On the Security of Universal Re-Encryption

Fabio Banfi[1], Ueli Maurer[1], and Silvia Ritsch[2]

[1] Department of Computer Science,
ETH Zurich,
Switzerland
{fabio.banfi,maurer}@inf.ethz.ch
[2] TU Eindhoven,
The Netherlands
s.ritsch@tue.nl

Abstract. A universal re-encryption (URE) scheme is a public-key encryption scheme enhanced with an algorithm that on input a ciphertext, outputs another ciphertext which is still a valid encryption of the underlying plaintext. Crucially, such a re-encryption algorithm does not need any key as input, but the ciphertext is guaranteed to be valid under the original key-pair. Therefore, URE schemes lend themselves naturally as building blocks of mixnets: A sender transmits the encryption of a message under the receivers public-key to a mixer, which re-encrypts it, and the receiver later retrieves the re-encrypted ciphertext, which will decrypt successfully to the original message.

Young and Yung (SCN 2018) argued that the original definition of URE by Golle et al. (CT-RSA 2004) was flawed, because it did not consider anonymity of encryption. This motivated them to claim that they finally put URE on solid grounds by presenting four formal security notions which they argued a URE should satisfy.

As our first contribution, we introduce a framework that allows to compactly define and relate security notions as *substitutions of systems*. Using such framework, as our second contribution we show that Young and Yung's four notions are not minimal, and therefore do not properly capture the essence of a secure URE scheme. We provide three definitions that imply (and are implied by) theirs. Using the constructive cryptography framework, our third contribution is to capture the essence of URE from an application point of view by providing a composable security notion that expresses the ideal use of URE in a mixnet. Finally, we show that the composable notion is implied by our three minimal notions.

Keywords: universal re-encryption · unlinkability · anonymity · composable security

Table of Contents

1 Introduction

1.1 Background and 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.

1.2 Contribution

The main goal of this paper 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.

A New Framework for Algebraic Proofs of Security. Most security proofs are based on the idea of transforming an adversary for a problem into another adversary for a different problem via a reduction. Usually security notions and hardness assumptions are phrased as distinction 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 distinction 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.

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+ulk-cpa, and ik-cpa+ulk-cpa.

Capturing the Essence of URE: Composable Semantics. Finally, we introduce two new composable notion for URE, also using substitutions, in order to capture the essence of URE from an *application point-of-view*. The first 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. The second notion captures the case of a dishonest mixer, and in this case we show that the stronger notion of ind-rcca is necessary. This means that the original ElGamal-based scheme put forth by Golle et al. (and also proven by Young and Yung to satisfy their notions) can't possibly be secure according to our stronger composable notion, if one wants meaningful security guarantees in the case of a dishonest mixer.

1.3 Related Work

The idea of building reductions by applying a number of algebraic operations was previously explored by Brzuska et al [BDF+18]. The authors define security notions as *packages* representing collections of oracles, and use their new framework to prove the KEM-DEM security of Cramer-Shoup's hybrid encryption scheme, as well as to prove the security of the composition of forward-secure key exchange protocols with symmetric-key protocols. 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.

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.

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 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 $\star$, $y \overset{\star}{\leftarrow} x$ 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 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 Systems

In this paper 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 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* $i \geq 1$*.*

In this paper we will describe systems informally or with intuitive pseudocode, rather than by the conditional probabilities characterizing them. For fixed sets $\mathcal{X}$ and $\mathcal{Y}$, we define some special stateless systems as follows.

Definition 2 (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.*
- $\perp$ *is an* $(\mathcal{X}, \{\perp\})$*-system that on input any* x *always outputs* $\perp$*.*

– 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 useful ways in which systems can be combined into new systems, as illustrated in Figure 1.

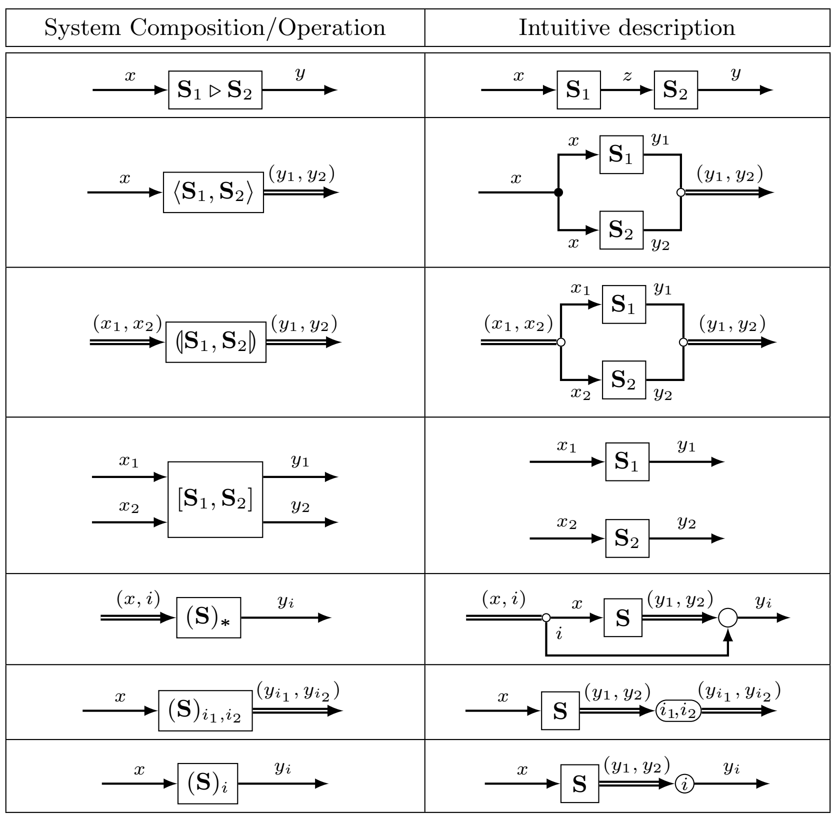


Fig. 1. Schematic representation of the systems from Definition 2 for $\ell = 2$.

Definition 3 (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* $(y_1, \ldots, y_\ell)$*.*
– $[\mathbf{S}_1, \ldots, \mathbf{S}_\ell]$ *is 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* $\mathbf{S}_i$ *and 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, then we use the notation* $[\![\mathbf{S}_1, \ldots, \mathbf{S}_\ell]\!]$ *to denote their* correlated *parallel composition, and make the parameter explicit.*
– $(\mathbf{S})_*$ *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* $(y_{j_1}, \ldots, y_{j_t})$*.*

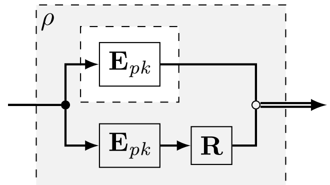
Finally, we assume that grouping tuples into tuples yields tuples, that is, for systems $\mathbf{R}, \mathbf{S}, \mathbf{T}$ *and* $(\,) \in \{\langle\,\rangle, (\!|\,|\!), [\,], [\![\,]\!]\}$*,* $(\mathbf{R}, \mathbf{S}, \mathbf{T}) \equiv (\mathbf{R}, (\mathbf{S}, \mathbf{T})) \equiv ((\mathbf{R},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

Let now us give some more intuition on Definition 3 via some concrete example. Consider systems $\mathbf{S}_{(\cdot)}, \mathbf{T}_{(\cdot)}, \mathbf{U}_{(\cdot)}, \mathbf{V}_{(\cdot)}$, each of which is parameterized by some value. Then, let's for example construct the following system, for some concrete values a, b, c:

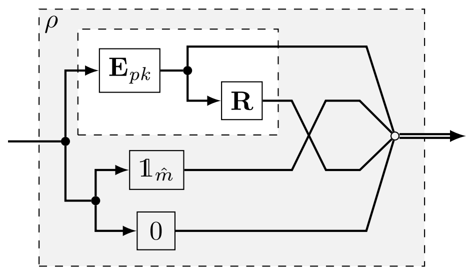
$$[\![\langle \mathbf{S}_a, \mathbf{T}_b \rangle \triangleright (\!| \mathbf{U}_a, \mathbf{V}_c |\!)_{2,1}, a, b]\!].$$

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 $\langle \mathbf{S}_a, \mathbf{T}_b \rangle$, which means that x will be input in parallel to both $\mathbf{S}_a$ and $\mathbf{T}_b$, 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 3, 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, in our proofs we will explicitly show how to factorize systems by exhibiting a function ρ (the reduction) that given a system of some special forms, maps it to another system. For example, looking ahead, in the proof of Lemma 1, for any system $\mathbf{S}$ and parameter x we define $\rho([\![\mathbf{S}, x]\!]) \doteq [\![\langle \mathbf{E}_x, \mathbf{S} \triangleright \mathbf{R} \rangle, x]\!]$, 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 $[\![\mathbf{E}_{pk}, pk]\!]$ can be factored out of $[\![\langle \mathbf{E}_{pk}, \mathbf{E}_{pk} \triangleright \mathbf{R} \rangle, pk]\!]$, that is, $\rho([\![\mathbf{E}_{pk}, pk]\!]) = [\![\langle \mathbf{E}_{pk}, \mathbf{E}_{pk} \triangleright \mathbf{R} \rangle, pk]\!]$. Visually, this can be seen as follows (ignoring pk):



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



We next introduce the abstraction of (in)distinguishability of systems, that is crucial for defining security notions and proving relations among them.

Definition 4 (Substitution). *A* substitution *is a set* $\{\mathbf{S}, \mathbf{T}\}$*, where* $\mathbf{S}$ *and* $\mathbf{T}$ *are two compatible systems, denoted* $\mathbf{S} \simeq \mathbf{T}$ *(or equivalently,* $\mathbf{T} \simeq \mathbf{S}$*).*

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* $\mathbf{T}$ $(\mathbf{S} \simeq \mathbf{T})$*, then we can also substitute system* $\mathbf{S}'$ *by system* $\mathbf{T}'$ $(\mathbf{S}' \simeq \mathbf{T}')$*"*, which we denote (and formalize below) as $\mathbf{S} \simeq \mathbf{T} \implies \mathbf{S}' \simeq \mathbf{T}'$. 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 factorization 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 $\mathbf{S}' \simeq \mathbf{T}' \iff \rho(\mathbf{S}) \simeq \rho(\mathbf{T})$, and since $\mathbf{S} \simeq \mathbf{T} \implies \rho(\mathbf{S}) \simeq \rho(\mathbf{T})$ (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.

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 $\mathbf{X}_0 \simeq \mathbf{X}_1$, 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 with probability* p*"*, means that the behaviors of $\mathbf{X}_0$ and $\mathbf{X}_1$ differs with probability p, denoted $\mathbf{X}_0 \simeq_p \mathbf{X}_1$. 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 $\mathsf{X}_i :\Longleftrightarrow \mathbf{X}_{i,0} \simeq \mathbf{X}_{i,1}$, for $i \in [\ell]$, and $\mathsf{Y} :\Longleftrightarrow \mathbf{Y}_0 \simeq \mathbf{Y}_1$. We say that $\mathsf{X}_1, \ldots, \mathsf{X}_\ell$ *imply* Y, denoted

$$\mathsf{X}_1 \ \wedge \ \cdots \ \wedge \ \mathsf{X}_\ell \implies \mathsf{Y},$$

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

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

We overload notation by also defining $\mathsf{X}_1 \ \wedge \ \cdots \ \wedge \ \mathsf{X}_{\ell_1} \implies \mathsf{Y}_1 \ \wedge \ \cdots \ \wedge \ \mathsf{Y}_{\ell_2}$, for some $\ell_1, \ell_2 \in \mathbb{N}$, as $\mathsf{X}_1 \ \wedge \ \cdots \ \wedge \ \mathsf{X}_{\ell_1} \implies \mathsf{Y}_i$ *for any* $i \in [\ell_2]$. We also use the natural shorthand notation $\mathsf{X}_1 \ \wedge \ \cdots \ \wedge \ \mathsf{X}_{\ell_1} \iff \mathsf{Y}_1 \ \wedge \ \cdots \ \wedge \ \mathsf{Y}_{\ell_2}$ to mean $\mathsf{X}_1 \wedge \cdots \wedge \mathsf{X}_{\ell_1} \implies \mathsf{Y}_1 \wedge \cdots \wedge \mathsf{Y}_{\ell_2}$ *and* $\mathsf{Y}_1 \wedge \cdots \wedge \mathsf{Y}_{\ell_2} \implies \mathsf{X}_1 \wedge \cdots \wedge \mathsf{X}_{\ell_1}$.

Finally, let us explain how we can *separate* security notions defined as substitutions. Let X and Y be some security notions defined as substitutions $\mathsf{X} :\Longleftrightarrow \mathbf{X}_0 \simeq \mathbf{X}_1$ and $\mathsf{Y} :\Longleftrightarrow \mathbf{Y}_0 \simeq \mathbf{Y}_1$. 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 $\mathbf{X}_0^{\Pi'} \simeq \mathbf{X}_1^{\Pi'}$, but $\mathbf{Y}_0^{\Pi'} \not\simeq \mathbf{Y}_1^{\Pi'}$, where by $\not\simeq$ we mean that the systems $\mathbf{Y}_0^{\Pi'}$ and $\mathbf{Y}_1^{\Pi'}$ are *trivially distinguishable*, and thus not substitutable (for example, $\mathbb{1}_x \not\simeq B$ and $0 \not\simeq 1$). 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 $\mathbf{Y}_0^{\Pi'} \not\simeq \mathbf{Y}_1^{\Pi'}$. We use the natural shorthand notation $\mathsf{X} \not\Longleftrightarrow \mathsf{Y}$ to mean $\mathsf{X} \not\Longrightarrow \mathsf{Y}$ *and* $\mathsf{Y} \not\Longrightarrow \mathsf{X}$.

Relating our Abstract Framework to Concrete Security. For two systems $\mathbf{S}$ and $\mathbf{T}$, we mentioned above that if $\mathbf{S} \simeq \mathbf{T}$ is a valid substitution, then so is $\rho(\mathbf{S}) \simeq \rho(\mathbf{T})$. 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 $\mathbf{S}_\kappa \simeq \mathbf{T}_\kappa$ to mean

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

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

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

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) factorization 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 Universal Re-Encryption

Definition 5. *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 paper 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 6. *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 $\mathtt{Enc}_{pk}(m)$.*
- $\mathbf{E}^{\$}_{pk} \doteq \mathbf{\$} \triangleright \mathbf{E}_{pk}$ *is an $(\mathcal{M}, \mathcal{C})$-system that on input m, samples $\tilde{m} \xleftarrow{\$} \mathcal{M}$ and outputs $\mathtt{Enc}_{pk}(\tilde{m})$.*
- $\mathbf{R}$ *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 (n, m, t, j), outputs m if $i = j$ and $\bot$ otherwise.*
- $\boldsymbol{pk}_{pk_1,\ldots,pk_n}$ *is an $([n], \mathcal{PK})$-system that on input i, outputs pk_i.*

We will use the systems from Definition 6 to build more complex systems through the system composition operations from Definition 3.

3 Game-Based Semantics of Universal Re-Encryption

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 3.3, and show that the resulting notions are equivalent in Appendix A.1. We then generalize such combined notions to arbitrary sets of receivers in Section 3.4, and show that they are implied by the combined notions for two receivers in Appendix A.2.

3.1 Notions of Security

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 $(sk, pk) \leftarrow \texttt{Gen}$. The first system, on input a message-integer pair $(m, t) \in \mathcal{M} \times \mathbb{N}$, encrypts m into $c \leftarrow \texttt{Enc}_{pk}(m)$, re-encrypts t times c, that is, computes $\hat{c}_i \leftarrow \texttt{Rnc}(\hat{c}_{i-1})$ for $i \in [t]$ and where $\hat{c}_0 \doteq c$, and finally decrypts $\hat{c}_t$ into $m' := \texttt{Dec}_{sk}(\hat{c}_t)$ 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 7 (cor)**.**

$$\llbracket (\!| \mathbf{E}_{pk}, * |\!) \triangleright \mathbf{R}^{*} \triangleright \mathbf{D}_{sk}, pk \rrbracket \doteq \llbracket (\!| *, * |\!)_1, pk \rrbracket,$$

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

For *robustness* (rob), we consider the substitution of the following two systems, both of which initially sample two independent key-pairs $(sk_1, pk_1) \leftarrow \texttt{Gen}$ and $(sk_2, pk_2) \leftarrow \texttt{Gen}$. The first system, on input a message-integer pair $(m, t) \in \mathcal{M} \times \mathbb{N}$, encrypts m into $c \leftarrow \texttt{Enc}_{pk_1}(m)$ using the public key from the first key-pair, re-encrypts t times c, that is, computes $\hat{c}_i \leftarrow \texttt{Rnc}(\hat{c}_{i-1})$ for $i \in [t]$ and where $\hat{c}_0 \doteq c$, and finally decrypts $\hat{c}_t$ into $m' := \texttt{Dec}_{sk_2}(\hat{c}_t)$ 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 $\perp$. 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 $\perp$.

Definition 8 (rob)**.**

$$\llbracket (\!| \mathbf{E}_{pk_1}, * |\!) \triangleright \mathbf{R}^{*} \triangleright \mathbf{D}_{sk_2}, pk_1, pk_2 \rrbracket \doteq \llbracket (\!| \perp, * |\!)_1, pk_1, pk_2 \rrbracket,$$

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

For *confidentiality*, modeled as (real-or-random) indistinguishability of ciphertexts under a chosen-plaintext attack ($\mathsf{ind\text{-}cpa}$), we consider the substitution of the following two systems, both of which initially sample a key-pair $(sk, pk) \leftarrow \texttt{Gen}$. The first system, on input a message $m \in \mathcal{M}$, encrypts m into $c \leftarrow \texttt{Enc}_{pk}(m)$ and outputs c. The second system, on input a message $m \in \mathcal{M}$, samples $\tilde{m}$, encrypts $\tilde{m}$ into $\tilde{c} \leftarrow \texttt{Enc}_{pk}(\tilde{m})$ 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 9 ($\mathsf{ind\text{-}cpa}$)**.**

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

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

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 $(sk_1, pk_1) \leftarrow \texttt{Gen}$ and $(sk_2, pk_2) \leftarrow \texttt{Gen}$. The first system has two sub-systems: The first, on input a message $m \in \mathcal{M}$, encrypts m into $c \leftarrow \texttt{Enc}_{pk_1}(m)$ 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 $c \leftarrow \texttt{Enc}_{pk_2}(m)$ 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 $c \leftarrow \texttt{Enc}_{pk_1}(m)$ 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 10 (ik-cpa)**.**

$$[\![\mathbf{E}_{pk_1}, \mathbf{E}_{pk_2}, pk_1, pk_2]\!] \stackrel{\frown}{=} [\![\mathbf{E}_{pk_1}, \mathbf{E}_{pk_1}, pk_1, pk_2]\!],$$

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

For *unlinkability* (ulk-cpa), we consider the substitution of the following two systems, both of which initially sample a key-pair $(sk, pk) \leftarrow \texttt{Gen}$. The first system, on input a message $m \in \mathcal{M}$, first encrypts m into $c \leftarrow \texttt{Enc}_{pk}(m)$. Then it computes $\hat{c} \leftarrow \texttt{Rnc}(c)$ 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 $c \leftarrow \texttt{Enc}_{pk}(m)$. Then it encrypts again m into $c' \leftarrow \texttt{Enc}_{pk}(m)$ using *fresh and independent randomness*. Finally, it computes $\hat{c} \leftarrow \texttt{Rnc}(c')$ 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 11 (ulk-cpa)**.**

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

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

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 12 (sulk-cpa)**.**

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

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

Young 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 we show that our notions are essentially equivalent. Moreover, as we will see in Section 3.2, 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 $(sk, pk) \leftarrow \texttt{Gen}$. The first system, on input a message $m \in \mathcal{M}$, first encrypts m into $c \leftarrow \texttt{Enc}_{pk}(m)$. Then it computes $\hat{c} \leftarrow \texttt{Rnc}(c)$ and outputs $(c, \hat{c})$. The second system, on input a message $m \in \mathcal{M}$, first encrypts m into $c \leftarrow \texttt{Enc}_{pk}(m)$. Then it samples $\tilde{m}$, encrypts $\tilde{m}$ into $\tilde{c} \leftarrow \texttt{Enc}_{pk}(\tilde{m})$, computes $\hat{c} \leftarrow \texttt{Rnc}(\tilde{c})$, 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 13 (ind-r-cpa)**.**

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

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

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 $(sk_1, pk_1) \leftarrow \texttt{Gen}$ and $(sk_2, pk_2) \leftarrow \texttt{Gen}$. The first system has two sub-systems: The first, on input a message $m \in \mathcal{M}$, encrypts m into $c \leftarrow \texttt{Enc}_{pk_1}(m)$ using the public key from the *first* key-pair, computes $\hat{c} \leftarrow \texttt{Rnc}(c)$, and then outputs $(c, \hat{c})$, while the second, on input a message $m \in \mathcal{M}$, encrypts m into $c \leftarrow \texttt{Enc}_{pk_2}(m)$ using the public key from the *second* key-pair, computes $\hat{c} \leftarrow \texttt{Rnc}(c)$, 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 $c \leftarrow \texttt{Enc}_{pk_2}(m)$ using the public key from the *second* key-pair, encrypts again m into $c' \leftarrow \texttt{Enc}_{pk_1}(m)$ using the public key from the *first* key-pair, then computes $\hat{c} \leftarrow \texttt{Rnc}(c')$ 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 14 (ik-r-cpa)**.**

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

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

3.2 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 2 summarizes all relations (both implications and separations) that we prove. Furthermore, in Appendix B we show that our notions are essentially equivalent to the ones introduced in [YY18].

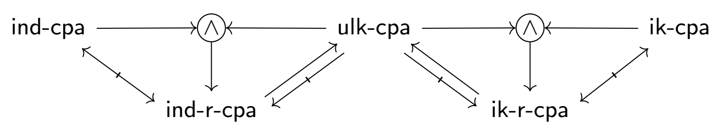


Fig. 2. Relations among encryption and re-encryption security notions.

Lemma 1. ind-cpa $\wedge$ ulk-cpa $\implies$ ind-r-cpa.

Proof. Let $(sk, pk) \leftarrow \texttt{Gen}$ and consider $\rho([\![\mathbf{S}, x]\!]) \doteq [\![\langle \mathbf{E}_x, \mathbf{S} \triangleright \mathbf{R} \rangle, x]\!]$. Then:

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

Lemma 2. ind-cpa $\not\Leftrightarrow$ ind-r-cpa.

Proof.

$\not\Rightarrow$: Let $\Pi \doteq (\texttt{Gen}, \texttt{Enc}, \texttt{Rnc}, \texttt{Dec})$. For any $(sk, pk) \in \operatorname{supp} \texttt{Gen}$, define $\Pi' \doteq (\texttt{Gen}', \texttt{Enc}', \texttt{Rnc}', \texttt{Dec}')$ as:

- $\texttt{Gen}' \doteq \texttt{Gen}$;
- $\texttt{Enc}'_{pk}(m) \doteq \texttt{Enc}_{pk}(m)$, for any $m \in \mathcal{M}$;
- $\texttt{Rnc}'(c) \doteq c$, for any $c \in \mathcal{C}$;
- $\texttt{Dec}'_{sk}(c) \doteq \texttt{Dec}_{sk}(c)$, for any $c \in \mathcal{C}$.

Let $(sk, pk) \leftarrow \texttt{Gen}$. If Π is correct, then Π' is clearly also correct, and if

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

then

$$[\![\mathbf{E}'_{pk}, pk]\!] \equiv [\![\mathbf{E}_{pk}, pk]\!] \simeq [\![\mathbf{E}^{\$}_{pk}, pk]\!] \equiv [\![\mathbf{E}'^{\$}_{pk}, pk]\!].$$

But clearly,

$$\begin{aligned}
[\![\mathbf{E}'_{pk} \triangleright \langle *, \mathbf{R}' \rangle, pk]\!] &\equiv [\![\mathbf{E}_{pk} \triangleright \langle *, * \rangle, pk]\!] \\
&\not\simeq [\![\langle \mathbf{E}_{pk}, \mathbf{E}^{\$}_{pk} \rangle, pk]\!] \\
&\equiv [\![\langle \mathbf{E}_{pk}, \mathbf{E}^{\$}_{pk} \triangleright \mathbf{R} \rangle, pk]\!].
\end{aligned}$$

$\not\Leftarrow$: Let $\Pi \doteq (\texttt{Gen}, \texttt{Enc}, \texttt{Rnc}, \texttt{Dec})$. For any $(sk, pk) \in \operatorname{supp} \texttt{Gen}$ and a fixed $\hat{m} \in \mathcal{M}$, define $\Pi' \doteq (\texttt{Gen}', \texttt{Enc}', \texttt{Rnc}', \texttt{Dec}')$ as:

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

Let $(sk, pk) \leftarrow \texttt{Gen}$. If Π is correct, then Π' is clearly also correct, and if

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

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

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

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

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

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

Lemma 3. ind-r-cpa $\implies$ ulk-cpa.

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

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

□

Lemma 4. ulk-cpa $\not\Longrightarrow$ ind-r-cpa.

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

– $\texttt{Gen}' \doteq \texttt{Gen}$;

- $\mathtt{Enc}'_{pk}(m) \doteq (\mathtt{Enc}_{pk}(m), \mathbb{1}\{m = \hat{m}\})$, 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 $(c,b) \in \mathcal{C} \times \{0,1\}$.

Let $(sk, pk) \leftarrow \mathtt{Gen}$. If Π is correct, then Π' is clearly also correct, and if

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

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

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

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

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

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

Lemma 5. ik-cpa $\wedge$ ulk-cpa $\implies$ ik-r-cpa.

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

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

Then:

$$\begin{aligned}
&[\![\mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R}\rangle, \mathbf{E}_{pk_2} \triangleright \langle *, \mathbf{R}\rangle, pk_1, pk_2]\!] \\
&\quad = \rho_1([\![\mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R}\rangle, pk_1]\!]) \\
&\quad \simeq \rho_1([\![\langle \mathbf{E}_{pk_1}, \mathbf{E}_{pk_1} \triangleright \mathbf{R}\rangle, pk_1]\!]) && \text{(ulk-cpa)} \\
&\quad = [\![\langle \mathbf{E}_{pk_1}, \mathbf{E}_{pk_1} \triangleright \mathbf{R}\rangle, \mathbf{E}_{pk_2} \triangleright \langle *, \mathbf{R}\rangle, pk_1, pk_2]\!] \\
&\quad = \rho_2([\![\mathbf{E}_{pk_2} \triangleright \langle *, \mathbf{R}\rangle, pk_2]\!]) \\
&\quad \simeq \rho_2([\![\langle \mathbf{E}_{pk_2}, \mathbf{E}_{pk_2} \triangleright \mathbf{R}\rangle, pk_2]\!]) && \text{(ulk-cpa)} \\
&\quad = [\![\langle \mathbf{E}_{pk_1}, \mathbf{E}_{pk_1} \triangleright \mathbf{R}\rangle, \langle \mathbf{E}_{pk_2}, \mathbf{E}_{pk_2} \triangleright \mathbf{R}\rangle, pk_1, pk_2]\!] \\
&\quad = \rho_3([\![\mathbf{E}_{pk_1}, \mathbf{E}_{pk_2}, pk_1, pk_2]\!]) \\
&\quad \simeq \rho_3([\![\mathbf{E}_{pk_1}, \mathbf{E}_{pk_1}, pk_1, pk_2]\!]) && \text{(ik-cpa)} \\
&\quad = [\![\langle \mathbf{E}_{pk_1}, \mathbf{E}_{pk_1} \triangleright \mathbf{R}\rangle, \langle \mathbf{E}_{pk_2}, \mathbf{E}_{pk_1} \triangleright \mathbf{R}\rangle, pk_1, pk_2]\!].
\end{aligned}$$ □

Lemma 6. $\mathsf{ik\text{-}cpa} \;\not\Leftrightarrow\; \mathsf{ik\text{-}r\text{-}cpa}$.

Proof.

$\not\Rightarrow$: Analogous to the case $\not\Rightarrow$ in the proof of Lemma 2.

$\not\Leftarrow$: 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 $(c, pk') \in \mathcal{C} \times (\mathcal{PK} \cup \{\bot\})$.

Let $(sk_1, pk_1) \leftarrow \mathtt{Gen}$ and $(sk_2, pk_2) \leftarrow \mathtt{Gen}$. If Π is correct, then Π' is clearly also correct, and if

$$\begin{gathered}
[\![\mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R}\rangle, \mathbf{E}_{pk_2} \triangleright \langle *, \mathbf{R}\rangle, pk_1, pk_2]\!] \\
\mathrel{\hat{=}} \\
[\![\mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R}\rangle, \langle \mathbf{E}_{pk_2}, \mathbf{E}_{pk_1} \triangleright \mathbf{R}\rangle, pk_1, pk_2]\!].
\end{gathered}$$

then with

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

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

But clearly,

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

□

Lemma 7. $\mathsf{ik\text{-}r\text{-}cpa} \implies \mathsf{ulk\text{-}cpa}$.

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

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

Then:

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

Lemma 8. $\textsf{ulk-cpa} \not\Longrightarrow \textsf{ik-r-cpa}$.

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

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

Let $(sk, pk) \leftarrow \texttt{Gen}$. If Π is correct, then Π' is clearly also correct, and if

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

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

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

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

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

Stronger Unlinkability. We next show that the strong unlinkability notion $\mathsf{sulk\text{-}cpa}$ we put forth is significantly stronger than the conventional unlinkability notion $\mathsf{ulk\text{-}cpa}$. In the proof of Lemma 10 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 $\mathtt{Enc}$, increased by 1 by $\mathtt{Rnc}$, and ignored by $\mathtt{Dec}$), the proof would still go through. This makes it evident that $\mathsf{ulk\text{-}cpa}$ is weaker than $\mathsf{sulk\text{-}cpa}$ in the sense that, in general, *a* $\mathsf{ulk\text{-}cpa}$*-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 9. $\mathsf{sulk\text{-}cpa} \implies \mathsf{ulk\text{-}cpa}$.

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

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

Lemma 10. $\mathsf{ulk\text{-}cpa} \;\not\Longrightarrow\; \mathsf{sulk\text{-}cpa}$.

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 $(c,b) \in \mathcal{C} \times \{0,1\}$.

Let $(sk, pk) \leftarrow \mathtt{Gen}$. If Π is correct, then Π' is clearly also correct, and if

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

then with $\rho([\![\mathbf{S}, x]\!]) \doteq [\![\mathbf{S} \triangleright (\!|\langle *, 0\rangle, \langle *, 1\rangle|\!), x]\!]$,

$$\begin{aligned}
[\![\mathbf{E}'_{pk} \triangleright \langle *, \mathbf{R}'\rangle, pk]\!] &\equiv [\![\mathbf{E}_{pk} \triangleright \langle *, \mathbf{R}\rangle \triangleright (\!|\langle *, 0\rangle, \langle *, 1\rangle|\!), pk]\!]\\
&= \rho([\![\mathbf{E}_{pk} \triangleright \langle *, \mathbf{R}\rangle, pk]\!])\\
&\simeq \rho([\![\langle \mathbf{E}_{pk}, \mathbf{E}_{pk} \triangleright \mathbf{R}\rangle, pk]\!])\\
&= [\![\langle \mathbf{E}_{pk}, \mathbf{E}_{pk} \triangleright \mathbf{R}\rangle \triangleright (\!|\langle *, 0\rangle, \langle *, 1\rangle|\!), pk]\!]\\
&\equiv [\![\langle \mathbf{E}'_{pk}, \mathbf{E}'_{pk} \triangleright \mathbf{R}'\rangle, pk]\!].
\end{aligned}$$

But clearly,

$$\begin{aligned}
[\![\mathbf{E}'_{pk} \triangleright \langle *, \mathbf{R}'\rangle, pk]\!] &\equiv [\![\mathbf{E}_{pk} \triangleright \langle *, \mathbf{R}\rangle \triangleright (\!|\langle *, 0\rangle, \langle *, 1\rangle|\!), pk]\!]\\
&\not\simeq [\![\langle \mathbf{E}_{pk}, \mathbf{E}_{pk}\rangle \triangleright (\!|\langle *, 0\rangle, \langle *, 0\rangle|\!), pk]\!]\\
&\equiv [\![\langle \mathbf{E}'_{pk}, \mathbf{E}'_{pk}\rangle, pk]\!]. && \square
\end{aligned}$$

3.3 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 3 summarizes all relations (both implications and separations) that we show in Appendix A.1. Furthermore, in Appendix C 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 Appendix D, we show that the original URE scheme based on ElGamal form [GJJS04] satisfies our strongest notion ind-ik-sulk-cpa.

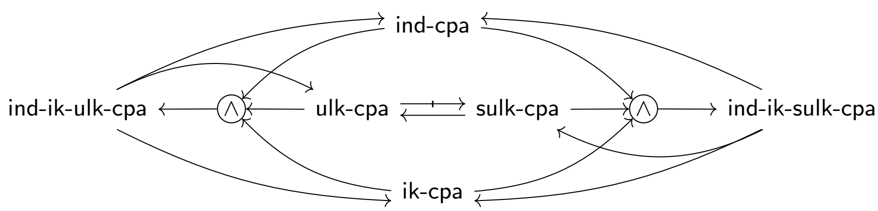


Fig. 3. Relations among combined notions.

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 $\perp$), by a pair of systems where $\mathbf{S}_i$, on input (m, t, j), always outputs m if $j = i$ and $\perp$ otherwise.

Definition 15 (cor-rob)**.**

$$\llbracket \llparenthesis \mathbf{E}_{pk_1}, *, * \rrparenthesis \triangleright \llparenthesis \mathbf{R}^*, * \rrparenthesis \triangleright \mathbf{D}_{sk_1, sk_2}, \llparenthesis \mathbf{E}_{pk_2}, *, * \rrparenthesis \triangleright \llparenthesis \mathbf{R}^*, * \rrparenthesis \triangleright \mathbf{D}_{sk_1, sk_2}, pk_1, pk_2 \rrbracket$$
$$\mathrel{\hat{=}}$$
$$\llbracket \llparenthesis *, \perp, * \rrparenthesis \triangleright \langle *, * \rangle_*, \llparenthesis *, \perp, * \rrparenthesis_{2,1,3} \triangleright \langle *, * \rangle_*, pk_1, pk_2 \rrbracket,$$

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

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 16 (ind-ik-ulk-cpa)**.**

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

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

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 17 (ind-ik-sulk-cpa)**.**

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

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

3.4 Generalizing the Notions: From 2 to Many Receivers

The combined notions introduced above are still a bit limited, because they only capture the case of two receivers. Nevertheless, as we explain now, it is straightforward to generalize such notions via a *generic hybrid argument.* In general, for two systems $\mathbf{S}_1$ and $\mathbf{T}_1$ we consider their generalized versions $\mathbf{S}_n$ and $\mathbf{T}_n$, for some $n \in \mathbb{N}$. Within our framework, an hybrid argument then corresponds to describing a generic reduction $\rho_i(\mathbf{X})$, for $i \in [n]$ and $\mathbf{X} \in \{\mathbf{S}_1, \mathbf{T}_1\}$, such that $\rho_1(\mathbf{S}_1) \equiv \mathbf{S}_n$, $\rho_n(\mathbf{T}_1) \equiv \mathbf{T}_n$, and for all $j \in [n-1]$, $\rho_j(\mathbf{T}_1) \equiv \rho_{j+1}(\mathbf{S}_1)$. Then clearly,

$$\mathbf{S}_n \equiv \rho_1(\mathbf{S}_1) \simeq \rho_1(\mathbf{T}_1) \equiv \rho_2(\mathbf{S}_1) \simeq \rho_2(\mathbf{T}_1) \equiv \cdots \equiv \rho_n(\mathbf{S}_1) \simeq \rho_n(\mathbf{T}_1) \equiv \mathbf{T}_n.$$

We now state the generic notions relative to a set $\mathcal{R}$ of receivers, and defer the proofs that they are implied by the two-users ones to Appendix A.2.

Definition 18 (n-cor-rob)**.**

$$[\![(\!|\mathbf{E}_{pk_1,\ldots,pk_n}, *, *|\!) \triangleright (\!|\mathbf{R}^*, *|\!) \triangleright \mathbf{D}_{sk_1,\ldots,sk_n}, \boldsymbol{pk}_{pk_1,\ldots,pk_n}]\!] \simeq [\![\mathbf{I}_n, \boldsymbol{pk}_{pk_1,\ldots,pk_n}]\!],$$

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

Definition 19 (n-ind-ik-ulk-cpa)**.**

$$[\![\mathbf{E}_{pk_1,\ldots,pk_n} \triangleright \langle *, \mathbf{R}\rangle, \boldsymbol{pk}_{pk_1,\ldots,pk_n}]\!] \simeq [\![(\!|*, *|\!)_1 \triangleright \langle \mathbf{E}^{\$}_{pk_1}, \mathbf{E}^{\$}_{pk_1} \triangleright \mathbf{R}\rangle, \boldsymbol{pk}_{pk_1,\ldots,pk_n}]\!],$$

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

Definition 20 (n-ind-ik-sulk-cpa)**.**

$$[\![\mathbf{E}_{pk_1,\ldots,pk_n} \triangleright \langle *, \mathbf{R}\rangle, \boldsymbol{pk}_{pk_1,\ldots,pk_n}]\!] \simeq [\![(\!|*, *|\!)_1 \triangleright \langle \mathbf{E}^{\$}_{pk_1}, \mathbf{E}^{\$}_{pk_1}\rangle, \boldsymbol{pk}_{pk_1,\ldots,pk_n}]\!],$$

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

4 Composable Semantics of Universal Re-Encryption

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], in which security statements naturally compose. 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], and three kinds of anonymous signature schemes [BM21]. 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, for example in [BM20] it is shown that anonymous and IND-CPA (probabilistic) symmetric-key encryption, from an authentic anonymous channel (plus a resource modeling a shared secret key) constructs a secure (that is, both authenticated *and confidential*) anonymous channel.

In this work, 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.

4.1 Constructive Cryptography

Originally introduced in [MR11] under the name of abstract cryptography and later instantiated as constructive cryptography (CC) in [Mau12], CC is a theory that allows to define security of cryptographic schemes and protocols as statements about constructions of ideal resources from assumed resources, which we model as systems from Section 2.2 enhanced with *interfaces*.

Definition 21 ($\mathcal{P}$-Resource). *For a party set $\mathcal{P}$, a $\mathcal{P}$-*resource R *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 R" *means inputting (P, x) to R, and to* "obtain x from interface P of R"*, means getting an output (P, x) from R.*

A $\mathcal{P}$-resource can be transformed into another $\mathcal{P}$-resource, exhibiting a different behavior, by applying a local converter at one of its interfaces.

Definition 22 (Local Converter). *A local converter α is a system with* in *and* out *interfaces (as per Definition 21), which can be applied to an interface $P \in \mathcal{P}$ of a $\mathcal{P}$-resource R, denoted $\alpha^P\mathsf{R}$, which is in turn a $\mathcal{P}$-resource. $\alpha^P\mathsf{R}$ behaves as R, except that:*

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

For another local converter β, $\alpha\beta$ is the local converter resulting by connecting interface in *of α to interface* out *of β.*

A protocol can then be defined as a collection of local protocols, describing the behavior of each party associated with an interface of a resource.

Definition 23 ($\mathcal{A}$-Converter). *For a set $\mathcal{A}$, an $\mathcal{A}$-converter $\boldsymbol{\alpha}$ is a collection of local converters α_A, for $A \in \mathcal{A}$. For $\mathcal{P}$-resource R with $\mathcal{A} \subseteq \mathcal{P}$, we define $\boldsymbol{\alpha}\,\mathsf{R}$ as the resource resulting by applying α_A to interface A or R for each $A \in \mathcal{A}$, that is, $(\alpha_A)^A((\alpha_B)^B(\cdots\mathsf{R}))$, for all $A, B, \ldots \in \mathcal{A}$. For another $\mathcal{A}$-converter $\boldsymbol{\beta}$,$\boldsymbol{\alpha\beta}$ is an $\mathcal{A}$-converter $\boldsymbol{\gamma}$ with $\gamma_A \doteq \alpha_A\beta_A$, for each $A \in \mathcal{A}$.*

The following two lemmas are directly implied by Definitions 21, 22 and 23.

Lemma 11 (Sequential Composition of $\mathcal{A}$-Converters). *For $\mathcal{P}$-resource R and $\mathcal{A}$-converters $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$, for $\mathcal{A} \subseteq \mathcal{P}$, $\boldsymbol{\alpha}\,(\boldsymbol{\beta}\,\mathsf{R}) \equiv \boldsymbol{\alpha\beta}\,\mathsf{R}$.* □

Lemma 12 (Commutativity of $\mathcal{A}$-Converters). *For $\mathcal{P}$-resource R, $\mathcal{A}$-converter $\boldsymbol{\alpha}$ and $\mathcal{B}$-converter $\boldsymbol{\beta}$, for $\mathcal{A}, \mathcal{B} \subseteq \mathcal{P}$ with $\mathcal{A} \cap \mathcal{B} = \varnothing$, $\boldsymbol{\alpha\beta}\,\mathsf{R} \equiv \boldsymbol{\beta\alpha}\,\mathsf{R}$.* □

Finally, we can define composable security of a protocol modeled by a converter $\boldsymbol{\pi}$ as follows.

Definition 24 (Construction). *For $\mathcal{P}$-resources R and S with honest parties set $\mathcal{H} \subseteq \mathcal{P}$ and $\mathcal{H}$-converter $\boldsymbol{\pi}$ (the protocol), we write $\mathsf{R} \xrightarrow{\boldsymbol{\pi}} \mathsf{S}$ if and only if there exists, for $\overline{\mathcal{H}} \doteq \mathcal{P} \setminus \mathcal{H}$, an $\overline{\mathcal{H}}$-converter* sim *(the simulator) such that $\boldsymbol{\pi}\,\mathsf{R} \simeq \mathsf{sim}\,\mathsf{S}$.*

The advantage of composable security notions, as opposed to simple substitutions from Section 3 capturing conventional game-based security notions, is that they naturally compose.

Theorem 1 (Composition). *For $\mathcal{P}$-resources R, S, and T with honest parties set $\mathcal{H} \subseteq \mathcal{P}$ and $\mathcal{H}$-converters $\boldsymbol{\pi}_1, \boldsymbol{\pi}_2$, if $\mathsf{R} \xrightarrow{\boldsymbol{\pi}_1} \mathsf{S}$ and $\mathsf{S} \xrightarrow{\boldsymbol{\pi}_2} \mathsf{T}$, then $\mathsf{R} \xrightarrow{\boldsymbol{\pi}_2\boldsymbol{\pi}_1} \mathsf{T}$.*

Proof. Let $\mathsf{sim}_1, \mathsf{sim}_2$ be $\overline{\mathcal{H}}$-converters such that $\boldsymbol{\pi}_1\,\mathsf{R} \simeq \mathsf{sim}_1\,\mathsf{S}$ and $\boldsymbol{\pi}_2\,\mathsf{S} \simeq \mathsf{sim}_2\,\mathsf{T}$. Then, with $\rho_1(\mathsf{X}) \doteq \boldsymbol{\pi}_2\,\mathsf{X}$ and $\rho_2(\mathsf{X}) \doteq \mathsf{sim}_1\,\mathsf{X}$, for any $\mathcal{P}$-resource X, by Lemma 11 we have $\boldsymbol{\pi}_2\boldsymbol{\pi}_1\,\mathsf{R} \simeq \boldsymbol{\pi}_2\mathsf{sim}_1\,\mathsf{S}$ and $\mathsf{sim}_1\boldsymbol{\pi}_2\,\mathsf{S} \simeq \mathsf{sim}_1\mathsf{sim}_2\,\mathsf{T}$. Therefore, by Lemma 12 we obtain $\boldsymbol{\pi}_2\boldsymbol{\pi}_1\,\mathsf{R} \simeq \mathsf{sim}_1\mathsf{sim}_2\,\mathsf{T}$. □

4.2 Assumed and Ideal Resources

In this work we only 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 $\mathcal{H} \doteq \mathcal{S} \cup \mathcal{R} \cup \{M\}$. 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}.

Definition 25 ($\mathsf{AUT}_{\mathcal{X}}^{\mathcal{A} \to \mathcal{B}}$, $\mathsf{1\text{-}AUT}_{\mathcal{X}}^{\mathcal{A} \to \mathcal{B}}$, $\mathsf{AUT}_{\mathcal{X}}^{\mathcal{A} \leftrightarrow \mathcal{B}}$). *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) at interfaces E, 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 $\mathsf{AUT}_{\mathcal{X}}^{\mathcal{A} \to \mathcal{B}}$ we additionally have:

- *On input $(x, A) \in \mathcal{X} \times \mathcal{A}$ at interface B, output (B, x) at interfaces E, A.*

If $\mathcal{A}$ (or $\mathcal{B}$) is singleton set $\mathcal{A} = \{A\}$, we use A instead of $\mathcal{A}$ as superscript.

Definition 26 ($\mathsf{ULK}_{\mathcal{M}}^{\mathcal{S} \to \mathcal{R}}$). *For $S \in \mathcal{S}$ and $R \in \mathcal{R}$, we define the resource* ULK *as follows: Initially set $M \leftarrow [\,]$, and then:*

- *On input $(m, R) \in \mathcal{M} \times \mathcal{R}$ at interface S, output S at interface E and set $M[R] \overset{\cup}{\leftarrow} \{m\}$.*
- *On input $\diamond$ at interface R, output $(R, |M[R]|)$ at interface E.*
- *On input R at interface E, output $M[R]$ at interface R and set $M[R] \leftarrow \varnothing$.*

4.3 First Main Result: Single Honest Mixer

We now show that if a URE scheme satisfies $\mathsf{ind\text{-}ik\text{-}sulk\text{-}cpa}$ security, then it also securely constructs the resource $\mathsf{ULK}_{\mathcal{M}}^{\mathcal{S} \to \mathcal{R}}$, if appropriately used in conjunction with resources $\mathsf{1\text{-}AUT}_{\mathcal{PK}}^{\mathcal{R} \to \mathcal{S}}$, $\mathsf{AUT}_{\mathcal{C}}^{\mathcal{S} \to M}$, 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.

Definition 27 ($\boldsymbol{\pi}_{\mathsf{URE}}$). *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 protocols π_S, for any $S \in \mathcal{S}$, π_R, for any $R \in \mathcal{R}$, and π_M, which are defined as follows:*[3]

- *π_S: 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 output (c, M) to $\mathsf{AUT}_{\mathcal{C}}^{\mathcal{S} \to M}$ though interface* in.
- *π_M: 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 $\mathcal{B}' \overset{\cup}{\leftarrow} \{\hat{c}\}$. Then set $\mathcal{B} \leftarrow \mathcal{B}'$.*

[3] Note that it is straightforward to formally define π_S, π_M, and π_R with pseudocode, as done in the proof of Theorem 2, but for better readability in the main body, we decided to describe them informally.

2. *Get* $\hat{c} \leftarrow \mathtt{Rnc}(c)$ *and set* $\mathcal{B} \stackrel{\cup}{\leftarrow} \{\hat{c}\}$.

- *On input* $(R, \diamond)$ *from* $\mathsf{AUT}^{M \leftrightarrow \mathcal{R}}_{\{\diamond\}\cup 2^{\mathcal{C}}}$ *through interface* in, *output* $(\mathcal{B}, R)$ *to* $\mathsf{AUT}^{M \leftrightarrow \mathcal{R}}_{\{\diamond\}\cup 2^{\mathcal{C}}}$ *through interface* in.
- *On input* $(R, \mathcal{O}_R)$ *from* $\mathsf{AUT}^{M \leftrightarrow \mathcal{R}}_{\{\diamond\}\cup 2^{\mathcal{C}}}$ *through interface* in, *set* $\mathcal{B} \stackrel{\setminus}{\leftarrow} \mathcal{O}_R$.

– π_R: *Upon initialization, get* $(sk_R, pk_R) \leftarrow \mathtt{Gen}$, *output* (pk_R, S) *to* $\mathsf{AUT}^{\mathcal{R} \to \mathcal{S}}_{\mathcal{PK}}$ *through interface* in *for each* $S \in \mathcal{S}$, *and then on input* $\diamond$ *at interface* out:
1. *Output* $\diamond$ *to* $\mathsf{AUT}^{M \leftrightarrow \mathcal{R}}_{\{\diamond\}\cup 2^{\mathcal{C}}}$ *through interface* in.
2. *On input* $(M, \mathcal{B})$ *from* $\mathsf{AUT}^{M \leftrightarrow \mathcal{R}}_{\{\diamond\}\cup 2^{\mathcal{C}}}$ *through interface* in, *set* $\mathcal{O}_R \leftarrow \varnothing$, *and then for each* $c \in \mathcal{B}$ *get* $m \leftarrow \mathtt{Dec}_{sk_R}$, *and if* $m \neq \bot$, *set* $\mathcal{O}_R \stackrel{\cup}{\leftarrow} \{m\}$.
3. *Output* $\mathcal{O}_R$ *to* $\mathsf{AUT}^{M \leftrightarrow \mathcal{R}}_{\{\diamond\}\cup 2^{\mathcal{C}}}$ *through interface* in.

We can now define what it means for the protocol $\boldsymbol{\pi}_{\mathsf{URE}}$, and therefore for the underlying URE scheme Π_{URE}, to be composably secure.

Definition 28 ($\mathsf{hm\text{-}ure}$). $\left[1\text{-}\mathsf{AUT}^{\mathcal{R} \to \mathcal{S}}_{\mathcal{PK}}, \mathsf{AUT}^{\mathcal{S} \to M}_{\mathcal{C}}, \mathsf{AUT}^{M \leftrightarrow \mathcal{R}}_{\{\diamond\}\cup 2^{\mathcal{C}}}\right] \xrightarrow{\boldsymbol{\pi}_{\mathsf{URE}}} \mathsf{ULK}^{\mathcal{S} \to \mathcal{R}}_{\mathcal{M}}$.

Finally, our first main result is that the game-based notions imply this new composable notion.

Theorem 2. $\mathsf{cor} \wedge \mathsf{rob} \wedge \mathsf{ind\text{-}cpa} \wedge \mathsf{ik\text{-}cpa} \wedge \mathsf{sulk\text{-}cpa} \implies \mathsf{hm\text{-}ure}$.

Proof. Let $n \doteq |\mathcal{R}|$, assume $\mathcal{R} = \{R_1, \ldots, R_n\}$, and let $pk_i \doteq pk_{R_i}$, for $i \in [n]$. By combining Lemma 13 and Lemma 22, we can use the substitution n-$\mathsf{cor\text{-}rob}$, and by combining Lemma 15 and Lemma 24, we can use the substitution n-$\mathsf{ind\text{-}ik\text{-}sulk\text{-}cpa}$. Define sim, ρ_1, and ρ_2 as in Figure 4, and also define hybrid resources $\mathbf{H}_0$ to $\mathbf{H}_3$ as in Figure 5, where changes from the previous hybrid are highlighted in dark gray. Then, for a fixed $R \in \mathcal{R}$:

$$
\begin{aligned}
\pi_{\mathsf{URE}} & \left[1\text{-}\mathsf{AUT}^{\mathcal{R} \to \mathcal{S}}_{\mathcal{PK}}, \mathsf{AUT}^{\mathcal{S} \to M}_{\mathcal{C}}, \mathsf{AUT}^{M \leftrightarrow \mathcal{R}}_{\{\diamond\}\cup 2^{\mathcal{C}}}\right] \\
& \equiv \mathbf{H}_0 && \text{(monolithic representation)} \\
& \equiv \rho_1(\llbracket (\!| \mathbf{E}_{pk_1,\ldots,pk_n}, *, * |\!) \triangleright (\!| \mathbf{R}^*, * |\!) \triangleright \mathbf{D}_{sk_1,\ldots,sk_n}, \boldsymbol{pk}_{pk_1,\ldots,pk_n} \rrbracket) \\
& && \text{(by inspection)} \\
& \doteq \rho_1(\llbracket \mathbf{I}_n, \boldsymbol{pk}_{pk_1,\ldots,pk_n} \rrbracket) && (\mathcal{R}\text{-}\mathsf{cor\text{-}rob}) \\
& \equiv \mathbf{H}_1 && \text{(by inspection)} \\
& = \rho_2(\llbracket \mathbf{E}_{pk_1,\ldots,pk_n} \triangleright \langle *, \mathbf{R} \rangle, \boldsymbol{pk}_{pk_1,\ldots,pk_n} \rrbracket) \\
& \doteq \rho_2(\llbracket (\!| *, * |\!)_1 \triangleright \langle \mathbf{E}^{\$}_{pk_1}, \mathbf{E}^{\$}_{pk_1} \rangle, \boldsymbol{pk}_{pk_1,\ldots,pk_n} \rrbracket) && (\mathcal{R}\text{-}\mathsf{ind\text{-}ik\text{-}sulk\text{-}cpa}) \\
& = \mathbf{H}_2 \\
& \equiv \mathbf{H}_3 && \text{(by inspection)} \\
& \equiv \mathsf{sim}\, \mathsf{ULK}^{\mathcal{S} \to \mathcal{R}}. && \text{(monolithic representation)}
\end{aligned}
$$

□

$\rho_1(\llbracket \mathbf{S}, \boldsymbol{pk}_{\mathcal{R}} \rrbracket)$

init:
- $\mathcal{B}, \mathcal{D} \leftarrow \varnothing$
- **for** $R \in \mathcal{R}$ **do**
  - $pk_R \leftarrow \boldsymbol{pk}_{\mathcal{R}}(R)$
  - **out**$(E; (R, pk_R))$

iface $S(m \in \mathcal{M}, R \in \mathcal{R})$:
- $(\mathcal{B}, \mathcal{D}) \leftarrow \mathsf{Rnc}(\mathcal{B}, \mathcal{D})$
- $c \leftarrow \mathtt{Enc}_{pk_R}(m)$
- **out**$(E; (S, c))$
- $\hat{c} \leftarrow \mathtt{Rnc}(m)$
- $\mathcal{B} \xleftarrow{\cup} \{\hat{c}\}$
- $\mathcal{D} \xleftarrow{\cup} \{(S, m, 1)\}$

iface $R(\diamond)$:
- $\mathcal{O}_E, \mathcal{O}_R, \mathcal{D}' \leftarrow \varnothing$
- **out**$(E; R)$
- **out**$(E; \mathcal{B})$
- **for** $(S, m, t) \in \mathcal{D}$ **do**
  - $m \leftarrow \mathbf{S}(S, m, t, R)$
  - **if** $m \neq \perp$ **then**
    - $\mathcal{O}_E \xleftarrow{\cup} \{\hat{c}\}$
    - $\mathcal{O}_R \xleftarrow{\cup} \{m\}$
    - $\mathcal{D}' \xleftarrow{\cup} \{(S, m, t, R)\}$
- $\mathcal{B} \xleftarrow{\setminus} \mathcal{O}_E$
- $\mathcal{D} \xleftarrow{\setminus} \mathcal{D}'$
- **out**$(E; \mathcal{O}_E)$
- **out**$(R; \mathcal{O}_R)$

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** $(S, m, t) \in \mathcal{D}$ **do**
  - $\mathcal{D}' \xleftarrow{\cup} \{(S, m, t+1)\}$
- **return** $(\mathcal{B}', \mathcal{D}')$

$\rho_2(\llbracket \mathbf{S}, \boldsymbol{pk}_{\mathcal{R}} \rrbracket)$

init:
- $\mathcal{B} \leftarrow \varnothing, M, C \leftarrow [\,]$
- **for** $R \in \mathcal{R}$ **do**
  - $pk_R \leftarrow \boldsymbol{pk}_{\mathcal{R}}(R)$
  - **out**$(E; (R, pk_R))$

iface $S(m \in \mathcal{M}, R \in \mathcal{R})$:
- $\mathcal{B} \leftarrow \mathsf{Rnc}(\mathcal{B}, M)$
- $(c, \hat{c}) \leftarrow \mathbf{S}(R, m)$
- **out**$(E; (S, c))$
- $\mathcal{B} \xleftarrow{\cup} \{\hat{c}\}$
- $M[R] \xleftarrow{\cup} \{m\}$
- $C[(R, m)] \leftarrow \hat{c}$

iface $R(\diamond)$:
- $\mathcal{O}_E, \mathcal{O}_R \leftarrow \varnothing$
- **out**$(E; R)$
- **out**$(E; \mathcal{B})$
- **for** $m \in M[R]$ **do**
  - $\mathcal{O}_E \xleftarrow{\cup} \{\hat{c}\}$
- $\mathcal{O}_R \leftarrow M[R]$
- $M[R] \leftarrow \varnothing$
- $\mathcal{B} \xleftarrow{\setminus} \mathcal{O}_E$
- **out**$(E; \mathcal{O}_E)$
- **out**$(R; \mathcal{O}_R)$

func $\mathsf{Rnc}(\mathcal{B}, M)$:
- $\mathcal{B}' \leftarrow \varnothing$
- **for** $R \in \mathcal{R}$ **do**
  - **for** $m \in M[R]$ **do**
    - $c \leftarrow C[(R, m)]$
    - $\hat{c} \leftarrow \mathtt{Rnc}(c)$
    - $\mathcal{B}' \xleftarrow{\cup} \{\hat{c}\}$
- **return** $\mathcal{B}'$

sim

init:
- $\mathcal{B} \leftarrow \varnothing$
- $\tilde{R} \xleftarrow{\$} \mathcal{R}, \tilde{m} \xleftarrow{\$} \mathcal{M}$
- **for** $R \in \mathcal{R}$ **do**
  - $(sk_R, pk_R) \leftarrow \mathtt{Gen}$
  - **out**$(\mathsf{out}; (R, pk_R))$

iface $\mathsf{in}(S \in \mathcal{S})$:
- $\mathcal{B} \leftarrow \mathsf{Rnc}(\mathcal{B})$
- $c \leftarrow \mathtt{Enc}_{pk_{\tilde{R}}}(\tilde{m})$
- **out**$(\mathsf{out}; (S, c))$
- $\hat{c} \leftarrow \mathtt{Enc}_{pk_{\tilde{R}}}(\tilde{m})$
- $\mathcal{B} \xleftarrow{\cup} \{\hat{c}\}$

iface $\mathsf{in}(R \in \mathcal{R}, \ell \in \mathbb{N})$:
- $\mathcal{O}_E \leftarrow \varnothing$
- **out**$(\mathsf{out}; R)$
- **out**$(\mathsf{out}; \mathcal{B})$
- $\mathcal{O}_E \xleftarrow{\$} \{\mathcal{A} \subseteq \mathcal{B} : |\mathcal{A}| = \ell\}$
- $\mathcal{B} \xleftarrow{\setminus} \mathcal{O}_E$
- **out**$(\mathsf{out}; \mathcal{O}_E)$
- **out**$(\mathsf{in}; \diamond)$

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** $\mathcal{B}'$

Fig. 4. Reductions and simulator for the proof of Theorem 2, for $S \in \mathcal{S}$ and $R \in \mathcal{R}$.

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

$\mathbf{H}_0$

init:
- $\mathcal{B} \leftarrow \varnothing$
- **for** $R \in \mathcal{R}$ **do**
  - $(sk_R, pk_R) \leftarrow \texttt{Gen}$
  - **out**$(E; (R, pk_R))$

iface $S(m \in \mathcal{M}, R \in \mathcal{R})$:
- $\mathcal{B} \leftarrow \mathsf{Rnc}(\mathcal{B})$
- $c \leftarrow \texttt{Enc}_{pk_R}(m)$
- **out**$(E; (S, c))$
- $\hat{c} \leftarrow \texttt{Rnc}(m)$
- $\mathcal{B} \xleftarrow{\cup} \{\hat{c}\}$

iface $R(\diamond)$:
- $\mathcal{O}_E, \mathcal{O}_R \leftarrow \varnothing$
- **out**$(E; R)$
- **out**$(E; \mathcal{B})$
- **for** $\hat{c} \in \mathcal{B}$ **do**
  - $m \leftarrow \texttt{Dec}_{sk_R}(\hat{c})$
  - **if** $m \neq \perp$ **then**
    - $\mathcal{O}_E \xleftarrow{\cup} \{\hat{c}\}$
    - $\mathcal{O}_R \xleftarrow{\cup} \{m\}$
- $\mathcal{B} \xleftarrow{\setminus} \mathcal{O}_E$
- **out**$(E; \mathcal{O}_E)$
- **out**$(R; \mathcal{O}_R)$

func $\mathsf{Rnc}(\mathcal{B})$:
- $\mathcal{B}' \leftarrow \varnothing$
- **for** $c \in \mathcal{B}$ **do**
  - $\hat{c} \leftarrow \texttt{Rnc}(c)$
  - $\mathcal{B}' \xleftarrow{\cup} \{\hat{c}\}$
- **return** $\mathcal{B}'$

$\boxed{\mathbf{H}_1}$ $\boxed{\mathbf{H}_2}$

init:
- $\mathcal{B} \leftarrow \varnothing, M, C \leftarrow [\,]$
- $\boxed{\tilde{R} \xleftarrow{\$} \mathcal{R}, \tilde{m} \xleftarrow{\$} \mathcal{M}}$
- **for** $R \in \mathcal{R}$ **do**
  - $(sk_R, pk_R) \leftarrow \texttt{Gen}$
  - **out**$(E; (R, pk_R))$

iface $S(m \in \mathcal{M}, R \in \mathcal{R})$:
- $\mathcal{B} \leftarrow \mathsf{Rnc}(\mathcal{B}, M)$
- $\boxed{c \leftarrow \texttt{Enc}_{pk_R}(m)}$
- $\boxed{c \leftarrow \texttt{Enc}_{pk_{\tilde{R}}}(\tilde{m})}$
- **out**$(E; (S, c))$
- $\boxed{\hat{c} \leftarrow \texttt{Rnc}(m)}$
- $\boxed{\hat{c} \leftarrow \texttt{Enc}_{pk_{\tilde{R}}}(\tilde{m})}$
- $\mathcal{B} \xleftarrow{\cup} \{\hat{c}\}$
- $M[R] \xleftarrow{\cup} \{m\}$
- $C[(R, m)] \leftarrow \hat{c}$

iface $R(\diamond)$:
- $\mathcal{O}_E, \mathcal{O}_R \leftarrow \varnothing$
- **out**$(E; R)$
- **out**$(E; \mathcal{B})$
- **for** $m \in M[R]$ **do**
  - $\mathcal{O}_E \xleftarrow{\cup} \{\hat{c}\}$
- $\mathcal{O}_R \leftarrow M[R]$
- $M[R] \leftarrow \varnothing$
- $\mathcal{B} \xleftarrow{\setminus} \mathcal{O}_E$
- **out**$(E; \mathcal{O}_E)$
- **out**$(R; \mathcal{O}_R)$

func $\mathsf{Rnc}(\mathcal{B}, M)$:
- $\mathcal{B}' \leftarrow \varnothing$
- **for** $R \in \mathcal{R}$ **do**
  - **for** $m \in M[R]$ **do**
    - $c \leftarrow C[(R,m)]$
    - $\hat{c} \leftarrow \texttt{Rnc}(c)$
    - $\mathcal{B}' \xleftarrow{\cup} \{\hat{c}\}$
- **return** $\mathcal{B}'$

$\mathbf{H}_3$

init:
- $\mathcal{B} \leftarrow \varnothing, M \leftarrow [\,]$
- $\tilde{R} \xleftarrow{\$} \mathcal{R}, \tilde{m} \xleftarrow{\$} \mathcal{M}$
- **for** $R \in \mathcal{R}$ **do**
  - $(sk_R, pk_R) \leftarrow \texttt{Gen}$
  - **out**$(E; (R, pk_R))$

iface $S(m \in \mathcal{M}, R \in \mathcal{R})$:
- $\mathcal{B} \leftarrow \mathsf{Rnc}(\mathcal{B})$
- $c \leftarrow \texttt{Enc}_{pk_{\tilde{R}}}(\tilde{m})$
- **out**$(E; (S, c))$
- $\hat{c} \leftarrow \texttt{Enc}_{pk_{\tilde{R}}}(\tilde{m})$
- $\mathcal{B} \xleftarrow{\cup} \{\hat{c}\}$
- $M[R] \xleftarrow{\cup} \{m\}$

iface $R(\diamond)$:
- $\mathcal{O}_E, \mathcal{O}_R \leftarrow \varnothing$
- **out**$(E; R)$
- **out**$(E; \mathcal{B})$
- $\ell \leftarrow |\mathcal{O}_R|$
- $\mathcal{O}_E \xleftarrow{\$} \{\mathcal{A} \subseteq \mathcal{B} : |\mathcal{A}| = \ell\}$
- $\mathcal{O}_R \leftarrow M[R]$
- $M[R] \leftarrow \varnothing$
- $\mathcal{B} \xleftarrow{\setminus} \mathcal{O}_E$
- **out**$(E; \mathcal{O}_E)$
- **out**$(R; \mathcal{O}_R)$

func $\mathsf{Rnc}(\mathcal{B})$:
- $\mathcal{B}' \leftarrow \varnothing$
- **for** $c \in \mathcal{B}$ **do**
  - $\hat{c} \leftarrow \texttt{Rnc}(c)$
  - $\mathcal{B}' \xleftarrow{\cup} \{\hat{c}\}$
- **return** $\mathcal{B}'$

Fig. 5. Hybrids for the proof of Theorem 2, for $S \in \mathcal{S}$ and $R \in \mathcal{R}$.

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.*

4.4 Second Main Result: Single Dishonest Mixer

We now consider the case where the mixer is dishonest, that is, $\mathcal{H} \doteq \mathcal{S} \cup \mathcal{R}$ (and $\overline{\mathcal{H}} = \{M, E\}$). This means that we define security of a URE scheme as in Definition 28, but where no protocol converter is attached to interface M of the assumed resource. More precisely, we are considering security of an $\mathcal{H}$-protocol $\boldsymbol{\pi}'_{\mathsf{URE}}$ which is composed only by the local protocols π_S (for $S \in \mathcal{S}$) and π_R (for $R \in \mathcal{R}$) from Definition 27. In order to meaningfully adapt Definition 28 to $\boldsymbol{\pi}'_{\mathsf{URE}}$, we need to introduce the following resources (for this specific honest and dishonest parties sets $\mathcal{H}$ and $\overline{\mathcal{H}}$): the *insecure* and the *confidential channels*.

Definition 29 ($\mathsf{INS}_{\mathcal{C}}^{\mathcal{S}\to\mathcal{R}}$)**.** *For $S \in \mathcal{S}$ and $R \in \mathcal{R}$, we define the resource $\mathsf{INS}_{\mathcal{C}}^{\mathcal{S}\to\mathcal{R}}$ as follows:*

- *On input $(c, R) \in \mathcal{C} \times \mathcal{R}$ at interface S, output (S, c) at interfaces E, M.*
- *On input $(c, R) \in \mathcal{C} \times \mathcal{R}$ at interface $I \in \{E,M\}$, output (I, c) at interface R.*

Definition 30 ($\mathsf{CNF}_{\mathcal{M}}^{\mathcal{S}\to\mathcal{R}}$)**.** *For $S \in \mathcal{S}$ and $R \in \mathcal{R}$, we define the resource $\mathsf{CNF}_{\mathcal{M}}^{\mathcal{S}\to\mathcal{R}}$ as follows, where initially $i \leftarrow 0$ and $T \leftarrow [\,]$:*

- *On input $(m, R) \in \mathcal{M} \times \mathcal{R}$ at interface S, output $(S, |m|, i)$ at interfaces E, M, and set $T[i] \leftarrow (S, m, R)$ and $i \xleftarrow{+} 1$.*
- *On input $(m, R) \in \mathcal{M} \times \mathcal{R}$ at interface $I \in \{E, M\}$, output (I, m) at interface R.*
- *On input $i \in \mathbb{N}$ at interface $I \in \{E, M\}$, get $(S, m, R) \leftarrow T[i]$, and output (S, m) at interface R.*

We can now define the composable security of $\boldsymbol{\pi}'_{\mathsf{URE}}$ as follows.

Definition 31 (dm-ure)**.** $\left[1\text{-}\mathsf{AUT}_{\mathcal{PK}}^{\mathcal{R}\to\mathcal{S}}, \mathsf{AUT}_{\mathcal{C}}^{\mathcal{S}\to M}, \mathsf{AUT}_{\{\diamond\}\cup 2^{\mathcal{C}}}^{M\leftrightarrow\mathcal{R}}\right] \xrightarrow{\boldsymbol{\pi}'_{\mathsf{URE}}} \mathsf{CNF}_{\mathcal{M}}^{\mathcal{S}\to\mathcal{R}}.$

It is easy to see that, since now the mixer is dishonest, the assumed resource behaves exactly as the insecure channel $\mathsf{INS}_{\mathcal{C}}^{\mathcal{S}\to\mathcal{R}}$, since now the adversary (controlling interfaces E and M) not only will see every ciphertext input by the honest senders, but it will also be able to inject ciphertexts to the receivers. Therefore, as it has been shown in [CMT13,BMPR21], it is possible to construct the confidential channel $\mathsf{CNF}_{\mathcal{M}}^{\mathcal{S}\to\mathcal{R}}$ from $\mathsf{INS}_{\mathcal{C}}^{\mathcal{S}\to\mathcal{R}}$, if the scheme is ind-rcca secure.

Theorem 3. cor $\wedge$ rob $\wedge$ ind-rcca $\implies$ dm-ure. □

References

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. doi:10.1007/978-3-319-16295-9_12.

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. doi:10.1007/3-540-45539-6_18.

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. doi:10.1007/978-3-030-03332-3_9.

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. doi:10.1007/978-3-030-57990-6_23.

BM21. Fabio Banfi and Ueli Maurer. Composable notions for anonymous and authenticated communication. Cryptology ePrint Archive, Report 2021/1581, 2021. https://eprint.iacr.org/2021/1581.

BMPR21. Christian Badertscher, Ueli Maurer, Christopher Portmann, and Guilherme Rito. Revisiting (R)CCA security and replay protection. In Juan Garay, editor, *PKC 2021, Part II*, volume 12711 of *LNCS*, pages 173–202. Springer, Heidelberg, May 2021. doi:10.1007/978-3-030-75248-4_7.

CMT13. Sandro Coretti, Ueli Maurer, and Björn Tackmann. Constructing confidential channels from authenticated channels - public-key encryption revisited. In Kazue Sako and Palash Sarkar, editors, *ASIACRYPT 2013, Part I*, volume 8269 of *LNCS*, pages 134–153. Springer, Heidelberg, December 2013. doi:10.1007/978-3-642-42033-7_8.

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. doi:10.1007/978-3-540-24660-2_14.

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. doi:10.1007/978-3-540-24638-1_9.

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. doi:10.1007/978-3-642-39077-7_2.

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. doi:10.1007/3-540-46035-7_8.

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.

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. doi:10.1007/978-3-540-74143-5_8.

MR11. Ueli Maurer and Renato Renner. Abstract cryptography. In Bernard Chazelle, editor, *ICS 2011*, pages 1–21. Tsinghua University Press, January 2011.

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. doi:10.1007/978-3-540-74143-5_29.

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. doi:10.1007/978-3-030-84259-8_10.

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. doi:10.1007/978-3-540-24638-1_18.

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. doi:10.1007/978-3-319-98113-0_14.

A Missing Proofs

In this section (and also in Appendix C), some proofs (of both implications and separations) use the exact same sequence of factorizations 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.

A.1 Combined Notions

Lemma 13. $\mathsf{cor} \wedge \mathsf{rob} \iff \mathsf{cor\text{-}rob}$.

Proof.

$\Longrightarrow$: Let $(sk_1, pk_1) \leftarrow \texttt{Gen}$ and $(sk_2, pk_2) \leftarrow \texttt{Gen}$, and consider

- $\rho_1([\![\mathbf{S}, x]\!]) \doteq [\![\langle \mathbf{S}, \llparenthesis \mathbf{E}_x, * \rrparenthesis \triangleright \mathbf{R}^* \triangleright \mathbf{D}_{sk_2} \rangle_*,$ $\langle \llparenthesis \mathbf{E}_{pk_2}, * \rrparenthesis \triangleright \mathbf{R}^* \triangleright \mathbf{D}_{sk_1}, \llparenthesis \mathbf{E}_{pk_2}, * \rrparenthesis \triangleright \mathbf{R}^* \triangleright \mathbf{D}_{sk_2} \rangle_*, x, pk_2]\!]$,
- $\rho_2([\![\mathbf{S}, x]\!]) \doteq [\![\langle \llparenthesis *, * \rrparenthesis_1, \llparenthesis \mathbf{E}_{pk_1}, * \rrparenthesis \triangleright \mathbf{R}^* \triangleright \mathbf{D}_{sk_2} \rangle_*,$ $\langle \llparenthesis \mathbf{E}_x, * \rrparenthesis \triangleright \mathbf{R}^* \triangleright \mathbf{D}_{sk_1}, \mathbf{S} \rangle_*, pk_1, x]\!]$,
- $\rho_3([\![\mathbf{S}, x, y]\!]) \doteq [\![\langle \llparenthesis *, * \rrparenthesis_1, \mathbf{S} \rangle_*, \langle \llparenthesis \mathbf{E}_y, * \rrparenthesis \triangleright \mathbf{R}^* \triangleright \mathbf{D}_{sk_1}, \llparenthesis *, * \rrparenthesis_1 \rangle_*, x, y]\!]$, and
- $\rho_4([\![\mathbf{S}, x, y]\!]) \doteq [\![\langle \llparenthesis *, * \rrparenthesis_1, \llparenthesis \bot, * \rrparenthesis_1 \rangle_*, \langle \mathbf{S}, \llparenthesis *, * \rrparenthesis_1 \rangle_*, y, x]\!]$.

Then:

$$
\begin{aligned}
&[\![\llparenthesis \mathbf{E}_{pk_1}, *, * \rrparenthesis \triangleright \llparenthesis \mathbf{R}^*, * \rrparenthesis \triangleright \mathbf{D}_{sk_1,sk_2}, \llparenthesis \mathbf{E}_{pk_2}, *, * \rrparenthesis \triangleright \llparenthesis \mathbf{R}^*, * \rrparenthesis \triangleright \mathbf{D}_{sk_1,sk_2}, pk_1, pk_2]\!] \\
&\qquad \equiv [\![\langle \llparenthesis \mathbf{E}_{pk_1}, * \rrparenthesis \triangleright \mathbf{R}^* \triangleright \mathbf{D}_{sk_1}, \llparenthesis \mathbf{E}_{pk_1}, * \rrparenthesis \triangleright \mathbf{R}^* \triangleright \mathbf{D}_{sk_2} \rangle_*, \\
&\qquad\qquad \langle \llparenthesis \mathbf{E}_{pk_2}, * \rrparenthesis \triangleright \mathbf{R}^* \triangleright \mathbf{D}_{sk_1}, \llparenthesis \mathbf{E}_{pk_2}, * \rrparenthesis \triangleright \mathbf{R}^* \triangleright \mathbf{D}_{sk_2} \rangle_*, pk_1, pk_2]\!] \\
&\qquad = \rho_1([\![\llparenthesis \mathbf{E}_{pk_1}, * \rrparenthesis \triangleright \mathbf{R}^* \triangleright \mathbf{D}_{sk_1}, pk_1]\!]) \\
&\qquad \mathrel{\widehat{=}} \rho_1([\![\llparenthesis *, * \rrparenthesis_1, pk_1]\!]) && (\mathsf{cor}) \\
&\qquad = [\![\langle \llparenthesis *, * \rrparenthesis_1, \llparenthesis \mathbf{E}_{pk_1}, * \rrparenthesis \triangleright \mathbf{R}^* \triangleright \mathbf{D}_{sk_2} \rangle_*, \\
&\qquad\qquad \langle \llparenthesis \mathbf{E}_{pk_2}, * \rrparenthesis \triangleright \mathbf{R}^* \triangleright \mathbf{D}_{sk_1}, \llparenthesis \mathbf{E}_{pk_2}, * \rrparenthesis \triangleright \mathbf{R}^* \triangleright \mathbf{D}_{sk_2} \rangle_*, pk_1, pk_2]\!] \\
&\qquad = \rho_2([\![\llparenthesis \mathbf{E}_{pk_2}, * \rrparenthesis \triangleright \mathbf{R}^* \triangleright \mathbf{D}_{sk_2}, pk_2]\!]) \\
&\qquad \mathrel{\widehat{=}} \rho_2([\![\llparenthesis *, * \rrparenthesis_1, pk_2]\!]) && (\mathsf{cor}) \\
&\qquad = [\![\langle \llparenthesis *, * \rrparenthesis_1, \llparenthesis \mathbf{E}_{pk_1}, * \rrparenthesis \triangleright \mathbf{R}^* \triangleright \mathbf{D}_{sk_2} \rangle_*, \\
&\qquad\qquad \langle \llparenthesis \mathbf{E}_{pk_2}, * \rrparenthesis \triangleright \mathbf{R}^* \triangleright \mathbf{D}_{sk_1}, \llparenthesis *, * \rrparenthesis_1 \rangle_*, pk_1, pk_2]\!] \\
&\qquad = \rho_3([\![\llparenthesis \mathbf{E}_{pk_1}, * \rrparenthesis \triangleright \mathbf{R}^* \triangleright \mathbf{D}_{sk_2}, pk_1, pk_2]\!]) \\
&\qquad \mathrel{\widehat{=}} \rho_3([\![\llparenthesis \bot, * \rrparenthesis_1, pk_1, pk_2]\!]) && (\mathsf{rob}) \\
&\qquad = [\![\langle \llparenthesis *, * \rrparenthesis_1, \llparenthesis \bot, * \rrparenthesis_1 \rangle_*, \langle \mathbf{E}_{pk_2} \triangleright \mathbf{R}^* \triangleright \mathbf{D}_{sk_1}, \llparenthesis *, * \rrparenthesis_1 \rangle_*, pk_1, pk_2]\!] \\
&\qquad = \rho_4([\![\llparenthesis \mathbf{E}_{pk_2}, * \rrparenthesis \triangleright \mathbf{R}^* \triangleright \mathbf{D}_{sk_1}, pk_2, pk_1]\!]) \\
&\qquad \mathrel{\widehat{=}} \rho_4([\![\llparenthesis \bot, * \rrparenthesis_1, pk_2, pk_1]\!]) && (\mathsf{rob}) \\
&\qquad = [\![\langle \llparenthesis *, * \rrparenthesis_1, \llparenthesis \bot, * \rrparenthesis_1 \rangle_*, \langle \llparenthesis \bot, * \rrparenthesis_1, \llparenthesis *, * \rrparenthesis_1 \rangle_*, pk_1, pk_2]\!] \\
&\qquad \equiv [\![\llparenthesis *, \bot, * \rrparenthesis \triangleright \langle *, * \rangle_*, \llparenthesis *, \bot, * \rrparenthesis_{2,1,3} \triangleright \langle *, * \rangle_*, pk_1, pk_2]\!].
\end{aligned}
$$

$\Longleftarrow$: Let $(sk_1, pk_1) \leftarrow \texttt{Gen}$ and $(sk_2, pk_2) \leftarrow \texttt{Gen}$, and consider $\rho_i(\llbracket \mathbf{S}, \mathbf{T}, x, y \rrbracket) \doteq \llbracket (\!| *, \langle *, i \rangle |\!) \triangleright \mathbf{S}, x \rrbracket$, for $i \in \{1, 2\}$. Then:

$$\begin{aligned}
&\llbracket (\!| \mathbf{E}_{pk_1}, * |\!) \triangleright \mathbf{R}^{*} \triangleright \mathbf{D}_{sk_1}, pk_1 \rrbracket \\
&\qquad \equiv \llbracket (\!| *, \langle *, 1 \rangle |\!) \triangleright (\!| \mathbf{E}_{pk_1}, *, * |\!) \triangleright (\!| \mathbf{R}^{*}, * |\!) \triangleright \mathbf{D}_{sk_1, sk_2}, pk \rrbracket \\
&\qquad = \rho_1(\llbracket (\!| \mathbf{E}_{pk_1}, *, * |\!) \triangleright (\!| \mathbf{R}^{*}, * |\!) \triangleright \mathbf{D}_{sk_1, sk_2}, \\
&\qquad\qquad (\!| \mathbf{E}_{pk_2}, *, * |\!) \triangleright (\!| \mathbf{R}^{*}, * |\!) \triangleright \mathbf{D}_{sk_1, sk_2}, pk_1, pk_2 \rrbracket) \\
&\qquad \simeq \rho_1(\llbracket (\!| *, \bot, * |\!) \triangleright \langle *, * \rangle_{*}, \\
&\qquad\qquad (\!| *, \bot, * |\!)_{2,1,3} \triangleright \langle *, * \rangle_{*}, pk_1, pk_2 \rrbracket) && (\textsf{cor-rob}) \\
&\qquad = \llbracket (\!| *, \langle *, 1 \rangle |\!) \triangleright (\!| *, \bot, * |\!) \triangleright \langle *, * \rangle_{*}, pk_1 \rrbracket \\
&\qquad \equiv \llbracket (\!| *, * |\!)_1, pk_1 \rrbracket,
\end{aligned}$$

and

$$\begin{aligned}
&\llbracket (\!| \mathbf{E}_{pk_1}, * |\!) \triangleright \mathbf{R}^{*} \triangleright \mathbf{D}_{sk_2}, pk_1, pk_2 \rrbracket \\
&\qquad \equiv \llbracket (\!| *, \langle *, 2 \rangle |\!) \triangleright (\!| \mathbf{E}_{pk_1}, *, * |\!) \triangleright (\!| \mathbf{R}^{*}, * |\!) \triangleright \mathbf{D}_{sk_1, sk_2}, pk_1, pk_2 \rrbracket \\
&\qquad = \rho_2(\llbracket (\!| \mathbf{E}_{pk_1}, *, * |\!) \triangleright (\!| \mathbf{R}^{*}, * |\!) \triangleright \mathbf{D}_{sk_1, sk_2}, \\
&\qquad\qquad (\!| \mathbf{E}_{pk_2}, *, * |\!) \triangleright (\!| \mathbf{R}^{*}, * |\!) \triangleright \mathbf{D}_{sk_1, sk_2}, pk_1, pk_2 \rrbracket) \\
&\qquad \simeq \rho_2(\llbracket (\!| *, \bot, * |\!) \triangleright \langle *, * \rangle_{*}, \\
&\qquad\qquad (\!| *, \bot, * |\!)_{2,1,3} \triangleright \langle *, * \rangle_{*}, pk_1, pk_2 \rrbracket) && (\textsf{cor-rob}) \\
&\qquad = \llbracket (\!| *, \langle *, 2 \rangle |\!) \triangleright (\!| *, \bot, * |\!) \triangleright \langle *, * \rangle_{*}, pk_1, pk_2 \rrbracket \\
&\qquad \equiv \llbracket \bot, pk_1, pk_2 \rrbracket. && \square
\end{aligned}$$

Lemma 14. $\textsf{ind-cpa} \land \textsf{ik-cpa} \land \textsf{ulk-cpa} \implies \textsf{ind-ik-ulk-cpa}$.

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

- $\rho_1(\llbracket \mathbf{S}, \mathbf{T}, x, y \rrbracket) \doteq \llbracket \mathbf{S} \triangleright \langle *, \mathbf{R} \rangle, \mathbf{T} \triangleright \langle *, \mathbf{R} \rangle, x, y \rrbracket$,
- $\rho_2(\llbracket \mathbf{S}, x \rrbracket) \doteq \llbracket \mathbf{S}, \mathbf{S}, x, pk_2 \rrbracket$, and
- $\rho_3(\llbracket \mathbf{S}, x \rrbracket) \doteq \llbracket \langle \mathbf{S}, \mathbf{S} \triangleright \mathbf{R} \rangle, \langle \mathbf{S}, \mathbf{S} \triangleright \mathbf{R} \rangle, x, pk_2 \rrbracket$.

Then:

$$\begin{aligned}
&\llbracket \mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R} \rangle, \mathbf{E}_{pk_2} \triangleright \langle *, \mathbf{R} \rangle, pk_1, pk_2 \rrbracket \\
&\qquad = \rho_1(\llbracket \mathbf{E}_{pk_1}, \mathbf{E}_{pk_2}, pk_1, pk_2 \rrbracket) \\
&\qquad \simeq \rho_1(\llbracket \mathbf{E}_{pk_1}, \mathbf{E}_{pk_1}, pk_1, pk_2 \rrbracket) && (\textsf{ik-cpa}) \\
&\qquad = \llbracket \mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R} \rangle, \mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R} \rangle, pk_1, pk_2 \rrbracket \\
&\qquad = \rho_2(\llbracket \mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R} \rangle, pk_1 \rrbracket) \\
&\qquad \simeq \rho_2(\llbracket \langle \mathbf{E}_{pk_1}, \mathbf{E}_{pk_1} \triangleright \mathbf{R} \rangle, pk_1 \rrbracket) && (\textsf{ulk-cpa}) \\
&\qquad = \llbracket \langle \mathbf{E}_{pk_1}, \mathbf{E}_{pk_1} \triangleright \mathbf{R} \rangle, \langle \mathbf{E}_{pk_1}, \mathbf{E}_{pk_1} \triangleright \mathbf{R} \rangle, pk_1, pk_2 \rrbracket \\
&\qquad = \rho_3(\llbracket \mathbf{E}_{pk_1}, pk_1 \rrbracket) \\
&\qquad \simeq \rho_3(\llbracket \mathbf{E}^{\$}_{pk_1}, pk_1 \rrbracket) && (\textsf{ind-cpa}) \\
&\qquad = \llbracket \langle \mathbf{E}^{\$}_{pk_1}, \mathbf{E}^{\$}_{pk_1} \triangleright \mathbf{R} \rangle, \langle \mathbf{E}^{\$}_{pk_1}, \mathbf{E}^{\$}_{pk_1} \triangleright \mathbf{R} \rangle, pk_1, pk_2 \rrbracket. && \square
\end{aligned}$$

Lemma 15. $\mathsf{ind\text{-}cpa} \wedge \mathsf{ik\text{-}cpa} \wedge \mathsf{sulk\text{-}cpa} \implies \mathsf{ind\text{-}ik\text{-}sulk\text{-}cpa}$.

Proof. As for Lemma 14, but with $\rho_3(\llbracket \mathbf{S}, x \rrbracket) \doteq \llbracket \langle \mathbf{S}, \mathbf{S} \rangle, \langle \mathbf{S}, \mathbf{S} \rangle, x, pk_2 \rrbracket$. □

Lemma 16. $\mathsf{ind\text{-}ik\text{-}ulk\text{-}cpa} \implies \mathsf{ind\text{-}cpa}$.

Proof. Let $(sk, pk) \leftarrow \mathtt{Gen}$ and consider $\rho(\llbracket \mathbf{S}, \mathbf{T}, x, y \rrbracket) \doteq \llbracket (\mathbf{S})_1, x \rrbracket$. Then:

$$\begin{aligned}
\llbracket \mathbf{E}_{pk}, pk \rrbracket &\equiv \llbracket (\mathbf{E}_{pk} \triangleright \langle *, \mathbf{R} \rangle)_1, pk \rrbracket \\
&= \rho(\llbracket \mathbf{E}_{pk} \triangleright \langle *, \mathbf{R} \rangle, \mathbf{E}_{pk'} \triangleright \langle *, \mathbf{R} \rangle, pk, pk' \rrbracket) \\
&\risingdotseq \rho(\llbracket \langle \mathbf{E}^{\$}_{pk}, \mathbf{E}^{\$}_{pk} \triangleright \mathbf{R} \rangle, \langle \mathbf{E}^{\$}_{pk}, \mathbf{E}^{\$}_{pk} \triangleright \mathbf{R} \rangle, pk, pk' \rrbracket) && (\mathsf{ind\text{-}ik\text{-}ulk\text{-}cpa}) \\
&= \llbracket \langle \mathbf{E}^{\$}_{pk}, \mathbf{E}^{\$}_{pk} \triangleright \mathbf{R} \rangle_1, pk \rrbracket \\
&\equiv \llbracket \mathbf{E}^{\$}_{pk}, pk \rrbracket.
\end{aligned}$$

□

Lemma 17. $\mathsf{ind\text{-}ik\text{-}ulk\text{-}cpa} \implies \mathsf{ik\text{-}cpa}$.

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

- $\rho_1(\llbracket \mathbf{S}, \mathbf{T}, x, y \rrbracket) \doteq \llbracket (\mathbf{S})_1, (\mathbf{T})_1, x, y \rrbracket$ and
- $\rho_2(\llbracket \mathbf{S}, \mathbf{T}, x, y \rrbracket) \doteq \llbracket (\mathbf{S})_1, (\mathbf{S})_1, x, y \rrbracket$.

Then:

$$\begin{aligned}
&\llbracket \mathbf{E}_{pk_1}, \mathbf{E}_{pk_2}, pk_1, pk_2 \rrbracket \\
&\quad \equiv \llbracket (\mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R} \rangle)_1, (\mathbf{E}_{pk_2} \triangleright \langle *, \mathbf{R} \rangle)_1, pk_1, pk_2 \rrbracket \\
&\quad = \rho_1(\llbracket \mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R} \rangle, \mathbf{E}_{pk_2} \triangleright \langle *, \mathbf{R} \rangle, pk_1, pk_2 \rrbracket) \\
&\quad \risingdotseq \rho_1(\llbracket \langle \mathbf{E}^{\$}_{pk_1}, \mathbf{E}^{\$}_{pk_1} \triangleright \mathbf{R} \rangle, \langle \mathbf{E}^{\$}_{pk_1}, \mathbf{E}^{\$}_{pk_1} \triangleright \mathbf{R} \rangle, pk_1, pk_2 \rrbracket) && (\mathsf{ind\text{-}ik\text{-}ulk\text{-}cpa}) \\
&\quad = \llbracket \langle \mathbf{E}^{\$}_{pk_1}, \mathbf{E}^{\$}_{pk_1} \triangleright \mathbf{R} \rangle_1, \langle \mathbf{E}^{\$}_{pk_1}, \mathbf{E}^{\$}_{pk_1} \triangleright \mathbf{R} \rangle_1, pk_1, pk_2 \rrbracket \\
&\quad = \rho_2(\llbracket \langle \mathbf{E}^{\$}_{pk_1}, \mathbf{E}^{\$}_{pk_1} \triangleright \mathbf{R} \rangle, \langle \mathbf{E}^{\$}_{pk_1}, \mathbf{E}^{\$}_{pk_1} \triangleright \mathbf{R} \rangle, pk_1, pk_2 \rrbracket) \\
&\quad \risingdotseq \rho_2(\llbracket \mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R} \rangle, \mathbf{E}_{pk_2} \triangleright \langle *, \mathbf{R} \rangle, pk_1, pk_2 \rrbracket) && (\mathsf{ind\text{-}ik\text{-}ulk\text{-}cpa}) \\
&\quad = \llbracket (\mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R} \rangle)_1, (\mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R} \rangle)_1, pk_1, pk_2 \rrbracket \\
&\quad \equiv \llbracket \mathbf{E}_{pk_1}, \mathbf{E}_{pk_1}, pk_1, pk_2 \rrbracket.
\end{aligned}$$

□

Lemma 18. $\mathsf{ind\text{-}ik\text{-}ulk\text{-}cpa} \implies \mathsf{ulk\text{-}cpa}$.

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

- $\rho_1(\llbracket \mathbf{S}, \mathbf{T}, x, y \rrbracket) \doteq \llbracket \mathbf{S}, x \rrbracket$ and
- $\rho_2(\llbracket \mathbf{S}, \mathbf{T}, x, y \rrbracket) \doteq \llbracket \langle (\mathbf{S})_1, (\mathbf{S})_1 \triangleright \mathbf{R} \rangle, x \rrbracket$.

Then:

$$
\begin{aligned}
&[\![\mathbf{E}_{pk} \triangleright \langle *, \mathbf{R}\rangle, pk]\!] \\
&\qquad = \rho_1([\![\mathbf{E}_{pk} \triangleright \langle *, \mathbf{R}\rangle, \mathbf{E}_{pk'} \triangleright \langle *, \mathbf{R}\rangle, pk, pk']\!]) \\
&\qquad \doteq \rho_1([\![\langle \mathbf{E}^{\$}_{pk}, \mathbf{E}^{\$}_{pk} \triangleright \mathbf{R}\rangle, \langle \mathbf{E}^{\$}_{pk}, \mathbf{E}^{\$}_{pk} \triangleright \mathbf{R}\rangle, pk, pk']\!]) && \textsf{(ind-ik-ulk-cpa)} \\
&\qquad = [\![\langle \mathbf{E}^{\$}_{pk}, \mathbf{E}^{\$}_{pk} \triangleright \mathbf{R}\rangle, pk]\!] \\
&\qquad \equiv [\![\langle \langle \mathbf{E}^{\$}_{pk}, \mathbf{E}^{\$}_{pk} \triangleright \mathbf{R}\rangle_1, \langle \mathbf{E}^{\$}_{pk}, \mathbf{E}^{\$}_{pk} \triangleright \mathbf{R}\rangle_1 \triangleright \mathbf{R}\rangle, pk]\!] \\
&\qquad = \rho_2([\![\langle \mathbf{E}^{\$}_{pk}, \mathbf{E}^{\$}_{pk} \triangleright \mathbf{R}\rangle, \langle \mathbf{E}^{\$}_{pk}, \mathbf{E}^{\$}_{pk} \triangleright \mathbf{R}\rangle, pk, pk']\!]) \\
&\qquad \doteq \rho_2([\![\mathbf{E}_{pk} \triangleright \langle *, \mathbf{R}\rangle, \mathbf{E}_{pk'} \triangleright \langle *, \mathbf{R}\rangle, pk, pk']\!]) && \textsf{(ind-ik-ulk-cpa)} \\
&\qquad = [\![\langle (\mathbf{E}_{pk} \triangleright \langle *, \mathbf{R}\rangle)_1, (\mathbf{E}_{pk} \triangleright \langle *, \mathbf{R}\rangle)_1 \triangleright \mathbf{R}\rangle, pk]\!] \\
&\qquad \equiv [\![\langle \mathbf{E}_{pk}, \mathbf{E}_{pk} \triangleright \mathbf{R}\rangle, pk]\!]. && \square
\end{aligned}
$$

Lemma 19. ind-ik-sulk-cpa $\implies$ ind-cpa.

Proof. Analogous to the proof of Lemma 16. $\square$

Lemma 20. ind-ik-sulk-cpa $\implies$ ik-cpa.

Proof. Analogous to the proof of Lemma 17. $\square$

Lemma 21. ind-ik-sulk-cpa $\implies$ sulk-cpa.

Proof. As for Lemma 18, but with $\rho_2([\![\mathbf{S}, \mathbf{T}, x, y]\!]) \doteq [\![\langle (\mathbf{S})_1, (\mathbf{S})_1\rangle, x]\!]$. $\square$

A.2 Generalizing the Notions: From 2 to n Receivers

Lemma 22. cor-rob $\implies$ n-cor-rob.

Proof. Let $\rho([\![\mathbf{S}_1, \ldots, \mathbf{S}_n, x_1, \ldots, x_n]\!]) \doteq [\![\mathbf{S}', \boldsymbol{pk}_{x_1,\ldots,x_n}]\!]$, where for $i, j \in [n]$, $m \in \mathcal{M}$, and $t \in \mathbb{N}$, $\mathbf{S}'(i, m, t, j) \doteq \mathbf{S}_i(m, t, j)$. Let $(sk_1, pk_1) \leftarrow \mathtt{Gen}$, …, $(sk_n, pk_n) \leftarrow \mathtt{Gen}$. Then:

– $[\![(\!|\mathbf{E}_{pk_1,\ldots,pk_n}, *, *|\!) \triangleright (\!|\mathbf{R}^*, *|\!) \triangleright \mathbf{D}_{sk_1,\ldots,sk_n}, \boldsymbol{pk}_{pk_1,\ldots,pk_n}]\!]$
$\equiv \rho([\![(\!|\mathbf{E}_{pk_1}, *, *|\!) \triangleright (\!|\mathbf{R}^*, *|\!) \triangleright \mathbf{D}_{sk_1,\ldots,sk_n}, \ldots,$
$(\!|\mathbf{E}_{pk_n}, *, *|\!) \triangleright (\!|\mathbf{R}^*, *|\!) \triangleright \mathbf{D}_{sk_1,\ldots,sk_n}, pk_1, \ldots, pk_n]\!])$.

– $[\![\mathbf{I}_n, \boldsymbol{pk}_{pk_1,\ldots,pk_n}]\!] \equiv \rho([\![\langle (\!|*, *|\!)_1, \underbrace{(\!|\bot, *|\!)_1, \ldots, (\!|\bot, *|\!)_1}_{n-1 \text{ times}}\rangle_*,$
$\langle (\!|\bot, *|\!)_1, (\!|*, *|\!)_1, \underbrace{(\!|\bot, *|\!)_1, \ldots, (\!|\bot, *|\!)_1}_{n-2 \text{ times}}\rangle_*, \ldots,$
$\langle \underbrace{(\!|\bot, *|\!)_1, \ldots, (\!|\bot, *|\!)_1}_{n-1 \text{ times}}, (\!|*, *|\!)_1\rangle_*, pk_1, \ldots, pk_n]\!])$.

For $i \in [n]$ and $j \in \{i+1, \ldots, n\}$, also let

$$
\begin{aligned}
\rho_{i,j}([\![\mathbf{S}, \mathbf{T}, x, y]\!]) \doteq [\![&\mathbf{H}_1, \ldots, \mathbf{H}_{i-1}, \mathbf{S}, \mathbf{H}_{i+1}, \ldots, \mathbf{H}_{j-1}, \mathbf{T}, \mathbf{H}_{j+1}, \ldots, \mathbf{H}_n, \\
&pk_1, \ldots, pk_{i-1}, x, pk_{i+1}, \ldots, pk_{j-1}, y, pk_{j+1}, \ldots, pk_n]\!],
\end{aligned}
$$

where $\mathbf{H}^{i,j}_\ell$ is the hybrid system that on input $(i', m, t, j') \in [n] \times \mathcal{M} \times \mathbb{N} \times [n]$:

– If $(i', j') \leq_{\text{lex}} (i, j)$: If $i' = j'$, output m, otherwise output $\bot$.
– Otherwise: Output $\texttt{Dec}_{sk_{j'}}(\texttt{Rnc}^t(\texttt{Enc}_{pk_{i'}}(m)))$.

($\leq_{\text{lex}}$ is the lexicographic order on $[n]^2$.) Clearly,

– $\rho \circ \rho_{1,1}(\llbracket (\mathbf{E}_{pk}, *, *) \triangleright (\mathbf{R}^*, *) \triangleright \mathbf{D}_{sk,sk'}, (\mathbf{E}_{pk'}, *, *) \triangleright (\mathbf{R}^*, *) \triangleright \mathbf{D}_{sk,sk'}, pk, pk' \rrbracket)$
$\equiv \llbracket (\mathbf{E}_{pk_1,\ldots,pk_n}, *, *) \triangleright (\mathbf{R}^*, *) \triangleright \mathbf{D}_{sk_1,\ldots,sk_n}, \boldsymbol{pk}_{pk_1,\ldots,pk_n} \rrbracket$,
– $\rho \circ \rho_{n,n}(\llbracket \langle (*, *)_1, (\bot, *)_1 \rangle_*, \langle (\bot, *)_1, (*, *)_1 \rangle_*, pk, pk' \rrbracket) \equiv \llbracket \mathbf{I}_n, \boldsymbol{pk}_{pk_1,\ldots,pk_n} \rrbracket$,
– $\rho_{k,\ell+1}(\llbracket (\mathbf{E}_{pk}, *, *) \triangleright (\mathbf{R}^*, *) \triangleright \mathbf{D}_{sk,sk'}, (\mathbf{E}_{pk'}, *, *) \triangleright (\mathbf{R}^*, *) \triangleright \mathbf{D}_{sk,sk'}, pk, pk' \rrbracket)$
$\equiv \rho_{k,\ell}(\llbracket \langle (*, *)_1, (\bot, *)_1 \rangle_*, \langle (\bot, *)_1, (*, *)_1 \rangle_*, pk, pk' \rrbracket)$,
for all $k \in [n-1]$, $\ell \in \{k, \ldots, n-1\}$, and
– $\rho_{k,n}(\llbracket (\mathbf{E}_{pk}, *, *) \triangleright (\mathbf{R}^*, *) \triangleright \mathbf{D}_{sk,sk'}, (\mathbf{E}_{pk'}, *, *) \triangleright (\mathbf{R}^*, *) \triangleright \mathbf{D}_{sk,sk'}, pk, pk' \rrbracket)$
$\equiv \rho_{k+1,k+2}(\llbracket \langle (*, *)_1, (\bot, *)_1 \rangle_*, \langle (\bot, *)_1, (*, *)_1 \rangle_*, pk, pk' \rrbracket)$,
for all $k \in [n-2]$.

Therefore, by the discussion in Section 3.4, this implies

$$\llbracket (\mathbf{E}_{pk_1,\ldots,pk_n}, *, *) \triangleright (\mathbf{R}^*, *) \triangleright \mathbf{D}_{sk_1,\ldots,sk_n}, \boldsymbol{pk}_{pk_1,\ldots,pk_n} \rrbracket \simeq \llbracket \mathbf{I}_n, \boldsymbol{pk}_{pk_1,\ldots,pk_n} \rrbracket. \quad \square$$

Lemma 23. $\mathsf{ind\text{-}ik\text{-}ulk\text{-}cpa} \implies \mathcal{R}\text{-}\mathsf{ind\text{-}ik\text{-}ulk\text{-}cpa}$.

Proof. Let $\rho(\llbracket \mathbf{S}_1, \ldots, \mathbf{S}_n, x_1, \ldots, x_n \rrbracket) \doteq \llbracket \mathbf{S}', \boldsymbol{pk}_{x_1,\ldots,x_n} \rrbracket$, where for $i \in [n]$, $\mathbf{S}'(m, i) \doteq \mathbf{S}_i(m)$. Let $(sk_1, pk_1) \leftarrow \texttt{Gen}$, …, $(sk_n, pk_n) \leftarrow \texttt{Gen}$. Then:

– $\llbracket \mathbf{E}_{pk_1,\ldots,pk_n} \triangleright \langle *, \mathbf{R} \rangle, \boldsymbol{pk}_{pk_1,\ldots,pk_n} \rrbracket$
$\equiv \rho(\llbracket \mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R} \rangle, \ldots, \mathbf{E}_{pk_n} \triangleright \langle *, \mathbf{R} \rangle, pk_1, \ldots, pk_n \rrbracket)$.
– $\llbracket (*, *)_1 \triangleright \langle \mathbf{E}^\$_{pk_1}, \mathbf{E}^\$_{pk_1} \triangleright \mathbf{R} \rangle, \boldsymbol{pk}_{pk_1,\ldots,pk_n} \rrbracket$
$\equiv \rho(\llbracket \langle \mathbf{E}^\$_{pk_1}, \mathbf{E}^\$_{pk_1} \triangleright \mathbf{R} \rangle, \ldots, \langle \mathbf{E}^\$_{pk_1}, \mathbf{E}^\$_{pk_1} \triangleright \mathbf{R} \rangle, pk_1, \ldots, pk_n \rrbracket)$.

For $i \in [n]$, also let

$$\begin{aligned} \rho_i(\llbracket \mathbf{S}, x \rrbracket) \doteq \llbracket & \underbrace{\langle \mathbf{E}^\$_{pk_1}, \mathbf{E}^\$_{pk_1} \triangleright \mathbf{R} \rangle, \ldots, \langle \mathbf{E}^\$_{pk_1}, \mathbf{E}^\$_{pk_1} \triangleright \mathbf{R} \rangle}_{i-1 \text{ times}}, \mathbf{S}, \\ & \mathbf{E}_{pk_{i+1}} \triangleright \langle *, \mathbf{R} \rangle, \ldots, \mathbf{E}_{pk_n} \triangleright \langle *, \mathbf{R} \rangle, \\ & pk_1, \ldots, pk_{i-1}, x, pk_{i+1}, \ldots, pk_n \rrbracket. \end{aligned}$$

Clearly,

– $\rho \circ \rho_1(\llbracket \mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R} \rangle, pk_1 \rrbracket) \equiv \llbracket \mathbf{E}_{pk_1,\ldots,pk_n} \triangleright \langle *, \mathbf{R} \rangle, \boldsymbol{pk}_{pk_1,\ldots,pk_n} \rrbracket$,
– $\rho \circ \rho_n(\llbracket \langle \mathbf{E}^\$_{pk_1}, \mathbf{E}^\$_{pk_1} \triangleright \mathbf{R} \rangle, pk_1 \rrbracket) \equiv \llbracket (*, *)_1 \triangleright \langle \mathbf{E}^\$_{pk_1}, \mathbf{E}^\$_{pk_1} \triangleright \mathbf{R} \rangle, \boldsymbol{pk}_{pk_1,\ldots,pk_n} \rrbracket$, and
– $\rho_j(\llbracket \langle \mathbf{E}^\$_{pk_1}, \mathbf{E}^\$_{pk_1} \triangleright \mathbf{R} \rangle, pk \rrbracket) \equiv \rho_{j+1}(\llbracket \mathbf{E}_{pk_{j+1}} \triangleright \langle *, \mathbf{R} \rangle, pk_{j+1} \rrbracket)$, for all $j \in [n-1]$.

Therefore, by the discussion in Section 3.4, this implies

$$\llbracket \mathbf{E}_{pk_1,\ldots,pk_n} \triangleright \langle *, \mathbf{R} \rangle, \boldsymbol{pk}_{pk_1,\ldots,pk_n} \rrbracket \simeq \llbracket (*, *)_1 \triangleright \langle \mathbf{E}^\$_{pk_1}, \mathbf{E}^\$_{pk_1} \triangleright \mathbf{R} \rangle, \boldsymbol{pk}_{pk_1,\ldots,pk_n} \rrbracket. \quad \square$$

Lemma 24. $\mathsf{ind\text{-}ik\text{-}sulk\text{-}cpa} \implies \mathcal{R}\text{-}\mathsf{ind\text{-}ik\text{-}sulk\text{-}cpa}$.

Proof. As for Lemma 23, but with

$$\begin{aligned}\rho_i(\llbracket \mathbf{S}, x \rrbracket) \doteq \llbracket &\underbrace{\langle \mathbf{E}^{\$}_{pk_1}, \mathbf{E}^{\$}_{pk_1} \rangle, \dots, \langle \mathbf{E}^{\$}_{pk_1}, \mathbf{E}^{\$}_{pk_1} \rangle}_{i-1 \text{ times}}, \mathbf{S}, \\ &\mathbf{E}_{pk_{i+1}} \triangleright \langle *, \mathbf{R} \rangle, \dots, \mathbf{E}_{pk_n} \triangleright \langle *, \mathbf{R} \rangle, \\ &pk_1, \dots, pk_{i-1}, x, pk_{i+1}, \dots, pk_n \rrbracket. \end{aligned}$$ □

B 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 Young and Yung's Notions

Definition 32 (lor-ind-cpa)**.**

$$\llbracket (\!| *, * |\!)_1 \triangleright \mathbf{E}_{pk}, pk \rrbracket \simeq \llbracket (\!| *, * |\!)_2 \triangleright \mathbf{E}_{pk}, pk \rrbracket,$$

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

Definition 33 (lor-ik-cpa)**.**

$$\llbracket \mathbf{E}_{pk_1}, pk_1, pk_2 \rrbracket \simeq \llbracket \mathbf{E}_{pk_2}, pk_1, pk_2 \rrbracket,$$

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

Definition 34 (lor-ind-r-cpa)**.**

$$\llbracket (\!| \mathbf{E}_{pk} \triangleright \langle *, \mathbf{R} \rangle, \mathbf{E}_{pk} |\!), pk \rrbracket \simeq \llbracket (\!| \mathbf{E}_{pk}, \mathbf{E}_{pk} \triangleright \langle \mathbf{R}, * \rangle |\!), pk \rrbracket,$$

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

Definition 35 (lor-ik-r-cpa)**.**

$$\llbracket \langle \mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R} \rangle, \mathbf{E}_{pk_2} \rangle, pk_1, pk_2 \rrbracket \simeq \llbracket \langle \mathbf{E}_{pk_1}, \mathbf{E}_{pk_2} \triangleright \langle \mathbf{R}, * \rangle \rangle, pk_1, pk_2 \rrbracket,$$

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

B.2 Equivalence of the Notions

Lemma 25. lor-ind-cpa $\iff$ ind-cpa.

Proof.

$\Longrightarrow$: Let $(sk, pk) \leftarrow \texttt{Gen}$ and consider $\rho(\llbracket \mathbf{S}, x \rrbracket) \doteq \llbracket \langle *, \$ \rangle \triangleright \mathbf{S}, x \rrbracket$. Then:

$$\begin{aligned}
\llbracket \mathbf{E}_{pk}, pk \rrbracket &\equiv \llbracket \langle *, \$ \rangle \triangleright (\!| *, * |\!)_1 \triangleright \mathbf{E}_{pk}, pk \rrbracket \\
&= \rho(\llbracket (\!| *, * |\!)_1 \triangleright \mathbf{E}_{pk}, pk \rrbracket) \\
&\simeq \rho(\llbracket (\!| *, * |\!)_2 \triangleright \mathbf{E}_{pk}, pk \rrbracket) && \text{(lor-ind-cpa)} \\
&= \llbracket \langle *, \$ \rangle \triangleright (\!| *, * |\!)_2 \triangleright \mathbf{E}_{pk}, pk \rrbracket \\
&\equiv \llbracket \mathbf{E}^{\$}_{pk}, pk \rrbracket.
\end{aligned}$$

$\Longleftarrow$: Let $(sk, pk) \leftarrow \texttt{Gen}$ and consider $\rho_i(\llbracket \mathbf{S}, x \rrbracket) \doteq \llbracket (\!| *, * |\!)_i \triangleright \mathbf{S}, x \rrbracket$, for $i \in \{1, 2\}$. Then:

$$\begin{aligned}
\llbracket (\!| *, * |\!)_1 \triangleright \mathbf{E}_{pk}, pk \rrbracket &= \rho_1(\llbracket \mathbf{E}_{pk}, pk \rrbracket) \\
&\simeq \rho_1(\llbracket \mathbf{E}^{\$}_{pk}, pk \rrbracket) && \text{(ind-cpa)} \\
&= \llbracket (\!| *, * |\!)_1 \triangleright \mathbf{E}^{\$}_{pk}, pk \rrbracket \\
&\equiv \llbracket (\!| *, * |\!)_2 \triangleright \mathbf{E}^{\$}_{pk}, pk \rrbracket \\
&= \rho_2(\llbracket \mathbf{E}^{\$}_{pk}, pk \rrbracket) \\
&\simeq \rho_2(\llbracket \mathbf{E}_{pk}, pk \rrbracket) && \text{(ind-cpa)} \\
&\equiv \llbracket (\!| *, * |\!)_2 \triangleright \mathbf{E}_{pk}, pk \rrbracket.
\end{aligned}$$

□

Lemma 26. lor-ik-cpa $\iff$ ik-cpa.

Proof.

$\Longrightarrow$: Let $(sk_1, pk_1) \leftarrow \texttt{Gen}$ and $(sk_2, pk_2) \leftarrow \texttt{Gen}$, and consider $\rho(\llbracket \mathbf{S}, x, y \rrbracket) \doteq \llbracket \mathbf{E}_x, \mathbf{S}, x, y \rrbracket$. Then:

$$\begin{aligned}
\llbracket \mathbf{E}_{pk_1}, \mathbf{E}_{pk_2}, pk_1, pk_2 \rrbracket &= \rho(\llbracket \mathbf{E}_{pk_2}, pk_1, pk_2 \rrbracket) \\
&\simeq \rho(\llbracket \mathbf{E}_{pk_1}, pk_1, pk_2 \rrbracket) && \text{(lor-ik-cpa)} \\
&= \llbracket \mathbf{E}_{pk_1}, \mathbf{E}_{pk_1}, pk_1, pk_2 \rrbracket.
\end{aligned}$$

$\Longleftarrow$: Let $(sk_1, pk_1) \leftarrow \texttt{Gen}$ and $(sk_2, pk_2) \leftarrow \texttt{Gen}$, and consider $\rho(\llbracket \mathbf{S}, \mathbf{T}, x, y \rrbracket) \doteq \llbracket \mathbf{T}, x, y \rrbracket$. Then:

$$\begin{aligned}
\llbracket \mathbf{E}_{pk_1}, pk_1, pk_2 \rrbracket &= \rho(\llbracket \mathbf{E}_{pk_1}, \mathbf{E}_{pk_1}, pk_1, pk_2 \rrbracket) \\
&\simeq \rho(\llbracket \mathbf{E}_{pk_1}, \mathbf{E}_{pk_2}, pk_1, pk_2 \rrbracket) && \text{(ik-cpa)} \\
&= \llbracket \mathbf{E}_{pk_2}, pk_1, pk_2 \rrbracket.
\end{aligned}$$

□

Lemma 27. lor-ind-r-cpa $\iff$ ind-r-cpa.

Proof.

$\Longrightarrow$: Let $(sk, pk) \leftarrow \texttt{Gen}$ and consider $\rho(\llbracket \mathbf{S}, x \rrbracket) \doteq \llbracket \langle *, \$ \rangle \triangleright (\mathbf{S})_{1,2}, x \rrbracket$. Then:

$$\begin{aligned}
\llbracket \mathbf{E}_{pk} \triangleright \langle *, \mathbf{R} \rangle, pk \rrbracket &\equiv \llbracket \langle *, \$ \rangle \triangleright (\!| \mathbf{E}_{pk} \triangleright \langle *, \mathbf{R} \rangle, \mathbf{E}_{pk} |\!)_{1,2}, pk \rrbracket \\
&= \rho(\llbracket (\!| \mathbf{E}_{pk} \triangleright \langle *, \mathbf{R} \rangle, \mathbf{E}_{pk} |\!), pk \rrbracket) \\
&\simeq \rho(\llbracket (\!| \mathbf{E}_{pk}, \mathbf{E}_{pk} \triangleright \langle \mathbf{R}, * \rangle |\!), pk \rrbracket) \qquad \text{(lor-ind-r-cpa)} \\
&= \llbracket \langle *, \$ \rangle \triangleright (\!| \mathbf{E}_{pk}, \mathbf{E}_{pk} \triangleright \langle \mathbf{R}, * \rangle |\!)_{1,2}, pk \rrbracket \\
&\equiv \llbracket \langle \mathbf{E}_{pk}, \mathbf{E}^{\$}_{pk} \triangleright \mathbf{R} \rangle, pk \rrbracket.
\end{aligned}$$

$\Longleftarrow$: Let $(sk, pk) \leftarrow \texttt{Gen}$ and consider $\rho_1(\llbracket \mathbf{S}, x \rrbracket) \doteq \llbracket (\!| \mathbf{S}, \mathbf{E}_x |\!), x \rrbracket$ and $\rho_2(\llbracket \mathbf{S}, x \rrbracket) \doteq \llbracket (\!| \mathbf{E}_x, (\mathbf{S})_{2,1} |\!), x \rrbracket$. Then:

$$\begin{aligned}
\llbracket (\!| \mathbf{E}_{pk} \triangleright \langle *, \mathbf{R} \rangle, \mathbf{E}_{pk} |\!), pk \rrbracket &= \rho_1(\llbracket \mathbf{E}_{pk} \triangleright \langle *, \mathbf{R} \rangle, pk \rrbracket) \\
&\simeq \rho_1(\llbracket \langle \mathbf{E}_{pk}, \mathbf{E}^{\$}_{pk} \triangleright \mathbf{R} \rangle, pk \rrbracket) \qquad \text{(ind-r-cpa)} \\
&= \llbracket (\!| \langle \mathbf{E}_{pk}, \mathbf{E}^{\$}_{pk} \triangleright \mathbf{R} \rangle, \mathbf{E}_{pk} |\!), pk \rrbracket \\
&= \llbracket (\!| \mathbf{E}_{pk}, \langle \mathbf{E}^{\$}_{pk} \triangleright \mathbf{R}, \mathbf{E}_{pk} \rangle |\!), pk \rrbracket \\
&\equiv \llbracket (\!| \mathbf{E}_{pk}, \langle \mathbf{E}_{pk}, \mathbf{E}^{\$}_{pk} \triangleright \mathbf{R} \rangle_{2,1} |\!), pk \rrbracket \\
&= \rho_2(\llbracket \langle \mathbf{E}_{pk}, \mathbf{E}^{\$}_{pk} \triangleright \mathbf{R} \rangle, pk \rrbracket) \\
&\simeq \rho_2(\llbracket \mathbf{E}_{pk} \triangleright \langle *, \mathbf{R} \rangle, pk \rrbracket) \qquad \text{(ind-r-cpa)} \\
&= \llbracket (\!| \mathbf{E}_{pk}, (\mathbf{E}_{pk} \triangleright \langle *, \mathbf{R} \rangle)_{2,1} |\!), pk \rrbracket \\
&\equiv \llbracket (\!| \mathbf{E}_{pk}, \mathbf{E}_{pk} \triangleright \langle \mathbf{R}, * \rangle |\!), pk \rrbracket.
\end{aligned}$$

□

Lemma 28. lor-ik-r-cpa $\Longleftrightarrow$ ik-r-cpa.

Proof.

$\Longrightarrow$: Let $(sk_1, pk_1) \leftarrow \texttt{Gen}$ and $(sk_2, pk_2) \leftarrow \texttt{Gen}$, and consider $\rho(\llbracket \mathbf{S}, x, y \rrbracket) \doteq \llbracket \mathbf{E}_x \triangleright \langle *, \mathbf{R} \rangle, (\mathbf{S})_{3,2}, x, y \rrbracket$. Then:

$$\begin{aligned}
&\llbracket \mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R} \rangle, \mathbf{E}_{pk_2} \triangleright \langle *, \mathbf{R} \rangle, pk_1, pk_2 \rrbracket \\
&\quad \equiv \llbracket \mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R} \rangle, \langle \mathbf{E}_{pk_1}, \mathbf{E}_{pk_2} \triangleright \langle \mathbf{R}, * \rangle \rangle_{3,2}, pk_1, pk_2 \rrbracket \\
&\quad = \rho(\llbracket \langle \mathbf{E}_{pk_1}, \mathbf{E}_{pk_2} \triangleright \langle \mathbf{R}, * \rangle \rangle, pk_1, pk_2 \rrbracket) \\
&\quad \simeq \rho(\llbracket \langle \mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R} \rangle, \mathbf{E}_{pk_2} \rangle, pk_1, pk_2 \rrbracket) \qquad \text{(lor-ik-r-cpa)} \\
&\quad = \llbracket \mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R} \rangle, \langle \mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R} \rangle, \mathbf{E}_{pk_2} \rangle_{3,2}, pk_1, pk_2 \rrbracket \\
&\quad \equiv \llbracket \mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R} \rangle, \langle \mathbf{E}_{pk_2}, \mathbf{E}_{pk_1} \triangleright \mathbf{R} \rangle, pk_1, pk_2 \rrbracket.
\end{aligned}$$

$\Longleftarrow$: Note that, by Lemma 7, ik-r-cpa $\Longrightarrow$ ulk-cpa. Therefore, we can use

$$\llbracket \langle \mathbf{E}_{pk_2}, \mathbf{E}_{pk_2} \triangleright \mathbf{R} \rangle, pk_2 \rrbracket \simeq \llbracket \mathbf{E}_{pk_2} \triangleright \langle *, \mathbf{R} \rangle, pk_2 \rrbracket.$$

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

- $\rho_1(\llbracket \mathbf{S}, \mathbf{T}, x, y \rrbracket) \doteq \llbracket \langle \mathbf{T}, \mathbf{E}_x \rangle, y, x \rrbracket$ and

- $\rho_2(\llbracket \mathbf{S}, x \rrbracket) \doteq \llbracket \langle \mathbf{E}_{pk_1}, (\mathbf{S})_{2,1} \rangle, pk_1, x \rangle \rrbracket$.

Then:

$$
\begin{aligned}
&\llbracket \langle \mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R} \rangle, \mathbf{E}_{pk_2} \rangle, pk_1, pk_2 \rrbracket \\
&\qquad = \rho_1(\llbracket \mathbf{E}_{pk_2} \triangleright \langle *, \mathbf{R} \rangle, \mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R} \rangle, pk_2, pk_1 \rrbracket) \\
&\qquad \hat{=} \rho_1(\llbracket \mathbf{E}_{pk_2} \triangleright \langle *, \mathbf{R} \rangle, \langle \mathbf{E}_{pk_1}, \mathbf{E}_{pk_2} \triangleright \mathbf{R} \rangle, pk_2, pk_1 \rrbracket) && (\textsf{ik-r-cpa}) \\
&\qquad = \llbracket \langle \langle \mathbf{E}_{pk_1}, \mathbf{E}_{pk_2} \triangleright \mathbf{R} \rangle, \mathbf{E}_{pk_2} \rangle, pk_1, pk_2 \rrbracket \\
&\qquad \equiv \llbracket \langle \mathbf{E}_{pk_1}, \langle \mathbf{E}_{pk_2} \triangleright \mathbf{R}, \mathbf{E}_{pk_2} \rangle \rangle, pk_1, pk_2 \rrbracket \\
&\qquad \equiv \llbracket \langle \mathbf{E}_{pk_1}, \langle \mathbf{E}_{pk_2}, \mathbf{E}_{pk_2} \triangleright \mathbf{R} \rangle_{2,1} \rangle, pk_1, pk_2 \rrbracket \\
&\qquad = \rho_2(\llbracket \langle \mathbf{E}_{pk_2}, \mathbf{E}_{pk_2} \triangleright \mathbf{R} \rangle, pk_2 \rrbracket) \\
&\qquad \hat{=} \rho_2(\llbracket \mathbf{E}_{pk_2} \triangleright \langle *, \mathbf{R} \rangle, pk_2 \rrbracket) && (\textsf{ulk-cpa}) \\
&\qquad = \llbracket \langle \mathbf{E}_{pk_1}, (\mathbf{E}_{pk_2} \triangleright \langle *, \mathbf{R} \rangle)_{2,1} \rangle, pk_1, pk_2 \rrbracket \\
&\qquad = \llbracket \langle \mathbf{E}_{pk_1}, \mathbf{E}_{pk_2} \triangleright \langle \mathbf{R}, * \rangle \rangle, pk_1, pk_2 \rrbracket. && \square
\end{aligned}
$$

C Variant of All-in-One 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 6. Nevertheless, ind-ik-r-cpa is less directly relatable to our composable notions than ind-ik-ulk-cpa.

Definition 36 (ind-ik-cpa)**.**

$$\llbracket \mathbf{E}_{pk_1}, \mathbf{E}_{pk_2}, pk_1, pk_2 \rrbracket \hat{=} \llbracket \mathbf{E}^{\$}_{pk_1}, \mathbf{E}^{\$}_{pk_1}, pk_1, pk_2 \rrbracket,$$

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

Definition 37 (ind-ik-r-cpa)**.**

$$
\begin{gathered}
\llbracket \mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R} \rangle, \mathbf{E}_{pk_2} \triangleright \langle *, \mathbf{R} \rangle, pk_1, pk_2 \rrbracket \\
\hat{=} \\
\llbracket \langle \mathbf{E}_{pk_1}, \mathbf{E}^{\$}_{pk_1} \triangleright \mathbf{R} \rangle, \langle \mathbf{E}_{pk_2}, \mathbf{E}^{\$}_{pk_1} \triangleright \mathbf{R} \rangle, pk_1, pk_2 \rrbracket,
\end{gathered}
$$

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

Lemma 29. ind-cpa $\wedge$ ik-cpa $\iff$ ind-ik-cpa.

Proof.

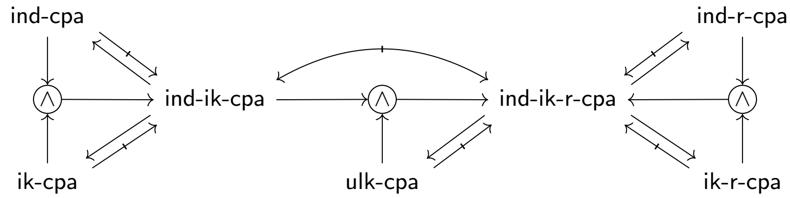


Fig. 6. Relations among ciphertext-indistinguishability, key-indistinguishability, and unlinkability.

- $\Longrightarrow$: Let $(sk_1, pk_1) \leftarrow \texttt{Gen}$ and $(sk_2, pk_2) \leftarrow \texttt{Gen}$, and consider $\rho([\![\mathbf{S}, x]\!]) \doteq [\![\mathbf{S}, \mathbf{S}, x, pk_2]\!]$. Then:

$$\begin{aligned}
[\![\mathbf{E}_{pk_1}, \mathbf{E}_{pk_2}, pk_1, pk_2]\!] &\simeq [\![\mathbf{E}_{pk_1}, \mathbf{E}_{pk_1}, pk_1, pk_2]\!] && (\textsf{ik-cpa}) \\
&= \rho([\![\mathbf{E}_{pk_1}, pk_1]\!]) \\
&\simeq \rho([\![\mathbf{E}^{\$}_{pk_1}, pk_1]\!]) && (\textsf{ind-cpa}) \\
&= [\![\mathbf{E}^{\$}_{pk_1}, \mathbf{E}^{\$}_{pk_1}, pk_1, pk_2]\!].
\end{aligned}$$

- $\Longleftarrow$: Let $(sk, pk) \leftarrow \texttt{Gen}$ and $(sk', pk') \leftarrow \texttt{Gen}$, and consider $\rho([\![\mathbf{S}, \mathbf{T}, x, y]\!]) \doteq [\![\mathbf{S}, x]\!]$. Then:

$$\begin{aligned}
[\![\mathbf{E}_{pk}, pk]\!] &= \rho([\![\mathbf{E}_{pk}, \mathbf{E}_{pk'}, pk, pk']\!]) \\
&\simeq \rho([\![\mathbf{E}^{\$}_{pk}, \mathbf{E}^{\$}_{pk}, pk, pk']\!]) && (\textsf{ind-ik-cpa}) \\
&= [\![\mathbf{E}^{\$}_{pk}, pk]\!].
\end{aligned}$$

  Let $(sk_1, pk_1) \leftarrow \texttt{Gen}$ and $(sk_2, pk_2) \leftarrow \texttt{Gen}$, and consider $\rho_i([\![\mathbf{S}_1, \mathbf{S}_2, x, y]\!]) \doteq [\![\mathbf{E}_x, \mathbf{S}_{1-i}, x, y]\!]$, for $i \in \{1, 2\}$. Then:

$$\begin{aligned}
[\![\mathbf{E}_{pk_1}, \mathbf{E}_{pk_2}, pk_1, pk_2]\!] &= \rho_1([\![\mathbf{E}_{pk_1}, \mathbf{E}_{pk_2}, pk_1, pk_2]\!]) \\
&\simeq \rho_1([\![\mathbf{E}^{\$}_{pk_1}, \mathbf{E}^{\$}_{pk_1}, pk_1, pk_2]\!]) && (\textsf{ind-ik-cpa}) \\
&= [\![\mathbf{E}_{pk_1}, \mathbf{E}^{\$}_{pk_1}, pk_1, pk_2]\!] \\
&= \rho_2([\![\mathbf{E}^{\$}_{pk_1}, \mathbf{E}^{\$}_{pk_1}, pk_1, pk_2]\!]) \\
&\simeq \rho_2([\![\mathbf{E}_{pk_1}, \mathbf{E}_{pk_2}, pk_1, pk_2]\!]) && (\textsf{ind-ik-cpa}) \\
&= [\![\mathbf{E}_{pk_1}, \mathbf{E}_{pk_1}, pk_1, pk_2]\!]. && \square
\end{aligned}$$

Lemma 30. $\textsf{ind-cpa} \;\not\Longrightarrow\; \textsf{ind-ik-cpa}$.

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

- $\texttt{Gen}' \doteq \texttt{Gen}$;
- $\texttt{Enc}'_{pk}(m) \doteq (\texttt{Enc}_{pk}(m), pk)$, 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 $(c, pk') \in \mathcal{C} \times \mathcal{PK}$.

Let $(sk, pk) \leftarrow \mathtt{Gen}$. If Π is correct, then Π' is clearly also correct, and if

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

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

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

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

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

□

Lemma 31. ik-cpa $\not\Rightarrow$ 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 $(c, m) \in \mathcal{C} \times \mathcal{M}$.

If Π is correct, then Π' is clearly also correct, and if

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

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

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

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

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

□

Lemma 32. $\mathsf{ind\text{-}r\text{-}cpa} \wedge \mathsf{ik\text{-}r\text{-}cpa} \iff \mathsf{ind\text{-}ik\text{-}r\text{-}cpa}$.

Proof.

$\Longrightarrow$: Let $(sk_1, pk_1) \leftarrow \texttt{Gen}$ and $(sk_2, pk_2) \leftarrow \texttt{Gen}$, and consider $\rho([\![\mathbf{S}, x]\!]) \doteq [\![\mathbf{S}, \langle \mathbf{E}_{pk_2}, (\mathbf{S})_2 \rangle, x, pk_2]\!]$. Then:

$$\begin{aligned}
&[\![\mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R}\rangle, \mathbf{E}_{pk_2} \triangleright \langle *, \mathbf{R}\rangle, pk_1, pk_2]\!] \\
&\quad \simeq [\![\mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R}\rangle, \langle \mathbf{E}_{pk_2}, \mathbf{E}_{pk_1} \triangleright \mathbf{R}\rangle, pk_1, pk_2]\!] && (\mathsf{ik\text{-}r\text{-}cpa}) \\
&\quad \equiv [\![\mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R}\rangle, \langle \mathbf{E}_{pk_2}, (\mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R}\rangle)_2\rangle, pk_1, pk_2]\!] \\
&\quad = \rho([\![\mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R}\rangle, pk_1]\!]) \\
&\quad \simeq \rho([\![\langle \mathbf{E}_{pk_1}, \mathbf{E}^{\$}_{pk_1} \triangleright \mathbf{R}\rangle, pk_1]\!]) && (\mathsf{ind\text{-}r\text{-}cpa}) \\
&\quad = [\![\langle \mathbf{E}_{pk_1}, \mathbf{E}^{\$}_{pk_1} \triangleright \mathbf{R}\rangle, \langle \mathbf{E}_{pk_2}, \langle \mathbf{E}_{pk_1}, \mathbf{E}^{\$}_{pk_1} \triangleright \mathbf{R}\rangle_2\rangle, pk_1, pk_2]\!] \\
&\quad \equiv [\![\langle \mathbf{E}_{pk_1}, \mathbf{E}^{\$}_{pk_1} \triangleright \mathbf{R}\rangle, \langle \mathbf{E}_{pk_2}, \mathbf{E}^{\$}_{pk_1} \triangleright \mathbf{R}\rangle, pk_1, pk_2]\!].
\end{aligned}$$

$\Longleftarrow$: Let $(sk, pk) \leftarrow \texttt{Gen}$ and $(sk', pk') \leftarrow \texttt{Gen}$, and consider $\rho([\![\mathbf{S}, \mathbf{T}, x, y]\!]) \doteq [\![\mathbf{S}, x]\!]$. Then:

$$\begin{aligned}
[\![\mathbf{E}_{pk} \triangleright \langle *, \mathbf{R}\rangle, pk]\!] &= \rho([\![\mathbf{E}_{pk} \triangleright \langle *, \mathbf{R}\rangle, \mathbf{E}_{pk'} \triangleright \langle *, \mathbf{R}\rangle, pk, pk']\!]) \\
&\simeq \rho([\![\langle \mathbf{E}_{pk}, \mathbf{E}^{\$}_{pk} \triangleright \mathbf{R}\rangle, \langle \mathbf{E}_{pk'}, \mathbf{E}^{\$}_{pk} \triangleright \mathbf{R}\rangle, pk, pk']\!]) && (\mathsf{ind\text{-}ik\text{-}r\text{-}cpa}) \\
&= [\![\langle \mathbf{E}_{pk}, \mathbf{E}^{\$}_{pk} \triangleright \mathbf{R}\rangle, pk]\!].
\end{aligned}$$

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

- $\rho_1([\![\mathbf{S}, \mathbf{T}, x, y]\!]) \doteq [\![\mathbf{E}_x \triangleright \langle *, \mathbf{R}\rangle, \mathbf{T}, x, y]\!]$ and
- $\rho_2([\![\mathbf{S}, \mathbf{T}, x, y]\!]) \doteq [\![\mathbf{E}_x \triangleright \langle *, \mathbf{R}\rangle, \langle \mathbf{E}_y, (\mathbf{S})_2\rangle, x, y]\!]$.

Then:

$$\begin{aligned}
&[\![\mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R}\rangle, \mathbf{E}_{pk_2} \triangleright \langle *, \mathbf{R}\rangle, pk_1, pk_2]\!] \\
&\quad = \rho_1([\![\mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R}\rangle, \mathbf{E}_{pk_2} \triangleright \langle *, \mathbf{R}\rangle, pk_1, pk_2]\!]) \\
&\quad \simeq \rho_1([\![\langle \mathbf{E}_{pk_1}, \mathbf{E}^{\$}_{pk_1} \triangleright \mathbf{R}\rangle, \langle \mathbf{E}_{pk_2}, \mathbf{E}^{\$}_{pk_1} \triangleright \mathbf{R}\rangle, pk_1, pk_2]\!]) && (\mathsf{ind\text{-}ik\text{-}r\text{-}cpa}) \\
&\quad = [\![\mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R}\rangle, \langle \mathbf{E}_{pk_2}, \mathbf{E}^{\$}_{pk_1} \triangleright \mathbf{R}\rangle, pk_1, pk_2]\!] \\
&\quad \equiv [\![\mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R}\rangle, \langle \mathbf{E}_{pk_2}, \langle \mathbf{E}_{pk_1}, \mathbf{E}^{\$}_{pk_1} \triangleright \mathbf{R}\rangle_2\rangle, pk_1, pk_2]\!] \\
&\quad = \rho_2([\![\langle \mathbf{E}_{pk_1}, \mathbf{E}^{\$}_{pk_1} \triangleright \mathbf{R}\rangle, \langle \mathbf{E}_{pk_2}, \mathbf{E}^{\$}_{pk_1} \triangleright \mathbf{R}\rangle, pk_1, pk_2]\!]) \\
&\quad \simeq \rho_2([\![\mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R}\rangle, \mathbf{E}_{pk_2} \triangleright \langle *, \mathbf{R}\rangle, pk_1, pk_2]\!]) && (\mathsf{ind\text{-}ik\text{-}r\text{-}cpa}) \\
&\quad \equiv [\![\mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R}\rangle, \langle \mathbf{E}_{pk_2}, (\mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R}\rangle)_2\rangle, pk_1, pk_2]\!] \\
&\quad = [\![\mathbf{E}_{pk_1} \triangleright \langle *, \mathbf{R}\rangle, \langle \mathbf{E}_{pk_2}, \mathbf{E}_{pk_1} \triangleright \mathbf{R}\rangle, pk_1, pk_2]\!].
\end{aligned}$$

□

Lemma 33. $\mathsf{ind\text{-}r\text{-}cpa} \;\not\Longrightarrow\; \mathsf{ind\text{-}ik\text{-}r\text{-}cpa}$.

Proof. Analogous to the proof of Lemma 30. □

Lemma 34. $\mathsf{ik\text{-}r\text{-}cpa} \;\not\Longrightarrow\; \mathsf{ind\text{-}ik\text{-}r\text{-}cpa}$.

Proof. Analogous to the proof of Lemma 31. □

Lemma 35. $\mathsf{ind\text{-}ik\text{-}cpa} \wedge \mathsf{ulk\text{-}cpa} \implies \mathsf{ind\text{-}ik\text{-}r\text{-}cpa}$.

Proof. Analogous to the proof of Lemma 5. □

Lemma 36. $\mathsf{ind\text{-}ik\text{-}cpa} \not\Longleftrightarrow \mathsf{ind\text{-}ik\text{-}r\text{-}cpa}$.

Proof. Analogous to the proofs of both Lemma 2 and Lemma 6. □

Lemma 37. $\mathsf{ind\text{-}ik\text{-}r\text{-}cpa} \implies \mathsf{ulk\text{-}cpa}$.

Proof. Implied by both Lemma 32 + Lemma 3 and Lemma 32 + Lemma 7. □

Lemma 38. $\mathsf{ulk\text{-}cpa} \not\Longrightarrow \mathsf{ind\text{-}ik\text{-}r\text{-}cpa}$.

Proof. By Lemma 32, $\mathsf{ind\text{-}ik\text{-}r\text{-}cpa} \implies \mathsf{ik\text{-}r\text{-}cpa}$, but by Lemma 8, $\mathsf{ulk\text{-}cpa} \not\Longrightarrow \mathsf{ik\text{-}r\text{-}cpa}$, hence $\mathsf{ulk\text{-}cpa} \implies \mathsf{ind\text{-}ik\text{-}cpa}$ would lead to a contradiction. □

D 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 $g \in \mathbb{G}$.

D.1 Decisional Diffie-Hellman Assumption

We can base all results of this paper 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 38 (DDH Systems).

- $\mathbf{S}_0^{\mathsf{ddh}}$*: on input* $\diamond$*, output* $(g^\alpha, g^\beta, g^{\alpha\beta}) \in \mathbb{G}^3$*, for* $\alpha, \beta \xleftarrow{\$} \mathbb{Z}_q$ *(only once).*
- $\mathbf{S}_1^{\mathsf{ddh}}$*: 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 39 (ddh)**.** $\mathbf{S}_0^{\mathsf{ddh}} \simeq \mathbf{S}_1^{\mathsf{ddh}}$.

D.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), 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 40. $\Pi_{\mathsf{URE\text{-}ElGamal}} = (\mathtt{Gen}, \mathtt{Enc}, \mathtt{Rnc}, \mathtt{Dec})$*, with private-key space* $\mathcal{SK} \doteq \mathbb{Z}_q$*, public-key space* $\mathcal{PK} \doteq \mathbb{G}$*, message space*[4] $\mathcal{M} = \mathbb{G}$*, and ciphertext space* $\mathcal{C} \doteq \mathbb{G}^4$*, is defined as follows:*

- $\mathtt{Gen}() \doteq (sk, g^{sk})$*, for* $sk \xleftarrow{\$} \mathbb{Z}_q$.
- $\mathtt{Enc}_{pk}(m) \doteq (m \cdot pk^{\kappa_0}, g^{\kappa_0}, pk^{\kappa_1}, g^{\kappa_1})$*, for* $\kappa_0, \kappa_1 \xleftarrow{\$} \mathbb{Z}_q$.
- $\mathtt{Rnc}((\alpha_0, \beta_0, \alpha_1, \beta_1)) \doteq (\alpha_0\alpha_1^{\kappa_0'}, \beta_0\beta_1^{\kappa_0'}, \alpha_1^{\kappa_1'}, \beta_1^{\kappa_1'})$*, for* $\kappa_0', \kappa_1' \xleftarrow{\$} \mathbb{Z}_q$.
- $\mathtt{Dec}_{sk}((\alpha_0, \beta_0, \alpha_1, \beta_1)) \doteq \begin{cases} \alpha_0/\beta_0^{sk} & \textit{if } \alpha_1/\beta_1^{sk} = 1, \\ \perp & \textit{otherwise.} \end{cases}$

In the following we understand the systems from Definition 6 as being implicitly parameterized on $\Pi_{\mathsf{URE\text{-}ElGamal}}$.

Lemma 39. $\mathsf{cor}^{\Pi_{\mathsf{URE\text{-}ElGamal}}}$ *holds unconditionally.*

Proof. Let $(m,t) \in \mathbb{G} \times \mathbb{N}$. Then, for $\kappa_0^0, \kappa_1^0, \kappa_0^1, \kappa_1^1, \ldots, \kappa_0^t, \kappa_1^t \xleftarrow{\$} \mathbb{Z}_q$, $(sk, pk) \leftarrow \mathtt{Gen}$, $\sigma \doteq \sum_{i=0}^{t} \kappa_0^i \prod_{j=0}^{i-1} \kappa_1^j$, and $\omega \doteq \prod_{i=0}^{t} \kappa_1^i$, on input (m,t) the system $[\![(\mathbf{E}_{pk}, *) \triangleright \mathbf{R}^* \triangleright \mathbf{D}_{sk}, pk]\!]$ 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 40. $\mathsf{rob}^{\Pi_{\mathsf{URE\text{-}ElGamal}}}$ *holds unconditionally with probability* $\frac{1}{q}$.

[4] Note that in Definition 5 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).

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), $(sk_2, pk_2) \leftarrow \texttt{Gen}$, $\sigma \doteq \sum_{i=0}^{t} \kappa_0^i \prod_{j=0}^{i-1} \kappa_1^j$, and $\omega \doteq \prod_{i=0}^{t} \kappa_1^i$, on input (m,t) the system $\llbracket (\mathbf{E}_{pk_1}, *) \triangleright \mathbf{R}^* \triangleright \mathbf{D}_{sk_2}, pk_1, pk_2 \rrbracket$ will output

$$\begin{aligned} \texttt{Dec}_{sk_2}(\texttt{Rnc}^t(\texttt{Enc}_{pk_1}(m))) &= \texttt{Dec}_{sk_2}(\texttt{Rnc}^t((m \cdot pk_1^{\kappa_0}, g^{\kappa_0}, pk_1^{\kappa_1}, g^{\kappa_1}))) \\ &= \texttt{Dec}_{sk_2}((m \cdot pk_1^{\sigma}, g^{\sigma}, pk_1^{\omega}, g^{\omega})) \\ &= \bot, \end{aligned}$$

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,

$$\llbracket (\mathbf{E}_{pk_1}, *) \triangleright \mathbf{R}^* \triangleright \mathbf{D}_{sk_2}, pk_1, pk_2 \rrbracket \simeq_{\frac{1}{q}} \llbracket \bot, pk_1, pk_2 \rrbracket. \qquad \square$$

Lemma 41. $\mathsf{ddh} \implies \mathsf{ind\text{-}cpa}^{\Pi_{\mathsf{URE\text{-}ElGamal}}}$.

Proof. Let define reduction ρ as follows: For $i \in \{0,1\}$, the system $\rho(\mathbf{S}_i^{\mathsf{ddh}}) \doteq \llbracket \mathbf{S}, pk \rrbracket$ initially inputs $\diamond$ to $\mathbf{S}_i^{\mathsf{ddh}}$ obtaining (x,y,z), and then defines:

- $pk \doteq x$.
- $\mathbf{S}$: 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:

- $\rho(\mathbf{S}_0^{\mathsf{ddh}}) \equiv \llbracket \mathbf{E}_{pk}, pk \rrbracket$: 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.
- $\rho(\mathbf{S}_1^{\mathsf{ddh}}) \equiv \llbracket \mathbf{E}_{pk}^{\$}, pk \rrbracket$: 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

$$\begin{aligned} (m \cdot z^u x^v, y^u g^v, x^{\kappa_1} g^{\kappa_1}, g^{\kappa_1}) &= (m \cdot g^{\gamma u + \alpha v + (\alpha\beta u - \alpha\beta u)}, g^{\beta u + v}, g^{\alpha\kappa_1}, g^{\kappa_1}) \\ &= (m \cdot g^{u(\gamma - \alpha\beta)} \cdot g^{\alpha(\beta u + v)}, g^{\beta u + v}, g^{\alpha\kappa_1}, g^{\kappa_1}) \\ &= (\tilde{m} \cdot pk^{\kappa_0}, g^{\kappa_0}, pk^{\kappa_1}, g^{\kappa_1}), \end{aligned}$$

  which is distributed exactly as the output of $\mathbf{E}_{pk}^{\$}$ on input m.

Therefore, $\llbracket \mathbf{E}_{pk}, pk \rrbracket \equiv \rho(\mathbf{S}_0^{\mathsf{ddh}}) \simeq \rho(\mathbf{S}_1^{\mathsf{ddh}}) \equiv \llbracket \mathbf{E}_{pk}^{\$}, pk \rrbracket$. $\square$

Lemma 42. $\mathsf{ddh} \implies \mathsf{ik\text{-}cpa}^{\Pi_{\mathsf{URE\text{-}ElGamal}}}$.

Proof. For $i \in \{1,2\}$, let define reduction ρ_i as follows: For $j \in \{0,1\}$, the system $\rho_i(\mathbf{S}_j^{\mathsf{ddh}}) \doteq \llbracket \mathbf{E}_{pk_1}, \mathbf{S}, pk_1, pk_2 \rrbracket$ initially inputs $\diamond$ to $\mathbf{S}_j^{\mathsf{ddh}}$ obtaining (x_1, y_1, z_1), and then 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 $a, b, c \xleftarrow{\$} \mathbb{Z}_q$. It then defines:

– $pk_1 \doteq x_1$ and $pk_2 \doteq x_2$.
– $\mathbf{S}$: 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,

$$\begin{aligned}[\![\mathbf{E}_{pk_1}, \mathbf{E}_{pk_1}, pk_1, pk_2]\!] &\equiv \rho_1(\mathbf{S}_0^{\mathsf{ddh}}) \\ &\simeq \rho_1(\mathbf{S}_1^{\mathsf{ddh}}) && (\mathsf{ddh}) \\ &\equiv \rho_2(\mathbf{S}_1^{\mathsf{ddh}}) \\ &\simeq \rho_2(\mathbf{S}_0^{\mathsf{ddh}}) && (\mathsf{ddh}) \\ &\equiv [\![\mathbf{E}_{pk_1}, \mathbf{E}_{pk_2}, pk_1, pk_2]\!]. && \square\end{aligned}$$

Lemma 43. $\mathsf{ddh} \implies \mathsf{ulk\text{-}cpa}^{\Pi_{\mathsf{URE\text{-}ElGamal}}}$.

Proof. For $i \in \{1, 2\}$, let define reduction ρ_i as follows: For $j \in \{0, 1\}$, the system $\rho_i(\mathbf{S}_j^{\mathsf{ddh}}) \doteq [\![\mathbf{S}, pk]\!]$ initially inputs $\diamond$ to $\mathbf{S}_j^{\mathsf{ddh}}$ obtaining (x, y, z), and then defines:

– $pk \doteq x$.
– $\mathbf{S}$: 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 showed in the proof of Lemma 41, 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 showed in the proof of Lemma 41, 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,

$$\begin{aligned} [\![\mathbf{E}_{pk} \triangleright \langle *, \mathbf{R}\rangle, pk]\!] &\equiv \rho_1(\mathbf{S}_0^{\mathsf{ddh}}) \\ &\simeq \rho_1(\mathbf{S}_1^{\mathsf{ddh}}) && (\mathsf{ddh}) \\ &\equiv \rho_2(\mathbf{S}_1^{\mathsf{ddh}}) \\ &\simeq \rho_2(\mathbf{S}_0^{\mathsf{ddh}}) && (\mathsf{ddh}) \\ &\equiv [\![\langle \mathbf{E}_{pk}, \mathbf{E}_{pk} \triangleright \mathbf{R}\rangle, pk]\!]. \end{aligned}$$ □

Lemma 44. $\mathsf{ddh} \implies \mathsf{sulk\text{-}cpa}^{\Pi_{\mathsf{URE\text{-}ElGamal}}}$.

Proof. Similar to the proof of Lemma 43. □

Corollary 1. $\mathsf{ddh} \implies \mathsf{ind\text{-}ik\text{-}sulk\text{-}cpa}^{\Pi_{\mathsf{URE\text{-}ElGamal}}}$.

Corollary 2. $\mathsf{ddh} \implies \mathsf{cc\text{-}ure}^{\Pi_{\mathsf{URE\text{-}ElGamal}}}$.