An Efficient Robust Secret Sharing Scheme with Optimal Cheater Resiliency

Partha Sarathi Roy[1]⋆, Avishek Adhikari[1] ⋆ ⋆⋆, Rui Xu[2]⋆⋆⋆, Kirill Morozov[3]†,
and Kouichi Sakurai[4] ⋆⋆

[1] Department of Pure Mathematics, University of Calcutta, India;
royparthasarathi0@gmail.com, avishek.adh@gmail.com
[2] Graduate School of Mathematics, Kyushu University, Japan;
r-xu@math.kyushu-u.ac.jp
[3] Institute of Mathematics for Industry, Kyushu University, Japan;
morozov@imi.kyushu-u.ac.jp
[4] Graduate School of Information Science and Electrical Engineering, Kyushu University, Japan;
sakurai@csce.kyushu-u.ac.jp

Abstract. In this paper, we consider the problem of (t, δ) robust secret sharing secure against rushing adversary. We design a simple t-out-of-n secret sharing scheme, which can reconstruct the secret in presence of t cheating participants except with probability at most δ, provided $t < n/2$. The later condition on cheater resilience is optimal for the case of public reconstruction of the secret, on which we focus in this work.

Our construction improves the share size of Cevallos et al. (EUROCRYPT-2012) robust secret sharing scheme by applying the "authentication tag compression" technique devised by Carpentieri in 1995. Our improvement is by a constant factor that does not contradict the asymptotic near-optimality of the former scheme. To the best of our knowledge, the proposed scheme has the smallest share size, among other efficient rushing (t, δ) robust secret sharing schemes with optimal cheater resilience.

Key words: Robust secret sharing, optimal cheater resiliency, rushing adversary.

⋆ Research supported in part by National Board for Higher Mathematics, Department of Atomic Energy, Government of India (No 2/48(10)/2013/NBHM(R.P.)/R&D II/695)

⋆⋆ The authors are thankful to DST, Govt. of India and JSPS, Govt. of Japan for providing partial support for this collaborative research work under India Japan Cooperative Science Programme (vide Memo no. DST/INT/JSPS/P-191/2014 dated May 27, 2014).

⋆⋆⋆ The author is supported by The China Scholarship Council, No. 201206340057.

† The author is supported by a *kakenhi* Grant-in-Aid for Young Scientists (B) 24700013 from Japan Society for the Promotion of Science.

1 Introduction

Secret sharing scheme is one of the key components in various cryptographic protocols and in particular distributed systems. Shamir [26] and Blakley [4] independently addressed this problem in 1979 when they introduced the concept of the threshold secret sharing. A (t, n) *threshold scheme* is a method where n pieces of the secret, called *shares* are distributed to n participants so that the secret can be reconstructed from the knowledge of any $t + 1$ or more shares, while it cannot be reconstructed from the knowledge of fewer than $t + 1$ shares, where $t + 1 \leq n$. More formally, in a secret sharing scheme, there exist 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 (t, 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 $t+1$) pool their shares to reconstruct the secret.

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

1. **Correctness:** Any set of $t + 1$ or more parties can reconstruct the secret by pooling their shares.
2. **Secrecy:** Any set of t or less participants can not reconstruct the secret. Moreover, for $perfect\ secrecy$, any set of t or less participants will have no information regarding the secret.

In the basic form of secret sharing schemes, it was assumed that everyone involved with the protocol is semi-honest. But for the real life scenario, this assumption may not hold good due to the presence of adversary. This idea leads to the development of secret sharing under various adversarial models. It may happen that some participants behave maliciously during the execution of the protocol. Malicious participants may submit incorrect shares resulting in incorrect secret reconstruction. Secret sharing schemes that either detect or identify participants who submit incorrect shares during the recovery of secret have been extensively studied. Tompa and Woll [28] first presented a cheater-detecting secret sharing scheme and this work is followed by several other works (for example, [1], [2], [11], [6], [23], [24]). McEliece and Sarwate [21] were the first to point out cheater identification in secret sharing schemes and this work is followed by several other works (for example, [17], [22], [8], [31]). Verifiable secret sharing schemes [12] have been proposed for environments where the shares given to participants by the dealer may not be correct i.e., the dealer of these shares may be corrupted. These typically involve protocols that can be performed by various subsets of participants in order to check that the shares they possess are consistent in some sense. While such schemes make it apparent that cheating has occurred, they do not necessarily permit honest participants to recover the correct secret. This observation led to *robust secret sharing schemes* [25]. Informally, robust secret sharing schemes allow the correct secret to be recovered even when some of the shares presented during an attempted reconstruction are incorrect. In this paper, we deal with robust secret sharing schemes. More specifically, we show that the share size in Cevallos et al. scheme [5] can be further reduced.

1.1 State of The Art & Our Contribution

In case of up to t cheaters among n ($\geq 3t+1$) participants, it was observed by McEliece and Sarwate [21] that Shamir secret sharing scheme [26] is robust via its connection to Reed-Solomon codes. However, for the case when $n = 2t+1$, the above observation does not work. One solution to this problem, considered e.g., by Rabin and Ben-Or [25] is for the dealer to authenticate shares using some message authentication code [30].

In perfectly secure (even not robust) secret sharing schemes, the size of a share is at least that of the secret. Therefore, the main point in optimization of robust secret sharing is to reduce the *overhead* needed for ensuring robustness while efficiently reconstructing the secret. If efficient reconstruction is not required and $n \geq 2t+2$ then one may use the ideal (i.e. without any overhead) scheme by Jhanwar and Safavi-Naini [15]. The case $n \geq 2t+1$ can also be handled by the scheme of Cramer et al. [9] which features a constant overhead. Finally, a (quasi-)linear overhead in the number of players and the security parameter with efficient reconstruction was achieved by Cevallos et al. [5].

In this paper, we show that the overhead in Cevallos et al. scheme [5] can be further reduced by applying an authentication tag compression technique by Carpentieri [7]. The later technique was in fact proposed for improving the share size of the Rabin and Ben-Or scheme [25], which was a basis of Cevallos et al. construction. Since the scheme [5] is nearly-optimal, we achieve a constant factor improvement in the overhead. For example, for $t \leq 2$ we improve the overhead of Cevallos et al. by the factor of about 2/3.

Table 1. Comparison of Our Proposal to Existing Efficient Robust Secret Sharing Schemes.

Scheme	Overhead (bits)
Rabin and Ben-Or [25]	$3nk$
Cevallos et al. [5]	$3nq$
Proposed	$(2n+t-2)q$

Here, k is the security parameter and q, which depends on k, is the parameter associated with the overhead (more specifically, the elements used to authenticate shares are chosen from the field of size 2^q).

1.2 Applications of Robust Secret Sharing Schemes

In the information-theoretically secure setting, the most natural application of robust secret sharing is related to the distributed information storage, such as for instance, secure cloud storage. User's data can be stored with several storage providers in a shared form. Clearly, an ordinary Shamir secret sharing provides protection against *passive* attacks where unqualified coalitions of storage providers may try to recover the secret. Also, reliability is ensured such that an information loss at several (few enough) providers does not hinder the reconstruction. However, in case of *active* attacks, when provider(s) deliberately submit incorrect shares, the recovery of a correct secret becomes crucial – and this is exactly the scenario [29, 18], where robust secret sharing manifests its importance.

Moreover, robust secret sharing is also related to Secure Message Transmission (SMT) protocols [13, 20]. Here, the sender is connected with the receiver by n distinct channels, t of which are controlled by an adversary. SMT realizes a private and reliable transmission in this setting. Finally, the techniques used in robust secret sharing schemes may also be applied to realizing verifiable secret sharing and secure multi party computation [25].

1.3 Roadmap

In section 2, the necessary prerequisites for the proposed construction are provided. In section 3, we discuss the related definition, the adversarial model and authentication techniques. In section 4, our construction along with its security proof is provided and finally we conclude in section 5.

2 Preliminaries

2.1 Message Authentication Codes

Carter and Wegman [30] invented unconditionally secure message authentication code which is a tool that enables to verify the integrity of a message without assuming any computational hardness.

Definition 1. *A message authentication code (or MAC) for a finite message space $\mathcal{M}$ consists of a function $MAC : \mathcal{M} \times \mathcal{K} \rightarrow \mathcal{T}$ for finite sets $\mathcal{K}$ and $\mathcal{T}$. It is called ϵ-secure if for all $m, m' \in \mathcal{M}$ with $m \neq m'$ and for all $\tau, \tau' \in \mathcal{T}$:*

$$P[MAC(m', K) = \tau' | MAC(m, K) = \tau] \leq \epsilon,$$

where the random variable K is uniformly distributed over $\mathcal{K}$.

Example: $MAC : \mathbb{F} \times \mathbb{F}^2 \rightarrow \mathbb{F}$ with $(m, (\alpha, \beta)) \rightarrow \alpha.m + \beta$ is a ϵ-secure MAC with $\epsilon = 1/|\mathbb{F}|$, where $\mathcal{M}$ is a finite field $\mathbb{F}$.
More generally, as first shown in [10], [16], [27]

$$MAC : \mathbb{F}^l \times \mathbb{F}^2 \rightarrow \mathbb{F}, ((m_1, \ldots, m_l), (\alpha, \beta)) \rightarrow \Sigma_{k=1}^{l} \alpha^i.m_i + \beta \qquad (1)$$

is a ϵ-secure MAC with $\epsilon = l/|\mathbb{F}|$.

2.2 The Reed-Solomon Code

Let $(a_0, \ldots, a_t) \in \mathbb{F}^{t+1}$ and $f(x) = a_0 + a_1 x + \ldots + a_t x^t \in \mathbb{F}[X]$ be a polynomial of degree at most t. Let $x_1, x_2, \ldots, x_n \in \mathbb{F}\backslash\{0\}$, for $n > t$, be distinct elements. Then $C = (f(x_1), f(x_2), \ldots, f(x_n))$ is a codeword of Reed-Solomon error correcting code [19] of the message $(a_0, \ldots, a_t)$. Reed-Solomon code can correct up to e erroneous symbols, i.e. when e out of n evaluation points $f(x_i)$ $(1 \leq i \leq n)$ are manipulated, the polynomial (i.e., the message) can be uniquely determined if and only if $n \geq t+1+2e$. Note that there exist efficient algorithms implementing Reed-Solomon decoding, such as Berlekamp-Welch algorithm [3].

3 (t, δ) Robust Secret Sharing Scheme

In a (t, δ) *robust secret sharing scheme*, there exists a set of n participants, denoted by $\mathcal{P} = \{P_1, \ldots, P_n\}$ and two special participants called the dealer and the reconstructor, denoted by $\mathcal{D}$ and $\mathcal{R}$ respectively. A (t, δ) robust 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, which is known as *share*, to each participant.
2. **Reconstruction Phase:** In this phase, all the participants communicate their shares to the reconstructor.

In the sharing phase the dealer, in presence of an adversary $\mathcal{A}$ who can corrupt at most t participants, wants to share the secret s ($\in$ *secret space*) in such a way that satisfies the following two conditions:

1. **Privacy:** Before reconstruction phase is started, the adversary has no more information on the shared secret s than he had before the execution of sharing phase. This is called *perfect* privacy.
2. **Reconstructibility:** At the end of reconstruction phase, the reconstructor $\mathcal{R}$ outputs $s = s'$ except with probability at most δ.

3.1 Adversarial Model

The dealer $\mathcal{D}$ and the reconstructor $\mathcal{R}$ are assumed to be honest. The dealer delivers the shares to respective participants over point-to-point private channels.

We assume that $\mathcal{A}$ is computationally unbounded, active, adaptive, rushing adversary who can corrupt up to $t < n/2$ participants (but neither $\mathcal{D}$ nor $\mathcal{R}$). Once a participant P_i is corrupted, the adversary learns her share and internal state. Moreover from that point onwards, $\mathcal{A}$ has full control over P_i. By being *active*, we mean that $\mathcal{A}$ can deviate from the protocol in an arbitrary manner. By being *adaptive*, we mean that after each corruption, $\mathcal{A}$ can decide on whom to corrupt next, depending on the information she has obtained so far. During the reconstruction phase, the adversary gets to see the communication between all participants P_i and the reconstructor $\mathcal{R}$. By assumption, the adversary controls the information that the corrupted participants send to $\mathcal{R}$. By being *rushing* we mean that in every communication round, $\mathcal{A}$ can decide the messages of corrupted participants after seeing the messages of honest participants.

Note that assuming $\mathcal{R}$ to be honest is equivalent to assuming a broadcast channel available to each participant. In the later case, each participant simply broadcasts her share, executes the reconstruction algorithm and output the result.

3.2 Share Authentication

Suppose the dealer $\mathcal{D}$ wants to share the secret s with the help of a polynomial $f(x)$ of degree at most t over a finite field $\mathbb{F}$ as in Shamir scheme [26]. 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 can alter the original share at the time of reconstruction, the correctness may not hold good.

Let s_i be the Shamir share for the player P_i. For every pair of players P_i and P_j, P_i's Shamir share s_i is authenticated to the player P_j with an authentication tag $\tau_{i,j}$ obtained by message authentication code, where the corresponding authentication key $k_{j,i}$ is held by player P_j. Specifically, this step may be done by choosing $k_{j,i} = (g_{j,i}, b_{j,i})$ uniformly at random from $\mathbb{F} \times \mathbb{F}$ and then computing $\tau_{j,i} = s_i g_{j,i} + b_{j,i}$.

This similar method was used by Rabin and Ben-Or [25], but Carpentieri [7] observed that the authentication tags can be compressed as follows. Instead of first choosing the authentication key and then calculating the authentication tag, one may first fix the authentication tag and then may find the authentication key.

In Rabin and Ben-Or setting, for pairwise authentication, each player will get $n-1$ keys and $n-1$ tags. By using the above trick, one may, 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 $c_i = (d_{i,1}, \ldots, d_{i,t})$, where $d_{i,j}$ for $j \in \{1, \ldots, t\}$ is randomly chosen from $\mathbb{F}$ and the authentication tag of P_i against P_j's key is $\tau_{i,j} = \alpha_i d_{j,1} + \alpha_i^2 d_{j,2} + \cdots + \alpha_i^t d_{j,t}$. Compared to the setting of Rabin and Ben-Or, each player now gets a *seed* of t field elements from which the $n-1$ authentication tags are generated. Thus, the share size of each player is reduced by $n-t-1$ field elements.

4 Optimal Cheater Resilient Robust Secret Sharing with Improved Share Size

The paper [5] can be considered as an adaptation of the Rabin and Ben-Or [25] scheme with modified reconstruction technique (against rushing adversary). In our proposal, we use the share authentication method derived from that of [7] (as described in the previous section) and adapt it to the reconstruction technique of [5].

4.1 Proposed Scheme

- **Initialization:** For $i = 1, \ldots, n$, let the distinct elements $\alpha_i \in \mathbb{F}_{2^m} \setminus \{0\}$ be fixed and public. Moreover, let α_i be also non-zero and distinct in $\mathbb{F}_{2^q}$, where m, q are two positive integers and the cardinalities of both fields are larger than n.
- **Sharing Phase:**
  - The dealer $\mathcal{D}$ chooses randomly a polynomial $f(x) \in \mathbb{F}_{2^m}[X]$ of degree at most t, where $f(0) = s$ is the secret to be shared, and computes $f(\alpha_i) = s_i$ in $\mathbb{F}_{2^m}$, where $i = 1, \ldots, n$.
  - If $q < m$, we let $l = m/q$ (for simplicity, assuming that l is an integer) and $s_j = s_{j,1}|| \ldots ||s_{j,l}$.
    $\mathcal{D}$ chooses randomly $d_{i,1}, \ldots, d_{i,t}$ and $g_{i,j}$ from F_{2^q}, and computes
    $b_{i,j} = \begin{cases} g_{i,j}s_j + \Sigma_{k=1}^{t}\alpha_i^k d_{j,k} \text{ for } q \geq m \\ \Sigma_{k=1}^{l} g_{i,j}^k s_{j,k} + \Sigma_{k=1}^{t}\alpha_i^k d_{j,k} \text{ for } q < m \end{cases}$
    where $j = 1, \ldots, i-1, i+1, \ldots, n$ and $i = 1, \ldots, n$.

  - $\mathcal{D}$ privately sends to each P_i the share

$$S_i = (s_i, d_{i,1}, \ldots, d_{i,t}, g_{i,1}, \ldots, g_{i,i-1}, g_{i,i+1}, \ldots, g_{i,n},$$
$$b_{i,1}, \ldots, b_{i,i-1}, b_{i,i+1}, \ldots, b_{i,n}).$$

- **Reconstruction Phase:**
  - **Round 1:** Each P_i sends $(s'_i, d'_{i,1}, \ldots, d'_{i,t})$ to the reconstructor $\mathcal{R}$.
  - **Round 2:** Each P_i sends
    $(g'_{i,1}, \ldots, g'_{i,i-1},\ g'_{i,i+1}, \ldots,\ g'_{i,n},\ b'_{i,1}, \ldots, b'_{i,i-1}, b'_{i,i+1}, \ldots, b'_{i,n})$
    to the reconstructor $\mathcal{R}$.
  - **Computation by $\mathcal{R}$:**
    1. $\mathcal{R}$ sets v_{ij}, $i, j \in \{1, 2. \ldots, n\}$, to be 1 if P_i's authentication tag is accepted by P_j, i.e., if $b'_{i,j} = \begin{cases} g'_{i,j}s'_j + \Sigma_{k=1}^{t}\alpha_i^k d'_{j,k} \text{ for } q \geq m \\ \Sigma_{k=1}^{l} {g'}_{i,j}^{k} s'_{j,k} + \Sigma_{k=1}^{t}\alpha_i^k d'_{j,k} \text{ for } q < m \end{cases}$,
       otherwise she sets v_{ij} to 0.
    2. $\mathcal{R}$ computes the largest set $\mathcal{I} \subseteq \{1, 2, \ldots, n\}$ with the property that
       $$\forall i \in \mathcal{I} : |\{j \in \mathcal{I} | v_{ij} = 1\}| = \Sigma_{j \in \mathcal{I}} v_{ij} \geq t + 1.$$
       Clearly, $\mathcal{I}$ contains all honest participants. Let $e = |\mathcal{I}| - (t+1)$ be the maximum number of corrupted participants in $\mathcal{I}$.
    3. Using the error correction algorithm for Reed-Solomon code, $\mathcal{R}$ computes a polynomial $f(x) \in \mathbb{F}_{2^m}[X]$ of degree at most t such that $f(\alpha_i) = s'_i$ for at least $(t+1) + \frac{e}{2}$ participants i in $\mathcal{I}$.
       If no such polynomial exists then output $\perp$,
       otherwise, output $s = f(0)$.

Remark 1. In the proposed scheme, a tradeoff between cheating probability and share size can be arranged. So, within the natural restrictions, the parameters can be set flexibly. Hence, q can be smaller or larger than m.

4.2 Security Proof

Lemma 1. *The above scheme provides perfect secrecy, i.e. the adversary $\mathcal{A}$ controlling any t participants 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 t in x, and the share of each P_i is

$$S_i = (s_i, d_{i,1}, \dots, d_{i,t}, g_{i,1}, \dots, g_{i,i-1}, g_{i,i+1}, \dots, g_{i,n},\\ b_{i,1}, \dots, b_{i,i-1}, b_{i,i+1}, \dots, b_{i,n}).$$

Without loss of generality, we may assume that the first t participants $P_1, \dots, P_t$ are under $\mathcal{A}$'s control. Now, according to *Lagrange's interpolation*, $t+1$ such values s_i fully define a degree-t polynomial. Thus, we need to choose one more s_i, where $i \in \{1, 2, \dots, n\} \setminus L$ and $L = \{1, 2, \dots, t\}$. Without loss of generality, we may assume that $i = t+1$. Let us now estimate the information regarding s_{t+1} which is available to each P_i, $i \in L$, via $(g_{i,t+1}, b_{i,t+1})$.

Case 1 $(q \geq m)$**:**

For all $i \in L$,

$$b_{i,t+1} = g_{i,t+1}s_{t+1} + \alpha_i d_{t+1,1} + \alpha_i^2 d_{t+1,2} + \cdots + \alpha_i^t d_{t+1,t}.$$

So, for all $i \in L$,

$$b_{i,t+1} - g_{i,t+1}s_{t+1} = \alpha_i d_{t+1,1} + \alpha_i^2 d_{t+1,2} + \cdots + \alpha_i^t d_{t+1,t}.$$

Note that the above system of linear equations is associated with the following matrix, which is non-singular in $\mathbb{F}_{2^q}$:

$$\begin{bmatrix} \alpha_1 \ \alpha_1^2 \dots \alpha_1^t \\ \alpha_2 \ \alpha_2^2 \dots \alpha_2^t \\ \dots\dots\dots\dots \\ \alpha_t \ \alpha_t^2 \dots \alpha_t^t \end{bmatrix}.$$

It is trivial to see that the linear system is consistent for all possible values of s_{t+1}. Now, we conclude that $\mathcal{A}$ can guess the correct s_{t+1} with probability at most $\frac{1}{2^m}$ as $s_{t+1} \in \mathbb{F}_{2^m}$.

Case 2 $(q < m)$**:**
For all $i \in L$,

$$b_{i,t+1} = \Sigma_{k=1}^{l} g_{i,t+1}^k s_{t+1,k} + \Sigma_{k=1}^{t} \alpha_i^k d_{t+1,k}.$$

Here $q < m$, $l = m/q$ (for simplicity, l is assumed to be an integer) and $s_j = s_{j,1}|| \dots ||s_{j,l}$. So, for all $i \in L$,

$$b_{i,t+1} - \Sigma_{k=1}^{l} g_{i,t+1}^{k} s_{t+1,k} = \Sigma_{k=1}^{t} \alpha_i^k d_{t+1,k}.$$

Now, for any fixed value of $s_{t+1} = s_{t+1,1}|| \dots ||s_{t+1,l}$, we can use the same argument as in Case 1 in order to show that the probability for $\mathcal{A}$ to guess s_{t+1} correctly is at most $(1/2^q)^l = 1/2^m$.

Lemma 2. *Any corrupted participant P_i who submits $s'_i \neq s_i$ in Round 1 of the reconstruction phase will be accepted by an honest participant with probability at most* $\epsilon = \begin{cases} \frac{1}{2^q} \text{ for } q \geq m \\ \frac{l}{2^q} \text{ for } q < m \end{cases}$.

Proof: Without loss of generality, we assume that the corrupted participant is P_1 who submits $s'_i \neq s_i$ in Round 1 of the reconstruction phase.
Case 1 ($q \geq m$):
P_1 will be accepted by honest P_j if $b_{j,1} = g_{j,1}s'_1 + \alpha_j d'_{1,1} + \alpha_j^2 d'_{1,2} + \dots + \alpha_j^t d'_{1,t}$. Thus P_1 has to guess $g_{j,1}$ correctly. Now, let

$$g_{j,1}s'_i + \Sigma_{k=1}^{t} \alpha_j^k d'_{1,k} = g_{j,1}s_i + \Sigma_{k=1}^{t} \alpha_j^k d_{1,k}.$$

Then,

$$g_{j,1} = (s'_1 - s_1)^{-1} \Sigma_{k=1}^{t} \alpha_j^k (d_{1,k} - d'_{1,k}).$$

Note that $g_{j,1}$ is independent of all information that the adversary $\mathcal{A}$ has obtained and $g_{j,1} \in \mathbb{F}_{2^q}$. Thus, P_1 will be accepted by P_j with probability at most $\frac{1}{2^q} \geq Pr(v_{1j} = 1)$. Therefore, any dishonest participant P_i submitting $s'_i \neq s_i$ in Round 1 of the reconstruction phase will be accepted by a honest participant P_j with probability $Pr(v_{ij} = 1) \leq 1/2^q$.
Case 2 ($q < m$):
P_1 will be accepted by honest P_j if $b_{j,1} = \Sigma_{k=1}^{l} {g'}_{j,1}^{k} s'_{1,k} + \Sigma_{k=1}^{t} \alpha_j^k d'_{1,k}$. As $s_1 \neq s'_1$, at least one of $s_{1,k} \neq s'_{1,k}$. Assume that only one $s_{1,k} \neq s'_{1,k}$. So, as in Case 1, P_1 will be accepted by P_j with probability at most $\frac{1}{2^q} \geq Pr(v_{1j} = 1)$. Taking into account the union bound, P_1 will be accepted by P_j with probability at most $\frac{l}{2^q} \geq Pr(v_{1j} = 1)$. Therefore, any dishonest participant P_i submitting $s'_i \neq s_i$ in Round 1 of the reconstruction phase will be accepted by a honest participant P_j with probability $Pr(v_{ij} = 1) \leq l/2^q$.

Theorem 1. *For any positive integer t such that $n = 2t + 1$, the proposed construction forms (t, δ)-robust secret sharing scheme for n participants with the space of secrets $\mathbb{F}_{2^m}$ and*

$$\delta \leq e.((t+1)\epsilon)^{(t+1)/2}$$

where $e = exp(1)$ and $\epsilon = \begin{cases} \frac{1}{2^q} \text{ for } q \geq m \\ \frac{l}{2^q} \text{ for } q < m \end{cases}$.

Proof:
Privacy: Follows from Lemma 1.
Reconstructability: From Lemma 2, we have found that $Pr(v_{ij} = 1) \leq \epsilon$. The rest of the proof is the same as in [5, Theorem 3.1].

4.3 Discussion

Let us compute the share size. During the sharing phase, each party gets one element from $\mathbb{F}_{2^m}$ and $2n+t-2$ elements from $\mathbb{F}_{2^q}$. Therefore, the share size of each participant is $m + (2n+t-2)q$ bits.

Consider the following instantiation. By Theorem 1, the resulting secret sharing scheme is δ-robust for $\delta \leq e.((t+1)\epsilon)^{(t+1)/2}$. Therefore, for a given security parameter k, setting $q = \begin{cases} \lceil \log(t+1) + \frac{2}{t+1}(k + \log(e)) \rceil \text{ for } q \geq m \\ \lceil \log(t+1) + \log(l) + \frac{2}{t+1}(k + \log(e)) \rceil \text{ for } q < m \end{cases}$, we obtain $\delta \leq 2^{-k}$.

Every perfectly secure secret sharing scheme must have the share size at least that of the secret. The first term in the sum is responsible for this, while the second term characterizes an overhead required for the share authentication. In Table 1, we compare the overhead of our scheme with those of the schemes by Rabin and Ben-Or [25], and Cevallos et al [5]. We can see that when $t \leq 2$, our scheme reduces the overhead by the factor about 2/3 as compared to that of Cevallos et al.

5 Conclusion

We have shown and analyzed a new robust secret sharing scheme, which combines the techniques of [7] and [5] with an improvement of share size over the robust secret sharing scheme of [5]. The scheme of [5] has nearly-optimal share size, so that our improvement is by a constant factor. To the best of our knowledge, the proposed scheme has the smallest share size, among other efficient (t, δ) robust secret sharing schemes with optimal cheater resilience, secure against rushing adversary.

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. Berlekamp, E.R., Welch, L.R.: *Error correction of algebraic block codes.* U.S. Patent Number 4, 633.470 (1986)
4. Blakley G.R.: *Safeguarding cryptographic keys.* AFIPS 1979, 313-317 (1979)
5. Cevallos, A., Fehr, S., Ostrovsky, R., Rabani, Y.: *Unconditionally-secure robust secret sharing with compact shares.* EUROCRYPT 2012, 195-208 (2012)
6. 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)
7. Carpentieri, M.: *A perfect threshold secret sharing scheme to identify cheaters.* Design Codes Cryptography 5(3), 183-187 (1995)
8. Choudhury, A.: *Brief announcement: optimal amortized secret sharing with cheater identification.* PODC 2012, 101-102 (2012)
9. Cramer R., Damgard I., Fehr S.: *On the cost of reconstructing a secret, or VSS with optimal reconstruction phase.* CRYPTO 2001, 503-523 (2001)

10. Den Boer, B.: *A simple and key-economical unconditional authentication scheme.* Journal of Computer Security 2, 65-72 (1993)
11. 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)
12. Chor, B., Goldwasser, S., Micali, S., and Awerbuch, B.: *Verifiable Secret Sharing and Achieving Simultaneity in the Presence of Faults (Extended Abstract).* FOCS 1985, 383-395 (1985)
13. Dolev, D., Dwork, C., Waarts, O., Yung, M.: *Perfectly secure message transmission.* FOCS 1990, 36-45 (1990). Journal version in J. ACM 40(1), 17-47 (1993)
14. Ishai, Y., Ostrovsky, R., Seyalioglu, H.: *Identifying cheaters without an honest majority.* TCC 2012, 21-38 (2012)
15. Mahabir Prasad Jhanwar, Reihaneh Safavi-Naini: Unconditionally-secure ideal robust secret sharing schemes for threshold and multilevel access structure. J. Mathematical Cryptology 7(4), 279-296 (2013)
16. Johansson T., Kabatianskii G., Smeets B.: *On the relation between A-codes and codes correcting independent errors.* EUROCRYPT 93, 1-11 (1994)
17. Kurosawa, K., Obana, S., Ogata, W.: *t-cheater identifiable (k, n) threshold secret sharing schemes.* CRYPTO 1995, 410-423 (1995)
18. Lakshmanan, S., Ahamad, M., Venkateswaran, H.: *Responsive security for stored data.* IEEE Trans. Parallel Distrib. Syst. 14(9), 818-828 (2003)
19. MacWilliams, F. J., Sloane, N. J. A.: *The theory of error-correcting codes* (Vol. 16). Elsevier (1977)
20. Martin, K.M., Paterson, M.B., Stinson, D.R.: *Error decodable secret sharing and one-round perfectly secure message transmission for general adversary structures.* Cryptography and Communications 3(2), 65-86 (2011)
21. McEliece, R., Sarwate, D.: *On sharing secrets and reed-solomon codes.* Commun. ACM 24(9), 583-584 (1981)
22. Obana, S.: *Almost optimum t-cheater identifiable secret sharing schemes.* EUROCRYPT 2011, 284-302 (2011)
23. Obana S., Araki T.: *Almost optimum secret sharing schemes secure against cheating for arbitrary secret distribution.* ASIACRYPT 2006, 364-379 (2006)
24. Ogata W., Kurosawa K., Stinson D. R.: *Optimum secret sharing scheme secure against cheating.* SIAM J. Discrete Math., 20(1), 79-95 (2006)
25. Rabin, T., Ben-Or, M.: *Verifiable secret sharing and multiparty protocols with honest majority (extended abstract).* STOC 1989, 73-85 (1989)
26. Shamir A.: *How to share a secret.* Comm. ACM 22(11), 612-613 (1979)
27. Taylor, R.: *An Integrity Check Value Algorithm for Stream Ciphers.* CRYPTO 1993, 40-48 (1994)
28. Tompa, M., Woll, H.: *How to share a secret with cheaters.* J. Cryptology 1(2), 133-138 (1988)
29. Waldman, M., Rubin, A.D., Cranor, L.F.: *The architecture of robust publishing systems.* ACM Trans. Internet Techn. 1(2), 199-230 (2001)
30. Wegman M.N., Lawrence Carter J.: *New classes and applications of hash functions.* FOCS 1979, 175-182 (1979)
31. Xu R., Morozov K., Takagi T.: *On Cheater Identifiable Secret Sharing Schemes Secure Against Rushing Adversary.* IWSEC 2013, 258-271 (2013)