IEICE TRANSACTIONS

on Fundamentals of Electronics, Communications and Computer Sciences

VOL. E100-A NO. 12
DECEMBER 2017

A PUBLICATION OF THE ENGINEERING SCIENCES SOCIETY

The Institute of Electronics, Information and Communication Engineers
Kikai-Shinko-Kaikan Bldg., 5-8, Shibakoen 3 chome, Minato-ku, TOKYO, 105-0011 JAPAN

PAPER *Special Section on Information Theory and Its Applications*

A Cheating-Detectable (k, L, n) Ramp Secret Sharing Scheme**

Wataru NAKAMURA[†*a)], ***Nonmember***, **Hirosuke YAMAMOTO**[††b)], ***Fellow***, ***and*** **Terence CHAN**[†††c)], ***Nonmember***

SUMMARY In this paper, we treat (k, L, n) ramp secret sharing schemes (SSSs) that can detect impersonation attacks and/or substitution attacks. First, we derive lower bounds on the sizes of the shares and random number used in encoding for given correlation levels, which are measured by the mutual information of shares. We also derive lower bounds on the success probabilities of attacks for given correlation levels and given sizes of shares. Next we propose a strong (k, L, n) ramp SSS against substitution attacks. As far as we know, the proposed scheme is the first strong (k, L, n) ramp SSSs that can detect substitution attacks of at most $k-1$ shares. Our scheme can be applied to a secret S^L uniformly distributed over $\mathrm{GF}(p^m)^L$, where p is a prime number with $p \geq L+2$. We show that for a certain type of correlation levels, the proposed scheme can achieve the lower bounds on the sizes of the shares and random number, and can reduce the success probability of substitution attacks within nearly L times the lower bound when the number of forged shares is less than k. We also evaluate the success probability of impersonation attack for our schemes. In addition, we give some examples of insecure ramp SSSs to clarify why each component of our scheme is essential to realize the required security.
key words: *ramp secret sharing schemes, cheating detection, impersonation attacks, substitution attacks, mutual information of shares*

1. Introduction

Secret sharing schemes (SSSs) [1], [2] are methods to keep a secret S securely from both loss and leakage by encoding S into n shares $(V_1, \ldots, V_n)$. For example, in (k, n) SSSs, S can be decoded from any k shares but no information of S can be obtained from $k-1$ or less shares. In (k, L, n) ramp SSSs [3], [4], the secret $S^L = (S_1, S_2, \ldots, S_L)$ is encoded so that S^L can be decoded from any k shares, no information of S^L can be obtained from $k-L$ or less shares, and for each $1 \leq j \leq L$, the conditional entropy of S^L given $k-j$ shares is equal to $(j/L)H(S^L)$. Furthermore, strong (k, L, n) ramp SSSs are proposed in [4]. In weak (k, L, n) ramp SSSs, some of S_i in S^L may leak explicitly if $k-j$ shares leak for $1 \leq j \leq L-1$. But, in strong (k, L, n) ramp SSSs, any information of any $(S_{i_1}, S_{i_2}, \ldots, S_{i_j})$ does not leak even if $k-j$ shares leak for $1 \leq j \leq L-1$. Hence, strong (k, L, n) ramp SSSs are desirable for security.

An important issue on SSSs is cheating detection. An attacker may forge shares in order to make the decoder to decode an incorrect secret. Such cheating is classified into *impersonation attacks* and *substitution attacks*. In the impersonation attacks, an attacker forges shares without knowing the legitimate shares. On the other hand, in the substitution attacks, an attacker forges shares after he/she gets the legitimate shares.

For (k, n) SSSs, cheating-detectable schemes are well studied [5]–[12]. Ogata et al. [6] derived a lower bound on the size of shares for the given success probability of substitution attack, and proposed a scheme which achieves the lower bound. Cabello et al. [7] also proposed another scheme against substitution attacks which is almost optimum in the sense of share size.

It is also known that mutual information of shares plays an important role in the detection of impersonation attacks. Iwamoto et al. [9] defined *correlation level* based on mutual information of shares, and proved coding theorems using correlation level for blockwise $(2, 2)$ SSSs against impersonation attacks. Koga and Koyano [10] extended the definition of correlation level to symbolwise (k, n) SSSs to prove coding theorems.

On the other hand, for ramp SSSs, Ogata [13] proposed a scheme against substitution attacks. Also, Cramer et al. [8] defined a notion of *algebraic manipulation detection* (AMD) codes, and proposed a method to convert SSSs into cheating-detectable ones. By applying AMD codes to ramp SSSs, we can construct ramp SSSs against substitution attacks. But, these schemes do not satisfy fully the security condition of (k, L, n) ramp SSSs. Furthermore, there is no research on ramp SSSs based on correlation level.

In this paper, we treat cheating-detectable (k, L, n) ramp SSSs and analyze the security of schemes based on correlation level as [9] and [10]. First, we derive lower bounds on the sizes of the shares and random number used in encoding, and the success probabilities of attacks for given correlation level. We also derive lower bounds on the success probabilities of attacks for the given size of shares. Next, we propose a strong (k, L, n) ramp SSS against substitution attacks. As

Manuscript received January 30, 2017.
Manuscript revised June 4, 2017.
[†]The author was with the Department of Mathematical Informatics, The University of Tokyo, Tokyo, 113-8656 Japan.
[††]The author is with the Department of Complexity Science and Engineering, The University of Tokyo, Kashiwa-shi, 277-8561 Japan.
[†††]The author is with the Division of Information Technology, Engineering and the Environment, University of South Australia, Adelaide, 5095, Australia.
[*]Presently, with Hitachi, Ltd., Japan.
[**]This paper was presented in part at 2016 International Symposium on Information Theory and Its Applications (ISITA2016). This research was supported in part by JSPS Bilateral Joint Research Project S14719, ARC Discovery Project DP150103658, and JST ERATO Kawarabayashi Large Graph Project.
a) E-mail: wn.whlesp@gmail.com
b) E-mail: hirosuke@ieee.org
c) E-mail: Terence.Chan@unisa.edu.au
DOI: 10.1587/transfun.E100.A.2709

far as we know, the proposed scheme is the first one that satisfies fully the condition of strong (k, L, n) ramp SSSs and can detect substitution attacks of at most $k-1$ shares. Our scheme can be applied to a secret S^L uniformly distributed over $\mathrm{GF}(p^m)^L$, where p is a prime number with $p \geq L+2$.

For a given certain type of correlation level, our strong (k, L, n) ramp SSS can attain the optimal sizes of the shares and random number. Furthermore, our scheme can reduce the success probability of substitution attacks within nearly L times its lower bound when the number of forged shares a satisfies $1 \leq a \leq k-1$. We also evaluate the success probability of impersonation attack for our schemes.

When $L=1$, our scheme corresponds to the (k, n) SSS treated by Cabello et al., but how to extend their scheme to (k, L, n) ramp SSSs is not so trivial.

The rest of this paper is organized as follows. In Sect. 2, we describe the notation, the system model, and known results. Then, we consider the converse part of coding theorem in Sect. 3, in which several new lower bounds are derived. Next we consider the direct part of coding theorem in Sect. 4, and we propose a ramp SSS to prove the direct part. Finally in Sect. 5, we show examples of insecure ramp SSSs to clarify why each component of the proposed scheme is necessary to achieve the required security.

2. Preliminaries

2.1 Notation

Throughout this paper, $H_p(\cdot)$ and $I_p(\cdot;\cdot)$ denote entropy and mutual information with base p in logarithm, respectively. For simplicity of notation, the base is often omitted. For positive integers a and b, $[a]$ and $[a, b]$ are defined by $[a] := \{1, 2, \ldots, a\}$ and $[a, b] := \{a, a+1, \ldots, b\}$, respectively. For a subset $\mathcal{I} = \{i_1, i_2, \ldots, i_\ell\} \subseteq [n]$, $X_{\mathcal{I}}$ denotes $(X_{i_1}, X_{i_2}, \ldots, X_{i_\ell})$. For a finite set $\mathcal{A}$, $|\mathcal{A}|$ stands for the cardinality of $\mathcal{A}$.

2.2 System Model

Let $S^L = S_1 S_2 \ldots S_L$ be a secret, where all S_j, $1 \leq j \leq L$, are mutually independent and have the same probability distribution P_S over a finite set $\mathcal{S}$. The encoder φ, which generates n shares $V_1, V_2, \ldots, V_n$, is defined as a function $\varphi : \mathcal{S}^L \times \mathcal{R} \to \mathcal{V}_1 \times \mathcal{V}_2 \times \cdots \times \mathcal{V}_n$ i.e. $(V_1, V_2, \ldots, V_n) = \varphi(S^L, R)$, where $\mathcal{V}_i$ is the range of the i-th share V_i and R is a uniform random number over a finite set $\mathcal{R}$. For each $\mathcal{K} = \{i_1, i_2, \ldots, i_k\} \subseteq [n]$, a decoder $\psi_{\mathcal{K}}$ is defined as $\psi_{\mathcal{K}} : \mathcal{V}_{i_1} \times \cdots \times \mathcal{V}_{i_k} \to \mathcal{S}^L \cup \{\perp\}$, where $\perp$ is the special symbol to represent the detection of cheating[†]. For simplicity of notation, we omit $\mathcal{K}$ of $\psi_{\mathcal{K}}$ in the following.

(φ, ψ) is called a (k, L, n) ramp SSS if it satisfies the following two conditions [4].

(i) For any $\mathcal{K} \subseteq [n]$ with $|\mathcal{K}| = k$, it holds that

$$\psi(V_{\mathcal{K}}) = S^L. \tag{1}$$

(ii) For any $j \in [L]$ and for any $\mathcal{I} \subseteq [n]$ with $|\mathcal{I}| = k - j$, it holds that

$$H(S^L \mid V_{\mathcal{I}}) = \frac{j}{L} H(S^L). \tag{2}$$

In particular, a (k, L, n) ramp scheme with $L = 1$ is called a (k, n) SSS.

Furthermore, (φ, ψ) is called a strong (k, L, n) ramp SSS if it satisfies the following condition (iii) besides (i) and (ii).

(iii) For any $j \in [L]$, any $\mathcal{I} \subseteq [n]$ with $|\mathcal{I}| = k - j$, and any $\mathcal{J} \subseteq [L]$ with $|\mathcal{J}| = j$, it holds that

$$H(S_{\mathcal{J}} \mid V_{\mathcal{I}}) = H(S_{\mathcal{J}}). \tag{3}$$

If (φ, ψ) satisfies (i) and (ii) but not (iii), we call it a weak (k, L, n) ramp SSS.

We assume that a cheater can forge at most $k-1$ shares out of any k shares. For $\mathcal{O} = \{i_1, \ldots, i_a\}$, let $\overline{V}_{\mathcal{O}}$ and $V_{\mathcal{O}}$ be the forged shares and the corresponding original shares, respectively, and let $V_{\mathcal{I}}$ be the remaining shares satisfying $|\mathcal{I}| = k - a$ and $\mathcal{O} \cap \mathcal{I} = \emptyset$. We consider two types of attacks. An attack without knowing $V_{\mathcal{O}}$, i.e., an attack such that $\overline{V}_{\mathcal{O}}$ is independent of $(V_{\mathcal{O}}, V_{\mathcal{I}})$, is called an impersonation attack. On the other hand, an attack using $V_{\mathcal{O}}$, i.e., an attack such that $V_{\mathcal{I}}$, $V_{\mathcal{O}}$, and $\overline{V}_{\mathcal{O}}$ make a Markov chain in this order, is called a substitution attack[††].

The success of impersonation attacks can be defined by either $\psi(\overline{V}_{\mathcal{O}}, V_{\mathcal{I}}) \neq \perp$ or $\psi(\overline{V}_{\mathcal{O}}, V_{\mathcal{I}}) \notin \{S^L, \perp\}$. On the other hand, for substitution attacks, only the latter definition makes sense because the former is always satisfied by $\overline{V}_{\mathcal{O}} = V_{\mathcal{O}}$. Hence, for a forged shares, we consider two kinds of the success probability of impersonation attack, $P_{\mathrm{imp}^*(a)}$ and $P_{\mathrm{imp}(a)}$, and the success probability of substitution attack, $P_{\mathrm{sub}(a)}$, which are defined as follows[†††]:

$$P_{\mathrm{imp}^*(a)} = \max_{\substack{\mathcal{O}, \mathcal{I} \subseteq [n]: \\ |\mathcal{O}|=a, |\mathcal{I}|=k-a, \\ \mathcal{O} \cap \mathcal{I} = \emptyset}} \max_{P_{\overline{V}_{\mathcal{O}}}} \Pr\{\psi(\overline{V}_{\mathcal{O}}, V_{\mathcal{I}}) \neq \perp\}, \tag{4}$$

$$P_{\mathrm{imp}(a)} = \max_{\substack{\mathcal{O}, \mathcal{I} \subseteq [n]: \\ |\mathcal{O}|=a, |\mathcal{I}|=k-a, \\ \mathcal{O} \cap \mathcal{I} = \emptyset}} \max_{P_{\overline{V}_{\mathcal{O}}}} \Pr\{\psi(\overline{V}_{\mathcal{O}}, V_{\mathcal{I}}) \notin \{S^L, \perp\}\}, \tag{5}$$

$$P_{\mathrm{sub}(a)} = \max_{\substack{\mathcal{O}, \mathcal{I} \subseteq [n]: \\ |\mathcal{O}|=a, |\mathcal{I}|=k-a, \\ \mathcal{O} \cap \mathcal{I} = \emptyset}} \max_{v_{\mathcal{O}} \in \mathcal{V}_{\mathcal{O}}} \max_{P_{\overline{V}_{\mathcal{O}} | V_{\mathcal{O}}}} \Pr\{\psi(\overline{V}_{\mathcal{O}}, V_{\mathcal{I}}) \notin \{S^L, \perp\} \mid V_{\mathcal{O}} = v_{\mathcal{O}}\}. \tag{6}$$

[†]In this paper, we always assume that $i_\ell \neq i_{\widehat{\ell}}$ for $\ell \neq \widehat{\ell}$ in $\{i_1, i_2, \ldots, i_k\}$.

[††]We suppose that cheaters *do not* know the secret S^L (except for information obtained from $V_{\mathcal{O}}$ in substitution attacks). This model is sometimes called OKS model [11], [12] named after the authors of [6].

[†††]The success of an impersonation attack is usually defined as $\psi(\overline{V}_{\mathcal{O}}, V_{\mathcal{I}}) \neq \perp$ (e.g., [9], [10]). But, in this paper, we also consider $P_{\mathrm{imp}(a)}$ because a lower bound on $P_{\mathrm{imp}(a)}$ immediately gives a lower bound on $P_{\mathrm{sub}(a)}$.

Remark 1: For $1 \le a \le b \le k-1$, it holds that $P_{\mathrm{imp}(a)} \le P_{\mathrm{sub}(a)} \le P_{\mathrm{sub}(b)}$, but it does not always hold that $P_{\mathrm{imp}^*(a)} \le P_{\mathrm{sub}(a)}$, $P_{\mathrm{imp}^*(a)} \le P_{\mathrm{imp}^*(b)}$, or $P_{\mathrm{imp}(a)} \le P_{\mathrm{imp}(b)}$.

Next, we give the definition of correlation level.

Definition 1: The correlation level of $(V_1, V_2, \ldots, V_n)$ is defined as $(l_1, l_2, \ldots, l_{k-1})_p$ if for any $j \in [2, k]$ and any $\{i_1, \ldots, i_j\} \subseteq [n]$, it holds that

$$I_p(V_{i_1}; V_{i_2} \mid V_{i_3}, \ldots, V_{i_j}) = l_{j-1}. \tag{7}$$

In other words, $I_p(V_{i_1}; V_{i_2}) = l_1$ for $j = 2$.

Remark 2: Correlation level was introduced in [9] for blockwise $(2, 2)$ SSSs, and the notion was extended to symbolwise (k, n) SSSs in [10]. In [10], correlation level is defined as $(n-1)$-tuple rather than $(k-1)$-tuple since decoding from more than k shares is also considered. However, since we only consider decoding from just k shares in this paper, we define correlation level as Definition 1.

Remark 3: From (7) and the chain rule of mutual information, for any $j \in [2, k]$ and distinct j shares $V_{i_1}, \ldots, V_{i_j}$,

$$I_p(V_{i_j}; V_{i_1}, \ldots, V_{i_{j-1}}) = \sum_{\ell=1}^{j-1} l_\ell. \tag{8}$$

2.3 Known Results

For the case without cheating detection, Yamamoto [4] gave a construction of a strong (k, L, n) ramp SSS for a secret S^L uniformly distributed over $\mathrm{GF}(p^m)^L$, where p^m satisfies

$$(k < p^m,\ n \le p^m - L + 1) \text{ or } (n = k \ge p^m,\ L = 1). \tag{9}$$

In Yamamoto's scheme, shares $V_1, \ldots, V_n \in \mathrm{GF}(p^m)$ are given by

$$[V_1 \ \cdots \ V_n] := [S_1 \ \cdots \ S_L \ R_1 \ \cdots \ R_{k-L}]A. \tag{10}$$

Here, $(R_1, \ldots, R_{k-L})$ is a uniform random number over $\mathrm{GF}(p^m)^{k-L}$, and $A \in \mathrm{GF}(p^m)^{k\times n}$ is a matrix such that any k column vectors out of $\{\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n, \boldsymbol{e}_1, \ldots, \boldsymbol{e}_L\}$ are linearly independent, where $\{\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n\}$ and $\{\boldsymbol{e}_1, \ldots, \boldsymbol{e}_k\}$ denote the n columns of A and the k columns of k-dimensional unit matrix, respectively. The matrix A is called a generator matrix of a strong (k, L, n) ramp SSS. Its existence is guranteed if (9) holds.

We note that in the case of $L = 1$, Yamamoto's scheme is reduced to Karnin et al.'s [14] for (k, n) SSSs, which can be applied to S not necessarily uniformly distributed.

Next, we consider schemes with cleating detection capability. For (k, n) SSSs against impersonation attacks, Koga–Koyano [10] derived the following theorem[†].

[†]Theorem 1 is a special case of [10, Theorem 1], which also treats more general attacks than impersonation attacks and decoding with more than k shares.

Theorem 1 ([10, Theorem 1]): For any (k, n) SSS with correlation level $(l_1, \ldots, l_{k-1})$,

$$\log|\mathcal{V}_i| \ge H(S) + \sum_{j=1}^{k-1} l_j, \quad i = 1, \ldots, n, \tag{11}$$

$$\log|\mathcal{R}| \ge (k-1)H(S) + \sum_{j=1}^{k-1} j l_j, \tag{12}$$

$$\log P_{\mathrm{imp}^*(1)} \ge -\sum_{j=1}^{k-1} l_j. \tag{13}$$

Furthermore, Koga–Koyano proposed a scheme which achieves the bounds (11)–(13) when S is uniformly distributed.

Ogata et al. [6] derived a lower bound on the success probability of substitution attack for (k, n) SSS with the given size of shares.

Theorem 2 ([6, Theorem 3.2]): For any (k, n) SSS, it holds that

$$P_{\mathrm{sub}(a)} \ge \frac{|\mathcal{S}| - 1}{|\mathcal{V}_i| - 1}, \quad a = 1, \ldots, k-1. \tag{14}$$

From (14), any (k, n) SSS with $P_{\mathrm{sub}(a)} \le \delta$ requires $|\mathcal{V}_i| \ge (|\mathcal{S}| - 1)/\delta + 1$. Ogata et al. also proposed a scheme which achieves their bound (14) when S is uniformly distributed and the size of shares satisfies a certain condition.

We also note that Cabello et al. [7] proposed another (k, n) SSS with detection of substitution attacks[††], which corresponds to the case of $L = 1$ of our (k, L, n) ramp SSS proposed in Sect. 4.

[††]Cabello et al.'s scheme is for general access structures.

3. Converse Part

In this section, we will derive lower bounds on the sizes of the shares and random number used in encoding and the success probabilities of attacks. We also give bounds on the success probabilities of attacks for the given size of shares. Theorems 3 and 4 hold for any base of logarithm larger than 1, as long as the same base is used for entropy, mutual information, and correlation level. For simplicity of notation, we omit the base of logarithm.

Theorem 3: For any (k, L, n) ramp SSS (φ, ψ) with correlation level $(l_1, \ldots, l_{k-1})$,

$$\log|\mathcal{V}_i| \ge \frac{1}{L}H(S^L) + \sum_{j=1}^{k-1} l_j, \quad i = 1, \ldots, n, \tag{15}$$

$$\log|\mathcal{R}| \ge \frac{k-L}{L}H(S^L) + \sum_{j=1}^{k-1} j l_j, \tag{16}$$

$$\log P_{\mathrm{imp}^*(a)} \ge -\sum_{j=1}^{a}\sum_{j'=1}^{k-a} l_{j+j'-1}, \quad a = 1, \ldots, k-1, \tag{17}$$

$$\log P_{\mathrm{sub}(a)} \geq \log P_{\mathrm{imp}(a)} \geq -\sum_{j=1}^{a}\sum_{j'=1}^{k-a} l_{j+j'-1} + \log\left(1 - Q_{\max,L}\right), \quad a = L, \ldots, k-1, \quad (18)$$

where

$$Q_{\max,L} := \max_{s^L \in \mathcal{S}^L} P_{S^L}(s^L). \quad (19)$$

Furthermore, if (φ, ψ) is a strong (k, L, n) ramp SSS, then

$$\log P_{\mathrm{sub}(a)} \geq \log P_{\mathrm{imp}(a)} \geq -\sum_{j=1}^{a}\sum_{j'=1}^{k-a} l_{j+j'-1} + \log\left(1 - (Q_{\max})^a\right), \quad a = 1, \ldots, L-1, \quad (20)$$

where

$$Q_{\max} := \max_{s \in \mathcal{S}} P_S(s). \quad (21)$$

Lower bounds (15)–(17) can be proved in the same way as Theorem 1, i.e. [10, Theorem 1] . Note that (17) does not give any lower bound of $P_{\mathrm{imp}(a)}$ and $P_{\mathrm{sub}(a)}$ as described in Remark 1. Yet, by deriving a relation between $P_{\mathrm{imp}^*(a)}$ and $P_{\mathrm{imp}(a)}$, we can prove (18) and (20) as shown later.

Proof of Theorem 3: First, we prove (15). For any $\mathcal{K} \subseteq [n]$ with $|\mathcal{K}| = k$ and any $i \in \mathcal{K}$, it holds that

$$\begin{aligned} H(V_i) &= H(V_i \mid V_{\mathcal{K}\setminus\{i\}}) + I(V_i; V_{\mathcal{K}\setminus\{i\}}) \\ &\geq I(V_i; S^L \mid V_{\mathcal{K}\setminus\{i\}}) + I(V_i; V_{\mathcal{K}\setminus\{i\}}) \\ &= \frac{1}{L} H(S^L) + \sum_{j=1}^{k-1} l_j, \end{aligned} \quad (22)$$

where the last equality holds from (7) and $I(V_i; S^L \mid V_{\mathcal{K}\setminus\{i\}}) = H(S^L)/L$ derived from (1) and (2). Combining (22) with $\log|\mathcal{V}_i| \geq H(V_i)$, we obtain (15).

For any $\{i_1, \ldots, i_k\} \subseteq [n]$, we can derive (16) as follows:

$$\begin{aligned} \log|\mathcal{R}| \geq H(R) &\overset{\text{(a)}}{\geq} H(V_{i_1}, \ldots, V_{i_k}) - H(S^L) \\ &= \sum_{j=1}^{k} H(V_{i_j} \mid V_{i_1}, \ldots, V_{i_{j-1}}) - H(S^L) \\ &\overset{\text{(b)}}{\geq} \sum_{j=1}^{k} \left(\frac{1}{L} H(S^L) + \sum_{\ell=j}^{k-1} l_\ell \right) - H(S^L) \\ &= \frac{k-L}{L} H(S^L) + \sum_{j=1}^{k-1} j l_j, \end{aligned} \quad (23)$$

where (a) holds because $(V_{i_1}, \ldots, V_{i_k})$ is determined by (S^L, R), and (b) holds because for any $j \in [k]$, (8) and (22) implies that.

$$\begin{aligned} H(V_{i_j} \mid V_{i_1}, \ldots, V_{i_{j-1}}) &= H(V_{i_j}) - I(V_{i_j}; V_{i_1}, \ldots, V_{i_{j-1}}) \\ &\geq \frac{1}{L} H(S^L) + \sum_{\ell=1}^{k-1} l_\ell - \sum_{\ell=1}^{j-1} l_\ell \\ &= \frac{1}{L} H(S^L) + \sum_{\ell=j}^{k-1} l_\ell. \end{aligned} \quad (24)$$

Next, we will prove (17). Let $a \in [k-1]$, $\mathcal{O} = \{i_1, \ldots, i_a\} \subseteq [n]$, and $\mathcal{I} = \{i_{a+1}, \ldots, i_k\} \subseteq [n] \setminus \mathcal{O}$. Suppose that $V_{\mathcal{O}}$ is forged as $\overline{V}_{\mathcal{O}}$ and $V_{\mathcal{I}}$ is legitimate. Define $\mathcal{A} \subseteq \mathcal{V}_{i_1} \times \cdots \times \mathcal{V}_{i_k}$ as $\mathcal{A} := \{(v_{\mathcal{O}}, v_{\mathcal{I}}) : \psi(v_{\mathcal{O}}, v_{\mathcal{I}}) \neq \perp\}$. Then, (17) can be derived as follows:

$$\begin{aligned} \log P_{\mathrm{imp}^*(a)} &\overset{\text{(a)}}{\geq} \log \sum_{(v_{\mathcal{O}}, v_{\mathcal{I}}) \in \mathcal{A}} P_{V_{\mathcal{O}}}(v_{\mathcal{O}}) P_{V_{\mathcal{I}}}(v_{\mathcal{I}}) \\ &\overset{\text{(b)}}{=} -\left(\sum_{(v_{\mathcal{O}}, v_{\mathcal{I}}) \in \mathcal{A}} P_{V_{\mathcal{O}} V_{\mathcal{I}}}(v_{\mathcal{O}}, v_{\mathcal{I}}) \right) \cdot \log \frac{\sum_{(v_{\mathcal{O}}, v_{\mathcal{I}}) \in \mathcal{A}} P_{V_{\mathcal{O}} V_{\mathcal{I}}}(v_{\mathcal{O}}, v_{\mathcal{I}})}{\sum_{(v_{\mathcal{O}}, v_{\mathcal{I}}) \in \mathcal{A}} P_{V_{\mathcal{O}}}(v_{\mathcal{O}}) P_{V_{\mathcal{I}}}(v_{\mathcal{I}})} \\ &\overset{\text{(c)}}{\geq} -\sum_{(v_{\mathcal{O}}, v_{\mathcal{I}}) \in \mathcal{A}} P_{V_{\mathcal{O}} V_{\mathcal{I}}}(v_{\mathcal{O}}, v_{\mathcal{I}}) \log \frac{P_{V_{\mathcal{O}} V_{\mathcal{I}}}(v_{\mathcal{O}}, v_{\mathcal{I}})}{P_{V_{\mathcal{O}}}(v_{\mathcal{O}}) P_{V_{\mathcal{I}}}(v_{\mathcal{I}})} \\ &= -I(V_{i_1}, \ldots, V_{i_a}; V_{i_{a+1}}, \ldots, V_{i_k}) \\ &= -\sum_{j=1}^{a} I(V_{i_j}; V_{i_{a+1}}, \ldots, V_{i_k} \mid V_{i_1}, \ldots, V_{i_{j-1}}) \\ &= -\sum_{j=1}^{a}\sum_{j'=1}^{k-a} I(V_{i_j}; V_{i_{a+j'}} \mid V_{i_1}, \ldots, V_{i_{j-1}}, V_{i_{a+1}}, \ldots, V_{i_{a+j'-1}}) \\ &= -\sum_{j=1}^{a}\sum_{j'=1}^{k-a} l_{j+j'-1}. \end{aligned} \quad (25)$$

Here, (a) follows from that the RHS is the probability such that an impersonation attack generating $\overline{V}_{\mathcal{O}}$ according to $P_{V_{\mathcal{O}}}$ is not detected, (b) from that $\sum_{(v_{\mathcal{O}}, v_{\mathcal{I}}) \in \mathcal{A}} P_{V_{\mathcal{O}} V_{\mathcal{I}}}(v_{\mathcal{O}}, v_{\mathcal{I}}) = 1$, and (c) from the log-sum inequality.

In order to derive (18) and (20), we need the following lemma.

Lemma 1: Suppose that for any $\mathcal{O} \subseteq [n]$ with $|\mathcal{O}| = a$ and any $\mathcal{I} \subseteq [n] \setminus \mathcal{O}$ with $|\mathcal{I}| = k - a$,

$$\Pr\{\psi(\overline{V}_{\mathcal{O}}, V_{\mathcal{I}}) = S^L\} \leq \varepsilon \Pr\{\psi(\overline{V}_{\mathcal{O}}, V_{\mathcal{I}}) \neq \perp\}. \quad (26)$$

Then,

$$P_{\mathrm{imp}(a)} \geq (1 - \varepsilon) P_{\mathrm{imp}^*(a)}. \quad (27)$$

Proof: From the definition of $P_{\mathrm{imp}(a)}$ given by (5), we have

$$\begin{aligned} P_{\mathrm{imp}(a)} &\geq \Pr\{\psi(\overline{V}_{\mathcal{O}}, V_{\mathcal{I}}) \notin \{S^L, \perp\}\} \\ &= \Pr\{\psi(\overline{V}_{\mathcal{O}}, V_{\mathcal{I}}) \neq \perp\} - \Pr\{\psi(\overline{V}_{\mathcal{O}}, V_{\mathcal{I}}) = S^L\} \\ &\geq (1 - \varepsilon) \Pr\{\psi(\overline{V}_{\mathcal{O}}, V_{\mathcal{I}}) \neq \perp\}, \end{aligned} \quad (28)$$

where the last inequality follows from (26). Since (28) holds for any $(\overline{V}_{\mathcal{O}}, V_{\mathcal{I}})$ satisfying the maximization condition of (4), we obtain (27). □

Now we prove (18). For any $a \in [L, k-1]$, any $\mathcal{O} \subseteq [n]$ with $|\mathcal{O}| = a$, any $\mathcal{I} \subseteq [n] \setminus \mathcal{O}$ with $|\mathcal{I}| = k - a$, and any $P_{\overline{V}_{\mathcal{O}}}$, we have that

$$\begin{aligned}
&\Pr\{\psi(\overline{V}_{\mathcal{O}}, V_{\mathcal{I}}) = S^L\} \\
&= \sum_{s^L \in \mathcal{S}^L} \Pr\{S^L = s^L\} \Pr\{\psi(\overline{V}_{\mathcal{O}}, V_{\mathcal{I}}) = s^L\} \\
&\leq Q_{\max,L} \sum_{s^L \in \mathcal{S}^L} \Pr\{\psi(\overline{V}_{\mathcal{O}}, V_{\mathcal{I}}) = s^L\} \\
&= Q_{\max,L} \Pr\{\psi(\overline{V}_{\mathcal{O}}, V_{\mathcal{I}}) \neq \perp\}, \qquad (29)
\end{aligned}$$

where the first equality holds since S^L, $\overline{V}_{\mathcal{O}}$, and $V_{\mathcal{I}}$ are mutually independent by the definitions of impersonation attacks and (k, L, n) ramp SSSs. Combining (29) with Lemma 1, we obtain

$$P_{\mathrm{imp}(a)} \geq (1 - Q_{\max,L})\, P_{\mathrm{imp}^*(a)}, \quad a = L, \ldots, k-1. \qquad (30)$$

Hence, (18) holds from (17), (30), and $P_{\mathrm{sub}(a)} \geq P_{\mathrm{imp}(a)}$.

Finally, we prove (20). Suppose that (φ, ψ) is a strong (k, L, n) ramp SSS, and fix $a \in [L-1]$, $\mathcal{O} \subseteq [n]$ with $|\mathcal{O}| = a$, $\mathcal{I} \subseteq [n] \setminus \mathcal{O}$ with $|\mathcal{I}| = k - a$, and $P_{\overline{V}_{\mathcal{O}}}$ arbitrarily. Denote by $\psi(\overline{V}_{\mathcal{O}}, V_{\mathcal{I}})_{[a]}$ the first a symbols of $\psi(\overline{V}_{\mathcal{O}}, V_{\mathcal{I}})$ if $\psi(\overline{V}_{\mathcal{O}}, V_{\mathcal{I}}) \neq \perp$. Otherwise, define $\psi(\overline{V}_{\mathcal{O}}, V_{\mathcal{I}})_{[a]} = \perp$. Similarly, let $S^L_{[a]}$ be the first a symbols of S^L. Then, we have

$$\begin{aligned}
&\Pr\{\psi(\overline{V}_{\mathcal{O}}, V_{\mathcal{I}}) = S^L\} \leq \Pr\{\psi(\overline{V}_{\mathcal{O}}, V_{\mathcal{I}})_{[a]} = S^L_{[a]}\} \\
&= \sum_{s^a \in \mathcal{S}^a} \Pr\{S^L_{[a]} = s^a\} \Pr\{\psi(\overline{V}_{\mathcal{O}}, V_{\mathcal{I}})_{[a]} = s^a\} \\
&\leq (Q_{\max})^a \sum_{s^a \in \mathcal{S}^a} \Pr\{\psi(\overline{V}_{\mathcal{O}}, V_{\mathcal{I}})_{[a]} = s^a\} \\
&= (Q_{\max})^a \Pr\{\psi(\overline{V}_{\mathcal{O}}, V_{\mathcal{I}}) \neq \perp\}, \qquad (31)
\end{aligned}$$

where the first equality holds since $S_{[a]}$, $\overline{V}_{\mathcal{O}}$, and $V_{\mathcal{I}}$ are mutually independent. Combining (31) with Lemma 1, we obtain

$$P_{\mathrm{imp}(a)} \geq \left(1 - (Q_{\max})^a\right) P_{\mathrm{imp}^*(a)}, \quad a = 1, \ldots, L-1. \qquad (32)$$

Hence, (20) follows from (17), (32), and $P_{\mathrm{sub}(a)} \geq P_{\mathrm{imp}(a)}$. □

The next theorem gives lower bounds of $P_{\mathrm{imp}^*(1)}$, $P_{\mathrm{imp}(1)}$, $P_{\mathrm{sub}(a)}$ based on the cardinalities of shares, i.e., $|\mathcal{V}_i|$.

Theorem 4: For any (k, L, n) ramp SSS (φ, ψ) and any $i \in [n]$, it holds that

$$\log P_{\mathrm{imp}^*(1)} \geq \frac{1}{L} H(S^L) - \log |\mathcal{V}_i|. \qquad (33)$$

Furthermore, if (φ, ψ) is a strong (k, L, n) ramp SSS,

$$\begin{aligned}
\log P_{\mathrm{sub}(a)} &\geq \log P_{\mathrm{imp}(1)} \\
&\geq \frac{1}{L} H(S^L) - \log |\mathcal{V}_i| + \log(1 - Q_{\max}), \\
&\qquad a = 1, \ldots, k-1. \qquad (34)
\end{aligned}$$

Proof of Theorem 4: From (22) and (25), for any $\mathcal{K} \subseteq [n]$ with $|\mathcal{K}| = k$ and any $i \in \mathcal{K}$,

$$\log |\mathcal{V}_i| \geq \frac{1}{L} H(S^L) + I(V_i; V_{\mathcal{K} \setminus \{i\}}), \qquad (35)$$

$$\log P_{\mathrm{imp}^*(1)} \geq -I(V_i; V_{\mathcal{K} \setminus \{i\}}). \qquad (36)$$

Hence we have (33).

Furthermore, if (φ, ψ) is a strong (k, L, n) ramp SSS, then from (32) and (33), we have the second inequality in (34). On the other hand, the first inequality in (34) holds since $P_{\mathrm{sub}(a)} \geq P_{\mathrm{sub}(1)} \geq P_{\mathrm{imp}(1)}$ holds for $1 \leq a \leq k-1$. Hence Theorem 4 is proved. □

Remark 4: We note that (15)–(18) in Theorem 3 and (33) in Theorem 4 hold even if S_j is not i.i.d. for $1 \leq j \leq k$. If S_j is i.i.d., we have in Theorems 3 and 4 that $\frac{1}{L} H(S^L) = H(S)$, $\frac{k-L}{L} H(S^L) = (k-L) H(S)$, and $Q_{\max,L} = (Q_{\max})^L$.

Remark 5: When S_j is uniformly distributed over $\mathcal{S}$, from (34) we have

$$P_{\mathrm{sub}(a)} \geq \frac{|\mathcal{S}| - 1}{|\mathcal{V}_i|}, \quad a = 1, \ldots, k-1. \qquad (37)$$

We note that this bound is not tight because it is looser than Ogata et al.'s bound (14) in the case of $L = 1$.

4. Direct Part

In this section, we propose a strong (k, L, n) ramp SSS against substitution attacks. Here, we assume that each S_j is uniformly distributed over $\mathcal{S} = \mathrm{GF}(p^m)$, where m is a positive integer and p is a prime number satisfying $p \geq L + 2$. Also, let $l \in [m]$, and we assume that the following two conditions hold:

$$(k < p^m,\ n \leq p^m - L + 1) \text{ or } (n = k \geq p^m,\ L = 1), \qquad (38)$$

$$(k < p^l,\ n \leq p^l) \text{ or } (n = k \geq p^l). \qquad (39)$$

Let $f : \mathrm{GF}(p^m) \to \mathrm{GF}(p^l)$ be a surjective linear mapping. Then, from Lemma 4 in Appendix, f satisfies the following properties:

$$\forall x_1, x_2 \in \mathrm{GF}(p^m),\ f(x_1 + x_2) = f(x_1) + f(x_2), \qquad (40)$$

$$\forall y \in \mathrm{GF}(p^l),\ |\{x \in \mathrm{GF}(p^m) : f(x) = y\}| = p^{m-l}. \qquad (41)$$

For instance, f is given by the mapping that extracts l

digits of fixed positions from m digits of x in vector representation.

Now we explain the encoding procedure. We define each share V_i, $1 \le i \le n$, as $V_i := (W_i, U_i)$, where $W_i \in \mathrm{GF}(p^m)$ is a share of $S^L = S_1 S_2 \ldots S_L$ obtained by a linear strong (k, L, n) ramp SSS, and $U_i \in \mathrm{GF}(p^l)$ is a share of $f\Big(\sum_{j=1}^{L}(S_j)^{j+1}\Big)$ obtained by a linear (k, n) SSS. Specifically, we define W_i and U_i as follows:

$$[W_1 \ \cdots \ W_n] = [S_1 \ \cdots \ S_L \ R_1 \ \cdots \ R_{k-L}]A, \tag{42}$$

$$[U_1 \ \cdots \ U_n] = \Big[f\Big(\sum_{j=1}^{L}(S_j)^{j+1}\Big) \ R'_1 \ \cdots \ R'_{k-1}\Big]B, \tag{43}$$

where A and B are generator matrices of a strong (k, L, n) ramp SSS and a (k, n) SSS, respectively, and $(R_1, \ldots, R_{k-L}, R'_1, \ldots, R'_{k-1})$ is a uniform random number over $\mathrm{GF}(p^m)^{k-L} \times \mathrm{GF}(p^l)^{k-1}$.

Next we describe the decoding procedure. Let $\widehat{V}_{i_1}, \ldots, \widehat{V}_{i_k}$ be the input of the decoder, where $\widehat{V}_{i_j} = (\widehat{W}_{i_j}, \widehat{U}_{i_j})$ for $1 \le j \le k$. In order to define the decoder, we derive a relationship among legitimate shares $(W_{i_1}, U_{i_1}), \ldots, (W_{i_k}, U_{i_k})$. Define $C \in \mathrm{GF}(p^m)^{k\times k}$ and $D \in \mathrm{GF}(p^l)^{k\times k}$ as

$$C = (c_{ij}) := \big[\boldsymbol{a}_{i_1} \quad \cdots \quad \boldsymbol{a}_{i_k}\big]^{-1}, \tag{44}$$

$$D = (d_{ij}) := \big[\boldsymbol{b}_{i_1} \quad \cdots \quad \boldsymbol{b}_{i_k}\big]^{-1}, \tag{45}$$

where $(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n)$ and $(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n)$ are the columns of A and B, respectively. Then, from (42) and (43) we have

$$[S_1 \ \cdots \ S_L \ R_1 \ \cdots \ R_{k-L}] = [W_{i_1} \ \cdots \ W_{i_k}]C, \tag{46}$$

$$\Big[f\Big(\sum_{j=1}^{L}(S_j)^{j+1}\Big) \ R'_1 \ \cdots \ R'_{k-1}\Big] = [U_{i_1} \ \cdots \ U_{i_k}]D. \tag{47}$$

Consequently,

$$S_j = \sum_{\ell=1}^{k} c_{\ell j} W_{i_\ell}, \quad j = 1, \ldots, L, \tag{48}$$

$$R_j = \sum_{\ell=1}^{k} c_{\ell(j+L)} W_{i_\ell}, \quad j = 1, \ldots, k-L, \tag{49}$$

$$f\Big(\sum_{j=1}^{L}(S_j)^{j+1}\Big) = \sum_{\ell=1}^{k} d_{\ell 1} U_{i_\ell}, \tag{50}$$

$$R'_j = \sum_{\ell=1}^{k} d_{\ell(j+1)} U_{i_\ell}, \quad j = 1, \ldots, k-1. \tag{51}$$

From (48) and (50), it always holds for legitimate shares that

$$f\Big(\sum_{j=1}^{L}\Big(\sum_{\ell=1}^{k} c_{\ell j} W_{i_\ell}\Big)^{j+1}\Big) = \sum_{\ell=1}^{k} d_{\ell 1} U_{i_\ell}. \tag{52}$$

Accordingly, for the input $(\widehat{W}_{i_1}, \widehat{U}_{i_1}), \ldots, (\widehat{W}_{i_k}, \widehat{U}_{i_k})$, the decoder checks the following relation:

$$f\Big(\sum_{j=1}^{L}\Big(\sum_{\ell=1}^{k} c_{\ell j} \widehat{W}_{i_\ell}\Big)^{j+1}\Big) = \sum_{\ell=1}^{k} d_{\ell 1} \widehat{U}_{i_\ell}. \tag{53}$$

If (53) holds, the decoder outputs $\widehat{S}^L = \widehat{S}_1 \ldots \widehat{S}_L$ where

$$\widehat{S}_j = \sum_{\ell=1}^{k} c_{\ell j} \widehat{W}_{i_\ell}, \quad j = 1, \ldots, L. \tag{54}$$

Otherwise, the decoder outputs $\perp$.

Theorem 5: The above scheme is a strong (k, L, n) ramp SSS with correlation level $(0, \ldots, 0, l)_p$ such that

$$\log_p |\mathcal{V}_i| = m + l, \quad i = 1, \ldots, n, \tag{55}$$

$$\log_p |\mathcal{R}| = (k - L)m + (k - 1)l, \tag{56}$$

$$P_{\mathrm{imp}^*(a)} = p^{-l}, \quad a = 1, \ldots, k-1, \tag{57}$$

$$P_{\mathrm{imp}(a)} = p^{-l}(1 - p^{-m\cdot\min\{a,L\}}), \quad a = 1, \ldots, k-1, \tag{58}$$

$$P_{\mathrm{sub}(a)} \le Lp^{-l}, \quad a = 1, \ldots, k-1. \tag{59}$$

Remark 6: By comparing Theorem 5 with Theorem 3, we note that in the proposed scheme, $|\mathcal{V}_i|$, $|\mathcal{R}|$, $P_{\mathrm{imp}^*(a)}$, $1 \le a \le k-1$, and $P_{\mathrm{imp}(a)}$, $L \le a \le k-1$, achieves the minimums in (k, L, n) ramp SSSs with correlation level $(0, \ldots, 0, l)_p$. Also, $\log_p P_{\mathrm{sub}(a)}$, $L \le a \le k-1$, is within $\log_p L - \log_p(1 - p^{-mL})$ from the bound (18). In addition, $P_{\mathrm{imp}(a)}$, $1 \le a \le L-1$, achieves the minimum in strong (k, L, n) ramp SSSs with correlation level $(0, \ldots, 0, l)_p$, and $\log_p P_{\mathrm{sub}(a)}$, $1 \le a \le L-1$, is within $\log_p L - \log_p(1 - p^{-ma})$ from the bound (20). Furthermore, by comparing (37) with (59), $P_{\mathrm{sub}(a)}$, $1 \le a \le k-1$, is within $L/(1 - p^{-m})$ times the lower bound of strong (k, L, n) ramp SSSs with $|\mathcal{V}_i| = p^{m+l}$. Table 1 summarizes the success probabilities of substitution attacks and impersonation attacks for the proposed scheme.

Remark 7: It is an open problem whether we can construct a strong (k, L, n) ramp SSS with any given correlation level $(l_1, \ldots, l_{k-1})_p$ such that $l_1, \ldots, l_{k-2}$ can also contribute to detection of substitution attacks.

Now, we prove Theorem 5.

Proof of Theorem 5: First we prove the following lemma.

Lemma 2: For any $\{i_1, \ldots, i_k\} \subseteq [n]$, $(2k-1)$-tuple $(W_{i_1}, \ldots, W_{i_k}, U_{i_1}, \ldots, U_{i_{k-1}})$ is uniformly distributed over $\mathrm{GF}(p^m)^k \times \mathrm{GF}(p^l)^{k-1}$. In particular, these $2k-1$ random variables are mutually independent.

Proof: From (48)–(51) and $d_{k1} \neq 0$, which follows from (50) and the definition of (k, n) SSSs, there is a one-to-one correspondence between $(W_{i_1}, \ldots, W_{i_k}, U_{i_1}, \ldots, U_{i_{k-1}})$ and $(S_1, \ldots, S_L, R_1, \ldots, R_{k-L}, R'_1, \ldots, R'_{k-1})$. Indeed, when $W_{i_1}, \ldots, W_{i_k}, U_{i_1}, \ldots, U_{i_{k-1}}$ are given, $S_1, \ldots, S_L, R_1, \ldots, R_{k-L}$ are determined by (48) and (49), and $R'_1, \ldots, R'_{k-1}$

Table 1 Success probabilities of substitution attacks and impersonation attacks (c.l.: correlation level, l.b.: lower bound, l.b.^{*1}: (18), l.b.^{*2}: (20)).

		Among (k, L, n) ramp SSSs with c.l. $(0, \ldots, 0, l)_p$	Among strong (k, L, n) ramp SSSs with c.l. $(0, \ldots, 0, l)_p$
$P_{\mathrm{imp}^*(a)}$	$(1 \le a \le k-1)$	optimal	optimal
$P_{\mathrm{imp}(a)}$	$(1 \le a \le L-1)$	(l.b. is unknown)	optimal
$P_{\mathrm{imp}(a)}$	$(L \le a \le k-1)$	optimal	optimal
$P_{\mathrm{sub}(a)}$	$(1 \le a \le L-1)$	(l.b. is unknown)	Less than nearly L times l.b.^{*2}
$P_{\mathrm{sub}(a)}$	$(L \le a \le k-1)$	Less than nearly L times l.b.^{*1}	Less than nearly L times l.b.^{*1}

are determined by

$$\begin{aligned} R'_j &= \sum_{\ell=1}^{k} d_{\ell(j+1)} U_{i_\ell} \\ &= \sum_{\ell=1}^{k-1} d_{\ell(j+1)} U_{i_\ell} \\ &\quad + \frac{d_{k(j+1)}}{d_{k1}} \left[f\left(\sum_{j=1}^{L} \left(\sum_{\ell=1}^{k} c_{\ell j} W_{i_\ell} \right)^{j+1} \right) - \sum_{\ell=1}^{k-1} d_{\ell 1} U_{i_\ell} \right], \\ &\quad j = 1, \ldots, k-1. \end{aligned} \tag{60}$$

Hence, from the assumption that each S_j is uniformly distributed, $(W_{i_1}, \ldots, W_{i_k}, U_{i_1}, \ldots, U_{i_{k-1}})$ is uniformly distributed over $\mathrm{GF}(p^m)^k \times \mathrm{GF}(p^l)^{k-1}$. In particular, these $2k-1$ random variables are mutually independent. □

In order to prove Theorem 5, it suffices to prove the following Claims 1–4:

Claim 1: (φ, ψ) is a strong (k, L, n) ramp SSS.

Claim 2: Correlation level is $(0, \ldots, 0, l)_p$.

Claim 3: $|\mathcal{V}_i|$ and $|\mathcal{R}|$ satisfy (55) and (56), respectively.

Claim 4: The success probabilities of attacks satisfy (57)–(59).

Proof of Claim 1: From legitimate k shares, S^L can be decoded correctly. Also, for any $j \in [L]$ and any $\mathcal{I} \subseteq [n]$ with $|\mathcal{I}| = k - j$, it holds that

$$\begin{aligned} H(S^L \mid V_{\mathcal{I}}) &= H(S^L \mid W_{\mathcal{I}}, U_{\mathcal{I}}) \\ &\overset{(a)}{=} H(S^L \mid W_{\mathcal{I}}) \overset{(b)}{=} \frac{j}{L} H(S^L), \end{aligned} \tag{61}$$

where (a) and (b) hold from the following reasons.

(a) $W_{\mathcal{I}} \to S^L \to \sum_{j=1}^{L} (S_j)^{j+1} \to U_{\mathcal{I}}$ forms a Markov chain in this order. Furthermore, since $U_{\mathcal{I}}$ is a set of $k-j$ shares of $\sum_{j=1}^{L} (S_j)^{j+1}$ by a (k, n) SSS, $U_{\mathcal{I}}$ and $\sum_{j=1}^{L} (S_j)^{j+1}$ are statistically independent. Hence $(S^L, W_{\mathcal{I}})$ and $U_{\mathcal{I}}$ are statistically independent, which implies equality (a).

(b) $W_{\mathcal{I}}$ is a set of $k-j$ shares of S^L by a (k, L, n) ramp SSS.

In addition, for any $\mathcal{J} \subseteq [L]$ with $|\mathcal{J}| = j$,

$$\begin{aligned} H(S_{\mathcal{J}} \mid V_{\mathcal{I}}) &= H(S_{\mathcal{J}} \mid W_{\mathcal{I}}, U_{\mathcal{I}}) \\ &\overset{(c)}{=} H(S_{\mathcal{J}} \mid W_{\mathcal{I}}) \overset{(d)}{=} H(S_{\mathcal{J}}), \end{aligned} \tag{62}$$

where (c) holds since $(S_{\mathcal{J}}, W_{\mathcal{I}})$ and $U_{\mathcal{I}}$ are statistically independent, and (d) holds since $W_{\mathcal{I}}$ is a set of $k-j$ shares of S^L by a strong (k, L, n) ramp SSS. Hence, (φ, ψ) is a strong (k, L, n) ramp SSS. □

Proof of Claim 2: For any $j \in [2, k-1]$ and any distinct j shares $V_{i_1}, \ldots, V_{i_j}$, $I_p(V_{i_1}; V_{i_2} \mid V_{i_3}, \ldots, V_{i_j}) = 0$ because $V_{i_1}, \ldots, V_{i_j}$ are mutually independent (see, Lemma 2). In addition, for any distinct k shares $V_{i_1}, \ldots, V_{i_k}$, it holds that

$$\begin{aligned} &I_p(V_{i_1}; V_{i_2} \mid V_{i_3}, \ldots, V_{i_k}) \\ &\quad = H_p(V_{i_1} \mid V_{i_3}, \ldots, V_{i_k}) - H_p(V_{i_1} \mid V_{i_2}, V_{i_3}, \ldots, V_{i_k}) \\ &\quad = l. \end{aligned} \tag{63}$$

Here, the last equality holds since $W_{i_1}, \ldots, W_{i_k}, U_{i_2}, \ldots, U_{i_k}$ are mutually independent and U_{i_1} is a function of $W_{i_1}, \ldots, W_{i_k}, U_{i_2}, \ldots, U_{i_k}$. Consequently,

$$H_p(V_{i_1} \mid V_{i_3}, \ldots, V_{i_k}) = H_p(V_{i_1}) = m + l, \tag{64}$$

$$\begin{aligned} H_p(V_{i_1} \mid V_{i_2}, \ldots, V_{i_k}) &= H_p(W_{i_1}, U_{i_1} \mid V_{i_2}, \ldots, V_{i_k}) \\ &= H_p(W_{i_1} \mid V_{i_2}, \ldots, V_{i_k}) \\ &= H_p(W_{i_1}) = m. \end{aligned} \tag{65}$$

Thus, the correlation level of shares is $(0, \ldots, 0, l)_p$ proving our claim. □

Proof of Claim 3: (55) follows from $V_i \in \mathrm{GF}(p^m) \times \mathrm{GF}(p^l)$. Also, since the random number used in encoding is $(R_1, \ldots, R_{k-L}, R'_1, \ldots, R'_{k-1}) \in \mathrm{GF}(p^m)^{k-L} \times \mathrm{GF}(p^l)^{k-1}$, (56) is satisfied. □

Proof of Claim 4: For $1 \le a \le k-1$, suppose that in decoding, $V_{\mathcal{O}} = (W_{\mathcal{O}}, U_{\mathcal{O}})$, $\mathcal{O} = \{i_1, \ldots, i_a\}$, are forged into $\overline{V}_{\mathcal{O}} = (\overline{W}_{\mathcal{O}}, \overline{U}_{\mathcal{O}})$, and $V_{\mathcal{I}} = (W_{\mathcal{I}}, U_{\mathcal{I}})$, $\mathcal{I} = \{i_{a+1}, \ldots, i_k\}$, are legitimate. When the attack is not detected, the decoder outputs $\widetilde{S}^L = \widetilde{S}_1 \ldots \widetilde{S}_L$ obtained by

$$\widetilde{S}_j = \sum_{\ell=1}^{a} c_{\ell j} \overline{W}_{i_\ell} + \sum_{\ell=a+1}^{k} c_{\ell j} W_{i_\ell}. \tag{66}$$

Let

$$\begin{aligned} \Delta_j(W_{\mathcal{O}}, \overline{W}_{\mathcal{O}}) &= \widetilde{S}_j - S_j \\ &= \sum_{\ell=1}^{a} c_{\ell j} \overline{W}_{i_\ell} - \sum_{\ell=1}^{a} c_{\ell j} W_{i_\ell}, \quad j = 1, \ldots, L. \end{aligned} \tag{67}$$

From (53) and (54), attack is successful (i.e., $\psi(\overline{V}_O, V_{\mathcal{I}}) \notin \{S^L, \perp\}$) if

$$f\Big(\sum_{j=1}^{L}\Big(\sum_{\ell=1}^{a} c_{\ell j}\overline{W}_{i_\ell} + \sum_{\ell=a+1}^{k} c_{\ell j}W_{i_\ell}\Big)^{j+1}\Big) = \sum_{\ell=1}^{a} d_{\ell 1}\overline{U}_{i_\ell} + \sum_{\ell=a+1}^{k} d_{\ell 1}U_{i_\ell} \tag{68}$$

and

$$\Delta_j(W_O, \overline{W}_O) \neq 0 \quad \text{for some } j \in [L]. \tag{69}$$

On the other hand, from (52), the legitimate shares satisfy

$$f\Big(\sum_{j=1}^{L}\Big(\sum_{\ell=1}^{a} c_{\ell j}W_{i_\ell} + \sum_{\ell=a+1}^{k} c_{\ell j}W_{i_\ell}\Big)^{j+1}\Big) = \sum_{\ell=1}^{a} d_{\ell 1}U_{i_\ell} + \sum_{\ell=a+1}^{k} d_{\ell 1}U_{i_\ell}. \tag{70}$$

From (68), (70), and (40), we have

$$f\Big(g(\overline{W}_O, W_O, W_{\mathcal{I}})\Big) = \sum_{\ell=1}^{a} d_{\ell 1}(\overline{U}_{i_\ell} - U_{i_\ell}), \tag{71}$$

where $g(\overline{W}_O, W_O, W_{\mathcal{I}})$ is defined as

$$\begin{aligned} &g(\overline{W}_O, W_O, W_{\mathcal{I}}) \\ &:= \sum_{j=1}^{L}\Big(\sum_{\ell=1}^{a} c_{\ell j}\overline{W}_{i_\ell} + \sum_{\ell=a+1}^{k} c_{\ell j}W_{i_\ell}\Big)^{j+1} - \sum_{j=1}^{L}\Big(\sum_{\ell=1}^{a} c_{\ell j}W_{i_\ell} + \sum_{\ell=a+1}^{k} c_{\ell j}W_{i_\ell}\Big)^{j+1} \\ &= \sum_{j=1}^{L}\Big(\sum_{\ell=1}^{a} c_{\ell j}W_{i_\ell} + \sum_{\ell=a+1}^{k} c_{\ell j}W_{i_\ell} + \Delta_j(W_O, \overline{W}_O)\Big)^{j+1} - \sum_{j=1}^{L}\Big(\sum_{\ell=1}^{a} c_{\ell j}W_{i_\ell} + \sum_{\ell=a+1}^{k} c_{\ell j}W_{i_\ell}\Big)^{j+1}. \end{aligned} \tag{72}$$

Hence the condition $\psi(\overline{V}_O, V_{\mathcal{I}}) \notin \{S^L, \perp\}$ is given by (69) and (71), and the condition $\psi(\overline{V}_O, V_{\mathcal{I}}) \neq \perp$ is given by (71).

We prove that the success probabilities of impersonation attacks satisfy (57) and (58). First, (57) follows from

$$\begin{aligned} &\Pr\{\psi(\overline{V}_O, V_{\mathcal{I}}) \neq \perp\} \\ &= \Pr\Big\{f\Big(g(\overline{W}_O, W_O, W_{\mathcal{I}})\Big) = \sum_{\ell=1}^{a} d_{\ell 1}\overline{U}_{i_\ell} - \sum_{\ell=1}^{a} d_{\ell 1}U_{i_\ell}\Big\} \\ &\overset{(a)}{=} p^{-l}. \end{aligned} \tag{73}$$

Here (a) holds because $(\overline{W}_O, \overline{U}_O), W_O, U_O, W_{\mathcal{I}}$ are mutually independent, U_O is uniformly distributed over $\mathrm{GF}(p^m)^a$, and $d_{11}, \ldots, d_{a1}$ are non-zero by the definition of (k, n) SSSs.

Next, (58) follows from

$$\begin{aligned} &\Pr\{\psi(\overline{V}_O, V_{\mathcal{I}}) \notin \{S^L, \perp\}\} \\ &= \Pr\Big\{f\Big(g(\overline{W}_O, W_O, W_{\mathcal{I}})\Big) = \sum_{\ell=1}^{a} d_{\ell 1}\overline{U}_{i_\ell} - \sum_{\ell=1}^{a} d_{\ell 1}U_{i_\ell} \text{ and } \exists j \in [L], \sum_{\ell=1}^{a} c_{\ell j}\overline{W}_{i_\ell} \neq \sum_{\ell=1}^{a} c_{\ell j}W_{i_\ell}\Big\} \\ &\overset{(b)}{=} \sum_{(\overline{w}_O, \overline{u}_O) \in \overline{\mathcal{V}}_O} \Pr\{(\overline{W}_O, \overline{U}_O) = (\overline{w}_O, \overline{u}_O)\} \sum_{w_O : \exists j \in [L], \sum_{\ell=1}^{a} c_{\ell j}\overline{w}_{i_\ell} \neq \sum_{\ell=1}^{a} c_{\ell j}w_{i_\ell}} \Pr\{W_O = w_O\} \\ &\qquad \cdot \Pr\Big\{f\Big(g(\overline{w}_O, w_O, W_{\mathcal{I}})\Big) = \sum_{\ell=1}^{a} d_{\ell 1}\overline{u}_{i_\ell} - \sum_{\ell=1}^{a} d_{\ell 1}U_{i_\ell}\Big\} \\ &\overset{(c)}{=} p^{-l} \sum_{(\overline{w}_O, \overline{u}_O) \in \overline{\mathcal{V}}_O} \Pr\{(\overline{W}_O, \overline{U}_O) = (\overline{w}_O, \overline{u}_O)\} \cdot \Pr\Big\{\exists j \in [L], \sum_{\ell=1}^{a} c_{\ell j}\overline{w}_{i_\ell} \neq \sum_{\ell=1}^{a} c_{\ell j}W_{i_\ell}\Big\} \\ &\overset{(d)}{=} p^{-l}(1 - p^{-m \cdot \min\{a, L\}}), \end{aligned} \tag{74}$$

where (b)–(d) hold from the following reasons.

(b) $(\overline{W}_O, \overline{U}_O), W_O, U_O, W_{\mathcal{I}}$ are mutually independent.

(c) The following relation holds by the same reason as (a) in (73):

$$\Pr\Big\{f\Big(g(\overline{w}_O, w_O, W_{\mathcal{I}})\Big) = \sum_{\ell=1}^{a} d_{\ell 1}\overline{u}_{i_\ell} - \sum_{\ell=1}^{a} d_{\ell 1}U_{i_\ell}\Big\} = p^{-l}.$$

(d) Define $C_a \in \mathrm{GF}(p^m)^{a \times L}$ as the submatrix obtained from the first a rows of C. Then, (d) follows from

$$\begin{aligned} &\Pr\Big\{\exists j \in [L], \sum_{\ell=1}^{a} c_{\ell j}\overline{w}_{i_\ell} \neq \sum_{\ell=1}^{a} c_{\ell j}W_{i_\ell}\Big\} \\ &= \Pr\Big\{[\overline{w}_{i_1} - W_{i_1} \ \cdots \ \overline{w}_{i_a} - W_{i_a}]C_a \neq [0 \ \cdots \ 0]\Big\} \\ &\overset{(e)}{=} 1 - \frac{(p^m)^{a - \operatorname{rank} C_a}}{p^{ma}} \\ &= 1 - p^{-m \operatorname{rank} C_a} \\ &\overset{(f)}{=} 1 - p^{-m \cdot \min\{a, L\}}, \end{aligned} \tag{75}$$

where (e) holds because just $(p^m)^{a - \operatorname{rank} C_a}$ values of $(w_{i_1}, \ldots, w_{i_a}) \in \mathrm{GF}(p^m)^a$ satisfy $[\overline{w}_{i_1} - w_{i_1} \ \cdots \ \overline{w}_{i_a} - w_{i_a}]C_a = [0 \ \cdots \ 0]$, and W_O is uniformly distributed over $\mathrm{GF}(p^m)^a$. Finally, since $(W_{i_{L+1}}, \ldots, W_{i_k})$ is a set of $k - L$ shares of $(S_1, \ldots, S_L)$ by a (k, L, n) ramp SSS, $(S_1, \ldots, S_L)$ is still uniformly distributed over $\mathrm{GF}(p^m)^L$ when $W_{i_{L+1}}, \ldots, W_{i_k}$ are given. From this and

$$[S_1 \cdots S_L] = [W_{i_1} \cdots W_{i_L}]C_L + [W_{i_{L+1}} \cdots W_{i_k}] \begin{bmatrix} c_{(L+1)1} & \cdots & c_{(L+1)L} \\ \vdots & & \vdots \\ c_{k1} & \cdots & c_{kL} \end{bmatrix}, \tag{76}$$

C_L is regular, which implies $\operatorname{rank} C_a = \min\{a, L\}$. Hence (f) holds.

Now, we can prove (59). As $P_{\mathrm{sub}(a)}$ is non-decreasing in a, it suffices to focus on the special case when $a = k-1$, i.e., $\mathcal{O} = \{i_1, \dots, i_{k-1}\}$ and $\mathcal{I} = \{i_k\}$. We evaluate the success probability of substitution attack for the case that the values of forged shares are $V_O = v_O = (w_O, u_O)$. For each $q \in [L]$, define $\overline{\mathcal{V}}'_{O,q}$ as

$$\begin{aligned} \overline{\mathcal{V}}'_{O,q} := \{(\overline{w}_O, \overline{u}_O) \in (\mathrm{GF}(p^m) \times \mathrm{GF}(p^l))^{k-1} :& \\ \Pr\{(\overline{W}_O, \overline{U}_O) = (\overline{w}_O, \overline{u}_O) \mid V_O = v_O\} > 0,& \\ \Delta_q(w_O, \overline{w}_O) \neq 0,& \\ \Delta_j(w_O, \overline{w}_O) = 0, \quad j = q+1, \dots, L\}.& \end{aligned} \tag{77}$$

Then, the following lemma holds.

Lemma 3: Fix $q \in [L]$ and $(\overline{w}_O, \overline{u}_O) \in \overline{\mathcal{V}}'_{O,q}$ arbitrarily. Then, the equation

$$f(g(\overline{w}_O, w_O, w_{i_k})) = \sum_{\ell=1}^{k-1} d_{\ell 1}(\overline{u}_{i_\ell} - u_{i_\ell}) \tag{78}$$

has at most qp^{m-l} solutions for $w_{i_k} \in \mathrm{GF}(p^m)$.

Proof of Lemma 3: When $(\overline{w}_O, \overline{u}_O) \in \overline{\mathcal{V}}'_{O,q}$, $g(\overline{w}_O, w_O, w_{i_k})$ can be represented as

$$\begin{aligned} g(\overline{w}_O, w_O, w_{i_k}) &= \sum_{j=1}^{q} \left(\sum_{\ell=1}^{k-1} c_{\ell j} w_{i_\ell} + c_{kj} w_{i_k} + \Delta_j(w_O, \overline{w}_O) \right)^{j+1} \\ &\quad - \sum_{j=1}^{q} \left(\sum_{\ell=1}^{k-1} c_{\ell j} w_{i_\ell} + c_{kj} w_{i_k} \right)^{j+1}. \end{aligned} \tag{79}$$

Hence the polynomial $g(\overline{w}_O, w_O, w_{i_k})$ in w_{i_k} has degree at most q, and the term of degree q is

$$(q+1)(c_{kq} w_{i_k})^q \Delta_j(w_O, \overline{w}_O). \tag{80}$$

We have $q + 1 \neq 0$ and $\Delta_j(w_O, \overline{w}_O) \neq 0$ from $L + 1 < p$ and $(\overline{w}_O, \overline{u}_O) \in \overline{\mathcal{V}}'_{O,q}$, respectively. In addition, $c_{kq} \neq 0$ holds from (48) and the fact that no information on S_q can be obtained from $(W_{i_1}, \dots, W_{i_{k-1}})$. Hence the coefficient of $w_{i_k}^q$ in (80) is non-zero. Therefore, $g(\overline{w}_O, w_O, w_{i_k})$ is degree q in w_{i_k}.

In addition, the equation $f(\alpha) = \sum_{\ell=1}^{k-1} d_{\ell 1}(\overline{u}_{i_\ell} - u_{i_\ell})$ is satisfied for just p^{m-l} values of $\alpha \in \mathrm{GF}(p^m)$, say $\alpha_1, \dots, \alpha_{p^{m-l}}$. As $g(\overline{w}_O, w_O, w_{i_k})$ is degree q in w_{i_k}, for each $1 \leq j \leq p^{m-l}$, there are at most q values of $w_{i_k} \in \mathrm{GF}(p^m)$ satisfying $g(\overline{w}_O, w_O, w_{i_k}) = \alpha_j$. Hence (78) can be satisfied for at most qp^{m-l} values of $w_{i_k} \in \mathrm{GF}(p^m)$. □

Using Lemma 3, the success probability of substitution attack can be evaluated as follows.

$$\begin{aligned} &\Pr\{\psi(\overline{V}_O, V_{i_k}) \notin \{S^L, \perp\} \mid V_O = v_O\} \\ &= \Pr\{(69), (71) \mid V_O = v_O\} \\ &= \sum_{q=1}^{L} \sum_{\overline{v}_O \in \overline{\mathcal{V}}'_{O,q}} \Pr\{(71), \overline{V}_O = \overline{v}_O \mid V_O = v_O\} \\ &= \sum_{q=1}^{L} \sum_{\overline{v}_O \in \overline{\mathcal{V}}'_{O,q}} \Pr\{\overline{V}_O = \overline{v}_O \mid V_O = v_O\} \\ &\qquad \cdot \Pr\{(71) \mid V_O = v_O, \overline{V}_O = \overline{v}_O\} \\ &\overset{\text{(a)}}{\leq} Lp^{-l} \sum_{q=1}^{L} \sum_{\overline{v}_O \in \overline{\mathcal{V}}'_{O,q}} \Pr\{\overline{V}_O = \overline{v}_O \mid V_O = v_O\} \\ &\leq Lp^{-l}. \end{aligned} \tag{81}$$

Here, (a) holds since

$$\begin{aligned} &\Pr\{(71) \mid V_O = v_O, \overline{V}_O = \overline{v}_O\} \\ &\overset{\text{(b)}}{=} \Pr\left\{ f(g(\overline{w}_O, w_O, W_{i_k})) = \sum_{\ell=1}^{k-1} d_{\ell 1}(\overline{u}_{i_\ell} - u_{i_\ell}) \;\middle|\; V_O = v_O \right\} \\ &\overset{\text{(c)}}{\leq} p^{-m} \cdot qp^{m-l} = qp^{-l} \leq Lp^{-l}, \end{aligned} \tag{82}$$

where (b) follows the Markov chain $\overline{V}_O \to V_O \to W_{i_k}$ and (c) follows from Lemma 2, which implies $\Pr\{W_{i_k} = w_{i_k} \mid V_O = v_O\} = p^{-m}$ for any $w_{i_k} \in \mathrm{GF}(p^m)$, and Lemma 3. Since (81) holds for any v_O, we have (59). □

Since Claims 1–4 are satisfied as proved in the above, Theorem 5 holds. □

5. Reasonableness of the Proposed Construction

In this section, we explain the reasonableness of the proposed construction. Specifically, we explain why we must use strong (k, L, n) ramp SSSs, not weak ones, for $(W_1, \dots, W_n)$, and why we use the function $\sum_{j=1}^{L}(S_j)^{j+1}$, not $\sum_{j=1}^{L}(S_j)^2$, for $(U_1, \dots, U_n)$, in order to detect cheating.

First note that our scheme makes good use of the fact that $(W_1, \dots, W_n)$ are the shares of a strong (k, L, n) ramp SSS, which implies that no information of any S_i in $(S_1, \dots, S_L)$ leaks out even from any $k-1$ shares, i.e.,

$$c_{kq} \neq 0, \quad q = 1, \dots, L. \tag{83}$$

In the following, we give an example to show that if $(W_1, \dots, W_n)$ are defined so that (83) is not satisfied, then the scheme cannot always detect cheating. More clearly, if A in (42) is from a weak ramp SSS, instead of a strong ramp SSS, where some symbols leak out explicitly when the number of shares is less than k, (59) does not always hold.

Example 1: Set the parameters as $(k, L, n) = (3, 2, 3)$, $p = 5$, and $m = l = 1$. Denote $\mathrm{GF}(5) = \{0, 1, 2, 3, 4\}$. Define A in (42) and B in (43) as

$$A = \begin{bmatrix} 3 & 3 & 0 \\ 0 & 0 & 1 \\ 2 & 3 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 0 & 0 \\ 4 & 1 & 0 \\ 4 & 0 & 1 \end{bmatrix}. \tag{84}$$

Note that A is a generator matrix of a weak ramp SSS and the legitimate shares satisfy $S_1 = W_1 + W_2$, $S_2 = W_1 - W_2 + W_3$. Furthermore, we have from (43) that $S_1^2 + S_2^3 = U_1 + U_2 + U_3$. Accordingly, for the input $(\widehat{W}_1, \widehat{U}_1)$, $(\widehat{W}_2, \widehat{U}_2)$, and $(\widehat{W}_3, \widehat{U}_3)$, the decoder checks whether it holds that

$$(\widehat{W}_1 + \widehat{W}_2)^2 + (\widehat{W}_1 - \widehat{W}_2 + \widehat{W}_3)^3 = \widehat{U}_1 + \widehat{U}_2 + \widehat{U}_3. \tag{85}$$

For this scheme, a cheater can succeed in a substitution attack by forging (W_1, U_1) and (W_2, U_2) as $\overline{W}_1 = W_1 + \alpha$, $\overline{U}_1 = U_1 + (W_1 + W_2 + 2\alpha)^2 - (W_1 + W_2)^2$, $\overline{W}_2 = W_2 + \alpha$, and $\overline{U}_2 = U_2$, where $\alpha \neq 0$. Indeed, it holds that $(\overline{W}_1 + \overline{W}_2)^2 + (\overline{W}_1 - \overline{W}_2 + W_3)^3 = \overline{U}_1 + \overline{U}_2 + U_3$, which means that the attack is not detected, and $\widehat{S}_1 = \overline{W}_1 + \overline{W}_2 = S_1 + 2\alpha \neq S_1$ is decoded. Hence $P_{\mathrm{sub}(2)} = 1$ holds for this scheme.

Our scheme satisfies (59). If there exists a scheme which uses a function of $(S_1, \ldots, S_L)$ with a smaller degree instead of $\sum_{j=1}^{L} (S_j)^{j+1}$, then the scheme might achieve less $P_{\mathrm{sub}(a)}$ than (59). It is an open problem whether such a scheme exists or not. In the next example, we consider a scheme which defines $(U_1, \ldots, U_n)$ as the shares of $\sum_{j=1}^{L} (S_j)^2$ instead of $\sum_{j=1}^{L} (S_j)^{j+1}$. This scheme might seem natural, but it cannot always detect cheating as shown below.

Example 2: Set the parameters as $(k, L, n) = (3, 3, 3)$, $p = 5$, and $m = l = 1$. Denote $\mathrm{GF}(5) = \{0, 1, 2, 3, 4\}$. Define the shares $V_i = (W_i, U_i)$, $i = 1, 2, 3$, as

$$\begin{bmatrix} W_1 & W_2 & W_3 \end{bmatrix} = \begin{bmatrix} S_1 & S_2 & S_3 \end{bmatrix} A, \tag{86}$$

$$\begin{bmatrix} U_1 & U_2 & U_3 \end{bmatrix} = \begin{bmatrix} S_1^2 + S_2^2 + S_3^2 & R_1' & R_2' \end{bmatrix} B, \tag{87}$$

where A and B are defined by

$$A = \begin{bmatrix} 1 & 1 & 2 \\ 1 & 2 & 3 \\ 2 & 3 & 3 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 0 & 0 \\ 4 & 1 & 0 \\ 4 & 0 & 1 \end{bmatrix}. \tag{88}$$

We note that A is a generator matrix of a strong (k, L, n) ramp SSS. Then, the legitimate shares satisfy

$$S_1 = 4W_1 + W_2 + 3W_3, \tag{89}$$

$$S_2 = W_1 + 3W_2 + 3W_3, \tag{90}$$

$$S_3 = 3W_1 + 3W_2 + 2W_3, \tag{91}$$

$$S_1^2 + S_2^2 + S_3^2 = U_1 + U_2 + U_3. \tag{92}$$

Accordingly, for the input $(\widehat{W}_1, \widehat{U}_1)$, $(\widehat{W}_2, \widehat{U}_2)$, and $(\widehat{W}_3, \widehat{U}_3)$, the decoder checks whether it holds that

$$\begin{aligned}(4\widehat{W}_1 + \widehat{W}_2 + 3\widehat{W}_3)^2 + (\widehat{W}_1 + 3\widehat{W}_2 + 3\widehat{W}_3)^2 \\ + (3\widehat{W}_1 + 3\widehat{W}_2 + 2\widehat{W}_3)^2 = \widehat{U}_1 + \widehat{U}_2 + \widehat{U}_3.\end{aligned} \tag{93}$$

For this scheme, a cheater can succeed in a substitution attack by forging (W_1, U_1) and (W_2, U_2) as $\overline{W}_1 = W_1 + 2\alpha$, $\overline{W}_2 = W_2 + \alpha$, $\overline{U}_1 = U_1 + \alpha(W_1 + 2W_2) + \alpha^2$, $\overline{U}_2 = U_2$, where $\alpha \neq 0$. Indeed, it holds that

$$\begin{aligned}&(4\overline{W}_1 + \overline{W}_2 + 3W_3)^2 + (\overline{W}_1 + 3\overline{W}_2 + 3W_3)^2 \\ &\quad + (3\overline{W}_1 + 3\overline{W}_2 + 2W_3)^2 \\ &= (4W_1 + W_2 + 3W_3 + 4\alpha)^2 + (W_1 + 3W_2 + 3W_3)^2 \\ &\quad + (3W_1 + 3W_2 + 2W_3 + 4\alpha)^2 \\ &= (4W_1 + W_2 + 3W_3)^2 + (W_1 + 3W_2 + 3W_3)^2 \\ &\quad + (3W_1 + 3W_2 + 2W_3)^2 + \alpha(W_1 + 2W_2) + 2\alpha^2 \\ &= U_1 + U_2 + U_3 + \alpha(W_1 + 2W_2) + 2\alpha^2 \\ &= \overline{U}_1 + \overline{U}_2 + U_3.\end{aligned} \tag{94}$$

Hence, the attack is not detected, and $\widehat{S}_1 = 4\overline{W}_1 + \overline{W}_2 + 3W_3 = S_1 + 3\alpha \neq S_1$ is decoded. Therefore, $P_{\mathrm{sub}(2)} = 1$ holds for this scheme.

6. Conclusion

In this paper, we treated on cheating-detectable (k, L, n) ramp SSSs. In the converse part, we derived lower bounds on the sizes of the shares and random number used in encoding, and the success probabilities of impersonation attack and substitution attack for (k, L, n) ramp SSSs with given correlation level. We also derived a converse theorem in the form of lower bounds on the success probabilities of attacks for the given size of shares. In the direct part, we proposed a strong (k, L, n) ramp SSS which can detect substitution attacks. For any correlation level $(0, \ldots, 0, l)_p$, the proposed (k, L, n) ramp SSS attains the optimal sizes of the shares and random number. Furthermore, the proposed scheme can attain the success probabilities of substitution attacks and impersonation attacks as shown in Table 1. Finally, we explained the reasonableness of the proposed construction by showing examples of schemes similar to the proposed one but unable to detect substitution attacks.

Acknowledgment

The authors would like to thank the anonymous reviewers for their helpful comments.

References

[1] A. Shamir, "How to share a secret," Commun. ACM, vol.22, no.11, pp.612–613, Nov. 1979.
[2] G.R. Blakley, "Safeguarding cryptographic keys," Proc. National Computer Conference, vol.48, pp.313–317, 1979.

[3] G.R. Blakley and C. Meadows, "Security of ramp schemes," Proc. CRYPTO 1984, pp.242–268, Aug. 1984.
[4] H. Yamamoto, "Secret sharing system using (k, L, n) threshold scheme," IECE Trans., vol.J68-A, no.9, pp.945–952, Sept. 1985 (in Japanese). English Translation: Electronics and Communications in Japan, Part 1, vol.69, no.9, pp.46–54, Sept. 1986.
[5] M. Tompa and H. Woll, "How to share a secret with cheaters," J. Cryptology, vol.1, no.3, pp.133–138, Oct. 1989.
[6] W. Ogata, K. Kurosawa, and D.R. Stinson, "Optimum secret sharing scheme secure against cheating," SIAM J. Discrete Math., vol.20, no.1, pp.79–95, 2006.
[7] S. Cabello, C. Padró, and G. Sáez, "Secret sharing schemes with detection of cheaters for a general access structure," Designs, Codes and Cryptography, vol.25, no.2, pp.175–188, Feb. 2002.
[8] R. Cramer, Y. Dodis, S. Fehr, C. Padró, and D. Wichs, "Detection of algebraic manipulation with applications to robust secret sharing and fuzzy extractors," Proc. EUROCTYPT 2008, pp.471–488, April 2008.
[9] M. Iwamoto, H. Koga, and H. Yamamoto, "Coding theorems for a (2, 2)-threshold scheme with detectability of impersonation attacks," IEEE Trans. Inf. Theory, vol.58, no.9, pp.6194–6206, Sept. 2012.
[10] H. Koga and K. Koyano, "On the role of mutual information between the shares in a robust (k, n)-threshold scheme," Proc. 2012 International Symposium on Information Theory and Its Applications (ISITA), pp.260–264, Oct. 2012.
[11] T. Araki and W. Ogata, "A simple and efficient secret sharing scheme secure against cheating," IEICE Trans. Fundamentals, vol.E94-A, no.6, pp.1338–1345, June 2011.
[12] S. Obana and K. Tsuchida, "Cheating detectable secret sharing schemes supporting an arbitrary finite field," Proc. 9th International Workshop on Security (IWSEC), pp.88–97, Aug. 2014.
[13] W. Ogata, "On the practical secret sharing scheme," IEICE Trans. Fundamentals, vol.E84-A, no.1, pp.256–261, Jan. 2001.
[14] E.D. Karnin, J.W. Greene, and M.E. Hellman, "On secret sharing systems," IEEE Trans. Inf. Theory, vol.29, no.1, pp.35–41, Jan. 1983.
[15] W. Nakamura, H. Yamamoto, and T. Chan, "A ramp threshold secret sharing scheme against cheating by substitution attacks, "Proc. 2016 International Symposium on Information Theory and Its Applications (ISITA), pp.345–349, Oct. 2016.

Appendix: Surjective Linear Mapping

Lemma 4: For any surjective linear mapping $f : \mathrm{GF}(p^m) \to \mathrm{GF}(p^l)$, it holds that for any $y \in \mathrm{GF}(p^l)$,

$$|\{x \in \mathrm{GF}(p^m) : f(x) = y\}| = p^{m-l}. \qquad (\mathrm{A}\cdot 1)$$

Proof: For any $y \in \mathrm{GF}(p^l)$, choose $x_y \in \mathrm{GF}(p^m)$ satisfying $f(x_y) = y$ arbitrarily, and define $\mathcal{Z}_y := \{x \in \mathrm{GF}(p^m) : f(x) = y\}$. Then, (A·1) is derived from $|\mathcal{Z}_y| = |\operatorname{Ker} f| = p^{m-l}$, where the first equality follows from $\mathcal{Z}_y = \{x \in \mathrm{GF}(p^m) : f(x - x_y) = 0\} = \{x_y + x' : x' \in \operatorname{Ker} f\}$, and the second equality follows from $|\mathrm{GF}(p^m)|/|\operatorname{Ker} f| = |\mathrm{GF}(p^m)/\operatorname{Ker} f| = |\operatorname{Im} f| = |\mathrm{GF}(p^l)|$. □

Wataru Nakamura received the Bachelor's degree in engineering and the Master's degree in information science and technology in 2015 and 2017, respectively, from the University of Tokyo, Japan. He is now with Hitachi, Ltd.

Hirosuke Yamamoto was born in Wakayama, Japan, in 1952. He received the B.E. degree from Shizuoka University, Shizuoka, Japan, in 1975 and the M.E. and Ph.D. degrees from the University of Tokyo, Tokyo, Japan, in 1977 and 1980, respectively, all in electrical engineering. In 1980, he joined Tokushima University. He was an Associate Professor at Tokushima University from 1983 to 1987, the University of Electro-Communications from 1987 to 1993, and the University of Tokyo from 1993 to 1999. Since 1999, he has been a Professor at the University of Tokyo and is currently with the department of Complexity Science and Engineering at the university. In 1989–1990, he was a Visiting Scholar at the Information Systems Laboratory, Stanford University, Stanford, CA. His research interests are in Shannon theory, data compression algorithms, and information theoretic cryptology. Dr. Yamamoto served as the Chair of IEEE Information Theory Society Japan Chapter in 2002–2003, the TPC Co-Chair of the ISITA2004, the TPC Chair of the ISITA2008, the President of the SITA (Society of Information Theory and its Applications) in 2008–2009, the President of the ESS (Engineering Sciences Society) of IEICE in 2012–2013, an Auditor of the IEICE in 2016–2017, an Associate Editor for Shannon Theory, the IEEE Transactions on Information Theory in 2007–2010, and the Editor-in-Chief for the IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences in 2009–2011. He is a Fellow of the IEICE and the IEEE.

Terence Chan received his B.Sc (Math), Master's and Ph.D. degrees in Information Engineering in 1996, 1998 and 2000 respectively, all from The Chinese University of Hong Kong. In 2001, he was a visiting assistant professor in the Department of Information Engineering at the same university. From February 2002 to June 2004, he was a Post-doctoral Fellow at the Department of Electrical and Computer Engineering at the University of Toronto. He was an assistant professor in University of Regina from 2004–2006. He is currently an Associate Professor in Institute for Telecommunications Research at University of South Australia. He received the Croucher Foundation Fellowship in 2002 respectively. He respectively serves as the Technical and General Co-Chair for the 2011 and 2015 IEEE International Symposium On Network Coding.