathcal{M}\times\mathcal{S}}_{n\to 1}$ (composed in parallel), can construct $\mathsf{A\text{-}AUT}^{\mathcal{M}}_{n\to 1}$. We prove this in Section 4.2.1.

The main goal of this chapter is to show how to get around this impossibility result by rethinking what can actually be achieved in this setting. We still did not discuss the guarantees of the receiver: In $\mathsf{A\text{-}AUT}^{\mathcal{X}}_{n\to 1}$, while only the value x input by the sender S_i is leaked to the adversary, the receiver will see both x and the sender's identity S_i. Therefore, we identify two natural ways in which we can modify this resource such that we can then make meaningful statements. We see this systematic approach as a further contribution of this chapter.

- We introduce the new resource *de-anonymizable authenticated channel* $\mathsf{D\text{-}AUT}^{\mathcal{X}}_{n\to 1}$, which is similar to $\mathsf{A\text{-}AUT}^{\mathcal{X}}_{n\to 1}$, except that it only guarantees authenticity of a sender once it decides to give up its anonymity. In more detail, a sender S_i can send a value x, and both the adversary and the receiver will only see x, but can decide at a later point to leak its identity to both parties, and this capability is not available to the adversary. This channel could be used for example in an anonymous auction, where bids need to be anonymous but the winner is required to later give up its anonymity in order to (authentically) claim the winning bet.

- We also introduce the new ideal resource *receiver-side anonymous authenticated channel* $\mathsf{RA\text{-}AUT}^{\mathcal{X}}_{n\to 1}$, which is similar to $\mathsf{A\text{-}AUT}^{\mathcal{X}}_{n\to 1}$, except that the anonymity of the sender is guaranteed also towards the receiver, not just the adversary. Therefore, $\mathsf{RA\text{-}AUT}^{\mathcal{X}}_{n\to 1}$ also captures *internal* anonymity.

In the following table we summarize the guarantees provided by those resources.

Channel	Leaked	Inject	Received
$\mathsf{A\text{-}AUT}^{\mathcal{X}}_{n\to 1}$	x	no	S_i, x
$\mathsf{D\text{-}AUT}^{\mathcal{X}}_{n\to 1}$	$x/(S_i, x)$	$\tilde{x}/\cancel{(S_j, \tilde{x})}$	$x/(S_i, x)$
$\mathsf{RA\text{-}AUT}^{\mathcal{X}}_{n\to 1}$	x	no	x

We can now summarize our contribution as providing constructions that, compared to equation (4.1), (i) use a different set of assumed resources, (ii) realize a different kind of ideal resource, or (iii) both. For (i) we show that a new scheme that we introduce, *bilateral signatures*, can be used to construct $\mathsf{A\text{-}AUT}^{\mathcal{M}}_{n\to 1}$ if we further assume a (single-use) authenticated channel from the receiver to the senders, $\mathsf{1\text{-}AUT}^{\mathcal{PK}}_{n\leftarrow 1}$. Informally, we show that

$$[\mathsf{1\text{-}AUT}^{\mathcal{PK}}_{n\to 1}, \mathsf{1\text{-}AUT}^{\mathcal{PK}}_{n\leftarrow 1}, \mathsf{A\text{-}INS}^{\mathcal{M}\times\mathcal{S}}_{n\to 1}] \overset{\boldsymbol{\pi}_{\mathsf{BS}}}{\Longrightarrow} \mathsf{A\text{-}AUT}^{\mathcal{M}}_{n\to 1},$$

which amounts to giving composable semantics to bilateral signatures. For (ii) we show that $\mathsf{D\text{-}AUT}^{\mathcal{M}}_{n\to 1}$ can be constructed from the original set of assumed resources from equation (4.1) using *partial signatures* from [BD09, SY09]. Informally, we show that

$$[\mathsf{1\text{-}AUT}^{\mathcal{PK}}_{n\to 1}, \mathsf{A\text{-}INS}^{\mathcal{M}\times\mathcal{S}}_{n\to 1}] \overset{\boldsymbol{\pi}_{\mathsf{PS}}}{\Longrightarrow} \mathsf{D\text{-}AUT}^{\mathcal{M}}_{n\to 1},$$

which amounts to giving composable semantics to partial signatures. Finally, for (iii) we show that $\mathsf{RA\text{-}AUT}^{\mathcal{M}}_{n\to 1}$ can be constructed using *ring signatures* [RST01, BKM06] if instead of $\mathsf{1\text{-}AUT}^{\mathcal{PK}}_{n\to 1}$, we assume a (single-use) *broadcast authenticated channel*, $\mathsf{1\text{-}AUT}^{\mathcal{PK}}_{n\circlearrowleft 1}$, which from each sender authentically transmits a message to the receiver, as well as all other senders. Informally, we show that

$$[\mathsf{1\text{-}AUT}^{\mathcal{PK}}_{n\circlearrowleft 1}, \mathsf{A\text{-}INS}^{\mathcal{M}\times\mathcal{S}}_{n\to 1}] \overset{\boldsymbol{\pi}_{\mathsf{RS}}}{\Longrightarrow} \mathsf{RA\text{-}AUT}^{\mathcal{M}}_{n\to 1},$$

which amounts to giving composable semantics to ring signatures.

4.1.4 Constructive Cryptography with Specifications

For the construction based on partial signatures, we will need an extended version of constructive cryptography that defines statements via *specifications*, rather than resources as introduced in Section 2.4. For this,

we will loosely follow the work of Maurer and Renner [MR16], and later, when presenting the construction itself in Section 4.4.2, we will further incorporate newer concepts from the work of Jost and Maurer [JM20]. In order to keep the presentation self-contained, we will only glance over the necessary components of such extension of CC.

Roughly speaking, a specification is a set of resources. Another important concept, is that of a *relaxation*, which can be seen as a way to map a single resource to a specification. Within our formalism of CC based on substitutions, the most fundamental relaxation is the so-called *substitution-relaxation*.[1] For a resource R and a substitution s, it is defined as

$$\mathsf{R}^{\mathsf{s}} \doteq \{\mathsf{S} \mid \mathsf{s} \implies \mathsf{S} \eqsim \mathsf{R}\}.$$

The set R^{s} can be understood as the set of all resources that are s-*close* to R, that is, all resources where applying the substitution s (wherever possible), yields R. More precisely, assuming s is defined as $\mathbf{X}_0 \eqsim \mathbf{X}_1$, for some systems $\mathbf{X}_0, \mathbf{X}_1$, R^{s} is comprised of all resources S for which there exist an (efficient) transformation ρ_{S} such that $\mathsf{S} \equiv \rho_{\mathsf{S}}(\mathbf{X}_0) \eqsim \rho_{\mathsf{S}}(\mathbf{X}_1) \equiv \mathsf{R}$. Since specifications themselves can be relaxed, for a specification $\mathcal{S}$, we further have

$$\mathcal{S}^{\mathsf{s}} \doteq \bigcup_{\mathsf{R} \in \mathcal{S}} \mathsf{R}^{\mathsf{s}} = \{\mathsf{S} \mid \exists \mathsf{R} \in \mathcal{S} : \mathsf{s} \implies \mathsf{S} \eqsim \mathsf{R}\}.$$

This allows for an alternative definition of the construction statement from Definition 2.4.3: Given two resources REAL and IDEAL, a substitution s, we can say that a protocol $\boldsymbol{\pi}$ constructs IDEAL from REAL assuming s if there exists a simulator $\boldsymbol{\sigma}$ such that

$$\boldsymbol{\pi}\,\mathsf{REAL} \in (\boldsymbol{\sigma}\,\mathsf{IDEAL})^{\mathsf{s}}. \tag{4.2}$$

Note that by understanding single resources as singleton specifications, we can replace $\in$ by $\subseteq$, and therefore composition trivially follows by the transitivity of the subset relation (see [MR16] for more details.)

4.2 Anonymous and Authenticated Resources

In this section we present the n-resources that we need later in order to make our security statements. Instead of bold-face letters, for such

[1] In [MR16], this corresponds to the ε-relaxation.

resources we will use suggestive sans-serif abbreviations. We describe all resources first on an intuitive level, and then formally following the model introduced in [BM20] and already used in Chapter 3, in which communication is modeled by a sender buffer $\mathfrak{S}$ and a receiver buffer $\mathfrak{R}$, both allowing to insert single elements and to read in chunks. Note that all our resources are parameterized by an arbitrary set $\mathcal{X}$, but we will make the instantiation of such set implicit when showing constructions.

We begin by describing the three single-use authenticated channels needed as assumed resources in order to authentically exchange public keys. The first such resource is $\mathsf{1\text{-}AUT}^{\mathcal{X}}_{n\to 1}$, which allows to input a value once at every sender interface S_i, for $i \in [n]$, and allows to read these values at the receiver and adversary interfaces, R and E, respectively. Based on this resource, we then simply define $\mathsf{1\text{-}AUT}^{\mathcal{X}}_{n\leftarrow 1}$ as somewhat the dual of this, namely, the resource that allows to input a value once at the receiver interface R, and that allows to read this value at every sender and adversary interface, S_i, for $i \in [n]$, and E, respectively. Finally, we also need the resource $\mathsf{1\text{-}AUT}^{\mathcal{X}}_{n\circlearrowright 1}$, which similarly to $\mathsf{1\text{-}AUT}^{\mathcal{X}}_{n\to 1}$ allows to input a value once at every sender interface S_i, for $i \in [n]$, but additionally allows to read these values at all the sender interfaces S_i as well. We formally describe these three resources in Figure 4.1. We tacitly assume that protocols first use those resources to exchange public-keys, and only once all keys have been exchanged, they use the channel resources. We also point out that our results are in a model in which public keys are therefore assumed to always be honestly generated. We leave open the problem of strengthening the model by replacing these resources by a *certificate authority*, which would allow the adversary to also register keys.

We next describe the assumed channel resource $\mathsf{A\text{-}INS}^{\mathcal{X}}_{n\to 1}$ as well as the three different ideal anonymous channel resources $\mathsf{A\text{-}AUT}^{\mathcal{X}}_{n\to 1}$, $\mathsf{D\text{-}AUT}^{\mathcal{X}}_{n\to 1}$, and $\mathsf{RA\text{-}AUT}^{\mathcal{X}}_{n\to 1}$ (all depicted in Figure 4.2).

- The *anonymous insecure channel* $\mathsf{A\text{-}INS}^{\mathcal{X}}_{n\to 1}$, formalized in Figure 4.3. allows to input multiple values at every sender interface S_i, for $i \in [n]$. Those values are stored in the sender buffer $\mathfrak{S}$, from which they can be read at the adversary interface E. Moreover, at this interface $\mathsf{A\text{-}INS}^{\mathcal{X}}_{n\to 1}$ also allows the adversary to inject multiple arbitrary values. Those values are stored in the receiver buffer $\mathfrak{R}$, from which they can be read at the receiver interface R.

- In the *anonymous authenticated channel* $\mathsf{A\text{-}AUT}^{\mathcal{X}}_{n\to 1}$, formalized in

$\mathsf{1\text{-}AUT}^{\mathcal{X}}_{n\to 1}$

$x_1, \ldots, x_n \in \mathcal{X} \cup \{\bot\}$
Initialize:
  $x_1, \ldots, x_n \leftarrow \bot$
Interface $S_i(\xi \in \mathcal{X})$: // $i \in [n]$
  $x_i \leftarrow \xi$
Interface $E(\diamond)$:
  $\mathfrak{O} \leftarrow \{(i, x_i) \,|\, i \in [n]\}$
  return $\mathfrak{O}$
Interface $R(\diamond)$:
  $\mathfrak{O} \leftarrow \{(i, x_i) \,|\, i \in [n]\}$
  return $\mathfrak{O}$

$\mathsf{1\text{-}AUT}^{\mathcal{X}}_{n\leftarrow 1}$

$x \in \mathcal{X} \cup \{\bot\}$
Initialize:
  $x \leftarrow \bot$
Interface $S_i(\diamond)$: // $i \in [n]$
  return x
Interface $E(\diamond)$:
  return x
Interface $R(\xi \in \mathcal{X})$:
  $x \leftarrow \xi$

$\mathsf{1\text{-}AUT}^{\mathcal{X}}_{n\circlearrowleft 1}$

$x_1, \ldots, x_n \in \mathcal{X} \cup \{\bot\}$
Initialize:
  $x_1, \ldots, x_n \leftarrow \bot$
Interface $S_i(\xi \in \mathcal{X})$: // $i \in [n]$
  $x_i \leftarrow \xi$
Interface $S_i(\diamond)$: // $i \in [n]$
  $\mathfrak{O} \leftarrow \{(i, x_i) \,|\, i \in [n]\}$
  return $\mathfrak{O}$
Interface $E(\diamond)$:
  $\mathfrak{O} \leftarrow \{(i, x_i) \,|\, i \in [n]\}$
  return $\mathfrak{O}$
Interface $R(\diamond)$:
  $\mathfrak{O} \leftarrow \{(i, x_i) \,|\, i \in [n]\}$
  return $\mathfrak{O}$

Figure 4.1: Formal description of the *single use authenticated channels* $\mathsf{1\text{-}AUT}^{\mathcal{X}}_{n\to 1}$, $\mathsf{1\text{-}AUT}^{\mathcal{X}}_{n\leftarrow 1}$, and $\mathsf{1\text{-}AUT}^{\mathcal{X}}_{n\circlearrowleft 1}$.

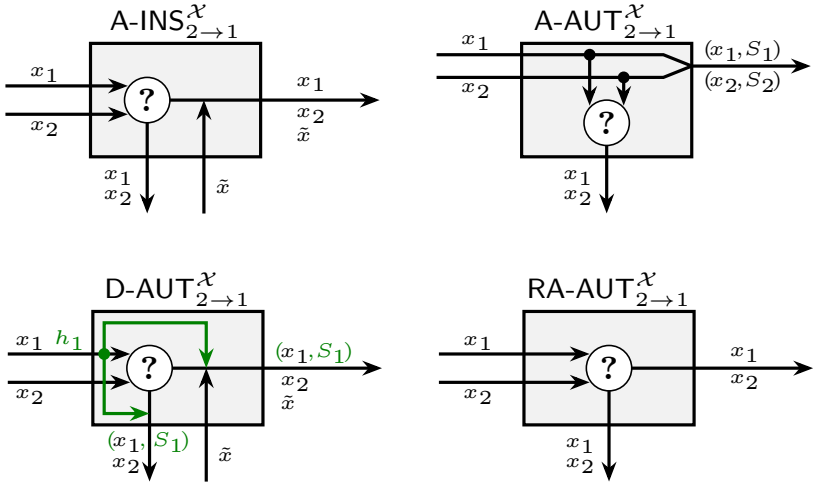


Figure 4.2: Sketches of the anonymous channel resources for $n = 2$ senders (S_1 sending m_1 and S_2 sending m_2). For D-AUT$^{\mathcal{X}}_{2\to1}$, only S_1 de-anonymizes its message (in green).

Figure 4.4, the sender buffer $\mathfrak{S}$ is used exactly as in A-INS$^{\mathcal{X}}_{n\to1}$, except that for every value sent, information about the sender is also stored, but not leaked to the adversary. Unlike A-INS$^{\mathcal{X}}_{n\to1}$, at the interface E, A-AUT$^{\mathcal{X}}_{n\to1}$ only allows the adversary to select which values previously input by a sender will be transmitted to the receiver. Those values, along with the sender information, will be transferred from the sender buffer $\mathfrak{S}$ to the receiver buffer $\mathfrak{R}$, from which they can be read at the receiver interface R.

- The *de-anonymizable authenticated channel* D-AUT$^{\mathcal{X}}_{n\to1}$, formalized in Figure 4.5, allows to input two type of values at every sender interface S_i, for $i \in [n]$: one to commit a value $x \in \mathcal{X}$, $(\underline{\texttt{cmt}}, x)$, and the other to authenticate a previously committed value $x' \in \mathcal{X}$, $(\underline{\texttt{aut}}, h_{x'})$, where $h_{x'}$ is a handle for x' generated by D-AUT$^{\mathcal{X}}_{n\to1}$. Those values are stored in the sender buffer $\mathfrak{S}$, from which they can be read at the adversary interface E. Information about the sender is also stored, but is only leaked to the adversary along with $\underline{\texttt{aut}}$

values. At the interface E, $\mathsf{D\text{-}AUT}^{\mathcal{X}}_{n\to 1}$ allows the adversary to select which values (of both types) previously input by a sender will be transmitted to the receiver, as well as to inject additional `cmt` values. Those values, including sender information only in case of `aut` values, will be transferred from the sender buffer $\mathfrak{S}$ to the receiver buffer $\mathfrak{R}$, from which they can be read at the receiver interface R.

- The *receiver-side anonymous authenticated channel* $\mathsf{RA\text{-}AUT}^{\mathcal{X}}_{n\to 1}$, formalized in Figure 4.6, works exactly as $\mathsf{A\text{-}AUT}^{\mathcal{X}}_{n\to 1}$, except that sender information is concealed from the receiver as well (and therefore never stored in the buffers $\mathfrak{S}$ and $\mathfrak{R}$).

4.2.1 No Anonymity Preservation from DSS

In this section we briefly formalize the simple intuition that regular digital signature schemes (DSS) do not preserve anonymity. We do so in a more generic and composable way: What we prove is that actually no protocol can enhance an insecure channel to an authentic one while preserving its anonymity by only having public one-time authentic information flowing from the receivers to the sender. Clearly, using DSS in the usual way is just one of the possible such protocols.

Proposition 4.2.1. *For any protocol $\boldsymbol{\pi}$, any simulator $\boldsymbol{\sigma}$, and any $\varepsilon < 1 - \frac{1}{n}$,*

$$\boldsymbol{\pi}\,[\mathsf{1\text{-}AUT}^{\mathcal{PK}}_{n\to 1}, \mathsf{A\text{-}INS}^{\mathcal{M}\times\mathcal{S}}_{n\to 1}] \not\approx_{\varepsilon} \boldsymbol{\sigma}\,\mathsf{A\text{-}AUT}^{\mathcal{M}}_{n\to 1}.$$

Proof. Let $\boldsymbol{\pi}$ be any n-protocol and $\boldsymbol{\sigma}$ any simulator. Recall the definition of distinguishing advantage from Section 2.3.3. We prove the statement concretely by showing that there is a distinguisher $\mathbf{D}$ such that

$$\Delta^{\mathbf{D}}(\boldsymbol{\pi}\,[\mathsf{1\text{-}AUT}^{\mathcal{PK}}_{n\to 1}, \mathsf{A\text{-}INS}^{\mathcal{M}\times\mathcal{S}}_{n\to 1}], \boldsymbol{\sigma}\,\mathsf{A\text{-}AUT}^{\mathcal{M}}_{n\to 1}) \geq 1 - \frac{1}{n},$$

which is sufficient to prove the claim. $\mathbf{D}$ works as follows. First, it chooses a random message $m \xleftarrow{\$} \mathcal{M}$ and a random index $i \xleftarrow{\$} [n]$, and inputs m at interface S_i. Then it inputs $\diamond$ at interface E of (possibly emulated) $\mathsf{A\text{-}INS}^{\mathcal{M}\times\mathcal{S}}_{n\to 1}$, and obtains[2] $(0, m, \sigma)$. It subsequently inputs i at interface

[2] Note that we are assuming (w.l.o.g.) that $\boldsymbol{\pi}$ always transmits m.

$\mathsf{A\text{-}INS}^{\mathcal{X}}_{n\to 1}$

$\mathfrak{S}, \mathfrak{R} \subseteq \mathbb{N} \times \mathcal{X}$
$c_S, c_R, t_S, t_R \in \mathbb{N}$
Initialize:
  $\mathfrak{S}, \mathfrak{R} \leftarrow \varnothing$
  $c_S, c_R \leftarrow 1$
  $t_S, t_R \leftarrow 0$
Interface $S_i(x \in \mathcal{X})$: // $i \in [n]$
  $t_S \leftarrow t_S + 1$
  $\mathfrak{S} \leftarrow \mathfrak{S} \cup \{(t_S, x)\}$
Interface $E(\diamond)$:
  $\mathfrak{O} \leftarrow \{(j, x) \in \mathfrak{S} \mid c_S \leq j \leq t_S\}$
  $c_S \leftarrow t_S + 1$
  return $\mathfrak{O}$
Interface $E(x \in \mathcal{X})$:
  $t_R \leftarrow t_R + 1$
  $\mathfrak{R} \leftarrow \mathfrak{R} \cup \{(t_R, x)\}$
Interface $R(\diamond)$:
  $\mathfrak{O} \leftarrow \{(j, x) \in \mathfrak{R} \mid c_R \leq j \leq t_R\}$
  $c_R \leftarrow t_R + 1$
  return $\mathfrak{O}$

Figure 4.3: Formal description of the *insecure anonymous channel* $\mathsf{A\text{-}INS}^{\mathcal{X}}_{n\to 1}$.

$\mathsf{A\text{-}AUT}^{\mathcal{X}}_{n\to 1}$

$\mathfrak{S}, \mathfrak{R} \subseteq (\mathbb{N} \times \mathcal{X} \times \mathbb{N}) \cup (\mathbb{N} \times \{\bot\}^2)$
$c_S, c_R, t_S, t_R \in \mathbb{N}$
Initialize:
  $\mathfrak{S}, \mathfrak{R} \leftarrow \varnothing$
  $c_S, c_R \leftarrow 1$
  $t_S, t_R \leftarrow 0$
Interface $S_i(x \in \mathcal{X})$: // $i \in [n]$
  $t_S \leftarrow t_S + 1$
  $\mathfrak{S} \leftarrow \mathfrak{S} \cup \{(t_S, x, i)\}$
Interface $E(\diamond)$:
  $\mathfrak{O} \leftarrow \{(j, x) \in \mathbb{N} \times \mathcal{X} \mid \exists\, i \in [n] : (j, x, i) \in \mathfrak{S},\ c_S \le j \le t_S\}$
  $c_S \leftarrow t_S + 1$
  return $\mathfrak{O}$
Interface $E(j \in \mathbb{N})$:
  if $\exists\, x \in \mathcal{X}, i \in [n] : (j, x, i) \in \mathfrak{S}$ **then**
    $t_R \leftarrow t_R + 1$
    $\mathfrak{R} \leftarrow \mathfrak{R} \cup \{(t_R, x, i)\}$
Interface $R(\diamond)$:
  $\mathfrak{O} \leftarrow \{(j, x, i) \in \mathfrak{R} \mid c_R \le j \le t_R\}$
  $c_R \leftarrow t_R + 1$
  return $\mathfrak{O}$

Figure 4.4: Formal description of the *anonymous authenticated channel* $\mathsf{A\text{-}AUT}^{\mathcal{X}}_{n\to 1}$.

$\mathsf{D\text{-}AUT}^{\mathcal{X}}_{n\to 1}$

$\mathfrak{S} \subseteq (\{\underline{\texttt{cmt}}\} \times \mathbb{N} \times \mathcal{X} \times [n] \times \mathbb{N}) \cup (\{\underline{\texttt{aut}}\} \times \mathbb{N}^2 \times \mathcal{X} \times [n])$
$\mathfrak{R} \subseteq (\{\underline{\texttt{cmt}}\} \times \mathbb{N} \times \mathcal{X}) \cup (\{\underline{\texttt{aut}}\} \times \mathbb{N}^2 \times [n])$; $\mathfrak{L} \subseteq \mathbb{N}^2$
$c_S, c_R, t_S, t_R, h_1, \ldots, h_n \in \mathbb{N}$
Initialize:
  $\mathfrak{S}, \mathfrak{R}, \mathfrak{L} \leftarrow \varnothing$; $c_S, c_R \leftarrow 1$; $t_S, t_R, h_1, \ldots, h_n \leftarrow 0$
Interface $S_i(\underline{\texttt{cmt}}, x \in \mathcal{X})$: // $i \in [n]$
  $t_S \leftarrow t_S + 1$; $h_i \leftarrow h_i + 1$; $\mathfrak{S} \leftarrow \mathfrak{S} \cup \{(\underline{\texttt{cmt}}, t_S, x, i, h_i)\}$
  return h_i
Interface $S_i(\underline{\texttt{aut}}, h \in \mathbb{N})$: // $i \in [n]$
  if $\exists j \in \mathbb{N}, x \in \mathcal{X} : (\underline{\texttt{cmt}}, j, x, i, h) \in \mathfrak{S}$ **then**
    $t_S \leftarrow t_S + 1$; $\mathfrak{S} \leftarrow \mathfrak{S} \cup \{(\underline{\texttt{aut}}, t_S, j, x, i)\}$
Interface $E(\diamond)$:
  $\mathfrak{O} \leftarrow \{(\underline{\texttt{cmt}}, j \in \mathbb{N}, x \in \mathcal{X}) \mid \exists i \in [n], h \in \mathbb{N} : (\underline{\texttt{cmt}}, j, x, i, h) \in \mathfrak{S},$
    $c_S \le j \le t_S\} \cup \{(\underline{\texttt{aut}}, j, j', x, i) \in \mathfrak{S} \mid c_S \le j \le t_S\}$
  $c_S \leftarrow t_S + 1$
  return $\mathfrak{O}$
Interface $E(j \in \mathbb{N})$:
  if $\exists x \in \mathcal{X}, i \in [n], h \in \mathbb{N} : (\underline{\texttt{cmt}}, j, x, i, h) \in \mathfrak{S}$ **then**
    $t_R \leftarrow t_R + 1$; $\mathfrak{R} \leftarrow \mathfrak{R} \cup \{(\underline{\texttt{cmt}}, t_R, x)\}$; $\mathfrak{L} \leftarrow \mathfrak{L} \cup \{(j, t_R)\}$
  else if $\exists j' \in \mathbb{N}, x \in \mathcal{X}, i \in [n] : (\underline{\texttt{aut}}, j, j', x, i) \in \mathfrak{S}$ **then**
    if $\exists j'' \in \mathbb{N} : (j', j'') \in \mathfrak{L}$ **then**
      $t_R \leftarrow t_R + 1$; $\mathfrak{R} \leftarrow \mathfrak{R} \cup \{(\underline{\texttt{aut}}, t_R, j'', i)\}$
Interface $E(\underline{\texttt{cmt}}, x \in \mathcal{X})$:
  $t_R \leftarrow t_R + 1$; $\mathfrak{R} \leftarrow \mathfrak{R} \cup \{(\underline{\texttt{cmt}}, t_R, x)\}$
Interface $R(\diamond)$:
  $\mathfrak{O} \leftarrow \{(\underline{\texttt{cmt}}, j, x), (\underline{\texttt{aut}}, j, j', i) \in \mathfrak{R} \mid c_R \le j \le t_R\}$; $c_R \leftarrow t_R + 1$
  return $\mathfrak{O}$

Figure 4.5: Formal description of the *de-anonymizable authenticated channel* $\mathsf{D\text{-}AUT}^{\mathcal{X}}_{n\to 1}$.

$\mathsf{RA\text{-}AUT}^{\mathcal{X}}_{n\to 1}$

$\mathfrak{S}, \mathfrak{R} \subseteq (\mathbb{N} \times \mathcal{X}) \cup (\mathbb{N} \times \{\perp\})$
$c_S, c_R, t_S, t_R \in \mathbb{N}$
Initialize:
  $\mathfrak{S}, \mathfrak{R} \leftarrow \varnothing$
  $c_S, c_R \leftarrow 1$
  $t_S, t_R \leftarrow 0$
Interface $S_i(x \in \mathcal{X})$: // $i \in [n]$
  $t_S \leftarrow t_S + 1$
  $\mathfrak{S} \leftarrow \mathfrak{S} \cup \{(t_S, x)\}$
Interface $E(\diamond)$:
  $\mathfrak{O} \leftarrow \{(j, x) \in \mathfrak{S} \mid c_S \leq j \leq t_S\}$
  $c_S \leftarrow t_S + 1$
  return $\mathfrak{O}$
Interface $E(j \in \mathbb{N})$:
  if $\exists\, x \in \mathcal{X} : (j, x) \in \mathfrak{S}$ **then**
    $t_R \leftarrow t_R + 1$
    $\mathfrak{R} \leftarrow \mathfrak{R} \cup \{(t_R, x)\}$
Interface $R(\diamond)$:
  $\mathfrak{O} \leftarrow \{(j, x) \in \mathfrak{S} \mid c_R \leq j \leq t_R\}$
  $c_R \leftarrow t_R + 1$
  return $\mathfrak{O}$

Figure 4.6: Formal description of the *receiver-side anonymous authenticated channel* $\mathsf{RA\text{-}AUT}^{\mathcal{X}}_{n\to 1}$.

E of (possibly emulated) $\mathsf{1\text{-}AUT}^{\mathcal{PK}}_{n\to 1}$, obtains (possibly emulated) public one-time authentic value pk_i, and then emulates the (fixed and publicly known) protocol $\boldsymbol{\pi}$ on input pk_i and (m, σ) at interface R. Finally, $\mathbf{D}$ outputs 0 if and only if it obtains (m, i) from its emulation. We now analyze two cases. First, assume that $\mathbf{D}$ is interacting with the real-world resource $\boldsymbol{\pi}\,[\mathsf{1\text{-}AUT}^{\mathcal{PK}}_{n\to 1}, \mathsf{A\text{-}INS}^{\mathcal{M}\times\mathcal{S}}_{n\to 1}]$. Then by the correctness of $\boldsymbol{\pi}$, $\mathbf{D}$ will obtain (m, i) with probability 1 from its emulation. On the other hand, if $\mathbf{D}$ is interacting with the ideal-resource $\boldsymbol{\sigma}\,\mathsf{A\text{-}AUT}^{\mathcal{M}}_{n\to 1}$ instead, then $\mathbf{D}$ will obtain (m, i) with probability at most $\frac{1}{n}$ from its emulation. This is because $\boldsymbol{\sigma}$ has no better choice than to actually emulate $\boldsymbol{\pi}$ as well, and choose at random one of the n public one-time authentic values from emulated $\mathsf{A\text{-}AUT}^{\mathcal{M}}_{n\to 1}$ to generate σ (since it does not obtain the index of the sender from $\mathsf{A\text{-}AUT}^{\mathcal{M}}_{n\to 1}$). Therefore, $\mathbf{D}$'s advantage is at least $1 - \frac{1}{n}$. □

4.3 Anonymous Authenticity

We start by introducing a new flavor of a signature scheme with some anonymity property, dubbed *bilateral signatures*. This scheme shares the syntax of designated verifier signatures (DVS): both sender and receiver have a key-pair; signing a message requires the secret key of the sender and the public key of the receiver, and verifying a signature requires the secret key of the receiver and the public key of the sender. The receiver's key-pair is essentially what allows to circumvent the impossibility result from Section 4.2.1, by introducing one-time authenticated information from the receiver to the senders: it enables indistinguishability of signatures by making verification exclusive to the receiver, as opposed to public.

Definition 4.3.1 (Bilateral Signature Scheme)**.** A *bilateral signature scheme (BSS)* $\Sigma_{\mathtt{BS}} \doteq (\mathtt{Gen}_S, \mathtt{Gen}_R, \mathtt{Sgn}, \mathtt{Vrf})$ over message-space $\mathcal{M}$ and signature-space $\mathcal{S}$ (with $\perp \notin \mathcal{M} \cup \mathcal{S}$), is such that

- $\mathtt{Gen}_S$ is a distribution over the sender key-spaces $\mathcal{SK}_S \times \mathcal{PK}_S$;
- $\mathtt{Gen}_R$ is a distribution over the receiver key-spaces $\mathcal{SK}_R \times \mathcal{PK}_R$;
- $\mathtt{Sgn} : \mathcal{SK}_S \times \mathcal{PK}_R \times \mathcal{M} \to \mathcal{S}$ is a probabilistic function;
- $\mathtt{Vrf} : \mathcal{SK}_R \times \mathcal{PK}_S \times \mathcal{M} \times \mathcal{S} \to \{0, 1\}$ is a deterministic function.

We require the above to be efficiently samplable/computable. For sender key-pair $(ssk, spk) \in \mathcal{SK}_S \times \mathcal{PK}_S$ and receiver key-pair $(rsk, rpk) \in \mathcal{SK}_R \times \mathcal{PK}_R$ we use the short-hand notation $\mathtt{Sgn}_{ssk,rpk}(\cdot)$ for $\mathtt{Sgn}(ssk, rpk, \cdot)$ and $\mathtt{Vrf}_{rsk,spk}(\cdot,\cdot)$ for $\mathtt{Vrf}(rsk, spk, \cdot, \cdot)$. Moreover, we assume *correctness* of Σ_{BS}, that is, for all key-pairs (ssk, spk) and (rsk, rpk) distributed according to $\mathtt{Gen}_S$ and $\mathtt{Gen}_R$, respectively, all messages $m \in \mathcal{M}$, and all signatures $\sigma \in \mathcal{S}$,

$$\mathtt{Vrf}_{rsk,spk}(m, \sigma) = \mathbb{1}\big\{\sigma \in \mathrm{supp}\,(\mathtt{Sgn}_{ssk,rpk}(m))\big\}.$$

Note that we only introduce bilateral signatures as an abstract syntactic object. As we discuss in Section 4.3.3, there exist concrete schemes satisfying such syntax, as well as the semantics we define later. Nevertheless, such schemes provide additional security guarantees that are not required in our setting. We leave the problem of finding a bilateral signature scheme which is *minimal*.

4.3.1 Game-Based Security of Bilateral Signatures

We begin our study of the semantics of bilateral signatures by defining their game-base security. In order to define the security of a fixed scheme Σ_{BS}, we define the following systems (where the dependency on Σ_{BS} is implicit), parameterized by keys $(ssk, spk) \in \mathcal{SK}_S \times \mathcal{PK}_S$, $\boldsymbol{spk} \doteq (spk_1, \ldots, spk_n) \in \mathcal{PK}_S^n$, for any $n \in \mathbb{N}$, and $(rsk, rpk) \in \mathcal{SK}_R \times \mathcal{PK}_R$.

- $\mathbf{S}_{ssk,rpk}$: On input $m \in \mathcal{M}$, get $\sigma \leftarrow \mathtt{Sgn}_{ssk,rpk}(m)$ and output σ.
- $\mathbf{V}_{rsk,spk}$: On input $(m, \sigma) \in \mathcal{M} \times \mathcal{S}$, get $b := \mathtt{Vrf}_{rsk,spk}(m, \sigma)$ and output b.
- $\rho^{\mathsf{uf}}(\mathbf{X}) \equiv [\![\mathbf{X}', \mathbf{Y}']\!]$, for some correlated systems $\mathbf{X}'$ and $\mathbf{Y}'$ that behave as follows: Initially set $\mathcal{Q} \subseteq \mathcal{M} \times \mathcal{S}$ to $\varnothing$, and then:
  - On input $m \in \mathcal{M}$ to $\mathbf{X}'$, forward m to $\mathbf{X}$, obtain $\sigma \in \mathcal{S}$, set $\mathcal{Q}$ to $\mathcal{Q} \cup \{(m, \sigma)\}$, and output σ.
  - On input $(m, \sigma) \in \mathcal{M} \times \mathcal{S}$ to $\mathbf{Y}'$, output 1 if $(m, \sigma) \in \mathcal{Q}$ and 0 otherwise.
- $\rho^{n\text{-}\mathsf{ik}}([\![\mathbf{X}, \mathbf{Y}]\!]) \equiv [\![[\![\mathbf{X}'_1, \mathbf{Y}'_1]\!], \ldots, [\![\mathbf{X}'_n, \mathbf{Y}'_n]\!]]\!]$, for some correlated systems $\mathbf{X}'_1, \mathbf{Y}'_1, \ldots, \mathbf{X}'_n, \mathbf{Y}'_n$ that behave as follows: Set $\mathcal{Q}_i \subseteq \mathcal{M} \times \mathcal{S}$ to $\varnothing$, for each $i \in [n]$, and then:

- On input $m \in \mathcal{M}$ to $\mathbf{X}'_i$, forward m to $\mathbf{X}$, obtain $\sigma \in \mathcal{S}$, set $\mathcal{Q}_i$ to $\mathcal{Q}_i \cup \{(m, \sigma)\}$, and output σ.
- On input $(m, \sigma) \in \mathcal{M} \times \mathcal{S}$ to $\mathbf{Y}'_i$, if $(m, \sigma) \in \mathcal{Q}_j$, for some $j \in [n] \setminus \{i\}$, output 0, otherwise forward (m, σ) to $\mathbf{Y}$, obtain $b \in \{0, 1\}$, and output b.

In our definitions, all keys will *always* be random variables distributed (as key-pairs) according to $\Sigma_{\mathtt{BS}}$'s $\mathtt{Gen}_S$ and $\mathtt{Gen}_R$.

We begin by defining authenticity of bilateral signatures. For this, we define a distinguishing problem between a real system that correctly generates and verifies signatures, via a signing oracle for one sender and a verification oracle for one receiver, and an ideal system that correctly generates signatures, but only correctly verifies signatures previously output by the signing oracle.

Definition 4.3.2 (uf-bs)**.**

$$[\![[\![\mathbf{S}_{ssk,rpk}, \mathbf{V}_{rsk,spk}]\!], spk, rpk]\!] \eqsim [\![\rho^{\mathsf{uf}}(\mathbf{S}_{ssk,rpk}), spk, rpk]\!],$$

for $(ssk, spk) \leftarrow \mathtt{Gen}_S$ and $(rsk, rpk) \leftarrow \mathtt{Gen}_R$.

Note that usually when authenticity is interpreted as unforgeability, as we do here, the related security notion is defined as a game where an adversary must first interact with a system implementing some oracles, and eventually attempt to come up with a concrete forgery. Nevertheless, defining unforgeability (hence, authenticity) through a distinguishing problem is not uncommon (see [Ros21] for example). The latter suits us better because it more directly relates to composable notions of security, and moreover it can be easily shown that it is implied by the former: as opposed to the real system, valid forgeries in the ideal system are falsely reported to be incorrect, thus trivially allowing to distinguish (see Section 2.3.4 for a more detailed discussion)

We next define anonymity of bilateral signatures. For this, we define a distinguishing problem between a real system that correctly generates and verifies signatures, via signing and verification oracles for n (different) senders and one receiver, and an ideal system that also correctly generates and verifies signatures, but via n copies of signing and verification oracles for the *same* sender and one receiver. The ideal system is also such that if a signature obtained from the i-th signing oracle is input to the j-th verification oracle, for $j \neq i$, then 0 is output.

Definition 4.3.3 (n-ik-bs)**.**

$$[\![[\![\mathbf{S}_{ssk_1,rpk}, \mathbf{V}_{rsk,spk_1}]\!], \ldots, [\![\mathbf{S}_{ssk_n,rpk}, \mathbf{V}_{rsk,spk_n}]\!], \boldsymbol{spk}, rpk]\!]$$
$$\eqsim$$
$$[\![\rho^{n\text{-ik}}([\![\mathbf{S}_{ssk_1,rpk}, \mathbf{V}_{rsk,spk_1}]\!]), \boldsymbol{spk}, rpk]\!],$$

for independent $(ssk_1, spk_1), \ldots, (ssk_n, spk_n) \leftarrow \mathtt{Gen}_S$, $(rsk, rpk) \leftarrow \mathtt{Gen}_R$, and $\boldsymbol{spk} \doteq (spk_1, \ldots, spk_n)$.

Finally, we define a combined notion for bilateral signatures capturing both authenticity and anonymity at once. For this, we define a distinguishing problem between a real system that correctly generates and verifies signatures, via signing and verification oracles for n (different) senders and one receiver, and an ideal system that also correctly generates signatures and only correctly verifies signatures previously signed, but via n copies of signing and verification oracles for the *same* sender and one receiver.

Definition 4.3.4 (n-ik-uf-bs)**.**

$$[\![[\![\mathbf{S}_{ssk_1,rpk}, \mathbf{V}_{rsk,spk_1}]\!], \ldots, [\![\mathbf{S}_{ssk_n,rpk}, \mathbf{V}_{rsk,spk_n}]\!], \boldsymbol{spk}, rpk]\!]$$
$$\eqsim$$
$$[\![\rho^{n\text{-ik}} \circ \rho^{\mathsf{uf}}(\mathbf{S}_{ssk_1,rpk}), \boldsymbol{spk}, rpk]\!]$$

for independent $(ssk_1, spk_1), \ldots, (ssk_n, spk_n) \leftarrow \mathtt{Gen}_S$, $(rsk, rpk) \leftarrow \mathtt{Gen}_R$, and $\boldsymbol{spk} \doteq (spk_1, \ldots, spk_n)$.

We now show that, as expected, uf-bs and n-ik-bs imply n-ik-uf-bs.

Lemma 4.3.5. (uf-bs, n-ik-bs) $\xrightarrow{1,1}$ n-ik-uf-bs.

Proof. Let $(ssk_1, spk_1), \ldots, (ssk_n, spk_n) \leftarrow \mathtt{Gen}_S$, $(rsk, rpk) \leftarrow \mathtt{Gen}_R$, $\boldsymbol{spk} \doteq (spk_1, \ldots, spk_n)$, and consider

$$\rho([\![\mathbf{X}, x, y]\!]) \doteq [\![\rho^{n\text{-ik}}(\mathbf{X}), \boldsymbol{spk}', y]\!],$$

where $\boldsymbol{spk}' \doteq (x, spk_2, \ldots, spk_n)$. Then:

$$\begin{aligned}
&[\![[\![\mathbf{S}_{ssk_1,rpk}, \mathbf{V}_{rsk,spk_1}]\!], \ldots, [\![\mathbf{S}_{ssk_n,rpk}, \mathbf{V}_{rsk,spk_n}]\!], \boldsymbol{spk}, rpk]\!] \\
&\quad \doteqdot [\![\rho^{n\text{-ik}}([\![\mathbf{S}_{ssk_1,rpk}, \mathbf{V}_{rsk,spk_1}]\!]), \boldsymbol{spk}, rpk]\!] && (n\text{-ik-bs}) \\
&\quad = \rho([\![[\![\mathbf{S}_{ssk_1,rpk}, \mathbf{V}_{rsk,spk_1}]\!], spk_1, rpk]\!]) \\
&\quad \doteqdot \rho([\![\rho^{\mathsf{uf}}(\mathbf{S}_{ssk_1,rpk}), spk_1, rpk]\!]) && (\mathsf{uf\text{-}bs}) \\
&\quad = [\![\rho^{n\text{-ik}} \circ \rho^{\mathsf{uf}}(\mathbf{S}_{ssk_1,rpk}), \boldsymbol{spk}, rpk]\!]. && \square
\end{aligned}$$

4.3.2 Composable Security of Bilateral Signatures

We continue our study of the semantics of bilateral signatures by defining their composable security in the constructive cryptography framework. Recall that we want to define composable security of a bilateral signature scheme Σ_{BS} as the construction of the resource $\mathsf{A\text{-}AUT}^{\mathcal{M}}_{n\to 1}$ from the resources $\mathsf{1\text{-}AUT}^{\mathcal{PK}_S}_{n\to 1}$, $\mathsf{1\text{-}AUT}^{\mathcal{PK}_R}_{n\leftarrow 1}$, and $\mathsf{A\text{-}INS}^{\mathcal{M}\times\mathcal{S}}_{n\to 1}$. In order to make this statement formal, we need to define how a protocol $\boldsymbol{\pi}_{\mathsf{BS}}$, attached to the resource $[\mathsf{1\text{-}AUT}^{\mathcal{PK}_S}_{n\to 1}, \mathsf{1\text{-}AUT}^{\mathcal{PK}_R}_{n\leftarrow 1}, \mathsf{A\text{-}INS}^{\mathcal{M}\times\mathcal{S}}_{n\to 1}]$, naturally makes use of Σ_{BS}. First, $\boldsymbol{\pi}_{\mathsf{BS}}$ runs $\mathtt{Gen}_S$ for every sender S_i, for $i \in [n]$, generating key-pairs $(ssk_1, spk_1), \ldots, (ssk_n, spk_n)$, as well as $\mathtt{Gen}_R$ for the receiver R, generating the key-pair (rsk, rpk). Then it transmits the sender public keys $spk_1, \ldots, spk_n$ to the receiver through $\mathsf{1\text{-}AUT}^{\mathcal{PK}_S}_{n\to 1}$ and the receiver public key rpk to each of the senders through $\mathsf{1\text{-}AUT}^{\mathcal{PK}_R}_{n\leftarrow 1}$. After that, once a sender S_i inputs a message m on its interface, $\boldsymbol{\pi}_{\mathsf{BS}}$ uses ssk_i and rpk to generate $\sigma \leftarrow \mathtt{Sgn}_{ssk_i,rpk}(m)$, and inputs (m, σ) to the interface S_i of $\mathsf{A\text{-}INS}^{\mathcal{M}\times\mathcal{S}}_{n\to 1}$. Once the receiver R inputs $\diamond$ on its interface, $\boldsymbol{\pi}_{\mathsf{BS}}$ also inputs $\diamond$ to the interface R of $\mathsf{A\text{-}INS}^{\mathcal{M}\times\mathcal{S}}_{n\to 1}$, obtaining a set $\mathfrak{O} \subseteq \mathbb{N} \times \mathcal{M} \times \mathcal{S}$, and outputs the set $\{(j, m, i) \mid \exists\,(j, m, \sigma) \in \mathfrak{O}, i \in [n] : \mathtt{Vrf}_{rsk,spk_i}(m, \sigma) = 1\}$ to R. We call $\boldsymbol{\pi}_{\mathsf{BS}}$ the protocol using Σ_{BS} in the *natural way*. We can now show that game-based security of bilateral signatures implies their composable security.

Theorem 4.3.6.

$$[\mathsf{1\text{-}AUT}^{\mathcal{PK}_S}_{n\to 1}, \mathsf{1\text{-}AUT}^{\mathcal{PK}_R}_{n\leftarrow 1}, \mathsf{A\text{-}INS}^{\mathcal{M}\times\mathcal{S}}_{n\to 1}] \xrightarrow{\boldsymbol{\pi}_{\mathsf{BS}};\, n\text{-ik-uf-bs}} \mathsf{A\text{-}AUT}^{\mathcal{M}}_{n\to 1}.$$

Proof. Let define systems

$$\mathbf{X} \doteq [\![[\![\mathbf{S}_{ssk_1,rpk}, \mathbf{V}_{rsk,spk_1}]\!], \ldots, [\![\mathbf{S}_{ssk_n,rpk}, \mathbf{V}_{rsk,spk_n}]\!], \boldsymbol{spk}, rpk]\!],$$
$$\mathbf{Y} \doteq [\![\rho^{n\text{-}\mathsf{ik}} \circ \rho^{\mathsf{uf}}(\mathbf{S}_{ssk_1,rpk}), \boldsymbol{spk}, rpk]\!],$$

for independent $(ssk_1, spk_1), \ldots, (ssk_n, spk_n) \leftarrow \mathtt{Gen}_S$ and $(rsk, rpk) \leftarrow \mathtt{Gen}_R$. We now need to provide a simulator $\boldsymbol{\sigma}$ and a transformation ρ such that

$$\rho(\mathbf{X}) \equiv \boldsymbol{\pi}_{\mathsf{BS}}\,[\mathsf{1\text{-}AUT}^{\mathcal{PK}_S}_{n\to 1}, \mathsf{1\text{-}AUT}^{\mathcal{PK}_R}_{n\leftarrow 1}, \mathsf{A\text{-}INS}^{\mathcal{M}\times\mathcal{S}}_{n\to 1}],$$
$$\rho(\mathbf{Y}) \equiv \boldsymbol{\sigma}\,\mathsf{A\text{-}AUT}^{\mathcal{M}}_{n\to 1}.$$

The simulator $\boldsymbol{\sigma}$ first sets $\mathcal{Q} \leftarrow \varnothing$. Then it generates n sender key-pairs $(ssk_1, spk_1), \ldots, (ssk_n, spk_n) \leftarrow \mathtt{Gen}_S$ as well as one receiver key-pair $(rsk, rpk) \leftarrow \mathtt{Gen}_R$, and on input $\diamond$ to the interfaces E emulating $\mathsf{1\text{-}AUT}^{\mathcal{PK}_S}_{n\to 1}$ and $\mathsf{1\text{-}AUT}^{\mathcal{PK}_R}_{n\leftarrow 1}$, $\boldsymbol{\sigma}$ outputs $\{(i, spk_i) \mid i \in [n]\}$ and rpk, respectively, at the same interface. Whenever $\diamond$ is input to the interfaces E emulating $\mathsf{A\text{-}INS}^{\mathcal{M}\times\mathcal{S}}_{n\to 1}$, $\boldsymbol{\sigma}$ also inputs $\diamond$ to the interface E of $\mathsf{A\text{-}AUT}^{\mathcal{M}}_{n\to 1}$, obtaining a set $\mathfrak{O} \subseteq \mathbb{N} \times \mathcal{M}$. It then outputs the set $\{(j, m, \mathtt{Sgn}_{ssk_1,rpk}(m)) \mid \exists\,(j, m) \in \mathfrak{O}\}$ to E, and sets $\mathcal{Q} \leftarrow \mathcal{Q} \cup \mathfrak{O}$. Whenever (m, σ) is input to the interface E emulating $\mathsf{A\text{-}INS}^{\mathcal{M}\times\mathcal{S}}_{n\to 1}$, if $(j, m, \sigma) \in \mathcal{Q}$ for some $j \in \mathbb{N}$, then $\boldsymbol{\sigma}$ inputs j to the E interface of $\mathsf{A\text{-}AUT}^{\mathcal{M}}_{n\to 1}$.

The transformation $\rho([\![[\![\mathbf{X}_1, \mathbf{Y}_1]\!], \ldots, [\![\mathbf{X}_n, \mathbf{Y}_n]\!], \boldsymbol{x}, y]\!])$ simply works by emulating $\boldsymbol{\pi}_{\mathsf{BS}}[\mathsf{1\text{-}AUT}^{\mathcal{PK}_S}_{n\to 1}, \mathsf{1\text{-}AUT}^{\mathcal{PK}_R}_{n\leftarrow 1}, \mathsf{A\text{-}INS}^{\mathcal{M}\times\mathcal{S}}_{n\to 1}]$, but replacing any calls to $\mathtt{Gen}_R, \mathtt{Gen}_S$ by the appropriate value from $\boldsymbol{x}, y$, any call to $\mathtt{Sgn}_{ssk_i,rpk}$ by a call to $\mathbf{X}_i$, and any call to $\mathtt{Vrf}_{rsk,spk_i}$ by a call to $\mathbf{Y}_i$. □

4.3.3 Relations with Previous Notions and Schemes

As we pointed out earlier, bilateral signatures share the same syntax of designated verifier signatures (DVS). This does not mean that, as a cryptographic scheme, they are the same. In fact, what matters are also the *semantics* of such scheme, that is, how its security is defined. On a high level, for DVS (game-based) security corresponds to being unable to tell whether a signature was produced by the sender or by the receiver, and therefore anonymity in not necessarily guaranteed among signatures generated by different senders. Instead, for bilateral signatures, the latter property is exactly what defines security, in terms of anonymity. Moreover,

the characterizing feature of DVS is irrelevant: For bilateral signatures, we do not want to (necessarily) hide the role of the sender, or respectively of the receiver; a bilateral signature scheme in principle allows an adversary to tell that the signature was generated by one of the senders, and in particular, *not* by the receiver, and therefore such a scheme would *not* be a secure DVS. Recently, in [MPR21] this characterizing feature of DVS that hides *both* the sender and the receivers has been modeled composably, where guarantees are provided not only to honest parties, but also to dishonest ones.

Nevertheless, in [JSI96], where DVS were originally introduced, the concept of *strong* DVS was mentioned, requiring a DVS scheme to additionally provide indistinguishably of signatures produced by different senders (the same property capturing anonymity of bilateral signatures). This notion was later formalized in [LV05], and it was shown how to enhance any DVS scheme to additionally satisfy this stronger notion, dubbed PSI-CMA-security. Clearly, such a DVS scheme would also be a bilateral signature scheme, albeit not *minimal*, in the sense that it would provide additional unnecessary security guarantees.

We now informally argue that the concrete scheme DVSBMH from [LV05] achieves our composable notion for bilateral signatures, that is, it constructs $\mathsf{A\text{-}AUT}^{\mathcal{M}}_{n\to 1}$ from $[\mathsf{1\text{-}AUT}^{\mathcal{PK}_S}_{n\to 1}, \mathsf{1\text{-}AUT}^{\mathcal{PK}_R}_{n\leftarrow 1}, \mathsf{A\text{-}INS}^{\mathcal{M}\times\mathcal{S}}_{n\to 1}]$ when used in the natural way. To do so, it suffices to relate the notions DVSBMH has been shown to satisfy to our game-based notions of uf-security and ik-security; then Lemma 4.3.5 implies that DVSBMH is also uf-ik-secure, and by Theorem 4.3.6 it is therefore also composably secure, as per Theorem 4.3.6. Note that, syntactically, DVSBMH is actually a *universal* DVS (UDVS) scheme, that is, a regular signature scheme equipped with additional functions emulating those of a DVS scheme. Therefore, using DVSBMH in the natural way means in particular to first produce a signature with the base signing function, and then feeding it along with the message and the receiver's public key to a further "designation" function, which will produce the final signature to be transmitted.

Unforgeability. In [LV05] DVSBMH has been shown to be st-dv-uf-secure, a notion introduced in [SWP04] which is a stronger version of the earlier notion of dv-uf-security from [SBWP03]. The former is stronger in the sense that, unlike the latter, it provides the attacker access to the verification oracle (in addition to a signing one), and therefore it

directly relates to our uf-security notion for bilateral signatures from Definition 4.3.2.

Anonymity. In [LV05] DVSBMH has been shown to be psi-cma-secure, a notion introduced there and that also relates to our counterpart for bilateral signatures, ik-security from Definition 4.3.3, but less directly. This is because psi-cma-security is essentially defined as key-indistinguishability of signatures, but only for *two* senders and one receiver, and therefore the ik-security of DVSBMH incurs a loss of multiplicative factor $(n-1)$, which can be shown via a standard hybrid argument.

4.4 De-Anonymizable Authenticity

In the previous section we studied a way to achieve the anonymous resource $\mathsf{A\text{-}AUT}^{\mathcal{X}}_{n\to 1}$, at the cost of assuming additional one-time authenticated information from the receiver to all senders. In this section we tackle what can be interpreted as the dual problem, that is, we study what can at most be achieved by only assuming one-time authenticated information from the receivers to the sender (in addition to an insecure channel). Considering to our impossibility result from Section 4.2.1, we know that the constructed resource will be necessarily weaker than $\mathsf{A\text{-}AUT}^{\mathcal{X}}_{n\to 1}$.

Considering the constraint on the assumed resources, intuitively we need a scheme that, on the sender side, requires the same input as regular signatures, that is, just a secret key and a message. But since anonymity is unachievable if both the message and the signature are disclosed, one either needs to relax the security definition of digital signatures, or to slightly change their syntax.

A first workaround to this impossibility was initially studied by Yang et al. [YWDW06], and subsequently refined independently by Fischlin [Fis07] and Zhang and Imai [ZI09], where the first approach is taken and essentially the anonymity of the signature alone is considered. Modeling such a security definition composably, makes it apparent how, from an application point of view, this approach is moot: it requires to assume that an adversary only sees signatures in transit, but not messages. Clearly, a different kind of assumed resources is needed; ideally, the message should be transmitted over a confidential channel. Composably, this hints to the fact that anonymous signatures might only be appropriate in a context where one wants to combine signatures with public-key encryption. This

can be interpreted as the study of anonymity preservation of signcryption, and we briefly discuss this in Section 4.6.

A different workaround, following the second approach, was independently taken later by Saraswat and Yun [SY09] and by Bellare and Duan [BD09]. There, the syntax of regular DSS was slightly modified to allow the signature to bear some form of anonymity. More precisely, the security definitions are changed to capture anonymity when the message and only a portion of the signature are disclosed, and authenticity only once the full signature is disclosed. We remark that the two works essentially introduce the same syntax and security notions, but [SY09] uses the term anonymous signatures introduced earlier in [YWDW06], whereas [BD09] adopts the new term *partial signatures*, which we will adopt here as well. More precisely, in such a scheme the signing function returns a signature that is defined as a tuple (σ, τ), where σ is called the *stub*, τ the *tag*, and (σ, τ) the *full signature*. Then the stub σ alone guarantees anonymity of the sender on a message m (but not its authenticity), whereas authenticity of m (but not anonymity anymore) is guaranteed once the tag τ is subsequently disclosed.

Definition 4.4.1 (Partial Signature Scheme)**.** A *partial signature scheme (PSS)* $\Sigma_{\mathsf{PS}} \doteq (\mathtt{Gen}, \mathtt{Sgn}, \mathtt{Vrf})$ over message-space $\mathcal{M}$, stub-space $\mathcal{S}$, and tag-space $\mathcal{T}$ (with $\perp \notin \mathcal{M} \cup \mathcal{S} \cup \mathcal{T}$), is such that

- $\mathtt{Gen}$ is a distribution over the key-spaces $\mathcal{SK} \times \mathcal{PK}$;
- $\mathtt{Sgn} : \mathcal{SK} \times \mathcal{M} \to \mathcal{S} \times \mathcal{T}$ is a probabilistic function;
- $\mathtt{Vrf} : \mathcal{PK} \times \mathcal{M} \times \mathcal{S} \times \mathcal{T} \to \{0, 1\}$ is a deterministic function.

We require the above to be efficiently samplable/computable. For key-pair $(sk, pk) \in \mathcal{SK} \times \mathcal{PK}$ we use the short-hand notation $\mathtt{Sgn}_{sk}(\cdot)$ for $\mathtt{Sgn}(sk, \cdot)$ and $\mathtt{Vrf}_{pk}(\cdot, \cdot, \cdot)$ for $\mathtt{Vrf}(pk, \cdot, \cdot, \cdot)$. Moreover, we assume *correctness* of Σ_{PS}, that is, for all key-pairs (sk, pk) distributed according to $\mathtt{Gen}$, all messages $m \in \mathcal{M}$, and all signatures $(\sigma, \tau) \in \mathcal{S} \times \mathcal{T}$,

$$\mathtt{Vrf}_{pk}(m, \sigma, \tau) = \mathbb{1}\{(\sigma, \tau) \in \mathrm{supp}\,(\mathtt{Sgn}_{sk}(m))\}.$$

4.4.1 Game-Based Security of Partial Signatures

We begin our study of the semantics of partial signatures by defining their game-base security. Originally, in [YWDW06] anonymous signatures (the

precursors of partial signatures), were only defined to be unforgeable and anonymous, by requiring that no adversary can forge valid signatures and distinguish signatures when messages are withheld, respectively. In [SY09] and [BD09], for the succeeding partial signatures, the unforgeability notion is essentially unchanged, whereas anonymity is defined with a game where the adversary sees only a part of the signatures, but also the whole associated messages. Additionally, both works realize that a crucial third security guarantee is also necessary: *unambiguouity* (named unpretendability in [SY09]). This notion ensures that only the original creator of a signature is able to later show that it indeed generated it. This security guarantee is modeled via a game where an adversary tries to come up with two messages m_0, m_1, a stub σ, and two tags τ_0, τ_1, such that $\mathtt{Vrf}_{pk_0}(m_0, \sigma, \tau_0) = \mathtt{Vrf}_{pk_1}(m_1, \sigma, \tau_1) = 1$, for two different public keys pk_0, pk_1, which in our setting must be two of the n known (and fixed) sender public keys. In Section 4.4.3 we relate those notions from the literature to the new definitions we introduce next.

In order to define the security of a fixed scheme Σ_{PS}, we define the following systems (where the dependency on Σ_{PS} is implicit), parameterized by keys $sk \in \mathcal{SK}$, $pk \in \mathcal{PK}$, $\boldsymbol{pk} \doteq (pk_1, \ldots, pk_n) \in \mathcal{PK}^n$, for any $n \in \mathbb{N}$.

- $\mathbf{S}_{sk}$: On input $m \in \mathcal{M}$, get $(\sigma, \tau) \leftarrow \mathtt{Sgn}_{sk}(m)$ and output (σ, τ).
- $\mathbf{S}^{-}_{sk}$: On input $m \in \mathcal{M}$, get $(\sigma, \tau) \leftarrow \mathtt{Sgn}_{sk}(m)$ and output σ.
- $\mathbf{V}_{pk}$: On input $(m, \sigma, \tau) \in \mathcal{M} \times \mathcal{S} \times \mathcal{T}$, get $b := \mathtt{Vrf}_{pk}(m, \sigma, \tau)$ and output b.
- $\rho^{\mathsf{uf}}(\mathbf{X}) \equiv [\![\mathbf{X}', \mathbf{Y}']\!]$, for some correlated systems $\mathbf{X}'$ and $\mathbf{Y}'$ that behave as follows: Initially set $\mathcal{Q} \subseteq \mathcal{M} \times \mathcal{S} \times \mathcal{T}$ to $\varnothing$, and then:
  - On input $m \in \mathcal{M}$ to $\mathbf{X}'$, forward m to $\mathbf{X}$, obtain (σ, τ), set $\mathcal{Q}$ to $\mathcal{Q} \cup \{(m, \sigma, \tau)\}$, and output (σ, τ).
  - On input $(m, \sigma, \tau) \in \mathcal{M} \times \mathcal{S} \times \mathcal{T}$ to $\mathbf{Y}'$, output 1 if $(m, \sigma, \tau) \in \mathcal{Q}$ and 0 otherwise.
- $\rho^{n\text{-}\mathsf{ua}}([\mathbf{X}_1, \ldots, \mathbf{X}_n]) \equiv [\![\mathbf{X}'_1, \ldots, \mathbf{X}'_n]\!]$, for some correlated systems $\mathbf{X}'_1, \ldots, \mathbf{X}'_n$ that behave as follows: Initially set $\mathcal{Q} \subseteq \mathcal{S}$ to $\varnothing$, and then:

  - On input $m \in \mathcal{M}$ to $\mathbf{X}'_i$, for $i \in [n]$, forward m to $\mathbf{X}_i$, obtain $\sigma \in \mathcal{S}$, and if $\sigma \in \mathcal{Q}$, output $\perp$, otherwise set $\mathcal{Q}$ to $\mathcal{Q} \cup \{\sigma\}$, and output σ.

- $\rho^{n\text{-ua-uf}}([\mathbf{X}_1, \ldots, \mathbf{X}_n]) \equiv [\![[\![\mathbf{X}'_1, \mathbf{Y}'_1]\!], \ldots, [\![\mathbf{X}'_n, \mathbf{Y}'_n]\!]]\!]$, for some correlated systems $\mathbf{X}'_1, \mathbf{Y}'_1, \ldots, \mathbf{X}'_n, \mathbf{Y}'_n$ that behave as follows: Initially set $\mathcal{Q} \subseteq \mathcal{S}$, $\mathcal{Q}_1, \ldots \mathcal{Q}_n \subseteq \mathcal{M} \times \mathcal{S} \times \mathcal{T}$ to $\varnothing$, and then:

  - On input $m \in \mathcal{M}$ to $\mathbf{X}'_i$, for $i \in [n]$, forward m to $\mathbf{X}_i$, obtain $(\sigma, \tau) \in \mathcal{S} \times \mathcal{T}$, and if $\sigma \in \mathcal{Q}$, output $\perp$, otherwise set $\mathcal{Q}$ to $\mathcal{Q} \cup \{\sigma\}$, $\mathcal{Q}_i$ to $\mathcal{Q}_i \cup \{(m, \sigma, \tau)\}$, and output σ.
  - On input $(m, \sigma, \tau) \in \mathcal{M} \times \mathcal{S} \times \mathcal{T}$ to $\mathbf{Y}'_i$, for $i \in [n]$, output 1 if $(m, \sigma, \tau) \in \mathcal{Q}_i$ and 0 otherwise.

In our definitions, all keys will *always* be random variables distributed (as key-pairs) according to Σ_{PS}'s $\mathtt{Gen}$.

We begin by defining authenticity of partial signatures. For this, we define a distinguishing problem between a real system that correctly generates and verifies signatures (stub-tag pairs) and an ideal system that correctly generates signatures, but only correctly verifies signatures previously output by the signing oracle.

Definition 4.4.2 (uf-ps)**.**

$$[\![[\![\mathbf{S}_{sk}, \mathbf{V}_{pk}]\!], \boldsymbol{pk}]\!] \eqsim [\![\rho^{\mathsf{uf}}(\mathbf{S}_{sk}), \boldsymbol{pk}]\!],$$

for $(sk, pk) \leftarrow \mathtt{Gen}$.

We next define unambiguity of partial signatures. For this, we define a distinguishing problem between a real system that correctly generates signatures via signing oracles for n (different) senders, and an ideal system that also correctly generates signatures for n (different) senders, but guarantees that the same stub is never output more than once.

Definition 4.4.3 (n-ua-ps)**.**

$$[\![\mathbf{S}_{sk_1}, \ldots, \mathbf{S}_{sk_n}, \boldsymbol{pk}]\!] \eqsim [\![\rho^{n\text{-ua}}([\mathbf{S}_{sk_1}, \ldots, \mathbf{S}_{sk_n}]), \boldsymbol{pk}]\!],$$

for independent $(sk_1, pk_1), \ldots, (sk_n, pk_n) \leftarrow \mathtt{Gen}$ and $\boldsymbol{pk} \doteq (pk_1, \ldots, pk_n)$.

We next define a combined notion for bilateral signatures capturing both authenticity and unambiguity at once. For this, we define a distinguishing problem between a real system that correctly generates and verifies signatures, via signing and verification oracles for n (different) senders, and an ideal system that also correctly generates signatures for n (different) senders, but only correctly verifies signatures previously generated by the corresponding signing oracle, and never repeats stubs.

Definition 4.4.4 (n-ua-uf-ps)**.**

$$[\![[\![\mathbf{S}_{sk_1}, \mathbf{V}_{pk_1}]\!], \ldots, [\![\mathbf{S}_{sk_n}, \mathbf{V}_{pk_n}]\!], \boldsymbol{pk}]\!] \eqsim [\![\rho^{n\text{-ua-uf}}([\mathbf{S}_{sk_1}, \ldots, \mathbf{S}_{sk_n}]), \boldsymbol{pk}]\!],$$

for independent $(sk_1, pk_1), \ldots, (sk_n, pk_n) \leftarrow \mathsf{Gen}$ and $\boldsymbol{pk} \doteq (pk_1, \ldots, pk_n)$.

We now show that, as expected, uf-ps and n-ua-ps imply n-ua-uf-ps.

Lemma 4.4.5. (uf-ps, n-ua-ps) $\xrightarrow{n,1}$ n-ua-uf-ps.

Proof. Let $(sk_1, pk_1), \ldots, (sk_n, pk_n) \leftarrow \mathsf{Gen}$, $\boldsymbol{pk} \doteq (pk_1, \ldots, pk_n)$, and consider

- $\rho_i([\![[\![\mathbf{X}, \mathbf{Y}]\!], x]\!]) \doteq [\![\rho^{\mathsf{uf}}(\mathbf{S}_{sk_1}), \ldots, \rho^{\mathsf{uf}}(\mathbf{S}_{sk_{i-1}}), [\![\mathbf{X}, \mathbf{Y}]\!],$
  $[\![\mathbf{S}_{sk_{i+1}}, \mathbf{V}_{pk_{i+1}}]\!], \ldots, [\![\mathbf{S}_{sk_n}, \mathbf{V}_{pk_n}]\!], \boldsymbol{pk}']\!]$, for any $i \in [n]$, where $\boldsymbol{pk}' \doteq (pk_1, \ldots, pk_{i-1}, x, pk_{i+1}, \ldots, pk_n)$, and
- $\rho([\![\mathbf{X}_1, \ldots, \mathbf{X}_n, \boldsymbol{x}]\!]) \doteq [\![\rho^{\mathsf{uf}}(\mathbf{X}_1), \ldots, \rho^{\mathsf{uf}}(\mathbf{X}_n), \boldsymbol{x}]\!]$.

Then, using Lemma 2.3.2:

$$\begin{aligned}
&[\![[\![\mathbf{S}_{sk_1}, \mathbf{V}_{pk_1}]\!], \ldots, [\![\mathbf{S}_{sk_n}, \mathbf{V}_{pk_n}]\!], \boldsymbol{pk}]\!] \\
&\quad \eqsim [\![\rho^{\mathsf{uf}}(\mathbf{S}_{sk_1}), \ldots, \rho^{\mathsf{uf}}(\mathbf{S}_{sk_n}), \boldsymbol{pk}]\!] && (n \text{ times uf-ps}) \\
&\quad = \rho([\![\mathbf{S}_{sk_1}, \ldots, \mathbf{S}_{sk_n}, \boldsymbol{pk}]\!]) \\
&\quad \eqsim \rho([\![\rho^{n\text{-ua}}([\mathbf{S}_{sk_1}, \ldots, \mathbf{S}_{sk_n}]), \boldsymbol{pk}]\!]) && (n\text{-ua-ps}) \\
&\quad \equiv [\![\rho^{n\text{-ua-uf}}([\mathbf{S}_{sk_1}, \ldots, \mathbf{S}_{sk_n}]), \boldsymbol{pk}]\!]. && \square
\end{aligned}$$

Finally, we define anonymity of partial signatures. For this, we define a distinguishing problem between a real system that correctly generates *only* stubs, via (reduced) signing oracles for n (different) senders, and an ideal system that also correctly generates only stubs, but via n copies of (reduced) signing oracles for the *same* sender.

Definition 4.4.6 (n-ik-ps)**.**

$$[\![\mathbf{S}^{-}_{sk_1}, \ldots, \mathbf{S}^{-}_{sk_n}, \boldsymbol{pk}]\!] \backsimeq [\![\mathbf{S}^{-}_{sk_1}, \ldots, \mathbf{S}^{-}_{sk_1}, \boldsymbol{pk}]\!]$$

for independent $(sk_1, pk_1), \ldots, (sk_n, pk_n) \leftarrow \mathtt{Gen}$ and $\boldsymbol{pk} \doteq (pk_1, \ldots, pk_n)$.

Unlike what we did for bilateral signatures (and will later do for ring signatures as well), it is not possible to define a combined security notion for partial signatures capturing both uf-ua-security and ik-security at once. This is because a unified distinguishing problem would necessarily require a full signing oracle, in order to model unforgeability, thus making it possible to trivially distinguish signatures generated by different senders, that is, making the modeling of anonymity impossible.

4.4.2 Composable Security of Partial Signatures

As it is made clear by the concrete construction given in [BD09], partial signature schemes inherently involve a special form of commitment. In fact, such straightforward construction from a regular signature scheme and a commitment scheme involves generating a normal signature on the message, and committing to it and the verification key. The resulting commitment bitstring will then be the stub σ (the one ensuring anonymity, but not authenticity), and the opening (or "decommital key") will correspond to the tag τ (the one ensuring authenticity, but not anonymity). More details are found in Section 4.4.3.

From this, it becomes immediately apparent that trying to capture security of partial signatures in a composable fashion, would necessarily incur the so-called *simulator commitment problem*. In this specific case, the issue is as follows: Intuitively, in the real world a sender S_i, for $i \in [n]$, generates a full signature (σ, τ) on a message m, and in a first phase sends only (m, σ) to the receiver R, while in a second phase it sends (m, σ, τ), which must satisfy $\mathtt{Vrf}_{pk_i}(m, \sigma, \tau) = 1$. But in the ideal world, during the first phase the simulator only receives the message m from $\mathsf{D\text{-}AUT}^{\mathcal{M}}_{n\to 1}$, and does not know who the sender is (in particular, it does not know the value $i \in [n]$). Even though it emulates all n secret/public keys sk_i, pk_i of the senders, it must output a partial signature σ by producing a full signature (σ, τ) for m using a *different* random secret key sk (this difference in the real and ideal worlds is what exactly captures anonymity of the stub σ). In the second phase, once it obtains the identity i of the

sender S_i who sent m, the simulator must be able to output, along with the previously defined stub σ, a valid tag τ that satisfies $\mathtt{Vrf}_{pk_i}(m, \sigma, \tau) = 1$. But because upon generation of σ from m, the simulator did not use sk_i, it is infeasible for it to correctly generate such a valid τ.

Recently, a generic workaround to this problem was put forth by Jost and Maurer [JM20], where the use of a new type of relaxation, the so-called *interval-wise relaxation*, allows to make formal statements capturing security notions that in regular composability frameworks would incur in the commitment problem. The interval-wise relaxation builds upon the combination of two other relaxations, the *from-relaxation* and the *until-relaxation*. Informally, given a resource RES and two monotone predicates P_1, P_2 (on the history of events happening globally[3] in an experiment involving RES), the from-relaxation $\mathsf{RES}^{[P_1}$ is the specification that consists of all resources behaving arbitrarily until P_2 is true and exactly as RES afterwards, whereas the until-relaxation $\mathsf{RES}^{P_2]}$ is the specification that consists of all resources behaving exactly as RES until P_1 is true and arbitrarily afterwards. The *from-until-relaxation* $\mathsf{RES}^{[P_1,P_2]}$ is then defined as the specification that consists of all resources behaving exactly as RES from when P_1 is true and until P_2 is true, and arbitrarily otherwise. Technically, the from-until-relaxation is actually defined as the transitive closure of applying the from-relaxation and until-relaxation in alternating order to RES, but can be shown to be equivalent to the specifications $((\mathsf{RES}^{[P_1}){}^{P_2]}){}^{[P_1}$ and $((\mathsf{RES}^{P_2]}){}^{[P_1}){}^{P_2]}$. Finally, lifting the original definition from [JM20] to our framework, for a substitution s, the interval-wise relaxation $\mathsf{RES}^{[P_1,P_2]:\mathsf{s}}$ corresponds to all resources in $\mathsf{RES}^{[P_1,P_2]}$ that are also s-close to RES. Formally, this is defined using the substitution-relaxation introduced in Section 4.1.4 as $\mathsf{RES}^{[P_1,P_2]:\mathsf{s}} \doteq ((\mathsf{RES}^{[P_1,P_2]})^{\mathsf{s}})^{[P_1,P_2]}$. Therefore, again understanding single resources as singleton sets, we can enhance the specification-based construction statement from equation (4.2) into

$$\boldsymbol{\pi}\,\mathsf{REAL} \subseteq \bigcap_{(P_1,P_2,\mathsf{s},\boldsymbol{\sigma})\in\Omega} (\boldsymbol{\sigma}\,\mathsf{IDEAL})^{[P_1,P_2]:\mathsf{s}},$$

for an appropriate set Ω. More precisely, each element $(P_1, P_2, \boldsymbol{\sigma}, \mathsf{s})$ describes a time-interval $[P_1, P_2]$ in which the resource $\boldsymbol{\pi}\,\mathsf{REAL}$ can be

[3] Such a predicate is monotone if once it is true for an event on such global events history, it stays true for all future events in the list of events representing the history.

abstracted as an elements s-close to IDEAL, with respect to the simulator $\boldsymbol{\sigma}$. As we showed in Theorem 2.4.4 for the resource-based construction statement used throughout this thesis, in [JM20] it is shown that indeed the interval-wise specification-based construction statement above satisfies composition.

Recall that we want to define composable security of a partial signature scheme Σ_{PS} as the construction of the resource $\mathsf{D\text{-}AUT}_{n\to 1}^{\mathcal{M}}$ from the resources $\mathsf{1\text{-}AUT}_{n\to 1}^{\mathcal{PK}}$, and $\mathsf{A\text{-}INS}_{n\to 1}^{\phi(\mathcal{M},\mathcal{S},\mathcal{T})}$, with

$$\phi(\mathcal{M},\mathcal{S},\mathcal{T}) \doteq (\{\underline{\mathtt{cmt}}\}\times\mathcal{M}\times\mathcal{S})\cup(\{\underline{\mathtt{aut}}\}\times\mathcal{M}\times\mathcal{S}\times\mathcal{T}).$$

In order to make this statement formal, we need to define how a protocol $\boldsymbol{\pi}_{\mathsf{PS}}$, attached to the resource $[\mathsf{1\text{-}AUT}_{n\to 1}^{\mathcal{PK}}, \mathsf{A\text{-}INS}_{n\to 1}^{\phi(\mathcal{M},\mathcal{S},\mathcal{T})}]$, naturally makes use of Σ_{PS}. First, $\boldsymbol{\pi}_{\mathsf{PS}}$ runs $\mathtt{Gen}$ for every sender S_i, for $i\in[n]$, generating key-pairs $(sk_1,pk_1),\ldots,(sk_n,pk_n)$. Then it transmits the public keys $pk_1,\ldots,pk_n$ to the receiver through $\mathsf{1\text{-}AUT}_{n\to 1}^{\mathcal{PK}}$. After that, for each sender S_i it sets up two look-up tables, modeled here as sets $\mathfrak{H}_i\subseteq\mathbb{N}\times\mathcal{M}\times\mathcal{S}\times\mathcal{T}$ and $\mathfrak{H}'_i\subseteq\mathbb{N}\times\mathcal{M}\times\mathcal{S}$, as well as a handle value $h_i\in\mathbb{N}$, initially set to 0. Then sender S_i might input messages of two different types on its interface:

- $(\underline{\mathtt{cmt}},m)$, for some $m\in\mathcal{M}$: in this case, $\boldsymbol{\pi}_{\mathsf{PS}}$ uses sk_i to generate $(\sigma,\tau)\leftarrow\mathtt{Sgn}_{sk_i}(m)$, and inputs $(\underline{\mathtt{cmt}},m,\sigma)$ to the interface S_i of $\mathsf{A\text{-}INS}_{n\to 1}^{\phi(\mathcal{M},\mathcal{S},\mathcal{T})}$. Then it sets $h_i\leftarrow h_i+1$ and $\mathfrak{H}_i\leftarrow\mathfrak{H}_i\cup\{(h_i,m,\sigma,\tau)\}$.
- $(\underline{\mathtt{aut}},h)$, for some $h\in\mathbb{N}$: in this case, $\boldsymbol{\pi}_{\mathsf{PS}}$ first checks whether $(h,m,\sigma,\tau)\in\mathfrak{H}_i$, for some m,σ,τ. If that is the case, then $\boldsymbol{\pi}_{\mathsf{PS}}$ inputs $(\underline{\mathtt{aut}},m,\sigma,\tau)$ to the interface S_i of $\mathsf{A\text{-}INS}_{n\to 1}^{\phi(\mathcal{M},\mathcal{S},\mathcal{T})}$.

Once the receiver R inputs $\diamond$ on its interface, $\boldsymbol{\pi}_{\mathsf{PS}}$ also inputs $\diamond$ to the interface R of $\mathsf{A\text{-}INS}_{n\to 1}^{\phi(\mathcal{M},\mathcal{S},\mathcal{T})}$, obtaining a set $\mathfrak{O}\subseteq(\mathbb{N}\times\{\underline{\mathtt{cmt}}\}\times\mathcal{M}\times\mathcal{S})\cup(\mathbb{N}\times\{\underline{\mathtt{aut}}\}\times\mathcal{M}\times\mathcal{S}\times\mathcal{T})$. Then it sets $\mathfrak{H}'\leftarrow\mathfrak{H}'\cup\{(j,m,\sigma)\,|\,(j,(\underline{\mathtt{cmt}},m,\sigma))\in\mathfrak{O}\}$, computes the sets $\mathfrak{O}'\doteq\{(\underline{\mathtt{cmt}},j,m)\,|\,\exists\,\sigma\in\mathcal{S}:(j,(\underline{\mathtt{cmt}},m,\sigma))\in\mathfrak{O}\}$, $\mathfrak{O}''\doteq\{(\underline{\mathtt{aut}},j',j,i)\,|\,\exists\,m\in\mathcal{M},\sigma\in\mathcal{S},\tau\in\mathcal{T}:(j',\underline{\mathtt{aut}},m,\sigma,\tau)\in\mathfrak{O},(j,m,\sigma)\in\mathfrak{H}',\mathtt{Vrf}_{pk_i}(m,\sigma,\tau)=1\}$, and outputs the set $\mathfrak{O}'\cup\mathfrak{O}''$ to R. We call $\boldsymbol{\pi}_{\mathsf{PS}}$ the protocol using Σ_{PS} in the *natural way*.

Intuitively, we model composable security of a partial signature scheme by making a statement for each interval defined by a sequence of inputs at

the sender interfaces $\{S_i\}_{i=1}^n$ that are of the same type, that is, either all are of the form $(\underline{\texttt{cmt}}, \cdot)$ (*messages*), or all are of the form $(\underline{\texttt{aut}}, \cdot)$ (*handles*). This way, we make sure that the individual security statement is within an interval in which the simulator cannot incur the commitment problem. For this we define the following predicates:

- $P_{\mathsf{msg}(j)}$: true if j-th sender input is a *message* m (E would obtain (m, σ));
- $P_{\mathsf{hnd}(j)}$: true if j-th sender input is a *handle* h (E would obtain (m, σ, τ));
- $P_{\mathsf{fst}(j)}$: true at *first* consecutive sender input of *same type as the j-th*;
- $P_{\mathsf{lst}(j)}$: true at *last* consecutive sender input of *same type as the j-th.*

ol using Σ_{PS} in the natural way.

Finally, we show that game-based security of partial signatures implies their composable security.

Theorem 4.4.7. *There exist (efficient) simulators $\boldsymbol{\sigma}_{\mathsf{m}}, \boldsymbol{\sigma}_{\mathsf{h}}$, such that*

$$\boldsymbol{\pi}_{\mathsf{PS}}\,[1\text{-}\mathsf{AUT}_{n\to 1}^{\mathcal{PK}}, \mathsf{A}\text{-}\mathsf{INS}_{n\to 1}^{\phi(\mathcal{M},\mathcal{S},\mathcal{T})}] \subseteq \bigcap_{(P_1,P_2,\mathsf{s},\boldsymbol{\sigma})\in\Omega} (\boldsymbol{\sigma}\ \mathsf{D}\text{-}\mathsf{AUT}_{n\to 1}^{\mathcal{M}})^{[P_1,P_2]:\mathsf{s}},$$

for

$$\begin{aligned}\Omega = &\{(P_{\mathsf{fst}(j)}, P_{\mathsf{lst}(j)}, n\text{-}\mathsf{ik}\text{-}\mathsf{ps}, \boldsymbol{\sigma}_{\mathsf{m}})\}_{j\in[t]:P_{\mathsf{msg}(j)}} \\ &\cup \{(P_{\mathsf{fst}(j)}, P_{\mathsf{lst}(j)}, n\text{-}\mathsf{ua}\text{-}\mathsf{uf}\text{-}\mathsf{ps}, \boldsymbol{\sigma}_{\mathsf{h}})\}_{j\in[t]:P_{\mathsf{hnd}(j)}},\end{aligned}$$

where $t \in \mathbb{N}$ is an upper-bound on the number of transmitted messages and $\boldsymbol{\pi}_{\mathsf{PS}}$ is the protocol using Σ_{PS} in the natural way.

Proof. Let $t \in \mathbb{N}$ and define systems

$$\begin{aligned}\mathbf{X}_{\mathsf{m}} &\doteq [\![\mathbf{S}_{sk_1}^-, \ldots, \mathbf{S}_{sk_n}^-, \boldsymbol{pk}]\!], \\ \mathbf{Y}_{\mathsf{m}} &\doteq [\![\underbrace{\mathbf{S}_{sk_1}^-, \ldots, \mathbf{S}_{sk_1}^-}_{n \text{ times}}, \boldsymbol{pk}]\!], \\ \mathbf{X}_{\mathsf{h}} &\doteq [\![[\![\mathbf{S}_{sk_1}, \mathbf{V}_{pk_1}]\!], \ldots, [\![\mathbf{S}_{sk_n}, \mathbf{V}_{pk_n}]\!], \boldsymbol{pk}]\!], \\ \mathbf{Y}_{\mathsf{h}} &\doteq [\![\rho^{n\text{-}\mathsf{ua}\text{-}\mathsf{uf}\text{-}\mathsf{ps}}([\mathbf{S}_{sk_1}, \ldots, \mathbf{S}_{sk_n}]), \boldsymbol{pk}]\!],\end{aligned}$$

for independent $(sk_1, pk_1), \ldots, (sk_n, pk_n) \leftarrow \mathtt{Gen}$, $\boldsymbol{pk} \doteq (pk_1, \ldots, pk_n)$, and random variable $I \xleftarrow{\$} [n]$. We now need to provide simulators $\boldsymbol{\sigma}_{\mathsf{h}}$, $\boldsymbol{\sigma}_{\mathsf{m}}$ and transformations ρ_{h}, ρ_{m} so that during interval $[P_{\mathsf{fst}(j)}, P_{\mathsf{lst}(j)}]$, for any $j \in [t]$ such that $P_{\mathsf{msg}(j)}$,

$$\rho_{\mathsf{m}}(\mathbf{X}_{\mathsf{m}}) \equiv \boldsymbol{\pi}_{\mathsf{PS}}\,[\mathsf{1\text{-}AUT}^{\mathcal{PK}}_{n\to 1}, \mathsf{A\text{-}INS}^{\phi(\mathcal{M},\mathcal{S},\mathcal{T})}_{n\to 1}],$$
$$\rho_{\mathsf{m}}(\mathbf{Y}_{\mathsf{m}}) \equiv \boldsymbol{\sigma}_{\mathsf{m}}\,\mathsf{D\text{-}AUT}^{\mathcal{M}}_{n\to 1},$$

and during interval $[P_{\mathsf{fst}(j)}, P_{\mathsf{lst}(j)}]$, for any $j \in [t]$ such that $P_{\mathsf{hnd}(j)}$,

$$\rho_{\mathsf{h}}(\mathbf{X}_{\mathsf{h}}) \equiv \boldsymbol{\pi}_{\mathsf{BS}}\,[\mathsf{1\text{-}AUT}^{\mathcal{PK}}_{n\to 1}, \mathsf{A\text{-}INS}^{\phi(\mathcal{M},\mathcal{S},\mathcal{T})}_{n\to 1}],$$
$$\rho_{\mathsf{h}}(\mathbf{Y}_{\mathsf{h}}) \equiv \boldsymbol{\sigma}_{\mathsf{h}}\,\mathsf{D\text{-}AUT}^{\mathcal{M}}_{n\to 1}.$$

For any $j \in [t]$ such that $P_{\mathsf{msg}(j)}$, the simulator $\boldsymbol{\sigma}_{\mathsf{m}}$ first generates n key-pairs $(sk_1, pk_1), \ldots, (sk_n, pk_n) \leftarrow \mathtt{Gen}$, and on input $\diamond$ to the interfaces E emulating $\mathsf{1\text{-}AUT}^{\mathcal{PK}}_{n\to 1}$, $\boldsymbol{\sigma}_{\mathsf{m}}$ outputs $\{(i, pk_i) \,|\, i \in [n]\}$ at the same interface. Whenever $\diamond$ is input to the interfaces E emulating $\mathsf{A\text{-}INS}^{\phi(\mathcal{M},\mathcal{S},\mathcal{T})}_{n\to 1}$, $\boldsymbol{\sigma}_{\mathsf{m}}$ also inputs $\diamond$ to the interface E of $\mathsf{D\text{-}AUT}^{\mathcal{M}}_{n\to 1}$, obtaining a set $\mathfrak{O} \subseteq \{\underline{\mathtt{cmt}}\} \times \mathbb{N} \times \mathcal{M}$.[4] It then outputs the set $\{(j, \underline{\mathtt{cmt}}, m, \sigma) \,|\, (\sigma, \cdot) \leftarrow \mathtt{Sgn}_{sk_I}(m), \exists\,(\underline{\mathtt{cmt}}, j, m) \in \mathfrak{O}\}$ to E. Whenever (m, σ) is input to the interface E emulating $\mathsf{A\text{-}INS}^{\phi(\mathcal{M},\mathcal{S},\mathcal{T})}_{n\to 1}$, $\boldsymbol{\sigma}_{\mathsf{m}}$ inputs $(\underline{\mathtt{cmt}}, m)$ to the E interface of $\mathsf{D\text{-}AUT}^{\mathcal{M}}_{n\to 1}$.

For any $j \in [t]$ such that $P_{\mathsf{msg}(j)}$, the transformation $\rho_{\mathsf{m}}(\llbracket \mathbf{X}_1, \ldots, \mathbf{X}_n, \boldsymbol{x} \rrbracket)$ simply works by emulating $\boldsymbol{\pi}_{\mathsf{PS}}[\mathsf{1\text{-}AUT}^{\mathcal{PK}}_{n\to 1}, \mathsf{A\text{-}INS}^{\phi(\mathcal{M},\mathcal{S},\mathcal{T})}_{n\to 1}]$ during interval $[P_{\mathsf{fst}(j)}, P_{\mathsf{lst}(j)}]$, but replacing any call to $\mathtt{Gen}$ by the appropriate value from $\boldsymbol{x}$, any call to $\mathtt{Sgn}_{sk_i}$ by a call to $\mathbf{X}_i$, and using x_i from $\boldsymbol{x} = (x_1, \ldots, x_n)$ as pk_i to implement $\mathtt{Vrf}_{pk_i}$.

For any $j \in [t]$ such that $P_{\mathsf{hnd}(j)}$, the simulator $\boldsymbol{\sigma}_{\mathsf{h}}$ first sets $\mathcal{Q} \leftarrow \varnothing$. Then it generates n key-pairs $(sk_1, pk_1), \ldots, (sk_n, pk_n) \leftarrow \mathtt{Gen}$, and on input $\diamond$ to the interfaces E emulating $\mathsf{1\text{-}AUT}^{\mathcal{PK}}_{n\to 1}$, $\boldsymbol{\sigma}_{\mathsf{h}}$ outputs $\{(i, pk_i) \,|\, i \in [n]\}$ at the same interface. Whenever $\diamond$ is input to the interfaces E emulating $\mathsf{A\text{-}INS}^{\phi(\mathcal{M},\mathcal{S},\mathcal{T})}_{n\to 1}$, $\boldsymbol{\sigma}_{\mathsf{h}}$ also inputs $\diamond$ to the interface E of $\mathsf{D\text{-}AUT}^{\mathcal{M}}_{n\to 1}$, obtaining a set $\mathfrak{O} \subseteq \{\underline{\mathtt{aut}}\} \times \mathbb{N}^2 \times \mathcal{M} \times [n]$.[5] It then outputs the set $\mathfrak{T} \doteq \{(j, \underline{\mathtt{aut}}, m, \mathtt{Sgn}_{sk_i}(m)) \,|\, \exists\,(\underline{\mathtt{aut}}, j, j', m, i) \in \mathfrak{O}\}$ to E, and sets $\mathcal{Q} \leftarrow$

[4] Recall that $\boldsymbol{\sigma}_{\mathsf{m}}$ is working in an interval $[P_{\mathsf{fst}(j)}, P_{\mathsf{lst}(j)}]$ for $j \in [t]$ such that $P_{\mathsf{msg}(j)}$.

[5] Recall that $\boldsymbol{\sigma}_{\mathsf{h}}$ is working in an interval $[P_{\mathsf{fst}(j)}, P_{\mathsf{lst}(j)}]$ for $j \in [t]$ such that $P_{\mathsf{hnd}(j)}$.

$\mathcal{Q} \cup \{(j, m, \sigma, \tau) \mid (j, \underline{\mathtt{aut}}, m, \sigma, \tau) \in \mathfrak{T}\}$. Whenever (m, σ, τ) is input to the interface E emulating $\mathsf{A\text{-}INS}_{n\to 1}^{\phi(\mathcal{M},\mathcal{S},\mathcal{T})}$, if $(j, m, \sigma, \tau) \in \mathcal{Q}$ for some $j \in \mathbb{N}$, then $\boldsymbol{\sigma}$ inputs j to the E interface of $\mathsf{D\text{-}AUT}_{n\to 1}^{\mathcal{M}}$.

For any $j \in [t]$ such that $P_{\mathsf{hnd}(j)}$, the transformation $\rho_{\mathsf{h}}(\llbracket\llbracket \mathbf{X}_1, \mathbf{Y}_1\rrbracket, \ldots, \llbracket \mathbf{X}_n, \mathbf{Y}_n\rrbracket, \boldsymbol{x}\rrbracket)$ simply works by emulating $\boldsymbol{\pi}_{\mathsf{PS}}[\mathsf{1\text{-}AUT}_{n\to 1}^{\mathcal{PK}}, \mathsf{A\text{-}INS}_{n\to 1}^{\phi(\mathcal{M},\mathcal{S},\mathcal{T})}]$ during interval $[P_{\mathsf{fst}(j)}, P_{\mathsf{lst}(j)}]$, but replacing any call to $\mathtt{Gen}$ by the appropriate value from $\boldsymbol{x}$, any call to $\mathtt{Sgn}_{sk_i}$ by a call to $\mathbf{X}_i$, and any call to $\mathtt{Vrf}_{pk_i}$ by a call to $\mathbf{Y}_i$. □

Remark. It is natural to ask whether regular signatures would also satisfy Theorem 4.4.7. This would correspond to asking whether a partial signature scheme with empty strings as stubs would still satisfy Theorem 4.4.7. The short answer is no, because it is easy to see that such a scheme does not necessarily achieve unambiguity. Nevertheless, we point out that in principle it should be possible to construct unambiguous regular signature schemes, but still we chose to use partial signatures instead because they offer more: If the adversary also publishes its public-key, then non-empty stubs and unambiguity ensure that it cannot falsely claim any message of the honest senders. This would follow trivially by appropriately extending our definitions, but it would not if a regular signature scheme was used instead. We leave the problem of formalizing this variant open for future work.

4.4.3 Relations with Previous Notions and Schemes

Our game-based definitions for partial signatures closely resemble the ones from the literature, except that we chose to phrase the notions as distinguishing problems, whereas [BD09] defines unforgeability and unambiguity as forgery problems and anonymity as a bit-guessing problem. [BD09] also introduces various constructions satisfying their definitions, one being the so-called StC (sign-then-commit) construction. This partial signature scheme is based on a regular signature scheme and a commitment scheme, and works as follows: to create a stub-tag pair (σ, τ) on a message m under secret-key sk (and corresponding public-key pk), the new signing function simply produces a regular signature s on m using the base signature scheme, then produces a commitment-decommitment pair (c, d) on the concatenation of s and pk, and finally sets $\sigma \doteq c$ and $\tau \doteq (s, d)$. Verification is then defined in the straightforward way.

We now informally argue that the simple StC construction[6] achieves our composable notion for bilateral signatures, that is, it constructs $\mathsf{D\text{-}AUT}^{\mathcal{M}}_{n\to 1}$ from $[\mathsf{1\text{-}AUT}^{\mathcal{PK}}_{n\to 1}, \mathsf{A\text{-}INS}^{\phi(\mathcal{M},\mathcal{S},\mathcal{T})}_{n\to 1}]$ when used in the natural way. To do so, it suffices to relate the notions StC has been shown to satisfy to our game-based notions of uf-security, ua-security, and ik-security; then Lemma 4.4.5 implies that StC is also uf-ua-secure, and by Theorem 4.4.7 it is therefore also composably secure, as per Theorem 4.4.7.

Unforgeability. In [BD09] StC has been shown to be unforgeable if the base signature scheme is unforgeable and the base commitment scheme is hiding. The unforgeability notion for partial signatures from [BD09] is slightly stronger than ours, in the sense that the signing oracle only returns stubs, and allows the adversary to later selectively see any associated tags. Such notion can be appropriately weakened, and then shown to be equivalent to our distinguishing problem from Definition 4.4.2, since being able to distinguish the two systems implies being able to find a valid forgery. Therefore, StC also satisfies our uf-security notion for partial signatures.

Unambiguity. In [BD09] StC has been shown to be unambiguous if the base commitment scheme is binding. The unambiguity notion for partial signatures from [BD09] is slightly stronger than ours, in the sense that the adversary can choose itself public keys, messages, stub and tags of the forgery. Such notion can be appropriately weakened, and then shown to be equivalent to our distinguishing problem from Definition 4.4.3, since being able to distinguish the two systems implies being able to find a valid forgery. In more detail, this is so because the two systems behave identically until the distinguisher manages to come up with a verification query (m', σ, τ') for the j-th verification oracle such that it previously queried the i-th signing oracle on m, for $i \neq j$, and obtained (σ, τ), and hence distinguishing between the two implies finding such a forgery. Therefore, StC also satisfies our ua-security notion for partial signatures.

Anonymity. In [BD09] StC has been shown to be anonymous if the base commitment scheme is hiding. The anonymity notion for partial signatures from [BD09] is slightly different than ours because it is only defined for two senders, and it is phrased as a bit-guessing problem. Nevertheless, it can be shown to be equivalent to our distinguishing problem from Definition 4.4.6,

[6] One could make analogous arguments for the other constructions from [BD09].

up to a multiplicative loss factor of $(n-1)$, via a standard hybrid argument. Therefore, StC also satisfies our ik-security notion for partial signatures.

4.5 Receiver-Side Anonymous Authenticity

One of the first alternative signature schemes providing some form of anonymity were *group signatures*, introduced by Chaum and Van Heyst [Cv91]. The main idea is that members of a group share a public verification key, which can be used to verify a message-signature pair generated by any of the group members using their own (different) secret keys. Anonymity is enforced by ensuring that the verification process does not reveal any partial information about the secret key used to generate the signature, hence effectively allowing a member to anonymously sign a message on behalf of the group. Technically, this is achieved by assigning the role of group manager to a selected member, which is responsible for generating all members' secret keys as well as the group's public verification key. Therefore, the group manager also has the ability to reveal the original signer.

This drawback of group signatures was later circumvented by Rivest, Shamir, and Tauman [RST01], who introduced *ring signature*. In this new scheme, a signature is generated by using not only the sender secret key, but also all the public keys of the group's members, called a ring in this context. Therefore, a signature must be transmitted along with the list of all public keys used, and anonymity is again enforced by requiring that the verification process does not reveal any partial information about the secret key used to generate the signature. Another advantage of ring signatures, compared to group signatures, is that the ring can be dynamically chosen by the sender, and does not require any cooperation.

The syntax of a ring signature scheme, for a fixed ring size of $n \in \mathbb{N}$, extends that of a regular DSS as follows: each sender generates its key-pair (sk_i, pk_i), for $i \in [n]$, but in order to generate a signature σ on a message m, in addition to sk_i, the list $\boldsymbol{pk} \doteq (pk_1, \ldots, pk_n)$ of all other senders public keys is needed. Moreover, also the index i itself is required by the signing function, in order to link the given secret key to the public key of the sender. Then, the receiver can verify that σ is a valid signature for m by using $\boldsymbol{pk}$, and be assured that the message was authentically transmitted by one of the known senders, and no external adversary.

Definition 4.5.1 (Ring Signature Scheme)**.** A *ring signature scheme (RSS)* $\Sigma_{\mathsf{RS}} \doteq (\mathtt{Gen}, \mathtt{Sgn}, \mathtt{Vrf})$ for $n \geq 2$ users over message-space $\mathcal{M}$ and signature-space $\mathcal{S}$ (with $\perp \notin \mathcal{M} \cup \mathcal{S}$), is such that

- $\mathtt{Gen}$ is a distribution over the key-space $\mathcal{SK} \times \mathcal{PK}$;
- $\mathtt{Sgn} : [n] \times \mathcal{SK} \times \mathcal{PK}^n \times \mathcal{M} \to \mathcal{S}$ is a probabilistic function;
- $\mathtt{Vrf} : \mathcal{PK}^n \times \mathcal{M} \times \mathcal{S} \to \{0,1\}$ is a deterministic function.

We require the above to be efficiently samplable/computable. For index $i \in [n]$ and keys $sk \in \mathcal{SK}$, $\boldsymbol{pk} \doteq (pk_1, \ldots, pk_n) \in \mathcal{PK}^n$, for any $n \in \mathbb{N}$, we use the short-hand notation $\mathtt{Sgn}_{i,sk,\boldsymbol{pk}}(\cdot)$ for $\mathtt{Sgn}(i, sk, \boldsymbol{pk}, \cdot)$ and $\mathtt{Vrf}_{\boldsymbol{pk}}(\cdot,\cdot)$ for $\mathtt{Vrf}(\boldsymbol{pk}, \cdot, \cdot)$. Moreover, we assume *correctness* of Σ_{RS}, that is, for all $n \geq 2$, all $i \in [n]$, all possible lists of n key-pairs $(sk_1, pk_1), \ldots, (sk_n, pk_n)$ distributed according to $\mathtt{Gen}$, with $\boldsymbol{pk} \doteq (pk_1, \ldots, pk_n)$, all messages $m \in \mathcal{M}$, and all signatures $\sigma \in \mathcal{S}$,

$$\mathtt{Vrf}_{\boldsymbol{pk}}(m, \sigma) = \mathbb{1}\left\{\sigma \in \bigcup_{i=1}^{n} \operatorname{supp}\left(\mathtt{Sgn}_{i,sk_i,\boldsymbol{pk}}(m)\right)\right\}.$$

4.5.1 Game-Based Security of Ring Signatures

When ring signatures were introduced in [RST01], no formal game-based security definitions were given, this was only done later in [BKM06]. There, a stronger model than the one considered here was introduced, namely one where the adversary can generate and publish its own public key, which, as discussed in Section 4.2, would require a certificate authority. Therefore, here we use adapted versions of the weaker security notions of *unforgeability against fixed-ring attacks* and *basic anonymity* from [BKM06]. In Section 4.5.3 we relate those notions from the literature to the new combined definition we introduce next.

In order to define the security of a fixed scheme Σ_{RS}, we define the following systems (where the dependency on Σ_{RS} is implicit), parameterized by index $i \in [n]$ and keys $sk \in \mathcal{SK}$, $\boldsymbol{sk} \doteq (sk_1, \ldots, sk_n) \in \mathcal{SK}^n$, $\boldsymbol{pk} \doteq (pk_1, \ldots, pk_n) \in \mathcal{PK}^n$, for any $n \in \mathbb{N}$.

- $\mathbf{S}_{\boldsymbol{sk},\boldsymbol{pk}}$: On input $(i, m) \in [n] \times \mathcal{M}$, get $\sigma \leftarrow \mathtt{Sgn}_{i,sk_i,\boldsymbol{pk}}(m)$ and output σ.

- $\mathbf{S}_{i,sk,\boldsymbol{pk}}$: On input $m \in \mathcal{M}$, get $\sigma \leftarrow \mathtt{Sgn}_{i,sk,\boldsymbol{pk}}(m)$ and output σ.
- $\mathbf{V}_{\boldsymbol{pk}}$: On input $(m, \sigma) \in \mathcal{M} \times \mathcal{S}$, get $b := \mathtt{Vrf}_{\boldsymbol{pk}}(m, \sigma)$ and output b.
- $\rho^{n\text{-}\mathsf{uf}}(\mathbf{X}) \equiv [\![\mathbf{X}', \mathbf{Y}']\!]$, for some correlated systems $\mathbf{X}'$ and $\mathbf{Y}'$ that behave as follows: Initially set $\mathcal{Q} \subseteq \mathcal{M} \times \mathcal{S}$ to $\varnothing$, and then:
  - On input $(i, m) \in [n] \times \mathcal{M}$ to $\mathbf{X}'$, forward m to $\mathbf{X}$, obtain $\sigma \in \mathcal{S}$, set $\mathcal{Q}$ to $\mathcal{Q} \cup \{(m, \sigma)\}$, and output σ.
  - On input $(m, \sigma) \in \mathcal{M} \times \mathcal{S}$ to $\mathbf{Y}'$, output 1 if $(m, \sigma) \in \mathcal{Q}$ and 0 otherwise.
- $\rho^{\mathsf{uf}}(\mathbf{X}) \equiv [\![\mathbf{X}', \mathbf{Y}']\!]$, for some correlated systems $\mathbf{X}'$ and $\mathbf{Y}'$ that behave as follows: Initially set $\mathcal{Q} \subseteq \mathcal{M} \times \mathcal{S}$ to $\varnothing$, and then:
  - On input $m \in \mathcal{M}$ to $\mathbf{X}'$, forward m to $\mathbf{X}$, obtain $\sigma \in \mathcal{S}$, set $\mathcal{Q}$ to $\mathcal{Q} \cup \{(m, \sigma)\}$, and output σ.
  - On input $(m, \sigma) \in \mathcal{M} \times \mathcal{S}$ to $\mathbf{Y}'$, output 1 if $(m, \sigma) \in \mathcal{Q}$ and 0 otherwise.
- $\rho^{n\text{-}\mathsf{ik}}([\![\mathbf{X}, \mathbf{Y}]\!]) \equiv [\![[\![\mathbf{X}'_1, \mathbf{Y}'_1]\!], \ldots, [\![\mathbf{X}'_n, \mathbf{Y}'_n]\!]]\!]$, for some correlated systems $\mathbf{X}'_1, \mathbf{Y}'_1, \ldots, \mathbf{X}'_n, \mathbf{Y}'_n$ that behave as follows: Set $\mathcal{Q}_i \subseteq \mathcal{M} \times \mathcal{S}$ to $\varnothing$, for each $i \in [n]$, and then:
  - On input $m \in \mathcal{M}$ to $\mathbf{X}'_i$, forward m to $\mathbf{X}$, obtain $\sigma \in \mathcal{S}$, set $\mathcal{Q}_i$ to $\mathcal{Q}_i \cup \{(m, \sigma)\}$, and output σ.
  - On input $(m, \sigma) \in \mathcal{M} \times \mathcal{S}$ to $\mathbf{Y}'_i$, if $(m, \sigma) \in \mathcal{Q}_j$, for some $j \in [n] \setminus \{i\}$, output 0, otherwise forward (m, σ) to $\mathbf{Y}$, obtain $b \in \{0, 1\}$, and output b.

In our definitions, all keys will *always* be random variables distributed (as key-pairs) according to Σ_{RS}'s `Gen`.

We begin by defining authenticity of ring signatures. For this, define a distinguishing problem between a real system that correctly generates and verifies signatures, via a signing oracle for one sender and a verification oracle for one receiver, and an ideal system that correctly generates signatures, but only correctly verifies signatures previously output by the signing oracle.

Definition 4.5.2 (uf-rs)**.**

$$[\![[\![\mathbf{S}_{\boldsymbol{sk},\boldsymbol{pk}}, \mathbf{V}_{\boldsymbol{pk}}]\!], \boldsymbol{pk}]\!] \eqsim [\![\rho^{n\text{-}\mathsf{uf}}(\mathbf{S}_{\boldsymbol{sk},\boldsymbol{pk}}), \boldsymbol{pk}]\!],$$

for independent $(sk_1, pk_1), \ldots, (sk_n, pk_n) \leftarrow \mathtt{Gen}$, $\boldsymbol{sk} \doteq (sk_1, \ldots, sk_n)$, and $\boldsymbol{pk} \doteq (pk_1, \ldots, pk_n)$.

We next define anonymity of ring signatures. For this, we define a distinguishing problem between a real system that correctly generates and verifies signatures, via signing and verification oracles for n (different) senders, and an ideal system that also correctly generates and verifies signatures, but via n copies of signing and verification oracles for the *same* sender. The ideal system is also such that if a signature obtained from the i-th signing oracle is input to the j-th verification oracle, for $j \neq i$, then 0 is output.

Definition 4.5.3 (ik-rs)**.**

$$[\![[\![\mathbf{S}_{1,sk_1,\boldsymbol{pk}}, \mathbf{V}_{\boldsymbol{pk}}]\!], \ldots, [\![\mathbf{S}_{n,sk_n,\boldsymbol{pk}}, \mathbf{V}_{\boldsymbol{pk}}]\!], \boldsymbol{pk}]\!]$$
$$\eqsim$$
$$[\![\rho^{n\text{-}\mathsf{ik}}([\![\mathbf{S}_{1,sk_1,\boldsymbol{pk}}, \mathbf{V}_{\boldsymbol{pk}}]\!]), \boldsymbol{pk}]\!],$$

for independent $(sk_1, pk_1), \ldots, (sk_n, pk_n) \leftarrow \mathtt{Gen}$ and $\boldsymbol{pk} \doteq (pk_1, \ldots, pk_n)$.

Finally, we define a combined notion for ring signatures capturing both authenticity and anonymity at once. For this, we define a distinguishing problem between a real system that correctly generates and verifies signatures, via signing and verification oracles for n (different) senders, and an ideal system that also correctly generates signatures and only correctly verifies signatures previously signed, but via n copies of signing and verification oracles for the *same* sender.

Definition 4.5.4 (ik-uf-rs)**.**

$$[\![[\![\mathbf{S}_{1,sk_1,\boldsymbol{pk}}, \mathbf{V}_{\boldsymbol{pk}}]\!], \ldots, [\![\mathbf{S}_{n,sk_n,\boldsymbol{pk}}, \mathbf{V}_{\boldsymbol{pk}}]\!], \boldsymbol{pk}]\!]$$
$$\eqsim$$
$$[\![\rho^{n\text{-}\mathsf{ik}} \circ \rho^{\mathsf{uf}}(\mathbf{S}_{1,sk_1,\boldsymbol{pk}}), \boldsymbol{pk}]\!],$$

for independent $(sk_1, pk_1), \ldots, (sk_n, pk_n) \leftarrow \mathtt{Gen}$ and $\boldsymbol{pk} \doteq (pk_1, \ldots, pk_n)$.

We now show that, as expected, uf-rs and n-ik-rs imply n-ik-uf-rs.

Lemma 4.5.5. $(\mathsf{uf\text{-}rs}, n\text{-}\mathsf{ik\text{-}rs}) \xrightarrow{1,1} n\text{-}\mathsf{ik\text{-}uf\text{-}rs}$.

Proof. Let $(sk_1, pk_1), \ldots, (sk_n, pk_n) \leftarrow \mathtt{Gen}$, $\boldsymbol{sk} \doteq (sk_1, \ldots, sk_n)$, $\boldsymbol{pk} \doteq (pk_1, \ldots, pk_n)$, and consider

- $\rho_1([\![\mathbf{X}, \mathbf{Y}]\!]) \equiv [\![\mathbf{X}', \mathbf{Y}']\!]$, for some correlated systems $\mathbf{X}'$ and $\mathbf{Y}'$ that behave as follows:
  - On input $m \in \mathcal{M}$ to $\mathbf{X}'$, forward $(1, m)$ to $\mathbf{X}$, obtain $\sigma \in \mathcal{S}$, and output σ.
  - On input $(m, \sigma) \in \mathcal{M} \times \mathcal{S}$ to $\mathbf{Y}'$, forward (m, σ) to $\mathbf{Y}$, obtain $b \in \{0, 1\}$, and output b.
- $\rho_2([\![\mathbf{X}, \boldsymbol{x}]\!]) \doteq [\![\rho^{n\text{-}\mathsf{ik}} \circ \rho_1(\mathbf{X}), \boldsymbol{x}]\!]$.

Then:

$$
\begin{aligned}
&[\![[\![\mathbf{S}_{1,sk_1,\boldsymbol{pk}}, \mathbf{V}_{\boldsymbol{pk}}]\!], \ldots, [\![\mathbf{S}_{n,sk_n,\boldsymbol{pk}}, \mathbf{V}_{\boldsymbol{pk}}]\!], \boldsymbol{pk}]\!] \\
&\quad \doteqdot [\![\rho^{n\text{-}\mathsf{ik}}([\![\mathbf{S}_{1,sk_1,\boldsymbol{pk}}, \mathbf{V}_{\boldsymbol{pk}}]\!]), \boldsymbol{pk}]\!] && (n\text{-}\mathsf{ik\text{-}rs}) \\
&\quad \equiv [\![\rho^{n\text{-}\mathsf{ik}} \circ \rho_1([\![\mathbf{S}_{\boldsymbol{sk},\boldsymbol{pk}}, \mathbf{V}_{\boldsymbol{pk}}]\!]), \boldsymbol{pk}]\!] \\
&\quad = \rho_2([\![[\![\mathbf{S}_{\boldsymbol{sk},\boldsymbol{pk}}, \mathbf{V}_{\boldsymbol{pk}}]\!], \boldsymbol{pk}]\!]) \\
&\quad \doteqdot \rho_2([\![\rho^{n\text{-}\mathsf{uf}}(\mathbf{S}_{\boldsymbol{sk},\boldsymbol{pk}}), \boldsymbol{pk}]\!]) && (\mathsf{uf\text{-}rs}) \\
&\quad = [\![\rho^{n\text{-}\mathsf{ik}} \circ \rho_1 \circ \rho^{n\text{-}\mathsf{uf}}(\mathbf{S}_{\boldsymbol{sk},\boldsymbol{pk}}), \boldsymbol{pk}]\!] \\
&\quad \equiv [\![\rho^{n\text{-}\mathsf{ik}} \circ \rho^{\mathsf{uf}}(\mathbf{S}_{1,sk_1,\boldsymbol{pk}}), \boldsymbol{pk}]\!]. && \square
\end{aligned}
$$

4.5.2 Composable Security of Ring Signatures

We continue our study of the semantics of ring signatures by defining their composable security in the constructive cryptography framework. Composable security notions for ring signatures have been previously studied in [YO07] within the universal composability (UC) framework. There, an ideal functionality was introduced, and it was shown to be securely realized by a protocol employing ring signatures. Unlike with our approach, such functionality was completely tailored to the ring signature scheme used by the protocol, that is, it exported operations such as

signing and verifying, it did not model a communication channel between senders and receiver. Here we define an ideal resource, independent of any cryptographic scheme, and show that (among other possible ones), a protocol employing ring signatures indeed realizes such a resource.

Recall that we want to define composable security of a ring signature scheme Σ_{RS} as the construction of the resource $\mathsf{RA\text{-}AUT}^{\mathcal{M}}_{n\to 1}$ from the resources $\mathsf{1\text{-}AUT}^{\mathcal{PK}}_{n\bigcirc 1}$ and $\mathsf{A\text{-}INS}^{\mathcal{M}\times\mathcal{S}}_{n\to 1}$. In order to make this statement formal, we need to define how a protocol $\boldsymbol{\pi}_{\mathsf{RS}}$, attached to the resource $[\mathsf{1\text{-}AUT}^{\mathcal{PK}}_{n\bigcirc 1}, \mathsf{A\text{-}INS}^{\mathcal{M}\times\mathcal{S}}_{n\to 1}]$, naturally makes use of Σ_{RS}. First, $\boldsymbol{\pi}_{\mathsf{RS}}$ runs $\mathtt{Gen}$ for every sender S_i, for $i \in [n]$, generating key-pairs $(sk_1, pk_1), \ldots, (sk_n, pk_n)$. Then it transmits the public keys $\boldsymbol{pk} \doteq (pk_1, \ldots, pk_n)$ to the receiver and all senders through $\mathsf{1\text{-}AUT}^{\mathcal{PK}}_{n\bigcirc 1}$. After that, once a sender S_i inputs a message m on its interface, $\boldsymbol{\pi}_{\mathsf{RS}}$ uses sk_i and $\boldsymbol{pk}$ to generate $\sigma \leftarrow \mathtt{Sgn}_{i,sk_i,\boldsymbol{pk}}(m)$, and inputs (m, σ) to the interface S_i of $\mathsf{A\text{-}INS}^{\mathcal{M}\times\mathcal{S}}_{n\to 1}$. Once the receiver R inputs $\diamond$ on its interface, $\boldsymbol{\pi}_{\mathsf{RS}}$ also inputs $\diamond$ to the interface R of $\mathsf{A\text{-}INS}^{\mathcal{M}\times\mathcal{S}}_{n\to 1}$, obtaining a set $\mathfrak{O} \subseteq \mathbb{N} \times \mathcal{M} \times \mathcal{S}$, and outputs the set $\{(j, m) \mid \exists\, (j, m, \sigma) \in \mathfrak{O} : \mathtt{Vrf}_{\boldsymbol{pk}}(m, \sigma) = 1\}$ to R. We call $\boldsymbol{\pi}_{\mathsf{RS}}$ the protocol using Σ_{RS} in the *natural way*. We can now show that game-based security of ring signatures implies their composable security.

Theorem 4.5.6. $[\mathsf{1\text{-}AUT}^{\mathcal{PK}}_{n\bigcirc 1}, \mathsf{A\text{-}INS}^{\mathcal{M}\times\mathcal{S}}_{n\to 1}] \xrightarrow{\boldsymbol{\pi}_{\mathsf{RS}};\, n\text{-}\mathsf{ik\text{-}uf\text{-}rs}} \mathsf{RA\text{-}AUT}^{\mathcal{M}}_{n\to 1}$.

Proof. Let define systems

$$\mathbf{X} \doteq [\![[\![\mathbf{S}_{1,sk_1,\boldsymbol{pk}}, \mathbf{V}_{\boldsymbol{pk}}]\!], \ldots, [\![\mathbf{S}_{n,sk_n,\boldsymbol{pk}}, \mathbf{V}_{\boldsymbol{pk}}]\!], \boldsymbol{pk}]\!],$$
$$\mathbf{Y} \doteq [\![\rho^{n\text{-}\mathsf{ik}} \circ \rho^{\mathsf{uf}}(\mathbf{S}_{1,sk_1,\boldsymbol{pk}}), \boldsymbol{pk}]\!],$$

for independent $(sk_1, pk_1), \ldots, (sk_n, pk_n) \leftarrow \mathtt{Gen}$ and $\boldsymbol{pk} \doteq (pk_1, \ldots, pk_n)$. We now need to provide a simulator $\boldsymbol{\sigma}$ and a transformation ρ such that

$$\rho(\mathbf{X}) \equiv \boldsymbol{\pi}_{\mathsf{RS}}\, [\mathsf{1\text{-}AUT}^{\mathcal{PK}}_{n\bigcirc 1}, \mathsf{A\text{-}INS}^{\mathcal{M}\times\mathcal{S}}_{n\to 1}],$$
$$\rho(\mathbf{Y}) \equiv \boldsymbol{\sigma}\, \mathsf{RA\text{-}AUT}^{\mathcal{M}}_{n\to 1}.$$

The simulator $\boldsymbol{\sigma}$ first sets $\mathcal{Q} \leftarrow \varnothing$. Then it generates n key-pairs $(sk_1, pk_1), \ldots, (sk_n, pk_n) \leftarrow \mathtt{Gen}$, sets $\boldsymbol{pk} \doteq (pk_1, \ldots, pk_n)$, and on input $\diamond$ to the interfaces E emulating $\mathsf{1\text{-}AUT}^{\mathcal{PK}}_{n\bigcirc 1}$, $\boldsymbol{\sigma}$ outputs $\{(i, pk_i) \mid i \in [n]\}$ at the same interface. Whenever $\diamond$ is input to the interfaces E emulating $\mathsf{A\text{-}INS}^{\mathcal{M}\times\mathcal{S}}_{n\to 1}$, $\boldsymbol{\sigma}$ also inputs $\diamond$ to the interface E of $\mathsf{RA\text{-}AUT}^{\mathcal{M}}_{n\to 1}$, obtaining a

set $\mathfrak{O} \subseteq \mathbb{N} \times \mathcal{M}$. It then outputs the set $\{(j, m, \mathtt{Sgn}_{1,sk_1,\boldsymbol{pk}}(m)) \mid \exists\,(j,m) \in \mathfrak{O}\}$ to E, and sets $\mathcal{Q} \leftarrow \mathcal{Q} \cup \mathfrak{O}$. Whenever (m, σ) is input to the interface E emulating $\mathsf{A\text{-}INS}^{\mathcal{M}\times\mathcal{S}}_{n\to 1}$, if $(j, m, \sigma) \in \mathcal{Q}$ for some $j \in \mathbb{N}$, then $\boldsymbol{\sigma}$ inputs j to the E interface of $\mathsf{RA\text{-}AUT}^{\mathcal{M}}_{n\to 1}$.

The transformation $\rho([\![[\![\mathbf{X}_1, \mathbf{Y}_1]\!], \ldots, [\![\mathbf{X}_n, \mathbf{Y}_n]\!], \boldsymbol{x}]\!])$ simply works by emulating $\boldsymbol{\pi}_{\mathsf{RS}}[\mathsf{1\text{-}AUT}^{\mathcal{PK}}_{n\bigcirc 1}, \mathsf{A\text{-}INS}^{\mathcal{M}\times\mathcal{S}}_{n\to 1}]$, but replacing any calls to $\mathtt{Gen}$ by the appropriate value from $\boldsymbol{x}$, any call to $\mathtt{Sgn}_{i,sk_i,\boldsymbol{pk}}$ by a call $\mathbf{X}_i$, and any call to $\mathtt{Vrf}_{\boldsymbol{pk}}$ by a call to $\mathbf{Y}_i$. □

4.5.3 Relations with Previous Notions and Schemes

Our game-based definitions for ring signatures closely resemble the ones from the literature, except that we chose to phrase the notions as distinguishing problems, whereas [BKM06] defines unforgeability as a forgery problem and anonymity as a bit-guessing problem. [BKM06] also introduces a construction satisfying their (stronger) definitions, which we call the BKM construction here. This ring signature scheme is based on a public-key encryption scheme, a regular signature scheme, a ZAP (i.e., a two-round public-coin witness-indistinguishable proof system, where the first round is a random string from the verifier to the prover), and roughly works as follows: Sender S_i initially generates a public-key encryption key-pair (sk_i^E, pk_i^E) and a regular signature key-pair (sk_i^S, pk_i^S). In order to generate a ring signature on a message m, S_i first produces a regular signature σ' on m with its signing key sk_i^S. Then S_i produces ciphertexts C_j^*, for $j \in [n]$, using encryption keys $pk_1^S, \ldots, pk_n^S$, where C_i^* is the encryption of σ' and the other ciphertexts are encryptions of random bit-strings instead. Finally, using the ZAP S_i produces a proof π, stating that one of the ciphertexts is indeed an encryption of a valid signature on m with respect to the public verification key of one of the ring members (that is, pk_i^S). Verification is then defined in the straightforward way.

We now informally argue that the BKM construction achieves our composable notion for ring signatures, that is, it constructs $\mathsf{RA\text{-}AUT}^{\mathcal{M}}_{n\to 1}$ from $[\mathsf{1\text{-}AUT}^{\mathcal{PK}}_{n\bigcirc 1}, \mathsf{A\text{-}INS}^{\mathcal{M}\times\mathcal{S}}_{n\to 1}]$ when used in the natural way. To do so, we first observe that the stronger notions of *unforgeability w.r.t. insider corruption* and *anonymity against attribution attacks* that BKM has been shown to satisfy in [BKM06], trivially imply the weaker notions of *unforgeability against fixed-ring attacks* and *basic anonymity*, respectively, that [BKM06] also defines. It then suffices to relate the latter notions

to our game-based notions of uf-security and ik-security, respectively, since Lemma 4.5.5 then implies that BKM is also uf-ik-secure, which by Theorem 4.5.6 is therefore also composably secure, as per Theorem 4.5.6.

Unforgeability. In [BKM06] the BKM construction has been shown to be unforgeable against insider corruption, and therefore also against fixed-ring attacks, if the base signature scheme is unforgeable. The original notion of unforgeability against fixed-ring attacks, [BKM06, Definition 5], can be shown to be equivalent to our distinguishing problem from Definition 4.4.2, since being able to distinguish the two systems implies being able to find a valid forgery. Therefore, the BKM construction also satisfies our uf-security notion for ring signatures.

Anonymity. In [BKM06] the BKM construction has been shown to be anonymous against attribution attacks, and therefore it also satisfies basic anonymity, if the base public-key encryption scheme is IND-CPA-secure and the ZAP is witness-indistinguishable. The original notion of basic anonymity, [BKM06, Definition 5], is slightly different than our ik-security notion because it is only defined for two senders, and it is phrased as a bit-guessing problem. Nevertheless, it can be shown to be equivalent to our distinguishing problem from Definition 4.5.3, up to a multiplicative loss factor of $(n-1)$, via a standard hybrid argument. Therefore, the BKM construction also satisfies our ik-security notion for ring signatures.

4.6 Anonymous Signatures and Signcryption

In this section we briefly discuss anonymous signatures, the precursors of partial signatures. As we mentioned above, in the setting we are considering such scheme's security would not be possible to model, since we fixed the anonymous insecure channel $\mathsf{A\text{-}INS}^{\mathcal{X}}_{n\to 1}$ as the assumed resource. But if we would strengthen this assumption, it would then be possible to model anonymous signatures' security as well. More concretely, if we additionally include to the assumed resources the anonymous confidential channel $\mathsf{A\text{-}CNF}^{\mathcal{X}}_{n\to 1}$, as informally described in Section 4.1.2, it would then be possible to define composable security of a protocol π_{AS} using anonymous signatures as the construction of the anonymous secure channel $\mathsf{A\text{-}SEC}^{\mathcal{M}}_{n\to 1}$, also informally described in Section 4.1.2, from $\mathsf{1\text{-}AUT}^{\mathcal{PK}}_{n\to 1}$,

$\mathsf{A\text{-}INS}^{\mathcal{S}}_{n\to 1}$, and $\mathsf{A\text{-}CNF}^{\mathcal{M}}_{n\to 1}$, that is,

$$[\mathsf{1\text{-}AUT}^{\mathcal{PK}}_{n\to 1}, \mathsf{A\text{-}INS}^{\mathcal{S}}_{n\to 1}, \mathsf{A\text{-}CNF}^{\mathcal{M}}_{n\to 1}] \xRightarrow{\boldsymbol{\pi}_{\mathsf{AS}}} \mathsf{A\text{-}SEC}^{\mathcal{M}}_{n\to 1}.$$

Intuitively, $\boldsymbol{\pi}_{\mathsf{AS}}$ would use $\mathsf{A\text{-}INS}^{\mathcal{S}}_{n\to 1}$ to transmit the signature, and $\mathsf{A\text{-}CNF}^{\mathcal{M}}_{n\to 1}$ for the message, so that the latter is not leaked to the adversary, which therefore cannot use it to verify and hence break anonymity.

Furthermore, the resource $\mathsf{A\text{-}CNF}^{\mathcal{M}}_{n\to 1}$ could in principle be constructed from $\mathsf{1\text{-}AUT}^{\mathcal{PK}'}_{n\leftarrow 1}$ and $\mathsf{A\text{-}INS}^{\mathcal{C}}_{n\to 1}$ via a protocol $\boldsymbol{\pi}_{\mathsf{APKE}}$ making use of a public-key encryption scheme satisfying appropriate anonymity properties. Then, similarly as the result from [KMO+13], one could show that

$$[\mathsf{1\text{-}AUT}^{\mathcal{PK}'}_{n\leftarrow 1}, \mathsf{A\text{-}INS}^{\mathcal{C}}_{n\to 1}] \xRightarrow{\boldsymbol{\pi}_{\mathsf{APKE}}} \mathsf{A\text{-}CNF}^{\mathcal{M}}_{n\to 1}.$$

Finally, one could compose the two schemes using the *encrypt-and-sign* paradigm, resulting in an anonymous signcryption scheme. By Theorem 2.4.4, the composed protocol $\boldsymbol{\pi}_{\mathsf{SC}} = \boldsymbol{\pi}_{\mathsf{AS}}\,\boldsymbol{\pi}_{\mathsf{APKE}}$ would then imply the construction

$$[\mathsf{1\text{-}AUT}^{\mathcal{PK}}_{n\to 1}, \mathsf{1\text{-}AUT}^{\mathcal{PK}'}_{n\leftarrow 1}, \mathsf{A\text{-}INS}^{\mathcal{C}\times\mathcal{S}}_{n\to 1}] \xRightarrow{\boldsymbol{\pi}_{\mathsf{SC}}} \mathsf{A\text{-}SEC}^{\mathcal{M}}_{n\to 1}. \tag{4.3}$$

Referring to the results from [BBM18], which attest that signcryption realizes a (non-anonymous) secure network from a (non-anonymous) insecure one, it is possible to draw a similar conclusion as we did in Chapter 3 for authenticated encryption, namely that equation (4.3) represents the composable confirmation that this particular instantiation of the encrypt-and-sign paradigm is *anonymity-preserving*.

Chapter 5

Anonymity Creation

5.1 Introduction

5.1.1 Motivation

Introduced in [GJJS04] by Golle et al., *universal re-encryption* (URE) is a cryptographic primitive originally intended as a building block for mix networks, or *mixnets* for short. URE is like a regular public-key encryption scheme, but enhanced with a re-encryption algorithm, that on input a ciphertexts produces a fresh ciphertext still valid for the underlying plaintext under the original key-pair, and crucially does not require any key material as input. The guarantee that a mixnet aims to provide, is that after a sender submits a message and later the intended receiver fetches such message, an external observer cannot link the two actions together. This property is called *unlinkability*, and is an enabler of resistance against traffic analysis. URE schemes lend themselves naturally as building blocks of such mixnets by having senders encrypt their messages under the public-keys of the intended receivers and authentically publishing the ciphertexts on a bulletin board, an honest mixer regularly re-encrypting all posted ciphertexts, and receivers fetching all ciphertexts and figuring out which ones were meant for them.

Recently, Young and Yung [YY18] pointed out that the original combined security notion of URE of Golle et al. [GJJS04] was flawed, because it captured confidentiality (IND-CPA) and anonymity (key-

indistinguishability) of the re-encryption function, but only confidentiality (and not anonymity) of the encryption function. They then claimed to provide the first formal foundation of URE security, by essentially splitting the security notion from [GJJS04] into three separate formal notions, and additionally requiring key-indistinguishability of encryption. Nevertheless, we argue that they came short of properly capturing the essence of URE, because their notions do not directly capture unlinkability as an atomic property of an URE scheme, but rather mix it once with confidentiality and once with anonymity.

5.1.2 Contributions

The main goal of this chapter is to once more re-analyze the security foundations of URE, and finally put this primitive on solid grounds. On the one hand, we show that Young and Yung's notions from [YY18] fall short of capturing the essence of URE, which is unlinkability. On the other hand, we introduce two composable notions that capture the essence of URE from an application point-of-view, and show that the mentioned game-based security notions for URE only satisfy the weaker one. All our results are shown using a new framework that we introduce.

Capturing the Essence of URE: Minimal Game-Based Notions. Using substitutions, we then show that Young and Yung's notions are not minimal. More precisely, we introduce three minimal notions of security, *confidentiality* (ind-cpa), *anonymity* (ik-cpa), and *unlinkability* (ulk-cpa), and show that their four notions are implied by and imply ours. More precisely, we unveil that their four notions are ind-cpa, ik-cpa, ind-cpa combined with ulk-cpa, and ik-cpa combined with ulk-cpa.

Capturing the Essence of URE: Composable Semantics. Secondly, we introduce a new composable notion for URE, also using substitutions, in order to capture the essence of URE from an *application point-of-view*. This notion captures the case of an honest mixer, and we show that our game-based notions, and therefore Young and Yung's notions, imply it.

5.1.3 Related Work

URE was originally introduced by Golle et al. in [GJJS04], and its security foundation was crucially analyzed much later in Young and Yung in [YY18].

Both these works considered security under chosen-plaintext attacks, as we also do here. An interesting line of research, started by Groth [Gro04], continued by Prabhakaran and Rosulek [PR07], and culminating in the recent work by Wang et al. [WCY+21], studies URE security under the stronger model of chosen-ciphertext attacks, where URE is often referred to as re-randomizable encryption.

Regarding composable notions, Wikström [Wik04] introduces a UC-functionality capturing security of an ElGamal re-encryption protocol that is *not* universal, that is, re-encryption is performed by the mixers by decrypting and then encrypting again, and thus is inherently more complex than our notion. In [PR07] a so-called "replayable message posting" UC-functionality is introduced, but which does not directly capture the application of URE in the context of mixnets, and additionally assumes perfect unlinkability and chosen-ciphertext attacks security.

5.2 Universal Re-Encryption

5.2.1 Extending the Systems Algebra

Recall the notion of cryptographic systems from Section 2.2. For fixed sets $\mathcal{X}$ and $\mathcal{Y}$, we additionally define some special stateless systems as follows.

Definition 5.2.1 (Special Systems)**.** For any sets $\mathcal{X}, \mathcal{Y}$, we define some special $(\mathcal{X}, \mathcal{Y})$-systems (where $\mathcal{X}$ and $\mathcal{Y}$ are implicit and always clear from the context) that behave as follows:

- $*$ is an $(\mathcal{X}, \mathcal{X})$-system that on input x, outputs x.
- $\mathbb{1}_\xi$ is an $(\mathcal{X}, \{0,1\})$-system that on input x, outputs 1 if $x = \xi$ and 0 otherwise.
- $\bot$ is an $(\mathcal{X}, \{\bot\})$-system that on input any x always outputs $\bot$.
- y is an $(\mathcal{X}, \mathcal{Y})$-system, where $y \in \mathcal{Y}$, that on input any x always outputs y.
- Y is an $(\mathcal{X}, \mathcal{Y})$-system, where Y is a random variable over $\mathcal{Y}$, that on input any x, outputs some y with probability $\Pr[Y = y]$.

- **$** is an $(\mathcal{X}, \mathcal{Y})$-system that on input any x, outputs some y with uniform probability over $\mathcal{Y}$.

We next describe some additional useful ways in which systems can be combined into new systems, as illustrated in Figure 5.1.

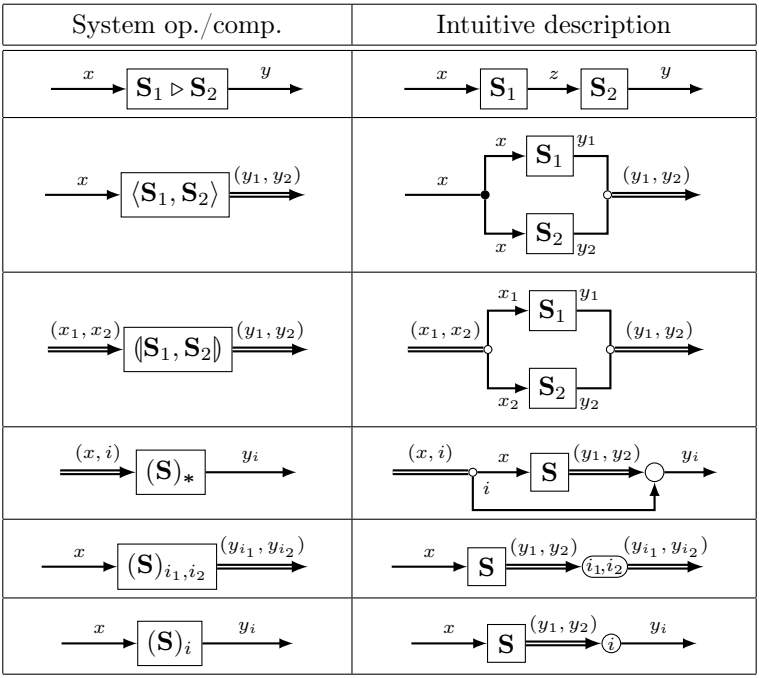


Figure 5.1: Schematic representation of the systems from Definition 5.2.1 for $\ell = 2$.

Definition 5.2.2 (System Compositions/Operations)**.** Let $\ell \in \mathbb{N}$. For $(\mathcal{X}_i, \mathcal{Y}_i)$-system $\mathbf{S}_i$, for each $i \in [\ell]$, $(\mathcal{X}, \bigtimes_{i=1}^{\ell} \mathcal{Y}_i)$-system $\mathbf{S}$, and pairwise different integers $i_1, \ldots, i_t \subseteq [\ell]$, for $t \leq \ell$, we define the systems that behave as follows:

- $\mathbf{S}_1 \triangleright \cdots \triangleright \mathbf{S}_\ell$ is an $(\mathcal{X}_1, \mathcal{Y}_\ell)$-system defined only if $\mathcal{Y}_i \subseteq \mathcal{X}_{i+1}$, for all $i \in [\ell - 1]$, that on input x, inputs x to $\mathbf{S}_1(x)$ and obtains y_1, then inputs y_1 to $\mathbf{S}_2$ and obtains y_2, and so on, until it finally outputs y_ℓ.

- $\langle \mathbf{S}_1, \ldots, \mathbf{S}_\ell \rangle$ is an $(\mathcal{X}, \bigtimes_{i=1}^{\ell} \mathcal{Y}_i)$-system defined only if $\mathcal{X} = \mathcal{X}_i$, for all $i \in [\ell]$, that on input x, for each $i \in [\ell]$ inputs x to $\mathbf{S}_i$ and obtains y_i, and then outputs $(y_1, \ldots, y_\ell)$.
- $(\!|\mathbf{S}_1, \ldots, \mathbf{S}_\ell|\!)$ is a $(\bigtimes_{i=1}^{\ell} \mathcal{X}_i, \bigtimes_{i=1}^{\ell} \mathcal{Y}_i)$-system that on input $(x_1, \ldots, x_\ell)$, for each $i \in [\ell]$ inputs x_i to $\mathbf{S}_i$ and obtains y_i, and then outputs $(y_1, \ldots, y_\ell)$.
- $(\mathbf{S})_*$ is a $([\ell] \times \mathcal{X}, \bigcup_{i=1}^{\ell} \mathcal{Y}_i)$-system that on input (i, x), inputs x to $\mathbf{S}$ and obtains $(y_1, \ldots, y_\ell)$, and then outputs y_i.
- $(\mathbf{S})_{i_1,\ldots,i_t}$ is an $(\mathcal{X}, \bigtimes_{i=1}^{t} \mathcal{Y}_{j_i})$-system that on input x, inputs x to $\mathbf{S}$ and obtains $(y_1, \ldots, y_\ell)$, and then outputs $(y_{j_1}, \ldots, y_{j_t})$.

Finally, we assume that grouping tuples into tuples yields tuples, that is, for systems $\mathbf{R}, \mathbf{S}, \mathbf{T}$, we assume $\langle \mathbf{R}, \mathbf{S}, \mathbf{T} \rangle \equiv \langle \mathbf{R}, \langle \mathbf{S}, \mathbf{T} \rangle \rangle \equiv \langle \langle \mathbf{R}, \mathbf{S} \rangle, \mathbf{T} \rangle$ and $(\!|\mathbf{R}, \mathbf{S}, \mathbf{T}|\!) \equiv (\!|\mathbf{R}, (\!|\mathbf{S}, \mathbf{T}|\!)|\!) \equiv (\!|(\!|\mathbf{R}, \mathbf{S}|\!), \mathbf{T}|\!)$.

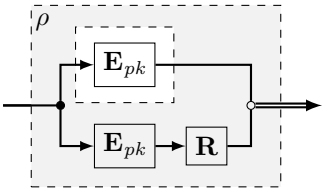
Let now us give some more intuition on Definition 5.2.2 via some concrete example. Consider systems $\mathbf{X}_{(\cdot)}, \mathbf{Y}_{(\cdot)}, \mathbf{U}_{(\cdot)}, \mathbf{V}_{(\cdot)}$, each of which is parameterized by some value. Then, let's for example construct the following system, for some concrete values a, b, c:

$$[\![\langle \mathbf{X}_a, \mathbf{Y}_b \rangle \triangleright (\!| \mathbf{U}_a, \mathbf{V}_c |\!)_{2,1}, a, b]\!].$$

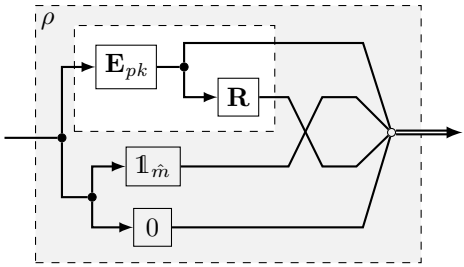
This systems allows interaction with three sub-systems in parallel, where some of them are correlated. Concretely, the last two sub-systems simply return the corresponding value, on input $\diamond$ (note that, in a sense, we did not make public all three parameters), whereas the first sub-system, on input some value x, will output a tuple (z', y'), in a way that also depend on a, b, c. More precisely, x will first be fed to the system $\langle \mathbf{X}_a, \mathbf{Y}_b \rangle$, which means that x will be input in parallel to both $\mathbf{X}_a$ and $\mathbf{Y}_b$, and the resulting values y and z will be collected into a tuple (y, z). This will then be input to the system $(\!|\mathbf{U}_a, \mathbf{V}_c|\!)$, which means that y will be input to $\mathbf{U}_a$, resulting in y', whereas z will be input to $\mathbf{V}_b$, resulting in z'. As before, the resulting values y' and z' will be collected into a tuple (y', z'). Finally, this tuple will be permuted into (z', y'), the output of the whole sub-system.

Since, as per Definition 5.2.2, systems can appear as sub-system of other systems, we need a way to make this explicit, in order to later

relate security notions based on systems. To achieve this, the proofs in this chapter will explicitly show how to factorize systems by exhibiting a function ρ (the transformation) as per Section 2.2.2, that given a system of some special form, maps it to another system, but additionally using operations and compositions from Definition 5.2.2. For example, looking ahead, in the proof of Lemma 5.3.9, for any system $\mathbf{X}$ and parameter x we define $\rho(\llbracket \mathbf{X}, x \rrbracket) \doteq \llbracket \langle \mathbf{E}_x, \mathbf{X} \triangleright \mathbf{R} \rangle, x \rrbracket$, for systems $\mathbf{E}_x$ and $\mathbf{R}$ defined later. Then we use ρ to show that, for $(sk, pk) \leftarrow \texttt{Gen}$, the system $\llbracket \mathbf{E}_{pk}, pk \rrbracket$ can be factored out of $\llbracket \langle \mathbf{E}_{pk}, \mathbf{E}_{pk} \triangleright \mathbf{R} \rangle, pk \rrbracket$, that is, $\rho(\llbracket \mathbf{E}_{pk}, pk \rrbracket) = \llbracket \langle \mathbf{E}_{pk}, \mathbf{E}_{pk} \triangleright \mathbf{R} \rangle, pk \rrbracket$. Visually, this can be seen as follows (ignoring pk):



Looking again ahead, let us consider the proof of Lemma 5.3.10 for a slightly more complex example. There, in the second part of the proof we define $\rho(\llbracket \mathbf{X}, x \rrbracket) \doteq \llbracket \langle *, * \rangle \triangleright (\!| \mathbf{X}, \langle \mathbb{1}_{\hat{m}}, 0 \rangle |\!)_{1,3,2,4}, x \rrbracket$ and then show that, for $(sk, pk) \leftarrow \texttt{Gen}$, the system $\llbracket \mathbf{E}_{pk} \triangleright \langle *, \mathbf{R} \rangle, pk \rrbracket$ can be factored out of $\llbracket \langle *, * \rangle \triangleright (\!| \mathbf{E}_{pk} \triangleright \langle *, \mathbf{R} \rangle, \langle \mathbb{1}_{\hat{m}}, 0 \rangle |\!)_{1,3,2,4}, pk \rrbracket$. Visually, this can be seen as follows (ignoring pk and making some simplifications, such as turning the systems $*$ into wires):



5.2.2 Universal Re-Encryption

Definition 5.2.3. A *universal re-encryption* (URE) scheme for private-key space $\mathcal{SK}$, public-key space $\mathcal{PK}$, message space $\mathcal{M} = \{0,1\}^\kappa$, for some $\kappa \in \mathbb{N}$, and ciphertext space $\mathcal{C}$, is a tuple $\Pi_{\mathsf{URE}} = (\mathtt{Gen}, \mathtt{Enc}, \mathtt{Rnc}, \mathtt{Dec})$ where:

- $\mathtt{Gen}$ is the *key-pair distribution* over $\mathcal{SK} \times \mathcal{PK}$;
- $\mathtt{Enc}$ is the probabilistic *encryption algorithm* that on input a public key $pk \in \mathcal{PK}$ and a message $m \in \mathcal{M}$, outputs a ciphertext $c \in \mathcal{C}$;
- $\mathtt{Rnc}$ is the probabilistic *re-encryption algorithm* that on input a ciphertext $c \in \mathcal{C}$ outputs a new ciphertext $\hat{c} \in \mathcal{C}$;
- $\mathtt{Dec}$ is the deterministic *decryption algorithm* that on input a secret key $sk \in \mathcal{SK}$ and a ciphertext $c \in \mathcal{C}$, outputs a message $m \in \mathcal{M}$.

As customary, for $sk \in \mathcal{SK}$ and $pk \in \mathcal{PK}$, we write $\mathtt{Enc}_{pk}(\cdot)$ for $\mathtt{Enc}(pk, \cdot)$ and $\mathtt{Dec}_{sk}(\cdot)$ for $\mathtt{Dec}(sk, \cdot)$.

In this chapter all notions are relative to some fixed URE scheme Π_{URE}, defining sets $\mathcal{SK}$, $\mathcal{PK}$, $\mathcal{M}$, and $\mathcal{C}$, and for which we define the following parameterized systems.

Definition 5.2.4. For parameters $sk, sk_1, \ldots, sk_n \in \mathcal{SK}$, and $pk, pk_1, \ldots, pk_n \in \mathcal{PK}$, we define the parameterized systems that behave as follows:

- $\mathbf{E}_{pk}$ is an $(\mathcal{M}, \mathcal{C})$-system that on input m, outputs $\mathtt{Enc}_{pk}(m)$.
- $\mathbf{X}^{\$} \doteq \$ \triangleright \mathbf{X}$, for any system $\mathbf{X}$, is an $(\mathcal{M}, \mathcal{C})$-system that on input m, samples $\tilde{m} \xleftarrow{\$} \mathcal{M}$, forwards $\tilde{m}$ to $\mathbf{X}$, obtains c, and outputs c (analogous to $\rho^{\mathsf{cpa}}(\mathbf{X})$ for symmetric encryption from Chapter 3).
- $\mathbf{R}$ is a $(\mathcal{C}, \mathcal{C})$-system that on input c, outputs $\mathtt{Rnc}(c)$.
- $\mathbf{R}^*$ is a $(\mathcal{C} \times \mathbb{N}, \mathcal{C})$-system that on input (c, t), outputs $\mathtt{Rnc}^t(c)$.
- $\mathbf{D}_{sk}$ is a $(\mathcal{C}, \mathcal{M})$-system that on input c, outputs $\mathtt{Dec}_{sk}(c)$.
- $\mathbf{E}_{pk_1,\ldots,pk_n}$ is a $(\mathcal{M} \times [n], \mathcal{C})$-system that on input (m, i), outputs $\mathtt{Enc}_{pk_i}(m)$.

- $\mathbf{D}_{sk_1,\ldots,sk_n}$ is a $(\mathcal{C} \times [n], \mathcal{M})$-system that on input (c, i), outputs $\mathtt{Dec}_{sk_i}(c)$.
- $\mathbf{I}_n$ is an $([n] \times \mathcal{M} \times \mathbb{N} \times [n], \mathcal{M} \cup \{\bot\})$-system that on input (i, m, t, j), outputs m if $i = j$ and $\bot$ otherwise.

We will use the systems from Definition 5.2.4 to build more complex systems through the system composition operations from Definition 5.2.2.

5.3 Game-Based Semantics of URE

We begin by defining security of a fixed URE scheme where for notions naturally living in a multi-user setting (such as robustness and anonymity), we only consider the case of two receivers. We combine our notions into single security definitions in Section 5.3.4, where we also show that the resulting notions are equivalent. We then generalize such combined notions to arbitrary number of receivers in Section 5.3.5, where we also show that they are implied by the combined notions for two receivers.

5.3.1 Minimal Notions

The first notions we introduce are the ones that intuitively only capture a single security guarantee.

For *correctness* (cor), we consider the substitution of the following two systems, both of which initially sample a key-pair $(sk, pk) \leftarrow \mathtt{Gen}$. The first system, on input a message-integer pair $(m, t) \in \mathcal{M} \times \mathbb{N}$, encrypts m into $c \leftarrow \mathtt{Enc}_{pk}(m)$, re-encrypts t times c, that is, computes $\hat{c}_i \leftarrow \mathtt{Rnc}(\hat{c}_{i-1})$ for $i \in [t]$ and where $\hat{c}_0 \doteq c$, and finally decrypts $\hat{c}_t$ into $m' := \mathtt{Dec}_{sk}(\hat{c}_t)$ and outputs m'. The second system, on input a message-integer pair $(m, t) \in \mathcal{M} \times \mathbb{N}$, simply outputs m. Both systems also give access in parallel to the public key pk. The intuition is that the scheme is correct if encrypting, re-encrypting an arbitrary number of times, and then decrypting with the correct secret key, results in the original message.

Definition 5.3.1 (cor)**.**

$$[\![(\!|\mathbf{E}_{pk}, *|\!) \triangleright \mathbf{R}^* \triangleright \mathbf{D}_{sk}, pk]\!] \eqsim [\![(\!|*, *|\!)_1, pk]\!],$$

for $(sk, pk) \leftarrow \mathtt{Gen}$.

For *robustness* (rob), we consider the substitution of the following two systems, both of which initially sample two independent key-pairs $(sk_1, pk_1), (sk_2, pk_2) \leftarrow \mathtt{Gen}$. The first system, on input a message-integer pair $(m, t) \in \mathcal{M} \times \mathbb{N}$, encrypts m into $c \leftarrow \mathtt{Enc}_{pk_1}(m)$ using the public key from the first key-pair, re-encrypts t times c, that is, computes $\hat{c}_i \leftarrow \mathtt{Rnc}(\hat{c}_{i-1})$ for $i \in [t]$ and where $\hat{c}_0 \doteq c$, and finally decrypts $\hat{c}_t$ into $m' := \mathtt{Dec}_{sk_2}(\hat{c}_t)$ using the secret key from the second key-pair, and outputs m'. The second system, on input a message-integer pair $(m, t) \in \mathcal{M} \times \mathbb{N}$, simply outputs $\bot$. Both systems also give access in parallel to the public keys pk_1 and pk_2. The intuition is that the scheme is robust if encrypting, re-encrypting an arbitrary number of times, and then decrypting with an incorrect secret key, results in $\bot$.

Definition 5.3.2 (rob)**.**

$$[\![(\!|\mathbf{E}_{pk_1}, *|\!) \triangleright \mathbf{R}^* \triangleright \mathbf{D}_{sk_2}, pk_1, pk_2]\!] \eqsim [\![(\!|\bot, *|\!)_1, pk_1, pk_2]\!],$$

for independent $(sk_1, pk_1), (sk_2, pk_2) \leftarrow \mathtt{Gen}$.

For *confidentiality*, modeled as (real-or-random) indistinguishability of ciphertexts under a chosen-plaintext attack (ind-cpa), we consider the substitution of the following two systems, both of which initially sample a key-pair $(sk, pk) \leftarrow \mathtt{Gen}$. The first system, on input a message $m \in \mathcal{M}$, encrypts m into $c \leftarrow \mathtt{Enc}_{pk}(m)$ and outputs c. The second system, on input a message $m \in \mathcal{M}$, samples $\tilde{m}$, encrypts $\tilde{m}$ into $\tilde{c} \leftarrow \mathtt{Enc}_{pk}(\tilde{m})$ and outputs $\tilde{c}$. Both systems also give access in parallel to the public key pk. The intuition is that the scheme is confidential if regular encryptions or encryptions of unrelated messages are indistinguishable.

Definition 5.3.3 (ind-cpa)**.**

$$[\![\mathbf{E}_{pk}, pk]\!] \eqsim [\![\mathbf{E}^{\$}_{pk}, pk]\!],$$

for $(sk, pk) \leftarrow \mathtt{Gen}$.

For *anonymity*, modeled as key-indistinguishability under a chosen-plaintext attack (ik-cpa), we consider the substitution of the following two systems, both of which initially sample two independent key-pairs $(sk_1, pk_1), (sk_2, pk_2) \leftarrow \mathtt{Gen}$. The first system has two sub-systems: The first, on input a message $m \in \mathcal{M}$, encrypts m into $c \leftarrow \mathtt{Enc}_{pk_1}(m)$ using

the public key from the *first* key-pair and outputs c, while the second, on input a message $m \in \mathcal{M}$, encrypts m into $c \leftarrow \mathtt{Enc}_{pk_2}(m)$ using the public key from the *second* key-pair and outputs c; The second system also has two sub-systems: Both of them, on input a message $m \in \mathcal{M}$, encrypt m into $c \leftarrow \mathtt{Enc}_{pk_1}(m)$ using the public key from the *first* key-pair and output c. Both systems also give access in parallel to the public keys pk_1 and pk_2. The intuition is that the scheme is anonymous if encryptions under different public keys are indistinguishable.

Definition 5.3.4 (ik-cpa)**.**

$$[\![\mathbf{E}_{pk_1}, \mathbf{E}_{pk_2}, pk_1, pk_2]\!] \eqsim [\![\mathbf{E}_{pk_1}, \mathbf{E}_{pk_1}, pk_1, pk_2]\!],$$

for independent $(sk_1, pk_1), (sk_2, pk_2) \leftarrow \mathtt{Gen}$.

For *unlinkability* (ulk-cpa), we consider the substitution of the following two systems, both of which initially sample a key-pair $(sk, pk) \leftarrow \mathtt{Gen}$. The first system, on input a message $m \in \mathcal{M}$, first encrypts m into $c \leftarrow \mathtt{Enc}_{pk}(m)$. Then it computes $\hat{c} \leftarrow \mathtt{Rnc}(c)$ and outputs $(c, \hat{c})$. Formally, we model this using the operator $\triangleright$ for systems that forwards c from system $\mathbf{E}_{pk}$ to system $\langle *, \mathbf{R} \rangle$, which in turn internally feeds c in parallel to systems $*$ and $\mathbf{R}$, and collects the outputs c and $\hat{c}$ in the tuple $(c, \hat{c})$. The second system, on input a message $m \in \mathcal{M}$, first encrypts m into $c \leftarrow \mathtt{Enc}_{pk}(m)$. Then it encrypts again m into $c' \leftarrow \mathtt{Enc}_{pk}(m)$ using *fresh and independent randomness.* Finally, it computes $\hat{c} \leftarrow \mathtt{Rnc}(c')$ and outputs $(c, \hat{c})$. Formally, we model this by composing the two systems $\mathbf{E}_{pk}$ and $\mathbf{E}_{pk} \triangleright \mathbf{R}$ with the system operator $\langle \cdot, \cdot \rangle$. Both systems also give access in parallel to the public key pk. The intuition is that the scheme is unlinkable if an encryption and its re-encryption are indistinguishable from an encryption and the re-encryption of another fresh encryption of the same message.

Definition 5.3.5 (ulk-cpa)**.**

$$[\![\mathbf{E}_{pk} \triangleright \langle *, \mathbf{R} \rangle, pk]\!] \eqsim [\![\langle \mathbf{E}_{pk}, \mathbf{E}_{pk} \triangleright \mathbf{R} \rangle, pk]\!],$$

for $(sk, pk) \leftarrow \mathtt{Gen}$.

For *strong unlinkability* (sulk-cpa), we consider the same substitution as for regular unlinkability, except that we replace the system $\mathbf{E}_{pk} \triangleright \mathbf{R}$

by the system $\mathbf{E}_{pk}$ as a sub-system of the right-hand side system. The intuition is that the scheme is strongly unlinkable if an encryption and its re-encryption are indistinguishable from two fresh encryptions of the same message.

Definition 5.3.6 (sulk-cpa)**.**

$$[\![\mathbf{E}_{pk} \triangleright \langle *, \mathbf{R}\rangle, pk]\!] \eqsim [\![\langle \mathbf{E}_{pk}, \mathbf{E}_{pk}\rangle, pk]\!],$$

for $(sk, pk) \leftarrow \mathtt{Gen}$.

5.3.2 Young and Yung's Combined Notions

We now introduce the security notions from in [YY18] that aim at capturing confidentiality and anonymity of the re-encryption function. Note that we introduce a different flavor than the one introduced there, but in Appendix B.1 we show that our notions are essentially equivalent. Moreover, as we will see in Section 5.3.3, these two notions are not necessary, if a URE scheme already satisfies ind-cpa, ik-cpa, and ulk-cpa.

For *confidentiality of re-encryption* (ind-r-cpa), we consider the substitution of the following two systems, both of which initially sample a key-pair $(sk, pk) \leftarrow \mathtt{Gen}$. The first system, on input a message $m \in \mathcal{M}$, first encrypts m into $c \leftarrow \mathtt{Enc}_{pk}(m)$. Then it computes $\hat{c} \leftarrow \mathtt{Rnc}(c)$ and outputs $(c, \hat{c})$. The second system, on input a message $m \in \mathcal{M}$, first encrypts m into $c \leftarrow \mathtt{Enc}_{pk}(m)$. Then it samples $\tilde{m}$, encrypts $\tilde{m}$ into $\tilde{c} \leftarrow \mathtt{Enc}_{pk}(\tilde{m})$, computes $\hat{c} \leftarrow \mathtt{Rnc}(\tilde{c})$, and finally outputs $(c, \hat{c})$. Both systems also give access in parallel to the public key pk. The intuition is that the scheme has confidential re-encryption if an encryption and its re-encryption are indistinguishable from an encryption and the re-encryption of the encryption of an unrelated message.

Definition 5.3.7 (ind-r-cpa)**.**

$$[\![\mathbf{E}_{pk} \triangleright \langle *, \mathbf{R}\rangle, pk]\!] \eqsim [\![\langle \mathbf{E}_{pk}, \mathbf{E}^{\$}_{pk} \triangleright \mathbf{R}\rangle, pk]\!],$$

for $(sk, pk) \leftarrow \mathtt{Gen}$.

For *anonymity of re-encryption* (ik-r-cpa), we consider the substitution of the following two systems, both of which initially sample two independent key-pairs $(sk_1, pk_1), (sk_2, pk_2) \leftarrow \mathtt{Gen}$. The first system has

two sub-systems: The first, on input a message $m \in \mathcal{M}$, encrypts m into $c \leftarrow \mathtt{Enc}_{pk_1}(m)$ using the public key from the *first* key-pair, computes $\hat{c} \leftarrow \mathtt{Rnc}(c)$, and then outputs $(c, \hat{c})$, while the second, on input a message $m \in \mathcal{M}$, encrypts m into $c \leftarrow \mathtt{Enc}_{pk_2}(m)$ using the public key from the *second* key-pair, computes $\hat{c} \leftarrow \mathtt{Rnc}(c)$, and then outputs $(c, \hat{c})$ The second system also has two sub-systems: The first is the same as in the first system, whereas the second, on input a message $m \in \mathcal{M}$, encrypts m into $c \leftarrow \mathtt{Enc}_{pk_2}(m)$ using the public key from the *second* key-pair, encrypts again m into $c' \leftarrow \mathtt{Enc}_{pk_1}(m)$ using the public key from the *first* key-pair, then computes $\hat{c} \leftarrow \mathtt{Rnc}(c')$ and outputs $(c, \hat{c})$. Both systems also give access in parallel to the public keys pk_1 and pk_2. The intuition is that the scheme has anonymous re-encryption if two pairs consisting of an encryption and its re-encryption under two independent public keys are indistinguishable from an encryption and its re-encryption paired with and encryption and the re-encryption of an encryption of the same message under an unrelated public key.

Definition 5.3.8 (ik-r-cpa)**.**

$$[\![\mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R}\rangle, \mathbf{E}_{pk_2} \triangleright \langle *, \mathbf{R}\rangle, pk_1, pk_2]\!]$$
$$\eqsim$$
$$[\![\mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R}\rangle, \langle \mathbf{E}_{pk_2}, \mathbf{E}_{pk_1} \triangleright \mathbf{R}\rangle, pk_1, pk_2]\!],$$

for independent $(sk_1, pk_1), (sk_2, pk_2) \leftarrow \mathtt{Gen}$.

5.3.3 Relations Among Security Notions

Minimality of ind-cpa**,** ik-cpa**, and** ulk-cpa**.** We begin by showing that the four notions ind-cpa, ik-cpa, ind-r-cpa, and ik-r-cpa put forth by [YY18] are *not* minimal, in the sense that they are all implied by the three notions ind-cpa, ik-cpa, and ulk-cpa, and vice versa. Figure 5.2 summarizes all relations (both implications and separations) that we prove. Furthermore, in Appendix B.1 we show that our notions are essentially equivalent to the ones introduced in [YY18].

Lemma 5.3.9. $(\mathsf{ind\text{-}cpa}, \mathsf{ulk\text{-}cpa}) \xrightarrow{1,1} \mathsf{ind\text{-}r\text{-}cpa}$.

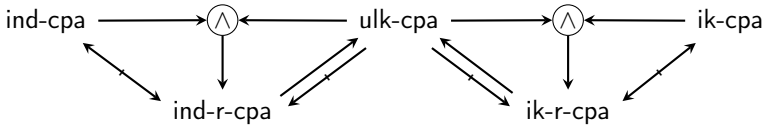


Figure 5.2: Relations among encryption and re-encryption security notions.

Proof. Let $(sk, pk) \leftarrow \mathtt{Gen}$ and consider $\rho(\llbracket \mathbf{X}, x \rrbracket) \doteq \llbracket \langle \mathbf{E}_x, \mathbf{X} \triangleright \mathbf{R} \rangle, x \rrbracket$. Then:

$$\begin{aligned}
\llbracket \mathbf{E}_{pk} \triangleright \langle *, \mathbf{R} \rangle, pk \rrbracket &\eqsim \llbracket \langle \mathbf{E}_{pk}, \mathbf{E}_{pk} \triangleright \mathbf{R} \rangle, pk \rrbracket && \text{(ulk-cpa)} \\
&= \rho(\llbracket \mathbf{E}_{pk}, pk \rrbracket) \\
&\eqsim \rho(\llbracket \mathbf{E}^{\$}_{pk}, pk \rrbracket) && \text{(ind-cpa)} \\
&= \llbracket \langle \mathbf{E}_{pk}, \mathbf{E}^{\$}_{pk} \triangleright \mathbf{R} \rangle, pk \rrbracket. && \square
\end{aligned}$$

Lemma 5.3.10. ind-cpa $\leftarrow\!\!\!\!\!\rightarrow$ ind-r-cpa.

Proof.

- ind-cpa $\not\rightarrow$ ind-r-cpa: Let $\Pi \doteq (\mathtt{Gen}, \mathtt{Enc}, \mathtt{Rnc}, \mathtt{Dec})$. For any $(sk, pk) \in \operatorname{supp} \mathtt{Gen}$, define $\Pi' \doteq (\mathtt{Gen}', \mathtt{Enc}', \mathtt{Rnc}', \mathtt{Dec}')$ as:
  - $\mathtt{Gen}' \doteq \mathtt{Gen}$;
  - $\mathtt{Enc}'_{pk}(m) \doteq \mathtt{Enc}_{pk}(m)$, for any $m \in \mathcal{M}$;
  - $\mathtt{Rnc}'(c) \doteq c$, for any $c \in \mathcal{C}$;
  - $\mathtt{Dec}'_{sk}(c) \doteq \mathtt{Dec}_{sk}(c)$, for any $c \in \mathcal{C}$;

  with corresponding systems $\mathbf{E}'_{pk}$, $\mathbf{R}'$, and $\mathbf{D}'_{sk}$. Let $(sk, pk) \leftarrow \mathtt{Gen}$. If Π is correct, then Π' is clearly also correct, and if

  $$\llbracket \mathbf{E}_{pk}, pk \rrbracket \eqsim \llbracket \mathbf{E}^{\$}_{pk}, pk \rrbracket,$$

  then

  $$\llbracket \mathbf{E}'_{pk}, pk \rrbracket \equiv \llbracket \mathbf{E}_{pk}, pk \rrbracket \eqsim \llbracket \mathbf{E}^{\$}_{pk}, pk \rrbracket \equiv \llbracket \mathbf{E}'^{\$}_{pk}, pk \rrbracket.$$

But clearly,

$$\begin{aligned}\llbracket \mathbf{E}'_{pk} \triangleright \langle *, \mathbf{R}' \rangle, pk \rrbracket &\equiv \llbracket \mathbf{E}_{pk} \triangleright \langle *, * \rangle, pk \rrbracket \\ &\not\equiv \llbracket \langle \mathbf{E}_{pk}, \mathbf{E}^{\$}_{pk} \rangle, pk \rrbracket \\ &\equiv \llbracket \langle \mathbf{E}_{pk}, \mathbf{E}^{\$}_{pk} \triangleright \mathbf{R} \rangle, pk \rrbracket.\end{aligned}$$

- ind-r-cpa $\not\longrightarrow$ ind-cpa: Let $\Pi \doteq (\mathtt{Gen}, \mathtt{Enc}, \mathtt{Rnc}, \mathtt{Dec})$. For any $(sk, pk) \in \operatorname{supp} \mathtt{Gen}$ and a fixed $\hat{m} \in \mathcal{M}$, define $\Pi' \doteq (\mathtt{Gen}', \mathtt{Enc}', \mathtt{Rnc}', \mathtt{Dec}')$ as:
  - $\mathtt{Gen}' \doteq \mathtt{Gen}$;
  - $\mathtt{Enc}'_{pk}(m) \doteq (\mathtt{Enc}_{pk}(m), \mathbb{1}\{m = \hat{m}\})$, for any $m \in \mathcal{M}$;
  - $\mathtt{Rnc}'((c, b)) \doteq (\mathtt{Rnc}(c), 0)$, for any $(c, b) \in \mathcal{C} \times \{0, 1\}$;
  - $\mathtt{Dec}'_{sk}((c, b)) \doteq \mathtt{Dec}_{sk}(c)$, for any $(c, b) \in \mathcal{C} \times \{0, 1\}$;

  with corresponding systems $\mathbf{E}'_{pk}$, $\mathbf{R}'$, and $\mathbf{D}'_{sk}$. Let $(sk, pk) \leftarrow \mathtt{Gen}$. If Π is correct, then Π' is clearly also correct, and if

$$\llbracket \mathbf{E}_{pk} \triangleright \langle *, \mathbf{R} \rangle, pk \rrbracket \eqsim \llbracket \langle \mathbf{E}_{pk}, \mathbf{E}^{\$}_{pk} \triangleright \mathbf{R} \rangle, pk \rrbracket,$$

  then with $\rho(\llbracket \mathbf{X}, x \rrbracket) \doteq \llbracket \langle *, * \rangle \triangleright (\!| \mathbf{X}, \langle \mathbb{1}_{\hat{m}}, 0 \rangle |\!)_{1,3,2,4}, x \rrbracket$,

$$\begin{aligned}\llbracket \mathbf{E}'_{pk} \triangleright \langle *, \mathbf{R}' \rangle, pk \rrbracket &\equiv \llbracket \langle *, * \rangle \triangleright (\!| \mathbf{E}_{pk} \triangleright \langle *, \mathbf{R} \rangle, \langle \mathbb{1}_{\hat{m}}, 0 \rangle |\!)_{1,3,2,4}, pk \rrbracket \\ &= \rho(\llbracket \mathbf{E}_{pk} \triangleright \langle *, \mathbf{R} \rangle, pk \rrbracket) \\ &\eqsim \rho(\llbracket \langle \mathbf{E}_{pk}, \mathbf{E}^{\$}_{pk} \triangleright \mathbf{R} \rangle, pk \rrbracket) \\ &= \llbracket \langle *, * \rangle \triangleright (\!| \langle \mathbf{E}_{pk}, \mathbf{E}^{\$}_{pk} \triangleright \mathbf{R} \rangle, \langle \mathbb{1}_{\hat{m}}, 0 \rangle |\!)_{1,3,2,4}, pk \rrbracket \\ &\equiv \llbracket \langle \mathbf{E}'_{pk}, \mathbf{E}'^{\$}_{pk} \triangleright \mathbf{R}' \rangle, pk \rrbracket.\end{aligned}$$

  But with random variable $B \in \{0, 1\}$ such that $\Pr[B = 1] = \frac{1}{|\mathcal{M}|}$,

$$\begin{aligned}\llbracket \mathbf{E}'_{pk}, pk \rrbracket &\equiv \llbracket \langle *, * \rangle \triangleright (\!| \mathbf{E}_{pk}, \mathbb{1}_{\hat{m}} |\!), pk \rrbracket \\ &\not\equiv \llbracket \langle *, * \rangle \triangleright (\!| \mathbf{E}^{\$}_{pk}, B |\!), pk \rrbracket \\ &\equiv \llbracket \mathbf{E}'^{\$}_{pk}, pk \rrbracket,\end{aligned}$$

  since clearly $\mathbb{1}_{\hat{m}} \not\equiv B$. □

Lemma 5.3.11. ind-r-cpa $\xrightarrow{2}$ ulk-cpa.

Proof. Let $(sk, pk) \leftarrow \mathtt{Gen}$ and consider $\rho(\llbracket \mathbf{X}, x \rrbracket) \doteq \llbracket \langle \mathbf{E}_x, (\mathbf{X})_2 \rangle, x \rrbracket$. Then:

$$\begin{aligned}
\llbracket \mathbf{E}_{pk} \triangleright \langle *, \mathbf{R} \rangle, pk \rrbracket &\eqsim \llbracket \langle \mathbf{E}_{pk}, \mathbf{E}^{\$}_{pk} \triangleright \mathbf{R} \rangle, pk \rrbracket && \text{(ind-r-cpa)} \\
&\equiv \llbracket \langle \mathbf{E}_{pk}, \langle \mathbf{E}_{pk}, \mathbf{E}^{\$}_{pk} \triangleright \mathbf{R} \rangle_2 \rangle, pk \rrbracket \\
&= \rho(\llbracket \langle \mathbf{E}_{pk}, \mathbf{E}^{\$}_{pk} \triangleright \mathbf{R} \rangle, pk \rrbracket) \\
&\eqsim \rho(\llbracket \mathbf{E}_{pk} \triangleright \langle *, \mathbf{R} \rangle, pk \rrbracket) && \text{(ind-r-cpa)} \\
&= \llbracket \langle \mathbf{E}_{pk}, (\mathbf{E}_{pk} \triangleright \langle *, \mathbf{R} \rangle)_2 \rangle, pk \rrbracket \\
&\equiv \llbracket \langle \mathbf{E}_{pk}, \mathbf{E}_{pk} \triangleright \mathbf{R} \rangle, pk \rrbracket. && \square
\end{aligned}$$

Lemma 5.3.12. ulk-cpa $\not\longrightarrow$ ind-r-cpa.

Proof. Let $\Pi \doteq (\mathtt{Gen}, \mathtt{Enc}, \mathtt{Rnc}, \mathtt{Dec})$. For any $(sk, pk) \in \operatorname{supp} \mathtt{Gen}$ and a fixed $\hat{m} \in \mathcal{M}$, define $\Pi' \doteq (\mathtt{Gen}', \mathtt{Enc}', \mathtt{Rnc}', \mathtt{Dec}')$ as:

- $\mathtt{Gen}' \doteq \mathtt{Gen}$;
- $\mathtt{Enc}'_{pk}(m) \doteq (\mathtt{Enc}_{pk}(m), \mathbb{1}\{m = \hat{m}\})$, for any $m \in \mathcal{M}$;
- $\mathtt{Rnc}'((c, b)) \doteq (\mathtt{Rnc}(c), b)$, for any $(c, b) \in \mathcal{C} \times \{0, 1\}$;
- $\mathtt{Dec}'_{sk}((c, b)) \doteq \mathtt{Dec}_{sk}(c)$, for any $(c, b) \in \mathcal{C} \times \{0, 1\}$;

with corresponding systems $\mathbf{E}'_{pk}$, $\mathbf{R}'$, and $\mathbf{D}'_{sk}$. Let $(sk, pk) \leftarrow \mathtt{Gen}$. If Π is correct, then Π' is clearly also correct, and if

$$\llbracket \mathbf{E}_{pk} \triangleright \langle *, \mathbf{R} \rangle, pk \rrbracket \eqsim \llbracket \langle \mathbf{E}_{pk}, \mathbf{E}_{pk} \triangleright \mathbf{R} \rangle, pk \rrbracket,$$

then with $\rho(\llbracket \mathbf{X}, x \rrbracket) \doteq \llbracket \langle *, * \rangle \triangleright (\!| \mathbf{X}, \langle \mathbb{1}_{\hat{m}}, \mathbb{1}_{\hat{m}} \rangle |\!)_{1,3,2,4}, x \rrbracket$,

$$\begin{aligned}
\llbracket \mathbf{E}'_{pk} \triangleright \langle *, \mathbf{R}' \rangle, pk \rrbracket &\equiv \llbracket \langle *, * \rangle \triangleright (\!| \mathbf{E}_{pk} \triangleright \langle *, \mathbf{R} \rangle, \langle \mathbb{1}_{\hat{m}}, \mathbb{1}_{\hat{m}} \rangle |\!)_{1,3,2,4}, pk \rrbracket \\
&= \rho(\llbracket \mathbf{E}_{pk} \triangleright \langle *, \mathbf{R} \rangle, pk \rrbracket) \\
&\eqsim \rho(\llbracket \langle \mathbf{E}_{pk}, \mathbf{E}_{pk} \triangleright \mathbf{R} \rangle, pk \rrbracket) \\
&= \llbracket \langle *, * \rangle \triangleright (\!| \langle \mathbf{E}_{pk}, \mathbf{E}_{pk} \triangleright \mathbf{R} \rangle, \langle \mathbb{1}_{\hat{m}}, \mathbb{1}_{\hat{m}} \rangle |\!)_{1,3,2,4}, pk \rrbracket \\
&\equiv \llbracket \langle \mathbf{E}'_{pk}, \mathbf{E}'_{pk} \triangleright \mathbf{R}' \rangle, pk \rrbracket.
\end{aligned}$$

But with random variable $B \in \{0,1\}$ such that $\Pr[B=1] = \frac{1}{|\mathcal{M}|}$,

$$\begin{aligned}\llbracket \mathbf{E}'_{pk} \triangleright \langle *, \mathbf{R}' \rangle, pk \rrbracket &\equiv \llbracket \langle *, * \rangle \triangleright (\!| \mathbf{E}_{pk} \triangleright \langle *, \mathbf{R} \rangle, \langle \mathbb{1}_{\hat{m}}, \mathbb{1}_{\hat{m}} \rangle |\!)_{1,3,2,4}, pk \rrbracket \\ &\not\equiv \llbracket \langle *, * \rangle \triangleright (\!| \langle \mathbf{E}_{pk}, \mathbf{E}^{\$}_{pk} \triangleright \mathbf{R} \rangle, \langle \mathbb{1}_{\hat{m}}, B \rangle |\!)_{1,3,2,4}, pk \rrbracket \\ &\equiv \llbracket \langle \mathbf{E}'_{pk}, \mathbf{E}'^{\$}_{pk} \triangleright \mathbf{R}' \rangle, pk \rrbracket.\end{aligned}$$

since clearly $\mathbb{1}_{\hat{m}} \not\equiv B$. □

Lemma 5.3.13. (ik-cpa, ulk-cpa) $\xrightarrow{1,2}$ ik-r-cpa.

Proof. Let $(sk_1, pk_1), (sk_2, pk_2) \leftarrow \mathtt{Gen}$, and consider

- $\rho_1(\llbracket \mathbf{X}, x \rrbracket) \doteq \llbracket \mathbf{X}, \mathbf{E}_{pk_2} \triangleright \langle *, \mathbf{R} \rangle, x, pk_2 \rrbracket$,
- $\rho_2(\llbracket \mathbf{X}, x \rrbracket) \doteq \llbracket \langle \mathbf{E}_{pk_1}, \mathbf{E}_{pk_1} \triangleright \mathbf{R} \rangle, \mathbf{X}, pk_1, x \rrbracket$, and
- $\rho_3(\llbracket \mathbf{X}, \mathbf{T}, x, y \rrbracket) \doteq \llbracket \langle \mathbf{E}_x, \mathbf{X} \triangleright \mathbf{R} \rangle, \langle \mathbf{E}_y, \mathbf{T} \triangleright \mathbf{R} \rangle, x, y \rrbracket$.

Then:

$$\begin{aligned}&\llbracket \mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R} \rangle, \mathbf{E}_{pk_2} \triangleright \langle *, \mathbf{R} \rangle, pk_1, pk_2 \rrbracket \\ &\quad = \rho_1(\llbracket \mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R} \rangle, pk_1 \rrbracket) \\ &\quad \mathrel{\widehat{=}} \rho_1(\llbracket \langle \mathbf{E}_{pk_1}, \mathbf{E}_{pk_1} \triangleright \mathbf{R} \rangle, pk_1 \rrbracket) && \text{(ulk-cpa)} \\ &\quad = \llbracket \langle \mathbf{E}_{pk_1}, \mathbf{E}_{pk_1} \triangleright \mathbf{R} \rangle, \mathbf{E}_{pk_2} \triangleright \langle *, \mathbf{R} \rangle, pk_1, pk_2 \rrbracket \\ &\quad = \rho_2(\llbracket \mathbf{E}_{pk_2} \triangleright \langle *, \mathbf{R} \rangle, pk_2 \rrbracket) \\ &\quad \mathrel{\widehat{=}} \rho_2(\llbracket \langle \mathbf{E}_{pk_2}, \mathbf{E}_{pk_2} \triangleright \mathbf{R} \rangle, pk_2 \rrbracket) && \text{(ulk-cpa)} \\ &\quad = \llbracket \langle \mathbf{E}_{pk_1}, \mathbf{E}_{pk_1} \triangleright \mathbf{R} \rangle, \langle \mathbf{E}_{pk_2}, \mathbf{E}_{pk_2} \triangleright \mathbf{R} \rangle, pk_1, pk_2 \rrbracket \\ &\quad = \rho_3(\llbracket \mathbf{E}_{pk_1}, \mathbf{E}_{pk_2}, pk_1, pk_2 \rrbracket) \\ &\quad \mathrel{\widehat{=}} \rho_3(\llbracket \mathbf{E}_{pk_1}, \mathbf{E}_{pk_1}, pk_1, pk_2 \rrbracket) && \text{(ik-cpa)} \\ &\quad = \llbracket \langle \mathbf{E}_{pk_1}, \mathbf{E}_{pk_1} \triangleright \mathbf{R} \rangle, \langle \mathbf{E}_{pk_2}, \mathbf{E}_{pk_1} \triangleright \mathbf{R} \rangle, pk_1, pk_2 \rrbracket. && \square\end{aligned}$$

Lemma 5.3.14. ik-cpa $\leftarrow\!\!\!\!\!\!\rightarrow$ ik-r-cpa.

Proof.

- ik-cpa $\not\rightarrow$ ik-r-cpa: Analogous to the case $\not\rightarrow$ in the proof of Lemma 5.3.10.

- ik-r-cpa $\not\longrightarrow$ ik-cpa: Let $\Pi \doteq (\mathtt{Gen}, \mathtt{Enc}, \mathtt{Rnc}, \mathtt{Dec})$. For any $(sk, pk) \in \operatorname{supp} \mathtt{Gen}$, define $\Pi' \doteq (\mathtt{Gen}', \mathtt{Enc}', \mathtt{Rnc}', \mathtt{Dec}')$ as:
  - $\mathtt{Gen}' \doteq \mathtt{Gen}$;
  - $\mathtt{Enc}'_{pk}(m) \doteq (\mathtt{Enc}_{pk}(m), pk)$, for any $m \in \mathcal{M}$;
  - $\mathtt{Rnc}'((c, pk')) \doteq (\mathtt{Rnc}(c), \bot)$, for any $(c, pk') \in \mathcal{C} \times (\mathcal{PK} \cup \{\bot\})$;
  - $\mathtt{Dec}'_{sk}((c, pk')) \doteq \mathtt{Dec}_{sk}(c)$, for any $(c, pk') \in \mathcal{C} \times (\mathcal{PK} \cup \{\bot\})$;

  with corresponding systems $\mathbf{E}'_{pk}$, $\mathbf{R}'$, and $\mathbf{D}'_{sk}$. Let (sk_1, pk_1), $(sk_2, pk_2) \leftarrow \mathtt{Gen}$. If Π is correct, then Π' is clearly also correct, and if

$$[\![\mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R}\rangle, \mathbf{E}_{pk_2} \triangleright \langle *, \mathbf{R}\rangle, pk_1, pk_2]\!] \\ \eqsim \\ [\![\mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R}\rangle, \langle \mathbf{E}_{pk_2}, \mathbf{E}_{pk_1} \triangleright \mathbf{R}\rangle, pk_1, pk_2]\!].$$

  then with

$$\rho([\![\mathbf{X}, \mathbf{Y}, x, y]\!]) \doteq [\![\mathbf{X} \triangleright (\!|\langle *, x\rangle, \langle *, \bot\rangle|\!), \mathbf{Y} \triangleright (\!|\langle *, y\rangle, \langle *, \bot\rangle|\!), x, y]\!],$$

$$\begin{aligned}
&[\![\mathbf{E}'_{pk_1} \triangleright \langle *, \mathbf{R}'\rangle, \mathbf{E}'_{pk_2} \triangleright \langle *, \mathbf{R}'\rangle, pk_1, pk_2]\!] \\
&\quad\equiv [\![\mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R}\rangle \triangleright (\!|\langle *, pk_1\rangle, \langle *, \bot\rangle|\!), \\
&\qquad \mathbf{E}_{pk_2} \triangleright \langle *, \mathbf{R}\rangle \triangleright (\!|\langle *, pk_2\rangle, \langle *, \bot\rangle|\!), pk_1, pk_2]\!] \\
&\quad= \rho([\![\mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R}\rangle, \mathbf{E}_{pk_2} \triangleright \langle *, \mathbf{R}\rangle, pk_1, pk_2]\!]) \\
&\quad\eqsim \rho([\![\mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R}\rangle, \langle \mathbf{E}_{pk_2}, \mathbf{E}_{pk_1} \triangleright \mathbf{R}\rangle, pk_1, pk_2]\!]) \\
&\quad= [\![\mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R}\rangle \triangleright (\!|\langle *, pk_1\rangle, \langle *, \bot\rangle|\!), \\
&\qquad \langle \mathbf{E}_{pk_2}, \mathbf{E}_{pk_1} \triangleright \mathbf{R}\rangle \triangleright (\!|\langle *, pk_2\rangle, \langle *, \bot\rangle|\!), pk_1, pk_2]\!] \\
&\quad\equiv [\![\mathbf{E}'_{pk_1} \triangleright \langle *, \mathbf{R}'\rangle, \langle \mathbf{E}_{pk_2}, \mathbf{E}'_{pk_1} \triangleright \mathbf{R}'\rangle, pk_1, pk_2]\!].
\end{aligned}$$

  But clearly,

$$\begin{aligned}
[\![\mathbf{E}'_{pk_1}, \mathbf{E}'_{pk_2}, pk_1, pk_2]\!] &\equiv [\![\mathbf{E}_{pk_1} \triangleright \langle *, pk_1\rangle, \mathbf{E}_{pk_2} \triangleright \langle *, pk_2\rangle, pk_1, pk_2]\!] \\
&\not\equiv [\![\mathbf{E}_{pk_1} \triangleright \langle *, pk_1\rangle, \mathbf{E}_{pk_1} \triangleright \langle *, pk_1\rangle, pk_1, pk_2]\!] \\
&\equiv [\![\mathbf{E}'_{pk_1}, \mathbf{E}'_{pk_1}, pk_1, pk_2]\!].
\end{aligned}$$

  □

Lemma 5.3.15. ik-r-cpa $\xrightarrow{2}$ ulk-cpa.

Proof. Let $(sk, pk), (sk', pk') \leftarrow \mathtt{Gen}$, and consider

- $\rho_1([\![\mathbf{X}, \mathbf{Y}, x, y]\!]) \doteq [\![\mathbf{Y}, y]\!]$ and
- $\rho_2([\![\mathbf{X}, \mathbf{Y}, x, y]\!]) \doteq [\![\langle \mathbf{E}_y, (\mathbf{Y})_2 \rangle, y]\!]$.

Then:

$$
\begin{aligned}
&[\![\mathbf{E}_{pk} \triangleright \langle *, \mathbf{R} \rangle, pk]\!] \\
&\quad = \rho_1([\![\mathbf{E}_{pk'} \triangleright \langle *, \mathbf{R} \rangle, \mathbf{E}_{pk} \triangleright \langle *, \mathbf{R} \rangle, pk', pk]\!]) \\
&\quad \mathrel{\hat{=}} \rho_1([\![\mathbf{E}_{pk'} \triangleright \langle *, \mathbf{R} \rangle, \langle \mathbf{E}_{pk}, \mathbf{E}_{pk'} \triangleright \mathbf{R} \rangle, pk', pk]\!]) && \text{(ik-r-cpa)} \\
&\quad = [\![\langle \mathbf{E}_{pk}, \mathbf{E}_{pk'} \triangleright \mathbf{R} \rangle, pk]\!] \\
&\quad \equiv [\![\langle \mathbf{E}_{pk}, \langle \mathbf{E}_{pk}, \mathbf{E}_{pk'} \triangleright \mathbf{R} \rangle_2 \rangle, pk]\!] \\
&\quad = \rho_2([\![\mathbf{E}_{pk'} \triangleright \langle *, \mathbf{R} \rangle, \langle \mathbf{E}_{pk}, \mathbf{E}_{pk'} \triangleright \mathbf{R} \rangle, pk', pk]\!]) \\
&\quad \mathrel{\hat{=}} \rho_2([\![\mathbf{E}_{pk'} \triangleright \langle *, \mathbf{R} \rangle, \mathbf{E}_{pk} \triangleright \langle *, \mathbf{R} \rangle, pk', pk]\!]) && \text{(ik-r-cpa)} \\
&\quad = [\![\langle \mathbf{E}_{pk}, (\mathbf{E}_{pk} \triangleright \langle *, \mathbf{R} \rangle)_2 \rangle, pk]\!] \\
&\quad \equiv [\![\langle \mathbf{E}_{pk}, \mathbf{E}_{pk} \triangleright \mathbf{R} \rangle, pk]\!]. && \square
\end{aligned}
$$

Lemma 5.3.16. ulk-cpa $\not\longrightarrow$ ik-r-cpa.

Proof. Let $\Pi \doteq (\mathtt{Gen}, \mathtt{Enc}, \mathtt{Rnc}, \mathtt{Dec})$. For any $(sk, pk) \in \operatorname{supp} \mathtt{Gen}$, define $\Pi' \doteq (\mathtt{Gen}', \mathtt{Enc}', \mathtt{Rnc}', \mathtt{Dec}')$ as:

- $\mathtt{Gen}' \doteq \mathtt{Gen}$;
- $\mathtt{Enc}'_{pk}(m) \doteq (\mathtt{Enc}_{pk}(m), pk)$, for any $m \in \mathcal{M}$;
- $\mathtt{Rnc}'((c, pk')) \doteq (\mathtt{Rnc}(c), pk')$, for any $(c, pk') \in \mathcal{C} \times (\mathcal{PK} \cup \{\bot\})$;
- $\mathtt{Dec}'_{sk}((c, pk')) \doteq \mathtt{Dec}_{sk}(c)$, for any $(c, pk') \in \mathcal{C} \times (\mathcal{PK} \cup \{\bot\})$;

with corresponding systems $\mathbf{E}'_{pk}$, $\mathbf{R}'$, and $\mathbf{D}'_{sk}$. Let $(sk, pk) \leftarrow \mathtt{Gen}$. If Π is correct, then Π' is clearly also correct, and if

$$[\![\mathbf{E}_{pk} \triangleright \langle *, \mathbf{R} \rangle, pk]\!] \mathrel{\hat{=}} [\![\langle \mathbf{E}_{pk}, \mathbf{E}_{pk} \triangleright \mathbf{R} \rangle, pk]\!],$$

then with $\rho([\![\mathbf{X}, x]\!]) \doteq [\![\mathbf{X} \triangleright (\!|\langle *, x\rangle, \langle *, x\rangle|\!), x]\!]$,

$$\begin{aligned}
[\![\mathbf{E}'_{pk} \triangleright \langle *, \mathbf{R}'\rangle, pk]\!] &\equiv [\![\mathbf{E}_{pk} \triangleright \langle *, \mathbf{R}\rangle \triangleright (\!|\langle *, pk\rangle, \langle *, pk\rangle|\!), pk]\!] \\
&= \rho([\![\mathbf{E}_{pk} \triangleright \langle *, \mathbf{R}\rangle, pk]\!]) \\
&\eqsim \rho([\![\langle \mathbf{E}_{pk}, \mathbf{E}_{pk} \triangleright \mathbf{R}\rangle, pk]\!]) \\
&= [\![\langle \mathbf{E}_{pk}, \mathbf{E}_{pk} \triangleright \mathbf{R}\rangle \triangleright (\!|\langle *, pk\rangle, \langle *, pk\rangle|\!), pk]\!] \\
&\equiv [\![\langle \mathbf{E}'_{pk}, \mathbf{E}'_{pk} \triangleright \mathbf{R}'\rangle, pk]\!].
\end{aligned}$$

But clearly, for $(sk_1, pk_1), (sk_2, pk_2) \leftarrow \mathtt{Gen}$,

$$\begin{aligned}
&[\![\mathbf{E}'_{pk_1} \triangleright \langle *, \mathbf{R}'\rangle, \mathbf{E}'_{pk_2} \triangleright \langle *, \mathbf{R}'\rangle, pk_1, pk_2]\!] \\
&\quad\equiv [\![\mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R}\rangle \triangleright (\!|\langle *, pk_1\rangle, \langle *, pk_1\rangle|\!), \\
&\qquad \mathbf{E}_{pk_2} \triangleright \langle *, \mathbf{R}\rangle \triangleright (\!|\langle *, pk_2\rangle, \langle *, pk_2\rangle|\!), pk_1, pk_2]\!] \\
&\quad\not\equiv [\![\mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R}\rangle \triangleright (\!|\langle *, pk_1\rangle, \langle *, pk_1\rangle|\!), \\
&\qquad \langle \mathbf{E}_{pk_2}, \mathbf{E}_{pk_1} \triangleright \mathbf{R}\rangle \triangleright (\!|\langle *, pk_2\rangle, \langle *, pk_1\rangle|\!), pk_1, pk_2]\!] \\
&\quad\equiv [\![\mathbf{E}'_{pk_1} \triangleright \langle *, \mathbf{R}'\rangle, \langle \mathbf{E}_{pk_2}, \mathbf{E}'_{pk_1} \triangleright \mathbf{R}'\rangle, pk_1, pk_2]\!].
\end{aligned}$$

□

Stronger Unlinkability. We next show that the strong unlinkability notion sulk-cpa we put forth is significantly stronger than the conventional unlinkability notion ulk-cpa. In the proof of Lemma 5.3.18 we used a minimal counterexample, but if instead of a bit $b \in \{0,1\}$ we would append a counter $t \in \{0,1\}^k$, for some $k \in \mathbb{N}$, to the underlying ciphertext (initialized to 0 by Enc, increased by 1 by Rnc, and ignored by Dec), the proof would still go through. This makes it evident that ulk-cpa is weaker than sulk-cpa in the sense that, in general, *a* ulk-cpa*-secure scheme does not hide the number of re-encryptions a ciphertext went through.* In practice, this translates into such a scheme not hiding the number of hops a message goes through in a mixnet, which is a property that was ignored in [YY18].

Lemma 5.3.17. sulk-cpa $\xrightarrow{2}$ ulk-cpa.

Proof. Let $(sk, pk) \leftarrow \mathtt{Gen}$ and consider $\rho([\![\mathbf{X}, x]\!]) \doteq [\![\mathbf{E}_x, (\mathbf{X})_2, x]\!]$. Then:

$$\begin{aligned}
[\![\mathbf{E}_{pk} \triangleright \langle *, \mathbf{R}\rangle, pk]\!] &\eqsim [\![\langle \mathbf{E}_{pk}, \mathbf{E}_{pk}\rangle, pk]\!] && \text{(sulk-cpa)}\\
&\equiv [\![\langle \mathbf{E}_{pk}, \langle \mathbf{E}_{pk}, \mathbf{E}_{pk}\rangle_2\rangle, pk]\!]\\
&= \rho([\![\langle \mathbf{E}_{pk}, \mathbf{E}_{pk}\rangle, pk]\!])\\
&\eqsim \rho([\![\mathbf{E}_{pk} \triangleright \langle *, \mathbf{R}\rangle, pk]\!]) && \text{(sulk-cpa)}\\
&= [\![\langle \mathbf{E}_{pk}, (\mathbf{E}_{pk} \triangleright \langle *, \mathbf{R}\rangle)_2\rangle, pk]\!]\\
&\equiv [\![\langle \mathbf{E}_{pk}, \mathbf{E}_{pk} \triangleright \mathbf{R}\rangle, pk]\!]. && \square
\end{aligned}$$

Lemma 5.3.18. ulk-cpa $\not\longrightarrow$ sulk-cpa.

Proof. Let $\Pi \doteq (\mathtt{Gen}, \mathtt{Enc}, \mathtt{Rnc}, \mathtt{Dec})$. For any $(sk, pk) \in \operatorname{supp} \mathtt{Gen}$, define $\Pi' \doteq (\mathtt{Gen}', \mathtt{Enc}', \mathtt{Rnc}', \mathtt{Dec}')$ as:

- $\mathtt{Gen}' \doteq \mathtt{Gen}$;
- $\mathtt{Enc}'_{pk}(m) \doteq (\mathtt{Enc}_{pk}(m), 0)$, for any $m \in \mathcal{M}$;
- $\mathtt{Rnc}'((c, b)) \doteq (\mathtt{Rnc}(c), 1)$, for any $(c, b) \in \mathcal{C} \times \{0, 1\}$;
- $\mathtt{Dec}'_{sk}((c, b)) \doteq \mathtt{Dec}_{sk}(c)$, for any $(c, b) \in \mathcal{C} \times \{0, 1\}$;

with corresponding systems $\mathbf{E}'_{pk}$, $\mathbf{R}'$, and $\mathbf{D}'_{sk}$. Let $(sk, pk) \leftarrow \mathtt{Gen}$. If Π is correct, then Π' is clearly also correct, and if

$$[\![\mathbf{E}_{pk} \triangleright \langle *, \mathbf{R}\rangle, pk]\!] \eqsim [\![\langle \mathbf{E}_{pk}, \mathbf{E}_{pk} \triangleright \mathbf{R}\rangle, pk]\!],$$

then with $\rho([\![\mathbf{X}, x]\!]) \doteq [\![\mathbf{X} \triangleright (\!|\langle *, 0\rangle, \langle *, 1\rangle|\!), x]\!]$,

$$\begin{aligned}
[\![\mathbf{E}'_{pk} \triangleright \langle *, \mathbf{R}'\rangle, pk]\!] &\equiv [\![\mathbf{E}_{pk} \triangleright \langle *, \mathbf{R}\rangle \triangleright (\!|\langle *, 0\rangle, \langle *, 1\rangle|\!), pk]\!]\\
&= \rho([\![\mathbf{E}_{pk} \triangleright \langle *, \mathbf{R}\rangle, pk]\!])\\
&\eqsim \rho([\![\langle \mathbf{E}_{pk}, \mathbf{E}_{pk} \triangleright \mathbf{R}\rangle, pk]\!])\\
&= [\![\langle \mathbf{E}_{pk}, \mathbf{E}_{pk} \triangleright \mathbf{R}\rangle \triangleright (\!|\langle *, 0\rangle, \langle *, 1\rangle|\!), pk]\!]\\
&\equiv [\![\langle \mathbf{E}'_{pk}, \mathbf{E}'_{pk} \triangleright \mathbf{R}'\rangle, pk]\!].
\end{aligned}$$

But clearly,

$$\begin{aligned}
[\![\mathbf{E}'_{pk} \triangleright \langle *, \mathbf{R}'\rangle, pk]\!] &\equiv [\![\mathbf{E}_{pk} \triangleright \langle *, \mathbf{R}\rangle \triangleright (\!|\langle *, 0\rangle, \langle *, 1\rangle|\!), pk]\!]\\
&\neq [\![\langle \mathbf{E}_{pk}, \mathbf{E}_{pk}\rangle \triangleright (\!|\langle *, 0\rangle, \langle *, 0\rangle|\!), pk]\!]\\
&\equiv [\![\langle \mathbf{E}'_{pk}, \mathbf{E}'_{pk}\rangle, pk]\!]. && \square
\end{aligned}$$

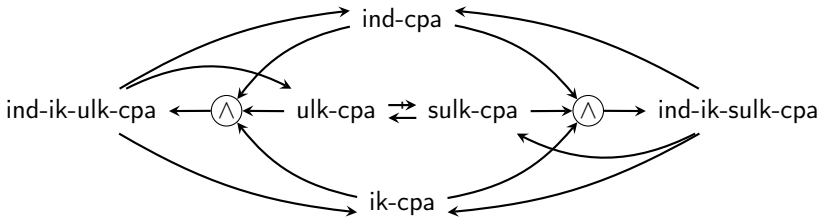


Figure 5.3: Relations among combined notions.

5.3.4 Combined Notions

In this section we introduce three notions that capture more security guarantees at once, which will be easier to relate to the composable notions we will introduce later. Figure 5.3 summarizes all relations (both implications and separations) that we show in this section. Furthermore, in Appendix B.1.3 we describe a different combined notion, ind-ik-r-cpa, that would result by naturally combining Young and Yung's ind-r-cpa and ik-r-cpa notions (but which is less directly relatable to our composable notions). There, we also show some implications and separations. Finally, in Section 5.5, we show that the original URE scheme based on ElGamal form [GJJS04] satisfies our strongest notion ind-ik-sulk-cpa.

For the combined notion of *correctness and robustness* (cor-rob), we want to be able to substitute a pair of systems $\mathbf{S}_1$ and $\mathbf{S}_2$ depending on two independent key-pairs (sk_1, pk_1) and (sk_2, pk_2), where system $\mathbf{S}_i$, for $i \in [2]$, on input a tuple $(m, t, j) \in \mathcal{M} \times \mathbb{N} \times [2]$ encrypts m using pk_i, re-encrypts the resulting ciphertext t times, decrypts it with key sk_j, and outputs the resulting message (or $\bot$), by a pair of systems where $\mathbf{S}_i$, on input (m, t, j), always outputs m if $j = i$ and $\bot$ otherwise.

Definition 5.3.19 (cor-rob)**.**

$$[\![(\!|\mathbf{E}_{pk_1}, *, *|\!) \triangleright (\!|\mathbf{R}^*, *|\!) \triangleright \mathbf{D}_{sk_1,sk_2}, (\!|\mathbf{E}_{pk_2}, *, *|\!) \triangleright (\!|\mathbf{R}^*, *|\!) \triangleright \mathbf{D}_{sk_1,sk_2}, pk_1, pk_2]\!]$$
$$\eqsim$$
$$[\![(\!|*, \bot, *|\!) \triangleright \langle *, * \rangle_*, (\!|*, \bot, *|\!)_{2,1,3} \triangleright \langle *, * \rangle_*, pk_1, pk_2]\!],$$

for independent $(sk_1, pk_1), (sk_2, pk_2) \leftarrow \mathtt{Gen}$.

For the combined notion of *confidentiality, anonymity, and unlinkability* (ind-ik-ulk-cpa), we want to be able to substitute a pair of systems that encrypt and then re-encrypt under two independent keys, by a pair of systems both first sampling $\tilde{m}$, producing two independent encryptions of $\tilde{m}$ under the first key, and only re-encrypting the second ciphertext.

Definition 5.3.20 (ind-ik-ulk-cpa)**.**

$$[\![\mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R}\rangle, \mathbf{E}_{pk_2} \triangleright \langle *, \mathbf{R}\rangle, pk_1, pk_2]\!]$$
$$\eqsim$$
$$[\![\langle \mathbf{E}^{\$}_{pk_1}, \mathbf{E}^{\$}_{pk_1} \triangleright \mathbf{R}\rangle, \langle \mathbf{E}^{\$}_{pk_1}, \mathbf{E}^{\$}_{pk_1} \triangleright \mathbf{R}\rangle, pk_1, pk_2]\!],$$

for independent $(sk_1, pk_1), (sk_2, pk_2) \leftarrow \mathtt{Gen}$.

For the combined notion of *confidentiality, anonymity, and unlinkability* (ind-ik-ulk-cpa), we want to be able to substitute a pair of systems that encrypt and then re-encrypt under two independent keys, by a pair of systems both first sampling $\tilde{m}$, and producing two independent encryptions of $\tilde{m}$ under the first key.

Definition 5.3.21 (ind-ik-sulk-cpa)**.**

$$[\![\mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R}\rangle, \mathbf{E}_{pk_2} \triangleright \langle *, \mathbf{R}\rangle, pk_1, pk_2]\!]$$
$$\eqsim$$
$$[\![\langle \mathbf{E}^{\$}_{pk_1}, \mathbf{E}^{\$}_{pk_1}\rangle, \langle \mathbf{E}^{\$}_{pk_1}, \mathbf{E}^{\$}_{pk_1}\rangle, pk_1, pk_2]\!],$$

for independent $(sk_1, pk_1), (sk_2, pk_2) \leftarrow \mathtt{Gen}$.

In the following, (as well as in Appendix B.1.3), some proofs (of both implications and separations) use the exact same sequence of transformations as previous proofs (but on possibly different systems). In such cases, instead of essentially repeating the exact same argument, we say that the proof is *analogous* to a previous one.

Lemma 5.3.22. (cor, rob) $\iff$ cor-rob.

Proof.

- (cor, rob) $\xrightarrow{2,2}$ cor-rob: Let $(sk_1, pk_1), (sk_2, pk_2) \leftarrow \mathtt{Gen}$, and consider

– $\rho_1(\llbracket \mathbf{X}, x \rrbracket)$
$$\doteq \llbracket \langle \mathbf{X}, (\!|\mathbf{E}_x, *|\!) \triangleright \mathbf{R}^* \triangleright \mathbf{D}_{sk_2} \rangle_*, \langle (\!|\mathbf{E}_{pk_2}, *|\!) \triangleright \mathbf{R}^* \triangleright \mathbf{D}_{sk_1}, (\!|\mathbf{E}_{pk_2}, *|\!) \triangleright \mathbf{R}^* \triangleright \mathbf{D}_{sk_2} \rangle_*, x, pk_2 \rrbracket,$$
– $\rho_2(\llbracket \mathbf{X}, x \rrbracket)$
$$\doteq \llbracket \langle (\!|*, *|\!)_1, (\!|\mathbf{E}_{pk_1}, *|\!) \triangleright \mathbf{R}^* \triangleright \mathbf{D}_{sk_2} \rangle_*, \langle (\!|\mathbf{E}_x, *|\!) \triangleright \mathbf{R}^* \triangleright \mathbf{D}_{sk_1}, \mathbf{X} \rangle_*, pk_1, x \rrbracket,$$
– $\rho_3(\llbracket \mathbf{X}, x, y \rrbracket)$
$$\doteq \llbracket \langle (\!|*, *|\!)_1, \mathbf{X} \rangle_*, \langle (\!|\mathbf{E}_y, *|\!) \triangleright \mathbf{R}^* \triangleright \mathbf{D}_{sk_1}, (\!|*, *|\!)_1 \rangle_*, x, y \rrbracket, \text{ and}$$
– $\rho_4(\llbracket \mathbf{X}, x, y \rrbracket) \doteq \llbracket \langle (\!|*, *|\!)_1, (\!|\bot, *|\!)_1 \rangle_*, \langle \mathbf{X}, (\!|*, *|\!)_1 \rangle_*, y, x \rrbracket.$

Then:

$$\begin{aligned}
&\llbracket (\!|\mathbf{E}_{pk_1}, *, *|\!) \triangleright (\!|\mathbf{R}^*, *|\!) \triangleright \mathbf{D}_{sk_1,sk_2}, (\!|\mathbf{E}_{pk_2}, *, *|\!) \triangleright (\!|\mathbf{R}^*, *|\!) \triangleright \mathbf{D}_{sk_1,sk_2}, \\
&\qquad pk_1, pk_2 \rrbracket \\
&\quad \equiv \llbracket \langle (\!|\mathbf{E}_{pk_1}, *|\!) \triangleright \mathbf{R}^* \triangleright \mathbf{D}_{sk_1}, (\!|\mathbf{E}_{pk_1}, *|\!) \triangleright \mathbf{R}^* \triangleright \mathbf{D}_{sk_2} \rangle_*, \\
&\qquad \langle (\!|\mathbf{E}_{pk_2}, *|\!) \triangleright \mathbf{R}^* \triangleright \mathbf{D}_{sk_1}, (\!|\mathbf{E}_{pk_2}, *|\!) \triangleright \mathbf{R}^* \triangleright \mathbf{D}_{sk_2} \rangle_*, pk_1, pk_2 \rrbracket \\
&\quad = \rho_1(\llbracket (\!|\mathbf{E}_{pk_1}, *|\!) \triangleright \mathbf{R}^* \triangleright \mathbf{D}_{sk_1}, pk_1 \rrbracket) \\
&\quad \hat{=} \rho_1(\llbracket (\!|*, *|\!)_1, pk_1 \rrbracket) \qquad \text{(cor)} \\
&\quad = \llbracket \langle (\!|*, *|\!)_1, (\!|\mathbf{E}_{pk_1}, *|\!) \triangleright \mathbf{R}^* \triangleright \mathbf{D}_{sk_2} \rangle_*, \\
&\qquad \langle (\!|\mathbf{E}_{pk_2}, *|\!) \triangleright \mathbf{R}^* \triangleright \mathbf{D}_{sk_1}, (\!|\mathbf{E}_{pk_2}, *|\!) \triangleright \mathbf{R}^* \triangleright \mathbf{D}_{sk_2} \rangle_*, pk_1, pk_2 \rrbracket \\
&\quad = \rho_2(\llbracket (\!|\mathbf{E}_{pk_2}, *|\!) \triangleright \mathbf{R}^* \triangleright \mathbf{D}_{sk_2}, pk_2 \rrbracket) \\
&\quad \hat{=} \rho_2(\llbracket (\!|*, *|\!)_1, pk_2 \rrbracket) \qquad \text{(cor)} \\
&\quad = \llbracket \langle (\!|*, *|\!)_1, (\!|\mathbf{E}_{pk_1}, *|\!) \triangleright \mathbf{R}^* \triangleright \mathbf{D}_{sk_2} \rangle_*, \\
&\qquad \langle (\!|\mathbf{E}_{pk_2}, *|\!) \triangleright \mathbf{R}^* \triangleright \mathbf{D}_{sk_1}, (\!|*, *|\!)_1 \rangle_*, pk_1, pk_2 \rrbracket \\
&\quad = \rho_3(\llbracket (\!|\mathbf{E}_{pk_1}, *|\!) \triangleright \mathbf{R}^* \triangleright \mathbf{D}_{sk_2}, pk_1, pk_2 \rrbracket) \\
&\quad \hat{=} \rho_3(\llbracket (\!|\bot, *|\!)_1, pk_1, pk_2 \rrbracket) \qquad \text{(rob)} \\
&\quad = \llbracket \langle (\!|*, *|\!)_1, (\!|\bot, *|\!)_1 \rangle_*, \langle \mathbf{E}_{pk_2} \triangleright \mathbf{R}^* \triangleright \mathbf{D}_{sk_1}, (\!|*, *|\!)_1 \rangle_*, pk_1, pk_2 \rrbracket \\
&\quad = \rho_4(\llbracket (\!|\mathbf{E}_{pk_2}, *|\!) \triangleright \mathbf{R}^* \triangleright \mathbf{D}_{sk_1}, pk_2, pk_1 \rrbracket) \\
&\quad \hat{=} \rho_4(\llbracket (\!|\bot, *|\!)_1, pk_2, pk_1 \rrbracket) \qquad \text{(rob)} \\
&\quad = \llbracket \langle (\!|*, *|\!)_1, (\!|\bot, *|\!)_1 \rangle_*, \langle (\!|\bot, *|\!)_1, (\!|*, *|\!)_1 \rangle_*, pk_1, pk_2 \rrbracket \\
&\quad \equiv \llbracket (\!|*, \bot, *|\!) \triangleright \langle *, * \rangle_*, (\!|*, \bot, *|\!)_{2,1,3} \triangleright \langle *, * \rangle_*, pk_1, pk_2 \rrbracket.
\end{aligned}$$

- cor-rob $\xrightarrow{1}$ cor: Let $(sk_1, pk_1), (sk_2, pk_2) \leftarrow \mathtt{Gen}$, and consider $\rho([\![\mathbf{X}, \mathbf{Y}, x, y]\!]) \doteq [\![(\!|*, \langle *, 1\rangle|\!) \triangleright \mathbf{X}, x]\!]$. Then:

$$
\begin{aligned}
&[\![(\!|\mathbf{E}_{pk_1}, *|\!) \triangleright \mathbf{R}^* \triangleright \mathbf{D}_{sk_1}, pk_1]\!] \\
&\quad \equiv [\![(\!|*, \langle *, 1\rangle|\!) \triangleright (\!|\mathbf{E}_{pk_1}, *, *|\!) \triangleright (\!|\mathbf{R}^*, *|\!) \triangleright \mathbf{D}_{sk_1,sk_2}, pk]\!] \\
&\quad = \rho([\![(\!|\mathbf{E}_{pk_1}, *, *|\!) \triangleright (\!|\mathbf{R}^*, *|\!) \triangleright \mathbf{D}_{sk_1,sk_2}, \\
&\qquad (\!|\mathbf{E}_{pk_2}, *, *|\!) \triangleright (\!|\mathbf{R}^*, *|\!) \triangleright \mathbf{D}_{sk_1,sk_2}, pk_1, pk_2]\!]) \\
&\quad \doteq \rho([\![(\!|*, \bot, *|\!) \triangleright \langle *, *\rangle_*, \\
&\qquad (\!|*, \bot, *|\!)_{2,1,3} \triangleright \langle *, *\rangle_*, pk_1, pk_2]\!]) \qquad \text{(cor-rob)} \\
&\quad = [\![(\!|*, \langle *, 1\rangle|\!) \triangleright (\!|*, \bot, *|\!) \triangleright \langle *, *\rangle_*, pk_1]\!] \\
&\quad \equiv [\![(\!|*, *|\!)_1, pk_1]\!],
\end{aligned}
$$

- cor-rob $\xrightarrow{1}$ rob: Let $(sk_1, pk_1), (sk_2, pk_2) \leftarrow \mathtt{Gen}$, and consider $\rho([\![\mathbf{X}, \mathbf{Y}, x, y]\!]) \doteq [\![(\!|*, \langle *, 2\rangle|\!) \triangleright \mathbf{X}, x]\!]$. Then:

$$
\begin{aligned}
&[\![(\!|\mathbf{E}_{pk_1}, *|\!) \triangleright \mathbf{R}^* \triangleright \mathbf{D}_{sk_2}, pk_1, pk_2]\!] \\
&\quad \equiv [\![(\!|*, \langle *, 2\rangle|\!) \triangleright (\!|\mathbf{E}_{pk_1}, *, *|\!) \triangleright (\!|\mathbf{R}^*, *|\!) \triangleright \mathbf{D}_{sk_1,sk_2}, pk_1, pk_2]\!] \\
&\quad = \rho([\![(\!|\mathbf{E}_{pk_1}, *, *|\!) \triangleright (\!|\mathbf{R}^*, *|\!) \triangleright \mathbf{D}_{sk_1,sk_2}, \\
&\qquad (\!|\mathbf{E}_{pk_2}, *, *|\!) \triangleright (\!|\mathbf{R}^*, *|\!) \triangleright \mathbf{D}_{sk_1,sk_2}, pk_1, pk_2]\!]) \\
&\quad \doteq \rho([\![(\!|*, \bot, *|\!) \triangleright \langle *, *\rangle_*, \\
&\qquad (\!|*, \bot, *|\!)_{2,1,3} \triangleright \langle *, *\rangle_*, pk_1, pk_2]\!]) \qquad \text{(cor-rob)} \\
&\quad = [\![(\!|*, \langle *, 2\rangle|\!) \triangleright (\!|*, \bot, *|\!) \triangleright \langle *, *\rangle_*, pk_1, pk_2]\!] \\
&\quad \equiv [\![\bot, pk_1, pk_2]\!]. \qquad \square
\end{aligned}
$$

Lemma 5.3.23. (ind-cpa, ik-cpa, ulk-cpa) $\xrightarrow{1,1,1}$ ind-ik-ulk-cpa.

Proof. Let $(sk_1, pk_1), (sk_2, pk_2) \leftarrow \mathtt{Gen}$, and consider

- $\rho_1([\![\mathbf{X}, \mathbf{Y}, x, y]\!]) \doteq [\![\mathbf{X} \triangleright \langle *, \mathbf{R}\rangle, \mathbf{Y} \triangleright \langle *, \mathbf{R}\rangle, x, y]\!]$,
- $\rho_2([\![\mathbf{X}, x]\!]) \doteq [\![\mathbf{X}, \mathbf{X}, x, pk_2]\!]$, and
- $\rho_3([\![\mathbf{X}, x]\!]) \doteq [\![\langle \mathbf{X}, \mathbf{X} \triangleright \mathbf{R}\rangle, \langle \mathbf{X}, \mathbf{X} \triangleright \mathbf{R}\rangle, x, pk_2]\!]$.

Then:

$$\begin{aligned}
&[\![\mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R}\rangle, \mathbf{E}_{pk_2} \triangleright \langle *, \mathbf{R}\rangle, pk_1, pk_2]\!] \\
&\quad = \rho_1([\![\mathbf{E}_{pk_1}, \mathbf{E}_{pk_2}, pk_1, pk_2]\!]) \\
&\quad \mathrel{\hat{=}} \rho_1([\![\mathbf{E}_{pk_1}, \mathbf{E}_{pk_1}, pk_1, pk_2]\!]) && \text{(ik-cpa)} \\
&\quad = [\![\mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R}\rangle, \mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R}\rangle, pk_1, pk_2]\!] \\
&\quad = \rho_2([\![\mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R}\rangle, pk_1]\!]) \\
&\quad \mathrel{\hat{=}} \rho_2([\![\langle \mathbf{E}_{pk_1}, \mathbf{E}_{pk_1} \triangleright \mathbf{R}\rangle, pk_1]\!]) && \text{(ulk-cpa)} \\
&\quad = [\![\langle \mathbf{E}_{pk_1}, \mathbf{E}_{pk_1} \triangleright \mathbf{R}\rangle, \langle \mathbf{E}_{pk_1}, \mathbf{E}_{pk_1} \triangleright \mathbf{R}\rangle, pk_1, pk_2]\!] \\
&\quad = \rho_3([\![\mathbf{E}_{pk_1}, pk_1]\!]) \\
&\quad \mathrel{\hat{=}} \rho_3([\![\mathbf{E}^{\$}_{pk_1}, pk_1]\!]) && \text{(ind-cpa)} \\
&\quad = [\![\langle \mathbf{E}^{\$}_{pk_1}, \mathbf{E}^{\$}_{pk_1} \triangleright \mathbf{R}\rangle, \langle \mathbf{E}^{\$}_{pk_1}, \mathbf{E}^{\$}_{pk_1} \triangleright \mathbf{R}\rangle, pk_1, pk_2]\!]. && \square
\end{aligned}$$

Lemma 5.3.24. $(\mathsf{ind\text{-}cpa}, \mathsf{ik\text{-}cpa}, \mathsf{sulk\text{-}cpa}) \xrightarrow{1,1,1} \mathsf{ind\text{-}ik\text{-}sulk\text{-}cpa}$.

Proof. As for Lemma 5.3.23, but with

$$\rho_3([\![\mathbf{X}, x]\!]) \doteq [\![\langle \mathbf{X}, \mathbf{X}\rangle, \langle \mathbf{X}, \mathbf{X}\rangle, x, pk_2]\!]. \qquad \square$$

Lemma 5.3.25. $\mathsf{ind\text{-}ik\text{-}ulk\text{-}cpa} \xrightarrow{1} \mathsf{ind\text{-}cpa}$.

Proof. Let $(sk, pk) \leftarrow \mathtt{Gen}$ and consider $\rho([\![\mathbf{X}, \mathbf{Y}, x, y]\!]) \doteq [\![(\mathbf{X})_1, x]\!]$. Then:

$$\begin{aligned}
[\![\mathbf{E}_{pk}, pk]\!] &\equiv [\![(\mathbf{E}_{pk} \triangleright \langle *, \mathbf{R}\rangle)_1, pk]\!] \\
&= \rho([\![\mathbf{E}_{pk} \triangleright \langle *, \mathbf{R}\rangle, \mathbf{E}_{pk'} \triangleright \langle *, \mathbf{R}\rangle, pk, pk']\!]) \\
&\mathrel{\hat{=}} \rho([\![\langle \mathbf{E}^{\$}_{pk}, \mathbf{E}^{\$}_{pk} \triangleright \mathbf{R}\rangle, \langle \mathbf{E}^{\$}_{pk}, \mathbf{E}^{\$}_{pk} \triangleright \mathbf{R}\rangle, pk, pk']\!]) \quad \text{(ind-ik-ulk-cpa)} \\
&= [\![\langle \mathbf{E}^{\$}_{pk}, \mathbf{E}^{\$}_{pk} \triangleright \mathbf{R}\rangle_1, pk]\!] \\
&\equiv [\![\mathbf{E}^{\$}_{pk}, pk]\!]. && \square
\end{aligned}$$

Lemma 5.3.26. $\mathsf{ind\text{-}ik\text{-}ulk\text{-}cpa} \xrightarrow{2} \mathsf{ik\text{-}cpa}$.

Proof. Let $(sk_1, pk_1), (sk_2, pk_2) \leftarrow \mathtt{Gen}$, and consider

- $\rho_1([\![\mathbf{X}, \mathbf{Y}, x, y]\!]) \doteq [\![(\mathbf{X})_1, (\mathbf{Y})_1, x, y]\!]$ and

- $\rho_2(\llbracket \mathbf{X}, \mathbf{Y}, x, y \rrbracket) \doteq \llbracket (\mathbf{X})_1, (\mathbf{X})_1, x, y \rrbracket$.

Then:

$$
\begin{aligned}
&\llbracket \mathbf{E}_{pk_1}, \mathbf{E}_{pk_2}, pk_1, pk_2 \rrbracket \\
&\quad \equiv \llbracket (\mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R} \rangle)_1, (\mathbf{E}_{pk_2} \triangleright \langle *, \mathbf{R} \rangle)_1, pk_1, pk_2 \rrbracket \\
&\quad = \rho_1(\llbracket \mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R} \rangle, \mathbf{E}_{pk_2} \triangleright \langle *, \mathbf{R} \rangle, pk_1, pk_2 \rrbracket) \\
&\quad \eqsim \rho_1(\llbracket \langle \mathbf{E}^{\$}_{pk_1}, \mathbf{E}^{\$}_{pk_1} \triangleright \mathbf{R} \rangle, \langle \mathbf{E}^{\$}_{pk_1}, \mathbf{E}^{\$}_{pk_1} \triangleright \mathbf{R} \rangle, pk_1, pk_2 \rrbracket) \quad \text{(ind-ik-ulk-cpa)} \\
&\quad = \llbracket \langle \mathbf{E}^{\$}_{pk_1}, \mathbf{E}^{\$}_{pk_1} \triangleright \mathbf{R} \rangle_1, \langle \mathbf{E}^{\$}_{pk_1}, \mathbf{E}^{\$}_{pk_1} \triangleright \mathbf{R} \rangle_1, pk_1, pk_2 \rrbracket \\
&\quad = \rho_2(\llbracket \langle \mathbf{E}^{\$}_{pk_1}, \mathbf{E}^{\$}_{pk_1} \triangleright \mathbf{R} \rangle, \langle \mathbf{E}^{\$}_{pk_1}, \mathbf{E}^{\$}_{pk_1} \triangleright \mathbf{R} \rangle, pk_1, pk_2 \rrbracket) \\
&\quad \eqsim \rho_2(\llbracket \mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R} \rangle, \mathbf{E}_{pk_2} \triangleright \langle *, \mathbf{R} \rangle, pk_1, pk_2 \rrbracket) \quad \text{(ind-ik-ulk-cpa)} \\
&\quad = \llbracket (\mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R} \rangle)_1, (\mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R} \rangle)_1, pk_1, pk_2 \rrbracket \\
&\quad \equiv \llbracket \mathbf{E}_{pk_1}, \mathbf{E}_{pk_1}, pk_1, pk_2 \rrbracket. \qquad \square
\end{aligned}
$$

Lemma 5.3.27. ind-ik-ulk-cpa $\xrightarrow{2}$ ulk-cpa.

Proof. Let $(sk, pk), (sk', pk') \leftarrow \mathtt{Gen}$, and consider

- $\rho_1(\llbracket \mathbf{X}, \mathbf{Y}, x, y \rrbracket) \doteq \llbracket \mathbf{X}, x \rrbracket$ and
- $\rho_2(\llbracket \mathbf{X}, \mathbf{Y}, x, y \rrbracket) \doteq \llbracket \langle (\mathbf{X})_1, (\mathbf{X})_1 \triangleright \mathbf{R} \rangle, x \rrbracket$.

Then:

$$
\begin{aligned}
&\llbracket \mathbf{E}_{pk} \triangleright \langle *, \mathbf{R} \rangle, pk \rrbracket \\
&\quad = \rho_1(\llbracket \mathbf{E}_{pk} \triangleright \langle *, \mathbf{R} \rangle, \mathbf{E}_{pk'} \triangleright \langle *, \mathbf{R} \rangle, pk, pk' \rrbracket) \\
&\quad \eqsim \rho_1(\llbracket \langle \mathbf{E}^{\$}_{pk}, \mathbf{E}^{\$}_{pk} \triangleright \mathbf{R} \rangle, \langle \mathbf{E}^{\$}_{pk}, \mathbf{E}^{\$}_{pk} \triangleright \mathbf{R} \rangle, pk, pk' \rrbracket) \quad \text{(ind-ik-ulk-cpa)} \\
&\quad = \llbracket \langle \mathbf{E}^{\$}_{pk}, \mathbf{E}^{\$}_{pk} \triangleright \mathbf{R} \rangle, pk \rrbracket \\
&\quad \equiv \llbracket \langle \langle \mathbf{E}^{\$}_{pk}, \mathbf{E}^{\$}_{pk} \triangleright \mathbf{R} \rangle_1, \langle \mathbf{E}^{\$}_{pk}, \mathbf{E}^{\$}_{pk} \triangleright \mathbf{R} \rangle_1 \triangleright \mathbf{R} \rangle, pk \rrbracket \\
&\quad = \rho_2(\llbracket \langle \mathbf{E}^{\$}_{pk}, \mathbf{E}^{\$}_{pk} \triangleright \mathbf{R} \rangle, \langle \mathbf{E}^{\$}_{pk}, \mathbf{E}^{\$}_{pk} \triangleright \mathbf{R} \rangle, pk, pk' \rrbracket) \\
&\quad \eqsim \rho_2(\llbracket \mathbf{E}_{pk} \triangleright \langle *, \mathbf{R} \rangle, \mathbf{E}_{pk'} \triangleright \langle *, \mathbf{R} \rangle, pk, pk' \rrbracket) \quad \text{(ind-ik-ulk-cpa)} \\
&\quad = \llbracket \langle (\mathbf{E}_{pk} \triangleright \langle *, \mathbf{R} \rangle)_1, (\mathbf{E}_{pk} \triangleright \langle *, \mathbf{R} \rangle)_1 \triangleright \mathbf{R} \rangle, pk \rrbracket \\
&\quad \equiv \llbracket \langle \mathbf{E}_{pk}, \mathbf{E}_{pk} \triangleright \mathbf{R} \rangle, pk \rrbracket. \qquad \square
\end{aligned}
$$

Lemma 5.3.28. ind-ik-sulk-cpa $\xrightarrow{1}$ ind-cpa.

Proof. Analogous to the proof of Lemma 5.3.25. □

Lemma 5.3.29. ind-ik-sulk-cpa $\xrightarrow{2}$ ik-cpa.

Proof. Analogous to the proof of Lemma 5.3.26. □

Lemma 5.3.30. ind-ik-sulk-cpa $\xrightarrow{2}$ sulk-cpa.

Proof. As for Lemma 5.3.27, but with

$$\rho_2([\![\mathbf{X}, \mathbf{Y}, x, y]\!]) \doteq [\![\langle (\mathbf{X})_1, (\mathbf{X})_1 \rangle, x]\!].$$ □

5.3.5 Generalizing the Notions: From 2 to n Receivers

In this section we define the generic notions for $n \geq 2$ receivers. Next, using the abstraction of the hybrid argument via substitutions from Section 2.3.2, we prove that they are implied by the two-users ones.

Definition 5.3.31 (n-cor-rob)**.**

$$[\![(\!|\mathbf{E}_{pk_1,\ldots,pk_n}, *, *|\!) \triangleright (\!|\mathbf{R}^*, *|\!) \triangleright \mathbf{D}_{sk_1,\ldots,sk_n}, \boldsymbol{pk}]\!]$$
$$\eqsim$$
$$[\![\mathbf{I}_n, \boldsymbol{pk}]\!],$$

for $(sk_1, pk_1), \ldots, (sk_n, pk_n) \leftarrow \mathtt{Gen}$ and $\boldsymbol{pk} \doteq (pk_1, \ldots, pk_n)$.

Definition 5.3.32 (n-ind-ik-ulk-cpa)**.**

$$[\![\mathbf{E}_{pk_1,\ldots,pk_n} \triangleright \langle *, \mathbf{R} \rangle, \boldsymbol{pk}]\!]$$
$$\eqsim$$
$$[\![(\!|*, *|\!)_1 \triangleright \langle \mathbf{E}^{\$}_{pk_1}, \mathbf{E}^{\$}_{pk_1} \triangleright \mathbf{R} \rangle, \boldsymbol{pk}]\!],$$

for $(sk_1, pk_1), \ldots, (sk_n, pk_n) \leftarrow \mathtt{Gen}$ and $\boldsymbol{pk} \doteq (pk_1, \ldots, pk_n)$.

Definition 5.3.33 (n-ind-ik-sulk-cpa)**.**

$$[\![\mathbf{E}_{pk_1,\ldots,pk_n} \triangleright \langle *, \mathbf{R} \rangle, \boldsymbol{pk}]\!]$$
$$\eqsim$$
$$[\![(\!|*, *|\!)_1 \triangleright \langle \mathbf{E}^{\$}_{pk_1}, \mathbf{E}^{\$}_{pk_1} \rangle, \boldsymbol{pk}]\!],$$

for $(sk_1, pk_1), \ldots, (sk_n, pk_n) \leftarrow \mathtt{Gen}$ and $\boldsymbol{pk} \doteq (pk_1, \ldots, pk_n)$.

Lemma 5.3.34. $(\mathsf{cor}, \mathsf{rob}) \xrightarrow{n, n(n-1)} n\text{-}\mathsf{cor}\text{-}\mathsf{rob}$.

Proof (sketch). This statement can be proven by generalizing (the first part of) the proof of Lemma 5.3.22. More specifically, the cor substitution is used n times, essentially to replace calls to $\mathtt{Dec}_{pk_i} \circ \mathtt{Rnc}^t \circ \mathtt{Enc}_{sk_i}$ by the identity function, for any $i \in [n]$ and $t \in \mathbb{N}$, and the rob substitution is used $n(n-1)$ times, essentially to replace calls to $\mathtt{Dec}_{pk_i} \circ \mathtt{Rnc}^t \circ \mathtt{Enc}_{sk_j}$ by $\bot$, for any $i \in [n]$, $j \in [n] \setminus \{i\}$, and $t \in \mathbb{N}$. □

Lemma 5.3.35. $\mathsf{ind\text{-}ik\text{-}ulk\text{-}cpa} \xrightarrow{n-1} n\text{-}\mathsf{ind\text{-}ik\text{-}ulk\text{-}cpa}$.

Proof. Let $(sk_1, pk_1), \ldots, (sk_n, pk_n) \leftarrow \mathtt{Gen}$, $\boldsymbol{pk} \doteq (pk_1, \ldots, pk_n)$, and consider

- $\rho_1([\![\mathbf{X}, \mathbf{Y}, x, y]\!])$
  $\doteq [\![\mathbf{X}, \mathbf{Y}, \mathbf{E}_{pk_3} \triangleright \langle *, \mathbf{R}\rangle, \ldots, \mathbf{E}_{pk_n} \triangleright \langle *, \mathbf{R}\rangle, x, y, pk_3, \ldots, pk_n]\!]$,
  and
- $\rho_i([\![\mathbf{X}, \mathbf{Y}, x, y]\!])$
  $\doteq [\![\underbrace{\langle \$ \triangleright (\mathbf{X})_1, \$ \triangleright (\mathbf{X})_1 \triangleright \mathbf{R}\rangle, \ldots, \langle \$ \triangleright (\mathbf{X})_1, \$ \triangleright (\mathbf{X})_1 \triangleright \mathbf{R}\rangle}_{i \text{ times}},$
  $\mathbf{Y}, \mathbf{E}_{pk_{i+2}} \triangleright \langle *, \mathbf{R}\rangle, \ldots, \mathbf{E}_{pk_n} \triangleright \langle *, \mathbf{R}\rangle,$
  $x, pk_2, \ldots, pk_i, y, pk_{i+2}, \ldots, pk_n]\!]$,
  for $i = 2, \ldots, n-1$.

Note that:

- $\rho_1([\![\mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R}\rangle, \mathbf{E}_{pk_2} \triangleright \langle *, \mathbf{R}\rangle, pk_1, pk_2]\!])$
  $\equiv [\![\mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R}\rangle, \ldots, \mathbf{E}_{pk_n} \triangleright \langle *, \mathbf{R}\rangle, \boldsymbol{pk}]\!]$,
- $\rho_{n-1}([\![\langle \mathbf{E}^{\$}_{pk_1}, \mathbf{E}^{\$}_{pk_1} \triangleright \mathbf{R}\rangle, \langle \mathbf{E}^{\$}_{pk_1}, \mathbf{E}^{\$}_{pk_1} \triangleright \mathbf{R}\rangle, pk_1, pk_n]\!])$
  $\equiv [\![\underbrace{\langle \mathbf{E}^{\$}_{pk_1}, \mathbf{E}^{\$}_{pk_1} \triangleright \mathbf{R}\rangle, \ldots, \langle \mathbf{E}^{\$}_{pk_1}, \mathbf{E}^{\$}_{pk_1} \triangleright \mathbf{R}\rangle}_{n \text{ times}}, \boldsymbol{pk}]\!]$, and
- $\rho_i([\![\langle \mathbf{E}^{\$}_{pk_1}, \mathbf{E}^{\$}_{pk_1} \triangleright \mathbf{R}\rangle, \langle \mathbf{E}^{\$}_{pk_1}, \mathbf{E}^{\$}_{pk_1} \triangleright \mathbf{R}\rangle, pk_1, pk_{i+1}]\!])$

$$\equiv \rho_{i+1}([\![\mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R}\rangle, \mathbf{E}_{pk_{i+2}} \triangleright \langle *, \mathbf{R}\rangle, pk_1, pk_{i+2}]\!]),$$

for all $i \in [n-2]$.

Then, since by ind-ik-ulk-cpa we have

$$[\![\mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R}\rangle, \mathbf{E}_{pk_{i+1}} \triangleright \langle *, \mathbf{R}\rangle, pk_1, pk_{i+1}]\!]$$
$$\mathrel{\widehat{=}}$$
$$[\![\langle \mathbf{E}^{\$}_{pk_1}, \mathbf{E}^{\$}_{pk_1} \triangleright \mathbf{R}\rangle, \langle \mathbf{E}^{\$}_{pk_1}, \mathbf{E}^{\$}_{pk_1} \triangleright \mathbf{R}\rangle, pk_1, pk_{i+1}]\!],$$

for any $i \in [n-1]$, by Lemma 2.3.2 it follows that

$$\rho_1([\![\mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R}\rangle, \mathbf{E}_{pk_2} \triangleright \langle *, \mathbf{R}\rangle, pk_1, pk_2]\!])$$
$$\mathrel{\widehat{=}}$$
$$\rho_{n-1}([\![\langle \mathbf{E}^{\$}_{pk_1}, \mathbf{E}^{\$}_{pk_1} \triangleright \mathbf{R}\rangle, \langle \mathbf{E}^{\$}_{pk_1}, \mathbf{E}^{\$}_{pk_1} \triangleright \mathbf{R}\rangle, pk_1, pk_n]\!]).$$

Therefore, with $\rho([\![\mathbf{X}_1, \ldots, \mathbf{X}_n, \boldsymbol{x}]\!]) \doteq [\![\mathbf{X}', \boldsymbol{x}]\!]$, where $\mathbf{X}'(m,i) \doteq \mathbf{S}_i(m)$, for $i \in [n]$,

$$\begin{aligned}
&[\![\mathbf{E}_{pk_1,\ldots,pk_n} \triangleright \langle *, \mathbf{R}\rangle, \boldsymbol{pk}]\!] \\
&\quad\equiv \rho([\![\mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R}\rangle, \ldots, \mathbf{E}_{pk_n} \triangleright \langle *, \mathbf{R}\rangle, \boldsymbol{pk}]\!]) \\
&\quad\equiv \rho \circ \rho_1([\![\mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R}\rangle, \mathbf{E}_{pk_2} \triangleright \langle *, \mathbf{R}\rangle, pk_1, pk_2]\!]) \\
&\quad\mathrel{\widehat{=}} \rho \circ \rho_{n-1}([\![\langle \mathbf{E}^{\$}_{pk_1}, \mathbf{E}^{\$}_{pk_1} \triangleright \mathbf{R}\rangle, \langle \mathbf{E}^{\$}_{pk_1}, \mathbf{E}^{\$}_{pk_1} \triangleright \mathbf{R}\rangle, pk_1, pk_n]\!]) \\
&\quad\equiv \rho([\![\underbrace{\langle \mathbf{E}^{\$}_{pk_1}, \mathbf{E}^{\$}_{pk_1} \triangleright \mathbf{R}\rangle, \ldots, \langle \mathbf{E}^{\$}_{pk_1}, \mathbf{E}^{\$}_{pk_1} \triangleright \mathbf{R}\rangle}_{n \text{ times}}, \boldsymbol{pk}]\!]) \\
&\quad\equiv [\![(\!|*, *|\!)_1 \triangleright \langle \mathbf{E}^{\$}_{pk_1}, \mathbf{E}^{\$}_{pk_1} \triangleright \mathbf{R}\rangle, \boldsymbol{pk}]\!].
\end{aligned}$$

□

Lemma 5.3.36. ind-ik-sulk-cpa $\xrightarrow{n-1}$ n-ind-ik-sulk-cpa.

Proof. As for Lemma 5.3.35, but with

$$\begin{aligned}
\rho_i([\![\mathbf{X}, \mathbf{Y}, x, y]\!]) \doteq [\![&\underbrace{\langle \$ \triangleright (\mathbf{X})_1, \$ \triangleright (\mathbf{X})_1\rangle, \ldots, \langle \$ \triangleright (\mathbf{X})_1, \$ \triangleright (\mathbf{X})_1\rangle}_{i \text{ times}}, \\
&\mathbf{Y}, \mathbf{E}_{pk_{i+2}} \triangleright \langle *, \mathbf{R}\rangle, \ldots, \mathbf{E}_{pk_n} \triangleright \langle *, \mathbf{R}\rangle, \\
&x, pk_2, \ldots, pk_i, y, pk_{i+2}, \ldots, pk_n]\!].
\end{aligned}$$

□

5.4 Composable Semantics of URE

The goal of this section is to define security of universal re-encryption from an *application point of view*. We do so using the framework of constructive cryptography (CC) [MR11, Mau12] as introduced in Section 2.4. Previously, composable semantics of other cryptographic schemes with anonymity properties have been considered in CC: anonymous PKE [KMO+13], anonymous (probabilistic) MACs [AHM+15], anonymous (probabilistic) symmetric-key encryption and authenticated encryption [BM20], as presented in Chapter 3, and three kinds of anonymous signature schemes [BM22], as presented in Chapter 4. The common thread for all these four works, is that the statements shown exclusively capture anonymity *preservation*. More precisely, all statements show that a certain scheme realizes some ideal resource that captures some kind of security in conjunction with anonymity, if used with an assumed resource that captures a weaker form of security (than the kind captured by the ideal resource) *but already in conjunction with anonymity*. Even more concretely, recall for example how in Chapter 3 [BM20] we have shown that anonymous and IND-CPA (probabilistic) symmetric-key encryption, from an authenticated anonymous channel (plus a resource modeling a shared secret key), constructs a secure (that is, both authenticated *and confidential*) anonymous channel.

In this chapter, we show (for the first time) a construction that potentially captures the *creation* of anonymity. We will assume resources that explicitly leak the identity of senders and receivers, and therefore, if used naively, trivially allow to link senders to receivers. Using URE, we are able to construct, from such assumed resources, and ideal resource that leaks the identities, but *hides the links between senders and receivers*. Therefore, under certain circumstances (that is, the traffic from senders to receivers is "large"), such ideal resource also guarantees anonymity of both senders and receivers.

We consider the simple case of a single honest mixer between the senders and the receivers, where senders authentically send ciphertexts to the mixer, which re-encrypts each stored ciphertext on each new input, and where receivers fetch the list of all ciphertexts from the mixer, decrypt the ones meant for them, and finally tell the mixer which ciphertexts are to be deleted.

5.4.1 Assumed and Ideal Resources

In this chapter we deviate slightly from the modeling of communication channels adopted in the previous two chapters. More specifically, for the assumed resources we make the simplifying assumption of a passive adversary that can only eavesdrop, but cannot control communication, that is, can neither drop, nor reorder, nor replay messages. Put in other words, messages input by honest parties are instantly delivered. On the other hand, we now consider channels with both multiple senders *and multiple receivers*. More precisely, with senders set $\mathcal{S}$, receivers set $\mathcal{R}$, mixer M and adversary E, we consider $\mathcal{P}$-resources with $\mathcal{P} = \mathcal{S} \cup \mathcal{R} \cup \{M, E\}$, where $\mathcal{S}$, $\mathcal{R}$, and $\{M, E\}$ are pairwise disjoint. Let the honest parties set by $\mathcal{H} \doteq \mathcal{S} \cup \mathcal{R} \cup \{M\}$, and for a set $\mathcal{S}$, let $2^{\mathcal{S}}$ denote its power set, that is, $2^{\mathcal{S}} \doteq \{\mathcal{S}' \mid \mathcal{S}' \subseteq \mathcal{S}\}$. We describe such resources for $\mathcal{A}, \mathcal{B} \subseteq \mathcal{H}$, and sets $\mathcal{X} \in \{\mathcal{PK}, \mathcal{C}, \{\diamond\} \cup 2^{\mathcal{C}}\}$ and $\mathcal{M}$ defined by a fixed URE scheme Π_{URE}.

We begin by defining the assumed *non-anonymous* resources: the single-use authenticated channel $\mathsf{1\text{-}AUT}^{\mathcal{X}}_{\mathcal{A}\to\mathcal{B}}$, the (multi-use) authenticated channel $\mathsf{AUT}^{\mathcal{X}}_{\mathcal{A}\to\mathcal{B}}$, and the bi-directional (multi-use) authenticated channel $\mathsf{AUT}^{\mathcal{X}}_{\mathcal{A}\leftrightarrow\mathcal{B}}$. Since we are now considering multiple senders and receivers at the same time, input messages are always accompanied by a recipient, and since we are now considering non-anonymous channels, the sender and receiver identities will always be leaked to the eavesdropping adversary. Moreover, unlike in the previous two chapters, here we use the names of the sender and receiver sets in the names of the channel resources, rather than their cardinalities.

Definition 5.4.1 ($\mathsf{1\text{-}AUT}^{\mathcal{X}}_{\mathcal{A}\to\mathcal{B}}$, $\mathsf{AUT}^{\mathcal{X}}_{\mathcal{A}\to\mathcal{B}}$, $\mathsf{AUT}^{\mathcal{X}}_{\mathcal{A}\leftrightarrow\mathcal{B}}$)**.** For $A \in \mathcal{A}$, we define the resource $\mathsf{AUT}^{\mathcal{X}}_{\mathcal{A}\to\mathcal{B}}$ as follows:

- On input $(x, B) \in \mathcal{X} \times \mathcal{B}$ at interface A, output (A, x, B) at interface E and (A, x) at interface B.

For the resource $\mathsf{1\text{-}AUT}^{\mathcal{X}}_{\mathcal{A}\to\mathcal{B}}$, interface A becomes inactive after the first input. For $B \in \mathcal{B}$, for the resource $\mathsf{AUT}^{\mathcal{X}}_{\mathcal{A}\leftrightarrow\mathcal{B}}$ we additionally have:

- On input $(x, A) \in \mathcal{X} \times \mathcal{A}$ at interface B, output (B, x, A) at interface E and (B, x) at interface A.

If $\mathcal{A}$ (or $\mathcal{B}$) is singleton set $\mathcal{A} = \{A\}$, we use A instead of $\mathcal{A}$ as superscript.

Next, we define the ideal resource that URE realizes: the *unlinkable communication channel* $\mathsf{ULK}^{\mathcal{X}}_{\mathcal{S}\to\mathcal{R}}$. Intuitively, this channel allows senders to input messages for receivers and receivers to retrieve messages meant for them, but in such a way that the adversary *cannot link these actions together*. More precisely, $\mathsf{ULK}^{\mathcal{X}}_{\mathcal{S}\to\mathcal{R}}$ allows a sender $S \in \mathcal{S}$ to input a value $x \in \mathcal{X}$ addressed to some receiver $R \in \mathcal{R}$, so that the adversary only sees that S *input something*, neither what nor to whom, and subsequently, receiver R can query the channel for messages addressed to her, but again so that the adversary only sees that R *fetched something*, neither what nor from whom.

Definition 5.4.2 ($\mathsf{ULK}^{\mathcal{X}}_{\mathcal{S}\to\mathcal{R}}$)**.** For $S \in \mathcal{S}$ and $R \in \mathcal{R}$, we define the resource $\mathsf{ULK}^{\mathcal{X}}_{\mathcal{S}\to\mathcal{R}}$ as follows: Initially set $M \leftarrow [\,]$, and then:

- On input $(x, R) \in \mathcal{X} \times \mathcal{R}$ at interface S, output S at interface E and set $M[R] \xleftarrow{\cup} \{x\}$.
- On input $\diamond$ at interface R, first output $(R, |M[R]|)$ at interface E, and then output $M[R]$ at interface R and set $M[R] \leftarrow \varnothing$.

5.4.2 Main Result: Single Honest Mixer

We now show that if a URE scheme satisfies both n-cor-rob and n-ind-ik-sulk-cpa, then it also securely constructs the resource $\mathsf{ULK}^{\mathcal{M}}_{\mathcal{S}\to\mathcal{R}}$, if appropriately used in conjunction with resources $\text{1-}\mathsf{AUT}^{\mathcal{PK}}_{\mathcal{R}\to\mathcal{S}}$, $\mathsf{AUT}^{\mathcal{C}}_{\mathcal{S}\to M}$, and $\mathsf{AUT}^{\{\diamond\}\cup 2^{\mathcal{C}}}_{M\leftrightarrow\mathcal{R}}$. For this, we need to first describe the behavior of the protocol $\boldsymbol{\pi}_{\mathsf{URE}}$, implicitly parameterized by a generic URE scheme Π_{URE}, when attached to such resources composed in parallel. On a high level, the protocol allows a sender to input a message addressed to a specific receiver, and sends its encryption to the mixer via $\mathsf{AUT}^{\mathcal{C}}_{\mathcal{S}\to M}$. The encryption is performed using the receiver public key, which the sender received through $\text{1-}\mathsf{AUT}^{\mathcal{PK}}_{\mathcal{R}\to\mathcal{S}}$. The mixer keeps all ciphertexts in a buffer, and whenever it receives a new ciphertext, it re-encrypts every ciphertext in the buffer, as well as the new one, which it then adds to the buffer. Note that the mixer does not know to whom the ciphertexts are addressed, but since re-encryption is universal, it does not need a public key to perform this operation. Finally, a receiver can query the mixer via $\mathsf{AUT}^{\{\diamond\}\cup 2^{\mathcal{C}}}_{M\leftrightarrow\mathcal{R}}$ for all stored ciphertexts, trial decrypt those addressed to her, and instruct the

mixer to remove them from the buffer. A formal description of $\boldsymbol{\pi}_{\mathsf{URE}}$ follows.

Definition 5.4.3 ($\boldsymbol{\pi}_{\mathsf{URE}}$)**.** For $\mathcal{H} \doteq \mathcal{S} \cup \mathcal{R} \cup \{M\}$, the $\mathcal{H}$-protocol $\boldsymbol{\pi}_{\mathsf{URE}}$ using a URE scheme $\Pi_{\mathsf{URE}} \doteq (\mathtt{Gen}, \mathtt{Enc}, \mathtt{Rnc}, \mathtt{Dec})$ is composed by the local converters enc, attached to an interface $S \in \mathcal{S}$, dec, attached to an interface $R \in \mathcal{R}$, and rnc, attached to interface M. They are defined as follows:

- enc: Upon initialization, for each $R \in \mathcal{R}$ obtain (R, pk_R) from $\mathsf{1\text{-}AUT}^{\mathcal{PK}}_{\mathcal{R}\to\mathcal{S}}$ though interface in, and then on input $(m, R) \in \mathcal{M} \times \mathcal{R}$ at interface out, get $c \leftarrow \mathtt{Enc}_{pk_R}(m)$ and input (c, M) to $\mathsf{AUT}^{\mathcal{C}}_{\mathcal{S}\to M}$ though interface in.

- rnc: Upon initialization, set $\mathcal{B} \leftarrow \varnothing$, and then:

  - On input (S, c) from $\mathsf{AUT}^{\mathcal{C}}_{\mathcal{S}\to M}$ through interface in:
    1. Set $\mathcal{B}' \leftarrow \varnothing$, and then for each $c' \in \mathcal{B}$ get $\hat{c}' \leftarrow \mathtt{Rnc}(c')$ and set $\mathcal{B}' \xleftarrow{\cup} \{\hat{c}\}$. Then set $\mathcal{B} \leftarrow \mathcal{B}'$.
    2. Get $\hat{c} \leftarrow \mathtt{Rnc}(c)$ and set $\mathcal{B} \xleftarrow{\cup} \{\hat{c}\}$.
  - On input $(R, \diamond)$ from $\mathsf{AUT}^{\{\diamond\}\cup 2^{\mathcal{C}}}_{M\leftrightarrow\mathcal{R}}$ through interface in, input $(\mathcal{B}, R)$ to $\mathsf{AUT}^{\{\diamond\}\cup 2^{\mathcal{C}}}_{M\leftrightarrow\mathcal{R}}$ through interface in.
  - On input $(R, \mathfrak{O}_R)$ from $\mathsf{AUT}^{\{\diamond\}\cup 2^{\mathcal{C}}}_{M\leftrightarrow\mathcal{R}}$ through interface in, set $\mathcal{B} \xleftarrow{\wedge} \mathfrak{O}_R$.

- dec: Upon initialization, get $(sk_R, pk_R) \leftarrow \mathtt{Gen}$, input (pk_R, S) to $\mathsf{1\text{-}AUT}^{\mathcal{PK}}_{\mathcal{R}\to\mathcal{S}}$ through interface in for each $S \in \mathcal{S}$, and then on input $\diamond$ at interface out:
  1. Input $\diamond$ to $\mathsf{AUT}^{\{\diamond\}\cup 2^{\mathcal{C}}}_{M\leftrightarrow\mathcal{R}}$ through interface in.
  2. On input $(M, \mathcal{B})$ from $\mathsf{AUT}^{\{\diamond\}\cup 2^{\mathcal{C}}}_{M\leftrightarrow\mathcal{R}}$ through interface in, set $\mathfrak{O}_E, \mathfrak{O}_R \leftarrow \varnothing$, and then for each $c \in \mathcal{B}$ get $m \leftarrow \mathtt{Dec}_{sk_R}(c)$, and if $m \neq \perp$, set $\mathfrak{O}_E \xleftarrow{\cup} \{c\}$ and $\mathfrak{O}_R \xleftarrow{\cup} \{m\}$.
  3. Input $\mathfrak{O}_E$ to $\mathsf{AUT}^{\{\diamond\}\cup 2^{\mathcal{C}}}_{M\leftrightarrow\mathcal{R}}$ through interface in.
  4. Output $\mathfrak{O}_R$ at interface out.

$\rho_1(\llbracket \mathbf{S}, \boldsymbol{pk} \rrbracket)$

Initialize:
  $\mathcal{B}, \mathcal{D} \leftarrow \varnothing$
  for $i \in [n]$ **do**
    for $S \in \mathcal{S}$ **do**
      out$(\mathsf{out}; (R_i, pk_i, S))$
Interface $S(m, R_i)$: // $S \in \mathcal{S}$
  $(\mathcal{B}, \mathcal{D}) \leftarrow \mathsf{Rnc}(\mathcal{B}, \mathcal{D})$
  $c \leftarrow \mathtt{Enc}_{pk_i}(m)$
  out$(E; (S, c, M))$
  $\hat{c} \leftarrow \mathtt{Rnc}(m)$
  $\mathcal{B} \xleftarrow{\cup} \{\hat{c}\}$; $\mathcal{D} \xleftarrow{\cup} \{(i, m, 1)\}$
Interface $R_i(\diamond)$: // $i \in [n]$
  $\mathfrak{O}_E, \mathfrak{O}_R, \mathcal{D}' \leftarrow \varnothing$
  out$(E; (R_i, \diamond, M))$
  out$(E; (M, \mathcal{B}, R_i))$
  for $(j, m, t) \in \mathcal{D}$ **do**
    $m \leftarrow \mathbf{S}(j, m, t, i)$
    if $m \neq \perp$ **then**
      $\mathfrak{O}_E \xleftarrow{\cup} \{\hat{c}\}$
      $\mathfrak{O}_R \xleftarrow{\cup} \{m\}$
      $\mathcal{D}' \xleftarrow{\cup} \{(j, m, t)\}$
  $\mathcal{B} \xleftarrow{>} \mathfrak{O}_E$; $\mathcal{D} \xleftarrow{>} \mathcal{D}'$
  out$(E; (R_i, \mathfrak{O}_E, M))$
  out$(R_i; \mathfrak{O}_R)$
func $\mathsf{Rnc}(\mathcal{B}, \mathcal{D})$:
  $\mathcal{B}', \mathcal{D}' \leftarrow \varnothing$
  for $c \in \mathcal{B}$ **do**
    $\hat{c} \leftarrow \mathtt{Rnc}(c)$
    $\mathcal{B}' \xleftarrow{\cup} \{\hat{c}\}$
  for $(i, m, t) \in \mathcal{D}$ **do**
    $\mathcal{D}' \xleftarrow{\cup} \{(i, m, t + 1)\}$
  return $(\mathcal{B}', \mathcal{D}')$

$\rho_2(\llbracket \mathbf{S}, \boldsymbol{pk} \rrbracket)$

Initialize:
  $\mathcal{B} \leftarrow \varnothing$
  $M, C \leftarrow [\,]$
  for $i \in [n]$ **do**
    for $S \in \mathcal{S}$ **do**
      out$(\mathsf{out}; (R_i, pk_i, S))$
Interface $S(m, R_i)$: // $S \in \mathcal{S}$
  $\mathcal{B} \leftarrow \mathsf{Rnc}(\mathcal{B}, M)$
  $(c, \hat{c}) \leftarrow \mathbf{S}(i, m)$
  out$(E; (S, c, M))$
  $\mathcal{B} \xleftarrow{\cup} \{\hat{c}\}$
  $M[i] \xleftarrow{\cup} \{m\}$
  $C[(i, m)] \leftarrow \hat{c}$
Interface $R_i(\diamond)$: // $i \in [n]$
  $\mathfrak{O}_E, \mathfrak{O}_R \leftarrow \varnothing$
  out$(E; (R_i, \diamond, M))$
  out$(E; (M, \mathcal{B}, R_i))$
  for $m \in M[i]$ **do**
    $\mathfrak{O}_E \xleftarrow{\cup} \{\hat{c}\}$
  $\mathfrak{O}_R \leftarrow M[i]$
  $M[i] \leftarrow \varnothing$
  $\mathcal{B} \xleftarrow{>} \mathfrak{O}_E$
  out$(E; (R_i, \mathfrak{O}_E, M))$
  out$(R_i; \mathfrak{O}_R)$
func $\mathsf{Rnc}(\mathcal{B}, M)$:
  $\mathcal{B}' \leftarrow \varnothing$
  for $i \in [n]$ **do**
    for $m \in M[i]$ **do**
      $c \leftarrow C[(i, m)]$
      $\hat{c} \leftarrow \mathtt{Rnc}(c)$
      $\mathcal{B}' \xleftarrow{\cup} \{\hat{c}\}$
  return $\mathcal{B}'$

Figure 5.4: Transformations for the proof of Theorem 5.4.4.

σ

Initialize:
- $\mathcal{B} \leftarrow \varnothing$
- $\tilde{m} \xleftarrow{\$} \mathcal{M}$
- **for** $i \in [n]$ **do**
  - $(sk_i, pk_i) \leftarrow \mathtt{Gen}$
  - **for** $S \in \mathcal{S}$ **do**
    - **out**(out; (R_i, pk_i, S))

Interface in(S):
- $\mathcal{B} \leftarrow \mathsf{Rnc}(\mathcal{B})$
- $c \leftarrow \mathtt{Enc}_{pk_1}(\tilde{m})$
- **out**(out; (S, c, M))
- $\hat{c} \leftarrow \mathtt{Enc}_{pk_1}(\tilde{m})$
- $\mathcal{B} \xleftarrow{\cup} \{\hat{c}\}$

Interface in(R_i, ℓ):
- $\mathfrak{O}_E \leftarrow \varnothing$
- **out**(out; $(R_i, \diamond, M)$)
- **out**(out; $(M, \mathcal{B}, R_i)$)
- $\mathfrak{O}_E \xleftarrow{\$} \{\mathcal{A} \subseteq \mathcal{B} : |\mathcal{A}| = \ell\}$
- $\mathcal{B} \xleftarrow{\supset} \mathfrak{O}_E$
- **out**(out; $(R_i, \mathfrak{O}_E, M)$)

func $\mathsf{Rnc}(\mathcal{B})$:
- $\mathcal{B}' \leftarrow \varnothing$
- **for** $c \in \mathcal{B}$ **do**
  - $\hat{c} \leftarrow \mathtt{Rnc}(c)$
  - $\mathcal{B}' \xleftarrow{\cup} \{\hat{c}\}$
- **return** $\mathcal{B}'$

$\mathbf{H}_0$

Initialize:
- $\mathcal{B} \leftarrow \varnothing$
- **for** $i \in [n]$ **do**
  - $(sk_i, pk_i) \leftarrow \mathtt{Gen}$
  - **for** $S \in \mathcal{S}$ **do**
    - **out**$(E; (R_i, pk_i, S))$

Interface $S(m, R_i)$: // $S \in \mathcal{S}$
- $\mathcal{B} \leftarrow \mathsf{Rnc}(\mathcal{B})$
- $c \leftarrow \mathtt{Enc}_{pk_i}(m)$
- **out**$(E; (S, c, M))$
- $\hat{c} \leftarrow \mathtt{Rnc}(m)$
- $\mathcal{B} \xleftarrow{\cup} \{\hat{c}\}$

Interface $R_i(\diamond)$: // $i \in [n]$
- $\mathfrak{O}_E, \mathfrak{O}_R \leftarrow \varnothing$
- **out**$(E; (R_i, \diamond, M))$
- **out**$(E; (M, \mathcal{B}, R_i))$
- **for** $\hat{c} \in \mathcal{B}$ **do**
  - $m \leftarrow \mathtt{Dec}_{sk_i}(\hat{c})$
  - **if** $m \neq \perp$ **then**
    - $\mathfrak{O}_E \xleftarrow{\cup} \{\hat{c}\}$
    - $\mathfrak{O}_R \xleftarrow{\cup} \{m\}$
- $\mathcal{B} \xleftarrow{\supset} \mathfrak{O}_E$
- **out**$(E; (R_i, \mathfrak{O}_E, M))$
- **out**$(R; \mathfrak{O}_R)$

func $\mathsf{Rnc}(\mathcal{B})$:
- $\mathcal{B}' \leftarrow \varnothing$
- **for** $c \in \mathcal{B}$ **do**
  - $\hat{c} \leftarrow \mathtt{Rnc}(c)$
  - $\mathcal{B}' \xleftarrow{\cup} \{\hat{c}\}$
- **return** $\mathcal{B}'$

Figure 5.5: Simulator and hybrid $\mathbf{H}_0$ for the proof of Theorem 5.4.4.

$\boxed{\mathbf{H}_1}$ $\boxed{\mathbf{H}_2}$

Initialize:
  $\mathcal{B} \leftarrow \varnothing$; $M, C \leftarrow [\,]$; $\tilde{m} \xleftarrow{\$} \mathcal{M}$
  for $i \in [n]$ **do**
    $(sk_i, pk_i) \leftarrow \mathtt{Gen}$
    for $S \in \mathcal{S}$ **do**
      out$(E; (R_i, pk_i, S))$
Interface $S(m, R_i)$: // $S \in \mathcal{S}$
  $\mathcal{B} \leftarrow \mathsf{Rnc}(\mathcal{B}, M)$
  $c \leftarrow \mathtt{Enc}_{pk_i}(m)$
  $c \leftarrow \mathtt{Enc}_{pk_1}(\tilde{m})$
  out$(E; (S, c, M))$
  $\hat{c} \leftarrow \mathsf{Rnc}(m)$; $\hat{c} \leftarrow \mathtt{Enc}_{pk_1}(\tilde{m})$
  $\mathcal{B} \xleftarrow{\cup} \{\hat{c}\}$
  $M[i] \xleftarrow{\cup} \{m\}$; $C[(i, m)] \leftarrow \hat{c}$
Interface $R_i(\diamond)$: // $i \in [n]$
  $\mathfrak{O}_E, \mathfrak{O}_R \leftarrow \varnothing$
  out$(E; (R_i, \diamond, M))$
  out$(E; (M, \mathcal{B}, R_i))$
  for $m \in M[i]$ **do**
    $\mathfrak{O}_E \xleftarrow{\cup} \{\hat{c}\}$
  $\mathfrak{O}_R \leftarrow M[i]$; $M[i] \leftarrow \varnothing$
  $\mathcal{B} \xleftarrow{\sim} \mathfrak{O}_E$
  out$(E; (R_i, \mathfrak{O}_E, M))$
  out$(R; \mathfrak{O}_R)$
func $\mathsf{Rnc}(\mathcal{B}, M)$:
  $\mathcal{B}' \leftarrow \varnothing$
  for $i \in [n]$ **do**
    for $m \in M[i]$ **do**
      $c \leftarrow C[(i, m)]$
      $\hat{c} \leftarrow \mathtt{Rnc}(c)$; $\mathcal{B}' \xleftarrow{\cup} \{\hat{c}\}$
  return $\mathcal{B}'$

$\mathbf{H}_3$

Initialize:
  $\mathcal{B} \leftarrow \varnothing$
  $M \leftarrow [\,]$
  $\tilde{m} \xleftarrow{\$} \mathcal{M}$
  for $i \in [n]$ **do**
    $(sk_i, pk_i) \leftarrow \mathtt{Gen}$
    for $S \in \mathcal{S}$ **do**
      out$(E; (R_i, pk_i, S))$
Interface $S(m, R_i)$: // $S \in \mathcal{S}$
  $\mathcal{B} \leftarrow \mathsf{Rnc}(\mathcal{B})$
  $c \leftarrow \mathtt{Enc}_{pk_1}(\tilde{m})$
  out$(E; (S, c, M))$
  $\hat{c} \leftarrow \mathtt{Enc}_{pk_1}(\tilde{m})$
  $\mathcal{B} \xleftarrow{\cup} \{\hat{c}\}$
  $M[i] \xleftarrow{\cup} \{m\}$
Interface $R_i(\diamond)$: // $i \in [n]$
  $\mathfrak{O}_E, \mathfrak{O}_R \leftarrow \varnothing$
  out$(E; (R_i, \diamond, M))$
  out$(E; (M, \mathcal{B}, R_i))$
  $\ell \leftarrow |\mathfrak{O}_R|$
  $\mathfrak{O}_E \xleftarrow{\$} \{\mathcal{A} \subseteq \mathcal{B} : |\mathcal{A}| = \ell\}$
  $\mathfrak{O}_R \leftarrow M[i]$
  $M[i] \leftarrow \varnothing$
  $\mathcal{B} \xleftarrow{\sim} \mathfrak{O}_E$
  out$(E; (R_i, \mathfrak{O}_E, M))$
  out$(R; \mathfrak{O}_R)$
func $\mathsf{Rnc}(\mathcal{B})$:
  $\mathcal{B}' \leftarrow \varnothing$
  for $c \in \mathcal{B}$ **do**
    $\hat{c} \leftarrow \mathtt{Rnc}(c)$
    $\mathcal{B}' \xleftarrow{\cup} \{\hat{c}\}$
  return $\mathcal{B}'$

Figure 5.6: Hybrids $\mathbf{H}_1$–$\mathbf{H}_3$ for the proof of Theorem 5.4.4.

Finally, we can now show that the protocol $\boldsymbol{\pi}_{\mathsf{URE}}$, and therefore the underlying URE scheme Π_{URE}, is composably secure.

Theorem 5.4.4. *With* $n \doteq |\mathcal{R}|$,

$$\left[\mathsf{1\text{-}AUT}^{\mathcal{PK}}_{\mathcal{R}\to\mathcal{S}}, \mathsf{AUT}^{\mathcal{C}}_{\mathcal{S}\to M}, \mathsf{AUT}^{\{\diamond\}\cup 2^{\mathcal{C}}}_{M\leftrightarrow\mathcal{R}}\right] \xrightarrow{\boldsymbol{\pi}_{\mathsf{URE}};\, n\text{-cor-rob}, n\text{-ind-ik-sulk-cpa}} \mathsf{ULK}^{\mathcal{M}}_{\mathcal{S}\to\mathcal{R}}.$$

Proof. Let $n \doteq |\mathcal{R}|$, $(sk_1, pk_1), \ldots, (sk_n, pk_n) \leftarrow \mathtt{Gen}$, and $\boldsymbol{pk} \doteq (pk_1, \ldots, pk_n)$. Assume $\mathcal{R} = \{R_1, \ldots, R_n\}$, and let $pk_i \doteq pk_{R_i}$, for $i \in [n]$. We also assume that i is retrievable from R_i. Define ρ_1, ρ_2, and $\boldsymbol{\sigma}$ as in Figures 5.4 and 5.5, and also define hybrid resources $\mathbf{H}_0$ to $\mathbf{H}_3$ as in Figures 5.5 and 5.6, where changes from the previous hybrid are highlighted in dark gray. Then:

$$\begin{aligned}
&\boldsymbol{\pi}_{\mathsf{URE}}\left[\mathsf{1\text{-}AUT}^{\mathcal{PK}}_{\mathcal{R}\to\mathcal{S}}, \mathsf{AUT}^{\mathcal{C}}_{\mathcal{S}\to M}, \mathsf{AUT}^{\{\diamond\}\cup 2^{\mathcal{C}}}_{M\leftrightarrow\mathcal{R}}\right] \\
&\quad\equiv \mathbf{H}_0 && \text{(monolithic representation)} \\
&\quad\equiv \rho_1(\llbracket(\!|\mathbf{E}_{pk_1,\ldots,pk_n}, *, *|\!) \triangleright (\!|\mathbf{R}^{*}, *|\!) \triangleright \mathbf{D}_{sk_1,\ldots,sk_n}, \boldsymbol{pk}\rrbracket) && \text{(by inspection)} \\
&\quad\eqsim \rho_1(\llbracket\mathbf{I}_n, \boldsymbol{pk}\rrbracket) && (n\text{-cor-rob}) \\
&\quad\equiv \mathbf{H}_1 && \text{(by inspection)} \\
&\quad= \rho_2(\llbracket\mathbf{E}_{pk_1,\ldots,pk_n} \triangleright \langle *, \mathbf{R}\rangle, \boldsymbol{pk}\rrbracket) \\
&\quad\eqsim \rho_2(\llbracket(\!|*, *|\!)_1 \triangleright \langle \mathbf{E}^{\$}_{pk_1}, \mathbf{E}^{\$}_{pk_1}\rangle, \boldsymbol{pk}\rrbracket) && (n\text{-ind-ik-sulk-cpa}) \\
&\quad= \mathbf{H}_2 \\
&\quad\equiv \mathbf{H}_3 && \text{(by inspection)} \\
&\quad\equiv \boldsymbol{\sigma}\,\mathsf{ULK}_{\mathcal{S}\to\mathcal{R}}. && \text{(monolithic representation)}
\end{aligned}$$

□

5.4.3 When Does Unlinkability Imply Anonymity?

Note that, as discussed before, unlikability only implies anonymity under certain circumstances. In fact, if right after initialization a sender S sends a message m to a receiver R through $\mathsf{ULK}^{\mathcal{M}}_{\mathcal{S}\to\mathcal{R}}$, and right after that, R fetches its messages, then an eavesdropping adversary E will learn that indeed the sender was S, the receiver was R, and will clearly also link the two actions together. In particular, this means that E can link the sender to a specific ciphertext it saw, and we want to understand

when this becomes impossible to do for E. Therefore, a natural question is, *under what circumstances does* $\mathsf{ULK}^{\mathcal{M}}_{\mathcal{S}\to\mathcal{R}}$ *provide anonymity of the senders?* Consider now the case where, right after initialization, the following sequence of actions takes place: (1) sender S_0 sends message m_0 to receiver R_0, (2) sender S_1 sends message m_1 to receiver R_1, (3) R_0 fetches its messages, and (4) R_1 fetches its messages. Now, the guarantee provided by $\mathsf{ULK}^{\mathcal{M}}_{\mathcal{S}\to\mathcal{R}}$ is that E cannot link any of the two senders to any of the two receivers, that is, E will be unable to distinguish the case that S_i sent to R_i from the case that S_i sent to R_{1-i}, for $i \in \{0,1\}$. This implies that now E cannot link any ciphertext it sees to neither S_0 nor S_1. Moreover, after those four actions take place, that is, after the set M kept by $\mathsf{ULK}^{\mathcal{M}}_{\mathcal{S}\to\mathcal{R}}$ is empty again, the state of anonymity is equivalent to the one right after initialization. Therefore, to answer the above question, *senders are guaranteed to be anonymous among the set of senders that sent messages since the last time that M was not empty.*

5.5 ElGamal-Based Universal Re-Encryption

In this section we fix a cyclic group $\mathbb{G} = \langle g \rangle$ of order $q \doteq |\mathbb{G}|$ with generator $g \in \mathbb{G}$.

5.5.1 Decisional Diffie-Hellman Assumption

We can base all results of this chapter on a single assumption, that we also define as a substitution. The decisional Diffie-Hellman (DDH) problem for $\mathbb{G}$ states that it is hard to distinguish triplets of the form $(g^\alpha, g^\beta, g^{\alpha\beta}) \in \mathbb{G}^3$, for $\alpha, \beta \xleftarrow{\$} \mathbb{Z}_q$, from triplets of the form $(g^\alpha, g^\beta, g^\gamma) \in \mathbb{G}^3$, for $\alpha, \beta, \gamma \xleftarrow{\$} \mathbb{Z}_q$. To formalize this assumption as a substitution, we define the following systems.

Definition 5.5.1 (DDH Systems)**.**

- $\mathbf{S}^{\mathsf{ddh}}_0$: on input $\diamond$, output $(g^\alpha, g^\beta, g^{\alpha\beta}) \in \mathbb{G}^3$, for $\alpha, \beta \xleftarrow{\$} \mathbb{Z}_q$ (only once).

- $\mathbf{S}^{\mathsf{ddh}}_1$: on input $\diamond$, output $(g^\alpha, g^\beta, g^\gamma) \in \mathbb{G}^3$, for $\alpha, \beta, \gamma \xleftarrow{\$} \mathbb{Z}_q$ (only once).

We can now capture such assumption as a substitution, and consequently treat it as a notion which we can relate to other security notions, for a specific scheme based on DDH.

Definition 5.5.2 (ddh)**.** $\mathbf{S}_0^{\mathsf{ddh}} \doteq \mathbf{S}_1^{\mathsf{ddh}}$.

5.5.2 Security of ElGamal-Based URE Scheme

We now define the concrete ElGamal-based URE scheme introduced by Golle et al. [GJJS04] (that is, we specify a concrete instantiation of Definition 5.2.3), and then prove that it satisfies all our notions. In our proofs we will use common re-randomization techniques, as introduced for example in [BBM00], in order to be able to use a single DDH instance to simulate encryption of many messages, both under a public key defined by such instance and an independent one.

Definition 5.5.3. $\Pi_{\texttt{URE-ElGamal}} = (\texttt{Gen}, \texttt{Enc}, \texttt{Rnc}, \texttt{Dec})$, with private-key space $\mathcal{SK} \doteq \mathbb{Z}_q$, public-key space $\mathcal{PK} \doteq \mathbb{G}$, message space[1] $\mathcal{M} = \mathbb{G}$, and ciphertext space $\mathcal{C} \doteq \mathbb{G}^4$, is defined as follows:

- $\texttt{Gen}() \doteq (sk, g^{sk})$, for $sk \xleftarrow{\$} \mathbb{Z}_q$.
- $\texttt{Enc}_{pk}(m) \doteq (m \cdot pk^{\kappa_0}, g^{\kappa_0}, pk^{\kappa_1}, g^{\kappa_1})$, for $\kappa_0, \kappa_1 \xleftarrow{\$} \mathbb{Z}_q$.
- $\texttt{Rnc}((\alpha_0, \beta_0, \alpha_1, \beta_1)) \doteq (\alpha_0 \alpha_1^{\kappa_0'}, \beta_0 \beta_1^{\kappa_0'}, \alpha_1^{\kappa_1'}, \beta_1^{\kappa_1'})$, for $\kappa_0', \kappa_1' \xleftarrow{\$} \mathbb{Z}_q$.
- $\texttt{Dec}_{sk}((\alpha_0, \beta_0, \alpha_1, \beta_1)) \doteq \begin{cases} \alpha_0/\beta_0^{sk} & \text{if } \alpha_1/\beta_1^{sk} = 1, \\ \perp & \text{otherwise.} \end{cases}$

In the following we understand the systems from Definition 5.2.4 as being implicitly parameterized on $\Pi_{\mathsf{URE\text{-}ElGamal}}$.

Lemma 5.5.4. $\mathsf{cor}^{\Pi_{\mathsf{URE\text{-}ElGamal}}}$ *holds unconditionally.*

Proof. Let $(m, t) \in \mathbb{G} \times \mathbb{N}$. Then, for $\kappa_0^0, \kappa_1^0, \kappa_0^1, \kappa_1^1, \ldots, \kappa_0^t, \kappa_1^t \xleftarrow{\$} \mathbb{Z}_q$, $(sk, pk) \leftarrow \texttt{Gen}$, $\sigma \doteq \sum_{i=0}^{t} \kappa_0^i \prod_{j=0}^{i-1} \kappa_1^j$, and $\omega \doteq \prod_{i=0}^{t} \kappa_1^i$, on input (m, t)

[1] Note that in Definition 5.2.3 we specified that $\mathcal{M} \doteq \{0,1\}^\kappa$, for some $\kappa \in \mathbb{N}$, whereas here we consider group elements, rather than bitstrings. Since message should have the same length, we implicitly assume some padding takes place (e.g., via hashing).

the system $[\![(\!|\mathbf{E}_{pk}, *|\!) \triangleright \mathbf{R}^* \triangleright \mathbf{D}_{sk}, pk]\!]$ will output

$$\begin{aligned}\mathtt{Dec}_{sk}(\mathtt{Rnc}^t(\mathtt{Enc}_{pk}(m))) &= \mathtt{Dec}_{sk}(\mathtt{Rnc}^t((m \cdot pk^{\kappa_0}, g^{\kappa_0}, pk^{\kappa_1}, g^{\kappa_1}))) \\ &= \mathtt{Dec}_{sk}((m \cdot pk^{\sigma}, g^{\sigma}, pk^{\omega}, g^{\omega})) \\ &= m \cdot pk^{\sigma}/g^{\sigma \cdot sk} \\ &= m \cdot g^{sk \cdot \sigma}/g^{\sigma \cdot sk} \\ &= m,\end{aligned}$$

since $pk^{\omega}/g^{\omega \cdot sk} = g^{sk \cdot \omega}/g^{\omega \cdot sk} = 1$. Therefore,

$$[\![(\!|\mathbf{E}_{pk}, *|\!) \triangleright \mathbf{R}^* \triangleright \mathbf{D}_{sk}, pk]\!] \equiv [\![(\!|*, *|\!)_1, pk]\!]. \qquad \square$$

Lemma 5.5.5. $\mathsf{rob}^{\Pi_{\mathsf{URE\text{-}ElGamal}}}$ *holds unconditionally with probability* $\frac{1}{q}$.

Proof. Let $(m, t) \in \mathbb{G} \times \mathbb{N}$. Then, for $\kappa_0^0, \kappa_1^0, \kappa_0^1, \kappa_1^1, \ldots, \kappa_0^t, \kappa_1^t \xleftarrow{\$} \mathbb{Z}_q$, $(sk_1, pk_1), (sk_2, pk_2) \leftarrow \mathtt{Gen}$, $\sigma \doteq \sum_{i=0}^{t} \kappa_0^i \prod_{j=0}^{i-1} \kappa_1^j$, and $\omega \doteq \prod_{i=0}^{t} \kappa_1^i$, on input (m, t) the system $[\![(\!|\mathbf{E}_{pk_1}, *|\!) \triangleright \mathbf{R}^* \triangleright \mathbf{D}_{sk_2}, pk_1, pk_2]\!]$ will output

$$\begin{aligned}\mathtt{Dec}_{sk_2}(\mathtt{Rnc}^t(\mathtt{Enc}_{pk_1}(m))) &= \mathtt{Dec}_{sk_2}(\mathtt{Rnc}^t((m \cdot pk_1^{\kappa_0}, g^{\kappa_0}, pk_1^{\kappa_1}, g^{\kappa_1}))) \\ &= \mathtt{Dec}_{sk_2}((m \cdot pk_1^{\sigma}, g^{\sigma}, pk_1^{\omega}, g^{\omega})) \\ &= \bot,\end{aligned}$$

since $pk_1^{\omega}/g^{\omega \cdot sk_2} = g^{sk_1 \cdot \omega}/g^{\omega \cdot sk_2} = 1$ if and only if $sk_1 = sk_2$, which happens with probability $\frac{1}{q}$. Therefore,

$$[\![(\!|\mathbf{E}_{pk_1}, *|\!) \triangleright \mathbf{R}^* \triangleright \mathbf{D}_{sk_2}, pk_1, pk_2]\!] \approx_{\frac{1}{q}} [\![\bot, pk_1, pk_2]\!]. \qquad \square$$

Lemma 5.5.6. $\mathsf{ddh} \xrightarrow{1} \mathsf{ind\text{-}cpa}^{\Pi_{\mathsf{URE\text{-}ElGamal}}}$.

Proof. Consider $\rho(\mathbf{X}) \equiv [\![\mathbf{X}', pk]\!]$, which initially inputs $\diamond$ to $\mathbf{X}$, obtains (x, y, z), sets $pk \doteq x$, and with system $\mathbf{X}'$ behaving as follows: On input $m \in \mathbb{G}$, get $u, v, \kappa_1 \xleftarrow{\$} \mathbb{Z}_q$ and output $(m \cdot z^u x^v, y^u g^v, x^{\kappa_1} g^{\kappa_1}, g^{\kappa_1})$. Then:

- $\rho(\mathbf{S}_0^{\mathsf{ddh}}) \equiv [\![\mathbf{E}_{pk}, pk]\!]$: We have that $(x, y, z) = (g^{\alpha}, g^{\beta}, g^{\alpha\beta})$, for $\alpha, \beta \xleftarrow{\$} \mathbb{Z}_q$, hence with $sk \doteq \alpha$ and $\kappa_0 \doteq \beta u + v$ we get

$$\begin{aligned}(m \cdot z^u x^v, y^u g^v, x^{\kappa_1} g^{\kappa_1}, g^{\kappa_1}) &= (m \cdot g^{\alpha\beta u + \alpha v}, g^{\beta u + v}, g^{\alpha\kappa_1}, g^{\kappa_1}) \\ &= (m \cdot g^{\alpha(\beta u + v)}, g^{\beta u + v}, g^{\alpha\kappa_1}, g^{\kappa_1}) \\ &= (m \cdot pk^{\kappa_0}, g^{\kappa_0}, pk^{\kappa_1}, g^{\kappa_1}),\end{aligned}$$

  which is distributed exactly as the output of $\mathbf{E}_{pk}$ on input m.

- $\rho(\mathbf{S}_1^{\mathsf{ddh}}) \equiv [\![\mathbf{E}_{pk}^{\$}, pk]\!]$: We have that $(x, y, z) = (g^{\alpha}, g^{\beta}, g^{\gamma})$, for $\alpha, \beta, \gamma \xleftarrow{\$} \mathbb{Z}_q$, hence with $sk \doteq \alpha$, $\kappa_0 \doteq \beta u + v$, and $\tilde{m} \doteq m \cdot g^{u(\gamma - \alpha\beta)}$ (thus, $\tilde{m} \xleftarrow{\$} \mathbb{G}$) we get

$$\begin{aligned}
&(m \cdot z^u x^v, y^u g^v, x^{\kappa_1} g^{\kappa_1}, g^{\kappa_1}) \\
&\quad = (m \cdot g^{\gamma u + \alpha v + (\alpha\beta u - \alpha\beta u)}, g^{\beta u + v}, g^{\alpha\kappa_1}, g^{\kappa_1}) \\
&\quad = (m \cdot g^{u(\gamma - \alpha\beta)} \cdot g^{\alpha(\beta u + v)}, g^{\beta u + v}, g^{\alpha\kappa_1}, g^{\kappa_1}) \\
&\quad = (\tilde{m} \cdot pk^{\kappa_0}, g^{\kappa_0}, pk^{\kappa_1}, g^{\kappa_1}),
\end{aligned}$$

  which is distributed exactly as the output of $\mathbf{E}_{pk}^{\$}$ on input m.

Therefore, $[\![\mathbf{E}_{pk}, pk]\!] \equiv \rho(\mathbf{S}_0^{\mathsf{ddh}}) \eqsim \rho(\mathbf{S}_1^{\mathsf{ddh}}) \equiv [\![\mathbf{E}_{pk}^{\$}, pk]\!]$. □

Lemma 5.5.7. $\mathsf{ddh} \xrightarrow{2} \mathsf{ik\text{-}cpa}^{\Pi_{\mathsf{URE\text{-}ElGamal}}}$.

Proof. For $i \in \{1, 2\}$, consider $\rho_i(\mathbf{X}) \equiv [\![\mathbf{E}_{pk_1}, \mathbf{X}', pk_1, pk_2]\!]$, which initially inputs $\diamond$ to $\mathbf{X}$, obtains (x_1, y_1, z_1), sets $(x_2, y_2, z_2) \leftarrow (x_1 \cdot g^a, y_1^c \cdot g^b, z_1^c \cdot x_1^b \cdot y_1^{ac} \cdot g^{ab})$, for $a, b, c \xleftarrow{\$} \mathbb{Z}_q$, $pk_1 \doteq x_1$, $pk_2 \doteq x_2$, and with system $\mathbf{X}'$ behaving as follows: On input $m \in \mathbb{G}$, get $u, v, \kappa_1 \xleftarrow{\$} \mathbb{Z}_q$ and output $(m \cdot z_i^u x_i^v, y_i^u g^v, x_i^{\kappa_1} g^{\kappa_1}, g^{\kappa_1})$. Then,

- $\rho_1(\mathbf{S}_0^{\mathsf{ddh}}) \equiv [\![\mathbf{E}_{pk_1}, \mathbf{E}_{pk_1}, pk_1, pk_2]\!]$: We have that $(x_1, y_1, z_1) = (g^{\alpha}, g^{\beta}, g^{\alpha\beta})$, for $\alpha, \beta \xleftarrow{\$} \mathbb{Z}_q$, hence with $sk_1 \doteq \alpha$ and $\kappa_0 \doteq \beta u + v$ we get

$$\begin{aligned}
(m \cdot z_1^u x_1^v, y_1^u g^v, x_1^{\kappa_1} g^{\kappa_1}, g^{\kappa_1}) &= (m \cdot g^{\alpha\beta u + \alpha v}, g^{\beta u + v}, g^{\alpha\kappa_1}, g^{\kappa_1}) \\
&= (m \cdot g^{\alpha(\beta u + v)}, g^{\beta u + v}, g^{\alpha\kappa_1}, g^{\kappa_1}) \\
&= (m \cdot pk_1^{\kappa_0}, g^{\kappa_0}, pk_1^{\kappa_1}, g^{\kappa_1}),
\end{aligned}$$

  which is distributed exactly as the output of $\mathbf{E}_{pk_1}$ on input m.

- $\rho_1(\mathbf{S}_0^{\mathsf{ddh}}) \equiv [\![\mathbf{E}_{pk_1}, \mathbf{E}_{pk_2}, pk_1, pk_2]\!]$: We have that $(x_2, y_2, z_2) = (g^{\alpha'}, g^{\beta'}, g^{\alpha'\beta'})$, for $\alpha', \beta' \xleftarrow{\$} \mathbb{Z}_q$ (because $\alpha' \doteq \alpha + a$, $\beta' \doteq \beta c + b$, and $\alpha, \beta, a, b, c \xleftarrow{\$} \mathbb{Z}_q$), hence with $sk_2 \doteq \alpha'$ and $\kappa_0 \doteq \beta u + v$ we get

$$\begin{aligned}
(m \cdot z_2^u x_2^v, y_2^u g^v, x_2^{\kappa_1} g^{\kappa_1}, g^{\kappa_1}) &= (m \cdot g^{\alpha'\beta' u + \alpha' v}, g^{\beta' u + v}, g^{\alpha'\kappa_1}, g^{\kappa_1}) \\
&= (m \cdot g^{\alpha'(\beta' u + v)}, g^{\beta' u + v}, g^{\alpha'\kappa_1}, g^{\kappa_1}) \\
&= (m \cdot pk_2^{\kappa_0}, g^{\kappa_0}, pk_2^{\kappa_1}, g^{\kappa_1}),
\end{aligned}$$

which is distributed exactly as the output of $\mathbf{E}_{pk_2}$ on input m.

- $\rho_1(\mathbf{S}_1^{\mathsf{ddh}}) \equiv \rho_2(\mathbf{S}_1^{\mathsf{ddh}})$: We have that $(x_1, y_1, z_1) = (g^\alpha, g^\beta, g^\gamma)$ and $(x_2, y_2, z_2) = (g^{\alpha'}, g^{\beta'}, g^{\gamma'})$, for $\alpha, \beta, \gamma \xleftarrow{\$} \mathbb{Z}_q$ and $\alpha' \doteq \alpha + a, \beta' \doteq \beta c + b, \gamma' \doteq \gamma c + \alpha b + \beta a c + ab$. Hence, $\alpha', \beta', \gamma' \xleftarrow{\$} \mathbb{Z}_q$, which implies that (x_1, y_1, z_1) and (x_2, y_2, z_2) are identically distributed, thus $\rho_1(\mathbf{S}_1^{\mathsf{ddh}})$ and $\rho_2(\mathbf{S}_1^{\mathsf{ddh}})$ have the same behavior.

Therefore,

$$\begin{aligned}
[\![\mathbf{E}_{pk_1}, \mathbf{E}_{pk_1}, pk_1, pk_2]\!] &\equiv \rho_1(\mathbf{S}_0^{\mathsf{ddh}}) \\
&\eqsim \rho_1(\mathbf{S}_1^{\mathsf{ddh}}) && (\mathsf{ddh}) \\
&\equiv \rho_2(\mathbf{S}_1^{\mathsf{ddh}}) \\
&\eqsim \rho_2(\mathbf{S}_0^{\mathsf{ddh}}) && (\mathsf{ddh}) \\
&\equiv [\![\mathbf{E}_{pk_1}, \mathbf{E}_{pk_2}, pk_1, pk_2]\!]. && \square
\end{aligned}$$

Lemma 5.5.8. $\mathsf{ddh} \xrightarrow{2} \mathsf{ulk\text{-}cpa}^{\Pi_{\mathsf{URE\text{-}ElGamal}}}$.

Proof. For $i \in \{1, 2\}$, consider $\rho_i(\mathbf{X}) \equiv [\![\mathbf{X}', pk]\!]$, which initially inputs $\diamond$ to $\mathbf{X}$, obtains (x, y, z), sets $pk \doteq x$, and with system $\mathbf{X}'$ behaving as follows: On input $m \in \mathbb{G}$, get $u, v, \kappa_1, u', v', \kappa_1' \xleftarrow{\$} \mathbb{Z}_q$, and set $c_1 \doteq (m \cdot z^u x^v, y^u g^v, x^{\kappa_1} g^{\kappa_1}, g^{\kappa_1})$ and $c_2' \doteq (m \cdot z^{u'} x^{v'}, y^{u'} g^{v'}, x^{\kappa_1'} g^{\kappa_1'}, g^{\kappa_1'})$. Then set $c_2 \doteq c_1$, $\hat{c}_1 \doteq \mathtt{Rnc}(c_1)$, and $\hat{c}_2 \doteq \mathtt{Rnc}(c_2')$. Finally, output $(c_i, \hat{c}_i)$. Then:

- $\rho_1(\mathbf{S}_0^{\mathsf{ddh}}) \equiv [\![\mathbf{E}_{pk} \triangleright \langle *, \mathbf{R} \rangle, pk]\!]$: As we already showed in the proof of Lemma 5.5.6, if $(x, y, z) = (g^\alpha, g^\beta, g^{\alpha\beta})$, for $\alpha, \beta \xleftarrow{\$} \mathbb{Z}_q$, then $(m \cdot z^u x^v, y^u g^v, x^{\kappa_1} g^{\kappa_1}, g^{\kappa_1})$ is distributed exactly as the output of $\mathbf{E}_{pk}$ on input m, therefore $(c_1, \hat{c}_1)$ is distributed exactly as the output of $\mathbf{E}_{pk} \triangleright \langle *, \mathbf{R} \rangle$ on input m.

- $\rho_2(\mathbf{S}_0^{\mathsf{ddh}}) \equiv [\![\langle \mathbf{E}_{pk}, \mathbf{E}_{pk} \triangleright \mathbf{R} \rangle, pk]\!]$: As we already showed in the proof of Lemma 5.5.6, if $(x, y, z) = (g^\alpha, g^\beta, g^{\alpha\beta})$, for $\alpha, \beta \xleftarrow{\$} \mathbb{Z}_q$, then $(m \cdot z^u x^v, y^u g^v, x^{\kappa_1} g^{\kappa_1}, g^{\kappa_1})$ and $(m \cdot z^{u'} x^{v'}, y^{u'} g^{v'}, x^{\kappa_1'} g^{\kappa_1'}, g^{\kappa_1'})$ are independent and both distributed exactly as the output of $\mathbf{E}_{pk}$ on input m, therefore $(c_2, \hat{c}_2)$ is distributed exactly as the output of $\langle \mathbf{E}_{pk}, \mathbf{E}_{pk} \triangleright \mathbf{R} \rangle$ on input m.

- $\rho_1(\mathbf{S}_1^{\mathsf{ddh}}) \equiv \rho_2(\mathbf{S}_1^{\mathsf{ddh}})$: We have that $(x, y, z) = (g^\alpha, g^\beta, g^\gamma)$, for $\alpha, \beta, \gamma \xleftarrow{\$} \mathbb{Z}_q$, which implies that $(c_1, \hat{c}_1)$ and $(c_2, \hat{c}_2)$ are identically distributed, thus $\rho_1(\mathbf{S}_1^{\mathsf{ddh}})$ and $\rho_2(\mathbf{S}_1^{\mathsf{ddh}})$ have the same behavior.

Therefore,

$$\begin{aligned}
[\![\mathbf{E}_{pk} \triangleright \langle *, \mathbf{R}\rangle, pk]\!] &\equiv \rho_1(\mathbf{S}_0^{\mathsf{ddh}}) \\
&\eqsim \rho_1(\mathbf{S}_1^{\mathsf{ddh}}) && (\mathsf{ddh}) \\
&\equiv \rho_2(\mathbf{S}_1^{\mathsf{ddh}}) \\
&\eqsim \rho_2(\mathbf{S}_0^{\mathsf{ddh}}) && (\mathsf{ddh}) \\
&\equiv [\![\langle \mathbf{E}_{pk}, \mathbf{E}_{pk} \triangleright \mathbf{R}\rangle, pk]\!]. && \square
\end{aligned}$$

Lemma 5.5.9. $\mathsf{ddh} \xrightarrow{2} \mathsf{sulk\text{-}cpa}^{\Pi_{\mathsf{URE\text{-}ElGamal}}}$.

Proof. Similar to the proof of Lemma 5.5.8. $\square$

We can now reduce the security of the construction all the way down to a single assumption, ddh. For this, first note that by combining Lemmata 5.5.4, 5.5.5 and 5.3.34, we obtain the following result.

Corollary 5.5.10. $n\text{-}\mathsf{cor\text{-}rob}^{\Pi_{\mathsf{URE\text{-}ElGamal}}}$ *holds unconditionally with probability* $\frac{n(n-1)}{q}$.

Moreover, by combining Lemmata 5.5.6, 5.5.7, 5.5.9, 5.3.24 and 5.3.36, we obtain the following result.

Corollary 5.5.11. $\mathsf{ddh} \xrightarrow{5(n-1)} n\text{-}\mathsf{ind\text{-}ik\text{-}sulk\text{-}cpa}^{\Pi_{\mathsf{URE\text{-}ElGamal}}}$.

Finally, Corollaries 5.5.10 and 5.5.11 imply the following result.

Corollary 5.5.12.

$$\left[1\text{-}\mathsf{AUT}^{\mathcal{PK}}_{\mathcal{R}\to\mathcal{S}}, \mathsf{AUT}^{\mathcal{C}}_{\mathcal{S}\to M}, \mathsf{AUT}^{\{\diamond\}\cup 2^{\mathcal{C}}}_{M\leftrightarrow\mathcal{R}}\right] \xrightarrow{\boldsymbol{\pi}_{\mathsf{URE}};\,\mathsf{ddh}} \mathsf{ULK}^{\mathcal{M}}_{\mathcal{S}\to\mathcal{R}}.$$

Chapter 6

Conclusion

In this thesis we continued the important task of expanding the library of construction statements in constructive cryptography, specifically by filling gaps in the composable treatment of schemes designed with anonymity-focused applications in mind. As a result, we have gained a deeper understanding of the practical applications of these schemes and the essential security notions required for their effective utilization. Along the way, we also introduced a new framework for reasoning about security notions, which lends itself as a unifier of game-based and composable notions. We next discuss in more details our results and some open problems.

The Substitutions Framework. In Chapter 2, we put forth the framework of substitutions, which we consistently used throughout the thesis to define and relate security notions, both game-based and composable ones. This abstract framework allowed us to greatly simplify proofs, that if otherwise carried out in one of the conventional languages commonly used in the cryptographic literature, would have potentially been longer, less formal, and more prone to contain gaps.

Being for the most part algebraic, our framework potentially enables the automated verification, which is an interesting open problem. We hope that our framework spark interest in the cryptographic and sees adoption outside of the scope of this thesis.

Secret-Key Anonymity Preservation. In Chapter 3, we focused on

filling a gap in the composable treatment of anonymity preservation in the *secret-key* setting. We began by casting key-indistinguishability notions for symmetric-key encryption from the literature into our substitution framework, and we also proposed new notions capturing anonymity for authenticated encryption. We then verified with a composable analysis, that indeed such notions capture anonymity preservation.

We focused on the case of many senders and a single receiver. A natural follow-up would be the study of the dual case of a single sender and multiple receivers.

Public-Key Anonymity Preservation. In Chapter 4, we focused on filling a gap in the composable treatment of anonymity preservation in the *public-key* setting. This gap proved more challenging to fill, since we begun with an impossibility result. We then identified three possible alternative approaches to fill the gap, ranging from anonymous authenticity, through de-anonymizable authenticity, to receiver-side anonymous authenticity. For the first, we used a new type of schemes, bilateral signatures, for the second we used partial signatures, and for the latter we used ring signatures.

Since the scope of this work was very ample, we see it as merely paving the way. For example, additional alternative solutions circumventing our impossibility result, employing different schemes, might be interesting to analyze. Moreover, all of our results hold under static corruptions, therefore a natural extension would be to consider a stronger security model capturing adaptive corruptions. This would allow to rely on stronger game-based notions from the literature for partial signatures and ring signatures.

Anonymity Creation. Finally, in Chapter 5 we shifted our focus from the preservation of anonymity to its *creation* (in the public-key setting). We did so by first identifying the minimal game-based definitions of universal re-encryption (URE) that truly capture its essence, which we established to be unlinkability, a property that was previously entangled with confidentiality and key-indistinguishability. We then attested this by providing composable semantics for URE, where we showed that indeed the careful use of this scheme yields an unlinkable network, which enables anonymous communication, under the right circumstances.

We only considered the case of a single honest mixer, and left open the problem to consider more, and potentially dishonest ones.

Appendix A

Details of Chapter 3

A.1 Weak Robustness

Recall the cascading operator $\triangleright$ for systems defined informally in Section 3.2.3 (and also formally defined later in Definition 5.2.2). Then, weak robustness (wrob) for authenticated encryption is simply defined as the substitution

$$\mathbf{E}_{k_1} \triangleright \mathbf{D}_{k_2} \eqsim \bot\!\!\!\bot$$

for $k_1, k_2 \leftarrow \mathsf{Gen}$, and where the system $\bot\!\!\!\bot$ always outputs $\bot$ (also formally defined later in Definition 5.2.1). Now, to see that indeed 2-ik-ae implies wrob, consider

$$\rho([\![[\![\mathbf{X}_1, \mathbf{Y}_1]\!], [\![\mathbf{X}_2, \mathbf{Y}_2]\!]]\!]) \doteq \mathbf{X}_1 \triangleright \mathbf{Y}_2.$$

Then:

$$\begin{aligned} \mathbf{E}_{k_1} \triangleright \mathbf{D}_{k_2} &= \rho([[\![\mathbf{E}_{k_1}, \mathbf{D}_{k_1}]\!], [\![\mathbf{E}_{k_2}, \mathbf{D}_{k_2}]\!]]) \\ &\eqsim \rho([\![\rho^{\mathsf{ae}}(\mathbf{E}_{k_1}), \rho^{\mathsf{ae}}(\mathbf{E}_{k_1})]\!]) && \text{(2-ik-cca)} \\ &\equiv \bot\!\!\!\bot, && \text{(A.1)} \end{aligned}$$

where we next justify equation (A.1). The system $\rho([\![\rho^{\mathsf{ae}}(\mathbf{E}_{k_1}), \rho^{\mathsf{ae}}(\mathbf{E}_{k_1})]\!])$ internally keeps a set $\mathcal{Q}_1 \subseteq \mathcal{M} \times \mathcal{C}$ for the first instance of $\rho^{\mathsf{ae}}(\mathbf{E}_{k_1})$ and a set $\mathcal{Q}_2 \subseteq \mathcal{M} \times \mathcal{C}$ for the second instance of $\rho^{\mathsf{ae}}(\mathbf{E}_{k_1})$, but only $\mathcal{Q}_1$ is updated after each new query to $\rho([\![\rho^{\mathsf{ae}}(\mathbf{E}_{k_1}), \rho^{\mathsf{ae}}(\mathbf{E}_{k_1})]\!])$, whereas $\mathcal{Q}_2$

always remains empty. Therefore, on input a message m, the system $\rho([\![\rho^{\mathsf{ae}}(\mathbf{E}_{k_1}), \rho^{\mathsf{ae}}(\mathbf{E}_{k_1})]\!])$ checks whether a certain pair (m', c') in contained in $\mathcal{Q}_2$, but since the set is always empty, the check will always fail and therefore the decryption oracle emulated by the second instance of $\rho^{\mathsf{ae}}(\mathbf{E}_{k_1})$ will always output $\perp$, and so will $\rho([\![\rho^{\mathsf{ae}}(\mathbf{E}_{k_1}), \rho^{\mathsf{ae}}(\mathbf{E}_{k_1})]\!])$.

Using Lemma 2.3.2, this result can be easily generalized to any $n \in \mathbb{N}$.

Appendix B

Details of Chapter 5

B.1 Relations to Young and Yung's Notions

In this section we bridge the gap between our security notions ind-cpa, ik-cpa, ind-r-cpa, and ik-r-cpa, and the corresponding notions introduced by Young and Yung [YY18]. They phrase their four notions as *single-challenge*, *left-or-right*, *bit-guessing problems*. On the other hand, out notions are phrased as *multi-challenge*, *real-or-random*, *distinction problems* (abstracted as substitutions). It is trivial to transform a (uniform) bit-guessing problem into a distinction one, as well as relating a single-challenge to a multi-challenge one. Here we show that the equivalent multi-challenge distinction-based left-or-right notions of Young and Yung are equivalent to our real-or-random ones.

Another gap between our notions and Young and Yung's, which is unbridgeable, is that in their model the adversary can choose the randomness given to the encryption oracles. This could easily integrated in our setting, but we decided not to in order to keep the treatment self-contained.

B.1.1 Young and Yung's Original Notions.

Definition B.1.1 (lor-ind-cpa)**.**

$$[\![(\!|*,*|\!)_1 \triangleright \mathbf{E}_{pk}, pk]\!] \eqsim [\![(\!|*,*|\!)_2 \triangleright \mathbf{E}_{pk}, pk]\!],$$

for $(sk, pk) \leftarrow \texttt{Gen}$.

Definition B.1.2 (lor-ik-cpa)**.**

$$[\![\mathbf{E}_{pk_1}, pk_1, pk_2]\!] \eqsim [\![\mathbf{E}_{pk_2}, pk_1, pk_2]\!],$$

for independent $(sk_1, pk_1) \leftarrow \texttt{Gen}$ and $(sk_2, pk_2) \leftarrow \texttt{Gen}$.

Definition B.1.3 (lor-ind-r-cpa)**.**

$$[\![(\!|\mathbf{E}_{pk} \triangleright \langle *, \mathbf{R}\rangle, \mathbf{E}_{pk}|\!), pk]\!] \eqsim [\![(\!|\mathbf{E}_{pk}, \mathbf{E}_{pk} \triangleright \langle \mathbf{R}, *\rangle|\!), pk]\!],$$

for $(sk, pk) \leftarrow \texttt{Gen}$.

Definition B.1.4 (lor-ik-r-cpa)**.**

$$[\![\langle \mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R}\rangle, \mathbf{E}_{pk_2}\rangle, pk_1, pk_2]\!] \eqsim [\![\langle \mathbf{E}_{pk_1}, \mathbf{E}_{pk_2} \triangleright \langle \mathbf{R}, *\rangle\rangle, pk_1, pk_2]\!],$$

for independent $(sk_1, pk_1) \leftarrow \texttt{Gen}$ and $(sk_2, pk_2) \leftarrow \texttt{Gen}$.

B.1.2 Equivalence of the Notions.

Lemma B.1.5. lor-ind-cpa $\iff$ ind-cpa.

Proof.

- lor-ind-cpa $\xrightarrow{1}$ ind-cpa: Let $(sk, pk) \leftarrow \texttt{Gen}$ and consider $\rho([\![\mathbf{X}, x]\!]) \doteq [\![\langle *, \$\rangle \triangleright \mathbf{X}, x]\!]$. Then:

$$\begin{aligned}
[\![\mathbf{E}_{pk}, pk]\!] &\equiv [\![\langle *, \$\rangle \triangleright (\!|*, *|\!)_1 \triangleright \mathbf{E}_{pk}, pk]\!] \\
&= \rho([\![(\!|*, *|\!)_1 \triangleright \mathbf{E}_{pk}, pk]\!]) \\
&\eqsim \rho([\![(\!|*, *|\!)_2 \triangleright \mathbf{E}_{pk}, pk]\!]) && \text{(lor-ind-cpa)} \\
&= [\![\langle *, \$\rangle \triangleright (\!|*, *|\!)_2 \triangleright \mathbf{E}_{pk}, pk]\!] \\
&\equiv [\![\mathbf{E}^{\$}_{pk}, pk]\!].
\end{aligned}$$

- ind-cpa $\xrightarrow{2}$ lor-ind-cpa: Let $(sk, pk) \leftarrow \texttt{Gen}$ and consider $\rho_i([\![\mathbf{X}, x]\!]) \doteq$

$[\![(\!|*,*|\!)_i \triangleright \mathbf{X}, x]\!]$, for $i \in \{1,2\}$. Then:

$$\begin{aligned}
[\![(\!|*,*|\!)_1 \triangleright \mathbf{E}_{pk}, pk]\!] &= \rho_1([\![\mathbf{E}_{pk}, pk]\!]) \\
&\doteq \rho_1([\![\mathbf{E}^{\$}_{pk}, pk]\!]) && \text{(ind-cpa)} \\
&= [\![(\!|*,*|\!)_1 \triangleright \mathbf{E}^{\$}_{pk}, pk]\!] \\
&\equiv [\![(\!|*,*|\!)_2 \triangleright \mathbf{E}^{\$}_{pk}, pk]\!] \\
&= \rho_2([\![\mathbf{E}^{\$}_{pk}, pk]\!]) \\
&\doteq \rho_2([\![\mathbf{E}_{pk}, pk]\!]) && \text{(ind-cpa)} \\
&\equiv [\![(\!|*,*|\!)_2 \triangleright \mathbf{E}_{pk}, pk]\!]. && \square
\end{aligned}$$

Lemma B.1.6. lor-ik-cpa $\iff$ ik-cpa.

Proof.

- lor-ik-cpa $\xrightarrow{1}$ ik-cpa: Let $(sk_1, pk_1), (sk_2, pk_2) \leftarrow \texttt{Gen}$, and consider $\rho([\![\mathbf{X}, x, y]\!]) \doteq [\![\mathbf{E}_x, \mathbf{X}, x, y]\!]$. Then:

$$\begin{aligned}
[\![\mathbf{E}_{pk_1}, \mathbf{E}_{pk_2}, pk_1, pk_2]\!] &= \rho([\![\mathbf{E}_{pk_2}, pk_1, pk_2]\!]) \\
&\doteq \rho([\![\mathbf{E}_{pk_1}, pk_1, pk_2]\!]) && \text{(lor-ik-cpa)} \\
&= [\![\mathbf{E}_{pk_1}, \mathbf{E}_{pk_1}, pk_1, pk_2]\!].
\end{aligned}$$

- ik-cpa $\xrightarrow{1}$ lor-ik-cpa: Let $(sk_1, pk_1), (sk_2, pk_2) \leftarrow \texttt{Gen}$, and consider $\rho([\![\mathbf{X}, \mathbf{Y}, x, y]\!]) \doteq [\![\mathbf{Y}, x, y]\!]$. Then:

$$\begin{aligned}
[\![\mathbf{E}_{pk_1}, pk_1, pk_2]\!] &= \rho([\![\mathbf{E}_{pk_1}, \mathbf{E}_{pk_1}, pk_1, pk_2\,]\!]) \\
&\doteq \rho([\![\mathbf{E}_{pk_1}, \mathbf{E}_{pk_2}, pk_1, pk_2\,]\!]) && \text{(ik-cpa)} \\
&= [\![\mathbf{E}_{pk_2}, pk_1, pk_2]\!]. && \square
\end{aligned}$$

Lemma B.1.7. lor-ind-r-cpa $\iff$ ind-r-cpa.

Proof.

- lor-ind-r-cpa $\xrightarrow{1}$ ind-r-cpa: Let $(sk, pk) \leftarrow \texttt{Gen}$ and consider

$\rho(\llbracket \mathbf{X}, x \rrbracket) \doteq \llbracket \langle *, \$ \rangle \triangleright (\mathbf{X})_{1,2}, x \rrbracket$. Then:

$$\begin{aligned}
\llbracket \mathbf{E}_{pk} \triangleright \langle *, \mathbf{R} \rangle, pk \rrbracket &\equiv \llbracket \langle *, \$ \rangle \triangleright (\!|\mathbf{E}_{pk} \triangleright \langle *, \mathbf{R} \rangle, \mathbf{E}_{pk}|\!)_{1,2}, pk \rrbracket \\
&= \rho(\llbracket (\!|\mathbf{E}_{pk} \triangleright \langle *, \mathbf{R} \rangle, \mathbf{E}_{pk}|\!), pk \rrbracket) \\
&\eqsim \rho(\llbracket (\!|\mathbf{E}_{pk}, \mathbf{E}_{pk} \triangleright \langle \mathbf{R}, * \rangle|\!), pk \rrbracket) \quad \text{(lor-ind-r-cpa)} \\
&= \llbracket \langle *, \$ \rangle \triangleright (\!|\mathbf{E}_{pk}, \mathbf{E}_{pk} \triangleright \langle \mathbf{R}, * \rangle|\!)_{1,2}, pk \rrbracket \\
&\equiv \llbracket \langle \mathbf{E}_{pk}, \mathbf{E}^{\$}_{pk} \triangleright \mathbf{R} \rangle, pk \rrbracket.
\end{aligned}$$

- ind-r-cpa $\xrightarrow{2}$ lor-ind-r-cpa: Let $(sk, pk) \leftarrow \texttt{Gen}$ and consider $\rho_1(\llbracket \mathbf{X}, x \rrbracket) \doteq \llbracket (\!|\mathbf{X}, \mathbf{E}_x|\!), x \rrbracket$ and $\rho_2(\llbracket \mathbf{X}, x \rrbracket) \doteq \llbracket (\!|\mathbf{E}_x, (\mathbf{X})_{2,1}|\!), x \rrbracket$. Then:

$$\begin{aligned}
\llbracket (\!|\mathbf{E}_{pk} \triangleright \langle *, \mathbf{R} \rangle, \mathbf{E}_{pk}|\!), pk \rrbracket &= \rho_1(\llbracket \mathbf{E}_{pk} \triangleright \langle *, \mathbf{R} \rangle, pk \rrbracket) \\
&\eqsim \rho_1(\llbracket \langle \mathbf{E}_{pk}, \mathbf{E}^{\$}_{pk} \triangleright \mathbf{R} \rangle, pk \rrbracket) \quad \text{(ind-r-cpa)} \\
&= \llbracket (\!|\langle \mathbf{E}_{pk}, \mathbf{E}^{\$}_{pk} \triangleright \mathbf{R} \rangle, \mathbf{E}_{pk}|\!), pk \rrbracket \\
&= \llbracket (\!|\mathbf{E}_{pk}, \langle \mathbf{E}^{\$}_{pk} \triangleright \mathbf{R}, \mathbf{E}_{pk} \rangle|\!), pk \rrbracket \\
&\equiv \llbracket (\!|\mathbf{E}_{pk}, \langle \mathbf{E}_{pk}, \mathbf{E}^{\$}_{pk} \triangleright \mathbf{R} \rangle_{2,1}|\!), pk \rrbracket \\
&= \rho_2(\llbracket \langle \mathbf{E}_{pk}, \mathbf{E}^{\$}_{pk} \triangleright \mathbf{R} \rangle, pk \rrbracket) \\
&\eqsim \rho_2(\llbracket \mathbf{E}_{pk} \triangleright \langle *, \mathbf{R} \rangle, pk \rrbracket) \quad \text{(ind-r-cpa)} \\
&= \llbracket (\!|\mathbf{E}_{pk}, (\mathbf{E}_{pk} \triangleright \langle *, \mathbf{R} \rangle)_{2,1}|\!), pk \rrbracket \\
&\equiv \llbracket (\!|\mathbf{E}_{pk}, \mathbf{E}_{pk} \triangleright \langle \mathbf{R}, * \rangle|\!), pk \rrbracket. \qquad \square
\end{aligned}$$

Lemma B.1.8. lor-ik-r-cpa $\iff$ ik-r-cpa.

Proof.

- lor-ik-r-cpa $\xrightarrow{1}$ ik-r-cpa: Let $(sk_1, pk_1), (sk_2, pk_2) \leftarrow \texttt{Gen}$, and consider $\rho(\llbracket \mathbf{X}, x, y \rrbracket) \doteq \llbracket \mathbf{E}_x \triangleright \langle *, \mathbf{R} \rangle, (\mathbf{X})_{3,2}, x, y \rrbracket$. Then:

$$\begin{aligned}
&\llbracket \mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R} \rangle, \mathbf{E}_{pk_2} \triangleright \langle *, \mathbf{R} \rangle, pk_1, pk_2 \rrbracket \\
&\quad\equiv \llbracket \mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R} \rangle, \langle \mathbf{E}_{pk_1}, \mathbf{E}_{pk_2} \triangleright \langle \mathbf{R}, * \rangle \rangle_{3,2}, pk_1, pk_2 \rrbracket \\
&\quad= \rho(\llbracket \langle \mathbf{E}_{pk_1}, \mathbf{E}_{pk_2} \triangleright \langle \mathbf{R}, * \rangle \rangle, pk_1, pk_2 \rrbracket) \\
&\quad\eqsim \rho(\llbracket \langle \mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R} \rangle, \mathbf{E}_{pk_2} \rangle, pk_1, pk_2 \rrbracket) \quad \text{(lor-ik-r-cpa)} \\
&\quad= \llbracket \mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R} \rangle, \langle \mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R} \rangle, \mathbf{E}_{pk_2} \rangle_{3,2}, pk_1, pk_2 \rrbracket \\
&\quad\equiv \llbracket \mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R} \rangle, \langle \mathbf{E}_{pk_2}, \mathbf{E}_{pk_1} \triangleright \mathbf{R} \rangle, pk_1, pk_2 \rrbracket.
\end{aligned}$$

- ik-r-cpa $\xrightarrow{3}$ lor-ik-r-cpa: Note that, by Lemma 5.3.15, ik-r-cpa $\xrightarrow{2}$ ulk-cpa. Therefore, we can use

$$[\![\langle \mathbf{E}_{pk_2}, \mathbf{E}_{pk_2} \triangleright \mathbf{R}\rangle, pk_2]\!] \doteqdot [\![\mathbf{E}_{pk_2} \triangleright \langle *, \mathbf{R}\rangle, pk_2]\!],$$

  which means we are using ik-r-cpa twice. Let $(sk_1, pk_1), (sk_2, pk_2) \leftarrow \mathtt{Gen}$, and consider

  - $\rho_1([\![\mathbf{X}, \mathbf{Y}, x, y]\!]) \doteq [\![\langle \mathbf{Y}, \mathbf{E}_x\rangle, y, x]\!]$ and
  - $\rho_2([\![\mathbf{X}, x]\!]) \doteq [\![\langle \mathbf{E}_{pk_1}, (\mathbf{X})_{2,1}\rangle, pk_1, x\rangle]\!]$.

  Then:

$$\begin{aligned}
&[\![\langle \mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R}\rangle, \mathbf{E}_{pk_2}\rangle, pk_1, pk_2]\!] \\
&\quad = \rho_1([\![\mathbf{E}_{pk_2} \triangleright \langle *, \mathbf{R}\rangle, \mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R}\rangle, pk_2, pk_1]\!]) \\
&\quad \doteqdot \rho_1([\![\mathbf{E}_{pk_2} \triangleright \langle *, \mathbf{R}\rangle, \langle \mathbf{E}_{pk_1}, \mathbf{E}_{pk_2} \triangleright \mathbf{R}\rangle, pk_2, pk_1]\!]) && \text{(ik-r-cpa)} \\
&\quad = [\![\langle \langle \mathbf{E}_{pk_1}, \mathbf{E}_{pk_2} \triangleright \mathbf{R}\rangle, \mathbf{E}_{pk_2}\rangle, pk_1, pk_2]\!] \\
&\quad \equiv [\![\langle \mathbf{E}_{pk_1}, \langle \mathbf{E}_{pk_2} \triangleright \mathbf{R}, \mathbf{E}_{pk_2}\rangle\rangle, pk_1, pk_2]\!] \\
&\quad \equiv [\![\langle \mathbf{E}_{pk_1}, \langle \mathbf{E}_{pk_2}, \mathbf{E}_{pk_2} \triangleright \mathbf{R}\rangle_{2,1}\rangle, pk_1, pk_2]\!] \\
&\quad = \rho_2([\![\langle \mathbf{E}_{pk_2}, \mathbf{E}_{pk_2} \triangleright \mathbf{R}\rangle, pk_2]\!]) \\
&\quad \doteqdot \rho_2([\![\mathbf{E}_{pk_2} \triangleright \langle *, \mathbf{R}\rangle, pk_2]\!]) && \text{(ulk-cpa)} \\
&\quad = [\![\langle \mathbf{E}_{pk_1}, (\mathbf{E}_{pk_2} \triangleright \langle *, \mathbf{R}\rangle)_{2,1}\rangle, pk_1, pk_2]\!] \\
&\quad = [\![\langle \mathbf{E}_{pk_1}, \mathbf{E}_{pk_2} \triangleright \langle \mathbf{R}, *\rangle\rangle, pk_1, pk_2]\!]. && \square
\end{aligned}$$

B.1.3 Variant of Combined Notions

In this section we introduce a different combined notion, ind-ik-r-cpa, that would result by naturally combining Young and Yung's ind-r-cpa and ik-r-cpa notions. We show that together, those two notions imply ind-ik-r-cpa, and also that ind-ik-r-cpa is implied by the combined notion for confidentiality and anonymity, ind-ik-cpa, taken together with unlinkability. All shown relations are summarized in Figure B.1. Nevertheless, ind-ik-r-cpa is less directly relatable to our composable notions than ind-ik-ulk-cpa.

Definition B.1.9 (ind-ik-cpa)**.**

$$[\![\mathbf{E}_{pk_1}, \mathbf{E}_{pk_2}, pk_1, pk_2]\!] \doteqdot [\![\mathbf{E}^{\$}_{pk_1}, \mathbf{E}^{\$}_{pk_1}, pk_1, pk_2]\!],$$

for independent $(sk_1, pk_1), (sk_2, pk_2) \leftarrow \mathtt{Gen}$.

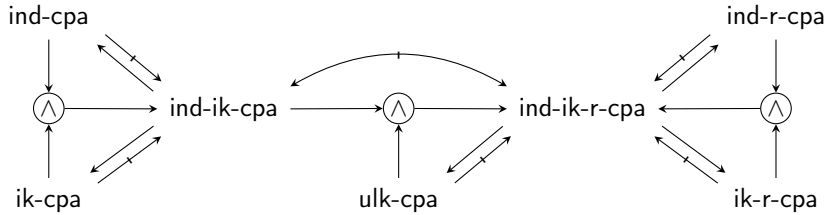


Figure B.1: Relations among ciphertext-indistinguishability, key-indistinguishability, and unlinkability.

Definition B.1.10 (ind-ik-r-cpa)**.**

$$[\![\mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R}\rangle, \mathbf{E}_{pk_2} \triangleright \langle *, \mathbf{R}\rangle, pk_1, pk_2]\!]$$
$$\hat{=}$$
$$[\![\langle \mathbf{E}_{pk_1}, \mathbf{E}^{\$}_{pk_1} \triangleright \mathbf{R}\rangle, \langle \mathbf{E}_{pk_2}, \mathbf{E}^{\$}_{pk_1} \triangleright \mathbf{R}\rangle, pk_1, pk_2]\!],$$

for independent $(sk_1, pk_1), (sk_2, pk_2) \leftarrow \mathtt{Gen}$.

Lemma B.1.11. $(\mathsf{ind\text{-}cpa}, \mathsf{ik\text{-}cpa}) \iff \mathsf{ind\text{-}ik\text{-}cpa}$.

Proof.

- $(\mathsf{ind\text{-}cpa}, \mathsf{ik\text{-}cpa}) \xrightarrow{1,1} \mathsf{ind\text{-}ik\text{-}cpa}$: Let $(sk_1, pk_1), (sk_2, pk_2) \leftarrow \mathtt{Gen}$ and consider $\rho([\![\mathbf{X}, x]\!]) \doteq [\![\mathbf{X}, \mathbf{X}, x, pk_2]\!]$. Then:

$$\begin{aligned}
[\![\mathbf{E}_{pk_1}, \mathbf{E}_{pk_2}, pk_1, pk_2]\!] &\hat{=} [\![\mathbf{E}_{pk_1}, \mathbf{E}_{pk_1}, pk_1, pk_2]\!] && (\mathsf{ik\text{-}cpa})\\
&= \rho([\![\mathbf{E}_{pk_1}, pk_1]\!])\\
&\hat{=} \rho([\![\mathbf{E}^{\$}_{pk_1}, pk_1]\!]) && (\mathsf{ind\text{-}cpa})\\
&= [\![\mathbf{E}^{\$}_{pk_1}, \mathbf{E}^{\$}_{pk_1}, pk_1, pk_2]\!].
\end{aligned}$$

- $\mathsf{ind\text{-}ik\text{-}cpa} \xrightarrow{1} \mathsf{ind\text{-}cpa}$: Let $(sk, pk), (sk', pk') \leftarrow \mathtt{Gen}$, and consider

$\rho([\![\mathbf{X}, \mathbf{Y}, x, y]\!]) \doteq [\![\mathbf{X}, x]\!]$. Then:

$$\begin{aligned}
[\![\mathbf{E}_{pk}, pk]\!] &= \rho([\![\mathbf{E}_{pk}, \mathbf{E}_{pk'}, pk, pk']\!]) \\
&\eqsim \rho([\![\mathbf{E}^{\$}_{pk}, \mathbf{E}^{\$}_{pk}, pk, pk']\!]) && \text{(ind-ik-cpa)} \\
&= [\![\mathbf{E}^{\$}_{pk}, pk]\!].
\end{aligned}$$

- ind-ik-cpa $\xrightarrow{2}$ ik-cpa: Let $(sk_1, pk_1), (sk_2, pk_2) \leftarrow \mathtt{Gen}$, and consider $\rho_i([\![\mathbf{X}_1, \mathbf{X}_2, x, y]\!]) \doteq [\![\mathbf{E}_x, \mathbf{X}_{1-i}, x, y]\!]$, for $i \in \{1, 2\}$. Then:

$$\begin{aligned}
[\![\mathbf{E}_{pk_1}, \mathbf{E}_{pk_2}, pk_1, pk_2]\!] &= \rho_1([\![\mathbf{E}_{pk_1}, \mathbf{E}_{pk_2}, pk_1, pk_2]\!]) \\
&\eqsim \rho_1([\![\mathbf{E}^{\$}_{pk_1}, \mathbf{E}^{\$}_{pk_1}, pk_1, pk_2]\!]) && \text{(ind-ik-cpa)} \\
&= [\![\mathbf{E}_{pk_1}, \mathbf{E}^{\$}_{pk_1}, pk_1, pk_2]\!] \\
&= \rho_2([\![\mathbf{E}^{\$}_{pk_1}, \mathbf{E}^{\$}_{pk_1}, pk_1, pk_2]\!]) \\
&\eqsim \rho_2([\![\mathbf{E}_{pk_1}, \mathbf{E}_{pk_2}, pk_1, pk_2]\!]) && \text{(ind-ik-cpa)} \\
&= [\![\mathbf{E}_{pk_1}, \mathbf{E}_{pk_1}, pk_1, pk_2]\!]. && \square
\end{aligned}$$

Lemma B.1.12. ind-cpa $\not\longrightarrow$ ind-ik-cpa.

Proof. Let $\Pi \doteq (\mathtt{Gen}, \mathtt{Enc}, \mathtt{Rnc}, \mathtt{Dec})$. For any $(sk, pk) \in \operatorname{supp} \mathtt{Gen}$, define $\Pi' \doteq (\mathtt{Gen}', \mathtt{Enc}', \mathtt{Rnc}', \mathtt{Dec}')$ as:

- $\mathtt{Gen}' \doteq \mathtt{Gen}$;
- $\mathtt{Enc}'_{pk}(m) \doteq (\mathtt{Enc}_{pk}(m), pk)$, for any $m \in \mathcal{M}$;
- $\mathtt{Rnc}'((c, pk')) \doteq (\mathtt{Rnc}(c), pk')$, for any $(c, pk') \in \mathcal{C} \times \mathcal{PK}$;
- $\mathtt{Dec}'_{sk}((c, pk')) \doteq \mathtt{Dec}_{sk}(c)$, for any $(c, pk') \in \mathcal{C} \times \mathcal{PK}$;

with corresponding systems $\mathbf{E}'_{pk}$, $\mathbf{R}'$, and $\mathbf{D}'_{sk}$. Let $(sk, pk) \leftarrow \mathtt{Gen}$. If Π is correct, then Π' is clearly also correct, and if

$$[\![\mathbf{E}_{pk}, pk]\!] \eqsim [\![\mathbf{E}^{\$}_{pk}, pk]\!],$$

then with $\rho([\![\mathbf{X}, x]\!]) \doteq [\![\mathbf{X} \triangleright \langle *, x\rangle, x]\!]$,

$$\begin{aligned}
[\![\mathbf{E}'_{pk}, pk]\!] &\equiv [\![\mathbf{E}_{pk} \triangleright \langle *, pk\rangle, pk]\!] \\
&= \rho([\![\mathbf{E}_{pk}, pk]\!]) \\
&\eqsim \rho([\![\mathbf{E}^{\$}_{pk}, pk]\!]) \\
&= [\![\mathbf{E}^{\$}_{pk} \triangleright \langle *, pk\rangle, pk]\!] \\
&\equiv [\![\mathbf{E}'^{\$}_{pk}, pk]\!].
\end{aligned}$$

But clearly, for $(sk_1, pk_1), (sk_2, pk_2) \leftarrow \mathtt{Gen}$,

$$\begin{aligned}
[\![\mathbf{E}'_{pk_1}, \mathbf{E}'_{pk_2}, pk_1, pk_2]\!] &\equiv [\![\mathbf{E}_{pk_1} \triangleright \langle *, pk_1\rangle, \mathbf{E}_{pk_2} \triangleright \langle *, pk_2\rangle, pk_1, pk_2]\!] \\
&\neq [\![\mathbf{E}^{\$}_{pk_1} \triangleright \langle *, pk_1\rangle, \mathbf{E}^{\$}_{pk_1} \triangleright \langle *, pk_1\rangle, pk_1, pk_2]\!] \\
&\equiv [\![\mathbf{E}'^{\$}_{pk_1}, \mathbf{E}'^{\$}_{pk_1}, pk_1, pk_2]\!].
\end{aligned}$$

□

Lemma B.1.13. ik-cpa $\not\to$ ind-ik-cpa.

Proof. Let $\Pi \doteq (\mathtt{Gen}, \mathtt{Enc}, \mathtt{Rnc}, \mathtt{Dec})$. For any $(sk, pk) \in \operatorname{supp} \mathtt{Gen}$, define $\Pi' \doteq (\mathtt{Gen}', \mathtt{Enc}', \mathtt{Rnc}', \mathtt{Dec}')$ as:

- $\mathtt{Gen}' \doteq \mathtt{Gen}$;
- $\mathtt{Enc}'_{pk}(m) \doteq (\mathtt{Enc}_{pk}(m), m)$, for any $m \in \mathcal{M}$;
- $\mathtt{Rnc}'((c, m)) \doteq (\mathtt{Rnc}(c), m)$, for any $(c, m) \in \mathcal{C} \times \mathcal{M}$;
- $\mathtt{Dec}'_{sk}((c, m)) \doteq \mathtt{Dec}_{sk}(c)$, for any $(c, m) \in \mathcal{C} \times \mathcal{M}$;

with corresponding systems $\mathbf{E}'_{pk}$, $\mathbf{R}'$, and $\mathbf{D}'_{sk}$. Let $(sk_1, pk_1), (sk_2, pk_2) \leftarrow \mathtt{Gen}$. If Π is correct, then Π' is clearly also correct, and if

$$[\![\mathbf{E}_{pk_1}, \mathbf{E}_{pk_2}, pk_1, pk_2]\!] \eqsim [\![\mathbf{E}_{pk_1}, \mathbf{E}_{pk_1}, pk_1, pk_2]\!],$$

then with $\rho([\![\mathbf{X}, x]\!]) \doteq [\![\langle \mathbf{X}, * \rangle, x]\!]$,

$$\begin{aligned}
[\![\mathbf{E}'_{pk}, pk]\!] &\equiv [\![\langle \mathbf{E}_{pk}, * \rangle, pk]\!] \\
&= \rho([\![\mathbf{E}_{pk}, pk]\!]) \\
&\eqsim \rho([\![\mathbf{E}^{\$}_{pk}, pk]\!]) \\
&= [\![\langle \mathbf{E}^{\$}_{pk}, * \rangle, pk]\!] \\
&\equiv [\![\mathbf{E}'^{\$}_{pk}, pk]\!].
\end{aligned}$$

But clearly,

$$\begin{aligned}\llbracket \mathbf{E}'_{pk_1}, \mathbf{E}'_{pk_2}, pk_1, pk_2 \rrbracket &\equiv \llbracket \langle \mathbf{E}_{pk_1}, * \rangle, \langle \mathbf{E}_{pk_2}, * \rangle, pk_1, pk_2 \rrbracket \\ &\neq \llbracket \$ \triangleright \langle \mathbf{E}_{pk_1}, * \rangle, \$ \triangleright \langle \mathbf{E}_{pk_1}, * \rangle, pk_1, pk_2 \rrbracket \\ &\equiv \llbracket \mathbf{E}'^{\$}_{pk_1}, \mathbf{E}'^{\$}_{pk_1}, pk_1, pk_2 \rrbracket. \end{aligned}$$ □

Lemma B.1.14. $(\mathsf{ind\text{-}r\text{-}cpa}, \mathsf{ik\text{-}r\text{-}cpa}) \iff \mathsf{ind\text{-}ik\text{-}r\text{-}cpa}$.

Proof.

- $(\mathsf{ind\text{-}r\text{-}cpa}, \mathsf{ik\text{-}r\text{-}cpa}) \xrightarrow{1,1} \mathsf{ind\text{-}ik\text{-}r\text{-}cpa}$: Let $(sk_1, pk_1), (sk_2, pk_2) \leftarrow \mathtt{Gen}$, and consider $\rho(\llbracket \mathbf{X}, x \rrbracket) \doteq \llbracket \mathbf{X}, \langle \mathbf{E}_{pk_2}, (\mathbf{X})_2 \rangle, x, pk_2 \rrbracket$. Then:

$$\begin{aligned}&\llbracket \mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R} \rangle, \mathbf{E}_{pk_2} \triangleright \langle *, \mathbf{R} \rangle, pk_1, pk_2 \rrbracket \\ &\quad \eqsim \llbracket \mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R} \rangle, \langle \mathbf{E}_{pk_2}, \mathbf{E}_{pk_1} \triangleright \mathbf{R} \rangle, pk_1, pk_2 \rrbracket && (\mathsf{ik\text{-}r\text{-}cpa}) \\ &\quad \equiv \llbracket \mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R} \rangle, \langle \mathbf{E}_{pk_2}, (\mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R} \rangle)_2 \rangle, pk_1, pk_2 \rrbracket \\ &\quad = \rho(\llbracket \mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R} \rangle, pk_1 \rrbracket) \\ &\quad \eqsim \rho(\llbracket \langle \mathbf{E}_{pk_1}, \mathbf{E}^{\$}_{pk_1} \triangleright \mathbf{R} \rangle, pk_1 \rrbracket) && (\mathsf{ind\text{-}r\text{-}cpa}) \\ &\quad = \llbracket \langle \mathbf{E}_{pk_1}, \mathbf{E}^{\$}_{pk_1} \triangleright \mathbf{R} \rangle, \langle \mathbf{E}_{pk_2}, \langle \mathbf{E}_{pk_1}, \mathbf{E}^{\$}_{pk_1} \triangleright \mathbf{R} \rangle_2 \rangle, pk_1, pk_2 \rrbracket \\ &\quad \equiv \llbracket \langle \mathbf{E}_{pk_1}, \mathbf{E}^{\$}_{pk_1} \triangleright \mathbf{R} \rangle, \langle \mathbf{E}_{pk_2}, \mathbf{E}^{\$}_{pk_1} \triangleright \mathbf{R} \rangle, pk_1, pk_2 \rrbracket. \end{aligned}$$

- $\mathsf{ind\text{-}ik\text{-}r\text{-}cpa} \xrightarrow{1} \mathsf{ind\text{-}r\text{-}cpa}$: Let $(sk, pk), (sk', pk') \leftarrow \mathtt{Gen}$, and consider $\rho(\llbracket \mathbf{X}, \mathbf{Y}, x, y \rrbracket) \doteq \llbracket \mathbf{X}, x \rrbracket$. Then:

$$\begin{aligned}\llbracket \mathbf{E}_{pk} \triangleright \langle *, \mathbf{R} \rangle, pk \rrbracket &= \rho(\llbracket \mathbf{E}_{pk} \triangleright \langle *, \mathbf{R} \rangle, \mathbf{E}_{pk'} \triangleright \langle *, \mathbf{R} \rangle, pk, pk' \rrbracket) \\ &\eqsim \rho(\llbracket \langle \mathbf{E}_{pk}, \mathbf{E}^{\$}_{pk} \triangleright \mathbf{R} \rangle, \langle \mathbf{E}_{pk'}, \mathbf{E}^{\$}_{pk} \triangleright \mathbf{R} \rangle, pk, pk' \rrbracket) \\ &\qquad (\mathsf{ind\text{-}ik\text{-}r\text{-}cpa}) \\ &= \llbracket \langle \mathbf{E}_{pk}, \mathbf{E}^{\$}_{pk} \triangleright \mathbf{R} \rangle, pk \rrbracket. \end{aligned}$$

- $\mathsf{ind\text{-}ik\text{-}r\text{-}cpa} \xrightarrow{2} \mathsf{ik\text{-}r\text{-}cpa}$: Let $(sk_1, pk_1), (sk_2, pk_2) \leftarrow \mathtt{Gen}$, and consider
  - $\rho_1(\llbracket \mathbf{X}, \mathbf{Y}, x, y \rrbracket) \doteq \llbracket \mathbf{E}_x \triangleright \langle *, \mathbf{R} \rangle, \mathbf{Y}, x, y \rrbracket$ and

– $\rho_2([\![\mathbf{X}, \mathbf{Y}, x, y]\!]) \doteq [\![\mathbf{E}_x \triangleright \langle *, \mathbf{R}\rangle, \langle \mathbf{E}_y, (\mathbf{X})_2\rangle, x, y]\!]$.

Then:

$$
\begin{aligned}
&[\![\mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R}\rangle, \mathbf{E}_{pk_2} \triangleright \langle *, \mathbf{R}\rangle, pk_1, pk_2]\!] \\
&\quad = \rho_1([\![\mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R}\rangle, \mathbf{E}_{pk_2} \triangleright \langle *, \mathbf{R}\rangle, pk_1, pk_2]\!]) \\
&\quad \simeq \rho_1([\![\langle \mathbf{E}_{pk_1}, \mathbf{E}^{\$}_{pk_1} \triangleright \mathbf{R}\rangle, \langle \mathbf{E}_{pk_2}, \mathbf{E}^{\$}_{pk_1} \triangleright \mathbf{R}\rangle, pk_1, pk_2]\!]) \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad (\textsf{ind-ik-r-cpa}) \\
&\quad = [\![\mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R}\rangle, \langle \mathbf{E}_{pk_2}, \mathbf{E}^{\$}_{pk_1} \triangleright \mathbf{R}\rangle, pk_1, pk_2]\!] \\
&\quad \equiv [\![\mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R}\rangle, \langle \mathbf{E}_{pk_2}, \langle \mathbf{E}_{pk_1}, \mathbf{E}^{\$}_{pk_1} \triangleright \mathbf{R}\rangle_2\rangle, pk_1, pk_2]\!] \\
&\quad = \rho_2([\![\langle \mathbf{E}_{pk_1}, \mathbf{E}^{\$}_{pk_1} \triangleright \mathbf{R}\rangle, \langle \mathbf{E}_{pk_2}, \mathbf{E}^{\$}_{pk_1} \triangleright \mathbf{R}\rangle, pk_1, pk_2]\!]) \\
&\quad \simeq \rho_2([\![\mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R}\rangle, \mathbf{E}_{pk_2} \triangleright \langle *, \mathbf{R}\rangle, pk_1, pk_2]\!]) \qquad (\textsf{ind-ik-r-cpa}) \\
&\quad \equiv [\![\mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R}\rangle, \langle \mathbf{E}_{pk_2}, (\mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R}\rangle)_2\rangle, pk_1, pk_2]\!] \\
&\quad = [\![\mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R}\rangle, \langle \mathbf{E}_{pk_2}, \mathbf{E}_{pk_1} \triangleright \mathbf{R}\rangle, pk_1, pk_2]\!]. \qquad \square
\end{aligned}
$$

Lemma B.1.15. ind-r-cpa $\not\longrightarrow$ ind-ik-r-cpa.

Proof. Analogous to the proof of Lemma B.1.12. □

Lemma B.1.16. ik-r-cpa $\not\longrightarrow$ ind-ik-r-cpa.

Proof. Analogous to the proof of Lemma B.1.13. □

Lemma B.1.17. (ind-ik-cpa, ulk-cpa) $\xrightarrow{1,2}$ ind-ik-r-cpa.

Proof. Analogous to the proof of Lemma 5.3.13. □

Lemma B.1.18. ind-ik-cpa $\not\longleftrightarrow$ ind-ik-r-cpa.

Proof. Analogous to the proofs of both Lemma 5.3.10 and Lemma 5.3.14. □

Lemma B.1.19. ind-ik-r-cpa $\xrightarrow{3}$ ulk-cpa.

Proof. Implied by Lemma B.1.14 and Lemma 5.3.11 (as well as by Lemma B.1.14 and Lemma 5.3.15, but requires ind-ik-r-cpa *four* times). □

Lemma B.1.20. ulk-cpa $\not\longrightarrow$ ind-ik-r-cpa.

Proof. By Lemma B.1.14, ind-ik-r-cpa $\xrightarrow{2}$ ik-r-cpa, but by Lemma 5.3.16, ulk-cpa $\not\longrightarrow$ ik-r-cpa, hence ulk-cpa $\longrightarrow$ ind-ik-cpa would lead to a contradiction. □

Bibliography

[ABN10] Michel Abdalla, Mihir Bellare, and Gregory Neven. Robust encryption. In Daniele Micciancio, editor, *TCC 2010*, volume 5978 of *LNCS*, pages 480–497. Springer, Heidelberg, February 2010.

[AGM18] Gorjan Alagic, Tommaso Gagliardoni, and Christian Majenz. Unforgeable quantum encryption. In Jesper Buus Nielsen and Vincent Rijmen, editors, *EUROCRYPT 2018, Part III*, volume 10822 of *LNCS*, pages 489–519. Springer, Heidelberg, April / May 2018.

[AHM+14] Joël Alwen, Martin Hirt, Ueli Maurer, Arpita Patra, and Pavel Raykov. Key-indistinguishable message authentication codes. In Michel Abdalla and Roberto De Prisco, editors, *SCN 14*, volume 8642 of *LNCS*, pages 476–493. Springer, Heidelberg, September 2014.

[AHM+15] Joël Alwen, Martin Hirt, Ueli Maurer, Arpita Patra, and Pavel Raykov. Anonymous authentication with shared secrets. In Diego F. Aranha and Alfred Menezes, editors, *LATINCRYPT 2014*, volume 8895 of *LNCS*, pages 219–236. Springer, Heidelberg, September 2015.

[AR02] Martín Abadi and Phillip Rogaway. Reconciling two views of cryptography (the computational soundness of formal encryption). *Journal of Cryptology*, 15(2):103–127, March 2002.

[BBDP01] Mihir Bellare, Alexandra Boldyreva, Anand Desai, and David Pointcheval. Key-privacy in public-key encryption. In Colin Boyd, editor, *ASIACRYPT 2001*, volume 2248 of *LNCS*, pages 566–582. Springer, Heidelberg, December 2001.

[BBM00] Mihir Bellare, Alexandra Boldyreva, and Silvio Micali. Public-key encryption in a multi-user setting: Security proofs and improvements. In Bart Preneel, editor, *EUROCRYPT 2000*, volume 1807 of *LNCS*, pages 259–274. Springer, Heidelberg, May 2000.

[BBM18] Christian Badertscher, Fabio Banfi, and Ueli Maurer. A constructive perspective on signcryption security. In Dario Catalano and Roberto De Prisco, editors, *SCN 18*, volume 11035 of *LNCS*, pages 102–120. Springer, Heidelberg, September 2018.

[BC05] Michael Backes and Christian Cachin. Public-key steganography with active attacks. In Joe Kilian, editor, *TCC 2005*, volume 3378 of *LNCS*, pages 210–226. Springer, Heidelberg, February 2005.

[BD09] Mihir Bellare and Shanshan Duan. Partial signatures and their applications. Cryptology ePrint Archive, Report 2009/336, 2009. `https://eprint.iacr.org/2009/336`.

[BDF+18] Chris Brzuska, Antoine Delignat-Lavaud, Cédric Fournet, Konrad Kohbrok, and Markulf Kohlweiss. State separation for code-based game-playing proofs. In Thomas Peyrin and Steven Galbraith, editors, *ASIACRYPT 2018, Part III*, volume 11274 of *LNCS*, pages 222–249. Springer, Heidelberg, December 2018.

[BDJR97] Mihir Bellare, Anand Desai, Eric Jokipii, and Phillip Rogaway. A concrete security treatment of symmetric encryption. In *38th FOCS*, pages 394–403. IEEE Computer Society Press, October 1997.

[Bel22] Mihir Bellare. Personal communication, July 2022.

[BKM06] Adam Bender, Jonathan Katz, and Ruggero Morselli. Ring signatures: Stronger definitions, and constructions without random oracles. In Shai Halevi and Tal Rabin, editors, *TCC 2006*, volume 3876 of *LNCS*, pages 60–79. Springer, Heidelberg, March 2006.

[BM20] Fabio Banfi and Ueli Maurer. Anonymous symmetric-key communication. In Clemente Galdi and Vladimir Kolesnikov, editors, *SCN 20*, volume 12238 of *LNCS*, pages 471–491. Springer, Heidelberg, September 2020.

[BM22] Fabio Banfi and Ueli Maurer. Anonymous authenticated communication. In Clemente Galdi and Stanislaw Jarecki, editors, *SCN 2022*, volume 13409 of *LNCS*, pages 289–312. Springer, Cham, 2022.

[BMPZ19] Fabio Banfi, Ueli Maurer, Christopher Portmann, and Jiamin Zhu. Composable and finite computational security of quantum message transmission. In Dennis Hofheinz and Alon Rosen, editors, *TCC 2019, Part I*, volume 11891 of *LNCS*, pages 282–311. Springer, Heidelberg, December 2019.

[BMR23] Fabio Banfi, Ueli Maurer, and Silvia Ritsch. On the security of universal re-encryption. Cryptology ePrint Archive, Paper 2023/1165, 2023. `https://eprint.iacr.org/2023/1165`.

[BN00] Mihir Bellare and Chanathip Namprempre. Authenticated encryption: Relations among notions and analysis of the generic composition paradigm. In Tatsuaki Okamoto, editor, *ASIACRYPT 2000*, volume 1976 of *LNCS*, pages 531–545. Springer, Heidelberg, December 2000.

[BPW07] Michael Backes, Birgit Pfitzmann, and Michael Waidner. The reactive simulatability (rsim) framework for asynchronous systems. *Information and Computation*, 205(12):1685–1720, 2007.

[BR06] Mihir Bellare and Phillip Rogaway. The security of triple encryption and a framework for code-based game-playing proofs. In Serge Vaudenay, editor, *EUROCRYPT 2006*,

volume 4004 of *LNCS*, pages 409–426. Springer, Heidelberg, May / June 2006.

[BT16] Mihir Bellare and Björn Tackmann. The multi-user security of authenticated encryption: AES-GCM in TLS 1.3. In Matthew Robshaw and Jonathan Katz, editors, *CRYPTO 2016, Part I*, volume 9814 of *LNCS*, pages 247–276. Springer, Heidelberg, August 2016.

[Can01] Ran Canetti. Universally composable security: A new paradigm for cryptographic protocols. In *42nd FOCS*, pages 136–145. IEEE Computer Society Press, October 2001.

[CR19] John Chan and Phillip Rogaway. Anonymous AE. In Steven D. Galbraith and Shiho Moriai, editors, *ASIACRYPT 2019, Part II*, volume 11922 of *LNCS*, pages 183–208. Springer, Heidelberg, December 2019.

[Cv91] David Chaum and Eugène van Heyst. Group signatures. In Donald W. Davies, editor, *EUROCRYPT'91*, volume 547 of *LNCS*, pages 257–265. Springer, Heidelberg, April 1991.

[Des00] Anand Desai. The security of all-or-nothing encryption: Protecting against exhaustive key search. In Mihir Bellare, editor, *CRYPTO 2000*, volume 1880 of *LNCS*, pages 359–375. Springer, Heidelberg, August 2000.

[Fis99] Marc Fischlin. Pseudorandom function tribe ensembles based on one-way permutations: Improvements and applications. In Jacques Stern, editor, *EUROCRYPT'99*, volume 1592 of *LNCS*, pages 432–445. Springer, Heidelberg, May 1999.

[Fis07] Marc Fischlin. Anonymous signatures made easy. In Tatsuaki Okamoto and Xiaoyun Wang, editors, *PKC 2007*, volume 4450 of *LNCS*, pages 31–42. Springer, Heidelberg, April 2007.

[FOR17] Pooya Farshim, Claudio Orlandi, and Răzvan Roşie. Security of symmetric primitives under incorrect usage of keys. *IACR Trans. Symm. Cryptol.*, 2017(1):449–473, 2017.

[GJJS04] Philippe Golle, Markus Jakobsson, Ari Juels, and Paul F. Syverson. Universal re-encryption for mixnets. In Tatsuaki Okamoto, editor, *CT-RSA 2004*, volume 2964 of *LNCS*, pages 163–178. Springer, Heidelberg, February 2004.

[GM84] Shafi Goldwasser and Silvio Micali. Probabilistic encryption. *Journal of Computer and System Sciences*, 28(2):270–299, 1984.

[Gro04] Jens Groth. Rerandomizable and replayable adaptive chosen ciphertext attack secure cryptosystems. In Moni Naor, editor, *TCC 2004*, volume 2951 of *LNCS*, pages 152–170. Springer, Heidelberg, February 2004.

[HLv02] Nicholas J. Hopper, John Langford, and Luis von Ahn. Provably secure steganography. In Moti Yung, editor, *CRYPTO 2002*, volume 2442 of *LNCS*, pages 77–92. Springer, Heidelberg, August 2002.

[HTT18] Viet Tung Hoang, Stefano Tessaro, and Aishwarya Thiruvengadam. The multi-user security of GCM, revisited: Tight bounds for nonce randomization. In David Lie, Mohammad Mannan, Michael Backes, and XiaoFeng Wang, editors, *ACM CCS 2018*, pages 1429–1440. ACM Press, October 2018.

[JBB18] Daniel Jost, Christian Badertscher, and Fabio Banfi. A note on the equivalence of IND-CCA & INT-PTXT and IND-CCA & INT-CTXT. Cryptology ePrint Archive, Report 2018/135, 2018. `https://eprint.iacr.org/2018/135`.

[JM20] Daniel Jost and Ueli Maurer. Overcoming impossibility results in composable security using interval-wise guarantees. In Daniele Micciancio and Thomas Ristenpart, editors, *CRYPTO 2020, Part I*, volume 12170 of *LNCS*, pages 33–62. Springer, Heidelberg, August 2020.

[JSI96] Markus Jakobsson, Kazue Sako, and Russell Impagliazzo. Designated verifier proofs and their applications. In Ueli M. Maurer, editor, *EUROCRYPT'96*, volume 1070 of *LNCS*, pages 143–154. Springer, Heidelberg, May 1996.

[KL20] Jonathan Katz and Yehuda Lindell. *Introduction to modern cryptography*. CRC press, 2020.

[KMO+13] Markulf Kohlweiss, Ueli Maurer, Cristina Onete, Björn Tackmann, and Daniele Venturi. Anonymity-preserving public-key encryption: A constructive approach. In Emiliano De Cristofaro and Matthew K. Wright, editors, *PETS 2013*, volume 7981 of *LNCS*, pages 19–39. Springer, Heidelberg, July 2013.

[Kra01] Hugo Krawczyk. The order of encryption and authentication for protecting communications (or: How secure is SSL?). In Joe Kilian, editor, *CRYPTO 2001*, volume 2139 of *LNCS*, pages 310–331. Springer, Heidelberg, August 2001.

[KTR13] Ralf Küsters, Max Tuengerthal, and Daniel Rausch. The IITM model: a simple and expressive model for universal composability. Cryptology ePrint Archive, Report 2013/025, 2013. `https://eprint.iacr.org/2013/025`.

[LV05] Fabien Laguillaumie and Damien Vergnaud. Designated verifier signatures: Anonymity and efficient construction from any bilinear map. In Carlo Blundo and Stelvio Cimato, editors, *SCN 04*, volume 3352 of *LNCS*, pages 105–119. Springer, Heidelberg, September 2005.

[Mau02] Ueli M. Maurer. Indistinguishability of random systems. In Lars R. Knudsen, editor, *EUROCRYPT 2002*, volume 2332 of *LNCS*, pages 110–132. Springer, Heidelberg, April / May 2002.

[Mau12] Ueli Maurer. Constructive cryptography – a new paradigm for security definitions and proofs. In Sebastian Mödersheim and Catuscia Palamidessi, editors, *Theory of Security and Applications – TOSCA 2011*, pages 33–56, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg.

[Möl04] Bodo Möller. A public-key encryption scheme with pseudorandom ciphertexts. In Pierangela Samarati, Peter Y. A. Ryan, Dieter Gollmann, and Refik Molva, editors, *ESORICS 2004*, volume 3193 of *LNCS*, pages 335–351. Springer, Heidelberg, September 2004.

[MPR07] Ueli M. Maurer, Krzysztof Pietrzak, and Renato Renner. Indistinguishability amplification. In Alfred Menezes, editor, *CRYPTO 2007*, volume 4622 of *LNCS*, pages 130–149. Springer, Heidelberg, August 2007.

[MPR21] Ueli Maurer, Christopher Portmann, and Guilherme Rito. Giving an adversary guarantees (or: How to model designated verifier signatures in a composable framework). In Mehdi Tibouchi and Huaxiong Wang, editors, *ASIACRYPT 2021, Part III*, volume 13092 of *LNCS*, pages 189–219. Springer, Heidelberg, December 2021.

[MR11] Ueli Maurer and Renato Renner. Abstract cryptography. In Bernard Chazelle, editor, *ICS 2011*, pages 1–21. Tsinghua University Press, January 2011.

[MR16] Ueli Maurer and Renato Renner. From indifferentiability to constructive cryptography (and back). In Martin Hirt and Adam D. Smith, editors, *TCC 2016-B, Part I*, volume 9985 of *LNCS*, pages 3–24. Springer, Heidelberg, October / November 2016.

[MRT12] Ueli Maurer, Andreas Rüedlinger, and Björn Tackmann. Confidentiality and integrity: A constructive perspective. In Ronald Cramer, editor, *TCC 2012*, volume 7194 of *LNCS*, pages 209–229. Springer, Heidelberg, March 2012.

[NY90] Moni Naor and Moti Yung. Public-key cryptosystems provably secure against chosen ciphertext attacks. In *22nd ACM STOC*, pages 427–437. ACM Press, May 1990.

[PR07] Manoj Prabhakaran and Mike Rosulek. Rerandomizable RCCA encryption. In Alfred Menezes, editor, *CRYPTO 2007*, volume 4622 of *LNCS*, pages 517–534. Springer, Heidelberg, August 2007.

[PW01] Birgit Pfitzmann and Michael Waidner. A model for asynchronous reactive systems and its application to secure message transmission. In *2001 IEEE Symposium on Security and Privacy*, pages 184–200. IEEE Computer Society Press, May 2001.

[RBBK01] Phillip Rogaway, Mihir Bellare, John Black, and Ted Krovetz. OCB: A block-cipher mode of operation for efficient authenticated encryption. In Michael K. Reiter and Pierangela Samarati, editors, *ACM CCS 2001*, pages 196–205. ACM Press, November 2001.

[Rog04] Phillip Rogaway. Nonce-based symmetric encryption. In Bimal K. Roy and Willi Meier, editors, *FSE 2004*, volume 3017 of *LNCS*, pages 348–359. Springer, Heidelberg, February 2004.

[Rog11] Phillip Rogaway. Evaluation of some blockcipher modes of operation. Cryptography Research and Evaluation Committees (CRYPTREC) for the Government of Japan, 2011. `https://web.cs.ucdavis.edu/~rogaway/papers/modes.pdf`.

[Rog13] Phillip Rogaway. The evolution of authenticated encryption. Workshop on Real-World Cryptography, 2013. `https://crypto.stanford.edu/RealWorldCrypto/slides/phil.pdf`.

[Ros21] Mike Rosulek. The joy of cryptography, 2021. `https://joyofcryptography.com`.

[RS92] Charles Rackoff and Daniel R. Simon. Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack. In Joan Feigenbaum, editor, *CRYPTO'91*, volume 576 of *LNCS*, pages 433–444. Springer, Heidelberg, August 1992.

[RS06] Phillip Rogaway and Thomas Shrimpton. A provable-security treatment of the key-wrap problem. In Serge Vaudenay, editor, *EUROCRYPT 2006*, volume 4004 of *LNCS*, pages 373–390. Springer, Heidelberg, May / June 2006.

[RST01] Ronald L. Rivest, Adi Shamir, and Yael Tauman. How to leak a secret. In Colin Boyd, editor, *ASIACRYPT 2001*, volume 2248 of *LNCS*, pages 552–565. Springer, Heidelberg, December 2001.

[SBWP03] Ron Steinfeld, Laurence Bull, Huaxiong Wang, and Josef Pieprzyk. Universal designated-verifier signatures. In Chi-Sung Laih, editor, *ASIACRYPT 2003*, volume 2894 of *LNCS*, pages 523–542. Springer, Heidelberg, November / December 2003.

[Sho01] Victor Shoup. OAEP reconsidered. In Joe Kilian, editor, *CRYPTO 2001*, volume 2139 of *LNCS*, pages 239–259. Springer, Heidelberg, August 2001.

[Shr04] Tom Shrimpton. A characterization of authenticated-encryption as a form of chosen-ciphertext security. Cryptology ePrint Archive, Report 2004/272, 2004. `https://eprint.iacr.org/2004/272`.

[SWP04] Ron Steinfeld, Huaxiong Wang, and Josef Pieprzyk. Efficient extension of standard Schnorr/RSA signatures into universal designated-verifier signatures. In Feng Bao, Robert Deng, and Jianying Zhou, editors, *PKC 2004*, volume 2947 of *LNCS*, pages 86–100. Springer, Heidelberg, March 2004.

[SY09] Vishal Saraswat and Aaram Yun. Anonymous signatures revisited. In Josef Pieprzyk and Fangguo Zhang, editors, *ProvSec 2009*, volume 5848 of *LNCS*, pages 140–153. Springer, Heidelberg, November 2009.

[vH04] Luis von Ahn and Nicholas J. Hopper. Public-key steganography. In Christian Cachin and Jan Camenisch, editors, *EUROCRYPT 2004*, volume 3027 of *LNCS*, pages 323–341. Springer, Heidelberg, May 2004.

[WCY+21] Yi Wang, Rongmao Chen, Guomin Yang, Xinyi Huang, Baosheng Wang, and Moti Yung. Receiver-anonymity in rerandomizable RCCA-secure cryptosystems resolved. In Tal Malkin and Chris Peikert, editors, *CRYPTO 2021, Part IV*, volume 12828 of *LNCS*, pages 270–300, Virtual Event, August 2021. Springer, Heidelberg.

[Wik04] Douglas Wikström. A universally composable mix-net. In Moni Naor, editor, *TCC 2004*, volume 2951 of *LNCS*, pages 317–335. Springer, Heidelberg, February 2004.

[YO07] Kazuki Yoneyama and Kazuo Ohta. Ring signatures: Universally composable definitions and constructions. *IPSJ Digital Courier*, 3:571–584, 2007.

[YWDW06] Guomin Yang, Duncan S. Wong, Xiaotie Deng, and Huaxiong Wang. Anonymous signature schemes. In Moti Yung, Yevgeniy Dodis, Aggelos Kiayias, and Tal Malkin, editors, *PKC 2006*, volume 3958 of *LNCS*, pages 347–363. Springer, Heidelberg, April 2006.

[YY18] Adam L. Young and Moti Yung. Semantically secure anonymity: Foundations of re-encryption. In Dario Catalano and Roberto De Prisco, editors, *SCN 18*, volume 11035 of *LNCS*, pages 255–273. Springer, Heidelberg, September 2018.

[ZI09] Rui Zhang and Hideki Imai. Strong anonymous signatures. In Moti Yung, Peng Liu, and Dongdai Lin, editors, *Inscrypt 2008*, volume 5487 of *LNCS*, pages 60–71, Heidelberg, 2009. Springer.

Curriculum Vitae

Fabio Matteo Banfi
Citizen of Switzerland.
Born on June 21, 1990, in Zurich, Switzerland.

University Studies

2012–2015	*B.Sc. ETH in Computer Science,* ETH Zurich, Switzerland.
2015–2017	*M.Sc. ETH in Computer Science,* ETH Zurich, Switzerland.
2017–2023	*Dr. sc. ETH Zurich in Computer Science,* ETH Zurich, Switzerland.