Formalization of Information-Theoretic Security for Encryption and Key Agreement, Revisited

Junji Shikata *

Abstract

In this paper, we revisit formalizations of information-theoretic security for symmetric-key encryption and key agreement protocols. In general, we can formalize information-theoretic security in various ways: some of them can be formalized as stand-alone security by extending (or relaxing) Shannon's perfect secrecy; some of them can be done based on composable security. Then, a natural question about this is: what is the gap between the formalizations? To answer the question, we investigate relationships between several formalizations of information-theoretic security for symmetric-key encryption and key agreement protocols. Specifically, for symmetric-key encryption protocols which may have decryption-errors, we deal with the following formalizations of security: formalizations extended (or relaxed) from Shannon's perfect secrecy by using mutual information and statistical distance; information-theoretic analogue of indistinguishability by Goldwasser and Micali; and the ones of composable security by Maurer et al. and Canetti. Then, we show that those formalizations are essentially equivalent under both one-time and multiple-use models. Under the both models, we also derive lower bounds of the adversary's (or distinguisher's) advantage and secret-key size required under all of the above formalizations. Although some of them are already known, we can derive them all at once through our relationships between the formalizations. In addition, we briefly observe impossibility results which easily follow from the lower bounds. The similar results are also shown for key agreement protocols which may have agreement-errors.

Keywords: composable security, information-theoretic security, key agreement, symmetric-key encryption, unconditional security.

1 Introduction

Background and Related Works. The security of cryptographic protocols in information-theoretic cryptography does not require any computational assumption based on computationally hard problems, such as the integer factoring and discrete logarithm problems. In addition, since the security definition in information-theoretic cryptography is formalized by use of some information-theoretic measure (e.g. entropy or statistical distance), it does not depend on a specific computational model and can provide security which does not compromise even if computational technology intensively develops or a new computational technology (e.g. quantum computation) appears in the future. In this sense, it is interesting to study and develop cryptographic protocols with information-theoretic security.

As fundamental cryptographic protocols we can consider symmetric-key encryption and key-agreement protocols, and the model of the protocols falls into a very simple and basic scenario where there are two honest players (named Alice and Bob) and an adversary (named Eve). Up to date, various results on the topic of those protocols with information-theoretic security have been reported

*Graduate School of Environment and Information Sciences, Yokohama National University, 79-7 Tokiwadai, Hodogaya-ku, Yokohama 240-8501, Japan. E-mail: shikata@ynu.ac.jp

and developed since Shannon's work [27]. In most of those results the traditional security definition has been given as *stand-alone security* in the sense that the protocols will be used in a stand-alone way: in symmetric-key encryption, the security is formalized as $I(M;C) = 0$ (Shannon's perfect secrecy) or its variant (e.g. $I(M;C) \leq \epsilon$ for some small ϵ), where M and C are random variables which take values on sets of plaintexts and ciphertexts, respectively; similarly, in key agreement the security is usually formalized as $I(K;T) = 0$ or its variant (e.g. $I(K;T) \leq \epsilon$), where K and T are random variables which take values on sets of shared keys and transcripts, respectively. The problem with the traditional definition of stand-alone security is that, if a protocol is composed with other ones, the security of the combined protocol may not be clear. Namely, it is not always guaranteed that the composition of individually *secure* protocols results in the *secure* protocol, where *secure* is meant in the sense of the traditional definition of stand-alone security.

On the other hand, *composable security* (or security under composition) can guarantee that a protocol remains to be secure after composed with other ones. The previous frameworks of this line of researches are based on the *ideal-world/real world paradigm*, and the paradigm includes *universal composability* by Canetti [6] and *reactive simulatability* by Backes, Pfitzmann and Waidner [2] (See also [5, 24, 12, 23, 3] for related works). In addition, the explicit and simple paradigm for composable security was given by Maurer [18], and this approach is called *constructive cryptography* where the security definitions of cryptographic systems can be understood as constructive statements: the idea is to consider cryptographic protocols as transformations which construct cryptographically *stronger* systems from *weaker* ones. Using the framework of constructive cryptography, Maurer and Tackmann [21] studied the authenticate-then-encrypt paradigm for symmetric-key encryption with computational security. Recently, Maurer and Renner [19] proposed a new framework in an abstract way, called *abstract cryptography*. The framework is described at a higher level of abstraction than [18, 21], and various notions and methodologies (e.g. universal composability [6], reactive simulatability [2], and indifferentiability [20]) can be captured in the framework.

Up to date, there are a few works which report a gap between formalizations of the stand-alone security and composable security for multiparty computation in information-theoretic settings [1, 10, 15]. In particular, Kushilevitz, Lindell and Rabin [15] investigated the gap between them in several settings (i.e., perfect/statistical security and composition with adaptive/fixed inputs), and they showed a condition that a protocol having stand-alone security is not necessarily secure under universal composition.

Our Contributions. We can formalize information-theoretic security for symmetric-key encryption and key agreement protocols in various ways: some of them can be formalized as stand-alone security by extending Shannon's perfect secrecy; some of them can be done based on composable security. Then, a natural question about this is: what is the gap between the formalizations? To answer the question, we investigate relationships between several formalizations of information-theoretic security for symmetric-key encryption and key agreement protocols. Specifically, for symmetric-key encryption protocols which may have decryption-errors, we deal with the following formalizations of security:

(i) Formalization extended (or relaxed) from Shannon's perfect secrecy by using mutual information;

(ii) Another one extended (or relaxed) from Shannon's perfect secrecy by using statistical distance;

(iii) Formalization by information-theoretic analogue of indistinguishability by Goldwasser and Micali [13];

(iv) Formalizations of composable security by Maurer et al. [19, 21] and Canetti [5, 6].

Then, we explicitly show that those formalizations are essentially equivalent under both one-time and multiple-use models, and in particular, it turns out that the formalizations of the stand-alone and composable security are equivalent, though it seems to be the folklore or implicitly assumed that the stand-alone security formalizations are sufficient for providing composable security in the information-theoretic settings. Under the both models, we also derive lower bounds of the adversary's (or distinguisher's) advantage and secret-key size required under all of the above formalizations. Although some of them are already known, we can derive them all at once through our relationships between the formalizations. In addition, we briefly observe impossibility results which easily follow from the lower bounds. Furthermore, we show similar results (i.e., relationships between formalizations, lower bounds, and impossibility results) for key agreement protocols which may have agreement-errors. We summarize our technical results above in Table 1.

Table 1: Summary of our results

Protocols		Relationships between formalizations	Lower bounds		Impossibility results
			Adversary's (distinguisher's) advantage	Key-size	
Symmetric-key encryption	one-time	Th.1	Th.2	Cor.1	Contrapositive of Cor.1
	multiple-use	Th.3	Th.4	Cor.2	Contrapositive of Cor.2
Key-agreement		Th.5	Th.6	Cor.3	Prop.6 and Cor.4,5

Independent Works Related. Independently of our work, a few papers [14, 4] recently report the equivalence between several formalizations of stand-alone security for encryption in information-theoretic settings as follows, though they do not consider composable security.

Iwamoto and Ohta [14] recently showed equivalence of the following formalizations of stand-alone security for symmetric-key encryption protocols: two formalizations extended (or relaxed) from Shannon's perfect secrecy by using statistical distance (one of them is equal to (ii) above); information-theoretic indistinguishability (the same as (iii)); and information-theoretic semantic security. They also showed that there is a formalization extended from Shannon's perfect secrecy such that it is stronger than those formalizations. Note that they only investigate security notions under the one-time model, and it is assumed that encryption and decryption algorithms are deterministic and that there is no decryption-error in the protocols.

Bellare, Tessaro, and Vardy [4] recently study security definitions and schemes for encryption in the model of the wiretap channels. In particular, in the model of wiretap channels, they showed that the following formalizations of stand-alone security are equivalent: formalizations extended (or relaxed) from Shannon's perfect secrecy by using mutual information and statistical distance (the ones similar to (i) and (ii), respectively); information-theoretic indistinguishability (the one similar to (iii)) which is called *distinguishing security* in [4]; and information-theoretic semantic security. They also showed that the first formalization by using mutual information with restriction on that only uniformly distributed plaintexts are input is weaker than those formalizations.

Organization. The rest of this paper is organized as follows. In Section 2, we survey composable security and its formalization based on [19, 21] which is similar in spirit to previous ones in [2, 5, 6, 24]. In Section 3, we show the equivalence between several security formalizations for symmetric-key encryption protocols in both one-time and multiple-use models. In the both models, we also derive lower bounds of adversary's (or distinguisher's) advantage and secret-key size required under all the formalizations. In addition, impossibility results are briefly observed. In Section 4, we show similar results for key agreement protocols. Finally, we conclude the paper in Section 5.

Notation. In this paper, for a random variable X which takes values in a finite set $\mathcal{X}$, the min-entropy and max-entropy of X are denoted by $H_\infty(X)$ and $H_0(X)$, respectively. Also, $I(X;Y)$ denotes the mutual information between X and Y, and we denote the statistical distance between two distributions P_X and P_Y by $\Delta(P_X, P_Y)$. For completeness, we describe the definitions in Appendix A.

For a joint random variable $(X_1, X_2, \ldots, X_n)$, we denote its associated probability distribution by $P_{X_1 X_2 \ldots X_n}$. And, the entropy, mutual information, and statistical distance of joint random variables are similarly defined by regarding $(X_1, X_2, \ldots, X_n)$ as a single vector-valued random variable. In this paper, for a random variable X which takes values in $\mathcal{X}$, we especially write P_{XX} for the distribution on $\mathcal{X} \times \mathcal{X}$ defined by $P_{XX}(x, x') := P_X(x)$ if $x = x'$, and $P_{XX}(x, x') := 0$ if $x \neq x'$.

Furthermore, $|\mathcal{X}|$ denotes the cardinality of $\mathcal{X}$. Also, $\wp(\mathcal{X}) := \{P_X \text{ on } \mathcal{X}\}$ is the set of all probability distributions P_X on $\mathcal{X}$ (or the set of all random variables X which take values in $\mathcal{X}$).

2 Composable Security

In this paper, we consider a very basic scenario where there are three entities, Alice, Bob (honest players), and Eve (an adversary).

2.1 Definition of Systems

Following the notions in [19] [21], we describe three types of systems: resources, converters and distinguishers (See [19] [21] for more details).

A *resource* is a system with three interfaces labeled A, B, and E, where A, B, and E imply three entities, Alice, Bob, and Eve, respectively. If two resources R, S are used in parallel, this system is called parallel composition of R and S and denoted by $R \parallel S$. We note that $R \parallel S$ is also a resource.

A *converter* is a system with two kinds of interfaces: the first kind of interfaces are designated as the *inner* interfaces which can be connected to interfaces of a resource, and combining a converter and a resource by the connection results in a new resource; the second kind of interfaces are designed as the *outer* interfaces which can be provided as the new interfaces of the combined resource. For a resource R and a converter π, we write $\pi(R)$ for the system obtained by combining R and π, and $\pi(R)$ behaves as a resource, again. A *protocol* is a pair of converters $\pi = (\pi_A, \pi_B)$ for the honest players, Alice and Bob, and the resulting system by applying π to a resource R is denoted by $\pi(R)$ or $\pi_A \pi_B(R)$. For converters (or protocols) π, ϕ, the *sequential composition* of them, denoted by $\phi \circ \pi$, is defined by $(\phi \circ \pi)(R) := \phi(\pi(R))$ for a resource R. In contrast, the *parallel composition* of converters (or protocols) π, ϕ, denoted by $\pi \parallel \phi$, is defined by $(\pi \parallel \phi)(R \parallel S) := \pi(R) \parallel \phi(S)$ for resources R, S.

A *distinguisher* for an n-interface resource is a system with $n + 1$ interfaces: n interfaces are connected to n interfaces of the resource, respectively; and the other interface outputs a bit (i.e., 1 or 0). For a resource R and a distinguisher D, we write DR for the system obtained by combining R and D, and we regard DR as a binary random variable. The purpose of distinguishers is to distinguish two resources, and the advantage of a distinguisher D for two resources R_0, R_1 is defined by

$$\Delta^D(R_0, R_1) := \Delta(DR_0, DR_1),$$

where $\Delta(DR_0, DR_1)$ is the statistical distance of the binary random variables DR_0 and DR_1. Let $\mathcal{D}$ be a set of all distinguishers, and we define

$$\Delta^{\mathcal{D}}(R_0, R_1) := \sup_{D \in \mathcal{D}} \Delta^D(R_0, R_1).$$

Note that $\mathcal{D}$ contains not only polynomial-time distinguishers but also computationally unbounded ones, since this paper deals with information-theoretic security.

2.2 Definition of Security

The security definition we focus on in this paper is derived from the paradigm of constructive cryptography [18]. Technically, the formal definition is based on the works in [19, 21] (see [19, 21] for details), and is similar in spirit to previous simulation-based definitions in [2, 5, 6, 24]. The idea in the paradigm of constructive cryptography includes comparison of the *real* and *ideal* systems: the real system means construction $\pi(R)$ by applying a protocol π to a resource R; and the ideal system consists of the *ideal functionality* (such as ideal channels) S including description of a security goal and a simulator σ connected to the interface of E, which we denote by $\sigma(S)$. If the difference of the two resources, $\pi(R)$ and $\sigma(S)$, is a small quantity (i.e., $\Delta^{\mathcal{D}}(\pi(R), \sigma(S)) \le \epsilon$ for small ϵ), we consider that the protocol π securely constructs S from R. More formally, we define the security as follows.

Definition 1 [19, 21] For resources R, S, we say that a protocol π *constructs S from R with error* $\epsilon \in [0, 1]$, denoted by $R \overset{\pi,\epsilon}{\Longrightarrow} S$, if the following two conditions are satisfied:

1. Availability: For the set of all distinguishers $\mathcal{D}$, we have $\Delta^{\mathcal{D}}(\pi(\perp^E(R)), \perp^E(S)) \le \epsilon$, where $\perp^E$ is the converter which blocks the E-interface for distinguishers when it is attached to R.

2. Security: There exists a simulator σ such that, for the set of all distinguishers $\mathcal{D}$, we have $\Delta^{\mathcal{D}}(\pi(R), \sigma(S)) \le \epsilon$.

In the above definition, we do not require the condition that the simulator is efficient (i.e., polynomial-time). In other words, the simulator may be inefficient.

The advantage of the above security definition lies in that a protocol having this kind of security remains to be secure even if it is composed with other protocols. Formally, this can be stated as follows.

Proposition 1 [19, 21] *Let R, S, T and U be resources, and let π, ϕ be converters (or protocols) such that $R \overset{\pi,\epsilon}{\Longrightarrow} S$ and $S \overset{\phi,\delta}{\Longrightarrow} T$. Then, we have the following:*

(1) $\phi \circ \pi$ satisfies $R \overset{\phi\circ\pi,\epsilon+\delta}{\Longrightarrow} T$;

(2) $\pi \parallel id$ satisfies $R \parallel U \overset{\pi\parallel id,\epsilon}{\Longrightarrow} S \parallel U$; and

(3) $id \parallel \pi$ satisfies $U \parallel R \overset{id\parallel\pi,\epsilon}{\Longrightarrow} U \parallel S$,

where id is the trivial converter which makes the interfaces of the subsystem accessible through the interfaces of the combined system.

We note that the first property in Proposition 1 means the security for sequential composition. In addition, as stated in [19] three properties in Proposition 1 imply the security for parallel composition in the following sense: For resources R, R', S, S' and converters π, ϕ such that $R \overset{\pi,\epsilon}{\Longrightarrow} S$ and $R' \overset{\phi,\delta}{\Longrightarrow} S'$, $\pi \parallel \phi$ satisfies $R \parallel R' \overset{\pi\parallel\phi,\epsilon+\delta}{\Longrightarrow} S \parallel S'$.

2.3 Ideal Functionality/Channels

In this section, we give several definitions of ideal functionality of resources such as the authenticated channel and key sharing resources which are necessary to discuss in this paper.

- Authenticated Channel: An *authenticated channel* usable once, denoted by $\bullet\!\!\longrightarrow$, transmits a message (or a plaintext) m from Alice's interface (i.e., A-interface) to Bob's interface (i.e., B-interface) without any error/replacement. If Eve is active, through the E-interface Eve obtains m, and she obtains nothing, otherwise. Similarly, an authenticated channel from B-interface to A-interface can be defined and denoted by $\longleftarrow\!\!\bullet$. For a positive integer t, we write $(\bullet\!\!\longrightarrow)^t$ for the composition of invoked t authenticated channels $\bullet\!\!\longrightarrow \| \bullet\!\!\longrightarrow \| \cdots \| \bullet\!\!\longrightarrow$ (t times), and we write $(\bullet\!\!\longrightarrow)^\infty$ if arbitrarily many use of $\bullet\!\!\longrightarrow$ is allowed. Similarly, $(\longleftarrow\!\!\bullet\ )^t$ and $(\longleftarrow\!\!\bullet\ )^\infty$ can be defined.

- Secure Channel: A *secure channel* usable once, denoted by $\bullet\!\!\longrightarrow\!\!\bullet$, transmits a plaintext m from A-interface to B-interface without any error/replacement. Even if Eve is active, she obtains nothing except for the length of the plaintexts and cannot replace m with another plaintext. Also, for a positive integer t, we write $(\bullet\!\!\longrightarrow\!\!\bullet)^t$ for the composition of invoked t secure channels $\bullet\!\!\longrightarrow\!\!\bullet \| \bullet\!\!\longrightarrow\!\!\bullet \| \cdots \| \bullet\!\!\longrightarrow\!\!\bullet$ (t times).

- Key Sharing Resource (with Uniform Distribution): A *key sharing resource* with the uniform distribution usable once, denoted by $\bullet\!\!=\!\!=\!\!\bullet$, means the ideal resource with no input which generates a uniform random string k and outputs it at both interfaces of Alice and Bob. Even if Eve is active, her interface outputs no information on k and cannot replace k with another one. More generally, if such a key k is chosen according to a distribution P_K (not necessarily the uniform distribution), we denote the key sharing resource by $[P_K]$.

- Correlated Randomness Resource (or Key Distribution Resource): Let P_{XY} be a probability distribution with random variables X and Y. A *correlated randomness resource* usable once, denoted by $[P_{XY}]$, means the resource with no input which randomly generates (x, y) according to the distribution P_{XY} and outputs x and y at interfaces of Alice and Bob, respectively. Even if Eve is active, her interface outputs no information on (x, y) and cannot replace it with another one. Note that the resource $[P_{XY}]$ includes $[P_K]$ (and hence $\bullet\!\!=\!\!=\!\!\bullet$) as a special case.

3 Symmetric-key Encryption

3.1 Protocol Execution

We explain the traditional protocol execution of symmetric-key encryption. In the following, let $\mathcal{M}$ (resp. $\mathcal{C}$) be a finite set of plaintexts (resp. a finite set of ciphertexts) and $\tilde{\mathcal{M}} := \mathcal{M} \cup \{\perp\}$. Also, let M (resp. $\tilde{M}$) be a random variable which takes plaintexts in $\mathcal{M}$ (resp. $\tilde{\mathcal{M}}$) and P_M (resp. $P_{\tilde{M}}$) its distribution. C denotes a random variable which takes ciphertexts $c \in \mathcal{C}$.

Let $\pi_{enc} = (\pi^A_{enc}, \pi^B_{enc})$ be an encryption protocol as defined in the next page, where π^A_{enc} (resp. π^B_{enc}) is a converter at Alice's (resp. Bob's) side.

Symmetric-key Encryption Protocol π_{enc}
Input of Alice's outer interface: $m \in \mathcal{M}$ Input of Alice's inner interface: $k \in \mathcal{K}$ by accessing $[P_K]$ Input of Bob's inner interface: $k \in \mathcal{K}$ by accessing $[P_K]$ Output of Bob's outer interface: $\tilde{m} \in \tilde{\mathcal{M}}$ 1. π^A_{enc} computes $c = \pi^A_{enc}(k, m)$ and sends c to π^B_{enc} by $\bullet\!\!\longrightarrow$. 2. π^B_{enc} computes $\tilde{m} = \pi^B_{enc}(k, c)$ and outputs $\tilde{m}$.

Note that we do not require any restriction on the protocol execution of symmetric-key encryption such as: an encryption algorithm is deterministic; or for each $k \in \mathcal{K}$, $\pi_{enc}^A(k, \cdot) : \mathcal{M} \to \mathcal{C}$ is injective; or a decryption algorithm is deterministic; or it has to be satisfied that $\pi_{enc}^B(k, \pi_{enc}^A(k, m)) = m$ for any possible k and m. Therefore, we deal with a general case of the protocol execution of symmetric-key encryption. In particular, it should be noted that: π_{enc}^A can be probabilistic (i.e., not necessarily deterministic); for each $k \in \mathcal{K}$, $\pi_{enc}^A(k, \cdot)$ may not be injective; π_{enc}^B can be probabilistic; and a decryption-error may occur.

If a symmetric-key encryption protocol π_{enc} is usable at most one time (i.e., the one-time model), the purpose of π_{enc} is to transform the resources $[P_K]$ and $\bullet\!\!\longrightarrow$ into the secure channel $\bullet\!\!\longrightarrow\!\!\bullet$. Also, the purpose of a multiple-use (say, t times) symmetric-key encryption protocol π_{enc} with a same secret-key $k \in \mathcal{K}$ is to transform $[P_K]$ and $(\bullet\!\!\longrightarrow)^t$ into $(\bullet\!\!\longrightarrow\!\!\bullet)^t$.

3.2 Security Definitions Revisited: Formalizations and Relationships

In this section, we revisit the formalization of several information-theoretic security notions for symmetric-key encryption in the one-time model. The most famous one is the notion of perfect secrecy by Shannon[27]: $I(M;C) = 0$. As an extended (or a relaxed) version, we can also consider its variant: $I(M;C) \le \epsilon$ for some extremely small quantity ϵ. Along with this concept, we first consider the following two definitions.

Definition 2 Let π be a symmetric-key encryption protocol in the one-time model. Let P_M be a certain probability distribution on $\mathcal{M}$. Then, π is said to be *ϵ-secure for P_M* if it satisfies the following conditions: (i) *Correctness* $P(M \ne \tilde{M}) \le \epsilon$; and (ii) *Secrecy* $I(M;C) \le \epsilon$. In particular, π is said to be *perfectly-secure for P_M* if it is 0-secure for P_M.

Definition 3 Let π be a symmetric-key encryption protocol in the one-time model. Then, π is said to be *ϵ-secure*, if for any probability distribution $P_M \in \wp(\mathcal{M})$, we have:

$$\text{(i) } \textit{Correctness} \quad P(M \ne \tilde{M}) \le \epsilon; \quad \text{and (ii) } \textit{Secrecy} \quad I(M;C) \le \epsilon.$$

In particular, π is said to be *perfectly-secure* if it is 0-secure.

The difference of Definitions 2 and 3 is that we consider security only for a certain distribution of plaintexts or for all distributions of plaintexts. Obviously, Definition 3 is stronger than Definition 2, since we can find a distribution P_M and π such that π is ϵ-secure for P_M but it is not ϵ-secure. In this paper, we are interested in the security of Definition 3 or other formalizations of strong security for symmetric-key encryption protocols. We now define various types of security formalizations as follows.

Definition 4 Let π be a symmetric-key encryption protocol in the one-time model where $\mathcal{M}$ and $\mathcal{C}$ are finite sets of plaintexts and ciphertexts, respectively. We define the following formalizations of Correctness and Secrecy.

1. Correctness: (I) $\beta_{\pi,1} := \sup_{P_M} P(M \ne \tilde{M})$, (II) $\beta_{\pi,2} := \sup_{P_M} \Delta(P_{M\tilde{M}}, P_{MM})$,
   (III) $\beta_{\pi,3} := \max_m \Delta(P_{\tilde{M}|M=m}, P_{M|M=m})$.
2. Secrecy: (i) $\alpha_{\pi,1} := \sup_{P_M} I(M;C)$, (ii) $\alpha_{\pi,2} := \sup_{P_M} \Delta(P_{MC}, P_M P_C)$,
   (iii) $\alpha_{\pi,3} := \max_m \max_{m' \ne m} \Delta(P_{C|M=m}, P_{C|M=m'})$, (iv) $\alpha_{\pi,4} := \inf_{P_Q} \sup_{P_M} \Delta(P_{MC}, P_M P_Q)$,
   (v) $\alpha_{\pi,5} := \inf_{P_Q} \max_m \Delta(P_{C|M=m}, P_Q)$,

where the supremum ranges over all $P_M \in \wp(\mathcal{M})$ and the infimum ranges over all $P_Q \in \wp(\mathcal{C})$. Then, π is said to be (δ, ϵ)-*secure in the sense of Type* (i, j) *in the one-time model*, if π satisfies $\beta_{\pi,i} \leq \delta$ and $\alpha_{\pi,j} \leq \epsilon$.

By Definition 4, we can obtain fifteen kinds of security formalizations. In particular, several important formalizations known so far can be captured within Definition 4 as follows.

- The formalization in Definition 3 corresponds to the security in the sense of Type $(1, 1)$.
- The formalization using statistical distance instead of mutual information in Definition 3 corresponds to the security in the sense of Type $(1, 2)$.
- The formalization based on information-theoretic analogue of indistinguishability by Goldwasser and Micali [13] corresponds to the security in the sense of Type $(1, 3)$: $\alpha_{\pi,3}$ means the adversary's advantage for distinguishing the views (i.e., distributions of ciphertexts) in the protocol execution when two different plaintexts are inputted.
- The formalizations based on information-theoretic composable security by Maurer et al. [19, 21] and Canetti [5, 6] are closely related to the security in the sense of Type $(2, 4)$ and Type $(3, 5)$, respectively (anyway, we will see $(\beta_{\pi,2}, \alpha_{\pi,4}) = (\beta_{\pi,3}, \alpha_{\pi,5})$ by Theorem 1): a distinguisher arbitrarily chooses a random variable M (or a plaintext m) and inputs it into A-interface; then, $\beta_{\pi,2}$ (or $\beta_{\pi,3}$) means the distinguisher's advantage for distinguishing real output and ideal one at B-interface, and $\beta_{\pi,2}$ is the same as the formalization of availability in Definition 1 for symmetric-key encryption protocols in the one-time model; and $\alpha_{\pi,4}$ (or $\alpha_{\pi,5}$) means the distinguisher's advantage for distinguishing real output and simulator's output (according to P_Q) at E-interface. Actually, validity of using the simple formalization $\alpha_{\pi,4}$ instead of the formalization of security in Definition 1 for symmetric-key encryption is shown by Proposition 2 below.

Proposition 2 *The formalization of security in Definition 1 for a symmetric-key encryption protocol* π *in the one-time model is lower-and-upper bounded as follows:*

$$\max(\alpha_{\pi,4}, \beta_{\pi,2}) \leq \inf_{\sigma} \Delta^{\mathcal{D}}(\pi(\bullet\!\!\longrightarrow\!\!|| \ [P_K]), \sigma(\bullet\!\!\longrightarrow\!\!\bullet)) \leq \alpha_{\pi,4} + \beta_{\pi,2}.$$

Proof. By focusing on distributions of input at A-interface, output at B-interface and output at E-interface, for simplicity, we write $\inf_{P_Q} \sup_{P_M} \Delta(P_{M\tilde{M}C}, P_{MM}P_Q)$ for $\inf_\sigma \Delta^{\mathcal{D}}(\pi(\bullet\!\!\longrightarrow\!\!|| \ [P_K]), \sigma(\bullet\!\!\longrightarrow\!\!\bullet))$.

For any distributions $P_M \in \wp(\mathcal{M})$ and $P_Q \in \wp(\mathcal{C})$, we have

$$\begin{aligned} \Delta(P_{M\tilde{M}C}, P_{MM}P_Q) &\leq \Delta(P_{M\tilde{M}C}, P_{MMC}) + \Delta(P_{MMC}, P_{MM}P_Q) \\ &= \Delta(P_{M\tilde{M}}, P_{MM}) + \Delta(P_{MC}, P_M P_Q). \end{aligned}$$

By taking the supremum over all $P_M \in \wp(\mathcal{M})$ and the infimum over all $P_Q \in \wp(\mathcal{C})$, we have

$$\begin{aligned} \inf_{P_Q} \sup_{P_M} \Delta(P_{M\tilde{M}C}, P_{MM}P_Q) &\leq \sup_{P_M} \Delta(P_{M\tilde{M}}, P_{MM}) + \inf_{P_Q} \sup_{P_M} \Delta(P_{MC}, P_M P_Q) \\ &= \alpha_{\pi,4} + \beta_{\pi,2}. \end{aligned}$$

In addition, from Proposition 7 in Appendix A, it is clear that $\Delta(P_{MC}, P_M P_Q) \leq \Delta(P_{M\tilde{M}C}, P_{MM}P_Q)$ for any $P_M \in \wp(\mathcal{M})$ and $P_Q \in \wp(\mathcal{C})$. Therefore, we obtain $\alpha_{\pi,4} \leq \inf_{P_Q} \sup_{P_M} \Delta(P_{M\tilde{M}C}, P_{MM}P_Q)$. Similarly, we have $\beta_{\pi,2} \leq \inf_{P_Q} \sup_{P_M} \Delta(P_{M\tilde{M}C}, P_{MM}P_Q)$. $\square$

We next show the relationships between security formalizations of Type (i,j) for $i \in \{1,2,3\}$ and $j \in \{1,2,\dots,5\}$. The following theorem (i.e., Theorem 1) states that any formalization of Type (i,j) in Definition 4 is equivalently sufficient to define security, if δ and ϵ are extremely small quantities. In this sense, we can say that all formalizations in Definition 4 are essentially equivalent.

Theorem 1 *Let π be a symmetric-key encryption protocol in the one-time model. Then, we have explicit relationships between $\alpha_{\pi,i}$, $\beta_{\pi,j}$ for $i \in \{1,2,\dots,5\}$, $j \in \{1,2,3\}$ as follows:*

$$\beta_{\pi,1} = \beta_{\pi,2} = \beta_{\pi,3}; \text{ and}$$
$$\frac{1}{2}\alpha_{\pi,2} \le \alpha_{\pi,4} = \alpha_{\pi,5} \le \alpha_{\pi,3} \le 2\alpha_{\pi,2}, \quad \frac{2}{\ln 2}\alpha_{\pi,2}^2 \le \alpha_{\pi,1} \le -2\alpha_{\pi,2}\log\frac{2\alpha_{\pi,2}}{|\mathcal{M}|\ |\mathcal{C}|}.$$

In particular, for any $i,j \in \{1,2,\dots,5\}$ and any $s,t \in \{1,2,3\}$, we have

$$\lim_{(\beta_{\pi,s},\alpha_{\pi,i})\to(0,0)} (\beta_{\pi,t},\alpha_{\pi,j}) = (0,0),$$

where the limit is taken by changing $[P_K]$ or π[1].

Proof. First, we show relationships between formalizations of correctness.

(i) We show $\beta_{\pi,1} = \beta_{\pi,2}$: For any π and for any distribution P_M, we have $\Delta(P_{MM}, P_{M\tilde{M}}) = P(M \neq \tilde{M})$ by Proposition 8 in Appendix A, from which it is straightforward to have $\beta_{\pi,1} = \beta_{\pi,2}$.

(ii) We show $\beta_{\pi,2} = \beta_{\pi,3}$: For an arbitrary distribution P_M, we have

$$\begin{aligned} 2\Delta(P_{M\tilde{M}}, P_{MM}) &= \sum_{m,\tilde{m}} |P_{M\tilde{M}}(m,\tilde{m}) - P_{MM}(m,\tilde{m})| \\ &= \sum_m P_M(m) \sum_{\tilde{m}} |P_{\tilde{M}|M}(\tilde{m}|m) - P_{M|M}(\tilde{m}|m)| \\ &\le \max_m \sum_{\tilde{m}} |P_{\tilde{M}|M}(\tilde{m}|m) - P_{M|M}(\tilde{m}|m)| \\ &= 2\max_m \Delta(P_{\tilde{M}|M=m}, P_{M|M=m}). \end{aligned}$$

Therefore, $\beta_{\pi,2} \le \beta_{\pi,3}$.

Let $m_1 \in \mathcal{M}$ be a plaintext such that it gives $\beta_{\pi,3}$. For any $\epsilon > 0$, we define a distribution P_{M_1} by

$$P_{M_1}(m) := \begin{cases} 1-\delta \text{ if } m = m_1, \\ \frac{\delta}{|\mathcal{M}|-1} \text{ otherwise,} \end{cases}$$

where δ is a non-negative real number such that $0 \le \delta\beta_{\pi,3} \le \epsilon$. Then, we have

$$\begin{aligned} \beta_{\pi,2} &\ge \Delta(P_{M_1\tilde{M}_1}, P_{M_1M_1}) \\ &\ge (1-\delta)\Delta(P_{\tilde{M}_1|M_1=m_1}, P_{M_1|M_1=m_1}) \\ &= (1-\delta)\beta_{\pi,3} \\ &\ge \beta_{\pi,3} - \epsilon. \end{aligned}$$

[1]Note that $\alpha_{\pi,i}$ $(2 \le i \le 5)$ are of the same order and the order of $\alpha_{\pi,1}$ may not be the same as those of $\alpha_{\pi,i}$ $(2 \le i \le 5)$.

We next show relationships between formalizations of secrecy.

(1) We show that $\frac{2}{\ln 2}\alpha_{\pi,2}^2 \le \alpha_{\pi,1} \le -2\alpha_{\pi,2}\log\frac{2\alpha_{\pi,2}}{|\mathcal{M}|\ |\mathcal{C}|}$: From Theorem 16.3.2[7] (or see Corollary 8 in Appendix A), it follows that, for any P_M and any π,

$$\begin{aligned} I(M;C) &\le -2\Delta(P_{MC}, P_M P_C)\log\frac{2\Delta(P_{MC}, P_M P_C)}{|\mathcal{M}|\cdot|\mathcal{C}|} \\ &\le -2\alpha_{\pi,2}\log\frac{2\alpha_{\pi,2}}{|\mathcal{M}|\cdot|\mathcal{C}|}. \end{aligned}$$

Therefore, we have

$$\alpha_{\pi,1} \le -2\alpha_{\pi,2}\log\frac{2\alpha_{\pi,2}}{|\mathcal{M}|\cdot|\mathcal{C}|}.$$

On the other hand, from Theorem 12.6.1[7] (or see Corollary 7 in Appendix A), it follows that, for any P_M and any π,

$$\Delta(P_{MC}, P_M P_C) \le \sqrt{\frac{\ln 2}{2}} I(M;C)^{\frac{1}{2}}.$$

Therefore, we have $\alpha_{\pi,2} \le \sqrt{\frac{\ln 2}{2}}\alpha_{\pi,1}^{\frac{1}{2}}$.

(2) We show $\alpha_{\pi,3} \le 2\alpha_{\pi,2}$: For any $\epsilon > 0$, and for $m_0, m_1 \in \mathcal{M}$ $(m_0 \ne m_1)$ such that $\alpha_{\pi,3} = \Delta(P_{C|M=m_0}, P_{C|M=m_1})$, we define a distribution $P_{\hat{M}}$ by

$$P_{\hat{M}}(m) := \begin{cases} \frac{1}{2}(1-\delta) \text{ if } m \in \{m_0, m_1\}, \\ \frac{\delta}{|\mathcal{M}|-2} \text{ otherwise,} \end{cases}$$

where δ is a non-negative real number such that $0 \le \delta\alpha_{\pi,3} \le 2\epsilon$. Then, we have

$$\begin{aligned} \alpha_{\pi,2} &\ge \Delta(P_{\hat{M}\hat{C}}, P_{\hat{M}} P_{\hat{C}}) \\ &\ge \frac{1}{2}(1-\delta)\{\Delta(P_{\hat{C}|\hat{M}=m_0}, P_{\hat{C}}) + \Delta(P_{\hat{C}|\hat{M}=m_1}, P_{\hat{C}})\} \\ &\ge \frac{1}{2}(1-\delta)\Delta(P_{\hat{C}|\hat{M}=m_0}, P_{\hat{C}|\hat{M}=m_1}) \\ &= \frac{1}{2}(1-\delta)\alpha_{\pi,3} \\ &\ge \frac{1}{2}\alpha_{\pi,3} - \epsilon. \end{aligned}$$

(3) We show that $\alpha_{\pi,5} \le \alpha_{\pi,3}$: Let $m_0 \in \mathcal{M}$ be a plaintext such that it gives $\alpha_{\pi,5}$, and set $P_Q := P_{C|M=m_1}$ by choosing $m_1 \in \mathcal{M}$ $(m_1 \ne m_0)$. Then, we have

$$\begin{aligned} \alpha_{\pi,5} &\le \Delta(P_{C|M=m_0}, P_Q) \\ &= \Delta(P_{C|M=m_0}, P_{C|M=m_1}) \\ &\le \alpha_{\pi,3}. \end{aligned}$$

(4) We show that $\alpha_{\pi,4} = \alpha_{\pi,5}$: For arbitrary distributions P_Q and P_M, we have

$$\begin{aligned} 2\Delta(P_{MC}, P_M P_Q) &= \sum_{m,c} |P_{MC}(m,c) - P_M(m)P_Q(c)| \\ &= \sum_m P_M(m) \sum_c |P_{C|M}(c|m) - P_Q(c)| \\ &\leq \max_m \sum_c |P_{C|M}(c|m) - P_Q(c)| \\ &= 2\max_m \Delta(P_{C|M=m}, P_Q). \end{aligned}$$

Therefore, $\alpha_{\pi,4} \leq \alpha_{\pi,5}$.

Next, we show $\alpha_{\pi,5} \leq \alpha_{\pi,4}$. Let $m_1 \in \mathcal{M}$ be a plaintext such that it gives $\alpha_{\pi,5}$. For any $\epsilon > 0$, we define a distribution P_{M_1} by

$$P_{M_1}(m) := \begin{cases} 1-\delta \text{ if } m = m_1, \\ \frac{\delta}{|\mathcal{M}|-1} \text{ otherwise,} \end{cases}$$

where δ is a non-negative real number such that $0 \leq \delta\alpha_{\pi,5} \leq \epsilon$. Then, for any $P_Q \in \wp(\mathcal{C})$, we have

$$\begin{aligned} \sup_{P_M} \Delta(P_{MC}, P_M P_Q) &\geq \Delta(P_{M_1C_1}, P_{M_1}P_Q) \\ &\geq (1-\delta)\Delta(P_{C_1|M_1=m_1}, P_Q). \end{aligned}$$

Therefore, by taking the infimum over all $P_Q \in \wp(\mathcal{C})$, we have $\alpha_{\pi,5} - \epsilon \leq \alpha_{\pi,4}$.

(5) We show that $\frac{1}{2}\alpha_{\pi,2} \leq \alpha_{\pi,4}$: For arbitrary distributions P_Q and P_M, we have

$$\begin{aligned} \Delta(P_{MC}, P_M P_C) &\leq \Delta(P_{MC}, P_M P_Q) + \Delta(P_M P_Q, P_M P_C) \\ &= \Delta(P_{MC}, P_M P_Q) + \Delta(P_Q, P_C) \\ &\leq 2\Delta(P_{MC}, P_M P_Q). \end{aligned}$$

Therefore, $\alpha_{\pi,2} \leq 2\alpha_{\pi,4}$. $\square$

3.3 Lower Bounds and Impossibility Results in One-time Model

In this section, under each of the security formalizations in Definition 4, we derive lower bounds of the adversary's (or distinguisher's) advantage and the required size of secret-keys. First, we note the following lower bound shown in [25].

Proposition 3 ([25]) *Let π be a symmetric-key encryption protocol in the one-time model. Then, for any simulator σ on $\mathcal{C}$, and for the set of all distinguishers $\mathcal{D}$, we have*

$$\Delta^{\mathcal{D}}(\pi(\bullet\!\!\longrightarrow \| \ [P_K]), \sigma(\bullet\!\!\longrightarrow\!\!\bullet)) \geq 1 - \frac{|\mathcal{K}|}{|\mathcal{M}|}.$$

In [25] Pope showed the above lower bound by only considering a distinguisher that inputs the uniformly distributed plaintexts into the symmetric-key encryption protocol for distinguishing real output and ideal one. We now derive lower bounds for the adversary's (or distinguisher's) advantage under all formalizations in Definition 4 at once through our relationships (The proof follows from Proposition 2, Theorem 1, and Proposition 3).

Theorem 2 *For any symmetric-key encryption protocol π in the one-time model, we have:*

$$(i) \quad \sqrt{\frac{\ln 2}{2}}\alpha_{\pi,1}^{\frac{1}{2}} + \beta_{\pi,j} \geq \frac{1}{2}\left(1 - \frac{|\mathcal{K}|}{|\mathcal{M}|}\right) \textit{ for } j \in \{1,2,3\};$$

$$(ii) \quad \alpha_{\pi,2} + \beta_{\pi,j} \geq \frac{1}{2}\left(1 - \frac{|\mathcal{K}|}{|\mathcal{M}|}\right) \textit{ for } j \in \{1,2,3\};$$

$$(iii) \quad \alpha_{\pi,i} + \beta_{\pi,j} \geq 1 - \frac{|\mathcal{K}|}{|\mathcal{M}|} \textit{ for } i \in \{3,4,5\} \textit{ and } j \in \{1,2,3\},$$

where $\alpha_{\pi,i}$ and $\beta_{\pi,j}$ are parameters for secrecy and correctness, respectively, defined in Definition 4.

We do not know whether the lower bounds in Theorem 2 are tight in the sense that there exists a protocol π (and $[P_K]$) such that equality holds for given advantage (in particular, given positive $\alpha_{\pi,i}$ and $\beta_{\pi,j}$) in general. However, we note that they are tight in the sense that there exists a protocol π (and $[P_K]$) such that equality holds (e.g., the one-time pad for zero advantage).

From Theorem 2, we obtain the following lower bounds for the size of secret-keys (Corollary 1 below). The proof of Corollary 1 immediately follows from Theorem 2, and we omit the proof.

Corollary 1 *Suppose that a symmetric-key encryption protocol π is (δ,ϵ)-secure in the sense of Type (i,j) in the one-time model. Then, we have the following lower bounds for the size of secret-keys:*

$$(i) \quad |\mathcal{K}| \geq \left\{1 - \left(\sqrt{2\ln 2}\epsilon^{\frac{1}{2}} + 2\delta\right)\right\}|\mathcal{M}| \textit{ for } j = 1 \textit{ and } i \in \{1,2,3\};$$

$$(ii) \quad |\mathcal{K}| \geq \{1 - 2(\epsilon + \delta)\}|\mathcal{M}| \textit{ for } j = 2 \textit{ and } i \in \{1,2,3\};$$

$$(iii) \quad |\mathcal{K}| \geq \{1 - (\epsilon + \delta)\}|\mathcal{M}| \textit{ for } j \in \{3,4,5\} \textit{ and } i \in \{1,2,3\}.$$

Remark 1 As described in [28], it is known that: *Let $\{\Phi_r | r \in \mathcal{R}\}$ be a family of (hash) functions from $\mathcal{S}$ to $\mathcal{T}$ such that: each Φ_r maps $\mathcal{S}$ injectively into $\mathcal{T}$; and there exists $\epsilon \in [0,1]$ such that $\Delta(\Phi_H(s), \Phi_H(s')) \leq \epsilon$ for all $s, s' \in \mathcal{S}$, where H is uniformly distributed over $\mathcal{R}$. Then, we have $|\mathcal{R}| \geq (1-\epsilon)|\mathcal{S}|$.* Corollary 1 can be understood as an extension of the above statement (see (iii) in Corollary 1). Actually, we do not necessarily assume that: for each $k \in \mathcal{K}$, $\pi^A(k,\cdot) : \mathcal{M} \to \mathcal{C}$ is deterministic and injective (Note that δ can be zero if $\pi^A(k,\cdot)$ is injective); or P_K is uniform.

By considering a contrapositive of Corollary 1, we obtain the following impossibility result: There exists no symmetric-key encryption protocol which is (δ,ϵ)-secure in the sense of Type (i,j) in the one-time model, if δ and ϵ are some real numbers such that they do not satisfy the corresponding inequality among (i)-(iii) in Corollary 1.

3.4 Multiple-use Model

We extend the results in the one-time model in Sections 3.2 and 3.3 to the ones in the multiple-use model where a symmetric-key encryption protocol can be used multiple times (say, at most T times) with a same secret-key. First, we give the following definition by extending Definition 4.

Definition 5 Let π be a multiple-use symmetric-key encryption protocol where the number of protocol execution with a same secret-key is up to T. For every positive integer $t \leq T$, we define the following formalizations of Correctness and Secrecy.

1. Correctness:

$$(I) \quad \beta_{\pi,t,1} := \sup_{P_{M_1 M_2 \ldots M_t}} P((M_1, M_2, \ldots, M_t) \neq (\tilde{M}_1, \tilde{M}_2, \ldots, \tilde{M}_t)),$$

$$(II) \quad \beta_{\pi,t,2} := \sup_{P_{M_1 M_2 \ldots M_t}} \Delta(P_{M_1\tilde{M}_1, M_2\tilde{M}_2, \ldots, M_t\tilde{M}_t}, P_{M_1M_1, M_2M_2, \ldots, M_tM_t}),$$

$$(III) \quad \beta_{\pi,t,3} := \max_{(m_1,m_2,\ldots,m_t)} \Delta(P_{\tilde{M}_1\tilde{M}_2\ldots\tilde{M}_t | M_1=m_1, M_2=m_2, \ldots, M_t=m_t}, P_{M_1M_2\ldots M_t | M_1=m_1, M_2=m_2, \ldots, M_t=m_t}).$$

2. Secrecy: (i) $\alpha_{\pi,t,1} := \sup_{P_{M_1M_2\ldots M_t}} I(M_t; C_t|M_1C_1, M_2C_2, \ldots M_{t-1}C_{t-1})$,

(ii) $\alpha_{\pi,t,2} := \sup_{P_{M_1M_2\ldots M_t}} \Delta(P_{M_tC_t|M_1C_1,M_2C_2,\ldots,M_{t-1}C_{t-1}}, P_{M_t|M_1C_1,M_2C_2,\ldots,M_{t-1}C_{t-1}} P_{C_t|M_1C_1,M_2C_2,\ldots,M_{t-1}C_{t-1}})$,

(iii) $\alpha_{\pi,t,3} := \max_{((m_1,c_1),(m_2,c_2),\ldots,(m_{t-1},c_{t-1}))} \max_{(m,m') \text{ s.t. } m\neq m' \text{ and } m,m'\notin\{m_1,m_2,\ldots,m_{t-1}\}} \Delta(P_{C|M=m,(M_1,C_1)=(m_1,c_1),\ldots,(M_{t-1},C_{t-1})=(m_{t-1},c_{t-1})}, P_{C|M=m',(M_1,C_1)=(m_1,c_1),\ldots,(M_{t-1},C_{t-1})=(m_{t-1},c_{t-1})})$,

(iv) $\alpha_{\pi,t,4} := \inf_{P_{Q_1Q_2\ldots Q_t}} \sup_{P_{M_1M_2\ldots M_t}} \Delta(P_{M_1C_1,M_2C_2,\ldots,M_tC_t}, P_{M_1Q_1,M_2Q_2,\ldots,M_tQ_t})$,

(v) $\alpha_{\pi,t,5} := \inf_{P_{Q_1Q_2\ldots Q_t}} \max_{(m_1,m_2,\ldots,m_t)} \Delta(P_{C_1C_2\ldots C_t|M_1=m_1,M_2=m_2,\ldots,M_t=m_t}, P_{Q_1Q_2\ldots Q_t})$,

where, for every $i \le t$, a random variable M_i may depend on previous information which an adversary (or a distinguisher) obtains before (e.g., $M_1C_1, M_2C_2, \ldots, M_{i-1}C_{i-1}$), while Q_i depends only on $Q_1, Q_2, \ldots, Q_{i-1}$; the supremum is taken over all $P_{M_1M_2\cdots M_t} \in \wp(\mathcal{M}^t)$; and the infimum is taken over all $P_{Q_1Q_2\ldots Q_t} \in \wp(\mathcal{C}^t)$. Then, π is said to be (δ, ϵ, T)*-secure in the sense of Type* (i, j) *in the multiple-use model*, if π satisfies

$$\max_{1\le t\le T}\{\beta_{\pi,t,i}\} \le \delta \text{ and } \max_{1\le t\le T}\{\alpha_{\pi,t,j}\} \le \epsilon.$$

We now explain the meaning of formalizations of Correctness (I)-(III) and Secrecy (i)-(v) in detail as follows.

- (I), (II) and (III). Formalizations of correctness which are simple extension from the ones in Definition 4 for t protocol execution. The supremum is taken over all distributions $P_{M_1M_2\cdots M_t}$, where for every $i \le t$ a random variable M_i may depend on previous information (e.g., $(M_1, M_2, \ldots, M_{i-1})$ or $(M_1\tilde{M}_1, M_2\tilde{M}_2, \ldots, M_{i-1}\tilde{M}_{i-1})$).

- (i) and (ii). Formalizations based on Shannon's notion of independence of plaintexts and ciphertexts (i.e., independence of M_t and C_t) under CPA (chosen plaintext attacks) by an adversary: An adversary is allowed to access the encryption oracle; he/she makes a query, an arbitrarily chosen random variable M_i $(i < t)$, and obtains a corresponding answer C_i, where M_i may depend on previous ones $M_1C_1, M_2C_2, \ldots, M_{i-1}C_{i-1}$.

- (iii). Formalization of indistinguishability under CPA by an adversary: An adversary is allowed to access the encryption oracle; he/she makes a query, an arbitrarily chosen plaintext $M_i = m_i$ $(i < t)$, and obtains a corresponding ciphertext $C_i = c_i$ as an answer; The purpose of the adversary is to maximize his/her advantage for distinguishing two distributions of ciphertexts, $P_{C|M=m}$ and $P_{C|M=m'}$ by arbitrarily choosing plaintexts m, m' $(m \neq m')$ with query/answer pairs $(m_1, c_1), (m_2, c_2), \ldots, (m_{t-1}, c_{t-1})$.

- (iv) and (v). Formalizations based on composable security, and $(\beta_{\pi,t,2}, \alpha_{\pi,t,4})$ and $(\beta_{\pi,t,3}, \alpha_{\pi,t,5})$ mean distinguishing advantage by a distinguisher which can communicate with an adversary: For every $i \le t$, a distinguisher arbitrarily chooses a random variable M_i (or a plaintext m_i), which may depend on the information the distinguisher has obtained before (e.g., M_i may depend on $M_1C_1, M_2C_2, \ldots, M_{i-1}C_{i-1}$), and inputs it into A-interface; the distinguisher gets a decrypted plaintext $\tilde{M}_i$ or the genuine plaintext M_i from B-interface, and via an adversary it obtains a real ciphertext C_i or simulator's output Q_i from E-interface. Since Alice and Bob are not corrupted and the adversary cannot delete, insert or forge a ciphertext on the authenticated channel, what the adversary can do is to send the distinguisher a ciphertext obtained at E-interface.

The validity of using the simple formalization $\alpha_{\pi,t,4}$ instead of the formalization of security in Definition 1 is well explained by Proposition 4 below.

Proposition 4 *The formalization of security in Definition 1 for a symmetric-key encryption protocol π in the multiple-use model is lower-and-upper bounded as follows:*

$$\max(\alpha_{\pi,t,4}, \beta_{\pi,t,2}) \leq \inf_{\sigma} \Delta^{\mathcal{D}}(\pi((\bullet\!\!\longrightarrow)^t \| \ [P_K]), \sigma((\bullet\!\!\longrightarrow\!\!\bullet)^t)) \leq \alpha_{\pi,t,4} + \beta_{\pi,t,2}.$$

Proof. The proof can be shown in a way similar to that of Proposition 2. However, for completeness, we give it below.

By focusing on distributions of input at A-interface, output at B-interface and output at E-interface, for simplicity, we identify the following two formalizations:

$$\inf_{\sigma} \Delta^{\mathcal{D}}(\pi((\bullet\!\!\longrightarrow)^t \| \ [P_K]), \sigma((\bullet\!\!\longrightarrow\!\!\bullet)^t)) \quad \text{and}$$
$$\inf_{P_{Q_1Q_2\cdots Q_t}} \sup_{P_{M_1M_2\cdots M_t}} \Delta(P_{M_1\tilde{M}_1C_1, M_2\tilde{M}_2C_2, \ldots, M_t\tilde{M}_tC_t}, P_{M_1M_1Q_1, M_2M_2Q_2, \ldots, M_tM_tQ_t}),$$

where for every $i \leq t$, M_i may depend on the information which a distinguisher obtained before (e.g., $M_1\tilde{M}_1C_1, M_2\tilde{M}_2C_2, \ldots, M_{i-1}\tilde{M}_{i-1}C_{i-1}$), and Q_i depends only on $Q_1, Q_2, \ldots, Q_{i-1}$.

For any distributions $P_{M_1M_2\cdots M_t} \in \wp(\mathcal{M}^t)$ and $P_{Q_1Q_2\cdots Q_t} \in \wp(\mathcal{C}^t)$, we have

$$\begin{aligned}
&\Delta(P_{M_1\tilde{M}_1C_1, M_2\tilde{M}_2C_2, \ldots, M_t\tilde{M}_tC_t}, P_{M_1M_1Q_1, M_2M_2Q_2, \ldots, M_tM_tQ_t}) \\
&\leq \Delta(P_{M_1\tilde{M}_1C_1, M_2\tilde{M}_2C_2, \ldots, M_t\tilde{M}_tC_t}, P_{M_1M_1C_1, M_2M_2C_2, \ldots, M_tM_tC_t}) \\
&\quad + \Delta(P_{M_1M_1C_1, M_2M_2C_2, \ldots, M_tM_tC_t}, P_{M_1M_1Q_1, M_2M_2Q_2, \ldots, M_tM_tQ_t}) \\
&= \Delta(P_{M_1\tilde{M}_1, M_2\tilde{M}_2, \ldots, M_t\tilde{M}_t}, P_{M_1M_1, M_2M_2, \ldots, M_tM_t}) \\
&\quad + \Delta(P_{M_1C_1, M_2C_2, \ldots, M_tC_t}, P_{M_1Q_1, M_2Q_2, \ldots, M_tQ_t})
\end{aligned}$$

By taking the supremum over all $P_{M_1M_2\cdots M_t} \in \wp(\mathcal{M}^t)$ and the infimum over all $P_{Q_1Q_2\cdots Q_t} \in \wp(\mathcal{C}^t)$, we have

$$\inf_{\sigma} \Delta^{\mathcal{D}}(\pi((\bullet\!\!\longrightarrow)^t \| \ [P_K]), \sigma((\bullet\!\!\longrightarrow\!\!\bullet)^t)) \leq \alpha_{\pi,t,4} + \beta_{\pi,t,2}.$$

In addition, it is easy to see that $\max(\alpha_{\pi,t,4}, \beta_{\pi,t,2}) \leq \inf_{\sigma} \Delta^{\mathcal{D}}(\pi((\bullet\!\!\longrightarrow)^t \| \ [P_K]), \sigma((\bullet\!\!\longrightarrow\!\!\bullet)^t))$ by Proposition 7 in Appendix A. $\square$

One may think of a little difference in the adversary's (or distinguisher's) choice of random variables $M_1, M_2, \ldots, M_t$ in the formalizations in Definition 5: In (I) and (II), M_i may depend on previous ones, say $M_1\tilde{M}_1, M_2\tilde{M}_2, \ldots, M_{i-1}\tilde{M}_{i-1}$; In (i), (ii) and (iv), M_i may depend on $M_1C_1, M_2C_2, \ldots, M_{i-1}C_{i-1}$; and in the formalization of security in Definition 1, M_i may depend on the information which the distinguisher obtained before (e.g., $M_1\tilde{M}_1C_1, M_2\tilde{M}_2C_2, \ldots, M_{i-1}\tilde{M}_{i-1}C_{i-1}$). However, we eventually take the supremum over all $P_{M_1M_2\cdots M_t} \in \wp(\mathcal{M}^t)$ for all the formalizations, and the above difference does not have any effect on the results in this paper.

Even in the multiple-use model, we next show equivalence between security formalizations of Type (i, j) for $i \in \{1, 2, 3\}$ and $j \in \{1, 2, \ldots, 5\}$ as follows.

Theorem 3 *Let π be a multiple-use symmetric-key encryption protocol where the number of protocol execution with a same secret-key is up to T. Then, we have explicit relationships between $\alpha_{\pi,t,i}$, $\beta_{\pi,t,j}$ for any $i \in \{1, 2, \ldots, 5\}$, $j \in \{1, 2, 3\}$ and $t \in \{1, 2, \ldots, T\}$ as follows:*

$$\begin{aligned}
&\beta_{\pi,t,1} = \beta_{\pi,t,2} = \beta_{\pi,t,3}, \ \textit{and} \\
&\frac{1}{4}\alpha_{\pi,t,2} \leq \alpha_{\pi,t,4} = \alpha_{\pi,t,5} \leq \alpha_{\pi,t,3} \leq 2\alpha_{\pi,t,2}, \quad \frac{2}{\ln 2}\alpha_{\pi,t,2}^2 \leq \alpha_{\pi,t,1} \leq -2\alpha_{\pi,t,2} \log \frac{2\alpha_{\pi,t,2}}{|\mathcal{M}|^t \ |\mathcal{C}|^t}.
\end{aligned}$$

In particular, for any $t \in \{1, 2, \ldots, T\}$, any $i, j \in \{1, 2, \ldots, 5\}$, and any $s, u \in \{1, 2, 3\}$, we have

$$\lim_{(\beta_{\pi,t,s}, \alpha_{\pi,t,i}) \to (0,0)} (\beta_{\pi,t,u}, \alpha_{\pi,t,j}) = (0, 0),$$

where the limit is taken by changing $[P_K]$ or π.

Proof. The proof can be shown by extending that of Theorem 1, and it is given in Appendix B. □

Furthermore, we extend the lower bounds in Section 3.3 to the ones in the multiple-use model.

Lemma 1 *Let π be a multiple-use symmetric-key encryption protocol where the number of protocol execution with a same secret-key is t. Also, let $P_{M_1, M_2, \ldots, M_t}$ be a distribution on $\mathcal{M}^t$. Then, for any simulator σ on $\mathcal{C}$, there exists a distinguisher D which utilizes $P_{M_1, M_2, \ldots, M_t}$ for distinguishing advantage such that*

$$\Delta^D(\pi((\bullet\!\!\longrightarrow)^t || \ [P_K]), \sigma((\bullet\!\!\longrightarrow\!\!\bullet)^t)) \geq 1 - \frac{|\mathcal{K}|}{2^{H_\infty(M_1, M_2, \ldots, M_t)}}. \tag{1}$$

In particular, for any simulator σ on $\mathcal{C}$, and for the set of all distinguishers $\mathcal{D}$, we have

$$\Delta^{\mathcal{D}}(\pi((\bullet\!\!\longrightarrow)^t || \ [P_K]), \sigma((\bullet\!\!\longrightarrow\!\!\bullet)^t)) \geq 1 - \frac{|\mathcal{K}|}{|\mathcal{M}|^t}.$$

The inequality (1) is an extension of the lower bound in [25] (see Proposition 3). Actually, if we assume that $t = 1$ and P_{M_1} is uniform in Lemma 1, we obtain Proposition 3. The proof of Lemma 1 is given in Appendix C. From Lemma 1, we obtain the following lower bounds (The proofs are very similar to those in Section 3.3).

Theorem 4 *For any multiple-use symmetric-key encryption protocol π where the number of protocol execution with a same secret-key is t, we have the following lower bounds:*

$$\begin{aligned}
&(i) \quad \sqrt{\frac{\ln 2}{2}} \alpha_{\pi,t,1}^{\frac{1}{2}} + \beta_{\pi,t,j} \geq \frac{1}{2}\left(1 - \frac{|\mathcal{K}|}{|\mathcal{M}|^t}\right) \ \textit{for } j \in \{1, 2, 3\}; \\
&(ii) \quad \alpha_{\pi,t,2} + \beta_{\pi,t,j} \geq \frac{1}{2}\left(1 - \frac{|\mathcal{K}|}{|\mathcal{M}|^t}\right) \ \textit{for } j \in \{1, 2, 3\}; \\
&(iii) \quad \alpha_{\pi,t,i} + \beta_{\pi,t,j} \geq 1 - \frac{|\mathcal{K}|}{|\mathcal{M}|^t} \ \textit{for } i \in \{3, 4, 5\} \textit{ and } j \in \{1, 2, 3\},
\end{aligned}$$

where $\alpha_{\pi,t,i}$ and $\beta_{\pi,j}$ are parameters for secrecy and correctness, respectively, defined in Definition 5.

Corollary 2 *Suppose a symmetric-key encryption protocol π is (δ, ϵ, T)-secure in the sense of Type (i, j) in the multiple-use model. Then, we have the following lower bounds for the size of secret-keys:*

$$\begin{aligned}
&(i) \quad |\mathcal{K}| \geq \left\{1 - \left(\sqrt{2\ln 2}\epsilon^{\frac{1}{2}} + 2\delta\right)\right\} |\mathcal{M}|^T \ \textit{ for } j = 1 \textit{ and } i \in \{1, 2, 3\}, \\
&(ii) \quad |\mathcal{K}| \geq \{1 - 2(\epsilon + \delta)\} |\mathcal{M}|^T \ \textit{ for } j = 2 \textit{ and } i \in \{1, 2, 3\}, \\
&(iii) \quad |\mathcal{K}| \geq \{1 - (\epsilon + \delta)\} |\mathcal{M}|^T \ \textit{ for } j \in \{3, 4, 5\} \textit{ and } i \in \{1, 2, 3\}.
\end{aligned}$$

By considering a contrapositive of Corollary 2, we obtain the following impossibility result: There exists no symmetric-key encryption protocol which is (δ, ϵ, T)-secure in the sense of Type (i, j) in the multiple-use model, if δ and ϵ are some real numbers such that they do not satisfy the corresponding inequality among (i)-(iii) in Corollary 2.

4 Key Agreement

4.1 Protocol Execution

We explain protocol execution of key agreement. Let $\mathcal{X}$ and $\mathcal{Y}$ be finite sets. Suppose that Alice and Bob can have access to an ideal resource, and that they can finally obtain $x \in \mathcal{X}$ and $y \in \mathcal{Y}$, respectively. For simplicity, suppose that the resource is given by a correlated randomness resource $[P_{XY}]$. In addition, we assume that there is the bidirectional (or unidirectional) authenticated channel available between Alice and Bob, and that Eve can eavesdrop on all information transmitted by the channel without any error.

Let $\mathcal{K}$ be a set of keys, and let K be a random variable which takes values on $\mathcal{K}$ in $\bullet\!\!=\!\!=\!\!\bullet$ (or more generally, $[P_K]$). Also, let $\mathcal{T}$ be a set of transcripts between Alice and Bob. Let $\pi_{ka} = (\pi_{ka}^A, \pi_{ka}^B)$ be a key agreement protocol, where π_{ka}^A (resp. π_{ka}^B) is a converter at Alice's (resp. Bob's) side, defined below: Let l be a positive integer and $n = 2l-1$; The converter π_{ka}^A consists of (probabilistic) functions $f_1, f_3, f_5, \ldots, f_{2l-1}$ and g_A, and the converter π_{ka}^B consists of (probabilistic) functions $f_2, f_4, f_6, \ldots, f_{2l-2}$ and g_B, where the functions $f_1, f_2, \ldots, f_n, g_A, g_B$ are defined as follows:

$$f_i : \mathcal{X} \times \mathcal{T}^{i-1} \to \mathcal{T},\ t_i = f_i(x, t_1, t_2, t_3, \ldots, t_{i-1}) \text{ for } i = 1, 3, \ldots, 2l-1;$$
$$f_j : \mathcal{Y} \times \mathcal{T}^{j-1} \to \mathcal{T},\ t_j = f_j(y, t_1, t_2, t_3, \ldots, t_{j-1}) \text{ for } j = 2, 4, \ldots, 2l-2;$$
$$g_A : \mathcal{X} \times \mathcal{T}^n \to \mathcal{K},\ k_A = g_A(x, t_1, t_2, t_3, \ldots, t_n); \quad g_B : \mathcal{Y} \times \mathcal{T}^n \to \mathcal{K},\ k_B = g_B(y, t_1, t_2, t_3, \ldots, t_n).$$

Key Agreement Protocol π_{ka}

Input of Alice's inner interface: $x \in \mathcal{X}$ by accessing $[P_{XY}]$
Input of Bob's inner interface: $y \in \mathcal{Y}$ by accessing $[P_{XY}]$
Output of Alice's outer interface: $k_A \in \mathcal{K}$
Output of Bob's outer interface: $k_B \in \mathcal{K}$

1. π_{ka}^A computes $t_1 = f_1(x)$ and sends t_1 to π_{ka}^B by $\bullet\!\!\longrightarrow$.
2. For k from 1 to $(n-1)/2$,
   2-1. π_{ka}^B computes $t_{2k} = f_{2k}(y, t_1, t_2, \ldots, t_{2k-1})$. Then, π_{ka}^B sends t_{2k} to π_{ka}^A by $\longleftarrow\!\!\bullet$.
   2-2. π_{ka}^A computes $t_{2k+1} = f_{2k+1}(x, t_1, t_2, \ldots, t_{2k})$. Then, π_{ka}^A sends t_{2k+1} to π_{ka}^B by $\bullet\!\!\longrightarrow$.
3. π_{ka}^A computes $k_A = g_A(x, t_1, t_2, \ldots, t_n)$ and outputs k_A.
   Similarly, π_{ka}^B computes $k_B = g_B(y, t_1, t_2, \ldots, t_n)$ and outputs k_B.

Note that, if only the unidirectional authenticated channel from Alice to Bob is available, the functions f_i for even i could be understood as trivial functions which always return a certain single point (or symbol). Similarly, we can capture the case of only the unidirectional authenticated channel from Bob to Alice being available.

For every i with $1 \le i \le n$, T_i denotes a random variable which takes values $t_i \in \mathcal{T}$, and let $T^n := (T_1, T_2, \ldots, T_n)$ be the joint random variable which takes values $t^n = (t_1, t_2, \ldots, t_n) \in \mathcal{T}^n$. Also, let K_A and K_B be the random variables which take values $k_A \in \mathcal{K}$ and $k_B \in \mathcal{K}$, respectively.

For simplicity, we assume that a key agreement protocol π_{ka} can be used at most one time (i.e., we deal with key agreement protocols in the one-time model). Therefore, the purpose of the key agreement protocol is to transform a correlated randomness resource $[P_{XY}]$ and channels $(\bullet\!\!\longrightarrow)^l \parallel (\longleftarrow\!\!\bullet\ )^{l-1}$ into a key sharing resource $\bullet\!\!=\!\!=\!\!\bullet$ (or more generally, $[P_K]$).

4.2 Security Definitions Revisited: Formalizations and Relationships

As in the case of symmetric-key encryption protocols, let's consider the following traditional formalization of security for key agreement protocols (e.g. [8, 9, 11, 16, 17, 22]).

Definition 6 Let π be a key agreement protocol. Then, π is said to be *ϵ-secure* if it satisfies the following conditions:

$$P(K_A \neq K_B) \leq \epsilon, \ \log|\mathcal{K}| - H(K_A) \leq \epsilon, \ \text{and } I(K_A; T^n) \leq \epsilon.$$

In particular, π is said to be *perfectly-secure* if it is 0-secure.

We now consider the following formalizations of information-theoretic security for key agreement.

Definition 7 Let π be a key agreement protocol such that P_K is the uniform distribution over $\mathcal{K}$ (i.e., $[P_K]=\bullet\!\!=\!\!=\!\!\bullet$). We define the following formalizations of Correctness and Security.

1. Correctness: (I) $\beta_{\pi,1} := \max(P(K_A \neq K_B), \log|\mathcal{K}| - H(K_A))$,
   (II) $\beta_{\pi,2} := \Delta(P_{K_A K_B}, P_{KK})$.
2. Security: (i) $\alpha_{\pi,1} := I(K_A; T^n)$, (ii) $\alpha_{\pi,2} := \Delta(P_{K_A T^n}, P_{K_A} P_{T^n})$,
   (iii) $\alpha_{\pi,3} := \inf_{P_Q} \Delta(P_{K_A T^n}, P_{K_A} P_Q)$, where the infimum ranges over all $P_Q \in \wp(\mathcal{T}^n)$.

Then, π is said to be *(δ,ϵ)-secure in the sense of Type (i,j)*, if π satisfies $\beta_{\pi,i} \leq \delta$ and $\alpha_{\pi,j} \leq \epsilon$.

The traditional definition in Definition 6 corresponds to the security in the sense of Type $(1,1)$. The composable security by Maurer et al. [19, 21] and Canetti [5, 6] is closely related to the security in the sense of Type $(2,3)$: $\beta_{\pi,2}$ means distinguisher's advantage for distinguishing real output and ideal one at honest players' interfaces, and $\beta_{\pi,2}$ is the same as the formalization of availability in Definition 1 for key agreement; $\alpha_{\pi,3}$ means distinguisher's advantage for distinguishing real transcripts and simulator's output at E-interface, together with output at A-interface. Note that the formalization $\alpha_{\pi,3}$ is simple, and validity of $\alpha_{\pi,3}$ is well explained by the following proposition.

Proposition 5 *The formalization of security in Definition 1 for a key agreement protocol π is lower-and-upper bounded as follows:*

$$\max\left(\frac{1}{3}\alpha_{\pi,3}, \beta_{\pi,2}\right) \leq \inf_{\sigma} \Delta^{\mathcal{D}}(\pi((\bullet\!\!\longrightarrow)^l \| (\longleftarrow\!\!\bullet)^{l-1} \| \ [P_{XY}]), \sigma(\bullet\!\!=\!\!=\!\!\bullet)) \leq \alpha_{\pi,3} + 2\beta_{\pi,2}.$$

Proof. By focusing on distributions of output at A's, B's and E's interfaces, for simplicity, we write $\inf_{P_Q} \Delta(P_{K_A K_B T^n}, P_{KK} P_Q)$ for $\inf_\sigma \Delta^{\mathcal{D}}(\pi((\bullet\!\!\longrightarrow)^l \| (\longleftarrow\!\!\bullet)^{l-1} \| \ [P_{XY}]), \sigma(\bullet\!\!=\!\!=\!\!\bullet))$, where P_K is the uniform distribution over $\mathcal{K}$.

For any distribution $P_Q \in \wp(\mathcal{C})$, we have

$$\begin{aligned}
\Delta(P_{K_A K_B T^n}, P_{KK} P_Q) &\leq \Delta(P_{K_A K_B T^n}, P_{K_A K_A T^n}) + \Delta(P_{K_A K_A T^n}, P_{K_A K_A} P_Q) \\
&\quad + \Delta(P_{K_A K_A} P_Q, P_{KK} P_Q) \\
&= P(K_A \neq K_B) + \Delta(P_{K_A T^n}, P_{K_A} P_Q) + \Delta(P_{K_A}, P_K) \\
&\leq \Delta(P_{K_A T^n}, P_{K_A} P_Q) + 2\Delta(P_{K_A K_B}, P_{KK}).
\end{aligned}$$

By taking the infimum over all $P_Q \in \wp(\mathcal{T}^n)$, we have

$$\begin{aligned}
\inf_{P_Q} \Delta(P_{K_A K_B T^n}, P_{KK} P_Q) &\leq \inf_{P_Q} \Delta(P_{K_A T^n}, P_{K_A} P_Q) + 2\Delta(P_{K_A K_B}, P_{KK}) \\
&= \alpha_{\pi,3} + 2\beta_{\pi,2}.
\end{aligned}$$

In addition, for any distribution $P_Q \in \wp(\mathcal{C})$ we have

$$\begin{aligned}
\Delta(P_{K_A T^n}, P_{K_A} P_Q) &\leq \Delta(P_{K_A K_A T^n}, P_{K_A K_B T^n}) + \Delta(P_{K_A K_B T^n}, P_{KK} P_Q) + \Delta(P_{KK} P_Q, P_{K_A K_A} P_Q) \\
&= P(K_A \neq K_B) + \Delta(P_{K_A K_B T^n}, P_{KK} P_Q) + \Delta(P_K, P_{K_A}) \\
&\leq 2\Delta(P_{K_A K_B}, P_{KK}) + \Delta(P_{K_A K_B T^n}, P_{KK} P_Q) \\
&\leq 3\Delta(P_{K_A K_B T^n}, P_{KK} P_Q).
\end{aligned}$$

By taking the infimum over all $P_Q \in \wp(\mathcal{T}^n)$, we have

$$\frac{1}{3}\alpha_{\pi,3} \leq \inf_{P_Q} \Delta(P_{K_A K_B T^n}, P_{KK} P_Q).$$

Finally, it is straightforward to see that $\beta_{\pi,2} \leq \inf_{P_Q} \Delta(P_{K_A K_B T^n}, P_{KK} P_Q)$. $\square$

Then, as in the case of symmetric-key encryption, we can show the following theorem which states essential equivalence of all the formalizations (i.e., six possible formalizations above).

Theorem 5 *Let π be a key agreement protocol such that P_K is the uniform distribution over $\mathcal{K}$. Then, we have explicit relationships between $\alpha_{\pi,i}$, $\beta_{\pi,j}$ for $i \in \{1,2,3\}$, $j \in \{1,2\}$ as follows:*

$$\begin{aligned}
&(1) \quad \beta_{\pi,2} \leq \beta_{\pi,1} + \sqrt{\frac{\beta_{\pi,1} \ln 2}{2}} \quad \textit{and} \quad \beta_{\pi,1} \leq -2\beta_{\pi,2} \log \frac{2\beta_{\pi,2}}{|\mathcal{K}|}, \\
&(2) \quad \frac{2}{\ln 2}\alpha_{\pi,2}^2 \leq \alpha_{\pi,1} \leq -2\alpha_{\pi,2} \log \frac{2\alpha_{\pi,2}}{|\mathcal{K}||\mathcal{T}|^n}, \quad (3) \alpha_{\pi,3} \leq \alpha_{\pi,2} \leq 2\alpha_{\pi,3}.
\end{aligned}$$

In particular, for any $i, j \in \{1,2,3\}$ and for any $s, t \in \{1,2\}$, we have

$$\lim_{(\beta_{\pi,s}, \alpha_{\pi,i}) \to (0,0)} (\beta_{\pi,t}, \alpha_{\pi,j}) = (0,0),$$

where the limit is taken by changing $[P_{XY}]$ or π.

Proof. First, we show (1): By Lemma 3 in Appendix A, we have

$$\begin{aligned}
\beta_{\pi,2} &= \Delta(P_{K_A K_B}, P_{KK}) \\
&\leq P(K_A \neq K_B) + \min(\Delta(P_{K_A}, P_K), \Delta(P_{K_B}, P_K)).
\end{aligned}$$

In addition, by Proposition 9 in Appendix A we have

$$\begin{aligned}
\Delta(P_{K_A}, P_K)^2 &\leq \frac{\ln 2}{2} D(P_{K_A} || P_K) \\
&= \frac{\ln 2}{2} (\log |\mathcal{K}| - H(K_A)) \\
&\leq \frac{\ln 2}{2} \beta_{\pi,1}.
\end{aligned}$$

Therefore, we have $\beta_{\pi,2} \leq \beta_{\pi,1} + \sqrt{\frac{\beta_{\pi,1} \ln 2}{2}}$.

Conversely, we have

$$\begin{aligned}
P(K_A \neq K_B) &\leq \beta_{\pi,2}, \text{ and} \\
\log |\mathcal{K}| - H(K_A) &\leq -2\Delta(P_{K_A}, P_K) \log \frac{2\Delta(P_{K_A}, P_K)}{|\mathcal{K}|} \qquad (2) \\
&\leq -2\beta_{\pi,2} \log \frac{2\beta_{\pi,2}}{|\mathcal{K}|},
\end{aligned}$$

where (2) follows from Proposition 10. Thus, we obtain

$$\beta_{\pi,1} \le -2\beta_{\pi,2} \log \frac{2\beta_{\pi,2}}{|\mathcal{K}|}.$$

Next, the proof of (2) is given in the same way as that of Theorem 1, and we omit it.

Finally, we show (3): By definition, we have $\alpha_{\pi,3} \le \alpha_{\pi,2}$. In addition, for any $\epsilon > 0$, there is a distribution P_Q such that $\alpha_{\pi,3} + \epsilon \ge \Delta(P_{K_A T^n}, P_{K_A} P_Q)$. Then, we have

$$\begin{aligned} \alpha_{\pi,2} &\le \Delta(P_{K_A T^n}, P_{K_A} P_Q) + \Delta(P_{K_A} P_Q, P_{K_A} P_{T^n}) \\ &\le \alpha_{\pi,3} + \epsilon + \Delta(P_Q, P_{T^n}) \\ &\le 2(\alpha_{\pi,3} + \epsilon), \end{aligned}$$

where the last inequality follows from $\Delta(P_Q, P_{T^n}) \le \Delta(P_{K_A} P_Q, P_{K_A T^n}) \le \alpha_{\pi,3} + \epsilon$. Thus, we obtain $\alpha_{\pi,2} \le 2\alpha_{\pi,3}$. $\square$

4.3 Lower Bounds and Impossibility Results in One-time Model

For any key agreement protocol which constructs a key sharing resource $[P_K]$ starting from a correlated randomness resource $[P_{XY}]$, we show a lower bound on the advantage of distinguishers as follows. The proof is given in Appendix D.

Lemma 2 *Let $[P_K]$ be a key sharing resource. For any key agreement protocol π, and for any simulator σ, we have*

$$\Delta^{\mathcal{D}}(\pi((\bullet\!\!\longrightarrow)^l \| (\longleftarrow\!\!\bullet)^{l-1} \| \ [P_{XY}]), \sigma([P_K])) \ge 1 - 2^{H_0(X,Y) - H_\infty(K)}.$$

In particular, we have

$$\Delta^{\mathcal{D}}(\pi((\bullet\!\!\longrightarrow)^l \| (\longleftarrow\!\!\bullet)^{l-1} \| \ [P_{XY}]), \sigma(\bullet\!\!=\!\!=\!\!\bullet)) \ge 1 - \frac{2^{H_0(X,Y)}}{|\mathcal{K}|}.$$

From Lemma 2, we obtain lower bounds of the adversary's (or distinguisher's) advantage (Theorem 6) and the required size of a correlated randomness resource (Corollary 3) as follows.

Theorem 6 *For any key agreement protocol π such that P_K is the uniform distribution over $\mathcal{K}$, we have the following lower bounds:*

$$(i) \quad \sqrt{\frac{\ln 2}{2}} \alpha_{\pi,1}^{\frac{1}{2}} + 2\left(1 + \sqrt{\frac{\ln 2}{2}}\right) \beta_{\pi,1}^{\frac{1}{2}} \ge 1 - \frac{2^{H_0(X,Y)}}{|\mathcal{K}|}, \quad \textit{if } \beta_{\pi,1} \in [0,1];$$

$$(ii) \quad \alpha_{\pi,i} + 2\left(1 + \sqrt{\frac{\ln 2}{2}}\right) \beta_{\pi,1}^{\frac{1}{2}} \ge 1 - \frac{2^{H_0(X,Y)}}{|\mathcal{K}|} \quad \textit{for } i \in \{2,3\}, \textit{ if } \beta_{\pi,1} \in [0,1];$$

$$(iii) \quad \sqrt{\frac{\ln 2}{2}} \alpha_{\pi,1}^{\frac{1}{2}} + 2\beta_{\pi,2} \ge 1 - \frac{2^{H_0(X,Y)}}{|\mathcal{K}|}; \quad (iv) \quad \alpha_{\pi,i} + 2\beta_{\pi,2} \ge 1 - \frac{2^{H_0(X,Y)}}{|\mathcal{K}|} \quad \textit{for } i \in \{2,3\},$$

where $\alpha_{\pi,i}$ and $\beta_{\pi,j}$ are parameters for security and correctness, respectively, defined in Definition 7.

Proof. By Proposition 5, we have

$$\inf_{\sigma} \Delta^{\mathcal{D}}(\pi((\bullet\!\!\longrightarrow)^l \| (\longleftarrow\!\!\bullet)^{l-1} \| \ [P_{XY}]), \sigma(\bullet\!\!=\!\!=\!\!\bullet)) \le \alpha_{\pi,3} + 2\beta_{\pi,2}. \tag{3}$$

Therefore, by (3) and Lemma 2 we obtain

$$\alpha_{\pi,3} + 2\beta_{\pi,2} \geq 1 - \frac{2^{H_0(X,Y)}}{|\mathcal{K}|}.$$

From Theorem 5, we have explict relationships between $\alpha_{\pi,i}$ and $\beta_{\pi,j}$ as follows:

$$\begin{aligned} \beta_{\pi,2} &\leq \beta_{\pi,1} + \sqrt{\frac{\ln 2}{2}}\beta_{\pi,1}^{\frac{1}{2}} \\ &\leq \left(1+\sqrt{\frac{\ln 2}{2}}\right)\beta_{\pi,1}^{\frac{1}{2}} \text{ if } \beta_{\pi,1} \in [0,1]; \\ \alpha_{\pi,3} &\leq \alpha_{\pi,2} \leq \sqrt{\frac{\ln 2}{2}}\alpha_{\pi,1}^{\frac{1}{2}}. \end{aligned}$$

Therefore, by combining the above inequalities we obtain all lower bounds in Theorem 6. □

Corollary 3 *Suppose that a key agreement protocol π is (δ, ϵ)-secure in the sense of Type (i,j) in which P_K is the uniform distribution over $\mathcal{K}$. Then, we have the following lower bounds for the size of a correlated randomness resource:*

$$(i) \quad 2^{H_0(X,Y)} \geq \left\{1 - \left[\sqrt{\frac{\ln 2}{2}}\epsilon^{\frac{1}{2}} + 2\left(1+\sqrt{\frac{\ln 2}{2}}\right)\delta^{\frac{1}{2}}\right]\right\}|\mathcal{K}| \text{ for } i=j=1, \text{ if } \delta \in [0,1];$$

$$(ii) \quad 2^{H_0(X,Y)} \geq \left\{1 - \left[\epsilon + 2\left(1+\sqrt{\frac{\ln 2}{2}}\right)\delta^{\frac{1}{2}}\right]\right\}|\mathcal{K}| \text{ for } i=1 \text{ and } j \in \{2,3\}, \text{ if } \delta \in [0,1];$$

$$(iii) \quad 2^{H_0(X,Y)} \geq \left\{1 - \left(\sqrt{\frac{\ln 2}{2}}\epsilon^{\frac{1}{2}} + 2\delta\right)\right\}|\mathcal{K}| \text{ for } i=2 \text{ and } j=1;$$

$$(iv) \quad 2^{H_0(X,Y)} \geq \{1 - (\epsilon + 2\delta)\}|\mathcal{K}| \text{ for } i=2 \text{ and } j \in \{2,3\}.$$

Proof. The proof of Corollary 3 immediately follows from Theorem 6. □

Finally, from Lemma 2 we obtain Proposition 6 which is an impossibility result for key agreement. Also, we provide Corollaries 4 and 5 below, as illustrations of impossibility results which are special cases of Proposition 6 (The proofs immediately follow from Theorem 6 and Proposition 6).

Proposition 6 *Let $[P_K]$ be a key sharing resource, and let $[P_{XY}]$ be a correlated randomness resource. In addition, let $\hat{\epsilon}$ be a real number such that $\hat{\epsilon} < 1 - 2^{H_0(X,Y) - H_\infty(K)}$. Then, there exists no key agreement protocol π such that $(\bullet\!\!\longrightarrow)^\infty \| (\longleftarrow\!\!\bullet)^\infty \| \, [P_{XY}] \overset{\pi,\hat{\epsilon}}{\Longrightarrow} [P_K]$.*

Corollary 4 *There is no key agreement protocol π such that $(\bullet\!\!\longrightarrow)^\infty \| (\longleftarrow\!\!\bullet)^\infty \overset{\pi,\hat{\epsilon}}{\Longrightarrow} [P_K]$ for $\hat{\epsilon} < 1 - 1/2^{H_\infty(K)}$. In particular, there is no (δ,ϵ)-secure key agreement in the sense of Type (i,j) which constructs $\bullet\!\!\Longleftrightarrow\!\!\bullet$ (even with 1-bit) starting from authenticated communications, if $\delta, \epsilon \in [0,1]$ are some real numbers such that:*

$$(i) \quad \sqrt{\frac{\ln 2}{2}}\epsilon^{\frac{1}{2}} + 2\left(1+\sqrt{\frac{\ln 2}{2}}\right)\delta^{\frac{1}{2}} < \frac{1}{2} \text{ for } i=j=1;$$

$$(ii) \quad \epsilon + 2\left(1+\sqrt{\frac{\ln 2}{2}}\right)\delta^{\frac{1}{2}} < \frac{1}{2} \text{ for } i=1 \text{ and } j \in \{2,3\};$$

$$(iii) \quad \sqrt{\frac{\ln 2}{2}}\epsilon^{\frac{1}{2}} + 2\delta < \frac{1}{2} \text{ for } i=2 \text{ and } j=1;$$

$$(iv) \quad \epsilon + 2\delta < \frac{1}{2} \text{ for } i=2 \text{ and } j \in \{2,3\}.$$

Corollary 5 *Let l and s be nonnegative integers with $l < s$. In addition, we denote the l-bit key sharing resource by $\bullet\!\!=\!\!=\!\!\bullet_l$, and let $[P_K]_s$ be an s-bit key sharing resource with min-entropy $H_\infty(K)$. Then, there is no protocol π such that* $(\bullet\!\!\longrightarrow)^\infty \| (\longleftarrow\!\!\bullet)^\infty \| \bullet\!\!=\!\!=\!\!\bullet_l \overset{\pi,\hat{\epsilon}}{\Longrightarrow} [P_K]_s$ *for $\hat{\epsilon} < 1 - 2^{l-H_\infty(K)}$. In particular, there is no (δ, ϵ)-secure key agreement (or key-expansion) protocol in the sense of Type (i, j) which constructs the s-bit key sharing resource $\bullet\!\!=\!\!=\!\!\bullet_s$ from the l-bit key sharing resource $\bullet\!\!=\!\!=\!\!\bullet_l$, if $\delta, \epsilon \in [0, 1]$ are some real numbers which satisfy inequality in Corollary 4.*

5 Conclusion

In this paper, we investigated relationships between formalizations of information-theoretic security for symmetric-key encryption and key-agreement protocols in a general setting (i.e., encryption and key-agreement protocols may have decryption-errors and agreement-errors, respectively). Specifically, we showed that, for symmetric-key encryption, the following formalizations are essentially all equivalent in both one-time and multiple-use models:

- Stand-alone security including formalizations of extended (or relaxed) Shannon's secrecy using mutual information and statistical distance, and that of information-theoretic indistinguishability by Goldwasser and Micali; and
- Composable security including formalizations of Maurer et al. and Canetti.

In the both models, we also derived lower bounds of the adversary's (or distinguisher's) advantage and secret-key size required under all of the above formalizations. In particular, we could derive them all at once through our relationships between the formalizations. In addition, we briefly observed impossibility results which easily follow from the lower bounds.

Furthermore, we showed similar results (i.e., relationships between formalizations of stand-alone and composable security, lower bounds, and impossibility results) for key agreement protocols.

Our technical results above are summarized in Table 1 in Section 1.

Acknowledgements. I would like to thank Ueli Maurer for introducing and explaining me his framework of constructive cryptography and its related topics. Motivated by discussion with him when I was visiting ETH Zürich, Switzerland, I started this work. I would also like to thank Mitsugu Iwamoto for giving me the information on his recent work [14] and fruitful discussion on an earlier version of this paper. Finally, I would like to thank anonymous reviewers for helpful comments on an earlier version of this paper.

References

[1] M. Backes, J. Müller-Quade, and D. Unruh, *On the Necessity of Rewinding in Secure Multiparty Computation*, Proc. of TCC 2007, pp.157-173, Springer, 2007.

[2] M. Backes, B. Pfitzmann, M. Waindner, *A Universally Composable Cryptographic Library*, IACR Cryptology ePrint Archive, 2003. `http://eprint.iacr.org/2003/015`

[3] D. Beaver, *Secure Multiparty Protocols and Zero-knowledge proof Systems Tolerating a Faulty Minority*, J. Cryptology, 4, pp.75-122, 1991.

[4] M. Bellare, S. Tessaro, and A. Vardy, *A Cryptographic Treatment of the Wiretap Channel*, IACR Cryptology ePrint Archive: `http://eprint.iacr.org/2012/015`

[5] R. Canetti, *Security and Composition of Multiparty Cryptographic Protocols*, J. Cryptology, 13, pp.143-202, 2000.

[6] R. Canetti, *Universally Composable Security: A New Paradigm for Cryptographic Protocols*, Proc. of the 42nd IEEE Symposium on Foundations of Computer Science (FOCS 2001), pp.136-145, 2001. IACR Cryptology ePrint Archive (updated version): `http://eprint.iacr.org/2000/067`

[7] T. M. Cover, J. A. Thomas, *Elements of Information Theory*, Wiley-Interscience Publication, John Wiley & Sons, Inc., 1991.

[8] I. Csiszár, *Almost Independence and Secrecy Capacity*, Probl. Pered. Inform. (Special issue devoted to M. S. Pinsker), vol. 32, no. 1, pp. 48-57, 1996.

[9] I. Csiszár and P. Narayan, *Common Randomness and Secret Key Generation with a Helper*, IEEE Trans. on Information Theory, Vol. 46, No. 2, pp.344-366, 1993.

[10] Y. Dodis and S. Micali, *Parallel Reducibility for Information-Theoretically Secure Computation*, Proc. of CRYPTO 2000, pp.74-92, Springer, 2000.

[11] S. Dziembowski and U. Maurer, *On Generating the Initial Key in the Bounded-Storage Model*, Advances in Cryptology - EUROCRYPT 2004, LNCS 3027, pp.126-137, Springer, 2004.

[12] S. Goldwasser, L. Levin, *Fair Computation of General Functions in Presence of Immoral Majority*, CRYPTO'90, LNCS 537, Springer, 1990.

[13] S. Goldwasser and S. Micali, *Probabilistic encryption*, Journal of Computer and System Sciences, vol. 28, no. 2, pp. 270.299, 1984.

[14] M. Iwamoto and K. Ohta, *Security Notions for Information Theoretically Secure Encryptions*, Proc. of 2011 IEEE International Symposium on Information Theory (ISIT 2011), pp.1743-1747, 2011.

[15] E. Kushilevitz, Y. Lindell, and T. Rabin, *Information-Theoretically Secure Protocols and Security Under Composition*, Proc. of the 38th STOC, pp.109-118, 2006. IACR Cryptology ePrint Archive (full version): `http://eprint.iacr.org/2009/630`

[16] U. Maurer, *Secret Key Agreement by Public Discussion From Common Information*, IEEE Trans. on Information Theory, Vol. 39, pp.733-742, 1993.

[17] U. Maurer, *The Strong Secret Key Rate of Discrete Random Triples*, Communications and Cryptography - Two Sides of One Tapestry, Kluwer Academic Publishers, pp. 271-285, 1994.

[18] U. Maurer, *Constructive Cryptography - A Primer*, FC 2010, LNCS 6052, p. 1, Springer, 2010.

[19] U. Maurer and R. Renner, *Abstract Cryptography*, ICS 2011, Tsinghua University Press, pp.1-21, Jan 2011.

[20] U. Maurer, R. Renner, C. Holenstein, *Indifferentiability, Impossibility Results on Reductions, and Applications to the random oracle methodology*, TCC 2004, LNCS 2951, pp.21-39, Springer, 2004.

[21] U. Maurer, B. Tackmann, *On the Soundness of Authenticate-then-Encrypt: Formalizing the Malleability of Symmetric Encryption*, ACM CCS'10, Chicago, Illinois, USA, pp.505-515, 2010.

[22] U. Maurer and S. Wolf, *Secret-Key Agreement over Unauthenticated Public Channels - Part I: Definitions and a Completeness Result*, IEEE Trans. on Information Theory, vol. 49, no. 4, 2003.

[23] S. Micali, P. Rogaway, *Secure Computation*, CRYPTO '91, LNCS 576, pp.392-404, Springer, 1991.

[24] B. Pfitzmann, M. Waidner, *A Model for Asynchronous Reactive Systems and its Application to Secure Message Transmission*, IEEE Symposium on Security and Privacy, pp.184-200, 2001.

[25] G. Pope, *Distinguishing Advantage Lower Bounds for Encryption and Authentication Protocols*, Research project course at the Department of Computer Science, ETH Zurich, 2008.

[26] R. Renner and S. Wolf, *Simple and Tight Bounds for Information Reconciliation and Privacy Amplification*, ASIACRYPT 2005, Springer, 2005.

[27] C. E. Shannon, *Communication theory of secrecy systems*, Bell System Technical Journal, vol. 28, pp. 656-715, 1949.

[28] V. Shoup, *A Computational Introduction to Number Theory and Algebra*, Exercise 8.64 in Chapter 8, page 265, Second Edition, Cambridge University Press, 2009.

Appendix A: Definitions and Inequality

Definition 8 Let X be a random variable which takes values in a finite set $\mathcal{X}$. Then, the min-entropy $H_\infty(X)$ and the max-entropy $H_0(X)$ are defined by

$$H_\infty(X) = \min_{x\in\mathcal{X}}\{-\log P_X(x)\}, \quad H_0(X) = \log|\{x \in \mathcal{X} | P_X(x) > 0\}|.$$

Definition 9 Let X, Y, and Z be random variables associated with distributions P_X, P_Y, and P_Z, respectively. The *mutual information between X and Y*, denoted by $I(X;Y)$, is defined by

$$I(X;Y) := H(X) - H(X|Y),$$

where $H(X)$ (resp. $H(X|Y)$) is the entropy (resp. the conditional entropy). Also, the *conditional mutual information of X and Y given Z*, denoted by $I(X;Y|Z)$, is defined by

$$I(X;Y|Z) := \sum_z P_Z(z) I(X;Y|Z=z).$$

Definition 10 Let X, Y, and Z be random variables associated with distributions P_X, P_Y, and P_Z, respectively, where X and Y take values in a finite set $\mathcal{X}$. The *statistical distance between two distributions P_X and P_Y (or two random variables X and Y)*, denoted by $\Delta(P_X, P_Y)$ (or $\Delta(X,Y)$), is defined by

$$\Delta(P_X, P_Y) := \frac{1}{2}\sum_{x\in\mathcal{X}} |P_X(x) - P_Y(x)|.$$

Also, for conditional probabilities $P_{X|Z} := P_{XZ}/P_Z$ and $P_{Y|Z} := P_{YZ}/P_Z$, the statistical distance between $P_{X|Z}$ and $P_{Y|Z}$, denoted by $\Delta(P_{X|Z}, P_{Y|Z})$ (or $\Delta(X, Y|Z)$), can be defined by

$$\Delta(P_{X|Z}, P_{Y|Z}) := \sum_z P_Z(z)\Delta(P_{X|Z=z}, P_{Y|Z=z}).$$

Then, by definitions, note that $\Delta(P_{X|Z}, P_{Y|Z}) = \Delta(P_{ZX}, P_{ZY})$.

In this section, we describe several inequalities which are necessary to show the proofs of propositions in this paper.

Proposition 7 *Let (X,Y) and (X',Y') be random variables associated with two joint distributions P_{XY} and $P_{X'Y'}$, respectively, on a finite set. Then, we have*

$$\max\left(\Delta(P_X, P_{X'}), \Delta(P_Y, P_{Y'})\right) \leq \Delta(P_{XY}, P_{X'Y'})$$

Proof. From the definition of statistical distance, it follows that

$$\begin{aligned}
2\cdot\Delta(P_{XY}, P_{X'Y'}) &= \sum_x \sum_y |P_{XY}(x,y) - P_{X'Y'}(x,y)| \\
&\geq \sum_x \left|\sum_y P_{XY}(x,y) - \sum_y P_{X'Y'}(x,y)\right| \\
&= \sum_x |P_X(x) - P_{X'}(x)| \\
&= 2\cdot\Delta(P_X, P_{X'}). \ \square
\end{aligned}$$

Proposition 8 *Let X and X' be random variables associated with two distributions P_X and $P_{X'}$, respectively, on a finite set. For an arbitrary random variable Y associated with a distribution P_Y, we have $\Delta(P_{XXY}, P_{XX'Y}) = P(X \neq X')$.*

Proof. The proof follows from the following direct calculation:

$$\begin{aligned}
2\cdot\Delta(P_{XXY}, P_{XX'Y}) &= \sum_x \sum_{x'} \sum_y \left|P_{XXY}(x,x',y) - P_{XX'Y}(x,x',y)\right| \\
&= \sum_x \sum_{x'=x} \sum_y \left|P_{XXY}(x,x',y) - P_{XX'Y}(x,x',y)\right| \\
&\quad + \sum_x \sum_{x'\neq x} \sum_y \left|P_{XXY}(x,x',y) - P_{XX'Y}(x,x',y)\right| \\
&= \sum_x \sum_y (P_{XY}(x,y) - P_{XX'Y}(x,x,y)) + \sum_x \sum_{x'\neq x} \sum_y P_{XX'Y}(x,x',y) \\
&= 1 - P(X = X') + P(X \neq X') \\
&= 2P(X \neq X'). \ \square
\end{aligned}$$

Corollary 6 *Let X and X' be random variables associated with two distributions P_X and $P_{X'}$, respectively, on a finite set. Then, we have $\Delta(P_X, P_{X'}) \leq P(X \neq X')$.*

Proof. The proof follows from Propositions 7 and 8. $\square$

Proposition 9 *[7] Let X_1 and X_2 be random variables associated with two distributions P_{X_1} and P_{X_2}, respectively, on a finite set. Then, we have*

$$D(P_{X_1} \parallel P_{X_2}) \geq \frac{2}{\ln 2}\Delta(P_{X_1}, P_{X_2})^2.$$

Corollary 7 *Let X and Y be random variables associated with two distributions P_X and P_Y, respectively. Then, we have*

$$I(X;Y) \geq \frac{2}{\ln 2}\Delta(P_{XY}, P_X P_Y)^2.$$

Proof. The proof immediately follows from Proposition 9 by setting $P_{X_1} := P_{XY}$ and $P_{X_2} := P_X P_Y$. $\square$

Proposition 10 *[7] Let X_1 and X_2 be random variables associated with two distributions P_{X_1} and P_{X_2}, respectively, on a finite set $\mathcal{X}$ such that $\Delta(P_{X_1}, P_{X_2}) \le \frac{1}{4}$. Then, we have*

$$|H(X_1) - H(X_2)| \le -2\Delta(P_{X_1}, P_{X_2}) \log \frac{2\Delta(P_{X_1}, P_{X_2})}{|\mathcal{X}|}.$$

Corollary 8 *Let X and Y be random variables which take values in finite sets $\mathcal{X}$ and $\mathcal{Y}$, respectively. If $\Delta(P_{XY}, P_X P_Y) \le \frac{1}{4}$, we have*

$$I(X;Y) \le -2\Delta(P_{XY}, P_X P_Y) \log \frac{2\Delta(P_{XY}, P_X P_Y)}{|\mathcal{X}||\mathcal{Y}|}.$$

Proof. The proof immediately follows from Proposition 10 by setting $P_{X_1} := P_{XY}$ and $P_{X_2} := P_X P_Y$. $\square$

Lemma 3 *For a key agreement protocol, we have*

$$\begin{aligned} P(K_A \ne K_B) &\le \Delta(P_{K_A K_B}, P_{KK}) \\ &\le P(K_A \ne K_B) + \min(\Delta(P_{K_A}, P_K), \Delta(P_{K_B}, P_K)). \end{aligned}$$

Proof. Since we can easily see the existence of a distinguisher with advantage $P(K_A \ne K_B)$, the first inequality of the two is easy. We show the second inequality in the following. From triangle inequality, we have

$$\begin{aligned} \Delta(P_{K_A K_B}, P_{KK}) &\le \Delta(P_{K_A K_B}, P_{K_A K_A}) + \Delta(P_{K_A K_A}, P_{KK}) \\ &= P(K_A \ne K_B) + \Delta(P_{K_A}, P_K). \end{aligned}$$

Similarly, it is shown that $\Delta(P_{K_A K_B}, P_{KK}) \le P(K_A \ne K_B) + \Delta(P_{K_B}, P_K)$. $\square$

Appendix B: Proof of Theorem 3

The proof of Theorem 3 can be given by the similar idea used in the proof of Theorem 1.

First, we show relationships between formalizations of correctness.

(i) We show $\beta_{\pi,t,1} = \beta_{\pi,t,2}$: This is straightforward from Proposition 8 in Appendix A.

(ii) We show $\beta_{\pi,t,2} = \beta_{\pi,t,3}$: For arbitrary random variables $(M_1, M_2, \ldots, M_t)$, we have

$$\begin{aligned} &2\Delta(P_{M_1\tilde{M}_1, M_2\tilde{M}_2, \ldots, M_t\tilde{M}_t}, P_{M_1M_1, M_2M_2, \ldots, M_tM_t}) \\ &= \sum_{(m_1,\tilde{m}_1),\ldots,(m_t,\tilde{m}_t)} |P_{M_1\tilde{M}_1, M_2\tilde{M}_2, \ldots, M_t\tilde{M}_t}((m_1,\tilde{m}_1), \ldots, (m_t,\tilde{m}_t)) \\ &\qquad\qquad -P_{M_1M_1, M_2M_2, \ldots, M_tM_t}((m_1,\tilde{m}_1), \ldots, (m_t,\tilde{m}_t))| \\ &= \sum_{(m_1,\ldots,m_t)} P_{M_1M_2\ldots M_t}(m_1, m_2, \ldots, m_t) \cdot \\ &\qquad \sum_{(\tilde{m}_1,\ldots,\tilde{m}_t)} |P_{\tilde{M}_1\ldots\tilde{M}_t|M_1\ldots M_t}(\tilde{m}_1, \ldots, \tilde{m}_t|m_1, \ldots, m_t) - P_{M_1\ldots M_t|M_1\ldots M_t}(\tilde{m}_1, \ldots, \tilde{m}_t|m_1, \ldots, m_t)| \\ &\le \max_{(m_1,\ldots,m_t)} \sum_{(\tilde{m}_1,\ldots,\tilde{m}_t)} |P_{\tilde{M}_1\ldots\tilde{M}_t|M_1\ldots M_t}(\tilde{m}_1, \ldots, \tilde{m}_t|m_1, \ldots, m_t) \\ &\qquad\qquad -P_{M_1\ldots M_t|M_1\ldots M_t}(\tilde{m}_1, \ldots, \tilde{m}_t|m_1, \ldots, m_t)| \\ &= 2 \max_{(m_1,\ldots,m_t)} \Delta(P_{\tilde{M}_1\tilde{M}_2\ldots\tilde{M}_t|M_1=m_1, M_2=m_2, \ldots, M_t=m_t}, P_{M_1M_2\ldots M_t|M_1=m_1, M_2=m_2, \ldots, M_t=m_t}). \end{aligned}$$

Therefore, we have $\beta_{\pi,t,2} \le \beta_{\pi,t,3}$.

Let $m_1, m_2, \ldots, m_t \in \mathcal{M}$ be plaintexts such that

$$\beta_{\pi,t,3} = \Delta(P_{\tilde{M}_1\tilde{M}_2\ldots\tilde{M}_t|M_1=m_1,M_2=m_2,\ldots,M_t=m_t}, P_{M_1M_2\ldots M_t|M_1=m_1,M_2=m_2,\ldots,M_t=m_t}).$$

For any $\epsilon > 0$, we define a distribution $P_{M_1M_2\cdots M_t}$ as follows: for every i with $1 \le i \le t$, we define a distribution P_{M_i} on $\mathcal{M}$ by

$$P_{M_i}(m) := \begin{cases} 1-\delta_i \text{ if } m = m_i, \\ \frac{\delta_i}{|\mathcal{M}|-1} \text{ if } m \ne m_i, \end{cases}$$

where δ_i $(1 \le i \le t)$ are non-negative real numbers such that $0 \le \beta_{\pi,t,3}\sum_{i=1}^{t}\delta_i \le \epsilon$. Then, we have

$$\begin{aligned}
\beta_{\pi,t,2} &\ge \Delta(P_{M_1\tilde{M}_1,M_2\tilde{M}_2,\ldots,M_t\tilde{M}_t}, P_{M_1M_1,M_2M_2,\ldots,M_tM_t}) \\
&\ge \prod_{i=1}^{t}(1-\delta_i)\Delta(P_{\tilde{M}_1\tilde{M}_2\cdots\tilde{M}_t|M_1=m_1,M_2=m_2,\ldots,M_t=m_t}, P_{M_1M_2\ldots M_t|M_1=m_1,M_2=m_2,\ldots,M_t=m_t}) \\
&\ge (1-\sum_{i=1}^{t}\delta_i)\Delta(P_{\tilde{M}_1\tilde{M}_2\cdots\tilde{M}_t|M_1=m_1,M_2=m_2,\ldots,M_t=m_t}, P_{M_1M_2\ldots M_t|M_1=m_1,M_2=m_2,\ldots,M_t=m_t}) \\
&\ge \beta_{\pi,t,3} - \epsilon.
\end{aligned}$$

Secondly, we show relationships between formalizations of secrecy.

(1) We show that $\frac{2}{\ln 2}\alpha_{\pi,t,2}^2 \le \alpha_{\pi,t,1} \le -2\alpha_{\pi,t,2}\log\frac{2\alpha_{\pi,t,2}}{|\mathcal{M}|^t|\mathcal{C}|^t}$: For any $P_{M_1M_2\cdots M_{t-1}M_t} \in \wp(\mathcal{M}^t)$ and any π, let $Z_{t-1} := (M_1C_1, M_2C_2, \ldots, M_{t-1}C_{t-1})$. Considering the relationship between statistical distance and conditional mutual information derived from Theorem 16.3.2[7], it follows that,

$$I(M_t;C_t|Z_{t-1}) \le -2\Delta(P_{M_tC_t|Z_{t-1}}, P_{M_t|Z_{t-1}}P_{C_t|Z_{t-1}})\log\frac{2\Delta(P_{M_tC_t|Z_{t-1}}, P_{M_t|Z_{t-1}}P_{C_t|Z_{t-1}})}{|\mathcal{M}|^t|\mathcal{C}|^t}.$$

Therefore, we have

$$\alpha_{\pi,t,1} \le -2\alpha_{\pi,t,2}\log\frac{2\alpha_{\pi,t,2}}{|\mathcal{M}|^t|\mathcal{C}|^t}.$$

On the other hand, by the relationship between conditional statistical distance and conditional mutual information derived from Theorem 12.6.1[7], it follows that, for any $P_{M_1M_2\cdots M_{t-1}M_t} \in \wp(\mathcal{M}^t)$ and any π,

$$\Delta(P_{M_tC_t|Z_{t-1}}, P_{M_t|Z_{t-1}}P_{C_t|Z_{t-1}}) \le \sqrt{\frac{\ln 2}{2}}I(M_t;C_t|Z_{t-1})^{\frac{1}{2}}.$$

Therefore, we have $\alpha_{\pi,t,2} \le \sqrt{\frac{\ln 2}{2}}\alpha_{\pi,t,1}^{\frac{1}{2}}$.

(2) We show $\alpha_{\pi,t,3} \le 2\alpha_{\pi,t,2}$: Let $m_1, m_2, \ldots, m_{t-1}, \hat{m}_0, \hat{m}_1 \in \mathcal{M}$ such that

$$\begin{aligned}
\alpha_{\pi,t,3} = \Delta(&P_{C_t|M=\hat{m}_0,(M_1,C_1)=(m_1,c_1),\ldots,(M_{t-1},C_{t-1})=(m_{t-1},c_{t-1})}, \\
&P_{C_t|M=\hat{m}_1,(M_1,C_1)=(m_1,c_1),\ldots,(M_{t-1},C_{t-1})=(m_{t-1},c_{t-1})}).
\end{aligned}$$

In the following, we set $Z_{t-1} := (M_1C_1, M_2C_2, \ldots, M_{t-1}C_{t-1})$ and $z_{t-1} := ((m_1, c_1), (m_2, c_2), \ldots, (m_{t-1}, c_{t-1}))$. For any $\epsilon > 0$, and for every i, we define a distribution P_{M_i} on $\mathcal{M}$ as follows: For every i with $i \le t-1$,

$$P_{M_i}(m) := \begin{cases} 1-\delta_i \text{ if } m = m_i, \\ \frac{\delta_i}{|\mathcal{M}|-1} \text{ if } m \ne m_i, \end{cases}$$

and for $i = t$,

$$P_{M_t}(m) := \begin{cases} \frac{1}{2}(1-\delta_t) \text{ if } m \in \{\hat{m}_0, \hat{m}_1\}, \\ \frac{\delta_t}{|\mathcal{M}|-2} \text{ if } m \notin \{\hat{m}_0, \hat{m}_1\}, \end{cases}$$

where δ_i $(1 \le i \le t)$ are non-negative real numbers such that $0 \le \alpha_{\pi,t,3} \sum_{i=1}^{t} \delta_i \le 2\epsilon$. Then, we have

$$\begin{aligned}
\alpha_{\pi,t,2} &\ge \Delta(P_{M_tC_t|Z_{t-1}}, P_{M_t|Z_{t-1}}P_{C_t|Z_{t-1}}) \\
&= \sum_z P_{Z_{t-1}}(z)\Delta(P_{M_tC_t|Z_{t-1}=z}, P_{M_t|Z_{t-1}=z}P_{C_t|Z_{t-1}=z}) \\
&\ge \prod_{i=1}^{t-1}(1-\delta_i)\Delta(P_{M_tC_t|Z_{t-1}=z_{t-1}}, P_{M_t|Z_{t-1}=z_{t-1}}P_{C_t|Z_{t-1}=z_{t-1}}) \\
&\ge \frac{1}{2}\prod_{i=1}^{t}(1-\delta_i)\{\Delta(P_{C_t|M_t=\hat{m}_0,Z_{t-1}=z_{t-1}}, P_{C_t|Z_{t-1}=z_{t-1}}) + \\
&\qquad\qquad \Delta(P_{C_t|M_t=\hat{m}_1,Z_{t-1}=z_{t-1}}, P_{C_t|Z_{t-1}=z_{t-1}})\} \\
&\ge \frac{1}{2}\prod_{i=1}^{t}(1-\delta_i)\Delta(P_{C_t|M_t=\hat{m}_0,Z_{t-1}=z_{t-1}}, P_{C_t|M_t=\hat{m}_1,Z_{t-1}=z_{t-1}}) \\
&= \frac{1}{2}\prod_{i=1}^{t}(1-\delta_i)\alpha_{\pi,t,3} \\
&\ge \frac{1}{2}(1-\sum_{i=1}^{t}\delta_i)\alpha_{\pi,t,3} \\
&\ge \frac{1}{2}\alpha_{\pi,t,3} - \epsilon.
\end{aligned}$$

(3) We show that $\alpha_{\pi,t,5} \le \alpha_{\pi,t,3}$: Let $m_1, m_2, \ldots, m_{t-1}, m_t \in \mathcal{M}$ such that

$$\alpha_{\pi,t,5} = \inf_{P_{Q_1Q_2\ldots Q_t}} \Delta(P_{C_1C_2\ldots C_t|M_1=m_1,M_2=m_2,\ldots,M_t=m_t},\ P_{Q_1Q_2\ldots Q_t}).$$

We set $P_{Q_i} := P_{C_i|M_1=m_1,M_2=m_2,\ldots,M_i=m_i}$ for $i = 1, 2, \ldots, t-1$ and

$$P_{Q_t} := P_{C_t|M_1=m_1,M_2=m_2,\ldots,M_{t-1}=m_{t-1},M_t=\hat{m}_t}$$

for some $\hat{m}_t \ne m_t$. Then, we have

$$\begin{aligned}
\alpha_{\pi,t,5} &\le \Delta(P_{C_1C_2\ldots C_t|M_1=m_1,M_2=m_2,\ldots,M_t=m_t},\ P_{Q_1Q_2\ldots Q_t}) \\
&\le \max_{(c_1,c_2,\ldots,c_{t-1})}\max_{(m_t,\hat{m}_t)} \Delta(P_{C_t|M=m_t,(M_1,C_1)=(m_1,c_1),\ldots,(M_{t-1},C_{t-1})=(m_{t-1},c_{t-1})}, \\
&\qquad\qquad P_{C_t|M=\hat{m}_t,(M_1,C_1)=(m_1,c_1),\ldots,(M_{t-1},C_{t-1})=(m_{t-1},c_{t-1})}) \\
&\le \alpha_{\pi,t,3}.
\end{aligned}$$

(4) We show $\alpha_{\pi,t,4} = \alpha_{\pi,t,5}$: For arbitrary random variables $(M_1, M_2, \ldots, M_t)$ and $(Q_1, Q_2, \ldots, Q_t)$, we have

$$\begin{aligned}
&2\Delta(P_{M_1C_1,M_2C_2,\ldots,M_tC_t}, P_{M_1Q_1,M_2Q_2,\ldots,M_tQ_t}) \\
&= \sum_{(m_1,c_1),\ldots,(m_t,c_t)} |P_{M_1C_1,M_2C_2,\ldots,M_tC_t}((m_1,c_1),\ldots,(m_t,c_t)) \\
&\qquad\qquad\qquad -P_{M_1Q_1,M_2Q_2,\ldots,M_tQ_t}((m_1,c_1),\ldots,(m_t,c_t))| \\
&= \sum_{(m_1,\ldots,m_t)} P_{M_1M_2\ldots M_t}(m_1,m_2,\ldots,m_t) \cdot \\
&\quad \sum_{(c_1,\ldots,c_t)} |P_{C_1C_2\ldots C_t|(M_1M_2\ldots M_t)=(m_1,m_2,\ldots,m_t)}(c_1,c_2,\ldots,c_t) - P_{Q_1Q_2\ldots Q_t}(c_1,c_2,\ldots,c_t)| \\
&\le \max_{(m_1,m_2,\ldots,m_t)} \sum_{(c_1,\ldots,c_t)} |P_{C_1\ldots C_t|(M_1\ldots M_t)=(m_1,\ldots,m_t)}(c_1,\ldots,c_t) - P_{Q_1\ldots Q_t}(c_1,\ldots,c_t)| \\
&= 2\max_{(m_1,m_2,\ldots,m_t)} \Delta(P_{C_1C_2\ldots C_t|M_1=m_1,M_2=m_2,\ldots,M_t=m_t},\ P_{Q_1Q_2\ldots Q_t}).
\end{aligned}$$

Therefore, we have $\alpha_{\pi,t,4} \le \alpha_{\pi,t,5}$.

Next, we show $\alpha_{\pi,t,5} \le \alpha_{\pi,t,4}$. Let $m_1, m_2, \ldots, m_t \in \mathcal{M}$ be plaintexts such that

$$\alpha_{\pi,t,5} = \inf_{P_{Q_1Q_2\ldots Q_t}} \Delta(P_{C_1C_2\ldots C_t|M_1=m_1,M_2=m_2,\ldots,M_t=m_t},\ P_{Q_1Q_2\ldots Q_t}).$$

For any $\epsilon > 0$, we define a distribution $P_{\hat{M}_1\hat{M}_2\cdots\hat{M}_t}$ as follows: for every i with $1 \le i \le t$, we define a distribution $P_{\hat{M}_i}$ on $\mathcal{M}$ by

$$P_{\hat{M}_i}(m) := \begin{cases} 1-\delta_i \text{ if } m = m_i, \\ \frac{\delta_i}{|\mathcal{M}|-1} \text{ if } m \ne m_i, \end{cases}$$

where δ_i $(1 \le i \le t)$ are non-negative real numbers such that $0 \le \alpha_{\pi,t,5}\sum_{i=1}^t \delta_i \le \epsilon$. Then, for any $P_{Q_1Q_2\ldots Q_t} \in \wp(\mathcal{C}^t)$, we have

$$\begin{aligned}
&\sup_{P_{M_1M_2\ldots M_t}} \Delta(P_{M_1C_1,M_2C_2,\ldots,M_tC_t}, P_{M_1Q_1,M_2Q_2,\ldots,M_tQ_t}) \\
&\ge \Delta(P_{\hat{M}_1\hat{C}_1,\hat{M}_2\hat{C}_2,\ldots,\hat{M}_t\hat{C}_t}, P_{\hat{M}_1Q_1,\hat{M}_2Q_2,\ldots,\hat{M}_tQ_t}) \\
&\ge \prod_{i=1}^t (1-\delta_i)\Delta(P_{\hat{C}_1\hat{C}_2\cdots\hat{C}_t|\hat{M}_1=m_1,\hat{M}_2=m_2,\ldots,\hat{M}_t=m_t}, P_{Q_1Q_2\ldots Q_t}) \\
&\ge (1-\sum_{i=1}^t \delta_i)\Delta(P_{\hat{C}_1\hat{C}_2\cdots\hat{C}_t|\hat{M}_1=m_1,\hat{M}_2=m_2,\ldots,\hat{M}_t=m_t}, P_{Q_1Q_2\ldots Q_t}).
\end{aligned}$$

Therefore, by taking the infimum over all $P_{Q_1Q_2\ldots Q_t} \in \wp(\mathcal{C}^t)$, we have $\alpha_{\pi,t,4} \ge \alpha_{\pi,t,5} - \epsilon$.

(5) We show $\frac{1}{4}\alpha_{\pi,t,2} \le \alpha_{\pi,t,4}$: For every i with $1 \le i \le t$, and for arbitrary random variables $(M_1, M_2, \ldots, M_i)$ and $(Q_1, Q_2, \ldots, Q_i)$, we set $Z_i := (M_1C_1, M_2C_2, \ldots, M_iC_i)$ and $\hat{Q}_i := (M_1Q_1, M_2Q_2, \ldots, M_iQ_i)$. Then, we have

$$\begin{aligned}
\Delta(P_{M_tC_t|Z_{t-1}}, P_{M_t|Z_{t-1}}P_{C_t|Z_{t-1}}) &\le \Delta(P_{M_tC_t|Z_{t-1}}, P_{M_t|Z_{t-1}}P_{Q_t}) + \Delta(P_{M_t|Z_{t-1}}P_{Q_t}, P_{M_t|Z_{t-1}}P_{C_t|Z_{t-1}}) \\
&= \Delta(P_{M_tC_t|Z_{t-1}}, P_{M_t|Z_{t-1}}P_{Q_t}) + \Delta(P_{Q_t}, P_{C_t|Z_{t-1}}) \\
&\le 2\Delta(P_{M_tC_t|Z_{t-1}}, P_{M_t|Z_{t-1}}P_{Q_t}) \\
&= 2\Delta(P_{Z_t}, P_{Z_{t-1}M_t}P_{Q_t}). \qquad (4)
\end{aligned}$$

On the other hand, we have

$$\begin{aligned}\Delta(P_{Z_t}, P_{Z_{t-1}M_t}P_{Q_t}) &\le \Delta(P_{Z_t}, P_{\hat{Q}_{t-1}M_t}P_{Q_t}) + \Delta(P_{\hat{Q}_{t-1}M_t}P_{Q_t}, P_{Z_{t-1}M_t}P_{Q_t}) \\ &= \Delta(P_{Z_t}, P_{\hat{Q}_t}) + \Delta(P_{\hat{Q}_{t-1}M_t}, P_{Z_{t-1}M_t}) \\ &\le 2\Delta(P_{Z_t}, P_{\hat{Q}_t}). \end{aligned} \tag{5}$$

From (4) and (5), it follows that $\Delta(P_{M_tC_t|Z_{t-1}}, P_{M_t|Z_{t-1}}P_{C_t|Z_{t-1}}) \le 4\Delta(P_{Z_t}, P_{\hat{Q}_t})$. Therefore, we obtain $\alpha_{\pi,t,2} \le 4\alpha_{\pi,t,4}$. □

Appendix C: Proof of Lemma 1

Let $\pi = (\pi^A, \pi^B)$. In the following, for $\boldsymbol{m} = (m_1, m_2, \ldots, m_t) \in \mathcal{M}^t$ and $\boldsymbol{c} = (c_1, c_2, \ldots, c_t) \in \mathcal{C}^t$, we briefly write $\boldsymbol{c} = \pi^A(k, \boldsymbol{m})$ if $c_i = \pi^A(k, m_i)$ for every i with $1 \le i \le t$. Similarly, for $\tilde{\boldsymbol{m}} = (\tilde{m}_1, \tilde{m}_2, \ldots, \tilde{m}_t) \in \tilde{\mathcal{M}}^t$, we write $\tilde{\boldsymbol{m}} = \pi^B(k, \boldsymbol{c})$ if $\tilde{m}_i = \pi^B(k, c_i)$ for every i.

For $\boldsymbol{m} = (m_1, m_2, \ldots, m_t) \in \mathcal{M}^t$, $\tilde{\boldsymbol{m}} = (\tilde{m}_1, \tilde{m}_2, \ldots, \tilde{m}_t) \in \tilde{\mathcal{M}}^t$, let $\Omega^{\pi,\mathcal{C}^t}_{\boldsymbol{m},\tilde{\boldsymbol{m}}} := \{\boldsymbol{c} \in \mathcal{C}^t | \exists k \in \mathcal{K}$ such that $\boldsymbol{c} = \pi^A(k, \boldsymbol{m})$ and $\tilde{\boldsymbol{m}} = \pi^B(k, \boldsymbol{c})\}$. For any $\boldsymbol{m} \in \mathcal{M}^t$, $\tilde{\boldsymbol{m}} \in \tilde{\mathcal{M}}^t$, and $k \in \mathcal{K}$, we also define $\Omega^{\pi,\mathcal{C}^t}_{\boldsymbol{m},\tilde{\boldsymbol{m}},k} := \{\boldsymbol{c} \in \mathcal{C}^t | \boldsymbol{c} = \pi^A(k, \boldsymbol{m})$ and $\tilde{\boldsymbol{m}} = \pi^B(k, \boldsymbol{c})\}$. Then, for any simulator σ, and for any distinguisher D which utilizes a certain distribution $P_{M_1M_2\cdots M_t}$ for distinguishing advantage, we have

$$\begin{aligned}\Delta^D(\pi((\bullet\!\!\longrightarrow)^t \| \, [P_K]), \sigma((\bullet\!\!\longrightarrow\!\!\bullet)^t)) &\ge \sum_{(\boldsymbol{m},\tilde{\boldsymbol{m}}),\boldsymbol{c}\in\Omega^{\pi,\mathcal{C}^t}_{\boldsymbol{m},\tilde{\boldsymbol{m}}}} \left(P_\pi(\boldsymbol{m},\tilde{\boldsymbol{m}},\boldsymbol{c}) - P_\sigma(\boldsymbol{m},\tilde{\boldsymbol{m}},\boldsymbol{c})\right), \\ &= 1 - \sum_{(\boldsymbol{m},\tilde{\boldsymbol{m}}),\boldsymbol{c}\in\Omega^{\pi,\mathcal{C}^t}_{\boldsymbol{m},\tilde{\boldsymbol{m}}}} P_\sigma(\boldsymbol{m},\tilde{\boldsymbol{m}},\boldsymbol{c}), \end{aligned} \tag{6}$$

where P_π and P_σ are distributions by the systems $\pi((\bullet\!\!\longrightarrow)^t \| \, [P_K])$ and $\sigma((\bullet\!\!\longrightarrow\!\!\bullet)^t)$, respectively.

We now need the following claim to complete the proof.

Claim 1 *Suppose that, for every i $(1 \le i \le t)$, π^B deterministically executes the i-th decryption. Then, we have*

$$\sum_{(\boldsymbol{m},\tilde{\boldsymbol{m}}),\boldsymbol{c}\in\Omega^{\pi,\mathcal{C}^t}_{\boldsymbol{m},\tilde{\boldsymbol{m}}}} P_\sigma(\boldsymbol{m},\tilde{\boldsymbol{m}},\boldsymbol{c}) \le \frac{|\mathcal{K}|}{2^{H_\infty(M_1,M_2,\ldots,M_t)}}.$$

Proof. We note that $P_\sigma(\boldsymbol{m},\tilde{\boldsymbol{m}},\boldsymbol{c}) = 0$ if $\boldsymbol{m} \ne \tilde{\boldsymbol{m}}$, and that $P_\sigma(\boldsymbol{m},\tilde{\boldsymbol{m}},\boldsymbol{c}) = P_{M_1M_2\cdots M_t}(\boldsymbol{m})P_\sigma(\boldsymbol{c})$ if $\boldsymbol{m} = \tilde{\boldsymbol{m}} \in \mathcal{M}^t$. Thus, we have

$$\begin{aligned}\sum_{(\boldsymbol{m},\tilde{\boldsymbol{m}}),\boldsymbol{c}\in\Omega^{\pi,\mathcal{C}^t}_{\boldsymbol{m},\tilde{\boldsymbol{m}}}} P_\sigma(\boldsymbol{m},\tilde{\boldsymbol{m}},\boldsymbol{c}) &= \sum_{\boldsymbol{m}} P_{M_1M_2\cdots M_t}(\boldsymbol{m}) \sum_{\boldsymbol{c}\in\Omega^{\pi,\mathcal{C}^t}_{\boldsymbol{m},\boldsymbol{m}}} P_\sigma(\boldsymbol{c}) \\ &\le \frac{1}{2^{H_\infty(M_1,M_2,\ldots,M_t)}} \sum_{\boldsymbol{m}} \sum_{k\in\mathcal{K}} \sum_{\boldsymbol{c}\in\Omega^{\pi,\mathcal{C}^t}_{\boldsymbol{m},\boldsymbol{m},k}} P_\sigma(\boldsymbol{c}) \\ &= \frac{1}{2^{H_\infty(M_1,M_2,\ldots,M_t)}} \sum_{k\in\mathcal{K}} \left(\sum_{\boldsymbol{m}} \sum_{\boldsymbol{c}\in\Omega^{\pi,\mathcal{C}^t}_{\boldsymbol{m},\boldsymbol{m},k}} P_\sigma(\boldsymbol{c}) \right) \\ &\le \frac{1}{2^{H_\infty(M_1,M_2,\ldots,M_t)}} \sum_{k\in\mathcal{K}} 1 \qquad (7) \\ &= \frac{|\mathcal{K}|}{2^{H_\infty(M_1,M_2,\ldots,M_t)}}. \end{aligned}$$

where (7) follows from $\Omega^{\pi,\mathcal{C}^t}_{\boldsymbol{m},\boldsymbol{m},k} \cap \Omega^{\pi,\mathcal{C}^t}_{\boldsymbol{m}',\boldsymbol{m}',k} = \emptyset$ if $\boldsymbol{m} \neq \boldsymbol{m}'$, since we assume that π^B deterministically executes the i-th decryption for every i $(1 \leq i \leq t)$. $\square$

We are back to the proof of Lemma 1. If π^B is deterministic, the proof of the following first inequality in Lemma 1 directly follows from (6) and Claim 1:

$$\Delta^D(\pi((\bullet\!\!\longrightarrow)^t || \, [P_K]), \sigma((\bullet\!\!\longrightarrow\!\!\bullet)^t)) \geq 1 - \frac{|\mathcal{K}|}{2^{H_\infty(M_1,M_2,\ldots,M_t)}}.$$

We next consider the above lower bound in the case of π^B being probabilistic. Let $\mathcal{R}$ be a finite set of random numbers, and suppose that π^B chooses a random number $r \in \mathcal{R}$ to execute each decryption according to a probability distribution P_R. For each $r \in \mathcal{R}$, we define a symmetric-key encryption protocol $\pi_r = (\pi^A, \pi^B_r)$ such that π^B_r is equal to π^B with a fixed $r \in \mathcal{R}$. For every i-th decryption $(1 \leq i \leq t)$, π^B chooses a deterministic π^B_r from $\{\pi^B_r | r \in \mathcal{R}\}$ according to P_R, and hence Claim 1 can be applied. Namely, the above lower bound cannot be improved. Therefore, the above lower bound holds without any assumption on π^B.

The second inequality in Lemma 1 follows from

$$\begin{aligned}
\Delta^{\mathcal{D}}(\pi((\bullet\!\!\longrightarrow)^t || \, [P_K]), \sigma((\bullet\!\!\longrightarrow\!\!\bullet)^t)) &\geq \sup_{P_{M_1 M_2 \cdots M_t}} \left(1 - \frac{|K|}{2^{H_\infty(M_1,M_2,\ldots,M_t)}}\right) \\
&= 1 - \frac{|K|}{2^{\sup_{P_{M_1 M_2 \cdots M_t}} H_\infty(M_1,M_2,\ldots,M_t)}} \\
&= 1 - \frac{|\mathcal{K}|}{|\mathcal{M}|^t}.
\end{aligned}$$

Therefore, the proof of Lemma 1 is completed. $\square$

Appendix D: Proof of Lemma 2

Let $\mathrm{Supp}(P_{XY}) = \{(x,y) | P_{XY}(x,y) > 0\} \subset \mathcal{X} \times \mathcal{Y}$ be the support of P_{XY}. For any $k_A \in \mathcal{K}$, and $k_B \in \mathcal{K}$, we define

$$\Omega^{\pi,\mathcal{T}^n}_{k_A,k_B} := \left\{ t^n = (t_1, t_2, \ldots, t_n) \in \mathcal{T}^n \;\middle|\; \begin{array}{l} \exists (x,y) \in \mathrm{Supp}(P_{XY}) \text{ such that} \\ t_i = f_i(x, t_1, \ldots, t_{i-1}) \text{ for odd } i \\ t_j = f_j(y, t_1, \ldots, t_{j-1}) \text{ for even } j \\ k_A = g_A(x, t_1, t_2, \ldots, t_n) \\ k_B = g_B(y, t_1, t_2, \ldots, t_n) \end{array} \right\}.$$

For any $(x,y) \in \mathrm{Supp}(P_{XY})$, $k_A \in \mathcal{K}$, and $k_B \in \mathcal{K}$, we also define

$$\Omega^{\pi,\mathcal{T}^n}_{k_A,k_B,x,y} := \left\{ t^n = (t_1, t_2, \ldots, t_n) \in \mathcal{T}^n \;\middle|\; \begin{array}{l} t_i = f_i(x, t_1, \ldots, t_{i-1}) \text{ for odd } i \\ t_j = f_j(y, t_1, \ldots, t_{j-1}) \text{ for even } j \\ k_A = g_A(x, t_1, t_2, \ldots, t_n) \\ k_B = g_B(y, t_1, t_2, \ldots, t_n) \end{array} \right\}.$$

Then, for any simulator σ, we have

$$\begin{aligned}
&\Delta^{\mathcal{D}}(\pi((\bullet\!\!\longrightarrow)^l \| (\longleftarrow\!\!\bullet)^{l-1} \| \ [P_{XY}])), \sigma([P_K])) \\
&\geq \frac{1}{2} \sum_{(k_A, k_B, t^n) \in \mathcal{K}\times\mathcal{K}\times\mathcal{T}^n} |P_\pi(k_A, k_B, t^n) - P_\sigma(k_A, k_B, t^n)| \\
&= \max_{\mathcal{B}\subset\mathcal{K}\times\mathcal{K}\times\mathcal{T}^n} \{P_\pi(\mathcal{B}) - P_\sigma(\mathcal{B})\} \\
&\geq \sum_{(k_A,k_B), t^n \in \Omega^{\pi,\mathcal{T}^n}_{k_A,k_B}} \left(P_\pi(k_A, k_B, t^n) - P_\sigma(k_A, k_B, t^n)\right), \\
&= 1 - \sum_{(k_A,k_B), t^n \in \Omega^{\pi,\mathcal{T}^n}_{k_A,k_B}} P_\sigma(k_A, k_B, t^n), \qquad (8)
\end{aligned}$$

where P_π and P_σ are distributions by the systems $\pi((\bullet\!\!\longrightarrow)^l \| (\longleftarrow\!\!\bullet)^{l-1} \| \ [P_{XY}])$ and $\sigma([P_K])$, respectively.

We now need the following claim.

Claim 2 *Suppose that g_A and g_B in the key agreement protocol π are deterministic. Then, we have*

$$\sum_{(k_A,k_B), t^n \in \Omega^{\pi,\mathcal{T}^n}_{k_A,k_B}} P_\sigma(k_A, k_B, t^n) \leq 2^{H_0(X,Y) - H_\infty(K)}.$$

Proof. We note that $P_\sigma(k_A, k_B, t^n) = 0$ if $k_A \neq k_B$, and that $P_\sigma(k_A, k_B, t^n) = P_K(k)P_\sigma(t^n)$ if $k_A = k_B = k \in \mathcal{K}$. Thus, we have

$$\begin{aligned}
\sum_{(k_A,k_B), t^n \in \Omega^{\pi,\mathcal{T}^n}_{k_A,k_B}} P_\sigma(k_A, k_B, t^n) &= \sum_k P_K(k) \sum_{t^n \in \Omega^{\pi,\mathcal{T}^n}_{k,k}} P_\sigma(t^n) \\
&\leq \frac{1}{2^{H_\infty(K)}} \sum_k \sum_{(x,y)\in Supp(P_{XY})} \sum_{t^n \in \Omega^{\pi,\mathcal{T}^n}_{k,k,x,y}} P_\sigma(t^n) \\
&= \frac{1}{2^{H_\infty(K)}} \sum_{(x,y)\in Supp(P_{XY})} \left(\sum_k \sum_{t^n \in \Omega^{\pi,\mathcal{T}^n}_{k,k,x,y}} P_\sigma(t^n) \right) \\
&\leq \frac{1}{2^{H_\infty(K)}} \sum_{(x,y)\in Supp(P_{XY})} 1 \qquad (9) \\
&= 2^{H_0(X,Y) - H_\infty(K)}.
\end{aligned}$$

where (9) follows from $\Omega^{\pi,\mathcal{T}^n}_{k,k,x,y} \cap \Omega^{\pi,\mathcal{T}^n}_{k',k',x,y} = \emptyset$ if $k \neq k'$, since we assume that g_A and g_B are deterministic. □

We are back to the proof of Lemma 2. If g_A and g_B are deterministic, the proof of Lemma 2 directly follows from (8) and Claim 2. We next show that the statement of Lemma 2 is true, even if we remove the assumption. Suppose that g_A or g_B is probabilistic. Let $\mathcal{R}_A$ (resp. $\mathcal{R}_B$) be a finite set, and suppose that g_A (resp. g_B) chooses a random number $r_A \in \mathcal{R}_A$ (resp. $r_B \in \mathcal{R}_B$) according to a probability distribution P_{R_A} (resp. P_{R_B}). For each fixed $(r_A, r_B) \in \mathcal{R}_A \times \mathcal{R}_B$, a key agreement protocol $\pi_{(r_A,r_B)}$ is specified in which g_A with inputting r_A and g_B with inputting r_B are deterministic. Therefore, we can apply the lower bound derived before. Hence, even if g_A (resp. g_B) chooses $r_A \in \mathcal{R}_A$ (resp. $r_B \in \mathcal{R}_B$) according to P_{R_A} (resp. P_{R_B}), this lower bound cannot be improved. Therefore, the proof of the lemma is completed. □