IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 16, 2019, accepted March 5, 2019, date of publication March 15, 2019, date of current version March 29, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2903823

Quantum Wireless Network Private Query With Multiple Third Parties

NA LI[1,2], JIAN LI[1], XIUBO CHEN[3], AND YUGUANG YANG[4]

[1]School of Computer, Beijing University of Posts and Telecommunications, Beijing 100876, China
[2]Jilin Medical University, Jilin City 132013, China
[3]State Key Laboratory of Networking and Switching Technology, Information Security Center, Beijing University of Posts and Telecommunications, Beijing 100876, China
[4]College of Computer Science and Technology, Beijing University of Technology, Beijing 100124, China

Corresponding author: Jian Li (proflijian@126.com)

This work was supported in part by the National Natural Science Foundation of China under Grant U1636106, Grant 61472048, Grant 61671087, and Grant 61572053, and in part by the Beijing University of Posts and Telecommunications Excellent Ph.D. Students Foundation under Grant CX2017313.

ABSTRACT With the development of quantum wireless networks, the practical application of quantum private query (QPQ) should conform to the features of quantum wireless networks to achieve any-to-any query, and QPQ requires a new query mechanism. We first propose a scheme for a network private query in a quantum wireless network with multiple third parties, in which any user can query any database with the assistance of the third parties, by measuring each of the distant nodes that initially share entanglement with each other. The required entanglement among these nodes is established by the third-party intermediate node equipped with GHZ generator using multi-qubit GHZ states. A bilayer network topology, as well as the corresponding private query protocol, ensures the rapid and secure private query. Under the protection of the multi-qubit GHZ state's quantum correlation, the privacy of Alice and Bob is protected from the third parties' fake entangled attack and external attack, and they cannot obtain the privacy of each other by taking quantum memory attack. The performance parameters of the proposed scheme are described based on the analysis of classical wireless communication cost and communication delay.

INDEX TERMS Quantum private query, quantum wireless network, security.

I. INTRODUCTION

In a type of applications, the two authorized parties not only expect their information to be protected from external attackers, but also their respective privacy against each other. This type of problem is formalized as symmetrically private information retrieval (SPIR) by Gertner *et al.* [1], where the privacy of the user, as well as the security of the database, is guaranteed. Quantum private query (QPQ) falls into this category, which also protects database security while protecting user privacy. That is, the user, Alice, wants to retrieve an entry from a database, the database holder Bob cannot obtain the information about which entry she wants. Simultaneously, Bob cannot disclose more information than what Alice wants. The SPIR with information-theoretic security is proved to be impossible [2].

Giovannetti *et al.* [3], [4] presented the first QPQ protocol (GLM protocol) in 2008. Then, the protocol was improved by Olejnik [5] (O-protocol) in 2011. Nevertheless, the above two protocols are arduous to implement because they depend on oracle operations. When a large database is concerned, the oracle dimension is very high. Besides, it is affected by channel loss attack. Accordingly, it is not practical. To solve this problem, Jakobi *et al.* [6] first proposed a new practical private database queries protocol based on a quantum key distribution (QKD) protocol (J-protocol). In fact, the earliest QKD-based scheme is based on the Bennett-Brassard (BB84) QKD protocol [7], but its disadvantage is that if the user performs a quantum memory attack, then the security of the database is gone. Jakobi *et al.* use the Scarani-Acin-Ribordy-Gisin (SARG04) QKD protocol [8] instead of BB84 protocol to resist quantum memory attacks. Since then, a host of attention has been focused on QKD-based QPQ protocols, and quite a few similar protocols were proposed [9], [10], [12]–[35].

Existing works on QPQ mainly research from three aspects: research on the methods of oblivious key distribution [9], [10], [12]–[21], research on the classic

The associate editor coordinating the review of this manuscript and approving it for publication was Marcello Caleffi.

post-processing (CPP) algorithms [20], [22]–[24] and research on the ways to stand against channel noise [21], [23], [25]. In the first aspect, Gao *et al.* [9] and Yang *et al.* [10] proposed flexible QPQ protocols, which use the thoughts of B92 protocol [11] to improve J-protocol. By adjusting the value of a parameter θ, Gao *et al.*'s protocol exhibits better database security when $\theta < \frac{\pi}{4}$, while Yang *et al.*'s protocol can simultaneously obtain better database security and user privacy under the same conditions. Zhang *et al.* [12] presented a QPQ protocol based on counterfactual quantum key distribution. By adding key detection devices to QKD devices, the user privacy and database security can be kept secure. To ensure the security against the joint-measurement (JM) attack, Wei *et al.* [19] presented a novel QPQ protocol based on a two-way QKD scheme and Yang *et al.* [20] proposed a CPP algorithm. In terms of improving CPP algorithms, Rao and Jakobi [22] proposed $N - N$ and $rM - N$ schemes to improve CPP scheme of J-protocol, which reduce the communication complexity from $O(N\log N)$ to $O(N)$. However, the aforementioned schemes still suffer the problem that there is no error-correction algorithm in post-processing, which is not really practical. Therefore, Gao *et al.* [23] proposed an effective error-correction method which makes such QPQ more practical. Regarding the communication efficiency and security, Yang *et al.* [24] presented a novel CPP scheme to reduce the communication complexity and improve the security. In terms of ways to stand against channel noise, Chan *et al.* [21] proposed a fault-tolerant QPQ protocol in which a novel error-correction algorithm is used to cope with noisy channels, accompanied by a proof-of-concept demonstration of the protocol over a deployed fiber. Gao *et al.* [23] proposed a novel error-correction method in post-processing which also can stand against channel noise. Yang *et al.* [25] presented a robust QPQ protocol based on alternative sequences of single-qubit measurements which can resist channel noise.

To the best of our knowledge, all existing QPQ protocols concentrate on point-to-point private query between two remote parties. However, with the development of quantum wireless network, the practical application of QPQ should conform to the features of quantum wireless network to achieve any-to-any query. Wireless technology has supplied more flexible and inexpensive ways in the quantum communication field, QPQ requires a new query mechanism. The wireless network is integrated with quantum physics to guarantee the security of the network, named quantum wireless network. Quantum entanglement is an important characteristic of quantum physics. Based on quantum entanglement, quantum wireless network private query (QWNPQ) can be realized without transmitting qubits between the user and the database. Thus far, there is no work focused on QWNPQ. In this paper, we present a novel QWNPQ with multiple third parties scheme, in which the third-party Trent prepares and distributes the multi-qubit GHZ states to Alice, Bob and other related third-party intermediate nodes after the user Alice requests to query the database Bob in the wireless network. Subsequently, they randomly select the X basis $\{|+x\rangle, |-x\rangle\}$ or Y basis $\{|+y\rangle, |-y\rangle\}$ to measure the GHZ particles in their hands and record the measurement results, where $|\pm x\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$, $|\pm y\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm i|1\rangle)$. Trent uses the quantum correlation of the multi-qubit GHZ state to assist Alice in obtaining one or more entries from Bob's database with the help of other third-party intermediate nodes. The proposed protocol is secure for both Alice and Bob's private information. It is worth noting that, there is a requirement that the third parties Trent and other intermediate nodes cannot collude with any of Alice and Bob.

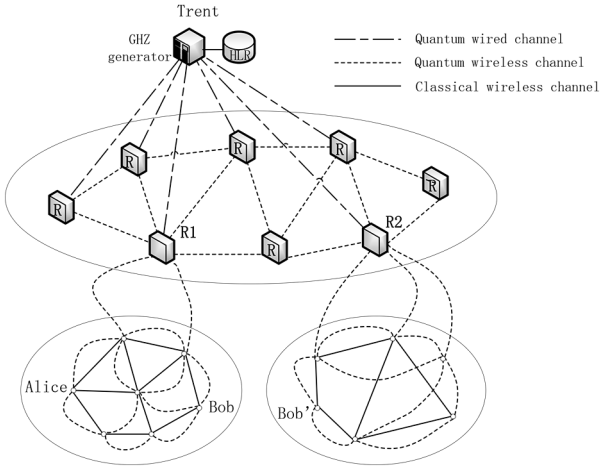


FIGURE 1. Bilayer network topology for QWNPQ.

The remainder of this paper is organized as follows. The next section introduces bilayer network topology for QWNPQ and the proposed QWNPQ protocol. Sect. III analyzes the security of the proposed protocol. Finally, a discussion and conclusion is drawn in Sect. IV.

II. QUANTUM WIRELESS PRIVATE QUERY NETWORK

A. BILAYER NETWORK TOPOLOGY FOR QWNPQ

In the bilayer network topology for QWNPQ, as is presented in Figure. 1, the spatially separated nodes are distributed on two layers: one layer is quantum backbone routers(QBRs) and the other layer is the terminals under the QBRs. The QBRs can store-and-forward information and function as quantum relays for some time; the terminals under their coverage are distributed mobile quantum devices with both quantum and wireless communication capabilities. The home location register (HLR) is responsible for recording the current location of terminals. The node equipped with the GHZ generator in the core network is responsible for generating the GHZ states and distributing the particles to corresponding nodes through quantum wired channels. Based on this flexible network topology, the quantum wireless channels (QWCs) are established only when necessary, thus the resource consumption can be largely reduced.

B. QWNPQ PROTOCOL

We start by describing the protocol that Alice and Bob (Bob') in Figure. 1 must follow. Suppose that any user Alice intends

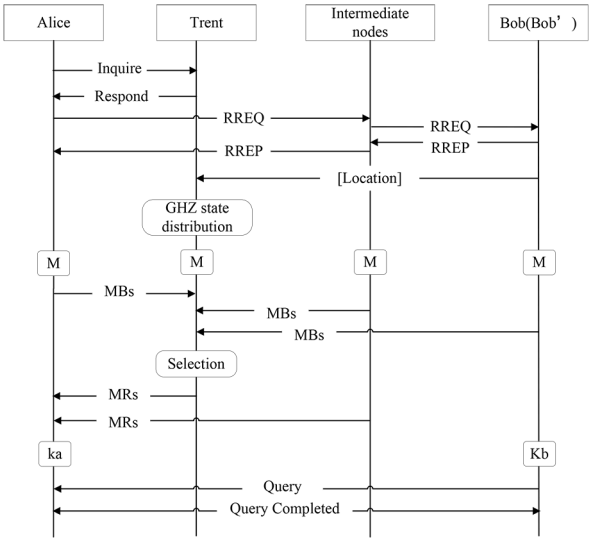


FIGURE 2. QWNPQ protocol with multiple third parties.

to query any database Bob(Bob') in a distance of the network, but she doesn't know his location or if they are within the same QBR's coverage. The entire process of the protocol is shown in Figure. 2.

1) Alice inquires of Trent the location information of the database Bob(Bob') and then Trent looks up the information in his HLR database. In response, Trent informs Alice whether Bob(Bob') is under the coverage of R1 or R2.
2) Once receiving the response information from Trent, Alice broadcasts a route request (RREQ) to her neighbor nodes and the RREQ eventually arrives at Bob(Bob') by the forwarding of a few intermediate nodes via classical wireless channels (CWCs). To search an appropriate path from Alice to Bob(Bob') with small routing overheads, an on-demand routing protocol [36] is initiated.
3) After the routing path is determined, Bob(Bob') sends a route reply (RREP) along the inverse path backward to the source node Alice. Meanwhile, Bob(Bob') will send to Trent a message that indicates the location of all nodes on the path.
4) According to the location of the database, Trent prepares multi-qubit GHZ states. If the database Alice wants to query is under the same route as her, in the position of Bob under R1, Trent prepares four-qubit GHZ states because four nodes including Alice, Bob, Trent and R1 are selected to participate in the query; if the database is under different route, in the position of Bob' under R2, then Trent prepares five-qubit GHZ states because the number of selected nodes is five, which include Alice, Bob', Trent, R1 and R2. The multi-qubit GHZ state required in our protocol is recorded as $|GHZ\rangle_{12\ldots n} = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes n} + |1\rangle^{\otimes n})$, where n denotes the number of involved nodes. Here, $n = 4$ when the database is Bob or $n = 5$ when the database is Bob'. Trent keeps his first particle and distributes the remaining particles to the relevant nodes, respectively.
5) After receiving the particles, the receivers declare which particles are not received successfully. All of the lost particles declared by all sides should be discarded. Because the entangled particles do not carry any private information, thereby they cannot obtain any benefit from cheating. Therefore, the protocol is completely loss tolerant. Then Trent and the receivers use decoy-state security check to ensure the secure distribution of entangled particles. If it is distributed securely, the protocol continues, otherwise the protocol is re-executed.
6) Alice, Bob(Bob') and the third-party intermediate nodes randomly select the X basis or Y basis to measure the particles in their hands, and record the selected measurement bases and the obtained measurement results.
7) Alice, Bob(Bob') and the third-party intermediate nodes except for Trent announce their own measurement bases. Based on the announced information of bases, Trent selects a GHZ state, for instance, the jth GHZ state, which is measured under the X basis by all parties. Trent announces his own measurement result of this GHZ state and secretly sends j to Alice. Simultaneously, he informs other intermediate nodes to also announce their own measurement results corresponding to this state, respectively.
8) According to the measurement results announced by these third parties and her own measurement result, Alice infers Bob's measurement result of this state. If the number of $|-x\rangle$ is even in the measurement results of all nodes except for Bob, it can be inferred that Bob's measurement result is $|+x\rangle$; if the number is odd, Bob's measurement result is $|-x\rangle$. Alice uses Bob's measurement of this state as her own key k_a, and Bob records all his measurement results as K_b.
9) When an N-bit database is concerned, Alice calculates $s = j - i$, and secretly sends s to Bob. Bob calculates $E_N = X_N \oplus K_{b-s}$, and sends E_N to Alice. At this time, Alice can use k_a to decrypt E_i and get X_i.

III. SECURITY ANALYSIS

In the protocol, only the user Alice and the database Bob have their own private information, the third parties do not have private information, who just assist the network private query to be successfully implemented. Alice and Bob do not trust the third parties. Therefore, in the security analysis, it is also necessary to analyze the third parties' attack on Alice and Bob's privacy. The third parties are not allowed to collude with either Alice or Bob. We will analyze the security of the proposed protocol from three aspects. First, the third parties' attack on Alice and Bob's privacy. Second, external attack. Finally, the attack between Alice and Bob.

A. THE THIRD PARTIES' ATTACK

1) THE THIRD-PARTY TRENT's FAKE ENTANGLED ATTACK

Trent prepares a fake entangled state in the form of $|\varphi\rangle_{AI_1I_2\ldots I_{n-3}} \otimes |\phi\rangle_{TB(B')}$ ($n = 4$ or $n = 5$). He keeps the first

particle and distributes the remaining particles to the involved nodes. For instance, Trent prepares and distributes the quantum state $|\Psi\rangle = |0\rangle_{AI_1I_2\ldots I_{n-3}}^{\otimes(n-2)} \otimes (|00\rangle + |11\rangle)_{TB(B')}/\sqrt{2}$. Subsequently, Trent does not directly measure the particles in his hands, but uses quantum memory devices to store them. After Bob announces his own measurement bases, he uses the same ones as Bob to measure the particles in his hands. Trent can obtain the measurement results associated with Bob(Bob'), according to the expansion equation under different measurement bases in the following Eq.(1),

$$\begin{aligned}&\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{TB(B')}\\ &= \frac{1}{\sqrt{2}}(|+x\rangle|+x\rangle + |-x\rangle|-x\rangle)_{TB(B')}\\ &= \frac{1}{\sqrt{2}}(|+y\rangle|-y\rangle + |-y\rangle|+y\rangle)_{TB(B')}. \end{aligned} \quad (1)$$

Trent can then use these associated measurement results to eavesdrop private information from Bob's database. As an example, Trent pretends to be Alice to send Bob the fake s', and makes him to use it to move his own measurement results, encrypt database X_N, and send E_N. At this time, Trent can decrypt E_N through his own measurement result to obtain the private information of the database. When Trent launches such an attack, the prepared quantum state is a dichotomic n-party entangled state, which is not a real n-party one. Therefore, decoy-state security check can be used to detect the quantum states shared by Alice, Bob and the third parties for resisting the fake entangled attack initiated by Trent. This technique is enlightened by BB84 QKD protocol, which has been proved to be unconditionally secure [7]. In this way, Trent cannot get Bob's privacy. For Alice's privacy, Trent cannot get it either, because he does not know s that Alice secretly sends to Bob.

2) THE OTHER THIRD-PARTY INTERMEDIATE NODES' ATTACK

Since they do not prepare and distribute quantum states, the attack mode of these intermediate nodes is different from Trent. Under a semi-trusted model, they simply record and announce their own measurement bases and results to assist in the successful completion of the query. Their cheating by announcing error measurement bases and results cannot bring them any benefit. Alice may get a wrong answer which will be found at a later time. Under a malicious model, they may conduct a Denial of Service attack in which one or more malignant parties simply wish to prevent message distribution, or simply the defective nodes that operate in good faith but incur failures beyond their control. If no bit survives at Alice's end finally, the protocol fails. Alice can request Trent to handle this issue and re-execute the protocol.

B. EXTERNAL ATTACK

In the stage of the GHZ state preparation and distribution, the external attack has no meaning because the GHZ particles at this point have not carried any privacy about Alice and Bob. Once the entanglement is securely distributed, external eavesdropper cannot reconstruct the unknown quantum information. Therefore, the security of quantum wired channels concerns the secure distribution of entangled particles. To resist the external attack on the channels, in step 5) we use decoy-state security check between the generator and the receiver. So the security against external attack is guaranteed.

C. INSIDE PARTICIPANT ATTACK

Since all the involved nodes randomly choose the X basis or Y basis to measure the particles in their hands, Alice can perform quantum memory attack. When Alice launches this attack, she does not directly measure the particles in her hands, but waits until Bob announces the measurement bases and uses the same ones as Bob to do the measurement. Nevertheless, without the assistance of the third-party intermediate nodes, Alice cannot infer Bob's measurement results from his own measurements. Moreover, there is no JM attack, because the number of database entries obtained by Alice can be controlled by Trent without being limited to one bit and then no post-processing is required.

Consequently, under the protection of the multi-qubit GHZ state's quantum correlation, Alice and Bob cannot obtain the privacy of each other. The protocol is secure.

IV. DISCUSSION AND CONCLUSION

A. DISCUSSION

1) CLASSICAL WIRELESS COMMUNICATION COST

Classical wireless communication cost is the number of the data transmission required in the scheme, which includes all the classical information transmitted by the involved nodes. Therefore, the cost of one query is the product of the number of data and the hop count that the information needs to be transmitted. The total cost is the sum of all the transmissions in the process of query. In our QWNPQ scheme, every node involved in the query except for Trent needs to announce their own measurement bases, which cost one c-bit respectively. In addition, every node except for Alice and Bob(Bob') needs to announce one c-bit measurement results to the destination node Alice respectively, thus the classical wireless communication cost of our scheme is $C = 1\times(n+1)+1\times\sum_{i=2}^{n-1} H_d^i = 1 \times (n+1) + 1 \times \sum_{i=2}^{n-1}(n-i) = \frac{1}{2}(n^2 - n + 4)$, where H_d^i denote the classical wireless communication hop number from the ith node to the destination node on quantum paths.

2) QUANTUM COMMUNICATION DELAY

The wireless communication and measurements can introduce extra delay in quantum communication, which includes wireless medium access delay, the transmission and propagation delay, node processing delay. The short delay is pursued because of the limited decoherence time in quantum memory and quality of service (QOS) need.

Hypothesize that each measurement delay is D_m seconds and each wireless communication delay is D_w seconds.

In the scheme, the measurement and the classical wireless communication at each node are performed simultaneously. Then the wireless communication delay is the time required from the farthest node to the destination node for one packet transmitted, since when the farthest node sends its classical information, the other related nodes can send theirs simultaneously without any mutual interference. Thus, the total quantum communication delay of our scheme is written as $D = D_m + D_w \times max\left\{H_d^i\right\}_b + D_w \times max\left\{H_d^i\right\}_r$, where $max\left\{H_d^i\right\}_b$ is the biggest hop number from the farthest node to the destination node Trent when the related nodes announce the information of bases, $max\left\{H_d^i\right\}_r$ is the biggest hop number from the farthest node to the destination node Alice when the related nodes announce their measurement results.

B. CONCLUSION

We have presented a novel QWNPQ with multiple third parties scheme, which uses a flexible bilayer network topology to ensure the rapid and secure private query. Our protocol inherits the good features as of previous point-to-point schemes, it is loss tolerant and robust against quantum memory attack. In addition, it has the following excellent features. With the help of the third parties, the protocol can determinately control the number of database entries Alice obtains from Bob, and Alice can directly gets the corresponding number of key bits at one time without post-processing. Compared with a single third party, multiple third parties make it more difficult for Alice to guess Bob's measurement results and better protect Bob's privacy. Further, since the number of key bits obtained by Alice can be controlled by the third-party without being limited to one bit and no post-processing is required, thus there is no JM attack. Moreover, under the protection of the multi-qubit GHZ state's quantum correlation, the privacy of Alice and Bob is protected from the third parties' fake entangled attack and external attack, and they cannot obtain the privacy of each other by taking quantum memory attack. The high security of our scheme is fully demonstrated. Our scheme is scalable and can be also used to wired or hybrid quantum networks. For the classical channels, programmable network architecture can be considered.

In the actual implementation of the protocol, the GHZ states generated and distributed by the generator will inevitably be affected by the noise inherent in the channels when transmitted through the quantum wired channels. However, this problem can be addressed by the quantum entanglement distillation method to keep the multi-qubit GHZ state the same as it generated.

REFERENCES

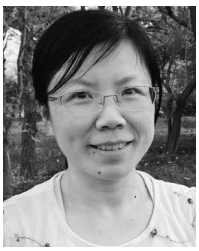
[1] Y. Gertner, Y. Ishai, E. Kushilevitz, and T. Malkin, "Protecting data privacy in private information retrieval schemes," *J. Comput. Syst. Sci.*, vol. 60, no. 3, pp. 592–629, 2000.
[2] H.-K. Lo, "Insecurity of quantum secure computations," *Phys. Rev. A, Gen. Phys.*, vol. 56, no. 2, p. 1154, 1997.
[3] V. Giovannetti, S. Lloyd, and L. Maccone, "Quantum private queries," *Phys. Rev. Lett.*, vol. 100, no. 23, 2008, Art. no. 230502.
[4] V. Giovannetti, S. Lloyd, and L. Maccone, "Quantum private queries: Security analysis," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3465–3477, Jul. 2010.
[5] L. Olejnik, "Secure quantum private information retrieval using phase-encoded queries," *Phys. Rev. A, Gen. Phys.*, vol. 84, no. 2, 2011, Art. no. 022313.
[6] M. Jakobi *et al.*, "Practical private database queries based on a quantum-key-distribution protocol," *Phys. Rev. A, Gen. Phys.*, vol. 83, no. 2, 2011, Art. no. 022301.
[7] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE Int. Conf. Comput., Syst. Signal Process.*, 1984, pp. 175–179.
[8] V. Scarani, A. Acin, G. Ribordy, and N. Gisin, "Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations," *Phys. Rev. Lett.*, vol. 92, no. 5, 2004, Art. no. 057901.
[9] F. Gao, B. Liu, Q.-Y. Wen, and H. Chen, "Flexible quantum private queries based on quantum key distribution," *Opt. Express*, vol. 20, no. 16, pp. 17411–17420, 2012.
[10] Y.-G. Yang, S.-J. Sun, P. Xu, and J. Tian, "Flexible protocol for quantum private query based on B92 protocol," *Quantum Inf. Process.*, vol. 13, no. 3, pp. 805–813, 2014.
[11] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," *Phys. Rev. Lett.*, vol. 68, no. 21, p. 3121, 1992.
[12] J.-L. Zhang, F.-Z. Guo, F. Gao, B. Liu, and Q.-Y. Wen, "Private database queries based on counterfactual quantum key distribution," *Phys. Rev. A, Gen. Phys.*, vol. 88, no. 2, 2013, Art. no. 022334.
[13] Y.-G. Yang, S. -J. Sun, J. Tian, and P. Xu, "Secure quantum private query with real-time security check," *Optik*, vol. 125, no. 19, pp. 5538–5541, 2014.
[14] C.-Y. Wei, F. Gao, Q.-Y. Wen, and T.-Y. Wang, "Practical quantum private query of blocks based on unbalanced-state Bennett-Brassard-1984 quantum-key-distribution protocol," *Sci. Rep.*, vol. 4, no. 4, 2014, Art. no. 7537.
[15] F. Yu and D. Qiu, "Coding-based quantum private database query using entanglement," *Quantum Inf. Comput.*, vol. 14, pp. 91–106, Jan. 2014.
[16] B. Liu, F. Gao, W. Huang, and Q. Wen, "QKD-based quantum private query without a failure probability," *Sci. China Phys., Mech. Astron.*, vol. 58, no. 10, 2015, Art. no. 100301.
[17] H. Lai, M. A. Orgun, J. Pieprzyk, J. Xiao, L. Xue, and Z. Jia, "Controllable quantum private queries using an entangled Fibonacci-sequence spiral source," *Phys. Lett. A*, vol. 379, nos. 40–41, pp. 2561–2568, 2015.
[18] Y.-G. Yang, M.-O. Zhang, and R. Yang, "Private database queries using one quantum state," *Quantum Inf. Process.*, vol. 14, no. 3, pp. 1017–1024, 2015.
[19] C.-Y. Wei, T.-Y. Wang, and F. Gao, "Practical quantum private query with better performance in resisting joint-measurement attack," *Phys. Rev. A, Gen. Phys.*, vol. 93, no. 4, 2016, Art. no. 042318.
[20] Y.-G. Yang *et al.*, "Quantum private query with perfect user privacy against a joint-measurement attack," *Phys. Lett. A*, vol. 380, no. 48, pp. 4033–4038, 2016.
[21] P. Chan, I. Lucio-Martinez, X. Mo, C. Simon, and W. Tittel, "Performing private database queries in a real-world environment using a quantum protocol," *Sci. Rep.*, vol. 4, Jun. 2014, Art. no. 5233.
[22] M. V. P. Rao and M. Jakobi, "Towards communication-efficient quantum oblivious key distribution," *Phys. Rev. A, Gen. Phys.*, vol. 87, no. 1, 2013, Art. no. 012331.
[23] F. Gao, B. Liu, W. Huang, and Q.-Y. Wen, "Postprocessing of the oblivious key in quantum private query," *IEEE J. Sel. Topics Quantum Electron.*, vol. 21, no. 3, May/Jun. 2014, Art. no. 6600111.
[24] Y.-G. Yang, Z.-C. Liu, X.-B. Chen, W.-F. Cao, Y.-H. Zhou, and W.-M. Shi, "Novel classical post-processing for quantum key distribution-based quantum private query," *Quantum Inf. Process.*, vol. 15, no. 9, pp. 3833–3840, 2016.
[25] Y. Yang, Z. Liu, X. Chen, Y. Zhou, and W. Shi, "Robust QKD-based private database queries based on alternative sequences of single-qubit measurements," *Sci. China Phys., Mech. Astron.*, vol. 60, no. 12, 2017, Art. no. 120311.
[26] S.-J. Sun, Y.-G. Yang, and M.-O. Zhang, "Relativistic quantum private database queries," *Quantum Inf. Process.*, vol. 14, no. 4, pp. 1443–1450, 2015.
[27] F. Yu, D. Qiu, H. Situ, X. Wang, and S. Long, "Enhancing user privacy in SARG04-based private database query protocols," *Quantum Inf. Process.*, vol. 14, no. 11, pp. 4201–4210, 2015.

[28] S.-W. Xu, Y. Sun, and S. Lin, *Quantum Private Query Based on Single-Photon Interference*. Norwell, MA, USA: Kluwer, 2016, pp. 1–10.
[29] L. Jian, Y.-G. Yang, X.-B. Chen, Y.-H. Zhou, and W.-M. Shi, "Practical quantum private database queries based on passive round-robin differential phase-shift quantum key distribution," *Sci. Rep.*, vol. 6, Aug. 2016, Art. no. 31738.
[30] L.-Y. Zhao *et al.*, "Loss-tolerant measurement-device-independent quantum private queries," *Sci. Rep.*, vol. 7, Jan. 2017, Art. no. 39733.
[31] A. Maitra, G. Paul, and S. Roy, "Device-independent quantum private query," *Phys. Rev. A, Gen. Phys.*, vol. 95, no. 4, 2017, Art. no. 042344.
[32] M. Xu, R.-H. Shi, Z.-Y. Luo, and Z.-W. Peng, "Nearest private query based on quantum oblivious key distribution," *Quantum Inf. Process.*, vol. 16, no. 12, p. 286, 2017.
[33] R.-H. Shi, Y. Mu, H. Zhong, J. Cui, and S. Zhang, "Privacy-preserving point-inclusion protocol for an arbitrary area based on phase-encoded quantum private query," *Quantum Inf. Process.*, vol. 16, no. 1, p. 8, Jan. 2017.
[34] C.-Y. Wei, X.-Q. Cai, B. Liu, T.-Y. Wang, and F. Gao, "A generic construction of quantum-oblivious-key-transfer-based private query with ideal database security and zero failure," *IEEE Trans. Comput.*, vol. 67, no. 1, pp. 2–8, Jan. 2018.
[35] J. Basak and S. Maitra, "Clauser–Horne–Shimony–Holt versus three-party pseudo-telepathy: On the optimal number of samples in device-independent quantum private query," *Quantum Inf. Process.*, vol. 17, no. 4, p. 77, 2018.
[36] J. Shen, H. Tan, J. Wang, J. Wang, and S. Lee, "A novel routing protocol providing good transmission reliability in underwater sensor networks," *J. Internet Technol.*, vol. 16, no. 1, pp. 171–178, 2015.

NA LI was born in Jilin, China, in 1982. She received the M.Eng. degree from the School of Computer Science and Technology, Changchun University of Science and Technology, Changchun, China, in 2011. She is currently pursuing the Ph.D. degree with the School of Computer, Beijing University of Posts and Telecommunications, Beijing, China. Her main research interests include information security, quantum secure communication, and quantum cryptography.

JIAN LI received the Ph.D. degree from the Beijing Institute of Technology, in 2005. He is currently a Professor with the School of Computer, Beijing University of Posts and Telecommunications, Beijing, China. His research interests include information security and quantum cryptography.

XIUBO CHEN received the Ph.D. degree from the Beijing University of Posts and Telecommunications, Beijing, China, in 2009, where she is currently an Associate Professor with the School of Cyberspace Security. Her research interests include cryptography, information security, quantum network coding, and quantum private communication.



YUGUANG YANG received the Ph.D. degree from the Beijing University of Posts and Telecommunications, in 2006. She is currently a Professor with the School of Computer, Beijing University of Technology, Beijing, China. Her research interests include cryptography and information security.