LETTER

Strong Security of the Strongly Multiplicative Ramp Secret Sharing Based on Algebraic Curves

Ryutaroh MATSUMOTO[†a)], *Senior Member*

SUMMARY We introduce a coding theoretic criterion for Yamamoto's strong security of the ramp secret sharing scheme. After that, by using it, we show the strong security of the strongly multiplicative ramp secret sharing proposed by Chen et al. in 2008.

key words: *ramp secret sharing, multiplicative secret sharing, strong security, algebraic geometry code*

1. Introduction

Secret sharing [1] is a well-established topic in the information security [2]. It attracts renewed interest after Cramer et al. [3] revealed that any linear secret sharing with the so-called multiplicative (or strongly multiplicative) property can be used for the secure multiparty computation. Later, the multiplicative properties were generalized to the ramp secret sharing [4], [5]. In [5, Section 4], the authors also provided two explicit constructions of the strongly multiplicative ramp secret sharing based on algebraic curves, which can be regarded as algebraic geometric generalizations of the McEliece-Sarwate ramp secret sharing [6] based on the Reed-Solomon codes.

A set W of shares is said to be *forbidden* if W has no information about the secret vector $\vec{s}$, and said to be *qualified* if $\vec{s}$ can be reconstructed from W [7]. W is said to be *intermediate* if it is neither qualified nor forbidden. The ramp secret sharing allows the existence of intermediate sets, while the perfect secret sharing prohibits the intermediate sets. The merit of ramp secret sharing is that the sizes of shares can be smaller than that of the secret.

In ramp secret sharing [8]–[10], an intermediate set may have critical partial information about the secret, as follows: Suppose that the secret is a 17-letter string "username:password", and an intermediate set W has partial information of 8 letters. The set W may be able to reconstruct "password", which is very undesirable. In order to prevent such a situation, Yamamoto [7], [9] defined the notion of strong security for the ramp secret sharing, which requires any substring of the secret must not be reconstructed by an intermediate set (a formal definition is given later). An explicit construction with the strong security had remain unknown for many years, but recently Nishiara and Takizawa [11] proved that the the McEliece-Sarwate ramp secret sharing [6] mentioned earlier has the strong security. The purpose of this brief letter is to prove the strong security of [5, Section 4.3], after introducing a generic criterion for the strong security constructed from a nested pair of linear codes.

2. Coding Theoretic Criterion for the Strong Security

Let $\mathbf{F}_q$ be the finite field with q elements. We consider a linear ramp secret sharing constructed from a nested pair $C_2 \subset C_1 \subset \mathbf{F}_q^n$ as described in [4, Section 4.2]. Let $L = \dim C_1 - \dim C_2$. A secret vector $\vec{s} \in \mathbf{F}_q^L$ is identified with a coset in the quotient linear space C_1/C_2, by a fixed $\mathbf{F}_q$-linear *isomorphism* $f : \mathbf{F}_q^L \to C_1/C_2$. The number of possible secrets is q^L. The share vector $\vec{x} = (x_1, \ldots, x_n)$ is chosen *uniformly* randomly from $f(\vec{s}) \subset \mathbf{F}_q^n$. x_i is the i-th share. An example of secret sharing by using $C_2 \subset C_1$ will be given in Example 4.

A coding theoretic criterion for such a linear ramp secret sharing was given in [12, Theorem 19], but we introduce a slightly more refined criterion. Firstly, we present a slightly generalized definition of the strong security [7], [9].

Definition 1: For a finite set J of positive integers, we define P_J as the projection map from $\mathbf{F}_q^n$ (or $\mathbf{F}_q^L$) sending $(x_1, \ldots, x_n) \in \mathbf{F}_q^n$ to $(x_j)_{j\in J} \in \mathbf{F}_q^{|J|}$. For fixed $I \subset \{1, \ldots, L\}$ and $J \subset \{1, \ldots, n\}$, the secret sharing constructed from $C_2 \subset C_1$ and $f : \mathbf{F}_q^L \to C_1/C_2$ is said to be strongly secure with respect to I and J if $P_J(\vec{x})$ and $P_I(\vec{s})$ are statistically independent, that is, the share set J has absolutely no information about the part $P_I(\vec{s})$ of the secret, where $\vec{s}$ is the uniform random variable of secrets and $\vec{x}$ is the random variable of share vectors.

Proposition 2: We retain notations from Definition 1. Let

$$C_3 = \{\vec{x} \mid \vec{x} \in f(\vec{s}), \vec{s} \in \mathbf{F}_q^L, P_I(\vec{s}) = \vec{0}\}.$$

The ramp secret sharing in Definition 1 is strongly secure with respect to I and J if and only if $P_J(C_1) = P_J(C_3)$.

In order to prove Proposition 2, we review the next lemma from [13, Section 2].

Lemma 3: We retain notations from Definition 1. The set J is forbidden if and only if $P_J(C_1) = P_J(C_2)$. ■

Proof of Proposition 2: By $f_{|P_I(\mathbf{F}_q^L)}$ we denote the restriction

Manuscript received August 15, 2014.
Manuscript revised February 3, 2015.

[†]The author is with the Department of Communications and Computer Engineering, Tokyo Institute of Technology, Tokyo, 152-8550 Japan.
a) E-mail: ryutaroh@it.ce.titech.ac.jp

DOI: 10.1587/transfun.E98.A.1576

of f to $P_I(\mathbf{F}_q^L)$, that is, the map restricting the domain of f to the subset $P_I(\mathbf{F}_q^L)$. The strong security condition with respect to I and J is equivalent to the condition that J is a forbidden set in the secret sharing constructed from $C_3 \subset C_1$ and $f_{|P_I(\mathbf{F}_q^L)}$. Then the claim of Proposition 2 immediately follows from Lemma 3. ■

3. Strong Security of the Strongly Multiplicative Ramp Secret Sharing

The ramp secret sharing proposed in [5, Section 4.3] is as follows. For terminologies in the algebraic geometry codes, please refer to [14]. Let $F/\mathbf{F}_q$ be an algebraic function field of one variable, $Q_1, \ldots, Q_L, P_1, \ldots, P_n$ pairwise distinct places of degree one in F, and G a divisor of F whose support does not contain $Q_1, \ldots, Q_L, P_1, \ldots, P_n$.

Define

$$\begin{aligned} C_1 &= \{(h(P_1), \ldots, h(P_n)) \mid h \in \mathcal{L}(G)\}, \\ C_2 &= \{(h(P_1), \ldots, h(P_n)) \mid h \in \mathcal{L}(G), \forall i, h(Q_i) = 0\} \\ &= \{(h(P_1), \ldots, h(P_n)) \mid h \in \mathcal{L}(G - Q_1 - \cdots - Q_L)\} \end{aligned}$$

If

$$\deg G \geq L + 2g - 1, \tag{1}$$

where g is the genus of F, then for every secret $(s_1, \ldots, s_L)$ there exists a *nonempty* coset

$$\{(h(P_1), \ldots, h(P_n)) \mid h \in \mathcal{L}(G), h(Q_i) = s_i\}. \tag{2}$$

A necessary and sufficient condition for

$$\dim C_1/C_2 = L \tag{3}$$

is

$$\begin{aligned} L = {} & \dim G - \dim(G - P_1 - \cdots - P_n) \\ & - (\dim(G - Q_1 - \cdots - Q_L) \\ & - \dim(G - Q_1 - \cdots - Q_L - P_1 - \cdots - P_n)). \end{aligned}$$

To ensure the existence of an $\mathbf{F}_q$-linear isomorphism f introduced in Section 2, hereafter we assume both (1) and (3). Under the assumption (1) and (3), we define f to be $f(s_1, \ldots, s_L) = \{(h(P_1), \ldots, h(P_n)) \mid h \in \mathcal{L}(G)$ such that $h(Q_i) = s_i$ for all $i = 1, \ldots, L\}$.

Example 4: The most-known algebraic curve in coding theory is the Hermitian curve [14]. Its function field with $q = 4$ can be described as follows: Let $F = \mathbf{F}_4(x, y)$ with the algebraic relation $y^2 + y - x^3 = 0$. This function field has genus $g = 1$. There is a unique place Q that is a common zero of two functions $1/x$ and $1/y$. The degree of Q is one. All other places of degree one in F are zeros of the equation $y^2 + y - x^3 = 0$ in $\mathbf{F}_4^2$. Let $L = 2$, $Q_1 = (0, 0)$ and $Q_2 = (0, 1)$. Let $P_1, \ldots, P_6$ be all places of degree one other than Q, Q_1, Q_2, that is, $P_1 = (1, \alpha)$, $P_2 = (1, \alpha^2)$, $P_3 = (\alpha, \alpha)$, $P_4 = (\alpha, \alpha^2)$, $P_5 = (\alpha^2, \alpha)$, $P_6 = (\alpha^2, \alpha^2)$, where α is a primitive element of $\mathbf{F}_4$. We choose $G = 3Q$ and we have $\deg G = 3$. The linear space $\mathcal{L}(G)$ becomes the $\mathbf{F}_4$-linear space spanned by 1, x and y. The evaluation of a function $h \in \mathcal{L}(G)$ at P_i is done by substituting x by the first component of P_i and y by the second of P_i. Therefore a generator matrix of C_1 can be written as

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & \alpha & \alpha & \alpha^2 & \alpha^2 \\ \alpha & \alpha^2 & \alpha & \alpha^2 & \alpha & \alpha^2 \end{pmatrix}. \tag{4}$$

On the other hand, $h \in \mathcal{L}(G)$ satisfies $h(Q_1) = h(Q_2) = 0$ if and only if h is a scalar multiple of x. Therefore, a generator matrix of C_2 can be written as

$$\begin{pmatrix} 1 & 1 & \alpha & \alpha & \alpha^2 & \alpha^2 \end{pmatrix},$$

and we see that both (1) and (3) hold.

According to Eq. (2), for secret $(s_1, s_2) \in \mathbf{F}_4^L$, a share vector $(x_1, \ldots, x_6)$ is chosen randomly from the coset

$$\left\{ (s_1, r, s_2 - s_1) \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & \alpha & \alpha & \alpha^2 & \alpha^2 \\ \alpha & \alpha^2 & \alpha & \alpha^2 & \alpha & \alpha^2 \end{pmatrix} \mid r \in \mathbf{F}_4 \right\}. \tag{5}$$

The matrix in Eq. (5) is the same as the generator matrix in Eq. (4).

Theorem 5: We retain the above notations in this section and I and J from Definition 1. The ramp secret sharing of [5, Section 4.3] is strongly secure with respect to I and J if

$$|J| \leq \deg G - |I| - 2g + 1. \tag{6}$$

Proof: We consider the dimension of $P_J(C_3)$ in Proposition 2. By reordering indices we may assume $J = \{1, \ldots, |J|\}$. The code $P_J(C_3)$ can be rewritten as $P_J(C_3) = \{(h(P_1), \ldots, h(P_{|J|})) \mid h \in \mathcal{L}(G - \sum_{i \in I} Q_i)\}$. By [14, Theorem 2.2.2]

$$\begin{aligned} & \dim P_J(C_3) \\ = {} & \underbrace{\dim \mathcal{L}(G - \sum_{i \in I} Q_i)}_{= \deg G - |I| - g + 1} - \underbrace{\dim \mathcal{L}(G - \sum_{i \in I} Q_i - \sum_{j \in J} P_j)}_{= \deg G - |I| - |J| - g + 1} \qquad (7) \\ = {} & |J|, \qquad (8) \end{aligned}$$

where the equalities of the first and the second terms in (7) follow from the Riemann-Roch theorem [14, Theorem 1.5.17] and $\deg G - |I| \geq \deg G - |I| - |J| \geq 2g - 1$, the latter of which is implied by (6). Equation (8) implies $\mathbf{F}_q^{|J|} = P_J(C_3) \subseteq P_J(C_1) \subseteq \mathbf{F}_q^{|J|}$. By Proposition 2 the secret sharing is strongly secure with respect to I and J. ■

Example 6: We retain notations from Example 4. Let $I = \{1\}$ and $J = \{1\}$, which satisfy the assumption in Theorem 5. Then $P_J(\vec{x}) = (x_1)$, and $x_1 = (1 - \alpha)s_1 + r + \alpha s_2$ by Eq. (5). We can see that x_1 can become any value in $\mathbf{F}_4$ by changing r, and that no information about s_1 or s_2 can be inferred from x_1.

Acknowledgments

This research is partly supported by the JSPS Grant Nos.

23246071 and 26289116.

References

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

[2] D.R. Stinson, Cryptography Theory and Practice, 3rd ed., Chapman & Hall/CRC, 2006.

[3] R. Cramer, I. Damgård, and U. Maurer, "General secure multi-party computation from any linear secret-sharing scheme," Advances in Cryptology — EUROCRYPT 2000, ed. B. Preneel, Lecture Notes in Computer Science, vol.1807, pp.316–334, Springer-Verlag, 2000.

[4] H. Chen, R. Cramer, S. Goldwasser, R. de Haan, and V. Vaikuntanathan, "Secure computation from random error correcting codes," Advances in Cryptology — EUROCRYPT 2007, Lecture Notes in Computer Science, vol.4515, pp.291–310, Springer-Verlag, 2007.

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

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

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

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

[9] H. Yamamoto, "Secret sharing system using (k, l, n) threshold scheme," Electronics and Communications in Japan (Part I: Communications), vol.69, no.9, pp.46–54, 1986. (the original Japanese version published in 1985).

[10] W. Ogata, K. Kurosawa, and S. Tsujii, "Nonperfect secret sharing schemes," Advances in Cryptology — AUSCRYPT'92, Lecture Notes in Computer Science, vol.718, pp.56–66, Springer-Verlag, 1993.

[11] M. Nishiara and K. Takizawa, "Strongly secure secret sharing scheme with ramp threshold based on Shamir's polynomial interpolation scheme," IEICE Trans. Fundamentals (Japanese Edition), vol.J92-A, no.12, pp.1009–1013, Dec. 2009. URL: http://ci.nii.ac.jp/naid/110007483234/en

[12] 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, vol.E95-A, no.11, pp.2067–2075, Nov. 2012.

[13] O. Geil, S. Martin, R. Matsumoto, D. Ruano, and Y. Luo, "Relative generalized Hamming weights of one-point algebraic geometric codes," IEEE Trans. Inform. Theory, vol.60, no.10, pp.5938–5949, Oct. 2014.

[14] H. Stichtenoth, "Algebraic Function Fields and Codes," 2nd ed., Graduate Texts in Mathematics, vol.254, Springer-Verlag, Berlin Heidelberg, 2009.