Quantum Information Processing (2022) 21:82
https://doi.org/10.1007/s11128-022-03426-8

Secure device-independent quantum bit-wise XOR summation based on a pseudo-telepathy game

Cai Zhang[1] · Tingting Wei[1]

Received: 15 September 2021 / Accepted: 9 January 2022 / Published online: 17 February 2022

Abstract

We present a device-independent quantum bit-wise XOR summation protocol based on a pseudo-telepathy multi-partite GHZ game proposed by Brassard et al. In this game, n participants can win the game with certainty with a quantum strategy, but using any classical strategy, they can only win the game with a probability that differs from $1/2$ by more than a fraction that is exponentially small in the number of participants. We also analyse the correctness and security of the proposed protocol, showing that it can resist well-known outside and participant attacks.

Keywords Quantum summation · Device-independent · Multi-partite GHZ game · Quantum information

1 Introduction

Since Mayers and Yao [1] presented the idea of device independence (DI) where the security of schemes depends on a statistical test performed on spatially separated measurement devices, it has been gaining attention recently [2–14]. Most DI protocols involved quantum key distribution [2–9], and the rest of them focused on quantum bit commitment, quantum coin tossing, position verification [10–14], and quantum secure direct communication [15]. However, few researchers investigated DI multi-partite secure quantum computation protocols. In 2019, Roy et al. [16] proposed a device-independent secret sharing protocol where a d-dimensional N-partite linear game is employed. Inspired by their work, we design a device-independent quantum bit-wise XOR summation protocol relying on the pseudo-telepathy multi-partite GHZ game [17, 18].

✉ Tingting Wei
tingtingwei2011@126.com

[1] College of Mathematics and Informatics, South China Agricultural University, Guangzhou 510642, China

Secure multi-party quantum summation [19–23] is a fundamental primitive of secure multi-party quantum computation [24–28], whose objectives are to protect the privacy of participants' inputs and to guarantee the correctness of summation result. Heinrich et al. first studied summation of sequences in quantum settings [19–21]. After that, an increasing number of researchers have been exploring this topic. Du et al. [22] utilized non-orthogonal states to design a secure quantum addition module $n + 1$ ($n \geq 2$) protocol. Chen et al. [23] proposed a protocol with multi-partite GHZ states. Zhang et al. presented quantum summation protocols using various quantum resources such as single photons in two-degree freedom [29], genuinely maximally entangled six-qubit states [30] and single qubits [31]. Shi et al. [32] put forward a quantum addition modulo N protocol with the quantum Fourier transform, where the participants' inputs are encoded on the phase information. Later, Shi et al. [33] suggested a quantum method to solve a class of special two-party summation problems. Liu et al. [34] constructed multi-partite entangled states from Bell states for a quantum summation protocol. In 2018, Yang et al. [35] come up with a quantum solution to secure summation using n-partite d-dimensional entangled states.

The game theory is an interesting field where each player chooses the best strategy to obtain their payoffs. The Kolkata restaurant problem is one of the interesting problems. Ramzan [36] investigated the three-player quantum Kolkata restaurant problem under decoherence in 2012. Sharif et al. [37] studied strategies in a symmetric quantum Kolkata restaurant problem based on an initial GHZ-type entanglement where each player used the same 8-dimensional representation of the unitary operator of SU(3) in their paper. Other multi-partite games (where each player has more than binary choices) were also studied [38]. The game theory in quantum settings is also usually used to design device-independent quantum cryptographic protocols. As such, we tried to find games that suit the design of device-independent quantum summation and finally found that the pseudo-telepathy multi-partite GHZ game proposed in [17] appropriate for this task. In this paper, we present a device-independent quantum bitwise XOR summation protocol based on this game in which participants are able to win the game with certainty with a quantum strategy.

The rest paper is organized as follows. In Sect. 2, we review the pseudo-telepathy game G_n in [17]. In Sect. 3, we describe our protocol in detail, followed by the correctness and the security analyses in Sect. 4. Finally, we make conclusions in Sect. 5.

2 The pseudo-telepathy G_n game

In this section, we introduce the game G_n ($n \geq 3$) in [17] that is composed of n players $P_1, P_2, \ldots, P_n$. Before the game starts, the players can communicate and discuss their strategies. After receiving their inputs, they are not allowed to communicate any more. An n-bit string $x_1x_2 \ldots x_n$ is uniformly chosen from a set of n-bit strings, in which each string contains an even number of 1. x_i ($i = 1, 2, \ldots, n$) is sent to P_i. P_i then outputs $a_i \in \{0, 1\}$. The players win the game if

$$\sum_{i=1}^{n} a_i \equiv \frac{1}{2}\sum_{i=1}^{n} x_i \pmod 2, \tag{1}$$

where $x = x_1x_2 \ldots x_n$ is the question and $a = a_1a_2 \ldots a_n$ is the answer.

Brassard et al. [17] have shown that no classical strategy for the game G_n can be successful with a probability better than $\frac{1}{2} + 2^{-\lceil n/2 \rceil}$. They also gave a quantum strategy to win the game with certainty rested on a GHZ state $|\Phi_n^+\rangle = \frac{1}{\sqrt{2}}|0^n\rangle + \frac{1}{\sqrt{2}}|1^n\rangle$, the Hadamard transform and a unitary transform defined by $S|b\rangle \mapsto (i)^b|b\rangle$, where $b \in \{0, 1\}$ and i is the imaginary unit.

For the design of our protocol, we employ another quantum strategy that also wins the game with certainty.

Quantum strategy to win the game: Before the game starts, n players $P_1, P_2, \ldots, P_n$ share an n-partite GHZ state $|\Psi\rangle = \frac{1}{\sqrt{2}}\sum_{r=0}^{1}|r\rangle_1|r\rangle_2 \ldots |r\rangle_n$, where the subscripts clarify that the i^{th} $(i = 1, 2, \ldots, n)$ particle is hold by P_i.

For the question $x_k = 0$ $(k = 1, 2, \ldots, n)$, P_i measures their particle with an observable $X = |0_0\rangle\langle 0_0| - |1_0\rangle\langle 1_0|$, where $|b_0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^b|1\rangle), b \in \{0, 1\}$. If P_i gets the eigenvalue $(-1)^b$ as a measurement result, he/she outputs $a_k = b$ as an answer to the question x_k. Similarly, for the question $x_k = 1$ $(k = 1, 2, \ldots, n)$, P_i measures their particle with an observable $Y = |0_1\rangle\langle 0_1| - |1_1\rangle\langle 1_1|$, where $|b_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i(-1)^b|1\rangle), b \in \{0, 1\}$. He/she sets $a_k = b$ if the measurement result $(-1)^b$ is obtained.

We now show that the probability of winning the game using the above quantum strategy is 1. First, the basis $\{|0\rangle, |1\rangle\}$ can be expressed in the basis $\{|0_0\rangle, |1_0\rangle\}$ and in the basis $\{|0_1\rangle, |1_1\rangle\}$ as

$$\begin{aligned} |0\rangle &= \frac{1}{\sqrt{2}}(|0_0\rangle + |1_0\rangle), \\ |1\rangle &= \frac{1}{\sqrt{2}}(|0_0\rangle - |1_0\rangle), \end{aligned} \tag{2}$$

and

$$\begin{aligned} |0\rangle &= \frac{1}{\sqrt{2}}(|0_1\rangle + |1_1\rangle), \\ |1\rangle &= \frac{-i}{\sqrt{2}}(|0_1\rangle - |1_1\rangle), \end{aligned} \tag{3}$$

respectively.

We also have the following facts

$$\begin{aligned} (-i)^j &= 1, \text{ if } j \bmod 4 = 0, \\ (-i)^j &= -1, \text{ if } j \bmod 4 = 2. \end{aligned} \tag{4}$$

As $x_1x_2 \ldots x_n$ is uniformly chosen from the set of strings with each element of the set containing an even number of 1s, the equation $\sum_{i=1}^{n} x_i \equiv 0 \pmod 2$ holds. In our case, the order of different measurements is not important. If $\frac{1}{2}\sum_{i=1}^{n} x_i \equiv 0 \pmod 2$, which means the number of 1s in $x_1x_2 \ldots x_n$ is divisible by 4, we may assume without loss of generality that the first j ($j \bmod 4 = 0$ and $j \leq n$) players measure their respective particles with the observable Y, and the other players measure their respective particles with the observable X. We can deduce the following

$$\begin{aligned}
|\Psi\rangle &= \frac{1}{\sqrt{2}}\sum_{r=0}^{1}|r\rangle_1|r\rangle_2\ldots|r\rangle_n \\
&= \frac{1}{\sqrt{2}}\sum_{r=0}^{1}\left(\left(\frac{(-i)^r}{\sqrt{2}}\sum_{b^1=0}^{1}(-1)^{rb^1}|b^1{}_1\rangle_1\right)\left(\frac{(-i)^r}{\sqrt{2}}\sum_{b^2=0}^{1}(-1)^{rb^2}|b^2{}_1\rangle_2\right)\ldots\right.\\
&\quad\left(\frac{(-i)^r}{\sqrt{2}}\sum_{b^j=0}^{1}(-1)^{rb^j}|b^j{}_1\rangle_j\right)\left(\frac{1}{\sqrt{2}}\sum_{b^{j+1}=0}^{1}(-1)^{rb^{j+1}}|b^{j+1}{}_0\rangle_{j+1}\right)\ldots\\
&\quad\left.\left(\frac{1}{\sqrt{2}}\sum_{b^n=0}^{1}(-1)^{rb^n}|b^n{}_0\rangle_n\right)\right)\\
&= \left(\frac{1}{\sqrt{2}}\right)^{n+1}\left(\sum_{b^1,b^2,\ldots,b^n=0}^{1}|b^1{}_1\rangle_1|b^2{}_1\rangle_2\ldots|b^j{}_1\rangle_j|b^{j+1}{}_0\rangle_{j+1}\ldots|b^n{}_0\rangle_n\right.\\
&\quad\left.+(-i)^j\sum_{b^1,b^2,\ldots,b^n=0}^{1}(-1)^{\sum_{k=1}^{n}b^k}|b^1{}_1\rangle_2|b^2{}_1\rangle_2\ldots|b^j{}_1\rangle_j|b^{j+1}{}_0\rangle_{j+1}\ldots|b^n{}_0\rangle_n\right)\\
&= \left(\frac{1}{\sqrt{2}}\right)^{n+1}\left(\sum_{b^1,b^2,\ldots,b^n=0}^{1}|b^1{}_1\rangle_1|b^2{}_1\rangle_2\ldots|b^j{}_1\rangle_j|b^{j+1}{}_0\rangle_{j+1}\ldots|b^n{}_0\rangle_n\right.\\
&\quad\left.+\sum_{b^1,b^2,\ldots,b^n=0}^{1}(-1)^{\sum_{k=0}^{n}b^k}|b^1{}_1\rangle_1|b^2{}_1\rangle_2\ldots|b^j{}_1\rangle_j|b^{j+1}{}_0\rangle_{j+1}\ldots|b^n{}_0\rangle_n\right)\\
&= \left(\frac{1}{\sqrt{2^{n-1}}}\right)\sum_{b^1+b^2+\cdots+b^n\equiv 0(\bmod 2)}|b^1{}_1\rangle_1|b^2{}_1\rangle_2\ldots|b^j{}_1\rangle_j|b^{j+1}{}_0\rangle_{j+1}\ldots|b^n{}_0\rangle_n,
\end{aligned} \tag{5}$$

according to Eqs. (2–4). Thus, after measurement, P_i ($i = 1, 2, \ldots, n$) gives the answer b^i, which satisfies

$$\sum_{i=1}^{n}b^i \equiv \frac{1}{2}\sum_{i=1}^{n}x_i \equiv 0 \pmod 2, \tag{6}$$

and they win the game.

On the other hand, if $\frac{1}{2}\sum_i^n x_i \equiv 1 \pmod 2$, which means the number of 1s in $x_1x_2\ldots x_n$ is congruent to 2 modulo 4 (note that $\sum_i^n x_i \equiv 0 \pmod 2$ is required), we may also assume without loss of generality that the first j ($j \bmod 4 = 2$ and $j \leq n$) players measure their respective particles with the observable Y, and the other players measure their respective particles with the observable X. Similarly, we can obtain

$$\begin{aligned}|\Psi\rangle &= \frac{1}{\sqrt{2}}\sum_{r=0}^{1}|r\rangle_1|r\rangle_2\ldots|r\rangle_n\\ &= \frac{1}{\sqrt{2^{n-1}}}\sum_{b^1+b^2+\cdots+b^n\equiv 1(\bmod 2)}|{b^1}_1\rangle_2|{b^2}_1\rangle_2\ldots|{b^j}_1\rangle_j|{b^{j+1}}_0\rangle_{j+1}\ldots|{b^n}_0\rangle_n.\end{aligned} \tag{7}$$

Again, the answer b^i $(i = 1, 2, \ldots, n)$ offered by P_i meets

$$\sum_{i}^{n} b^i \equiv \frac{1}{2}\sum_{i}^{n} x_i \equiv 1 \pmod 2, \tag{8}$$

and they win the game. In either case, the players win the game with certainty.

3 The protocol

In this section, we will employ the game G_n to design a device-independent quantum bit-wise XOR summation protocol. In our protocol, n parties $P_1, P_2, \ldots, P_n$, want to compute the bit-wise XOR summation of their private bit strings with the help of a third party (TP) in such a way that the privacy of their inputs is preserved and the correctness of summation result is guaranteed. TP is assumed to be semi-honest, which means that TP loyally executes the protocol, records all its intermediate computations, and might intend to steal the participants' private inputs from the record, but he cannot be corrupted by the adversary.

Precisely, suppose P_i $(i = 1, 2, \ldots, n$ and $n > 2)$ has a private bit string M_i of length N

$$M_i = \left(m_i^1, m_i^2, \ldots, m_i^N\right), \tag{9}$$

where $m_i^t \in \{0, 1\}$ $(t = 1, 2, \ldots, N)$. $\mathrm{P}_1, \mathrm{P}_2, \ldots, \mathrm{P}_n$ would like to jointly compute the summation of their private bit strings as follows:

$$\begin{aligned}M &= M_1 \oplus M_2 \oplus \cdots \oplus M_n\\ &= \left(m_1^1 \oplus \cdots \oplus m_n^1, m_1^2 \oplus \cdots \oplus m_n^2, \ldots, m_1^N \oplus \cdots \oplus m_n^N\right),\end{aligned} \tag{10}$$

where $\oplus$ denotes addition modulo 2.

Like other device-independent quantum cryptographic protocols, we list a minimal set of assumptions determining the security before our protocol description:

1. All parties' laboratories are perfectly isolated and no unwanted information can leak out to outside the laboratories.
2. Every party holds a trusted random number generator.

3. Every party has a measurement device with two inputs {0, 1} in their laboratory. There are two outputs for each input. In addition, the measurement devices are causally independent and also independent of the source.

Let's first give the outline of our protocol which consists of two parts. The first part employs the G_n game to guarantee the device independence. During the game, a semi-honest party and n parties are involved. The second part aims at the secure computation of summation of all parties' private bit strings. In this part, all parties use their outputs as their private keys to encrypt their private bit strings and get the summation result by bit-wise XORing their encrypted bit strings.

To make sure that there are at least N n-partite GHZ states after the testing procedure, we set

$$M = \lceil(\lceil\frac{1}{1-\mu}\rceil + \delta)N\rceil, \tag{11}$$

where $\lceil\ \rceil$ denotes the ceiling function, μ is the probability that an n-partite state is chosen to start the G_n game and δ is a small positive real number less than 1.

The protocol works as follows.

(S1) For each round $i \in \{1, 2, \ldots, M\}$:

(a) All n parties share an n-partite GHZ state

$$|\psi^i\rangle = \frac{1}{\sqrt{2}}\sum_{r^i=0}^{1}|r^i\rangle_1|r^i\rangle_2\cdots|r^i\rangle_n. \tag{12}$$

(b) One of n parties chooses a random bit T_i with $Pr(T_i = 1) = \mu$ and announces their choice to other parties.

(c) For $T_i = 1$, TP uniformly selects $x_1x_2\ldots x_n$ from the set of strings, each element of which contains an even number of 1s, and then sends x_j $(j = 1, 2, \ldots, n)$ to P_j.

(d) All parties input $x_1, x_2, \ldots, x_n$ to their respective measurement devices and output $a_1, a_2, \ldots, a_n$, respectively. They then announce their input and output pairs. Meanwhile, they define a random variable V_i as follows:

$$V_i = \begin{cases} 1, & \text{if they win the } G_n \text{ game,} \\ 0, & \text{otherwise.} \end{cases} \tag{13}$$

(S2) Testing: All parties compute $V = \frac{\sum_{i=1}^{M} V_i}{\sum_{i=1}^{M} T_i}$. The protocol will be aborted if $V < 1 - \eta$, where η is the noise tolerance. Otherwise, the protocol will proceed to the next step. Similar to [16], the protocol will be aborted with the probability less than $(1 - \mu(1 - e^{2\eta^2})))^M$.

(S3) Encryption: With high probability, there are at least N rounds such that $T_i = 0$. This means n parties share at least N n-partite GHZ states (if not, they abort the protocol). They choose the first N ones and measure their respective particles with the observable X. Concretely, for the k^{th} $(k = 1, 2, \ldots, N)$ n-partite GHZ state, they all input 0 to their measurement devices, P_j $(j = 1, 2, \ldots, n)$ records their output as a_j^k. Later, Pj computes $C_j = (m_j^1 \oplus a_j^1, m_j^2 \oplus a_j^2, \ldots, m_j^N \oplus a_j^N)$ according to their bit string $M_j = \left(m_j^1, m_j^2, \ldots, m_j^N\right)$ and announces C_j.

(S4) Computation: All parties can get the result by computing $C_1 \oplus C_2 \oplus \cdots \oplus C_n = M_1 \oplus M_2 \oplus \cdots \oplus M_n = M$, as the summation result required.

Note that there are also different procedures for the self-testing of n-partite GHZ states [39, 40]. The procedure in [39] can also be used for the design of n-party $(n \geq 4)$ quantum summation based on the n-partite partially GHZ state, but the procedure is more complex than that proposed by Brassard et al. [17]. The procedure in [40] works only in the three-party scenario.

4 Analysis

In this section, we analyse the correctness and the security of our protocol.

4.1 Correctness

We first show that if P_i $(i = 1, 2, \ldots, n)$ honestly offers their bit string M_i, they will finally get the correct summation result

$$\begin{aligned} M &= M_1 \oplus M_2 \oplus \cdots \oplus M_n \\ &= \left(m_1^1 \oplus \cdots \oplus m_n^1, m_1^2 \oplus \cdots \oplus m_n^2, \ldots, m_1^N \oplus \ldots \oplus m_n^N\right). \end{aligned} \tag{14}$$

Clearly, N n-partite GHZ states are used for the summation computation. Using the similar method for Eq. (5), we expand each $|\psi^k\rangle$ $(k = 1, 2, \ldots, N)$ in the basis $\{|0_0\rangle, |1_0\rangle\}$ as follows:

$$\begin{aligned} |\psi^k\rangle &= \frac{1}{\sqrt{2}} \sum_{r^k=0}^{1} |r^k\rangle_1 |r^k\rangle_2 \cdots |r^k\rangle_n \\ &= \frac{1}{\sqrt{2^{n-1}}} \sum_{a_1^k + a_2^k + \cdots + a_n^k \equiv 0(\bmod 2)} |(a_1^k)_0\rangle_1 |(a_2^k)_0\rangle_2 \cdots |(a_n^k)_0\rangle_n. \end{aligned} \tag{15}$$

Note that $a_1^k + a_2^k + \cdots + a_n^k \equiv 0(\text{mod}2)$.

After P_i measures their particle with the X observable, he/she will get

$$(a_i^1, a_i^2, \ldots, a_i^N). \tag{16}$$

P_i then calculates $C_i = (m_i^1 \oplus a_i^1, m_i^2 \oplus a_i^2, \ldots, m_i^N \oplus a_i^N)$ and announces it. All parties eventually compute

$$
\begin{aligned}
& C_1 \oplus C_2 \oplus \cdots \oplus C_n \\
& = \left(\bigoplus \sum_{i=1}^{n} m_i^1 \oplus a_i^1, \bigoplus \sum_{i=1}^{n} m_i^2 \oplus a_i^2, \ldots, \bigoplus \sum_{i=1}^{n} m_i^N \oplus a_i^N \right) \\
& = \left(\bigoplus \sum_{i=1}^{n} m_i^1 \oplus \bigoplus \sum_{i=1}^{n} a_i^1, \bigoplus \sum_{i=1}^{n} m_i^2 \oplus \bigoplus \sum_{i=1}^{n} a_i^2, \ldots, \bigoplus \sum_{i=1}^{n} m_i^N \oplus \bigoplus \sum_{i=1}^{n} a_i^N \right) \\
& = \left(\bigoplus \sum_{i=1}^{n} m_i^1, \bigoplus \sum_{i=1}^{n} m_i^2, \ldots, \bigoplus \sum_{i=1}^{n} m_i^N \right) \\
& = M_1 \oplus M_2 \oplus \ldots \oplus M_n = M,
\end{aligned}
\tag{17}
$$

where $\bigoplus \sum$ is defined as $\bigoplus \sum_{i=1}^{n} x_i = x_1 \oplus x_2 \oplus \ldots \oplus x_n$.

Thus, all parties will get the correct summation result by an honest implementation in the absence of effective eavesdropping.

4.2 Security

In this subsection, we analyse the security of our protocol. A theorem to ensure that the n-partite GHZ state is genuinely shared among n parties is first presented, depending on which the analyses of outside and participant attacks follow.

Theorem 1 *If the testing phase of the presented protocol is successful, then the n parties can share genuine n-partite GHZ states securely for large M.*

Proof In our protocol, all the M n-partite GHZ states $\{\left|\psi^i\right\rangle | i = 1, 2, \ldots, M\}$ correspond to the random bit string $T = (T_1, T_2, \ldots, T_M) \in \{0, 1\}^M$ in the follow way: $|\psi^i\rangle$ will be used in the testing phase for $T_i = 1$. For the $i \in \{1, 2, \ldots, M\}$ such that $T_i = 1$, a random variable V_i is defined by: $V_i = 1$, if the parties win the G_n game; otherwise, $V_i = 0$. Further, we define $V = \frac{\sum_{i=1}^{M} V_i}{\sum_{i=1}^{M} T_i}$, then $E(V) = 1$. By applying Hoeffding bound [41], we obtain

$$
\begin{aligned}
& \Pr(|V - \mathbb{E}(V)| \geq \varepsilon) \\
& \quad = \Pr(|\frac{\sum_{i=1}^{M} V_i}{\sum_{i=1}^{M} T_i} - \mathbb{E}(\frac{\sum_{i=1}^{M} V_i}{\sum_{i=1}^{M} T_i})| \geq \varepsilon) \\
& \quad = \Pr(|\frac{1}{M}(\sum_{i=1}^{M} V_i - \mathbb{E}(\sum_{i=1}^{M} V_i))| \geq \frac{\varepsilon \sum_{i=1}^{M} T_i}{M}) \\
& \quad \leq \exp\left(-2\frac{\varepsilon^2 (\sum_{i=1}^{M} T_i)^2}{M}\right) = \epsilon_{\text{test}},
\end{aligned}
\tag{18}
$$

where ϵ_{test} is a negligibly small positive value. ε can be expressed in terms of ϵ_{test} as

$$
\varepsilon = \sqrt{\frac{M}{2(\sum_{i=1}^{M} T_i)^2} \ln\left(\frac{1}{\epsilon_{\text{test}}}\right)}. \tag{19}
$$

We can also define $V' = \frac{\sum_{\{T_i=0\}} V_i}{M-\sum_i T_i}$. From the corollary of Serfling lemma [42], we then have $\Pr(|V - V'| \geq \lambda) \leq \epsilon_{\mathrm{qs}}$, where ϵ_{qs} is a small quantity and

$$\lambda = \sqrt{\frac{M\left(\sum_i T_i + 1\right)}{2\left(\sum_i T_i\right)^2\left(M - \sum_i T_i\right)} \ln\left(\frac{1}{\epsilon_{\mathrm{qs}}}\right)}. \tag{20}$$

Because $\sum_i T_i \approx \mu M$, ε and λ will approach zero when M is large enough. We can therefore conclude that if a randomly chosen subset of the set $\{\left|\psi^i\right\rangle | i = 1, 2, \ldots, M\}$ passes the testing phase of our protocol, then the rest entangled states are genuinely shared in the n-partite GHZ state form among n parties and the measurement devices also fulfil the requirements. □

The security of our protocol relies on a property of quantum entanglement called polygamy stating that all maximally entangled states are (classically and quantically) uncorrelated with any other system [43].

For the outside attacks from Eve, as the correlations obtained in the testing phase of our protocol guarantees that the shared entangled state is of the form $|\psi^i\rangle = \frac{1}{\sqrt{2}} \sum_{r^i=0}^{1} |r^i\rangle_1 |r^i\rangle_2 \cdots |r^i\rangle_n$, and the measurement devices also meet our specifications, we conclude that these correlations must be independent of any information that the eavesdropper Eve can obtain according to the polygamy of entanglement.

For the participant attacks from dishonest parties, consider the k^{th} $(k = 1, 2, \ldots, N)$ n-partite GHZ state among them $|\psi^k\rangle = \frac{1}{\sqrt{2}} \sum_{r^k=0}^{1} |r^k\rangle_1 |r^k\rangle_2 \cdots |r^k\rangle_n$ that is used to generate parties' keys and the case where $n-2$ dishonest parties intend to steal the other two parties' private inputs (say, P_w's and P_v's private inputs). When P_i $(i = 1, 2, \ldots, n)$ measures their particle belonging to this state with the observable X and obtains the measurement result a_i^k, they have

$$a_1^k + a_2^k + \cdots + a_n^k \equiv 0(\mathrm{mod} 2), \tag{21}$$

based on Eq. (15).

To learn about P_w's private bit m_w^k and P_v's private bit m_v^k, the dishonest parties should know a_w^k and a_v^k that are used to encrypt m_w^k and m_v^k, respectively. However, they can only attain $a_w^k + a_v^k(\mathrm{mod} 2)$ from Eq. (21) and their respective measurement results with the observable X. They cannot get the exact values of a_w^k and a_v^k and thus fail to find out the values of m_w^k and m_v^k.

Note that any $n-1$ dishonest parties can easily get the rest one's private bit string. That is to say, our protocol is secure against $(n-2)$-party collusive attacks.

5 Conclusions

We have designed the device-independent quantum summation protocol using the pseudo-telepathy multi-partite GHZ game in which n participants can win the game with certainty with the quantum strategy. No classical strategy exists that can win the game with a probability that differs from $1/2$ by more than a fraction that is exponentially small in the number of participants. The security analysis has shown that it is secure against $(n-2)$-party collusive attacks. Note that we assumed that the measurement devices are causally independent in our protocol, and thus, extending our protocol to a fully device-independent one would be our future work.

Acknowledgements This work is supported by the National Natural Science Foundation of China (Grant Nos. 61902132, 11647140), the Guangdong Basic and Applied Basic Research Foundation (Grant No. 2021A1515011985), and the Natural Science Foundation of Guangdong Province of China (Grant No. 2018A030310147).

References

1. Mayers, D., Yao, A.: In: Proceedings 39th Annual Symposium on Foundations of Computer Science (Cat. No. 98CB36280). IEEE, pp. 503–509 (1998)
2. Acín, A., Massar, S., Pironio, S.: Efficient quantum key distribution secure against no-signalling eavesdroppers. New J. Phys. **8**(8), 126 (2006)
3. 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**(23), 230501 (2007)
4. Pironio, S., Acin, A., Brunner, N., Gisin, N., Massar, S., Scarani, V.: Device-independent quantum key distribution secure against collective attacks. New J. Phys. **11**(4), 045021 (2009)
5. McKague, M.: Device independent quantum key distribution secure against coherent attacks with memoryless measurement devices. New J. Phys. **11**(10), 103037 (2009)
6. Masanes, L., Pironio, S., Acín, A.: Secure device-independent quantum key distribution with causally independent measurement devices. Nat. Commun. **2**, 238 (2011)
7. Barrett, J., Colbeck, R., Kent, A.: Memory attacks on device-independent quantum cryptography. Phys. Rev. Lett. **110**(1), 010503 (2013)
8. Lim, C.C.W., Portmann, C., Tomamichel, M., Renner, R., Gisin, N.: Device-independent quantum key distribution with local Bell test. Phys. Rev. X **3**(3), 031006 (2013)
9. Vazirani, U., Vidick, T.: Fully device independent quantum key distribution. Commun. ACM **62**(4), 133–133 (2019)
10. Kaniewski, J., Wehner, S.: Device-independent two-party cryptography secure against sequential attacks. New J. Phys. **18**(5), 055004 (2016)
11. Silman, J., Chailloux, A., Aharon, N., Kerenidis, I., Pironio, S., Massar, S.: Fully distrustful quantum bit commitment and coin flipping. Phys. Rev. Lett. **106**, 220501 (2011)
12. Adlam, E., Kent, A.: Device-independent relativistic quantum bit commitment. Phys. Rev. A **92**, 022315 (2015)
13. Aharon, N., Massar, S., Pironio, S., Silman, J.: Device-independent bit commitment based on the CHSH inequality. New J. Phys. **18**(2), 025014 (2016)
14. Ribeiro, J., Thinh, L.P., Kaniewski, J.M.K., Helsen, J., Wehner, S.: Device independence for two-party cryptography and position verification with memoryless devices. Phys. Rev. A **97**, 062307 (2018)
15. Zhou, L., Sheng, Y.B., Long, G.L.: Device-independent quantum secure direct communication against collective attacks. Sci. Bull. **65**(1), 12 (2020)
16. Roy, S., Mukhopadhyay, S.: Device independent quantum secret sharing in arbitrary even dimension. Phys. Rev. A **100**(1), 012319 (2019)
17. Brassard, G., Broadbent, A., Tapp, A.: In: WADS (2003)
18. Boyer, M.:Extended GHZ n-player games with classical probability of winning tending to 0, eprint. arXiv:quant-ph/0408090v4 (2004)
19. Heinrich, S.: Quantum summation with an application to integration. J. Complex. **18**(1), 1 (2002)
20. Heinrich, S., Novak, E.: On a problem in quantum summation. J. Complex. **19**(1), 1 (2003)
21. Heinrich, S., Kwas, H., Wozniakowski, M.: Quantum Boolean summation with repetitions in the worst-average setting. arXiv:quant-ph/0311036 (2003)
22. Du, J.Z., Chen, X.B., Wen, Q.Y., Zhu, F.C.: Secure multiparty quantum summation. Acta Phys. Sin. **56**(11), 6214 (2007)

23. Chen, X.B., Xu, G., Yang, Y.X., Wen, Q.Y.: An efficient protocol for the secure multi-party quantum summation. Int. J. Theor. Phys. **49**(11), 2793 (2010)
24. Lo, H.K.: Insecurity of quantum secure computations. Phys. Rev. A **56**, 1154 (1997)
25. Crépeau, C., Gottesman, D., Smith, A.: In: Proceedings of the Thiry-Fourth Annual ACM Symposium on Theory of Computing (ACM, 2002), pp. 643–652
26. Chau, H.F.: Quantum-classical complexity-security tradeoff in secure multiparty computations. Phys. Rev. A **61**, 032308 (2000)
27. Ben-Or, M., Crepeau, C., Gottesman, D., Hassidim, A., Smith, A.: In: 47th Annual IEEE Symposium on Foundations of Computer Science, 2006. FOCS'06. IEEE, pp. 249–260 (2006)
28. Smith, A.: Multi-party Quantum Computation. arXiv:quant-ph/0111030 (2010)
29. Zhang, C., Sun, Z., Huang, Y., Long, D.: High-capacity quantum summation with single photons in both polarization and spatial-mode degrees of freedom. Int. J. Theor. Phys. **53**(3), 933 (2014)
30. Zhang, C., Sun, Z.W., Huang, X., Long, D.Y.: Three-party quantum summation without a trusted third party. Int. J. Quantum Inf. **13**(02), 1550011 (2015)
31. 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**(1), 1750010 (2017)
32. Shi, R.H., Mu, Y., Zhong, H., Cui, J., Zhang, S.: Sci. Rep. **6**, 19655 (2016)
33. Shi, R.H., Zhang, S.: Secure multiparty quantum computation for summation and multiplication. Quantum Inf. Process. **16**(9), 225 (2017)
34. Liu, W., Wang, Y.B., Fan, W.Q.: An novel protocol for the quantum secure multi-party summation based on two-particle bell states. Int. J. Theor. Phys. **56**(9), 2783 (2017)
35. Yang, H.Y., Ye, T.Y.: Secure multi-party quantum summation based on quantum Fourier transform. Quantum Inf. Process. **17**(6), 129 (2018)
36. Ramzan, M.: Three-player quantum Kolkata restaurant problem under decoherence. Quantum Inf. Process. **12**(1), 577 (2013)
37. Sharif, P., Heydari, H.: In: AIP Conference Proceedings (American Institute of Physics, 2012), pp. 492–496
38. Kastampolidou, K., Papalitsas, C., Andronikos, T.: DKPRG or how to succeed in the kolkata paise restaurant gamevia TSP. arXiv preprint arXiv:2101.07760 (2021)
39. Šupić, I., Coladangelo, A., Augusiak, R., Acín, A.: Self-testing multipartite entangled states through projections onto two systems. New J. Phys. **20**(8), 083041 (2018)
40. Breiner, S., Kalev, A., Miller, C.A.: Parallel self-testing of the GHZ state with a proof by diagrams. arXiv preprint arXiv:1806.04744 (2018)
41. Hoeffding, W.: In: The Collected Works of Wassily Hoeffding (Springer, 1994), pp. 409–426
42. Serfling, R.J.: Probability inequalities for the sum in sampling without replacement. Ann. Stat, pp. 39–48 (1974)
43. Cavalcanti, D., Brandão, F.G., Cunha, M.T.: Are all maximally entangled states pure? Phys. Rev. A **72**(4), 040303 (2005)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.