Optimal multiple assignment scheme for strongly secure ramp secret sharing schemes with general access structures

Ryutaroh Matsumoto
Dept. of Communications and Computer Engineering, Tokyo Institute of Technology, Meguro-ku, Tokyo 152–8550, Japan
a) ryutaroh@matsumoto.org

Abstract: Iwamoto et al. proposed the strong security definition for ramp secret sharing schemes with general access structures, and also proposed an integer optimization approach to construct a secret sharing with the smallest share size and general access structure, based on a threshold secret sharing scheme. This note proves that if the underlying threshold scheme is strongly secure then the constructed multiple assignment scheme gives a strongly secure secret sharing scheme.

Keywords: secret sharing, access structure, strong security

References

1 Introduction

Secret sharing (SS) [1] 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. A set of participants is called forbidden if the set has absolutely no information about the secret. A secret sharing scheme is called perfect [2] if every set of participants is always qualified or forbidden. If a set is neither qualified or forbidden in a secret sharing scheme, the scheme is said to be ramp or non-perfect. A set is said to be intermediate if it is neither qualified nor forbidden. A merit of the ramp schemes is to reduce share size (the number of bits) while keeping the secret size [3, 4, 5]. A drawback of ramp schemes is that part of the secret can be known to an intermediate set of participants. To exclude such a possibility, Yamamoto and Iwamoto [4, 6] defined the notion of strong security for the ramp schemes.

On the other hand, traditionally, the access structure called the threshold structure has been the most focused one, where a set of participants is qualified if and only if the number of participants is \( \geq t \). A scheme with a threshold structure is called a threshold scheme. A well-known method to realize an arbitrary access structure is the multiple assignment scheme proposed by Shamir [1] and named by Ito et al. [7]. It assigns multiple shares of a threshold scheme to single participant, and a single share can be assigned to multiple participants.

Ito et al. [7] did not consider to minimize the share size. Later, Iwamoto et al. [8] proposed an integer optimization approach to construct a secret sharing scheme with the minimum share size based on a threshold scheme. Despite they proposed the strong security criterion, they did not considered the strong security property of their proposal [8]. This note shows that if the underlying threshold scheme is strongly secure in the sense of [6] then the scheme constructed by [8] is also strongly secure.

2 Notation and the main lemma

Let \( q \) be a prime power, and \( \mathbb{F}_q \) the finite field with \( q \) elements. In this note we assume that secret and all shares are vectors over \( \mathbb{F}_q \). We will define the access structure when there are \( n \) participants and secret consists of \( L \) symbols in \( \mathbb{F}_q \). Let \( V_i \)
be the random variable of the $i$-th share for $i = 1, \ldots, n$, and $S$ the random variable of the secret. We assume the uniform probability distribution of $S$. The encoding rule of a secret sharing scheme is a conditional joint probability distribution of $(V_1, \ldots, V_n)$ given secret $S$. The encoding rule determines a joint probability distribution of $(S, V_1, \ldots, V_n)$. For a set $T$, $2^T$ denotes its power set. Let $T_0$ be a subset of $T$, and we have $|2^T| = 2^{|T|}$. For $i = 0, \ldots, L$, we define $A_i \subset 2^{\{1, \ldots, n\}}$ by

$$A_i = \{ A \subset \{1, \ldots, n\} \mid I(S, (V_j)_{j \in A}) = i \},$$

where $I(\cdot, \cdot)$ is the mutual information in $\log_q$. We assume

$$2^{\{1, \ldots, n\}} = \bigcup_{i=0}^L A_i.$$

The collection $A_0, \ldots, A_L$ is called the access structure. Recall that secret $S$ is a random variable on $\mathbb{F}_q^L$. Let $S_i$ be the $i$-th component of $S$. A given secret sharing scheme is said to be strongly secure [6] when $A \in A_i, B \subset \{1, \ldots, L\}$ and $|B| = L - i$ implies $I((S_j)_{j \in B}; (V_k)_{k \notin A}) = 0$.

The multiple assignment map was introduced in [1] and named in [7], which is reviewed in the following. It constructs a secret sharing scheme with $m$ participants. Usually the underlying secret sharing scheme is a threshold scheme. The original scheme and the constructed scheme have the same structure of the original scheme by $f$. In the new constructed secret sharing scheme, the $i$-th participant receives $\{W_j \mid j \in \Phi(i)\}$ as his/her share, which is denoted by $V_i$. Denote the access structure of the original scheme by $A_0^{\text{old}}, \ldots, A_L^{\text{old}}$, and that of the new constructed scheme by $A_0^{\text{new}}, \ldots, A_L^{\text{new}}$.

**Main Lemma:** If the original secret sharing scheme generating $W_1, \ldots, W_m$ is strongly secure then the constructed scheme is also strongly secure.

**Proof:** Let $V_i$ be the $i$-th share of the new constructed scheme, and $A_i^{\text{new}} \subset \{1, \ldots, n\}$ represent a set of shares $V_i$. Since $V_i$ consists of $W_1, \ldots, W_m$, the set

$$A_i^{\text{old}} = \bigcup_{\Phi(i) \in A_i^{\text{new}}} \Phi(i)$$

is the set of original shares corresponding to the set $A_i^{\text{new}}$ of the new shares. For a set $B \subseteq \{1, \ldots, L\}$, we have the equality

$$I((V_i)_{i \in A_i^{\text{new}}}; (S_j)_{j \in B}) = I((W_i)_{i \in A_i^{\text{old}}}; (S_j)_{j \in B}),$$

which implies

$$A_i^{\text{new}} \in A_i^{\text{new}} \Leftrightarrow A_i^{\text{old}} \in A_i^{\text{old}}. \quad (1)$$

Equation (1) and the strong security of the original scheme generating $W_1, \ldots, W_m$ imply the strong security of the new constructed scheme.

**3 How to construct strongly secure optimal multiple assignment scheme**

Nishiara and Takizawa [9] proved that the McEliece-Sarwate ramp secret sharing scheme [10] is strongly secure. The McEliece-Sarwate scheme satisfies the defi-
nition of \((t, L, m)\)-ramp secret sharing scheme required in [8 Section 5]. Therefore one can apply Iwamoto et al.’s proposal [8] to the McEliece-Sarwate scheme. Iwamoto et al.’s proposal [8] generates a multiple assignment scheme that is optimal in the sense that it minimizes the share sizes. By the main lemma proved in this note, one can see that the constructed ramp secret sharing scheme is strongly secure.

Acknowledgment

The author would like to thank Prof. Mitsugu Iwamoto for helpful discussion. This research is partly supported by the Japan Society for the Promotion of Science Grant Nos. 23246071 and 26289116.