2016

An efficient quantum scheme for Private Set Intersection

Run-hua Shi
University of Wollongong, rshi@uow.edu.au

Yi Mu
University of Wollongong, ymu@uow.edu.au

Hong Zhong
Anhui University

Jie Cui
Anhui University

Shun Zhang
Anhui University

Publication Details

Shi, R., Mu, Y., Zhong, H., Cui, J. & Zhang, S. (2016). An efficient quantum scheme for Private Set Intersection. Quantum Information Processing, 15 (1), 363-371.

An efficient quantum scheme for Private Set Intersection

Abstract

Private Set Intersection allows a client to privately compute set intersection with the collaboration of the server, which is one of the most fundamental and key problems within the multiparty collaborative computation of protecting the privacy of the parties. In this paper, we first present a cheat-sensitive quantum scheme for Private Set Intersection. Compared with classical schemes, our scheme has lower communication complexity, which is independent of the size of the server's set. Therefore, it is very suitable for big data services in Cloud or large-scale client-server networks.

Disciplines

Engineering | Science and Technology Studies

Publication Details

Shi, R., Mu, Y., Zhong, H., Cui, J. & Zhang, S. (2016). An efficient quantum scheme for Private Set Intersection. Quantum Information Processing, 15 (1), 363-371.

An Efficient Quantum Scheme for Private Set Intersection

Run-hua Shi[1,2] Yi Mu[2] Hong Zhong[1] Jie Cui[1] Shun Zhang[1]
1. School of Computer Science and Technology, Anhui University, Hefei City, 230601, China
2. Centre for Computer and Information Security Research, School of Computing and Information Technology, University of Wollongong, Wollongong NSW 2522, Australia
(Emails: hfsrh@sina.com, ymu@uow.edu.au, zhongh@mail.ustc.edu.cn, cvjxabcd@126.com, shzhang27@163.com)

Abstract. Private set intersection allows a client to privately compute set intersection with the collaboration of the server, which is one of the most fundamental and key problems within the multi-party collaborative computation of protecting the privacy of the parties. In this paper, we first present a cheat-sensitive quantum scheme for private set intersection. Compared with classical schemes, our scheme has lower communication complexity, which is independent of the size of the server's set. Therefore, it is very suitable for big data services in Cloud or large-scale client-server networks.

Keywords: Secure Multiparty Quantum Computation; Private Set Intersection; Cheat-sensitive.

1. Introduction

Private set intersection (PSI) is a primitive of secure multi-party computation that enables two parties – a client and a server – to compute the intersection of their respective sets without disclosing anything about their inputs. The client will learn the intersection of the two sets and the server will learn nothing [1]. PSI is also known as Private Matching (PM) [2].

There are many practical applications of PSI (or PM) for protecting the privacy of the parties, such as National Security and Law Enforcement [3], Genomic Sequences Query [4], Joint Market Investigation [5], Privacy-Preserving Data Mining [6], Matching the Data Outsourced to Cloud Storage Services [7], Location-Based Sharing Services [8], and other online services [9].

Because of its importance and wide applicability, many schemes for PSI and its variants have been proposed [1-3,10-15]. Among these schemes, the most efficient PSI scheme requires $O(n+m)$ costs in communication complexity, which increases linearly with both the client's set size, n, and the server's set size, m. Generally speaking, the size of the server's set is larger than that of the client's set. In order to reduce the communication complexity further, Wu *et al*. [2] presented an efficient PM scheme for very large m, which requires $O(nlog^2m)$ costs in communication complexity.

As we know, quantum cryptography has the advantage of higher security than classical cryptography. However, to the best of our knowledge, there is no any quantum scheme for PSI. In this paper, we first proposed a novel quantum scheme for PSI. The proposed scheme only requires $O(n)$ communication complexity, completely irrespective of the server set size, m. Therefore, it is especially suitable for large-scale client-server networks or Cloud service models.

2. Proposed Scheme

We informally give a definition of Private Set Intersection first and then present our quantum scheme for Private Set Intersection.

Definition 1. Private Set Intersection (PSI) - There are two parties, a client and a server. The client inputs a private set C and the server inputs a private set S. After running a PSI procedure, the client outputs the intersection of their respective sets, i.e., $C \cap S$, but the server gets nothing except the client's set size. In addition, PSI should meet the following requirements.

Correctness. The client finally outputs the exact (possibly empty) intersection of their respective sets.

Client Privacy. The server gets no information about the client's set elements, except his/her set size.

Server Privacy. The client learns no information about the subset $S - C \cap S$ (that is, the subset of elements on the server that are *NOT* in the intersection of their respective sets), except knowing the subset $C \cap S$.

Suppose the client's private set $C = \{c_1, c_2, \cdots, c_n\}$ and the server's private set $S = \{s_1, s_2, \cdots s_m\}$, and all elements of the sets C and S lie in $\mathbb{Z}_N^*$, where $\mathbb{Z}_N^* = \{1,2, \dots, N-1\}$ and N is a natural number, which is far larger than n and m (i.e., $N \gg n, m$). In the following scheme, we only consider the honest-but-curious parties, who follow the protocol (honesty), but record everything they see and try to extract a secret (curiosity). The proposed scheme consists of 4 steps, which are described in detail as follows:

Step 1. The client prepares n encoded states, $|\psi_i\rangle = \frac{|0\rangle + |c_i\rangle}{\sqrt{2}}$ for $i = 1$ to n, where c_i is his/her ith private element in C (i.e., $c_i \in C$). Furthermore, the client sends all encoded states to the server by an authenticated quantum channel [16,17,26,27].

Step 2. After receiving all encoded states sent from the client, the server applies a quantum operator G on each received state, and then sends them back to the client, where $G = -U_0 U_S$. Here, U_0 and U_S are unitary operators [18], defined as follows:

$$U_0|x\rangle = \begin{cases} |x\rangle & if \ x \neq 0 \\ -|0\rangle & if \ x = 0 \end{cases}, \tag{1}$$

$$U_S|x\rangle = \begin{cases} -|x\rangle & if \ x \in S \\ |x\rangle & if \ x \notin S \end{cases}, \tag{2}$$

where $|x\rangle$ is any basis state in N-dimensional Hilbert space. That is, U_0 maps $|0\rangle$ to $-|0\rangle$ and leaves the remaining $|x\rangle$ alone, and U_S maps $|x\rangle$ to $-|x\rangle$ if $x \in S$ and $|x\rangle$ otherwise. Then we get

$$\begin{aligned} |\phi_i\rangle &= G|\psi_i\rangle \\ &= G\frac{|0\rangle+|c_i\rangle}{\sqrt{2}} \\ &= -U_0 U_S \frac{|0\rangle+|c_i\rangle}{\sqrt{2}} \\ &= -\frac{U_0 U_S|0\rangle + U_0 U_S|c_i\rangle}{\sqrt{2}} \\ &= \begin{cases} -\frac{U_0|0\rangle - U_0|c_i\rangle}{\sqrt{2}} & if \ c_i \in S \\ -\frac{U_0|0\rangle + U_0|c_i\rangle}{\sqrt{2}} & if \ c_i \notin S \end{cases} \\ &= \begin{cases} \frac{|0\rangle+|c_i\rangle}{\sqrt{2}} & if \ c_i \in S \\ \frac{|0\rangle-|c_i\rangle}{\sqrt{2}} & if \ c_i \notin S \end{cases}. \end{aligned} \tag{3}$$

Step 3. For each state returned from the server, the client performs an honest test. That is, he/she check whether the superposition in the corresponding encoded state is preserved as follows: $\frac{|0\rangle+|c_i\rangle}{\sqrt{2}}$ or $\frac{|0\rangle-|c_i\rangle}{\sqrt{2}}$. Since the two possible states are obviously orthogonal and further the client knows the value of c_i, therefore he/she is able to completely distinguish them by a von Neumann measurement. If the client finds a cheat of the server (that is, the measured result is not $\frac{|0\rangle+|c_i\rangle}{\sqrt{2}}$ or $\frac{|0\rangle-|c_i\rangle}{\sqrt{2}}$), he/she will terminate this protocol; otherwise continue to the next step.

Step 4. The client gets the phase information $p(i)$ of each returned state by distinguishing it between $\frac{|0\rangle+|c_i\rangle}{\sqrt{2}}$ and $\frac{|0\rangle-|c_i\rangle}{\sqrt{2}}$, i.e., $p(i) = 1$ if it is in the state $\frac{|0\rangle+|c_i\rangle}{\sqrt{2}}$, and $p(i) = -1$ otherwise. Furthermore, if $p(i) = 1$, then $c_i \in C \cap S$; otherwise $c_i \notin C \cap S$. Finally, the client outputs all elements that the phase information is equal to one (i.e., $\{c_i | c_i \in C \wedge p(i) = 1$ for $i = 1$ to $n\}$). However, the server gets nothing except the size of the set C of the client.

3. Analysis

Correctness. The scheme proposed above clearly and rightly works when the client and the server honestly execute the protocol. If $c_i \in S$, it can easily see that $p(i) = 1$ by Eq.(3). Therefore, the client rightly outputs the intersection of their respective sets by n von Neumann measurements. That is, the proposed PSI scheme is correct.

Client Privacy mainly depends on the server's impossibility of discriminating the encoded quantum state sent from the client, thank to two basic laws of quantum theory: No-Cloning Theorem which forbids the creation of identical copies of an arbitrary unknown quantum state, and Heisenberg Uncertainty Principle which implies that it is impossible to measure the state of any system without disturbing that system.

In order to extract the secret information about c_i from the encoded state $|\psi_i\rangle$=$\frac{|0\rangle+|c_i\rangle}{\sqrt{2}}$, the server must measure the state $|\psi_i\rangle$. However, he cannot perform the equivalent measurement which the client does, because he does not know c_i. Therefore, if the server measures the encoded state, he will certainly disturb it. In the following section, we will analyze two measure-based attacks by a dishonest server in detail.

First, if the server directly measures the encoded state $\frac{|0\rangle+|c_i\rangle}{\sqrt{2}}$ by a simple projective measurement (intercept), the measured result can be either $|0\rangle$ or $|c_i\rangle$ with the probabilities $\frac{1}{2}$ and $\frac{1}{2}$, respectively. If he gets $|c_i\rangle$, he can successfully pass the honest test by re-preparing and returning a new quantum system in the state $|\psi_i\rangle = \frac{|0\rangle+|c_i\rangle}{\sqrt{2}}$ (resend). However, if he gets $|0\rangle$, he cannot pass the honest test. In short, this intercept-resend attack will be discovered in the honest test with the probability of $\frac{1}{2}$. That is, our scheme is cheat sensitive [19,20,21]. In order to further resist this intercept-resend attack, in principle the client can replace the encoded state $|\psi_i\rangle = \frac{|0\rangle+|c_i\rangle}{\sqrt{2}}$ with states of the form $\frac{e^{i\theta}|0\rangle+|c_i\rangle}{\sqrt{2}}$ [19], where the phase θ is a parameter randomly and privately selected by the client. Since the server does not know the value of θ, it will be clearly impossible for him to reprepare the correct reply state after his measurement.

Second, we further discuss a more complicated entangle-measure attack by a dishonest server that he/she is able to prepare an ancillary system and entangle the ancillary system with the quantum system carried the encoded states by his local unitary operations, and afterwards he can measure the ancillary system to get the partial information about the client's private inputs. For simplicity, we only consider the client's quantum system in the general state of $\frac{|0\rangle+|k\rangle}{\sqrt{2}}$, where k is a private element of the client's set C. Suppose that the initial state of the ancillary system is $|0\rangle_S$ and the server's dishonest action when he receives the client's encoded states can be described by a unitary operator $\widetilde{U}_{cs}$, which acts on the client's quantum system c and the server's ancillary system s. We can describe it as follows:

$$\widetilde{U}_{cs}|0\rangle_c|0\rangle_s = \sqrt{\eta_0}|0\rangle_c|\phi_0\rangle_s + \sqrt{1-\eta_0}|V_0\rangle_{cs}, \tag{4}$$

$$\widetilde{U}_{cs}|k\rangle_c|0\rangle_s = \sqrt{\eta_k}|k\rangle_c|\phi_k\rangle_s + \sqrt{1-\eta_k}|V_k\rangle_{cs}, \tag{5}$$

$$\widetilde{U}_{cs}\left(\frac{|0\rangle+|k\rangle}{\sqrt{2}}\right)_c|0\rangle_s = \sqrt{\eta_{+k}}\left(\frac{|0\rangle+|k\rangle}{\sqrt{2}}\right)_c|\phi_{+k}\rangle_s + \sqrt{1-\eta_{+k}}|V_{+k}\rangle_{cs}, \tag{6}$$

where $|V_0\rangle_{cs}$, $|V_k\rangle_{cs}$ and $|V_{+k}\rangle_{cs}$ are a vector orthogonal to $|0\rangle_c|\phi_0\rangle_s$, $|k\rangle_c|\phi_k\rangle_s$ and $|+k\rangle_c|\phi_{+k}\rangle_s$ ($|+k\rangle = \frac{|0\rangle+|k\rangle}{\sqrt{2}}$), respectively, i.e.,

$$_c\langle 0|_s\langle\phi_0|V_0\rangle_{cs} = 0, \tag{7}$$

$$_c\langle k|_s\langle\phi_k|V_k\rangle_{cs} = 0, \tag{8}$$

$$_c\langle +k|_s\langle\phi_{+k}|V_{+k}\rangle_{cs} = 0. \tag{9}$$

In order to completely pass the honest test (that is, the returned system c must be $\frac{|0\rangle+|k\rangle}{\sqrt{2}}$ without consideration of the phase transformation), we can easily deduce that the following condition holds in Eq. (6):

$$\eta_{+k} = 1. \tag{10}$$

That is,

$$\widetilde{U}_{cs}\left(\frac{|0\rangle+|k\rangle}{\sqrt{2}}\right)_c|0\rangle_s = \left(\frac{|0\rangle+|k\rangle}{\sqrt{2}}\right)_c|\phi_{+k}\rangle_s. \tag{11}$$

In addition, obviously the returned states cannot contain other vectors except the vectors of $|0\rangle_c$ and $|k\rangle_c$. Thus, in order to fully pass the honest test, Eqs. (4) and (5) must be restrained as the following expressions, accordingly:

$$\widetilde{U}_{cs}|0\rangle_c|0\rangle_s = \sqrt{\eta_0}|0\rangle_c|\phi_0\rangle_s + \sqrt{1-\eta_0}|k\rangle_c|\phi_k\rangle_s, \tag{12}$$

$$\widetilde{U}_{cs}|k\rangle_c|0\rangle_s = \sqrt{\eta_k}|k\rangle_c|\phi_k\rangle_s + \sqrt{1-\eta_k}|0\rangle_c|\phi_0\rangle_s. \tag{13}$$

Given from Eq. (11), when $k = 0$, it further gets,

$$\widetilde{U}_{cs}|0\rangle_c|0\rangle_s = |0\rangle_c|\phi_0\rangle_s. \tag{14}$$

It implies,

$$\eta_0 = 1. \tag{15}$$

Then, we get

$$\begin{aligned}
\widetilde{U}_{cs}|k\rangle_c|0\rangle_s &= \widetilde{U}_{cs}\left[\sqrt{2}(\tfrac{|k\rangle+|0\rangle-|0\rangle}{\sqrt{2}})\right]_c|0\rangle_s \\
&= \widetilde{U}_{cs}\left[\sqrt{2}|+k\rangle-|0\rangle\right]_c|0\rangle_s \\
&= \sqrt{2}\widetilde{U}_{cs}|+k\rangle_c|0\rangle_s - \widetilde{U}_{cs}|0\rangle_c|0\rangle_s \\
&= \sqrt{2}|+k\rangle_c|\phi_{+k}\rangle_s - |0\rangle_c|\phi_0\rangle_s \quad \text{(by Eq.(11))} \\
&= \sqrt{2}(\tfrac{|0\rangle+|k\rangle}{\sqrt{2}})_c|\phi_{+k}\rangle_s - |0\rangle_c|\phi_0\rangle_s \\
&= |0\rangle_c|\phi_{+k}\rangle_s + |k\rangle_c|\phi_{+k}\rangle_s - |0\rangle_c|\phi_0\rangle_s.
\end{aligned} \tag{16}$$

If we compute the scalar product between Eqs. (13) and (16), then we will obtain the identity

$$\begin{aligned}
1 &= \sqrt{1-\eta_k}\ {}_s\langle\phi_0|\phi_{+k}\rangle_s + \sqrt{\eta_k}\ {}_s\langle\phi_k|\phi_{+k}\rangle_s \\
&\quad -\sqrt{1-\eta_k}\ {}_s\langle\phi_0|\phi_0\rangle_s \\
&= \sqrt{1-\eta_k}\ {}_s\langle\phi_0|\phi_{+k}\rangle_s + \sqrt{\eta_k}\ {}_s\langle\phi_k|\phi_{+k}\rangle_s \\
&\quad -\sqrt{1-\eta_k}.
\end{aligned} \tag{17}$$

Since ${}_s\langle\phi_0|\phi_{+k}\rangle_s \leq 1$ and ${}_s\langle\phi_k|\phi_{+k}\rangle_s \leq 1$, so we get

$$1 \leq \sqrt{1-\eta_k} + \sqrt{\eta_k} - \sqrt{1-\eta_k}. \tag{18}$$

That is,

$$1 \leq \sqrt{\eta_k}, \tag{19}$$

which implies

$$\eta_k = 1. \tag{20}$$

Thus, we can obtain the following expanded expression

$$\begin{aligned}
\widetilde{U}_{cs}\left(\tfrac{|0\rangle+|k\rangle}{\sqrt{2}}\right)_c|0\rangle_s &= \tfrac{\widetilde{U}_{cs}|0\rangle_c|0\rangle_s+\widetilde{U}_{cs}|k\rangle_c|0\rangle_s}{\sqrt{2}} \\
&= \tfrac{|0\rangle_c|\phi_0\rangle_s+|k\rangle_c|\phi_k\rangle_s}{\sqrt{2}}.
\end{aligned} \tag{21}$$

Similarly, if we compute the scalar product between Eqs. (11) and (21), then we will obtain

$$1 = \tfrac{1}{2}\ {}_s\langle\phi_0|\phi_{+k}\rangle_s + \tfrac{1}{2}\ {}_s\langle\phi_k|\phi_{+k}\rangle_s. \tag{22}$$

By Eq. (22), it gives

$${}_s\langle\phi_0|\phi_{+k}\rangle_s = 1, \tag{23}$$

$${}_s\langle\phi_k|\phi_{+k}\rangle_s = 1. \tag{24}$$

From Eqs. (23) and (24), it shows that if the server wants to be sure that he passes the honest test, then the final states of the ancillary system s for any choice of k will coincide with $|\phi_0\rangle_s$, that is, the states of the ancillary system

s are independent of the secret k. Therefore, even though the server performs an entangle-measure attack, he cannot yet obtain any secret information about the secret k from the encoded state $\frac{|0\rangle+|k\rangle}{\sqrt{2}}$.

Server Privacy. If the client honestly executes the protocol, he/she cannot obtain any secret information about the server's private set, except knowing $C \cap S$. If the client is dishonest, it is possible for him/her to perform a cheating strategy as follows: he/she sends a false state $\frac{|j\rangle+|k\rangle}{\sqrt{2}}$ to the server, instead of the true state $\frac{|0\rangle+|k\rangle}{\sqrt{2}}$. Accordingly, the returned state from the server must be in either $\frac{|j\rangle+|k\rangle}{\sqrt{2}}$ or $\frac{|j\rangle-|k\rangle}{\sqrt{2}}$. However, from the states of $\frac{|j\rangle+|k\rangle}{\sqrt{2}}$ or $\frac{|j\rangle-|k\rangle}{\sqrt{2}}$, the client cannot get the right phase information $p(j)$ or $p(k)$, while he/she can infer that $p(j) = p(k)$ or $p(j) \neq p(k)$, but not deduce whether j or k belongs to the server's private set.

We have analyzed the security of proposed protocols in ideal settings. However, in practical settings, there may be some faults (e.g., noise and error) in the quantum channel and measurement. In order to ensure its security in practical settings, we can use the fault tolerant technologies, such as decoherence-free states and error-correcting code, which were introduced in References [22,23]. In addition, please note that we only consider the honest-but-curious parties in our protocols, which is similar to the semi-honesty model in the classical settings. In classical settings, any secure protocol in semi-honesty model can be correspondingly translated into a secure protocol in malicious model. However, it still needs to further study how to translate a protocol from semi-honesty model to malicious model in quantum settings. It is also our future work (especially, the definition of malicious model in quantum settings).

In addition, the authenticated quantum channel can ensure the security of quantum communications. Like most existing secure multiparty quantum computations, our scheme needs there is an authenticated quantum channel. This is the only assumption we need to have for the scheme to work. In principle, we may use a quantum authentication scheme (QAS) [24] based on Clifford operators introduced in [25] to implement it. We may also use quantum encryptions combined with classical authenticated keys [26,27]. In addition, we may still ensure the authentication by sharing the entangled quantum resources in advance or using the detecting (or decoy) particle technologies.

Finally, we analyze the communication costs of the proposed scheme. We can easily see that the client sends and receives n encoded states, respectively. So the communication complexity is $O(n)$, irrespective of the size of the server's set. Compared to the classical PSI schemes with $O(n+m)$ communication complexity, our proposed scheme has a very significant reduction in the communication complexity due to $O(n)$ communication complexity.

4. Conclusion

In this paper, we first presented a quantum method to solve PSI problem. In the proposed PSI scheme, the client first prepares n encoded states, and then sends them to the server. After applying n quantum operators, the server sends these encoded states back to the client. Finally the client performs n von Neumann measurements to privately choose out all elements of the intersection of their respective sets. During this process, two parties only require to exchange n quantum states. Obviously, both computation and communication complexities of the proposed scheme are $O(n)$, which are independent of the server's set size m. Therefore, it is very suitable for big data services in Cloud or large-scale client-server networks

Acknowledgments. This work was supported by National Natural Science Foundation of China (Nos 61173187, 61173188 and 11301002), the Ministry of Education institution of higher learning doctor discipline and scientific research fund aids a project financially (No.20133401110004), Natural Science Foundation of Anhui Province (Nos 11040606M141 and 1408085QF107), and the 211 Project of Anhui University (Nos 33190187 and 17110099).

References

[1] Freedman, M.J., Nissim, K., Pinkas, B.: Efficient Private Matching and Set Intersection. In Proc. of EUROCRYPT, LNCS 3027, (Interlaken, Switzerland, 2004) 1–19 (2004)

[2] Wu, M.E., Chang, S.Y., Lu, C.J., Sun, H.M.: A communication-efficient private matching scheme in Client-Server model. Information Sciences 275(10), 348-359 (2014)

[3] Cristofaro, E. De, Tsudik, G.: Fast and Private Computation of Cardinality of Set Intersection and Union. In Proc. of Financial Crypto, LNCS 6052, (Canary Islands, Spain, 2010) 143–159 (2010)

[4] Zhan, J., Cabrera, L., Osman, G., Shah, R.: Using Private Matching for Securely Querying Genomic Sequences. In Proc. of IEEE Third International Conference on Privacy, Security, Risk and Trust (passat) and Third International Conference On Social Computing (socialcom), (IEEE, 2011) 1163–1168 (2011)

[5] Li, Y., Tygar, J., Hellerstein, J.: Private matching. In Proc. of Computer Security in the 21st Century, 25–50 (2005)

[6] Chun, J.Y., Hong, D., Jeong, I.R., Lee, D.H.: Privacy-preserving disjunctive normal form operations on distributed sets. Information Sciences 231(10), 113–122 (2013)

[7] Pervez, Z., Awan, A.A., Khattak, A.M., Lee, S., Huh, E.N.: Privacy-aware searching with oblivious term matching for cloud storage. Journal of Supercomputing 63(2), 538–560 (2013)

[8] Narayanan, A., Thiagarajan, N., Lakhani, M., Hamburg, M., Boneh, D.: Location privacy via private proximity testing. In Proceedings of the Network and Distributed System Security Symposium (NDSS 2011), (San Diego, CA, USA), (2011)

[9] Bursztein, E., Hamburg, M., Lagarenne, J., Boneh, D.: Openconflict: preventing real time map hacks in online games. In Proc. of IEEE S&P 2011, 506–520 (2011)

[10] Hazay, C., Lindell, Y.: Efficient protocols for set intersection and pattern matching with security against malicious and covert adversaries. In Proc. of Theory of Cryptography Conference (TCC), LNCS 4948, (New York, USA, 2008), 155－175 (2008)

[11] Liu, L., Cao, Z.: Private matching protocols without error probability. In Proc. of the IEEE International Conference on Computer Science and Automation Engineering (CSAE), vol. 4, (IEEE, 2011) 363–366 (2011)

[12] Marconi, L., Conti, M., Pietro, R. Di: Cassandra: a probabilistic, efficient, and privacy-preserving solution to compute set intersection. International Journal of Information Security 10(5), 1–19 (2011)

[13] Kerschbaum, F.: Outsourced private set intersection using homomorphic encryption. In Proc. of ACM ASIACCS 2012, 85－86 (2012)

[14] Cristofaro, E.D., Tsudik, G.: Experimenting with Fast Private Set Intersection. In Proc. of the 5th International Conference on Trust & Trustworthy Computing (TRUST 2012), LNCS 7344, 55-73 (2012)

[15] Shao, Z.Y. and Yan, B.: Private set intersection via public key encryption with keywords search. Security and Communication Networks 8(3), 396-402 (2015)

[16] Barnum, H., Cr´epeau, C., Gottesman, D., Smith, A. and Tapp, A.: Authentication of quantum messages. In Proc. of 43rd Annual IEEE Symposium on Foundations of Computer Science (FOCS), 449–458 (2002)

[17] Aharonov, D., Ben-Or, M. and Eban, E.: Interactive proofs for quantum computations. In Proc. of Innovations in Computer Science, arxiv.org/abs/0810.5375 (2008)

[18] Grover, L. K: A fast quantum mechanical algorithm for database search. In Proc. of 28th Annual ACM Symposium on Theory of Computing, 212-219 (1996)

[19] Giovannetti, V., Lloyd, S. and Maccone, L.: Quantum private queries. Phys. Rev. Lett. 100(23), 230502 (2008)

[20] Olejnik, L.: Secure quantum private information retrieval using phase-encoded queries. Phys. Rev. A 84(2), 022313 (2011)

[21] Li, Y.B., Wen, Q.Y., Li, Z.C., Qin, S.J. and Yang, Y.T.: Cheat sensitive quantum bit commitment via pre- and post- selected quantum states. Quantum Inf. Process. 13(1) 141-149 (2014)

[22] Li, Y.B., Qin, S.J., Yuan, Z., Huang, W., Sun, Y.: Quantum private comparison against decoherence noise. Quantum Inf. Process. 12(6), 2191-2205 (2013)

[23] Li, Y.B., Wang, T.Y., Chen, H.Y, Li, M.D., Yang, Y.T.: Fault-Tolerate Quantum Private Comparison Based on GHZ States and ECC. Int. J. Theor. Phys. 52(8), 2818-2825 (2013)

[24] Barnum, H., Cr´epeau, C., Gottesman, D., Smith, A. and Tapp, A.: Authentication of quantum messages. In Proc. of 43rd Annual IEEE Symposium on Foundations of Computer Science (FOCS), 449–458 (2002)

[25] Aharonov, D., Ben-Or, M. and Eban, E.: Interactive proofs for quantum computations. In Proc. of Innovations in Computer Science, arxiv.org/abs/0810.5375 (2008)

[26] Yu, K.F., Yang, C.W., Liao, C.H., Hwang, T.: Authenticated semi-quantum key distribution protocol using Bell states. Quantum Inf. Process. 13(6), 1457-1465 (2014)

[27] Guan, D.J., Wang, Y.J., Zhuang, E.S.: A practical protocol for three-party authenticated quantum key distribution. Quantum Inf. Process. 13(11), 2355-2374 (2014)