Secure message transmission

against rational multiple adversaries

Kenya Yasui[1*], Yoshifumi Manabe[1]

[1] Faculty of Informatics, Kogakuin University, Shinjuku, Tokyo, Japan.

* Corresponding author. email: em17019@ns.kogakuin.ac.jp
Manuscript submitted January 10, 2014; accepted March 8, 2014.

Abstract: This paper shows an information theoretically secure message transmission against multiple adversaries. Fujita and Koshiba showed a secure message transmission against one rational adversary using the Garay and Ostrovsky's protocol. We consider multiple adversaries and improve existing protocols. Moreover, we define the safety probability equation of the proposed protocol. By using the equation, the sender knows how many paths to increase for safe transmission. We analyze each adversary's strategy in a multiple adversary environment using game theory and show that the proposed protocol is safe and reliable. By the several simulations, we show that the proposed protocol is safe and reliable against various adversaries under realistic conditions.
Key words: Information Theoretical Security, Game theory, Secret Sharing, Transmission Protocol

1. Introduction

Recently, the computation power of computer systems is rapidly increasing by GPGPU, clusters, and cloud computing. Therefore, an information theoretical secure protocol become more effective than computational secure protocols in some applications. Compared to computationally secure protocols, information theoretically secure protocols have advantages such as eliminating the key management issue; are less vulnerable to the man-in-the-middle and are robust to adversaries with unlimited computational power. Game theory is a method of mathematically and logically analyzing what kind of strategy is taken given a state to people with multiple utilities. We improve existing ASMT protocol in order to be used for multiple adversary environments in Session 3. The probability of safety and reliability of the proposed protocols improved in Session 4. We analyze the security under multiple adversary environments using game theory. We show the simulation result of the protocol in Session 5.

2. Secret Sharing Transmission Protocol

A Secret Sharing Transmission Protocol has information theoretic security by using secret sharing algorithm. For example Almost Everywhere Secure Computation was proposed by Garay and Ostrovsky.[2]

2.1. Garay and Ostrovsky's ASMT Protocol

In message transmission, safety means that the transmission contents are not leaked out. Reliability means that the message is correctly received by the receiver. A protocol satisfying safety and reliability is called Perfect Secure Message Transmission(PSMT). Almost SMT (ASMT) fails to send a message with a small probability. Garay and Ostrovsky's protocol, shown showin in Fig. 1, is three round ASMT protocol. Q-bit data to be sent is encoded to a 12q bit data by a coding method that is capable of error correction up to 1/4 data errors.[2] The encoding and decoding algorithm are denoted Enc and Dec, respectively. The sender can not detect eavesdropping but can detect tampering. The transmission uses a public path that anyone can browse but can not tamper. Tampering detection is enabled by releasing a part of the transmission message using the public path.

2.1.1. Reliability

Set l' such that l' > 3l. Suppose that a tampered path is not detected by tampering more than l' bits that is greater than the error correction capability in the round 1. In round 2 the probability that the tampered l' bits are not included in the published 3l bits is $(4/5)^{l'}$. The probability that an adversary's tampering is not detected is $(1-(4/5)^{l'})^k$ when the adversary tampers at k paths.

2.1.2. Safety

If n ≥ t – 1(t : the number of paths dominated by an adversary), the adversary cannot restore the message m when at least one of the n paths is not dominated, so the safety is satisfied.

The number of paths: n
Message to be sent: m ($|m|<q$)
Round 1.
Sender: The sender generates and transmits random bits R_i ($|R_i| = 15l$ ($q \le l$)) for each path i ($1 \le i \le n$).
Receiver: Let the received bits on the path i be R_i'. The receiver regards the path as a tampering path when $|R_i'| \neq 15l$.
Round 2.
Sender: The sender transmits R_i^* in which randomly selected $12l$ bits are replaced with * in R_i using the public path.
Receiver: The receiver compares R_i * for each path and R_i'. The receiver transmits the tampered path as *0* and the non-tampered path as *1* to the sender using the public path.

Thereafter, the tampered paths are not used.

The sender considers $12l$ bits not published by R_i^* as $\bar{Ri}$.

The receiver considers $12l$ bits not published by R_i^* as $\bar{Ri}'$.

Round 3.
Sender: The sender adjusts the length of message m to q bits. The sender decides m_i such that $m = m_1 \oplus m_2 \oplus \ldots \oplus m_{n'}$ (n': the number of non-tampered paths). The sender transmits $s_i = Enc(m_i) \oplus \bar{Ri}$ ($1 \le i \le n'$) on the public path.
Receiver: The receiver calculates $m'_i = Dec(s_i \oplus \bar{Ri}')$ and restores the message by $m' = m'_1 \oplus m'_2 \oplus \ldots \oplus m'_{n'}$.

Fig. 1 Garay and Ostrovsky's ASMT Protocol

2.1.3. Problem for multiple adversaries

As an extension of the model that there are multiple adversaries, the following problem must be considered. When some adversary tampers and the number of available paths decreases, the possibility that the dominant rate by another adversary among the remaining paths might become high. The probability that an adversary dominates all the remaining paths becomes high when many adversaries tamper. In order to lower the possibility, this paper proposes the following method to increase the number of paths when the number of paths to be used decreases due to tampering. Next, we propose an improved Garay and Ostrovsky's ASMT Protocol for multiple adversaries.

2.2. Proposed protocol

Adversaries who conspire are considered as one adversary. Multiple adversaries are independent of each other. If an independent adversary dominates the same path, the adversary is noticed that there is another adversary on the path. Assume that the sender considers the calculation cost to start message transmission. So, the sender does not use all the existing paths from the beginning. Initially, randomly selected n paths among all existing paths are used and check tampering using the same algorithm as Garay and Ostrovsky's ASMT Protocol. Unused paths are added when some paths are detected as being tampered.

The sender transmits a message after increasing the number of paths so as to satisfy the required safety probability. In the next section, we will calculate the probability of safety and reliability when the number of paths is increased. After round 2 in ASMT, the following procedure is executed

The sender calculates current security probability using equation (1).
If the probability is less than the sender's required security level, the sender randomly selects unused paths and verifies tampering on the new paths by using round 1 and 2. If no tampering is detected, the paths are added for the transmission.

Round 3. Same as Fig 1.

Fig. 2 Proposed protocol

3. Secret Sharing Transmission Protocol's safety and reliability

Assumptions for probability calculation are shown below. The total number of paths is h. The number of paths currently used for transmission is x. The number of decreased paths is y. The number of added paths is z. The number of adversaries is e. The number of paths dominated by each adversary are $k_1, k_2, k_3, \ldots, k_e$. Safety probability is obtained from the above values. The transmission is safe if the number of some adversary's dominant paths is less than the number of currently using paths.

$$P_1 = \prod_{i=1}^{e} P_{1,i} \quad \text{if } k_i \geq x - y + z \quad P_{1,i} = \left(1 - \frac{\binom{h-x-z}{k_i-x-z+y}}{\binom{h-y}{k_i}}\right) \qquad (1)$$

$$\text{otherwise} \quad P_{1,i} = 1$$

Based on this safety probability, the sender decides to send the message using the current paths or to add some number of new paths to increase the safety. This probability changes when a tamper detection occurs and the number of usable paths is decreased. If the probability is higher than the security required by the sender, the message is transmitted. If no new path is available when the probability is lower than the require level, the transmission is interrupted.

4. Game theory for Secret Sharing Transmission Protocol

In this section, game theory is applied to analyze protocols proposed in Section 3. Even in a realistic model in which there are multiple adversaries, when n ≥ t + 1 is satisfied, this paper shows that the proposed protocol is ASMT.

4.1. Game theory

Game theory is a method of mathematically and logically analyzing what kind of strategy is taken when given a state to people with multiple utilities. Each adversary select a strategy that maximizes its utility in the given situation. Using game theory, it is possible to obtain the outcome when each adversary acts reasonably.

4.2. Adversary's utility on transmission path

In this paper, we assume the adversary's utility as follows.

Adversary's Utility
1. u_1 : Obtains the content of the message(contains increasing the dominant rate)
2. u_2 : The sender fails to send the correct message.
3. u_3 : Tempers paths in which another adversary dominates.
4. u_4 : Interrupts the transmission protocol

Fig. 3 Adversary's Utility

4.3. Validation against adversary utilities

When verifying the strategy of multiple adversaries, assume that there are adversaries with diferrent utilitiy. When some adversary pursues a utility other than the adversary's first utility by a strategy, the strategy can be regarded as the same strategy that the adversary first pursues the same strategy but pursues another utility as the second or lower utility. Therefore, there is no need to consider the second or lower utility other than the

adversary's first utility. We will examine the strategies of each adversary who pursues each utility first and examine the influence on the transmission protocol.

4.3.1. Wiretap only utility

The utility of wiretap only is u_1. Let us consider an adversary whose maximum utility is u_1. If an adversary dominates all transmission paths, the adversary is able to obtain outgoing messages. Accordingly, this utility is a utility including a strategy to raise the dominant rate. Since the adversary cannot execute actions other than tampering and wiretapping, and tampering is detected by the sender with high probability, there is no action to take for the adversary to increase the domination rate of the adversary. The only possibility to increase the domination rate of adversary A is that another adversary, say adversary B, tampers a path that is not dominated by adversary A and the sender uses another path that is dominated by A. Since all adversaries are independent and no collusion exists, there is no way for adversary A to make adversary B tamper a specific path.
Thus, this type of adversary just executes wiretapping.

4.3.2. Wiretap and tampering utility

The utilities of wiretap and tampering are the following three of u_2, u_3 and u_4. These three utilities cause an increase or decrease the number of paths by tampering. Next, we verify whether these three utilities degrade the safety and reliability of the transmission protocol.

4.3.3. Impact of tampering

Changes in the adversary's dominance must be taken into consideration with all tampering utilities. Reduction in reliability occurs when there is many tampering or when there are adversaries with a high dominant rate. The utilities u_2 and u_4 correspond to this case.

If an adversary whose maximum utility is u_3 wishes to lower the dominant rate of a hostile adversary on a dominated path, the adversary with utility u_3 intentionally tampers hostile's paths. Then, the tampered paths are detected and other paths are used. The alteration caused by the utility u_3 occurs only in a certain path. If tampering occurs on many paths by many adversaries, this situation is the same as considering u_4 that is many tampering described later.

Next, we discuss an adversary whose maximum utility is u_2 or u_4 which may degrade the reliability. The utility u_2 can be obtained with the small probability by the coding shown in Section 3.1.1. The success probability is $(4/5)^l$ depending on the bit length. It can be approximated to zero if l is taken large enough. So, it is almost impossible to achieve this utility. Adversaries whose maximum utility is u_4 need to dominate many paths. The higher the dominated path rate of the adversary, the greater the impact on safety and reliability becomes. In order to avoid the problem, the sender uses the equation P_1 and adds new paths. The reliability and safety are determined by how many paths are not tampered among the entire paths.

We showed how all utilities effected the transmission protocol. In conclusion, if the sender prepares a sufficient number of paths and transmit with satisfactory probability, the reliability and safety is achieved. In the next section, we show the relationship between the tampering rate and the reliability.

5. Simulation for Secret Sharing Transmission Protocol

In this section, using the probability formula in Section 4, we show the calculation result. In the calculation, we assume three types of adversaries. (1) Only tampering of u_4. (2) Only wiretap of u_1. (3) tampering or wiretap of u_3. An adversary tampers a path only if another adversary dominates on the path. The upper limit of the number of adversaries is changed from 1 to 100 and calculated the possibility of an adversary dominates all using paths and interrupts transmission. The calculation result is shown in Fig. 5, 6. Three types of adversaries are randomly placed with the same probability. The calculation is executed 1000 times and the number of times each event occurred is summed up.

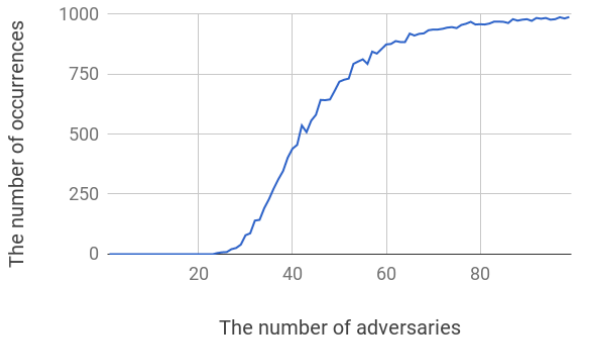


Fig. 5 The number of times transmission interrupt occurred

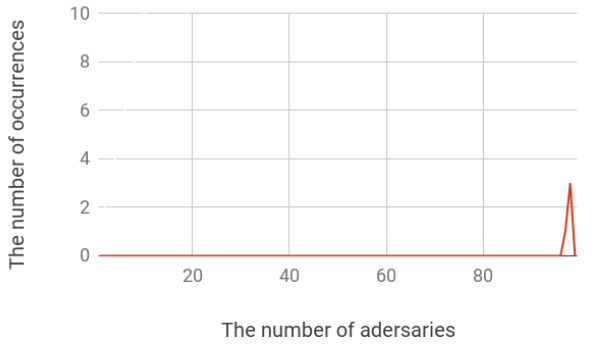


Fig. 6 The number of times data leakage occurred

Also, we changed the number of three types of adversaries. The result is shown in Fig. 7, 8, 9.

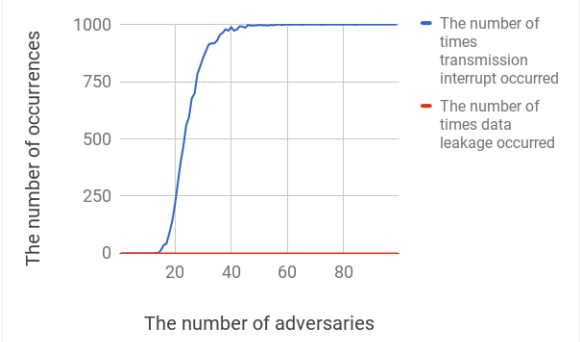


Fig. 7 The case when the ratio of (type(1), type(2), type(3))=(0.8,0.1,0.1)

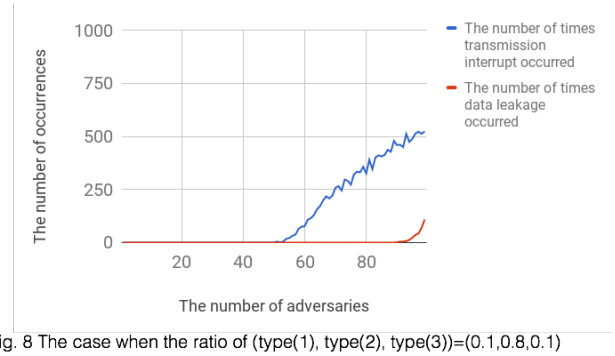


Fig. 8 The case when the ratio of (type(1), type(2), type(3))=(0.1,0.8,0.1)

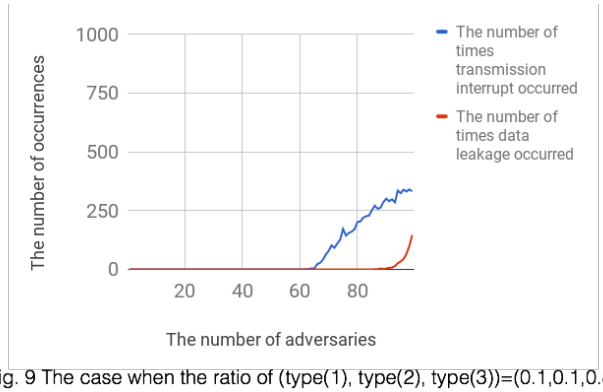


Fig. 9 The case when the ratio of (type(1), type(2), type(3))=(0.1,0.1,0.8)

Fig. 5-6 indicate that when three types of adversaries have the same ratio, the paths are tampered and the message cannot be sent. Even if an adversary whose dominance rate is high wiretaps transmission, the probability of the data leaked is small. Thus, as shown in Fig. 5-9, the possibility of transmission interrupt is much higher than the one of data leakage in any cases. If the transmission is not interrupted, the possibility that the data is not leaked is very high. Thus, the sender needs to avoid transmission interrupt. In order to achieve this, the sender needs to prepare enough number of untapped paths using equation P_1.

6. Conclusion

In this paper, improvements are made to the existing ASMT protocol by increasing the number of paths based on the equation of the safety and the reliability. The probability of safety and reliability that varies depending on the strategies of multiple adversaries is discussed. We considered the cases when there are several types of adversaries who have different utilities using game theory. The calculation result shows that the safety and the reliability are almost achieved. For further future study, we use this calculation result to make statistics that can predict the total number of adversaries from the number of tampering under the real world.

References

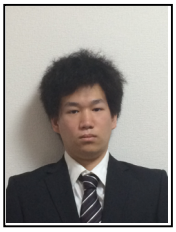
[1] Maiki Fujita and Takeshi Koshiba. ”Perfectly secure message transmission scheme against rational adversaries” SCIS 2016. In Japanese.

[2] Juan A Garay and Rafail Ostrovsky. (2008) “Almost everywhere secure computation.” Advances in Cryptology—EUROCRYPT. LNCS 4965. Springer Berlin Heidelberg, pp.307-323.

[3] Adi Shamir. (1979) “How to share a secret.” Communications of the ACM 22(11): pp.612-613.

[4] Danny Dolev and Cynthia Dwork，Orli Warts, Moti Yung. (1993) “Perfectly secure message transmission.” J.ACM 40(1): pp.17-47.

[5] Matthew Franklin and Rebecca N. Wright. (2000) “Secure communication in minimal connectivity models.” J.Cryptol 13(1): pp.9-30.



Kenya Yasui was born in Tokyo, Japan in 1993. He is in his first year for his master's in Faculty of Informatics, Kogakuin University. His research interest includes game theory, onion routing, blockchain.

Yoshifumi Manabe was born in Osaka, Japan in 1960. He received B.E., M.E., and Dr. E. degrees from Osaka University, Osaka, Japan in 1983, 1985, and 1993, respectively.
From 1985 to 2013, he worked for Nippon Telegraph and Telephone Corporation. He was a guest associate professor of Kyoto University in 2001-2013. Since 2013, he is a professor of Kogakuin University. His research interest includes cryptography, distributed algorithms, and game theory.

Dr. Manabe is Member of ACM, IEEE, IPSJ, JSIAM and IEICE.