PAPER *Special Section on Cryptography and Information Security*

Linear Algebraic Approach to Strongly Secure Ramp Secret Sharing for General Access Structures with Application to Symmetric PIR**

Reo ERIGUCHI[†*a)], **Noboru KUNIHIRO**[††], ***Nonmembers, and*** **Koji NUIDA**[†††*], ***Member***

SUMMARY Ramp secret sharing is a variant of secret sharing which can achieve better information ratio than perfect schemes by allowing some partial information on a secret to leak out. Strongly secure ramp schemes can control the amount of leaked information on the components of a secret. In this paper, we reduce the construction of strongly secure ramp secret sharing for general access structures to a linear algebraic problem. As a result, we show that previous results on strongly secure network coding imply two linear transformation methods to make a given linear ramp scheme strongly secure. They are explicit or provide a deterministic algorithm while the previous methods which work for any linear ramp scheme are non-constructive. In addition, we present a novel application of strongly secure ramp schemes to symmetric PIR in a multi-user setting. Our solution is advantageous over those based on a non-strongly secure scheme in that it reduces the amount of communication between users and servers and also the amount of correlated randomness that servers generate in the setup.

key words: *secret sharing, general access structure, strong security, private information retrieval*

1. Introduction

1.1 Backgrounds

Secret sharing [2], [3] is a cryptographic primitive to share a secret $\boldsymbol{s} = (s_1, \ldots, s_L)$ among a set P of n participants in such a way that authorized sets in a family $\Phi \subseteq 2^P$ are able to recover $\boldsymbol{s}$ while forbidden sets in $\Psi \subseteq 2^P$ learn no information. If a secret sharing scheme is perfect, that is, $\Phi \cup \Psi = 2^P$, then $\boldsymbol{s}$ is perfectly private against an adversary. However, the perfect secrecy is too strong for real-world applications and may result in large storage overhead. It is then more important to reduce the overhead even at the cost of giving up the perfect secrecy, that is, $\Phi \cup \Psi \neq 2^P$. For this purpose, the notion of ramp secret sharing was proposed [4]–[6]. A ramp secret sharing scheme for an L-level access structure $\mathcal{A}_L = (\Gamma_j)_{0 \leq j \leq L}$ guarantees that Γ_L is the family of authorized sets, Γ_0 is the family of forbidden sets, and every set in Γ_j obtains information on $\boldsymbol{s}$ with a ratio of j/L.

1.1.1 Strong Security

Secret sharing is directly applied to distributed data storage, in which each sub-secret s_j represents a confidential file and shares are stored, e.g., by servers. We should prevent meaningful information on s_j from being revealed when some fraction of $\boldsymbol{s}$ is leaked. To address this problem, the notion of strong security [6], [7] guarantees that for each j, no subset in Γ_j obtains information on any $L - j$ sub-secrets.

Iwamoto and Yamamoto [7] proposed an explicit method to make a given ramp scheme for a general access structure strongly secure, assuming that the initial scheme satisfies a special property of partial decryptability. Then Eriguchi and Kunihiro [8] gave probabilistic methods assuming that the initial scheme satisfies linearity, which is a more common property of secret sharing. However, their methods are non-constructive and there is no method to verify the resulting scheme is indeed strongly secure except for the brute-force approach, which involves checking exponentially many matrices for non-singularity. In summary, it is unknown whether there is an explicit construction of strongly secure schemes from a given linear ramp scheme.

1.1.2 Application to Symmetric PIR

Another important application of secret sharing is private information retrieval (PIR) [9], in which a user can retrieve a value in a database replicated among the set P of n servers without letting them know the index. A PIR scheme has a response pattern $\Phi \subseteq 2^P$ if the user can retrieve one from responses of any set of servers $A \in \Phi$, and has a collusion pattern $\Psi \subseteq 2^P$ if any collusion of $B \in \Psi$ gets no information on the user's index. Symmetric PIR (SPIR) [10] is a variant of PIR which additionally guarantees that the user does not

Manuscript received March 2, 2022.
Manuscript revised July 15, 2022.
Manuscript publicized September 13, 2022.

[†] The author is with The University of Tokyo, Tokyo, 113-8654 Japan.

[††] The author is with University of Tsukuba, Tsukuba-shi, 305-8573 Japan.

[†††] The author is with Kyushu University, Fukuoka-shi, 819-0395 Japan.

[*] Presently, with National Institute of Advanced Industrial Science and Technology (AIST), Tokyo, Japan.

[**] This paper is presented in part at International Symposium on Information Theory and Its Applications (ISITA), 2020 [1]. This research was partially supported by JST CREST Grant Number JPMJCR2113, Japan and JSPS KAKENHI Grant Numbers JP20J20797 and JP19K22838. This research was in part conducted under a contract of "Research and development on new generation cryptography for secure wireless communication services" among "Research and Development for Expansion of Radio Wave Resources (JPJ000254)," which was supported by the Ministry of Internal Affairs and Communications, Japan.

a) E-mail: reo-eriguchi@g.ecc.u-tokyo.ac.jp

DOI: 10.1587/transfun.2022CIP0001

learn database records that he does not query. Recently, Song and Hayashi [11] have shown a transformation from a linear ramp secret sharing scheme for $\mathcal{A}_L = (\Gamma_j)_{0 \le j \le L}$ to an SPIR scheme with response pattern Γ_L and collusion pattern Γ_0.

In a real-world situation, there are many users having different response patterns that reflect their individual requirements, e.g., some user has access to a smaller number of servers than others. We consider a system model, in which there are non-colluding users each of whom has one of M response patterns $\Phi_1 \supseteq \cdots \supseteq \Phi_M$. We aim at realizing SPIR for (Φ_i, Ψ) between every user with response pattern Φ_i and servers. There are two naive solutions based on [11].

Solution I: To construct an SPIR scheme Π_1 for (Φ_1, Ψ) and use it for every user.

Since $\Phi_i \subseteq \Phi_1$, it works regardless of a user's response pattern. However, always assuming the worst case Φ_1 leads to a loss of efficiency. If Π_1 is constructed based on [11], a user with other response patterns Φ_i receives shares of a ramp scheme whose family of authorized sets is Φ_1, which results in unnecessarily higher communication cost.

Solution II: To construct M independent SPIR schemes $\Pi_1, \ldots, \Pi_M$ such that Π_i works for (Φ_i, Ψ) and use Π_i between a user and servers if the user has a response pattern Φ_i.

In this solution, however, servers need to generate M kinds of correlated randomness in the setup, each of which is a share of a ramp secret sharing scheme corresponding to Π_i. It is then important to devise a solution which provides the best of both worlds: it achieves minimal communication for a user with response pattern Φ_i and only needs correlated randomness whose amount is independent of M.

1.2 Our Results

1.2.1 Explicit and Deterministic Constructions of Strongly Secure Schemes

We propose two different methods to transform any linear ramp secret sharing scheme for a general access structure to a strongly secure one (Table 1). Our methods only require that an initial scheme satisfies linearity, which is a more common property of secret sharing than partial decryptability. The first one explicitly provides a desired transformation (Theorem 1). As a result, it always provides a strongly secure scheme and does not need to verify the correctness. Furthermore, the transformation is *universal* [13] in the sense that the same transformation is applicable to any ramp scheme. It has a drawback that the resulting scheme must be defined over an extension field, which means that the domains of secrets and shares have to be enlarged. To overcome it, we also show a deterministic algorithm to make any linear ramp scheme strongly secure while its time complexity is doubly exponential in the number of participants n (Theorem 2). The advantage is that it need not enlarge the domains if an initial scheme is defined over a sufficiently large field. See Sect. 4.3 for a more detailed comparison.

Table 1 Comparison of methods to make a ramp secret sharing scheme realizing $\mathcal{A}_L$ strongly secure. Let q, q' denote the sizes of the fields over which the initial and resulting schemes are defined, respectively. Let m^* denote the total number of shares distributed among participants in the optimal multiple assignment scheme.

Method	Initial scheme	Field size q'	Design
[7]	Partially decryptable	$2L$	Explicit
[12]	Multiple assignment	$L + m^*$	Optimization
[8]	Linear	$q^{O(L^2)}$	Non-constructive
[8]	Linear	$O(2^{L+n})$	Non-constructive
Theorem 1	Linear	q^{2L}	Explicit
Theorem 2	Linear	$2^{O(L2^n)}$	Deterministic

Our technical novelty is abstraction of a linear algebraic property common to both strongly secure linear ramp schemes for *general* access structures and strongly secure network codes [14]. As pointed out in [14], network codes were connected to *threshold* schemes in the sense that an adversary wiretapping j edges in a network code is viewed as the one who obtains j shares of a threshold scheme. However, it is not straightforward to generalize the connection to general access structures since the amount of leaked information is determined by Γ_j rather than the number of shares. The connection revealed by our result shows that two algorithms to construct strongly secure network codes [15], [16] can be used to make linear ramp schemes strongly secure.

1.2.2 Application to Multi-User SPIR

Based on a strongly secure ramp scheme, we provide a more efficient solution to SPIR in the above multi-user setting. We first formalize that problem by introducing a notion of *dynamic* SPIR scheme Π for $(\Phi_1, \ldots, \Phi_M; \Psi)$, in which every user can choose any Φ_i before generating queries but possibly after servers generate correlated randomness, and then it proceeds as an SPIR scheme with response pattern Φ_i and collusion pattern Ψ (Definition 4). We then construct a more efficient dynamic SPIR scheme than those based on the naive solutions described above (Theorem 4). Our solution has the following advantages:

- If a user has a response pattern Φ_M, the communication ratio of our scheme is the minimal information ratio of a linear ramp scheme whose family of authorized sets is Φ_M, which is generally smaller than that of Solution I.
- The servers need to generate only one share of the underlying ramp scheme as correlated randomness while they must generate M shares in Solution II.

We note that in our scheme, the communication ratio for a user with response pattern Φ_i, $i \neq M$ is possibly larger than that of Solution I. Our solution is especially useful in applications in which most of users have Φ_M while only a small fraction of them have Φ_i, $i \neq M$.

1.3 Related Work

Strongly secure ramp schemes for threshold access structures are studied in [6], [17], [18]. Matsumoto [12] showed a construction of strongly secure ramp schemes based on a multiple assignment technique [19]. Specifically, it assigns each participant a set of multiple shares generated by a threshold ramp scheme. By solving a certain optimization problem, one can find the optimal assignment as well as optimal parameters including the total number m^* of shares. However, it is shown in [19] that there exists an access structure which cannot be realized by that technique. Moreover, the associated optimization problem involves exponentially many variables.

Although related notions of multi-user PIR are studied in [20], [21], their results do not apply to our setting since database privacy is not considered. In the single-user setting, PIR and SPIR have been extensively studied in the literature to determine the optimal capacity since they were introduced in [9], [10]; e.g., see [11], [22] and references therein.

2. Preliminaries

2.1 Notations

Let $[m] = \{1, \ldots, m\}$ and $\mathbb{F}_q$ denote the field of size q. Throughout the paper all vectors are row vectors unless otherwise indicated. Let $\boldsymbol{e}_i$ denote the vector whose i-th entry is 1 and others are all 0. Let $\boldsymbol{0}_m$ denote the zero vector of length m. Unless otherwise indicated, the sets indexing the rows and columns of a matrix $\boldsymbol{M} \in \mathbb{F}_q^{r\times c}$ are identified with $[r]$ and $[c]$, respectively. Let $\mathrm{row}(\boldsymbol{M}) \subseteq \mathbb{F}_q^c$ denote the row space of $\boldsymbol{M}$. For $C \subseteq [c]$, we write $\boldsymbol{M}[C] \in \mathbb{F}_q^{r\times|C|}$ for the sub-matrix obtained by restricting the columns to C. For a family of matrices $(\boldsymbol{M}_i \in \mathbb{F}_q^{r_i\times c})_{i\in I}$ and $A \subseteq I$, we define $\boldsymbol{M}_A$ as the $(\sum_{i\in A} r_i)$-by-c matrix obtained by vertically concatenating $\boldsymbol{M}_i$, $i \in A$. Let $\boldsymbol{I}_m$ denote the identity matrix of size m and $\boldsymbol{O}_{m,j}$ denote the m-by-j zero matrix.

2.2 Secret Sharing

Let $P = [n]$ be the set of n participants and let 2^P denote the power set of P. A family $\mathcal{F} \subseteq 2^P$ is called monotonically increasing (resp. decreasing) if $A \in \mathcal{F}$ and $A \subseteq B$ (resp. $B \subseteq A$) imply $B \in \mathcal{F}$ for any $A, B \in 2^P$. An L-level access structure $\mathcal{A}_L = (\Gamma_j)_{0\le j\le L}$ on P is a tuple of $L+1$ families such that $\bigcup_{0\le j\le L} \Gamma_j = 2^P$, $\Gamma_j \cap \Gamma_k = \emptyset$ for $j \neq k$, and $\bigcup_{\ell\ge j} \Gamma_\ell$ is monotonically increasing for any $j \in [L]$.

Let $S = (S_1, \ldots, S_L)$ be a tuple of L mutually independent uniform random variables over the alphabet $\mathcal{X}$ and $V_1, \ldots, V_n$ be n random variables. Write $S_B = (S_i)_{i\in B}$ for $B \subseteq [L]$ and $V_A = (V_i)_{i\in A}$ for $A \subseteq P$. We say that $\Sigma = (S, V_1, \ldots, V_n)$ is a ramp secret sharing scheme realizing an L-level access structure $\mathcal{A}_L = (\Gamma_j)_{0\le j\le L}$ [23] if $\Gamma_j = \{A \subseteq P : H(S|V_A) = ((L-j)/L)H(S)\}$ for any $0 \le j \le L$, where $H(\cdot)$ and $H(\cdot|\cdot)$ are the entropy and the conditional entropy, respectively. A set of participants is called authorized (resp. forbidden) if it is in Γ_L (resp. Γ_0). The information ratio $\sigma(\Sigma)$ is defined by $\sum_{i\in P} H(V_i)/H(S)$.

Strongly secure ramp secret sharing schemes guarantee that no set in Γ_j has information on $L-j$ sub-secrets.

Definition 1 ([6], [7]). *Let $\Sigma = (S, V_1, \ldots, V_n)$ be a ramp secret sharing scheme realizing an L-level access structure $\mathcal{A}_L = (\Gamma_j)_{0\le j\le L}$. We say that Σ is strongly secure if $H(S_B|V_A) = H(S_B)$ for any $j \in [L-1]$, $A \in \Gamma_j$, and $B \subseteq [L]$ of size $L-j$.*

A ramp secret sharing scheme $\Sigma = (S, V_1 \ldots, V_n)$ is called $\mathbb{F}_q$-linear if there exist $L+n$ full row-rank matrices $\boldsymbol{U}_\ell \in \mathbb{F}_q^{1\times e}$, $\ell \in [L]$ and $\boldsymbol{W}_i \in \mathbb{F}_q^{d_i\times e}$, $i \in P$ such that the distribution of S_ℓ is given by $\boldsymbol{U}_\ell(R_1, \ldots, R_e)^\top$ and that of V_i is given by $\boldsymbol{W}_i(R_1, \ldots, R_e)^\top$, where the R_j's are mutually independent uniform random variables on $\mathbb{F}_q$. We can identify any linear ramp scheme with a pair of two matrices $(\boldsymbol{U}_{[L]}, \boldsymbol{W}_P)$. The information ratio is given by $\sigma(\Sigma) = \sum_{i\in P} d_i/L$. If Σ realizes $\mathcal{A}_L = (\Gamma_j)_{0\le j\le L}$, a set A is in Γ_j if and only if $\dim(\mathrm{row}(\boldsymbol{U}_{[L]}) \cap \mathrm{row}(\boldsymbol{W}_A)) = j$ [24].

A linear ramp scheme Σ provides an efficient share algorithm Σ.Share. Let $\boldsymbol{s} = (s_i)_{i\in[L]}$ be a secret drawn from the uniform distribution on $\mathbb{F}_q^L$. Σ.Share on input $\boldsymbol{s}$ chooses a vector $\boldsymbol{\rho} \in \mathbb{F}_q^e$ uniformly at random conditioned on $\boldsymbol{s}^\top = \boldsymbol{U}_{[L]}\boldsymbol{\rho}^\top$ and sets the i-th share as $\boldsymbol{v}_i = (\boldsymbol{W}_i\boldsymbol{\rho}^\top)^\top \in \mathbb{F}_q^{d_i}$.

2.3 Network Coding

Let L be a message length. We call a vector in $F := \mathbb{F}_q^m$ a packet. A network instance is a tuple of a directed acyclic graph $G = (\mathcal{V}, \mathcal{E})$, a source node s_G, and a set of sink nodes T_G, where s_G generates L packets $\boldsymbol{X} = (\boldsymbol{X}_1, \ldots, \boldsymbol{X}_L)^\top \in F^L$ and each edge carries one packet. A linear network code $\mathcal{N}$ is a family of vectors $(\boldsymbol{W}_e \in \mathbb{F}_q^{1\times L})_{e\in\mathcal{E}}$ such that:

1. For any $e = (u, v) \in \mathcal{E}$, $\boldsymbol{W}_e$ is an $\mathbb{F}_q$-linear combination of vectors $\boldsymbol{W}_f$ indexed by the incoming edges f to u.
2. For any $t \in T_G$, $\mathrm{rank}(\boldsymbol{W}_A) = L$, where A denotes the set of all the incoming edges to t.

We can identify $\mathcal{N}$ with a matrix $\boldsymbol{W}_\mathcal{E} \in \mathbb{F}_q^{|\mathcal{E}|\times L}$. If we let every edge $e \in \mathcal{E}$ carry a packet $\boldsymbol{W}_e\boldsymbol{X}$, then every sink node can recover $\boldsymbol{X}$ from packets transmitted over its incoming edges. Let $S = (S_1, \ldots, S_L)$ be a uniform random variable on F^L representing $\boldsymbol{X}$. Let V_e be a random variable on F representing a packet transmitted over $e \in \mathcal{E}$. Write $S_B = (S_i)_{i\in B}$ for $B \subseteq [L]$ and $V_A = (V_e)_{e\in A}$ for $A \subseteq \mathcal{E}$.

Fix an integer k such that $k < L$. For $j \in [k]$, we consider an adversary who wiretaps a set of j edges A and obtains $\boldsymbol{W}_A\boldsymbol{X}$. We may assume that $\boldsymbol{W}_A$ is full row-rank[†]. A strongly secure network code protects every subset of all the L packets $\boldsymbol{X}$ of size $L-j$ from the wiretapper. We follow the definition of strongly secure network codes given in [16].

[†] If $\boldsymbol{W}_e$ is spanned by the other rows $\boldsymbol{W}_f$, $f \in A \setminus \{e\}$, then the adversary can locally compute $\boldsymbol{W}_e\boldsymbol{X}$ without wiretapping e.

Definition 2 ([16]). *A linear network code $\mathcal{N}$ represented by $\boldsymbol{W}_{\mathcal{E}}$ is said to be strongly k-secure if $H(S_B|V_A) = H(S_B)$ for any $j \in [k]$, $A \subseteq \mathcal{E}$ of size j, and $B \subseteq [L]$ of size $L - j$. We simply say that it is strongly secure if $k = L - 1$.*

3. Linear Algebraic Problem Related to Strong Security

We abstract a linear algebraic problem which connects strongly secure ramp schemes with network codes.

3.1 Strongly Secure Ramp Secret Sharing

Let $\Sigma = (S, V_1, \ldots, V_n)$ be an $\mathbb{F}_q$-linear ramp secret sharing scheme and $(\boldsymbol{U}_{[L]}, \boldsymbol{W}_P)$ be the associated pair of matrices. The access structure and the information ratio of Σ do not change if Σ is viewed as an $\mathbb{F}_{q^m}$-linear scheme for $m \geq 1$.

We associate each subset $A \subseteq P$ with a set of row vectors $C^A(\Sigma) = \{\boldsymbol{c} \in \mathbb{F}_q^L : \boldsymbol{c}\boldsymbol{U}_{[L]} \in \operatorname{row}(\boldsymbol{W}_A)\}$. It follows that $C^A(\Sigma)$ is a j-dimensional vector space over $\mathbb{F}_q$ if $A \in \Gamma_j$, namely, an $[L, j]$-linear code over $\mathbb{F}_q$. It is shown in [8] that a linear ramp secret sharing scheme Σ corresponding to $(\boldsymbol{U}_{[L]}, \boldsymbol{W}_P)$ is strongly secure if and only if $C^A(\Sigma)$ is an MDS code for any $A \subseteq P$. Let $\boldsymbol{G}^A \in \mathbb{F}_q^{j\times L}$ be a generator matrix of $C^A(\Sigma)$. A well-known characterization of MDS codes implies that Σ is strongly secure if and only if

$$\det(\boldsymbol{G}^A[C]) \neq 0 \qquad (1)$$

for any $j \in [L-1]$, $A \in \Gamma_j$, and $C \subseteq [L]$ of size j.

There is a framework for transforming a given $\mathbb{F}_q$-linear ramp scheme Σ into another scheme based on a non-singular matrix [7]. Let $(\boldsymbol{U}_{[L]}, \boldsymbol{W}_P)$ be the pair of matrices associated with Σ. For a non-singular matrix $\boldsymbol{T} \in \mathbb{F}_{q^m}^{L\times L}$, define an $\mathbb{F}_{q^m}$-linear ramp scheme $\Sigma_{\boldsymbol{T}}$ as the one associated with $(\boldsymbol{T}^{-1}\boldsymbol{U}_{[L]}, \boldsymbol{W}_P)$. That is equivalent to applying the linear transformation $\boldsymbol{T}$ to a secret vector and then generating shares for its image using Σ. The access structure and the information ratio of $\Sigma_{\boldsymbol{T}}$ are the same as Σ. A generator matrix of $C^A(\Sigma_{\boldsymbol{T}})$ is given by $\boldsymbol{G}^A\boldsymbol{T}$ if $\boldsymbol{G}^A$ is a generator matrix of $C^A(\Sigma)$. Thus, $\Sigma_{\boldsymbol{T}}$ is strongly secure if and only if $\det((\boldsymbol{G}^A\boldsymbol{T})[C]) \neq 0$ for any $j \in [L-1]$, $A \in \Gamma_j$, and $C \subseteq [L]$ of size j. Now, consider the following problem.

Problem 1. *Let $\mathcal{M}_j \subseteq \mathbb{F}_q^{j\times L}$, $j \in [L-1]$ be given $L - 1$ families of full row-rank matrices. Let $\mathbb{F}_{q^m}/\mathbb{F}_q$ be a field extension of degree m. Find a non-singular matrix $\boldsymbol{T} \in \mathbb{F}_{q^m}^{L\times L}$ such that* $\det((\boldsymbol{G}\boldsymbol{T})[C]) \neq 0$ *for any $j \in [L-1]$, $\boldsymbol{G} \in \mathcal{M}_j$, and $C \subseteq [L]$ of size j.*

The construction of strongly secure schemes based on the transformation method of [7] is reduced to solving Problem 1 for $\mathcal{M}_j = \mathcal{S}_j(\Sigma) := \{\boldsymbol{G}^A : A \in \Gamma_j\}$. Note that the degree m should be as small as possible since the length of each share of $\Sigma_{\boldsymbol{T}}$ increases m times while $\sigma(\Sigma_{\boldsymbol{T}}) = \sigma(\Sigma)$.

3.2 Strongly Secure Network Coding

In the context of network coding, several methods have been devised in [14]–[16] to transform a linear network code $\mathcal{N}$ represented by $\boldsymbol{W}_{\mathcal{E}}$ into a strongly secure one. A basic strategy used in the literature is as follows: (1) identifying $F = \mathbb{F}_q^m$ with $\mathbb{F}_{q^m}$, multiply a message $\boldsymbol{X} \in F^L$ by a fixed non-singular matrix $\boldsymbol{T} \in \mathbb{F}_{q^m}^{L\times L}$ and (2) send $\boldsymbol{T}\boldsymbol{X} \in F^L$ as an input message using $\mathcal{N}$. We denote this new linear network code by $\mathcal{N}_{\boldsymbol{T}}$. It follows from a similar argument in [13] that $\mathcal{N}_{\boldsymbol{T}}$ is strongly secure if and only if $\boldsymbol{S} := \boldsymbol{T}^{-1}$ satisfies

$$\operatorname{rank}(\boldsymbol{S}_B) + \operatorname{rank}(\boldsymbol{W}_A) = \operatorname{rank}\begin{bmatrix}\boldsymbol{S}_B\\ \boldsymbol{W}_A\end{bmatrix}, \qquad (2)$$

for any $j \in [L-1]$, $A \subseteq \mathcal{E}$ of size j, and $B \subseteq [L]$ of size $L - j$. Here, $\boldsymbol{S}_B$ is the $|B| \times L$ matrix consisting only of the rows $\boldsymbol{S}_\ell$, $\ell \in B$ of $\boldsymbol{S}$. The left-hand side is equal to L since $\boldsymbol{S}_B$ and $\boldsymbol{W}_A$ are full row-rank. By multiplying the matrix $[\boldsymbol{S}_B^\top, \boldsymbol{W}_A^\top]^\top$ on the right side by $\boldsymbol{T}$ and performing the elementary row operation, we see that the right-hand side is equal to $L - j + \operatorname{rank}((\boldsymbol{W}_A\boldsymbol{T})[C])$, where $C = [L] \setminus B$. Thus, Eq. (2) holds if and only if $\operatorname{rank}((\boldsymbol{W}_A\boldsymbol{T})[C]) = j$.

We interpret the above discussion in the setting of Problem 1. Let $\mathcal{N}$ be a linear network code represented by a matrix $\boldsymbol{W}_{\mathcal{E}}$ over $\mathbb{F}_q$. For a non-singular matrix $\boldsymbol{T} \in \mathbb{F}_{q^m}^{L\times L}$, a linear network code $\mathcal{N}_{\boldsymbol{T}}$ is strongly secure if and only if $\boldsymbol{T}$ is a solution to Problem 1 for $\mathcal{M}_j = \mathcal{U}_j(\boldsymbol{W}_{\mathcal{E}}) := \{\boldsymbol{W}_A : A \text{ is a subset of } \mathcal{E} \text{ of size } j \text{ with } \operatorname{rank}(\boldsymbol{W}_A) = j\}$.

4. Explicit and Deterministic Constructions of Strongly Secure Schemes

The above linear algebraic connection shows that previous results on strongly secure network coding imply two constructions of strongly secure ramp secret sharing schemes.

4.1 Explicit Construction Based on Rank-Metric Codes

An explicit construction of strongly secure network codes based on rank-metric codes is given in [15]. Rank-metric code C is an $[\ell, k]$-linear code over $\mathbb{F}_{q^m}$. The distance between $\boldsymbol{X} \in C$ and $\boldsymbol{Y} \in C$ is given by $\operatorname{rank}(\phi(\boldsymbol{X}) - \phi(\boldsymbol{Y}))$, where ϕ is an isomorphism from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q^{m\times 1}$ and is applied on the row vectors $\boldsymbol{X}$ and $\boldsymbol{Y}$ entry-wise. The rank-metric code C is called MRD if $m \geq \ell$ and $d = \ell - k + 1$.

For any integers m and L satisfying $m \geq 2L$, let $C \subseteq \mathbb{F}_{q^m}^{2L}$ be an $[2L, L]$-linear MRD code with generator matrix $\boldsymbol{G} \in \mathbb{F}_{q^m}^{L\times 2L}$. The existence of such codes is guaranteed by Gabidulin codes [25], which are generated by $\boldsymbol{G} = (g_j^{q^{i-1}})_{i\in[L], j\in[2L]}$ for linearly independent elements $g_j \in \mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Without loss of generality, we may assume that $\boldsymbol{G}$ has the form of $\boldsymbol{G} = [\boldsymbol{I}_L, \boldsymbol{T}^\top]$ for some L-by-L matrix $\boldsymbol{T}$. The result of [15] implies that $\boldsymbol{T}$ is a solution to Problem 1 for $\mathcal{M}_j = \mathcal{R}_j(\mathbb{F}_q) := \{\boldsymbol{W} \in \mathbb{F}_q^{j\times L} : \operatorname{rank}(\boldsymbol{W}) = j\}$.

We provide a simpler proof of it for the convenience of the reader. Suppose that $\det((\boldsymbol{W}\boldsymbol{T})[C]) = 0$ for some $j \in [L-1]$, $\boldsymbol{W} \in \mathcal{M}_j$, and $C \subseteq [L]$ of size j. For ease of notation, we assume that $C = [j]$. Set $\boldsymbol{M} = \boldsymbol{T}[C] \in \mathbb{F}_{q^m}^{L\times j}$.

Let $\boldsymbol{v} \in \mathbb{F}_{q^m}^{j}$ be a non-zero vector such that $\boldsymbol{W}\boldsymbol{M}\boldsymbol{v}^\top = \boldsymbol{0}$ and let $\widetilde{\boldsymbol{v}} = (\boldsymbol{v}, \boldsymbol{0}_{L-j})$. Set $\boldsymbol{Y} = \phi(\widetilde{\boldsymbol{v}}\boldsymbol{G}) \in \mathbb{F}_q^{m\times 2L}$ and let $\boldsymbol{Y}_1, \boldsymbol{Y}_2 \in \mathbb{F}_q^{m\times L}$ be such that $\boldsymbol{Y} = [\boldsymbol{Y}_1, \boldsymbol{Y}_2]$. Since $\boldsymbol{v}\boldsymbol{M}^\top\boldsymbol{W}^\top = \boldsymbol{0}$, it holds that $\boldsymbol{Y}_2\boldsymbol{W}^\top = \boldsymbol{O}_{m,j}$. The form of $\widetilde{\boldsymbol{v}}\boldsymbol{G}$ implies that $\boldsymbol{Y}_1\boldsymbol{Z}^\top = \boldsymbol{O}_{m,L-j}$, where $\boldsymbol{Z} = [\boldsymbol{O}_{L-j,j}, \boldsymbol{I}_{L-j}] \in \mathbb{F}_q^{(L-j)\times L}$. We obtain $\mathrm{rank}(\phi(\widetilde{\boldsymbol{v}}\boldsymbol{G})) \leq 2L - (\mathrm{rank}(\boldsymbol{Z}^\top) + \mathrm{rank}(\boldsymbol{W}^\top)) = L$. However, since C is MRD, we must have $\mathrm{rank}(\phi(\widetilde{\boldsymbol{v}}\boldsymbol{G})) \geq L + 1$.

We show an explicit construction of strongly secure ramp secret sharing schemes. Let $m \geq 2L$ and $\boldsymbol{G} = \begin{bmatrix}\boldsymbol{I}_L & \boldsymbol{T}^\top\end{bmatrix}$ be a generator matrix of an $[2L, L]$-linear MRD code over $\mathbb{F}_{q^m}$. Then $\boldsymbol{T} \in \mathbb{F}_{q^m}^{L\times L}$ is a solution to Problem 1 for $\mathcal{M}_j = \mathcal{R}_j(\mathbb{F}_q)$. Since $\mathcal{S}_j(\Sigma) \subseteq \mathcal{R}_j(\mathbb{F}_q)$ for any $\mathbb{F}_q$-linear ramp secret sharing scheme Σ, $\boldsymbol{T}$ is also a solution to Problem 1 for $\mathcal{M}_j = \mathcal{S}_j(\Sigma)$ and hence $\Sigma_{\boldsymbol{T}}$ is strongly secure.

Theorem 1. *For any m and L with $m \geq 2L$, there exists an explicit construction of $\boldsymbol{T} \in \mathbb{F}_{q^m}^{L\times L}$ such that $\Sigma_{\boldsymbol{T}}$ is strongly secure for any $\mathbb{F}_q$-linear ramp scheme Σ.*

4.2 Deterministic Algorithm

A deterministic algorithm to construct a strongly secure network code is proposed in [16]. To explain it in the setting of Problem 1, let $(\boldsymbol{W}_e \in \mathbb{F}_q^{1\times L})_{e\in[N]}$ be a family of N row vectors. Note that N corresponds to the number of edges in the network. Let $\widetilde{N}$ be the *reduced size* [16] of the matrix $\boldsymbol{W}_{[N]}$, which is the number of rows of a maximal sub-matrix $\boldsymbol{W}_A$ such that any pair of rows is linearly independent. Set

$$K = \widetilde{N} + \sum_{i=1}^{L-2} \binom{L-1}{i}\binom{\widetilde{N}}{i+1}. \tag{3}$$

The algorithm of [16] takes as input $\boldsymbol{W}_{[N]}$ and any m satisfying $q^m > K$, and outputs a matrix $\boldsymbol{T} \in \mathbb{F}_{q^m}^{L\times L}$ such that $\boldsymbol{T}$ is a solution to Problem 1 for $\mathcal{M}_j = \mathcal{U}_j(\boldsymbol{W}_{[N]})$. Its time complexity is $O((LN^2 + L^2K)\mathsf{poly}(m, \log q))$.

Now, we can design a deterministic algorithm to obtain $\boldsymbol{T}$ for a given linear ramp scheme Σ such that $\Sigma_{\boldsymbol{T}}$ is strongly secure. Let Σ be an $\mathbb{F}_q$-linear ramp scheme with L-level access structure $\mathscr{A}_L = (\Gamma_j)_{0\leq j\leq L}$. First, let $\boldsymbol{G}^A \in \mathbb{F}_q^{j\times L}$ be a generator matrix of $C^A(\Sigma)$ for $j \in [L-1]$ and $A \in \Gamma_j$. Note that finding $\boldsymbol{G}^A$ is equivalent to computing the kernel of $[\boldsymbol{U}_{[L]}^\top, \boldsymbol{W}_A^\top]$, which can be done in polynomial time in j, L and $\log q$, e.g., by Gaussian elimination. Next, construct a set $\mathcal{G} \subseteq \mathbb{F}_q^L$ as $\mathcal{G} = \{\boldsymbol{v} : \boldsymbol{v}$ is a row of $\boldsymbol{G}^A$ for some $A\}$. Set $N = |\mathcal{G}|$ and write $\mathcal{G} = \{\boldsymbol{W}_e : e \in [N]\}$, that is, remove repeated elements. Let $\widetilde{N}$ be the reduced size of $\boldsymbol{W}_{[N]}$ and set K as in Eq. (3). Finally, run the algorithm of [16] for $\boldsymbol{W}_{[N]}$ and any m satisfying $q^m > K$ and obtain $\boldsymbol{T} \in \mathbb{F}_{q^m}^{L\times L}$. $\boldsymbol{T}$ is a solution to Problem 1 for $\mathcal{M}_j = \mathcal{U}_j(\boldsymbol{W}_{[N]})$. Since $\mathcal{S}_j(\Sigma) \subseteq \mathcal{U}_j(\boldsymbol{W}_{[N]})$, $\boldsymbol{T}$ is also a solution to Problem 1 for $\mathcal{M}_j = \mathcal{S}_j(\Sigma)$, which implies that $\Sigma_{\boldsymbol{T}}$ is strongly secure.

Theorem 2. *Let Σ be an $\mathbb{F}_q$-linear ramp scheme with L-level access structure $\mathscr{A}_L$. Define N and K as above and let m be any integer satisfying $q^m > K$. Then there exists a deterministic algorithm which outputs $\boldsymbol{T} \in \mathbb{F}_{q^m}^{L\times L}$ such that $\Sigma_{\boldsymbol{T}}$ is strongly secure.*

The resulting scheme has a field size $q^m > K$ in the worst-case. We have an upper bound $K \leq \widetilde{N} + 2^{L-1+\widetilde{N}} = 2^{O(L2^n)}$ since $N \leq \sum_{j\in[L-1]} j|\Gamma_j| \leq L2^n$. Letting $\sigma = n\sigma(\Sigma)$, the above algorithm has time complexity $O(2^n\mathsf{poly}(L, \sigma, \log q)) + O((LN^2 + L^2K)\mathsf{poly}(m, \log q)) = 2^{O(L2^n)}\mathsf{poly}(L, \sigma, m, \log q)$.

4.3 Comparison

In this section, we give a more detailed explanation of Table 1. We compare our transformations in Theorems 1 and 2 with [7], [8], [12] in terms of the assumption on an initial scheme, the design of transformations, and the field size.

(1) Assumption on an Initial Scheme

Theorems 1, 2, and [8] only require that an initial scheme be linear, which is satisfied by most of the previously proposed secret sharing schemes. To be precise, let Σ be an $\mathbb{F}_q$-linear ramp secret sharing scheme realizing an L-level access structure $\mathscr{A}_L = (\Gamma_j)_{0\leq j\leq L}$. If $q' = q^m$ exceeds the field size shown in Table 1, they can give a matrix $\boldsymbol{T} \in \mathbb{F}_{q^m}^{L\times L}$ to transform Σ into a strongly secure $\mathbb{F}_{q'}$-linear scheme $\Sigma_{\boldsymbol{T}}$. On the other hand, the method in [7] assumes that an initial scheme is partially decryptable, which means that every subset in Γ_j completely determines some j sub-secrets (see [7] for the formal definition). However, there is no construction of partially decryptable ramp schemes except one that must have a higher information ratio than linear perfect schemes [7]. The construction of [12] can only be applied to ramp schemes obtained by a multiple assignment technique [19], which are a subclass of linear schemes. It is also known that there exists an access structure which cannot be realized by that technique [19]. We conclude that our methods are advantageous over [7], [12] in that it is applied to a wider class of ramp schemes.

(2) Design of Transformation

Theorem 1 explicitly constructs a matrix $\boldsymbol{T}$ from a certain MRD code. It is also *universal* [13] in the sense that $\boldsymbol{T}$ is able to transform any $\mathbb{F}_q$-linear ramp scheme Σ into a strongly secure one. Theorem 2 provides a deterministic algorithm to obtain $\boldsymbol{T}$ while its time complexity is doubly exponential in n. However, it still works since n is fairly small in application to distributed data storage (e.g., $n = 6$) and also since once $\boldsymbol{T}$ is found, we can efficiently share and reconstruct secrets using the resulting strongly secure scheme. Our constructions being explicit and providing a deterministic algorithm are preferable to the non-constructive methods of [8], which fail to find $\boldsymbol{T}$ with non-zero probability. Moreover, they provide no method to verify the resulting scheme is indeed strongly secure except for the brute-force approach of checking whether all the linear codes $C^A(\Sigma_{\boldsymbol{T}})$ are MDS. Theorem 1 is preferable even to the construction of [12] in that it gives an explicit transformation while [12] needs to solve an optimization problem with exponentially many (in n) variables.

(3) Field Size

The field sizes q' required by [7], [12], the second method of [8], and Theorem 2 are independent of q. Thus, they can be applied to $\mathbb{F}_q$-linear ramp schemes Σ without taking a field extension if q is sufficiently large. For example, since we have $K = 2^{O(L2^n)}$, Theorem 2 can transform an $\mathbb{F}_q$-linear scheme with $q = 2^{\Omega(L2^n)}$ into a strongly secure one without increasing the share size. The construction of [12] requires $q' \geq L + m^*$, where m^* is the total number of shares distributed to participants. Since m^* is obtained only after solving the associated optimization problem, we have no explicit upper bound on m^*. On the other hand, the field size required by Theorem 1 is q^{2L}, which means that we must take a field extension of degree $2L$. It is smaller than the first method of [8], which needs the degree to be $O(L^2)$.

4.4 Example

We provide a simple and concrete example of our constructions to demonstrate how a ramp scheme is converted into a strongly secure one with the help of a network code.

Assume that the set P of $n = 7$ participants is divided into two parts P_1, P_2 with $|P_1| = 4$ and $|P_2| = 3$. Consider the following four conditions on a subset $A \subseteq P$:

(C-1) $|A \cap P_2| \geq 3$;
(C-2) $|A \cap P_1| \geq 1$ and $|A \cap P_2| \geq 2$;
(C-3) $|A \cap P_1| \geq 2$ and $|A \cap P_2| \geq 1$;
(C-4) $|A \cap P_1| \geq 4$.

Let $L = 3$ and $\mathcal{A}_L = (\Gamma_0, \Gamma_1, \Gamma_2, \Gamma_3)$ be a 3-level access structure such that Γ_j consists of all subsets satisfying exactly j out of the above four conditions.

Let $q = 11$. A possible construction of a ramp secret sharing scheme Σ realizing $\mathcal{A}_L$ is as follows: Given a secret $(s_1, s_2, s_3) \in \mathbb{F}_q^3$, set $(t^{(1)}, t^{(2)}, t^{(3)}, t^{(4)}) = (s_1, s_1+s_2, s_2+s_3, s_3)$ and share each $t^{(i)}$ in such a way that any set of participants satisfying the condition (C-i) reconstructs $t^{(i)}$ and others learn no information. The latter procedure can be done by splitting $t^{(i)}$ into two random elements a_1, a_2 as $t^{(i)} = a_1 + a_2$ and sharing each a_j among participants in P_j with the threshold specified by (C-i).

Observe that the above ramp scheme Σ is not strongly secure. Indeed, for any set A satisfying the condition (C-2) only, the strong security requires that shares held by players in A reveal no information on every set of two sub-secrets since $A \in \Gamma_1$. However, players in A can reconstruct $t^{(2)} = s_1 + s_2$ and hence $H(S_1S_2|V_A) = (1/2)H(S_1S_2) < H(S_1S_2)$.

To make the naive scheme strongly secure, we first determine generator matrices $\boldsymbol{G}^A$ of $C^A(\Sigma)$ for all $A \in \Gamma_1 \cup \Gamma_2$. Take a set A satisfying the conditions (C-1) and (C-2) as an example. Then, players in A learn $t^{(1)} = s_1$ and $t^{(2)} = s_1 + s_2$, and hence $C^A(\Sigma)$ is generated by

$$\boldsymbol{G}^A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}.$$

In general, we see that if $A \in \Gamma_j$, the rows of a generator matrix $\boldsymbol{G}^A$ are some j rows of a matrix

$$\boldsymbol{M} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}.$$

In view of Problem 1, we can make Σ strongly secure if we find a 3-by-3 matrix $\boldsymbol{T}$ such that every minor of $\boldsymbol{MT}$ of order 1 or order 2 is non-zero. A network code $\mathcal{N}$ related to Σ is the same as the one shown in [16, Fig. 1] except that (m_1, m_2, m_3) is replaced with (s_1, s_2, s_3). Indeed, it can be seen that a vector $\boldsymbol{W}_e$ associated with every edge e is one of the rows of $\boldsymbol{M}$.

If we move to an extension field $\mathbb{F}_{q^6}$, we have a $[6,3]$-linear MRD code over $\mathbb{F}_{q^6}$ with generator matrix $\boldsymbol{G} = \begin{bmatrix} \boldsymbol{G}_1 & \boldsymbol{G}_2 \end{bmatrix} = (g_j^{q^{i-1}})_{1 \leq i \leq 3, 1 \leq j \leq 6} \in \mathbb{F}_{q^6}^{3\times 6}$, where the g_j's form a basis of $\mathbb{F}_{q^6}$. Set $\boldsymbol{T}_1 := \boldsymbol{G}_1^{-1}\boldsymbol{G}_2$. The result of [15] shows that if $\boldsymbol{T}_1(s_1, s_2, s_3)^\top$ is sent as an input message in $\mathcal{N}$ instead of $(s_1, s_2, s_3)^\top$, then this new network code $\mathcal{N}_{\boldsymbol{T}_1}$ is strongly secure. Based on the connection shown in Sect. 3, by setting $\boldsymbol{T}_1(s_1, s_2, s_3)^\top$ as a secret, we can make Σ a strongly secure ramp scheme, which is indeed the statements of Theorem 1. Although the information ratio does not change, the share size increases by six times due to the field extension $\mathbb{F}_{q^6}/\mathbb{F}_q$.

In this example, we can also find $\boldsymbol{T}$ from matrices over $\mathbb{F}_q$ and hence do not need to increase the share size. As shown in [16, Fig. 4], if one inputs the matrix $\boldsymbol{M}$ associated with the network code $\mathcal{N}$ to the deterministic algorithm [16], it outputs the following matrix

$$\boldsymbol{T}_2 = \begin{bmatrix} 1 & 1 & 4 \\ 1 & 2 & 5 \\ 1 & 3 & 7 \end{bmatrix} \in \mathbb{F}_q^{3\times 3}.$$

Then, the transformed network code $\mathcal{N}_{\boldsymbol{T}_2}$, in which $\boldsymbol{T}_2(s_1, s_2, s_3)^\top$ is sent as an input message in $\mathcal{N}$, is strongly secure. Again, based on the connection in Sect. 3, we can obtain a strongly secure ramp scheme by setting $\boldsymbol{T}_2(s_1, s_2, s_3)^\top$ as a secret for Σ. We note that the bound on the field size given by Theorem 2 is a sufficient condition. As in this case, a desired matrix $\boldsymbol{T}$ can be found from ones over a smaller field depending on an initial ramp scheme.

5. Application to Multi-User SPIR

5.1 System Model

Let P be a set of n servers. Suppose that every server has a copy of a database $\boldsymbol{D} = (D_1, \ldots, D_m) \in \mathbb{F}_q^m$. Let Ψ be a monotonically decreasing family on P and suppose that a set of servers $B \in \Psi$ can collude. There are an arbitrary number of non-colluding users each of whom wants to retrieve L values $D_T := \{D_\tau : \tau \in T\}$ for a set $T \subseteq [m]$ of size L. Let

$\Phi_1 \supseteq \cdots \supseteq \Phi_M$ be a chain of M monotonically increasing families on P such that $\Phi_i \cap \Psi = \emptyset$ for all $i \in [M]$. Each user has a response pattern Φ_i for some $i \in [M]$, that is, he receives answers from servers in $A \in \Phi_i$ when computing data items. Our aim is to realize a scheme such that it serves as SPIR for (Φ_i, Ψ) between a user and servers (see Definition 3) if the user has a response pattern Φ_i.

5.2 Formalization of Dynamic SPIR

We first recall the definition of SPIR [10].

Definition 3 ([10]). *Let Φ, Ψ be monotonically increasing and decreasing families on P, respectively, such that $\Phi \cap \Psi = \emptyset$. An L-message SPIR (L-SPIR) scheme Π for (Φ, Ψ) is a tuple of four algorithms $\Pi = (\mathsf{Setup}, \mathsf{Que}, \mathsf{Ans}, \mathsf{Rec})$, where:*

- Setup *takes no input and outputs correlated randomness $(r_1, \ldots, r_n)$;*
- Que *takes as input a set $T \subseteq [m]$ of size L and outputs a query vector $(q_1, \ldots, q_n)$;*
- Ans *takes as input $i \in P$, a query q_i, a database $\boldsymbol{D}$ and a random string r_i, and outputs an answer a_i;*
- Rec *takes as input $A \in \Phi$ and answers $(a_i)_{i \in A}$, and outputs a set of values $\widetilde{D}$*[†]*;*

satisfying the following properties:

- ***Correctness.*** *For any database $\boldsymbol{D} \in \mathbb{F}_q^m$, any set $T \subseteq [m]$ of size L, any $(r_1, \ldots, r_n) \leftarrow \mathsf{Setup}()$, any $(q_1, \ldots, q_n) \leftarrow \mathsf{Que}(T)$ and any $A \in \Phi$, it holds that $\mathsf{Rec}(A, (\mathsf{Ans}(i, q_i, \boldsymbol{D}, r_i))_{i \in A}) = D_T$;*
- ***User Privacy.*** *For any $\boldsymbol{D} \in \mathbb{F}_q^m$, any set $T, T' \subseteq [m]$ of size L and any $B \in \Psi$, the distributions $(q_i)_{i \in B}$ and $(q'_i)_{i \in B}$ are perfectly identical, where $(q_1, \ldots, q_n) \leftarrow \mathsf{Que}(T)$ and $(q'_1, \ldots, q'_n) \leftarrow \mathsf{Que}(T')$;*
- ***Database Privacy.*** *For any set $T \subseteq [m]$ of size L, any $\boldsymbol{D}, \boldsymbol{D}' \in \mathbb{F}_q^m$ such that $D_T = D'_T$, and any $(q_1, \ldots, q_n) \leftarrow \mathsf{Que}(T)$, the distributions $(\mathsf{Ans}(i, q_i, \boldsymbol{D}, r_i))_{i \in P}$ and $(\mathsf{Ans}(i, q_i, \boldsymbol{D}', r_i))_{i \in P}$ are perfectly identical, where $(r_1, \ldots, r_n) \leftarrow \mathsf{Setup}()$.*

The communication (resp. randomness) ratio is defined as $\mathsf{CC}(\Pi) = \sum_{i \in P} \ell_{\mathsf{Ans}(i,\cdot)}/(L \log q)$ (resp. $\mathsf{RC}(\Pi) = \ell_{\mathsf{Setup}}/(L \log q)$), where $\ell_{\mathsf{Ans}(i,\cdot)}$ (resp. ℓ_{Setup}) is the output length of $\mathsf{Ans}(i, \cdot)$ (resp. $\mathsf{Setup}()$).

Next, we formalize the notion of dynamic SPIR.

Definition 4 (Dynamic SPIR). *Let Ψ be a monotonically decreasing family on P. Let $\Phi_1 \supseteq \cdots \supseteq \Phi_M$ be a chain of M monotonically increasing families on P such that $\Phi_i \cap \Psi = \emptyset$ for all $i \in [M]$. A dynamic SPIR scheme Π for $\mathcal{F} = (\Phi_1, \ldots, \Phi_M; \Psi)$ is a tuple of four algorithms $\Pi = (\mathsf{Setup}, \mathsf{Que}, \mathsf{Ans}, \mathsf{Rec})$, where:*

- *The syntax is the same as Definition 3 except that Que and Rec additionally take as input an index $i \in [M]$;*

satisfying the following property:

- *For any $i \in [M]$,*
$$\Pi_i = (\mathsf{Setup}(), \mathsf{Que}(\cdot; i), \mathsf{Ans}, \mathsf{Rec}(\cdot; i))$$
is an L_i-SPIR scheme for (Φ_i, Ψ), where $L_i \in \mathbb{N}$.

The communication (resp. randomness) ratio is defined as $\mathsf{CC}(\Pi) = (\mathsf{CC}(\Pi_i))_{i \in [M]}$ (resp. $\mathsf{RC}(\Pi) = (\mathsf{RC}(\Pi_i))_{i \in [M]}$).

A dynamic SPIR scheme realizes SPIR between users with different response patterns and servers. In the setup, servers jointly generate $(r_i)_{i \in P} \leftarrow \mathsf{Setup}()$ and Server i stores r_i. A user with response pattern Φ_j generates $(q_i)_{i \in P} \leftarrow \mathsf{Que}(T; j)$ and sends q_i to Server i. In response to that, Server i returns $a_i = \mathsf{Ans}(i, q_i, \boldsymbol{D}, r_i)$. If the user receives answers from a set of servers $A \in \Phi_j$, he can compute $D_T = \mathsf{Rec}(A, (a_i)_{i \in A}; j)$. Since users are supposed to be non-colluding, servers may use the same correlated randomness for all users to protect database privacy.

5.3 Our Construction of Dynamic SPIR

We first show a technical property of strongly secure ramp schemes that facilitates the construction of dynamic SPIR.

Theorem 3. *Let Σ be a strongly secure $\mathbb{F}_q$-linear ramp secret sharing scheme with L-level access structure $\mathcal{A}_L = (\Gamma_j)_{0 \leq j \leq L}$ on P. Let Φ be a monotonically increasing family on P. Define $\alpha = \alpha_\Sigma(\Phi) := \max\{j : \Phi \subseteq \Gamma_j \cup \cdots \cup \Gamma_L\}$. Then, there exists an algorithm $\mathsf{Reconst}_\alpha$ such that $\mathsf{Reconst}_\alpha(A, (\boldsymbol{v}_i)_{i \in A}) = \boldsymbol{s}$ for any $A \in \Phi$, $\boldsymbol{s} \in \mathbb{F}_q^\alpha$ and $(\boldsymbol{v}_i)_{i \in P} \leftarrow \Sigma.\mathsf{Share}(\boldsymbol{s}, \boldsymbol{0}_{L-\alpha})$.*

Proof. The algorithm $\mathsf{Reconst}_\alpha$ is shown in Fig. 1. Let $A \in \Phi$, $\boldsymbol{s} \in \mathbb{F}_q^\alpha$ and $(\boldsymbol{v}_i)_{i \in P}$ be an output of $\Sigma.\mathsf{Share}(\boldsymbol{s}, \boldsymbol{0}_{L-\alpha})$. There exists a vector $\boldsymbol{\rho}$ such that $\boldsymbol{U}_{[L]}\boldsymbol{\rho}^\top = (\boldsymbol{s}, \boldsymbol{0}_{L-\alpha})^\top$ and $\boldsymbol{W}_i\boldsymbol{\rho}^\top = \boldsymbol{v}_i^\top$ for $i \in P$. Since Σ is strongly secure, the property (1) in Sect. 3.1 implies that every set of j column vectors of $\boldsymbol{G}^A$ is linearly independent. The rank of $\boldsymbol{G}_1$ obtained at Step 3 is α and hence there is at most one solution to the linear equation at Step 4. On the other hand, since $\boldsymbol{\Lambda}\boldsymbol{v}_A^\top = \boldsymbol{\Lambda}\boldsymbol{W}_A\boldsymbol{\rho}^\top = \boldsymbol{G}^A\boldsymbol{U}_{[L]}\boldsymbol{\rho}^\top = \boldsymbol{G}^A(\boldsymbol{s}, \boldsymbol{0}_{L-\alpha})^\top = \boldsymbol{G}_1\boldsymbol{s}^\top$, $\boldsymbol{s}$ is the unique solution to $\boldsymbol{G}_1\boldsymbol{x}^\top = \boldsymbol{\Lambda}\boldsymbol{v}_A^\top$. Therefore, the output

$\mathsf{Reconst}_\alpha$. Given a set $A \in \Phi$ and a tuple of shares $(\boldsymbol{v}_i)_{i \in A}$:

1. Let $j \geq \alpha$ be such that $A \in \Gamma_j$.
2. Compute a generator matrix $\boldsymbol{G}^A \in \mathbb{F}_q^{j \times L}$ of $C^A(\Sigma)$ and a matrix $\boldsymbol{\Lambda}$ such that $\boldsymbol{G}^A\boldsymbol{U}_{[L]} = \boldsymbol{\Lambda}\boldsymbol{W}_A$.
3. Let $\boldsymbol{G}_1 \in \mathbb{F}_q^{j \times \alpha}, \boldsymbol{G}_2 \in \mathbb{F}_q^{j \times (L-\alpha)}$ be such that $\boldsymbol{G}^A = [\boldsymbol{G}_1 \quad \boldsymbol{G}_2]$.
4. Output a solution $\boldsymbol{x} \in \mathbb{F}_q^\alpha$ to a linear equation $\boldsymbol{G}_1\boldsymbol{x}^\top = \boldsymbol{\Lambda}\boldsymbol{v}_A^\top$, where $\boldsymbol{v}_A$ is the vector obtained by concatenating $\boldsymbol{v}_i$ for $i \in A$.

Fig. 1 The algorithm $\mathsf{Reconst}_\alpha$.

[†] Rec is allowed to additionally take as input random strings for Que since the same user runs both of them. For simplicity, we avoid passing such strings explicitly from Que to Rec.

Setup. Output $(\boldsymbol{r}_i)_{i\in P} \leftarrow \Sigma.\mathsf{Share}(\boldsymbol{0}_L)$.
Que. Given $i \in [M]$ and a set $T = \{\tau_1, \ldots, \tau_\alpha\}$ of $\alpha = L_i$ indices:

1. Let $\begin{bmatrix} \boldsymbol{s}_1^\top & \cdots & \boldsymbol{s}_m^\top \end{bmatrix} = \begin{bmatrix} \boldsymbol{e}_{\tau_1}^\top & \cdots & \boldsymbol{e}_{\tau_\alpha}^\top \end{bmatrix}^\top \in \mathbb{F}_q^{\alpha\times m}$.
2. For each $j \in [m]$, compute $(\boldsymbol{v}_{ji})_{i\in P} \leftarrow \Sigma.\mathsf{Share}(\boldsymbol{s}_j, \boldsymbol{0}_{L-\alpha})$.
3. Output $\boldsymbol{q}_i = (\boldsymbol{v}_{1i}, \ldots, \boldsymbol{v}_{mi})$ for $i \in P$.

Ans. Given $i \in P$, a query $\boldsymbol{q}_i = (\boldsymbol{v}_{ji})_{j\in[m]}$, a database $\boldsymbol{D} = (D_j)_{j\in[m]} \in \mathbb{F}_q^m$ and a random string $\boldsymbol{r}_i$, output $\boldsymbol{a}_i = \sum_{j\in[m]} D_j \boldsymbol{v}_{ji} + \boldsymbol{r}_i$.
Rec. Given $i \in [M]$, $A \in \Phi_i$ and answers $(\boldsymbol{a}_i)_{i\in A}$, output $\widetilde{D} = \mathsf{Reconst}_\alpha(A, (\boldsymbol{a}_i)_{i\in A})$, where $\alpha = L_i$.

Fig. 2 A dynamic SPIR scheme based on a strongly secure ramp scheme.

of $\mathsf{Reconst}_\alpha$ is equal to the correct secret $\boldsymbol{s}$. □

Now, we present our construction of dynamic SPIR.

Theorem 4. *Let $\mathcal{A}_L = (\Gamma_j)_{0\le j\le L}$ be an L-level access structure. Let Ψ be a monotonically decreasing family and $\Phi_1 \supseteq \cdots \supseteq \Phi_M$ be a chain of monotonically increasing ones such that $\Psi \subseteq \Gamma_0$ and $\Phi_i \cap \Gamma_0 = \emptyset$ for all $i \in [M]$. If there exists a strongly secure $\mathbb{F}_q$-linear ramp scheme Σ realizing $\mathcal{A}_L$ with information ratio σ, there exists a dynamic SPIR scheme Π for $\mathcal{F} = (\Phi_1, \ldots, \Phi_M; \Psi)$ such that* $\mathsf{CC}(\Pi) = \mathsf{RC}(\Pi) = (L\sigma/\alpha_\Sigma(\Phi_i))_{i\in[M]}$.

Proof. Let $L_i = \alpha_\Sigma(\Phi_i)$ for any $i \in [M]$. Consider the dynamic SPIR scheme shown in Fig. 2. We show that $\Pi_i = (\mathsf{Setup}, \mathsf{Que}(\cdot; i), \mathsf{Ans}, \mathsf{Rec}(\cdot; i))$ is an L_i-SPIR scheme for (Φ_i, Ψ). Let $(\boldsymbol{U}_{[L]}, \boldsymbol{W}_P)$ be a pair of matrices associated with Σ, where $\boldsymbol{U}_\ell \in \mathbb{F}_q^{1\times e}$ for $\ell \in [L]$ and $\boldsymbol{W}_i \in \mathbb{F}_q^{d_i\times e}$ for $i \in P$. To see the correctness, let $(\boldsymbol{r}_i)_{i\in P}$ be an output of Setup. There is a vector $\boldsymbol{\rho}_0$ such that $\boldsymbol{U}_{[L]}\boldsymbol{\rho}_0^\top = \boldsymbol{0}_L$ and $\boldsymbol{W}_i\boldsymbol{\rho}_0^\top = \boldsymbol{r}_i^\top$ for $i \in P$. At Step 2 of Que, for each $j \in [m]$, there exists a vector $\boldsymbol{\rho}_j$ such that $\boldsymbol{U}_{[L]}\boldsymbol{\rho}_j^\top = (\boldsymbol{s}_j, \boldsymbol{0}_{L-\alpha})^\top$ and $\boldsymbol{W}_i\boldsymbol{\rho}_j^\top = \boldsymbol{v}_{ji}^\top$ for $i \in P$. In Ans, it holds that $\boldsymbol{a}_i^\top = \sum_j D_j \boldsymbol{W}_i \boldsymbol{\rho}_j^\top + \boldsymbol{W}_i\boldsymbol{\rho}_0^\top = \boldsymbol{W}_i\boldsymbol{\xi}^\top$, where $\boldsymbol{\xi} = \sum_j D_j\boldsymbol{\rho}_j^\top + \boldsymbol{\rho}_0$. Then, $(\boldsymbol{a}_i)_{i\in P}$ is a possible output of $\Sigma.\mathsf{Share}(D_{\tau_1}, \ldots, D_{\tau_\alpha}, \boldsymbol{0}_{L-\alpha})$ since

$$\boldsymbol{U}_{[L]}\boldsymbol{\xi}^\top = \begin{bmatrix} \sum_j D_j \boldsymbol{s}_j^\top \\ \boldsymbol{0}_{L-\alpha}^\top \end{bmatrix} = \begin{bmatrix} D_{\tau_1} & \cdots & D_{\tau_\alpha} & \boldsymbol{0}_{L-\alpha} \end{bmatrix}^\top .$$

The correctness follows since $\mathsf{Reconst}_\alpha$ correctly recovers $\boldsymbol{s} \in \mathbb{F}_q^\alpha$ from $(\boldsymbol{v}_i)_{i\in A}$ if $A \in \Phi$ and $(\boldsymbol{v}_i)_{i\in P} \leftarrow \Sigma.\mathsf{Share}(\boldsymbol{s}, \boldsymbol{0}_{L-\alpha})$. The user privacy follows from the privacy of Σ since a tuple of shares $(\boldsymbol{q}_i)_{i\in B}$ reveals nothing on secrets $\boldsymbol{s}_j$, $j \in [m]$ if $B \in \Psi \subseteq \Gamma_0$.

To see the database privacy, let $\boldsymbol{D}, \boldsymbol{D}'$ be such that $D_T = D'_T$. Let $\boldsymbol{q}_i = (\boldsymbol{v}_{ji})_{j\in[m]}$ be a query sent to $i \in P$. For each $j \in [m]$, there exists a vector $\boldsymbol{\rho}_j$ such that $\boldsymbol{U}_{[L]}\boldsymbol{\rho}_j^\top = (\boldsymbol{s}_j, \boldsymbol{0}_{L-\alpha})^\top$ and $\boldsymbol{W}_i\boldsymbol{\rho}_j^\top = \boldsymbol{v}_{ji}^\top$ for $i \in P$. Note that the distribution of outputs of Setup is the same as that of $(\boldsymbol{W}_i\boldsymbol{\rho}_0^\top)_{i\in P}$ where $\boldsymbol{\rho}_0$ is randomly chosen from $V := \{\boldsymbol{\rho} \in \mathbb{F}_q^e : \boldsymbol{U}_{[L]}\boldsymbol{\rho}^\top = \boldsymbol{0}_L\}$. It is sufficient to show a bijection $\theta : V \to V$ such that $(\mathsf{Ans}(i, \boldsymbol{q}_i, \boldsymbol{D}', \boldsymbol{r}'_i))_{i\in P} = (\mathsf{Ans}(i, \boldsymbol{q}_i, \boldsymbol{D}, \boldsymbol{r}_i))_{i\in P}$ for any $\boldsymbol{\rho} \in V$, where $\boldsymbol{r}_i^\top = \boldsymbol{W}_i\boldsymbol{\rho}^\top$ and $(\boldsymbol{r}'_i)^\top = \boldsymbol{W}_i\theta(\boldsymbol{\rho})^\top$. Set $\boldsymbol{\zeta} = \sum_{j\in[m]}(D_j - D'_j)\boldsymbol{\rho}_j$ and define $\theta(\boldsymbol{\rho}) = \boldsymbol{\rho} + \boldsymbol{\zeta}$. Since $D_T = D'_T$ and $\boldsymbol{s}_j = \boldsymbol{0}_\alpha$ for $j \notin T$, we have that $\boldsymbol{U}_{[L]}\boldsymbol{\zeta}^\top = \sum_{j\notin T}(D_j - D'_j)(\boldsymbol{s}_j, \boldsymbol{0}_{L-\alpha})^\top = \boldsymbol{0}_L$ and hence $\boldsymbol{\zeta} \in V$. Since V is a linear space, θ is indeed a bijection. It also holds that $\mathsf{Ans}(i, \boldsymbol{q}_i, \boldsymbol{D}', \boldsymbol{r}'_i) - \mathsf{Ans}(i, \boldsymbol{q}_i, \boldsymbol{D}, \boldsymbol{r}_i) = \sum_{j\in[m]}(D'_j - D_j)\boldsymbol{W}_i\boldsymbol{\rho}_j^\top + \boldsymbol{W}_i\boldsymbol{\zeta}^\top = \boldsymbol{0}$.

Finally, since $\sum_{j\in P} \ell_{\mathsf{Ans}(j,\cdot)} = \ell_{\mathsf{Setup}} = L\sigma \log q$, we have that $\mathsf{CC}(\Pi_i) = \mathsf{RC}(\Pi_i) = L\sigma/\alpha_\Sigma(\Phi_i)$ for $i \in [M]$. □

Table 2 Comparison of dynamic SPIR schemes for $\mathcal{F} = (\Phi_1, \ldots, \Phi_M; \Psi)$ based on Solutions I, II [11] and ours (Corollary 1). We show their communication and randomness ratios when a user chooses (Φ_i, Ψ) for $1 \le i \le M$.

Construction	Communication	Randomness
Solution I [11]	$\lambda_{q,L}(\Phi_1, \Psi)$	$\lambda_{q,L}(\Phi_1, \Psi)$
Solution II [11]	$\lambda_{q,L}(\Phi_i, \Psi)$	$\sum_{j=1}^M \lambda_{q,L}(\Phi_j, \Psi)$
Ours (Corollary 1)	$\dfrac{L\lambda_{q,L}(\Phi_M, \Psi)}{\alpha_\Sigma(\Phi_i)}$	$\dfrac{L\lambda_{q,L}(\Phi_M, \Psi)}{\alpha_\Sigma(\Phi_i)}$

Since any linear ramp scheme can be made strongly secure without increasing the information ratio, we have the following corollary.

Corollary 1. *Using the notations in Theorem 4, if there exists an $\mathbb{F}_q$-linear ramp scheme realizing $\mathcal{A}_L$ with information ratio σ, there exists a dynamic SPIR scheme Π for $\mathcal{F} = (\Phi_1, \ldots, \Phi_M; \Psi)$ such that* $\mathsf{CC}(\Pi) = \mathsf{RC}(\Pi) = (L\sigma/\alpha_\Sigma(\Phi_i))_{i\in[M]}$.

5.4 Comparison

We show the advantage of our dynamic SPIR scheme over two constructions that are naturally implied by the SPIR scheme in [11] (Table 2). Let Φ (resp. Ψ) be a monotonically increasing (resp. decreasing) family. We define $\lambda_{q,L}(\Phi, \Psi)$ as the minimum information ratio of $\mathbb{F}_q$-linear ramp schemes with L-level access structure $\mathcal{A}_L = (\Gamma_j)_{0\le j\le L}$ such that $\Phi = \Gamma_L$ and $\Psi = \Gamma_0$. According to [11], there exists an L-SPIR scheme Π for (Φ, Ψ) such that $\mathsf{CC}(\Pi) = \mathsf{RC}(\Pi) = \lambda_{q,L}(\Phi, \Psi)$. Let $\Phi_1 \supseteq \cdots \supseteq \Phi_M$ be a chain of M monotonically increasing families and Ψ be a monotonically decreasing family of subsets of P such that $\Phi_i \cap \Psi = \emptyset$ for all $i \in [M]$. Note that $\lambda_{q,L}(\Phi_1, \Psi) \ge \lambda_{q,L}(\Phi_2, \Psi) \ge \cdots \ge \lambda_{q,L}(\Phi_M, \Psi)$. We first recall two naive solutions based on [11], which we described in Sect. 1.1.2.

Solution I: To build an SPIR scheme Π_0 for (Φ_1, Ψ) and use it regardless of a user's choice (Φ_i, Ψ).

Since $\Phi_i \subseteq \Phi_1$, one obtains a dynamic SPIR scheme $\Pi^{(1)}$ for $\mathcal{F} = (\Phi_1, \ldots, \Phi_M; \Psi)$ such that $\mathsf{CC}(\Pi^{(1)}) = \mathsf{RC}(\Pi^{(1)}) = (\lambda_{q,L}(\Phi_1, \Psi))_{1\le i\le M}$. However, always assuming the worst case (Φ_1, Ψ) results in an unnecessarily high communication ratio $\lambda_{q,L}(\Phi_1, \Psi)$ when a user has a response pattern Φ_M.

Solution II: To build M SPIR schemes Π_i, each for (Φ_i, Ψ), and use Π_i if a user's response pattern is (Φ_i, Ψ).

The resulting scheme is a dynamic SPIR scheme $\Pi^{(2)}$ for $\mathcal{F}$

such that $\mathsf{CC}(\Pi^{(2)}) = (\lambda_{q,L}(\Phi_i, \Psi))_{1\le i\le M}$. However, since the Π_i's are possibly different schemes, servers must store M shares of zero as correlated randomness. That is, $\mathsf{RC}(\Pi^{(2)}) = (\sum_{j=1}^{M} \lambda_{q,L}(\Phi_j, \Psi))_{1\le i\le M}$.

Our solution is as follows. We build a ramp scheme Σ realizing $\mathscr{A}_L = (\Gamma_j)_{0\le j\le L}$ such that $\Gamma_0 = \Psi$ and $\Gamma_L = \Phi_M$. Corollary 1 implies a dynamic SPIR scheme $\Pi^{(3)}$ for $\mathscr{F}$ such that $\mathsf{CC}(\Pi^{(3)}) = \mathsf{RC}(\Pi^{(3)}) = (L\lambda_{q,L}(\Phi_M, \Psi)/\alpha_\Sigma(\Phi_i))_{1\le i\le M}$. Our solution is advantageous when a user has a response pattern Φ_M. Since $\alpha_\Sigma(\Phi_M) = L$, the communication and randomness ratios are both $\lambda_{q,L}(\Phi_M, \Psi)$. Those of Solution I are both $\lambda_{q,L}(\Phi_1, \Psi)$, which is generally greater than $\lambda_{q,L}(\Phi_M, \Psi)$. The randomness ratio of Solution II is $\sum_{j=1}^{M} \lambda_{q,L}(\Phi_j, \Psi)$, which is at least M times larger than $\lambda_{q,L}(\Phi_M, \Psi)$.

References

[1] R. Eriguchi, N. Kunihiro, and K. Nuida, "A linear algebraic approach to strongly secure ramp secret sharing for general access structures," 2020 Int. Symp. Inf. Theory Appl. (ISITA), pp.427–431, 2020.

[2] G.R. Blakley, "Safeguarding cryptographic keys," 1979 Int. Workshop Managing Req. Knowledge (MARK), pp.313–318, 1979.

[3] A. Shamir, "How to share a secret," Commun. ACM, vol.22, no.11, pp.612–613, 1979.

[4] R.J. McEliece and D.V. Sarwate, "On sharing secrets and Reed-Solomon codes," Commun. ACM, vol.24, no.9, pp.583–584, 1981.

[5] G.R. Blakley and C. Meadows, "Security of ramp schemes," Adv. Cryptol. – CRYPTO '84, pp.242–268, 1985.

[6] H. Yamamoto, "Secret sharing system using (k, L, n) threshold scheme," Electron. Commun. Japan (Part I: Commun.), vol.69, no.9, pp.46–54, 1986.

[7] M. Iwamoto and H. Yamamoto, "Strongly secure ramp secret sharing schemes for general access structures," Inf. Proc. Lett., vol.97, no.2, pp.52–57, 2006.

[8] R. Eriguchi and N. Kunihiro, "Strong security of linear ramp secret sharing schemes with general access structures," Inf. Proc. Lett., vol.164, p.106018, 2020.

[9] B. Chor, O. Goldreich, E. Kushilevitz, and M. Sudan, "Private information retrieval," J. ACM, vol.45, no.6, pp.965–982, 1998.

[10] Y. Gertner, Y. Ishai, E. Kushilevitz, and T. Malkin, "Protecting data privacy in private information retrieval schemes," J. Comput. Syst. Sci., vol.60, no.3, pp.592–629, 2000.

[11] S. Song and M. Hayashi, "Equivalence of non-perfect secret sharing and symmetric private information retrieval with general access structure," 2021 IEEE Int. Symp. Inf. Theory (ISIT), pp.982–987, 2021.

[12] R. Matsumoto, "Optimal multiple assignment scheme for strongly secure ramp secret sharing schemes with general access structures," IEICE Commun. Express, vol.4, no.11, pp.317–320, 2015.

[13] D. Silva and F.R. Kschischang, "Universal secure network coding via rank-metric codes," IEEE Trans. Inf. Theory, vol.57, no.2, pp.1124–1135, 2011.

[14] K. Harada and H. Yamamoto, "Strongly secure linear network coding," IEICE Trans. Fundamentals, vol.E91-A, no.10, pp.2720–2728, Oct. 2008.

[15] J. Kurihara, T. Uyematsu, and R. Matsumoto, "Explicit construction of universal strongly secure network coding via MRD codes," 2012 IEEE Int. Symp. Inf. Theory (ISIT), pp.1483–1487, 2012.

[16] K. Kurosawa, H. Ohta, and K. Kakuta, "How to make a linear network code (strongly) secure," Des. Codes Cryptogr., vol.82, no.3, pp.559–582, 2017.

[17] M. Nishiara and K. Takizawa, "Strongly secure secret sharing scheme with ramp threshold based on Shamir's polynomial interpolation scheme," IEICE Trans. Fundamentals (Japanese Edition), vol.J92-A, no.12, pp.1009–1013, Dec. 2009.

[18] U. Martínez-Peñas, "Communication efficient and strongly secure secret sharing schemes based on algebraic geometry codes," IEEE Trans. Inf. Theory, vol.64, no.6, pp.4191–4206, 2018.

[19] M. Iwamoto, H. Yamamoto, and H. Ogawa, "Optimal multiple assignments based on integer programming in secret sharing schemes with general access structures," IEICE Trans. Fundamentals, vol.E90-A, no.1, pp.101–112, Jan. 2007.

[20] S. Li and M. Gastpar, "Single-server multi-user private information retrieval with side information," 2018 IEEE Int. Symp. Inf. Theory (ISIT), pp.1954–1958, 2018.

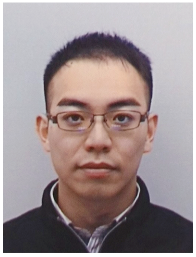
[21] W. Barnhart and Z. Tian, "The capacity of multi-user private information retrieval for computationally limited databases," 2020 IEEE Annu. Ubiquitous Comput. Electron. Mobile Commun. Conf. (UEMCON), pp.0759–0763, 2020.

[22] X. Yao, N. Liu, and W. Kang, "The capacity of private information retrieval under arbitrary collusion patterns for replicated databases," IEEE Trans. Inf. Theory, vol.67, no.10, pp.6841–6855, 2021.

[23] K. Kurosawa, K. Okada, K. Sakano, W. Ogata, and S. Tsujii, "Nonperfect secret sharing schemes and matroids," Adv. Cryptol. – EUROCRYPT '93, pp.126–141, 1994.

[24] O. Farràs, T.B. Hansen, T. Kaced, and C. Padró, "On the information ratio of non-perfect secret sharing schemes," Algorithmica, vol.79, no.4, pp.987–1013, 2017.

[25] E.M. Gabidulin, "Theory of codes with maximum rank distance," Prob. Inf. Transmission, vol.21, no.1, pp.1–12, 1985.



Reo Eriguchi received his B.E. in mathematical engineering and information physics and M.E. in science from The University of Tokyo in 2018 and 2020, respectively. He was a research assistant at National Institute of Advanced Industrial Science and Technology (AIST) from 2020 to 2021. He is a doctoral course student at The University of Tokyo.

Noboru Kunihiro received his B.E., M.E. and Ph.D. in mathematical engineering and information physics from The University of Tokyo in 1994, 1996 and 2001, respectively. He has been a professor of University of Tsukuba since 2019. He was a researcher of NTT Communication Science Laboratories from 1996 to 2002. He was an associate professor of the University of Electro-Communications from 2002 to 2008. He was an associate professor of The University of Tokyo from 2008 to 2019. His research interest includes cryptography and information security.

Koji Nuida received his Ph.D. (Mathematical Sciences) from The University of Tokyo in 2006. He was a researcher at National Institute of Advanced Industrial Science and Technology (AIST) from 2006 to 2018, an associate professor at The University of Tokyo from 2018 to 2021, and has been a professor at Kyushu University since 2021. His research interest includes mathematical cryptography, group theory, and combinatorics.