Quantum Inf Process (2017) 16:225
DOI 10.1007/s11128-017-1676-x

Quantum solution to a class of two-party private summation problems

Run-Hua Shi[1] · **Shun Zhang**[1]

Received: 28 March 2017 / Accepted: 20 July 2017 / Published online: 28 July 2017

Abstract In this paper, we define a class of special two-party private summation (S2PPS) problems and present a common quantum solution to S2PPS problems. Compared to related classical solutions, our solution has advantages of higher security and lower communication complexity, and especially it can ensure the fairness of two parties without the help of a third party. Furthermore, we investigate the practical applications of our proposed S2PPS protocol in many privacy-preserving settings with big data sets, including private similarity decision, anonymous authentication, social networks, secure trade negotiation, secure data mining.

Keywords Quantum cryptography · Quantum computation · Secure multi-party quantum computation · Privacy-preserving

1 Introduction

Secure multi-party computation (SMC) allows a number of mutually distrustful parties to compute a joint function of their inputs without leaking any information about their respective private inputs. Due to its important military and business values, SMC has raised widespread concerns and has been extensively researched in the cryptographic community, since it was first introduced by Yao [1] and extended by Goldreich et al. [2].

The general SMC problem is well known to be solvable, in theory, using circuit evaluation protocols [3,4]. However, the communication complexity of these protocols depends on the size of the circuit that expresses the functionality to be computed [5].

✉ Run-Hua Shi
hfsrh@sina.com

[1] School of Computer Science and Technology, Anhui University, 230601 Hefei City, China

As Goldreich pointed out [6], using the general solution to solve specific problems can be impractical; problem-specific solutions should be developed, for efficiency reasons.

Subsequently, solutions for some specific SMC problems [7–12] have appeared that use well-known primitive protocols as important building blocks, such as oblivious transfer [13], homomorphic encryption [14], Yao's millionaire problem [1], and zero-knowledge proof [15]. Compared with general circuit evaluation protocols, these specific protocols have reduced complexity, especially communication complexity. However, for many applications with big data sets, these existing protocols are still not efficient enough due to their linear communication complexities, which is relative to the size of data sets. Furthermore, it is also difficult for these protocols to guarantee the fairness to all participants without the help of a third party. In addition, the security of most existing SMC protocols is based on unproven difficulty assumptions, which are vulnerable to attack by the quantum computer.

As we know, with the advent of fast quantum algorithms [16,17], classical cryptosystems, including symmetric and asymmetric (i.e., public key) cryptosystems, are facing enormous threat and challenges. On the other hand, quantum cryptography opens a new era. The security of quantum cryptography is based on the physical principles of quantum mechanics, so it can provide unconditional security in theory. Since Bennett and Brassard presented the first quantum key distribution protocol [18], quantum cryptography has been widely studied and rapidly developed. Nowadays, many results have been reported, such as quantum encryption [19], quantum secret sharing [20], quantum secure direct communication [21], and quantum signature [22]. Furthermore, SMC is also studied extensively in quantum cryptography [23–25]. Especially, another more practical kind of quantum SMC protocol, called Quantum Private Query [26–30], has drawn attention recently. However, unfortunately, Lo [31], Colbeck [32] and Buhrman et al. [33] independently pointed out that unconditionally secure nonrelativistic two-party computations are impossible. Later results further show that although there is not a perfectly secure two-party computation, quantum protocols, such as quantum bit commitment [34] and quantum coin tossing [18], can still provide a reasonable security improvement over corresponding classical protocols.

In this paper, we focus on a specific class of SMC problems, involving two participants, conventionally called Alice and Bob, in which Alice and Bob have a private vector $(x_1, x_2, \ldots, x_N)$ and $(y_1, y_2, \ldots, y_N)$, respectively, for which they want to jointly compute the summation $\sum_{i=1}^{N} f(x_i, y_i)$ without revealing any private information, where $f(x_i, y_i) \in \{0, 1\}$. Hereafter, we call these special two-party private summation problems S2PPS problems.

To our knowledge, no quantum protocol currently exists for this kind of two-party private summation problem. Furthermore, we are deeply inspired by some novel quantum protocols [35–38], which achieve an exponential reduction in communication complexity compared to classical solutions. Since unconditionally secure two-party quantum protocols require the help of a third party, we seek practically secure quantum protocol for S2PPS problems. In this paper, we present a cheat-sensitive quantum solution to S2PPS problems, in which a dishonest party cannot perform a cheat strategy without risking detection by the honest party. Compared with classical related solutions [7–12], the proposed solution has the advantages of higher security, lower communication complexity, and perfect fairness.

The paper is organized as follows. In next section, we present a cheat-sensitive quantum solution to S2PPS problems, and in Sect. 3 give a security analysis and performance comparisons. In addition, we discuss practical applications in Sect. 4. We conclude in Sect. 5.

2 Proposed protocol

We first give an informal definition of special two-party private summation (S2PPS).

Definition 1 *(S2PPS problem).* Two parties, Alice and Bob, have a private vector $(x_1, x_2, \ldots, x_N)$ and $(y_1, y_2, \ldots, y_N)$, respectively, and they want to jointly compute the summation $\sum_{i=1}^{N} f(x_i, y_i)$ without revealing any other private information except the summation $\sum_{i=1}^{N} f(x_i, y_i)$, where $f(x_i, y_i) \in \{0, 1\}$.

Definition 2 *(S2PPS protocol).* Alice and Bob input a private vector $(x_1, x_2, \ldots, x_N)$ and $(y_1, y_2, \ldots, y_N)$, respectively. After executing this protocol, both Alice and Bob output the result of $\sum_{i=1}^{N} f(x_i, y_i)$, where $f(x_i, y_i) \in \{0, 1\}$. In addition, this protocol should meet the following requirements:

Correctness Two honest parties get the right result for $\sum_{i=1}^{N} f(x_i, y_i)$.

Alice's Privacy Bob cannot learn any secret information about Alice's x_i except possible information deduced from the result $\sum_{i=1}^{N} f(x_i, y_i)$ and his private vector $(y_1, y_2, \ldots, y_N)$.

Bob's Privacy Alice cannot get any secret information about Bob's y_i except possible information inferred from $\sum_{i=1}^{N} f(x_i, y_i)$ and her private vector $(x_1, x_2, \ldots, x_N)$.

Fairness Two parties are perfect peer entities, and they can get the result $\sum_{i=1}^{N} f(x_i, y_i)$ with equal opportunities. In addition, the probabilities of two parties' successfully cheating are exactly equal.

In the following protocol, suppose that Alice's private vector is $(x_0, x_1, \ldots, x_{N-1})$ and Bob's private vector $(y_0, y_1, \ldots, y_{N-1})$. For simplicity, furthermore, we assume that all components of the two vectors lie in Z_N, where $Z_N = \{0, 1, 2, \ldots, N-1\}$ and $N = 2^n$. The proposed protocol consists of 5 steps, which are described in detail as follows.

3 Analysis

3.1 The correctness

By the definition in Step 3 of the proposed protocol, t is the number of $i \in \{0, 1, 2, \ldots, N-1\}$ such that $f(x_i, y_i) = 1$ on the resultant state $\frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} \mid i\rangle \mid x_i\rangle \mid y_i\rangle \mid f(x_i, y_i)\rangle$. Obviously, t is equal to $\sum_{i=1}^{N} f(x_i, y_i)$ because of $f(x_i, y_i) \in \{0, 1\}$. Furthermore, in the next step, two parties count t using quantum counting algorithm, respectively. So the correctness of the proposed protocol is guaranteed by quantum counting algorithm.

Quantum S2PPS protocol

1 Alice and Bob prepare an initial state $\mid \psi_0\rangle = \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1} \mid i\rangle \bigotimes \mid 0\rangle$, respectively. Furthermore, Alice applies an oracle operator U_A to her initial state $\mid \psi_0\rangle$, which implements $\frac{1}{\sqrt{N}}\sum_{i=0}^{N-1} \mid i\rangle \bigotimes \mid 0\rangle \to \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1} \mid i\rangle \mid x_i\rangle$. At the same time, Bob performs an oracle operator U_B on his initial state $\mid \psi_0\rangle$, which implements $\frac{1}{\sqrt{N}}\sum_{i=0}^{N-1} \mid i\rangle \bigotimes \mid 0\rangle \to \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1} \mid i\rangle \mid y_i\rangle$. Let $\mid \psi_A\rangle = \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1} \mid i\rangle \mid x_i\rangle$ and $\mid \psi_B\rangle = \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1} \mid i\rangle \mid y_i\rangle$. Then, Alice sends the state $\mid \psi_A\rangle$ to Bob through the quantum channel and Bob sends the state $\mid \psi_B\rangle$ to Alice through the quantum channel.

2 After receiving the other party's quantum state $\mid \psi_B\rangle$ or $\mid \psi_A\rangle$, Alice and Bob further generate the state $\mid \psi_{AB}\rangle = \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1} \mid i\rangle \mid x_i\rangle \mid y_i\rangle$ by the similar oracle operators as described above, respectively. That is, Alice with all x_is applies the oracle operator U_A to her received state $\mid \psi_B\rangle = \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1} \mid i\rangle \mid y_i\rangle$ and an auxiliary state $\mid 0\rangle$ and then obtains the state $\mid \psi_{AB}\rangle = \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1} \mid i\rangle \mid x_i\rangle \mid y_i\rangle$. Similarly, Bob with all y_is applies the oracle operator U_B to his received state $\mid \psi_A\rangle = \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1} \mid i\rangle \mid x_i\rangle$ and an auxiliary state $\mid 0\rangle$ and then gets the state $\mid \psi_{AB}\rangle = \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1} \mid i\rangle \mid x_i\rangle \mid y_i\rangle$. Furthermore, two parties apply another oracle operator U_f to their respective quantum state $\mid \psi_{AB}\rangle$, which implements $\mid \psi_{AB}\rangle \bigotimes \mid 0\rangle \to \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1} \mid i\rangle \mid x_i\rangle \mid y_i\rangle \mid f(x_i, y_i)\rangle$. Call the resultant state $\mid \tilde{\psi}_{AB}\rangle$.

3 Alice and Bob execute quantum counting algorithm [39–41] to count t, respectively, where t is the number of $i \in \{0, 1, 2, \ldots, N-1\}$ such that $f(x_i, y_i) = 1$ on $\mid \psi_{AB}\rangle$. After executing quantum counting algorithm, Alice and Bob get $\tilde{t}_A$ and $\tilde{t}_B$, the quantum estimator of t, respectively.

4 Two parties exchange $\tilde{t}_A$ and $\tilde{t}_B$ by using quantum bit string commitment protocol [42] as follows: (1) Alice commits the bit string $\tilde{t}_A$ to Bob, and Bob commits the bit string $\tilde{t}_B$ to Alice; (2) Alice opens her bit string commitment, $\tilde{t}_A$, and Bob opens his string commitment, $\tilde{t}_B$; (3) Alice and Bob verify the validness of the other's bit string commitment.

5 After verifying the validness of the other's counting result, Alice and Bob compare two counting results. If the difference of two counting results is more than 2ε(*i.e.*, $|\tilde{t}_A - \tilde{t}_B| > 2\varepsilon$), where ε is error of estimation in quantum counting algorithm, she (or he) will find the cheating of the other party. Otherwise she (or he) will believe that the other party is honest.

3.2 Alice's privacy

In our proposed protocol, before exchanging the quantum counting results, Alice only sends the state $\mid \psi_A\rangle$ to Bob without any classical information, where $\mid \psi_A\rangle = \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1} \mid i\rangle \mid x_i\rangle$. Although all classical information about Alice's private vector is embedded into the state $\mid \psi_A\rangle$, anyone cannot extract all this information only from $\mid \psi_A\rangle$.

On the one hand, a dishonest Bob can make a projective measurement on the state $\mid \psi_A\rangle$ (i.e., $\frac{1}{\sqrt{N}}\sum_{i=0}^{N-1} \mid i\rangle \mid x_i\rangle$). Accordingly, he will get $|i\rangle|x_i\rangle$ for any i with the probability of $\frac{1}{N}$. So the system A sent by Alice can be characterized by the quantum ensemble $\varepsilon \equiv \{p_i, \rho_A l(i)\}$, where $p_i = \frac{1}{N}$ is Bob's probability of getting the component x_i (Assuming that initially Bob does not have any prior information on Alice's private vector), and

$$\rho_A(i) = |i\rangle|x_i\rangle\langle x_i|\langle i| . \tag{1}$$

Furthermore, Holevo's theorem [43] tells us that the accessible information available to Bob by any measurement on ρ_A is bounded by the entropy

$$\begin{aligned} I \leq \mathcal{X}(\varepsilon) &= S(\rho_A) - \frac{1}{N}\sum_{i=0}^{N-1} S(\rho_A(i)) \\ &= S(\rho_A), \end{aligned} \tag{2}$$

where $\rho_A = \sum_{i=0}^{N-1} \rho_A(i)/N$ is the average state of A. So $I \leq S(\rho_A) = n$. That is, Bob can extract at most a component x_i (n bits) of Alice's private vector by any possible measurement.

On the other hand, if Bob extracts the partial private information about Alice's private vector, where the maximum amount is just equal to that of a component of Alice's private vector (i.e., one-Nth of Alice private information), he will certainly lose the chance to further get $\tilde{t}_B$, which is an estimation of t, due to No-cloning Theorem which forbids the creation of identical copies of an arbitrary unknown quantum state. However, in order to complete the honest test of Alice in Step 5, Bob can try to steal as much information as possible from Alice's quantum commitment. By the results of Ref. [42], the information about the $n \approx Cn'$ bit string accessible to Bob is at most $\log n'$ bits, where C is a positive constant. Furthermore, his probability of identifying all n bits (i.e., $\tilde{t}_A$) is at most $\epsilon = 2^{-(n - \log n'))}$. That is, the successful probability of his cheating is at most ϵ. Therefore, if Bob extracts Alice's partial private information from the state $|\psi_A\rangle$, he will be detected in later honest test performed by Alice with the probability of $(1-\epsilon)$ at least, where $\epsilon = 2^{-(n-\log n')}$.

3.3 Bob's privacy

Similarly, a dishonest Alice can get one component of Bob's private vector by her local measurement. However, her dishonesty will be detected by Bob with the probability of $(1-\epsilon)$ at least, where $\epsilon = 2^{-(n-\log n')}$.

3.4 Fairness

In the S2PPS protocol proposed above, we see that the two parties, Alice and Bob, execute the same prescribed procedures, which include exchanging two initial quantum states, running the quantum counting algorithm, exchanging the counting results by a quantum bit string commitment protocol, and finally comparing the counting results. From this point of view, two parties are perfect peer entities.

In addition, by the analysis above, the successful probabilities of two parties' cheating are exactly equal, i.e., $\epsilon = 2^{-(n-\log n')}$.

To sum up, Alice and Bob in our proposed protocol are perfect peer entities and each obtains the result of $\sum_{i=0}^{N-1} f(x_i, y_i)$ with the equal opportunity. Therefore, our proposed protocol ensures perfect fairness for the two parties. By contrast, in the corresponding classical protocols, either the help of a third party is needed, or one party first gets the final results and then tells the other party. (But the one can cheat, so it is difficult to ensure the fairness).

3.5 Efficiency

Here, we mainly analyze the communication costs of the proposed protocol. From Step 1 to Step 3 of this protocol, we can easily see that Alice and Bob only exchange two quantum messages (i.e., $|\psi_A\rangle$ and $|\psi_B\rangle$), where the size of each quantum message is $2n$ qubits ($n = \log N$). In addition, the quantum cost of quantum bit string commitment protocol is $2n$ qubits. Finally, two parties open (i.e., exchange) two classical messages (i.e.,$\tilde{t}_A$ and $\tilde{t}_B$), where the bit length of the classical messages is n bits. Therefore, the communication complexity of our proposed protocol is $O(\log N)$ (i.e., transmitting $O(\log N)$ qubits/bits). Obviously, our proposed protocol achieves a significant reduction in communication complexity, compared to the classical related protocols with the linear communication complexity (i.e., transmitting $O(N)$ messages, each with $\log N$ bits).

4 Applications

In this section, we further investigate practical applications of proposed quantum S2PPS protocol in many privacy-preserving settings.

4.1 The Hamming distance problem

Definition 3 *(Hamming distance)*. For any $X, Y \in \{0, 1\}^N$, the Hamming weight of X, denoted by $|X|$, is the number of 1's in X, and the Hamming distance of X and Y is $|X \oplus Y|$, with "$\oplus$" being bit-wise XOR. Furthermore, if $X = (x_1, x_2, \ldots, x_N)$ and $Y = (y_1, y_2, \ldots, y_N)$, then $|X \oplus Y| = \sum_{i=1}^{N} x_i \oplus y_i$.

In S2PPS problem, let the Boolean function $f(x_i, y_i) = x_i \bigoplus y_i$, where $x_i, y_i \in \{0, 1\}$ and $\oplus$ denotes bit-wise XOR. It is equivalent to privately compute the value of $\sum_{i=1}^{N} x_i \oplus y_i$, which is the Hamming distance between two private vectors X and Y. Then S2PPS problem will become the Hamming distance problem, in which two parties have a private 0/1 vector, respectively, and they want to jointly compute the Hamming distance between two private vectors (i.e., $\sum_{i=1}^{N} x_i \oplus y_i$) without revealing their respective private information.

Obviously, the smaller the Hamming distance is, the more similar the two vectors are; if the Hamming distance is equal to 0, two vectors are identical. So, the Hamming distance problem can be widely applied to privately determine the similarity in fields, such as biological information, medical care and e-commerce. In addition, based on the Hamming distance problem, we can also solve the socialist millionaires' problem by introducing a secure hash function, in which two parties want to decide whether their private secrets a and b are equal or not. Obviously, if $a = b$, then the Hamming distance between the bit strings of $h(a)$ and $h(b)$ is 0.

4.2 Private set intersection/union cardinality

Definition 4 *(Private Set Intersection/Union Cardinality problem).* There are two parties, similarly called Alice and Bob. Alice and Bob have a private set A and B, respectively, and they want to jointly compute the cardinality of the intersection/union of their respective sets, i.e., $|A \cap B| / \left|A \bigcup B\right|$ without revealing their respective private information.

Without loss of generality, suppose that all components of two sets belong to Z_N. Furthermore, Alice and Bob transform their respective private set to an N-dimensional 0/1 vector in the following encoding method: the ith component of the vector is equal to 1 if i belongs to her/his set, and 0 otherwise. In addition, let the Boolean function $f(x_i, y_i) = x_i \wedge y_i / f(x_i, y_i) = x_i \vee y_i$ in our S2PPS problem, where $x_i, y_i \in \{0, 1\}$, and $\wedge$, $\vee$ denote the Boolean operator AND, OR, respectively. It is equivalent to privately compute the value of $\sum_{i=1}^{N} x_i \wedge y_i / \sum_{i=1}^{N} x_i \vee y_i$ with two private N-dimensional 0/1 vectors, which represent two private sets. Then S2PPS problem will become Private Set Intersection/Union Cardinality problem.

There are many important applications of Private Set Intersection/Union Cardinality problem in the real world. For instance, Private Set Intersection Cardinality (PSI-CA) can be used in anonymous authentication, authenticating a remote user without revealing his/her identity, e.g., when a remote user requests the server to authenticate his/her legality, the server asks the user to jointly execute a quantum PSI-CA (i.e., S2PPS) protocol and further verifies whether the intersection cardinality of their respective private sets is equal to a constant, which is assigned by a trusted third party in advance. Moreover, Private Set Union Cardinality (PSU-CA) problem is useful in social networks, e.g., when two parties want to privately determine the number of all connections in order to decide whether it exceeds a threshold value, it only needs to jointly run a quantum PSU-CA (i.e., S2PPS) protocol, where each element of their respective private sets represents a connection.

4.3 Secure trade negotiation

In the S2PPS problem, let the Boolean function $f(x_i, y_i) = (x_i > y_i)$, i.e., $f(x_i, y_i) = 1$ if $x_i > y_i$, and 0 otherwise. Equivalently, we may jointly compute the value of $\sum_{i=1}^{N}(x_i > y_i)$ with two private data sets. Similarly, this S2PPS problem can be applied in some complicated cryptographic tasks, e.g., in a trade negotiation, one party has N products, each with a minimum price, and hopes to sell more at the highest possible prices. The other party wants to buy these products, but he is not willing to buy one over a maximum price. Before starting the negotiation, two parties want to determine whether the number of the products which can be traded (i.e., satisfying the traded property that the maximum price of the buyer is bigger than the minimum price of the seller) is over a threshold value, and otherwise they will cancel this negotiation. In order to fulfil the task, they only need to jointly run a quantum S2PPS protocol, where each element of their respective private sets represents a minimum / maximum price.

5 Conclusion

We defined and investigated a class of special two-party private summation (S2PPS) problems. Inspired by quantum fast algorithms, we focused on a quantum solution to the S2PPS problem and presented a cheat-sensitive quantum S2PPS protocol, in which the dishonest party's cheating can be detected by the other party with high probability (i.e., $1 - \epsilon$ at least, where $\epsilon = 2^{-(n - \log n')}$). The proposed S2PPS protocol makes ingenious use of a quantum counting algorithm and a quantum bit string commitment protocol, where the former greatly improves the efficiency and the latter ensures perfect fairness. In addition, we studied its practical applications for different cryptographic tasks, such as private similarity decision, anonymous authentication, social networks, secure trade negotiations, and privacy-preserving data mining.

At present, we only give an approximate quantum solution to S2PPS problems in theory, i.e., the proposed protocol only obtains an approximate value of the summation, so our future work seeks a precise quantum approach to solve S2PPS problems.

Acknowledgements This wok was supported by National Natural Science Foundation of China (No. 61173187) and Talents Youth Fund of Anhui Province Universities (No. 2013SQRL006ZD).

References

1. Yao, A.C.: Protocols for secure computations. In: Proceedings of the 23rd IEEE Symposium on Foundations of Computer Science (FOCS' 82), p. 160 (1982)
2. Goldreich, O., Micali, S., Wigderson, A.: How to play ANY mental game. In: Proceedings of the 19th Annual ACM Symposium on Theory of Computing (STOC'87), p. 218 (1987)
3. Yao, A.C.: How to generate and exchange secrets. In: Proceedings of the 27th Annual Symposium on Foundations of Computer Science (FOCS'86), p. 162 (1986)
4. Lindell, Y., Pinkas, B.: A proof of Yao's protocol for secure two-party computation. J. Cryptol. **22**, 161 (2009)
5. Lindell, Y., Pinkas, B.: Secure multiparty computation for privacy-preserving data mining. J. Priv. Confid. **1**, 59 (2009)
6. Goldreich, O.: Secure Multi-Party Computation (Final (incomplete) Draft, Version 1.4). http://www.wisdom.weizmann.ac.il/~oded/PSX/prot.pdf
7. Atallah, M.J., Du, W.: Secure multi-party computational geometry. In: Proceedings of the 7th International Workshop on Algorithms and Data Structures, LNCS 2125, p. 165 (2001)
8. Freedman, M.J., Nissim, K., Pinkas, B.: Efficient private matching and set intersection. In: Proceedings of the Advances in Cryptology—Eurocrypt 2004, LNCS 3027, p. 1 (2004)
9. Cristofaro, E.D., Gasti, P., Tsudik, G.: Fast and private computation of cardinality of set intersection and union. In: Proceedings of the Cryptology and Network Security, LNCS 7712, p. 218 (2012)
10. Wu, M.E., Chang, S.Y., Lu, C.J., Sun, H.M.: A communication-efficient private matching scheme in Client–Server model. Inf. Sci. **275**, 348 (2014)
11. Vaidya, J., Shafiq, B., Fan, W., Mehmood, D., Lorenzi, D.: A random decision tree framework for privacy-preserving data mining. IEEE Trans. Dependable Secur. Comput. **11**, 399 (2014)
12. Debnath, S.K., Dutta, R.: Secure and efficient private set intersection cardinality using bloom filter. In: Proceedings of the Information Security, LNCS 9290, p. 209 (2015)
13. Chan, P., Lucio-Martinez, I., Mo, X.F., Simon, C., Tittel, W.: Performing private database queries in a real-world environment using a quantum protocol. Sci. Rep. **4**, 5233 (2014)
14. Tan, S.H., Kettlewell, J.A., Ouyang, Y.K., Chen, L., Fitzsimons, J.F.: A quantum approach to homomorphic encryption. Sci. Rep. **6**, 33467 (2016)
15. Brassard, G.: Modern Cryptology: A Tutorial. Lecture Notes in Computer Science, vol. 325. Springer, New York (1988)

16. Shor, P.W.: Algorithms for quantum computation—discrete logarithms and factoring. In: Proceedings of the 35th Annual Symposium on the Foundations of Computer Science, p. 124 (1994)
17. Grover, L.K.: A fast quantum mechanical algorithm for database search. In: Proceedings of the 28th Annual ACM Symposium on Theory of Computing, p. 212 (1996)
18. Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. In: Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, p. 175 (1984)
19. Boykin, P.O., Roychowdhury, V.: Optimal encryption of quantum bits. Phys. Rev. A **67**, 042317 (2003)
20. Lai, H., Zhang, J., Luo, M.X., Pan, L., Pieprzyk, J., Xiao, F.Y., Orgun, M.A.: Hybrid threshold adaptable quantum secret sharing scheme with reverse Huffman–Fibonacci-tree coding. Sci. Rep. **6**, 31350 (2016)
21. Farouk, A., Zakaria, M., Megahed, A., Omara, F.A.: A generalized architecture of quantum secure direct communication for N disjointed users with authentication. Sci. Rep. **5**, 16080 (2015)
22. Wang, T.Y., Cai, X.Q., Ren, Y.L., Zhang, R.L.: Security of quantum digital signatures for classical messages. Sci. Rep. **5**, 9231 (2015)
23. Crépeau, C., Gottesman, D., Smith, A.: Secure multi-party quantum computation. In: Proceedings of the Thirty-Fourth Annual ACM Symposium on Theory of Computing, p. 643 (2002)
24. Ben-or, M., Crépeau, C., Gottesman, D., Hassidim, A., Smith, A.: Secure multiparty quantum computation with (only) a strict honest majority. In: Proceedings of the 47th Annual IEEE Symposium on Foundations of Computer Science, p. 249 (2006)
25. Unruh, D.: Universally composable quantum multi-party computation. In: Proceedings of the Advances in Cryptology—EUROCRYPT 2010, LNCS 6110, p. 486 (2010)
26. Jakobi, M., Simon, C., Gisin, N., et al.: Practical private database queries based on a quantum key distribution protocol. Phys. Rev. A **83**, 022301 (2011)
27. Gao, F., Liu, B., Wen, Q., Chen, H.: Flexible quantum private queries based on quantum key distribution. Opt. Express **20**, 17411 (2012)
28. Gao, F., Liu, B., Huang, W., Wen, Q.: Post-processing of the oblivious key in quantum private queries. IEEE. J. Sel. Top. Quantum Electr. **21**, 6600111 (2015)
29. Liu, B., Gao, F., Huang, W., Wen, Q.: QKD-based quantum private query without a failure probability. Sci. China Phys. Mech. Astron. **58**, 100301 (2015)
30. Wei, C., Wang, T., Gao, F.: Practical quantum private query with better performance in resisting joint-measurement attack. Phys. Rev. A **93**, 042318 (2016)
31. Lo, H.K.: Insecurity of quantum secure computations. Phys. Rev. A **56**, 1154 (1997)
32. Colbeck, R.: Impossibility of secure two-party classical computation. Phys. Rev. A **76**, 062308 (2007)
33. Buhrman, H., Christandl, M., Schaffner, C.: Complete insecurity of quantum protocols for classical two-party computation. Phys. Rev. Lett. **109**, 160501 (2012)
34. Hardy, L., Kent, A.: Cheat sensitive quantum bit commitment. Phys. Rev. Lett. **92**, 157901 (2004)
35. Giovannetti, V., Lloyd, S., Maccone, L.: Quantum private queries. Phys. Rev. Lett. **100**, 230502 (2008)
36. Olejnik, L.: Secure quantum private information retrieval using phase-encoded queries. Phys. Rev. A **84**, 022313 (2011)
37. Shi, R.H., Mu, Y., Zhong, H., Zhang, S.: Quantum oblivious set-member decision protocol. Phys. Rev. A **92**, 022309 (2015)
38. Shi, R.H., Mu, Y., Zhong, H., Cui, J., Zhang, S.: Secure multiparty quantum computation for summation and multiplication. Sci. Rep. **6**, 19655 (2016)
39. Brassard, G., Høyer, P., Tapp, A.: Quantum counting. In: Proceedings of the 25th International Colloquium on Automata, Languages and Programming, LNCS 1443, p. 820 (1998)
40. Mosca, M.: Counting by quantum eigenvalue estimation. Theor. Comput. Sci. **264**, 139 (2001)
41. Diao, Z.J., Huang, C.F., Wang, K.: Quantum counting: algorithm and error distribution. Acta. Appl. Math. **118**, 147 (2012)
42. Kent, A.: Quantum bit string commitment. Phys. Rev. Lett. **90**, 237901 (2003)
43. Holevo, A.: Probabilistic and Statistical Aspects of Quantum Theory. Publications of the Scuola Normale Superiore. Springer, New York (2011)