Device-independent quantum private query

Arpita Maitra,[1,*] Goutam Paul,[2,†] and Sarbani Roy[3,‡]
[1] *Indian Institute of Management Calcutta, Kolkata 700104, West Bengal, India*
[2] *Indian Statistical Institute, Kolkata 700108, West Bengal, India*
[3] *Indian Institute of Technology Kharagpur, Kharagpur 721302, West Bengal, India*

(Received 9 January 2017; published 28 April 2017)

In quantum private query (QPQ), a client obtains values corresponding to his or her query only, and nothing else from the server, and the server does not get any information about the queries. V. Giovannetti *et al.* [Phys. Rev. Lett. **100**, 230502 (2008)] gave the first QPQ protocol and since then quite a few variants and extensions have been proposed. However, none of the existing protocols are device independent; i.e., all of them assume implicitly that the entangled states supplied to the client and the server are of a certain form. In this work, we exploit the idea of a local CHSH game and connect it with the scheme of Y. G. Yang *et al.* [Quantum Info. Process. **13**, 805 (2014)] to present the concept of a device-independent QPQ protocol.

DOI: 10.1103/PhysRevA.95.042344

I. INTRODUCTION

During the last two decades, the quantum key distribution (QKD) has remained the main theme of quantum cryptography. In recent times, however, several other quantum cryptographic primitives are being explored and quantum private query (QPQ) is one of them. In QPQ, a client issues queries to a database and obtains the real values without knowing anything else about the database, whereas the server should not gain any information about the queries. Here, we assume that Bob is the database holder or server and Alice is the client. The first protocol in this domain had been proposed by Giovannetti *et al.* in [1], followed by [2] and [3]. However, this scheme is highly theoretical and difficult to implement. For implementation purposes, Jakobi *et al.* [4] came out with a QPQ protocol which was based on the SARG04 QKD protocol [5]. In 2012, Gao *et al.* [6] proposed a flexible generalization of [4]. Rao *et al.* [7] suggested two more efficient modifications of classical postprocessing in the protocol of Jakobi *et al.* In 2013, Zhang *et al.* [8] proposed a QPQ protocol based on a counterfactual QKD scheme [9]. In 2014, Yang *et al.* came out with a flexible QPQ protocol [10] which was based on the B92 QKD scheme [11]. This domain is gradually improving. This is evident from the large number of published articles [12–15] in the last 2 years.

The security of all these protocols is defined on the basis of the following facts:

(a) Bob knows the whole key which will be used for the encryption of the database.

(b) Alice knows a fraction of bits of the key.

(c) Bob does not get any information about the position of the bits which are known to Alice.

Thus, it is vary natural that in the QPQ protocol, there is no need for an outsider adversary. Unlike the QKD, here, one of the legitimate parties is playing the role of an adversary. Alice tries to extract more information about the raw key bits, whereas Bob tries to learn the position of the bits known to Alice.

We identify that the security of all the existing protocols is based on the fact that Bob relies on his devices, i.e., the source which supplies the qubits and the detectors which measure the qubits. Thus, similarly to the QKD protocols, the trustworthiness of the devices are implicit in the security proofs of the protocols. In the current work, we try to understand whether we can remove such trustworthiness in the devices as in the device-independent QKD (DI-QKD) [16–20].

In the DI-QKD, a statistical test known as the Bell test [21] or CHSH test [22] is performed to verify whether the shared entangled states between the legitimate parties are maximally entangled. If the states are maximally entangled, then the QKD protocol provides unconditional security. However, the test has to be performed nonlocally. In other words, two distant parties (Alice and Bob) have to be involved in the CHSH test.

Very recently, Lim *et al.* [23] proposed a DI-QKD scheme where they exploit the idea of the local CHSH test. In the local CHSH test, the sender performs the CHSH test at his or her end as a motivation towards certifying whether the states to be used for the QKD are maximally entangled.

In the case of QPQ, we identify that if the states shared between Bob and Alice are not in a certain form, then Alice can always apply some strategies which help her to extract more information about the raw key bits than what is suggested by the protocol. Thus, it is necessary for Bob to certify whether the states are in the desired form. Motivated by the idea of the local CHSH test of Lim *et al.* [23], we, here, propose a protocol which provides this certification. The value obtained from the test will depend upon Alice's predefined success probability of learning about the raw key bits: in other words, how much information about the key has to be allowed to Alice by the protocol.

Here, we work on the QPQ protocol presented by Yang *et al.* [10]. Note that this protocol [10] can be performed by a certain kind of mixed state also [namely, $(|0,\phi_0\rangle\langle 0,\phi_0| + |1,\phi_1\rangle\langle 1,\phi_1|)/2$]. Since we want to prove device-independence security by exploiting the idea of the local CHSH test, we work with the entanglement-based version. Further, our suggested scheme for testing device independence lies on top of the QPQ protocol, meaning that Bob performs the local CHSH game before starting the QPQ protocol presented in [10]. One can replace that QPQ part with

[*] arpita76b@gmail.com
[†] goutam.paul@isical.ac.in
[‡] sarbani16roy@gmail.com

any other entanglement-based QPQ protocol (which might not be performed by any mixed state) and our scheme will work there too.

The QPQ protocol can be viewed as a two-party (mistrustful) cryptography, i.e., two parties that want to perform a certain task together without fully trusting each other. In this regard, one may mention [24–28] that similar ideas have been exploited to propose imperfect coin flipping and bit commitment in the device-independent setting.

We first revisit the protocol of Yang *et al.* [10]. Next, we show how Alice could choose a strategy to extract more information about the raw key bits if the shared entanglement between her and Bob is not in the desired form. We, then, come out with the idea of a local CHSH-like test which is exploited to certify whether the states are secure for the QPQ protocol. All the lemmas and theorems used to prove the security of the proposed protocol are given in the Appendix.

II. REVISITING THE PROTOCOL IN [10]

In this section we revisit the protocol for quantum private query proposed in [10]. The protocol exploits the idea of the B92 quantum key distribution scheme. There are two phases in the protocol, namely, key generation and private query. In the key generation phase, 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 $|\phi_1\rangle_A = \cos(\frac{\theta}{2})|0\rangle - \sin(\frac{\theta}{2})|1\rangle$. Here, subscript B stands for Bob and subscript A stands for Alice. θ may vary from 0 to $\frac{\pi}{2}$. After receiving the qubits from Bob, Alice announces the position of the qubits that have ultimately reached her end. Bob discards the lost photons. After postselection, Bob measures his qubits in the $\{|0\rangle_B,|1\rangle_B\}$ basis, whereas Alice measures her qubits either in the $\{|\phi_0\rangle_A,|\phi_0^\perp\rangle_A\}$ basis or in the $\{|\phi_1\rangle_A,|\phi_1^\perp\rangle_A\}$ basis randomly. If Alice's measurement result gives $|\phi_0^\perp\rangle$, she concludes that the raw key bit at Bob's end must be 1. If it is $|\phi_1^\perp\rangle$, the raw key bit must be 0. Bob and Alice execute classical postprocessing so that Alice's information on the key reduces to one bit or more. Bob knows the whole key, whereas Alice generally knows several bits of the key.

In the private query phase, if Alice knows the jth bit of key K and wants to know the ith element of the database, she declares the integer $s = j - i$. Bob shifts K by s and hence gets a new key, say K_0. Bob encrypts his database by this new key K_0 with a one-time pad and sends the encrypted database to Alice. Alice decrypts the value with her jth key bit and gets the required element of the database.

The security of the protocol comes from the fact that Alice knows the final key partially. Thus, even if she gets access to the whole encrypted database, she cannot obtain the complete information about the database. Now, we calculate the success probability of Alice's guessing a bit in the raw key.

As Bob measures his qubits only in the $\{|0\rangle_B,|1\rangle_B\}$ basis, he will get either $|0\rangle$ with probability $\frac{1}{2}$ or $|1\rangle$ with probability $\frac{1}{2}$. When Bob gets $|0\rangle$, Alice should get $|\phi_0\rangle$. If she chooses the $\{|\phi_0\rangle_A,|\phi_0^\perp\rangle_A\}$ basis, she will get $|\phi_0\rangle$ with probability 1 and never get $|\phi_0^\perp\rangle$. However, if she chooses the $\{|\phi_1\rangle_A,|\phi_1^\perp\rangle_A\}$ basis, she will get either $|\phi_1\rangle$ with probability $\cos^2\theta$ or $|\phi_1^\perp\rangle$ with probability $\sin^2\theta$. We formalize all the conditional probabilities in the following table.

	Alice's conditional probability			
	$A = \|\phi_0\rangle$	$A = \|\phi_0^\perp\rangle$	$A = \|\phi_1\rangle$	$A = \|\phi_1^\perp\rangle$
$B = 0$	$\frac{1}{2}\cdot 1$	$\frac{1}{2}\cdot 0$	$\frac{1}{2}\cdot\cos^2\theta$	$\frac{1}{2}\cdot\sin^2\theta$
$B = 1$	$\frac{1}{2}\cdot\cos^2\theta$	$\frac{1}{2}\cdot\sin^2\theta$	$\frac{1}{2}\cdot 1$	$\frac{1}{2}\cdot 0$

According to the protocol, when Alice gets $|\phi_0^\perp\rangle$, she outputs 1. And when she gets $|\phi_1^\perp\rangle$, she outputs 0. Thus, the success probability of Alice's guessing a bit in the raw key can be written as

$$\begin{aligned}\Pr(A = B) &= \Pr(A = 0, B = 0) + \Pr(A = 1, B = 1)\\ &= \Pr(B = 0)\cdot\Pr(A = 0|B = 0)\\ &\quad + \Pr(B = 1)\cdot\Pr(A = 1|B = 1)\\ &= \tfrac{1}{2}\cdot\Pr(A = \phi_1^\perp|B = 0)\\ &\quad + \tfrac{1}{2}\cdot\Pr(A = \phi_0^\perp|B = 1).\end{aligned} \tag{1}$$

From the above table, we can see that Alice's success probability becomes $\frac{\sin^2\theta}{2}$.

III. BIASED CHOICE OF ALICE'S BASIS

Suppose Bob trusts the source, i.e., he believes that the states shared between Alice and him are of a certain form [10]. Let the source supply some arbitrary entangled states $(\alpha|0\rangle_B|\phi_0\rangle_A + \beta|1\rangle_B|\phi_1\rangle_A)$, where $|\alpha|^2 = (\frac{1}{2}+\epsilon)$ and $|\beta|^2 = (\frac{1}{2}-\epsilon)$ to Bob. Suppose Alice has this information and also the information on the values of α and β. In this case, she chooses the basis as follows:

(a) $\{|\phi_0\rangle_A,|\phi_0^\perp\rangle_A\}$ with probability $\frac{1}{2}-\epsilon$;

(b) $\{|\phi_1\rangle_A,|\phi_1^\perp\rangle_A\}$ with probability $\frac{1}{2}+\epsilon$.

Her success probability can be calculated from the following table.

	Alice's conditional probability			
	$A = \|\phi_0\rangle$	$A = \|\phi_0^\perp\rangle$	$A = \|\phi_1\rangle$	$A = \|\phi_1^\perp\rangle$
$B = 0$	$1\cdot(\frac{1}{2}-\epsilon)$	0	$(\cos^2\theta)\cdot(\frac{1}{2}+\epsilon)$	$(\sin^2\theta)\cdot(\frac{1}{2}+\epsilon)$
$B = 1$	$(\cos^2\theta)\cdot(\frac{1}{2}-\epsilon)$	$(\sin^2\theta)\cdot(\frac{1}{2}-\epsilon)$	$1\cdot(\frac{1}{2}+\epsilon)$	0

Following Eq. (1), it becomes $(\frac{1}{2}+2\epsilon^2)\sin^2\theta$.

Thus, if Alice and Bob do not share the entangled states of the certain kind, then Alice can always extract more information about the raw key bit following the suggested strategy. The bias in the bases of Alice depends on the values of α and β. For example, if $\alpha = \frac{1}{2}-\epsilon$ and $\beta = \frac{1}{2}+\epsilon$, then Alice chooses $\{|\phi_0\rangle_A,|\phi_0^\perp\rangle_A\}$ with probability $\frac{1}{2}+\epsilon$ and chooses $\{|\phi_1\rangle_A,|\phi_1^\perp\rangle_A\}$ with probability $\frac{1}{2}-\epsilon$.

To mitigate this problem, Bob has to remove his trust in the devices and has to perform some local test at his end to become sure that the states shared between them are of the specific form [10]. As we consider the entanglement version of the QPQ protocol, we suggest a local statistical test which is actually the CHSH test performed locally. The difference is that, for this test, we do not require the perfect CHSH value. The value depends on the value of θ.

However, when the states are of the form given in [10], then the above strategy does not help Alice to extract more information about the raw key bit. Let Bob and Alice share the entangled states of the specific form and Alice choose her measurement bases $\{|\phi_0\rangle_A,|\phi_0^\perp\rangle_A\}$ and $\{|\phi_1\rangle_A,|\phi_1^\perp\rangle_A\}$ with probability $\frac{1}{2}-\epsilon$ and $\frac{1}{2}+\epsilon$, respectively. In this case, following Eq. (1), the success probability becomes $\frac{\sin^2\theta}{2}$.

Thus, it will be necessary for Bob to certify that these shared states are of the certain form. In the following section we propose a protocol which certifies this. Thus, Bob is no longer required to put trust in the source as well as the detectors. By performing a test which is almost like the CHSH test at his end, he first checks whether the states follow the desired property. Conditional on the success of the test, Bob proceeds to QPQ. Here, we consider detectors with unit efficiency. However, for practical implementation of the suggested protocol, one has to consider detectors with nonunit efficiency.

One may wonder why we have not chosen quantum-state tomography to check whether the states are of the certain form. The reason is that tomography would require an infinite number of states to achieve perfect accuracy. On the other hand, choosing a different avenue of the local CHSH game, we are able to analyze the security of our protocol for a finite number of states.

IV. OUR PROTOCOL AND THE LOCAL CHSH GAME

Before describing the proposed protocol, we first enumerate the assumptions required for the security of the protocol. These are summarized as follows:

(1) Devices are causally independent; i.e., each use of the device is independent of the previous use. This assumption implies that the devices are memoryless.

(2) Alice and Bob's laboratories are perfectly secured; i.e., no information is leaked from their laboratories.

(3) All the detectors at Bob's end have unit efficiency; i.e., he always gets conclusive outcomes.

Our protocol is described in Algorithm 1. For brevity, we write γn and $(1-\gamma)n$ instead of $\lceil \gamma n\rceil$ and $\lfloor (1-\gamma)n\rfloor$, respectively.

Algorithm 1: Our proposed protocol, Π.

1. Bob starts with n entangled states.
2. Bob divides the given entangled pairs into two sets. One is Γ_{CHSH} and the other is Γ_{QPQ}. The set Γ_{CHSH} contains γn entangled states, whereas Γ_{QPQ} contains $(1-\gamma)n$ entangled states for $0<\gamma<1$.
3. For rounds $i\in\{1,\dots,\gamma n\}$
   (a) Bob chooses $x_i\in\{0,1\}$ and $y_i\in\{0,1\}$ uniformly at random.
   (b) If $x_i=0$, he measures the first particle of the entangled state in the $\{|0\rangle,|1\rangle\}$ basis, and if $x_i=1$, he measures it in the $\{|+\rangle,|-\rangle\}$ basis.
   (c) Similarly, if $y_i=0$, Bob measures the second particle of the entangled state in the $\{|\psi_1\rangle,|\psi_1^\perp\rangle\}$ basis, and if $y_i=1$, he measures it in the $\{|\psi_2\rangle,|\psi_2^\perp\rangle\}$ basis.
   (d) The output is recorded as $a_i\in\{0,1\}$ ($b_i\in\{0,1\}$) for the first (second) particle. The encoding for $a_i(b_i)$ is as follows.
      (i) For the first particle in each pair, $a_i=0$ if the measurement result is $|0\rangle$ or $|+\rangle$, and $a_i=1$ if the result is $|1\rangle$ or $|-\rangle$.
      (ii) For the second particle in each pair, $b_i=0$ if the measurement result is $|\psi_1\rangle$ or $|\psi_2\rangle$, and $b_i=1$ if the measurement result is $|\psi_1^\perp\rangle$ or $|\psi_2^\perp\rangle$.
   (e) Testing: For the test round $i\in\Gamma_{\text{CHSH}}$, define
$$Y_i=\begin{cases}1 & \text{if } \; a_i\oplus b_i=x_i\wedge y_i,\\ 0 & \text{if } \; \text{otherwise.}\end{cases}$$
4. If $\frac{1}{\gamma n}\sum_i Y_i<\frac{1}{8}(\sin\theta(\sin\psi_1+\sin\psi_2)+\cos\psi_1-\cos\psi_2)+\frac{1}{2}$, Bob aborts the protocol.
5. Conditional on the event that the local CHSH test at Bob's end has been successful, Bob proceeds to the subset Γ_{QPQ} and sends one half of the remaining $(1-\gamma)n$ entangled pairs to Alice.
6. Alice performs the private query phase as in [10].

Note that we are dealing with several bases, namely, $\{\phi_0,\phi_0^\perp\}$, $\{\phi_1,\phi_1^\perp\}$, $\{\psi_1,\psi_1^\perp\}$, and $\{\psi_2,\psi_2^\perp\}$. It should be clarified that where the $\{\phi_0,\phi_0^\perp\}$ and $\{\phi_1,\phi_1^\perp\}$ bases are chosen by Alice for the QPQ protocol, and the $\{\psi_1,\psi_1^\perp\}$ and $\{\psi_2,\psi_2^\perp\}$ bases are chosen by Bob to perform the local CHSH test. Here, we consider $|\psi_1\rangle=\cos\frac{\psi_1}{2}|0\rangle+\sin\frac{\psi_1}{2}|1\rangle$ and $|\psi_2\rangle=\cos\frac{\psi_2}{2}|0\rangle+\sin\frac{\psi_2}{2}|1\rangle$.

In the QPQ protocol in [10], Bob measures his particles in the $\{|0\rangle,|1\rangle\}$ basis only. Hence, the protocol can be performed by the mixed states also. One may think that for the local CHSH game here, it is sufficient to measure Bob's first particle in the $\{|0\rangle,|1\rangle\}$ basis only as Bob does not need to test the coherence (purity) of the states. However, note that our proposal for the local CHSH game lies on top of the QPQ protocol [10]. In other words, Bob performs the local CHSH test followed by the QPQ protocol presented in [10]. One can replace the QPQ part with any other entanglement-based QPQ protocol which might not be performed by mixed states. Hence, it is necessary to use the $\{|+\rangle,|-\rangle\}$ basis in the proposed CHSH test.

Next, we analyze case by case situation for the proposed CHSH-like test. Let Bob obtained the entangled states of the form $\frac{1}{\sqrt{2}}(|0\rangle_B|\phi_0\rangle_A+|1\rangle_B|\phi_1\rangle_A)$. We calculate the conditional probabilities for each case and list them in Table I.

Since $\Pr(x_i,y_i)=\frac{1}{4}$ for all x_i and y_i, multiplying each individual probability in Table I by $\frac{1}{4}$ gives the corresponding joint probabilities. We have

$$\begin{aligned}
&\Pr(a_i\oplus b_i=x_i\wedge y_i)\\
&\quad=\Pr((x_i,y_i)=(0,0)\quad\text{and}\quad((a_i,b_i)=(0,0)\text{ or }(1,1)))\\
&\qquad+\Pr((x_i,y_i)=(0,1)\quad\text{and}\quad((a_i,b_i)=(0,0)\text{ or }(1,1)))\\
&\qquad+\Pr((x_i,y_i)=(1,0)\quad\text{and}\quad((a_i,b_i)=(0,0)\text{ or }(1,1)))\\
&\qquad+\Pr((x_i,y_i)=(1,1)\quad\text{and}\quad((a_i,b_i)=(0,1)\text{ or }(1,0))).
\end{aligned}$$

TABLE I. Conditional probability of (a_i,b_i) given (x_i,y_i).

(x_i,y_i)	(a_i,b_i)	$\Pr((a_i,b_i)\mid(x_i,y_i))$
(0, 0)	(0, 0)	$\frac{1}{2}\cos^2(\frac{\theta-\psi_1}{2})$
	(0, 1)	$\frac{1}{2}\sin^2(\frac{\theta-\psi_1}{2})$
	(1, 0)	$\frac{1}{2}\cos^2(\frac{\theta+\psi_1}{2})$
	(1, 1)	$\frac{1}{2}\sin^2(\frac{\theta+\psi_1}{2})$
(0, 1)	(0, 0)	$\frac{1}{2}\cos^2(\frac{\theta-\psi_2}{2})$
	(0, 1)	$\frac{1}{2}\sin^2(\frac{\theta-\psi_2}{2})$
	(1, 0)	$\frac{1}{2}\cos^2(\frac{\theta+\psi_2}{2})$
	(1, 1)	$\frac{1}{2}\sin^2(\frac{\theta+\psi_2}{2})$
(1, 0)	(0, 0)	$\cos^2(\frac{\theta}{2})\cos^2\frac{\psi_1}{2}$
	(0, 1)	$\cos^2(\frac{\theta}{2})\sin^2\frac{\psi_1}{2}$
	(1, 0)	$\sin^2(\frac{\theta}{2})\sin^2\frac{\psi_1}{2}$
	(1, 1)	$\sin^2(\frac{\theta}{2})\cos^2\frac{\psi_1}{2}$
(1, 1)	(0, 0)	$\cos^2(\frac{\theta}{2})\cos^2\frac{\psi_2}{2}$
	(0, 1)	$\cos^2(\frac{\theta}{2})\sin^2\frac{\psi_2}{2}$
	(1, 0)	$\sin^2(\frac{\theta}{2})\sin^2\frac{\psi_2}{2}$
	(1, 1)	$\sin^2(\frac{\theta}{2})\cos^2\frac{\psi_2}{2}$

Adding the joint probabilities for the corresponding rows, we find that the above quantity is equal to $\frac{1}{8}[\sin\theta(\sin\psi_1+\sin\psi_2)+(\cos\psi_1-\cos\psi_2)]+\frac{1}{2}$.

In Fig. 1, we plot the joint probability as a function of θ, for the angles $(\psi_1,\psi_2)=\{(\frac{\pi}{4},3\frac{\pi}{4}),\ (3\frac{\pi}{16},13\frac{\pi}{16}),\text{ and }(9\frac{\pi}{32},23\frac{\pi}{32})\}$. A magnified view of the plot for the region from $\theta=\frac{\pi}{4}$ to $\theta=\frac{\pi}{2}$ appears on the right. In the plot it is shown that when $\theta=\frac{\pi}{2}$, the joint probability reaches a value equal to $\cos^2\frac{\pi}{8}$.

V. SECURITY ANALYSIS

In this section, we prove the security of the proposed protocol. In an earlier section, we showed that if the shared entangled states are not in a certain form, then Alice may extract more information than what is suggested by the protocol. So, at the beginning of the protocol either Bob has to trust devices blindly (device-dependent assumption on which the security of the existing protocols depends) or he needs to test some statistical property by measuring the given entangled states (device-independent assumption). The security of the proposed protocol comes from the following result.

Theorem 1. If for a random subset $\Gamma_{\text{CHSH}}\subset\{1,\ldots,n\}$ of size γn, where $\gamma>0$, the fraction of the inputs $(x_i,\ y_i)$, $i\in\Gamma_{\text{CHSH}}$, which satisfies the CHSH condition, i.e., $(a_i\oplus b_i=x_i\wedge y_i)$ is equal to $\frac{1}{8}(\sin\theta(\sin\psi_1+\sin\psi_2)+\cos\psi_1-\cos\psi_2)+\frac{1}{2}-\delta$, then for the remaining subset $\Gamma_{\text{QPQ}}\subset\{1,\ldots,n\}$ of size $(1-\gamma)n$, a fraction of inputs (x_i,y_i), $i\in\Gamma_{\text{QPQ}}$, which satisfies the CHSH condition, is also equal to $\frac{1}{8}(\sin\theta(\sin\psi_1+\sin\psi_2)+\cos\psi_1-\cos\psi_2)+\frac{1}{2}-\delta$, with a negligible statistical deviation ν.

Here, $\delta=\sqrt{\frac{1}{2\gamma n}\ln\frac{1}{\epsilon_{\text{CHSH}}}}$, $\nu=\sqrt{\frac{(\gamma n+1)}{2\gamma^2(1-\gamma)n^2}\ln\frac{1}{\epsilon_{\text{QPQ}}}}$, and ϵ_{CHSH} and ϵ_{QPQ} are negligibly small values.

In the second result, we show that when n is sufficiently large, then conditional on the success of the above local CHSH test, one may proceed to the QPQ protocol proposed by Yang *et al.* [10] for the remaining subset Γ_{QPQ}.

Theorem 2. Conditional on the event that the local CHSH test has been successful for the subset Γ_{CHSH}, Bob can proceed to the QPQ protocol for the remaining subset Γ_{QPQ} securely when $n\to\infty$.

In [10], the authors consider the security issues for two cases: (a) dishonest Alice and honest Bob and (b) honest Alice and dishonest Bob. As the second phase of our protocol is the same as the QPQ protocol proposed by Yang *et al.* [10], the security issues for the second part of the current protocol remain the same.

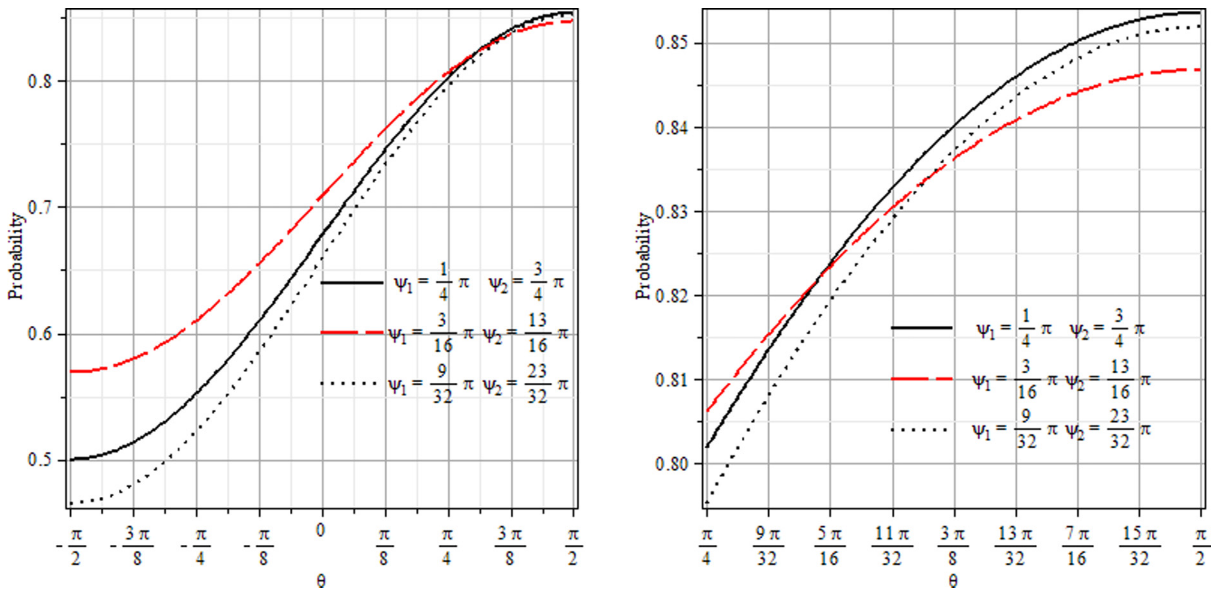

FIG. 1. The value of $\Pr(a_i\oplus b_i=x_i\wedge y_i)$ with respect to θ.

VI. DISCUSSION AND CONCLUSION

In this paper, we propose a device-independent scenario in quantum private query. Exploiting the idea of a local CHSH test we show how Bob can remove his trust in devices. The proposed protocol is divided into two distinct parts. In the first part, Bob performs the local CHSH test at his end. Conditional on the event that the local CHSH test has been successful, Bob proceeds to the QPQ protocol. We worked here on the QPQ protocol proposed by Yang *et al.* [10]. However, one can exploit any entanglement-based QPQ protocol for the second phase of our proposed scheme. Here, we assume that the detectors have unit efficiency. However, it remains open what would happen if the detectors were imperfect, i.e., had nonunit efficiency.

APPENDIX: LEMMAS AND PROOFS

Lemma 1 (Chernoff-Hoeffding [29]). Let $X = \frac{1}{n}\sum_i X_i$ be the average of n independent random variables $X_1, X_2, \ldots, X_n$ with values [0,1], and let $\mathbb{E}[X] = \frac{1}{n}\sum_i \mathbb{E}[X_i]$ be the expectation value of X; then for any $\delta > 0$, we have $\Pr[|X - \mathbb{E}[X]| \geqslant \delta] \leqslant \exp(-2\delta^2 n)$.

Lemma 2 (Serfling [30]). Let $\{x_1, x_2, \ldots, x_n\}$ be a list of values in $[a,b]$ (not necessarily distinct). Let $\overline{x} = \frac{1}{n}\sum_i x_i$ be the average of these random variables. Let k be the number of random variables $X_1, X_2, \ldots, X_k$ chosen from the list without replacement. Then for any value of $\delta > 0$, we have $\Pr[|X - \overline{x}| \geqslant \delta] \leqslant \exp(\frac{-2\delta^2 kn}{(n-k+1)(b-a)})$, where $X = \frac{1}{k}\sum_i X_i$.

Lemma 3 (corollary to Serfling lemma [23]). Let $\mathbb{X} = \{x_1, x_2 \ldots x_n\}$ be a list of (not necessarily distinct) values in [0,1] with the average $\mu_{\mathbb{X}} = \frac{1}{n}\sum_{i=1} x_i$. Let $\mathbb{T}$ be a subset of $\mathbb{X}$ of size t with average $\mu_{\mathbb{T}} = \frac{1}{t}\sum_{i\in\mathbb{T}} x_i$. Let $\mathbb{K}$ be the remaining subset of $\mathbb{X}$ of size k (i.e., $t + k = n$). If the average of the subset $\mathbb{K}$ is $\mu_{\mathbb{K}} = \frac{1}{n-t}\sum_{i\in\mathbb{K}} x_i$, then for any value of $\epsilon > 0$, we have $\Pr(|\mu_{\mathbb{K}} - \mu_{\mathbb{T}}| \geqslant \sqrt{\frac{n(t+1)}{2t^2(n-t)}\ln\frac{1}{\epsilon}}) \leqslant \epsilon$.

Proof of Theorem 1. We define a random variable Y_i as follows: $Y_i = 1$ if $a_i \oplus b_i = x_i \wedge y_i$; $Y_i = 0$ otherwise. Now we choose a random subset $\Gamma_{\text{CHSH}} \subset \{1, \ldots, n\}$ of size γn for any $\gamma > 0$ and define $Y = \frac{1}{\gamma n}\sum_{i\in\Gamma_{\text{CHSH}}} Y_i$. Here, Y is called the observed average value. Let the expected value of Y for that subset be $\mathbb{E}(Y) = \frac{1}{8}(\sin\theta(\sin\psi_1 + \sin\psi_2) + \cos\psi_1 - \cos\psi_2) + \frac{1}{2}$. Then applying the Chernoff bound (Lemma 1) we get $\Pr[|Y - \mathbb{E}(Y)| \geqslant \delta] \leqslant \exp(-2\delta^2\gamma n)$.

Let ϵ_{CHSH} be a negligibly small value. Equating $\exp(-2\delta^2\gamma n)$ with ϵ_{CHSH} we can find the value of $\delta = \sqrt{\frac{1}{2\gamma n}\ln\frac{1}{\epsilon_{\text{CHSH}}}}$.

Again, we consider the remaining subset $\Gamma_{\text{QPQ}} \subset \{1, \ldots, n\}$ of size $(1-\gamma)n$ and define $Y' = \frac{1}{(1-\gamma)n}\sum_{i\in\Gamma_{\text{QPQ}}} Y_i$. Now, from Lemma 3, it can be shown that $\Pr(|Y - Y'| \geqslant \nu) \leqslant \exp(\frac{-2\gamma^2\nu^2(n-\gamma n)n^3}{(\gamma n+1)n^2})$.

Let ϵ_{QPQ} be a negligibly small value. Then, equating the right-hand side with ϵ_{QPQ}, we get ν. ■

Proof of Theorem 2. In the asymptotic limit, i.e., when $n \rightarrow \infty$, the expressions for δ and ν tend to 0. This implies that in the asymptotic case, $Y = Y' = \mathbb{E}(\mathbb{Y})$. Thus by calculating the value of Y for the subset Γ_{CHSH}, Bob can certify that entangled states for the subset Γ_{QPQ} are of the desired type and hence can be exploited securely for the QPQ protocol. Alice cannot extract more information about the raw key bits than suggested by the protocol. ■

[1] V. Giovannetti, S. Lloyd, and L. Maccone, Phys. Rev. Lett. **100**, 230502 (2008).

[2] V. Giovannetti, S. Lloyd, and L. Maccone, IEEE Trans. Info. Theory **56**, 3465 (2010).

[3] L. Olejnik, Phys. Rev. A **84**, 022313 (2011).

[4] M. Jakobi, C. Simon, N. Gisin, J. D. Bancal, C. Branciard, N. Walenta, and H. Zbinden, Phys. Rev. A **83**, 022301 (2011).

[5] V. Scarani, A. Acín, G. Ribordy, and N. Gisin, Phys. Rev. Lett. **92**, 057901 (2004).

[6] F. Gao, B. Liu, Q. Y. Wen, and H. Chen, Opt. Express **20**, 17411 (2012).

[7] M. V. Panduranga Rao and M. Jakobi, Phys. Rev. A **87**, 012331 (2013).

[8] J. L. Zhang, F. Z. Guo, F. Gao, B. Liu, and Q. Y. Wen, Phys. Rev. A **88**, 022334 (2013).

[9] T.-G. Noh, Phys. Rev. Lett. **103**, 230501 (2009).

[10] Y. G. Yang, S. J. Sun, P. Xu, and J. Tiang, Quant. Info. Proc. **13**, 805 (2014).

[11] C. H. Bennett, Phys. Rev. Lett. **68**, 3121, (1992).

[12] C. Y. Wei, F. Gao, Q. Y. Wen, and T. Y. Wang, Sci. Rep. **4**, 7537 (2014).

[13] P. Chan, I. Lucio-Martinez, X. Mo, C. Simon, and W. Tittel, Sci. Rep. **4**, 5233 (2014).

[14] F. Gao, B. Liu, W. Huang, and Q. Y. Wen, IEEE J. Select. Topics Quantum Electron. **21**, 6600111 (2015).

[15] B. Liu, F. Gao, and W. Huang, Sci. China Phys. Mech. Astron. **58**, 100301 (2015).

[16] D. Mayers and A. C. C. Yao, in Proceedings of the 39th Annual Symposium on Foundations of Computer Science (FOCS 98) (IEEE Computer Society, Washington, DC, 1998), p. 503.

[17] A. Acín, N. Gisin, and L. Masanes, Phys. Rev. Lett. **97**, 120405 (2006).

[18] A. Acín, S. Massar, and S. Pironio, New J. Phys. **8**, 126 (2006).

[19] V. Scarani, N. Gisin, N. Brunner, L. Masanes, S. Pino, and A. Acín, Phys. Rev. A **74**, 042339 (2006).

[20] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007).

[21] J. S. Bell, Physics **1**, 195 (1964).

[22] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. **23**, 880 (1969).

[23] C. Ci Wen Lim, C. Portmann, M. Tomamichel, R. Renner, and N. Gisin, Phys. Rev. X **3**, 031006 (2013).

[24] J. Silman, A. Chailloux, N. Aharon, I. Kerenidis, S. Pironio, and S. Massar, Phys. Rev. Lett. **106**, 220501 (2011).

[25] N. Aharon, S. Massar, S. Pironio, and J. Silman, New J. Phys. **18**, 025014 (2016).

[26] J. Kaniewski and S. Wehner, New J. Phys. **18**, 055004 (2016).

[27] J. Ribeiro, L. P. Thinh, J. Kaniewski, J. Helsen, and S. Wehner, arXiv:1606.08750.

[28] J. Ribeiro, G. Murta, and S. Wehner, arXiv:1609.08487.

[29] W. Hoeffding, J. Am. Stat. Assoc. **58**, 13 (1963).

[30] R. J. Serfling, Ann. Stat. **2**, 39 (1974).