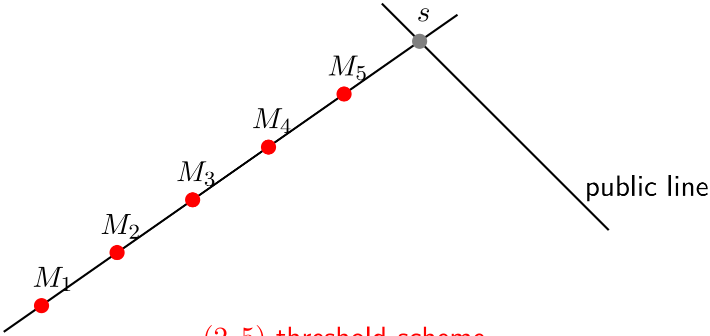
Error Decodable Secret Sharing and One-Round Perfectly Secure Message Transmission for General Adversary Structures

Keith M. Martin Maura B. Paterson Douglas R. Stinson

MITACS Network Security and Cryptography Workshop
23 June 2010

Secret Sharing Scheme

- A bank has 5 managers.
- No single manager is trusted to open the safe.
- Any pair of managers are allowed to open it together.



$(2, 5)$-threshold scheme

(k, n)-Threshold Scheme *(Blakley, Shamir 1979)*

linear scheme: (over GF(p))

$$M = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & 2 & 4 & \cdots & 2^{k-1} \\ \vdots & & & & \vdots \\ 1 & i & i^2 & \cdots & i^{k-1} \\ \vdots & & & & \vdots \end{pmatrix}$$

secret: s

randomisation:

$\mathbf{r} = (r_1 = s, r_2, \ldots, r_k)$

shares: $M_i \cdot \mathbf{r} = f(i)$

$f(x) =$

$r_1 + r_2 x + r_3 x^2 + \cdots + r_k x^{k-1}$

$$\sum_{j=1}^{k} \alpha_{i_j} M_{i_j} = (1, 0, \ldots, 0) \Rightarrow \sum_{j=1}^{k} \alpha_{i_j} (M_{i_j} \cdot \mathbf{r}) = (1, 0, \ldots, 0) \cdot \mathbf{r} = s$$

M has rank k (Vandermonde)

More General Schemes

Set of participants: $S = \{1, 2, \ldots, n\}$

Definition (monotone access structure)

Collection Σ of subsets of S such that $A' \in \Sigma$ whenever $A' \supseteq A$ and $A \in \Sigma$.

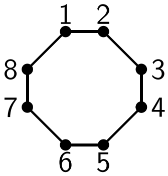
- $A \in \Sigma$ authorised set
- $B \in \Sigma^c := \mathcal{P}(S) \setminus \Sigma$ unauthorised set

Definition (linear secret sharing scheme realising Σ)

$n' \times d$ matrix M over $GF(p)$ where
$(1, 0, 0, \ldots, 0) \in$ span(rows $I_1, I_2, \ldots, I_j$) iff $\{i_1, i_2, \ldots, i_j\} \in \Sigma$.

Example

$n = 8, n' = 12$
$\Sigma : \{\{1,2\},\{2,3\},\{3,4\},\{4,5\},\{5,6\},\{7,8\},\{8,1\}\}$



$$M = \left(\begin{array}{ccccc}
0 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 \\
\hline
1 & 0 & 1 & 0 & 0 \\
\hline
0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 \\
\hline
1 & 0 & 0 & 1 & 0 \\
\hline
0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 1 \\
\hline
1 & 0 & 0 & 0 & 1 \\
\hline
0 & 0 & 0 & 0 & 1 \\
0 & 1 & 0 & 0 & 0 \\
\hline
1 & 1 & 0 & 0 & 0
\end{array}\right)$$

Ramp Schemes

Definition (*perfect* secret sharing scheme)

unauthorised sets are unable to determine any information about s

Example ((t, k, n)-ramp scheme)

Take a (k, n)-threshold scheme and define the secret to be $r_1, r_2, r_3, \ldots, r_{k-t}$ (*i.e.* the first $k - t$ coefficients of f).
Then:

- Any k users can recover the secret.
- Any set of at most t users learns no information about the secret.
- If $k > t + 1$, then the ramp scheme is not perfect.

Information Rate

Definition (information rate of a secret sharing scheme)

(size of the secret)/(size of the largest share)

- Every perfect scheme has information rate at most 1.
- An ideal secret sharing scheme has information rate 1.
- Shamir's secret sharing scheme is ideal.
- The previously described (t, k, n)-ramp scheme has (optimal) information rate $k - t$.

(k, n)-Threshold Schemes and Reed-Solomon Codes

$$\mathbf{r} \rightarrow f(x) = s + r_2 x + r_3 x^2 + \cdots + r_k x^{k-1}$$
$$\rightarrow \text{ shares } (f(1), f(2), \ldots, f(n))$$

The code

$$\mathcal{C} = \{(f(1), f(2), \ldots, f(n)) : f \in \mathrm{GF}(p)[x],\ \deg f < k\}$$

is an $[n, k, n-k+1]$ Reed-Solomon code.

Conclusion: Given the shares of all participants, the secret can be recovered even if $(n-k)/2$ of the shares are corrupted.

Error Correction for General Schemes?

Kaoru Kurosawa: *eprint.iacr.org/2009/263*

General Error Decodable Secret Sharing Scheme and Its Application

e.g. $n = 8$, access structure

$\Sigma: \ \{\{1,2\},\{2,3\},\{3,4\},\{4,5\}\{5,6\},\{6,7\},\{7,8\},\{8,1\}\}$

$(s_1, s_2, s_3, s_4, s_5, s_6, s_7, s_8)$ share vector

$\downarrow$

$(s_1, s_2, \skull, s_4, \skull, s_6, \skull, s_8)$ corrupt positions of $B \in \Sigma^c$

$\downarrow$

$(t_1, t_2, t_3, t_4, t_5, t_6, t_7, t_8)$ corrupted share vector

Given $(t_1, t_2, t_3, t_4, t_5, t_6, t_7, t_8)$ can you recover the secret?

General Adversary Structures

- Σ =access structure
- Γ =monotone adversary structure

Definition (monotone adversary structure)

Collection Γ of subsets of S such that $A' \in \Gamma$ whenever $A' \subseteq A$ and $A \in \Gamma$.

Examples:

- $\Gamma = \Sigma^c$ (e.g., as considered by Kurosawa)
- Γ is the collection of subsets of size at most t

Γ-Error Decodable Secret Sharing

Γ-error decodable secret sharing scheme realising an access structure Σ: if shares belonging to members of a set $W \in \Gamma$ are corrupted then the following decoding algorithm succeeds in recovering the correct secret.

Definition (decoding algorithm)

Input: A possibly corrupted share list $\mathbf{t} = (t_1, t_2, \ldots, t_n)$.

1. $\forall$ possible randomisation vectors $\mathbf{r}$ compute the share list $\mathbf{v} = (v_1, v_2, \ldots, v_n) \in \mathrm{GF}(p)^n$.
   If $\{j : v_j \neq t_j\} \in \Gamma$ then r_1 is a candidate secret.
2. If $\exists$ unique candidate secret s, return s.
3. If there are no candidate secrets, or if there is more than one candidate secret, return $\perp$.

A Necessary and Sufficient Condition for Γ-Error Decodability

Definition (condition $Q(\Gamma, \Gamma, \Sigma^c)$)

$\forall$ $W_1, W_2 \in \Gamma$, $B \in \Sigma^c$ we have $W_1 \cup W_2 \cup B \neq S$.

Theorem (Fehr-Maurer '02)

A secret sharing scheme is Γ-Error Decodable if and only if condition $Q(\Gamma, \Gamma, \Sigma^c)$ is satisfied.

Proof:

A Necessary and Sufficient Condition for Γ-Error Decodability

Definition (condition $Q(\Gamma, \Gamma, \Sigma^c)$)

$\forall$ $W_1, W_2 \in \Gamma$, $B \in \Sigma^c$ we have $W_1 \cup W_2 \cup B \neq S$.

Theorem (Fehr-Maurer '02)

A secret sharing scheme is Γ-Error Decodable if and only if condition $Q(\Gamma, \Gamma, \Sigma^c)$ is satisfied.

Proof: $(\Rightarrow)$:

$$\begin{array}{cccccl} & W_1 & W_2 & B & & \\ \mathbf{v}^2 & \boxed{X'} & \boxed{Y'} & \boxed{Z} & \rightarrow & s_2 \neq s_1 \end{array}$$

$$\mathbf{v}^1 \; \boxed{X} \; \boxed{Y} \; \boxed{Z} \rightarrow s_1$$

A Necessary and Sufficient Condition for Γ-Error Decodability

Definition (condition $Q(\Gamma, \Gamma, \Sigma^c)$)

$\forall\ W_1, W_2 \in \Gamma,\ B \in \Sigma^c$ we have $W_1 \cup W_2 \cup B \neq S$.

Theorem (Fehr-Maurer '02)

A secret sharing scheme is Γ-Error Decodable if and only if condition $Q(\Gamma, \Gamma, \Sigma^c)$ is satisfied.

Proof: $(\Rightarrow)$:

$$
\begin{array}{cc|c|c|c|l}
 & \multicolumn{1}{c}{} & \multicolumn{1}{c}{W_1} & \multicolumn{1}{c}{W_2} & \multicolumn{1}{c}{B} & \\
\cline{3-5}
\mathbf{v}^2 & & X' & Y' & Z & \rightarrow s_2 \neq s_1 \\
\cline{3-5}
 & \multicolumn{1}{c}{} & \multicolumn{1}{c}{} & \multicolumn{1}{c}{\downarrow} & \multicolumn{1}{c}{} & \\
\cline{3-5}
\mathbf{t} & & X & Y' & Z & \rightarrow \perp \\
\cline{3-5}
 & \multicolumn{1}{c}{} & \multicolumn{1}{c}{\uparrow} & \multicolumn{1}{c}{} & \multicolumn{1}{c}{} & \\
\cline{3-5}
\mathbf{v}^1 & & X & Y & Z & \rightarrow s_1 \\
\cline{3-5}
\end{array}
$$

A Necessary and Sufficient Condition for Γ-Error Decodability

Definition (condition $Q(\Gamma, \Gamma, \Sigma^c)$)

$\forall\ W_1, W_2 \in \Gamma$, $B \in \Sigma^c$ we have $W_1 \cup W_2 \cup B \neq S$.

Theorem (Fehr-Maurer '02)

A secret sharing scheme is Γ-Error Decodable if and only if condition $Q(\Gamma, \Gamma, \Sigma^c)$ is satisfied.

Proof: $(\Leftarrow)$:

$$W_1\, W_2\ \ B$$

$$\mathbf{t}\ \ \boxed{X \mid Y' \mid Z}\ \ \rightarrow \perp$$

A Necessary and Sufficient Condition for Γ-Error Decodability

Definition (condition $Q(\Gamma, \Gamma, \Sigma^c)$)

$\forall\ W_1, W_2 \in \Gamma,\ B \in \Sigma^c$ we have $W_1 \cup W_2 \cup B \neq S$.

Theorem (Fehr-Maurer '02)

A secret sharing scheme is Γ-Error Decodable if and only if condition $Q(\Gamma, \Gamma, \Sigma^c)$ is satisfied.

Proof: $(\Leftarrow)$:

$$\begin{array}{c|c|c|c|l}
\multicolumn{1}{c}{} & \multicolumn{1}{c}{W_1} & \multicolumn{1}{c}{W_2} & \multicolumn{1}{c}{B} & \\
\cline{2-4}
\mathbf{v}^2 & X' & Y' & Z & \to s_2 \neq s_1 \\
\cline{2-4}
\multicolumn{1}{c}{} & \multicolumn{1}{c}{} & \multicolumn{1}{c}{\uparrow} & \multicolumn{1}{c}{} & \\
\cline{2-4}
\mathbf{t} & X & Y' & Z & \to \perp \\
\cline{2-4}
\multicolumn{1}{c}{} & \multicolumn{1}{c}{\downarrow} & \multicolumn{1}{c}{} & \multicolumn{1}{c}{} & \\
\cline{2-4}
\mathbf{v}^1 & X & Y & Z & \to s_1 \\
\cline{2-4}
\end{array}$$

Efficiency of Error Decoding

- Generating the shares for any linear secret-sharing scheme is efficient.
- There are efficient algorithms for decoding Reed-Solomon codes.
- For adversary structures other than the threshold case it is not generally known whether there exists an error decodable secret sharing scheme with efficient decoding.

Kurosawa's Polynomial Time Error Decodable Scheme (Generalisation)

Takes any linear Σ^c-error decodable secret sharing scheme and constructs a Σ^c-error decodable secret sharing scheme with polynomial time decoding*, but having larger shares.

Kurosawa's Polynomial Time Error Decodable Scheme (Generalisation)

Takes any linear Σ^c-error decodable secret sharing scheme and constructs a Σ^c-error decodable secret sharing scheme with polynomial time decoding*, but having larger shares.

* polynomial in the total size of the shares. If the total size of the shares is polynomial in the number of participants, (*e.g.* for an ideal scheme) then Kurosawa's scheme can be decoded in time polynomial in the number of participants.

Kurosawa's Polynomial Time Scheme

$$\begin{array}{cccccc} & & & s & & \\ & & & \downarrow & & \\ v^1 & v^2 & v^3 & v^4 & \cdots & v^n \end{array}$$

level 1

M is used to generate share vector $\mathbf{v}$ corresponding to secret s

Kurosawa's Polynomial Time Scheme

$$\begin{array}{cccccc} & & & s & & \\ & & & \downarrow & & \\ \mathbf{w}^1 & v^2 & v^3 & v^4 & \cdots & v^n \\ \boxed{u_1^1} & \boxed{u_2^1} & \boxed{u_3^1} & \boxed{u_4^1} & \cdots & \boxed{u_n^1} \end{array}$$

level 1 — M is used to generate share vector $\mathbf{v}$ corresponding to secret s

level 2 — For $i = 1, 2, \ldots, n$ share v^i is converted to new secret vector $\mathbf{w}^i$ and M is used to generate corresponding share vector $\mathbf{u}^i$. Note: $\mathbf{w}^i$ includes the randomness used to generate $\mathbf{u}^i$.

Kurosawa's Polynomial Time Scheme

$$\begin{array}{c} s \\ \downarrow \end{array}$$

$\mathbf{w}^1$	$\mathbf{w}^2$	v^3	v^4	$\cdots$	v^n
u_1^1	u_2^1	u_3^1	u_4^1	$\cdots$	u_n^1
u_1^2	u_2^2	u_3^2	u_4^2	$\cdots$	u_n^2

level 1 — M is used to generate share vector $\mathbf{v}$ corresponding to secret s

level 2 — For $i = 1, 2, \ldots, n$ share v^i is converted to new secret vector $\mathbf{w}^i$ and M is used to generate corresponding share vector $\mathbf{u}^i$. Note: $\mathbf{w}^i$ includes the randomness used to generate $\mathbf{u}^i$.

Kurosawa's Polynomial Time Scheme

$$\begin{array}{ccccccl}
 & & & s & & & \\
 & & & \downarrow & & & \\
\mathbf{w}^1 & \mathbf{w}^2 & \mathbf{w}^3 & \mathbf{w}^4 & \cdots & \mathbf{w}^n & \text{level 1} \\
\boxed{u_1^1} & \boxed{u_2^1} & \boxed{u_3^1} & \boxed{u_4^1} & \cdots & \boxed{u_n^1} & \\
\boxed{u_1^2} & \boxed{u_2^2} & \boxed{u_3^2} & \boxed{u_4^2} & \cdots & \boxed{u_n^2} & \\
\boxed{u_1^3} & \boxed{u_2^3} & \boxed{u_3^3} & \boxed{u_4^3} & \cdots & \boxed{u_n^3} & \text{level 2} \\
 & & & \vdots & & & \\
\boxed{u_1^n} & \boxed{u_2^n} & \boxed{u_3^n} & \boxed{u_4^n} & \cdots & \boxed{u_n^n} &
\end{array}$$

M is used to generate share vector $\mathbf{v}$ corresponding to secret s

For $i = 1, 2, \ldots, n$ share v^i is converted to new secret vector $\mathbf{w}^i$ and M is used to generate corresponding share vector $\mathbf{u}^i$. Note: $\mathbf{w}^i$ includes the randomness used to generate $\mathbf{u}^i$.

Participant j receives share $\bigcup_{i=1}^{n} u_j^i \cup \mathbf{w}^j$, i.e., the jth column of data.

Kurosawa's Polynomial Time Scheme -Efficient Decoding

1. $\forall\ i$, generate share vector corresponding to secret vector $\mathbf{w}^i$, compare with other participants' level 2 shares.
2. If the set of positions where they differ is not in Γ, conclude that $\mathbf{w}^i$ is corrupted.
   Note: This can be done efficiently if $\Gamma = \Sigma^c$ because the scheme is linear.
3. Use uncorrupted level 1 shares to recover s.

received shares

$$\begin{array}{cccccc} \mathbf{w}^1 & \mathbf{w}^2 & \mathbf{w}^3 & \mathbf{w}^4 & \cdots & \mathbf{w}^n \\ \boxed{t_1^1} & \boxed{t_2^1} & \boxed{t_3^1} & \boxed{t_4^1} & \cdots & \boxed{t_n^1} \\ \boxed{t_1^2} & \boxed{t_2^2} & \boxed{t_3^2} & \boxed{t_4^2} & \cdots & \boxed{t_n^2} \\ & & & \vdots & & \end{array} \quad =? \quad \begin{array}{cccccc} & \mathbf{w}^2 & & & & \\ & \downarrow & & & & \\ \boxed{u_1^2} & \boxed{u_2^2} & \boxed{u_3^2} & \boxed{u_4^2} & \cdots & \boxed{u_n^2} \end{array}$$

Reducing the Storage Requirements of Kurosawa's Scheme

How to reduce the size of the level 2 shares:

- The level 2 schemes need not be perfect; they are only used to authenticate the level 1 shares.
- It suffices for the level 2 shares to be assigned using any (possibly non-perfect) secret-sharing scheme with the following properties:
  1. Sets of participants in Σ^c learn no information about the secret.
  2. For any two adversary sets $W_1, W_2 \in \Gamma$, the participants in $S \setminus (W_1 \cup W_2)$ should be able to recover the secret (this property is required to ensure that a level 2 share list, corrupted by an adversary set in Γ, determines a unique level 1 secret).
- Often, we can replace M by an appropriate ramp scheme.

Reducing the Storage Requirements of Kurosawa's Scheme (cont.)

How to reduce the number of level 2 schemes required:

- $A \subseteq S :=$ participants whose level 1 shares are shared using level 2 schemes.
- Decoding succeeds if we can find an authorised set whose shares are confirmed to be uncorrupted:

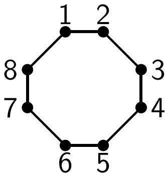
$\forall W \subseteq A$ with $W \in \Gamma$ we have $A \setminus W \in \Sigma$.

Corollary: The number of level 2 schemes required is upper bounded by

$$1 + \max_{W \in \Gamma} |W| + \max_{B \in \Sigma^c} |B|.$$

Example

$n = 8$, $\Sigma : \{\{1,2\},\{2,3\},\{3,4\},\{4,5\},\{5,6\},\{7,8\},\{8,1\}\}$



Γ: single participants

- It suffices to provide level 2 sharings for $\{1,2,3,4\}$ (given one adversary in $\{1,2,3,4\}$, there is still an uncorrupted authorised set in $\{1,2,3,4\}$).
  (This cuts the number of level 2 schemes needed by half.)
- We can use a $(4,6,8)$-ramp scheme ($|S \backslash (W_1 \cup W_2)| = 6$, and the maximum size of an unauthorised subset is 4).
  (This requires at most half the storage of any perfect scheme.)

One-Round (n, t)-Perfectly Secure Message Transmission *(Dolev, Dwark, Waarts, Yung 1993)*

Alice transmits a message s to Bob by sending information over n channels so that:

- Bob recovers s even if Eve corrupts $\leq t$ of the channels;
- Eve learns no information about s from the information Alice sent on the channels she corrupts.

- A (n, t)-PSMT scheme exists iff $n \geq 3t + 1$. (Dolev *et al.*)
- Desmedt, Wang and Burmester (2005):
  If Eve corrupts channels corresponding to a set in Γ then one-round PSMT is possible iff condition $Q(\Gamma, \Gamma, \Gamma)$ holds.
- When Γ is a threshold structure, the Dolev *et al* result is recovered.

One-Round (Γ, Σ^c)-PSMT

We consider a more general setting:

- Bob correctly recovers s if the information sent on a set $W \in \Gamma$ of channels is changed.
- Eve learns nothing about s if she eavesdrops on a set $D \in \Sigma^c$ of channels.

Theorem

A one-round (Γ, Σ^c)-PSMT scheme exists iff condition $Q(\Gamma, \Gamma, \Sigma^c)$ holds.

Proof: $(\Leftarrow)$: Use a Γ-error decodable secret sharing scheme realising Σ, send a share down each channel!
$(\Rightarrow)$: Use the proof technique from the error-decodability theorem.
Corollary: A one-round (Γ, Σ^c)-PSMT scheme exists iff there exists a Γ-error decodable secret sharing scheme realising Σ.

So are they really just the same thing?

So are they really just the same thing?

Not quite...

So are they really just the same thing?

Not quite...

Theorem

A one-round (Γ, Σ^c)-PSMT scheme is equivalent to a (not necessarily perfect) secret-sharing scheme where

- *the authorised sets are those of the form $S \setminus (W_1 \cup W_2)$ with $W_1, W_2 \in \Gamma$,*
- *the unauthorised sets belong to Σ^c.*

So are they really just the same thing?

Not quite...

Theorem

A one-round (Γ, Σ^c)*-PSMT scheme is equivalent to a (not necessarily perfect) secret-sharing scheme where*

- *the authorised sets are those of the form* $S \setminus (W_1 \cup W_2)$ *with* $W_1, W_2 \in \Gamma$*,*
- *the unauthorised sets belong to* Σ^c*.*

Corollary: A one-round (n, t)-PSMT scheme is equivalent to a $(t, n-2t, n)$-ramp scheme.

Efficiency of One-Round PSMT: Number of Channels

S -set of channels, Γ -active adversary, Σ^c -passive adversary

The minimum number of channels needed for one-round (Γ, Σ^c)-PSMT is $|T|$, where $T \subseteq S$ is the smallest subset for which $Q(\Gamma_T, \Gamma_T, \Sigma^c_T)$ holds.
Note: Γ_T denotes the restriction of Γ to T, and Σ^c_T denotes the restriction of Σ^c to T.

Corollary:

$$|T| \leq 1 + 2\max_{W \in \Gamma}|W| + \max_{B \in \Sigma^c}|B|.$$

(In the threshold case this reproves the result that one-round (n, t)-PSMT is possible iff $n \geq 3t + 1$.)

Efficiency of One-Round PSMT: Transmitted Info

Definition (overhead)

(total information sent over all channels)/(size of message s)

- Desmedt *et al.* describe a construction for a one-round (Γ, Γ)-PSMT for any Γ satisfying $Q(\Gamma, \Gamma, \Gamma)$ that's equivalent to a known secret sharing scheme construction.
- Kurosawa points out that in the threshold case this has a worse overhead than if an ideal threshold scheme is used.
- You can do better still if you use a ramp scheme!

Corollary (Fitzi *et al*): The optimal overhead of a one-round (n, t)-PSMT scheme is $n/(n - 3t)$.
Proof: Use the equivalence with ramp schemes and the fact that the optimal information rate of a (t, k, n)-ramp scheme is $k - t$ (Jackson & Martin).

Open Problems

- Do there exist constructions of one-round (Γ, Σ^c)-PSMT schemes with polynomial time message recovery for general Γ, Σ with lower communication overheads?
- Is it possible to determine in general which classes of Γ and Σ can be realised by schemes with efficient decoding/message recovery?
- Is it possible to find efficient decoding/message recovery techniques for specific classes of Γ and Σ?