Advances in Mathematics of Communications
Volume 13, No. 1, 2019, 1–10
doi:10.3934/amc.2019001

STRONGLY SECURE QUANTUM RAMP SECRET SHARING CONSTRUCTED FROM ALGEBRAIC CURVES OVER FINITE FIELDS

Ryutaroh Matsumoto*
Department of Information and Communication Engineering
Nagoya University
Nagoya, Aichi 464-8603, Japan
and
Department of Mathematical Sciences
Aalborg University, Denmark

(Communicated by Patrick Solé)

Abstract. The first construction of strongly secure quantum ramp secret sharing by Zhang and Matsumoto had an undesirable feature that the dimension of quantum shares must be larger than the number of shares. By using algebraic curves over finite fields, we propose a new construction in which the number of shares can become arbitrarily large for fixed dimension of shares.

1. Introduction

Secret sharing (SS) scheme encodes a secret into multiple shares being distributed to participants, so that only qualified sets of shares can reconstruct the secret perfectly [17]. The secret and shares are traditionally classical information [17], but now quantum secret and quantum shares can also be used [7, 8, 15].

In perfect SS, if a set of shares is not qualified, that is, it cannot reconstruct the secret perfectly, then the set has absolutely no information about the secret. It is well-known that the share sizes in perfect SS must be larger than or equal to that of the secret, both in classical and quantum cases. To overcome this inefficiency of storing shares, the ramp classical SS was proposed [1, 12, 18], which reduces the share sizes at the cost of allowing partial information leakage to non-qualified sets of shares. In ramp SS, a share set is said to be forbidden if it has no information about secret, while it is said to be intermediate if it is neither qualified nor forbidden [9, 18].

The first quantum ramp SS was proposed by Ogawa et al. [13], which made the share size L times smaller than its secret, where L is the number of qudits in the secret. In their study [13], there were two drawbacks. Firstly, it does not control how information is leaked to a non-qualified set of shares, and there exists an undesirable case in which an intermediate set of shares can understand a qudit

2010 *Mathematics Subject Classification:* Primary: 81P94; Secondary: 94A62, 94B27.
Key words and phrases: Algebraic curve, quantum secret sharing, non-perfect secret sharing, ramp secret sharing.
This research is partly supported by the National Institute of Information and Communications Technology, Japan, and by the Japan Society for the Promotion of Science Grant Nos. 23246071 and 26289116, and the Villum Foundation through their VELUX Visiting Professor Programme 2013–2014.
* Corresponding author.

in the secret, as demonstrated in [19]. To exclude such a possibility, we introduced a notion of the strong security of quantum ramp SS, which ensures no intermediate set can understand a qudit in the secret (see [19] for its formal definition) and proposed an explicit construction with the strong security.

The second drawback of [13] as well as our previous proposal [19] is that the dimension of quantum shares must be larger than that of the number of participants. When the number of participants is large, handling quantum shares become more difficult, because handling large dimensional quantum systems are generally more difficult than smaller ones. Our previous proposal [19] solved the first drawback but did not the second. The purpose of this paper is to solve the first and the second drawbacks of [13] simultaneously.

We will proceed as follows: Firstly, we modify the strong security definition given in [19] in Section 2, because the previous definition in [19] required that all the qualified sets are of the same size, and also that all the forbidden sets are of the same size. Secondly, in Section 3, based on a general construction of quantum *ramp* secret sharing from CSS codes [10], we give a general construction of strongly secure quantum ramp secret sharing from a pair of linear codes over a finite field. Thirdly, in Section 4, we carry over the classical strongly secure ramp SS [6, 11] using algebraic curves to the quantum setting, then we prove that the proposed quantum SS has the strong security. We also present sufficient conditions for its qualified, intermediate, and forbidden sets by using results in Section 3, as the construction of Section 4 is a special case of the construction in Section 3. We conclude this paper in Section 6.

2. Extended definition of the strong security

Let q be a prime power, $\mathcal{G}_i$ $(i = 1, \ldots, L)$ and $\mathcal{H}_j$ $(j = 1, \ldots, n)$ be the q-dimensional complex linear spaces, where $\mathcal{G}_i$ contains the i-th qudit of the quantum secret, while $\mathcal{H}_j$ contains the j-th quantum share. L is the number of qudits in secret and n is the number of shares or participants. In this paper we consider the so-called pure state scheme [7, 8], in which a pure state secret is converted to pure state shares. Encoding is an isometric complex linear map from $\bigotimes_{i=1}^{L} \mathcal{G}_i$ to $\bigotimes_{j=1}^{n} \mathcal{H}_j$. A subset $J \subset \{1, \ldots, n\}$ is said to be qualified if the quantum secret is perfectly reconstructed from the aggregated shares in $\bigotimes_{j\in J} \mathcal{H}_j$, forbidden if the aggregated shares in $\bigotimes_{j\in J} \mathcal{H}_j$ is always the same quantum state regardless of the quantum secret, and intermediate otherwise, as defined in [13].

We introduce a new definition of the strong security, which does not require the qualified and the forbidden sets being the same size. Let $I \subseteq \{1, \ldots, L\}$, $J \subseteq \{1, \ldots, n\}$, $\overline{I} = \{1, \ldots, L\} \setminus I$, and $\overline{J} = \{1, \ldots, n\} \setminus J$. Define $\mathcal{G}_I = \bigotimes_{i\in I} \mathcal{G}_i$, and $\mathcal{G}_{\overline{I}} = \bigotimes_{i\in \overline{I}} \mathcal{G}_i$. The idea behind the following strong security with respect to I and J is that the share set J has no idea on what is a quantum state ρ_I on the part $\mathcal{G}_I$ of the quantum secret. To formally express this idea, the quantum state σ_J of shares on $\bigotimes_{j\in J} \mathcal{H}_j$ is required to be independent of ρ_I. On the other hand, σ_J also depends on the quantum state on $\mathcal{G}_{\overline{I}}$. When an illegitimate owner of the shares in J is guessing ρ_I, she or he is assumed to have no prior knowledge on the part $\mathcal{G}_{\overline{I}}$, which enables us to use the fully mixed state as the state on $\mathcal{G}_{\overline{I}}$.

By using the above ideas, we formally define our extended version of the strong security.

Definition 2.1. We retain notations from the above discussion. A quantum ramp secret sharing scheme is said to be strongly secure with respect to I and J if the quantum state σ_J on the share set J is always the same state regardless of the quantum state $\rho_I \otimes \rho_{\overline{I},\mathrm{mix}}$ of the whole quantum secret, where $\rho_{\overline{I},\mathrm{mix}}$ is the fully mixed state on $\mathcal{G}_{\overline{I}}$.

In our previous paper [19], a (k, L, n) quantum ramp SS (in the sense of [13]) was said to be strongly secure if all I and J with $|I| + |J| \leq k$ satisfy Definition 2.1, where k was the minimum size of share sets which can perfectly reconstruct the secret, and L, n had the same meaning as the present paper.

3. General construction of strongly secure quantum secret sharing schemes

In this section we propose a new general construction of strongly secure quantum ramp secret sharing from a pair of linear codes $C_2 \subsetneq C_1 \subseteq \mathbf{F}_q^n$ with $\dim C_1 - \dim C_2 = L$, The construction in this section is a special case of [10], but in [10] the strong security was not defined nor discussed. We emphasize that the general construction [15] of quantum secret sharing from MSP, which is equivalent to a pair of linear codes, did not cover ramp schemes, and the following results cannot be obtainind by [15] (without properly generalizing [15] to ramp schemes).

Encoding is done as follows: We will encode a quantum secret to n qudits in $\bigotimes_{j=1}^n \mathcal{H}_j$ by a complex linear isometric embedding. To specify such an embedding, it is enough to specify the image of each basis state $|\vec{s}\rangle \in \bigotimes_{i=1}^L \mathcal{G}_i$. Fix an $\mathbf{F}_q$-linear isomorphism $f : \mathbf{F}_q^{\dim C_1 - \dim C_2} \to C_1/C_2$. We encode $|\vec{s}\rangle$ to

$$\frac{1}{\sqrt{|C_2|}} \sum_{\vec{x} \in f(\vec{s})} |\vec{x}\rangle \in \bigotimes_{j=1}^n \mathcal{H}_j. \tag{1}$$

Recall that by definition of f, $f(\vec{s})$ is a subset of C_1, $f(\vec{s}) \cap f(\vec{s}_1) = \emptyset$ if $\vec{s} \neq \vec{s}_1$, and $f(\vec{s})$ contains $|C_2|$ vectors. From these properties we see that (1) defines a complex linear isometric embedding. The quantum system $\mathcal{H}_j$ is distributed to the j-th participant. For $I \subset \{1, \ldots, L\}$, the map P_I denotes the projection of a vector to the index set I, that is, for $\vec{s} = (s_1, \ldots, s_L) \in \mathbf{F}_q^L$, $P_I(\vec{s}) = (s_i)_{i \in I}$, which is a vector with $|I|$ components.

Proposition 1. *Let $f : \mathbf{F}_q^L \to C_1/C_2$ be as above. Define*

$$C_1' = \{(\vec{x}, P_{\overline{I}}(\vec{s})) \mid \vec{s} \in \mathbf{F}_q^L, \vec{x} \in f(\vec{s})\}, \tag{2}$$

$$C_2' = \{(\vec{x}, P_{\overline{I}}(\vec{s})) \mid \vec{s} \in \mathbf{F}_q^L, P_I(\vec{s}) = \vec{0}, \vec{x} \in f(\vec{s})\}. \tag{3}$$

Then the quantum ramp SS constructed from $C_1 \supsetneq C_2$ is strongly secure with respect to I and J if and only if

$$\dim P_J(C_1') - \dim P_J(C_2') = 0, \tag{4}$$

$$\dim P_{\overline{J} \cup \{n+1, \ldots, n+|\overline{I}|\}}(C_1') - \dim P_{\overline{J} \cup \{n+1, \ldots, n+|\overline{I}|\}}(C_2') = |I|. \tag{5}$$

Proof. By reordering indices we may assume $I = \{1, \ldots, |I|\}$. For $\vec{s}_I \in \mathbf{F}_q^{|I|}$ define

$$f'(\vec{s}_I) = \{(\vec{x}, \vec{s}_{\overline{I}}) \mid \vec{s}_{\overline{I}} \in \mathbf{F}_q^{|\overline{I}|}, \vec{x} \in f(\vec{s}_I \vec{s}_{\overline{I}})\}.$$

We have $\dim C_1' = \dim C_1$, $\dim C_2' = \dim C_2 + |\overline{I}|$, and f' is an $\mathbf{F}_q$-linear isomorphism from $\mathbf{F}_q^{|I|}$ to C_1'/C_2'. In the definition of strong security, the quantum secret

has the form

$$\left(\sum_{\vec{s}_I\in\mathbf{F}_q^{|I|}}\alpha(\vec{s}_I)|\vec{s}_I\rangle\right)\left(\sum_{\vec{s}_I\in\mathbf{F}_q^{|I|}}\alpha(\vec{s}_I)\langle\vec{s}_I|\right)\otimes\frac{1}{q^{|\overline{I}|}}\sum_{\vec{s}_{\overline{I}}\in\mathbf{F}_q^{|\overline{I}|}}|\vec{s}_{\overline{I}}\rangle\langle\vec{s}_{\overline{I}}|,$$

whose purification is

$$\sum_{\vec{s}_I\in\mathbf{F}_q^{|I|}}\alpha(\vec{s}_I)|\vec{s}_I\rangle\otimes\frac{1}{\sqrt{q^{|\overline{I}|}}}\sum_{\vec{s}_{\overline{I}}\in\mathbf{F}_q^{|\overline{I}|}}|\vec{s}_{\overline{I}}\rangle|\vec{s}_{\overline{I}}\rangle_R, \tag{6}$$

where $|\vec{s}_{\overline{I}}\rangle_R$ is a state vector in the reference system for purification. The encoding procedure (1) transforms (6) to

$$\begin{aligned}&\frac{1}{\sqrt{q^{|\overline{I}|}}}\sum_{\vec{s}_I\in\mathbf{F}_q^{|I|}}\alpha(\vec{s}_I)\frac{1}{\sqrt{|C_2|}}\sum_{\vec{s}_{\overline{I}}\in\mathbf{F}_q^{|\overline{I}|}}\sum_{\vec{x}\in f(\vec{s}_I\,\vec{s}_{\overline{I}})}|\vec{x}\rangle|\vec{s}_{\overline{I}}\rangle_R\\ =\;&\frac{1}{\sqrt{|C_2'|}}\sum_{\vec{s}_I\in\mathbf{F}_q^{|I|}}\alpha(\vec{s}_I)\sum_{\vec{y}\in f'(\vec{s}_I)}|\vec{y}\rangle.\end{aligned}$$

The joint quantum state of shares and the reference system for purification can be regarded as encoded shares from the quantum secret

$$\sum_{\vec{s}_I\in\mathbf{F}_q^{|I|}}\alpha(\vec{s}_I)|\vec{s}_I\rangle,$$

by using C_1'/C_2' and f'. Equations (4) and (5) is the necessary and sufficient condition [10] for J to be a forbidden set, which shows the theorem. □

Remark 1. A corresponding construction for classical secret sharing was proposed as [11].

4. Explicit Construction of strongly secure quantum ramp SS

In the previous constructions [13, 19] of quantum ramp SS, shares are generated by using evaluations of a polynomial at pairwise distinct numbers in the finite field $\mathbf{F}_q$ with q elements. Obviously q must be larger than n in those constructions. In the above constructions, the dimension of quantum shares is also q, and larger values of q usually make implementation difficult. The restriction $q > n$ also exists in the classical SS based on evaluations of a polynomial [12, 14]. One of standard ways in classical SS to overcome the restriction $q > n$ is to use points on an algebraic curve as done in [5, 6]. We will propose an explicit strongly secure quantum ramp SS based on the idea in [5, 6]. We note that the classical strong security of [6] was shown in [11].

It is well-known that an algebraic curve is mathematically equivalent to an algebraic function field of one variable [16]. So we will describe our proposal by using terminology of algebraic function fields, as done in [6].

Example 1. Let F be the field obtained by adding y to $\mathbf{F}_4(x)$, where y is a root of the univariate polynomial $y^2 + y = x^3$ (x^3 is regarded as a coefficient). Then F is an algebraic function field of one variable, and denoted by $\mathbf{F}_4(x, y)$. The process of creating $\mathbf{F}_4(x, y)$ from $\mathbf{F}_4(x)$ is the same in spirit as creating the field of complex numbers from that of real numbers by adding a root of $z^2 = -1$.

Observe also that the equation $y^2 + y = x^3$ can also be seen as an algebraic curve. There are eight points $R_1, \ldots, R_8 \in \mathbf{F}_4^2$ satisfying $y^2 + y = x^3$. For example, $(x, y) = (0, 1)$ satisfies $y^2 + y = x^3$ and can be R_1. Those eight points can be used for evaluations in the SS proposed in [5, 6] and also in our proposal described later. Note that usable points for evaluation increase from 4 to 8.

In the following we will use so-called $\mathbf{F}_q$-rational places. $R_1, \ldots, R_8$ are examples of $\mathbf{F}_4$-rational places in this function field. The solutions of the defining equation of F, e.g. $y^2 + y = x^3$, are a subset of $\mathbf{F}_q$-rational places, provided that the curve defined by the equation is *smooth*. See [16] for formal definitions.

We return to the general description of our proposal. Let $P_1, \ldots, P_n, Q_1, \ldots, Q_L$ be pairwise distinct $\mathbf{F}_q$-rational places of $F/\mathbf{F}_q$. A divisor of $F/\mathbf{F}_q$ is a formal sum of (not necessarily $\mathbf{F}_q$-rational) places of $F/\mathbf{F}_q$.The support of a divisor G is the set of places whose coefficients in G are nonzero. For example, the support of $2R_1 - R_3$ is the set $\{R_1, R_3\}$. Let G be a divisor whose support contains none of $P_1, \ldots, P_n, Q_1, \ldots, Q_L$. For any divisor G, there is a finite-dimensional $\mathbf{F}_q$-linear space $\mathcal{L}(G)$, see [16] for a formal definition.

Example 2. Consider again $\mathbf{F}_4(x, y)/\mathbf{F}_4$ introduced in Example 1. Let Q be the common pole of x and y, in other words, the unique point at infinity belonging to the projective algebraic curve defined by $y^2 + y = x^3$. Then a basis of $\mathcal{L}(uQ)$ as an $\mathbf{F}_4$-linear space is

$$\{x^a y^b \mid 0 \le a, 0 \le b \le 1, 2a + 3b \le u\}. \tag{7}$$

Thus, an element $h \in \mathcal{L}(uQ)$ is a polynomial in which every term is a multiple of a monomial in (7). We can obtain a value in $\mathbf{F}_4$ by substituting x, y in h by components in R_i (for example $R_1 = (0, 1)$) defined in Example 1. The obtained value is called the evaluation of h at $R_i$and denoted by $h(R_i)$.

In our proposal as well as [6], we also use another linear space $\mathcal{L}(G-Q_1-\cdots-Q_L)$. When $G = uQ$ as above, we have

$$\mathcal{L}(G - Q_1 - \cdots - Q_L) = \{h \in \mathcal{L}(G) \mid h(Q_i) = 0, \text{ for } i = 1, \ldots, L\}.$$

Now we are ready to describe our proposal by algebraic function fields. Since we assumed $\dim \mathcal{G}_i = \dim \mathcal{H}_j = q$ for all i, j, we can assume their orthonormal basis to be $\{|a\rangle \mid a \in \mathbf{F}_q\}$. Then the basis of $\bigotimes_{i=1}^{L} \mathcal{G}_i$ can be written as $\{|\vec{s}\rangle \mid \vec{s} \in \mathbf{F}_q^L\}$. To describe quantum ramp SS, it is sufficient to specify the quantum state of shares corresponding to a quantum secret $|\vec{s}\rangle \in \bigotimes_{i=1}^{L} \mathcal{G}_i$ for every $\vec{s} \in \mathbf{F}_q^L$ as done in [13, 19]. We assume that

$$L = \dim \mathcal{L}(G) - \dim \mathcal{L}(G - Q_1 - \cdots - Q_L), \tag{8}$$

$$0 = \dim \mathcal{L}(G - P_1 - \cdots - P_n). \tag{9}$$

The secret $|\vec{s}\rangle$ is encoded to

$$\frac{1}{\sqrt{q^{\dim \mathcal{L}(G-Q_1-\cdots-Q_L)}}} \sum_{\substack{h \in \mathcal{L}(G) \\ (h(Q_1),\ldots,h(Q_L))=\vec{s}}} |h(P_1)\rangle \otimes |h(P_2)\rangle \otimes \cdots \otimes |h(P_n)\rangle. \tag{10}$$

The mapping $h \in \mathcal{L}(G)$ to $(h(Q_1), \ldots, h(Q_L))$ is $\mathbf{F}_q$-linear and its kernel is $\mathcal{L}(G - Q_1 - \cdots - Q_L)$ (see the end of Example 2). By (8) this mapping is surjective, and for any $\vec{s} \in \mathbf{F}_q^L$ there exist $q^{\dim \mathcal{L}(G-Q_1-\cdots-Q_L)}$ elements $h \in \mathcal{L}(G)$ satisfying $(h(Q_1),\ldots, h(Q_L)) = \vec{s}$, which justifies the normalization factor in (10).

On the other hand, (9) ensures that the mapping $h \in \mathcal{L}(G)$ to $(h(P_1), \ldots, h(P_n))$ is $\mathbf{F}_q$-linear and injective. This guarantees that terms appearing in the summation of (10) do not overlap for different $\vec{s}$, $\vec{s}' \in \mathbf{F}_q^L$, which means that the encoded shares (10) for different $\vec{s}$, $\vec{s}'$ are orthogonal to each other. From these discussions we see that (10) maps an orthonormal basis to a subset of an orthonormal basis, and that (10) defines a complex linear isometric embedding, from $\bigotimes_{i=1}^{L} \mathcal{G}_i$ to $\bigotimes_{j=1}^{n} \mathcal{H}_j$.

Remark 2. One of the two classical ramp SS proposed by Chen et al. [6] is as follows: For a classical secret $(s_1, \ldots, s_L) \in \mathbf{F}_q^L$, an element $h \in \mathcal{L}(G)$ with $h(Q_i) = s_i$ $(i = 1, \ldots, L)$ is chosen uniformly randomly. Then the j-th share is computed as $h(P_j)$. Its similarity to our proposal (10) should be obvious.

For its strong security, we have the following theorem.

Theorem 4.1. *The above quantum ramp SS is strongly secure with respect to $I \subset \{1, \ldots, L\}$ and $J \subset \{1, \ldots, n\}$ if*

$$|J| \le |\overline{I}| + \min\{\deg G - L - 2g(F) + 1, n - 1 - \deg G\}, \tag{11}$$

where $g(F)$ denotes the genus of the algebraic function field $F/\mathbf{F}_q$, see [16] for its definition.

Example 3. In Example 2, we have $g(F) = 1$ and $\deg uQ = u$.

Proof. Hereafter we make a different assumption $\overline{I} = \{1, \ldots, |\overline{I}|\}$. When we apply Proposition 1 to the proposed quantum ramp SS, C_1' and C_2' in Proposition 1 become

$$\begin{aligned} C_1' &= \{(f(P_1), \ldots, f(P_n), f(Q_1), \ldots, f(Q_{|\overline{I}|})) \mid f \in \mathcal{L}(G)\}, \\ C_2' &= \{(f(P_1), \ldots, f(P_n), f(Q_1), \ldots, f(Q_{|\overline{I}|})) \mid f \in \mathcal{L}(G), \forall i \in I, f(Q_i) = 0\} \\ &= \{(f(P_1), \ldots, f(P_n), f(Q_1), \ldots, f(Q_{|\overline{I}|})) \mid f \in \mathcal{L}(G - \sum_{i \in I} Q_i)\}. \end{aligned}$$

Equation (11) ensures that

$$\begin{aligned} & |J| \le |\overline{I}| + n - 1 - \deg G \\ \Leftrightarrow\ & \deg G \le |\overline{J}| + |\overline{I}| - 1. \end{aligned} \tag{12}$$

By [16], (12) implies that the mapping $\mathcal{L}(G) \ni h \mapsto (h(P_{j_1}), \ldots, h(P_{j_{|\overline{J}|}}), h(Q_{i_1}), \ldots, h(Q_{i_{|\overline{I}|}})) \in P_J(C_1')$ is $\mathbf{F}_q$-linear and bijective, where $\{i_1, \ldots, i_{|\overline{I}|}\} = \overline{I}$ and $\{j_1, \ldots, j_{|\overline{J}|}\} = \overline{J}$. The above mapping also gives $P_J(C_2')$ as its image of $\mathcal{L}(G - \sum_{i \in I} Q_i)$. Equation (8) implies

$$|I| = \dim \mathcal{L}(G) - \dim \mathcal{L}(G - \sum_{i \in I} Q_i),$$

which in turn implies (5) by the above bijection between $\mathcal{L}(G)$ and $P_J(C_1')$.

On the other hand, (11) also ensures that

$$\begin{aligned} & |J| \le |\overline{I}| + \deg G - L - 2g(F) + 1 \\ \Leftrightarrow\ & |J| \le \deg G - |I| - 2g(F) + 1 \\ \Leftrightarrow\ & |J| \le \deg(G - \sum_{i \in I} Q_i) - 2g(F) + 1. \end{aligned} \tag{13}$$

By [16], (13) implies that the mapping $\mathcal{L}(G - \sum_{i \in I} Q_i) \ni h \mapsto (h(P_{j_1'}), \ldots, h(P_{j_{|J|}'})) \in \mathbf{F}_q^{|J|}$ is $\mathbf{F}_q$-linear and surjective, where $\{j_1', \ldots, j_{|J|}'\} = J$. On the other

hand, the image of the above mapping is $P_J(C_2')$, which means that $P_J(C_2') = \mathbf{F}_q^{|J|} = P_J(C_1')$, which in turn means that (4) holds. Since we have confirmed (4) and (5), the proof of Theorem 4.1 is completed by using Proposition 1. □

For quantum ramp SS to be useful, a procedure for reconstructing the quantum secret and sufficient conditions for qualified and forbidden sets are indispensable. On the other hand, actually the above proposal is a special case of quantum ramp SS constructed from algebraic curves studied in [10]. By straightforward application of [10], $\{1, \ldots, n\} \supset J$ is qualified if

$$|J| \geq \max\{1 + \deg G, n - (\deg G - L - 2g(F) + 1)\}, \tag{14}$$

and J is forbidden if

$$|J| \leq \min\{\deg G - L - 2g(F) + 1, n - 1 - \deg G\}. \tag{15}$$

Note that (11) contains (15) as its special case $|\bar{I}| = 0$. The reconstruction procedure in [10] can also be used for the proposal in this paper.

To make n larger with fixed q, we must find an algebraic function fields with many $\mathbf{F}_q$-rational places. It is well-known [16] that the number of $\mathbf{F}_q$-rational places is at most $1 + q + g(F)\lfloor 2\sqrt{q} \rfloor$. $F/\mathbf{F}_4$ in Examples 1–3 reaches this upper bound, because the place Q in Example 2 is also $\mathbf{F}_4$-rational and $F/\mathbf{F}_4$ in Examples 1–3 has nine $\mathbf{F}_4$-rational places. Requiring more $\mathbf{F}_q$-rational places generally makes $g(F)$ larger, which makes inequalities (11), (14) and (15) weaker. Therefore, for fixed q and n, it is desirable to use an algebraic function field with smaller $g(F)$. Search for such ones has been an active research area in pure mathematics for past 30 years, see [16]. In particular, it is known that for fixed q we can construct an algebraic function field with arbitrarily many $\mathbf{F}_q$-rational places.

5. Preferable divisors and algebraic function fields

In this section, we clarify which divisor and algebraic function field provide a preferable strongly secure quantum secret sharing. Firstly, we consider which divisor G is preferable with fixed L and function field F. The chosen divisor G must satisfy the assumption (8). We have to make $\deg G \geq L - 1$, otherwise $\dim \mathcal{L}(G) \leq L - 1$ and (8) cannot hold. When $\deg G \geq L + 2g(F) - 1$, then we always have $\dim \mathcal{L}(G) = \deg G - g(F) + 1$ and $\dim \mathcal{L}(G - Q_1 - \cdots - Q_L) = \deg G - L - g(F) + 1$, which implies (8). So we see that $\deg G \geq L + 2g(F) - 1$ is a sufficient condition for (8). There is no necessary and sufficient condition for (8) in terms of $\deg G$ because $\deg G$ cannot completely determine $\dim \mathcal{L}(G - Q_1 - \cdots - Q_L)$.

In order to discuss which divisor G is preferable, we must fix the target access structure. An access structure consists of a family of forbidden sets and that of qualified sets. For simplicity of discussion, we assume that r or more shares must be qualified and t or less shares must be forbidden. This type of access structures is often studied, e.g., in [2, 3, 4]. Requirements on divisors G are determined by r and t. In ramp quantum secret sharing, a share set is qualified if and only if its complement is forbidden [13]. This implies that $n - t$ or more shares must be qualified. We may assume $r = n - t$ without loss of generality only in this paragraph. Since the construction considered in this paper is a special case of [10, Section 6], by [10, Eq. (28)], the following condition ensures our requirement:

$$\max\{1 + \deg G, n - (\deg G - L - 2g(F) + 1)\} \leq r = n - t. \tag{16}$$

In light of (11) in Theorem 4.1, we should choose a divisor G with the largest possible value of $\min\{\deg G - L - 2g(F) + 1, n - 1 - \deg G\}$ as long as (16) holds. Such a choice of $\deg G$ can be determined by a simple computer search, as it is a simple search of integers.

Next, we will consider which function field F is preferable for our construction, by investigating which values of r and t can be realized. Since a share set is qualified if and only if its complement is forbidden [13], we must have $r \le n - t$. Since we have $r > t$, we must have $r > n/2 > t$.

Ogawa et al.'s construction [13] and our previous construction [19] with strong security can realize any values of r and t provided that $L \le r - t$ and $r > n/2 > t$, with sufficiently large q. Maximum values of n are $q - 1$ by [13] and $q - L$ by [19]. For a special case $g(F) = 0$ and $1 \le t' \le (n - L)/2$ in our construction, by (16) the choice of $\deg G = t' + L - 1$ gives $r \le n - t'$ and $t \ge t'$. Since $r \le n - t$ we see that $r = n - t'$ and $t = t'$, which exactly matches with the constructions in [13, 19]. This is not a coincidence as [19] can be interpreted as a special case of the proposed construction with $g(F) = 0$.

The difference $r - t$ is called the threshold gap in secret sharing [3, 4]. We have seen that the threshold gap L can be realized with $g(F) = 0$ by choosing $t' = (n - L)/2$, when the number of participants are bounded by $q - 1$. A larger genus $g(F) > 0$ enables larger values of n as we have more points on a curve. However, the threshold gap also increases from L, as we will see below.

Suppose that the number of qudits in a quantum secret is L, as before. We assume Eq. (8). By [10, Eq. (28)], we have

$$\begin{aligned} t &\ge \min\{n - 1 - \deg G, \deg G - L - 2g(F) + 1\}, \\ r &\le \max\{1 + \deg G, n - (\deg G - L - 2g(F) + 1)\}. \end{aligned}$$

Thus,

$$r - t \le \max\{L + 2g(F), 2 + 2\deg G - n, n - 2(\deg G - L - 2g(F) + 1)\}.$$

The threshold gap $r - t$ can be smaller than $L + 2g(F)$, but the upper bound $L + 2g(F)$ is often tight, as we will see below.

Since a larger value of threshold gap implies more intermediate sets (sets of shares neither qualified or forbidden), we prefer smaller values of threshold gap and genus $g(F)$. Thus, for a fixed number of shares or participants, algebraic function fields of smaller genera are preferable. On the other hand, for fixed q and n, there are lower bounds on $g(F)$, see for example [16].

Example 4. We consider the algebraic function field of Example 2, and let $L = 1$. Suppose that we want to share a quantum secret to $n = 7$ participants so that two or less participants have absolutely no information about the quantum secret (but three or more participant could have some information). By [10, Eq. (28)], we have to choose

$$2 \le n - \max\{1 + \deg G, n - (\deg G - L - 2g(F) + 1)\},$$

which reduces to

$$4 = \deg G.$$

Again by [10, Eq. (28)], we see that 5 or more participants can reconstruct the quantum secret. The estimate of threshold gap [10, Eq. (28)] is equal to $L + 2g(F)$ as above.

We will see that our estimate of the threshold gap is tight. To consider the actual value of threshold gap, we have to fix G, $Q_1, \ldots, Q_L$, and $P_1, \ldots, P_n$.

Let $G = 4Q$, $Q_1 = (0,0)$, and $P_1, \ldots, P_7$ be the rest of $\mathbf{F}_4$-rational places in the algebraic function field.

We consider whether or not three participants can have nonzero information. Let $\{P_1, \ldots, P_3\}$ be rational places corresponding to participants. Then

$$\begin{aligned} & \dim\{(f(P_1), \ldots, f(P_3)) \mid f \in \mathcal{L}(G)\} \\ = \ & \dim \mathcal{L}(G) - \dim \mathcal{L}(G - P_1 - P_2 - P_3) \\ = \ & 3 - 1 = 2, \end{aligned} \tag{17}$$

and

$$\begin{aligned} & \dim\{(f(P_1), \ldots, f(P_3)) \mid f \in \mathcal{L}(G - Q_1)\} \\ = \ & \dim \mathcal{L}(G - Q_1) - \dim \mathcal{L}(G - Q_1 - P_1 - P_2 - P_3) \\ = \ & 2 - \dim \mathcal{L}(G - Q_1 - P_1 - P_2 - P_3), \end{aligned} \tag{18}$$

The zeros of $x(x-1)$ consist of $(0,0) = Q_1$, $(0,1)$, $(1,\alpha)$, $(1,\alpha^2)$, where α is a primitive element of $\mathbf{F}_4$. When P_1, P_2, P_3 are $(0,1)$, $(1,\alpha)$, $(1,\alpha^2)$, the function $x(x-1)$ belongs to $\mathcal{L}(G - Q_1 - P_1 - P_2 - P_3)$ and (17) and (18) are different. It implies that the three participants corresponding to $(0,1)$, $(1,\alpha)$, $(1,\alpha^2)$ have nonzero information about the quantum secret by the main theorem of [10], and our estimate $t \geq 2$ is tight. By [13], this also implies that the complementary set of participants cannot perfectly reconstruct the quantum secret, and our estimate $r \leq 5$ is also tight. With this example, our estimate of threshold gap ≤ 3 is tight and cannot be improved further.

6. Conclusion

In this paper we argued that the previously proposed strongly secure quantum ramp SS [19] becomes difficult in implementation when the number n of participants is large, because the dimension q of each quantum share must be $> n$. To overcome this drawback, we proposed new quantum ramp SS that allows arbitrarily large n for fixed q while retaining the strong security. The proposed construction is similar to the classical ramp SS proposed by Chen et al. [6].

References

[1] G. R. Blakley and C. Meadows, Security of ramp schemes, in *Advances in Cryptology–CRYPTO'84*, vol. 196 of Lecture Notes in Computer Science, Springer-Verlag, 1985, 242–269.

[2] A. Bogdanov, S. Guo and I. Komargodski, Threshold secret sharing requires a linear size alphabet, in *Theory of Cryptography* (eds. M. Hirt and A. Smith), Springer Berlin Heidelberg, Berlin, Heidelberg, **9986** (2016), 471–484.

[3] I. Cascudo, R. Cramer and C. Xing, Bounds on the threshold gap in secret sharing and its applications, *IEEE Trans. Inform. Theory*, **59** (2013), 5600–5612.

[4] I. Cascudo, J. Skovsted Gundersen and D. Ruano, Improved bounds on the threashold gap in ramp secret sharing, 2018, Cryptology ePrint Archive 2018/099.

[5] H. Chen and R. Cramer, Algebraic geometric secret sharing schemes and secure multi-party computations over small fields, in *Advances in Cryptology – CRYPT 2006* (ed. C. Dwork), vol. 4117 of Lecture Notes in Computer Science, Springer-Verlag, 2006, 521–536.

[6] H. Chen, R. Cramer, R. de Haan and I. Cascudo Pueyo, Strongly multiplicative ramp schemes from high degree rational points on curves, in *Advances in Cryptology – EUROCRYPT 2008* (ed. N. Smart), vol. 4965 of Lecture Notes in Computer Science, Springer-Verlag, 2008, 451–470.

[7] R. Cleve, D. Gottesman and H.-K. Lo, How to share a quantum secret, *Phys. Rev. Lett.*, **83** (1999), 648–651.

[8] D. Gottesman, Theory of quantum secret sharing, *Phys. Rev. A*, **61** (2000), 042311.

[9] M. Iwamoto and H. Yamamoto, Strongly secure ramp secret sharing schemes for general access structures, *Inform. Process. Lett.*, **97** (2006), 52–57.
[10] R. Matsumoto, Coding theoretic construction of quantum ramp secret sharing, *IEICE Trans. Fundamentals*, **E101-A** (2018), 1215–1222.
[11] R. Matsumoto, Strong security of the strongly multiplicative ramp secret sharing based on algebraic curves, *IEICE Trans. Fundamentals*, **E98-A** (2015), 1576–1578.
[12] R. J. McEliece and D. V. Sarwate, On sharing secrets and Reed-Solomon codes, *Comm. ACM*, **24** (1981), 583–584.
[13] T. Ogawa, A. Sasaki, M. Iwamoto and H. Yamamoto, Quantum secret sharing schemes and reversibility of quantum operations, *Phys. Rev. A*, **72** (2005), 032318.
[14] A. Shamir, How to share a secret, *Comm. ACM*, **22** (1979), 612–613.
[15] A. D. Smith, Quantum secret sharing for general access structures, 2000, arXiv:quant-ph/0001087,
[16] H. Stichtenoth, *Algebraic Function Fields and Codes*, vol. 254 of Graduate Texts in Mathematics, 2nd edition, Springer-Verlag, Berlin Heidelberg, 2009.
[17] D. R. Stinson, *Cryptography Theory and Practice*, 3rd edition, Chapman & Hall/CRC, 2006.
[18] H. Yamamoto, Secret sharing system using (k, l, n) threshold scheme, *Electronics and Communications in Japan (Part I: Communications)*, **69** (1986), 46–54, (the original Japanese version published in 1985).
[19] P. Zhang and R. Matsumoto, Quantum strongly secure ramp secret sharing, *Quantum Information Processing*, **14** (2015), 715–729.

Received for publication March 2015.

E-mail address: ryutaroh.matsumoto@nagoya-u.jp