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 $(\text{share}_1', \cdots, \text{share}_n')$. In this paper, we first prove that there exists an error decodable secret sharing scheme if and only if the adversary structure $\Gamma$ satisfies a certain condition called $Q^3$. Next for any $\Gamma$ 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 $\Gamma$. We finally show an application 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 $(\text{share}_1', \cdots, \text{share}_n')$, 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 structures, where an access structure $\Sigma$ is defined by

$$\Sigma = \{ A \mid A \subseteq \{1, \cdots, n\} \text{ is an access set} \}.$$
The complement of $\Sigma$ is called the adversary structure and denoted by $\Gamma$. That is,

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

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 $\Gamma$ if and only if $\Gamma$ satisfies a certain condition called $Q^3$.

Next for any $\Gamma$ 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 $\Gamma$.

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

Related works: The notions of adversary structures $\Gamma$ and $Q^3$ were introduced by Hirt and Maurer in the context of multi-party protocols [4]. $\Gamma$ satisfies $Q^3$ if $(B_k \cup B_l \cup B_j) \neq \{1, \ldots, n\}$ for any $B_k, B_l, B_j \in \Gamma$. For example, the $\Gamma$ 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 $\mathcal{P} = \{P_1, \ldots, P_n\}$ 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 $s \in F$ and a random string $r$

$$\text{Dealer}(s, r) = (\text{share}_1, \ldots, \text{share}_n),$$

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

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

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

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

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

2
Let Reconstruct be a reconstruction algorithm such that

\[
\text{Reconstruct}(A, \text{share}_A) = \begin{cases} 
  s & \text{if } A \in \Sigma \\
  \bot & \text{if } A \not\in \Sigma
\end{cases}
\]

**Definition 2.1** We say that \((\Sigma, \text{Dealer}, \text{Reconstruct})\) 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 \(\Sigma\) if and only if \(\Sigma\) is monotone [5].

**Definition 2.2** \(\Sigma\) 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 \(\Sigma\) 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 \(s \in F\), the dealer first chooses a random vector \(r \in F^{d-1}\) and compute a vector

\[
v = M \times \begin{pmatrix} s \\ r \end{pmatrix},
\]

where \(v = (v_1, \cdots, v_\ell)^T\).

2. Let \(\text{LSSS}(s, r) = (\text{share}_1, \cdots, \text{share}_n)\), where

\[
\text{share}_i = \{v_j \mid \psi(j) = i\} \tag{3}
\]

The dealer gives \(\text{share}_i\) 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 \((M, \psi)\) is a monotone span program which realizes \(\Sigma\).
3 Error Decodable Condition

Let $(\Sigma, \text{Dealer}, \text{Reconstruct})$ 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

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

where $e = (e_1, \ldots, e_n)$ is an error vector.  \footnote{It is assumed that $\text{share}_i$ and $e_i$ are elements of some Abelian group for each $i$. For example, the operation is bit-wise XOR.} Under what condition can we recover $s$ correctly from $y$? In this section, we show an answer to this problem.

Let

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

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

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

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

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

**Lemma 3.1** $\Gamma$ satisfies $Q^3$ if and only if

$$\text{support}(\text{Dealer}(s, r) - \text{Dealer}(s', r')) \nsubseteq (B_i \cup B_j)$$

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

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

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

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

for all $i \in B_h$, where

$$\text{Dealer}(s, r) = (\text{share}_1, \ldots, \text{share}_n),$$

$$\text{Dealer}(s', r') = (\text{share'}_1, \ldots, \text{share'}_n)$$
This means that
\[ \text{support}(\text{Dealer}(s, r) - \text{Dealer}(s', r')) \subseteq \{1, \cdots, n\} \setminus B_h = (B_i \cup B_j) \]
because \( \{1, \cdots, n\} = B_h \cup B_i \cup B_j \).

(2) Suppose that
\[ \text{support}(\text{Dealer}(s, r) - \text{Dealer}(s', r')) \subseteq (B_i \cup B_j) \]
for some \( s, s', r, r' \) such that \( s \neq s' \) and some \( B_i, B_j \in \Gamma \). Let
\[ X = \text{support}(\text{Dealer}(s, r) - \text{Dealer}(s', r')). \]
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
\[ \text{share}_i = \text{share}'_i, \]
where
\[ \text{Dealer}(s, r) = (\text{share}_1, \cdots, \text{share}_n), \]
\[ \text{Dealer}(s', r') = (\text{share}'_1, \cdots, \text{share}'_n) \]
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 \( \Gamma \) does not satisfy \( Q^3 \). Q.E.D.

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

(Proof) We cannot compute \( s \) correctly if and only if
\[ y = \text{Dealer}(s, r) + e = \text{Dealer}(s', r') + e' \]
for some \( e, e' \) such that
\[ \text{support}(e) \in \Gamma \quad \text{and} \quad \text{support}(e') \in \Gamma \]
for some \( s, s', r, r' \) such that \( s \neq s' \). In this case, we have
\[ \text{Dealer}(s, r) - \text{Dealer}(s', r') = e' - e. \]
This holds if and only if
\[ \text{support}(\text{Dealer}(s, r) - \text{Dealer}(s', r')) \subseteq \text{support}(e') \cup \text{support}(e). \] (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 $\Gamma$ satisfies $Q^3$. Q.E.D.

Let $\text{Decode}$ be an algorithm such that

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

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

**Theorem 3.1** There exists an error decodable secret sharing scheme $(\Sigma, \text{Dealer}, \text{Reconstruct}, \text{Decode})$ 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 $\text{Decode}$ implicitly 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 $\Gamma$ 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 $(M, \psi)$ for $\Gamma$, where $|S|$ denotes the bit length of the secrets.

We fix $(M, \psi)$ 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 $\ell$.

### 4.1 Weak Secret Sharing Scheme

We first show a weak error decodable secret sharing scheme

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

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

- $\text{Decode}_i$ always outputs the correct secret $s$ or $\bot$. (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 $s \in \mathbb{F}$, the dealer chooses random $r \in \mathbb{F}^{d-1}$, and computes

$$LSSS(s, r) = (\text{share}_1, \cdots, \text{share}_n)$$

according to eq.(3).

2. The dealer gives $(s, r)$ and share$_i$ to $P_i$ as his share.

3. For each $j \neq i$, the dealer gives share$_j$ to $P_j$ as his share.

**Reconstruction 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 $(s', r')$ and $y_i$, and each $P_j \neq P_i$ revealed $y_j$. Let $y = (y_1, \cdots, y_n)$.

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

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

**Lemma 4.1** Suppose that $\Gamma$ 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

$$y = LSSS(s, r) + e_1$$

for some error vector $e_1$ such that support$(e_1) \in \Gamma$. Next define $e_2 = y - LSSS(s', r')$. Then

$$y = LSSS(s', r') + e_2.$$

First suppose that $P_i$ is honest. Then it is clear that $LSSS(s', r') = LSSS(s, r)$. This means that $e_2 = e_1$. Hence we obtain that

$$\text{support}(e_2) = \text{support}(e_1) \in \Gamma.$$ 

In this case, Decode$_i$ outputs $x = s' = s$ according to (d1). Next suppose that $P_i$ is a cheater and $(s, r') \neq (s, r)$.

- If $s' = s$, then $x = s$ or $\perp$ according to (d1) and (d2).

- If $s' \neq s$, then we obtain that

$$y = LSSS(s, r) + e_1 = LSSS(s', r') + e_2.$$ 

Hence

$$LSSS(s, r) - LSSS(s', r') = e_2 - e_1.$$ 

This means that $\Gamma$ 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 \( \Gamma \) which satisfies \( Q^3 \). Let \((M, \psi)\) be a monotone span program which realizes \( \Gamma \). For simplicity, assume that \( \ell = n \) and \( \psi(i) = i \) for \( i = 1, \ldots, n \).

**Distribution algorithm:** (See Fig.1.)

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

**Reconstruction algorithm:** The members of an access set \( A \) can reconstruct \( s \) as follows. Suppose that \( A = \{i_1, \ldots, i_h\} \).

- For \( j = 1, \ldots, h \), run the reconstruction algorithm of \( \Pi_{i_j} \) and recover \( v_{i_j} \).
- Recover \( s \) by applying the reconstruction algorithm of the LSSS to these \( v_{i_j} \).

**Error-decoding algorithm:**

- For \( i = 1, \ldots, n \), run the error-decoding algorithm of \( \Pi_i \) 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 \( \Gamma \) which satisfies \( Q^3 \). Further each algorithm runs in polynomial time in \( |S| \) and \( \ell \).

The size of shares \( \widetilde{\text{share}}_i \) of each \( P_i \) is given by

\[
|\widetilde{\text{share}}_i| = (d + \ell \cdot |\text{share}_i|)|S|, \tag{6}
\]

where \( \text{share}_i \) 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 \( A \) can observe and forge the messages sent through some subset of \( n \) channels.

Let the adversary structure \( \Gamma \) be the family of subsets of \( n \) channels that the adversary \( A \) can corrupt. A PSMT is a scheme which satisfies perfect privacy and perfect reliability even in the presence of infinitely powerful adversary \( A \) who can corrupt any subset of \( \Gamma \). Perfect privat means that \( A \) 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 \( \Gamma \) 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 \( s \in F \), the sender chooses random \( r_1, \cdots, r_T \in F \) 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

\[
\sum_{i=1}^{T} (n - |B_i|) \cdot |S|.
\]

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 \((\Sigma, \text{Dealer}, \text{Reconstruct}, \text{Decode})\) shown in 4.2.

1. For a secret \( s \in F \), the sender computes
\[
\text{Dealer}(s,r) = (\text{share}_1, \cdots, \text{share}_n).
\]

and sends \( \text{share}_i \) through channel \( i \) for \( i = 1, \cdots, n \).
2. Suppose that the receiver received \( \tilde{\text{share}}_i \) through channel \( i \) for \( i = 1, \ldots, n \). He reconstructs \( s \) by applying \( \text{Decode} \) to \( (\tilde{\text{share}}_1, \ldots, \tilde{\text{share}}_n) \).

From Theorem 4.1, we obtain the following theorem.

**Theorem 5.1** The above scheme is a 1-Round PSMT for any \( \Gamma \) which satisfies \( Q^0 \). Further the sender and the receiver runs in polynomial time in \( |S| \) and \( \ell \).

### 5.4 Comparison

In our scheme, the total communication cost is

\[
\text{Comm}_{\text{our}} = \sum_{i=1}^{n} |\tilde{\text{share}}_i| = \sum_{i=1}^{n} (d + \ell \cdot |\text{share}_i|)|S| = (nd + \ell^2)|S|
\]

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

\[
\text{Comm}_{\text{dsw}} = \sum_{i=1}^{T} (n - |B_i|)|S|
\]

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

We can see that \( \text{Comm}_{\text{our}} \) is much smaller than \( \text{Comm}_{\text{dsw}} \) 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

\[
\text{Comm}_{\text{dsw}} = \binom{n}{t} (n - t)|S|,
\]

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

\[
\text{Comm}_{\text{our}} = (n(t + 1) + n^2)|S| = n(n + t + 1)|S|.
\]

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

\(^2\) For this model, Dolev et al. [2] showed a scheme such that the total communication cost is \( n|S| \).
<table>
<thead>
<tr>
<th></th>
<th>General Adversary</th>
<th>Threshold Adversary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desmedt et al. [3]</td>
<td>$\sum_{i=1}^{n} (n -</td>
<td>B_i</td>
</tr>
<tr>
<td>Proposed</td>
<td>$(nd + \ell^2) S$</td>
<td>$\mathcal{O}(t^2)$</td>
</tr>
</tbody>
</table>

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 $\Gamma$ satisfying $Q^2$ is NP-hard.

References


