An Efficient t-Cheater Identifiable Secret Sharing Scheme with Optimal Cheater Resiliency

Partha Sarathi Roy & Avishek Adhikari

Department of Pure Mathematics, University of Calcutta.
royparthasarathi0@gmail.com, avishek.adh@gmail.com

Rui Xu

Graduate School of Mathematics, Kyushu University.
r-xu@math.kyushu-u.ac.jp

Kirill Morozov

Institute of Mathematics for Industry, Kyushu University.
morozov@imi.kyushu-u.ac.jp

Kouichi Sakurai

Graduate School of Information Science and Electrical Engineering, Kyushu University.
sakurai@csce.kyushu-u.ac.jp

Abstract

In this paper, we present an efficient k-out-of-n secret sharing scheme, which can identify up to t rushing cheaters, with probability at least $1-\epsilon$, where $0 < \epsilon < 1/2$, provided $t < k/2$. This is the optimal number of cheaters that can be tolerated in the setting of public cheater identification, on which we focus in this work. In our scheme, the set of all possible shares V_i satisfies the condition that $|V_i| = \frac{(t+1)^{2n+k-3}|S|}{\epsilon^{2n+k-3}}$, where S denotes the set of all possible secrets. In PODC-2012, Ashish Choudhury came up with an efficient t-cheater identifiable k-out-of-n secret sharing scheme, which was a solution of an open problem proposed by Satoshi Obana in EUROCRYPT-2011. The share size, with respect to a secret consisting of one field element, of Choudhury's proposal in PODC-2012 is $|V_i| = \frac{(t+1)^{3n}|S|}{\epsilon^{3n}}$. Therefore, our scheme presents an improvement in share size over the above construction. Hence, to the best of our knowledge, our proposal currently has the minimal share size among existing efficient schemes with optimal cheater resilience, in the case of a single secret.

Keywords : cheater identifiable secret sharing, share size, rushing adversary.

1 Introduction:

According to *Time Magazine*, May 4, 1992, control of nuclear weapons in Russia involves a two-out-of-three mechanism. In order to launch a nuclear missile, the cooperation of at least two parties out of three is needed. The three parties involved are the President, the Defence

Minister and the Defence Ministry. A similar situation may occur in a bank. There are many such instances in today's open system environment. In the open system environment, it is important to restrict access of confidential information in the system or on certain nodes in the system. Access is gained through a key, password or token and governed by a secure key management scheme. If the key or the password is shared among several participants in such a way that it can be reconstructed only by a significantly large and responsible group acting in agreement, then a high degree of security is attained.

Shamir [22] and Blakley [3] independently addressed this problem in 1979 when they introduced the concept of a threshold secret sharing scheme. A (k, n) *threshold scheme* is a method where n pieces of information of the secret, called *shares* are distributed to n participants so that the secret can be reconstructed from the knowledge of any k or more shares and the secret cannot be reconstructed from the knowledge of fewer than k shares, where $k \leq n$. More formally, in a secret sharing scheme, there exists a set of n parties, denoted by $\mathcal{P} = \{P_1, \ldots, P_n\}$ and a special party called the dealer, denoted by $\mathcal{D}$. A (k, n) threshold secret sharing scheme consists of two phases:

1. **Sharing Phase:** During this phase, the dealer $\mathcal{D}$ shares the secret among the n participants. In this phase the dealer sends some information, known as *share*, to each participant.

2. **Reconstruction Phase:** In this phase, a set of parties (of size at least k) pool their shares to reconstruct the secret.

In the sharing phase dealer wants to share the secret in such a way that satisfies the following two conditions:

1. **Correctness:** Any set of k or more parties can reconstruct the secret by pooling their shares.

2. **Secrecy:** Any set of $(k-1)$ or less participants can not reconstruct the secret. Moreover, for $perfect\ secrecy$, any set of $(k-1)$ or less participants will have no information regarding the secret.

In a secret sharing scheme, it is assumed that everyone involved with the protocol is honest or semi honest. But for the real life scenario, this assumption may not hold well. It may happen that some participants behave maliciously during the execution of the protocol. Malicious participants may submit incorrect shares resulting in incorrect secret. This observation led to some interesting protocols viz. *secret sharing scheme with cheating detection*, *secret sharing scheme with cheating identification*, *robust secret sharing scheme*, *verifiable secret sharing scheme*.

Tompa and Woll [23] first presented a cheater detecting secret sharing scheme. This work is followed by several other works (for example, [1], [2], [9], [5], [18], [20]). However, all these schemes can only detect cheating, without identifying the exact identity of the cheaters, who submitted incorrect shares.

McElice and Sarwate [16] were the first to point out cheater identification in secret sharing schemes. There was a shortcoming that to identify the cheaters, more than k participants are required in the reconstruction phase of a (k, n) threshold secret sharing scheme. The question is whether the cheater identification is possible or not with the minimum number of shares (namely k), which are required to reconstruct the secret. *Secret Sharing with Cheater*

Identification (SSCI) is the answer to this question, and it is the main focus of our paper. More specifically, in the setting of public cheater identification [17], we propose an SSCI with reduced share size, compared to existing SSCI schemes, while retaining efficiency and optimal resiliency.

In another variant called *robust* secret sharing [4, 8, 9], the main goal is to ensure successful reconstruction of a correct secret (possibly from more than a threshold of k shares), while disregarding identities of the cheaters.

In this work, we assume the dealer to be *honest*. The case of (possibly) dishonest dealer is handled by *verifiable secret sharing* [10]. For more information on adversary models in secret sharing see [15].

There are two types of cheater identification in secret sharing: *private* as e.g. in [21, 6, 19] and *public* as e.g. in [14, 17, 7, 26]. A reconstruction algorithm of SSCI with public cheater identification can be run by an external entity. This is an essential advantage of SSCI with public cheater identification over those with private one. However, SSCI with public cheater identification is only possible for the case of honest majority [14, 17], while for the case of SSCI with private cheater identification honest majority is not required [12]. In this work, we only deal with *public* cheater identification.

1.1 The State of the Art and Our Results

It has been proved in [14] and [17] that an SSCI scheme with public cheater identification, capable of identifying up to t cheaters, is possible if and only if $t < k/2$. So, any publicly cheater identifiable SSCI scheme with $k = 2t + 1$ is said to be *optimal cheater resilient*. The lower bound [14] on the share size $|V_i|$ of such schemes is $|V_i| \geq \frac{|S|-1}{\epsilon} + 1$. We summarize the properties of existing SSCI schemes with public cheater identification in Table 1.

Table 1: Comparison of Our Proposal to Existing SSCI schemes.

Scheme	#Cheaters	Share Size	Efficiency	Rushing
[14]	$t < k/3$	$\|V_i\| = \|S\|/\epsilon^{t+2}$	Yes	No
[17]	$t < k/3$	$\|V_i\| = \|S\|/\epsilon$	Yes	No
[17]	$t < k/2$	$\|V_i\| \approx (n.(t+1).2^{3t-1}\|S\|)/\epsilon$	No	No
[17]	$t < k/2$	$\|V_i\| \approx ((n.(t+1).2^{3t})^2\|S\|)/\epsilon$	No	No
[7]	$t < k/2$	$\|V_i\| = (t+1)^{3n}\|S\|/\epsilon^{3n}$	Yes	Yes
[26]	$t < k/3$	$\|V_i\| = \|S\|/\epsilon^{n-t+1}$	Yes	Yes
Proposed	$t < k/2$	$\|V_i\| = (t+1)^{2n+k-3}\|S\|/\epsilon^{2n+k-3}$	Yes	Yes

In [17], two publicly cheater identifiable SSCI schemes with optimal cheater resilience were proposed, however, both of them were inefficient. Choudhury [7] came up with an efficient solution, but the scheme in [7] deals with multiple secrets. In the case of a single secret, the scheme of [7] is not optimal. In Table 1, we provide the share size of [7] *with respect to a single secret*, for a fair comparison with our scheme. We can see that the open question is to fill the gap between the optimal share size and that of the existing schemes when a single secret is to be shared. One improvement came from Xu et al. [26] but they did not achieve the optimal share size. Moreover, their scheme is not an optimal cheater resilient as it tolerates $t < k/3$

cheaters. We provide an SSCI scheme with better share size than [7] with optimal cheater resilience. To the best of our knowledge, the proposed scheme is the most efficient optimal cheater resilience scheme with respect to the share size.

2 t-Cheater Identifiable (k, n) Threshold Schemes

2.1 Secret Sharing with Cheater Identification (SSCI)

In the model of SSCI, there exists a set of n parties, denoted by $\mathcal{P} = \{P_1, \ldots, P_n\}$ and a special party called the dealer, denoted by $\mathcal{D}$. There exist two different centralized adversaries, denoted by $\mathcal{A}_{Lis}$ and $\mathcal{A}_{Cheat}$, respectively. The adversary $\mathcal{A}_{Lis}$ is a static, computationally unbounded, rushing, passive adversary, who can control any $(k-1)$ out of the n parties. On the other hand, the adversary $\mathcal{A}_{Cheat}$ is a static, computationally unbounded, rushing, malicious adversary, who can control any t out of the n parties. By being rushing we mean that the adversary can observe the information sent by all the honest players at each communication round, prior to deciding on his own messages. It is also assumed that $\mathcal{A}_{Lis}$ does not cooperate with $\mathcal{A}_{Cheat}$. This implies that $\mathcal{A}_{Cheat}$ will not get any information about the computation and communication of the parties, which may be under the control of $\mathcal{A}_{Lis}$, but not under the control of $\mathcal{A}_{Cheat}$. Similarly, $\mathcal{A}_{Lis}$ will not get any information about the computation and communication of the parties, which may be under the control of $\mathcal{A}_{Cheat}$, but not under the control of $\mathcal{A}_{Lis}$.

Any SSCI scheme consists of the following two phases [7]:

1. **Sharing Phase:** During this phase, $\mathcal{D}$ takes the secret s and generates n shares for the secret, denoted by $V_1, \ldots, V_n$ and assigns V_i to the party P_i.

2. **Reconstruction Phase:** During this phase, a set of m parties, where $m \geq k$, publicly produce their shares to reconstruct the secret. These m parties can be any m parties out of the n parties.

   - Then a cheating identification algorithm is publicly applied on the m shares produced by the m parties to identify the invalid shares.
   - Let L be the set of parties who are identified to be the cheaters by the cheater identification algorithm.
     - If $(m - |L|) \geq k$, then a publicly known reconstruction function, called Rec, is applied on the shares produced by the parties not in L, to reconstruct a secret s'. Finally, s' and L are the outputs of the reconstruction phase.
     - If $(m - |L|) < k$, then $\perp$ and L are the outputs of the reconstruction phase.

We require an SSCI scheme to satisfy the following properties [7]:

- **Perfect Secrecy:** At the end of the sharing phase, the adversary $\mathcal{A}_{Lis}$ should not get any information about the secret s (in information-theoretic sense) from the shares of the parties (at most $(k-1)$) under its control.

- **Correctness:** During the reconstruction phase, if any party P_i is under the control of $\mathcal{A}_{Cheat}$ and produces incorrect share $V_i' \neq V_i$, then except with error probability ϵ, P_i will be identified as a cheater and will be included in the set L.

2.2 Communication Model

Communication model assumes that the dealer and the participants are pairwise connected by a private and authenticated channel. We further assume that a common broadcast channel is also available to every participant and the dealer.

2.3 Cheater Identification and Share Authentication

Let the dealer $\mathcal{D}$ share the secret s with the help of a polynomial $f(x)$ of degree at most $(k-1)$ as in Shamir scheme [22]. Then the share of a player P_i is just $f(\alpha_i)$, where α_i is a publicly known non-zero field element. Now, if there are some malicious participants, who may modify the original share at the time of reconstruction, then correctness will not hold and there will be no option for cheating identification. Therefore, the dealer should generate some authentication information by which each participant can check consistency of the share of other participants. Suppose, P_j wants to verify the share of P_i. For this verification, at the sharing phase the dealer randomly chooses an authentication key $k_{j,i}$, computes the authentication tag $\tau_{j,i}$ and privately sends the key $k_{j,i}$ to P_j so that the later can verify authenticity of P_i's share.

Denote by $d_{i,0}$ the Shamir share for player P_i, and use the authentication code (MAC : $\mathcal{M} \times \mathcal{K} \to \mathcal{T}, \mathcal{M} = \mathbb{F}, \mathcal{K} = \mathbb{F} \times \mathbb{F}$, *and* $\mathcal{T} = \mathbb{F}$, *where* $\mathbb{F}$ *is a finite field*) [24, 25, 13]. In particular, for every pair of players P_i and P_j, P_i's Shamir share $d_{i,0}$ is authenticated with an authentication tag $\tau_{i,j}$, where the corresponding authentication key $k_{j,i}$ is held by player P_j. Specifically, choose $k_{j,i} = (g_{j,i}, b_{j,i})$ randomly from $\mathbb{F} \times \mathbb{F}$ and compute $\tau_{j,i} = d_{i,0}g_{j,i} + b_{j,i}$.

In fact, this method was used by Rabin and Ben-Or [21], but Carpentieri [6] observed that the authentication code can be used more cleverly. Instead of first choosing the authentication key and then calculating the authentication tag, one can first fix the authentication tag and then find the authentication key. The intention for such the reversion of the authentication protocol is to compress the authentication tags. In Rabin and Ben-Or setting, each player will get $n-1$ keys and $n-1$ tags for pair-wise authentication. By using the above trick, one can, instead of sending $n-1$ tags to each player, send a *seed* c_i to player P_i. Then, the necessary authentication tags will be generated from the *seed* c_i together with some public information. In fact, the *seed* for P_i is $c_i = (d_{i,1}, \ldots, d_{i,k-1})$, where $d_{i,j}$ for $j \in \{1, \ldots, k-1\}$ is randomly chosen from $\mathbb{F}$ and the authentication tag of P_i against P_j's key is $\tau_{i,j} = \alpha_i d_{j,1} + \alpha_i^2 d_{j,2} + \cdots + \alpha_i^{k-1} d_{j,k-1}$. Compared to the setting of Rabin and Ben-Or, each player now gets a *seed* of $k-1$ field elements from which the $n-1$ authentication tags are generated. Thus, the share size of each player is reduced by $n-k$ filed elements.

3 Proposed Optimal Cheater Resilient ($t < k/2$) SSCI scheme with Public Cheater Identification

3.1 High-Level Idea

We first observe that Choudhury's scheme [7] in the case of single secret can be considered as an adaptation of the Rabin and Ben-Or [21] scheme to the case of public cheater identification (against rushing adversary). Next, we recall that Carpentieri [6] presented a method to reduce the overhead need for authentication in the Rabin and Ben-Or scheme as described in the previous section. In our proposal, we use the share authentication method derived from that

of Carpentieri by adapting the latter to the case of public cheater identification and rushing adversary.

3.2 Our Proposal

- **Initialization:** For $i = 1, \ldots, n$, let the distinct elements $\alpha_i \in \mathbb{F} \setminus \{0\}$ be fixed and public, where $\mathbb{F}$ is a finite field..
- **Sharing Phase:**
  - The dealer $\mathcal{D}$ chooses randomly a polynomial $f(x)$ of degree at most $(k-1)$ in x from $\mathbb{F}[X]$ such that $f(0) = s$, where s is the secret to be shared. Also, the dealer $\mathcal{D}$ computes $f(\alpha_i) = d_{i,0}$, where $i = 1, \ldots, n$.
  - The dealer $\mathcal{D}$ chooses randomly $d_{i,1}, \ldots, d_{i,k-1}$ and $g_{i,j}$ from $\mathbb{F}$, where $j = 1, \ldots, i-1, i+1, \ldots, n$ and $i = 1, \ldots, n$. The dealer computes $b_{i,j} = \alpha_i d_{j,1} + \alpha_i^2 d_{j,2} + \ldots + \alpha_i^{k-1} d_{j,k-1} - g_{i,j} d_{j,0}$, where $j = 1, \ldots, i-1, i+1, \ldots, n$ and $i = 1, \ldots, n$.
  - $\mathcal{D}$ sends each P_i the share $V_i = (d_{i,0}, \ldots, d_{i,k-1}, g_{i,1}, \ldots, g_{i,i-1}, g_{i,i+1}, \ldots, g_{i,n}, b_{i,1}, \ldots, b_{i,i-1}, b_{i,i+1}, \ldots, b_{i,n})$.
- **Reconstruction Phase:** Denote the set of m $(\geq k)$ participants taking part in the reconstruction as *core*.
  - **Round 1:** Each $P_i \in core$ broadcasts $d'_{i,0}, d'_{i,1}, \ldots, d'_{i,k-1}$.
  - **Round 2:** Each $P_i \in core$ broadcasts $(g'_{i,1}, \ldots, g'_{i,i-1}, g'_{i,i+1}, \ldots, g'_{i,n}, b'_{i,1}, \ldots, b'_{i,i-1}, b'_{i,i+1}, \ldots, b'_{i,n})$.
  - **Local Computation:** For each $P_i \in core$ computes $support_i = \{P_j : \alpha_j d'_{i,1} + \alpha_j^2 d'_{i,2} + \ldots + \alpha_j^{k-1} d'_{i,k-1} = g'_{j,i} d'_{i,0} + b'_{j,i} \& P_j \in core\} \cup \{P_i\}$.
    If $|support_i| < t+1$, then put P_i in L, where L is the list of the cheaters.
    - If $m - |L| \geq k$ **:** Using $d'_{i,0}$ for all $P_i \in core \setminus L$, interpolate a poly $f'(x)$. If degree of $f'(x)$ is less or equal to k, output $(f'(0), L)$ otherwise output $(\perp, L)$.
    - If $m - |L| < k$ **:** Output $(\perp, L)$.

Theorem 3.1. *The above scheme provides perfect secrecy. That is, any adversary $\mathcal{A}_{Lis}$ controlling any $(k-1)$ parties during the sharing phase, will get no information about the secret s.*

Proof. The dealer $\mathcal{D}$ shares the secret s through a polynomial $f(x)$, where the degree of the polynomial is at most $(k-1)$ in x, and the share of each P_i is $V_i = (d_{i,0}, \ldots, d_{i,k-1}, g_{i,1}, \ldots, g_{i,i-1}, g_{i,i+1}, \ldots, g_{i,n}, b_{i,1}, \ldots, b_{i,i-1}, b_{i,i+1}, \ldots, b_{i,n})$.
Without loss of generality, we may assume that the first $(k-1)$ participants, i.e., $P_1, \ldots, P_{k-1}$, are under the control of the adversary $\mathcal{A}_{Lis}$. Now, according to Lagrange interpolation, k such values $d_{i,0}$ fully define a degree-$(k-1)$ polynomial. On the other hand, $k-1$ such values provide no information on s, according to the perfect privacy property of Shamir scheme. Thus, we need to choose one more $d_{i,0}$, where $i \in \{1, 2, \ldots, n\} \setminus I$, where $I = \{1, 2, \ldots, k-1\}$. Without loss of generality, we may assume that $i = k$. Note that each player P_i $(i \in I)$ has the information $(g_{i,k}, b_{i,k})$ regarding $d_{k,0}$.

So, for all $i \in I$,

$$b_{i,k} + g_{i,k}d_{k,0} = \alpha_i d_{k,1} + \alpha_i^2 d_{k,2} + \ldots + \alpha_i^{k-1} d_{k,k-1}.$$

As the matrix $\begin{bmatrix} \alpha_1 & \alpha_1^2 & \ldots & \alpha_1^{k-1} \\ \alpha_2 & \alpha_2^2 & \ldots & \alpha_2^{k-1} \\ \ldots & \ldots & \ldots & \ldots \\ \alpha_{k-1} & \alpha_{k-1}^2 & \ldots & \alpha_{k-1}^{k-1} \end{bmatrix}$ is non-singular, the above system of linear equations is consistent for all possible values of $d_{k,0}$. Thus, $\mathcal{A}_{Lis}$ can guess the correct $d_{k,0}$ with probability $\frac{1}{|\mathbb{F}|}$, i.e., $\mathcal{A}_{Lis}$ has no information regarding $d_{k,0}$. Hence, the theorem. □

Theorem 3.2. *The proposed scheme satisfies correctness condition. That is, during the reconstruction phase, if any $P_i \in$ core is under the control of rushing $\mathcal{A}_{Cheat}$ and produces $d'_{i,0} \neq d_{i,0}$, then except with error probability $\epsilon = \frac{t+1}{|\mathbb{F}|}$, P_i will be identified as a cheater and will be included in the list L.*

Proof. Without loss of generality, let *core* be formed by the first m parties, namely $P_1, \ldots, P_m$, where $m \geq k$. Moreover, let $P_1, \ldots, P_t$ be under the control of $\mathcal{A}_{Cheat}$. Now suppose that P_1 submits $d'_{1,0} \neq d_{1,0}$ and P_1 is not identified as a cheater. This implies that $|support_1| \geq t+1$. In the worst case, $P_1, \ldots, P_t$ may be present in $support_1$, as all of them are under the control of $\mathcal{A}_{Cheat}$. But $|support_1| \geq t+1$ implies that there exists at least one honest party in *core*, say P_j, such that $P_j \in support_1$. This is possible only if $g_{j,1}d'_{1,0} + b_{j,1} = \alpha_j d'_{1,1} + \alpha_j^2 d'_{1,2} + \ldots + \alpha_j^{k-1} d'_{1,k-1}$. Now in *Round* 1 of reconstruction phase P_1 broadcasts $d'_{i,0}, d'_{i,1}, \ldots, d'_{i,k-1}$ and in *Round* 2 of reconstruction phase P_j broadcasts $g_{j,1}, b_{j,1}$. So, in *Round* 1 of the reconstruction phase, a rushing $\mathcal{A}_{Cheat}$ will have no information about the $g_{j,1}$. Thus, the probability that P_1 can ensure that $g_{j,1}d'_{1,0} + b_{j,1} = \alpha_j d'_{1,1} + \alpha_j^2 d'_{1,2} + \ldots + \alpha_j^{k-1} d'_{1,k-1}$ even if $d'_{1,0} \neq d_{1,0}$ is the same as the probability that P_1 correctly guesses $g_{j,1}$. However, the probability that P_1 correctly guesses $g_{j,1}$ is $\frac{1}{|\mathbb{F}|}$, as $g_{j,1}$ is uniformly and randomly selected from $\mathbb{F}$.

Finally, P_1 may apply his attack against all $t+1$ honest players. Cheating just one of them is enough to get success. Therefore, taking into account the union bound, the successful probability for player P_1 is $\frac{t+1}{|\mathbb{F}|} = \epsilon$.

□

Share Size:
During the sharing phase, each party gets $2n+k-2$ elements from the field $\mathbb{F}$ of order p. So, $|V_i| = p^{2n+k-2}$ which is $\frac{(t+1)^{2n+k-3}|S|}{\epsilon^{2n+k-3}}$.

Remark 3.3. *The* seed $c_i = (d_{i,1}, \ldots, d_{i,k-1})$ *can not contain less than $k-1$ field elements. If this would be the case (say the* seed c_i *contained $k-2$ elements), then $k-1$ passive cheaters could use the equations*

$$g_{i,k}d_{k,0} + b_{i,k} = \alpha_i d_{k,1} + \alpha_i^2 d_{k,2} + \cdots + \alpha_i^{k-2} d_{k,k-2}$$

to solve Shamir share $d_{k,0}$ for player P_k, thus violating the perfect privacy property of Shamir secret sharing. This shows that "compression" to $k-1$ field elements is optimal.

4 Conclusion

We proposed a simple and efficient, with respect to both share size and computation, SSCI scheme for public cheater identification and optimal cheater resilience. To the best of our knowledge the proposed optimally resilient scheme is the most efficient with respect to share

size, among other existing computationally efficient scheme with optimal resilience, for the case of a single secret. It is an interesting open problem to design a computationally efficient and optimal cheater resilient SSCI scheme with *optimal* share size in the setting of public cheater identification.

References

[1] Araki T., Obana S.: *Flaws in some secret sharing schemes against cheating*. ACISP 2007, 122-132 (2007).

[2] Araki T.: *Efficient (k, n) threshold secret sharing schemes secure against cheating from n-1 cheaters*. ACISP 2007, 133-142 (2007).

[3] Blakley G.R.: *Safeguarding cryptographic keys*. AFIPS 1979, 313-317 (1979).

[4] Cevallos, A., Fehr, S., Ostrovsky, R., Rabani, Y.: *Unconditionally-secure robust secret sharing with compact shares*. EUROCRYPT 2012, 195-208 (2012).

[5] Cabello S., Padro C., Saez G.: *Secret sharing schemes with detection of cheaters for a general access structure*. Design Codes Cryptography, 25(2), 175-188 (2002).

[6] Carpentieri, M.: *A perfect threshold secret sharing scheme to identify cheaters*. Design Codes Cryptography 5(3), 183-187 (1995).

[7] Choudhury, A.: *Brief announcement: optimal amortized secret sharing with cheater identification*. PODC 2012, 101-102 (2012).

[8] Cramer R., Damgard I., Fehr S.: *On the cost of reconstructing a secret, or VSS with optimal reconstruction phase*. CRYPTO 2001, 503-523 (2001).

[9] Cramer R., Dodis Y., Fehr S., Padro C., Wichs D.: *Detection of algebraic manipulation with applications to robust secret sharing and fuzzy extractors*. EUROCRYPT 2008, 471-488 (2008).

[10] B. Chor, S. Goldwasser, S. Micali, and B. Awerbuch. *Verifiable Secret Sharing and Achieving Simultaneity in the Presence of Faults (Extended Abstract)*. FOCS 1985, 383-395 (1985).

[11] Feldman P. and Micali S.: *An Optimal Probabilistic Protocol for Synchronous Byzantine Agreement*. SIAM Journal on Computing, 26(4), 873-933 (1997).

[12] Ishai, Y., Ostrovsky, R., Seyalioglu, H.: *Identifying cheaters without an honest majority*. TCC 2012, 21-38 (2012).

[13] Johansson T., Kabatianskii G., Smeets B.: *On the relation between A-codes and codes correcting independent errors*. EUROCRYPT 93, 1-11 (1993).

[14] Kurosawa, K., Obana, S., Ogata, W.: *t-cheater identifiable (k, n) threshold secret sharing schemes*. CRYPTO 1995, 410-423 (1995).

[15] Martin K. M.: *Challenging the adversary model in secret sharing schemes*.

[16] McEliece, R., Sarwate, D.: *On sharing secrets and reed-solomon codes*. Commun. ACM 24(9), 583-584 (1981).

[17] Obana, S.: *Almost optimum t-cheater identifiable secret sharing schemes*. EUROCRYPT 2011, 284-302 (2011).

[18] Obana S., Araki T.: *Almost optimum secret sharing schemes secure against cheating for arbitrary secret distribution*. ASIACRYPT 2006, 364-379 (2006).

[19] Ogata W., Kurosawa K.: *Provably secure metering scheme*. ASIACRYPT 2000, 388-398 (2000).

[20] Ogata W., Kurosawa K., Stinson D. R.: *Optimum secret sharing scheme secure against cheating*. SIAM J. Discrete Math. 20(1), 79-95 (2006).

[21] Rabin, T., Ben-Or, M.: *Verifiable secret sharing and multiparty protocols with honest majority (extended abstract)*. STOC 1989, 73-85 (1989).

[22] Shamir A.: *How to share a secret*. Comm. ACM 22(11), 612-613 (1979).

[23] Tompa, M., Woll, H.: *How to share a secret with cheaters*. J. Cryptology 1(2), 133-138 (1988).

[24] Wegman M.N., Lawrence Carter J.: *New classes and applications of hash functions*. FOCS 1979, 175-182 (1979).

[25] Wegman M.N., Lawrence Carter J.: *New hash functions and their use in authentication and set equality*. Journal of Computer and System Science 22(3), 265-279 (1981).

[26] Xu R., Morozov K., Takagi T.: *On Cheater Identifiable Secret Sharing Schemes Secure Against Rushing Adversary*. IWSEC 2013, 258-271 (2013).