SCIENTIFIC REPORTS

OPEN

SUBJECT AREAS:
QUBITS
LASERS, LEDS AND LIGHT SOURCES
QUANTUM INFORMATION
QUANTUM OPTICS

Received
19 June 2014

Accepted
27 November 2014

Published
18 December 2014

Correspondence and requests for materials should be addressed to F.G. (gaof@bupt.edu.cn)

Practical quantum private query of blocks based on unbalanced-state Bennett-Brassard-1984 quantum-key-distribution protocol

Chun-Yan Wei[1,2], Fei Gao[1], Qiao-Yan Wen[1] & Tian-Yin Wang[2]

[1]State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China, [2]School of Mathematical Science, Luoyang Normal University, Luoyang 471022, China.

Until now, the only kind of practical quantum private query (QPQ), quantum-key-distribution (QKD)-based QPQ, focuses on the retrieval of a single bit. In fact, meaningful message is generally composed of multiple adjacent bits (i.e., a multi-bit block). To obtain a message $a_1a_2\cdots a_l$ from database, the user Alice has to query l times to get each a_i. In this condition, the server Bob could gain Alice's privacy once he obtains the address she queried in any of the l queries, since each a_i contributes to the message Alice retrieves. Apparently, the longer the retrieved message is, the worse the user privacy becomes. To solve this problem, via an unbalanced-state technique and based on a variant of multi-level BB84 protocol, we present a protocol for QPQ of blocks, which allows the user to retrieve a multi-bit block from database in one query. Our protocol is somewhat like the high-dimension version of the first QKD-based QPQ protocol proposed by Jacobi *et al.*, but some nontrivial modifications are necessary.

Private information retrieval (PIR), introduced by Chor *et al.*[1], allows a user (say Alice) to retrieve a bit x_i from a database $X=(x_1,x_2,\cdots,x_n)$ held by a server (say Bob), without revealing the retrieval address i (user privacy). A symmetrically private information retrieval (SPIR)[2] scheme is a PIR scheme satisfying an additional requirement named "database security", that is, Alice should not get more information than x_i from database. In recent years, many SPIR protocols have been proposed in classical cryptography. However, the security of most classical cryptosystems is based on the assumptions of computational complexity which might be vulnerable to quantum computation[3,4]. One may want to know whether this drawback can be overcome by quantum protocols as that in quantum key distribution (QKD)[5].

In fact, since user privacy and database security appear to be conflicting, the task of SPIR cannot be realized ideally even in quantum cryptography[6]. More practically, the quantum scheme for SPIR problem, called quantum private query (QPQ)[7], loosens the security into the following. (1) (Database security) Alice can elicit a few more bits than the ideal requirement (i.e., just 1 bit) from database, and (2) (user privacy) user privacy is guarded in the sense of cheat-sensitivity (that is, Bob's attack will be discovered by Alice with a nonzero probability if he tries to obtain Alice's retrieval address), and it would be better if the probability for Bob to reveal the address Alice queries can be kept small meanwhile.

Most earlier QPQ protocols[7,8,9] utilizing unitary operations, show great significance in theory, but are difficult to be implemented when a large database is concerned. In 2011, Jakobi *et al.*[10] proposed a QPQ protocol (J-protocol) based on SARG04 QKD scheme[11]. As many QKD protocols have been realized experimentally, QKD-based quantum private query is more practical and hence has attracted a great deal of concern. In 2012, Gao *et al.*[12] presented a flexible generalization of J-protocol. Afterwards, Panduranga Rao *et al.*[13] also gave two modifications of J-protocol's postprocessing. Recently, Zhang *et al.*[14] designed a QPQ protocol based on a novel counterfactual QKD protocol.

However, the queried message is generally supposed to be a single bit in the above practical QPQ protocols, which is not the fact in a real implementation. In fact, meaningful message is generally composed of multiple adjacent bits, hence Alice has to query many times from database to obtain the entire message in the bit-by-bit way. Here, we turn to a more realistic model called "QPQ of blocks" (QPQB), which allows the user to retrieve a multi-bit block (i.e., multiple adjacent bits) from database in one query. In our QPQB model, for the sake of

simplicity, the database X is partitioned into entries (blocks) with the same length l. Concretely, $X=(X_1,X_2,\cdots,X_N)$, and each entry X_k ($1 \le k \le N$) is an l-bit message. Here, N is the number of entries in database, and k is the address of the entry X_k.

It is worth noting that, the idea of "QPQ of blocks" is natural but nontrivial, since the security of single-bit QPQ cannot be achieved as ideally as that of QKD with the composable security definition[15,16] (e.g., Bob always has a nonzero probability to reveal Alice's retrieval address). Concretely, suppose the database stores blocks of information with the same length of 100 bits and the total number of blocks is 100, then there are 10, 000 bits information in total. If Alice wants the information of the 14th block which contains the bits from 1401st to 1500th, then she has to make 100 queries to obtain these bits in the single-bit QPQ scenario. While as we know, Bob always has a nonzero probability p (though it might be very small) to reveal the retrieval address in each bit query. Obviously, once Bob obtains the address of the queried bit in any one of the 100 queries, he can infer which block Alice is retrieving. That is, the probability with which user privacy keeps secret is only $(1-p)^{100}$ in this condition. Apparently, the security degrades very fast with the size of blocks, which is a significant problem for QPQ in real-world applications. Luckily in QPQ of blocks, Alice can obtain the entire block in one query, and as to user privacy, it only needs to hide the address of the block instead of the addresses of its bits. Hence, similar to that pointed out by Chor *et al.*[17], remarkable saving is possible by utilizing the block structure, and the research on QPQB may be an interesting and worthwhile work.

To fulfill the task of QPQB, we first review the idea for realizing QKD-based QPQ of single bit. As we know, distributing an **oblivious** key is of vital importance to achieve it[10]. That is, Alice and Bob should share a raw key K^r in the way that (1) Bob knows K^r entirely, (2) Alice knows only part of its bits, and (3) Bob does not know which bits are known to Alice. After some classical postprocessing on the raw key, Alice only knows roughly one bit in the final key K^f and Bob still does not know which bit is known to Alice. Then, the final key is used to encrypt database so that (1) Alice can subsequently recover the bit she queries from the encrypted database with her known bit in K^f, and (2) both user privacy and database security are well protected.

Following the above idea, each l-bit entry in QPQB needs to be encrypted by an l-bit string (i.e., l adjacent bits) which should be (1) completely known or unknown to Alice, and (2) completely known to Bob while he does not know whether it is known to Alice. Intuitively, we need to design a $d(=2^l)$-level oblivious QKD protocol in which transmitting one qudit can provide l adjacent bits satisfying the above two requirements. Naturally, we expect that it can be achieved by generalizing the SARG04 protocol[11] on which J-protocol[10] is based to its d-level version. However, it is scarcely possible. Concretely in the SARG04 protocol, the fact that (1) each key bit is encoded on the basis of the qubit (that is, $|0\rangle$ and $|1\rangle$ represent bit 0, while $|+\rangle$ and $|-\rangle$ represent bit 1), and (2) only two complementary bases can be exploited owing to its decipher method, makes it can only generate one bit in the raw key by transmitting one carrier state of any dimension. That is, SARG04 protocol which can be used to generate an oblivious key, cannot be generalized to the high-dimension version. Oppositely, as we know, BB84 protocol[18] can be generalized to the high-dimension versions[19,20,21], but they cannot be used to distribute oblivious key since they are vulnerable to the quantum memory attack[10]. Then, how to overcome this barrier?

In this paper, via an unbalanced-state technique, we design a new QKD scheme which is indeed an intermediate of BB84 and SARG04 protocols. It can not only be used to generate oblivious key, but also be generalized to its high-dimension version (detailed analysis is shown in Methods). On this basis, we propose a quantum protocol for QPQ of blocks, in which the database security is guarded by the impossibility of reliably distinguishing non-orthogonal states, while user privacy is protected by the fact that the states with identical support cannot be unambiguously discriminated. Moreover, our protocol is cheat-sensitive and loss-tolerant.

Results

Here, we give a quantum protocol for QPQ of blocks, which allows the user to retrieve an l-bit entry from database in one query. Our protocol is based on a variant of multi-level BB84 protocol in which the carrier states are transmitted with different probabilities.

Proposed protocol for QPQ of blocks. Let $d = 2^l$, then $B_1=\{|j\rangle\}_{j=0}^{d-1}$ and $B_2=\left\{|\bar{j}\rangle=\frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}\omega^{jk}|k\rangle\right\}_{j=0}^{d-1}$ are two complementary orthogonal bases for d-level quantum system, where $\omega=e^{\frac{2\pi i}{d}}$. The carrier states adopted in our protocol are chosen from the bases B_1 and B_2, and $|j\rangle(|\bar{j}\rangle)$ represents an l-bit string, i.e., the binary representation of j. A detailed description of the protocol is as follows:

(R1) Alice sends Bob a long sequence of qudits which are chosen from basis B_1 or B_2, and among them, each state in $\left\{|0\rangle,|1\rangle,\cdots,\left|\frac{d}{2}-1\right\rangle,\left|\overline{\frac{d}{2}}\right\rangle,\cdots,|\overline{d-1}\rangle\right\}$ is prepared with probability $\frac{\alpha}{d}$, while each in $\left\{|\bar{0}\rangle,|\bar{1}\rangle,\cdots,\left|\overline{\frac{d}{2}-1}\right\rangle,\left|\frac{d}{2}\right\rangle,\cdots,|d-1\rangle\right\}$ is prepared with probability $\frac{1-\alpha}{d}$. Here, $\alpha\in\left(0,\frac{1}{2}\right)$.

(R2) Bob measures each received qudit in basis B_1 or B_2 randomly.

(R3) Bob announces in which instances he has successfully detected the qudits; the ones which are not detected are discarded.

(R4) Bob chooses some positions randomly and requires Alice to announce the states of the transmitted qudits there. Then he discards his outputs which are obtained by measuring qudits in incompatible bases, and compares the remaining ones with Alice's announcement. If the error rate is higher than a certain threshold value, or the proportions of the states $|j\rangle$ $(|\bar{j}\rangle)$ $(0\le j\le d-1)$ do not coincide with the corresponding probabilities with which they should be prepared in step (R1), the protocol terminates.

(R5) Bob announces all measurement bases he chose in step (R2).

(R6) After dropping the checking qudits, Alice and Bob share an oblivious raw key K^r successfully. Concretely, each element in K^r is corresponding to one measurement result of Bob and hence is an l-bit string entirely known to Bob. Apparently, Alice would know half of the elements in K^r by checking the measurement bases announced by Bob. It is worth noting that the raw key is determined by the receiver Bob's measurement outputs rather than Alice's state preparation, which is quite different from previous protocols.

(R7) Enough qudits should be transmitted so that the number of elements in K^r equals to kN (k is a security parameter, and we will discuss its value later). The raw key is cut into k substrings in the way that each substring has N elements. These substrings are added bitwise (see Fig. 1) to obtain the final key K^f, and Alice's information on K^f is reduced to roughly one element after that. This process is similar to that in Ref. 10.

(R8) If Alice does not know any element in K^f finally, the protocol fails.

(R9) Suppose that Alice knows the mth element K_m^f in K^f and wants the nth entry X_n in database, she announces the number $s = m - n$. Then Bob encrypts the database by bitwise adding K^f, shifted by s elements, and sends the encrypted database to Alice. Obviously, X_n is encrypted by K_m^f and consequently can be correctly recovered by Alice.

Features of our protocol. Our protocol is somewhat like the high-dimension version of J-protocol, but some nontrivial modifications are necessary. On one hand, the oblivious raw key in J-protocol is

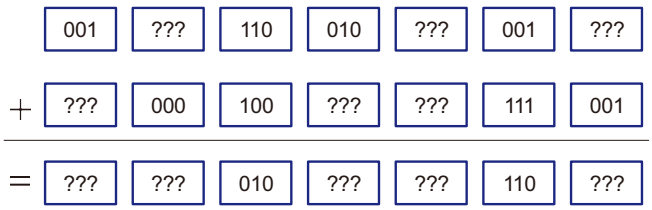

Figure 1 | (Gao): Bitwise adding (taking $l = 3$ for example) — an adequate classical postprocessing to reduce Alice's knowledge on the final key. Clearly, Alice's information on the sum string is lower than that on the initial strings. Question marks symbolize Alice's unknown bits.

determined by the qudit sender's state preparation, but in our protocol it is determined by the receiver Bob's measurement results (see step (R6)) and hence is entirely known to Bob. On the other hand, the raw key bits are encoded onto the states of the qudits in our protocol while they are encoded onto the bases of the qudits in J-protocol. For these reasons, our protocol can not only resist the quantum memory attack by Bob, but also distribute l adjacent bits in K^r by transmitting one qudit, which ensures the realization of "QPQ of blocks".

Our protocol is loss-tolerant. Note that the qudits in $B_1 \cup B_2$ are linearly dependent and cannot be unambiguously discriminated by Bob[22,23]. Furthermore, Alice never declares the correct measurement bases in our protocol. It means that Bob cannot make sure the state (or basis) of the qudit by any method. Therefore even in the shield of channel loss, the information Bob could obtain is inconclusive and it would be subsequently compressed in the bitwise-adding phase. Hence, Bob cannot cheat by lying in step (R3) (i.e., announcing that a qudit is lost when he gets an unwanted result) to obtain virtual benefit.

Following the protocol, Alice will know on average $\bar{n} = N\left(\frac{1}{2}\right)^k$ elements in K^r after step (R7). And P_0, the probability that she does not know any element at all and the protocol fails, is $\left[1-\left(\frac{1}{2}\right)^k\right]^N$. By choosing an appropriate value of k, we can ensure both $\bar{n} \ll N$ and small P_0 (see Table 1), which implies a successful execution of the protocol. For example, for a database with 10^5 entries, $k = 15$ is an appropriate choice which provides Alice with $\bar{n} = 3.05$ known elements in the final key on average, whereas the probability of failure is only about 4.7%. On the other hand, even if Alice knows $\bar{n} > 1$ elements in K^r, she can only obtain one chosen entry of the database, because the other $\bar{n}$-1 entries known to her will be at random positions in the database.

Now, we study some general attacks and analyze the security of our protocol.

Database security. To elicit more entries from database, Alice has to know more elements (i.e., Bob's measurement outputs) in the raw key K^r. For this purpose, Alice generally prepares bipartite entangled states $|\Psi\rangle_{AB}$, keeps systems A by herself, and sends systems B to Bob in step (R1). Then after Bob announces the measurement bases, Alice infers Bob's measurement results by measuring corresponding systems A. Without loss of generality, we assume that $|\Psi\rangle_{AB}$ can be expressed as

$$|\Psi\rangle_{AB} = \sum_{j=0}^{d-1} a_j \left|\beta_j\right\rangle_A |j\rangle_B, \tag{1}$$

$$= \sum_{k=0}^{d-1} b_k |\gamma_k\rangle_A \left|\bar{k}\right\rangle_B, \tag{2}$$

where $|j\rangle \in B_1$ and $\left|\bar{k}\right\rangle \in B_2$.

Let's discuss the conditions for Alice to pass Bob's checking. When being requested to declare the state of one qudit in step (R4), Alice first measure corresponding system A, i.e., discriminating $\left\{\left|\beta_j\right\rangle\right\}_{j=1}^d$ or $\{|\gamma_k\rangle\}_{k=1}^d$ randomly. If the measurement result is $|\beta_j\rangle$ ($|\gamma_k\rangle$), she announces $|j\rangle$ $\left(\left|\bar{k}\right\rangle\right)$ to Bob. To give correct qudit state, system A need to be discriminated perfectly no matter which basis Bob chooses, that is, the following conditions must hold.

(i) $\langle\beta_j|\beta_k\rangle = \delta_{jk}$, for $j,k = 0,1,\cdots,d-1$.

(ii) $\langle\gamma_j|\gamma_k\rangle = \delta_{jk}$, for $j,k = 0,1,\cdots,d-1$.

Meanwhile, to satisfy the required proportions of the qudits, the following conditions must hold.

(iii) $|a_0|^2 = |a_1|^2 = \cdots = \left|a_{\frac{d}{2}-1}\right|^2 = \frac{2\alpha}{d}$, $\left|a_{\frac{d}{2}}\right|^2 = \left|a_{\frac{d}{2}+1}\right|^2 = \cdots = |a_{d-1}|^2 = \frac{2-2\alpha}{d}$.

(iv) $|b_0|^2 = |b_1|^2 = \cdots = \left|b_{\frac{d}{2}-1}\right|^2 = \frac{2-2\alpha}{d}$, $\left|b_{\frac{d}{2}}\right|^2 = \left|b_{\frac{d}{2}+1}\right|^2 = \cdots = |b_{d-1}|^2 = \frac{2\alpha}{d}$.

Since $\left|\bar{k}\right\rangle = \frac{1}{\sqrt{d}}\sum_{j=0}^{d-1} \omega^{jk}|j\rangle$, equation (2) can be written as

$$|\Psi\rangle_{AB} = \frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}\left\{\sum_{k=0}^{d-1} b_k \omega^{jk}|\gamma_k\rangle_A\right\}|j\rangle_B. \tag{3}$$

If conditions (ii) and (iv) hold, by comparing equation (1) with equation (3), we have

$$|a_0|^2 = |a_1|^2 = \cdots = |a_{d-1}|^2 = \frac{1}{d}. \tag{4}$$

It is clearly contradict with condition (iii). In other words, entangled state which satisfies the above four conditions simultaneously is nonexistent. To avoid being detected, at least two entangled states are needed. One satisfies conditions (i) and (iii) (corresponding to the situation that the carrier states are chosen from B_1), the other satisfies conditions (ii) and (iv).

Therefore, Alice can prepare a long sequence of entangled states which are randomly in state

$$|\Psi_1\rangle = \sum_{j=0}^{\frac{d}{2}-1}\sqrt{\frac{2\alpha}{d}}\left|\phi_j\right\rangle_A |j\rangle_B + \sum_{j=\frac{d}{2}}^{d-1}\sqrt{\frac{2-2\alpha}{d}}\left|\phi_j\right\rangle_A |j\rangle_B \tag{5}$$

or

$$|\Psi_2\rangle = \sum_{j=0}^{\frac{d}{2}-1}\sqrt{\frac{2-2\alpha}{d}}\left|\phi_j\right\rangle_A |\bar{j}\rangle_B + \sum_{j=\frac{d}{2}}^{d-1}\sqrt{\frac{2\alpha}{d}}\left|\phi_j\right\rangle_A |\bar{j}\rangle_B, \tag{6}$$

where $\langle\phi_j|\phi_k\rangle = \delta_{jk}$, and sends systems B to Bob in step (R1) while keeping systems A by herself. To announce the state of one qudit correctly in step (R4), she first measures corresponding system A in basis $\left\{\left|\phi_j\right\rangle\right\}_{j=0}^{d-1}$. If the measurement result is $|\phi_j\rangle$ and she prepares $|\Psi_1\rangle$ ($|\Psi_2\rangle$) in this position, she announces $|j\rangle$ ($|\bar{j}\rangle$) to Bob. Clearly, this kind of attack cannot be detected by Bob.

Table 1 | Possible choices of k for different database sizes N, as well as the failure probability P_0 and expected number of entries $\bar{n}$ an honest Alice would gain from database

N	10^3	5×10^3	10^4	5×10^4	10^5	10^6	10^8
k	8	11	12	14	15	18	25
$\bar{n}$	3.91	2.44	2.44	3.05	3.05	3.81	2.98
P_0	0.020	0.087	0.087	0.047	0.047	0.022	0.051

Now, we discuss the maximal information Alice could gain by this attack. Without loss of generality, we suppose that Alice prepares $|\Psi_2\rangle$ in some position. Then, she can select different strategies to obtain Bob's measurement result after step (R5). If the basis Bob announced in step (R5) is B_2 (which appears with probability $\frac{1}{2}$), Alice measures system A in basis $\left\{\left|\phi_j\right\rangle\right\}_{j=0}^{d-1}$ and hence gets Bob's output completely (see equation(6)). If the basis announced by Bob is B_1 (which also appears with probability $\frac{1}{2}$), since $|\bar{j}\rangle=\frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}\omega^{jk}|k\rangle$, we have

$$|\Psi_2\rangle=\frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}\left|\varphi_j\right\rangle_A|j\rangle_B, \tag{7}$$

where $\left|\varphi_j\right\rangle=\sum_{k=0}^{\frac{d}{2}-1}\sqrt{\frac{2-2\alpha}{d}}\omega^{jk}|k\rangle+\sum_{k=\frac{d}{2}}^{d-1}\sqrt{\frac{2\alpha}{d}}\omega^{jk}|k\rangle$. Hence, system A would randomly collapse to one of the linearly independent symmetric states $\left\{\left|\varphi_j\right\rangle\right\}_{j=0}^{d-1}$ when Bob measures system B in basis B_1. Therefore, to infer Bob's measurement result, Alice need to make an unambiguous discrimination on the symmetric states $\left\{\left|\varphi_j\right\rangle\right\}_{j=0}^{d-1}$[24] with the maximum average success probability being $d\times min\left\{\frac{2\alpha}{d},\frac{2-2\alpha}{d}\right\}$, i.e., 2α. Consequently, Alice can obtain at most $n_A=N\left(\frac{1}{2}+\alpha\right)^k$ entries from database by this means. When α is small, Alice's advantage decreases distinctly. Moreover, with the growth of database size N, the ratio $\frac{n_A}{N}$ which represents the percentage of the entries Alice would obtain from database, decreases rapidly (see Table 2). Take $\alpha=0.1$, $N=10^5$ for example, dishonest user can get at most 40 entries which occupy only 0.05% of the total entries. It is very little relation to database security for such a complex attack.

Now, we consider a more general attack. For those positions where Alice prepares $|\Psi_1\rangle$ ($|\Psi_2\rangle$) while Bob's measurement basis is B_2 (B_1), Alice can postpone the measurement on corresponding systems A held by herself until the very end of the protocol, so that she can know which of them contribute to an element in the final key K^f. Then she can perform a joint measurement on them to guess the final added value in K^f in the way similar to that in Refs. 10, 12. The maximal success probability of Alice's joint unambiguous state discrimination (USD) measurement on m systems declines rapidly with the increase of m even in the simplest situation when $d=2$ (see Fig. 2), which means a high security degree for the database security under this kind of attack.

User privacy. If Bob is dishonest and wants to reveal the address Alice is retrieving, he has to make clear the question whether the measurement basis announced by himself is coincide with the basis of the qudit (i.e., whether the corresponding element in K^r is conclusive in Alice's view) for each received qudit. Therefore, he has to devote himself to judging which basis the qudit is chosen from, i.e., discriminating two equally likely mixed states

$$\rho_1=\sum_{j=0}^{\frac{d}{2}-1}\frac{2\alpha}{d}|j\rangle\langle j|+\sum_{j=\frac{d}{2}}^{d-1}\frac{2-2\alpha}{d}|j\rangle\langle j|, \tag{8}$$

and

$$\rho_2=\sum_{j=0}^{\frac{d}{2}-1}\frac{2-2\alpha}{d}|\bar{j}\rangle\langle\bar{j}|+\sum_{j=\frac{d}{2}}^{d-1}\frac{2\alpha}{d}|\bar{j}\rangle\langle\bar{j}|. \tag{9}$$

ρ_1 and ρ_2 cannot be unambiguously discriminated because they have the same support[22,23,25]. However, the protocol is not perfectly concealing because $\rho_1\neq\rho_2$. Bob can make a minimal error discrimination (MED) on them, with the minimal error probability P_E[26] being

$$P_E=\frac{1}{2}\left(1-\frac{1}{2}tr|\rho_2-\rho_1|\right). \tag{10}$$

By simple computation, we find that q_{st}, the element in the sth row and tth column of matrix ρ_2-ρ_1, satisfies

$$q_{st}=\begin{cases}\frac{1-2\alpha}{d}, & \text{if } s=t<\frac{d}{2}\\ \frac{2\alpha-1}{d}, & \text{if } s=t\geq\frac{d}{2}\\ 0, & \text{if } s-t \text{ is nonzero and even}\\ \frac{4(1-2\alpha)}{d^2(1-\omega^{s-t})}, & \text{if } s-t \text{ is odd}\end{cases} \tag{11}$$

for $s,t=0,1,\cdots,d-1$. To keep things straightforward, we depict the relationship between P_E and α, l in Fig. 3. Obviously, the minimal

Table 2 | Alice's advantages for database of different sizes. Here, $\alpha=0.1$

N	10^3	5×10^3	10^4	5×10^4	10^5	10^6	10^8
$\bar{n}$	3.91	2.44	2.44	3.05	3.05	3.81	2.98
n_A	16.80	18.14	21.77	39.18	47.02	101.56	284.30
$\frac{n_A}{N}$	0.0168	0.0036	0.0022	0.0008	0.0005	0.0001	2.8×10^{-6}

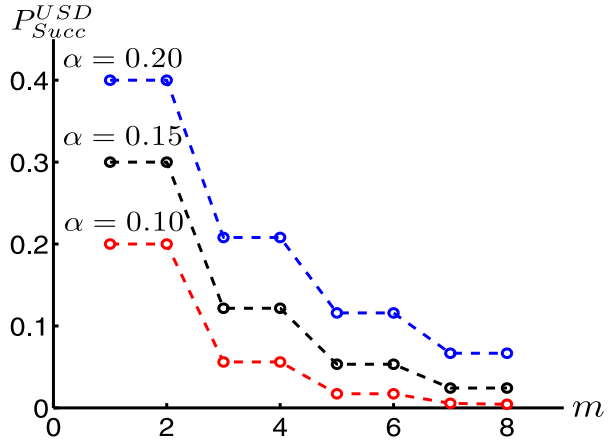

Figure 2 | (Gao): For $d = 2$, the maximal success probability P_{succ}^{USD} of Alice's joint unambiguous state discrimination (USD) on m systems declines rapidly with the increase of m.

error probability P_E increases with the growth of l and α. Even in the most favorable situation to Bob where $l = 1$ and α is very close to zero, he would make a mistake in the MED measurement on each received qudit with a probability no less than 14.64%. Obviously, it is very difficult for Bob to get Alice's privacy after the bitwise adding phase in step (R7), thus assuring the user privacy in our protocol.

It is worth noting that Bob's attack would be discovered by Alice, because the qudit would be disturbed inevitably in the MED measurement and subsequently Bob could not always output correct value in K^r. Take $d = 2$ for example, the carrier states are chosen from $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. Here, both $|0\rangle$ and $|-\rangle$ are prepared with probability $\frac{\alpha}{2}$, while both $|1\rangle$ and $|+\rangle$ are prepared with probability $\frac{1-\alpha}{2}$. Hence, $\rho_1 = \alpha|0\rangle\langle 0| + (1-\alpha)|1\rangle\langle 1|$, $\rho_2 = (1-\alpha)|+\rangle\langle +| + \alpha|-\rangle\langle -|$. The minimal error probability P_E is $\frac{2-\sqrt{2}+2\sqrt{2}\alpha}{4}$, which is larger than 14.64% for all $\alpha \in \left(0, \frac{1}{2}\right)$, and the MED measurement operators[26] are $\Pi_1 = |\xi_1\rangle\langle\xi_1|$, $\Pi_2 = |\xi_2\rangle\langle\xi_2|$, where

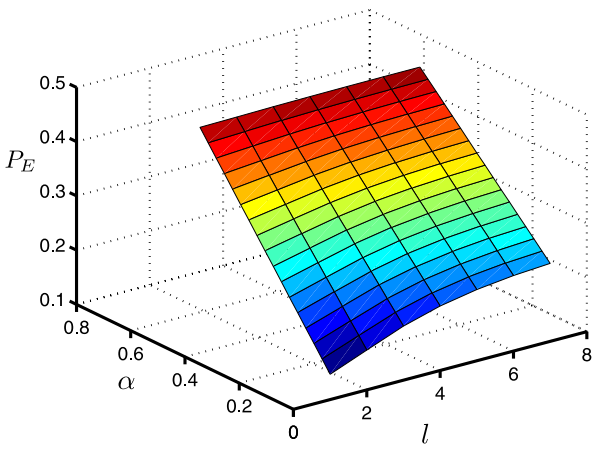

Figure 3 | (Gao): The influence of parameter α and block length l on P_E. Here, P_E is the minimal error probability of Bob's minimal error discrimination on each qudit.

$$|\xi_1\rangle = \frac{1}{\sqrt{4-2\sqrt{2}}}\left[\left(1-\sqrt{2}\right)|0\rangle + |1\rangle\right], \tag{12}$$

$$|\xi_2\rangle = \frac{1}{\sqrt{4+2\sqrt{2}}}\left[\left(1+\sqrt{2}\right)|0\rangle + |1\rangle\right]. \tag{13}$$

Therefore, the minimal error discrimination of ρ_1 and ρ_2 is equivalent to measuring the received qubit in basis $\{|\xi_1\rangle, |\xi_2\rangle\}$. Without loss of generality, we suppose that the qubit sent by Alice is $|0\rangle$ and corresponding measurement basis announced by Bob is $\{|0\rangle, |1\rangle\}$, then Bob should output 0 in the generation of raw key to avoid being detected. However, since both $|0\rangle$ and $|1\rangle$ can collapse to $|\xi_1\rangle$ or $|\xi_2\rangle$ in the MED measurement (see equations (12,13)), Bob could not output correct result all the time after making the MED measurement on it. His attack would be discovered afterwards when offering false entry to Alice. It indicates that our protocol is also cheat-sensitive.

Discussion

Compared to QPQ of single bit, QPQ of blocks is not only a more realistic model for application but also a nontrivial idea in security. In this paper, based on a variant of high-dimension BB84 scheme, we propose a protocol to realize QPQ of blocks. Our protocol is cheat-sensitive and loss-tolerant. Besides, the security of our protocol is well protected and the advantages of both sides are strictly limited by α. Furthermore, parameter α can be changed to balance the advantage between user privacy and database security to satisfy different application requirements. Concretely, in the scenario where the user privacy is emphasized, α should be given a larger value; if the database security is more concerned, α should be assigned a smaller one. Moreover, in the situation where "fairness to both sides" is pursued, by making a trade-off between user privacy and database security, we can roughly estimate a proper value for α (see Supplementary information). From an experimental viewpoint, the d-dimension carrier state in our protocol can be prepared with current technology, e.g., a single photon distributed over d orthogonal modes as considered in Refs. 27, 28. Recently, some high-dimension BB84-like quantum key distribution protocol has been demonstrated[29], which also provides fundamental assurance to the application of our protocol.

Methods

By using a special technique in BB84 protocol, i.e., transmitting the carrier states $|0\rangle$, $|1\rangle$,$|+\rangle$, $|-\rangle$ with different probabilities $\frac{\alpha}{2}, \frac{1-\alpha}{2}, \frac{1-\alpha}{2}, \frac{\alpha}{2}$ $\left(0 < \alpha < \frac{1}{2}\right)$ respectively, we obtain an intermediate of BB84 and SARG04 protocols, which can be called unbalanced-state BB84 (US-BB84) protocol (see Table 3). Similar to BB84 protocol, the key bit in US-BB84 protocol is encoded on the state rather than the basis of the qubit. Obviously, the US-BB84 protocol can be generalized to its high-dimension version in the same way as BB84 does[19,20,21]. Now, we show that it can also be used to distribute an oblivious key as follows:

- (S1) Alice sends Bob a long sequence of qubits, in which *both* $|0\rangle$ *and* $|-\rangle$ *are prepared with probability* $\frac{\alpha}{2}$, *while both* $|1\rangle$ *and* $|+\rangle$ *are prepared with probability* $\frac{1-\alpha}{2}$. Here the parameter $\alpha \in \left(0, \frac{1}{2}\right)$. $|0\rangle$ and $|+\rangle$ represent bit 0, while $|1\rangle$ and $|-\rangle$ represent 1.
- (S2) Bob measures the received qubits in basis $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$ randomly.
- (S3) Bob randomly chooses some positions and requires Alice to announce the states of the transmitted qubits there. Then he discards his outputs which are obtained by measuring the qubits in incompatible bases, and compares the remaining ones with Alice's announcement. If the error rate is higher than a certain threshold value, or *the proportions* $p(|0\rangle)$, $p(|1\rangle)$, $p(|+\rangle)$, $p(|-\rangle)$ *do not coincide with the probabilities* $\frac{\alpha}{2}, \frac{1-\alpha}{2}, \frac{1-\alpha}{2}, \frac{\alpha}{2}$, the protocol terminates. Here $p(|0\rangle)$, $p(|1\rangle)$, $p(|+\rangle)$ and $p(|-\rangle)$ represent the proportions of the states $|0\rangle$, $|1\rangle$, $|+\rangle$, $|-\rangle$ in Bob's remaining outputs.

Table 3 | Comparison of BB84, SARG04 and US-BB84 protocols. The last two columns show that only the high-dimension US-BB84 protocol can be used to realize QPQ of blocks

QKD protocol	state preparation	coding style	generalized to an high-dimension version	used to generate an oblivious key
BB84	randomly chosen ($\alpha = 0.5$)	state	✓	×
SARG04	similar to $\alpha = 0$	basis	×	✓
US-BB84	$0 < \alpha < 0.5$	state	✓	✓

- (S4) Bob announces all measurement bases he chose.
- (S5) After dropping the checking qubits, Alice and Bob successfully share an oblivious key K^r, which is composed of Bob's measurement outputs and hence is entirely known to Bob. Obviously, Alice would know half of the bits in K^r by checking the measurement bases announced by Bob.

As shown above, Bob knows the oblivious key entirely, but he cannot reliably infer which bits are known to Alice, because the carrier states are linearly dependent and cannot be unambiguously discriminated. On the other hand, we now show that, owing to the checking of the proportions of carrier states in step (S3), Alice could not obtain the whole key even using entanglement-measurement attack. Generally, Alice can prepare bipartite entangled states in the following forms

$$|\Psi\rangle = a_0|\varphi_0\rangle_A|0\rangle_B + a_1|\varphi_1\rangle_A|1\rangle_B \tag{14}$$

$$= b_0|\gamma_0\rangle_A|+\rangle_B + b_1|\gamma_1\rangle_A|-\rangle_B, \tag{15}$$

and sends systems B to Bob in step (S1). When being requested to declare the state of one qubit in step (S3), Alice first measures system A, i.e., discriminating the states $\{|\varphi_i\rangle\}_{i=0}^1$ or $\{|\gamma_i\rangle\}_{i=0}^1$ randomly. Then if the measurement result is $|\varphi_0\rangle$ ($|\varphi_1\rangle$), she announces $|0\rangle$ ($|1\rangle$) to Bob; if the measurement result is $|\gamma_0\rangle$ ($|\gamma_1\rangle$), she announces $|+\rangle$ ($|-\rangle$) to Bob. Note that in step (S3), Bob's measurement result would be thrown away if he measures the qubit in basis $\{|0\rangle, |1\rangle\}$ ($\{|+\rangle, |-\rangle\}$) while Alice announces the state $|+\rangle$ or $|-\rangle$ ($|0\rangle$ or $|1\rangle$).

Take $\alpha = 0.1$ for example, to pass Bob's checking in step (S3), Alice has to ensure that (1) she can always declare the states of transmitted qubits correctly, which means that $\langle\varphi_0|\varphi_1\rangle = 0$ and $\langle\gamma_0|\gamma_1\rangle = 0$, and (2) after Bob discards the results which are obtained by measuring qubits in incompatible bases, the states $|0\rangle, |1\rangle, |+\rangle, |-\rangle$ should occupy 10%, 40%, 40%, 10% of the remaining ones respectively. Therefore, $|\Psi\rangle$ must have the following forms

$$|\Psi\rangle = \sqrt{0.2}|\varphi_0\rangle_A|0\rangle_B + \sqrt{0.8}|\varphi_0^\perp\rangle_A|1\rangle_B, \tag{16}$$

$$= \sqrt{0.8}|\gamma_0\rangle_A|+\rangle_B + \sqrt{0.2}|\gamma_0^\perp\rangle_A|-\rangle_B. \tag{17}$$

By simple computation, we can find that equations (16) and (17) cannot be satisfied simultaneously. That is, there is no such an entangled state that Alice could pass Bob's checking in step (S3).

However, Alice can prepare a long sequence of entangled states randomly in

$$|\Psi\rangle_1 = \sqrt{0.2}|\varphi_0\rangle_A|0\rangle_B + \sqrt{0.8}|\varphi_0^\perp\rangle_A|1\rangle_B \tag{18}$$

or

$$|\Psi\rangle_2 = \sqrt{0.8}|\gamma_0\rangle_A|+\rangle_B + \sqrt{0.2}|\gamma_0^\perp\rangle_A|-\rangle_B, \tag{19}$$

and sends systems B to Bob in step (S1). When being asked to announce the state of one qubit in step (S3), if Alice prepared $|\Psi\rangle_1$ there, she measures system A in basis $\{|\varphi_0\rangle, |\varphi_1\rangle\}$, then announces $|0\rangle$ ($|1\rangle$) to Bob when the measurement output is $|\varphi_0\rangle$ ($|\varphi_1\rangle$). In this case, Bob would discard his measurement result if he measures this qubit in basis $\{|+\rangle, |-\rangle\}$. The situation is similar when Alice prepares $|\Psi\rangle_2$. Obviously, Alice can pass Bob's checking in this way.

Then, how many bits can be gained by Alice via this attack? Without loss of generality, we assume that Alice prepares $|\Psi\rangle_1$ and sends system B to Bob. If the measurement basis anouced by Bob in step (S4) is $\{|0\rangle, |1\rangle\}$ (which occurs with probability $\frac{1}{2}$), Alice can undoubtedly obtain this key bit by measuring system A in basis $\{|\varphi_0\rangle, |\varphi_0^\perp\rangle\}$ (see equation (18)); if the announced basis is $\{|+\rangle, |-\rangle\}$ (which also occurs with probability $\frac{1}{2}$), note that $|\Psi\rangle_1$ can also be written as

$$|\Psi\rangle_1 = \frac{1}{\sqrt{2}}\left\{\sqrt{0.2}|\varphi_0\rangle + \sqrt{0.8}|\varphi_0^\perp\rangle\right\}_A|+\rangle_B + \frac{1}{\sqrt{2}}\left\{\sqrt{0.2}|\varphi_0\rangle - \sqrt{0.8}|\varphi_0^\perp\rangle\right\}_A|-\rangle_B. \tag{20}$$

Alice can infer the key bit by unambiguously discriminating the non-orthogonal states $\sqrt{0.2}|\varphi_0\rangle + \sqrt{0.8}|\varphi_0^\perp\rangle$ and $\sqrt{0.2}|\varphi_0\rangle - \sqrt{0.8}|\varphi_0^\perp\rangle$ with maximal average success probability being 0.2. That is, Alice can obtain 60% (a little larger than 50% an honest Alice could obtain) of the key bits at most. In fact, Alice could not obtain the whole key as long as $\alpha \neq \frac{1}{2}$.

1. Chor, B., Goldreich, O., Kushilevitz, E. & Sudan, M. Private information retrieval. In *Proceedings of the 36th Annual Symposium on Foundations of Computer Science, Milwaukee, Wisconsin, U.S.A.* Los Alamitos: IEEE Comp. Soc. Press, pp. 41–51 (Oct. 23–25 1995).
2. Gentner, Y., Ishai, Y., Kushilevitz, E. & Malkin, T. Protecting data privacy in private information retrieval schemes. *J. Comput. Syst. Sci.* **60**, 592–629 (2000).
3. Shor, P. W. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science, Santa Fe, New Mexico, U.S.A.* Los Alamitos: IEEE Comp. Soc. Press, pp. 124–134 (Nov. 20–22 1994).
4. Grover, L. K. A fast quantum mechanical algorithm for database search. In *Proceedings of the 28th Annual ACM Symposium on Theory of Computing, Philadephia, Pennsylvania, U.S.A.* New York: ACM Press, pp. 212–219 (May 22–24 1996).
5. Gisin, N., Ribordy, G., Tittel, W. & Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **74**, 145–195 (2002).
6. Lo, H.-K. Insecurity of quantum secure computations. *Phys. Rev. A* **56**, 1154–1162 (1997).
7. Giovannetti, V., Lloyd, S. & Maccone, L. Quantum Private Queries. *Phys. Rev. Lett*, **100**, 230502 (2008).
8. Giovannetti, V., Lloyd, S. & Maccone, L. Quantum Private Queries: securety analysis. *IEEE T. Inform. Theory* **56**, 3465–3477 (2010).
9. Olejnik, L. Secure quantum private information retrieval using phase-encoded queries. *Phys. Rev. A* **84**, 022313 (2011).
10. Jakobi, M. *et al*. Practicle private database queries based on a quantum-key-distribution protocol. *Phys. Rev. A* **83**, 022301 (2011).
11. Scarani, V., Acín, A., Ribordy, G. & Gisin, N. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Phys. Rev. Lett.* **92**, 057901 (2004).
12. Gao, F., Liu, B., Wen, Q. Y. & Chen, H. Flexible quantum private queries based on quantum key distribution. *Opt. Express* **20**, 17411–17420 (2012).
13. Panduranga Rao, M. V. & Jakobi M. Towards communication-efficient quantum oblivious key distribution. *Phys. Rev. A* **87**, 012331 (2013).
14. Zhang, J. L., Guo, F. Z., Gao, F., Liu, B. & Wen, Q. Y. Private database queries based on counterfactual quantum key distribution. *Phys. Rev. A* **88**, 022334 (2013).
15. Fred Fung, C.-H., Ma, X. F. & Chau, H. F. Practical issues in quantum-key-distribution postprocessing. *Phys. Rev. A* **81**, 012318 (2010).
16. Ma, X. F., Fred Fung, C.-H., Boileau, J. C. & Chau, H. F. Universally composable and customizable post-processing for practical quantum key distribution. *Comput. Secur.* **30**, 172–177(2011).
17. Chor, B., Goldreich, O., Kushilevitz, E. & Sudan, M. Private Information Retrieval. *J. ACM* **45**, 965 (1998).
18. Bennett, C, H & Brassard, G. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE Int. Conf. on Computers, Systems and Signal Processing, Bangalore, India* New York: IEEE press, pp. 175–179 (Dec. 10–12 1984).
19. Bechmann-Pasquinucci, H. & Tittel, W. Quantum cryptography using larger alphabets. *Phys. Rev. A* **61**, 062308 (2000).
20. Bourennane, M., Karlsson, A. & Björk, G. Quantum key distribution using multilevel encoding. *Phys. Rev. A* **64**, 012306 (2001).
21. Cerf, N. J., Bourennane, M., Karlsson, A. & Gisin, N. Security of quantum key distribution using d-level systems. *Phys. Rev. Lett.* **88**, 127902 (2002).
22. Herzog, U. & Bergou, J, A. Optimum unambiguous discrimination of two mixed quantum states. *Phys. Rev. A* **71**, 050301 (2005).
23. Chefles, A. Unambiguous Discrimination Between Linearly-Independent Quantum States. e-print arXiv: quant-ph/9807022v1.

24. Chefles, A. & Barnett, S. M. Optimum unambiguous discrimination between linearly independent symmetric states. *Phys. Lett. A* **250**, 223–229 (1998).
25. Raynal, P. Unambiguous State Discrimination of two density matrices in Quantum Information Theory. e-print arXiv: quant-ph/0611133.
26. Bergou, J. A. Discrimination of quantum states. *J. Mod. Opt.* **57**, 160–180 (2010).
27. Massar, S. Quantum fingerprinting with a single particle. *Phys. Rev. A* **71**, 012310 (2005).
28. Garcia-Escartin, J. C. & Chamorro-Posada, P. SWAP test Hong-Ou-Mandel effect are equivelent. *Phys. Rev. A* **87**, 052330 (2013).
29. Etcheverry, S. *et al*. Quantum key distribution session with 16-dimensional photonic states. *Sci. Rep.* **3**, 2316 (2013).

Acknowledgments

This work is supported by NSFC (Grant Nos. 61300181, 61272057, 61202434, 61170270, 61100203, 61121061, 61202317)), Beijing Natural Science Foundation (Grant No. 4122054), Beijing Higher Education Young Elite Teacher Project (Grant Nos. YETP0475, YETP0477), the Program for Science & Technology Innovation Talents in Universities of Henan Province (Grant No. 13HASTIT042), the Young Key Teacher Foundation of Henan Province's Universities (Grant No. 2012GGJS-157), the Natural Science Foundation of Henan Province (Grant Nos. 132300410316, 132300410313), and the Natural Science Foundation of Education Bureau of Henan Province (Grant Nos. 12B120009, 13A110800, 13B110150).

Author contributions

Q.Y.W., F.G. and T.Y.W. analyzed the previous QPQ protocols. All authors designed the new protocol. C.Y.W. and F.G. analyzed its features and security, wrote the main manuscript text and prepared all figures. All authors reviewed the manuscript.

Additional information

Supplementary information accompanies this paper at http://www.nature.com/scientificreports

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

How to cite this article: 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. *Sci. Rep.* **4**, 7537; DOI:10.1038/srep07537 (2014).