Universal Electronic Cash

Tatsuaki Okamoto Kazuo Ohta

NTT Laboratories
Nippon Telegraph and Telephone Corporation
1-2356, Take, Yokosuka-shi, Kanagawa-ken, 238-03 Japan

Abstract

This paper proposes the first ideal untraceable electronic cash system which solves the most crucial problem inherent with real cash and all previous untraceable electronic cash systems. The main advantage of the new system is that the customer can subdivide his cash balance, C (dollars), into many pieces in any way he pleases until the total value of all subdivided piece equals C. This system can be implemented efficiently. In a typical implementation, the data size of one piece of electronic cash is less than 100 bytes regardless of the face value of piece, the computation time for each transaction is several seconds, assuming the existence of a Rabin scheme chip. The security of this scheme relies on the difficulty of factoring.

1 Introduction

Electronic cash is one of the most important applications of modern cryptology because an electronic money (cash) system will be widely installed in the near future; smart cards will become electronic wallets storing electronic cash. The security of real cash heavily depends on physical properties such as the difficulty of reproducing bills and coins. The security of electronic cash systems cannot depend on any physical condition, but must be guaranteed by mathematics. Here, cryptographic techniques are essentially used to guarantee security. Then, information itself has a value, and electronic cash can be transfered through networks.

What then is the ideal cash system? The criteria describing the ideal cash system are as follows:

(a) *Independence*: The security of electronic cash cannot depend on any physical condition. Then the cash can be transfered through networks.

(b) *Security*: The ability to copy (reuse) and forge the cash must be prevented.

(c) *Privacy (Untraceability)*: The privacy of the user should be protected. That is, the relationship between the user and his purchases must be untraceable by anyone.

(d) *Off-line payment*: When a user pay the electronic cash to a shop, the procedure between the user and the shop should be executed in an off-line manner. That is, the shop does not need to be linked to the host in user's payment procedure.

J. Feigenbaum (Ed.): Advances in Cryptology - CRYPTO '91, LNCS 576, pp. 324-337, 1992.

(e) *Transferability*: The cash can be transfered to other users.

(f) *Dividability*: One issued piece of cash worth value C (dollars) can be subdivided into many pieces such that each subdivided piece is worth any desired value less than C and the total value of all pieces is equivalent to C.

Several electronic cash systems have been proposed by [Ch, Da, PW, EGY, OkOh2, CFN, OkOh1]. The security of the electronic cash system by [EGY] depends on a physical condition. Therefore, [EGY] does not satisfy criterion (a). There are two types of electronic cash systems satisfying criteria (a), (b) and (c); *on-line untraceable* electronic cash systems, and *off-line untraceable* electronic cash systems.

Some *on-line untraceable* electronic cash systems have been proposed by [Ch, Da, PW], which satisfy criteria (a) through (f) except criterion (d). However, the on-line cash systems are not practical from the viewpoints of turn-around-time, communication cost, and database-maintainance cost. Therefore, the off-line cash systems are preferable from the practical viewpoint, although they are technically difficult to construct.

An *off-line untraceable* electronic cash system satisfying criteria (a), (b), (c) and (d) was firstly proposed by [CFN], based on the cut-and-choose methodology and a collision free one-way function technique. An electronic cash system satisfying criteria (a), (b), (c), (d) and (e) was then proposed by [OkOh1]. In [OkOh1], the disposable zero-knowledge authentication scheme is used in place of the collision free function technique in [CFN].

In [OkOh1], an electronic coupon ticket system was also proposed, in which one piece of electronic cash can be subdivided into many pieces whose values are all equivalent. In this system, however, if a customer pays for an article with cents, the store receives an enormous number of one-cent electronic coupon tickets from the customer (for example, when the price of the article is \$356.27, the store receives 35627 electronic coupon tickets, where the data size of each ticket is several kilobytes. So, the store receives about 200 megabytes of data for purchasing just one article.) Therefore, no electronic cash system satisfying criterion (f) as well as the other criteria (a) through (e) has been proposed so far.

It must be noted that even the real cash system cannot satisfy criterion (f). This is the reason why we must hold many bills and coins in our wallets. On the other hand, other typical exchange systems such as bank notes and credit cards do not satisfy criteria (a) and (c). Prepaid cards such as telephone cards do not satisfy criterion (a), although they almost satisfy critria (b) through (f). Therefore, we do not have the ideal cash system so far, either electronic or real.

In this paper, we propose the first electronic cash system that satisfies all six criteria. That is, this system is the first version of the ideal cash system. Moreover, the new system is more efficient and practical than any previous system even if we restrict the comparison to the two criteria (a) through (d).

Our scheme uses the cut-and-choose methodology as all previous schemes. The new key techniques of our scheme are the square root molulo N (N is the Williams integer), and the hierarchical structure table. The former is used mainly for criteria (a) through (e) (or in place of the techniques such as the collision free function [CFN], and disposable zero-knowledge authentication [OkOh1]. The latter combined with the former is used for criterion (f), where the hierarchical structure table corresponds to the structure of the cash system.

This paper is constructed as follows: First, in section 2, we will introduce the background of the key techniques including the number theoretic conventions, and the hierarchical structure table of the cash system. In section 3, we will propose the basic version of our electronic cash system. Section 4 explains how electronic credits can be transfered to another customer. Section 5 estimates the properties of the electronic cash system.

2 Preparations

2.1 Number Theoretic Conventions

Definition 2.1 *N is called the Blum integer [Bl] if $N = PQ$ (P, Q are prime) and $P = 3 \pmod 4$, and $Q = 3 \pmod 4$.*
N is called the Williams integer [W] if $N = PQ$ (P, Q are prime) and $P = 3 \pmod 8$, and $Q = 7 \pmod 8$. Note that the Williams interger is a specific type of the Blum integer. So, the Williams integer has all properties of the Blum integer.

Let (x/N) denote the Jacobi symbol, when N is a composite number, and denote the Legendre symbol, when N is a prime. When $N = PQ$ (P, Q are prime), we can classify Z_N^* into four classes; $Z_{(1,1)} = \{x \in Z_N^* \mid (x/P) = 1, (x/Q) = 1\}$ $Z_{(1,-1)} = \{x \in Z_N^* \mid (x/P) = 1, (x/Q) = -1\}$, $Z_{(-1,1)} = \{x \in Z_N^* \mid (x/P) = -1, (x/Q) = 1\}$, and $Z_{(-1,-1)} = \{x \in Z_N^* \mid (x/P) = -1, (x/Q) = -1\}$.

Clearly, $Z_{(1,1)}$ denotes the set of quadratic residue intergers in Z_N^*. Hereafter, we often write QR_N as $Z_{(1,1)}$, and QNR_N as the other classes.

Proposition 2.2 *Let N be the Blum integer, and $x \in QR_N$. Then, for any integer t ($1 \leq t$), there are four values y_1, y_2, y_3, y_4 such that $y_i^{2^t} \equiv x \pmod N$ and that $y_1 \in Z_{(1,1)}$, $y_2 \in Z_{(1,-1)}$, $y_3 \in Z_{(-1,1)}$, $y_4 \in Z_{(-1,-1)}$.*
In addition, $y_1 \equiv -y_4 \pmod N$, $y_2 \equiv -y_3 \pmod N$, $(y_1/N) = (y_4/N) = 1$, and $(y_2/N) = (y_3/N) = -1$.

The above proposition immediately implies that four values of 2^t-th root y of x can be uniquely determined by two bit information; one is whether $(y/N) = 1$ or -1, and the other is whether $y < N/2$ or not. In other words, when $y < N/2$, there are two values of y, one of which is $(y/N) = 1$ and the other is $(y/N) = -1$.

$x^{1/2^t} \bmod N$ ($1 \leq t$) can be computed efficiently (in expected polynomial time) from x, P, Q [R, Ber], and (y/N) can also be computed efficiently from y and N, while to compute $x^{1/2^t} \bmod N$ from x and N is as difficult as factoring N [R].

Proposition 2.3 *Let $N = PQ$ be the Williams integer. Then, for any $x \in Z_N^*$, either one of $x, -x, 2x$ and $-2x$ is in QR_N. In addition, when $ax \in QR_N$ (a is either $1, -1, 2$, or -2), bx is not in QR_N ($b \neq a$, and b is either $1, -1, 2$, or -2).*

The above proposition is easily proven by the following result;

$$(-1/P) = -1, (-1/Q) = -1, (2/P) = -1, (2/Q) = 1.$$

Definition 2.4 *Let N be the Williams integer, and $x \in QR_N$.*

$$[x^{1/2^t} \bmod N]_{QR} = y$$

such that $y^{2^t} = x \bmod N$ *and* $y \in QR_N$. $(1 \leq t)$

$$[x^{1/2^t} \bmod N]_1 = y'$$

such that $y'^{2^t} = x \bmod N$, $(y'/N) = 1$ *and* $0 < y' < N/2$. $(1 \leq t)$

$$[x^{1/2^t} \bmod N]_{-1} = y''$$

such that $y''^{2^t} = x \bmod N$, $(y''/N) = -1$ *and* $0 < y'' < N/2$. $(1 \leq t)$
Let N *be the Williams integer, and* $z \in Z_N^*$.

$$< z >_{QR} = dz \bmod N$$

such that $d \in \{\pm 1, \pm 2\}$ *and* $dz \bmod N \in QR_N$.

$$< z >_1 = d'z \bmod N$$

such that $d' \in \{1, 2\}$ *and* $(d'z/N) = 1$.

$$< z >_{-1} = d''z \bmod N$$

such that $d'' \in \{1, 2\}$ and $(d''z/N) = -1$.

From the properties of the Williams number (and the Blum number), each value of y, y', y'', d, d', d'' is uniquely determined respectively.

2.2 Hierarchical Structure Table

In our cash system, the hierarchical structure table plays an important role because it allows the issued electronic bill C to be subdivided into many pieces such that each subdivided piece is worth any desired value less than C and the total value of all pieces is equivalent to C.

The hierarchical structure table is a tree of t levels, in which each node has two sons, the unique root node exists at the top of the tree. So, there are 2^{i-1} nodes at the i-th level.

Here, we show the significance of the tree in our cash system. For easy understanding, we use a simple example, where the tree has three levels, and the value of the issued bill C is \$100. The nodes of the i-th level correspond to $\$100/2^{i-1}$. So, the customer can use the bill in \$25 increments, since the nodes of the bottom level (the third level) correspond to \$25 (see Figure 1).

We give two restrictions to the usage of the bill with relating to the tree as follows:

1. The value corresponding to a node, N, is the total of the values corresponding to nodes that are the direct sons of N.

2. When a node (the corresponding value) is used, all descendant nodes and all ancestor nodes of this node cannot be used.

3. No node can be used more than once.

We show the case when customer Alice uses \$75 first and then uses \$25. When she uses \$75, she must use node Γ_{00} (\$50), and node Γ_{010} (\$25). From the above restrictions, only Γ_{011} (\$25) can be used after the use of Γ_{00} and Γ_{010} (see Figure 2).

More generally, if Alice wants to use a bill worth \$1000 by the cent, she would need a hierarchical structure table of 17 levels ($\log_2 100000 \approx 16.5$). She would then use about 8 nodes in average (minimum: one node; maximum: 16 nodes) in order to pay by the cent for each purchase (e.g., \$334.36 payment).

Moreover, in our concrete cash scheme that will be shown in the following sections, we need two hierarchical structure tables (Γ table and Λ table); Γ table is used to realize the first restriction, and Λ table to realize the second restriction. Γ table and Λ table have the same structure such that they are trees with the same topology (or the same number of layers), and that $\Gamma_{j_1 \dots j_t}$ and $\Lambda_{j_1 \dots j_t}$ both correspond to the same position node ($\mathrm{Node}_{j_1 \dots j_t}$) of the money structure table. In the example of Figures 1 and 2, Γ_{00} and Λ_{00} correspond to the same position node, the left node of \$50, of the money structure table.

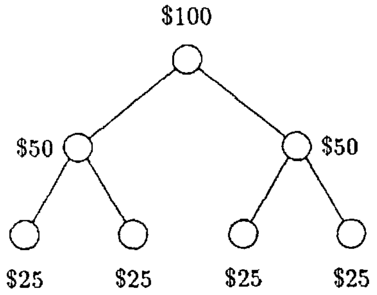

Figure 1: Hierarchical Structure Table (Money Structure)

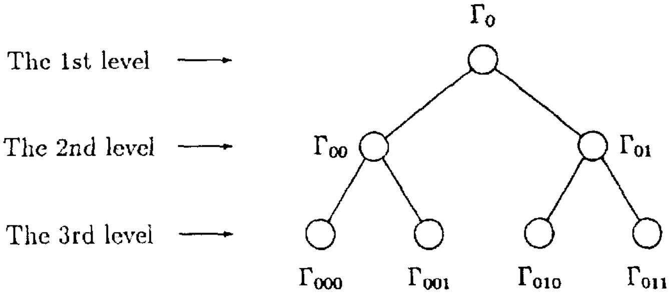

Figure 2: Hierarchical Structure Table (Γ Table)

3 Basic Universal Electronic Cash Scheme

In this section, we introduce the basic universal electronic cash scheme which satisfies the five criteria ((a) through (f) except (c)(Transferability)).

3.1 Protocol

Protocol 1 (Basic universal electronic cash):

For blind digital signatures[Ch], bank A has generated keys of the RSA scheme; $(e_A, n_A; d_A)$, $(e'_A, n'_A; d'_A)$, $(e''_A, n''_A; d''_A)$, ..., where (e_A, n_A),(e'_A, n'_A), ... are public keys, and $d_A, d'_A, \ldots$ are the corresponding secret keys. A has published $(e_A, n_A), (e'_A, n'_A), (e''_A, n''_A), \ldots$, where (e_A, n_A) corresponds to the *electronic license* that A issues, and (e'_A, n'_A), $(e''_A, n''_A), \ldots$ correspond to the value of the *electronic bill* that A issues. For example, \$100 corresponds to (e'_A, n'_A), and \$500 corresponds to (e''_A, n''_A), etc. Bank A also sets the security parameter $K = O(|n_A|) = O(|n'_A|) = \ldots$ (for example, $K = 40$).

A has also published three randomized hash functions, $f_\Gamma, f_\Lambda, f_\Omega$, to generate the hierarchical structure tables, Γ table and Λ table. Here, the function values are assumed to distribute uniformly (for example, the universal hash functions [CW], and pseudo-random generator). Note that the one-wayness or collision-freeness is not required for these functions.

Customer P has a bank account number ID_P and has generated the key of the RSA scheme, $(e_P, n_P; d_P)$, and published (e_P, n_P) for digital signatures.

Note 1: Any multiple blind digital signature [OkOh1] can be used in place of the RSA scheme for bank A above. For example, the blind digital signature scheme based on the Fiat-Shamir signature scheme [OkOh2] can be used for this purpose. Moreover, any digital signature scheme can be used in place of the RSA scheme for customer P above. For example, [FOM] can be used for this purpose.

Note 2: The secure exchange problem is out of the scope of this paper. For example, A and P exchange electronic cash and withdrawal, P and V exchange payment and articles, and V and A exchange payment history and credit. The secure exchange problem can be practically solved by the usage of digital signature schemes. More secure but less efficient solutions for this problem has been shown in [EGL].

Part I.

When a customer P opens an account at bank A, A issues an electronic license $B = \{B_i \mid 1 \leq i \leq K/2\}$ to use the electronic cash of bank A. (Precisely, the electronic license is $(B, \{I_i, N_i\}, L)$. For simplicity, however, we simply call it B.) To get B, P conducts the following protocol with A. This procedure is executed *only once* when P opens the account, unless P uses the electronic cash invalidly.

Step 1: Customer P chooses a random value a_i, and the Williams integers N_i with two large prime factors P_i, Q_i ($N_i = P_i Q_i$), where $P_i \equiv 3 \pmod 8$ and $Q_i \equiv 7 \pmod 8$, for $i = 1, \ldots, K$.

Step 2: P forms and sends K blind candidates $W_i (i = 1, \ldots, K)$ to bank A.

$$W_i = r_i^{e_A} g(I_i \parallel N_i) \bmod n_A \quad \text{for } 1 \leq i \leq K,$$

where $r_i \in Z_{n_A}$ is a random integer, g is an appropriate one-way hash function, and

$$S_i = ID_P \parallel a_i \parallel (g(ID_P \parallel a_i))^{d_P} \bmod n_P,$$
$$= S_{1,i} \parallel S_{2,i},$$
$$I_{1,i} = S_{1,i}^2 \bmod N_i,\ I_{2,i} = S_{2,i}^2 \bmod N_i,$$
$$I_i = I_{1,i} \parallel I_{2,i}.$$

Here, $\parallel$ denotes the concatenation.

Step 3: A chooses a random subset of $K/2$ blind candidates indices $U = \{i_j\}, 1 \leq i_j \leq K$ for $1 \leq j \leq K/2$ and transmits it to P.

Step 4: P displays the a_i, P_i, Q_i, $(g(ID_P \parallel a_i))^{d_P} \bmod n_P$, ID_P, r_i for all i in U, then A checks them. If they are not valid, A halts this protocol. To simplify notations, we will assume that $U = \{K/2+1, K/2+2, \ldots, K\}$.

Step 5: A gives P

$$(\prod_{i=1}^{K/2} W_i)^{d_A} \bmod n_A.$$

Step 6: P can then extract the electronic license $B = (\prod_{i=1}^{K/2} g(I_i \parallel N_i))^{d_A} \bmod n_A$.

Part II.

When customer P wants bank A to issue an electronic bill worth \$100, C, which corresponds to (e'_A, n'_A), P conducts the following protocol with A.

Step 1: P chooses a random value b, forms and sends Z to A.

$$Z = r^{e'_A} g(B \parallel b) \bmod n'_A,$$

where $r \in Z_{n'_A}$ is a random integer.

Step 2: A gives $Z^{d'_A} \bmod n'_A$ to P and charges P's account \$100.

Step 3: P can then extract the electronic bill $C = (g(B \parallel b))^{d'_A} \bmod n'_A$.

Part III.

To pay a shop V a certain amount of money, P and V proceed as follows:
First, for easy understanding, we will show a simple example of this protocol, when P pays \$75 to V based on the hierarchical structure table of three levels, as was shown in subsection 2.2. Here, we assume that P has received \$100 bill C from Bank A in Part II.

Step 1: As the preliminary stage of Part III, P computes the value of $\Gamma_{i,0}$ $(i = 1, \ldots, K/2)$ as follows:

$$\Gamma_{i,0} =< f_\Gamma(C \parallel 0 \parallel N_i) >_{QR}.$$

(See Subsection 2.1 for the notation of $<>_{QR}$.)

Step 2: When P decides to pay \$75, first P computes $X_{i,00}$ (corresponding to \$50) and $X_{i,010}$ (corresponding to \$25) $(i = 1, \ldots, K/2)$ as follows:

$$X_{i,00} = [\Gamma_{i,0}^{1/4} \bmod N_i]_{-1}$$

$$X_{i,010} = [(\Omega_{i,0}^2\Gamma_{i,0})^{1/8} \bmod N_i]_{-1}.$$

Here, $\Omega_{i,0} =< f_\Omega(C \parallel 0 \parallel N_i) >_1$.
P sends (I_i, N_i, $X_{i,00}$, $X_{i,010}$) ($i = 1, \ldots, K/2$) and (B, C) to V.

Note: The above calculation of $X_{i,00}$ and $X_{i,010}$ is based on the following algorithm:

$$X_{i,00} = [\Gamma_{i,00}^{1/2} \bmod N_i]_{-1},$$

$$X_{i,010} = [\Gamma_{i,010}^{1/2} \bmod N_i]_{-1},$$

where

$$\Gamma_{i,00} = [\Gamma_{i,0}^{1/2} \bmod N_i]_{QR}$$

$$\Gamma_{i,01} = [\Omega_{i,0}\Gamma_{i,0}^{1/2} \bmod N_i]_{QR}$$

$$\Gamma_{i,010} = [\Gamma_{i,01}^{1/2} \bmod N_i]_{QR}$$

Here, summarizing the algorithm, first, the Γ table of the correponding nodes ($\Gamma_{i,00}$, $\Gamma_{i,010}$) are calculated, then the square roots of these values in QNR (these Jacobi symbol values are -1) are $X_{i,00}$ and $X_{i,010}$.

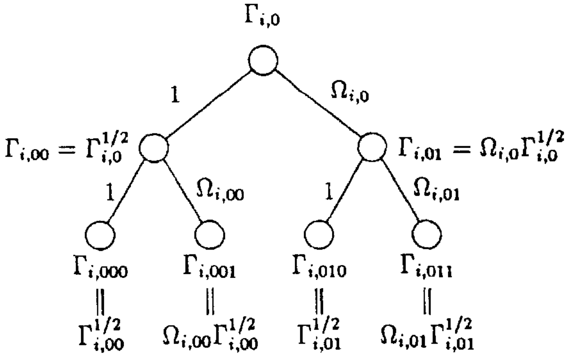

Figure 3: Node Values of Γ Table (Three Layer Example)

Step 3: V verifies the validity of the signatures B for $\{(I_i, N_i)\}$, and C for B. V computes $\Omega_{i,0}$, $f_\Gamma(C \parallel 0 \parallel N_i)$ then verifies the validity of $X_{i,00}$ and $X_{i,010}$ ($i = 1, \ldots, K/2$) such that

$$(X_{i,00}/N_i) = (X_{i,010}/N_i) = -1,$$

$$X_{i,00}^4 = d_i f_\Gamma(C \parallel 0 \parallel N_i) \bmod N_i$$

$$X_{i,010}^8 = d_i\Omega_{i,0}^2 f_\Gamma(C \parallel 0 \parallel N_i) \bmod N_i,$$

where $d_i \in \{\pm1, \pm2\}$ ($i = 1, \ldots, K/2$). If they are valid, V selects random bits, $E_{i,00}$, $E_{i,010} \in \{0, 1\}$ ($i = 1, \ldots, K/2$), and sends them to P. Otherwise V halts this protocol.

Step 4: P computes

$$Y_{i,00} = [\Lambda_{i,00}^{1/2} \bmod N_i]_{(-1)^{E_{i,00}}},$$

$$Y_{i,010} = [\Lambda_{i,010}^{1/2} \bmod N_i]_{(-1)^{E_{i,010}}},$$

and sends $(Y_{i,00}, Y_{i,010})$ $(i = 1, \ldots, K/2)$ to V. Here,

$$\Lambda_{i,00} =< f_\Lambda(C \parallel 00 \parallel N_i) >_{QR},$$

$$\Lambda_{i,010} =< f_\Lambda(C \parallel 010 \parallel N_i) >_{QR}.$$

Step 5: V verifies that

$$(Y_{i,00}/N_i) = (-1)^{E_{i,00}}, (Y_{i,010}/N_i) = (-1)^{E_{i,010}},$$

$$Y_{i,00}^2 = d_i' f_\Lambda(C \parallel 00 \parallel N_i) \bmod N_i,$$

$$Y_{i,010}^2 = d_i'' f_\Lambda(C \parallel 010 \parallel N_i) \bmod N_i,$$

where $d_i', d_i'' \in \{\pm 1, \pm 2\}$ $(i = 1, \ldots, K/2)$. If verification succeeds, V accepts P's messages as \$75 from electronic bill C.

Next, we show the protocol of Part III in general cases. Here, we assume that Γ table has more than t levels, and that the node corresponding to the value of P's payment to V is $\Gamma_{j_1 \ldots j_t}$ (and $\Lambda_{j_1 \ldots j_t}$), where $j_1, \ldots, j_t \in \{0, 1\}$. Usually, there are several nodes which correspond to the payment (e.g., in the above simple example, two nodes form P's \$75 payment). Then, the following protocol of each node must be executed simultaneously, in the same manner as the above protocol, which has two nodes.

Step 1: This preliminary stage of Part III is the same as the above protocol.

Step 2: When P determines the node, $\Gamma_{j_1 \cdots j_t}$ (and $\Lambda_{j_1 \ldots j_t}$), corresponding to the payment, P computes $X_{i,j_1 \cdots j_t}$,

$$X_{i,j_1 \cdots j_t} = [(\Omega_{i,j_1 \cdots j_{t-1}}^{2^{t-1} j_t} \Omega_{i,j_1 \cdots j_{t-2}}^{2^{t-2} j_{t-1}} \cdots \Omega_{i,j_1}^{2 j_2} \Gamma_{i,0})^{1/2^t} \bmod N_i]_{-1},$$

where $\Omega_{i,j_1 \cdots j_t} =< f_\Omega(C \parallel j_1 \parallel \cdots \parallel j_t \parallel N_i) >_1$.
P sends $(I_i, N_i, X_{i,j_1 \cdots j_t})$ $(i = 1, \ldots, K/2)$ and (B, C) to V.
Note: The above calculation of $X_{i,j_1 \cdots j_t}$ is based on the following algorithm:

$$X_{i,j_1 \cdots j_t} = [\Gamma_{i,j_1 \cdots j_t}^{1/2} \bmod N_i]_{-1},$$

where

$$\Gamma_{i,j_1 \cdots j_{t+1}} = [\Omega_{i,j_1 \cdots j_t}^{j_{t+1}} \Gamma_{i,j_1 \cdots j_t}^{1/2} \bmod N_i]_{QR}.$$

Step 3: V verifies the validity of the signatures B for $\{(I_i, N_i)\}$, and C for B. V computes $\Omega_{i,j_1 \ldots j_t}$ (if $j_{t+1} = 1$) then verifies the validity of $X_{i,j_1 \cdots j_t}$ $(i = 1, \ldots, K/2)$ such that

$$(X_{i,j_1 \cdots j_t}/N_i) = -1,$$

$$X_{i,j_1 \cdots j_t}^{2^t} = d_i \Omega_{i,j_1 \cdots j_{t-1}}^{2^{t-1} j_t} \Omega_{i,j_1 \cdots j_{t-2}}^{2^{t-2} j_{t-1}} \cdots \Omega_{i,j_1}^{2 j_2} f_\Gamma(C \parallel 0 \parallel N_i) \bmod N_i,$$

where $d_i \in \{\pm 1, \pm 2\}$ $(i = 1, \ldots, K/2)$. If they are valid, V selects random bits, $E_{i,j_1 \cdots j_t} \in \{0, 1\}$ $(i = 1, \ldots, K/2)$, and sends them to P. Otherwise V halts this protocol.

Step 4: P computes

$$Y_{i,j_1\cdots j_t} = [\Lambda_{i,j_1\cdots j_t}^{1/2} \bmod N_i]_{(-1)^{E_{i,j_1\cdots j_t}}}.$$

Here,

$$\Lambda_{i,j_1\cdots j_t} = < f_\Lambda(C \parallel j_1 \parallel \cdots \parallel j_t \parallel N_i) >_{QR}.$$

Step 5: V verifies that

$$(Y_{i,j_1\cdots j_t}/N_i) = (-1)^{E_{i,j_1\cdots j_t}},$$

$$Y_{i,j_1\cdots j_t}^2 = d'_i f_\Lambda(C \parallel j_1 \parallel \cdots \parallel j_t \parallel N_i) \bmod N_i,$$

where $d'_i \in \{\pm 1, \pm 2\}$ $(i = 1, \ldots, K/2)$. If verification succeeds, V accepts P's messages as payment of the amount due.

Note: To prevent bank A from crediting an invalid shop's account in Part III, we can enhance the protocol as follows: Here, we simply write E_i as $E_{i,j_1\cdots j_t}$. V selects a random value E'_i, and sends V's identity ID_V, time T, and E'_i $(i = 1, \ldots, K/2)$ to P in place of sending E_i. V computes $(E_1, \ldots, E_{K/2}) = h(ID_V \parallel T \parallel E'_1 \cdots E'_{K/2})$, where h is a one-way function whose output is uniformly random. P also computes E_i $(i = 1, \ldots, K/2)$.

Part IV.

For bank A to credit V's account by the appropriate amount, V sends the history of Part III of this protocol, H, to A, which credits V's account. After checking the validity of H, bank A must store H in its database. If A finds an invalid payment, A reveal the secret information S_i of costomer P who is responsible for the invalid payment from H and the related history.

(End of Protocol 1)

Note 1: Since bank A has already known $K/2$ pieces of S_i in Part I (e.g., $S_{K/2+1}, \ldots, S_K$), $(K/2+1)$ pieces of S_i shown by A are the evidence of the invalid payment by a customer.

Note 2: Bank A can store H with dividing it into two parts, H_1 and H_2. H_1 is used to check the invalid payment, and H_2 is to compute S_i when A finds an invalid payment. H_1 consists of the hashed value of C and the nodes corresponding to the payment. Here, the hashed value of C is the searching key in the database, and H_1 can be very short (e.g, 10 bytes). On the other hand, H_2 is almost same as H, and is pointed from H_1. Therefore, H_1 can be stored in a database which is easy of access, while H_2 can be stored in a device such as a magnetic tape and a laser disk, which is not easy of access but has big capacity. H_1 and H_2 (especially H_2) can be stored in a distributed manner.

3.2 Correctness

Here, we show briefly that Protocol 1 satisfies the five criteria of (a)*Independence*, (b)*Security*, (c)*Privacy*, (d)*Off-line payment*, and (f)*Divisibility*. Among them, criteria (a) and (d) are clearly satisfied. Therefore, we show that the other three criteria are satisfied.

- *Privacy:* First, if the customer accurately follows the protocol, even the coalition of bank A and store V cannot get any knowledge about the identity of P with non-negligible probability, assuming that factoring is difficult for A and V.

- *Dividability:* As shown in Subsection 2.2, if three restrictions on the usage of the hierarchical structure table are satisfied, then the dividability condition is satisfied. (In the next item (security), we will show that the second and third restrictions are securely realized. The first restriction can be clearly realized as a protocol.) Then, when R is the ratio of the value of an electronic bill, C, (e.g, \$1000) to the minimum unit of payment (e.g., 1 cent), then the processing and communication amounts for payment are in proportion to $\log_2 R$.

- *Security:* First, we show that the third restriction of the hierarchical structure table (Subsection 2.2) is securely realized. If customer P uses any part of C (any node of the hierarchical structure table of C) more than once, bank A can obtain the identity of P with overwhelming probability, since the Williams integer N can be factored in polynomial-time from $[x^{1/2} \bmod N]_1$ and $[x^{1/2} \bmod N]_{-1}$, and since V challenges P randomly using Λ table, along with the cut-and-choose methodology. Next, we show that the second restriction of the hierarchical structure table (Subsection 2.2) is securely realized. Here, for easily understanding, we use the simple example, where the value of C is \$100, and P pays \$75 to V (Figure 1, 2, and 3). Note that the cut-and-choose methodology is also implicitly crucial in assuring correctness, although we omit a detailed explanation here (roughly, thanks to this methodology, we can assume that I_i, N_i are correctly generated).
  First, we show that the first restriction is satisfied: that is, when nodes Γ_{00}, Γ_{010} are used, then all descendant and ancestor nodes of these nodes, Γ_0, Γ_{000}, Γ_{001}, and Γ_{01}, cannot be used. When Γ_{00} is used, P sends $X_{i,00} = [\Gamma_{i,00}^{1/2} \bmod N_i]_{-1}$ $(i = 1, \ldots, K/2)$ to V (finally to A). Then, if P uses Γ_{000}, P sends $X_{i,000} = [\Gamma_{i,000}^{1/2} \bmod N_i]_{-1}$ $(i = 1, \ldots, K/2)$. Since $[\Gamma_{i,00}^{1/2} \bmod N_i]_1 = X_{i,000}^2 \bmod N_i$, A can factor N_i from $X_{i,00}$ and $X_{i,000}^2 \bmod N_i$ (then, the identity of P is revealed). Similarly, if Γ_0 or Γ_{001} is used with Γ_{00}, or if Γ_0 or Γ_{01} is used with Γ_{010}, then the identity of P is revealed. Therefore, when Γ_{00}, Γ_{010} are used, then Γ_0, Γ_{000}, Γ_{001}, and Γ_{01}, cannot be used, with concealing the identity of P.
  Finally, we show the necessity of Ω, using a simple example. Assume that $\Omega_{i,j_1\cdots j_t}$ is a constant value, e.g., 3. Then, in Figure 3, $\Gamma_{01} = 3(\Gamma_0)^{1/2}$, where we omitt the suffix of i and $\bmod N_i$, for simplicity. So, when a customer uses the nodes of Γ_{00} and Γ_{01}, he opens the values of $X_{00} = (\Gamma_0)^{1/4}$ and $X_{01} = (3(\Gamma_0)^{1/2})^{1/2} = 3^{1/2}(\Gamma_0)^{1/4}$, where the jacobi symbol values of X_{00} and X_{01} are -1. Then, the shop can obtain $3^{1/2}$ by calculating X_{01}/X_{00}, where the jacobi symbol of this value is 1. The same situation occurs when the customer uses the nodes of Γ_{000} and Γ_{001}, and so on. Therefore, suppose that a customer uses Γ_{000}, Γ_{001}, Γ_{010}, and Γ_{0110}, whose usage is valid. (So, he opens X_{000}, X_{001}, X_{010}, and X_{0110}.) Then, the shop can calculate $A = 3^{1/2}$ by X_{001}/X_{000}, and also calculate the value of X_{011} by AX_{010}. Therefore, the shop can factor N by using the values of X_{011} and $(X_{0110})^2$, where the jacobi symbol of X_{011} is -1 and that of $(X_{0110})^2$ is 1. Thus, the shop can know the customer's ID, although the customer uses the nodes validly.

4 Transferable Universal Electronic Cash

In this section, we propose an electronic cash scheme satisfying the criterion of (e) *Transferability* in addition to the other five criteria.

Protocol 2. (Transferable universal electronic cash)

This protocol is constructed based on Protocol 1. To simplify the description of this protocol, we suppose an example similar to that in Section 3, where C is worth \$100, customer P_1 who has spent \$75 transfers the remaining \$25 to customer P_2, and P_2 uses \$25 at shop V.

Part I.
When customers P_1 and P_2 open their accounts at bank A, A issues electronic licenses $B^{(j)}$ to a customer P_j ($j = 1, 2$). Hereafter, in this protocol, $x^{(j)}$ means x of P_j, where variable x follows the definition in Protocol 1.

Part II.
Suppose that customer P_1 has bank A issue an electronic bill worth \$100, C.

Part III.
To transfer C to another customer P_2, P_1 and P_2 proceeds as follows:
(Step 1) P_2 takes the role of V in Protocol 1 as P_1 pays shop P_2 \$25 (corresponding to node Γ_{011}) (Part III of Protocol 1).
(Step 2) P_1 sends certification T that denotes the transfer of C from P_1 to P_2. For example, P_1 sends a (Rabin scheme) digital signature $T = (< g(C \parallel 011 \parallel B^{(2)} >_{QR})^{1/2} \bmod N_1^{(1)}$.

Part IV.
To pay shop V \$25, P_2 and V proceed as follows:
(Step 1) P_2 sends the history of Part III of this protocol, $H^{(1)}$, to V. V checks the validity of $H^{(1)}$.
(Step 2) P_2 follows Part III of Protocol 1 with shop V to pay C. Here, P_2 sends V messages corresponding to nodes $\Gamma_{011}^{(2)}$ and $\Lambda_{011}^{(2)}$.

Part V.
To have bank A credit V's account by \$25, V sends the history of Part IV of this protocol, $H^{(2)}$, to A, which credits V's account. Bank A must store $H^{(2)}$ in its database.
(End of Protocol 2)

5 Performance Estimation

We will briefly explain an example of the new cash system implementation. Here we assume that $K = 40$, $|N_i|$ is 64 bytes, and the hierarchical structure table has 17 levels. We also assume that a bank issues a piece of cash worth \$1000 to customer Alice. Alice can disburse her cash in any way she pleases until the total expended equals \$1000. Then, she uses just 64 bytes of data for the electronic bill (C) worth \$1000 and her proper data (electronic license, B) is about several kilobytes. Thus the total amount of data is small enough to be stored on typical smart cards. When she buys several articles (e.g., the total payment for them is \$334.36) at a store, her card transmits only 20 kilobytes on average. The computation time for generating the data representing the payment (e.g., \$334.36) that will be sent to the store is about several seconds, assuming the existence of a Rabin scheme chip of 30 Kbps (kilo-bit per second). If the value of the payment is known in advance, the computation for the payment can be executed in advance.

6 Conclusion

In this paper, we have proposed the first ideal untraceable electronic cash system, The customer can subdivide his cash balance, C (dollars), into many pieces in any way he pleases until the total value of all subdivided piece equals C. A smart card equipped with a Rabin scheme chip and the distributed database system for a bank to store H_1 and H_2 should be implemented efficiently to realize the universal electronic cash system. From a theoretical viewpoint, it remains open to construct an unconditionally untraceable universal electronic cash system.

Acknowledgments

Authors wish to thank A. Herzberg, S. Kurihara, K. Sakurai and A. Shamir for their useful discussions.

References

[Ber] E.R.Berlekamp, "Factoring Polynomials over Large Finite Fields," Math. Comp., Vol.24, No.111, pp.713-735 (1970)

[Bl] M.Blum, "Coin flipping by telephone", IEEE, COMPCON, pp.133-137 (1982)

[Ch] D.Chaum, "Security without Identification: Transaction Systems to Make Big Brother Obsolete," Comm. of the ACM, 28, 10, pp.1030-1044 (1985)

[CFN] D.Chaum, A.Fiat and M. Naor, "Untraceable Electronic Cash," Proc. of Crypto'88, pp.319-327 (1988)

[CW] J.L.Carter and M.N.Wegman, "Universal Classes of Hash Functions," Journal of Computer and System Sciences, 18, pp.143-154 (1979)

[Da] I.B.Damgård, "Payment Systems and Credential Mechanisms with Provable Security Against Abuse by Individuals," Proc. of Crypto'88, pp.328-335 (1988)

[EGL] S.Even, O.Goldreich, A.Lempel: "A Randomized Protocol for Signing Contracts", Proc. of Crypto'82, pp.205-210 (1982)

[EGY] S.Even, O.Goldreich, Y.Yacobi: "Electronic Wallet", Proc. of Crypto'83, pp.383-386 (1983)

[FOM] A.Fujioka, T.Okamoto, S.Miyaguchi: "ESIGN: An Efficient Digital Signature Implementation for Smart Cards", to appear in Proc. of Eurocrypt'91

[H] B.Hayes, "Anonymous One-Time Signatures and Flexible Untraceable Electronic Cash," Proc. of Auscrypt'90, pp.294-305 (1990)

[OkOh1] T.Okamoto, and K.Ohta "Disposable Zero-Knowledge Authentications and Their Applications to Untraceable Electronic Cash," Proc. of Crypto'89, pp.481-496 (1989)

[OkOh2] T.Okamoto, and K.Ohta "Divertible Zero-Knowledge Interactive Proofs and Commutative Random Self-Reducible," Proc. of Eurocrypt'89 (1989)

[PW] B.Pfitzmann, M.Waidner, "How to Break and Repair a "Provably Secure" Untraceable Payment System," to appear in Proc. of Crypto'91

[R] M.O.Rabin, "Digitalized Signatures and Public-Key Functions as Intractable as Factorization," Tech. Rep., MIT/LCS/TR-212, MIT Lab. Comp. Sci., (1979)

[W] H.C.Williams, "A Modification of the RSA Public-Key Encryption Procedure," IEEE Trans. on Information Theory, Vol.IT-26, No.6, pp.726-729 (1980)