Int J Software Informatics, Volume 8, Issue 3-4 (2014), pp. 339–343
International Journal of Software and Informatics, ISSN 1673-7288

E-mail: ijsi@iscas.ac.cn
http://www.ijsi.org
Tel: +86-10-62661040

Quantum Anonymous Ranking with d-level Single-Particle States

Qingbin Luo[1], Guowu Yang[2], Kun She[1], Xiaoyu Li[1], Yuqi Wang[2,3], and Fan Yang[2]

[1] (School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China)

[2] (School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China)

[3] (School of Computer Science, Minnan Normal University, Zhangzhou 363000, China)

Abstract In this paper, a novel quantum anonymous multiparty, multidata ranking (QAMMR) protocol with d-level single-particle states is proposed. Unlike the QKD-based QAMMR protocol in Ref. [1], the proposed protocol only need to operate single-particle states without distributing keys among the participants. $n(n \geqslant 3)$ participants can correctly and anonymously obtain the rankings of their data, with the help of a semi-honest third party. It is shown that nobody except the participant himself can match the identity with his data by security analysis.

Key words: multiparty quantum computation; anonymous ranking; single-particle state

Luo QB, Yang GW, She K, Li XY, Wang YQ and Yang F. Quantum anonymous ranking with d-level single-particle states. *Int J Software Informatics*, **Vol.8, No.3-4 (2014): 339–343. http://www.ijsi.org/1673-7288/8/i202.htm**

1 Introduction

Secure multiparty computation (SMC) is a subfield of cryptography and a basic topic in the distributed computation, which enables parties to perform correct, joint, distributed computation tasks without leaking their privates inputs. In the real world, the parties in these computations are partially trusted or competitive. Therefore, privacy naturally becomes the issue that participants are very concerned about. Since Yao[2] presented the famous Yao's millionaire problem, many classical results that the privacy of participants' inputs is guaranteed by the assumptions of computational complexity have been gained[2–6]. However, with the rapid development of quantum algorithms and quantum computing[7,8], these assumptions are facing severe challenges. To solve this problem, many research groups focus on the quantum version of secure multiparty computation, including quantum oblivious transfer[9–12], quantum secret sharing[13–16], quantum private database queries[17–20], quantum private comparison[21–24] and so on.

Quantum anonymous ranking is another branch of secure multiparty quantum computation. Huang et al in Ref. [1] first put forward the conception of quantum

This work is sponsored by the National Natural Science Foundation of China(Grant Nos.61272175)
Corresponding author: Qingbin Luo, Kun She, Email: qingbinluo@126.com, kunshe@126.com
Received 2014-08-29; Revised 2014-11-01; Accepted 2014-11-05.

anonymous ranking and presented a new quantum cryptographic primitive, the quantum anonymous multiparty, multidata ranking (QAMMR). The features of the QAMMR protocols are as follows.

(R1) Correctness. Every participant can correctly gain the sorted results of his data.

(R2) Anonymity. Nobody except a participant himself should get the sorted results of his data.

(R3) Untraceability. Nobody except a participant himself can match his identity with his data.

(R4) Security. The proposed protocol is secure against the quantum adversary. Then, Huang et al presented three QAMMR protocols, which were QAMMR protocol in semi-honest model, the QSS-based QAMMR protocol and the QKD-based QAMMR protocol. The participants in the first protocol were semi-honest, and each of the last two protocols was proposed with the help of a semi-honest third party.

In this paper, we present a novel QAMMR protocol based on d level single-particle states, with the help of a semi-honest third party. Here semi-honest third party (TP) refers, he/she will be strictly in accordance with the implementation of the protocol. That is to say TP will not conspire with external attackers or participants, even though he may be very curious about participants' data, and want to deduce them. As same as Ref. [1], the sequencing principle as follow is employed. Suppose n participants $P_1, P_2, \cdots, P_n$ want to know the rankings of their data sets of non-negative integers $D_{P_1}, D_{P_2}, \cdots, D_{P_n}$. Set $D = D_{P_1} \bigcup D_{P_2} \bigcup \cdots \bigcup D_{P_n} = \{d_1, d_2, \cdots, d_{|D|}\}$, where $d_1 \leqslant d_2 \leqslant \cdots \leqslant d_{|D|}$, and $|D|$ is the number of elements contained in the data set D. After the joint quantum computation without leaking the information of participants' data to others, if every participant gains the value of $|D^{d_i}| = |D^{d_i}_{P_1}| + |D^{d_i}_{P_2}| + \cdots + |D^{d_i}_{P_n}|$ for $1 \leqslant i \leqslant |D|$ (where $|D^{d_i}_{P_j}|$ means the number of d_i contained in data set D_{P_j}), They can respectively gain the rankings of their data in ascending order(e.g. the ranking of d_i in data set D is $|D^{d_1}| + |D^{d_2}| + \cdots + |D^{d_{i-1}}| + 1$). To be sure, no secure anonymous multiparty multidata ranking protocol [1] if $n = 2$, so the number of participants in the proposed protocol is also supposed to be larger than 2.

The rest of this paper is organized as follows. In Sect.2, the proposed protocol is described in details. In Sect.3, the security are analysed. Finally, a short conclusion is given in Sect.4.

2 The Quantum Anonymous Ranking Protocol

In a d-level quantum system, a common orthogonal basis is $B_Z = \{|0\rangle, |1\rangle, \cdots, |d-1\rangle\}$. The other orthogonal basis used in the following protocol can be obtained through quantum Fourier transform operator F transform B_Z, it is $B_F = \{F|0\rangle, F|1\rangle, \cdots, F|d-1\rangle\}$. The quantum Fourier transform defined as follows

$$F|j\rangle = \frac{1}{\sqrt{d}} \sum_{k=1}^{d-1} e^{\frac{2\pi ijk}{d}} |k\rangle, j = 0, 1, \cdots, d-1. \quad (1)$$

Obviously, B_Z and B_F are two mutually unbias bases. Then we introduce a

unitary transform operation used in the following text.

$$U = \sum_{k=1}^{d-1} |k \oplus 1\rangle\langle k| \tag{2}$$

where the symbol $\oplus$ denotes addition module d. The effect of the operation U can be illustrated as

$$U^x|j\rangle = |j \oplus x\rangle, j = 0, 1, \cdots, d-1 \tag{3}$$

and

$$U^x F|j\rangle = e^{-\frac{2\pi ijx}{d}} F|j \oplus x\rangle, j = 0, 1, \cdots, d-1 \tag{4}$$

where U^x presents performing the operation U x times.

Suppose the measurement value of the single-particle states $|0\rangle$ and $F|0\rangle$ are 0, $|1\rangle$ and $F|1\rangle$ are $1, \cdots, |d-1\rangle$ and $F|d-1\rangle$ are $d-1$ in the bases $B_Z = \{|0\rangle, |1\rangle, \cdots, |d-1\rangle\}$ and $B_F = \{F|0\rangle, F|1\rangle, \cdots, F|d-1\rangle\}$ respectively. Now, let us describe our QAMMR protocol in detail. Suppose $n(n \geqslant 3)$ participants want to know the rankings of their data, where the data set of the participant P_i is $D_{P_i} = \{m_1^i, m_2^i, \cdots, m_{k_i}^i\}$, and $D_{P_i} \subseteq \{1, 2, \cdots, N\}$. Then they can proceed as follows.

Step 1. TP distributes a random N-dit and d-ary secret key to each of the participants, the method in Ref. [1] is employed. We denote the key that TP distribute to participant P_i as $K^i = [K_1^i, K_2^i, \cdots, K_N^i]$.

Step 2. TP randomly prepares $N + \delta$ single-particle states from $\{|0\rangle, |1\rangle, \cdots, |d-1\rangle, F|0\rangle, F|1\rangle, \cdots, F|d-1\rangle\}$ and records which basis these states belong to, where δ is the check rate. The particle sequence formed by these states is denoted as S_0. Then TP send the sequence S_0 to participant P_1.

Step 3. After receiving the particle sequence S_0, participant P_1 do eavesdropping check with TP firstly. Concretely, after obtaining the acknowledgement of participant P_1 from a classical authentication channel, TP announces the positions and bases of δ decoy particles. Participant P_1 measure these particles and checks whether eavesdroppers exist in the quantum channels. If the error rate is greater than the predetermined threshold($\tau = 2 \sim 8.9\%$[25]), the protocol is aborted, Otherwise, participant P_1 encodes all his/her data. Specifically, if the nonnegative integer $m_i^1 (1 \leqslant i \leqslant k_1)$ are contained in his/her data set, he/she performs the unitary operator U on the remaining m_i^1th single-particle state. And the unitary operator $U^{K_j^1}$ is performed on the remaining jth$((1 \leqslant j \leqslant N))$ single-particle state. Participant P_1 randomly prepare δ decoy particles from $\{|0\rangle, |1\rangle, \cdots, |d-1\rangle, F|0\rangle, F|1\rangle, \cdots, F|d-1\rangle\}$ and insert them into the encoded N particles, which forms the new sequence S_1. Then he/she send the sequence S_1 to participant P_2.

Step 4. The rest of the $n-1$ participants execute the procedures just like what participant P_1 do in step 3 one after another. Finally, the last participant P_n sends all the processed particle sequence S_n to TP.

Step 5. After receiving the particle sequence S_n, TP do eavesdropping check with participant P_n firstly. If no eavesdropper exist, TP has received S_n securely.

Then TP measures the remaining N particles in S_n with right bases, the measurement outcome is recorded as $V = [V_1, V_2, \cdots, V_N]$. Suppose the initial value of these states is $I = [I_1, I_2, \cdots, I_N]$, $|D^i|$ is computed as $|D^i| = V_i \ominus I_i \ominus \sum_{j=1}^{n} K_i^j$ (where the symbol $\ominus$ denotes subtraction module d). Finally, TP publicly announces all the values of $|D^i|(1 \leqslant i \leqslant N)$. According to the announced values, each of the n participants can gain the rankings of his data. For example, participant P_i will know the ranking of his datum m_j^i is $|D^1| + |D^2| + \cdots + |D^{m_j^i - 1}| + 1$.

In this protocol, the data from different participants could be same, and ones from the same participant are different, so $d > n$ is necessary. If the actions of participants are limited, such as not connive or will not destroy the protocol to get the information of others, the first step in the protocol can be omitted. In addition, the receiver should set up a wavelength filter and a photon number filter to prevent the invisible photon attack[26] and delay-photon Trojan horse attack[27].

3 Security Analysis

If a quantum attacker(an outside attacker, a participant P_j or the semi-honest third party TP) wonders the secret inputs of participant P_i, he/she will do two things: one is that he/she must know the key K^i, the other is that he/she must know the actions of participant P_i without disturbing the decoy particles. For the first case, the outside attacker and participant P_j will not get the key K^i by the security analysis in Ref. [1]. However, TP knows the key K^i, can he/she take certain measures to know P_i's actions? It is impossible. Participant P_i should set up a wavelength filter and a photon number filter to prevent the invisible photon attack and delay-photon Trojan horse attack. The proposed protocol is secure against intercept-resend attack similar to Ref. [24]. Then we consider the circumstance in which more than one attacker try to eavesdrop the secret inputs of P_i. No mater what kind attack the attackers utilize, they also cannot success since they are unable get the key K^i. Hence, we have demonstrated that the quantum attackers will neither gain the data of participants and nor match the data with participants' identity. It is evident that the proposed protocol is correct, so our protocol satisfies the features (R1)–(R4).

4 Conclusion

This paper proposes an novel QAMMR protocol using d-level single-particle states. In this protocol, n participants can know the rankings of their data set in size within one execution, with the help of a semi-honest third party. Huang et al. also proposed a QAMMR protocol based on d-level single-particle states[1]. The Difference between the two protocols is that our protocol does not distribute keys among the participants. It is known that nobody except a participant himself can neither gain the ranking of his data nor match his data with his identity by the secure analysis.

References

[1] Huang W, Wen Q Y, Liu B, et al. Quantum anonymous ranking. Phys. Rev. A, 2014, 89(3): 032325.

[2] Yao AC. Protocols for secure computations. Proc. of 23rd IEEE Symposium on Foundations of Computer Science (FOCS 82). Washington, DC, USA. 1982. 160–164.
[3] Goldreich O, Micali S, Wigderson A. How to play ANY mental game. Proc. of the Nineteenth Annual ACM Conference on Theory of Computing. NewYork. 1987. 218–229.
[4] Canetti R, Lindell Y, Ostrovsky R, et al. Universally composable two-party and multi-party secure computation. Proc. of the Thiry-fourth Annual ACM Symposium on Theory of Computing. ACM. 2002. 494–503.
[5] Canetti R. Security and composition of multiparty cryptographic protocols. Journal of Cryptology, 2000, 13(1): 143–202.
[6] Lindell Y, Pinkas B. Secure multiparty computation for privacy-preserving data mining. Journal of Privacy and Confidentiality, 2009, 1(1): 59–98.
[7] Shor PW. Algorithms for quantum computation: discrete logarithms and factoring. Proc. 35th Annual Symposium on Foundations of Computer Science. IEEE. 1994. 124–134.
[8] Grover LK. Quantum mechanics helps in searching for a needle in a haystack. Phys. Rev. Lett., 1997, 79(2): 325–328.
[9] Bennett CH, Brassard G, Crpeau C, et al. Practical quantum oblivious transfer. Advances in CryptologyCRYPTO96. Springer Berlin Heidelberg, 1992: 351–366.
[10] Crpeau C. Quantum oblivious transfer. Journal of Modern Optics, 1994, 41(12): 2445–2454.
[11] Mayers D. Quantum key distribution and string oblivious transfer in noisy channels. Advances in CryptologyCRYPTO96. Springer Berlin Heidelberg, 1996: 343–357.
[12] Winkler S, Wullschleger J. On the efficiency of classical and quantum oblivious transfer reductions. Advances in CryptologyCRYPTO 2010. Springer Berlin Heidelberg, 2010: 707–723.
[13] Hillery M, Buzek V, Berthiaume A. Quantum secret sharing. Phys. Rev. A, 1999, 59(3): 1829–1834.
[14] Xiao L, Long G L, Deng F G, et al. Efficient multiparty quantum-secret-sharing schemes. Phys. Rev. A, 2004, 69(5): 052307.
[15] Zhang Z, Li Y, Man Z. Multiparty quantum secret sharing. Phys. Rev. A, 2005, 71(4): 044301.
[16] Chen XB, Niu XX, Zhou XJ, et al. Multi-party quantum secret sharing with the single-particle quantum state to encode the information. Quantum Inf. Process, 2013, 12(1): 365–380.
[17] Giovannetti V, Lloyd S, Maccone L. Quantum private queries. Phys. Rev. Lett., 2008, 100(23): 230502.
[18] Jakobi M, Simon C, Gisin N, et al. Practical private database queries based on a quantum-key-distribution protocol. Phys. Rev. A, 2011, 83(2): 022301.
[19] Giovannetti V, Lloyd S, Maccone L. Quantum private queries: security analysis. IEEE Trans. on Information Theory, 2010, 56(7): 3465–3477.
[20] Zhang JL, Guo FZ, Gao F, et al. Private database queries based on counterfactual quantum key distribution. Phys. Rev. A, 2013, 88(2): 022334.
[21] Yang YG, Wen QY. An efficient two-party quantum private comparison protocol with decoy photons and two-photon entanglement. Journal of Physics A: Mathematical and Theoretical, 2009, 42(5): 055305.
[22] Tseng HY, Lin J, Hwang T. New quantum private comparison protocol using EPR pairs. Quantum Inf Process, 2012, 11(2): 373–384.
[23] Liu B, Gao F, Jia H, et al. Efficient quantum private comparison employing single photons and collective detection. Quantum Inf. Process, 2013, 12(2): 887–897.
[24] Luo QB, Yang GW, She K, et al. Multi-party quantum private comparison protocol based on d-dimensional entangled states. Quantum Inf. Process, 2014, 13(10): 2343–2352.
[25] Chang YJ, Tsai CW, Hwang T. Multi-user private comparison protocol using GHZ class states. Quantum Inf. Process, 2013, 12(2): 1077–1088.
[26] Li XH, Deng FG, Zhou HY. Improving the security of secure direct communication based on the secret transmitting order of particles. Phys. Rev. A, 2006, 74(5): 054302.
[27] Cai QY. Eavesdropping on the two-way quantum communication protocols with invisible photons. Phys. Lett. A, 2006, 351(1): 23–25.