Quantum Inf Process (2018) 17:77
https://doi.org/10.1007/s11128-018-1849-2

Clauser–Horne–Shimony–Holt versus three-party pseudo-telepathy: on the optimal number of samples in device-independent quantum private query

Jyotirmoy Basak[1] · **Subhamoy Maitra**[1]

Received: 28 November 2017 / Accepted: 14 February 2018 / Published online: 21 February 2018

Abstract In device-independent (DI) paradigm, the trustful assumptions over the devices are removed and CHSH test is performed to check the functionality of the devices toward certifying the security of the protocol. The existing DI protocols consider infinite number of samples from theoretical point of view, though this is not practically implementable. For finite sample analysis of the existing DI protocols, we may also consider strategies for checking device independence other than the CHSH test. In this direction, here we present a comparative analysis between CHSH and three-party Pseudo-telepathy game for the quantum private query protocol in DI paradigm that appeared in Maitra et al. (Phys Rev A 95:042344, 2017) very recently.

Keywords CHSH · Pseudo-telepathy · QKD · QPQ

1 Introduction

In recent times, most of the quantum protocols involve sharing of entangled states. In case these are generated by a third party, it is almost mandatory to measure the quantum states used for the protocol to check whether those are actually in the intended form or not. If an entangled state is not what is expected, the adversary may obtain certain extra information, thereby violating the security of the cryptographic scheme. This leads to the development of the idea toward testing the states generated by third-party devices before proceeding for the actual protocol. Mayers and Yao first proposed the idea of

✉ Subhamoy Maitra
subho@isical.ac.in

Jyotirmoy Basak
bjyotirmoy.93@gmail.com

[1] Applied Statistics Unit, Indian Statistical Institute, Kolkata, India

self-testing of quantum device [1]. For quantum cryptographic protocols, such self-testing is defined in DI paradigm that guarantees security under certain assumptions.

Generally, the quantum protocols involve sharing of the Bell states or some other two-qubit entangled states. For this reason, violation of CHSH inequality [2] or CHSH test [3] is exploited in most of the device-independent quantum cryptographic protocols (e.g., [4–6]). The security analysis generally considers infinite number of samples and asymptotic treatment. However, for all practical purposes, we have finite number of samples, and thus, we would always like to **minimize** the amount of samples required. In this direction, we study the very recently proposed DI-QPQ [4] (a modification of [7] to obtain device independence) as a framework in comparing the number of samples using different games. Thus, here we consider how to use quantum multiparty pseudo-telepathy game [8] in such scenario and compare its performance with CHSH game in terms of number of samples.

While investigating the performance of CHSH as well as three-party pseudo-telepathy game for DI-QPQ, it is noted that for a significant range of parameters, the success probability of the pseudo- telepathy game is higher than CHSH. The relation between the required sample size and corresponding success probability for testing DI is well known where one can see that the sample size is inversely proportional with the success probability of DI testing. Thus, for a considerable range of parameters, where the success probability of three-party pseudo-telepathy game is higher compared to CHSH, one can use the first one instead of the second to obtain better efficiency. With this understanding, we propose a certain strategies for testing device independence to minimize the overall sample size.

As we have initially noted, entanglement is the key resource in the domain of quantum communication. Thus, before proceeding further, let us outline certain important (non-exhaustive though) references toward the application of quantum entanglement. Such applications include the broad field of quantum information processing, such as quantum key distribution, quantum secure direct communication, quantum dense coding, quantum computation, besides quantum teleportation. One may refer to the initial works about quantum information processing related to entanglement as in [9,10]. There are also applications in quantum dense coding [11], quantum secure direct communication [12,13], hyper-entanglement [14], quantum computation [15–17], quantum-controlled teleportation [18,19], joint remote control [20] and joint remote state preparation [21] to refer a few. Next, we get into the specific background that is required for understanding this work.

2 Background

In this section, we present several related backgrounds.

2.1 CHSH and parity game

The CHSH game [3] is played by two players: Alice and Bob (in the same team) are not allowed to communicate in any manner after the initial setup where they may share an entangled state. The referee provides one random bit x to Alice and one random bit

y to Bob. Alice has to provide the referee a bit a, and Bob has to send b. The referee declares Alice and Bob the winner if $a \oplus b = x \wedge y$; otherwise, they are considered defeated.

When Alice and Bob participate in classical setup, the maximum success probability they can achieve is 0.75. However, when they share each particle of a maximally entangled state and follow some specific kind of measurement strategy, they can win the game with the probability $\cos^2(\frac{\pi}{8})$. Instead of exploiting the maximally entangled state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, if Alice and Bob share any (non-maximally entangled) state, then the success probability reduces. Such states have been exploited in [4].

In the parity (multiparty pseudo-telepathy) game [22], each player A_i receives a single input bit x_i and is requested to produce a single output bit y_i. The players are promised that there is an even number of 1's among their inputs. Without being allowed to communicate after receiving their inputs, the players are challenged to produce a collective output that contains an even number of 1's if and only if the number of 1's in the input is divisible by 4. More formally, it requires that $\sum_i^n y_i \equiv \frac{1}{2}\sum_i^n x_i (\mathrm{mod}\ 2)$, provided $\sum_i^n x_i \equiv 0 (\mathrm{mod}\ 2)$. If we consider the game for three parties, then the maximum success probability achieved in classical case equals to 0.75. However, if the three parties share three-qubit maximally entangled state and perform some particular measurements, they can achieve success with certainty (probability 1) in the quantum case. To match it with the ideas in [4], instead of the GHZ state $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$, if three parties share a (non-maximally entangled) state, the maximum success probability decreases. However, still this will be significantly better for certain range of parameters than that of [4]. This is explained in Sect. 4.

2.2 Estimation of sample size for finite sample scenario

Generally, if we like to distinguish one event having probability p and another having probability $p(1+\epsilon)$, where ϵ is small, then the approximate number of samples required is $O(\frac{1}{p\epsilon^2})$. Informally speaking, one may have a confidence of more than 99% in distinguishing two events with $\frac{64}{p\epsilon^2}$ samples. A more involved expression related to sample size in finite sample scenario can be obtained using Chernoff–Hoeffding [23] bound.

Proposition 1 *Let* $X = \frac{1}{m}\sum_{1\le i\le m} X_i$ *be the average of* m *independent random variables* $X_1, X_2, \ldots, X_m$ *with values* $[0,1]$*, and let* $\mathbb{E}[X] = \frac{1}{m}\sum_{1\le i\le m}\mathbb{E}[X_i]$ *be the expected value of* X*. Then for any* $\delta > 0$*, we have* $\Pr[|X - \mathbb{E}[X]| \ge \delta] \le \exp(-2\delta^2 m)$.

In our case, if the test succeeds, we set $X_i = 1$; otherwise, $X_i = 0$. Let us consider $\mathbb{E}[X] = \mathbb{E}[X_i] = p$ and let the variable X denotes the actual success probability p'. Now the question is how large should "the number of samples" be so that we get a good "accuracy" with high "confidence"? More precisely, suppose we want to estimate the success probability p within an error margin of ϵp and confidence $1-\gamma$, that is,

$$\Pr[|p' - p| \le \epsilon p] \ge 1 - \gamma, \tag{1}$$

where p' and p are the estimated and the expected values, respectively. Comparing Eq. (1) with Proposition 1, and given ϵ, p and γ, we obtain $\exp(-2\epsilon^2 p^2 m) \leq \gamma$, i.e., $m \geq \frac{1}{2\epsilon^2 p^2} \ln \frac{1}{\gamma}$. This implies that as the value of the success probability increases, the required sample size decreases. Denoting the maximum success probability for a specific θ by $p_{\max}$, one can write,

$$m_{\text{opt}} = \frac{1}{2\epsilon^2 p_{\max}^2} \ln \frac{1}{\gamma} \tag{2}$$

This m_{opt} gives the optimal value of the sample size required to certify a given state where the value of θ corresponding to this state is already known.

2.3 Device independence in QPQ

Here we are interested in investigating how the number of samples toward testing an entangled state can be reduced. Thus, instead of getting into tedious security proofs based on several complicated assumptions, we like to present our assumptions related to device independence. We consider that the required qubits, the quantum gates (unitary operations) and the measurement devices will be provided by the third party. That is, in the DI setting, the security of the protocol can be guaranteed even after removing this trustful assumption over the source, circuits and measurement devices. In the DI-QPQ protocol, the server asks for non-optimally entangled states from a third party and also the measurement devices are purchased from outside. The claimed idea of [4] is as follows.

The two-qubit entangled state involved in quantum private query (QPQ) protocol is of the form

$$|\psi_{\text{QPQ}}\rangle = \frac{1}{\sqrt{2}}(|0\rangle_B|\phi_0\rangle_A + |1\rangle_B|\phi_1\rangle_A) \tag{3}$$

where $|\phi_0\rangle_A = \cos(\frac{\theta}{2})|0\rangle + \sin(\frac{\theta}{2})|1\rangle$ and $|\phi_1\rangle_A = \cos(\frac{\theta}{2})|0\rangle - \sin(\frac{\theta}{2})|1\rangle$. The success probability of this version of CHSH game (this is not exactly the CHSH game with maximally entangled state) for this state $|\psi_{\text{QPQ}}\rangle$ will be $\frac{1}{8}(\sin\theta(\sin\psi_1 + \sin\psi_2) + \cos\psi_1 - \cos\psi_2) + \frac{1}{2}$ where $|\psi_1\rangle$ and $|\psi_2\rangle$ are the chosen measurement basis and this success probability value can be maximized by choosing appropriate measurement basis $|\psi_1\rangle$ and $|\psi_2\rangle$ for a particular θ.

From the expression derived in Sect. 2.2, it is clear that the expected sample size is inversely proportional with the success probability. So, when we consider the finite sample device- independent QPQ protocol, we have to maximize the success probability corresponding to a particular state (i.e., for a particular value of θ) to optimize the overall sample size. This is done by properly choosing the values of ψ_1, ψ_2. Note that this optimal choice of ψ_1 and ψ_2 is only valid for the purpose of DI testing as this ψ_1 and ψ_2 is not involved in the actual execution of QPQ protocol [4]. However for testing purpose, it is better to use the optimized basis for lesser number of samples.

In the DI-QPQ protocol [4], Bob and Alice share entangled states of the form $\frac{1}{\sqrt{2}}(|0\rangle_B|\phi_0\rangle_A + |1\rangle_B|\phi_1\rangle_A)$, where $|\phi_0\rangle_A = \cos(\frac{\theta}{2})|0\rangle + \sin(\frac{\theta}{2})|1\rangle$ and $|\phi_1\rangle_A =$

$\cos(\frac{\theta}{2})|0\rangle - \sin(\frac{\theta}{2})|1\rangle$. The value of θ is known to all. Bob chooses two measurement bases namely $\{|\psi_1\rangle, |\psi_1^{\perp}\rangle\}$ and $\{|\psi_2\rangle, |\psi_2^{\perp}\rangle\}$, to play the local CHSH game. Here, $|\psi_1\rangle = \cos\frac{\psi_1}{2}|0\rangle + \sin\frac{\psi_1}{2}|1\rangle$ and $|\psi_2\rangle = \cos\frac{\psi_2}{2}|0\rangle + \sin\frac{\psi_2}{2}|1\rangle$.

Thus, Bob gets the success probability in terms of θ, ψ_1 and ψ_2 which is equal to $\frac{1}{8}(\sin\theta(\sin\psi_1 + \sin\psi_2) + \cos\psi_1 - \cos\psi_2) + \frac{1}{2}$. To maximize the quantity, we have to maximize $\sin\theta(\sin\psi_1 + \sin\psi_2) + \cos\psi_1 - \cos\psi_2$. Calculation shows that the optimal value of ψ_1, ψ_2 corresponding to a particular θ will be $\psi_1 = (\frac{\pi}{2} - \tan^{-1}(\text{cosec}\,\theta))$ and $\psi_2 = (\frac{\pi}{2} + \tan^{-1}(\text{cosec}\,\theta))$. So, the optimal sample size required to test the source device in two-party scenario can be found by expression 2 where the value of ψ_1, ψ_2 corresponding to the value $p_{\max}$ will be $\psi_1 = (\frac{\pi}{2} - \tan^{-1}(\text{cosec}\,\theta))$ and $\psi_2 = (\frac{\pi}{2} + \tan^{-1}(\text{cosec}\,\theta))$. While evaluating with our new proposal, we will compare with this optimized data and show when we can obtain better result.

2.3.1 A caveat on device independence and security proofs

Now it is important to describe what provides the device independence in [4]. The proof of device independence is varied and not streamlined. In [4], the claim of device independence comes from the following:

- The server (Bob) asks for entangled states of the form $\frac{1}{\sqrt{2}}(|0\rangle_B|\phi_0\rangle_A + |1\rangle_B|\phi_1\rangle_A)$ from third party (TP) as described before. This is basically dependent on θ, i.e., the server provides the value of θ to the TP and the TP provides the required (non-maximal) entangled states.
- The server obtains the measurement devices (MDs) from the third party too that will be able to measure in certain measurement basis. These MDs are memoryless, and thus, each measurement will be independent. Further during the run time, it is assumed that the MDs cannot communicate to any body other than Bob, i.e., no information is leaked from the devices.

Based on these assumptions, it is claimed that by performing the CHSH test Bob should obtain certain result related to success probability which he already knows. In case the experimental data closely match with what he expects, then he will believe on the entangled states obtained as well as the MDs which were provided by TP.

We like to add the following point here. When the server (Bob) receives an entangled state as above, he may keep one particle with him and communicate the other one to the client (Alice). This is because the idea of device independence exploits non-locality. With one MD at Bob's side and another at Alice's, the security notions should work if they play the game and then publicly announces the classical outcome. Then, Bob and Alice will get to know each other's input as well as outcome after completion of the game and consequently together can estimate whether the correct state is supplied. On the other hand, there could be an argument that Alice may be colluded with the TP and possibly that is the reason the complete game was played in the server side for checking the states in [4]. However, the exact security issues here are not clear. On the other hand, this does not affect the work in this initiative as we are primarily interested about studying the number of samples and not the security issues.

We conclude this discussion with some issues related to security proofs. In the domain of cryptology, there are two directions.

– One may provide certain schemes with design details as well as certain justifications toward security and then wait for the cryptanalytic results. This mostly happens in the actual implementations that are in the application domain. The cryptanalytic efforts continue, and once a system is attacked, necessary countermeasures are taken. However, no specific formal security proof is provided. For example, design of commercial stream or block ciphers still follow this line. This was the scenario when BB84 protocol [24] was first proposed as, at that time, the security claims were justified from certain laws of Physics.
– Providing schemes with complete security proofs. In this case, certain basic assumptions are considered, and based on that there are formal-looking security proofs. These are mostly popular in theoretical world. However, certain systems are arriving in market where security proofs are advertised. The main problem in this domain is that in certain cases flaws are identified in many security proofs. In fact, larger the proof, lesser the confidence as many of the long proofs require more serious attention. However, in the positive direction we must appreciate that after the publication of the BB84 protocol, in last three decades researchers have noted many important theoretical proofs justifying several security aspects of BB84 and its variants.

This is an age-old philosophical debate. In this paper, the DI idea that we mention (toward reducing the number of samples) using pseudo-telepathy is not supported by rigorous proof. However, one may refer to [25] and the references therein to get a view of how pseudo-telepathy games may yield device-independent certification given an entangled state.

2.4 Our contribution

– In Sect. 3, we note that the test for device independence should be applied on a slightly modified state than the state being used as in [4]. This provides a much better probability compared to that has been achieved in [4], with the expense of one additional CNOT gate only. In fact, this shows that how even without considering the maximally entangled state, one can simulate the CHSH game like behavior by changing the measurement basis in one MD.
– In Sect. 4, we exploit the three-party pseudo- telepathy game for a transformed three-qubit non-maximally entangled state and show how it provides even better probability.

3 Analysis of CHSH game with modified two-qubit entangled states

In this section, we analyze case-by-case situation of the CHSH test for a modified two-qubit entangled state of the form

$$\frac{1}{\sqrt{2}}\left(\cos\frac{\theta}{2}|00\rangle + \sin\frac{\theta}{2}|01\rangle + \cos\frac{\theta}{2}|11\rangle - \sin\frac{\theta}{2}|10\rangle\right) \tag{4}$$

The motivation here is as follows. In the QPQ protocol [7], generally the client learns only a few bits of the shared secret key, while the server learns it all. This is done by certain modification of a quantum key distribution protocol. The entangled state of Eq. (3), used in [7], could provide expected $\frac{1}{2}\sin^2\theta$ proportion of shared secret key bits to the client. Generally, the client will try to learn only a few bits, and thus, the value of θ will be very small. The method presented in [4] requires lower probability (more samples) for small θ. We show that with proper choice of the entangled state this can be improved a lot. In fact, one may keep the DI-QPQ protocol [4] exactly the same, but use our strategy only for testing DI.

3.1 Success probability calculation

In this case, Bob performs CNOT operation over the original two- qubit state shared in DI-QPQ protocol [4] by considering the first qubit of the state as a control bit and second qubit as a target bit. The resulting state after performing this operation will be of the form as mentioned in Eq. 4. We have already mentioned the details of the game in Sect. 2.1.

1. **For input** $xy = 00$: Bob's first quantum device measures the first qubit of the modified state in $\{|0\rangle, |1\rangle\}$ basis, and the second quantum device measures the second qubit of the modified state in $\{|\psi_1\rangle, |\psi_1^{\perp}\rangle\}$ basis. In this case, the probability of obtaining each of 00 and 11 from the two quantum devices (as output) is $\frac{1}{2}\cos^2(\frac{\theta-\psi_1}{2})$ and $\frac{1}{2}\cos^2(\frac{\theta-\psi_1}{2})$, respectively. So, the total winning probability in this case is $\cos^2(\frac{\theta-\psi_1}{2})$.
2. **For input** $xy = 01$: Bob's first quantum device measures the first qubit of the modified state in $\{|0\rangle, |1\rangle\}$ basis, and the second quantum device measures the second qubit of the modified state in $\{|\psi_2\rangle, |\psi_2^{\perp}\rangle\}$ basis. In this case, the probability of obtaining each of 00 and 11 from the two quantum devices (as output) is $\frac{1}{2}\cos^2(\frac{\theta-\psi_2}{2})$ and $\frac{1}{2}\cos^2(\frac{\theta-\psi_2}{2})$, respectively. So, the total winning probability in this case is $\cos^2(\frac{\theta-\psi_2}{2})$.
3. **For input** $xy = 10$: Bob's first quantum device measures the first qubit of the modified state in $\{|+\rangle, |-\rangle\}$ basis, and the second quantum device measures the second qubit of the modified state in $\{|\psi_1\rangle, |\psi_1^{\perp}\rangle\}$ basis. In this case, the probability of obtaining each of 00 and 11 from the two quantum devices (as output) is $\frac{1}{4}[\cos(\frac{\theta-\psi_1}{2}) - \sin(\frac{\theta-\psi_1}{2})]^2$ and $\frac{1}{4}[\cos(\frac{\theta-\psi_1}{2}) - \sin(\frac{\theta-\psi_1}{2})]^2$, respectively. So, the total winning probability in this case is $\frac{1}{2}[\cos(\frac{\theta-\psi_1}{2}) - \sin(\frac{\theta-\psi_1}{2})]^2$.
4. **For input** $xy = 11$: Bob's first quantum device measures the first qubit of the modified state in $\{|+\rangle, |-\rangle\}$ basis, and the second quantum device measures the second qubit of the modified state in $\{|\psi_2\rangle, |\psi_2^{\perp}\rangle\}$ basis. In this case, the probability of obtaining each of 01 and 10 from the two quantum devices (as output) is $\frac{1}{4}[\cos(\frac{\theta-\psi_2}{2}) + \sin(\frac{\theta-\psi_2}{2})]^2$ and $\frac{1}{4}[\cos(\frac{\theta-\psi_2}{2}) + \sin(\frac{\theta-\psi_2}{2})]^2$, respectively. So, the total winning probability in this case is $\frac{1}{2}[\cos(\frac{\theta-\psi_2}{2}) + \sin(\frac{\theta-\psi_2}{2})]^2$.

As all the cases can happen with equal probability (for random choice of inputs), the overall probability of winning the CHSH game with this modified two-qubit entangled state is

$$\frac{1}{2} + \frac{1}{8}[\cos(\theta - \psi_1) + \cos(\theta - \psi_2) - \sin(\theta - \psi_1) + \sin(\theta - \psi_2)].$$

3.2 Appropriate choice of measurement basis

From the discussion of the previous subsection, we can see that for the modified two-qubit entangled state, Bob gets the success probability in terms of θ, ψ_1 and ψ_2 which is equal to $\frac{1}{2}+\frac{1}{8}[\cos(\theta-\psi_1)+\cos(\theta-\psi_2)-\sin(\theta-\psi_1)+\sin(\theta-\psi_2)]$. To maximize the quantity, we have to maximize $\cos(\theta-\psi_1)+\cos(\theta-\psi_2)-\sin(\theta-\psi_1)+\sin(\theta-\psi_2)$.

Now, we can write,

$$[\cos(\theta - \psi_1) - \sin(\theta - \psi_1)] + [\cos(\theta - \psi_2) + \sin(\theta - \psi_2)]$$

Setting $\theta - \psi_1 = A$, $\theta - \psi_2 = B$, $1 = r_1 \sin\phi_1 = r_1 \cos\phi_1$ (for the first half of the expression) and $1 = r_2 \sin\phi_2 = r_2 \cos\phi_2$ (for the second half of the expression), we get

$$\begin{aligned}&(r_1 \sin\phi_1 \cos A - r_1 \cos\phi_1 \sin A)\\ &\quad +(r_2 \sin\phi_2 \cos B + r_2 \cos\phi_2 \sin B)\\ &= r_1 \sin(\phi_1 - A) + r_2 \sin(\phi_2 + B),\end{aligned}$$

where $r_1^2 = r_2^2 = 2$ and $\tan\phi_1 = \tan\phi_2 = 1$, i.e, $\phi_1 = \phi_2 = \tan^{-1}(1) = \frac{\pi}{4}$.

Again, the value $r_1 \sin(\phi_1 - A) + r_2 \sin(\phi_2 + B)$ will be maximum when both $\sin(\phi_1 - A) = 1$ and $\sin(\phi_2 + B) = 1$, i.e., when $(\phi_1 - A) = \frac{\pi}{2}$ and $(\phi_2 + B) = \frac{\pi}{2}$. From that, after putting the value of A and B we get, $\psi_1 = (\frac{\pi}{4} + \theta)$ and $\psi_2 = (\theta - \frac{\pi}{4})$.

From the discussion, it is clear that the optimal value of $|\psi_1\rangle$ and $|\psi_2\rangle$ corresponding to a particular θ will be $\psi_1 = (\frac{\pi}{4} + \theta)$ and $\psi_2 = (\theta - \frac{\pi}{4})$. So, the success probability corresponding to each theta will be maximum for this particular choice of measurement basis. By putting this value into the success probability expression of the modified state (as derived in previous subsection), we can see that for this particular choice of measurement basis, the success probability value of CHSH game with this modified state for different values of θ is constant and this success probability value is the maximum success probability that we can get for two-qubit entangled states in CHSH game. This is indeed natural as we are making local transformation at one side and then accordingly modifying the measurement basis.

We like to refer that this success probability is significantly greater than what could be obtained in [4] for $\theta \leqslant \frac{\pi}{2}$ that is presented in Fig. 2.

4 Analysis of three-party quantum pseudo-telepathy with transformed three-qubit entangled states

In this section, we analyze case-by-case situation of the proposed multiparty pseudo-telepathy (parity) test for a three-qubit entangled states of the form

$$\frac{1}{\sqrt{2}}\left(\cos\frac{\theta}{2}|000\rangle + \sin\frac{\theta}{2}|010\rangle + \cos\frac{\theta}{2}|111\rangle - \sin\frac{\theta}{2}|100\rangle\right).$$

We have already mentioned the details of the game in Sect. 2.1.

1. **For input** $x_1x_2x_3 = 000$: The quantum devices perform Hadamard operation over individual qubits and measure each qubit in $\{|0\rangle, |1\rangle\}$ basis. In this case, probability of obtaining each of 000, 110, 011, 101 from the three quantum devices (as output) is $\frac{1}{4}\cos^2(\frac{\theta}{2})$, $\frac{1}{4}\cos^2(\frac{\theta}{2})$, $\frac{1}{4}(\cos\frac{\theta}{2} - \sin\frac{\theta}{2})^2$ and $\frac{1}{4}(\cos\frac{\theta}{2} + \sin\frac{\theta}{2})^2$, respectively. So, the total winning probability in this case is $\frac{1}{4}(3 + \cos\theta)$.
2. **For input** $x_1x_2x_3 = 110$: Each of the first two quantum devices perform the unitary operator S (as described in [22]) over the first two particles. Then, all the devices perform Hadamard operation over the individual qubits and measure each qubit in $\{|0\rangle, |1\rangle\}$ basis. In this case, probability of getting each of 100, 010, 001, 111 from the three quantum devices (as output) is $\frac{1}{4}$, $\frac{1}{4}$, $\frac{1}{4}\cos^2(\frac{\theta}{2})$ and $\frac{1}{4}\cos^2(\frac{\theta}{2})$, respectively. Thus, the total winning probability in this case becomes $\frac{1}{4}(3+\cos\theta)$.
3. **For input** $x_1x_2x_3 = 011$: The devices first perform S over the last two qubits, and then, all the devices apply Hadamard operation over the individual qubits and then measure each qubit in $\{|0\rangle, |1\rangle\}$ basis. In this case, probability of getting each of 100, 010, 001, 111 from the three quantum devices (as output) is $\frac{1}{16}[3 + \cos\theta + 2\sin\theta]$, $\frac{1}{16}[3+\cos\theta-2\sin\theta]$, $\frac{1}{16}[3+\cos\theta-2\sin\theta]$ and $\frac{1}{16}[3+\cos\theta+2\sin\theta]$, respectively. Hence, here we obtain the total winning probability as $\frac{1}{4}(3 + \cos\theta)$.
4. **For input** $x_1x_2x_3 = 101$: The devices first perform S over the first and third qubits, and then, all the devices perform Hadamard operation over individual qubits and measure each qubit in $\{|0\rangle, |1\rangle\}$ basis. In this case, probability of getting each of 100, 010, 001, 111 from the three quantum devices (as output) is $\frac{1}{16}[3 + \cos\theta + 2\sin\theta]$, $\frac{1}{16}[3+\cos\theta-2\sin\theta]$, $\frac{1}{16}[3+\cos\theta+2\sin\theta]$ and $\frac{1}{16}[3+\cos\theta-2\sin\theta]$, respectively. Thus, the winning probability becomes $\frac{1}{4}(3 + \cos\theta)$.

As all the cases can happen with equal probability (for random choice of inputs from the set {000, 110, 011, 101}), the overall probability of winning the multiparty pseudo-telepathy game with this specified form of three-qubit entangled state is

$$4 \times \frac{1}{4} \times \frac{1}{4}(3 + \cos\theta) = \frac{1}{4}(3 + \cos\theta)$$

which is equal to 1 (i.e., maximum) when $\theta = 0$, i.e., the success probability will be maximum for three-qubit maximally entangled (GHZ) states. We like to refer that this success probability is greater than what could be obtained in [4] for certain ranges of θ that is presented in Fig. 2.

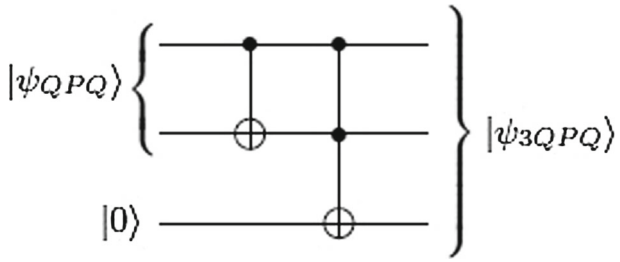

Fig. 1 Circuit diagram for transformed state

4.1 Transformation of two-qubit state into three qubit

In the DI-QPQ [4] setup, Bob holds the initial two-qubit entangled state and say that it can perform either local CHSH test or local parity test before proceeding for the actual QPQ protocol. When Bob performs the local parity test, he has to first transform the initial two-qubit entangled state $|\psi_{\text{QPQ}}\rangle$ into three-qubit entangled state $|\psi_{3\text{QPQ}}\rangle$ as follows:

- Bob first performs the CNOT operation over the initial two-qubit entangled state by considering first qubit as a control bit and second qubit as a target bit.
- After performing the CNOT operation, Bob will add an ancilla qubit $|0\rangle$ in his end and perform Toffoli operation by considering the two qubits of the modified entangled state as control bit and the ancilla qubit as a target bit.
- After performing these operations, the resulting state will be of the form

$$\frac{1}{\sqrt{2}}\left(\cos\frac{\theta}{2}|000\rangle + \sin\frac{\theta}{2}|010\rangle + \cos\frac{\theta}{2}|111\rangle - \sin\frac{\theta}{2}|100\rangle\right)$$

  The circuit diagram corresponding to this transformation is shown in Fig. 1.
- Bob will perform multiparty pseudo-telepathy (parity) game [22] with this transformed state.

Now the success probability of the parity game with this transformed three-qubit state will be $\frac{1}{4}(3+\cos\theta)$ which equals 1 for $\theta = 0$.

4.2 Comparative study

Let us consider the actual two-qubit entangled state shared in QPQ protocol which is of the form $\frac{1}{\sqrt{2}}(\cos\frac{\theta}{2}|00\rangle + \sin\frac{\theta}{2}|01\rangle + \cos\frac{\theta}{2}|10\rangle - \sin\frac{\theta}{2}|11\rangle)$, then the success probability of CHSH game (maximum success probability corresponding to each θ) for this state equals to $\frac{1}{8}(\sin\theta(\sin\psi_1 + \sin\psi_2) + \cos\psi_1 - \cos\psi_2) + \frac{1}{2}$ where $\psi_1 = (\frac{\pi}{2} - \tan^{-1}(\text{cosec}\,\theta))$ and $\psi_2 = (\frac{\pi}{2} + \tan^{-1}(\text{cosec}\,\theta))$.

Instead of the actual state, if we consider the modified two-qubit entangled state of the form $\frac{1}{\sqrt{2}}(\cos\frac{\theta}{2}|00\rangle + \sin\frac{\theta}{2}|01\rangle + \cos\frac{\theta}{2}|11\rangle - \sin\frac{\theta}{2}|10\rangle)$, then according to the discussion in Sect. 3, the success probability of CHSH game (maximum success

probability corresponding to each θ) for this state equals to $\frac{1}{2}+\frac{1}{8}[\cos(\theta-\psi_1)+\cos(\theta-\psi_2)-\sin(\theta-\psi_1)+\sin(\theta-\psi_2)]$ where $\psi_1=(\theta+\frac{\pi}{4})$ and $\psi_2=(\theta-\frac{\pi}{4})$. With this particular choice of basis, the actual success probability is further improved and it provides the same result as obtained in the CHSH game with maximally entangled state.

Further, if we consider the transformed three-qubit entangled state of the form $\frac{1}{\sqrt{2}}(\cos\frac{\theta}{2}|000\rangle+\sin\frac{\theta}{2}|010\rangle+\cos\frac{\theta}{2}|111\rangle-\sin\frac{\theta}{2}|100\rangle)$, then according to the discussion in Sect. 4, the success probability of parity game for this state equals to $\frac{1}{4}(3+\cos\theta)$

The comparative study between the success probability values of two games (for different form of states) corresponding to different values of θ from 0 to $\frac{\pi}{2}$ is shown in Fig. 2.

From the graph, it is clear that for CHSH game, the value of success probability varies between 0.75 and $\cos^2\frac{\pi}{8}$ for the actual state shared in QPQ protocol and the success probability of the two-qubit modified entangled state (as discussed in Sect. 4) remains constant, i.e., $\cos^2\frac{\pi}{8}$ irrespective of the value of θ. For the parity game, the value of the success probability for the transformed three-qubit entangled state (as discussed in Sect. 4) varies between 1 to 0.75. From the graph (as well as from calculation), it is clear that at $\theta\approx 1.14$, the success probability of parity game and the success probability of CHSH game for the modified two-qubit state becomes equal. Thus, for all the values of $\theta<1.14$, the success probability of parity game for transformed three-qubit state is higher compared to the success probability of CHSH game for the modified two-qubit state. On the other hand, for $\theta\geq 1.14$, the success probability of CHSH game for modified two-qubit state is higher compared to the success probability of parity game for transformed three-qubit state.

Similarly, for the value of $\theta\approx 1.2$, the success probability of parity game and the success probability of CHSH game for the actual two-qubit state becomes equal, and beyond that point, the success probability of CHSH game for actual two-qubit state

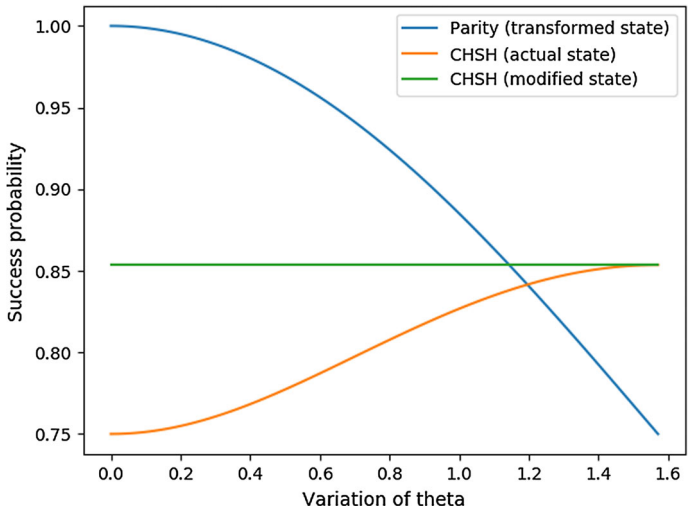

Fig. 2 Comparative study of success probabilities between CHSH and parity game for DI-QPQ protocol

is higher compared to the success probability of parity game for transformed three-qubit state. However, the success probability value of CHSH game for the modified two-qubit state is always higher as compared to the success probability value for the actual two- qubit state and the two becomes equal for $\theta = 1.57$.

In case we are interested for small values of θ, the parity game as in Sect. 4 will be the best suited for testing DI. Thus, [4, Algorithm 1] should be parameterized based on the value of θ. Further parity game does not require modifying the measurement bases as it is required for the CHSH test as described in Sect. 3.

4.3 Toward security analysis for finite samples

As we consider finite number of samples in our modified testing mechanism, in testing phase, we need to check whether the success probability value lies within the interval $\left[p_{\text{QPQ}} - \epsilon p_{\text{QPQ}}, p_{\text{QPQ}} + \epsilon p_{\text{QPQ}}\right]$, where p_{QPQ} is the intended success probability corresponding to a particular form of state (i.e., for a particular value of θ) and ϵ is the accuracy parameter chosen by the server (Bob). When the states successfully pass this test, Bob proceeds further for the actual QPQ protocol; otherwise, he aborts.

In [4], the authors outlined an attack strategy over the QPQ protocol where they have shown that if there is ϵ_A amount of bias in the choice of measurement basis by the client (i.e., Alice), then she can extract $(\frac{1}{2} + 2\epsilon_A^2)\sin^2\theta$ fraction of entire key stream, where the amount of extra information leaked is $2\epsilon_A^2 \sin^2\theta$. Toward resisting such leakage (which arises due to the finite sample size), Bob must bound the value of ϵ_A so that the additional information which is leaked to Alice should be infinitesimally small. In this direction, one may quantify the security of a protocol in the following manner.

The additional information leaked to the adversary (client) for our optimal sample protocol due to the biased choice of the client's measurement basis will be proportional to the value of ϵ, where ϵ is the accuracy parameter chosen by the server. This can be justified as follows. Let, instead of the correct states, Bob is provided with the states of the form $(\alpha|0\rangle_B|\phi_0\rangle_A + \beta|1\rangle_B|\phi_1\rangle_A)$ where $|\alpha|^2 = (\frac{1}{2} + \epsilon_A)$ and $|\beta|^2 = (\frac{1}{2} - \epsilon_A)$.

When Bob performs the CHSH test, the success probability for the modified states becomes $p' = \frac{1}{2} + \frac{1}{8}\sin\theta(\sin\psi_1 + \sin\psi_2) + \frac{1}{4}\sqrt{\frac{1}{4} - \epsilon_A^2}(\cos\psi_1 - \cos\psi_2) + \frac{1}{4}\epsilon_A\cos\theta(\cos\psi_1 + \cos\psi_2)$. Now p' must lie within the interval $[p_{\text{QPQ}} - \epsilon p_{\text{QPQ}}, p_{\text{QPQ}} + \epsilon p_{\text{QPQ}}]$, where p_{QPQ} is the intended success probability of the modified state and ϵ is the accuracy parameter chosen by Bob.

Thus from the lower and upper bounds, we get $\epsilon_A^2 \geq -\frac{2\epsilon p_{\text{QPQ}}}{\cos\psi_1}$ and $\epsilon_A^2 \leq \frac{2\epsilon p_{\text{QPQ}}}{\cos\psi_1}$, respectively. Since negative ϵ_A is not meaningful, we have the solution as

$$\epsilon_A \leq \sqrt{\frac{2\epsilon p_{\text{QPQ}}}{\cos\psi_1}}. \tag{5}$$

Thus, to deceive Bob, the states should be prepared in such a way that the value of ϵ_A must satisfy the condition $\epsilon_A \leq \sqrt{\frac{2\epsilon p_{\text{QPQ}}}{\cos\psi_1}}$. Otherwise, the value of p' will not lie within

the specified interval and Bob has to abort the protocol. As for a given θ, the values of p_{QPQ}, ψ_1 and ψ_2 are constant, we can write $\epsilon_A \leq k\sqrt{\epsilon}$, where k is a constant.

Similarly, for the given erroneous state $(\alpha|0\rangle_B|\phi_0\rangle_A + \beta|1\rangle_B|\phi_1\rangle_A)$, when Bob performs the parity test, the success probability of parity test for the transformed states becomes $p'' = \frac{1}{4}[1 + \cos\theta + 2\sqrt{\frac{1}{4} - \epsilon_A^2}(1 + \cos\theta)]$. This value of p'' must lie within the interval $[p_{\mathrm{QPQ}} - \epsilon p_{\mathrm{QPQ}}, p_{\mathrm{QPQ}} + \epsilon p_{\mathrm{QPQ}}]$, where p_{QPQ} is the intended success probability of the transformed state.

Now from the left and right inequalities, we get $\epsilon_A^2 \geq -\epsilon$ and $\epsilon_A^2 \leq \epsilon$, respectively. Since negative ϵ_A is not meaningful, we have the solution as

$$\epsilon_A \leq \sqrt{\epsilon}. \tag{6}$$

Analyzing both the relation between ϵ_A and ϵ for CHSH test and parity test in Eqs. (5) and (6), respectively, one may conclude that the maximum value of ϵ_A is related to the square root of the value of chosen accuracy parameter (i.e., ϵ). From the discussion in [4], the additional information leaked to Alice equals to $2\epsilon_A^2 \sin^2\theta$. As the value of ϵ_A is proportional with the square root of the chosen accuracy parameter ϵ, the maximum information leaked to Alice will be proportional with the value of the chosen accuracy parameter ϵ.

5 Discussion and conclusion

In this work, we propose several strategies to improve the test of device independence in the device-independent quantum private query Protocol. Our motivation comes from the analysis in finite sample scenario, which is mandatory for actual implementation of the protocol. We derive the relation between the required sample size and corresponding success probability and propose optimal testing mechanisms for DI-QPQ protocol. CHSH tests on different versions of the entangled states are studied. Further, we also consider the three-party pseudo-telepathy as a tool for testing DI and show that it provides significantly better results for practical purposes.

Acknowledgements The authors like to acknowledge the reviewers for their detailed comments that substantially improved the technical as well as editorial quality of this paper. The second author likes to acknowledge the grant from the project "Cryptography & Cryptanalysis: How far can we bridge the gap between Classical and Quantum Paradigm," awarded by the Scientific Research Council of the Department of Atomic Energy (DAE-SRC), the Board of Research in Nuclear Sciences (BRNS).

References

1. Mayers, D., Yao, A.: Self testing quantum apparatus. Quantum Inf. Comput. **4**(4), 273–286 (2004)
2. Cirel'son, B.S.: Quantum generalizations of Bell's inequality. Lett. Math. Phys. **4**(2), 93–100 (1980)
3. Clauser, J.F., Horne, M.A., Shimony, A., Holt, R.A.: Proposed experiment to test local hidden-variable theories. Phys. Rev. Lett. **23**, 880–884 (1969)
4. Maitra, A., Paul, G., Roy, S.: Device-independent quantum private query. Phys. Rev. A **95**, 042344 (2017)
5. Aharon, N., Massar, S., Pironio, S., Silman, J.: Device-independent bit commitment based on the CHSH inequality. New J. Phys. **18**(2), 025014 (2016)

6. Gisin, N., Pironio, S., Sangouard, N.: Proposal for implementing device-independent quantum key distribution based on a heralded qubit amplifier. Phys. Rev. Lett. **105**, 070501 (2010)
7. Yang, Y.G., Sun, S.J., Xu, P., Tiang, J.: Flexible protocol for quantum private query based on B92 protocol. Quantum Inf. Process **13**, 805–813 (2014)
8. Brassard, G., Broadbent, A., Tapp, A.: Quantum pseudo-telepathy. Found. Phys. **35**(11), 1877–1907 (2005)
9. Ekert, A.K.: Quantum cryptography based on Bell's theorem. Phys. Rev. Lett. **67**, 661 (1991)
10. Bennett, C.H., Brassard, G., Mermin, N.D.: Quantum cryptography without Bell's theorem. Phys. Rev. Lett. **68**, 557 (1992)
11. Bennett, C.H., Brassard, G., Popescu, S., Schumacher, B., Smolin, J.A., Wootters, W.K.: Purification of noisy entanglement and faithful teleportation via noisy channels. Phys. Rev. Lett. **76**, 722 (1996)
12. Long, G.L., Liu, X.S.: Theoretically efficient high-capacity quantum-key-distribution scheme. Phys. Rev. A **65**, 032302 (2002)
13. Deng, F.G., Long, G.L., Liu, X.S.: Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. Phys. Rev. A **68**, 042317 (2003)
14. Ren, B.C., Du, F.F., Deng, F.G.: Hyper-entanglement concentration for two-photon four-qubit systems with linear optics. Phys. Rev. A **88**, 012302 (2013)
15. Long, G.L., Xiao, L.: Parallel quantum computing in a single ensemble quantum computer. Phys. Rev. A **69**, 052303 (2004)
16. Feng, G.R., Xu, G.F., Long, G.L.: Experimental realization of non-adiabatic holonomic quantum computation. Phys. Rev. Lett. **110**, 190501 (2013)
17. Wei, H.R., Deng, F.G.: Universal quantum gates for hybrid systems assisted by quantum dots inside double-sided optical micro-cavities. Phys. Rev. A **87**, 022305 (2013)
18. Li, Z., Long, L.R., Zhou, P., Yin, C.L.: Probabilistic multiparty-controlled teleportation of an arbitrary m-qubit state with a pure entangled quantum channel against collective noise. Sci. China Ser. G Phys. Mech. Astron. **55**, 2445–2451 (2012)
19. Long, L.R., Li, H.W., Zhou, P., Fan, C., Yin, C.L.: Multiparty-controlled teleportation of an arbitrary GHZ-class state by using a d-dimensional $(N + 2)$-particle non-maximally entangled state as the quantum channel. Sci. China Ser. G Phys. Mech. Astron. **54**, 484–490 (2011)
20. Lv, S.X., Zhao, Z.W., Zhou, P.: Joint remote control of an arbitrary single-qubit state by using a multi-particle entangled state as the quantum channel. Quantum Inf. Process. **17**, 8 (2018)
21. Yu, R.F., Lin, Y.J., Zhou, P.: Joint remote preparation of arbitrary two- and three-photon state with linear-optical elements. Quantum Inf. Process. **15**, 4785 (2016)
22. Brassard, G., Broadbent, A., Tapp, A.: Multi-party pseudo-telepathy. Springer, Berlin (2003)
23. Hoeffding, W.: Probability Inequalities for sums of bounded random variables. J Am Stat Assoc **58**(301), 13–30 (1963)
24. Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. In: Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, pp. 10–12 (1984)
25. Mancinska, L.: Maximally entangled state in pseudo-telepathy games. In: Calude, C.S., Freivalds, R., Iwama, K. (eds.) Computing with new resources. Lecture Notes in Computer Science, vol. **8808**, pp. 200–207 (2014)