


Article

Development of Quantum Private Queries Protocol on Collective-Dephasing Noise Channel

Jingbo Zhao ¹, Wenbin Zhang ¹, Yulin Ma ¹, Xiaohan Zhang ¹ and Hongyang Ma ^{2,*} 

¹ School of Information and Control Engineering Qingdao University of Technology, Qingdao 266033, China; zhaojingbo6666@163.com (J.Z.); zwb1996zwb1996@163.com (W.Z.); mayulin6466@163.com (Y.M.); zXH1996zXH@126.com (X.Z.)

² School of Sciences Qingdao University of Technology, Qingdao 266033, China

* Correspondence: hongyang_ma@aliyun.com

Received: 10 February 2020; Accepted: 10 March 2020; Published: 12 March 2020



Abstract: Quantum private queries can commonly protect important information in a good many of domains, such as finance, business, military, which use quantum effects to achieve unprecedented classical private queries. However, quantum state can be easily affected by environmental noise, which affects the actual effect of quantum private queries. This paper developed a new quantum private query protocol based on four qubits logical Bell state to resist the collective-dephasing noise. The symmetric private information retrieval problem, which is the most influential problem in the process of quantum private query, was solved well by quantum oblivious transfer. It introduces the construction of four qubits logical Bell state. The quantum private query protocol innovates the quantum key distribution process by using the four qubits logical Bell state as the measurement base to measure the logical qubits, and ensures the function of quantum oblivious transmission. The protocol cannot only resist the noise influence of the communication process, but also ensure the security of both sides of the communication.

Keywords: quantum private query; quantum oblivious transfer; decoherence-free state; four logical Bell states

1. Introduction

Bennett and Brassard proposed the first QKD protocol which is also known as BB84 protocol using single-photon polarization states in 1984 [1]. Since then, a lot of research on quantum cryptography has been done. After 30 years' development, the quantum cryptography protocol has been proposed for many territories including quantum key distribution protocol [2–5], quantum secret sharing protocol [6], quantum direct communication protocol [7], quantum teleportation [8] and quantum private query protocol what we will study in this paper.

Quantum private query (QPQ) is an important branch of quantum cryptography. One of the most important problems is the Symmetric Private Information Retrieval (SPIR) problem. This problem mainly involves two aspects: the first aspect is the database security problem, i.e., Bob does not want Alice to obtain any information other than the k pieces of information she wants to retrieve; the other aspect is user privacy, i.e., Alice does not want Bob to know what information she wants to query. The quantum oblivious key distribution protocol has been proposed by predecessors, which is a good solution to the SPIR problem. On this basis, this paper also improves the process of the oblivious key distribution, to improve the quantum private query protocol.

With the increasing of protocol security, various attack methods emerge one after another, such as false entanglement attack, joint-measurement (JM) attack [9], etc. Therefore, it is necessary to study a more secure, practical and efficient QPQ protocol in view of the shortcomings of the existing QPQ protocol. In the communication process, photons inevitably face noise interference caused by thermal fluctuations, vibration and optical fiber defects. Therefore, from the perspective of practical implementation feasibility, it is very important to eliminate the negative effects of noise. There are many methods to resist the environmental noise on quantum private query. In reference [3], quantum error correction code is used to eliminate the influence of environmental noise. Decoherence-free (DF) [10] states are also used to resist collective noise [11]. Because decoherence-free state has the characteristic of resisting the invariance of collective noise, we use it to resist collective noise in this paper.

Based on the above analysis, this paper improves the process of quantum oblivious key distribution. The logical Bell state (i.e., 4 qubit decoherence-free state) [11] is used to overcome the collective-dephase noise and improve the quantum private query protocol. In addition, database security and user privacy can be guaranteed.

2. Background

2.1. Logical Bell State on Collective-Dephasing Noise

With the change of collective-dephasing noise [12–15], the horizontally polarized state of a photon $|0\rangle$ will remain, the vertically polarized state of a photon $|1\rangle$ will be turned into $e^{i\varphi}|1\rangle$, that φ is the parameter of the collective-dephasing noise changing with time. Two logical qubits are defined as $|0_{dp}\rangle = |01\rangle$ and $|1_{dp}\rangle = |10\rangle$, they can resist the collective-dephasing noise [16]. Their superposition state is $|\pm_{dp}\rangle = \frac{1}{\sqrt{2}}(|0_{dp}\rangle \pm |1_{dp}\rangle) = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$. The entanglement swapping between the four logical Bell states described in formula (1) can also immune to the collective-dephasing noise. Over here $|\phi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$ and $|\psi^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$ are four original Bell state [17]. Clearly, these logical Bell states can be distinguished from one another by applying two Bell state measurements to the first and third qubits and the second and fourth qubits [18].

$$\begin{aligned}
 |\Phi_{dp}^+\rangle_L &= \frac{1}{\sqrt{2}}(|0_{dp}\rangle_L|0_{dp}\rangle_L + |1_{dp}\rangle_L|1_{dp}\rangle_L) \\
 &= \frac{1}{\sqrt{2}}(|\phi^+\rangle_{13}|\phi^+\rangle_{24} - |\phi^-\rangle_{13}|\phi^-\rangle_{24}) \\
 |\Phi_{dp}^-\rangle_L &= \frac{1}{\sqrt{2}}(|0_{dp}\rangle_L|0_{dp}\rangle_L - |1_{dp}\rangle_L|1_{dp}\rangle_L) \\
 &= \frac{1}{\sqrt{2}}(|\phi^-\rangle_{13}|\phi^+\rangle_{24} - |\phi^+\rangle_{13}|\phi^-\rangle_{24}) \\
 |\Psi_{dp}^+\rangle_L &= \frac{1}{\sqrt{2}}(|0_{dp}\rangle_L|1_{dp}\rangle_L + |1_{dp}\rangle_L|0_{dp}\rangle_L) \\
 &= \frac{1}{\sqrt{2}}(|\psi^+\rangle_{13}|\psi^+\rangle_{24} - |\psi^-\rangle_{13}|\psi^-\rangle_{24}) \\
 |\Psi_{dp}^-\rangle_L &= \frac{1}{\sqrt{2}}(|0_{dp}\rangle_L|1_{dp}\rangle_L - |1_{dp}\rangle_L|0_{dp}\rangle_L) \\
 &= \frac{1}{\sqrt{2}}(|\psi^-\rangle_{13}|\psi^+\rangle_{24} - |\psi^+\rangle_{13}|\psi^-\rangle_{24})
 \end{aligned} \tag{1}$$

2.2. Entanglement Swapping Results of Logical Bell States on Collective-Dephasing Noise

When we are in the context of the collective-dephasing noise channel, we can perform an entanglement swapping of two logical Bell states. For example, if we want to do the entanglement swapping on the logical Bell states $|\Phi_{dp}^+\rangle$ and $|\Phi_{dp}^-\rangle$, the only thing we need to do is to take Bell measure on the four qubits of the two logical Bell states. Each subscript represents the order in which the qubits are located [19]. Let us take an example to illustrate. When the measuring result is $|\phi^+\phi^+\rangle$, it means that the logical Bell state we choose is $|\Phi_{dp}^+\rangle$. We show the entanglement swapping results of all the logical Bell states in Table 1.

$$\begin{aligned}
 |\Phi_{dp}^+\rangle_{1234} \otimes |\Phi_{dp}^+\rangle_{5678} &= \frac{1}{\sqrt{2}}(|0_{dp}\rangle|0_{dp}\rangle + |1_{dp}\rangle|1_{dp}\rangle)_{1234} \\
 &\otimes \frac{1}{\sqrt{2}}(|0_{dp}\rangle|0_{dp}\rangle + |1_{dp}\rangle|1_{dp}\rangle)_{5678} \\
 &= \frac{1}{\sqrt{2}}(|00110011\rangle + |01100110\rangle \\
 &+ |10011001\rangle + |11001100\rangle)_{15263748} \\
 &= \frac{1}{4}(|\phi^+\phi^+\rangle|\phi^+\phi^+\rangle - |\phi^+\phi^+\rangle|\phi^-\phi^-\rangle \\
 &+ |\phi^+\phi^-\rangle|\phi^+\phi^-\rangle - |\phi^+\phi^-\rangle|\phi^-\phi^+\rangle \\
 &- |\phi^-\phi^+\rangle|\phi^+\phi^-\rangle + |\phi^-\phi^+\rangle|\phi^-\phi^+\rangle \\
 &- |\phi^-\phi^-\rangle|\phi^+\phi^+\rangle + |\phi^-\phi^-\rangle|\phi^-\phi^-\rangle \\
 &+ |\psi^+\psi^+\rangle|\psi^+\psi^+\rangle - |\psi^+\psi^+\rangle|\psi^-\psi^-\rangle \\
 &+ |\psi^+\psi^-\rangle|\psi^+\psi^-\rangle - |\psi^+\psi^-\rangle|\psi^-\psi^+\rangle \\
 &- |\psi^-\psi^+\rangle|\psi^+\psi^-\rangle + |\psi^-\psi^+\rangle|\psi^-\psi^+\rangle \\
 &- |\psi^-\psi^-\rangle|\psi^+\psi^+\rangle + |\psi^-\psi^-\rangle|\psi^-\psi^-\rangle)_{15263748} \\
 &= \frac{1}{2}(|\Phi_{dp}^+\rangle|\Phi_{dp}^+\rangle + |\Phi_{dp}^-\rangle|\Phi_{dp}^-\rangle \\
 &+ |\Psi_{dp}^+\rangle|\Psi_{dp}^+\rangle + |\Psi_{dp}^-\rangle|\Psi_{dp}^-\rangle)_{15263748}
 \end{aligned} \tag{2}$$

Table 1. Entanglement swapping results of arbitrary two logical Bell states under collective-dephasing noises.

Two Logical Bell States	Two Logical Bell States after Entanglement Swapping
$[(\Phi_{dp}^+\rangle, \Phi_{dp}^+\rangle), (\Phi_{dp}^-\rangle, \Phi_{dp}^-\rangle), (\Psi_{dp}^+\rangle, \Psi_{dp}^+\rangle), (\Psi_{dp}^-\rangle, \Psi_{dp}^-\rangle)]_{12345678}$	00
$[(\Phi_{dp}^+\rangle, \Phi_{dp}^-\rangle), (\Phi_{dp}^-\rangle, \Phi_{dp}^+\rangle), (\Psi_{dp}^+\rangle, \Psi_{dp}^-\rangle), (\Psi_{dp}^-\rangle, \Psi_{dp}^+\rangle)]_{12345678}$	01
$[(\Phi_{dp}^+\rangle, \Psi_{dp}^+\rangle), (\Phi_{dp}^-\rangle, \Psi_{dp}^-\rangle), (\Psi_{dp}^+\rangle, \Phi_{dp}^+\rangle), (\Psi_{dp}^-\rangle, \Phi_{dp}^-\rangle)]_{12345678}$	10
$[(\Phi_{dp}^+\rangle, \Psi_{dp}^-\rangle), (\Phi_{dp}^-\rangle, \Psi_{dp}^+\rangle), (\Psi_{dp}^+\rangle, \Phi_{dp}^-\rangle), (\Psi_{dp}^-\rangle, \Phi_{dp}^+\rangle)]_{12345678}$	11

What we are going to do is encode the original Bell state into two bits of classical information, Their correspondence are $|\phi^+\rangle$, $|\phi^-\rangle$, $|\psi^+\rangle$ and $|\psi^-\rangle$ for “00”, “01”, “10”, and “11”, respectively. After calculation, it is not difficult to deduce that the encoding of the two original Bell states is the

same before and after the XOR operation, and this property is still true in the logical Bell state. In this case, the corresponding rule of the code becomes $|\Phi_{dp}^+\rangle, |\Phi_{dp}^-\rangle, |\Psi_{dp}^+\rangle$ and $|\Psi_{dp}^-\rangle$ for “00”, “01”, “10”, and “11”. The subscript “ dp ” in the formula indicates that the logical Bell state can resist the collective-dephasing noise.

3. Protocol Process

Quantum private query protocol consists of three parts: key distribution, post-processing and information acquisition.

In the second stage, after post-processing, the key will be diluted, to the point that Alice only knows a few keys and Bob knows all keys [20]. The optimal outcome is that Alice only knows one bit of information of all keys, and Bob does not know where the bit that Alice knows is in all keys [21–23]. Among them, step (1) to step (5) are the quantum key distribution process, step (6) to step (9) are the post-processing process, and step (10) to step (11) are the information acquisition process. The protocol process will be described in detail:

Quantum key distribution process:

Step1: Bob creates a string of particles and sends the particles to Alice, each one of them is randomly placed in one of four quantum states of $\{|0_{dp}0_{dp}\rangle, |1_{dp}1_{dp}\rangle, |0_{dp}1_{dp}\rangle, |1_{dp}0_{dp}\rangle\}$. Among them $\{|0_{dp}0_{dp}\rangle, |1_{dp}1_{dp}\rangle\}$ represent classical bit “0” and $\{|0_{dp}1_{dp}\rangle, |1_{dp}0_{dp}\rangle\}$ represent classical bit “1”.

Step2: Alice receives the particles and uses two measurement base “+”, “-” to measure each particle at random. Thereinto “+” = $\{|\Phi_{dp}^+\rangle, |\Phi_{dp}^-\rangle\}$ and “-” = $\{|\Psi_{dp}^+\rangle, |\Psi_{dp}^-\rangle\}$. These four states respectively correspond to $\{|0_{dp}0_{dp}\rangle, |0_{dp}1_{dp}\rangle, |1_{dp}0_{dp}\rangle, |1_{dp}1_{dp}\rangle\}$.

Step3: Alice declares which positions the particles are in, discarding the rest.

Step4: For each particle that Alice gets the result of measurement, Bob declares two states: one is the logical Bell state corresponding to the particle that was just sent, and the other is the random logical Bell state under the other base. Alice can speculate the particle state with a half probability. The deterministic results are shown in Table 2 and the uncertain results are shown in Table 3 below.

Table 2. Deterministic results.

Quantum States Sent by Bob	Measurement Selected by Alice	Possible Measurement	The States of Bob’s Statement	The Results of Alice’s Measurement
$ 0_{dp}0_{dp}\rangle(\Phi_{dp}^+\rangle)$	$\{ \Phi_{dp}^+\rangle, \Phi_{dp}^-\rangle\}$	$ \Phi_{dp}^+\rangle$	$\{ \Phi_{dp}^+\rangle, \Psi_{dp}^+\rangle\}$	$ \Phi_{dp}^+\rangle$
		$ \Phi_{dp}^-\rangle$	$\{ \Phi_{dp}^+\rangle, \Psi_{dp}^-\rangle\}$	$ \Phi_{dp}^+\rangle$
		$ \Phi_{dp}^+\rangle$	$\{ \Phi_{dp}^+\rangle, \Psi_{dp}^+\rangle\}$	$ \Phi_{dp}^-\rangle$
		$ \Phi_{dp}^-\rangle$	$\{ \Phi_{dp}^+\rangle, \Psi_{dp}^-\rangle\}$	$ \Phi_{dp}^-\rangle$
$ 0_{dp}1_{dp}\rangle(\Phi_{dp}^-\rangle)$	$\{ \Psi_{dp}^+\rangle, \Psi_{dp}^-\rangle\}$	$ \Psi_{dp}^+\rangle$	$\{ \Phi_{dp}^-\rangle, \Psi_{dp}^+\rangle\}$	$ \Psi_{dp}^+\rangle$
		$ \Psi_{dp}^-\rangle$	$\{ \Phi_{dp}^-\rangle, \Psi_{dp}^-\rangle\}$	$ \Psi_{dp}^+\rangle$
		$ \Psi_{dp}^-\rangle$	$\{ \Phi_{dp}^-\rangle, \Psi_{dp}^+\rangle\}$	$ \Psi_{dp}^-\rangle$
		$ \Psi_{dp}^+\rangle$	$\{ \Phi_{dp}^-\rangle, \Psi_{dp}^-\rangle\}$	$ \Psi_{dp}^-\rangle$
$ 1_{dp}0_{dp}\rangle(\Psi_{dp}^+\rangle)$	$\{ \Psi_{dp}^+\rangle, \Psi_{dp}^-\rangle\}$	$ \Psi_{dp}^+\rangle$	$\{ \Psi_{dp}^+\rangle, \Phi_{dp}^+\rangle\}$	$ \Psi_{dp}^+\rangle$
		$ \Psi_{dp}^-\rangle$	$\{ \Psi_{dp}^+\rangle, \Phi_{dp}^-\rangle\}$	$ \Psi_{dp}^+\rangle$
		$ \Psi_{dp}^-\rangle$	$\{ \Psi_{dp}^+\rangle, \Phi_{dp}^+\rangle\}$	$- \Psi_{dp}^-\rangle$
		$ \Psi_{dp}^+\rangle$	$\{ \Psi_{dp}^+\rangle, \Phi_{dp}^-\rangle\}$	$- \Psi_{dp}^-\rangle$
$ 1_{dp}1_{dp}\rangle(\Psi_{dp}^-\rangle)$	$\{ \Phi_{dp}^+\rangle, \Phi_{dp}^-\rangle\}$	$ \Phi_{dp}^+\rangle$	$\{ \Psi_{dp}^-\rangle, \Phi_{dp}^+\rangle\}$	$ \Phi_{dp}^+\rangle$
		$ \Phi_{dp}^-\rangle$	$\{ \Psi_{dp}^-\rangle, \Phi_{dp}^-\rangle\}$	$ \Phi_{dp}^+\rangle$
		$ \Phi_{dp}^-\rangle$	$\{ \Psi_{dp}^-\rangle, \Phi_{dp}^+\rangle\}$	$- \Phi_{dp}^-\rangle$
		$ \Phi_{dp}^+\rangle$	$\{ \Psi_{dp}^-\rangle, \Phi_{dp}^-\rangle\}$	$- \Phi_{dp}^-\rangle$

Table 3. Indeterminate results.

Quantum States sent by Bob	Measurement Selected by Alice	Possible Measurement	The States of Bob's Statement	The Results of Alice's Measurement
$ 0_{dp}0_{dp}\rangle(\Phi_{dp}^+\rangle)$	$\{ \Psi_{dp}^+\rangle, \Psi_{dp}^-\rangle\}$	$ \Psi_{dp}^+\rangle$	$\{ \Phi_{dp}^+\rangle, \Psi_{dp}^+\rangle\}$?
		$ \Psi_{dp}^-\rangle$	$\{ \Phi_{dp}^+\rangle, \Psi_{dp}^-\rangle\}$?
$ 0_{dp}1_{dp}\rangle(\Phi_{dp}^-\rangle)$	$\{ \Phi_{dp}^+\rangle, \Phi_{dp}^-\rangle\}$	$ \Phi_{dp}^+\rangle$	$\{ \Phi_{dp}^+\rangle, \Psi_{dp}^+\rangle\}$?
		$ \Phi_{dp}^-\rangle$	$\{ \Phi_{dp}^-\rangle, \Psi_{dp}^-\rangle\}$?
$ 1_{dp}0_{dp}\rangle(\Psi_{dp}^+\rangle)$	$\{ \Phi_{dp}^+\rangle, \Phi_{dp}^-\rangle\}$	$ \Phi_{dp}^+\rangle$	$\{ \Phi_{dp}^-\rangle, \Psi_{dp}^+\rangle\}$?
		$ \Phi_{dp}^-\rangle$	$\{ \Phi_{dp}^+\rangle, \Psi_{dp}^-\rangle\}$?
$ 1_{dp}1_{dp}\rangle(\Psi_{dp}^-\rangle)$	$\{ \Psi_{dp}^+\rangle, \Psi_{dp}^-\rangle\}$	$ \Psi_{dp}^+\rangle$	$\{ \Psi_{dp}^+\rangle, \Phi_{dp}^+\rangle\}$?
		$ \Psi_{dp}^-\rangle$	$\{ \Psi_{dp}^-\rangle, \Phi_{dp}^-\rangle\}$?

Step5: Bob keeps all the bits that Alice had measured as the oblivious keys, in the ideal case, Alice would only know a half of them, but Bob does not know which bits Alice got.

Post-processing process:

Step6: Next, we use a more advanced post-processing method to improve the security of the protocol [24]. After quantum key distribution, Bob and Alice will get an n-bit raw key, which we define as R. Bob knows every qubit information in R and Alice only knows a half of them, N represents the number of entries. R can be expressed as q_1, q_2, \dots, q_N , thereinto, q_j represents the j th digit in the raw key. Calculate $Q_j \sum_{m=0}^{l-1} (q_{j-m} + q_{j+m})$, thereinto, $q_{N+x} := q_x, 1 \leq x \leq l, j = 1, 2, 3, \dots, N, l$ is a security limits.

Step7: Convert Q_j to the binary number $Q'_j = p_1^j, p_2^j, \dots, p_{\lceil \log(2l+1) \rceil}^j$.

Step8: To get the j th bit of the final key, we need to perform an XOR addition operation on all the bits of Q'_j . The expression is as follows:

$$O_j = \bigoplus_{i=1}^{\lceil \log(2l+1) \rceil} p_i^j \tag{3}$$

Step9: If Alice does not produce the final key bit at the end of the above step, repeat the quantum oblivious key distribution step.

Information acquisition process:

Step10: Alice and Bob correspond "0" and "1" to an n-bit $K = \{b_1, b_2, \dots, b_n\}$ and $\bar{K} = \{\bar{b}_1, \bar{b}_2, \dots, \bar{b}_n\}$ random number, where n is the length of the entry in the database. The "n" could be any number. Thereinto, $\bar{b}_i = 1 \oplus b_i, b_i = \{0, 1\}$. By generating O_j with the corresponding n-bit random number, then, we get the final key O. To be specific, when we get O_j as 0 (1), then we will know the j th position of the final key O'_j is the value of $K(\bar{K})$.

Step11: After Alice knows the i th $K(\bar{K})$ in the final key O, if she wants to retrieve X_j on the j th position of the final key, Alice announces a number "s", where $s = j - i$. Bob shifts the key O by s, then he uses the

shifted key O' to encrypt his own database. Finally, Alice can use the key $K(\bar{K})$ to get the information X_j she wants.

4. Security Analysis

4.1. Database Security Analysis

When Alice is dishonest, Bob will be considered to be the honest one automatically. Next, we will focus on database security and analyze what the impact of Alice’s attack has on database security. A defect was found in reference [25], i.e., the parity check information of two consecutive key bits O_j and O_{j+1} can be derived from the generated key bits q_j and q_{j+k} . If q_j and q_{j+k} have been tested successfully, then the parity check information of O_j and O_{j+1} will be derived. The scheme mentioned in this article provides more protection for parity between key bits, $2l + 1$ raw key bit addition operation is mainly used in this post-processing process. After the decimal to binary conversion and the subsequent XOR addition operation, Alice’s threat to the database is greatly reduced and the security of the database is increased [26,27].

The final key bit O_j in reference [28] is generated by calculating $O_j = XOR(q_j, q_{j+1}, \dots, q_{j+k-1})$, the parity information of the k qubits is represented by the final key. Because of the special way that the final key bit is generated, odd-even check will not damage the $2l + 1$ qubits in this scheme. Following the method in step (6) to generate the final key, we calculate $\sum_{m=0}^{m=l} (q_{j-m} + q_{j+m})$ first, and convert it to binary form $p_1^j, p_2^j, \dots, p_{[\log(2l+1)]}^j, j = 1, 2, \dots, N$, then get the final key bit O_j . To verify, we assume that $l = 2$, the possible values of $q_{j-2}, q_{j-1}, q_j, q_{j+1}, q_{j+2}$ are {00000, 00001, 00010, 00011, 00100, 00101, 00110, 00111, 01000, 01001, 01010, 01011, 01100, 01101, 01110, 01111, 10000, 10001, 10010, 10011, 10100, 10101, 10110, 10111, 11000, 11001, 11010, 11011, 11100, 11101, 11110, 11111}. The possible decimal set is {0, 1, 2, 3, 4, 5}, the corresponding binary number is {000, 001, 010, 011, 100, 101}. Performing formula(3) operation on the resulting binary number, then the corresponding XOR of 000, 001, 010, 011, 100, 101 is 0, 1, 1, 0, 1, 0. According to the above analysis, we found that $q_{j-2}, q_{j-1}, q_j, q_{j+1}, q_{j+2}$ have no linear correlation to the final key bit. Therefore, it can be proved that the joint measurement is invalid.

In case of that Alice’s registers have quantum memory, it is possible for Alice to delay Bob’s measurements after he announces his state during the quantum oblivious key distribution phase. If Alice is going to make a joint quantum measurement for $2l + 1$ qubits, as the analysis we have mentioned above, the final key bit 0 corresponds to the possible initial value of {00000, 00111, 01011, 01101, 01110, 10011, 10101, 10110, 11001, 11010, 11100, 11111} and 1 corresponds to a possible initial value of {00001, 00010, 00011, 00100, 00101, 00110, 01000, 01001, 01010, 01100, 01111, 10000, 10001, 10010, 10100, 10111, 11000, 11011, 11101, 11110}. We can assume that all the five states Bob publishes are logical Bell states $\{|\Phi_{dp}^+\rangle, |\Psi_{dp}^-\rangle\}$, Alice can make the unambiguous state discrimination (USD) [29,30] on $p_0^{O_j}$ and $p_1^{O_j}$ to clearly distinguish the two mixed states corresponding to parity.

Reference [30] points out that the probability Q_F of clearly distinguishing the minimum failure is at least twice the probability P_E of the minimum error of two arbitrarily mixed quantum states in the fuzzy discrimination. Therefore, we should use a fuzzy test to get the most information. The conclusion of reference [20] is used to distinguish the two mixed states p_1 and p_2 under the prior probability of ρ_1 and ρ_2 , thereinto, $p_1 + p_2 = 1, P_E = \frac{1}{2} - \frac{1}{2}Tr|p_2\rho_2 - p_1\rho_1|$. For the other operand σ , it has $|\sigma| = \sqrt{\sigma + \sigma}$. The smallest error probability to distinguish $p_0^{O_j}$ from $p_1^{O_j}$ is

$$P_E = \frac{1}{2} - \frac{1}{2}Tr|\frac{3}{8}p_0^{O_j} - \frac{5}{8}p_1^{O_j}| = 0.262 \tag{4}$$

We can use the same way to calculate the other minimum error probability of l . Given the database size N , Alice can get a certain number of bits $\bar{n} = P_E[\frac{N}{2l+1}]$. As l increases, the certain number of bits \bar{n} is decreasing. Therefore, Alice’s advantage of using unambiguous state discrimination attacks is significantly reduced.

4.2. User Privacy Security Analysis

When Bob is dishonest, Alice will be considered to be the honest one automatically. This protocol is similar to many other QPQ protocols, since user privacy are sensitive to fraud and the nonorthogonal quantum states are used to protect user security. In this scenario, there is no measurement that allows Bob to know the deterministic results and Alice’s bit information. If Bob tries to obtain benefits by operating a single qubit q_j , this operation will affect the accuracy probability of $2l + 1$ key bits which uses the q_j . Therefore, bringing in a value error into $2l + 1$ key bits is easier to detect by Alice.

In addition, value errors will lead Bob to shift the final key bit incorrectly, giving completely random answers during the classic secret query phase and causing an error in the user’s query result. They will have negative impacts on the reputation of the database owner.

4.3. The Eva Attack

Suppose there is a third-party eavesdropper Eve in the communication process.

If Eve intercepts the initial quantum state that Bob sends to Alice in step (1): Because Eve cannot tell which one of the four states $\{|0_{dp}0_{dp}\rangle, |1_{dp}1_{dp}\rangle, |0_{dp}1_{dp}\rangle, |1_{dp}0_{dp}\rangle\}$ that she has intercepted, and the measurement will cause the original quantum state to collapse, Bob and Alice will find the presence of the eavesdropper.

If Eve intercepts the detected particles declared by Alice in step (3): Because Bob declares two states in step (4), and Alice’s choice of measurement base is random in step (2). Eve does not know the measurement base chosen by Alice, then, Eve cannot determine the result of the key obtained by Alice. So, Eve’s attack is invalid. Let us elaborate it with an example. Assuming the initial state is $|0_{dp}0_{dp}\rangle$, when Bob declares $\{|\Phi_{dp}^+\rangle, |\Psi_{dp}^+\rangle\}$ and only Alice makes a measurement with "+" base, then Alice can get the result. To make the result intuitively, after omitting the denominator and the distribution probability, the formulas are expressed as:

$$\begin{aligned} \langle \Phi_{dp}^+ | 0_{dp}0_{dp} \rangle | \Phi_{dp}^+ \rangle &= | \Phi_{dp}^+ \rangle \\ \langle \Phi_{dp}^- | 0_{dp}0_{dp} \rangle | \Phi_{dp}^- \rangle &= | \Phi_{dp}^- \rangle \end{aligned} \tag{5}$$

Third-party attack is a threat based on quantum state transmission. In our protocol, only Bob prepares the initial quantum state and sends it to Alice, Alice does not send the quantum state back to Bob. If Eve eavesdrops this process, it is meaningless for her to obtain the initial quantum state.

5. Conclusions

This paper mainly studies the quantum private query protocol based on logical Bell state in the environment of collective-dephasing noise. We proposed a new method of quantum oblivious key distribution to develop a new quantum private query protocol based on four qubits logical Bell state. Logical Bell state is used as measurement basis to measure the logical quantum bits. The function of quantum oblivious transmission can be ensured. By mapping one bit $0(1)$ to multi-bit key $K(\bar{K})$, multi-bit queries can be implemented in a single query. The complexity of communication can be reduced.

The method we use to obtain the final key ensures that the whole parity information of $2l + 1$ qubits will not be affected. By analyzing the attack from the user Alice and the attack from the database owner Bob, it is verified that this scheme is sensitive to spoofing and can resist the joint quantum state measurement attack effectively. By analyzing third-party attacks, Eva could not obtain valid information in the communication process. Therefore, this protocol cannot only resist the noise influence of the communication process, but also ensure the security of both sides of the communication.

Author Contributions: Methodology, W.Z.; Investigation, W.Z.; Writing—Original Draft Preparation, Y.M.; Writing—Review and Editing, X.Z.; Supervision, J.Z. and H.M. All authors have read and agreed to the published version of the manuscript.

Funding: The work was supported by the Shandong Province Higher Educational Science and Technology Program (Grant No. J18KZ012), the National Natural Science Foundation of China (Grant Nos.11975132, 61772295), and the Shandong Provincial Natural Science Foundation, China (Grant No. ZR2019YQ01).

Conflicts of Interest: The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

Abbreviations

The following abbreviations are used in this manuscript:

QPQ	Quantum Private Query
QKD	Quantum Key Distribution
SPIR	Symmetric Private Information Retrieval
JM	Joint-Measurement
DF	Decoherence-Free

References

1. Bennett, C.H.; Brassard, G. Quantum cryptography: Public-key distribution and coin tossing. In Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, 9–12 December 1984; pp. 175–179.
2. Ma, H.; Teng, J.; Hu, T.; Shi, P.; Wang, S. Co-communication Protocol of Underwater Sensor Networks with Quantum and Acoustic Communication Capabilities. *Wireless Pers Commun.* Available online: <https://doi.org/10.1007/s11277-020-07192-7> (accessed on 6 February 2020). [[CrossRef](#)]
3. Shi, P.; Li, N.; Wang, S.; Liu, Z.; Ren, M.; Ma, H. Quantum Multi-User Broadcast Protocol for the “Platform as a Service” Model. *Sensors* **2019**, *19*, 5257. [[CrossRef](#)] [[PubMed](#)]
4. Ma, H.-Y.; Xu, P.-A.; Shao, C.-H.; Chen, L.; Li, J.-X.; Pan, Q. Quantum Private Query Based on Stable Error Correcting Code in the Case of Noise. *Int. J. Theor. Phys.* **2019**, *58*, 4241–4248.
5. Teng, J.; Ma, H. Dynamic asymmetric group key agreement protocol with traitor traceability. *IET Inf. Secur.* **2019**, *13*, 703–710. [[CrossRef](#)]
6. Hillery, M.; Buzek, V.; Berthiaume, A. Quantum secret sharing. *Phys. Rev. A* **1999**, *59*, 1829–1834. [[CrossRef](#)]
7. Long, G.L.; Liu, X.S. Theoretically efficient high-capacity quantum-key-distribution scheme. *Phys. Rev. A* **2002**, *65*, 032302. [[CrossRef](#)]
8. Yang, L.; Ma, H.; Zheng, C.; Ding, X.; Gao, J.; Long, G. Quantum secure communication scheme based on quantum teleportation. *J. Phys.* **2017**, *66*, 37–47.
9. Wei, C.Y.; Wang, T.Y.; Gao, F. Practical quantum private query with better performance in resisting joint-measurement attack. *Phys. Rev. A* **2016**, *93*, 042318. [[CrossRef](#)]
10. Walton, Z.D.; Abouraddy, A.F.; Sergienko, A.V.; Saleh, B.E.; Teich, M.C. Decoherence-free subspaces in quantum key distribution. *Phys. Rev. Lett.* **2003**, *91*, 087901. [[CrossRef](#)]
11. Ye, T. Error tolerance of quantum steganography over collective noise channel. *Sci. China Phys. Mech. Astron.* **2015**, *1*, 010301. [[CrossRef](#)]

12. Lin, J.; Hwang, T. Bell state entanglement swappings over collective noises and their applications on quantum cryptography. *Quant. Inf. Process.* **2013**, *12*, 1089–1107. [[CrossRef](#)]
13. Yang, C.; Guo, Y.N.; Peng, H.P.; Lu, Y.B. Dynamics of local quantum uncertainty for a two-qubit system under dephasing noise. *Laser Phys.* **2019**, *30*, 015203. [[CrossRef](#)]
14. Chang, L.W.; Zhang, Y.Q.; Tian, X.X.; Qian, Y.H.; Zheng, S.H. Fault tolerant controlled quantum dialogue against collective noise. *Chin. Phys. B* **2020**, *29*, 010304. [[CrossRef](#)]
15. Li, X.H.; Deng, F.G.; Zhou, H.Y. Faithful qubit transmission against collective noise without ancillary qubits. *Appl. Phys. Lett.* **2007**, *91*, 144101. [[CrossRef](#)]
16. Zhang, Z.J. Robust multiparty quantum secret key sharing over two collective-noise channels. *Phys. A* **2006**, *361*, 233–238. [[CrossRef](#)]
17. Gu, B.; Mu, L.; Ding, L.; Zhang, C.; Li, C. Fault tolerant three-party quantum secret sharing against collective noise. *Opt. Commun.* **2010**, *283*, 3099–3103. [[CrossRef](#)]
18. Yang, C.W.; Tsai, C.W.; Hwang, T. Fault tolerant two-step quantum secure direct communication protocol against collective noises. *Sci. China Phys. Mech. Astron.* **2011**, *54*, 496–501. [[CrossRef](#)]
19. Hsieh, C.R.; Tsai, C.W.; Hwang, T. Quantum secret sharing using GHZ-like state. *Commun. Theor. Phys.* **2010**, *54*, 1019.
20. Shi, W.X.; Liu, X.T.; Wang, J.; Tang, C.J. Multi-Bit Quantum private query. *Commun. Theor. Phys.* **2015**, *64*, 299–304. [[CrossRef](#)]
21. Yang, Y.G.; Yang, R.; Cao, W.F.; Chen, X.B.; Zhou, Y.H.; Shi, W.M. Flexible quantum oblivious transfer. *Int. J. Theor. Phys.* **2017**, *56*, 1286–1297. [[CrossRef](#)]
22. Yang, Y.G.; Sun, S.J.; Wang, Y. Quantum oblivious transfer based on a quantum symmetrically private information retrieval protocol. *Int. J. Theor. Phys.* **2015**, *54*, 910–916. [[CrossRef](#)]
23. Jakobi, M.; Simon, C.; Gisin, N.; Bancal, J.D.; Branciard, C.; Walenta, N.; Zbinden, H. Practical private database queries based on a quantum-key-distribution protocol. *Phys. Rev. A* **2011**, *83*, 022301. [[CrossRef](#)]
24. Yang, Y.G.; Liu, Z.C.; Chen, X.B.; Cao, W.F.; Zhou, Y.H.; Shi, W.M. Novel classical post-processing for quantum key distribution-based quantum private query. *Quant. Inf. Process.* **2016**, *15*, 3833–3840. [[CrossRef](#)]
25. Bennett, C.H.; Brassard, G.; Popescu, S.; Schumacher, B.; Smolin, J.A.; Wootters, W.K. Purification of noisy entanglement and faithful teleportation via noisy channels. *Phys. Rev. Lett.* **1996**, *76*, 722–725. [[CrossRef](#)]
26. Wei, C.Y.; Cai, X.Q.; Liu, B.; Wang, T.Y.; Gao, F. A generic construction of quantum-oblivious-key transfer-based private query with ideal database security and zero failure. *IEEE Trans. Comput.* **2017**, *67*, 2–8. [[CrossRef](#)]
27. Gao, F.; Qin, S.J.; Huang, W.; Wen, Q.Y. Quantum private query: A new kind of practical quantum cryptographic protocol. *Sci. China Phys. Mech. Astron.* **2019**, *62*, 70301. [[CrossRef](#)]
28. Rao, M.V.P.; Jakobi, M. Towards communication-efficient quantum oblivious key distribution. *Phys. Rev. A* **2013**, *87*, 012331.
29. Raynal, P. Unambiguous state discrimination of two density matrices in quantum information theory. *arXiv* **2006**, arXiv:0611133.
30. Herzog, U.; Bergou, J.A. Optimum unambiguous discrimination of two mixed quantum states. *Phys. Rev. A* **2005**, *71*, 050301. [[CrossRef](#)]

