General Error Decodable Secret Sharing Scheme and Its Application

Kaoru Kurosawa

Department of Computer and Information Sciences,
Ibaraki University,
4-12-1 Nakanarusawa, Hitachi, Ibaraki 316-8511, Japan,
e-mail: kurosawa@mx.ibaraki.ac.jp

Abstract

Consider a model of secret sharing schemes with cheaters. We say that a secret sharing scheme is error decodable if we can still recover the secret s correctly from a noisy share vector $(\mathtt{share}'_1, \cdots, \mathtt{share}'_n)$. In this paper, we first prove that there exists an error decodable secret sharing scheme if and only if the adversary structure Γ satisfies a certain condition called Q^3. Next for any Γ which satisfies Q^3, we show an error decodable secret sharing scheme such that the decoding algorithm runs in polynomial-time in $|S|$ and the size of a linear secret sharing scheme (monotone span program) which realzes Γ. We finally show an applicaiton to 1-round Perfectly Secure Message Transmission schemes (PSMT).

Keywords: secret sharing, cheater, error decodable, PSMT

1 Introduction

Consider a model of secret sharing schemes with cheaters as follows. The members of some non-access set B are cheaters and they open forged shares in the reconstruction phase while all the other participants are honest and open valid shares. We say that a secret sharing scheme is error decodable if we can still recover the secret s correctly from the noisy share vector $(\mathtt{share}'_1, \cdots, \mathtt{share}'_n)$, where n is the number of participants. For example, Shamir's (k, n)-threshold secret sharing scheme is error decodable if and only if $n \geq 3(k-1)+1$ [7]. In this case, the decoding algorithm runs in polynomial time in n and $|S|$, where $|S|$ denotes the size of s.

On the other hand, threshold secret sharing schemes have been generalized to access strcutures, where an access strcuture Σ is defined by

$$\Sigma = \{A \mid A \subseteq \{1, \cdots, n\} \text{ is an access set}\}.$$

The complement of Σ is called the adversary structure and denoted by Γ. That is,

$$\Gamma = \{B \mid B \subset \{1, \cdots, n\} \text{ is a non-access set}\}.$$

Now does there exist an error decodable secret sharing scheme for general secret sharing schemes ? This fundamental problem has not been solved so far.

In this paper, we first prove that there exists an error decodable secret sharing scheme for Γ if and only if Γ satisfies a certain condition called Q^3.

Next for any Γ which satisfies Q^3, we show an error decodable secret sharing scheme such that the decoding algorithm runs in polynomial-time in $|S|$ and the size of a linear secret sharing scheme (monotone span program) which realizes Γ.

We finally show its applicaiton to 1-round Perfectly Secure Message Transmission schemes (PSMT) [2, 3].

Related works: The notions of adversary structures Γ and Q^3 were introduced by Hirt and Maurer in the context of multi-party protocols [4]. Γ satisfies Q^3 if $(B_h \cup B_i \cup B_j) \neq \{1, \cdots, n\}$ for any $B_h, B_i, B_j \in \Gamma$. For example, the Γ of a (k, n)-threshold secret sharing scheme satisfies Q^3 if and only if $n \geq 3(k-1)+1$.

2 Preliminaries

2.1 Secret Sharing Scheme

In a secret sharing scheme, the dealer distributes a secret s to n participants $\mathcal{P} = \{P_1, \cdots, P_n\}$ in such a way that some subsets of the participants can reconstruct s while the other subsets of the participants have no information on s. A subset of the participants who can reconstruct s is called an access set.

More formally, let F be a finite field. A dealer is a probabilistic polynomial time algorithm Dealer such that on input a secret $s \in \mathsf{F}$ and a random string r

$$\mathsf{Dealer}(s, r) = (\mathtt{share}_1, \cdots, \mathtt{share}_n),$$

where $\mathtt{share}_i$ is given to a participant P_i. For a subset $A \subseteq \{1, \cdots, n\}$, let

$$\mathsf{share}_A = \{\mathsf{share}_i \mid i \in A\}.$$

Let S denote a random variable induced by s, and SHARE_A denote a random variable induced by $\mathtt{share}_A$. We require that

$$H(S \mid \mathrm{SHARE}_A) = 0 \text{ or } H(S), \tag{1}$$

where H denotes entropy. A is called an access set if $H(S \mid \mathrm{SHARE}_A) = 0$, and a non-access set if $H(S \mid \mathrm{SHARE}_A) = H(S)$. The family of access sets is called an access structure Σ.

Let $\mathsf{Reconstruct}$ be a reconstruction algorithm such that

$$\mathsf{Reconstruct}(A, \mathtt{share}_A) = \begin{cases} s & if \quad A \in \Sigma \\ \perp & if \quad A \notin \Sigma \end{cases}$$

Definition 2.1 *We say that* $(\Sigma, \mathsf{Dealer}, \mathsf{Reconstruct})$ *is a secret sharing scheme. In particular, it is called perfect if eq.(1) holds.*

There exists a perfect secret sharing scheme for an access structure Σ if and only if Σ is monotone [5].

Definition 2.2 Σ *is monotone if* $A \in \Sigma$ *and* $A' \supseteq A$*, then* $A' \in \Sigma$.

In what follows, a secret sharing scheme means a perfect secret sharing scheme.

2.2 Linear Secret Sharing Scheme (LSSS)

A secret sharing scheme for any monotone access structure Σ can be realized by a linear secret sharing scheme (LSSS). Let

$$M = \begin{pmatrix} m_1 \\ \vdots \\ m_\ell \end{pmatrix}$$

be an $\ell \times d$ matrix over a finite field F and $\psi : \{1, \cdots, \ell\} \to \{1, \cdots, n\}$ be a labeling function, where $\ell \geq d$ and $\ell \geq n$.

Distribution algorithm:

1. To share a secret $s \in \mathsf{F}$, the dealer first chooses a random vector $\mathbf{r} \in \mathsf{F}^{d-1}$ and compute a vector
$$\mathtt{v} = M \times \begin{pmatrix} s \\ \mathbf{r} \end{pmatrix}, \tag{2}$$
where $\mathtt{v} = (v_1, \cdots, v_\ell)^T$.

2. Let $\mathsf{LSSS}(s, \mathtt{r}) = (\mathtt{share}_1, \cdots, \mathtt{share}_n)$, where
$$\mathtt{share}_i = \{v_j \mid \psi(j) = i\} \tag{3}$$
The dealer gives $\mathtt{share}_i$ to P_i as a share for $i = 1, \cdots, n$.

Reconstruction algorithm: A subset of participants A can reconstruct the secret s if and only if $(1, 0, \cdots, 0)$ is in the linear span of

$$M_A = \{m_j \mid \psi(j) \in A\}.$$

Definition 2.3 *We say that the above* (M, ψ) *is a monotone span program which realizes* Σ.

3 Error Decodable Condition

Let $(\Sigma, \mathsf{Dealer}, \mathsf{Reconstruct})$ be a secret sharing scheme. The adversary structure is defined as the family of non-access sets

$$\Gamma = \{B \mid B \notin \Sigma\}.$$

Suppose that the members of some non-access set $B \in \Gamma$ are cheaters, and they open forged shares in the reconstruction phase. In this case, a noisy share vector is revealed such that

$$\mathbf{y} = \mathsf{Dealer}(s, r) + \mathsf{e}$$

where $\mathsf{e} = (e_1, \cdots, e_n)$ is an error vector. [1] Under what condition can we recover s correctly from $\mathbf{y}$? In this section, we show an answer to this problem.

Let

$$\mathit{support}(\mathsf{e}) = \{i \mid e_i \neq 0\}.$$

Then $\mathit{support}(\mathsf{e}) \in \Gamma$ because the cheaters belong to a non-access set $B \in \Gamma$.

Definition 3.1 *Γ satisfies Q^3 if $(B_h \cup B_i \cup B_j) \neq \{1, \cdots, n\}$ for any $B_h, B_i, B_j \in \Gamma$.*

For example, the adversary structure Γ of a (k, n)-threshold secret sharing scheme satisfies Q^3 iff $n \geq 3(k-1)+1$, where

$$\Gamma = \{B \mid |B| \leq k-1\}.$$

Lemma 3.1 *Γ satisfies Q^3 if and only if*

$$\mathit{support}(\mathsf{Dealer}(s, r) - \mathsf{Dealer}(s', r')) \not\subseteq (B_i \cup B_j) \tag{4}$$

for any s, s', r, r' such that $s \neq s'$ and for any $B_i, B_j \in \Gamma$.

(Proof) (1) Suppose that Γ does not satisfy Q^3. Then there exist $B_h, B_i, B_j \in \Gamma$ such that

$$\{1, \cdots, n\} = B_h \cup B_i \cup B_j.$$

Since B_h is a non-access set, the members of B_h have no information on the secret s. Therefore, there exist some s, s', r, r' such that $s \neq s'$ and

$$\mathtt{share}_i = \mathtt{share}'_i$$

for all $i \in B_h$, where

$$\begin{aligned} \mathsf{Dealer}(s, r) &= (\mathtt{share}_1, \cdots, \mathtt{share}_n), \\ \mathsf{Dealer}(s', r') &= (\mathtt{share}'_1, \cdots, \mathtt{share}'_n) \end{aligned}$$

[1] It is assumed that $\mathtt{share}_i$ and e_i are elements of some Abelian group for each i. For exapmple, the operation is bit-wise XOR.

This means that

$$\mathit{support}(\mathsf{Dealer}(s,r) - \mathsf{Dealer}(s',r')) \subseteq \{1,\cdots,n\} \setminus B_h = (B_i \cup B_j)$$

because $\{1,\cdots,n\} = B_h \cup B_i \cup B_j$.

(2) Suppose that

$$\mathit{support}(\mathsf{Dealer}(s,r) - \mathsf{Dealer}(s',r')) \subseteq (B_i \cup B_j)$$

for some s, s', r, r' such that $s \neq s'$ and some $B_i, B_j \in \Gamma$. Let

$$X = \mathit{support}(\mathsf{Dealer}(s,r) - \mathsf{Dealer}(s',r')).$$

We show that $B_h = X^c$ is a non-access set, where ^{c} denotes the complement. Note that for all $i \in B_h$, it holds that

$$\mathtt{share}_i = \mathtt{share}'_i,$$

where

$$\begin{aligned} \mathsf{Dealer}(s,r) &= (\mathtt{share}_1, \cdots, \mathtt{share}_n), \\ \mathsf{Dealer}(s',r') &= (\mathtt{share}'_1, \cdots, \mathtt{share}'_n) \end{aligned}$$

This means that B_h is not an access set because B_h cannot determine s or s'. Hence B_h is a non-access set. Hence

$$\{1,\cdots,n\} = X^c \cup X = B_h \cup X \subseteq B_h \cup B_i \cup B_j.$$

This means that Γ does not satisfy Q^3.

Q.E.D.

Lemma 3.2 *There exists an algorithm which can recoever s correctly from* $\mathtt{y}$ *for any error vector* e *such that* $\mathit{support}(\mathsf{e}) \in \Gamma$ *if and only if* Γ *satisfies* Q^3.

(Proof) We cannot compute s correctly if and only if

$$\mathbf{y} = \mathsf{Dealer}(s,r) + \mathsf{e} = \mathsf{Dealer}(s',r') + \mathsf{e}'$$

for some e, e' such that

$$\mathit{support}(\mathsf{e}) \in \Gamma \text{ and } \mathit{support}(\mathsf{e})' \in \Gamma$$

for some s, s', r, r' such that $s \neq s'$. In this case, we have

$$\mathsf{Dealer}(s,r) - \mathsf{Dealer}(s',r') = \mathsf{e}' - \mathsf{e}.$$

This holds if and only if

$$\mathit{support}(\mathsf{Dealer}(s,r) - \mathsf{Dealer}(s',r')) \subseteq \mathit{support}(\mathsf{e}') \cup \mathit{support}(\mathsf{e}). \tag{5}$$

To summarize, we cannot compute s correctly if and only if eq.(5) holds. Now Lemma 3.1 implies that we can compute s correctly if and only if Γ satisfies Q^3.

Q.E.D.

Let Decode be an algorithm such that

$$\mathsf{Decode}(\mathsf{Dealer}(s,r)+\mathsf{e}) = \begin{cases} s & if \quad support(\mathsf{e}) \in \Gamma \\ \perp & if \quad support(\mathsf{e}) \notin \Gamma \end{cases}$$

Definition 3.2 *We say that* $(\Sigma, \mathsf{Dealer}, \mathsf{Reconstruct}, \mathsf{Decode})$ *is an error decodable secret sharing scheme.*

Theorem 3.1 *There exists an error decodable secret sharing scheme* $(\Sigma, \mathsf{Dealer}, \mathsf{Reconstruct}, \mathsf{Decode})$ *if and only if* $\Gamma = \Sigma^c$ *satisfies* Q^3.

(Proof) From Lemma 3.2.

Q.E.D.

4 Polynomial-Time Error Decodable Scheme

The Decode implicitely shown in the proof of Lemma 3.2 recovers s by exhaustive search in general. Hence it runs in exponential time.

In this section, for any Γ which satisfies Q^3, we show an error decodable secret sharing scheme such that the decoding algorithm runs in polynomial time in $|S|$ and the size of a monotone span program (M, ψ) for Γ, where $|S|$ denotes the bit length of the secrets.

We fix (M, ψ) such that M is an $\ell \times d$ matrix. We then say that an algorithm runs in polynomial time if it runs in polynomial time in $|S|$ and ℓ.

4.1 Weak Secret Sharing Scheme

We first show a weak error decodable secret sharing scheme

$$\Pi_i = (\Sigma, \mathsf{Dealer}_i, \mathsf{Reconstruct}_i, \mathsf{Decode}_i)$$

for each $1 \leq i \leq n$. It has the following properties.

- Decode_i always outputs the correct secret s or $\perp$. (It never outputs a wrong s'.) Further it outputs s if P_i is honest.
- The members of a non-access set B learns no information on s if $i \notin B$.
- Each algorithm runs in polynomial time.

Distribution algorithm: (See Fig.1.)

1. For a secret $s \in \mathsf{F}$, the dealer chooses random $\mathbf{r} \in \mathsf{F}^{d-1}$, and computes
$$\mathsf{LSSS}(s, \mathtt{r}) = (\mathtt{share}_1, \cdots, \mathtt{share}_n)$$
according to eq.(3).
2. The dealer gives $(s, \mathtt{r})$ and $\mathtt{share}_i$ to P_i as his share.
3. For each $j \neq i$, the dealer gives $\mathtt{share}_j$ to P_j as his share.

Reconstruciton algorithm: The members of an access set A can reconstruct s by applying the reconstruction algorithm of the LSSS to their shares.

Error-decoding algorithm: Suppose that P_i revealed $(s', \mathtt{r}')$ and y_i, and each $P_j \neq P_i$ revealed y_j. Let $\mathtt{y} = (y_1, \cdots, y_n)$.

(d1) If *support*$(\mathtt{y} - \mathsf{LSSS}(s, \mathtt{r})) \in \Gamma$, then output $x = s'$.

(d2) Otherwise output $x = \perp$.

Lemma 4.1 *Suppose that* Γ *satisfies* Q^3.

- Decode_i *always outputs the correct secret* s *or* $\perp$. *(It never outputs a wrong* s'.*) Further it outputs* s *if* P_i *is honest.*
- *The members of a non-access set* B *learns no information on* s *if* $i \notin B$.
- *Each algorithm runs in polynomial time.*

(Proof) It is easy to see 2 and 3. We will prove 1. First it is easy to see that
$$\mathbf{y} = \mathsf{LSSS}(s, \mathtt{r}) + \mathtt{e}_1$$
for some error vector $\mathtt{e}_1$ such that *support*$(\mathtt{e}_1) \in \Gamma$. Next define $\mathtt{e}_2 = \mathtt{y} - \mathsf{LSSS}(s', \mathtt{r}')$. Then
$$\mathtt{y} = \mathsf{LSSS}(s', \mathtt{r}') + \mathtt{e}_2.$$

First suppose that P_i is honest. Then it is clear that $\mathsf{LSSS}(s', \mathtt{r}') = \mathsf{LSSS}(s, \mathtt{r})$. This means that $\mathtt{e}_2 = \mathtt{e}_1$. Hence we obtain that
$$\mathit{support}(\mathtt{e}_2) = \mathit{support}(\mathtt{e}_1) \in \Gamma.$$
In this case, Decode_i outputs $x = s' = s$ according to (d1). Next suppose that P_i is a cheater and $(s, \mathtt{r}') \neq (s, \mathtt{r})$.

- If $s' = s$, then $x = s$ or $\perp$ according to (d1) and (d2).
- If $s' \neq s$, then we obtain that
$$\mathbf{y} = \mathsf{LSSS}(s, \mathtt{r}) + \mathtt{e}_1 = \mathsf{LSSS}(s', \mathtt{r}') + \mathtt{e}_2.$$
Hence
$$\mathsf{LSSS}(s, \mathtt{r}) - \mathsf{LSSS}(s', \mathtt{r}') = \mathtt{e}_2 - \mathtt{e}_1.$$
This means that Γ does not satisfy Q^3 from Lemma 3.1.

Q.E.D.

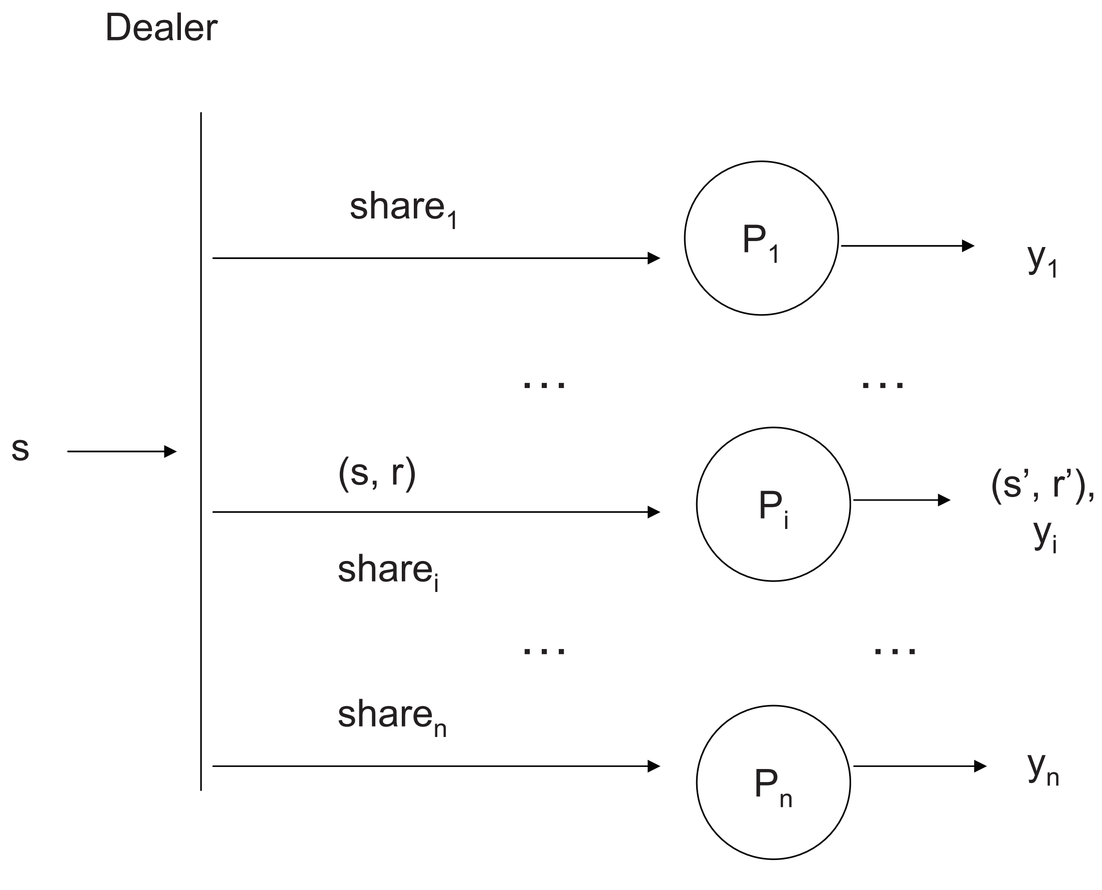

Figure 1: Weak secret sharing scheme $\Pi_i(s)$

4.2 Full Scheme

We now show a polynomial-time error decodable secret sharing scheme for any Γ which satisfies Q^3. Let (M, ψ) be a monotone span program which realizes Γ. For simplicity, assume that $\ell = n$ and $\psi(i) = i$ for $i = 1, \cdots, n$.

Distribution algorithm: (See Fig.1.)

1. For a secret $s \in \mathsf{F}$, the dealer chooses random $\mathbf{r} \in \mathsf{F}^{d-1}$, and computes $\mathtt{v} = (v_1, \cdots, v_n)$ according to eq.(2).
2. For $i = 1, \cdots, n$, the dealer runs the distribution algorithm of our weak error decodable secret sharing scheme Π_i by letting v_i be a secret.

Reconstruciton algorithm: The members of an access set A can reconstruct s as follows. Suppose that $A = \{i_1, \cdots, i_h\}$.

- For $j = 1, \cdots, h$, run the reconstruction algorithm of Π_{i_j} and recover v_{i_j}.
- Recover s by applying the reconstruction algorithm of the LSSS to these v_{i_j}.

Error-decoding algorithm:

- For $i = 1, \cdots, n$, run the error-decoding algorithm of Π_i and recover x_i. From Lemma 4.1, we have $x_i = v_i$ or $\perp$. Further $x_i = v_i$ if P_i is honest.
- Recover s by applying the reconstruction algorithm of the LSSS to x_i such that $x_i \neq \perp$.

From Lemma 4.1, we obtain the following theorem.

Theorem 4.1 *The above scheme is an error decodable secret sharing scheme for any Γ which satisfies Q^3. Further each algorithm runs in polynomial time in $|S|$ and ℓ.*

The size of shares $\widetilde{\mathtt{share}}_i$ of each P_i is given by

$$|\widetilde{\mathtt{share}}_i| = (d + \ell \cdot |\mathtt{share}_i|)|S|, \tag{6}$$

where $\mathtt{share}_i$ is the share of the underlying LSSS.

5 Application to 1-Round PSMT

5.1 PSMT

The model of Perfectly Secure Message Transmission schemes (PSMT) was introduced by Dolev et al. [2]. In this model, there are n channels between a sender and a receiver, and they share no key. The sender wishes to send a secret s to the receiver securely and reliably. An adversary $\mathbf{A}$ can observe and forge the messages sent through some subset of n channels.

Let the adversary structure Γ be the family of subsets of n channels that the adversary $\mathbf{A}$ can corrupt. A PSMT is a scheme which satisfies perfect privacy and perfect reliablity even in the presence of infinitely powerful adversary $\mathbf{A}$ who can corrupt any subset of Γ. Perfect privact means that $\mathbf{A}$ learns no information on s. Perfect reliability means that the receiver can output $\hat{s} = s$ correctly.

5.2 Previous 1-Round PSMT for Adversary Structure

Desmedt, Wang and Burmester [3] showed that there exists a 1-round PSMT if and only if the adversary structure Γ satisfies Q^3. Their 1-round PSMT is described as follows. Let

$$\Gamma^+ = \{B_1, \cdots, B_T\}$$

be the family of maximal non-access sets.

1. For a secret $s \in \mathsf{F}$, the sender chooses random $r_1, \cdots, r_T \in \mathsf{F}$ such that

$$s = r_1 + \cdots r_T.$$

2. For $i = 1, \cdots, T$, the sender sends r_i through all channels belonging to $\{1, \cdots, n\} \setminus B_i$.

The total communication cost is given by

$$\sum_{i=1}^{T} (n - |B_i|) \cdot |S|. \tag{7}$$

5.3 Proposed 1-Round PSMT for Adversary Structure

We show a more efficient 1-round PSMT by using our error decodable secret sharing scheme $(\Sigma, \mathsf{Dealer}, \mathsf{Reconstruct}, \mathsf{Decode})$ shown in 4.2.

1. For a secret $s \in \mathsf{F}$, the sender computes

$$\mathsf{Dealer}(s, r) = (\widetilde{\mathtt{share}}_1, \cdots, \widetilde{\mathtt{share}}_n),$$

and sends $\widetilde{\mathtt{share}}_i$ through channel i for $i = 1, \cdots, n$.

2. Suppose that the receiver received $\widetilde{\mathtt{share}}_i'$ through channel i for $i = 1, \cdots, n$. He reconstructs s by applying Decode to $(\widetilde{\mathtt{share}}_1', \cdots, \widetilde{\mathtt{share}}_n')$.

From Theorem 4.1, we obtain the following theorem.

Theorem 5.1 *The above scheme is a* 1*-Round PSMT for any* Γ *which satisfies* Q^3*. Further the sender and the receiver runs in polynomail time in* $|S|$ *and* ℓ*.*

5.4 Comparison

In our scheme, the total communication cost is

$$\begin{aligned}\mathsf{Comm}_{our} &= \sum_{i=1}^{n} |\widetilde{\mathtt{share}}_i| = \sum_{i=1}^{n} (d + \ell \cdot |\mathtt{share}_i|)|S| \\ &= (nd + \ell^2)|S|\end{aligned}$$

from eq.(6), where an $\ell \times d$ matrix M is used in the LSSS. In the scheme of Desmedt et al. [3], the total communication cost is

$$\mathsf{Comm}_{dbw} = \sum_{i=1}^{T} (n - |B_i|)|S|$$

from eq.(7), where T is the number of maximal non-access sets B_i.

We can see that Comm_{our} is much smaller than Comm_{dbw} in general because the latter depends on T. For example, suppose that $n = 3t + 1$, and consider a threshold adversary who corrupts at most t channels. [2] Then $T = \binom{n}{t}$. Hence

$$\mathsf{Comm}_{dbw} = \binom{n}{t}(n - t)|S|,$$

Thus the communication cost of Desmedt et al. scheme is exponential in t. On the other hand, there exists a monotone span program (M, ψ) such that M is an $n \times (t + 1)$ matrix for the threshold adversary. Hence

$$\mathsf{Comm}_{our} = (n(t + 1) + n^2)|S| = n(n + t + 1)|S|$$

Thus our communication cost is $\mathcal{O}(n^2) = \mathcal{O}(t^2)$. (See Table 1.)

[2] For this model, Dolev et al. [2] showed a scheme such that the total communication cost is $n|S|$.

Table 1: Total Communication cost

	General Adversary	Threshold Adversary
Desmedt et al. [3]	$\sum_{i=1}^{T}(n - \|B_i\|)\|S\|$	$exp(t)$
Proposed	$(nd + \ell^2)\|S\|$	$\mathcal{O}(t^2)$

6 Discussion

It is the best that there exists a polynomial-time decoding algorithm for the underlying LSSS. In this case, we do not have to use our scheme of Sec.4.2. For example, Shamir's (k, n)-threshold secret sharing scheme (which is an LSSS) has a polynomial-time decoding algorithm. On the other hand, it is known that the decoding problem of general linear codes is NP-hard [1].

It will be a future work to prove or disprove that the decoding problem of LSSS for any Γ satisfying Q^3 is NP-hard.

References

[1] E. R. Berlekamp, R. J. McEliece and H. C. A. van Tilborg," On the inherent intractability of certain coding problems," IEEE Trans. Inf. Theory, vol. IT-24, no. 3, pp. 384?386, May 1978.

[2] D.Dolev, C.Dwork, O.Waarts, M.Yung: Perfectly Secure Message Transmission. J. ACM 40(1): pp.17–47 (1993)

[3] Y.Desmedt, Y.Wang and M.Burmester: A Complete Characterization of Tolerable Adversary Structures for Secure Point-to-Point Transmissions Without Feedback. ISAAC 2005: 277-287

[4] M. Hirt and U.Maurer: Player Simulation and General Adversary Structures in Perfect Multiparty Computation. J. Cryptology 13(1): 31-60 (2000)

[5] M. Ito, A. Saio, Takao Nishizeki: Multiple Assignment Scheme for Sharing Secret. J. Cryptology 6(1): 15-20 (1993)

[6] M.V.N.A.Kumar, P.R.Goundan, K.Srinathan, C.P.Rangan: On perfectly secure cmmunication over arbitrary networks. PODC 2002: 193-202

[7] R.McEliece and D.Sarwate: On Sharing Secrets and Reed-Solomon Codes. Commun. ACM 24(9): 583-584 (1981)