THEORY OF COMPUTING, Volume 8 (2012), pp. 369–374
www.theoryofcomputing.org

NOTE

Quantum Private Information Retrieval with Sublinear Communication Complexity

François Le Gall*

Received: July 29, 2011; published: July 26, 2012.

Abstract: This note presents a quantum protocol for private information retrieval, in the case of a single (honest) server and with information-theoretical privacy, that has $O(\sqrt{n})$-qubit communication complexity, where n denotes the size of the database. In comparison, it is known that any classical protocol must use $\Omega(n)$ bits of communication in this setting.

ACM Classification: F.2.3

AMS Classification: 81P68

Key words and phrases: private information retrieval, quantum communication complexity

1 Introduction

Private information retrieval deals with the design and the analysis of protocols that allow a user to retrieve an item from a server without revealing which item it is retrieving. This field, introduced in a seminal paper by Chor, Kushilevitz, Goldreich, and Sudan [2], has been the subject of intensive research due to the growing ubiquity of public databases. Examples of applications include ensuring consumer privacy in e-commerce transactions or reading webpages on the Internet without revealing the user's preferences.

In the case of a single server and of information-theoretical privacy, which is the focus of this note, private information retrieval can be described as follows. The server has a database $\mathbf{A} = (\mathbf{a}^1, \mathbf{a}^2, \cdots, \mathbf{a}^\ell) \in \Sigma^\ell$, where $\Sigma = \{0,1\}^r$ is a set of items represented as r-bit strings, and the user has an index $i \in \{1, \ldots, \ell\}$.

*Partly supported by the JSPS, under the grant-in-aid for research activity start-up No. 22800006.

DOI: 10.4086/toc.2012.v008a016

A private information retrieval protocol is a (classical or quantum) communication protocol between the server and the user such that, when the user and the server both follow the protocol, the user always outputs the item $\mathbf{a}^i$ and the server gets no information about the index i, in the following sense (note that the privacy condition concerns only the user's input). Let $V_S(\mathbf{A},i)$ denote the server's view of the communication generated by the protocol when the server has input $\mathbf{A}$ and the user has input i. The privacy condition is that, for any database $\mathbf{A} \in \Sigma^\ell$ and any two indexes $i, j \in \{1,\dots,\ell\}$, the views $V_S(\mathbf{A},i)$ and $V_S(\mathbf{A},j)$ are identical. While several subtleties arise when trying to formally define the server's view in an arbitrary quantum protocol, the above description will be sufficient for our purpose due to the limited interaction between the server and the user in the quantum protocols described in this note.

It is easy to show that, classically, downloading the whole database is essentially optimal: any classical protocol must communicate a number of bits linear in the size of the database [2]. The communication complexity of quantum protocols for private information retrieval has first been investigated by Nayak [8], and then by Kerenidis and de Wolf [5]. These works focused on two-message quantum protocols, and established a connection with locally decodable codes and random access codes. In particular it was proved that, for a single server, any private two-message quantum protocol must use a linear amount of communication. This note shows that this lower bound does not hold for quantum protocols using more than two messages and describes how to construct a three-message quantum protocol for private information retrieval with sublinear communication complexity, thus breaking for the first time the linear barrier in the single-server and information-theoretical privacy setting. This is also the first example in (quantum or classical) single-server information-theoretic private information retrieval where protocols with more than two messages outperform protocols with one round of communication. Our main result is the following theorem.

Theorem 1.1. *Let ℓ and r be any positive integers. There exists a private information retrieval quantum protocol that, for any database $\mathbf{A} \in \Sigma^\ell$ with $\Sigma = \{0,1\}^r$, uses $2\ell + 2r$ qubits of communication.*

The protocol we design to prove Theorem 1.1, described in Section 2, combines the properties of two-party entanglement with a technique similar to the one used in the Bernstein-Vazirani algorithm [1], and ensures the user's privacy in the following sense: at no time the server holds any (quantum) information about the user's input i.

Since the overall size of the database is ℓr bits, Theorem 1.1 gives a quadratic improvement over classical protocols and two-message quantum protocols whenever $\ell + r = O(\sqrt{\ell r})$, for example when $\ell = \Theta(r)$. The same quadratic improvement can also be obtained for other values of ℓ and r: the idea is to decompose the database into about $\sqrt{\ell r}$ blocks, each of size about $\sqrt{\ell r}$ bits. The case $r = 1$ (i. e., binary databases) is illustrated in the following corollary.

Corollary 1.2. *There exists a private information retrieval quantum protocol that, for any binary database $\mathbf{A} \in \{0,1\}^\ell$, uses $O(\sqrt{\ell})$ qubits of communication.*

Proof. Let $\mathbf{A} = (a^1,\dots,a^\ell) \in \{0,1\}^\ell$ be the binary database held by the server. For convenience, let us assume that $\ell = s^2$ for some positive integer s (a similar argument works for any value of ℓ). We construct the database $\mathbf{B} = (\mathbf{b}^1,\dots,\mathbf{b}^s)$ such that, for each $k \in \{1,\dots,s\}$, the k-th block is $\mathbf{b}^k = (a^{(k-1)s+1},\dots,a^{ks}) \in \{0,1\}^s$. Note that the bit a^i is contained in the block $\mathbf{b}^j$ with $j = \lceil i/s \rceil$. By running the protocol of Theorem 1.1 where, as inputs, the server has database $\mathbf{B}$ and the user has index j, the user is able to recover the whole block $\mathbf{b}^j$, and thus the bit a^i, using $O(s)$ qubits of communication. $\square$

We stress that this note considers only the setting where the parties do not deviate from the protocol, as often assumed in works focusing on algorithmic or complexity-theoretic aspects of private information retrieval. While this restriction may reduce the applicability of our result, we believe that it nevertheless illustrates the subtle interplay of interaction and quantum information in protecting privacy. Indeed, even in this setting, a linear amount of communication is needed for classical protocols and for two-message quantum protocols. A natural open problem is to investigate if the upper bounds in Theorem 1.1 and Corollary 1.2 are tight and, more specifically, to prove lower bounds on the communication complexity of quantum protocols for private information retrieval that exchange more than two messages.

Other related works Several other aspects of quantum protocols for private information retrieval have been investigated. Jain, Radhakrishnan and Sen [4] have shown a linear lower bound on the communication complexity of private information retrieval quantum protocols in a setting where the user is allowed to perform superposition attacks (while our work considers only servers that follow the protocol). Giovannetti, Lloyd and Maccone [3] studied a slightly different cryptographic primitive called "quantum private query," in which the user should always detect if the server has been trying to cheat to obtain information about its input i (but, contrary to the setting of the present note, has not to prevent leakage of information about i), and presented a cheat sensitive quantum protocol with logarithmic communication complexity. The case of multiple servers has been studied in [5, 6], while the case of symmetric private information retrieval, where the server's privacy is also taken into consideration, has also been studied in [3, 4, 6]. Privacy issues in quantum communication complexity have been studied in [7] as well. Let us mention that quantum protocols for symmetric private information retrieval are also studied under the name of quantum oblivious transfer protocols, especially when the server and the user may deviate from the protocol (i. e., when considering malicious parties).

2 Proof of Theorem 1.1

We suppose that the reader is familiar with quantum computation and refer to, e. g., [9] for an introduction to this field. Let us first describe some of our notations. Given two bits $a, b \in \{0,1\}$, we write their parity as $a \oplus b$. For any two elements $\mathbf{u} = (u_1, \ldots, u_r)$ and $\mathbf{v} = (v_1, \ldots, v_r)$ in $\Sigma = \{0,1\}^r$, let us write $\mathbf{u} \cdot \mathbf{v} = u_1 v_1 \oplus \cdots \oplus u_r v_r$ and $\mathbf{u} \oplus \mathbf{v} = (u_1 \oplus v_1, \ldots, u_r \oplus v_r)$. Note that $\mathbf{u} \cdot \mathbf{v}$ is a bit and $\mathbf{u} \oplus \mathbf{v}$ is an element of Σ. Our protocol will use the Pauli gate

$$\mathrm{Z} := \sum_{z \in \{0,1\}} (-1)^z |z\rangle\langle z|$$

acting on one qubit and the Hadamard transform

$$\mathrm{H}_r := \frac{1}{\sqrt{|\Sigma|}} \sum_{\mathbf{y}, \mathbf{z} \in \Sigma} (-1)^{\mathbf{y} \cdot \mathbf{z}} |\mathbf{y}\rangle\langle \mathbf{z}|$$

acting on r qubits. It will also use the gates

$$\begin{aligned}\mathrm{CNOT}^{(\mathsf{R}_1,\mathsf{R}_2)} &:= \sum_{\mathbf{y},\mathbf{z}\in\Sigma} |\mathbf{y}\rangle_{\mathsf{R}_1}|\mathbf{z}\oplus\mathbf{y}\rangle_{\mathsf{R}_2}\langle\mathbf{y}|_{\mathsf{R}_1}\langle\mathbf{z}|_{\mathsf{R}_2} \quad \text{and}\\ \mathrm{U}_{\mathbf{b}}^{(\mathsf{R}_1,\mathsf{Q})} &:= \sum_{\mathbf{y}\in\Sigma, z\in\{0,1\}} |\mathbf{y}\rangle_{\mathsf{R}_1}|z\oplus\mathbf{b}\cdot\mathbf{y}\rangle_{\mathsf{Q}}\langle\mathbf{y}|_{\mathsf{R}_1}\langle z|_{\mathsf{Q}}\,,\end{aligned}$$

where R_1 and R_2 denote two r-qubit registers, Q denotes a one-qubit register, and $\mathbf{b}$ is any element in Σ. The gate CNOT performs a bitwise XOR of the first register into the second, while the gate $\mathrm{U}_{\mathbf{b}}$ performs an XOR of the inner product of the first register and $\mathbf{b}$ into the second register.

We now present the proof of Theorem 1.1.

Proof of Theorem 1.1. The protocol uses $\ell+2$ quantum registers: registers R and R' each consisting of r qubits, and registers $\mathsf{Q}_1,\ldots,\mathsf{Q}_\ell$ each consisting of one qubit. For any database $\mathbf{A}=(\mathbf{a}^1,\ldots,\mathbf{a}^\ell)\in\Sigma^\ell$, let us denote by $|\Phi_{\mathbf{A}}\rangle$ the quantum state

$$|\Phi_{\mathbf{A}}\rangle := \frac{1}{\sqrt{2^r}}\sum_{\mathbf{x}\in\Sigma}|\mathbf{x}\rangle_{\mathsf{R}}|\mathbf{x}\rangle_{\mathsf{R}'}|\mathbf{x}\cdot\mathbf{a}^1\rangle_{\mathsf{Q}_1}\cdots|\mathbf{x}\cdot\mathbf{a}^\ell\rangle_{\mathsf{Q}_\ell}$$

in registers $(\mathsf{R},\mathsf{R}',\mathsf{Q}_1,\ldots,\mathsf{Q}_\ell)$. The protocol is described in Figure 1. It consists of three messages and uses a total amount of $2\ell+2r$ qubits of communication.

Server's input: $\mathbf{A}=(\mathbf{a}^1,\ldots,\mathbf{a}^\ell)\in\Sigma^\ell$

User's input: $i\in\{1,\ldots,\ell\}$

1. The server constructs the quantum state $|\Phi_{\mathbf{A}}\rangle$ and sends registers R', $\mathsf{Q}_1,\ldots,\mathsf{Q}_\ell$ to the user.
2. The user applies Z over register Q_i and sends back registers $\mathsf{Q}_1,\ldots,\mathsf{Q}_\ell$ to the server.
3. The server applies $\mathrm{U}_{\mathbf{a}^k}^{(\mathsf{R},\mathsf{Q}_k)}$, for each $k\in\{1,\ldots,\ell\}$, and sends to the user register R.
4. The user applies $\mathrm{CNOT}^{(\mathsf{R},\mathsf{R}')}$, applies H_r over register R, and then measures R in the computational basis.

Figure 1: Quantum private information retrieval protocol.

We first show that in this protocol the user always outputs the correct element of the database. Observe that, at the end of Step 2, the state is

$$|\Phi\rangle = \frac{1}{\sqrt{2^r}}\sum_{\mathbf{x}\in\Sigma}(-1)^{\mathbf{x}\cdot\mathbf{a}^i}|\mathbf{x}\rangle_{\mathsf{R}}|\mathbf{x}\rangle_{\mathsf{R}'}|\mathbf{x}\cdot\mathbf{a}^1\rangle_{\mathsf{Q}_1}\cdots|\mathbf{x}\cdot\mathbf{a}^\ell\rangle_{\mathsf{Q}_\ell}\,.$$

At Step 4, just before the user performs the measurement, the state is $|\mathbf{a}^i\rangle_{\mathsf{R}}|\mathbf{0}\rangle_{\mathsf{R}'}|0\rangle_{\mathsf{Q}_1}\cdots|0\rangle_{\mathsf{Q}_\ell}$, and measuring register R gives the element $\mathbf{a}^i$ with probability 1. Let us now consider the user's privacy. The only information about i that a server following the protocol can obtain is from registers $\mathsf{R}, \mathsf{Q}_1, \ldots, \mathsf{Q}_\ell$ of the state $|\Phi\rangle$. Since tracing out register R' in $|\Phi\rangle\langle\Phi|$ gives the density matrix

$$\frac{1}{2^r}\sum_{\mathbf{x}\in\Sigma}|\mathbf{x}\rangle_{\mathsf{R}}|\mathbf{x}\cdot\mathbf{a}^1\rangle_{\mathsf{Q}_1}\cdots|\mathbf{x}\cdot\mathbf{a}^\ell\rangle_{\mathsf{Q}_\ell}\langle\mathbf{x}|_{\mathsf{R}}\langle\mathbf{x}\cdot\mathbf{a}^1|_{\mathsf{Q}_1}\cdots\langle\mathbf{x}\cdot\mathbf{a}^\ell|_{\mathsf{Q}_\ell},$$

the server obtains no information about the user's input. $\square$

Remark As already mentioned, in this note we only consider the case where the server follows the protocol. This assumption is used in the analysis of the protocol of Figure 1 in order to ensure that the server prepares the state $|\Phi_{\mathbf{A}}\rangle$ at Step 1. Note that if, instead of $|\Phi_{\mathbf{A}}\rangle$, the server prepared for example the state

$$|\Phi'_{\mathbf{A}}\rangle := \frac{1}{\sqrt{2^r}}\sum_{\mathbf{x}\in\Sigma}|\mathbf{x}\rangle_{\mathsf{R}}|\mathbf{0}\rangle_{\mathsf{R}'}|\mathbf{x}\cdot\mathbf{a}^1\rangle_{\mathsf{Q}_1}\cdots|\mathbf{x}\cdot\mathbf{a}^\ell\rangle_{\mathsf{Q}_\ell},$$

then it would be able to recover the index i with probability one at Step 3.

Acknowledgements

The author is grateful to Takeshi Koshiba, Harumichi Nishimura, and Ronald de Wolf for helpful discussions about this work. He also thanks the anonymous reviewers for very valuable comments and suggestions.

References

[1] ETHAN BERNSTEIN AND UMESH VAZIRANI: Quantum complexity theory. *SIAM J. Comput.*, 26(5):1411–1473, 1997. Preliminary version in STOC'93. [doi:10.1137/S0097539796300921] 370

[2] BENNY CHOR, ODED GOLDREICH, EYAL KUSHILEVITZ, AND MADHU SUDAN: Private information retrieval. *J. ACM*, 45(6):965–981, 1998. Preliminary version in FOCS'95. [doi:10.1145/293347.293350] 369, 370

[3] VITTORIO GIOVANNETTI, SETH LLOYD, AND LORENZO MACCONE: Quantum private queries. *Phys. Rev. Lett.*, 100:230502, Jun 2008. [doi:10.1103/PhysRevLett.100.230502] 371

[4] RAHUL JAIN, JAIKUMAR RADHAKRISHNAN, AND PRANAB SEN: A property of quantum relative entropy with an application to privacy in quantum communication. *J. ACM*, 56(6):33, 2009. Preliminary version in FOCS'02. [doi:10.1145/1568318.1568323] 371

[5] IORDANIS KERENIDIS AND RONALD DE WOLF: Exponential lower bound for 2-query locally decodable codes via a quantum argument. *J. Comput. System Sci.*, 69(3):395–420, 2004. Preliminary version in STOC'03. [doi:10.1016/j.jcss.2004.04.007] 370, 371

[6] IORDANIS KERENIDIS AND RONALD DE WOLF: Quantum symmetrically-private information retrieval. *Inform. Process. Lett.*, 90(3):109–114, 2004. [doi:10.1016/j.ipl.2004.02.003] 371

[7] HARTMUT KLAUCK: Quantum and approximate privacy. *Theory of Computing Systems*, 37(1):221–246, 2004. Preliminary version in STACS'02. [doi:10.1007/s00224-003-1113-7] 371

[8] ASHWIN NAYAK: Optimal lower bounds for quantum automata and random access codes. In *Proc. 40th FOCS*, pp. 369–377. IEEE Comp. Soc. Press, 1999. [doi:10.1109/SFFCS.1999.814608] 370

[9] MICHAEL NIELSEN AND ISAAC CHUANG: *Quantum Computation and Quantum Information*. Cambridge University Press, 2000. 371

AUTHOR

François Le Gall
Assistant professor
Department of Computer Science
The University of Tokyo
legall@is.s.u-tokyo.ac.jp
http://www.francoislegall.com

ABOUT THE AUTHOR

FRANÇOIS LE GALL received his Ph. D. from the University of Tokyo in 2006; his advisor was Hiroshi Imai. His research interests include quantum computation, computational complexity, and algorithms for algebraic problems (especially the group isomorphism problem and matrix multiplication). On weekends or holidays, he enjoys going for a hike around Tokyo with his wife.