Information-Theoretic Timed-Release Security: Key-Agreement, Encryption, and Authentication Codes*

Yohei Watanabe, Takenobu Seito, Junji Shikata

Graduate School of Environment and Information Sciences,
Yokohama National University, Japan.
watanabe-yohei-xs@ynu.jp, {takenobu.seito, shikata}@ynu.ac.jp

Abstract

In this paper, we study timed-release cryptography with information-theoretic security. As fundamental cryptographic primitives with information-theoretic security, we can consider key-agreement, encryption, and authentication codes. Therefore, in this paper we deal with information-theoretic timed-release security for all those primitives. Specifically, we propose models and formalizations of security for information-theoretic timed-release key-agreement, encryption, and authentication codes; we also derive tight lower bounds on entities' memory-sizes required for all those ones; and we show optimal constructions of all those ones. Furthermore, we investigate a relationship of mechanisms between information-theoretic timed-release key-agreement and information-theoretic key-insulated key-agreement. It turns out that there exists a simple algorithm which converts the former into the latter, and vice versa. In the sense, we conclude that these two mechanisms are essentially close.

1 Introduction

The security of most of present cryptographic systems is based on the assumption of difficulty of computationally hard problems such as the integer factoring problem or the discrete logarithm problem in finite fields or elliptic curves. However, taking into account recent rapid development of algorithms and computer technologies, such a system based on the assumption of difficulty of computationally hard problems might not maintain sufficient long-term security. In fact, it is known that quantum computers can easily solve the factoring and discrete logarithm problems. From these aspects, it is necessary and interesting to consider cryptographic techniques whose security does not depend on any computationally hard problems, especially for the long-term security.

Informally, the goal of timed-release cryptography is to securely send a certain information into the future. For instance, in timed-release encryption, a sender transmits a ciphertext so that a receiver can decrypt it when the time which the sender specified has come, and the receiver cannot decrypt it before the time. The timed-release cryptography was first proposed by May [11] in 1993, and after that, Rivest et al. [13] developed it in a systematic and formal way. Since Rivest et al. gave a formal definition of timed-release encryption in [13], various researches on timed-release cryptography including timed-release signatures (e.g., [1, 8, 9]) and timed-release encryption have been done based on computational security. In particular, timed-release public key encryption (TR-PKE for short) has been recently researched intensively. Chan et al.[4] proposed the first TR-PKE scheme, but did not present a formal security definition. Cathalo et al.[2] and Chalkias et al.[3] proposed direct

*This paper is the full version of [18], which is presented at ICITS 2012 at Montreal, Canada.

constructions of TR-PKE schemes based on number-theoretic assumptions in the random oracle model. Independently, Cheon et al. [6] proposed a generic construction of TR-PKE and it is efficient and provably secure in the standard model. And also, Fujioka et al.[7] proposed a generic construction of TR-PKE that guarantees strong security in the random oracle model. It also should be noted that Choen et al.[5] recently shows relationships between TR-PKE and key-insulated public-key encryption (KI-PKE for short) with computational security setting.

To the best of our knowledge, there is no paper which reports on the study of information-theoretic timed-release cryptography. If a sender wants to transmit a message far into the future, information-theoretic security will be helpful in constructing timed-release mechanism, since its security can provide the long-term security. In this paper, we study timed-release cryptography with information-theoretic security. As fundamental cryptographic primitives with information-theoretic security, we can consider information-theoretically secure key-agreement, encryption, and authentication codes. Therefore, in this paper, we deal with information-theoretic timed-release security for all those primitives. Specifically, the contribution of this paper is as follows.

- **TR-KA.** We propose a model and formalization of security for timed-release key-agreement (TR-KA for short) in information-theoretic security setting. We also derive tight lower bounds on entities' memory-sizes required for TR-KA. In addition, we propose an optimal direct construction of TR-KA based on multivariate polynomials over finite fields.

- **TRE.** We propose a model and formalization of security for timed-release encryption (TRE for short) in information-theoretic security setting. In addition, we derive tight lower bounds on entities' memory-sizes required for TRE. Furthermore, we present a simple generic construction of TRE: TRE can be constructed from TR-KA and the one-time pad. In particular, the application of our optimal direct construction of TR-KA in the generic construction leads to an optimal direct construction of TRE.

- **TRA-code.** We propose a model and formalization of security for timed-release authentication codes (TRA-codes for short) in information-theoretic security setting. We also derive tight lower bounds on entities' memory-sizes required for TRA-codes. In addition, we present two kinds of constructions, generic and direct ones. Our generic construction of TRA-codes is simple: TRA-codes can be constructed from TR-KA and traditional A-codes. Since the generic construction does not lead to an optimal construction of TRA-codes, we also propose a direct construction which is optimal.

- **Relation between TR-KA and KI-KA.** We investigate and show relationship between TR-KA and key-insulated key-agreement (KI-KA for short) [15] in information-theoretic security setting. It turns out that there exists a simple algorithm which converts TR-KA into KI-KA, and vice versa. Therefore, we can conclude that the mechanisms of TR-KA and KI-KA are essentially close. Note that this relationship in information-theoretic security setting is analogous to that of TR-PKE and KI-PKE in computational security setting shown in [5].

2 TR-KA: Timed-Release Key-Agreement with Information-Theoretic Security

2.1 Model and Security Definition

In this section we show a model and a security definition of timed-release key-agreement (TR-KA for short) with information-theoretic security. This is done based on those of timed-release schemes with computational security and those of traditional key-agreement with information-theoretic security.

For simplicity, we assume that there is a trusted authority whose role is to generate and to distribute secret-keys of entities. We call this model the *trusted initializer model* as in [12]. In TR-KA, there are $n+2$ entities, n users $U_1, U_2, \ldots, U_n$, a time-server T for broadcasting *time-signals* and a trusted initializer TI, where n is a positive integer. In this paper, we assume that the identity of each user U_i is also denoted by U_i. In addition, when any two users communicate each other in a timed-release scheme (i.e., not only TR-KA but also TRE and TRA-codes in the following sections) under consideration in this paper, we call a user who specifies the time a *sender* and the other a *receiver* for convenience.

Informally, TR-KA is executed as follows. In the initial phase, TI generates secret-keys on behalf of U_i $(1 \le i \le n)$ and the time-server T. After distributing these keys via secure channels, TI deletes them in his memory. Any user U_{i_1} can specify future time when U_{i_1} wants to share a common-key with a user U_{i_2}, and he computes a common-key in advance by using U_{i_1}'s secret-key and the identity U_{i_2}. And U_{i_1} tells U_{i_2} the future time which U_{i_1} specified. The time-server T periodically broadcasts a time-signal at each time which is generated by using T's master-key. When the specified time has come, U_{i_2} can compute a common-key shared with U_{i_1} by using U_{i_2}'s secret-key, the identity U_{i_1} and a time-signal of the specified time. Note that each user has two kinds of secret-keys: one is used for generating a common-key when he is a sender; and the other is used for deriving a common-key when he is a receiver. In TR-KA, we consider a non-interactive model where any two users can share a common-key without interactive communications.

Formally, we give the definition of TR-KA as follows.[1]

Definition 1 (TR-KA)**.** *A* timed-release key-agreement *(*TR-KA *for short)* Π *involves* $n+2$ *entities, TI,* $U_1, U_2, \ldots, U_n$ *and T, and consists of a four-tuple of algorithms (Setup, Ext, KeyGen, KeyDer) with five spaces,* $\mathcal{TCK}, \mathcal{TUK}, \mathcal{TMK}, \mathcal{T}$*, and* $\mathcal{TI}$*, where all of the above algorithms except Setup are deterministic and all of the above spaces are finite. In addition,* Π *is executed with four phases as follows.*

- ***Notation:***
  - *Entities: TI is a trusted initializer,* U_i *(*$1 \le i \le n$*) is a user and T is a time-server which broadcasts time-signals. Let* $\mathcal{U} := \{U_1, U_2, \ldots, U_n\}$ *be the set of all users.*
  - *Spaces:* $\mathcal{TCK}$ *is a set of possible common-keys, and* $\mathcal{TMK}$ *is a set of possible master-keys.* $\mathcal{T} := \{1, 2, \ldots, \tau\}$ *is a set of time.* $\mathcal{TI}^{(t)}$ *is a set of time-signals at time* t*. Let* $\mathcal{TI} := \bigcup_{i=1}^{\tau} \mathcal{TI}^{(i)}$*. Also,* $\mathcal{TUK}_i^{(S)}$ *is a set of possible* U_i*'s secret-keys for common-key generation. And also,* $\mathcal{TUK}_i^{(R)}$ *is a set of possible* U_i*'s secret-keys for common-key derivation. Then,* $\mathcal{TUK}_i := \mathcal{TUK}_i^{(S)} \times \mathcal{TUK}_i^{(R)}$ *is the set of possible secret-keys for* U_i *with an associated probability distribution* P_{TUK_i}*. Let* $\mathcal{TUK}^{(S)} := \bigcup_{i=1}^{n} \mathcal{TUK}_i^{(S)}$*,* $\mathcal{TUK}^{(R)} := \bigcup_{i=1}^{n} \mathcal{TUK}_i^{(R)}$*, and* $\mathcal{TUK} := \bigcup_{i=1}^{n} \mathcal{TUK}_i$*.*
  - *Algorithms: Setup is a key generation algorithm which on input a security parameter* 1^k*, outputs users' secret-keys and a time-server's master-key, Ext:* $\mathcal{TMK} \times \mathcal{T} \to \mathcal{TI}$ *is a time-signal generation algorithm for T, KeyGen:* $\mathcal{TUK}^{(S)} \times \mathcal{T} \times \mathcal{U} \to \mathcal{TCK}$ *is a common-key generation algorithm and KeyDer:* $\mathcal{TUK}^{(R)} \times \mathcal{TI} \times \mathcal{U} \to \mathcal{TCK}$ *is a common-key derivation algorithm.*

1. ***Key Generation and Distribution.*** *In the initial phase, TI generates the following keys by using Setup: a master-key* $tmk^* \in \mathcal{TMK}$ *for T; and a secret-key* $tuk_i = (tuk_i^{(S)}, tuk_i^{(R)}) \in \mathcal{TUK}_i$

[1] Note that our models of information-theoretically secure timed-release schemes (i.e., Definitions 1, 4 and 6) are almost the same as those of computationally secure timed-release schemes [2, 4, 5, 6, 7] except for considering the trusted initializer in our models.

for U_i $(i = 1, 2, \ldots, n)$. These keys are distributed to corresponding entities via secure channels. After distributing these keys, TI deletes them from his memory. And, T and U_i keep their keys secret, respectively.

2. ***Time-signal Generation.*** *For broadcasting a time-signal at each time, T generates a time-signal $tmk^{(t)}$ =$Ext(tmk^*, t) \in \mathcal{TI}^{(t)}$ by using a master key tmk^* and time $t \in \mathcal{T}$. Then, T broadcasts it to all users via a (authenticated) broadcast channel.*

3. ***Common-key Generation.*** *If U_{i_1} wants to share a common-key with U_{i_2} at future time t, U_{i_1} computes a common-key to be shared with U_{i_2} in advance, $tck^{(t)}_{i_1,i_2}$ =$KeyGen(tuk^{(S)}_{i_1}, t, U_{i_2}) \in \mathcal{TCK}$, by using his secret-key $tuk^{(S)}_{i_1}$, time t, and the receiver's identity U_{i_2}. And, U_{i_1} tells U_{i_2} the specified time t via an authenticated channel.*

4. ***Common-key Derivation.*** *On receiving the specified time t from U_{i_1}, and if the time t has come, U_{i_2} computes a common-key $tck^{(t)}_{i_1,i_2}$ =$KeyDer(tuk^{(R)}_{i_2}, tmk^{(t)}, U_{i_1})$ by using his secret-key $tuk^{(R)}_{i_2}$, a time-signal $tmk^{(t)}$ at time t, and the sender's identity U_{i_1}.*

In the model of TR-KA, we require the following equation holds: For all possible $t \in \mathcal{T}$, $i_1, i_2 \in \{1, 2, \ldots, n\}$, $tuk^{(S)}_{i_1} \in \mathcal{TUK}^{(S)}_{i_1}$, $tuk^{(R)}_{i_2} \in \mathcal{TUK}^{(R)}_{i_2}$, $tmk^{(t)} \in \mathcal{TI}^{(t)}$, we have $KeyGen(tuk^{(S)}_{i_1}, t, U_{i_2}) = KeyDer(tuk^{(R)}_{i_2}, tmk^{(t)}, U_{i_1})$. The above requirement implies that any two users can share a common-key at the specified time without any error if they correctly follow the specification of TR-KA. In addition, $tck^{(t)}_{i_1,i_2}$ means a shared key between U_{i_1} and U_{i_2} at time t when U_{i_1} is the sender and U_{i_2} is the receiver, and we note that $tck^{(t)}_{i_1,i_2} \neq tck^{(t)}_{i_2,i_1}$ in general.

We now define several notation to formalize security of TR-KA as follows. For any finite set $\mathcal{Z}$ and any non-negative integer z, let $\mathcal{P}(\mathcal{Z}, z) := \{Z \subset \mathcal{Z} | |Z| \leq z\}$ be the family of all subsets of $\mathcal{Z}$ whose cardinality is less than or equal to z. Let ω $(< n)$ be the maximum number of possible colluders. For a set of colluders $W = \{U_{l_1}, U_{l_2}, \ldots, U_{l_j}\} \in \mathcal{P}(\mathcal{U}, \omega)$, $\mathcal{TUK}^{(S)}_W := \mathcal{TUK}^{(S)}_{l_1} \times \mathcal{TUK}^{(S)}_{l_2} \times \cdots \times \mathcal{TUK}^{(S)}_{l_j}$ denotes the set of possible W's secret-keys for common-key generation, and $\mathcal{TUK}^{(R)}_W := \mathcal{TUK}^{(R)}_{l_1} \times \mathcal{TUK}^{(R)}_{l_2} \times \cdots \times \mathcal{TUK}^{(R)}_{l_j}$ denotes the set of possible W's secret-keys for common-key derivation. And, let $\mathcal{TCK}^{(t)}_{i_1,i_2}$ be the set of possible common-keys shared between U_{i_1} and U_{i_2} at the time $t \in \mathcal{T}$. Furthermore, let $TCK^{(t)}_{i_1,i_2}, TMK, TUK^{(S)}_W, TUK^{(R)}_W$, and $TI^{(1)}, \ldots, TI^{(\tau)}$ be random variables which take values on $\mathcal{TCK}^{(t)}_{i_1,i_2}, \mathcal{TMK}, \mathcal{TUK}^{(S)}_W, \mathcal{TUK}^{(R)}_W$, and $\mathcal{TI}^{(1)}, \ldots, \mathcal{TI}^{(\tau)}$, respectively.

Next, we formalize a security definition of TR-KA based on the idea of timed-release security and traditional key-agreement with information-theoretic security. In TR-KA, we consider the following security goal and attacking model. First, the security goal which we consider is basically the same as that of the traditional key-agreement: an adversary (or a dishonest entity) cannot obtain any information on a common-key shared between two honest users. In addition to this, we want to require that even a legitimate receiver cannot obtain any information on a common-key to be shared before the specified time comes (i.e., before a time-signal at the specified time is received), since we consider timed-release security in this paper. Secondly, as an attacking model we consider the following three types of attacks: (1) an attack by a dishonest time-server; (2) an attack by colluders (i.e., dishonest users) not including a receiver; and (3) an attack by colluders including a receiver. By combining the security goal and attacks mentioned above, we formally define security of TR-KA as follows.

Definition 2. Let Π be TR-KA. Π is said to be (n, ω, τ)-secure if the following conditions are satisfied:

(1) For any $U_{i_1}, U_{i_2} \in \mathcal{U}$ and $t \in \mathcal{T}$, it holds that

$$H(TCK^{(t)}_{i_1,i_2} \mid TMK) = H(TCK^{(t)}_{i_1,i_2}).$$

(2) For any $W \in \mathcal{P}(\mathcal{U}, \omega)$, $U_{i_1}, U_{i_2} \in \mathcal{U}$ such that $U_{i_1}, U_{i_2} \notin W$, and for any $t \in \mathcal{T}$, it holds that

$$H(TCK^{(t)}_{i_1,i_2} \mid TUK^{(S)}_W, TUK^{(R)}_W, TI^{(1)}, \dots, TI^{(\tau)}) = H(TCK^{(t)}_{i_1,i_2}).$$

(3) For any $W \in \mathcal{P}(\mathcal{U}, \omega)$, $U_{i_1}, U_{i_2} \in \mathcal{U}$ such that $U_{i_1} \notin W$ and $U_{i_2} \in W$, for any $t \in \mathcal{T}$, it holds that

$$H(TCK^{(t)}_{i_1,i_2} \mid TUK^{(S)}_W, TUK^{(R)}_W, TI^{(1)}, \dots, TI^{(t-1)}, TI^{(t+1)}, \dots, TI^{(\tau)}) = H(TCK^{(t)}_{i_1,i_2}).$$

Intuitively, the meaning of formalizations (1)-(3) in Definition 2 is explained as follows: (1) a dishonest time-server cannot obtain any information on a common-key shared between two honest users. However, we assume that the time-server correctly broadcasts a time-signal at each time; (2) No information on a common-key shared between two honest users is obtained by any colluding group W not including a legitimate receiver, even if W obtains time-signals at all the time; (3) No information on a common-key between two users at the specified time is obtained by any colluding group W including a legitimate (but dishonest) receiver, even if W obtains time-signals at all the time except the specified time.[2]

2.2 Lower Bounds

In this section, we derive lower bounds of entities' memory-sizes required for secure TR-KA as follows. The proof is given in Appendix A.

Theorem 1. *Let* Π *be* (n, ω, τ)*-secure TR-KA, and we assume that all entropies on common-keys are equal, namely* $H(TCK) = H(TCK^{(t)}_{i_1,i_2})$ *for any* $i_1, i_2 \in \{1, 2, \dots, n\}$ *and* $t \in \mathcal{T}$*. Then, we have*

$$(i)\ H(TUK^{(R)}_i) \geq (\omega + 1)H(TCK), \quad (ii)\ H(TUK^{(S)}_i) \geq (\tau + \omega)H(TCK),$$
$$(iii)\ H(TI^{(t)}) \geq (\omega + 1)H(TCK), \quad (iv)\ H(TMK) \geq \tau(\omega + 1)H(TCK).$$

As we will see in the next section, the above lower bounds are tight since our construction will meet all the above inequalities with equalities. Therefore, we define optimality of constructions of TR-KA as follows.

Definition 3. *A construction of* (n, ω, τ)*-secure TR-KA is said to be* optimal *if it meets equality in every inequality of (i)-(iv) in Theorem 1.*

2.3 Construction

We present a construction, which is provably secure TR-KA in our model, by using multivariate polynomials over finite fields. In addition, it is shown that the construction is optimal. The detail of our construction of TR-KA Π=(*Setup, Ext, KeyGen, KeyDer*) is given as follows.

[2] In this sense, we have formalized the security notion stronger than the security that a dishonest receiver cannot obtain any information on a common-key to be shared before the specified time comes.

1. ***Setup***. For a security parameter 1^k, *Setup* outputs matching secret-keys tuk_i and tmk^* for U_i $(1 \leq i \leq n)$ and T, respectively, as follows. *Setup* picks a k-bit prime power q, where $q > \max(n, \tau)$, and constructs the finite field $\mathbb{F}_q$ with q elements. We assume that the identity of each user U_i is encoded as $U_i \in \mathbb{F}_q \backslash \{0\}$. Also, we assume $\mathcal{T} = \{1, 2, \ldots, \tau\} \subset \mathbb{F}_q \backslash \{0\}$ by using appropriate encoding. And, *Setup* chooses uniformly at random $f(x, y) := \sum_{i=0}^{\omega} \sum_{j=0}^{\omega} a_{ij} x^i y^j$, $tmk^*(x, z) := \sum_{i=0}^{\omega} \sum_{k=0}^{\tau-1} b_{ik} x^i z^k$ over $\mathbb{F}_q$ with three variables x, y and z in which each degree of x and y is at most ω, and the degree of z is at most $\tau - 1$. *Setup* also computes $tuk_i^{(S)}(y, z) := f(U_i, y) + tmk^*(U_i, z)$ and $tuk_i^{(R)}(x) := f(x, U_i)$ $(1 \leq i \leq n)$. Then, *Setup* outputs secret-keys $tuk_i := (tuk_i^{(S)}(y, z), tuk_i^{(R)}(x))$ $(1 \leq i \leq n)$ and $tmk^* := tmk^*(x, z)$ for U_i $(1 \leq i \leq n)$ and T, respectively.

2. ***Ext***. For $tmk^* = tmk^*(x, z)$ and time $t \in \mathcal{T}$, *Ext* outputs a time-signal at time t, $tmk^{(t)}(x) := tmk^*(x, t)$.

3. ***KeyGen***. For a secret-key $tuk_{i_1}^{(S)}$, the specified time t and an identity U_{i_2}, *KeyGen* generates a common-key shared between U_{i_1} and U_{i_2}, $tck_{i_1,i_2}^{(t)} := tuk_{i_1}^{(S)}(U_{i_2}, t)$, and outputs it.

4. ***KeyDer***. For a secret-key $tuk_{i_2}^{(R)}$, a time-signal $tmk^{(t)}$ at the specified time t and an identity U_{i_1}, *KeyDer* outputs a common-key shared between U_{i_1} and U_{i_2}, $tck_{i_1,i_2}^{(t)} := tuk_{i_2}^{(R)}(U_{i_1}) + tmk^{(t)}(U_{i_1})$.

The security and optimality of the above construction is stated as follows.

Theorem 2. *The resulting TR-KA Π by the above construction is (n, ω, τ)-secure and optimal.*

Proof. In this proof, we can write $f(x, y)$ and $tmk^*(x, z)$ in the form of

$$f(x,y) := (1, x, \ldots, x^\omega) A \begin{pmatrix} 1 \\ y \\ \vdots \\ y^\omega \end{pmatrix} \text{ and } tmk^*(x,z) := (1, x, \ldots, x^\omega) B \begin{pmatrix} 1 \\ z \\ \vdots \\ z^{\tau-1} \end{pmatrix},$$

respectively, where A is an $(\omega+1) \times (\omega+1)$ matrix and B is an $(\omega+1) \times \tau$ matrix, respectively. To complete the proof of Theorem 2, we show the following lemmas.

Lemma 1. *The above construction meets $H(TCK_{i_1,i_2}^{(t)} \mid TMK) = H(TCK_{i_1,i_2}^{(t)})$ for any $U_{i_1}, U_{i_2} \in \mathcal{U}$ and $t \in \mathcal{T}$.*

Proof. Consider the case that TS will guess $tck_{i_1,i_2}^{(t)} = f(U_{i_1}, U_{i_2}) + tmk^*(U_{i_1}, t)$ by using his master key. Since TS knows tmk^*, he can compute $tmk^*(U_{i_1}, t)$. Therefore, he has to guess $f(U_{i_1}, U_{i_2})$. However, by applying $X := O$, $A := A$ and $Y := O$ in Proposition 1 in Appendix B, there are at least q candidates of A. Then, by applying $\boldsymbol{x} := (1, U_{i_1}, U_{i_1}^2, \ldots, U_{i_1}^\omega)$, $A := A$ and $\boldsymbol{y} := {}^t(1, U_{i_2}, U_{i_2}^2, \ldots, U_{i_2}^\omega)$ in Proposition 2 in Appendix B, TS cannot guess $f(U_{i_1}, U_{i_2}) = \boldsymbol{x} A \boldsymbol{y}$ with probability larger than $1/q$. On the other hand, it is clear that $H(TCK_{i_1,i_2}^{(t)}) = \log_2 q$. Hence, for any $U_{i_1}, U_{i_2} \in \mathcal{U}$ and $t \in \mathcal{T}$, $H(TCK_{i_1,i_2}^{(t)} \mid TMK) = H(TCK_{i_1,i_2}^{(t)}) = \log_2 q$. □

Lemma 2. *The above construction meets $H(TCK_{i_1,i_2}^{(t)} \mid TUK_W^{(S)}, TUK_W^{(R)}, TI^{(1)}, \ldots, TI^{(\tau)}) = H(TCK_{i_1,i_2}^{(t)})$ for any U_{i_1}, $U_{i_2} \in \mathcal{U}$ and $W \in \mathcal{P}(\mathcal{U}, \omega)$ such that $U_{i_1}, U_{i_2} \notin W$, and for any $t \in \mathcal{T}$.*

Proof. Without loss of generality, we consider that $W := \{U_1, \ldots, U_\omega\}$ is a set of colluders such that $U_{i_1}, U_{i_2} \notin W$, and we write $\boldsymbol{x_i} := (1, U_i, U_i^2, \ldots, U_i^\omega)$ $(1 \leq i \leq n)$. Consider the case that a group of colluders W not including a targeted receiver will guess $tck_{i_1,i_2}^{(t)} = f(U_{i_1}, U_{i_2}) + tmk^*(U_{i_1}, t)$ by using their secret-keys and all time-signals. Since W can compute tmk^* by all time-signals, W can correctly obtain $tmk^*(U_{i_1}, t)$. Therefore, the purpose of W is to guess $f(U_{i_1}, U_{i_2})$. Since W can calculate $tmk^*(U_l, z)$ $(1 \leq l \leq \omega)$ and hence $tuk_l^{(S)}(y, z) - tmk^*(U_l, z) = f(U_l, y)$ $(1 \leq l \leq \omega)$, W gets

$$f(U_l, y) = \boldsymbol{x}_l A \begin{pmatrix} 1 \\ y \\ \vdots \\ y^\omega \end{pmatrix},$$

for $1 \leq l \leq \omega$. Thus, W can know the following matrix:

$$X_U A := \begin{pmatrix} \boldsymbol{x}_1 \\ \boldsymbol{x}_2 \\ \vdots \\ \boldsymbol{x}_\omega \end{pmatrix} A.$$

In addition, W knows

$$f(x, U_l) = (1, x, \ldots, x^\omega)\ A\ {}^t\boldsymbol{x}_l,$$

for $1 \leq l \leq \omega$ by their secret-keys $tuk_W^{(R)}$. Thus, W can know the following matrix:

$$A\ {}^tX_U = A\ ({}^t\boldsymbol{x}_1, {}^t\boldsymbol{x}_2, \ldots, {}^t\boldsymbol{x}_\omega).$$

By applying $X := X_U$, $A := A$ and $Y := {}^tX_U$ in Proposition 1 in Appendix B, there are at least q candidates of A. In addition, $\{\boldsymbol{x}_{i_1}, \boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_\omega\}$ and $\{\boldsymbol{x}_{i_2}, \boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_\omega\}$ are linearly independent, respectively, since $U_{i_1}, U_{i_2} \notin W$. Therefore, W cannot guess $f(U_{i_1}, U_{i_2}) = \boldsymbol{x}_{i_1} A\ {}^t\boldsymbol{x}_{i_2}$ with probability larger than $1/q$ by Proposition 2 in Appendix B. Thus, we have $H(TCK_{i_1,i_2}^{(t)} \mid TUK_W^{(S)}, TUK_W^{(R)}, TI^{(1)}, \ldots, TI^{(\tau)}) = \log_2 q$. Hence, for any U_{i_1}, $U_{i_2} \in \mathcal{U}$ such that $U_{i_1}, U_{i_2} \notin W$, and for any $t \in \mathcal{T}$, $H(TCK_{i_1,i_2}^{(t)} \mid TUK_W^{(S)}, TUK_W^{(R)}, TI^{(1)}, \ldots, TI^{(\tau)}) = H(TCK_{i_1,i_2}^{(t)}) = \log_2 q$. □

Lemma 3. *The above construction meets* $H(TCK_{i_1,i_2}^{(t)} \mid TUK_W^{(S)}, TUK_W^{(R)}, TI^{(1)}, \ldots, TI^{(t-1)}, TI^{(t+1)}, \ldots, TI^{(\tau)}) = H(TCK_{i_1,i_2}^{(t)})$ *for any* $U_{i_1}, U_{i_2} \in \mathcal{U}$ *and* $W \in \mathcal{P}(\mathcal{U}, \omega)$ *such that* $U_{i_1} \notin W$ *and* $U_{i_2} \in W$, *and for any* $t \in \mathcal{T}$.

Proof. Without loss of generality, we suppose that $W := \{U_1, \ldots, U_\omega\}$ is a set of colluders such that $U_{i_1} \notin W$, U_{i_1} is a targeted sender, U_ω is a targeted receiver, and τ is a specified time. In addition, we write $\boldsymbol{x_i} := (1, U_i, U_i^2, \ldots, U_i^\omega)$ $(1 \leq i \leq n)$ and $\boldsymbol{y_i} := {}^t(1, i, i^2, \ldots, i^{\tau-1})$ $(1 \leq i \leq \tau)$. Consider the case that a group of colluders W will guess $tck_{i_1,\omega}^{(\tau)} = f(U_{i_1}, U_\omega) + tmk^*(U_{i_1}, \tau)$ by using their secret-keys and time-signals at all the time except the specified time. Note that W can get $f(U_{i_1}, U_\omega)$ since $U_\omega \in W$. Thus, W tries to obtain $tmk^*(x, z)$ to know $tmk^*(U_{i_1}, \tau)$. W can compute $tuk_l^{(S)}(y, z) - f(U_l, z) = tmk^*(U_l, z)$ $(1 \leq l \leq \omega)$, and hence W gets

$$tmk^*(U_l, z) = \boldsymbol{x}_l B \begin{pmatrix} 1 \\ z \\ \vdots \\ z^{\tau-1} \end{pmatrix},$$

for $1 \leq l \leq \omega$. Thus, W can know the following matrix:

$$X_U B := \begin{pmatrix} \boldsymbol{x}_1 \\ \boldsymbol{x}_2 \\ \vdots \\ \boldsymbol{x}_\omega \end{pmatrix} B.$$

In addition, W obtains $tmk^*(x,t) = (1, x, \ldots, x^\omega)B\boldsymbol{y}_t$ for $1 \leq t \leq \tau - 1$ by time-signals at all except the time τ. Thus, W can know the following matrix:

$$BY_T := B(\boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_{\tau-1}).$$

By applying $X := X_U$, $A := B$ and $Y := Y_T$ in Proposition 1 in Appendix B, there are at least q candidates of B. In addition, $\{\boldsymbol{x}_{i_1}, \boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_\omega\}$ and $\{\boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_\tau\}$ are linearly independent, respectively, since $U_{i_1} \notin W$. Therefore, W cannot guess $tmk^*(U_{i_1}, \tau) = \boldsymbol{x}_{i_1} B \boldsymbol{y}_\tau$ with probability larger than $1/q$ from Proposition 2 in Appendix B. Thus, we have $H(TCK_{i_1,\omega}^{(\tau)} \mid TUK_W^{(S)}, TUK_W^{(R)}, TI^{(1)}, TI^{(2)}, \ldots, TI^{(\tau-1)}) = \log_2 q$. Hence, in general, for any U_{i_1}, $U_{i_2} \in \mathcal{U}$ such that $U_{i_1} \notin W$ and $U_{i_2} \in W$, and for any $t \in \mathcal{T}$, it holds that

$$H(TCK_{i_1,i_2}^{(t)} \mid TUK_W^{(S)}, TUK_W^{(R)}, TI^{(1)}, \ldots, TI^{(t-1)}, TI^{(t+1)}, \ldots, TI^{(\tau)}) = H(TCK_{i_1,i_2}^{(t)}) = \log_2 q.$$

□

Proof of Theorem 2. It follows that our construction satisfies the conditions (1)-(3) in Definition 2 from the above lemmas. Finally, it is straightforward to see that the construction satisfies all the lower bounds in Theorem 1 with equalities. Therefore, the above construction is optimal. □

3 TRE: Timed-Release Encryption with Information-Theoretic Security

In this section, we show a model and a security formalization of timed-release encryption (TRE for short) with information-theoretic security. We also show that TRE can be constructed from TR-KA and the one-time pad in a generic and simple way. In addition, we derive tight lower bounds on entities' memory-sizes required for TRE.

3.1 Model and Security Definition

We propose a model and a security definition of TRE, based on that of timed-release encryption with computational security (e.g., [13]) and that of the traditional encryption with information-theoretic security (e.g., [16]). Formally, we give a definition of TRE in the TI-model as in the case of TR-KA.

Definition 4 (TRE). *A timed-release encryption (*TRE *for short)* Σ *involves* $n+2$ *entities, TI,* $U_1, U_2, \ldots, U_n$ *and T, and consists of a four-tuple of algorithms (EGen, EExt, Enc, Dec) with six spaces,* $\mathcal{C}, \mathcal{M}_E, \mathcal{USK}, \mathcal{EMK}, \mathcal{T}$*, and* $\mathcal{ETI}$*, where all of the above algorithms except EGen are deterministic and all of the above spaces are finite. In addition,* Σ *is executed with four phases as follows.*

– ***Notation:***

- *Entities: TI,* U_i $(1 \leq i \leq n)$*, T, and* $\mathcal{U}$ *are the same as those in Definition 1.*

- *Spaces: $\mathcal{T}$ is the same as that in Definition 1. $\mathcal{C}$ is a set of possible ciphertexts, $\mathcal{M}_E$ is a set of possible plaintexts with a probability distribution P_M, $\mathcal{EMK}$ is a set of possible master-keys. $\mathcal{ETI}^{(t)}$ is a set of time-signals at time t. Let $\mathcal{ETI} := \bigcup_{i=1}^{\tau} \mathcal{ETI}^{(i)}$. Also, $\mathcal{EK}_i$ is a set of possible encryption-keys for U_i, $\mathcal{DK}_i$ is a set of possible decryption-keys for U_i, and $\mathcal{USK}_i := \mathcal{EK}_i \times \mathcal{DK}_i$ is a set of possible secret-keys for U_i. Let $\mathcal{EK} := \bigcup_{i=1}^{n} \mathcal{EK}_i$, $\mathcal{DK} := \bigcup_{i=1}^{n} \mathcal{DK}_i$ and $\mathcal{USK} := \bigcup_{i=1}^{n} \mathcal{USK}_i$.*
- *Algorithms: EGen is a key generation algorithm which on input a security parameter 1^k, outputs each user's secret-key and a server's master-key, EExt: $\mathcal{EMK} \times \mathcal{T} \to \mathcal{ETI}$ is a time-signal generation algorithm for T, Enc: $\mathcal{M}_E \times \mathcal{EK} \times \mathcal{T} \times \mathcal{U} \to \mathcal{C}$ is an encryption algorithm, and Dec: $\mathcal{C} \times \mathcal{DK} \times \mathcal{ETI} \times \mathcal{U} \to \mathcal{M}_E$ is a decryption algorithm.*

1. ***Key Generation and Distribution.*** *In the initial phase, TI generates the following keys by using EGen: a master-key $emk^* \in \mathcal{EMK}$ for T; a secret-key $usk_i = (ek_i, dk_i) \in \mathcal{USK}_i$ for U_i $(i = 1, 2, \ldots, n)$. These keys are distributed to corresponding entities via secure channels. After distributing these keys, TI deletes them from his memory. And, T and U_i keep their keys secret, respectively.*

2. ***Time-signal Generation.*** *For broadcasting a time-signal at each time, T generates a time-signal $emk^{(t)}$ =EExt$(emk^*, t) \in \mathcal{ETI}^{(t)}$ by using a master-key $emk^* \in \mathcal{EMK}$ and time $t \in \mathcal{T}$. Then, T broadcasts it to all users via a (authenticated) broadcast channel.*

3. ***Encryption.*** *U_{i_1} specifies time t when U_{i_2} can decrypt a ciphertext, and then U_{i_1} computes a ciphertext, $c^{(t)}_{i_1,i_2}$ =Enc$(m, ek_{i_1}, t, U_{i_2}) \in \mathcal{C}$, by a plaintext $m \in \mathcal{M}_E$, an encryption-key $ek_{i_1} \in \mathcal{EK}$, the specified time t and the identity U_{i_2}. And, U_{i_1} sends a pair of the ciphertext and the specified time, $(c^{(t)}_{i_1,i_2}, t)$, to U_{i_2} via an authenticated channel.*

4. ***Decryption.*** *Suppose that U_{i_2} has received $(c^{(t)}_{i_1,i_2}, t)$ from U_{i_1}. After receiving a time-signal $emk^{(t)}$ at the specified time t, U_{i_2} recovers m =Dec$(c^{(t)}_{i_1,i_2}, dk_{i_2}, emk^{(t)}, U_{i_1})$ by a ciphertext $c^{(t)}_{i_1,i_2}$, a decryption-key dk_{i_2}, a time-signal $emk^{(t)}$, and the identity U_{i_1}.*

In the model of TRE, we require the following equation holds: For all possible $t \in \mathcal{T}$, $i_1, i_2 \in \{1, 2, \ldots, n\}$, $ek_{i_1} \in \mathcal{EK}_{i_1}$, $dk_{i_2} \in \mathcal{DK}_{i_2}$, $emk^{(t)} \in \mathcal{ETI}^{(t)}$, we have

$$Dec(Enc(m, ek_{i_1}, t, U_{i_2}), dk_{i_2}, emk^{(t)}, U_{i_1}) = m.$$

The above requirement means correctness of TRE.

Next, we provide a security definition of TRE based on the idea of timed-release security and the traditional encryption with information-theoretic security. The choice of possible colluders $W \in \mathcal{P}(\mathcal{U}, \omega)$ is the same as that in TR-KA. For a set of colluders $W = \{U_{l_1}, U_{l_2}, \ldots, U_{l_j}\} \in \mathcal{P}(\mathcal{U}, \omega)$, $\mathcal{EK}_W := \mathcal{EK}_{l_1} \times \mathcal{EK}_{l_2} \times \cdots \times \mathcal{EK}_{l_j}$ is a set of W's encryption-keys, and $\mathcal{DK}_W := \mathcal{DK}_{l_1} \times \mathcal{DK}_{l_2} \times \cdots \times \mathcal{DK}_{l_j}$ is a set of W's decryption-keys. Also, let $\mathcal{C}^{(t)}_{i_1,i_2}$ be a finite set of possible ciphertexts sent from U_{i_1} to U_{i_2} such that it can be decrypted at the time t. Furthermore, let M, $C^{(t)}_{i_1,i_2}$, EMK, EK_W, DK_W, and $ETI^{(1)}, \ldots, ETI^{(\tau)}$ be random variables which take values on $\mathcal{M}_E$, $\mathcal{C}^{(t)}_{i_1,i_2}$, $\mathcal{EMK}$, $\mathcal{EK}_W$, $\mathcal{DK}_W$, and $\mathcal{ETI}^{(1)}, \ldots, \mathcal{ETI}^{(\tau)}$, respectively.

Similarly as in Definition 2 we consider the following three types of security notions for TRE: (1) A dishonest time-server cannot obtain any information on an underlying plaintext from a target ciphertext transmitted on the channel; (2) No information on an underlying plaintext from a target ciphertext is obtained by any colluding group W not including a legitimate receiver, even if W obtains time-signals at all the time; (3) No information on an underlying plaintext from a target ciphertext is obtained by any colluding group W including a legitimate (but dishonest) receiver, even if W obtains time-signals at all the time except the specified time.

The formalizations of the above security notions for TRE are given as follows.

Definition 5. Let Σ be TRE. Σ is said to be (n, ω, τ)-secure if the following conditions are satisfied:

(1) For any $U_{i_1}, U_{i_2} \in \mathcal{U}$ and any $t \in \mathcal{T}$, it holds that

$$H(M \mid C_{i_1,i_2}^{(t)}, EMK) = H(M).$$

(2) For any $W \in \mathcal{P}(\mathcal{U}, \omega)$, $U_{i_1}, U_{i_2} \in \mathcal{U}$ such that $U_{i_1}, U_{i_2} \notin W$, and for any $t \in \mathcal{T}$, it holds that

$$H(M \mid C_{i_1,i_2}^{(t)}, EK_W, DK_W, ETI^{(1)}, \ldots, ETI^{(\tau)}) = H(M).$$

(3) For any $W \in \mathcal{P}(\mathcal{U}, \omega)$, $U_{i_1}, U_{i_2} \in \mathcal{U}$ such that $U_{i_1} \notin W$ and $U_{i_2} \in W$, for any $t \in \mathcal{T}$, it holds that

$$H(M \mid C_{i_1,i_2}^{(t)}, EK_W, DK_W, ETI^{(1)}, \ldots, ETI^{(t-1)}, ETI^{(t+1)}, \ldots, ETI^{(\tau)}) = H(M).$$

3.2 Lower Bounds

We derive lower bounds on entities' memory-sizes required for secure TRE as follows.

Theorem 3. *Let Σ be an (n, ω, τ)-secure TRE. Then, we have*

$$(i)\ H(DK_i) \geq (\omega + 1)H(M), \quad (ii)\ H(EK_i) \geq (\tau + \omega)H(M),$$
$$(iii)\ H(ETI^{(t)}) \geq (\omega + 1)H(M), \quad (iv)\ H(EMK) \geq \tau(\omega + 1)H(M).$$

Proof. The proof is given in Appendix C. The proof is similar to that of Theorem 1, however, in the proof there are several technical points which are complicated than that of Theorem 1 (See Appendix C for details). □

As we will see in the next section, the above lower bounds are tight since an instantiation of our generic construction will meet all the above inequalities with equalities.

3.3 Construction of TRE from TR-KA and One-time Pad

We present a generic construction of TRE Σ=(*EGen, EExt, Enc, Dec*) starting from TR-KA Π=(*Setup, Ext, KeyGen, KeyDer*) and the one-time pad. In our construction, Π and Σ satisfy the following conditions: $\mathcal{EMK} = \mathcal{TMK}$; $\mathcal{ETI} = \mathcal{TI}$; $\mathcal{EK} = \mathcal{TUK}^{(S)}$; and $\mathcal{DK} = \mathcal{TUK}^{(R)}$.

1. ***EGen***. For a security parameter 1^k, *EGen* outputs matching secret-keys $usk_i = (ek_i, dk_i)$ and emk^* for U_i $(1 \leq i \leq n)$ and T, respectively, as follows. *EGen* calls *Setup* with input 1^k. Suppose $(tuk_1^{(S)}, tuk_1^{(R)}, tuk_2^{(S)}, tuk_2^{(R)}, \ldots, tuk_n^{(S)}, tuk_n^{(R)}, tmk^*) \leftarrow Setup(1^k)$. Then, *EGen* outputs secret-keys $ek_i := tuk_i^{(S)}$, $dk_i := tuk_i^{(R)}$, and $emk^* := tmk^*$ for U_i $(1 \leq i \leq n)$ and T, respectively.

2. ***EExt***. For a master-key $emk^* = tmk^*$ and time t, *EExt* calls *Ext*, and let $tmk^{(t)} = Ext(tmk^*, t)$. Then, *EExt* outputs a time-signal at the time t, $emk^{(t)} := tmk^{(t)}$.

3. ***Enc.*** For a plaintext m, an encryption-key $ek_{i_1} = tuk_{i_1}^{(S)}$, the specified time t and an identity U_{i_2}, *Enc* calls *KeyGen*, and suppose $tck_{i_1,i_2}^{(t)}$ $=KeyGen(tuk_{i_1}^{(S)},\ t, U_{i_2})$. Then, *Enc* outputs a ciphertext $c_{i_1,i_2}^{(t)} := m \oplus tck_{i_1,i_2}^{(t)}$.

4. ***Dec.*** For a ciphertext $c_{i_1,i_2}^{(t)}$, a decryption-key $dk_{i_2} = tuk_{i_2}^{(R)}$, a time-signal $emk^{(t)} = tmk^{(t)}$ at the specified time t and an identity U_{i_1}, *Dec* calls *KeyDer*, and suppose $tck_{i_1,i_2}^{(t)}$ $=KeyDer(tuk_{i_2}^{(R)}$, $tmk^{(t)}, U_{i_1})$. Then, *Dec* outputs a plaintext $m := c_{i_1,i_2}^{(t)} \oplus tck_{i_1,i_2}^{(t)}$.

The security of the above construction is shown as follows.

Theorem 4. *Given (n, ω, τ)-secure TR-KA Π in which common-keys are uniformly distributed over $\mathcal{TCK}$ (i.e., $H(TCK_{i,j}^{(t)}) = \log_2 |\mathcal{TCK}|$ for any i, j, and t), then the TRE Σ formed by the above construction based on Π is (n, ω, τ)-secure.*

Proof. Let Z be a random variable such that: (1) $Z = EMK$; or (2) $Z = (EK_W, DK_W, ETI^{(1)}, \ldots, ETI^{(\tau)})$ with $U_{i_1}, U_{i_2} \notin W$; or (3) $Z = (EK_W, DK_W, ETI^{(1)}, \ldots, ETI^{(t-1)}, ETI^{(t+1)}, \ldots, ETI^{(\tau)})$ with $U_{i_1} \notin W$ and $U_{i_2} \in W$.

Then, for any random variable Z of (1)-(3) mentioned above, we have

$$H(M \mid C, Z) = H(M), \tag{1}$$

where (1) follows from Definition 2 and perfect secrecy of one-time pad $c = m \oplus tck_{i_1,i_2}^{(t)}$ (i.e., each pair of M, TCK, Z is independent). Therefore, the above construction satisfies the conditions (1)-(3). □

Remark 1. *Although in this paper we have presented the direct proof of Theorem 1 (i.e., the lower bounds in TR-KA), we can also prove Theorem 1 by using Theorem 3 (i.e., the lower bounds in TRE) and the above generic construction where uniformly distributed plaintexts are taken.*

Remark 2. *In the above generic construction, we suppose P_M to be uniform (i.e., uniformly distributed plaintexts) and apply the direct (and optimal) construction of TR-KA in Section 2.3. Then, the resulting direct construction of TRE meets equality in every inequality of (i)-(iv) in Theorem 3. Therefore, the resulting direct construction is optimal and the lower bounds in Theorem 3 are tight.*

4 TRA-codes: Timed-Release Authentication Codes

In this section, we show a model and a security definition of timed-release authentication codes (TRA-codes for short). We also derive tight lower bounds on entities' memory-sizes required for TRA-codes. In addition, we present two kinds of constructions of TRA-codes, generic and direct ones. Our generic construction is simple, while our direct construction is optimal.

4.1 Model and Security Definition

We newly propose a model and a security definition of TRA-codes, based on that of timed-release signatures with computational security (e.g., [8]) and that of the traditional authentication code with information-theoretic security (e.g., [17]).

Formally, we give a definition of TRA-codes in the TI-model as in the case of TR-KA.

Definition 6 (TRA-codes)**.** *A timed-release authentication code (*TRA-code *for short)* Λ *involves* $n+2$ *entities, TI,* $U_1, U_2, \ldots, U_n$ *and T, and consists of a four-tuple of algorithms (TAGen, AExt, TAuth, TVer) with six spaces,* $\mathcal{M}_{\mathcal{A}}$*,* $\mathcal{A}$*,* $\mathcal{E}$*,* $\mathcal{AMK}$*,* $\mathcal{T}$ *and* $\mathcal{ATI}$*, where all of the above algorithms except TAGen are deterministic and all of the above spaces are finite. In addition,* Λ *is executed with four phases as follows.*

– ***Notation:***

- *Entities: TI,* U_i $(1 \leq i \leq n)$*, T, and* $\mathcal{U}$ *are the same as those in Definition 1.*
- *Spaces:* $\mathcal{T}$ *is the same as that in Definition 1.* $\mathcal{A}$ *is a set of possible authenticators (or tags),* $\mathcal{M}_A$ *is a set of possible messages,* $\mathcal{AMK}$ *is a set of possible master-keys.* $\mathcal{ATI}^{(t)}$ *is a set of time-signals at time t. Let* $\mathcal{ATI} := \bigcup_{t=1}^{\tau} \mathcal{ATI}^{(t)}$*. Also,* $\mathcal{E}_i^{(S)}$ *is a set of possible* U_i*'s authentication-keys,* $\mathcal{E}_i^{(R)}$ *is a set of possible* U_i*'s verification-keys, and* $\mathcal{E}_i := \mathcal{E}_i^{(S)} \times \mathcal{E}_i^{(R)}$ *is a set of possible secret-keys for* U_i*. Let* $\mathcal{E}^{(S)} := \bigcup_{i=1}^{n} \mathcal{E}_i^{(S)}$*,* $\mathcal{E}^{(R)} := \bigcup_{i=1}^{n} \mathcal{E}_i^{(R)}$*, and* $\mathcal{E} := \bigcup_{i=1}^{n} \mathcal{E}_i$*.*
- *Algorithms: TAGen is a key generation algorithm which on input a security parameter* 1^k*, outputs each user's secret-key and a time-server's master-key, AExt:* $\mathcal{AMK} \times \mathcal{T} \to \mathcal{ATI}$ *is a time-signal generation algorithm for T, TAuth:* $\mathcal{M}_A \times \mathcal{E}^{(S)} \times \mathcal{T} \times \mathcal{U} \to \mathcal{A}$ *is an authentication algorithm, and TVer:* $\mathcal{M}_A \times \mathcal{A} \times \mathcal{T} \times \mathcal{E}^{(R)} \times \mathcal{ATI} \times \mathcal{U} \to \{true, false\}$ *is a verification algorithm.*

1. ***Key Generation and Distribution.*** *In the initial phase, TI generates the following keys by using TAGen: a master-key* $amk^* \in \mathcal{AMK}$ *for T; a secret-key* $e_i = (e_i^{(S)}, e_i^{(R)}) \in \mathcal{E}_i$ *for* U_i $(i = 1, 2, \ldots, n)$*. These keys are distributed to corresponding entities via secure channels. After distributing these keys, TI deletes them from his memory. And, T and* U_i *keep their keys secret, respectively.*

2. ***Time-signal Generation.*** *For broadcasting a time-signal at each time, T generates a time-signal* $amk^{(t)}$ *=AExt(*amk^*, t*)* $\in \mathcal{ATI}^{(t)}$ *by using a master-key* $amk^* \in \mathcal{AMK}$ *and time* $t \in \mathcal{T}$*. Then, T broadcasts it to all users via a (authenticated) broadcast channel.*

3. ***Authentication.*** U_{i_1} *specifies time t when* U_{i_2} *can verify validity of a message m, and then* U_{i_1} *computes an authenticator,* $\alpha_{i_1,i_2}^{(t)}$ *=TAuth(*$m, e_{i_1}^{(S)}, t, U_{i_2}$*)* $\in \mathcal{A}$*, by the message* $m \in \mathcal{M}_A$*, an authentication-key* $e_{i_1}^{(S)}$*, the specified time t and the identity* U_{i_2}*. And,* U_{i_1} *sends* $(m, \alpha_{i_1,i_2}^{(t)}, t)$ *to* U_{i_2} *via an insecure channel.*

4. ***Verification.*** *Suppose that* U_{i_2} *has received* $(m, \alpha_{i_1,i_2}^{(t)}, t)$ *from* U_{i_1}*. After receiving a time-signal* $amk^{(t)}$ *at the specified time t,* U_{i_2} *checks the validity of* $\alpha_{i_1,i_2}^{(t)}$ *by a verification-key* $e_{i_2}^{(R)}$*, a time-signal* $amk^{(t)}$ *and the identity* U_{i_1}*: If* $TVer(m, \alpha_{i_1,i_2}^{(t)}, t, e_{i_2}^{(R)}, amk^{(t)}, U_{i_1}) = true$*, then* U_{i_2} *accepts* $(m, \alpha_{i_1,i_2}^{(t)}, t)$ *as valid, and rejects it otherwise.*

In the model of TRA-codes, we require the following equation holds: for all possible $t \in \mathcal{T}$, $i_1, i_2 \in \{1, 2, \ldots, n\}$, $e_{i_1}^{(S)} \in \mathcal{E}_{i_1}^{(S)}$, $e_{i_2}^{(R)} \in \mathcal{E}_{i_2}^{(R)}$, $amk^{(t)} \in \mathcal{ATI}^{(t)}$, we have

$$TVer(m, TAuth(m, e_{i_1}^{(S)}, t, U_{i_2}), t, e_{i_2}^{(R)}, amk^{(t)}, U_{i_1}) = true.$$

The above requirement means correctness of TRA-codes.

Next, we provide a security notion and its formalization for TRA-codes based on the idea of timed-release security and the traditional authentication code with information-theoretic security.

The choice of possible colluders $W \in \mathcal{P}(\mathcal{U}, \omega)$ is the same as that in TR-KA. For a set of colluders $W := \{U_{l_1}, U_{l_2}, \dots, U_{l_j}\} \in \mathcal{P}(\mathcal{U}, \omega)$, $\mathcal{E}_W^{(S)} := \mathcal{E}_{l_1}^{(S)} \times \mathcal{E}_{l_2}^{(S)} \times \cdots \times \mathcal{E}_{l_j}^{(S)}$ is a set of W's authentication-keys, and $\mathcal{E}_W^{(R)} := \mathcal{E}_{l_1}^{(R)} \times \mathcal{E}_{l_2}^{(R)} \times \cdots \times \mathcal{E}_{l_j}^{(R)}$ is a set of W's verification-keys. In TRA-codes, we consider *impersonation attacks* and *substitution attacks* as follows. (a) *Impersonation attacks:* an adversary (or a dishonest entity) tries to generate a fraudulent authenticated message at time t, $(m, \alpha_{i_1,i_2}^{(t)}, t)$, that has not been legally generated by a sender U_{i_1} but will be accepted by a receiver U_{i_2}. (b) *Substitution attacks:* an adversary (or a dishonest entity) tries to generate a fraudulent authenticated message at time t_2, $(m', \alpha_{i_1,i_2}^{(t_2)}, t_2)$, that has not been legally generated by a sender U_{i_1} but will be accepted by a receiver U_{i_2}, after observing a valid authenticated message at time t_1, $(m, \alpha_{i_1,i_2}^{(t_1)}, t_1)$ with $(m, \alpha_{i_1,i_2}^{(t_1)}, t_1) \neq (m', \alpha_{i_1,i_2}^{(t_2)}, t_2)$. Similarly as in Definition 2 we consider the following three types of security notions for TRA-codes: (1) A dishonest time-server cannot succeed in each of the *impersonation attack* and *substitution attack*; (2) Any colluding group W not including a legitimate receiver cannot succeed in each of the *impersonation attack* and *substitution attack*, even if W obtains time-signals at all the time; (3) Any colluding group W including a legitimate (but dishonest) receiver cannot check the validity of a target authenticated message without a time-signal at the specified time, even if W obtains time-signals at all the time except the specified time. To formalize this security notion, we consider it to be a kind of security against impersonation attacks at the future specified time: Any colluding group W including a receiver cannot succeed in impersonation attacks at the future specified time, even if W obtains time-signals at all the time except the specified time.

The formalizations of the above three types of security notions for TRA-codes are given as follows.

Definition 7. *Let Λ be a TRA-code. Λ is said to be $(n, \omega, \tau; \epsilon)$-secure, if* $\max(P_{Server}, P_1, P_2) \leq \epsilon$, *where P_{Server}, P_1 and P_2 are defined as follows.*

(1) Attacks by a dishonest time-server. Let $P_{Server} := \max(P_{I_S}, P_{S_S})$, where P_{I_S} and P_{S_S} are given as follows.

1-1) Impersonation attacks. The success probability of this attack denoted by P_{I_S} is defined as follows: For any $U_{i_1}, U_{i_2} \in \mathcal{U}$ and any $t \in \mathcal{T}$, we define $P_{I_S}(U_{i_1}, U_{i_2}, t)$ by

$$P_{I_S}(U_{i_1}, U_{i_2}, t) := \max_{(m, \alpha_{i_1,i_2}^{(t)}, t)} \max_{amk^*} \max_{amk^{(t)}}$$

$$Pr(TVer(m, \alpha_{i_1,i_2}^{(t)}, t, e_{i_2}^{(R)}, amk^{(t)}, U_{i_1}) = true \mid amk^*).$$

The probability P_{I_S} is defined as $P_{I_S} := \max_{U_{i_1}, U_{i_2}, t} P_{I_S}(U_{i_1}, U_{i_2}, t)$.

1-2) Substitution attacks. The success probability of this attack denoted by P_{S_S} is defined as follows: For any $U_{i_1}, U_{i_2} \in \mathcal{U}$ and any $t_1, t_2 \in \mathcal{T}$, we define $P_{S_S}(U_{i_1}, U_{i_2}, t_1, t_2)$ by

$$P_{S_S}(U_{i_1}, U_{i_2}, t_1, t_2) := \max_{(m', \alpha_{i_1,i_2}^{(t_2)}, t_2)} \max_{(m, \alpha_{i_1,i_2}^{(t_1)}, t_1) \neq (m', \alpha_{i_1,i_2}^{(t_2)}, t_2)} \max_{amk^*} \max_{amk^{(t_2)}}$$

$$Pr(TVer(m', \alpha_{i_1,i_2}^{(t_2)}, t_2, e_{i_2}^{(R)}, amk^{(t_2)}, U_{i_1}) = true \mid (m, \alpha_{i_1,i_2}^{(t_1)}, t_1), amk^*).$$

The probability P_{S_S} is defined as $P_{S_S} := \max_{U_{i_1}, U_{i_2}, t_1, t_2} P_{S_S}(U_{i_1}, U_{i_2}, t_1, t_2)$.

(2) Attacks by colluders not including a legitimate receiver. Let $P_1 := \max(P_{I_1}, P_{S_1})$, where P_{I_1} and P_{S_1} are given as follows.

2-1) Impersonation attacks. The success probability of this attack denoted by P_{I_1} is defined as follows: For any set of colluders $W \in \mathcal{P}(\mathcal{U}, \omega)$, any $U_{i_1}, U_{i_2} \in \mathcal{U}$ such that $U_{i_1}, U_{i_2} \notin W$ and for any $t \in \mathcal{T}$, we define $P_{I_1}(U_{i_1}, U_{i_2}, W, t)$ by

$$P_{I_1}(U_{i_1}, U_{i_2}, W, t) := \max_{(m,\alpha^{(t)}_{i_1,i_2},t)} \max_{e^{(S)}_W} \max_{e^{(R)}_W} \max_{amk^{(1)},\ldots,amk^{(\tau)}} \\ Pr(TVer(m, \alpha^{(t)}_{i_1,i_2}, t, e^{(R)}_{i_2}, amk^{(t)}, U_{i_1}) = true \\ \mid e^{(S)}_W, e^{(R)}_W, amk^{(1)}, \ldots, amk^{(\tau)}).$$

The probability P_{I_1} is defined as $P_{I_1} := \max_{U_{i_1},U_{i_2},W,t} P_{I_1}(U_{i_1}, U_{i_2}, W, t)$.

2-2) Substitution attacks. The success probability of this attack denoted by P_{S_1} is defined as follows: For any set of colluders $W \in \mathcal{P}(\mathcal{U}, \omega)$, any $U_{i_1}, U_{i_2} \in \mathcal{U}$ such that $U_{i_1}, U_{i_2} \notin W$ and for any $t_1, t_2 \in \mathcal{T}$, we define $P_{S_1}(U_{i_1}, U_{i_2}, W, t_1, t_2)$ by

$$P_{S_1}(U_{i_1}, U_{i_2}, W, t_1, t_2) := \max_{(m',\alpha^{(t_2)}_{i_1,i_2},t_2)} \max_{(m,\alpha^{(t_1)}_{i_1,i_2},t_1) \neq (m',\alpha^{(t_2)}_{i_1,i_2},t_2)} \max_{e^{(S)}_W} \max_{e^{(R)}_W} \\ \max_{amk^{(1)},\ldots,amk^{(\tau)}} Pr(TVer(m', \alpha^{(t_2)}_{i_1,i_2}, t_2, e^{(R)}_{i_2}, amk^{(t_2)}, U_{i_1}) = true \\ \mid (m, \alpha^{(t_1)}_{i_1,i_2}, t_1), e^{(S)}_W, e^{(R)}_W, amk^{(1)}, \ldots, amk^{(\tau)}).$$

And, P_{S_1} is defined as $P_{S_1} := \max_{U_{i_1},U_{i_2},W,t_1,t_2} P_{S_1}(U_{i_1}, U_{i_2}, W, t_1, t_2)$.

(3) An attack by colluders including a legitimate (but dishonest) receiver. The success probability of this attack denoted by P_2 is defined as follows: For any set of colluders $W \in \mathcal{P}(\mathcal{U}, \omega)$, any $U_{i_1}, U_{i_2} \in \mathcal{U}$ such that $U_{i_1} \notin W$ and $U_{i_2} \in W$, and for any $t \in \mathcal{T}$, we define $P_2(U_{i_1}, U_{i_2}, W, t)$ by

$$P_2(U_{i_1}, U_{i_2}, W, t) := \max_{(m,\alpha^{(t)}_{i_1,i_2},t)} \max_{e^{(S)}_W} \max_{e^{(R)}_W} \max_{amk^{(1)},\ldots,amk^{(t-1)},amk^{(t+1)},\ldots,amk^{(\tau)}} \\ Pr(TVer(m, \alpha^{(t)}_{i_1,i_2}, t, e^{(R)}_{i_2}, amk^{(t)}, U_{i_1}) = true \\ \mid e^{(S)}_W, e^{(R)}_W amk^{(1)}, \ldots, amk^{(t-1)}, amk^{(t+1)}, \ldots, amk^{(\tau)}).$$

The probability P_2 is defined as $P_2 := \max_{U_{i_1},U_{i_2},W,t} P_2(U_{i_1}, U_{i_2}, W, t)$.

4.2 Lower Bounds

We derive lower bounds on success probabilities of attacks and memory-sizes required for $(n, \omega, \tau; \epsilon)$-secure TRA-codes. Let $\mathcal{MA}^{(t)}_{i_1,i_2} := \{(m, \alpha^{(t)}_{i_1,i_2}) \in \mathcal{M}_A \times \mathcal{A} \mid m \in \mathcal{M}_A$ and $TAuth(m, e^{(S)}_{i_1}, t, U_{i_2}) = \alpha^{(t)}_{i_1,i_2}$ for some $e^{(S)}_{i_1} \in \mathcal{E}^{(S)}_{i_1}\}$ be a set of possible pairs of messages and authenticators such that each element of the set can be generated by the sender U_{i_1} to send it to U_{i_2} at specified future time t. Furthermore, let $MA^{(t)}_{i_1,i_2}$, AMK, $E^{(S)}_W$, $E^{(R)}_W$, $ATI^{(1)}$, …, $ATI^{(\tau)}$ be random variables which take values in $\mathcal{MA}^{(t)}_{i_1,i_2}$, $\mathcal{AMK}$, $\mathcal{E}^{(S)}_W$, $\mathcal{E}^{(R)}_W$, $\mathcal{ATI}^{(1)}$, …, $\mathcal{ATI}^{(\tau)}$, respectively.

We assume that there exist the following mappings in the model of TRA-codes: for every $i, j \in \{1, 2, \ldots, n\}$ and every $t \in \{1, 2, \ldots, \tau\}$,

$$\lambda_i \; : \; \mathcal{E}^{(S)}_i \to \mathcal{E}^{(S)}_{i,1} \times \cdots \times \mathcal{E}^{(S)}_{i,n},$$

$$\begin{aligned}
\pi_j &: \mathcal{E}_j^{(R)} \to \mathcal{E}_{1,j}^{(R)} \times \cdots \times \mathcal{E}_{n,j}^{(R)}, \\
f^{(t)} &: \mathcal{ATI}^{(t)} \to \mathcal{ATI}_1^{(t)} \times \cdots \times \mathcal{ATI}_n^{(t)}, \\
g &: \mathcal{AMK} \to \mathcal{AMK}_1 \times \cdots \times \mathcal{AMK}_n, \\
g_i &: \mathcal{AMK}_i \to \mathcal{ATI}_i^{(1)} \times \cdots \times \mathcal{ATI}_i^{(\tau)}, \\
\rho_{i,j} &: \mathcal{E}_{i,j}^{(S)} \to \mathcal{E}_{i,j}^{(R)} \times \mathcal{AMK}_i,
\end{aligned}$$

where $\mathcal{E}_{i,j}^{(S)}$ is a set of possible U_i's authetication-keys which are actually used to communicate with a receiver U_j; $\mathcal{E}_{i,j}^{(R)}$ is a set of possible U_j's verification-keys which are actually used to communicate with a sender U_i; $\mathcal{ATI}_i^{(t)}$ is a set of possible information on time-signals at time t when U_i becomes a sender; $\mathcal{AMK}_i$ is a set of possible partial information about master-keys when U_i becomes a sender[3]. Note that each user has the potential to become an adversary, but each user is honest when he is a sender. Hence, if a sender U_i is fixed and $amk_i^{(t)} \in \mathcal{ATI}_i^{(t)}$ is given, TRA-codes look like MRA-codes [14]. From this, it would be natural to assume a mapping $\mathcal{E}_{i,j}^{(S)} \to \mathcal{E}_{i,j}^{(R)}$, if $amk_i^{(t)} \in \mathcal{ATI}_i^{(t)}$ is given, in TRA-codes as in the model of MRA-codes (see Definition 3.1 in [14]). In addition, from the footnote of this page, we have assumed the above mapping $\rho_{i,j} : \mathcal{E}_{i,j}^{(S)} \to \mathcal{E}_{i,j}^{(R)} \times \mathcal{AMK}_i$. From the explanation, we consider that the assumption of existence of the above mappings is not so strange, rather natural, and we will show that these mappings actually exist in our simple direct construction in Section 4.4.

Then, we can derive lower bounds on success probabilities of attacks as follows.

Theorem 5. *For any $i_1, i_2 \in \{1, 2, \ldots, n\}$, any time $t \in \mathcal{T}$, any colluding group W with $U_{i_1}, U_{i_2} \notin W$, and $\tilde{W}$ with $U_{i_1} \notin \tilde{W}$ and $U_{i_2} \in \tilde{W}$, it holds that*

1. $\log P_{I_S}(U_{i_1}, U_{i_2}, t) \geq -I(MA_{i_1,i_2}^{(t)}; E_{i_1,i_2}^{(R)} \mid AMK)$
2. $\log P_{S_S}(U_{i_1}, U_{i_2}, t_1, t_2) \geq -I(\tilde{M}A_{i_1,i_2}^{(t_2)}; E_{i_1,i_2}^{(R)} \mid AMK, MA_{i_1,i_2}^{(t_1)})$
3. $\log P_{I_1}(U_{i_1}, U_{i_2}, W, t) \geq -I(MA_{i_1,i_2}^{(t)}; E_{i_1,i_2}^{(R)} \mid E_W^{(S)}, E_W^{(R)}, ATI^{(1)}, \ldots, ATI^{(\tau)})$
4. $\log P_{S_1}(U_{i_1}, U_{i_2}, W, t_1, t_2) \geq -I(\tilde{M}A_{i_1,i_2}^{(t_2)}; E_{i_1,i_2}^{(R)} \mid E_W^{(S)}, E_W^{(R)}, ATI^{(1)}, \ldots, ATI^{(\tau)}, MA_{i_1,i_2}^{(t_1)})$
5. $\log P_2(U_{i_1}, U_{i_2}, \tilde{W}, t) \geq -I(MA_{i_1,i_2}^{(t)}; ATI_{i_1}^{(t)} \mid E_{\tilde{W}}^{(S)}, E_{\tilde{W}}^{(R)}, ATI^{(1)}, \ldots, ATI^{(t-1)}, ATI^{(t+1)}, \ldots, ATI^{(\tau)})$

The proof can be shown in a way similar to that of [14, Theorem 3.2].

We next show lower bounds on memory-sizes of entities in TRA-codes. The proof is given in Appendix D.

Theorem 6. *Let Λ be an $(n, \omega, \tau; \epsilon)$-secure TRA-code. Let $q := \epsilon^{-1}$. Then, for any $i_1, i_2 \in \{1, 2, \ldots, n\}$ and $t \in \{1, 2, \ldots, \tau\}$, we have*

$$\begin{aligned}
&(i) \quad |\mathcal{E}_{i_2}^{(R)}| \geq q^{2(\omega+1)}, \quad (ii)\ |\mathcal{E}_{i_1}^{(S)}| \geq q^{2\omega+\tau+1}, \\
&(iii) \quad |\mathcal{ATI}^{(t)}| \geq q^{\omega+1}, \quad (iv)\ |\mathcal{AMK}| \geq q^{\tau(\omega+1)}, \\
&(v) \quad |\mathcal{A}_{i_1,i_2}^{(t)}| \geq q.
\end{aligned}$$

As we will see in Section 4.4, the above lower bounds are all tight since our direct construction will meet all the above inequalities with equalities. Therefore, we define optimality of constructions of TRA-codes as follows.

Definition 8. *A construction of $(n, \omega, \tau; \epsilon)$-secure TRA-codes is said to be* optimal *if it meets equality in every inequality of (i)-(v) in Theorem 6.*

[3] We assume that each user U_i potentially has partial information on a master-key, since a sender U_i can specify any time t (i.e., the sender U_i can generate $amk_i^{(t)} \in \mathcal{ATI}_i^{(t)}$ for $1 \leq \forall t \leq \tau$) but he cannot generate a time-signal $amk^{(t)} \in \mathcal{ATI}^{(t)}$.

4.3 Generic Construction of TRA-codes from TR-KA and A-codes

We propose a generic construction of $(n, \omega, \tau; \epsilon)$-secure TRA-codes from TR-KA and the traditional A-codes (e.g., [17]). First, we briefly explain the traditional A-codes as follows.

A-codes. We consider a scenario where there are three entities, a sender S, a receiver R, and an adversary A. The A-code Θ consists of a three-tuple of algorithms (*AGen*, *Auth*, *Ver*) with three spaces, $\tilde{\mathcal{M}}$, $\tilde{\mathcal{A}}$ and $\tilde{\mathcal{E}}$, where they are finite sets of possible messages, possible authenticators (or tags) and possible secret-keys, respectively. *AGen* is a key generation algorithm, which takes a security parameter on input and outputs a secret-key e. *Auth* is an algorithm for generating an authenticator. *Auth* takes a message $m \in \tilde{\mathcal{M}}$ and a secret-key $e \in \tilde{\mathcal{E}}$ on input and outputs an authenticator $\alpha \in \tilde{\mathcal{A}}$, and we write $\alpha = \mathit{Auth}(m, e)$ for it. On receiving (m, α), a receiver R can check the validity of it by using *Ver*. *Ver* takes a message m, an authenticator α and a secret-key e on input, and outputs *true* or *false*, and we write *true*$= \mathit{Ver}(m, \alpha, e)$ or *false*$= \mathit{Ver}(m, \alpha, e)$ for it. In A-codes, there are two kinds of attacks: *impersonation attacks* and *substitution attacks*. Here, Θ is said to be ϵ-*secure* if each of success probabilities of these attacks is at most ϵ (e.g., see [17] for details).

The detail of our generic construction of TRA-codes Λ=(*TAGen, AExt, TAuth, TVer*) by using TR-KA Π=(*Setup, Ext, KeyGen, KeyDer*) and A-codes Θ=(*AGen, Auth, Ver*) is given as follows. In our construction, Π, Θ and Λ satisfy the following conditions: $\mathcal{M}_A \times \mathcal{T} \subset \tilde{\mathcal{M}}$; $\mathcal{TCK} \subset \tilde{\mathcal{E}}$; $\mathcal{A} = \tilde{\mathcal{A}}$; $\mathcal{AMK} = \mathcal{TMK}$; $\mathcal{ATI} = \mathcal{TI}$; $\mathcal{E}^{(S)} = \mathcal{TUK}^{(S)}$; and $\mathcal{E}^{(R)} = \mathcal{TUK}^{(R)}$.

1. ***TAGen***. For a security parameter 1^k, *TAGen* outputs matching secret-keys $e_i = (e_i^{(S)}, e_i^{(R)})$ and amk^* for U_i $(1 \le i \le n)$ and T, respectively, as follows. *TAGen* calls *Setup* with input 1^k, and suppose $(tuk_1^{(S)}, tuk_1^{(R)}, tuk_2^{(S)}, tuk_2^{(R)},$ $\ldots, tuk_n^{(S)}, tuk_n^{(R)}, tmk^*) \leftarrow \mathit{Setup}(1^k)$. Then, *TAGen* outputs secret-keys $e_i^{(S)} := tuk_i^{(S)}, e_i^{(R)} := tuk_i^{(R)}$ and $amk^* := tmk^*$ for U_i $(1 \le i \le n)$ and T, respectively.

2. ***AExt***. For a master-key $amk^* = tmk^*$ and time t, *AExt* calls *Ext*, and suppose $tmk^{(t)} = \mathit{Ext}(tmk^*, t)$. Then, *AExt* outputs a time-signal at time t, $amk^{(t)} := tmk^{(t)}$.

3. ***TAuth***. For a message m, an authentication-key $e_{i_1}^{(S)} = tuk_{i_1}^{(S)}$, the specified time t and an identity U_{i_2}, *TAuth* calls *KeyGen*, and suppose $tck_{i_1,i_2}^{(t)} = \mathit{KeyGen}(tuk_{i_1}^{(S)}, t, U_{i_2})$. Then, *TAuth* calls *Auth*, and it computes an authenticator $\alpha = \mathit{Auth}((m, t), tck_{i_1,i_2}^{(t)})$. Finally, *TAuth* outputs an authenticator at time t, $\alpha_{i_1,i_2}^{(t)} := \alpha$.

4. ***TVer***. For a message m, the specified time t, an authenticator $\alpha_{i_1,i_2}^{(t)}$, a verification-key $e_{i_2}^{(R)} = tuk_{i_2}^{(R)}$, a time-signal $amk^{(t)} = tmk^{(t)}$ at the specified time t and an identity U_{i_1}, *TVer* calls *KeyDer* with inputting them, and suppose $tck_{i_1,i_2}^{(t)} = \mathit{KeyDer}(tuk_{i_2}^{(R)}, tmk^{(t)}, U_{i_1})$. Then, *TVer* outputs *true* if $\mathit{Ver}((m, t), \alpha_{i_1,i_2}^{(t)}, tck_{i_1,i_2}^{(t)}) =$*true*, and outputs *false* otherwise.

The security of the above construction is shown as follows.

Theorem 7. *Given an ϵ-secure A-code Θ and (n, ω, τ)-secure TR-KA Π in which common-keys are uniformly distributed over $\mathcal{TCK}$, then the TRA-code Λ formed by the above construction based on Θ and Π is $(n, \omega, \tau; \epsilon)$-secure.*

Proof. First, we show the proof of $P_{S_S} \le \epsilon$ to prove $P_{Server} \le \epsilon$ (i.e., condition (1)). Assume that TS tries to generate a fraudulent authenticated message at time t_2, (m', α', t_2), that will be accepted by a receiver U_{i_2}, after observing a valid authenticated message at time t_1, (m, α, t_1). Then, we have

$$\begin{aligned}
&\max_{(m',\alpha^{(t_2)}_{i_1,i_2},t_2)} \max_{(m,\alpha^{(t_1)}_{i_1,i_2},t_1)\neq(m',\alpha^{(t_2)}_{i_1,i_2},t_2)} \max_{amk^*} \max_{amk^{(t_2)}} \\
&\qquad \Pr(\mathit{TVer}(m', \alpha^{(t_2)}_{i_1,i_2}, t_2, e^{(R)}_{i_2}, amk^{(t_2)}, U_{i_1}) = \mathit{true} \mid (m, \alpha^{(t_1)}_{i_1,i_2}, t_1), amk^*) \\
&= \max_{(m',\alpha',t_2)} \max_{(m,\alpha,t_1)\neq(m',\alpha',t_2)} \max_{tmk^{(t_2)}} \max_{tmk^*} \\
&\qquad \Pr(\mathit{KeyDer}(tuk^{(R)}_{i_2}, tmk^{(t_2)}, U_{i_1}) = tck^{(t_2)}_{i_1,i_2} \wedge \mathit{Ver}((m', t_2), \alpha', tck^{(t_2)}_{i_1,i_2}) = \mathit{true} \mid (m, \alpha, t_1), tmk^*)
\end{aligned}$$

$$= \max_{(m',\alpha',t_2)} \max_{(m,\alpha,t_1)\neq(m',\alpha',t_2)} \max_{tmk^*} \Pr(\mathit{Ver}((m', t_2), \alpha', tck^{(t_2)}_{i_1,i_2}) = \mathit{true} \mid (m, \alpha, t_1), tmk^*) \tag{2}$$

$$= \max_{(m',\alpha',t_2)} \max_{(m,\alpha,t_1)\neq(m',\alpha',t_2)} \Pr(\mathit{Ver}((m', t_2), \alpha', C) = \mathit{true} \mid (m, \alpha, t_1)) \leq P_S \leq \epsilon, \tag{3}$$

where (2) follows from the correctness of TR-KA, (3) follows from Definition 2 (i.e., tmk^* is unhelpful to guess $tck^{(t_2)}_{i_1,i_2}$), and P_S is the success probability of substitution attacks in ϵ-secure A-codes. Thus, we have $P_{S_S} \leq \epsilon$. In a manner similar to this, we can prove $P_{I_S} \leq \epsilon$. Therefore, we have $P_{Server} = \max(P_{I_S}, P_{S_S}) \leq \epsilon$.

Next, we show the proof of $P_{S_1} \leq \epsilon$ to prove $P_1 \leq \epsilon$ (i.e., condition (2)). Assume that any colluding group W not including a targeted receiver tries to generate a fraudulent authenticated message at time t_2, (m', α', t_2), that will be accepted by a receiver U_{i_2}, after observing a valid authenticated message at time t_1, (m, α, t_1). Let $\text{Info}(W) := (e^{(S)}_W, e^{(R)}_W, amk^{(1)}, \ldots, amk^{(\tau)}) = (tuk^{(S)}_W, tuk^{(R)}_W, tmk^{(1)}, \ldots, tmk^{(\tau)})$. Then, we have

$$\begin{aligned}
&\max_{(m',\alpha^{(t_2)}_{i_1,i_2},t_2)} \max_{(m,\alpha^{(t_1)}_{i_1,i_2},t_1)\neq(m',\alpha^{(t_2)}_{i_1,i_2},t_2)} \max_{\text{Info}(W)} \\
&\qquad \Pr(TVer(m', \alpha^{(t_2)}_{i_1,i_2}, t_2, e^{(R)}_{i_2}, amk^{(t_2)}, U_{i_1}) = \mathit{true} \mid (m, \alpha^{(t_1)}_{i_1,i_2}, t_1), \text{Info}(W)) \\
&= \max_{(m',\alpha',t_2)} \max_{(m,\alpha,t_1)\neq(m',\alpha',t_2)} \max_{\text{Info}(W)} \\
&\qquad \Pr(\mathit{KeyDer}(tuk^{(R)}_{i_2}, tmk^{(t_2)}, U_{i_1}) = tck^{(t_2)}_{i_1,i_2} \wedge \mathit{Ver}((m', t_2), \alpha', tck^{(t_2)}_{i_1,i_2}) = \mathit{true} \mid (m, \alpha, t_1), \text{Info}(W))
\end{aligned}$$

$$= \max_{((m',t_2),\alpha',t_2)} \max_{((m,t_1),\alpha,t_1)\neq((m',t_2),\alpha',t_2)} \max_{\text{Info}(W)} \Pr(Ver((m', t_2), \alpha', tck^{(t_2)}_{i_1,i_2}) = \mathit{true} \mid ((m, t_1), \alpha, t_1), \text{Info}(W)) \tag{4}$$

$$= \max_{((m',t_2),\alpha',t_2)} \max_{((m,t_1),\alpha,t_1)\neq((m',t_2),\alpha',t_2)} \Pr(Ver((m', t_2), \alpha', tck^{(t_2)}_{i_1,i_2}) = \mathit{true} \mid ((m, t_1), \alpha, t_1)) \tag{5}$$

$$\leq P_S \leq \epsilon.$$

where (4) follows from the correctness of TR-KA, (5) follows from Definition 2 (i.e., $\text{Info}(W)$ is unhelpful to guess $tck^{(t_2)}_{i_1,i_2}$), and P_S is the success probability of substitution attacks in ϵ-secure A-codes. Thus, we have $P_{S_1} \leq \epsilon$. In a manner similar to this, we can prove $P_{I_1} \leq \epsilon$. Therefore, we have $P_1 = \max(P_{I_1}, P_{S_1}) \leq \epsilon$.

Finally, we show the proof of $P_2 \leq \epsilon$ (i.e., condition (3)). Assume that any colluding group W including a legitimate (but dishonest) receiver tries to check the validity of a target authenticated message without a time-signal at the specified time, even if W obtains time-signals at all the time except the specified time. Let

$$\begin{aligned}
\text{Info}(W) &:= (e^{(S)}_W, e^{(R)}_W, amk^{(1)}, \ldots, amk^{(t-1)}, amk^{(t+1)}, \ldots, amk^{(\tau)}) \\
&= (tuk^{(S)}_W, tuk^{(R)}_W, tmk^{(1)}, \ldots, tmk^{(t-1)}, tmk^{(t+1)}, \ldots, tmk^{(\tau)}).
\end{aligned}$$

Then, we have

$$
\begin{aligned}
&\max_{(m,\alpha^{(t)}_{i_1,i_2},t)}\ \max_{\mathrm{Info}(W)} \Pr(TVer(m,\alpha^{(t)}_{i_1,i_2},t,e^{(R)}_{i_2},amk^{(t)},U_{i_1}) = true \mid \mathrm{Info}(W))\\
&= \max_{(m,\alpha^{(t)}_{i_1,i_2},t)}\ \max_{\mathrm{Info}(W)} \Pr(KeyDer(tuk^{(R)}_{i_2},tmk^{(t)},U_{i_1}) = tck^{(t)}_{i_1,i_2} \wedge Ver((m,t),\alpha,tck^{(t)}_{i_1,i_2}) = true \mid \mathrm{Info}(W))\\
&\le \max_{(m,\alpha^{(t)}_{i_1,i_2},t)}\ \max_{\mathrm{Info}(W)} \Pr(Ver((m,t),\alpha,tck^{(t)}_{i_1,i_2}) = true \mid \mathrm{Info}(W))\\
&= \max_{(m,\alpha^{(t)}_{i_1,i_2},t)} \Pr(Ver((m,t),\alpha,tck^{(t)}_{i_1,i_2}) = true) \qquad (6)\\
&\le P_I \le \epsilon.
\end{aligned}
$$

where (6) follows from Definition 2 (i.e., Info(W) is unhelpful to guess $tck^{(t_2)}_{i_1,i_2}$) and P_I is the success probability of impersonation attacks in ϵ-secure A-codes. Thus, we have $P_2 \le \epsilon$. □

Remark 3. *Even if we apply optimal constructions of TR-KA and A-codes in the above generic construction, we cannot obtain an optimal construction of TRA-codes. For example, consider the optimal construction of TR-KA in Section 2.3 and the well-known optimal construction of A-codes given by $Auth(m,e) = am + b$, where m is an element of a finite field $\mathbb{F}_q$ and $e = (a,b) \in \mathbb{F}_q^2$. We can quite smoothly apply these constructions in our generic construction since both ones are given based on polynomials over $\mathbb{F}_q$. However, the resulting construction of TRA-codes is not optimal. Therefore, in the next section we will show that there exists a direct construction (i.e., a construction from scratch) which satisfies Definition 8.*

4.4 Direct Construction of TRA-codes by Polynomials over Finite Fields

We propose a direct construction of $(n,\omega,\tau;\epsilon)$-secure TRA-codes. In addition, it is shown that the construction is optimal. The detail of our construction of TRA-codes Λ=(*AGen, AExt, TAuth, TVer*) is given as follows.

1. ***AGen***. For a security parameter 1^k, *AGen* outputs matching secret-keys e_i and amk^* for U_i $(1 \le i \le n)$ and T, respectively, as follows. *AGen* picks a k-bit prime power q, where $q > \max(n,\tau)$, and constructs the finite field $\mathbb{F}_q$ with q elements. We assume that the identity of each user U_i is encoded as $U_i \in \mathbb{F}_q \backslash \{0\}$. Also, we assume $\mathcal{T} = \{1,2,\ldots,\tau\} \subset \mathbb{F}_q \backslash \{0\}$ by using appropriate encoding. And, *AGen* chooses uniformly at random $f(x,y) := \sum_{i=0}^{\omega}\sum_{j=0}^{\omega} a_{ij}x^iy^j$, $g(x,y) := \sum_{i=0}^{\omega}\sum_{j=0}^{\omega} b_{ij}x^iy^j$, and $amk^*(x,z) := \sum_{i=0}^{\omega}\sum_{k=0}^{\tau-1} c_{ik}x^iz^k$ over $\mathbb{F}_q$ with three variables x, y and z in which each degree of x and y is at most ω, and the degree of z is at most $\tau - 1$. *AGen* also computes $e^{(S)}_i$:= $(g(U_i,y)$, $f(U_i,\ y) + amk^*(U_i,\ z))$ and $e^{(R)}_i := (g(x,U_i),\ f(x,U_i))$ $(1 \le i \le n)$. Then, *AGen* outputs secret-keys $e_i := (e^{(S)}_i,\ e^{(R)}_i)$ $(1 \le i \le n)$ and $amk^* := amk^*(x,z)$ for U_i $(1 \le i \le n)$ and T, respectively.

2. ***AExt***. For $amk^* = amk^*(x,z)$ and time $t \in \mathcal{T}$, *Ext* outputs a time-signal at time t, $amk^{(t)}(x) := amk^*(x,t)$.

3. ***TAuth***. For a message m, a secret-key $e^{(S)}_{i_1}$, the specified time t and an identity U_{i_2}, *TAuth* generates an authenticator, $\alpha^{(t)}_{i_1,i_2} := g(U_{i_1},U_{i_2})m+\ f(U_{i_1},U_{i_2}) + amk^*(U_{i_1},t)$, and outputs it.

4. ***TVer***. For the message m, the authenticator $\alpha^{(t)}_{i_1,i_2}$, the specified time t, a secret-key $e^{(R)}_{i_2}$, a time-signal $amk^{(t)}$ at the specified time t and an identity U_{i_1}, *TVer* outputs *true* if $\alpha^{(t)}_{i_1,i_2} = g(U_{i_1}, U_{i_2})m+f(U_{i_1}, U_{i_2}) + amk^*(U_{i_1}, t)$ holds, and otherwise outputs *false*.

The security and optimality of the above construction is stated as follows.

Theorem 8. *The resulting TRA-code* Λ *by the above construction is* $(n, \omega, \tau; 1/q)$*-secure and optimal.*

Proof. In this proof, we can write $f(x, y)$, $g(x, y)$ and $tmk^*(x, z)$ in the form of

$$f(x,y) := (1, x, \ldots, x^\omega)A \begin{pmatrix} 1 \\ y \\ \vdots \\ y^\omega \end{pmatrix},\ g(x,y) := (1, x, \ldots, x^\omega)B \begin{pmatrix} 1 \\ y \\ \vdots \\ y^\omega \end{pmatrix},\ \text{and } amk^*(x,z) := (1, x, \ldots, x^\omega)C \begin{pmatrix} 1 \\ z \\ \vdots \\ z^{\tau-1} \end{pmatrix},$$

respectively, where A and B are $(\omega+1)\times(\omega+1)$ matrices and C is an $(\omega+1)\times\tau$ matrix, respectively. To complete the proof of Theorem 8, we show the following lemmas.

Lemma 4. *The above construction satisfies* $P_{Server} \le \frac{1}{q}$.

Proof. First, we show the proof of $P_{S_S} \le 1/q$. Assume that TS will generate a fraudulent authenticated message at time t_2 $(m', \alpha^{(t_2)}_{i_1,i_2}, t_2)$, under the following conditions: TS can obtain a valid authenticated message $(m, \alpha^{(t_1)}_{i_1,i_2}, t_1)$ where $m \ne m'$ and knows his master-key amk^*. To begin with, since TS knows amk^*, he can compute $amk^*(U_{i_1}, t_2)$. Therefore, he tries to generate $g(U_{i_1}, U_{i_2})m' + f(U_{i_1}, U_{i_2})$. Moreover, TS can obtain $g(U_{i_1}, U_{i_2})m + f(U_{i_1}, U_{i_2})$ by calculating $\alpha^{(t_1)}_{i_1,i_2} - amk^*(U_{i_1}, t_1)$. However, by applying $X := O$, $A := A$ and $Y := O$ in Proposition 1 in Appendix B, there are at least q candidates of A. Then, by applying $\boldsymbol{x} := (1, U_{i_1}, U^2_{i_1}, \ldots, U^\omega_{i_1})$, $A := A$ and $\boldsymbol{y} := {}^t(1, U_{i_2}, U^2_{i_2}, \ldots, U^\omega_{i_2})$ in Proposition 2 in Appendix B, TS cannot guess $f(U_{i_1}, U_{i_2}) = \boldsymbol{x}A\boldsymbol{y}$ with probability larger than $1/q$. In a similar way, we can prove that TS cannot guess $g(U_{i_1}, U_{i_2})$ with probability larger than $1/q$. Hence, $P_{S_S} \le 1/q$. We can also prove $P_{S_I} \le 1/q$. Thus, we have $P_{Server} = \max(P_{S_I}, P_{S_S}) \le 1/q$. □

Lemma 5. *The above construction satisfies* $P_1 \le \frac{1}{q}$.

Proof. First, we show the proof of $P_{1_S} \le 1/q$. Without loss of generality, we consider that $W := \{U_1, \ldots, U_\omega\}$ is a set of colluders such that $U_{i_1}, U_{i_2} \notin W$, and we write $\boldsymbol{x_i} := (1, U_i, U^2_i, \ldots, U^\omega_i)$ $(1 \le i \le n)$. Assume that W will generate a fraudulent authenticated message at time t_2 $(m', \alpha^{(t_2)}_{i_1,i_2}, t_2)$, under the following conditions: W can obtain ω user's secret-keys, all time-signals, and a valid authenticated message $(m, \alpha^{(t_1)}_{i_1,i_2}, t_1)$ where $m \ne m'$. Note that W can compute amk^* by all time-signals and calculate $amk^*(U_{i_1}, t_1)$ and $amk^*(U_{i_1}, t_2)$. Therefore, W tries to generate $g(U_{i_1}, U_{i_2})(m - m')$ to succeed in this substitution attack, since $\alpha^{(t_2)}_{i_1,i_2} = \alpha^{(t_1)}_{i_1,i_2} - g(U_{i_1}, U_{i_2})(m-m') - amk^*(U_{i_1}, t_1) + amk^*(U_{i_1}, t_2)$. W can compute $g(U_l, y)$ $(1 \le l \le \omega)$ by using $e^{(S)}_l(y, z)$ and $amk^*(U_l, z)$. Hence, W gets

$$g(U_l, y) = \boldsymbol{x}_l B \begin{pmatrix} 1 \\ y \\ \vdots \\ y^\omega \end{pmatrix},$$

for $1 \le l \le \omega$. Thus, W can know the following matrix:

$$X_U B := \begin{pmatrix} \boldsymbol{x}_1 \\ \boldsymbol{x}_2 \\ \vdots \\ \boldsymbol{x}_\omega \end{pmatrix} B.$$

In addition, W knows

$$g(x, U_l) = (1, x, \dots, x^\omega) B\ {}^t\boldsymbol{x}_l,$$

for $1 \le l \le \omega$ by their verification-keys $f(x, U_l)$ $(1 \le l \le \omega)$. Thus, W can know the following matrix:

$$B\ {}^tX_U := B\ ({}^t\boldsymbol{x}_1, {}^t\boldsymbol{x}_2, \cdots, {}^t\boldsymbol{x}_\omega).$$

By applying $X := X_U$, $A := B$ and $Y := {}^tX_U$ in Proposition 1 in Appendix B, there are at least q candidates of B. In addition, $\{\boldsymbol{x}_{i_1}, \boldsymbol{x}_1, \boldsymbol{x}_2, \dots, \boldsymbol{x}_\omega\}$ and $\{\boldsymbol{x}_{i_2}, \boldsymbol{x}_1, \boldsymbol{x}_2, \dots, \boldsymbol{x}_\omega\}$ are linearly independent, respectively, since $U_{i_1}, U_{i_2} \notin W$. Therefore, W cannot guess $g(U_{i_1}, U_{i_2}) = \boldsymbol{x}_{i_1} B\ {}^t\boldsymbol{x}_{i_2}$ with probability larger than $1/q$ by Proposition 2 in Appendix B. Hence, $P_{1_S} \le 1/q$. We can also prove $P_{1_I} \le 1/q$. Thus, we have $P_1 = \max(P_{1_I}, P_{1_S}) \le 1/q$. □

Lemma 6. *The above construction satisfies* $P_2 \le \frac{1}{q}$.

Proof. Without loss of generality, we suppose that $W := \{U_1, \dots, U_\omega\}$ is a set of colluders such that $U_{i_1} \notin W$, U_{i_1} is a targeted sender, U_ω is a targeted receiver, and τ is a specified time. In addition, we write $\boldsymbol{x_i} := (1, U_i, U_i^2, \dots, U_i^\omega)$ $(1 \le i \le n)$ and $\boldsymbol{y_i} := {}^t(1, i, i^2, \dots, i^{\tau-1})$ $(1 \le i \le \tau)$. To succeed in the substitution attack by a group of colluders W, W will try to check the validity of a target authenticated message without a time-signal at the specified time under the following conditions: W can obtain ω user's secret-keys, time-signals at all the time except the specified time τ, and a valid authenticated message $(m, \alpha_{i_1,\omega}^{(t_1)}, t)$. Note that W can get $f(U_{i_1}, U_\omega)$ and $g(U_{i_1}, U_\omega)$ since $U_\omega \in W$. Thus, W tries to obtain $amk^*(x, z)$ to know $f(U_{i_1}, U_\omega) + amk^*(U_{i_1}, \tau)$. W can compute $amk^*(U_l, z)$ $(1 \le l \le \omega)$ by using $e_l^{(S)}(y, z)$ and $f(U_l, z)$. Hence, W gets

$$amk^*(U_l, z) = \boldsymbol{x}_l C \begin{pmatrix} 1 \\ z \\ \vdots \\ z^{\tau-1} \end{pmatrix},$$

for $1 \le l \le \omega$. Thus, W can know the following matrix:

$$X_U C := \begin{pmatrix} \boldsymbol{x}_1 \\ \boldsymbol{x}_2 \\ \vdots \\ \boldsymbol{x}_\omega \end{pmatrix} C.$$

In addition, W obtains $amk^*(x, t) = (1, x, \dots, x^\omega) C\boldsymbol{y}_t$ for $1 \le t \le \tau - 1$ by time-signals at all except the time τ. Thus, W can know the following matrix:

$$CY_T := C(\boldsymbol{y}_1, \boldsymbol{y}_2, \cdots, \boldsymbol{y}_{\tau-1}).$$

By applying $X := X_U$, $A := C$ and $Y := Y_T$ in Proposition 1 in Appendix B, there are at least q candidates of C. In addition, $\{\boldsymbol{x}_{i_1}, \boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_\omega\}$ and $\{\boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_\tau\}$ are linearly independent, respectively, since $U_{i_1} \notin W$. Therefore, W cannot guess $amk^*(U_{i_1}, z) = \boldsymbol{x}_{i_1} C \boldsymbol{y}_\tau$ with probability larger than $1/q$ by Proposition 2 in Appendix B. Thus, we have $P_2 \leq 1/q$. □

Proof of Theorem 8. It follows that $\max(P_{Server}, P_1, P_2) \leq 1/q$ from the above lemmas. Finally, it is straightforward to see that the construction satisfies all the lower bounds in Theorem 6 with equalities. Therefore, the above construction is optimal. □

5 Relation to Information-Theoretic Key-Insulated Security

In this section, we show relationship between TR-KA and key-insulated key-agreement (KI-KA for short) in information-theoretic security setting.

5.1 Key-Insulated Key Agreement (KI-KA)

Recently, information-theoretically secure KI-KA is proposed by Seito and Shikata [15]. In KI-KA, there are $\tilde{n}$ users $U_1, U_2, \ldots, U_{\tilde{n}}$ where $\tilde{n}$ is a positive integer. And each user has two kinds of devices: a trusted device (e.g., a smart card, USB flash memory) which stores a master-key; and an insecure device in which a user's secret-key is stored. Here, the notion of a *secure device* implies that it is usually isolated from a network (e.g. the Internet or LAN) and that the attacker can neither wiretap nor substitute information stored in the device via the network. Here, we assume that the user U_i's secure device is expressed as H_i $(1 \leq i \leq \tilde{n})$. We also assume that the lifetime of systems is divided into discrete periods. And, at the beginning of each period j, U_i receives key-updating information from H_i by connecting with H_i, then U_i computes a secret-key at the period j by using the secret-key of the previous period and key-updating information. And then, any user U_{i_1} can share a common-key with any user U_{i_2} at a period j.

Formally, we describe the definition of the model of KI-KA shown in [15].

Definition 9 (KI-KA [15])**.** *A key-insulated key-agreement (KI-KA for short) $\tilde{\Pi}$ involves $2\tilde{n}+1$ entities, TI, U_1, U_2, ..., $U_{\tilde{n}}$ and H_1, H_2, ..., $H_{\tilde{n}}$, and consists of a four-tuple of algorithms (KGen, KUpd*, KUpd, KDer) with six spaces, $\mathcal{CK}$, $\mathcal{I}$, $\tilde{\mathcal{T}}$, $\hat{\mathcal{T}}$, $\mathcal{MK}$ and $\mathcal{UK}$, where all of the above algorithms except KGen are deterministic and all of the above spaces are finite. And, the detail of the notation is as follows.*

- *Entities: TI is a trusted initializer, U_i $(1 \leq i \leq \tilde{n})$ is a user and H_i $(1 \leq i \leq \tilde{n})$ is a secure device for U_i. Let $\tilde{\mathcal{U}} := \{U_1, U_2, \ldots, U_{\tilde{n}}\}$ be a set of users, and $\tilde{\mathcal{H}} := \{H_1, H_2, \ldots, H_{\tilde{n}}\}$ is a set of devices. It is assumed that the identity of each user U_i is also denoted by U_i.*

- *Spaces: $\mathcal{CK}$ is a set of possible common-keys, $\mathcal{I}_i$ is a set of possible key-updating information for U_i. Let $\mathcal{I} := \mathcal{I}_1 \cup \mathcal{I}_2 \cup \ldots \cup \mathcal{I}_{\tilde{n}}$. And $\tilde{\mathcal{T}} := \{1, 2, \ldots, N\}$ is a set of time periods. Let $\hat{\mathcal{T}} := \tilde{\mathcal{T}} \cup \{0\}$. Also $\mathcal{MK}_i$ is a set of possible master-keys for H_i. Let $\mathcal{MK} := \mathcal{MK}_1 \cup \mathcal{MK}_2 \cup \ldots \cup \mathcal{MK}_{\tilde{n}}$. And also $\mathcal{UK}_i^{(j)}$ is a set of possible secret-keys at a period j for U_i. Let $\mathcal{UK}_i := \mathcal{UK}_i^{(0)} \cup \mathcal{UK}_i^{(1)} \cup \ldots \cup \mathcal{UK}_i^{(N)}$ and $\mathcal{UK} := \mathcal{UK}_1 \cup \mathcal{UK}_2 \cup \ldots \cup \mathcal{UK}_{\tilde{n}}$.*

- *Algorithms: KGen is a key generation algorithm which on input a security parameter 1^k, outputs each user U_i's initial secret-key $uk_i^{(0)} \in \mathcal{UK}_i^{(0)}$ (i.e., a secret-key at the period 0) and each device H_i's master-key $mk_i \in \mathcal{MK}_i$. And, KUpd*: $\mathcal{MK} \times \hat{\mathcal{T}} \times \tilde{\mathcal{T}} \to \mathcal{I}$ is a key-updating algorithm for H_i $(1 \leq i \leq \tilde{n})$, and we write $mk_i^{(h,j)}$ =KUpd*(mk_i, h, j) where $mk_i^{(h,j)} \in \mathcal{I}_i$ is key-updating* *information. Also, KUpd: $\mathcal{UK} \times \mathcal{I} \to \mathcal{UK}$ is a key-updating algorithm for U_i ($1 \le i \le \tilde{n}$), and we describe $uk_i^{(j)}$ =KUpd($uk_i^{(h)}$, $mk_i^{(h,j)}$) where $uk_i^{(j)} \in \mathcal{UK}_i^{(j)}$ is a U_i's secret-key at a period j. KDer: $\mathcal{UK} \times \tilde{\mathcal{U}} \to \mathcal{CK}$ is a key derivation algorithm, and we write $ck_{i_1,i_2}^{(j)}$ =KDer($uk_{i_1}^{(j)}$,U_{i_2}) where $ck_{i_1,i_2}^{(j)} \in \mathcal{CK}$ is a common-key shared between U_{i_1} and U_{i_2} at a period j.*

In KI-KA, it is required that the following equation holds: for all possible $j \in \tilde{\mathcal{T}}$, $i_1, i_2 \in \{1, 2, \ldots, \tilde{n}\}$, $uk_{i_1}^{(j)} \in \mathcal{UK}_{i_1}^{(j)}$ and $uk_{i_2}^{(j)} \in \mathcal{UK}_{i_2}^{(j)}$, we have *KDer*($uk_{i_1}^{(j)}$, U_{i_2}) = *KDer*($uk_{i_2}^{(j)}$, U_{i_1}).

And, in KI-KA, the following security goal is considered.

- The adversary does not obtain any information on a common-key shared between two honest users at a target period.

And, as an adversarial model, it is assume that an adversary can obtain the following information on user's keys exposed in KI-KA.

- A user's secret-key from the insecure device.
- A user's master-key exposed (or robbed) from the secure device.

Especially, in KI-KA, it is considered that the following two types of exposure from targeted users.

- Type A: Targeted users' secret-keys exposure, which models compromise of targeted users' secret-keys from their insecure devices (i.e., the attack to steal a secret-key stored in an insecure device via a network).
- Type B: Targeted users' master-keys exposure, which models compromise of their secure devices by physical means (i.e., the attack to steal a master-key stored in a secure device directly).

To show the formal definition of the above security notions, we describe the several notations. Let ψ be the number of possible users whose master-keys are exposed, let λ be the number of possible users whose secret-keys are exposed per period, and let $\tilde{\omega}$ be a nonnegative integer with $\tilde{\omega} \ge \psi + \lambda$. And, let γ be the number of possible periods at which secret-keys are exposed per user. And also, let $\Psi := \{U_{i_1}, U_{i_2}, \ldots, U_{i_\psi}\} \in \mathcal{P}(\tilde{U}, \psi)$ be a set of users whose master-keys are exposed, and $\mathcal{MK}_\Psi := \mathcal{MK}_{i_1} \times \mathcal{MK}_{i_2} \times \cdots \times \mathcal{MK}_{i_\psi}$ be a set of master-keys exposed. Also let $\Lambda^{(j)} := \{U_{l_1}, U_{l_2}, \ldots, U_{l_\lambda}\} \in \mathcal{P}(\tilde{U}, \lambda)$ be a set of users whose secret-keys at the period j are exposed. Here, we note that $\Lambda^{(j)}$ satisfies the following condition: for every $i \in \{1, 2, \ldots, \tilde{n}\}$, $|\{j | U_i \in \Lambda^{(j)}$ for some $j \in \tilde{\mathcal{T}}\}| \le \gamma$. The above condition implies that for every U_i, the number of periods at which U_i's secret-keys may be exposed is at most γ. Also, let $\mathcal{UK}_\Lambda^{(j)} := \mathcal{UK}_{l_1}^{(j)} \times \mathcal{UK}_{l_2}^{(j)} \times \cdots \times \mathcal{UK}_{l_\lambda}^{(j)}$ be a set of users' secret-keys exposed at the period j.

And, let $\mathcal{CK}_{i_1,i_2}^{(j)}$ be a finite set of possible common-keys shared between U_{i_1} and U_{i_2} at a period j. Also, let $\mathcal{I}_i^{(h,j)} \subset \mathcal{I}_i$ be a finite set of possible U_i's key-updating information which is used for key-updating process from a period h to a period j. And, let $CK_{i_1,i_2}^{(j)}$, MK_Ψ and $UK_\Lambda^{(1)}, \ldots, UK_\Lambda^{(N)}$ be random variables which take values on $\mathcal{CK}_{i_1,i_2}^{(j)}$, $\mathcal{MK}_\Psi$ and $\mathcal{UK}_\Lambda^{(1)}, \ldots, \mathcal{UK}_\Lambda^{(N)}$, respectively. With these notation, we formally define security notions of KI-KA as follows.

Definition 10 ([15]). *Let $\tilde{\Pi}$ be a KI-KA and $\tilde{\omega} \ge \psi + \lambda$. $\tilde{\Pi}$ is said to be* $(\tilde{n}, \tilde{\omega}; N, \gamma)$-secure*, if the following conditions are satisfied:*

1. *For any U_{i_1}, $U_{i_2} \in \tilde{\mathcal{U}}$ and any $j \in \tilde{\mathcal{T}}$, it holds that $H(CK_{i_1,i_2}^{(j)} | UK_{i_1}^{(j)}, U_{i_2}) = 0$.*

2. *For any set of users $\Psi \in \mathcal{P}(\tilde{\mathcal{U}}, \psi)$ whose master-keys are exposed, any set of users $\Lambda^{(j)} \in \mathcal{P}(\tilde{\mathcal{U}}, \lambda)$ whose secret-keys at the period j are exposed, and any target period $t \in \tilde{\mathcal{T}}$, it holds that*

$$H(CK_{i_1,i_2}^{(t)} | MK_\Psi, UK_\Lambda^{(1)}, \ldots, UK_\Lambda^{(N)}) = H(CK_{i_1,i_2}^{(t)}).$$

under each of the following conditions: (a) any U_{i_1}, $U_{i_2} \notin \Psi$ and U_{i_1}, $U_{i_2} \notin \Lambda^{(t)}$; (b) any U_{i_1}, $U_{i_2} \in \Psi$ and U_{i_1}, $U_{i_2} \notin \Lambda^{(j)}$ $(1 \le j \le N)$.

In this paper, we introduce a slightly weaker security: There is no exposure of users' secret-keys at the target period; and either Type A (users' secret-key exposure) or Type B (users' master-key exposure) occurs. Formally, it is stated as follows.

Definition 11. *Let $\tilde{\Pi}$ be a KI-KA. $\tilde{\Pi}$ is said to be $(\tilde{n}, \tilde{\omega}; N, \gamma)$-*weakly-secure*, if the following conditions are satisfied.*

1. *For any $U_{i_1}, U_{i_2} \in \tilde{\mathcal{U}}$ and any $j \in \tilde{\mathcal{T}}$, it holds that $H(CK_{i_1,i_2}^{(j)} | UK_{i_1}^{(j)}, U_{i_2}) = 0$.*
2. *For any $U_{i_1}, U_{i_2} \in \tilde{\mathcal{U}}$ and any target period $t \in \tilde{\mathcal{T}}$, the following security conditions are sarisfied:*
   (a) *For any set of users $\Lambda^{(j)} \in \mathcal{P}(\tilde{\mathcal{U}}, \tilde{\omega})$ whose secret-keys at the period j $(1 \le j \le N, j \ne t)$ are exposed, it holds that*

   $$H(CK_{i_1,i_2}^{(t)} | UK_\Lambda^{(1)}, \ldots, UK_\Lambda^{(t-1)}, UK_\Lambda^{(t+1)}, \ldots, UK_\Lambda^{(N)}) = H(CK_{i_1,i_2}^{(t)}).$$

   (b) *For any set of users $\Psi \in \mathcal{P}(\tilde{\mathcal{U}}, \tilde{\omega})$ whose master-keys are exposed such that $U_{i_1}, U_{i_2} \notin \Psi$, it holds that $H(CK_{i_1,i_2}^{(t)} | MK_\Psi) = H(CK_{i_1,i_2}^{(t)})$.*

5.2 Relationship between TR-KA and KI-KA

In KI-KA, any user cannot update a secret-key without using key-updating information which is generated by the master-key. That is to say, the user's key-updating process is *controlled* by the device's master-key and key-updating information. On the other hand, in TR-KA, no receiver can derive a common-key without using a time-signal corresponding to a designated period (time). Namely, the receiver's common-key derivation process is *controlled* by the time-server's master-key and the time-signal. From the above observation, the mechanisms of KI-KA and TR-KA are similar in the point that a common-key (or a secret-key required for deriving a common-key) derivation process is *controlled* by a master-key.

The above statement is explicitly shown by proposing two generic constructions (or converters) in a simple way: one is a construction of KI-KA from TR-KA; and the other is a construction of TR-KA from KI-KA. In the following sections, we will see that the mechanisms of TR-KA and KI-KA are essentially close by showing the generic constructions.

5.2.1 KI-KA from TR-KA

We first propose a simple algorithm which converts a secure TR-KA Π=(*Setup, Ext, KeyGen, KeyDer*) into a secure KI-KA $\tilde{\Pi}$=(*KGen, KUpd*, KUpd, KDer*). More precisely, we propose a generic construction method of KI-KA by using TR-KA, and it meets the security requirements of KI-KA. The detail of the construction is as follows.

1. ***KGen***. For a security parameter 1^k, *KGen* outputs matching secret-keys for $U_1, \ldots, U_{\tilde{n}}$ and $H_1, \ldots, H_{\tilde{n}}$ as follows. *KGen* calls *Setup* with taking on input 1^k. Let ($tuk_1^{(S)}$, $tuk_1^{(R)}$, $tuk_2^{(S)}$, $tuk_2^{(R)}$, $\ldots$, $tuk_{\tilde{n}}^{(S)}$, $tuk_{\tilde{n}}^{(R)}$, tmk^*) be the output from *Setup*. Then, *KGen* outputs secret-keys $uk_i^{(0)} := (tuk_i^{(S)}, tuk_i^{(R)}, 0)$ and $mk_i := tmk^*$ for U_i and H_i, respectively.
2. ***KUpd*** * **and *KUpd***. For two periods $h \in \hat{\mathcal{T}}$, $j \in \tilde{\mathcal{T}}$ and $mk_i = tmk^*$, *KUpd** calls *Ext* and generates $tmk^{(j)} = Ext(tmk^*, j)$. Then, *KUpd** outputs a key-updating information $mk_i^{(h,j)} := tmk^{(j)}$. On the other hand, for $mk_i^{(h,j)}$ and $uk_i^{(h)} :=(tuk_i^{(S)}, tuk_i^{(R)}, h, tmk^{(h)})$, *KUpd* generates a secret-key at the period j, $uk_i^{(j)} :=(tuk_i^{(S)}, tuk_i^{(R)}, j, tmk^{(j)})$, and outputs it.
3. ***KDer***. For $uk_{i_1}^{(j)} = (tuk_{i_1}^{(S)}, tuk_{i_1}^{(R)}, j, tmk^{(j)})$ and an identity U_{i_2}, *KDer* calls *KeyGen* and *KeyDer* and generates the following two values:

$$tck_{i_1,i_2}^{(j)} = KeyGen(tuk_{i_1}^{(S)}, j, U_{i_2}), \quad tck_{i_2,i_1}^{(j)} = KeyDer(tuk_{i_1}^{(R)}, tmk^{(j)}, U_{i_2}).$$

Then, *KDer* outputs a common-key at a period j, $ck_{i_1,i_2}^{(j)} := tck_{i_1,i_2}^{(j)} \oplus tck_{i_2,i_1}^{(j)}$.

The security of the above construction is shown as follows.

Theorem 9. *If TR-KA Π is (n, ω, τ)-secure and common-keys are uniformly distributed over $\mathcal{TCK}$, then the KI-KA $\tilde{\Pi}$ formed by the above construction is $(\tilde{n}, \tilde{\omega}; N, \gamma)$-weakly-secure, where $\tilde{n} = n$, $\tilde{\omega} = \omega$ and $\gamma = \tau - 1$. Furthermore, the sizes of secret-keys required in the above construction are given as follows:*

$$|\mathcal{MK}_i| = |\mathcal{TMK}|, \quad |\mathcal{UK}_i^{(j)}| = |\mathcal{TUK}_i^{(S)}| \cdot |\mathcal{TUK}_i^{(R)}| \cdot |\mathcal{TI}^{(j)}| \cdot \tau,$$
$$|\mathcal{CK}_{i_1,i_2}^{(j)}| = |\mathcal{TCK}_{i_1,i_2}^{(j)}|, \quad |\mathcal{I}_i^{(h,j)}| = |\mathcal{TI}^{(j)}|.$$

Proof. From the requirement of TR-KA shown in Section 2, it is obvious that the proposed construction satisfies the first condition in Definition 11. And, we show the proposed construction fulfills the second conditions (a) and (b) in Definition 11. In the following, suppose that U_{i_1} and U_{i_2} are target users and $t \in \tilde{\mathcal{T}}$ is a target period, and that the adversary tries to obtain any information about a common-key $ck_{i_1,i_2}^{(t)}$ shared between U_{i_1} and U_{i_2} at the period t.

Condition (a). We consider the following case for (a) in Definition 11:

1. No devices' master-key is compromised, and no sender's secret-keys is compromised, i.e., $\Psi = \emptyset$ and $U_{i_1} \notin \Lambda^{(j)}$ for $1 \le j \le N$. Let $\Lambda^{(j)} := \{U_1, U_2, \ldots, U_{\tilde{\omega}-1}, U_{i_2}\}$[4] be a set of users whose secret-keys at the period j is compromised ($1 \le j \le N$, $j \ne t$); and

2. No user's secret-key at the targeted period t is compromised, i.e., $\Lambda^{(t)} := \emptyset$.

Then, we have

$$\begin{aligned}
& H(CK_{i_1,i_2}^{(t)} | UK_{\Lambda}^{(1)}, \ldots, UK_{\Lambda}^{(t-1)}, UK_{\Lambda}^{(t+1)}, \ldots, UK_{\Lambda}^{(N)}) \\
= \; & H(TCK_{i_1,i_2}^{(t)} \oplus TCK_{i_2,i_1}^{(t)} | TUK_W^{(S)}, TUK_W^{(R)}, TI^{(1)}, \ldots, TI^{(t-1)}, TI^{(t+1)}, \ldots, TI^{(N)}) \qquad (7) \\
= \; & H(TCK_{i_1,i_2}^{(t)} | TUK_W^{(S)}, TUK_W^{(R)}, TI^{(1)}, \ldots, TI^{(t-1)}, TI^{(t+1)}, \ldots, TI^{(N)}) \\
= \; & H(TCK_{i_1,i_2}^{(t)}) \qquad (8) \\
= \; & H(CK_{i_1,i_2}^{(t)}), \qquad (9)
\end{aligned}$$

[4] The case of $U_{i_2} \notin \Lambda^{(j)}$ can be similarly discussed, and we omit it here.

where $W = \{U_1, U_2, \ldots, U_{\tilde{\omega}-1}, U_{i_2}\}$, (7) and (9) follow from the construction, and (8) follows from Definition 2.

Condition (b). We consider the following case for (b) in Definition 11:

- No user's secret-key is compromised through a whole period, i.e. $\Lambda^{(j)} = \emptyset$ for $1 \le j \le N$. Let $\Psi (\neq \emptyset)$ be an arbitrary set of users whose master-keys are exposed (Note that $MK_\Psi = \{tmk^*\}$ for any $\Psi \neq \emptyset$ from the construction).

Then, we have

$$\begin{aligned} H(CK^{(t)}_{i_1,i_2}|MK_\Psi) &= H(TCK^{(t)}_{i_1,i_2} \oplus TCK^{(t)}_{i_2,i_1}|TMK) &(10)\\ &= H(TCK^{(t)}_{i_1,i_2} \oplus TCK^{(t)}_{i_2,i_1}) &(11)\\ &= H(CK^{(t)}_{i_1,i_2}), &(12)\end{aligned}$$

where (10) and (12) follow from the construction, and (11) follows from Definition 2. □

5.2.2 TR-KA from KI-KA

Next, we show a simple algorithm which converts a secure KI-KA $\tilde{\Pi}$=(*KGen, KUpd*, KUpd, KDer*) into a secure TR-KA Π=(*Setup, Ext, KeyGen, KeyDer*). We now describe a construction method of Π from $\tilde{\Pi}$.

1. ***Setup***. For a security parameter 1^k, *Setup* outputs each entity's secret-key as follows. *Setup* calls *KGen* with inputs 1^k to generate secret-keys for two sets $\tilde{\mathcal{U}} := \{U_{1.S}$, $U_{1.R}$, $U_{2.S}$, $U_{2.R}$, $\ldots$, $U_{n.S}$, $U_{n.R}\}$[5] and $\tilde{\mathcal{H}} := \{H_{1.S}$, $H_{1.R}$, $H_{2.S}$, $H_{2.R}$, $\ldots$, $H_{n.S}$, $H_{n.R}\}$. Let ($uk^{(0)}_{1.S}$, $uk^{(0)}_{1.R}$, $uk^{(0)}_{2.S}$, $uk^{(0)}_{2.R}$, $\ldots$, $uk^{(0)}_{n.S}$, $uk^{(0)}_{n.R}$, $mk_{1.S}$, $mk_{1.R}$, $mk_{2.S}$, $mk_{2.R}$, $\ldots$, $mk_{n.S}$, $mk_{n.R}$) be the output from *KGen*. Then, *Setup* outputs secret-keys $tuk^{(S)}_i$:=($uk^{(0)}_{i.S}$, $mk_{i.S}$), $tuk^{(R)}_i := uk^{(0)}_{i.R}$ and tmk^* :=($mk_{1.R}$, $mk_{2.R}$, $\ldots$, $mk_{n.R}$).

2. ***Ext***. For a master-key $tmk^* = (mk_{1.R}, mk_{2.R}, \ldots, mk_{n.R})$ and a period j, *Ext* calls *KUpd** n times and generates $mk^{(0,j)}_{i.R}$ =$KUpd^*(mk_{i.R}, 0, j)$ $(1 \le j \le n)$. Then, *Ext* outputs a time-signal at the period j, $tmk^{(j)}$:=($mk^{(0,j)}_{1.R}$, $\ldots$, $mk^{(0,j)}_{n.R}$).

3. ***KeyGen***. For $tuk^{(S)}_{i_1} = (uk^{(0)}_{i_1.S}, mk_{i_1.S})$ and a period j, and an identity U_{i_2}, *KeyGen* calls *KUpd** and *KUpd* generates $mk^{(0,j)}_{i_1.S}$ =$KUpd^*(mk_{i_1.S}, 0, j)$ and $uk^{(j)}_{i_1.S}$ =$KUpd(uk^{(0)}_{i_1.S}, mk^{(0,j)}_{i_1,S})$. Then, *KeyGen* computes $ck^{(j)}_{i_1.S,i_2.R}$ =$KDer(uk^{(j)}_{i_1.S}, U_{i_2.R})$ and outputs a common-key at a period j, $tck^{(j)}_{i_1,i_2} := ck^{(j)}_{i_1.S,i_2.R}$.

4. ***KeyDer***. For $tuk^{(R)}_{i_2} = uk^{(0)}_{i_2.R}$, $tmk^{(j)} = (mk^{(0,j)}_{1.R}, \ldots, mk^{(0,j)}_{n.R})$ and an identity U_{i_1}, *KeyDer* calls *KUpd* and generates $uk^{(j)}_{i_2.R}$ =$KUpd(uk^{(0)}_{i_2.R}, mk^{(0,j)}_{i_2.R})$. Then, *KeyGen* generates $ck^{(j)}_{i_2.R,i_1.S}$ =*KDer* ($uk^{(j)}_{i_2.R}$, $U_{i_1.S}$), and outputs a common-key at a period j, $tck^{(j)}_{i_1,i_2} := ck^{(j)}_{i_2.R,i_1.S}$.

We give a proof that the above construction is secure TR-KA as follows.

[5] In this construction, each identity $U_i \in \mathcal{U}$ consists of two identities $U_{i.S}, U_{i.R} \in \tilde{\mathcal{U}}$.

Theorem 10. *If KI-KA $\tilde{\Pi}$ is $(\tilde{n}, \tilde{\omega}; N, N)$-secure with $\frac{1}{2}\tilde{n} \leq \tilde{\omega}$, then the TR-KA Π formed by the above construction is (n, ω, τ)-secure, where $n = \frac{1}{2}\tilde{n}$, $\omega \leq \tilde{\omega} - \frac{1}{2}\tilde{n}$, and $\tau = N$. Furthermore, the sizes of secret-keys required in the above construction are as follows:*

$$|\mathcal{TMK}| = |\mathcal{MK}|^n, \quad |\mathcal{TUK}_i^{(S)}| = |\mathcal{UK}_i^{(0)}| \cdot |\mathcal{MK}_i|, \quad |\mathcal{TUK}_i^{(R)}| = |\mathcal{UK}_i^{(0)}|,$$
$$|\mathcal{TCK}_{i_1,i_2}^{(j)}| = |\mathcal{CK}_{i_1,i_2}^{(j)}|, \quad |\mathcal{TI}^{(j)}| = |\mathcal{I}_i^{(0,j)}|^n.$$

Proof. We show that the proposed construction satisfies the conditions (1)-(3) in Definition 2. In the following, suppose that U_{i_1} and U_{i_2} are target users, and that $t \in \mathcal{T}$ is the specified time.

Condition (1). Suppose $n \leq \tilde{\omega}$. Then, we have

$$\begin{aligned} H(TCK_{i_1,i_2}^{(t)}|TMK^*) &= H(CK_{i_1,i_2}^{(t)}|MK_\Psi) \\ &= H(CK_{i_1,i_2}^{(t)}) \qquad (13) \\ &= H(TCK_{i_1,i_2}^{(t)}), \qquad (14) \end{aligned}$$

where $\Psi = \{U_{1.R}, U_{2.R}, \ldots, U_{n.R}\}$, (13) follows from Definition 10, and (14) follows by the construction.

Condition (2). Suppose $n + \omega \leq \tilde{\omega}$. Without loss of generality, we consider the following case.

- $W = \{U_1, U_2, \ldots, U_\omega\}$ is a set of colluders such that $U_{i_1}, U_{i_2} \notin W$.
- W tries to obtain any information on $tck_{i_1,i_2}^{(t)}$.

Then, we have

$$\begin{aligned} & H(TCK_{i_1,i_2}^{(t)}|TUK_W^{(S)}, TUK_W^{(R)}, TI^{(1)}, \ldots, TI^{(\tau)}) \\ & \geq H(CK_{i_1,i_2}^{(t)}|MK_\Psi, UK_\Lambda^{(1)}, \ldots, UK_\Lambda^{(\tau)}) \\ & = H(CK_{i_1,i_2}^{(t)}) \qquad (15) \\ & = H(TCK_{i_1,i_2}^{(t)}), \qquad (16) \end{aligned}$$

where $\Psi = \{U_{1.S}, U_{2.S}, \ldots, U_{\omega.S}\}$ and $\Lambda^{(j)} = \{U_{1.R}, U_{2.R}, \ldots, U_{n.R}\}$ $(1 \leq j \leq \tau)$, (15) follows from Definition 10, and (16) follows by the construction. Obviously, we have

$$H(TCK_{i_1,i_2}^{(t)}|TUK_W^{(S)}, TUK_W^{(R)}, TI^{(1)}, \ldots, TI^{(\tau)}) \leq H(TCK_{i_1,i_2}^{(t)}).$$

Therefore, we obtain $H(TCK_{i_1,i_2}^{(t)}|TUK_W^{(S)}, TUK_W^{(R)}, TI^{(1)}, \ldots, TI^{(\tau)}) = H(TCK_{i_1,i_2}^{(t)})$.

Condition (3). Suppose $n + \omega \leq \tilde{\omega}$. Without loss of generality, we consider the following case.

- $W := \{U_1, U_2, \ldots, U_{\omega-1}, U_{i_2}\}$ is a set of colluders including a legitimate (but dishonest) receiver U_{i_2}.
- W tries to obtain any information about $tck_{i_1,i_2}^{(t)}$ by using information on time-signals at all the time except the specified time t.

Then, we obtain

$$H(TCK_{i_1,i_2}^{(t)}|TUK_W^{(S)}, TUK_W^{(R)}, TI^{(1)}, \ldots, TI^{(t-1)}, TI^{(t+1)}, \ldots, TI^{(\tau)})$$

$$\begin{aligned}
&\geq H(CK^{(t)}_{i_1,i_2}|MK_{\Psi}, UK^{(1)}_{\Lambda}, \ldots, UK^{(\tau)}_{\Lambda}) \\
&= H(CK^{(t)}_{i_1,i_2}) && (17) \\
&= H(TCK^{(t)}_{i_1,i_2}), && (18)
\end{aligned}$$

where $\Psi = \{U_{1.S}, U_{2.S}, \ldots, U_{\omega-1.S}, U_{i_2.S}\}$ and $\Lambda^{(j)} = \{U_{1.R}, U_{2.R}, \ldots, U_{n.R}\}$ $(1 \leq j \leq \tau,\ j \neq t)$, (17) follows from Definition 10, and (18) follows by the construction. Therefore, we have

$$H(TCK^{(t)}_{i_1,i_2}|TUK^{(S)}_{W}, TUK^{(R)}_{W}, TI^{(1)}, \ldots, TI^{(t-1)}, TI^{(t+1)}, \ldots, TI^{(\tau)}) = H(TCK^{(t)}_{i_1,i_2}).$$

□

6 Concluding Remarks

In this paper, we studied timed-release cryptography with information-theoretic security. Specifically, we first proposed a model and formalization of security for timed-release key-agreement (TR-KA) in information-theoretic security setting. In addition, we derived tight lower bounds on memory-sizes required for TR-KA, and we proposed the optimal direct construction.

Also, we proposed models and formalizations of security for timed-release encryption (TRE) and authentication-codes (TRA-codes) in information-theoretic security setting. We also presented simple generic constructions of TRE and TRA-codes, respectively. Furthermore, we derived tight lower bounds on memory-sizes required for TRE and TRA-codes, respectively, and we also proposed optimal direct constructions of TRE and TRA-codes, respectively.

Moreover, we showed the relationship between TR-KA and key-insulated key-agreement (KI-KA) in information-theoretic security setting. We have shown that there exists a simple algorithm which converts TR-KA into KI-KA, and vice versa. Therefore, we conclude that the mechanisms of TR-KA and KI-KA are essentially close.

Acknowledgments. The authors would like to thank anonymous reviewers of ICITS 2012 for their valuable comments.

References

[1] Boneh, D., Naor, M.: Timed Commitments. In: Bellare, M. (ed.) Advances in Cryptology - CRYPTO 2000, LNCS 1880, pp. 236-254, Springer, Heidelberg (2000).

[2] Cathalo, J., Libert, B., Quisquater, J.-J.: Efficient and Non-Interactive Timed-Release Encryption. In: Qing, S., Mao, W., López, J., Wang, G. (eds.) ICICS 2005, LNCS 3783, pp. 291-303, Springer, Heidelberg (2005).

[3] Chalkias, K., Hiristu-Varsakelis, D., Stephanides, G.: Improved Anonymous Timed-Release Encryption. In: Biskup, J., López, J. (eds.) ESORICS 2007, LNCS 4734, pp. 311-326, Springer, Heidelberg (2007).

[4] Chan, A.C.-F, Blake, I.F.: Scalable, Server-Passive, User-Anonymous Timed-Release Public Key Encryption from Bilinear Pairing. In: 25th International Conference on Distributed Computing Systems, pp. 504-513, IEEE, Los Almitos (2005). The full version is available at http://eprint.iacr.org/2004/211

[5] Cheon, J.H., Hopper, N., Kim Y., Osipkov I.: Timed-Release and Key-Insulated Public key Encryption. In: Di Crescenzo, G., Rubin, A. (eds.) FC 2006, LNCS 4107, pp. 191-205, Springer, Heidelberg (2006). The full version is available at `http://eprint.iacr.org/2004/231`

[6] Cheon, J.H., Hopper, N., Kim Y., Osipkov I.: Provably Secure Timed-Release Public Key Encryption. In: ACM Trans. Information and System Security 11(2), pp. 1-44, (2008).

[7] Fujioka, A., Okamoto, Y., Saito, T.: Generic Construction of Strongly Secure Timed-Release Public-Key Encryption. In: Parampalli, U., Hawkes, P. (eds.) ACISP 2011, LNCS 6812, pp. 319-336, Springer, Heidelberg (2011).

[8] Garay, J.A., Jakobsson, C.: Timed Release of Standard Digital Signatures, In: Blaze, M. (ed) FC 2002, LNCS 2357, pp. 168-182, Springer, Heidelberg (2003).

[9] Garay, J.A. Pomerance, M.: Timed Fair Exchange of Standard Signatures. In: Wright, R.N. (ed.) FC 2003, LNCS 2742, pp. 190-207, Springer, Heidelberg (2003).

[10] Kurosawa, K., Yoshida, T., Desmedt, Y., Burmester, M.: Some Bounds and a Construction for Secure Broadcast Encryption. In: Ohta, K., Pei, D. (eds.) Advances in Cryptology - ASIACRYPT'98, LNCS 1514, pp. 420-433, Springer, Heidelberg (1998)

[11] May, T.C.: Timed-release crypto. manuscript (1993).

[12] Rivest, R.: Unconditionally Secure Commitment and Oblivious Transfer Schemes Using Private Channels and a Trusted Initializer. manuscript (1999), available at `http://people.csail.mit.edu/rivest/Rivest-commitment.pdf`

[13] Rivest, R., Shamir, A., Wagner, D.A.: Time-lock puzzles and timed-release crypto. In: MIT LCS Tech. Report. MIT LCS TR-684 (1996).

[14] Safavi-naini, R., Wang, H.: Multireceiver Authentication Codes: Model, Bounds, Constructions and Extentions. In: Information and Computation, vol.151, pp.148-172.(1999)

[15] Seito, T., Shikata, J.: Information-Theoretically Secure Key-Insulated Key-Agreement. In: 2011 IEEE Information Theory Workshop (ITW), pp. 287-291, IEEE (2011).

[16] Shannon, C.E.: Communication theory of secrecy systems. Bell System Technical Journal 28, pp. 656-715, (1949).

[17] Simmons, G.J.: Authentication Theory/Coding Theory. In: Blakley, G.R. Chaum, D. (eds.) Advances in Cryptology - CRYPTO'84, LNCS 196, pp. 411-431, Springer, Heidelberg (1985).

[18] Watanabe, Y., Seito, T., Shikata, J.: Information-Theoretic Timed-Release Security: Key-Agreement, Encryption, and Authentication Codes. In: Smith, A. (ed.) 6th International Conference on Information-Theoretic Security, LNCS 7412, pp. 167-187, Springer, Heidelberg (2012).

A Proof of Theorem 1

The proof follows from the following lemmas.

Lemma 7. *$H(TUK_i^{(R)}) \geq (\omega+1)H(TCK)$ for any $i \in \{1, 2, \ldots, n\}$.*

Proof. For arbitrary $i \in \{1,2,\ldots,n\}$, we take a subset $B := \{l_1, l_2, \ldots, l_{\omega+1}\} \subset \{1,2,\ldots,n\}$ of indices of users such that $i \notin B$. Let $D_k := (l_k, i)$ and $W_k := \{l_1, l_2, \ldots, l_k\}$ for each k with $1 \leq k \leq \omega + 1$. Then, we have

$$\begin{aligned}
H(TUK_i^{(R)}) &\geq H(TUK_i^{(R)} \mid TI^{(t)}) \\
&\geq I(TCK_{D_1}^{(t)}, TCK_{D_2}^{(t)}, \ldots, TCK_{D_{\omega+1}}^{(t)}; TUK_i^{(R)} \mid TI^{(t)}) \\
&= H(TCK_{D_1}^{(t)}, TCK_{D_2}^{(t)}, \ldots, TCK_{D_{\omega+1}}^{(t)} \mid TI^{(t)}) \\
&\qquad - H(TCK_{D_1}^{(t)}, TCK_{D_2}^{(t)}, \ldots, TCK_{D_{\omega+1}}^{(t)} \mid TI^{(t)}, TUK_i^{(R)}) \\
&= H(TCK_{D_1}^{(t)}, TCK_{D_2}^{(t)}, \ldots, TCK_{D_{\omega+1}}^{(t)} \mid TI^{(t)}) \\
&= \sum_{k=1}^{\omega+1} H(TCK_{D_k}^{(t)} \mid TI^{(t)}, TCK_{D_1}^{(t)}, TCK_{D_2}^{(t)}, \ldots, TCK_{D_{k-1}}^{(t)}) \\
&\geq \sum_{k=1}^{\omega+1} H(TCK_{D_k}^{(t)} \mid TUK_{W_{k-1}}^{(S)}, TI^{(t)}) \\
&= \sum_{k=1}^{\omega+1} H(TCK_{D_k}^{(t)}) \qquad (19) \\
&= (\omega+1) H(TCK),
\end{aligned}$$

where (19) follows from the condition (2) in Definition 2. □

Lemma 8. *$H(TUK_i^{(S)}) \geq (\tau + \omega) H(TCK)$ for any $i \in \{1,2,\ldots,n\}$.*

Proof. For arbitrary $i \in \{1,2,\ldots,n\}$, we take a subset $B := \{l_1, l_2, \ldots, l_{\omega+1}\} \subset \{1,2,\ldots,n\}$ of indices of users such that $i \notin B$. Let $D_k := (i, l_k)$ and $W_k := \{l_1, l_2, \ldots, l_k\}$ for each k with $1 \leq k \leq \omega + 1$. Also, let $F_k^{(t)} := (TCK_{D_k}^{(1)}, TCK_{D_k}^{(2)},$
$\ldots, TCK_{D_k}^{(t)})$ and $G_k^{(t)} := (TCK_{D_1}^{(t)}, TCK_{D_2}^{(t)}, \ldots, TCK_{D_k}^{(t)})$ for $1 \leq k \leq \omega + 1$ and $1 \leq t \leq \tau$. Then, we have

$$\begin{aligned}
&H(TUK_i^{(S)}) \\
&\geq H(F_1^{(\tau)}, G_{\omega+1}^{(t)}) \\
&= H(F_1^{(\tau)}) + H(G_{\omega+1}^{(t)} \mid F_1^{(\tau)}) \\
&= \sum_{t=1}^{\tau} H(TCK_{D_1}^{(t)} \mid F_1^{(t-1)}) + \sum_{k=2}^{\omega+1} H(TCK_{D_k}^{(t)} \mid F_1^{(\tau)}, TCK_{D_2}^{(t)}, \ldots, TCK_{D_{k-1}}^{(t)}) \\
&\geq \sum_{t=1}^{\tau} H(TCK_{D_1}^{(t)} \mid TUK_{D_1}^{(R)}, TI^{(1)}, \ldots, TI^{(t-1)}) \\
&\qquad\qquad + \sum_{k=2}^{\omega+1} H(TCK_{D_k}^{(t)} \mid TUK_{W_{k-1}}^{(R)}, TI^{(1)}, \ldots, TI^{(\tau)}) \\
&= \sum_{t=1}^{\tau} H(TCK_{D_1}^{(t)}) + \sum_{k=2}^{\omega+1} H(TCK_{D_k}^{(t)}) \qquad (20) \\
&= (\tau + \omega) H(TCK),
\end{aligned}$$

where (20) follows from the conditions (2) and (3) in Definition 2. □

Lemma 9. *$H(TI^{(t)} \mid TI^{(1)}, \ldots, TI^{(t-1)}) \geq (\omega+1)H(TCK)$ for any $t \in \mathcal{T}$. In particular, $H(TI^{(t)}) \geq (\omega+1)H(TCK)$ for any $t \in \mathcal{T}$.*

Proof. For arbitrary $i \in \{1, 2, \ldots, n\}$, we take a subset $B := \{l_1, l_2, \ldots, l_{\omega+1}\} \subset \{1, 2, \ldots, n\}$ of indices of users such that $i = l_1$. Let $D_k := (l_k, i)$ and $W_k := \{l_1, l_2, \ldots, l_k\}$ for each k with $1 \leq k \leq \omega + 1$. Then, we have

$$\begin{aligned}
&H(TI^{(t)} \mid TI^{(1)}, \ldots, TI^{(t-1)}) \\
&\geq H(TI^{(t)} \mid TUK_i^{(R)}, TI^{(1)}, \ldots, TI^{(t-1)}) \\
&\geq I(TCK_{D_1}^{(t)}, TCK_{D_2}^{(t)}, \ldots, TCK_{D_{\omega+1}}^{(t)}; TI^{(t)} \mid TUK_i^{(R)}, TI^{(1)}, \ldots, TI^{(t-1)}) \\
&= H(TCK_{D_1}^{(t)}, TCK_{D_2}^{(t)}, \ldots, TCK_{D_{\omega+1}}^{(t)} \mid TUK_i^{(R)}, TI^{(1)}, \ldots, TI^{(t-1)}) \\
&\qquad - H(TCK_{D_1}^{(t)}, \ldots, TCK_{D_{\omega+1}}^{(t)} \mid TUK_i^{(R)}, TI^{(1)}, \ldots, TI^{(t)}) \\
&= H(TCK_{D_1}^{(t)}, TCK_{D_2}^{(t)}, \ldots, TCK_{D_{\omega+1}}^{(t)} \mid TUK_i^{(R)}, TI^{(1)}, \ldots, TI^{(t-1)}) \\
&= \sum_{k=1}^{\omega+1} H(TCK_{D_k}^{(t)} \mid TUK_i^{(R)}, TI^{(1)}, \ldots, TI^{(t-1)}, TCK_{D_1}^{(t)}, \ldots, TCK_{D_{k-1}}^{(t)}) \\
&\geq \sum_{k=1}^{\omega+1} H(TCK_{D_k}^{(t)} \mid TUK_{W_{k-1}}^{(S)}, TUK_i^{(R)}, TI^{(1)}, \ldots, TI^{(t-1)}) \\
&= \sum_{k=1}^{\omega+1} H(TCK_{D_k}^{(t)}) \qquad (21) \\
&= (\omega+1)H(TCK),
\end{aligned}$$

where (21) follows from the condition (3) in Definition 2. □

Lemma 10. *$H(TMK) \geq \tau(\omega+1)H(TCK)$.*

Proof. We have

$$\begin{aligned}
H(TMK) &\geq I(TI^{(1)}, \ldots, TI^{(\tau)}; TMK) \\
&= H(TI^{(1)}, \ldots, TI^{(\tau)}) - H(TI^{(1)}, \ldots, TI^{(\tau)} \mid TMK) \\
&= H(TI^{(1)}, \ldots, TI^{(\tau)}) \\
&= \sum_{t=1}^{\tau} H(TI^{(t)} \mid TI^{(1)}, \ldots, TI^{(t-1)}) \\
&= \tau(\omega+1)H(TCK),
\end{aligned}$$

where the last equality follows from Lemma 9. □

Proof of Theorem 1: From Lemmas 7-10, the proof of Theorem 1 is completed. □

B Technical Propositions

Proposition 1. *Let X be an $h \times i$ matrix, A be an $i \times j$ matrix, Y be a $j \times k$ matrix, W be an $h \times j$ matrix, and Z be an $i \times k$ matrix, respectively, where all entries of the matrices are elements in $\mathbb{F}_q$. When X, Y, W and Z are given, there are at least q solutions of A for the simultaneous linear equations, $W = XA$ and $Z = AY$, if $i > h$ and $j > k$.*

Proof. First, let X, A, and Y be

$$X = \begin{pmatrix} x_{1,1} & x_{1,2} & \cdots & x_{1,i} \\ x_{2,1} & x_{2,2} & \cdots & x_{2,i} \\ \vdots & \vdots & \ddots & \vdots \\ x_{h,1} & x_{h,2} & \cdots & x_{h,i} \end{pmatrix}, \ A = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,j} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,j} \\ \vdots & \vdots & \ddots & \vdots \\ a_{i,1} & a_{i,2} & \cdots & a_{i,j} \end{pmatrix} \text{ and } Y = \begin{pmatrix} y_{1,1} & y_{1,2} & \cdots & y_{1,k} \\ y_{2,1} & y_{2,2} & \cdots & y_{2,k} \\ \vdots & \vdots & \ddots & \vdots \\ y_{j,1} & y_{j,2} & \cdots & y_{j,k} \end{pmatrix},$$

respectively. Then, we can write

$$W = \begin{pmatrix} w_{1,1} & w_{1,2} & \cdots & w_{1,j} \\ w_{2,1} & w_{2,2} & \cdots & w_{2,j} \\ \vdots & \vdots & \ddots & \vdots \\ w_{h,1} & w_{h,2} & \cdots & w_{h,j} \end{pmatrix} \text{ and } Z = \begin{pmatrix} z_{1,1} & z_{1,2} & \cdots & z_{1,k} \\ z_{2,1} & z_{2,2} & \cdots & z_{2,k} \\ \vdots & \vdots & \ddots & \vdots \\ z_{i,1} & z_{i,2} & \cdots & z_{i,k} \end{pmatrix},$$

such that

$$\begin{aligned} w_{\ell,m} &= x_{\ell,1}a_{1,m} + x_{\ell,2}a_{2,m} + \cdots + x_{\ell,i}a_{i,m} \text{ for } 1 \le \ell \le h,\ 1 \le m \le j, \\ z_{\ell,m} &= a_{\ell,1}y_{1,m} + a_{\ell,2}y_{2,m} + \cdots + a_{\ell,j}y_{j,m} \text{ for } 1 \le \ell \le i,\ 1 \le m \le k. \end{aligned}$$

Since we have the equation $WY = XZ$, it holds that, for any α, β with $1 \le \alpha \le h$ and $1 \le \beta \le k$,

$$w_{\alpha,1}y_{1,\beta} + w_{\alpha,2}y_{2,\beta} + \cdots + w_{\alpha,j}y_{j,\beta} = x_{\alpha,1}z_{1,\beta} + x_{\alpha,2}z_{2,\beta} + \cdots + x_{\alpha,i}z_{i,\beta}.$$

Thus, with respect to unknowns $a_{s,t}$ $(1 \le s \le i,\ 1 \le t \le j)$, we have at most $hj + ik - hk$ linearly independent equations. Therefore, the number of unknowns not uniquely determined is at least

$$ij - (hj + ik - hk) = (i - h)(j - k),$$

and it is positive if $i > h$ and $j > k$. From this, it follows that A has at least q solutions. □

Proposition 2. *Let $i > h$ and $j > k$, and suppose that X, A, Y, W, and Z are the same as those in Proposition 1. Let $\boldsymbol{x} := (x_1, x_2, \ldots, x_i) \in (\mathbb{F}_q)^i$ and $\boldsymbol{y} := {}^t(y_1, y_2, \ldots, y_j) \in (\mathbb{F}_q)^j$ be vectors such that: $\boldsymbol{x}$ is not contained in the $\mathbb{F}_q$-vector space generated by row vectors of X; and $\boldsymbol{y}$ is not contained in the $\mathbb{F}_q$-vector space generated by column vectors of Y. Suppose that such X, Y, W, Z, $\boldsymbol{x}$, and $\boldsymbol{y}$ are arbitrarily given, and each entry of A is chosen from $\mathbb{F}_q$ uniformly at random such that $W = XA$ and $Z = AY$. Then, an element $\boldsymbol{x}A\boldsymbol{y} \in \mathbb{F}_q$ cannot be guessed with probability larger than $1/q$.*

Proof. Let $\chi := \{A \mid XA = W, AY = Z\}$ be the set of solutions of A for the simultaneous linear equations, $W = XA$ and $Z = AY$. First, we show the following lemmas.

Lemma 11. *Define $\chi_0 := \{A \mid XA = O, AY = O\}$, and let A_1 be a solution in χ. Then, χ_0 is a linear space over $\mathbb{F}_q$ with $\dim \chi_0 \ge 1$, and $\chi = \{A_0 + A_1 \mid A_0 \in \chi_0\}$.*

Proof. It is straightforward to see that χ_0 is a linear space over $\mathbb{F}_q$, and $\dim \chi_0 \ge 1$ follows from the special case of $W = Z = O$ in Proposition 1.

For generally given W and Z, let A_1 be an element in χ. For any $A \in \chi$, it holds that $XA = W$ and $AY = Z$, and hence $X(A - A_1) = O$ and $(A - A_1)Y = O$, which implies $A - A_1 \in \chi_0$. Thus, we have $\chi = \{A_0 + A_1 \mid A_0 \in \chi_0\}$. □

Lemma 12. *Let X and Y be an $h \times i$ matrix and a $j \times k$ matrix, respectively, with $i > h$ and $j > k$. Then, the $\mathbb{F}_q$-linear mapping $f : \chi_0 \to \mathbb{F}_q$ defined by $f(A) := \boldsymbol{x}A\boldsymbol{y}$ is surjective.*

Proof. First, we assume that X and Y are $(i-1)\times i$ matrix and $j \times (j-1)$ matrix, respectively, such that rank $X = i-1$ and rank $Y = j-1$. It is obvious that the mapping f is $\mathbb{F}_q$-linear. In addition, since f is $\mathbb{F}_q$-linear, Imf is a linear subspace of $\mathbb{F}_q$. Therefore, by Lemma 11, dim(Im f) is 0 or 1. We will show that dim(Im f) $= 1$ (i.e., Im $f = \mathbb{F}_q$). To prove this, it is sufficient to show that, for $A, A' \in \chi_0$ with $A \neq A'$, we have $\boldsymbol{x}A\boldsymbol{y} \neq \boldsymbol{x}A'\boldsymbol{y}$. Suppose on the contrary that $\boldsymbol{x}A\boldsymbol{y} = \boldsymbol{x}A'\boldsymbol{y}$. Let $\hat{X} := \begin{pmatrix} X \\ \boldsymbol{x} \end{pmatrix}$ and $\hat{Y} := (Y, \boldsymbol{y})$. Then, since $XA = XA' = O$ and $AY = A'Y = O$, we obtain $\hat{X}A\hat{Y} = \hat{X}A'\hat{Y}$. Since $\hat{X}$ and $\hat{Y}$ are invertible, we have $A = A'$, which implies contradiction. Therefore, f is surjective.

Next, we consider a general case that X and Y are $h \times i$ matrix and $j \times k$ matrix, respectively, with $i > h$ and $j > k$. Let $\tilde{X}$ be an $(i-1)\times i$ matrix such that: rank $\tilde{X} = i-1$; $\boldsymbol{x}$ is not contained in the $\mathbb{F}_q$-vector space generated by row vectors of $\tilde{X}$; and the $\mathbb{F}_q$-vector space generated by row vectors of $\tilde{X}$ contains the vector space generated by row vectors of X. Similarly, let $\tilde{Y}$ be an $j \times (j-1)$ matrix such that: rank $\tilde{Y} = j-1$; $\boldsymbol{y}$ is not contained in the $\mathbb{F}_q$-vector space generated by column vectors of $\tilde{Y}$; and the $\mathbb{F}_q$-vector space generated by column vectors of $\tilde{Y}$ contains the vector space generated by column vectors of Y. Letting $\tilde{\chi}_0 := \{A \mid \tilde{X}A = O,\ A\tilde{Y} = O\}$, and we have $\tilde{\chi}_0 \subset \chi_0$. Therefore, it holds that $f : \chi_0 \to \mathbb{F}_q$ defined by $f(A) := \boldsymbol{x}A\boldsymbol{y}$ is surjective, since $f \mid \tilde{\chi}_0$ is surjective as shown by the above paragraph. □

Proof of Proposition 2. We show that, if A is chosen from χ uniformly at random, a value of $\boldsymbol{x}A\boldsymbol{y}$ cannot be guessed with probability larger than $1/q$. For proving it, it is sufficient to show that, for every $t \in \mathbb{F}_q$, $\Pr[t = \boldsymbol{x}A\boldsymbol{y}] = 1/q$ if A is chosen from χ uniformly at random. Define $\hat{f} : \chi \to \mathbb{F}_q$ by $\hat{f}(A) := \boldsymbol{x}A\boldsymbol{y}$, and fix some $A_1 \in \chi$. Then, arbitrary $A \in \chi$ is expressed by $A = A_0 + A_1$ ($A_0 \in \chi_0$) by Lemma 11, and then, $\hat{f}(A) = \boldsymbol{x}A_0\boldsymbol{y} + \boldsymbol{x}A_1\boldsymbol{y} = f(A_0) + \boldsymbol{x}A_1\boldsymbol{y}$. Note that A being chosen from χ uniformly at random is equivalent to that A_0 being chosen from χ_0 uniformly at random. If A_0 is chosen from χ_0 uniformly at random, we have $\Pr[t = f(A_0)] = 1/q$ for every $t \in \mathbb{F}_q$ since f is $\mathbb{F}_q$-linear and surjective by Lemma 12. Therefore, since $f(A_0)$ takes every value of $\mathbb{F}_q$ with equal probability and $\boldsymbol{x}A_1\boldsymbol{y}$ is fixed, $\hat{f}(A) = f(A_0) + \boldsymbol{x}A_1\boldsymbol{y}$ takes every value of $\mathbb{F}_q$ with equal probability. □

C Proof of Theorem 3

The proof of Theorem 3 follows from the lemmas in this appendix. In this appendix, for any $i, j \in \{1, 2, \ldots, n\}$ and any $t \in \{1, 2, \ldots, \tau\}$, $M_{i,j}^{(t)}$ denotes the random variable which takes plaintexts to be sent from U_i to U_j at time t, and $M_{i,j}^{(t)}$ is i.i.d. according to P_M.

Lemma 13. *$H(DK_i) \geq (\omega+1)H(M)$ for any $i \in \{1, 2, \ldots, n\}$.*

Proof. For arbitrary $i \in \{1, 2, \ldots, n\}$, we take a subset $B := \{l_1, l_2, \ldots, l_{\omega+1}\} \subset \{1, 2, \ldots, n\}$ of indices of users such that $i \notin B$. Let $D_k := (l_k, i)$ with $1 \leq k \leq \omega+1$. Then, we have

$$\begin{aligned}
H(DK_i) &\geq H(DK_i \mid ETI^{(t)}, C_{D_1}^{(t)}, C_{D_2}^{(t)}, \ldots, C_{D_{\omega+1}}^{(t)}) \\
&\geq I(M_{D_1}^{(t)}, M_{D_2}^{(t)}, \ldots, M_{D_{\omega+1}}^{(t)}; DK_i \mid ETI^{(t)}, C_{D_1}^{(t)}, C_{D_2}^{(t)}, \ldots, C_{D_{\omega+1}}^{(t)}) \\
&= H(M_{D_1}^{(t)}, M_{D_2}^{(t)}, \ldots, M_{D_{\omega+1}}^{(t)} \mid ETI^{(t)}, C_{D_1}^{(t)}, C_{D_2}^{(t)}, \ldots, C_{D_{\omega+1}}^{(t)}) \\
&\qquad - H(M_{D_1}^{(t)}, M_{D_2}^{(t)}, \ldots, M_{D_{\omega+1}}^{(t)} \mid ETI^{(t)}, DK_i, C_{D_1}^{(t)}, C_{D_2}^{(t)}, \ldots, C_{D_{\omega+1}}^{(t)}) \\
&= H(M_{D_1}^{(t)}, M_{D_2}^{(t)}, \ldots, M_{D_{\omega+1}}^{(t)} \mid ETI^{(t)}, C_{D_1}^{(t)}, C_{D_2}^{(t)}, \ldots, C_{D_{\omega+1}}^{(t)})
\end{aligned}$$

$$\begin{aligned} &= \sum_{k=1}^{\omega+1} H(M_{D_k}^{(t)} \mid ETI^{(t)}, M_{D_1}^{(t)}, M_{D_2}^{(t)}, \ldots, M_{D_{k-1}}^{(t)}, C_{D_1}^{(t)}, C_{D_2}^{(t)}, \ldots, C_{D_{\omega+1}}^{(t)}) \\ &= \sum_{k=1}^{\omega+1} H(M_{D_k}^{(t)}) \qquad (22) \\ &= (\omega+1)H(M), \end{aligned}$$

where (22) is shown by following: Let $W_k := \{l_1, l_2, \ldots, l_{k-1}, l_{k+1}, \ldots, l_{\omega+1}\}$ for each k with $1 \leq k \leq \omega+1$. Then, we have

$$\begin{aligned} & H(M_{D_k}^{(t)} \mid C_{D_k}^{(t)}, EK_{W_k}, ETI^{(t)}) \\ = \; & H(M_{D_k}^{(t)} \mid C_{D_k}^{(t)}, EK_{W_k}, ETI^{(t)}, M_{D_1}^{(t)}, \ldots, M_{D_{k-1}}^{(t)}, M_{D_{k+1}}^{(t)}, \ldots, M_{D_{\omega+1}}^{(t)}) \\ \leq \; & H(M_{D_k}^{(t)} \mid M_{D_1}^{(t)}, \ldots, M_{D_{k-1}}^{(t)}, C_{D_1}^{(t)}, \ldots, C_{D_{\omega+1}}^{(t)}, ETI^{(t)}) \\ \leq \; & H(M_{D_k}^{(t)}). \end{aligned}$$

And, we have $H(M_{D_k}^{(t)} \mid C_{D_k}^{(t)}, EK_{W_k}, ETI^{(t)}) = H(M_{D_k}^{(t)})$ from the condition (2) in Definition 5. Therefore, we have $H(M_{D_k}^{(t)} \mid M_{D_1}^{(t)}, \ldots, M_{D_{k-1}}^{(t)}, C_{D_1}^{(t)}, \ldots, C_{D_{\omega+1}}^{(t)}, ETI^{(t)}) = H(M_{D_k}^{(t)})$. □

Lemma 14. *$H(EK_i) \geq (\tau+\omega)H(M)$ for any $i \in \{1, 2, \ldots, n\}$.*

Proof. For arbitrary $i \in \{1, 2, \ldots, n\}$, we take a subset $B := \{l_1, l_2, \ldots, l_{\omega+1}\} \subset \{1, 2, \ldots, n\}$ of indices of users such that $i \notin B$. Let $D_k := (i, l_k)$ with $1 \leq k \leq \omega+1$. Also, let $F_k^{(t)} := (M_{D_k}^{(1)}, M_{D_k}^{(2)}, \ldots, M_{D_k}^{(t)})$, $G_k^{(t)} := (M_{D_1}^{(t)}, M_{D_2}^{(t)}, \ldots, M_{D_k}^{(t)})$, $FC_k^{(t)} := (C_{D_k}^{(1)}, C_{D_k}^{(2)}, \ldots, C_{D_k}^{(t)})$, and $GC_k^{(t)} := (C_{D_1}^{(t)}, C_{D_2}^{(t)}, \ldots, C_{D_k}^{(t)})$ for $1 \leq k \leq \omega+1$ and $1 \leq t \leq \tau$. Then, we have

$$\begin{aligned} & H(EK_i) \\ & = H(EK_i \mid F_1^{(\tau-1)}, G_{\omega+1}^{(\tau)}) \\ & \geq I(EK_i; FC_1^{(\tau-1)}, GC_{\omega+1}^{(\tau)} \mid F_1^{(\tau-1)}, G_{\omega+1}^{(\tau)}) \\ & = H(FC_1^{(\tau-1)}, GC_{\omega+1}^{(\tau)} \mid F_1^{(\tau-1)}, G_{\omega+1}^{(\tau)}) - H(FC_1^{(\tau-1)}, GC_{\omega+1}^{(\tau)} \mid F_1^{(\tau-1)}, G_{\omega+1}^{(\tau)}, EK_i) \\ & = H(FC_1^{(\tau-1)}, GC_{\omega+1}^{(\tau)} \mid F_1^{(\tau-1)}, G_{\omega+1}^{(\tau)}) \qquad (23) \\ & = H(FC_1^{(\tau-1)} \mid F_1^{(\tau-1)}, G_{\omega+1}^{(\tau)}) + H(GC_{\omega+1}^{(\tau)} \mid F_1^{(\tau-1)}, G_{\omega+1}^{(\tau)}, FC_1^{(\tau-1)}) \\ & = \sum_{t=1}^{\tau-1} H(C_{D_1}^{(t)} \mid F_1^{(\tau-1)}, G_{\omega+1}^{(\tau)}, C_{D_1}^{(1)}, \ldots, C_{D_1}^{(t-1)}) + \sum_{j=1}^{\omega+1} H(C_{D_j}^{(\tau)} \mid F_1^{(\tau-1)}, G_{\omega+1}^{(\tau)}, FC_1^{(\tau-1)}, C_{D_1}^{(\tau)}, \ldots, C_{D_{j-1}}^{(\tau)}) \\ & \geq (\tau+\omega)H(M), \qquad (24) \end{aligned}$$

where (23) follows from *Enc* algorithm (i.e., $H(FC_1^{(\tau-1)}, GC_{\omega+1}^{(\tau)} \mid F_1^{(\tau-1)}, G_{\omega+1}^{(\tau)}, EK_i) = 0$), and (24) follows from the following claims:

Claim 1. *$H(C_{D_1}^{(t)} \mid F_1^{(\tau-1)}, G_{\omega+1}^{(\tau)}, C_{D_1}^{(1)}, \ldots, C_{D_1}^{(t-1)}) \geq H(M_{D_1}^{(\tau)})$ for $1 \leq t \leq \tau-1$.*

Proof. Let $\tilde{F}_1^{(t,\tau-1)} := (M_{D_1}^{(1)}, M_{D_1}^{(2)}, \ldots, M_{D_1}^{(t-1)}, M_{D_1}^{(t+1)}, \ldots, M_{D_1}^{(\tau-1)})$.

First, since $M_{D_1}^{(t)}$ is independent of $(\tilde{F}_1^{(t,\tau-1)}, G_{\omega+1}^{(\tau)}, C_{D_1}^{(1)}, \ldots, C_{D_1}^{(t-1)})$ and $C_{D_1}^{(t)}$ (see Definition 5), we have

$$H(C_{D_1}^{(t)} \mid F_1^{(\tau-1)}, G_{\omega+1}^{(\tau)}, C_{D_1}^{(1)}, \ldots, C_{D_1}^{(t-1)}) = H(C_{D_1}^{(t)} \mid \tilde{F}_1^{(t,\tau-1)}, G_{\omega+1}^{(\tau)}, C_{D_1}^{(1)}, \ldots, C_{D_1}^{(t-1)}). \qquad (25)$$

Next, we have

$$\begin{aligned}
&H(C_{D_1}^{(t)}, M_{D_1}^{(t)}, EK_i, DK_{l_1}, ETI^{(t)} \mid \tilde{F}_1^{(t,\tau-1)}, G_{\omega+1}^{(\tau)}, C_{D_1}^{(1)}, \ldots, C_{D_1}^{(t-1)}) \\
=&H(M_{D_1}^{(t)}, EK_i, DK_{l_1}, ETI^{(t)} \mid \tilde{F}_1^{(t,\tau-1)}, G_{\omega+1}^{(\tau)}, C_{D_1}^{(1)}, \ldots, C_{D_1}^{(t-1)}) \\
&\qquad + H(C_{D_1}^{(t)} \mid F_1^{(\tau-1)}, G_{\omega+1}^{(\tau)}, C_{D_1}^{(1)}, \ldots, C_{D_1}^{(t-1)}, EK_i, DK_{l_1}, ETI^{(t)}) \\
=&H(M_{D_1}^{(t)}, EK_i, DK_{l_1}, ETI^{(t)} \mid \tilde{F}_1^{(t,\tau-1)}, G_{\omega+1}^{(\tau)}, C_{D_1}^{(1)}, \ldots, C_{D_1}^{(t-1)}), \qquad (26)
\end{aligned}$$

where (26) follows from *Enc* algorithm in Definition 4 (i.e., $H(C_{i,l_1}^{(t)} \mid M_{i,l_1}^{(t)}, EK_i) = 0$).

On the other hand, we have

$$\begin{aligned}
&H(C_{D_1}^{(t)}, M_{D_1}^{(t)}, EK_i, DK_{l_1}, ETI^{(t)} \mid \tilde{F}_1^{(t,\tau-1)}, G_{\omega+1}^{(\tau)}, C_{D_1}^{(1)}, \ldots, C_{D_1}^{(t-1)}) \\
=&H(C_{D_1}^{(t)}, EK_i, DK_{l_1}, ETI^{(t)} \mid \tilde{F}_1^{(t,\tau-1)}, G_{\omega+1}^{(\tau)}, C_{D_1}^{(1)}, \ldots, C_{D_1}^{(t-1)}) \\
&\qquad + H(M_{D_1}^{(t)} \mid \tilde{F}_1^{(t,\tau-1)}, G_{\omega+1}^{(\tau)}, C_{D_1}^{(1)}, \ldots, C_{D_1}^{(t)}, EK_i, DK_{l_1}, ETI^{(t)}) \\
=&H(C_{D_1}^{(t)}, EK_i, DK_{l_1}, ETI^{(t)} \mid \tilde{F}_1^{(t,\tau-1)}, G_{\omega+1}^{(\tau)}, C_{D_1}^{(1)}, \ldots, C_{D_1}^{(t-1)}), \qquad (27)
\end{aligned}$$

where (27) follows from *Dec* algorithm in Definition 4 (i.e., $H(M_{i,l_1}^{(t)} \mid C_{i,l_1}^{(t)}, DK_{l_1}, ETI^{(t)}) = 0$).

Therefore, we have

$$\begin{aligned}
&H(C_{D_1}^{(t)} \mid \tilde{F}_1^{(t,\tau-1)}, G_{\omega+1}^{(\tau)}, C_{D_1}^{(1)}, \ldots, C_{D_1}^{(t-1)}) + H(EK_i, DK_{l_1}, ETI^{(t)} \mid \tilde{F}_1^{(t,\tau-1)}, G_{\omega+1}^{(\tau)}, C_{D_1}^{(1)}, \ldots, C_{D_1}^{(t-1)}) \\
\geq&H(C_{D_1}^{(t)}, EK_i, DK_{l_1}, ETI^{(t)} \mid \tilde{F}_1^{(t,\tau-1)}, G_{\omega+1}^{(\tau)}, C_{D_1}^{(1)}, \ldots, C_{D_1}^{(t-1)}) \\
=&H(M_{D_1}^{(t)}, EK_i, DK_{l_1}, ETI^{(t)} \mid \tilde{F}_1^{(t,\tau-1)}, G_{\omega+1}^{(\tau)}, C_{D_1}^{(1)}, \ldots, C_{D_1}^{(t-1)}) \qquad (28) \\
=&H(M_{D_1}^{(t)}) + H(EK_i, DK_{l_1}, ETI^{(t)} \mid \tilde{F}_1^{(t,\tau-1)}, G_{\omega+1}^{(\tau)}, C_{D_1}^{(1)}, \ldots, C_{D_1}^{(t-1)}), \qquad (29)
\end{aligned}$$

where (28) follows from (26) and (27), and (29) follows from that $M_{D_1}^{(t)}$ is independent of $(EK_i, DK_{l_1}, ETI^{(t)}, \tilde{F}_1^{(t,\tau-1)}, G_{\omega+1}^{(\tau)}, C_{D_1}^{(1)}, \ldots, C_{D_1}^{(t-1)})$.

Hence, we have

$$H(C_{D_1}^{(t)} \mid \tilde{F}_1^{(t,\tau-1)}, G_{\omega+1}^{(\tau)}, C_{D_1}^{(1)}, \ldots, C_{D_1}^{(t-1)}) \geq H(M_{D_1}^{(t)}). \qquad (30)$$

Finally, from (25) and (30), we have $H(C_{D_1}^{(t)} \mid F_1^{(\tau-1)}, G_{\omega+1}^{(\tau)}, C_{D_1}^{(1)}, \ldots, C_{D_1}^{(t-1)}) \geq H(M_{D_1}^{(t)})$ for $1 \leq t \leq \tau - 1$. □

Claim 2. *$H(C_{D_j}^{(\tau)} \mid F_1^{(\tau-1)}, G_{\omega+1}^{(\tau)}, FC_1^{(\tau-1)}, C_{D_1}^{(\tau)}, \ldots, C_{D_{j-1}}^{(\tau)}) \geq H(M_{D_j}^{(\tau)})$ for $1 \leq j \leq \omega + 1$.*

Proof. We can prove this lemma in a similar way to the proof of Claim 1. Let $\tilde{G}_{j,\omega+1}^{(\tau)} := (M_{D_1}^{(\tau)}, M_{D_2}^{(\tau)}, \ldots, M_{D_{j-1}}^{(\tau)}, M_{D_{j+1}}^{(\tau)}, \ldots, M_{D_{\omega+1}}^{(\tau)})$.

First, since $M_{D_j}^{(\tau)}$ is independent of $(F_1^{(\tau-1)}, \tilde{G}_{j,\omega+1}^{(\tau)}, FC_1^{(\tau-1)}, C_{D_1}^{(\tau)}, \ldots, C_{D_{j-1}}^{(\tau)})$ and $C_{D_j}^{(\tau)}$ (see Definition **??**), we have

$$H(C_{D_j}^{(\tau)} \mid F_1^{(\tau-1)}, G_{\omega+1}^{(\tau)}, FC_1^{(\tau-1)}, C_{D_1}^{(\tau)}, \ldots, C_{D_{j-1}}^{(\tau)}) = H(C_{D_j}^{(\tau)} \mid F_1^{(\tau-1)}, \tilde{G}_{j,\omega+1}^{(\tau)}, FC_1^{(\tau-1)}, C_{D_1}^{(\tau)}, \ldots, C_{D_{j-1}}^{(\tau)}). \qquad (31)$$

Next, we have

$$\begin{aligned}
&H(C_{D_j}^{(\tau)}, M_{D_j}^{(\tau)}, EK_i, DK_{l_j}, ETI^{(\tau)} \mid F_1^{(\tau-1)}, \tilde{G}_{j,\omega+1}^{(\tau)}, FC_1^{(\tau-1)}, C_{D_1}^{(\tau)}, \dots, C_{D_{j-1}}^{(\tau)}) \\
=&H(M_{D_j}^{(\tau)}, EK_i, DK_{l_j}, ETI^{(\tau)} \mid F_1^{(\tau-1)}, \tilde{G}_{j,\omega+1}^{(\tau)}, FC_1^{(\tau-1)}, C_{D_1}^{(\tau)}, \dots, C_{D_{j-1}}^{(\tau)}) \\
&\qquad + H(C_{D_j}^{(\tau)} \mid F_1^{(\tau-1)}, G_{\omega+1}^{(\tau)}, FC_1^{(\tau-1)}, C_{D_1}^{(\tau)}, \dots, C_{D_{j-1}}^{(\tau)}, M_{D_j}^{(t)}, EK_i, DK_{l_j}, ETI^{(\tau)}) \\
=&H(M_{D_j}^{(\tau)}, EK_i, DK_{l_j}, ETI^{(\tau)} \mid F_1^{(\tau-1)}, \tilde{G}_{j,\omega+1}^{(\tau)}, FC_1^{(\tau-1)}, C_{D_1}^{(\tau)}, \dots, C_{D_{j-1}}^{(\tau)}), \qquad (32)
\end{aligned}$$

where (32) follows from *Enc* algorithm in Definition 4 (i.e., $H(C_{i,l_j}^{(\tau)} \mid M_{i,l_j}^{(\tau)}, EK_i) = 0$).

On the other hand, we have

$$\begin{aligned}
&H(C_{D_j}^{(\tau)}, M_{D_j}^{(\tau)}, EK_i, DK_{l_j}, ETI^{(\tau)} \mid F_1^{(\tau-1)}, \tilde{G}_{j,\omega+1}^{(\tau)}, FC_1^{(\tau-1)}, C_{D_1}^{(\tau)}, \dots, F_1^{(\tau-1)}, G_{\omega+1}^{(\tau)}, C_{D_{j-1}}^{(\tau)}) \\
=&H(C_{D_j}^{(\tau)}, EK_i, DK_{l_j}, ETI^{(\tau)} \mid F_1^{(\tau-1)}, \tilde{G}_{j,\omega+1}^{(\tau)}, FC_1^{(\tau-1)}, C_{D_1}^{(\tau)}, \dots, C_{D_{j-1}}^{(\tau)}) \\
&\qquad + H(M_{D_j}^{(\tau)} \mid F_1^{(\tau-1)}, \tilde{G}_{j,\omega+1}^{(\tau)}, FC_1^{(\tau-1)}, C_{D_1}^{(\tau)}, \dots, C_{D_j}^{(\tau)}, EK_i, DK_{l_j}, ETI^{(\tau)}) \\
=&H(C_{D_j}^{(\tau)}, EK_i, DK_{l_j}, ETI^{(\tau)} \mid F_1^{(\tau-1)}, \tilde{G}_{j,\omega+1}^{(\tau)}, FC_1^{(\tau-1)}, C_{D_1}^{(\tau)}, \dots, C_{D_{j-1}}^{(\tau)}), \qquad (33)
\end{aligned}$$

where (33) follows from *Dec* algorithm in Definition 4 (i.e., $H(M_{i,l_j}^{(\tau)} \mid C_{i,l_j}^{(\tau)}, DK_{l_j}, ETI^{(\tau)}) = 0$).

Therefore, we have

$$\begin{aligned}
&H(C_{D_j}^{(\tau)} \mid F_1^{(\tau-1)}, \tilde{G}_{j,\omega+1}^{(\tau)}, FC_1^{(\tau-1)}, C_{D_1}^{(\tau)}, \dots, C_{D_{j-1}}^{(\tau)}) \\
&\qquad\qquad + H(EK_i, DK_{l_j}, ETI^{(\tau)} \mid F_1^{(\tau-1)}, \tilde{G}_{j,\omega+1}^{(\tau)}, FC_1^{(\tau-1)}, C_{D_1}^{(\tau)}, \dots, C_{D_{j-1}}^{(\tau)}) \\
\geq&H(C_{D_j}^{(\tau)}, EK_i, DK_{l_j}, ETI^{(\tau)} \mid F_1^{(\tau-1)}, \tilde{G}_{j,\omega+1}^{(\tau)}, FC_1^{(\tau-1)}, C_{D_1}^{(\tau)}, \dots, C_{D_{j-1}}^{(\tau)}) \\
=&H(M_{D_j}^{(\tau)}, EK_i, DK_{l_j}, ETI^{(\tau)} \mid F_1^{(\tau-1)}, \tilde{G}_{j,\omega+1}^{(\tau)}, FC_1^{(\tau-1)}, C_{D_1}^{(\tau)}, \dots, C_{D_{j-1}}^{(\tau)}) \qquad (34) \\
=&H(M_{D_j}^{(\tau)}) + H(EK_i, DK_{l_j}, ETI^{(\tau)} \mid F_1^{(\tau-1)}, \tilde{G}_{j,\omega+1}^{(\tau)}, FC_1^{(\tau-1)}, C_{D_1}^{(\tau)}, \dots, C_{D_{j-1}}^{(\tau)}), \qquad (35)
\end{aligned}$$

where (34) follows from (33) and (32), and (35) follows from that $M_{D_j}^{(\tau)}$ is independent of $(EK_i, DK_{l_j}, ETI^{(\tau)}, F_1^{(\tau-1)}, \tilde{G}_{j,\omega+1}^{(\tau)}, FC_1^{(\tau-1)}, C_{D_1}^{(\tau)}, \dots, C_{D_{i-1}}^{(\tau)})$.

Hence, we have

$$H(C_{D_j}^{(\tau)} \mid F_1^{(\tau-1)}, \tilde{G}_{j,\omega+1}^{(\tau)}, FC_1^{(\tau-1)}, C_{D_1}^{(\tau)}, \dots, C_{D_{j-1}}^{(\tau)}) \geq H(M_{D_j}^{(\tau)}). \qquad (36)$$

Finally, from (31) and (36), we have $H(C_{D_j}^{(\tau)} \mid F_1^{(\tau-1)}, G_{\omega+1}^{(\tau)}, FC_1^{(\tau-1)}, C_{D_1}^{(\tau)}, \dots, C_{D_{j-1}}^{(\tau)}) \geq H(M_{D_j}^{(\tau)})$ for $1 \leq j \leq \omega + 1$. □

Proof of Lemma 14: Now, the proof of Lemma 14 is completed. □

Lemma 15. *$H(ETI^{(t)} \mid ETI^{(1)}, \dots, ETI^{(t-1)}) \geq (\omega + 1)H(M)$ for any $t \in \mathcal{T}$. In particular, $H(ETI^{(t)}) \geq (\omega + 1)H(M)$ for any $t \in \mathcal{T}$.*

Proof. For arbitrary $i \in \{1, 2, \dots, n\}$, we take a subset $B := \{l_1, l_2, \dots, l_{\omega+1}\} \subset \{1, 2, \dots, n\}$ of indices of users such that $i = l_1$. Let $D_k := (l_k, i)$ with $1 \leq k \leq \omega + 1$. Then, we have

$$H(ETI^{(t)} \mid ETI^{(1)}, \dots, ETI^{(t-1)})$$

$$
\begin{aligned}
&\geq H(ETI^{(t)} \mid C^{(t)}_{D_1}, C^{(t)}_{D_2}, \ldots, C^{(t)}_{D_{\omega+1}}, DK_i, ETI^{(1)}, \ldots, ETI^{(t-1)})\\
&\geq I(M^{(t)}_{D_1}, M^{(t)}_{D_2}, \ldots, M^{(t)}_{D_{\omega+1}}; ETI^{(t)} \mid C^{(t)}_{D_1}, C^{(t)}_{D_2}, \ldots, C^{(t)}_{D_{\omega+1}}, DK_i, ETI^{(1)}, \ldots, ETI^{(t-1)})\\
&= H(M^{(t)}_{D_1}, M^{(t)}_{D_2}, \ldots, M^{(t)}_{D_{\omega+1}} \mid C^{(t)}_{D_1}, C^{(t)}_{D_2}, \ldots, C^{(t)}_{D_{\omega+1}}, DK_i, ETI^{(1)}, \ldots, ETI^{(t-1)})\\
&\qquad -H(M^{(t)}_{D_1}, M^{(t)}_{D_2}, \ldots, M^{(t)}_{D_{\omega+1}} \mid C^{(t)}_{D_1}, C^{(t)}_{D_2}, \ldots, C^{(t)}_{D_{\omega+1}}, DK_i, ETI^{(1)}, \ldots, ETI^{(t)})\\
&= H(M^{(t)}_{D_1}, M^{(t)}_{D_2}, \ldots, M^{(t)}_{D_{\omega+1}} \mid C^{(t)}_{D_1}, C^{(t)}_{D_2}, \ldots, C^{(t)}_{D_{\omega+1}}, DK_i, ETI^{(1)}, \ldots, ETI^{(t-1)})\\
&= \sum_{k=1}^{\omega+1} H(M^{(t)}_{D_k} \mid C^{(t)}_{D_1}, C^{(t)}_{D_2}, \ldots, C^{(t)}_{D_{\omega+1}}, DK_i, ETI^{(1)}, \ldots, ETI^{(t-1)}, M^{(t)}_{D_1}, \ldots, M^{(t)}_{D_{k-1}})\\
&= \sum_{k=1}^{\omega+1} H(M^{(t)}_{D_k}) \qquad (37)\\
&= (\omega+1)H(M),
\end{aligned}
$$

where (37) is shown by following: Let $W_k := \{l_1, l_2, \ldots, l_{k-1}, l_{k+1}, \ldots, l_{\omega+1}\}$ for each k with $1 \leq k \leq \omega+1$. Then, we have

$$
\begin{aligned}
& H(M^{(t)}_{D_k} \mid C^{(t)}_{D_k}, EK_{W_k}, DK_i, ETI^{(1)}, \ldots, ETI^{(t-1)})\\
= \;& H(M^{(t)}_{D_k} \mid C^{(t)}_{D_k}, EK_{W_k}, DK_i, ETI^{(1)}, \ldots, ETI^{(t-1)}, M^{(t)}_{D_1}, \ldots, M^{(t)}_{D_{k-1}}, M^{(t)}_{D_{k+1}}, \ldots, M^{(t)}_{D_{\omega+1}})\\
\leq \;& H(M^{(t)}_{D_k} \mid C^{(t)}_{D_1}, C^{(t)}_{D_2}, \ldots, C^{(t)}_{D_{\omega+1}}, DK_i, ETI^{(1)}, \ldots, ETI^{(t-1)}, M^{(t)}_{D_1}, \ldots, M^{(t)}_{D_{k-1}})\\
\leq \;& H(M^{(t)}_{D_k}).
\end{aligned}
$$

And, we have $H(M^{(t)}_{D_k} \mid C^{(t)}_{D_k}, EK_{W_k}, DK_i, ETI^{(1)}, \ldots, ETI^{(t-1)}) = H(M^{(t)}_{D_k})$ from the condition (3) in Definition 5. Hence, $H(M^{(t)}_{D_k} \mid C^{(t)}_{D_1}, C^{(t)}_{D_2}, \ldots, C^{(t)}_{D_{\omega+1}}, DK_i, ETI^{(1)}, \ldots, ETI^{(t-1)}, M^{(t)}_{D_1}, \ldots, M^{(t)}_{D_{k-1}}) = H(M^{(t)}_{D_k})$. □

Lemma 16. *$H(EMK) \geq \tau(\omega+1)H(M)$.*

Proof. The proof can be shown by the same way as in the proof of Lemma 10. □

Proof of Theorem 3: From Lemmas 13-16, the proof of Theorem 3 is completed. □

D Proof of Theorem 6

The proof of Theorem 6 follows from the lemmas in this appendix. In order to complete the proof of Theorem 6, we show the following lemmas.

Lemma 17. *$|\mathcal{E}^{(R)}_{i_2}| \geq q^{2(\omega+1)}$ for any $i_2 \in \{1, 2, \ldots, n\}$.*

Proof. For arbitrary $i_1, i_2 \in \{1, 2, \ldots, n\}$, let $W_{i_1} := \{U_1, \ldots, U_{i_1-1}, U_{i_1+1}, \ldots, U_{\omega+1}\}$ such that $U_{i_2} \notin W_{i_1}$. Then, for any $t_1, t_2 \in \mathcal{T}$, we have

$$
\begin{aligned}
\left(\frac{1}{q}\right)^{2(\omega+1)} &\geq \prod_{i_1=1}^{\omega+1} P_{I_1}(U_{i_1}, U_{i_2}, W_{i_1}, t_1) P_{S_1}(U_{i_1}, U_{i_2}, W_{i_1}, t_1, t_2)\\
&\geq 2^{-\sum_{i_1=1}^{\omega+1} H(E^{(R)}_{i_1,i_2} | E^{(S)}_{W_{i_1}})} \qquad (38)
\end{aligned}
$$

$$\begin{aligned}
&\geq 2^{-\sum_{i_1=1}^{\omega+1} H(E_{i_1,i_2}^{(R)}|E_1^{(S)},\ldots,E_{i_1-1}^{(S)})} \\
&\geq 2^{-\sum_{i_1=1}^{\omega+1} H(E_{i_1,i_2}^{(R)}|E_{1,i_2}^{(S)},\ldots,E_{i_1-1,i_2}^{(S)})} && (39) \\
&\geq 2^{-\sum_{i_1=1}^{\omega+1} H(E_{i_1,i_2}^{(R)}|E_{1,i_2}^{(R)},\ldots,E_{i_1-1,i_2}^{(R)})} && (40) \\
&= 2^{-H(E_{1,i_2}^{(R)},\ldots,E_{\omega+1,i_2}^{(R)})} \\
&\geq 2^{-H(E_{i_2}^{(R)})} && (41) \\
&\geq 2^{-\log|\mathcal{E}_{i_2}^{(R)}|} = \frac{1}{|\mathcal{E}_{i_2}^{(R)}|},
\end{aligned}$$

where (38) follows from Theorem 5, and (39), (40), and (41) follow from the mappings, λ_{i_1} for $1 \leq i_1 \leq \omega$, ρ_{i_1,i_2} for $1 \leq i_1 \leq \omega$, and π_{i_2}, respectively. Therefore, we have $|\mathcal{E}_{i_2}^{(R)}| \geq q^{2(\omega+1)}$. □

Lemma 18. $|\mathcal{ATI}^{(t)}| \geq q^{\omega+1}$ *for any* $t \in \mathcal{T}$.

Proof. For arbitrary $i_1, i_2 \in \{1, 2, \ldots, n\}$, let $\tilde{W}_{i_1} := \{U_1, \ldots, U_{i_1-1}, U_{i_1+1}, \ldots, U_{\omega+1}\}$ such that $U_{i_2} \in \tilde{W}_{i_1}$. Then, for any $t \in \mathcal{T}$, we have

$$\begin{aligned}
\left(\frac{1}{q}\right)^{\omega+1} &\geq \prod_{i_1=1}^{\omega+1} P_2(U_{i_1}, U_{i_2}, \tilde{W}_{i_1}, t) \\
&\geq 2^{-\sum_{i_1=1}^{\omega+1} H(ATI_{i_1}^{(t)}|E_{\tilde{W}_{i_1}}^{(S)})} && (42) \\
&\geq 2^{-\sum_{i_1=1}^{\omega+1} H(ATI_{i_1}^{(t)}|E_1^{(S)},\ldots,E_{i_1-1}^{(S)})} \\
&\geq 2^{-\sum_{i_1=1}^{\omega+1} H(ATI_{i_1}^{(t)}|AMK_1,\ldots,AMK_{i_1-1})} && (43) \\
&\geq 2^{-\sum_{i_1=1}^{\omega+1} H(ATI_{i_1}^{(t)}|ATI_1^{(t)},\ldots,ATI_{i_1-1}^{(t)})} && (44) \\
&= 2^{-H(ATI_1^{(t)},\ldots,ATI_{\omega+1}^{(t)})} \\
&\geq 2^{-H(ATI^{(t)})} && (45) \\
&\geq 2^{-\log|\mathcal{ATI}^{(t)}|} = \frac{1}{|\mathcal{ATI}^{(t)}|},
\end{aligned}$$

where (42) follows from Theorem 5; (43) follow from the mappings λ_{i_1} and ρ_{i_1,i_2} for $1 \leq i_1 \leq \omega$; (44) and (45) follow from the mappings g_{i_1} for $1 \leq i_1 \leq \omega$, and $f^{(t)}$, respectively. Therefore, we have $|\mathcal{ATI}^{(t)}| \geq q^{\omega+1}$. □

Lemma 19. $|\mathcal{AMK}| \geq q^{\tau(\omega+1)}$.

Proof. For arbitrary $i_1, i_2 \in \{1, 2, \ldots, n\}$, let $\tilde{W}_{i_1} := \{U_1, \ldots, U_{i_1-1}, U_{i_1+1}, \ldots, U_{\omega+1}\}$ such that $U_{i_2} \in \tilde{W}_{i_1}$. Then, for any $t \in \mathcal{T}$, we have

$$\begin{aligned}
\left(\frac{1}{q}\right)^{\tau(\omega+1)} &\geq \prod_{t=1}^{\tau} \prod_{i_1=1}^{\omega+1} P_2(U_{i_1}, U_{i_2}, \tilde{W}_{i_1}, t) \\
&\geq 2^{-\sum_{t=1}^{\tau} \sum_{i_1=1}^{\omega+1} H(ATI_{i_1}^{(t)}|E_{\tilde{W}_{i_1}}^{(S)},ATI^{(1)},\ldots,ATI^{(t-1)})} && (46) \\
&\geq 2^{-\sum_{t=1}^{\tau} \sum_{i_1=1}^{\omega+1} H(ATI_{i_1}^{(t)}|E_1^{(S)},\ldots,E_{i_1-1}^{(S)},ATI^{(1)},\ldots,ATI^{(t-1)})} \\
&\geq 2^{-\sum_{t=1}^{\tau} \sum_{i_1=1}^{\omega+1} H(ATI_{i_1}^{(t)}|AMK_1,\ldots,AMK_{i_1-1},ATI^{(1)},\ldots,ATI^{(t-1)})} && (47)
\end{aligned}$$

$$
\begin{aligned}
&\geq 2^{-\sum_{t=1}^{\tau}\sum_{i_1=1}^{\omega+1} H(ATI_{i_1}^{(t)}|ATI_1^{(t)},\ldots,ATI_{i_1-1}^{(t)},ATI^{(1)},\ldots,ATI^{(t-1)})} && (48)\\
&= 2^{-\sum_{t=1}^{\tau} H(ATI_1^{(t)},\ldots,ATI_{\omega+1}^{(t)}|ATI^{(1)},\ldots,ATI^{(t-1)})}\\
&\geq 2^{-\sum_{t=1}^{\tau} H(ATI^{(t)}|ATI^{(1)},\ldots,ATI^{(t-1)})} && (49)\\
&= 2^{-H(ATI^{(1)},\ldots,ATI^{(\tau)})}\\
&\geq 2^{-H(AMK)} && (50)\\
&\geq 2^{-\log|\mathcal{AMK}|} = \frac{1}{|\mathcal{AMK}|},
\end{aligned}
$$

where (46) follows from Theorem 5; (47) follow from the mappings λ_{i_1} and ρ_{i_1,i_2} for $1 \leq i_1 \leq \omega$; (48) and (49) follow from the mappings g_{i_1} for $1 \leq i_1 \leq \omega$ and $f^{(t)}$, respectively; (50) follows from the deterministic algorithm (i.e., mapping) *AExt*: $\mathcal{AMK} \times \mathcal{T} \to \mathcal{ATI}$. Therefore, we have $|\mathcal{AMK}| \geq q^{\tau(\omega+1)}$. □

Lemma 20. *$|\mathcal{E}_{i_1}^{(S)}| \geq q^{2\omega+\tau+1}$ for any $i_1 \in \{1, 2, \ldots, n\}$.*

Proof. For arbitrary $i_1, i_2 \in \{1, 2, \ldots, n\}$, let $W_{i_2} := \{U_1, \ldots, U_{i_2-1}, U_{i_2+1}, \ldots, U_{\omega+1}\}$ such that $U_{i_1} \notin W_{i_2}$, and $\tilde{W} \in \mathcal{P}(\mathcal{U}, \omega)$ such that $U_{i_1} \notin \tilde{W}$ and $U_{i_2} \in \tilde{W}$. Then, for any $t, t_1, t_2 \in \mathcal{T}$, we have

$$
\begin{aligned}
&\log\left(\frac{1}{q}\right)^{2\omega+\tau+1}\\
\geq\ &\log\left(\prod_{t=2}^{\tau} P_2(U_{i_1}, U_{i_2}, \tilde{W}, t) \prod_{i_2=1}^{\omega+1} P_{I_1}(U_{i_1}, U_{i_2}, W_{i_2}, t_1) P_{S_1}(U_{i_1}, U_{i_2}, W_{i_2}, t_1, t_2)\right)\\
\geq\ &-\sum_{t=2}^{\tau} H(ATI_{i_1}^{(t)} \mid E_{\tilde{W}}^{(S)}, E_{\tilde{W}}^{(R)}, ATI^{(1)}, \ldots, ATI^{(t-1)}, ATI^{(t+1)}, \ldots, ATI^{(\tau)})\\
&\qquad -\sum_{i_2=1}^{\omega+1} H(E_{i_1,i_2}^{(t)} \mid E_{W_{i_2}}^{(S)}, E_{W_{i_2}}^{(R)}, ATI^{(1)}, \ldots, ATI^{(\tau)}) \qquad (51)\\
\geq\ &-\sum_{t=2}^{\tau} H(ATI_{i_1}^{(t)} \mid ATI^{(1)}, ATI^{(2)}, \ldots, ATI^{(t-1)})\\
&\qquad -\sum_{i_2=1}^{\omega+1} H(E_{i_1,i_2}^{(t)} \mid E_{W_{i_2}}^{(R)}, ATI^{(1)}, \ldots, ATI^{(\tau)})\\
\geq\ &-\sum_{t=2}^{\tau} H(ATI_{i_1}^{(t)} \mid ATI^{(2)}, ATI^{(3)}, \ldots, ATI^{(t-1)})\\
&\qquad -\sum_{i_2=1}^{\omega+1} H(E_{i_1,i_2}^{(t)} \mid E_1^{(R)}, \ldots, E_{i_2-1}^{(R)} ATI^{(2)}, \ldots, ATI^{(\tau)})\\
\geq\ &-\sum_{t=2}^{\tau} H(ATI_{i_1}^{(t)} \mid ATI_{i_1}^{(2)}, ATI_{i_1}^{(3)}, \ldots, ATI_{i_1}^{(t-1)})\\
&\qquad -\sum_{i_2=1}^{\omega+1} H(E_{i_1,i_2}^{(t)} \mid E_{i_1,1}^{(R)}, \ldots, E_{i_1,i_2-1}^{(R)}, ATI_{i_1}^{(2)}, \ldots, ATI_{i_1}^{(\tau)}) \qquad (52)\\
=\ &-H(ATI_{i_1}^{(2)}, ATI_{i_1}^{(3)}, \ldots, ATI_{i_1}^{(\tau)}, E_{i_1,1}^{(R)}, \ldots, E_{i_1,\omega+1}^{(R)})\\
\geq\ &-H(AMK_{i_1}, E_{i_1,1}^{(R)}, \ldots, E_{i_1,\omega+1}^{(R)}) \qquad (53)
\end{aligned}
$$

$$
\begin{aligned}
&\geq -H(E_{i_1,1}^{(S)},\ldots,E_{i_1,\omega+1}^{(S)}) && (54)\\
&\geq -H(E_{i_1}^{(S)}) && (55)\\
&\geq -\log|\mathcal{E}_{i_1}^{(S)}|,
\end{aligned}
$$

where (51) follows from Theorem 5; (52) follows from the mappings π_{i_2} for $1 \leq i_2 \leq \omega$ and $f^{(t)}$ for $2 \leq t \leq \tau$; (53), (54), and (55) follow from the mappings, g_{i_1}, ρ_{i_1,i_2} for $1 \leq i_2 \leq \omega+1$, and λ_{i_1}, respectively. Therefore, $|\mathcal{E}_{i_1}^{(S)}| \geq q^{2\omega+\tau+1}$. □

Lemma 21. *$|\mathcal{A}_{i_1,i_2}^{(t)}| \geq q$ for any $i_1, i_2 \in \{1,2,\ldots,n\}$ and $t \in \mathcal{T}$.*

Proof. Let $W = \emptyset$. Then, we have

$$
\begin{aligned}
\frac{1}{q} &\geq P_{I_1}(U_{i_1}, U_{i_2}, W, t)\\
&\geq 2^{-I(MA_{i_1,i_2}^{(t)};E_{i_1,i_2}^{(R)}|ATI^{(1)},\ldots,ATI^{(\tau)})} && (56)\\
&= 2^{-I(M;E_{i_1,i_2}^{(R)}|ATI^{(1)},\ldots,ATI^{(\tau)})-I(A_{i_1,i_2}^{(t)};E_{i_1,i_2}^{(R)}|ATI^{(1)},\ldots,ATI^{(\tau)},M)}\\
&= 2^{-I(A_{i_1,i_2}^{(t)};E_{i_1,i_2}^{(R)}|ATI^{(1)},\ldots,ATI^{(\tau)},M)}\\
&\geq 2^{-H(A_{i_1,i_2}^{(t)})} \geq \frac{1}{|\mathcal{A}_{i_1,i_2}^{(t)}|},
\end{aligned}
$$

where (56) follows from Theorem 5. Therefore, we have $|\mathcal{A}_{i_1,i_2}^{(t)}| \geq q$. □

Proof of Theorem 6: From Lemmas 17-21, the proof of Theorem 6 is completed. □