IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received July 2, 2019, accepted July 19, 2019, date of publication July 23, 2019, date of current version August 14, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2930548

QKD-Based Quantum Private Query Protocol in the Single-Photon Interference Communication System

BIN LIU[1,2], ZHI-FENG GAO[1], DI XIAO[1], WEI HUANG[1,2], ZHI-QING ZHANG[3], YANG LI[2], AND BING-JIE XU[2]

[1]Postdoctoral Station of Computer Science and Technology, College of Computer Science, Chongqing University, Chongqing 400044, China
[2]Science and Technology on Communication Security Laboratory, Institute of Southwestern Communication, Chengdu 610041, China
[3]Chongqing University—University of Cincinnati Joint Co-op Institute, Chongqing 400044, China

Corresponding authors: Bin Liu (liubin31416@gmail.com), Wei Huang (huangwei096505@aliyun.com), and Bing-jie Xu (xbjpku@163.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 61702061, Grant 61702469, Grant 61771439, Grant 61572089, and Grant 61802037, in part by the China Postdoctoral Science Foundation Funded Project under Grant 2017M612912, in part by the Chongqing Postdoctoral Science Foundation Funded Project under Grant Xm2017041, in part by the Fundamental Research Funds for the Central Universities under Grant 106112016CDJXY180001 and Grant 2019CDJSK04XK23, in part by the National Cryptography Development Fund under Grant MMJJ20170120, in part by the Sichuan Youth Science and Technology Foundation under Grant 2017JQ0045, and in part by the Natural Science Foundation Project of CQ under Grant cstc2017rgzn-zdyfX0042.

ABSTRACT In this paper, we propose a quantum-key-distribution-based quantum private query protocol (QKD-based QPQ) utilizing the uncertainty relation of the photon path and the interference result in the single-photon interference circuit. The proposed protocol is loss-tolerant and easy to be realized in the quantum communication systems based on single-photon interference. Without any assumption on the dishonest party's computation ability, we prove that the dishonest user can only steal a little more than one item from the database, and any dishonest action of the database would be found by the user with a nonzero probability. Compared with other QKD-based QPQ protocols utilizing single-photon interference, the proposed protocol uses less quantum devices, which means the costs of the proposed protocol is lower.

INDEX TERMS Quantum information processing, quantum key distribution, quantum private query.

I. INTRODUCTION

The applications of quantum mechanics have brought great changes to information processing. On one hand, quantum computation has enormous potential to accelerate the solution of many important problems such as factoring large number [1] and searching a database [2]. On the other hand, quantum communication can achieve higher security and lower communication complexity in some communication tasks such as key distribution and secure multi-party computation. Since the first quantum key distribution (QKD) protocol has been proposed in 1984 [3], quantum communication has developed rapidly in both theory and experiment. Various of quantum cryptographic protocols have been proposed and been proved secure in theory, such as QKD [4], [5], quantum secure direct communication [6]–[11], quantum secret sharing [12]–[17], and so on [18], [19]. And some of the above protocols have succeeded in experiments and even practical applications. Meanwhile, analysis and protocols towards practical quantum communication systems have also been studied adequately.

A symmetrically private information retrieval (SPIR) protocol is a protocol that allows a user to retrieve a certain item from a database without revealing which item is retrieved and symmetrically the user may not learn any item other than the one she requested. Quantum private query (QPQ) is the application of quantum mechanics in the SPIR problem. With some necessary relaxations the fundamental assumptions, QPQ can provide information-theoretic security for the SPIR protocols. Furthermore, QPQ can also reduce the communication complexity and the computation complexity compared with the classical SPIR protocols. QPQ protocols have been first designed based on a quantum unitary operation which contains the information of the whole database. In the above protocols, the user sends the querying states to the database, then the database encodes the information of

The associate editor coordinating the review of this manuscript and approving it for publication was SK Hafizul Islam.

the queried item into the querying state by performing the above operations and sends it back to the user, and with some necessary additional systems in some protocols. This method can protect the privacies of the user and database against the adversaries with unlimited computation ability. Meanwhile it can also reduce both the communication complexity and the computation complexity. However, it is very difficult to implement with today's technology.

A practical way to achieve QPQ is based on the technology of quantum key distribution, which is called QKD-based QPQ or quantum-oblivious-key-transfer-based QPQ. In QKD-based QPQ protocols, the user and the database first generate an oblivious key where the database knows each of its bits but the user only knows a little more than one bit. And then they complete the private query utilizing the oblivious key. This method is much easier to implement than the QPQ protocols based on unitary operations and draws a lot of attention. This practical type of QPQ can be implemented utilizing various kinds of quantum communication technologies, for example ones based on the single-photon interference. In this paper, we propose a QKD-based QPQ protocol utilizing the uncertainty relation of the photon path and the interference result in the single-photon interference circuit. The proposed protocol needs less quantum communication devices than other QPQ protocols utilizing the technology of single-photon interference. And we also proved the security of the proposed protocol from both the user's privacy and the database's privacy.

This paper is organized as follows. Next section gives detailed discussions of the existing works on QPQ. The prearrangement knowledge and the basic hypothesis of the proposed protocol are introduced in section III. Section IV describes the detailed processes and the correctness analysis of the proposed protocol. The security analysis and the comparison of the proposed protocol and other QPQ protocol utilizing the technology of single-photon interference are given section V. And a brief conclusion is given in section VI.

II. RELATED WORKS

There are mainly two types of QPQ protocols. One is based on the oracle, which is a unitary operation in which the whole database is encoded into. The other is based on quantum oblivious key, which can be distributed by the technology of QKD. Considering that the security of all the classical SPIR protocols is based on computation complexity, both the two type of QPQ protocols have improved the security of SPIR problem compared with the classical protocols.

The oracle-based QPQ can also reduce the communication complexity and the computation complexity of the SPIR problem. The first QPQ protocol is proposed by Giovannetti et al. in 2008 (G-protocol), which is base on the oracle [20]. In the above protocol, the user encodes the information of which item he is interested in in a query state, and sends it and a detection state to the database in a random order, where the detection state is in the superposition of the query state and the state $|0\rangle^{\otimes m}$. If the database attempts to steal user's privacy, the user would find out his dishonest action with the probability 1/4. And the dishonest user can get 2 items of the database if he gives up to detect the honesty of the database. In 2010, Giovannetti et al. analyzed the security of their protocol in detail [21]. In 2011, Olejnik proposed a QPQ protocol in which the user only need to send the query state to the database, however, the security of the database's privacy has not been analyzed [22]. Therefore, Olejnik's protocol is just a private information retrieval protocol, but not a SPIR one. In 2014, Yu and Qiu [23] proposed a QPQ protocol utilizing entangled query state instead of superposed states in Olejnik's protocol. Compared to Olejnik's protocol, Yu's protocol can prevent a dishonest-but-conscientious database from stealing user's privacy. Experiments for small databases have been performed by De Martini *et al.* [24] and Wang *et al.* [25] in 2009 and 2011, respectively. However, for large databases, this method becomes too difficult to realize with today's technology.

In 2011, Jakobi et al. proposed a practical QPQ protocol [26] (J-protocol) based on a variant of the QKD protocol proposed by Scarani et al. (SARG04 protocol) [27]. The quantum processes in this QPQ protocol are the same with that in the QKD protocol, therefore, J-protocol can be realized with today's quantum communication technology in principle. Besides, J-protocol can protect the user's privacy better than the oracle-based QPQ protocols and can tolerate the channel loss while the oracle-based QPQ protocols cannot. However, the communication complexity of J-protocol is larger than the oracle-based QPQ protocols. The next year, Gao et al. improved J-protocol [28]. The improved protocol is more flexible in the balance of the two participants' privacies and the balance of the failure probability and the communication complexity, which can meet the complex requirements better in the practical applications. Because of the better security and practicability that J-protocol and Gao's improved version have achieved, this new type of QPQ has attracted lots of attention immediately. Some scholars focused on the classical post-processes used in the QKD-based QPQ protocols [29], [30], including the process of raw oblivious key dilution, the process of error correction and so on. The others have proposed various QKD-based QPQ protocols utilizing different quantum communication technologies [31]–[41].

Single-photon interference is an important technology for quantum communications. Based on the basic ideal of encoding information in the phase difference of the pluses in single-photon interference circuit, scholars have proposed many kinds of quantum communication protocols with different characteristics and applications. As for QPQ utilizing the technology of single-photon interference, Zhang et al. proposed a counterfactual QKD-based QPQ protocol in 2013 [40]. In 2015, Liu et al. proposed a QKD-based QPQ protocol based on the RRDPS-QKD protocol, which is the first QKD-based QPQ protocol with zero failure probability [37]. The next year, two QKD-based QPQ protocols [41] with simpler interference circuits have been proposed by Xu et al. In this paper, we further simplify the circuit of the

QKD-based QPQ protocol utilizing the technology of single-photon interference, by using less quantum communication devices than the above three protocols, which implies that the proposed QPQ protocol is easier to realize and with lower costs.

III. PRELIMINARIES

In this section, we will introduce some basic concepts in this paper, including the basic assumptions of QPQ and QKD-based QPQ, the common processes of QKD-based QPQ protocols, and the encoding mode used in the newly proposed protocol below.

A. BASIC ASSUMPTIONS OF QPQ

QPQ is the quantum solution for SPIR problem. Two parties are related in QPQ protocols, the owner of a database composed of a certain number of items, and the user who wants to query one of the items in a certain position.

Different from the classical protocols for SPIR problem which can only achieve computational security, QPQ is considered to be more secure since its security is based on the physical principles. However, as one of the two-party secure computation problems, the perfect protocol for SPIR problem does not exist even in quantum cryptography. In fact, the basic assumptions for QPQ have been relaxed compared with the classical SPIR problem. In a perfect SPIR protocol, the database could not get any information about which item the user is interested in; and the user could get no information about the database other than the item he queried. While QPQ has relaxed the security assumptions on both sides of the database's security and the user's privacy in the following ways. For the security of the database, QPQ allows dishonest users to get a little more items of the database, for example, the dishonest user can get 2 items including the one he is querying in G-protocol, and about 2-5 items in J-protocol. And for the privacy of the user, QPQ protocols are cheat-sensitive, which means that the user would discover the dishonest actions of the database with a no-zero probability provided the database attempts to steal the user's privacy.

B. PROCESSES OF QKD-BASED QPQ PROTOCOL

QKD-based QPQ protocol utilizing the technology of QKD to generate an oblivious key. Generally, QKD-based QPQ protocols can be generally divided into the following three Stages.

- **Raw oblivious key distribution**. In this stage, the database and the user, utilizing the technology of QKD, generate a raw oblivious key which meets the following conditions.

  [R1] The database has full information of the raw oblivious key.

  [R2] For each bit of the raw oblivious key, the user knows its value with a certain probability.
- **Final oblivious key generation**. In this stage, the database and the user together process the raw oblivious key into the final oblivious key which meets the following conditions.

  [F1] The database has full information of the final oblivious key.

  [F2] The user knows a little more bits than one of the final oblivious key, usually 2-5 bits.
- **Private query**. With the final oblivious key, the database and the user perform the task of private query.

C. THE ENCODING MODE

The proposed protocol here utilizes the uncertainty between the observations of the photon path and the interference result of two pulses in the single-photon interference (See in Fig. 1).

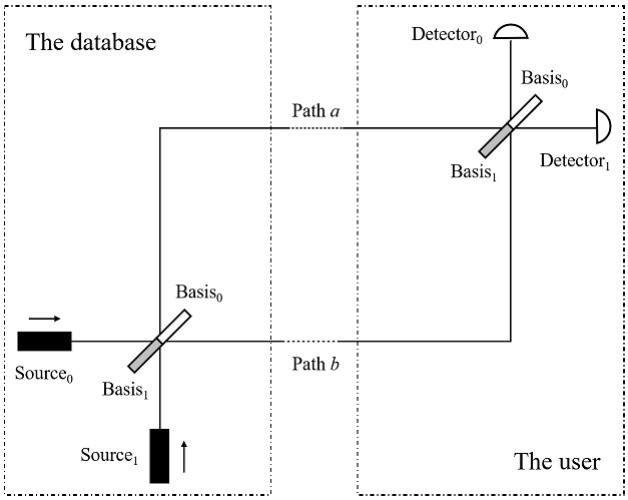

FIGURE 1. The interference circuit utilized in the proposed protocol.

Two bases are used in the communication system. Basis$_0$ is a lens which always transmits the coming light pulse but never reflect it; when the database (the user) chooses Basis$_0$, he prepares (measures) the signal in the path of the transmitted photon. Basis$_1$ is a beam splitter which transmits the coming light pulse with the probability 50% and never reflect it with the same probability; when the database (the user) chooses Basis$_1$, he prepares (measures) the signal in the interference result of the two pulses. When the database chooses Basis$_0$ (Basis$_1$), he encodes the information in the photon path (the interference result). And when the user chooses Basis$_0$ (Basis$_1$), he decodes the information from the photon path (the interference result).

When the protocol starts, the database chooses to emit a signal photon into the circuit from Source$_0$ to encode a classical bit 0, or from Source$_1$ to encode a classical bit 1. The user records a classical bit 0 for the present signal if Detector$_0$ clicks, and 1 if Detector$_1$ clicks. When a single photon emitted from Source$_0$ passes through the database's beam splitter, the state of the position of the photon changes from $|S_0\rangle$ to

$$|P_{01}\rangle = U_1|S_0\rangle = \frac{1}{\sqrt{2}}|b\rangle + \frac{\mathrm{i}}{\sqrt{2}}|a\rangle, \tag{1}$$

where $|S_0\rangle$, $|a\rangle$ and $|b\rangle$ represent that the photon is in the path connected to Source$_0$, Path a, and Path b, respectively, and U_1 describes the operation when a photon passes the beam splitter. And for the single photon emitted from Source$_1$, the position state changes from $|S_0\rangle$ to

$$|P_{11}\rangle = U_1|S_1\rangle = \frac{\mathrm{i}}{\sqrt{2}}|b\rangle + \frac{1}{\sqrt{2}}|a\rangle, \tag{2}$$

where $|S_1\rangle$ represents that the photon is in the path connected to Source$_1$. Obliviously, when a photon from Source$_0$ (Source$_1$) passes the lens at the database's side, the state changes from $|S_0\rangle$ to $|P_{00}\rangle = |b\rangle$ (from $|S_1\rangle$ to $|P_{01}\rangle = |a\rangle$). Similarly, when a photon in Path a (Path b) passes the lens at the user's side, the state changes from $|a\rangle$ to $|P_{a0}\rangle = |D_1\rangle$ (from $|b\rangle$ to $|P_{b0}\rangle = |D_0\rangle$), where $|D_0\rangle$ and $|D_1\rangle$ represent the path leading to Detector$_0$ and Detector$_1$, respectively. And when a photon in Path a passes the beam splitter at the user's side, the position state changes from $|a\rangle$ to

$$|P_{a1}\rangle = U_1|a\rangle = \frac{\mathrm{i}}{\sqrt{2}}|D_0\rangle + \frac{1}{\sqrt{2}}|D_1\rangle. \tag{3}$$

And for a photon in Path b, the state changes from $|b\rangle$ to

$$|P_{b1}\rangle = U_1|b\rangle = \frac{1}{\sqrt{2}}|D_0\rangle + \frac{\mathrm{i}}{\sqrt{2}}|D_1\rangle. \tag{4}$$

For the communication process utilizing the above circuit, there are four different cases according to the bases the database and the user choose.

C_{00} If the database and the user both choose Basis$_0$, Detector$_0$ (Detector$_1$) would click provided the photon is emitted from Source$_0$ (Source$_1$). And in this case, the user will get **an identical bit** with the one the database has encoded.

C_{01} If the database chooses Basis$_0$ and the user chooses Basis$_1$, the photon would be reflected or transmitted randomly by the user's beam splitter no matter which path it passes, and Detector$_0$ and Detector$_1$ would click randomly. In this case, the user will get **a random bit** which is independent with the database's bit.

C_{10} If the database chooses Basis$_1$ and the user chooses Basis$_0$, the photon would be reflected or transmitted randomly by the database's beam splitter and passes to path a or path b randomly, and Detector$_0$ and Detector$_1$ would click randomly. In this case, the user will get **a random bit** which is independent with the database's bit.

C_{11} If the database and the user both choose Basis$_1$, Detector$_1$ (Detector$_0$) would click provided the photon is emitted from Source$_0$ (Source$_1$). And in this case, the user will get **an opposite bit** with the one the database has encoded. Specifically, if the database emits a single-photon signal from Source$_0$, when it has passed the beam splitter, the photon position state becomes $|P_{01}\rangle$ in Equation 1. When the two pulses in the two paths have passed the user's beam splitter together, the photon position state becomes

$$\begin{aligned}|P_{011}\rangle &= \frac{1}{\sqrt{2}}|P_{b1}\rangle + \frac{\mathrm{i}}{\sqrt{2}}|P_{a1}\rangle \\ &= \frac{1}{\sqrt{2}}(\frac{1}{\sqrt{2}}|D_0\rangle + \frac{\mathrm{i}}{\sqrt{2}}|D_1\rangle) \\ &\quad + \frac{\mathrm{i}}{\sqrt{2}}(\frac{\mathrm{i}}{\sqrt{2}}|D_0\rangle + \frac{1}{\sqrt{2}}|D_1\rangle) \\ &= \mathrm{i}|D_1\rangle. \end{aligned} \tag{5}$$

Similarly, if the database emits a single photon signal from Source$_1$, the photon position state finally becomes

$$\begin{aligned}|P_{111}\rangle &= \frac{1}{\sqrt{2}}|P_{a1}\rangle + \frac{\mathrm{i}}{\sqrt{2}}|P_{b1}\rangle \\ &= \frac{1}{\sqrt{2}}(\frac{\mathrm{i}}{\sqrt{2}}|D_0\rangle + \frac{1}{\sqrt{2}}|D_1\rangle) \\ &\quad + \frac{\mathrm{i}}{\sqrt{2}}(\frac{1}{\sqrt{2}}|D_0\rangle + \frac{\mathrm{i}}{\sqrt{2}}|D_1\rangle) \\ &= \mathrm{i}|D_0\rangle. \end{aligned} \tag{6}$$

The position states of the photon in the above four cases are summarized in Table 2. From Table 2, we can get the conclusion that if the database and the user choose the same basis, the user could decode the bit the database has encoded in the signal. And if the database and the user choose different bases, the user would get a random bit and knows nothing about the bit the database has encoded.

IV. PROTOCOL

Utilizing the encoding mode described in subsection III-C, we propose a QKD-based QPQ protocol in this section. As most of the previous protocols, there are three stages in the proposed protocol.

A. RAW OBLIVIOUS KEY DISTRIBUTION

The first stage is **raw oblivious key distribution stage**, which contains all the quantum processes of the protocol. When the database and the user set up a communication circuit as in Table 1, they can perform the first stage. Before the quantum process of the raw key distribution, the database generates two random and secret strings S and DA with the same length, where S controls the photon comes from which source and the bits of DA are used to control the encoding basis. And the user also generates a random and secret string U with the same length, which is used to control the decoding basis. Suppose the s_i, d_i and u_i are the ith bit of S, DA and U respectively. For the ith signal, they attempt to generate a key bit as follows. Note that the generated raw oblivious key would be a substring of DA in the following processes.

1.1 The database emits a single photon into the circuit from Source$_{s_i}$ and chooses basis$_{d_i}$ to encode s_i.

1.2 The user chooses basis$_{u_i}$ to decode the information encoded in the coming signal.

1.3 The user records a bit $k_i = r_i \oplus u_i$ if Detector$_{r_i}$ clicks, where $\oplus$ represents the plus module 2. Then the user

TABLE 1. The position states of the photon in different cases.

$\|S_x\rangle$	D_y	$\|P_{xy}\rangle$	U_z	$\|P_{xyz}\rangle$
$\|S_0\rangle$	0	$\|b\rangle$	0	$\|D_0\rangle$
			1	$\frac{\|D_0\rangle+\mathrm{i}\|D_1\rangle}{\sqrt{2}}$
$\|S_1\rangle$	0	$\|a\rangle$	0	$\|D_1\rangle$
			1	$\frac{\mathrm{i}\|D_0\rangle+\|D_1\rangle}{\sqrt{2}}$
$\|S_0\rangle$	1	$\frac{\mathrm{i}\|a\rangle+\|b\rangle}{\sqrt{2}}$	0	$\frac{\|D_0\rangle+\mathrm{i}\|D_1\rangle}{\sqrt{2}}$
			1	$\mathrm{i}\|D_1\rangle$
$\|S_1\rangle$	1	$\frac{\|a\rangle+\mathrm{i}\|b\rangle}{\sqrt{2}}$	0	$\frac{\mathrm{i}\|D_0\rangle+\|D_1\rangle}{\sqrt{2}}$
			1	$\mathrm{i}\|D_0\rangle$

Here, $|S_x\rangle$ represents the choice of the database on the sources. D_y (U_z) represents the database's (the user's) choice of the basis, $|P_{xy}\rangle$ represents the position state of the photon in public channel and $|P_{xyz}\rangle$ represents the position state of the photon before it arrives at the detectors.

informs the database that he has measured the *i*th signal successfully.

1.4 When the database receives the notification that the user has measured the *i*th signal successfully, he records a bit "d_i" in the raw oblivious key RK_d, and publishes a set of two ordered pairs $\{< s_i, d_i >, < x, d_i \oplus 1 >\}$, where x is a random bit and the order of the elements in the set is random.

1.5 When the user receives the above set, he compares the set and the order pair $< k_i, u_i >$. If $< k_i, u_i > \notin \{< s_i, d_i >, < x, d_i \oplus 1 >\}$, with the probability 25%, the user records a bit "$u_i \oplus 1$" in the raw oblivious key RK_u, otherwise, he records an ambiguous bit "?" in the raw oblivious key RK_u.

After the processes above, the database and the user have generated a raw oblivious key where the database has full information and the user only knows the values of a quarter of its bits.

Now we analyze the correctness of the above processes. Obliviously, RK_d is a substring of DA since RK_d contains the bits where the encoding signal has been successfully measured by the user. And the information of each bit in RK_d encoded in the basis of the signal. For each bit in RK_u, if the user chooses the same basis with the database, according to the measurement results in Table 2 and the steps 1.3 and 1.5, the user would record an ambiguous bit "?" in RK_u, since his order pair would be $< s_i, d_i > \in \{< s_i, d_i >, < x, d_i \oplus 1 >\}$ and he cannot deduce the value of the bit in RK_d. If the user chooses a different basis from the database's, the measurement result would be totally random, and he would record a certain bit $u_i \oplus 1$ which is identical with d_i provided $k_i \neq x$. The probability that the user gets a certain bit in RK_u is $1/2 \times 1/2 = 1/4$, 1/2 for choosing a different basis and 1/2 for recording a different result.

B. THE CLASSICAL POST-PROCESSING AND PRIVATE QUERY

In last subsection, the database and the user have generated a raw oblivious key with about 1/4 of its bits known by the user. This means the structure of the raw oblivious key is the same with that in the J-protocol [26]. Thus, the database and the user can just adopt the classical post-processes in ref. [26] to producing a final oblivious key. However, in J-protocol, the expectation of the number of the items that the user can get is fixed for a database with a certain number of items. For example, for a database with 10^5 items, the expectation should be $10^5 \times 0.25^7 \approx 6.10$ [26], or the failure probability would be too large. And this is not very suitable for practical applications. In 2012, Gao et al. proposed a flexible QPQ protocol by modifying the encoding and decoding mode in the raw oblivious key generation process [28]. Considering the encoding mode in the proposed protocol, it is difficult to take similar strategies with Gao's protocol. Here we adopt a different post-process strategy to make the protocol more suitable than J-protocol in practical applications. Suppose the number of the items in the database is N and the tolerable failure probability for the protocol is p, then the security parameter k should be

$$k = \lfloor \log_4 \frac{\sqrt[N]{2}}{\sqrt[N]{2} - \sqrt[N]{p}} \rfloor. \tag{7}$$

In the first stage, the database and the user should generate a raw oblivious key RK_d with $2kN$ bits. And the classical post-processing and the private query are as follows.

2.1 The database produces two final oblivious keys with N, FK_{d1} and FK_{d2}. The i-th bit in FK_{d1} is

$$\bigoplus_{j=0}^{k-1} D_{jN+i}, \tag{8}$$

where, D_l is the l-th bit in RK_d. And The i-th bit in FK_{d2} is

$$\bigoplus_{j=k}^{2k-1} D_{jN+i}. \tag{9}$$

2.2 The user produces two final oblivious keys with N, FK_{u1} and FK_{u2}. The i-th bit in FK_{u1} is

$$\bigoplus_{j=0}^{k-1} U_{jN+i}, \tag{10}$$

where, U_l is the l-th bit in RK_u, and if one of the above bits is "?", the result is "?". And The i-th bit in FK_{u2} is

$$\bigoplus_{j=k}^{2k-1} U_{jN+i}. \tag{11}$$

If both FK_{u1} and FK_{u2} contain at least one explicit bit, with a probability larger than p, the oblivious key distribution is considered to be succeed and they continue to the private query stage.

3.1 Suppose the position of an explicit bit in FK_{u1} (FK_{u2}) is pos_1 (pos_2) and the position of the user's interested item in the database is pos_0. Then the user sends the database two integers $pos_1 - pos_0$ and $pos_2 - pos_0$.
3.2 The user and the database both sift FK_{u1} and FK_{d1} by $pos_1 - pos_0$, and sift FK_{u2} and FK_{d2} by $pos_2 - pos_0$, so that the two explicit bits in the sifted keys are at the same position of the user's expected bit in the database.
3.3 The database encodes all the items with FK_{d1} and FK_{ds} orderly.
3.4 The user decodes his expected item with the two explicit bits above.

Now we analyze the failure probability of the proposed protocol. For each bit in the FK_{u1}, the probability that the user gets an explicit conclusion is 0.25^k, therefore, the failure probability for FK_{u1}, i.e., the probability that the user gets no explicit bit in FK_{u1}, is

$$(1-(\frac{1}{4})^k)^N \leq (1-\frac{1}{\log_4 \frac{1}{1-\sqrt[N]{\frac{p}{2}}}})^N = \frac{p}{2}. \tag{12}$$

Similarly, the failure probability for FK_{u2} is also no larger than $p/2$. And the failure probability for the whole protocol p' satisfying

$$p' \leq 1-(1-\frac{p}{2})^2 < p. \tag{13}$$

Following the steps in subsections IV-A and IV-B, the database and the user can finish the private query. The average number that the user can get will be analyzed in next section.

V. ANALYSIS

A. THE AVERAGE NUMBER OF THE ITEMS THE USER CAN GET

For an honest user, the average number of the items he could get can be described as follows

$$n = 1 + \frac{N-1}{4^{2k}} = 1 + \frac{N-1}{16^k}, \tag{14}$$

where the first addend 1 represents the item that the user wants to query, and the second addend $(N-1)/(4^{2k})$ is the expectation of the number of the items that the user can get except for the one he wants to query. Note that the security parameter k is a function of the database size N and the tolerable failure probability p, so the value of n is also confirmed by N and p. According to Equation 7, the parameter k adds 1 every time the N grows 4 times. In equation 14, n increases in local interval with the same k, however, the general trend of n declines since the denominator of the second addend increase 16 times every time the numerator increases 4 times. The relationship of n and N for fixed p is shown in Figure 2.

It is very difficult to calculate an accurate expectation of the number of the items that a dishonest user can get, and we will analyze it in next subsection.

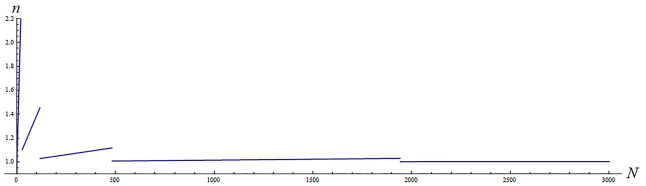

FIGURE 2. The relationship of n and N when $p = 0.001$.

B. THE SECURITY OF THE DATABASE

In this subsection, we analyze the security of the privacy of the database. We first analyze the security of the database against **individual attacks**, where the dishonest user is limited that he can only operate on each signal individually. Since the technologies of quantum memory and joint measurement are very difficult, especially in the single-photon interference system, the individual attack is the only possible attack type which can be achieved with today's technology.

If the user cannot transfer and store the received signals, he has to measure them immediately after he receives them. Since the value of the raw oblivious key is encoded by the string DA, if the database encodes a key bit 0, the state of the signal should be $|P_{00}\rangle$ or $|P_{10}\rangle$ randomly. That means, without any information on the basis, the state of the received signal is the following mixed state in the user's sight,

$$\rho_0 = \frac{1}{2}|P_{00}\rangle\langle P_{00}| + \frac{1}{2}|P_{10}\rangle\langle P_{10}| = I_{ab}. \tag{15}$$

And the state for bit 1 is

$$\rho_1 = \frac{1}{2}|P_{01}\rangle\langle P_{01}| + \frac{1}{2}|P_{11}\rangle\langle P_{11}| = I_{ab} = \rho_0. \tag{16}$$

Therefore, for each signal, the user could not get any additional information provided he measured it before the database has published the set in Step 1.4. In this situation, the dishonest user can only steal the information in classical post-processing. Step 2.1 and 2.2 are deterministic classical processes where the dishonest user cannot attack actively. And he can get more information by choosing optimal pos_1 and pos_2 in Step 3.1. For example, suppose FK_{u1} and FK_{u2} are ?1???0??1 and ?1?????1? respectively. The user would get only one item if he chooses the second bit in both FK_{u1} and FK_{u2} to encrypt the target item, while two items if he chooses the sixth bit in FK_{u1} and the eighth bit in FK_{u2} to encrypt the target item. We have simulated the above strategy for many cases and the results show that the dishonest user can get about 1 to 3 items on average, which is smaller than the original expectations in [26]. Table 2 describes the results of the simulation, where we choose 15 cases when the number of the items in the database is 10^4, 5×10^4, 10^5, 5×10^5 and 10^6, and the tolerable failure probability is 0.01, 0.001 and 0.0001. And for each case, we simulate 100 times for the QPQ process and record the average number and the maximal number of the items that the dishonest user can get.

If the dishonest user can store the received signal and measure it individually after the database has published the set which contains the correct state of the signal, the user can get

TABLE 2. The simulation result for the strategy of the dishonest user who cannot store the received signals.

	10^4	5×10^4	10^5	5×10^5	10^6
0.01	1.30, 2	1.26, 2	1.00, 1	0.99, 1	1.04, 2
0.001	1.24, 2	1.16, 2	1.74, 3	0.99, 1	1.02, 2
0.0001	3.05, 5	1.20, 2	1.71, 2	1.52, 2	1.04, 2

Here, the row heads are the tolerable failure probabilities and the column heads are the database sizes. And the first number in each blank is the average number that the dishonest user has got in the 100 simulations, and the second one is the maximal number.

more information about the database. With the information of the set the database has published, the user can perform an optimal unambiguous state discrimination between the two states in the set to get an explicit result with a probability p_{un}, where

$$p_{un} \leq 1 - |\langle P_{s_i d_i} | P_{x d_i \oplus 1} \rangle| = 1 - \frac{1}{\sqrt{2}}. \tag{17}$$

Here, p_{un} is larger than the legal probability 1/4. We have also simulated this attack, see Table 3.

TABLE 3. The simulation result for the strategy of the dishonest user who can store the received signals.

	10^4	5×10^4	10^5	5×10^5	10^6
0.01	2.09, 4	2.04, 3	1.54, 3	1.59, 2	1.97, 2
0.001	2.15, 3	2.10, 3	2.84, 4	1.54, 2	1.94, 3
0.0001	5.00, 7	2.02, 3	2.79, 4	3.12, 4	1.98, 3

Here, the row heads are the tolerable failure probabilities and the column heads are the database sizes. And the first number in each blank is the average number that the dishonest user has got in the 100 simulations, and the second one is the maximal number.

For the dishonest user who is only limited by the principles of quantum mechanics, he can perform the joint measurement on the k signals which contribute to the same bit in the final oblivious key. To simplify the analysis, we assume that performs I, Z_{ab}, X_{ab} and Y_{ab} to the received states if the set of the database is $\{<0,0>, <0,1>\}$, $\{<0,0>, <1,1>\}$, $\{<1,0>, <1,1>\}$ and $\{<1,0>, <0,1>\}$ respectively, where

$$I = |a\rangle\langle a| + |b\rangle\langle b|, \tag{18}$$
$$Z_{ab} = |a\rangle\langle a| - |b\rangle\langle b|, \tag{19}$$
$$X_{ab} = |a\rangle\langle b| + |b\rangle\langle a|, \tag{20}$$
$$Y_{ab} = |a\rangle\langle b| - |b\rangle\langle a|. \tag{21}$$

And we have

$$\begin{aligned} Z_{ab}\{|P_{00}\rangle, |P_{11}\rangle\} &= Z_{ab}\{|a\rangle, \frac{1}{\sqrt{2}}(|a\rangle + \mathrm{i}|b\rangle)\} \\ &= \{|a\rangle, -\frac{\mathrm{i}}{\sqrt{2}}(\mathrm{i}|a\rangle + |b\rangle)\}, \end{aligned} \tag{22}$$

$$\begin{aligned} X_{ab}\{|P_{10}\rangle, |P_{11}\rangle\} &= X_{ab}\{|b\rangle, \frac{1}{\sqrt{2}}(|a\rangle + \mathrm{i}|b\rangle)\} \\ &= \{|a\rangle, \frac{1}{\sqrt{2}}(\mathrm{i}|a\rangle + |b\rangle)\}, \end{aligned} \tag{23}$$

$$\begin{aligned} Y_{ab}\{|P_{10}\rangle, |P_{01}\rangle\} &= Y_{ab}\{|b\rangle, \frac{1}{\sqrt{2}}(\mathrm{i}|a\rangle + |b\rangle)\} \\ &= \{|a\rangle, -\frac{\mathrm{i}}{\sqrt{2}}(\mathrm{i}|a\rangle + |b\rangle)\}. \end{aligned} \tag{24}$$

And expressing the above state in the form of density matrix, the above sets are in the same form $\{\rho_a, \rho_+\}$, where

$$\rho_a = |a\rangle\langle a|, \tag{25}$$
$$\rho_+ = \frac{1}{2}(|a\rangle\langle a| + \mathrm{i}|a\rangle\langle b| - \mathrm{i}|b\rangle\langle a| + |b\rangle\langle b|). \tag{26}$$

Thus, this powerful but difficult attack equals to discriminate the following two states,

$$\rho_e = 2^{-k+1} \bigotimes_{i=1}^{k} \rho_i, \tag{27}$$

where ρ_i could be ρ_a or ρ_+ satisfying that the total number of ρ_+ is even, and

$$\rho_o = 2^{-k+1} \bigotimes_{j=1}^{k} \rho_j, \tag{28}$$

where ρ_j could be ρ_a or ρ_+ satisfying that the total number of ρ_+ is odd. We can get the following conclusion by mathematics induction,

$$\rho_e - \rho_o = (\rho_a - \rho_+)^{\otimes k}. \tag{29}$$

The minimum error probability to discriminate ρ_e and ρ_o is

$$P_e = \frac{1}{2} - \frac{1}{2}\mathrm{tr}(|\rho_e - \rho_o|) = \frac{1}{2} - \frac{1}{2\sqrt{2}^k}. \tag{30}$$

And the optimal probability for unambiguous state discrimination can be bounded by

$$P_{opt} \leq 1 - F(\rho_e, \rho_o) = 1 - \mathrm{Tr}(\sqrt{\rho_e^{\frac{1}{2}} \rho_o \rho_e^{\frac{1}{2}}}). \tag{31}$$

where, $F(\rho_0, \rho_1)$ is the fidelity. Though P_e and P_{opt} decline rapidly with k, the information leakage is still serious because of the joint measurement attack. Simulation results show that, taking 0.001 as the tolerable failure probability, the dishonest user can get about 25 items on average for a 1000-item database, 61 for a 10^4-item one, 625 for a 10^5-item one and 987 for a 10^6 one. Almost all the QKD-based QPQ protocols utilizing one-way quantum communication faces such severe threat and the effective defensive strategy is to adopt two-way quantum communication as the protocol in Ref. [42].

C. THE PRIVACY OF THE USER

A dishonest database in QPQ would try to find out which item the user is interested in. The best individual attack for the database is to prepare an intermediate state between the two states in the set that he would publish later or the state orthogonal with it. Then this bit would be an inconclusive result with a higher probability than usual if he prepares an intermediate state, and be a conclusive result with higher probability if he prepares the orthogonal state. To be more

specific, the dishonest database may prepare the following state

$$|\phi\rangle = \mathrm{i}\cos\frac{\pi}{8}|a\rangle + \sin\frac{\pi}{8}|b\rangle, \tag{32}$$

and sends it to the user in step 1.1. If the database publish the set $\{< 1, 0 >, < 0, 1 >\}$, which represents the states $\{|a\rangle, (\mathrm{i}|a\rangle + |b\rangle)/\sqrt{2}\}$, the user would get an inconclusive bit with the probability $1/2+\sqrt{2}/4$ (≈ 0.85). And if he publish the set $\{< 1, 1 >, < 0, 0 >\}$, the user would get conclusive with the probability of 85%. This strategy would help the database to guess the user's privacy better than usual, however, the user would find out Bob's attack with probability 1/2 since by performing the above attack, Bob would fail to share an identical key with the user and has to send the user a random data. Generally speaking, on one hand, the dishonest actions of the database cannot help him to steal the user's privacy explicitly, and on the other hand, the user would find the cheating with a non-zero probability.

D. COMPARISON WITH OTHER QKD-BASED QPQ WITH SINGLE-PHOTON INTERFERENCE

As we know, there exist three other QKD-based QPQ protocols with the technology of single-photon interference. The first one (C-protocol) [40] is the counterfactual one proposed by Zhang et al. The second one (R-protocol) [37] is the QKD-based QPQ protocol based on the RRDPS-QKD protocol [43]. The last one (S-protocol) [41] is the QPQ based on single-photon interference proposed by Xu et al. Each protocol has its own features and advantages, for example, counterfactual QPQ protocol and the protocol proposed by Xu et al. are more flexible for databases of various sizes, and in the QPQ protocol based on RRDPS-QKD, an honest user will obtain is always one and the failure probability is always zero. And the main advantage of the proposed protocol is the lower price compared the others since both the amount and the kind of quantum devices in the interference circuit are the fewest, see Table 4. In C-protocol, a source emits a single-photon state into the circuit, the two participants use two half-wave plates (HWP) to alter the state of the photon. The protocol needs three detectors to encode information and check the potential attacks. Besides, C-protocol also requires polarization beam splitter, optical switch and an additional source to finish the detections. In R-protocol, to generate a RRDPS signal, plenty of BSs are needed. And in S-protocol, the information is encoded by in the phase difference of the two wave packets, therefore, two phase modulators (PM) are necessary. While our protocol encodes the information in the position of the photon and the interference result of the two wave packets, thus, our protocol needs no PM.

And as analyzed above, the newly presented postprocessing strategy in our protocol can achieve higher security of the database.

TABLE 4. Comparison of the devices used in the QPQ protocols utilizing single-photon interference.

	Source	BS	PM	D	HWP	Others	Sum
C-protocol	1	2	0	3	2	3	11
R-protocol	1	N	0	2	0	0	N+3
S-protocol	1	2	2	2	0	0	7
Our protocol	2	2	0	2	0	0	6

Here, BS represents beam splitter, PM represents phase modulator, D represents detector and HWP represents half-wave plate. Others include polarization beam splitter, optical switch, and so on.

VI. CONCLUSION

In this paper, we propose a QKD-based QPQ protocol utilizing single-photon interference and analyze the security of the database and the privacy of the user. The proposed protocol requires less quantum communication devices than other relevant protocols with similar technologies. And it also protects the security of the database better because of the different post-processing strategies. Though the post-processing strategy is protective against most of the attacks to the database, the effect is not obvious against the joint measurement attacks. As most QPQ protocols which employ one-way quantum communications, the proposed protocol is also sensitive for the powerful joint measurement attacks. How to resist the joint measurement attacks in one-way QPQ protocols is still an important and challenging problem.

REFERENCES

[1] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proc. 35th Annu. IEEE Symp. Found. Comput. Sci.*, Santa Fe, NM, USA, Nov. 1994, pp. 124–134.
[2] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proc. 28th Annu. ACM Symp. Theory Comput.*, May 1996, p. 212.
[3] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE Int. Conf. Comput., Syst. Signal Process.*, Bangalore, India, Dec. 1984, pp. 1–7.
[4] P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," *Phys. Rev. Lett.*, vol. 85, no. 2, pp. 441–444, Jul. 2000.
[5] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Rev. Mod. Phys.*, vol. 81, no. 3, pp. 1301–1350, Sep. 2009.
[6] G.-L. Long and X.-S. Liu, "Theoretically efficient high-capacity quantum-key-distribution scheme," *Phys. Rev. A, Gen. Phys.*, vol. 65, no. 3, 2002, Art. no. 032302.
[7] F.-G. Deng and G.-L. Long, "Controlled order rearrangement encryption for quantum key distribution," *Phys. Rev. A, Gen. Phys.*, vol. 68, no. 4, 2003, Art. no. 042315.
[8] K. Boström and T. Felbinger, "Deterministic secure direct communication using entanglement," *Phys. Rev. Lett.*, vol. 89, Oct. 2002, Art. no. 187902.
[9] S. Lin, Q.-Y. Wen, F. Gao, and F.-C. Zhu, "Quantum secure direct communication with x-type entangled states," *Phys. Rev. A, Gen. Phys.*, vol. 78, Dec. 2008, Art. no. 064304.
[10] F. Gao, S.-J. Qin, Q.-Y. Wen, and F.-C. Zhu, "Cryptanalysis of multiparty controlled quantum secure direct communication using Greenberger–Horne–Zeilinger state," *Opt. Commun.*, vol. 283, no. 1, pp. 192–195, 2010.
[11] W. Huang, Q.-Y. Wen, H.-Y. Jia, S.-J. Qin, and F. Gao, "Fault tolerant quantum secure direct communication with quantum encryption against collective noise," *Chin. Phys. B*, vol. 21, no. 10, 2012, Art. no. 100308.
[12] R. Cleve, D. Gottesman, and H.-K. Lo, "How to share a quantum secret," *Phys. Rev. Lett.*, vol. 83, no. 3, pp. 648–651, 1999.
[13] M. Hillery, V. Bužek, and A. Berthiaume, "Quantum secret sharing," *Phys. Rev. A, Gen. Phys.*, vol. 59, no. 3, pp. 1824–1829, 1999.
[14] Y.-G. Yang, Q.-Y. Wen, and X. Zhang, "Multiparty simultaneous quantum identity authentication with secret sharing," *Sci. China G, Phys. Mech. Astron.*, vol. 51, no. 3, pp. 321–327, 2008.

[15] S.-J. Qin, F. Gao, Q.-Y. Wen, and F.-C. Zhu, "Security of quantum secret sharing with two-particle entanglement against individual attacks," *Quant. Inf. Comput.*, vol. 9, pp. 765–772, Sep. 2009.
[16] S. Lin, Q.-Y. Wen, S.-J. Qin, and F.-C. Zhu, "Multiparty quantum secret sharing with collective eavesdropping-check," *Opt. Commun.*, vol. 282, pp. 4455–4459, Nov. 2009.
[17] T.-Y. Wang and Q.-Y. Wen, "Security of a kind of quantum secret sharing with single photons," *Quant. Inf. Comput.*, vol. 11, pp. 434–443, May 2011.
[18] W. Huang, H.-J. Zuo, and Y.-B. Li, "Cryptanalysis and improvement of a multi-user quantum communication network using X-type entangled states," *Int. J. Theor. Phys.*, vol. 52, no. 4, pp. 1354–1361, 2013.
[19] L.-G. Qin, X. Feng, M. Hafezi, Y. Zhang, J. Guo, G. Dong, and Y. Qin, "Investigating the tribological and biological performance of covalently grafted chitosan coatings on Co–Cr–Mo alloy," *Tribol. Int.*, vol. 127, pp. 302–312, 2018.
[20] V. Giovannetti, S. Lloyd, and L. Maccone, "Quantum private queries," *Phys. Rev. Lett.*, vol. 100, no. 23, 2008, Art. no. 230502.
[21] V. Giovannetti, S. Lloyd, and L. Maccone, "Quantum private queries: Security analysis," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3465–3477, Jul. 2010.
[22] L. Olejnik, "Secure quantum private information retrieval using phase-encoded queries," *Phys. Rev. A, Gen. Phys.*, vol. 84, no. 2, 2011, Art. no. 022313.
[23] F. Yu and D. Qiu, "Coding-based quantum private database query using entanglement," *Quantum Inf. Comput.*, vol. 14, pp. 91–106, Jan. 2014.
[24] F. De Martini, V. Giovannetti, S. Lloyd, L. Maccone, E. Nagali, L. Sansoni, and F. Sciarrino, "Experimental quantum private queries with linear optics," *Phys. Rev. A, Gen. Phys.*, vol. 80, no. 1, 2009, Art. no. 010302.
[25] C. Wang, L. Hao, and L.-J. Zhao, "Implementation of quantum private queries using nuclear magnetic resonance," *Chin. Phys. Lett.*, vol. 28, no. 8, 2011, Art. no. 080302.
[26] M. Jakobi, C. Simon, N. Gisin, J.-D. Bancal, C. Branciard, N. Walenta, and H. Zbinden, "Practical private database queries based on a quantum-key-distribution protocol," *Phys. Rev. A, Gen. Phys.*, vol. 83, no. 2, 2011, Art. no. 022301.
[27] V. Scarani, A. Acín, G. Ribordy, and N. Gisin, "Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations," *Phys. Rev. Lett.*, vol. 92, no. 5, 2004, Art. no. 057901.
[28] F. Gao, B. Liu, Q.-Y. Wen, and H. Chen, "Flexible quantum private queries based on quantum key distribution," *Opt. Express*, vol. 20, no. 16, pp. 17411–17420, 2012.
[29] F. Gao, B. Liu, W. Huang, and Q.-Y. Wen, "Postprocessing of the oblivious key in quantum private query," *IEEE J. Sel. Topics Quantum Electron.*, vol. 21, no. 3, May/Jun. 015, Art. no. 6600111.
[30] P. Chan, I. Lucio-Martinez, X. Mo, C. Simon, and W. Tittel, "Performing private database queries in a real-world environment using a quantum protocol," *Sci. Rep.*, vol. 4, Jun. 2014, Art. no. 5233x.
[31] Y.-G. Yang, S.-J. Sun, P. Xu, and J. Tian, "Flexible protocol for quantum private query based on B92 protocol," *Quantum Inf. Process.*, vol. 13, no. 3, pp. 805–813, 2014.
[32] Y.-G. Yang, S.-J. Sun, J. Tian, and P. Xu, "Secure quantum private query with real-time security check," *Optik*, vol. 125, no. 19, pp. 5538–5541, 2014.
[33] Y.-G. Yang, M.-O. Zhang, and R. Yang, "Private database queries using one quantum state," *Quantum Inf. Process.*, vol. 14, no. 3, pp. 1017–1024, 2015.
[34] S. J. Sun, Y. G. Yang, and M. O. Zhang, "Relativistic quantum private database queries," *Quantum Inf. Process.*, vol. 14, no. 4, pp. 1443–1450, 2015.
[35] M. V. P. Rao and M. Jakobi, "Towards communication-efficient quantum oblivious key distribution," *Phys. Rev. A, Gen. Phys.*, vol. 87, no. 1, 2013, Art. no. 012331.
[36] D. S. Shen, X. C. Zhu, W. P. Ma, X. R. Yin, and M. L. Wang, "Improvement on private database queries based on the quantum key distribution," *J. Optoelectron. Adv. Mater.*, vol. 14, pp. 504–510, May 2012.
[37] B. Liu, F. Gao, W. Huang, and Q. Wen, "QKD-based quantum private query without a failure probability," *Sci. China Phys., Mech. Astron.*, vol. 58, no. 10, p. 100301, 2015.
[38] C.-Y. Wei, X.-Q. Cai, B. Liu, T.-Y. Wang, and F. Gao, "A generic construction of quantum-oblivious-key-transfer-based private query with ideal database security and zero failure," *IEEE Trans. Comput.*, vol. 67, no. 1, pp. 2–8, Jan. 2018.
[39] F. Gao, S.-J. Qin, W. Huang, and Q.-Y. Wen, "Quantum private query: A new kind of practical quantum cryptographic protocol," *Sci. China Phys., Mech. Astron.*, vol. 62, no. 7, 2019, Art. no. 70301.
[40] J.-L. Zhang, F.-Z. Guo, F. Gao, B. Liu, and Q.-Y. Wen, "Private database queries based on counterfactual quantum key distribution," *Phys. Rev. A, Gen. Phys.*, vol. 88, no. 2, p. 022334, 2013.
[41] S.-W. Xu, Y. Sun, and S. Lin, "Quantum private query based on single-photon interference," *Quantum Inf. Process.*, vol. 15, pp. 3301–3310, Aug. 2016.
[42] C.-Y. Wei, T.-Y. Wang, and F. Gao, "Practical quantum private query with better performance in resisting joint-measurement attack," *Phys. Rev. A, Gen. Phys.*, vol. 93, no. 4, p. 042318, 2016.
[43] T. Sasaki, Y. Yamamoto, and M. Koashi, "Practical quantum key distribution protocol without monitoring signal disturbance," *Nature*, vol. 509, pp. 475–479, May 2014.

BIN LIU was born in Taiyuan, Shanxi, China. He received the B.S. degree in mathematics and applied mathematics and the Ph.D. degree in cryptography from the Beijing University of Posts and Telecommunications (BUPT), Beijing, China, in 2009 and 2015, respectively.

He is currently an Associate Professor with the College of Computer Science, Chongqing University, Chongqing, China. His research interests include quantum cryptography, quantum information processing, and quantum communication.

Dr. Liu is a member of the Chinese Association for Cryptologic Research.

ZHI-FENG GAO was born in Lvliang, Shanxi, China. He received the B.S. degree in software engineering from Shanxi University, Taiyuan, China, in 2017. He is currently pursuing the master's degree with Chongqing University, Chongqing, China. His research interests include quantum cryptography, data mining, and machine learning.

DI XIAO received the B.S. degree from Sichuan University, Chengdu, China, and the M.S. and Ph.D. degrees from Chongqing University, Chongqing, China, where he accomplished the Postdoctoral Research, from 2006 to 2008. From December 2008 to December 2009, he visited the Department of Computer Science, New Jersey Institute of Technology, Newark, NJ, USA. He is currently a Full Professor with the College of Computer Science, Chongqing University. He has published more than 90 academic journal papers. His research interests include signal processing in encrypted domain, compressive sensing, and quantum information processing. He was selected as 2014–2017 Elsevier Most Cited Chinese Researcher.

WEI HUANG received the B.S. degree in mathematics and applied mathematics and the Ph.D. degree in cryptography from the Beijing University of Posts and Telecommunications, Beijing, China, in 2009 and 2015, respectively. He is currently a Senior Engineer with the Department of Science and Technology on Communication Security Laboratory, Institute of Southwestern Communication, Chengdu, China. His research interests include quantum cryptography, quantum secure communication, and quantum information.

ZHI-QING ZHANG received the B.S. degree in materials science and engineering from Northwestern Polytechnic University, Xi'an, China, in 2002, and the Ph.D. degree in materials science and engineering from Tsinghua University, Beijing, China, in 2007. He is currently a Professor with the College of Materials Science and Engineering, Chongqing University, Chongqing, China. His research interests include big data, computational materials science, and quantum information.

YANG LI received the B.S. degree in physics and the Ph.D. degree in radio physics from Peking University, Beijing, China, in 2007 and 2012, respectively. He is currently a Senior Engineer with the Department of Science and Technology on Communication Security Laboratory, Institute of Southwestern Communication, Chengdu, China. His research interests include quantum cryptography, quantum secure communication, and quantum information.

BING-JIE XU received the B.S. degree in electronics and the Ph.D. degree in radio physics from Peking University, Beijing, China, in 2007 and 2012, respectively. He is currently a Senior Engineer with the Department of Science and Technology on Communication Security Laboratory, Institute of Southwestern Communication, Chengdu, China. His research interests include quantum cryptography, quantum secure communication, and quantum information.