IEEE Transactions on Quantum Engineering

Received 30 July 2024; revised 17 December 2024; accepted 13 January 2025; date of publication 17 January 2025; date of current version 4 February 2025.

Digital Object Identifier 10.1109/TQE.2025.3530939

Advance Sharing Procedures for the Ramp Quantum Secret Sharing Schemes With the Highest Coding Rate

RYUTAROH MATSUMOTO (Member, IEEE)

Department of Information and Communications Engineering, Institute of Science Tokyo, Tokyo 152-8550, Japan

Corresponding author: Ryutaroh Matsumoto (e-mail: ryutaroh@ict.e.titech.ac.jp)

This work was supported in part by the Japan Society for the Promotion of Science under Grant 23K10980.

ABSTRACT In some quantum secret sharing schemes, it is known that some shares can be distributed to participants before a secret is given to the dealer. However, it is unclear whether some shares can be distributed before a secret is given in the ramp quantum secret sharing schemes with the highest coding rate. This article proposes procedures to distribute some shares before a secret is given in those schemes. The new procedures enhance the applicability of the secret sharing schemes to wider scenarios as some participants can be unavailable when the dealer obtains the quantum secret. Then, it is proved that our new encoding procedures retain the correspondences between quantum secrets and quantum shares in the original schemes, which ensures that the highest coding rates of the original schemes are also retained.

INDEX TERMS Advance sharing, quantum secret sharing, ramp secret sharing.

I. INTRODUCTION

The study of quantum information processing has gained much attention recently. One reason is the increase in the size of quantum computers [1]. The storage and communication of quantum information are still difficult experimentally, but they will probably become easier and less expensive in the future. Classical secret sharing, in which secrets and shares are both classical information, is nowadays used in practice, for example, in distributed storage systems. In a distributed storage system [2], data are stored in multiple storages, which increases the risk of data leakage. Secret sharing schemes decrease that risk with multiple storages. It is likely that quantum secret sharing schemes play similar roles in the future quantum information era.

This article considers sharing a quantum secret by quantum shares. It is assumed that there are no interactions among the dealer and the participants, except for the distribution of quantum shares from the dealer to the participants. Such a problem formulation was initiated by Cleve et al. [3] and Gottesman [4] and is the most natural quantum counterpart of the classical secret sharing considered by Shamir [5] and Blakley [6].

The coding rate is an important parameter in secret sharing schemes. It is defined as the ratio of the secret size to the average share size [3], [4], [7]. Higher coding rates are desirable. Another important property of secret sharing schemes is the access structure, which consists of three families of qualified sets, forbidden sets, and intermediate sets [7]. A set S of shares is called qualified (respectively, forbidden) if S allows the reconstruction of the secret (respectively, has no information about the secret). A set S of shares is called intermediate if it is neither qualified nor forbidden. If a secret sharing scheme has no intermediate set, it is called perfect. The coding rate cannot be greater than 1 if it is perfect [4]. Ogawa et al. [7] proposed ramp quantum secret sharing schemes, which enable coding rates greater than 1, at the cost of allowing intermediate sets. This article considers a q-dimensional quantum system $\mathcal{H}_q$ and calls it a qudit, where q is a prime power. A (k, L, n) ramp quantum secret sharing scheme encodes L-qudit quantum secret into n shares, each of which is 1 qudit in $\mathcal{H}_q$. The parameter k decides the access structure mentioned earlier, as follows. In a (k, L, n) scheme, a set S is qualified if $|S| \geq k$, forbidden if $|S| \leq k - L$, and intermediate otherwise (i.e., $k - L + 1 \leq |S| \leq k - 1$). Among (k, L, n) schemes, Ogawa et al.'s one has the highest possible coding rate L, and first, Ogawa et al.'s ramp quantum secret sharing is considered in Section II. The scheme by Cleve et al. [3] is a special case of Ogawa et al.'s scheme corresponding to the case $L = 1$.

As mentioned before, an intermediate set has nonzero information about the secret in a ramp scheme. In the classical secret sharing scheme, when the secret $\vec{s} = (s_1, \ldots, s_L)$,

Iwamoto and Yamamoto [8] showed an explicit example of ramp schemes, in which a component s_i in the secret can be reconstructed from an intermediate set S. In order to prevent such information leakage, Yamamoto [9] defined the strong security for the (k, L, n) classical ramp secret sharing scheme, in which any set S of shares has no information about part $(s_i : i \in T)$ of the secret if $|S| + |T| \leq k$. In the context of ramp quantum secret sharing, Zhang and Matsumoto [10] showed an explicit example from Ogawa et al.'s [7] scheme in which an intermediate set leaks part of the quantum secret similarly to the classical case in this paragraph. They also introduced a strong security definition into ramp quantum secret sharing and explicitly constructed a (k, L, n) strongly secure ramp quantum secret sharing scheme whose coding rate L is as high as Ogawa et al.'s scheme [7]. On the other hand, the Zhang–Matsumoto scheme has a more stringent condition on the number n of participants, that is, $n \leq q - L$, while Ogawa et al.'s scheme has a milder condition $n \leq q - 1$. The condition $n \leq q - 1$ also exists in Shamir's scheme [5], [6], but in the classical case, q can be made almost arbitrarily large. On the other hand, because the quantum system $\mathcal{H}_q$ cannot be chosen freely, the symbol size q cannot be adjusted in the quantum case as easily as the classical case. Therefore, both Ogawa et al.'s scheme and Zhang–Matsumoto scheme are practically useful depending on applications.

It is sometimes convenient to distribute shares before a secret is given to the dealer. One example of such situations was discussed in [11], which considered sharing a classical secret by quantum shares. Such distribution of shares before a given secret is named "advance sharing" [11]. Advance sharing is a trivial problem when both secret and shares are classical. For example, encoding 1-bit secret s into two shares $(x, s + x)$ provides a (1,2) perfect secret sharing scheme, and the first share x is clearly advance shareable, where x is a random bit. Advance sharing enhances the applicability of secret sharing schemes to wider scenarios.

On the other hand, when secrets are quantum, it is nontrivial to realize advance sharing. This article focuses on the case of quantum secrets. The first quantum advance sharing was realized in [12], which enabled advance sharing for some specific schemes. On the other hand, any quantum error-correcting code and its erasure decoding algorithm can be used as a quantum secret sharing scheme [3], [4], and Shibata and Matsumoto [13] clarified how to realize advance sharing with a quantum secret sharing scheme constructed from a p-adic quantum stabilizer code, where p is a prime number. Based on [13], Masumori and Matsumoto [14] showed how to realize advance sharing with a limited special case of Ogawa et al.'s scheme [7], where the dimension q of $\mathcal{H}_q$ was restricted to a prime number. Because the general method [13] for advance sharing cannot handle stabilizer codes over $\mathcal{H}_q$ with nonprime q, the previous proposal [14] of advance sharing for Ogawa et al.'s scheme [7] cannot be immediately extended to the general case of Ogawa et al.'s scheme [7].

When advance sharing for the strongly secure scheme [10] is considered, another limitation of [13] appears. The strong security property in [10] is realized by a careful correspondence between quantum secrets and quantum shares. On the other hand, the general method [13] for advance sharing destroys the correspondence between quantum secrets and quantum shares when it is applied to a ramp quantum secret sharing scheme. The general method [13] seems almost impossible to be applied for realizing advance sharing with the strongly secure scheme [10].

This article proposes new encoding procedures of quantum secrets into quantum shares for realizing advance sharing with Ogawa et al.'s scheme [7] and Zhang–Matsumoto scheme [10]. The new procedures enhance the applicability of the scheme proposed in [7] and [10] to wider scenarios in which some participants are unavailable when the dealer obtains quantum secrets to be shared. Both procedures retain the correspondence between quantum secrets and quantum shares in the original schemes. Therefore, all properties in the original schemes, such as coding rates, access structures, strong security, etc., remain the same as the originals. In particular, the highest coding rates are retained from the original schemes [7], [10]. The proposed new encoding procedures add extra useful functionalities to the original ramp quantum schemes [7], [10]. The differences among the original schemes [7], [10] and the proposals are summarized in Table I.

The rest of this article is organized as follows. In Section II, necessary contents from [7] are reviewed, a new encoding procedure is given for [7], and it is proven that the correspondence between secrets and shares is retained from [7]. Section III has a similar structure to Section II. In Section III, [10] is reviewed, a new encoding procedure for [10] is proposed, and it is proved that the same correspondence between secrets and shares is retained. In Sections II and III, illustrating examples of the original and the proposed encoding are included. Finally, Section IV concludes this article and gives future research agenda.

II. ADVANCE SHARING WITH THE QUANTUM RAMP SECRET SHARING SCHEME IN [7]

A. SHORT REVIEW OF QUANTUM SECRET SHARING

In this section, the quantum secret sharing considered in this article and its security model of secret sharing schemes are briefly described. In short, it is exactly the same as in [3] and [7]. When both secret and shares are classical information, this model is equivalent to the Shamir–Blakley scheme [15].

It is always assumed that there are n participants and each participant receives one share from the dealer. The entire set of shares/participants is denoted by $\{1, \ldots, n\}$. Therefore, any subset $A \subset \{1, \ldots, n\}$ corresponds to some set of shares/participants.

Let q be a prime power, $\mathbf{F}_q$ be the finite field with q elements, and $\{|i\rangle : i \in \mathbf{F}_q\}$ be an orthonormal basis of $\mathcal{H}_q$. For

IEEE Transactions on Quantum Engineering

TABLE I. Comparisons of the Original and the Proposed Encoding Procedures

	Ogawa et al. [7]	Zhang-Matsumoto [10]	Section II	Section III
Dimension of a quantum share	q	q	q	q
Number of symbols in quantum secrets	L	L	L	L
Maximum number of participants	$q-1$	$q-L$	$q-1$	$q-L$
Coding rate	L	L	L	L
Minimum number of participants to reconstruct secrets	k	k	k	k
Maximum number of participants with no information about secrets	$k-L$	$k-L$	$k-L$	$k-L$
Strong security	No	Yes	No	Yes
Maximum number of shares distributed in advance	0	0	$k-L$	$k-L$

$\vec{s}=(s_1,\ldots,s_L)\in\mathbf{F}_q^L$, one has

$$|\vec{s}\rangle = |s_1\rangle\otimes\cdots\otimes|s_L\rangle\in\mathcal{H}_q^{\otimes L}.$$

The dealer encodes the quantum secret $|\vec{s}\rangle$ (or a linear combination of $|\vec{s}\rangle$) into some pure state $|\varphi\rangle\in\mathcal{H}_q^{\otimes n}$. The dealer distributes each qudit in $|\varphi\rangle$ to each participant. Observe that no measurement, classical communications, or teleportation of quantum states are involved here, in contrast to [16]. Also, observe that the purpose and the procedure are different from those in quantum secure direct communication (QSDC) [17]. There seems no explicit relationship between the QSDC and the quantum secret sharing considered here.

A set $A\subset\{1,\ldots,n\}$ is said to be qualified if $|\vec{s}\rangle$ can be reconstructed from $\mathrm{Tr}_{\overline{A}}[|\varphi\rangle\langle\varphi|]$, said to be forbidden if $\mathrm{Tr}_{\overline{A}}[|\varphi\rangle\langle\varphi|]$ is independent of $|\vec{s}\rangle$, and said to be intermediate if A is neither qualified nor forbidden [7], where $\mathrm{Tr}_{\overline{A}}$ denotes the partial trace over $\overline{A}=\{1,\ldots,n\}\setminus A$. As mentioned in Section I, a quantum secret sharing scheme is said to be a ramp scheme if there is no intermediate set.

In Sections II-E and III-D, it will be shown that our proposed encoding procedures retain the correspondences between quantum secrets and quantum shares from [7] and [10]. This means that qualified sets and forbidden sets remain the same as in [7] and [10].

More importantly, since the correspondences between secrets and shares are the same as in [7] and [10], new encoding procedures are as much secure as the original ones under any security models and assumptions, and any new security argument is unnecessary unless a security property not considered in [7] and [10] is required.

Although cheating participants can be considered among legitimate ones and adversaries outside of legitimate participants [18], [19], these scenarios are not considered. Approximate quantum secret sharing [20] is not considered either, as it is not included in the original encoding procedures [7], [10]. However, since those other scenarios are also important, advance sharing in them should also be investigated in future.

The standard metrics for evaluating secret sharing schemes are coding rates and access structures [7], and sometimes the strong security [9], [10]. The proposed encoding procedures retain those evaluation metrics from the original schemes [7], [10], and they enable advance sharing that enhances the applicability of secret sharing schemes to wider scenarios.

B. OGAWA ET AL.'S SCHEME

Let n be the number of shares/participants, and it is assumed that $n\le q-1$. Let $\alpha_1,\ldots,\alpha_n$ be distinct nonzero[1] elements in $\mathbf{F}_q$. The construction of a (k,L,n) ramp quantum scheme will be reviewed. For $\vec{c}=(c_1,\ldots,c_k)\in\mathbf{F}_q^k$, the polynomial $f_{\vec{c}}(x)$ is defined as

$$f_{\vec{c}}(x)=c_1+c_2x+\cdots+c_kx^{k-1}. \tag{1}$$

A quantum secret $|\vec{s}\rangle\in\mathcal{H}_q^{\otimes L}$ is encoded to

$$\frac{1}{\sqrt{q^{k-L}}}\sum_{\vec{c}\in D(\vec{s})}|f_{\vec{c}}(\alpha_1)\rangle\otimes|f_{\vec{c}}(\alpha_2)\rangle\otimes\cdots\otimes|f_{\vec{c}}(\alpha_n)\rangle \tag{2}$$

where $D(\vec{s})$ is the set of vectors $\vec{c}\in\mathbf{F}_q^k$ whose leftmost L components are the same as those in $\vec{s}$. The quantum state in (2) consists of n qudits. The ith qudit in (2) is distributed to the ith participant.

C. EXAMPLE OF THE ORIGINAL ENCODING

Let $q=4$, $n=3$, $k=2$, $L=1$, and $\alpha_i=\alpha^i\in\mathbf{F}_4$, where α is a primitive element of $\mathbf{F}_4$. The standard encoding procedure in (2) encodes a quantum secret $|\vec{s}\rangle$ for $\vec{s}=(s)\in\mathbf{F}_4^1$ into $\frac{1}{\sqrt{4}}\sum_{\vec{c}\in D(\vec{s})}|f_{\vec{c}}(\alpha_1)\rangle\otimes|f_{\vec{c}}(\alpha_2)\rangle\otimes|f_{\vec{c}}(\alpha_3)\rangle=\frac{1}{\sqrt{4}}(|s,\ s,\ s\rangle+|s+\alpha,\ s+\alpha^2,\ s+1\rangle+|s+\alpha^2,\ s+1,\ s+\alpha\rangle+|s+1,\ s+\alpha,\ s+\alpha^2\rangle)$. As every qudit seems to depend on the quantum secret $|\vec{s}\rangle$, from the encoding procedure in [7], it seems unclear how one share is advance shareable.

D. PROPOSED ADVANCE SHARING PROCEDURE FOR [7]

This section proposes an advance sharing procedure, which retains the correspondence between a quantum secret and quantum shares given in (2), where the (k,L,n) quantum ramp scheme was considered.

An elementary lemma in linear algebra and polynomials is introduced as follows.

Lemma 1: Let $\mathcal{P}_m$ be the set of univariate polynomials $f(x)$ over $\mathbf{F}_q$ with $\deg(f)<m$. Consider the evaluation map $\mathrm{ev}(f)=(f(\alpha_1),\ldots,f(\alpha_n))$, where $\alpha_1,\ldots,\alpha_n$ are pairwise distinct as before, while $\alpha_1,\ldots,\alpha_n$ may contain $0\in\mathbf{F}_q$. The map ev is a linear map from $\mathcal{P}_m$ to $\mathbf{F}_q^n$. If $m\le n$, then ev is injective, and if $m\ge n$, then ev is surjective.

Proof: Suppose that $m\le n$. If $\mathrm{ev}(f)=\vec{0}$, then $f(\alpha_1)=\cdots=f(\alpha_n)=0$. Since $\deg(f)<m\le n$, this means that $f(x)$ is the zero polynomial. It is seen that $\ker(\mathrm{ev})=\{0\}$ when $m\le n$, which means that ev is an injective linear map.

[1] Ogawa et al. [7] allowed zero, but it was a mistake.

By the previous discussion, ev is injective on $\mathcal{P}_n$. Since $\dim \mathcal{P}_n = n$, the image $\mathrm{ev}(\mathcal{P}_n)$ of $\mathcal{P}_n$ under the map ev is $\mathbf{F}_q^n$. This means that ev is surjective on $\mathcal{P}_m$ if $m \geq n$. ■

The distribution of $k-L$ shares is considered before $|\vec{s}\rangle$ is given to the dealer. By reassigning indices, we may assume that the dealer wants to advance share the first to the $(k-L)$th shares. Let

$$|\Psi\rangle = \frac{1}{\sqrt{q^{k-L}}} \sum_{\vec{r}\in\mathbf{F}_q^{k-L}} |\vec{r}\rangle \otimes |\vec{r}\rangle \tag{3}$$

where $|\vec{r}\rangle = |r_1\rangle \otimes \cdots \otimes |r_{k-L}\rangle$ for $\vec{r} = (r_1, \ldots, r_{k-L}) \in \mathbf{F}_q^{k-L}$. Note that $|\Psi\rangle$ consists of $2(k-L)$ qudits, as $|\vec{r}\rangle$ consists of $(k-L)$ qudits.

Suppose that the quantum secret is $|\vec{s}\rangle = |s_1\rangle \otimes \cdots \otimes |s_L\rangle \in \mathcal{H}_q^{\otimes L}$ with $\vec{s} = (s_1, \ldots, s_L) \in \mathbf{F}_q^L$. For $\vec{r} \in \mathbf{F}_q^{k-L}$ and $\vec{s}$, let $g_{\vec{r},\vec{s}}(x)$ be a univariate polynomial such that $g_{\vec{r},\vec{s}}(x) \in \{f_{\vec{c}}(x) : \vec{c} \in D(\vec{s})\}$ and $g_{\vec{r},\vec{s}}(x)(\alpha_i) = r_i$ for $i = 1, \ldots, k-L$.

Proposition 2: For given $\vec{r}$ and $\vec{s}$, the polynomial $g_{\vec{r},\vec{s}}(x)$ exists uniquely.

Proof: Let $f_{\vec{c}}(x)$ for $\vec{c} \in D(\vec{s})$, as defined in (1) and (2). Recall that the coefficients $c_1, \ldots, c_L$ are known as $c_1 = s_1, \ldots, c_L = s_L$ by the condition $\vec{c} \in D(\vec{s})$. The coefficients $c_{L+1}, \ldots, c_k$ in $f_{\vec{c}}(x)$ will be regarded as $k-L$ unknowns in a system of linear equations. For $i = 1, \ldots, k-L$, the condition $g_{\vec{r},\vec{s}}(x)(\alpha_i) = r_i$ can be written as

$$c_{L+1} + c_{L+1}\alpha_i + \cdots + c_k\alpha_i^{k-L-1} \tag{4}$$

$$= \frac{r_i - s_1 - s_2\alpha_i - \cdots - s_L\alpha_i^{L-1}}{\alpha_i^L}. \tag{5}$$

The polynomial $f(x) = c_{L+1} + \cdots + c_k x^{k-L-1} \in \mathcal{P}_{k-L}$ corresponds to a solution of the system of linear equations if $\mathrm{ev}(f) = ((r_1 - s_1 - s_2\alpha_1 - \cdots - s_L\alpha_1^{L-1})/\alpha_1^L, \ (r_2 - s_1 - s_2\alpha_2 - \cdots - s_L\alpha_2^{L-1})/\alpha_2^L, \ldots, (r_{k-L} - s_1 - s_2\alpha_{k-L} - \cdots - s_L\alpha_{k-L}^{L-1})/\alpha_{k-L}^L)$, where the map ev is from $\mathcal{P}_{k-L}$ to $\mathbf{F}_q^{k-L}$. By Lemma 1, it can be seen that the solution of the system of linear equations considered here exists uniquely, which ensures the unique existence of $g_{\vec{r},\vec{s}}(x)$ for given $\vec{r}$ and $\vec{s}$. ■

Remark 3: The coefficients of $g_{\vec{r},\vec{s}}(x)$ can be more explicitly described in terms of $\vec{r}$ and $\vec{s}$, as follows. As in the proof of Proposition 2, let $f(x) = c_{L+1} + \cdots + c_k x^{k-L-1}$. $(b_1, \ldots, b_{k-L}) = ((r_1 - s_1 - s_2\alpha_1 - \cdots - s_L\alpha_1^{L-1})/\alpha_1^L, (r_2 - s_1 - s_2\alpha_2 - \cdots - s_L\alpha_2^{L-1})/\alpha_2^L, \ldots, (r_{k-L} - s_1 - s_2\alpha_{k-L} - \cdots - s_L\alpha_{k-L}^{L-1})/\alpha_{k-L}^L)$ are also used. As shown in the proof of Proposition 2, $f(\alpha_i) = b_i$ for $i = 1, \ldots, k-L$. To determine $f(x)$, we can use the Lagrange interpolation formula [15, Ch. 13]. For $i = 1, \ldots, k-L$, let

$$\ell_i(x) = \prod_{1\leq j\leq k-L, j\neq i} \frac{x - \alpha_j}{\alpha_i - \alpha_j}.$$

Then, $f(x) = c_{L+1} + \cdots + c_k x^{k-L-1}$ is given as

$$f(x) = \sum_{i=1}^{k-L} b_i \ell_i(x)$$

$$= \sum_{i=1}^{k-L} \frac{r_i - s_1 - s_2\alpha_i - \cdots - s_L\alpha_i^{L-1}}{\alpha_i^L} \ell_i(x)$$

and one has

$$g_{\vec{r},\vec{s}}(x) = s_1 + s_2 x + \cdots + s_L x^{L-1} + c_{L+1}x^L + \cdots + c_k x^{k-1}$$

$$= x^L f(x) + \sum_{i=1}^{L} s_i x^{i-1}.$$

Now, a new encoding procedure enabling advance sharing is described. By Proposition 2, one can define a unitary map U_{enc} from $\mathcal{H}_q^{\otimes k}$ to $\mathcal{H}_q^{\otimes(n-k+L)}$ sending a quantum state $|\vec{r}\rangle|\vec{s}\rangle$ to $|g_{\vec{r},\vec{s}}(\alpha_{k-L+1})\rangle \otimes \cdots \otimes |g_{\vec{r},\vec{s}}(\alpha_n)\rangle$. Note that $k = n - k + L$ by [7, Lemma 2].

The proposed procedure for advance sharing is as follows.

1) The dealer distributes $k-L$ qudits in the left half of (3).
2) After the quantum secret $|\vec{s}\rangle$ is given, the dealer applies U_{enc} to the remaining half of (3) and $|\vec{s}\rangle$. Then, the quantum state of all the n shares becomes

$$\frac{1}{\sqrt{q^{k-L}}} \sum_{\vec{r}\in\mathbf{F}_q^{k-L}} |\vec{r}\rangle \otimes |g_{\vec{r},\vec{s}}(\alpha_{k-L+1})\rangle \otimes \cdots \otimes |g_{\vec{r},\vec{s}}(\alpha_n)\rangle. \tag{6}$$

Remark 4: When $k-L-1$ or a fewer shares are advance shared, the dealer can simply keep some shares in the advance sharing phase in our proposal. On the other hand, it is impossible to advance share $k-L+1$ or more shares. When a set J of shares is not forbidden, the shares in J depend on quantum secrets [7, Th. 2]. Thus, in order for a set J of shares to be advance shareable, J must be a forbidden set. In Ogawa et al.'s (k, L, n) scheme, any $k-L+1$ or more shares cannot form a forbidden set and cannot be advance shareable. Our proposal makes advance shareable sets as large as possible.

E. PROOF OF CORRECTNESS

It is clear from Section II-D that the proposed procedure can distribute $k-L$ or a fewer shares before a secret is given to the dealer. On the other hand, at this point, it is unknown whether or not the proposed encoding procedure produces the same quantum states of shares as the original procedure [7]. In order to show their sameness, in this section, it will be proved that the proposed procedure gives the same quantum state of n shares as the original scheme by Ogawa et al. [7] for a given quantum secret $|\vec{s}\rangle$. In (2), the set of indices appearing in the quantum state is

$$V_1 = \{(f_{\vec{c}}(\alpha_1), \ldots, f_{\vec{c}}(\alpha_n)) : \vec{c} \in D(\vec{s})\}. \tag{7}$$

In (6), the set of indices appearing in the quantum state is

$$V_2 = \{(r_1, \ldots, r_{k-L}, g_{\vec{r},\vec{s}}(\alpha_{k-L+1}), \ldots, g_{\vec{r},\vec{s}}(\alpha_n)) : \vec{r} \in \mathbf{F}_q^{k-L}\}. \tag{8}$$

Theorem 5: For a fixed quantum secret $|\vec{s}\rangle$ for $\vec{s} \in \mathbf{F}_q^L$, the proposed procedure gives the same quantum state of shares as the original scheme by Ogawa et al. [7].

Proof: Equation (2) can be written as

$$\frac{1}{\sqrt{q^{k-L}}} \sum_{(v_1,\ldots,v_n)\in V_1} |v_1\rangle \otimes \cdots \otimes |v_n\rangle \tag{9}$$

and (6) can be written as

$$\frac{1}{\sqrt{q^{k-L}}} \sum_{(v_1,\ldots,v_n)\in V_2} |v_1\rangle \otimes \cdots \otimes |v_n\rangle. \tag{10}$$

To prove the theorem, it must be proven that (9) and (10) are equal. In order to prove the equality between (9) and (10), it is enough to show that the sets (7) and (8) are the same. To show the equality between two sets (7) and (8), in (11), it will be shown that there is a one-to-one correspondence between elements in the two sets (7) and (8).

For fixed $\vec{s} \in \mathbf{F}_q^L$ and $\vec{r} \in \mathbf{F}_q^{k-L}$, by Proposition 2, there exists a unique polynomial $f_{\vec{c}}$ with $\vec{c} \in D(\vec{s})$. This correspondence gives a bijection sending $\vec{r} \in \mathbf{F}_q^{k-L}$ to $f_{\vec{c}}$ with $\vec{c} \in D(\vec{s})$. By the definition of $g_{\vec{r},\vec{s}}$, one has

$$\begin{aligned} &(r_1, \ldots, r_{k-L}, g_{\vec{r},\vec{s}}(\alpha_{k-L+1}), \ldots, g_{\vec{r},\vec{s}}(\alpha_n)) \in V_2 \\ &= (g_{\vec{r},\vec{s}}(\alpha_1), \ldots, g_{\vec{r},\vec{s}}(\alpha_n)) \\ &= (f_{\vec{c}}(\alpha_1), \ldots, f_{\vec{c}}(\alpha_n)) \in V_1 \end{aligned} \tag{11}$$

which shows the theorem, where $\vec{c}$ is chosen according to $\vec{r}$. ■

F. EXAMPLE OF THE PROPOSED ENCODING

Definitions from Section II-C are reused. Let $q = 4$, $n = 3$, $k = 2$, $L = 1$, and $\alpha_i = \alpha^i \in \mathbf{F}_4$, where α is a primitive element of $\mathbf{F}_4$. Note that since q is not a prime number, this case cannot be handled in the previous research [14]. In our proposal, the dealer prepares 2-qudit entangled state $\frac{1}{2}\sum_{r\in\mathbf{F}_4} |r\rangle|r\rangle$ and send 1 qudit in it. Then, the dealer is given a quantum secret $|\vec{s}\rangle$ for $\vec{s} = (s) \in \mathbf{F}_4^1$. Then, one has

$$g_{r,s}(x) = \frac{r-s}{\alpha_1}x + s.$$

The unitary map U_{enc} sends $|r\rangle|s\rangle$ to $|\frac{r-s}{\alpha_1}\alpha_2 + s\rangle|\frac{r-s}{\alpha_1}\alpha_3 + s\rangle$. Now, it is clear that the leftmost share can be distributed before the secret $|s\rangle$ is given, in contrast to Section II-C.

III. ADVANCE SHARING WITH A QUANTUM RAMP SECRET SHARING SCHEME IN [10]

A. ZHANG AND MATSUMOTO'S SCHEME

As mentioned before, Zhang and Matsumoto [10] also proposed a (k, L, n) ramp quantum secret sharing scheme. Their proposal has strong security in contrast to [7], and the maximum possible number of participants was smaller, that is, $n \le q - L$. As in Section II, $\alpha_1, \ldots, \alpha_n$ are pairwise distinct elements in $\mathbf{F}_q$. Extra elements $\beta_1, \ldots, \beta_L$ are chosen such that all $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_L$ are pairwise distinct. In [10], any of $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_L$ can be $0 \in \mathbf{F}_q$. For $\vec{s} \in \mathbf{F}_q^L$, one has

$$D_{\mathrm{ZM}}(\vec{s}) = \{\vec{c} \in \mathbf{F}_q^k : f_{\vec{c}}(\beta_i) = s_i \text{ for } i = 1, \ldots, L\} \tag{12}$$

where $f_{\vec{c}}(x)$ is as defined in (1). For a given quantum secret $|\vec{s}\rangle$, in [10], the quantum state of n shares is obtained as

$$\frac{1}{\sqrt{q^{k-L}}} \sum_{\vec{c}\in D_{\mathrm{ZM}}(\vec{s})} |f_{\vec{c}}(\alpha_1)\rangle \otimes |f_{\vec{c}}(\alpha_2)\rangle \otimes \cdots \otimes |f_{\vec{c}}(\alpha_n)\rangle \tag{13}$$

B. EXAMPLE OF THE ORIGINAL ENCODING

Let $q = 7$, $n = 4$, $k = 3$, $L = 2$, $(\alpha_1, \ldots, \alpha_4) = (6, 2, 4, 5)$, and $(\beta_1, \beta_2) = (1, 3)$. This example is the same as [10, Example 2]. For $\vec{s} = (s_1, s_2)$, $D_{\mathrm{ZM}}(\vec{s})$ contains $(c_1, \ldots, c_3)$ if and only if

$$\begin{cases} c_1 + c_2 + c_3 = s_1 \\ c_1 + 3c_2 + 2c_3 = s_2. \end{cases}$$

The solution of the aforementioned system of linear equations for $(c_1, \ldots, c_3)$ is $D_{\mathrm{ZM}}(\vec{s}) = \{(5s_1 + 3s_2 + 3c_3, 3s_1 + 4s_2 + 3c_3, c_3) : c_3 \in \mathbf{F}_7\}$, which is the same [10, eq. (3)]. For a given quantum state $|\vec{s}\rangle = |s_1\rangle \otimes |s_2\rangle$, the quantum state of four shares is (the normalizing constant $1/\sqrt{7}$ is omitted) $\sum_{c_3=0}^{6} \otimes_{i=1}^{4} |\alpha_i^2 c_3 + \alpha_i(3s_1 + 4s_2 + 3c_3) + (5s_1 + 3s_2 + 3c_3)\rangle = |2s_1 + 6s_2\rangle \otimes |4s_1 + 4s_2\rangle \otimes |3s_1 + 5s_2\rangle \otimes |6s_1 + 2s_2\rangle + \cdots$, which is equivalent to [10, eq. (5)]. Since the quantum state of every qudit seems to depend on s_1 and s_2, from the encoding procedure in [10], it seems unclear how one share is advance shareable.

C. PROPOSED ADVANCE SHARING PROCEDURE FOR [10]

The distribution $k - L$ shares is considered before $|\vec{s}\rangle$ is given to the dealer. By reassigning indices, we may assume that the dealer wants to advance share the first to the $(k - L)$th shares. Consider $|\Psi\rangle$ as defined in (3).

Suppose that the quantum secret is $|\vec{s}\rangle = |s_1\rangle \otimes \cdots \otimes |s_L\rangle \in \mathcal{H}_q^{\otimes L}$ with $\vec{s} = (s_1, \ldots, s_L) \in \mathbf{F}_q^L$. For $\vec{r} \in \mathbf{F}_q^{k-L}$ and $\vec{s}$, let $h_{\vec{r},\vec{s}}(x)$ be a univariate polynomial such that $h_{\vec{r},\vec{s}}(x) \in \{f_{\vec{c}}(x) : \vec{c} \in D_{\mathrm{ZM}}(\vec{s})\}$ and $h_{\vec{r},\vec{s}}(x)(\alpha_i) = r_i$ for $i = 1, \ldots, k - L$.

Proposition 6: For given $\vec{r}$ and $\vec{s}$, the polynomial $h_{\vec{r},\vec{s}}(x)$ exists uniquely.

Proof: Consider $\mathcal{P}_k$ as defined in Lemma 1 and a polynomial $f(x) \in \mathcal{P}_k$. The condition $f(x) \in \{f_{\vec{c}}(x) : \vec{c} \in D_{\mathrm{ZM}}(\vec{s})\}$ means that $f(\beta_i) = s_i$ for $i = 1, \ldots, L$. Together with the conditions $f(\alpha_i) = r_i$ for $i = 1, \ldots, k - L$, the required $h_{\vec{r},\vec{s}}(x)$ is a polynomial $f(x) \in \mathcal{P}_k$ such that $\mathrm{ev}'(f) = (s_1, \ldots, s_L, r_1, \ldots, r_{k-L})$, where $\mathrm{ev}'(f) = (f(\beta_1), \ldots, f(\beta_L), f(\alpha_1), \ldots, f(\alpha_{k-L}))$. By Lemma 1, it can be seen that such a polynomial $f(x)$ exists uniquely, which is $h_{\vec{r},\vec{s}}(x)$. ■

Remark 7: Similarly to Remark 3, a more explicit description of $h_{\vec{r},\vec{s}}(x)$ will be given, which is determined by the equality condition $(h_{\vec{r},\vec{s}}(\beta_1), \ldots, h_{\vec{r},\vec{s}}(\beta_L), h_{\vec{r},\vec{s}}(\alpha_1), \ldots, h_{\vec{r},\vec{s}}(\alpha_{k-L})) = (s_1, \ldots, s_L, r_1, \ldots, r_{k-L})$. The

determination of $h_{\vec{r},\vec{s}}(x)$ is known as the Lagrange interpolation [15, Ch. 13], which can be computed as follows. In order to use the Lagrange interpolation formula, define $\beta_{L+j} = \alpha_j$ for $j = 1, \ldots, k-L$, and

$$\ell_i(x) = \prod_{1 \le j \le k, j \ne i} \frac{x - \beta_j}{\beta_i - \beta_j}.$$

Now, $h_{\vec{r},\vec{s}}(x)$ can be obtained as

$$h_{\vec{r},\vec{s}}(x) = \sum_{i=1}^{L} s_i \ell_i(x) + \sum_{i=1}^{k-L} r_i \ell_{i+L}(x).$$

Let us describe a new encoding procedure enabling advance sharing. By Proposition 6, a unitary map $U_{\mathrm{ZM,enc}}$ from $\mathcal{H}_q^{\otimes k}$ to $\mathcal{H}_q^{\otimes(n-k+L)}$ sending a quantum state $|\vec{r}\rangle|\vec{s}\rangle$ to $|h_{\vec{r},\vec{s}}(\alpha_{k-L+1})\rangle \otimes \cdots \otimes |h_{\vec{r},\vec{s}}(\alpha_n)\rangle$ can be defined. Note that $k = n - k + L$ by [7, Lemma 2].

The proposed procedure for advance sharing is as follows.

1) The dealer distributes $k - L$ qudits in the left half of (3).
2) After the quantum secret $|\vec{s}\rangle$ is given, the dealer applies $U_{\mathrm{ZM,enc}}$ to the remaining half of (3) and $|\vec{s}\rangle$. Then, the quantum state of all the n shares becomes

$$\frac{1}{\sqrt{q^{k-L}}} \sum_{\vec{r} \in \mathbf{F}_q^{k-L}} |\vec{r}\rangle \otimes |h_{\vec{r},\vec{s}}(\alpha_{k-L+1})\rangle \otimes \cdots \otimes |h_{\vec{r},\vec{s}}(\alpha_n)\rangle. \tag{14}$$

Remark 8: When $k - L - 1$ or a fewer shares are advance shared, the dealer can simply keep some shares in the advance sharing phase in our proposal as in Remark 4. On the other hand, as in Remark 4, it is impossible to advance share $k - L + 1$ or more shares, because in Zhang and Matsumoto's (k, L, n) scheme [10], any $k - L + 1$ or more shares cannot form a forbidden set. Therefore, similarly to Remark 4, our proposal makes advance shareable sets as large as possible.

D. PROOF OF CORRECTNESS

By the same reason explained at the beginning of Section II-E, in this section, it will be proven that the proposed procedure gives the same quantum state of shares as the original [10] for a given quantum secret $|\vec{s}\rangle$. In (13), the set of indices appearing in the quantum state is

$$\{(f_{\vec{c}}(\alpha_1), \ldots, f_{\vec{c}}(\alpha_n)) : \vec{c} \in D_{\mathrm{ZM}}(\vec{s})\}. \tag{15}$$

In (14), the set of indices appearing in the quantum state is

$$\{(r_1, \ldots, r_{k-L}, h_{\vec{r},\vec{s}}(\alpha_{k-L+1}), \ldots, h_{\vec{r},\vec{s}}(\alpha_n) : \vec{r} \in \mathbf{F}_q^{k-L}\}. \tag{16}$$

Theorem 9: For a fixed quantum secret $|\vec{s}\rangle$ for $\vec{s} \in \mathbf{F}_q^L$, the proposed procedure gives the same quantum state of shares as the original [10].

Proof: In order to prove the theorem, it is enough to show that the sets (15) and (16) are the same. For fixed $\vec{s} \in \mathbf{F}_q^L$ and $\vec{r} \in \mathbf{F}_q^{k-L}$, by Proposition 6, there exists a unique polynomial $f_{\vec{c}}(x)$ with $\vec{c} \in D_{\mathrm{ZM}}(\vec{s})$. This correspondence gives a bijection between $\vec{r} \in \mathbf{F}_q^{k-L}$ to $f_{\vec{c}}(x)$ with $\vec{c} \in D(\vec{s})$. By the definition of $h_{\vec{r},\vec{s}}$, one has

$$\begin{aligned} &(r_1, \ldots, r_{k-L}, h_{\vec{r},\vec{s}}(\alpha_{k-L+1}), \ldots, h_{\vec{r},\vec{s}}(\alpha_n)) \\ =\ &(h_{\vec{r},\vec{s}}(\alpha_1), \ldots, h_{\vec{r},\vec{s}}(\alpha_n)) \\ =\ &(f_{\vec{c}}(\alpha_1), \ldots, f_{\vec{c}}(\alpha_n)) \end{aligned}$$

which shows the theorem, where $\vec{c}$ is chosen according to $\vec{r}$. ■

E. EXAMPLE OF THE PROPOSED ENCODING

Definitions from Section III-B are reused. Let $q = 7$, $n = 4$, $k = 3$, $L = 2$, $(\alpha_1, \ldots, \alpha_4) = (6, 2, 4, 5)$, and $(\beta_1, \beta_2) = (1, 3)$. In our proposal, the dealer prepares 2-qudit entangled state $\frac{1}{\sqrt{7}} \sum_{r \in \mathbf{F}_7} |r\rangle|r\rangle$ and send 1 qudit in it. Then, the dealer is given a quantum secret $|\vec{s}\rangle$ for $\vec{s} = (s_1, s_2) \in \mathbf{F}_7^2$. Then, one has

$$h_{r,s_1,s_2}(x) = (r - 2s_1 + s_2)x^2 + (4s_1 - 4r)x + (3r - s_1 - s_2)$$

because $h_{r,s_1,s_2}(x)$ satisfies $h_{r,s_1,s_2}(\alpha_1) = h_{r,s_1,s_2}(6) = r$, $h_{r,s_1,s_2}(\beta_1) = h_{r,s_1,s_2}(1) = s_1$, and $h_{r,s_1,s_2}(\beta_2) = h_{r,s_1,s_2}(3) = s_2$. The unitary map $U_{\mathrm{ZM,enc}}$ sends $|r\rangle|s_1\rangle|s_2\rangle$ to $|h_{r,s_1,s_2}(\alpha_2)\rangle|h_{r,s_1,s_2}(\alpha_3)\rangle|h_{r,s_1,s_2}(\alpha_3)\rangle$. Now, it is clear that the leftmost share can be distributed before the secret $|\vec{s}\rangle$ is given, in contrast to Section III-B.

IV. CONCLUDING REMARKS

This article proposed new encoding procedures for Ogawa et al.'s [7] and Zhang and Matsumoto [10] ramp quantum secret sharing schemes and allowed the dealer to distribute shares in those schemes before secrets are given. This enhances the applicability of the secret sharing schemes by Ogawa et al. [7] and by Zhang and Matsumoto [10] to wider scenarios in which some participants are unavailable when the dealer obtains a secret. It was also proved that the new proposed encoding procedures retain desirable properties, such as coding rates, access structures, and strong security from the original schemes. It was also proved that the advance shareable sets are made as large as possible in the proposed encoding procedures.

Similarly to [13], there could exist a general method to construct an advance sharing procedure for any stabilizer-based quantum secret sharing, while retaining the correspondence between secrets and shares. Its investigation could be a future research agenda.

As mentioned in Section II-A, it seems also important to study advance sharing with other scenarios of quantum secret sharing, for example, [18], [19], [20]. It is also another research agenda.

ACKNOWLEDGMENT

The author deeply thanks the reviewers for helpful comments that improved this article.

REFERENCES

[1] F. Arute et al., "Quantum supremacy using a programmable superconducting processor," *Nature*, vol. 574, pp. 505–510, Oct. 2019, doi: 10.1038/s41586-019-1666-5.

[2] V. Attasena, J. Darmont, and N. Harbi, "Secret sharing for cloud data security: A survey," *Very Large Data Bases J.*, vol. 26, no. 5, pp. 657–681, Oct. 2017, doi: 10.1007/s00778-017-0470-9.

[3] R. Cleve, D. Gottesman, and H.-K. Lo, "How to share a quantum secret," *Phys. Rev. Lett.*, vol. 83, no. 3, pp. 648–651, Jul. 1999, doi: 10.1103/PhysRevLett.83.648.

[4] D. Gottesman, "Theory of quantum secret sharing," *Phys. Rev. A*, vol. 61, no. 4, Mar. 2000, Art. no. 042311, doi: 10.1103/PhysRevA.61.042311.

[5] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, Nov. 1979, doi: 10.1145/359168.359176.

[6] G. R. Blakley, "Safeguarding cryptographic keys," in *Proc. Int. Workshop Manag. Requirements Knowl.*, Jun. 1979, pp. 242–269, doi: 10.1109/MARK.1979.8817296.

[7] T. Ogawa, A. Sasaki, M. Iwamoto, and H. Yamamoto, "Quantum secret sharing schemes and reversibility of quantum operations," *Phys. Rev. A*, vol. 72, no. 3, Sep. 2005, Art. no. 032318, doi: 10.1103/PhysRevA.72.032318.

[8] M. Iwamoto and H. Yamamoto, "Strongly secure ramp secret sharing schemes for general access structures," *Inf. Process. Lett.*, vol. 97, no. 2, pp. 52–57, Jan. 2006, doi: 10.1016/j.ipl.2005.09.012.

[9] H. Yamamoto, "Secret sharing system using (k, l, n) threshold scheme," *Electron. Commun. Jpn. I, Commun.*, vol. 69, no. 9, pp. 313–317, 1985, doi: 10.1002/ecja.4410690906.

[10] P. Zhang and R. Matsumoto, "Quantum strongly secure ramp secret sharing," *Quantum Inf. Process.*, vol. 14, no. 2, pp. 715–729, Feb. 2015, doi: 10.1007/s11128-014-0863-2.

[11] R. Miyajima and R. Matsumoto, "Advance sharing of quantum shares for classical secrets," *IEEE Access*, vol. 10, pp. 94458–94468, 2022, doi: 10.1109/ACCESS.2022.3204389.

[12] S. H. Lie and H. Jeong, "Randomness cost of masking quantum information and the information conservation law," *Phys. Rev. A*, vol. 101, May 2020, Art. no. 052322, doi: 10.1103/PhysRevA.101.052322.

[13] M. Shibata and R. Matsumoto, "Advance sharing of quantum shares for quantum secrets," *IEICE Trans. Fundam. Electron., Commun. Comput. Sci.*, vol. E107-A, no. 8, pp. 1247–1254, Aug. 2024, doi: 10.1587/transfun.2023EAP1041.

[14] S. Masumori and R. Matsumoto, "Advance sharing with Ogawa et al.'s ramp quantum secret sharing scheme for prime-dimensional quantum systems," in *Proc. Int. Symp. Inf. Theory Appl.*, Nov. 2024, pp. 50–52, doi: 10.48550/arXiv.2404.15646.

[15] D. R. Stinson, *Cryptography Theory and Practice*, 3rd ed. London, U.K.: Chapman & Hall, 2006. [Online]. Available: https://www.routledge.com/Cryptography-Theory-and-Practice/Stinson-Paterson/p/book/9781032476049

[16] M. Hillery, V. Bužek, and A. Berthiaume, "Quantum secret sharing," *Phys. Rev. A*, vol. 59, pp. 1829–1834, Mar. 1999, doi: 10.1103/PhysRevA.59.1829.

[17] D. Pan et al., "The evolution of quantum secure direct communication: On the road to the qinternet," *IEEE Commun. Surv. Tuts.*, vol. 26, no. 3, pp. 1898–1949, Third Quarter 2024, doi: 10.1109/COMST.2024.3367535.

[18] C. Crépeau, D. Gottesman, and A. Smith, "Secure multi-party quantum computation," in *Proc. 34th Annu. ACM Symp. Theory Comput.*, 2002, pp. 643–652, doi: 10.1145/509907.510000.

[19] M. Ben-Or, C. Crépeau, D. Gottesman, A. Hassidim, and A. Smith, "Secure multiparty quantum computation with (only) a strict honest majority," in *Proc. 47th Annu. IEEE Symp. Found. Comput. Sci.*, 2006, pp. 249–260, doi: 10.1109/FOCS.2006.68.

[20] C. Crépeau, D. Gottesman, and A. Smith, "Approximate quantum error-correcting codes and secret sharing schemes," in *Proc. Annu. Int. Conf. Theory Appl. Cryptographic Techn.*, 2005, pp. 285–301, doi: 10.1007/11426639_17.

Ryutaroh Matsumoto (Member, IEEE) was born in Nagoya, Japan, in 1973. He received the B.E. degree in computer science, the M.E. degree in information processing, and the Ph.D. degree in electrical and electronic engineering from the Tokyo Institute of Technology, Tokyo, Japan, in 1996, 1998, and 2001, respectively.

From 2001 to 2004, he was an Assistant Professor with the Department of Information and Communications Engineering, Tokyo Institute of Technology, where he was an Associate Professor from 2004 to 2017. From 2017 to 2020, he was an Associate Professor with the Department of Information and Communication Engineering, Nagoya University, Nagoya, Japan. In 2011 and 2014, he was as a Velux Visiting Professor with the Department of Mathematical Sciences, Aalborg University, Aalborg, Denmark. Since 2020, he has been an Associate Professor with the Department of Information and Communications Engineering, Tokyo Institute of Technology, where he became a Full Professor in 2022. His research interests include error-correcting codes, quantum information theory, information-theoretic security, and communication theory.

Dr. Matsumoto was a recipient of the Young Engineer Award from the Institute of Electronics, Information and Communication Engineers (IEICE) and the Ericsson Young Scientist Award from Ericsson Japan in 2001. He was also a recipient of the Best Paper Awards from the IEICE in 2001, 2008, 2011, and 2014.