Almost Optimum t-Cheater Identifiable Secret Sharing Schemes

Satoshi Obana

NEC
obana@bx.jp.nec.com

Abstract. In Crypto'95, Kurosawa, Obana and Ogata proposed a k-out-of-n secret sharing scheme capable of identifying up to t cheaters with probability $1-\epsilon$ under the condition $t \leq \lfloor (k-1)/3 \rfloor$. The size of share $|\mathcal{V}_i|$ of the scheme satisfies $|\mathcal{V}_i| = |\mathcal{S}|/\epsilon^{t+2}$, which was the most efficient scheme known so far. In this paper, we propose new k-out-of-n secret sharing schemes capable of identifying cheaters. The proposed scheme possesses the same security parameters t, ϵ as those of Kurosawa *et al.*. The scheme is surprisingly simple and its size of share is $|\mathcal{V}_i| = |\mathcal{S}|/\epsilon$, which is much smaller than that of Kurosawa *et al.* and is almost optimum with respect to the size of share; that is, the size of share is only one bit longer than the existing bound. Further, this is the first scheme which can identify cheaters, and whose size of share is independent of any of n, k and t. We also present schemes which can identify up to $\lfloor (k-2)/2 \rfloor$, and $\lfloor (k-1)/2 \rfloor$ cheaters whose sizes of share can be approximately written by $|\mathcal{V}_i| \approx (n \cdot (t+1) \cdot 2^{3t-1} \cdot |\mathcal{S}|)/\epsilon$ and $|\mathcal{V}_i| \approx ((n \cdot t \cdot 2^{3t})^2 \cdot |\mathcal{S}|)/\epsilon^2$, respectively. The number of cheaters that the latter two schemes can identify meet the theoretical upper bound.

Keywords: Secret Sharing, Cheater Identification, Reed-Solomon Code, Universal Hash.

1 Introduction

Secret sharing scheme is a cryptographic primitive in which a secret is divided into shares and distributed among participants in such a way that only a qualified set of participants can recover the secret. It is a fundamental building block for many cryptographic protocols and is often used in the general composition of secure multiparty computations. Because of their importance in cryptography it has been studied actively for more than three decades since the seminal papers by Shamir [23] and Blakley [3].

Cheating prevention is one of the main topics in secret sharing schemes. Tompa and Woll first considered a secret sharing scheme capable of detecting the presence of cheating when invalid shares are submitted in the secret reconstruction phase [25]. For the problem of detecting cheating, the upper bound of the size of share and efficient constructions have been actively studied so far [1, 2, 6, 9, 16, 19].

Secret sharing schemes that not only detect the presence of cheating but also identify cheaters who submit invalid shares are also a hot topic in this area. Rabin and Ben-Or proposed a k-out-of-n secret sharing scheme capable of identifying cheaters [21]. The size of share $|\mathcal{V}_i|$ of their scheme is $|\mathcal{V}_i| = |\mathcal{S}|^{3n-2}$ where $|\mathcal{S}|$ denotes the size of secret[1]. In [12], Kurosawa, Obana and Ogata showed that when the number of cheater t satisfies $t \leq \lfloor (k-1)/3 \rfloor$ the share size is greatly reduced compared to that of [21]. The size of share of their scheme is $|\mathcal{V}_i| = |\mathcal{S}|/\epsilon^{t+2}$, which until now has been the most efficient scheme, despite the fact that the bit length of their scheme is still linear to the number of cheaters. The lower bound of share size is given by Kurosawa *et al.* as follows [12]:

$$|\mathcal{V}_i| \geq \frac{|\mathcal{S}| - 1}{\epsilon} + 1 \tag{1}$$

where ϵ denotes the successful cheating probability of cheaters. Though, the sizes of shares of all the existing schemes are far from the above bound.

In this paper, we first present efficient k-out-of-n threshold secret sharing schemes capable of identifying up to t cheaters under the condition $t \leq \lfloor (k-1)/3 \rfloor$. While this condition is the same as that of Kurosawa *et al.* [12], the share size is dramatically reduced compared to [12]. Namely, the share size of the first scheme satisfies $|\mathcal{V}_i| = |\mathcal{S}|/\epsilon$ and is only one bit longer than the bound of eq. (1). We also present a scheme with the desired property that the successful cheating probability of cheaters can be determined without regard to the size of the secret, which is not the case in the first scheme. Further, we present k-out-of-n threshold schemes capable of detecting up to t cheaters such that $t \leq \lfloor (k-2)/2 \rfloor$ and $t \leq \lfloor (k-1)/2 \rfloor$, respectively. The numbers of cheaters these two schemes can identify reach the theoretical limit when k is even and for any k, respectively. The sizes of share of the schemes can be approximately written by $|\mathcal{V}_i| \approx (n \cdot t \cdot 2^{3t-1} \cdot |\mathcal{S}|)/\epsilon$ and $|\mathcal{V}_i| \approx ((n \cdot t \cdot 2^{3t})^2 \cdot |\mathcal{S}|)/\epsilon^2$, respectively, which are also much smaller than that of Kurosawa *et al.* despite the difference of their cheater identifiabilities.

We note that secret sharing schemes against cheating are strongly related to secure message transmission schemes as mentioned in [11, 13]. Therefore, we believe that ideas used to construct proposed schemes will help to construct secure message transmission schemes.

The rest of the paper is organized as follows. In Section 2, we briefly review models of secret sharing schemes capable of identifying cheaters, and we discuss related work. In Section 3, we present almost optimum schemes which can identify up to $\lfloor (k-1)/3 \rfloor$ cheaters. In Sections 4 and 5, we give efficient schemes which can identify up to $\lfloor (k-2)/2 \rfloor$ cheaters and $\lfloor (k-1)/2 \rfloor$ cheaters, respectively. In Section 6, we summarize our work.

[1] Throughout the paper, we use notations $|\mathcal{X}|$ and $\mathtt{X}$ to denote the cardinality of a set $\mathcal{X}$ and a random variable over $\mathcal{X}$, respectively.

2 Preliminaries

2.1 Secret Sharing Schemes

In the model of secret sharing schemes, there are n participants $\mathcal{P} = \{P_1, \ldots, P_n\}$ and a dealer D. The model consists of two algorithms: $\mathsf{ShareGen}$ and $\mathsf{Reconst}$. The 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 participant P_i. In a usual setting, $\mathsf{ShareGen}$ is invoked by the dealer. The secret reconstruction algorithm $\mathsf{Reconst}$ takes a list of shares and outputs a secret $s \in \mathcal{S}$.

The set of participants who are allowed to reconstruct the secret is characterized by an *access structure* $\Gamma \subseteq 2^{\mathcal{P}}$; that is, participants $P_{i_1}, \ldots, P_{i_k}$ 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 $\Gamma = \{\mathcal{A} \mid \mathcal{A} \subseteq 2^{\mathcal{P}}, |\mathcal{A}| \geq k\}$.) 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 $\Pr[\mathtt{S} = s \mid \mathtt{V}_{i_1} = v_{i_1}, \ldots, \mathtt{V}_{i_k} = v_{i_k}] = \Pr[\mathtt{S} = s]$ for any $s \in \mathcal{S}$.

We note that only perfect secret sharing schemes are dealt with in this paper.

2.2 t-Cheater Identifiable Secret Sharing Schemes

A secret sharing scheme capable of identifying cheaters was first presented by Rabin and Ben-Or [21]. 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 they cannot be identified as cheaters in reconstructing the secret.

As with ordinary secret sharing schemes, this model consists of $\mathsf{ShareGen}$ and $\mathsf{Reconst}$. The share generation algorithm $\mathsf{ShareGen}$ is the same as that in the ordinary secret sharing schemes. Two types of secret reconstruction algorithms have been defined so far depending on whether identification of the cheater is done *privately* or *publicly*. We will use $\mathsf{Reconst}^{(\mathsf{pri})}$ and $\mathsf{Reconst}^{(\mathsf{pub})}$ to denote secret reconstruction algorithms which identify cheaters privately and publicly, respectively. A secret reconstruction algorithm $\mathsf{Reconst}^{(\mathsf{pri})}$ takes a share called a *base share* and a list of shares as input and outputs a pair of a secret and a set of cheaters; that is, if no cheater is identified $\mathsf{Reconst}^{(\mathsf{pri})}$ outputs a pair $(s, \emptyset)$ where s is a secret reconstructed. If $\mathsf{Reconst}^{(\mathsf{pri})}$ finds cheaters and the secret s can be reconstructed from valid shares submitted, it outputs (s, L) (where $s \in \mathcal{S}$ and $L \neq \emptyset$ is a set of cheaters submit invalid shares,) otherwise (i.e. if a secret cannot be reconstructed from valid shares,) it outputs $(\perp, L)$ where $\perp (\notin \mathcal{S})$ is a special symbol indicating that cheating was detected and, again, L is a set of cheaters. In $\mathsf{Reconst}^{(\mathsf{pri})}$, the base share becomes a basis for deciding whether a participant submitting a share to $\mathsf{Reconst}^{(\mathsf{pri})}$ is a cheater. On the other hand,

$\mathsf{Reconst}^{(\mathsf{pub})}$ identifies cheaters without a trusted share: it takes a list of shares as input and outputs a pair of a secret and a set of cheaters. We require that the algorithms $\mathsf{ShareGen}$ and $\mathsf{Reconst}$ satisfy the following *correctness* condition:

$$\Pr[(v_1,\ldots,v_n) \leftarrow \mathsf{ShareGen}(s);\ (\hat{s},L) \leftarrow \mathsf{Reconst}(v_{i_1},\ldots,v_{i_m}) : s = \hat{s} \wedge L = \emptyset] = 1$$

for any $s \in \mathcal{S}$, for any $i_1,\ldots,i_m$ such that $m \geq k$.

The security of the model can be formalized by the following simple game defined for any k-out-of-n threshold secret sharing scheme $\mathbf{SS} = (\mathsf{ShareGen}, \mathsf{Reconst})$ and for any (not necessarily polynomially bounded) Turing machine $\mathsf{A}^{(t)} = (\mathsf{A}_1^{(t)}, \mathsf{A}_2^{(t)})$, where $\mathsf{A}^{(t)}$ represents t cheaters $P_{i_1},\ldots,P_{i_t}$ who try to cheat honest participants $P_{i_{t+1}},\ldots,P_{i_m}$ where $m \geq k$.

$\mathsf{Game}(\mathbf{SS}, \mathsf{A}^{(t)})$
$s \leftarrow \mathcal{S}$; `// according to the probability distribution over` $\mathcal{S}$.
$(v_1,\ldots,v_n) \leftarrow \mathsf{ShareGen}(s)$;
$(i_1,\ldots,i_t) \leftarrow \mathsf{A}_1^{(t)}()$;
$(v'_{i_1},\ldots,v'_{i_t},i_{t+1},\ldots,i_m) \leftarrow \mathsf{A}_2^{(t)}(v_{i_1},\ldots,v_{i_t})$;

Cheaters P_{i_j} succeeds in cheating if $\mathsf{Reconst}$ fails to identify P_{i_j} as a cheater when a secret reconstructed is not identical to the original one. In the public model, we will denote successful cheating probability of P_{i_j} against $\mathbf{SS}^{(\mathsf{pub})}$ by $\epsilon(\mathbf{SS}^{(\mathsf{pub})}, \mathsf{A}^{(t)}, P_{i_j})$ where $\epsilon(\mathbf{SS}^{(\mathsf{pub})}, \mathsf{A}^{(t)}, P_{i_j})$ is define as follows:

$$\epsilon(\mathbf{SS}^{(\mathsf{pub})}, \mathsf{A}^{(t)}, P_{i_j}) = \Pr[(s',L) \leftarrow \mathsf{Reconst}^{(\mathsf{pub})}(v'_{i_1},\ldots,v'_{i_t},v_{i_{t+1}},\ldots,v_{i_k}) : i_j \notin L].$$

On the other hand, in the private model, successful cheating probability of P_{i_j} is defined for each P_ℓ submitting base share. Therefore, we will define such probability $\epsilon(\mathbf{SS}^{(\mathsf{pri})}, \mathsf{A}^{(t)}, P_{i_j}, P_{i_\ell})$ by

$$\begin{aligned}&\epsilon(\mathbf{SS}^{(\mathsf{pri})}, \mathsf{A}^{(t)}, P_{i_j}, P_{i_\ell})\\ &= \Pr[(s',L) \leftarrow \mathsf{Reconst}^{(\mathsf{pri})}(v_{i_\ell}, (v'_{i_1},\ldots,v'_{i_t},v_{i_{t+1}},\overset{v_{i_\ell}}{\ldots},v_{i_k})) : i_j \notin L]\end{aligned}$$

where the first argument v_{i_ℓ} of $\mathsf{Reconst}^{(\mathsf{pri})}$ denotes a base share. The probabilities are taken over the distribution of $\mathcal{S}$, and over the random tapes of $\mathsf{ShareGen}$ and $\mathsf{A}^{(t)}$. Note that the above game implicitly assumes *simultaneous secret reconstruction*; that is, all the participants submit their shares simultaneously to secret reconstruction algorithm in reconstructing the secret. Therefore, so-called "rushing adversary" who tries to forge its share *after* observing shares of honest participants is not allowed in this model.

Cheaters in this model can be classified into two classes: *non-critical cheaters* and *critical cheaters*. Non-critical cheaters only disclose their information to other cheaters or forge their shares in such a way that their forgeries do not cause the secret reconstruction algorithm to reconstruct a different secret from the original one. On the other hand, critical cheaters submit forged shares which cause the secret reconstruction algorithm to reconstruct a different secret from

the original one. In this paper we focus on identifying only critical cheaters since the goal of the cheaters in the models considered is to make other participants reconstruct an *invalid* secret. The formal definition of a critical cheater for public cheater identification models are given as follows:

Definition 1. *Let* $(v_1, \ldots, v_n)$ *be output of* $\mathsf{ShareGen}^{(\mathsf{pub})}(s)$. *A participants* P_j *who submit* v'_j *to* $\mathsf{Reconst}^{(\mathsf{pub})}$ *is called* a critical cheater *if and only if there exist* $i_1, i_2, \ldots, i_{k-1}$ *such that*

$$\Pr[(s', L) \leftarrow \mathsf{Reconst}^{(\mathsf{pub})}(v_{i_1}, \ldots, v_{i_{k-1}}, v'_j) : s' \neq s \wedge s' \in \mathcal{S}] \neq 0\,.$$

In the case of private cheater identification model, a critical cheater may vary according to a participant who submit base share.

Definition 2. *Let* $(v_1, \ldots, v_n)$ *be output of* $\mathsf{ShareGen}^{(\mathsf{pri})}(s)$. *A participants* P_j *who submit* v'_j *to* $\mathsf{Reconst}^{(\mathsf{pri})}$ *is called* a critical cheater against P_ℓ *if and only if there exist* $i_1, i_2, \ldots, i_{k-2}$ *such that*

$$\Pr[(s', L) \leftarrow \mathsf{Reconst}^{(\mathsf{pri})}(v_\ell, (v_{i_1}, \ldots, v_{i_{k-2}}, v'_j)) : s' \neq s \wedge s' \in \mathcal{S}] \neq 0\,.$$

Based on the above definition, we define the security of secret sharing schemes capable of identifying cheaters for both public and private models as follows:

Definition 3. *A* (k, n) *threshold secret sharing scheme* $\mathbf{SS}^{(\mathsf{pub})} = (\mathsf{ShareGen}^{(\mathsf{pub})}, \mathsf{Reconst}^{(\mathsf{pub})})$ *is called a* (t, ϵ) *cheater identifiable secret sharing scheme with public cheater identification if* $\epsilon(\mathbf{SS}^{(\mathsf{pub})}, \mathsf{A}^{(t)}, P_j) \leq \epsilon$ *for any* $\mathsf{A}^{(t)}$ *representing set of* t *or less cheaters* $\mathcal{P}$, *for any critical cheater* $P_j \in \mathcal{P}$.

Definition 4. *A* (k, n) *threshold secret sharing scheme* $\mathbf{SS}^{(\mathsf{pri})} = (\mathsf{ShareGen}^{(\mathsf{pri})}, \mathsf{Reconst}^{(\mathsf{pri})})$ *is called a* (t, ϵ) *cheater identifiable secret sharing scheme with private cheater identification if* $\epsilon(\mathbf{SS}^{(\mathsf{pri})}, \mathsf{A}^{(t)}, P_j, P_\ell) \leq \epsilon$ *for any* $\mathsf{A}^{(t)}$ *representing set of* t *or less cheaters* $\mathcal{P}$, *for any critical cheater* $P_i \in \mathcal{P}$ *and for any honest participant* P_ℓ.

We note that (t, ϵ) publicly cheater identifiable schemes for $\epsilon < 1$ exist only if $t \leq \lfloor (k-1)/2 \rfloor$ whereas $(k-1, \epsilon)$ cheater identifiable scheme with private cheater identification can be constructed. This is because cheaters can easily generate arbitrary number of consistent shares by invoking $\mathsf{ShareGen}$ with forged secret s' as input and distribute them among the cheaters in publicly cheater identifiable schemes. In this case, it is impossible to identify cheaters unless we can determine cheaters on a majority basis.

We also note that the model of (t, ϵ) cheater identifiable secret sharing scheme is different from that of the verifiable secret sharing (VSS for short) in the sense that the dealer is honest in the (t, ϵ) cheater identifiable secret sharing whereas the dealer may cheat in the VSS.

2.3 Related Work

In this subsection, we briefly review a known bound and constructions of (t, ϵ) cheater identifiable secret sharing schemes and related topics.

The capability to identify cheaters in secret sharing schemes was first pointed out by McEliece and Sarwate [15]. Namely, they observed that a list of shares of Shamir's (k, n) threshold secret sharing scheme constitutes a codeword of Reed-Solomon code. Therefore, if $k + 2t + 1$ shares containing up to t invalid shares are submitted in reconstructing a secret, the secret reconstruction algorithm can identify all cheaters with probability 1. However, this observation does not directly lead to constructing (t, ϵ) cheater identifiable secret sharing schemes since $k + 1$ or more shares are required to identify cheaters.

(t, ϵ) cheater identifiable (k, n) secret sharing scheme with private cheater identification are presented in various literature. Here, we will briefly review previous results. In [21, 22], Rabin and Ben-Or presented a scheme on which they constructed a verifiable secret sharing scheme. The property of their scheme can be summarized by the following proposition:

Proposition 1. [21, 22] *There exists $(k-1, \epsilon)$ cheater identifiable (k, n) threshold secret sharing scheme with private cheater identification with parameter $|\mathcal{S}| = p$, $\epsilon = 1/p$, and $|\mathcal{V}_i| = p^{3n-2}$ where p is a prime power.*

Carpentieri proposed a scheme in which the size of share is reduced compared to [21, 22]:

Proposition 2. [5] *There exists $(k-1, \epsilon)$ cheater identifiable (k, n) threshold secret sharing scheme with private cheater identification with parameter $|\mathcal{S}| = p$, $\epsilon = 1/p$, and $|\mathcal{V}_i| = p^{k+2(n-1)}$ where p is a prime power.*

Ogata and Kurosawa proposed an elegant scheme in which the size of share is independent of n:

Proposition 3. [18] *There exists $(k-1, \epsilon)$ cheater identifiable (k, n) threshold secret sharing scheme with private cheater identification with parameter $|\mathcal{S}| = p$, $\epsilon = (k-1)/(p-1)$, and $|\mathcal{V}_i| = p^{2k+1}$ where p is a prime power.*

We note that the schemes in [21, 22] (Proposition 1) and [5] (Proposition 2) are secure even when cheater *knows* shares of $n-1$ participants whereas the scheme in [18] (Proposition 3) ensures security against cheaters who know at most $k-1$ shares.

With respect to a scheme with public cheater identification, Kurosawa, Obana and Ogata presented an efficient scheme whose share size only depends on the maximum number of cheaters [12]. The properties of their scheme can be summarized as follows:

Proposition 4. [12] *If $t \leq \lfloor (k-1)/3 \rfloor$, there exists (t, ϵ) cheater identifiable (k, n) threshold secret sharing scheme with public cheater identification with parameter $|\mathcal{S}| = p$, $\epsilon = 1/q$ and $|\mathcal{V}_i| = p \cdot q^{t+2}$ where p, q are prime powers satisfying $q \geq n \cdot p - t$.*[2]

[2] though this limitation is not addressed in [12], it follows directly from Bush bound on orthogonal array of strength $t + 1$.

In [12], Kurosawa *et al.* also showed a lower bound of share size for (t, ϵ) cheater identifiable secret sharing schemes with both publicly and privately cheater identification as follows:

Proposition 5. [12] *The size of share for (t, ϵ) cheater identifiable (k, n) threshold secret sharing schemes is lower bounded by* $|\mathcal{V}_i| \geq \dfrac{|\mathcal{S}| - 1}{\epsilon} + 1$.

However, share sizes of existing schemes are far from the above bound. Therefore, it was not clear whether the above bound is tight.

3 Publicly Cheater Identifiable Schemes for $t \leq \lfloor \frac{k-1}{3} \rfloor$

In this section, we present two efficient (t, ϵ) cheater identifiable (k, n) threshold secret sharing schemes with public cheater identification under the condition $t \leq \lfloor (k-1)/3 \rfloor$. The first scheme is almost optimum with respect to the share size; that is, the bit length of shares of the scheme is only one bit longer than the lower bound of Proposition 5. The second scheme, even though the share size is slightly larger than the first scheme, possesses a particular merit in that the successful cheating probability of cheaters can be chosen without regard to the size of the secret, which is the case neither in the first scheme nor in the scheme of [12].

As with the scheme in [12], the proposed scheme uses Reed-Solomon code to identify cheaters. The major difference between the scheme in [12] and the proposed scheme is as follows. In [12], a share of each participant consists of (1) a share of Shamir's (k, n) secret sharing for a secret, (2) a share of Shamir's (t, n) secret sharing scheme for a key of strongly universal hash functions of strength $t + 1$ (please refer to [24] for the definition,) and (3) a hash value of (1) under the key (2). Here, Reed-Solomon code is used in (2) to make cheaters impossible to alter the value of the key, which is used to examine the validity of shares (as pointed out in [15], (t, n) secret sharing scheme is equivalent to codeword of generalized Reed-Solomon code). Since the size of key of the strongly universal hash function of strength $t + 1$ is as large as $1/\epsilon^{t+1}$ the share size of the scheme in [12] grows linear with the number of cheaters. On the other hand, a share of the proposed scheme only consists of (1) a share of Shamir's (k, n) secret sharing for a secret, and (2) a hash value of (1) computed by a strongly universal hash function of strength $t+1$. Interestingly, the key used to compute hash values is not explicitly shared among the participants but is recovered from the hash values in the secret reconstruction phase by utilizing the error correction capability of Reed-Solomon code. This is made possible by choosing a strongly universal hash family based on polynomials over a finite field. Since the size of hash value is equal to $1/\epsilon$ in the proposed scheme, we see that the share size $|\mathcal{V}_i|$ of the proposed scheme satisfies $|\mathcal{V}_i| = |\mathcal{S}|/\epsilon$, which is independent of any of k, n and t. The detailed description of the first scheme is given in the next subsection.

3.1 An Almost Optimum Scheme

The share generation algorithm ShareGen and the secret reconstruction algorithm Reconst of the first scheme are described as follows where p and q are prime powers such that $q \geq n \cdot p$ and $\psi : GF(p) \times \{1, \ldots, n\} \rightarrow GF(q)$ is an injective function (e.g. $\psi(x, y) = (y-1) \cdot p + x$ for prime numbers p, q.)

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

1. Generate a random polynomial $f_s(x) \in GF(p)[X]$ of degree $k-1$ such that $f_s(0) = s$.
2. Generate a random polynomial $C(x) \in GF(q)[X]$ of degree t.
3. Compute $v_i = (f_s(i), C(\psi(f_s(i), i)))$ and output $(v_1, \ldots, v_n)$.

Secret Reconstruction and Cheater Identification: On input a list of m ($\geq k$) shares $((v_{s,i_1}, v_{C,i_1}), \ldots, (v_{s,i_m}, v_{C,i_m}))$, the secret reconstruction algorithm Reconst output a secret or a list of identities of cheaters as follows.

1. Reconstruct $\hat{C}(x)$ from $(v_{C,i_1}, \ldots, v_{C,i_m})$ using an error correction algorithm of generalized Reed-Solomon Code (e.g. Berlekamp algorithm.)
2. Check if $v_{C,i_j} = \hat{C}(\psi(v_{s,i_j}, i_j))$ holds (for $1 \leq j \leq m$.) If $v_{C,i_j} \neq \hat{C}(\psi(v_{s,i_j}, i_j))$ then i_j is added to the list of cheaters L.
3. If $|L| \leq m - k$ then reconstruct $f_s(x)$ from (k or more) shares v_{i_j} such that $i_j \notin L$ using Lagrange interpolation, and output $(f_s(0), L)$ if $\deg(f_s) \leq k-1$, otherwise Reconst output $(\perp, L)$. Reconst also output $(\perp, L)$ if $|L| > m - k$ holds.

Security of the proposed scheme can be summarized by the following theorem.

Theorem 1. *If $t \leq \lfloor (k-1)/3 \rfloor$ then the proposed scheme is a (t, ϵ) cheater identifiable secret sharing scheme with public cheater identification such that*

$$|\mathcal{S}| = p, \quad \epsilon = 1/q, \quad q \geq n \cdot p, \quad |\mathcal{V}_i| = p \cdot q \ (= |\mathcal{S}|/\epsilon) .$$

Proof. First, we show that the scheme is perfect. It is well known that $v_{s,i_1}, \ldots, v_{s,i_k}$ do not reveal any information about the secret since each $v_{s,i}$ is a share of Shamir's k-out-of-n secret sharing scheme. Further, it is easy to see that the knowledge about $v_{C,i}$ does not leak any information about the secret since the polynomial $C(x)$ is completely independent of the secret s.

Next we show that the scheme is (t, ϵ) cheater identifiable. The following two facts are key to prove (t, ϵ) cheater identifiability of the scheme:

1. $(C(x_1), C(x_2), \ldots, C(x_k))$ is a codeword of the Reed-Solomon Code with minimum distance $k - t$. Therefore, if $k - t > 2t$ (i.e. $t \leq \lfloor (k-1)/3 \rfloor$) then $C(x)$ can be reconstructed even when t points are forged.

2. A family of functions $\{C(x) \mid C(x) \in GF(q)[X],\ \deg(C(x)) \leq t\}$ is a strong class of universal hash functions $GF(q) \to GF(q)$ with strength $t+1$; that is, the following equality holds for any distinct $x_1, \ldots, x_t, x_{t+1} \in GF(q)$ and for any $y_1, \ldots, y_t, y_{t+1} \in GF(q)$.

$$\Pr[C(x_{t+1}) = y_{t+1} \mid C(x_1) = y_1, \ldots, C(x_t) = y_t] = 1/q\,. \tag{2}$$

Without loss of generality, we can assume $P_1, \ldots, P_t$ are cheaters who cooperatively try to fool the other participants by forging (part of) their shares. Suppose that P_1 is a critical cheater who is told the values $v_2, \ldots, v_t$ (i.e. the shares of $P_2, \ldots, P_t$) and submits invalid share $v'_1 = (v'_{s,1}, v'_{C,1})$ such that $v'_{s,1} \neq v_{s,1}$. P_1 is not identified as a cheater only if he submits $v'_{C,1}$ such that $v'_{C,1} = C(\psi(v'_{s,1}, 1))$ since $\mathsf{Reconst}$ can recover the original $C(x)$ even when t shares are forged. Further, since $\{C(x) \mid C(x) \in GF(q)[X], \deg(C(x)) \leq t\}$ is a strong class of universal hash functions and $\psi(v'_{s,1}, 1)$ is different from any of $\psi(v_{s,i}, i)$ $(1 \leq i \leq t,)$ the following equation holds:

$$\Pr[C(\psi(v'_{s,1}, 1)) = v'_{C,1} \mid C(\psi(v_{s,i}, i)) = v_{C,i} \ \text{(for } 1 \leq i \leq t)] = 1/q$$

where the probability is taken over the random choice of $C(x)$. Since the above discussion holds for any critical cheater P_i $(1 \leq i \leq t,)$ we see that no critical cheater can succeed in cheating without being identified with probability better than $1/q$. □

It should be noted that the size of share of the proposed scheme is independent of any of n, k and t, though, there is an implicit limitation on the parameter that $\epsilon < 1/(n \cdot |\mathcal{S}|)$ must holds. This is similar limitation of Shamir's secret sharing scheme which implicitly requires $|\mathcal{S}| > n$.

3.2 A Scheme with Flexible Parameter Choice

As we noted in the previous section, there is such a limitation in the first scheme that the successful cheating probability of cheaters must be smaller than $\frac{1}{n \cdot |\mathcal{S}|}$. This limitation is not desirable, especially when we want to share a secret with large size. Consider the situation in which we want to share a 1M bit secret (i.e. $|\mathcal{S}| = 2^{2^{20}}$,) with the first scheme. In this case, the share size becomes as large as 2M bit with a security level of $\epsilon < 1/2^{2^{20}}$ whereas $\epsilon = 1/2^{128}$ will be sufficient in real life. The second scheme is useful in such a situation since the successful cheating probability of cheaters can be chosen without regard to the size of the secret and the share size can be made reasonable in the second scheme. For example, when we share a 1M bit secret with the second scheme with $\epsilon = 1/2^{128}$, the share size is only (1M+282) bit.

The basic idea of the second scheme is same as the first scheme. We introduce the following trick to the first scheme so that we can determine $|\mathcal{S}|$ and ϵ flexibly. In the first scheme, the random polynomial $C(x)$ must be chosen from $GF(q)[X]$ such that $q \geq n \cdot |\mathcal{S}|$ in order to ensure $\psi(v_i, i) \neq \psi(v_j, j)$ for any distinct (i, v_i) and (j, v_j), which causes $\epsilon \leq \frac{1}{n \cdot |\mathcal{S}|}$. In the second scheme, we introduce

almost universal hash function (e.g. [24]) $\phi_e : \mathcal{S} \to GF(p)$ (where $\mathcal{S} = GF(p^N)$) and modify the input of $C(x)$ ($C_s(x)$ in the second scheme) to $\psi(\phi_e(v_i), i)$ where $\psi : GF(p) \times \{1 \ldots, n\}$ is an injective function. The use of ϕ_e allows $\psi(\phi_e(v_i), i) = \psi(\phi_e(v_i'), i)$ with small probability, though, the limitation of $\epsilon < \frac{1}{n \cdot |\mathcal{S}|}$ can be eliminated since the range of ϕ_e is chosen flexibly by choosing the parameter p, N and introduce a universal hash family $\phi_e(x_0, \ldots, x_{N-1}) = \sum_{i=0}^{N-1} x_i \cdot e^i$ defined over $GF(p)$. The share generation algorithm and the secret reconstruction algorithm of the second scheme are described as follows:

Share Generation: On input a secret $(s_0, \ldots, s_{N-1}) \in GF(p^N)$, the share generation algorithm ShareGen outputs a list of shares $(v_1, \ldots, v_n)$ as follows:

1. Generate a random polynomial $f_s(x) \in GF(p^N)[X]$ of degree $k-1$ such that $f_s(0) = s$.
2. Generate $e \in GF(p)$ randomly and construct a random polynomial $C_e(x) \in GF(p)[X]$ of degree t such that $C_e(0) = e$.
3. Generate random polynomials $C_s(x) \in GF(q)[X]$ of degree t such that $q \geq n \cdot p$.
4. Compute $v_{s,i} = (v_{s,i,0}, \ldots, v_{s,i,N-1}) = f_s(i)$ where $v_{s,i,j} \in GF(p)$ (for $0 \leq j \leq N-1$), $v_{C_e,i} = C_e(i)$ and $v_{C_s,i} = C_s(\psi(\sum_{j=0}^{N-1} v_{s,i,j} \cdot e^j, i))$.
5. Compute $v_i = (v_{s,i}, v_{C_e,i}, v_{C_s,i})$ and output $(v_1, \ldots, v_n)$.

Secret Reconstruction and Cheater Identification: On input a list of m ($m \geq k$) shares $((v_{s,i_1}, v_{C_e,i_1}, v_{C_s,i_1}), \ldots, (v_{s,i_m}, v_{C_e,i_m}, v_{C_s,i_m}))$ the secret reconstruction algorithm Reconst outputs a secret or a list of identities of cheaters as follows.

1. Reconstruct $\hat{C}_s(x)$ and $\hat{C}_e(x)$ from $(v_{C_s,i_1}, \ldots, v_{C_s,i_m})$ and $(v_{C_e,i_1}, \ldots, v_{C_e,i_m})$, respectively using an error correction algorithm of Reed-Solomon code.
2. Check if $v_{C_e,i_j} = \hat{C}_e(i_j)$ (for $1 \leq j \leq m$.) If $v_{C_e,i_j} \neq \hat{C}_e(i_j)$ then i_j is added to the list of cheaters L.
3. Compute $\hat{e} = \hat{C}_e(0)$.
4. Check if $v_{C_s,i_j} = \hat{C}_s(\psi(\sum_{\ell=0}^{N-1} v_{s,i_j,\ell} \cdot \hat{e}^\ell, i_j))$ holds (for $1 \leq j \leq m$.) i_j is added to the list of cheaters L if this is not the case.
5. If $|L| \leq m - k$ then reconstruct $f_s(x)$ from (k or more) shares v_{i_j} such that $i_j \notin L$ using Lagrange interpolation, and output $(f_s(0), L)$ if $\deg(f_s) \leq k-1$, otherwise Reconst output $(\perp, L)$. Reconst also output $(\perp, L)$ if $|L| > m - k$ holds.

Security of the proposed scheme can be summarized by the following theorem. Note that the successful cheating probability ϵ can be chosen without regard to $|\mathcal{S}|$ by selecting the value of p appropriately.

Theorem 2. *If $t \leq \lfloor (k-1)/3 \rfloor$ then the proposed scheme is a (t, ϵ) cheater identifiable secret sharing scheme with public cheater identification such that*

$$|\mathcal{S}| = p^N, \quad \epsilon = (N-1)/p + 1/q \leq N/p, \quad q \geq n \cdot p, \quad |\mathcal{V}_i| = p^{N+1} \cdot q\,.$$

Proof. As in the proof of Theorem 1, we can assume $P_1, \ldots, P_t$ are cheaters who cooperatively try to fool the other participants by forging (part of) their shares. Suppose that P_1 is a critical cheater who submits invalid share $v'_1 = (v'_{s,1}, v'_{C_e,1}, v'_{C_s,1})$ such that $v'_{s,1} \neq v_{s,1}$. Since $(v_{C_e,i_1}, \ldots, v_{C_e,i_m})$ is a codeword of Reed-Solomon Code capable of correcting up to t errors, t cheaters cannot alter the value of e. Therefore, P_1 is not identified as a cheater only if he submits $(v'_{s,1}, v'_{C_e}, v'_{C_s,1})$ such that $v'_{C_s,1} = C_s(\psi(\sum_{\ell=0}^{N-1} v'_{s,i,\ell} \cdot e^\ell, 1))$ where e is uniformly and randomly distributed over $GF(p)$. There are two cases to consider in computing such probability. In the first case suppose that P_1 forged its share in a way that $v'_{C_s,1} \neq v_{C_s,1}$. In this case, successful cheating probability ϵ_1 of P_1 who knows that $v_{C_s,i} = C_s(\psi(\sum_{\ell=0}^{N-1} v_{s,i,\ell} \cdot e^\ell, i))$ hold for $1 \leq i \leq t$ is computed as follows (for simplicity we will denote $\sum_{\ell=0}^{N-1} v_{s,i,\ell} \cdot e^\ell$ by $\phi_e(v_{s,i})$.)

$$
\begin{aligned}
\epsilon_1 &= \Pr[v'_{C_s,1} = C_s(\psi(\phi_e(v'_{s,1}), 1)) \mid v_{C_s,i} = C_s(\psi(\phi_e(v_{s,i}), i)) \ \text{(for } 1 \leq i \leq t)] \\
&= \Pr[\phi_e(v_{s,i}) \neq \phi_e(v'_{s,i})] \\
&\quad \cdot \Pr\left[v'_{C_s,1} = C_s(\psi(\phi_e(v'_{s,1}), 1)) \,\middle|\, \begin{array}{c} v_{C_s,i} = C_s(\psi(\phi_e(v_{s,i}), i)) \ \text{(for } 1 \leq i \leq t), \\ \phi_e(v_{s,i}) \neq \phi_e(v'_{s,i}) \end{array} \right] \\
&\leq 1/q
\end{aligned}
$$

where the last inequality directly follows from the fact that $\{C_s\}$ is a family of a strong class of strongly universal hash function with strength $t+1$ (see the proof of Theorem 1 for details.)

Next we consider the second case in which P_1 forged its share in a way that $v'_{C_s,1} = v_{C_s,1}$ holds. In this case ϵ_1 is computed as follows.

$$
\begin{aligned}
\epsilon_1 &= \Pr[v'_{C_s,1} = C_s(\psi(\phi_e(v'_{s,1}), 1)) \mid v_{C_s,i} = C_s(\psi(\phi_e(v_{s,i}), i)) \ \text{(for } 1 \leq i \leq t)] \\
&= \Pr[\phi_e(v_{s,i}) = \phi_e(v'_{s,i})] + \Pr[\phi_e(v_{s,i}) \neq \phi_e(v'_{s,i})] \\
&\quad \cdot \Pr\left[v'_{C_s,1} = C_s(\psi(\phi_e(v'_{s,1}), 1)) \,\middle|\, \begin{array}{c} v_{C_s,i} = C_s(\psi(\phi_e(v_{s,i}), i)) \ \text{(for } 1 \leq i \leq t), \\ \phi_e(v_{s,i}) \neq \phi_e(v'_{s,i}) \end{array} \right] \\
&\leq \Pr[\phi_e(v_{s,i}) = \phi_e(v'_{s,i})] + 1/q \ \leq \ (N-1)/p + 1/q
\end{aligned}
$$

where the last two inequalities follows from the property of a strong class of universal hash functions and the well-known fact that a polynomial of degree $N-1$ (e.g. ϕ_e) has at most $N-1$ roots. It is easy to see that the successful cheating probability of any critical cheater is upper bounded by N/p since $(N-1)/p + 1/q \leq N/p$ holds. □

Note that the bit length of shares $\log |\mathcal{V}_i|$ is approximately $\log |\mathcal{S}| + 2\log(1/\epsilon) + 2\log\log|\mathcal{S}|$ in the above scheme. Therefore, we can determine size of the secret and successful cheating probability flexibly only by paying $\log(1/\epsilon) + 2\log\log|\mathcal{S}|$ additional bits compared to the bound.

4 A Publicly Cheater Identifiable Scheme for $t \leq \lfloor \frac{k-2}{2} \rfloor$

In this section we show that we can construct a very efficient publicly cheater identifiable scheme even when the number of cheaters t does not satisfy $t \leq \lfloor (k-1)/3 \rfloor$. More precisely, we present a publicly cheater identifiable scheme whose secret reconstruction algorithm can catch up to $\lfloor (k-2)/2 \rfloor$ cheaters. We note that the cheater identifiability of the scheme is nearly optimum since $t = \lfloor (k-1)/2 \rfloor$ is the theoretical upper bound for public cheater identification. Furthermore, the size of share $|\mathcal{V}_i|$ of the proposed scheme is much smaller than that of [12] despite the difference of their cheater identifiabilities.

The share generation algorithm of the proposed scheme is exactly the same as the one presented in §3.1. To identify more than $(k-1)/3$ cheaters, the secret reconstruction algorithm examines the *consistency* of all the possible $\binom{k}{t+2}$ subsets of k shares input to the algorithm. Here, the consistency of $t+2$ shares (v_{s,i_j}, v_{C,i_j}) $(1 \leq j \leq t+2)$ is examined by verifying whether $t+2$ points $(\psi(v_{s,i_j}, i_j), v_{C,i_j})$ $(1 \leq j \leq t+2)$ lie on a polynomial of degree t. The intuition behind the idea is as follows. Suppose t cheaters try to fool the reconstruction algorithm by forging their shares. Since we assume $t \leq \lfloor (k-2)/2 \rfloor$, there are at least $t+2$ unforged shares input to the reconstruction algorithm. Therefore, we can guarantee that (1) there exists at least one subset of consistent shares of size $t+2$ (i.e. shares which does not contain a forged share,) and (2) any subsets of size $t+2$ contain at least two unforged shares. We will make use of these facts to catch cheaters since $t+2$ shares containing both forged and unforged shares can be consistent only with very low probability. The detailed description of the proposed reconstruction algorithm is described as follows.

Secret Reconstruction and Cheater Identification for $t \leq \lfloor (k-2)/2 \rfloor$: On input a list of $m (\geq k)$ shares $((v_{s,i_1}, v_{C,i_1}), \ldots, (v_{s,i_m}, v_{C,i_m}))$, the secret reconstruction algorithm $\mathsf{Reconst}$ output a secret or a list of identities of cheaters as follows.

1. If $t \leq (m-1)/3$ holds, outputs $(s, L) \leftarrow \mathsf{Reconst}^{(3t+1)}((v_{s,i_1}, v_{C,i_1}), \ldots, (v_{s,i_m}, v_{C,i_m}))$, where $\mathsf{Reconst}^{(3t+1)}$ denotes the secret reconstruction algorithm for $t \leq \lfloor (k-1)/3 \rfloor$ (i.e. $\mathsf{Reconst}$ presented in §3.1.)
2. Otherwise, let $L \leftarrow \{i_1, \ldots, i_m\}$ and repeat the following steps 2a–2b for all subsets $\mathcal{I} \subseteq \{i_1, \ldots, i_m\}$ such that $|\mathcal{I}| = t+2$.
   (a) Compute $c_{\mathcal{I}}$ by $c_{\mathcal{I}} = \sum_{i \in \mathcal{I}} v_{C,i} \cdot \prod_{\substack{j \in \mathcal{I} \\ j \neq i}} \frac{1}{\psi(v_{s,i}, i) - \psi(v_{s,j}, j)}$, where $c_{\mathcal{I}}$ is the coefficient of x^{t+1} of the polynomial $C(x)$ constructed from the $t+2$ points $(\psi(v_{s,i}, i), v_{C,i})$ $(i \in \mathcal{I}.)$
   (b) If $c_{\mathcal{I}} = 0$ holds, then $L \leftarrow L \setminus \mathcal{I}$ (i.e. remove $\mathcal{I}$ from the list of cheaters.) Note that $c_{\mathcal{I}} = 0$ holds if all of $t+2$ shares are unforged since we choose random polynomial $C(x)$ of degree t in the share generation algorithm.
3. If $|L| \leq m-k$ holds then reconstruct $f_s(x)$ from (k or more) shares v_{s,i_j} such that $i_j \notin L$ using Lagrange interpolation, and output $(f_s(0), L)$ if $\deg(f_s) \leq k-1$, otherwise $\mathsf{Reconst}$ output $(\perp, L)$. $\mathsf{Reconst}$ also output $(\perp, L)$ if $|L| > m-k$ holds.

Security of the proposed scheme can be summarized by the following theorem.

Theorem 3. *If $t \leq \lfloor (k-2)/2 \rfloor$ then the proposed scheme is a (t, ϵ) cheater identifiable secret sharing scheme with public cheater identification such that*

$$|\mathcal{S}| = p, \quad \epsilon = \frac{(t+1) \cdot 2^{3t-1}}{p}, \quad q \geq n \cdot p, \quad |\mathcal{V}_i| = p \cdot q \ (\approx \tfrac{n \cdot (t+1) \cdot 2^{3t-1} \cdot |\mathcal{S}|}{\epsilon}) .$$

Proof. As in the proof of Theorem 1, we can assume $P_1, \ldots, P_t$ are cheaters who cooperatively try to fool the other participants $P_{t+1}, \ldots, P_m$ by forging (part of) their shares. Suppose that P_1 is a critical cheater who submits invalid share $v'_1 = (v'_{s,1}, v'_{C,1})$ such that $v'_{s,1} \neq v_{s,1}$. We will show that the probability that the successful cheating probability of P_1 is upper bounded by ϵ $(= \frac{(t+1) \cdot 2^{3t-1}}{p})$.

From the proof of Theorem 1, it is easy to see that, if $t \leq (m-1)/3$ holds, the successful cheating probability of P_1 is upper bounded by $q (< \epsilon)$ since we can apply error correction algorithm of the generalized Reed-Solomon codes to $(v'_{C,1}, \ldots, v'_{C,t}, v_{C,t+1}, \ldots, v_{C,m})$.

Now we will show the proposed reconstruction algorithm can catch cheaters with probability better than $1 - \epsilon$ even against $t > (k-1)/3$ cheaters. It suffices to show that the probability that there exists at least one subset $\mathcal{I} \subseteq \{1, \ldots, m\}$ such that (1) $1 \in \mathcal{I}$, (2) $|\mathcal{I}| = t+2$, and (3) $c_{\mathcal{I}} = 0$, is lower bounded by ϵ.

Toward showing the above, we will first show that the probability $\epsilon(\mathcal{I})$ that $c_{\mathcal{I}} = 0$ holds for given $\mathcal{I}$ is lower bounded by $(t+1)/p$ for any $\mathcal{I}$ such that $1 \in \mathcal{I}$ and $|\mathcal{I}| = t+2$. Without loss of generality, we can assume $\mathcal{I} = \{\ell_1, \ell_2, \ldots, \ell_{t+2}\}$ and $P_{\ell_1} \ldots, P_{\ell_{t'}}$ $(t' \leq t)$ are cheaters.

To evaluate $\epsilon(\mathcal{I})$, we will analyze the structure of $c_{\mathcal{I}}$. Here, we will use the notation ψ_i to denote $\psi(v_{s,i}, i)$ and the notation X' to indicate the variable X is owned and controlled by the cheaters.

$$c_{\mathcal{I}} = \sum_{\ell_i \in \mathcal{I}} v_{C,\ell_i} \cdot \prod_{\substack{\ell_j \in \mathcal{I} \\ j \neq i}} \frac{1}{\psi_{\ell_i} - \psi_{\ell_j}} = \sum_{i=1}^{t'} v'_{C,\ell_i} \cdot \prod_{\substack{j=1 \\ j \neq i}}^{t'} \frac{1}{\psi'_{\ell_i} - \psi'_{\ell_j}} \prod_{j=t'+1}^{t+2} \frac{1}{\psi'_{\ell_i} - \psi_{\ell_j}}$$
$$+ \sum_{j=t'+1}^{t+2} v_{C,\ell_j} \cdot \prod_{i=1}^{t'} \frac{1}{\psi_{\ell_j} - \psi'_{\ell_i}} \prod_{\substack{i=t'+1 \\ i \neq j}}^{t+2} \frac{1}{\psi_{\ell_j} - \psi_{\ell_i}}$$

We will rewrite $v'_{C,\ell_i} \cdot \prod_{j=1, j \neq i}^{t'} \frac{1}{\psi'_{\ell_i} - \psi'_{\ell_j}}$ by A_i where each A_i is determined by the shares submitted by the cheaters and is known to the cheaters. Furthermore, to make the proof clearer, we replace $v_{C,i}$ by $C(\psi_i)$ where $C(x)$ is a polynomial chosen by the dealer in the share generation phase.

$$c_{\mathcal{I}} = \sum_{i=1}^{t'} A_i \cdot \prod_{j=t'+1}^{t+2} \frac{1}{\psi'_{\ell_i} - \psi_{\ell_j}} + \sum_{j=t'+1}^{t+2} C(\psi_{\ell_j}) \cdot \prod_{i=1}^{t'} \frac{1}{\psi_{\ell_j} - \psi'_{\ell_i}} \prod_{\substack{i=t'+1 \\ i \neq j}}^{t+2} \frac{1}{\psi_{\ell_j} - \psi_{\ell_i}} \quad (3)$$

With the knowledge about shares owned by the cheaters, the number of possible candidates for $(\psi_{\ell_{t'+1}}, \ldots, \psi_{\ell_{t+2}}, C)$ becomes $p^{t-t'+2} \times q^{t-t'+1}$ since (1) ψ_{ℓ_i} $(t' +$

$1 \le i \le t+2$) look randomly, uniformly and independently distributed over the set $\Psi_{\ell_i} = \{\psi(v_{s,\ell_i}, \ell_i) \mid v_{s,\ell_i} \in GF(p)\}$ even with the knowledge of cheaters, and (2) $(\psi_{\ell_{t'+1}}, v_{C,\ell_{t'+1}}), \ldots, (\psi_{\ell_{t+1}}, v_{C,\ell_{t+1}})$ uniquely determines the polynomial $C(x)$.

Now, we will estimate the upper bound of the number of $(\psi_{\ell_{t'+1}}, \ldots, \psi_{\ell_{t+2}}, C)$ with which $c_{\mathcal{I}} = 0$. For any fixed $(\psi_{\ell_{t'+1}}, \ldots, \psi_{\ell_{t+1}}, C) = (\hat{\psi}_{\ell_{t'+1}}, \ldots, \hat{\psi}_{\ell_{t+1}}, \hat{C})$, eq (3) is rewritten as follows:

$$c_{\mathcal{I}} = \sum_{i=1}^{t'} \frac{\hat{A}_i}{\psi'_{\ell_i} - \psi_{\ell_{t+2}}} + \sum_{j=t'+1}^{t+1} \frac{\hat{B}_j}{\hat{\psi}_{\ell_j} - \psi_{\ell_{t+2}}} + \hat{C}(\psi_{t+2}) \cdot \prod_{i=1}^{t'} \frac{1}{\psi_{\ell_{t+2}} - \psi'_{\ell_i}} \prod_{i=t'+1}^{t+1} \frac{1}{\psi_{\ell_{t+2}} - \hat{\psi}_{\ell_i}}$$

where $\hat{A}_i = A_i \cdot \prod_{j=t'+1}^{t+1} \frac{1}{\psi'_{\ell_i} - \hat{\psi}_{\ell_j}}$, $\hat{B}_j = \hat{C}(\hat{\psi}_{\ell_j}) \cdot \prod_{i=1}^{t'} \frac{1}{\hat{\psi}_{\ell_j} - \psi'_{\ell_i}} \cdot \prod_{i=t'+1}^{t+1} \frac{1}{\hat{\psi}_{\ell_j} - \hat{\psi}_{\ell_i}}$ are constant once ψ'_{ℓ_i} $(1 \le i \le t')$, $\hat{\psi}_{\ell_j}$ $(t'+1 \le j \le t+1)$, and $\hat{C}$ are fixed. It is easy to see that there are at most $t+1$ values of $\psi_{\ell_{t+2}}$ with which $c_{\mathcal{I}} = 0$. Therefore, the upper bound of the number of zeros of eq. (3) can be evaluated as follows:

$$\begin{aligned}
&|\{(\psi_{\ell_{t'+1}}, \ldots, \psi_{\ell_{t+2}}, C) \mid c_{\mathcal{I}} = 0 \text{ holds}\}| \\
&\le |\{(\psi_{\ell_{t'+1}}, \ldots, \psi_{\ell_{t+1}}) \mid \psi_{\ell_i} \in \Psi_{\ell_i} \ (t'+1 \le i \le t+1)\}| \\
&\quad \times |\{C(x) \mid C(\psi_{\ell_i}) = v_{C,\ell_i} \ (1 \le i \le t')\}| \times (t+1) \ = \ p^{t-t'+1} \cdot q^{t-t'+1} \cdot (t+1)
\end{aligned}$$

Therefore, the lower bound of $\epsilon(\mathcal{I})$ is given as follows: $\epsilon(\mathcal{I}) \le \frac{p^{t-t'+1} \cdot q^{t-t'+1} \cdot (t+1)}{p^{t-t'+2} \cdot q^{t-t'+1}} = (t+1)/p$.

From the above inequality and the fact that the number of subsets $\mathcal{I}$ of $\{1, \ldots, 3t\}$ such that $1 \in \mathcal{I}$ and $|\mathcal{I}| = t+2$ is equal to $\binom{3t-1}{t+1}$, the successful cheating probability ϵ is given as follows:

$$\begin{aligned}
&\epsilon = \Pr[\text{there exists } \mathcal{I} \text{ such that } c_{\mathcal{I}} = 0,\ 1 \in \mathcal{I},\ |\mathcal{I}| = t+2] \\
&\le \sum_{\left\{\mathcal{I} \middle| \substack{1 \in \mathcal{I}, \\ |\mathcal{I}| = t+2}\right\}} \epsilon(\mathcal{I}) \ = \ \left|\left\{\mathcal{I} \middle| \begin{matrix} 1 \in \mathcal{I}, \\ |\mathcal{I}| = t+2 \end{matrix}\right\}\right| \cdot \epsilon(\mathcal{I}) \ \le \ \binom{3t-1}{t+1} \cdot \frac{t+1}{p} \ \le \ \frac{(t+1) \cdot 2^{3t-1}}{p}
\end{aligned}$$

The size of share satisfies $|\mathcal{V}_i| = p \cdot q$ and is approximately written by $|\mathcal{V}_i| \approx \frac{n \cdot (t+1) \cdot 2^{3t-1} |\mathcal{S}|}{\epsilon}$ since $q \approx n \cdot p$ and $p \le \frac{(t+1) \cdot 2^{3t-1}}{\epsilon}$. □

Though size of share grows exponentially with the number of cheaters, the size of share is much smaller compared to Kurosawa *et al.* [12] whose size of share is as large as $|\mathcal{S}|/\epsilon^{t+2}$ (note that $\frac{1}{\epsilon} \gg 2$.) Even compared to the theoretical lower bound of eq. (1), the bit length of the proposed scheme is only $3t + \log t + \log n$ bit longer. On the other hand, the drawback of the proposed reconstruction algorithm is its computational inefficiency. In fact the reconstruction algorithm

requires to compute Lagrange interpolation $\binom{3t}{t+2}$ times to identify cheaters. However, in the usual setting, the cheater identification of the proposed scheme is still feasible. Consider, for example, the situation where we want to catch up to 10 cheaters (i.e. $t = 10$). The number of Lagrange interpolation we have to invoke is $\binom{30}{12} = 4,118,725$, which is indeed feasible even by the current personal computer.

We should note that the similar (brute force search) technique can be applied to the scheme given in the section §3.2.

5 A Publicly Cheater Identifiable Scheme for $t \leq \lfloor \frac{k-1}{2} \rfloor$

The scheme presented in Section 4 meets the theoretical upper bound $t = \lfloor (k-1)/2 \rfloor$ on number of cheaters that a scheme can identify *when the threshold k is even.* This is because $\lfloor (k-2)/2 \rfloor = \lfloor (k-1)/2 \rfloor$ holds for even k. When k is odd, on the other hands, the scheme will fail to catch $\lfloor (k-1)/2 \rfloor (> \lfloor (k-2)/2 \rfloor)$ cheaters. In this section we present a publicly cheater identifiable scheme which can catch $\lfloor (k-1)/2 \rfloor$ cheaters. The size of shares $|\mathcal{V}_i|$ of the proposed scheme is not so small as the scheme for $t \leq \lfloor (k-2)/2 \rfloor$, though, the size of shares of the scheme is still much smaller than that of [12].

Here, we will review the scheme presented in the previous section to explain the idea behind the proposed scheme for $t \leq \lfloor (k-1)/2 \rfloor$. The reconstruction algorithm of the scheme for $t \leq \lfloor (k-2)/2 \rfloor$ identifies cheaters by checking the degree of the polynomial reconstructed from $t+2$ points. Using this technique, it can be ensured that (1) $t+2$ points containing forged share cannot construct a polynomial with degree less than or equal to t and, (2) $t+2$ points containing no forged share construct a polynomial with degree less than or equal to t. Unfortunately, we cannot apply this technique when $t = \lfloor (k-1)/2 \rfloor$ since any $t+2$ shares contain at least one forged share and we cannot find set of honest shares (and, therefore, cannot identify cheaters correctly.)

To make it possible to find honest shares by examining consistency of $t+1$ shares, a share v_i of the proposed scheme consists of $v_i = (v_{s,i}, v_{C_0,i}, v_{C_1,i})$ where $v_{s,i}$ is a share of Shamir's k-out-of-n scheme and $v_{C_0,i}, v_{C_1,i}$ are the points on the polynomials $C_0(x) = \sum_{i=0}^{t} a_{0,i}x^i$ and $C_1(x) = \sum_{i=0}^{t} a_{1,i}x^i$ such that $a_{0,0} = a_{1,t}$. Then we can verify the consistency of $t+1$ shares by examining the equality $\hat{a}_{0,t} = \hat{a}_{1,t}$ where $\hat{a}_{0,0}$ and $\hat{a}_{1,t}$ are coefficients of x^0 and x^t of polynomials $\hat{C}_0$ and $\hat{C}_1$, respectively, where $\hat{C}_0$ and $\hat{C}_1$ are polynomials reconstructed from $t+1$ shares. Since an additional element (i.e. $v_{C_1,i}$) is required in the proposed scheme, the size of share is larger than that of the scheme for $t \leq \lfloor (k-2)/2 \rfloor$.

The share generation algorithm ShareGen and the secret reconstruction algorithm Reconst of the proposed scheme are described as follows where p and q are prime powers such that $q \geq n \cdot p$ and $\psi : GF(p) \times \{1, \ldots, n\} \to GF(q)$ is an injective function.

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

1. Generate a random polynomial $f_s(x) \in GF(p)[X]$ of degree $k-1$ such that $f_s(0) = s$.
2. Generate random polynomials $C_0(x) = \sum_{i=0}^{t} a_{0,i}x^i, C_1(x) = \sum_{i=0}^{t} a_{1,i}x^i \in GF(q)[X]$ such that the $a_{0,0} = a_{1,t}$.
3. Compute $v_i = (f_s(i), C_0(\psi(f_s(i), i)), C_1(\psi(f_s(i), i)))$ and output $(v_1, \ldots, v_n)$.

Secret Reconstruction and Cheater Identification: On input a list of m ($\geq k$) shares $((v_{s,i_1}, v_{C_0,i_1}, v_{C_1,i_1}), \ldots, (v_{s,i_m}, v_{C_0,i_m}, v_{C_1,i_m}))$, the secret reconstruction algorithm $\mathsf{Reconst}$ output a secret or a list of identities of cheaters as follows.

1. If $t \leq \lfloor (m-1)/3 \rfloor$ holds, outputs $(s, L) \leftarrow \mathsf{Reconst}^{(3t+1)}((v_{s,i_1}, v_{C_0,i_1}), \ldots, (v_{s,i_m}, v_{C_0,i_m}))$, where $\mathsf{Reconst}^{(3t+1)}$ denotes the secret reconstruction algorithm for $t \leq \lfloor (k-1)/3 \rfloor$ (i.e. $\mathsf{Reconst}$ presented in §3.1.)
2. Otherwise, let $L \leftarrow \{i_1, \ldots, i_m\}$ and repeat the following steps 2a–2b for all subsets $\mathcal{I} \subseteq \{i_1, \ldots, i_m\}$ such that $|\mathcal{I}| = t+1$.
   (a) Compute $a_{\mathcal{I},0}$ and $a_{\mathcal{I},1}$ as follows:

$$a_{\mathcal{I},0} = \sum_{\ell \in \mathcal{I}} v_{C_0,\ell} \cdot \prod_{\substack{j \in \mathcal{I} \\ j \neq \ell}} \frac{-\psi(v_{s,j}, j)}{\psi(v_{s,\ell}, \ell) - \psi(v_{s,j}, j)}$$
$$a_{\mathcal{I},1} = \sum_{\ell \in \mathcal{I}} v_{C_1,\ell} \cdot \prod_{\substack{j \in \mathcal{I} \\ j \neq \ell}} \frac{1}{\psi(v_{s,\ell}, \ell) - \psi(v_{s,j}, j)}$$

   where $a_{\mathcal{I},0}$ and $a_{\mathcal{I},1}$ are coefficients of x^0 and x^t of the polynomials $C_0(x)$ and $C_1(x)$ constructed from the $t+1$ points $(\psi(v_{s,i}, i), v_{C_0,i})$ $(i \in \mathcal{I})$ and $(\psi(v_{s,i}, i), v_{C_1,i})$ $(i \in \mathcal{I})$, respectively.
   (b) If $a_{\mathcal{I},0} = a_{\mathcal{I},1}$ holds then $L \leftarrow L \setminus \mathcal{I}$ (i.e. remove $\mathcal{I}$ from the list of cheaters.)
3. If $|L| \leq m-k$ holds then reconstruct $f_s(x)$ from (k or more) shares v_{s,i_j} such that $i_j \notin L$ using Lagrange interpolation, and output $(f_s(0), L)$ if $\deg(f_s) \leq k-1$, otherwise $\mathsf{Reconst}$ output $(\perp, L)$. $\mathsf{Reconst}$ also output $(\perp, L)$ if $|L| > m-k$ holds.

Security of the proposed scheme can be summarized by the following theorem.

Theorem 4. *If $t \leq \lfloor (k-1)/2 \rfloor$ then the proposed scheme is a (t, ϵ) cheater identifiable secret sharing scheme with public cheater identification such that*

$$|\mathcal{S}| = p, \quad \epsilon = \frac{t \cdot 2^{3t}}{p}, \quad q \geq n \cdot p, \quad |\mathcal{V}_i| = p \cdot q^2 \ \left(\approx \frac{(n \cdot t \cdot 2^{3t})^2 \cdot |\mathcal{S}|}{\epsilon^2}\right).$$

Proof. The proof is similar to that of Theorem 3 except that we pay attention to the 0-th and the t-th degree coefficients of polynomials $C_0(x)$ and $C_1(x)$, respectively, in analyzing the security of the proposed scheme.

As in the proof of Theorem 3, we can assume $P_1, \ldots, P_t$ are cheaters who cooperatively try to fool the other participants $P_{t+1}, \ldots, P_m$ by forging (part of) their shares. Suppose that P_1 is a critical cheater who submits invalid share $v'_1 = (v'_{s,1}, v'_{C_0,1}, v'_{C_1,1})$ such that $v'_{s,1} \neq v_{s,1}$. We will show that the probability that the successful cheating probability of P_1 is upper bounded by ϵ $(= \frac{t \cdot 2^{3t}}{p})$.

From the proof of Theorem 1, it is easy to see that, if $t \leq (m-1)/3$ holds, the successful cheating probability of P_1 is upper bounded by $q(< \epsilon)$.

Now we will show the proposed reconstruction algorithm can catch cheaters with probability better than $1-\epsilon$ even against $t = \lfloor (k-1)/2 \rfloor$ cheaters. It suffices to show that the probability that there exists at least one subset $\mathcal{I} \subseteq \{1, \ldots, m\}$ such that (1) $1 \in \mathcal{I}$, (2) $|\mathcal{I}| = t+1$, and (3) $a_{\mathcal{I},0} = a_{\mathcal{I},1}$, is lower bounded by ϵ.

Toward showing the above, we will first show that the probability $\epsilon(\mathcal{I})$ that $a_{\mathcal{I},0} = a_{\mathcal{I},1}$ holds for given $\mathcal{I}$ is lower bounded by $2t/p$ for any $\mathcal{I}$ such that $1 \in \mathcal{I}$ and $|\mathcal{I}| = t+1$. Without loss of generality, we can assume $\mathcal{I} = \{\ell_1, \ell_2, \ldots, \ell_{t+1}\}$ and $P_{\ell_1} \ldots, P_{\ell_{t'}}$ $(t' \leq t)$ are cheaters.

To evaluate $\epsilon(\mathcal{I})$, we will analyze the structures of $a_{\mathcal{I},0}$ and $a_{\mathcal{I},1}$. As in the proof of Theorem 3, we will use the notation ψ_i to denote $\psi(v_{s,i}, i)$ and the notation X' to indicate the variable X is owned and controlled by the cheaters. By the similar discussion to the proof of Theorem 3, $a_{\mathcal{I},0}$ and $a_{\mathcal{I},1}$ can be rewritten as follows:

$$a_{\mathcal{I},0} = \sum_{i=1}^{t'} A_{0,i} \cdot \prod_{j=t'+1}^{t+1} \frac{-\psi_{\ell_j}}{\psi'_{\ell_i} - \psi_{\ell_j}} + \sum_{j=t'+1}^{t+1} C_0(\psi_{\ell_j}) \cdot \prod_{i=1}^{t'} \frac{-\psi'_{\ell_i}}{\psi_{\ell_j} - \psi'_{\ell_i}} \prod_{\substack{i=t'+1 \\ i \neq j}}^{t+1} \frac{-\psi_{\ell_i}}{\psi_{\ell_j} - \psi_{\ell_i}} \quad (4)$$

$$a_{\mathcal{I},1} = \sum_{i=1}^{t'} A_{1,i} \cdot \prod_{j=t'+1}^{t+1} \frac{1}{\psi'_{\ell_i} - \psi_{\ell_j}} + \sum_{j=t'+1}^{t+1} C_1(\psi_{\ell_j}) \cdot \prod_{i=1}^{t'} \frac{1}{\psi_{\ell_j} - \psi'_{\ell_i}} \prod_{\substack{i=t'+1 \\ i \neq j}}^{t+1} \frac{1}{\psi_{\ell_j} - \psi_{\ell_i}} \quad (5)$$

With the knowledge about shares owned by the cheaters, the number of possible candidates for $(\psi_{\ell_{t'+1}}, \ldots, \psi_{\ell_{t+1}}, C_0, C_1)$ becomes $p^{t-t'+1} \times q^{2(t-t')+1}$ since (1) ψ_{ℓ_i} $(t'+1 \leq i \leq t+1)$ look randomly, uniformly and independently distributed over the set $\Psi_{\ell_i} = \{\psi(v_{s,\ell_i}, \ell_i) \mid v_{s,\ell_i} \in GF(p)\}$ even with the knowledge of cheaters, and (2) $(\psi_{\ell_{t'+1}}, v_{C_0,\ell_{t'+1}}, v_{C_1,\ell_{t'+1}}) \ldots (\psi_{\ell_t}, v_{C_0,\ell_t}, v_{C_1,\ell_t})$ and $(\psi_{\ell_{t+1}}, v_{C_0,\ell_{t+1}})$ uniquely determines the polynomials $C_0(x)$ and $C_1(x)$ such that $a_{0,t} = a_{1,t}$ holds.

Now, we will estimate the upper bound of the number of $(\psi_{\ell_{t'+1}}, \ldots, \psi_{\ell_{t+1}}, C_0, C_1)$ with which $a_{\mathcal{I},0} = a_{\mathcal{I},1}$. By the similar discussion to the proof of Theorem 3, we can show that, for any fixed $(\psi_{\ell_{t'+1}}, \ldots, \psi_{\ell_t}, C_0, C_1) = (\hat{\psi}_{\ell_{t'+1}}, \ldots, \hat{\psi}_{\ell_t}, \hat{C}_0, \hat{C}_1)$, eq. (4) and eq. (5) are rewritten as follows:

$$\begin{aligned} a_{\mathcal{I},0} = \sum_{i=1}^{t'} \frac{-\hat{A}_{i,0} \cdot \psi_{\ell_{t+1}}}{\psi'_{\ell_i} - \psi_{\ell_{t+1}}} + \sum_{j=t'+1}^{t} \frac{-\hat{B}_{j,0} \cdot \psi_{\ell_{t+1}}}{\hat{\psi}_{\ell_j} - \psi_{\ell_{t+1}}} \\ + \hat{C}_0(\psi_{t+1}) \cdot \prod_{i=1}^{t'} \frac{-\psi_{\ell_{t+1}}}{\psi_{\ell_{t+1}} - \psi'_{\ell_i}} \prod_{i=t'+1}^{t} \frac{-\psi_{\ell_{t+1}}}{\psi_{\ell_{t+1}} - \hat{\psi}_{\ell_i}} \end{aligned}$$

$$\begin{aligned} a_{\mathcal{I},1} = \sum_{i=1}^{t'} \frac{\hat{A}_{i,1}}{\psi'_{\ell_i} - \psi_{\ell_{t+1}}} + \sum_{j=t'+1}^{t} \frac{\hat{B}_{j,1}}{\hat{\psi}_{\ell_j} - \psi_{\ell_{t+1}}} \\ + \hat{C}_1(\psi_{t+1}) \cdot \prod_{i=1}^{t'} \frac{1}{\psi_{\ell_{t+1}} - \psi'_{\ell_i}} \prod_{i=t'+1}^{t} \frac{1}{\psi_{\ell_{t+1}} - \hat{\psi}_{\ell_i}} \end{aligned}$$

where $\hat{A}_{i,0}, \hat{B}_{j,0}, \hat{A}_{i,1}$ and $\hat{B}_{j,1}$ are constant once ψ'_{ℓ_i} $(1 \le i \le t')$, $\hat{\psi}_{\ell_j}$ $(t'+1 \le j \le t)$, $\hat{C}_0$, and $\hat{C}_1$ are fixed. We see that there are at most $2t$ values of $\psi_{\ell_{t+1}}$ with which $a_{\mathcal{I},0} = a_{\mathcal{I},1}$ since solving $\psi_{\ell_{t+1}}$ such that $a_{\mathcal{I},0}(\psi_{\ell_{t+1}}) = a_{\mathcal{I},1}(\psi_{\ell_{t+1}})$ is equivalent to solving the equation $A_{\mathcal{I}}(\psi_{\ell_{t+1}}) = 0$ for a polynomial $A_{\mathcal{I}}$ of degree $2t$ where $A_{\mathcal{I}}$ is uniquely determined from $a_{\mathcal{I},0}$ and $a_{\mathcal{I},1}$. Therefore, the upper bound of the number of $(\psi_{\ell_{t'+1}}, \ldots, \psi_{\ell_{t+1}}, C_0, C_1)$ such that $a_{\mathcal{I},0} = a_{\mathcal{I},1}$ can be evaluated as follows:

$$
\begin{aligned}
&|\{(\psi_{\ell_{t'+1}}, \ldots, \psi_{\ell_{t+1}}, C_0, C_1) \mid a_{\mathcal{I},0} = a_{\mathcal{I},1} \text{ holds}\}| \\
&\le |\{(\psi_{\ell_{t'+1}}, \ldots, \psi_{\ell_t}) \mid \psi_{\ell_i} \in \Psi_{\ell_i}\ (t'+1 \le i \le t)\}| \\
&\qquad \times \left| \left\{ (C_0(x), C_1(x)) \,\middle|\, \begin{matrix} C_0(\psi_i) = v_{C_0,i},\ C_1(\psi_i) = v_{C_1,i}\ (1 \le i \le t'), \\ a_{0,0} = a_{1,t} \end{matrix} \right\} \right| \times 2t \\
&= p^{t-t'} \cdot q^{2(t-t')+1} \cdot 2t
\end{aligned}
$$

Therefore, we see that $\epsilon(\mathcal{I})$ is lower bounded by $\epsilon(\mathcal{I}) \le 2t/p$ since $\epsilon(\mathcal{I}) \le \frac{p^{t-t'} \cdot q^{2(t-t')+1} \cdot 2t}{p^{t-t'+1} \cdot q^{2(t-t')+1}} = 2t/p$ holds.

From the above inequality and the fact that the number of subsets $\mathcal{I}$ of $\{1, \ldots, 3t\}$ such that $1 \in \mathcal{I}$ and $|\mathcal{I}| = t+1$ is equal to $\binom{3t-1}{t}$, the successful cheating probability ϵ is given as follows:

$$
\begin{aligned}
\epsilon &= \Pr[\text{there exists } \mathcal{I} \text{ such that } \Delta c_{\mathcal{I}} = 0,\ 1 \in \mathcal{I},\ |\mathcal{I}| = t+1] \\
&\le \sum_{\left\{\mathcal{I} \,\middle|\, \begin{smallmatrix} 1 \in \mathcal{I}, \\ |\mathcal{I}| = t+1 \end{smallmatrix}\right\}} \epsilon(\mathcal{I}) \;=\; \left| \left\{ \mathcal{I} \,\middle|\, \begin{matrix} 1 \in \mathcal{I}, \\ |\mathcal{I}| = t+1 \end{matrix} \right\} \right| \cdot \epsilon(\mathcal{I}) \;\le\; \binom{3t-1}{t} \cdot \frac{t}{p} \;\le\; \frac{t \cdot 2^{3t}}{p}
\end{aligned}
$$

The size of share satisfies $|\mathcal{V}_i| = p \cdot q$ and is approximately written by $|\mathcal{V}_i| \approx \frac{(n \cdot t \cdot 2^{3t})^2 |\mathcal{S}|}{\epsilon^2}$ since $q \approx n \cdot p$ and $p \le \frac{t \cdot 2^{3t}}{\epsilon}$. □

6 Conclusion

In this paper, we present efficient (t, ϵ) cheater identifiable (k, n) threshold secret sharing schemes under the conditions $t \le \lfloor (k-1)/3 \rfloor$, $t \le \lfloor (k-2)/2 \rfloor$ and $t \le \lfloor (k-1)/2 \rfloor$, respectively. The schemes which can catch $\lfloor (k-1)/3 \rfloor$ cheaters are the first schemes whose share size is independent of any of n, k and t. Further, in one of these schemes, the share size is almost optimum in the sense that the bit length of the share is only one bit longer than the bound given in [12]. The schemes which can catch $t \le \lfloor (k-2)/2 \rfloor$ cheaters and $t \le \lfloor (k-1)/2 \rfloor$ cheaters are, though the bit length of shares grows linear to the number of cheaters, shown to be much more efficient with respect to the size of share compared to [12] and the other schemes with private cheater identification.

In our future work, we will focus on finding an efficient scheme under the condition $t \le \lfloor (k-1)/2 \rfloor$ such that the size of share is independent of any of n, k and t, and the computational cost for identifying cheaters is small.

References

1. T. Araki, "Efficient (k, n) Threshold Secret Sharing Scheme Secure against Cheating from $n - 1$ Cheaters," Proc. ACISP'07, Lecture Notes in Computer Science, vol. 4586, Springer Verlag, pp. 133–142, 2007.
2. T. Araki and S. Obana, "Flaws in Some Secret Sharing Schemes against Cheating," Proc. ACISP'07, Lecture Notes in Computer Science, vol. 4586, Springer Verlag, pp. 122–132, 2007.
3. G. R. Blakley, "Safeguarding cryptographic keys," Proc. AFIPS 1979, National Computer Conference, vol. 48, pp. 313–137, 1979.
4. E. F. Brickell and D. R. Stinson, "The Detection of Cheaters in Threshold Schemes," SIAM Journal on Discrete Mathematics, vol. 4, no. 4, pp. 502–510, 1991.
5. M. Carpentieri, "A Perfect Threshold Secret Sharing Scheme to Identify Cheaters," Designs, Codes and Cryptography, vol. 5, no. 3, pp. 183–187, 1995.
6. R. Cramer, Y. Dodis, S. Fehr, C. Padró, D. Wichs, "Detection of Algebraic Manipulation with Applications to Robust Secret Sharing and Fuzzy Extractors," Proc. Eurocrypt 2008, Lecture Notes in Computer Science, vol. 4965, Springer Verlag, pp. 471–488, 2008.
7. M. Carpentieri, A. De Santis and U. Vaccaro, "Size of Shares and Probability of Cheating in Threshold Schemes," Proc. Eurocrypt'93, Lecture Notes in Computer Science, vol. 765, Springer Verlag, pp. 118–125, 1993.
8. R. Cramer, I. Damgård and S. Fehr, "On the Cost of Reconstruction a Secret, or VSS with Optimal Reconstruction Phase," Proc. Crypto'01, Lecture Notes in Computer Science, vol. 2139, Springer Verlag, pp. 503–523, 2001.
9. 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, 2002.
10. B. den Boer, "A Simple and Key-Economical Unconditional Authentication Scheme," Journal of Computer Security, vol. 2, pp. 65–71, 1993.
11. D. Dolev, C. Dwork, O. Waarts, M. Yung, "Perfectly Secure Message Transmission," Journal of the ACM, vol. 40, no. 1, pp. 17–47, 1993.
12. K. Kurosawa, S. Obana and W. Ogata, "t-Cheater Identifiable (k, n) Secret Sharing Schemes," Proc. Crypto'95, Lecture Notes in Computer Science, vol. 963, Springer Verlag, pp. 410–423, 1995.
13. K. Kurosawa, K. Suzuki, "Almost Secure (1-Round, n-Channel) Message Transmission Scheme," Proc. ICITS, 2007.
14. F. MacWilliams and N. Sloane, "The Theory of Error Correcting Codes," North Holland, Amsterdam, 1977.
15. R. J. McEliece and D. V. Sarwate, "On Sharing Secrets and Reed-Solomon Codes," Communications of the ACM, vol 24, issue 9, pp. 583-584, 1981.
16. S. Obana and T. Araki, "Almost Optimum Secret Sharing Schemes Secure Against Cheating for Arbitrary Secret Distribution," Proc. Asiacrypt 2006, Lecture Notes in Computer Science, vol. 4284, Springer Verlag, pp. 364–379, 2006.
17. W. Ogata and K. Kurosawa, "Optimum Secret Sharing Scheme Secure against Cheating," Proc. Eurocrypt'96, Lecture Notes in Computer Science, vol. 1070, Springer Verlag, pp. 200–211, 1996.
18. W. Ogata and K. Kurosawa, "Provably Secure Metering Scheme," Proc. Asiacrypt'00, Lecture Notes in Computer Science, vol. 1976, Springer Verlag, pp. 388–398, 2000.

19. W. Ogata, K. Kurosawa and D. R. Stinson, "Optimum Secret Sharing Scheme Secure against Cheating," SIAM Journal on Discrete Mathematics, vol. 20, no. 1, pp. 79–95, 2006.
20. T. Pedersen, "Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing," Proc. Crypto'91, Lecture Notes in Computer Science, vol 576, Springer Verlag, pp. 129–149, 1991.
21. T. Rabin and M. Ben-Or, "Verifiable Secret Sharing and Multiparty Protocols with Honest Majority," Proc. STOC'89, pp. 73–85.
22. T. Rabin, "Robust Sharing of Secrets When the Dealer is Honest or Cheating," Journal of the ACM, vol. 41, no. 6, pp. 1089–1109, 1994.
23. A. Shamir, "How to Share a Secret," Communications of the ACM, vol. 22, issue 11, pp. 612–613, 1979.
24. D. R. Stinson, "On the Connections between Universal Hashing, Combinatorial Designs and Error-Correcting Codes," Congressus Numerantium 114, pp. 7–27, 1996.
25. M. Tompa and H. Woll, "How to Share a Secret with Cheaters," Journal of Cryptology, vol. 1, no. 3, pp. 133-138, 1989.