IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received December 12, 2018, accepted January 11, 2019, date of publication January 17, 2019, date of current version March 20, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2893341

Quantum Private Query With Perfect Performance Universally Applicable Against Collective-Noise

NA LI[1,2], JIAN LI[1], XIUBO CHEN[3], AND YUGUANG YANG[4]

[1]School of Computer Science, Beijing University of Posts and Telecommunications, Beijing 100876, China
[2]Jilin Medical University, Jilin 132013, China
[3]State Key Laboratory of Networking and Switching Technology, Information Security Center, Beijing University of Posts and Telecommunications, Beijing 100876, China
[4]College of Computer Science and Technology, Beijing University of Technology, Beijing 100124, China

Corresponding author: Jian Li (lina68001@126.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 1636106, Grant 61472048, Grant 61671087, and Grant 61572053 and in part by the BUPT Excellent Ph.D. Students Foundation under Grant CX2017313.

ABSTRACT Almost all of the previous quantum private query (QPQ) protocols are always based on an ideal environment without any noise. Nevertheless, due to the defects of the channel, channel noise inevitably exists in the actual transmission process, which will give rise to transmission error and reduce the probability of successful quantum transmission. An eavesdropper may disguise her actions as channel noise to avoid being detected by legitimate parties during security checks. To solve this problem, we present a QPQ protocol with perfect performance universally applicable against collective noise. Concretely, the protocol encodes bits in noiseless subspace and thus can function over a quantum channel subjected to an arbitrary degree of collective noise, as occurs, for instance, due to polarization rotation in an optical fiber. Furthermore, Bob cannot get the information about Alice's choice at all by taking fake entangled attack and by taking fake photon attack, the probability Bob can get the information about Alice's choice is only approximately 6.7%, which is far less than the probability of 25% in Yang *et al.*'s protocol. Moreover, the conclusiveness of the user Alice's measurement results is subject to quantum randomness rather than allowing Alice to choose by herself to obtain a conclusive result in Wei *et al.*'s protocol, which prevents Alice's intuitive attack and meanwhile makes it arduous for Bob to perform the joint-measurement attack. Our protocol uses only one state, which reduces the communication complexity, and is, therefore, an effective QPQ solution with the high-security level.

INDEX TERMS Quantum private query, collective-noise, security.

I. INTRODUCTION

In quantum communication, the two authorized parties not only wish their information to be protected from external eavesdropping, but also their respective privacy against each other. This type of task is popularly known as symmetrically-private information retrieval (SPIR) [3], where the privacy of the user, as well as the security of the database, is guaranteed. Quantum private query (QPQ) falls into this category. QPQ not only protects Alice's privacy when she makes a query to Bob's database, that is, Bob cannot obtain what Alice queries, but also protects the security of Bob's database, that is, he cannot give Alice more information. The SPIR of information theory security does not exist [4].

Giovannetti *et al.* [5] proposed the first QPQ protocol in 2008. The security relies on the fact that it is impossible to completely distinguish non-orthogonal states, and Bob's cheating will introduce interference. Communication and computational complexity both decrease exponentially. A proof-of-principle experiment was published [6], and the security of the protocol was demonstrated [7]. Then, Olejnik [8] proposed an improved protocol of Giovannetti *et al.*'s protocol in 2011. It is more effective in terms of communication complexity and the rounds.

Nevertheless, the above two QPQ protocols are arduous to implement and have three disadvantages: (1) when the database is large, the oracle dimension is high. Accordingly, it is not easy to achieve, thereby not practical; (2) it is just cheat-sensitive, and Bob can still get Alice's query item to some extent; (3) it is affected by channel loss attack. Jakobi *et al.* [9] first proposed a practical private database

queries protocol based on a QKD protocol that can solve the above mentioned problems. Actually, the earliest QKD-based scheme is based on BB84 protocol, but its downside is that if the user performs a quantum storage attack, then the security of the database is gone. Scarani*et al.* [10] use SARG04 protocol instead of BB84 protocol to resist quantum storage attacks. Since then, a lot of attention has been focused on QKD-based QPQ protocols, and experimental studies on it have been developing very fast [1], [2], [11]–[33].

The SARG-based protocol has a host of advantages, such as easy implementation, better protection of user privacy, suitability for large databases, and resistance to channel loss and quantum storage attacks. However, the disadvantage is poor flexibility. In Jakobi *et al.*'s protocol, either Bob's database leaks too much, or the probability of failure is too high. Therefore, Gao *et al.* [11] generalized the Jakobi *et al.*'s protocol and proposed a flexible QKD-based QPQ. It can solve the above problems using the thoughts of B92 to improve SARG04. By adjusting the value of a parameter θ, it can achieve better performance with lesser rounds and the effect of Alice's joint-measurement (JM) attack is not obvious when the smaller value is taken. When $\theta < \frac{\pi}{4}$, Gao *et al.*'s protocol shows better database security than Jakobi *et al.*'s protocol, but Bob is able to correctly guess the address of Alice's querying with a higher probability. Therefore, Yang *et al.* [12] proposed a flexible QPQ protocol based on B92 protocol. It can simultaneously obtain better database security and a lower probability with which Bob can correctly guess the address of Alice's querying when $\theta < \frac{\pi}{4}$. Zhang *et al.* [13] proposed a QPQ protocol based on counterfactual quantum key distribution. By adding key detection devices to QKD devices, the user privacy and database security can be kept secure. Taking advantage of the inefficiencies of the counterfactual QKD, the protocol has achieved excellent flexibility and extensibility by adjusting related parameters. Considering the real noisy channels, Chan *et al.* [14] presented a fault-tolerant QPQ protocol using a novel error correction algorithm to cope with noisy channels, then they gave a proof-of-concept demonstration of the protocol over a deployed fiber. Wei *et al.* [2] proposed a novel QPQ protocol based on a two-way QKD scheme, which behaves much better in resisting JM attack. Yang *et al.* [15] presented a protocol in which the special way of classical post-processing of oblivious key ensures the security against the JM attack.

To the best of our knowledge, almost all of the previous QPQ protocols are always based on ideal environment without any noise [1], [2], [5], [8], [9], [11]–[13], [15]–[33]. However, any experimental implementation of QPQ naturally has to deal with the issue of noise in the quantum channel, whether it is a free-space channel or an optical fiber channel. Due to channel imperfections, such as the fluctuation of the fiber birefringence changes the polarization state of the photon, channel noise inevitably exists in the actual transmission process, which will reduce the transmission success rate of the quantum information. An eavesdropper may disguise her actions as channel noise to avoid being detected by legitimate parties during security checks. The following methods have been proposed to reduce the effects of channel noise, such as quantum error correction code (QECC) [34], quantum error rejection [35]–[37], decoherence free subspace (DFS) [38], [39] and entanglement purification [40], [41].

However, these methods work only when the environmental impact is weak and the probability of qubits being affected is low. Fortunately, when they interact with environment, not all quantum states are vulnerable. When photons are transmitted in a medium, such as an optical fiber, and the coupling between environment and qubits occurs, the particularly relevant symmetry that appears gives rise to so-called collective noise. For free-space channels, they are immune to the effect, the coupling between the qubits and the molecules in the atmosphere can be absorbed in a dielectric constant to very good approximation. The transformation of collective noise can be described by a unitary operator $U(t)$, where t denotes the time of transmission. In general, no matter what kind of error model is chosen, noise in one channel is often considered as collective noise. In other words, we assume that the fluctuation of the channel is exceedingly slow in time, so that the adjacent photons are suspected of being affected by the same noise. As mentioned in [42], if the time delay between the photons is small enough, the effect of collective noise on the state of N-qubit can be described as

$$\rho_N \Rightarrow [U(t)]^{\otimes N} \rho_N [U(t)^+]^{\otimes N}, \tag{1}$$

where $[U(t)]^{\otimes N} = U(t) \otimes \cdots \otimes U(t)$ denotes the N unitary transformation, and $U(t)$ represents the tensor product of the unitary transformation. Actually, there are quantum states that are invariant under collective noise, no matter how strong the interaction with environment is. These quantum states are called decoherent free (DF) states and have been applied to protect quantum information.

In this paper, we present a QPQ protocol with perfect performance universally applicable against collective noise. Concretely, the protocol encodes bits in noiseless subspace and thus can function over a quantum channel subjected to an arbitrary degree of collective noise, as occurs, for instance, due to polarization rotation in an optical fiber. Furthermore, Bob cannot get the information about Alice's choice at all by taking fake entangled attack and by taking fake photon attack, the probability Bob can get the information about Alice's choice is only approximately 6.7%, which is far less than the probability of 25% in Yang *et al.*'s protocol [1], which ensures perfect user privacy. Moreover, the conclusiveness of the user Alice's measurement results is subject to quantum randomness in our protocol rather than allowing Alice to choose by herself to obtain a conclusive result in Wei *et al.*'s protocol [2], which prevents Alice's intuitive attack and meanwhile makes it arduous for Bob to perform JM attack to ensure perfect database security and user privacy. Compared with most existing protocols using two to four quantum states, our protocol uses only one state, which reduces the

communication complexity, and is therefore an effective QPQ solution with high security level.

The rest of this paper is organized as follows. The next section introduces the proposed QPQ with perfect performance universally applicable against collective noise. Sect. III analyzes the security of the proposed protocol. Finally, a conclusion is given in Sect. IV.

II. PROTOCOL

We start by describing the protocol that Alice and Bob must follow. First, the normalized DF state of a photon quartet required in our protocol is defined as:

$$\left|\phi_0'\right\rangle = \frac{1}{\sqrt{2}}\left(|\phi_0\rangle + |\phi_1\rangle\right), \tag{2}$$

let $|\phi_0\rangle = \frac{1}{\sqrt{2}}\left(|u\rangle - |v\rangle\right), |\phi_1\rangle = \frac{1}{\sqrt{6}}\left(2|w\rangle - |u\rangle - |v\rangle\right)$, where, $|u\rangle = \frac{1}{\sqrt{2}}\left(|0101\rangle + |1010\rangle\right), |v\rangle = \frac{1}{\sqrt{2}}\left(|0110\rangle + |1001\rangle\right)$, $|w\rangle = \frac{1}{\sqrt{2}}\left(|0011\rangle + |1100\rangle\right)$. The state $\left|\phi_0'\right\rangle$ is invariant under collective noise, for this reason, the state can be decomposed into the above superpositions in any basis. Our protocol is described as follows.

1) Bob prepares a sequence of photon quartets $\left|\phi_0'\right\rangle$ and sends them to Alice.
2) Alice generates a random string $a \in \{0,1\}^N$. For each of the photon quartets she received, Alice chooses to measure it in the basis $\{|\phi_0\rangle, |\phi_1\rangle\}$ and resend it back to Bob in the same state she found if $a_i = 1$ or reflect it directly without measurement if $a_i = 0$, then declares which quartets are not received successfully. We call the quartets measured SIFT quartets, and those reflected CTRL ones.
3) Bob generates a random string $b \in \{0,1\}^N$. He measures the ith received quartet in the basis $\{|\phi_0\rangle, |\phi_1\rangle\}$ if $b_i = 0$ or the basis $\left\{\left|\phi_0'\right\rangle, \left|\phi_1'\right\rangle\right\}$ if $b_i = 1$ and stores the random string b as the final key K^r. Here, $\left|\phi_1'\right\rangle = \frac{1}{\sqrt{2}}\left(|\phi_0\rangle - |\phi_1\rangle\right)$. Then he declares which quartets are not received successfully. All of the lost quartets declared by both sides should be discarded.
4) For each quartet, Bob announces one bit '0' or '1', where '0' represents that his measurement result is in the state $|\phi_0\rangle$ or $\left|\phi_0'\right\rangle$, while '1' implies his measurement result is $|\phi_1\rangle$ or $\left|\phi_1'\right\rangle$. Given this information, and using the procedure described above, Alice can determine, for each quartet, whether or not her measurement is conclusive, and if conclusive, the value of the encoded bit.
5) Alice interprets her measurement results in the step 2). According to her choice and Bob's declaration, Alice can obtain the key bit with a certain probability. As an example, suppose Bob's declaration is 0 and Alice's SIFT measurement result is $|\phi_1\rangle$, she can conclude that the quartet must be in the state $\left|\phi_0'\right\rangle$, which corresponds to the raw key bit 1. By this way, a raw key is obtained by Alice and Bob, which is known all to Bob and $\frac{1}{4}$ to Alice. If no bit survives at Alice's end, repeat the above steps.
6) Bob chooses some key bit randomly and asks Alice to publish a_i and her measurement result (if $a_i = 1$) for the chosen ith bit. If Alice provides the incorrect information, Bob will declare to abort the protocol; otherwise, they continue to step 7).
7) When an N-bit database is concerned, enough quartets should be transmitted so that the length of K^r equals to kN. Alice and Bob cut the raw key into k substrings, and add these k substrings bitwise to obtain the final key K in order that Alice knows only roughly one bit. Then, Bob encrypts his database with the key K. Suppose Alice knows the jth bit K_j and wants the ith item X_i of the database, she announces the number $s = j - i$. Then, Bob shifts K by s and uses it to encrypt his database. Thus, X_i is encrypted by K_j, and consequently can be correctly decrypted by Alice.

III. SECURITY ANALYSIS

Now we analyze the security of the proposed protocol in terms of user privacy and database security.

A. USER PRIVACY

We will analyze user privacy against three kinds of attacks from Bob.

1) FAKE ENTANGLED ATTACK

Without loss of generality, in step 1) Bob can prepare a fake entangled state

$$\left|\Phi_0'\right\rangle = \frac{1}{\sqrt{2}}(|\phi_0\rangle_1 |\varepsilon_1\rangle_2 + |\phi_1\rangle_1 |\varepsilon_2\rangle_2). \tag{3}$$

He sends the first quartet to Alice in step 1) and stores corresponding system 2 in his register. Obviously, the joint system, that is, system 1 and 2, would be in state $\left|\Phi_0'\right\rangle$, $\left|\Phi_1'\right\rangle = |\phi_0\rangle_1 |\varepsilon_1\rangle_2$ or $\left|\Phi_2'\right\rangle = |\phi_1\rangle_1 |\varepsilon_2\rangle_2$ with probabilities 1/2, 1/4 and 1/4 respectively after Alice chooses CTRL or SIFT. Thus, if Bob can discriminate these three states when he receives the quartet resent by Alice, he can guess Alice's choice.

After receiving the quartet resent from Alice, Bob can measure the joint system to distinguish whether Alice has measured this quartet and infer the bit value she recorded. Only when knowing that the joint system is in state $\left|\Phi_0'\right\rangle$ ($\left|\Phi_1'\right\rangle$, $\left|\Phi_2'\right\rangle$), Bob can confirm that Alice gets a conclusive raw key bit and can correctly guess the corresponding bit value 0 (1) simultaneously, by announcing the measurement result represented by one bit value. For instance, once he identifies that the joint system is in state $\left|\Phi_1'\right\rangle$ at this time, Bob knows that Alice has measured the quartet and he can announce one bit '1', which means that his measurement result is in the state $|\phi_1\rangle$ or $\left|\phi_1'\right\rangle$, in order that Alice can get a conclusive raw key bit, and she records this bit value as 1. Obviously, only if Bob can identify anyone of the three states

$\left\{\left|\Phi_i'\right\rangle\right\}_{i=0}^{2}$ unambiguously, he can get virtual benefit without being detected.

Because Bob cannot identify any state in $\left\{\left|\Phi_i'\right\rangle\right\}_{i=0}^{2}$ unambiguously, so our protocol is cheat-sensitive. First of all, Bob cannot unambiguously discriminate the three states from each other because they are linearly dependent. Then, Bob cannot unambiguously discriminate the state $\left\{\left|\Phi_i'\right\rangle\right\}$ from the set $C_i = \left\{\left|\Phi_i'\right\rangle\right\}_{i=0}^{2} \setminus \left\{\left|\Phi_i'\right\rangle\right\}$ even using the optimal measurement, because $\left|\Phi_i'\right\rangle$ can be linearly expressed with the states in C_i. Besides, Bob cannot unambiguously identify the set $C_i = \left\{\left|\Phi_i'\right\rangle\right\}_{i=0}^{2} \setminus \left\{\left|\Phi_i'\right\rangle\right\}$ with a nonzero probability when the joint system is in one state within $C_i = \left\{\left|\Phi_i'\right\rangle\right\}_{i=0}^{2} \setminus \left\{\left|\Phi_i'\right\rangle\right\}$.

In more detail, the effect of the attack on the three states $\left\{\left|\Phi_i'\right\rangle\right\}_{i=0}^{2}$ can be described as

$$\begin{aligned}
&|\phi_0\rangle|\varepsilon_1\rangle + |\phi_1\rangle|\varepsilon_2\rangle \\
&\quad= |0101\rangle\left|\varepsilon_{0101}^{6}\right\rangle - |0110\rangle\left|\varepsilon_{0110}^{7}\right\rangle \\
&\qquad - |1001\rangle\left|\varepsilon_{1001}^{10}\right\rangle + |1010\rangle\left|\varepsilon_{1010}^{11}\right\rangle \\
&\qquad + |0011\rangle\left|\varepsilon_{0011}^{4}\right\rangle - |0101\rangle\left|\varepsilon_{0101}^{6}\right\rangle \\
&\qquad - |0110\rangle\left|\varepsilon_{0110}^{7}\right\rangle - |1001\rangle\left|\varepsilon_{1001}^{10}\right\rangle \\
&\qquad - |1010\rangle\left|\varepsilon_{1010}^{11}\right\rangle + |1100\rangle\left|\varepsilon_{1100}^{13}\right\rangle; \\
|\phi_0\rangle|\varepsilon_1\rangle &= |0101\rangle\left|\varepsilon_{0101}^{6}\right\rangle - |0110\rangle\left|\varepsilon_{0110}^{7}\right\rangle \\
&\quad - |1001\rangle\left|\varepsilon_{1001}^{10}\right\rangle + |1010\rangle\left|\varepsilon_{1010}^{11}\right\rangle; \\
|\phi_1\rangle|\varepsilon_2\rangle &= |0011\rangle\left|\varepsilon_{0011}^{4}\right\rangle - |0101\rangle\left|\varepsilon_{0101}^{6}\right\rangle \\
&\quad - |0110\rangle\left|\varepsilon_{0110}^{7}\right\rangle - |1001\rangle\left|\varepsilon_{1001}^{10}\right\rangle \\
&\quad - |1010\rangle\left|\varepsilon_{1010}^{11}\right\rangle + |1100\rangle\left|\varepsilon_{1100}^{13}\right\rangle. \qquad (4)
\end{aligned}$$

Because $\left|\varepsilon_{0000}^{1}\right\rangle = \left|\varepsilon_{0001}^{2}\right\rangle = \left|\varepsilon_{0010}^{3}\right\rangle = \left|\varepsilon_{0011}^{4}\right\rangle = \left|\varepsilon_{0100}^{5}\right\rangle = \left|\varepsilon_{0101}^{6}\right\rangle = \left|\varepsilon_{0110}^{7}\right\rangle = \left|\varepsilon_{0111}^{8}\right\rangle = \left|\varepsilon_{1000}^{9}\right\rangle = \left|\varepsilon_{1001}^{10}\right\rangle = \left|\varepsilon_{1010}^{11}\right\rangle = \left|\varepsilon_{1011}^{12}\right\rangle = \left|\varepsilon_{1100}^{13}\right\rangle = \left|\varepsilon_{1101}^{14}\right\rangle = \left|\varepsilon_{1110}^{15}\right\rangle = \left|\varepsilon_{1111}^{16}\right\rangle$, so Bob cannot unambiguously discriminate the three states $\left\{\left|\Phi_i'\right\rangle\right\}_{i=0}^{2}$, thereby his trick will be detected. The whole system's states of Bob's auxiliary particles and the qubits 1,2,3,4 are the tensor product of Bob's auxiliary states and the initial quantum system $\left(\left|\phi_0'\right\rangle, |\phi_0\rangle, |\phi_1\rangle\right)$. This means that if Bob's attack does not want to be detected, it will not affect the entire system. That is to say, all Bob's attacks will be detected.

2) FAKE PHOTON ATTACK

Bob can prepare a fake photon state

$$\left|\Psi_0'\right\rangle = cos\theta\,|\phi_0\rangle + sin\theta\,|\phi_1\rangle, \qquad (5)$$

where the parameter $\theta \in (0, \pi/2)$.

In order to get information about Alice's choice, Bob should distinguish between two states $\rho_1 = \left|\Psi_0'\right\rangle\left\langle\Psi_0'\right|$ and $\rho_2 = \frac{1}{2}|\phi_0\rangle\langle\phi_0| + \frac{1}{2}|\phi_1\rangle\langle\phi_1|$. Because the sets $\left\{\left|\Psi_0'\right\rangle\right\}$ and $\{|\phi_0\rangle, |\phi_1\rangle\}$ are linearly dependent each other and cannot be unambiguously discriminated, so Bob can get the information by making a minimum-error-discrimination (MED) [43] on ρ_1 and ρ_2. The MED probability attainable is $P_1 = \frac{1}{2}(1 - \frac{1}{2}tr \mid \rho_2 - \rho_1 \mid)$. So we can get the MED probability of discriminating between ρ_1 and ρ_2:

$$P_1 = \frac{2-\sqrt{3}}{4} \approx 6.7\%. \qquad (6)$$

However, under normal circumstances, to get information about Alice's choice, Bob should distinguish between two states $\rho_1' = \left|\phi_0'\right\rangle\left\langle\phi_0'\right|$ and $\rho_2' = \frac{1}{2}|\phi_0\rangle\langle\phi_0| + \frac{1}{2}|\phi_1\rangle\langle\phi_1|$. So we get the MED probability to discriminate between ρ_1' and ρ_2':

$$P_{honest} = \frac{2-\sqrt{3}}{4}, \qquad (7)$$

which is equal to the value in the above fake photon attack. It means that Bob's fake photon attack cannot bring him any benefit.

Then again, Bob has to announce a fake random number sequence in step 4), because he has made a MED measurement. Alice may get a wrong answer which will be found at a later time, because Alice's key rests on the random number sequence.

3) THE JOINT-MEASUREMENT ATTACK

The carrier states and the information concerning which carrier states contribute to one final key bit are two essential elements hold simultaneously by the party who can do the JM attack. Considering Bob has the opportunity to get the carrier states and the information about which carrier states contribute to one final key bit, thus he can conduct JM attack. In more detail, in step 1) Bob can also send the first particle of $\left|\Phi_0'\right\rangle$ to Alice, then for the k quartets contributing to one final key bit, their k corresponding joint systems are defined as $|\Lambda\rangle$, would be in one state within the set $A = \left\{\otimes_{i=1}^{k}|K_i\rangle \,|\, |K_i\rangle \in \left\{\left|\Phi_0'\right\rangle, \left|\Phi_1'\right\rangle, \left|\Phi_2'\right\rangle\right\}\right\}$. Let n denote the number of 1 represented by $\left|\Phi_1'\right\rangle$ and $\left|\Phi_2'\right\rangle$ in the set $\{|K_1\rangle, |K_2\rangle, \ldots, |K_k\rangle\}$, then $|\Lambda\rangle = \otimes_{i=1}^{k}|K_i\rangle$ would be in the set

$$A_0 = \left\{\otimes_{i=1}^{k}|K_i\rangle||K_i\rangle \in \left\{|\Phi_0'\rangle, \left|\Phi_1'\right\rangle, \left|\Phi_2'\right\rangle\right\}, n \mod 2 = 0\right\},$$

when Alice got a conclusive final key bit 0 in this position, or in the set

$$A_1 = \left\{\otimes_{i=1}^{k}|K_i\rangle||K_i\rangle \in \left\{|\Phi_0'\rangle, |\Phi_1'\rangle, \left|\Phi_2'\right\rangle\right\}, n \mod 2 = 1\right\},$$

when Alice got a conclusive final key bit 1, or in the set

$$A_? = A \setminus \left\{A_0 \bigcup A_1\right\},$$

when Alice got an inconclusive final key bit.

Obviously, Bob can successfully conduct the effective JM attack without being detected only when he can identify any one of the above three sets A_i ($i \in \{0, 1, ?\}$). Nevertheless, Bob cannot identify them, because the conclusiveness of Alice's measurement results is subject to quantum randomness, and Bob cannot identify any state in $\left\{\left|\Phi_i'\right\rangle\right\}_{i=0}^{2}$

unambiguously as mentioned above. Therefore, the cheat sensitivity of our protocol still holds under JM attack. Moreover, for Bob, the JM attack is formidable, because it is more complicated than that by Alice. Alice only needs to infer the final key bit while Bob has to distinguish whether Alice has got a conclusive final key bit as well.

In conclusion, Bob takes all the attacks, and even includes JM attack, he cannot obtain any benefit, thus the user privacy can be guaranteed perfectly. It can be said that our protocol is cheat-sensitive.

B. DATABASE SECURITY

We will analyze the database security against three kinds of attacks from Alice.

1) FAKE ENTANGLED ATTACK

For the quartets received from Bob, Alice can attach an auxiliary system on the quartet as that in Eq. (3) and send the first quartet back to Bob in step 2) in order that she can measure the auxiliary systems jointly to infer the final key directly, but this attack would be detected by Bob. Obviously, the joint system, that is, system 1 and 2, would be in state $\left|\Phi_0'\right\rangle$, $\left|\Phi_1'\right\rangle = |\phi_0\rangle_1 |\varepsilon_1\rangle_2$ or $\left|\Phi_2'\right\rangle = |\phi_1\rangle_1 |\varepsilon_2\rangle_2$ with probabilities 1/2, 1/4 and 1/4 respectively after Bob's measurement. Only when Alice can identify anyone of the three states $\left\{\left|\Phi_i'\right\rangle\right\}_{i=0}^{2}$ unambiguously, she can infer whether Bob has measured the quartet in the basis $\{|\phi_0\rangle, |\phi_1\rangle\}$ or $\left\{\left|\phi_0'\right\rangle, \left|\phi_1'\right\rangle\right\}$, thus inferring the bit value of key b. As an example, once she identifies that the joint system is in state $\left|\Phi_0'\right\rangle$, Alice knows that Bob has measured the quartet in the basis $\left\{\left|\phi_0'\right\rangle, \left|\phi_1'\right\rangle\right\}$ and concludes that the value of b is 1; if the joint system is in state $\left|\Phi_1'\right\rangle$ or $\left|\Phi_2'\right\rangle$, Alice knows that Bob has measured the quartet in the basis $\{|\phi_0\rangle, |\phi_1\rangle\}$ and concludes that the value of b is 0.

However, as can be seen from the above analysis, Alice cannot identify any state in $\left\{\left|\Phi_i'\right\rangle\right\}_{i=0}^{2}$ unambiguously, so she cannot get virtual benefit without being detected.

2) FAKE PHOTON ATTACK

For the quartets received from Bob, Alice can send Bob fake photon states in order to infer more raw key bits subsequently. Without loss of generality, Alice's fake photon states can be expressed as

$$\left|\phi'\right\rangle = cos\theta\,|\phi_0\rangle + sin\theta\,|\phi_1\rangle\,, \tag{8}$$

where the parameter $\theta \in (0, \pi/2)$.

After Bob measures $\left|\phi'\right\rangle$ in the basis dtermined by the random string b, we can get the measurement results $\left|\phi_0'\right\rangle$, $\left|\phi_1'\right\rangle$, $|\phi_0\rangle$ and $|\phi_1\rangle$ with probabilities $\frac{1}{2}(cos\theta + sin\theta)^2$, $\frac{1}{2}(cos\theta - sin\theta)^2$, $cos^2\theta$ and $sin^2\theta$ respectively, which should be close to 3/8, 1/8, 1/4 and 1/4 respectively, in order to avoid being detected by Bob. That is, $\frac{1}{2}(cos\theta + sin\theta)^2 = \frac{3}{8}$, $\frac{1}{2}(cos\theta - sin\theta)^2 = \frac{1}{8}$, $cos^2\theta = \frac{1}{4}$, $sin^2\theta = \frac{1}{4}$. However, no such value of θ can satisfy these four equations simultaneously. As an example, when $cos^2\theta = \frac{1}{4}$, i.e., $\theta = \frac{\pi}{3}$, the probabilities of obtaining the measurement results $\left|\phi_0'\right\rangle$, $\left|\phi_1'\right\rangle$, $|\phi_1\rangle$ are $\frac{1}{2}(cos\theta + sin\theta)^2\big|_{\theta=\frac{\pi}{3}} = \frac{1}{8}(1+\sqrt{3})^2$, $\frac{1}{2}(cos\theta - sin\theta)^2\big|_{\theta=\frac{\pi}{3}} = \frac{1}{8}(1-\sqrt{3})^2$ and $sin^2\theta\big|_{\theta=\frac{\pi}{3}} = \frac{3}{4}$, respectively. Clearly, it means that Alice's attack will introduce some errors which will be detected by Bob with a certain probability in step 6).

3) THE JOINT-MEASUREMENT ATTACK

The only way to resist JM attack is to isolate two essential elements, that is, the carrier states and the information concerning which carrier states contribute to one final key bit, from each other. Our protocol has both of the above two elements, so it can resist the JM attack effectively. Concretely, Alice cannot make sure which of the quartets should be jointly measured to infer a final key bit without knowing the measurement results Bob announces in step 4) when she holds the quartets from Bob in step 2), and the quartets are not in her site anymore because she has to resend them back to Bob in step 2) when she knows which of the quartets should be jointly measured in step 4).

More generally, Alice can attach an auxiliary system on the quartet as that in Eq. (3) and send the first particle back to Bob in step 2) in order that she can measure the auxiliary systems jointly to infer the final key directly, but her attack will be detected by Bob. As mentioned above, because the whole system's states of Alice's auxiliary particles and the qubits 1,2,3,4 are the tensor product of Alice's auxiliary states and the initial quantum system $(\left|\phi_0'\right\rangle, |\phi_0\rangle, |\phi_1\rangle)$. This means that if Alice's attack does not desire to be detected it will not affect the entire system. In fact, under the condition $|\varepsilon_1\rangle = |\varepsilon_2\rangle$, the auxiliary system would collapse to $|\varepsilon_1\rangle$ no matter which state the quartet is in. In this case, Alice cannot obtain the final key bit even using JM attack. Therefore, our protocol is secure in terms of the database security.

IV. CONCLUSION

We have presented a QPQ protocol with perfect performance universally applicable against collective noise. It has the following excellent features:

(1) It is universally applicable against collective noise, which reduces the error rate in the protocol. Although the scheme uses entanglement coding, only single-qubit measurements are required. Therefore, the proposed protocol is feasible utilizing current technologies.

(2) It can ensure perfect user privacy. Bob can obtain the information about Alice's choice with a certain probability by taking fake entangled attack in Yang *et al.*'s protocol [1] and Wei *et al.*'s protocol [2], while in our protocol he cannot get the information at all. Furthermore, by taking fake photon attack, the probability Bob can get the information about Alice's choice is only approximately 6.7% in our protocol,

which is far less than the probability of 25% in Yang *et al.*'s protocol. Moreover, the conclusiveness of Alice's measurement results is subject to quantum randomness, so it is arduous for Bob to perform JM attack.

(3) It can ensure perfect database security. Unlike Wei *et al.*'s protocol [2], where it allows Alice to choose by herself when to obtain a conclusive result, which may result in new attacks, the conclusiveness of measurement results is subject to quantum randomness in our protocol. As a result, our protocol does not involve the intuitive attack on the database in Wei *et al.*'s protocol. Moreover, Alice's fake photon attack and the JM attack cannot bring her any benefit.

(4) It is an effective QPQ solution with high security level, using only one quantum state. Compared with Yang's protocol [45], where the protocol uses two states, our protocol uses only one state, which simplifies the protocol and reduces the communication complexity.

In the practical implementation of our protocol, only the state $|\phi_0\rangle$ needs to be prepared and can be produced by using spontaneous parametric down conversion (SPDC). The state $|\phi_0\rangle$ can be obtained from two synchronized SPDC sources for photon pairs in the singlet state $|\Psi^-\rangle$, which can be achieved by combining the devices in [44], and the other states $|\phi_1\rangle$, $|\phi_0'\rangle$ and $|\phi_1'\rangle$ can be prepared by replacing the output of the device in [44].

To the best of our knowledge, in real implementation of the protocols based on two-way quantum communication, Bob can take Trojan horse attacks, which threaten user privacy. But Alice has the ability to eliminate the threats of certain Trojan horse attacks [46], [47]. However, all potential manipulations Bob could do on the particles should be controlled by Alice, which is probably not feasible in an actual implementation. This is an inherent limitation in the development of technology.

REFERENCES

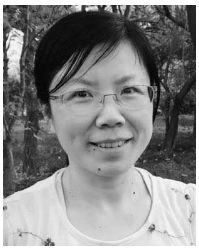
[1] Y.-G. Yang, M.-O. Zhang, and R. Yang, "Private database queries using one quantum state," *Quantum Inf. Process.*, vol. 14, no. 3, pp. 1017–1024, 2015.
[2] C.-Y. Wei, T.-Y. Wang, and F. Gao, "Practical quantum private query with better performance in resisting joint-measurement attack," *Phys. Rev. A, Gen. Phys.*, vol. 93, no. 4, p. 042318, 2016.
[3] Y. Gertner, Y. Ishai, E. Kushilevitz, and T. Malkin, "Protecting data privacy in private information retrieval schemes," *J. Comput. Syst. Sci.*, vol. 60, no. 3, pp. 592–629, 2000.
[4] H.-K. Lo, "Insecurity of quantum secure computations," *Phys. Rev. A, Gen. Phys.*, vol. 56, no. 2, p. 1154, 1997.
[5] V. Giovannetti, S. Lloyd, and L. Maccone, "Quantum private queries," *Phys. Rev. Lett.*, vol. 100, no. 23, p. 230502, 2008.
[6] F. De Martini *et al.*, "Experimental quantum private queries with linear optics," *Phys. Rev. A, Gen. Phys.*, vol. 80, no. 1, p. 010302, 2009.
[7] 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.
[8] L. Olejnik, "Secure quantum private information retrieval using phase-encoded queries," *Phys. Rev. A, Gen. Phys.*, vol. 84, no. 2, p. 022313, 2011.
[9] M. Jakobi *et al.*, "Practical private database queries based on a quantum-key-distribution protocol," *Phys. Rev. A, Gen. Phys.*, vol. 83, no. 2, p. 022301, 2011.
[10] V. Scarani, A. Acin, 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, p. 057901, 2004.
[11] 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.
[12] 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.
[13] 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.
[14] 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. 5233.
[15] Y.-G. Yang *et al.*, "Quantum private query with perfect user privacy against a joint-measurement attack," *Phys. Lett. A*, vol. 380, no. 48, pp. 4033–4038, 2016.
[16] M. V. P. Rao and M. Jakobi, "Towards communication-efficient quantum oblivious key distribution," *Phys. Rev. A, Gen. Phys.*, vol. 87, no. 1, p. 012331, 2013.
[17] 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.
[18] C.-Y. Wei, F. Gao, Q.-Y. Wen, and T. Y. Wang, "Practical quantum private query of blocks based on unbalanced-state bennett-brassard-1984 quantum-key-distribution protocol," *Sci. Rep.*, vol. 4, no. 4, p. 7537, 2014.
[19] F. Yu and D. Qiu, "Coding-based quantum private database query using entanglement," *Quantum Inf. Comput.*, vol. 14, nos. 1–2, pp. 91–106, 2014.
[20] 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. 2015, Art. no. 6600111.
[21] 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.
[22] H. Lai, M. A. Orgun, J. Pieprzyk, J. Xiao, L. Xue, and Z. Jia, "Controllable quantum private queries using an entangled fibonacci-sequence spiral source," *Phys. Lett. A*, vol. 379, nos. 40–41, pp. 2561–2568, 2015.
[23] 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.
[24] F. Yu, D. Qiu, H. Situ, X. Wang, and S. Long, "Enhancing user privacy in $SARG_{04}$-based private database query protocols," *Quantum Inf. Process.*, vol. 14, no. 11, pp. 4201–4210, 2015.
[25] Y.-G. Yang, Z.-C. Liu, X.-B. Chen, W.-F. Cao, Y.-H. Zhou, and W.-M. Shi, "Novel classical post-processing for quantum key distribution-based quantum private query," *Quantum Inf. Process.*, vol. 15, no. 9, pp. 3833–3840, 2016.
[26] S.-W. Xu, Y. Sun, and S. Lin, *Quantum Private Query Based on Single-Photon Interference*. Norwell, MA, USA: Kluwer Academic, 2016, pp. 1–10.
[27] L. Jian, Y. G. Yang, X. B. Chen, Y. H. Zhou, and W. M. Shi, "Practical quantum private database queries based on passive round-robin differential phase-shift quantum key distribution," *Sci. Rep.*, vol. 6, p. 31738, Aug. 2016.
[28] L.-Y. Zhao *et al.*, "Loss-tolerant measurement-device-independent quantum private queries," *Sci. Rep.*, vol. 7, Jan. 2017, Art. no. 39733.
[29] A. Maitra, G. Paul, and S. Roy, "Device-independent quantum private query," *Phys. Rev. A, Gen. Phys.*, vol. 95, no. 4, p. 042344, 2017.
[30] M. Xu, R.-H. Shi, Z.-Y. Luo, and Z.-W. Peng, "Nearest private query based on quantum oblivious key distribution," *Quantum Inf. Process.*, vol. 16, no. 12, p. 286, 2017.
[31] R.-H. Shi, Y. Mu, H. Zhong, J. Cui, and S. Zhang, "Privacy-preserving point-inclusion protocol for an arbitrary area based on phase-encoded quantum private query," *Quantum Inf. Process.*, vol. 16, no. 1, p. 8, 2017.
[32] 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.
[33] J. Basak and S. Maitra, "Clauser–Horne–Shimony–Holt versus three-party pseudo-telepathy: On the optimal number of samples in device-independent quantum private query," *Quantum Inf. Process.*, vol. 17, no. 4, p. 77, 2018.
[34] P. W. Shor, "Scheme for reducing decoherence in quantum computer memory," *Phys. Rev. A, Gen. Phys.*, vol. 52, no. 4, pp. R2493, 1995.

[35] X.-H. Li, F.-G. Deng, and H.-Y. Zhou, "Faithful qubit transmission against collective noise without ancillary qubits," *Appl. Phys. Lett.*, vol. 91, no. 14, p. 144101, 2007.
[36] D. B. de Brito and R. V. Ramos, "Passive quantum error correction with linear optics," *Phys. Lett. A*, vol. 352, no. 3, pp. 206–209, 2006.
[37] C. Han, Z.-W. Zhou, and G.-C. Guo, "Long distance quantum communication over a noisy channel," *J. Phys. B, At., Mol. Opt. Phys.*, vol. 39, no. 7, p. 1677, 2006.
[38] Z. D. Walton, A. F. Abouraddy, A. V. Sergienko, B. E. Saleh, and M. C. Teich, "Decoherence-free subspaces in quantum key distribution," *Phys. Rev. Lett.*, vol. 91, no. 8, p. 087901, 2003.
[39] L. Xi-Han, D. Xiao-Jiao, S. Yu-Bo, Z. Hong-Yu, and D. Fu-Guo, "Faithful quantum entanglement sharing based on linear optics with additional qubits," *Chin. Phys. B*, vol. 18, no. 9, p. 3710, 2009.
[40] J. W. Pan, C. Simon, Č. Brukner, and A. Zeilinger, "Entanglement purification for quantum communication," *Nature*, vol. 410, no. 6832, pp. 1067–1070, 2001.
[41] C. Simon and J. W. Pan, "Polarization entanglement purification using spatial entanglement," *Phys. Rev. Lett.*, vol. 89, no. 25, p. 257901, 2002.
[42] P. Zanardi and M. Rasetti, "Noiseless quantum codes," *Phys. Rev. Lett.*, vol. 79, no. 17, p. 3306, 1997.
[43] J. A. Bergou, "Discrimination of quantum states," *J. Modern Opt.*, vol. 57, no. 3, pp. 160–180, 2010.
[44] M. Bourennane, M. Eibl, S. Gaertner, C. Kurtsiefer, A. Cabello, and H. Weinfurter, "Decoherence-free quantum information processing with four-photon entangled states," *Phys. Rev. Lett.*, vol. 92, no. 10, p. 107901, 2004.
[45] Y. Yang, Z. Liu, X. Chen, Y. Zhou, and W. Shi, "Robust QKD-based private database queries based on alternative sequences of single-qubit measurements," *Sci. China Phys., Mech. Astron.*, vol. 60, no. 12, p. 120311, 2017.
[46] Q.-Y. Cai, "Eavesdropping on the two-way quantum communication protocols with invisible photons," *Phys. Lett. A*, vol. 351, nos. 1–2, pp. 23–25, 2006.
[47] F.-G. Deng, P. Zhou, X.-H. Li, C.-Y. Li, and H.-Y. Zhou. (2005). "Robustness of two-way quantum communication protocols against trojan horse attack." [Online]. Available: https://arxiv.org/abs/quant-ph/0508168

NA LI was born in Jilin, China, in 1982. She received the M.Eng. degree from the School of Computer Science and Technology, Changchun University of Science and Technology, Changchun, China, in 2011. She is currently pursuing the Ph.D. degree with the Beijing University of Posts and Telecommunications. Her main research interests include information security, quantum secure communication, and quantum cryptography.

JIAN LI received the Ph.D. degree from the Beijing Institute of Technology, in 2005. He is currently a Professor with the School of Computer Science, Beijing University of Posts and Telecommunications, Beijing, China. His research interests include information security and quantum cryptography.

XIUBO CHEN received the Ph.D. degree from the Beijing University of Posts and Telecommunications, Beijing, China, in 2009, where she is currently an Associate Professor with the School of Cyberspace Security. Her research interests include cryptography, information security, quantum network coding, and quantum private communication.



YUGUANG YANG received the Ph.D. degree from the Beijing University of Posts and Telecommunications, in 2006. She is currently a Professor with the School of Computer Science, Beijing University of Technology, Beijing, China. Her research interests include cryptography and information security.