Cheating Detectable Secret Sharing Schemes Supporting an Arbitrary Finite Field*

Satoshi Obana and Kazuya Tsuchida

Hosei University, Japan
obana@hosei.ac.jp

Abstract. In this paper, we present k-out-of-n threshold secret sharing scheme which can detect share forgery by at most $k-1$ cheaters. Though, efficient schemes with such a property are presented so far, some schemes cannot be applied when a secret is an element of $\mathbb{F}_{2^N}$ and some schemes require a secret to be an element of a multiplicative group. The schemes proposed in the paper possess such a merit that a secret can be an element of arbitrary finite field. Let $|\mathcal{S}|$ and ϵ be the size of secret and successful cheating probability of cheaters, respectively. Then the sizes of share $|\mathcal{V}_i|$ of two proposed schemes respectively satisfy $|\mathcal{V}_i| = (2 \cdot |\mathcal{S}|)/\epsilon$ and $|\mathcal{V}_i| = (4 \cdot |\mathcal{S}|)/\epsilon$ which are only 2 and 3 bits longer than the existing lower bound.

Keywords: Secret Sharing, Cheating Detection, Arbitrary Finite Field.

1 Introduction

Secret sharing scheme is a fundamental primitive in designing various cryptographic protocols in distributed environment. It enables us to securely manage a secret in a way that only a qualified set of users can recover the secret and no information about the secret is revealed to non-qualified set of users. Because of its importance, secret sharing have been studied actively so far since the seminal paper by Shamir [23] and Blakley [4].

Tompa and Woll have pointed out that in Shamir's k-out-of-n threshold secret sharing scheme is vulnerable to share forgery [24]. More precisely, they pointed out that even a single user can cheat other users with probability 1 by submitting forged shares in Shamir's threshold scheme. They also presented a scheme which can detect the fact of cheating when invalid shares are submitted. Since the paper by Tompa and Wall, cheating prevention has been one of the hottest issues in the study of secret sharing scheme, and various models (e.g., cheating detection [1–3, 5, 7, 8, 12, 16, 18, 19, 24], cheater identification [10, 11, 13–15, 20, 21, 25], robust secret sharing [9, 22], etc.) have been presented so far.

In this paper, we study secret sharing schemes capable of detecting cheating. More precisely, we study k-out-of-n threshold secret sharing scheme which can detect share forgery by at most $k-1$ cheaters. There are two different models for

* This work was supported by JSPS KAKENHI Grant Number 24800064.

M. Yoshida and K. Mouri (Eds.): IWSEC 2014, LNCS 8639, pp. 88–97, 2014.

secret sharing schemes capable of detecting such cheating. Carpentieri, De Santis and Vaccaro [7] first considered a model in which cheaters who *know* the secret try to make another user reconstruct an invalid secret. We call this model the *"CDV model."* In [19], Ogata, Kurosawa and Stinson introduced another model assuming weaker cheaters who *do not* know the secret in forging their shares. We call this model the *"OKS model."* As noted in [16], the merit of schemes secure in CDV model is that schemes are guaranteed to be secure regardless of the probability distribution of a secret to be shared. On the other hand, schemes secure in OKS model cannot guarantee security when the probability distribution of a secret is very much biased. However, once we can assume the probability distribution of a secret is not so much biased, schemes secure in OKS model possess a particular merit in that the size of share can be made smaller than schemes secure in CDV model. In fact, it is shown in [19] that when a secret is uniformly distributed, the lower bound of the size of share $|\mathcal{V}_i|$ is $(|\mathcal{S}|-1)/\epsilon^2+1$ in CDV model, whereas the lower bounds of the size of share in the OKS model is $(|\mathcal{S}|-1)/\epsilon+1$ where $|\mathcal{S}|$ and ϵ denote the size of the secret to be shared and the successful cheating probability of cheaters. Therefore, when we want to share a small size of secret, and we require a security level of $\epsilon \approx 1/|\mathcal{S}|$ (which is often the case when sharing a small size of secret), the lower bound of bit length of share in OKS model is about 33% shorter than the bound in CDV model.

The contribution of the paper is to present cheating detectable k-out-of-n threshold secret sharing schemes which are suitable for sharing a small size of secret (i.e., $\epsilon \approx 1/|\mathcal{S}|$) and are proven to be secure against $k-1$ cheaters in OKS model. The proposed schemes possess an extra merit in that they support an arbitrary finite field, that is, the proposed schemes guarantee security no matter what finite field a secret belongs to. We note that the proposed schemes are the first schemes which possesses such a property. Though efficient schemes suitable for sharing a small size of secret are presented so far [3, 8, 17, 19], some schemes cannot be applied when a secret is an element of $\mathbb{F}_{2^N}$ and some schemes require a secret to be an element of a multiplicative group or an element of a special type of a finite field or an additive group. Therefore, to show the existence of schemes supporting an arbitrary finite field is interesting from a theoretical point of view. Furthermore, when we employ secret sharing scheme as a building block of cryptographic protocols, supporting an arbitrary finite field will become a highly desired property. For example, consider a case in which we want to execute computation over an elliptic curve over $\mathbb{F}_{3^N}$ in a distributed manner using secure multi-party computation (MPC for short). In such the case, we must employ a secret sharing scheme supporting $\mathbb{F}_{3^N}$ since the algebraic structure must be preserved to enable MPC. Since today's cryptographic protocol often uses multiple algebraic structures (e.g., $\mathbb{F}_{2^N}, \mathbb{F}_{3^N}$, and $\mathbb{F}_p$) in a single protocol, a secret sharing scheme employed as a building block of such a protocol is desired to support as many mathematical structures as possible for easy implementation of the protocol, which motivate us to consider a cheating detectable secret sharing schemes supporting an arbitrary finite field.

The proposed schemes are not only capable of supporting an arbitrary finite field but also efficient with respect to sizes of shares. Let $|\mathcal{S}|$ and ϵ be the size of secret and successful cheating probability of cheaters, respectively. Then the sizes of share $|V_i|$ of two proposed schemes respectively satisfy $|\mathcal{V}_i| = (2 \cdot |\mathcal{S}|)/\epsilon$ and $|\mathcal{V}_i| = (4 \cdot |\mathcal{S}|)/\epsilon$ which are only 2 and 3 bits longer than the lower bound.

It should be noted that here we focus on the problem of detecting cheating by cheaters with unlimited computational power, and therefore, schemes based on computational assumptions (e.g., [20]) are not within the scope of this paper.

2 Preliminaries

2.1 Secret Sharing Schemes

In secret sharing schemes, there are n users $\mathcal{P} = \{P_1, \ldots, P_n\}$ and a dealer D. The set of users who are allowed to reconstruct the secret is characterized by an *access structure* $\Gamma \subseteq 2^{\mathcal{P}}$; that is, users $P_{i_1}, \ldots, P_{i_k}$ are allowed to reconstruct the secret if and only if $\{P_{i_1}, \ldots, P_{i_k}\} \in \Gamma$ (for instance, the access structure of a k-out-of-n threshold secret sharing scheme is defined by $\Gamma = \{\mathcal{A} \mid \mathcal{A} \in 2^{\mathcal{P}}, |\mathcal{A}| \geq k\}$.) A model consists of two algorithms: $\mathsf{ShareGen}$ and $\mathsf{Reconst}$. Share generation algorithm $\mathsf{ShareGen}$ takes a secret $s \in \mathcal{S}$ as input and outputs a list $(v_1, v_2, \ldots, v_n)$. Each $v_i \in \mathcal{V}_i$ is called a *share* and is given to a user P_i. In a usual setting, $\mathsf{ShareGen}$ is invoked by the dealer. Secret reconstruction algorithm $\mathsf{Reconst}$ takes a list of shares and outputs a secret $s \in \mathcal{S}$.

A secret sharing scheme is called *perfect* if the following two conditions are satisfied for the output $(v_1, \ldots, v_n)$ of $\mathsf{ShareGen}(\hat{s})$ where the probabilities are taken over the random tape of $\mathsf{ShareGen}$.

1. if $\{P_{i_1}, \ldots, P_{i_k}\} \in \Gamma$ then $\Pr[\mathsf{Reconst}(v_{i_1}, \ldots, v_{i_k}) = \hat{s}] = 1$,
2. if $\{P_{i_1}, \ldots, P_{i_k}\} \notin \Gamma$ then $\Pr[\mathcal{S} = s \mid \mathcal{V}_{i_1} = v_{i_1}, \ldots, \mathcal{V}_{i_k} = v_{i_k}] = \Pr[\mathcal{S} = s]$ for any $s \in \mathcal{S}$.

2.2 Secret Sharing Schemes Secure against Cheating

A secret sharing schemes capable of detecting cheating was first presented by Tompa and Woll [24]. They considered the scenario in which cheaters who do not belong to the access structure submit forged shares in the secret reconstruction phase. Such cheaters will succeed if another users in the reconstruction accepts an incorrect secret.

As in ordinary secret sharing schemes, this model consists of two algorithms. A share generation algorithm $\mathsf{ShareGen}$ is the same as that in the ordinary secret sharing schemes. A secret reconstruction algorithm $\mathsf{Reconst}$ is slightly changed: it takes a list of shares as input and outputs either a secret or the special symbol $\perp$ ($\perp \notin \mathcal{S}$.) $\mathsf{Reconst}$ outputs $\perp$ if and only if cheating has been detected. To formalize the models, we define the following simple game for any (k, n) threshold secret sharing scheme $\mathbf{SS} = (\mathsf{ShareGen}, \mathsf{Reconst})$ and for any (not necessarily polynomially bounded) Turing machine $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$, where $\mathcal{A}$ represents cheaters

$P_{i_1}, \ldots, P_{i_{k-1}}$ who try to cheat P_{i_k}. Please note that we will focus on the (k, n) threshold type access structure throughout the paper.

$\mathsf{Game}(\mathbf{SS}, \mathcal{A})$
$s \leftarrow \mathcal{S}$; // according to the probability distribution over $\mathcal{S}$.
$(v_1, \ldots, v_n) \leftarrow \mathsf{ShareGen}(s)$;
$(i_1, \ldots, i_{k-1}) \leftarrow \mathcal{A}_1(X)$;
// set $X = s$ for the CDV model, $X = \emptyset$ for the OKS model.
$(v'_{i_1}, \ldots, v'_{i_{k-1}}, i_k) \leftarrow \mathcal{A}_2(v_{i_1}, \ldots, v_{i_{k-1}}, X)$;

The advantage of cheaters is expressed as $Adv(\mathbf{SS}, \mathcal{A}) = \Pr[s' \in \mathcal{S} \wedge s' \neq s]$, where $s' = \mathsf{Reconst}(v'_{i_1}, v'_{i_2}, \ldots, v'_{i_{k-1}}, v_{i_k})$ and the probability is taken over the distribution of $\mathcal{S}$, and over the random tapes of $\mathsf{ShareGen}$ and $\mathcal{A}$.

Definition 1. *A (k, n) threshold secret sharing scheme* **SS** *is called a (k, n, ϵ)-*secure secret sharing scheme *if $Adv(\mathbf{SS}, \mathcal{A}) \leq \epsilon$ for any cheater $\mathcal{A}$.*

2.3 Previous Work

In this subsection, we briefly review the known bounds and constructions of (k, n, ϵ)-secure secret sharing schemes. A lower bound for the size of shares in the CDV model is described as follows:

Proposition 1. ***[7]*** *In the CDV model, the size of shares for $(k, n, \epsilon_{\mathsf{CDV}})$-secure secret sharing schemes is lower bounded by $|\mathcal{V}_i| \geq \frac{|\mathcal{S}|}{\epsilon_{\mathsf{CDV}}}$.*

Ogata *et al.* improved this bound when the secret is uniformly distributed:

Proposition 2. ***[19]*** *In the CDV model, if the secret is uniformly distributed, then the size of shares $|\mathcal{V}_i|$ for $(k, n, \epsilon_{\mathsf{CDV}})$-secure secret sharing schemes is lower bounded by $|\mathcal{V}_i| \geq \frac{|\mathcal{S}|-1}{\epsilon^2_{\mathsf{CDV}}} + 1$.*

Ogata *et al.* also presented the lower bound for the size of shares for $(k, n, \epsilon_{\mathsf{OKS}})$-secure secret sharing scheme in the OKS model as follows.

Proposition 3. ***[19]*** *In the OKS model, the size of shares for $(k, n, \epsilon_{\mathsf{OKS}})$-secure secret sharing schemes is lower bounded by $|\mathcal{V}_i| \geq \frac{|\mathcal{S}|-1}{\epsilon_{\mathsf{OKS}}} + 1$.*

Ogata *et al.* presented an optimum $(k, n, \epsilon_{\mathsf{OKS}})$-secure secret sharing schemes that satisfies the bound of Proposition 3 with equality [19].

Proposition 4. ***[19]*** *There exists a $(k, n, \epsilon_{\mathsf{OKS}})$-secure secret sharing scheme in the OKS model such that $|\mathcal{V}_i| = \frac{|\mathcal{S}|-1}{\epsilon_{\mathsf{OKS}}} + 1$. The scheme is $(k, n, \epsilon_{\mathsf{OKS}})$-secure if the secret is uniformly distributed.*

Though the scheme is optimum with respect to size of share, the scheme possesses such a drawback that the parameter of the size of secret is very much limited. Namely, if we require $\epsilon \approx 1/|\mathcal{S}|$ the size of the secret $|\mathcal{S}|$ must satisfy $|\mathcal{S}| = q + 1$ where $q^2 + q + 1$ is a prime power.

Cabello, Padró and Sáez presented nearly optimum $(k, n, \epsilon_{\mathsf{OKS}})$-secure secret sharing scheme in the OKS model [8].

Proposition 5. *[8] There exists a $(k, n, \epsilon_{\mathsf{OKS}})$-secure secret sharing scheme in the OKS model such that $|\mathcal{S}| = p, |\mathcal{V}_i| = |\mathcal{S}|/\epsilon_{\mathsf{OKS}}$ and $\epsilon_{\mathsf{OKS}} = 1/p$.*

In the scheme presented in [8], a secret can be almost an arbitrary element of finite field. Though, unfortunately, the scheme does not guarantee security when a secret is an element of $\mathbb{F}_{2^N}$. More precisely, $\epsilon_{\mathsf{OKS}} = 1$ holds when we apply the scheme to a secret s such that $s \in \mathbb{F}_{2^N}$.

Araki and Ogata presented a $(k, n, \epsilon_{\mathsf{OKS}})$ schemes in the OKS model which are also nearly optimum with respect to the size of secret [3].

Proposition 6. *[3] There exists a $(k, n, \epsilon_{\mathsf{OKS}})$-secure secret sharing scheme in the OKS model such that $|\mathcal{S}| = (p-1)^N, |\mathcal{V}_i| \approx |\mathcal{S}|/\epsilon_{\mathsf{OKS}}$ and $\epsilon_{\mathsf{OKS}} = 1/(p-1)$.*

Though the scheme possesses many desired properties, a secret s must be an element of $\mathbb{Z}_p^*$ and, therefore, does not support $\mathbb{F}_{2^N}$ which is suited for dealing with digital data in current computers.

Araki and Ogata also presented a $(k, n, \epsilon_{\mathsf{OKS}})$ scheme in which a secret can be an element of an arbitrary finite field.

Proposition 7. *[3] There exists a $(k, n, \epsilon_{\mathsf{OKS}})$-secure secret sharing scheme in the OKS model such that $|\mathcal{S}| = p^N, |\mathcal{V}_i| = p^{N+2}$ and $\epsilon_{\mathsf{OKS}} = (N+1)/p$.*

Though the scheme supports an arbitrary finite field, the successful cheating probability ϵ_{OKS} must satisfy $\epsilon \geq 1/\sqrt{|\mathcal{S}|}$, which is suitable for sharing a large secret, but not necessarily suitable for sharing a small size of secret.

To summarize the previous work on secret sharing schemes capable of detecting cheating, we realize that there is no existing scheme which satisfy all the following requirements:

- The secret can be an element of an arbitrary finite field, that is, the scheme is secure no matter what finite field the secret belongs to.
- The scheme provide adequate level of security even if the size of secret is relatively small. More precisely, the scheme supports ϵ such that $\epsilon \approx 1/|\mathcal{S}|$.
- The size of share is small. It is desired that $|\mathcal{V}_i| \approx |\mathcal{S}|/\epsilon$ (i.e., nearly optimum with respect to the bound presented in Proposition 3.)

3 Proposed Schemes

In this section, we propose two efficient $(k, n, \epsilon_{\mathsf{OKS}})$-secure secret sharing schemes in the OKS model which are proven to be secure when a secret is uniformly distributed. The proposed schemes possess such a merit that a secret to be shared can be an element of an arbitrary finite field, which is not the case in most existing schemes.

The basic idea behind both constructions is to share a secret s and its check digit $A(s)$ using Shamir's k-out-of-n secret sharing scheme where both s and $A(s)$ are elements of the same finite field $\mathbb{F}$. In the proposed schemes, verification functions $A : \mathbb{F} \to \mathbb{F}$ are carefully chosen so that the successful cheating probability is small for any finite field $\mathbb{F}$. The sizes of share $|\mathcal{V}_i|$ in the proposed schemes satisfy $|\mathcal{V}_i| = (2 \cdot |\mathcal{S}|)/\epsilon_{\mathsf{OKS}}$ and $|\mathcal{V}_i| = (4 \cdot |\mathcal{S}|)/\epsilon_{\mathsf{OKS}}$, which are only two and three bits longer than the lower bound given in Proposition 3, respectively.

3.1 Scheme with a Check Digit Based on Polynomial

In the first scheme, the verification function $A : \mathbb{F} \to \mathbb{F}$ is defined by $A(s) = s^2 + s^3$. We should note that a verification function $A'(s) = s^2$ used in [8] does not guarantee security when a secret is an element of $\mathbb{F}_{2^N}$, and a verification function $A''(s) = s^3$ does not guarantee security when a secret is an element of $\mathbb{F}_{3^N}$. Nevertheless, when we use $A(s) = A'(s) + A''(s)$ as a verification function, the security of the scheme is proven for any finite field $\mathbb{F}$. The share generation algorithm ShareGen and the share reconstruction algorithm Reconst of the first scheme is described as follows where p is an arbitrary prime power.

Share Generation: On input a secret $s \in \mathbb{F}_p$, the share generation algorithm ShareGen outputs a list of shares $(v_1, \ldots, v_n)$ as follows:

1. Generate a random polynomials $f_s(x) \in \mathbb{F}_p[X]$ and $f_a(x) \in \mathbb{F}_p[X]$ of degree at most $k-1$ such that $f_s(0) = s$ and $f_a(0) = s^2 + s^3$.
2. Compute $v_i = (f_s(i), f_a(i))$ and output $(v_1, \ldots, v_n)$.

Secret Reconstruction and Validity Check: On input a list of m shares $(v_{i_1}, \ldots, v_{i_m})$ (where $m \geq k$), the secret reconstruction algorithm Reconst outputs a secret s or $\perp$ as follows:

1. Reconstruct $\hat{f}_s(x)$ and $\hat{f}_a(x)$ from $v_{i_1}, \ldots, v_{i_m}$ using Lagrange interpolation.
2. If $\deg(\hat{f}_s) > k-1$ or $\deg(\hat{f}_a) > k-1$ holds, output $\perp$.
3. Compute $\hat{s} = \hat{f}_s(0)$ and $\hat{a} = \hat{f}_a(0)$.
4. Output $\hat{s}$ if $\hat{a} = \hat{s}^2 + \hat{s}^3$ holds. Otherwise Reconst outputs $\perp$.

The properties of the first scheme is summarized by the following theorem.

Theorem 1. *The above scheme is (k, n, ϵ)-secure secret sharing schemes in the OKS model with parameters $|\mathcal{S}| = p$ and $|\mathcal{V}_i| = p^2$ $(= (2 \cdot |\mathcal{S}|)/\epsilon)$. When the secret is uniformly distributed over $\mathbb{F}_p$, the successful cheating probability $\epsilon = Adv(\mathbf{SS}, \mathcal{A})$ of any cheater $\mathcal{A}$ satisfies $\epsilon = 1/p$ if $p = 3^N$, or $\epsilon = 2/p$ otherwise.*

The size of shares in the first scheme is only two bits longer than the lower bound of Proposition 3 since $\frac{2|\mathcal{S}|}{\epsilon} < 4(\frac{|\mathcal{S}|-1}{\epsilon} + 1)$ holds when $|\mathcal{S}| > 2$.

Proof. We consider the worst case where just k users take part in secret reconstruction. This case is the worst since $\deg(\hat{f}_s) < k$ and $\deg(\hat{f}_a) < k$ hold with probability 1 in this case. Without loss of generality, we can assume users $P_1, \ldots, P_{k-1}$ are cheaters who try to cheat user P_k. Now, consider such a situation that cheater P_i $(1 \leq i \leq k-1)$ submits a (possibly forged) share $v'_i = (v_{s,i} + \delta_{s,i}, v_{a,i} + \delta_{a,i})$ and P_1 submits a unforged share $v_k = (v_{s,k}, v_{a,k})$ to Reconst. Since $\hat{s}$ and $\hat{a}$ is computed using Lagrange interpolation, the value of $\hat{s}$ is described as follows where s is an original secret:

$$\begin{aligned}\hat{s} &= \left(\sum_{i=1}^{k-1} \prod_{j=1, j\neq i}^{k} \frac{-j}{i-j}(v_{s,i} + \delta_{s,i})\right) + \prod_{j=1}^{k-1} \frac{-j}{k-j} v_{s,k} \\ &= \left(\sum_{i=1}^{k} \prod_{j=1, j\neq i}^{k} \frac{-j}{i-j} v_{s,i}\right) + \left(\sum_{i=1}^{k-1} \prod_{j=1, j\neq i}^{k} \frac{-j}{i-j} \delta_{s,i}\right) \;=\; s + \delta_s\end{aligned}$$

Here, $\delta_s = \sum_{i=1}^{k-1}(\prod_{j=1,j\neq i}^{k} \frac{-j}{i-j}\delta_{s,i})$ is not only known to cheaters but also arbitrarily controlled by cheaters by choosing $\delta_{s,i}$ $(1 \leq i \leq k-1)$ appropriately. With the same discussion, $\hat{a}$ is also denoted as $\hat{a} = s^2 + s^3 + \delta_a$ where δ_a is known to and arbitrarily controlled by cheaters. Now we will evaluate the successful cheating probability ϵ of cheaters $P_1, \ldots, P_{k-1}$. From the definition of Reconst, it is clear that cheaters succeed in cheating if $\hat{a} = \hat{s}^2 + \hat{s}^3$ holds. Since $\hat{s} = s + \delta_s$ and $\hat{a} = s^2 + s^3 + \delta_a$ hold, this equation is equivalent to the following equation where $\delta_s \neq 0$:

$$3\delta_s s^2 + (3\delta_s^2 + 2\delta_s)s + \delta_s^2 + \delta_s^3 - \delta_a = 0\,. \tag{1}$$

Therefore, cheaters succeeds in cheating if the original secret s is a root of eq. (1). Since $\delta_s \neq 0$, it is easy to see that the coefficient of s^2 of eq. (1) (i.e., $3\delta_s$) cannot be zero if the order p of the finite field satisfy $p \neq 3^N$. Therefore, there are at most two roots for eq. (1) and the successful cheating probability ϵ satisfies $\epsilon = 2/p$ when the secret is uniformly distributed over $\mathbb{F}_p$. Now we consider the case where $p = 3^N$ holds. In this case, eq. (1) is equivalent to $2\delta_s s + \delta_s^2 + \delta_s^3 - \delta_a = 0$ since $3 = 0$ holds in $\mathbb{F}_{3^N}$. It is obvious that the number of roots of the above equation becomes one. Therefore $\epsilon = 1/p$ holds when $p = 3^N$. □

3.2 A Scheme with a Check Digit Based on Multiplicative Inverse

The first scheme can be viewed as a patch to the scheme presented in [8] so that the resulting scheme can be secure even when the secret is an element of $\mathbb{F}_{2^N}$. In this subsection, we show how to construct a scheme supporting an arbitrary finite field in more direct manner. Namely, in the second scheme, we use multiplicative inverse as a verification function. We choose $A(s) = s^{-1}$ as a verification function because a verification function A must be a non-linear function, and multiplicative inverse is one of the most fundamental non-linear functions in finite field. Moreover, unlike s^2 and s^3, s^{-1} does not reflects a characteristics of underlying finite field when s is manipulated to $s+\delta_s$. However, multiplicative inverse s^{-1} cannot be directly used as a check digit for $s \in \mathbb{F}$ since multiplicative inverse cannot be defined when $s = 0$ holds. Therefore, we define $A(0) = 1$ (multiplicative identity of $\mathbb{F}$) as an exception so that $A : \mathbb{F} \to \mathbb{F}$ is defined for any finite field $\mathbb{F}$ and for any input $s \in \mathbb{F}$. The complete description of the second scheme is described as follows where p is an arbitrary prime power.

Share Generation: On input a secret $s \in \mathbb{F}_p$, the share generation algorithm ShareGen outputs a list of shares $(v_1, \ldots, v_n)$ as follows:

1. Generate a random polynomials $f_s(x) \in \mathbb{F}_p[X]$ and $f_a(x) \in \mathbb{F}_p[X]$ of degree at most $k-1$ such that $f_s(0) = s$ $f_a(0) = A(s)$ where $A(s)$ is defined as follows:
$$A(s) = \begin{cases} s^{-1} & (\text{if } s \neq 0) \\ 1 & (\text{if } s = 0) \end{cases}$$
2. Compute $v_i = (f_s(i), f_a(i))$ and output $(v_1, \ldots, v_n)$.

Secret Reconstruction and Validity Check: On input a list of m shares $(v_{i_1}, \ldots, v_{i_m})$, the secret reconstruction algorithm Reconst outputs a secret s or $\perp$ as follows:

1. Reconstruct $\hat{f}_s(x)$ and $\hat{f}_a(x)$ from $v_{i_1}, \ldots, v_{i_m}$ using Lagrange interpolation.
2. If $\deg(\hat{f}_s) > k-1$ or $\deg(\hat{f}_a) > k-1$ holds, output $\perp$.
3. Output $\hat{s}$ if $\hat{a} = A(\hat{s})$ holds, or Reconst outputs $\perp$ otherwise.

The properties of the first scheme is summarized by the following theorem.

Theorem 2. *The above scheme is (k, n, ϵ)-secure secret sharing schemes in the OKS model with parameters $|\mathcal{S}| = p$ and $|\mathcal{V}_i| = p^2$ $(= (4 \cdot |\mathcal{S}|)/\epsilon)$. When the secret is uniformly distributed over $\mathbb{F}_p$, the successful cheating probability $\epsilon = Adv(\mathbf{SS}, \mathcal{A})$ of any cheater $\mathcal{A}$ satisfies $\epsilon = 4/p$ if $p = 2^N$, or $\epsilon = 3/p$ otherwise.*

The size of shares in the second scheme is only three bits longer than the lower bound of Proposition 3 since $\frac{4|\mathcal{S}|}{\epsilon} < 8(\frac{|\mathcal{S}|-1}{\epsilon} + 1)$ holds when $|\mathcal{S}| > 2$.

Proof. As in the proof of Theorem 1, we consider the worst case where just k users take part in secret reconstruction and assume users $P_1, \ldots, P_{k-1}$ are cheaters who try to cheat user P_k. Now, consider such a situation that cheater P_i $(1 \leq i \leq k-1)$ submits a (possibly forged) share $v_i' = (v_{s,i} + \delta_{s,i}, v_{a,i} + \delta_{a,i})$ and P_1 submits a unforged share $v_k = (v_{s,k}, v_{a,k})$ to Reconst. As the same discussion done in proving Theorem 1, $\hat{s}$ and $\hat{a}$ reconstructed from submitted shares can be written by $\hat{s} = s + \delta_s$ and $\hat{a} = A(s) + \delta_a$, respectively, where s is an original secret, and $\delta_s \neq 0$ and δ_a are known to and arbitrarily controlled by cheaters.

Now we will evaluate the successful cheating probability ϵ of cheaters $P_1, \ldots, P_{k-1}$. From the definition of Reconst, it is clear that cheaters succeed in cheating if $A(s) + \delta_a = A(s + \delta_s)$ holds. There are the following three cases to consider, and we will clarify a condition on s, δ_s and δ_a such that cheaters succeed in cheating cheating if the condition is satisfied for each case.

Case 1 ($s = 0$ and $s + \delta_s \neq 0$): In this case, $A(s) = 1$, $\hat{s} = \delta_s$ and $\hat{a} = A(s) + \delta_a = 1 + \delta_a$ hold. Therefore, cheaters succeeds in cheating if $1 + \delta_a = \delta_s^{-1}$ (or equivalently, $\delta_a = \delta_s^{-1} - 1$) holds.

Case 2 ($s \neq 0$ and $s + \delta_s = 0$): In this case, $A(s) = s^{-1}$, $\hat{s} = s + \delta_s = 0$ and $\hat{a} = A(s) + \delta_a = s^{-1} + \delta_a$ hold. Therefore, cheaters succeeds in cheating if $s^{-1} + \delta_a = 1$ (or equivalently, $\delta_a = \delta_s^{-1} + 1$) holds.

Case 3 ($s \neq 0$ and $s + \delta_s \neq 0$): In this case, $A(s) = s^{-1}$, $\hat{s} = s + \delta_s$ and $\hat{a} = A(s) + \delta_a = s^{-1} + \delta_a$ hold. Therefore, cheaters succeeds in cheating if $s^{-1} + \delta_a = (s + \delta_s)^{-1}$ (or equivalently, $(s^{-1} + \delta_a)(s + \delta_s) = 1$) holds.

Therefore, the best strategy for cheaters is to choose δ_s and δ_a such that $\delta_a = \delta_s^{-1} - 1$ or $\delta_a = \delta_s^{-1} + 1$ holds. We will evaluate the successful cheating probability ϵ in such cases. Now suppose $p \neq 2^N$, and cheaters control $\hat{s} = s + \delta_s$ and $\hat{a} = A(s) + \delta_a$ so that they satisfy $\delta_a = \delta_s^{-1} + 1$. In this case, cheaters succeed in cheating if $s = 0$ holds or the secret s is a root of equation $(s^{-1} + \delta_a)(s + \delta_s) = 1$, which is equivalent to the following equation:

$$\delta_a s^2 + \delta_a \delta_s s + \delta_s = 0 \tag{2}$$

It is obvious that there are at most two roots which satisfy above equation. Therefore, the successful cheating probability ϵ satisfies $\epsilon = 3/p$ since there are at most three values of s with which cheaters succeeds in cheating. It is easy to see that $\epsilon = 3/p$ holds when cheaters control $\hat{s} = s + \delta_s$ and $\hat{a} = A(s) + \delta_a$ so that they satisfy $\delta_a = \delta_s^{-1} - 1$.

Now suppose $p = 2^N$. In this case $\delta_s^{-1} + 1 = \delta_s^{-1} - 1$ holds since $1 = -1$ holds in $\mathbb{F}_{2^N}$. Therefore, cheaters who control $\hat{s} = s + \delta_s$ and $\hat{a} = A(s) + \delta_a$ so that they satisfy $\delta_a = \delta_s^{-1} + 1$ succeeds in cheating with probability $4/p$ since cheater succeeds in cheating if $s = 0$ or $s + \delta_s = 0$ holds or s is a root of eq. (2). □

4 Concluding Remarks

In this paper, we present k-out-of-n threshold secret sharing schemes which can detect share forgery by at most $k-1$ cheaters. The schemes proposed in the paper possess such a merit that a secret can be an element of arbitrary finite field. Let $|\mathcal{S}|$ and ϵ be the size of secret and successful cheating probability of cheaters, respectively. Then the sizes of share $|V_i|$ of two proposed schemes respectively satisfy $|\mathcal{V}_i| = (2 \cdot |\mathcal{S}|)/\epsilon$ and $|\mathcal{V}_i| = (4 \cdot |\mathcal{S}|)/\epsilon$ which are only 2 and 3 bits longer than the lower bound. It is easy to see that the verification function used in the proposed schemes can be apply to any linear secret sharing schemes to make them secure against share forgery by non-qualified set of users.

To construct a scheme supporting an arbitrary finite field and the size of share is smaller than the proposed schemes is our future challenge.

References

1. Araki, T.: Efficient (*k*,*n*) Threshold Secret Sharing Schemes Secure Against Cheating from $n - 1$ Cheaters. In: Pieprzyk, J., Ghodosi, H., Dawson, E. (eds.) ACISP 2007. LNCS, vol. 4586, pp. 133–142. Springer, Heidelberg (2007)
2. Araki, T., Obana, S.: Flaws in Some Secret Sharing Schemes Against Cheating. In: Pieprzyk, J., Ghodosi, H., Dawson, E. (eds.) ACISP 2007. LNCS, vol. 4586, pp. 122–132. Springer, Heidelberg (2007)
3. Araki, T., Ogata, W.: A Simple and Efficient Secret Sharing Scheme Secure against Cheating. IEICE Trans. Fundamentals E94-A(6), 1338–1345 (2011)
4. Blakley, G.R.: Safeguarding cryptographic keys. In: Proc. AFIPS 1979, National Computer Conference, vol. 48, pp. 313–317 (1979)
5. Brickell, E.F., Stinson, D.R.: The Detection of Cheaters in Threshold Schemes. SIAM Journal on Discrete Mathematics 4(4), 502–510 (1991)
6. Carpentieri, M.: A Perfect Threshold Secret Sharing Scheme to Identify Cheaters. Designs, Codes and Cryptography 5(3), 183–187 (1995)
7. Carpentieri, M., De Santis, A., Vaccaro, U.: Size of Shares and Probability of Cheating in Threshold Schemes. In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 118–125. Springer, Heidelberg (1994)
8. Cabello, S., Padró, C., Sáez, G.: Secret Sharing Schemes with Detection of Cheaters for a General Access Structure. Designs, Codes and Cryptography 25(2), 175–188 (2002)

9. Cevallos, A., Fehr, S., Ostrovsky, R., Rabani, Y.: Unconditionally-secure Robust Secret Sharing with Compact Shares. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 195–208. Springer, Heidelberg (2012)
10. Choudhury, A.: Brief announcement: Optimal Amortized Secret Sharing with Cheater Identification. In: Proc. PODC 2012, p. 101. ACM (2012)
11. Cramer, R., Damgård, I.B., Fehr, S.: On the Cost of Reconstructing a Secret, or VSS with Optimal Reconstruction Phase. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 503–523. Springer, Heidelberg (2001)
12. Cramer, R., Dodis, Y., Fehr, S., Padró, C., Wichs, D.: Detection of Algebraic Manipulation with Applications to Robust Secret Sharing and Fuzzy Extractors. In: Smart, N.P. (ed.) EUROCRYPT 2008. LNCS, vol. 4965, pp. 471–488. Springer, Heidelberg (2008)
13. Kurosawa, K., Obana, S., Ogata, W.: t-Cheater Identifiable (k, n) Threshold Secret Sharing Schemes. In: Coppersmith, D. (ed.) CRYPTO 1995. LNCS, vol. 963, pp. 410–423. Springer, Heidelberg (1995)
14. McEliece, R.J., Sarwate, D.V.: On Sharing Secrets and Reed-Solomon Codes. Communications of the ACM 24(9), 583–584 (1981)
15. Obana, S.: Almost Optimum t-Cheater Identifiable Secret Sharing Schemes. In: Paterson, K.G. (ed.) EUROCRYPT 2011. LNCS, vol. 6632, pp. 284–302. Springer, Heidelberg (2011)
16. Obana, S., Araki, T.: Almost Optimum Secret Sharing Schemes Secure Against Cheating for Arbitrary Secret Distribution. In: Lai, X., Chen, K. (eds.) ASIACRYPT 2006. LNCS, vol. 4284, pp. 364–379. Springer, Heidelberg (2006)
17. Ogata, W., Araki, T.: Cheating Detectable Secret Sharing Schemes for Random Bit String. IEICE Trans. Fundamentals E96-A(11), 2230–2234 (2013)
18. Ogata, W., Eguchi, H.: Cheating Detectable Threshold Scheme against Most Powerful Cheaters for Long Secrets. Designs, Codes and Cryptography (published online, October 2012)
19. Ogata, W., Kurosawa, K., Stinson, D.R.: Optimum Secret Sharing Scheme Secure against Cheating. SIAM Journal on Discrete Mathematics 20(1), 79–95 (2006)
20. Pedersen, T.P.: Non-interactive and Information-Theoretic Secure Verifiable Secret Sharing. In: Feigenbaum, J. (ed.) CRYPTO 1991. LNCS, vol. 576, pp. 129–140. Springer, Heidelberg (1992)
21. Rabin, T., Ben-Or, M.: Verifiable Secret Sharing and Multiparty Protocols with Honest Majority. In: Proc. STOC 1989, pp. 73–85 (1989)
22. Rabin, T.: Robust Sharing of Secrets When the Dealer is Honest or Cheating. Journal of the ACM 41(6), 1089–1109 (1994)
23. Shamir, A.: How to Share a Secret. Communications of the ACM 22(11), 612–613 (1979)
24. Tompa, M., Woll, H.: How to Share a Secret with Cheaters. Journal of Cryptology 1(3), 133–138 (1989)
25. Xu, R., Morozov, K., Takagi, T.: On Cheater Identifiable Secret Sharing Schemes Secure against Rushing Adversary. In: Sakiyama, K., Terada, M. (eds.) IWSEC 2013. LNCS, vol. 8231, pp. 258–271. Springer, Heidelberg (2013)