Geometric and Computational Approach to Classical and Quantum Secret Sharing

Ryutaroh Matsumoto[1], Diego Ruano[2]

[1] *Tokyo Institute of Technology, Japan, ryutaroh@rmatsumoto.org*
[2] *Aalborg University, Denmark, diego@math.aau.dk*

1 Introduction

Secret sharing (SS) [15] is a cryptographic scheme to encode a secret to multiple shares being distributed to participants, so that only qualified (or authorized) sets of participants can reconstruct the original secret from their shares. Traditionally both secret and shares were classical information (bits). Several authors [5, 7, 16] extended the traditional SS to a 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 the secret. By tolerating partial information leakage to unqualified sets, the size of shares can be smaller than that of the secret. Such an SS is called a ramp (or non-perfect) SS [2, 13, 17]. The quantum ramp SS was proposed by Ogawa et al. [14]. In their construction [14] as well as its improvement [18], the size of shares can be L times smaller relative to quantum secret than its previous construction [5, 7, 16], where L is the number of qudits in quantum secret.

Classical secret sharing is said to be linear if a linear combination of shares corresponds to the linear combination of the original secrets [4]. It is also known that every linear ramp secret sharing can be expressed by a nested pair of linear codes $C_2 \subset C_1 \subset \mathbf{F}_q^n$. On the other hand, a nest code pair $C_2 \subset C_1 \subset \mathbf{F}_q^n$ can also give a quantum secret sharing as described in [10]. A share set is said to be forbidden if it has no information about the secret. It is natural to express conditions for qualified and forbidden sets in terms of $C_2 \subset C_1$, and the following is known:

Theorem 1 *[1, 9, 10] Let $J \subseteq \{1, \ldots, n\}$, and define $P_J : \mathbf{F}_q^n \to \mathbf{F}_q^{|J|}$, $(x_1, \ldots, x_n) \mapsto (x_j : j \in J)$. We consider classical and quantum secret sharing constructed from $C_2 \subset C_1$. J can be regarded as a share set, and J is qualified in the classical secret sharing if and only if*

$$\dim P_J(C_1)/P_J(C_2) = \dim C_1/C_2, \tag{1}$$

and J is forbidden in the classical secret sharing if and only if

$$P_J(C_1) = P_J(C_2). \tag{2}$$

Let $\overline{J} = \{1, \ldots, n\} \setminus J$. In the quantum secret sharing, J is qualified if and only if

$$\textit{both} \begin{cases} \textit{(1) is true}, \\ P_{\overline{J}}(C_1) = P_{\overline{J}}(C_2) \end{cases} \quad \textit{i.e.,} \begin{cases} J \textit{ is classically qualified}, \\ \overline{J} \textit{ is classically forbidden} \end{cases} \tag{3}$$

hold, and J is forbidden if and only if $\overline{J}$ is qualified.

Since C_1 and C_2 are linear codes, it is natural to use algebraic geometry codes to construct C_1 and C_2 [3]. Let F be an algebraic function field of one variable with genus $g(F)$, $P_1, \ldots, P_n$ its rational places, $G_1 \geq G_2$ divisors whose support contain none of $P_1, \ldots, P_n$. Define $C(P_1 + \cdots + P_n, G_1) = \{(f(P_1), \ldots, f(P_n)) \mid f \in \mathscr{L}(G_1)\}$. By the Riemann-Roch theorem, for $C_1 = C(P_1 + \cdots + P_n, G_1)$ and $C_2 = C(P_1 + \cdots + P_n, G_2)$, it is straightforward to see

Theorem 2 *Equation (1) holds if*

$$|J| \geq 1 + \deg G_1. \tag{4}$$

Equation (2) holds if

$$|J| \leq \deg G_2 - 2g(F) + 1. \tag{5}$$

Equation (3) holds if

$$|J| \geq \max\{1 + \deg G_1, n - (\deg G_2 - 2g(F) + 1)\}. \tag{6}$$

The purpose of this note is to find sufficient conditions **less** demanding than (4)–(6) by using geometric properties of the set of points $\{P_j \mid j \in J\}$.

2 Geometric and Computational Analysis of Qualified and Forbidden Sets

2.1 Computational Approach

Fix a rational place Q arbitrarily. When $C_1 = C(P_1 + \cdots + P_n, G_1)$ and $C_2 = C(P_1 + \cdots + P_n, G_2)$, (1) holds

$$\begin{aligned}
&\Leftrightarrow \quad C(\sum_{j\in J} P_j, G_1)/C(\sum_{j\in J} P_j, G_2) \simeq C(P_1 + \cdots + P_n, G_1)/C(P_1 + \cdots + P_n, G_2) \\
&\Leftrightarrow \quad \ker(P_J) \cap C(P_1 + \cdots + P_n, G_1) = \ker(P_J) \cap C(P_1 + \cdots + P_n, G_2) \\
&\Leftrightarrow \quad C(\sum_{j\notin J} P_J, G_1 - \sum_{j\in J} P_j) = C(\sum_{j\notin J} P_J, G_2 - \sum_{j\in J} P_j) \\
&\Leftrightarrow \quad f_1 \in \mathscr{L}(G_1 - \sum_{j\in J} P_j) \Rightarrow \exists f_2 \in \mathscr{L}(G_2 - \sum_{j\in J} P_j) \text{ s.t. } f_1(P_j) = f_2(P_j) \forall j \notin J \\
&\Leftrightarrow \quad f_1 \in \mathscr{L}(G_1 - \sum_{j\in J} P_j) \Rightarrow \exists f_2 \in \mathscr{L}(G_2 - \sum_{j\in J} P_j) \text{ s.t. } f_1 - f_2 \in \mathscr{L}(G_1 - \sum_{j\notin J} P_j) \\
&\Leftrightarrow \quad \forall f_1 \in \mathscr{L}(G_1 - \sum_{j\in J} P_j), \exists f_2 \in \mathscr{L}(G_2 - \sum_{j\in J} P_j), \exists f_3 \in \mathscr{L}(G_1 - \sum_{j=1}^{n} P_j) \text{ s.t. } f_1 = f_2 + f_3 \\
&\Leftrightarrow \quad \mathscr{L}(G_1 - \sum_{j\in J} P_j) \subseteq \mathscr{L}(G_1 - \sum_{j=1}^{n} P_j) + \mathscr{L}(G_2 - \sum_{j\in J} P_j)
\end{aligned}$$

$$\Leftrightarrow \quad v_Q(\mathscr{L}(G_1 - \sum_{j\in J} P_j)) \subseteq v_Q(\mathscr{L}(G_1 - \sum_{j=1}^{n} P_j) + \mathscr{L}(G_2 - \sum_{j\in J} P_j))$$

$$\Leftarrow \quad v_Q(\mathscr{L}(G_1 - \sum_{j\in J} P_j)) \subseteq v_Q(\mathscr{L}(G_1 - \sum_{j=1}^{n} P_j)) \cup v_Q(\mathscr{L}(G_2 - \sum_{j\in J} P_j)). \tag{7}$$

For any rational place Q and any divisor G of F, $v_Q(\mathscr{L}(G))$ can be computed by **Gröbner bases** and the algorithm in [11], provided that the defining equations of F is in special position with respect to Q [6, 8, 12].

We turn our attention to (2). Equation (2) holds

$$\begin{aligned}
&\Leftrightarrow \quad C(\sum_{j\in J} P_j, G_1) = C(\sum_{j\in J} P_j, G_2) \\
&\Leftrightarrow \quad \forall f_1 \in \mathscr{L}(G_1), \exists f_2 \in \mathscr{L}(G_2) \text{ s.t. } f_1 - f_2 \in \mathscr{L}(-\sum_{j\in J} P_j + G_1) \\
&\Leftrightarrow \quad \forall f_1 \in \mathscr{L}(G_1), \exists f_2 \in \mathscr{L}(G_2), \exists f_3 \in \mathscr{L}(-\sum_{j\in J} P_j + G_1) \text{ s.t. } f_1 = f_2 + f_3 \\
&\Leftrightarrow \quad \mathscr{L}(G_1) = \mathscr{L}(G_2) + \mathscr{L}(G_1 - \sum_{j\in J} P_j) \\
&\Leftrightarrow \quad v_Q(\mathscr{L}(G_1)) = v_Q(\mathscr{L}(G_2) + \mathscr{L}(G_1 - \sum_{j\in J} P_j)) \\
&\Leftarrow \quad v_Q(\mathscr{L}(G_1)) = v_Q(\mathscr{L}(G_2)) \cup v_Q(\mathscr{L}(G_1 - \sum_{j\in J} P_j)).
\end{aligned} \tag{8}$$

A similar sufficient condition for (3) can be deduced from (4) and (5).

2.2 Explicit Sufficient Conditions

We explicitly write sufficient conditions for (7) and (8), and examine if they are easier to hold than (4) and (5) for one point AG codes with $G_1 = m_1 Q$ and $G_2 = m_2 Q$. For any divisor G, let $H_Q(G) = -v_Q(\mathscr{L}(G + \infty Q) \setminus \{0\})$. Observe that $H_Q(0)$ is the Weierstrass semigroup at Q. The conductor of $H_Q(G)$ is defined as $\min\{i \in H_Q(G) \mid i \leq j \in \mathbf{N} \Rightarrow j \in H_Q(G)\}$, which generalizes the conductor of the Weierstrass semigroup $H_Q(0)$.

Equation (7) holds if

$$\begin{aligned}
& v_Q(\mathscr{L}(m_1 Q - \sum_{j\in J} P_j) \setminus \{0\}) = \emptyset \\
\Leftrightarrow \quad & m_1 \leq \min H_Q(-\sum_{j\in J} P_j) - 1
\end{aligned} \tag{9}$$

We see that condition (9) is less demanding than (4), because $\min H_Q(-\sum_{j\in J} P_j) \geq |J|$.

Similarly, (8) holds if

$$m_2 \geq \text{the conductor of } H_Q(-\sum_{j\in J} P_j) - 1 \tag{10}$$

We also see that condition (10) is less demanding than (5), because the conductor of $H_Q(-\sum_{j\in J} P_j)$ is $\leq 2g(F)$. We can also make a similar improvement over (6): Condition (6) holds if

$$m_1 \leq \min H_Q(-\sum_{j\in J} P_j) - 1 \text{ and } m_2 \geq \text{the conductor of } H_Q(-\sum_{j\notin J} P_j) - 1.$$

In particular, for elliptic function fields ($g(F) = 1$),

$$(9) \quad \Leftrightarrow \quad \begin{cases} m_1 + 1 \leq |J| & \text{if } \exists f \in \mathscr{L}(\infty Q), (f)_0 = \sum_{j\in J} P_j, \\ m_1 \leq |J| & \text{otherwise} \end{cases} \tag{11}$$

$$(10) \quad \Leftrightarrow \quad \begin{cases} |J| \leq m_2 - 1 & \text{if } \exists f \in \mathscr{L}(\infty Q), (f)_0 = \sum_{j\in J} P_j, \\ |J| \leq m_2 & \text{otherwise} \end{cases} \tag{12}$$

Acknowledgment

The authors gratefully acknowledge the support from Japan Society for the Promotion of Science (Grant Nos. 23246071 and 26289116), from the Spanish MINECO (Grant No. MTM2012-36917-C03-03), the Danish Council for Independent Research (Grant No. DFF-4002-00367) and from the "Program for Promoting the Enhancement of Research Universities" at Tokyo Institute of Technology.

References

[1] T. Bains. Generalized Hamming weights and their applications to secret sharing schemes. Master's thesis, University of Amsterdam, Feb. 2008. supervised by R. Cramer, G. van der Geer, and R. de Haan.

[2] 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.

[3] H. Chen, R. Cramer, R. de Haan, and I. Cascudo Pueyo. Strongly multiplicative ramp schemes from high degree rational points on curves. In N. Smart, editor, *Advances in Cryptology – EUROCRYPT 2008*, volume 4965 of *Lecture Notes in Computer Science*, pages 451–470. Springer-Verlag, 2008. doi:10.1007/978-3-540-78967-3_26.

[4] H. Chen, R. Cramer, S. Goldwasser, R. de Haan, and V. Vaikuntanathan. Secure computation from random error correcting 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.

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

[6] O. Geil and R. Pellikaan. On the structure of order domains. *Finite Fields and Their Appl.*, 8:369–396, 2002.

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

[8] C. Heegard, J. Little, and K. Saints. Systematic encoding via Gröbner bases for a class of algebraic-geometric Goppa codes. *IEEE Trans. Inform. Theory*, 41(6):1752–1761, Nov. 1995.

[9] 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.

[10] R. Matsumoto. Coding theoretic construction of quantum ramp secret sharing. (version 4 or later), May 2014. arXiv:1405.0149v5.

[11] R. Matsumoto and S. Miura. Finding a basis of a linear system with pairwise distinct discrete valuations on an algebraic curve. *J. Symbolic Comput.*, 30(3):309–323, Sept. 2000. doi:10.1006/jsco.2000.0372.

[12] R. Matsumoto and S. Miura. On construction and generalization of algebraic geometry codes. In T. Katsura et al., editors, *Proc. Algebraic Geometry, Number Theory, Coding Theory, and Cryptography*, pages 3–15, Univ. Tokyo, Japan, Jan. 2000. Available from: http://www.rmatsumoto.org/repository/weight-construct.pdf.

[13] W. Ogata, K. Kurosawa, and S. Tsujii. Nonperfect secret sharing schemes. In *Advances in Cryptology – AUSCRYPT '92*, volume 718 of *Lecture Notes in Computer Science*, pages 56–66. Springer-Verlag, 1993. doi:10.1007/3-540-57220-1_52.

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

[15] A. Shamir. How to share a secret. *Comm. ACM*, 22(11):612–613, Nov. 1979. doi:10.1145/359168.359176.

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

[17] 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.

[18] P. Zhang and R. Matsumoto. Quantum strongly secure ramp secret sharing. *Quantum Information Processing*, 14(2):715–729, Feb. 2015. doi:10.1007/s11128-014-0863-2.