1-1-2016

Comment on "secure quantum private information retrieval using phase-encoded queries"

Runhua Shi
Anhui University, rshi@uow.edu.au

Yi Mu
University of Wollongong, ymu@uow.edu.au

Hong Zhong
Anhui University

Shun Zhang
Anhui University

Comment on "secure quantum private information retrieval using phase-encoded queries"

Abstract

2016 American Physical Society.In this Comment, we reexamine the security of phase-encoded quantum private query (QPQ). We find that the current phase-encoded QPQ protocols, including their applications, are vulnerable to a probabilistic entangle-and-measure attack performed by the owner of the database. Furthermore, we discuss how to overcome this security loophole and present an improved cheat-sensitive QPQ protocol without losing the good features of the original protocol.

Disciplines

Engineering | Science and Technology Studies

Publication Details

Shi, R., Mu, Y., Zhong, H. & Zhang, S. (2016). Comment on "secure quantum private information retrieval using phase-encoded queries". Physical Review A - Atomic, Molecular, and Optical Physics, 94 (6), 066301-1-066301-4.

Comment on "Secure quantum private information retrieval using phase-encoded queries"

Run-hua Shi,[1,2,*] Yi Mu,[2] Hong Zhong,[1] and Shun Zhang[1]
[1]*School of Computer Science and Technology, Anhui University, Hefei City 230601, China*
[2]*Centre for Computer and Information Security Research, School of Computing and Information Technology, University of Wollongong, Wollongong, New South Wales 2522, Australia*
(Received 1 May 2016; published 27 December 2016)

In this Comment, we reexamine the security of phase-encoded quantum private query (QPQ). We find that the current phase-encoded QPQ protocols, including their applications, are vulnerable to a probabilistic entangle-and-measure attack performed by the owner of the database. Furthermore, we discuss how to overcome this security loophole and present an improved cheat-sensitive QPQ protocol without losing the good features of the original protocol.

DOI: 10.1103/PhysRevA.94.066301

I. INTRODUCTION

With the rapid development of quantum computations and quantum communications, classical cryptography, including symmetric cryptography and public key cryptography, is facing enormous threats and challenges. On the other hand, quantum cryptography brings a new dawn for information security research.

Quantum cryptography can provide the unconditional security, which is guaranteed by physical principles of quantum mechanics. Compared to classical cryptography, the most important advantage is that an eavesdropper or attacker can easily be detected by using the characteristics of quantum mechanics.

Private query is a special privacy-preserving problem [1,2], which involves two parties, a user Alice and a server Bob where Alice wants to obtain an element of the database privately held by Bob, but she does not want Bob to know which element she is interested in, and in turn, Bob wants to limit Alice's information about the other elements, that is, Alice cannot get other elements except the one she wanted in the database.

In 2007, Giovannetti *et al.* [3] first presented a cheat-sensitive quantum protocol to solve the private query problem. Compared to the classical related protocols, their quantum private query (QPQ) protocol achieves an exponential reduction both in communication complexity and in computational complexity. In 2011, Olejnik further proposed a phase-encoded QPQ protocol [4]. In comparison with the original QPQ protocol [3], the phase-encoded QPQ protocol displays two prominent advantages: lower communication cost and better implementability. Due to its good properties, there are lots of important applications of phase-encoded QPQ especially in some privacy-preserving settings, such as oblivious set-member decision [5], private set intersection [6], secure data mining [7], and so on.

However, in this Comment, we find a serious security problem for all current quantum protocols based on the phase-encoded QPQ, that is, these protocols are vulnerable to a probabilistic entangle-and-measure attack performed by the owner of the database. Furthermore, we present improvements to overcome this security loophole.

II. REVIEW OF PHASE-ENCODED QPQ

Here, we simply review the original phase-encoded QPQ presented by Olejnik [4]. Suppose that Bob privately owns an N-element database: $d(i)$ for $i = 0$ to $N-1$, where $d(i) \in \{0,1\}$ and Alice wants to obtain the ith element of the database. For this, Alice sends a single query state $|\psi\rangle = \frac{|0\rangle+|i\rangle}{\sqrt{2}}$ to Bob through a quantum channel. Then Bob performs an oracle operator U on the query state $|\psi\rangle$ where the operator U is defined by

$$U = \begin{pmatrix} (-1)^{d(0)} & & & \\ & (-1)^{d(1)} & & \\ & & \ddots & \\ & & & (-1)^{d(N-1)} \end{pmatrix}, \tag{1}$$

$$|\Psi\rangle = \frac{|0\rangle + |i\rangle}{\sqrt{2}} \xrightarrow{U} |\varphi\rangle, \tag{2}$$

$$|\varphi\rangle = \frac{|0\rangle + (-1)^{d(i)}|i\rangle}{\sqrt{2}}. \tag{3}$$

Clearly,

$$|\varphi\rangle = \begin{cases} \frac{|0\rangle+|i\rangle}{\sqrt{2}}, & \text{if } d(i) = 0, \\ \frac{|0\rangle-|i\rangle}{\sqrt{2}}, & \text{if } d(i) = 1. \end{cases} \tag{4}$$

Furthermore, Bob sends state $|\varphi\rangle$ back to Alice. Finally, Alice gets the ith element $d(i)$ by distinguishing whether the returned state is $\frac{|0\rangle+|i\rangle}{\sqrt{2}}$ or $\frac{|0\rangle-|i\rangle}{\sqrt{2}}$.

III. ANALYSIS OF PHASE-ENCODED QPQ

Since Alice knows the value i, she can distinguish between $\frac{|0\rangle+|i\rangle}{\sqrt{2}}$ and $\frac{|0\rangle-|i\rangle}{\sqrt{2}}$ by performing a von Neumann measurement where the measurement operators are defined by

$$P_{+i} = \tfrac{1}{2}(|0\rangle\langle 0| + |0\rangle\langle i| + |i\rangle\langle 0| + |i\rangle\langle i|), \tag{5}$$

$$P_{-i} = \tfrac{1}{2}(|0\rangle\langle 0| - |0\rangle\langle i| - |i\rangle\langle 0| + |i\rangle\langle i|), \tag{6}$$

Obviously, the two measurement operators satisfy the completeness and the orthogonality, i.e.,

$$P_{+i} + P_{-i} = I, \tag{7}$$

$$P_{+i} P_{-i} = 0. \tag{8}$$

*Corresponding author: shirh@ahu.edu.cn

Furthermore, we define

$$|+i\rangle = \frac{|0\rangle + |i\rangle}{\sqrt{2}}, \tag{9}$$

$$|-i\rangle = \frac{|0\rangle - |i\rangle}{\sqrt{2}}, \tag{10}$$

Then, it will get the following equations:

$$\langle +i|P_{+i}|+i\rangle = 1, \tag{11}$$

$$\langle -i|P_{+i}|-i\rangle = 0, \tag{12}$$

$$\langle +i|P_{-i}|+i\rangle = 0, \tag{13}$$

$$\langle -i|P_{-i}|-i\rangle = 1. \tag{14}$$

Therefore, Alice can perfectly distinguish two possible returned states (i.e., $|+i\rangle$ and $|-i\rangle$). That is, the phase-encoded QPQ is correct.

In Ref. [4], the author pointed out that, if a dishonest Bob performs an intercept-and-resend attack, he might eventually succeed but not with more than a 50% chance. However, the author did not consider more attacks performed by Bob. In the following section, we will discuss a more complicated entangle-and-measure attack by a dishonest Bob as follows:

After receiving the query state, Bob first prepares an ancillary state $|0\rangle_B$ and then performs an oracle operator $\tilde{U}_f$ on the query state $|\Psi\rangle_A$ and the ancillary state $|0\rangle_B$ where the oracle operator $\tilde{U}_f$ is defined by [8,9]

$$\tilde{U}_f\colon\ |x\rangle|y\rangle \rightarrow\ |x\rangle|y \oplus f(x)\rangle. \tag{15}$$

Clearly, we can get

$$\langle y|\langle x|\tilde{U}_f^+\tilde{U}_f|x\rangle|y\rangle = \langle f(x)\oplus y|\langle x\,|x\rangle|y\oplus f(x)\rangle = 1. \tag{16}$$

That is, $\tilde{U}_f^+\tilde{U} = I$, which satisfies the unitarity.
So,

$$\begin{aligned}\tilde{U}_f|\psi\rangle_A|0\rangle_B &= \tilde{U}_f\frac{|0\rangle_A + |i\rangle_A}{\sqrt{2}}|0\rangle_B \\ &= \frac{\tilde{U}_f|0\rangle_A|0\rangle_B + \tilde{U}_f|i\rangle_A|0\rangle_B}{\sqrt{2}} \\ &= \frac{|0\rangle_A|0\oplus f(0)\rangle_B + |i\rangle_A|0\oplus f(i)\rangle_B}{\sqrt{2}} \\ &= \frac{|0\rangle_A|f(0)\rangle_B + |i\rangle_A|f(i)\rangle_B}{\sqrt{2}}.\end{aligned} \tag{17}$$

Please note that here $f(\cdot)$ is a classical function, which is usually defined as a one-to-one mapping, e.g., $f(i) = i$ in order to later steal the maximum possible information.

Furthermore, we call the resultant state $|\Phi\rangle_{AB}$, i.e., $|\Phi\rangle_{AB} = \frac{|0\rangle_A|f(0)\rangle_B + |i\rangle_A|f(i)\rangle_B}{\sqrt{2}}$, where the subscripts A and B denote quantum subsystems prepared originally by Alice and Bob, respectively. Then Bob sends the query subsystem A back to Alice and keeps the ancillary subsystem B in hand. After receiving the returned subsystem A, Alice performs a von Neumann measurement $\{P_{+i}, P_{-i}\}$ on A. Then, it will get

$$p_{+i} = {}_{AB}\langle\phi|P_{+i}\otimes I|\phi\rangle_{AB} = \tfrac{1}{2}, \tag{18}$$

$$p_{-i} = {}_{AB}\langle\phi|P_{-i}\otimes I|\phi\rangle_{AB} = \tfrac{1}{2}, \tag{19}$$

$$\frac{P_{+i}\otimes I|\phi\rangle_{AB}}{\sqrt{p_{+i}}} = \frac{|0\rangle_A + |i\rangle_A}{\sqrt{2}}\otimes\frac{|f(0)\rangle_B + |f(i)\rangle_B}{\sqrt{2}}, \tag{20}$$

$$\frac{P_{-i}\otimes I|\phi\rangle_{AB}}{\sqrt{p_{-i}}} = \frac{|0\rangle_A - |i\rangle_A}{\sqrt{2}}\otimes\frac{|f(0)\rangle_B - |f(i)\rangle_B}{\sqrt{2}}. \tag{21}$$

After the measurement the whole quantum system AB will be collapsed into state $\frac{P_{+i}\otimes I|\phi\rangle_{AB}}{\sqrt{p_{i+}}}$ or $\frac{P_{-i}\otimes I|\phi\rangle_{AB}}{\sqrt{p_{i-}}}$ with the probability of p_{+i} or p_{-i}, respectively. That is, Alice will get the measured result $\frac{|0\rangle_A+|i\rangle_A}{\sqrt{2}}$ or $\frac{|0\rangle_A-|i\rangle_A}{\sqrt{2}}$ with the same probability of $\frac{1}{2}$, respectively. However, in current phase-encoded QPQ protocols [4–6] as long as the returned system is in state $\frac{|0\rangle_A+|i\rangle_A}{\sqrt{2}}$ or $\frac{|0\rangle_A-|i\rangle_A}{\sqrt{2}}$, Alice will believe that Bob is honest. By Eqs. (20) and (21), Bob can steal the partial information about Alice's secret i [i.e., $f(i)$] with the probability of $\frac{1}{2}$ by measuring his ancillary system B afterwards, whereas Alice cannot find his cheat. For example, if $f(i) = i$, then $f(0) \neq f(i)$ $(i \neq 0)$. Accordingly, Bob can fully steal Alice's secret i with the probability of $\frac{1}{2}$, but Alice cannot detect his eavesdropping. Therefore, the current phase-encoded QPQ protocols are vulnerable to the probabilistic entangle-and-measure attack by dishonest Bob. Please note that the original QPQ [3] is not phase encoded, so Alice can easily find this cheat if she gets an orthogonal state (i.e, $\frac{|0\rangle|A(0)\rangle-|j\rangle|A(j)\rangle}{\sqrt{2}}$) rather than the real returned state (i.e, $\frac{|0\rangle|A(0)\rangle+|j\rangle|A(j)\rangle}{\sqrt{2}}$). That is, the original QPQ protocol can resist this attack [10].

In order to resist this attack, Alice can send two or more same query states to Bob and further checks whether all returned states are identical, that is, they are all in $\frac{|0\rangle+|i\rangle}{\sqrt{2}}$ (or $\frac{|0\rangle-|i\rangle}{\sqrt{2}}$). If they are not same, it will show that Bob is dishonest. However, if Alice sends multiple same query states to Bob, on the other hand, Bob can successfully perform the intercept-and-resend attack with more than a 50% chance. For example, if Alice sends two same query states (i.e., $\{\frac{|0\rangle+|i\rangle}{\sqrt{2}}, \frac{|0\rangle-|i\rangle}{\sqrt{2}}\}$) to Bob, then Bob can successfully steal Alice's secret i with $\frac{3}{4}$ probability by directly measuring two query states on the computational basis.

In order to overcome this difficulty, we further present an improved QPQ protocol in which Alice still sends multiple same query systems to Bob, but these query systems are all in mixed states not pure states such that it can fully resist the intercept-and-resend attack performed by Bob.

IV. IMPROVED QPQ PROTOCOL

Suppose that Bob owns a private N-element database: $\{d(0),d(1),\ldots,d(i),\ldots,d(N-1)\}$, where $N = 2^n$ and $d(i) \in \{0,1\}$ and Alice wants to obtain the ith element of the database but not revealing the secret i. The improved protocol is described in detail as follows:

Step 1. Alice first prepares two n-qubit states $\frac{|0\rangle+|i\rangle}{\sqrt{2}}$ and $|0\rangle$. Then, Alice generates a $2n$-qubit entangled state by sending

the two n-qubit states through n controlled-NOT (CNOT) gates where each qubit of the first state is the control qubit and each qubit of the second state is the corresponding target qubit. After performing all CNOT gates, the $2n$ qubits will be entangled as the following state $|\psi_1\rangle$:

$$|\psi_1\rangle = \text{CNOT}(1,n+1)\otimes\text{CNOT}(2,n+2)\otimes\text{CNOT}(n,2n)\times\left[\frac{|0\rangle+|i\rangle}{\sqrt{2}}\otimes|0\rangle\right]=\frac{|0\rangle|0\rangle+|i\rangle|i\rangle}{\sqrt{2}}. \quad (22)$$

Step 2. Furthermore, Alice prepares another $2n$-qubit state $|\psi_2\rangle=\frac{|0\rangle|0\rangle+|i\rangle|i\rangle}{\sqrt{2}}$ where the preparation process is the same as that of Step 1.

Step 3. Alice uses four registers h_1, h_2, t_1, and t_2 to store the $4n$ qubits where register h_j contains the first n qubits of $|\psi_j\rangle$ and accordingly register t_j contains the second n qubits for $j=1,2$. Then Alice sends registers t_1 and t_2 to Bob while she keeps registers h_1 and h_2 in hand.

Step 4. After receiving registers t_1 and t_2, Bob applies an oracle operator U to the states in registers t_1 and t_2, respectively, and then sends them back to Alice where the operator U is defined by Eqs. (1)–(3).

Step 5. After receiving the returned registers t_1 and t_2, each integrated quantum system in Alice's hands should be in the following state:

$$\frac{|0\rangle_{h_j}|0\rangle_{t_j}+(-1)^{d(i)}|i\rangle_{h_j}|i\rangle_{t_j}}{\sqrt{2}}, \quad (23)$$

where the subscripts h_j and t_j denote different registers for $j=1,2$, respectively. Subsequently, Alice performs a test procedure to check Bob's honesty as follows:

(5.1) Alice again applies n CNOT gates to each $2n$ qubit where each qubit in register t_j is the control qubit and each qubit in register h_j is the corresponding target qubit. Thus, we get

$$\text{CNOT}^{\otimes n}\left[\frac{|0\rangle_{h_j}|0\rangle_{t_j}+(-1)^{d(i)}|i\rangle_{h_j}|i\rangle_{t_j}}{\sqrt{2}}\right]=|0\rangle_{h_j}\frac{|0\rangle_{t_j}+(-1)^{d(i)}|i\rangle_{t_j}}{\sqrt{2}}. \quad (24)$$

(5.2) Then, Alice measures the states in registers h_1 and h_2 on the computational basis, respectively, and further checks whether both measured results are $|0\rangle$. If the measured results are not $|0\rangle$, she will terminate this protocol; otherwise she will continue to the next step.

(5.3) Furthermore, Alice measures the states in registers t_1 and t_2 by a von Neumann measurement $\{P_{+i},P_{+i}\}$, respectively, and further checks whether they are in $\frac{|0\rangle_{t_j}+|i\rangle_{t_j}}{\sqrt{2}}$ or $\frac{|0\rangle_{t_j}-|i\rangle_{t_j}}{\sqrt{2}}$, but it requires that two measured results are identical. If Alice finds a cheat from Bob, she will terminate this protocol; otherwise she will continue to the next step.

Step 6. After completing the honesty test, Alice extracts out the phase information $d(i)$ from register t_1 or t_2 by distinguishing between $\frac{|0\rangle_{t_j}+|i\rangle_{t_j}}{\sqrt{2}}$ and $\frac{|0\rangle_{t_j}-|i\rangle_{t_j}}{\sqrt{2}}$, that is, $d(i)=0$ if it is in state $\frac{|0\rangle_{t_j}+|i\rangle_{t_j}}{\sqrt{2}}$ and $d(i)=1$ otherwise.

TABLE I. The different results of Bob's performing the measure-and-resend attack.

Q_{t_j}	Q_{h_j}	R_{t_j}	Pass Step 5.2	Pass Step 5.3	Fully pass Step 5
$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	Yes	No	No
$\|i\rangle$	$\|i\rangle$	$\|0\rangle$	No	No	No
		$\|i\rangle$	Yes	No	No
		$\frac{\|0\rangle+\|i\rangle}{\sqrt{2}}$	Yes/no	No	No

Note. Q_{t_j}, Q_{h_j} and R_{t_j} denote the possible states measured by Bob in register t_j, the collapsed state in register h_j, and the possible state returned by Bob in register t_j, respectively.

V. ANALYSIS OF THE IMPROVED QPQ PROTOCOL

The correctness proof of our improved QPQ protocol is same as that of the original phase-encoded QPQ protocol [4]. So we mainly focus on the security of our improved QPQ protocol in the following section.

A. Alice's privacy

Similarly, Alice's privacy is based on the fact that Bob is not able to distinguish the states of the query subsystems (i.e., registers t_1 and t_2) due to two basic quantum principles: the no-cloning theorem and the Heisenberg uncertainty principle. First, Bob cannot copy the unknown state in register t_j because of the no-cloning theorem. Second, Bob cannot yet measure it to directly extract Alice's secret information, and otherwise his dishonesty will be found by Alice in a later test procedure. Unlike these cheat-sensitive QPQ protocols [3,4] in which Bob can also successfully pass Alice's honesty test with the probability of $\frac{1}{2}$ if he performs an intercept-and-resend attack, our improved QPQ protocol can fully resist this attack. In our improved protocol, the query subsystem is entangled with another ancillary subsystem held in Alice's hands (i.e., $\frac{|0\rangle_{h_j}|0\rangle_{t_j}+|i\rangle_{h_j}|i\rangle_{t_j}}{\sqrt{2}}$), and both subsystems will be checked in a later honesty test, respectively. If Bob measures the query subsystem in register t_j, which is a mixed state $\rho_{t_j}=\frac{|0\rangle_{t_j}\langle 0|+|i\rangle_{t_j}\langle i|}{2}$ before Step 5, it will certainly disentangle the entanglement of two subsystems h_j and t_j. Accordingly, Alice's measured results in her honesty test will not be both $|0\rangle_{h_j}$ and $\frac{|0\rangle_{t_j}\pm|i\rangle_{t_j}}{\sqrt{2}}$, which is shown in Table I in detail. From Table I, we can easily deduce that Bob cannot pass two honesty tests successfully if he performs the intercept-and-resend attack.

Furthermore, if Bob performs an entangle- and-measure attack described above in Sec. III, the returned quantum subsystems in register t_j will still be in a mixed state (i.e, $\rho_{t_j}=\frac{|0\rangle_{t_j}\langle 0|+|i\rangle_{t_j}\langle i|}{2}$) even after Step 5.2, not a pure state, due to the ancillary system of Bob [please see Eqs. (17)–(21)]. Then, in Step 5.3, Alice will get $\frac{|0\rangle_{t_j}+|i\rangle_{t_j}}{\sqrt{2}}$ or $\frac{|0\rangle_{t_j}-|i\rangle_{t_j}}{\sqrt{2}}$ with equal probability by the analysis above in Sec. III. However, the two measured results in registers t_1 and t_2 may be different due to the measurement's randomness. Therefore, if Bob performs

the entangle-and-measure attack, he might eventually succeed but not with more than a 50% chance.

In a word, Alice in our improved QPQ protocol can find the intercept-and-resend attack of a dishonest Bob with a 100% chance and the entangle-and-measure attack with a 50% chance. That is, Alice can check the honesty of Bob with a 50% chance, which is a strict bound for a cheat strategy. Similarly, our improved QPQ protocol is also a cheat-sensitive quantum protocol.

B. Bob's privacy

As demonstrated in Ref. [3], Bob's privacy (i.e., the database security) is ensured by the finite number of signals Bob is sending back to Alice. In our improved QPQ protocol, if Alice is dishonest, she can send two different query subsystems to Bob and further get two different query results [e.g., $d(i)$ and $d(i')$], but she will lose the ability to check the honesty of Bob. Furthermore, a dishonest Alice can send a false query state to Bob, e.g., a general state $\frac{1}{\sqrt{N}}\sum|i\rangle$ instead of the true query state $\frac{|0\rangle+|i\rangle}{\sqrt{2}}$. Accordingly, the returned state in Step 5 will be in $\frac{1}{\sqrt{N}}\sum(-1)^{d(i)}|i\rangle$, where $d(i)\in\{0,1\}$, but Alice can only extract one item $d(i)$ from state $\frac{1}{\sqrt{N}}\sum(-1)^{d(i)}|i\rangle$. Similarly, if Alice performs this attack, she will also lose the chance to check the honesty of Bob.

In addition, compared to the original QPQ protocol [3], our improved QPQ protocol achieves the same communication complexity, but it keeps better implementability of the phase-encoded QPQ protocol [4].

VI. CONCLUSION

We reexamine the security of the phase-encoded QPQ protocols and find that there is a security flaw in these protocols. Furthermore, we give an improved cheat-sensitive QPQ protocol to overcome this flaw. Compared to the original QPQ protocols, the improved protocol does not lose any good feature.

ACKNOWLEDGMENTS

This work was supported by the National Natural Science Foundation of China (Grants No. 61572001, No. 61173187, and No. 11301002), and the Ministry of Education Institution of Higher Learning Doctor Discipline and Scientific Research Fund aids the project financially (Project No. 20133401110004).

[1] B. Chor, E. Kushilevitz, O. Goldreich, and M. Sudan, Private information retrieval, J. Assoc. Comput. Mach. **45**, 965 (1998).

[2] Ä. Baumeler and A. Broadbent, Quantum private information retrieval has linear communication complexity, J. Cryptology **28**, 161 (2015).

[3] V. Giovannetti, S. Lloyd, and L. Maccone, Quantum Private Queries, Phys. Rev. Lett. **100**, 230502 (2008).

[4] L. Olejnik, Secure quantum private information retrieval using phase-encoded queries, Phys. Rev. A **84**, 022313 (2011).

[5] R.-H. Shi, Y. Mu, H. Zhong, and S. Zhang, Quantum oblivious set-member decision protocol, Phys. Rev. A **92**, 022309 (2015).

[6] R.-H. Shi, Y. Mu, H. Zhong, J. Cui, and S. Zhang, An efficient quantum scheme for private set intersection, Quantum Inf. Process. **15**, 363 (2016).

[7] J. Vaidya, B. Shafiq, W. Fan, D. Mehmood, and D. Lorenzi, A random decision tree framework for privacy-preserving data mining, IEEE Trans. Dependable Secure Comput. **11**, 399 (2014).

[8] L. K. Grover, A fast quantum mechanical algorithm for database search, in *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing, Philadelphia, 1996* (ACM, New York, 1996), pp. 212–219.

[9] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, UK, 2010).

[10] V. Giovannetti, S. Lloyd, and L. Maccone, Quantum private queries: Security analysis, IEEE Trans. Inf. Theory **56**, 3465 (2010).