Письма в ЭЧАЯ. 2007. Т. 4, № 2(138). С. 273–278

SIMULATION ON QUANTUM AUTHENTICATION

M. Dobšíček[1]

Department of Computer Science and Engineering, FEE CTU, Prague, Czech Republic

This paper divides into two main parts. The first one discusses authentication of quantum messages. Especially, the protocol proposed in [1] for one qubit message-length case is considered. The protocol uses a shared EPR pair as a secret key. In the second part it is shown how such a protocol can be simulated using the Quantum-Octave package. Quantum-Octave is a set of functions for Matlab-like numerical environment allowing calculations with general density matrices.

Настоящая статья состоит из двух частей. В первой части рассматривается проблема установления подлинности квантового сообщения. А именно изучается протокол для однобуквенного сообщения, предложенный в [1]. Данный протокол использует распределенную ЕПР-пару в качестве секретного ключа. Во второй части показано, каким образом данный протокол может быть симулирован с помощью пакета Quantum-Octave. Данный пакет представляет собой набор функций, позволяющий производить численные расчеты в средах типа MatLab с использованием общих матриц плотности.

INTRODUCTION

Technologies for trust and security represent a challenging problem for the digital nowadays. The current state of the art is the public-key cryptography which, as many other cryptographic primitives, depends directly or indirectly on the assumed computational hardness of such problems in number theory as factoring of integers or computing discrete logarithms. Since there is no proof of such a hardness, we talk about conditional security.

C. H. Bennett and G. Brassard have used quantum resources to develop the protocol BB84 for unconditionally secure key exchange if we assume the quantum mechanics to be correct. The secure key exchanged in unconditionally secure manner can be used for one-time pad systems, which are again unconditionally secure. First commercial products offering the BB84 protocol are already available. They work as point-to-point systems over a fiber optic line, up to 70 km of length, at rates approximately 100 Kb/s.

An open question is whether quantum resources can help to improve security or effectiveness of message authentication. Generally, we can consider authentication of classic messages as well as quantum ones. D. W. Leung has proposed a protocol [2] based on a modified private quantum channel. H. Barnum and co-workers presented a secret-key quantum authentication

[1] E-mail: dobsicm@fel.cvut.cz

protocol [3] that uses stabilizer purity testing codes. In [1] the authors studied a qubit authentication using a unitary coding set and a key of minimal length. The following section discusses their protocol in greater depth. One may also think to use quantum teleportation for authenticated qubit transfer. However, under this scenario, two classic bits have to be transferred over an authenticated channel, thus the problem only shifts to another one.

1. QUBIT AUTHENTICATION

1.1. The Protocol. The description of a protocol for one qubit message-length case as presented in [1] follows.

Prepositions. Party A wants to send an arbitrary qubit described by the density operator ρ_M acting on a two-dimensional message space $\mathcal{M}$. As in a classic case, some tag needs to be appended to a message, in order to allow the recipient party B to convince himself about the authenticity of the message. Let the tag be given by a density operator ρ_T acting on a two-dimensional tag space $\mathcal{T}$. The space $\mathcal{T}$ has to be divided into two orthogonal subspaces. One subspace represents a valid tag, while the other represents an invalid tag. Without loss of generality, the state $\rho_T = |0\rangle\langle 0|_T$ can be fixed as a valid tag.

The space of tagged messages is defined as $\varepsilon = \mathcal{M} \otimes \mathcal{T}$; the tagged message, as $\rho_\varepsilon = \rho_M \otimes \rho_T$. On space ε a unitary coding set $\{Id_\varepsilon, U_\varepsilon\}$ is defined, where Id_ε is the identity matrix and U_ε a unitary transformation. The shared secret key has the form of maximally entangled EPR pair. Each of the parties owns one qubit of publicly known state $|\psi\rangle_{AB} = \frac{1}{\sqrt{2}}(|01\rangle_{AB} - |10\rangle_{AB})$. The state of the global system (secret key + tagged message) is given by

$$\rho_{AB\varepsilon} = |\psi\rangle\langle\psi|_{AB} \otimes \rho_\varepsilon = |\psi\rangle\langle\psi|_{AB} \otimes \rho_M \otimes |0\rangle\langle 0|_T. \tag{1}$$

Encoding. Party A performs an encoding operation

$$E_{A\varepsilon} = |0\rangle\langle 0|_A \otimes Id_B \otimes Id_\varepsilon + |1\rangle\langle 1|_A \otimes Id_B \otimes U_\varepsilon. \tag{2}$$

The encoding operation can be seen as a selection of operation from the set $\{Id_\varepsilon, U_\varepsilon\}$ triggered by the resulting state of the key. Once the operation is selected, it is applied to ρ_ε before sending it through the quantum channel. The state of the global system after the encoding operation is given by

$$\rho^e_{AB\varepsilon} = E_{A\varepsilon}\rho_{AB\varepsilon}E^\dagger_{A\varepsilon} = \frac{1}{2}\big(|01\rangle\langle 01| \otimes \rho_\varepsilon - |01\rangle\langle 10| \otimes \rho_\varepsilon U^\dagger_\varepsilon - \\ -|10\rangle\langle 01| \otimes U_\varepsilon\rho_\varepsilon + |10\rangle\langle 10| \otimes U_\varepsilon\rho_\varepsilon U^\dagger_\varepsilon\big). \tag{3}$$

Decoding. Party B performs a decoding operation

$$D_{B\varepsilon} = Id_A \otimes |0\rangle\langle 0|_B \otimes U^\dagger_\varepsilon + Id_A \otimes |1\rangle\langle 1|_B \otimes Id_\varepsilon. \tag{4}$$

The state of the global system after the decoding operation is given by

$$\rho^d_{AB\varepsilon} = D_{B\varepsilon}\rho^e_{AB\varepsilon}D^\dagger_{B\varepsilon} = \frac{1}{2}\big(|01\rangle\langle 01| \otimes \rho_\varepsilon - |01\rangle\langle 10| \otimes \big(\rho_\varepsilon U^\dagger_\varepsilon\big)U_\varepsilon - \\ -|10\rangle\langle 01| \otimes U^\dagger_\varepsilon\left(U_\varepsilon\rho_\varepsilon\right) + |10\rangle\langle 10| \otimes U^\dagger_\varepsilon\big(U_\varepsilon\rho_\varepsilon U^\dagger_\varepsilon\big)U_\varepsilon\big). \tag{5}$$

Verification. Party B receives decoded tagged message ρ^d_ε by tracing out the key from the state of the global system. $\rho^d_\varepsilon = \mathrm{Tr}_{AB}\left(\rho^d_{AB\varepsilon}\right) = 1/2\left(\rho_\varepsilon + \rho_\varepsilon\right) = \rho_\varepsilon$. Finally, the tag portion of ρ_ε is measured and if it belongs to a valid tag subspace of space $\mathcal{T}$, then extracted message ρ_M is considered to be authentic.

1.2. Message Attack. Let us now consider a «message attack» performed by some adversary party E. This party with full access to a public quantum channel sees the state

$$\rho^e_\varepsilon = \mathrm{Tr}_{AB}\left(E_{A\varepsilon}\left(|\psi\rangle\langle\psi|_{AB}\otimes\rho_M\otimes|0\rangle\langle 0|_T\right)E^\dagger_{A\varepsilon}\right) = \\ = \frac{1}{2}\left(\rho_M\otimes|0\rangle\langle 0|_T + U_\varepsilon\left(\rho_M\otimes|0\rangle\langle 0|_T\right)U^\dagger_\varepsilon\right). \quad (6)$$

The task is to find a transformation Q_E which, applied to ρ^e_ε, will modify the ρ_M keeping the tag portion intact. The authors of [1] have an existential proof that such a transformation always exists regardless of the choice of U_ε, thus the protocol is not secure. However, they do not state the form of such a transformation and its consequences.

Contribution. Let U_ε be a separable gate of the form $U_\varepsilon = U_M \otimes U_T$, then

$$\rho^e_\varepsilon = \frac{1}{2}\left(\rho_M\otimes|0\rangle\langle 0|_T + \left(U_M\rho_M U^\dagger_M\right)\otimes\left(U_T|0\rangle\langle 0|_T U^\dagger_T\right)\right). \quad (7)$$

For $Q_E = X\otimes Id$, where $Q_E \in \varepsilon$, $X \in \mathcal{M}$, $Id \in \mathcal{T}$, we have $\rho^{e,E}_\varepsilon = Q_E\rho^e_\varepsilon Q^\dagger_E$;

$$\rho^{e,E}_\varepsilon = \frac{1}{2}\left(X\rho_M X^\dagger\otimes|0\rangle\langle 0|_T + \left(X\left(U_M\rho_M U^\dagger_M\right)X^\dagger\right)\otimes\left(U_T|0\rangle\langle 0|_T U^\dagger_T\right)\right). \quad (8)$$

After the decoding operation we have

$$\rho^{d,E}_\varepsilon = \frac{1}{2}\left(X\rho_M X^\dagger\otimes|0\rangle\langle 0|_T + \left(U^\dagger_M X U_M\rho_M U^\dagger_M X^\dagger U_M\right)\otimes\left(U^\dagger_T U_T|0\rangle\langle 0|_T U^\dagger_T U_T\right)\right), \quad (9)$$

and $\mathrm{Tr}_M\left(\rho^{d,E}_\varepsilon\right) = |0\rangle\langle 0|_T$.

Hence the adversary party is always able to change ρ_M keeping the tag portion intact, and there are *no limits* on the form of unitary matrix X. This means that the adversary party, having some statistics of usually sent states ρ_M, is able to prepare such X that will cause maximal damage or even modify ρ_M at will.

1.3. Secret-Key Discussion. Shared EPR pair was used as a secret key in the protocol. It is also possible to use a classical one-bit key for selecting the operation from the set $\{Id, U_\varepsilon\}$. However, authenticating quantum data makes sense only in a scenario where the reliable technology for quantum information processing is available. From this point of view it is more logical to use a quantum key instead of classic one. A quantum key has also better key-management properties due to the no-cloning theorem.

Anyway, EPR pair might get corrupted in the transit. In such a case, the protocol does not behave in a deterministic way any more. One solution is to use entanglement purification [4] to establish a clean pair. In situations where the purification processes cannot be used for some reason (e.g., noninteractive processes), we need to evaluate how much the determinism of the protocol depends on the purity of the key.

Contribution. Let us correlate the EPR-pair corruption with the quantity of maximally mixed state in a mixture. The density operator of the key $|\psi\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|01\rangle_{AB} - |10\rangle_{AB}\right)$ is $|\psi\rangle\langle\psi|_{AB}$. Let the mixture be a function of p of the form

$$\rho_{p,AB} = (1-p)\,|\psi\rangle\langle\psi|_{AB} + p\frac{Id_{AB}}{4}\,. \tag{10}$$

When the protocol is executed with this mixture the resulting global state of the system is

$$\rho^{d}_{AB\varepsilon} = D_{AB\varepsilon}\left(E_{AB\varepsilon}\left(\rho_{p,AB}\otimes\rho_M\otimes|0\rangle\langle 0|_T\right)E^{\dagger}_{AB\varepsilon}\right)D^{\dagger}_{AB\varepsilon}, \tag{11}$$

and

$$\begin{aligned}\rho^{d}_{\varepsilon} = \mathrm{Tr}_{AB}\left(\rho^{d}_{AB\varepsilon}\right) = \frac{2-p}{2}\left(\rho_M\otimes|0\rangle\langle 0|_T\right) + \\ + \frac{p}{4}\left(U^{\dagger}_{\varepsilon}\left(\rho_M\otimes|0\rangle\langle 0|_T\right)U_{\varepsilon} + U_{\varepsilon}\left(\rho_M\otimes|0\rangle\langle 0|_T\right)U^{\dagger}_{\varepsilon}\right).\end{aligned} \tag{12}$$

Here, we can see that the probability of ρ^{d}_{ε} passing B's verification test is unpleasantly high. Even for $p=1$, i.e., maximally mixed state of the key, the probability P that B will receive state $|0\rangle\langle 0|_T$ (and accept ρ_M as authentic) after the measurement of the tag portion is $P \geqslant 1/2$. Equality $P = 1/2$ holds for the case $p = 1$ and both U_{ε} and $U^{\dagger}_{\varepsilon}$ take the tag portion to $|1\rangle\langle 1|_T$.

With a good protocol, the probability of accepting a message should decrease very fast to zero if something is wrong with the key. Clearly, this is not the case.

2. SIMULATION

Research in the field of quantum algorithms is rarely accompanied with experimental work on a quantum computer. Instead, it employs an abstract notation with qubits, registers and a small set of suitable elementary gates. An environment for calculations and simulations which integrates all the abstractions by design, can be useful and help to focus on the problem being solved. Such an environment has two main parts: an executive kernel and a programming language. Nowadays, we distinguish among imperative, functional and logical programming languages. The basic construction of an imperative language is a command that assigns a value to some variable, e.g., $x := y + 3$. This reflects the underlying hardware architecture of current microprocessors. Functional languages are based on lambda calculus. Logical languages are based on predicate logic.

B. Ömer in [5] studied semantics and abstractions of a programming language suitable for a quantum computer. He developed a language called QCL (Quantum Computer Language) based on formalism of finite dimensional Hilbert spaces. Unfortunately, this language does not support general density matrices and partial operations. Density matrices formalism is needed if we want to study a subsystem of a larger system. One of suitable environments for operations with density matrices is Quantum-Octave formerly developed by P. Gawron and J. Miszczak. Quantum-Octave is a set of functions for Octave, which is a free implementation of Matlab-like environment for numerical simulations.

In the following paragraph we show how to simulate the protocol for qubit authentication using the Quantum-Octave package. First, we need to create the key $|\psi\rangle\langle\psi|_{AB} = \frac{1}{2}(|01\rangle - |10\rangle) \otimes (\langle 01| - \langle 10|)$ and the global state $\rho_{AB\varepsilon} = |\psi\rangle\langle\psi|_{AB} \otimes \rho_M \otimes |0\rangle\langle 0|_T$.

```
#Initial state
vector = Ket([0,0]); state = State(vector);

gate = Circuit(
   ProductGate    (2, Not, [1,2]),
   ProductGate    (2, H  , [1]),
   ControlledGate (2, Not, [1],[2]));

#Apply the circuit to produce the EPR-pair
key    = Evolve(gate,state);
global = kron(key, kron(msg, State(Ket([0])))) ;
```

The next step is to prepare the encoding and decoding unitary matrices,

$$E_{A\varepsilon} = |0\rangle\langle 0|_A \otimes Id_B \otimes Id_\varepsilon + |1\rangle\langle 1|_A \otimes Id_B \otimes U_\varepsilon$$

and

$$D_{B\varepsilon} = Id_A \otimes |0\rangle\langle 0|_B \otimes U_\varepsilon^\dagger + Id_A \otimes |1\rangle\langle 1|_B \otimes Id_\varepsilon.$$

```
P0=Projection([0]); P1=Projection([1]); U=kron(H,H)*CNOT;

E = kron(P0, kron(Id, Id(2))) + kron(P1, kron(Id, U));
D = kron(Id, kron(P0, U')) + kron(Id, kron(P1,Id(2)));
```

Now we are ready to evolve the system and measure the tag.

```
global2 = Evolve(E,global);
global3 = Evolve(D,global2);

#Trace out the key and measure the tag-portion
tagged_message = PTrace(global3,[1,2])
result = Measure(tagged_message,"IZ");
```

CONCLUSIONS

The protocol for qubit authentication as proposed in [1] was discussed in the first part of the paper. The authors of the paper [1] evaluated the protocol as unsuitable due to probability $P = 1$ that the adversary party E is able to modify the message in the channel keeping the tag portion intact. However, they do not state a form and consequences of such an attack. This paper considers the case where the transformation U_ε from the coding set $\{Id, U_\varepsilon\}$ is a separable gate. In such a scenario, E's attack could have the form $Q_E = X \otimes Id$, where X is a unitary matrix without further conditions.

Then it has been shown that the protocol does not reflect the secret-key impurity in a secure manner. Even if the secret key is close to the maximally mixed state (unacceptable situation) the probability of accepting a corrupted message ρ_M as authentic is $P \geqslant 1/2$.

In the second part of the paper, it has been shown how to simulate the discussed protocol using the Quantum-Octave package. The Quantum-Octave package is based on the density matrices formalism for quantum computing and uses imperative programming language style. People familiar with languages such as Pascal or C will find it easy to learn.

Acknowledgements. This work was supported by the Grant Agency of the Czech Technical University under the grant CTU0507213.

REFERENCES

1. *Curty M. et al.* Qubit Authentication // Phys. Rev. A. 2002. V. 66. P. 022301.
2. *Leung D. W.* Quantum Vernam Cipher // Quant. Inform. & Computation. 2002. V. 2(1). P. 14–34.
3. *Barnum H. et al.* Authentication of Quantum Messages. quant-ph/0205128.
4. *Bennett C. H. et al.* Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels // Phys. Rev. Lett. 1996. V. 76. P. 722–725.
5. *Ömer B.* Structured Quantum Programming. Ph.D. Thesis, TU Vienna. Vienna, 2003.