mathematics

IMPACT FACTOR 2.3

CITESCORE 4.0

Article

Device Independent Quantum Private Queries Based on Quantum Key Distribution

Li Liu, Qingshan Du and Xu Gao

Special Issue

Quantum Cryptography and Applications

Edited by

Dr. Chun-Wei Yang, Dr. Chia-Wei Tsai and Dr. Jason Lin

MDPI

https://doi.org/10.3390/math13060951

mathematics

MDPI

Article

Device Independent Quantum Private Queries Based on Quantum Key Distribution

Li Liu [1,2,*], Qingshan Du [3] and Xu Gao [3]

[1] School of Communication and Information Engineering, Xi'an University of Posts and Telecommunications, Xi'an 710121, China
[2] Shaanxi Key Laboratory of Information Communication Network and Security, Xi'an University of Posts and Telecommunications, Xi'an 710121, China
[3] Xi'an Modern Control Technology Research Institute, Xi'an 710121, China; 5099121032@email.ncu.edu.cn (Q.D.); g_36795@163.com (X.G.)
* Correspondence: liu_li@xupt.edu.cn

Abstract: Symmetric private information retrieval (SPIR) protocol is proposed for users to retrieve items from a database holder without revealing the retrieval address, and meanwhile the users cannot learn any additional entries of the database. Quantum key distribution (QKD)-based quantum private queries (QPQs) are the most practical protocols for the SPIR problem. However, most existing protocols assume ideal devices. To overcome this drawback, we propose a device independent QPQ protocol based on QKD with imperfect sources and detectors. By constructing the semi-definite programming optimization problem, we give the CHSH test threshold and prove the correctness of our protocol. We use the shift and permutation post-processing technique to further improve the security. We compare the performance of our protocol with a recent full device-independent QPQ. and discuss their relative advantages. The simulation results show that our protocol improves database security, user privacy and efficiency. The number of final key bits that Alice knows is close to 1, and Bob's guessing probability is below 0.15 in our protocol. Moreover, the proposed scheme can be used for any entanglement-based QPQ protocol to remove trust on the devices.

Keywords: quantum key distribution; quantum private queries; device independent; security analysis

MSC: 81P94

Academic Editor: Raymond Lee

Received: 12 February 2025
Revised: 9 March 2025
Accepted: 12 March 2025
Published: 13 March 2025

Citation: Liu, L.; Du, Q.; Gao, X. Device Independent Quantum Private Queries Based on Quantum Key Distribution. *Mathematics* **2025**, *13*, 951. https://doi.org/10.3390/math13060951

1. Introduction

With the development of telecommunication technology, security and data privacy have attracted wide attention. Users of digital services may not want their information to be leaked to database holders. Private information retrieval (PIR) provides a scheme for this scenario [1,2]. PIR allows user Alice to retrieve an item from database holder Bob without revealing the retrieval address (user privacy). However, in some cases, the database holder may not want to reveal more information about the database than Alice requires (database privacy). Taking this additional security requirement into account is very necessary, especially when the information in the database is valuable and sensitive, such as medical records and bank accounts. This can be achieved by symmetrically private information retrieval (SPIR) [3–5].

Since user privacy and database security seem to be in conflict, it is difficult to design information-theoretic secure SPIR schemes [6]. Researchers have studied a weaker version

of SPIR, called private query (PQ) [7–10]. In the PQ protocol, users are allowed to obtain more than one item of the database than SPIR. On the other hand, if the database holder Bob tries to gain Alice's retrieval address, then Alice can detect that, which is called cheat sensitivity for user privacy. But it is still hard to achieve in the classical domain. Meanwhile, classical schemes might be vulnerable to a quantum adversary [11]. To overcome these problems, quantum private query (QPQ) protocol has been proposed.

In 2008, Giovannetti et al. proposed the first QPQ protocol performed by unitary operations [12], followed by [13,14]. However, all of these protocols are difficult to implement. To make QPQ practical, Jakobi et al. have proposed a new QPQ protocol based on the SARG04 QKD [15]. This type of QPQ protocol is called QKD-based QPQ. Since QKD has been widely studied in both theoretical and experimental research fields [16–24], QKD-based QPQ protocol is easier to implement than the original QPQ. Based on different types of QKD protocols, various QKD-based QPQ protocols have been proposed [25–31]. Furthermore, some techniques have been applied to improve the performance of QPQs. Wei et al. [32] have presented a special "low-shift and addition" technique to establish a generic construction of QKD-based QPQs with ideal database security. Considering that weak coherent pulse sources are usually used in practical implementation, the decoy state method is adopted in the QPQ protocol [33,34].

QKD-based QPQs can be viewed as a cryptographic protocol in which two parties are dishonest [12–15]. QKD-based QPQs can generally be performed in the following three steps. (1) Oblivious raw key distribution. Alice and Bob first generate an oblivious raw key. (2) Post-processing. In order to reduce Alice's known bits, Alice and Bob cut the raw key into several substrings with equal length and add them bitwise to obtain the final key. Then Alice knows only one (or a little more than one) bit of the final key. (3) Private query. Alice announces a shift to the final key according to the item she wants to query. Then Bob uses the shifted key to encrypt the database and sends the whole encrypted database to Alice. Finally, Alice can know exactly the bit she wants by decrypting the database, which means that a private query has been performed successfully. The security of all of the above 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. To remove trustful assumptions, a device-independent QPQ protocol (DI-QPQ) has been described in [35]. However, it requires the assumption that all detectors at Bob's end have unit efficiency; that is, he always obtains a conclusive outcome. Recently, Basak et al. have proposed a QPQ protocol for full DI certification using a self-test strategy (FDI-QPQ) [36], followed by [37].

To perform the QPQ protocol with imperfect sources and detectors, we utilize the idea of a local CHSH test proposed by Lim et al. [38]. In the local CHSH test, the sender executes the CHSH test at its terminal as an incentive to verify whether the states used for QKD are maximally entangled. The local CHSH test can provide a certification with imperfect sources. On the other hand, for imperfect detectors, we apply the Navascués–Pironio–Acín (NPA) method arising from quantum non-locality in DI quantum information processing [39]. Inspired by the NPA method, a semi-definite programming (SDP) optimization problem is proposed to analyze the security of QKD [40].

In this paper, by analyzing the security of the DI-QPQ protocol, we find that it cannot achieve full device independent because it requires the assumption that all detectors have unit efficiency. To address this challenge, we propose a QPQ protocol with imperfect sources and detectors (called ISD-QPQ). By adopting the local CHSH test, Bob can certify whether the states are in the desired form or not. We employ the NPA method to construct the SDP optimization problem to solve the predefined threshold probability and Alice's success guess probability. We use the shift and permutation post-processing method to

further improve the efficiency and security of our protocol. Furthermore, we discuss the database security and user privacy of our ISD-QPQ protocol.

The paper is organized as follows. In Section 2, we review the DI-QPQ protocol and analyze the security under imperfect sources and detectors. Next, in Section 3, we detail our IFD-QPQ protocol. In Section 4, by constructing the SDP optimization problem, we prove the correctness, database security and user privacy of IFD-QPQ protocol. The simulation results are shown in Section 5. Finally, Section 6 gives the conclusion.

2. Analysis of DI-QPQ with Imperfect Source and Detectors

2.1. Review of DI-QPQ Protocol

With the idea of a local CHSH-like test, Maitra. A. et al. have proposed the DI-QPQ protocol [35]. This QPQ protocol no longer requires trust in the source as well as the detectors. We first review the DI-QPQ protocol as follows.

(1) Bob prepares a long sequence of entangled states $\frac{1}{\sqrt{2}}(|0\rangle_B|\phi_0\rangle_A + |1\rangle_B|\phi_1\rangle_A)$, where $|\phi_0\rangle_A = \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}|1\rangle$ and $|\phi_1\rangle_A = \cos\frac{\theta}{2}|0\rangle - \sin\frac{\theta}{2}|1\rangle$.

(2) For each prepared entangled state, Bob divides it into two sets. One is N_{CHSH} and the other is N_{QPQ}. The set N_{CHSH} contains γn entangled states, whereas N_{QPQ} contains $(1-\gamma)n$ entangled states for $0 < \gamma < 1$.

(3) For rounds $i \in \{1, \ldots, \gamma n\}$

- Bob chooses $x_i \in \{0,1\}$ and $y_i \in \{0,1\}$ uniformly at random. 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. 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. Here, we consider $|\psi_1\rangle = \cos\frac{\psi_1}{2}|0\rangle + \sin\frac{\psi_1}{2}|1\rangle$ and $|\psi_2\rangle = \cos\frac{\psi_2}{2}|0\rangle + \sin\frac{\psi_2}{2}|1\rangle$.
- Bob records and encodes the output as $a_i \in \{0,1\}(b_i \in \{0,1\})$ for the first (second) particle. 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 $|-\rangle$. 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 result is $|\psi_1^{\perp}\rangle$ or $|\psi_2^{\perp}\rangle$.
- Define $Y_i = 1$, if $a_i \oplus b_i = x_i \wedge y_i$; otherwise, $Y_i = 0$.

(4) If $\frac{1}{\gamma n}\sum_i Y_i < P = \frac{1}{8}[\sin\theta(\sin\psi_1 + \sin\psi_2) + \cos\psi_1 - \cos\psi_2] + \frac{1}{2}$, Bob aborts the protocol.

(5) Conditional on the event that the local N_{CHSH} test at Bob's end has been successful, Bob proceeds to the subset N_{QPQ} and sends the other half of the remaining $(1-\gamma)n$ entangled pairs to Alice.

(6) Alice performs the private query phase as in [26] or any other entanglement-based QPQ protocol.

2.2. Security of DI-QPQ Protocol with Imperfect Sources and Detectors

We analyze the security of DI-QPQ protocol under imperfect sources in practical. Suppose that the source provides arbitrary entangled states $\alpha|0\rangle_B|\phi_0\rangle_A + \beta|1\rangle_B|\phi_1\rangle_A$, where $|\alpha|^2 = \frac{1}{2} + \tau$ and $|\beta|^2 = \frac{1}{2} - \tau$. The joint probability $\Pr(a_i \oplus b_i = x_i \wedge y_i)$ can be calculated by

$$\begin{aligned}\Pr(a_i \oplus b_i = x_i \wedge y_i) = \frac{1}{4}[&\Pr(00|00) + \Pr(11|00) + \Pr(00|01) + \Pr(11|01) \\ &+ \Pr(00|10) + \Pr(11|10) + \Pr(01|11) + \Pr(10|11)],\end{aligned} \tag{1}$$

where the conditional probability of (a_i, b_i) given (x_i, y_i) can be obtained by

$$\begin{aligned}\Pr(00|00) &= (\bar{\alpha}\langle\phi_0|\langle 0| + \bar{\beta}\langle\phi_1|\langle 1|)(|0\rangle\langle 0| \otimes |\psi_1\rangle\langle\psi_1|)(\alpha|\phi_0\rangle|0\rangle + \beta|\phi_1\rangle|1\rangle) \\ &= |\alpha|^2(\cos\frac{\theta}{2}\cos\frac{\psi_1}{2} + \sin\frac{\theta}{2}\sin\frac{\psi_1}{2})^2 \\ &= |\alpha|^2\cos^2(\frac{\theta-\psi_1}{2}).\end{aligned} \tag{2}$$

Similarly, we have

$$\begin{aligned}\Pr(11|00) &= |\beta|^2\sin^2(\frac{\theta+\psi_1}{2}), \\ \Pr(00|01) &= |\alpha|^2\cos^2(\frac{\theta-\psi_2}{2}), \\ \Pr(11|01) &= |\beta|^2\sin^2(\frac{\theta+\psi_2}{2}), \\ \Pr(00|10) &= \frac{1}{2}[\alpha\cos(\frac{\theta-\psi_1}{2}) + \beta\sin(\frac{\theta+\psi_1}{2})]^2, \\ \Pr(11|10) &= \frac{1}{2}[\alpha\sin(\frac{\theta-\psi_1}{2}) - \beta\cos(\frac{\theta+\psi_1}{2})]^2, \\ \Pr(01|11) &= \frac{1}{2}[\alpha\sin(\frac{\theta-\psi_2}{2}) + \beta\cos(\frac{\theta+\psi_2}{2})]^2, \\ \Pr(10|11) &= \frac{1}{2}[\alpha\cos(\frac{\theta-\psi_2}{2}) - \beta\sin(\frac{\theta+\psi_2}{2})]^2.\end{aligned} \tag{3}$$

According to these conditional probabilities, we can obtain

$$\begin{aligned}\Pr(a_i \oplus b_i = x_i \wedge y_i) =& \frac{1}{8}\big(\sin\theta(\sin\psi_1 + \sin\psi_2) + 2\tau\cos\theta(\cos\psi_1 + \cos\psi_2) \\ &+ 2\sqrt{\frac{1}{4} - \tau^2}(\cos\psi_1 - \cos\psi_2)\big) + \frac{1}{2}.\end{aligned} \tag{4}$$

Thus, by calculating the maximum of above equation while traversing the parameter τ, we find that

$$\Pr(a_i \oplus b_i = x_i \wedge y_i) < \frac{1}{8}[\sin\theta(\sin\psi_1 + \sin\psi_2) + \cos\psi_1 - \cos\psi_2] + \frac{1}{2}, \tag{5}$$

where $\tau \in [0, \frac{1}{2}]$. The simulation result is shown in Section 5. That is, in DI-QPQ protocol, the joint probability $\Pr(a_i \oplus b_i = x_i \wedge y_i)$ is always less than the threshold parameter P. If Alice and Bob do not share the entangled states of the certain kind, Bob will discover and abort the protocol by performing the local test at his end. Bob can then remove his trust in the source. However, the DI-QPQ protocol requires the assumption that all detectors at Bob's end have unit efficiency, i.e., he always receives conclusive outcomes. For practical implementation of the protocol, imperfect detectors are generally exploited. Therefore, it is necessary to study the QPQ protocol for imperfect sources and detectors. To solve this problem, we propose a practical QPQ protocol with imperfect sources and detectors, called ISD-QPQ protocol.

3. Practical Quantum Private Queries with Imperfect Sources and Detectors

Here, we detail our proposed ISD-QPQ protocol as follows.

(1) The database holder Bob prepares a long sequence of entangled photon pairs in the state

$$|\Phi\rangle_{BA} = \frac{1}{\sqrt{2}}(|0\rangle_B|\phi_0\rangle_A + |1\rangle_B|\phi_1\rangle_A), \tag{6}$$

where

$$|\phi_0\rangle_A = \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}|1\rangle,$$
$$|\phi_1\rangle_A = \cos\frac{\theta}{2}|0\rangle - \sin\frac{\theta}{2}|1\rangle. \tag{7}$$

The parameter $\theta \in (0, \frac{\pi}{2})$ can be selected flexibly.

(2) For each prepared entangled state, Bob divides it into two sets N_{CHSH} and N_{QPQ}. The set N_{CHSH} contains γn entangled states, which is used to conduct the CHSH local test, whereas N_{QPQ} contains $(1-\gamma)n$ entangled states for $0 < \gamma < 1$, which is used to perform private queries.
For round $i \in \{1, \ldots, \gamma n\}$ in N_{CHSH}, Bob chooses $x_i \in \{0,1\}$ and $y_i \in \{0,1\}$ uniformly at random. $x_i = 0$ denotes Bob measures the first particle of the entangled state in the $\{|0\rangle, |1\rangle\}$ basis. If $x_i = 1$, he measures it in the $\{|+\rangle, |-\rangle\}$ basis. 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. Here, we consider

$$|\psi_1\rangle = \cos\frac{\psi_1}{2}|0\rangle + \sin\frac{\psi_1}{2}|1\rangle,$$
$$|\psi_2\rangle = \cos\frac{\psi_2}{2}|0\rangle + \sin\frac{\psi_2}{2}|1\rangle. \tag{8}$$

We use positive-operator valued measures (POVMs) to describe Bob's measurements: Bob randomly performs one of two possible POVMs denoted by $\{E_x^a, M_y^b\}$, where $x \in \{0,1\}$ and $y \in \{0,1\}$ represent the basis choice for the first and the second particles of the entangled state, respectively. Taking signal loss and detection inefficiency into account, each measurement has three possible outcomes $a, b \in \{0, 1, \emptyset\}$, where $\emptyset$ represents the empty detection event.

(3) Bob records and encodes the output as $a_i \in \{0,1\} (b_i \in \{0,1\})$ for the first (second) particle. For the first particle in each pair, $a_i = 0$ if the measurement result is $|0\rangle$ and $a_i = 1$ if the result is $|1\rangle$. 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 result is $|\psi_1^{\perp}\rangle$ or $|\psi_2^{\perp}\rangle$.

(4) Define Y_i for the test round $i \in N_{CHSH}$

$$Y_i = \begin{cases} 1 & \text{if } a_i \oplus b_i = x_i \wedge y_i, \\ 0 & \text{if otherwise.} \end{cases} \tag{9}$$

If $\frac{1}{\gamma n}\sum_i Y_i < P^*$, Bob aborts the protocol.

(5) Conditional on the event that the local N_{CHSH} test at Bob's end has been successful, Bob proceeds to the subset N_{QPQ} and sends the photon A of the remaining $(1-\gamma)n$ entangled states in each pair to Alice. $|\phi_0\rangle$ and $|\phi_1\rangle$ represent the bits 0 and 1.

(6) Alice declares which qubits are received successfully. The bits carried by the lost photons are discarded. For each successfully received qubit, Bob measures his corresponding qubits in the $\{|0\rangle_B, |1\rangle_B\}$ basis. Then, Alice chooses to 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 is $|\phi_0^{\perp}\rangle$, she can obtain 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. We also use POVMs $\{A_x^a\}$ and $\{B_y^b\}$ to describe Alice's and Bob's measurements, where $x \in \{0,1\}$ and $y \in \{0\}$ represent the basis choice, respectively. Taking signal loss and detection inefficiency into account, each measurement has three possible outcomes $a, b \in \{0, 1, \emptyset\}$.

(7) Then, they store the measurement results of remaining signal states as the raw key. They share the raw key K^r, in which Bob knows all the bits while Alice only knows part of K^r.

(8) Alice and Bob perform classical post-processing. Assume an N-bit database is concerned, the created string should be of length $k \times N$ (k is a security parameter). Bob first randomly announces a permutation mapping, then Alice announces a shift s_0 from $\{0, 1, \ldots, kN-1\}$ randomly. After that, they shift the raw key by s_0, then apply the permutation mapping on it and cut it into k N-bit substrings. These substrings are added bitwise to obtain the final key K^f in order that Alice knows only roughly one bit in K^f . If Alice does not know any bit of K^f, the protocol is aborted.

(9) Suppose Alice knows the j-th bit K_j^f and wants the i-th item X_i in the database, then she declares a shift $s = j - i$. Bob encrypts his database with K^f shifted by s, i.e., $C_n = X_n \oplus K_{n+s}^f$, and sends the encrypted database C_n to Alice. Then, Alice recovers the wanted item by her known bit, i.e., $C_i = X_i \oplus K_j^f$.

For each prepared entangled state, Bob divides it into two sets to perform the CHSH local test steps and the QPQ steps, respectively. Our scheme for testing steps lies on top of the QPQ protocol, which means that Bob performs the local CHSH test before starting the QPQ protocol. Here, we work on the QPQ protocol presented in [26]. It is also feasible to replace the QPQ step of our scheme with any entanglement-based QPQ protocol. Then, our scheme can be used for any entanglement-based QPQ protocol to remove trust in the devices. The simplified ISD-QPQ protocol flowchart as shown below (Figure 1):

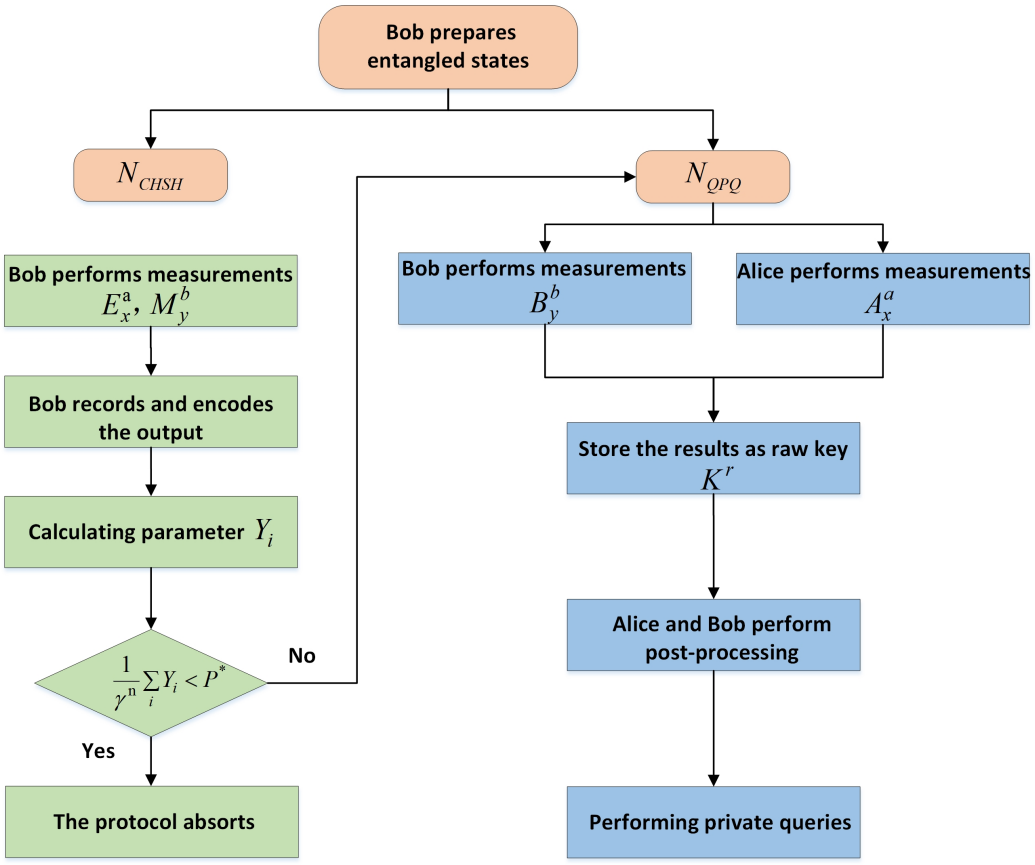

Figure 1. The ISD-QPQ protocol flowchart.

4. Security Analysis

Before analyzing the security of our ISD-QPQ protocol, we first enumerate the assumptions required for the security of the protocol as follows:

(1) Devices are causally independent. This assumption implies that the devices are memoryless.
(2) The adversary's attacks are independent and identically distributed.
(3) All the detectors at Bob's end have a trusted loss.

In the QPQ protocol, security consists mainly of two parts, database security and user privacy, without considering the attack of the third party. Alice can control the sources and detectors on the Bob side, and she may use the imperfect device with bias to simulate a lossy device. It is necessary to require that the dishonest Alice's attack strategy is independent of the loss. Dishonest Alice cannot control the sources and measurement devices in Bob's lab after the devices are installed.

4.1. SDP Optimization Problem for Bounding the Joint Probability

To compute the security of the protocol, we need to give the bound of P^*. This bound can be used to check whether the entangled states are credible. Here, we employ the SDP optimization method to estimate the P^*, which converts the initial characterization problem into a hierarchy of semi-definite programs. More specifically, a hierarchy of conditions necessarily satisfied by any distributions representing the probabilities come from local measurements on a shared quantum state was introduced. Each condition in this hierarchy is formulated as a semi-definite program. Each hierarchy forms a convex set that is approximated to the quantum set from outside. By going to higher hierarchies, the approximation becomes tighter. Thus, using this method, we can optimize to bound P^* over the various convex sets.

The probability distribution is said to admit a quantum system if for all a, b, x, y there exists a set of measurement operators $\{E_x^a, M_y^b\}$ and a quantum state ρ such that

$$p(a, b|x, y) = tr(\rho E_x^a \otimes M_y^b). \tag{10}$$

where ρ is shared by two parties, Alice and Bob. $\{E_x^a\}_{a\in A, x\in X}, \{M_y^b\}_{b\in B, y\in Y}$ are the measurement operators in Bob's testing step, where $A, B \in \{0, 1, \emptyset\}$ are outcome sets, and $X, Y \in \{0, 1\}$ are input sets.

The POVMs follow the following properties: (i) for any x, y, $E_x^a E_x^{a'} = 0$ and $M_y^b M_y^{b'} = 0$ for $a \neq a', b \neq b'$, (ii) $\Sigma_a E_x^a = \mathbb{I}$ and $\Sigma_b M_y^b = \mathbb{I}$, (iii) $(E_x^a)^2 = E_x^a = (E_x^a)^\dagger$ and $(M_y^b)^2 = M_y^b = (M_y^b)^\dagger$, (iv) $[E_x^a, M_y^b] = 0$. Note that with this SDP method, detailed characterization of the quantum signals and measurements, including their dimensions, is no longer required in the analysis.

A series of necessary conditions satisfied by the probabilities of quantum observation can be introduced. Let $\mathsf{S} = \{S_1, \ldots, S_n\}$ be a set of n operators, where each element is a linear combination of products of E_x^a and M_y^b. The PSD Gram matrix G associated to the set S has the definition:

$$G_{i,j} = \mathrm{Tr}(S_i^\dagger S_j \rho). \tag{11}$$

Taking $\mathsf{S} = \{E_x^a, M_y^b, E^\emptyset\}$. The important point is that $G_{i,j}$ partially reflects the properties (i)–(iv) satisfied by the operators E_x^a and M_y^b. For instance, property (i) and (iii) implies $\mathrm{Tr}(S_i^\dagger S_j \rho) = \mathrm{Tr}(M_m^c M_m^{c'} \rho) = 0$ for $c \neq c'$ and $\mathrm{Tr}(S_i^\dagger S_j \rho) = \mathrm{Tr}(M_m^c M_m^c \rho) = \mathrm{Tr}(M_m^c \rho)$ for $c = c'$, where $m = x, y$, $c = a, b$; suppose S contains operators $S_1 = M_m^1, \ldots,$ and $S_{|c|} = M_m^{|c|}$, then property (ii) implies $\sum_{i=1}^{|c|} \mathrm{Tr}(S_i \rho) = \mathrm{Tr}(\sum_c M_m^c \rho) = 1$. In addition, suppose that

S contains an operator $S_i = E_x^a$ and $S_j = M_y^b E_{x'}^{a'} M_{y'}^b$, then the property (iv) implies $\mathrm{Tr}(S_i^\dagger S_j \rho) = \mathrm{Tr}(E_x^a M_y^b E_{x'}^{a'} M_{y'}^b \rho) = \mathrm{Tr}(E_x^a E_{x'}^{a'} M_y^b M_{y'}^{b'} \rho)$.

From the definition, the operators of each set S produce a different Gram matrix G and form different linear constraints. The choice of a particular S can be organized in a hierarchical structure. More specifically, S can be defined as

$$\begin{aligned} \mathsf{S}_1 &= \{E_x^a, M_y^b\} \\ \mathsf{S}_2 &= \mathsf{S}_1 \bigcup \{E_x^a E_{x'}^{a'}, E_x^a M_{y'}^b, M_y^b M_{y'}^{b'}\} \\ \mathsf{S}_3 &= \mathsf{S}_2 \bigcup \{E_x^a E_{x'}^{a'} E_x^a, E_x^a M_y^b E_x^a, E_x^a M_y^b M_{y'}^{b'}, E_x^a E_x^{a'} M_{y'}^b, M_y^b M_{y'}^{b'} M_y^b, \dots\} \\ \mathsf{S}_4 &= \dots \end{aligned} \tag{12}$$

It is evident that $\mathsf{S}_1 \subseteq \mathsf{S}_2 \subseteq \dots$. We define the quantum set by $\mathsf{Q}(\lambda)$, which is formed by the measurement statistics compatible with the set of prepared quantum signals and Bob's measurements. Moreover, denote the set of probability distributions defined by the hierarchy of step n as $\mathsf{Q}(\lambda)_n$. Then, we have $\mathsf{Q}(\lambda) \subseteq \mathsf{Q}(\lambda)_n$. It has been proved in [41] that $\mathsf{Q}(\lambda)_n$ converges to the quantum set, $\lim_{n\to\infty} \mathsf{Q}_n = \mathsf{Q}$. Thus, by going to higher hierarchies, the approximation of P^* by the SDP becomes tighter.

We first consider the first hierarchy ($k = 1$), where the corresponding set of operators is chosen as in S_1. Gram matrix $[G]_1$ is shown in below:

$$[G]_1 = \left(\begin{array}{c|c|c|c|c|c} & I|\Phi\rangle_{BA} & A_0^0|\Phi\rangle_{BA} & E_1^0|\Phi\rangle_{BA} & M_0^0|\Phi\rangle_{BA} & M_1^0|\Phi\rangle_{BA} \\ \hline \langle\Phi|_{BA} I & \lambda & \langle\Phi|_{BA} E_0^0|\Phi\rangle_{BA} & \langle\Phi|_{BA} E_1^0|\Phi\rangle_{BA} & \langle\Phi|_{BA} M_0^0|\Phi\rangle_{BA} & \langle\Phi|_{BA} M_1^0|\Phi\rangle_{BA} \\ \hline \langle\Phi|_{BA} E_0^0 & \langle\Phi|_{BA} E_0^0|\Phi\rangle_{BA} & \langle\Phi|_{BA} E_0^0|\Phi\rangle_{BA} & \langle\Phi|_{BA} E_0^0 E_1^0|\Phi\rangle_{BA} & \langle\Phi|_{BA} E_0^0 M_0^0|\Phi\rangle_{BA} & \langle\Phi|_{BA} E_0^0 M_1^0|\Phi\rangle_{BA} \\ \hline \langle\phi_{BA}|E_1^0 & \langle\Phi|_{BA} E_1^0|\Phi\rangle_{BA} & \langle\Phi|_{BA} E_0^0 E_1^0|\Phi\rangle_{BA} & \langle\Phi|_{BA} E_1^0|\Phi\rangle_{BA} & \langle\Phi|_{BA} E_1^0 M_0^0|\Phi\rangle_{BA} & \langle\Phi|_{BA} E_1^0 M_1^0|\Phi\rangle_{BA} \\ \hline \langle\Phi_{BA}|M_0^0 & \langle\Phi|_{BA} M_0^0|\Phi\rangle_{BA} & \langle\Phi|_{BA} E_0^0 M_0^0|\Phi\rangle_{BA} & \langle\Phi|_{BA} E_1^0 M_0^0|\Phi\rangle_{BA} & \langle\Phi|_{BA} M_0^0|\Phi\rangle_{BA} & \langle\Phi|_{BA} M_0^0 M_1^0|\Phi\rangle_{BA} \\ \hline \langle\Phi_{BA}|M_1^0 & \langle\Phi|_{BA} M_1^0|\Phi\rangle_{BA} & \langle\Phi|_{BA} E_0^0 M_1^0|\Phi\rangle_{BA} & \langle\Phi|_{BA} E_1^0 M_1^0|\Phi\rangle_{BA} & \langle\Phi|_{BA} M_1^0 M_0^0|\Phi\rangle_{BA} & \langle\Phi|_{BA} M_1^0|\Phi\rangle_{BA} \end{array}\right) \tag{13}$$

$$\begin{aligned} P^* = \frac{1}{4}[&\Pr(00|00) + \Pr(11|00) + \Pr(00|01) + \Pr(11|01) \\ &+ \Pr(00|10) + \Pr(11|10) + \Pr(01|11) + \Pr(10|11)], \end{aligned} \tag{14}$$

where the conditional probability of (a_i, b_i) given (x_i, y_i) can be obtained by

$$\Pr(00|00) = \langle\Phi|_{BA}(E_0^0 \otimes M_0^0)|\Phi\rangle_{BA}. \tag{15}$$

Similarly, we have

$$\begin{aligned} \Pr(11|00) &= \langle\Phi|_{BA} E_0^1 M_0^1|\Phi\rangle_{BA}, & \Pr(00|01) &= \langle\Phi|_{BA} E_0^0 M_0^1|\Phi\rangle_{BA}, \\ \Pr(11|01) &= \langle\Phi|_{BA} E_1^0 M_1^1|\Phi\rangle_{BA}, & \Pr(00|10) &= \langle\Phi|_{BA} E_0^1 M_0^0|\Phi\rangle_{BA}, \\ \Pr(11|10) &= \langle\Phi|_{BA} E_1^1 M_1^0|\Phi\rangle_{BA}, & \Pr(01|11) &= \langle\Phi|_{BA} E_0^1 M_1^1|\Phi\rangle_{BA}, \\ \Pr(10|11) &= \langle\Phi|_{BA} E_1^1 M_0^1|\Phi\rangle_{BA}. \end{aligned} \tag{16}$$

Under the conditions that p_{det} is fixed to some experimental model, P^* is calculated using the SDP method. In particular, the SDP problem for maximizing the probability P^* is as follows:

$$\begin{aligned} &\text{maximize}: P^* \\ &\text{subject to}: \langle \Phi|\Phi\rangle = \lambda, \\ &\qquad\qquad G \geq 0, \\ &\qquad\qquad \mathrm{Tr}(P_k G) = p_k, \\ &\qquad\qquad \mathrm{Tr}(T_k G) = t_k, \end{aligned} \tag{17}$$

where P_k's and T_k's are constant matrices. Note that P_k's are used to extract the terms in G that are associated with the observed distributions $p(a, b|x, y)$; meanwhile, T_k's are used to extract the terms in G that are associated with the linear constraints induced by the quantum operators and states.

Additionally, we require that Bob's measurements satisfy basis-independent assumption: measurement operators corresponding to detection loss are the same for both measurement settings, i.e., $E_0^{\emptyset} = E_1^{\emptyset}$ and $M_0^{\emptyset} = M_1^{\emptyset}$. This is to ensure that the probability of detecting a signal is independent of Bob's measurement choice, which is necessary to rule out detection side-channel attacks exploiting the channel loss. Thus, Bob's three-outcome POVM is equivalent to a two-outcome POVM that determines the key bit, preceded by a basis-independent "filter".

4.2. Correctness

We analyze the correctness of our proposed ISD-QPQ protocol. When Alice and Bob are honest, Alice can correctly guess only part bits of the entire raw key R at step (8). The success probability of Alice's guessing a bit in the raw key can be obtained by

$$\begin{aligned} P_{guess} &= \Pr(a = 0, b = 0) + \Pr(a = 1, b = 1) \\ &= \Pr(a = 0|b = 0)\Pr(b = 0) + \Pr(a = 1|b = 1)\Pr(b = 1). \end{aligned} \tag{18}$$

Assume that all detectors have unit efficiency, that is, they always obtain conclusive outcomes. The success guess probability of Alice will be $\frac{\sin^2\theta}{2}$. Then, we apply the shift and permutation method [27] for classical post-processing. Alice can correctly guess a final key bit with probability $(\frac{\sin^2\theta}{2})^k$. Considering the imperfect source and detectors, we still adopt the SDP method to maximize the success probability.

With the SDP method, the transmission channel can be seen as an isometric evolution in higher dimension that takes the initial quantum signal state to some pure output signal state $|\phi_z\rangle$, where $z \in \{0, 1\}$. The inner product of the output states is preserved after transmission. For each qubit successfully received, Bob measures his corresponding qubits in the $\{|0\rangle_B, |1\rangle_B\}$ basis. Then, Alice's qubit randomly collapses to one state in set $\{|\phi_0\rangle_A, |\phi_1\rangle_A\}$. The POVMs $\{A_y^b\}$ can be assumed as projective measurements in higher dimensions, where $y \in \{0, 1\}$ represents the basis selection. Given signal loss and detection inefficiency, there are three possible outcomes $b \in \{0, 1, \emptyset\}$ for each measurement. Then, we say that the probabilities of observing outcomes b given setting y and z admits a quantum system, if there exist a quantum state $|\phi_z\rangle$ and operators A_y^b such that

$$p(b|y, z) = \langle \phi_z | A_y^b | \phi_z \rangle. \tag{19}$$

where the operators $\{A_y^b\}$ follow the properties:

$$\begin{aligned} &(i)\ \text{ for any } y, A_y^b A_y^{b'} = 0, \forall\ b \neq b', \\ &(ii)\ \Sigma_b A_y^b = \mathbb{I}, \\ &(iii)\ (A_y^b)^2 = A_y^b = (A_y^b)^\dagger. \end{aligned}$$

Denote $\mathcal{S} = \{S_1, \ldots, S_m\}$ as a finite set of m operators, where each element is a linear combination of products of $\{A_y^b\}$. We define the $nm \times nm$ block Gram matrix G:

$$\begin{aligned} &G = \Sigma_{z,z'=1}^{n} G^{zz'} \otimes |e_z\rangle\langle e_{z'}|, \\ &\text{with, } G_{(i,j)}^{zz'} = \langle \phi_z | S_i^\dagger \cdot S_j | \phi_{z'} \rangle \end{aligned} \tag{20}$$

in which $G_{(i,j)}^{zz'}$ is defined as the inner product of $\langle \phi_z | S_i^\dagger$ and $S_j | \phi_{z'} \rangle$, for all $z, z' \in [n]$, $i, j \in [m]$. $G_{(i,j)}^{zz'}$ is the ij-entry of the matrix $G^{zz'}$ and $\{|e_z\rangle\}_{z=1}^n$ represents the standard orthonormal basis of $\mathbb{R}^n$.

The entries of every sub-block reflect the properties of (i)–(iii). Property (i) implies $\langle \phi_z | A_0^0 A_0^0 | \phi_{z'} \rangle = \langle \phi_z | A_0^0 | \phi_{z'} \rangle$ and $\langle \phi_z | A_0^0 A^\varnothing | \phi_{z'} \rangle = 0$; property (ii) implies that we can introduce the identity operator $\mathbb{I}$ and remove one of the operators; meanwhile the property (iii) implies $\langle \phi_z | A_y^b A_y^{b'} | \phi_z \rangle = (\langle \phi_z | A_y^{b'} A_y^b | \phi_z \rangle)^\dagger$. In addition, due to the overlaps of the receive states are known, we have $\langle \phi_z | \mathbb{I} | \phi_{z'} \rangle = \lambda_{zz'}$.

Then, we can construct a hierarchical structure $\mathcal{S}$:

$$\begin{aligned} \mathcal{S}_1 &= \{\mathbb{I}, A_y^b\} \\ \mathcal{S}_2 &= \mathcal{S}_1 \bigcup \{A_y^b A_{y'}^{b'}\} \\ \mathcal{S}_3 &= \mathcal{S}_2 \bigcup \{A_y^b A_{y'}^{b'} A_y^b\} \\ \mathcal{S}_4 &= \ldots \end{aligned} \tag{21}$$

After the key establishment phase, suppose that Alice and Bob share N raw key bits: Alice can correctly guess NP_{guess} bits of the entire raw key R and only NP_{guess}^k bits through classical post-processing. The SDP problem for maximizing the success probability is as follows:

$$\begin{aligned} \text{maximize} &: P_{guess} \\ \text{subject to} &: \langle \phi_z | \phi_{z'} \rangle = \lambda_{zz'}, \forall z, z' \\ &\quad G \geq 0, \\ &\quad \mathrm{Tr}(F_k G) = f_k, \\ &\quad \mathrm{Tr}(R_k G) = r_k, \\ &\quad p_{\mathrm{det}} \text{ fixed to experimental model} \end{aligned} \tag{22}$$

where F_k's are used to pick up the terms in G which are associated with the observed distributions $p(b|x,y)$ and R_k's are used to pick up the terms in G which are associated with the linear constraints. This SDP is based on Alice and Bob's measurements and the SDP in Section 4.1 is used to calculate P^* in the CHSH test steps on Bob's side. So, these two SDP problems are optimal for different sets of states and measurements, respectively.

4.3. Database Security

Database security implies that even a dishonest Alice cannot obtain more items in Bob's database, that is, Alice only knows one (or a little more) bit of the final key. To get more key bits, an intuitive way for Alice is to adopt the optimal unambiguous state discrimination (USD) measurement strategy [42]. To discriminate between two quantum states, the success probability of USD measurement P_{USD} is bounded by $1 - F(\rho_0, \rho_1)$, where $F(\rho_0, \rho_1)$ is the fidelity between the two states to be distinguished. In our ISD-QPQ protocol, dishonest Alice wants to discriminate $|\phi_0\rangle$ and $|\phi_1\rangle$, the success probability P_{USD} is

$$P_{USD} = 1 - \cos\theta, \tag{23}$$

where $\theta \in [0, \frac{\pi}{2}]$.

ISD-QPQ can resist Alice's joint USD measurement attack. Since our protocol exploits the shift and permutation method in classical post-processing, Alice cannot ensure the information about which qubits contribute to one final key bit. Even if Alice cheats by performing the measurement in step (10) instead of step (7), the success probability P_{USD} can be reduced to $(1 - \cos\theta)^k$ by post-processing. If malicious Alice performs the joint USD measurement, she can gain Δn extra bits. We have the following:

$$\Delta n = N(1 - \cos\theta)^k - N(\frac{\sin^2\theta}{2})^k, \tag{24}$$

where N is the number of entries in the database. For our protocol, we can choose the optimal k to make the probability that dishonest Alice can know more than the expected number of the final key bits and the protocol does not abort very low.

4.4. User Privacy

User privacy denotes that Bob can deduce the retrieval address with higher probability, in other words, Bob has to obtain the raw key bits which are known to Alice. Bob also has to correctly obtain the right key bit value for Alice, otherwise he may provide a false database item to Alice and can be discovered. This case in the QPQ protocol is called cheat-sensitive. All Bob's attacks to infer the retrieval address can be discovered by Alice with a nonzero probability in our protocol; see the details in the following.

In the ISD-QPQ protocol, Alice does not report anything about her measurement outcome. Therefore, dishonest Bob has no information about Alice's measurement basis and outcomes. One possible attack strategy for dishonest Bob is to prepare fake states to receive the corresponding value of Alice's raw key bits. Since Alice chooses the measurement basis chosen randomly and independently of Bob, he has to guess Alice's basis randomly. Assume Bob sends a fake state $|X\rangle = \cos x|0\rangle + \sin x|1\rangle$ to Alice. Alice chooses to measure her qubits with projection measurement. The probability for Alice to obtain the outcomes 0 and 1 are $\sin^2(\frac{\theta}{2} + x)$ and $\sin^2(\frac{\theta}{2} - x)$, respectively. We derive that when $x = \frac{\pi}{4}$, Bob can obtain information on the conclusive results of Alice's bits with an optimal probability. However, Bob would induce some errors by this attack, because he cannot obtain Alice's key bit with certainty. As a result, Bob may give Alice the wrong answer, and she can discover Bob's attack with a certain probability.

Performing special measurements is another attack strategy for dishonest Bob. Assume Bob uses other measurement bases instead of von Neumann measurement on his particle. As shown in [26], Bob will improve the conclusive success probability of key bits, but he will certainly miss the value of the key bit. Thus, Bob will run the risk of being discovered if he tries to obtain Alice's retrieval address. In conclusion, our ISD-QPQ protocol is cheat-sensitive.

5. Simulation Results

We first simulate the relationship between joint probability $\Pr(a_i \oplus b_i = x_i \wedge y_i)$ and choice of θ with different values of τ, as shown in Figure 2. It shows that the joint probability with imperfect sources is always lower than in the ideal case. Then, we can set the value of the black asterisk curve as the joint probability threshold P in the DI-QPQ protocol. By performing the CHSH local test on Bob's side, the protocol can be implemented only when the prepared entanglement state is of a specific form. When the entanglement state is the other form, Bob will abort the protocol. Therefore, Bob can remove his trust in sources. The security of DI-QPQ protocol with imperfect sources is proved.

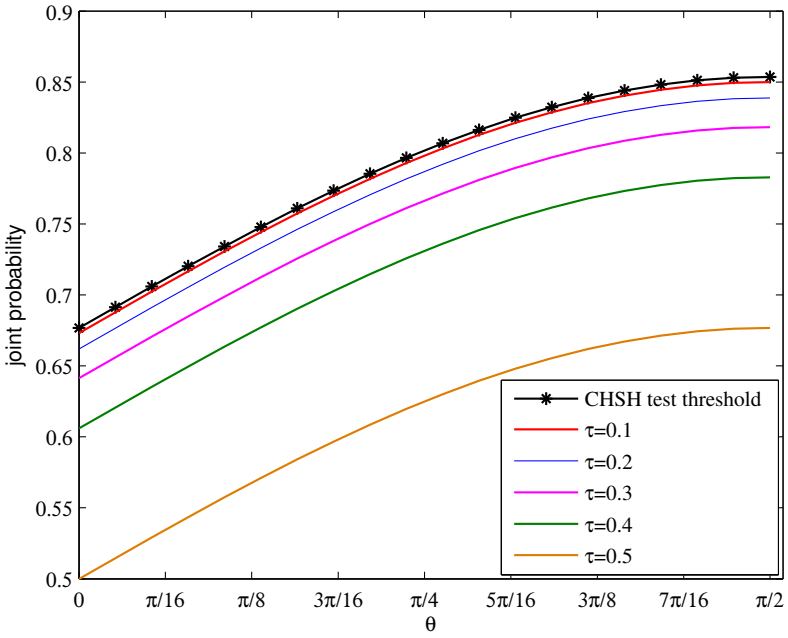

Figure 2. The relationship between $\Pr(a_i \oplus b_i = x_i \wedge y_i)$ and θ of DI-QPQ under different value of τ. The black asterisk line indicates the ideal case in which the sources are perfect. The solid curves from top to bottom, respectively, represent $\tau = 0.1, 0.2, 0.3, 0.4, 0.5$. Assume $|\psi_1\rangle = \frac{\pi}{4}$ and $|\psi_2\rangle = \frac{3\pi}{4}$.

In order to analyze the ISD-QPQ protocol in a realistic detection model, we consider the detection loss rate ϵ. We maximize P^* over the set of compatible probabilities using the first level of the hierarchy; the results of the numerical optimization are shown in Figure 3. When imperfect detectors are considered, the joint probability P^* in the ISD-QPQ protocol is lower than in the previous DI-QPQ protocol. This is expected since imperfect detectors will induce detection loss. In addition, by using the SDP optimization method, we can obtain the CHSH test threshold of our ISD-QPQ protocol with fixed detection loss.

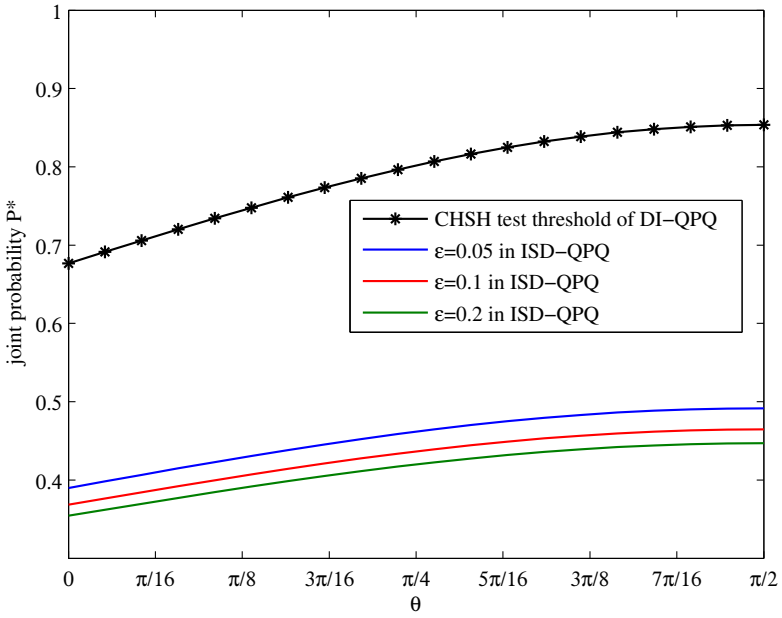

Figure 3. The relationship between P^* and θ of ISD-QPQ under different detection loss ϵ. The black asterisk line indicates the CHSH test threshold of DI-QPQ. The solid curves from top to bottom, respectively, represent $\epsilon = 0.05, 0.1, 0.2$. Assume $|\psi_1\rangle = \frac{\pi}{4}$ and $|\psi_2\rangle = \frac{3\pi}{4}$. The optimization is carried out with the MATLAB 2016a packages YALMIP [43] and the SDP solvers SEDUMI [44].

We simulate the success probability of Alice guessing a bit in the raw key using a realistic model, which includes imperfect sources and detectors. As Alice uses two threshold detectors, there are four possible outcomes when she measures a state. By randomly mapping double clicks to 0 or 1, Alice's measurement realizes a POVM with three outcomes: 0, 1 and inconclusive [45]. Let $P(0,y)$ denote the probability of obtaining the outcomes b. We have the following

$$\begin{aligned} P(0,y) &= C_0(y)N_1(y) + \frac{C_0(y)C_1(y)}{2}, \\ P(1,y) &= C_1(y)N_0(y) + \frac{C_0(y)C_1(y)}{2}, \\ P(\emptyset,y) &= N_0(y)N_1(y), \end{aligned} \tag{25}$$

where $y \in \{0,1\}$ represents the basis choice, C_0 and C_1 (N_0 and N_1) denote the event of detection D_0 and D_1 click (do not click), respectively. The notation $b \in \{0,1,\emptyset\}$ represents the outcomes considering the detection loss. The probability of detecting a signal p_{det} is then given by $p_{det} = P(0,y) + P(1,y)$.

Subsequently, we use the first level of the hierarchy to maximize P_{guess} over the set of compatible probabilities, and the result of the numerical optimization is shown in Figure 4. We compare the success guess probabilities of our ISD-QPQ protocol with the DI-QPQ protocol in [35] and the more recent FDI-QPQ protocol in [31]. It can be clearly seen that our protocol can provide a lower success guess probability than the other two protocols. As a result, the total number of bits consumed is less. By applying the classical post-processing method given in our protocol, Alice knows only roughly one bit in the final key. The results are shown in Figure 5.

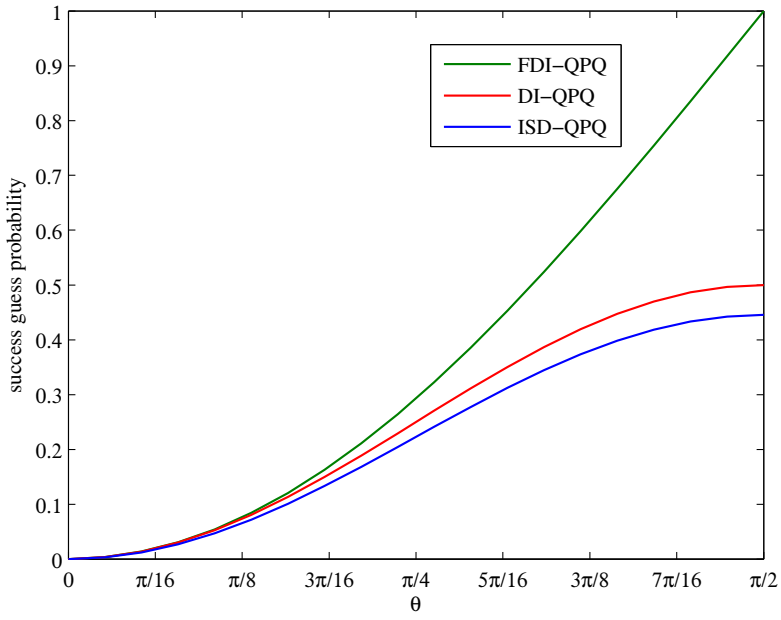

Figure 4. The relationship between success guess probability P_{guess} and θ under different QPQ protocol. The blue curve denotes the simulation result of our ISD-QPQ protocol, the green curve and red curve are the simulation results of the FDI-QPQ and DI-QPQ protocol, respectively. Assume detection loss $\epsilon = 0.1$. The comparison is based on the same experiment parameters.

In addition, to characterize database security, we simulate the relationship between Alice's extra bits and the post-processing parameter k when θ is fixed. The result is shown in Figure 6. We can see that when k increases, the extra bits known for Alice Δn decrease. We choose the optimal k to ensure that Δn is small enough. The larger k implies that more

key bits are consumed. This indicates that the database of our protocol is secure. Compared with the FDI-QPQ protocol in [36], our ISD-QPQ protocol has better performance in terms of database security.

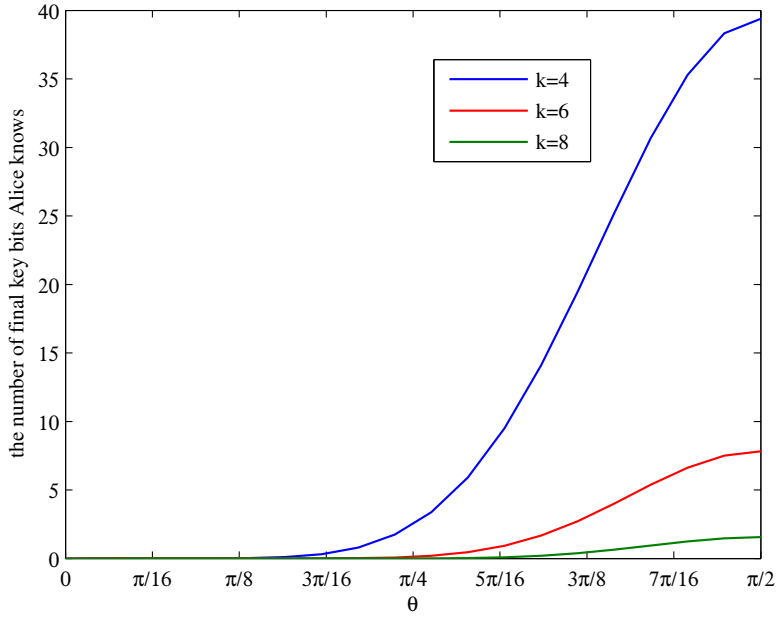

Figure 5. The relationship between the number of final key bits Alice knows and θ with different values of post-processing parameter k in ISD-QPQ protocol. The curve from top to bottom, respectively, represent $k = 4, 6, 8$. Assume the size of database is $N = 1000$.

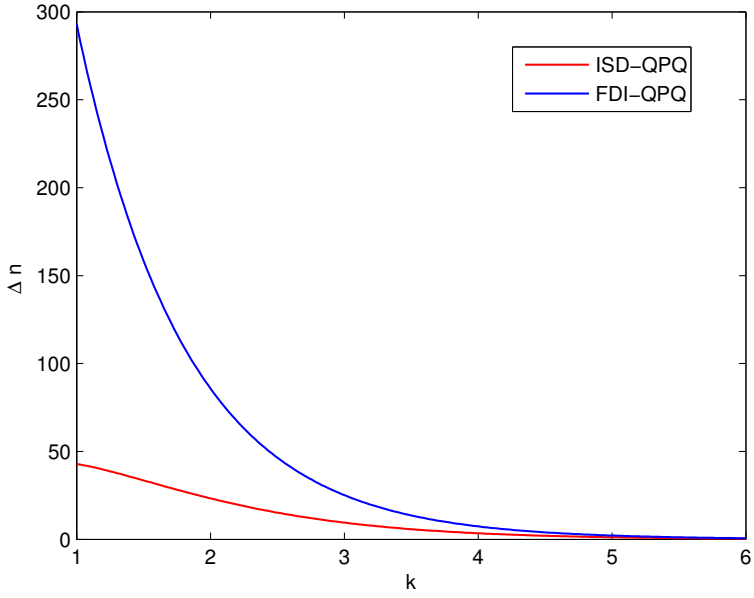

Figure 6. The relationship between extra bits Δn Alice obtained and post-processing parameter k of our ISD-QPQ and FDI-QPQ protocols. Assume the size of database is $N = 1000$ and $\theta = \frac{\pi}{2}$.

Figure 7 shows the relationship between Bob's guess probability for Alice's query item and θ. We can find that Bob's guess probability gradually tends to 0.15 as θ tends to $\frac{\pi}{4}$. Moreover, Bob's guess probability is lower in our protocol than in the FDI-QPQ protocol, which is approximately equal to 0.5 [36]. This simulation results indicates that our ISD-QPQ protocol ensures user privacy against dishonest Bob.

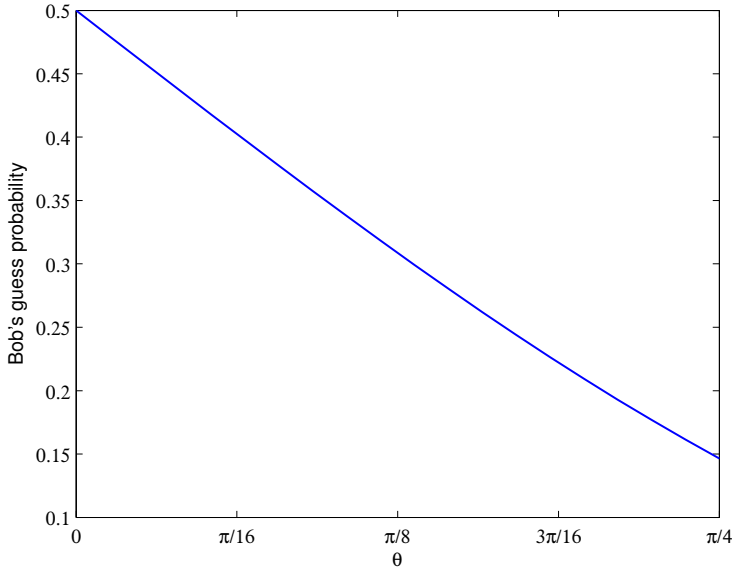

Figure 7. The relationship between Bob's guessing probability and θ of our ISD-QPQ protocol. Assume the size of database is $N = 1000$.

We compare our proposed ISD-QPQ protocol with some existing protocols, as shown in Table 1. We choose the optimal k to ensure that $\Delta n \ll N$ is small enough. Set $N = 1000$ according to the security analysis above.

Table 1. The performance comparison of our ISD-QPQ protocol with Yang-QPQ [26], DI-QPQ [35] and FDI-QPQ [36] protocols.

Protocols	Source	Detector	P_{guess}	Δn
ISD-QPQ	imperfect	with trust loss	0.227	6
Yang-QPQ	trust	trust	0.145	5
DI-QPQ	imperfect	with unit efficiency	0.253	5
FDI-QPQ	imperfect	without noise	0.286	9

Furthermore, the different choice of θ in our QPQ protocol affects security. From Figures 4 and 5, it can be clearly seen that as θ tends to $\frac{\pi}{2}$, the probability of success guessing and the number of final key bits Alice knows gradually increases. With the increase in θ, the database security will decrease. From Figure 7, we can find that Bob's guess probability gradually tends to 0.15 as θ tends to $\frac{\pi}{4}$. We derive that when $x = \frac{\pi}{4}$, Bob can obtain information on the conclusive results of Alice's bits with an optimal probability. Therefore, the optimal choice of θ in our QPQ protocol is $\frac{\pi}{4}$.

Finally, we discuss how the value of γ affects the security and efficiency of our protocol. For each prepared entangled state, Bob divides it into two sets N_{CHSH} and N_{QPQ}. The set N_{CHSH} contains γn entangled states, which is used to conduct the CHSH local test, whereas N_{QPQ} contains $(1-\gamma)n$ entangled states for $0 < \gamma < 1$, which is used to perform private queries. Assuming the size of the database is N and the post-processing parameter k, we have the total number of prepared entangled states $n = \frac{kN}{1-\gamma}$. As the value of γ increases, the efficiency of our protocol will increase. We define the security parameter $t = \frac{\gamma P^* kN}{1-\gamma}$. Taking into account the trade-off between security and efficiency, the optimal value of γ can be obtained by $t \geq 0.5N$. For example, assume $N = 1000$, $k = 3$ and $P^* = 0.78$, and we can choose $\gamma = 0.39$.

6. Conclusions

QKD-based QPQs are the most practical protocols for the SPIR problem. However, most existing protocols assume ideal devices. Considering the practical application of QPQ

protocols, we first analyze the security of the DI-QPQ protocol with imperfect sources and detectors, which requires the assumption that all detectors have unit efficiency. To overcome this drawback, we propose our ISD-QPQ protocol with imperfect sources and detectors. Performing the local CHSH test, Bob can check that the states are of the desired form. We prove the security and correctness of the ISD-QPQ protocol. By constructing the SDP optimization problem with the NPA method, we derive the CHSH test threshold and prove the correctness of our protocol. With this SDP method, detailed characterization of the quantum signals and measurements, including their dimensions, is no longer required in the analysis. Furthermore, we use the shift and permutation post-processing method to further improve the security of our protocol.

The simulation results show that the protocol can be implemented only when the prepared entanglement state is of a specific form. Therefore, Bob can remove his trust in sources. When simulating the success guess probability and the number of final key bits Alice knows, we find that our protocol consumes fewer bits than the FDI-QPQ protocol and DI-QPQ protocol, that is, our protocol has higher efficiency. The security of database and user privacy are analyzed. Our ISD-QPQ protocol has higher security than the FDI-QPQ protocol in terms of both database security and user privacy. In addition, we discuss the optimal choice of θ and γ.

Furthermore, by replacing the QPQ steps with other entanglement-based QPQ protocol, our scheme can be used for any entanglement-based QPQ protocol to remove trust on devices. However, it remains an open problem to remove the assumption that Bob's device has a trusted loss value.

Author Contributions: Conceptualization, L.L.; methodology, L.L.; software, Q.D. and X.G.; validation, L.L. and Q.D.; formal analysis, L.L. and Q.D.; investigation, L.L.; writing—original draft preparation, L.L.; writing—review and editing, L.L. and Q.D.; visualization, Q.D. and X.G.; funding acquisition, L.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Youth Program of Shaanxi Provincial Department of Science and Technology (2024JC-YBQN-0630).

Data Availability Statement: The original contributions presented in the study are included in the article; further inquiries can be directed to the corresponding author.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

PIR	Private information retrieval
SPIR	Symmetric private information retrieval
QKD	Quantum key distribution
PQ	Private query
QPQ	Quantum private query
DI	Device-independent
NPA	Navascués–Pironio–Acín
SDP	Semi-definite programming
LSA	Low-shift and addition
FDI-QPQ	Full DI certification quantum private query
ISD-QPQ	Quantum private query with imperfect sources and detectors
POVM	Positive operator value measurement
USD	Unambiguous state discrimination

References

1. Chor, B.; Kushilevitz, E.; Goldreich, O.; Sudan, M. Private Information Retrieval. *J. ACM* **1998**, *45*, 968–981. [CrossRef]
2. Chor, B.; Goldreich, O.; Kushilevitz, E.; Sudan, M. Private information retrieval. In Proceedings of the 36th Annual Symposium on Foundations of Computer Science, Milwaukee, WI, USA, 23–25 October 1995; IEEE: New York, NY, USA, 1995; p. 41.
3. Gertner, Y.; Ishai, Y.; Kushilevitz, E.; Malkin, T. Protecting Data Privacy in Private Information Retrieval Schemes. *J. Comput. Syst. Sci.* **2000**, *60*, 592–629. [CrossRef]
4. Wang, S. Symmetric private information retrieval supported by quantum-secure e key-exchange network. *Light. Sci. Appl.* **2022**, *11*, 301. [CrossRef] [PubMed]
5. Hayashi, M.; Song, S. Unified Approach to Secret Sharing and Symmetric Private Information Retrieval With Colluding Servers in Quantum Systems. *IEEE Trans. Inf. Theory* **2023**, *69*, 6537–6563. [CrossRef]
6. Lo, H. Insecurity of quantum secure computations. *Phys. Rev. A* **1997**, *56*, 1154–1162. [CrossRef]
7. Lipmaa, H. An Oblivious Transfer Protocol with Log-Squared Communication. In Proceedings of the International Conference on Information Security, Singapore, 20–23 September 2005; pp. 357–371.
8. Chou, T.; Orlandi, C. The Simplest Protocol for Oblivious Transfer. In Proceedings of the International Conference on Cryptology and Information Security in Latin America, Guadalajara, Mexico, 23–26 August 2015; pp. 40–58.
9. Kon, W.Y.; Lim, C.C.W. Provably Secure Symmetric Private Information Retrieval with Quantum Cryptography. *Entropy* **2021**, *23*, 54. [CrossRef]
10. Gong, L.H.; Li, M.L.; Cao, H.; Wang, B. Novel semi-quantum private comparison protocol with Bell states. *Laser Phys. Lett.* **2024**, *21*, 055209. [CrossRef]
11. Ostrovsky, R.; Iii, W.E.S. A Survey of Single-Database Private Information Retrieval: Techniques and Applications. *Int. Workshop Public Key Cryptogr.* **2007**, *4450*, 393–411.
12. Giovannetti, V.; Lloyd, S.; Maccone, L. Quantum private queries. *Phys. Rev. Lett.* **2008**, *100*, 230502. [CrossRef]
13. Olejnik, L. Secure quantum private information retrieval using phase-encoded queries. *Phys. Rev. A* **2011**, *84*, 3242–3244. [CrossRef]
14. Giovannetti, V.; Lloyd, S.; Maccone, L. Quantum Private Queries: Security Analysis. *IEEE Trans. Inf. Theory* **2010**, *56*, 3465–3477. [CrossRef]
15. Jakobi, M.; Simon, C.; Gisin, N.; Bancal, J.D.; Branciard, C.; Walenta, N.; Zbinden, H. Practical private database queries based on a quantum-key-distribution protocol. *Phys. Rev. A* **2011**, *83*, 022301. [CrossRef]
16. Yin, H.L.; Chen, T.Y.; Yu, Z.W.; Liu, H.; You, L.X.; Zhou, Y.H.; Chen, S.J.; Mao, Y.; Huang, M.Q. Measurement-Device-Independent Quantum Key Distribution Over a 404km Optical Fiber. *Phys. Rev. Lett.* **2016**, *117*, 190501. [CrossRef]
17. Lucamarini, M.; Yuan, Z.L.; Dynes, J.F.; Shields, A.J. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. *Nature* **2018**, *557*, 7705. [CrossRef]
18. Wang, W.; Wang, R.; Hu, C.; Zapatero, V.; Qian, L.; Qi, B.; Curty, M.; Lo, H.K. Fully Passive Quantum Key Distribution. *Phys. Rev. Lett.* **2023**, *130*, 220801. [CrossRef]
19. Makarov, V.; Abrikosov, A.; Chaiwongkhot, P.; Fedorov, A.K.; Huang, A.; Kiktenko, E.; Petrov, M.; Ponosova, A.; Ruzhitskaya, D.; Tayduganov, A. Preparing a commercial quantum key distribution system for certification against implementation loopholes. *Phys. Rev. Appl.* **2023**, *22*, 044076. [CrossRef]
20. Zhou, L.; Lin, J.; Jing, Y.; Yuan, Z. Twin-field quantum key distribution without optical frequency dissemination. *Nat. Commun.* **2023**, *14*, 928. [CrossRef]
21. Zhou, Y.; Yin, Z.Q.; Shan, Y.G.; Wang, Z.H.; Wang, S.; Chen, W.; Guo, G.C.; Han, Z.F. Phase-error-rate analysis for quantum key distribution with phase postselection. *Phys. Rev. A* **2024**, *109*, 022416. [CrossRef]
22. Zeng, P.; Zhou, H.; Wu, W.; Ma, X. Mode-pairing quantum key distribution. *Nat. Commun.* **2022**, *13*, 3903. [CrossRef]
23. Chen, Y.A.; Zhang, Q.; Chen, T.Y.; Cai, W.Q.; Liao, S.K.; Zhang, J.; Chen, K.; Yin, J.; Ren, J.G.; Chen, Z. An integrated space-to-ground quantum communication network over 4,600 kilometres. *Nature* **2021**, *589*, 214–219. [CrossRef]
24. Zhou, S.; Xie, Q.M.; Zhou, N.R. Measurement-free mediated semi-quantum key distribution protocol based on single-particle states. *Laser Phys. Lett.* **2024**, *21*, 065207. [CrossRef]
25. Gao, F.; Liu, B.; Huang, W.; Wen, Q.Y. Postprocessing of the oblivious key in quantum private query. *IEEE J. Sel. Top. Quantum Electron.* **2015**, *21*, 6600111. [CrossRef]
26. Yang, Y.G.; Sun, S.J.; Xu, P.; Tiang, J. Flexible protocol for quantum private query based on B92 protocol. *Quantum Inf. Process.* **2014**, *13*, 805–813. [CrossRef]
27. Wei, C.Y.; Wang, T.Y.; Gao, F. Practical quantum private query with better performance in resisting joint-measurement attack. *Phys. Rev. A* **2016**, *93*, 042318. [CrossRef]
28. Wei, C.Y.; Cai, X.Q.; Wang, T.Y.; Qin, S.J.; Gao, F.; Wen, Q.Y. Error Tolerance Bound in QKD-Based Quantum Private Query. *IEEE J. Sel. Areas Commun.* **2020**, *38*, 517–527. [CrossRef]

29. Gao, F.; Qin, S.J.; Huang, W.; Wen, Q.Y. Quantum private query: A new kind of practical quantum cryptographic protocol. *Sci. China Phys. Mech. Astron.* **2019**, *62*, 70301. [CrossRef]
30. Yang, Y.G.; Yang, P.Z.; Xu, G.B.; Jiang, D.H.; Zhou, Y.H.; Shi, W.M.; Li, D. Error-Tolerant Measurement-Device-Independent Quantum Private Queries of Blocks. *Int. J. Theor. Phys.* **2024**, *63*, 1–13. [CrossRef]
31. Basak, J. Multi-user semi-device independent quantum private query. *Quantum Inf. Process.* **2023**, *22*, 276. [CrossRef]
32. Wei, C.Y.; Cai, X.Q.; Liu, B.; Wang, T.; Gao, F. A generic construction of quantum-oblivious-key-transfer-based private query with ideal database security and zero failure. *IEEE Trans. Comput.* **2018**, *67*, 2–8. [CrossRef]
33. Liu, L.; Guo, F.Z.; Wen, Q.Y. Practical decoy-state quantum private queries against joint-measurement attack under weak coherent pulse sources. *Quantum Inf. Process.* **2021**, *20*, 392. [CrossRef]
34. Liu, B.; Xia, S.; Xiao, D.; Huang, W.; Xu, B.; Li, Y. Decoy-state method for quantum-key-distribution-based quantum private query. *Sci. China Phys. Mech. Astron.* **2022**, *65*, 240312. [CrossRef]
35. Maitra, A.; Paul, G.; Roy, S. Device-independent quantum private query. *Phys. Rev. A* **2017**, *95*, 042344. [CrossRef]
36. Basak, J.; Chakraborty, K.; Maitra, A.; Maitra, S. Improved and Formal Proposal for Device Independent Quantum Private Query. *J. Phys. A Math. Theor.* **2024**, *57*, 085302. [CrossRef]
37. Basak, J.; Chakraborty, K. Fully device independent quantum private query. *Adv. Math. Commun.* **2024**, *19*, 494–545. [CrossRef]
38. Lim, C.C.W.; Portmann, C.; Tomamichel, M.; Renner, R.; Gisin, N. Device-Independent Quantum Key Distribution with Local Bell Test. *Phys. Rev. X* **2013**, *3*, 031006. [CrossRef]
39. Navascués, M.; Pironio, S.; Acín, A. Bounding the set of Quantum Correlations. *Phys. Rev. Lett.* **2007**, *98*, 010401. [CrossRef]
40. Liu, L.; Wang, Y.; Lavie, E.; Ricou, A.; Wang, C.; Guo, F.Z.; Lim, C.C.W. Practical quantum key distribution with non-phase-randomized coherent states Authors. *Phys. Rev. Appl.* **2019**, *12*, 024048. [CrossRef]
41. Wang, Y.; Primaatmaja, I.W.; Lavie, E.; Varvitsiotis, A.; Lim, C.C.W. Characterising the correlations of prepare-and-measure quantum networks. *NPJ Quantum Inf.* **2019**, *5*, 17. [CrossRef]
42. Gaidash, A.; Kozubov, A.; Miroshnichenko, G. Countermeasures for advanced unambiguous state discrimination attack on quantum key distribution protocol based on weak coherent states. *Phys. Scr.* **2019**, *94*, 12. [CrossRef]
43. Löfberg, J. YALMIP: A Toolbox for Modeling and Optimization in MATLAB. In Proceedings of the IEEE International Conference on Robotics and Automation (IEEE Cat. No. 04CH37508), Taipei, Taiwan, 2–4 September 2004; pp. 284–289.
44. Sturm, J.F. Using SeDuMi 1.02, A Matlab toolbox for optimization over symmetric cones. *Optim. Methods Softw.* **1999**, *11*, 625–653. [CrossRef]
45. Inamori, H.; Lütkenhaus, N.; Mayers, D. Unconditional Security of Practical Quantum Key Distribution. *Eur. Phys. J. D* **2007**, *41*, 599. [CrossRef]