

# Improvement of Efficiency in (Unconditional) Anonymous Transferable E-Cash<sup>\*</sup>

Sébastien Canard<sup>1</sup>, Aline Gouget<sup>2</sup>, and Jacques Traoré<sup>1</sup>

<sup>1</sup> Orange Labs R&D, 42 rue des Coutures, F-14066 Caen, France.

<sup>2</sup> Gemalto, 6, rue de la Verrerie, F-92190 Meudon, France.

**Abstract.** The practical advantage expected from transferable e-cash compare to non-transferable is the significant reduction of the interaction number between the bank and the users. However, this property is not fulfilled by *anonymous* transferable e-cash schemes of the state-of-the-art. In this paper, we first present a transferable e-cash scheme with a reduced number of communications between the bank and the users that fulfils the *computational anonymity* property. Next, we present a transferable e-cash scheme with a reduced interaction number that fulfils the *unconditional anonymity*. This latter scheme is quite less efficient.

**Keywords.** Electronic cash, anonymity, transferability.

## 1 Introduction

In regular cash systems, users withdraw coins from a bank, and then pay merchants using coins. Next, merchants can use the received coins to pay another merchant or deposit coins to the bank. Moreover, regular cash systems protect the anonymity of users.

Emulating regular cash in the electronic setting implies providing the user anonymity against both the bank and the merchant during a purchase, i.e., it must be impossible to link two spends and a spend to a withdrawal. Ideally, the anonymity of honest users must be protected and the identity of cheaters must be recovered without using a trusted third party. As it is easy to duplicate electronic data, an e-cash system must prevent a user from double-spending. An electronic coin system must also prevent a merchant from depositing the same coin twice.

The transferability property is another fundamental property of regular cash. However, it has received only little attention in the electronic setting. This may be explained by the impossibility to transfer a coin without increasing its size [6]. It is clearly a limitation but this apparent drawback is not unacceptable for some practical applications depending

---

<sup>\*</sup> This work has been partially financially supported by the European Commission through the IST Program under Contract IST-2002-507932 ECRYPT.

on the amount of available storage data and the growth of the coin size. The main expected advantage of the transferability property compare to non-transferability for e-cash is the decrease of the interaction number between the bank and the users. Thus, as on-line electronic payment systems require communications with a central authority during the payment transaction, then transferability is only an issue for off-line systems.

### 1.1 Related Works

As far as we know, the transferability property in e-cash schemes has received only little attention.

In 1989, Okamoto and Ohta [11] proposed a transferable e-cash scheme that does not provide the anonymity property since it is possible to link several spends of the same user. Next, van Antwerpen [15] proposed a method for transferring e-cash which was later sketched in [6]. This transferable e-cash scheme fulfils the user anonymity. However, at any time a user wants to act as a payee during a spending protocol, he has to beforehand interact with the bank in a protocol corresponding to the withdrawal of a coin with no monetary value. This drawback implies a significative increase of the number of transactions between the bank and users which make the scheme less attractive in the transferability setting where the aim is precisely to decrease these communications.

### 1.2 Our Contribution and Organization of the Paper

We present two anonymous transferable e-cash schemes that improve the state-of-the-art on anonymous transferable e-cash by addressing the problem of decreasing the interaction number between the bank and users. Indeed, it is no more necessary for a payee to beforehand interact with the bank for receiving a coin. Both schemes allow to withdraw efficiently a set of coins (a wallet) instead of a coin.

Section 2 introduces the security model and some useful tools. In Section 3, we present a first transferable scheme that fulfils a computational anonymity and in Section 4 we present a second transferable e-cash scheme that fulfils an unconditional anonymity at the cost of a less efficient result. We conclude in Section 5.

## 2 Definitions and Useful Tools

In this section, we first define transferable e-cash algorithms, global variables and oracles. Next, we describe the security properties.

## 2.1 Algorithms

A transferable e-cash system involves two types of player: a bank  $\mathcal{B}$  and a user  $\mathcal{U}$ . A wallet  $W$  and a coin  $C$  are both represented by an identifier  $S$  and some values  $\pi$  needed to prove their validity.

– **ParamGen**( $k$ ) is a probabilistic algorithm that outputs the parameters of the system  $Par$  (including the security parameter  $k$ ).

– **BKeyGen**( $Par$ ) (resp. **UKeyGen**( $Par$ )) is a probabilistic algorithm executed by  $\mathcal{B}$  (resp.  $\mathcal{U}$ ) that outputs its key pair  $(sk_{\mathcal{B}}, pk_{\mathcal{B}})$  (resp.  $(sk_{\mathcal{U}}, pk_{\mathcal{U}})$ ).

– **Withdraw**( $\mathcal{B}(sk_{\mathcal{B}}, pk_{\mathcal{B}}, pk_{\mathcal{U}}, Par)$ ,  $\mathcal{U}(sk_{\mathcal{U}}, pk_{\mathcal{U}}, pk_{\mathcal{B}}, Par)$ ) is an interactive protocol where  $\mathcal{U}$  withdraws a wallet from  $\mathcal{B}$ . At the end,  $\mathcal{U}$  either gets a wallet  $W = (S, \pi)$  and outputs  $OK$ , or outputs  $\perp$ . The output of  $\mathcal{B}$  is either its view  $\mathcal{V}_{\mathcal{B}}^W$  of the protocol (including  $pk_{\mathcal{U}}$ ), or  $\perp$ .

– **Spend**( $\mathcal{U}_1(S, \pi, pk_{\mathcal{U}_2}, Par)$ ,  $\mathcal{U}_2(sk_{\mathcal{U}_2}, pk_{\mathcal{B}}, Par)$ ) is an interactive protocol where  $\mathcal{U}_1$  gives a coin to  $\mathcal{U}_2$ .  $\mathcal{U}_2$  outputs either  $C = (S, \pi)$  or  $\perp$ , and  $\mathcal{U}_1$  either saves that  $C$  is spent and outputs  $OK$ , or outputs  $\perp$ .

– **Deposit**( $\mathcal{U}(C, sk_{\mathcal{U}}, pk_{\mathcal{U}}, pk_{\mathcal{B}}, Par)$ ,  $\mathcal{B}(sk_{\mathcal{B}}, pk_{\mathcal{B}}, pk_{\mathcal{U}}, \mathcal{L}, Par)$ ) is an interactive protocol where  $\mathcal{U}$  deposits a coin  $C = (S, \pi)$  at the bank  $\mathcal{B}$ . If  $(S, \pi)$  is not consistent/fresh, then  $\mathcal{B}$  outputs  $\perp_1$ . Else, if  $S$  belongs to  $\mathcal{L}$ , then there is an entry  $(S, \tilde{\pi})$  and  $\mathcal{B}$  outputs  $(\perp_2, S, \pi, \tilde{\pi})$ . Else,  $\mathcal{B}$  adds  $(S, \pi)$  to  $\mathcal{L}$ , credits  $\mathcal{U}$ 's account, and returns  $\mathcal{L}$ .  $\mathcal{U}$ 's output is  $OK$  or  $\perp$ .

– **Identify**( $S, \pi, \tilde{\pi}, Par$ ) is a deterministic algorithm executed by  $\mathcal{B}$  that outputs a public key  $pk_{\mathcal{U}}$  and a proof  $\Pi_G$ . If the users who had submitted  $\pi$  and  $\tilde{\pi}$  are not malicious, then  $\Pi_G$  is evidence that  $pk_{\mathcal{U}}$  is the registered public key of a user that double-spent a coin.

– **VerifyGuilt**( $pk_{\mathcal{U}}, \Pi_G, Par$ ) is a deterministic algorithm that can be executed by any actor. It outputs 1 if  $\Pi_G$  is correct and 0 otherwise.

## 2.2 Global Variables and Oracles

The set of user's public (resp. secret) keys is denoted by  $\mathcal{PK} = \{(i, pk_i) : i \in \mathbb{N}\}$  (resp.  $\mathcal{SK} = \{(i, sk_i) : i \in \mathbb{N}\}$ ;  $sk_i = \perp$  if user  $i$  is corrupted).

The oracle **Create**( $i$ ) creates a new honest user. **Corrupt**( $i, pk_i$ ) creates a new corrupted user with public key  $pk_i$  and **Corrupt**( $i$ ) corrupts user  $i$  by giving the secret key of user  $i$  to the caller.

The oracle **Suppl**( $i$ ) (resp. **Withd**( $i$ )) plays the bank (resp. user  $i$ ) side of a **Withdraw** protocol. The oracle **Withd&Suppl**( $i$ ) plays both sides of a **Withdraw** protocol and outputs the communications between  $\mathcal{B}$  and  $\mathcal{U}$ .

The oracle **Rcv**( $i$ ) (resp. **Spd**( $i$ )) plays the role of  $\mathcal{U}_2$  (resp.  $\mathcal{U}_1$ ) with secret keys of user  $i$  in the **Spend** protocol. The oracle **Spd&Rcv**( $i_1, i_2, j$ )

plays the role of both  $\mathcal{U}_1$  with secret keys of user  $i_1$  and  $\mathcal{U}_2$  with secret keys of user  $i_2$  during the spend protocol of the coin  $j$  and outputs the communications. We define four prototypes:  $\mathbf{Spd\&Rcv}(\perp, \perp, j)$ ,  $\mathbf{Spd\&Rcv}(i_1, \perp, \perp)$ ,  $\mathbf{Spd\&Rcv}(i_1, i_2, \perp)$  and  $\mathbf{Spd\&Rcv}(\perp, i_2, j)$ , where  $\perp$  denotes a random choice for a user or a coin.

The oracle  $\mathbf{CreditAccount}()$  plays the role of  $\mathcal{B}$  during a **Deposit** protocol. If the executed **Deposit** protocol outputs  $(\perp_2, S, \pi, \tilde{\pi})$ , then it runs the algorithm **Identify** on inputs  $(S, \pi, \tilde{\pi})$  and outputs the result. The oracle  $\mathbf{Depo}(i)$  plays the role of the user  $i$  during a **Deposit** protocol.

### 2.3 Security Properties

**Unforgeability.** Users cannot spend more coins than they honestly got. *Game.* Let an adversary  $\mathcal{A}$  be a p.p.t. Turing Machine with access to  $\mathcal{PK}$ .

1.  $\mathcal{A}$  is given the public key  $pk_{\mathcal{B}}$  and  $Par$ .
2.  $\mathcal{A}$  can play as many times as he wants with the oracles: **Create**, **Corrupt**, **Suppl**, **Withd&Suppl**, **Spd**, **Spd&Rcv**, **Rcv** and **CreditAccount**.

Let  $q_W$  (resp.  $q_S$ , resp.  $q_C$ ) denote the number of successful queries to **Suppl** (resp. **Spd**, resp. **Corrupt**). Let  $w_i$  denote the number of withdrawn coins of the  $i$ -th query and  $c_i$  denote the number of coins get back from the  $i$ -th corrupted user. Then,  $\mathcal{A}$  wins if, at any time of the game, he makes  $\sum_{i=1}^{q_W} w_i + q_S + \sum_{i=1}^{q_C} c_i + 1$  successful queries to the **Rcv** oracle.

**Anonymity.** The bank, even cooperating with users, cannot link spend and/or withdrawal transactions according to the underlying user identity. *Game.* Let an adversary  $\mathcal{A}$  be a p.p.t. Turing Machine with access to  $\mathcal{PK}$ .

1.  $\mathcal{A}$  is given  $(sk_{\mathcal{B}}, pk_{\mathcal{B}})$  and  $Par$ , and  $\mathcal{A}$  can play with the oracles: **Create**, **Corrupt**, **Withd**, **Spd**, **Spd&Rcv**, **Rcv** and **Depo**.
2. At any time,  $\mathcal{A}$  chooses two honest user public keys  $pk_{i_0}, pk_{i_1} \in \mathcal{PK}$  such that users  $i_0$  and  $i_1$  own coins of the same size<sup>1</sup> and they have been manipulated only by the oracles: **Create**, **Withd**, **Spd**, **Spd&Rcv** $(i_1, \perp, \perp)$ , **Spd&Rcv** $(\perp, \perp, j)$  and **Depo**.
3. A bit  $b$  is secretly and randomly chosen. Then  $\mathcal{A}$  plays with **Spd** $(i_b, \perp)$ .
4.  $\mathcal{A}$  outputs a bit  $b'$ .

We require that, for every  $\mathcal{A}$  playing this game, the probability that  $b = b'$  differs from  $1/2$  by a fraction that is at most negligible.

<sup>1</sup>  $\mathcal{A}$  is not allowed to use the coin size that necessary grows when transferred [6].

**Identification of double-spenders.** No collection of users can double-spend a coin twice without revealing one of their identities.

*Game.* Let an adversary  $\mathcal{A}$  be a p.p.t. Turing Machine with access to  $\mathcal{PK}$ .

1.  $\mathcal{A}$  is given the public key  $pk_B$  and  $Par$ .
2.  $\mathcal{A}$  can play as many times as he wants with the oracles: **Create**, **Corrupt**, **Suppl**, **Withd&Suppl**, **Spd**, **Spd&Rcv**, **Rcv** and **CreditAccount**.

$\mathcal{A}$  wins if, at any time of the game, the oracle **CreditAccount** outputs  $(\perp_2, S, \pi, \tilde{\pi})$  and the output of the oracle **Identify** on inputs  $(S, \pi, \tilde{\pi})$  is not a registered user public key.

**Exculpability.** The bank, even cooperating with malicious users, cannot falsely accuse (with a proof) honest users from having double-spent a coin.

*Game.* Let an adversary  $\mathcal{A}$  be a p.p.t. Turing Machine with access to  $\mathcal{PK}$ .

1.  $\mathcal{A}$  is given the key pair  $(pk_B, sk_B)$  and  $Par$ .
2.  $\mathcal{A}$  can play as many times as he wants with the oracles: **Create**, **Corrupt**, **Withd**, **Spd**, **Spd&Rcv**, **Rcv** and **Depo**.
3. At any time of the game,  $\mathcal{A}$  outputs two spends  $(S, \pi)$  and  $(S, \tilde{\pi})$ .

$\mathcal{A}$  wins if the outputs of the algorithm **Identify** on inputs  $(S, \pi, \tilde{\pi})$  is the public key  $pk$  of an honest user together with a valid proof  $\Pi_G$ , and the output of the algorithm **VerifyGuilt** on inputs  $(pk, \Pi_G)$  is 1.

## 2.4 Useful Tools

**Signature of knowledge.** We consider zero-knowledge proofs of knowledge (ZKPK) constructed over a group  $\mathcal{G}$  either of prime or unknown order. We use proofs of knowledge of a discrete logarithm [14, 10] or of a representation, a proof of equality of two known representations [6], and a proof that a committed value is less than another committed value [5].

These proofs are three-move protocols between a prover and a verifier: a commitment  $t$ , a question  $c$  and an answer  $s$ . The soundness of these constructions ensures that given a single  $t$ , if someone is able to provide  $s$  and  $s'$  related to  $c$  and  $c'$  s.t.  $c \neq c'$ , then it is possible to compute the secret.

These interactive proofs can also be used non interactively (a.k.a. *signatures of knowledge*) by using the Fiat-Shamir heuristic [9]. Their security has been proven in [13], using the forking lemma.

**Caménisch-Lysyanskaya Signature Scheme.** These signature schemes are proposed in [3] with in addition some specific protocols:

- an efficient protocol between a user  $\mathcal{U}$  and a signer  $\mathcal{S}$  that permits  $\mathcal{U}$  to obtain from  $\mathcal{S}$  a signature  $\sigma$  of some commitment  $C$  on values  $(x_1, \dots, x_l)$  unknown from  $\mathcal{S}$ .  $\mathcal{S}$  computes  $\text{CLSign}(C)$  and  $\mathcal{U}$  gets  $\sigma = \text{Sign}(x_1, \dots, x_l)$  that can be verified by  $\text{Verif}(\sigma, (x_1, \dots, x_l)) = 1$ .
- an efficient proof of knowledge of a signature on committed values, denoted by  $PK(\alpha_1, \dots, \alpha_l, \beta : \beta = \text{Sign}(\alpha_1, \dots, \alpha_l))$ .

### 3 Transferable Compact E-cash Scheme

In this section, we present a transferable e-cash scheme with a reduced number of communications between the bank and the users that fulfills the security properties given in Section 2.3. Moreover, the proposed construction allows to withdraw efficiently a wallet instead of a coin.

#### 3.1 Overview of our construction

Our construction is based on the compact e-cash scheme [2]. More precisely, in the withdrawal, the user obtains from the bank a CL signature (see Section 2.4) on some data related to the withdrawn wallet. The spending of a withdrawn coin consists in the computation by the payer of a serial number  $S$  and a validity tag  $T$  used in case of double-spending.

The main modification comes from the possibility for the receiver to spend later a received coin. This is done by modifying the challenge sent by the receiver during a **Spend**: it should include a receiver identifier (here  $u_j$ ), it should be verifiable (here using the Dodis-Yampolskiy pseudo-random function [8]) and it should be signed by the payer (here with the signature of knowledge of the payment validity) that permits the receiver to get a payer validation that he is allowed to spend later the coin.

Moreover, the security tag includes the serial number of the coin (so as to prevent double-spending) and the history of the coin (so as to prevent a fraud on the anonymity of the spenders done by the bank).

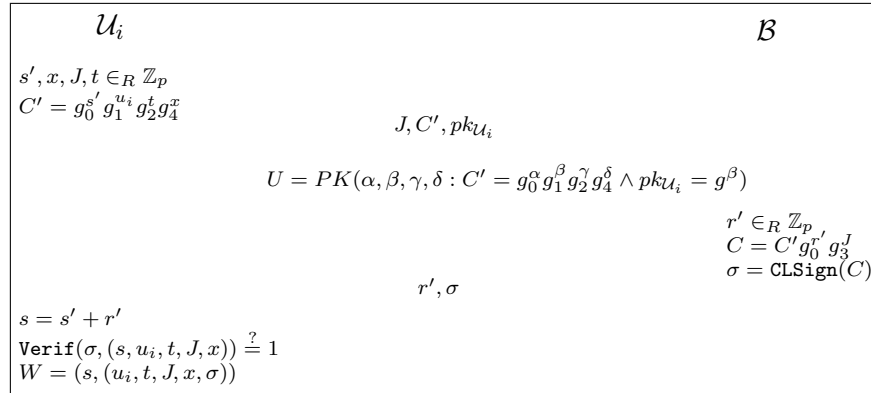
#### 3.2 Description of the Scheme

**Setup.** Let  $k$  be a security parameter. Let  $\mathcal{G}$  be a group of prime order  $p$  and  $g, g_0, g_1, g_2, g_3, g_4, g_5$  are random generators in  $\mathcal{G}$ . These data constitute the public parameters  $Par$ . Let  $\mathcal{H}$  be a cryptographic hash function. In the following,  $a||b$  denotes the concatenation of  $a$  and  $b$ .

In the **BKeyGen** algorithm,  $\mathcal{B}$  computes two key pairs  $(sk_{\mathcal{B},1}, pk_{\mathcal{B},1})$  and  $(sk_{\mathcal{B},2}, pk_{\mathcal{B},2})$  of a CL signature scheme (see Section 2.4) that permit it to sign wallets and enroll users, respectively. Then, during the **UKeyGen** algorithm, each user  $\mathcal{U}_i$  obtains a certificate  $C_i$  associated to his public key  $pk_{\mathcal{U}_i} = g_0^{u_i}$  (related to  $sk_{\mathcal{U}_i} = u_i \in_R \mathcal{G}$ ). The certificate is a CL (verifiable) signature done by  $\mathcal{B}$ :  $C_i = \text{Sign}(u_i, w_i)$  where  $w_i$  is a random value.

**Withdrawal Protocol.** A wallet is a signature under the bank's public key  $pk_{\mathcal{B}}$  on the set of values  $(s, u_i, t, J, x)$  where  $u_i$  is the user secret key,  $s, t$  and  $x$  are random values and  $J$  is the number of coins contained in the wallet. The value  $s$  implicitly defines  $J$  unlinkable *serial numbers* and the value  $t$  implicitly defines  $J$  unlinkable *blinding values*.

A user  $\mathcal{U}_i$  using  $(u_i, g_0^{u_i})$  interacts with  $\mathcal{B}$  using  $(sk_{\mathcal{B},1}, pk_{\mathcal{B},1})$  as described in Figure 1 in a protocol close to the ones in [2, 5]. At the end,  $\mathcal{U}_i$



**Fig. 1.** Withdrawal protocol

gets a wallet  $\mathcal{W} = (S, \pi) = (s, (u_i, t, J, x, \sigma))$  where  $\sigma$  is a CL signature on  $(s, u_i, t, J, x)$ .

**Spending a withdrawn coin.** A user  $\mathcal{U}_i$ , owning  $W = (s, (u_i, t, J, x, \sigma))$  withdrawn from  $\mathcal{B}$ , wants to spend a coin to a user  $\mathcal{U}_j$ . The protocol is similar to the one of the compact e-cash system, except that  $\mathcal{U}_j$  computes the *random* value  $r$  using her secret key  $u_j$  and some data  $d'$ .

1.  $\mathcal{U}_j$  computes  $r = g_0^{\frac{1}{u_j + d'}}$  where  $d'$  represents some data related to the transaction. Next,  $\mathcal{U}_j$  sends  $r$  and  $d'$  to  $\mathcal{U}_i$ .

- $\mathcal{U}_i$  computes  $R = \mathcal{H}(r||d||d')$  (where  $d$  represent some data related to the transaction) and chooses an unspent coin  $j \in [1, J]$ . Next,  $\mathcal{U}_i$  computes  $S = g_5^{\frac{1}{s+j+1}}$ ,  $T = pk_{\mathcal{U}_i} g_5^{\frac{R}{t+j+1}}$  and a proof of validity:

$$V = PK(\alpha, \beta, \delta, \zeta, \eta, \iota, \theta : \alpha = \mathbf{Sign}(\iota, \beta, \delta, \zeta, \theta) \wedge \eta \in [1, \zeta] \wedge \wedge S = g_5^{\frac{1}{\beta+\eta+1}} \wedge T = g_0^\delta g_5^{\frac{R}{\iota+\eta+1}})(S, T, r)$$

where the signature is the signature  $\sigma$  of the withdrawn wallet.

- The spent coin is represented by  $(S, \pi = (T, V, r, d, d'))$ . Implicitly, a related variable  $hist$  is initialized to  $hist := S||T$ .

**Spending a received coin.** Assume that a user  $\mathcal{U}_i$  owns a coin  $C = (S, \pi = (\pi_1, \dots, \pi_l))$ , where  $\pi_k$  corresponds to  $T_k, V_k, r_k, d_k, d'_k$ ,  $1 \leq k \leq l$ , that he legitimately received by another user. Since  $\mathcal{U}_i$  legitimately received  $C$ , it is necessary that  $r_l = g_0^{1/(u_i+d'_l)}$  and thus  $r_l$  involves  $u_i$ .

The spending of the coin  $C$  by user  $\mathcal{U}_i$  to user  $\mathcal{U}_j$  consists first in computing a security tag  $T$  implying the identifier  $u_i$  that is certified by the bank in order to be able to recover his identity in case of double-spending. Next,  $\mathcal{U}_i$  proves that the same identifier  $u_i$  is embedded into  $T$  and in the challenge  $r_l$  of the previous spending (using the validity proof of the Dodis-Yampolskiy PRF and the signature of knowledge of the previous spending).

- $\mathcal{U}_j$  computes  $r = g_0^{\frac{1}{u_j+d'}}$  where  $d'$  represents some data related to the transaction. Next  $\mathcal{U}_j$  sends  $r$  and  $d'$  to  $\mathcal{U}_i$ .
- $\mathcal{U}_i$  computes  $R = \mathcal{H}(r||d||d')$ ,  $h = \mathcal{H}(hist)$ ,  $T = pk_{\mathcal{U}_i} g_5^{\frac{R}{u_i+S+h}}$  and a proof of validity:

$$V = PK(\alpha, \beta, \gamma : T = g^\alpha g_5^{\frac{R}{\alpha+S+h}} \wedge r_l = g_0^{\frac{1}{\alpha+d'_l}} \wedge \beta = \mathbf{Sign}(\alpha, \gamma))(S, T, r)$$

where the signature corresponds to the certificate of user  $\mathcal{U}_i$ .

- The spent coin is  $(S, \pi = (\pi_1, \dots, \pi_l, \pi_{l+1}))$  where  $\pi_{l+1}$  corresponds to  $T, V, r, d, d'$ . The value  $hist$  is updated by  $hist := hist||T$ .

**Deposit protocol.** A coin may have been spent several times before being deposited at the bank. Then, a coin is represented by  $(S, (\pi_1, \dots, \pi_l))$  where  $\pi_k$ ,  $1 \leq k \leq l$ , corresponds to  $T_k, V_k, r_k, d_k, d'_k$ .

The bank  $\mathcal{B}$  first verifies the consistency of the coin (i.e. computes the values  $R$  using the hash function  $\mathcal{H}$  and the values  $r$  and  $d$  to check



the validity proofs). Next  $\mathcal{B}$  verifies whether or not the coin has already been deposited by checking if the identifier  $S$  is already in the database of spent coins. If not,  $\mathcal{B}$  credits the user account. Otherwise,  $\mathcal{B}$  checks the freshness of the coin. If  $R_l = \tilde{R}_l$  the depositer is a cheater. Else, the coin is fresh, there is a double-spending and  $\mathcal{B}$  uses the identify protocol.

**Identify protocol.** In case of a double-spending detection,  $\mathcal{B}$  has to retrieve the cheater identity from two deposited coins  $(S, \pi = (\pi_1, \dots, \pi_l))$  and  $(S, \tilde{\pi} = (\tilde{\pi}_1, \dots, \tilde{\pi}_l))$  with the same serial number  $S$ . Then,  $\mathcal{B}$  looks for the minimal value  $k_{min}$  of  $k$  such that  $\pi_k \neq \tilde{\pi}_k$  (this case always happens) and recovers the cheater's identity using the two double spending equations  $T_{k_{min}}$  and  $\tilde{T}_{k_{min}}$  included in  $\pi_{k_{min}}$  and  $\tilde{\pi}_{k_{min}}$ . Then,  $\mathcal{B}$  computes  $R_{k_{min}} = \mathcal{H}(r_{k_{min}} \| d_{k_{min}} \| d'_{k_{min}})$  and  $\tilde{R}_{k_{min}} = \mathcal{H}(\tilde{r}_{k_{min}} \| \tilde{d}_{k_{min}} \| \tilde{d}'_{k_{min}})$ . Finally,  $\mathcal{B}$  gets the public key of the cheater by computing:

$$pk_{\mathcal{U}} = (T_{k_{min}}^{\tilde{R}_{k_{min}}} / \tilde{T}_{k_{min}}^{R_{k_{min}}})^{\frac{1}{\tilde{R}_{k_{min}} - R_{k_{min}}}}$$

### 3.3 Security Proof

**Theorem 1.** *In the random oracle model, the transferable compact e-cash scheme fulfils:*

- *The unforgeability property under the unforgeability of the CL signature scheme.*
- *The anonymity property under the security of the Dodis-Yampolskiy PRF.*
- *The identification property under the unforgeability of the signatures of knowledge and the soundness of the underlying proofs of knowledge.*
- *The exculpability property under the DL assumption.*

**Unforgeability.** We want to show that if an adversary  $\mathcal{A}$  is able to break the unforgeability of our construction, then it is possible to break the unforgeability of the CL signature scheme under adaptive chosen message attacks. More precisely, we have access to two signature oracles, both related to the CL signature scheme but with two different key pairs (one for the enrollment and one for the withdrawal). Our aim is to break the unforgeability of one among the two CL signature schemes involved in the construction. Let us consequently consider two different games with two adversaries.

In game 1, we play the role of an honest bank with access to a CL signature oracle for each enrollment, when  $\mathcal{A}$  is active or not. In game 2,

we play the role of an honest bank with access to a CL signature oracle for each withdrawal.

In both games, after each successful spending executed by  $\mathcal{A}$ , we extract, using standard techniques, all the values embedded into the valid proof of knowledge  $V$  of the last spending. For the CL signature, these values corresponds either to  $(s, u, t, J, x, \sigma)$  when a withdrawn coin is spent or to  $(u, w, C)$  when a received coin is spent. By assumption, at any time of both games, there are more spent coins than  $\mathcal{A}$  can legitimately own, and there is no detection of double-spending.

In game 1, if  $\mathcal{A}$  uses the spending of a received coin, then it is necessary that one signature  $C$  on a message  $m = (u, w)$  does not come from the signature oracle. Thus, this one more signature is a forgery in the first CL's scheme on  $m = (u, w)$ . Otherwise, abort the game and output  $\perp$ .

In game 2, if  $\mathcal{A}$  uses the spending of a withdrawn coin, it is necessary that one signature  $\sigma$  on a message  $m = (s, u, t, J, x)$  is unknown and does not come from the signature oracle. Thus, this one more signature is a signature (forgery) in the second CL's scheme on the message  $m = (s, u, t, J, x)$ . Otherwise, abort the game and output  $\perp$ .

Consequently, by playing randomly one of the two above games until the result is not  $\perp$ , we can break the unforgeability of the CL signature scheme in expected running-time polynomial which is impossible.

Since our proof requires rewinding to extract the values, it is valid only against sequential attacks and not in a concurrent setting where  $\mathcal{A}$  is allowed to interact with  $\mathcal{B}$  in an arbitrarily interleaving manner. Indeed, our machine may be forced to rewind an exponential number of times. This drawback can be overcome by using well-know techniques [7] that require from the user the encryption of all values in a verifiable manner [4].

**Anonymity.** An adversary  $\mathcal{A}$  can succeed in breaking the anonymity property using several ways:

1.  $\mathcal{A}$  can succeed by linking a withdrawal and a (first) spending or two spends related to two withdrawn coins. This is impossible since if such an adversary exists, it would also break the anonymity property of the compact e-cash scheme [2].
2.  $\mathcal{A}$  can succeed by linking the spending of a withdrawn coin and the spending of a received coin. That means that  $\mathcal{A}$  succeeded in linking  $T = pk_U g_5^{R/(t+j+1)}$  and  $(\tilde{r} = g_0^{1/(u+\tilde{d})}, \tilde{T} = pk_U g_5^{\tilde{R}/(u+\tilde{S}+\tilde{h})})$ . This comes to decide whether the two values  $g^{1/(u+d)}$  and  $g^u g_5^{1/(t+j+1)}$  embed the same  $u$  or not. This is impossible since even if  $\mathcal{A}$  has access

to the values  $g^u$  and  $g^{\frac{1}{u+d}}$ , he cannot decide whether this is the same  $u$  due to the security of the Dodis-Yampolskiy PRF [8].

3.  $\mathcal{A}$  can succeed by linking two spends of two received coins. That means that  $\mathcal{A}$  succeeded in linking  $(r = g_0^{1/(u+d)}, T = pk_{\mathcal{U}}g_5^{R/(u+S+h)})$  and  $(\tilde{r} = g_0^{1/(u+\tilde{d})}, \tilde{T} = pk_{\mathcal{U}}g_5^{\tilde{R}/(u+\tilde{S}+\tilde{h})})$ . This comes to decide whether the two values  $g^{\frac{1}{u+d}}$  and  $g^{\frac{1}{u+\tilde{d}}}$  embed the same  $u$  or not. This is impossible since the Dodis-Yampolskiy PRF is secure.

Note that a user can legitimately received twice the same coin without compromising his anonymity due to the  $h$  involved in the value  $T$ .

*Remark 1.* Assume that  $\mathcal{A}$  is an unbounded adversary. Then  $\mathcal{A}$  can break the unconditional anonymity. Indeed, given  $T = pk_{\mathcal{U}}g_5^{R/(u+S+h)}$ ,  $\mathcal{A}$  knows or can compute  $S$ ,  $h = \mathcal{H}(hist)$  and  $R = \mathcal{H}(r_2, d_2, d'_2)$  and  $\mathcal{A}$  is assumed to be able to compute  $sk_v = v$  for every public key  $pk_v = g_0^v$ . Finally,  $\mathcal{A}$  simply checks whether  $T_2 \stackrel{?}{=} g_0^v g_5^{R_2/(v+S+h_2)}$ .

**Identification of Double-spenders.** Suppose that an adversary  $\mathcal{A}$  succeeds in breaking the identification of double-spender property. That means that there are two valid spends with the same serial number  $S = g_5^{1/s+j+1}$  and two different proofs  $\pi = (\pi_1, \dots, \pi_l)$  and  $\tilde{\pi} = (\tilde{\pi}_1, \dots, \tilde{\pi}_l)$ . The double-spending has been detected at rank  $k$ , which means that for all  $j < k$ ,  $\pi_j = \tilde{\pi}_j$  and that  $\pi_k \neq \tilde{\pi}_k$ . Note that the receivers are honest, and thus the values  $R_k$  and  $\tilde{R}_k$  are different and correctly computed.

1. Case  $k = 1$ : since the two spends are correct,  $R_1$  and  $\tilde{R}_1$  uniquely fix  $T_1 = pk_{\mathcal{U}}g_5^{R_1/(t+j+1)}$  and  $\tilde{T}_1 = pk_{\mathcal{U}}g_5^{\tilde{R}_1/(t+j+1)}$  as the only security tags to accompany serial number  $S$  except if  $\mathcal{A}$  has succeeded in faking the proof of knowledge  $V_1$  (or  $\tilde{V}_1$ ). Moreover, the embedded public key necessary belongs to a registered user, except if  $\mathcal{A}$  has forged the CL signature scheme. Both cases only happens with negligible probability.
2. Case  $k > 1$ : since the two spends are correct,  $R_k$  and  $\tilde{R}_k$  uniquely fix  $T_k = pk_{\mathcal{U}}g_5^{R_k/(u+S+1)}$  and  $\tilde{T}_k = pk_{\mathcal{U}}g_5^{\tilde{R}_k/(u+S+1)}$  as the only possible security tags except if  $\mathcal{A}$  has faked  $V_k$  (or  $\tilde{V}_k$ ). Moreover, the public key belongs to a registered user, except if  $\mathcal{A}$  has forged the CL signature scheme. Both cases only happens with negligible probability.

**Exculpability.** Suppose that an adversary  $\mathcal{A}$  succeeded in breaking the exculpability property. That means that there are two valid spends

with the same serial number  $S = g_5^{1/s+j+1}$  and two different proofs  $\pi = (\pi_1, \dots, \pi_l)$  and  $\tilde{\pi} = (\tilde{\pi}_1, \dots, \tilde{\pi}_l)$ . The double-spending can be detected at rank  $k$ , which means that for all  $j < k$ ,  $\pi_j = \tilde{\pi}_j$  and  $\pi_k \neq \tilde{\pi}_k$ . The receivers are honest and thus the values  $R_k$  and  $\tilde{R}_k$  are correct and different. As spends are correct,  $V_k$  (resp.  $\tilde{V}_k$ ) includes a proof that  $T_k$  (resp.  $\tilde{T}_k$ ) is well-formed. Thus, since the user is honest,  $\mathcal{A}$  has faked  $T_k$  or  $\tilde{T}_k$ .

We now use  $\mathcal{A}$  to break the one-more discrete logarithm problem [1]. Given  $l + 1$  values, we have to find the discrete logarithm of all these values, and we can ask a discrete logarithm oracle at most  $l$  times. We first associate each value to the public key of one user (assuming there are at most  $l$  users) and we ask the oracle each time  $\mathcal{A}$  corrupt a user. It is moreover possible to simulate all withdrawals and spends using standard techniques (in the random oracle model). At the end,  $\mathcal{A}$  outputs two correctly formed  $T_k$  and  $\tilde{T}_k$  and the associated proofs of validity. Thus,  $T_k$  and  $\tilde{T}_k$  are both formed from the same public key of a honest user.

From the two proofs of validity, we can extract the user secret key and thus break the one-more discrete logarithm. Indeed, since the user is honest, this discrete logarithm has not been requested to the oracle.

## 4 Unconditionally Anonymous Transferable Scheme

In this section, we present a transferable e-cash system providing the same features than the scheme presented in Section 3. In addition, the proposed scheme fulfils an unconditional anonymity. However, it necessitates a pre-computing phase before spending a withdrawn coin.

### 4.1 Overview of our construction

We adapt the scheme presented at Section 3 in order to get an unconditional anonymity of users. The withdrawal phase is unchanged and the spending phase also involves a challenge sent by the receiver including a receiver identifier  $u_j$ , that is verifiable and that is signed by the payer.

The main modification is the computation of the challenge sent by the receiver during the spending phase that will be used during the next spending. This challenge should provide an unconditional anonymity instead of a computational one. Then, the receiver computes the commitment  $t$  corresponding to the ZKPK of a representation  $(r, w)$  and that will be signed by the spender;  $t$  will necessary be used during the next spending. In case of double-spending,  $t$  will correspond to two different questions. Two different answers will thus permits to retrieve in particular  $r$ . This value  $r$  is moreover used in  $T = g^u h^r = pk_U h^r$  and thus

$pk_{\mathcal{U}}$  can be retrieved. Finally, we introduce a pre-computation phase to achieve the unconditional anonymity.

## 4.2 Description of the Scheme

The setup and the withdrawal protocol are unchanged from Section 3.2.

**Pre-computation phase.** Before spending a withdrawn coin, a user  $\mathcal{U}_i$  has to execute a *pre-computation* phase which is necessary to achieve the unconditional anonymity. This phase is similar to the spending protocol for a withdrawn coin defined in Section 3.2 with  $\mathcal{U}_i = \mathcal{U}_j$ . The main difference is the computation of the random value involving the receiver secret key; due to lack of space, this computation is only detailed in the spending protocol below.

Next,  $\mathcal{U}_i$  takes at random a bit  $B$ . If  $B = 0$ , then the pre-computation phase is over. Else,  $\mathcal{U}_i$  executes with himself the spending protocol.

**Spending protocol.** A user  $\mathcal{U}_i$ , owning a coin  $(S, \pi = (\hat{T}, \pi_0, \pi_1, \dots, \pi_l))$  where  $\pi_k = (V_k, T_k, T'_k, t_k, d_k)$ ,  $1 \leq k \leq l$  and  $l$  is the number of time this coin has been spent, can spend this coin to a user  $\mathcal{U}_j$ .

1.  $\mathcal{U}_j$  chooses at random  $r, w, a, b$ , computes  $T = g_0^{u_j} h^r$ ,  $T' = g^r h^w$  and  $t = g^a h^b$ , and sends  $T, T'$  and  $t$  to  $\mathcal{U}_i$ .
2. Since  $\mathcal{U}_i$  legitimately received this coin, it is necessary that  $T_l = g^{u_i} h^{r_l}$ ,  $T'_l = g^{r_l} h^{w_l}$ ,  $t_l = g^{a_l} h^{b_l}$  and  $\mathcal{U}_i$  knows the values of  $r_l, w_l, a_l$  and  $b_l$ .  $\mathcal{U}_i$  first computes  $R = \mathcal{H}(T||T'||t||d)$  where  $d$  represents some data related to the spending and next computes a proof of validity of the spent coin, that is, the signature of knowledge:

$$V = PK(\alpha, \beta, \gamma, \delta, \zeta : \\ T_l = g_0^\alpha g_5^\beta \wedge T'_l = g_0^\beta g_5^\zeta \wedge \gamma = \text{Sign}(\alpha, \delta))(S, T_l, T'_l, t_l)$$

This proof is done by using as a commitment for  $T'_l$  the value  $t_l$  and as a challenge the value  $R$ . Consequently, to prove the knowledge of  $r_l$  and  $w_l$  such that  $T'_l = g_0^{r_l} g_5^{w_l}$ ,  $\mathcal{U}_i$  uses  $(t_l, R, (s_r = a_l - Ru_i, s_w = b_l - R w_l))$  as a signature of knowledge (see Section 2.4).

3. The spent coin is represented by  $(S, \pi = (\hat{T}, \pi_0, \dots, \pi_{l+1}))$  where  $\pi_{l+1} = (V, T, T', t, d)$ .

**Deposit and Identify Protocol.** The deposit phase of a coin  $(S, \pi = (\hat{T}, \pi_0, \dots, \pi_l))$ , where  $\pi_i = (V_i, T_i, T'_i, d_i, t_i)$ ,  $0 \leq i \leq l$ , is similar to the one presented in Section 3.2 except that the value  $R$  is computed as  $R = \mathcal{H}(T_l \| T'_l \| t_l \| d_l)$ .

In case of a double-spending detection, the bank  $\mathcal{B}$  has two deposited coins  $C = (S, \pi = (\hat{T}, \pi_0, \pi_1, \dots))$  and  $\tilde{C} = (S, \tilde{\pi} = (\tilde{T}, \tilde{\pi}_0, \tilde{\pi}_1, \dots))$ . If  $\hat{T} \neq \tilde{T}$ , then  $\mathcal{B}$  retrieves  $pk_{\mathcal{U}}$  by computing  $pk_{\mathcal{U}} = (\hat{T}^{\tilde{R}} / \tilde{T}^R)^{1/(\tilde{R}-R)}$ . Else,  $\mathcal{B}$  looks for the minimum value  $k$  such that  $\pi_k \neq \tilde{\pi}_k$ ; this case always happens. Both  $\pi_k$  and  $\tilde{\pi}_k$  are correct and thus both  $V_k$  and  $\tilde{V}_k$  include a proof that  $T_k = \tilde{T}_k$  is well-formed. Moreover, both proofs necessary use the same commitment  $t$ . Using standard technique and the soundness of the proof of knowledge (see Section 2.4),  $\mathcal{B}$  can easily retrieve  $g_0^{u_{k-1}}$  by first retrieving  $r_{k-1}$  and thus, using  $T_{k-1}$ , the identity of the double-spender.

### 4.3 Achieving the Unconditional Anonymity

Due to lack of space, we only give security arguments for the unconditional anonymity property of our scheme. It is unconditionally impossible to learn anything about the user identity from a withdrawal due to the unconditional security of the Pedersen commitment. More precisely, the user identity is embedded twice during a spending protocol.

- In the Pedersen commitment  $T = g^u h^r$  which is unconditionally hiding [12]. Thus, no Shannon information about  $u$  is revealed in  $T$ .
- In the zero-knowledge signature of knowledge  $V$ . The zero-knowledge property of the underlying proof of knowledge is also unconditional. Thus, no Shannon information about  $u$  is revealed in  $V$ .

During the pre-computation phase, the security tag  $\hat{T} = pk_{\mathcal{U}} g_5^{R_0/(t+j+1)}$  (computed as in the first scheme) does not compromise the unconditional anonymity. Indeed, even if  $\mathcal{A}$  knows  $R_0 = \mathcal{H}(r_0, d_0, d'_0)$ , and that for every  $pk_v = g_0^v$ ,  $\mathcal{A}$  can compute  $sk_v = v$ ,  $\mathcal{A}$  does not know neither  $t_0$  nor  $j_0$  and thus  $\mathcal{A}$  cannot determine which public key  $pk_{\mathcal{U}}$  is embedded into  $\hat{T}$ .

This pre-computation phase may introduce some flaws for other security properties, such as the double-spender identification. Indeed,  $\mathcal{A}$  can make the pre-computation twice, one with  $R = \mathcal{H}(T_0 \| T'_0 \| t_0 \| d_0)$  and the other with  $\tilde{R} = \mathcal{H}(\tilde{T}_0 \| \tilde{T}'_0 \| \tilde{t} \| \tilde{d})$ , such that  $R = \tilde{R}$ . However, since the hash function is collision resistant, it is necessary that  $T_0 = \tilde{T}_0$ ,  $T'_0 = \tilde{T}'_0$  and  $t_0 = \tilde{t}_0$ . The value  $T_0$  will be necessary used during the first **Spend** protocol, i.e. either during the pre-computation phase or during an effective spending protocol. Thus,  $\mathcal{A}$  necessary succeeded in faking a proof

of knowledge or forged the CL signature scheme, which happens with negligible probability.

## 5 Conclusion

In this paper, we present two transferable e-cash schemes that improve the efficiency of anonymous transferable e-cash schemes by addressing the problem of decreasing the number of interaction between the bank and users. The first scheme fulfils the computational anonymity property whereas the second one fulfils an unconditional anonymity at the cost of a less efficient result. Moreover, both schemes allow to withdraw efficiently a wallet instead of a coin at a time.

## References

1. M. Bellare, C. Namprempre, D. Pointcheval, and M. Semanko. The One-More-RSA-Inversion Problems and the Security of Chaum's Blind Signature Scheme. *J. Cryptology*, 16(3):185–215, 2003.
2. J. Camenisch, S. Hohenberger, and A. Lysyanskaya. Compact E-Cash. In *EUROCRYPT 2005*, volume 3494 of *LNCS*, pages 302–321, 2005.
3. J. Camenisch and A. Lysyanskaya. Signature Schemes and Anonymous Credentials from Bilinear Maps. In *CRYPTO 2004*, volume 3152 of *LNCS*, pages 56–72, 2004.
4. J. Camenisch and V. Shoup. Practical Verifiable Encryption and Decryption of Discrete Logarithms. In *CRYPTO'03*, volume 2729 of *LNCS*, pages 126–144, 2003.
5. S. Canard, A. Gouget, and E. Hufschmitt. A Handy Multi-coupon System. In *ACNS 2006*, volume 3989 of *LNCS*, pages 66–81, 2006.
6. D. Chaum and T.P. Pedersen. Transferred Cash Grows in Size. In *EUROCRYPT '92*, volume 658 of *LNCS*, pages 390–407, 1992.
7. I. Damgård. Efficient Concurrent Zero-Knowledge in the Auxiliary String Model. In *EUROCRYPT 2000*, pages 418–430, 2000.
8. Y. Dodis and A. Yampolskiy. A Verifiable Random Function with Short Proofs and Keys. In *PKC'05*, pages 416–431, 2005.
9. A. Fiat and A. Shamir. How to Prove Yourself: Practical Solutions to Identification and Signature Problems. In *CRYPTO '86*, volume 263 of *LNCS*, pages 186–194, 1986.
10. M. Girault, G. Poupard, and J. Stern. On the Fly Authentication and Signature Schemes Based on Groups of Unknown Order. *J. Cryptology*, 19(4):463–487, 2006.
11. T. Okamoto and K. Ohta. Disposable Zero-Knowledge Authentications and Their Applications to Untraceable Electronic Cash. In *CRYPTO '89*, volume 435 of *LNCS*, pages 481–496, 1989.
12. T.P. Pedersen. Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing. In *CRYPTO '91*, volume 576 of *LNCS*, pages 129–140, 1991.
13. D. Pointcheval and J. Stern. Security Arguments for Digital Signatures and Blind Signatures. *J. Cryptology*, 13(3):361–396, 2000.
14. C.P. Schnorr. Efficient Identification and Signatures for Smart Cards. In *CRYPTO '89*, pages 239–252, 1989.
15. H. van Antwerpen. Electronic Cash. Master's thesis, CWI, 1990.