Secure Modulo Zero-Sum Randomness as Cryptographic Resource

Masahito Hayashi[1,2] and Takeshi Koshiba[3]

[1] Graduate School of Mathematics, Nagoya University
masahito@math.nagoya-u.ac.jp
[2] Centre for Quantum Technologies, National University of Singapore
[3] Faculty of Education and Integrated Arts and Sciences, Waseda University
tkoshiba@waseda.jp

Abstract. We propose a new cryptographic resource, which we call *modulo zero-sum randomness*, for several cryptographic tasks. The modulo zero-sum randomness $X_1, \ldots, X_m$ is distributed randomness among m parties, where $X_1, \ldots, X_m$ are independent of each other but $\sum X_i = 0$ holds. By using modulo zero-sum randomness, we show that multi-party secure computation for some additively homomorphic functions is efficiently realized without the majority honest nor secure communication channels (but public channel). We also construct secret sharing protocols without secure communication channels. Moreover, we consider a new cryptographic task *multi-party anonymous authentication*, which is realized by modulo zero-sum randomness. Furthermore, we discuss how to generate modulo zero-sum randomness from some information theoretic assumption. Finally, we give a quantum verification protocol of testing the property of modulo zero-sum randomness.

Keywords: cryptographic resource, public channel, multi-party secure computation, secret sharing, authentication, quantum verification

1 Introduction

In cryptography, we often focus on cryptographic resources such as secure agreed keys and common randomness: secure agreed keys play an important role for message authentication and common reference strings are essential for the universal composable security. In this paper, we propose yet another cryptographic resource, which we call *modulo zero-sum randomness*. When m players exist, secure modulo zero-sum randomness is given as random numbers X_i in $\mathbb{F}_q^c$ for $i = 1, \ldots, m$ as follows. The relation $\sum_{i=1}^m X_i = 0$ holds and any $m-1$ variables among $X_1, \ldots, X_m$ are independent of each other. Player i has the randomness X_i and does not know any other random variables except for the above zero-sum condition.

In the standard setting of multi-party secure computation, many cryptographic protocols require secure communication channels between any distinct

two players [11, 3]. For example, secure multi-party secure computation for homomorphic functions can be realized without majority honesty, it requires so many secure communication channels [4]. Also, any existing secret sharing protocol requires many secure communication channels [23, 15, 1, 22, 26, 27, 21, 13]. In this paper, using the secure modulo zero-sum randomness, we propose protocols to realize these tasks without secure communication channels (but public channel). That is, based on secure modulo zero-sum randomness, we construct a protocol for multi-party secure computation for some additively homomorphic functions without the majority honesty nor secure communication channels. Also, based on the secure modulo zero-sum randomness, we construct secret sharing protocols without secure communication channels.

As an alternative approach to realize multi-party secure computation without the majority honesty nor secure communication channels, we can take secure message transmission [6, 2, 18, 25]. Secure message transmission is a cryptographic protocol between two parties, between which there are several channels, to send messages privately and reliably. Secure message transmission protocols can simulate a secure communication channel between the two parties. In the standard setting of secure message transmission, the majority honesty over the channels is required. If the public channel is available in secure message transmission, then such a barrier can be overcome [7, 24, 17] and multi-party secure computation can be realized by using secure message transmission with the public channel [8]. However, the respective simulations of the secure communication channels are quite inefficient.

As another application, we propose *multi-party anonymous authentication*, which is a new cryptographic task. Consider the case when a certain project requires the approvals from all the players. We are required to verify that all the players approve the project by confirming the contents of the project. Additionally, we might require the anonymity for this approval due to the following reason. This is because if a person disagreeing to the project can be identified, a player might hesitate to disagree to it even when he/she does not agree on it in his/her mind. In this paper, using secure modulo zero-sum randomness, we construct a protocol to realize multi-party anonymous authentication without secure communication channel.

Indeed, secure modulo zero-sum randomness can be generated by multi-party secure computation for modulo sum. In this sense, the generation of secure modulo zero-sum randomness can be regarded as an equivalent task to multi-party secure computation for modulo sum. In addition, we also discuss several methods to generate secure modulo zero-sum randomness.

This paper is organized as follows. Section 2 defines a new cryptographic resource *modulo zero-sum randomness* and discuss the equivalence to related secure computation protocols. Section 3 extends the results in Section 2 to secure computation with respect to additively homomorphic functions. Section 4 provides secret sharing protocols without secure communication channels. Section 5 proposes a new cryptographic task *multi-party anonymous authentication*, which employs modulo zero-sum randomness. Section 6 discusses how to generate se-

cure modulo zero-sum randomness. While, in general, it is difficult to examine the property of secure modulo zero-sum randomness, Section 7 shows that if we are allowed to use quantum algorithms it is possible to verify that the resource satisfies the property of secure modulo zero-sum randomness.

2 Secure Modulo Zero-Sum Randomness, its Variant Tasks and Reducibilities among them

First, we give the rigorous definition of secure modulo zero-sum randomness for the random numbers $X_i \in \mathbb{F}_q^c$ with $i = 1, \ldots, m$. The random numbers $X_i \in \mathbb{F}_q^c$ with $i = 1, \ldots, m$ is called secure modulo zero-sum randomness when the following conditions hold.

(1) *Modulo zero condition*: The relation $\sum_{i=1}^m X_i = 0$ holds.
(2) *Independence condition*: Any $m-1$ variables among $X_1, \ldots, X_m$ are independent of each other.
(3) *Secrecy condition*: Player i has the randomness X_i and does not know any other random variables except for the modulo zero condition. Let W_i be the information of Player i except for X_i. Then, the relation $I(X_1, \ldots, X_m; X_i W_i) = I(X_1, \ldots, X_m; X_i)$ holds.

We address some tasks of secure computation, which are variants of modulo zero-sum randomness and show reducibilities among them.

The tasks are to evaluate functions with multiple inputs without revealing the information for respective inputs when these inputs are given by different players. As typical example, we focus on the secure modulo sum, i.e., a task to calculate the modulo sum $Y_1 + \cdots + Y_m$ as a function with m inputs $Y_i \in \mathbb{F}_q^c$. Here, the m inputs are given by m different players, and it is required to calculate the output without informing their inputs to other players. It is known that secure multiparty computation for modulo sum is possible without the majority honesty [4]. That is, even when the majority of players do not behaves honestly, the secrecy of each input can be guaranteed. However, it requires secure communication channels.

When no secure communication channel is available, to realize the above task only with public channels, it is natural to employ cryptographic resources.

Now let us define two tasks related to secure modulo zero-sum randomness.

Task A : Player m must calculate the modulo sum $Y_1 + \cdots + Y_{m-1}$, where Player i has the secret input $Y_i \in \mathbb{F}_q^c$ for $i = 1, \ldots, m-1$.
Task B : All the players must calculate the modulo sum $Y_1 + \cdots + Y_m$.

We investigate reducibilities among Task A, Task B, and secure modulo zero-sum randomness, which is a cryptographic resource. In both tasks A and B, it is also required that any $m-2$ players cannot obtain information for the remaining players. Then, secure modulo zero-sum randomness and both tasks A and B can be equivalent to each other in the following sense.

Theorem 1. *When public channels are freely available and there are m honest players, secure modulo zero-sum randomness, Task* A*, and Task* B *are reducible to each other.*

Proof. First, we show that Task A is reducible to the secure modulo zero-sum randomness. When the m players have secure modulo zero-sum randomness $X_i \in \mathbb{F}_q^c$ for $i = 1, \ldots, m$, Task A can be realized as in Protocol 1.

Second, we show that Task B is reducible to Task A. After the execution of Task A, Player m sends $Y_1 + \cdots + Y_{m-1} + Y_m$ to all the remaining players. Since Task A is done by m honest players, the resulting protocol satisfies the requirements for Task B.

Finally, we show that the secure modulo zero-sum randomness is reducible to Task B. After the execution of Task B, Player i sets X_i to be Y_i for $i = 1, \ldots, m-1$ and Player m sets X_m to be $Y_m - (Y_1 + \cdots + Y_{m-1} + Y_m)$. Since Task B is done by m honest players, the resulting randomness satisfies the requirements for the secure modulo zero-sum randomness. □

Protocol 1 Secure Modulo Sum Protocol without Secure Communication
STEP 1: Player i sends the information $Z_i := Y_i + X_i$ to Player m via public channel.
STEP 2: Player m calculates $X_m + \sum_{i=1}^{m-1} Z_i$, which equals $\sum_{i=1}^{m} Y_i$.

3 Secure Multi-party Computation of Homomorphic Functions

The discussion in the previous section can be extended to a homomorphic function with respect to addition. Let $f : (\mathbb{F}_q^c)^m \to \mathbb{F}_q^c$ be an additively homomorphic function whose value can be determined by a linear combination of inputs. That is,

$$f(Y_1, \ldots, Y_m) = \tilde{f}(\alpha_1 Y_1 + \cdots + \alpha_m Y_m),$$

where $\alpha_1, \ldots, \alpha_m$ are all in $\mathbb{F}_q^c$ and $\tilde{f} : \mathbb{F}_q^c \to \mathbb{F}_q^c$ is a some function. For the security, we also assume that f is sensitive in the sense that the image of f distributes uniformly at random when some argument is chosen uniformly at random and the other arguments are fixed.

The task can be realized in Protocol 2, which employs secure modulo zero-sum randomness $X_i \in \mathbb{F}_q^c$ for $i = 1, \ldots, m$.

Theorem 2. *Suppose that the adversary collapses at most $m - 1$ players. Then Protocol 2 securely computes f.*

Proof. For the proof, we follow the convention in [10]. First, we assume that the adversary $\mathcal{A}$ collapses Players $1, \ldots, m - 1$. Since Protocol 2 is essentially

non-interactive, what the adversary $\mathcal{A}$ can do is just sending a fake value Z_i' instead of Z_i for Player i. Then, the adversary $\mathcal{A}$'s view is described as

$$\{X_1, \ldots, X_{m-1}, Y_1, \ldots, Y_{m-1}, Z_1', \ldots, Z_{m-1}', Z_m, f(Y_1, \ldots, Y_m)\}.$$

Now, we constructe a simulator $\mathcal{S}$ which takes X_m, Y_m, $\tilde{f}(X_m + \alpha_m Y_m)$ and $f(Y_1, \ldots, Y_m)$ as inputs. $\mathcal{S}$ can compute $Z_1', \ldots, Z_{m-1}'$ as $\mathcal{A}$ does. Also $\mathcal{S}$ can compute Z_m as

$$Z_m = f(Y_1, \ldots, Y_m) - \sum_{i=1}^{m-1} \tilde{f}(X_i + \alpha_i Y_i).$$

Thus, we can say that the simulator $\mathcal{S}$ perfectly simulates $\mathcal{A}$'s view.

Next, we consider the case that $\mathcal{A}$ collapses Players $1, \ldots, k$, where $k < m-1$. In this case, we can similarly construct a simulator $\mathcal{S}$. The difference is that $\mathcal{S}$ can compute $Z = Z_{k+1} + \cdots + Z_m$ instead of Z_m. Since $\tilde{f}$ is sensitive, we can take random values from the image of $\tilde{f}$ for $Z_{k+1}, \ldots, Z_{m-1}$. $\mathcal{S}$ can set $Z_m = Z - (Z_{k+1} + \cdots + Z_{m-1})$. This is also a perfect simulation of $\mathcal{A}$'s view. □

Protocol 2 Secure Computation for an additively homomorphic function f

STEP 1: Player i computes $Z_i := \tilde{f}(X_i + \alpha_i Y_i)$ and distributes it to all the other players via public channel.

STEP 2: Each player collects all $Z_1, \ldots, Z_m$ and computes $\sum_{i=1}^m Z_i$, which equals

$$\sum_{i=1}^{m} \tilde{f}(X_i + \alpha_i Y_i) = \tilde{f}\left(\sum_{i=1}^{m} X_i + \sum_{i=1}^{m} \alpha_i Y_i\right) = f(Y_1, \ldots, Y_m).$$

4 Secret Sharing without Secure Communication Channel

4.1 Basic Protocol

While there are many secret sharing protocols, they requires secure communication channel in the dealing phase [23]. Now, we propose a secret sharing protocol without use of secure communication channel. Assume that there are m players and Player 1 has a secret message $Y \in \mathbb{F}_q^c$. Our task is the following without use of secure communication channel. Player m can decode the secret message Y only when all the $m-1$ players except for Player 1 collaborate for the decoding. A conventional secret sharing protocol does not achieve this requirement because it employs secure communication channels in the dealing step.

When the m players have secure modulo zero-sum randomness $X_i \in \mathbb{F}_q^c$ for $i = 1, \ldots, m$, this task can be realized as Protocol 3.

Protocol 3 Secret Sharing without secure communication channel

STEP 1: [Dealing] Player 1 sends the information $Z := X_1 + Y$ to Player m via public channel.

STEP 2: Players $2, \ldots, m-1$ send their randomness $X_2, \ldots, X_{m-1}$ to Player m via public channel.

STEP 3: [Reconstruction] Player m reconstructs the original information $Z + \sum_{i=2}^{m} X_i$, which equals Y.

4.2 Cheater Detectable Protocol

However, this protocol cannot detect whether Players $2, \ldots, m-1$ send incorrect information. To resolve this problem, we propose the following protocol (Protocol 4), which employs secure modulo zero-sum randomness $X_i \in \mathbb{F}_q^c$ for $i = 1, \ldots, m$. In this protocol, the information Y transmitted from Player 1 is a non-zero element of $\mathbb{F}_q$. Hence, Y is subject to the uniform distribution on $\mathbb{F}_q \setminus \{0\}$. When the size of information to be transmitted is large, we use algebraic extension. We identify the vector space $\mathbb{F}_q^c$ with the finite filed $\mathbb{F}_{q'}$ with $q' = q^c$ by considering algebraic extension.

Protocol 4 Cheater Detectable Secret Sharing without secure communication channel

STEP 1: Players $2, \ldots, m-1$ send their randomness $X_2, \ldots, X_{m-1}$ to Player m via public channel.

STEP 2: [Dealing] Player 1 sends the information $Z := X_1 Y$ to Player m via public channel.

STEP 3: [Reconstruction] If $Z \neq 0$, Player m define $Y' := -Z(\sum_{i=2}^{m} X_i)^{-1}$. If Y' belongs to $\mathbb{F}_q \subset \mathbb{F}_{q'}$, Player m considers that there is no cheating and Y' equals the original information Y. If Y' does not belong to $\mathbb{F}_q \subset \mathbb{F}_{q'}$, Player m considers that there is cheating and discard Y'.

Now, we analyze the performance of Protocol 4. If Players $2, \ldots, m-1$ use the information in the dealing phase, these players can make a cheat. Hence, it is essential to put the transmission of the random variables $X_2, \ldots, X_{m-1}$ before the dealing phase. The performance with all the honest players can be analyzed as follows. When $X_1 \neq 0$, Player m reconstructs the original information Y. This probability is $1 - q^{-c}$.

Next, as an attack, we assume that at least one of Players $2, \ldots, m-1$ makes Player m to decode a different information from Y that belongs to $\mathbb{F}_q$. We call this attack the modification attack. For simplicity, we consider the case when all of Players $2, \ldots, m-1$ collude for the modification attack.

Theorem 3. *When all of Players* $2, \ldots, m-1$ *collude for the modification attack, they succeed the attack with probability* $\frac{q-1}{q'-1}$.

Proof. When $X_1 \neq 0$, to succeed this attack, the sum V' of variables sent from Players $2, \ldots, m-1$ to m needs to satisfy the condition $-X_1^{-1}(V' + X_m) \in \mathbb{F}_q \setminus \{1\}$. When we denote the sum $\sum_{i=2}^{m-1} X_i$ by V, the above condition is equivalent to the following condition. There exists an element $A(\neq 1) \in \mathbb{F}_q$ such that $V' - V - X_1 = -AX_1$, i.e., $V' = V + (1 - A)X_1$. Since X_1 is subject to the uniform distribution on $\mathbb{F}_{q'} \setminus \{0\}$, the variable $(1-A)X_1$ is subject to the uniform distribution on $\mathbb{F}_{q'} \setminus \{0\}$. Since the number of $A(\neq 1) \in \mathbb{F}_q$ is $q-1$, the probability to satisfy the condition required to V' is $\frac{q-1}{q'-1}$. □

Indeed, there exist so many secret sharing protocols with dishonest players. Some of them can identify the cheating players [15, 1, 22, 26, 27, 21, 13]. However, all the existing protocols require secure communication channels in the dealing phase. The advantage of this protocol is unnecessity of secure communication channels due to use of secure modulo zero-sum randomness.

5 Multi-party Anonymous Authentication

5.1 Basic Protocol

Suppose that a certain project written as the variable $Y \in \mathbb{F}_q^d$ requires the approvals from all of m players. Our requirement is the following. We verify that all m players approve the project by confirming the contents Y. Additionally, we require anonymity for this approval.

We consider the following simple protocol by using secure modulo zero-sum randomness $X_i \in \mathbb{F}_q^c$ for $i = 1, \ldots, m$. If the i-th player agrees the project, he/she sends his/her random variable X_i to the other players via public channel. Otherwise, he/she sends another variable to the other players via public channel. Then, each player calculates the sum of the received variable and his/her own variable. If the sum is zero, the project can be considered to be approved.

However, this protocol has the following problem. There is a possibility that Player i incorrectly receives a different information Y' from Y as the project. This case is called a mismatched recognition. In fact, when the secrecy of the information Y is required, it might be distributed via secure communication channel priorly. This assumption is natural because it is usual to require the secrecy of the contents of the project. Hence, we need to be careful about a mismatched recognition. That is, we need to verify that each player makes the decision based on the correct information Y.

To prevent a mismatched recognition, as illustrated in Fig. 1, attaching the message authentication protocol [16, 20] to information Y, we propose the following protocol as Protocol 5. As a preparation of Protocol 5, from secure modulo zero-sum randomness $X_i \in \mathbb{F}_q^c$ for $i = 1, \ldots, m$, we generate an $e \times d$ Toeplitz matrix T_i and a variable $A_i \in \mathbb{F}_q^e$, where we choose the integers e and d to satisfy $2e+d-1 = c$. (Note that Toeplitz matrices can be used universal hash functions. You may consult with a textbook [9].) Indeed, since an $e \times d$ Toeplitz matrix T_i needs $e + d - 1$ elements of $\mathbb{F}_q$, the pair of T_i and A_i requires $2e + d - 1 = c$

elements of $\mathbb{F}_q$. In the following, we also assume that the variable $Y \in \mathbb{F}_q^d$ describing the project has been distributed to all the players priorly while there is a possibility of a mismatched recognition.

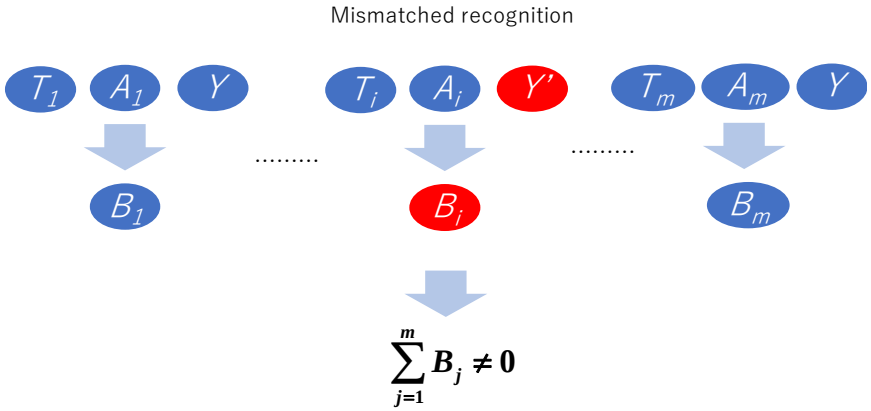

Fig. 1. Mismatched recognition.

Protocol 5 Multi-party Anonymous Authentication

STEP 1: [Voting] Player i sends $B_i \in \mathbb{F}_q^e$ to the remaining players via public channel. If Player i agrees the project described by Y, he/she chooses B_i as $T_iY + A_i$. Otherwise, he/she chooses B_i subject to the uniform distribution on $\mathbb{F}_q^e$.

STEP 2: [Verification] Each player calculates $\sum_{i=1}^n B_i$. If it is zero, the project can be considered to be approved.

5.2 Analysis with honest players

When all the players send $T_iY + A_i$ based on the same variable Y, we have $\sum_{i=1}^n B_i = \sum_{i=1}^n T_iY + A_i = (\sum_{i=1}^n T_i)Y + (\sum_{i=1}^n A_i) = 0Y + 0 = 0$ and all the players find that all of them approve the project written by Y. Hence, for security analysis, we need the analysis on the case when at least one player disagrees the project and/or at least one player recognizes a different information from Y. For this aim, we have the following two theorems.

Theorem 4. *When at least one player i' disagrees the project, the probability of $\sum_{i=1}^n B_i = 0$ is q^{-e}.*

Proof. Since $B_{i'}$ is subject to the uniform distribution on $\mathbb{F}_q^e$, the probability of $\sum_{i=1}^n B_i = 0$ is q^{-e}. □

Theorem 5. *When all the players agree the project and at least there one player i recognizes the information Y_i that is different from the information Y_1 recognized by Players 1, the probability of $\sum_{i=1}^{n} B_i = 0$ is q^{-e}.*

This theorem ensures that if the project is approved by this protocol, all the players confirm no mismatched recognition.

Proof. Assume that players $i_1, \ldots, i_k$ recognize the information $Y_{i_1}, \ldots, Y_{i_k}$ that is different from the information Y_1 recognized by Players 1. Also assume that other players recognize the same information Y_1 recognized by Players 1. We define the variable $V_{i_j} := Y_{i_j} - Y_1$ for $j = 1, \ldots, k$. Then, we have

$$\sum_{i=1}^{n} B_i = \sum_{j=1}^{k} T_{i_j} V_{i,j}. \tag{1}$$

Since $V_{i,j} \neq 0$, the variable $T_{i_j} V_{i,j}$ is independently subject to the uniform distribution on $\mathbb{F}_q^e$. Hence, $\sum_{j=1}^{k} T_{i_j} V_{i,j}$ is also subject to the uniform distribution on $\mathbb{F}_q^e$. Therefore, we obtain the desired statement. □

5.3 Analysis with malicious player

Now, we consider the case with a malicious player. When malicious Player j makes rushing, Player i can realize the situation $\sum_{i=1}^{n} B_i = 0$ by sending $-\sum_{i \neq j} B_i$ unless all the player do not approve the same variable Y. Hence, when we employ Protocol 5, we need to trust all the players. To avoid such an attack, we proposed another protocol (Protocol 6), which trust Player 1.

Protocol 6 Secure Multi-party Anonymous Authentication

STEP 1: [Voting] Player i sends $B_i \in \mathbb{F}_q^e$ to Player 1 via public channel. If Player i agree the project described by Y, he/she chooses B_i as $T_i Y + A_i$. Otherwise, he/she chooses B_i subject to the uniform distribution on $\mathbb{F}_q^e$.

STEP 2: [Verification] Player 1 calculates $\sum_{i=1}^{n} B_i$, where $B_1 := T_1 Y + A_1$. If it is zero, the project can be considered to be approved.

STEP 3: [Notification] Player 1 sends the above result to other players.

Now, we consider the following type of malicious player. Assume that malicious Players $l, \ldots, m$ wants to make the following situation by colluding together. Here, for the notational convenience, we assume that Players $l, \ldots, m$ are malicious. Players $1, \ldots, l-1$ consider that the project is described by another information $Y_1, \ldots, Y_{l-1}$, and they approve this project based on this incorrect information. Then, Player 1 announces that all the player approve the project based on the same information while they are not the same. For this kind of attack, we have the following theorem.

Theorem 6. *Malicious Players $l, \ldots, m$ succeed the above attack with probability q^{-e}.*

Proof. To realize this situation, $\sum_{i=l}^{m} B_i$ needs to be $-\sum_{i=1}^{l-1} T_i Y_i + A_i$, which is calculated as

$$\begin{aligned} -\sum_{i=1}^{l-1} T_i Y_i + A_i &= -\sum_{i=2}^{l-1} T_i (Y_i - Y_1) - \sum_{i=1}^{l-1} T_i Y_1 + A_i \\ &= -\sum_{i=2}^{l-1} T_i (Y_i - Y_1) + \sum_{j=l}^{m} T_j Y_1 + A_j. \end{aligned}$$

We define the set $\{i_1, \ldots, i_k\} := \{i \in [2, l-1] | Y_i \neq Y_1\}$. Then, $T_{i_1}(Y_{i_1} - Y_1), \ldots, T_{i_k}(Y_{i_k} - Y_1)$ are independently subject to the uniform distribution on $\mathbb{F}_q^e$. Since A_i is subject to the uniform distribution on $\mathbb{F}_q^e$ for $i = 2, \ldots, l-1$, B_i is independent of $T_i Y_i$. Hence, Players $l, \ldots, m$ cannot obtain any information $T_i Y_i$ from B_i for $2, \ldots, l-1$. Thus, letting

$$V := (B_2, \ldots, B_{m-1}, T_l, \ldots, T_m, A_l, \ldots, A_m, Y_1, \ldots, Y_{l-1}),$$

we obtain

$$\begin{aligned} & I(-\sum_{i=2}^{l-1} T_i (Y_i - Y_1) + \sum_{j=l}^{m} T_j Y_1 + A_j; V) \\ =& I(-\sum_{i=2}^{l-1} T_i (Y_i - Y_1); V) = 0. \end{aligned} \tag{2}$$

Since $-\sum_{i=2}^{m-1} T_i (Y_i - Y_1)$ is subject to the uniform distribution, Players $l, \ldots, m$ can make the situation $\sum_{i=1}^{n} B_i = 0$ with probability q^{-e}. □

6 How to Generate Module Zero-Sum Randomness

6.1 From secure agreed random numbers

Also, we discuss the generation of secure modulo zero-sum randomness from secure modulo sum in Section 2, we discuss another method for this generation. Secure modulo zero-sum randomness among m players can be generated from several pairs of secure agreed random numbers as follows. Assume that ith player and $i+1$-th player share the secret random number $Z_i \in \mathbb{F}_q^c$. Also, we assume that the first player and the m-th player share the secret random number $Z_m \in \mathbb{F}_q^c$. Then, the first player puts the random variable $X_1 := Z_1 - Z_m$, and Player i puts the random variable $X_i := Z_i - Z_{i-1}$. The resultant variables $X_1, \ldots, X_m$ satisfies the condition $\sum_{i=1}^{m} X_i = 0$ and the independence between any $n-1$ variables of them.

6.2 Asymptotically approximated generation from information theoretical assumption

Secure modulo zero-sum randomness among m players can be generated from information theoretical assumption with asymptotically negligible error. A sequence of random variables $X_{i,n} \in \mathbb{F}_q^{c_n}$ is called secure modulo zero-sum randomness with asymptotically negligible error when

$$D(P_{X_{1,n}}, \ldots, X_{m,n}, P_{\tilde{X}_{1,n},\ldots,\tilde{X}_{m,n}}) \to 0 \tag{3}$$

where D is the variational distance and $\tilde{X}_{1,n}, \ldots, \tilde{X}_{m,n}$ is a secure modulo zero-sum randomness among m players. Here, $\lim_{n\to\infty} \frac{c_n}{n}$ is called the generation rate.

For example, secure modulo zero-sum randomness among m players can be generated with asymptotically negligible error when the multiple access channel satisfies a certain condition and they can use the multiple access channel n times. The detail construction will be given in [14]. Also, with asymptotically negligible error, it can be extracted from the n-fold independent and identical distribution of a certain joint distribution of m random variables $Z_1, \ldots, Z_m$ only with public communication when the joint distribution satisfies a certain condition [14].

7 Quantum Verification Protocol

In the classical case, we have no method to verify the distribution of the randomness $X_1, \ldots, X_m$ satisfies the condition of secure modulo zero-sum randomness among m players. However, when we can use quantum system, we have such a desired method as follows. First, we generate m pair of secure secret keys required in Section 6.1 by using quantum key distribution. Then, we apply the protocol given in Section 6.1. This method certainly generates secure modulo zero-sum randomness. However, since this method goes through the conventional quantum key distribution, this method is not a direct method to generate this kind of resource. Hence, we propose a direct verifiable construction by using the GHZ state as follows.

For this aim, we introduce the phase basis state. The phase basis $\{|z\rangle_p\}_{z\in\mathbb{F}_q}$ is defined as [12, Section 8.1.2]

$$|z\rangle_p := \frac{1}{\sqrt{q}} \sum_{x\in\mathbb{F}_q} \omega^{-\operatorname{tr} xz} |x\rangle,$$

where $|x\rangle$ expresses the computational basis, $\omega := \exp\frac{2\pi i}{p}$ and $\operatorname{tr} y$ for $y \in \mathbb{F}_q$ is $\mathrm{Tr} M_y$ where M_y denotes the multiplication map $x \mapsto yx$ with the identificiation of the finite field $\mathbb{F}_q$ with the vector space $\mathbb{F}_p^t$.

Then, we define the phase GHZ state $|GHZ\rangle_p := \frac{1}{\sqrt{q}} \sum_{x\in\mathbb{F}_q} |x, \ldots, x\rangle_p$ on the composite system of m copies of the quantum system spanned by $\{|x\rangle\}_{x\in\mathbb{F}_q}$. When all the players apply measurement on the computational basis and the

initial state is $|GHZ\rangle_p$, the outcome satisfies the conditions of secure modulo zero-sum randomness. If they have $2n_1 + n_2$ copies of the same state ρ, it can be verified as Protocol 7.

Protocol 7 Verified Generation of Secure Modulo Zero-Sum Randomness

STEP 1: [Phase basis check] They randomly choose n_1 copies, and apply the measurement of the phase basis. If their outcomes are the same, the test is passed.

STEP 2: [Computational basis check] They randomly choose n_1 copies, and apply the measurement of the computational basis. If the modulo sums of their outcomes are zero, the test is passed.

STEP 3: [Generation] They apply the measurement of the computational basis to the remaining n_2 copies. The outcomes are used as n_2 secure modulo zero-sum randomness.

Theorem 7. *Assume that $\alpha > \frac{1}{2n_1+n_2}$. If the test is passed, with significance level α, we can guarantee that the resultant state σ on each remaining system satisfies*

$$\mathrm{Tr}\sigma|GHZ\rangle_p\ {}_p\langle GHZ| \ge 1 - \frac{1}{\alpha(2n_1+1)}. \tag{4}$$

Proof. Let P_1 and P_2 be the projections to the subspaces accepting the phase basis check and the computational basis check, respectively. We randomly choose one remaining system. Let A be the random permutation of $P_1^{\otimes n_1} \otimes P_2^{\otimes n_1} \otimes (I - |GHZ\rangle_p\ {}_p\langle GHZ|)$, which expresses the event that they accept the test and the state on the remaining system is orthogonal to the state $|GHZ\rangle_p\ {}_p\langle GHZ|$. Since $P_1 \ge |GHZ\rangle_p\ {}_p\langle GHZ|$ and $P_2 \ge |GHZ\rangle_p\ {}_p\langle GHZ|$, the similar discussion to [19, Appendix] yields that $\|A\| \le \frac{1}{2n_1+1}$. Hence, any initial state satisfies $\mathrm{Tr}A \le \frac{1}{2n_1+1}$.

Now, we assume that the probability accepting the test is less than α. Then, under the condition that they accept the test, the probability of the event orthogonal to the state $(|GHZ\rangle_p\ {}_p\langle GHZ|)^{\otimes n_2}$ is upper bounded by $\frac{1}{\alpha} \cdot \frac{1}{2n_1+1}$. Hence, we obtain the desired statement. □

[Note that the significance level is the maximum passing probability when malicious Bob sends incorrect states so that the resultant state α does not satisfy Eq. (4).] The proof of the theorem is given below. From the theorem and the relation between the fidelity and trace norm [40][(6.106)], we can conclude the verifiability: if they passed the test, they can guarantee that

$$\|\sigma - |GHZ\rangle_p\ {}_p\langle GHZ|\|_1 \le \frac{1}{\sqrt{\alpha(2n_1+1)}} \tag{5}$$

with significance level α.

References

1. A. Adhikari, K. Morozov, S. Obana, P. S. Roy, K. Sakurai, and R. Xu: Efficient threshold secret sharing schemes secure against rushing cheaters, in *Proc. the 9th International Conference on Information Theoretic Security (ICITS 2016)*, Lecture Notes in Computer Science 10015, pp.3–23, Springer (2016).
2. S. Agarwal, R. Cramer, and R. de Haan: Asymptotically optimal two-round perfectly secure message transmission, *Advances in Cryptology — CRYPTO 2006*, Lecture Notes in Computer Science 4117, pp.394–408, Springer (2006).
3. M. Ben-Or, S. Goldwasser, and A. Wigderson: Complete theorem for non-cryptographic fault-tolerant distributed computation, in *Proc. the 20th Annual Symposium on Theory of Computation (STOC'88)*, pp.1–10 (1988).
4. B. Chor and E. Kushilevitz: A communication-privacy tradeoff for modular addition, *Information Processing Letters*, 45(4):205–210 (1993).
5. B. Chor and N. Shani: The privacy of dense symmetric functions, *Computational Complexity*, 5(1):43–59 (1995)
6. D. Dolev, C. Dwork, O. Waarts, and M. Yung: Perfectly secure message transmission, *J. ACM* 40(1):17–47 (1993).
7. M. Franklin and R. N. Wright: Secure communication in minimal connectivity models, *J. Cryptology* 13(1):9–30 (2000).
8. J. A. Garay and R. Ostrovsky: Almost-everywhere secure computation, *Advances in Cryptology — EUROCRYPT 2008*, Lecture Notes in Computer Science 4965, pp.307–323, Springer (2008).
9. R. M. Gray: Toeplitz and circulant matrices: A review, Foundations and Trends in Communications and Information Theory, Vol.2, No.3, pp.155–239 (2006).
10. O. Goldreich: *Foundations of Cryptography, Volume 2: Basic Applications*, Cambridge University Press (2009).
11. O. Goldreich, S. Micali, and A. Wigderson: How to play any mental game or a complete theorem for protocols with honest majority, in *Proc. the 19th Annual ACM Symposium on Theory of Computation (STOC'87)*, pp.218–229 (1987).
12. M. Hayashi: *Group Representation for Quantum Theory*, Springer (2017).
13. M. Hayashi and T. Koshiba: Universal construction of cheater-identifiable secret sharing against rushing cheaters without honest majority, to appear in *Proc. 2018 IEEE Symposium on Information Theory (ISIT 2018)*. Also available in arXiv:1701.04470 (2017).
14. M. Hayashi, in preparation.
15. Y. Ishai, R. Ostrovsky, and H. Seyalioglu: Identifying cheaters without an honest majority, in *Proc. the 9th Theory of Cryptography Conference (TCC 2012)*, Lecture Notes in Computer Science 7194, pp.21–38, Springer (2012).
16. H. Krawczyk: New hash functions for message authentication, *EUROCRYPT'95*, Lecture Notes in Computer Science 921, pp.301–310, Springer (1995).
17. T. Koshiba and S. Sawada: Public discussion must be back and forth in secure message transmission, in *Proc. the 13th International Conference on Information Security and Cryptology (ICISC 2010)*, Lecture Notes in Computer Science 6829, pp.325–337, Springer (2011).
18. K. Kurosawa and K. Suzuki: Truly efficient 2-round perfectly secure message transmission scheme, *IEEE Transactions on Information Theory* 55(11):5223–5232 (2009).
19. D. Markham and A. Krause: A simple protocol for certifying graph states and applications in quantum networks, arXiv: 1801.05057 (2018).

20. U. M. Maurer: A unified and generalized treatment of authentication theory, in *Proc. the 13th Annual Symposium on Theoretical Aspects of Computer Science (STACS'96)*, Lecture Notes in Computer Science 1046, pp.387–398 Springer (1996).
21. T. Rabin and M. Ben-Or: Verifiable secret sharing and multiparty protocols with honest majority, in *Proc. the 21st Annual ACM Symposium on Theory of computing (STOC 1989)*, pp.73–85 (1989).
22. P. S. Roy, A. Adhikari, R. Xu, K. Morozov, and K. Sakurai: An efficient t-cheater identifiable secret sharing scheme with optimal cheater resiliency, Cryptology Eprint Archive 2014/628 (2014).
23. A. Shamir: How to share a secret, *Communications of the ACM*, 22(11):612–613 (1979).
24. 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).
25. G. Spini and G. Zémor: Perfectly secure message transmission in two rounds, *Proc. the 14th Theory of Cryptography Conference (TCC2016-B)*, Lecture Notes in Computer Science 9985, pp.286–304, Springer (2016).
26. R. Xu, K. Morozov, and T. Takagi: On cheater identifiable secret sharing schemes secure against rushing adversary, in *Proc. the 8th International Workshop on Security (IWSEC 2013)*, Lecture Notes in Computer Science 8231, pp.258–271, Springer (2013).
27. R. Xu, K. Morozov, and T. Takagi: Cheater identifiable secret sharing schemes via multi-receiver authentication, in *Proc. the 9th International Workshop on Security (IWSEC 2014)*, Lecture Notes in Computer Science 8639, pp.72–87, Springer (2014).