Symmetrically private information retrieval based on blind quantum computing

Zhiwei Sun,[1,*] Jianping Yu,[1] Ping Wang,[2,†] and Lingling Xu[3]

[1]*College of Information Engineering, Shenzhen University, Shenzhen, Guangdong 518060, People's Republic of China*

[2]*College of Computer Science and Software Engineering, Shenzhen University, Shenzhen 518060, People's Republic of China*

[3]*School of Computer Science and Engineering, South China University of Technology, Guangzhou 510006, People's Republic of China*

(Received 11 November 2014; published 4 May 2015)

Universal blind quantum computation (UBQC) is a new secure quantum computing protocol which allows a user Alice who does not have any sophisticated quantum technology to delegate her computing to a server Bob without leaking any privacy. Using the features of UBQC, we propose a protocol to achieve symmetrically private information retrieval, which allows a quantum limited Alice to query an item from Bob with a fully fledged quantum computer; meanwhile, the privacy of both parties is preserved. The security of our protocol is based on the assumption that malicious Alice has no quantum computer, which avoids the impossibility proof of Lo. For the honest Alice, she is almost classical and only requires minimal quantum resources to carry out the proposed protocol. Therefore, she does not need any expensive laboratory which can maintain the coherence of complicated quantum experimental setups.

DOI: 10.1103/PhysRevA.91.052303 PACS number(s): 03.67.Dd, 03.67.Hk

I. INTRODUCTION

Consider the following scenario: Alice wants to obtain the bth information from a database D, which is hosted by Bob and has N information. But she does not want Bob to learn which information she wanted. One simple solution is to ask for a copy of the whole database. While protecting the privacy of Alice, it is equally important that Alice should not be allowed to learn more than the amount of information that she pays for. For example, the information stored in the database may be both valuable and sensitive, and Bob wants to sell it piece by piece. This is referred to as database privacy, and the corresponding protocol is called symmetrically private information retrieval (SPIR), which is also known as 1-out-of-N oblivious transfer (OT). The symmetry means that Bob should not obtain the item that Alice is interested in (Alice's privacy). At the same time, Alice should not receive more information than she is entitled to (Bob's privacy). The 1-out-of-N OT is a generalization of the 1-out-of-2 OT which was originally introduced by Rabin [1] in 1981 and by Even, Goldreich, and Lempel [2] in 1985. The 1-out-of-2 OT can be described as follows. Bob sends two bits to Alice such that Alice only obtains one desired bit and knows nothing about the other bit and Bob is oblivious to which item she wanted.

It is well known that nontrivial two-party cryptographic primitives cannot be securely implemented if only error-free communication is available where the computing power and memory of the players are not limited. In other words, classical OT is not possible with unconditional security which might be broken by the strong ability of some advanced algorithms like quantum computation [3,4]. One might hope to use quantum information theory for these tasks. It is known to all that quantum information behaves in a way that is fundamentally different from classical information. Here, information is stored in qubits, such as the polarization state of a single photon. And the use of quantum information theory has proven extremely successful for unconditional secure key distribution between two honest parties [5,6]. In fact, there is an existing approach in the quantum world to OT [7]. Unfortunately, it is found that it offers no complete protection for both sides. Later, it has been proven that [8], in the case of two mutually distrusting parties with universal quantum computers available, even with quantum communication, unconditionally secure OT remains impossible: any protocol that guarantees that Bob gets no information whatsoever about which database item Alice has retrieved will leave the database completely vulnerable to attack by Alice.

However, there are several scenarios where these impossibility results do not apply, namely, (1) if the computing power of parties is bounded, (2) if the communication is noisy, (3) if the security conditions are relaxed, and (4) if the adversary is under some physical limitation.

For the first scenario, it is well known in classical cryptography that the security of protocols is based on plausible but unproven complexity assumptions [1,9], such as hardness of factoring or discrete logarithms. The second scenario has been used to construct both OT and bit commitment protocols in various models for the noise [10,11]. Recently, the third scenario has also been considered. Several quantum protocols have been proposed in this vein based on a cheat sensitive model [12,13], in which Bob is kept honest by the possibility of being caught cheating. Some researchers have considered the fourth scenario in the case that the adversary's quantum memory size is bounded [14,15]. In this paper, we focus on the scenario where the adversarial Alice has no quantum computer. There are at least three reasons why this may be a good idea: first, if we assume that Alice's quantum computer is unavailable, we avoid the impossibility result of Lo [8]. Second, a first-generation quantum computer will probably be implemented in the "cloud" style [16], since only a limited number of groups, such as governments and huge industries, will be able to possess it. Actually, the situation that not all the participants can afford expensive quantum resources and quantum operations is more common in various applications. Therefore, it is reasonable to assume that the

[*] sunzhiwei1986@gmail.com

[*] Corresponding author: wangping@szu.edu.cn

TABLE I. Comparison of several protocols where the impossibility does not apply.

Protocol	Security	Conditions for which security is known to hold
Computational [1]	Proven secure	Adversary has limited classical computational capability
Cheat sensitive [12,13]	Specific attacks discussed In Refs. [12,13]	No additional conditions
Noisy quantum storage [11]	Unconditional secure	Parameters of the adversary's quantum memory are known
Bounded quantum storage [14]	Unconditional secure	Adversary's quantum memory size is bounded
Our protocol	Unconditional secure	Adversary has limited quantum computational resources

user Alice has no ability to afford any quantum computer in the real-world environment for a long term. Third, the honest Alice is almost classical in our protocol and is only required to do measurements, such as the polarization measurement with a threshold detector. Thus, our protocol can reduce not only honest Alice's computational burden of the communication but also the cost of the quantum hardware devices in the practical implementation. A brief comparison of the above mentioned protocols is given in Table I.

It turns out that this is indeed possible: we present a protocol for symmetrically private information retrieval in which Alice with limited quantum resources learns the bth item of the database that is held by Bob with the universal quantum computer. Our protocol is perfectly concealing, i.e., Bob has no information whatsoever about which database element Alice has retrieved. And Alice with limited quantum resources can only be accessible to the bth information of the database.

Our protocol is based on the universal blind quantum computing (UBQC) protocol which was first proposed by Broadbent, Fitzsimons, and Kashefi [17] by using the measurement-based model of Raussendorf and Briegel [18]. In their protocol, Alice (who does not have any quantum computational resources or quantum memory) interacts with Bob (who has a quantum computer) in order to obtain the outcome of her target computation such that privacy is preserved. In other words, Bob learns nothing about Alice's inputs, outputs, or desired computation. However, in the case of SPIR the situation is slightly different from the blind quantum computation. On the one hand, the number of possible computing is very limited, and Bob might be able to exploit the fact. Thus, Bob can obtain the item that Alice is interested in. On the other hand, Alice may calculate f_i and f_j at the same time pretending to be calculating only f_k, where $i \neq j$. Due to the blindness, Bob cannot know this fact, and he wrongly thinks that Alice is calculating only f_k. Therefore, Alice can obtain more information than she should.

In order to protect Bob's privacy, first, we must make sure that there are problems that are solvable in polynomial time only on a quantum computer; second, the presented protocol must prevent Alice from calculating f_i and f_j at the same time, where $i \neq j$. Fortunately, we know that there is an entire class of problems, which are solvable in polynomial time only on a quantum computer [20], for example, the simulation of a complex quantum system [19] and the factoring of RSA problems. Although the RSA challenge, RSA-768 (where the numbers are labeled according to their number of binary digits), was broken in 2009 [21], so far there have not been designed any efficient classical algorithms to factor bigger numbers, such as RSA-1024 and RSA-2048. However, it is known that Shor's quantum algorithm can factor these RSA problems efficiently [3]. We denote the set of this kind of class of problems as F; i.e., F is the set of problems that are solvable in polynomial time only on a quantum computer. We denote $|f_i|$ as the number of computing f_i in the UBQC protocol. Let $F^{'}$ be the subset of F satisfying the property that $n/2 < |f_l| \leqslant n$, where $f_l \in F$ and n is a predetermined number by Alice and Bob, i.e., $F^{'} = \{f_l : n/2 < |f_l| \leqslant n, f_l \in F\}$. Since the problem f_l is solvable in polynomial time only on a quantum computer, for a malicious Alice without a quantum computer, she cannot compute f_l by herself in a reasonable time. Meanwhile, since $f_l \in F^{'}$, Alice cannot compute f_i and f_j at the same time within n steps, where $i \neq j$ and $f_i, f_j \in F^{'}$. Therefore, Bob can use the outcome of f_l as a secret key k_l to encrypt message m_l using a one-time-pad. Without knowing the key k_l, Alice cannot decrypt the message m_l. Thus, Bob's privacy is perfect. In order to avoid the leakage of Alice's information on the computation size, Bob is required to send n qubits to Alice. Alice measures the qubits which are isolated from the actual computation. Then, she measures the rest qubits according to the desired problem f_b. Therefore, Bob cannot distinguish Alice's computation from the number of possible computing, which prevents Bob from knowing Alice's item of interest.

The basic idea of our protocol is that Bob selects randomly N problems from $F^{'}$, and computes them as the secret keys to encrypt the message of database. Alice uses the UBQC protocol to compute the desired function f_b. Then, she can (only) decrypt the message m_b from Bob. Alice has no quantum computer, so she cannot compute other keys. Therefore, Bob's privacy is preserved. On the other hand, because of the unconditional security of the UBQC protocol, i.e., the fact that Alice's input, output, and algorithm are secret to Bob whatever he does, Bob cannot obtain the item b that Alice chooses. Namely, Alice's privacy is also preserved.

This paper is arranged as follows. The next section gives our protocol. Then, the security of the protocol is discussed. Finally, we give a conclusion.

II. DESCRIPTION OF THE PROTOCOL

In our protocol, the UBQC of Ref. [16] is used. In this UBQC protocol, Alice does only measurements, such as the polarization measurements with a threshold detector. And it is well known that the measurement of a state is much easier than the generation of a single-qubit state. Therefore, this UBQC protocol eases Alice's burden. Furthermore, the security of the UBQC protocol is based on a no-signaling principle, which makes the security proof against Bob become trivially simple in our presented SPIR protocol. In other words, the merits of Ref. [16] are preserved. Before giving our quantum private queries protocol, we review the blind quantum computing protocol of Ref. [16], which can be briefly described as follows:

(1) Bob prepares a resource state of measurement-based quantum computation. Any resource state can be used for this purpose [16].

(2) Bob sends a particle of the resource state to Alice through the quantum channel.

(3) Alice measures the particle in a certain angle which is determined by the algorithm in her mind.

They repeat steps 2 and 3 until the computation is finished. Note that whichever states malicious Bob prepares instead of the correct resource state, and whichever states malicious Bob sends to Alice, Bob cannot learn anything about Alice's information, since Alice does not send any signal to Bob and therefore, because of the no-signaling principle, Bob cannot gain any information about Alice by measuring his system. Otherwise, it contradicts the no-signaling principle.

In our protocol, a user Alice with limited quantum computational resources can query an item from a database held by Bob such that Bob cannot learn which element was retrieved, while Alice cannot obtain more information than what she queried. We assume there is no unwanted leakage of information from Alice's laboratory. And Alice and Bob have predetermined the set of problems, $F^{'}$. Our protocol is described as follows.

(1) Alice and Bob first carry out the quantum key distribution protocol to share a secret key K.

(2) Then, Bob chooses uniformly and randomly N problems $f_1,\ldots,f_N$ from $F^{'}$ where f_l is the description of the computation. Bob sends $f_1,\ldots,f_N$ to Alice using the shared secret key K. Note that Alice without a quantum computer cannot compute any function f_l, and she also cannot compute f_i and f_j at the same time within one UBQC, where $l,i,j \in \{1,\cdots,N\}, i \neq j$.

(3) Alice chooses a $b \in \{1,\cdots,N\}$ that is the item she wants from the database, and keeps it secret. Then, Alice delegates her computation f_b to Bob in such a way that Bob cannot learn anything about Alice's input, output, and f_b [16]. The actual computation is measurement based [18].

(4) More specifically, Bob prepares n states of measurement-based quantum computation, where the number n is predetermined by Alice and Bob before the protocol.

(5) Bob sends a particle of the n states to Alice through the quantum channel.

(6) Alice measures the particle in a certain angle which is determined by the algorithm in her mind.

(7) They repeat steps 5 and 6 until the computation is finished.

(8) As described in the Introduction, Bob announces the encrypted database $m_i^{'} = m_i \oplus f_i^{'}$, where m_i is the ith information of the database, $f_i^{'}$ is the computation result of the ith function f_i, and $i \in \{1,\cdots,N\}$. Then Alice can obtain $m_b = m_b^{'} \oplus f_b^{'}$ and read m_b.

III. SECURITY OF THE PROTOCOL

In the following, we will show that the proposed SPIR protocol is secure against Bob with a fully fledged quantum computer and secure against Alice, who has only limited quantum computational resources.

For the honest server Bob, Alice will obtain the correct answer of her desired item, since what Alice and Bob did is nothing but a usual measurement-based quantum computation and one-time-pad encryption. If Bob is dishonest, Bob may carry out the protocol as he wishes; i.e., Bob may prepare other states instead of the correct resource state, and send them to Alice. Since we have no verification procedure in our protocol, Alice cannot detect Bob's malicious behavior. However, there is only one-way communication from Bob to Alice, i.e., Alice does not send any signal to Bob. Because of the no-signaling principle, Bob gains no useful information regarding Alice's choice b. Otherwise, it contradicts the no-signaling principle. For the mathematical proof of the security against malicious Bob based on the no-signaling principle, refer to Sec. I of the Appendix of Ref. [16]. On the other hand, if Bob carries out the protocol dishonestly, after completion of the protocol, Alice can find that Bob sends incorrect query results. Bob's malicious behaviors will inevitably affect his reputation, and users may not buy Bob's database any more. Therefore, it is inadvisable for Bob to perform the protocol dishonestly. We have proven that the proposed protocol is secure against server Bob. Now we turn to the question of Bob's privacy.

For the user Alice, the useful information she received from Bob is f_i and $m_i^{'}$, where $i \in \{1,\cdots,N\}$. Using the property of UBQC, Alice successfully computes f_b based on her choice b, and gets the computation result $f_b^{'}$. Thus, Alice can correctly decrypt the bth message m_b of the database. On the conditions that Alice has only limited computational resources or power, and f_i can be computed in polynomial time only on a quantum computer, and f_i and f_j cannot be computed at the same time within n steps of the measurement-based quantum computation, Alice cannot learn the computation results $f_1^{'},\cdots,f_N^{'}$ other than $f_b^{'}$, where $i,j \in \{1,\cdots,N\}, i \neq j$. On the other hand, because of the property of the one-time-pad, without knowing $f_l^{'}$, Alice cannot learn m_l where $l \in \{1,\cdots,N\} - \{b\}$. Thus, the proposed protocol is also secure against Alice, who has only limited quantum computational resources.

IV. CONCLUSION

In this paper, we exploit a new application from a theoretical point of view that UBQC can be used to implement private queries. And 1-out-of-2 OT is just a special case of our protocol when $N = 2$. In our protocol, quantum limited Alice can query an item from Bob with a fully fledged quantum computer; meanwhile, the privacy of both parties is preserved. The security of our protocol is based on the condition that malicious Alice has no quantum computer. It is known to all that it is still a long way to build large-scale quantum computers. Thus, in the future there may be only a small number of costly quantum servers available in corporations and governments. It will be a long time before some users can afford expensive quantum computers. Therefore, our assumption is reasonable at least in the near future.

On the other hand, our protocol is a good solution for the scenario that user Alice wants to query secret information (e.g., national security importance, or proprietary and containing commercial secrets, or health records, or similar private records) from a power Bob (corporation or government) but does not want Bob to learn which information she wanted; meanwhile, Bob does not want her to learn the information that she does not pay for. For the honest Alice, she only requires minimal quantum resources to carry out the proposed protocol. Therefore, she does not need any expensive laboratory which can maintain the coherence of complicated quantum experimental setups. Thus, only with a weak computational device, Alice can access the resources of the power Bob (or calling him "Cloud"). This is similar to the cloud computing paradigm in which computing resources such as processing, memory, and storage are not physically present at the user's location. Instead, a service provider owns and manages these resources, and users access them via the Internet. Our proposal shows a theoretical study that UBQC can be developed for a new protocol. And it is also interesting whether UBQC can be used to carry out bit commitment or secure communication. This deserves further study.

ACKNOWLEDGMENTS

The authors are grateful to the anonymous referees for their valuable comments and suggestions that help to improve the paper. This work is supported by the National Natural Science Foundation of China under Grants No. 61272013, No. 61171072, No. 61402293, and No. 61202466, Natural Science Foundation of Guangdong Province (No. S2013040011789), Shenzhen Technology Plan (No. JCYJ20130401095947219), and Natural Science Foundation of SZU (No. 201435).

[1] M. O. Rabin, How to exchange secrets by oblivious transfer, Technical Report TR-81, Harvard Aiken Computation Laboratory, 1981.

[2] S. Even, O. Goldreich, and A. Lempel, A randomized protocol for signing contracts, Commun. ACM **28**, 637 (1985).

[3] P. W. Shor, Algorithms for quantum computation: Discrete logarithms and factoring, in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science* (IEEE, Los Alamitos, 1994), pp. 124–134.

[4] L. K. Grover, A fast quantum mechanical algorithm for database search, in *Proceedings of the 28th Annual ACM Symposium on Theory of Computing* (ACM, New York, 1996), pp. 212–219.

[5] H. K. Lo and H. F. Chau, Unconditional security of quantum key distribution over arbitrarily long distances, Science **283**, 2050 (1999).

[6] P. W. Shor and J. Preskill, Simple proof of security of the BB84 quantum key distribution protocol, Phys. Rev. Lett. **85**, 441 (2000).

[7] C. H. Bennett, G. Brassard, C. Crépeau, and M.-H. Skubiszewska, in *Practical Quantum Oblivious Transfer, CRYPTO'91* (Springer, Berlin, Heidelberg, 1992), pp. 351–366.

[8] H.-K. Lo, Insecurity of quantum secure computations, Phys. Rev. A **56**, 1154 (1997).

[9] C. Crépeau and J. Kilian, Achieving oblivious transfer using weakened security assumptions, in *Proceedings of the 29th Annual Symposium on Foundations of Computer Science* (IEEE, New York, 1988), pp. 42–52.

[10] S. Wehner, C. Schaffner, and M. B. Terhal, Cryptography from Noisy Storage, Phys. Rev. Lett. **100**, 220502 (2008).

[11] R. König, S. Wehner, and J. Wullschleger, Unconditional security from noisy quantum storage, IEEE Trans. Inf. Theor. **58**, 1962 (2012).

[12] M. Jakobi, C. Simon, N. Gisin, J.-D. Bancal, C. Branciard, N. Walenta, and H. Zbinden, Practical private database queries based on a quantum-key-distribution protocol, Phys. Rev. A **83**, 022301 (2011).

[13] F. Gao, B. Liu, Q.-Y. Wen, and H. Chen, Flexible quantum private queries based on quantum key distribution, Opt. Express **20**, 17411 (2012).

[14] I. B. Damgárd, S. Fehr, L. Salvail, and C. Schaffner, in *Secure Identification and QKD in the Bounded-Quantum-Storage Model, CRYPTO' 2007* (Springer, Berlin, Heidelberg, 2007), pp. 342–359.

[15] I. B. Damgárd, S. Fehr, L. Salvail, and C. Schaffner, Cryptography in the bounded-quantum-storage model, SIAM J. Comput. **37**, 1865 (2008).

[16] T. Morimae and K. Fujii, Blind quantum computation protocol in which Alice only makes measurements, Phys. Rev. A **87**, 050301 (2013).

[17] A. Broadbent, J. Fitzsimons, and E. Kashefi, Universal blind quantum computation, in *Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science* (IEEE, Piscataway, 2009), pp. 517–526.

[18] R. Raussendorf and H. J. Briegel, A One-Way quantum computer, Phys. Rev. Lett. **86**, 5188 (2001).

[19] R. P. Feynman, Simulating physics with computers, Int. J. Theor. Phys. **21**, 467 (1982).

[20] S. Barz, J. F. Fitzsimons, E. Kashefi, and P. Walther, Experimental verification of quantum computation, Nat. Phys. **9**, 727 (2013).

[21] T. Kleinjung *et al.*, in *Factorization of a 768-bit RSA Modulus, CRYPTO' 2010* (Springer, Berlin, Heidelberg, 2010), pp. 333–350.