Truly Efficient 2-Round Perfectly Secure Message Transmission Scheme

Kaoru Kurosawa[1] and Kazuhiro Suzuki[2]

[1] Department of Computer and Information Sciences, Ibaraki University
kurosawa@mx.ibaraki.ac.jp
[2] Venture Business Laboratory, Ibaraki University, Hitachi, Ibaraki 316-8511, Japan
tutetuti@dream.com

Abstract. In the model of perfectly secure message transmission schemes (PSMTs), there are n channels between a sender and a receiver. An infinitely powerful adversary **A** may corrupt (observe and forge) the messages sent through t out of n channels. The sender wishes to send a secret s to the receiver perfectly privately and perfectly reliably without sharing any key with the receiver.
In this paper, we show the first 2-round PSMT for $n = 2t + 1$ such that not only the transmission rate is $O(n)$ but also the computational costs of the sender and the receiver are both polynomial in n. This means that we solve the open problem raised by Agarwal, Cramer and de Haan at CRYPTO 2006.
The main novelty of our approach is to introduce a notion of *pseudo-basis* to the coding theory. It will be an independent interest for coding theory, too.

Keywords: Perfectly secure message transmission, information theoretic security, efficiency

1 Introduction

In the model of (r-round, n-channel) message transmission schemes [2], there are n channels between a sender and a receiver. An infinitely powerful adversary **A** may corrupt (observe and forge) the messages sent through t out of n channels. The sender wishes to send a secret s to the receiver in r-rounds without sharing any key with the receiver.

We say that a message transmission scheme is perfectly secure if it satisfies perfect privacy and perfect reliability. The perfect privacy means that the adversary **A** learns no information on s, and the perfect reliability means that the receiver can output $\hat{s} = s$ correctly.

For $r = 1$, Dolev et al. showed that there exists a 1-round perfectly secure message transmission scheme (PSMT) if and only if $n \geq 3t + 1$ [2]. They also showed an efficient 1-round PSMT [2].

For $r \geq 2$, it is known that there exists a 2-round PSMT if and only if $n \geq 2t + 1$ [2]. However, it is very difficult to construct an efficient scheme for

$n = 2t + 1$. Dolev et al. [2] showed a 3-round PSMT such that the transmission rate is $O(n^5)$, where the transmission rate is defined as

$$\frac{\text{the total number of bits transmitted}}{\text{the size of the secrets}}.$$

Sayeed et al. [7] showed a 2-round PSMT such that the transmission rate is $O(n^3)$.

Recently, Srinathan et al. showed that n is a lower bound on the transmission rate of 2-round PSMT [8]. Then Agarwal, Cramer and de Haan [1] showed a 2-round PSMT such that the transmission rate is $O(n)$ at CRYPTO 2006 based on the work of Srinathan et al. [8] [3]. However, the communication complexity is exponential because the sender must broadcast consistency check vectors of size [4]

$$w = \binom{n-1}{t+1} = \binom{2t}{t+1}.$$

In other words, Agarwal et al. [1] achieved the transmission rate of $O(n)$ by sending exponentially many secrets. Therefore, the computational costs of the sender and the receiver are both exponential. Indeed, the authors wrote [1, Sec.6] that:

"We do not know whether a similar protocol can exist where sender and receiver restricted to polynomial time (in terms of the number of channels n) only".

In this paper, we solve this open problem. That is, we show the first 2-round PSMT for $n = 2t + 1$ such that not only the transmission rate is $O(n)$ but also the computational costs of the sender and the receiver are both polynomial in n.

Table 1. 2-Round PSMT for $n = 2t + 1$

	Trans. rate	com. complexity	Receiver	Sender
Agarwal et al. [1]	$O(n)$	exponential	exponential	exponential
This paper	$O(n)$	$O(n^3)$	poly	poly

The main novelty of our approach is to introduce a notion of *pseudo-basis* to the coding theory. Let $\mathcal{C}$ be a linear code of length n over a finite field F with the minimum Hamming distance $d = t+1$. Consider a message transmission scheme such that the sender chooses a codeword $X_i = (x_{i1}, \cdots, x_{in})$ of $\mathcal{C}$ randomly and

[3] Srinathan et al. claimed that they constructed a 2-round PSMT such that the transmission rate is $O(n)$ in [8]. However, Agarwal et al. pointed out that it has a flaw in [1].

[4] Indeed, in [1, page 407], it is written that "at most $O(w)$ indices and field elements are broadcast ....", where w is defined in [1, page 403] as shown above.

sends x_{ij} through channel j for $j = 1, \cdots, n$. Note that the receiver can detect t errors, but cannot correct them because $d = t + 1$.

If the sender sends many codewords, however, then we can do something better. Suppose that the sender sent X_i as shown above, and the receiver received $Y_i = X_i + E_i$ for $i = 1, \cdots, m$, where E_i is an error vector caused by the adversary. We now observe that the dimension of the space $\mathcal{E}$ spanned by the error vectors $E_1, \cdots, E_m$ is at most t because the adversary corrupts at most t channels. Suppose that $\{E_{i_1}, \cdots, E_{i_k}\}$ is such a basis, where $k \leq t$. For the same indices, we say that $\mathcal{B} = \{Y_{i_1}, \cdots, Y_{i_k}\}$ is a *pseudo-basis* of $\mathcal{Y} = \{Y_1, \cdots, Y_m\}$. We then show that a receiver can find a pseudo-basis $\mathcal{B}$ of $\mathcal{Y}$ in polynomial time.

By using this algorithm, we first show a 3-round PSMT for $n = 2t + 1$ such that the transmission rate is $O(n)$ and the computational cost of the sender and the receiver are both polynomial in n. (See Fig.4.) Then combining the technique of [8, 1], we show a 2-round PSMT such that not only the transmission rate is $O(n)$ but also the computational cost of the sender and the receiver are both polynomial in n.

(Remark) Recently, Fitzi et al. showed an efficient 2-round PSMT for $n \geq (2+\epsilon)t$ for any constant $\epsilon > 0$ [4], but not for $n = 2t + 1$.

2 Main Idea

Suppose that there are n channels between the sender and the receiver, and an adversary may corrupt t out of n channels. We use F to denote $GF(p)$, where p is a prime such that $p > n$. [5]

Let $\mathcal{C}$ be a linear code of length n such that a codeword is $X = (f(1), \cdots, f(n))$, where $f(x)$ is a polynomial over F with $\deg f(x) \leq t$.

2.1 Difference from Random t Errors

Consider a message transmission scheme such that the sender chooses a codeword $X = (f(1), \cdots, f(n))$ of $\mathcal{C}$ randomly, and sends $f(i)$ through channel i for $i = 1, \cdots, n$. Then the adversary learns no information on $f(0)$ even if she observes t channels because $\deg f(x) \leq t$. Thus perfect privacy is satisfied.

If $n = 3t+1$, then the minimum Hamming distance of $\mathcal{C}$ is $d = n-t = 2t+1$. Hence the receiver can correct t errors caused by the adversary. Thus perfect reliability is also satisfied. Therefore we can obtain a 1-round PSMT easily.

If $n = 2t + 1$, however, the minimum Hamming distance of $\mathcal{C}$ is $d = n - t = t + 1$. Hence the receiver can only detect t errors, but cannot correct them. This is the main reason why the construction of PSMT for $n = 2t + 1$ is difficult.

What is a difference between usual error correction and PSMTs ? If the sender sends a single codeword $X \in \mathcal{C}$ only, then the adversary causes t errors

[5] We adopt $GF(p)$ only to make the presentation simpler, where the elements are denoted by $0, 1, 2, \cdots$. But in general, our results hold for any finite field F whose size is larger than n.

randomly. Hence there is no difference. If the sender sends many codewords $X_1, \cdots, X_m \in \mathcal{C}$, however, the errors are not totally random. This is because the errors always occur at the same t (or less) places !

To see this more precisely, suppose that the receiver received

$$Y_i = X_i + E_i, \tag{1}$$

where $E_i = (e_{i1}, \cdots, e_{in})$ is an error vector caused by the adversary. Define

$$\mathit{support}(E_i) = \{j \mid e_{ij} \neq 0\}.$$

Then there exist some t-subset $\{j_1, \cdots, j_t\}$ of n channels such that each error vector E_i satisfies

$$\mathit{support}(E_i) \subseteq \{j_1, \cdots, j_t\}, \tag{2}$$

where $\{j_1, \cdots, j_t\}$ is the set of channels that the adversary forged.

This means that the space $\mathcal{E}$ spanned by $E_1, \cdots, E_m$ has dimension at most t. We will exploit this fact extensively.

2.2 Pseudo-Basis and Pseudo-Dimension

For $i = 1, \cdots, m$, suppose that the receiver received Y_i such that

$$Y_i = X_i + E_i, \tag{3}$$

where $X_i \in \mathcal{C}$ is a codeword that the sender sent and E_i is the error vector caused by the adversary. We say that $\{E_1, \cdots, E_m\}$ is the real error-vector set of $\mathcal{Y} = \{Y_1, \cdots, Y_m\}$. We also say that $\mathcal{E}$ is the real error-vector space if it is spanned by the real error-vector set $\{E_1, \cdots, E_m\}$.

For two vectors Y and E, we write

$$Y = E \bmod \mathcal{C}$$

if $Y - E \in \mathcal{C}$. In particular, eq.(3) means that

$$Y_i = E_i \bmod \mathcal{C}.$$

Let $\mathcal{Y} = \{Y_1, \cdots, Y_m\}$ be a set of received words. We say that $\{E_1, \cdots, E_m\}$ is an admissible error-vector set of $\mathcal{Y}$ if each E_i satisfies $Y_i = X_i + E_i$ for some codeword X_i, and

$$|\bigcup_i \mathit{support}(E_i)| \leq t \tag{4}$$

We say that $\mathcal{E}$ is an admissible error-vector space of $\mathcal{Y}$ if it is spanned by an admissible error-vector set $\{E_1, \cdots, E_m\}$.

For given $\mathcal{Y}$, an admissible error-vector set $\{E_1, \cdots, E_m\}$ may not be unique. Nevertheless, the following results holds for any admisible error-vector set.

We begin with a definition of *linearly pseudo-express*.

Definition 1. *We say that $Y \in \mathcal{Y}$ is linearly pseudo-expressed by $\{B_1, \cdots, B_k\}$ if there exists some $\alpha = (a_1 \cdots, a_k)$ such that*

$$Y = a_1 B_1 + \cdots + a_k B_k \bmod \mathcal{C}.$$

Lemma 1. *Let $\{E_1, \cdots, E_m\}$ be an admissible error-vector set of $\mathcal{Y}$. Then E_i is linearly expressed by $\{E_{j1}, \cdots, E_{jk}\}$ if and only if Y_i is linearly pseudo-expressed by $\{Y_{j1}, \cdots, Y_{jk}\}$.*

(Proof) Let $Y_i = X_i + E_i$ for each i, where X_i is a codeword. Suppose that

$$E_i = a_1 E_{j1} + \cdots + a_k E_{jk}$$

for some $a_1, \cdots, a_k$. Then in mod$\mathcal{C}$,

$$\begin{aligned} & Y_i - (a_1 Y_{j1} + \cdots + a_k Y_{jk}) \\ &= (X_i + E_i) - a_1(X_{j1} + E_{j1}) - \cdots - a_k(X_{j1} + E_{j1}) \\ &= E_i - a_1 E_{j1} - \cdots - a_k E_{jk} \\ &= 0 \end{aligned}$$

Hence Y_i is linearly pseudo-expressed by $\{Y_{j1}, \cdots, Y_{jk}\}$ if E_i is linearly expressed by $\{E_{j1}, \cdots, E_{jk}\}$. Next suppose that

$$Y_i - (a_1 Y_{j1} + \cdots + a_k Y_{jk}) = 0 \bmod \mathcal{C}.$$

Then in mod$\mathcal{C}$,

$$\begin{aligned} 0 &= Y_i - (a_1 Y_{j1} + \cdots + a_k Y_{jk}) \\ &= (X_i + E_i) - a_1(X_{j1} + E_{j1}) - \cdots - a_k(X_{j1} + E_{j1}) \\ &= E_i - a_1 E_{j1} - \cdots - a_k E_{jk} \end{aligned}$$

Hence

$$E_i - a_1 E_{j1} - \cdots - a_k E_{jk} \in \mathcal{C}.$$

From eq.(4), the Hamming weight of the left hand side is at most t while the minimum Hamming weight of $\mathcal{C}$ is $t+1$. Therefore, $E_i - a_1 E_{j1} - \cdots - a_k E_{jk}$ is a zero-vector. Hence we obtain that

$$E_i = a_1 E_{j1} + \cdots + a_k E_{jk}.$$

This means that if Y_i is linearly pseudo-expressed by $\{Y_{j1}, \cdots, Y_{jk}\}$, ten E_i is linearly expressed by $\{E_{j1}, \cdots, E_{jk}\}$.

Q.E.D.

We next define *pseudo-span*.

Definition 2. *We say that $\{Y_{j1}, \cdots, Y_{jk}\} \subset \mathcal{Y}$ pseudo-spans $\mathcal{Y}$ if each $Y_i \in \mathcal{Y}$ can be written as*

$$Y_i = a_1 Y_{j1} + \cdots + a_k Y_{jk} \bmod \mathcal{C}$$

for some $a_i \in \mathsf{F}$.

We then define a *pseudo-basis* and the *pseudo-dimension* of $\mathcal{Y}$.

Definition 3. – *We say that* $\{Y_{j1}, \cdots, Y_{jk}\}$ *is a pseudo-basis of* $\mathcal{Y}$ *if it is a minimum set which pseudo-spans* $\mathcal{Y}$.
– *Suppose that* $\{Y_{j1}, \cdots, Y_{jk}\}$ *is a pseudo-basis of* $\mathcal{Y}$, *where* $k = |\{Y_{j1}, \cdots, Y_{jk}\}|$. *Then we say that* $\mathcal{Y}$ *has the pseudo-dimension* k.

Theorem 1. *Let* $\{E_1, \cdots, E_m\}$ *be an admissible error-vector set of* $\mathcal{Y}$. *Then* $\mathcal{B}_e = \{E_{j1}, \cdots, E_{jk}\}$ *is a basis of the admisible error-vector space* $\mathcal{E}$ *if and only if* $\mathcal{B}_y = \{Y_{j1}, \cdots, Y_{jk}\}$ *is a pseudo-basis of* $\mathcal{Y}$. *(Note that* $\mathcal{B}_e$ *and* $\mathcal{B}_y$ *have the same indices.)*

In particular, the pseudo-dimension of $\mathcal{Y}$ *is equal to the dimension of* $\mathcal{E}$.

(Proof) Suppose that $\mathcal{B}_e$ is a basis of $\mathcal{E}$. That is, $\mathcal{B}_e$ is a minimum set which spans $\mathcal{E}$. Since $\mathcal{B}_e$ spans $\mathcal{E}$, $\mathcal{B}_y$ pseudo-spans $\mathcal{Y}$ from Lemma 1.

Suppose that $\mathcal{B}_y$ is not minimum. That is, suppose that there exists a smaller subset of $\mathcal{Y}$ which pseudo-spans $\mathcal{Y}$. Then the corresponding subset of $\{E_1, \cdots, E_m\}$ also spans $\mathcal{E}$ from Lemma 1. However, this contradcits to the fact that $\mathcal{B}_e$ is minimum. Hence $\mathcal{B}_y$ is minimum. This shows that $\mathcal{B}_y$ is a pseudo-basis of $\mathcal{Y}$.

Similarly, $\mathcal{B}_e$ is a basis of $\mathcal{E}$ if $\mathcal{B}_y$ is a pseudo-basis of $\mathcal{Y}$.

Hnece the pseudo-dimension of $\mathcal{Y}$ is equal to the dimension of $\mathcal{E}$.

Q.E.D.

Since the real error-vector set is an admisible error-vector set, we obtain the following corollary from Theorem 1.

Corollary 1. *Let* $\{E_1, \cdots, E_m\}$ *be the real error-vector set of* $\mathcal{Y}$. *If* $\mathcal{B}_y = \{Y_{j1}, \cdots, Y_{jk}\}$ *is a pseudo-basis of* $\mathcal{Y}$, *then* $\mathcal{B}_e = \{E_{j1}, \cdots, E_{jk}\}$ *is a basis of the real error-vector space.*

Let $\{E_1, \cdots, E_m\}$ be the real error-vector set of $\mathcal{Y}$, and let $\{X_1, \cdots, X_m\}$ be the codewords which the sender sent. Define

$$\mathsf{FORGED} = \bigcup_{i=1}^{m} support(E_i).$$

That is, FORGED is the set of all channels that the adversary forged. Suppose that $\mathcal{B}_y = \{Y_{j1}, \cdots, Y_{jk}\}$ is a pseudo-basis of $\mathcal{Y}$. Then from Corollary 1, it holds that

$$\mathsf{FORGED} = \bigcup_{i=1}^{m} support(E_i) \tag{5}$$

$$= \bigcup_{i=1}^{k} support(E_{ji}) \tag{6}$$

$$= \bigcup_{i=1}^{k} support(Y_{ji} - X_{ji}), \tag{7}$$

where eq.(5) comes from the definition of FORGED, eq.(6) holds because $\{E_{j1}, \cdots, E_{jk}\}$ is a basis and eq.(7) holds because $Y_{ji} = X_{ji} + E_{ji}$.

The following theorem is clear since the adversary forges at most t channels.

Theorem 2. *The pseudo-dimension of $\mathcal{Y}$ is at most t.*

(Proof) The dimension of the real error-vector space is at most t because the adversary forges at most t channels. Hence from Theorem 1, The pseudo-dimension of $\mathcal{Y}$ is at most t.

Q.E.D.

2.3 How to Find Pseudo-Basis

In this subsection, we show a polynomial time algorithm which finds the pseudo-dimension k and a pseudo-basis $\mathcal{B} = \{B_1, \cdots, B_k\}$ of $\mathcal{Y} = \{Y_1, \cdots, Y_m\}$.

Theorem 1 shows that $\mathcal{B}_y = \{Y_{j1}, \cdots, Y_{jk}\}$ is a pseudo-basis of $\mathcal{Y}$ if and only if $\mathcal{B}_e = \{E_{j1}, \cdots, E_{jk}\}$ is a basis of an admisible error-vector space $\mathcal{E}$, where $\{E_1, \cdots, E_m\}$ is the admissible error-vector set. On the other hand, we can find a basis of a vector space easily by using a greedy algorithm as shown in Fig.1. This means that a pseudo-basis $\mathcal{B}$ can be found by using a similar greedy algorithm.

Fig. 1. How to Find a Basis of $\mathcal{E}$

Input: $\{E_1, \cdots, E_m\}$.

1. Let $i = 1$ and $\mathcal{B} = \emptyset$.
2. While $i \leq m$ and $|\mathcal{B}| < t$, do:
(a) Check if Y_i is linearly expressed by $\mathcal{B}$.
If NO, then add E_i to $\mathcal{B}$.
(b) Let $i \leftarrow i + 1$.
3. Output $\mathcal{B}$ as a basis and $k = |\mathcal{B}|$ as the dimension.

Remember that Y is linearly pseudo-expressed by $\{B_1, \cdots, B_k\}$ if there exists some $\alpha = (a_1 \cdots, a_k)$ such that

$$X(\alpha) = Y - (a_1 B_1 + \cdots + a_k B_k) \in \mathcal{C} \tag{8}$$

Let

$$X(\alpha) = (x_1(\alpha), \cdots, x_n(\alpha)).$$

Then it is clear that $x_j(\alpha)$ is a linear expression of $(a_1 \cdots, a_k)$ from eq.(8).

In Fig.2, we show a polynomial time algorithm which checks if Y is linearly pseudo-expressed by $\{B_1, \cdots, B_k\}$. It is easy to see that each coefficient of $f_\alpha(x)$ is a linear expression of $(a_1 \cdots, a_k)$. Hence at step 3, $f_\alpha(j) = x_j(\alpha)$ is a linear

equation on $(a_1 \cdots, a_k)$. It is now clear that the algorithm of Fig.2 outputs YES if and only if $X(\alpha) \in \mathcal{C}$ for some α. Hence it outputs YES if and only if Y is linearly pseudo-expressed by $\{B_1, \cdots, B_k\}$.

Fig. 2. How to Check if Y is linearly pseudo-expressed by $\mathcal{B}$

Input: Y and $\mathcal{B} = \{B_1, \cdots, B_k\}$.

1. Construct $X(\alpha) = (x_1(\alpha), \cdots, x_n(\alpha))$ of eq.(8).
2. Construct a polynomial $f_\alpha(x)$ with $\deg f_\alpha(x) \leq t$ such that
   $f_\alpha(i) = x_i(\alpha)$
   for $i = 1, \cdots, t+1$ by using Lagrange formula.
3. Output YES if the following set of linear equations has a solution α.
   $f_\alpha(t+2) = x_{t+2}(\alpha)$,
   $\vdots$
   $f_\alpha(n) = x_n(\alpha)$.
   Otherwise output NO.

In Fig.3, we show a polynomial time algorithm which finds the pseudo-dimension k and a pseudo-basis $\mathcal{B} = \{B_1, \cdots, B_k\}$ of $\mathcal{Y} = \{Y_1, \cdots, Y_m\}$. Note that Fig.3 is almost the same as Fig.1. Indeed, it is obtained by replacing E_i of Fig.1 with Y_i. We call the algorithm of Fig.1 the real-basis finding algorithm, and call the algorithm of Fig.3 the pseudo-basis finding algorithm

Let $\{E_1, \cdots, E_m\}$ be an admissble error-vector set of $\mathcal{Y}$, and let $\mathcal{E}$ be the vector space spanned by $\{E_1, \cdots, E_m\}$. Supppose that we apply the real-basis finding algorithm to $\{E_1, \cdots, E_m\}$, and apply the pseudo-basis finding algorithm to $\mathcal{Y} = \{Y_1, \cdots, Y_m\}$. The real-basis finding algorithm outputs a basis $\mathcal{B}'$ of $\mathcal{E}$. We will show that the pseudo-basis finding algorithm outputs a pseudo-basis $\mathcal{B}$ of $\mathcal{Y}$.

Step 2(a) is the only difference between the two algorithms. Further from Lemma 1, Y_i is added to $\mathcal{B}$ at step 2(a) if and only if E_i is added to $\mathcal{B}'$ at step 2(a). Hence the pseudo-basis finding algorithm behaves in the same way as the real-basis finding algorithm. In particular, if the real-basis finding algorithm outputs $\mathcal{B}' = \{E_{j1}, \cdots, E_{jk}\}$, then the pseudo-basis finding algorithm outputs $\mathcal{B} = \{Y_{j1}, \cdots, Y_{jk}\}$. Therefore $\mathcal{B}$ is a pseudo-basis of $\mathcal{Y}$ from Theorem 1 because $\mathcal{B}'$ is a basis of $\mathcal{E}$.

2.4 Broadcast

We say that a sender (receiver) broadcasts x if it she sends x over all n channels. Since the adversary corrupts at most t out of $n = 2t + 1$ channels, the receiver (sender) receives x correctly from at least $t+1$ channels. Therefore, the receiver (sender) can accept x correctly by taking the majority vote.

Fig. 3. How to Find a Pseudo-Basis $\mathcal{B}$ of $\mathcal{Y}$

Input: $\mathcal{Y} = \{Y_1, \cdots, Y_m\}$.

1. Let $i = 1$ and $\mathcal{B} = \emptyset$.
2. While $i \leq m$ and $|\mathcal{B}| < t$, do:
(a) Check if Y_i is linearly pseudo-expressed by $\mathcal{B}$ by using Fig.2.
If NO, then add Y_i to $\mathcal{B}$.
(b) Let $i \leftarrow i + 1$.
3. Output $\mathcal{B}$ as a pseudo-basis and $k = |\mathcal{B}|$ as the pseudo-dimension.

2.5 How to Apply to 3-Round PSMT

We now present an efficient 3-round PSMT for $n = 2t + 1$ in Fig.4.

Fig. 4. Our 3-round PSMT for $n = 2t + 1$

The sender wishes to send $\ell = nt$ secrets $s_1, \cdots, s_\ell \in \mathsf{F}$ to the receiver.

1. The sender sends a random codeword $X_i = (f_i(1), \cdots, f_i(n))$,
and the receiver receives $Y_i = X_i + E_i$ for $i = 1, \cdots, \ell + t$,
where $\deg f_i(x) \leq t$ and E_i is the error vector caused by the adversary.
2. The receiver finds a pseudo-basis $\mathcal{B} = \{Y_{j1}, \cdots, Y_{jk}\}$, where $k \leq t$,
by using the algorithm of Fig.3.
He then broadcasts $\mathcal{B}$ and $\Lambda_{\mathcal{B}} = \{j_1, \cdots, j_k\}$.
3. The sender constructs FORGED of eq.(7) from $\{E_j = Y_j - X_j \mid j \in \Lambda_{\mathcal{B}}\}$,
encrypts $s_1, \cdots, s_\ell$ by using $\{f_i(0) \mid i \notin \Lambda_{\mathcal{B}}\}$ as the key of one-time pad,
and then broadcasts FORGED and the ciphertexts.
4. The receiver reconstructs $f_i(x)$ by ignoring all channels of FORGED,
and applying Lagrange formula to the remaining elements of Y_i.
He then decrypts the ciphertexts by using $\{f_i(0) \mid i \notin \Lambda_{\mathcal{B}}\}$.

Further by combining the technique of [8, 1], we can construct a 2-round PSMT such that not only the transmission rate is $O(n)$, but also the computational cost of the sender and the receiver are both polynomial in n. The details will be given in the following sections.

3 Details of Our 3-Round PSMT

In this section, we describe the details of our 3-round PSMT for $n = 2t + 1$ which was outlined in Sec.2.5, and prove its security. We also show that the

transmission rate is $O(n)$ and the computational cost of the sender and the receiver are both polynomial in n.

Remember that FORGED is the set of all channels which the adversary forged, and "broadcast" is defined in Sec.2.4.

3.1 3-round Protocol for $n = 2t + 1$

The sender wishes to send $\ell = nt$ secrets $s_1, \cdots, s_\ell \in \mathsf{F}$ to the receiver.

Step 1. The sender does the following for $i = 1, 2, \cdots, t + \ell$.

1. She chooses a polynomial $f_i(x)$ over F such that $\deg f_i(x) \leq t$ randomly. Let $X_i = (f_i(1), \cdots, f_i(n))$.
2. She send $f_i(j)$ through channel j for $j = 1, \cdots, n$. The receiver then receives $Y_i = X_i + E_i$, where E_i is the error vector caused by the adversary.

Step 2. The receiver does the following.

1. Find the pseudo-dimension k and a pseudo-basis $\mathcal{B} = \{Y_{j1}, \cdots, Y_{jk}\}$ of $\{Y_1, \cdots, Y_{t+\ell}\}$ by using the algorithm of Fig.3.
2. Broadcast k, $\mathcal{B}$ and $\Lambda_{\mathcal{B}} = \{j_1, \cdots, j_k\}$. where $\Lambda_{\mathcal{B}}$ is the set of indices of $\mathcal{B}$.

Step 3. The sender does the following.

1. Construct FORGED of eq.(7) from $\{E_j = Y_j - X_j \mid j \in \Lambda_{\mathcal{B}}\}$.
2. Compute $c_1 = s_1 + f_{i_1}(0), \cdots, c_\ell = s_\ell + f_{i_\ell}(0)$ for $i_1, \cdots, i_\ell \notin \Lambda_{\mathcal{B}}$.
3. Broadcast FORGED and $(c_1, \cdots, c_\ell)$.

Step 4. The receiver does the following. Let $Y_i = (y_{i1}, \cdots, y_{in})$.

1. For each $i \notin \Lambda_{\mathcal{B}}$, find a polynomial $f'_i(x)$ with $\deg f'_i(x) \leq t$ such that
$$f'_i(j) = y_{i,j}$$
for all $j \notin$ FORGED.
2. Compute $s'_1 = c_1 - f'_{i_1}(0), \cdots, s'_\ell = c_\ell - f'_{i_\ell}(0)$ for $i_1, \cdots, i_\ell \notin \Lambda_{\mathcal{B}}$.
3. Output $(s'_1, \cdots, s'_\ell)$.

3.2 Security

We first prove the perfect privacy. Consider $f_i(x)$ such that $i \notin \Lambda_{\mathcal{B}}$. For such i, Y_i is not broadcast at step 2-2. Hence the adversary observes at most t elements of $(f_i(1), \cdots, f_i(n))$. This means that she has no information on $f_i(0)$ because $\deg f_i(x) \leq t$. Therefore since $\{f_i(0) \mid i \notin \Lambda_{\mathcal{B}}\}$ is used as the key of one-time-pad, the adversary learns no information on $s_1, \cdots, s_\ell$.

We next prove the perfect reliability. We first show that there exist ℓ indices $i_1, i_2, \cdots, i_\ell$ such that
$$\{i_1, i_2, \cdots, i_\ell\} \subseteq \{1, 2, \cdots, t + \ell\} \setminus \Lambda_{\mathcal{B}}.$$

This is because

$$t + \ell - |\Lambda_{\mathcal{B}}| \geq t + \ell - t = \ell.$$

from Theorem 2. We next show that $f'_i(x) = f_i(x)$ for each $i \notin \Lambda_{\mathcal{B}}$ at Step 4. This is because

$$f'_i(j) = y_{i,j} = x_{i,j} = f_i(j)$$

for all $j \notin \mathsf{FORGED}$, and

$$n - |\mathsf{FORGED}| \geq 2t + 1 - t \geq t + 1.$$

Also note that $\deg f_i(x) \leq t$ and $\deg f'_i(x) \leq t$. Therefore $s'_i = s_i$ for $i = 1, \cdots, \ell$.

3.3 Efficiency

Let $|\mathsf{F}|$ denote the bit length of the field elements. Let $\mathsf{COM(i)}$ denote the communication complexity of Step i for $i = 1, 2, 3$. Then

$$\begin{aligned}
\mathsf{COM}(1) &= O(n(t+\ell))|\mathsf{F}|) = O(n\ell|\mathsf{F}|),\\
\mathsf{COM}(2) &= O(n^2 t|\mathsf{F}|) = O(n\ell|\mathsf{F}|),\\
\mathsf{COM}(3) &= O(n\ell|\mathsf{F}| + tn\log_2 n) = O(n\ell|\mathsf{F}|)
\end{aligned}$$

since $\ell = nt$. Hence the total communication complexity is $O(n\ell|\mathsf{F}|) = O(n^3|\mathsf{F}|)$. Further the sender sends ℓ secrets $s_1, \cdots, s_\ell \in \mathsf{F}$. Therefore, the transmission rate is $O(n)$ because

$$\frac{n\ell|\mathsf{F}|}{\ell|\mathsf{F}|} = n.$$

It is easy to see that the computational costs of the sender and the receiver are both polynomial in n.

4 Our Basic 2-Round PSMT

In this section, we show our basic 2-round PSMT for $n = 2t + 1$ such that the transmission rate is $O(n^2 t)$ and the computational costs of the sender and the receiver are both polynomial in n.

For two vectors $U = (u_1, \cdots, u_n)$ and $Y = (y_1, \cdots, y_n)$, define

$$\begin{aligned}
d_u(U, Y) &= \{u_j \mid u_j \neq y_j\}\\
d_I(U, Y) &= \{j \mid u_j \neq y_j\}.
\end{aligned}$$

Remember that $\mathcal{C}$ is the set of all $(f(1), \cdots, f(n))$ such that $\deg f(x) \leq t$.

4.1 Randomness Extractor

Suppose that the adversary has no information on ℓ out of m random elements $r_1, \cdots, r_m \in \mathsf{F}$. In this case, let $R(x)$ be a polynomial with $\deg R(x) \leq m - 1$ such that $R(i) = r_i$ for $i = 1, \cdots, m$. Then it is well known [1, Sec.2.4] that the adversary has no information on

$$z_1 = R(m+1), \cdots, z_\ell = R(m+\ell).$$

4.2 Basic 2-round Protocol

The sender wishes to send a secret $s \in \mathsf{F}$ to the receiver.

Step 1. The receiver does the following for $i = 1, 2, \ldots, n$.

1. He chooses a random polynomial $f_i(x)$ such that $\deg f_i(x) \leq t$.
2. He sends
$$X_i = (f_i(1), \cdots, f_i(n))$$
through channel i, and the sender receives
$$U_i = (u_{i1}, \ldots, u_{in}).$$
3. Through each channel j, he sends $f_i(j)$ and the sender receives
$$y_{ij} = f_i(j) + e_{ij},$$
where e_{ij} is the error caused by the adversary. Let
$$Y_i = (y_{i1}, \cdots, y_{in}),\ E_i = (e_{i1}, \cdots, e_{in}).$$

Step 2. The sender does the following.

1. For $i = 1, \cdots, n$,
   (a) If $u_{ii} \neq y_{ii}$ or $|d_u(U_i, Y_i)| \geq t + 1$ or $U_i \notin \mathcal{C}$,
   then broadcast "ignore channel i". [6]
   This channel will be ignored from now on because it is forged clearly.
   (b) Else define r_i as
   $$r_i = u_{ii} = y_{ii}. \tag{9}$$
2. Find a polynomial $R(x)$ with $\deg R(x) \leq n - 1$ such that
$$R(i) = r_i$$
for each i.
3. Compute $R(n + 1)$ and broadcast
$$c = s + R(n + 1).$$
4. Find the pseudo-dimension k and a pseudo-basis $\mathcal{B} = \{Y_{j1}, \cdots, Y_{jk}\}$ of $\{Y_1, \cdots, Y_n\}$ by using the algorithm of Fig.3.
Broadcast $k, \mathcal{B}$ and $\Lambda_{\mathcal{B}} = \{j_1, \cdots, j_k\}$.
5. Broadcast $d_u(U_i, Y_i)$ and $d_I(U_i, Y_i)$ for each i.

Step 3. The receiver does the following.

1. Construct FORGED of eq.(7) from $\{E_i = Y_i - X_i \mid i \in \Lambda_{\mathcal{B}}\}$.

[6] For simplicity, we assume that there are no such channels in what follows.

2. For each i, find a polynomial $u_i(x)$ with $\deg u_i(x) \leq t$ such that

$$u_i(j) = u_{ij} \text{ for all } j \in d_I(U_i, Y_i),$$
$$u_i(j) = f_i(j) \text{ for all } j \text{ such that } j \notin d_I(U_i, Y_i) \text{ and } j \notin \mathsf{FORGED}$$

3. Find a polynomial $R'(x)$ with $\deg R'(x) \leq n-1$ such that

$$R'(i) = u_i(i)$$

for each i. [7]

4. Compute $R'(n+1)$ and output

$$s' = c - R'(n+1).$$

4.3 Security

We first prove the perfect privacy.

Lemma 2. *There is at least one r_i on which the adversary has no information.*

Proof. Consider a non-corrupted channel i such that $i \notin \Lambda_{\mathcal{B}}$. First the sender does not broadcast r_i at step 2-4 because $i \notin \Lambda_{\mathcal{B}}$. Next because $f_i(i)$ is sent through channel i that the adversary does not corrupt, we have

$$r_i = u_{ii} = f_i(i).$$

Further the adversary observes at most t values of $(f_i(1), \cdots, f_i(n))$. Hence the adversary has no information on $r_i = f_i(i)$ because $\deg f_i(x) \leq t$.

Finally there exists at least one non-corrupted channel i such that $i \notin \Lambda_{\mathcal{B}}$ because

$$n - t - |\Lambda_{\mathcal{B}}| \geq n - 2t = 1.$$

□

Therefore, the adversary has no information on $R(n+1)$ from Sec.4.1. Hence she learns no information on s from $c = s + R(n+1)$.

We next prove the perfect reliability. If $j \notin \mathsf{FORGED}$ and $j \notin d_I(U_i, Y_i)$, then $f_i(j) = y_{ij} = u_{ij}$ from the definition of $d_I(U_i, Y_i)$. Therefore, at step 3-2,

$$u_i(j) = u_{ij}$$

for all $j \in d_I(U_i, Y_i)$, and for all j such that $j \notin d_I(U_i, Y_i)$ and $j \notin \mathsf{FORGED}$. This means that $u_i(j) = u_{ij}$ for each $j \in (\overline{\mathsf{FORGED}} \cup d_I(U_i, Y_i))$, where

$$|\overline{\mathsf{FORGED}} \cup d_I(U_i, Y_i))| \geq |\overline{\mathsf{FORGED}}| \geq n - t = (2t+1) - t = t + 1.$$

[7] "for each i" can be replaced by "for each $i \notin \Lambda_{\mathcal{B}}$" at step 2-2 and step 3-3.

Further since $\deg u_i(x) \leq t$ and $U_i \in \mathcal{C}$, it holds that

$$(u_i(1), \cdots, u_i(n)) = (u_{i1}, \cdots, u_{in}).$$

In particular, $u_i(i) = u_{ii}$. Therefore from eq.(9), we have that

$$R(i) = r_i = u_{ii} = u_i(i) = R'(i)$$

for each i. Hence we obtain that $R'(x) = R(x)$ because $\deg R'(x) \leq n-1$ and $\deg R(x) \leq n-1$. Consequently,

$$s' = c - R'(n+1) = c - R(n+1) = s.$$

Thus the receiver can compute $s' = s$ correctly.

4.4 Efficiency

Let $\mathsf{COM(i)}$ denote the communication complexity of Step i for $i = 1, 2$. Note that $|d_u(U_i, Y_i)| = |d_I(U_i, Y_i)| \leq t$ for each i. Then

$$\begin{aligned}
\mathsf{COM(1)} &= O(n(n+n)|\mathsf{F}|) = O(n^2|\mathsf{F}|), \\
\mathsf{COM(2)} &= O((|d_I(U_i, Y_i)| \log_2 n + |d_u(U_i, Y_i)||\mathsf{F}|)n^2 \\
&\quad + (\log_2 n + n|\mathcal{B}||\mathsf{F}| + |\Lambda_{\mathcal{B}}| \log_2 n)n + |\mathsf{F}|n) \\
&= O(tn^2 \log_2 n + tn^2|\mathsf{F}| + n \log_2 n + n^2 t|\mathsf{F}| + tn \log_2 n + |\mathsf{F}|n) \\
&= O(n^2 t|\mathsf{F}|)
\end{aligned}$$

because $|\mathcal{B}| = |\Lambda_{\mathcal{B}}| \leq t$. Hence the total communication complexity is $O(n^2 t|\mathsf{F}|)$. The transmission rate is $O(n^2 t)$ because the sender sends one secret.

It is easy to see that the computational cost of the sender and the receiver are polynomial in n.

5 More Efficient 2-Round Protocol

In our basic 2-round protocol, the sender sends a single secret. In this section, we show a more efficient 2-round protocol such that the sender sends t^2 secrets by running the basic protocol t times in parallel. This implies that we can reduce the transmission rate from $O(n^2 t)$ to $O(n^2)$.

5.1 Protocol

The sender wishes to send $\ell = t^2$ secrets $s_1, s_2, \ldots, s_\ell \in \mathsf{F}$ to the receiver.

Step 1. The receiver does the following for each channel i.
For $h = 0, 1, \cdots, t-1$;

1. He chooses a random polynomial $f_{i+hn}(x)$ such that $\deg f_{i+hn}(x) \leq t$.

2. He sends
$$X_{i+hn} = (f_{i+hn}(1), \cdots, f_{i+hn}(n))$$
through channel i, and the sender receives
$$U_{i+hn} = (u_{i+hn,1}, \cdots, u_{i+hn,n})$$
3. Through each channel j, he sends $f_{i+hn}(j)$ and the sender receives
$$y_{i+hn,j} = f_{i+hn}(j) + e_{i+hn,j},$$
where $e_{i+hn,j}$ is the error caused by the adversary. Let
$$Y_{i+hn} = (y_{i+hn,1}, \cdots, y_{i+hn,n}),\ E_{i+hn} = (e_{i+hn,1}, \cdots, e_{i+hn,n}).$$

Step 2. The sender does the following.

1. Find the pseudo-dimension k and a pseudo-basis $\mathcal{B} = \{Y_{j1}, \ldots, Y_{jk}\}$ of $\{Y_1, \cdots, Y_{tn}\}$ by using the algorithm of Fig.3.
Broadcast $k, \mathcal{B}$ and $\Lambda_{\mathcal{B}} = \{j_1, \cdots, j_k\}$.
2. For $i = 1, \cdots, n$,
   (a) If $u_{i+hn,i} \neq y_{i+hn,i}$ or $|d_u(U_{i+hn}, Y_{i+hn})| \geq t+1$ or $U_{i+hn} \notin \mathcal{C}$ for some h, then broadcast "ignore channel i". [8]
   This channel will be ignored from now on because it is forged clearly.
   (b) Else define r_{i+hn} as
$$r_{i+hn} = u_{i+hn,i} = y_{i+hn,i} \tag{10}$$
   for $h = 0, \cdots, t-1$.
3. Find a polynomial $R(x)$ with $\deg R(x) \leq nt - 1$ such that
$$R(i + hn) = r_{i+hn}$$
for each $i + hn$.
4. Compute $R(nt+1), \cdots, R(nt+\ell)$ and broadcast
$$c_1 = s_1 + R(nt+1), \cdots, c_\ell = s_\ell + R(nt+\ell).$$
5. Broadcast $d_u(U_{i+hn}, Y_{i+hn})$ and $d_I(U_{i+hn}, Y_{i+hn})$ for each $i + hn$.

Step 3. The receiver does the following.

1. Construct FORGED of eq.(7) from $\{E_i = Y_i - X_i \mid i \in \Lambda_{\mathcal{B}}\}$.
2. For each $i+hn$, find a polynomial $u_{i+hn}(x)$ with $\deg u_{i+hn}(x) \leq t$ such that
$u_{i+hn}(j) = u_{i+hn,j}$ for all $j \in d_I(U_{i+hn}, Y_{i+hn})$
$u_{i+hn}(j) = f_{i+hn}(j)$ for all j such that $j \notin d_I(U_{i+hn}, Y_{i+hn})$ and $j \notin$ FORGED
3. Find a polynomial $R'(x)$ with $\deg R'(x) \leq nt - 1$ such that
$$R'(i + hn) = u_{i+hn}(i)$$
for each $i + hn$. [9]
4. Compute $R'(nt+1), \cdots, R'(nt+\ell)$ and output
$$s'_1 = c_1 - R'(nt+1), \cdots, s'_\ell = c_\ell - R'(nt+\ell).$$

[8] For simplicity, we assume that there are no such channels in what follows.
[9] "for each $i + hn$" can be replaced by "for each $i + hn \notin \Lambda_{\mathcal{B}}$" at step 2-3 and step 3-3.

5.2 Security

We first prove the perfect privacy.

Lemma 3. *There exists a subset $A \subset \{r_1, \cdots, r_{tn}\}$ such that $|A| \geq \ell$ and the adversary has no information on A.*

Proof. Consider a non-corrupted channel i such that $i + hn \notin \Lambda_{\mathcal{B}}$. First the sender does not broadcast r_{i+hn} at step 2-1 because $i + hn \notin \Lambda_{\mathcal{B}}$. Next since $f_{i+hn}(i)$ is sent through channel i that the adversary does not corrupt, we have

$$r_{i+hn} = u_{i+hn,i} = f_{i+hn}(i).$$

Further the adversary observes at most t values of $(f_{i+hn}(1), \cdots, f_{i+hn}(n))$. Hence the adversary has no information on $r_{i+hn} = f_{i+hn}(i)$ because $\deg f_{i+hn}(x) \leq t$.

Note that the adversary corrupts at most t channels and for each corrupted channel i, the adversary gets $r_i, r_{i+n}, \ldots, r_{i+(t-1)n}$. Therefore, there exists a subset $A \subset \{r_1, \cdots, r_{tn}\}$ such that

$$|A| \geq nt - |\Lambda_{\mathcal{B}}| - t^2 = nt - k - t^2$$

and the adversary has no information on A. Finally

$$nt - k - t^2 \geq (2t+1)t - t - t^2 = t^2 = \ell.$$

□

Therefore, the adversary has no information on $R(nt+1)$, …, $R(nt+\ell)$ from Sec.4.1. Hence she learns no information on s_i for $i = 1, \cdots, \ell$.

We next prove the perfect reliability. If $j \notin \mathsf{FORGED}$ and $j \notin d_I(U_{i+hn}, Y_{i+hn})$, then $f_{i+hn}(j) = y_{i+hn,j} = u_{i+hn,j}$ from the definition of $d_I(U_{i+hn}, Y_{i+hn})$. Therefore,

$$u_{i+hn}(j) = u_{i+hn,j}$$

for all $j \in d_I(U_{i+hn}, Y_{i+hn})$, and for all j such that $j \notin d_I(U_{i+hn}, Y_{i+hn})$ and $j \notin \mathsf{FORGED}$. This means that $u_{i+hn}(j) = u_{i+hn,j}$ for each $j \in (\overline{\mathsf{FORGED}} \cup d_I(U_{i+hn}, Y_{i+hn}))$, where

$$|\overline{\mathsf{FORGED}} \cup d_I(U_{i+hn}, Y_{i+hn}))| \geq |\overline{\mathsf{FORGED}}| \geq n - t = 2t + 1 - t = t + 1.$$

Further since $\deg u_{i+hn}(x) \leq t$ and $U_{i+hn} \in \mathcal{C}$, it holds that

$$(u_{i+hn}(1), \cdots, u_{i+hn}(n)) = (u_{i+hn,1}, \cdots, u_{i+hn,n}).$$

In particular, $u_{i+hn}(i) = u_{i+hn,i}$. Therefore from eq.(10), we have that

$$R(i+hn) = r_{i+hn} = u_{i+hn,i} = u_{i+hn}(i) = R'(i+hn)$$

for each $i + hn$. Hence we obtain that $R'(x) = R(x)$ because $\deg R'(x) \leq nt - 1$ and $\deg R(x) \leq nt - 1$. Consequently,

$$s'_i = c_i - R'(nt+i) = c_i - R(nt+i) = s_i.$$

Thus the receiver can compute $s'_i = s_i$ correctly for $i = 1, \cdots, \ell$.

5.3 Efficiency

Let $\mathsf{COM(i)}$ denote the communication complexity of Step i for $i = 1, 2$. Note that $|d_u(U_{i+hn}, Y_{i+hn})| = |d_I(U_{i+hn}, Y_{i+hn})| \leq t$ for each $i + hn$. Then

$$\begin{aligned}
\mathsf{COM(1)} &= O(tn(n+n)|\mathsf{F}|) = O(tn^2|\mathsf{F}|),\\
\mathsf{COM(2)} &= O((|d_I(U_{i+hn}, Y_{i+hn})| \log_2 n + |d_u(U_{i+hn}, Y_{i+hn})||\mathsf{F}|)tn \times n\\
&\qquad + (\log_2 n + n|\mathcal{B}||\mathsf{F}| + |\Lambda_{\mathcal{B}}| \log_2 n)n + t^2|\mathsf{F}|n)\\
&= O(n^2t^2 \log_2 n + n^2t^2|\mathsf{F}| + n \log_2 n + n^2t|\mathsf{F}| + tn \log_2 n + t^2|\mathsf{F}|n)\\
&= O(n^2t^2|\mathsf{F}|)
\end{aligned}$$

because $|\mathcal{B}| = |\Lambda_{\mathcal{B}}| \leq t$. Hence, the total communication complexity is $O(n^2t^2|\mathsf{F}|)$, and the transmission rate is $O(n^2)$ because the sender sends t^2 secrets.

It is easy to see that the computational costs of the sender and the receiver are both polynomial in n.

6 Final 2-Round PSMT

The transmission rate is still $O(n^2)$ in the 2-round PSMT shown in Sec.5. In this section, we show how to reduce it to $O(n)$ by using the technique of [1, page 406] and [8]. Then we can obtain the first 2-round PSMT for $n = 2t + 1$ such that not only the transmission rate is $O(n)$ but also the computational costs of the sender and the receiver are both polynomial in n.

6.1 Generalized Broadcast

Suppose that the receiver knows the locations of k ($\leq t$) channels that the adversary forged, and the sender knows the value of k. For example, suppose that the receiver knows that channels $1, 2, \cdots, k$ are forged. Note that the adversary can corrupt at most $t - k$ channels among the remaining $n - k$ channels $k + 1, \cdots, n$.

In this case, it is well known that the sender can send $k + 1$ field elements $u_1, u_2, \ldots, u_{k+1}$ reliably with the communication complexity $O(n|\mathsf{F}|)$ as follows.

1. The sender finds a polynomial $p(x)$ with $\deg p(x) \leq k$ such that $p(1) = u_1$, $p(2) = u_2$, ... , $p(k + 1) = u_{k+1}$.
2. She sends $p(i)$ through channel i for $i = 1, \cdots, n$.

Without loss of generality, suppose that the receiver knows that channels $1, \cdots, k$ are forged by the adversary. Then he consider a shortened code such that a codeword is $(p(k+1), \cdots, p(n))$. The minimum Hamming distance of this code is $(n - k) - k = 2t + 1 - 2k = 2(t - k) + 1$. Hence the receiver can correct the remaining $t - k$ errors.

This means that the receiver can decode $(p(k+1), \cdots, p(n))$ correctly. Then he can reconstruct $p(x)$ by using Lagrange formula because

$$n - k = 2t + 1 - k \geq 2k + 1 - k = k + 1 \geq \deg p(x) + 1.$$

Therefore he can obtain $u_1 = p(1), \ldots, u_{k+1} = p(k + 1)$ correctly.

6.2 Matching of Graph

Let $G = (\mathsf{V}, \mathsf{E})$ be the undirected simple graph with the vertex set V and the edge set E. A *matching* of the graph G is an edge set $M \subseteq \mathsf{E}$ such that no two edges in M are connected. A matching M is said to be *maximal* if there is no matching $M' \neq M$ such that $M \subseteq M'$.

We can find a maximal matching M of G easily (in polynomial time) by using a greedy algorithm as follows.

1. Let $M = \emptyset$.
2. For each edge e in E, do:
   If e is not connected to any edge in M, then add e to M.
3. Output M.

Definition 4. *For a vertex $v \in V$, let $\deg_G(v)$ denote the number of edges which are connected to v. Define*

$$D_{max} = \max_{v \in V} \deg_G(v).$$

We then say that D_{max} be the maximum degree of the graph G.

Theorem 3. *For a graph $G = (\mathsf{V}, \mathsf{E})$, let M be a maximal matching and D_{max} be the maximum degree. Then $|\mathsf{E}| \leq 2|M| \cdot D_{max}$.*

Proof. For a maximal matching M, define

$$V(M) = \{v \in V \mid \text{some } e \in M \text{ is connected to a vertex } v\}.$$

Delete all the edges connected to $V(M)$ from G. Then from the definition of maximal matching, we have no edges. Further $|V(M)| = 2|M|$. Therefore,

$$|\mathsf{E}| \leq \Sigma_{x \in V(M)} \deg_G(x) \leq 2|M|D_{max}.$$

□

In [1, page 406] and [8], a *maximum* matching was used. Instead we use a *maximal* matching because it is sufficient for our purpose, and it is easier to find a maximal matching than a maximum matching.

6.3 How to Improve Step 2-5

In the 2-round PSMT shown in Sec.5, step 2-5 is the most expensive part, where the sender broadcasts $d_u(U_{i+hn}, Y_{i+hn})$ and $d_I(U_{i+hn}, Y_{i+hn})$ for each $i + hn$.

In this subsection, we will show a method which reduces the communication complexity of step 2-5 from $O(n^2t^2|\mathsf{F}|)$ to $O(n^2t|\mathsf{F}|)$. We modify step 2-5 as follows.

Step 2. The sender does the following.

5' For $h = 0, 1, \cdots, t-1$, do:
   (a) Construct an undirected graph $G_h = (\mathsf{N}, \mathsf{E}_h)$ such that $(i,j) \in \mathsf{E}_h$ if and only if $u_{i+hn,j} \neq y_{i+hn,j}$ or $u_{j+hn,i} \neq y_{j+hn,i}$. [10]
   (b) Find a maximal matching M_h of G_h.
   (c) For each edge $e = (i,j) \in M_h$,
      i. If $u_{i+hn+i,j} \neq y_{i+hn+i,j}$ then broadcast $x_e = ((h,i,j), u_{i+hn,j}, y_{i+hn,j})$.
      ii. Else broadcast $x_e = ((h,i,j), u_{j+hn,i}, y_{j+hn,i})$.
   (d) Send $\{d_u(U_{i+hn}, Y_{i+hn}) \mid i = 1, \cdots, n\}$ and $\{d_I(U_{i+hn}, Y_{i+hn}) \mid i = 1, \cdots, n\}$ to the receiver by using the generalized broadcasting as shown below.

If there exists an edge $e = (i,j) \in M_h$, then channel-i is forged or channel-j is forged. Therefore,

$$|M_h| \leq t$$

from the definition of maximal matching. For each h, the communication complexity of step 2-5'(c) is $O(tn|\mathsf{F}|)$ because $|M_h| \leq t$. For all h, the communication complexity is $O(nt^2|\mathsf{F}|)$

After step 2-5'(c), the receiver can find at least one forged channel from each x_e, where $e \in M_h$. Hence he can find at least $|M_h|$ forged channels from $\{x_e \mid e \in M_h\}$ from the definition of maximal matching.

Hence the sender can send $|M_h| + 1$ field elements reliably with the communication complexity $O(n|\mathsf{F}|)$ by using the generalized broadcasting (see Sec.6.1).

Next from Theorem 3, we obtain that

$$|\mathsf{E}_h| \leq 2|M_h|t$$

because $\deg_{G_h}(i) \leq t$ for all i from step 2-2(a). Further it is easy to see that

$$\sum_{i=1}^{n} |d_u(U_{i+hn}, Y_{i+hn})| = \sum_{i=1}^{n} |d_u(U_{i+hn}, Y_{i+hn})| \leq 2|\mathsf{E}_h| \leq 4|M_h|t$$

Therefore, for each h, the sender can send $\{d_u(U_{i+hn}, Y_{i+hn}) \mid i = 1, \cdots, n\}$ and $\{d_I(U_{i+hn}, Y_{i+hn}) \mid i = 1, \cdots, n\}$ to the receiver reliably with the communication complexity $O(nt|\mathsf{F}|)$ by using generalized broadcasting. For all h, the communication complexity is $O(nt^2|\mathsf{F}|)$.

This means that the sender can send all $d_u(U_{i+hn}, Y_{i+hn})$ and $d_I(U_{i+hn}, Y_{i+hn})$ reliably with the communication complexity $O(nt^2|\mathsf{F}|)$.

6.4 Final Efficiency

Consequently, we obtain $\mathsf{COM}(2) = O(n^2t|\mathsf{F}|)$ because the communication complexity of step 2-5' is now reduced to $O(n^2t|\mathsf{F}|)$. On the other hand, $\mathsf{COM}(1) = O(n^2t|\mathsf{F}|)$ from Sec.5.3. To summarize,

$$\mathsf{COM}(1) = O(n^2t|\mathsf{F}|) \text{ and } \mathsf{COM}(2) = O(n^2t|\mathsf{F}|)$$

[10] This means that channel-i is forged or channel-j is forged.

in our final 2-round PSMT. Hence, the total communication complexity is $O(n^3|\mathsf{F}|)$ because $n = 2t + 1$.

Now the transmission rate is $O(n)$ because the sender sends t^2 secrets which is $O(n^2|\mathsf{F}|)$. Finally, it is easy to see that the computational costs of the sender and the receiver are both polynomial in n.

Acknowledgement

We would like to thank Jun Furukawa and Adi Shamir for useful discussion.

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. D.Dolev, C.Dwork, O.Waarts, M.Yung: Perfectly Secure Message Transmission. J. ACM 40(1): pp.17–47 (1993)
3. Y.Desmedt, Y.Wang and M.Burmester: A Complete Characterization of Tolerable Adversary Structures for Secure Point-to-Point Transmissions Without Feedback. ISAAC 2005: pp.277–287 (2005)
4. M.Fitzi, M.Franklin, J.Garay, S.Vardhan: Towards Optimal and Efficient Perfectly Secure Message Transmission. TCC 2007: pp.311–322 (2007)
5. M.Hirt, U.Maurer: Player Simulation and General Adversary Structures in Perfect Multiparty Computation. J. Cryptology 13(1): pp.31–60 (2000)
6. M.V.N.A.Kumar, P.R.Goundan, K.Srinathan, C.P.Rangan: On perfectly secure communication over arbitrary networks. PODC 2002: pp.193–202 (2002)
7. H.Md.Sayeed and H.Abu-Amara: Efficient Perfectly Secure Message Transmission in Synchronous Networks. Inf. Comput. 126(1): pp.53–61 (1996)
8. K. Srinathan, Arvind Narayanan, C. Pandu Rangan: Optimal Perfectly Secure Message Transmission. CRYPTO 2004: pp.545–561 (2004)