A model of quantum communication device for quantum hashing

A. Vasiliev
Kazan Federal University, 18 Kremlyovskaya St., Kazan 420008, Russian Federation
E-mail: Alexander.KSU@gmail.com

Abstract. In this paper we consider a model of quantum communications between classical computers aided with quantum processors, connected by a classical and a quantum channel. This type of communications implying both classical and quantum messages with moderate use of quantum processing is implicitly used in many quantum protocols, such as quantum key distribution or quantum digital signature. We show that using the model of a quantum processor on multiatomic ensembles in the common QED cavity we can speed up quantum hashing, which can be the basis of quantum digital signature and other communication protocols.

1. Introduction
Nowadays the area of quantum computing technology is in active experimental phase, but a large-scale fully functional quantum computer has a long way to come. However, quantum communications are already here and further development of communication devices and protocols may give rise to new commercial products.

In this research we propose a model for one such device, which we have called a Quantum Communication Device and which can be seen as a part of quantum communication system. The main purpose of developing quantum communications is to implement quantum cryptographic protocols that outperform their classical counterparts. Among them is the well-known Quantum Digital Signature protocol [1].

In [2] we have proposed a quantum hashing technique that can be used in this protocol, and it also proved useful for constructing efficient quantum algorithms [3] and quantum communication protocols [4].

The model of the quantum processor on multiatomic ensembles in the common QED cavity we consider here was investigated in [5]. Using the logical encoding of qubits and the properties of the basic operations of this architecture we can speed up quantum hashing and thus performing communication protocols that are based on it.

2. A model of the quantum communication device
Due to severe limits of existing physical implementations of quantum computer it is natural to consider the restricted models of quantum computations. The one we use here is a hybrid classical-quantum model, where small quantum processor is controlled by a classical computer. To support this idea, we may note that such protocols as Quantum Key Distribution and Quantum Digital Signature (both demonstrated experimentally) imply both classical and
quantum messages between communicating parties and a very moderate use of quantum processing device.

Based on this considerations we use the scheme of quantum communications (depicted in Figure 1), where communicating parties are classical computers aided with quantum processors on multatomic ensembles in the common QED cavity [5], connected by a classical and a quantum channel.

In [5] we have investigated computational capabilities of such a quantum processor under the logical encoding of the states $|0_L\rangle$, $|1_L\rangle$ by pairs of physical qubits in states $|0\rangle$, $|1\rangle$ (see Figure 2).

This encoding eliminates the need for implementing single qubit gates, since our two-qubit gates are logical single-qubit in this encoding.

2.1. Basic operations of the quantum processor

The basic operations of the quantum processor are given by the underlying physical model and include the following.

- A Quantum Excitation Transfer between two ensembles (QET($\theta$)) is defined by

$$
\begin{align*}
|0\rangle|1\rangle & \rightarrow \cos \frac{\theta}{2}|0\rangle|1\rangle - i \sin \frac{\theta}{2}|1\rangle|0\rangle, \\
|1\rangle|0\rangle & \rightarrow -i \sin \frac{\theta}{2}|0\rangle|1\rangle + \cos \frac{\theta}{2}|1\rangle|0\rangle.
\end{align*}
$$

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{figure1.png}
\caption{A simple abstraction of quantum communications over classical and quantum channels. $A$ and $B$ are classical computers aided with quantum processors.}
\end{figure}

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{figure2.png}
\caption{Pairwise qubit encoding. Small circles denote the processing nodes in the indicated quantum states.}
\end{figure}
In the encoded setting QET(\(\theta\)) gate is actually a single-qubit rotation by the angle \(-\theta\) about the \(\hat{x}\) axis.

• PHASE(\(\chi\)) operation is given by

\[
\begin{align*}
|0\rangle|1\rangle & \rightarrow e^{-i\chi/2}|0\rangle|1\rangle \\
|1\rangle|0\rangle & \rightarrow e^{i\chi/2}|1\rangle|0\rangle
\end{align*}
\]

In the logical encoding PHASE(\(\chi\)) turns our composite qubit around the axis \(\hat{z}\).

Based on the model of atomic transistor [6] it is possible to perform a Controlled-QET operation (denoted by C(QET)), that corresponds to logical Controlled NOT gate (up to the relative phase shift, that can be made global by adding PHASE operation, see Figure 3).

We have proved that the set of quantum gates \(\{\text{C(QET)}, \text{QET}(\theta), \text{PHASE}(\chi)\}\) is universal for the Hilbert subspace spanned by encoded states \(|0_L\rangle = |01\rangle, |1_L\rangle = |10\rangle\) (for proof see [5]).

Though the architecture provides a universal set of quantum gates it is possible to speed up the usual implementation of some class of useful operations, in particular those used in the algorithm of quantum hashing.

3. Quantum hashing

In this section we recall the construction of quantum hash function from [2].

Let \(q = 2^n\) and \(B = \{b_1, b_2, \ldots, b_d\} \subset \mathbb{Z}_q\). We define a quantum hash function \(\psi_{q,B} : \{0,1\}^n \rightarrow (\mathbb{C}^2)^{\otimes (\log d+1)}\) as follows. For an input \(x \in \{0,1\}^n\) we let

\[
|\psi_{q,B}(x)\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^{d} |i\rangle \left( \cos \frac{2\pi b_i x}{q} |0\rangle + \sin \frac{2\pi b_i x}{q} |1\rangle \right) .
\]

(1)

It follows from this definition that the quantum hash \(|\psi_{q,B}(x)\rangle\) of an \(n\)-bit string \(x\) consists of \(\log d + 1\) qubits. We have shown in [2] that \(d\) can be about \(O(n)\) without loosing the quality of hashing. Thus, this function maps \(n\)-bit inputs to quantum states of \(O(\log n)\) qubits.

4. Algorithmic implementation of quantum hashing

In order to describe the implementation of the quantum hashing we use the following notations from [3].

We define a Compound Controlled Rotation operator (CCR):

\[
\text{CCR}_{q,B}(\theta) = \text{CCR}_{q,B,1}(\theta) \cdot \text{CCR}_{q,B,2}(\theta) \cdots \text{CCR}_{q,B,d}(\theta) ,
\]

(2)
CCR_{q,B,i}(\theta) = \begin{pmatrix} \cos \frac{2\pi b_i \theta}{q} & -\sin \frac{2\pi b_i \theta}{q} \\ \sin \frac{2\pi b_i \theta}{q} & \cos \frac{2\pi b_i \theta}{q} \end{pmatrix} \begin{pmatrix} |i\rangle \\ |\psi_{q,B,i}(0)\rangle \end{pmatrix}.

Figure 4. A circuit for the operator CCR_{q,B,i}(\theta), that rotates the target qubit by the angle $2\theta$ if the control qubits were in the state $|i\rangle$. Here, the single-qubit rotation is made around the $\hat{y}$ axis of the Bloch sphere.

\begin{figure}
\centering
\includegraphics[width=\textwidth]{figure4}
\caption{A circuit for the operator CCR_{q,B,i}(\theta), that rotates the target qubit by the angle $2\theta$ if the control qubits were in the state $|i\rangle$. Here, the single-qubit rotation is made around the $\hat{y}$ axis of the Bloch sphere.}
\end{figure}

\begin{figure}
\centering
\includegraphics[width=\textwidth]{figure5}
\caption{An algorithm, that hashes an $n$-bit input $w = w_0 \ldots w_{n-1}$ into the state $|\psi_{q,B}(M)\rangle$ of $O(\log n)$ qubits. $R(\theta_{i,j})$ denotes a rotation by an angle $\frac{4\pi b_i 2^j}{q}$ around the $\hat{y}$ axis of the Bloch sphere.}
\end{figure}

where operator $CCR_{q,B,i}(\theta)$ rotates the target qubit by the angle $\theta$ if the control qubits were in the state $|i\rangle$ (its circuit representation is given in Figure 4).

In [3] we have given an efficient algorithm for computing quantum hash function in the model of quantum branching programs. This procedure (illustrated in Figure 5) consists of the following steps:

0. Initialization of the log $d + 1$ qubits in the state $|0\ldots00\rangle$.
1. Application of Hadamard transform to the first log $d$ qubits:

$$\frac{1}{\sqrt{d}} \sum_{i=1}^{d} |i\rangle |0\rangle = |\psi_{q,B}(0)\rangle.$$ (3)

2. Application of $CCR_{q,B}(w)$ creates the quantum hash of the input bit string $w = w_0 \ldots w_{n-1}$, which is also treated as a number $w = w_0 + w_1 2^1 + \ldots + w_{n-1} 2^{n-1}$:

$$CCR_{q,B}(w) |\psi_{q,B}(0)\rangle = |\psi_{q,B}(w)\rangle.$$ (4)
5. Physical implementation of quantum hashing
In [5] we have proposed an effective physical implementation of compound multiply controlled operators for the model of quantum processor on multiatomic ensembles in the QED cavity. \( CCR_{q,B,i}(\theta) \) is exactly such operator and thus can be accelerated in this architecture.

The key idea is to use the C(QET) operation to compute the logical AND operation in a manner depicted in Figure 6.

Let \( C^t(U) \) be the general controlled gate, defined by the following equation in [7]:

\[
C^t(U)|c_1c_2\ldots c_t|\psi\rangle = |c_1c_2\ldots c_t\rangle U^{c_1c_2\ldots c_t}|\psi\rangle.
\]

Figure 7 demonstrates how the logical \( C^t(U) \) gate can be reduced to the sequence of \( 2(t-1) \) C(QET) operations (which are implemented by two elementary gates in our model) and a Controlled-\( U \) gate. This scheme requires \( t-1 \) ancillary processing nodes instead of full logical qubits.

Finally, using the known construction [7] Controlled-\( U \) gate can decomposed into two CNOT gates (implemented here by C(QET) gate) and five single qubit rotations (corresponding to QET and PHASE operations).

Acknowledgments
The work is performed according to the Russian Government Program of Competitive Growth of Kazan Federal University. Work was in part supported by the Russian Foundation for Basic Research (under the grants 14-07-00878, 14-07-00557, 15-37-21160).
References

[1] Gottesman D and Chuang I 2001 Quantum digital signatures Tech. Rep. arXiv:quant-ph/0105032 Cornell University Library URL http://arxiv.org/abs/quant-ph/0105032

[2] Ablayev F M and Vasiliev A V 2014 Laser Physics Letters 11 025202 URL http://stacks.iop.org/1612-202X/11/i=2/a=025202

[3] Ablayev F and Vasiliev A 2014 Computing with New Resources Lecture Notes in Computer Science ed Calude C S, Freivalds R and Kazuo I (Springer International Publishing) pp 149–160 ISBN 978-3-319-13349-2 URL http://dx.doi.org/10.1007/978-3-319-13350-8_11

[4] Vasiliev A 2015 International Journal of Applied Engineering Research 10 31415–31426

[5] Ablayev F, Andrianov S, Moiseev S and Vasiliev A 2013 Lobachevskii Journal of Mathematics 34 291–303 ISSN 1995-0802 (Preprint http://arxiv.org/abs/1301.2201) URL http://dx.doi.org/10.1134/S1995080213040094

[6] Moiseev S A, Andrianov S N and Moiseev E S 2013 Optics and Spectroscopy 115 356–362 ISSN 0030-400X URL http://link.springer.com/10.1134/S0030400X13090166

[7] Nielsen M A and Chuang I L 2000 Quantum Computation and Quantum Information 1st ed (Cambridge University Press) ISBN 0521635039 URL http://www.worldcat.org/isbn/521635039