SCIENTIFIC REPORTS

OPEN

Loss-tolerant measurement-device-independent quantum private queries

Received: 11 August 2016
Accepted: 28 November 2016
Published: 04 January 2017

Liang-Yuan Zhao[1,2], Zhen-Qiang Yin[1,2], Wei Chen[1,2], Yong-Jun Qian[1,2], Chun-Mei Zhang[1,2,†,‡], Guang-Can Guo[1,2] & Zheng-Fu Han[1,2]

Quantum private queries (QPQ) is an important cryptography protocol aiming to protect both the user's and database's privacy when the database is queried privately. Recently, a variety of practical QPQ protocols based on quantum key distribution (QKD) have been proposed. However, for QKD-based QPQ the user's imperfect detectors can be subjected to some detector- side-channel attacks launched by the dishonest owner of the database. Here, we present a simple example that shows how the detector-blinding attack can damage the security of QKD-based QPQ completely. To remove all the known and unknown detector side channels, we propose a solution of measurement-device-independent QPQ (MDI-QPQ) with single- photon sources. The security of the proposed protocol has been analyzed under some typical attacks. Moreover, we prove that its security is completely loss independent. The results show that practical QPQ will remain the same degree of privacy as before even with seriously uncharacterized detectors.

An ideal symmetrically private information retrieval (SPIR) protocol[1] allows a user, e.g. Alice, to extract an item of a database without revealing any information about which one she has retrieved to the database owner, e.g. Bob (*perfect user privacy*). Meanwhile, Alice can obtain only one item in a single query (*perfect database privacy*). SPIR can be used in the internet search and online transactions for the valuable and sensitive information. A SPIR protocol is a 1-out-of-N oblivious transfer (OT) protocol essentially[2]. In the 1-out-of-N OT, Bob sends N bits and Alice chooses which one she obtains. At the end of the protocol Alice knows the chosen bit value but has no information about other bits, while Bob is entirely ignorant of which bit Alice received. The security of classical OT relies on the unproven computational assumptions[1]. Unfortunately, Lo has proven that quantum mechanics along cannot provide unconditionally secure perfect quantum OT either[3]. This implies the impossibility of perfect quantum SPIR. It can be concluded from Lo's proof that if a quantum SPIR has perfect user privacy, then Alice can perform an Einstein-Podolsky-Rosen-type[4] attack to access the entire database without being detected.

Despite the no-go theorem about ideal quantum SPIR, some interesting degree of security can be achieved with changes in the model or the security requirements of the protocol. The first attempt of combining the quantum mechanics with SPIR was made by Kerenidis and De Wolf[5]. However, in their protocol, the database is replicated over more than one owner and it preserves database privacy against only honest user. In 2008, Giovannetti, Lloyd and Maccone proposed a cheat sensitive quantum protocol (GLM08 protocol), named quantum private queries (QPQ), to solve the SPIR problem[6]. The term cheat sensitive means that Alice can catch Bob cheating with a nonvanishing (but nonunity) probability if Bob attempts to learn what Alice queries. The imperfect user privacy is the reason that QPQ can evade the no-go proof of Lo[3]. The security of GLM08 has been analyzed strictly[7] and a proof-of-principle experiment has been implemented by De Martini *et al.*[8]. In the experiment, the bits of database were represented by an array of half-wave plates. If there existed a half-wave plate in one spatial mode, it meant that the corresponding bit was 1. Otherwise the bit was 0. For the user Alice, she prepared two non-orthogonal polarized states (the query state and test state), and sent them to Bob in a random order. The query state was

[1]Key Laboratory of Quantum Information, University of Science and Technology of China, CAS, Hefei, 230026, China. [2]Synergetic Innovation Center of Quantum Information & Quantum Physics, University of Science and Technology of China, Hefei, 230026, China. †Present address: Institute of Signal Processing and Transmission, Nanjing University of Posts and Telecommunications, Nanjing 210003, China. ‡Present address: Key Lab of Broadband Wireless Communication and Sensor Network Technology, Nanjing University of Posts and Telecommunications, Ministry of Education, Nanjing 210003, China. Correspondence and requests for materials should be addressed to Z.-Q.Y. (email: yinzq@ustc.edu.cn)

routed into the desired spatial mode to obtain the retrieved bit value. Combining this value with the test state, Alice could verify the honesty of Bob with a certain probability.

The advantage of GLM08 and its improved version[9] is that the communication and computational complexity has been reduced exponentially. However, the security of the protocols may be seriously compromised in the presence of losses and it will be difficult to retrieve when the dimension of the database is large. In 2011, Jakobi *et al.*[10] proposed a QPQ protocol ($\mathrm{J}^{+}11$ protocol) based on the Scarani-Acin-Ribordy-Gisin 2004 (SARG04) quantum key distribution (QKD) protocol[11]. $\mathrm{J}^{+}11$ is completely impervious to losses and can be easily implemented for large database with mature QKD technology. By adjusting the coefficients of the sent states, Gao *et al.* made the $\mathrm{J}^{+}11$ flexible for either better user privacy or better database privacy ($\mathrm{G}^{+}12$ protocol)[12]. Referring to the two-way QKD scheme, the QPQ has been designed to perform better in resisting the joint-measurement attack[13]. The QKD-based QPQ is a very practical solution and has been generalized with other QKD protocols[14–16]. The first experimental demonstration of $\mathrm{J}^{+}11$ and $\mathrm{G}^{+}12$ has been done on a QKD system[17] with some necessary modifications by Chan *et al.*[18]. In their experiment, four polarized states from two orthonormal bases were prepared randomly by Bob using the phase-randomized weak coherent state (PR-WCS) source. The faint laser pulses were transmitted to Alice trough a 12.4 km dark fiber with sequences of strong light, which acted as quantum frames[17] to synchronize and compensate the time shift. Alice measured the faint pulses by passively selecting one of the bases randomly. After the classical postprocessing, including Bob announcing pairs of non-orthogonal states, key compression and error correction, Alice performed a total of 11 queries at the single-photon level. This experiment shows the feasibility of QKD-based QPQ with state-of-the-art technology. Note that the novel error-correcting code developed by Chan *et al.*[18] and another one by Gao *et al.*[19] to address the noise in the channel can protect the privacy of both parties. As the above QPQ protocols focused mainly on retrieving a single bit, multi-bit block QPQ has been proposed[20,21], in which Alice could obtain several desired bits by just one query. Nevertheless, we still focus on the single-bit QPQ protocols in this paper for there are still many problems needed to be solved.

Note that the quantum processes of the $\mathrm{J}^{+}11$ have no difference from the implementation of SARG04 QKD. The practical security loopholes[22,23], especially the detector side channels[24–26], in QKD may still exist in practical $\mathrm{J}^{+}11$ system, which could damage the security of the system. In the following, we will give a strategy of detector-blinding attack on the practical $\mathrm{J}^{+}11$ and $\mathrm{G}^{+}12$ systems and show how it breaks the user privacy completely. To remove all the known and unknown detector-side-channel attacks launched by dishonest Bob, we propose a measurement-device-independent QPQ (MDI-QPQ) protocol with single-photon sources. MDI-QPQ benefits from the idea of MDI-QKD[27–36] and enriches the application of the MDI paradigm in the mistrustful quantum cryptography[37]. Moreover, the security of our protocol is loss-tolerant.

In MDI-QKD, the detector side channels are removed by using the Bell state measurement (BSM) conducted by an untrusted third party. The two legitimate parties need only to know their state preparations. MDI-QPQ is similar to MDI-QKD in that Alice and Bob also need to characterize only their state prepare processes. A slight difference is that the BSM is played by Alice because there is no third party here. Nevertheless, Alice needs only to obtain a Bell state outcome from her measurement device, but does not have to characterize it anymore. Thus, the idea of MDI-QKD can be modified to defend a dishonest Bob's detector-side-channel attacks in MDI-QPQ. However, note that the untrusted measurement device is now in Alice's laboratory, which is different from MDI-QKD. We emphasize that Alice should protect the classical information of her state preparations from leakage to both the measurement device and Bob. Considering that, we must be careful when adapting the MDI paradigm into the mistrustful quantum cryptography where the legitimate parties do not trust each other.

Results

The principle of detector-blinding attack on the practical QKD-based QPQ systems. To demonstrate that the detector side channels do exit in previous practical QKD-based QPQ systems, let us take the detector-blinding attack as an example. We first briefly review the basic ingredients of the $\mathrm{J}^{+}11$ protocol. In the $\mathrm{J}^{+}11$ protocol, four qubits from two mutually unbiased bases, e.g., the rectilinear basis $\{|0\rangle, |1\rangle\}$ and the diagonal basis $\{|+\rangle, |-\rangle\}$, are sent randomly from Bob to Alice. Here, $|0\rangle$ and $|1\rangle$ represent the horizontal and vertical polarization states, $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, respectively. The rectilinear basis stands for the raw key bit 0 and the diagonal basis refers to the raw key bit 1. Alice measures the states in the two bases randomly. For each of the successfully detected photons, Bob tells Alice two states which are composed of the actually sent state and a random one from the other basis. Combining with her measurement result, Alice can decode the raw key bit certainly with probability $\frac{1}{4}$. Then, the raw key are divided into several substrings by Bob with the length equaling to the database and are added bitwise to generate the final key. Ideally, Alice will know only one final key and Bob has no information of its position. Alice computes the position difference between the known final key and her desired element of the database, and announces it to Bob. Bob shifts the final key according to the difference value and encrypts the database. At last, Alice can obtain that element from the encrypted database privately with the known final key.

Seeing the quantum processes of $\mathrm{J}^{+}11$ are the same with SARG04 QKD, we find that the principle of the detector-blinding attack on practical $\mathrm{J}^{+}11$ system is similar to the one in QKD[26,38] with changes only in the classical postprocesses. For definiteness, let Alice chooses the bases actively with two single-photon detectors. Assume that in classical linear mode, the detector $i \in \{1, 2\}$ always clicks from a trigger pulse with optical peak power $\geq p_{\mathrm{always},i}$, and never clicks from a trigger pulse with optical peak power $\leq p_{\mathrm{never},i}$. A perfect detector-blinding attack is possible if the equation

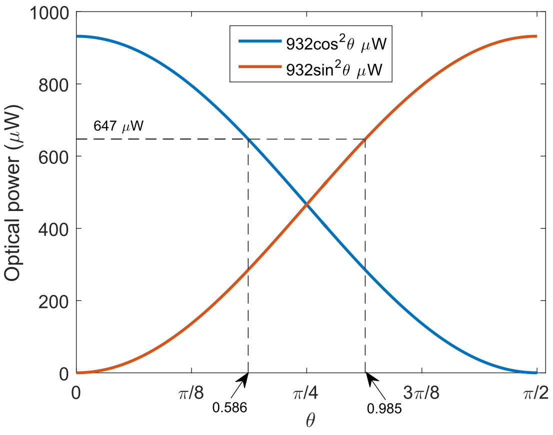

Figure 1. Relationship between the optical power of the pulse reaching the two detectors and the value of *θ* when Alice chooses a different basis with Bob. The dotted box indicates the range of *θ* that fulfils equation (2), which implies that dishonest Bob can launch a perfect detector-blinding attack.

$$\frac{1}{2}(\max_i\{p_{\text{always},i}\}) < \min_i\{p_{\text{never},i}\} \tag{1}$$

is satisfied[26], where $\frac{1}{2}$ is the mutual projection probability of the honest states from different bases. Equation (1) implies that if Alice's basis differs from Bob's, then neither of the two detectors would click.

The procedures of the detector-blinding attack launched by dishonest Bob in practical $\mathrm{J}^{+}11$ system are as follows. First, Bob transmits bright light into Alice's detectors to convert them into classical linear model. Then, instead of preparing the sent states in single-photon pulses, Bob sends them by bright trigger pulses with peak power just above $\max_i\{p_{\text{always},i}\}$. Consequently, Alice has a successful click only if her basis is consistent with the sent state due to equation (1). Meanwhile, the non-detected trials will be discarded and announced by Alice because of the loss-tolerant property of the protocol. Thus, Bob will know which cases Alice has successful clicks, and her bases and measurement results correspondingly. Based on these information, Bob can determine with certainty whether Alice will obtain a conclusive raw key bit. For example, Bob sends the state $|0\rangle$ and Alice has a click, which implies that Alice has chosen the rectilinear basis and obtained the $|0\rangle$ state. Then, Bob can make Alice acquire a conclusive raw key bit 1 if he announces the states pair $\{|1\rangle, |-\rangle\}$. Otherwise, he announces the states $\{|0\rangle, |+\rangle\}$ and Alice will have an inconclusive result. Finally, Bob could control precisely which final key is known to Alice by dividing the raw key properly, which means the user privacy is damaged completely.

As for $\mathrm{G}^{+}12$ protocol, Bob sends the states $\{|0\rangle, |1\rangle, |0'\rangle, |1'\rangle\}$ to Alice, which is the difference from $\mathrm{J}^{+}11$. The states $|0'\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle$ and $|1'\rangle = \sin\theta|0\rangle - \cos\theta|1\rangle$, where $\theta \in \left(0, \frac{\pi}{2}\right)$. To perform a perfect detector-blinding attack as above, the relationship of equation (1) should be modified to

$$\begin{aligned} \cos^2\theta(\max_i\{p_{\text{always},i}\}) &< \min_i\{p_{\text{never},i}\},\\ \sin^2\theta(\max_i\{p_{\text{always},i}\}) &< \min_i\{p_{\text{never},i}\}, \end{aligned} \tag{2}$$

where $\cos^2\theta$ and $\sin^2\theta$ are the mutual projection probabilities of the honest states from different bases. Here, we take some specified values $\max_i\{p_{\text{always},i}\} = 932\ \mu$W and $\min_i\{p_{\text{never},i}\} = 647\ \mu$W for the simulation[26]. In this case, the range of θ that fulfils equation (2) is demonstrated in Fig. 1. We can see that if the selected value θ falls into the span of $0.586 \le \theta \le 0.985$, then dishonest Bob can launch the attack perfectly. However, when the θ is outside of the above range, Bob's detector-blinding attack will introduce errors in Alice's raw key. Note that $\theta = \frac{\pi}{4}$ is the case for $\mathrm{J}^{+}11$, and the equation (1) is also satisfied.

From the above attack we can conclude that it is crucial to ensure that the experimental implementations of QKD-based QPQ are also secure. However, there is a gap between the theory and practice of QPQ in terms of the single-photon detectors, which dishonest Bob may exploit to break the user privacy without being detected. To solve this problem, the MDI-QPQ protocol is proposed in the following.

Protocol of loss-tolerant MDI-QPQ.

For the purpose of being completely loss independent, we demonstrate the polarization encoding MDI-QPQ protocol with single-photon sources.

(1) Bob sends, uniformly at random, one of the four polarized states $|0\rangle$, $|1\rangle$, and

$$\begin{aligned} |0_b'\rangle &= \cos\theta_b|0\rangle + \sin\theta_b|1\rangle,\\ |1_b'\rangle &= \sin\theta_b|0\rangle - \cos\theta_b|1\rangle, \end{aligned}$$

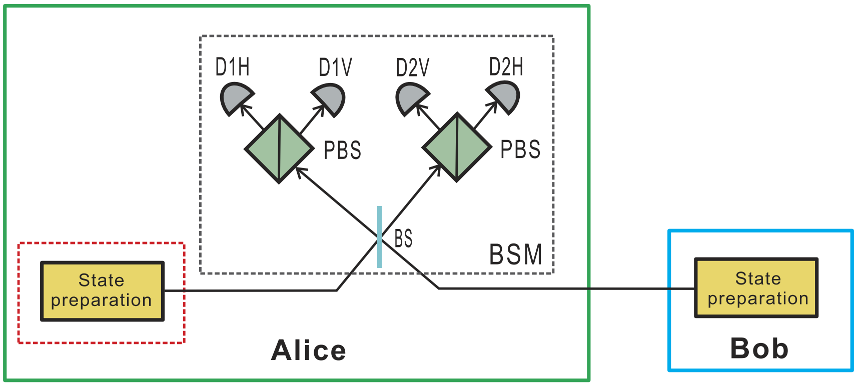

Figure 2. Schematic diagram of loss-tolerant MDI-QPQ for the honest parties. The BS represents 50:50 beam splitter, and PBS stands for polarization beam splitter. Alice and Bob prepare honest polarization states randomly with single-photon sources. Alice makes the BSMs. A joint click on D1H and D2V or D1V and D2H implies a projection into Bell state $|\Psi^{-}\rangle$ and will be recorded by Alice. The red dotted box means that the classical information of Alice's state preparation is not leaked to the BSM and Bob. The grey dotted box represents that Alice needs not to trust the BSM device.

(Combinations)	$\|\Psi^{-}\rangle$			
	$\|0\rangle$	$\|1\rangle$	$\|0'_b\rangle$	$\|1'_b\rangle$
$\|0\rangle$	0	$\frac{1}{2}$	$\frac{1}{2}\sin^2\theta_b$	$\frac{1}{2}\cos^2\theta_b$
$\|1\rangle$	$\frac{1}{2}$	0	$\frac{1}{2}\cos^2\theta_b$	$\frac{1}{2}\sin^2\theta_b$
$\|0'_a\rangle$	$\frac{1}{2}\sin^2\theta_a$	$\frac{1}{2}\cos^2\theta_a$	$\frac{1}{2}\sin^2(\theta_b-\theta_a)$	$\frac{1}{2}\cos^2(\theta_b-\theta_a)$
$\|1'_a\rangle$	$\frac{1}{2}\cos^2\theta_a$	$\frac{1}{2}\sin^2\theta_a$	$\frac{1}{2}\cos^2(\theta_b-\theta_a)$	$\frac{1}{2}\sin^2(\theta_b-\theta_a)$

Table 1. Theoretical probabilities of obtaining Bell state $|\Psi^{-}\rangle$ for different combinations of the honest states. These can be calculated by the interferences of the honest states at the beam splitter.

to Alice, where $\theta_b \in \left(0, \frac{\pi}{2}\right)$ and can be adjusted to make the protocol have different degree of security. The rectilinear basis $\{|0\rangle, |1\rangle\}$ encodes the raw key bit 0, and the basis $\{|0'_b\rangle, |1'_b\rangle\}$ corresponds to the raw key bit 1.

(2) Alice prepares one of the four polarized states $|0\rangle$, $|1\rangle$, and

$$|0'_a\rangle = \cos\theta_a|0\rangle + \sin\theta_a|1\rangle,$$
$$|1'_a\rangle = \sin\theta_a|0\rangle - \cos\theta_a|1\rangle,$$

randomly and independently of Bob (the value of θ_a is related to θ_b and is calculated in next section in detail). Then, she projects her and Bob's states into a Bell state (see Fig. 2). If the BSM does not output a Bell state, then Alice asks Bob to restart step (1). Otherwise, Alice records the measurement result. In fact, she needs to identify only the Bell state $|\Psi^{-}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$, which means that the BSM can be built with only linear optical elements. Theoretical probabilities of obtaining the projection $|\Psi^{-}\rangle$ for different combinations of the honest states are shown in Table 1. Repeat steps (1) and (2) until $k \times N$ successful BSMs are made, where k is a natural number determined by the security analysis and N is the number of database's bits. Note that this step will make the protocol completely independent of losses.

(3) For each trial Alice obtained a Bell state $|\Psi^{-}\rangle$, Bob announces bit 0 to Alice if he has sent states $|0\rangle$ or $|0'_b\rangle$, while reveals bit 1 if he has sent states $|1\rangle$ or $|1'_b\rangle$.

(4) Alice decodes Bob's states to acquire the corresponding raw key bits. It can be done depending on her state and the bit declared in step (3). The decoding process is given in next section specifically. Here, we take that the $\theta_a = \theta_b = \frac{\pi}{4}$ and Bob sends state $|0\rangle$ as an example. Now Bob will announce bit 0. According to Table 1, Alice can rule out $|0'_b\rangle$ and conclude that the raw key is 0 certainly only if she prepared the state $|0'_a\rangle$. Both the conclusive and inconclusive raw key are retained.

(5) Now, a string of raw key with length $k \times N$ are distributed between Bob and Alice, where Bob knows every bit value and Alice knows partially. Then, Bob cuts the raw key into N substrings of length k and tells each bit's position to Alice. The bits of every substring are added bitwise by Alice and Bob to form their final key of length N, respectively. For reducing the computation complexity of the error-correction procedure, if Alice is left with no final key bit composed by k conclusive raw key bits, henceforth referred to *query key* in this paper, then the protocol has to be restarted.

(6) Alice and Bob perform error correction on Alice's final key using the method proposed by Chan *et al.*[18]. After that, Alice estimates the error rate of every query key. If all the error rates are less than some prescribed value, 10^{-3} for example[18], then the protocol goes to the next step. Otherwise, the protocol aborts.

	$\vert\Psi^-\rangle$					$\vert\Psi^-\rangle$			
($\Delta\theta=0$)	$\vert 0\rangle$	$\vert 1\rangle$	$\vert 0'_b\rangle$	$\vert 1'_b\rangle$	**($\Delta\theta=\frac{\pi}{2}$)**	$\vert 0\rangle$	$\vert 1\rangle$	$\vert 0'_b\rangle$	$\vert 1'_b\rangle$
$\vert 0\rangle$	0	$\frac{1}{2}$	$\frac{1}{2}\sin^2\theta_b$	$\frac{1}{2}\cos^2\theta_b$	$\vert 0\rangle$	0	$\frac{1}{2}$	$\frac{1}{2}\sin^2\theta_b$	$\frac{1}{2}\cos^2\theta_b$
$\vert 1\rangle$	$\frac{1}{2}$	0	$\frac{1}{2}\cos^2\theta_b$	$\frac{1}{2}\sin^2\theta_b$	$\vert 1\rangle$	$\frac{1}{2}$	0	$\frac{1}{2}\cos^2\theta_b$	$\frac{1}{2}\sin^2\theta_b$
$\vert 0'_a\rangle$	$\frac{1}{2}\sin^2\theta_b$	$\frac{1}{2}\cos^2\theta_b$	0	$\frac{1}{2}$	$\vert 0'_a\rangle$	$\frac{1}{2}\cos^2\theta_b$	$\frac{1}{2}\sin^2\theta_b$	$\frac{1}{2}$	0
$\vert 1'_a\rangle$	$\frac{1}{2}\cos^2\theta_b$	$\frac{1}{2}\sin^2\theta_b$	$\frac{1}{2}$	0	$\vert 1'_a\rangle$	$\frac{1}{2}\sin^2\theta_b$	$\frac{1}{2}\cos^2\theta_b$	0	$\frac{1}{2}$

Table 2. Theoretical probabilities of obtaining Bell state $|\Psi^-\rangle$ for $\Delta\theta=0$ and $\Delta\theta=\frac{\pi}{2}$ in the honest protocol.

(7) Alice announces to Bob a shift value that will align one of the query key bits to the bit in the database she wants to retrieve. Then, Bob shifts his final key cyclically with this value, and uses the shifted key to encrypt his database by one-time-pad. Bob sends the encrypted database to Alice. Consequently, Alice can decode the queried item with that query key.

The security of MDI-QPQ is completely loss independent with single-photon sources. The reasons are as follows. First, we prove that the degree of insecurity for the database privacy is completely independent of the losses in practical system. Note that the four honest states are linearly dependent, implying that the unambiguous state discrimination (USD) is not applicable here[39]. Moreover, the density matrix of the state received by Alice in step (2) is

$$\rho=\frac{1}{4}\sum_{i=1}^{4}\rho_i=\frac{I}{2}, \tag{3}$$

where I is the identity operator in two-dimensional Hilbert space, $\rho_1=|0\rangle\langle 0|$, $\rho_2=|1\rangle\langle 1|$, $\rho_3=|0'_b\rangle\langle 0'_b|$, and $\rho_4=|1'_b\rangle\langle 1'_b|$. Equation (3) means that the identity operator can be resolved as a weighted sum over the density matrix ρ_i, resulting that the maximal-confidence discrimination (MCD) of the four honest states can be done without inconclusive results[40]. Namely, the MCD coincides with the minimum-error discrimination (MED), and the maximal guessing probability cannot be increased by admitting inconclusive results. Therefore, in step (2), Alice cannot keep only the conclusive raw key by USD or MCD, and discard the inconclusive ones which can be attributed to the losses. On the other hand, thanks to the elegant design of SARG04 QKD, Alice still has to distinguish two non-orthogonal states even if she can store the photons and delay the measurements after step (3). If the distinguished result is uncertain, she has no chance to disregard it because this state has been declared detected successfully in step (2) and will be used for the following postprocessing. Consequently, Alice cannot know all the raw key, let alone the final key, no matter how many losses in the practical system.

As the BSM can be fabricated by a dishonest Bob, the measurement device can be designed to discriminate the four honest states randomly prepared by Alice, and announce the result to Bob through classical communication. The discrimination of Alice's four honest states can be regarded as distinguishing the state ρ in equation (3) with $\rho_1=|0\rangle\langle 0|$, $\rho_2=|1\rangle\langle 1|$, $\rho_3=|0'_a\rangle\langle 0'_a|$, and $\rho_4=|1'_a\rangle\langle 1'_a|$. For the reasons explained above, Bob cannot resort to the USD and MCD to unambiguously distinguish Alice's state. His optimal discrimination of Alice's state is the MED. Thus, he would not determine the conclusiveness of Alice's raw key with certainty. Namely, he will not acquire the position of the query key exactly at last. In a word, neither dishonest party will benefit from the losses in the practical implementation.

Correctness. The degree of privacy for MDI-QPQ will be analyzed in three aspects. The first is the correctness of the protocol when both parties are honest. It can be seen from Table 1 that, to make the protocol work correctly, the absolute value of the difference between θ_a and θ_b should satisfies

$$\Delta\theta=|\theta_a-\theta_b|=\begin{cases}0 \text{ or } \pi,\\ \frac{\pi}{2} \text{ or } \frac{3\pi}{2}.\end{cases} \tag{4}$$

As there is no difference in the performance of the protocol for $\Delta\theta=0$ and $\Delta\theta=\pi$ (for $\Delta\theta=\frac{\pi}{2}$ and $\Delta\theta=\frac{3\pi}{2}$ as well), we will choose $\Delta\theta=0$ and $\Delta\theta=\frac{\pi}{2}$ for demonstration. Now, the Table 1 becomes the Table 2.

We make an example to show how Alice obtains a conclusive raw key in the honest protocol. For $\Delta\theta=0$, if Bob has sent state $|0\rangle$ and announced bit 0, according to Table 2, Alice can identify Bob's state $|0\rangle$ and thus the raw key 0 with certainty only if she has prepared state $|0'_a\rangle$. However, she will obtain an inconclusive result if she prepared states $|1\rangle$ or $|1'_a\rangle$. For $\Delta\theta=\frac{\pi}{2}$, if Bob has sent state $|0\rangle$ and announced bit 0, according to Table 2, Alice can identify Bob's state $|0\rangle$ and thus the raw key 0 with certainty only if she has prepared state $|1'_a\rangle$. However, she will obtain an inconclusive result if she prepared states $|1\rangle$ or $|0'_a\rangle$.

As Alice selects the four states randomly, in the absence of noise, the probability that BSM yields the above conclusive raw key is

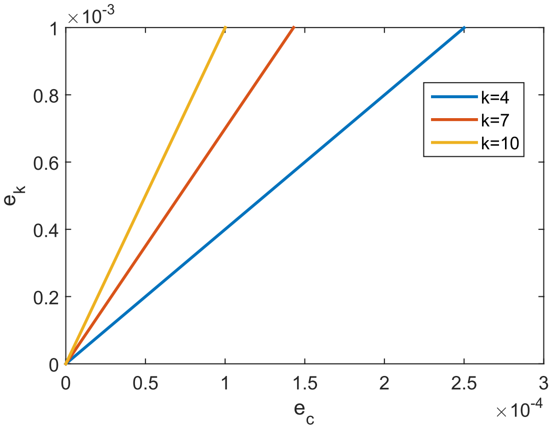

Figure 3. Relationships between the error rates e_k of the query key without error correction and e_c of the conclusive raw key for $k=4$, $k=7$ and $k=10$ (from right to left).

$$
\begin{aligned}
p_c &= \frac{\frac{1}{4} \times \frac{1}{2}\sin^2\theta_b}{\frac{1}{4} \times \left(\frac{1}{2} + \frac{1}{2}\sin^2\theta_b + \frac{1}{2}\cos^2\theta_b\right)}\\
&= \frac{\sin^2\theta_b}{2},
\end{aligned} \tag{5}
$$

for both $\Delta\theta = 0$ and $\Delta\theta = \frac{\pi}{2}$. Without error correction, the average number of Alice's query key is $\bar{n} = N(p_c)^k$. The probability that she will know none query key is $p_0 = [1 - (p_c)^k]^N$. It implies that the correctness of MDI-QPQ is the same with G$^+$12 in the noiseless case. For databases with different number of bits N, we can choose suitable k and θ_b to make both the $\bar{n}$ and p_0 be small.

In the presence of noise, the error rate of the query key before error correction is

$$
e_k = \sum_{\substack{i=1\\ (i \text{ odd})}}^{k} \binom{k}{i} e_c^i (1 - e_c)^{k-i}, \tag{6}
$$

where e_c is the error rate of the conclusive raw key and odd errors happened in the the query key's k conclusive raw key bits. The relationships between the error rates e_k and e_c for different k are shown in Fig. 3. It can be seen that even for very little noise, the error rate of the query key will increase to the threshold value 10^{-3} quickly. Thus, it is necessary to add the error-correction procedure[18] into the protocol.

Database privacy. Dishonest Alice will try to know as many query key as possible. Assume that Alice controls everything except Bob's single-photon source. It is in Alice's best interest to replace the noisy channel with a noiseless one to receive the states correctly each time. Although it is no matter that the channel is lossy, the all powerful dishonest Alice can use a lossless one instead. We also suppose she has perfect detectors and perfect quantum memories.

The imperfect privacy of database is guaranteed by the theorem that nonorthogonal quantum states cannot be distinguished perfectly[41]. And Alice must announce which states have been projected to Bell state $|\Psi^-\rangle$ successfully before Bob tells some classical information of his sent states. Therefore, Alice inevitably obtains some inconclusive raw key with certain probability, which results in inconclusive final key.

As analyzed in J$^+$11 and G$^+$12 protocols[10,12], Alice can increase the probability p_c by storing the received photons in quantum memories and performing the USD measurements after step (3). The successful probability of the USD, for Bob's announced two honest states, is $1 - |\langle 0|0_b'\rangle| = 1 - \cos\theta_b$. Thus, the MDI-QPQ will obtain better database privacy for small θ_b.

In this cheating strategy, Alice deviates from the MDI protocol to obtain more items of the database. However, our protocol is designed to protect only an honest Alice. Thus, it does not matter that the advantage of the MDI paradigm will not exist for a dishonest Alice.

User privacy. Dishonest Bob will try to acquire the position of the item Alice queries. In the following, we will analyze the user privacy under the fact that Alice does not have to trust her measurement device. That is to say, we assume that the measurement device is built by dishonest Bob which contains his cheating equipment. Because the outcome of the measurement cannot reveal Alice's state with certainty, the measurement device can send classical information to Bob. These are equivalent to that the measurement device is placed in Bob's side and Bob announces the measurement results. Thus, all the detector side channels are removed. What Alice needs only to pay attention is to protect the classical information of her state preparation from leakage to the

	$\lvert\Psi^-\rangle$					$\lvert\Psi^-\rangle$			
$(\Delta\theta=0)$	$\lvert 0\rangle$	$\lvert 1\rangle$	$\lvert 0'_a\rangle$	$\lvert 1'_a\rangle$	**$(\Delta\theta=\frac{\pi}{2})$**	$\lvert 0\rangle$	$\lvert 1\rangle$	$\lvert 0'_a\rangle$	$\lvert 1'_a\rangle$
$\lvert 0''_b\rangle$	$\frac{1}{2}\sin^2\frac{\theta_b}{2}$	$\frac{1}{2}\cos^2\frac{\theta_b}{2}$	$\frac{1}{2}\sin^2\frac{\theta_b}{2}$	$\frac{1}{2}\cos^2\frac{\theta_b}{2}$	$\lvert 0''_b\rangle$	$\frac{1}{2}\sin^2\frac{\theta_b}{2}$	$\frac{1}{2}\cos^2\frac{\theta_b}{2}$	$\frac{1}{2}\cos^2\frac{\theta_b}{2}$	$\frac{1}{2}\sin^2\frac{\theta_b}{2}$
$\lvert 1''_b\rangle$	$\frac{1}{2}\cos^2\frac{\theta_b}{2}$	$\frac{1}{2}\sin^2\frac{\theta_b}{2}$	$\frac{1}{2}\cos^2\frac{\theta_b}{2}$	$\frac{1}{2}\sin^2\frac{\theta_b}{2}$	$\lvert 1''_b\rangle$	$\frac{1}{2}\cos^2\frac{\theta_b}{2}$	$\frac{1}{2}\sin^2\frac{\theta_b}{2}$	$\frac{1}{2}\sin^2\frac{\theta_b}{2}$	$\frac{1}{2}\cos^2\frac{\theta_b}{2}$

Table 3. Theoretical probabilities of obtaining Bell state $\lvert\Psi^-\rangle$ for different combinations of Bob's cheating states and Alice's honest states in the first middle-state attack.

untrusted measurement device and Bob. Moreover, we suppose that both parties' single-photon sources, the channels and the detectors are perfect. All these conditions will maximize the probability that Bob knows the item Alice queries.

Empty-pulse attack. Based on the above assumptions, we first introduce an *empty-pulse* attack in which Bob does not send any state in step (1). However, Bob places a cheating equipment in the measurement device to discriminate Alice's states with minimum error rate. The measurement device will send the discrimination result to Bob and output a BSM projection randomly to honest Alice. Note that the four states sent randomly by Alice are pairs of two orthogonal states with the same *prior* probability $\frac{1}{4}$. Thus, the guessing probability of the four honest states for the MED is $\frac{1}{2}$[42]. Namely, Bob's discrimination has an error rate of $\frac{1}{2}$.

For instance, assume $\Delta\theta=0$ and the result of the MED is state $\lvert 0\rangle$. According to Table 2, Bob announces 0 in step (3) to expect Alice to acquire conclusive raw key 1. If the MED is right, Bob gains the information both on the conclusiveness and bit value of Alice's raw key. However, if the MED is wrong, Alice will obtain conclusive key only if she prepares state $\lvert 0'_a\rangle$. Now, Alice deems the raw key value is 0, which is different from Bob's expectation. As Alice prepares the states randomly, in the empty-pulse attack the probability that Alice has conclusive raw key is

$$\begin{aligned} p_c^{\mathrm{emp}} &= \frac{1}{2} + \frac{1}{2} \times \frac{1}{4} \\ &= \frac{5}{8}, \end{aligned} \tag{7}$$

and the bit error rate of Bob's corresponding raw key is $\frac{1}{2}$.

Middle-state attack 1. Another more powerful attack is the *middle-state* attack proposed in the security analysis of J$^+$11 and G$^+$12 protocols[10,12]. In the middle-state attack on MDI-QPQ, Bob keeps the measurement device doing the BSM. However, instead of transmitting the honest states to Alice in step (1), he sends the middle state $\lvert 0''_b\rangle$ (or $\lvert 1''_b\rangle$) and announcing 1 (or 0) in step (3) to expect Alice to acquire a conclusive raw key. The forms of the two middle states are that

$$\begin{aligned} \lvert 0''_b\rangle &= \cos\frac{\theta_b}{2}\lvert 0\rangle + \sin\frac{\theta_b}{2}\lvert 1\rangle, \\ \lvert 1''_b\rangle &= \sin\frac{\theta_b}{2}\lvert 0\rangle - \cos\frac{\theta_b}{2}\lvert 1\rangle. \end{aligned}$$

The theoretical probabilities for the middle states and Alice's honest states being projected into Bell state $\lvert\Psi^-\rangle$ are shown in Table 3. Take the example that Bob sends state $\lvert 0''_b\rangle$ and announces bit 1. From Table 3 and the part of Table 2 for $\Delta\theta=0$, it can be seen that Alice will obtain a conclusive raw key if she prepares states $\lvert 1\rangle$ or $\lvert 1'_a\rangle$. As for $\Delta\theta=\pi/2$, Alice will obtain a conclusive raw key if she prepares states $\lvert 1\rangle$ or $\lvert 0'_a\rangle$. Because Alice prepares the states randomly, as shown in Table 3, the probability of obtaining a conclusive raw key in both cases is

$$\begin{aligned} p_{c1}^{\mathrm{mid1}} &= \frac{\frac{1}{4} \times \frac{1}{2} \times \left(\cos^2\frac{\theta_b}{2} + \cos^2\frac{\theta_b}{2}\right)}{\frac{1}{4} \times \frac{1}{2} \times \left(\sin^2\frac{\theta_b}{2} + \cos^2\frac{\theta_b}{2} + \sin^2\frac{\theta_b}{2} + \cos^2\frac{\theta_b}{2}\right)} \\ &= \cos^2\frac{\theta_b}{2}. \end{aligned} \tag{8}$$

If Bob wants Alice to obtain an inconclusive raw key, he sends $\lvert 0''_b\rangle$ (or $\lvert 1''_b\rangle$) but announces 0 (or 1). Now, Alice will gets a conclusive result with probability

$$\begin{aligned} p_{c2}^{\mathrm{mid1}} &= \frac{\frac{1}{4} \times \frac{1}{2} \times \left(\sin^2\frac{\theta_b}{2} + \sin^2\frac{\theta_b}{2}\right)}{\frac{1}{4} \times \frac{1}{2} \times \left(\sin^2\frac{\theta_b}{2} + \cos^2\frac{\theta_b}{2} + \sin^2\frac{\theta_b}{2} + \cos^2\frac{\theta_b}{2}\right)} \\ &= \sin^2\frac{\theta_b}{2}. \end{aligned} \tag{9}$$

for both $\Delta\theta=0$ and $\Delta\theta=\frac{\pi}{2}$.

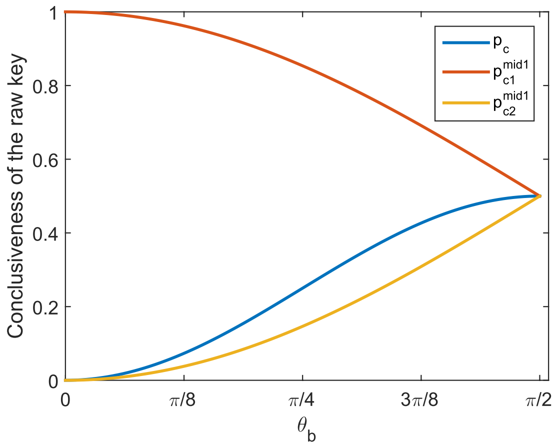

Figure 4. The probabilities of Alice acquiring a conclusive raw key in the honest protocol and in the first middle-state attack for different θ_b. The curves represent p_{c1}^{mid1}, p_c and p_{c2}^{mid1} from up to down.

	$\lvert\Psi^-\rangle$					$\lvert\Psi^-\rangle$			
$(\Delta\theta=0)$	$\lvert 0\rangle$	$\lvert 1\rangle$	$\lvert 0'_a\rangle$	$\lvert 1'_a\rangle$	$(\Delta\theta=\frac{\pi}{2})$	$\lvert 0\rangle$	$\lvert 1\rangle$	$\lvert 0'_a\rangle$	$\lvert 1'_a\rangle$
$\lvert 0''_b\rangle$	$\frac{1}{2}\sin^2\frac{\theta_b}{2}$	$\frac{1}{2}\cos^2\frac{\theta_b}{2}$	$\frac{1}{2}\sin^2\frac{\theta_b}{2}$	$\frac{1}{2}\cos^2\frac{\theta_b}{2}$	$\lvert 0''_b\rangle$	$\frac{1}{2}\sin^2\left(\frac{\theta_b}{2}\pm\frac{\pi}{4}\right)$	$\frac{1}{2}\cos^2\left(\frac{\theta_b}{2}\pm\frac{\pi}{4}\right)$	$\frac{1}{2}\sin^2\left(\frac{\theta_b}{2}\pm\frac{\pi}{4}\right)$	$\frac{1}{2}\cos^2\left(\frac{\theta_b}{2}\pm\frac{\pi}{4}\right)$
$\lvert 1''_b\rangle$	$\frac{1}{2}\cos^2\frac{\theta_b}{2}$	$\frac{1}{2}\sin^2\frac{\theta_b}{2}$	$\frac{1}{2}\cos^2\frac{\theta_b}{2}$	$\frac{1}{2}\sin^2\frac{\theta_b}{2}$	$\lvert 1''_b\rangle$	$\frac{1}{2}\cos^2\left(\frac{\theta_b}{2}\pm\frac{\pi}{4}\right)$	$\frac{1}{2}\sin^2\left(\frac{\theta_b}{2}\pm\frac{\pi}{4}\right)$	$\frac{1}{2}\cos^2\left(\frac{\theta_b}{2}\pm\frac{\pi}{4}\right)$	$\frac{1}{2}\sin^2\left(\frac{\theta_b}{2}\pm\frac{\pi}{4}\right)$

Table 4. Theoretical probabilities of obtaining Bell state $|\Psi^-\rangle$ for different combinations of Bob's cheating states and Alice's honest states in the second middle-state attack. The operator '+' in '±' stands for the case $\theta_a-\theta_b=\frac{\pi}{2}$, while the operator '−' in '±' represents the case $\theta_a-\theta_b=-\frac{\pi}{2}$.

The relationships between p_c, p_{c1}^{mid1}, p_{c2}^{mid1} and θ_b are plotted in Fig. 4. We can see that Bob can increase or decrease the conclusiveness of Alice's raw key in the middle-state attack. Thus, he will improve the accuracy of the estimation for Alice's query address. However, it can be viewed from Tables 2 and 3 that now Alice will register the conclusive raw key bit value as 0 or 1 with equal probability, implying that the bit error rate of Bob's corresponding raw key is $\frac{1}{2}$.

Middle-state attack 2. There is another middle-state attack in which Bob can reduce the bit error rate of his raw key at the price of compromising his control of the conclusiveness of Alice's raw key. The difference with the above one is that Bob now sends the following two middle states

$$\begin{aligned} |0''_b\rangle &= \cos\frac{\theta_a}{2}|0\rangle + \sin\frac{\theta_a}{2}|1\rangle, \\ |1''_b\rangle &= \sin\frac{\theta_a}{2}|0\rangle - \cos\frac{\theta_a}{2}|1\rangle. \end{aligned}$$

The theoretical probabilities for these two middle states and Alice's honest states being projected into Bell state $|\Psi^-\rangle$ are shown in Table 4. For the case $\Delta\theta=0$, the two middle-state attacks are the same. In the following, we consider only the situation $\Delta\theta=\frac{\pi}{2}$ and assume the parties select $\theta_a=\theta_b+\frac{\pi}{2}$. When Bob chooses the cheating strategy of sending the middle state $|0''_b\rangle$ (or $|1''_b\rangle$) and announcing 1 (or 0), the probability which Alice obtains conclusive raw key is a constant

$$\begin{aligned} p_{c1}^{\text{mid2}} &= \frac{\frac{1}{4}\times\frac{1}{2}\times\left(\sin^2\left(\frac{\theta_b}{2}+\frac{\pi}{4}\right)+\cos^2\left(\frac{\theta_b}{2}+\frac{\pi}{4}\right)\right)}{2\times\frac{1}{4}\times\frac{1}{2}\times\left(\sin^2\left(\frac{\theta_b}{2}+\frac{\pi}{4}\right)+\cos^2\left(\frac{\theta_b}{2}+\frac{\pi}{4}\right)\right)} \\ &= \frac{1}{2}. \end{aligned} \tag{10}$$

If Bob chooses sending $|0''_b\rangle$ (or $|1''_b\rangle$) but announces 0 (or 1), Alice will gets a conclusive raw key with $p_{c2}^{\text{mid2}}=\frac{1}{2}$ as well. It implies that the conclusiveness of Alice's raw key is independent of Bob's cheating strategies. Comparing with p_{c1}^{mid1} and p_{c2}^{mid1}, it shows that Bob has limited control over Alice's raw key.

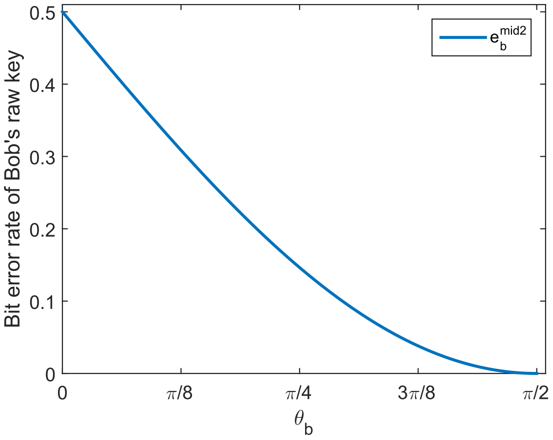

Figure 5. The relationship between the error rate of Bob's raw key and θ_b in the second middle-state attack for $\Delta\theta = \frac{\pi}{2}$.

Take the cheating strategy that Bob sends the middle state $|0''_b\rangle$ and announces 1 for instance. Alice will obtain a conclusive raw key if she prepares state $|1\rangle$ or $|0'_a\rangle$. Seeing Table 4, the probability for states combination $\{|0'_a\rangle$ and $|0''_b\rangle\}$ being projected into $|\Psi^-\rangle$ is larger than the combination $\{|1\rangle$ and $|0''_b\rangle\}$. Thus, it is reasonable for Bob to guess that Alice has prepared state $|0'_a\rangle$ under the hypothesis that she obtained a conclusive result. If this is indeed the case, then Alice's conclusive raw key bit is 0. However, if in fact, Alice prepares the state $|1\rangle$, she will identify the conclusive raw key bit 1 and Bob has a error in this raw key. Thus, the error rate of Bob's raw key when compared with Alice's conclusive results is

$$\begin{aligned} e_b^{\mathrm{mid2}} &= \frac{\frac{1}{4} \times \frac{1}{2} \times \cos^2\left(\frac{\theta_b}{2} + \frac{\pi}{4}\right)}{\frac{1}{4} \times \frac{1}{2} \times \left(\sin^2\left(\frac{\theta_b}{2} + \frac{\pi}{4}\right) + \cos^2\left(\frac{\theta_b}{2} + \frac{\pi}{4}\right)\right)} \\ &= \cos^2\left(\frac{\theta_b}{2} + \frac{\pi}{4}\right). \end{aligned} \tag{11}$$

The relationship between e_b^{mid2} and θ_b is plotted in Fig. 5. It shows that if Bob pursues a low error rate of his raw key for $\Delta\theta = \frac{\pi}{2}$, he can perform the second middle-state attack.

Comparing the two middle-state attacks, it shows that there is a trade-off between the control of the conclusiveness and knowing the value of Alice's raw key. The first one allows Bob to obtain strong control on the conclusiveness of Alice's raw key while makes him completely ignore of the key's value. On the other hand, the second one let Bob know nonvanishing information on the value of the raw key, but his control on the key is limited.

In the above three attacks once Bob tries to gather more information on Alice's query item than the honest protocol, it will make him loss the information on the raw key bit value, even he can control the measurement device. By designing the error-correction code properly, Bob's final key is still not exactly the same with Alice's corresponding query key at last[18], which means that he may provide wrong answers. And it can be detected by Alice at a later time with a nonvanishing (but nonunity) probability. It shows that loss-tolerant MDI-QPQ is cheat sensitive for user privacy.

Actually, seeing Table 2, if Bob knows that one of Alice's raw key is conclusive and its bit value is 0 (or 1) at the same time, then he can also correctly guess that the basis Alice used to prepare her state is $\{|0'_a\rangle, |1'_a\rangle\}$ (or $\{|0\rangle, |1\rangle\}$) (note that in J$^+$11 and G$^+$12, Bob will correctly guess the basis Alice used to measure the state she received). However, since Alice has protected the classical information of her state preparation from leakage to Bob, the *no-signaling principle* implies that Bob's probability to guess her basis correctly is no more than $\frac{1}{2}$. Thus, in MDI-QPQ, dishonest Bob cannot simultaneously have the bit value and the conclusiveness information of Alice's raw key, which is similar to J$^+$11 and G$^+$12 protocols[10,12].

Discussion

We have proposed a detector-blinding attack launched by dishonest Bob on the practical QKD-based QPQ system. Specifically, perfect detector-blinding attack is always possible for practical J$^+$11 system, and is possible for G$^+$12 with a certain range of θ. However, the detector-blinding attack may introduce some errors in Alice's raw key with smaller and larger θ value for G$^+$12. To make the practical QKD-based QPQ systems secure again, we proposed the method of loss-tolerant MDI-QPQ. Compared with previous QKD-based QPQ, it has a distinct advantage of removing all the detector side channels. We have proven the security of loss-tolerant MDI-QPQ under some typical attacks. It would be meaningful to have a more general security analysis in the future. Moreover, the source flaws should be considered in the security analysis, because it has been assumed that both parties' sources are trusted in this paper. We should examine this condition carefully in practice.

For the experiment of the proposed loss-tolerant MDI-QPQ, it can benefit from the rapid development of MDI-QKD experiments[28–35] with only few necessary modifications. The major changes for the quantum process are the coefficients of the states prepared by both parties and they have to use single-photon sources. The remaining setups, like the BSM device, do not need to be modified. It shows that our proposal is feasible with the existed MDI-QKD experiments.

In the experiments of quantum cryptography, a PR-WCS source is always used to substitute the single-photon source, which is not easy for state-of-the-art technology. However, when we employ PR-WCS sources, the security of MDI-QPQ may be compromised due to the multi-photon pulses. Note that one could close the potential security loophole by limiting the total number of transmitted pulses, resulting that the protocol maybe not completely loss independent[43]. Another problem is that the projection $|\Psi^-\rangle$ from the case when the parties prepare the states in bases $\{|0'_{a(b)}\rangle, |1'_{a(b)}\rangle\}$ will introduce a high inherent error rate for Alice's raw key. Thus, an appropriate error-correction code is needed for the correctness of the protocol. Or one can refer the setup proposed for MDI-SARG04 QKD with PR-WCS sources[44]. We will deal with these obstacles in the following research to make the loss-tolerant MDI-QPQ more practical.

References

1. Gertner, Y., Ishai, Y., Kushilevitz, E. & Malkin, T. Protecting data privacy in private information retrieval schemes. *Journal of Computer and System Sciences* **60,** 592–629 (2000).
2. Rabin, M. O. How to exchange secrets with oblivious transfer. *Technical Report TR-81*, *Aiken Computation Lab*, *Harvard University* (1981).
3. Lo, H.-K. Insecurity of quantum secure computations. *Physical Review A* **56,** 1154 (1997).
4. Einstein, A., Podolsky, B. & Rosen, N. Can quantum-mechanical description of physical reality be considered complete? *Physical Review* **47,** 777–780 (1935).
5. Kerenidis, I. & De Wolf, R. Quantum symmetrically-private information retrieval. *Information Processing Letters* **90,** 109–114 (2004).
6. Giovannetti, V., Lloyd, S. & Maccone, L. Quantum private queries. *Physical Review Letters* **100,** 230502 (2008).
7. Giovannetti, V., Lloyd, S. & Maccone, L. Quantum private queries: security analysis. *IEEE Transactions on Information Theory* **56,** 3465–3477 (2010).
8. De Martini, F. *et al.* Experimental quantum private queries with linear optics. *Physical Review A* **80,** 010302 (2009).
9. Olejnik, L. Secure quantum private information retrieval using phase-encoded queries. *Physical Review A* **84,** 022313 (2011).
10. Jakobi, M. *et al.* Practical private database queries based on a quantum-key-distribution protocol. *Physical Review A* **83,** 022301 (2011).
11. Scarani, V., Acin, A., Ribordy, G. & Gisin, N. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Physical Review Letters* **92,** 057901 (2004).
12. Gao, F., Liu, B., Wen, Q.-Y. & Chen, H. Flexible quantum private queries based on quantum key distribution. *Optics Express* **20,** 17411–17420 (2012).
13. Wei, C.-Y., Wang, T.-Y. & Gao, F. Practical quantum private query with better performance in resisting joint-measurement attack. *Physical Review A* **93,** 042318 (2016).
14. Yang, Y.-G., Sun, S.-J., Xu, P. & Tian, J. Flexible protocol for quantum private query based on b92 protocol. *Quantum Information Processing* **13,** 805–813 (2014).
15. Zhang, J.-L., Guo, F.-Z., Gao, F., Liu, B. & Wen, Q.-Y. Private database queries based on counterfactual quantum key distribution. *Physical Review A* **88,** 022334 (2013).
16. Liu, B., Gao, F., Huang, W. & Wen, Q. Qkd-based quantum private query without a failure probability. *Science China Physics, Mechanics & Astronomy* **58,** 1–6 (2015).
17. Lucio-Martinez, I., Chan, P., Mo, X., Hosier, S. & Tittel, W. Proof-of-concept of real-world quantum key distribution with quantum frames. *New Journal of Physics* **11,** 095001 (2009).
18. Chan, P., Lucio-Martinez, I., Mo, X., Simon, C. & Tittel, W. Performing private database queries in a real-world environment using a quantum protocol. *Scientific Reports* **4,** 5233 (2014).
19. Gao, F., Liu, B., Huang, W. & Wen, Q.-Y. Postprocessing of the oblivious key in quantum private query. *IEEE Journal of Selected Topics in Quantum Electronics* **21,** 1–11 (2015).
20. Wei, C.-Y., Gao, F., Wen, Q.-Y. & Wang, T.-Y. Practical quantum private query of blocks based on unbalanced-state bennett-brassard-1984 quantum-key-distribution protocol. *Scientific Reports* **4,** 7537 (2014).
21. Wei-Xu, S., Xing-Tong, L., Jian, W. & Chao-Jing, T. Multi-bit quantum private query. *Communications in Theoretical Physics* **64,** 299 (2015).
22. Scarani, V. *et al.* The security of practical quantum key distribution. *Reviews of Modern Physics* **81,** 1301 (2009).
23. Lo, H.-K., Curty, M. & Tamaki, K. Secure quantum key distribution. *Nature Photonics* **8,** 595–604 (2014).
24. Qi, B., Fung, C.-H. F., Lo, H.-K. & Ma, X. Time-shift attack in practical quantum cryptosystems. *Quantum Information & Computation* **7,** 73–82 (2007).
25. Makarov, V., Anisimov, A. & Skaar, J. Effects of detector efficiency mismatch on security of quantum cryptosystems. *Physical Review A* **74,** 022313 (2006).
26. Lydersen, L. *et al.* Hacking commercial quantum cryptography systems by tailored bright illumination. *Nature Photonics* **4,** 686–689 (2010).
27. Lo, H.-K., Curty, M. & Qi, B. Measurement-device-independent quantum key distribution. *Physical Review Letters* **108,** 130503 (2012).
28. Rubenok, A., Slater, J. A., Chan, P., Lucio-Martinez, I. & Tittel, W. Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks. *Physical Review Letters* **111,** 130501 (2013).
29. Liu, Y. *et al.* Experimental measurement-device-independent quantum key distribution. *Physical Review Letters* **111,** 130502 (2013).
30. da Silva, T. F. *et al.* Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits. *Physical Review A* **88,** 052303 (2013).
31. Tang, Z. *et al.* Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution. *Physical Review Letters* **112,** 190503 (2014).
32. Tang, Y.-L. *et al.* Measurement-device-independent quantum key distribution over 200 km. *Physical Review Letters* **113,** 190501 (2014).
33. Wang, C. *et al.* Phase-reference-free experiment of measurement-device-independent quantum key distribution. *Physical Review Letters* **115,** 160502 (2015).
34. Comandar, L. *et al.* Quantum key distribution without detector vulnerabilities using optically seeded lasers. *Nature Photonics* **10,** 312–315 (2016).

35. Yin, H.-L. *et al.* Measurement-device-independent quantum key distribution over a 404 km optical fiber. *Physical Review Letters* **117,** 190501 (2016).
36. Xu, F., Curty, M., Qi, B. & Lo, H.-K. Measurement-device-independent quantum cryptography. *IEEE Journal of Selected Topics in Quantum Electronics* **21,** 1–11 (2015).
37. Zhao, L. *et al.* Measurement-device-independent quantum coin tossing. *Physical Review A* **92,** 062327 (2015).
38. Makarov, V. Controlling passively quenched single photon detectors by bright light. *New Journal of Physics* **11,** 065003 (2009).
39. Chefles, A. Unambiguous discrimination between linearly independent quantum states. *Physics Letters A* **6,** 339–347 (1998).
40. Herzog, U. Optimal state discrimination with a fixed rate of inconclusive results: Analytical solutions and relation to state discrimination with a fixed error rate. *Physical Review A* **86,** 032314 (2012).
41. Wootters, W. K. & Zurek, W. H. A single quantum cannot be cloned. *Nature* **299,** 802–803 (1982).
42. Bae, J. Structure of minimum-error quantum state discrimination. *New Journal of Physics* **15,** 073037 (2013).
43. Pappa, A., Chailloux, A., Diamanti, E. & Kerenidis, I. Practical quantum coin flipping. *Physical Review A* **84,** 052305 (2011).
44. Mizutani, A., Tamaki, K., Ikuta, R., Yamamoto, T. & Imoto, N. Measurement-device-independent quantum key distribution for scarani-acin-ribordy-gisin 04 protocol. *Scientific Reports* **4,** 5236 (2014).

Acknowledgements

The work is supported by the Strategic Priority Research Program (B) of the Chinese Academy of Sciences (Grant Nos XDB01030100 and XDB01030300), the National Key Research and Development Program of China (Grant No. 2016YFA0302600), and National Natural Science Foundation of China (Grant Nos 61475148 and 61575183).

Author Contributions

L.-Y.Z., Z.-Q.Y., W.C., G.-C.G. and Z.-F.H. conceived the project. L.-Y.Z. and Y.-J.Q. analyzed the detector-blinding attack. L.-Y.Z., Z.-Q.Y. and C.-M.Z. designed the protocol. L.-Y.Z. and Z.-Q.Y. performed the security analysis. L.-Y.Z. wrote the paper.

Additional Information

Competing financial interests: The authors declare no competing financial interests.

How to cite this article: Zhao, L.-Y. *et al.* Loss-tolerant measurement-device-independent quantum private queries. *Sci. Rep.* **7**, 39733; doi: 10.1038/srep39733 (2017).

Publisher's note: Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.