Computers, Materials & Continua CMC, vol.64, no.3, pp.1915-1928, 2020

Privacy-Preserving Decision Protocols Based on Quantum Oblivious Key Distribution

Kejia Zhang[1, 2, 3, 4], Chunguang Ma[5], Zhiwei Sun[4, 6, *], Xue Zhang[2, 3], Baomin Zhou[2] and Yukun Wang[7]

Abstract: Oblivious key transfer (OKT) is a fundamental problem in the field of secure multi-party computation. It makes the provider send a secret key sequence to the user obliviously, i.e., the user may only get almost one bit key in the sequence which is unknown to the provider. Recently, a number of works have sought to establish the corresponding quantum oblivious key transfer model and rename it as quantum oblivious key distribution (QOKD) from the well-known expression of quantum key distribution (QKD). In this paper, a new QOKD model is firstly proposed for the provider and user with limited quantum capabilities, where both of them just perform computational basis measurement for single photons. Then we show that the privacy for both of them can be protected, since the probability of getting other's raw-key bits without being detected is exponentially small. Furthermore, we give the solutions to some special decision problems such as set-member decision and point-inclusion by announcing the improved shifting strategies followed QOKD. Finally, the further discussions and applications of our ideas have been presented.

Keywords: Quantum cryptography, quantum computing, privacy-preserving, quantum oblivious key distribution, set-member decision, point-inclusion decision.

[1] School of Computer Science and Technology, Harbin Engineering University, Harbin, 150001, China.

[2] School of Mathematical Science, Heilongjiang University, Harbin, 150080, China.

[3] State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, 100876, China.

[4] Center for Quantum Computing, Peng Cheng Laboratory, Shenzhen, 518055, China.

[5] College of Computer Science and Engineering, Shandong University of Science and Technology, Qingdao, 266590, China.

[6] School of Artificial Intelligence, Shenzhen Polytechnic, Shenzhen, 518055, China.

[7] Department of Electrical and Computer Engineering, National University of Singapore, 117583, Singapore.

[*] Corresponding Author: Zhiwei Sun. Email: smeker@szpt.edu.cn.

Received: 21 January 2020; Accepted: 23 April 2020.

1 Introduction

As one of the fastest growing field of modern science, cryptography is the basic theory to ensure the security of our private information. However, with the development of quantum computation, some cryptography protocols based on difficult math problems (such as large integer decomposition) may be no longer safe. In order to solve these potential loopholes, one of the attempts is directly applying quantum mechanical properties to design cryptography protocols. The first quantum cryptography protocol was proposed by Bennett et al. [Bennett and Brassard (1984)]. Since then, many branches have been generated during past 30 years, such as quantum secret sharing (QSS) [Hillery, Buzek and Berthiaume (1999); Cleve, Gottesman and Lo (1999); Xiao, Long, Deng et al. (2004); Hsieh, Tasi and Hwang (2010)], quantum secure direct communication (QSDC) [Wang, Deng, Li et al. (2005); Lin, Wen, Gao et al. (2008)], quantum private comparison [Yang and Wen (2009); Liu, Xu, Yang et al.(2019)], quantum identity authentication (QIA) [Zhang, Zeng, Zhou et al. (2006); Yang, Wen and Zhang (2008); Zhang (2009)], quantum signature (QS) [Chuang and Gottesman (2001); Zeng and Keitel (2002); Clarke, Collins, Dunjko et al. (2012); Dunjko, Wallden and Andersson (2014);Wallden, Dunjko, Kent et al. (2015); Shang, Pei, Chen et al. (2019)] and other new applications [Qu, Cheng, Wang et al. (2019); Qu, Li, Xu et al. (2019); Liu, Gao, Liu et al. (2019)].

In the course of quantum cryptography, people would like to give some novel methods to solve special problems in the extended scenarios of secure multi-party computation (SMPC). The following private query requirement is important in many scenarios: for a database provider and a user, how to make the provider answer the user's query without leaking any additional messages, where the user's query content should not be recognized by the database provider neither? In classical cryptography, the proposed task can be solved by oblivious transfer (OT) [Kolesnikov and Kumaresan (2013)] or symmetrically private information retrieval (SPIR) [Gertner, Ishai, Kushilevitz et al. (2000)]. In quantum world, Kerenidis et al. [Kerenidis and Wolf (2004)] constructed the corresponding quantum symmetrically private information retrieval (QSPIR) systems. Later Giovannetti et al. [Giovannetti, Lloyd and Maccone (2008); Giovannetti, Lloyd and Maccone (2010)] proposed a simplified solution to the problem above with cheat sensitive quantum private query (QPQ) protocols. Derived from Lo 's results [Lo (1998)], Jakobi et al. [Jakobi, Simon, Gisin et al. (2011)] gave a more practical and secure method to design QPQ protocols with a novel technique named quantum oblivious key distribution (QOKD). Here, it should be pointed out that the interesting definition of QOKD is combing the expressions of oblivious key transfer (OKT) and quantum key distribution (QKD). In 2012, Gao et al. [Gao, Liu, Wen et al. (2012)] improved Jakobi et al.'s results [Jakobi, Simon, Gisin et al. (2011)] with better privacy for both the user and provider in the view of QOKD. Since then, QOKD is considered as a fundamental technique which is widely applied in further research of QPQ. In 2013, Panduranga et al. [Panduranga and Jakobi (2013)] began to focus on the compressing of the shared raw keys in QOKD to protect the privacy of QPQ. Until 2015, Gao et al. [Gao, Liu, Huang et al. (2015)] analyzed the unavailability of the existing postprocessing methods of QOKD and provided a series of necessary improvements. Their works make great contributions to the development of QOKD and QPQ. Based on Gao et al.'s results, Liu et al. [Liu, Gao, Huang et al. (2015)] proposed a novel QPQ protocol based on QOKD without a

failure probability in 2015. Wei et al. [Wei, Gao, Wen et al. (2014); Wei, Wang and Gao (2016); Wei, Cai, Liu et al. (2018)] provided some practical QPQ protocols by improving the performance of QOKD. The detailed analysis of QOKD applied in QPQ can be seen in Gao et al. [Gao, Qin, Huang et al. (2019)].

With our analysis, the reason why QOKD can be widely applied in QPQ is that it provides a solution to reduce the communication and computational complexity in practical sense. That is to say, even if large database is concerned, the dimension of oracle operations will be not increased. Moreover, the participants' privacy can be naturally preserved without so much complex analysis. With its better performance, a question is directly arising that "Shall we solve some SMPC problems in practice with QOKD except for QPQ ones?" In order to answer this question, we focus on the solution of privacy-preserving decision (PPD) problems [Gu, Yang and Yin (2018); Yin, Ju, Yin et al. (2019)] in SMPC by applying the technique of QOKD. Specifically, the proposed PPD requires a user (Alice) to decide whether her private secret is an element of a server's (Bob) private set, while Alice and Bob should not reveal their secrets to each other. Recently, Shi et al. creatively gave the corresponding quantum PPD versions by expressing quantum oblivious set-member decision (QOSMD) [Shi, Mu, Zhong et al. (2015)] and quantum point inclusion decision (QPID) [Shi, Mu, Zhong et al. (2017)]. For QOSMD, Alice's private secret is her identity and Bob's private set involves a list of members in his group. For QPID, Alice has a private point and Bob has a private area. They would determine whether the point is inside the area secretly. Both of them can be seen as special types of PPD in quantum area.

In this paper, the solutions to privacy-preserving decision (PPD) problems will be presented with the technique of QOKD. Specifically, a new method to design QOKD protocol is proposed in Section 2, where the provider and user just have limited quantum capabilities by performing computational basis measurement for single photons. And its security analysis is also provided in this section. Then, we present a universal model to solve some PPD problems (OSMD and PID) based on QOKD with different encoding and shifting strategies in Section 3. Furthermore, the necessary comparisons and further discussions are given in Section 4. Finally, we summarize a conclusion in Section 5.

2 The QOKD protocol for the participants with limited quantum capabilities

Compared with QKD, the task of QOKD is to share asymmetric keys between the provider and user in an oblivious manner, where the provider gets the whole key sequence and the user has to recognize only one key bit which is unknown to the provider. In this section, a more practical QOKD model is proposed in terms of following scenario: The users Alice and Bob have limited quantum capabilities, i.e., both of them can only receive quantum signals and perform computational basis measurement for single photons. In order to simplify our description, a trusted center Charlie is involved to prepare and distribute the necessary entangled particles for Alice and Bob. Without loss of generality, the following four-party entangled state [Pivoluska, Huber and Malik (2018)] is previously introduced to the presented QOKD protocol

$$|\Psi\rangle = \frac{1}{2}\left(|000\rangle + |111\rangle + |220\rangle + |331\rangle\right). \tag{1}$$

2.1 The proposed QOKD protocol

Here the summarized process of our QOKD protocol can be seen in Fig. 1 and the detailed steps are shown as follows:

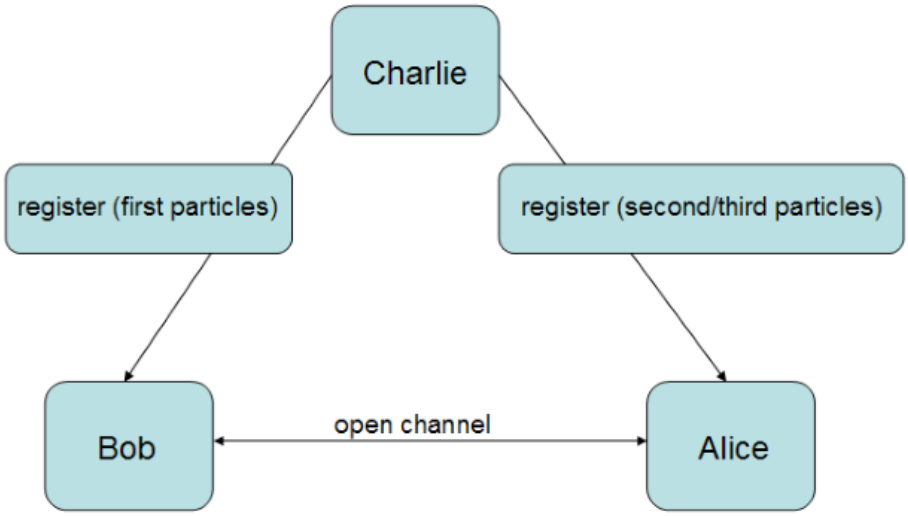

Figure 1: The summarized process of QOKD protocol

[Step 1] The trusted center Charlie firstly prepares n $|\Psi\rangle$ with three registers t_1, t_2, t_3 to store the qudits, where the first qudit sequence is stored in t_1, and the second and third qudit sequences are randomly stored in t_2 or t_3. Then he randomly inserts some decoy states into the transferred qudit sequence and sends the new register t_1' to the provider Bob, register t_2' to the user Alice and keeps t_3 himself, here the decoy states are chosen from the four-dimensional computational basis and Fourier basis.

[Step 2] After confirming the received registers, Charlie announces the positions of decoy states to detect eavesdropping. For each of the announced positions, Alice and Bob randomly choose computational basis or Fourier basis to measure the announced states and publish their measurement results. If the error rate is larger than threshold value, the protocol will be aborted and restarted by Charlie.

[Step 3] For the left qudits, Alice and Bob measure them in the computational basis and generate the raw key sequence K_A and K_B respectively with the following encoding rule:

$$\left(|0\rangle,|3\rangle\right)\rightarrow 0,\left(|1\rangle,|2\rangle\right)\rightarrow 1. \tag{2}$$

In this sense, Alice can only recognize some bits of K_B according to the structure of $|\Psi\rangle$ with the following reasons:

(1) When Alice gets the measurement result $|0\rangle$ $\left(|1\rangle\right)$, the state $|\Psi\rangle$ will collapse into $|000\rangle$ or $|220\rangle$ ($|111\rangle$ or $|331\rangle$). That is to say she only recognizes the results of Bob's

site with the probability of $3/16$, because she cannot determine whether her kept qudit is from t_2 or t_3.

(2) When Alice gets $|2\rangle$ ($|3\rangle$), $|\Psi\rangle$ will collapse into $|220\rangle$ ($|331\rangle$). Here she can directly recognize Bob's corresponding raw key bits.

From the analysis above, Alice will only keep the measurement results $|2\rangle$, $|3\rangle$ and discard the other results. Hence the expression of the shared K_A and K_B may be seen as

$$K_A = \{-,-,\cdots,k_i,-,\cdots,k_j,-,\cdots\} \tag{3}$$

$$K_B = \{k_1,k_2,\cdots,k_i,k_{i+1},\cdots,k_j,k_{j+1},\cdots\}. \tag{4}$$

[Step 4] Once the raw key-bit sequences are established without dispute, Charlie will discard his kept particles t_3.

[Step 5] Finally, the subsequent postprocess of K_A and K_B should be introduced in the following two phases.

[Compression Phase] In this phase, Zhao et al.'s method [Zhao, Yin, Chen et al. (2017)] can be used to compress the raw keys, and ensure Alice only get one bits of the final sequence. If Alice finds she has no final key bit left, then the protocol will be restarted.

[Error Correction Phase] Similarly, the necessary error correction is implied in our protocol using the method proposed by Gao et al. [Gao, Liu, Huang et al. (2015)]. If the error rate is less than some threshold value, Alice and Bob will accept the protocol. Otherwise, the protocol should be aborted.

Finally, the optimal case for shared oblivious key sequence is Alice can recognize only one bit of K_B.

2.2 The secure analysis of the proposed QOKD protocol

For a secure QOKD protocol, Alice's and Bob's privacy should be protected. In the view of this, the security analysis of our protocol is shown with the following two aspects:

Bob's privacy If Alice is dishonest, she will do her best to obtain more key bits beyond her legally authority. However, in the presented QOKD protocol above, it is not difficult to see that Alice cannot get additional information of K_B from her local measurement with the following two situations:

(1) If Alice gets $|0\rangle$ ($|1\rangle$) in Step 3, she will recognize Bob's key bit 0 or 1 with the probability of $3/16$. In order to show that, it should be firstly pointed out that Alice gets $|0\rangle$ ($|1\rangle$) with the probability of $p_0(p_1) = 1/2 \cdot 1/4 + 1/2 \cdot 1/2 = 3/8$. When Alice gets the measurement result $|0\rangle$ ($|1\rangle$), she cannot make sure whether the state collapses into $|000\rangle$ or $|220\rangle$ ($|111\rangle$ or $|331\rangle$). Hence the corresponding result in Bob's site may be $|0\rangle$ or $|2\rangle$. According to the encoding rule in Eq. (2), she infers Bob's key bit is 0 or 1 with the

probability of $1/2$. Above all, she infers Bob's one key bit with the probability of $3/16$.

(2) If Alice gets $|2\rangle$ ($|3\rangle$) in Step 3, Bob's measurement results must be $|2\rangle$ ($|3\rangle$). Since Alice gets $|2\rangle$ ($|3\rangle$) with the probability of $p_2(p_3)=1/4\cdot 1/2=1/8$, she can recognize Bob's one key bit with the probability of $1/8$.

From the analysis above, it can be seen that Alice can infer Bob's one key bit in specify position with the average successful probability $p_a^s=3/16\cdot 2+1/8\cdot 2=5/8$. Intuitively, if Alice would like to get m bits, the successful probability will be

$$p_a^m=C_n^m\left(5/8\right)^m\left(3/8\right)^{n-m}, \tag{5}$$

here n represents the number of shared key bits. While another idea may be arising that "Is Alice able to perform other attack strategies?" Since the exchange of classical messages is assumed secure, the dishonest Alice has to perform intercept-resend attack to the qudits transferred from Charlie to Bob and try to get additional key bits of K_B beyond her authority. In order to show the availability of the intercept-resend attack, Alice is assumed to intercept x particles of the transferred $n+d$ qudits and measure them with local computational basis measurement without loss of generality, here d is the number of inserted decoy states. Obviously, there is only one case for all x particles to escape the detection and get Bob's keys, that is all of them are not decoy states. Actually, Alice's attack will not be detected with the probability of

$$\begin{aligned} P_e &= \frac{C_n^x}{C_{n+d}^x} \\ &= \frac{n!}{(n-x)!}\frac{(n+d-x)!}{(n+d)!} \\ &= \prod_{k=n}^{n-x+1}\frac{k}{k+d} \\ &\sim \mathrm{O}\left(\left(\frac{1}{d}\right)^x\right) \end{aligned} \tag{6}$$

So, if the number of the decoy states d is large enough, P_e will approach to zero. That is to say, this attack cannot pass the eavesdropping detection step.

Alice's privacy Fortunately, Alice's privacy can be also protected in the presented protocol, as Bob cannot determine which positions of the raw key-bit sequence are known to Alice with the special structure of the applied entangled states. In order to simplify our description, the analysis is also focused on one bit with Bob's local computational basis measurement as follows:

(1) If Bob gets $|0\rangle$ ($|1\rangle$) in Step 3, the entangled state will collapse into $|000\rangle$ ($|111\rangle$). In

this sense, he cannot ensure whether the received register is t_2 or t_3 For Alice, as the corresponding measurement results $|0\rangle$ and $|1\rangle$ have been discarded, it is not helpful for Bob to recognize Alice's private key bits. Therefore, Bob's failure probability is $1/2$ which corresponds the cases to get $|0\rangle$ or $|1\rangle$.

(2) If Bob gets $|2\rangle$ ($|3\rangle$) in Step 3, he will recognize Alice's private key 0 or 1 with the probability of $1/8$, as the entangled state collapses into $|220\rangle$ or $|331\rangle$. Since Bob gets $|2\rangle$ ($|3\rangle$) with the probability of $p_2'(p_3') = 1/4$ and Alice receives the register t_2, t_3 randomly, Bob will infer Alice's key bit is 0 or 1 with the probability of $1/8$.

Similarly, Bob can infer Alice's one key bit in specify position with the average successful probability $p_b^s = 1/8 \cdot 2 = 1/4$. Intuitively, with m bits Bob would like to get, the successful probability will be

$$p_b^m = C_n^m \left(1/4\right)^m \left(3/4\right)^{n-m}, \tag{7}$$

here n represents the number of shared key bits. The performed intercept-resend attack can be also unavailable with similar analysis according to Eq. (6).

In addition, it should be pointed out that the postprocessing of the shared keys are performed locally by the users. Hence there exist no chance for anyone else to get the valid information of each private keys. That is why we just discuss the intercept-resend attack in this paper. From the analysis above, both the participants' privacy can be protected in the presented QOKD protocol.

3 Solutions to privacy-preserving decision (PPD) problems based on QOKD

As we know, privacy-preserving decision (PPD) problems have many special and significant applications in economic activities. In this section, we will solve some PPD problems such as set-member decision (SMD) and point-inclusion decision (PID) with the technique of QOKD.

3.1 Set-member decision protocol with QOKD

Without loss of generality, two participants Alice and Bob are involved in the SMD protocol. Here Alice is assumed to have a private secret m_A and Bob holds a private set $M = \{m_1, m_2, \cdots, m_i \cdots, m_t\} (t \le n-1)$. Alice wants to know whether her secret m_A is a member of Bob's secret set, while Alice and Bob should not reveal their secrets. In order to simplify the protocol, m_A and m_i are chosen from $Z_n^* = \{1,2\cdots, n-1\}$. The process can be seen as follows:

[Step 1] With the presented QOKD protocol in Section 2 (other secure QOKD protocols are also available), Alice and Bob share an n length oblivious key string $K = k_1 k_2 \cdots k_n (n \ge t)$, where Bob holds the whole sequence and Alice gets only one bit k_i.

[Step 2] Alice firstly announces to Bob a shift value S according to her private secret m_A and key k_i, i.e., $S=(m_A-i)\bmod n$. Then Bob shifts his key string cyclically by S bits and generates a shifted key sequence $K_B^{'}=k_1^{'}k_2^{'}\cdots k_n^{'}$. Furthermore, he encrypts $K_B^{'}$ into $K_B^{''}=k_1^{''}k_2^{''}\cdots k_n^{''}$ according to M as follows and sends the sequence $K_B^{''}$ to Alice.

Encrypting rule: For the subscript j of $K_B^{'}$, if $j\in M$, the corresponding key bit will become $k_j^{''}=k_j^{'}\oplus 1$, otherwise $k_j^{''}=k_j^{'}$, here $\oplus$ represents the XOR operation.

[Step 3] After receiving $K_B^{''}$ from Bob, Alice computes the corresponding $t=k_{m_A}^{''}\oplus k_i$. If $t=1$, Alice's secret m_A will belong to Bob's private set M; otherwise, $m_A\notin M$.

Example 1. Here we set a following example to describe our protocol. We suppose Alice has a private number $m_A=5$, Bob has a secret set $M=\{1,2,4,5,7,9\}$. The oblivious key sequence is established by $K=k_1k_2\cdots k_{10}$, where Bob holds the whole key sequence and Alice only knows k_3.

In Step 2, Alice firstly announces a shift value $S=5-3=2$ to Bob. Then Bob shifts his key string cyclically with 2 bits and generates a shifted key sequence $K_B^{'}=k_1^{'}k_2^{'}\cdots k_i^{'}\cdots k_{10}^{'}\left(k_{i+2\bmod 10}^{'}=k_i\right)$, here $k_5^{'}=k_3$. Furthermore, $K_B^{'}$ is encrypted into $K_B^{''}=k_1^{''}k_2^{''}\cdots k_i^{''}\cdots k_{10}^{''}$ with the presented rules above, where

$$k_1^{''}=k_1^{'}\oplus 1,k_2^{''}=k_2^{'}\oplus 1,k_4^{''}=k_4^{'}\oplus 1, \tag{8}$$

$$k_5^{''}=k_5^{'}\oplus 1,k_7^{''}=k_7^{'}\oplus 1,k_9^{''}=k_9^{'}\oplus 1, \tag{9}$$

$$k_3^{''}=k_3^{'},k_6^{''}=k_6^{'},k_8^{''}=k_8^{'}. \tag{10}$$

In Step 3, Alice computes

$$k_3+k_5^{''}=k_3+k_5^{'}+1=k_3+k_3+1=1 \tag{11}$$

and recognizes her private secret 5 is a member of Bob's secret set.

3.2 Point-inclusion decision protocol with QOKD

Here we discuss a similar solution with QOKD to the extended PPD problem in space case---point-inclusion decision (PID). In the presented protocol, Alice is assumed to have a private point Q and Bob holds a private area A. In PID, Alice wants to decide whether Q is inside A without disclosing their respective private information. The detailed process is described as follows:

[Step 1] Generally there exists a large plane area including Alice's point Q and Bob's area B. This area is uniformly partitioned into $r\times r$ grids, where r is a large enough integer, and its size can be determined by their accuracy requirements. These grids are labeled by Alice and Bob with a unique serial number in $[1,r^2]$ for both of them.

Without loss of generality, Alice's private point Q is labeled as $l_Q\left(Q\le r^2\right)$, Bob's private area B is labeled as $l_B=\{l_{B1},l_{B2},\cdots,l_{Bt}\}\left(t\le n,At\le r^2\right)$.

[Step 2] Previously, Alice and Bob share an n length oblivious key string $K = k_1 k_2 \cdots k_n \left(n \geq r^2\right)$ with the technique of QOKD, where Bob knows the whole key sequence and Alice knows only one bit k_i.

[Step 3] Alice firstly announces to Bob a shift value $l = \left(l_Q - i\right) \bmod n$. Then Bob generates a new key sequence $K_b^{'} = k_1^{'} k_2^{'} \cdots k_n^{'}$ by shifting K with l bits. Moreover, he encrypts $K_b^{'}$ with l_B and gets $K_b^{''}$ with the similar rules above:

Encoding rule: For the subscript j of $K_b^{'}$, if $j \in l_B$, the corresponding key bit will become $k_j^{''} = k_j^{'} \oplus 1$, otherwise $k_j^{''} = k_j^{'}$, here $\oplus$ represents the XOR operation.

[Step 4] Bob sends $K_b^{''}$ to Alice. Alice computes the corresponding $l = k_{l_Q}^{''} \oplus k_i$. If $l = 1$, Alice's private point Q will be inside of Bob's private area B; otherwise, Q will be out of B.

Example 2. Here a following example is set to explain the presented protocol. Previously, both of Alice's private point Q and Bob's private area B are assumed in the 10×10 plane area whose grids are labeled with $\{1,2,3,\cdots,100\}$. Alice's private point Q is labeled as $l_Q = 20$ and Bob's private area B is $l_B = \{15,16,\cdots,30\}$.

Then the shared oblivious key sequence in Step 2 is $K = k_1 k_2 \cdots k_{100}$, where Bob holds the whole sequence and Alice only knows k_{10}.

In Step 3, Alice firstly announces a shift value $S = 20 - 10 = 10$ to Bob. Then the key sequence $K_b^{'} = k_1^{'} k_2^{'} \cdots k_i^{'} \cdots k_{100}^{'} \left(k_{i+10 \bmod 100}^{'} = k_i\right)$ is shifted with 10 bits of K by Bob, here $k_{20}^{'} = k_{10}$. Furthermore, $K_b^{''} = k_1^{''} k_2^{''} \cdots k_i^{''} \cdots k_{100}^{''}$ is generated with l_B, where

$$k_{15}^{''} = k_{15}^{'} \oplus 1, k_{16}^{''} = k_{16}^{'} \oplus 1, \cdots, k_{30}^{''} = k_{30}^{'} \oplus 1 \tag{12}$$

and the other key bits $k_i^{''} = k_i^{'}$.

In Step 4, Alice computes

$$k_{10} + k_{20}^{''} = k_{10} + k_{20}^{'} + 1 = k_{10} + k_{10} + 1 = 1 \tag{13}$$

and recognizes her private point 20 is inside of B.

4 Further discussion

In this section, the availability and efficiency of the presented solutions of PPD problems will be discussed.

4.1 The availability of presented solutions

From the description above, three key factors make the solutions of PPD problems available---oblivious key sequence, accurate shifting value and encoding rule.

For SMD and PID, it can be seen that the accurate shifting values

$$S = \left(m_A - i\right) \bmod n, l = \left(l_Q - i\right) \bmod n \tag{14}$$

are determined by the subscript of Alice's private key bit k_i in the oblivious shared key

sequence K. With the shifted key sequence $K_B^{'}$ and $K_b^{'}$, Bob can hide his set M or area B with the encoding rule above. In the view of this, the most important step of our solutions is to design a secure and efficient method to distribute oblivious keys. Fortunately, we give one model to design QOKD protocols in Section 2, and prove it is immune to leak both the participants' privacy. Hence that is the reason why we do not provide additional security analysis of our solutions in Section 3.

Moreover, the presented QOKD protocol does not only improve its availability for the providers and users with limited quantum abilities, but also give a dispute resolution for the center. For example, Alice or Bob may want to verify whether both of them have performed the required local measurement or the shared entangled state is in the accurate form of Eq. (1). In this sense, Charlie just directly announces his own measurement results in the computational basis for single photons. If all the measurement results do not satisfy the certain property of Eq. (1), the protocol will be invalid. Hence this irrational denial of service is not helpful for each participant to get more information beyond his (her) authority in practice.

4.2 The efficiency of presented solutions

For a quantum cryptography protocol, improving its efficiency is as important as ensuring the security. From Tab. 1, the communication cost of our solutions is expressed. Combing with the QOKD protocol in Section 2, $2n$ qudits are transferred to the two users in order to distribute oblivious keys. It should be pointed out that the number of decoy states is determined by the security threshold required in practical quantum secure communication. Hence the cost of decoy states is not discussed here.

From the measurement resource cost, only single qudit measurement in the computational basis is performed by the users in our QOKD protocol. Hence the presented solutions of PPD problems can be realized by the current optical devices. For the classical communication complexity, only $n+s$ classical bits are transferred in the SMD and PID protocols, here s represents the shifted values announced by Alice, and n means the length of final encrypted key sequence. However, in Shi et al. [Shi, Mu, Zhong et al. (2017)], the $4n$ qubits and $2n$ classical bits should be transferred.

While it should be pointed out that the requirement to distribute entangled particles indeed affects the efficiency of our method to some extent. For the quantum cryptography protocols based on multiparty entangled states, the third party is necessary introduced to distribute entangled particles. If we assume one user to prepare and distribute entangled states in a two-party protocol, he (she) will be able to measure or entangle auxiliary particles to eavesdrop the other's privacy. However how to distribute entangled particles in an insecure environment to the rational users (they may perform some attacks to get their own profits later) is still an open problem for the further research.

Table 1: The cost of QOKD-based OSMD and QOKD-based PID protocols (*C*-basis means the computational basis)

Quantum Operations	**Null**
Quantum Measurements	$2n$ single measurement with *C*-basis
The Transferred Quantum Messages	$2n$ qudits
The Transferred Classical Messages	$n+s$ bits

5 Conclusion

In conclusion, a new QOKD protocol based on four-dimension entangled state is proposed. Here the provider and user just need to have limited quantum capabilities by performing computational basis measurement for single photons. Then it is proved to be secure without leaking the privacy of the participants. Based on the technique of QOKD, some direct solutions have been presented to the extended PPD problems---SMD and PID. Moreover, some further discussions of the solutions are provided in the view of availability and efficiency.

Finally, it should be pointed out that QOKD is a significant technique to design QSMC protocols. From the early attempts of QPQ to the presented SMD and PID, sharing oblivious keys between the users plays a fundamental role. It is hoped that our results would be helpful to the further study of quantum cryptography based on QOKD.

Funding Statement: This work is supported by National Natural Science Foundation of China under Grant Nos. 61802118, 61602316, 61932005, Open Foundation of State key Laboratory of Networking and Switching Technology (BUPT) under Grant No. SKLNST-2018-1-07, University Nursing Program for Young Scholars with Creative Talents in Heilongjiang Province under Grant No. UNPYSCT-2018015, Science and Technology Innovation Projects of Shenzhen under Grant Nos. JCYJ20190809152003992, JCYJ20170818140234295, JCYJ20170818144026871, JCYJ2017081802237376, Guangdong Natural Science Foundation under Grant No. 2017A030310134, 2018A030313957, Shenzhen Polytechnic Youth Innovation Project under Grant 6019310010K0, Natural Science Foundation of Heilongjiang Province under Grant No. LH2019F031 and Hei Long Jiang Postdoctoral Foundation under Grant No. LBH-Z17048. Professor Shenggen Zheng and Xiangfu Zou also give us some helpful comments. We are grateful for their constructive opinions.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

Bennett, C. H.; Brassard, G. (1984): Quantum cryptography: public key distribution and coin tossing. *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pp. 175-179.

Chuang, I.; Gottesman, D. (2001): Quantum digital signatures. *arXiv preprint quant-ph*. 0105032.

Clarke, P. J.; Collins, R. J.; Dunjko, V.; Andersson, E.; Buller, G. S. (2012): Experimental demonstration of quantum digital signatures using phase-encoded coherent states of light. *Nature Communications*, vol. 3, no. 6, pp. 1174.

Cleve, R.; Gottesman, D.; Lo, H. K. (1999): How to share a quantum secret. *Physical Review Letters*, vol. 83, no. 3, pp. 648-651.

Dunjko, V.; Wallden, P.; Andersson, E. (2014): Quantum digital signatures without quantum memory. *Physical Review Letters*, vol. 112, no. 4, pp. 040502.

Gao, F.; Liu, B.; Huang, W.; Wen, Q. Y. (2015): Postprocessing of the oblivious key in quantum private query. *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 21, no. 3, pp. 98-108.

Gao, F.; Liu, B.; Wen, Q. Y.; Chen, H. (2012): Flexible quantum private queries based on quantum key distribution. *Optics Express*, vol. 20, no. 16, pp. 17411-17420.

Gao, F.; Qin, S. J.; Huang, W.; Wen, Q. Y. (2019): Quantum private query: a new kind of practical quantum cryptographic protocols. *Science, China, Physics, Mechanics Astronomy*, vol. 62, no. 7, pp. 10-21.

Gertner, Y.; Ishai, Y.; Kushilevitz, E.; Malkin, T. (2000): Protecting data privacy in private information retrieval schemes. *Journal of Computer and System Sciences*, vol. 60, no. 3, pp. 592-629.

Giovannetti, V.; Lloyd, S.; Maccone, L. (2008): Quantum private query. *Physical Review Letters*, vol. 100, no. 23, pp. 230502.

Giovannetti, V.; Lloyd, S.; Maccone, L. (2010): Quantum private queries. *IEEE Transactions on Information Theory*, vol. 56, no. 7, pp. 3465-3477.

Gu, K.; Yang, L. H.; Yin, B. (2018): Location data record privacy protection based on differential privacy mechanism. *Information Technology and Control*, vol. 47, no. 4, pp. 639-654.

Hillery, M.; Buzek, V.; Berthiaume, A. (1999): Quantum secret sharing. *Physical Review A*, vol. 59, no. 3, pp. 1829.

Hsieh, C. R.; Tasi, C. W.; Hwang, Z. L. (2010): Quantum secret sharing using GHZ-like state. *Communications in Theoretical Physics*, vol. 54, pp. 1019-1022.

Jakobi, M.; Simon, C.; Gisin, N.; Bancal, J. D.; Branciard, C. (2011): Practical private database queries based on a quantum-key-distribution protocol. *Physical Review A*, vol. 83, no. 2, pp. 022301.

Kerenidis, I.; Wolf, R. D. (2004): Quantum symmetrically-private information retrieval. *Information Processing Letters*, vol. 90, no. 3, pp. 109-114.

Kolesnikov, V.; Kumaresan, R. (2013): Improved OT extension for transferring short secrets. *Advances in Cryptology-CRYPTO*, pp. 54-70.

Lin, S.; Wen, Q. Y.; Gao, F.; Zhu, F. C. (2008): Quantum secure direct communication with x-type entangled states. *Physical Review A*, vol. 78, pp. 5175-5179.

Liu, B.; Gao, F.; Huang, W.; Wen, Q. Y. (2015): QKD-based quantum private query without a failure probability. *Science, China, Physics, Mechanics, Astronomy*, vol. 58, no. 10, pp. 18-23.

Liu, W. J.; Gao, P.; Liu, Z.; Chen, H.; Zhang, M. (2019): A quantum-based database query scheme for privacy preservation in cloud environment. *Security and Communication Networks*, vol. 2019, pp. 1-14.

Liu, W. J.; Xu, Y.; Yang, C. N.; Yu. W. B.; Chi, L. H. (2019): Privacy-preserving quantum two-party geometric intersection. *Computers, Materials & Continua*, vol. 60, no. 3, pp. 1237-1250.

Lo, H. K. (1998): Insecurity of quantum secure computations. *Physical Review A*, vol. 56, no. 2, pp. 1154-1162.

Panduranga, R. M. V.; Jakobi, M. (2013): Towards communication-efficient quantum oblivious key distribution. *Physical Review A*, vol. 87, no. 1, pp. 012331.

Pivoluska, M.; Huber, M.; Malik, M. (2018): Layered quantum key distribution. *Physical Review A*, vol. 97, no. 3, pp. 032312.

Qu, Z. G.; Cheng, Z. W.; Wang, X. J. (2019): Matrix coding-based quantum image steganography algorithm. *IEEE Access*, vol. 7, pp. 35684-35698.

Qu, Z. G.; Li, Z. Y.; Xu, G.; Wu, S. Y.; Wang, X. J. (2019): Quantum image steganography protocol based on quantum image expansion and Grover search algorithm. *IEEE Access*, vol. 7, pp. 20849-50857.

Shang, P.; Pei, Z.; Chen, R.; Liu, J. W. (2019): Quantum homomorphic signature with repeatable verification, *Computers, Materials & Continua*, vol. 59, no. 1, pp. 149-165.

Shi, R. H.; Mu, Y.; Zhong, H.; Cui, J.; Zhang, S. (2017): Privacy-preserving point-inclusion protocol for an arbitrary area based on phase-encoded quantum private query. *Quantum Information Processing*, vol. 16, no. 1, pp. 8.

Shi, R. H.; Mu, Y.; Zhong, H.; Zhang, S. (2015): Quantum oblivious set-member decision protocol. *Physical Review A*, vol. 92, no. 2, pp. 022309.

Wallden, P.; Dunjko, V.; Kent, A.; Andersson, E. (2015): Quantum digital signatures with quantum-key-distribution components. *Physical Review A*, vol. 91, no. 4, pp. 042304.

Wang, C.; Deng, F. G.; Li, Y. S.; Liu, X. S.; Long, G. L. (2005): Quantum secure direct communication with high-dimension quantum superdense coding. *Physical Review A*, vol. 71, no. 4, pp. 044305.

Wei, C. Y.; Cai, X. Q.; Liu, B.; Wang, T. Y.; Gao, F. (2018): A generic construction of quantum-oblivious-key-transfer-based private query with ideal database security and zero failure. *IEEE Transactions on Computers*, vol. 67, no. 1, pp. 2-8.

Wei, C. Y.; Gao, F.; Wen, Q. Y.; Wang, T. Y. (2014): Practical quantum private query of blocks based on unbalanced-state bennett-brassard-1984 quantum-key-distribution protocol. *Scientific Reports*, vol. 4, pp. 7537.

Wei, C. Y.; Wang, T. Y.; Gao, F. (2016): Practical quantum private query with better performance in resisting joint-measurement attack. *Physical Review A*, vol. 93, no. 4, pp. 042318.

Xiao, L.; Long, G. L.; Deng, F. G.; Pan, J. W. (2004): Efficient multi-party quantum secret sharing schemes. *Physical Review A*, vol. 69, no. 5, pp. 521-524.

Yang, Y. G.; Wen, Q. Y. (2009): An efficient two-party quantum private comparison protocol with decoy photons and two-photon entanglement. *Journal of Physics A Mathematical and Theoretical*, vol. 42, no. 5, pp. 30-30.

Yang, Y. G.; Wen, Q. Y.; Zhang, X. (2008): Multiparty simultaneous quantum identity authentication with secret sharing. *Science in China Series G: Physics, Mechanics and Astronomy*, vol. 51, no. 3, pp. 321-327.

Yin, C. Y.; Ju, X. K.; Yin, Z. C.; Wang, J. (2019): Location recommendation privacy protection method based on location sensitivity division. *Journal on Wireless Communications and Networking*, doi.org/10.1186/s13638-019-1606-y.

Zeng, G. H.; Keitel, C. H. (2002): Arbitrated quantum-signature scheme. *Physical Review A*, vol. 65, no. 4, pp. 042312.

Zhang, X. L. (2009): One-way quantum identity authentication based on public key. *Chinese Science Bulletin*, vol. 54, no. 12, pp. 2018-2021.

Zhang, Z. S.; Zeng, G. H.; Zhou, N. R.; Xiong, J. (2006): Quantum identity authentication based on ping-pong technique for photons. *Physics Letters A*, vol. 356, no. 3, pp. 199-205.

Zhao, L. Y.; Yin, Z. Q.; Chen, W.; Qian, Y. J.; Zhang, C. M. et al. (2017): Loss-tolerant measurement-device-independent quantum private queries. *Scientific Reports*, vol. 7, pp. 39733.