Physics Letters A 380 (2016) 4033–4038

Contents lists available at ScienceDirect

Physics Letters A

www.elsevier.com/locate/pla

Quantum private query with perfect user privacy against a joint-measurement attack

Yu-Guang Yang [a,b,*], Zhi-Chao Liu [a], Jian Li [c], Xiu-Bo Chen [d], Hui-Juan Zuo [e], Yi-Hua Zhou [a], Wei-Min Shi [a]

[a] *College of Computer Science and Technology, Beijing University of Technology, Beijing 100124, China*
[b] *State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China*
[c] *School of Computer, Beijing University of Posts and Telecommunications, Beijing 100876, China*
[d] *Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, 100876, China*
[e] *College of Mathematics and Information Science, Hebei Normal University, Shijiazhuang 050024, China*

ARTICLE INFO

Article history:
Received 1 July 2016
Received in revised form 8 October 2016
Accepted 12 October 2016
Available online 14 October 2016
Communicated by P.R. Holland

Keywords:
Quantum private query
Quantum key distribution
Communication complexity
Security

ABSTRACT

The joint-measurement (JM) attack is the most powerful threat to the database security for existing quantum-key-distribution (QKD)-based quantum private query (QPQ) protocols. Wei et al. (2016) [28] proposed a novel QPQ protocol against the JM attack. However, their protocol relies on two-way quantum communication thereby affecting its real implementation and communication efficiency. Moreover, it cannot ensure perfect user privacy. In this paper, we present a new one-way QPQ protocol in which the special way of classical post-processing of oblivious key ensures the security against the JM attack. Furthermore, it realizes perfect user privacy and lower complexity of communication.

1. Introduction

According to the credibility of participants, cryptographic protocols are mainly divided into two categories: cryptographic protocols with trusted parties and the ones with distrusted parties. For the former, participants are trusted and the threats are mainly from outside attackers. For example, the QKD is aimed to generate a shared secret key between Alice and Bob symmetrically without being eavesdropped by outside attackers. By contrast, for the latter, participants are untrusted and the threats are mainly from inside attackers. As an important application of the latter, symmetrically private information retrieval (SPIR) [1] has drawn lots of attention. The SPIR problem is defined as follows. In a private database query, the user Alice wants to gain an item x_i of a database $\mathbf{X} = x_1\ x_2\ \ldots\ x_N$ without leaking the query address i to the database holder Bob (user privacy), and Bob does not want Alice to obtain any other information about his database except x_i (database security).

Since Gertner et al. introduced the concept of SPIR [1], various SPIR schemes have been proposed in classical cryptographic scenarios. Unfortunately, the security of most classical cryptosystems is based on the unproven assumptions of mathematical difficulty and might be vulnerable to the powerful ability of quantum computation [2,3]. Fortunately, this difficulty can be overcome by quantum cryptography [4,5], where the security is guaranteed by physical principles.

As the quantum counterpart of the SPIR problem, quantum private queries (QPQs) [6–10] have also attracted a great deal of attention. Obviously, the task of QPQ is different from that of QKD. That is, the main task of QPQ is aimed to generate an asymmetric key between Alice and Bob where the key is known all to Bob while a little fraction to Alice. Giovannetti et al. presented the first QPQ protocol (GLM protocol) [7–9]. Subsequently, Olejnik presented an improved QPQ protocol of GLM protocol (O-protocol) [10]. In their protocols [7–10], the database is modeled by an oracle operation which limits their implementation for large database. To solve this problem, Jakobi et al. [11] suggested the first practical QPQ protocol (J-protocol) based on the Scarani–Acin–Ribordy–Gisin (SARG04) QKD protocol [12]. Since then, some attempts have been made at constructing QKD-based QPQ protocols theoretically and experimentally [13–31].

[*] Corresponding author at: College of Computer Science and Technology, Beijing University of Technology, Beijing 100124, China.
E-mail address: yangyang7357@bjut.edu.cn (Y.-G. Yang).

http://dx.doi.org/10.1016/j.physleta.2016.10.017
0375-9601/© 2016 Elsevier B.V. All rights reserved.

Security is an important target in QPQ protocols. For most of existing QKD-based QPQ protocols, the JM attack by the user is the most powerful threat to database security. For example, in J-protocol [11], the expected number of bits $\bar{n} = 2.44$ is achieved by Alice in the honest case given $N = 10^4$, $k = 6$. By contrast, by the JM attack, i.e., joint optimal unambiguous-state-discrimination (USD) attack [32,33], Alice can obtain each final key bit with probability 0.05 by jointly measuring the six qubits contributing to it (see Fig. 2 in Ref. [11]), thus obtaining up to 500 bits from the database. This JM attack will be more and more challenging with the development of quantum memories. To resist such JM attack, Wei et al. [28] proposed a QPQ protocol based on two-way QKD [34]. They pointed out that to conduct the JM attack, Alice must have two elements, i.e., the quantum carriers and the information about which carriers contribute to one final key bit simultaneously. So in their protocol, Alice is forbidden to have these two elements simultaneously in order to resist the JM attack. However, their protocol relies on two-way quantum communication [35–38], thereby affecting its real implementation and communication efficiency. Furthermore, perfect user privacy cannot be ensured. Bob can obtain more or less information about Alice's key.

In fact, communication efficiency should also be considered in the design of QPQ protocols. Some works on classical post-processing of oblivious key were presented [39–42]. For example, Jakobi et al. gave a $kN \to N$ method, that is, it transforms a raw key with length kN into an N-bit final key by cutting it into k substrings of length N and adding these strings bitwise (here N is the total number of items in the database) [11]. To reduce this communication complexity, Rao et al. [40] presented $N \to N$ and $rM \to N$ (with $rM \ll N$) ones, respectively. However, Gao et al. [41] pointed out that in Rao et al.'s first scheme the parity information about the final key bits can be elicited by Alice and Alice maybe obtains all the items via multiple queries while the $rM \to N$ method is not of information-theoretical security from the aspect of information theory in the second scheme [40]. Yang et al. [42] also presented an $N \to N$ classical post-processing method.

Obviously, quantum oblivious key distribution and classical post-processing of oblivious key are inseparable and equivalently important in the design of QPQ protocols. Wei et al. just tackled the security problem against the JM attack from the viewpoint of designing quantum oblivious key distribution at the cost of reducing the communication efficiency. In this paper, we provide another clue, i.e., construct a special way of classical post-processing of oblivious key to ensure the security against the JM attack. Further we propose a novel one-way-six-state-QKD-based QPQ protocol. Compared with previous QPQ protocols [11,13–31], especially Wei et al.'s protocol [28], it has the following advantages: (1) it ensures the security against the JM attack by means of the special way of classical post-processing of oblivious key which is different from the idea of resisting the JM attack by designing subtle quantum oblivious key distribution as proposed by Wei et al. [28]; (2) it ensures perfect user privacy where Alice prepares the quantum carriers thereby preventing Bob from trying to eavesdrop Alice's key by fake-state attack; (3) it also ensures lower complexity of communication. Alice's conclusive key rate is $p = 1/4$ in existing QPQ protocols while $p = 1/6$ in our proposed QPQ protocol. Moreover, our protocol also retains the good merits such as loss tolerance and robustness against quantum memory attack.

The remainder of this paper is organized as follows. First, we present our protocol in Section 2 and analyze its security in Section 3. Then in Section 4, we describe the features of our protocol. Finally, we draw a conclusion in Section 5.

2. Protocol

Different from previous QKD-based QPQ protocols, where the database holder Bob prepares the quantum carriers and sends them to Alice, in our protocol Alice takes charge of preparing the carriers and sending them to Bob.

First, let's introduce the six quantum states used in our protocol, $|H\rangle$, $|V\rangle$, $|\pm\rangle = (|H\rangle \pm |V\rangle)/\sqrt{2}$, $|R\rangle = (|H\rangle + i|V\rangle)/\sqrt{2}$ and $|L\rangle = (|H\rangle - i|V\rangle)/\sqrt{2}$. The six states can be grouped into twelve non-orthogonal sets $\{|H\rangle, |+\rangle\}$, $\{|+\rangle, |V\rangle\}$, $\{|V\rangle, |-\rangle\}$, $\{|-\rangle, |H\rangle\}$, $\{|H\rangle, |R\rangle\}$, $\{|R\rangle, |V\rangle\}$, $\{|V\rangle, |L\rangle\}$, $\{|L\rangle, |H\rangle\}$, $\{|+\rangle, |R\rangle\}$, $\{|R\rangle, |-\rangle\}$, $\{|-\rangle, |L\rangle\}$, $\{|L\rangle, |+\rangle\}$, where the first state of each set represents the logical bit 0 and the second logical bit 1. Our protocol includes three phases and is described as follows.

2.1. Quantum oblivious key distribution

(1) Alice sends Bob a sequence of quantum states. And each quantum state is randomly in one of the six states $\{|H\rangle, |V\rangle, |+\rangle, |-\rangle, |R\rangle, |L\rangle\}$.

(2) Bob randomly measures each received qubit with one of the three bases $\{\mathbf{Z}, \mathbf{X}, \mathbf{Y}\}$, wherein, the $\mathbf{Z}$ basis represents $\{|H\rangle, |V\rangle\}$, the $\mathbf{X}$ basis represents $\{|+\rangle, |-\rangle\}$, and the $\mathbf{Y}$ basis represents $\{|R\rangle, |L\rangle\}$. Then Bob announces which qubits he has successfully detected; lost or not detected qubits are discarded.

(3) Bob chooses some qubits randomly, and then asks Alice to announce their initial states. Bob compares his measurement outcomes with Alice's declaration. In the ideal case, Bob has a conclusive result for each checking qubit with a probability of $p_B^c = 1/3$. Bob compares his measurement outcomes and Alice's declaration. The inconclusive outcomes are considered to match Alice's declaration automatically. If there is no mismatch, Bob judges no attacker exists. Otherwise the protocol aborts.

(4) For each qubit that Bob has successfully measured, he announces which set his measurement result is in. For example, if his measurement result is $|H\rangle$, he can announce a set randomly chosen from the four sets $\{|H\rangle, |+\rangle\}$, $\{|-\rangle, |H\rangle\}$, $\{|H\rangle, |R\rangle\}$, or $\{|L\rangle, |H\rangle\}$.

(5) Alice interprets Bob's measurement results according to her initial states, and she can obtain Bob's measurement results with a certain probability. For example, if Bob's declaration is the set $\{|H\rangle, |+\rangle\}(\{|V\rangle, |-\rangle\})$ and her initial state is $|-\rangle(|H\rangle)$, Alice knows Bob's measurement result must be in the state $|H\rangle(|-\rangle)$ which corresponds to the raw key bit 0(1). Here, the raw key bit is a logical number corresponding to the location which Bob's measurement result is at. As a result, a raw key $\mathbf{R}$ is obtained by Alice and Bob, and known all to Bob and $p = 1/6$ to Alice.

(6) If no bit survives at Alice's end, repeat the above steps.

2.2. Classical post-processing of the resulting oblivious key

The generated kN-bit raw key $\mathbf{R}$ is denoted by $q_1, q_2, \cdots, q_{kN}$. Here, q_j is the jth bit of the raw key $\mathbf{R}$. k is a security parameter.

(7) Bob transforms the raw key string $\mathbf{R}$ into a matrix $\mathbf{S}$

$$\mathbf{S} = \begin{bmatrix} q_1 & q_2 & \cdots & q_N \\ q_{N+1} & q_{N+2} & \cdots & q_{2N} \\ \cdots & \cdots & \cdots & \cdots \\ q_{N(k-1)+1} & q_{N(k-1)+2} & \cdots & q_{kN} \end{bmatrix}_{k \times N} . \tag{1}$$

(8) Bob randomly selects a row vector $\mathbf{T}$

$$\mathbf{T} = \begin{bmatrix} t_1 & t_2 & \cdots & t_k \end{bmatrix}, \tag{2}$$

where t_j is a positive integer, $j = 1, 2, \ldots, k$.

(9) Bob and Alice make a matrix multiplication and obtain the matrix