Perfectly Secure Message Transmission Scheme against Rational Adversaries

Maiki Fujita[1] and Takeshi Koshiba[2]

[1] Graduate School of Science and Engineering,
Saitama University,
Shimo-Okubo 255, Sakura-ku, Saitama 338-8570, Japan.

[2] Faculty of Education and Integrated Arts and Sciences,
Waseda University,
Nishi-Waseda 1-6-1, Shinjuku-ku, Tokyo 169-8050, Japan.
tkoshiba@waseda.jp

Abstract. Secure Message Transmission (SMT) is a two-party cryptographic scheme by which a sender securely and reliably sends messages to a receiver using n channels. Suppose that an adversary corrupts at most t out of n channels and makes eavesdropping or tampering over the corrupted channels. It is known that if $t < n/2$ then the perfect SMT (PSMT) in the information-theoretic sense is achievable and if $t \geq n/2$ then no PSMT scheme is possible to construct. If we are allowed to use a public channel in addition to the normal channels, we can achieve the almost reliable SMT (ARSMT), which admits transmission failures of small probability, against $t < n$ corruptions. In the standard setting in cryptography, the participants are classified into honest ones and corrupted ones: every honest participant follows the protocol but corrupted ones are controlled by the adversary and behave maliciously. As a real setting, the notion of rationality in the game theory is often incorporated into cryptography. In this paper, we first consider "rational adversary" who behaves according to his own preference in SMT. We show that it is possible to achieve PSMT even against any $t < n$ corruptions under some reasonable settings for rational adversaries.

Keywords: secure message transmission, secret sharing, rational adversary, cryptography, game theory

1 Introduction

It is common to use the information network to send and receive messages. In the physical sense, the channels between senders and receivers might be realized by combining apparatus for communication, which allow some adversary to eavesdrop or tamper. As a technique for protecting data over communication from their leakage, we often use public-key cryptosystems. Since the security of

public-key cryptosystems is based on computational assumptions and the computational assumptions might be falsified, it is desirable to develop methods of protecting data in the information-theoretic sense.

While a single communication channel is assumed in the typical two-party cryptographic schemes, the current information network technologies can let many channels be available. Secure Message Transmission (SMT), originally proposed by Dolev *et al.* [1], is a cryptographic scheme by which a sender securely sends messages to a receiver using multiple channels. Even if any adversary corrupts at most t out of n channels and makes eavesdropping or tampering over the corrupted channels, then any messages can be securely transmitted in the information-theoretic sense by using SMT. The requirement for SMT consists of the *privacy* and the *correctness*. The privacy means that any adversary cannot get any information about the message and the correctness means that the messages which the sender sends and which the receiver receives are agreed. If an SMT scheme satisfies both the requirements in the perfect sense, the scheme is called *perfect* SMT (PSMT). The most round-efficient PSMT scheme is given by Kurosawa and Suzuki [2]. Dolev *et al.* [1] showed that any one-round PSMT must satisfies $t < n/3$ and any PSMT whose round number is two or more must satisfies $t < n/2$. Franklin and Wright [3] considered the *almost reliable* SMT (ARSMT) which allows transmission failures of small probability. They showed that ARSMT against $t < n$ corruptions is achievable by using a public channel in addition to the normal channels. Moreover, the most round-efficient ARSMT protocols using public channels are given in [4, 5].

In the standard setting in cryptography, the participants are classified into honest ones and corrupted ones: the former ones follow the protocol and the later ones are controlled by the adversary and behave maliciously. Generally speaking, the adversarial behavior may be illegal and involve some risks. This means that some adversary in the standard cryptographic setting can act maliciously regardless of the risks. On the other hand, some adversary in reality decides his behavior by taking the risks into account. To formalize the above situation, we incorporate the notion of "rational player" of the game theory into cryptography. "Rational players" behave according to their own preference. That could provide a more realistic security model. The incorporation of the rationality into cryptography was firstly consider by Halpern and Teague [6]. They considered the rationality in Shamir's secret sharing scheme [7]. If the shareholders in Shamir's scheme are all honest, they can uniquely reconstruct the secret. Halpern and Teague [6] supposed that shareholders are rational. This means that each shareholder wants to know the secret but the number of shareholders who can reconstruct the secret should be minimized. It was shown that no shareholders can reconstruct the secret in the above rational setting. Since then, the rational secret sharing have been intensively studied [8–12].

In the study of the rational secret sharing, the Nash equilibria among several parties plays an important role. For protocols secure against rational players are designed to satisfy that obeying the protocols should be the Nash equilibrium. In some protocols, the simplest case of the rationality is considered. The simplest

case means that the game has one player (i.e., the adversary). As in the rational secret sharing, we essentially consider what is a Nash equilibrium strategy for the adversary. However, the Nash equilibrium of a one-player game is just a utility-optimization. Along this line, Groce *et al.* [13] incorporated the rationality into the Byzantine agreement, proposed by Pease, Shostak and Lamport [14]. We assume that there are n generals who want to decide the next operation, either "attack" or "retreat", and that the generals can directly communicate via channels with each other. For the next operation, they have to reach an agreement. If any adversary corrupts at most t out of n channels (for each general) and makes eavesdropping or tampering over the corrupted channels, it is possible to reach an agreement in the information-theoretic sense. In the standard setting, the bound $t < n/3$ is obtained [14]. Groce *et al.* [13] assume the rational adversarial generals only want to lead to a disagreement and consider that the agreement "retreat" is better than "attack". In this rational setting, we have a better bound $t < n$ than the standard case.

If we want to see more connections between cryptography and game theory, we may consult with [15, 16].

In this paper, we take the simplest case as in the rational Byzantine agreement [13] and consider "rational adversaries" who behave according to their own preference in "Secure Message Transmission" (SMT). We consider several cases for the preference and show that it is possible to achieve PSMT even against $t < n$ corruptions under some reasonable preference settings in the rational adversary model.

2 Secure Message Transmission

2.1 Definitions

We assume that our network can be represented as an incomplete graph. Two parties, a sender $\mathcal{S}$ and a receiver $\mathcal{R}$, correspond to a pair of nodes in the graph, where the two nodes are connected by n node-disjoint paths, called *channels*. In addition to the channels, we assume that there is an authentic and reliable *public channel* between the sender and the receiver. Messages $m \in \mathcal{M}$ over the public channel are publicly accessible and correctly delivered to the receiver. SMT protocols proceed in *rounds*. In each round, one party may synchronously send a message on each (normal or public) channel, while the other party will only receive the sent messages. The sent messages will be delivered before the next round starts.

The adversary $\mathcal{A}$ is computationally *unbounded* and can corrupt at most t nodes on channels between the sender and the receiver. A channel is said to be *corrupted* if at least one node on the channel is corrupted.

The adversary can eavesdrop and tamper over the corrupted channels. (Blocking messages sent over the channels is regarded as tampering.)

We refer to points during the protocol execution as view of the adversary $\mathcal{A}$, and denote it by $V_{\mathcal{A}}$. A view $V_{\mathcal{A}}$ consists of his randomly generated strings and some messages sent over the corrupted channel.

Here, we define SMT schemes as follows.

Definition 1. At the end of the protocol, if the following two properties hold, then the protocol can achieve (σ, ϵ)-SMT.

- *Privacy*:
  For any $m_1, m_2 \in \mathcal{M}$ and for any possible view V of the adversary, it holds that
  $$\left| \Pr[m = m_1 | V_A = V] - \Pr[m = m_2 | V_A = V] \right| \leq \sigma.$$
- *Correctness*:
  For any message $m \in \mathcal{M}$, the receiver $\mathcal{R}$ receives a message m' which satisfies that
  $$\Pr[m' \neq m] \leq \epsilon.$$

If a protocol achieves $(0, 0)$-SMT, the scheme is called *perfect* SMT (PSMT), and if the protocol achieves $(0, \epsilon)$-SMT, which admits transmission failures of small probability ϵ, the scheme is called *almost reliable* SMT (ARSMT).

For PSMT, Dolev *et al.* [1] showed the below.

Theorem 1. ([1]) *PSMT schemes are achievable if and only if any adversary can corrupt $t < n/2$ channels.*

2.2 Universal Hash Functions

Wegman and Carter [17] defined a notion of (almost) universal hash functions and gave its construction. We will consider SMT schemes in which universal hash functions are used.

Definition 2. Suppose that a class of hash functions $H = \{h : \{0,1\}^m \to \{0,1\}^\ell\}$, where $m \geq \ell$, satisfies the following: for any distinct $x_1, x_2 \in \{0,1\}^m$ and $y_1, y_2 \in \{0,1\}^\ell$,

$$\Pr_{h \in H}[h(x_1) = y_1 \wedge h(x_2) = y_2] \leq \gamma.$$

Then H is γ-almost strongly universal. In the above, the randomness comes from the uniform choice of h over H.

Here we mention a useful property of almost universal hash functions, which guarantees the security of some SMT protocols.

Lemma 1. ([5]) *Let $H = \{h : \{0,1\}^m \to \{0,1\}^\ell\}$ be a γ-almost strongly universal hash function family. The for any $(x_1, c_1) \neq (x_2, c_2) \in \{0,1\}^m \times \{0,1\}^\ell$, we have*

$$\Pr_{h \in H}[c_1 \oplus h(x_1) = c_2 \oplus h(x_2)] \leq 2^\ell \gamma.$$

In [17], Wegman and Carter constructed a family of $2^{1-2\ell}$-almost strongly universal hash functions. In particular, their hash function family $H_{wc} = \{h : \{0,1\}^m \to \{0,1\}^\ell\}$ satisfies that

$$\Pr_{h \in H_{wc}}[h(x_1) = y_1 \wedge h(x_2) = y_2] = 2^{1-2\ell}$$

for any distinct $x_1, x_2 \in \{0,1\}^m$ and for any $y_1, y_2 \in \{0,1\}^\ell$ and also

$$\Pr_{h \in H_{wc}}[c_1 \oplus h(x_1) \wedge c_2 h(x_2)] = 2^{1-\ell}$$

for any distict pairs $(x_1, c_1) \neq (x_2, c_2) \in \{0,1\}^m \times \{0,1\}^\ell$.

2.3 Secret sharing

Here, we briefly review Shamir's threshold secret sharing scheme [7]. We will use Shamir's scheme as an ingredient of our PSMT scheme.

Let $\mathbb{F}_p$ be a finite field of p elements and $s \in \mathbb{F}_p$ be a secret. The dealer randomly chooses a polynomial f (coefficients are elements in $\mathbb{F}_p$) of degree $n-1$ such that $f(0) = s$. The dealer divides s into shares $(s_1, s_2, \ldots, s_m)$, where $s_i = f(i)$, and distributes them to m shareholders. Then, if any n shareholders get together, they can recover the polynomial by using the Lagrange interpolation and then reconstruct s uniquely. This scheme is called (m, n)-*threshold* secret sharing, because any $n-1$ or less share holders cannot get any information on the secret s.

2.4 Secure Message Transmission with Public Channel

In this paper, we will discuss two SMT schemes. The first scheme is actually an ARSMT scheme with the public channel and we will show that the scheme works as a PSMT scheme in the rational adversary model. Here, we take an ARSMT scheme given by Shi, Jiang, Safavi-Naini, and Tuhin in [5] and call it *SJST11* protocol. Since we do not use any specific properties of the ARSMT scheme, we may use another ARSMT scheme (e.g., a scheme by Garay and Ostrovsky [4]) instead of Shi et al.'s scheme. The second scheme is a PSMT scheme without public channel, which we will propose later.

Let us review SJST11 ARSMT protocol with the public channel. Their protocol [5] has three rounds and achieves the correctness $\epsilon = (n-1) \cdot 2^{1-\ell}$, where ℓ is the length of hash values which are used in the protocol and proportional to the security parameter.

Protocol 1 (SJST11 ARSMT scheme [5])

Let n be the number of channels and m be a message that the sender $\mathcal{S}$ wants to send to the receiver $\mathcal{R}$.

1. For each number of i with $1 \leq i \leq n$, $\mathcal{S}$ chooses random bits $r_i \in \{0,1\}^\ell$ and $R_i \in \{0,1\}^m$ and sends the ith pair (r_i, R_i) to $\mathcal{R}$ over the ith channel.
2. For $i = 1, \ldots, n$, if $\mathcal{R}$ correctly receives a pair (r'_i, R'_i) over the ith channel (i.e., $r'_i \in \{0,1\}^\ell$ and $R'_i \in \{0,1\}^m$), $\mathcal{R}$ uniformly selects $h_i \leftarrow H$ and computes $T'_i = r'_i \oplus h_i(R'_i)$; otherwise, the ith channel is assumed *corrupted*. $\mathcal{R}$ then constructs an indicator bit string $B = b_1 b_2 \cdots b_n$ where $b_i = 1$ if the ith channel is corrupted and $b_i = 0$ otherwise. Finally, $\mathcal{R}$ sends $(B, (H_1, \ldots, H_n))$ over the public channel, where $H_i = (h_i, T'_i)$ if $b_i = 0$; and H_i is empty, otherwise.
3. $\mathcal{S}$ ignores the ith channel if $b_i = 1$. For $i = 1, \ldots, n$, if $b_i = 0$, $\mathcal{S}$ computes $T_i = r_i \oplus h_i(R_i)$ and checks $T'_i = T_i$; if $T'_i = T_i$, the ith channel is assumed *consistent*; otherwise, the ith channel is corrupted. $\mathcal{S}$ constructs an indicator bit string $V = v_1 v_2 \cdots v_n$, where $v_i = 1$ if the ith channel is considered consistent; otherwise $v_i = 0$. $\mathcal{S}$ sends the pair $(V, C = m \oplus (\bigoplus_{v_i=1} R_i))$ over the public channel.
4. $\mathcal{R}$ receives (V, C) and recovers $m = C \oplus (\bigoplus_{v_i=1} R'_i)$.

Theorem 2. ([5]) *Protocol 1 is a* $(0, (n-1) \cdot 2^{1-\ell})$*-ARSMT scheme against any adversary who corrupts* $t < n$ *channels.*

We can find a complete proof of the above theorem in [5]. For self-containment, we will give a brief sketch of the proof.

- *Privacy*:
  Since the sender $\mathcal{S}$ sends $C = m \oplus (\bigoplus R_i)$ over the public channel, the adversary can get $C = m \oplus (\bigoplus R_i)$. But m is masked by uniformly random R_i, thus the adversary has to corrupt all the normal channels to recover the original message m. Although the adversary can get $T'_i = r'_i \oplus h_i(R'_i) = r_i \oplus h_i(R_i)$, which may include information on R_i, $h(R_i)$ is masked by uniformly random r_i and r_i cannot be eavesdropped from any uncorrupted channels. Therefore, the adversary cannot get any information on m and thus Protocol 1 satisfies the perfect privacy.
- *Correctness*:
  Protocol 1 has three rounds. Since Protocol 1 uses only the public channel at the second and the third round, only chance the adversary tampers is at the first round. Suppose that the adversary tampers (r_i, R_i). If $(r_i, R_i) \neq (r'_i, R'_i)$ and $T_i = T'_i$ then $r_i \oplus h_i(R_i) = r'_i \oplus h_i(R'_i)$ holds and a wrong message would be recovered without being detected the tampering. We can bound the probability where the above (failure) event happens. Since there exists a $2^{1-2\ell}$-almost strongly universal hash function family [17] and the adversary corrupts at most $n-1$ normal channels, we can say that the failure event happens with probability at most $(n-1)2^{1-\ell}$ from Lemma 1. Finally note that if the adversary does not tamper any channel, the correct message would be recovered due to the construction of Protocol 1.

3 Game Theory for Secure Message Transmission

In the game theory (e.g., see [18]), we refer to each player's behavior as *strategy*, and denote it by σ. We refer to the evaluation value to be decided by the game as *utility*, and denote it by u. Since the utility is decided by the player's strategy, the utility when the player selects a strategy σ_i is denoted by $u(\sigma_i)$. Players who have the strategies and the utilities, and make decisions so as to get the highest utility values are called "rational players".

We have stated that the utility is determined by the player's strategy, but sometimes the utility in some game is not determined uniquely. For example, we assume a game where a player chooses a strategy σ, the utility is u_i with probability p and u_j with probability $1 - p$. Then the *expected* utility of this game when the player selects the strategy σ is defined as

$$u(\sigma) \;=\; p \cdot u_i + (1-p) \cdot u_j.$$

Rational players always choose the strategy that the expected utility is the highest.

3.1 Settings for Rational Adversaries

Players involved in SMT are (1) a sender and a receiver who want to securely and reliably transmit messages by using the SMT protocol and (2) an adversary who attacks on the protocol for SMT. While, in the standard cryptographic setting, we usually suppose that the adversary can take any thoughtless strategies for the attack, they are not realistic from the social/economic point of view. For example, if the tampering over a channel by the adversary is detected, the adversary's use of the channel might be prohibited or the adversary might compensate for the tampering.

We consider strategies of the rational adversary for SMT. The rational adversary can make "eavesdropping" or "tampering", so strategies of the rational adversary are defined as combinations over these actions. Tampering means replacing data over the channel with different data or blocking messages sent over the channel. We assume that strategies with respect to the tampering is either "tampering" or "not tampering". Eavesdropping means getting information over the corrupting channel. In this paper, we consider that there are no methods to detect eavesdropping, so we assume that strategies with respect to eavesdropping is "eavesdropping" only. To combine these actions, we define strategies of rational adversary in SMT are "eavesdropping and tampering" and "eavesdropping only". The former can be considered as *active* attack and the later as *passive* attack.

Next, we consider utilities of the rational adversary for SMT. The utilities depend on the result of the execution of the SMT protocol or information that the sender, the receiver or the adversary obtain. The results of the SMT protocol execution can be classified into (1) "success of the message transmission" which means that the receiver receives what the sender sends; (2) "failure of the

message transmission" which means that the receiver receives a wrong message, and (3) "abortion of the protocol" which means that either the sender or the receiver aborts the protocol execution. Besides these three utilities, we consider two more utilities: (4) "acquisition of the message" which means that the adversary get the message which the sender sends and (5) "detection of corrupted channels" which means that channels corrupted by the adversary are detected in the protocol.

Here, we summarize strategies and utilities for the rational adversary in SMT in Tables 1 and 2.

notation	strategy
σ_a	eavesdropping and tampering
σ_p	eavesdropping only

Table 1. Strategies for the rational adversary

notation	utility
u_s	success of the message transmission
u_f	failure of the message transmission
u_a	abortion of the protocol
u_d	detection of corrupted channels
u_q	acquisition of the message

Table 2. Utilities for the rational adversary

3.2 Preference of Rational Adversary

By using the utilities in Table 2, we define some reasonable settings. We consider settings for the standard (i.e., conventional) cryptographic model and two realistic models.

– *Standard cryptographic model* :
In this model, regardless of any risks, the adversary primally tries to get the message that the sender sends to the receiver by using the SMT protocol. Otherwise, he tries to obstruct the message transmission by making the protocol execution abort. Thus, the relation among the utilities must satisfy the following:

$$\min\{u_a, u_f\} > u_s, \quad u_q > 0 \quad \text{and} \quad u_d = 0.$$

– *"Timid" rational adversary model* :
In this model, we consider that the rational adversary is afraid of loss of the reliability. Precisely speaking, he is afraid of being exposed his dishonesty. For example, we assume that the adversary owns a channel and gains the usage fee from users. If he loses the reliability of the channel, then his gain may be decreased or he may be accused of his behavior. Thus, the relation among the utilities must satisfy the following:

$$\min\{u_a, u_f\} > u_s, \quad u_q > 0 \quad \text{and} \quad u_d < 0.$$

– *"Conservative" rational adversary model* :
In this model, we consider that the rational adversary is afraid of the environmental degradation. We suppose that the environmental degradation means that the traffic environment could be difficult to maintain because of the detection of some dishonesty. Thus, the adversary is afraid of being specified corrupted channels or the protocol abortion. Since the case of "detection of corrupted channels" is discussed above in the timid rational adversary model, we consider the case of "abortion of the protocol". Thus, we consider the following relation among the utilities:

$$u_f > u_s > u_a, \quad u_q > 0 \quad \text{and} \quad u_d = 0.$$

In this paper, we assume that the utilities are publicly known. Under this assumption, we will consider PSMT schemes in the timid rational adversary model and in the conservative rational adversary model.

4 Protocol against Timid Rational Adversary

In this section, we show that Shi et al.'s ARSMT scheme [5] works as a PSMT scheme in the timid rational adversary model. Note that their scheme (Protocol 1) uses the public channel.

Theorem 3. *If we set the parameter ℓ in Protocol 1 as*

$$\ell > 1 + \log \frac{(n-1)(.99u_f - u_s - u_d)}{-u_d}$$

and if the adversary corrupts $t < n$ channels, then Protocol 1, which uses the public channel, works as a PSMT scheme in the timid rational adversary model.

Remark. In the above, the constant .99 is not essential value. By that, we mean it is a constant close to 1.

As mentioned, Protocol 1 has the perfect privacy. Thus, in what follows, we discuss the perfect correctness of Protocol 1. Due to the construction of Protocol 1, if we can prevent the adversary from tampering during the execution of Protocol 1, then the perfect correctness can be guaranteed. To show this, we consider the expected utilities.

Strategies of the timid rational adversary is either σ_a, which denotes "eavesdropping and tampering", or σ_p, which denotes "eavesdropping only". We analyze these two strategies.

Case of strategy σ_a
For Protocol 1, it is known that the failure probability of the message transmission is at most $(n-1)2^{1-\ell}$. First, we consider this failure probability a bit more. Let E be the event that the message transmission fails. Then, E can be written as $E = E_1 \vee E_2 \vee \cdots \vee E_{n-1}$, where E_i is the event the adversary successfully tampers the data over the ith channel and $\Pr[E_i] = 2^{1-\ell}$. Thus, the upper bound of the failure probability is derived by the union bound. Tampering the data over the $i$the channel is independent to tampering the data over the jth channel, we can derive the lower bound of the failure probability. Let $p = 2^{1-\ell}$ for the simplicity. By the inclusion-exclusion principle and the independence among the sub-events $E_1, E_2, \ldots, E_{n-1}$, we have $\Pr[E] \geq p - (n-1)p^2$. Since the value p is a decreasing function in ℓ, we can say that $\Pr[E] \geq p - (n-1)p^2 > .99p$ in the asymptotic sense.

So if the rational adversary selects σ_a as his strategy, the adversary makes a failure with probability $.99(n-1)2^{1-\ell}$ at least and the utility u_f, and the corrupting channel is detected but the message transmission is succeeded with probability $1-(n-1)2^{1-\ell}$ at least and the utility $u_s + u_d$. Since $u_s + u_d < u_f$, we may assume that $u_s + u_d < .99u_f$. (We can take a larger constant, say .9999, as needed.)

Thus, we have that the expected utility satisfies

$$\begin{aligned} u(\sigma_a) &= u_f \cdot \Pr[E] + (u_s + u_d) \cdot \Pr[\bar{E}] \\ &> .99u_f(n-1)2^{1-\ell} + (u_s + u_d)(1 - (n-1)2^{1-\ell}). \end{aligned}$$

Case of strategy σ_p
If the rational adversary does not tamper, the receiver can reliably receive a message. And the sender and the receiver cannot detect any channel that is corrupted but not tampering. So the expected utility of the rational adversary who selects strategy σ_p is

$$u(\sigma_p) = u_s.$$

The rational adversary chooses the strategy whose expected utility is the highest. Since $\ell > 1 + \log(n-1)(.99u_f - u_s - u_d)/(-u_d)$ from the assumption, it holds that $u(\sigma_p) > u(\sigma_a)$, that is,

$$u_s > .99u_f(n-1)2^{1-\ell} + (1 - (n-1)2^{1-\ell})(u_s + u_d).$$

Thus, the rational adversary does not tamper in Protocol 1. Therefore, Protocol 1 (by setting appropriately the parameter ℓ) works as a PSMT scheme in the timid rational adversary model if the adversary corrupts $t < n$ channels.

Remark.
In the above discussion, we do not use all the properties in the timid rational adversary model. Thus, Theorem 3 can be generalized as follows.

Theorem 4. *Suppose that the rational adversary has the following relation of utilities:*

$$(.99u_f - u_s - u_d)/u_d < 0.$$

Then, Protocol 1 (by setting appropriately the parameter ℓ) works as a PSMT scheme against the above rational adversary if the adversary corrupts $t < n$ channels.

5 Protocol against Conservative Rational Adversary

Remember that the conservative rational adversary is afraid of the protocol abortion. In this section, we give a PSMT scheme in the conservative rational adversary model. Unlike the case of the timid rational adversary, we can construct a scheme without resorting the public channel. First, we give a description of the PSMT scheme.

Protocol 2

Let n be the number of channels and m a message that the sender $\mathcal{S}$ wants to send to the receiver $\mathcal{R}$.

1. For the ith channel with $1 \leq i \leq n$, $\mathcal{R}$ chooses a polynomial of degree $n-1$ whose coefficients are over finite field $\mathbb{F}_q$ $(m < q)$ and sends each value $f(i) \in \mathbb{F}_q$ over the ith channel.
2. By coin-flipping, $\mathcal{S}$ executes Sub-step 2(a) with probability p or Sub-step 2(b) with probability $1-p$.
   (a) Upon receiving $\tilde{f}(1), \tilde{f}(2), \ldots, \tilde{f}(n)$ from $\mathcal{R}$, $\mathcal{S}$ recovers a polynomial $\tilde{f}(x)$ which interpolates the data by using the Lagrange interpolation, and sends $s = \tilde{f}(0) + m$ over all the channels.
   (b) $\mathcal{S}$ sends the received data $(\tilde{f}(1), \tilde{f}(2), \ldots, \tilde{f}(n))$ over all the channels.
3. If the received data are not the same according to each channel, $\mathcal{R}$ aborts the protocol execution. If the received data is a single data s then $\mathcal{S}$ executes Sub-step 3(a), otherwise (the received data is a multiple data $\tilde{f}(1), \tilde{f}(2), \ldots, \tilde{f}(n)$) $\mathcal{S}$ executes Sub-step 3(b).
   (a) $\mathcal{R}$ retrieves $\tilde{m} = f(0) - s$ and terminates the execution of the protocol.
   (b) If $f(1), f(2), \ldots, f(n)$ which $\mathcal{R}$ sent in Step 1 and $\tilde{f}(1), \tilde{f}(2), \ldots, \tilde{f}(n)$ which $\mathcal{R}$ received are different, then $\mathcal{R}$ aborts the protocol execution. If these are the same, restart the protocol from Step 1.

Remark.
The number of repetitions in Protocol 2 depends on the probability parameter p and its expected number is $1/p$.

Theorem 5. *Protocol 2 with the parameter p satisfying*

$$0 < p \leq \frac{u_s - u_a}{(1 - 1/q) \cdot u_f + (1/q) \cdot u_s - u_a}$$

is a PSMT scheme in the conservative rational adversary model, if the adversary corrupts $t < n$ channels.

First, we see the perfect privacy of Protocol 2. In Protocol 2, we use Shamir's (n, n)-threshold secret sharing scheme. The receiver $\mathcal{R}$ sends $f(i)$, and the sender $\mathcal{S}$ calculates $\tilde{f}(x)$ from $\tilde{f}(1), \tilde{f}(2), \ldots, \tilde{f}(n)$ which $\mathcal{S}$ received by using the Lagrange interpolation, and sends $s = \tilde{f}(0) + m$ to all over the channels. So the adversary knows s and $f(i)$ which is sent over the at most $n-1$ corrupted channels. But because of the perfect secrecy of Shamir's scheme, the adversary cannot calculate $\tilde{f}(x)$ even if the adversary collects $n-1$ shares. So the adversary cannot guess the value of s and thus the adversary cannot know any information about m. Therefore, the perfect privacy holds.

Next, we move to the correctness of Protocol 2.

Strategies of the conservative rational adversary are "eavesdropping and tampering" and and "eavesdropping only". Now we respectively analyze these strategies.

Case of strategy $\boldsymbol{\sigma_a}$

The utility when the rational adversary tampers depends on the the action of $\mathcal{S}$ in Step 2. In the case that 2(a) is executed, if the adversary tampers $f(i)$, $\mathcal{S}$ cannot calculate the correct $\tilde{f}(x)$, and $\tilde{f}(0)$ is also different from $f(0)$ with probability $1 - 1/q$. Then $\mathcal{R}$ cannot get the correct message better than the random guessing. The utility is u_s if $\tilde{f}(0) = f(0)$ and u_f otherwise.

In the case that 2(b) is executed, if the adversary tampers $f(1), f(2), \ldots, f(n)$, $\mathcal{R}$ can detect tampering channels by comparing $f(1), f(2), \ldots, f(n)$ with $\tilde{f}(1), \tilde{f}(2), \ldots, \tilde{f}(n)$ which $\mathcal{S}$ sends, and $\mathcal{R}$ aborts. Even if the adversary also tampers $\tilde{f}(i)$, $\mathcal{R}$ also aborts by the disagreed data. In this case, the utility is u_a.

Then, the expected utility of the rational adversary who selects strategy σ_a is

$$u(\sigma_a) = p(1 - 1/q) \cdot u_f + (p/q) \cdot u_s + (1 - p) \cdot u_a.$$

Case of strategy $\boldsymbol{\sigma_p}$

If the rational adversary does not tamper, $\mathcal{R}$ can reliably receive a message. And $\mathcal{S}$ and $\mathcal{R}$ cannot detect any channel that is corrupted but not tampered. So the expected utility of the rational adversary who selects strategy σ_p is

$$u(\sigma_p) = u_s.$$

The rational adversary chooses the strategy whose expected utility is the highest, it holds that $u(\sigma_p) > u(\sigma_a)$, that is,

$$u_s > p(1 - 1/q) \cdot u_f + (p/q) \cdot u_s + (1 - p) \cdot u_a,$$

since $p < (u_s - u_a)/((1 - 1/q) \cdot u_f + (1/q) \cdot u_s - u_a) < 1$.

Thus, the rational adversary does not tamper in Protocol 2. Therefore Protocol 2 works as a PSMT scheme in conservative rational adversary model, if the adversary corrupts $t < n$ channels.

Remark.

In the above discussion, we do not use all the properties in the conservative rational adversary model. Thus, Theorem 5 can be generalized as follows.

Theorem 6. *Suppose that the rational adversary has the following relation of utilities:*

$$u_f > u_s > u_a.$$

Then, Protocol 2 (by setting appropriately the parameter p) works as a PSMT scheme against the above rational adversary if the adversary corrupts $t < n$ channels.

6 Conclusion

We have incorporated the notion of rationality in the game theory into secure message transmission. We have considered "rational adversary" who "fears for being detected of the corrupted channels" and "avoids the abortion of the protocol" as natural scenarios. In the first rational adversary scenario (i.e., timid rational adversary model), we have showed that the ARSMT protocol (Protocol 1), which uses the public channel, by Shi et al. [5] works as a PSMT scheme against $t < n$ corruptions. In the second rational adversary scenario (i.e., conservative rational adversary model), we have considered another protocol (Protocol 2), which does not use the public channel, and shown that Protocol 2 achieves PSMT against $t < n$ corruptions. These bounds in the rational adversary model make a contrast to the bound $t < n/2$ in the conventional cryptographic adversary in PSMT.

References

1. D. Dolev, C. Dwork, O. Waarts, and M. Yung, "Perfectly secure message transmission", *J. ACM* 40(1):17–47, 1993.
2. K. Kurosawa and K. Suzuki, "Truly efficient 2-round perfectly secure message transmission scheme", *IEEE Transactions on Information Theory* 55(11):5223–5232, 2009.
3. M. Franklin and R. N. Wright, "Secure communication in minimal connectivity models", *J. Cryptology* 13(1):9–30, 2000.
4. J. A. Garay and R. Ostrovsky, "Almost-everywhere secure computation", *Advances in Cryptology — EUROCRYPT 2008*, LNCS 4965, pp.307–323, Springer, 2008.
5. H. Shi, S. Jiang, R. Safavi-Naini, and M. A. Tuhin, "On optimal secure message transmission by public discussion", *IEEE Transactions on Information Theory* 57(1):572–585, 2011.
6. J. Halpern and V. Teague, "Rational secret sharing and multiparty computation", in *Proc. 36th Annual ACM Symposium on Theory of Computing*, pp.623–632, ACM, 2004.
7. A. Shamir, "How to share a secret", *Communications of the ACM* 22(11):612–613. 1979.
8. S. D. Gordon and J. Katz, "Rational secret sharing, revisited", in *Proc. 5th International Conference on Security and Cryptography for Networks*, LNCS 4116, pp.229–241, Springer, 2006.
9. S. Micali and A. Shelat, "Purely rational secret sharing", in *Proc. 6th Theory of Cryptography Conference*, LNCS 5444, pp.54–71, Springer, 2009.

10. G. Asharov and Y. Lindell, "Utility dependence in correct and fair rational secret sharing", *J. Cryptol.* 24(1):157-—202, 2011.
11. G. Fuchsbauer, J. Katz and D. Naccache, "Efficient rational secret sharing in standard communication networks", in *Proc. 7th Theory of Cryptography Conference*, LNCS 5978, pp.419–436, Springer, 2010..
12. A. Kawachi, Y. Okamoto, K. Tanaka and K. Yasunaga, "General constructions of rational secret sharing with expected constant-round reconstruction", *The Computer Journal*, to appear.
13. A. Groce, J. Katz, A. Thiruvengadam, and V. Zikas, "Byzantine agreement with a rational adversary", in *Proc. ICALP 2012*, Vol.2, LNCS 7392, pp.561–572, Springer, 2012.
14. M. Pease, R. Shostak, and L. Lamport, "Reaching agreement in the presence of faults", *J. ACM* 27(2):228–234, 1980.
15. J. Katz, "Bridging game theory and cryptography: Recent results and future directions", in *Proc. 5th Theory of Cryptography Conference*, LNCS 4948, pp.251–272, Springer, 2008.
16. Y. Dodis and T. Rabin, "Cryptography and game theory", in N. Nisan, T. Roughgarden, E. Tardos, and V.V. Vazirani (eds), *Algorithmic Game Theory*, pp.181–207, Cambridge Univ. Press, 2007.
17. M. Wegman and J. Carter, "New hash functions and their use in authentication and set equality", *J. Comput. Syst. Sci.* 22(2):265–279, 1981.
18. J. von Neumann and O. Morgenstern, *Theory of Games and Economic Behavior*, Princeton University Press, 2007.