Optik 126 (2015) 3206–3209

Contents lists available at ScienceDirect

Optik

journal homepage: www.elsevier.de/ijleo

Reductions between private information retrieval and oblivious transfer at the quantum level

Yu-Guang Yang[a,b,c,d,*], Si-Jia Sun[a], Qing-Xiang Pan[a], Peng Xu[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] *Beijing Key Laboratory of Trusted Computing, Beijing 100124, China*
[d] *National Engineering Laboratory for Critical Technologies of Information Security Classified Protection, Beijing 100124, China*

ARTICLE INFO

Article history:
Received 19 June 2014
Accepted 19 July 2015

Keywords:
Private information retrieval
Oblivious transfer
Reduction

ABSTRACT

Although private information retrieval and oblivious transfer are equivalent in classical cryptography, we show that the existence of secure quantum private information retrieval is necessary but not sufficient for secure quantum oblivious transfer, which provides a strong evidence of nonequivalence of two flavors of oblivious transfer at the quantum level.

1. Introduction

Private information retrieval (PIR) [1] deals with a situation in which there are a huge database and a user who wants to query, and the user wants to query the database while hiding the identity of the data-items she is after, not the existence of interaction with the user (user privacy). Its applications could include patent databases, stock quotes, media databases, etc.

Oblivious transfer (OT) is an important primitive extensively used in many cryptographic protocols. There are two major types of OTs. The original one [2] is referred to as all-or-nothing OT. Another type of OT is called one-out-of-two OT [3].

In classical cryptography, Crescenzo et al. concluded that single-database PIR implies OT [4]. They presented a reduction transforming any nontrivial single-database PIR into OT. In Ref. [5], it was shown that OT is complete, namely it can be used to construct any other protocol. That implies that there exists a reduction transforming OT into PIR. This classical reduction chain reveals the equivalence of the security of PIR and OT protocols at the classical level.

Given the Lo's no-go theorem [6], nonrelativistic quantum OT and PIR are impossible. But intriguingly, He and Wang proposed a nonrelativistic quantum all-or-nothing OT protocol [7] which does not rigorously satisfy the definition of ideal one-sided two-party quantum secure computation, on which the Lo's insecurity proof [6] was based. Thus it could remain unconditionally secure against the cheating strategy in the Lo's proof. This result seems to conflict with the Lo's conclusion (i.e., secure quantum one-out-of-two OT and quantum PIR would be possible) if the classical reductions held.

However, it has been realized that "the reductions and relations between classical cryptographic tasks need not necessarily apply to their quantum equivalents" [8,9]. In fact, in this paper we intend to build a PIR protocol on a secure quantum all-or-nothing OT protocol [7] and another PIR protocol on protocol P in Ref. [8] respectively. It will be shown that secure quantum OT implies secure quantum PIR. However if we build up a one-out-of-two OT protocol built upon the resultant secure quantum PIR protocol, it does not rigorously satisfy the definition of ideal one-sided two-party quantum secure computation, on which the Lo's insecurity proof [6] was based. In this sense, secure quantum PIR does not imply secure quantum OT, i.e., the above classical reduction chain is broken in the present quantum cryptography case. This result also provides a strong evidence of nonequivalence of two flavors of oblivious transfer at the quantum level.

The paper is organized as follows. In Section 2, two quantum PIR protocols are built upon secure quantum all-or-nothing OT [7] and protocol P in Ref. [8] respectively. The reduction transforming PIR into OT will be discussed in Section 3. A conclusion is summarized in Section 4.

[*] Corresponding author at: College of Computer Science and Technology, Beijing University of Technology, Beijing 100124, China. Tel.: +86 01067396818.
E-mail address: yangyang7357@bjut.edu.cn (Y.-G. Yang).

http://dx.doi.org/10.1016/j.ijleo.2015.07.149
0030-4026/© 2015 Elsevier GmbH. All rights reserved.

2. Reduction from OT to PIR

2.1. Quantum PIR protocol based on secure quantum all-or-nothing OT

Protocol P1:

(1) Bob chooses at random kN bits $r_1, r_2, \ldots, r_{kN}$;
(2) For each of these kN bits Bob uses the quantum all-or-nothing OT protocol to disclose the bit r_k to Alice;
(3) Alice and Bob execute postprocessing to the key $r_1, r_2, \ldots, r_{kN}$ to obtain the final N-bit key K so that Alice's known bits in the key are reduced to 1 bit or a little more by using the similar method in J-protocol (please see Fig. 1 in Ref. [10]). Bob encrypts his database with the final key K and Alice obtains the item she wanted with one of her known bits in K.

One can easily find that the secure quantum all-or-nothing OT protocol [7] can be used simply as a 'black box' primitive to build up a secure PIR protocol. This reason lies in that we need not deal with the details of the secure quantum all-or-nothing OT protocol [7] when it is used to build up a PIR protocol. Hence the proposed PIR protocol built upon the secure quantum all-or-nothing OT protocol [7] is also unconditionally secure against the cheating attack in the Lo's proof [6].

2.2. Quantum PIR protocol based on secure quantum one-out-of-two OT

Protocol P in Ref. [8] has been proved secure against the Lo's cheating [6] because it does not satisfy the rigorous definition of ideal one-out-of-two OT [6] but satisfy the definition of one-out-of-two OT [11]. We need not deal with the details of Protocol P in Ref. [8] so that we simply use it as a black box to build a quantum PIR protocol.

Protocol P2:

(1) Bob chooses at random $2K_s$ bits $r_1^1, r_2^1, r_1^2, r_2^2, \ldots, r_1^{K_s}, r_2^{K_s}$;
(2) For each r_1^j, r_2^j, $j = 1, 2, \ldots, K_s$, Bob uses Protocol P in Ref. [8] to disclose the secret bit r_k^j to Alice;
(3) Alice and Bob execute postprocessing to the key $r_1^1, r_2^1, r_1^2, r_2^2, \ldots, r_1^{K_s}, r_2^{K_s}$ to obtain the final N-bit key K so that Alice's known bits in the key are reduced to 1 bit or a little more. Bob encrypts his database with the final key K and Alice obtains the item she wanted with one of her known bits in K.

Protocol P in Ref. [8] can be used simply as a 'black box' primitive to build up a secure PIR protocol. This reason lies in that we need not deal with the details of Protocol P in Ref. [8] when it is used to build up a PIR protocol. Hence the proposed PIR protocol built upon Protocol P in Ref. [8] is also unconditionally secure against the cheating attack in the Lo's proof [6].

2.3. A concrete example: unconditionally secure quantum PIR protocol based on secure quantum all-or-nothing OT

Protocol Q

(1) *Preparation of the states*: Alice prepares n sets of four qubits in an entangled state $|\psi\rangle$ as described in Eq. (1). She keeps systems A_1 and A_2 of each $|\psi\rangle$ and sends systems B_1 and B_2 to Bob.

$$\begin{aligned}
|\psi\rangle &= |\psi_{B_1}\psi_{B_2}\psi_{A_1}\psi_{A_2}\rangle \\
&= (|0\rangle_{+}|0\rangle_{+}|0\rangle_{+}|0\rangle_{+} + |1\rangle_{+}|1\rangle_{+}|0\rangle_{+}|1\rangle_{+} \qquad (1)\\
&+|0\rangle_{\times}|0\rangle_{\times}|1\rangle_{+}|0\rangle_{+} + |1\rangle_{\times}|1\rangle_{\times}|1\rangle_{+}|1\rangle_{+})/2, ,
\end{aligned}$$

where $|0\rangle_{+}$ and $|1\rangle_{+}$ denote the two orthogonal states of a qubit. $|r\rangle_{\times} \equiv [|0\rangle_{+} + (-1)^r|1\rangle_{+}]/\sqrt{2}\,(r = 0,1)$, where $+(\times)$ stands for the rectilinear (diagonal) basis.

(2) Bob inputting c:

(2–1) For each $|\psi\rangle$, Bob views the state of systems B_1 and B_2 as $|r\rangle_q|r\rangle_q$, and he randomly picks $c \in \{0, 1\}$. If $c = 0$, he tries to decode q by projecting the two qubits into Φ^- and Ψ^+, and he sets $q = +$ $(q = \times)$ if the outcome is $\Phi^-(\Psi^+)$. Otherwise, if $c = 1$, Bob tries to decode r by projecting the two qubits into $|0\rangle_{\times}|0\rangle_{+}$ and $|1\rangle_{\times}|1\rangle_{+}$, and he sets $r = 0$ $(r = 1)$ if the outcome is $|0\rangle_{\times}|0\rangle_{+}$ $(|1\rangle_{\times}|1\rangle_{+})$. Here the Bell state $\Phi^{\pm} \equiv (|0\rangle_{+}|0\rangle_{+} \pm |1\rangle_{+}|1\rangle_{+})/\sqrt{2}$ and $\Psi^{\pm} \equiv (|0\rangle_{+}|1\rangle_{+} \pm |1\rangle_{+}|0\rangle_{+})/\sqrt{2}$.

(2–2) If the projection in (2–1) fails, Bob tells Alice to discard the corresponding $|\psi\rangle$.

(3) Verification 1:

(3–1) If the number of the remaining $|\psi\rangle$ is $n' \approx n/2$, they continue; otherwise, they abort the procedure.

(3–2) Alice randomly picks some of the remaining $|\psi\rangle$ and asks Bob to announce either their q or r depending on the value of c. To check Bob's announcement, Alice measures $\psi_{A_1}\psi_{A_2}$ in the basis $D_0 \equiv \{|0\rangle_{+}|0\rangle_{+}, |0\rangle_{+}|1\rangle_{+}, |1\rangle_{+}|0\rangle_{+}, |1\rangle_{+}|1\rangle_{+}\}$ and uses the result to calculate q, r that corresponds to $\psi_{B_1}\psi_{B_2}$.

(3–3) Bob randomly picks some other remaining $|\psi\rangle$ and asks Alice to announce both q and r. Alice performs the same measurement in (3–2) to obtain q, r to announce.(3–4) If {no conflicting results were found by both participants} and {the probabilities for $|r\rangle_q|r\rangle_q = |0\rangle_{+}|0\rangle_{+}$, $|r\rangle_q|r\rangle_q = |1\rangle_{+}|1\rangle_{+}$, $|r\rangle_q|r\rangle_q = |0\rangle_{\times}|0\rangle_{\times}$ and $|r\rangle_q|r\rangle_q = |1\rangle_{\times}|1\rangle_{\times}$ to occur are approximately the same}, they keep the remaining undiscarded and unverified $|\psi\rangle$ and continue.

(4) Alice inputting d:

(4–1) For each of the remaining m sets of $|\psi\rangle$, Alice picks $d = 0$ with the probability $p = 2/3$ and $d = 1$ with the probability $(1 - p) = 1/3$. If $d = 0$, she tries to decode s [defined as Eq. (2) by projecting $\psi_{A_1}\psi_{A_2}$ into the subspace supported by $\{|0\rangle_{+}|0\rangle_{+}, |1\rangle_{+}|1\rangle_{+}\}$. Here Bob's outcome s is defined as

$$s \equiv \begin{cases} Q, & c = 0, \\ r, & c = 1, \end{cases} \qquad (2)$$

where $Q = 0, 1$ for $q = +, \times$.

Otherwise, if $d = 1$, Alice tries to decode c by projecting $\psi_{A_1}\psi_{A_2}$ into $|1\rangle_{\times}|1\rangle_{\times}$ and $|0\rangle_{\times}|0\rangle_{\times}$. If the outcome is $|1\rangle_{\times}|1\rangle_{\times}(|0\rangle_{\times}|0\rangle_{\times})$, she knows that Bob has chosen $c = 0$ $(c = 1)$.

(4–2) If the projection in (4–1) fails, Alice tells Bob to discard the corresponding $|\psi\rangle$.

(5) Verification 2:

(5–1) If the number of the remaining $|\psi\rangle$ is about $m/2$, they continue; otherwise, they abort the procedure.

(5–2) Bob randomly picks some of the remaining $|\psi\rangle$ and asks Alice to announce either c or s depending on the value of d. Note that if $d = 0$, Alice needs to complete the measurement on $\psi_{A_1}\psi_{A_2}$ in the basis $\{|0\rangle_{+}|0\rangle_{+}, |1\rangle_{+}|1\rangle_{+}\}$, and she announces $s = 0$ $(s = 1)$ if the outcome is $(|0\rangle_{+}|0\rangle_{+}|1\rangle_{+}|1\rangle_{+})$.(5–3) If {no conflicting results were found} and {$d = 0$ occurs with the probability 2/3}, they keep the remaining undiscarded and unverified $|\psi\rangle$ and continue.