Almost Secure (1-Round, n-Channel) Message Transmission Scheme

Kaoru Kurosawa[1] and Kazuhiro Suzuki[2]

[1] Department of Computer and Information Sciences, Ibaraki University, Japan
kurosawa@mx.ibaraki.ac.jp
[2] Venture Business Laboratory, Ibaraki University, Japan
tutetuti@dream.com

Abstract. It is known that perfectly secure (1-round, n-channel) message transmission (MT) schemes exist if and only if $n \geq 3t + 1$, where t is the number of channels that the adversary can corrupt. Then does there exist an *almost* secure MT scheme for $n = 2t + 1$? In this paper, we first sum up a number flaws of the previous *almost* secure MT scheme presented at Crypto 2004 [3]. We next show an equivalence between almost secure MT schemes and secret sharing schemes with cheaters. By using our equivalence, we derive a lower bound on the communication complexity of almost secure MT schemes. Finally, we present a near optimum scheme which meets our bound approximately. This is the first construction of provably secure almost secure (1-round, n-channel) MT schemes for $n = 2t + 1$.

Keywords: Private and reliable transmission, information theoretic security, communication efficiency

1 Introduction

1.1 Message Transmission Scheme

The model of (r-round, n-channel) message transmission schemes was introduced by Dolev et al. [2]. In this model, there are n channels between a sender and a receiver while they share no keys. The sender wishes to send a secret s to the receiver in r-rounds securely and reliably. An adversary **A** can observe and forge the messages sent through t out of n channels.

We say that a (r-round, n-channel) message transmission scheme is perfectly t-secure if **A** learns no information on s (perfect privacy), and the receiver can output $\hat{s} = s$ correctly (perfect reliability) for any infinitely powerful adversary **A** who can corrupt at most t channels (in information theoretic sense). [4] Dolev et al. showed that [2]

[3] The authors already noted in thier presentation at Crypto'2004 that their scheme was flawed. It was Ronald Cramer who informed the authors of the flaw.

[4] Dolev et al. called it a perfectly secure message transmission scheme [2].

– $n \geq 3t + 1$ is necessary and sufficient for $r = 1$, and
– $n \geq 2t + 1$ is necessary and sufficient for $r = 2$

to achieve perfect t-security.

A perfectly t-secure scheme with optimum communication complexity is known for $r = 1$ and $n = 3t + 1$ [2, 6]. Based on the work of [5, 6], Agarwal et al. showed an asymptotically optimum perfectly t-secure scheme for $r = 2$ and $n = 2t + 1$ [1].

1.2 Secret Sharing Scheme with Cheaters

Tompa and Woll introduced a problem of cheating in (k, n) threshold secret sharing schemes [7]. In this problem $k - 1$ malicious participants aim to cheat an honest one by opening forged shares and causing the honest participant to reconstruct the wrong secret.

Ogata et al. derived a tight lower bound on the size of shares $|\mathcal{V}_i|$ for secret sharing schemes that protects against this type of attack: $|\mathcal{V}_i| \geq (|\mathcal{S}| - 1)/\delta + 1$, where $\mathcal{V}_i$ denotes the set of shares of participant P_i, $\mathcal{S}$ denotes the set of secrets, and δ denotes the cheating probability [4]. [5]

They also presented an optimum scheme, which meets the equality of their bound by using "difference sets" [4].

1.3 Our Contribution

As we mentioned, it is known that perfectly secure (1-round, n-channel) message transmission schemes exist if and only if $n \geq 3t + 1$, where t is the number of channels that adversary can corrupt. Then does there exist an *almost* secure scheme for $n = 2t + 1$? At Crypto 2004, Srinathan et al. [6, Sec.5] proposed an almost secure (1-round, n-channel) message transmission scheme for $n = 2t + 1$. However, the authors already noted in thier presentation at Crypto'2004 that their scheme was flawed.

In this paper, we first sum up a number of flaws of the above scheme. (Actually, they showed two schemes in [6], a perfectly t-secure scheme and an almost secure scheme. Agarwal et al. showed a flaw of the former one [1].)

Table 1. Previous Work and Our Contribution

	Perfectly t-secure	Almost secure
$r = 1$	$n \geq 3t + 1$	$n = 2t + 1$ This paper
$r = 2$	$n \geq 2t + 1$	–

[5] $|\mathcal{X}|$ denotes the cardinality of a set $\mathcal{X}$.

We next show an equivalence between almost secure (1-round, n-channel) message transmission schemes with $n = 2t + 1$ and secret sharing schemes with cheaters. By using our equivalence, we derive a lower bound on the communication complexity of almost secure (1-round, n-channel) message transmission schemes (in the above sense) such that

$$|\mathcal{X}_i| \geq (|\mathcal{S}| - 1)/\delta + 1,$$

where $\mathcal{X}_i$ denotes the set of messages sent through the ith channel and $\mathcal{S}$ denotes the set of secrets which the sender wishes to send to the receiver.

We finally show a near optimum scheme which meets our bound approximately. This is the first construction of almost secure (1-round, n-channel) message transmission schemes for $n = 2t + 1$.

Our results imply that $n \geq 2t+1$ is necessary and sufficient for almost secure (1-round, n-channel) message transmission schemes.

2 Flaw of the Previous Almost Secure MT Scheme

In this section, we sum up a number of flaws of the previous almost secure (1-round, n-channel) message transmission scheme [6, Sec.5]. [6] Let $n = 2t + 1$ in what follows.

2.1 Previous Almost Secure Message Transmission Scheme

Their scheme [6, Sec.5] is described is as follows. For simplicity, let $\mathbb{F}$ be a finite field $GF(q)$ such that q is a prime, and assume that the sender wishes to send a secret $s = (s_1, \ldots, s_{t+1})$ to the receiver, where each s_i is an element of $\mathbb{F}$. [7]

- **Enc**. The sender computes a ciphertext $(x_1, \cdots, x_n)$ from $s = (s_1, \ldots, s_{t+1})$ as follows.
  1. Randomly select n polynomials $p_1(x), \cdots, p_n(x)$ of degree at most t over $\mathbb{F}$ such that
  $$Q(1) = s_1, \cdots, Q(t+1) = s_{t+1}, \qquad (1)$$
  where [8] $Q(x) = p_1(0) + p_2(0)x + p_3(0)x^2 + \cdots + p_n(0)x^{n-1}$.
  2. For each (i, j) with $i \neq j$, randomly select one of the t points of intersection of p_i and p_j so that $r_{ij} \neq r_{ji}$ (denote the selected point by r_{ij}).
  3. For each i, let $x_i = (p_i(x), r_{ij}$ for all $j \neq i)$.
  4. Output $(x_1, x_2, \ldots, x_n)$.
- **Dec**. The receiver computes $s = (s_1, \ldots, s_{t+1})$ or $\perp$ from $(\hat{x}_1, \hat{x}_2, \ldots, \hat{x}_n)$ as follows, where $\hat{x}_i = (\hat{p}_i(x), \hat{r}_{ij}$ for all $j \neq i)$.

[6] They called it a Las Vegas scheme.

[7] In [6, Sec.5], the sender sends a message $m = (m_1, \cdots, m_{t+1})$ to the receiver by broadcasting $y = m + s$ through all the channels.

[8] In [6, Sec.5], they wrote this as $s = \text{EXTRAND}(p_1(0), \cdots, p_n(0))$.

1. Set $\Lambda = \{1, 2, \ldots, n\}$.
2. We say that the i-th channel ch_i *contradicts* the j-th channel ch_j if $\hat{p}_i$ and $\hat{p}_j$ do not intersect at $\hat{r}_{ij}$.
3. For each i, if ch_i is contradicted by at least $t+1$ channels then remove i from Λ.
4. If ch_i contradicts ch_j for some $i, j \in \Lambda$ then output **failure**.
5. If $|\Lambda| \leq t$, then output **failure**.
6. At this point, $\hat{p}_i = p_i$ for all $i \in \Lambda$ and $|\Lambda| \geq t+1$.
   Derive all the polynomials $p_1, \ldots, p_n$ from $\hat{p}_i$ and $\hat{r}_{ij}$ $(i \in \Lambda)$.
7. Compute s as $s = [Q(1), \ldots, Q(t+1)]$.

Srinathan et al. claimed the following lemmas for adversaries who can corrupts at most t out of n channels [6, Sec.5].

Lemma 1. *[6, Lemma 11]* **Reliability.** *The receiver will never output an incorrect value.*

Lemma 2. *[6, Lemma 13]* **Perfect Privacy.** *The adversary gains no information about the secret.*

2.2 Flaws

We show that the above two lemmas do not hold. In the above scheme, it is important to choose $p_1, \cdots, p_n$ randomly because otherwise we cannot ensure the perfect privacy. However, if the sender chooses $p_1, \cdots, p_n$ randomly, it has the following problems. For simplicity, suppose that $t = 2$ and $n = 2t + 1 = 5$. (It is easy to generalize the following argument to any $t \geq 2$.)

- **Sender's problem:** Since the polynomials $p_1, \ldots, p_5$ are randomly chosen, it can happen that some p_i and p_j do not intersect or intersect at one point. In these cases, the sender cannot execute Step 2 of **Enc**.
- **Perfect Privacy:** Suppose that the adversary **A** corrupts $t = 2$ channels 1 and 2. In most cases, **A** has no information on s_1, s_2, s_3 because eq.(1) has $t + 1 = 3$ equations and 3 unknown variables $p_3(0), p_4(0)$ and $p_5(0)$, where $p_3(0), p_4(0)$ and $p_5(0)$ are randomly chosen.
  However, with nonzero probability, it happens that $p_1(x)$ and $p_3(x)$ intersect at $x = 0$ and hence $r_{1,3} = 0$. In this case, **A** can compute $p_3(0)$, and she knows 3 values, $p_1(0), p_2(0)$ and $p_3(0)$. Consequently, **A** has only 2 unknown variables $p_4(0)$ and $p_5(0)$ in eq.(1). This means that **A** can learn some information on $s = (s_1, s_2, s_3)$ with nonzero probability. Therefore Lemma 2 (perfect privacy) does not hold.
- **Reliability:** Since the polynomials $p_1(x), \ldots, p_5(x)$ are all randomly chosen, it can happen that

$$b_1 = p_1(a_1) = \cdots = p_5(a_1)$$
$$b_2 = p_1(a_2) = \cdots = p_5(a_2)$$

with nonzero probability. That is, all polynomials go through (a_1, b_1) and (a_2, b_2). In this case, the sender will set $r_{ij} = a_1$ and $r_{ji} = a_2$ for each pair $i < j$.

Now consider an adversary **A** who corrupts channel 1 and replaces $p_1(x)$ with a random polynomial $p_1'(x)$. Then it can still happen that p_1' passes through (a_1, b_1) and (a_2, b_2) with nonzero probability. In this case, the receiver accepts p_1'. Hence the receiver outputs $\hat{s} \neq s$ because $p_1'(0) \neq p_1(0)$. After all, the receiver outputs $\hat{s} \neq s$ with nonzero probability. Therefore, Lemma 1 does not hold.

We cannot fix these flaws. To correct these flaws, **Enc** must choose $p_1, \cdots, p_5$ in such a way that

– p_i and p_j intersect at at least two points,
– $r_{ij} \neq 0$,
– and all intersection points are distinct

for each pair of (i, j). However, if so, the perfect privacy does not hold because $p_1, \cdots, p_5$ are not random.

Suppose that the adversary **A** corrupts $t = 2$ channels 1 and 2. Then she learns the values of $p_1(0), p_2(0)$. Hence she knows that $p_3(0), \ldots, p_5(0)$ are not elements of $\{p_1(0), p_2(0)\}$. That is, $p_3(0), \ldots, p_5(0)$ are not randomly chosen from $\mathbb{F}$. Hence she can learn some information on s from eq.(1).

3 Model

In this section, we define a model of Almost Secure (1-round, n-channel) message transmission schemes formally. In the model, there are n channels between a sender and a receiver. The sender wishes to send a secret s to the receiver secretly and reliably in one-round without sharing any keys. An adversary can observe and forge the messages sent through at most t out of n channels.

A (1-round, n-channel) message transmission scheme consists of a pair of algorithms $(\mathbf{Enc}, \mathbf{Dec})$ as follows. Let $\mathcal{S}$ denote the set of secrets.

– **Enc** is a probabilistic encryption algorithm which takes a secret $s \in \mathcal{S}$ as an input, and outputs a ciphertext $(x_1, \cdots, x_n)$, where x_i is the i-th channel's message.
– **Dec** is a deterministic decryption algorithm which takes an alleged ciphertext $(\hat{x}_1, \cdots, \hat{x}_n)$ and outputs $\hat{s} \in \mathcal{S}$ or **failure**.

We require that $\mathbf{Dec}(\mathbf{Enc}(s)) = s$ for any $s \in \mathcal{S}$. We assume a certain probability distribution over $\mathcal{S}$, and let S denote the random variable. Let X_i denote the random variable induced by x_i, and $\mathcal{X}_i$ denote the possible set of x_i for $1 \leq i \leq n$.

To define the security, we consider the following game among the sender, the receiver and an adversary **A**, where **A** is a (infinitely powerful) probabilistic Turing machine.

1. **A** chooses t channels, $i_1, \cdots, i_t$.
2. The sender chooses $s \in \mathcal{S}$ according to the distribution over $\mathcal{S}$, and uses **Enc** to compute $x_1, \cdots, x_n$. Then x_i is sent to the receiver through channel i for $1 \leq i \leq n$.
3. **A** observes $x_{i_1}, \cdots, x_{i_t}$, and forges them to $x'_{i_1}, \cdots, x'_{i_t}$. We allow x'_{i_j} to be the null string for $1 \leq j \leq t$.
4. The receiver receives $\hat{x}_i$ through channel i for $1 \leq i \leq n$, and uses **Dec** to compute

$$\mathbf{Dec}(\hat{x}_1, \cdots, \hat{x}_n) = \hat{s} \text{ or } \mathbf{failure}.$$

Definition 1. *We say that a (1-round, n-channel) message transmission scheme is (t, δ)-secure if the following conditions are satisfied for any adversary* **A** *who can corrupt at most t out of n channels.*

Privacy. **A** *learns no information on s. More precisely,*

$$\Pr(S = s \mid X_{i_1} = x_{i_1}, \cdots, X_{i_t} = x_{i_t}) = \Pr(S = s)$$

for any $s \in \mathcal{S}$ and any possible $x_{i_1}, \cdots, x_{i_t}$.

General Reliability. *The receiver outputs $\hat{s} = s$ or* **failure**. *(He never outputs a wrong secret.)*

Trivial Reliability. *If the t forged messages $x'_{i_1}, \cdots, x'_{i_t}$ are all null strings, then* **Dec** *outputs $\hat{s} = s$.*

Failure.

$$\Pr(\mathbf{Dec} \textit{ outputs } \mathbf{failure}) < \delta. \tag{2}$$

(The trivial reliability means that if t channel fail to deliver messages, then **Dec** outputs $\hat{s} = s$. Hence this is a reasonable requirement.)

4 Secret Sharing Scheme with Cheaters

In the model of secret sharing schemes, there is a probabilistic Turing machine D called a dealer. S denotes a random variable distributed over a finite set $\mathcal{S}$, and $s \in \mathcal{S}$ is called a secret. On input $s \in \mathcal{S}$, D outputs $(v_1, \ldots, v_n)$ according to some fixed probability distribution. For $1 \leq i \leq n$, each participant P_i holds v_i as his share. V_i denotes the random variable induced by v_i. Let $\mathcal{V}_i = \{v_i \mid \Pr[V_i = v_i] > 0\}$. $\mathcal{V}_i$ is the set of possible shares held by P_i.

Definition 2. *We say that D is a (k, n) threshold secret sharing scheme for S if the following two requirements hold:*

(A1) *Let $j \geq k$. Then there exists a unique $s \in \mathcal{S}$ such that*

$$\Pr[S = s \mid V_{i_1} = v_{i_1}, \ldots, V_{i_j} = v_{i_j}] = 1$$

for any $\{i_1, \ldots, i_j\} \subseteq \{1, \ldots, n\}$ and any $(v_{i_1}, \ldots, v_{i_j})$ with $\Pr[V_{i_1} = v_{i_1}, \ldots, V_{i_j} = v_{i_j}] > 0$.

(A2) *Let $j < k$. Then for each $s \in \mathcal{S}$,*

$$\Pr[S = s \mid V_{i_1} = v_{i_1}, \ldots, V_{i_j} = v_{i_j}] = \Pr[S = s]$$

for any $\{i_1, \ldots, i_j\} \subseteq \{1, \ldots, n\}$ and any $(v_{i_1}, \ldots, v_{i_j})$ with $\Pr[V_{i_1} = v_{i_1}, \ldots, V_{i_j} = v_{i_j}] > 0$.

Now we consider $k-1$ malicious participants who aim to cheat an honest one by opening forged shares and causing the honest participant to reconstruct the wrong secret.

Definition 3. *For $A = \{i_1, \cdots, i_k\}$ and $v_{i_1} \in \mathcal{V}_{i_1}, \ldots, v_{i_k} \in \mathcal{V}_{i_k}$, define*

$$\mathsf{Sec}_I(v_{i_1}, \ldots, v_{i_k}) = \begin{cases} s & \text{if } \exists s \in \mathcal{S} \text{ s.t. } \Pr[S = s \mid V_{i_1} = v_{i_1}, \cdots, V_{i_k} = v_{i_k}] = 1, \\ \perp & \text{otherwise.} \end{cases}$$

That is, $\mathsf{Sec}_I(v_{i_1}, \ldots, v_{i_k})$ denotes the secret reconstructed from the k possible shares $(v_{i_1}, \ldots, v_{i_k})$ associated with $(P_{i_1}, \ldots, P_{i_k})$, respectively. The symbol $\perp$ is used to indicate when no secret can be reconstructed from the k shares. We will often aggregate the first $k-1$ arguments of Sec_I into a vector, by defining $\mathbf{b} = (v_{i_1}, \ldots, v_{i_{k-1}})$ and $\mathsf{Sec}_I(\mathbf{b}, v_{i_k}) = \mathsf{Sec}_I(v_{i_1}, \ldots, v_{i_k})$.

Definition 4. *Suppose that $k-1$ cheaters $P_{i_1}, \ldots, P_{i_{k-1}}$ possesses the list of shares $\mathbf{b} = (v_{i_1}, \ldots, v_{i_{k-1}})$. Let $\mathbf{b}' = (v'_{i_1}, \ldots, v'_{i_{k-1}}) \neq \mathbf{b}$ be a list of $k-1$ forged shares. Then we say that P_{i_k} is* cheated *by $\mathbf{b}'$ if*

$$\mathsf{Sec}_I(\mathbf{b}', v_{i_k}) \notin \{\mathsf{Sec}_I(\mathbf{b}, v_{i_k}), \perp\}, \tag{3}$$

where v_{i_k} denotes the share of P_{i_k}.

To define a secure secret sharing scheme clearly, we consider the following game.

1. $k-1$ cheaters and the target participant are fixed. That is, we fix $i_1, \ldots, i_{k-1}$ and i_k.
2. The dealer picks $s \in \mathcal{S}$ according to distribution S, and uses D to compute shares $v_1, \ldots, v_n$ for the n participants. v_i is given to P_i for $i \in \{1, \ldots, n\}$.
3. Let $\mathbf{b} = (v_{i_1}, \ldots, v_{i_{k-1}})$. The cheaters jointly use a *probabilistic* algorithm A to compute forged shares $\mathbf{b}' = (v'_{i_1}, \ldots, v'_{i_{k-1}})$ from $\mathbf{b}$.
4. The cheaters open the forged shares $\mathbf{b}'$. If P_{i_k} is cheated by $\mathbf{b}'$ (as defined above), then we say that the cheaters win the cheating game.

Definition 5. *We say that a (k, n) threshold secret sharing scheme D is a (k, n, δ)* secure secret sharing scheme *if*

$$\Pr(\textit{cheaters win}) \leq \delta \tag{4}$$

for any $k-1$ cheaters $P_{i_1}, \ldots, P_{i_{k-1}}$, any target P_{i_k} and any cheating strategy.

Ogata et al. derived a lower bound on $|\mathcal{V}_i|$ of (k, n, δ) secure secret sharing schemes as follows [4].

Proposition 1. *[4] In a (k, n, δ) secure secret sharing scheme,*

$$|\mathcal{V}_i| \geq \frac{|\mathcal{S}| - 1}{\delta} + 1 \tag{5}$$

for any i.

We say that a (k, n, δ) secure secret sharing scheme is optimal if the above equality is satisfied for all i.

5 Equivalence

In this section, we show an equivalence between (t, δ)-secure (1-round, n-channel) message transmission schemes and $(t+1, n, \delta)$ secure secret sharing schemes.

5.1 From Secret Sharing to Message Transmission

Theorem 1. *Suppose that $n \geq 2t+1$. If there exists a $(t+1, n, \delta)$ secure secret sharing scheme D for S, then there exists a (t, ϵ)-secure (1-round, n-channel) message transmission scheme $(\mathbf{Enc}, \mathbf{Dec})$ for the same S such that*

$$\epsilon = (\binom{n}{t+1} - \binom{n-t}{t+1})\delta$$

Further it holds that $\mathcal{X}_i = \mathcal{V}_i$ for $1 \leq i \leq n$.

Proof. We construct $(\mathbf{Enc}, \mathbf{Dec})$ from D as follows. **Enc** is the same as D. That is, on input $s \in \mathcal{S}$, **Enc** runs $D(s)$ to generate $(x_1, \cdots, x_n) = (v_1, \cdots, v_n)$.

Our **Dec** is constructed as follows. On input $(\hat{x}_1, \cdots, \hat{x}_n)$, **Dec** computes $\mathsf{Sec}_I(\hat{x}_{i_1}, \cdots, \hat{x}_{i_{t+1}})$ for all $I = (i_1, \cdots, i_{t+1})$, where I is a subset of $\{1, \cdots, n\}$. If there exists some $\hat{s} \in \mathcal{S}$ such that

$$\mathsf{Sec}_I(\hat{x}_{i_1}, \cdots, \hat{x}_{i_{t+1}}) = \hat{s} \text{ or } \perp$$

for all $I = (i_1, \cdots, i_{t+1})$, then **Dec** outputs $\hat{s}$. Otherwise, **Dec** outputs **failure**.

We prove that the conditions of Def. 1 are satisfied. The privacy condition holds from (A1) of Def. 2.

Next note that

$$n - t \geq (2t+1) - t = t + 1. \tag{6}$$

Therefore, the trivial reliability holds from (A2) of Def. 2. We next show the general reliability. From eq.(6), there exists a $J = \{j_1, \cdots, j_{t+1}\}$ such that $\hat{x}_{j_1} = x_{j_1}, \cdots, \hat{x}_{j_{t+1}} = x_{j_{t+1}}$. For this J, it holds that

$$\mathsf{Sec}_J(\hat{x}_{j_1}, \cdots, \hat{x}_{j_{t+1}}) = s$$

from (A2) of Def. 2, where s is the original secret. Therefore, **Dec** outputs **failure** if there exists some $I = (i_1, \cdots, i_{t+1}) \neq J$ such that

$$\mathsf{Sec}_I(\hat{x}_{i_1}, \cdots, \hat{x}_{i_{t+1}}) = s' \in \mathcal{S}$$

with $s' \neq s$. This means that if **Dec** does not output **failure**, then there is no such I. Hence **Dec** outputs $\hat{s} = s$.

Finally we show

$$\Pr(\textbf{Dec} \text{ outputs } \textbf{failure}) < \left(\binom{n}{t+1} - \binom{n-t}{t+1} \right) \delta.$$

For simplicity, suppose that an adversary $\mathbf{A}$ corrupts channels $1, \cdots, t$ and forges $\mathbf{b}' = (x'_1, \cdots, x'_t)$. Then the number of subsets I of size $t+1$ such that $I \cap \{1, \cdots, t\} \neq \emptyset$ is given by $\binom{n}{t+1} - \binom{n-t}{t+1}$. $\square$

5.2 From Message Transmission to Secret Sharing

Suppose that there exists a (t, δ)-secure (1-round, n-channel) message transmission scheme such that $n = 2t + 1$. Then $n - t = (2t + 1) - t = t + 1$. Hence from the trivial reliability condition, we can define a function F_I such that

$$F_I(\hat{x}_{i_1}, \cdots, \hat{x}_{i_{t+1}}) = s_I \text{ or } \perp \tag{7}$$

for each $(t+1)$-subset $I = (i_1, \cdots, i_{t+1}) \subset \{1, \cdots, n\}$, where $s_I \in \mathcal{S}$. We say that a (t, δ)-secure (1-round, n-channel) message transmission scheme with $n = 2t+1$ is canonical if

$$\textbf{Dec}(\hat{x}_1, \cdots, \hat{x}_n) = \begin{cases} \hat{s} & \text{if } F_I(\hat{x}_{i_1}, \cdots, \hat{x}_{i_{t+1}}) = \hat{s} \text{ or } \perp \text{ for each } (t+1)\text{-subset } I \\ \textbf{failure} & \text{otherwise} \end{cases}$$

Theorem 2. *If there exists a canonical (t, δ)-secure (1-round, n-channel) message transmission scheme $(\textbf{Enc}, \textbf{Dec})$ with $n = 2t + 1$ for S, then there exists a $(t+1, n, \delta)$ secure secret sharing scheme D for the same S. Further it holds that $\mathcal{X}_i = \mathcal{V}_i$ for $1 \leq i \leq n$.*

Proof. We construct D from $(\textbf{Enc}, \textbf{Dec})$ as $D = \textbf{Enc}$. That is, on input $s \in \mathcal{S}$, D runs $\textbf{Enc}(s)$ to generate $(v_1, \cdots, v_n) = (x_1, \cdots, x_n)$.

We prove that the conditions of Def. 2 are satisfied. (A1) holds from the privacy condition of Def. 1. (A2) holds from the trivial reliability since $n - t = 2t + 1 - t = t + 1$.

We finally show eq.(4). Suppose that eq.(4) does not hold in the $(t + 1, n, \delta)$ secure secret sharing scheme. Then there exist some $\{i_1, \cdots, i_t\}$, a target i_{t+1} and some cheating strategy such that

$$\mathsf{Sec}_I(\mathbf{b}', v_{i_k}) \notin \{\mathsf{Sec}_I(\mathbf{b}, v_{i_k}), \perp\}$$

with probability more than δ.

For simplicity, suppose that $\{i_1, \cdots, i_t\} = \{1, 2, \cdots, t\}$ and $i_{t+1} = t+1$. Now in the attack game of the (t, δ)-secure (1-round, n-channel) message transmission scheme, consider an adversary **A** which chooses the corresponding t channels $\{1, 2, \cdots, t\}$ and forges $x_1, \cdots, x_t$ to $x'_1, \cdots, x'_t$ according to the cheating strategy above. Then

$$\mathsf{Sec}_I(x'_1, \cdots, x'_t, x_{t+1}) = s' \tag{8}$$

with probability more than δ for some $s' \neq s$, where $I = \{1, \cdots, t, t+1\}$. On the other hand, we have

$$\mathsf{Sec}_J(x_{t+1}, \cdots, x_{2t+1}) = s \tag{9}$$

for $J = \{t+1, \cdots, 2t+1\}$. In this case, **Dec** outputs **failure** from our definition of *canonical*. Hence

$$\Pr(\textbf{Dec} \text{ outputs } \textbf{failure}) > \delta.$$

However, this is against eq.(2). Therefore, eq.(4) must hold. □

5.3 Discussion

We show that *canonical* is a natural property that (t, δ)-secure (1-round, n-channel) message transmission schemes with $n = 2t + 1$ should satisfy. First from the proof of Theorem 1, we have the following corollary.

Corollary 1. *In Theorem 1, if $n = 2t+1$, then the message transmission scheme is canonical.*

Next suppose that there exists a (t, δ)-secure (1-round, n-channel) message transmission scheme with $n = 2t+1$. Remember that the sender sends a ciphertext $(x_1, \cdots, x_{2t+1})$ for a secret s, and the receiver receives $\hat{X} = (\hat{x}_1, \cdots, \hat{x}_n)$. For a $(t+1)$-subset $I = (i_1, \cdots, i_{t+1}) \subset \{1, \cdots, n\}$, define

$$G(I, \hat{X}) = F_I(\hat{x}_{i_1}, \cdots, \hat{x}_{i_{t+1}}).$$

(See eq.(7) for F_I.)

Definition 6. *We say that a $(t+1)$-subset I is an acceptable (sub)set for $\hat{X}$ if $G(I, \hat{X}) \neq \perp$.*

In a canonical scheme, it is easy to see that **Dec** outputs **failure** if and only if there exist two acceptable $(t+1)$-subsets I and J such that $G(I, \hat{X}) \neq G(J, \hat{X})$. We will show that this is a natural property that (t, δ)-secure (1-round, n-channel) message transmission schemes with $n = 2t + 1$ should satisfy.

Consider an adversary **A** who corrupts channels $1, \cdots, t$, and replaces x_i to a random x'_i for $1 \leq i \leq t$.

1. We first show that
   - there are only two acceptable sets I and J, and $G(I, \hat{X}) \neq G(J, \hat{X})$

with nonzero probability. In this case, the receiver cannot see if $G(I, \hat{X}) = s$ or $G(J, \hat{X}) = s$. Hence he must output **failure** to satisfy the general reliability condition.
The proof is as follows. From the trivial reliability, it holds that

$$G(I, \hat{X}) = s \tag{10}$$

for $I = \{t+1, \cdots, 2t+1\}$. Further there exists another acceptable set $J \neq I$ such that $G(I, \hat{X}) \neq G(J, \hat{X})$ with nonzero probability. Because otherwise we have a perfectly t-secure (1-round, n-channel) message transmission scheme with $n = 2t+1$, which is a contradiction.
Finally, there exist no other acceptable sets with high probability because x_i' is chosen randomly for $1 \leq i \leq t$.

2. Next we show that there exists a case such that the majority vote does not work. That is, we show that there exist acceptable sets I and $J_1, \cdots, J_{\binom{2t}{t+1}}$ such that
   - $G(I, \hat{X}) = s$ and
   - $G(J_1, \hat{X}) = \cdots, G(J_{\binom{2t}{t+1}}, \hat{X}) = s' \neq s$

   with nonzero probability. In this case, the receiver must output **failure** too to satisfy the general reliability condition.
   The proof is as follows. From the privacy condition, we have no information on s from $(x_{t+1}, \cdots, x_{2t})$. Therefore for $s' \neq s$, it holds that

$$\Pr[S = s', X_{t+1} = x_{t+1}, \cdots, X_{2t} = x_{2t}] > 0.$$

   Hence there exist some $b_1, \cdots, b_t, c_{2t+1}$ such that

$$\Pr[S = s', X_1 = b_1, \cdots, X_t = b_t, X_{t+1} = x_{t+1}, \cdots, X_{2t} = x_{2t}, X_{2t+1} = c_{2t+1}] > 0. \tag{11}$$

   Further it holds that $x_i' = b_i$ for $1 \leq i \leq t$ with nonzero probability because the adversary **A** chooses x_i' randomly. In this case, we have

$$\hat{x}_1 = b_1, \cdots, \hat{x}_t = b_t,\ \hat{x}_{t+1} = x_{t+1}, \cdots, \hat{x}_{2t} = x_{2t},\ \hat{x}_{2t+1} = x_{2t+1}.$$

   Therefore from eq.(11), for any $(t+1)$-subset $J \subset \{1, \cdots, 2t\}$, we obtain that

$$G(J, \hat{X}) = s'.$$

   The number of such J is $\binom{2t}{t+1}$. Finally, it is clear that $G(I, \hat{X}) = s$ for $I = \{t+1, \cdots, 2t+1\}$.

So the scheme must be canonical in the above two cases. Hence we consider that *canonical* is a natural property for $n = 2t+1$.

6 Lower Bound

In this section, we derive a lower bound on $|\mathcal{X}_i|$ of (t, δ)-secure (1-round, n-channel) message transmission schemes with $n = 2t+1$ by using our equivalence. Indeed, we obtain the following bound immediately from Proposition 1 and Theorem 2.

Corollary 2. *In a canonical (t, δ)-secure (1-round, n-channel) message transmission scheme with $n = 2t + 1$, it holds that*

$$|\mathcal{X}_i| \geq \frac{|\mathcal{S}| - 1}{\delta} + 1 \tag{12}$$

for any i.

7 Near Optimum Almost Secure MT Scheme

Ogata et al. showed a construction of optimum (k, n, δ) secure secret sharing schemes by using "difference sets" [4].

7.1 Optimum Robust Secret Sharing Scheme

Definition 7. *[3, p.397] A* planar difference set *modulo $N = \ell(\ell - 1) + 1$ is a set $B = \{d_0, d_1, \ldots, d_{\ell-1}\} \subseteq \mathbb{Z}_N$ with the property that the $\ell(\ell - 1)$ differences $d_i - d_j$ $(d_i \neq d_j)$, when reduced modulo N, are exactly the numbers $1, 2, \ldots, N - 1$ in some order.*

For example, $\{d_0 = 0, d_1 = 1, d_2 = 3\}$ is a planar difference set modulo 7 with $\ell = 3$. Indeed, the differences modulo 7 are

$$1 - 0 = 1,\ 3 - 0 = 3,\ 3 - 1 = 2,\ 0 - 1 = 6,\ 0 - 3 = 4,\ 1 - 3 = 5.$$

Proposition 2. *[3, p.398, Theorem 22] Let Π be a projective plane $PG(2, q)$. A point in Π can be represented as $(\beta_1, \beta_2, \beta_3) \in (\mathbb{F}_q)^3$, or $\alpha^i \in \mathbb{F}_{q^3}$ for some i, where α is a generator of $\mathbb{F}_{q^3}$. If $\ell = q + 1$ points $\alpha^{d_0}, \ldots, \alpha^{d_{\ell-1}}$ are the points on a line in Π, then $\{d_0, \ldots, d_{\ell-1}\}$ is a planar difference set modulo $q^2 + q + 1$.*

Let $\{d_0, \ldots, d_q\}$ be a planar difference set modulo $p = q^2 + q + 1$. Then a (k, n, δ) secure secret sharing scheme is obtained by applying Shamir's (k, n)-threshold secret sharing scheme to $\mathcal{S} = \{d_0, \ldots, d_q\}$ over $GF(p)$, where the secret s is uniformly distributed over $\mathcal{S}$ and $\delta = 1/(q + 1)$. In the reconstructoin phase, an honest participant outputs a reconstructed secret s' if $s' \in \mathcal{S}$, and $\perp$ otherwise.

Proposition 3. *[4, Corollary 4.5] Let q be a prime power that makes $q^2 + q + 1$ a prime. Then, there exists a (k, n, δ) secure secret sharing scheme for a uniform distribution over $\mathcal{S}$ which meets the bound (5) such that $|\mathcal{S}| = q + 1, \delta = 1/(q + 1)$ and $n < q^2 + q + 1$.*

From Proposition 1, this construction is optimum.

7.2 Near Optimum Almost Secure MT Scheme

From the above proposition, Theorem 1 and Corollary 1, we can obtain the following construction of (t, ϵ)-secure (1-round, n-channel) message transmission schemes.

Corollary 3. *Let q be a prime power that makes $q^2 + q + 1$ a prime. Then, there exists a (t, ϵ)-secure (1-round, n-channel) message transmission scheme with $n \geq 2t + 1$ for a uniform distribution over $\mathcal{S}$ such that $|\mathcal{S}| = q + 1, \delta = 1/(q + 1)$, $2t + 1 \leq n < q^2 + q + 1$ and*

$$|\mathcal{X}_i| = \frac{|\mathcal{S}| - 1}{\delta} + 1,$$

where

$$\epsilon = (\binom{n}{t+1} - \binom{n-t}{t+1})\delta.$$

Further if $n = 2t + 1$, the message transmission scheme is canonical.

Our (t, ϵ)-secure (1-round, n-channel) message transmission scheme is described as follows. Let $\{d_0, \ldots, d_q\}$ be a planar difference set modulo $p = q^2 + q + 1$. We assume that a message s is uniformly distributed over $\{0, 1, \cdots, q\}$.

1. For a message $s \in \{0, 1, \ldots, q\}$, let $y = d_s$. The sender applies Shamir's $(t + 1, n)$-threshold secret sharing scheme to the secret $y = d_s$ over $GF(p)$ to obtain the shares $(v_1, \cdots, v_n)$. She then sends $x_i = v_i$ to the receiver through the ith channel for $i = 1, \cdots, n$.
2. Suppose that the receiver received $(\hat{x}_1, \cdots, \hat{x}_n)$. He first reconstructs the secret y_I by applying Lagrange formula to $(\hat{x}_{i_1}, \cdots, \hat{x}_{i_{t+1}})$ for each subset $I = (i_1, \cdots, i_{t+1})$ of $\{1, \cdots, n\}$. If there exists some $\hat{s} \in \{0, 1, \ldots, q\}$ such that for all subset I,

$$y_I = d_{\hat{s}} \text{ or } y_I \notin \{d_0, \ldots, d_q\},$$

then he outputs $\hat{s}$. Otherwise the receiver outputs **failure**.

7.3 Generalization

Ogata et al. also showed another construction of optimum (k, n, δ) secure secret sharing schemes by using general "difference sets" [4].

Proposition 4. *[4, Corollary 4.5] For a positive integer u such that $4u - 1$ is a prime power, there exists a (k, n, δ) secure secret sharing scheme which meets the equality of our bound (5), such that $|\mathcal{S}| = 2u - 1, \delta = (u - 1)/(2u - 1), n < 4u - 1$.*

From the above proposition, Theorem 1 and Corollary 1, we can obtain another construction of (t, ϵ)-secure (1-round, n-channel) message transmission schemes as follows.

Corollary 4. *[4, Corollary 4.5] For a positive integer u such that $4u-1$ is a prime power, there exists (t,ϵ)-secure (1-round, n-channel) message transmission scheme with $n \geq 2t+1$ for a uniform distribution over $\mathcal{S}$ such that $|\mathcal{S}| = 2u-1, \delta = (u-1)/(2u-1), n < 4u-1$ and*

$$|\mathcal{X}_i| = \frac{|\mathcal{S}|-1}{\delta} + 1,$$

where

$$\epsilon = (\binom{n}{t+1} - \binom{n-t}{t+1})\delta.$$

Further if $n = 2t+1$, the message transmission scheme is canonical.

In these constructions, there is a gap of $\log_2(\binom{n}{t+1} - \binom{n-t}{t+1})$ bits from our lower bound of Corollary 2. This gap is, however, small enough for small t.

Our results imply that $n \geq 2t+1$ is necessary and sufficient for (t,ϵ)-secure (1-round, n-channel) message transmission schemes.

Theorem 3. *(t,ϵ)-secure (1-round, n-channel) message transmission schemes exist if and only if $n \geq 2t+1$.*

Proof. It is enough to prove that there exist no (t,ϵ)-secure (1-round, n-channel) message transmission schemes for $n \leq 2t$. Suppose that there exists a (t,ϵ)-secure (1-round, n-channel) message transmission scheme with $n \leq 2t$. Consider an adversary $\mathbf{A}$ who replaces $x_1, \cdots, x_t$ with null strings. Then the receiver receives $n-t$ messages $x_{t+1}, \cdots, x_n$, where $n-t \leq 2t-t = t$. Then from the privacy condition, the receiver obtains no information on s. On the other hand, from the trivial reliability condition, he must output s. This is a contradiction. □

8 Conclusion

In this paper, we first summed up a number of flaw of the previous almost secure (1-round, n-channel) message transmission scheme for $n = 2t+1$ which was presented at Crypto 2004. We next showed an equivalence between (t,δ)-secure (1-round, n-channel) message transmission scheme for $n = 2t+1$ and secret sharing schemes with cheaters. By using our equivalence, we derived a lower bound on the communication complexity. Finally, we presented a near optimum scheme which meets our bound approximately. This is the first construction of provably secure (t,δ)-secure (1-round, n-channel) message transmission schemes for $n = 2t+1$.

Our results imply that $n \geq 2t+1$ is necessary and sufficient for (t,ϵ)-secure (1-round, n-channel) message transmission schemes.

References

1. S.Agarwal, R.Cramer, and R. de Haan: Asymptotically Optimal Two-Round Perfectly Secure Message Transmission CRYPTO 2006: 394–408
2. D.Dolev, C.Dwork, O.Waarts, M.Yung: Perfectly Secure Message Transmission. J. ACM 40(1): 17–47 (1993)
3. F.J. MacWilliams and N.J.A. Sloanem *The Theory of Error-correcting Codes*, North-Holland, 1981.
4. W.Ogata, K.Kurosawa, D.Stinson: Optimum Secret Sharing Scheme Secure against Cheating. SIAM J. Discrete Math. 20(1): 79–95 (2006)
5. H.Md.Sayeed and H.Abu-Amara: Efficient Perfectly Secure Message Transmission in Synchronous Networks. Inf. Comput. 126(1): 53-61 (1996)
6. K. Srinathan, A.Narayanan, C. Pandu Rangan: Optimal Perfectly Secure Message Transmission. CRYPTO 2004: 545–561
7. M. Tompa and H. Woll, How to share a secret with cheaters, *Journal of Cryptology* **1** (1988), 133–138.