Journal of Information Processing Vol.24 No.4 680–689 (July 2016)

[DOI: 10.2197/ipsjjip.24.680]

Regular Paper

Information-theoretically Secure Timed-release Secret Sharing Schemes

Yohei Watanabe[1,†1,a)] Junji Shikata[1,2,b)]

Received: July 31, 2015, Accepted: March 4, 2016

Abstract: In modern cryptography, the secret sharing scheme is an important cryptographic primitive, and it is used in various situations. In this paper, timed-release secret sharing (TR-SS) schemes with information-theoretic security is first studied. TR-SS is a secret sharing scheme with the property that more than a threshold number of participants can reconstruct a secret by using their shares only when the time specified by a dealer has come. Specifically, in this paper we first introduce models and formalization of security for two kinds of TR-SS based on the traditional secret sharing scheme and information-theoretic timed-release security. We also derive tight lower bounds on the sizes of shares, time-signals, and entities' secret-keys required for each TR-SS scheme. In addition, we propose direct constructions for the TR-SS schemes. Each direct construction is optimal in the sense that the construction meets equality in each of our bounds, respectively. As a result, it is shown that timed-release security can be realized without any additional redundancy on the share size.

Keywords: information theoretic security, secret sharing schemes, timed-release security, unconditional security

1. Introduction

Secret sharing schemes were proposed independently by Shamir [29] and Blakley [4]. In a (k, n)-threshold secret sharing ((k, n)-SS for short) scheme (e.g., see Ref. [29]), a dealer shares a secret among all participants, and then, k participants can reconstruct the secret while any $k-1$ participants obtain no information on the secret. Since Shamir and Blakley proposed secret sharing schemes, various research on them have been reported.

On the other hand, "time" is intimately related to our lives. We get up, eat something, do a job, and get sleep at a time of our (or someone's) choice. For the above reason, it appears that cryptographic protocols associated with "time" are useful and meaningful. Actually, as those protocols, *timed-release cryptographic protocols* introduced in Ref. [25] are well-known.

From the above discussion, it is worth considering a secret sharing scheme with timed-release security. Therefore, we study such a scheme, which we call a *timed-release secret sharing* (TR-SS) scheme, in this paper.

Timed-Release Security. Informally, the goal of timed-release cryptography is *to securely send certain information into the future*. In timed-release cryptography, the following situation is considered [*1]: A sender can designate the time when receiver's functionality (e.g., decryption) is activated; there exists a time-server whose role is to generate and distribute some information associated with time (called *time-signals* in this paper) periodically; the sender and the time-server (resp., the receiver and the time-server) never communicate with each other. Therefore, the time-server does not need to know when the specified time is. For instance, in timed-release encryption (TRE), a sender transmits a ciphertext so that a receiver can decrypt it when the time specified by the sender has come, and the receiver cannot decrypt it before the time. At the specified time, the receiver can get the plaintext by using the time-signal, which is broadcasted by a time-server, at the specified time.

Timed-release cryptography was first proposed by May [25] in 1993, and after that, Rivest et al. [28] developed it in a systematic and formal way. Since Rivest et al. gave a formal definition of TRE in Ref. [28], various research on timed-release cryptography including timed-release signatures (e.g., Refs. [16], [17]) and timed-release encryption have been done based on computational security. In particular, TRE in the public-key setting has been recently researched on intensively (e.g., Refs. [10], [12], [13]), and Watanabe and Shikata [34] proposed computational secret sharing schemes with timed-release functionality. On the other hand, information-theoretically (or unconditionally) secure timed-release cryptography was proposed by Watanabe et al. [33]. In addition, they investigated not only encryption but also key-agreement and authentication codes with information-theoretic

[1] Graduate School of Environment and Information Sciences, Yokohama National University, Yokohama, Kanagawa 240–8501, Japan
[2] Institute of Advanced Sciences, Yokohama National University, Yokohama, Kanagawa 240–8501, Japan
[†1] Presently with Graduate School of Informatics and Engineering, The University of Electro-Communications
[a)] watanabe-yohei-xs@ynu.jp
[b)] shikata@ynu.ac.jp

This paper was presented in part at the 1st International Conference on Cryptography and Information Security in Balkans (BalkanCryptSec 2014), Turkey, October 2014 [35].

[*1] As another approach to timed-release functionality, time-lock puzzles [2], [22], [25], [28] are known. However, it is impossible to realize them in information-theoretic security settings since they guarantee timed-release functionality by requiring a receiver to run large computation. Note that in this setting, it is assumed that every entity (in particular, an adversary) has infinite computational power.

timed-release security. To the best of our knowledge, however, there is no paper which reports on the study of secret sharing schemes with information-theoretic timed-release security.

Our Contribution. In adding timed-release functionality to secret sharing schemes, we conceive the following two types of schemes.

One is a secret sharing scheme such that a time-signal at the specified time is required whenever a secret is reconstructed, which means a secret sharing scheme with a simple combination of traditional secret sharing functionality and timed-release functionality. For realizing it, we propose (k, n)-TR-SS in this paper. In (k, n)-TR-SS, a dealer can specify positive integers k, n with $k \leq n$, where n is the number of participants and k is a threshold value, and future time $t \in \mathcal{T} := \{1, 2, \ldots, \tau\}$ when a secret can be recovered; and the secret can be reconstructed from at least k shares and a time-signal at the specified time t. On the other hand, participants cannot reconstruct the secret without the time-signal even if they can obtain all shares. Specifically, we define a model and security notions of (k, n)-TR-SS, and we derive lower bounds on the sizes of shares, time-signals, and entities' secret keys required for (k, n)-TR-SS. Moreover, we provide a direct construction of (k, n)-TR-SS, which is constructed by using polynomials over finite fields and provably secure in our security definition. In addition, we show that the direct construction meets the lower bounds on the sizes of shares, time-signals, and entities' secret keys with equalities. Therefore, it turns out that our lower bounds are tight, and that the direct construction is optimal.

Another one is a *hybrid* TR-SS, which means a secret sharing scheme in which traditional secret sharing functionality and timed-release functionality are simultaneously realized. In our hybrid TR-SS, a secret can be reconstructed, if one of the following condition is satisfied: a secret can be reconstructed from k_1 shares and a time-signal at a specified time as in the (k_1, n)-TR-SS; or a secret can be reconstructed from k_2 shares as in the traditional (k_2, n)-SS. Hence, we consider two threshold values k_1, k_2 to define a model of the hybrid TR-SS, and we propose (k_1, k_2, n)-TR-SS as such a model, where $k_1 \leq k_2 \leq n$. Specifically, in (k_1, k_2, n)-TR-SS, a dealer can specify future time, and arbitrarily chooses k_1, k_2 and n. At least k_1 (and less than k_2) participants can reconstruct a secret with a time-signal at the specified time, and at least k_2 participants can reconstruct a secret *without* any time-signal (i.e., they can reconstruct from *only* their shares). Specifically, we define a model and security notions of (k_1, k_2, n)-TR-SS, and we derive *tight* lower bounds on the sizes of shares, time-signals, and entities' secret keys required for (k_1, k_2, n)-TR-SS. Moreover, we provide a direct constructions of (k_1, k_2, n)-TR-SS, which is an *optimal* construction, which meets the above lower bounds with equalities. To achieve its optimality, we use a public parameter, which is needed to reconstruct a secret and to reduce share sizes, in our construction. This technique is reasonable since public parameters are sometimes used in the context of secret sharing schemes such as Ref. [20].

In particular, a theoretically-interesting point in our results includes that the timed-release security can be realized without any additional redundancy on the share size in both schemes.

Related Work. There are many related works, e.g., fully dynamic secret sharing schemes [5], on-line secret sharing schemes [9], and secret sharing schemes with disenrollment capability [3]. In a nutshell, in such schemes, a dealer generates and distributes shares securely, and later on, the dealer can generate and publicly broadcast information for changing the shared secret or qualified sets. Our scheme differs from such schemes in that broadcasted information is generated independently of a shared secret (i.e., the broadcasted information can be generated by a third party).

The other type of related works dealing with the concept of time is a proactive secret sharing scheme [18]. In this scheme, broadcast channels among all participants are assumed. Each participant generates and broadcasts updating information to other participants, and then, they refresh their shares by using the updating information. Hence, shares leaked before that time become irrelevant. Namely, proactive secret sharing schemes realize *share-updating functionality*. In our scheme, such broadcast channels are not assumed and the concept of both schemes is completely different, though both schemes deal with the concept of time.

Further, our scheme is closely related to a compartmented secret sharing scheme [7], [31]. By considering a time-signal at the specified time as one of shares, we can regard a (k, n)-TR-SS scheme as a secret sharing scheme with a specific general access structure, which is any set of $k+1$ shares including a time-signal at the specified time. Therefore, we can transform the (k, n)-TR-SS with $\tau = 1$ to the compartmented $(k+1, k, 1, n)$-threshold scheme, and vice versa. Generally, in the compartmented $(k, k_1, \ldots, k_u, n)$-threshold scheme, there are disjoint user sets $\mathcal{P}_1, \ldots, \mathcal{P}_u$, and the access structure consists of sets of at least k shares which each includes at least k_i shares from participants of $\mathcal{P}_i$. Now, in a (k, n)-TR-SS scheme, we assume two disjoint sets $\mathcal{P}_1$, $\mathcal{P}_2$, where $\mathcal{P}_1$ is a set of all users and $\mathcal{P}_2$ is a time-server, and let $k_1 := k$ and $k_2 := 1$. Then, the scheme can be regarded as an compartmented $(k + 1, k, 1, n)$-threshold scheme. If the (k, n)-TR-SS scheme is optimal (the optimality will be defined in Section 2.2), then the resulting compartmented $(k + 1, k, 1, n)$-threshold scheme is also optimal (or also called *ideal*).

Applications of TR-SS. Our TR-SS is a secret sharing scheme with timed-release property, hence we can add timed-release functionality to applications of secret sharing schemes. Here, we consider information-theoretically secure key escrow with limited time span (see Ref. [8] for computationally secure one) as one of applications of TR-SS. In a key escrow scheme, a user sends shares of his secret key using encryption (or other cryptographic protocols) to trusted escrow agents in advance. Even if the user loses his ablity to access encrypted data (e.g., by accidental loss of the secret key), he can get the secret key reconstructed from agents' shares. However, considering the corruption of agents in practice, it is desirable to restrict the agents' power since they can access all encrypted data corresponding to the secret key. To achieve this, a key escrow scheme with limited time span (a.k.a. a time-controlled key escrow scheme) was proposed [8]. In the time-controlled key escrow scheme, a user and escrow agents can update a secret key and its shares at each time-period without any interaction. Therefore, at each time-period t, agents only have the power to access data encrypted at t (i.e., if some agents are cor-

rupted, they cannot access data encrypted before t). By using TR-SS to generate shares of a secret key, we can realize information-theoretically secure time-controlled key escrow schemes.

Furthermore, TR-SS can also provide other cryptographic protocols with timed-release functionality. For example, we can construct information-theoretically secure TRE in the two-user setting from $(1,1)$-TR-SS and the one-time pad as follows. For a plaintext M and a shared key K, a sender chooses a random number r whose length is equal to the plaintext-length, and computes a ciphertext $C := M \oplus r \oplus K$. Then, the sender specifies future time, and he generates one share from the secret r by $(1,1)$-TR-SS. A receiver can compute $C \oplus K = M \oplus r$ by using the shared key K in advance, however, he cannot obtain M until the specified time comes since he can get r only after the specified time. In a similar way, it is expected that TR-SS is useful for building other timed-release cryptographic protocols such as timed-release authentication code [33] in the two-user setting, and that TR-SS might be able to provide some new timed-release cryptographic protocols, e.g., timed-release threshold encryption.

Organization of This Paper. The rest of this paper is organized as follows. In Sections 2 and 3, we describe (k,n)-TR-SS and (k_1,k_2,n)-TR-SS, respectively, which are based on the ideas according to Refs. [21], [29], [33]. Specifically, in each section, we define a model and security of each scheme, and derive lower bounds on the sizes of shares, time-signals and secret keys required for each scheme, respectively. Furthermore, we propose a direct construction of each scheme, and show it is provably secure and optimal. In Section 4, we discuss some extensions such as TR-SS schemes with general access structures and robust TR-SS schemes. In Section 5, we conclude this paper.

Notation. Throughout this paper, we use the following notation. Generally speaking, X indicates a random variable which takes values in $\mathcal{X}$ (e.g., A, B, and C are random variables which take values in $\mathcal{A}, \mathcal{B}$, and $\mathcal{C}$, respectively). For any finite set $\mathcal{Z}$ and arbitrary non-negative integers z_1, z_2, let $\mathcal{PS}(\mathcal{Z}, z_1, z_2) := \{\mathcal{X} \subset \mathcal{Z} \mid z_1 \le |\mathcal{X}| \le z_2\}$ be the family of all subsets of $\mathcal{Z}$ whose cardinality is at least z_1 but no more than z_2.

2. (k,n)-timed-release Secret Sharing Scheme

In this section, we propose a model and a security definition of (k,n)-TR-SS. In (k,n)-TR-SS, a time-signal at the specified time is always required when a secret is reconstructed. In other words, a secret cannot be reconstructed without a time-signal at the specified time even if there are all shares.

2.1 The Model and Security Definition

First, we introduce the model of (k,n)-TR-SS. Unlike traditional secret sharing schemes [4], [29], we assume that there is a trusted authority (also called a trusted initializer) TA whose role is to generate and to distribute secret keys of entities. We call this model the *trusted initializer model* as in Ref. [27]. In (k,n)-TR-SS, there are $n+3$ entities, a dealer D, n participants $P_1, P_2, \ldots, P_n$, a time-server TS for broadcasting time-signals at most τ times and a trusted initializer TA, where k, n and τ are positive integers. In this paper, we assume that the identity of each user P_i is also denoted by P_i.

Informally, (k,n)-TR-SS is executed as follows. First, TA generates secret keys on behalf of D and TS. After distributing these keys via secure channels, TA deletes them in his memory [*2]. Next, D specifies future time, as D wants, when a secret is reconstructed by participants, and he generates n shares from the secret by using his secret key. And, D sends each share and the specified time to each participant, respectively, via secure channels. The time-server TS periodically broadcasts a time-signal which is generated by using his secret key. Note that there is no interaction between TS and D, hence TS may not know when the specified time is. Hence, D has to tell the specified time t to participants when sending shares, and TS has to broadcast time-signals at every time. When the specified time has come, at least k participants can compute the secret by using their shares and the time-signal of the specified time.

Formally, we give the definition of (k,n)-TR-SS as follows. In this model, let $\mathcal{P} := \{P_1, P_2, \ldots, P_n\}$ be a set of all participants. And also, $\mathcal{S}$ is a set of possible secrets with a probability distribution P_S, and $\mathcal{SK}$ is a set of possible secret keys. $\mathcal{T} := \{1, 2, \ldots, \tau\}$ is a set of time. Let $\mathcal{U}_i^{(t)}$ be the set of possible P_i's shares at the time $t \in \mathcal{T}$. Also, $\mathcal{U}_i := \bigcup_{l=1}^{\tau} \mathcal{U}_i^{(l)}$ is a set of possible P_i's shares for every $i \in \{1, 2, \ldots, n\}$, and let $\mathcal{U} := \bigcup_{l=1}^{n} \mathcal{U}_l$. In addition, $\mathcal{TI}^{(t)}$ is a set of time-signals at time t, and let $\mathcal{TI} := \bigcup_{l=1}^{\tau} \mathcal{TI}^{(l)}$. Furthermore, for any subset of participants $\mathcal{J} = \{P_{i_1}, \ldots, P_{i_j}\} \subset \mathcal{P}$, $\mathcal{U}_{\mathcal{J}}^{(t)} := \mathcal{U}_{i_1}^{(t)} \times \cdots \times \mathcal{U}_{i_j}^{(t)}$ denotes the set of possible shares held by $\mathcal{J}$.

Definition 1 ((k,n)-TR-SS)**.** *A (k,n)-timed-release secret sharing ((k,n)-TR-SS) scheme Π involves $n+3$ entities, TA, D, $P_1, \ldots, P_n$, and TS, and consists of four phases, Initialize, Extract, Share and Reconstruct, and five finite spaces, $\mathcal{S}$, $\mathcal{SK}$, $\mathcal{U}$, $\mathcal{T}$, and $\mathcal{TI}$. Π is executed based on the above phases as follows.*

a) Initialize. TA generates a secret key $sk \in \mathcal{SK}$ for TS and D. This key is distributed to TS and D via secure channels. After distributing the secret key, TA deletes it from his memory. And, D and TS keep their keys secret, respectively [*3].

b) Share. A dealer D randomly selects a secret $s \in \mathcal{S}$ according to P_S, and chooses k and n. If D wants the secret s to be reconstructed by participants at future time $t \in \mathcal{T}$, on input the secret $s \in \mathcal{S}$, specified time $t \in \mathcal{T}$ and a secret key sk, D computes a share $u_i^{(t)} \in \mathcal{U}_i^{(t)}$ for every P_i $(i = 1, 2, \ldots, n)$. And then, D sends a pair of the share and specified time, $(u_i^{(t)}, t)$, to P_i $(i = 1, 2, \ldots, n)$ via a secure channel [*4].

c) Extract. For broadcasting a time-signal at each time t, TS generates a time-signal $ts^{(t)} \in \mathcal{TI}^{(t)}$ by using his secret key sk and time $t \in \mathcal{T}$, where for simplicity we assume that $ts^{(t)}$ is deterministically computed by t and sk.

[*2] Note that we do not consider a situation where TA determines t in distribution phase since the role of TA is only to generate and distribute secret keys and such a scheme cannot be said to have the timed-release property.

[*3] If we consider a situation in which TS is trusted and has functionality of generating keys and distributing them to participants by secure private channels, we can identify TA with TS in the situation. However, there may be a situation in which the roles of TA and TS are quite different (e.g., TA is a provider of secure data storage service and TS is a time-signal broadcasting server). Therefore, we assume two entities TA and TS in our model to capture various situations.

[*4] More precisely, there is no need to keep the specified time confidential (D only has to send shares via secure channels).

d) Reconstruct. At the specified time t, any set of at least k participants $\mathcal{A} = \{P_{i_1}, \ldots, P_{i_j}\} \in \mathcal{PS}(\mathcal{P}, k, n)$ *can reconstruct the secret s by using their shares* $u_{i_1}^{(t)}, \ldots, u_{i_j}^{(t)}$ $(k \leq j \leq n)$ *and a time-signal* $ts^{(t)}$ *at the specified time.*

In the above model, we assume that Π meets the following *correctness* property: If D correctly completes the phase *Share* and TS correctly completes the phase *Extract*, then, for all possible $i \in \{1, 2, \ldots, n\}$, $t \in \mathcal{T}$, $s \in \mathcal{S}$, $u_i^{(t)} \in \mathcal{U}_i$, and $ts^{(t)} \in \mathcal{TI}^{(t)}$, it holds that any $\mathcal{A} \in \mathcal{PS}(\mathcal{P}, k, n)$ will correctly reconstruct the secret s at the end of phase *Reconstruct*, namely, $H(S \mid U_{\mathcal{A}}^{(t)}, TI^{(t)}) = 0$.

Next, we formalize a security definition of (k, n)-TR-SS based on the idea of the information-theoretic timed-release security [33] and secret sharing schemes (e.g., see Ref. [21]). In (k, n)-TR-SS, we consider the following two kinds of security. The first kind of security which we consider is basically the same as that of the traditional (k, n)-SS: less than k participants cannot obtain any information on a secret. In addition to this, as the second kind of security we want to require that even at least k participants cannot obtain any information on a secret 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. Therefore, we formally define secure (k, n)-TR-SS by Shannon entropy as follows (if readers are not familiar to Shannon entropy, see Ref. [14] for the excellent instruction).

Definition 2 (Security of (k, n)-TR-SS)**.** *Let* Π *be a* (k, n)*-TR-SS scheme.* Π *is said to be secure if the following conditions are satisfied:*

(i) For any $\mathcal{F} \in \mathcal{PS}(\mathcal{P}, 1, k-1)$ *and any* $t \in \mathcal{T}$*, it holds that* $H(S \mid U_{\mathcal{F}}^{(t)}, TI^{(1)}, \ldots, TI^{(\tau)}) = H(S)$.

(ii) For any $\mathcal{A} \in \mathcal{PS}(\mathcal{P}, k, n)$ *and any* $t \in \mathcal{T}$*, it holds that* $H(S \mid U_{\mathcal{A}}^{(t)}, TI^{(1)}, \ldots, TI^{(t-1)}, TI^{(t+1)}, \ldots, TI^{(\tau)}) = H(S)$.

Intuitively, the meaning of two conditions (i) and (ii) in Definition 2 is explained as follows. (i) No information on a secret is obtained by any set of less than k participants, even if they obtain time-signals at all the time; (ii) No information on a secret is obtained by any set of more than $k-1$ participants, even if they obtain time-signals at all the time except the specified time [*5].

Remark 1. *We can also consider the following security definition (the condition (iii)) instead of (i): No information on a secret is obtained by collusion of* TS *and any set of less than k participants, namely, this is defined as follows.*

(iii) For any $\mathcal{F} \in \mathcal{PS}(\mathcal{P}, 1, k-1)$ *and for any* $t \in \mathcal{T}$*, it holds that* $H(S \mid U_{\mathcal{F}}^{(t)}, SK) = H(S)$.

Note that the condition (iii) is stronger than (i). The reason for this is as follows. All time-signals $ts^{(1)}, \ldots, ts^{(\tau)}$ *can be deterministically generated from sk. Namely, it holds* $H(SK) \geq H(TI^{(1)}, \ldots, TI^{(\tau)})$*, and hence* $H(S \mid U_{\mathcal{F}}^{(t)}, SK) \leq H(S \mid U_{\mathcal{F}}^{(t)}, TI^{(1)}, \ldots, TI^{(\tau)}) \leq H(S)$*. Therefore, (iii) implies (i), and in this sense, we said that (iii) is stronger than (i). However, we do not consider (iii) in this paper because of the following two reasons: first, the condition (i) is more natural than (iii), since it does not seem natural to consider the situation that any set of less than k participants colludes with* TS *in the real world; and secondly, our lower bounds in Theorem 1 are still valid even under the conditions (ii) and (iii), in other words, even if we consider the conditions (ii) and (iii), we can derive the same lower bounds in Theorem 1 since Definition 2 is weaker. Interestingly, our direct construction in Section 2.3 also satisfies (iii), and tightness of our lower bounds and optimality of our direct construction will be valid not depending on the choice of the condition (i) or (iii). Furthermore, we do not have to consider an attack by dishonest* TS *only, since* TS*'s master-key is generated independently of a secret.*

[*5] In this sense, we have formalized the security notion stronger than the security that any set of more than $k-1$ participants cannot obtain any information on a secret *before* the specified time, as is the same approach considered in Ref. [33]. Actually, if we remove $TI^{(t+1)}, \ldots, TI^{(\tau)}$ from (ii) in Definition 2, we obtain the same lower bounds on sizes of shares, time-signals and secret keys as those in Theorem 1.

2.2 Lower Bounds

In this section, we show lower bounds on sizes of shares, time-signals, and secret keys required for secure (k, n)-TR-SS as follows.

Theorem 1. *Let* Π *be any secure* (k, n)*-TR-SS. Then, for any* $i \in \{1, 2, \ldots, n\}$ *and for any* $t \in \mathcal{T}$*, we have*

$$(I)\ H(U_i^{(t)}) \geq H(S), \qquad (II)\ H(TI^{(t)}) \geq H(S),$$
$$(III)\ H(SK) \geq \tau H(S).$$

Proof. The proof of Theorem 1 follows from the following lemmas.

Lemma 1. $H(U_i^{(t)}) \geq H(S)$ *for any* $i \in \{1, 2, \ldots, n\}$ *and any* $t \in \mathcal{T}$.

Proof. The proof can be proved in a way similar to the proof in Ref. [21], Theorem 1. For arbitrary $i \in \{1, 2, \ldots, n\}$, we take a subset $\mathcal{B}_i \in \mathcal{PS}(\mathcal{P} \setminus \{P_i\}, k-1, k-1)$ of participants. Then, for any $t \in \mathcal{T}$, we have

$$\begin{aligned} H(U_i^{(t)}) &\geq H(U_i^{(t)} \mid U_{\mathcal{B}_i}^{(t)}, TI^{(t)}) \geq I(S; U_i^{(t)} \mid U_{\mathcal{B}_i}^{(t)}, TI^{(t)}) \\ &= H(S \mid U_{\mathcal{B}_i}^{(t)}, TI^{(t)}) \quad (1) \\ &= H(S), \quad (2) \end{aligned}$$

where Eq. (1) follows from the correctness of (k, n)-TR-SS and Eq. (2) follows from the condition (i) in Definition 2. □

Lemma 2. $H(TI^{(t)} \mid TI^{(1)}, \ldots, TI^{(t-1)}) \geq H(S)$ *for any* $t \in \mathcal{T}$*. In particular,* $H(TI^{(t)}) \geq H(S)$ *for any* $t \in \mathcal{T}$.

Proof. For any $\mathcal{A} \in \mathcal{PS}(\mathcal{P}, k, n)$ and any $t \in \mathcal{T}$, we have

$$\begin{aligned} H(TI^{(t)}) &\geq H(TI^{(t)} \mid TI^{(1)}, \ldots, TI^{(t-1)}) \\ &\geq H(TI^{(t)} \mid U_{\mathcal{A}}^{(t)}, TI^{(1)}, \ldots, TI^{(t-1)}) \\ &\geq I(S; TI^{(t)} \mid U_{\mathcal{A}}^{(t)}, TI^{(1)}, \ldots, TI^{(t-1)}) \\ &= H(S \mid U_{\mathcal{A}}^{(t)}, TI^{(1)}, \ldots, TI^{(t-1)}) \quad (3) \\ &= H(S), \quad (4) \end{aligned}$$

where Eq. (3) follows from the correctness of (k, n)-TR-SS and Eq. (4) follows from the condition (ii) in Definition 2. □

Lemma 3. $H(SK) \geq \tau H(S)$.

Proof. We have

$$\begin{aligned} H(SK) &\geq I(TI^{(1)}, \ldots, TI^{(\tau)}; SK) \\ &= H(TI^{(1)}, \ldots, TI^{(\tau)}) - H(TI^{(1)}, \ldots, TI^{(\tau)} \mid SK) \\ &= H(TI^{(1)}, \ldots, TI^{(\tau)}) \end{aligned}$$

$$= \sum_{t=1}^{\tau} H(TI^{(t)} \mid TI^{(1)}, \ldots, TI^{(t-1)}) \geq \tau H(S),$$

where the last inequality follows from Lemma 2. □

Proof of Theorem 1: From Lemmas 1–3, the proof of Theorem 1 is completed. □

As we will see in Section 2.3, the above lower bounds are tight since our construction will meet all the above lower bounds with equalities.

We then define optimality of constructions of (k, n)-TR-SS as follows.

Definition 3. *A construction of secure (k, n)-TR-SS is said to be optimal if it meets equality in every bound of (i)–(iii) in Theorem 1.*

Remark 2. *The secret sharing scheme such that the size of each participant's share is equal to that of the secret is often called an ideal secret sharing scheme. The construction of (k, n)-TR-SS in Section 2.3 is optimal, hence, in this sense we achieve ideal (k, n)-TR-SS. In terms of the share size, an interesting point is that the timed-release property can be realized without any additional redundancy on the share size. Therefore in the sense of the bound on the share size, our results are also regarded as the extension of traditional secret sharing schemes.*

2.3 Direct Construction

We propose a direct construction of (k, n)-TR-SS. In addition, it is shown that our construction is optimal. The detail of our construction of (k, n)-TR-SS Π is given as follows.

a) *Initialize.* Let q be a prime power, where $q > \max\{n, \tau\}$, and let $\mathbb{F}_q$ be the finite field with q elements. We assume that the identity of each participant P_i is encoded as $P_i \in \mathbb{F}_q \backslash \{0\}$. Also, we assume $\mathcal{T} = \{1, 2, \ldots, \tau\} \subset \mathbb{F}_q \backslash \{0\}$ by using appropriate encoding [*6]. First, TA chooses uniformly at random τ numbers $r^{(j)} (j = 1, \ldots, \tau)$ from $\mathbb{F}_q$. TA sends a secret key $sk := (r^{(1)}, \ldots, r^{(\tau)})$ to TS and D via secure channels, respectively.

b) *Share.* First, D randomly chooses a secret $s \in \mathbb{F}_q$ according to a distribution P_S over $\mathbb{F}_q$. Also, D specifies the time t at which participants can reconstruct the secret. Next, D randomly chooses a polynomial $f(x) := c^{(t)} + \sum_{i=1}^{k-1} a_i x^i$ over $\mathbb{F}_q$, where $c^{(t)}$ is computed by $c^{(t)} := s + r^{(t)}$ and each coefficient a_i is randomly and uniformly chosen from $\mathbb{F}_q$. Finally, D computes $u_i^{(t)} := f(P_i)$ $(i = 1, 2, \ldots, n)$ and sends $(u_i^{(t)}, t)$ to P_i $(i = 1, 2, \ldots, n)$ via a secure channel.

c) *Extract.* For sk and time $t \in \mathcal{T}$, TS broadcasts t-th key $r^{(t)}$ as a time-signal at time t to all participants via a (authenticated) broadcast channel.

d) *Reconstruct.* First, a set of at least k participants $\mathcal{A} = \{P_{i_1}, P_{i_2}, \ldots, P_{i_k}\} \in \mathcal{PS}(\mathcal{P}, k, k)$ computes $c^{(t)}$ by Lagrange interpolation from their k shares: $c^{(t)} = \sum_{j=1}^{k} (\prod_{l \neq j} \frac{P_{i_j}}{P_{i_j} - P_{i_l}}) f(P_{i_j})$. After receiving $ts^{(t)} = r^{(t)}$, they can compute and get $s = c^{(t)} - r^{(t)}$.

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

[*6] It is enough to just consider an injective mapping $\mathcal{P} \to \mathbb{F}_q \setminus \{0\}$ as such a coding.

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

Proof. First, we show the proof of (i) in Definition 2. Assume that any $k-1$ participants $\mathcal{F} = \{P_{i_1}, \ldots, P_{i_{k-1}}\} \in \mathcal{PS}(\mathcal{P}, k-1, k-1)$ try to guess $c^{(t)}$ by using their shares. Note that they know $r^{(t)} = c^{(t)} - s$ and

$$f(P_{i_j}) = (1, P_{i_j}, \ldots, P_{i_j}^{k-1}) \begin{pmatrix} c^{(t)} \\ a_1 \\ \vdots \\ a_{k-1} \end{pmatrix},$$

for $j = 1, \ldots, k-1$. Thus, they can know the following:

$$\begin{pmatrix} 1 & P_{i_1} & \cdots & P_{i_1}^{k-1} \\ 1 & P_{i_2} & \cdots & P_{i_2}^{k-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & P_{i_{k-1}} & \cdots & P_{i_{k-1}}^{k-1} \end{pmatrix} \begin{pmatrix} c^{(t)} \\ a_1 \\ \vdots \\ a_{k-1} \end{pmatrix}. \tag{5}$$

However, from Eq. (5), they cannot guess at least one element of $(c^{(t)}, a_1, \ldots, a_{k-1})$ with probability larger than $1/q$ as in Shamir's secret sharing scheme [29]. Therefore, $H(S \mid U_{\mathcal{F}}^{(t)}, TI^{(1)}, \ldots, TI^{(\tau)}) = H(S)$ for any $\mathcal{F} \in \mathcal{PS}(\mathcal{P}, 1, k-1)$ and any $t \in \mathcal{T}$.

Next, we show the proof of (ii) in Definition 2. Suppose that all participants try to guess $r^{(t)}$ by using $c^{(t)}$ and time-signals at all the time except the time t, since they obtain $c^{(t)} = s + r^{(t)}$ from their shares. They get $\tau - 1$ time-signals $r^{(1)}, \ldots, r^{(t-1)}, r^{(t+1)}, \ldots, r^{(\tau)}$. However, since each time-signal is chosen uniformly at random from $\mathbb{F}_q$, they can guess $r^{(t)}$ only with probability $1/q$. By the security of one-time pad, for any $\mathcal{A} \in \mathcal{PS}(\mathcal{P}, k, n)$ and for any $t \in \mathcal{T}$, we have $H(S \mid U_{\mathcal{A}}^{(t)}, TI^{(1)}, \ldots, TI^{(t-1)}, TI^{(t+1)}, \ldots, TI^{(\tau)}) = H(S)$.

Finally, it is straightforward to see that the construction satisfies all the equalities of lower bounds in Theorem 1. Therefore, the above construction is optimal. □

3. (k_1, k_2, n)-timed-release Secret Sharing Scheme

In this section, we consider the following problem, "Can we realize traditional secret sharing functionality and timed-release secret sharing functionality simultaneously?". Therefore, we propose (k_1, k_2, n)-TR-SS, where k_1 and k_2 are threshold values with $1 \leq k_1 \leq k_2 \leq n$. (k_1, k_2, n)-TR-SS can realize timed-release functionality —a secret can be reconstructed from at least k_1 shares and a time-signal at the specified time— and traditional secret sharing functionality —a secret can be also reconstructed from only at least k_2 shares— simultaneously. In the case that $k = k_1 = k_2$, (k, k, n)-TR-SS can be considered as the traditional (k, n)-SS (for details, see Remark 3).

3.1 Model and Security Definition

In this section, we propose a model and a security definition of (k_1, k_2, n)-TR-SS. First, we introduce a model of (k_1, k_2, n)-TR-SS. In (k_1, k_2, n)-TR-SS, there are the same entities and sets as those of (k, n)-TR-SS. The main difference from (k, n)-TR-SS is that a dealer D can specify two kinds of threshold values, k_1 and k_2 with $k_1 \leq k_2 \leq n$: k_1 indicates the number of participants who

can reconstruct a secret s with the time-signal at the time specified by the dealer; and k_2 indicates the number of participants who can reconstruct s without any time-signals. We give the definition of (k_1, k_2, n)-TR-SS as follows.

Definition 4 ((k_1, k_2, n)-TR-SS)**.** *A (k_1, k_2, n)-timed-release secret sharing ((k_1, k_2, n)-TR-SS) scheme Θ involves $n + 3$ entities, TA, D, $P_1, \ldots, P_n$, and TS, and consists of five phases, Initialize, Extract, Share, Reconstruct with time-signals and Reconstruct without time-signals, and five finite spaces, $\mathcal{S}$, $\mathcal{SK}$, $\mathcal{U}$, $\mathcal{T}$, and $\mathcal{TI}$. Θ is executed based on the following phases as follows.*

a) Initialize. This phase follows the same procedure as that of (k, n)-TR-SS (see Definition 1).

b) Share. A dealer D randomly selects a secret $s \in \mathcal{S}$ according to P_S. Then, D chooses k_1, k_2 and n, and specifies future time $t \in \mathcal{T}$ when at least k_1 participants can reconstruct s. Then, on input the secret s, the specified time t and a secret key $sk \in \mathcal{SK}$, D computes a share $u_i^{(t)} \in \mathcal{U}_i^{(t)}$ for every P_i $(i = 1, 2, \ldots, n)$ and a public parameter $pp \in \mathcal{PP}$[*7*]*. And then, D discloses pp and sends a pair of the share and specified time, $(u_i^{(t)}, t)$, to P_i $(i = 1, 2, \ldots, n)$ via a secure channel, respectively.*

c) Extract. This phase follows the same procedure as that of (k, n)-TR-SS (see Definition 1).

d) Reconstruct with time-signals. At the specified time t, any set of participants $\mathcal{A} = \{P_{i_1}, \ldots, P_{i_j}\} \in \mathcal{PS}(\mathcal{P}, k_1, k_2 - 1)$ can reconstruct the secret s by using their shares $(u_{i_1}^{(t)}, \ldots, u_{i_j}^{(t)})$ $(k_1 \le j < k_2)$ and a time-signal of the specified time $ts^{(t)}$.

e) Reconstruct without time-signals. At any time (even before the specified time), any set of participants $\hat{\mathcal{A}} = \{P_{i_1}, \ldots, P_{i_j}\} \in \mathcal{PS}(\mathcal{P}, k_2, n)$ can reconstruct the secret s by using only their shares $(u_{i_1}^{(t)}, \ldots, u_{i_j}^{(t)})$ $(k_2 \le j \le n)$.

In the above model, we assume that Θ meets the following *correctness* properties:

(1) If D correctly completes the phase *Share* and TS correctly completes the phase *Extract*, then, for all possible $i \in \{1, 2, \ldots, n\}$, $t \in \mathcal{T}$, $s \in \mathcal{S}$, $u_i^{(t)} \in \mathcal{U}_i^{(t)}$, and $ts^{(t)} \in \mathcal{TI}^{(t)}$, it holds that any $\mathcal{A} \in \mathcal{PS}(\mathcal{P}, k_1, k_2 - 1)$ will correctly reconstruct the secret s at the end of phase *Reconstruct with time-signals*, namely, $H(S \mid U_{\mathcal{A}}^{(t)}, TI^{(t)}) = 0$.

(2) If D correctly completes the phase *Share*, then, for all possible $i \in \{1, 2, \ldots, n\}$, $t \in \mathcal{T}$, $s \in \mathcal{S}$, and $u_i^{(t)} \in \mathcal{U}_i^{(t)}$, it holds that any $\hat{\mathcal{A}} \in \mathcal{PS}(\mathcal{P}, k_2, n)$ will correctly reconstruct the secret s at the end of phase *Reconstruct without time-signals*, namely, $H(S \mid U_{\hat{\mathcal{A}}}^{(t)}) = 0$.

Next, we formalize a security definition of (k_1, k_2, n)-TR-SS in a similar way to that of (k, n)-TR-SS as follows. Note that the description of (the random variable of) the public parameters is omitted below since existing works using public parameters such as Ref. [20] do not explicitly describe the public parameter in the security definition.

Definition 5 (Security of (k_1, k_2, n)-TR-SS)**.** *Let Θ be a (k_1, k_2, n)-TR-SS scheme. Θ is said to be secure if the following conditions are satisfied:*

(i) For any $\mathcal{F} \in \mathcal{PS}(\mathcal{P}, 1, k_1 - 1)$ and any $t \in \mathcal{T}$, it holds that $H(S \mid U_{\mathcal{F}}^{(t)}, TI^{(1)}, \ldots, TI^{(\tau)}) = H(S)$.

(ii) For any $\hat{\mathcal{F}} \in \mathcal{PS}(\mathcal{P}, k_1, k_2 - 1)$ and any $t \in \mathcal{T}$, it holds that $H(S \mid U_{\hat{\mathcal{F}}}^{(t)}, TI^{(1)}, \ldots, TI^{(t-1)}, TI^{(t+1)}, \ldots, TI^{(\tau)}) = H(S)$.

In Definition 5, intuitively, the meaning of (i) is the same as that of (k, n)-TR-SS (Definition 2), and the meaning of the condition (ii) implies that no information on a secret is obtained by any set of at least k_1 but *no more than* k_2 participants, even if they obtain time-signals at all the time except the specified time. We can also consider a more strong security notion as discussed in (k, n)-TR-SS, however, we do not consider such a strong notion by the same reason as in the case of (k, n)-TR-SS.

Remark 3. *In the case of $k = k_1 = k_2$, the model and security definition of secure (k, k, n)-TR-SS (Definitions 1 and 2) are the same as those of traditional (k, n)-SS. Therefore, the model and security definition of (k_1, k_2, n)-TR-SS can be regarded as the natural extension of those of traditional secret sharing schemes.*

3.2 Lower Bounds

In this section, we show lower bounds on sizes of shares, time-signals, and secret keys required for secure (k_1, k_2, n)-TR-SS as follows. Note that in the proof, there are several technical points which are more complicated than that of Theorem 1.

Theorem 3. *Let Θ be any secure (k_1, k_2, n)-TR-SS. Then, for any $i \in \{1, 2, \ldots, n\}$ and for any $t \in \mathcal{T}$, we have*

$$(I)\ H(U_i^{(t)}) \ge H(S).$$

Moreover, if the above lower bound holds with equality (i.e., $H(U_i^{(t)}) = H(S)$ for any i and t), we have

$$(II)\ H(TI^{(t)}) \ge (k_2 - k_1)H(S), \quad (III)\ H(SK) \ge \tau(k_2 - k_1)H(S).$$

Proof. The proof of Theorem 3 follows from the following lemmas.

Lemma 4. *$H(U_i^{(t)}) \ge H(S)$ for any $i \in \{1, 2, \ldots, n\}$ and any $t \in \mathcal{T}$.*

Proof. The proof of this lemma can be proved in a way similar to the proof of Lemma 1. For arbitrary $i \in \{1, 2, \ldots, n\}$, we take a subset $\mathcal{B}_i \in \mathcal{PS}(\mathcal{P} \setminus \{P_i\}, k_2 - 1, k_2 - 1)$ of participants. Then, for any $t \in \mathcal{T}$, we have

$$\begin{aligned} H(U_i^{(t)}) &\ge H(U_i^{(t)} \mid U_{\mathcal{B}_i}^{(t)}, TI^{(1)}, \ldots, TI^{(t-1)}) && (6)\\ &\ge I(S; U_i^{(t)} \mid U_{\mathcal{B}_i}^{(t)}, TI^{(1)}, \ldots, TI^{(t-1)}) \\ &= H(S \mid U_{\mathcal{B}_i}^{(t)}, TI^{(1)}, \ldots, TI^{(t-1)}) && (7)\\ &= H(S), && (8) \end{aligned}$$

where Eq. (7) follows from the correctness of (k_1, k_2, n)-TR-SS and Eq. (8) follows from the condition (ii) in Definition 5. □

Lemma 5. *If $H(U_i^{(t)}) = H(S)$ for any $i \in \{1, 2, \ldots, n\}$ and $t \in \mathcal{T}$, $H(TI^{(t)}) \ge H(TI^{(t)} \mid TI^{(1)}, \ldots, TI^{(t-1)}) \ge (k_2 - k_1)H(S)$ for any $t \in \mathcal{T}$.*

Proof. The statement is true in the case that $k_1 = k_2$, since Shannon entropy is non-negative. Therefore, in the following, we assume $k_1 < k_2$. For arbitrary $i \in \{1, 2, \ldots, n\}$, we take a subset $\mathcal{B}_i \in \mathcal{PS}(\mathcal{P} \setminus \{P_i\}, k_2 - 1, k_2 - 1)$ of participants. For any $t \in \mathcal{T}$, we have

7 Although not used in the previous scheme, we here introduce a public parameter pp since we will need it in our construction in Section 3.3.

$$
\begin{aligned}
&H(TI^{(t)}) \qquad (9)\\
&\geq H(TI^{(t)} \mid TI^{(1)},\ldots,TI^{(t-1)})\\
&\geq I(TI^{(t)};U_1^{(t)},U_2^{(t)},\ldots,U_n^{(t)} \mid TI^{(1)},\ldots,TI^{(t-1)})\\
&= H(U_1^{(t)},U_2^{(t)},\ldots,U_n^{(t)} \mid TI^{(1)},\ldots,TI^{(t-1)})\\
&\quad - H(U_1^{(t)},U_2^{(t)},\ldots,U_n^{(t)} \mid TI^{(1)},\ldots,TI^{(t)})\\
&= H(U_1^{(t)},\ldots,U_{k_1}^{(t)} \mid TI^{(1)},\ldots,TI^{(t-1)})\\
&\quad + H(U_{k_1+1}^{(t)},\ldots,U_{k_2}^{(t)} \mid TI^{(1)},\ldots,TI^{(t-1)},U_1^{(t)},\ldots,U_{k_1}^{(t)})\\
&\quad\quad + H(U_{k_2+1}^{(t)},\ldots,U_n^{(t)} \mid TI^{(1)},\ldots,TI^{(t-1)},U_1^{(t)},\ldots,U_{k_2}^{(t)})\\
&\quad - H(U_1^{(t)},\ldots,U_{k_1}^{(t)} \mid TI^{(1)},\ldots,TI^{(t)})\\
&\quad\quad - H(U_{k_1+1}^{(t)},\ldots,U_{k_2}^{(t)} \mid TI^{(1)},\ldots,TI^{(t)},U_1^{(t)},\ldots,U_{k_1}^{(t)})\\
&\quad\quad\quad - H(U_{k_2+1}^{(t)},\ldots,U_n^{(t)} \mid TI^{(1)},\ldots,TI^{(t)},U_1^{(t)},\ldots,U_{k_2}^{(t)})\\
&\geq H(U_1^{(t)},\ldots,U_{k_1}^{(t)} \mid TI^{(1)},\ldots,TI^{(t)})\\
&\quad + H(U_{k_1+1}^{(t)},\ldots,U_{k_2}^{(t)} \mid TI^{(1)},\ldots,TI^{(t-1)},U_1^{(t)},\ldots,U_{k_1}^{(t)})\\
&\quad\quad + H(U_{k_2+1}^{(t)},\ldots,U_n^{(t)} \mid TI^{(1)},\ldots,TI^{(t)},U_1^{(t)},\ldots,U_{k_2}^{(t)})\\
&\quad - H(U_1^{(t)},\ldots,U_{k_1}^{(t)} \mid TI^{(1)},\ldots,TI^{(t)})\\
&\quad\quad - H(U_{k_1+1}^{(t)},\ldots,U_{k_2}^{(t)} \mid TI^{(1)},\ldots,TI^{(t)},U_1^{(t)},\ldots,U_{k_1}^{(t)})\\
&\quad\quad\quad - H(U_{k_2+1}^{(t)},\ldots,U_n^{(t)} \mid TI^{(1)},\ldots,TI^{(t)},U_1^{(t)},\ldots,U_{k_2}^{(t)})\\
&= H(U_{k_1+1}^{(t)},\ldots,U_{k_2}^{(t)} \mid TI^{(1)},\ldots,TI^{(t-1)},U_1^{(t)},\ldots,U_{k_1}^{(t)})\\
&\quad - H(U_{k_1+1}^{(t)},\ldots,U_{k_2}^{(t)} \mid TI^{(1)},\ldots,TI^{(t)},U_1^{(t)},\ldots,U_{k_1}^{(t)})\\
&\geq \sum_{i=k_1+1}^{k_2} H(U_i^{(t)} \mid TI^{(1)},\ldots,TI^{(t-1)},U_{\mathcal{B}_i}^{(t)})\\
&\quad - \sum_{i=k_1+1}^{k_2} H(U_i^{(t)} \mid TI^{(1)},\ldots,TI^{(t)},U_1^{(t)},\ldots,U_{i-1}^{(t)})\\
&= (k_2-k_1)H(S), \qquad (10)
\end{aligned}
$$

where Eq. (10) follows from Eq. (6) in the proof of Lemma 4, the assumption of $H(U_i^{(t)}) = H(S)$, and the following claim. □

Claim 1. *If $k_1 < k_2$ and $H(U_i^{(t)}) = H(S)$ for any $i \in \{1,2,\ldots,n\}$ and $t \in \mathcal{T}$, $H(U_i^{(t)} \mid U_{\mathcal{A}_i}, TI^{(t)}) = 0$ for any $i \in \{1,2,\ldots,n\}$, any $\mathcal{A}_i \in \mathcal{PS}(\mathcal{P}\setminus\{P_i\}, k_1, k_2-1)$, and any $t \in \mathcal{T}$.*

Proof. First, for arbitrary $i \in \{1,2,\ldots,n\}$, we take subsets $\mathcal{B}_i := \mathcal{PS}(\mathcal{P}\setminus\{P_i\}, k_1-1, k_1-1)$ and $\mathcal{A}_i := \mathcal{PS}(\mathcal{P}\setminus\{P_i\}, k_1, k_2-1)$ of participants such that $\mathcal{B}_i \subset \mathcal{A}_i$. Then, for any $t \in \mathcal{T}$, we have

$$
\begin{aligned}
H(U_i^{(t)}) &\geq H(U_i^{(t)} \mid U_{\mathcal{B}_i}^{(t)}, TI^{(t)}) \qquad (11)\\
&\geq H(U_i^{(t)} \mid U_{\mathcal{B}_i}^{(t)}, TI^{(t)}) - H(U_i^{(t)} \mid U_{\mathcal{B}_i}^{(t)}, TI^{(t)}, S) \qquad (12)\\
&= I(U_i^{(t)}; S \mid U_{\mathcal{B}_i}^{(t)}, TI^{(t)})\\
&= H(S \mid U_{\mathcal{B}_i}^{(t)}, TI^{(t)}) - H(S \mid U_{\mathcal{B}_i}^{(t)}, U_i^{(t)}, TI^{(t)})\\
&= H(S \mid U_{\mathcal{B}_i}^{(t)}, TI^{(t)}) \qquad (13)\\
&= H(S), \qquad (14)
\end{aligned}
$$

where Eq. (13) follows form the correctness of (k_1,k_2,n)-TR-SS and Eq. (14) follows from the condition (i) in Definition 5.

From the above inequalities and the assumption $H(U_i^{(t)}) = H(S)$, it follows that all quantities between $H(U_i^{(t)})$ and $H(S)$ are equal. Therefore, from Eq. (11) and Eq. (12), we have

$$H(U_i^{(t)} \mid U_{\mathcal{B}_i}^{(t)}, TI^{(t)}, S) = 0.$$

Hence, we have

$$
\begin{aligned}
H(U_i^{(t)} \mid U_{\mathcal{A}_i}^{(t)}, TI^{(t)}) &= H(U_i^{(t)} \mid U_{\mathcal{A}_i}^{(t)}, TI^{(t)}, S)\\
&\leq H(U_i^{(t)} \mid U_{\mathcal{B}_i}^{(t)}, TI^{(t)}, S) = 0.
\end{aligned}
$$

Since $H(U_i^{(t)} \mid U_{\mathcal{A}_i}^{(t)}, TI^{(t)}) \geq 0$, we have $H(U_i^{(t)} \mid U_{\mathcal{A}_i}^{(t)}, TI^{(t)}) = 0$. □

Lemma 6. *If $H(U_i^{(t)}) = H(S)$ for any $i \in \{1,2,\ldots,n\}$ and $t \in \mathcal{T}$, $H(SK) \geq \tau(k_2-k_1)H(S)$.*

Proof. We have

$$
\begin{aligned}
H(SK) &\geq I(TI^{(1)},\ldots,TI^{(\tau)}; SK)\\
&= H(TI^{(1)},\ldots,TI^{(\tau)}) - H(TI^{(1)},\ldots,TI^{(\tau)} \mid SK)\\
&= H(TI^{(1)},\ldots,TI^{(\tau)})\\
&= \sum_{t=1}^{\tau} H(TI^{(t)} \mid TI^{(1)},\ldots,TI^{(t-1)})\\
&\geq \tau(k_2-k_1)H(S),
\end{aligned}
$$

where the last inequality follows from Lemma 5. □

Proof of Theorem 3: From Lemmas 4–6, the proof of Theorem 3 is completed. □

As we will see in Section 3.3, the lower bounds in Theorem 3 are tight since our construction will meet all the above lower bounds with equalities.

We then define optimality of constructions of (k_1,k_2,n)-TR-SS as follows.

Definition 6. *A construction of secure (k_1,k_2,n)-TR-SS is said to be optimal if it meets equality in every bound of (i)–(iii) in Theorem 3.*

3.3 Optimal (but Restricted [*8]) Construction

We can consider a naive construction based on (k_1,n)-TR-SS and (k_2,n)-SS, however, this naive construction is not optimal since the share size is twice as large as the underlying secret size (see Appendix A.1 for details). To achieve an optimal construction, we use the technique in Ref. [20]: In the phase *Share*, the dealer computes public parameters, and the public parameters are broadcasted to participants or else stored on a publicly accessible authenticated bulletin board. Although we have to disclose k_2-k_1 elements in a finite field as a public parameter, each share can consist of only one element. In Ref. [20], Jhanwar and Safavi-Naini used this technique for reducing share sizes, and consequently they succeeded in constructing optimal share sizes. We note that although similar techniques that the dealer broadcasts several coefficients of the polynomial such as Refs. [5], [6], [23], [24] are known, the aim of their techniques differs from our aim. Specifically, it is to realize the functionality, whereas our aim is to reduce the share sizes, and consequently, to achieve an optimal construction. The detail of our construction is given as follows.

a) *Initialize.* Let q be a prime power, where $q > \max\{n,\tau\}$, and let $\mathbb{F}_q$ be the finite field with q elements. We assume that the identity of each participant P_i is encoded as $P_i \in \mathbb{F}_q\setminus\{0\}$. Also, we assume $\mathcal{T} = \{1,2,\ldots,\tau\} \subset \mathbb{F}_q\setminus\{0\}$ by using appropriate encoding. First, TA chooses ℓ, which

[*8] In this optimal construction, a dealer is only allowed to choose $\boldsymbol{k_1}$ and $\boldsymbol{k_2}$ such that $\boldsymbol{k_2 - k_1 \leq \ell}$, where $\boldsymbol{\ell}$ is determined by $\boldsymbol{TA}$ in the phase *Initialize*. In this sense, this construction is restricted.

is the maximum difference between k_2 and k_1. Note that k_1 and k_2 will be determined by a dealer D in the phase *Share*. Then, TA chooses $\tau\ell$ numbers $r_i^{(t)}$ ($1 \le i \le \ell$, and $1 \le t \le \tau$) from $\mathbb{F}_q$ uniformly at random. TA sends a secret key $sk := \{(r_1^{(t)}, r_2^{(t)}, \ldots, r_\ell^{(t)})\}_{1 \le t \le \tau}$ to TS and D via secure channels, respectively.

b) *Share.* First, D randomly selects a secret $s \in \mathbb{F}_q$ according to a distribution P_S over $\mathbb{F}_q$, and chooses k_1, k_2 and n such that $k_2 - k_1 \le \ell$. Also, D specifies the time t when at least k_1 participants can reconstruct the secret. Next, D randomly chooses a polynomial $f(x) := s + \sum_{i=1}^{k_2-1} a_i x^i$ over $\mathbb{F}_q$, where each coefficient a_i is randomly and uniformly chosen from $\mathbb{F}_q$. Then, D computes a share $u_i^{(t)} := f(P_i)$ and a public parameter $p_i^{(t)} := a_{k_1-1+i} + r_i^{(t)}$ ($i = 1, 2, \ldots, k_2 - k_1$). Finally, D sends $(u_i^{(t)}, t)$ to P_i ($i = 1, 2, \ldots, n$) via a secure channel and discloses $pp := (p_1^{(t)}, \ldots, p_{k_2-k_1}^{(t)})$.

c) *Extract.* For sk and time $t \in \mathcal{T}$, TS broadcasts a time-signal at time t, $ts^{(t)} := (r_1^{(t)}, r_2^{(t)}, \ldots, r_\ell^{(t)})$ to all participants via a (authenticated) broadcast channel.

d) *Reconstruct with time-signals.* Suppose that all participants receive $ts^{(t)} = (r_1^{(t)}, r_2^{(t)}, \ldots, r_\ell^{(t)})$. Let $\mathcal{A} = \{P_{i_1}, P_{i_2}, \ldots, P_{i_{k_1}}\} \in \mathcal{PS}(\mathcal{P}, k_1, k_1)$ be a set of any k_1 participants. First, each $P_{i_j} \in \mathcal{A}$ computes $a_{k_1-1+i} = p_i^{(t)} - r_i^{(t)}$ ($i = 1, 2, \ldots, k_2 - k_1$) and constructs $g(x) := \sum_{k_1}^{k_2-1} a_i x^i$. Then, each P_{i_j} computes $h(P_{i_j}) := f(P_{i_j}) - g(P_{i_j})$ ($j = 1, \ldots, k_1$) such that $h(x) := s + \sum_{i=1}^{k_1-1} a_i x^i$. Then, they compute

$$s = \sum_{j=1}^{k_1} \left(\prod_{l \ne j} \frac{P_{i_j}}{P_{i_j} - P_{i_l}} \right) h(P_{i_j}),$$

by Lagrange interpolation from $(h(P_{i_1}), \ldots, h(P_{i_{k_1}}))$.

e) *Reconstruct without time-signals.* Any $\hat{\mathcal{A}} = \{P_{i_1}, P_{i_2}, \ldots, P_{i_{k_2}}\} \in \mathcal{PS}(\mathcal{P}, k_2, k_2)$ computes

$$s = \sum_{j=1}^{k_2} \left(\prod_{l \ne j} \frac{P_{i_j}}{P_{i_j} - P_{i_l}} \right) f(P_{i_j}),$$

by Lagrange interpolation from their k_2 shares.

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

Theorem 4. *The resulting (k_1, k_2, n)-TR-SS Θ by the above construction is secure. Moreover, it is optimal if $k_2 - k_1 = \ell$.*

Proof. First, we show the proof of (i) in Definition 5. We can prove this as in Shamir's secret sharing scheme [29]. Assume that $k_1 - 1$ participants $\mathcal{F} = \{P_{i_1}, \ldots, P_{i_{k_1-1}}\} \in \mathcal{PS}(\mathcal{P}, k_1 - 1, k_1 - 1)$ try to guess s by using their shares, public parameters, and all time-signals. $\mathcal{F}$ can compute $g(x)$ from public parameters and the time-signal at the specified time, hence they can get $h(P_{i_l}) = f(P_{i_l}) - g(P_{i_l})$ ($l = 1, \ldots, k_1 - 1$). Thus, they can know the following:

$$\begin{pmatrix} 1 & P_{i_1} & \cdots & P_{i_1}^{k_1-1} \\ 1 & P_{i_2} & \cdots & P_{i_2}^{k_1-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & P_{i_{k_1-1}} & \cdots & P_{i_{k_1-1}}^{k_1-1} \end{pmatrix} \begin{pmatrix} s \\ a_1 \\ \vdots \\ a_{k_1-1} \end{pmatrix}. \tag{15}$$

However, from Eq. (15), they cannot guess at least one element of $(a_1, \ldots, a_{k_1-1})$ with probability larger than $1/q$. Therefore, from the property of the one-time pad, we have $H(S \mid U_{\mathcal{F}}^{(t)}, TI^{(1)}, \ldots, TI^{(\tau)}) = H(S)$ for any $\mathcal{F} \in \mathcal{PS}(\mathcal{P}, 1, k_1 - 1)$ and any $t \in \mathcal{T}$.

Next, we show the proof of (ii) in Definition 5. Without loss of generality, we suppose that $k_2 - k_1 = \ell$, and that $k_2 - 1$ participants try to guess s by using their shares, public parameters, and time-signals at all the time except the time t. First, they cannot guess at least one coefficient of $f(x)$ with probability larger than $1/q$ since the degree of $f(x)$ is at most $k_2 - 1$ as in Shamir's secret sharing scheme [29]. Therefore, they attempt to guess one of $a_{k_1}, \ldots, a_{k_2-1}$ by using their $k_2 - 1$ shares, public parameters and $\tau - 1$ time-signals, since if they obtain any one of these coefficient, they can get $f^*(P_{i_l})$ ($l = 1, \ldots, k_2 - 1$) such that the degree of $f^*(x)$ is $k_2 - 2$ and reconstruct s by Lagrange interpolation. They know $\tau - 1$ time-signals, however, these time-signals $\{(r_1^{(j)}, \ldots, r_\ell^{(j)})\}_{j=1,\ldots,t-1,t+1,\ldots,\tau}$ are independent of the time-signal $(r_1^{(t)}, \ldots, r_\ell^{(t)})$ at τ. Hence, by the security of one-time pad, they cannot guess each a_{k_1-1+i} ($= p_i^{(t)} - r_i^{(t)}$) ($1 \le i \le k_2 - k_1$) with probability larger than $1/q$ since each $r_i^{(t)}$ is chosen from $\mathbb{F}_q$ uniformly at random. Therefore, for any $\mathcal{A} \in \mathcal{PS}(\mathcal{P}, k_1, k_2 - 1)$ and any $t \in \mathcal{T}$, we have $H(S \mid U_{\mathcal{A}}^{(t)}, TI^{(1)}, \ldots, TI^{(t-1)}, TI^{(t+1)}, \ldots, TI^{(\tau)}) = H(S)$.

Finally, if $k_2 - k_1 = \ell$, it is straightforward to see that the construction satisfies all the equalities of lower bounds in Theorem 3. Therefore, the above construction is optimal if $k_2 - k_1 = \ell$. □

4. Extensions

In this section, we discuss the following extensions of our results in the previous sections.

Timed-release Secret Sharing with General Access Structures. In Ref. [19], a generic construction of secret sharing schemes for any general access structure by using threshold secret sharing schemes was proposed, and later such a technique was improved in terms of efficiency on share sizes in Refs. [1], [32]. We can realize a timed-release secret sharing scheme for any general access structures from (k, n)-TR-SS schemes based on the techniques [1], [32].

Robust Timed-release Secret Sharing Schemes. Robust secret sharing schemes [11], [15], [20], [26] are secret sharing schemes secure against malicious modification of shares. Technically, suppose that at most ω ($< n/2$) participants are allowed to modify their own shares so that a reconstructor recovers a secret s', which is different from the original secret s, from all n shares. Then, the secret sharing scheme is said to be (ω, δ)-robust if the success probability of the attack is at most δ. We can construct a (ω, δ)-robust TR-SS scheme by using $(\omega + 1, n)$-TR-SS schemes via two existing approaches: (1) the Rabin–Ben-Or (RB) approach [11], [26]; and (2) the Cramer–Damgård–Fehr (CDF) approach [15], [20]. Since each scheme can be easily constructed and security of each scheme can be proved by a slight modification to the original proof, we here briefly explain the two approaches below.

(1) The RB approach: We can construct a (ω, δ)-robust TR-SS scheme from a $(\omega + 1, n)$-TR-SS scheme and an information-theoretically secure authentication code (A-code for short) [30].

First, a dealer specifies time t, and generates n shares $u_1^{(t)}, \ldots, u_n^{(t)}$ of a secret s by using the $(\omega+1, n)$-TR-SS scheme. Next, he generates n^2 keys of the A-code, $k_i^{(j)}$ $(1 \le i, j \le n)$, and generates tags $tag_i^{(j)}$ by using $u_j^{(t)}$ and $k_i^{(j)}$. Then, P_i's share is $(u_i^{(t)}, k_i^{(1)}, \ldots, k_i^{(n)}, tag_1^{(i)}, \ldots, tag_n^{(i)})$. In the reconstruction phase, a reconstructor checks the validity of $u_i^{(t)}$ by using $k_j^{(i)}$ and $tag_j^{(i)}$. If the validity of $u_i^{(t)}$ is guaranteed by at least $\omega+1$ pairs of $k_j^{(i)}$ and $tag_j^{(i)}$, then the share is considered as the *valid* share. After receiving a time-signal at t, then the secret s can be recovered from at least $\omega+1$ valid shares and the time-signal.

(2) The CDF approach: We can also construct a (ω, δ)-robust TR-SS scheme from a $(\omega+1, n)$-TR-SS scheme and a traditional $(\omega+1, n)$-SS scheme. For simplicity, let $\mathcal{S} := \mathbb{F}_q$. First, as in the RB approach, a dealer specifies time t, and generates n shares $u_1^{(t)}, \ldots, u_n^{(t)}$ of a secret s by using the $(\omega+1, n)$-TR-SS scheme. Then, he chooses $r \in \mathbb{F}_q$ uniformly at random, and computes $tag := s \cdot r$. He generates n shares of r and tag by using the $(\omega+1, n)$-SS scheme, respectively. Let $\tilde{u}_1^{(t)}, \ldots, \tilde{u}_n^{(t)}$ be shares of r, and $\hat{u}_1^{(t)}, \ldots, \hat{u}_n^{(t)}$ be shares of tag, respectively. Then, P_i's share is $(u_i^{(t)}, \tilde{u}_i^{(t)}, \hat{u}_i^{(t)})$. In the reconstruction phase, a reconstructor chooses a subset of $\omega+1$ participants, and reconstructs s', r', and tag' from their shares and a time-signal at t. Then, he checks whether it holds $s' \cdot r' = tag'$ or not. If so, he accepts s' as the original secret. Otherwise, he chooses different $\omega+1$ participants and performs the above operation again.

5. Conclusion

In this paper, we showed how we realized information-theoretically secure secret sharing schemes with timed-release security. Specifically, we considered two schemes, a (k, n)-TR-SS scheme and a (k_1, k_2, n)-TR-SS scheme. In the former, at least k participants can reconstruct a secret only with a time-signal at the specified time. In the latter, at least k_2 participants can reconstruct a secret from only their shares as in the traditional secret sharing scheme, whereas at least k_1 (but less than k_2) participants can reconstruct a secret only with a time-signal at the specified time. We gave mathematical models and security definitions of both schemes, derived lower bounds on sizes of shares, time-signals, and secret keys required for both schemes. Moreover, we proposed optimal constructions of both schemes, and discussed the extensions of TR-SS schemes.

Acknowledgments The first author is supported by JSPS Research Fellowships for Young Scientists. This work (Yohei Watanabe) was supported by Grant-in-Aid for JSPS Fellows Grant Number 25·3998. This work (Junji Shikata) was in part supported by JSPS KAKENHI Grant Number 15H02710, and in part conducted under the auspices of the MEXT Program for Promoting the Reform of National Universities.

References

[1] Benaloh, J. and Leichter, J.: Generalized Secret Sharing and Monotone Functions, *Advances in Cryptology — CRYPTO '88*, Goldwasser, S. (Ed.), Vol.403, pp.27–35, Springer New York (1990).

[2] Bitansky, N., Goldwasser, S., Jain, A., Paneth, O., Vaikuntanathan, V. and Waters, B.: Time-Lock Puzzles from Randomized Encodings, Cryptology ePrint Archive, Report 2015/514 (2015).

[3] Blakley, B., Blakley, G., Chan, A. and Massey, J.: Threshold Schemes with Disenrollment, *Advances in Cryptology — CRYPTO '92*, Brickell, E. (Ed.), Vol.740, pp.540–548, Springer Berlin Heidelberg (1993).

[4] Blakley, G.: Safeguarding cryptographic keys, *Proc. 1979 AFIPS National Computer Conference*, Monval, NJ, USA, pp.313–317, AFIPS Press (1979).

[5] Blundo, C., Cresti, A., Santis, A. and Vaccaro, U.: Fully Dynamic Secret Sharing Schemes, *Advances in Cryptology — CRYPTO '93*, Stinson, D. (Ed.), Vol.773, pp.110–125, Springer Berlin Heidelberg (1994).

[6] Blundo, C., Cresti, A., Santis, A.D. and Vaccaro, U.: Fully dynamic secret sharing schemes, *Theoretical Computer Science*, Vol.165, No.2, pp.407–440 (1996).

[7] Brickell, E.: Some Ideal Secret Sharing Schemes, *Advances in Cryptology — EUROCRYPT '89*, Quisquater, J.-J. and Vandewalle, J. (Eds.), Lecture Notes in Computer Science, Vol.434, pp.468–475, Springer Berlin Heidelberg (1990).

[8] Burmester, M., Desmedt, Y. and Seberry, J.: Equitable Key Escrow with Limited Time Span (or, How to Enforce Time Expiration Cryptographically) Extended Abstract, *Advances in Cryptology — ASIACRYPT '98*, Ohta, K. and Pei, D. (Eds.), Vol.1514, pp.380–391, Springer Berlin Heidelberg (1998).

[9] Cachin, C.: On-line secret sharing, *Cryptography and Coding*, Boyd, C. (Ed.), Vol.1025, pp.190–198, Springer Berlin Heidelberg (1995).

[10] Cathalo, J., Libert, B. and Quisquater, J.-J.: Efficient and Non-interactive Timed-Release Encryption, *Information and Communications Security*, Qing, S., Mao, W., López, J. and Wang, G. (Eds.), Vol.3783, pp.291–303, Springer Berlin Heidelberg (2005).

[11] Cevallos, A., Fehr, S., Ostrovsky, R. and Rabani, Y.: Unconditionally-Secure Robust Secret Sharing with Compact Shares, *Advances in Cryptology — EUROCRYPT 2012*, Pointcheval, D. and Johansson, T. (Eds.), Vol.7237, pp.195–208, Springer Berlin Heidelberg (2012).

[12] Chalkias, K., Hristu-Varsakelis, D. and Stephanides, G.: Improved Anonymous Timed-Release Encryption, *Computer Security — ESORICS 2007*, Biskup, J. and López, J. (Eds.), Vol.4734, pp.311–326, Springer Berlin Heidelberg (2007).

[13] Chan, A.-F. and Blake, I.: Scalable, Server-Passive, User-Anonymous Timed Release Cryptography, *25th IEEE International Conference on Distributed Computing Systems*, *ICDCS 2015*, pp.504–513 (2005).

[14] Cover, T.M. and Thomas, J.A.: *Elements of Information Theory*, 2nd edition, Wiley-Interscience (2006).

[15] Cramer, R., Damgård, I. and Fehr, S.: On the Cost of Reconstructing a Secret, or VSS with Optimal Reconstruction Phase, *Advances in Cryptology — CRYPTO 2001*, Kilian, J. (Ed.), Vol.2139, pp.503–523, Springer Berlin Heidelberg (2001).

[16] Garay, J. and Jakobsson, M.: Timed Release of Standard Digital Signatures, *Financial Cryptography*, Blaze, M. (Ed.), FC 2002, Vol.2357, pp.168–182, Springer Berlin Heidelberg (2003).

[17] Garay, J. and Pomerance, C.: Timed Fair Exchange of Standard Signatures, *Financial Cryptography*, Wright, R. (Ed.), FC 2003, Vol.2742, pp.190–207, Springer Berlin Heidelberg (2003).

[18] Herzberg, A., Jarecki, S., Krawczyk, H. and Yung, M.: Proactive Secret Sharing Or: How to Cope With Perpetual Leakage, *Advances in Cryptology — CRYPTO '95*, Coppersmith, D. (Ed.), Vol.963, pp.339–352, Springer Berlin Heidelberg (1995).

[19] Ito, M., Saito, A. and Nishizeki, T.: Secret sharing scheme realizing general access structure, *Electronics and Communications in Japan* (*Part III: Fundamental Electronic Science*), Vol.72, No.9, pp.56–64 (1989). The preliminary version appeared in IEEE Globecom '87, pp.99–102.

[20] Jhanwar, M. and Safavi-Naini, R.: Unconditionally-Secure Robust Secret Sharing with Minimum Share Size, *Financial Cryptography and Data Security*, Sadeghi, A.-R. (Ed.), Vol.7859, pp.96–110, Springer Berlin Heidelberg (2013).

[21] Karnin, E., Greene, J. and Hellman, M.: On secret sharing systems, *IEEE Trans. Inf. Theory*, Vol.29, No.1, pp.35–41 (1983).

[22] Mahmoody, M., Moran, T. and Vadhan, S.: Time-Lock Puzzles in the Random Oracle Model, *Advances in Cryptology – CRYPTO 2011*, Rogaway, P. (Ed.), Lecture Notes in Computer Science, Vol.6841, pp.39–50, Springer Berlin Heidelberg (2011).

[23] Martin, K.M., Safavi-Naini, R. and Wang, H.: Bounds and Techniques for Efficient Redistribution of Secret Shares to New Access Structures, *The Computer Journal*, Vol.42, No.8, pp.638–649 (1999).

[24] Martin, K., Pieprzyk, J., Safavi-Naini, R. and Wang, H.: Changing Thresholds in the Absence of Secure Channels, *Information Security and Privacy*, Pieprzyk, J., Safavi-Naini, R. and Seberry, J. (Eds.), Vol.1587, pp.177–191, Springer Berlin Heidelberg (1999).

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

[26] Rabin, T. and Ben-Or, M.: Verifiable secret sharing and multiparty protocols with honest majority, *Proc. 21st Annual ACM Symposium on Theory of Computing*, *STOC '89*, pp.73–85, ACM (1989).

[27] Rivest, R.L.: Unconditionally secure commitment and Oblivious Transfer Schemes Using Private Channels and a Trusted Initializer (1999). manuscript.
[28] Rivest, R.L., Shamir, A. and Wagner, D.A.: Time-lock puzzles and timed-release crypto, Technical Report Technical memo MIT/LCS/TR-684, MIT Laboratory for Computer Science (1996). (Revision 3/10/96).
[29] Shamir, A.: How to share a secret, *Comm. ACM*, Vol.22, No.11, pp.612–613 (1979).
[30] Simmons, G.: Authentication Theory/Coding Theory, *Advances in Cryptology*, Blakley, G. and Chaum, D. (Eds.), Lecture Notes in Computer Science, Vol.196, pp.411–431, Springer Berlin Heidelberg (1985).
[31] Simmons, G.: How to (Really) Share a Secret, *Advances in Cryptology — CRYPTO '88*, Goldwasser, S. (Ed.), Lecture Notes in Computer Science, Vol.403, pp.390–448, Springer New York (1990).
[32] Tochikubo, K., Uyematsu, T. and Matsumoto, R.: Efficient Secret Sharing Schemes Based on Authorized Subsets, *IEICE Trans.*, Vol.88-A, No.1, pp.322–326 (2005).
[33] Watanabe, Y., Seito, T. and Shikata, J.: Information-Theoretic Timed-Release Security: Key-Agreement, Encryption, and Authentication Codes, *Information Theoretic Security*, Smith, A. (Ed.), Vol.7412, pp.167–186, Springer Berlin Heidelberg (2012).
[34] Watanabe, Y. and Shikata, J.: Timed-Release Computational Secret Sharing Scheme and Its Applications, *Provable Security*, Chow, S., Liu, J., Hui, L. and Yiu, S. (Eds.), Vol.8782, pp.326–333, Springer International Publishing (2014).
[35] Watanabe, Y. and Shikata, J.: Timed-Release Secret Sharing Schemes with Information Theoretic Security, *Cryptography and Information Security in the Balkans*, Ors, B. and Preneel, B. (Eds.), Vol.9024, pp.219–236, Springer International Publishing (2015).

Appendix

A.1 Naive Construction of (k_1, k_2, n)-TR-SS

Our idea of a naive construction is a combination of (k_1, n)-TR-SS (Section 2.3) and Shamir's (k_2, n)-SS [29].

a) *Initialize.* Let q be a prime power, where $q > \max\{n, \tau\}$, and let $\mathbb{F}_q$ be the finite field with q elements. We assume that the identity of each participant P_i is encoded as $P_i \in \mathbb{F}_q \backslash \{0\}$. Also, we assume $\mathcal{T} = \{1, 2, \ldots, \tau\} \subset \mathbb{F}_q \backslash \{0\}$ by using appropriate encoding. First, TA chooses uniformly at random τ numbers $r^{(j)}$ $(1 \le j \le \tau)$ from $\mathbb{F}_q$. TA sends a secret key $sk := (r^{(1)}, \ldots, r^{(\tau)})$ to TS and D via secure channels, respectively.

b) *Share.* First, D randomly chooses a secret $s \in \mathbb{F}_q$ according to a distribution P_S over $\mathbb{F}_q$. Also, D specifies the time t when at least k_1 participants can reconstruct the secret and chooses t-th key $r^{(t)}$. Next, D randomly chooses two polynomials $f_1(x) := s + r^{(t)} + \sum_{i=1}^{k_1-1} a_{1i}x^i$ and $f_2(x) := s + \sum_{i=1}^{k_2-1} a_{2i}x^i$ over $\mathbb{F}_q$, where each coefficient is randomly and uniformly chosen from $\mathbb{F}_q$. Then, D computes $u_i^{(t)} := (f_1(P_i), f_2(P_i))$. Finally, D sends $(u_i^{(t)}, t)$ to P_i $(i = 1, 2, \ldots, n)$ via a secure channel.

c) *Extract.* For sk and time $t \in \mathcal{T}$, TS broadcasts t-th key $r^{(t)}$ as a time-signal at time t to all participants via a (authenticated) broadcast channel.

d) *Reconstruct with time-signals.* First, $\mathcal{A} = \{P_{i_1}, P_{i_2}, \ldots, P_{i_{k_1}}\} \in \mathcal{PS}(\mathcal{P}, k_1, k_1)$ computes $s + r^{(t)}$ by Lagrange interpolation:

$$s + r^{(t)} = \sum_{j=1}^{k_1} \left(\prod_{l \neq j} \frac{P_{i_j}}{P_{i_j} - P_{i_l}} \right) f_1(P_{i_j}),$$

from $(f_1(P_{i_1}), \ldots, f_1(P_{i_{k_1}}))$. After receiving $ts^{(t)} = r^{(t)}$, they can compute s from $s + r^{(t)}$ and $ts^{(t)}$ by $(s + r^{(t)}) - ts^{(t)}$.

e) *Reconstruct without time-signals.* Any $\hat{\mathcal{A}} = \{P_{i_1}, P_{i_2}, \ldots, P_{i_{k_2}}\} \in \mathcal{PS}(\mathcal{P}, k_2, k_2)$ computes

$$s = \sum_{j=1}^{k_2} \left(\prod_{l \neq j} \frac{P_{i_j}}{P_{i_j} - P_{i_l}} \right) f_2(P_{i_j}),$$

by Lagrange interpolation from $(f_2(P_{i_1}), \ldots, f_2(P_{i_{k_2}}))$.

It is easy to see that the above construction is secure, since this construction is a simple combination of (k_1, n)-TR-SS and Shamir's (k_2, n)-SS. Also, the above construction is simple, however not optimal since the resulting share size is twice as large as that of secrets.

Yohei Watanabe received his B.E., M.E., and Ph.D. in information science from Yokohama National University, Japan, in 2011, 2013, and 2016, respectively. He was also a JSPS Research Fellow (DC1) from 2013 to 2016 during his Ph.D. course. He is currently a JSPS Research Fellow (PD) at the University of Electro-Communications from 2016. His research interests include cryptography and information security. He received the CSS Student Paper Prize from IPSJ in 2014, the Best Poster Award in the 9th International Workshop on Security (IWSEC 2014), and the SCIS Paper Prize from IEICE in 2016.

Junji Shikata received his B.S. and M.S. degrees in mathematics from Kyoto University, Kyoto, Japan, in 1994 and 1997, respectively, and Ph.D. degree in mathematics from Osaka University, Osaka, Japan, in 2000. From 2000 to 2002 he was a Postdoctoral Fellow at the Institute of Industrial Science, the University of Tokyo, Tokyo, Japan. Since 2002 he has been with the Graduate School of Environment and Information Sciences, Yokohama National University, Yokohama, Japan. From 2008 to 2009, he was a visiting researcher at the Department of Computer Science, Swiss Federal Institute of Technology (ETH), Zurich, Switzerland. Currently, he is a Professor of Yokohama National University. His research interests include cryptology, information theory, theoretical computer science, and computational number theory. Dr. Shikata received several awards including the 19th TELECOM System Technology Award from the Telecommunications Advancement Foundation in 2004, the Wilkes Award 2006 from the British Computer Society, and the Young Scientists' Prize, the Commendation for Science and Technology by the Minister of Education, Culture, Sports, Science and Technology in Japan in 2010.