Coding Theoretic Construction of Quantum Ramp Secret Sharing

Ryutaroh Matsumoto
Department of Communications and Computer Engineering
Tokyo Institute of Technology, 152-8550 Japan
Email: ryutaroh@it.ce.titech.ac.jp
http://www.rmatsumoto.org/research.html

8 July 2014

Abstract

We show a construction of a quantum ramp secret sharing scheme from a nested pair of linear codes. Necessary and sufficient conditions for qualified sets and forbidden sets are given in terms of combinatorial properties of nested linear codes. An algebraic geometric construction for quantum secret sharing is also given.

1 Introduction

Secret sharing (SS) [12] is a cryptographic scheme to encode a secret to multiple shares being distributed to participants, so that only qualified sets of participants can reconstruct the original secret from their shares. Traditionally both secret and shares were classical information (bits). Several authors [3, 7, 13] extended the traditional SS to quantum one so that a quantum secret can be encoded to quantum shares.

When we require unqualified sets of participants to have zero information of the secret, the size of each share must be larger than or equal to that of secret. By tolerating partial information leakage to unqualified sets, the size of shares can be smaller than that of secret. Such an SS is called a ramp SS [1, 15]. The quantum ramp SS was proposed by Ogawa et al. [11]. In their construction, each share is a quantum state on a q-dimensional complex linear space, and q has to be larger than or equal to the number n of participants. When n is large, q also has to be large. But it is not clear whether or not such a large dimensional quantum systems are always readily available. To deal with such a situation, we need a quantum ramp SS allowing $n > q$.

It is well-known that classical ramp SS can be constructed from a pair of linear codes $C_2 \subsetneq C_1 \subseteq \mathbf{F}_q^n$ [2, 4], where $\mathbf{F}_q$ is the finite field with q elements. We call a quantum state in a q-dimensional system as a qudit. In this paper we shall show the following.

Theorem 1 *Let $J \subseteq \{1, \ldots, n\}$ and $\overline{J} = \{1, \ldots, n\} \setminus J$. For $\vec{x} = (x_1, \ldots, x_n) \in \mathbf{F}_q^n$ define $P_J(\vec{x}) = (x_i)_{i \in J}$. We define $\widetilde{P}_J$ to be an $\mathbf{F}_q$-linear map from C_1/C_2 to $P_J(C_1)/P_J(C_2)$ sending $\vec{x} + C_2 \in C_1/C_2$ to $P_J(\vec{x}) + P_J(C_2) \in P_J(C_1)/P_J(C_2)$. A quantum ramp SS can be constructed from **any** $C_2 \subsetneq C_1 \subseteq \mathbf{F}_q^n$.*

1. *The constructed quantum SS encodes a quantum secret of* $(\dim C_1 - \dim C_2)$ *qudits to n shares. Each share is a qudit.*

2. *A set J of participants can reconstruct*

$$\dim \widetilde{P}_J(\ker(\widetilde{P}_{\overline{J}})) \tag{1}$$

qudits out of $(\dim C_1 - \dim C_2)$ *qudits of the encoded quantum secret. If*

$$\dim \widetilde{P}_J(\ker(\widetilde{P}_{\overline{J}})) = \dim C_1 - \dim C_2 \tag{2}$$

then the set J of participants can reconstruct the secret perfectly. This means that J is a qualified set. In this case $\overline{J}$ has no information of the secret, which means that $\overline{J}$ is a forbidden set.

3. *The condition (2) is equivalent to both*

$$\begin{aligned} \dim P_J(C_1) - \dim P_J(C_2) &= \dim C_1 - \dim C_2 \textit{ and} \quad (3)\\ \dim P_{\overline{J}}(C_1) - \dim P_{\overline{J}}(C_2) &= 0. \quad (4) \end{aligned}$$

Condition (4) is equivalent to

$$\dim C_2^{\perp} \cap \ker(P_J) - \dim C_1^{\perp} \cap \ker(P_J) = 0. \tag{5}$$

4. *Both (3) and (4) are also a necessary condition for J to be a qualified set.*

This paper is organized as follows: Section 2 proposes the encoding of secrets and shows Item 1 in Theorem 1. Section 3 proposes the decoding of secrets and it shows Items 2 and 3 in Theorem 1. Section 4 proves Item 4 in Theorem 1 by computing the Holevo information of the set J. It also computes the coherent information as a byproduct. Section 5 shows that Theorem 1 completely characterizes the qualified and forbidden sets of the quantum ramp SS by Ogawa et al. [11]. Section 6 gives an algebraic geometric construction. Section 7 gives concluding discussions.

2 Encoding Secrets

We shall propose a construction of a quantum ramp SS from a nested pair of linear codes $C_2 \subsetneq C_1 \subseteq \mathbf{F}_q^n$. Our proposal is a quantum version of classical ramp SS proposed by Chen et al. [2, Section 4.2]. Let $\mathcal{G}_i$ and $\mathcal{H}_j$ be q-dimensional complex linear spaces. We also assume that orthonormal bases of $\mathcal{G}_i$ and $\mathcal{H}_j$ are indexed by $\mathbf{F}_q$ as $\{|s\rangle\}_{s\in\mathbf{F}_q}$. The quantum secret is $\dim C_1 - \dim C_2$ qudits on $\bigotimes_{i=1}^{\dim C_1 - \dim C_2} \mathcal{G}_i$. Fix an $\mathbf{F}_q$-linear isomorphism $f : \mathbf{F}_q^{\dim C_1 - \dim C_2} \to C_1/C_2$. Also, $\{|\vec{s}\rangle \mid \vec{s} \in \mathbf{F}_q^{\dim C_1 - \dim C_2}\}$ is an orthonormal basis of $\bigotimes_{i=1}^{\dim C_1 - \dim C_2} \mathcal{G}_i$. We shall 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 $|\vec{s}\rangle \in \bigotimes_{i=1}^{\dim C_1 - \dim C_2} \mathcal{G}_i$. We encode $|\vec{s}\rangle$ to

$$\frac{1}{\sqrt{|C_2|}} \sum_{\vec{x}\in f(\vec{s})} |\vec{x}\rangle \in \bigotimes_{j=1}^{n} \mathcal{H}_j. \tag{6}$$

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 (6) defines a complex linear isometric embedding. The quantum system $\mathcal{H}_j$ is distributed to the j-th participant.

Example 2 *We show a slightly modified variant of Ogawa et al. [11] as an example. Let $q = 7$, $n = 5$, $L = 3$, $\alpha_1 = 3$, $\alpha_2 = 5$, $\alpha_3 = 6$, $\alpha_4 = 1$, $\alpha_5 = 4$. For s_1, s_2, $s_3 \in \mathbf{F}_7$, $|s_1 s_2 s_3\rangle$ is encoded to*

$$\frac{1}{\sqrt{7}} \sum_{r\in\mathbf{F}_7} \bigotimes_{j=1}^{5} |r + s_1\alpha_j + s_2\alpha_j^2 + s_3\alpha_j^3\rangle. \tag{7}$$

This encoding can be described by

$$\begin{array}{rcl} C_1 & = & \{(r + s_1\alpha_j + s_2\alpha_j^2 + s_3\alpha_j^3)_{j=1,\ldots,5} \mid r, s_1, s_2, s_3 \in \mathbf{F}_7\}, \\ C_2 & = & \{(r, r, r, r, r) \mid r \in \mathbf{F}_7\}, \\ f(s_1, s_2, s_3) & = & \{(r + s_1\alpha_j + s_2\alpha_j^2 + s_3\alpha_j^3)_{j=1,\ldots,5} \mid r \in \mathbf{F}_7\}. \end{array}$$

3 Decoding Secrets

3.1 Preliminary Algebra

In this subsection we show Item 3 in Theorem 1 in order to introduce the proposed decoding procedure. The equivalence between (4) and (5) follows from Forney's second duality lemma [6, Lemma 7] and $\ker(P_J) = \{(x_1, \ldots, x_n) \in \mathbf{F}_q^n \mid x_i = 0 \text{ if } i \in J\}$.

Equation (3) is equivalent to $\widetilde{P}_J$ being an isomorphism, and (4) is equivalent to $\widetilde{P}_{\overline{J}}$ being the zero map. From these observations we see that (3) and (4) imply (2) and vice versa. This finishes the proof of Item 3 in Theorem 1.

Remark 3 *Equation (5) corresponds to [8, Eq. (3)] for classical ramp SS.*

3.2 Proposed Decoding Procedure

Suppose that the quantum secret is

$$\sum_{\vec{s}\in\mathbf{F}_q^{\dim C_1-\dim C_2}} \alpha(\vec{s})|\vec{s}\rangle \in \bigotimes_{i=1}^{\dim C_1-\dim C_2} \mathcal{G}_i. \tag{8}$$

It is encoded to n qudits as

$$\sum_{\vec{s}\in\mathbf{F}_q^{\dim C_1-\dim C_2}} \alpha(\vec{s})\frac{1}{\sqrt{|C_2|}} \sum_{\vec{x}\in f(\vec{s})} |\vec{x}\rangle \in \bigotimes_{j=1}^{n} \mathcal{H}_j. \tag{9}$$

Decompose $\ker(\widetilde{P}_{\overline{J}})$ to a direct sum $V \oplus (\ker(\widetilde{P}_{\overline{J}}) \cap \ker(\widetilde{P}_J))$, and decompose C_1/C_2 to $W \oplus V \oplus \cap \ker(\widetilde{P}_J)$. Let $\mathcal{G}(J)$ to be the complex linear space spanned by $\{|\vec{s}\rangle \mid f(\vec{s}) \in V\}$. We have $\dim \mathcal{G}(J) = |\widetilde{P}_J(\ker(\widetilde{P}_{\overline{J}}))|$ because

$$\begin{array}{rl} & \dim \widetilde{P}_J(\ker(\widetilde{P}_{\overline{J}})) \\ = & \dim \ker(\widetilde{P}_{\overline{J}}) - \dim \ker(\widetilde{P}_{\overline{J}}) \cap \ker(\widetilde{P}_J) \\ = & \dim V. \end{array} \tag{10}$$

The space $\bigotimes_{i=1}^{\dim C_1 - \dim C_2} \mathcal{G}_i$ can be decomposed as $\mathcal{G}(J) \otimes \mathcal{G}_{\mathrm{rest}}$, where $\mathcal{G}_{\mathrm{rest}}$ is the complex linear space spanned by $\{|\vec{s}_{KW}\rangle \mid f(\vec{s}_{KW}) \in W \oplus \ker(\widetilde{P_J})\}$, and $|\vec{s}_J\rangle \otimes |\vec{s}_W + \vec{s}_K\rangle \in \mathcal{G}(J) \otimes \mathcal{G}_{\mathrm{rest}}$ is identified with $|\vec{s}\rangle \in \bigotimes_{i=1}^{\dim C_1 - \dim C_2} \mathcal{G}_i$ for $\vec{s} = \vec{s}_J + \vec{s}_W + \vec{s}_K$ with $\vec{s}_J \in f^{-1}(V)$, $\vec{s}_W \in f^{-1}(W)$ and $\vec{s}_K \in f^{-1}(\ker(\widetilde{P_J}))$. This identification is a unitary map between $\mathcal{G}(J) \otimes \mathcal{G}_{\mathrm{rest}}$ and $\bigotimes_{i=1}^{\dim C_1 - \dim C_2} \mathcal{G}_i$, because it is linear and preserves the inner product.

Example 4 *We retain the notations from Example 2. Let* $J = \{1,2,3\}$ *and* $\overline{J} = \{4,5\}$. *Firstly we examine* $\ker(\widetilde{P_{\overline{J}}}) \subset C_1/C_2$. *When* $(s_1,s_2,s_3) = (2,1,0)$ *or* $(s_1,s_2,s_3) = (0,0,1)$, $P_{\overline{J}}(f(s_1,s_2,s_3)) = P_{\overline{J}}(C_2)$, *from which we see that* $\ker(\widetilde{P_{\overline{J}}})$ *is two-dimensional linear space spanned by* $f(2,1,0)$ *and* $f(0,0,1)$. *On the other hand,* $P_J(f(2,1,0)) \neq P_J(C_2)$ *and* $P_J(f(0,0,1)) = P_J(C_2)$, *which mean that* $\ker(\widetilde{P_{\overline{J}}}) \cap \ker(\widetilde{P_J})$ *is one-dimensional linear space spanned by* $f(0,0,1)$. *We also observe that* V *is the one-dimensional space spanned by* $f(2,1,0)$, *that* $\ker(\widetilde{P_J})$ *is the one-dimensional space spanned by* $f(0,0,1)$. *There is some freedom in choosing* W, *for example, we can choose* W *as the one-dimensional space spanned by* $f(1,0,0)$.

$\mathcal{G}(J)$ *is the* 7*-dimensional complex linear space spanned by* $\{|2a\rangle \otimes |a\rangle \otimes |0\rangle \mid a \in \mathbf{F}_7\}$, *while* $\mathcal{G}_{\mathrm{rest}}$ *is the* 49*-dimensional complex linear space spanned by* $\{|s_1\rangle \otimes |0\rangle \otimes |s_3\rangle \mid s_1, s_3 \in \mathbf{F}_7\}$.

In this section we shall prove that a set J of participants can reconstruct the part of the quantum secret (8) from (9). The reconstructed part is a state in $\mathcal{G}(J)$. By reordering indices we may assume $J = \{1, \ldots, |J|\}$. We also assume

$$\dim \widetilde{P_J}(\ker(\widetilde{P_{\overline{J}}})) > 0, \tag{11}$$

otherwise the set J can reconstruct no part of the secret by the proposed decoding procedure.

The restriction of $\widetilde{P_J} \circ f$ to V is injective by the definition of V. This and the definitions of V and W imply that there exists an $\mathbf{F}_q$-linear isomorphism g_1 from $P_J(C_1)/P_J(C_2)$ to $\mathbf{F}_q^{\dim P_J(C_1) - \dim P_J(C_2)}$ with the following condition. When we write $\vec{s} = \vec{s}_J + \vec{s}_W + \vec{s}_K$ in the same way as the previous paragraph for $\vec{s} \in \mathbf{F}_q^{\dim C_1 - \dim C_2}$ then $g_1(\widetilde{P_J}(f(\vec{s})) = (\vec{s}_J, \vec{s}_W) \in \mathbf{F}_q^{\dim P_J(C_1) - \dim P_J(C_2)}$. If (2) holds then we have $V = C_1/C_2$ and we regard $\vec{s}_W$ and $\vec{s}_K$ as $\vec{0}$ and $\vec{s}_J$ as $\vec{s}$. Observe that g_1 is inverting the restriction of $\widetilde{P_J} \circ f$ to V.

On the other hand, there also exists an $\mathbf{F}_q$-linear epimorphism g_2 from $P_J(C_1)$ to $\mathbf{F}_q^{\dim P_J(C_2 \cap \ker(P_{\overline{J}}))}$ that is one-to-one on every coset belonging to the factor linear space $P_J(C_1)/P_J(C_2 \cap \ker(P_{\overline{J}}))$. The above map can be constructed as follows: Find a direct sum decomposition of $P_J(C_1) = P_J(C_2 \cap \ker(P_{\overline{J}})) \oplus U$ For $\vec{x} \in P_J(C_1)$, find a decomposition $\vec{x} = \vec{x}_1 + \vec{x}_2$ such that $\vec{x}_1 \in P_J(C_2 \cap \ker(P_{\overline{J}}))$ and $\vec{x}_2 \in U$. Then map $\vec{x}_1$ by a some fixed linear isomorphism from $P_J(C_2 \cap \ker(P_{\overline{J}}))$ to $\mathbf{F}_q^{\dim P_J(C_2 \cap \ker(P_{\overline{J}}))}$, while ignoring $\vec{x}_2$. Observe that g_2 is extracting the $P_J(C_2 \cap \ker(P_{\overline{J}}))$-component.

By a construction similar to g_2, there also exists an $\mathbf{F}_q$-linear epimorphism g_3 from $P_J(C_1)/P_J(C_2 \cap \ker(P_{\overline{J}}))$ to $\mathbf{F}_q^{\dim P_J(C_2) - \dim P_J(C_2 \cap \ker(P_{\overline{J}}))}$ that is one-to-one on on every coset belonging to the factor linear space $P_J(C_1)/P_J(C_2)$ such that the value of g_3 is determined by $\vec{s}_W$, $\vec{s}_K$, and $P_{\overline{J}}(\vec{x})$ independently of $\vec{s}_J$. Observe also that g_3 is extracting the $P_J(C_2)$-component from the factor linear space $P_J(C_1)/P_J(C_2 \cap \ker(P_{\overline{J}}))$.

Consider the $\mathbf{F}_q$-linear map g_4 from $P_J(C_1)$ to $\mathbf{F}_q^{\dim P_J(C_1)}$ sending $\vec{v} \in P_J(C_1)$ to $(g_1(\vec{v} + P_J(C_2)), g_2(\vec{v}), g_3(\vec{v} + P_J(C_2 \cap \ker(P_{\overline{J}}))))$. We see that g_4 is an $\mathbf{F}_q$-linear isomorphism because it is surjective and the domain and the image of g_4 have the same dimension.

For $\vec{v} \in P_J(C_1)$, we can construct a unitary operation sending $|\vec{v}\rangle \in \bigotimes_{j=1}^{|J|} \mathcal{H}_j$ to $|g_4(\vec{v}), \vec{0}\rangle \in \bigotimes_{j=1}^{|J|} \mathcal{H}_j$, where $\vec{0}$ is the zero vector of length $|J| - \dim P_J(C_1)$. Since this unitary operation does not change $\mathcal{H}_{|J|+1}, \ldots, \mathcal{H}_n$, it can be executed only by the first to the $|J|$-th participants. Applying the unitary operation to (9) gives

$$\begin{aligned} \sum_{\vec{s} \in \mathbf{F}_q^{\dim C_1 - \dim C_2}} \alpha(\vec{s}) \frac{1}{\sqrt{|C_2|}} \sum_{\vec{x} \in f(\vec{s})} |\vec{s}_J, \vec{s}_W, \\ g_2(P_J(\vec{x})), g_3(P_J(\vec{x}) + P_J(C_2 \cap \ker(P_{\overline{J}}))), \vec{0}, P_{\overline{J}}(\vec{x})\rangle. \end{aligned} \tag{12}$$

$g_2(P_J(\vec{x}))$ can become any vector in $\mathbf{F}_q^{\dim P_J(C_2 \cap \ker(P_{\overline{J}}))}$ independently of $\vec{s}_J$, $\vec{s}_W$, $\vec{s}_K$ and $P_{\overline{J}}(\vec{x})$. Hereafter we denote $g_2(P_J(\vec{x}))$ by $\vec{u}_1$. For a fixed $\vec{s} \in \mathbf{F}_q^{\dim C_1 - \dim C_2}$ $P_{\overline{J}}(\vec{x})$ can become any vector in the coset $\widetilde{P_{\overline{J}}}(f(\vec{s})) \in P_{\overline{J}}(C_1)/P_{\overline{J}}(C_2)$, and $\vec{s}_W$ determines which coset of $P_{\overline{J}}(C_1)/P_{\overline{J}}(C_2)$ contains $P_{\overline{J}}(\vec{x})$ independently of $\vec{s}_J$, $\vec{s}_K$ and $\vec{u}_1$. Hereafter we denote the coset $\widetilde{P_{\overline{J}}}(f(\vec{s})) = P_{\overline{J}}(\vec{x}) + P_{\overline{J}}(C_2)$ by $g_5(\vec{s}_W)$. By the definition of g_3, $g_3(P_J(\vec{x}) + P_J(C_2 \cap \ker(P_{\overline{J}})))$ is determined by only $\vec{s}_W$, $\vec{s}_K$ and $P_{\overline{J}}(\vec{x})$, that is, independent of $\vec{s}_J$. Hereafter we denote $g_3(P_J(\vec{x}) + P_J(C_2 \cap \ker(P_{\overline{J}})))$ by $g_6(\vec{s}_W, \vec{s}_K, P_{\overline{J}}(\vec{x}))$. By using these notations we can rewrite (12) as

$$\sum_{\vec{s} \in \mathbf{F}_q^{\dim C_1 - \dim C_2}} \alpha(\vec{s}) |\vec{s}_J\rangle \frac{1}{\sqrt{|C_2|}} \sum_{\substack{\vec{u}_1 \in \mathbf{F}_q^{\dim P_J(C_2 \cap \ker(P_{\overline{J}}))} \\ \vec{u}_2 \in g_5(\vec{s}_W)}} |\vec{s}_W, \vec{u}_1, g_6(\vec{s}_W, \vec{s}_K, \vec{u}_2), \vec{0}, \vec{u}_2\rangle, \tag{13}$$

which means that the part $|\vec{s}_J\rangle$ of the quantum secret (8) is reconstructed but in general entangled with the rest of quantum system.

If the quantum secret is a product state written as

$$\sum_{\vec{s}\in\mathbf{F}_q^{\dim C_1-\dim C_2}} \alpha(\vec{s})|\vec{s}\rangle = \left(\sum_{\vec{s}_J\in V}\alpha(\vec{s}_J)|\vec{s}_J\rangle\right)\otimes\left(\sum_{\vec{s}_W,\vec{s}_K}\alpha(\vec{s}_W,\vec{s}_K)|\vec{s}_W,\vec{s}_K\rangle\right)$$

then (13) can be written as

$$\left(\sum_{\vec{s}_J\in V}\alpha(\vec{s}_J)|\vec{s}_J\rangle\right)\otimes\left(\sum_{\vec{s}_W,\vec{s}_K}\alpha(\vec{s}_W,\vec{s}_K)\frac{1}{\sqrt{|C_2|}}\sum_{\substack{\vec{u}_1\in\mathbf{F}_q^{\dim P_J(C_2\cap\ker(P_{\overline{J}}))}\\ \vec{u}_2\in g_5(\vec{s}_W)}}|\vec{s}_W,\vec{u}_1,g_6(\vec{s}_W,\vec{s}_K,\vec{u}_2),\vec{0},\vec{u}_2\rangle\right),$$

and the reconstructed secret is not entangled with the rest of quantum system.

Observe also that the number of qudits in the reconstructed part is $\dim V = \dim\widetilde{P}_J(\ker(\widetilde{P_{\overline{J}}}))$ and if (2) holds then the entire secret is reconstructed. Because the complement of any qualified set is forbidden by [11, Proposition 3], we see that the set $\overline{J}$ of participants has no information on the quantum secret (8) if (2) holds. This finishes the proof of Item 2 in Theorem 1. ∎

Example 5 *We retain the notations from Example 4. We have* $J = \{1,2,3\}$, $\dim P_J(C_1) = 3$, *and* $\dim P_J(C_2) = 1$. $\dim P_J(C_1)/P_J(C_2) = 2$.

When we express

$$\vec{s} = \underbrace{a(2,1,0)}_{=\vec{s}_J} + \underbrace{s_3(0,0,1)}_{=\vec{s}_K} + \underbrace{s_1(1,0,0)}_{=\vec{s}_W},$$

and fix r in (7), the index vector $\vec{x}$ in (7) becomes

$$\begin{aligned}\vec{x} &= (r+a+3s_1+6s_3, r+5s_1+6s_3, r+6a+6s_1+6s_3,\\ &\qquad r+3a+s_1+s_3, r+3a+4s_1+s_3).\end{aligned}$$

$g_1((x_1,x_2,x_3)+P_J(C_2)) = (3x_2-x_1-2x_3,\ 2x_2-x_1-x_3) = (a,\ s_1)$. *We have* $C_2\cap\ker(P_{\overline{J}}) = \{0\}$ *and g_2 is the zero map. We have* $g_3(x_1,x_2) = 2x_1 - x_3 =$

$r + 3a + 6s_3$ and $g_4(x_1, x_2) = (a, s_1, r + 3a + 6s_3)$. Therefore, after applying the proposed decoding procedure, the state (7) of encoded shares becomes

$$\begin{aligned} & \frac{1}{\sqrt{7}} \sum_{r \in \mathbf{F}_7} |a, s_1, r + 3a + 6s_3, r + 3a + s_1 + s_3, r + 3a + 4s_1 + s_3\rangle \\ = \quad & \frac{1}{\sqrt{7}} \sum_{r' \in \mathbf{F}_7} |a, s_1, r' + 6s_3, r' + s_1 + s_3, r' + 4s_1 + s_3\rangle \end{aligned}$$

where $r' = r + 3a$.

We see that s_1 determines, independently of both a and s_3, the coset $\{(r' + s_1 + s_3, r' + 4s_1 + s_3) \mid r' \in \mathbf{F}_7\}$, which is $g_5(\vec{s}_W)$. $P_{\overline{J}}(\vec{x}) = (r' + s_1 + s_3, r' + 4s_1 + s_3)$, s_1 and s_3 uniquely determine $g_3(x_1, x_2, x_3) = r' + 6s_3$ which is g_6.

4 Holevo Information and Coherent Information of a Set of Shares

4.1 Holevo Information

In this section we prove that both (3) and (4) are necessary for J to be a qualified set. We use the Holevo information [10] defined as follows. Let $\mathcal{S}_{\text{in}}$ and $\mathcal{S}_{\text{out}}$ be sets of density matrices, Γ a completely positive trace-preserving map from $\mathcal{S}_{\text{in}}$ to $\mathcal{S}_{\text{out}}$, $\{\rho_1, \ldots, \rho_m\} \subset \mathcal{S}_{\text{in}}$, and P a probability distribution on $\{\rho_1, \ldots, \rho_m\}$. The Holevo information is defined as

$$K(P, \{\rho_1, \ldots, \rho_m\}, \Gamma) = H\left(\sum_{i=1}^{m} P(\rho_i)\Gamma(\rho_i)\right) - \sum_{i=1}^{m} P(\rho_i) H(\Gamma(\rho_i)), \tag{14}$$

where $H(\cdot)$ denotes the von Neumann entropy counted in $\log_q$. The Holevo information essentially expresses the classical information that can be transferred over Γ [10].

Let Γ_J be the completely positive trace-preserving map from $\mathcal{S}(\bigotimes_{i=1}^{\dim C_1 - \dim C_2} \mathcal{G}_i)$ to $\mathcal{S}(\bigotimes_{j \in J} \mathcal{H}_j)$ induced by the encoding procedure proposed in Section 2, where $\mathcal{S}(\cdot)$ denotes the set of density matrices on a complex space $\cdot$. By K_J we denote

$$K(\text{uniform distribution}, \{|\vec{s}\rangle\langle\vec{s}| \mid \vec{s} \in \mathrm{F}_q^{\dim C_1 - \dim C_2}\}, \Gamma_J). \tag{15}$$

By [11, Theorem 1] if

$$K_J < \dim C_1 - \dim C_2 \tag{16}$$

then J is not a qualified set. The encoding procedure in Section 2 is a pure state scheme [11, Section 2], that is, the quantum state of all the shares is pure if the encoded quantum secret is pure. By [11, Proposition 3], if $\overline{J}$ is not a forbidden set, then J is not a qualified set. By [11, Theorem 1] if

$$K_{\overline{J}} > 0 \tag{17}$$

then $\overline{J}$ is not a forbidden set.

We shall prove the next proposition. By (3), (4), (16) and (17), Proposition 6 implies that both (3) and (4) are necessary for J to be a qualified set.

Proposition 6

$$K_J = \dim P_J(C_1) - \dim P_J(C_2). \tag{18}$$

Proof. $\Gamma_J(|\vec{s}\rangle\langle\vec{s}|)$ is the partial trace of (9) over $\bigotimes_{j\in\overline{J}} \mathcal{H}_j$. By the definition of partial trace

$$\begin{aligned}
& \Gamma_J(|\vec{s}\rangle\langle\vec{s}|) \\
= & \frac{1}{|C_2|} \sum_{\vec{x}_1,\vec{x}_2\in f(\vec{s})} |P_J(\vec{x}_1)\rangle\langle P_J(\vec{x}_2)| \underbrace{\langle P_{\overline{J}}(\vec{x}_1)|P_{\overline{J}}(\vec{x}_2)\rangle}_{=1\Leftrightarrow \vec{x}_2\in\vec{x}_1+\ker(P_{\overline{J}})} \\
= & \frac{1}{|C_2|} \sum_{\vec{u}\in P_{\overline{J}}(f(\vec{s}))} \sum_{\vec{x}_1\in f(\vec{s})\cap P_{\overline{J}}^{-1}(\vec{u})} \sum_{\vec{x}_2\in f(\vec{s})\cap P_{\overline{J}}^{-1}(\vec{u})} |P_J(\vec{x}_1)\rangle\langle P_J(\vec{x}_2)| \\
= & \frac{1}{|C_2|} \sum_{\vec{u}\in P_{\overline{J}}(f(\vec{s}))} \left(\sum_{\vec{x}_1\in f(\vec{s})\cap P_{\overline{J}}^{-1}(\vec{u})} |P_J(\vec{x}_1)\rangle \right) \left(\sum_{\vec{x}_2\in f(\vec{s})\cap P_{\overline{J}}^{-1}(\vec{u})} \langle P_J(\vec{x}_2)| \right) \\
= & \frac{1}{|C_2|} \sum_{\vec{u}\in P_{\overline{J}}(f(\vec{s}))} \left(\sum_{\vec{x}_1\in f(\vec{s})\cap((\vec{0},\vec{u})+\ker(P_{\overline{J}}))} |P_J(\vec{x}_1)\rangle \right) \left(\sum_{\vec{x}_2\in f(\vec{s})\cap((\vec{0},\vec{u})+\ker(P_{\overline{J}}))} \langle P_J(\vec{x}_2)| \right).
\end{aligned} \tag{19}$$

For $\vec{u}_1, \vec{u}_2 \in P_{\overline{J}}(f(\vec{s}))$, if $f(\vec{s}) \cap ((\vec{0}, \vec{u}_1) + \ker(P_{\overline{J}})) = f(\vec{s}) \cap ((\vec{0}, \vec{u}_2) + \ker(P_{\overline{J}}))$ then $\vec{x}_1$ and $\vec{x}_2$ in (19) are taken over the same set $P_J(\vec{x}) + P_J(C_2 \cap \ker(P_{\overline{J}}))$, where $\vec{x}$ is any vector in $f(\vec{s}) \cap ((\vec{0}, \vec{u}_1) + \ker(P_{\overline{J}}))$. Otherwise $\vec{x}_1$ and $\vec{x}_2$ in (19) are taken over two disjoint sets in $P_J(f(\vec{s}))$. So (19) is equal to

$$\frac{1}{|C_2|} \sum_{A\in P_J(f(\vec{s}))/\sim} \left(\sum_{\vec{v}\in A} |\vec{v}\rangle \right) \left(\sum_{\vec{v}\in A} \langle\vec{v}| \right), \tag{20}$$

where $\sim$ is the equivalence relation that defines $\vec{v}_1, \vec{v}_2 \in P_J(\mathbf{F}_q^n)$ to be equivalent if $\vec{v}_1 \in \vec{v}_2 + P_J(C_2 \cap \ker(P_{\overline{J}}))$. (20) is an equal mixture of $|P_J(C_2)/P_J(C_2 \cap \ker(P_{\overline{J}}))|$ projection matrices to non-overlapping orthogonal spaces, therefore its von Neumann entropy is $\dim P_J(C_2) - \dim P_J(C_2 \cap \ker(P_{\overline{J}}))$, which is the second term in the right hand side of (14).

By (20), the density matrix of the first term in RHS of of (14) is

$$\begin{aligned} &\frac{1}{q^{\dim C_1 - \dim C_2}} \sum_{\vec{s} \in \mathbf{F}_q^{\dim C_1 - \dim C_2}} \frac{1}{|C_2|} \sum_{A \in P_J(f(\vec{s}))/\sim} \left(\sum_{\vec{v} \in A} |\vec{v}\rangle \right) \left(\sum_{\vec{v} \in A} \langle \vec{v}| \right) \\ = \;& \frac{1}{|C_1|}, \sum_{A \in P_J(C_1)/P_J(C_2 \cap \ker(P_{\overline{J}}))} \left(\sum_{\vec{v} \in A} |\vec{v}\rangle \right) \left(\sum_{\vec{v} \in A} \langle \vec{v}| \right). \end{aligned} \tag{21}$$

The von Neumann entropy of (21) is

$$\dim P_J(C_1) - \dim P_J(C_2 \cap \ker(P_{\overline{J}})) \tag{22}$$

by the same argument as the last paragraph. By (14) $K_J = \dim P_J(C_1) - \dim P_J(C_2)$. ■

4.2 Coherent Information

We use the same notation as (14). Denote by Γ_E the channel to the environment so that any pure state is mapped to a pure state by $\Gamma \otimes \Gamma_E$. The channel to the environment for Γ_J is $\Gamma_{\overline{J}}$. Then the coherent information of the input state ρ and the channel Γ is defined by [10]

$$H(\Gamma(\rho)) - H(\Gamma_E(\rho)). \tag{23}$$

Equation (23) can become negative. The quantum capacity is expressed by the maximum of the coherent information over ρ [5].

The coherent information of Γ_J and the completely mixed secret $\frac{1}{q^{\dim C_1 - \dim C_2}} \sum_{\vec{s} \in \mathbf{F}_q^{\dim C_1 - \dim C_2}} |\vec{s}\rangle\langle\vec{s}|$ is (22) subtracted by (22) with J substituted by $\overline{J}$. Therefore the coherent information is

$$\dim P_J(C_1) - \dim C_2 \cap \ker(P_{\overline{J}}) - (\dim P_{\overline{J}}(C_1) - \dim C_2 \cap \ker(P_J)). \tag{24}$$

We consider to maximize (24) by replacing C_1 by D such that $C_2 \subset D \subset C_1$. This amounts to maximize (23) over the quantum state completely mixed over the subspace spanned by $\{|\vec{s}\rangle \mid f(\vec{s}) \subset D\}$.

Lemma 7 *Let D be as above. Define*

$$D' = C_2 + (D \cap \ker(P_{\overline{J}})).$$

Then we have

$$\begin{aligned} & \dim P_J(D) - \dim C_2 \cap \ker(P_{\overline{J}}) - (\dim P_{\overline{J}}(D) - \dim C_2 \cap \ker(P_J)) \\ = & \dim P_J(D') - \dim C_2 \cap \ker(P_{\overline{J}}) - (\dim P_{\overline{J}}(D') - \dim C_2 \cap \ker(P_J)). \quad (25) \end{aligned}$$

Proof. Let $D = D' \oplus D''$. Then $\dim D'' = \dim P_{\overline{J}}(D'')$ because $D'' \cap \ker(P_{\overline{J}}) = \{\vec{0}\}$. Therefore the D'' component in D does not help to increase the value of (24). Thus D' yields the same value for (24) as D and we have (25). ∎

So we see that $D = C_2 + (C_1 \cap \ker(P_{\overline{J}}))$ maximizes the coherent information to its maximum value

$$\begin{aligned} & \dim P_J(C_2 + (C_1 \cap \ker(P_{\overline{J}}))) - \dim C_2 \cap \ker(P_{\overline{J}}) \\ & -(\underbrace{\dim P_{\overline{J}}(C_2 + (C_1 \cap \ker(P_{\overline{J}}))}_{=\dim P_{\overline{J}}(C_2)} - \dim C_2 \cap \ker(P_J)) \\ = & \dim P_J(C_2 + (C_1 \cap \ker(P_{\overline{J}}))) - \underbrace{(\dim C_2 \cap \ker(P_{\overline{J}}) + \dim P_{\overline{J}}(C_2) - \dim C_2 \cap \ker(P_J))}_{=\dim P_J(C_2)} \\ = & \dim \widetilde{P}_J(\ker \widetilde{P}_{\overline{J}}). \end{aligned}$$

We remark that the proposed decoding procedure in Section 3 reconstructs precisely that number of qudits in the secret.

5 Analysis of the Conventional Scheme

In this section we show that the conventional quantum ramp secret SS [11] can be regarded as a special case of the proposed construction, and its qualified and forbidden sets can be identified by Theorem 1. Let $\alpha_1, \ldots, \alpha_n$ be pairwise distinct nonzero[1] elements in $\mathbf{F}_q$, which correspond to $x_1, \ldots, x_n$ in [11]. Denote $(\alpha_1, \ldots, \alpha_n)$ by $\vec{\alpha}$. Let $\vec{v} \in (\mathbf{F}_q \setminus \{0\})^n$. Then the generalized Reed-Solomon code $\mathrm{GRS}_{n,k}(\vec{\alpha}, \vec{v})$ is [9, Section 10.§8]

$$\{(v_1 h(\alpha_1), \ldots, v_n h(\alpha_n)) \mid \deg h(x) \leq k-1\}, \quad (26)$$

[1] In [11] $\alpha_i = 0$ was not explicitly prohibited, but an author of [11] informed that α_i must be nonzero for all $i = 1, \ldots, n$.

where $h(x)$ is a univariate polynomial over $\mathbf{F}_q$. Let $\vec{1} = (1, \ldots, 1) \in \mathbf{F}_q^n$ and $\vec{\alpha}^L = (\alpha_1^L, \ldots, \alpha_n^L) \in \mathbf{F}_q^n$. The conventional scheme [11] is a special case of the proposed construction with $C_1 = \mathrm{GRS}_{n,k}(\vec{\alpha}, \vec{1})$ and $C_2 = \mathrm{GRS}_{n,k-L}(\vec{\alpha}, \vec{\alpha}^L)$. Observe that $C_2 \subsetneq C_1$, $\dim C_1 = k$, and $\dim C_2 = k - L$. By the property of the generalized Reed-Solomon codes (see e.g. [9, Section 11.§4]), any subset $J \subseteq \{1, \ldots, n\}$ satisfies both (3) and (4) if $|J| \geq \dim C_1$ and $|\overline{J}| \leq \dim C_2$. Observe that the original restriction $n = \dim C_1 + \dim C_2$ [11] is removed here.

6 Algebraic Geometric Construction

In this section we give a construction of $C_1 \supset C_2$ based on algebraic geometry (AG) codes. For terminology and mathematical notions of AG codes, please refer to [14]. Let $F/\mathbf{F}_q$ be an algebraic function field of one variable over $\mathbf{F}_q$, $P_1, \ldots, P_n$ pairwise distinct places of degree one in F, and G_1, G_2 divisors of F whose supports contain none of $P_1, \ldots, P_n$. We assume $G_1 \geq G_2$. Denote by $\mathcal{L}(G_1)$ the $\mathbf{F}_q$-linear space associated with G_1. The functional AG code associated with G_1, $P_1, \ldots, P_n$ is defined as

$$C(G_1, P_1, \ldots, P_n) = \{(f(P_1), \ldots, f(P_n)) \mid f \in \mathcal{L}(G_1)\}.$$

Since $G_1 \geq G_2$ we have $C(G_1, P_1, \ldots, P_n) \supseteq C(G_2, P_1, \ldots, P_n)$. We further assume $C(G_1, P_1, \ldots, P_n) \neq C(G_2, P_1, \ldots, P_n)$.

Theorem 8 *The ramp quantum SS constructed from $C(G_1, P_1, \ldots, P_n) \supsetneq C(G_2, P_1, \ldots, P_n)$ encodes $\dim C(G_1, P_1, \ldots, P_n) - \dim C(G_2, P_1, \ldots, P_n)$ qudits to n shares. We have*

$$\begin{aligned} & \dim C(G_1, P_1, \ldots, P_n) - \dim C(G_2, P_1, \ldots, P_n) \\ \geq\ & \deg G_1 - \deg G_2 - g(F), \end{aligned} \tag{27}$$

where $g(F)$ denotes the genus of F. A set $J \subseteq \{1, \ldots, n\}$ is a qualified set and its complement $\overline{J}$ is a forbidden set if

$$|J| \geq \max\{1 + \deg G_1, n - (\deg G_2 - 2g(F) + 1)\}. \tag{28}$$

Proof. Equation (27) follows just from

$$\dim C(G_1, P_1, \ldots, P_n) = \dim \mathcal{L}(G_1) - \dim \mathcal{L}(G_1 - P_1 - \cdots - P_n), \tag{29}$$

and the Riemann-Roch theorem [14]

$$\deg G_1 - g(F) + 1 \leq \dim \mathcal{L}(G_1) \leq \max\{0, \deg G_1 + 1\}, \tag{30}$$

where the left inequality of (30) becomes equality if

$$\deg G_1 \geq 2g(F) - 1. \tag{31}$$

Firstly we claim that (3) and (4) hold if

$$|J| \geq 1 + \deg G_1, \tag{32}$$
$$|\overline{J}| \leq \deg G_2 - 2g(F) + 1. \tag{33}$$

By reordering indices we may assume that $J = \{1, \ldots, |J|\}$. Observe that

$$P_J(C(G_1, P_1, \ldots, P_n)) = C(G_1, P_1, \ldots, P_{|J|}). \tag{34}$$

If (32) holds then by (30) we have $\mathcal{L}(G_1 - P_1 - \cdots - P_{|J|}) = \{0\}$, which means that $\mathcal{L}(G_1)$ is isomorphic to $C(G_1, P_1, \ldots, P_{|J|})$ as an $\mathbf{F}_q$-linear space by (29). By the same argument we also see that $\mathcal{L}(G_1)$ is isomorphic to $C(G_1, P_1, \ldots, P_n)$. Thus we have seen that (32) implies (3).

If (33) holds then

$$\deg(G_2 - P_{|J|+1} - \cdots - P_n) \geq 2g(F) - 1,$$

which implies by (31)

$$\dim \mathcal{L}(G_2 - P_{|J|+1} - \cdots - P_n) = \deg G_2 - |\overline{J}| - g(F) + 1. \tag{35}$$

By the same argument

$$\dim \mathcal{L}(G_2) = \deg G_2 - g(F) + 1. \tag{36}$$

Equations (29), (35) and (36) imply $\dim C(G_2, P_{|J|+1}, \ldots, P_n) = |\overline{J}|$, which in turn implies $C(G_2, P_{|J|+1}, \ldots, P_n) = \mathbf{F}_q^{|\overline{J}|}$. Therefore we see that (33) implies (4).

Finally noting (28) $\Rightarrow$ (32) and (33) finishes the proof. ∎

Remark 9 *As the generalized Reed-Solomon codes is a special case of AG codes with $g(F) = 0$ [14], Section 5 can also be deduced from Theorem 8 instead of using [9, Section 11.§4].*

Theorem 10 *We retain notations from Theorem 8 and assume* $\deg G_1 < n$. *The number (1) of qudits in quantum secret that can be decoded by J is*

$$\dim \frac{\mathcal{L}(G_1 - \sum_{j\in\overline{J}} P_j) + \mathcal{L}(G_2)}{(\mathcal{L}(G_1 - \sum_{j\in\overline{J}} P_j) + \mathcal{L}(G_2)) \cap (\mathcal{L}(G_1 - \sum_{j\in J} P_j) + \mathcal{L}(G_2))}. \tag{37}$$

Proof. Equation (1) is equal to

$$\dim \ker(\widetilde{P_{\overline{J}}}) - \dim \ker(\widetilde{P_J}) \cap \ker(\widetilde{P_{\overline{J}}}). \tag{38}$$

Since we assume $\deg G_1 < n$, the evaluation map $h \in \mathcal{L}(G_1) \mapsto (h(P_1), \ldots, h(P_n)) \in \mathbf{F}_q^n$ is injective and we can deal with the space of functions in $\mathcal{L}(G_1)$ to count the dimensions of (38).

For $h_1 + \mathcal{L}(G_2) \in \mathcal{L}(G_1)/\mathcal{L}(G_2)$, its corresponding coset belongs to $\ker(\widetilde{P_{\overline{J}}})$ if and only if there exists $h_2 \in \mathcal{L}(G_2)$ such that $h_1(P_j) - h_2(P_j) = 0$ for all $j \in \overline{J}$, which is equivalent to $h_1 - h_2 \in \mathcal{L}(G_1 - \sum_{j\in\overline{J}} P_j)$. In other words, the coset $h_1 + \mathcal{L}(G_2)$ satisfies the above condition if and only if there exists $h_1' \in \mathcal{L}(G_1 - \sum_{j\in\overline{J}} P_j)$ such that $h_1 \equiv h_1' \pmod{\mathcal{L}(G_2)}$. The dimension of space of cosets $h_1 + \mathcal{L}(G_2)$ with the above condition is given by

$$\dim \frac{\mathcal{L}(G_1 - \sum_{j\in\overline{J}} P_j) + \mathcal{L}(G_2)}{\mathcal{L}(G_2)}. \tag{39}$$

Moreover, while satisfying the condition of the last paragraph, the coset corresponding to $h_1 + \mathcal{L}(G_2)$ belongs to $\ker(\widetilde{P_J})$ if and only if there exists another $h_1'' \in \mathcal{L}(G_1 - \sum_{j\in J} P_j)$ such that $h_1 \equiv h_1'' \pmod{\mathcal{L}(G_2)}$. The dimension of space of cosets $h_1 + \mathcal{L}(G_2)$ with the above two conditions is given by

$$\dim \frac{(\mathcal{L}(G_1 - \sum_{j\in\overline{J}} P_j) + \mathcal{L}(G_2)) \cap (\mathcal{L}(G_1 - \sum_{j\in J} P_j) + \mathcal{L}(G_2))}{\mathcal{L}(G_2)}. \tag{40}$$

By (38), subtracting (40) from (39) gives (37). ∎

7 Conclusion

We have shown that a quantum ramp secret sharing scheme can be constructed from any nested pair of linear codes, and also shown necessary and sufficient conditions for the qualified and the forbidden sets as Theorem 1. A construction of nested linear codes is given by the algebraic geometry in Theorem 8. The following issues are future research agenda.

What is a better construction of $C_1 \supsetneq C_2$ than Theorem 8 when $q < n$? In particular, (33) should use both divisors G_1 and G_2 because (3) and (4) use both of nested linear codes. Also, J corresponds to a set of $\mathbf{F}_q$-rational points on an algebraic curve when AG codes are used, but only the size of J is taken into account in (33). The geometry of J should also be taken into account. We shall investigate them in future.

Acknowledgment

The author would like to thank Prof. Tomohiro Ogawa for clarification of [11]. This research is partly supported by the National Institute of Information and Communications Technology, Japan, and by the JSPS Grant Nos. 23246071 and 26289116.

References

[1] G. R. Blakley and C. Meadows. Security of ramp schemes. In *Advances in Cryptology–CRYPTO'84*, volume 196 of *Lecture Notes in Computer Science*, pages 242–269. Springer-Verlag, 1985. `doi:10.1007/3-540-39568-7_20`.

[2] H. Chen, R. Cramer, S. Goldwasser, R. de Haan, and V. Vaikuntanathan. Secure computation from random error correccting codes. In *Advances in Cryptology–EUROCRYPT 2007*, volume 4515 of *Lecture Notes in Computer Science*, pages 291–310. Springer-Verlag, 2007. `doi:10.1007/978-3-540-72540-4_17`.

[3] R. Cleve, D. Gottesman, and H.-K. Lo. How to share a quantum secret. *Phys. Rev. Lett.*, 83(3):648–651, July 1999. arXiv:quant-ph/9901025, `doi:10.1103/PhysRevLett.83.648`.

[4] R. dela Cruz, A. Meyer, and P. Solé. Extension of Massey scheme for secret sharing. In *Proc. ITW 2010*, Dublin, Ireland, 2010. arXiv:1004.2795, `doi:10.1109/CIG.2010.5592719`.

[5] I. Devetak. The private classical capacity and quantum capacity of a quantum channel. *IEEE Trans. Inform. Theory*, 51(1):44–55, Jan. 2005. arXiv:quant-ph/0304127, doi:10.1109/TIT.2004.839515.

[6] G. D. Forney, Jr. Dimension/length profiles and trellis complexity of linear block codes. *IEEE Trans. Inform. Theory*, 40(6):1741–1752, Nov. 1994. doi:10.1109/18.340452.

[7] D. Gottesman. Theory of quantum secret sharing. *Phys. Rev. A*, 61(4):042311, Mar. 2000. arXiv:quant-ph/9910067, doi:10.1103/PhysRevA.61.042311.

[8] J. Kurihara, T. Uyematsu, and R. Matsumoto. Secret sharing schemes based on linear codes can be precisely characterized by the relative generalized Hamming weight. *IEICE Trans. Fundamentals*, E95-A(11):2067–2075, Nov. 2012. doi:10.1587/transfun.E95.A.2067.

[9] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. Elsevier, Amsterdam, 1977.

[10] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, UK, 2000.

[11] T. Ogawa, A. Sasaki, M. Iwamoto, and H. Yamamoto. Quantum secret sharing schemes and reversibility of quantum operations. *Phys. Rev. A*, 72(3):032318, Sept. 2005. arXiv:quant-ph/0505001, doi:10.1103/PhysRevA.72.032318.

[12] A. Shamir. How to share a secret. *Comm. ACM*, 22(11):612–613, 1979.

[13] A. D. Smith. Quantum secret sharing for general access structures. Jan. 2000. arXiv:quant-ph/0001087.

[14] H. Stichtenoth. *Algebraic Function Fields and Codes*. Springer-Verlag, Berlin, 1993.

[15] H. Yamamoto. Secret sharing system using (k, l, n) threshold scheme. *Electronics and Communications in Japan (Part I: Communications)*, 69(9):46–54, 1986. (the original Japanese version published in 1985). doi:10.1002/ecja.4410690906.