Almost Optimum Secret Sharing with Cheating Detection

Mahabir Prasad Jhanwar[1,⋆] and Reihaneh Safavi-Naini[2,⋆⋆]

[1] CR Rao AIMSCS, UoH Campus, India
[2] Department of Computer Science, University of Calgary, Canada

Abstract. A (t, n, δ) secret sharing scheme with cheating detection property (SSCD) is a t-out-of-n threshold secret sharing scheme that has the following additional property; *the probability that any t malicious players can successfully cheat (without being caught) an honest player by opening forged shares and causing the honest player to reconstruct the wrong secret is at most δ*. There are two flavors of security for such schemes known as OKS and CDV. The lower bound on share sizes for an OKS-secure SSCD scheme is known, and concrete schemes in which share sizes are equal to (or almost the same as) the lower bound have been proposed, albeit with some *limitations*. We first present a OKS-secure scheme with share sizes only *one bit longer* than its existing lower bound. Our construction is free from any special requirements. We next present a CDV-secure SSCD scheme, where a stronger form of cheating is allowed. The share size of our CDV-secure scheme is also one bit longer than the existing lower bound.

1 Introduction

Secret sharing is one of the most important primitives in cryptography and in particular distributed systems. Let t, n be positive integers such that $1 \leq t < n$. In a *perfect* t-out-of-n secret sharing scheme [20,2], a dealer $\mathcal{D}$ distributes a secret s to n players, say $P_1, \ldots, P_n$ in such a way that the combined shares of any $t+1$ or more players can recover the secret s, but no subset of t or less shares can leak any information about the secret s, where the leakage is in information theoretic sense, and without assuming any limit on the computational resources of the adversary. An important efficiency parameter in secret sharing scheme is the size of shares. Let Σ_i be the set of possible shares for P_i, and Σ be the set of possible secrets. It is well known that, for t-out-of-n perfect secret sharing schemes, $|\Sigma_i| \geq |\Sigma|$ [12]. Schemes with $|\Sigma_i| = |\Sigma|$ are called *ideal*. Shamir [20] constructed an ideal (t, n)-threshold secret sharing scheme in which secrets and shares lie in a finite field $\mathbb{F}_q$, where $q > n$, and share generation uses

⋆ A major portion of the work was done when the author was a postdoctoral fellow at the Univeristy of Calgary.

⋆⋆ Financial support for this research was provided in part by Alberta Innovates - Technology Futures, in the Province of Alberta in Canada.

R.S. Chakraborty et al. (Eds.): SPACE 2015, LNCS 9354, pp. 359–372, 2015.
DOI: 10.1007/978-3-319-24126-5_21

evaluation of polynomials over $\mathbb{F}_q$. Let $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q$ be n distinct non-zero field elements known to all players (e.g., if $q > n$ is a prime, we can have $\alpha_j = j$). To share a secret $s \in \mathbb{F}_q$, a *trusted dealer* chooses t random elements $a_1, \ldots, a_t$, independently and randomly with uniform distribution, from $\mathbb{F}_q$. These random elements together with the secret s define a polynomial $f(x) = s + \sum_{i=1}^{t} a_i x^i$ that is used to generate a share $f(\alpha_j)$ for P_j. The correctness and privacy of Shamir secret scheme follow from properties of Lagrange interpolation (see § 2.2).

In its basic form, secret sharing assumes that the corrupted participants are passive (or semi-honest) and follow the protocol during the reconstruction phase. In practice however, one needs to consider stronger adversaries who deviate from the protocol, collude and submit wrong shares. Secret sharing schemes in presence of active adversaries have been considered in different settings and with different requirements. In this paper, we consider secret sharing with cheater detection (SSCD) introduced by Tompa and Woll [21], and focus on threshold schemes. In the following we shall first provide a brief introduction of SSCD schemes, the relevant questions there in, and finally present our contributions.

Informally, an SSCD scheme allows to detect if a set of submitted shares contain incorrect entries. To achieve cheating detection functionality, the reconstruction algorithm is enhanced by a checking mechanism, failing which, the reconstruction outputs a special symbol "$\perp$", indicating that some of the shares presented are incorrect. The two well known security models for SSCD schemes are given by OKS [17] and CDV [5], where the later guarantees stronger security. In the OKS model, t players, say $P_1, \ldots, P_t$, want to cheat a $(t+1)$th player, P_{t+1}, by opening incorrect shares $\mathsf{Sh}'_1, \ldots, \mathsf{Sh}'_t$. The cheaters *succeed if reconstruction does not output* $\perp$ *and the secret* s' *that is reconstructed from* $\mathsf{Sh}'_1, \ldots, \mathsf{Sh}'_t$ *and* Sh_{t+1} *is different from the shared secret* s. The CDV model has a stronger security requirements. It assumes that the t cheating players *also know the shared secret* s before cheating the $(t+1)$th player. Let δ_{oks} (resp., δ_{cdv}) denote the best probability of successful cheating under OKS (resp., CDV) model and for real numbers $\delta_{\mathsf{oks}}, \delta_{\mathsf{cdv}} > 0$, refer to the schemes as $(t, n, \delta_{\mathsf{oks}})$ OKS-secure and $(t, n, \delta_{\mathsf{cdv}})$ CDV-secure schemes. An SSCD scheme has direct applications to unconditionally secure robust secret sharing [7,6,11,10], secure message transmission [9,13], and cheater identifiable secret sharing [14].

Like basic secret sharing, the most important complexity measure of SSCD schemes is their share size, i.e., the maximum share size of each player. Tompa and Woll [21] have showed that an SSCD scheme *cannot be ideal*. Motivated by the true lower bounds on share sizes, Ogata, Kurosawa, and Stinson [17] showed the following lower bounds on $|\Sigma_i|$ for $(t, n, \delta_{\mathsf{oks}})$ OKS-secure and $(t, n, \delta_{\mathsf{cdv}})$ CDV-secure schemes, respectively:

$$|\Sigma_i| \geq \frac{|\Sigma| - 1}{\delta_{\mathsf{oks}}} + 1; \qquad |\Sigma_i| \geq \frac{|\Sigma| - 1}{\delta^2_{\mathsf{cdv}}} + 1. \tag{1}$$

One of the most important problems in this area is construction of SSCD schemes in which the share size is equal to (or almost the same as) the lower bounds.

1.1 Our Contributions

We first present an efficient $(t, n, \delta_{\mathsf{oks}})$ OKS-secure scheme with share size almost the same as the lower bound. The bit size $\log_2 |\Sigma_i|$ of shares in our scheme is only one bit longer than $\log_2(\frac{|\Sigma|-1}{\delta_{\mathsf{oks}}}+1)$, the bit size of lower bound. The scheme is a simple modification of t-out-of-n Shamir secret sharing, and it is obtained by choosing a polynomial whose degree is at most $2t$ (instead of t). We then apply the same technique to obtain an efficient $(t, n, \delta_{\mathsf{cdv}})$ CDV-secure scheme. The share size of CDV secure scheme is also one bit longer than the known lower bound. The schemes presented in this paper are proven secure without assuming any limit on the computational resources of the adversary.

1.2 Related Work

An OKS-secure scheme was proposed in [17] (a brief description is given in § 3.3). This is the only known scheme whose share size is exactly equal to the lower bound. However, the scheme imposes the restriction that the *secret be drawn with uniform distribution* from secret space. Later, a few other OKS-secure schemes were presented with share size *almost* the same as the lower bound [3,18,4,10]. However, they also impose restrictions. The OKS-secure scheme of [4] (based on [3,18]) requires *only non-binary fields* for secret space, which is a major restriction (see § 3.3 for a brief description of the scheme). The scheme in [10] (see also § 3.3) requires to publish a *checking* vector on an authenticated public bulleting board. There is no CDV-secure scheme with share size equal to the lower bound. An almost optimum scheme was also proposed in [4].

The cheating probability for all of the above schemes is dictated by the cardinality of the secret space S: $\delta = 1/|\Sigma|$. There are also schemes [15,8] where δ can be chosen such that $\delta \gg 1/|\Sigma|$. This is desirable as it allows flexibility in choosing the security level of the system. The problem of constructing OKS-secure (resp., CDV-secure) SSCD schemes that have share size equal to (or nearly the same) as the lower bound, and allow flexible security level is an interesting open question. In [1,16], secure SSCD schemes are proposed under a stronger cheating model, called CDV′, where up to $n-1$ players are allowed to cheat. A closely related cheating model was proposed by Pieprzyk and Zhang in [19] by introducing the concept of cheating-immune secret sharing scheme.

2 Preliminaries

2.1 Notations

For any positive integer n, we let $[n]$ denote the set $\{1, \ldots, n\}$. We write $|S|$ to denote the number of elements in the set S. We write $x \in_R S$ to indicate that x is chosen with respect to the uniform distribution on S. By $x \leftarrow S$, we assume x is chosen with arbitrary distribution. We let $\mathbb{F}_q$ denote a finite field with q elements, and $\mathbb{F}_q[X]$ denote the polynomial ring. For a finite field $\mathbb{F}_q$,

we let $\mathbb{F}_q^{\leq t}[X]$ denote the set $\{f \in \mathbb{F}_q[X] \mid \deg f \leq t\}$, where $t \in \mathbb{N} \cup \{0\}$ and $\deg f$ denotes the degree of f. For a positive integer n, let $\mathbb{Z}_n$ denote the ring of integers modulo n.

2.2 Lagrange Interpolation

Let t be a positive integer and $\mathbb{F}$ be a field. Given any $t+1$ pairs of field elements $(x_1, y_1), \ldots, (x_{t+1}, y_{t+1})$ with distinct x_i's, there exists a *unique* polynomial $f(x) \in \mathbb{F}[x]$ of degree at most t such that $f(x_i) = y_i$ for $1 \leq i \leq t+1$. The polynomial can be obtained using the Lagrange interpolation formula as follows,

$$f(x) = y_1 \lambda_{x_1}^A(x) + \cdots + y_{t+1} \lambda_{x_{t+1}}^A(x), \tag{2}$$

where $A = \{x_1, \ldots, x_{t+1}\}$ and $\lambda_{x_i}^A(x)$'s $(1 \leq i \leq t+1)$ are Lagrange basis polynomials, given by

$$\lambda_{x_i}^A(x) = \frac{\prod_{1 \leq j \leq t+1, j \neq i}(x - x_j)}{\prod_{1 \leq j \leq t+1, j \neq i}(x_i - x_j)} \ .$$

When the base point set $A = \{x_1, \ldots, x_{t+1}\}$ is clear from the context, we denote the interpolation of f by $f \leftarrow \mathsf{LagInt}(y_1, \ldots, y_{t+1})$, and $\lambda_{x_i}^A(x)$ by simply $\lambda_{x_i}(x)$.

2.3 Secret Sharing with Cheating Detection

Let t, n be positive integers such that $1 \leq t < n$. Informally, a t-out-of-n threshold secret sharing scheme enables a dealer, holding a secret piece of information, to distribute this secret among a set of n players such that, later, a subset of players can reconstruct the secret only if there cardinality is at least $t+1$. We let Σ denote the domain of secrets, and Σ_i denote the domain of shares of P_i, $1 \leq i \leq n$. Secutity of SSCD has been studied in different models. We consider the two main models, refered to as OKS [17] and CDV [5] . For fix real numbers $\delta_{\mathsf{oks}}, \delta_{\mathsf{cdv}} > 0$, the schemes secure under OKS model (resp. CDV model) are referred to as $(t, n, \delta_{\mathsf{oks}})$ OKS-secure (resp. $(t, n, \delta_{\mathsf{cdv}})$ CDV-secure) schemes.

Definition 1 (Secret Sharing with Cheating Detection). *A t-out-of-n secret sharing with cheating detection (SSCD) property is consist of two interactive protocols,* Share *and* Rec. *The share distribution protocol* Share *involves a dealer $\mathcal{D}$ and n players $P_1, \ldots, P_n$, and the reconstruction protocol* Rec *involves $P_1, \ldots, P_n$ and a reconstructor $\mathcal{R}$ (a third party). The protocols work as follows:*

- Share*: The dealer $\mathcal{D}$ runs the share distribution algorithm* Share*. It is a probabilistic algorithm that, on input $s \in \Sigma$ returns a share vector $(\mathsf{Sh}_1, \ldots, \mathsf{Sh}_n) \xleftarrow{\$} \mathsf{Share}(s)$, where each Sh_i is privately given to P_i.*
- Rec*: The secret reconstruction algorithm* Rec *is run by $\mathcal{R}$. It is a deterministic algorithm that on input the shares $\mathsf{Sh}_{i_1}, \ldots, \mathsf{Sh}_{i_{t+1}}$ of any $t+1$ players $P_{i_1}, \ldots, P_{i_{t+1}}$ returns a value $s \leftarrow \mathsf{Rec}(\mathsf{Sh}_{i_1}, \ldots, \mathsf{Sh}_{i_{t+1}})$, where $s \in \Sigma \cup \{\perp\}$. The symbol $\perp$ indicates that a cheating has occurred and the algorithm is unable to recover the shared secret.*

Definition 2 (SSCD Security under OKS Model). *Let $\delta_{\mathsf{oks}} > 0$. An* SSCD *scheme is said to be $(t, n, \delta_{\mathsf{oks}})$* OKS-secure *if* Share *and* Rec *protocols satisfy the following properties:*

- ***Correctness**: For every authorized set of players $B \subset \{P_1, \ldots, P_n\}$, i.e., $|B| \geq t+1$, and for every $s \in \Sigma$, we have*

$$\mathsf{Pr}[\mathsf{Rec}(\mathsf{Share}(s)_B) = s] = 1, \tag{3}$$

  where $\mathsf{Share}(s)_B$ denotes the restriction of the n length vector $\mathsf{Share}(s) = (\mathsf{Sh}_1, \ldots, \mathsf{Sh}_n)$ to its B-entries, i.e., $\mathsf{Share}(s)_B = \{\mathsf{Sh}_i\}_{P_i \in B}$, and the probability is computed over the random coins of Share.
- ***Perfect Privacy**: For an unauthorized set $A \subset \{P_1, \ldots, P_n\}$, i.e., $|A| \leq t$, for every pair of values $s_1, s_2 \in S$, and for every possible vector of shares $(\mathsf{Sh}_i)_{P_i \in A}$, it holds that*

$$\mathsf{Pr}[\mathsf{Share}(s_1)_A = (\mathsf{Sh}_i)_{P_i \in A}] = \mathsf{Pr}[\mathsf{Share}(s_2)_A = (\mathsf{Sh}_i)_{P_i \in A}], \tag{4}$$

  where the probabilities are computed over the random coins of Share.
- ***Cheating Detection**: The cheating detection property of an* OKS-secure SSCD *is measured by the maximum probability with which any unbounded adversary $\mathcal{A}_{\mathsf{oks}}$, who actively controls the outputs of up to t P_i, can win the following game -* $\mathsf{OKSGame}^{\mathcal{A}_{\mathsf{oks}}}_{\mathsf{SSCD}}$.

$s \leftarrow S$; $(\mathsf{Sh}_1, \ldots, \mathsf{Sh}_n) \xleftarrow{\$} \mathsf{Share}(s)$;
$(i_1, \ldots, i_t) \leftarrow \mathcal{A}_{\mathsf{oks}}$;
$(\mathsf{Sh}'_{i_1}, \ldots, \mathsf{Sh}'_{i_t}, i_{t+1}) \leftarrow \mathcal{A}_{\mathsf{oks}}(\mathsf{Sh}_{i_1}, \ldots, \mathsf{Sh}_{i_t})$;
$s' \leftarrow \mathsf{Rec}(\mathsf{Sh}'_{i_1}, \ldots, \mathsf{Sh}'_{i_t}, \mathsf{Sh}_{i_{t+1}})$;
$s' \leftarrow$ Game-Output .

Fig. 1. $\mathsf{OKSGame}^{\mathcal{A}_{\mathsf{oks}}}_{\mathsf{SSCD}}$: The Cheating Detection Game

The game is played between the dealer $\mathcal{D}$ and the adversary $\mathcal{A}_{\mathsf{oks}}$. In the game, $\mathcal{D}$ first picks a secret $s \in S$, and computes $(\mathsf{Sh}_1, \ldots, \mathsf{Sh}_n) \xleftarrow{\$} \mathsf{Share}(s)$. Next, $\mathcal{A}_{\mathsf{oks}}$ corrupts up to t players, say $P_{i_1}, \ldots, P_{i_t}$, learns their shares, and sends possibly modified shares $(\mathsf{Sh}'_{i_1}, \ldots, \mathsf{Sh}'_{i_t}) \leftarrow \mathcal{A}_{\mathsf{oks}}(\mathsf{Sh}_{i_1}, \ldots, \mathsf{Sh}_{i_t})$ along with the identity of a $(t+1)$th player, say $P_{i_{t+1}}$, to $\mathcal{R}$. The adversary is said to win if, $\mathsf{Rec}(\mathsf{Sh}'_{i_1}, \ldots, \mathsf{Sh}'_{i_t}, \mathsf{Sh}_{i_{t+1}}) = s'$ and $s' \notin \{s, \perp\}$. We measure $\mathcal{A}_{\mathsf{oks}}$'s success by the real number

$$Adv^{\mathcal{A}_{\mathsf{oks}}}_{\mathsf{SSCD}} = \mathsf{Pr}[s' \notin \{s, \perp\} \mid s' \leftarrow \mathsf{Rec}(\mathsf{Sh}'_{i_1}, \ldots, \mathsf{Sh}'_{i_t}, \mathsf{Sh}_{i_{t+1}})]. \tag{5}$$

The $(t, n, \delta_{\mathsf{oks}})$ security requires that $Adv^{\mathcal{A}_{\mathsf{oks}}}_{\mathsf{SSCD}} \leq \delta_{\mathsf{oks}}$.

Definition 3 (SSCD Security under CDV Model). *The security is strengthened under the* CDV *model for* SSCD *schemes. In the cheating detection game, it is assumed that t corrupted players also know the shared secret s before they attempt to cheat the $(t+1)$th player. Formally, an* SSCD *scheme is called $(t, n, \delta_{\mathsf{cdv}})$* CDV-secure *if* Share *and* Rec *protocols satisfy following properties:*

- *The* Correctness *and* Privacy *hold true as defined in Definition 2.*
- ***Cheating Detection**: Let $\mathcal{A}_{\mathsf{cdv}}$ denote the adversary in the* CDV *model. The cheating detection game, denoted by $\mathsf{CDVGame}^{\mathcal{A}_{\mathsf{cdv}}}_{\mathsf{SSCD}}$, is the same as the* OKS *cheating detection game, except the extra information s available to the adversary, as shown below.*

$$
\begin{array}{l}
s \leftarrow S;\ (\mathsf{Sh}_1, \ldots, \mathsf{Sh}_n) \xleftarrow{\$} \mathsf{Share}(s); \\
(i_1, \ldots, i_t) \leftarrow \mathcal{A}_{\mathsf{cdv}}; \\
(\mathsf{Sh}'_{i_1}, \ldots, \mathsf{Sh}'_{i_t}, i_{t+1}) \leftarrow \mathcal{A}_{\mathsf{cdv}}(\mathsf{Sh}_{i_1}, \ldots, \mathsf{Sh}_{i_t}, s); \\
s' \leftarrow \mathsf{Rec}(\mathsf{Sh}'_{i_1}, \ldots, \mathsf{Sh}'_{i_t}, \mathsf{Sh}_{i_{t+1}}); \\
s' \leftarrow \mathsf{Game\text{-}Output}\ .
\end{array}
$$

Fig. 2. $\mathsf{CDVGame}^{\mathcal{A}_{\mathsf{cdv}}}_{\mathsf{SSCD}}$: The Cheating Detection Game

The adversary is said to win if, $\mathsf{Rec}(\mathsf{Sh}'_{i_1}, \ldots, \mathsf{Sh}'_{i_t}, \mathsf{Sh}_{i_{t+1}}) = s'$ and $s' \notin \{s, \perp\}$. The advantage of $\mathcal{A}_{\mathsf{cdv}}$ is measured by $Adv^{\mathcal{A}_{\mathsf{cdv}}}_{\mathsf{SSCD}} = \mathsf{Pr}[s' \notin \{s, \perp\} \mid s' \leftarrow \mathsf{Rec}(\mathsf{Sh}'_{i_1}, \ldots, \mathsf{Sh}'_{i_t}, \mathsf{Sh}_{i_{t+1}})]$. The $(t, n, \delta_{\mathsf{cdv}})$ security requires that $Adv^{\mathcal{A}_{\mathsf{cdv}}}_{\mathsf{SSCD}} \leq \delta_{\mathsf{cdv}}$.

Known Lower Bounds. The lower bounds on the share sizes of both OKS-secure and CDV-secure schemes were presented by Ogata, Kurosawa and Stinson in [17]. In the following, we recall the bounds.

Theorem 1. *([17]) For any $(t, n, \delta_{\mathsf{oks}})$* OKS-secure SSCD *scheme with the domain of secrets is denoted by Σ, the size of the total shares of P_i for every $i \in [n]$ is lower bounded by*

$$|\Sigma_i| \geq \frac{|\Sigma| - 1}{\delta_{\mathsf{oks}}} + 1. \tag{6}$$

The lower bound under the CDV model was derived assuming that the secret is uniformly distributed.

Theorem 2. *([17]) For any $(t, n, \delta_{\mathsf{cdv}})$* CDV-secure SSCD *scheme where the domain of secret is Σ with uniform distribution, the size of total shares of P_i for every $i \in [n]$ is lower bounded by*

$$|\Sigma_i| \geq \frac{|\Sigma| - 1}{\delta^2_{\mathsf{cdv}}} + 1 \tag{7}$$

Although, the schemes proposed in this paper are not *flexible*, we include the following section for completeness.

2.4 Relationship between δ and $|\Sigma|$

The maximum cheating probability δ for existing schemes is largely dictated by the cardinality of secret space Σ and is given by $\delta \approx 1/|\Sigma|$. But from a practical perspective, it is important to choose δ independently. The schemes in [15,8] can choose δ that is arbitrarily larger than $1/|\Sigma|$. On the other hand, when the secret space is small, it is important for the scheme to have $\delta \ll 1/|\Sigma|$. For example, for 20 bit secret size, one may require $\delta = 1/2^{60} \ll 1/2^{20}$.

The construction of a flexible scheme with share size equal to, or nearly the same as, the known lower bound (under OKS/CDV or both models) is an interesting open problem.

3 A $(t, n, \delta_{\mathsf{oks}})$ OKS-secure SSCD Scheme

In this section, we present an $(t, n, \delta_{\mathsf{oks}})$ OKS-secure SSCD scheme with share size nearly the same as the lower bound of Theorem 1. In our scheme, the secrets are drawn from a finite field $\mathbb{F}_q$ and cheating probability is at most $\frac{1}{q}$. The information rate of our scheme is 1/2.

3.1 The Proposed Scheme Π_{aopt}

Let t and n be positive integers such that $1 \leq t < n$. Choose a finite field $\mathbb{F}_q$ with $q > 2n$. Choose $2n$ distinct points, $\alpha_1, \ldots, \alpha_{2n} \in \mathbb{F}_q$, known to all players. We now present our scheme.

- Share: On input a secret $s \in \mathbb{F}_q$, the share generation algorithm Share outputs a list of shares as follows. The dealer $\mathcal{D}$ randomly picks a polynomial $f \in_R \mathbb{F}_q^{\leq 2t}[x]$ such that $f(0) = s$. For every j in $1 \leq j \leq 2n$, it computes $s_j = f(\alpha_j)$. Finally, for every i in $1 \leq i \leq n$, player P_i gets $\mathsf{Sh}_i = (s_i, s_{n+i})$ as their share:

Share Distribution Algorithm
Secret $s \in \mathbb{F}_q$
$\downarrow f \in \mathbb{F}_q^{\leq 2t}[x]$
$f(\alpha_1), \ldots, f(\alpha_{2n})$
$P_i \leftarrow (f(\alpha_i), f(\alpha_{n+i}))$, $1 \leq i \leq n$

- Rec: The secret reconstruction algorithm Rec proceeds as follows. Suppose the following $t+1$ players $P_{i_1}, \ldots, P_{i_{t+1}}$ provided shares (correct or corrupted) $\mathsf{Sh}'_{i_1}, \ldots, \mathsf{Sh}'_{i_{t+1}}$ respectively. The share of P_i is corrupted if $\mathsf{Sh}'_i = (s'_i, s'_{n+i}) \neq (s_i, s_{n+i})$. This means $\mathcal{R}$ has $2t+2$ points $\{s'_{i_1}, s'_{n+i_1}, \ldots, s'_{i_{t+1}}, s'_{n+i_{t+1}}\}$ such that at most $2t$ of them are possibly modified. To detect a possible cheating $\mathcal{R}$ proceeds as follows.
  - First, it interpolates a unique polynomial $f' \leftarrow \mathsf{LagInt}(s'_{i_1}, s'_{n+i_1}, \ldots, s'_{i_{t+1}}, s'_{n+i_{t+1}})$ (see § 2.2 for Lagrange Interpolation LagInt).

- It then checks if the degree of $f' \stackrel{?}{=} 2t+1$. If yes, it outputs $\perp$ which indicates that cheating has occurred.
- Otherwise (i.e., when degree of $f' \leq 2t$), $\mathcal{R}$ outputs $f'(0)$ as the reconstructed secret.

3.2 Security

In order to prove the security of Π_{aopt}, we first prove two simple lemmas.

Lemma 1. *Let $\mathbb{F}$ be any finite field and let $\alpha_1, \ldots, \alpha_k \in \mathbb{F}$ be any k distinct points. Let $f = \sum_{i=0}^{k} a_i x^i$ be chosen at random from $\mathbb{F}^{\leq k}[x]$. Then given $f(\alpha_1)$, $\ldots, f(\alpha_k)$, it holds that one of the coefficients $\{a_i\}_{i=0}^{k}$ of f is uniformly distributed over $\mathbb{F}$.*

Proof: Given $f(\alpha_1), \ldots, f(\alpha_k)$ for a random $f \in \mathbb{F}^{\leq k}[x]$, we have the following system of linear equations, where $a_0, a_1, \ldots, a_k$ form the unknowns of the system:

$$\begin{bmatrix} 1 & \alpha_1 & \ldots & \alpha_1^k \\ 1 & \alpha_2 & \ldots & \alpha_2^k \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_k & \ldots & \alpha_k^k \end{bmatrix} \cdot \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_k \end{bmatrix} = \begin{bmatrix} f(\alpha_1) \\ f(\alpha_2) \\ \vdots \\ f(\alpha_k) \end{bmatrix} \tag{8}$$

Fixing any of the unknowns, e.g. a_1, will transform system (8) in to:

$$\begin{bmatrix} 1 & \alpha_1^2 & \ldots & \alpha_1^k \\ 1 & \alpha_2^2 & \ldots & \alpha_2^k \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_k^2 & \ldots & \alpha_k^k \end{bmatrix} \cdot \begin{bmatrix} a_0 \\ a_2 \\ \vdots \\ a_k \end{bmatrix} = \begin{bmatrix} f(\alpha_1) - a_1\alpha_1 \\ f(\alpha_2) - a_1\alpha_2 \\ \vdots \\ f(\alpha_k) - a_1\alpha_k \end{bmatrix} \tag{9}$$

Clearly, the resulting system admits a unique solution (for $(a_0, a_2, \ldots, a_k)^T$) as its coefficient matrix is non-singular. Therefore a_1 is uniformly distributed.

Lemma 2. *Let $\mathbb{F}$ be any finite field and let $a_0, \ldots, a_{j-1}, a_{j+1}, \ldots, a_k$ be any k points in $\mathbb{F}$. Let a_j be chosen at random from $\mathbb{F}$. Define $f_{a_j} = \sum_{i=0}^{k} a_i x^i \in \mathbb{F}^{\leq k}[x]$. Then for every $\alpha, \beta \in \mathbb{F}$ with $\alpha \neq 0$, it holds that $Pr[f_{a_j}(\alpha) = \beta] = \frac{1}{|\mathbb{F}|}$.*

Proof: Let $f_{a_j}(x) = a_0 + \cdots + a_j x^j + \cdots + a_k x^k$. Then $\Pr[f_{a_j}(\alpha) = \beta] = \Pr[a_0 + \cdots + a_j\alpha^j + \cdots + a_k\alpha^k] = \beta$, where the probability is computed over the random choice of $a_j \in \mathbb{F}$. Hence, for a randomly chosen $a_j \in \mathbb{F}$ we have

$$\begin{aligned} \Pr\left[\sum_{i=0}^{k} a_i\alpha^i = \beta\right] &= \Pr\left[a_j\alpha^j = \beta - \sum_{0\leq i\leq k; i\neq j} a_i\alpha^i\right] \\ &= \Pr\left[a_j = (\alpha^j)^{-1}\left(\beta - \sum_{0\leq i\leq k; i\neq j} a_i\alpha^i\right)\right] \\ &= \frac{1}{|\mathbb{F}|}, \end{aligned}$$

where the second equality holds since $\alpha \in \mathbb{F}$ and $\alpha \neq 0$ implying that α^j is invertible, and the last equality is due to the fact that a_j is randomly chosen from $\mathbb{F}$. This concludes the proof.

Theorem 3. *The* SSCD *scheme* Π_{aopt} *of § 3.1 is* $(t, n, \delta_{\mathsf{oks}})$ OKS-secure *with secret space* $\Sigma = \mathbb{F}_q$*, share space* $\Sigma_i = \mathbb{F}_q \times \mathbb{F}_q$ *for every* P_i*, and* $\delta_{\mathsf{oks}} = \frac{1}{q}$.

Proof: The correctness and privacy of Π_{aopt} follows immediately from Shamir secret sharing scheme: any set of $t+1$ players can reconstruct the secret as they hold $2t+2$ shares of f, while a set of t players have only $2t$ shares which do not leak any information about the secret as $f \in \mathbb{F}_q^{\leq 2t}[X]$.

We now derive the maximum probability of cheating. For notational clarity, suppose $t+1$ players $P_1, \ldots, P_{t+1}$ participate in the reconstruction. We further assume that $P_1, \ldots, P_t$ are corrupted and provide shares $\mathsf{Sh}'_1, \ldots, \mathsf{Sh}'_t$ such that $\mathsf{Sh}'_i = (s'_i, s'_{n+i}) \neq (s_i, s_{n+i})$ for at least one $i \in [t]$. The player P_{t+1} who is honest provides the correct share $\mathsf{Sh}_{t+1} = (s_{t+1}, s_{n+t+1})$. The cheating will not be detected if $s'_1, s'_{n+1}, \ldots, s'_t, s'_{n+t}$ and s_{t+1}, s_{n+t+1} lie on a polynomial of degree at most $2t$. The later is true iff s_{n+t+1} lies on the polynomial passing through $s'_1, s'_{n+1}, \ldots, s'_t, s'_{n+t}$ and s_{t+1}. Let $f' = \sum_{i=0}^{2t} b_i x^i$ be the unique polynomial passing through $2t+1$ points $s'_1, s'_{n+1}, \ldots, s'_t, s'_{n+t}$ and s_{t+1}. As f' is of degree at most $2t$, and the shares of the corrupted players constitute $2t$ points on f', the Lemma 1 implies that at least one coefficient of f' will remain uniform to the corrupted players. Therefore by Lemma 2 it holds that $\Pr[f'(\alpha_{n+t+1}) = s_{n+t+1}] = \frac{1}{q}$. This concludes the proof.

3.3 Efficiency Comparison

Previous Works. In [17] Ogata, Kurosawa and Stinson proposed a $(t, n, \delta_{\mathsf{oks}})$ OKS-secure SSCD scheme achieving the lower bound of Theorem 1. The scheme uses a combinatorial object called *difference set*. In the following we provide a brief description of their scheme. The scheme is denoted by Π_{oks}.

Definition 4. *([17]* (N, ℓ, λ) *Difference Set) Let* $(\Gamma, +)$ *be an Abelian (commutative) group of order* N*. A subset* $B \subset \Gamma$ *is called an* (N, ℓ, λ) *difference set if* $|B| = \ell$ *and the set of non-zero differences* $\{d - d' \mid d, d'(d \neq d') \in B\}$ *contains each non-zero element of* Γ *precisely* λ *times.*

For an (N, ℓ, λ) difference set $B \subset \Gamma$, it is clear that $|\Gamma| = N = \frac{\ell(\ell-1)}{\lambda} + 1$. The Π_{oks} scheme was constructed in [17] using a special (N, ℓ, λ) difference set $B \subset \Gamma$ such that $(\Gamma, +, \cdot)$ is a *field*. It is known that there exists an $(N, \ell, 1)$ difference set $B \subset \mathbb{Z}_N$ if ℓ is a prime power, and therefore the scheme of [17] can be instantiated using $B \subset \mathbb{Z}_N$ if N is also a prime, i.e., $(\mathbb{Z}_N, +, \cdot)$ is a field. It is also known that if $N \equiv 3 \pmod 4$ is a prime power, then there exists an (N, ℓ, λ) difference set B in the field $\mathbb{F}_N$ such that $N = 4k - 1$, $\ell = 2k - 1$, and $\lambda = k - 1$, where k is a positive integer. We now state the main theorem of [17].

Theorem 4. *([17]) Let N be a prime power, and t, n be positive integers such that $1 \leq t < n < N$. If there exists an (N, ℓ, λ) difference set B in $(\mathbb{F}_N, +)$, then there exists a $(t, n, \delta_{\mathsf{oks}})$* OKS-secure *secret sharing scheme for a uniformly distributed secret over $\Sigma = B$, such that $|\Sigma| = |B| = \ell$, $|\Sigma_i| = |\mathbb{F}_N| = \frac{\ell(\ell-1)}{\lambda} + 1$ for every $i \in [n]$ and $\delta_{\mathsf{oks}} = \frac{\lambda}{\ell}$, i.e., $|\Sigma_i| = \frac{|\Sigma|-1}{\delta_{\mathsf{oks}}} + 1$ for every $i \in [n]$ (meets the lower bound of Theorem 1).*

The Π_{oks} scheme does not work for an arbitrary prime power N; in particular, it also requires that there exists an (N, ℓ, λ) difference set for some $\ell, \lambda \in \mathbb{N}$. The scheme is proven secure only if secret is *chosen with uniform distribution*. The scheme was also compared in [18] to be less computationally efficient.

In [4] Cabello, Padró and Sáez proposed a method (based on [3,18]) that provides cheating detection functionality for any linear secret sharing scheme realizing general access structures. When their method is applied to Shamir secret sharing (for threshold access structure), it yields a $(t, n, \delta_{\mathsf{oks}})$ OKS-secure SSCD with almost optimum share sizes. A brief description of their scheme, denoted by Π_{cps}, is given below. Let $\mathbb{F}_q$ be a finite field with characteristic different from 2, and $q > n$. Let $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q$ be known to all players. For a given secret $s \in \mathbb{F}_q$, the dealer picks at random two polynomials $f_1, f_2 \in \mathbb{F}_q^{\leq t}[X]$ such that $f_1(0) = s$ and $f_2(0) = s^2$ respectively. Every player P_i receives the share $\mathsf{Sh}_i = (s_{i1}, s_{i2}) = (f_1(\alpha_i), f_2(\alpha_i))$. During reconstruction, for any $t+1$ players $P_{i_1}, \ldots, P_{i_{t+1}}$, $\mathcal{R}$ computes (s_1, s_2) from their shares, where $s_1 \leftarrow \mathsf{LagInt}(s_{i_1 1}, \ldots, s_{i_{t+1} 1})$ and $s_2 \leftarrow \mathsf{LagInt}(s_{i_1 2}, \ldots, s_{i_{t+1} 2})$. If $s_2 = s_1^2$, $\mathcal{R}$ outputs $s = s_1$ as the correct value of the shared secret; Otherwise when $s_2 \neq s_1^2$, it outputs $\perp$. Π_{cps} is summarized in the following theorem.

Theorem 5. *([4]) Let $\mathbb{F}_q$ be a finite field with characteristic different from 2, and $q > n$. The* SSCD *scheme Π_{cps} is $(t, n, \delta_{\mathsf{oks}})$* OKS-secure *with secret space $\Sigma = \mathbb{F}_q$, share space $\Sigma_i = \mathbb{F}_q \times \mathbb{F}_q$ for every P_i, and $\delta_{\mathsf{oks}} = \frac{1}{q}$. Clearly the share size $|\Sigma_i| = q^2$ is nearly the same as $\frac{|\Sigma|-1}{\delta_{\mathsf{oks}}} + 1 = q^2 - q + 1$.*

The main drawback of Π_{cps} is that it works for finite fields with characteristic different from 2. This is a serious constraint as binary fields make for a suitable choice in implementation of cryptographic protocols and in particular for resource constrained devices.

Recently, In [10] Jhanwar and Safavi-Naini proposed a $(t, n, \delta_{\mathsf{oks}})$ OKS-secure SSCD scheme with almost optimum share sizes. Let Π_{js} denote this scheme. The scheme works as follows. Consider a finite field $\mathbb{F}_q$ such that $q > n$. Let $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q$ be known to all players. For a given secret $s \in \mathbb{F}_q$, the dealer first picks at random $X(\neq 0), r \in \mathbb{F}_q$ and computes $Y = s + Xr$. It then picks at random two polynomials $f_1, f_2 \in \mathbb{F}_q^{\leq t}[X]$ such that $f_1(0) = s$ and $f_2(0) = r$ respectively. Every player P_i receives the share $\mathsf{Sh}_i = (s_i, r_i) = (f_1(\alpha_i), f_2(\alpha_i))$. The tuple (X, Y) is *kept as part of system's public parameters*. During reconstruction, for any $t+1$ players $P_{i_1}, \ldots, P_{i_{t+1}}$, $\mathcal{R}$ computes (s', r') from their shares, where $s' \leftarrow \mathsf{LagInt}(s_{i_1}, \ldots, s_{i_{t+1}})$ and $r' \leftarrow \mathsf{LagInt}(r_{i_1}, \ldots, r_{i_{t+1}})$. If $Y = s' + Xr'$,

the Rec outputs $s = s'$ as the correct value of the shared secret and it outputs $\perp$ if $Y \neq s' + Xr'$. We now state the security theorem of Π_{js}.

Theorem 6. *([10]) Let $\mathbb{F}_q$ be a finite field with $q > n$. The* SSCD *scheme Π_{js} is $(t, n, \delta_{\mathsf{oks}})$* OKS-secure *with secret space $\Sigma = \mathbb{F}_q$, share space $\Sigma_i = \mathbb{F}_q \times \mathbb{F}_q$ for every P_i, and $\delta_{\mathsf{oks}} = \frac{1}{q}$. Clearly the share size $|\Sigma_i| = q^2$ is nearly the same as $\frac{|\Sigma|-1}{\delta_{\mathsf{oks}}} + 1 = q^2 - q + 1$.*

The Π_{js} construction puts $X, Y \in \mathbb{F}_q$ as part of public parameters that are stored on a publicly accessible authenticated bulletin board. In the case when such public bulleting board is not available, the usual way out is to issue public parameters as part of shares to the players. Because X and Y are used in cheating detection, it is necessary to receive them in correct. But this may not be guaranteed, if they are issued as part of shares.

Efficiency of Our Scheme. We first note that our scheme Π_{opt} does not have any special requirements. Unlike the previous schemes [17,4], the secret in our scheme can be from any field. The only requirement is that the field size be $\geq 2n$. The security against cheating detection holds for arbitrary distribution of secret. Suppose $k = \lfloor \log_2 q \rfloor$. The shares in our scheme consist of $\log_2(q^2) = 2k$ bits, which is only one bit longer than $\log_2(\frac{|\Sigma|-1}{\delta} + 1) = \log_2(q(q-1)+1) \geq \log_2 q + \log_2(q-1) \geq 2k - 1$, the size of lower bound.

4 A $(t, n, \delta_{\mathsf{cdv}})$ CDV-secure SSCD Scheme

We present a $(t, n, \delta_{\mathsf{cdv}})$ CDV-secure SSCD scheme that is constructed using the technique in § 3.1. In CDV model, the reconstruction is against a stronger adversary who, in addition to the t shares, also knows the shared secret. In the share distribution phase of the new scheme, the dealer picks a polynomial f of degree at most $3t + 1$, and gives out 3 distinct points on f to every P_i. The shares of any t players and the additional knowledge of the shared secret give $3t+1$ points on f, which means f can not be fully reconstructed. But, any $t + 1$ shares give $3t + 3$ points on f, which is one point more than the required $3t + 2$ points. This extra point is used for cheating detection. We now formally describe the scheme.

4.1 The Proposed Scheme $\tilde{\Pi}_{\mathsf{aopt}}$

Let t and n are positive integers such that $1 \leq t < n$. Choose a finite field $\mathbb{F}_q$ with $q > 3n$. Choose $3n$ distinct points, $\alpha_1, \ldots, \alpha_{3n} \in \mathbb{F}_q$, known to all players. We now present our scheme.

- Share: On input a secret $s \in \mathbb{F}_q$, the share generation algorithm Share outputs a list of shares as follows. The dealer $\mathcal{D}$ randomly picks a polynomial $f \in_R \mathbb{F}_q^{\leq 3t+1}[x]$ such that $f(0) = s$. For every j in $1 \leq j \leq 3n$, the

dealer computes $s_j = f(\alpha_j)$. Finally, for every i in $1 \leq i \leq n$, P_i receives $\mathsf{Sh}_i = (s_i, s_{n+i}, s_{2n+i})$ as her share:

Share Distribution Algorithm
Secret $s \in \mathbb{F}_q$
$\downarrow f \in \mathbb{F}_q^{\leq 3t+1}[x]$
$f(\alpha_1), \ldots, f(\alpha_{3n})$
$P_i \leftarrow (f(\alpha_i), f(\alpha_{n+i}), f(\alpha_{2n+i}))$, $1 \leq i \leq n$

– Rec: The secret reconstruction algorithm Rec proceeds as follows. Suppose the following $t+1$ players $P_{i_1}, \ldots, P_{i_{t+1}}$ provided shares (correct or corrupted) $\mathsf{Sh}'_{i_1}, \ldots, \mathsf{Sh}'_{i_{t+1}}$ respectively. The share of P_i is corrupted if $\mathsf{Sh}'_i = (s'_i, s'_{n+i}, s'_{2n+i}) \neq (s_i, s_{n+i}, s_{2n+i})$. This means, $\mathcal{R}$ has $3t+3$ points such that at most $3t$ of them are possibly modified. To detect a possible cheating, $\mathcal{R}$ now proceeds as follows.
  - First, it interpolates a unique polynomial $f' \leftarrow \mathsf{LagInt}(\mathsf{Sh}'_{i_1}, \ldots, \mathsf{Sh}'_{i_{t+1}})$ (see § 2.2 for Lagrange Interpolation LagInt).
  - It then checks if the degree of $f' \stackrel{?}{=} 3t+2$. If yes, it outputs $\perp$ which indicates that cheating has occurred.
  - Otherwise (i.e., when degree of $f' \leq 3t+1$), $\mathcal{R}$ outputs $f'(0)$ as the reconstructed secret.

4.2 Security

Theorem 7. *The* SSCD *scheme* $\tilde{\Pi}_{\mathsf{aopt}}$ *of § 4.1 is* $(t, n, \delta_{\mathsf{cdv}})$ CDV-secure *with secret space* $\Sigma = \mathbb{F}_q$*, share space* $\Sigma_i = (\mathbb{F}_q)^3$ *for every* P_i*, and* $\delta_{\mathsf{cdv}} = \frac{1}{q}$.

Proof: The correctness and privacy of Π_{aopt} follow immediately from Shamir secret sharing scheme: any t players hold $3t$ shares which do not leak any information about the secret as $f \in \mathbb{F}_q^{\leq 3t+1}[X]$, and any $t+1$ players can reconstruct the secret as they hold $3t+3$ shares of f. We now derive the maximum probability of cheating. Suppose players $P_1, \ldots, P_{t+1}$ provide shares during reconstruction. We further assume that $P_1, \ldots, P_t$ are corrupted, and they know the shared secret s. The shares $\{(s'_i, s'_{n+i}, s'_{2n+i})\}_{i \in [t]}$ of corrupted players, together with s, give $3t+1$ points on f. As degree of f is at most $3t+1$, Lemma 1 and 2 together imply that $3t+3$ points of $\mathsf{Sh}'_1, \ldots, \mathsf{Sh}'_t$ and Sh_{t+1} lie on a polynomial of degree at most $3t+1$ with probability at most $1/q$.

4.3 Efficiency Comparison

In [4], Cabello, Padró and Sáez proposed a method (based on [3,18]) that provides cheating detection functionality (under CDV model) for any linear secret sharing scheme realizing general access structures. When their method is applied to Shamir secret sharing (for threshold access structure), it yields a $(t, n, \delta_{\mathsf{cdv}})$ CDV-secure SSCD with almost optimum share sizes. A brief description of their scheme, denoted as $\tilde{\Pi}_{\mathsf{cps}}$, is given below. Let us fix a finite field $\mathbb{F}_q$ with $q > n$. Let

$\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q$ be known to all players. For a given secret $s \in \mathbb{F}_q$ it first picks a random $r \in \mathbb{F}_q$. The dealer then picks at random polynomials $f_1, f_2, f_3 \in \mathbb{F}_q^{\leq t}[X]$ such that $f_1(0) = s$, $f_2(0) = r$ and $f_3(0) = rs$ respectively. Every player P_i receives the share $\mathsf{Sh}_i = (s_{i1}, s_{i2}, s_{i3}) = (f_1(\alpha_i), f_2(\alpha_i), f_3(\alpha_i))$. During reconstruction, for any $t+1$ players $P_{i_1}, \ldots, P_{i_{t+1}}$, $\mathcal{R}$ computes (s_1, s_2, s_3) from their shares, where $s_j \leftarrow \mathsf{LagInt}(s_{i_1 j}, \ldots, s_{i_{t+1} j})$, $j \in \{1, 2, 3\}$. If $s_3 = s_1 s_2$, the Rec outputs $s = s_1$ as the correct value of the shared secret; otherwise, i.e., when $s_3 \neq s_1 s_2$, it outputs $\perp$. The scheme $\tilde{\Pi}_{\mathsf{cps}}$ is almost optimum with respect to the lower bound of Theorem 1. $\tilde{\Pi}_{\mathsf{cps}}$ is summarized in the following theorem.

Theorem 8. *([4]) Let $\mathbb{F}_q$ be a finite field with $q > n$. The* SSCD *scheme $\tilde{\Pi}_{\mathsf{cps}}$ is $(t, n, \delta_{\mathsf{cdv}})$* CDV-secure *with secret space $\Sigma = \mathbb{F}_q$, share space $\Sigma_i = (\mathbb{F}_q)^3$ for every P_i, and $\delta_{\mathsf{cdv}} = \frac{1}{q}$. Clearly the share size $|\Sigma_i| = q^3$ is nearly the same as $\frac{|\Sigma|-1}{\delta_{\mathsf{cdv}}^2} + 1 = q^2(q-1) + 1 = q^3 - q^2 + 1$.*

Efficiency of Our Scheme. To the best of our knowledge the schemes $\tilde{\Pi}_{\mathsf{cps}}$ ([4]) and the proposed scheme $\tilde{\Pi}_{\mathsf{aopt}}$ are the only known schemes that are almost optimum with respect to the share size. Suppose $k = \lfloor \log_2 q \rceil$. The shares in our scheme consist of $\log_2(q^3) = 3k$ bits, which is only one bit longer than $\log_2(\frac{|\Sigma|-1}{\delta_{\mathsf{cdv}}^2} + 1) = \log_2(q^2(q-1)+1) \geq 2\log_2 q + \log_2(q-1) \geq 3k - 1$, the size of the lower bound.

5 Concluding Remarks

We presented a simple method for adding cheating detection to Shamir secret sharing scheme. We used the same approach for both security models of cheating detection. The resulting schemes have almost optimum share sizes. Unlike existing schemes, our constructions do not impose any special requirement on parameters. It is interesting to see if our technique can be generalized to work for any linear secret sharing scheme. It is also interesting to find its applicability for robust secret sharing and secure message transmission that are based on Shamir secret sharing.

Acknowledgments. The authors would like to thank a reviewer of SPACE 2015 for detailed comments.

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. Blakley, G.: Safeguarding cryptographic keys. AFIPS National Computer Conference 48, 313–317 (1979)

3. Cabello, S., Padró, C., Sáez, G.: Secret sharing schemes with detection of cheaters for a general access structure. In: Ciobanu, G., Păun, G. (eds.) FCT 1999. LNCS, vol. 1684, pp. 185–194. Springer, Heidelberg (1999)
4. Cabello, S., Padró, C., Sáez, G.: Secret sharing schemes with detection of cheaters for a general access structure. Des. Codes Cryptography 25(2), 175–188 (2002)
5. 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)
6. 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)
7. Cramer, R., Damgård, I., 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)
8. 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)
9. Dolev, D., Dwork, C., Waarts, O., Yung, M.: Perfectly secure message transmission. In: FOCS 1990, pp. 36–45. IEEE Computer Society (1990)
10. Jhanwar, M.P., Safavi-Naini, R.: On the Share Efficiency of Robust Secret Sharing and Secret Sharing with Cheating Detection. In: Paul, G., Vaudenay, S. (eds.) INDOCRYPT 2013. LNCS, vol. 8250, pp. 179–196. Springer, Heidelberg (2013)
11. Jhanwar, M.P., Safavi-Naini, R.: Unconditionally-secure ideal robust secret sharing schemes for threshold and multilevel access structure. J. Mathematical Cryptology 7(4), 279–296 (2013)
12. Karnin, E.D., Greene, J.W., Hellman, M.E.: On secret sharing systems. IEEE Transactions on Information Theory 29(1), 35–41 (1983)
13. Kurosawa, K., Suzuki, K.: Almost secure (1-round, n-channel) message transmission scheme. IEICE Transactions 92-A(1), 105–112 (2009)
14. 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)
15. 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)
16. Ogata, W., Eguchi, H.: Cheating detectable threshold scheme against most powerful cheaters for long secrets. Des. Codes Cryptography 71(3), 527–539 (2014)
17. Ogata, W., Kurosawa, K., Stinson, D.R.: Optimum secret sharing scheme secure against cheating. SIAM J. Discrete Math. 20(1), 79–95 (2006)
18. Padró, C., Sáez, G., Villar, J.L.: Detection of cheaters in vector space secret sharing schemes. Des. Codes Cryptography 16(1), 75–85 (1999)
19. Pieprzyk, J., Zhang, X.-M.: On cheating immune secret sharing. Discrete Mathematics & Theoretical Computer Science 6(2), 253–264 (2004)
20. Shamir, A.: How to share a secret. Communications of the ACM 22(11), 612–613 (1979)
21. Tompa, M., Woll, H.: How to share a secret with cheaters. J. Cryptology 1(2), 133–138 (1988)