Anonymous Quantum Cash

Yuuki Tokunaga,[1,2,*] Tatsuaki Okamoto,[1,†] and Nobuyuki Imoto[2,‡]
[1]*NTT laboratories, 1-1 Hikari-no-oka Yokosuka-shi, Kanagawa-ken 239-0847, Japan*
[2]*School of Advanced Sciences, The Graduate University for Advanced Studies(SOKENDAI), Hayama, Kanagawa, 240-0199, Japan*
(Dated: August 12, 2003)

The most important requirements of a cash system are *impossibility of counterfeiting* and *anonymity*. This paper proposes the first cash system that simultaneously satisfies both of these requirements without computational assumption. Our system is based on the quantum principle, and each bill or coin in our cash system is a quantum string, which is very suitable for constructing a cash system because a quantum string is impossible to copy in principle by "no cloning theorem" in the quantum physics. In addition, this paper presents a concrete example of quantum version of the threshold cryptography, that is, we show a distributed protocol (with threshold) of the quantum cash issuing and validity checking in our anonymous quantum cash scheme.

Keywords: quantum cryptography and security

I. INTRODUCTION

In 1969, Wiesner first came up with an elegant idea to utilize the quantum principle for realizing a cash system that satisfies an important requirement of cash, i.e., the impossibility of counterfeiting [1]. The security against general attack is shown in [2]. This cash system, however, does not satisfy the other important requirement of cash: *anonymity*. There also is an idea of quantum credit card [3], but the stress is laid on authentication, opposite to anonymity, in a credit card system.

Classically, Chaum proposed an electronic cash system satisfying both impossibility of counterfeiting and anonymity, however, it needs computational assumption. [4].

In this paper, we propose a quantum cash system toward satisfying the both requirements of cash: the impossibility of counterfeiting and anonymity without computational assumption.

II. PROPOSED ANONYMOUS QUANTUM CASH

A. Preliminary Phase

The bank uniformly selects $K1^{(v)}$ and $K2^{(v)}$ for each face value v of quantum bills. v is, for example, \$1, \$5, \$10, \$100, ... Here, $K1^{(v)} = (b^{(v)}_{1,1}, \ldots, b^{(v)}_{1,n+1}, b^{(v)}_{2,1}, \ldots, b^{(v)}_{2,n+1}, \cdots\cdots, b^{(v)}_{m,1}, \ldots, b^{(v)}_{m,n+1})$, $K2^{(v)} = (p^{(v)}_1, \ldots, p^{(v)}_m)$ are secret bases and bits kept only in the bank, where $b^{(v)}_{i,j}, p^{(v)}_i \in \{0,1\}$.

B. Withdrawal Phase

In the withdrawal phase, first, the bank constructs a quantum bill, $(v, |\phi\rangle)$, and sends it to a user through a quantum channel and a classical channel. The user then changes it by a randomized unitary transformation, and stores these information in a user's device equipped with quantum and classical registers or memories.

We will show this procedure in detail. First, the bank chooses a random string uniformly $r = (a_{1,1}, \ldots, a_{1,n}, a_{2,1}, \ldots, a_{2,n}, \cdots\cdots, a_{m,1}, \ldots, a_{m,n})$, $(a_{i,j} \in \{0,1\})$.

A quantum bill consists of v (classical string) and a quantum state (quantum string)

$$|\phi\rangle = |\phi_1\rangle \otimes |\phi_2\rangle \otimes \cdots \otimes |\phi_m\rangle,$$

where,

$$|\phi_i\rangle = |\psi_{a_{i,1} b^{(v)}_{i,1}}\rangle \otimes \cdots \otimes |\psi_{a_{i,n} b^{(v)}_{i,n}}\rangle \otimes |\psi_{\alpha_i b^{(v)}_{i,n+1}}\rangle,$$

$$\alpha_i = a_{i,1} \oplus \cdots \oplus a_{i,n} \oplus p^{(v)}_i.$$

Here, $|\psi_{a,b}\rangle$ is defined as follows.

$$\begin{aligned} |\psi_{00}\rangle &= |0\rangle\ , \\ |\psi_{10}\rangle &= |1\rangle\ , \\ |\psi_{01}\rangle &= (|0\rangle + |1\rangle)/\sqrt{2}\ , \\ |\psi_{11}\rangle &= (|0\rangle - |1\rangle)/\sqrt{2}\ . \end{aligned} \tag{1}$$

The value of b_i determines the basis. If b_i is 0 then a_i is encoded in basis Z $(|0\rangle, |1\rangle)$, if b_i is 1 then a_i is encoded in basis X ($(|0\rangle + |1\rangle)/\sqrt{2}$, $(|0\rangle - |1\rangle)/\sqrt{2}$).

If the user pays a shop this bill without any modification, the bank can find the information to whom the bill is issued by tracing the string r. As a result, the user's anonymity cannot be guaranteed.

To assure user's anonymity, the user applies a randomized unitary transformation to $|\phi\rangle$. First, a user picks a random string uniformly $t = (d_{1,1}, \ldots, d_{1,n}, d_{2,1}, \ldots, d_{2,n}, \cdots\cdots, d_{m,1}, \ldots, d_{m,n})$, $(d_{i,j} \in \{0,1\})$.

Here, we define a unitary transformation as follows:

$$U(\theta) = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}.$$

The user applies the following transformation, U, to $|\phi\rangle$.

$$U = U_1 \otimes U_2 \otimes \cdots \otimes U_n,$$

where,

$$U_i = U\left(\frac{\pi}{2} d_{i,1}\right) \otimes \cdots \otimes U\left(\frac{\pi}{2} d_{i,n}\right) \otimes U\left(\frac{\pi}{2} \delta_i\right),$$

and $\delta_i = d_{i,1} \oplus \cdots \oplus d_{i,n}$. We then obtain $|\phi'\rangle$ by this unitary transformation, U:

$$U:\ |\phi\rangle \mapsto |\phi'\rangle.$$

a. Remark Here, we ignore the global phase factor (see p.93 of [5]) because no one can distinguish the deference of the global phase factor.

*tokunaga@isl.ntt.co.jp
†okamoto@isl.ntt.co.jp
‡imoto@soken.ac.jp

C. Payment Phase

After the transformation, the user pays (i.e., sends) the quantum bill $(v, |\phi'\rangle)$ to a shop through a quantum and classical channel. The shop then transmits the bill to the bank for the validity checking. The bank first measures the quantum state $|\phi'\rangle$ with basis $K1^{(v)}$ and gets the string
$(a'_{1,1},\ldots,a'_{1,n},\alpha'_1,a'_{2,1},\ldots,a'_{2,n},\alpha'_2,\cdots\cdots,a'_{m,1},\ldots,a'_{m,n},\alpha'_n)$.
and checks the result whether $\alpha'_i = a'_{i,1}\oplus\ldots\oplus a'_{i,n}\oplus p_i^{(v)}$ $(i=1,\ldots,n)$. Even if one of α'_i is rejected, the bank rejects the quantum bill.

The bank then returns the checking result, "accept" or "reject", and the payment procedure completes.

When the bank rejects the bill, the bank stops all cash transaction and changes all quantum bills to new quantum bills with new secret bases all at once.

III. SECURITY OF THE ANONYMOUS QUANTUM CASH SCHEME

A. Anonymity

Through the transformation, U, of a user in the withdrawal phase, the user obtains $|\phi'\rangle$. $|\phi'\rangle$ encodes string r' and α', while $|\phi\rangle$ encodes string r (uniformly picked by the bank) and α, where $\alpha \equiv (\alpha_1,\alpha_2,\ldots,\alpha_n)$ and $\alpha' \equiv (\alpha'_1,\alpha'_2,\ldots,\alpha'_n)$. Since $r' = r\oplus t$ and t is uniformly selected by the user, r' is uniformly and independently distributed from r. Therefore, $|\phi'\rangle$ is perfectly unlinkable from $|\phi\rangle$.

b. Remark. We assume that the bank makes quantum bills honestly (or trusted third party checks whether the quantum bills are correct or not before the quantum bills are sent to the users). Otherwise, if the bank makes an incorrect quantum bill and sends it to a user, then the bank can trace the incorrect bill, because the user's unitary transformation keeps incorrect bills to incorrect bills. However, once correct quantum bills are sent to users, user's anonymity is kept perfectly, though original Wiesner's scheme cannot keep anonymity at all.

B. Impossibility of Counterfeiting

In this paper, we assume ideal communication channel, then we consider all errors are due to counterfeiters. So, even if an error is detected from a bill, it is due to a counterfeiter, then the bank rejects the bill and stops all cash transaction, and then changes all quantum bills to new quantum bills with new secret bases all at once.

We show our scheme is secure against the attack which measures each quantum bill individually. Note that we allow a counterfeiter global measurement for multiple qubits in a quantum bill. The robustness against global measurement for multiple quantum bills is still an open problem.

In a quantum bill $|\phi\rangle = |\phi_1\rangle\otimes|\phi_2\rangle\otimes\cdots\otimes|\phi_m\rangle$, the parts of quantum bill $|\phi_i\rangle$ and $|\phi_j\rangle$ $(i\neq j)$ are totally independent, then we first consider that $|\phi_i\rangle$ is tried to forge by a counterfeiter.

The secret bit p_i is embedded in $(n+1)$th qubit by taking XOR with $\alpha_i = a_{i,1}\oplus\ldots\oplus a_{i,n}$:the parity of n random numbers. Since same p_i is used in other quantum bills, it might leak some information about the secret bases or the secret bit itself. However, the p_i is embedded in $(n+1)$th qubit by taking XOR with α_i as described above, thus, single bit p_i is fully overlapping in $n+1$ qubits. Namely, one cannot get any information without knowing the parity of $n+1$ bits $a_{i,1}\oplus\ldots\oplus a_{i,n}\oplus(\alpha_i\oplus p_i) = p_i$ in $n+1$ qubits. The probability that parity 0 and parity 1 are distinguished correctly in such a situation is $1/2+e$, here, e decreases exponentially with n as shown in [7]. Therefore, a counterfeiter can extract secret information with exponentially small probability when he measures a quantum bill.

IV. THRESHOLD PROTOCOL FOR ISSUING AND CHECKING

If bank's secret key of a cash value is stolen by adversaries, then they can counterfeit quantum bills with this value freely as they like. So, to reduce such a risk, a distributed system is very effective, in which a secret key is split into several pieces, and each of several centers holds each secret piece, and in the daily operation and management, these several centers collaborate to issue a quantum bill and to check its validity.

In this paper, we propose such a distributed version (with threshold) of our anonymous quantum cash system. Our scheme employs Shamir's secret sharing scheme [6], i.e., t out of n scheme, in which a secret value is shared by n centers, and any t centers among them can recover the secret value, but any $t-1$ centers can obtain no information on it. In our scheme, n shares, $S_1,\ldots,S_n$, (classical strings) of bank's secret key (e.g., $K^{(v)}$) is given to n centers, $P_1,\ldots,P_n$. In the withdrawal phase, arbitrary t centers among the n centers collaborate to generate a quantum bill. Here, for simplicity, we assume $P_1,\ldots,P_t$, collaborate. First, P_1 generates a quantum string, which is the initial state, and makes the first unitary transformation on it with S_1, and sends it to P_2. P_2 makes another unitary transformation with S_2 and sends it to P_3. After repeating this procedure, finally P_t outputs a quantum bill and sends it to a user. Similarly, the validity check of a quantum bill can be made by arbitrary t centers. Here it is worth noting that the share, S_i, of each center P_i is kept secret inside each center during the collaboration.

Acknowledgments

We thank K. Shimizu and K. Suzuki of NTT for helpful discussions.

[1] S. Wiesner: Conjugate Coding, Manuscript written circa 1970, unpublished until it appeared in Sigact News, Vol.15, No.1 pp.78–88 (1983)
[2] H. K. Lo and H. Chau: Unconditional Security of Quantum Key Distribution over Arbitrary Long Distances, Science, Vol. 283, pp. 2050–2056 (1999).
[3] O. Hirota, Y. Ishii, Y. Saito and A. Hataya: A construction of quantum credit card with authentication, Nat. conf. of IEICE of Japan, A-7-6, 2002.
[4] D. Chaum: Security without identification: Transaction systems to make big brother obsolete, Communications of the ACM, Vol.28, No.10, pp.1030–1044 (1985).
[5] M. A. Nielsen and I. L. Chuang: Quantum Computation and Quantum Information, Cambridge University Press (2000).
[6] A. Shamir: How to Share a Secret, Comm. Assoc. Comput. Mach., Vol.22, No.11, pp.612–613 (1979)
[7] C. H. Bennett, T. Mor and J. A. Smolin: The parity Bit in Quantum Cryptography, Physical Review A, 54, 2675 (1996).