Round-Efficient Perfectly Secure Message Transmission Scheme Against General Adversary

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

In the model of Perfectly Secure Message Transmission Schemes (PSMTs), there are n channels between a sender and a receiver, and they share no key. An infinitely powerful adversary $\mathbf{A}$ can corrupt (observe and forge) the messages sent through some subset of n channels. For non-threshold adversaries called Q^2, Kumar et al. showed a many round PSMT [8].

In this paper, we show round efficient PSMTs against Q^2-adevrsaries. We first give a 3-round PSMT which runs in polynomial time in the size of the underlying linear secret sharing scheme. We next present a 2-round PSMT which is inefficient in general. (However, it is efficient for some special case.)

Keywords: PSMT, adevrsary structure, 3-round, 2-round, Q^2-adversary

1 Introduction

The model of Perfectly Secure Message Transmission schemes (PSMT) was introduced by Dolev et al. [4]. 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 while an infinitely powerful adversary $\mathbf{A}$ can corrupt (observe and forge) the messages sent through some subset of n channels. A PSMT is a scheme which satisfies perfect privacy and perfect reliablity. Perfect privacy means that $\mathbf{A}$ learns no information on s. Perfect reliability means that the receiver can output $\hat{s} = s$ correctly.

A threshold adversary can corrupt t out of n channels. Dolev et al. showed that there exists a 1-round PSMT if and only if $n \geq 3t + 1$ [4], and there exists a 2-round PSMT if and only if $n \geq 2t + 1$ [4]. For $n \geq 3t + 1$, they also showed an efficient 1-round PSMT [4].

For $n = 2t + 1$, on the other hand, Srinathan et al. showed that n is a lower bound on the transmission rate of 2-round PSMT [12]. After the works of [11, 1], Kurosawa and Suzuki [9] gave a polynomial-time 2-round PSMT with the transmission rate $O(n)$.

On the other hand, a non-threshold adversary $\mathbf{A}$ is characterized by an adversary structure Γ which is the family of subsets of n channels that $\mathbf{A}$ can corrupt. Γ is said to be Q^2 if

$$(B_i \cup B_j) \neq \{1, \cdots, n\}$$

for any $B_i, B_j \in \Gamma$, and Q^3 if

$$(B_h \cup B_i \cup B_j) \neq \{1, \cdots, n\}$$

for any $B_h, B_i, B_j \in \Gamma$ [6]. We say that an adversary $\mathbf{A}$ is Q^2 if the Γ is Q^2, and $\mathbf{A}$ is Q^3 if the Γ is Q^3. We also define the maximal adversary structure Γ^+ as follows.

$$\Gamma^+ = \{B \mid B \in \Gamma \text{ and } B' \notin \Gamma \text{ for any } B' \supset B\}.$$

Desmedt et al. showed that a 1-round PSMT exists if and only if an adversary $\mathbf{A}$ is Q^3 [5]. However, their scheme was inefficient. Kurosawa showed an efficient 1-round PSMT which runs in polynomial time in the size of the underlying linear secret sharing scheme [10].

Kumar et al. showed a *many* round PSMT against Q^2-adversaries [8].

In this paper, we show round-efficient PSMTs against Q^2-adversaries. We first give a 3-round PSMT which runs in polynomial time in the size of the underlying linear secret sharing scheme. We next present a 2-round PSMT which is inefficient in general. (However, it is efficient if $|\Gamma^+|$ is small.) Our first scheme is based on the verifiable secret sharing scheme of [2, 3], and our second scheme is based on the secret sharing scheme of [7].

We also show how to achieve a reliable broadcast functionality efficiently in this model.

	threshold adversary	non-threshold adversary
1-round	$n \geq 3t + 1$ [4]	Q^3 [5, 10]
2-round	$n \geq 2t + 1$ [4, 9]	Q^2 but not poly (this paper)
3-round		Q^2 and poly (this paper)

Table 1: Round complexity of PSMT

For $B \in \{1, \cdots, n\}$, B^c denotes the complement of B. That is, $B^c = \{1, \cdots, n\} \setminus B$.

	Kumar et al. [8]	Our scheme (poly)	Our scheme (not poly)
# of rounds	many	3	2

Table 2: PSMT against Q^2-adevrsaries

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. The family of access sets is called an access structure.

Definition 2.1 *An access structure Σ is monotone if $A \in \Sigma$ and $A' \supseteq A$, then $A' \in \Sigma$.*

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) (see [7]). Let M be an $\ell \times e$ matrix over a finite field F and $\psi : \{1, \cdots, \ell\} \to \{1, \cdots, n\}$ be a labeling function, where $\ell \geq e$ and $\ell \geq n$.

Distribution algorithm:

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

2. Let
$$\mathsf{LSSS}(s, \vec{\rho}) = (\mathtt{share}_1, \cdots, \mathtt{share}_n), \tag{2}$$
where $\mathtt{share}_i = \{v_j \mid \psi(j) = i\}$. 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

$$M_A = \{\vec{m}_j \mid \psi(j) \in A\},$$

where $\vec{m}_j$ denots the jth row of M.

Definition 2.2 *We say that the above* (M, ψ) *is a monotone span program which realizes* Σ.

The size of the LSSS is defined as ℓ which is the total number of field elements that are distributed by the dealer.

3 How to Broadcast

Suppose that there are n channels between a sender **S** and a receiver **R**, and there exists a Q^2 adversary **A** who is characterzed by an adversary structure Γ. Here we assume that $\Sigma = \Gamma^c$ is monotone. This means that if $B \in \Gamma$ and $B' \subseteq B$, then $B' \in \Gamma$.

In this section, we show how to achieve a reliable broadcast functionality efficiently in this model. We say that **S** broadcasts x if she sends x through all n channels. Since **A** corrupts some subset of channels, **R** receives x_i through channel i for $i = 1, \cdots, n$, where $x_i = x$ or $x_i \neq x$.

It is known that if **A** corrupts t out of $n = 2t + 1$ channels, then **R** can recover x by simply taking the majority vote. Hence a naive approach of **R** would be as follows. Let $\Gamma^+ = \{B_1, B_2, \cdots, B_L\}$.

> For $i = 1, \cdots, L$, do;
>   if $x_j = x_0$ for some x_0 for all $j \in B_i^c$,
>   then output x_0 and stop.

However, this algorithm is very inefficient because L is large in general. For exampl, if **A** corrupts t out of $n = 2t + 1$ channels, then $L = \binom{2t+1}{t}$ which is exponential.

3.1 Proposed Algorithm of Receiver

Now our algorithm of **R** is as follows.

> For $i = 1, \cdots, n$, do;
>   Let $C_i = \{j \mid x_j \neq x_i\}$.
>   If $C_i \in \Gamma$,
>   then output x_i and stop.

This algorithm is very efficient and runs in $O(n^2 T)$, where T denotes the time to check if $C_i \in \Gamma$. (See Fig.1.)

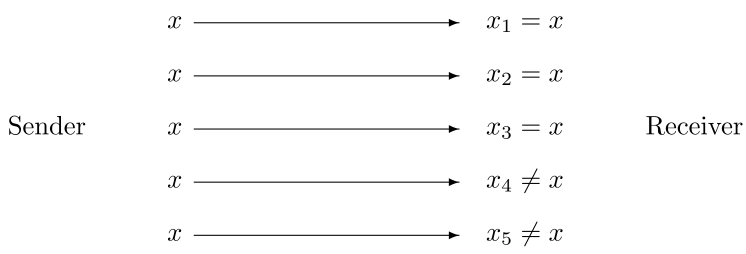

Figure 1: Example of Broadcast, where $C_1 = \{4, 5\}$

3.2 Correctness

The correctness of our algorithm is given by the following lemmas.

Lemma 3.1 **R** *outputs some* x_i.

(Proof.) It is enough to show that $C_i \in \Gamma$ for some i. Suppose that **A** corrupts $B \in \Gamma$. Then for each $i \notin B$,

$$C_i = B \in \Gamma.$$

This means that the Lemma holds.

Q.E.D.

Lemma 3.2 *If* $B \in \Gamma$*, then* $B^c \notin \Gamma$*. (That is,* $B^c \in \Sigma$*.)*

(Proof.) Suppose that $B \in \Gamma$. On the other hand, $B \cup B^c = \{1, \cdots, n\}$. Therefore $B^c \notin \Gamma$ because Γ is Q^2.

Q.E.D.

Lemma 3.3 *If* **R** *outputs* x_i*, then* $x_i = x$.

(Proof.) Suppose that **A** corrupts some $B \in \Gamma$. Suppose that **R** outputs x_i such that $x_i \neq x$. Then $i \in B$ clearly because $x_i \neq x$.

On the other hand, we have $x_j = x$ for all $j \in B^c$. Hence if $j \in B^c$, then $x_j = x \neq x_i$. This means that

$$C_i = \{j \mid x_j \neq x_i\} \supseteq B^c,$$

Therefore we have $C_i \notin \Gamma$ from Lemma 3.2. However this contradicts to our algorithm of **R**.

Q.E.D.

4 Efficient 3-Round PSMT against Q^2-Adversary

In this section, we show a polynomial-time 3-round PSMT against Q^2-adversary structures Γ. Let (M, ψ) be a monotone span program which realizes the access structure $\Sigma = \Gamma^c$. For simplicity, we assume that $\ell = n$ and $\psi(i) = i$ for $i = 1, \cdots, n$. Hence

$$M = \begin{pmatrix} \vec{m}_1 \\ \vdots \\ \vec{m}_n \end{pmatrix}$$

is an $n \times e$ matrix over a finite field F. In what follows, $(\vec{m}, \vec{v}^T)$ denotes the inner product of two vectors $\vec{m}$ and $\vec{v}$, where ^{T} denotes transpose.

4.1 Protocol

The 1st Round: For a secret $s \in \mathsf{F}$, the sender **S** chooses an $e \times e$ symmetric matrix $E = \{e_{ij}\}$ such that $e_{1,1} = s$ randomly. **S** then computes

$$\begin{pmatrix} \vec{v}_1 \\ \vdots \\ \vec{v}_n \end{pmatrix} = M \cdot E \tag{3}$$

and sends $\vec{v}_i$ through channel i for each i.

Note that $(M \cdot E) \cdot M^T$ is a symmetric matrix because E is a symmetric matrix. Hence

$$(\vec{v}_i, \vec{m}_j^T) = (\vec{v}_j, \vec{m}_i^T). \tag{4}$$

The 2nd Round: Suppose that receiver **R** received $\vec{v}_i'$ through channel i for $i = 1, \cdots, n$. **R** broadcasts all (i, j) such that

$$(\vec{v}_i', \vec{m}_j^T) \neq (\vec{v}_j', \vec{m}_i^T).$$

The 3rd Round: For each (i, j) that **R** broadcast, **S** broadcasts $b_{ij} = b_{ji}$ such that

$$b_{ij} = (\vec{v}_i, \vec{m}_j^T) = (\vec{v}_j, \vec{m}_i^T) = b_{ji}.$$

We say that channel i is bad if $(\vec{v}_i', \vec{m}_j^T) \neq b_{ij}$ for some $j \neq i$. Otherwise we say that channel i is good. Let BAD be the set of all bad channels, and GOOD be the set of all good channels.

Wlog, let $\mathsf{GOOD} = \{1, \cdots, t\}$. Then **R** reconstructs s by applying the reconstruction algorithm of the LSSS to $v_{1,1}', \cdots, v_{t,1}'$, where $\vec{v}_i' = (v_{i,1}', \cdots, v_{i,e}')$.

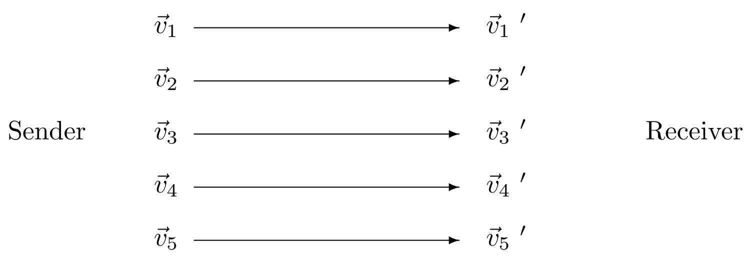

Figure 2: The 1st round of Our 3-Round PSMT

4.2 Security Proofs

Theorem 4.1 *The above protocol satisfies perfect privacy.*

(Proof.) An adversary **A** can corrupt some subset of channels $B \in \Gamma$. Note that B is a non-access set of the LSSS. Hence in the 1st round, **A** learns no information on s. (Note that only the first element of $\vec{v}_i$ is related to s.)

If **R** broadcasts (i, j) in the 2nd round, then **A** corrupted channel i or channel j. Hence **A** already knows the value of

$$b_{ij} = (\vec{v}_i, \vec{m}_j^T) = (\vec{v}_j, \vec{m}_i^T).$$

Hence **A** gains no information in the 3rd round even if **S** broadcasts b_{ij}. Thus **A** learns no information on s.

Q.E.D.

Suppose that an adversary **A** corrupts $B \in \Gamma$.

Lemma 4.1 *B^c is an access set of the LSSS.*

(Proof.) From Lemma 3.2.

Q.E.D.

Lemma 4.2 *$B^c \subseteq \mathsf{GOOD}$. Hence GOOD is also an access set of the LSSS.*

(Proof.) If channel i is bad, then it is clear that $i \in B$. This means that $\mathsf{BAD} \subseteq B$. Therefore

$$\mathsf{GOOD} = \mathsf{BAD}^c \supset B^c.$$

Hence GOOD is an access set of the LSSS from Lemma 4.1.

Q.E.D.

Lemma 4.3 *For any pair of good channels i and j, it holds that*

$$(\vec{v}_i', \vec{m}_j^T) = (\vec{v}_j', \vec{m}_i^T).$$

(Proof.) Suppose that there exist a pair of good channels i and j such that the above equation does not hold. Then **R** broadcasts the (i,j), and **S** broadcasts $b_{ij} = b_{ji}$. This means that $b_{ij} \neq (\vec{v}_i', \vec{m}_j^T)$ or $b_{ji} \neq (\vec{v}_j', \vec{m}_i^T)$. Hence channel i is bad or channel j is bad. This is a contradiction.

Q.E.D.

Lemma 4.4 *Without loss of generality, assume that* $\mathsf{GOOD} = \{1, \cdots, t\}$. *Then there exists a vector $\vec{x} = (s', \vec{\rho}')$ such that*

$$(v_{1,1}', \cdots, v_{t,1}')^T = M_0 \cdot \vec{x}^T,$$

where

$$M_0 = \begin{pmatrix} \vec{m}_1 \\ \vdots \\ \vec{m}_t \end{pmatrix}.$$

That is, $(v_{1,1}', \cdots, v_{t,1}')$ is a share vector of the LSSS with M_0.

(Proof.) From Lemma 4.3, there exists a_{ij} such that

$$(\vec{m}_i, \vec{v}_j'^T) = (\vec{v}_i', \vec{m}_j^T) = a_{ij}$$

for any (i,j) such that $i \in \mathsf{GOOD}$ and $j \in \mathsf{GOOD}$. Let $U_0 = \{a_{i,j}\}$ be a $t \times t$ symmetric matrix. Then U_0 can be written as

$$U_0 = M_0 \cdot V_0 = V_0^T \cdot M_0^T,$$

where $V_0 = [\vec{v}_1'^T, \cdots, \vec{v}_t'^T]$.

On the other hand, GOOD is an access set from Lemma 4.2. Therefore there exists a vector $\vec{\alpha}_0$ such that $\vec{\alpha}_0 \cdot M_0 = (1, 0, \cdots, 0)$. Hence

$$\vec{\alpha}_0 \cdot U_0 \quad = \quad \vec{\alpha}_0 \cdot M_0 \cdot V_0 = (1, 0, \cdots, 0) \cdot V_0 = (v_{1,1}', \cdots, v_{t,1}')$$

Now

$$\vec{\alpha}_0 \cdot U_0 \quad = \quad \vec{\alpha}_0 \cdot V_0^T \cdot M_0^T = \vec{x} \cdot M_0^T$$

where $\vec{x} = \vec{\alpha}_0 \cdot V_0^T$. Therefore,

$$(v_{1,1}', \cdots, v_{t,1}') = \vec{x} \cdot M_0^T.$$

Q.E.D.

Theorem 4.2 *The above protocol satisfies perfect reliability.*

(Proof.) The receiver **R** received $\vec{v}_i' = (v_{i,1}', \cdots, v_{i,e}')$ through channel i for $i = 1, \cdots, n$. Suppose that an adversary **A** corrupts $B \in \Gamma$. Wlog, let $B^c = \{1, \cdots, k\}$. Then it is clear that $\vec{v}_i' = \vec{v}_i$ for $i = 1, \cdots k$. Hence the original secret s is obtained if we apply the reconstruction algorithm of the LSSS to $(v_{1,1}', \cdots, v_{k,1}')$ from Lemma 4.1.

On the other hand, $B^c \subseteq \mathsf{GOOD}$ from Lemma 4.3. Hence, wlog, let $\mathsf{GOOD} = \{1, \cdots, t\}$, where $t \geq k$. Suppose that s' is obtained by applying the reconstruction algorithm of the LSSS to $(v_{1,1}', \cdots, v_{t,1}')$. Then it must be that $s' = s$ because $B^c \subseteq \mathsf{GOOD}$. Hence **R** can compute s correctly.

Q.E.D.

4.3 Efficiency

In the 1st round, the sender sends $\ell \cdot e$ field elements. (Remember that M is an $\ell \times e$ matrix.) In the 2nd round, the receiver sends $O(\ell^2 n)$ elements of Z_ℓ. In the 3rd round, the sender sends $O(\ell^2 n)$ field elements.

It is easy to see that the sender and the receiver run in polynomial time in the size of the LSSS (which is ℓ).

5 2-Round PSMT against Q^2-Adversary

In this section, we show a 2-round PSMT for Q^2-adversaries. It is inefficient in general. However, it is efficient if $L = |\Gamma^+|$ is small, where $\Gamma^+ = \{B_1, B_2, \cdots, B_L\}$ is the maximal adversary structure (such that Γ is Q^2).

5.1 Protocol

Let $s \in \mathsf{F}$ be a secret of the sender **S**. Let OK be $\emptyset$.

The 1st Round: For $i = 1, \cdots, L$, **R** chooses $r_i \in \mathsf{F}$ randomly, and sends r_i through all channels belonging to B_i^c. (In other words, **R** broadcasts r_i over B_i^c.)

The 2nd Round:

1. For $i = 1, \cdots, L$, **S** adds i to OK if she received some identical r_i' through all channels belonging to B_i^c.
2. **S** computes $c = s + \sum_{i \in \mathsf{OK}} r_i'$.
3. **S** broadcasts c and OK.

Finally **R** computes $\hat{s}$ such that

$$\hat{s} = c - \sum_{i \in \mathsf{OK}} r_i.$$

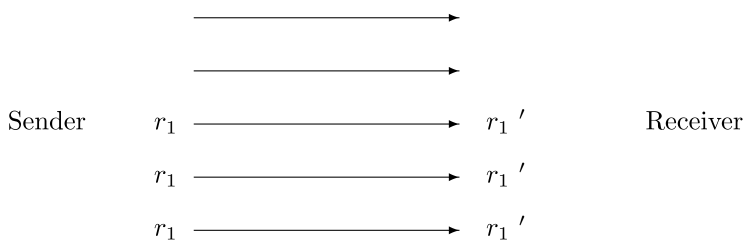

Figure 3: The 1st round of the proposed 2-Round PSMT, where $B_1 = \{1, 2\}$

5.2 Security Proofs

Theorem 5.1 *The above protocol satisfies perfect privacy.*

(Proof.) Suppose that an adversary **A** corrupted $B_j \in \Gamma$. Then **A** does not know r_j because **R** sent r_j through all channels belonging to B_j^c. Further **S** receives r_j correctly through all channels belonging to B_j^c. Hence $j \in \mathsf{OK}$. Therefore **S** learns no information on s from c because r_j works as the one-time pad.

Q.E.D.

Theorem 5.2 *The above protocol satisfies perfect reliability.*

(Proof.) We show that $r_i' = r_i$ if $i \in \mathsf{OK}$. Suppose that an adversary **A** corrupted $B_j \in \Gamma$. Then there exists some channel k such that $k \in B_i^c \setminus B_j$ because Γ is Q^2. This means that **S** receives r_i correctly through the channel k.

Hence if $i \in \mathsf{OK}$, then it must be that **S** received r_i correctly through all channels belonging to B_i^c. Therefore $r_i' = r_i$ if $i \in \mathsf{OK}$. It implies that **R** computes s correctly.

Q.E.D.

5.3 Efficiency

In the 1st round, the receiver sends $O(nL)$ field elements. In the 2nd round, the sender sends $O(n)$ field elements and $O(nL)$ elements of Z_L.

References

[1] S.Agarwal, R.Cramer and R.de Haan: Asymptotically Optimal Two-Round Perfectly Secure Message Transmission. CRYPTO 2006: pp.394–408 (2006)

[2] M. Ben-Or, S. Goldwasser, and A. Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation. In *Proceedings of the twentieth annual ACM Symp. Theory of Computing, STOC*, pp. 1–10, May 2–4, 1988.

[3] R. Cramer, I. Damgård, and U. M. Maurer. General secure multi-party computation from any linear secret-sharing scheme. In B. Preneel, editor, *Advances in Cryptology — Eurocrypt 2000, Proceedings (Lecture Notes in Computer Science 1807)*, pp. 316–334. Springer-Verlag, 2000. Bruges, Belgium, May 14–18.

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

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

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

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

[8] M. V. N. Ashwin Kumar, Pranava R. Goundan, K. Srinathan, C. Pandu Rangan: On perfectly secure cmmunication over arbitrary networks. PODC 2002, pp.193–202 (2002)

[9] K.Kurosawa and K.Suzuki: Truly Efficient 2-Round Perfectly Secure Message Transmission Scheme. IEEE Transactions on Information Theory, 55, 1, pp.5223–5232 (2009)

[10] Kaoru Kurosawa: General Error Decodable Secret Sharing Scheme and Its Application. IACR Cryptology ePrint Archive, Report 2009/263 (2009).

[11] H.Md.Sayeed and H.Abu-Amara: Efficient Perfectly Secure Message Transmission in Synchronous Networks. Inf. Comput. 126(1): pp.53–61 (1996)

[12] K. Srinathan, Arvind Narayanan, C. Pandu Rangan: Optimal Perfectly Secure Message Transmission. CRYPTO 2004: pp.545–561 (2004)