Perfectly Secure Message Transmission Against Rational Timid Adversaries

Maiki Fujita[1], Kenji Yasunaga[2], and Takeshi Koshiba[3](✉)

[1] Graduate School of Science and Engineering, Saitama University, Saitama, Japan
[2] Graduate School of Information Science and Technology, Osaka University, Osaka, Japan
yasunaga@ist.osaka-u.ac.jp
[3] Faculty of Education and Integrated Arts and Sciences, Waseda University, Tokyo, Japan
tkoshiba@waseda.jp

Abstract. Secure Message Transmission (SMT) is a two-party cryptographic protocol by which the sender can securely and reliably transmit messages to the receiver using multiple channels. It is assumed that an adversary corrupts a subset of the channels, and makes eavesdropping and tampering over the corrupted channels. In this work, we consider a game-theoretic security model for SMT. Specifically, we introduce a rational adversary who has the preference for the outcome of the protocol execution. We show that, under some reasonable assumption on the adversary's preference, even if the adversary corrupts all but one of the channels, it is possible to construct SMT protocols with perfect security against rational adversaries. More specifically, we consider "timid" adversaries who prefer to violate the security requirement of SMT, but do not prefer the tampering actions to be detected. In the traditional cryptographic setting, perfect SMT can be constructed only when the adversary corrupt a minority of the channels. Our results demonstrate a way of circumventing the impossibility results of cryptographic protocols based on a game-theoretic approach.

Keywords: Cryptography · Secure message transmission
Game theory · Rational adversary

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.

L. Bushnell et al. (Eds.): GameSec 2018, LNCS 11199, pp. 127–144, 2018.
https://doi.org/10.1007/978-3-030-01554-1_8

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. [10], is a cryptographic protocol by which a sender can transmit messages through multiple channels in a secure way. Even if any adversary corrupts t out of n channels and makes eavesdropping and tampering over the corrupted channels, the messages are securely and correctly transmitted to the receiver by using SMT. The requirements for SMT consist of *privacy* and *reliability*. The privacy guarantees that the adversary can obtain no information about the transmitted message, and the reliability does that the message transmitted by the sender is recovered by the receiver. If an SMT protocol satisfies both the requirements in the perfect sense, the protocol is called a *perfect* SMT. The most round-efficient perfect SMT is given by Kurosawa and Suzuki [29]. Dolev et al. [10] showed that any one-round perfect SMT must satisfy $t < n/3$ and any perfect SMT whose round complexity is at least two must satisfy $t < n/2$. Franklin and Wright [11] defined *almost-reliable* SMT, which allows transmission failures of small probability. They showed that almost-reliable SMT against $t < n$ corruptions is achievable by using a public channel in addition to the normal channels. Later, Garay and Ostrovsky [15] and Shi et al. [32] gave the most round-efficient almost-reliable SMT protocols using public channels.

In the standard setting in cryptography, the participants are assumed to be either honest or malicious. The former follow the protocol description honestly, and the later may deviate from the protocol maliciously. In general, malicious behavior may be illegal and involve some risks, which implies that adversaries in the standard cryptographic setting behave maliciously regardless of their risk. However, some adversary in reality may decide his behavior by taking the risk into account. To capture such situations, we incorporate the notion of "rational" participants of game theory into cryptography. Halpern and Teague [22] firstly studied the rational behavior of participants in cryptography in the context of secret sharing. Since then, rational secret sharing has been intensively studied [1,4,12,16,26–28]. Moreover, there have been many studies using game-theoretic analysis of cryptographic primitives/protocols, including two-party computation [3,18], leader election [2,17], Byzantine agreement [19], consensus [23], public-key encryption [35,36], delegation of computation [5,7,8,20,21,24], and protocol design [13,14]. Among them, several work [5,13,19–21] used the rationality of adversaries to circumvent the existing impossibility results.

Groce et al. [19] studied the problem of Byzantine agreement in the presence of a rational adversary. They showed that, given some knowledge of the adversary's preference, perfectly secure Byzantine agreement is possible for t corruptions among n players for any $t < n$, for which the impossibility against $t \geq n/2$ corruptions is known in the standard setting.

In this work, we show that the impossibility results of SMT can be also circumvented by considering the rationality of adversaries. As in the case of Byzantine agreement, we introduce a rational adversary for SMT who has some preference for the outcome of the protocol execution. More specifically, we define *timid* adversaries who prefer to violate the security requirements of SMT, but do not prefer the tampering actions to be detected. For such adversaries, first we show that the almost-reliable SMT protocol of [32], which employs a tamper-proof public channel, works as a "perfect" SMT protocol. Second, we show that, for "strictly" timid adversaries, who prefer being undetected to violating the security requirements, secret sharing schemes with some robustness can be used as a non-interactive SMT protocol. Both protocols are perfectly secure against timid adversaries corrupting t out of n channels for any $t < n$, which is impossible in the standard setting of SMT protocols. In addition, we present an impossibility result of constructing SMT protocols against general timid adversaries corrupting $t \geq n/2$ channels. The result demonstrates the necessities of the tamper-proof public channel in the first protocol and the restriction of strictly timid adversaries in the second protocol. The results are summarized in Table 1.

Table 1. Summary of previous work and our results.

Adversary types	PC*	Resiliency	Security	Construction
Malicious	–	$t < n/2$	Perfect	Exist [10,29]
Malicious	–	$t \geq n/2$	Perfect	Impossible [10]
Malicious	✓	$t < n$	Almost reliable	Exist [11,15,32])
Timid	✓	$t < n$	Perfect	Exist (Theorem 4)
Strictly timid	–	$t < n$	Perfect	Exist (Theorem 5)
Timid	–	$t \geq n/2$	Perfect	Impossible (Corollary 2)

* PC represents the use of the public channel.

2 Preliminaries

2.1 Secure Message Transmission

We assume that a sender $\mathcal{S}$ and a receiver $\mathcal{R}$ are connected by n channels, and they may use an authentic and reliable *public channel*. Messages sent 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 over each channel and the public channel. The messages will be delivered before the next round starts.

The adversary $\mathcal{A}$ can corrupt at most t channels. Such an adversary is referred to as *t-adversary*. Messages sent over corrupted channels can be eavesdropped and tampered by the adversary. We assume that $\mathcal{A}$ is computationally *unbounded*.

Let $\mathcal{M}$ be the message space. In SMT, the sender tries to send a message in $\mathcal{M}$ to the receiver by using n channels and the public channel, and the receiver outputs some message after the protocol execution. For an SMT protocol Π, let

M_S denote the random variable of the message sent by $\mathcal{S}$ and M_R the message output by $\mathcal{R}$ in Π. An execution of Π can be completely characterized by the random coins of all the parties, namely, $\mathcal{S}$, $\mathcal{M}$, and $\mathcal{A}$, and the message M_S sent by $\mathcal{S}$. Let $V_A(m, r_A)$ denote the *view* of $\mathcal{A}$ when the protocol is executed with $M_S = m$ and the random coins r_A of $\mathcal{A}$. Specifically, $V_A(m, r_A)$ consists of the messages sent over the corrupted channels and the public channel when the protocol is run with $M_S = m$ and $\mathcal{A}$'s random coins r_A.

We formally define the properties of SMT protocols.

Definition 1. *A protocol between $\mathcal{S}$ and $\mathcal{R}$ is* (ε, δ)-Secure Message Transmission (SMT) against t-adversary *if the following three conditions are satisfied against any t-adversary $\mathcal{A}$.*

- Correctness*: For any $m \in \mathcal{M}$, if $M_S = m$ and $\mathcal{A}$ does not corrupt any channels, then* $\Pr[M_R = m] = 1$*;*
- Privacy*: For any $m_0, m_1 \in \mathcal{M}$ and $r_A \in \{0,1\}^*$, it holds that*

$$\mathrm{SD}(V_A(m_0, r_A), V_A(m_1, r_A)) \leq \varepsilon,$$

  where $\mathrm{SD}(X, Y)$ *denotes the statistical distance between two random variables X and Y over a set Ω, which is defined by*

$$\mathrm{SD}(X, Y) = \frac{1}{2} \sum_{u \in \Omega} |\Pr[X = u] - \Pr[Y = u]|\,;$$

- Reliability*: For any message $m \in \mathcal{M}$, when $M_S = m$,*

$$\Pr[M_R \neq m] \leq \delta,$$

  where the probability is taken over the random coins of $\mathcal{S}$, $\mathcal{R}$, and $\mathcal{A}$.

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

For perfect SMT, Dolev *et al.* [10] showed the below.

Theorem 1 ([10]). *Perfect SMT protocols against t-adversary are achievable if and only if $t < n/2$.*

2.2 Secure Message Transmission with Public Channel

In this paper, we will employ an almost-reliable SMT protocol given by Shi, Jiang, Safavi-Naini, and Tuhin [32], and refer it as the SJST protocol. Note that we only use some specific properties of the SJST protocol in the security analysis. Thus, other protocols, such as one by Garay and Ostrovsky [15], can also be employed instead of the SJST protocol.

Let us review the SJST protocol, which uses the public channel. The protocol is based on the simple protocol for "static" adversaries in which the sender sends a random key R_i over the i-th channel for each $i \in \{1, \ldots, n\}$, and the encrypted message $c = m \oplus R_1 \oplus \cdots \oplus R_n$ over the public channel. Suppose that the adversary sees the messages sent over the corrupted channels, but does not change them. Since the adversary cannot see at least one key R_j when corrupting less than n channels, the mask $R_1 \oplus \cdots \oplus R_n$ for the encryption looks random for the adversary. Thus, the message m can be securely encrypted and reliably sent through the public channel. To cope with "active" adversaries, who may change messages sent over the corrupted channels, the SJST protocol employs a mechanism for detecting the adversary's tampering by using hash functions. Specifically, the *universal* hash functions (see Appendix A) satisfy the following property: when a pair of keys (r_i, R_i) is changed to $(r'_i, R'_i) \neq (r_i, R_i)$, the hash value for (r_i, R_i) is different from that for (r'_i, R'_i) with high probability if the hash function is chosen randomly after the tampering occurred. In the SJST protocol, the sender sends a pair of keys (r_i, R_i) over the i-th channel. Then, the receiver chooses n universal hash functions h_i's, and sends them over the public channel. By comparing hash values for (r_i, R_i)'s sent by the sender with those for (r'_i, R'_i)'s received by the receiver, they can identify the channels for which messages, i.e., keys, were tampered with. By ignoring keys sent over such channels, the sender can correctly encrypt a message m with untampered keys and send the encryption reliably over the public channel.

We describe the SJST protocol below, which is a three-round protocol, and achieves the reliability with $\delta = (n-1) \cdot 2^{1-\ell}$, where ℓ is the length of hash values.

Protocol 1 (The SJST protocol [32]**).** Let n be the number of channels, $m \in \mathcal{M}$ the message to be sent by the sender $\mathcal{S}$, and $H = \{h \colon \{0,1\}^k \to \{0,1\}^\ell\}$ a class of universal hash functions.

1. For each $i \in \{1, \ldots, n\}$, $\mathcal{S}$ chooses $r_i \in \{0,1\}^\ell$ and $R_i \in \{0,1\}^k$ uniformly at random, and sends the pair (r_i, R_i) over the i-th channel.
2. For each $i \in \{1, \ldots, n\}$, $\mathcal{R}$ receives (r'_i, R'_i) through the i-th channel, and then chooses $h_i \leftarrow H$ uniformly at random. If $|r'_i| \neq \ell$ or $|R'_i| \neq k$, set $b_i = 1$, and otherwise, set $b_i = 0$. Then, set $T'_i = r'_i \oplus h_i(R'_i)$, and $H_i = (h_i, T'_i)$ if $b_i = 0$, and $H_i = \perp$ otherwise. Finally, $\mathcal{R}$ sends $(B, H_1, \ldots, H_n)$ over the public channel, where $B = (b_1, \ldots, b_n)$.
3. $\mathcal{S}$ receives $(B, H_1, \ldots, H_n)$ through the public channel. For each $i \in \{1, \ldots, n\}$ with $b_i = 0$, $\mathcal{S}$ computes $T_i = r_i \oplus h_i(R_i)$, and sets $v_i = 0$ if $T_i = T'_i$, and $v_i = 1$ otherwise. Then, $\mathcal{S}$ sends (V, c) over the public channel, where $V = (v_1, \ldots, v_n)$, and $c = m \oplus (\bigoplus_{v_i=0} R_i)$.
4. On receiving (V, c), $\mathcal{R}$ recovers $m = c \oplus (\bigoplus_{v_i=0} R_i)$.

Theorem 2 ([32]**).** *The SJST protocol is* $(0, (n-1) \cdot 2^{1-\ell})$*-SMT against* t*-adversary for any* $t < n$.

We can find a complete proof of the above theorem in [32]. For self-containment, we give a brief sketch of the proof.

- *Privacy*: The adversary can get $c = m \oplus (\bigoplus_{v_i=0} R_i)$ through the public channel. Since m is masked by uniformly random R_i's, the adversary has to corrupt all the i-th channels with $v_i = 0$ to recover m. However, since any t-adversary can corrupt at most t $(< n)$ channels, the adversary can cause $v_i = 1$ for at most $n-1$ i's. Hence, there is at least one i with $v_i = 0$, for which the adversary cannot obtain R_i. Thus, the protocol satisfies the perfect privacy.
- *Reliability*: Since the protocol uses the public channel at the second and the third rounds, the adversary can tamper with channels only at the first round. Suppose that the adversary tampers with (r_i, R_i). If $R_i \neq R'_i$ and $T_i = T'_i$, then $\mathcal{R}$ would recover a wrong message, but the tampering is not detected. It follows from Lemma 1 that the probability that the above event happens is at most $(n-1)2^{1-\ell}$. Thus, the protocol achieves the reliability with $\delta = (n-1) \cdot 2^{1-\ell}$.

2.3 Robust Secret Sharing

Secret sharing, introduced by Shamir [31] and Blackley [6], enables us to distribute the secret information in a secure way. Let $s \in \mathbb{F}$ be a secret from some finite field $\mathbb{F}$. A (threshold) secret-sharing scheme gives a way for distributing s into n shares $s_1, \ldots, s_n$ such that, for some parameter $t > 0$, (1) any t shares give no information about s; and (2) any $t+1$ shares uniquely determine s. Shamir [31] give a scheme based on polynomial evaluations for any $t < n$.

Shamir's scheme also achieves *robustness* in the sense that even if $t/3$ shares are maliciously tampered, the original secret can be correctly recovered. Although the robustness is a desirable property, it is known that robust secret sharing is impossible when $t/2$ shares are tampered with [25].

In this work, we need a weaker notion of robustness in which any tampering actions should be detected with high probability. Such robust secret sharing was studied by Cramer et al. [9]. They introduced the notion of *algebraic manipulation detection (AMD) codes*, and presented a simple way for constructing robust secret sharing from *linear* secret sharing and AMD codes. More precisely, the robustness required for our protocol is slightly different from one defined in [9].[1]

Definition 2. *Let t, n be positive integers with $t < n$. A (t, n, δ)*-robust secret sharing *scheme with range $\mathcal{G}$ consists of two algorithms* $(\mathsf{Share}, \mathsf{Reconst})$ *satisfying the following conditions:*

- Correctness*: For any $s \in \mathcal{G}$ and $I \subseteq \{1, \ldots, n\}$ with $|I| > t$,*

$$\Pr\left[\mathsf{Reconst}\left(\{i, s_i\}_{i \in I}\right) = s\right] = 1,$$

where $(s_1, \ldots, s_n) \leftarrow \mathsf{Share}(s)$.

[1] The robustness in [9] requires that the output of the reconstruction algorithm should be either the original message or the failure symbol with high probability. Namely, it is allowed to recover the original message even if some shares are tampered with. In Definition 2, we require that if some shares are tampered with, the output of the reconstruction algorithm should be the failure symbol.

- Perfect Privacy*: For any $s, s' \in \mathcal{G}$ and $I \subseteq \{1, \ldots, n\}$ with $|I| \leq t$,

$$\mathrm{SD}\left(\{s_i\}_{i \in I}, \{s'_i\}_{i \in I}\right) = 0,$$

where $(s_1, \ldots, s_n) \leftarrow \mathsf{Share}(s)$ *and* $(s'_1, \ldots, s'_n) \leftarrow \mathsf{Share}(s')$*.*
- Robustness*: For any $s \in \mathcal{G}$ and $I \subseteq \{1, \ldots, n\}$ with $|I| \leq t$ and adversary $\mathcal{A}$, if $\tilde{s}_i \neq s_i$ for some $i \in \{1, \ldots, n\}$,*

$$\Pr\left[\mathsf{Reconst}\left(\{i, \tilde{s}_i\}_{i \in \{1, \ldots, n\}}\right) \neq \bot\right] \leq \delta,$$

where

$$\tilde{s}_i = \begin{cases} \mathcal{A}(i, s, \{s_i\}_{i \in I}) & \textit{if } i \in I \\ s_i & \textit{if } i \notin I \end{cases}$$

and $(s_1, \ldots, s_n) \leftarrow \mathsf{Share}(s)$*.*

We can see that the construction of [9] satisfies the above definition. Specifically, we have the following theorem, which will be used in our protocol against strictly timid adversaries in Sect. 4.2. See Appendix B for the proof.

Theorem 3. *Let $\mathbb{F}$ be a finite field of size q and characteristic p, and d an integer such that $d+2$ is not divisible by p. For any positive integers t and n satisfying $t < n \leq qd$, there is an explicit and efficient scheme of $(t, n, (d+1)/q)$-robust secret sharing with range $\mathbb{F}^d$, where each share is an element of $\mathbb{F}^{d+2}$.*

3 Rational Secure Message Transmission

We define our security model of SMT in the presence of a rational adversary. A rationality of the adversary is characterized by a *utility function* which represents the preference of the adversary over possible outcomes of the protocol execution.

We can consider various preferences of the adversary regarding the SMT protocol execution. The adversary may prefer to violate the privacy or the reliability of SMT protocols. In addition, the adversary may prefer to violate the above properties without the detection of tampering actions. Here, we consider the adversary who prefers (1) to violate the privacy, (2) to violate the reliability, (3) the tampering actions to be undetected, and (4) the protocol execution to be finished without abort.

To define the utility function, we specify the SMT game as follows.

The SMT Game. First set four parameters $\mathsf{guess} = \mathsf{suc} = \mathsf{detect} = \mathsf{abort} = 0$. Given an SMT protocol Π with the message space $\mathcal{M}$, choose $m \in \mathcal{M}$ uniformly at random, and run the protocol Π in which the message to be sent is $M_S = m$. In the protocol execution, as in the usual SMT, the adversary $\mathcal{A}$ can corrupt at most t channels, and tamper with any messages sent over the corrupted channels. If the protocol finishes with abort, set $\mathsf{abort} = 1$. If the sender or the receiver sends a special message "DETECTION" during the execution, set $\mathsf{detect} = 1$. After running the protocol, the receiver outputs M_R, and the adversary outputs M_A.

If $M_R = M_S$, set $\mathsf{suc} = 1$. If $M_A = M_S$, set $\mathsf{guess} = 1$. The outcome of the game is $(\mathsf{guess}, \mathsf{suc}, \mathsf{detect}, \mathsf{abort})$.

The utility of the adversary is defined as the expected utility in the SMT game.

Definition 3 (Utility). *The utility $u(\mathcal{A}, U)$ of the adversary $\mathcal{A}$ with utility function U is the expected value $E[U(\mathsf{out})]$, where U is a function that maps the outcome $\mathsf{out} = (\mathsf{guess}, \mathsf{suc}, \mathsf{detect}, \mathsf{abort})$ of the SMT game by $\mathcal{A}$ to real values, and the probability is taken over the random coins of the sender, the receiver, and the adversary, and a random choice of message M_S.*

The utility function U characterizes the type of adversaries. If the adversary has the preferences (1)-(4) as above, the utility function may have the property such that for any two outcomes $\mathsf{out} = (\mathsf{guess}, \mathsf{suc}, \mathsf{detect}, \mathsf{abort})$ and $\mathsf{out}' = (\mathsf{guess}', \mathsf{suc}', \mathsf{detect}', \mathsf{abort}')$ of the SMT game,

1. $U(\mathsf{out}) > U(\mathsf{out}')$ if $\mathsf{guess} > \mathsf{guess}'$, $\mathsf{suc} = \mathsf{suc}'$, $\mathsf{detect} = \mathsf{detect}'$, and $\mathsf{abort} = \mathsf{abort}'$;
2. $U(\mathsf{out}) > U(\mathsf{out}')$ if $\mathsf{guess} = \mathsf{guess}'$, $\mathsf{suc} < \mathsf{suc}'$, $\mathsf{detect} = \mathsf{detect}'$, and $\mathsf{abort} = \mathsf{abort}'$;
3. $U(\mathsf{out}) > U(\mathsf{out}')$ if $\mathsf{guess} = \mathsf{guess}'$, $\mathsf{suc} = \mathsf{suc}'$, $\mathsf{detect} < \mathsf{detect}'$, and $\mathsf{abort} = \mathsf{abort}'$;
4. $U(\mathsf{out}) > U(\mathsf{out}')$ if $\mathsf{guess} = \mathsf{guess}'$, $\mathsf{suc} = \mathsf{suc}'$, $\mathsf{detect} = \mathsf{detect}'$, and $\mathsf{abort} < \mathsf{abort}'$.

Based on the utility function of the adversary, we define the security of rational secure message transmission.

Definition 4 (Security of RSMT). *An SMT protocol Π is* perfectly secure against rational t-adversaries with utility function U *if there is a t-adversary $\mathcal{B}$ such that for any t-adversary $\mathcal{A}$,*

1. Perfect security*: Π is $(0, 0)$-SMT against $\mathcal{B}$; and*
2. Nash equilibrium*: $u(\mathcal{A}, U) \leq u(\mathcal{B}, U)$ in the SMT game.*

The perfect security guarantees that an adversary $\mathcal{B}$ is *harmless*. The Nash equilibrium guarantees that no adversary $\mathcal{A}$ can gain more utility than $\mathcal{B}$. Thus, the above security of RSMT implies that no adversary $\mathcal{A}$ can gain more utility than the harmless adversary. Namely, the adversary does not have an incentive to deviate from the strategy of the harmless adversary $\mathcal{B}$.

In the security proof of our protocol, we will consider an adversary $\mathcal{B}$ who does not corrupt any channels, and outputs M_A by choosing a message uniformly at random from $\mathcal{M}$. For such $\mathcal{B}$, the perfect privacy and reliability immediately follows if Π satisfies the correctness.

4 Protocols Against Timid Adversaries

We present several protocols that are secure against *timid* rational adversaries. Timid adversaries are rational adversaries who firstly do not prefer the tampering to be detected, and secondly prefer to violate the reliability.

More formally, utility function U of such adversaries should have the properties such that

1. $U(\mathsf{out}) > U(\mathsf{out}')$ if $\mathsf{suc} < \mathsf{suc}'$ and $\mathsf{detect} = \mathsf{detect}'$; and
2. $U(\mathsf{out}) > U(\mathsf{out}')$ if $\mathsf{suc} = \mathsf{suc}'$ and $\mathsf{detect} < \mathsf{detect}'$,

where $\mathsf{out} = (\mathsf{guess}, \mathsf{suc}, \mathsf{detect}, \mathsf{abort})$ and $\mathsf{out}' = (\mathsf{guess}', \mathsf{suc}', \mathsf{detect}', \mathsf{abort}')$ are the outcomes of the SMT game. Let U_{timid} be the set of utility functions that satisfy the above conditions.

In addition, timid adversaries may have the following property:

3. $U(\mathsf{out}) > U(\mathsf{out}')$ if $\mathsf{suc} > \mathsf{suc}'$ and $\mathsf{detect} < \mathsf{detect}'$.

Let $U^{\mathsf{st}}_{\mathsf{timid}}$ be the set of utility functions satisfying the above three conditions. An adversary is said to be *timid* if his utility function is in U_{timid}, and *strictly timid* if the utility function is in $U^{\mathsf{st}}_{\mathsf{timid}}$.

In the analysis of our protocols, we need the following four values of utility:

- u_1 is the utility when $\Pr[\mathsf{guess} = 1] = 1/|\mathcal{M}|$, $\mathsf{suc} = 0$, $\mathsf{detect} = 0$, and $\mathsf{abort} = 0$;
- u_2 is the utility when $\Pr[\mathsf{guess} = 1] = 1/|\mathcal{M}|$, $\mathsf{suc} = 1$, $\mathsf{detect} = 0$, and $\mathsf{abort} = 0$;
- u_3 is the utility when $\Pr[\mathsf{guess} = 1] = 1/|\mathcal{M}|$, $\mathsf{suc} = 0$, $\mathsf{detect} = 1$, and $\mathsf{abort} = 0$;
- u_4 is the utility when $\Pr[\mathsf{guess} = 1] = 1/|\mathcal{M}|$, $\mathsf{suc} = 1$, $\mathsf{detect} = 1$, and $\mathsf{abort} = 0$;

It follows from the properties of utility functions in U_{timid} that the relations $u_1 > \max\{u_2, u_3\}$ and $\min\{u_2, u_3\} > u_4$ hold. For utility functions in $U^{\mathsf{st}}_{\mathsf{timid}}$, it holds that $u_1 > u_2 > u_3 > u_4$.

4.1 Protocol with Public Channel

We show that the SJST protocol of [32] works as a perfect SMT protocol against timid adversaries. More specifically, we slightly modify the SJST protocol such that in the second and the third rounds, if $b_i = 1$ in B or $v_j = 1$ in V for some $i, j \in \{1, \ldots, n\}$, the special message "DETECTION" is also sent together. We clarify the parameters for which the SJST protocol works as RSMT against timid adversaries.

Theorem 4. *If the parameter ℓ in the SJST protocol satisfies*

$$\ell \geq \max\left\{1 + \log t + \log \frac{u_3 - u_4}{u_2 - u_4 - \alpha}, 1 + \frac{1}{t} \log \frac{u_1 - u_3}{\alpha}\right\}$$

for some $\alpha \in (0, u_2 - u_4)$, then the protocol is perfectly secure against rational t-adversaries with utility function $U \in U_{\mathsf{timid}}$ for any $t < n$.

Proof. We consider the adversary $\mathcal{B}$ in Definition 4 such that $\mathcal{B}$ does not corrupt any channels, and outputs a uniformly random message from $\mathcal{M}$ as M_A. Then, the perfect security of Definition 4 immediately follows.

Next, we show that the strategy of $\mathcal{B}$ is a Nash equilibrium. Note that $u(\mathcal{B}, U) = u_2$, since $\Pr[\mathsf{guess} = 1] = \Pr[M_A = M_S] = 1/|\mathcal{M}|$ in the SMT game. Thus, it is sufficient to show that $u(\mathcal{A}, U) \leq u_2$ for any t-adversary $\mathcal{A}$. Also, note that, since the SJST protocol achieves the perfect privacy, it holds that $\Pr[\mathsf{guess} = 1] = 1/|\mathcal{M}|$ for any t-adversary.

Since messages in the second and the third rounds are sent through the public channel, the adversary $\mathcal{A}$ can tamper with messages only in the first round. If $\mathcal{A}$ changes the lengths of r_i and R_i, the tampering of the i-th channel will be detected. Such channels are simply ignored in the second and third rounds. Thus, such tampering cannot increase the utility. Hence, we assume that $\mathcal{A}$ does not change the lengths of r_i and R_i in the first round.

Suppose that $\mathcal{A}$ corrupts some t channels in the first round. Namely, there are exactly t distinct i's such that $(r'_i, R'_i) \neq (r_i, R_i)$. Note that the tampering on the i-th channel such that $r'_i \neq r_i$ and $R'_i = R_i$ does not increase the probability that $\mathsf{suc} = 0$, but may increase the probability of detection. Thus, we also assume that $R'_i \neq R_i$ for all the corrupted channels. We define the following three events:

- E_1: No tampering action is detected in the protocol;
- E_2: At least one but not all tampering actions are detected;
- E_3: All the t tampering actions are detected.

Note that all the events are disjoint, and either event should occur. Namely, we have that $\Pr[E_1] + \Pr[E_2] + \Pr[E_3] = 1$. It follows from the discussion in Sect. A that the probability that the tampering action on one channel is not detected is $2^{1-\ell}$. Since each hash function h_i is chosen independently for each channel, we have that $\Pr[E_1] = 2^{(1-\ell)t}$. Similarly, we obtain that $\Pr[E_3] = (1 - 2^{1-\ell})^t$. Note that the utility when E_1 occurs is at most u_1. Also, the utilities when E_2 and E_3 occur are at most u_3 and u_4, respectively. Therefore, the utility of $\mathcal{A}$ is

$$\begin{aligned}
u(\mathcal{A}, U) &\leq u_1 \cdot \Pr[E_1] + u_3 \cdot \Pr[E_2] + u_4 \cdot \Pr[E_3] \\
&= u_3 + (u_1 - u_3) \Pr[E_1] - (u_3 - u_4) \Pr[E_3] \\
&\leq u_3 + (u_1 - u_3) 2^{(1-\ell)t} - (u_3 - u_4) \left(1 - t 2^{1-\ell}\right) \\
&\leq u_3 + \alpha - (u_3 - u_4) \left(1 - t 2^{1-\ell}\right) && (1) \\
&\leq u_2, && (2)
\end{aligned}$$

where we use the relations $\ell \geq 1 + \frac{1}{t} \log \frac{u_1 - u_3}{\alpha}$ and $\ell \geq 1 + \log t + \log \frac{u_3 - u_4}{u_2 - u_4 - \alpha}$ in (1) and (2), respectively. Thus, the utility of $\mathcal{A}$ is at most u_2, and hence the statement follows. □

If $u_2 > u_3$, which holds for strictly timid adversaries, by choosing $\alpha = u_2 - u_3$, the condition on ℓ is that

$$\ell \geq \max \left\{ 1 + \log t, 1 + \frac{1}{t} \log \frac{u_1 - u_3}{u_2 - u_3} \right\}.$$

4.2 Protocol Without Public Channel Against Strictly Timid Adversaries

We show that, under the condition that $u_2 > u_3$, robust secret sharing of Definition 2 gives a non-interactive perfect SMT protocol. Namely, we can construct a non-interactive protocol for strictly timid adversaries.

Let $(\mathsf{Share}, \mathsf{Reconst})$ be a (t, n, δ)-robust secret sharing scheme with range $\mathcal{M}$. In the protocol, given a message $m \in \mathcal{M}$, the sender generates n shares $(s_1, \ldots, s_n)$ by $\mathsf{Share}(m)$, and sends each s_i over the i-th channel. The receiver simply recovers the message by $\mathsf{Reconst}(\{i, \tilde{s}_i\}_{i\in\{1,\ldots,n\}})$, where $\tilde{s}_i$ is the received message over the i-th channel.

Theorem 5. *The above protocol based on a (t, n, δ)-robust secret sharing scheme is perfectly secure against rational t-adversaries with utility function $U \in U^{\mathsf{st}}_{\mathsf{timid}}$ if U satisfies that $u_2 > u_3$ and*

$$\delta \leq \frac{u_2 - u_3}{u_1 - u_3}.$$

Proof. As in the proof of Theorem 4, we consider $\mathcal{B}$ who does not corrupt any channels, and output a random message as M_A. Then, the perfect security immediately follows.

We show that, for any t-adversary $\mathcal{A}$, $u(\mathcal{A}, U) \leq u(\mathcal{B}, U)$. As discussed in the proof of Theorem 4, it is sufficient to prove that $u(\mathcal{A}, U) \leq u_2$ for any $\mathcal{A}$. Since the underlying secret sharing has the perfect privacy, we have that $\Pr[\mathsf{guess} = 1] = 1/|\mathcal{M}|$ for any t-adversary. Suppose $\mathcal{A}$ corrupts some t channels and alters some messages s_i into different $\tilde{s}_i$. It follows from the robustness of secret sharing that the tampering actions is detected with probability at least $1 - \delta$, in which case the secret is not recovered. Thus, the utility of $\mathcal{A}$ is

$$\begin{aligned} u(\mathcal{A}, U) &\leq (1 - \delta)u_3 + \delta u_1 \\ &\leq u_2, \qquad (3) \end{aligned}$$

where (3) follows from the assumption. Therefore, the statement follows. □

The following corollary immediately follows.

Corollary 1. *Let $\mathbb{F}$ be a finite field of size $q = 2^\ell$, and d be any odd integer. The non-interactive protocol based on Theorem 3 is an SMT protocol with message space $\mathbb{F}^d$ that is perfectly secure against rational t-adversaries with utility function $U \in U^{\mathsf{st}}_{\mathsf{timid}}$ for any $t < n \leq 2^\ell d$ if*

$$\ell \geq \log(d + 1) + \log \frac{u_1 - u_3}{u_2 - u_3}.$$

5 Impossibility Result for General Timid Adversaries

We show that there is no RSMT protocol without public channel that is secure against general timid t-adversaries for $t \geq n/2$. The result implies that the use of the public channel in Theorem 4 is necessary for achieving $t \geq n/2$. It also demonstrates the necessity of restricting the utility in Theorem 5 for constructing protocols for $t \geq n/2$ without using public channels.

Theorem 6. *For any SMT protocol without public channel that is perfectly secure against rational t-adversaries with utility function $U \in U_{\mathsf{timid}}$, if U has the relation*

$$u_2 < \frac{1}{2}\left(1 - \frac{1}{|\mathcal{M}|}\right) u_3$$

then $t < n/2$, where $\mathcal{M}$ is the message space of the protocol.

Proof. Let Π be a protocol in the statement. We construct a t-adversary $\mathcal{A}$ for $t = \lceil n/2 \rceil$ that can successfully attack Π. For simplicity, we assume that $n = 2t$.

Let $\mathcal{B}$ be any (harmless) adversary in the security of RSMT protocols of Definition 4. Since Π is $(0,0)$-SMT against $\mathcal{B}$, it holds that $u(\mathcal{B}, U) \leq u_2$. We show the existence of a t-adversary $\mathcal{A}$ that achieves $u(\mathcal{A}, U) > u_2$, which implies that Π cannot achieve a Nash equilibrium.

In the SMT game, a message $m \in \mathcal{M}$ is randomly chosen, and, on input m, Π generates $(s_1^j, \ldots, s_n^j)$ for $j = 1, \ldots,$ where s_i^j is the message to be sent over the i-th channel in the j-th round. In the game, $\mathcal{A}$ does the following:

- Randomly choose $I \subseteq \{1, \ldots, n\}$ such that $|I| = t$, and corrupt the i-th channel for every $i \in I$.
- Randomly choose $\tilde{m} \in \mathcal{M}$, and simulate Π on input $\tilde{m}$.
  Let $\tilde{s}_i^j$ be the message generated for the i-th channel in the j-th round.
- In each round j, for every $i \in I$, on receiving s_i^j through the i-th channel, exchange s_i^j for $\tilde{s}_i^j$.

For this attack, it is impossible for the receiver to distinguish which message, m or $\tilde{m}$, was originally transmitted by the sender, since both messages for m and $\tilde{m}$ are equally mixed. Hence, the probability that $\mathsf{suc} = 1$, denoted by p_s, is at most

$$p_s \leq \frac{1}{2}\left(1 - \frac{1}{|\mathcal{M}|}\right) + \frac{1}{|\mathcal{M}|} = \frac{1}{2}\left(1 + \frac{1}{|\mathcal{M}|}\right),$$

where $1/|\mathcal{M}|$ comes from the even that $\tilde{m} = m$.

Let p_d be the probability that Π outputs "DETECTION" messages during the execution against the above attack. Without loss of generality, we assume that if Π does not output "DETECTION" messages, the receiver outputs some message at the end of the protocol. If the tampering actions of $\mathcal{A}$ are not detected, the utility of $\mathcal{A}$ is at least u_1 with probability $1 - p_s$, and at least u_2 with probability p_s. If some tampering actions are detected, then there can be two cases: (1) the receiver does not output any message; and (2) the receiver outputs some message. In case (1), the utility of $\mathcal{A}$ is u_3. In case (2), the probability that the $\mathsf{suc} = 1$ is at most p_s by the same argument as above. Hence, the utility of

$\mathcal{A}$ when the tampering was detected is at least $(1 - p_s)u_3$. Thus, the utility of $\mathcal{A}$ in the SMT game is at least

$$\begin{aligned} u(\mathcal{A}, U) &\geq (1 - p_d)\left((1 - p_s)u_1 + p_s u_2\right) + p_d(1 - p_s)u_3 \\ &= (1 - p_s)u_1 + p_s u_2 - p_d\left((1 - p_s)u_1 + p_s u_2 - (1 - p_s)u_3\right) \\ &\geq (1 - p_s)u_3 \qquad (4) \\ &\geq \frac{1}{2}\left(1 - \frac{1}{|\mathcal{M}|}\right)u_3 \\ &> u_2, \qquad (5) \end{aligned}$$

where (4) follows from the fact that $p_d \leq 1$ and $(1-p_s)u_1+p_s u_2-(1-p_s)u_3 \geq 0$, and the assumption on U is used in (5). Therefore, $\mathit{\Pi}$ does not satisfy the security of RSMT protocols for $t \geq n/2$.

When $n = 2t-1$, the same attack of the above $\mathcal{A}$ can be realized by invalidating the n-th channel by substituting $\perp$ for every message over the n-th channel. □

The theorem gives the following corollary.

Corollary 2. *There is no SMT protocol without public channel that is perfectly secure against rational t-adversaries with utility function U for every $U \in U_{\mathsf{timid}}$ and $t \geq \lceil n/2 \rceil$.*

6 Conclusion

We have introduced the notion of rationality into secure message transmission. Specifically, we have defined timid adversaries, who prefer to violate the security requirements of SMT, but do not prefer the tampering actions to be detected. It is shown that some type of almost-reliable SMT protocols using a public channel (such as [32]) work as perfect SMT for any timid adversary corrupting $t < n$ channels. By imposing the assumption that $u_2 > u_3$, which captures strictly timid adversaries, it is possible to construct a non-interactive perfect SMT protocol against $t < n$ corruptions without using public channels.

A future work is to construct protocols against adversaries having different preferences from timid ones. It is important to clarify for which rational adversary the existing impossibility results hold.

Acknowledgements. This work was supported in part by JSPS Grant-in-Aid for Scientific Research Numbers 16H01705, 17H01695, and 18K11159. The second author thanks to Masaki Ueno for discussions about this work.

A Universal Hash Functions

Wegman and Carter [34] defined a notion of (almost) universal hash functions and gave its construction. We use an SMT protocol in which universal hash functions are used.

Definition 5. *Suppose that a class of hash functions $H = \{h\colon \{0,1\}^m \to \{0,1\}^\ell\}$, 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 called 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 **([32]).** *Let $H = \{h\colon \{0,1\}^m \to \{0,1\}^\ell\}$ 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 [34], Wegman and Carter constructed a family of $2^{1-2\ell}$-almost strongly universal hash functions. In particular, their hash function family $H_{wc} = \{h\colon \{0,1\}^m \to \{0,1\}^\ell\}$ 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

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

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

B Proof of Theorem 3

To prove the theorem, we define the notion of *algebraic manipulation detection (AMD) codes* in which the security requirement is slightly different from that in [9] for our purpose.

Definition 6. *An (M, N, δ)-*algebraic manipulation detection (AMD) code *is a probabilistic function $E\colon \mathcal{S} \to \mathcal{G}$, where $\mathcal{S}$ is a set of size M and $\mathcal{G}$ is an additive group of order N, together with a decoding function $D\colon \mathcal{G} \to \mathcal{S} \cup \{\perp\}$ such that*

- Correctness*: For any $s \in \mathcal{S}$,* $\Pr[D(E(s)) = s] = 1$.
- Security*: For any $s \in \mathcal{S}$ and $\Delta \in \mathcal{G} \setminus \{0\}$,* $\Pr[D(E(s) + \Delta) \neq \perp] \leq \delta$.

An AMD code is called systematic *if $\mathcal{S}$ is a group, and the encoding is of the form*

$$E\colon \mathcal{S} \to \mathcal{S} \times \mathcal{G}_1 \times \mathcal{G}_2, s \mapsto (s, x, f(x, s))$$

for some function f and random $x \in \mathcal{G}_1$. The decoding function D of a systematic AMD code is given by $D(s', x', f') = s'$ if $f' = f(x', s')$, and $\perp$ otherwise.

Note that, for a systematic AMD code, the correctness immediately follows from the definition of the decoding function. The security requirement can be stated such that for any $s \in \mathcal{S}$ and $(\Delta_s, \Delta_x, \Delta_f) \in \mathcal{S} \times \mathcal{G}_1 \times \mathcal{G}_2 \setminus \{(0,0,0)\}$, $\Pr_x[f(s + \Delta_s, x + \Delta_x) = f(s,x) + \Delta_f] \leq \delta$.

We show that a systematic AMD code given in [9] satisfies the above definition.

Proposition 1. *Let $\mathbb{F}$ be a finite field of size q and characteristic p, and d any integer such that $d+2$ is not divisible by p. Define the encoding function $E\colon \mathbb{F}^d \to \mathbb{F}^d \times \mathbb{F} \times \mathbb{F}$ by $E(s) = (s, x, f(x,s))$ where*

$$f(x,s) = x^{d+2} + \sum_{i=1}^{d} s_i x^i$$

and $s = (s_1, \ldots, s_d)$. Then, the construction is a systematic $(q^d, q^{d+2}, (d+1)/q)$-AMD code.

Proof. We show that for any $s \in \mathbb{F}^d$ and $(\Delta_s, \Delta_x, \Delta_f) \in \mathbb{F}^d \times \mathbb{F} \times \mathbb{F} \setminus \{(0^d, 0, 0)\}$, $\Pr[f(s + \Delta_s, x + \Delta_x) = f(s,x) + \Delta_f] \leq \delta$. The event in the probability is that

$$(x + \Delta_x)^{d+2} + \sum_{i=1}^{d} s'_i (x + \Delta_x)^i = x^{d+2} + \sum_{i=1}^{d} s_i x^i + \Delta_f, \tag{6}$$

where s'_i is the i-th element of $s + \Delta_s$. The left-hand side of (6) can be represented by

$$x^{d+2} + (d+2)\Delta_x x^{d+1} + \sum_{i=1}^{d} s'_i x^i + \Delta_x p(x)$$

for some polynomial $p(x)$ of degree at most d. Thus, (6) can be rewritten as

$$(d+2)\Delta_x x^{d+1} + \sum_{i=1}^{d} (s'_i - s_i) x^i + \Delta_x p(x) - \Delta_f = 0. \tag{7}$$

We discuss the probability that (7) happens when x is chosen uniformly at random. We consider the following cases:

1. When $\Delta_x \neq 0$, the coefficient of x^{d+1} is $(d+2)\Delta_x$, which is not zero by the assumption that $d+2$ is not divisible by p. Then, (7) has at most $d+1$ solutions x. Hence the event happens with probability at most $(d+1)/q$.
2. When $\Delta_x = 0$, we consider two subcases:
   (a) If $\Delta_s \neq 0$, then $s'_i - s_i \neq 0$ for some i. Hence (7) has at most d solutions x. Thus the event happens with probability at most d/p.
   (b) If $\Delta_s = 0$, (7) is equivalent to $\Delta_f = 0$. Since $\Delta_f \neq 0$ for this case, the event cannot happen.

In every case, the event happens with probability at most $(d+1)/q$. Thus the statement follows. □

As discussed in [9], a robust secret sharing scheme can be obtained by combining an AMD code and a linear secret sharing scheme. Let $(\mathsf{Share}, \mathsf{Reconst})$ be a (t, n)-secret sharing scheme with range $\mathcal{G}$ that satisfies correctness and perfect privacy of Definition 2, where we drop the parameter δ for robustness. A *linear* secret sharing scheme has the property that for any $s \in \mathcal{G}$, $(s_1, \ldots, s_n) \in \mathsf{Share}(s)$, and vector $(s'_1, \ldots, s'_n)$, which may contain $\perp$ symbols, it holds that $\mathsf{Reconst}(\{i, s_i + s'_i\}_{i \in I}) = s + \mathsf{Reconst}(\{i, s'_i\}_{i \in I})$ for any $I \subseteq \{1, \ldots, n\}$ with $|I| > t$, where $\perp + x = x + \perp = \perp$ for all x. Examples of linear secret sharing schemes are Shamir's scheme [31] and the simple XOR-based $(n-1, n)$-scheme, in which secret $s \in \{0,1\}^n$ is shared by $(s_1, \ldots, s_n)$ for random $s_i \in \{0,1\}^n$ with the restriction that $s_1 \oplus \cdots \oplus s_n = s$.

We show that the same construction as in [9] works as a construction of robust secret sharing of Definition 2.

Proposition 2. *Let* $(\mathsf{Share}, \mathsf{Reconst})$ *be a linear* (t, n)*-secret sharing scheme with range* $\mathcal{G}$ *that satisfies correctness and perfect privacy of Definition 2, and let* (E, D) *be an* (M, N, δ)*-AMD code of Definition 6 with* $|\mathcal{G}| = N$*. Then, the scheme* $(\mathsf{Share}', \mathsf{Reconst}')$ *defined by* $\mathsf{Share}'(s) = \mathsf{Share}(E(s))$ *and* $\mathsf{Reconst}'(S) = D(\mathsf{Reconst}(S))$ *is a* (t, n, δ)*-robust secret sharing scheme.*

Proof. Let $(s_1, \ldots, s_n) \in \mathsf{Share}'(s)$. Let $I \subseteq \{1, \ldots, n\}$ with $|I| \leq t$, and $(\tilde{s}_1, \ldots \tilde{s}_n)$ be a sequence of shares satisfying the requirement for input shares in robustness of Definition 2. We assume that $\tilde{s}_i = s_i + \varDelta'_i$ for each $i \in \{1, \ldots, n\}$. Note that $\varDelta'_i = 0$ for every $i \notin I$. Then,

$$\begin{aligned}
&\Pr\left[\mathsf{Reconst}'\left(\{i, \tilde{s}_i\}_{i \in \{1,\ldots,n\}}\right) \neq \perp\right] \\
&= \Pr\left[D\left(E(s) + \mathsf{Reconst}(\{i, \varDelta_i\}_{i \in \{1,\ldots,n\}})\right) \neq \perp\right] \\
&= \Pr\left[D\left(E(s) + \varDelta\right) \neq \perp\right],
\end{aligned}$$

where $\varDelta = \mathsf{Reconst}\left(\{i, \varDelta_i\}_{i \in \{1,\ldots,n\}}\right)$ is determined by the adversary. It follows from perfect privacy of the secret sharing scheme that $\varDelta$ is independent of $E(s)$. Thus, if $\tilde{s}_i \neq s_i$ for some $i \in \{1, \ldots, n\}$, the probability is at most δ by the security of the AMD code. Hence, the statement follows. □

By combining Shamir's secret sharing scheme with range $\mathbb{F}^d$ and the AMD code of Proposition 1, the robust secret sharing scheme of Theorem 3 is obtained by Proposition 2.

References

1. Abraham, I., Dolev, D., Gonen, R., Halpern, J.Y.: Distributed computing meets game theory: robust mechanisms for rational secret sharing and multiparty computation. In: Ruppert, E., Malkhi, D. (eds.) PODC, pp. 53–62. ACM (2006)
2. Abraham, I., Dolev, D., Halpern, J.Y.: Distributed protocols for leader election: a game-theoretic perspective. In: Afek, Y. (ed.) DISC 2013. LNCS, vol. 8205, pp. 61–75. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-41527-2_5

3. Asharov, G., Canetti, R., Hazay, C.: Toward a game theoretic view of secure computation. J. Cryptol. **29**(4), 879–926 (2016)
4. Asharov, G., Lindell, Y.: Utility dependence in correct and fair rational secret sharing. J. Cryptol. **24**(1), 157–202 (2011)
5. Azar, P.D., Micali, S.: Super-efficient rational proofs. In: Kearns, M., McAfee, R.P., Tardos, É. (eds.) EC 2013, pp. 29–30. ACM (2013)
6. Blakley, G.R.: Safeguarding cryptographic keys. Proc. Natl. Comput. Conf. **1979**(48), 313–317 (1979)
7. Campanelli, M., Gennaro, R.: Sequentially composable rational proofs. In: Khouzani, M.H.R., Panaousis, E., Theodorakopoulos, G. (eds.) GameSec 2015. LNCS, vol. 9406, pp. 270–288. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-25594-1_15
8. Campanelli, M., Gennaro, R.: Efficient rational proofs for space bounded computations. In: Rass, S., An, B., Kiekintveld, C., Fang, F., Schauer, S. (eds.) GameSec 2017. LNCS, vol. 10575, pp. 53–73. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-68711-7_4
9. Cramer, R., Dodis, Y., Fehr, S., Padró, C., Wichs, D.: Detection of algebraic manipulation with applications to robust secret sharing and fuzzy extractors. In: Smart, N. (ed.) EUROCRYPT 2008. LNCS, vol. 4965, pp. 471–488. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-78967-3_27
10. Dolev, D., Dwork, C., Waarts, O., Yung, M.: Perfectly secure message transmission. J. ACM **40**(1), 17–47 (1993)
11. Franklin, M.K., Wright, R.N.: Secure communication in minimal connectivity models. J. Cryptol. **13**(1), 9–30 (2000)
12. Fuchsbauer, G., Katz, J., Naccache, D.: Efficient rational secret sharing in standard communication networks. In: Micciancio, D. (ed.) TCC 2010. LNCS, vol. 5978, pp. 419–436. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-11799-2_25
13. Garay, J.A., Katz, J., Maurer, U., Tackmann, B., Zikas, V.: Rational protocol design: cryptography against incentive-driven adversaries. In FOCS, pp. 648–657. IEEE Computer Society (2013)
14. Garay, J.A., Katz, J., Tackmann, B., Zikas, V.: How fair is your protocol?: A utility-based approach to protocol optimality. In: Georgiou, C., Spirakis, P.G. (eds.) PODC, pp. 281–290. ACM (2015)
15. Garay, J.A., Ostrovsky, R.: Almost-everywhere secure computation. In: Smart [33], pp. 307–323 (2008)
16. Gordon, S.D., Katz, J.: Rational secret sharing, revisited. In: De Prisco, R., Yung, M. (eds.) SCN 2006. LNCS, vol. 4116, pp. 229–241. Springer, Heidelberg (2006). https://doi.org/10.1007/11832072_16
17. Gradwohl, R.: Rationality in the full-information model. In Micciancio [30], pp. 401–418 (2010)
18. Groce, A., Katz, J.: Fair computation with rational players. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 81–98. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-29011-4_7
19. Groce, A., Katz, J., Thiruvengadam, A., Zikas, V.: Byzantine agreement with a rational adversary. In: Czumaj, A., Mehlhorn, K., Pitts, A., Wattenhofer, R. (eds.) ICALP 2012 Part II. LNCS, vol. 7392, pp. 561–572. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-31585-5_50
20. Guo, S., Hubácek, P., Rosen, A., Vald, M.: Rational arguments: single round delegation with sublinear verification. In: Naor, M. (ed.) ITCS, pp. 523–540. ACM (2014)

21. Guo, S., Hubáček, P., Rosen, A., Vald, M.: Rational sumchecks. In: Kushilevitz, E., Malkin, T. (eds.) TCC 2016 Part II. LNCS, vol. 9563, pp. 319–351. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-49099-0_12
22. Halpern, J.Y., Teague, V.: Rational secret sharing and multiparty computation: extended abstract. In: Babai, L. (ed.) STOC, pp. 623–632. ACM (2004)
23. Halpern, J.Y., Vilaça, X.: Rational consensus: extended abstract. In: Giakkoupis, G. (ed.) PODC, pp. 137–146. ACM (2016)
24. Inasawa, K., Yasunaga, K.: Rational proofs against rational verifiers. IEICE Trans. **100–A**(11), 2392–2397 (2017)
25. Ishai, Y., Ostrovsky, R., Seyalioglu, H.: Identifying Cheaters without an honest majority. In: Cramer, R. (ed.) TCC 2012. LNCS, vol. 7194, pp. 21–38. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-28914-9_2
26. Kawachi, A., Okamoto, Y., Tanaka, K., Yasunaga, K.: General constructions of rational secret sharing with expected constant-round reconstruction. Comput. J. **60**(5), 711–728 (2017)
27. Kol, G., Naor, M.: Cryptography and game theory: designing protocols for exchanging information. In: Canetti, R. (ed.) TCC 2008. LNCS, vol. 4948, pp. 320–339. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-78524-8_18
28. Kol, G., Naor, M.: Games for exchanging information. In: Dwork, C. (ed.) STOC, pp. 423–432. ACM (2008)
29. Kurosawa, K., Suzuki, K.: Truly efficient 2-round perfectly secure message transmission scheme. IEEE Trans. Inf. Theory **55**(11), 5223–5232 (2009)
30. Micciancio, D. (ed.): TCC. LNCS, vol. 5978. Springer, Heidelberg (2010)
31. Shamir, A.: How to share a secret. Commun. ACM **22**(11), 612–613 (1979)
32. Shi, H., Jiang, S., Safavi-Naini, R., Tuhin, M.A.: On optimal secure message transmission by public discussion. IEEE Trans. Inf. Theory **57**(1), 572–585 (2011)
33. Smart, N.P. (ed.): EUROCRYPT. LNCS, vol. 4965. Springer, Heidelberg (2008)
34. Wegman, M.N., Carter, L.: New hash functions and their use in authentication and set equality. J. Comput. Syst. Sci. **22**(3), 265–279 (1981)
35. Yasunaga, K.: Public-key encryption with lazy parties. IEICE Trans. **99–A**(2), 590–600 (2016)
36. Yasunaga, K., Yuzawa, K.: Repeated games for generating randomness in encryption. IEICE Trans. **101–A**(4), 697–703 (2018)