Formalization of Information-Theoretic Security for Key Agreement, Revisited

Junji Shikata
Graduate School of Environment and Information Sciences
Yokohama National University
Yokohama, Japan
Email: shikata@ynu.ac.jp

***Abstract*—In this paper, we investigate relationships between the following formalizations of information-theoretic security for key agreement protocols which may have agreement-errors: formalizations extended (or relaxed) from Shannon's perfect secrecy by using mutual information and statistical distance; and the ones of composable security by Maurer et al. and Canetti. Then, we explicitly show that those are essentially equivalent. We also derive lower bounds on the adversary's (or distinguisher's) advantage and the size of a correlated randomness resource required under all of the above formalizations at once through our relationships. In addition, we observe impossibility results which easily follow from the lower bounds.**

I. Introduction

A. 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 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 and developed since Shannon's work [22]. 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 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 in 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 research are based on the *ideal-world/real world paradigm*, and the paradigm underlies *universal composability* by Canetti [5] and *reactive simulatability* by Backes, Pfitzmann and Waidner [2] (See also [3], [4], [10], [19], [20] for related works). In addition, the explicit and simple paradigm for composable security was given by Maurer [14], 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 [17] studied the authenticate-then-encrypt paradigm for symmetric-key encryption with computational security. Shortly afterward, Maurer and Renner [15] proposed a new framework in an abstract way, called *abstract cryptography*. The framework is described at a higher level of abstraction than [14], [17], and various notions and methodologies (e.g. universal composability [5], reactive simulatability [2], and indifferentiability [16]) 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], [8], [11]. In particular, Kushilevitz, Lindell and Rabin [11] 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.

B. Our Contributions

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

(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) Formalizations of composable security by Maurer et al. [15], [17] and Canetti [4], [5].

Then, we explicitly show that those formalizations are essentially equivalent, and in particular, it turns out that the formalizations of the stand-alone and composable security are equivalent. We also derive lower bounds on the adversary's (or distinguisher's) advantage and those of the size of a correlated randomness resource required under all of the above formalizations. Although some of them may be 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.

C. Notation

For a random variable X taking values in a finite set $\mathcal{X}$, the Shannon entropy and min-entropy of X are denoted by $H(X)$ and $H_\infty(X)$, respectively. Also, let $H_0(X) := \log|\{x \in \mathcal{X} \mid P_X(x) > 0\}|$. $I(X;Y)$ denotes the mutual information between X and Y, and we denote the statistical distance between two distributions P_X and P_Y by $\Delta(P_X, P_Y) := \frac{1}{2}\sum_x |P_X(x) - P_Y(x)|$. In this paper, for a random variable X taking 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 $x \neq x'$. Also, $\wp(\mathcal{X}) := \{P_X \text{ on } \mathcal{X}\}$ is the set of all probability distributions P_X on $\mathcal{X}$.

II. Composable Security

A. Definition of Systems

In this paper, we consider a very basic scenario where there are three entities, Alice, Bob (honest players), and Eve (an adversary). Following the notions in [15], [17], we describe three types of systems: resources, converters and distinguishers.

A *resource* is a system with three interfaces labeled A, B, and E, where A, B, and E represent 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. 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.

B. Definition of Security

The security definition we focus on in this paper is derived from the paradigm of constructive cryptography [14]. Technically, the formal definition is based on the works in [15], [17], and is similar in spirit to previous simulation-based definitions in [2], [4], [5], [20]. The idea in the paradigm of constructive cryptography includes comparison of the *real* and *ideal* systems: the real system means $\pi(R)$ obtained by applying a protocol π to a resource R; and the ideal system consists of the *ideal functionality* S 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, we consider that the protocol π securely constructs S from R. More formally, we define the security as follows.

Definition 1 ([15], [17]): 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 $\Delta^{\mathcal{D}}(\pi(\perp^E(R)), \perp^E(S)) \leq \epsilon$, 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 $\Delta^{\mathcal{D}}(\pi(R), \sigma(S)) \leq \epsilon$.

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 ([15], [17]): 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 [15] 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 $R \parallel R' \overset{\pi\parallel\phi,\epsilon+\delta}{\Longrightarrow} S \parallel S'$.

C. Ideal Functionality / Channels

We give several definitions of ideal functionality of resources which are necessary to discuss in this paper.

- An *authenticated channel* usable once, denoted by $\bullet\!\!\longrightarrow$, transmits a message 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 $\bullet\!\!\longrightarrow \parallel \bullet\!\!\longrightarrow \parallel \cdots \parallel \bullet\!\!\longrightarrow$ (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.
- 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 $[P_K]$.
- 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.

III. Model of Key Agreement

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 a 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 $[P_{XY}]$. 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 in $\mathcal{K}$ in $\bullet\!\!=\!\!=\!\!\bullet$ (or more generally, $[P_K]$). Also, let $\mathcal{T}$ be a set of transcripts between Alice and Bob. Let $\pi = (\pi_A, \pi_B)$ be a key agreement protocol, where π_A (resp. π_B) is a converter at Alice's (resp. Bob's) side, defined below: let l be a positive integer and $n = 2l-1$; π_A consists of (probabilistic) functions $f_1, f_3, f_5, \ldots, f_{2l-1}$ and g_A, and π_B consists of (probabilistic) functions $f_2, f_4, f_6, \ldots, f_{2l-2}$ and g_B, where $f_1, f_2, \ldots, f_n, g_A, g_B$ are defined as follows:

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

Key Agreement Protocol $\pi = (\pi_A, \pi_B)$

```
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. $\pi_A$ computes $t_1 = f_1(x)$ and sends $t_1$ to $\pi_B$ by $\bullet\!\!\longrightarrow$.
2. For $j$ from 1 to $(n-1)/2$,
     2-1. $\pi_B$ computes $t_{2j} = f_{2j}(y, t_1, t_2, \ldots, t_{2j-1})$.
          Then, $\pi_B$ sends $t_{2j}$ to $\pi_A$ by $\longleftarrow\!\!\bullet$.
     2-2. $\pi_A$ computes $t_{2j+1} = f_{2j+1}(x, t_1, t_2, \ldots, t_{2j})$.
          Then, $\pi_A$ sends $t_{2j+1}$ to $\pi_B$ by $\bullet\!\!\longrightarrow$.
3. $\pi_A$ computes $k_A = g_A(x, t_1, t_2, \ldots, t_n)$ and outputs $k_A$.
   Similarly, $\pi_B$ 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 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, $[P_K]$).

IV. Security Definitions Revisited

Let's consider the following traditional formalization of security for key agreement protocols (e.g. [6], [7], [9], [12], [13], [18]).

Definition 2: Let π be a key agreement protocol. Then, π is said to be *ϵ-secure*, if it satisfies $P(K_A \neq K_B) \le \epsilon$,

$\log|\mathcal{K}| - H(K_A) \leq \epsilon$, and $I(K_A; T^n) \leq \epsilon$. In particular, π is said to be *perfectly-secure* if $\epsilon = 0$ above.

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

Definition 3: Let π be a key agreement protocol such that P_K is uniform 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) $\alpha_{\pi,3} := \inf\limits_{P_Q} \Delta(P_{K_A T^n}, P_{K_A} P_Q)$, 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 2 corresponds to the security in the sense of Type $(1, 1)$. The composable security by Maurer et al. [15], [17] and Canetti [4], [5] 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 2: The formalization of security in Definition 1 for a key agreement π is lower-and-upper bounded by

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

Proof: The proof can be shown by using the properties of statistical distance (e.g., triangle inequality). The details of the proof is given in the full version [23]. ■

Then, we can show the following theorem which states essential equivalence of all the formalizations (i.e., six possible formalizations above).

Theorem 1: Let π be a key agreement protocol such that P_K is uniform 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:

(1) $\beta_{\pi,2} \leq \beta_{\pi,1} + \sqrt{\dfrac{\beta_{\pi,1} \ln 2}{2}}$ and $\beta_{\pi,1} \leq -2\beta_{\pi,2} \log \dfrac{2\beta_{\pi,2}}{|\mathcal{K}|}$;

(2) $\dfrac{2}{\ln 2}\alpha_{\pi,2}^2 \leq \alpha_{\pi,1} \leq -2\alpha_{\pi,2} \log \dfrac{2\alpha_{\pi,2}}{|\mathcal{K}||\mathcal{T}|^n}$;

(3) $\alpha_{\pi,3} \leq \alpha_{\pi,2} \leq 2\alpha_{\pi,3}$.

In particular, for any $i, j \in \{1, 2, 3\}$, $s, t \in \{1, 2\}$, 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 under the condition that $|\mathcal{K}|$, $|\mathcal{T}|$ and n are fixed[1].

Proof: We omit the proof because of lack of space. The proof idea is to use the properties of entropies and statistical distance, and the translations between them. The details of the proof is given in the full version [23]. ■

V. Lower Bounds and Impossibility Results

In this section we consider key agreement protocols which construct a key sharing resource $[P_K]$ starting from a correlated randomness resource $[P_{XY}]$. First, we show a lower bound on the advantage of distinguishers as follows.

Theorem 2: For any key agreement protocol π, and for any simulator σ, we have

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

In particular, $\Delta^{\mathcal{D}}(\pi((\bullet\!\!\longrightarrow)^l \| (\longleftarrow\!\!\bullet)^{l-1} \| \, [P_{XY}]), \sigma(\bullet\!\!=\!\!=\!\!\bullet))$

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

Proof: The proof is given in the full version [23]. ■

From Theorem 2, we obtain lower bounds on the adversary's (or distinguisher's) advantage (Th. 3) and the required size of a correlated randomness resource (Cor. 1) as follows.

Theorem 3: For any key agreement protocol π such that P_K is uniform over $\mathcal{K}$, we have the following lower bounds:

(i) $\sqrt{\dfrac{\ln 2}{2}}\alpha_{\pi,1}^{\frac{1}{2}} + 2(1 + \sqrt{\dfrac{\ln 2}{2}})\beta_{\pi,1}^{\frac{1}{2}} \geq 1 - \dfrac{2^{H_0(X,Y)}}{|\mathcal{K}|}$;

(ii) $\alpha_{\pi,i} + 2(1 + \sqrt{\dfrac{\ln 2}{2}})\beta_{\pi,1}^{\frac{1}{2}} \geq 1 - \dfrac{2^{H_0(X,Y)}}{|\mathcal{K}|}$ for $i \in \{2, 3\}$;

(iii) $\sqrt{\dfrac{\ln 2}{2}}\alpha_{\pi,1}^{\frac{1}{2}} + 2\beta_{\pi,2} \geq 1 - \dfrac{2^{H_0(X,Y)}}{|\mathcal{K}|}$;

(iv) $\alpha_{\pi,i} + 2\beta_{\pi,2} \geq 1 - \dfrac{2^{H_0(X,Y)}}{|\mathcal{K}|}$ for $i \in \{2, 3\}$,

where $\alpha_{\pi,i}$ and $\beta_{\pi,j}$ are parameters defined in Definition 3 and it is assumed that $\beta_{\pi,1} \in [0, 1]$.

Proof: The proof can be shown by combining Proposition 2 and Theorems 1 and 2. The details of the proof is given in the full version [23]. ■

Corollary 1: Suppose that a key agreement protocol π is (δ, ϵ)-secure in the sense of Type (i, j) and P_K is uniform over $\mathcal{K}$. Then, we have

$$2^{H_0(X,Y)} \geq \begin{cases} \{1 - [\sqrt{\tfrac{\ln 2}{2}}\epsilon^{\frac{1}{2}} + 2(1 + \sqrt{\tfrac{\ln 2}{2}})\delta^{\frac{1}{2}}]\}|\mathcal{K}| \text{ for } i = j = 1, \\ \{1 - [\epsilon + 2(1 + \sqrt{\tfrac{\ln 2}{2}})\delta^{\frac{1}{2}}]\}|\mathcal{K}| \text{ for } i = 1,\ j \in \{2, 3\}, \\ \{1 - (\sqrt{\tfrac{\ln 2}{2}}\epsilon^{\frac{1}{2}} + 2\delta)\}|\mathcal{K}| \text{ for } i = 2,\ j = 1, \\ \{1 - (\epsilon + 2\delta)\}|\mathcal{K}| \text{ for } i = 2,\ j \in \{2, 3\}, \end{cases}$$

where it is assumed that $\delta \in [0, 1]$ for $i = 1$.

[1] Note that $\alpha_{\pi,2}$ and $\alpha_{\pi,3}$ are of the same order and the orders between others may not be the same.

Finally, from Theorem 2 we obtain Proposition 3 which is an impossibility result for key agreement. Also, we provide Corollaries 2 and 3 below, as illustrations of impossibility results which are special cases of Proposition 3.

Proposition 3: 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 2: 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 $\bullet\!\!=\!\!=\!\!\bullet$ (even with 1-bit) starting from authenticated communications, if $\delta, \epsilon \in [0, 1]$ are some real numbers such that:

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

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

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

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

Corollary 3: Let $\bullet\!\!=\!\!=\!\!\bullet_s$ be the s-bit key sharing resource with the uniform distribution. Then, there is no protocol π such that $(\bullet\!\!\longrightarrow)^\infty \| (\longleftarrow\!\!\bullet)^\infty \| \; \bullet\!\!=\!\!=\!\!\bullet_s \overset{\pi,\hat{\epsilon}}{\Longrightarrow} [P_K]$ for $\hat{\epsilon} < 1 - 2^{s - H_\infty(K)}$. In particular, for $0 \le s < \hat{s}$, there is no (δ, ϵ)-secure key agreement (or key-expansion) protocol in the sense of Type (i, j) which constructs $\bullet\!\!=\!\!=\!\!\bullet_{\hat{s}}$ from $\bullet\!\!=\!\!=\!\!\bullet_s$, if $\delta, \epsilon \in [0, 1]$ are some real numbers which satisfy inequality in Corollary 2.

VI. Conclusion

In this paper, we investigated relationships between formalizations of information-theoretic security for key-agreement protocols in a general setting (i.e., the protocols may have agreement-errors). Specifically, we showed that the following formalizations are essentially all equivalent in the one-time model: (i) stand-alone security including formalizations of extended (or relaxed) Shannon's secrecy using mutual information and statistical distance; and (ii) composable security including formalizations by Maurer et al. and Canetti.

We also derived lower bounds on the adversary's (or distinguisher's) advantage and the size of a correlated randomness resource required under all of the above formalizations at once through our relationships. In addition, we observed impossibility results which follow from the lower bounds.

Although we derived lower bounds comprehensively through our relationships and the technique used to derive the bounds in this paper is different from previous ones, it is not clear that each of the bounds is tight. Therefore, our future works include investigation about tightness of our bounds.

Acknowledgment

The author wishes to thank Ueli Maurer for fruitful discussion on constructive cryptography and its related topics when the author was visiting ETH Zurich, Switzerland. The author also wishes to thank an anonymous referee for helpful comments.

References

[1] M. Backes, J. Müller-Quade, D. Unruh, "On the necessity of rewinding in secure multiparty computation," *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] R. Canetti, "Security and composition of multiparty cryptographic protocols," *J. Cryptology*, 13, pp. 143-202, 2000.

[5] R. Canetti, "Universally composable security: a new paradigm for cryptographic protocols," *The 42nd IEEE Symposium on Foundations of Computer Science* , pp. 136-145, 2001. *IACR Cryptology ePrint Archive* (updated version): http://eprint.iacr.org/2000/067

[6] 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.

[7] I. Csiszár, P. Narayan, "Common randomness and secret key generation with a helper," *IEEE Trans. Inform. Theory*, Vol. 46, No. 2, pp. 344-366, 1993.

[8] Y. Dodis, S. Micali, "Parallel reducibility for information-theoretically secure computation," *CRYPTO 2000*, pp. 74-92, Springer, 2000.

[9] S. Dziembowski, U. Maurer, "On generating the initial key in the bounded-storage model," *EUROCRYPT 2004*, LNCS 3027, pp. 126-137, Springer, 2004.

[10] S. Goldwasser, L. Levin, "Fair computation of general functions in presence of immoral majority," *CRYPTO'90*, LNCS 537, pp. 77-93, Springer, 1990.

[11] E. Kushilevitz, Y. Lindell, T. Rabin, "Information-theoretically secure protocols and security under composition," *The 38th STOC*, pp. 109-118, 2006. *IACR Cryptology ePrint Archive* (full version): http://eprint.iacr.org/2009/630

[12] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inform. Theory*, Vol. 39, pp. 733-742, 1993.

[13] 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.

[14] U. Maurer, "Constructive cryptography - a primer," *FC 2010*, LNCS 6052, p. 1, Springer, 2010.

[15] U. Maurer, R. Renner, "Abstract cryptography," *ICS 2011*, Tsinghua University Press, pp.1-21, 2011.

[16] 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.

[17] 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.

[18] U. Maurer, S. Wolf, "Secret-key agreement over unauthenticated public channels - part I: definitions and a completeness result," *IEEE Trans. Inform. Theory*, vol. 49, no. 4, pp. 822-831, 2003.

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

[20] 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.

[21] R. Renner, S. Wolf, "Simple and tight bounds for information reconciliation and privacy amplification," *ASIACRYPT 2005*, pp. 199-216, Springer, 2005.

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

[23] J. Shikata, "Formalization of information-theoretic security for encryption and key agreement, revisited," a full version of this paper, available at *IACR Cryptology ePrint Archive*: http://eprint.iacr.org/2012/383