Practical Quantum Private Query with Classical Participants *

Min Xiao(肖敏)[1], Di-Fang Zhang(张弟芳)[2**]

[1]*Institute of Computer Forensics, Chongqing University of Posts and Telecommunications, Chongqing 400065*
[2]*College of Computer Science and Technology, Chongqing University of Posts and Telecommunications, Chongqing 400065*

(Received 17 November 2018)

Quantum key distribution (QKD)-based quantum private query (QPQ) is a practical application of QKD, which relaxes the security condition of perfectly concealing a private query to a cheating-sensitive strategy. We propose a QPQ protocol based on the delegated QKD scheme (DQKD-based QPQ), in which two almost 'classical' clients (data user and database owner) can establish a 1-out-of-N oblivious key with the help of a cloud server with full quantum ability. Concretely, the two classical participants in the DQKD-based QPQ only need to access the quantum channel and reorder qubits, and the costly quantum operations, quantum state preparation and measurement are outsourced to a full quantum server in the cloud without leaking participants' privacy. The proposed protocol not only provides a cloud-based framework of QKD-based QPQ, but also obtains better security by a real-time security check, which can protect the security of the database and user against all potential attacks even if the quantum server is assumed to be a powerfully untrusted adversary.

PACS: 03.67.Dd, 03.67.Pp, 03.67.Hk DOI: 10.1088/0256-307X/36/3/030301

Symmetrically private information retrieval (SPIR) was first introduced by Gertner *et al.*[1] and was known as 1-out-of-N oblivious transfer (OT), which protects participants' privacy against each other and outside eavesdroppers. With the emergence of quantum computing, quantum private query (QPQ), an extension of SPIR to quantum world, has attracted much attention. A secure SPIR needs to ensure database security (a data user, Alice, retrieves only a single element from a database of size N) and user privacy (the database owner, Bob, cannot learn which element was retrieved by Alice). However, Lo[2] proved that SPIR with perfect security does not exist even in the case of quantum computing. Therefore, many attempts have been carried out to construct practical schemes by allowing reasonable assumptions about the computational capabilities of the participants and security conditions.[3]

Based on the limited and noisy quantum storage model, Konig *et al.*[4] presented OT and bit commitment protocols with unconditional security. By relaxing the security condition from the perfectly concealing to a cheat-sensitive strategy,[5] plenty of practical QPQ protocols are proposed.[3,6−12] In 2011, Jakobi *et al.*[7] used quantum key distribution (QKD) (SARG04[13]) to design a QPQ protocol (J-protocol), which only changes the post-processing of the QKD scheme and is characterized by practical feasibility, transmission loss tolerance and scalability to large databases. The no-signaling principle ensures the cheat-sensitive nature for user privacy. Although the database privacy is not perfect, the user's accessible information is restricted to a well-defined small percentage of the database elements. After that, many works are presented to improve the J-protocol from various directions, such as a more flexible and controllable version[8] of the J-protocol, enhancement of user privacy,[9,11] real-time security checks,[10] noise tolerance[3,12] and database security.[14]

Considering that there are still technological and commercial challenges to deploy a large-scale quantum computing world in practice, the user with limited quantum resources has become a common assumption in a lot of quantum communication and quantum computing research. The most representative works are the semi-quantum model and the outsourcing quantum computation model. A participant with semi-quantum[15] ability is limited to possessing no more than the following four capabilities: (1) accessing the quantum channel, (2) measuring the qubit in the computational base, (3) preparing qubits in the computational base, (4) reordering qubits. Yang *et al.*[16] integrated the idea of semi-quantum key distribution into QPQ, in which the data user only needs to prepare and measure qubits in the computational base. Delegated quantum computation (DQC)[17] and blind quantum computation (BQC)[18] are two typical outsourcing quantum computation models, which can be perceived as an extension of cloud computation to the quantum world and which permit a client with limited quantum ability to delegate her quantum computation tasks to powerful quantum servers while preserving the client's privacy. Based on the BQC model, Sun *et al.*[19] proposed a QPQ protocol between a query user and a full-quantum database server, in which the query user only does measurements.

In this Letter, the technology of delegated QKD (DQKD) is used to design a practical QPQ (DQKD-

*Supported by the National Key R&D Program of China under Grant No 2017YFB0802300, and the Foundation Science and Forefront Technology of Chongqing Science and Technology Commission of China under Grant No cstc2016jcyjA0571.
**Corresponding author. Email: S160201077@stu.cqupt.edu.cn

based QPQ) protocol in a cloud computing scenario, where the data user and database owner are both almost 'classical'. With the help of the quantum server, any clients (data owners or users) can securely share or retrieve data by portable devices anywhere and anytime. The research of QKD has been developed over more than 30 years and some experimental efforts[20,21] have been presented. This demonstrates that QKD will be a new practical technology with huge potential in the near future. Therefore, compared with other QPQ protocols, the QKD-based QPQ scheme may be more practical.

There are three types of participants in the proposed protocol: a database owner Bob, a data user Alice and a quantum server Charlie, where Alice and Bob are nearly classical, and Charlie possesses full quantum ability and acts as a cloud server which provides a costly quantum computing service. With the help of the cloud server, Alice retrieves an element in a database of size N held by Bob, while protecting their privacy against outside eavesdroppers and each other. To make the protocol more practical, we assume that Charlie is untrusted and will try his best to find as much secret information as possible. The protocol proceeds as follows: Step 1: Alice and Bob initiate a session of database private query and agree with the security parameter k and error rate t. Meanwhile, they also agree on a coding rule: the states $|0\rangle$ and $|1\rangle$ code for 0, and $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and $|-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$ represent bit 1.

Step 2: Bob requests Charlie to prepare a large enough qubit sequence S, in which each state is randomly and uniformly distributed over the set of the four possible states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. Then, Charlie publishes the states of the sequence S and sends S to Bob.

Step 3: For successfully received qubits, Bob records the announced states and uses the delay line to reorder them. Then, he randomly decides whether each of them is used for security detection or not. The security detection qubits form a detection sequence $S_{\rm D}$ and the remaining half of qubits form sequence $S_{\rm T}$. Finally, Bob sends the sequence $S_{\rm D}$ and $S_{\rm T}$ to Charlie and Alice, respectively.

Step 4: Charlie announces in which instance he has successfully received the qubit and then Bob informs Charlie of the correct measurement bases. Charlie performs measurements on these received qubits and announces the results. By comparing the results with the corresponding initial states announced by Charlie in step 2, Bob computes the error rate $\gamma = 1 - \frac{r}{q}$, where q is the total number of detection qubits, and r is the number of qubits confirmed as correct. If the error rate is higher than the predefined threshold value t, the protocol aborts.

Step 5: At the same time, Alice randomly reorders all received qubits and sends them to Charlie. Charlie announces in which instance he has received the qubit and Alice records these positions.

Step 6: After Bob declares that the security detection in step 4 is successful, Alice randomly chooses measurement bases $Z = \{|0\rangle, |1\rangle\}$ or $X = \{|+\rangle, |-\rangle\}$ and informs Charlie to measure all received qubits. Then, Charlie announces the measurement results and Alice rearranges these measurement results to recover their original orders in the sequence $S_{\rm T}$. The recovered sequence is denoted as $S_{\rm M}$, and its length should be no less than $2kN$. After that, Alice also tells Bob in which positions she has received the measurement results. As the J-protocol, the protocol is completely loss-independent, because Alice does not know the correct positions of the particles she holds in the original sequence S and she has no information on the sent bit value until now.

Step 7: Alice randomly chooses half of the positions in $S_{\rm M}$ and requests Bob to publish the corresponding initial states, then she compares Bob's announcement with the corresponding measurement result one by one and computes the error rate as in step 4. If the error rate is higher than the predefined threshold value t, the protocol aborts.

Step 8: Up to now, the state of the proposed protocol is exactly the same as the initial state in step 4 of the J-protocol in Ref. [7]. Therefore, the remaining procedures of the proposed protocol are to implement step 4 through step 8 of the J-protocol.

Without loss of generality, in mutually untrusted multi-party communications, the participants have more advantages than outside eavesdroppers. Therefore, the attacks from outside eavesdroppers can be grouped into attacks which are performed by the participants and we can assume that there is no outside eavesdroppers. To realize a secure QPQ protocol, two security requirements, database security and query user's privacy, need to be satisfied simultaneously. For the database security, there are two typical attacks from Charlie and Alice, respectively. Charlie may perform a malicious attack by preparing the deliberately designed resource state instead of that required by the client. At the same time, Alice may be curious about the database and may perform an optimal unambiguous state discrimination (USD) measurement attack or a joint measurement (JM) attack. Similarly, for the query user's privacy, the main attack sources are Charlie and Bob. Charlie may perform an improper measurement attack and Bob may prepare the intended entangled state or intermediate state. Note that in the proposed protocol, Alice and Bob are limited to being classical and cannot perform quantum attacks on their own unless Charlie helps them. Therefore, the attacks from Alice (Bob) discussed later are implemented by Alice (Bob) and Charlie in collaboration, and collusion attacks are not discussed separately. Next, we analyze all potential security threats from the three participants respectively and demonstrate that the proposed protocol can resist these attacks.

In our scheme, the untrusted server Charlie with full quantum ability prepares the necessary quantum resources and performs the measurements required by Alice or Bob. Generally, for eavesdropping privacy information, Charlie may prepare the quantum resources he wants instead of those the client requires, and perform his intended operations instead of those announced by Bob and Alice. Therefore, the check mechanism must be set to impede the undesired behaviors of Charlie. In addition, we think that there may exist a constraint of business reputation because the quality of service is the cornerstone of his business success and any cheating by Charlie may ruin his reputation as a service provider. Based on the above discussion, our analysis shows that the proposed protocol is still secure even if Charlie is untrusted.

In step 2, Charlie may prepare any states he wants instead of those he announces. One simple attack is that Charlie prepares a qubit sequence whose distribution is not random and uniform over the set of four possible states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, such as a sequence with particles in the same state. In this setting, to avoid his behavior being discovered directly, Charlie would not declare the actual quantum states. Thus there is inconsistency between his announcement and the actual particle state. In the security detection of step 4, the position of the detection particles is completely random from the view of Charlie, and thus Charlie can only correctly guess the state consistent in step 2 with probability $\frac{1}{2}$. Consequently, combined with the channel loss and noise, the error rate will be very high (more than $\frac{1}{2}$) and the protocol will abort.

As pointed out in Ref. [7], a more complex attack is that Charlie prepares the entangled state of two qubits $|\psi\rangle_{\rm BC} = \frac{1}{\sqrt{2}}(|0\rangle|R_0\rangle + |1\rangle|R_1\rangle)_{\rm BC}$ or $|\psi\rangle_{\rm BC} = \frac{1}{\sqrt{2}}(|+\rangle|R_0\rangle + |-\rangle|R_1\rangle)_{\rm BC}$ instead of a single qubit in step 2, where the first qubit B is sent to Bob and the second qubit C is kept in his quantum register (with $\langle R_0|R_1\rangle = 0$). In this setting, the first qubit is in the superposition state and Charlie can only announce one of two possible states. In the security detection of step 4, Charlie will measure the detection particles in the bases consistent with his announcement. Consequently, Charlie can send back the correct response to Bob with the probability $\frac{1}{2}$. Like the above simple attack, a high error rate will induce the protocol to abort. In addition, since Charlie does not know which particles are used for security detection or information encoding, he will obtain no information from the second particles.

In the proposed protocol, due to the security detection in step 7, all delay measurement attacks in Ref. [14], such as USD measurement attacks and JM attacks, are impossible for Charlie. When Charlie performs the measurement in step 6, he does not know the correct position of each particle due to the first security detection in step 2 and particle rearrangement by Alice in step 5. Furthermore, he also does not know which particles will be used to detect security or encode information in the following step 7. Therefore, Charlie cannot obtain extra information by his intended measurements. Moreover, an improper measurement will be detected in step 7 due to the high error rate.

In conclusion, it is impossible for Charlie to obtain the oblivious transfer key by sending the fake states or postponing the measurements. Moreover, the too high failure rate of the protocol will have a serious negative effect on his reputation and put Charlie at risk of business failure.

Malicious query user Alice always wants to obtain as many as possible bits about the raw key $K^{\rm r}$ by various intended measurements. In the following we analyze the database security against all kinds of potential attacks performed by Alice with the help of Charlie.

Table 1. The error rate incurred by intermediate state attack.

Initial state	$\|0'\rangle$				$\|1'\rangle$			
Measurement base in step (6)	Z		X		Z		X	
Measurement result in step (6)	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$
The probability of corresponding result	$\cos^2\frac{\pi}{8}$	$\sin^2\frac{\pi}{8}$	$\frac{1}{2}(\sin\frac{\pi}{8}+\cos\frac{\pi}{8})^2$	$\frac{1}{2}(\cos\frac{\pi}{8}-\sin\frac{\pi}{8})^2$	$\sin^2\frac{\pi}{8}$	$\cos^2\frac{\pi}{8}$	$\frac{1}{2}(\cos\frac{\pi}{8}-\sin\frac{\pi}{8})^2$	$\frac{1}{2}(\sin\frac{\pi}{8}+\cos\frac{\pi}{8})^2$
Bob's announcement	$\|0\rangle$		$\|+\rangle$		$\|1\rangle$		$\|-\rangle$	
Error rate	$\sin^2\frac{\pi}{8}$		$\frac{1}{2}(\cos\frac{\pi}{8}-\sin\frac{\pi}{8})^2$		$\sin^2\frac{\pi}{8}$		$\frac{1}{2}(\cos\frac{\pi}{8}-\sin\frac{\pi}{8})^2$	

As analyzed in Ref. [7], Alice can perform the USD measurement after Bob has announced the state pair (indicating the actual initial state) to discriminate two non-orthogonal states with higher success probability than by direct measurement. For the two equally likely states, the success probability of the USD measurement is bounded by $p^{\rm USD} = 1 - F(p_0, p_1)$, where $F(p_0, p_1)$ is the fidelity between the two quantum states one seeks to discriminate. In the proposed scheme, Alice can perform a USD measurement attack by the following strategy. In step 6, without any required measurements on Charlie's side, then Alice can request Bob to publish the initial states of detection particles and falsely claim that the security detection is successful. Subsequently, Alice directly requests Bob to publish the state pair for deducing the raw key. After that, Alice informs Charlie to perform USD measurement on all particles and send back the measurement results to her. Alice detects the honesty of Charlie by comparing Bob's announce-

ment with the measurement result on the detection particles and keeps the remaining measurement results for state discrimination analysis. Apparently, by the above strategy, Alice cannot obtain more advantages than the general USD measurement. Therefore, our scheme is as secure as the J-protocol under USD measurement attack. Moreover, by calculating, in Ref. [7], the authors have concluded that USD measurement can obtain only a small gain compared to the direct measurement and the risk of disclosing a raw key to Alice will not substantially increase, thus the security of Bob's database is not compromised.

Wei *et al.*[14] pointed out that to implement a JM attack, Alice must hold two essential elements simultaneously: the carrier states and the information about which carrier states contribute to one final key bit. In our protocol, Charlie holds all states and performs the measurement, but he does not know which states are the carrier states; on the contrary, Alice knows which carrier states contribute to one final key bit, but she only has classical ability and cannot measure the carrier states. Therefore, neither Charlie nor Alice can implement a JM attack individually. If Alice wants to execute the JM attack, she has to inform Charlie of which states will contribute to the one final key bit; apparently, this will put Alice at risk of leaking his query privacy. Therefore, the proposed protocol is immune to JM attack.

Dishonest database owner Bob always wants to infer Alice's retrieval address by deliberate state preparation, such as preparing an intermediate state or Bell state. In the proposed scheme, Bob is also limited to being classical and has no capability to prepare the initial quantum state. Therefore, Bob cannot launch an effective attack on his own unless Charlie can help him. In the J-protocol, user privacy is pursued in a cheat-sensitive manner. That is to say, dishonest Bob will run the risk of being discovered if he tries to obtain Alice's key information. The following analysis shows that the proposed protocol is also cheat-sensitive when Bob launches possible attacks with the help of Charlie.

In the J-protocol, Bob can prepare the exactly intermediate states $|0'\rangle$ or ($|1'\rangle$) between $|0\rangle$ and $|+\rangle$ or ($|1\rangle$ and $|-\rangle$) and announce the state pair $\{|0\rangle, |+\rangle\}$ in the key inference phase, here

$$\begin{aligned}|0'\rangle &= \cos\frac{\pi}{8}|0\rangle + \sin\frac{\pi}{8}|1\rangle \\ &= \frac{1}{\sqrt{2}}(\cos\frac{\pi}{8} + \sin\frac{\pi}{8})|+\rangle \\ &\quad + \frac{1}{\sqrt{2}}(\cos\frac{\pi}{8} - \sin\frac{\pi}{8})|-\rangle, \qquad (1)\\ |1'\rangle &= \sin\frac{\pi}{8}|0\rangle - \cos\frac{\pi}{8}|1\rangle \\ &= \frac{1}{\sqrt{2}}(\sin\frac{\pi}{8} - \cos\frac{\pi}{8})|+\rangle \\ &\quad + \frac{1}{\sqrt{2}}(\sin\frac{\pi}{8} + \cos\frac{\pi}{8})|-\rangle. \qquad (2)\end{aligned}$$

In Ref. [7], by the attack, Bob can bias the probability of conclusive results for Alice continuously between $p_c = \frac{1}{2}\sin^2\frac{\pi}{8} + \frac{1}{4}(\cos\frac{\pi}{8} - \sin\frac{\pi}{8})^2 = 0.1464$ and $1 - p_c = 0.8536$. The formula $\frac{1}{2}\sin^2\frac{\pi}{8}$ dedicates the probability that Alice obtains the conclusive 0 and $\frac{1}{4}(\cos\frac{\pi}{8} - \sin\frac{\pi}{8})^2$ is the probability that Alice obtains the conclusive 1. Apparently, we have $\frac{1}{2}\sin^2\frac{\pi}{8} = \frac{1}{4}(\cos\frac{\pi}{8} - \sin\frac{\pi}{8})^2$. That is to say, Bob may be more convinced that Alice will obtain a conclusive result on a qubit, but can only guess the bit value of the result at random. This situation will introduce error and Bob's cheating can subsequently be detected by Alice.

In the proposed protocol, with the help of Charlie, Bob can implement an intermediate state attack by the following strategy. In step 2, Bob requires Charlie to prepare particles which may be randomly in $\{|0'\rangle, |1'\rangle\}$. The protocol can run as the original protocol from step 1 to step 6. Due to Alice randomly reordering all received particles in step 5, Bob cannot obtain more information about the measurement bases and results in step 6 than a random guess. Therefore, in step 7, to keep the secret of the intermediate state from Alice, Bob will randomly announce $|0\rangle$ or $|+\rangle$ if the initial state is $|0'\rangle$, otherwise, he will randomly announce $|1\rangle$ or $|-\rangle$. According to Eqs. (1) and (2), Table 1 demonstrates that Bob's behavior will introduce error into the system inevitably and incur a high error rate; consequently, the protocol aborts. Moreover, even if Bob is lucky enough to pass the second security detection, the proposed protocol under the attack is as secure as the J-protocol, since the subsequent process is to perform steps 4–8 of the J-protocol.

In the J-protocol, Bob also can prepare entangled states

$$\begin{aligned}|\psi\rangle_{AB} &= \frac{1}{\sqrt{2}}(|0\rangle|R_0\rangle + |+\rangle|R_1\rangle)_{AB} \\ &= \frac{1}{\sqrt{2}}(\frac{1}{\sqrt{2}}(|0\rangle + |+\rangle)|R_+\rangle \\ &\quad + \frac{1}{\sqrt{2}}(|0\rangle - |+\rangle)|R_-\rangle)_{AB}, \qquad (3)\end{aligned}$$

where $\langle R_0|R_1\rangle = 0$, $|R_+\rangle = \frac{1}{\sqrt{2}}(|R_0\rangle + |R_1\rangle)$ and $|R_-\rangle = \frac{1}{\sqrt{2}}(|R_0\rangle - |R_1\rangle)$. Then, Bob sends the first particles to Alice and stores the second particles in his quantum memory. In the key inference phase, Bob announces the state pair $\{|0\rangle, |+\rangle\}$. After Alice has successfully measured the received qubits, Bob can measure the second particles B in the basis $\{|R_0\rangle, |R_1\rangle\}$ for recovering the sent bit value or in the basis $\{|R_+\rangle, |R_-\rangle\}$ for gaining some information on the conclusive result of Alice. In Ref. [7], they have demonstrated that the two objects cannot be achieved simultaneously.

In the proposed protocol, we assume that Bob and Charlie previously consult about the entangled state preparation and announcement, then the strategy that Bob uses to perform the attack is as fol-

lows. First, in the particle preparation, Bob may require Charlie to generate a two-particle entangled state $|\psi\rangle_{AB}$; for each entangled state, Charlie stores the second particle B in his quantum memory and sends the first particle A to Bob. Secondly, when receiving a particle A, Bob randomly decides whether it is used for security detection or not, then he sends all detection particles to Charlie and the remaining particles to Alice. Thirdly, Bob randomly chooses a measurement base $\{|R_0\rangle, |R_1\rangle\}$, $\{|R_+\rangle, |R_-\rangle\}$ and requires Charlie to measure all B particles in the designed bases. Subsequently, based on the measurement results and Eq. (3), Bob determines the correct measurement bases and informs Charlie to measure all detection particles in the correct bases. After the first security detection is successful and the measurement is implemented on Alice's side, Bob announces the initial state of the detection particle A, and the second security detection is performed based on the following rule: if the measurement base of the particle B is $\{|R_0\rangle, |R_1\rangle\}$, Bob can give a certain answer; if not, according to Eq. (3), he randomly selects $|0\rangle$ or $|+\rangle$ to publish. Apparently, the latter will introduce error and may make the protocol abort. If the second security detection is successful, the effect of the attack on the system security is the same as in the J-protocol.

Table 2. Comparisons with some existing QPQ protocols. Note that C represents classical ability, and Q denotes full quantum ability.

	Bob and Alice's ability	Resisting JM attack	Real-time security
Ref. [7]	Q–Q	No	No
Ref. [8]	Q–Q	No	No
Ref. [10]	Q–Q	No	Yes
Ref. [14]	Q–C	Yes	No
Ref. [16]	Q–C	Yes	No
Our protocol	C–C	Yes	Yes

Table 2 shows that, compared with similar existing QPQ schemes,[7,8,10,14,16] the proposed protocol has the following advantages in participants' quantum ability requirements and security. (1) Lightweight and almost classical participants of QPQ. Using the technology of the delegated QKD in the proposed scheme, the costly quantum computing tasks are delegated to a server with full quantum ability and the participating parties of QPQ are both almost classical and lightweight. This is undoubtedly very important for the current situation where quantum computing is very expensive and mobile devices are increasingly becoming an essential part of human life.[22] (2) Stronger database security. The proposed scheme can resist not only outside attacks, but also internal attacks even if the quantum server is untrusted and Alice colludes with the quantum server. Thus, compared with some protocols, the proposed protocol provides stronger database security. (3) Real-time security checks. The security check procedures in steps 4 and 7 can detect potential attacks in real time, especially any dishonest behaviors of the untrusted server.

Cloud computing is becoming increasingly popular since it offers users economical, effective and convenient access to information resources. Rationally, this convenient lifestyle may remain even with the rise of quantum computing. Therefore, it is of practical significance to research cloud-style quantum computing. In this study, we propose a cloud computing-based QPQ protocol, in which any two almost classical clients can securely share secret information with the help of a quantum server. In particular, even if the cloud server is untrusted, the proposed protocol can protect the participants' privacy. In addition, by replacing the quantum states with the resource states in Ref. [8], the proposed protocol can also flexibly control and adjust the privacy degree of the database and user. Our proposed scheme not only extends the QKD-based QPQ protocol to cloud computing mode, but also obtains other advantages, including real-time security checks and stronger resistance to internal and external attacks. In the future, it will be possible to improve communication efficiency and fault tolerance by more practical QKD technology.

References

[1] Gertner Y et al 2000 *J. Comput. Syst. Sci.* **60** 592
[2] Lo H K 1997 *Phys. Rev. A* **56** 1154
[3] Chan P et al 2015 *Sci. Rep.* **4** 5233
[4] Konig R et al 2012 *IEEE Trans. Inf. Theory* **58** 1962
[5] Hardy L and Kent A 2004 *Phys. Rev. Lett.* **92** 157901
[6] Giovannetti V et al 2008 *Phys. Rev. Lett.* **100** 230502
[7] Jakobi M et al 2011 *Phys. Rev. A* **83** 022301
[8] Gao F et al 2012 *Opt. Express* **20** 17411
[9] Maitra A et al 2017 *Phys. Rev. A* **95** 042344
[10] Yang Y G et al 2014 *Optik* **125** 5538
[11] Yu F et al 2015 *Quantum Inf. Process.* **14** 4201
[12] Wang T Y et al 2016 *Int. J. Theor. Phys.* **55** 3309
[13] Scarani V et al 2004 *Phys. Rev. Lett.* **92** 057901
[14] Wei C Y et al 2016 *Phys. Rev. A* **93** 042318
[15] Boyer M et al 2007 *Phys. Rev. Lett.* **99** 140501
[16] Yang Y G et al 2015 *Quantum Inf. Process.* **14** 1017
[17] Dunjko V et al 2014 *20th International Conference on the Theory, Application of Cryptology, Information Security* (Kaoshiung December 7–11 2014) p 406
[18] Dunjko V et al 2012 *Phys. Rev. Lett.* **108** 200502
[19] Sun Z et al 2015 *Phys. Rev. A* **91** 052303
[20] Wang S et al 2012 *Opt. Lett.* **37** 1008
[21] Wang S et al 2015 *Nat. Photon.* **9** 832
[22] Dinh H T et al 2013 *Wireless Commun. Mobile Comput.* **13** 1587