ITC 1/47
Journal of Information Technology and Control
Vol. 47 / No. 1 / 2018
pp. 107-117
DOI 10.5755/j01.itc.47.1.18021

A Simple Off-line E-Cash System with Observers

Received 2017/09/22 | Accepted after revision 2018/02/01

http://dx.doi.org/10.5755/j01.itc.47.1.18021

A Simple Off-line E-Cash System with Observers

Eligijus Sakalauskas, Inga Timofejeva, Aleksėjus Michalkovič, Jonas Muleravičius

Department of Applied Mathematics; Kaunas University of Technology; Studentų Str. 50, LT-51368, Kaunas, Lithuania; e-mails: eligijus.sakalauskas@ktu.lt, inga.timofejeva@ktu.edu, aleksejus.michalkovic@ktu.lt, jonas.muleravicius@ktu.edu

Corresponding author: aleksejus.michalkovic@ktu.lt

A simple mobile e-cash system with observers satisfying e-cash divisibility, partial anonymity, off-line payment, transferability and double-spending prevention requirements is presented. The proposed e-cash system is based on two well-known cryptographic primitives, namely ElGamal signature along with Schnorr identification protocols. Therefore, it can be considered simple in the sense of implementation and security considerations. The traditional and elliptic curve realizations of e-money system are presented. The system employs observers, i.e. cryptographic bank chips implemented in customer's payment device (e.g. smart phone) in order to avoid the increase in the size of transferred e-cash data, which is a major flaw of most divisible, anonymous, off-line and transferable e-cash systems. The security of the proposed e-money system is based on discrete logarithm problems in cyclic and elliptic curve groups. The system's security against chosen message attack is provided.

KEYWORDS: E-cash, E-wallet, Observer, ElGamal signature scheme, Schnorr identification scheme, Elliptic curve cryptography.

1. Introduction

The electronic wallet (e-wallet) designed to store and manage electronic cash has gained much popularity in the past decades. Since e-cash is considered the digital analogue of traditional cash it is desired for electronic money to satisfy the following properties:

Anonymity: The customer using his e-cash to pay for a product must remain anonymous against the recipient of the money as well as the bank. The possibility of identifying the identity of the customer must arise only when the money is spent illegitimately.

Unreusability: E-cash cannot be copied or double spent. This implies that e-wallet system has to minimize the risks for forgery and/or provide ways for the identification of a dishonest user.

Unforgeability: Only authorized parties (i.e. the bank) can produce e-cash.

Off-line Payment: The payment transaction must be performed off-line, i.e. no communication with the bank should be necessary during the payment protocol.

Divisibility: E-cash must be divisible, i.e. the customer should be able to divide it into smaller amounts.

Transferability: Received e-cash can be applied for other payments among customers, regardless of whether transactions are on-line or off-line.

Traditional e-cash systems consist of the following protocols: Withdrawal, Payment and Deposit. During Withdrawal protocol, customer receives e-cash from the bank and places it into his e-wallet, implying that the sum of money in customer's bank account is reduced by the sum of withdrawn e-cash. While Payment protocol, customer performs the payment of the sum (not exceeding e-cash he received) to the vendor. During Deposit protocol, vendor increases the balance of e-cash in his e-wallet, or deposits it to the bank.

One of the first e-cash systems introduced by Chaum, Fiat and Naor (CFN) in 1988 was based on cut and cut-and-choose approaches [7, 20]. However, the system was not efficient since the bank had to store $2k+3k^2$ bits (k is bank's secret key) for each Deposit protocol as well as each user's unique identifier $Id_{\mathbf{P}}$ for each Withdrawal protocol while the user and the merchant had to store $2k+4k^2$ and $2k+3k^2$ bits, respectively.

Later, Jones and Higgins developed Mondex e-cash system which used public key cryptography to transfer e-cash off-line [22]. The system was implemented in payment card's microchip and is still used nowadays by MasterCard Inc. However, significant disadvantage of Mondex system is that transactions are not truly anonymous. Unlike pre-paid phone cards, which are also based on smart card technology, the user cannot purchase a Mondex card without revealing his identity [1].

Off-line e-cash system with observers was first mentioned by Brands in [4]. He proposed the idea of the implementation of bank's trustee in purchaser's e-wallet in order to perform payments without connection to the bank. However, the cryptographic security of Brands e-cash system was never proven and hence this system was not activated.

Therefore, a lot of early e-cash systems that attempted to satisfy the main e-wallet properties defined above faced with such problems as the absence of full anonymity, increase of transferred e-cash data, lack of strong security analysis or the complexity of the realization. Nowadays, due to major breakthroughs in computer science as well as the boost in the popularity of electronic cash more e-cash systems dealing with those flaws seem to appear. We will provide a short overview of a few of such systems.

In [10], Eslami et al. presented an untraceable off-line anonymous electronic cash system based on cryptographic techniques such as ElGamal and blind signatures. Eslami and Talebi in [10] achieved the off-line property of e-cash system by the use of an expiration date for e-coins. Since the authors have used ElGamal functions as one of the key elements for the system, the security of e-wallet relied on the discrete logarithm problem and factoring problem.

Zhang et al. [23] presented a transferable optimal-size fair e-cash system with optimal anonymity. One of the goals of the presented system [23] was to eliminate the disadvantage of most already existing transferable e-cash systems which is that the size of coins grows linearly in the number of transfers. The solution implemented by authors was to use the different structure of the coin, specifically, dividing transferred coins into two parts. In order to achieve optimal anonymity, the authors employed Groth-Sahai proofs, the automorphic blind signature and the group blind signature.

Another approach to achieving the transferability of e-cash was proposed in [13]. The presented scheme [13] used Forward-Secure Multi-use Unidirectional Proxy Re-signature Scheme to achieve transferability, without any increase in the size of e-cash after each transfer. The proposed scheme also enabled off-line transactions which enforced user anonymity. The authors also included the Trusted Third Party which was the key element for double spending prevention.

In [16], we proposed an e-wallet system with off-line divisible and anonymous e-cash. The presented system [16] was also fully controlled by bank, thus the prevention of an overpayment and the detection of a dishonest user were provided. This system managed to deal with the problem of the increase of e-cash data during transfers among users by sacrificing honest user's anonymity against bank and off-line deposit.

In [2], Baldimtsi et al. presented an efficient and fully anonymous transferable e-cash scheme without trusted third parties. For the construction of such

e-cash system, the authors used malleable signatures to allow secure and anonymous transfer of the coins. The authors also presented an independent double-spending detection mechanism.

Canard et al. [5, 6] proposed an efficient divisible e-cash system secure in the standard model as opposed to most systems with such properties that were proven secure only in the random oracle model, but had either weak security or complex settings. Presented system [5, 6] was based on a new way of the construction of coins using unique and public global tree structure for all coins. Such an e-cash system uses constant time for withdrawal and payment protocols, while allowing the bank to quickly detect double-spending.

Another practical and secure divisible e-cash system proven secure in random oracle and standard models where the bandwidth of each protocol is constant was presented in [15]. The system [15] also provided withdrawing and spending of an arbitrary value of coins.

In [9], Chen et al. proposed an efficient transferable conditional e-payment system based on restrictive partially blind signature scheme. Since the system [9] did not employ cut-and-choose techniques or complicated knowledge proof protocols it was less complex in the sense of computation and communication.

Pointcheval et al. [17] proposed a first divisible e-cash system without a tree structure that allowed to achieve constant-time complexity with a fairly easy management of coins.

Kang et al. in [12] proposed a new untraceable off-line electronic cash scheme without merchant frauds, anonymity and expiration date faults. The authors also provided a security analysis of the scheme and a double spending detection mechanism.

Baseri et al. [3] proposed an untraceable anonymous unforgeable electronic cash system with double spending prevention constructed on the basis of [10] but without the weaknesses of [10]. In order to prevent faults of the system described in [10], Baseri et al. employed a special construction of e-coin, which contained both the expiration date and the identity of the customer.

Taking into account existing e-cash systems and their problems, we would like to propose an efficient and secure e-cash system based on the implementation of observers and providing e-cash divisibility, off-line payments, transferability, partial anonymity and double spending prevention. Partial anonymity means that the identity of customer will be revealed, if vendor deposits his e-cash in the bank. The main advantage of the proposed system is that e-cash transferred among the users is not growing in size.

The proposed e-cash system is based on the use of Trusted Third Party (TTP) which in this system is impersonated by the bank implementing its cryptographic chip in user's mobile device. Such an idea is known as Fair Offline e-Cash (FOLC).

Since the observer in this system is the chip implemented in user's device, it is necessary to supply the chip with proper cryptographic functions. In [21], we suggested using physical unclonable functions (PUFs, [14]) as a better way of ensuring the suitability of cryptographic functions and the security of e-money system. It was also mentioned in [21] that PUFs allow user to extract a unique unclonable code (UUC) for the chip and to create a unique cryptographic key. Thus, in this paper, we assume that observer chips are supplied with PUFs and the UUC is used as an identifier of the owner of the chip.

We introduce the following actors in our system:

Bruce – the bank. He generates public parameters of our system and supplies users Peg and Victor with their private and public data as well as with their observers (microchips for mobile devices).

Peg (**P**) – the purchaser. She is willing to purchase some goods from the vendor using our e-cash system. Bruce does not trust Peg and hence supplies her with an observer.

Oliver ($\boldsymbol{O_P}$) – an observer implemented in Peg's mobile device. Bruce completely trusts Oliver and generates private and public data for him. Oliver verifies information obtained from Peg and grants her e-cash to spend in case of validity. He also generates vital data, which cannot be altered by Peg.

Victor (**V**) – the vendor. He owns the goods, which Peg is willing to purchase. Bruce does not trust Victor and hence supplies him with an observer.

Olivia ($\boldsymbol{O_V}$) – an observer implemented in Victor's mobile device. Bruce completely trusts Olivia and generates private and public data for her. Olivia verifies information obtained from Victor and deposits e-cash to Victor's e-wallet in case of validity.

Two alternatives of the proposed e-money system are presented. The first one is based on the discrete

logarithm problem (DLP), or ElGamal cryptography, the second one – on elliptic curve discrete logarithm problem (ECDLP). In both cases, it is assumed that the discrete logarithm problem is intractable for security considerations.

The proposed e-cash scheme is based on two well-known cryptographic schemes, namely, Schnorr identification scheme and ElGamal signature scheme and their Elliptic Curve alternatives [19].

2. DLP Approach

Mathematical background of e-cash scheme

To start with, Bruce generates a strong prime p, i.e. $p = 2q + 1$, where q is a prime number, and an element g, satisfying the congruence $g^q \equiv 1 \bmod p$. The practical way to generate this element is to find a generator of the initial group $\boldsymbol{Z}_p$ and square it. The element g can be used to generate a cyclic subgroup $\boldsymbol{G}_q = \left\{ g^i \mid i = \overline{1,q} \right\}$ called a Sylow subgroup. Bruce also selects a hash function H such that $H : \{0,1\}^* \mapsto \boldsymbol{G}_q$.

Assume that Peg is a new client of the bank and is willing to use e-cash service provided by the bank. According to ElGamal signature and Schnorr identification schemes, Bruce generates the following private and public keys for Peg:

$$PrK_{\boldsymbol{P}} = x_P,\ PuK_{\boldsymbol{P}} = \left\{ G, A_P = G^{x_P} \right\}.$$

Bruce also supplies Peg with his trustee Oliver and generates the following data for him:

$$PrK_O = x_O,\ PuK_O = \left\{ G, A_O = G^{x_O}, A_P^{\ id_{\boldsymbol{P}}} \right\},$$

where $1 < x_P, x_O < q - 1$ and $id_{\boldsymbol{P}}$ is the Peg's identificator, i.e. a unique integer assigned to each client of the bank. Note that A_P is a public parameter associated with Peg. Bruce certificates the term $A_P^{\ id_{\boldsymbol{P}}}$.

The signature on the message $m \in \boldsymbol{G}_q$ is computed using ElGamal signature function $Sig_{ElG}^{x}(\ )$, where x denotes the private key of a signer:

$$\Sigma_m = Sig_{ElG}^{x}(m) = \{R, s\} = \\ = \left\{ G^k \bmod p, k^{-1}\left(h(m) - xR\right) \bmod q \right\},$$

where k is a random secret non-zero integer less than q.

The verification of the signature Σ_m on the message m is performed using verification function $Ver_{ElG}^{A}(\ )$, where A is a public key of a signer:

$$Ver_{ElG}^{A}(\Sigma_m, m) = \begin{cases} True, \text{ if } R \in \boldsymbol{G}_q \\ \text{and } A^R R^s = G^{h(m)} \bmod p; \\ False, \text{ otherwise.} \end{cases}$$

Schnorr interactive identification protocol is performed between Peg and Victor and consists of 4 steps:

1. Peg chooses $\xi \in \boldsymbol{Z}_q$ randomly and sends $W = G^{\xi}$ to Victor;
2. Victor sends randomly generated challenge $h \in \boldsymbol{Z}_q$ to Peg;
3. Peg sends the obtained response $r = \xi + xh$ to Victor;
4. Victor accepts if $G^r \equiv WA^h \bmod p$.

Description of cryptographic protocols

Assume Peg intends to purchase some goods from Victor and wants to pay him the sum of m_i in e-cash at the time instance t_i. Peg turns to Oliver to grant her the desired sum and the Withdrawal protocol is executed.

E-cash withdrawal protocol

Peg sends her observer Oliver the sum m_i, she intends to spend, and time instance t_i:

$$\mathbf{P} \longrightarrow \mathbf{O_P} : m_i, t_i\ .$$

Upon receiving data from Peg, Oliver performs the following actions:

- He verifies the correctness of the received time instance t_i and checks if the desired sum is available to spend, i.e.

$$Ver\left(t_i > t_{w0}\right); \\ Ver\left(m_i < m_{max}^{\mathbf{P}}\right),$$

where t_{w0} denotes time instance of the last withdrawal and $m_{max}^{\mathbf{P}}$ is the currently available sum in e-wallet.

- Oliver generates random integers $\xi_i^{(1)}, \xi_i^{(2)} \in \boldsymbol{Z}_q$ and computes Schnorr identification protocol

values $W_i^{(1)} = G^{\xi_i^{(1)}}$ and $W_i^{(2)} = G^{\xi_i^{(2)}}$.

– He then computes values $n_i^{(1)}, n_i^{(2)}, P_i^{(1)}, P_i^{(2)}$ and signs on values $P_i^{(1)}, P_i^{(2)}, A_P^{n_i^{(1)}}$:

$$
\begin{aligned}
n_i^{(1)} &= m_i \,||\, t_i;\\
n_i^{(2)} &= id_P \cdot n_i^{(1)};\\
P_i^{(1)} &= A_P^{N_i^{(1)}} \cdot W_i^{(1)};\\
P_i^{(2)} &= A_P^{N_i^{(2)}} \cdot W_i^{(2)};\\
\Sigma_i^{(1)} &= Sig_{ElG}^{x_O}\left(P_i^{(1)}\right);\\
\Sigma_i^{(2)} &= Sig_{ElG}^{x_O}\left(P_i^{(2)}\right);\\
\Sigma_i^{(3)} &= Sig_{ElG}^{x_O}\left(A_P^{n_i^{(1)}}\right),
\end{aligned}
$$

where $||$ denotes the concatenation of the sum m_i and time instance t_i. The result $n_i^{(1)}$ is represented by a single integer.

– Oliver saves the received time instance t_i as the time of the last withdrawal and subtracts the received sum from the amount of money in the Peg's e-wallet:

$$
\begin{aligned}
t_{w0} &\leftarrow t_i;\\
m_{max}^{\mathbf{P}} &\leftarrow m_{max}^{\mathbf{P}} - m_i.
\end{aligned}
$$

– Finally, Oliver sends the following data to Peg:

$$
\mathbf{O_P} \longrightarrow \mathbf{P}: \begin{array}{l} \xi_i^{(1)}, \xi_i^{(2)}, W_i^{(1)}, W_i^{(2)},\\ n_i^{(1)}, n_i^{(2)}, \Sigma_i^{(1)}, \Sigma_i^{(2)}, \Sigma_i^{(3)}. \end{array}
$$

After the e-cash Withdrawal protocol, Payment protocol can be executed.

Payment protocol

Schnorr interactive identification protocol is embedded into the payment protocol in order for Peg to prove her identity to Victor.

First of all, Peg sends Victor the payment sum m_i, she intends to spend, and time instance t_i along with signatures $\Sigma_i^{(1)}, \Sigma_i^{(2)}, \Sigma_i^{(3)}$ received from Oliver, and Schnorr protocol values $W_i^{(1)}, W_i^{(2)}$:

$$
\mathbf{P} \longrightarrow \mathbf{V}: m_i \,||\, t_i, \Sigma_i^{(1)}, \Sigma_i^{(2)}, \Sigma_i^{(3)}, W_i^{(1)}, W_i^{(2)}.
$$

Victor verifies correctness of the received time instance t_i, checks if the received sum is equal to the actual price m_i he is expected to receive and verifies validity of all the signatures, i.e.

$$
\begin{aligned}
&Ver\left(t_i > t_{p0}\right);\\
&Ver\left(m = m_i\right);\\
&A_{n_1} = A_P^{m_i || t_i};\\
&Ver_{ElG}^{A_O}\left(A_{n_1}, \Sigma_i^{(3)}\right);\\
&\tilde{P}_i^{(1)} = A_{n_1} \cdot W_i^{(1)};\\
&Ver_{ElG}^{A_O}\left(\tilde{P}_i^{(1)}, \Sigma_i^{(1)}\right);\\
&\tilde{P}_i^{(2)} = A_p^{id_P} \cdot A_{n_1} \cdot W_i^{(2)};\\
&Ver_{ElG}^{A_O}\left(\tilde{P}_i^{(2)}, \Sigma_i^{(2)}\right);
\end{aligned}
$$

where t_{p0} is the time instance of the last payment.

Victor wants to be sure that the user he is communicating with is Peg and hence initiates Schnorr identification protocol by sending randomly selected challenge $h_i \in \boldsymbol{Z}_q$ to her:

$$
\mathbf{V} \longrightarrow \mathbf{P}: h_i
$$

Upon receiving the challenge, Peg computes Schnorr protocol values $r_i^{(1)}, r_i^{(2)}$ and sends them to Victor:

$$
\begin{aligned}
r_i^{(1)} &= h_i \cdot x \cdot n_i^{(1)} + \xi_i^{(1)};\\
r_i^{(2)} &= h_i \cdot x \cdot n_i^{(2)} + \xi_i^{(2)};\\
\mathbf{P} &\longrightarrow \mathbf{V}: r_i^{(1)}, r_i^{(2)}.
\end{aligned}
$$

Victor verifies the following:

$$
\begin{aligned}
&Ver\left(G^{r_i^{(1)}} \cdot \left(\tilde{P}_i^{(1)}\left(W_i^{(1)}\right)^{-1}\right)^{-h_i} = W_i^{(1)}\right);\\
&Ver\left(G^{r_i^{(2)}} \cdot \left(\tilde{P}_i^{(2)}\left(W_i^{(2)}\right)^{-1}\right)^{-h_i} = W_i^{(2)}\right).
\end{aligned}
$$

The above verification equations hold since:

$$
\begin{aligned}
G^{r_i^{(1)}} \cdot \left(\tilde{P}_i^{(1)}\left(W_i^{(1)}\right)^{-1}\right)^{-h_i} &= G^{h_i \cdot x_P \cdot n_i^{(1)} + \xi_i^{(1)}} \cdot A_P^{-n_i^{(1)} h_i} =\\
&= G^{h_i \cdot x_P \cdot n_i^{(1)} + \xi_i^{(1)}} \cdot G^{-x_P n_i^{(1)} h_i} = W_i^{(1)};\\
G^{r_i^{(2)}} \cdot \left(\tilde{P}_i^{(2)}\left(W_i^{(2)}\right)^{-1}\right)^{-h_i} &= G^{h_i \cdot x_P \cdot n_i^{(2)} + \xi_i^{(2)}} \cdot A_P^{-n_i^{(2)} h_i} =\\
&= G^{h_i \cdot x_P \cdot n_i^{(2)} + \xi_i^{(2)}} \cdot G^{-x_P n_i^{(2)} h_i} = W_i^{(2)}.
\end{aligned}
$$

Victor saves the received time as the time of the last payment:

$$t_{p0} \leftarrow t_i;$$

If all the verifications Victor performed are successful, e-cash Deposit protocol can be performed.

E-cash deposit protocol

Victor sends his observer Olivia the following data received from Peg:

$$\mathbf{V} \longrightarrow \mathbf{O}_{\mathbf{V}} : m_i \,||\, t_i, \Sigma_i^{(1)}, \Sigma_i^{(2)}, \Sigma_i^{(3)}, W_i^{(1)}, W_i^{(2)}.$$

Upon receiving the data, Olivia verifies correctness of the received time instance t_i and validity of all the signatures:

$$\begin{aligned} &Ver\left(t_i > t_{d0}\right);\\ &A_{n_1} = A_P{}^{m_i||t_i};\\ &Ver_{ElG}^{A_O}\left(A_{n_1}, \Sigma_i^{(3)}\right);\\ &\tilde{P}_i^{(1)} = A_{n_1} \cdot W_i^{(1)};\\ &Ver_{ElG}^{A_O}\left(\tilde{P}_i^{(1)}, \Sigma_i^{(1)}\right);\\ &\tilde{P}_i^{(2)} = A_P^{id_P} \cdot A_{n_1} \cdot W_i^{(2)};\\ &Ver_{ElG}^{A_O}\left(\tilde{P}_i^{(2)}, \Sigma_i^{(2)}\right); \end{aligned}$$

where t_{d0} is the time instance of the last deposit.

Olivia saves the received time as the time of the last deposit and adds the received sum m_i to the total amount of e-cash $m_{max}^{\mathbf{V}}$ in the Victor's e-wallet:

$$\begin{aligned} t_{d0} &\leftarrow t_i;\\ m_{max}^{\mathbf{V}} &\leftarrow m_{max}^{\mathbf{V}} + m_i. \end{aligned}$$

Double spending prevention

In the case of double spending, Peg's unique identification number id_P can be revealed as explained below.

Since, Peg spent the same sum of money twice, she had to send Victor the following values:

$$\begin{aligned} r_i^{(1)} &= h_i \cdot x_P \cdot n_i^{(1)} + \xi_i^{(1)};\\ r_i^{(2)} &= h_i \cdot x_P \cdot n_i^{(2)} + \xi_i^{(2)};\\ r'^{(1)}_i &= h'_i \cdot x_P \cdot n_i^{(1)} + \xi_i^{(1)};\\ r'^{(2)}_i &= h'_i \cdot x_P \cdot n_i^{(2)} + \xi_i^{(2)}. \end{aligned}$$

where h_i and h'_i are random Schnorr protocol values generated by Victor during the first and the second payment protocols, respectively.

Then Peg's identity id_P can be computed in the following way:

$$\frac{r_i^{(2)} - r'^{(2)}_i}{r_i^{(1)} - r'^{(1)}_i} = \frac{\left(h_i - h'_i\right) \cdot x_P \cdot n_i^{(2)}}{\left(h_i - h'_i\right) \cdot x_P \cdot n_i^{(1)}} = \frac{id_P n_i^{(1)}}{n_i^{(1)}} = id_P.$$

It is important to note that the latter identity is valid, since all the actions are performed prime modulo q, and hence a non-zero element $r_i^{(1)} - r'^{(1)}_i$ is invertible since the algebraic structure $\boldsymbol{Z}_q$ is a field.

3. ECDLP Approach

Mathematical background of e-cash scheme

To start with, Bruce generates a prime p and constants a, b (positive integers satisfying condition $4a^3 + 27b^2 \neq 0$), that are associated with an elliptic curve $E_p(a,b)$ over the Galois Field F_p. We will denote the prime order of the elliptic curve by n. Next, Bruce determines a generator point G such that the multiples kG of the generator point G are (for $1 \leq k \leq n-1$) including point O located at infinity. Bruce also selects a hash function h such that $h : \{0,1\}^* \mapsto F_n$.

Assume that Peg is a new client of the bank and is willing to use e-cash service provided by the bank. According to ElGamal signature and Schnorr identification schemes, Bruce generates the following private and public keys for Peg:

$$\begin{aligned} &PrK_P = x_P,\\ &PuK_P = \left\{G, A_P = x_P \cdot G\right\} \end{aligned}$$

Bruce also supplies Peg with his trustee Oliver and generates the following data for him:

$$\begin{aligned} &PrK_O = x_O,\\ &PuK_O = \left\{G, A_O = x_O \cdot G, id_P \cdot A_P\right\} \end{aligned}$$

where $1 < x_P, x_O < n-1$ and id_P is the Peg's identifier, i.e. a unique integer assigned to each client of the bank. Note that A_P is a public parameter associated with Peg. Bruce certificates the term $id_P \cdot A_O$.

The signature on the message $m \in F_p$ is computed using ElGamal signature function $Sig^x_{ECElG}(\ )$, where x denotes the private key of a signer:

$$\begin{aligned}\Sigma_m &= Sig^x_{ECElG}(m) = \\ &\{R=(x_R,y_R),s\} = \\ &= \left\{k\cdot G, k^{-1}\left(h\cdot m + (x_R \bmod n)\cdot x\right) \bmod n\right\},\end{aligned}$$

where k is a random secret non-zero integer $k \in [1, n-1]$.

The verification of the signature Σ_m on the message m is performed using verification function $Ver^A_{ECElG}(\ )$, where A is a public key of a signer:

$$Ver^A_{ECElG}(\Sigma_m, m) = \begin{cases} True, \text{ if } [s \in [1,n-1], \\ R \in E(F_q), s\cdot R = h\cdot m\cdot G + k\cdot A]; \\ False, \text{ otherwise.}\end{cases}$$

Schnorr interactive identification protocol is performed between Peg and Victor and consists of 4 steps:

1. Peg chooses $\xi \in [1,n]$ randomly and sends $W = \xi \cdot G$ to Victor;
2. Victor sends randomly generated challenge $h \in [1,n]$ to Peg;
3. Peg sends the obtained response $r = \xi + x\cdot h$ to Victor;
4. Victor accepts if $r\cdot G \equiv W + h\cdot A \bmod n$.

Description of cryptographic protocols

Assume Peg intends to purchase some goods from Victor and wants to pay him the sum of m_i in e-cash at the time instance t_i. Peg turns to Oliver to grant her the desired sum and the Withdrawal protocol is executed.

E-cash withdrawal protocol

Peg sends her observer Oliver the sum m_i, she intends to spend, and time instance t_i:

$$\mathbf{P} \longrightarrow \mathbf{O_P} : m_i, t_i$$

Upon receiving data from Peg, Oliver performs the following actions:

- He verifies the correctness of the received time instance t_i and checks if the desired sum is available to spend, i.e.

$$\begin{aligned} &Ver(t_i > t_{w0}); \\ &Ver\left(m_i < m^{\mathbf{P}}_{max}\right),\end{aligned}$$

where t_{w0} denotes time instance of the last withdrawal and $m^{\mathbf{P}}_{max}$ is the currently available sum in e-wallet.

- Oliver generates random integers $\xi^{(1)}_i, \xi^{(2)}_i \in [1,n]$ and computes Schnorr identification protocol values $W^{(1)}_i = \xi^{(1)}_i \cdot G$, $W^{(2)}_i = \xi^{(2)}_i \cdot G$.
- He then computes values $n^{(1)}_i, n^{(2)}_i, P^{(1)}_i, P^{(2)}_i$ and signs on values $P^{(1)}_i, P^{(2)}_i, n^{(1)}_i \cdot A_P$:

$$\begin{aligned} n^{(1)}_i &= m_i \,||\, t_i; \\ n^{(2)}_i &= id_P + n^{(1)}_i; \\ P^{(1)}_i &= n^{(1)}_i \cdot A_P + W^{(1)}_i; \\ P^{(2)}_i &= n^{(2)}_i \cdot A_P + W^{(2)}_i; \\ \Sigma^{(1)}_i &= Sig^{x_O}_{ECElG}\left(P^{(1)}_i\right); \\ \Sigma^{(2)}_i &= Sig^{x_O}_{ECElG}\left(P^{(2)}_i\right); \\ \Sigma^{(3)}_i &= Sig^{x_O}_{ECElG}\left(n^{(1)}_i \cdot A_P\right),\end{aligned}$$

where $||$ denotes the concatenation of the sum m_i and time instance t_i. The result $n^{(1)}_i$ is represented by a single integer.

- Oliver saves the received time instance t_i as the time of the last withdrawal and subtracts the received sum from the amount of money in the Peg's e-wallet:

$$\begin{aligned} t_{w0} &\leftarrow t_i; \\ m^{\mathbf{P}}_{max} &\leftarrow m^{\mathbf{P}}_{max} - m_i.\end{aligned}$$

- Finally, Oliver sends the following data to Peg:

$$\mathbf{O_P} \longrightarrow \mathbf{P}: \begin{matrix} \xi^{(1)}_i, \xi^{(2)}_i, W^{(1)}_i, W^{(2)}_i, \\ n^{(1)}_i, n^{(2)}_i, \Sigma^{(1)}_i, \Sigma^{(2)}_i, \Sigma^{(3)}_i. \end{matrix}$$

After the e-cash Withdrawal protocol, Payment protocol can be executed.

Payment protocol

Schnorr interactive identification protocol is embedded into the payment protocol in order for Peg to

prove her identity to Victor.

First of all, Peg sends Victor the payment sum m_i, she intends to spend, and time instance t_i along with signatures $\Sigma_i^{(1)}, \Sigma_i^{(2)}, \Sigma_i^{(3)}$ received from Oliver, and Schnorr protocol values $W_i^{(1)}, W_i^{(2)}$:

$$\mathbf{P} \longrightarrow \mathbf{V} : m_i \,||\, t_i, \Sigma_i^{(1)}, \Sigma_i^{(2)}, \Sigma_i^{(3)}, W_i^{(1)}, W_i^{(2)}$$

Victor verifies correctness of the received time instance t_i, checks if the received sum m_i is equal to the actual price m he is expected to receive and verifies validity of all the signatures, i.e.:

$$\begin{aligned}
&Ver\left(t_i > t_{p0}\right);\\
&Ver\left(m = m_i\right);\\
&\tilde{A}_{n_1} = m_i \,||\, t_i \cdot A_P;\\
&Ver_{ECElG}^{A_O}\left(\tilde{A}_{n_1}, \Sigma_i^{(3)}\right);\\
&\tilde{P}_i^{(1)} = \tilde{A}_{n_1} + W_i^{(1)};\\
&Ver_{ECElG}^{A_O}\left(\tilde{P}_i^{(1)}, \Sigma_i^{(1)}\right);\\
&\tilde{P}_i^{(2)} = id_P \cdot A_P + \tilde{A}_{n_1} + W_i^{(2)};\\
&Ver_{ECElG}^{A_O}\left(\tilde{P}_i^{(2)}, \Sigma_i^{(2)}\right);
\end{aligned}$$

where t_{p0} is the time instance of the last payment.

Victor wants to be sure that the user he is communicating with is Peg and hence initiates Schnorr identification protocol by sending randomly selected challenge $h_i \in [1, n]$ to her:

$$\mathbf{V} \longrightarrow \mathbf{P} : h_i$$

Upon receiving the challenge, Peg computes Schnorr protocol values $r_i^{(1)}, r_i^{(2)}$ and sends them to Victor:

$$\begin{aligned}
&r_i^{(1)} = h_i \cdot x_P \cdot n_i^{(1)} + \xi_i^{(1)};\\
&r_i^{(2)} = h_i \cdot x_P \cdot n_i^{(2)} + \xi_i^{(2)};\\
&\mathbf{P} \longrightarrow \mathbf{V} : r_i^{(1)}, r_i^{(2)}.
\end{aligned}$$

Victor verifies the following:

$$\begin{aligned}
&Ver\left(G \cdot r_i^{(1)} + \left(\tilde{P}_i^{(1)} - W_i^{(1)}\right) \cdot (-h_i) = W_i^{(1)}\right);\\
&Ver\left(G \cdot r_i^{(2)} + \left(\tilde{P}_i^{(2)} - W_i^{(2)}\right) \cdot (-h_i) = W_i^{(2)}\right).
\end{aligned}$$

The above verification equations hold since:

$$\begin{aligned}
&r_i^{(1)} \cdot G + (-h_i) \cdot \left(\tilde{P}_i^{(1)} - W_i^{(1)}\right) =\\
&= (h_i \cdot x_P \cdot n_i^{(1)} + \xi_i^{(1)}) \cdot G + (-h_i) \cdot A_{n_1} =\\
&= h_i \cdot x_P \cdot n_i^{(1)} \cdot G + \xi_i^{(1)} \cdot G - h_i \cdot x_P \cdot n_i^{(1)} \cdot G = W_i^{(1)};\\
&r_i^{(2)} \cdot G + (-h_i) \cdot \left(\tilde{P}_i^{(2)} - W_i^{(2)}\right) =\\
&= (h_i \cdot x_P \cdot n_i^{(2)} + \xi_i^{(2)}) \cdot G + (-h_i) \cdot (id_P \cdot A_P + A_{n_1}) =\\
&= h_i \cdot x_P \cdot n_i^{(2)} \cdot G + \xi_i^{(2)} \cdot G - h_i \cdot x_P \cdot n_i^{(2)} \cdot G = W_i^{(2)}
\end{aligned}$$

Victor saves the received time as the time of the last payment:

$$t_{p0} \leftarrow t_i;$$

If all the verifications Victor performed are successful, e-cash Deposit protocol can be performed.

E-cash deposit protocol

Victor sends his observer Olivia the following data received from Peg:

$$\mathbf{V} \longrightarrow \mathbf{O}_\mathbf{V} : m_i \,||\, t_i, \Sigma_i^{(1)}, \Sigma_i^{(2)}, \Sigma_i^{(3)}, W_i^{(1)}, W_i^{(2)}.$$

Upon receiving the data, Olivia verifies correctness of the received time instance t_i and validity of all the signatures:

$$\begin{aligned}
&Ver\left(t_i > t_{d0}\right);\\
&\tilde{A}_{n_1} = m_i \,||\, t_i \cdot A_P;\\
&Ver_{ECElG}^{A_O}\left(\tilde{A}_{n_1}, \Sigma_i^{(3)}\right);\\
&\tilde{P}_i^{(1)} = \tilde{A}_{n_1} + W_i^{(1)};\\
&Ver_{ECElG}^{A_O}\left(\tilde{P}_i^{(1)}, \Sigma_i^{(1)}\right);\\
&\tilde{P}_i^{(2)} = id_P \cdot A_P + \tilde{A}_{n_1} + W_i^{(2)};\\
&Ver_{ECElG}^{A_O}\left(\tilde{P}_i^{(2)}, \Sigma_i^{(2)}\right);
\end{aligned}$$

where t_{d0} is the time instance of the last deposit.

Olivia saves the received time as the time of the last deposit and adds the received sum m_i to the total amount of e-cash $m_{max}^{\mathbf{V}}$ in the Victor's e-wallet:

$$\begin{aligned}
&t_{d0} \leftarrow t_i;\\
&m_{max}^{\mathbf{V}} \leftarrow m_{max}^{\mathbf{V}} + m_i.
\end{aligned}$$

Double spending prevention

In the case of double spending, Peg's unique identification number id_P can be revealed as explained below.

Since Peg spent the same sum of money twice, she had to send Victor the following values:

$$r_i^{(1)} = h_i \cdot x_P \cdot n_i^{(1)} + \xi_i^{(1)};$$
$$r_i^{(2)} = h_i \cdot x_P \cdot n_i^{(2)} + \xi_i^{(2)};$$

$$r'^{(1)}_i = h'_i \cdot x_P \cdot n_i^{(1)} + \xi_i^{(1)};$$
$$r'^{(2)}_i = h'_i \cdot x_P \cdot n_i^{(2)} + \xi_i^{(2)};$$

where h_i and h'_i are random Schnorr protocol values generated by Victor during the first and the second payment protocols, respectively.

Then Peg's identity id_P can be computed in the following way:

$$\left(\frac{r_i^{(2)} - r'^{(2)}_i}{r_i^{(1)} - r'^{(1)}_i} - 1\right) \cdot n_i^{(1)} =$$
$$= \left(\frac{(h_i - h'_i) \cdot x_P \cdot n_i^{(2)}}{(h_i - h'_i) \cdot x_P \cdot n_i^{(1)}} - 1\right) \cdot n_i^{(1)} =$$
$$= \left(\frac{id_p + n_i^{(1)}}{n_i^{(1)}} - 1\right) \cdot n_i^{(1)} = \frac{id_p}{n_i^{(1)}} \cdot n_i^{(1)} = id_p$$

4. Security Analysis of the Proposed E-cash System

This section will provide only the proof of the security of the DLP version of the proposed system, since the security of the ECDLP alternative can be proven analogously.

The aim of this section is to show that the proposed scheme cannot be attacked by using a chosen message. Our analysis is based on Theorem 7 of [8], i.e. we have to prove the perfect *d*-wise decorrelation of our scheme.

We start by revising the following known facts:

Proposition 1. Let *G* be a generator of the cyclic group $\boldsymbol{G}_q$ of cardinality *q* and let $x \in \boldsymbol{Z}_q$ be chosen at random. The element G^x has the same distribution in $\boldsymbol{G}_q$ as *x* has in $\boldsymbol{Z}_q$.

Proposition 2. Let z_0 be an arbitrary element of the multiplicative cyclic group $\boldsymbol{G}_q$. Choosing at random $z_1 \in \boldsymbol{Z}_q$ and setting $z = z_0 \cdot z_1$ gives the same distribution for *z* as choosing random *z*.

Corollary 3. If G_1 and G_2 are in $\boldsymbol{G}_q$ and if $x, y \in \boldsymbol{Z}_q$ are chosen uniformly at random, then the element *z* being computed by the expression

$$z = G_1^x \cdot G_2^y$$

is uniformly distributed in $\boldsymbol{G}_q$.

To prove the resistance of our scheme to chosen message attack (CMA), we also rely on the following facts:

Proposition 4. Let z_0 be an arbitrary element of the additive cyclic group $\boldsymbol{G}_q$. Choosing at random $z_1 \in \boldsymbol{Z}_q$ and setting $z = z_0 \cdot z_1$ gives the same distribution for *z* as choosing random *z*.

Corollary 5. Let *a*, *b* and *c* be three uniformly distributed random elements of the field of integers $\boldsymbol{Z}_q$. The element $a + bc$ is uniformly distributed in $\boldsymbol{Z}_q$.

Due to these facts at Step 4 of Schnorr identification both elements G^r and WA^h are distributed uniformly in $\boldsymbol{G}_q$ and hence both functions $f_1(r) = g^r$ and $f_2(W, h) = WA^h$ provide perfect 1-wise decorrelation. It is clear that an element *w* has the uniform distribution in $\boldsymbol{G}_q$ due to uniform distribution of ξ.

Next we consider the ElGamal signature. It is important to note that the version we are using is a modification of the original scheme and uses the hash of the message rather than a message itself. It was previously shown in [11] that the original scheme suggested by ElGamal was forgeable under CMA. Due to this fact Poincheval and Stern suggested a modification of the original scheme. The authors proved that the modified version of ElGamal digital signature is secure against adaptive CMA in [18].

Hence the security of our scheme against CMA relies on the following facts:

- Withdrawal protocol is secure since random variables $n_i^{(1)}, n_i^{(2)}, P_i^{(1)}, P_i^{(2)}$ are uniformly distributed either is $\boldsymbol{Z}_q$ (in case of $n_i^{(1)}, n_i^{(2)}$) or in $\boldsymbol{G}_q$ (in case of $P_i^{(1)}, P_i^{(2)}$) due to the facts, presented above. Hence these variables as functions have perfect 1-wise decorrelation. The signatures are secure due to [18].
- Payment protocol is secure since random variables $r_i^{(1)}, r_i^{(2)}$ are uniformly distributed in $\boldsymbol{Z}_q$ and

therefore have perfect 1-wise decorrelation.

- Deposit protocol is secure since all the random variables, involved in the protocol are uniformly distributed whereas digital signatures are secure due to [18].

Note, however, that neither the original ElGamal digital signature nor the modified version provide a uniform distribution for parameter $s = k^{-1}\left(h(m) - xR\right) \bmod q$ since the parameter $R = G^k \bmod p$ is not uniformly distributed in $\boldsymbol{G}_q$.

Assume that Peg performed the payment protocol correctly, i.e. Victor received the correct data presented above.

Proposition 6. No double spending by forgery of the data sent by Peg is possible.

Proof. The claim of the proposition is valid due to the fact that signatures are secure against chosen message attack. Hence the data cannot be forged since Peg has no access to Oliver's private key x_O, i.e. signatures $\Sigma_i^{(1)} = Sig_{ElG}^{x_O}\left(P_i^{(1)}\right)$, $\Sigma_i^{(2)} = Sig_{ElG}^{x_O}\left(P_i^{(2)}\right)$ and $\Sigma_i^{(3)} = Sig_{ElG}^{x_O}\left(A_P{}^{n_i^{(1)}}\right)$ as well as data signed have to remain intact. Since A_P is a generator of the group $\boldsymbol{G}_q$ no forgery of $n_i^{(1)}$ is possible, which also implies that the time instance t_i cannot be altered since the price of the desired good m_i cannot be affected by Peg. Furthermore, forging $n_i^{(2)}$ is impossible due to the following facts:

- $n_i^{(1)}$ and $n_i^{(2)}$ are mathematically linked;
- the public key $A_P{}^{id_P}$ is certificated and hence id_P cannot be forged;
- $\boldsymbol{Z}_q$ is a field and hence $n_i^{(1)}$ is invertible.

Unforged values of $n_i^{(1)}, n_i^{(2)}, P_i^{(1)}, P_i^{(2)}$ now imply the correct values of $W_i^{(1)}, W_i^{(2)}$ since $\boldsymbol{G}_q$ is a group and hence $A_P{}^{n_i^{(1)}}$ and $A_P{}^{n_i^{(2)}}$ are both invertible.

Let us now assume that Peg and Victor successfully executed all the protocols presented above.

Proposition 7. No forgery of the data sent by Peg is possible by Victor during the Deposit protocol.

Proof. Victor cannot forge any of the signatures received since private information from Peg's observer Oliver is unavailable to him. Furthermore, Victor cannot change neither the sum m_i nor the time instance t_i due to the structure of the data sent, i.e. by changing any of the components the concatenation result is affected. The correct values of m_i and t_i now imply the correct values of $W_i^{(1)}, W_i^{(2)}$ since $A_P{}^{n_i^{(1)}}$ is invertible and $A_P{}^{id_P}$ is certificated.

5. Conclusions

- The proposed e-cash system satisfies divisibility, partial anonymity, off-line payment, transferability and double-spending prevention requirements.
- Presented system is based on provable secure cryptographic primitives such as Schnorr identification and modified ElGamal e-signature and their Elliptic Curve alternatives. Thus, the security of the system relies on the security of these cryptographic primitives. In both cases, double spending prevention algorithm is presented.
- The use of well-known classical cryptographic protocols results in a simple and straightforward realization of the system.
- The system employs observers, i.e. cryptographic bank chips implemented in customer's payment device in order to satisfy off-line payment requirement and avoid the increase in the size of transferred e-cash data.
- The proposed e-wallet system can be implemented in Elliptic Curves as shown in the paper, thus higher performance and better security can be achieved.
- Due to algebraic properties of Schnorr identification and modified ElGamal e-signature protocols, it is possible to define basic parameters of the proposed system in such a way that would result in e-cash system's security against chosen message attack - CMA.
- Presented system is partially anonymous, i.e. the anonymity is provided against the vendor. However, in case of double spending, the identity of malicious purchaser is revealed. Hence, the purchaser cannot forge any data in order to perform double spending and remain undetected. Analogously, the vendor cannot perform double spending of the received e-cash during deposit protocol as well.

References

1. Abrazhevich, D. Electronic Payment Systems: A User-Centered Perspective and Interaction Design. Dennis Abrazhevich, 2004.
2. Baldimtsi, F., Chase, M., Fuchsbauer, G., Kohlweiss, M. Anonymous Transferable E-Cash. In Public Key Cryptography, 2015, 101-124.
3. Baseri, Y., Takhtaei, B., Mohajeri, J. Secure Untraceable Off-Line Electronic Cash System. Scientia Iranica, 2013, 20(3), 637-646.
4. Brands, S. Untraceable Off-Line Cash in Wallet With Observers. In Annual International Cryptology Conference, Springer, Berlin, Heidelberg, 1993, 302-318.
5. Canard, S., Pointcheval, D., Sanders, O., Traoré, J. Divisible E-Cash Made Practical. In IACR International Workshop on Public Key Cryptography, Springer, Berlin, Heidelberg, 2015, 77-100. https://doi.org/10.1007/978-3-662-46447-2_4
6. Canard, S., Pointcheval, D., Sanders, O., Traoré, J. Scalable Divisible E-Cash. In International Conference on Applied Cryptography and Network Security, Springer, Cham, 2015, 287-306. https://doi.org/10.1007/978-3-319-28166-7_14
7. Chaum, D., Fiat, A., Naor, M. Untraceable Electronic Cash. In Proceedings on Advances in cryptology, Springer-Verlag New York, Inc., 1990, 319-327. https://doi.org/10.1007/0-387-34799-2_25
8. Chaum, D., Pedersen, T. P. Transferred Cash Grows in Size. In Workshop on the Theory and Application of of Cryptographic Techniques, Springer, Berlin, Heidelberg, 1992, 390-407.
9. Chen, X., Li, J., Ma, J., Lou, W., Wong, D. S. New and Efficient Conditional E-Payment Systems with Transferability. Future Generation Computer Systems, 2014, 37, 252-258. https://doi.org/10.1016/j.future.2013.07.015
10. Eslami, Z., Talebi, M. A New Untraceable Off-Line Electronic Cash System. Electronic Commerce Research and Applications, 2011, 10(1), 59-66. https://doi.org/10.1016/j.elerap.2010.08.002
11. Goldwasser, S., Micali, S., Rivest, R. L. A Digital Signature Scheme Secure Against Adaptive Chosen-Message Attacks. SIAM Journal on Computing, 1988, 17(2), 281-308. https://doi.org/10.1137/0217017
12. Kang, B., Xu, D. An Untraceable Off-Line Electronic Cash Scheme Without Merchant Frauds. International Journal of Hybrid Information Technology, 2016, 9(1), 431-442. https://doi.org/10.14257/ijhit.2016.9.1.38
13. Kavitha, M., Sunitha, N. R., Amberker, B. B. A New Transferable Digital Cash Protocol Using Proxy Re-signature Scheme. Computational Intelligence and Information Technology, 2011, 194-199. https://doi.org/10.1007/978-3-642-25734-6_30
14. Maes, R. Physically Unclonable Functions. Springer-Verlag Berlin An, 2016.
15. Märtens, P. Practical Divisible E-Cash. IACR Cryptology ePrint Archive, 2015, 318.
16. Muleravičius, J., Sakalauskas, E., Timofejeva, I. On Methodology of E-wallet Construction for Partially Off-line Payment System. In International Conference on Information and Software Technologies, Springer International Publishing, 2016, 753-765. https://doi.org/10.1007/978-3-319-46254-7_61
17. Pointcheval, D., Sanders, O., Traoré, J. Cut Down the Tree to Achieve Constant Complexity in Divisible E-Cash. In IACR International Workshop on Public Key Cryptography, Springer, Berlin, Heidelberg, 2017, 61-90. https://doi.org/10.1007/978-3-662-54365-8_4
18. Pointcheval, D., Stern, J. Security Arguments for Digital Signatures and Blind Signatures. Journal of Cryptology, 2000, 13(3), 361-396. https://doi.org/10.1007/s001450010003
19. Rabah, K. Elliptic Curve Elgamal Encryption and Signature Schemes. Information Technology Journal, 2005, 4(3), 299-306. https://doi.org/10.3923/itj.2005.299.306
20. Rabin, M. Foundations of Secure Computations, Chapter "Digitalized Signatures". Academic Press, 1978, 16, 155-166.
21. Sakalauskas, E., Muleravicius, J., Timofejeva, I. Computational Resources for Mobile E-wallet System with Observers. Electronics, IEEE, 2017, 1-5.
22. Srivastava, L., Mansell, R. Electronic Cash and the Innovation Process: A Use Paradigm. University of Sussex, SPRU, 1998.
23. Zhang, J., Huo, L., Liu, X., Sui, C., Li, Z., Ma, J. Transferable Optimal-size Fair E-cash with Optimal Anonymity. In 2015 International Symposium on Theoretical Aspects of Software Engineering (TASE), IEEE, 2015, 139-142. https://doi.org/10.1109/TASE.2015.12