Proceedings of 2005 5th IEEE Conference on Nanotechnology
Nagoya, Japan, July 2005

Performing Authenticated Encryption with Nanoscale Phenomenon

Yi-Lin Ju, I-Ming Tsai and Sy-Yen Kuo
Department of Electrical Engineering, National Taiwan University
No.1, Sec. 4, Roosevelt Road, Taipei, Taiwan, 106
Telephone: +886-2-33663577, Fax: +886-2-23689172
E-mail: sykuo@cc.ee.ntu.edu.tw

***Abstract*— Recent progress in nanotechnology has focused on applying nanoscale phenomenon in physical layer or device level applications. In this paper, we show that nanoscale phenomenon can not only be used in physical layer, but also in high layer application such as communication protocols. In this paper, we study the possibility of performing authentication and encryption based on quantum entanglement, which is a phenomenon available only at the nanoscale level. Unlike classical authentication and encryption algorithms, the security of this protocol is based on nanoscale physical laws, instead of any unproven mathematic conjecture.**

***Index Terms*— Nanotechnology, Entanglement, Authentication, Quantum Circuits.**

I. Introduction

Nanotechnology is a highly interdisciplinary field of research and hence can be applied to many fields in computer science and electrical engineering. Today, nanoscale materials are used in electronic, magnetic, biomedical, pharmaceutical and many other physical layer or device level applications. In addition to these device level applications, it has been shown that nanoscale properties can also be applied to some high level applications. Cryptography, most notably key distribution, is one example. Quantum key distribution (QKD) [1] guarantees to distribute the key with absolute security. Another important topic in cryptography is *authentication*. Authentication is a process that you can used to verify that someone is exactly the one he/she claims. A typical example is to use username and password to verify the identity of a person. However, most classical authentication protocols are based on mathematical conjectures and are only conditionally secure. In this paper, we study the possibility of performing quantum authenticated encryption, whose security is based on nanoscale physical laws, instead of unproven mathematical hard problems.

II. Background

In quantum mechanics, the state of a single two-level quantum bit (qubit) can be written as a linear combination in a two-dimensional complex vector space as $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where α and β are complex numbers and $|\alpha|^2 + |\beta|^2 = 1$. The two orthonormal states $|0\rangle$ and $|1\rangle$ form a computational basis of the system. The contribution of each basis state to the overall state (in this case $|\alpha|$ and $|\beta|$) is called the probability amplitude. Similarly, a multi-qubit system can be modeled by a 2^n-dimensional vector space.

A qubit can be manipulated using *quantum gates.* An example of a quantum gate is the quantum **NOT** gate, For example, when a qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ goes through a quantum **NOT** gate (as depicted in Fig.1(a)), the state changes to $|\psi'\rangle = \beta|0\rangle + \alpha|1\rangle$. Another example is the *Hadamard* (**H**) gate, which changes $|0\rangle \rightarrow 1/\sqrt{2}(|0\rangle + |1\rangle)$ and $|1\rangle \rightarrow 1/\sqrt{2}(|0\rangle - |1\rangle)$. An example of a two-qubit gate is the **CONTROL-NOT** (**CN**) gate (as depicted in Fig.1(b)). A **CN** gate consists of one *control* bit x and one *target* bit y. The target qubit will be inverted only when the control qubit is $|1\rangle$. Assuming x is the control bit, the gate can be written as $\mathbf{CN}(|x, y\rangle)= |x, x \oplus y\rangle$, where $\oplus$ denotes exclusive-or. A three-qubit analogue to the **CN** gate is the **CCN** gate (as depicted in Fig.1(c)), which has two control qubits and one target qubit. The **CCN** gate performs $\mathbf{CCN}(|x, y, z\rangle)= |x, y, (x \cdot y) \oplus z\rangle$ and is universal in terms of Boolean functions. It is trivial to generalize the control part of these gates to any Boolean function. For example, a three-qubit **XOR-NOT** gate is to invert the target when the two control qubits differ from each other, as depicted in Fig.1(d).

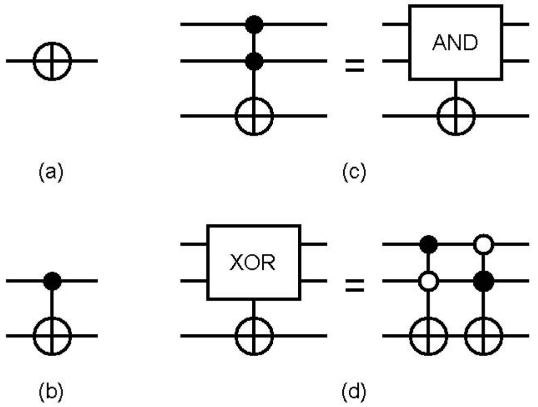

Fig. 1. The symbols of various quantum gates

0-7803-9199-3/05/$20.00 ©2005 IEEE

An interesting phenomenon in quantum mechanics is entanglement. Imagine that Alice and Bob share a two-qubit system in the state $1/\sqrt{2}(|00\rangle + |11\rangle)_{ab}$, where a and b denote Alice and Bob respectively. According to quantum mechanics, if Alice takes a measurement on qubit a, the state of the qubit will collapse to $|0\rangle$ with a probability of 1/2. Moreover, Alice immediately knows that the state of the other qubit (qubit b) must be $|0\rangle$. In other words, once the measurement result of one qubit is decided, the state of the other one is perfectly correlated and can be instantaneously decided, no matter how far away Alice and Bob are separated. Similarly, if the result of Alices measurement is $|1\rangle$, the other qubit will also be $|1\rangle$. This non-classical correlation among multiple quantum systems is called *quantum entanglement*, because they can not be written as separable states. Studies of different types of entanglement and their applications are an important issue in nanoscale physics.

Entanglement is a phenomenon in quantum mechanics. It has been found to be extremely useful not only at nanoscale device level but also in many high layer applications. Teleportation [2] is one such example. With quantum entanglement, teleportation demonstrates the ability of moving quantum states from one place to another place via a classical communication channel instantaneously. Assume Alice wants to send an unknown qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ to Bob, who shares an entanglement $1/\sqrt{2}(|00\rangle + |11\rangle)_{ab}$ with Alice. This can be done by performing a *Bell measurement* on qubit $|\psi\rangle$ and $|a\rangle$ and then announcing the measurement result. The basis of a Bell measurement is defined as

$$\left\{ \begin{array}{l} |\psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle), \\ |\phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle). \end{array} \right. \tag{1}$$

As we can see, the elements in the basis of a Bell measurement are orthogonal and they form a orthogonal matrix. In this example, the coefficients shown above are actually two interleaving *Hadamard* matrices:

$$H_2 = \left(\begin{array}{cc} 1 & 1 \\ 1 & -1 \end{array} \right). \tag{2}$$

where the subscript '2' denotes that it is a 2×2 Hadamard matrix. Theoretical study on Hadamard matrices shows that a necessary condition of the existence of an $n \times n$ Hadamard matrix is $n = 1$ or $n = 2$ or $n = 4p$ with p an integer. (It is conjectured that these are also sufficient conditions.) An easy way to build a $2n \times 2n$ Hadamard matrix H_{2n} is:

$$H_{2n} = \left(\begin{array}{cc} H_n & H_n \\ H_n & -H_n \end{array} \right). \tag{3}$$

Therefore, it is easy to build a $2^k \times 2^k$ Hadamard matrix H_{2^k} using Eq.(2) and Eq.(3) recursively. An example of an 8×8 Hadamard matrix which will shortly be used in this paper is shown as follows:

$$H_8 = \left(\begin{array}{rrrrrrrr} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{array} \right). \tag{4}$$

In the follow text, we will use $H_8^{i,j}$ to denote the element in row i and column j of an H_8, with $0 \leq i, j \leq 7$. Note that Hadamard matrices are orthogonal matrices. So, exchanging any two rows or two columns of a Hadamard matrix gives another Hadamard matrix.

III. Quantum Authentication Protocol

Authentication is one of the primary objectives of cryptography. It is a process of verifying someone's identity as what he/she claims (individual authentication) and/or verifying whether a message comes from the person indicated (message authentication). For example, in computer networks, you are required to enter your username and password to gain access to the server. The identity of a person or a computer system is given by, in general, a trusted third party such as a government or network administrator. Based on this, an architecture of quantum authentication is sketched as follows.

(1) Each applicant (Alice and Bob) in this protocol must obtain one qubit of an EPR pair from the authenticating server before they can be authenticated. The EPR pairs are shown below.

$$\left\{ \begin{array}{l} |\psi_a\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{\alpha a} \\ |\psi_b\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{\beta b} \end{array} \right. \tag{5}$$

The authenticating server keeps two qubits (α and β) while qubit a and b are given to Alice and Bob respectively.

(2) Assuming Alice wants to transmit a secret message $x \in \{0, 1\}$ to Bob, she can ask the trusted third party to perform a Bell measurement on qubit α and β. This causes an *entanglement swapping* and results in an entanglement between Alice and Bob (qubit a and b). The trusted third party then announces the result r, which is encoded as $r = 0$ in case the measurement result is in $\{|\psi^+\rangle, |\psi^-\rangle\}$, $r = 1$ otherwise.

(3) Alice takes a measurement on her qubit a and gets a result $p \in \{0, 1\}$. She then sends $m = x \oplus p$ to Bob via a public channel.

(4) Bob takes a measurement on his qubit b and gets a result $q \in \{0,1\}$. Then he can recover the secret bit by performing $x = r \oplus q \oplus m$.

Although this protocol works, after this process the applicant will lose his/her entanglement with the trusted third party. A more sophisticated protocol which preserves the entanglement between the trusted third party and the applicant is described as follows.

STEP 1 :
For those who want to be authenticated in this structure (Alice and Bob in this case), they must register to the authenticating server first. This procedure can be done by physically going to the authenticating server so the authenticating server can identify the applicant in a secure way. The authenticating server will issue a *quantum certificate* to the applicant if he/she passes the identification process. This certificate is prepared by the authenticating server using the following procedure. First, the server prepares a 6-qubit entanglement:

$$\frac{1}{2}(|000000\rangle + |010101\rangle + |101010\rangle + |111111\rangle). \qquad (6)$$

In the following text, we refer to these six qubits as m^1, m^2, e^1, e^2, c^1, and c^2, in that order. Then the authenticating server gives qubit c^1 and c^2 to the applicant. To distinguish between Alice and Bob, we will use m_a^1, m_a^2, e_a^1, e_a^2, c_a^1, and c_a^2 to denote the quantum certificate qubits for Alice. Similarly, m_b^1, m_b^2, e_b^1, e_b^2, c_b^1, and c_b^2 are used to denote the qubits for Bob. The initialization procedure of the certificate is depicted in Fig.2.

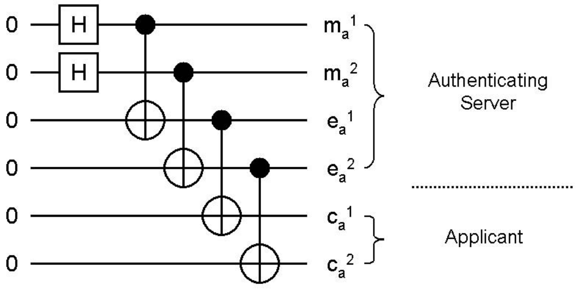

Fig. 2. A quantum circuit showing the initialization procedure

STEP 2 :
Assuming Alice wants to send confidential messages to Bob, she must make a request to the authenticating server so the server can *connect* the channel between Alice and Bob. This is done by first applying a Hadamard gate on m_a^2 and m_b^2 and then taking a measurement on m_a^1, m_a^2, m_b^1, and m_b^1 according to the following basis:

$$|\psi^i\rangle = (H_8^{i,0}|0\rangle + H_8^{i,1}|3\rangle + H_8^{i,2}|5\rangle + H_8^{i,3}|6\rangle$$
$$+H_8^{i,4}|9\rangle + H_8^{i,5}|10\rangle + H_8^{i,6}|12\rangle + H_8^{i,7}|15\rangle) \qquad (7)$$

for $0 \le i \le 7$, and

$$|\psi^i\rangle = (H_8^{i,0}|1\rangle + H_8^{i,1}|2\rangle + H_8^{i,2}|4\rangle + H_8^{i,3}|7\rangle$$
$$+H_8^{i,4}|8\rangle + H_8^{i,5}|11\rangle + H_8^{i,6}|13\rangle + H_8^{i,7}|14\rangle) \qquad (8)$$

for $8 \le i \le 15$, where $H_8^{x,y}$ indicates the element in row x and column y of H_8. For simplicity, we omit the probability amplitudes $(1/\sqrt{8})$ and denote the state in their decimal representation (*i.e.* $|3\rangle = |0011\rangle$ ... etc.). The qubit order is m_a^1, m_a^2, m_b^1, m_b^2. After the measurement, the trusted third party announces the result $r = 0$ if the measurement result is in $\{|\psi^0\rangle \dots |\psi^7\rangle\}$, $r = 1$ if the measurement result is in $\{|\psi^8\rangle \dots |\psi^{15}\rangle\}$. Note that this measurement also decides the state of the remaining qubits. If $r = 0$, the state of e_a^1, e_a^2, c_a^1, c_a^2, e_b^1, e_b^2, c_b^1, c_b^2, up to irrelevant phase differences, becomes

$$\begin{aligned} |\phi_1\rangle &= (|0000\rangle + |1111\rangle) \otimes (|0000\rangle + |1111\rangle) \\ &+ (|0101\rangle + |1010\rangle) \otimes (|0101\rangle + |1010\rangle). \end{aligned} \quad (9)$$

On the other hand, if $r = 1$, the state becomes

$$\begin{aligned} |\phi_2\rangle &= (|0000\rangle + |1111\rangle) \otimes (|0101\rangle + |1010\rangle) \\ &+ (|0101\rangle + |1010\rangle) \otimes (|0000\rangle + |1111\rangle) \end{aligned} (10)$$

The measurement by the trusted third party and the entangled result are depicted in Fig.3.

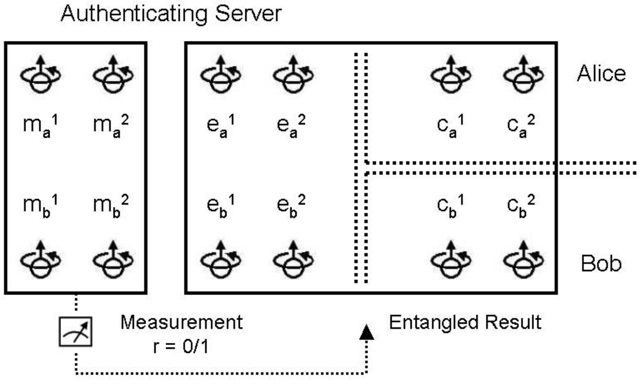

Fig. 3. The measurement causes an entangled result

STEP 3 :
After the channel is set up by the authenticating server, Alice prepares a qubit $|0\rangle$ and performs a **XOR-NOT** on it using c_a^1 and c_a^2 as the control qubits. Then Alice takes a measurement on this qubit and gets a result $p \in \{0,1\}$. Assuming Alice wants to send a secret bit $x \in \{0,1\}$ to Bob, she sends $m = p \oplus x$ to Bob via the classical public channel. Note that the state after Alice's measurement depends on her result. If the result $p = 0$, the state becomes

$$|\phi_1\rangle = (|0101\rangle + |1010\rangle) \otimes (|0101\rangle + |1010\rangle). \qquad (11)$$

However, if the result $p = 1$, the state becomes

$$|\phi_2\rangle = (|0000\rangle + |1111\rangle) \otimes (|0101\rangle + |1010\rangle). \quad (12)$$

Again, these states are shown according to the order e_a^1, e_a^2, c_a^1, c_a^2, e_b^1, e_b^2, c_b^1, c_b^2, up to irrelevant phase differences. The procedure taken by Alice in order to send a secret bit x to Bob is depicted in Fig.4.

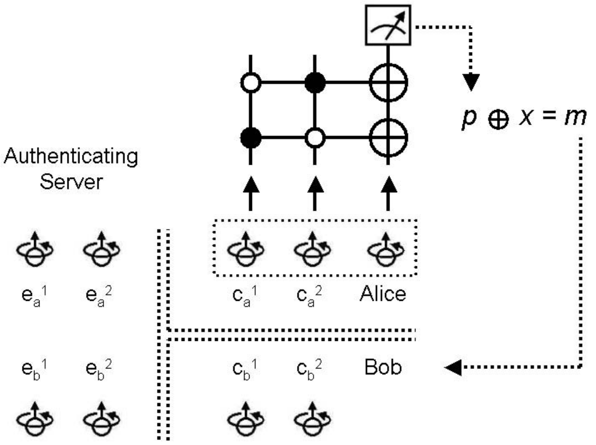

Fig. 4. Alice performs the measurement and sends m to Bob

STEP 4 :
After Bob receives the bit m from Alice, he prepares a qubit $|0\rangle$ and performs a **XOR-NOT** on it using c_b^1 and c_b^2 as the control qubits. Then he takes a measurement on this qubit and gets a result $q \in \{0, 1\}$. The secret bit x can now be recovered since $x = r \oplus q \oplus m$. The recovery procedure performed by Bob is depicted in Fig.5.

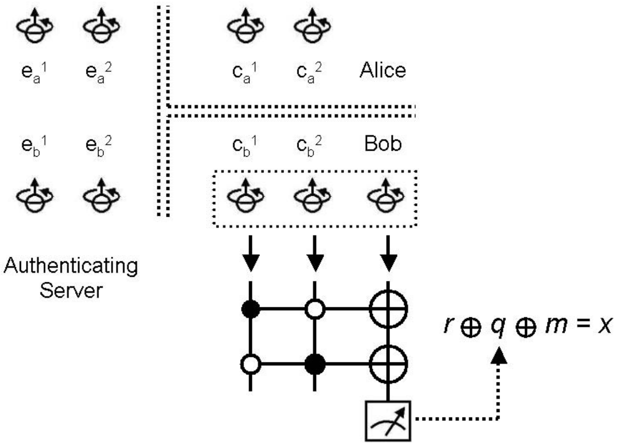

Fig. 5. Bob performs the measurement and extracts x

IV. Analysis And Discussion

In classical cryptography, mutual authentication can be achieved by getting together and negotiating a key secretly. However, in a network environment, manual delivery of keys between each user is not scalable. This is known as the key management problem. Therefore, automatic key management by a trusted third party is necessary. The applicant can get their identity by physically going to the trusted third party, just like applying for a driver license.

After each applicant gets his/her certificate, only classical public channels are required, no qubit exchange is necessary. The only message transmitted across the network is the information that travels in the classical public channel (*i.e.* r and m), which is public readable. Since, according to quantum mechanics, both the measurement results r and $m = p \oplus x$ are random numbers, they are useless for decryption.

Assuming a malicious Eve acts as a man-in-the-middle, Alice and Bob can still detect the existence of Eve because the correlation (*i.e.* entanglement) between Alice and Bob is not interceptable. To detect the existence of Eve, they can send the message first, then a simple error-checking mechanism can be used to check the integrity and reveal the existence of Eve.

Note that after Bob recovers the secret bit x, the state is still either $|\phi_1\rangle$ or $|\phi_2\rangle$ (up to irrelevant phase differences). This is a product state (with e_a^1, e_a^2, e_b^1, e_b^2 belongs to the authenticating server), which means Alice and Bob are no longer entangled. Moreover, each applicant has his/her own entanglement with the authenticating server and can be used later.

V. Conclusion

In this paper, we have demonstrated that nanoscale technologies can not only be used at the physical layer or device level, but also can be applied in high layer applications. We give an example of quantum authentication and encryption protocol. Unlike most classical cryptography primitives which are only conditionally secure, security of this protocol is based on nanoscale physical properties, instead of unproven mathematical hard problems.

References

[1] C. Bennett and G. Brassard, in *Proc. IEEE Int.Conf. on Computers, Systems and Signal Processing*, Bangalore, India (IEEE, New York, 1984), pp.175-179.

[2] C. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. Wootters, "Teleporting an Unknown Quantum State via Dual Classical and EPR Channels", *Phys. Rev. Lett.*, vol. 70, pp.1895-1899 (1993)