Quantum Information Processing (2022) 21:291
https://doi.org/10.1007/s11128-022-03639-x

Quantum verifiable protocol for secure modulo zero-sum randomness

Masahito Hayashi[1,2,3,4] · **Takeshi Koshiba**[5,6]

Received: 28 May 2022 / Accepted: 25 July 2022 / Published online: 13 August 2022

Abstract

We propose a new cryptographic resource, secure modulo zero-sum randomness, as a resource to implement a task of secure modulo summation, and its quantum protocol. Secure modulo summation is the calculation of modulo summation $Y_1 + \cdots + Y_m$ when m players have their individual variables $Y_1, \ldots, Y_m$ with keeping the secrecy of the individual variables. Secure modulo zero-sum randomness is a set of m variables $X_1, \ldots, X_m$ held by m players that satisfy the zero sum condition $X_1 + \cdots + X_m = 0$ with a certain security condition. This paper explains the relation between these two concepts and proposes a quantum verifiable protocol for secure modulo summation. The advantage for quantum protocol is the verifiability based on self-testing, which does not need to trust measurement devices and can be realized by using a statistical concept, significance level, while any classical method needs to trust several components of the protocol. Then, we propose various cryptographic applications for secure modulo zero-sum randomness. We also compare our quantum verifiable protocol with the conventional method for secure modulo summation.

✉ Masahito Hayashi
hayashi@sustech.edu.cn

Takeshi Koshiba
tkoshiba@waseda.jp

1 Shenzhen Institute for Quantum Science and Engineering, Southern University of Science and Technology, Nansan District, Shenzhen 518055, Guangdong, China

2 International Quantum Academy (SIQA), Futian District, Shenzhen 518048, Guangdong, China

3 Guangdong Provincial Key Laboratory of Quantum Science and Engineering, Southern University of Science and Technology, Nansan District, Shenzhen 518055, Guangdong, China

4 Graduate School of Mathematics, Nagoya University, Chikusa-ku, Nagoya 464-8602, Aichi, Japan

5 Faculty of Education and Integrated Arts and Sciences, Waseda University, Tokyo 169-8050, Japan

6 Quantum Computing Center, Keio University, Yokohama, Kanagawa 223-8522, Japan

Keywords Secure multiparty computation · Modulo summation · Quantum verification · Collusion resistance · Self-testing

1 Introduction

1.1 Quantum secure modulo summation via secure modulo zero-sum randomness and its verification

Recently, the development of quantum information processing has been actively studied. However, its advantageous application over classical information processing is limited. To enhance the study of this direction, we need to find more applications that have clear advantage over classical information processing. To propose such an application, this paper focuses on secure modulo summation and a new cryptographic concept, secure modulo zero-sum randomness.

Secure multiparty computation is an interesting topic in quantum information processing. Secure modulo summation is a typical example of secure multiparty computation [1, 2]. Using secure modulo summation, we can realize visual secret sharing [3, 4]. In this problem, m players have their individual variables $Y_1, \ldots, Y_m$. Unlike blind quantum computing [5–11], this problem setting assumes no server and discusses the secrecy of the variable Y_i to other players. The goal of a typical case is that all players commonly obtain the modulo summation $Y_1 + \cdots + Y_m$. We write modulo 2 sum by $+$ in this paper. As the secrecy condition, Player i's variable Y_i is not leaked to other players even when remaining $m-2$ players collude at most, which is referred as the minimum non-collusion condition. The key point of this discussion is that all players are divided into at least three groups. In fact, if all players are divided into only two groups, it is impossible to realize the secrecy for both groups simultaneously [12]. So many existing classical protocols realize this task by employing so many secret channels. If information on all the secret channels is leaked to the third party, the secrecy of Player i's variable Y_i does not hold. That is, to guarantee the secrecy, each player needs to verify all secret channels.

However, it is not a trivial task for Player i to realize secret channels without trusting other players. For example, the conventional quantum key distribution [13] realizes secure keys for secret channels, but the sender and the receiver are needed to be trusted. To resolve this problem, one can employ device independent quantum key distribution, which works even when the sender nor the receiver is not trusted [14–17]. This method essentially employs self-testing. However, even when quantum channels are available, it requires complicated combinations of use of quantum channels dependently on our assumption. For example, if Player i wants to verify the secrecy of the key to be shared by two other players, Player i needs to verify the quantum channel between the two players. For this aim, Player i needs to communicate with the two players via secret channels. Therefore, Player i consumes so many secret keys shared with the two players. In this way, the verification of conventional methods is not so simple. Although several quantum protocols for secure modulo summation are proposed [18–21], their verification has not been discussed.

The aim of this paper is to provide a construction of a more direct quantum protocol for secure modulo summation with verification. Moreover, we propose modulo zero-sum randomness as another new concept. 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. Secure modulo zero-sum randomness is a generalization of secure agreed key. When m players exist, secure modulo zero-sum randomness is given as random numbers X_i in $\mathbb{F}_2^c$ 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. The secure modulo zero-sum randomness is a kind of correlated randomness. Once m players share secure modulo zero-sum randomness, using broadcast public channel, i.e., a special channel that cannot be altered nor blocked and can be broadcast to all players, the m players can realize secure modulo summation.

The big advantage of use of quantum system is self-testing. Self-testing offers the verification of quantum measurement and states only with the minimum assumption [14, 15, 22–26]. That is, we do not need to trust any quantum device nor other players, and it is sufficient to assume the independence among several measurement devices. Although the stabilizer test can verify the GHZ state, it needs to assume that all players are trusted, which is different from the assumption of secure multiparty computation [7]. We propose a quantum protocol to generate secure modulo zero-sum randomness as follows. First, the m players share the GHZ state with respect to the phase basis. Then, they measure their own system with computation basis. Since the GHZ state can be regarded as a two-colorable graph state, it can be verified by self-testing [22, 25, 26]. However, all players need to verify it without trusting other players only with the minimum non-collusion condition. Due to this requirement, we cannot directly apply the existing methods for self-testing of the GHZ state because they did not care the minimum non-collusion condition. In this paper, similar to the references [26–28], using a statistical concept, significance level (or confidence level), we propose a new self-testing protocol to verify the GHZ state under the minimum non-collusion condition. This protocol is designed so that each player can verify a certain secrecy criterion of the generated GHZ state when $m-2$ remaining players collude at most. Combining them, we can realize a quantum protocol for secure modulo summation with verification. Also, we clarify that our method has an advantage over the simple combination of self-testing of Bell state.

1.2 Application of secure modulo zero-sum randomness

Although secure modulo zero-sum randomness realizes secure modulo summation in the above way and secure modulo summation can be applied to visual secret sharing [3, 4], secure modulo zero-sum randomness has many other useful applications as follows. These applications show usefulness of our verifiable quantum protocol to generate secure modulo zero-sum randomness.

- **Application to secret sharing:** In the standard setting of multi-party secure computation, many cryptographic protocols require secure communication channels between any distinct two players [29, 30]. For example, secure multi-party computation for homomorphic functions can be realized without honest majority, but it requires so many secure communication channels [1]. Also, any existing secret sharing protocol requires many secure communication channels [31–38]. In this paper, using the secure modulo zero-sum randomness, we propose protocols to realize these tasks without secure communication channels (but broadcast 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 honest majority nor secure communication channels. Also, based on the same resource, we construct secret sharing protocols without secure communication channels. We first give a basic protocol for secret sharing without secure communication channels. Then, utilizing universal hash functions, we adapt the basic protocol to a cheater detectable protocol without secure communication channels.
- **Application to securely computing additively homomorphic functions:** A standard method for multi-party secure computation requires honest majority or secure communication channels. Another method based on secure message transmission [39–42][1] realizes multi-party secure computation without honest majority nor secure communication channels. Instead of secure communication channel, we can employ secure message transmission, which is a cryptographic protocol between two parties, between which there are several channels, but some of them are corrupted, 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 *perfectly* secure message transmission, honest majority over the channels is required. If the broadcast public channel is available in secure message transmission, then such a barrier can be overcome [48–50] and multi-party secure computation can be realized by using secure message transmission with the broadcast public channel [51]. However, the respective simulations of the secure communication channels are quite inefficient. To resolve this problem, based on the secure modulo zero-sum randomness, this paper proposes an alternative method for securely computing additively homomorphic functions. Our protocol uses only broadcast public channel as well as the secure modulo zero-sum randomness.
- **Application to multi-party anonymous unanimous approval:** As another application, we propose *multi-party anonymous unanimous approval*, 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

[1] The same task as one-round secure message transmission can be realized as a special case of secure network coding without public channel [43–47]. The above special case means the case when the sender and the receiver are connected via several parallel channels.

secure modulo zero-sum randomness, we construct a protocol to realize multi-party anonymous unanimous approval 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.

1.3 Organization of this paper

This paper is organized as follows. Section 2 defines a new cryptographic resource *modulo zero-sum randomness* and discusses the equivalence to related secure computation protocols. Section 3 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. Section 4 provides secret sharing protocols without secure communication channels. Section 5 proposes a new cryptographic task *multi-party anonymous unanimous approval*, which employs modulo zero-sum randomness. By combining the results in Sects. 2 and 3, Sect. 6 extends the results in Sect. 2 to secure computation with respect to additively homomorphic functions. Section 7 proposes a quantum verifiable protocol for secure modulo summation. Section 8 compares our method with other methods. Section 9 gives the security proofs of our protocols. Section 10 makes conclusion. Appendix 1 shows the security of our quantum verifiable protocol given in Sect. 7. Appendix 1 gives the generalization to the case with a general finite filed $\mathbb{F}_q$ when we trust our measurement devices. Other appendices are denoted for the preparations for Appendix 1.

2 Secure modulo zero-sum randomness

First, we give the rigorous definition of secure modulo zero-sum randomness for the random numbers $X_i \in \mathbb{F}_2^c$ with $i = 1, \ldots, m$ under the ideal case.

Definition 1 (*Ideal case*) The random numbers $X_i \in \mathbb{F}_2^c$ with $i = 1, \ldots, m$ are called *secure modulo zero-sum randomness* when the following conditions hold.

- (Z1) *Modulo zero condition*: The relation $\sum_{i=1}^m X_i = 0$ holds.
- (Z2) *Independence condition*: Any $m - 1$ variables among $X_1, \ldots, X_m$ are independent of each other and subject to the uniform distribution.
- (Z3) *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.

Using modulo zero-sum randomness, we can realize the secure calculation of the modulo sum $Y_1 + \cdots + Y_m$ as a function with m inputs $Y_i \in \mathbb{F}_2^c$ without revealing the information for respective inputs. 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 multi-party computation for modulo sum is possible without honest majority [1]. That is, even when the majority of players do not behave 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 broadcast public channels, it is natural to employ cryptographic resources.

Now let us define the task of secure modulo summation when player j has the secret input $Y_j \in \mathbb{F}_2^c$ for $j = 1, \dots, m$.

(M1) *Reliability condition*: Any player i must calculate the modulo sum $Y_1 + \cdots + Y_m$ when all players are honest.

(M2) *Secrecy condition*: Assume that $m-2$ players except for Player j collude at most, which is called the *minimum non-collusion condition*. Also, their variables $Y_1, \dots, Y_m$ are assumed to be independent of each other and subject to the uniform distribution. Then, the variable X_j of player j is independent of the information Z obtained by the $m-2$ colluded players. That is, the relation $I(X_j; Z) = 0$ holds.

In secure computation, the aim of the adversarial is maliciously getting the input of the legitimate user. Hence, we do not care about the possibility that the adversarial disturbs the computation. As an optional requirement of secure computation, we often consider the following condition so-called fairness [52–54]; if the adversarial obtains an output, then the legitimate user also obtains the same output. Since this requirement is optional, we do not consider this condition. Indeed, we trivially obtain Theorem 1 (Fig. 1).

Protocol 1 Secure modulo sum protocol from secure modulo zero-sum randomness

STEP 1: Player i sends the information $Z_i := Y_i + X_i$ to all players via broadcast public channel.
STEP 2: Each player calculates $\sum_{i=1}^m Z_i$, which equals $\sum_{i=1}^m Y_i$.

Theorem 1 *Protocol 1 realizes secure modulo summation when secure modulo zero-sum randomness $X_1, \dots, X_m$ is shared. That is, when Protocol 1 is implemented by exchanging Z_j with $j = 1, \dots, m$, each player i obtains the modulo summation $\sum_{j=1}^m Y_j$ without revealing his/her own information Y_i unless all other players collude.*

This theorem can be generalized to secure multi-party computation of general homomorphic functions (see Sect. 6). This theorem can shown as follows. Since reliability condition holds for the equality $\sum_{i=1}^m Z_i = \sum_{i=1}^m Y_i$, we show only secrecy condition.

Due to the symmetry, it is sufficient to show the secrecy condition only for player 1 when $m-2$ players $3, \dots, m$ collude. The $m-2$ players have variables $X_3, \dots, X_m, Y_3, \dots, Y_m, Z_1, Z_2$. Since $Y_3, \dots, Y_m$, are independent of $X_3, \dots, X_m, X_1 + Y_1, X_2 + Y_2, Y_1$, we have

$$I(X_3, \dots, X_m, Y_3, \dots, Y_m, Z_1, Z_2; Y_1) \tag{1}$$

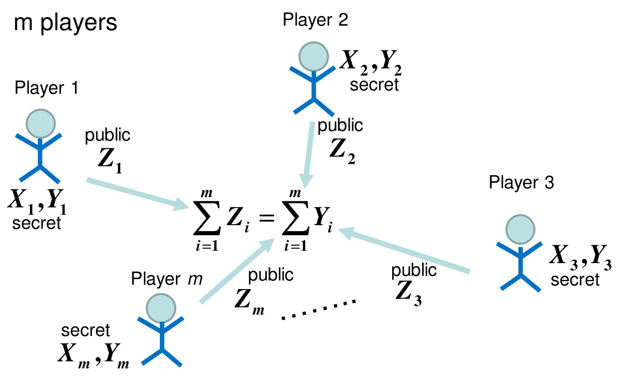

Fig. 1 Secure modulo sum protocol from secure modulo zero-sum randomness among m players. Each player j has randomness X_j, which satisfies the condition for secure modulo zero-sum randomness. Also, Each player j has another randomness Y_j. They intend to calculate the modulo sum $\sum_{j=1}^{m} Y_j$. They exchange $Z_j = X_j + Y_j$ via public channel

$$= I(X_3, \dots, X_m, X_1 + Y_1, X_2 + Y_2; Y_1), \tag{2}$$

where $I(A; B)$ means the mutual information between two systems A and B.

Since Y_2 is subject to the uniform distribution, $X_3, \dots, X_m, X_1, X_2 + Y_2$ are independent of each other and subject to the uniform distribution. Hence, $H(X_3, \dots, X_m, X_1+Y_1, X_2+Y_2|Y_1) = m \log 2$, which equals $H(X_3, \dots, X_m, X_1+Y_1, X_2+Y_2)$. Thus, $I(X_3, \dots, X_m, X_1+Y_1, X_2+Y_2; Y_1) = 0$, which shows secrecy condition.

Indeed, when secure modulo zero-sum randomness $X_1, \dots, X_m$ is shared, Protocol 2 realizes secure modulo summation as stated in Theorem 2. Further, the discussion in this section can be trivially extended to the case with replacement of $\mathbb{F}_2$ by $\mathbb{Z}_d$ and $\mathbb{F}_q$.

Theorem 2 *Protocol 2 realizes secure modulo zero-sum randomness.*

This theorem is shown in Sect. 9.1.

Protocol 2 Generation of secure modulo zero-sum randomness from secure modulo summation protocol

STEP 1: Player i generates the variable Y_i subject to the uniform distribution, which is independent of other variables.
STEP 2: All players calculate the modulo summation $\sum_{i=1}^{m} Y_i$ by the secure modulo summation protocol.
STEP 3: Player 1 set the variable $X_1 := Y_1 - \sum_{i=1}^{m} Y_i$. Player i set the variable $X_i := Y_i$ for $i = 2, \dots, m$.

3 Quantum protocol for secure modulo zero-sum randomness

Now, 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 $\{|z\rangle_p\}_{z\in\mathbb{F}_2}$ is defined

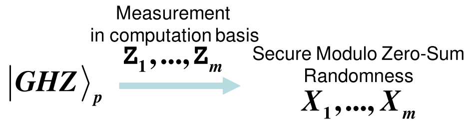

Fig. 2 Quantum generation of secure modulo zero-sum randomness. When the initial state is the GHZ state in phase basis, the measurement outcome in computational basis is secure modulo zero-sum randomness

as

$$|z\rangle_p := \frac{1}{\sqrt{2}} \sum_{x \in \mathbb{F}_2} (-1)^{xz} |x\rangle,$$

where $|x\rangle$ expresses the computational basis.

The phase GHZ state $|GHZ\rangle_p := \frac{1}{\sqrt{2}} \sum_{z \in \mathbb{F}_2} |z, \ldots, z\rangle_p$ is calculated as

$$|GHZ\rangle_p = \frac{1}{\sqrt{2^{m-1}}} \sum_{x_1,\ldots,x_m \in \mathbb{F}_2 : x_1+\cdots+x_m=0} |x_1, \ldots, x_m\rangle. \tag{3}$$

When all the players apply the measurement on the computational basis to the system whose initial state is $|GHZ\rangle_p$, Player i obtains the variable X_i. Then, the sum of m outcomes, i.e., $\sum_{i=1}^m X_i$ is zero, and $m-1$ outcomes are subject to the uniform distribution as Fig. 2. Hence, these outcomes satisfy the conditions of secure modulo zero-sum randomness. That is, when the initial state is guaranteed to be $|GHZ\rangle_p$, it is guaranteed that the outcomes are secure modulo zero-sum randomness.

When the m players apply Protocol 1 to the generated secure modulo zero-sum randomness, they can realize secure modulo summation. To verify its secrecy, each player has to verify the generated secure modulo zero-sum randomness. In secure modulo summation, when we focus on Player j, we assume that $m-2$ remaining players collude at most. Hence, Player j needs to verify that the colluded players have no information with respect to X_j under this assumption.

Definition 2 (*Player j's assumption*) If the following three conditions hold, we say that *Player j's assumption* holds.

(P1) Player j's quantum measurement has no correlation with those of other players.
(P2) Remaining players are divided into two groups S_1 and S_2, where the choice of this division is arbitrary. Both groups are not empty. There is no correlation between the two groups S_1 and S_2. That is, the groups S_1 and S_2 do not collude with each other.
(P3) Player j does not know the separation of remaining players by S_1 and S_2.

Indeed, when we trust their measurement devices, as Fig. 3, we can verify the state $|GHZ\rangle_p$ by using the two projections defined by

$$\begin{aligned}\tilde{P}_1 &:= \sum_{x_1,\ldots,x_m : x_1+\cdots+x_m=0} |x_1, \ldots, x_m\rangle\langle x_1, \ldots, x_m| \\ &= \frac{1}{2}(I + \mathsf{Z}_1 \cdots \mathsf{Z}_m) \end{aligned} \tag{4}$$

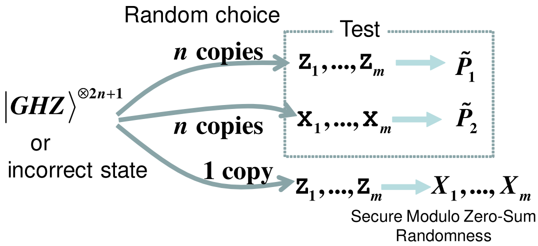

Fig. 3 Verification of GHZ state with trusted measurement device. We apply the random sampling test to verify the GHZ state

$$\tilde{P}_2 := \sum_z |z, \ldots, z\rangle_p\ {}_p\langle z, \ldots, z| = \prod_{i;i\neq j} \frac{1}{2}(I + \mathsf{X}_j\mathsf{X}_i), \tag{5}$$

where $\mathsf{Z} := \sum_x (-1)^x |x\rangle\langle x|$ and $\mathsf{X} := \sum_x |x+1\rangle\langle x|$. Here, the subscript of Z and X expresses the Hilbert space to be acted. Equation (5) shows that $\tilde{P}_2$ is written as the RHS for any $j = 1, \ldots, m$. For example, when j is fixed, the RHS of (5) means that the test $\tilde{P}_2$ is passed when the relation $\mathsf{X}_j = \mathsf{X}_i$ holds for any $i \neq j$. Hence, it is passed if and only if all variables $\mathsf{X}_1, \ldots, \mathsf{X}_m$ are the same.

Now, we assume that we prepare $2n + 1$ copies. Then, we randomly choose n copies and apply the test $\tilde{P}_1$. Also, we randomly choose n copies from the remaining $n + 1$ copies and apply the test $\tilde{P}_2$. If these tests are passed, the remaining copy can be considered to be close to the true state $|GHZ\rangle_p$. That is, applying the bit basis measurement to the remaining copies, we obtain the secure modulo zero-sum randomness. Combining Protocol 2, we can realize a quantum protocol for secure modulo summation with verification. This discussion can be extended to the case with a general finite field $\mathbb{F}_q$. Appendix 1 gives this generalization with a formal statement of this test.

However, when we cannot trust their measurement devices, the above method does not work. This problem can be resolved by using self-testing for the GHZ state, whose detail is described in Method section by employing a statistical concept, significance level in a way similar to the references [26–28].

4 Application 1: Secret sharing without secure communication channel

There are many secret sharing protocols, but these protocols require secure communication channel in the dealing phase [31]. The aim of this section is proposing a secret sharing protocol without use of secure communication channel as follows.

For this aim, in the discussions in Sects. 4, 5, and 6, we employ the finite field $\mathbb{F}_q$, where q is a power of 2. In this case, the finite field $\mathbb{F}_q$ can be regarded as an ℓ-dimensional vector space over $\mathbb{F}_2$. Hence, a c-dimensional vector space over $\mathbb{F}_q$ can be regarded as $\mathbb{F}_2^{c\ell}$. That is, a secure modulo zero-sum randomness $X_i \in \mathbb{F}_q^c$ with $i = 1, \ldots, m$ is defined as a secure modulo zero-sum randomness $X_i \in \mathbb{F}_2^{c\ell}$ with $i = 1, \ldots, m$. However, the discussions in Sects. 6, 4, and 5 can be extended to the

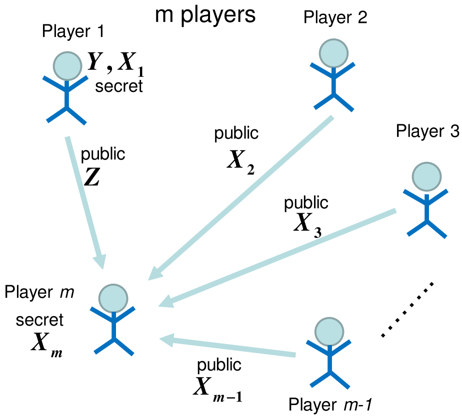

Fig. 4 Secret sharing without secure communication channel. This picture is applied to Protocols 3 and 4. The information Z sent via the public channel is defined dependently of which protocol is applied

case with a general finite field $\mathbb{F}_q$ because these discussions hold by replacing $\mathbb{F}_2$ with $\mathbb{F}_q$.

4.1 Basic protocol

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 (Fig. 4).

Protocol 3 Secret sharing without secure communication channel

STEP 1: [Dealing] Player 1 sends the information $Z := X_1 + Y$ to Player m via broadcast public channel.
STEP 2: [Reconstruction 1] Players $2, \ldots, m-1$ send their randomness $X_2, \ldots, X_{m-1}$ to Player m via broadcast public channel.
STEP 3: [Reconstruction 2] 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 nonzero 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: [Dealing] Player 1 sends the information $Z := X_1 Y$ to Player m via broadcast public channel.
STEP 2: [Reconstruction 1] Players $2, \ldots, m-1$ send their randomness $X_2, \ldots, X_{m-1}$ to Player m via broadcast public channel.
STEP 3: [Reconstruction 2] If $Z \neq 0$, Player m defines $Y' := -Z(\sum_{i=2}^{m} X_i)^{-1}$. 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. First of all, we consider the security of Protocol 4 and the success probability of the reconstruction of Protocol 4 when all the players are honest.

Theorem 3 *Suppose that all the players are honest in Protocol 4. Then, Protocol 4 has the perfect secrecy and the success probability of the reconstruction is* $1 - q^{-c}$.

The proof of Theorem 3 is given in Sect. 9.2. In this proof, we show that the protocol works well when $X_1 = 0$ and all the players are honest.

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. 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 4 *When all of Players* $2, \ldots, m-1$ *in Protocol 4 collude for the modification attack, they succeed the modification attack with probability* $\frac{q}{q'}$.

In Theorem 4, the successful events of the modification attack contain the case when Player m cannot recover the information Y due to $X_1 = 0$. The proof of Theorem 4 is also given in Sect. 9.2. Regardless of the modification attack (in the setting of Theorem 4), Protocol 4 maintains the perfect secrecy as discussed in the proof of Theorem 3.

Indeed, there exist so many secret sharing protocols with dishonest players. Some of them can identify the cheating players [32–38]. 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 Application 2: Multi-party anonymous unanimous approval

To consider a new cryptographic task, we 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.

5.1 Naive protocol

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

5.2 Basic protocol

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. This task is called *multi-party anonymous unanimous approval*.

To prevent a mismatched recognition, as illustrated in Fig. 5, attaching the message authentication protocol [55, 56] to information Y, we propose the following protocol as Protocol 5. As a preparation of Protocol 5, from secure modulo zero-sum randomness $X_i = (X_{i;k}) \in \mathbb{F}_q^c$ for $i = 1, \dots, m$, we generate an $e \times d$ Toeplitz matrix $T_i = (T_{i;k,l})_{k,l}$ and a variable $A_i = (A_{i;k}) \in \mathbb{F}_q^e$, where we choose the integers e and d to satisfy $2e + d - 1 = c$. That is, the component $T_{i;k,l}$ is given as $X_{i;k+l-1}$ and the component $A_{i;k}$ is given as $X_{i;e+d-1+k}$. (Note that Toeplitz matrices can be used universal hash functions. You may consult with a textbook [57].) 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.

Protocol 5 Multi-party Anonymous Unanimous Approval

STEP 1: [Voting] Player i sends $B_i \in \mathbb{F}_q^e$ to the remaining players via broadcast public channel. If Player i agrees on 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] Each player calculates $\sum_{i=1}^{n} B_i$. If the sum is zero, the project can be considered to be approved.

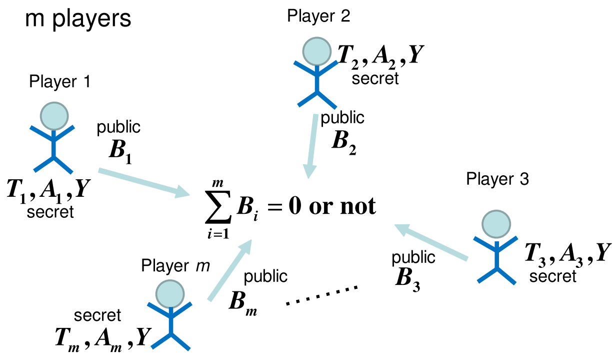

Fig. 5 Multi-party anonymous unanimous approval. Players exchange B_j and check whether the relation $\sum_{i=1}^{m} B_i = 0$

5.3 Analysis with honest players

When all the players send $T_i Y + A_i$ based on the same variable Y, we have $\sum_{i=1}^{m} B_i = \sum_{i=1}^{m} T_i Y + A_i = (\sum_{i=1}^{m} T_i)Y + (\sum_{i=1}^{m} A_i) = 0Y + 0 = 0$ 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 on the project and/or at least one player recognizes a different information from Y. For this aim, we have the following two theorems.

Theorem 5 *When at least one Player i' disagrees on the project, the probability of $\sum_{i=1}^{m} B_i = 0$ is q^{-e} whatever distribution the variable Y obeys.*

Theorem 5 can be shown as follows. Since $B_{i'}$ is subject to the uniform distribution on $\mathbb{F}_q^e$, the probability of $\sum_{i=1}^{m} B_i = 0$ is q^{-e}.

Theorem 6 *When all the players agree on the project and at least one Player i recognizes the information Y_i that is different from the information Y_1 recognized by Player 1, the probability of $\sum_{i=1}^{m} B_i = 0$ is q^{-e} whatever distribution the variable Y obeys.*

This theorem ensures that if the project is approved by this protocol, all the players confirm no mismatched recognition. Theorem 6 can be shown as follows. 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 Player 1. Also assume that other players recognize the same information Y_1 recognized by Player 1. We define the variable $V_{i_j} := Y_{i_j} - Y_1$ for $j = 1, \ldots, k$. Then, we have

$$\sum_{i=1}^{m} B_i = \sum_{j=1}^{k} T_{i_j} V_{i_j}. \tag{6}$$

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 in Theorem 6.

5.4 Analysis with malicious player

Now, we consider a set of malicious players. When malicious Player j makes *rushing*, Player j can realize the situation $\sum_{i=1}^m B_i = 0$ by sending $-\sum_{i \neq j} B_i$ unless all the players do not approve the same variable Y. Hence, when we employ Protocol 5, we need to trust all the players. To avoid the rushing attack, we propose another protocol (Protocol 6), which trusts only Player s.

Protocol 6 Secure multi-party anonymous unanimous approval with trusted player s

STEP 1: [Voting] Player i sends $B_i \in \mathbb{F}_q^e$ to Player 1 via broadcast public channel. If Player i agrees on 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 s calculates $\sum_{i=1}^m B_i$, where $B_s := T_s Y + A_s$. If it is zero, the project can be considered to be approved.

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

Here, for the notational convenience, we assume that Players $l, \ldots, m$ are malicious with $l \geq 3$ and Player s is one player among Players $1, \ldots, l-1$. Now, we consider the following type of malicious players. Assume that malicious Players $l, \ldots, m$ want to make the following situation by colluding together. Players $1, \ldots, l-1$ consider that the project is described by distinct variables $Y_1, \ldots, Y_{l-1}$, and they approve this project based on this incorrect information. Then, Player s announces that all the players 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 7 *In Protocol 6, malicious colluded Players $l, \ldots, m$ succeed the above attack with probability q^{-e} whatever distribution the variable Y obeys.*

Theorem 7 is shown in Sect. 9.3. When Player s cannot be trusted, Protocol 6 with trusted Player s does not necessarily work properly. Instead, we need to employ the following protocol. That is, due to Theorem 7, once a project is approved by Protocol 7, all players can consider that all payers approve the same project description Y.

Protocol 7 Secure multi-party anonymous unanimous approval without trusted player

STEP 1: [m applications] Protocol 6 with trusted Player s is performed for $s = 1, \ldots, m$.

STEP 2: [Verification] If the all players announce that the project is approved, the project can be considered to be approved.

Further, as a corollary of Theorem 7, we can guarantee the performance of Protocol of 7 as follows.

Corollary 8 *In Protocol 7, when the number of malicious colluded players is less than $m-1$, the malicious colluded players succeed the above attack with probability q^{-e} whatever distribution the variable Y obeys.*

6 Application 3: Secure multi-party computation of homomorphic functions

The aim of this section is proposing a method for securely computing additively homomorphic functions based on the secure modulo zero-sum randomness. Our protocol uses only broadcast public channel as well as the secure modulo zero-sum randomness. 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,

$$f(Y_1, \dots, Y_m) = \tilde{f}(\alpha_1 Y_1 + \cdots + \alpha_m Y_m), \tag{7}$$

where $\alpha_1, \dots, \alpha_m$ are all in $\mathbb{F}_q^c$ and $\tilde{f} : \mathbb{F}_q^c \to \mathbb{F}_q^c$ is 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.

Protocol 8 Secure Computation for an additively homomorphic function f that satisfies property (7)

A standard method for multi-party secure computation requires honest majority or secure communication channels. Another method based on secure message transmission [39–42][2] realizes multi-party secure computation without honest majority nor secure communication channels. Instead of secure communication channel, we can employ secure message transmission, which is a cryptographic protocol between two parties, between which there are several channels but some of them are corrupted, 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 *perfectly* secure message transmission, honest majority over the channels is required. If the broadcast public channel is available in secure message transmission, then such a barrier can be overcome [48–50] and multi-party secure computation can be realized by using secure message transmission with the broadcast public channel [51]. However, the respective simulations of the secure communication channels are quite inefficient. To resolve this problem, based on the secure modulo zero-sum randomness, this paper proposes an alternative method for securely computing additively homomorphic functions. Our protocol uses only broadcast public channel as well as the secure modulo zero-sum randomness.

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 $Z_1, \dots, Z_m$ and computes $\sum_{i=1}^m Z_i$.

The task can be realized in Protocol 8, which employs secure modulo zero-sum randomness $X_i \in \mathbb{F}_q^c$ for $i = 1, \dots, m$ and the broadcast public channel. That is, a player sends a message via the public channel, any other users can receive the same message. The security is defined in terms of the real/ideal paradigm of the universal composability [58, 59]. We will consider the security in the $(\mathcal{F}_{pub}, \mathcal{F}_{mzsr})$-hybrid model, where $\mathcal{F}_{pub}$ is a functionality of the broadcast public channel and $\mathcal{F}_{mzsr}$ is a functionality of the modulo zero-sum randomness. So, it is enough to provide simple definitions (without interaction with the adversary) of the functionalities.

Functionality $\mathcal{F}_{pub}$ (simple form)

Upon receiving $(Send, sid, R, x)$ from Party i, $\mathcal{F}_{pub}$ outputs $(Sent, sid, i, R, x)$ to all parties in R, where sid is a session id and R is a list of receivers of a message x.

Functionality $\mathcal{F}_{mzsr}$ (simple form)

$\mathcal{F}_{mzsr}^{q,c}$ proceeds as follows, when parameterized by the alphabet size q and the length c.

Upon receiving $(Request, sid)$ from Party i, $\mathcal{F}_{mzsr}^{q,c}$ generates modulo zero-sum randomness $X_1, \ldots, X_m$, each in $\mathbb{F}_2^c$, satisfying the modulo zero-sum condition and the independence condition and outputs $(Response, sid, i, j, X_j)$ to Party j for each $j = 1, \ldots, m$.

Now, we are ready to give the definitions of the correctness and the privacy.

Definition 3 Let $f(x_1, \ldots, x_m)$ be an m-party functionality and π be an m-party protocol. We say that the protocol is *correct* if honest parties do not get incorrect values in the presence of the adversary.

In fact, if π is correct, then the following holds.

(H1) The protocol aborts whenever it detects a cheating behavior of the adversary, or
(H2) honest parties must get the correct values if π does not abort.

Definition 4 Let $f(x_1, \ldots, x_m)$ be an m-party functionality and π be an m-party protocol. We say that the protocol *τ-securely computes f* with *perfect privacy* if there exists a simulator $\mathcal{S}$ for which the following holds. For any subset of corrupted parties $T \subseteq \{1, \ldots, m\}$ at most size τ by the adversary $\mathcal{A}$ and every m-tuple of inputs $\boldsymbol{x} = (x_1, \ldots, x_m)$, two probability distributions $Ideal_{f,\mathcal{S}}(\boldsymbol{x})$ and $Real_{\pi,\mathcal{A}}$ are identical.

1. $Ideal_{f,\mathcal{S}}(\boldsymbol{x})$ is defined as

$$(\mathcal{S}(T, \boldsymbol{x}[T], \boldsymbol{y}[T]), \boldsymbol{y}[\bar{T}]),$$

   where $\boldsymbol{y} = f(\boldsymbol{x})$, $\bar{T} = \{1, \ldots, m\} \setminus T$, and $\boldsymbol{v}[T]$ denotes the sub-vector $(v_j)_{j \in T}$ for a vector $\boldsymbol{v} = (v_1, \ldots, v_m)$. This is the joint distribution of the simulated view of the corrupted parties together with outputs of the honest parties in an ideal implementation of f.
2. $Real_{\pi,\mathcal{A}}$ is defined as

$$(View_{\pi,T}(\boldsymbol{x}), Output_{\pi,\bar{T}}(\boldsymbol{x})),$$

   where $View_{\pi,T}(\boldsymbol{x})$ is the joint view of the parties in T by executing π on input $\boldsymbol{x}$ and $Output_{\pi,\bar{T}}(\boldsymbol{x})$ is the output that π delivers to the honest parties in $\bar{T}$.

If f is a single-valued function and the functional value is required to be shared among all the parties, then we consider that $\boldsymbol{y} = (y, y, \ldots, y)$, where $y = f(\boldsymbol{x})$.

Theorem 9 *Let f be an additively homomorphic function of form Eq. (7). Then, Protocol 8 is correct in the semi-honest model.*

Theorem 9 can be shown as follows. Since the adversary does not alter Z_i due to the condition of broadcast public channel, each player can collect the correct values $Z_1, \ldots, Z_m$. Then each player computes

$$\begin{aligned}\sum_{i=1}^{m} Z_i &= \sum_{i=1}^{m} \tilde{f}(X_i + \alpha_i Y_i) \\ &= \tilde{f}\left(\sum_{i=1}^{m} X_i + \sum_{i=1}^{m} \alpha_i Y_i\right) = f(Y_1, \ldots, Y_m).\end{aligned} \tag{8}$$

This concludes the proof.

If we allow a malicious adversary $\mathcal{A}$, which can send a fake value for Z_i for Party i corrupted by $\mathcal{A}$. In this case, the correctness of Protocol 8 does not hold. A naive application of universal hash functions, which will be discussed in Application 2, does not work. In this paper, our concern is to demonstrate that the modulo zero-sum randomness contributes to simple cryptographic construction and thus we do not consider the correctness in the malicious model any more.

Theorem 10 *Let f be an additively homomorphic function of form Eq. (7). Then, f can be $(m-1)$-securely computed with perfect privacy by Protocol 8 in the $(\mathcal{F}_{pub}, \mathcal{F}_{mzsr})$-hybrid model.*

Theorem 10 is shown by following the convention in [60]. First, we assume that the adversary $\mathcal{A}$ collapses Players $1, \ldots, m-1$. Since Protocol 8 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, $Real_{\pi,\mathcal{A}}$ (with help of $\mathcal{F}_{pub}$ and $\mathcal{F}_{mzsr}$) is described as

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

since $\mathcal{A}$ can compute $Z_1, \ldots, Z_{m-1}$ and also $f(Y_1, \ldots, Y_m)$ from $Z_1, \ldots, Z_m$. Now, we construct a simulator $\mathcal{S}$ which takes $X_1, \ldots, X_{m-1}, Y_1, \ldots, Y_{m-1}$ as input with help of $\mathcal{F}_{mzsr}$. $\mathcal{S}$ can compute $Z_1', \ldots, Z_{m-1}'$ as $\mathcal{A}$ does. Also $\mathcal{S}$ can send $Y_1, \ldots, Y_{m-1}$ to the functionality f to get $f(Y_1, \ldots, Y_m)$. Then $\mathcal{S}$ 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 $Ideal_{f,\mathcal{S}}$ is identical to $Real_{\pi,\mathcal{A}}$.

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 $Real_{\pi,\mathcal{A}}$, which completes the proof of Theorem 10.

In the statement of Theorem 10, we do not clearly mention that the corruption is static or adaptive. Since Protocol 8 is essentially non-interactive, we do not distinguish static adversaries from adaptive ones.

7 Quantum verifiable generation of secure modulo zero-sum randomness

When we generate secure modulo zero-sum randomness from the GHZ state and we cannot trust their measurement devices, we need to employ the method of self-testing [14, 15, 22–26]. The following is the protocol to generate secure modulo zero-sum randomness with the verification by Player j. For this protocol, we prepare the following measurements.

$$\mathsf{A}(k) := (\mathsf{X} + (-1)^k \mathsf{Z})/\sqrt{2} \tag{9}$$

for $k = 0, 1$.

As requirements of verifiable generation of secure modulo zero-sum randomness for Player j, we focus on the following two concepts in the same way as [61]. One is *detectability*, which means that if the generated variables are not secure, such a faulty output is detected with high probability. That is, the generated variables $X_1, \dots, X_m$ should be close to the ideal variables when the test is passed. The detectability depends on the choice of the player. In this stage, only Player j's assumption is made, i.e., the state on the multiple-copy system does not necessarily have a tensor product form. The other is *acceptability*, which means that when all the players are honest, the verification should be passed with high probability. The acceptability does not depend on the player.

Then, we address Protocol 9 by Player j as Fig. 6. If they have the system of $4mn+1$ copies, Player j can verify the state of the remaining system by using Protocol 9. Here, to distinguish the real observable from the ideal observable, we denote the measured observables by $'$ (Table 1).

To rigorously discuss the detectability for Player j from a statistical viewpoint, we prepare a statistical concept, significance level, as follows [62].

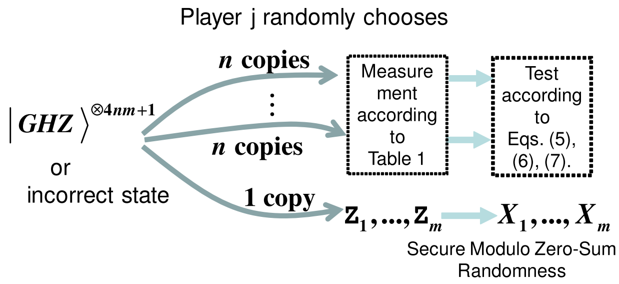

Fig. 6 Verification of GHZ state with untrusted measurement device for Player j. Player j verifies the GHZ state by using the random sampling

Protocol 9 Verifiable Generation of Secure Modulo Zero-Sum Randomness for Player j

STEP 1: One player, who is not necessarily trusted, prepares the system of $4mn+1$ copies, where each copy is composed of m qubits. Then, the player sends the respective qubits for all copies to the respective players. (Here, our result does not depend on the choice of this player. Hence, the player can be considered as an arbitrary player.)

STEP 2: Player j randomly divides the $4mn+1$ copies into $4m+1$ groups such that the final group is composed of one copy and the remaining groups are composed of n copies.

STEP 3: Players apply the measurement to the respective groups except for the final group as shown in Table 1.

STEP 4: Players except for Player j send their outcomes to Player j. Player j checks the following inequalities for their average values for $k=1,\ldots,j-1,j+1\ldots,m$.

$$\mathbb{A}[\mathsf{X}'_j\mathsf{X}'_k] \geq 1-\frac{c_1}{n}, \quad \mathbb{A}\Big[-\mathsf{Z}'_j\Big(\sum_{l\neq j}\mathsf{Z}'_l\Big)\Big] \geq 1-\frac{c_1}{n}, \tag{10}$$

$$\left|\mathbb{A}[\mathsf{Z}'_j]\right| \leq \frac{c_{1,0}}{\sqrt{n}} \tag{11}$$

$$\mathbb{A}\Big[\mathsf{A}(0)'_j\Big(\mathsf{X}'_k-\sum_{l\neq j}\mathsf{Z}'_l\Big)+\mathsf{A}(1)'_j\Big(\mathsf{X}'_k+\sum_{l\neq j}\mathsf{Z}'_l\Big)\Big] \geq 2\sqrt{2}-\frac{c_{1,0}}{\sqrt{n}}. \tag{12}$$

Here, $\mathbb{A}$ expresses the average of the observed values with respect to the observables inside of the bracket [ ]. The coefficients c_1 and $c_{1,0}$ can be chosen arbitrarily. If the above test is passed, Player j considers that the remaining copy is close to the phase GHZ state $|GHZ\rangle_p$.

STEP 5: Each Player k measures the final group with Z basis, and obtains the value X_k for $k=1,\ldots,m$.

Definition 5 (*Significance level*) If the following condition holds, we say that a condition $\mathcal{A}$ holds with *significance level* α when a test $\mathcal{T}$ is passed. Whatever malicious players make, if the resultant state σ after passing the test $\mathcal{T}$ does not satisfy the condition $\mathcal{A}$, the probability that the test $\mathcal{T}$ is passed is not greater than α. In other words, if the probability that the test $\mathcal{T}$ is passed is greater than α, if the resultant state σ after passing the test $\mathcal{T}$ satisfies the condition $\mathcal{A}$. That is, the significance level is the

Table 1 Measurement for each group

Group	Measurements
k-th group	$\mathsf{Z}'_j, \mathsf{X}'_k$
$m+k$-th group	$\mathsf{X}'_j, \mathsf{X}'_k$
$2m+k$-th group	$\mathsf{A}(0)'_j, \mathsf{X}'_k$
$3m+k$-th group	$\mathsf{A}(1)'_j, \mathsf{X}'_k$
j-th group	$\mathsf{Z}'_j, \mathsf{Z}'_1, \ldots, \mathsf{Z}'_{j-1}, \mathsf{Z}'_{j+1}, \ldots, \mathsf{Z}'_m$
$m+j$-th group	$\mathsf{X}'_j, \mathsf{Z}'_1, \ldots, \mathsf{Z}'_{j-1}, \mathsf{Z}'_{j+1}, \ldots, \mathsf{Z}'_m$
$2m+j$-th group	$\mathsf{A}(0)'_j, \mathsf{Z}'_1, \ldots, \mathsf{Z}'_{j-1}, \mathsf{Z}'_{j+1}, \ldots, \mathsf{Z}'_m$
$3m+j$-th group	$\mathsf{A}(1)'_j, \mathsf{Z}'_1, \ldots, \mathsf{Z}'_{j-1}, \mathsf{Z}'_{j+1}, \ldots, \mathsf{Z}'_m$

Here, k is chosen from $1,\ldots,j-1,j+1\ldots,m$

maximum passing probability when malicious players make incorrect operations so that the resultant state σ does not satisfy the condition $\mathcal{A}$.

In the following, we denote the joint distribution over $X_1, \ldots X_m$ by $P_{X_1,\ldots X_m}$ and employ this notation for other variables. The secrecy condition of the resultant variable of Protocol 9 by Player j is guaranteed as the following theorem.

Theorem 11 *Let Player j be an arbitrary chosen player among m players. When Player j's assumption holds and Protocol 9 by Player j is passed, with significance level α, Player j finds that*

$$\|P_{X_j,E} - P_{X_j}P_E\|_1 \le \frac{c_0}{n^{1/8}}, \tag{13}$$

$$\|P_{X_j} - P_{X_j|uni}\|_1 \le \frac{c_0}{n^{1/2}}, \tag{14}$$

where E describes all the information obtained by the group S_2 and c_0 is a constant dependent on $c_1, c_{1,0}$, and α. In other words, according to Definition 5, if Player j's assumption holds and the probability to pass Protocol 9 by Player j is greater than α, resultant state passing Protocol 9 by Player j satisfies conditions (13) and (14).

The reliability condition of the resultant variable of Protocol 9 by Player j is guaranteed as the following theorem.

Theorem 12 *When all players are honest and Protocol 9 by Player j is passed, with significance level α, Player j finds that the obtained distribution $P_{X_1,\ldots X_m}$ satisfies*

$$\|P_{X_1,\ldots X_m} - P_{X_1,\ldots X_m|ideal}\|_1 \le \frac{c_0' m^{1/2}}{n^{1/8}}, \tag{15}$$

where $P_{X_1,\ldots X_m|ideal}$ is the ideal distribution of secure modulo zero-sum randomness and c_0' is a constant dependent on $c_1, c_{1,0}$, and α. In other words, according to Definition 5, if all players are honest and the probability to pass Protocol 9 by Player j is greater than α, resultant state passing Protocol 9 by Player j satisfies condition (15).

Therefore, the detectability of Protocol 9 by Player j is guaranteed even with arbitrary large $c_1, c_{1,0} > 0$ by the above two theorems. In contrast, when we choose positive numbers $c_1, c_{1,0} > 0$ sufficiently large, the tests given by Eqs. (10), (11), and (12) are passed with a high probability close to 1, which implies the acceptability of Protocol 9 by Player j.

In order that all players consider that the obtained variable is a secure modulo zero-sum randomness, we need Protocol 10 by modifying Protocol 9. In Protocol 10, the $4m$ groups chosen by Player j and the final group can be considered as the $4m+1$ groups in Protocol 9 with Player j. Hence, we obtain the following corollary of Theorems 11 and 12 , which guarantees the detectability of Protocol 10.

Corollary 13 *When Player j's assumption holds for all j and Protocol 10 is passed, with significance level α, Player j finds that conditions* (13) and (14) *hold for $j = 1, \ldots, m$, and all the players find that the obtained distribution $P_{X_1,\ldots X_m}$ satisfies*

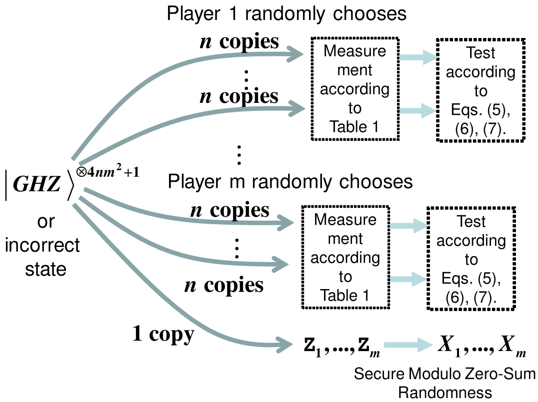

Fig. 7 Verification of GHZ state with untrusted measurement device for all players. All players verify the GHZ state by using the random sampling

condition (15). *In other words, if Player j's assumption holds for $j = 1, \ldots, m$ and the probability to pass Protocol* 10 *is greater than α, resultant state passing Protocol* 10 *satisfies conditions* (13),(14), and (15).

Hence, the detectability of Protocol 10 is guaranteed even with arbitrary large $c_1, c_{1,0} > 0$ by the above corollary. In addition, when we choose positive numbers $c_1, c_{1,0} > 0$ sufficiently large, the tests given by Eqs. (10), (11), and (12) for all j are passed with a high probability close to 1, which implies the acceptability of Protocol 10 (Fig. 7).

Protocol 10 Verifiable Generation of Secure Modulo Zero-Sum Randomness for all players

STEP 1: One player, who is not necessarily trusted, prepares the system of $4m^2n + 1$ copies, where each copy is composed of m qubits. Then, the player sends the respective qubits for all copies to the respective players. (Here, our result does not depend on the choice of this player. Hence, the player can be considered as an arbitrary player.)
STEP 2: The following step is done for $j = 1, \ldots, m$. Player j randomly choose $4m$ groups such that each group is composed of n copies. The remaining one copy is considered as the element of the final group, the $4m + 1$-th group.
STEP 3: Steps 3 and 4 for Protocol 9 for Player j are applied to $4m$ groups chosen by Player j for $j = 1, \ldots, m$. If all the tests in Step 4 for Protocol 9 for Player j are passed, they consider that the remaining copy is close to the phase GHZ state $|GHZ\rangle_p$.
STEP 4: Each Player k measures the final group with Z basis, and obtain the value X_k for $k = 1, \ldots, m$.

When we employ Protocol 10, we consider how many quantum communications can realize the following conditions.

(E1) With significance level α, Player j confirms that

$$\|P_{X_j,E} - P_{X_j} P_E\|_1 \le \epsilon, \tag{16}$$

where E describes all the information obtained by the group S_1 to satisfy the conditions $j \notin S_1$ and $(S_1 \cup \{j\})^c \neq \emptyset$ when the group S_1 does not collude another player.

(E2) When all players are honest and Protocol 9 by Player j is passed, with significance level α,

$$\| P_{X_1,\ldots,X_m} - P_{X_1,\ldots,X_m|ideal} \|_1 \le \epsilon. \tag{17}$$

Condition (E1) is the approximation version of Condition (Z3), and Condition (E2) is the approximation version of the combination of Conditions (Z1) and (Z2).

First, we consider condition (E1). When we employ Protocol 10, due to Corollary 13, n needs to be $O(\epsilon^{-8})$, i.e., we need $O(m^2\epsilon^{-8})$ copies. Next, we consider condition (E2). Due to Corollary 13, n needs to be $O(m^4\epsilon^{-8})$, i.e., we need $O(m^6\epsilon^{-8})$ copies. That is, to satisfy both conditions (E1) and (E2), we need $O(m^6\epsilon^{-8})$ copies. Since one copy needs m quantum communications, Protocol 10 needs $O(m^7\epsilon^{-8})$ quantum communications for this aim.

8 Comparison with other methods

In the following, we compare our method with three other methods.

8.1 Comparison with the method with agreed random numbers and self-testing of Bell state

We discuss the required number of quantum communications when the secure modulo randomness is generated by agreed random numbers and self-testing of Bell state. In this case, we focus on the case when Player j wishes to verify the generated secure modulo zero-sum randomness. When a part of a secret random number is shared by Player j, the secrecy of the secret random number can be directly verified by Player j. However, when the secret random number is not shared by Player j, Player j needs to ask both players sharing the secret random number to make measurement and send the outcome to Player j. The required communication between Player j and each player should be secret, which required another quantum communication and self-testing. Therefore, we can say that our method is more efficient than the above method.

In order to resolve the above problem, we can combine the classical secure modulo sum protocol [1, 2] and quantum key distribution with self-testing. When $m-2$ players collude together at most, the classical secure modulo sum protocol [1, 2] requires $O(m^2)$ secure classical communications. We consider the case when these secure classical communications are realized by quantum key distribution with self-testing. As a typical protocol, we consider the following protocol. Player i generates $X_{i,1},\ldots,X_{i,m-1}$ independently subject to the uniform distribution. Player i keeps $X_i := \sum_{j=1}^{m-1} X_{i,j}$ for $i = 1,\ldots,m-1$. Player i sends $X_{i,j}$ to Player j for $i,j = 1,\ldots,m-1$. Player j sends $\hat{X}_j := \sum_{i=1}^{m-1} X_{i,j}$ to Player m. Player m keeps $X_m := \sum_{j=1}^{m-1} \hat{X}_j$.

In this protocol, condition (Z2) is satisfied when the security of the channel between Players i and j holds for each $i \neq j$, which is formally stated as follows. Let $X_{i,(i,j)}$ and $X_{j,(i,j)}$ be the secure random seeds of Players i and j for the channel between

Players i and j. Then,

$$\left\| P_{X_{i,(i,j)},X_{j,(i,j)}} - P_{X_{i,(i,j)},X_{j,(i,j)}|ideal} \right\|_1 \leq \epsilon, \tag{18}$$

where $P_{X_{i,(i,j)},X_{j,(i,j)}|ideal}$ is the joint distribution when $X_{i,(i,j)}$ is subject to the uniform distribution and the relation $X_{i,(i,j)} = X_{j,(i,j)}$ holds with probability 1. The existing result [26, Theorem 1] guarantees that self-testing of Bell state with $O(\epsilon^{-4})$ quantum communications can generate the random numbers $X_{i,(i,j)}$ and $X_{j,(i,j)}$ to satisfy (18). Since the total number of secure classical communication is $m^2 - m$, $O(m^2\epsilon^{-4})$ quantum communications can realize condition (E1).

Next, we consider condition (E2). Assume that all players are honest, but their measurement devices and the generated quantum states cannot be trusted. Since this protocol contains $m(m-1)$ secure classical communications, under this protocol, when

$$\left\| P_{X_{i,(i,j)},X_{j,(i,j)}} - P_{X_{i,(i,j)},X_{j,(i,j)}|ideal} \right\|_1 \leq \frac{\epsilon}{m(m-1)}, \tag{19}$$

we obtain (17). Due to the existing result [26, Theorem 1], self-testing of Bell state with $O(m^8\epsilon^{-4})$ quantum communications can generate the random numbers $X_{i,(i,j)}$ and $X_{j,(i,j)}$ to satisfy (19). $O(m^{10}\epsilon^{-4})$ quantum communications can realize condition (E2).

Overall, the number of required quantum communications needs to be the larger number between the required numbers for both conditions (E1) and (E2). Hence, the required number of quantum communications in the above method is $O(m^{10}\epsilon^{-4})$, which is much larger than the number needed in Protocol 10, i.e., $O(m^7\epsilon^{-8})$ quantum communications when ϵ is fixed and m is large. That is, when ϵ is fixed and m is large, our method has an advantage for the required number of quantum communications over the above method based on a simple combination of the existing methods.

8.2 Other quantum methods for secure modulo summation

Using quantum systems, the references [18–21] proposed a protocol to securely calculate modulo summation, which is essentially equivalent to the generation of secure modulo zero-sum randomness. However, they did not propose a method to verify the secrecy and the correctness of their computation. In our method, instead of a direct computation of secure summation, we propose a method to generate secure modulo zero-sum randomness with a protocol (Protocol 9) to verify the secrecy and the correctness.

For example, the method proposed by the paper [20] is summarized as follows. First, $m-1$ players shares the GHZ state $|GHZ\rangle := \frac{1}{\sqrt{q}} \sum_{x\in\mathbb{F}_2} |x,\ldots,x\rangle$. Second, Player i applies Z^{X_i} and sends the system to Player m, where $\mathsf{Z} := \sum_{x\in\mathbb{F}_2} \omega^{\mathrm{tr} x}|x\rangle\langle x|$ and i runs from 1 to $m-1$. Third Player m measures the total system by the basis $\left\{\frac{1}{\sqrt{q}} \sum_{x\in\mathbb{F}_2} \omega^{-\mathrm{tr} xz}|x,\ldots,x\rangle\right\}_x$. Finally, Player m sends the outcome to all other players.

Since the quantum state used in their method is the GHZ state, it can be verified in the same way as in Sect. 3. In this case, Player i for $i \neq m$ can verify the GHZ state in the same way as Protocol 9. However, when Player m wishes to verify the secrecy of Y_m, the protocol is not so simple. In this case, in the verification stage, Player m needs to ask each player to make measurements and send back the outcomes. Further, these communications need to be secret, which requires additional quantum communication. Due to this problem, our method is more efficient than the combination of the method by [20] and the verification given in Protocol 9.

8.3 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 $X_{i,n} \in \mathbb{F}_2^{c_n}$ is called secure modulo zero-sum randomness with asymptotically negligible error when

$$D(P_{X_{1,n},\ldots,X_{m,n}}, P_{\tilde{X}_{1,n},\ldots,\tilde{X}_{m,n}}) \to 0 \tag{20}$$

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 [63]. 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 broadcast public communication when the joint distribution satisfies a certain condition [63].

However, this method requires noisy classical channel whose noise level is known to all players. Unfortunately, there is no method to guarantee such a noisy classical channel. Therefore, this method cannot be considered as a protocol to realize verifiable secure modulo summation.

9 Security proofs for our protocols

9.1 Security proof for Protocol 2

Now, we prove Theorem 2, i.e., the security of Protocol 2. Modulo zero condition follows from the relations $\sum_{i=1}^m X_i = Y_1 - \sum_{i=1}^m Y_i + \sum_{i=2}^m Y_i = 0$.

Independence condition holds as follows. $X_2, \ldots, X_m$ are independent of each other and subject to the uniform distribution because of their definition. Next, we focus on X_1 and $m-2$ variables among $X_2, \ldots, X_m$. As a typical case, we discuss $X_1, \ldots, X_{m-1}$. Since Y_m is subject to the uniform distribution, $Y_1 - \sum_{i=1}^m Y_i = -\sum_{i=2}^m Y_i$ is also subject to the uniform distribution even when $Y_2, \ldots, Y_{m-1}$ are fixed to certain values.

Hence, variables $X_1, \ldots, X_{m-1}$ are independent of each other and subject to the uniform distribution.

Secrecy condition is shown as follows. To discuss the secrecy of X_1, we consider the typical case when Players $2, \ldots, m-1$ collude. Since $\sum_{i=1}^{m} Y_i$ is independent of $Y_2, \ldots, Y_{m-1}$,

$$\begin{aligned} & I\left(X_1; X_2, \ldots, X_{m-2}, \sum_{i=1}^{m} Y_i\right) \\ &= I\left(-\sum_{i=2}^{m} Y_i; Y_2, \ldots, Y_{m-1}, \sum_{i=1}^{m} Y_i\right) \\ &= I\left(Y_1 - \sum_{i=1}^{m} Y_i; Y_2, \ldots, Y_{m-1} \middle| \sum_{i=1}^{m} Y_i\right) \\ &= I\left(Y_1; Y_2, \ldots, Y_{m-2} \middle| \sum_{i=1}^{m} Y_i\right) = 0. \end{aligned} \tag{21}$$

To discuss the secrecy of X_2, we consider the typical case when Players $3, \ldots, m$ collude. Since $\sum_{i=1}^{m} Y_i$ is independent of $Y_3, \ldots, Y_m$,

$$\begin{aligned} & I\left(X_2; X_3, \ldots, X_m, \sum_{i=1}^{m} Y_i\right) = I\left(Y_2; Y_3, \ldots, Y_m, \sum_{i=1}^{m} Y_i\right) \\ &= I\left(Y_2; Y_1 + Y_2 + \sum_{i=3}^{m} Y_i \middle| Y_3, \ldots, Y_m\right) \\ &= I\left(Y_2; Y_1 + Y_2 \middle| Y_3, \ldots, Y_m\right) = 0. \end{aligned} \tag{22}$$

As another case, we consider the case when Players $1, 3, \ldots, m-1$ collude. Since $\sum_{i=2}^{m} Y_i$ and $\sum_{i=1}^{m} Y_i$ are independent of $Y_3, \ldots, Y_{m-1}$,

$$\begin{aligned} & I\left(X_2; X_1, X_3, \ldots, X_{m-1}, \sum_{i=1}^{m} Y_i\right) \\ &= I\left(Y_2; -\sum_{i=2}^{m} Y_i, Y_3, \ldots, Y_{m-1}, \sum_{i=1}^{m} Y_i\right) \\ &= I\left(Y_2; -Y_2 - Y_m - \sum_{i=3}^{m-1} Y_i, Y_1 + Y_2 + Y_m + \sum_{i=3}^{m-1} Y_i \middle| Y_3, \ldots, Y_{m-1}\right) \\ &= I\left(Y_2; -Y_2 - Y_m, Y_1 + Y_2 + Y_m \middle| Y_3, \ldots, Y_{m-1}\right) \\ &= I\left(Y_2; Y_2 + Y_m, Y_1 \middle| Y_3, \ldots, Y_{m-1}\right) = 0. \end{aligned} \tag{23}$$

9.2 Security proof of Protocol 4

First, we show Theorem 3 as follows. If $X_1 = 0$ then $Z = 0$. In this case, $Y' = 0$. This is different from Y, which is nonzero. If $X_1 \neq 0$ then $Y' = Y$ and the reconstruction succeeds. Since the probability that $X_1 = 0$ is q^{-c}, the success probability is $1 - q^{-c}$. Hence, we choose c to be a sufficiently large number such that the failure probability q^{-c} is negligible. For the security, we assume that Players $2, \ldots, m$ collude to get $X_2 + \cdots + X_{m-1}$. If $X_1 = 0$ then $Z = 0$. Z does not include any information on Y. If $X_1 \neq 0$ then Z looks random. What they can do for guessing X_1 is just a random choice. This implies that X_m also looks random. Since $Y = Y' = -Z(\sum_{i=2}^{m} X_i)^{-1}$ and both its numerator and denominator are nonzero, what they can do for guessing Y is also a random choice. Thus, Protocol 4 has the perfect secrecy, which completes the proof of Theorem 3.

Next, we show Theorem 4 as follows. When $X_1 = 0$, Player m cannot recover the information Y; the modification attack is successful. This probability $1/q'$.

In the following, we consider the successful probability of the modification attack under the case with $X_1 \neq 0$. 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 $\frac{q-1}{q'-1}$, which completes the proof of Theorem 4.

Hence, in total, the successful probability of the modification attack is $\frac{1}{q'} + \frac{q'-1}{q'} \cdot \frac{q-1}{q'-1} = \frac{q}{q'}$.

9.3 Security proof of Protocol 6

Theorem 7 can be shown as follows. For simplicity, we assume that Player s is Player 1 and that malicious players are Players $l, \ldots, m$. 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

$$\begin{aligned} & I\left(-\sum_{i=2}^{l-1} T_i(Y_i - Y_1) + \sum_{j=l}^{m} T_j Y_1 + A_j; V\right) \\ & = I\left(-\sum_{i=2}^{l-1} T_i(Y_i - Y_1); V\right) = 0. \end{aligned} \tag{24}$$

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}.

10 Discussion

We have proposed a new concept of secure modulo sum randomness and a quantum protocol to generate it. We also have constructed its verification protocol that works even with untrusted measurement devices. Then, combining them, we have proposed a quantum verifiable protocol for secure modulo summation for m players even with untrusted measurement devices. This protocol guarantees secrecy for each player even when $m-2$ players collude at most.

However, the method used in this paper for self-testing is restricted to the case with the finite field $\mathbb{F}_2$. Existing methods for self-testing with a larger finite field $\mathbb{F}_q$ and operators X and Z have a more complicated structure than the self-testing method employed in this paper [64–66]. Therefore, in order to extend our method to the case with a general finite field $\mathbb{F}_q$, we need to combine the approach in this paper with a more advanced method for self-testing with a larger finite field $\mathbb{F}_q$ and operators X and Z. This is an interesting future study.

Finally, we compare our method to generate secure modulo zero-sum randomness with a method to generate secure modulo zero-sum randomness from secure agreed random numbers although the comparison with other methods [18–21] is given in Sect. 8.2. Secure modulo zero-sum randomness among m players can be generated from several pairs of secure agreed random numbers as follows. Assume that Player i and Player $i+1$ share the secret random number $Z_i \in \mathbb{F}_2^c$. Also, we assume that Player m and Player 1 share the secret random number $Z_m \in \mathbb{F}_2^c$. Then, Player 1 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 $X_1, \ldots, X_m$ satisfy the condition $\sum_{i=1}^{m} X_i = 0$ and the independence between any $n-1$ variables of them.

Indeed, secure agreed random numbers can be generated by using quantum key distribution. This method generates secure modulo zero-sum randomness if all the players are honest. However, each player does not have a method to verify whether other players are honest. Therefore, even when we apply the randomness generated by this method to Protocol 1, the obtained method does not satisfy the condition of verifiable secure modulo summation.

However, when Player j wishes to verify the generated secure modulo zero-sum randomness, he/she needs to verify the secrecy of all the secret random numbers. In this case, these secret random numbers need to be generated by quantum communication with self-testing. When we compare the required number of quantum communications for our method and the above method, as shown in Sect. 8, our method has an advantage over the above method with sufficiently large number m of players.

Unfortunately, our protocol for self-testing consumes a lot of quantum resources. Hence, it is needed to discuss whether we can reduce the required quantum resources or not. This is an interesting future study.

Acknowledgements MH is supported in part by the National Natural Science Foundation of China (Grant No. 62171212) and Guangdong Provincial Key Laboratory (Grant No. 2019B121203002), a JSPS Grant-in-Aids for Scientific Research (A) No. 17H01280 and for Scientific Research (B) No. 16KT0017, and Kayamori Foundation of Information Science Advancement No. K27-XX-467. TK is supported in part by a JSPS Grant-in-Aids for Scientific Research (A) No. 21H04879, and for Challenging Exploratory Research No. 19K22849 and MEXT Quantum Leap Flagship Program (MEXT Q-LEAP) Grant Nos. JPMXS0118067285 and JPMXS0120319794.

Author contributions All the authors contributed equally.

Data availability Data sharing is not applicable to this article as no datasets were generated or analyzed during the current study.

Code availability The authors declare that there are no custom codes in the manuscript. The mathematical algorithms are included within the paper.

Appendix A Summary of Appendix

The first aim of this appendix is providing the security proof for our quantum verifiable protocol to generate secure modulo zero-sum randomness. The second aim of this appendix is providing a quantum verifiable protocol to generate secure modulo zero-sum randomness with general dimension when the measurement device is trusted.

The appendix is organized as follows. First, as the preparation of the first aim, Appendix 1 evaluates the performance of the classical random sampling. Then, Appendix 1 reviews the existing result of self-testing of Bell state. By using these discussions, Appendix 1 shows the security of our quantum verifiable protocol to generate secure modulo zero-sum randomness, which is presented in Sect. 7. That is, we show Theorems 11 and 12 of the mainbody. Then, Appendix 1 presents a quantum verifiable protocol to generate secure modulo zero-sum randomness with general dimension when the measurement device is trusted.

Appendix B Classical random sampling

Proof We consider $n+1$ binary random variables $X_1, \ldots, X_{n+1}$ taking values in $\{0, 1\}$. We randomly choose n variables among $X_1, \ldots, X_{n+1}$ and observe them. We denote the remaining variable by Y. Let Z be the number of 1 among observed variables. $\square$

Lemma 3 of [26, Appendix C] is rewritten as follows.

Proposition 14 *With significance level α, we have For any constants c_1, $p*$ and α, there exists a constant c_2 such that with significance level α, we have*

$$\begin{aligned} p_* - \frac{c_2}{\sqrt{n}} \leq & Pr\Big(Y = 1 \Big| p_* - \frac{c_1}{\sqrt{n}} \leq \frac{Z}{n} \leq p_* + \frac{c_1}{\sqrt{n}}\Big) \\ \leq & p_* + \frac{c_2}{\sqrt{n}} \end{aligned} \tag{B1}$$

In other words, the probability $Pr\Big(p_* - \frac{c_1}{\sqrt{n}} \leq \frac{Z}{n} \leq p_* + \frac{c_1}{\sqrt{n}}\Big)$ is greater than α; condition (B1) holds.

When p_* is zero, we prepare a different type of evaluation as follows.

Proposition 15 *With significance level $\alpha \geq \frac{k+1}{n+1}$, we have*

$$Pr(Y = 1|Z \leq k) \leq \frac{k}{\alpha(n+1)} + \frac{1-\alpha}{\alpha(n-k)}. \tag{B2}$$

That is, for any constants c_1 and α, there exists a constant c_2 such that with significance level α, we have

$$Pr\Big(Y = 1 \Big| \frac{Z}{n} \leq \frac{c_1}{n}\Big) \leq \frac{c_2}{n}. \tag{B3}$$

In other words, the probability $Pr\Big(\frac{Z}{n} \leq \frac{c_1}{n}\Big)$ is greater than α, condition (B3) holds.

Proof We denote the number of 1 among $X_1, \ldots, X_{n+1}$ by the variable X. We assume that $P(X = x) = P_x$. Then, we have

$$Pr(Z = z, Y = y) = P_{z+y} \frac{\binom{n}{z}}{\binom{n+1}{z+y}}. \tag{B4}$$

That is,

$$Pr(Z = z, Y = 0) = P_z \frac{n-z+1}{n+1} \tag{B5}$$

$$Pr(Z = z, Y = 1) = P_{z+1} \frac{z+1}{n+1}. \tag{B6}$$

Thus, we have

$$Pr(Z = z) = P_z \frac{n-z+1}{n+1} + P_{z+1} \frac{z+1}{n+1}. \tag{B7}$$

Hence,

$$Pr(Z \leq k, Y = 1) = \sum_{z=0}^{k} P_{z+1} \frac{z+1}{n+1}, \tag{B8}$$

and

$$\frac{Pr(Z \leq k, Y = 1)}{Pr(Z \leq k)} = \frac{\sum_{z=0}^{k} P_{z+1} \frac{z+1}{n+1}}{(\sum_{z=0}^{k} P_z) + P_{k+1} \frac{k+1}{n+1}}. \tag{B9}$$

Since $\frac{1}{n+1} \leq \cdots \leq \frac{k}{n+1} \leq \frac{k+1}{n+1}$ and $1 \geq \frac{k+1}{n+1}$, we have

$$\begin{aligned} &\max_{(P_z)_{z=0}^{n+1}} \left\{ \frac{\sum_{z=0}^{k} P_{z+1} \frac{z+1}{n+1}}{(\sum_{z=0}^{k} P_z) + P_{k+1} \frac{k+1}{n+1}} \middle| (\sum_{z=0}^{k} P_z) + P_{k+1} \frac{k+1}{n+1} \geq \alpha \right\} \\ &= \max_{p} \left\{ \frac{(1-p)\frac{k}{n+1} + p\frac{k+1}{n+1}}{(1-p) + p\frac{k+1}{n+1}} \middle| (1-p) + p\frac{k+1}{n+1} \geq \alpha \right\} \end{aligned} \tag{B10}$$

The condition $(1-p) + p\frac{k+1}{n+1} \geq \alpha$ is equivalent to the condition $1 - \alpha \geq p(1 - \frac{k+1}{n+1}) = p\frac{n-k}{n+1}$, which is rewritten as $(1-\alpha)\frac{n+1}{n-k} \geq p$. Under this condition, we have

$$\begin{aligned} \frac{(1-p)\frac{k}{n+1} + p\frac{k+1}{n+1}}{(1-p) + p\frac{k+1}{n+1}} &= \frac{\frac{k}{n+1} + p\frac{1}{n+1}}{(1-p) + p\frac{k+1}{n+1}} \\ &\leq \frac{\frac{k}{n+1} + (1-\alpha)\frac{n+1}{n-k}\frac{1}{n+1}}{\alpha} \\ &= \frac{\frac{k}{n+1} + \frac{1-\alpha}{n-k}}{\alpha} = \frac{k}{\alpha(n+1)} + \frac{1-\alpha}{\alpha(n-k)}. \end{aligned} \tag{B11}$$

Combining (B10) and (B11), we obtain the desired statement. □

In this paper, we need to combine several statements with a certain significance level. The following lemma is useful for this aim.

Lemma 16 *We assume the following. When the test A_i is passed, the property B_i holds with significance level α for $i = 1, 2$. Then, the properties B_1 and B_2 hold with significance level α when the tests A_1 and A_2 are passed. In other words, if the probability to pass the tests A_1 and A_2 is greater than α, the resultant state passing the tests A_1 and A_2 satisfies the properties B_1 and B_2.*

Proof Lemma 16 is shown as follows. Let $\{P_\theta\}_{\theta \in \Theta}$ be the set of possible distributions. In the quantum setting, when we fix the measurements, dependently of the measurements and input states, we have the distribution P_θ over the measurement outcomes. Let $\mathcal{A}_i$ be the set of events to satisfy A_i for $i = 1, 2$. When the property B_i holds under the parameter θ, we write $B_i(\theta) = 1$. Otherwise, we write $B_i(\theta) = 0$.

The assumption implies that

$$\max\{P_\theta(\mathcal{A}_i)|B_i(\theta)=0\} \le \alpha. \tag{B12}$$

Hence,

$$\begin{aligned}
&\max\{P_\theta(\mathcal{A}_1\cap\mathcal{A}_2)|B_1(\theta)=0 \text{ or } B_2(\theta)=0\}\\
&\quad=\max(\max\{P_\theta(\mathcal{A}_1\cap\mathcal{A}_2)|B_1(\theta)=0\}, (\max\{P_\theta(\mathcal{A}_1\cap\mathcal{A}_2)|B_2(\theta)=0\})\\
&\quad\le\max(\max\{P_\theta(\mathcal{A}_1)|B_1(\theta)=0\}, \max\{P_\theta(\mathcal{A}_2)|B_2(\theta)=0\})\\
&\quad\le\alpha,
\end{aligned} \tag{B13}$$

which implies the desired statement. □

Appendix C Self-testing of Bell sate

To discuss the verification of the GHZ state, we review the existing result for self-testing of the Bell state by [26]. To fit our use, we consider the case when the Bell state is given as $\frac{1}{\sqrt{2}}(|00\rangle_p+|11\rangle_p)$.

We choose sufficiently large Hilbert spaces $\mathcal{H}_1''$ and $\mathcal{H}_2''$ so that the state on the composite system is the pure state $|\psi''\rangle$. Let X_i'', Z_i'', $\mathsf{A}(0)_i''$, $\mathsf{A}(1)_i''$ be operators on $\mathcal{H}_i$ for $i=1,2$.

Proposition 17 *When*

$$\langle\psi''|\mathsf{X}_1''\mathsf{X}_2''|\psi''\rangle \ge 1-\epsilon, \quad \langle\psi''|-\mathsf{Z}_1''\mathsf{Z}_2''|\psi''\rangle \ge 1-\epsilon, \tag{C1}$$

$$\langle\psi''|\mathsf{A}(0)_1''(\mathsf{X}_2''-\mathsf{Z}_2'')+\mathsf{A}(1)_1''(\mathsf{X}_2''+\mathsf{Z}_2'')|\psi''\rangle \ge 2\sqrt{2}-\epsilon, \tag{C2}$$

there exist a constant c_3 and isometries $U_1:\mathcal{H}_1''\to\mathcal{H}_1$ and $U_2:\mathcal{H}_2''\to\mathcal{H}_2$ such that the isometry $U=U_1U_2$ satisfies

$$\|U\mathsf{X}_1''U^\dagger-\mathsf{X}_1\| \le c_3\epsilon^{1/2}, \ \|U\mathsf{Z}_1''U^\dagger-\mathsf{Z}_1\| \le c_3\epsilon^{1/2} \tag{C3}$$

$$\|U\mathsf{X}_2''U^\dagger-\mathsf{X}_2\| \le c_3\epsilon^{1/2}, \ \|U\mathsf{Z}_2''U^\dagger-\mathsf{Z}_2\| \le c_3\epsilon^{1/2}. \tag{C4}$$

Equation (C3) follows from Proposition 1 of [26]. While Eq. (C4) does not appear in Proposition 1 of [26], it can be shown by using (E40) and (E41) of Lemma 9.

Now, we apply Proposition 17 to the case when we prepare $6m+1$ copies of the initial state and split them randomly into 6 groups and one final copy. The procedure is described as follows and is denoted by Protocol 11:

We apply Conditions (C5) and (C6) to Propositions 14 and 15 . Since $\frac{c_2}{n} \le \frac{c_2}{\sqrt{n}}$, combining Proposition 17, we obtain the following proposition.

Proposition 18 *For significance level α and a constant c_1, there exists a constant c_4 to satisfy the following condition. When the test given in Protocol 11 is passed, we*

Protocol 11 Self-testing of Bell state

STEP 1: Randomly divide $6m+1$ blocks into 6 groups, in which, the 1st - 6th groups are composed of m blocks.
STEP 2: Measure X_1', Z_1', $\mathsf{A}(0)_1'$, $\mathsf{A}(0)_1'$, $\mathsf{A}(1)_1'$, $\mathsf{A}(1)_1'$ on the system $\mathcal{H}_1'$ for the 1st - 6th groups.
STEP 3: The corresponding measurements on $\mathcal{H}_2'$ for the 6 groups are X_2', Z_2', X_2', Z_2', X_2', Z_2'.
STEP 4: Based on the above measurements, we check the following 3 inequalities for 6 average values:

$$\mathbb{A}[\mathsf{X}_1'\mathsf{X}_2'] \geq 1-\frac{c_1}{n}, \quad \mathbb{A}[-\mathsf{Z}_1'\mathsf{Z}_2'] \geq 1-\frac{c_1}{n}, \tag{C5}$$

$$\mathbb{A}[\mathsf{A}(0)_1'(\mathsf{X}_2'-\mathsf{Z}_2')+\mathsf{A}(1)_1'(\mathsf{X}_2'+\mathsf{Z}_2')] \geq \sqrt{2}-\frac{c_1}{\sqrt{n}}, \tag{C6}$$

Here, the average value in (C6) is calculated from the outcomes of the 3rd–6th groups.

can guarantee, with significance level α, that there exist isometries $U_1 : \mathcal{H}_1'' \to \mathcal{H}_1$ and $U_2 : \mathcal{H}_2'' \to \mathcal{H}_2$ such that the isometry $U = U_1U_2$ satisfies

$$\|UX_1''U^\dagger - X_1\| \leq \frac{c_4}{n^{1/4}}, \ \|UZ_1''U^\dagger - Z_1\| \leq \frac{c_4}{n^{1/4}} \tag{C7}$$

$$\|UX_2''U^\dagger - X_2\| \leq \frac{c_4}{n^{1/4}}, \ \|UZ_2''U^\dagger - Z_2\| \leq \frac{c_4}{n^{1/4}}. \tag{C8}$$

In other words, if the probability to pass Protocol 11 is greater than α, there exist isometries $U_1 : \mathcal{H}_1'' \to \mathcal{H}_1$ and $U_2 : \mathcal{H}_2'' \to \mathcal{H}_2$ such that resultant state passing Protocol 11 satisfies conditions (C7) and (C8).

Appendix D Security proof for quantum verifiable protocol to generate secure modulo zero-sum randomness

Proof of Theorem 11 of the mainbody Now, we show Theorem 11 of the mainbody by using Lemma 16, Propositions 15, and 18 , which are shown in Appendices. Before, we need to be careful in handling several statements with a certain significance level. As shown in Lemma 16, when several statements hold with significance level α, we obtain all of them simultaneously with significance level α.

First, we find the following. Condition (11) of the mainbody implies that relation (14) of the mainbody holds with significance level α.

Assume that S_1 is composed of $j_1, \ldots, j_l$. We focus on the quantum system of Player j and the quantum system of group S_1. The latter system is spanned by the basis

$$|x\rangle_{S_1} := \frac{1}{2^{(l-1)/2}} \sum_{x_{j_1},\ldots,x_{j_l}: x_{j_1}+\cdots+x_{j_l}=x} |x_{j_1}\rangle_{j_1} \cdots |x_{j_l}\rangle_{j_l}.$$

It is also spanned by $|z\rangle_{S_1;p} := |z\rangle_{j_1;p} \cdots |z\rangle_{j_l;p} = \frac{1}{\sqrt{2}}(|0\rangle_{S_2} + (-1)^z|1\rangle_{S_1})$. We define $\mathsf{Z}_{S_1} := |0\rangle_{S_1}\, {}_{S_1}\langle 0| - |1\rangle_{S_1}\, {}_{S_1}\langle 1|$ and $\mathsf{X}_{S_1} := |0\rangle_{S_1}\, {}_{S_1}\langle 1| + |0\rangle_{S_1}\, {}_{S_1}\langle 1|$. Similarly, we define Z_{S_2} and X_{S_2}. While the measurement Z_{S_1} can be done by the measurement $\mathsf{Z}_{j_1}, \ldots, \mathsf{Z}_{j_l}$, the measurement X_{S_1} can be done only by the measurement X_k for any $k \in S_1$. The same observation holds for Z_{S_2} and X_{S_2}. Therefore, our GHZ $|GHZ\rangle_p$ can be considered as $\frac{1}{\sqrt{2}}(\sum_z |z\rangle_p |z\rangle_{S_1;p} |z\rangle_{S_2;p})$.

When they measure Z_{S_2}, they obtain the outcome z and apply the unitary X_j^{-z}, the resultant state is the Bell state $\frac{1}{\sqrt{2}}(\sum_z |z\rangle_{j;p} |z\rangle_{S_1;p})$. When we measure X_j and X_{S_1} to the system in the state $\frac{1}{\sqrt{2}}(\sum_z |z\rangle_{j;p} |z\rangle_{S_1;p} |z\rangle_{S_2;p})$, the measurement outcome does not depend on the measurement outcome of Z_{S_2}. Therefore, we can consider that the measurements on the $j_1, j, m+j_1, m+j, 2m+j_1, 2m+j, 3m+j_1, 3m+j$-th groups can be considered as the measurement required in Proposition 18. Now, we denote the real operator on the final group by using $''$. The real quantum system of Player j, the groups S_1 and S_2 are denoted by $\mathcal{H}_j$, $\mathcal{H}_{S_1}$, and $\mathcal{H}_{S_2}$.

Using Proposition 18, we can guarantee, with significance level α, that there exist a constant c_2 and isometries $U_j : \mathcal{H}_j'' \to \mathcal{H}_j$ and $U_{S_1} : \mathcal{H}_{S_1}'' \to \mathcal{H}_{S_1}$ such that

$$\|U_j \mathsf{X}_j'' U_j^\dagger - \mathsf{X}_j\| \le c_2 n^{-1/4}, \ \|U_j \mathsf{Z}_j'' U_j^\dagger - \mathsf{Z}_j\| \le c_2 n^{-1/4}, \tag{D1}$$

$$\|U_{S_1} \mathsf{X}_{S_1}'' U_{S_1}^\dagger - \mathsf{X}_{S_1}\| \le c_2 n^{-1/4}, \tag{D2}$$

$$\|U_{S_1} \mathsf{Z}_{S_1}'' U_{S_1}^\dagger - \mathsf{Z}_{S_1}\| \le c_2 n^{-1/4}. \tag{D3}$$

We apply the same discussion to the case with switching S_1 and S_2. Then, we can guarantee, with significance level α, that there exists isometry $U_{S_2} : \mathcal{H}_{S_2}'' \to \mathcal{H}_{S_2}$ such that

$$\begin{aligned} \|U_{S_2} \mathsf{X}_{S_2}'' U_{S_2}^\dagger - \mathsf{X}_{S_2}\| &\le c_4 \sqrt{c_1} n^{-1/4}, \\ \|U_{S_2} \mathsf{Z}_{S_2}'' U_{S_2}^\dagger - \mathsf{Z}_{S_2}\| &\le c_4 \sqrt{c_1} n^{-1/4}. \end{aligned} \tag{D4}$$

We define two projections

$$\begin{aligned} P_1 &:= \sum_{*} |x_1\rangle_j |x_2\rangle_{S_1} |x_3\rangle_{S_2} \, {}_j\langle x_1| \, {}_{S_1}\langle x_2| \, {}_{S_2}\langle x_3| \\ &= \frac{1}{2}(I + \mathsf{Z}_j \mathsf{Z}_{S_1} \mathsf{Z}_{S_2}) \end{aligned} \tag{D5}$$

$$\begin{aligned} P_2 &:= \sum_{z} |z\rangle_{j;p} |z\rangle_{S_1;p} |z\rangle_{S_2;p} \, {}_{j;p}\langle z| \, {}_{S_1;p}\langle z| \, {}_{S_2;p}\langle z| \\ &= \frac{1}{4}(I + \mathsf{X}_j \mathsf{X}_{S_1})(I + \mathsf{X}_j \mathsf{Z}_{S_2}) \\ &= \frac{1}{4}(I + \mathsf{X}_j \mathsf{X}_{S_1} + \mathsf{X}_j \mathsf{Z}_{S_2} + \mathsf{X}_{S_1} \mathsf{Z}_{S_2}), \end{aligned} \tag{D6}$$

where $*$ expresses the sum for x_1, x_2, x_3 under the condition $x_1 + x_2 + x_3 = 0$. Then, we have $|GHZ\rangle_p \, {}_p\langle GHZ| = P_1 P_2$. Hence, for $U = U_j U_{S_1} U_{S_2}$, using (D5), we have

$$\|U^\dagger P_1 U - P_1''\| = \|P_1 - U P_1'' U^\dagger\|$$

$$\leq \frac{1}{2}\big(\|\mathsf{Z}_j - U_j \mathsf{Z}''_j U_j^\dagger\| + \|\mathsf{Z}_{S_1} - U_{S_1}\mathsf{Z}''_{S_1} U_{S_1}^\dagger + \|\mathsf{Z}_{S_2} - U_{S_2}\mathsf{Z}''_{S_2} U_{S_2}^\dagger\|\big) \tag{D7}$$

$$\|U^\dagger P_2 U - P''_2\| = \|P_2 - U P''_2 U^\dagger\|$$
$$\leq \frac{1}{2}\big(\|\mathsf{Z}_j - U_j \mathsf{Z}''_j U_j^\dagger\| + \|\mathsf{Z}_{S_1} - U_{S_1}\mathsf{Z}''_{S_1} U_{S_1}^\dagger\| + \|\mathsf{Z}_{S_2} - U_{S_2}\mathsf{Z}''_{S_2} U_{S_2}^\dagger\|\big). \tag{D8}$$

Applying Proposition 15 to P''_1 and P''_2, with significance level α and a constant c'_2, we have

$$\mathrm{Tr}\sigma(I - P''_i) \leq \frac{c'_2}{n} \tag{D9}$$

for $i = 1, 2$. Due to Lemma 16, combining (D1),(D2), (D3), (D4), (D7), (D8), and (D9), with significance level α, we have

$$\begin{aligned}
&\mathrm{Tr}\sigma U^\dagger(I - |GHZ\rangle_p\, {}_p\langle GHZ|)U \\
&\quad\leq \mathrm{Tr}\sigma U^\dagger((I - P_1) + (I - P_2))U \\
&\quad\leq \mathrm{Tr}\sigma(U^\dagger(I - P_1)U + U^\dagger(I - P_2)U) \\
&\quad\leq \mathrm{Tr}\sigma((I - P''_1) + (I - P''_2)) + \|U^\dagger P_1 U - P''_1\| + \|U^\dagger P_2 U - P''_2\| \\
&\quad\leq \frac{2c'_2}{n} + 3c_2 n^{-1/4}.
\end{aligned} \tag{D10}$$

Hence,

$$\|\sigma - U^\dagger|GHZ\rangle_p\, {}_p\langle GHZ|U\|_1 \leq \sqrt{\frac{2c'_2}{n} + 3c_2 n^{-1/4}}. \tag{D11}$$

Let $\tilde{P}_{X_j, X_{S_1}, X_{S_2}, E}$ be the joint distribution when Players apply the ideal measurements $U_j^\dagger \mathsf{Z}_j U_j$, $U_{S_1}^\dagger \mathsf{Z}_{S_1} U_{S_1}$, and $U_{S_2}^\dagger \mathsf{Z}_{S_2} U_{S_2}$. With significance level α, we have

$$\begin{aligned}
&\|P_{X_j,E} - P_{X_j}P_E\|_1 \\
&\quad\leq \|\tilde{P}_{X_j,E} - \tilde{P}_{X_j}P_E\|_1 + \|\tilde{P}_{X_j,E} - P_{X_j,E}\|_1 + \|\tilde{P}_{X_j} - P_{X_j}\|_1 \\
&\quad\leq \|\sigma - U^\dagger|GHZ\rangle_p\, {}_p\langle GHZ|U\|_1 + 2\|\mathsf{Z}_j - U_j\mathsf{Z}''_j U_j^\dagger\| \\
&\quad\leq \sqrt{\frac{2c'_2}{n} + 3c_2 n^{-1/4}} + 2c_2 n^{-1/4}.
\end{aligned} \tag{D12}$$

Therefore, with significance level α, we have (D12). Hence, we obtain the desired statement. □

Proof of Theorem 12 of the mainbody Now, we show Theorem 11 of the mainbody by using Lemma 16, Propositions 15, and 18 , which are shown in Appendices. We apply Proposition 18 to the case with X_i, X_j, Z_i, and Z_j for $i \neq j$. With significance level

α, we can guarantee that there exist a constant c_2 and isometries $U_i : \mathcal{H}_i'' \to \mathcal{H}_i$ and $U_j : \mathcal{H}_j'' \to \mathcal{H}_i$ such that

$$\begin{aligned}
&\|U_i \mathsf{X}_i'' U_i^\dagger - \mathsf{X}_i\| \le c_2 n^{-1/4},\ \|U_j \mathsf{X}_j'' U_j^\dagger - \mathsf{X}_j\| \le c_2 n^{-1/4}, \\
&\|U_i \mathsf{Z}_i'' U_i^\dagger - \mathsf{Z}_i\| \le c_2 n^{-1/4}, \|U_j \mathsf{Z}_j'' U_j^\dagger - \mathsf{Z}_j\| \le c_2 n^{-1/4}.
\end{aligned} \tag{D13}$$

With significant level α, we have (D13) with any $i \neq j$. Then, using the projections $\tilde{P}_1$ and $\tilde{P}_2$ defined in (4) and (5), we have $|GHZ\rangle_{p\ p}\langle GHZ| = \tilde{P}_1 \tilde{P}_2$. Hence, for $U = U_j U_{S_1} U_{S_2}$, using (D5), we have

$$\begin{aligned}
\|U^\dagger \tilde{P}_1 U - \tilde{P}_1''\| &= \|\tilde{P}_1 - U \tilde{P}_1'' U^\dagger\| \\
&\le \frac{1}{2} \sum_{i=1}^{m} \|\mathsf{Z}_i - U_i \mathsf{Z}_i'' U_i^\dagger\|,
\end{aligned} \tag{D14}$$

$$\begin{aligned}
\|U^\dagger \tilde{P}_2 U - P \tilde{P}_2''\| &= \|\tilde{P}_2 - U \tilde{P}_2'' U^\dagger\| \\
&\le \frac{1}{2} \sum_{i:i\neq j} (\|\mathsf{Z}_j - U_j \mathsf{Z}_j'' U_j^\dagger\| + \|\mathsf{Z}_i - U_i \mathsf{Z}_i'' U_i^\dagger\|) \\
&= \frac{m-1}{2} \left(\|\mathsf{Z}_j - U_j \mathsf{Z}_j'' U_j^\dagger\| + \frac{1}{2} \sum_{i:i\neq j} \|\mathsf{Z}_i - U_i \mathsf{Z}_i'' U_i^\dagger\| \right).
\end{aligned} \tag{D15}$$

Applying Proposition 15 to $\tilde{P}_1''$ and $\tilde{P}_2''$, with significance level α and a constant c_2', we have

$$\mathrm{Tr}\sigma(I - \tilde{P}_i'') \le \frac{c_2'}{n} \tag{D16}$$

for $i = 1, 2$.

Due to Lemma 16, combining (D13), (D14), (D15), and (D16), with significance level α, we have

$$\begin{aligned}
&\mathrm{Tr}\sigma U^\dagger (I - |GHZ\rangle_{p\ p}\langle GHZ|) U \\
&\le \mathrm{Tr}\sigma U^\dagger ((I - \tilde{P}_1) + (I - \tilde{P}_2)) U \\
&\le \mathrm{Tr}\sigma (U^\dagger (I - P_1) U + U^\dagger (I - P_2) U) \\
&\le \mathrm{Tr}\sigma ((I - \tilde{P}_1'') + (I - \tilde{P}_2'')) + \|U^\dagger \tilde{P}_1 U - \tilde{P}_1''\| + \|U^\dagger \tilde{P}_2 U - \tilde{P}_2''\| \\
&\le \frac{2c_2'}{n} + \frac{m + 2(m-1)}{2} c_2 n^{-1/4}.
\end{aligned} \tag{D17}$$

Hence,

$$\|\sigma - U^\dagger |GHZ\rangle_{p\ p}\langle GHZ| U\|_1 \le \sqrt{\frac{2c_2'}{n} + \frac{3m-2}{2} c_2 n^{-1/4}}. \tag{D18}$$

When we apply the measurement based on a POVM $M = \{M_i\}$ to the system whose state is ρ, we denote the output distribution by $\mathcal{P}_\rho^M$. For any POVM $M = \{M_i\}$, we have

$$\begin{aligned}
&\|\mathcal{P}_\sigma^M - \mathcal{P}^M_{|GHZ\rangle_p\, {}_p\langle GHZ|}\|_1 \\
&\le \sum_i \mathrm{Tr} M_i |\sigma - |GHZ\rangle_p\, {}_p\langle GHZ|| \\
&= \|\sigma - |GHZ\rangle_p\, {}_p\langle GHZ|\|_1 \\
&\le \sqrt{\frac{2c_2'}{n} + \frac{3m-2}{2} c_2 n^{-1/4}}.
\end{aligned} \tag{D19}$$

We denote the POVM corresponding to the ideal observables $\mathsf{Z}_1, \ldots, \mathsf{Z}_m$ (the real observables $\mathsf{Z}_1'', \ldots, \mathsf{Z}_m''$) by M_{ideal} (M_{real}). When we apply the measurement based on the POVM M_{ideal} (M_{real}) to the system whose state is σ, we denote the output distribution by $P^{M_{ideal}}_{X_1,\ldots,X_m}$ ($P^{M_{real}}_{X_1,\ldots,X_m}$). Since

$$P^{M_{real}}_{X_1,\ldots,X_m} = P^{M_{real}}_{X_1} P^{M_{real}}_{X_2|X_1} \cdots P^{M_{real}}_{X_m|X_1,\ldots,X_{m-1}} - P^{M_{ideal}}_{X_1,\ldots,X_m}, \tag{D20}$$

we have

$$\begin{aligned}
&\left\|\mathcal{P}_\sigma^{M_{real}} - \mathcal{P}_\sigma^{M_{ideal}}\right\|_1 = \left\|P^{M_{real}}_{X_1,\ldots,X_m} - P^{M_{ideal}}_{X_1,\ldots,X_m}\right\|_1 \\
&= \sum_{i=1}^m \Big\| P^{M_{real}}_{X_1} P^{M_{real}}_{X_2|X_1} \cdots P^{M_{real}}_{X_i|X_1,\ldots,X_{i-1}} \cdots P^{M_{ideal}}_{X_m|X_1,\ldots,X_{m-1}} \\
&- P^{M_{real}}_{X_1} P^{M_{real}}_{X_2|X_1} \cdots P^{M_{ideal}}_{X_i|X_1,\ldots,X_{i-1}} \cdots P^{M_{ideal}}_{X_m|X_1,\ldots,X_{m-1}} \Big\|_1 \\
&= \sum_{i=1}^m \Big\| P^{M_{real}}_{X_1} P^{M_{real}}_{X_2|X_1} \cdots P^{M_{real}}_{X_i|X_1,\ldots,X_{i-1}} \\
&- P^{M_{real}}_{X_1} P^{M_{real}}_{X_2|X_1} \cdots P^{M_{ideal}}_{X_i|X_1,\ldots,X_{i-1}} \Big\|_1 \\
&= \sum_{i=1}^m \max_{x_1,\ldots,x_{i-1}} \left\| P^{M_{real}}_{X_i|X_1=x_1,\ldots,X_{i-1}=x_{i-1}} - P^{M_{ideal}}_{X_i|X_1=x_1,\ldots,X_{i-1}=x_{i-1}} \right\|_1 \\
&= \sum_{i=1}^m \max_{x_1,\ldots,x_{i-1}} \|U_j \mathsf{Z}_j'' U_j^\dagger - \mathsf{Z}_j\| \le m c_2 n^{-1/4}.
\end{aligned} \tag{D21}$$

Since (D13) and (D16) hold with significance level α, combining (D19) and (D21), we have

$$\begin{aligned}
&\|P_{X_1,\ldots X_m} - P_{X_1,\ldots X_m|ideal}\|_1 \\
&\le \|\mathcal{P}_\sigma^{M_{real}} - \mathcal{P}^{M_{ideal}}_{|GHZ\rangle_p\, {}_p\langle GHZ|}\|_1
\end{aligned}$$

$$\leq \|\mathcal{P}_\sigma^{M_{real}} - \mathcal{P}_\sigma^{M_{ideal}}\|_1 + \|\mathcal{P}_\sigma^{M_{ideal}} - \mathcal{P}_{|GHZ\rangle_p\, {}_p\langle GHZ|}^{M_{ideal}}\|_1$$
$$\leq \sqrt{\frac{2c_2'}{n} + \frac{3m-2}{2}c_2 n^{-1/4}} + mc_2 n^{-1/4}. \tag{D22}$$

Thus, we obtain the desired statement. □

Appendix E Extension of quantum protocol for secure modulo zero-sum randomness to case with $\mathbb{F}_q$

Now, we extend our quantum protocol for secure modulo zero-sum randomness to the case with $\mathbb{F}_q$. The following discussion assumes trusted measurement devices. Our protocol with untrusted measurement devices cannot be extended to the case with $\mathbb{F}_q$.

When we employ a general finite field $\mathbb{F}_q$, the phase basis $\{|z\rangle_p\}_{z\in\mathbb{F}_q}$ is defined as [67, Section 8.1.2]

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

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

Then, the phase GHZ state $|GHZ\rangle_p := \frac{1}{\sqrt{q}} \sum_{z\in\mathbb{F}_q} |z,\ldots,z\rangle_p$ is calculated as

$$|GHZ\rangle_p = \frac{1}{\sqrt{q^{m-1}}} \sum_{x_1,\ldots,x_m\in\mathbb{F}_q : x_1+\cdots+x_m=0} |x_1,\ldots,x_m\rangle. \tag{D23}$$

When all the players apply measurement on the computational basis and the initial state is $|GHZ\rangle_p$, the sum of m outcomes is zero and $m-1$ outcomes are subject to the uniform distribution. Hence, these outcomes satisfy the conditions of secure modulo zero-sum randomness. That is, when the initial state is guaranteed to be $|GHZ\rangle_p$, it is guaranteed that the outcomes are secure modulo zero-sum randomness.

When we trust measurement devices, we can employ the following protocol to verify the state $|GHZ\rangle_p$.

Protocol 12 Verifiable Generation of Secure Modulo Zero-Sum Randomness

STEP 1: [Phase basis check] They prepare the system of $2n+1$ copies. They randomly choose n 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 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 one copy. The outcomes are used as secure modulo zero-sum randomness.

Theorem 19 *Assume that* $\alpha > \frac{1}{2n+1}$ *in Protocol 12. If the test is passed, with significance level* α*, we can guarantee that the resultant state* σ *on each remaining system satisfies*

$$\mathrm{Tr}\sigma |GHZ\rangle_p \, {}_p\langle GHZ| \geq 1 - \frac{1}{\alpha(2n+1)}. \tag{D24}$$

In other words, if the probability to pass the test is greater than α*, the resultant state passing the test satisfies condition* (D24).

In the above case, the significance level is the maximum passing probability when malicious Bob sends incorrect states so that the resultant state α does not satisfy Eq. (D24).

The proof of the theorem is given below. From the theorem and the relation between the fidelity and trace norm [68, (6.106)], we can conclude the verifiability: if they passed the test, they can guarantee that

$$\|\sigma - |GHZ\rangle_p \, {}_p\langle GHZ|\|_1 \leq \frac{1}{\sqrt{\alpha(2n+1)}} \tag{D25}$$

with significance level α. Therefore, when P_{ideal} is the ideal distribution of secure modulo zero-sum randomness and P_{real} is the real distribution obtained via the measurement with respect to the computation basis, we have

$$\|P_{real} - P_{ideal}\|_1 \leq \frac{1}{\sqrt{\alpha(2n+1)}}. \tag{D26}$$

Proof of Theorem 19 We choose a new coordinate $\bar{x}_1, \ldots, \bar{x}_m$ as $\bar{x}_1 = x_1 + \cdots + x_m$ and $\bar{x}_i = x_i$ for $i = 2, \ldots, m$. We denote the unitary corresponding to this coordinate conversion by U. When a matrix D is applied in the computation basis, the conversion on phase basis is given by $(D^{-1})^T$. Since

$$\left(\begin{pmatrix} 1 & & 0 \\ 1 & 1 & \\ \vdots & \ddots & \\ 1 & 0 & 1 \end{pmatrix}^{-1} \right)^T = \begin{pmatrix} 1 & -1 & \cdots & -1 \\ & 1 & & 0 \\ & & \ddots & \\ 0 & & & 1 \end{pmatrix}, \tag{D27}$$

we have

$$U|GHZ\rangle_p = |0\rangle|0, \ldots, 0\rangle_p. \tag{D28}$$

We denote the projection to $U^\dagger I \otimes |0, \ldots, 0\rangle_p \, {}_p\langle 0, \ldots, 0|U$ and $U^\dagger|0\rangle\langle 0| \otimes I^{\otimes m-1}U$ by $\tilde{P}_1$ and $\tilde{P}_2$, respectively. Then, we find that

$$\tilde{P}_1\tilde{P}_2 = |GHZ\rangle_p \, {}_p\langle GHZ|. \tag{D29}$$

Also, we find that $\tilde{P}_1$ and $\tilde{P}_2$ are 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 $\tilde{P}_1^{\otimes n} \otimes \tilde{P}_2^{\otimes n} \otimes (I - |GHZ\rangle_{p\ p}\langle GHZ|)$, which expresses the event that they accept the test and the state on the remaining system is orthogonal to the state $|GHZ\rangle_{p\ p}\langle GHZ|$. We define the projection $\bar{P}_i := \tilde{P}_i - \bar{P}_0$, where $\bar{P}_0 := |GHZ\rangle_{p\ p}\langle GHZ|$ for $i = 1, 2$. Also, we define the projection $\bar{P}_3 := I - |GHZ\rangle_{p\ p}\langle GHZ| - \bar{P}_1 - \bar{P}_2$. Then, we have 4 orthogonal projections $\bar{P}_0, \bar{P}_1, \bar{P}_2, \bar{P}_3$.

Then, we have

$$A = \sum_{v \in \{0,1,2,3\}^{2n_1+1}} \frac{|C_1(v)|}{|C_2(v)|} \bar{P}_v, \tag{D30}$$

where $\bar{P}_v$, $C_1(v)$, and $C_2(v)$ are defined by using the number $N_i(v)$ of i in v as

$$\bar{P}_v := \bar{P}_{v_1} \otimes \cdots \otimes \bar{P}_{v_{2n_1+1}} \tag{D31}$$

$$C_2(v) := \binom{2n_1 + 1}{N_0(v) N_1(v) N_2(v) N_3(v)} \tag{D32}$$

and

$$C_1(v) := \left\{ v' \,\middle|\, \begin{array}{l} \bar{P}_{v'} \\ \le \tilde{P}_1^{\otimes n} \otimes \tilde{P}_2^{\otimes n} \otimes (I - |GHZ\rangle_{p\ p}\langle GHZ|), \\ v' \text{ is given as a permutation of } v \end{array} \right\}. \tag{D33}$$

Then, we find that the maximum eigenvalue of A is $\frac{1}{2n+1}$.[3] Since we have $\|A\| \le \frac{1}{2n+1}$, any initial state ρ satisfies $\mathrm{Tr}\rho A \le \frac{1}{2n+1}$.

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 $|GHZ\rangle_{p\ p}\langle GHZ|$ is upper bounded by $\frac{1}{\alpha} \cdot \frac{1}{2n+1}$. Hence, we obtain the desired statement. □

References

1. Chor, B., Kushilevitz, E.: A communication-privacy tradeoff for modular addition. Inf. Process. Lett. **45**(4), 205–210 (1993)
2. Chor, B., Shani, N.: The privacy of dense symmetric functions. Comput. Complex. **5**(1), 43–59 (1995)
3. Naor, M., Shamir, A.: Visual cryptography, advances in cryptology. Eurocrypt Proc. LNCS **950**, 1–2 (1995)
4. Kafri, O., Keren, E.: Encryption of pictures and shapes by random grids. Opt. Lett. **12**(6), 377–379 (1987)
5. Broadbent, A., Fitzsimons, J.F., Kashefi, E.: Universal blind quantum computation. In: Proceedings of the 50th Annual IEEE Symposium on Foundation of Computer Science, p. 517 (2009)
6. Morimae, T., Fujii, K.: Blind quantum computation for Alice who does only measurements. Phys. Rev. A **87**, 050301(R) (2013)

[3] A similar discussion is given [69, Appendix].

7. Hayashi, M., Morimae, T.: Verifiable measurement-only blind quantum computing with stabilizer testing. Phys. Rev. Lett. **115**, 220502 (2015)
8. Barz, S., Kashefi, E., Broadbent, A., Fitzsimons, J.F., Zeilinger, A., Walther, P.: Demonstration of blind quantum computing. Science **335**, 303 (2012)
9. Barz, S., Fitzsimons, J.F., Kashefi, E., Walther, P.: Experimental verification of quantum computation. Nat. Phys. **9**, 727 (2013)
10. Marshall, K., Jacobsen, C.S., Schäfermeier, C., Gehring, T., Weedbrook, C., Andersen, U.L.: Continuous-variable quantum computing on encrypted data. Nat. Commun. **7**, 13795 (2016)
11. Huang, H.-L., Zhao, Q., Ma, X., Liu, C., Su, Z.-E., Wang, X.-L., Li, L., Liu, N.-L., Sanders, B.C., Lu, C.-Y., Pan, J.-W.: Experimental blind quantum computing for a classical client. Phys. Rev. Lett. **119**(5), 050503 (2017)
12. Buhrman, H., Christandl, M., Schaffner, C.: Complete insecurity of quantum protocols for classical two-party computation. Phys. Rev. Lett. **109**, 160501 (2012)
13. Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing, In: Proceedings IEEE International Conference on Computers, Systems and Signal Processing (Bangalore, India, 1984), pp. 175–179
14. Mayers, D., Yao, A.: in Foundations of Computer Science, 1998. Proceedings. 39th Annual Symposium on (IEEE, 1998) pp. 503–509
15. Mayers, D., Yao, A.: Quantum Inf. Comput. **4**, 273 (2004)
16. Acín, A., Brunner, N., Gisin, N., Massar, S., Pironio, S., Scarani, V.: Device-independent security of quantum cryptography against collective attacks. Phys. Rev. Lett. **98**, 230501 (2007)
17. Pironio, S., Acín, A., Brunner, N., Gisin, N., Massar, S., Scarani, V.: Device-independent quantum key distribution secure against collective attacks. New J. Phys. **11**, 045021 (2009)
18. Shi, R.H., Mu, Y., Zhong, H., Cui, J., Zhang, S.: Secure multiparty quantum computation for summation and multiplication. Sci. Rep. **6**, 19655 (2016)
19. Zhang, C., Situ, H., Huang, Q., Yang, P.: Multi-party quantum summation without a trusted third party based on single particles. Int. J. Quantum Inf. **15**(2), 1750010 (2017)
20. Yang, H.Y., Ye, T.Y.: Secure multi-party quantum summation based on quantum Fourier transform. Quantum Inf. Process. **17**(6), 129 (2018)
21. Zhang, C., Razavi, M., Sun, Z., Huang, Q., Situ, H.: Multi-party quantum summation based on quantum teleportation. Entropy **21**, 719 (2019)
22. McKague, M.: In: Theory of Quantum Computation, Communication, and Cryptography: 6th Conference, TQC 2011, pp. 104–120. Springer, Berlin Heidelberg (2011)
23. McKague, M., Mosca, M.: In: Theory of Quantum Computation, Communication, and Cryptography: 5th Conference, TQC 2010 (Springer, 2010) pp. 113–130
24. McKague, M., Yang, T.H., Scarani, V.: J. Phys. A Math. Theor. **45**, 455304 (2012)
25. Li, X., Wang, Y., Han, Y., Gao, F., Wen, Q.: Self-testing of symmetric three-qubit states, arXiv:1907.06397 (2019)
26. Hayashi, M., Hajdusek, M.: Self-guaranteed measurement-based blind quantum computation. Phys. Rev. A **97**, 052308 (2018)
27. Šupć, I., Bowles, J.: Self-testing of quantum systems: a review. Quantum **4**, 337 (2020)
28. Bancal, J.-D., Redeker, K., Sekatski, P., Rosenfeld, W., Sangouard, N.: Self-testing with finite statistics enabling the certification of a quantum network link, arXiv:1812.09117 (2018)
29. Goldreich, O., Micali, S., Wigderson, A.: How to play any mental game or a complete theorem for protocols with honest majority. In: Proceedings of the 19th Annual ACM Symposium on Theory of Computation (STOC'87), pp. 218–229 (1987)
30. Ben-Or, M., Goldwasser, S., Wigderson, A.: Complete theorem for non-cryptographic fault-tolerant distributed computation. In: Proceedings of the 20th Annual Symposium on Theory of Computation (STOC'88), pp. 1–10 (1988)
31. Shamir, A.: How to share a secret. Commun. ACM **22**(11), 612–613 (1979)
32. Rabin, T., Ben-Or, M.: Verifiable secret sharing and multiparty protocols with honest majority. In: Proceedings of the 21st Annual ACM Symposium on Theory of computing (STOC 1989), pp. 73–85 (1989)
33. Ishai, Y., Ostrovsky, R., Seyalioglu, H.: Identifying cheaters without an honest majority. In: Proceedings of the 9th Theory of Cryptography Conference (TCC 2012), Lecture Notes in Computer Science 7194, pp. 21–38, Springer (2012)

34. Xu, R., Morozov, K., Takagi, T.: On cheater identifiable secret sharing schemes secure against rushing adversary. In: Proceedings of the 8th International Workshop on Security (IWSEC 2013), Lecture Notes in Computer Science 8231, pp. 258–271, Springer (2013)
35. Roy, P.S., Adhikari, A., Xu, R., Morozov, K., Sakurai, K.: An efficient t-cheater identifiable secret sharing scheme with optimal cheater resiliency, Cryptology Eprint Archive 2014/628 (2014)
36. Xu, R., Morozov, K., Takagi, T.: Cheater identifiable secret sharing schemes via multi-receiver authentication. In: Proceedings of the 9th International Workshop on Security (IWSEC 2014), Lecture Notes in Computer Science 8639, pp. 72–87, Springer (2014)
37. Adhikari, A., Morozov, K., Obana, S., Roy, P.S., Sakurai, K., Xu, R.: Efficient threshold secret sharing schemes secure against rushing cheaters. In: Proceedings of the 9th International Conference on Information Theoretic Security (ICITS 2016), Lecture Notes in Computer Science 10015, pp. 3–23, Springer (2016)
38. Hayashi, M., Koshiba, T.: 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)
39. Dolev, D., Dwork, C., Waarts, O., Yung, M.: Perfectly secure message transmission. J. ACM **40**(1), 17–47 (1993)
40. Agarwal, S., Cramer, R., de Haan, R.: Asymptotically optimal two-round perfectly secure message transmission, Advances in Cryptology—CRYPTO 2006, Lecture Notes in Computer Science 4117, pp. 394–408, Springer (2006)
41. Kurosawa, K., Suzuki, K.: Truly efficient 2-round perfectly secure message transmission scheme. IEEE Trans. Inf. Theory **55**(11), 5223–5232 (2009)
42. Spini, G., Zémor, G.: Perfectly secure message transmission in two rounds. In: Proceedings of the 14th Theory of Cryptography Conference (TCC2016-B), Lecture Notes in Computer Science 9985, pp. 286–304, Springer (2016)
43. Jaggi, S., Langberg, M., Katti, S., Ho, T., Katabi, D., Médard, M.: Resilient network coding in the presence of byzantine adversaries. In: Proceedings of the IEEE INFOCOM 2007, Anchorage, AK, pp. 616–624 (2007)
44. Jaggi, S., Langberg, M., Katti, S., Ho, T., Katabi, D., Medard, M., Effros, M.: Resilient network coding in the presence of byzantine adversaries. IEEE Trans. Inf. Theory **54**(6), 2596–2603 (2008)
45. Jaggi, S., Langberg, M.: Resilient network coding in the presence of eavesdropping byzantine adversaries. In: Proceedings of 2007 IEEE International Symposium on Information Theory (ISIT 2007), Nice, France, pp. 541–545 (2007)
46. Yao, H., Silva, D., Jaggi, S., Langberg, M.: Network codes resilient to jamming and eavesdropping. IEEE/ACM Trans. Netw. **22**(6), 1978–1987 (2014)
47. Hayashi, M., Cai, N.: Asymptotically secure network code for active attacks and its application to network quantum key distribution arXiv:2003.12225 (2020)
48. Franklin, M., Wright, R.N.: Secure communication in minimal connectivity models. J. Cryptol. **13**(1), 9–30 (2000)
49. 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)
50. Koshiba, T., Sawada, S.: Public discussion must be back and forth in secure message transmission. In: Proceedings of the 13th International Conference on Information Security and Cryptology (ICISC 2010), Lecture Notes in Computer Science 6829, pp. 325–337, Springer (2011)
51. Garay, J.A., Ostrovsky, R.: Almost-everywhere secure computation. Advances in Cryptology—EUROCRYPT 2008, Lecture Notes in Computer Science 4965, pp. 307–323, Springer (2008)
52. Gordon, S.D., Hazay, C., Katz, J., Lindell, Y.: Complete fairness in secure two-party computation. In: 40th STOC, pp. 413–422 (2008)
53. Goldwasser, S., Levin, L.: Fair computation of general functions in presence of immoral majority. In: CRYPTO'90 (LNCS 537), pp. 77–93, Springer (1990)
54. Gordon, S.D., Katz, J.: Partial fairness in secure two-party computation. In: EUROCRYPT' 10, Springer (LNCS 6110) (2010)
55. Krawczyk, H.: New hash functions for message authentication, EUROCRYPT'95, Lecture Notes in Computer Science 921, pp. 301–310, Springer (1995)
56. Maurer, U.M.: A unified and generalized treatment of authentication theory. In: Proceedings of the 13th Annual Symposium on Theoretical Aspects of Computer Science (STACS'96), Lecture Notes in Computer Science 1046, pp. 387–398. Springer (1996)

57. Gray, R.M.: Toeplitz and circulant matrices: a review. Found. Trends Commun. Inf. Theory **2**(3), 155–239 (2006)
58. Canetti, R.: Universally composable security: a new paradigm for cryptographic protocols. In: Proceedings of the 42nd Annual Symposium on Foundations of Computer Science, FOCS 2001, pp. 136–145 (2001)
59. Canetti, R.: Universally composable security: a new paradigm for cryptographic protocols, Version of December 2018. Available at https://eprint.iacr.org/2000/067.pdf
60. Goldreich, O.: Foundations of Cryptography, Basic Applications, vol. 2. Cambridge University Press, Cambridge (2009)
61. Fujii, K., Hayashi, M.: Verifiable fault tolerance in measurement-based quantum computation. Phys. Rev. A Rapid Commun. **96**, 030301(R) (2017)
62. Lehmann, E.L., Romano, J.P.: Testing Statistical Hypotheses. Springer, Berlin (2005)
63. Hayashi, M.: Secure modulo sum via multiple access channel. In: Proceedings of 2021 IEEE International Symposium on Information Theory (ISIT), Melbourne, Victoria, Australia, 12–20 July 2021, pp. 1397–1402; arXiv:1812.10862
64. Coladangelo, A., Goh, K.T., Scarani, V.: All pure bipartite entangled states can be self-tested. Nat. Commun. **8**, 15485 (2017)
65. Kaniewski, J., Šupić, I., Tura, J., Baccari, F., Salavrakos, A., Augusiak, R.: Maximal nonlocality from maximal entanglement and mutually unbiased bases, and self-testing of two-qutrit quantum systems. Quantum **3**, 198 (2019)
66. Sarkar, S., Saha, D., Kaniewski, J., Augusiak, R.: Self-testing quantum systems of arbitrary local dimension with minimal number of measurements, arXiv: 1909.12722
67. Hayashi, M.: Group Representation for Quantum Theory. Springer, Berlin (2017)
68. Hayashi, M., Ishizaka, S., Kawachi, A., Kimura, G., Ogawa, T.: Introduction to Quantum Information Science, Graduate Texts in Physics, Springer (2014). (Originally published from Kyoritsu Shuppan in 2012 with Japanese.)
69. Markham, D., Krause, A.: A simple protocol for certifying graph states and applications in quantum networks. Cryptography **4**, 3 (2020)