On the Share Efficiency of Robust Secret Sharing and Secret Sharing with Cheating Detection*

Mahabir Prasad Jhanwar and Reihaneh Safavi-Naini

Department of Computer Science
University of Calgary, Canada

Abstract. In a basic (t, n)-threshold secret sharing scheme the adversary is passive and the security goal is to ensure that unauthorized subsets do not learn any information about the secret. In this paper we consider the case that the corrupted parties submit *incorrect* shares and there are extra security goals with respect to incorrect shares. We consider two such security requirements: in a (t, n)-threshold robust secret sharing (RSS) scheme we require that the shared secret can be recovered from the set of *all* n shares even if up to t of them are incorrect; and in a (t, n)-threshold secret sharing scheme with cheating detection (SSCD) property we require to prevent cheaters who try to make another player reconstruct an invalid secret.

We make the following contributions. Firstly, we construct a robust (t, n)-threshold secret sharing (RSS) scheme with the lowest known share size for $n = 2t+1$. In our RSS scheme the share size is $\log_2 s + \log_2 \frac{1}{\delta} + n$ bits which is less than the share size of the best known scheme by $\log_2 \frac{1}{\delta} + n$ bits. Here $\log_2 s$ bits denotes secret size and δ denotes error probability in reconstructing the correct secret. We then consider the problem of reducing the size of public information in RSS. We will motivate this problem and propose a scheme that nearly halves the amount of public information. For this we first construct a new variant of Shamir secret sharing scheme and then modify it to provide robustness. The construction achieves the least total share storage/communication among all known threshold robust secret sharing schemes.

The final contribution of this paper is the constriction of an optimal threshold secret sharing with *cheating detection* property. We propose a scheme that achieves the lower bound on the share size of cheating detection schemes, and hence is optimal. The scheme is the first to achieve the bound without having special requirements.

1 Introduction

Secret sharing is one of the most important primitive in cryptography and in particular distributed systems. In a (t, n)-threshold secret sharing scheme [26,1], a dealer $\mathcal{D}$ distributes a secret s to n players, say $P_1, \ldots, P_n$ in such a way that

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

G. Paul and S. Vaudenay (Eds.): INDOCRYPT 2013, LNCS 8250, pp. 179–196, 2013.

any $t+1$ or more players can recover the secret s, but any t or fewer players have no information on s. A piece of information given to P_i is called a share and is denoted by σ_i. The 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. An important efficiency parameter in secret sharing scheme is the size of shares. Let Σ_i be the set of possible shares for P_i. Let S be the set of possible secrets. Then it is well known that $|\Sigma_i| \geq |S|$ for any perfect (t, n)-threshold secret sharing scheme [15], i.e., $\log_2 \sigma_i \geq \log_2 s$. Schemes with $\log_2 \sigma_i = \log_2 s$ are called *ideal*.

In its basic form, secret sharing assumes that the corrupted participants are passive (or semi-honest) and follow the protocol during the reconstruction phase. In practice however one needs to consider stronger adversaries who deviate from the protocol, collude and submit wrong shares. There are a wide range of settings and security requirements that address active adversaries in secret sharing. In this paper we consider two particular formulation of security requirements for threshold secret sharing, known as robust secret sharing [4] and secret sharing with cheating detection [22]. In the following we briefly describe these two and then present our contributions. A closely related problem of *identifying cheaters* in secret sharing has also been studied [17,21,6,13] in the literature.

Robust Secret Sharing (RSS): In a *perfect* (t, n)*-threshold robust secret sharing* scheme, in addition to the requirement of perfect threshold secret sharing 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. Requiring that the set of uncorrupted shares have sufficient information to recover the secret implies that $n - t \geq t + 1$ and so $n \geq 2t + 1$ ($t \leq \frac{n-1}{2}$). When $n = 2t + 1$, the number of honest users is only one more than the colluders. It is known that in this case colluders will always succeed with some probability and that the share size of the users is always larger than the secret size. The extra share size is called the *share redundancy* and is defined as $\max_i\{\log_2 \sigma_i\} - \log_2 s$. Construction of schemes with the lowest probability of failure and the least share redundancy has been an active research area in recent years. The construction in [7] has the lowest known share redundancy equal to $2\log_2 \frac{1}{\delta} + 2n$ bits where δ is the probability of error in reconstructing the correct secret.

We also consider a new property for secret sharing schemes and study it for RSS. Secret sharing schemes, including robust schemes, use some public data during reconstruction. This public data enables users to store smaller shares. For example in Shamir secret sharing the public data is the interpolation points which is assigned to players individually but does not need to be made secret. The information is used during the reconstruction. By making these points public, the share size of the users is effectively halved. To implement such a scheme however one needs to provide a broadcast channel or authenticated bulletin board that will be used to make the required public data available for reconstruction. Reducing this public data is not only important from practical view point, but also raises interesting theoretical questions and in particular possible

tradeoff between the amount of public and private data in various schemes. To our knowledge this has not been considered before. We will discuss this in our contributions.

Secret Sharing with Cheating Detection (SSCD): The goal of secret sharing schemes with cheating detection property is to ensure detection of cheating by the malicious players who aim to cheat an honest player by opening incorrect shares and causing the honest player to reconstruct wrong secret. Specifically, suppose that t players, say $P_1, \ldots, P_t$, want to cheat a $(t+1)$th player, P_{t+1}, by opening modified shares $\sigma'_1, \ldots, \sigma'_t$. They succeed if the secret s' that is reconstructed from $\sigma'_1, \ldots, \sigma'_t$ and σ_{t+1} is different from the original secret s. In this case, we say that the *player* P_{t+1} *is cheated by the wrong shares* $\sigma'_1, \ldots, \sigma'_t$. Tompa and Woll [27] first considered this problem (see also [3,2,22]). Two different model exists for such a system. In the first one, known as CDV model, we suppose that the cheaters somehow know the value of the secret s. The other model OKS is characterized by the property that t cheaters (corrupted players) $P_1, \ldots, P_t$ does not have any idea about the secret s before they cheat P_{t+1}. Ogata, Kurosawa, and Stinson showed the following tight lower bound on share size in OKS model:

$$\log_2 \sigma_i \geq \log_2 s + \log_2 \frac{1}{\delta_c}, \tag{1}$$

where δ_c denotes the cheating probability. In OKS model, the only two known share-optimal schemes [23,22] impose *restrictions on the secret set*. Construction of SSCD schemes in this model that meet the lower bound is an interesting open problem.

1.1 Our Contribution

The contribution of this paper is three fold.

[i] A Threshold Robust Secret Sharing with the Lowest Redundancy. We propose a new (t, n)-threshold robust secret sharing scheme that has redundancy, $\log_2 \frac{1}{\delta} + n$ bits. Each user's share consists of two field elements and system's public parameters, in addition to the interpolation points, consists of two filed elements that are used to verify correctness of a reconstructed candidate secret. For share generation the scheme uses polynomials over finite fields, and for reconstruction Lagrange interpolation(s) to construct a candidate secret. The reconstruction algorithm loops over all subsets of size $t+1$ of n participants and so is computationally inefficient. A similar inefficiency exists in [7], which has had the shortest share size before this paper. It is worth noting that the best scheme [4] with computationally efficient reconstruction has share size which is substantially larger than our proposed scheme (see Sect. 3.3). Construction of RSS schemes with computationally efficient reconstruction and share size similar to ours is an interesting open question.

[ii] Reducing System's Public Information. In polynomial based schemes such as Shamir's scheme, each user is associated with two pieces of information:

one is an index/identity that can be made public, and a second that is the share of the secret. In some cases [27] to add extra security properties, the public part is also made private. On the other hand in some cases [14] to provide extra properties such as robustness, the public part of the user is enlarged, and/or the secret part of the share grows [4]. An interesting question is to what extent private *and* public information associated with a user can be reduced. In this paper we ask this question in the context of RSS and in particular our proposed RSS scheme. We show that the public information can be nearly halved. To achieve this we first construct a variant of Shamir secret sharing. We will then use this scheme to construct an RSS with the same share length (for the secure part of share) as the scheme in Sect. 3, but with the extra property that it has only $t+1$ field elements for its public values. This nearly halves the amount of public information and effectively results in the least total share storage/communication among all known threshold robust secret sharing schemes.

[iii] Secret Sharing with Cheating Detection. The robust secret sharing scheme in Sect. 3 builds on a secret sharing scheme with cheating detection property. We describe the underlying scheme in Sect. 5. In the previous section we noted the two common security models for secret sharing with cheating detection. We evaluate security of our scheme in OKS model and show that it has the smallest possible share size, satisfying with equality the lower bound in (1) for such schemes. There are two other known optimal schemes [22,23] in OKS model, both imposing restrictions on the secret set. In particular the scheme in [23] requires that the secret set be a finite field with characteristic different from 2, and the construction in [22] requires a number q such that q be a prime power and q^2+q+1 is a prime. The latter scheme also assumes that secret is *chosen with uniform distribution* hence using a weaker security notion. In our scheme secret can be from any finite field and the only requirement is that the field size to be $\geq n$ which is a general requirement for all schemes. We use the strong definition of security which requires security for any distribution on the secret set.

1.2 Related Work

It is known that, in the range $\frac{n}{3} \leq t < \frac{n}{2}$, robust secret sharing is possible, but only if one admits a small but positive failure probability (denoted as δ) in reconstructing the correct secret.The first solution to the problem of designing robust secret sharing schemes with absolute correctness in reconstruction (i.e., the error probability $\delta = 0$) was presented by McElice and Sarwate [20], where error correcting technique for Reed-Solomon codes are used to enhance the original Shamir secret sharing scheme with the robustness property. Their scheme assumes $n \geq 3t+1$. Moreover, it follows immediately from the theory of Reed-Solomon error correcting codes that the condition $n \geq 3t+1$ ($t \leq \frac{n-1}{3}$) is also necessary for Shamir's scheme to be robust with $\delta = 0$. In fact, the above is true for any (t, n)-threshold secret sharing scheme. It was shown in [16] that a secret sharing scheme realizing an access structure Γ has robustness property

with $\delta = 0$ precisely when the access structure Γ satisfies a condition called $\mathcal{Q}^3$ [12]. A monotone access structure Γ for a set $\mathcal{P}$ of participants is said to satisfy $\mathcal{Q}^3$ condition if $A_1 \cup A_2 \cup A_3 \neq \mathcal{P}$ for any $A_1, A_2, A_3 \in \Gamma^c$, where Γ^c is $2^{\mathcal{P}} \backslash \Gamma$. The (t, n)-threshold access structure satisfies $\mathcal{Q}^3$ precisely when $n \geq 3t + 1$.

Constructions for threshold robust secret sharing schemes with unconditional security for $n = 2t + 1$ can be broadly divided into two classes. We briefly describe the best scheme in each class. The scheme due to Cramer et al. [7] follows the approach of [2]. It uses standard Shamir secret sharing and distributes the shares of three field elements that are algebraically related: 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 $\rho = s \cdot r$. The reconstructor does the following: for every subset of $t + 1$ players, he reconstructs s', r' and ρ' and checks if $s' \cdot r' = \rho'$, 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 $s' \cdot r' \neq \rho'$ except with probability $1/|\mathbb{F}_q|$. Thus if $\lfloor \log_2 |\mathbb{F}_q| \rceil = k$, taking into account union bound over all subsets of size t + 1, gives a robust secret sharing scheme with failure probability $\delta = \frac{1}{2^{k-n}}$ and shares of size $3k$ $(= k + 2\log_2 \frac{1}{\delta} + 2n)$ bits. Therefore the redundancy in share size is $2\log_2 \frac{1}{\delta} + 2n$. The reconstruction procedure of this scheme has running time which is exponential in the number of players.

The second scheme is given by Cevellos, Fehr, Ostrovsky and Rabani [4], and is based on the scheme of Rabin and Ben-Or [25]. The Share distribution algorithm of this scheme is the same as the well-known scheme of Rabin and Ben-Or [25] which is the standard Shamir secret sharing scheme, but enhanced by means of an (unconditionally secure) message authentication code (MAC : $\mathcal{M} \times \mathcal{K} \to \mathcal{T}$, $\mathcal{M} = \mathbb{F}_q, \mathcal{K} = \mathbb{F}_q \times \mathbb{F}_q$, and $\mathcal{T} = \mathbb{F}_q$). In particular, for every pair of players P_i and P_j, P_i's Shamir share $s_i \in \mathcal{M}$ is authenticated with an authentication tag $\tau_{ij} \in \mathcal{T}$, where the corresponding authentication key $k_{ji} \in \mathcal{K}$ is given to player P_j. Therefore, beyond the actual Shamir share, every player gets $3n$ field elements as part of his share. The scheme by [4] 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. Finally the redundancy in share size for the scheme is $3\log_2 \frac{1}{\delta} + 3n\log_2(n\lambda)$ bits, where λ is an independent security parameter and δ is the scheme's error probability.

Cheating detection was first consisted by Tompa and Woll [27]. Their work was followed by a number of authors including [3,2,22]. In OKS model, the only two known share-optimal schemes [23,22] impose *restrictions on the secret set.* Construction of SSCD schemes in this model that meet the lower bound is an interesting open problem.

Applications. 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 [18,28,9] which shows importance of threshold robust secret sharing in practice. Threshold robust secret sharing has also direct application to Secure Message Transmission (SMT) [8,10,11]. In an unconditionally secure SMT, 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 [8,19]. Robust secret sharing schemes may also be seen as an stepping stone towards the construction of verifiable secret sharing (VSS) schemes [5,24], 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.

2 Preliminaries

2.1 Robust Secret Sharing

Secret sharing schemes, that satisfy the additional property, that the secret can be reconstructed from the set of *all* shares even if some players provide incorrect shares, are called *robust secret sharing schemes*. In order to clearly define the robustness property of a secret sharing, we describe a secret sharing scheme by means of two interactive protocols, Share and Rec, where Share involves a dealer $\mathcal{D}$ and n players $P_1, \ldots, P_n$, and the reconstruction protocol Rec involves the n players and the reconstructor $\mathcal{R}$, a trusted third party. 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. We now describe the protocols Share and Rec. Let $[n] = \{1, \ldots, n\}$.

- Share: The dealer $\mathcal{D}$ takes as input a secret $s \in S$, 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, each player P_i, communicates, possibly by means of several synchronous communication rounds[1], its share σ_i to $\mathcal{R}$. The reconstructor uses the received shares to produce an output s', which is supposed to be the secret s.

Security. We now define the security goals of a (t, n)-threshold robust secret sharing scheme. We begin by defining the adversary.

Adversarial Capability. We consider unbounded adversary. In the reconstruction phase Rec, the adversary $\mathcal{A}$ adaptively corrupts up to t players. The corruption can be done between communication rounds and continue as long as

[1] In each round, every player P_i sends *a part* of its full share σ_i. In case, when the Rec is *single round*, each player sends σ_i.

the total number of corrupted players does not exceed t. Once a player P_i is corrupted, the adversary learns P_i's share σ_i, and from then on, he controls the information that P_i send to $\mathcal{R}$. By a **rushing** adversary we mean, in every communication round, he can decide for every corrupted player on what this player should send to $\mathcal{R}$, depending on what he has seen so far and depending on what the honest players have sent to $\mathcal{R}$ in the current round. By contrast, a **non-rushing**[2] adversary is one who selects the corrupted shares before the start of each round.

Privacy. By the perfect privacy of a (t, n)-threshold RSS scheme we mean that at the end of the share distribution protocol Share, no t players has any information about the secret. Formally, for any subset $B \subset \{P_1, \ldots, P_n\}$ of size at most t and for every two elements $s_1, s_2 \in S$, we have

$$\text{Prob}[\text{Secret is } s_1 \mid \mathsf{view}_B] = \text{Prob}[\text{Secret is } s_2 \mid \mathsf{view}_B],$$

where view_B denotes the total available information for the members of B to see. The probabilities are taken over the random coins of Share.

Robustness. We now define the (t, δ)-robustness property of an n-player robust secret sharing scheme $\Pi = (\mathsf{Share}, \mathsf{Rec})$. To describe it clearly, we consider the following game called the "robustness game".

Robustness Game

1. **Share distribution phase:** The dealer $\mathcal{D}$ picks a secret $s \in S$, and uses Share to compute shares $\sigma_1, \ldots, \sigma_n$ for the n players; σ_i is given privately to P_i, $1 \leq i \leq n$.
2. **Reconstruction Phase:** In this phase, the adversary $\mathcal{A}$ adaptively corrupts up to t players as described above.
3. **Final Phase:** At the end of reconstruction phase, $\mathcal{R}$ has all the n shares and at most t of them are incorrect. Based on the shares, $\mathcal{R}$ outputs the secret s'. The adversary is said to win if $s' \neq s$.

We now define the advantage of $\mathcal{A}$ in the above game as

$$\text{Adv}^{\mathsf{Robust}}_{\Pi,(t,n)}(\mathcal{A}) = \text{Prob}[s' \neq s].$$

Definition 1. *A (t, n)-threshold robust secret sharing scheme $\Pi = (\mathsf{Share}, \mathsf{Rec})$ is said to be unconditionally secure with (t, δ)-robustness property against non-rushing adversary, if it has both perfect privacy and $Adv^{\mathsf{Robust}}_{\Pi,(t,n)}(\mathcal{A}) \leq \delta$ in the above game.*

In this paper, we present RSS schemes with single round reconstruction. The schemes are secure against non-rushing adversary.

[2] Security against non-rushing adversary makes sense in a communication model enhanced with a simultaneous broadcast channel, i.e., one by means of which all players broadcast their information at the same time.

2.2 Lagrange Interpolation

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

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

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

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

To simplify the notation, we write $\lambda_{x_i}(x)$ for $\lambda_{x_i}^A(x)$ when the description of the set A is clear from the context. We define Lagrange coefficients as $\lambda_{x_i} = \lambda_{x_i}(0)$. Therefore, from equation (2) we have $f(0) = \sum_{i=1}^{t+1} y_i \lambda_{x_i}$. One may also note that $\sum_{i=1}^{t+1} \lambda_{x_i} = 1$.

2.3 Shamir Secret Sharing

Let $f(x) = s + a_1 x + \cdots + a_t x^t$. The secret is $f(0) = s$. Player P_i will receive an ordered pair $(\alpha_i, f(\alpha_i))$. It is easy to show that this is a threshold scheme, since for any $t+1$ participants, there is only one polynomial of degree at most t passing through their $t+1$ points. Also it is a perfect threshold scheme since for any t points and any point $(0, s')$, there is a unique polynomial of degree at most t passing through their t points and $(0, s')$. The scheme becomes ideal if the values $\{\alpha_i\}_{i=1}^n$ are publicly revealed (the values does not yield any information about s) so that the share of player P_i is just the value $f(\alpha_i)$.

3 The New Scheme: RSSS-Basic

We noted that in the scheme in [7], the relation $\rho = s \cdot r$ is formed and ρ, r and s individually shared. Our first observation is that in [7] one only needs to distribute (Shamir secret sharing) shares of s and r and make ρ the public parameter. We note that, knowledge of ρ and t shares does not reveal any information about the secret and so this appears as a promising approach. This approach however does not guarantee the required robustness. Following this direction, we use the Rabin and Ben-Or's Information Checking [25] vectors[3] (relation) and construct an efficient RSS with unconditional security. We now describe our scheme.

[3] Information Checking Vector (α, β): Let $s \in \mathbb{F}_q$. Let $\alpha \neq 0$ and y be randomly chosen from $\mathbb{F}_q$ and $\beta = s + \alpha y$. Then the tuple (α, β) will reveal no information about s.

We have a group of n players $\{P_1, \ldots, P_n\}$. Let t and n are positive integers such that $n = 2t + 1$. We fix a finite field $\mathbb{F}_q$ with $q > n$, and n distinct points, $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q$, known to all players. We now present a (t, n)-threshold robust secret sharing scheme.

- Share: On input a secret $s \in \mathbb{F}_q$, the share generation algorithm Share outputs a list of shares as follows:
  - The dealer $\mathcal{D}$ chooses random $r, X(\neq 0) \in \mathbb{F}_q$ with uniform distribution and computes $Y = s + Xr$.
  - $\mathcal{D}$ chooses t random elements $f_1, \ldots, f_t$ from $\mathbb{F}_q$ independently with uniform distribution. These random elements together with s define a polynomial $f(x) = s + \sum_{i=1}^{t} f_i x^i$. $\mathcal{D}$ then computes $s_i = f(\alpha_i)$ for all $i \in [n]$.
  - $\mathcal{D}$ also picks t random elements $g_1, \ldots, g_t \in \mathbb{F}_q$ independently with uniform distribution. These random elements together with r define a polynomial $g(x) = r + \sum_{i=1}^{t} g_i x^i$. $\mathcal{D}$ then computes $r_i = g(\alpha_i)$ for all $i \in [n]$.
  - Every player P_i gets his/her share $\sigma_i = (s_i, r_i)$. The tuple (X, Y) is part of system's public parameters.
- Rec: The secret reconstruction algorithm Rec outputs the secret as follows:
  - Every player sends (s'_i, r'_i) to the reconstructor $\mathcal{R}$. Therefore, $\mathcal{R}$ receives n shares, at most t of which are possibly incorrect.
  - To reconstruct the secret, $\mathcal{R}$ does the following for *every subset* of $t + 1$ players $\{P_{i_1}, \ldots, P_{i_{t+1}}\}$:
    - Computes, $s' = \sum_{j=1}^{t+1} \lambda_{i_j} s'_{i_j}$ and $r' = \sum_{j=1}^{t+1} \lambda_{i_j} r'_{i_j}$ (Lagrange interpolation).
    - Checks, if $Y = s' + Xr'$.
    - If yes, $\mathcal{R}$ then outputs the secret as s'.

3.1 Privacy

The following theorem shows, that no t players has any information about the secret.

Theorem 1. *For any subset $B \subset \{P_1, \ldots, P_n\}$ of size t and its* view_B

$$Prob[\textit{Secret is } s_1 \mid \mathsf{view}_B] = Prob[\textit{Secret is } s_2 \mid \mathsf{view}_B],$$

for all $s_1, s_2 \in \mathbb{F}_q$, where view_B *denotes the elements, that the members of B see:* $\mathsf{view}_B = (X, Y, \{(s_i, r_i)_{P_i \in B}\})$.

Proof: Without loss of generality, let $B = \{P_1, \ldots, P_t\}$. Then view_B $= (X, Y, \{(s_i, r_i)_{i=1}^{t}\})$. For every choice of $s \in \mathbb{F}_q$ for secret, we have: a unique value for $r = X^{-1} \cdot (Y - s)$, a unique polynomial f of degree at most t such that $f(0) = s; f(\alpha_i) = s_i$ for $1 \leq i \leq t$, and a unique polynomial g of degree at most t such that $g(0) = r; g(\alpha_i) = r_i$ for $1 \leq i \leq t$. As the set of actual unknowns were chosen independently with uniform distribution, hence, for every $s \in \mathbb{F}_q$, $\Pr[s \text{ is secret} \mid (s_i, r_i)_{P_i \in B}] = \frac{1}{q^{2t+1}}$. Since the probability is the same for every $s \in \mathbb{F}_q$, the privacy follows.

3.2 Robustness

Theorem 2. *Let $\mathbb{F}_q$ be any finite field with q elements. Let $k = \lfloor \log_2 q \rceil$. Then for any positive integers n, t with $n = 2t + 1$, $q > n$, and secret space $\mathbb{F}_q$, RSSS-Basic forms an unconditional secure (t, n)-threshold robust secret sharing scheme with (t, δ) robustness against non-rushing adversary such that*

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

Proof: Consider an arbitrary set A of $t+1$ shares revealed in the reconstruction phase. If A consists exclusively of shares of honest players, then the secret s' reconstructed by $\mathcal{R}$ would certainly be the correct secret s. Else, either a failure would be detected, or an incorrect secret $s' \neq s$ is accepted based on the shares in A. We now compute the probability for the case when $s' \neq s$ but $Y = s' + Xr'$. Let $s' = s + \epsilon_s$ and $r' = r + \epsilon_r$. The value s' is accepted for the secret if and only if the corrupted shares in A leads to a pair $(\epsilon_s, \epsilon_r) \in \mathbb{F}_q \times \mathbb{F}_q$ such that $\epsilon_s \neq 0$ and $Y = (s+\epsilon_s) + X(r+\epsilon_r)$. But $Y = (s+\epsilon_s) + X(r+\epsilon_r) = s + Xr + \epsilon_s + X\epsilon_r$ implies $\epsilon_s + X\epsilon_r = 0$. Thus we see that, for every $(\epsilon_s, \epsilon_r) \in \mathbb{F}_q \times \mathbb{F}_q$ with $\epsilon_s \neq 0$, there is a unique value of $\epsilon_r = -X^{-1}\epsilon_s$ $(X \neq 0)$ such that $Y = (s + \epsilon_s) + X(r + \epsilon_r)$. Hence, for any set of $t+1$ shares containing at most t corrupted shares, a wrong secret is accepted with probability at most $\frac{1}{q}$. Therefore, taking into account, the union bound of probabilities over all subsets of size t+1, the probability that an incorrect secret is accepted in the reconstruction process is at most $\frac{2^n}{q} = \frac{1}{2^{k-n}}$.

3.3 Efficiency Comparison

Set the secret space $S = \mathbb{F}_q$. We now compare the share efficiency of our construction with the schemes of [7,4]. One may note that, for all the three schemes, the error probability δ is determined directly by the cardinality of the secret space. For our construction and [7], we have $\delta = \frac{2^n}{|\mathbb{F}_q|}$, i.e., $\log_2 \frac{1}{\delta} + n = \log_2 |\mathbb{F}_q|$. For [4], δ is dictated by $|\mathbb{F}_q|$ and an independent parameter λ[4]; specifically $\delta = \frac{1}{2^{n\frac{\log_2 |\mathbb{F}_q|}{\lambda} - n\log_2(n\cdot\lambda)}}$ (improved error probability over the other two schemes). We set $k = \lfloor \log_2 |\mathbb{F}_q| \rceil$ (in bits). The following table exhibit the individual share redundancy (in bits).

Table 1. Comparison Table

Scheme	Secret size	Redundancy	δ	Rec Complexity
[7]	k	$2(\log_2 \frac{1}{\delta} + n)$	$2^{-(k-n)}$	$\exp(n)$
[4]	k	$3\log_2 \frac{1}{\delta} + 3n\log_2(n\lambda)$	$2^{-(n\frac{k}{\lambda} - n\log_2(n\cdot\lambda))}$	poly(n)
RSSS-Basic	k	$\log_2 \frac{1}{\delta} + n$	$2^{-(k-n)}$	$\exp(n)$

[4] In [4], each player gets n tags and n keys beside the actual share. The length of tags and keys are determined by $MAC : \mathbb{F}_q \times (\mathbb{F}_q/2^\lambda)^2 \to \mathbb{F}_q/2^\lambda$. The tag space $\mathcal{T} = \mathbb{F}_q/2^\lambda$ and key space $\mathcal{K} = (\mathbb{F}_q/2^\lambda)^2$. Therefore, the share size redundancy is $3n\frac{\log_2 |\mathbb{F}_q|}{\lambda} = 3\log_2 \frac{1}{\delta} + 3n\log_2(n\lambda)$ bits.

4 Robust Secret Sharing with Savings on Public Data

In a secret sharing scheme shares carry information about the secret and need to be securely stored and so the share size is the main efficiency parameter of a secret sharing scheme. For reconstruction, secret sharing schemes may also use some public values associated with each player. For example in Shamir's secret sharing each user has an associated field element $\alpha_i \in \mathbb{F}_q$. The share of the player is $f(\alpha_i)$ which is securely stored by the user. The reconstruction needs the tuple $(\alpha_i, f(\alpha_i))$. The value α_i can be stored publicly and so is not considered in measuring share efficiency of schemes. This means without extra setup assumptions such as existence of a public bulletin board that allows access to the non-sensitive part of the secret when needed, for a $\log_2 |\mathbb{F}_q|$ bit secret in Shamir's scheme, $2\log_2 |\mathbb{F}_q|$ bits need to be stored and presented at the reconstruction time. Taking into account the interpolation points, for the robust secret sharing scheme in Section 3, a user's storage is essentially $3\log_2 |\mathbb{F}_q|$ bits and therefore the total communication[5] during reconstruction is $3n \log_2 |\mathbb{F}_q|$ bits. An interesting question is if the total share storage can be reduced.

In the following we present a threshold robust secret sharing for $n = 2t + 1$ with the property that we can save on t interpolation points. This is the least total share storage/communication among all known threshold robust secret sharing schemes.The scheme follows the approach of RSSS-Basic, in achieving robustness, but replaces the Shamir secret sharing with a new ideal polynomial based secret sharing that allows us to reduce the public values. We begin by first describing our variant of Shamir's scheme.

4.1 A Variant of Shamir Secret Sharing

We have a group of n players $\{P_1, \ldots, P_n\}$. Let t be a positive integer such that $1 \leq t \leq n$. We fix a prime $q > n$, and n distinct points, $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q$, known to all players. We now present a (t, n)-threshold secret sharing scheme.

- Share: On input a secret $s \in \mathbb{F}_q$, the share generation algorithm Share outputs a list of shares as follows:
  - The dealer $\mathcal{D}$ chooses t random elements $f_1, \ldots, f_t$ from $\mathbb{F}_q$ independently with uniform distribution. These random elements together with s define a polynomial $f(x) = s + \sum_{i=1}^{t} f_i x^i$. $\mathcal{D}$ then computes $s_i = f(\alpha_i)$ for all $i \in [n]$.
  - He then computes $\sigma_i = s + \alpha_i s_i$ for all $i \in [n]$.
  - For every $i \in [n]$, the dealer sends to player P_i the share σ_i.
- Rec: Any $t+1$ players $\{P_{i_1}, \ldots, P_{i_{t+1}}\}$ with their shares $\{\sigma_{i_1}, \ldots, \sigma_{i_{t+1}}\}$, compute the secret as follows: $s = \left(\lambda_{i_1} \prod_{j \neq 1} \alpha_{i_j} + \cdots + \lambda_{i_{t+1}} \prod_{j \neq t+1} \alpha_{i_j} + \prod_{j=1}^{t+1} \alpha_{i_j}\right)^{-1} \cdot \left(\lambda_{i_1} \prod_{j \neq 1} \alpha_{i_j} \sigma_{i_1} + \cdots + \lambda_{i_{t+1}} \prod_{j \neq t+1} \alpha_{i_j} \sigma_{i_{t+1}}\right)$.

[5] We are not counting the information which is same for all the players, like the threshold parameter or the description of the underlying field.

4.2 Correctness

The correctness of the scheme requires that any $t+1$ correct shares would output the original secret.

$$\begin{aligned}
&\lambda_{i_1} \prod_{j \neq 1} \alpha_{i_j} \sigma_{i_1} + \cdots + \lambda_{i_{t+1}} \prod_{j \neq t+1} \alpha_{i_j} \sigma_{i_{t+1}} \\
&= \lambda_{i_1} \prod_{j \neq 1} \alpha_{i_j} (s + \alpha_{i_1} s_{i_1}) + \cdots + \lambda_{i_{t+1}} \prod_{j \neq t+1} \alpha_{i_j} (s + \alpha_{i_{t+1}} s_{i_{t+1}}) \\
&= s(\lambda_{i_1} \prod_{j \neq 1} \alpha_{i_j} + \cdots + \lambda_{i_{t+1}} \prod_{j \neq t+1} \alpha_{i_j}) + \prod_{j=1}^{t+1} \alpha_{i_j} (\sum_{j=1}^{t+1} \lambda_{i_j} s_{i_j}) \\
&= s(\lambda_{i_1} \prod_{j \neq 1} \alpha_{i_j} + \cdots + \lambda_{i_{t+1}} \prod_{j \neq t+1} \alpha_{i_j}) + \prod_{j=1}^{t+1} \alpha_{i_j} s \\
&= s(\lambda_{i_1} \prod_{j \neq 1} \alpha_{i_j} + \cdots + \lambda_{i_{t+1}} \prod_{j \neq t+1} \alpha_{i_j} + \prod_{j=1}^{t+1} \alpha_{i_j}).
\end{aligned}$$

Remark 1. In the scheme, a user's share is $\sigma_i = s + \alpha_i s_i$, where $\{\alpha_1, \ldots, \alpha_n\}$ denotes the interpolation points. We observe that, correctness will still holds if a user's share is computed as follows: $(\beta_i, \sigma_i = s + \beta_i s_i)$ for $1 \leq i \leq n$, where $\{\beta_1, \ldots, \beta_n\}$ are random field elements and the interpolation points $\{\alpha_1, \ldots, \alpha_n\}$ are kept public as usual. This fact would help us derive the correctness of our robust secret sharing scheme in the next section.

4.3 Privacy

The privacy of the scheme follows as a special case of the privacy of information checking procedure from [25]. We first prove the following lemma for completeness.

Lemma 1. *([25]) Let $s \in \mathbb{F}_q$ be the secret. Let random elements $\alpha \neq 0$ and y are chosen from $\mathbb{F}_q$ independently with uniform distribution. Compute $\beta = s + \alpha y$. Then the tuple (α, β) will reveal no information about s.*

Proof: Note that for every value of s in $\mathbb{F}_q$, there exists a unique value for y in $\mathbb{F}_q$, namely $y = \alpha^{-1}(\beta - s)$, such that $\beta = s + \alpha y$. Therefore, Prob[secret is $s \mid (\alpha, \beta)$] = Prob[$y = \alpha^{-1}(\beta - s)$ is chosen] = $\frac{1}{|\mathbb{F}_q|}$. Thus (α, β) gives no information about s.

Rabin and Ben-Or [25] observed that, the above lemma immediately generalizes to the following. For a secret $s \in \mathbb{F}_q$, any positive integer ℓ, and $\alpha_1, \ldots, \alpha_\ell \in \mathbb{F}_q \backslash \{0\}$ choose random elements $y_1, \ldots, y_\ell \in \mathbb{F}_q$ independently with uniform distribution. Compute $\beta_i = s + \alpha_i y_i$ for $1 \leq i \leq \ell$. Then the tuples $\{(\alpha_i, \beta_i)\}_{1 \leq i \leq \ell}$ will reveal no information about s. We know that for Shamir secret sharing scheme, any t shares are independent from the secret s. Thus for any t Shamir shares $(s_{i_1}, \ldots, s_{i_t})$, the values $\sigma_{i_j} = s + \alpha_{i_j} s_{i_j}$, $1 \leq j \leq t$ will give no information about the secret s. This shows the perfect privacy of the above scheme.

4.4 The New Scheme: RSSS

Let $\mathbb{F}_q$ be a field. Let t and n are positive integers such that $n = 2t+1$. We now present an n-player robust secret sharing scheme.

- Share: On input a secret $s \in \mathbb{F}_q$, the share generation algorithm Share outputs a list of shares as follows:
  - The dealer $\mathcal{D}$ chooses random $r, X(\neq 0) \in \mathbb{F}_q$ with uniform distribution and computes $Y = s + Xr$.
  - The dealer chooses two sets of random t points $s_1, \ldots, s_t$ and $r_1, \ldots, r_t$ from $\mathbb{F}_q$ independently with uniform distribution.
  - It then computes unique set of t points $\alpha_1, \ldots, \alpha_t$, where $\alpha_i = r_i s_i^{-1}$, $1 \leq i \leq t$.
  - The dealer $\mathcal{D}$ then interpolates the unique polynomial f of degree at most t such that $f(0) = s$ and $f(\alpha_i) = s_i$ for all $1 \leq i \leq t$. The dealer also interpolates the unique polynomial g of degree at most t such that $g(0) = r$ and $g(\alpha_i) = r_i$ for all $1 \leq i \leq t$.
  - $\mathcal{D}$ picks $t+1$ random points $\beta_{t+1}, \ldots, \beta_n \in \mathbb{F}_q$ with uniform distribution, and also sets $\beta_i = \alpha_i$ for $1 \leq i \leq t$.
  - It then computes $s_i = f(\beta_i)$ for $t+1 \leq i \leq n$, $r_i = g(\beta_i)$ for $t+1 \leq i \leq n$, and $\alpha_i = r_i s_i^{-1}$ for $t+1 \leq i \leq n$.
  - The dealer finally computes $\sigma_i = s + r_i$ for all $i \in [n]$. Every participant P_i will receive an ordered pair (σ_i, α_i). The tuple (X, Y) along with $t+1$ points $\beta_{t+1}, \ldots, \beta_n$ are part of system's public parameters (Note that the players $\{P_1, \ldots, P_t\}$ have interpolation points $\beta_i = \alpha_i$, $1 \leq i \leq t$, respectively).
- Rec: The secret reconstruction algorithm Rec outputs the secret as follows:
  - Every player sends their share (σ'_i, α'_i) to the reconstructor $\mathcal{R}$.
  - To reconstruct the secret, $\mathcal{R}$ does the following for *every subset* of $t+1$ players $\{P_{i_1}, \ldots, P_{i_{t+1}}\}$:
    - $\mathcal{R}$ computes, $s' = \left(\lambda_{i_1} \prod_{j \neq 1} \alpha'_{i_j} + \cdots + \lambda_{i_{t+1}} \prod_{j \neq t+1} \alpha'_{i_j} + \prod_{j=1}^{t+1} \alpha'_{i_j}\right)^{-1} \cdot \left(\lambda_{i_1} \prod_{j \neq 1} \alpha'_{i_j} \sigma'_{i_1} + \cdots + \lambda_{i_{t+1}} \prod_{j \neq t+1} \alpha'_{i_j} \sigma'_{i_{t+1}}\right)$.
    - It then computes $r'_{i_j} = \sigma'_{i_j} - s'$ for all $1 \leq j \leq t+1$.
    - It computes $r' = \sum_{j=1}^{t+1} \lambda_{i_j} r_{i_j}$ and checks if $Y = s' + Xr'$.
    - If yes, then $\mathcal{R}$ outputs the secret as s'.

4.5 Correctness and Efficiency

During the reconstruction, if the $t+1$ shares $(\sigma'_{i_j}, \alpha'_{i_j})$'s are all correct i.e., $(\sigma'_{i_j}, \alpha'_{i_j}) = (\sigma_{i_j}, \alpha_{i_j})$ for all $1 \leq j \leq t+1$, then $s' = s$, the correct secret. This follows immediately from Remark 1 in Sect. 4.2. We now give a table to summarize the efficiency of the scheme.

Table 2. Comparison Table

Scheme	Redundancy	Rec Complexity	δ	Saving on Interpolation Pts
[7]	$2(\log_2 \frac{1}{\delta} + n)$	$\exp(n)$	$2^{-(k-n)}$	-
[4]	$3\log_2 \frac{1}{\delta} + 3n\log_2(n\lambda)$	$\text{poly}(n)$	$2^{-(n\frac{k}{\lambda} - n\log(n\cdot\lambda))}$	-
RSSS	$\log_2 \frac{1}{\delta} + n$	$\exp(n)$	$2^{-(k-n)}$	t

4.6 Privacy

The following theorem shows, that any t players get no information about the secret.

Theorem 3. *For any subset $B \subset \{P_1, \ldots, P_n\}$ of size t and its* view_B

$$Prob[Secret\ is\ s_1 \mid \mathsf{view}_B] = Prob[Secret\ is\ s_2 \mid \mathsf{view}_B],$$

for all $s_1, s_2 \in \mathbb{F}_q$, where view_B *denotes the elements, that the members of B see:* $\mathsf{view}_B = (X, Y, \{(\sigma_i, \alpha_i)_{P_i \in B}\})$.

Proof: Consider any set $B = \{P_{i_1}, \ldots, P_{i_t}\}$ of t players. Therefore, we have $\mathsf{view}_B = (X, Y, \{(\sigma_{i_j}, \alpha_{i_j})_{j=1}^{t}\})$. For every choice of $s \in \mathbb{F}_q$ for secret, we have: unique values for $r = X^{-1} \cdot (Y - s); r_{i_j} = \sigma_{i_j} - s,\ 1 \le j \le t; s_{i_j} = \alpha_{i_j}^{-1} \cdot (\sigma_{i_j} - s) = \alpha_{i_j}^{-1} \cdot r_{i_j},\ 1 \le j \le t$, a unique polynomial f of degree at most t satisfying $f(0) = s; f(\beta_{i_j}) = s_{i_j}$ for $1 \le j \le t$, and a unique polynomial g of degree at most t such that $g(0) = r; g(\beta_{i_j}) = r_{i_j}$ for $1 \le j \le t$. Therefore, the t players in B cannot rule out any element of $\mathbb{F}_q$ as a possibility for secret. This shows that view_B does not contain any information about the original secret.

4.7 Robustness

One may note that, both the schemes, RSSS-Basic and RSSS are similar. The later scheme achieves some advantage due to the restructuring of the former. In the previous section, we proved, the restructuring did not affect the privacy of the scheme and therefore the robustness property of RSSS remain the same as for RSSS-Basic. For completeness, we now state the theorem. The proof is similar to RSSS-Basic.

Theorem 4. *Let $\mathbb{F}_q$ be any finite field with q elements. Let $k = \lfloor \log_2 q \rceil$. Then for any positive integers n, t with $n = 2t + 1$, $q > n$, and secret space $\mathbb{F}_q$, RSSS forms an unconditional secure (t, n)-threshold robust secret sharing scheme with (t, δ) robustness against non-rushing adversary such that*

$$\delta \le \frac{1}{2^{k-n}} \ .$$

5 Secret Sharing with Cheating Detection

Tompa and Woll [27] introduced the problem of cheating detection in secret sharing. Suppose that, in a (t, n) threshold secret sharing scheme, t players, say $P_1, \ldots, P_t$, want to cheat a $(t+1)$th player, P_{t+1}, by opening modified shares $\sigma'_1, \ldots, \sigma'_t$. They succeed if the secret s' that is reconstructed from $\sigma'_1, \ldots, \sigma'_t$ and σ_{t+1} is different from the original secret s (see Section 2.1 of [22] for a thorough definition). There are two different models, CDV and OKS, for secret sharing schemes capable of detecting such cheating. The CDV model is characterized by the property that t cheaters (corrupted players) $P_1, \ldots, P_t$ somehow know the secret s before they cheat P_{t+1}, whereas in OKS model, they does not have any idea about the secret. In [22], a lower bound on share size has been derived for secret sharing schemes with cheating detection property in OKS model; $\log_2 \sigma_i \geq \log_2 s + \log_2 \frac{1}{\delta_c}$, where δ_c is the cheating probability. Therefore, in the above model, the redundancy in share size is at least $\log_2 \frac{1}{\delta_c}$.

One may easily note that our robust secret sharing scheme RSSS-Basic in Section 3 is build upon a secret sharing scheme with cheating detection property. We see that the share size, for the underlying secret sharing scheme with the property of cheating detection, meets the lower bound of [22]. We observe that this is the first such scheme. To the best of our knowledge, there exists two schemes [22,23] in the literature that satisfy the above lower bound, but both the schemes admit some limitations whereas our scheme is free from any such limitation. In particular, the scheme of [23] requires that the secret should lie in a field whose characteristic is different from 2, and the construction of [22] requires a number q such that q be a prime power and $q^2 + q + 1$ is also prime. The latter scheme also assumes that secret is *chosen with uniform distribution* and so effectively has a weaker security notion. In our scheme secret can be from any filed and only requires the field size to be $\geq n$. This is a general restriction on all scheme. We use the strong definition of security which requires security for any distribution on the secret set. For completeness, we now describe our scheme.

5.1 The Scheme

We have a group of n players $\{P_1, \ldots, P_n\}$. Let t be a positive integer such that $1 \leq t \leq n$. We fix a prime $q > n$, and n distinct points, $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q$, known to all players. We now present a (t, n)-threshold secret sharing scheme with cheating detection property.

- Share: On input a secret $s \in \mathbb{F}_q$, the share generation algorithm Share outputs a list of shares as follows:
  - The dealer $\mathcal{D}$ chooses random $r, X(\neq 0) \in \mathbb{F}_q$ with uniform distribution and computes $Y = s + Xr$.
  - The dealer $\mathcal{D}$ chooses t random elements $f_1, \ldots, f_t$ from $\mathbb{F}_q$ independently with uniform distribution. These random elements together with s define a polynomial $f(x) = s + \sum_{i=1}^{t} f_i x^i$. $\mathcal{D}$ then computes $s_i = f(\alpha_i)$ for all $i \in [n]$.

- $\mathcal{D}$ also chooses t random elements $g_1, \ldots, g_t$ from $\mathbb{F}_q$ independently with uniform distribution. These random elements together with r define a polynomial $g(x) = r + \sum_{i=1}^{t} g_i x^i$. $\mathcal{D}$ then computes $r_i = g(\alpha_i)$ for all $i \in [n]$.
- Every participant P_i will receive its share $\sigma_i = (s_i, r_i)$.
- The tuple (X, Y) is part of system's public parameters.

– Rec: Any qualified set of players ($t+1$ players) $\{P_{i_1}, \ldots, P_{i_{t+1}}\}$ will reconstruct the secret as follows.
- They obtain $s = \sum_{j=1}^{t+1} \lambda_{i_j} s_{i_j}$ and $r = \sum_{j=1}^{t+1} \lambda_{i_j} r_{i_j}$ from their shares.
- If $Y = s + Xr$, they take s as the correct value of the secret.

5.2 Security and Share Size Efficiency

The privacy of the scheme follows from Theorem 1. The cheating probability of the above scheme follows from Theorem 2, in particular the cheating probability δ_c is $\frac{1}{q} = \frac{1}{2^k}$ and it holds for arbitrary distribution on the secret space. The individual share size of each player is $\log_2 \sigma_i = 2k = \log_2 s + \log_2 \frac{1}{\delta_c}$. Therefore this scheme meets the lower bound of [22] in the OKS model. One may also note that, a secret sharing scheme with cheating detection property can also extracted from RSSS with the added property of saving t interpolation points.

Acknowledgments. The authors would like to thank Pengwei Wang for useful discussions. The Authors would also like to thank the reviewers for their comments.

References

1. Blakley, G.: Safeguarding cryptographic keys. AFIPS National Computer Conference 48, 313–317 (1979)
2. 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)
3. 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)
4. 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)
5. 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)
6. Choudhury, A.: Brief announcement: optimal amortized secret sharing with cheater identification. In: Kowalski, D., Panconesi, A. (eds.) PODC, pp. 101–102. ACM (2012)
7. Cramer, R., Damgård, I.B., Fehr, S.: On the cost of reconstructing a secret, or VSS with optimal reconstruction phase. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 503–523. Springer, Heidelberg (2001)

8. Dolev, D., Dwork, C., Waarts, O., Yung, M.: Perfectly secure message transmission. In: FOCS 1990, pp. 36–45. IEEE Computer Society (1990)
9. 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 amp; Exposition II, DISCEX 2001, vol. 2, pp. 184–195 (2001)
10. Garay, J., 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)
11. 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)
12. Hirt, M., Maurer, U.M.: Complete characterization of adversaries tolerable in secure multi-party computation (extended abstract). In: Burns, J.E., Attiya, H. (eds.) PODC, pp. 25–34. ACM (1997)
13. Ishai, Y., Ostrovsky, R., Seyalioglu, H.: Identifying cheaters without an honest majority. In: Cramer, R. (ed.) TCC 2012. LNCS, vol. 7194, pp. 21–38. Springer, Heidelberg (2012)
14. Jhanwar, M.P., Safavi-Naini, R.: Unconditionally-secure robust secret sharing with minimum share size. In: Sadeghi, A.-R. (ed.) FC 2013. LNCS, vol. 7859, pp. 96–110. Springer, Heidelberg (2013)
15. Karnin, E.D., Greene, J.W., Hellman, M.E.: On secret sharing systems. IEEE Transactions on Information Theory 29(1), 35–41 (1983)
16. Kurosawa, K.: General error decodable secret sharing scheme and its application. IACR Cryptology ePrint Archive, Report 2009/263 (2009), `http://eprint.iacr.org/`
17. Kurosawa, K., Obana, S., Ogata, W.: t-cheater identifiable (k, n) threshold secret sharing schemes. In: Coppersmith, D. (ed.) CRYPTO 1995. LNCS, vol. 963, pp. 410–423. Springer, Heidelberg (1995)
18. Lakshmanan, S., Ahamad, M., Venkateswaran, H.: Responsive security for stored data. IEEE Trans. Parallel Distrib. Syst. 14(9), 818–828 (2003)
19. 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)
20. McEliece, R.J., Sarwate, D.V.: On sharing secrets and Reed-Solomon codes. Commun. ACM 24(9), 583–584 (1981)
21. 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)
22. Ogata, W., Kurosawa, K., Stinson, D.R.: Optimum secret sharing scheme secure against cheating. SIAM J. Discrete Math. 20(1), 79–95 (2006)
23. Padro, C., Sáez, G., Villar, J.L.: Detection of cheaters in vector space secret sharing schemes. Des. Codes Cryptography 16(1), 75–85 (1999)
24. Pedersen, T.P.: Non-interactive and information-theoretic secure verifiable secret sharing. In: Feigenbaum, J. (ed.) CRYPTO 1991. LNCS, vol. 576, pp. 129–140. Springer, Heidelberg (1992)
25. 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)

26. Shamir, A.: How to share a secret. Communications of the ACM 22(11), 612–613 (1979)
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)