Unconditionally-Secure Robust Secret Sharing with Minimum Share Size

Mahabir Prasad Jhanwar and Reihaneh Safavi-Naini

Department of Computer Science
University of Calgary, Canada

Abstract. An n-player (t, δ)-secure threshold robust secret sharing scheme is a (t, n)-threshold secret sharing scheme with the additional property that the secret can be recovered, with probability at least $1-\delta$, from the set of *all* shares even if up to t players provide incorrect shares. The existing constructions of threshold robust secret sharing schemes for the range $n/3 \leq t < n/2$ have the share size larger than the secret size. An important goal in this area is to minimize the share size. In the paper, we propose a new unconditionally-secure threshold robust secret sharing scheme for the case $n \geq 2t + 2$ with share size equal to the secret size. This is the minimum possible size as dictated by the perfect secrecy of the scheme.

Keywords: Shamir secret sharing, robust secret sharing, secret sharing with cheating detection.

1 Introduction

Secret Sharing is one of the most important tools in modern cryptography. The concept and the first realization of secret sharing were presented independently in [24] and in [3]. In a secret sharing scheme, there exists a dealer, n participants, and possibly a reconstructor. The dealer splits a secret $s \in S$, into n pieces, called shares, and sends one share to each participant over a private point-to-point channel. An access structure is the set of subsets of participants that are qualified to recover the secret. In a (t, n)-threshold access structure, where $1 \leq t < n$, any $t + 1$ or more participants can reconstruct the secret, and the knowledge of t or less shares leaves the secret s indeterminate. A (t, n)-threshold secret sharing scheme is said to be *perfect* if no subset of t or less shares can leak any information about the secret s where the leakage is in information theoretic sense and without assuming any limit on the computational resources of the adversary.

In its basic form, secret sharing assumes that the corrupted participants are passive (or semi-honest) and follow the protocol during the reconstruction phase. Extensions of this basic model considers cases that the corrupted participants deviate from the protocol [19,27,22,4,6,20]. In these extensions different requirements such as cheater detection [4], cheater identification [20] and untrusted

A.-R. Sadeghi (Ed.): FC 2013, LNCS 7859, pp. 96–110, 2013.

dealer [8] have been considered. A minimal robust requirement when participants are allowed to submit incorrect shares, is that the set of all shares, some possibly corrupted, can recover the correct secret. Perfect secret sharing schemes that satisfy this additional property are called *robust secret sharing schemes.*

Threshold robust secret sharing schemes provide a powerful tool for building secure and reliable distributed data storage systems. Users' data (files) can be broken into pieces (shares) and stored on multiple servers such that privacy of data against servers is provided, and the system ensures recovery of the data when a subset of servers corrupt their stored shares, accidentally or intentionally. In recent years, systems and architectures based on this primitive have emerged [16,28,11] which shows importance of robust secret sharing in practice. Threshold robust secret sharing has also direct application to Secure Message Transmission (SMT). In an unconditionally secure SMT [10,12,13], a sender is connected to a receiver through n wires such that up to t of which are controlled by an adversary. The goal of an SMT protocol is to ensure that the message sent by the sender is received correctly by the receiver, and no information about the message is leaked to the adversary. Good threshold robust secret sharing schemes lead to good secure message transmission schemes [18]. Robust secret sharing schemes may also be seen as an stepping stone towards the construction of verifiable secret sharing (VSS) schemes [8], in which, in addition to the corrupted players, the dealer is dishonest and may hand out inconsistent shares. Finally robust secret sharing is an important primitive for secure multi-party computation.

1.1 Motivation

In perfect threshold robust secret sharing schemes, in addition to the requirement of perfect threshold secret sharing schemes,

- any $t+1$ shares reconstruct the secret, and any t shares give no information about the secret,

it is also required that,

- the secret can be reconstructed with high probability from the set of all shares, even if up to t shares are incorrect.

The reconstruction may be with, or without, a reconstructor, and may include one or more rounds of communication [9,7]. Also, reconstruction failure may be defined differently [9,7]. These variations of the model needs careful considerations in comparing schemes and their performances. A framework for considering robust secret sharing is provided in [23], which includes schemes in both the information-theoretic and computationally secure settings.

In this paper we shall follow the model of [7], where during the reconstruction, all the n players communicate their shares to a trusted third party called the reconstructor. Based on the received shares (some of them are incorrect), the reconstructor then produces an output s', which with a probability at least $1-\delta$ is the same as the original secret s.

Important efficiency measures for robust secret sharing schemes are the communication cost (number of communicated bits) of reconstruction [9] and the share size measured by the number of bits required to represent a share. In this paper we focus on the latter measure. It is well known that in any perfect secret sharing scheme, the length of a share σ_i is at least the length of the secret, that is $\log |S|$ [25]. Secret sharing schemes that meet this lower bound are called ideal [25]. Shamir secret sharing meets this lower bound and is ideal. This lower bound also holds for robust secret sharing scheme which are perfect secret sharing schemes. So a natural question is how much *redundancy*, that is extra share length compared to the secret length, is needed for robustness.

It follows from the theory of Reed-Solomon error correcting codes that Shamir secret sharing scheme is robust if (and only if) $t < n/3$ [1] and so no increase in the share size is needed to obtain robustness. On the other hand, the robust secret sharing is impossible if $t \geq n/2$: the (t, n)-threshold access structure requires at least $(t+1)$ correct shares for the recovery of the original secret. The interesting range is $n/3 \leq t < n/2$. In this range, all existing schemes have share sizes that are strictly larger than the secret size. The problem is naturally more difficult when t is maximal in the range $n/3 \leq t < n/2$ i.e., $n = 2t + 1$ (when n is odd) and $n = 2t + 2$ (when n is even). In particular, for the range $n/3 \leq t < n/2$, there is no known threshold robust secret sharing scheme such that,

- the maximum length of individual share size of a participant is the *same* as the secret size (thus no increase in the share size), and the *probability of correctly recovering the secret from the set of all shares* is at least $1 - \delta$, where δ is a negligible value.

This is irrespective of the computational complexity of reconstruction which can be exponential in n. The result of this paper shows that it is possible to keep the share size same as the secret size when $n \geq 2t + 2$.

1.2 Our Contribution

We consider the model of [7] in which reconstruction is by a trusted reconstructor, and propose a new construction of robust secret sharing which is based on Shamir's secret sharing and has share size equal to the secret size, which is the minimum required by perfect secret sharing schemes. That is, the extra robustness property is obtained without increasing the share size. The system's public parameter, in addition to what is required by Shamir's scheme, includes a structured matrix that has $O(n)$ random elements. This matrix can be distributed during share distribution, or stored on an authenticated and publicly accessible storage. The system works for $n \geq 2t + 2$ and effectively uses the share of the extra participants as the verification information. We note that if n is even, then $n = 2t + 2$ is the minimum required number of participants.

The reconstruction is one round and requires participants to send their shares to the reconstructor. The reconstruction is secure against a non-rushing adversary (this is properly defined in Sect. 2.2), and the reconstruction procedure may output an incorrect secret with a negligible probability. The reconstruction

algorithm however is inefficient and requires that all subsets of size $t+1$ of n shares be considered. Construction of schemes with the above properties and efficient reconstruction, remains an open problem.

1.3 Related Work

Cheating detection and providing robustness against cheaters, is an important problem in secret sharing schemes. Different models and constructions have been proposed for this problem over the year [22,4,6,19,27,20]. Robustness in the sense of recoverability of the secret when some shares are wrong is a basic property that ensures the secret is not lost because of the share corruption. Robust secret sharing with unconditional security was first considered by McEliece and Sarwate [19] where they pointed out the close relationship between Shamir secret sharing scheme and Reed-Solomon coding. Little is known about robust secret sharing for the range $n/3 \leq t < n/2$. The first scheme for the range $n/3 \leq t < n/2$ is due to Rabin and BenOr [22]. Their scheme consists of Shamir secret sharing, but enhanced by means of an unconditionally secure message authentication code. The constructions in [9,7] represent the two main approaches to this problem and provide the best performances in terms of trade-off results between share size and the reconstruction complexity (see Sect. 5 for their description). In [9], the redundancy of the share size is exactly two field elements (here $n = 2t+1$, secert size is one field element, and the reconstruction model is different). The reconstruction time is however exponential in n. The scheme in [7] has the smallest share size (see Sect. 6) among schemes with efficient (polynomial) reconstruction.

2 Preliminaries

We begin by formally defining the model of threshold robust secret sharing. The "definitions" are taken verbatim from [7].

2.1 Robust Secret Sharing

A threshold robust secret sharing scheme can be described by two interactive protocols, Share and Rec, where Share involves a dealer D and n players $P_1, \ldots, P_n$, and Rec involves the n players and a reconstructor R. The dealer is connected to every player by a secure, untappable channel. There is also a broadcast channel that can be used by everyone in the system. An n-player threshold robust secret sharing scheme for a secret space $\mathcal{S}$ consists of two phases, the *sharing* and the *reconstruction* phase, specified by two protocols Share and Rec respectively, described below. Let $[n] = \{1, \ldots, n\}$.

- Share: The dealer D takes as input a secret $s \in \mathcal{S}$, locally computes shares $\sigma_1, \ldots, \sigma_n$, and for every $i \in [n]$, sends the i-th share σ_i privately to player P_i.

– Rec: During reconstruction, player P_i, $i \in [n]$, communicates, possibly by means of several synchronous communication rounds, σ_i to the reconstructor R. The reconstructor R uses the received shares to produce an output s', which is supposed to be the original secret s.

2.2 Adversarial Capabilities

We now specify the capabilities (and limitations) of the adversary who has unbounded computing power. The goal of the adversary is to make the reconstructor output a value different from the original secret s.

– During the sharing phase, the adversary remains inactive, and does not learn any information about the secret as the shares are distributed using private channels between players and the dealer.
– After the sharing phase, the adversary can adaptively corrupt up to t of the players P_i, where t **is the threshold parameter**. The corruption can be done between communication rounds and continue as long as the total number of corrupted players does not exceed t. D or R are assumed incorruptible. Once a player P_i is corrupted, the adversary learns P_i's share σ_i, and from then on, the adversary has full control over P_i. The corruptions being adaptive means that after each corruption, the adversary can decide on whom to corrupt next depending on the shares he has seen so far.
– During the reconstruction phase, the adversary sees the communications between players P_i and the reconstructor R. Furthermore, he controls the information that the dishonest players send to the reconstructor R. Reconstruction in general has multiple rounds. In every communication round, for every corrupted player, the adversary decides what this player should send to R. A **rushing** adversary can choose these values after observing what honest players send to R in the current round. A **non-rushing** adversary selects the corrupted shares before the start of the reconstruction phase.

2.3 Security

An n-player robust secret sharing scheme (Share, Rec) is (t, δ)-secure if the following properties hold for any distribution of $s \in S$ and for any adversary as specified above:

1. Privacy: Before Rec starts, the adversary has no more information about the shared secret s than he had before the execution of Share.
2. Reconstructability: At the end of Rec, the reconstructor R outputs $s' = s$ with probability at least $1 - \delta$.

It is well known that in any perfect secret sharing scheme, the bit-size of a share σ_i is at least the same as the bit-size of secret, that is $\log |S|$ [25]. Much research

effort focused on finding the least required redundancy to achieve robustness. Let σ_i denotes the share for player P_i. The redundancy (also known as overhead) is measured by the quantity $\max_i\{\log \sigma_i\} - \log |S|$. For $t < n/3$, one can use Reed-Solomon error correcting codes to construct a robust secret sharing scheme with efficient reconstruction algorithm and no redundancy in the share size i.e., the share size is the same as the secret size [1]. On the other hand, for $t \geq n/2$ there is no solution to the problem (the (t, n)-threshold access structure requires at least $t + 1$ correct shares for the recovery of the original secret). In this work we construct a robust secret sharing scheme for $n = 2t + 2$ with no redundancy in the share size. The construction works for any t in the range $\frac{n}{3} \leq t \leq \frac{n}{2} - 1$.

3 The Proposed Scheme

The scheme of [9] can be understood as being obtained from a secret sharing scheme that allows error detection, i.e., that detects if a set of $t + 1$ shares contains some incorrect ones (but can not necessarily tell which ones). It was analyzed in [15] that any secret sharing scheme with error detection [5,21,27] can be transformed into a robust secret sharing scheme by looping over all sets of size $t+1$. This line of thinking has provided schemes with low share redundancy and the work in [9] represents the best so far. It is apparent that any such scheme will suffer from the same exponential complexity and our new proposal, being constructed on this line, is no exception, but what is interesting is that the proposed scheme employs a technique that leverage some extra public values to eliminate redundancy in the shares.

3.1 The Scheme

Let t and n are positive integers such that $n = 2t+2$. Let $\mathbb{F}_q$ be a finite field with q elements, where q is a prime power with $q > n$. We now present an n-player robust secret sharing scheme over $\mathbb{F}_q$ which is (t, δ) secure and individual share size is same as secret size.

- Share:
  - Let $s \in \mathbb{F}_q$ be a secret.
  - The dealer randomly chooses a polynomial $f(x) \in \mathbb{F}_q[x]$ of degree at most t such that $f(0) = s$ and computes $s_i = f(i)$ for all $i \in [t + 1]$.
  - D choose n vectors of length $t + 1$, $(r_{i1}, \ldots, r_{i(t+1)}) \in (\mathbb{F}_q)^n$, $1 \leq i \leq n$ such that any $t + 1$ of them are linearly independent (see below for such a selection) and for every $i \in [n]$, he computes $\sigma_i = \sum_{j=1}^{t+1} r_{ij} s_j \in \mathbb{F}_q$.
  - For every $i \in [n]$, the dealer D sends to player P_i the share σ_i (just one field element). The n vectors $\{(r_{i1}, \ldots, r_{i(t+1)})\}_{1 \leq i \leq n}$ are part of system's public parameters. The dealer can send the public parameters to users, using the broadcast channel. Alternatively the public parameters can be stored on a publicly accessible authenticated bulletin board.

– Rec:
  - Every player sends σ_i to the reconstructor R.
  - To reconstruct the secret, the reconstructor does the following for *every subset* of $t+1$ players.
    * He reconstructs $(s'_1, s'_2, \ldots, s'_{t+1})$ using $t+1$ shares by solving $t+1$ equations in $t+1$ variables.
    * He checks if $\sum_{j=1}^{t+1} r_{ij} s'_j = \sigma_i$ for *at least one of the remaining* $t+1$ shares, and halts if it holds.
  - R then computes (using Lagrange interpolation) a polynomial $f(x) \in \mathbb{F}_q[x]$ of degree at most t and outputs $s = f(0)$.

3.2 Remarks

Standard methods are available to choose n vectors of length $t+1$ over $\mathbb{F}_q$ with the property that any $t+1$ of them are linearly independent. For completeness we describe some of them here. Let $z_1, \ldots, z_n, w_1, \ldots, w_{t+1} \in \mathbb{F}_q$ be such that the z_i's are distinct, the w_j's are distinct, and $z_i + w_j \neq 0$ for all i, j. Define

$$r_i = \left(\frac{1}{z_i + w_1}, \ldots, \frac{1}{z_i + w_{t+1}} \right), \ 1 \leq i \leq n \ .$$

One can check that any $t+1$ vectors chosen among these n row vectors are linearly independent as the matrix so formed has non-zero determinant (see Ch 11, [17]). In particular let M denote the matrix with rows $r_1, \ldots, r_{t+1}$, then

$$\det(M) = \frac{\prod_{i<j}(z_j - z_i)(w_j - w_i)}{\prod_{i,j}(z_i + w_j)} \ .$$

The number of field elements that are distributed publicly is equal to $n+t+1$. Another way of selection is to choose an $n \times (t+1)$ Vandermonde matrix which also has the property that any $t+1$ rows are independent. A Vandermonde matrix of size $n \times (t+1)$ can be described by n elements and in this case only n field elements are distributed publicly.

4 Security

4.1 Perfect Secrecy

The secret is the constant term of a random polynomial of degree at most t. The $t+1$ evaluations of the polynomial, $\{s_1, \ldots, s_{t+1}\}$, are independent and are needed to reconstruct the secret. We will show that any group $\mathcal{CP} = \{P_{i_1}, \ldots, P_{i_t}\}$ of corrupted participants will be completely uncertain about at least one value from $\{s_1, \ldots, s_{t+1}\}$. This is true because the group $\mathcal{CP}$ has t shares $\{\sigma_{i_1}, \ldots, \sigma_{i_t}\}$ and these shares correspond to t equations,

$$M \cdot (s_1, \ldots, s_{t+1})^T = (\sigma_{i_1}, \ldots, \sigma_{i_t})^T \ ,$$

where M is the $t \times (t+1)$ matrix consisting of the t row vectors $r_{i_1}, \ldots r_{i_t}$ associated with the corrupted users, and 'T' denotes matrix transpose.

Let $M_1, \ldots, M_{t+1}$ be the column vectors of M. As M_i's constitute a set of $t+1$ t-dimensional vectors, they are linearly dependent. Thus there exists at least one column vector, without loss of generality say M_1, such that M_1 belongs to the subspace $\langle M_2, \ldots, M_{t+1} \rangle$. So there exists a $(t+1)$-dimensional vector $b = (b_1, \ldots, b_{t+1})$ such that $Mb^T = 0$ and $b_1 \neq 0$. Thus, we have

$$(\sigma_{i_1}, \ldots, \sigma_{i_t})^T = M \cdot (s_1, \ldots, s_{t+1})^T = M \cdot ((s_1, \ldots, s_{t+1})^T + \alpha(b_1, \ldots, b_{t+1})^T)$$

for all $\alpha \in \mathbb{F}_q$. Hence, given any $\beta_1 \in \mathbb{F}_q$, there exists $(\beta_1, \ldots, \beta_{t+1}) \in (\mathbb{F}_q)^{t+1}$ such that $M \cdot (\beta_1, \ldots, \beta_{t+1})^T = (\sigma_{i_1}, \ldots, \sigma_{i_t})^T$. Therefore, the participants in $\mathcal{CP}$ cannot rule out any element of $\mathbb{F}_q$ as a possibility for s_1. Thus, there exists q values for s_1 and distinct values for s_1 leads to distinct polynomials. This makes $f(0)$ indeterminate. □

4.2 Reliability

Theorem 1. *Let k be a security parameter. For any positive integer n and t such that $n = 2t + 2$, and any finite field $\mathbb{F}_q$ with $k = \lceil \log_2 q \rceil$, the pair* (Share, Rec) *forms an n-player (t, δ)-robust secret sharing for message space $\mathbb{F}_q$ with*

$$\delta \leq \frac{\sqrt{t+1}}{2^{k-n}} \ .$$

Proof. Consider the state of the reconstruction phase right before the reconstructor R has received the shares from the players. We may assume that at this stage the adversary has corrupted t players. Thus R has now n shares of which at most t are corrupted. To reconstruct the secret, R does the following for *every subset* of $t+1$ players.

(a) He computes $(s'_1, s'_2, \ldots, s'_{t+1})$ using $t+1$ chosen shares $(\sigma'_{i_1}, \sigma'_{i_2}, \ldots, \sigma'_{i_{t+1}})$ (by solving $t+1$ equations in $t+1$ variables).
(b) He then checks if $\sum_{j=1}^{t+1} r_{ij} s'_j = \sigma_i$ for *at least one of the remaining* $t+1$ shares, and halts if it holds.

Consider an arbitrary set $A = \{\sigma'_{i_1}, \ldots, \sigma'_{i_{t+1}}\}$ of $t+1$ shares submitted during the reconstruction phase. Let us assume that j $(0 \leq j \leq t)$ of them are corrupted. Let M be the matrix with rows $r_{i_1}, \ldots, r_{i_{t+1}}$ such that,

$$M \cdot (s'_1, \ldots, s'_{t+1})^T = (\sigma'_{i_1}, \ldots, \sigma'_{i_{t+1}})^T.$$

Then $(s'_1, \ldots, s'_{t+1})^T = \sigma'_{i_1} \tilde{M}_1 + \cdots + \sigma'_{i_{t+1}} \tilde{M}_{t+1}$, where the $\tilde{M}_i$'s are the columns of the inverse matrix M^{-1}. For a fix set of values of the j corrupted shares, there are q^{t+1-j} solution vectors to the above equality. Therefore the probability that the solution vector is a solution to one of the remaining equations is $\frac{t+1}{q^{t+1-j}}$, the maximum value is $\frac{t+1}{q}$ when $j = t$. Thus, taking into account union

bound over all subsets of size $t+1$ leaves us with the failure probability $\leq \frac{\sqrt{t+1}}{2^{k-n}}$ $\left(\text{as } (t+1) \cdot \binom{n}{t+1} \leq \sqrt{t+1} \cdot 2^n \text{ when } n = 2t+2 \text{ and } k = \lceil \log_2 q \rceil \right)$. □

The efficiency comparison for the proposed scheme with the known schemes (described below) is given in Sect. 6.

5 Known Schemes and Possible Extensions

Previous works on robust secret sharing schemes with unconditional security for the range $n/3 \leq t < n/2$ can be broadly divided into two classes. We now briefly recall the best scheme from each class.

The first one is due to Cramer et al. [9], based on an idea by [5]. The scheme works as follows. Using standard Shamir secret sharing, the dealer shares independently the actual secret $s \in \mathbb{F}_q$, a randomly chosen field element $r \in \mathbb{F}_q$, and their product $p = s \cdot r$. To reconstruct the secret, the reconstructor does the following: for every subset of $t+1$ players, he reconstructs s', r' and p' and checks if $s' \cdot r' = p'$, and halts and outputs s' if it is the case. One can show that for any subset of $t+1$ players: if $s' \neq s$ then $s' \cdot r' \neq p'$ except with probability $1/q$. Thus for a field of size 2^k, taking into account union bound over all subsets of size t + 1, gives a robust secret sharing scheme with failure probability 2^{k-n} and shares of size $3k$ bits (consisting of three field elements).

The second scheme is given by Cevellos, Fehr, Ostrovsky and Rabani [7], and is based on the scheme of Rabin and BenOr [22] with an elegant twist to its reconstruction algorithm. This scheme's description is given below.

– Share:
  - Choose a random polynomial $f(x) \in \mathbb{F}_q[X]$ with degree at most t such that $f(0) = s$.
  - Compute the Shamir shares $s_1 = f(x_1), \ldots, s_n = f(x_n)$, where x_i's are distinct points in $\mathbb{F}_q$.
  - For every pair $i, j \in [n]$, choose a random key $key_{ij} \in \mathcal{K}$ and compute $\tau_{ij} = MAC(key_{ji}, s_i)$, where $MAC : \mathbb{F}_q \times \mathcal{K} \to \mathcal{T}$ be an ϵ-secure MAC [29,30,7] with message space $\mathbb{F}_q$.
  - For every $i \in [n]$, the player P_i is given the share

$$\sigma_i = (s_i, \tau_{i1}, \ldots, \tau_{in}, key_{i1}, \ldots, key_{in}).$$

– Rec:
  - **First Round:** Every player P_i sends s_i and $\tau_{i1}, \ldots, \tau_{in}$. to the reconstructor $\mathcal{R}$.
  - **Second Round:** Every player P_i sends $key_{i1}, \ldots, key_{in}$ to $\mathcal{R}$.
  - **Local Computation:**
    * For every pair $i, j \in [n]$, $\mathcal{R}$ sets ν_{ij} to be 1 if the share s_i of player P_i is accepted by the corresponding key of player P_j, i.e., if $\tau_{ij} = \text{MAC}(key_{ji}, s_i)$, and else to 0.

* $\mathcal{R}$ computes the largest set $\mathcal{I} \subseteq [n]$ with the property that

$$\forall i \in \mathcal{I} : |\{j \in \mathcal{I} | \nu_{ij} = 1\}| = \sum_{j \in \mathcal{I}} \nu_{ij} \geq t + 1 \ ;$$

in other words, every share of a player in $\mathcal{I}$ is accepted by at least $t+1$ players in $\mathcal{I}$. Clearly $\mathcal{I}$ contains all honest players. Let $c = |\mathcal{I}| - (t+1)$ be the maximum number of corrupt players in $\mathcal{I}$.

* Use the Berlekamp-Welch algorithm [2,14] to compute a polynomial $f(x) \in \mathbb{F}[X]$ of degree at most t such that $f(x_i) = s_i$ for *at least* $(t+1) + \frac{c}{2}$ players i in $\mathcal{I}$. If no such polynomial exists then $\mathcal{R}$ outputs $\perp$; otherwise, he outputs $s = f(0)$.

The Share algorithm of this scheme is the same as the well-known scheme of Rabin and Ben-Or [22] which relies on message authentication. The redundancy in share size for Rabin and Ben-Or scheme consists of $3n$ elements from the field where the secret is drawn from. The scheme uses a message authentication code with *short* tags and keys and with the resulting weak security. The short tags and keys result in the required saving (improvement over Rabin and Ben-Or scheme) in the share size. The weakened security of authentication (and so higher chance of forging) is compensated with a more sophisticated reconstruction procedure which runs in polynomial time and results in an exponentially small failure probability. The overhead of the share size depends directly on the exponent of the failure probability.

Assuming the same share distribution as Rabin and Ben-Or's scheme [22], one may consider further reduction in authentication information and improvement in the reconstruction, to obtain shorter share sizes. In Sect. 5.1 we explore one such possibility by employing list decoding algorithm for Reed-Solomon codes [26] in the reconstruction algorithm of [7]. Our goal is to reduce δ, the error probability of the decoder, which will translate into smaller share size. Our analysis shows that this modification does not reduce δ and so the share size cannot be further reduced.

5.1 Using List Decoding to Improve Decoding Error in [7]

We begin by describing a natural modification to the Cevallos et al.'s Scheme.

- Share: Same
- Rec:
  - **First Round:** Same
  - **Second Round:** Same
  - **Local Computation:** Step 1 and 2 are the same as above. Recall that $c = |\mathcal{I}| - (t+1)$ is the maximum number of corrupt players in $\mathcal{I}$.
    * **Step 3 of Cevallos et al. scheme:** Use Berlekamp-Welch to compute a polynomial $f(x) \in \mathbb{F}[X]$ of degree at most t such that $f(x_i) \neq s_i$ for *at most* $\frac{c}{2}$ players in $\mathcal{I}$.

* **Modification:** Use list decoding algorithm for $[n = 2t+1, k = t+1, d = n-k+1 = t+1]$ Reed-Solomon codes [26] that corrects up to $n-\sqrt{nt}$ of errors, to compute a (list of) polynomial(s) $f(x) \in \mathbb{F}[X]$ of degree at most t such that $f(x_i) \neq s_i$ for at most $\frac{1}{1+\sqrt{\frac{t}{t+1+c}}}(c+1)$ players in $\mathcal{I}$.
* Find correct f from the decoding list and output $s = f(0)$.

5.2 Robustness

The analysis is similar to [7]. Define the following sets: $\mathcal{A} \subset [n]$ is the set of corrupted players that have handed in modified Shamir shares, and $\mathcal{P} \subset [n]$ is the set of corrupted players that have handed in the correct Shamir shares. It holds that $|\mathcal{A}| + |\mathcal{P}| = t$. The set $\mathcal{H} = [n] \backslash (\mathcal{A} \cup \mathcal{P})$ is the set of uncorrupted players.

The set $\mathcal{I}$ computed during reconstruction contains $\mathcal{H}$ and $\mathcal{P}$ with certainty. Thus, the reconstruction procedure is guaranteed to output the correct secret if at most $\frac{1}{\theta} \cdot (p+1)$ players $i \in \mathcal{A}$ end up in $\mathcal{I}$, where $p = |\mathcal{P}|$ and $\theta = \sqrt{\frac{t}{n}}$. Indeed, if $|\mathcal{A} \cap \mathcal{I}| \leq \frac{1}{\theta} \cdot (p+1)$, then the requirement for list-decoding is satisfied ($|\mathcal{I}| = t+1+c = t+1+p+e$ where $e = |\mathcal{A} \cap \mathcal{I}| \leq \frac{1}{\theta} \cdot (p+1)$ and thus $e = \frac{1}{\theta} \cdot (p+1) = \frac{1}{1+\theta}(p + \frac{1}{\theta}(p+1)+1) = \frac{1}{1+\theta}(c+1)$).

We need to find the probability $P[|\mathcal{A} \cap \mathcal{I}| > \frac{1}{\theta} \cdot (p+1)]$. It is sufficient to consider the case $p \leq \frac{\theta}{1+\theta} \cdot t$; indeed if $p > \frac{\theta}{1+\theta} \cdot t$ and thus $p \geq \frac{\theta}{1+\theta} \cdot (t-1)$ then obviously $|\mathcal{A}| \leq t - \frac{\theta}{1+\theta} \cdot (t-1) = \frac{1}{1+\theta} \cdot (t+1)$ and hence $P[|\mathcal{A} \cap \mathcal{P}| \leq \frac{1}{\theta} \cdot (p+1)]$. Thus

$$\delta = \sum_{p=1}^{\frac{\theta}{1+\theta} \cdot t} P[|\mathcal{A} \cap \mathcal{I}| > \frac{1}{\theta} \cdot (p+1)] \ .$$

For any p in the range $1 \leq p \leq \frac{\theta}{1+\theta} \cdot t$, we first compute $P[|\mathcal{A} \cap \mathcal{I}| > \frac{1}{\theta} \cdot (p+1)]$. Let us assume that $\frac{1}{\theta} \cdot (p+1)$ is an integer. In order to bound the above probability, it is convenient to introduce the following random variables:

- For every pair $i, j \in [n]$, we define the binary random variable V_{ij} that specifies if the player P_i's share and his submitted tag associated with player P_j are accepted by player P_j's key. Note that, all the V_{ij} with $i \in [n]$ and $j \in \mathcal{H}$ are independent. Further $P[V_{ij} = 1] \leq \epsilon$ for all $i \in \mathcal{A}$ and $j \in \mathcal{H}$.
- For every $i \in \mathcal{A}$ the random variable

$$N_i = \sum_{j \in \mathcal{H}} V_{ij} = |\{j \in \mathcal{H} | V_{ij} = 1\}| \ ,$$

  i.e., the number of honest players that accept P_i's incorrect share. Note that since the V_{ij}'s are independent for all $i \in [n]$ and $j \in \mathcal{H}$, so are all the N_i's.

$$
\begin{aligned}
P[|\mathcal{A}\cap\mathcal{I}| > \frac{1}{\theta}\cdot(p+1)] &= P[\Big(|\mathcal{A}\cap\mathcal{I}| = \frac{1}{\theta}\cdot(p+1)+1\Big)\cup\cdots\cup\Big(|\mathcal{A}\cap\mathcal{I}| = t-\frac{1}{\theta}\cdot(p+1)\Big)] \\
&\leq P[|\mathcal{A}\cap\mathcal{I}| = t-\frac{1}{\theta}\cdot(p+1)] \text{ (best strategy for adversary)} \\
&= P[\cap_{i\in\mathcal{A}\setminus\mathcal{P}}(N_i=1)] \\
&= \prod_{i\in\mathcal{A}\setminus\mathcal{P}} P[N_i=1] \\
&= \prod_{i\in\mathcal{A}\setminus\mathcal{P}} P[\exists\mathcal{H}_0\subseteq\mathcal{H}:(|\mathcal{H}_0|=1)\wedge(\forall j\in\mathcal{H}_0:V_{ij}=1)] \\
&\leq \prod_{i\in\mathcal{A}\setminus\mathcal{P}}\left(\sum_{\mathcal{H}_0\subseteq\mathcal{H}:|\mathcal{H}_0|=1} P[\forall j\in\mathcal{H}_0:V_{ij}=1)]\right) \\
&\leq \prod_{i\in\mathcal{A}\setminus\mathcal{P}}((t+1)\cdot\epsilon) \\
&= ((t+1)\cdot\epsilon)^{t-\frac{1}{\theta}\cdot(p+1)}
\end{aligned}
$$

We can now compute the robustness probability as follows:

$$
\begin{aligned}
\delta &= \sum_{p=1}^{\frac{\theta}{1+\theta}\cdot t} P[|\mathcal{A}\cap\mathcal{I}| > \frac{1}{\theta}\cdot(p+1)] \\
&\leq \sum_{p=1}^{\frac{\theta}{1+\theta}\cdot t} ((t+1)\cdot\epsilon)^{t-\frac{1}{\theta}\cdot(p+1)} \\
&\leq ((t+1)\cdot\epsilon)^{\frac{\theta}{1+\theta}\cdot t-\frac{1}{\theta}}(1+((t+1)\cdot\epsilon)^{\frac{1}{\theta}}+((t+1)\cdot\epsilon)^{\frac{2}{\theta}}+\cdots) \text{ [assuming, } \epsilon\leq\frac{1}{t+1}] \\
&\leq 2((t+1)\cdot\epsilon)^{\frac{\theta}{1+\theta}\cdot t-\frac{1}{\theta}}
\end{aligned}
$$

Note that the bound on δ is similar to the bound while considering the Berlekamp-Welch setting. Also note that we have not included the analysis for the required probability to find the correct polynomial from the list of polynomials output by the list decoding algorithm.

6 Efficiency Comparison

In this section we compare the efficiency of our scheme, in terms of relation among the following three parameters: secret size, the share size and the reliability in the reconstruction, with the schemes of Cramer et al. [9] and Cevallos et al. [7]. Note that our scheme works for $n \geq 2t+2$ while the other two schemes work for $n \geq 2t+1$. To share a k-bit secret among the n players using our proposed scheme, the failure probability is at most $\frac{\sqrt{t+1}}{2^{k-n}}$, and for the Cramer et al. scheme it is $\frac{1}{2^{k-n}}$. The share size for the two schemes are k bits and $3k$ bits, respectively.

Understanding the relation for [7] is more subtle. Here the failure probability depends on an extra parameter. Let λ be a parameter that can be chosen independent of the secret size k. The two parameters λ, k are used in the following MAC function which has been used in [7]:

$$MAC : GF(2^k) \times (GF(2^{k/\lambda}))^2 \to GF(2^{k/\lambda}) \ .$$

Sharing a k-bit secret among the n players using the scheme [7], results in the failure probability of at most $\frac{1}{2^{n\frac{k}{\lambda} - n\log(n\cdot\lambda)}}$. For $\lambda \leq n$, the failure probability is less than for the other schemes. The share size for [7] is $k + 3n\frac{k}{\lambda}$. Clearly [7] has efficient reconstruction complexity and improved failure probability. However the share size is higher than the other two schemes. In the table, the secret size and share size are given in bits.

Table 1. Comparison Table

Scheme	Secret size	Share size	Rec Complexity	δ	Public Parameters
[9]	k	$3k$	Exp. in n	$2^{-(k-n)}$	Nil
[7]	k	$k + 3n\frac{k}{\lambda}$	Poly. in n	$2^{-(n\frac{k}{\lambda} - n\log(n\cdot\lambda))}$	Nil
Proposed Scheme	k	k	Exp. in n	$\sqrt{t+1}\cdot 2^{-(k-n)}$	n field elements

The last column for public parameters represents the elements that are required in addition to the interpolating points for Shamir's secert sharing scheme.

7 Conclusion

The problem of the minimum share size for threshold robust secret sharing has received considerable attention in recent years. In this paper, we proposed and analyzed a new threshold robust secret sharing scheme for which the share size of participants is the same as the secret size. This is the minimum possible value for the share size of a perfect secret sharing scheme and hence also the least possible share size for threshold robust secret sharing. The result is interesting as it means that the extra robustness property can be obtained with no extra cost on the share size. However the scheme works only for $n \geq 2t + 2$ and effectively uses the share of one extra honest participant as the verification information. The reconstruction algorithm is exponential in the number of players. Construction of schemes with efficient reconstruction in our setting remains an open problem.

Acknowledgments. Financial support for this research was provided in part by Alberta Innovates - Technology Futures, in the Province of Alberta in Canada. The authors would also like to thank Pengwei Wang for many useful discussions.

References

1. Ben-Or, M., Goldwasser, S., Wigderson, A.: Completeness theorems for non-cryptographic fault-tolerant distributed computation (extended abstract). In: Simon, J. (ed.) STOC 1988, pp. 1–10. ACM (1988)
2. Berlekamp, E.R., Welch, L.R.: Error correction of algebraic block codes. U.S. patent number 4.633.470 (1986)
3. Blakley, G.: Safeguarding cryptographic keys. In: AFIPS National Computer Conference, vol. 48, pp. 313–317 (1979)
4. Brickell, E.F., Stinson, D.R.: The detection of cheaters in threshold schemes. SIAM J. Discrete Math. 4(4), 502–510 (1991)
5. Cabello, S., Padró, C., Sáez, G.: Secret sharing schemes with detection of cheaters for a general access structure. In: Ciobanu, G., Păun, G. (eds.) FCT 1999. LNCS, vol. 1684, pp. 185–194. Springer, Heidelberg (1999)
6. Carpentieri, M., De Santis, A., Vaccaro, U.: Size of shares and probability of cheating in threshold schemes. In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 118–125. Springer, Heidelberg (1994)
7. Cevallos, A., Fehr, S., Ostrovsky, R., Rabani, Y.: Unconditionally-secure robust secret sharing with compact shares. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 195–208. Springer, Heidelberg (2012)
8. Chor, B., Goldwasser, S., Micali, S., Awerbuch, B.: Verifiable secret sharing and achieving simultaneity in the presence of faults (extended abstract). In: FOCS 1985, pp. 383–395. IEEE Computer Society (1985)
9. Cramer, R., Damgård, I., Fehr, S.: On the cost of reconstructing a secret, or VSS with optimal reconstruction phase. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 503–523. Springer, Heidelberg (2001)
10. Dolev, D., Dwork, C., Waarts, O., Yung, M.: Perfectly secure message transmission. In: FOCS 1990, pp. 36–45. IEEE Computer Society (1990)
11. Ganger, G.R., Khosla, P.K., Bakkaloglu, M., Bigrigg, M.W., Goodson, G.R., Oguz, S., Pandurangan, V., Soules, C.A.N., Strunk, J.D., Wylie, J.J.: Survivable storage systems. In: Proceedings of DARPA Information Survivability Conference & Exposition II, DISCEX 2001, vol. 2, pp. 184–195 (2001)
12. Garay, J.A., Givens, C., Ostrovsky, R.: Secure message transmission with small public discussion. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 177–196. Springer, Heidelberg (2010)
13. Garay, J., Givens, C., Ostrovsky, R.: Secure message transmission by public discussion: A brief survey. In: Chee, Y.M., Guo, Z., Ling, S., Shao, F., Tang, Y., Wang, H., Xing, C. (eds.) IWCC 2011. LNCS, vol. 6639, pp. 126–141. Springer, Heidelberg (2011)
14. Gemmell, P., Sudan, M.: Highly resilient correctors for polynomials. Inf. Process. Lett. 43(4), 169–174 (1992)
15. Kurosawa, K., Suzuki, K.: Almost secure (1-round, n-channel) message transmission scheme. IEICE Transactions 92-A(1), 105–112 (2009)
16. Lakshmanan, S., Ahamad, M., Venkateswaran, H.: Responsive security for stored data. IEEE Trans. Parallel Distrib. Syst. 14(9), 818–828 (2003)
17. MacWilliams, F.J., Sloane, N.J.A.: The theory of error-correcting codes. North-Holland publishing company
18. 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)

19. McEliece, R.J., Sarwate, D.V.: On sharing secrets and Reed-Solomon codes. Commun. ACM 24(9), 583–584 (1981)
20. Obana, S.: Almost optimum t-cheater identifiable secret sharing schemes. In: Paterson, K.G. (ed.) EUROCRYPT 2011. LNCS, vol. 6632, pp. 284–302. Springer, Heidelberg (2011)
21. Ogata, W., Kurosawa, K., Stinson, D.R.: Optimum secret sharing scheme secure against cheating. SIAM J. Discrete Math. 20(1), 79–95 (2006)
22. Rabin, T., Ben-Or, M.: Verifiable secret sharing and multiparty protocols with honest majority (extended abstract). In: Johnson, D.S. (ed.) STOC 1989, pp. 73–85. ACM (1989)
23. Rogaway, P., Bellare, M.: Robust computational secret sharing and a unified account of classical secret-sharing goals. In: Ning, P., De Capitani di Vimercati, S., Syverson, P.F. (eds.) ACM Conference on Computer and Communications Security, pp. 172–184. ACM (2007)
24. Shamir, A.: How to share a secret. Communications of the ACM 22(11), 612–613 (1979)
25. Stinson, D.R.: An explication of secret sharing schemes. Des. Codes Cryptography 2(4), 357–390 (1992)
26. Sudan, M.: Decoding of Reed-Solomon codes beyond the error-correction bound. J. Complexity 13(1), 180–193 (1997)
27. Tompa, M., Woll, H.: How to share a secret with cheaters. J. Cryptology 1(2), 133–138 (1988)
28. Waldman, M., Rubin, A.D., Cranor, L.F.: The architecture of robust publishing systems. ACM Trans. Internet Techn. 1(2), 199–230 (2001)
29. Wegman, M.N., Carter, L.: New classes and applications of hash functions. In: FOCS 1979, pp. 175–182. IEEE Computer Society (1979)
30. Wegman, M.N., Carter, L.: New hash functions and their use in authentication and set equality. J. Comput. Syst. Sci. 22(3), 265–279 (1981)