Article

Strongly Secure Ramp Secret Sharing with More Participants based on Reed-Solomon Codes

Ryutaroh Matsumoto [1,2]

[1] Department of Information and Communication Engineering, Nagoya University, Nagoya, Japan.
[2] Department of Mathematical Sciences, Aalborg University, Denmark.

Version April 29, 2019 submitted to Cryptography

Abstract: The number of participants in the McEliece-Sarwate strongly secure ramp secret sharing scheme is at most $q - L$, where q is the size of each share and L is the number of symbols in the secret. We propose another construction of strongly secure ramp secret sharing that can support q participants also based on the Reed-Solomon codes.

Keywords: ramp secret sharing; strong security; Reed-Solomon code

MSC: 94A62

1. Introduction

Secret sharing is a scheme to share a secret among multiple participants so that only *qualified* sets of participants can reconstruct the secret, while *forbidden* sets have no information about the secret [12]. A piece of information received by a participant is called a *share*. A set of participants that is neither qualified nor forbidden is said to be *intermediate*. The access structure of a secret sharing scheme is the set of qualified sets, that of intermediate sets and that of forbidden sets.

It is well-known that the size of classical shares cannot be smaller than that of the classical secret in a perfect secret sharing scheme, where *perfect* means that there is no intermediate set, while *ramp* or *non-perfect* means that there exist intermediate sets [2,13,14]. An advantage of ramp schemes is that the size of secrets can be arbitrarily large for a fixed size of shares.

Ordinary ramp schemes have the following security risk: Suppose that classical secret is $\vec{m} = (m_1, \ldots, m_L)$, and an intermediate set has $\ell(\geq 1)$ symbol of information about $\vec{m}$. Then that intermediate set sometimes knows m_i explicitly for some i. This insecurity was mentioned in [9,14]. Iwamoto and Yamamoto [6] explicitly constructed such an example.

In order to address this security risk, Yamamoto [14] introduced the notion of strong security into ramp schemes: A secret sharing scheme with secret $\vec{m} = (m_1, \ldots, m_L)$ is said to be *strongly secure* if any $(L - \ell)$ symbols in $\vec{m}$ is always statistically independent of shares in an intermediate set that has ℓ symbol of information about $\vec{m}$, for $\ell = 1, \ldots, L - 1$.

The first ramp secret sharing scheme was proposed by McEliece and Sarwate [9]. It was based on the Reed-Solomon codes [11], and can support up to $q - L$ participants, where q is the size of shares and L is the number of symbols in the secret. Much later the McEliece-Sarwate scheme was proved to be strongly secure [10]. Often we can increase the size of shares to support more participants. However, if we cannot increase the size of secrets, the storage space of shares are wasted more. Thus, it is desirable to have another scheme that can support more participants.

The purpose of this short paper is to provide another construction of strongly secure ramp secret sharing schemes with more participants. After reviewing relevant definitions of secret sharing in Section 2, we will propose our new ramp secret sharing and will prove its strong security in Section 3.

2. Preliminaries

Let $\mathbf{F}_q$ be the finite field with q elements. In this paper we assume that each share belongs to $\mathbf{F}_q$.

Definition 1. *[2,14] A (k, L, n)-threshold ramp secret sharing scheme distributes a secret in $\mathbf{F}_q^L$ to n participants. Each share is one symbol in $\mathbf{F}_q$. k or more participants can reconstruct the secret, while $k - L$ or less participants have no information about the secret. By "no information" we mean the statistical independence between the secret and a set of shares.*

Definition 2. *[14] Assume that the probability distribution of secrets is uniform. A (k, L, n)-threshold ramp secret sharing scheme is said to be strongly secure, if any $L - \ell$ symbols in the secret and any set of $k - L + \ell$ shares are statistically independent of each other for $\ell = 1, \ldots, L - 1$.*

Iwamoto and Yamamoto [6] generalized Definition 2, and the generalized definition was mentioned in the introduction. The McEliece-Sarwate secret sharing [9] is a strongly secure (k, L, n)-threshold scheme.

3. Proposed Construction and Its Strong Security

3.1. Proposed Construction

Let $n \leq q$ and $\alpha_1, \ldots, \alpha_n$ be distinct elments in $\mathbf{F}_q$. We assume that $\alpha_1, \ldots, \alpha_L$ are nonzero. We will construct a strongly secure (k, L, n)-threshold scheme, with $n \leq q$ and

$$k \geq 2L. \tag{1}$$

Define an $[n, k]$ Reed-Solomon (RS) code as

$$\mathrm{RS}(n, k) = \{(f(\alpha_1), \ldots, f(\alpha_n)) : f(x) \in \mathbf{F}_q[x], \deg f(x) < k\}.$$

Hereafter we assume that secrets are uniformly distributed in $\mathbf{F}_q^L$. For a given secret $\vec{m} = (m_1, \ldots, m_L) \in \mathbf{F}_q^L$, find $g_1(x) = a_0 x^0 + \cdots + a_{L-1} x^{L-1}$ and such that $g_1(\alpha_j) = m_j / \alpha_j^{k-L}$ for all $j = 1, \ldots, L$. Such $g_1(x)$ always exists because computation of $g_1(x)$ is just the inverse mapping of the encoding of $\mathrm{RS}(L/2, L/2)$ for the codeword $(m_1/\alpha_1^{k-L}, \ldots, m_L/\alpha_L^{k-L})$. Let $g_2(x) = x^{k-L} g_1(x)$. Observe that $g_2(\alpha_j) = m_j$.

Randomly choose $b_0, \ldots, b_{k-L} \in \mathbf{F}_q$ and let

$$g_3(x) = g_2(x) + b_0 + b_1 x + \cdots + b_{k-L-1} x^{k-L-1}.$$

The dealer sends $g_3(\alpha_j)$ as a share to the j-th participant, for $j = 1, \ldots, n$.

Let $\vec{x}_1, \vec{x}_2 \in \mathbf{F}_q^n$ be two vectors of n shares, and assume that $\vec{x}_i$ corresponds to a secret $\vec{m}_i \in \mathbf{F}_q^L$ for $i = 1, 2$. A secret sharing scheme is said to be linear if the linearly combined share vector $\beta_1 \vec{x}_1 + \beta_2 \vec{x}_2$ corresponds to the linearly combined secret $\beta_1 \vec{m}_1 + \beta_2 \vec{m}_2$. It is known that any linear secret sharing scheme can be expressed by a nested pair of linear codes $C_2 \subset C_1 \subset \mathbf{F}_q^n$ with $\dim C_1 - \dim C_2 = L$ [1,3,4,7,8]. In our proposed scheme we have $C_2 = \mathrm{RS}(n, k - L)$ and $C_1 = \mathrm{RS}(n, k)$.

The coset distance of $C_1 \supset C_2$ is defined as [4]

$$d(C_1, C_2) = \min\{\mathrm{wt}(\vec{x}) \mid \vec{x} \in C_1 \setminus C_2\},$$

where $\mathrm{wt}(\vec{x})$ is the Hamming weight of $\vec{x}$. It was shown [1,3,4,7] that any $n + 1 - d(C_1, C_2)$ shares can reconstruct the secret and that any $d(C_2^\perp, C_1^\perp) - 1$ shares are statistically independent of the secret, where $C_1^\perp$ is the dual code of C_1. Since $d(\mathrm{RS}(n, k), \mathrm{RS}(n, k - L)) = n - k + 1$ and $d(\mathrm{RS}(n, k - L)^\perp, \mathrm{RS}(n, k)^\perp) = k - L + 1$, we know that the proposed ramp scheme is a (k, L, n)-threshold scheme.

3.2. Strong Security

Our remaining task is to examine the strong security of the proposed scheme. This subsection is devoted to a proof of its strong security. Without loss of generality we can consider the statistical independence between $m_1, \ldots, m_{L-\ell}$ and a set of $k - L + \ell$ shares.

In our proposed scheme, $b_0, \ldots, b_{k-L-1}$ serve as dummy randomness hiding $\vec{m}$. When we consider the secrecy of $m_1, \ldots, m_{L-\ell}$, the rest $m_{L-\ell+1}, \ldots, m_L$ of the secret $\vec{m}$ also serves as dummy randomness hiding $m_1, \ldots, m_{L-\ell}$.

For $g(x) = b_0 x^0 + \cdots + b_{k-L+\ell-1} x^{k-L+\ell-1}$, define $\widetilde{g}(x) = b_{k-L+\ell} x^{k-L+\ell} + \cdots + b_{k-1} x^{k-1}$ such that $\widetilde{g}(\alpha_j) = -\sum_{i=k-L}^{k-L+\ell-1} b_i \alpha_j^i$ for $j = 1, \ldots, L-\ell$. Such a $\widetilde{g}(x)$ is uniquely determined because it is the inverse of encoding of the $[L-\ell, L-\ell]$ generalized Reed-Solomon code. Define a linear code

$$D = \{(g(\alpha_1) + \widetilde{g}(\alpha_1), \ldots, g(\alpha_n) + \widetilde{g}(\alpha_n)) : \deg g(x) \le k - L + \ell - 1\}.$$

When we view $m_1, \ldots, m_{L-\ell}$ as the secret and the rest $m_{L-\ell+1}, \ldots, m_L$ as dummy randomness, the secret sharing scheme can be described by the nested pair of linear codes $D \subset C_1$, where $C_1 = \mathrm{RS}(n,k)$ as defined before.

For a subset $S \subset \mathbf{F}_q^n$ and $A \subset \{1, \ldots, n\}$, we mean $P_A(S) = \{(x_i)_{i \in A} : (x_1, \ldots, x_n) \in S\}$.

Lemma 1.

$$\dim P_A(\mathrm{RS}(n,k)) - \dim P_A(D) = \begin{cases} 0 & \text{if } 0 \le |A| \le k - L + \ell, \\ |A| - k - L + \ell & \text{if } k - L + \ell \le |A| \le k, \\ L - \ell & \text{if } k \le |A| \le n. \end{cases} \tag{2}$$

Proof. Since the minimum Hamming distance of $\mathrm{RS}(n,k)$ is $n - k + 1$, we have [11]

$$\dim P_A(\mathrm{RS}(n,k)) = \begin{cases} |A| & \text{if } 0 \le |A| \le k, \\ k & \text{if } k \le |A| \le n. \end{cases} \tag{3}$$

The codeword in D is the sum of a codeword in $\mathrm{RS}(n, k - L + \ell)$ and the codeword defined by $\widetilde{g}(x)$. The latter can be seen as a codeword in a generalized Reed-Solomon code of length n and dimension $L - \ell$. So, the Hamming weight of a codeword defined by $\widetilde{g}(x)$ is $\ge n + 1 - L + \ell$. There exists a codeword in $\mathrm{RS}(n, k - L + \ell)$ of Hamming weight $n - k + L - \ell + 1$. Since we have assumed $k \ge 2L$ in (1) and $\ell \ge 1$, we always have $n - k + L - \ell + 1 < n + 1 - L + \ell$. Under this condition, the minimum weight codeword in $\mathrm{RS}(n, k - L + \ell)$ cannot be canceled by a codeword defined by $\widetilde{g}(x)$. Therefore, the minimum Hamming distance of D is $n - k + L - \ell + 1$, which implies [11]

$$\dim P_A(D) = \begin{cases} |A| & \text{if } 0 \le |A| \le k - L + \ell, \\ k - L + \ell & \text{if } k - L + \ell \le |A| \le n. \end{cases} \tag{4}$$

Combining Eqs. (3) and (4) gives the claim of this lemma. □

The mutual information between $m_1, \ldots, m_{L-\ell}$ and the shares in A is [5]

$$\dim P_A(C_1) - P_A(D). \tag{5}$$

By Lemma 1, $|A| \le k - L + \ell$ implies that (5) is zero, which proves the strong security of the proposed ramp secret sharing scheme.

Funding: This research was funded by JSPS grant number 17K06419.

Conflicts of Interest: The author declares no conflict of interest.

1. Bains, T. Generalized Hamming weights and their applications to secret sharing schemes. Master's thesis, University of Amsterdam, 2008. (supervised by R. Cramer, G. van der Geer, and R. de Haan).
2. Blakley, G.R.; Meadows, C. Security of ramp schemes. Advances in Cryptology–CRYPTO'84. Springer-Verlag, 1985, Vol. 196, *Lecture Notes in Computer Science*, pp. 242–269. doi:10.1007/3-540-39568-7_20.
3. Chen, H.; Cramer, R.; Goldwasser, S.; de Haan, R.; Vaikuntanathan, V. Secure Computation from Random Error Correcting Codes. Advances in Cryptology–EUROCRYPT 2007. Springer-Verlag, 2007, Vol. 4515, *Lecture Notes in Computer Science*, pp. 291–310. doi:10.1007/978-3-540-72540-4_17.
4. Duursma, I.M.; Park, S. Coset bounds for algebraic geometric codes. *Finite Fields Appl.* **2010**, *16*, 36–55. doi:10.1016/j.ffa.2009.11.006.
5. Geil, O.; Martin, S.; Matsumoto, R.; Ruano, D.; Luo, Y. Relative generalized Hamming weights of one-point algebraic geometric codes. *IEEE Trans. Inform. Theory* **2014**, *60*, 5938–5949. doi:10.1109/TIT.2014.2345375.
6. Iwamoto, M.; Yamamoto, H. Strongly secure ramp secret sharing schemes for general access structures. *Inform. Process. Lett.* **2006**, *97*, 52–57. doi:10.1016/j.ipl.2005.09.012.
7. Kurihara, J.; Uyematsu, T.; Matsumoto, R. Secret Sharing Schemes Based on Linear Codes Can Be Precisely Characterized by the Relative Generalized Hamming Weight. *IEICE Trans. Fundamentals* **2012**, *E95-A*, 2067–2075. doi:10.1587/transfun.E95.A.2067.
8. Martínez-Peñas, U. On the similarities between generalized rank and Hamming weights and their applications to network coding. *IEEE Trans. Inform. Theory* **2016**, *62*, 4081–4095. doi:10.1109/TIT.2016.2570238.
9. McEliece, R.J.; Sarwate, D.V. On sharing secrets and Reed-Solomon codes. *Comm. ACM* **1981**, *24*, 583–584. doi:10.1145/358746.358762.
10. Nishiara, M.; Takizawa, K. Strongly Secure Secret Sharing Scheme with Ramp Threshold Based on Shamir's Polynomial Interpolation Scheme. *Trans. IEICE* **2009**, *J92-A*, 1009–1013. (in Japanese). http://ci.nii.ac.jp/naid/110007483234/en
11. Pless, V.S.; Huffman, W.C.; Brualdi, R.A. An Introduction to Algebraic Codes. In *Handbook of Coding Theory*; Pless, V.S.; Huffman, W.C., Eds.; Elsevier: Amsterdam, 1998; pp. 3–139.
12. Shamir, A. How to share a secret. *Comm. ACM* **1979**, *22*, 612–613. doi:10.1145/359168.359176.
13. Stinson, D.R. *Cryptography Theory and Practice*, 3rd ed.; Chapman & Hall/CRC, 2006. doi:10.1201/9781420057133.
14. Yamamoto, H. Secret sharing system using (k, L, n) threshold scheme. *Electronics and Communications in Japan (Part I: Communications)* **1986**, *69*, 46–54. (the original Japanese version published in 1985), doi:10.1002/ecja.4410690906.