Disposable Zero-Knowledge Authentications and Their Applications to Untraceable Electronic Cash

Tatsuaki Okamoto *Kazuo Ohta*

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

Abstract

In this paper, we propose a new type of authentication system, *disposable zero-knowledge authentication system*. Informally speaking, in this authentication system, double usage of the same authentication is prevented. Based on these disposable zero-knowledge authentication systems, we propose a new *untraceable electronic cash* scheme satisfying both *untraceability* and *unreusablity*. This scheme overcomes the problems of the previous scheme proposed by Chaum, Fiat and Naor through its greater efficiency and provable security under reasonable cryptographic assumptions. We also propose a scheme, *transferable untraceable electronic cash* scheme, satisfying *transferability* as well as the above two criteria, whose properties have not been previously proposed in any other scheme. Moreover, we also propose a new type of electronic cash, *untraceable electronic coupon ticket*, in which the value of one piece of the electronic cash can be subdivided into many pieces.

1. Introduction

"Zero-knowledge proofs" are useful for many application areas [B, BC, BCC, Cr, GMR, etc.]. A typical application area is authentication systems such as identifications and digital signatures [FFS, FS, GQ, MS, OhO]. For zero-knowledge proofs, coin flips of the prover are essential for zero-knowledgeness of the proof, while coin flips of the verifier are essential for the ability of the proof. Therefore, if the coin flips of the prover are restricted, the usage of the proof must be restricted under the zero-knowledge condition.

In this paper, by using this property of zero-knowledge proofs, we propose a new type of zero-knowledge authentication, *disposable zero-knowledge authentication*. Informally speaking, in this authentication double usage of the same authentication is prevented. This type of zero-knowledge authentication is considered to have many applications such as electronic cash, checks, and tickets, because in these applications a piece of information has value itself, and multiple invalid usage of this piece of information must be prevented.

To endow electronic cash with properties similar to those of real cash, electronic cash should satisfy the following conditions:

(1) *Untraceability*: The privacy of the user should be protected. That is, the relationship between the user and his purchases should be untraceable by anyone. Ideally, any partial information about the user's purchases should be untraceable by anyone (we call this property *perfect* untraceability).

G. Brassard (Ed.): Advances in Cryptology - CRYPTO '89, LNCS 435, pp. 481-496, 1990.

(2) *Unreusability*: The ability to use the electronic cash more than once should be prevented.
(3) *Transferability*: The electronic cash can be transfered to other users.

Criterion (1) can be satisfied by using blind signatures [Ch, D, OkO]. To satisfy criteria (1) and (2), Chaum, Fiat and Naor [CFN] have developed an elegant electronic cash scheme (*untraceable electronic cash*) based on the cut-and-choose methodology and collision free functions. However, their scheme has two major problems from the viewpoint of efficiency and formal provability of security:

- (Efficiency) In their scheme, a customer must undergo a complex procedure including the cut-and-choose methodology to obtain each electronic coin.
- (Provability of security) The assumptions under which the scheme is provably secure are not clear.

Although the scheme [CFN] satisfies the first two criteria, so far no scheme has been proposed that satisfies all three criteria: (1) untraceability, (2) unreusability, and (3) *transferability*.

In this paper, we propose a new untraceable electronic cash scheme that satisfies the criteria (1) and (2) based on disposable zero-knowledge authentications as well as the cut-and-choose methodology. This scheme overcomes the problems of the previous scheme [CFN] in the following ways:

- (Efficiency) In our scheme, a customer undergoes a complex procedure including the cut-and-choose methodology *only once* when he opens his account at a bank. After that, only a minimal procedure is required to obtain each electronic coin. In this case, however, our scheme does not satisfy *perfect* untraceability, although it satisfies untraceability. That is, the relationship between a user and his purchases cannot be traced by anyone, but a purchase history of an anonymous user can be traced.
  Note that, in our scheme, we can choose the degree of efficiency and the degree of untraceability, and they have a trade-off. If we choose the degree of untraceability as maximal (or perfect untraceability), the degree of efficiency is minimal (or comparable to that of the previous scheme [CFN]).
- (Provability of security) Our scheme is proven to be secure under the following assumptions:
  (i) (*Digital signature assumption*) There exists a secure digital signature scheme [GoMiRi] and secure multiple blind digital signature scheme. (If a secure multiple blind digital signature scheme exists, a secure digital signature scheme exits.)
  (ii) (*RSA assumption*) The RSA scheme is secure, and to break the RSA scheme in which the plaintext's redundancy is 0 is as hard to break as the RSA scheme in which the plaintext's redundancy is less than 1/2. (If the latter condition holds, the former condition holds.)

In this paper, we show a typical case where we construct our scheme based on the extended Fiat-Shamir scheme [GQ, OhO]. Note, however, that our scheme can be constructed based on other disposable zero-knowledge authentications with a unique solution S for I such that $(I, S) \in R$ (e.g., discrete logarithm problem).

In this case, the second assumption for the scheme's security is replaced by the following one (The first assumption is the same as above) :

(ii) (*Invulnerable relation assumption*) A relation R is *invulnerable* (it is hard to compute S from I, where $(I, S) \in R$). And, to compute S from I in which S's redundancy is 0 is as hard to compute as S from I in which S's redundancy is less than $1/2$.

Next, we propose a new electronic cash scheme, *transferable untraceable electronic cash* scheme that, to our knowledge, has never been proposed, that satisfies criteria (1), (2) and (3). This scheme is constructed based on the above untraceable electronic cash scheme.

Moreover, we also propose another type of electronic cash (*untraceable electronic coupon ticket*) with the following property: The value of one piece of electronic cash can be subdivided into many pieces. For example, a user with a piece of electronic cash worth \$100 could subdivide it into 100 pieces of cash worth \$1. If we add the notion of transferability (criterion (3)), *transferable* untraceable electronic coupon ticket could be constructed in a way similar to the transferable untraceable electronic cash.

2. Notations

(P, V) is an interactive pair of Turing machines, where P is the prover, and V is the verifier [GMR, TM]. Let $T \in \{P, V\}$. $T(s)$ denotes T begun with s on its input work tape. $(P, V)(I)$ refers to the probability space that assigns to the string σ the probability that (P, V), on input I, outputs σ.

$(P(s),\underline{V(t)})(I)$, V's history, denotes (I, t, ρ', m'), where ρ' is the finite prefix of V's random tape that was read, and m' is the final content of the communication channel tape on which P writes. P^A means P with oracle A, where P^A's oracle tapes correspond to P's communucation channel tapes with A. $R \subseteq X \times Y$ is a relation, where X and Y are sets of finite strings. $\|$ denotes concatenation.

3. Disposable Zero Knowledge Authentication

There are two types of interactive proofs. One is the interactive proof *for membership in language L*, in which a membership of an instance in language L is demonstrated [GMR]. The other is the interactive proof *for possession of knowledge*, in which a prover's possession of information is demonstrated [FFS, TW]. In the latter proof, the prover's power is bounded in polynomial time, while, in the former proof, its power is not bounded.

In this section, first, we show the *revealability* of the zero-knowledge interactive proofs for possession of knowledge. Then, we define the *disposable zero-knowledge authentication* and show an implementation of this authentication.

Definition 1. Let R be a relation, and (P, V) be a zero-knowledge interactive proof for possession of some S satisfying $(I, S) \in R$. We say that (P, V) is *k-revealable* if there exists a polynomial-time probabilistic Turing machine M_V (with complete control over V) that computes S' such that $(I, S') \in R$ after k executions

of the proof fixing the coin flips ρ of P with overwhelming probability, where ρ corresponds to one execution of the proof. (When $k = O(|I|^c)$ and c is a constant, k-revealable is called *poly-revealable*.)

Lemma 1. Every zero-knowledge interactive proof for possession of knowledge is poly-revealable.

Proof Sketch: From the definition of the soundness of the zero-knowledge interactive proof for possession of knowledge [FFS], the existence of M_V can be shown. **QED**

Lemma 2. If there exist secure encryption schemes, any NP relation has a 2-revealable zero-knowledge interactive proof for possession of knowledge.

Proof Sketch: Under the assumption that NP reductions are one-to-one and efficiently invertible, it suffices to prove that Blum's zero-knowledge interactive proof for possession of knowledge of the graph Hamiltonicity ([FFS]'s Theorem 1.) is 2-revealable. The iterated number of rounds of this proof is $|I|$ (one round means steps 1-7 of [FFS]'s Theorem 1.). Suppose that Blum's proof (P, V) is executed twice fixing the coin flips ρ of P. Let ρ'_i $(i = 1, 2)$ be the verifier's coin flip in the i-th execution of the proof, where $|\rho'_i| = |I|$. If $\rho'_1 \neq \rho'_2$, a Hamiltonian cycle S can be computed in polynomial-time from the history of the two executions of this proof. The probablity that $\rho'_1 \neq \rho'_2$ is $1 - 1/2^{|I|}$. **QED**

Definition 2. Let A be the authority, P_i be a prover with a secret knowledge S such that $(I, S) \in R$, and V_i be a verifier with public knowledge I and R. Each party follows the below authentication procedure:
(Step 1) Prover P_i sends a message X to authority A.
(Step 2) A generates a digital signature C of X and sends it to P_i. (C, X) means A's permission to P_i's authentication. One permission corresponds to one execution of the prover's authentication procedure.
(Step 3) P_i shows A's permission (C, X) and proves his possession of S to a verifier V_i. V_i accepts P_i to be valid if he verifies the validity of both (C, X) and his proof of possession of S.
Let $\overline{P}_i$ and $\overline{V}_i$ be valid prover and verifier that follow their designated protocols, respectively. Let $\widetilde{P}_i$ and $\widetilde{V}_i$ be invalid polynomial-time prover and verifier that can deviate from their correct protocols in arbitrary ways, respectively. Let P_i be either $\overline{P}_i$ or $\widetilde{P}_i$, and V_i be either $\overline{V}_i$ or $\widetilde{V}_i$.
Let $(A, \{P_i, V_i\})$ $(i = 1, 2, \ldots)$ be an *authentication system*, if the following two conditions are satisfied.

- *Completeness*: $\overline{P}_i(S)$'s authentication is accepted to be valid by $\overline{V}_i$ with overwhelming probability.
- *Soundness*: There exists a polynomial-time probabilistic Turing machine M_{P_i} (with complete control over P_i) such that if P_i's authentication is accepted to be valid by $\overline{V}_i$ with non-negligible probability, then M_{P_i} breaks cryptographic assumptions on A's digital signatures with overwhelming probability and the output produced by M_{P_i} on input I satisfies the relation R with overwhelming probability.

Note: Informally, soundness means that invalid prover $\widetilde{P}_i$ is accepted by $\overline{V}_i$ with negligible probability.

Definition 3. Authentication system $(A, \{P_i, V_i\})$ is *disposable zero-knowledge* if the following conditions are satisfied.

- *Zero-knowledgeness*: For any V_i, I, and t, there exists a polynomial-time probabilistic Turing machine $M^A_{V_i}$ such that $((C,X),(\overline{P}_i(S),\underline{V_i(t)})(I))$ and $M^A_{V_i}(I,t)$ are polynomially indistinguishable.
- *Disposability*: There exists a polynomial-time probabilistic Turing machine $M_{\overline{V}_i,\overline{V}_j}$ (with complete control over $\overline{V}_i$ and $\overline{V}_j$) such that if $\overline{P}_i$'s authentication is executed successfully twice with the same (C,X) to $\overline{V}_i$ and $\overline{V}_j$ respectively, then the output produced by $M_{\overline{V}_i,\overline{V}_j}$ on input I satisfies the relation R with overwhelming probability.

Note: Informally, zero-knowledgeness means that when valid prover $\overline{P}_i$'s authentication is executed once with the same (C,X), then any knowledge about secret information S cannot be revealed by anyone. Disposability means that valid prover $\overline{P}_i$'s authentication is executed twice with the same (C,X), then secret information S can be revealed by the coalition of the authority and valid verifiers.

Theorem 1. If there exist secure encryption schemes [GM] and secure digital signature schemes [GoMiRi], then a disposable zero-knowledge authentication system can be constructed using any NP relation.

Proof Sketch: Under the assumption that NP reductions are one-to-one and efficiently invertible, it suffices to prove that a disposable zero-knowledge authentication system can be constructed using Blum's zero-knowledge interactive proof for graph Hamiltonicity.

Construction:

The public input I is a graph, and S such that $(I,S) \in R$ is a Hamiltonian cycle in I. H is a probabilistic encryption [GM, Y].

(Step 1) P_i randomly permutes the vertices of graph I (using permutation π_k, $k = 1,2,\ldots,|I|$) to obtain

- Graph $\widehat{I}_k$,
- An $|I| \times |I|$ matrix $\alpha_k = \{\alpha_{kst} \mid s,t = 1,2,\ldots,|I|\}$, where $\alpha_{kst}=H(v_{kst})$, and $v_{kst} = 1$ if edge st is present in the $\widehat{I}_k$, and 0 otherwise, and
- $\beta_k = H(\pi_k)$.

P_i sends $X = (\alpha_1,\ldots,\alpha_{|I|},\beta_1,\ldots,\beta_{|I|})$ to authority A.

(Step 2) A generates a digital signature $\{C_k\}$ of $\{(\alpha_k,\beta_k)\}$ $(k = 1,2,\ldots,|I|)$ and sends them to P_i.

(Step 3-1) $k \leftarrow 1$.

(Step 3-2) P_i sends (α_k,β_k) and C_k to V_i.

(Step 3-3) V_i verifies the validity of the digital signature of C_k. If it is invalid, V_i rejects. Otherwise, V_i chooses at random $\rho'_k \in \{0,1\}$, and sends ρ'_k to P_i.

(Step 3-4) If $\rho'_k = 1$, P_i sets δ_k =(decryptions of α_{kst} and β_k). Otherwise, $\delta_k = \{$decryption of $\alpha_{kst} \mid$ edge st is in a Hamiltonian path in $\widehat{I}_k\}$. P_i sends δ_k to V_i.

(Step 3-5) If P_i is unable to perform steps 3-4 correctly, V_i rejects. Otherwise, $k \leftarrow k+1$ and go to step 3-2, if $k < |I|$. If $k = |I|$, V_i accepts.

Completeness: A valid prover can be accepted by a verifier with probability 1.

Soundness: If P_i's authentication is accepted to be valid by $\overline{V}_i$ with non-negligible probability, then P_i can generate A's digital signature for non-negligible fraction of the message space. Therefore, from the assumption of the existence of secure digital signature, there exists a polynomial-time probabilistic Turing machine M_{P_i} (with complete control over P_i) such that M_{P_i} breaks cryptographic assumptions of A's digital signature with overwhelming probability. On the other hand, if P_i's authentication is accepted to be valid by $\overline{V}_i$ with non-negligible probability, then, from the soundness of Blum's protocol, M_{P_i} on input I outputs S' such that $(I, S') \in R$ with overwhelming probability.

Zero-knowledgeness: In a manner similar to the proof of the zero-knowledgeness of Blum's protocol, it can be proven that $((C, X), (P_i(S), \underline{V_i(t)})(I))$ and $M^A_{V_i}(I, t)$ are polynomially indistinguishable.

Disposability: From Lemma 2., we can show that there exists a polynomial-time probabilistic Turing machine M_{V_i} that produces S' satisfying $(I, S') \in R$ with overwhelming probability. **QED**

An application to traceable electronic cash: Here, we show a straightforward application example of the disposable zero-knowledge authentication to traceable electronic cash sytems. Let authority A be a bank, prover P_i be a customer, and verifier V_i be a shop. The authority's permission (C, X) corresponds to an electronic coin worth \$100 that the bank issues to the customer when he withdraws \$100 from his account. When P_i purchases an article for \$100 from shop V_i, he makes the disposable zero-knowledge authentication regarding (C, X) to the shop. The shop sends the history of this authentication with (C, X) to the bank to obtain \$100 from the bank. If the customer uses (C, X) more than once, the bank will reveal S' satisfying $(I, S') \in R$, and withdraw more than the \$100 from his account to penalize the customer. Otherwise, S' is never revealed by anyone. Here, S' witnesses the customer's abuse of the electronic cash, and we assume that the bank and the customer have signed a contract such that the customer must pay a penalty to the bank when the bank reveals S' satisfying $(I, S') \in R$. In other words, we can consider this situation as a game between the bank and the customer. In this game, the customer loses and pay some money to the bank when the bank reveals S' satisfying $(I, S') \in R$, where I is determined by the customer.

Discussion: The above-mentioned example is an application to a *traceable* electronic cash system, in which the customer's purchase history is traceable. Although the above-mentioned example is very simple and efficient, we can easily construct other implementations with almost the same functions by using digital signatures of the customer without using disposable zero-knowledge authentication.

In contrast to this application, a number of distinct advantages can be realized by

applying disposable zero-knowledge authentication to *untraceable* electronic cash and tickets systems. We will describe these applications in some detail in sections 4, 5 and 6.

4. Untraceable Electronic Cash

In this section, we show an untraceable electronic cash scheme satisfying two criteria, *Untraceability* and *Unreusability*, based on disposable zero-knowledge authentications. This scheme has advantages over the previously proposed scheme [CFN] in the standpoints of efficiency and provability of its security, as described in Section 1. This scheme can be constructed based on some disposable zero-knowledge authentications with a unique solution S for I such that $(I, S) \in R$. In this section, however, we show a typical case based on the extended Fiat-Shamir scheme [GQ, OhO].

Before describing the untraceable electronic cash protocol, we will introduce a specific type of blind digital signature, *multiple* blind digital signature.

Definition 4. Let A, P, and e_A be a signer, requester, and the signer's public key, respectively. Let F be an algorithm for P, D be an algorithm for A, and $G_{e_A}(m_1, \ldots, m_k)$ be A's multiple digital signature of k messages, $m_1, \ldots, m_k$. Let (A, P, F, D, G) be a *multiple blind digital signature* system, if A and P follow the below procedure:

(Step 1) P generates k blind messages $\{F_{e_A}(m_i) \mid i = 1, 2, \ldots, k\}$ from k messages $\{m_i \mid i = 1, 2, \ldots, k\}$, and sends them to A. Here, each $F_{e_A}(m_i)$ is independently blinded.

(Step 2) A generates the multiple blind digital signature $D_{e_A}(F_{e_A}(m_1), \ldots, F_{e_A}(m_k))$ from the k blind messages, $F_{e_A}(m_1), \ldots, F_{e_A}(m_k)$, and sends it to P.

(Step 3) P extracts A's multiple digital signature $G_{e_A}(m_1, \ldots, m_k)$ of $m_1, \ldots, m_k$.

(A, P, F, D, G) is a *secure* multiple blind digital signature system, if (A, P, F, D, G) satisfies the criteria for blind digital signature [Ch, OkO] and P can generate $G_{e_A}(m_1, \ldots, m_k)$ from $D_{e_A}(m_1^{(1)}, \ldots, m_t^{(1)}), \ldots, D_{e_A}(m_1^{(l)}, \ldots, m_t^{(l)})$ with negligible probability, where k, t, l are positive integers, and for any subset $\{i_1, \ldots, i_j\} \subset \{1, \ldots, l\}$, $\{m_1, \ldots, m_k\} \neq \{m_1^{(i_1)}, \ldots, m_t^{(i_1)}, \ldots, m_1^{(i_j)}, \ldots, m_t^{(i_j)}\}$, and every m_i's and $m_i^{(j)}$'s are in a randomly determined negligible fraction $\mathcal{M}$ of the message space (e.g., $\mathcal{M} = \{m \mid |m|/c$-prefix of m is a (randomly) fixed sequence, where c is a constant $\}$).

Note: The secure multiple blind digital signature schemes seem to be implemented based on the previously proposed blind digital signature schemes [Ch, OkO]. Note that the multiple blind digital signature scheme contains the previous (single) blind digital signature scheme as a special case where $k = 1$. In the electronic cash scheme [CNF], the multiple blind digital signature scheme based on [Ch] has been used. We can also construct a multiple blind digital signature scheme based on a divertible zero-knowledge proof for *endomorphic* CRSR relation [OkO]. Here, note that, in this scheme based on [OkO], A must send a pre-message to P. However, for simplicity in this paper, we omit this pre-message sending phase

when describing the multiple blind digital signature.

Protocol 1. (Untraceable electronic cash) Bank A has a secure multiple blind digital signature generation algorithm D. A has published his public keys, e_A, e'_A, of this blind digital signature scheme, where e_A corresponds to the *electronic license* that A issues, and e'_A corresponds to the value of the *electronic coin* that A issues. The bank A also sets the security parameter $K = O(|n|)$. Customer P has a bank account number ID_P and a secure digital signature generation algorithm G, and publishes his public-key e_P of the digital signature scheme.

Part I.

When a customer P opens an account at bank A, A issues an electronic license B to use electronic cash of bank A. (Precisely, an electronic license is $(B, \{I_i, N_i, L_i\})$. For simplicity, however, we call B an electronic license.) To get B, P conducts the following protocol with A. This procedure is executed *only once* when P opens the account, unless P reuses the electronic cash invalidly.

(Step 1) Customer P chooses random values a_i, and composite numbers N_i with two large prime factors P_i, Q_i $(N_i = P_i \cdot Q_i)$, for $i = 1, \ldots, K$. P also fixes prime integer L_i such that $\gcd(L_i, \phi(N_i)) = 1$, where $\phi(N_i) = \mathrm{lcm}(P_i - 1, Q_i - 1)$. For simplicity, we assume that all $|N_i| = O(|e_A|)(i = 1, \ldots, K)$ are equivalent, and that $L_i = O(1)$.

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

$$W_i = F_{e_A}(I_i \parallel N_i \parallel L_i) \quad \text{for } 1 \le i \le K,$$

where

$$I_i = S_i^{L_i} \bmod N_i,$$

$$S_i = ID_P \parallel a_i \parallel G_{e_P}(ID_P \parallel a_i).$$

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

(Step 4) P displays the $a_i, P_i, Q_i, L_i, G_{e_P}(ID_P \parallel a_i)$, ID_P for all i in U, and random values that make messages W_i blinded, 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

$$D_{e_A}(W_1, \ldots, W_{K/2}).$$

(Step 6) P can then extract the electronic license B.

$$B = G_{e_A}(I_1 \parallel N_1 \parallel L_1, \quad \ldots \quad , I_{K/2} \parallel N_{K/2} \parallel L_{K/2}).$$

Notes:

(1) Every L_i's for every customers can be replaced by a unique prime integer L determined by the system (or a bank). Note that in this case P must select N_i such that $\gcd(L, \phi(N_i)) = 1$.

(2) For example, when we use the RSA multiple blind digital signature scheme [Ch, CFN], $B = \prod_{1 \le i \le K/2} g(I_i \parallel N_i \parallel L_i)^{1/e} \bmod n$, where (e, n) is A's RSA public key, and g is an appropriate one-way hash function.

Part II.

When customer P wants bank A to issue an electronic coin worth one dollar C which corresponds to e'_A, P conducts the following protocol with A (Precisely, an electronic coin is $(C, \{X_i\})$. For simplicity, however, we call C an electronic coin.):
(Step 1) P chooses random values R_i $(i = 1, \ldots, K/2)$, and forms and sends Z to A.

$$Z = F_{e'_A}(X_1 \parallel \ldots \parallel X_{K/2} \parallel B),$$

$$X_i = R_i^{L_i} \bmod N_i \quad \text{for } 1 \le i \le K/2.$$

(Step 2) A gives $D_{e'_A}(Z)$ to P and charges P's account one dollar.
(Step 3) P can then extract the electronic coin $C = G_{e'_A}(X_1 \parallel \ldots \parallel X_{K/2} \parallel B)$.

Note: We can reduce the amount of information that P posseses as follows:
In place of possessing $K/2$ pieces of information, $\{X_i \mid 1 \le i \le K/2\}$, P possesses only one piece of infromation X. In Part II, P obtains $C = G_{e'_A}(X \parallel B)$. In Part III, we regard X as X_i for all $1 \le i \le K/2$, and P computes $R_i = X^{1/L_i} \bmod N_i$ for $1 \le i \le K/2$.

Part III.

To pay a shop V one dollar, P and V proceed as follows:
For each $i = 1, 2, \ldots, K/2$, steps 1-4 are executed iteratedly.

(Step 1) P sends I_i, N_i, L_i, X_i to V. When $i = K/2$, P also sends B and C to V.
(Step 2) V selects a random value $E_i \in Z_{L_i}$, and sends it to P. When $i = K/2$, V verifies the validity of the signatures B for $\{(I_i, N_i, L_i)\}$, and C for $(X_1, \ldots, X_{K/2}, B)$. If B and C are valid, V selects a random value $E_{K/2} \in Z_{L_{K/2}}$, and sends it to P. Otherwise V halts this protocol.
(Step 3) P computes $Y_i = R_i \cdot S_i^{E_i} \bmod N_i$ and sends it to V.
(Step 4) V verifies that $Y_i^{L_i} \equiv X_i \cdot I_i^{E_i} \pmod{N_i}$.

If P passes this protocol successfully for all $i = 1, 2, \ldots, K/2$, then V accepts the electronic coin C as one dollar.

Notes:

(1) This protocol can be modified in a manner similar to the parallel version of the extended Fiat-Shamir scheme.
(2) To prevent bank A from crediting an invalid shop's account in Part IV, in steps 2 and 3, we can enhance the protocol as follows:
In step 2, V selects a random value d_i, and sends V's identity ID_V, time T, and d_i to P in place of sending E_i. V computes $E_i = f(ID_V \parallel T \parallel d_i)$, where f is a one-way function whose output is uniformly random. In step 3, P also computes E_i.

Part IV.
For bank A to credit V's account by one dollar, V sends the history of Part III of this protocol, H, to A, which credits V's account after verifying whether H is a correct history of Part III and whether H has not been stored already in A's database. If H is valid, bank A must store H in its database.

(End of Protocol 1)

In the rest of this paper, we adopt the following notations:
(1) $\overline{C}$ represents valid cash which is correctly issued by valid bank A through its designated protocol. $\overline{P}$ represents a valid customer with $\overline{C}$.
(2) $\widetilde{C}$ represents invalid cash generated through an arbitrary polynomial-time algorithm of an invalid customer $\widetilde{P}$.
(3) C represents either $\overline{C}$ or $\widetilde{C}$. P represents either $\overline{P}$ or $\widetilde{P}$.
(4) $\overline{H}$ represents the valid history of the protocol between a valid customer $\overline{P}$ and a valid shop $\overline{V}$.
(5) $\widetilde{H}$ represents an invalid history generated through an arbitrary polynomial-time algorithm of an invalid shop $\widetilde{V}$.
(6) H represents either $\overline{H}$ or $\widetilde{H}$. V represents either $\overline{V}$ or $\widetilde{V}$.

Definition 5. The untraceable electronic cash system (Protocol 1) is *secure* if the following conditions are satisfied:

- *Completeness*: Any valid cash $\overline{C}$ is accepted as valid by any shop $\overline{V}$ through part III of Protocol 1. Any valid history $\overline{H}$ is accepted as valid by bank $\overline{A}$.
- *Soundness*: Any invalid cash $\widetilde{C}$ is accepted by any shop $\overline{V}$ through part III of Protocol 1 with negligible probability. Any invalid history $\widetilde{H}$ is accepted by bank $\overline{A}$ with negligible probability.
- *Untraceability*: For any V, I_i, N_i, L_i, and t, there exists a polynomial-time probabilistic Turing machine M_V such that $(C, \{X_i\}, B)$, $(\overline{P}(\{S_i\}), \underline{V(t)})(\{I_i, N_i, L_i\}))$ and $M_V^A(\{I_i, N_i, L_i\}, t)$ are polynomially indistinguishable.
- *Unreusability*: There exists a polynomial-time probabilistic Turing machine $M_{\overline{V}_1,\overline{V}_2}$ (with complete control over $\overline{V}_1$ and $\overline{V}_2$) such that if $\overline{P}$'s coin $\overline{C}$ is used twice through part III of Protocol 1 to $\overline{V}_1$ and $\overline{V}_2$ respectively, then $M_{\overline{V}_1,\overline{V}_2}$, on input these histories $\overline{H}_1$ and $\overline{H}_2$, outputs at least one piece of information $S_i = ID_P \parallel a_i \parallel G_{e_P}(ID_P \parallel a_i)$ $(i \in \{1, \ldots, K/s\})$ with overwhelming probability.

Note: Informally, untraceability means that when a valid coin $\overline{C}$ is used only once, the identity of the customer who uses $\overline{C}$ cannot be revealed by anyone. Unreusability means that when a valid coin $\overline{C}$ is used twice, bank A can obtain the identity of the customer who uses $\overline{C}$ with overwhelming probability.

Theorem 2. Protocol 1 is secure if the following two assumptions are satisfied:
(*Digital signature assumption*) There exist a secure digital signature scheme [GoMi Ri] and a secure multiple blind digital signature scheme.
(*RSA assumption*) The RSA scheme is secure. And, to break the RSA scheme in which the plaintext's redundancy is 0 is as hard to break as the RSA scheme in

which the plaintext's redundancy is less than 1/2, where S's redundancy is r if S is randomly selected from a source with the entropy of $(1-r)|S|$ bits. (Here, "as hard as" is defined from the viewpoint of usual "polynomial-time reduction.")

Proof Sketch:

Completeness: $\overline{C}$ and $\overline{H}$ are accepted with probability 1.

Soundness: First, we prove the following (the soundness can be directly reduced from the folowing result if the digital signature assumption and RSA assumption are satisfied, because a polynomial-time algorithm can be constructed to break these assumptions using M_p if $\widetilde{C}$ is accepted):

There exists a polynomial-time probabilistic Turing machine M_P (with complete control over P) such that if C is accepted to be valid by $\overline{V}$ through part III of Protocol 1 with non-negligible probability, then M_P breaks cryptographic assumption on A's digital signatures with the public key e'_A, and, for any positive constant $b < 1$, M_P, on input $\{I_i\}$ and b, outputs a subset $\mathcal{S} \subset \{S_i\}$ such that $\#\mathcal{S}/(K/2) > b$ with overwhelming probability, where $\#$ denotes the cardinality of a subset.

If C is accepted by $\overline{V}$ with non-negligible probability, then P can generate A's digital signature for non-negligible fraction of the message space. Therefore, from the definition of secure blind digital signature [GoMiRi], there exists a polynomial-time probabilistic Turing machine M_P such that M_P breaks cryptographic assumptions of A's blind digital signature with overwhelming probability. Next we show that when C is accepted by $\overline{V}$ with non-negligible probability, then, for any positive constant $b < 1$, M_P can output a subset $\mathcal{S} \subset \{S_i\}$ such that $\#\mathcal{S}/(K/2) > b$ with overwhelming probability. Let T be the truncated execution tree of $(P, \overline{V})$. T has $(K/2)$ levels, and each vertex in T has at most L_i $(=O(1))$ sons, because $\overline{V}$ may ask L_i possible questions at each stage. A vertex is called heavy if it has at least two sons. If we can find a heavy vertex of the i-th level, we can compute S_i, since L_i is prime. Then, for a positive constant $b < 1$, we assume that at least $(1-b)(K/2)$ levels have at least one non-heavy vertex. Then, the total number of leaves in T is at most a negligible $(O(2^{-K}))$ fraction of the possible leaves. Therefore, for any positive constant $b < 1$, more than $b(K/2)$ levels have all heavy vertices. Hence, we can find at least one heavy vertex in each level with all heavy vertices in polynomial-time by blind exploration of T, since a non-negligible fraction of the leaves is assumed to survive the truncation.

Finally, we can conclude the proof of soundness by showing in a similar manner that there exists a polynomial-time probabilistic Turing machine M_V (with complete control V) such that if history H is accepted to be valid by $\overline{A}$ through part IV of Protocol 1 with non-negligible probability, then M_V breaks cryptographic assumption on A's digital signatures with the public key e'_A.

Untraceability: In a manner similar to the proof of the zero-knowledgeness of the extended Fiat-Shamir scheme [OhO], it can be proven that there exists M_V such that $(C, \{X_i\}, B)$, $(\overline{P}(\{S_i\}), \underline{V(t)})(\{I_i, N_i, L_i\}))$ and $M_V^A(\{I_i, N_i, L_i\}, t)$ are polynomially indistinguishable.

Disposability: We show that when $\overline{C}$ is used twice, any S_i cannot be revealed

with negligible probability. Let $\mathcal{E}=\{E_i \mid E_i$ selected by V_1 and E_i selected by V_2 are different in part III, $1 \le i \le K/2\}$. Then, for any positive constant $b < 1$, $\#\mathcal{E} > b(K/2)$ with overwhelming probability. Since L_i is prime, we can calculate $I_i^{1/L_i} \bmod N_i$ for i whose E_i is in $\mathcal{E}$. Therefore, to make all S_i's be concealed from anyone, at least $b(K/2)$ blind candidates W_i must be invalid in part I, and all these invalid candidates must not be selected in U. Hence, all S_i's can be concealed from anyone with probability $2^{-b(K/2)}$ (or negligible probability). In other words, if $\overline{C}$ is used twice, at least one piece of information S_i can be revealed with overwhelming probability. **QED**

5. Transferable Untraceable Electronic Cash

In this section, we propose an electronic cash scheme satisfying the criterion of *tranferability* in addition to untraceability and unreusability.

Protocol 2. (Transferable untraceable electronic cash)
This protocol is constructed based on Protocol 1. Therefore, undefined notations and procedures follow the definitions in Protocol 1. To simplify the description of this protocol, we suppose a case where bank A issues one dollar electronic coin C to customer P_1, who transfers C to customer P_2, and P_2 uses C 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 have bank A issue an electronic coin worth one dollar C.

Part III.
To transfer C to another customer P_2, P_1 and P_2 proceeds as follows:
(Step 1) P_1 and P_2 follow the same protocol as that for P_1 to pay shop P_2 one dollar (Part III of Protocol 1).
(Step 2) P_1 sends a certification T that denotes the transfer of C from P_1 to P_2. For example, P_1 sends a digital signature $G_{(N_1^{(1)}, L_1^{(1)})}(C \parallel B^{(2)})$ (e.g., $T = g(C \parallel B^{(2)})^{1/L_1^{(1)}} \bmod N_1^{(1)}$).
P_2 generates

$$R_i^{(2)} = (X_i^{(1)})^{1/L_i^{(2)}} \bmod N_i^{(2)} \quad \text{for } 1 \le i \le K/2.$$

If P_2 accepts P_1's electronic coin C through step 1 and verifies the validity of T, then P_2 pays one dollar to P_1.

Part IV.
To pay shop V one dollar, P_2 and V proceeds 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.

Part V.
To have bank A credit V's account by one dollar, V sends the history of Part IV of this protocol, $H^{(2)}$, to A, which credits V's account after verifying whether $H^{(2)}$ is a correct history of Part IV and whether $H^{(2)}$ has not been stored already in A's database. If $H^{(2)}$ is valid, bank A must store $H^{(2)}$ in its database.

(End of Protocol 2)

Note: Informally, Protocol 2 is secure if the following conditions are satisfied. The formal definition and proof regarding the security of Protocol 2 will be shown in the final paper.

- *Completeness*: Any (original/transfered) valid cash $\overline{C}$ of $\overline{P}_1$ and $\overline{P}_2$ is accepted to be valid by $\overline{P}_2$ and any shop V, respectively. Any valid history $\overline{H}^{(2)}$ is accepted to be valid by bank $\overline{A}$.
- *Soundness*: Any (transfered) invalid cash $\widetilde{C}$ is accepted by P_2 and any shop $\overline{V}$ with negligible probability. Any invalid history $\widetilde{H}^{(2)}$ is accepted by any bank with negligible probability.
- *Untraceability*: When a valid coin $\overline{C}$ is used only once, any knowledge about the identity of the customer who uses $\overline{C}$ cannot be revealed by anyone.
- *Unreusability*: When coin $\overline{C}$ is used twice correctly by a customer, bank $\overline{A}$ can obtain the identity of the customer with overwhelming probability. When coin $\overline{C}$ is used twice correctly by two different customers $\overline{P}_1$ and $\overline{P}_2$, bank $\overline{A}$ can obtain the identity of $\overline{P}_1$ with overwhelming probability.

6. Untraceable Electronic Coupon Tickets

In this section, we also propose another type of untraceable electronic cash (*untraceable electronic coupon ticket*) with the following property in addition to those of the untraceable electronic cash: The value of one piece of electronic cash can be subdivided into several pieces. For example, a user with a piece of electronic cash worth \$100 could subdivide it into 100 pieces of cash worth \$1. Here, the data size of 100 coupon tickets is comparable to one piece of electronic cash.

If we add the notion of transferability (criterion (3)), *transferable* untraceable electronic coupon ticket could be constructed in a way similar to the transferable untraceable electronic cash.

Protocol 3. (Untraceable electronic coupon ticket) This protocol is constructed based on Protocol 1. Therefore, undefined notations and procedures follow the definitions in Protocol 1.

Part I.
To obtain license B from bank A, customer P follows the same protocol with A as Part I of Protocol 1.

Part II.
To obtain a piece of information (electronic coupon tickets), C, which is 100 tickets

each worth \$1, customer P conducts the same protocol with bank A as Part II of Protocol 1. Here, the value of e' indicates the value and type of electronic coupon tickets C (e.g., 100 tickets each worth \$1).

Part III.
To pay shop V the j-th one dollar ticket ($1 \leq j \leq 100$), P and V proceeds as follows:
First, P generates $X_i^{<j>} = f_j(X_i)$ and $R_i^{<j>} = (X_i^{<j>})^{1/L_i} \bmod N_i$. Here, $f_j(x)$ means a one-way function with a parameter j. For example, we can construct f_j by a one-way function f such that

$$f_j(x) = f(x \parallel j), \quad \text{or} \quad f_j(x) = f(x \parallel 1^j).$$

For each $i = 1, 2, \ldots, K/2$, steps 1-4 are executed iteratedly.
(Step 1) and (Step 2) are the same as those of Protocol 1.
(Step 3) and (Step 4) are the same as those of Protocol 1 except replacing X_i and R_i by $X_i^{<j>}$ and $R_i^{<j>}$, respectively. Here, P also sends j, and V checks that $1 \leq j \leq 100$ and generates $X_i^{<j>} = f_j(X_i)$.
If P passes this protocol successfully for all $i = 1, 2, \ldots, K/2$, then V accepts the j-th one dollar ticket of the \$100 electronic coupon tickets C.

Part IV.
For bank A to credit V's account by one dollar, V sends the history of Part III of this protocol, $H^{<j>}$, to A, which credits V's account after verifying whether $H^{<j>}$ is a correct history of Part III and whether $H^{<j>}$ has not been stored already in A's database. If $H^{<j>}$ is valid, bank A must store $H^{<j>}$ in its database.

(End of Protocol 3)

7. Conclusion

In this paper, we have proposed a new type of authenticatication, *disposable zero-knowledge authentication*, and described its applications to untraceable electronic cash schemes. To find other applications of the disposable zero-knowledge authentication remains further work. We improved the efficiency of our scheme by reducing the degree of untraceability. We will concentrate on improving the efficiency of these schemes with perfect untraceability in further work. In the proof of the security of these protocols, we have supposed some assumptions. To reduce these assumptions to even more fundamental assumptions remains an open challenge.

Acknowledgements: We would like to thank Eugène van Heyst for many valuable comments and suggestions on the earlier version. We would also like to thank anonymous referees for their helpful comments.

References

[B] J.C.Benaloh, "Cryptographic capsules: A disjunctive promitive for interactive protocols," The Proc. of Crypto'86, pp.213-222 (1986)

[BC] G.Brassard and C.Crépeau, "Non-Transitive Transfer of Confidence: A perfect Zero-Knowledge Interactive Protocol for SAT and Beyond," The Proc. of FOCS'86, pp.188-195 (1986)

[BCC] G.Brassard, D.Chaum, and C.Crépeau, "Minimum Disclosure Proofs of Knowledge," Journal of Computer and System Sciences, Vol.37, pp.156-189 (1988)

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

[Cr] C.Crépeau, "A zero-knowledge poker protocol that achieves confidentiality of the players' strategy or How to achieve an electronic poker face," The Proc. of Crypto'86, pp.239-247 (1986)

[CFN] D.Chaum, A.Fiat and M. Naor, "Untraceable Electronic Cash," to appear in the Proc. of Crypto'88 (1988)

[D] I.B.Damgård, "Payment Systems and Credential Mechanisms with Provable Security Against Abuse by Individuals," to appear in the Proc. of Crypto'88 (1988)

[FFS] U.Feige, A.Fiat and A.Shamir, "Zero Knowledge Proofs of Identity," The Proc. of STOC, pp.210-217 (1987)

[FS] A.Fiat and A.Shamir, "How to Prove Yourself," The Proc. of Crypto'86, pp.186-199 (1986)

[GM] S.Goldwasser, and S.Micali, "Probabilistic Encryption," Journal of Computer and System Science, Vol.28, No.2 (1984)

[GMR] S.Goldwasser, S.Micali, and C.Rackoff, "Knowledge Complexity of Interactive Proofs," The Proc. of STOC, pp291-304 (1985)

[GoMiRi] S.Goldwasser, S.Micali, and R.Rivest, "A Digital Signature Scheme Secure Against Adaptive Chosen-Message Attacks," SIAM J.Compt., 17, 2, pp.281-308 (1988)

[GMW] O.Goldreich, S.Micali, and A.Wigderson, "Proofs that Yield Nothing But their Validity and a Methodology of Cryptographic Protocol Design," The Proc. of FOCS, pp.174-187 (1986)

[GQ] L.C.Guillou, and J.J.Quisquater, "A Practical Zero-Knowledge Protocol Fitted to Security Microprocessors Minimizing Both Transmission and Memory," The Proc. of Eurocrypto'88, pp.123-128 (1988)

[MS] S.Micali, and A.Shamir, "An Improvement of The Fiat-Shamir Identification and Signature Scheme," The Proc. of Crypto'88 (1988)

[OhO] K.Ohta, and T.Okamoto "A Modification of the Fiat-Shamir Scheme," to appear in the Proc. of Crypto'88 (1988)

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

[TW] M.Tompa and H.Woll, "Random Self-Reducibility and Zero Knowledge Interactive Proofs of Possession of Information," The Proc. of FOCS, pp472-482 (1987)

[Y] A.C. Yao: Theory and Applications of Trapdoor Functions, The Proc. of FOCS, pp.80-91 (1982)