On Methodology of E-wallet Construction for Partially Off-line Payment System

Jonas Mulerav̌cius(✉), Eligijus Sakalauskas, and Inga Timofejeva

Department of Applied Mathematics, Kaunas University of Technology,
Studentu Street 50, Kaunas, Lithuania
{jonas.muleravicius, inga.timofejeva}@ktu.edu,
eligijus.sakalauskas@ktu.lt

Abstract. We propose a methodology for the construction of e-wallet with off-line divisible e-cash, with such properties as anonymity against vendor and full traceability from bank. Since this system is fully controlled by bank from the issuance of e-money to e-cash deposit, the prevention of an overpayment and the detection of a dishonest user are provided.

Proposed system prevents the serious drawback of existing anonymous and divisible e-cash systems noticed by Chaum, namely the growth of the amount of information during e-cash transfers among the users. The prevention of this issue is achieved by sacrificing such valuable properties of existing e-cash systems as an honest user's anonymity against bank and off-line deposit.

The proof of the proposed construction's security is provided.

Keywords: Cryptography · E-cash · E-cash system · Homomorphic encryption · Paillier encryption · RSA textbook encryption

1 Introduction

Electronic Cash (E-cash) is the digital analogue of regular money. Hence, in general, it has to satisfy the same properties as the regular money (or as much as possible).

1.1 Overview of Existing E-cash Systems

One of the first e-cash systems, which was based on cut and cut-and-choose approach [23, 24], was introduced by Chaum, Fiat and Naor (CFN) in 1988. The system was not effective since the bank had to store $2k + 3k^2$ bits (where k is bank's secret key) after each Deposit protocol as well as each user's unique identificator Pk for each Withdrawal protocol, while the user had to store $2k + 4k^2$ bits per each e-coin in his e-wallet, and the merchant - $2k + 3k^2$ bits.

In 1993, Stefan Brands and Niels Ferguson [10] introduced two e-cash systems that were significantly more efficient than any other e-cash system created before. Bank had to store $6k$ bits for the public key, Purchaser had to put $12k$ bits in his wallet, while every e-coin in vendor's wallet took up $10k$ bits. This system was more efficient than Chaum's system, firstly, because of the elimination of the cut-and-choose proofs and,

G. Dregvaite and R. Damasevicius (Eds.): ICIST 2016, CCIS 639, pp. 753–765, 2016.
DOI: 10.1007/978-3-319-46254-7_61

secondly, because of the level of indirection added to double-spending detection, after which there was no need for bank to keep cryptographic information about each withdrawal [23].

In the late 1980 s and early 1990 s, cryptographers developed a system of rigorous security definitions to address philosophical notions such as privacy, unforgeability, proof of knowledge, etc. These definitions influenced e-cash research, making it possible to prove statements about the required properties of an e-cash system [3]. In later works [4, 6, 7], properties such as strong or weak exculpability, double spending prevention, untraceability, money divisibility, off-line payment, unlinkability, unforgeability, etc. were considered.

In 2005, Camenisch, Hohenberger, and Lysyanskaya (CHL) introduced Compact E-Cash [11]. The basic idea of this e-cash system was to use a pseudorandom function to generate a sequence of serial numbers from a single seed. The bank had to give the purchaser a blind signature on a secret seed value s. Alice(the purchaser) then had to generate e-coins with serial numbers $F_s(0), F_s(1), \ldots, F_s(W-1)$, where W is the amount of money in purchaser's e-wallet [3, 11]. Bank had to store $3k$ bits after each deposit, purchaser had to store $11k + \log(W)$ bits for the e-money, while vendor had to store $3k$ and $k + \log(W)$ bits. This CHL compact e-cash system was not better than the other e-cash systems, concerning the amount of data needed to store in each user's database, however it was better in a sense that every purchaser could make a payment himself, by using a secret seed value s.

Nevertheless, in 1998, Frankel, Tsiounis and Yung in [26] pointed out that to date, there have been no efficient systems that could offer provable security. They proposed a fair off-line e-cash system, where the trusted third party could revoke the anonymity under a warrant or in the case of specified suspicious activity.

In [22] the first e-cash system based on binary tree approach without the trusted third party was presented, providing both full unlinkability and anonymity, but, as it was noticed in [3], the system was extremely inefficient.

In [19] a transferable e-cash scheme based on CFN e-cash system with the reduced number of communications between the bank and users that fulfilled the computational anonymity property, was presented.

In 2013, Baseri et al., introduced e-cash scheme with five main protocols: initialization, withdrawal, payment, deposit, and the exchange [17]. His main goal was to take advantage of RSA-based method to attach the time to the structure of the signature. However, in [19] it was showed that Baseri's e-cash system has three drawbacks: the scheme cannot satisfy verifiability, unreuseability and unforgeability.

In [20] the construction with more advanced security and anonymity properties of e-cash system was presented, which provided e-cash transferability by capturing issues that were previously overlooked in [5, 10, 11, 17, 23, 27]. In [10] malleable signatures proposed by Chase [21] were used to allow secure and anonymous transferring of coins.

In [15], Chaum and Pedersen for the first time outlined the very significant property, which can be treated as an essential drawback of e-cash systems providing off-line payment, transferability and anonymity. The authors showed that this class of e-cash systems has the following problem – the informational size of e-cash grows after each transaction. This means that it is impossible to construct an electronic money system providing transferability without money growing in size when it is being transferred among the users. Furthermore, the authors proved there that it does not matter whether e-cash system is computationally untraceable or unconditionally untraceable. If e-cash system is based on full purchase anonymity, money divisibility and off-line payment, then the size of the data stored in the user's e-wallet will eventually become overwhelming.

The problem described above is also common for such e-cash systems as the system providing extensions of compact e-cash [3], Ferguson's scheme [6], Hanatani et al. e-cash [16].

In this paper, we concentrate our attention on the main properties of e-cash system overviewed below.

Divisibility. If a coin is not divisible, the purchaser must withdraw a coin whenever he spends it or withdraw many coins of various values and store them in his e-wallet, like with real cash, as proposed in [5]. Divisibility means that if one withdraws a certain amount of money, he can split into as many pieces as he wants with no need of cash return or re-withdrawal from bank at the moment of payment.

Anonymity. It means the user being not identifiable within a set of subjects, namely anonymity set, performing e-cash operations [3, 4].

Anonymity of e-cash can be split into such sections as **Anonymity of Withdrawal**– bank (or else) does not know how much money the subject has in his wallet as well as who is withdrawing money from it; **Anonymity of Payment** – nobody knows subject's payment history; **Anonymity of Deposit** – bank is not able to recognize who is depositing money unless double spending takes place; **Anonymity of Verification** – bank is not able to recognize who is requesting the verification of money.

In general, e-cash can be called *anonymous* if it satisfies the same characteristics as regular cash.

Off-line payment. In [14] a payment scheme is called online if the payment protocol requires the issuer or the acquirer to participate in the payment protocol online. Otherwise, it is called offline, which means there is no need in an additional connection to the bank in a moment of payment.

Transferability. It means that the payee in one payment transaction can spend the received money in a later payment to a third person without contacting the bank between the two transactions.

1.2 Our Proposal

In this paper, we would like to propose a methodology, avoiding the drawback noticed by Chaum in [15], by sacrificing two valuable e-cash properties, namely, anonymity against Bank and off-line deposit option for the Vendor. The latter property can be recovered by introducing tamper resistant observers to e-wallet. However, we will not consider this opportunity in this paper.

In proposed system, Bank (or e-money organization) is able to trace all payment operations of the Purchaser and identify him. Moreover, Bank is acting as Third

Trusted Party – TTP organization issuing e-cash, controlling its circulation and solving conflicts among the users: Purchasers and Vendors. This methodology has several advantages in the case of money laundering and other financial crimes.

Proposed methodology allows to construct e-cash and e-wallet system providing the following options:

1. E-cash placed in e-wallet is divisible.
2. Payments are anonymous against the Vendor and non-anonymous against the Bank, which is reckoned as TTP.
3. Payments are traceable by Bank after its deposit.
4. E-cash amount can be increased/decreased after e-cash income and outcome and its informational size does not grow.
5. All operations are performed without interactive proofs.

According to [26], e-cash system should be (1) provably secure, based on well understood assumptions, (2) efficient and (3) conceptually easy.

We are trying to follow these recommendations in the realization of proposed methodology. The implementation of e-cash in e-wallet system is very transparent and relatively simple since in our case the blinding and linear interpolation of signatures used for double spending prevention is avoided. We use a combination of well-known cryptographic homomorphic functions such as Paillier asymmetric encryption and modified textbook RSA signature schemes and e-cash operations are performed using computations with encrypted data. We have presented a security proof of this combination in random oracle model.

We consider e-cash system consisting of three parties the Bank (**B**), the Purchaser (**P**) and the Vendor (**V**). These parties are interacting by registration, withdrawal, payment and deposit protocols. We also assume that **B** acts as third trusted party for all users and that **B** computational resources are big enough to register all transactions among users for overspending prevention and dishonest user traceability.

E-wallet construction encompasses divisible e-cash implemented in certain mobile device to ensure execution of e-cash circulation protocols, i.e. in device with restricted power and computational resources.

2 Mathematical Background of E-cash Scheme

Proposed e-cash scheme is based on two homomorphic cryptographic schemes, namely, Paillier asymmetric encryption scheme and RSA textbook signature algorithm [1] for signing ciphertext obtained by Paillier encryption. We use the same modulus for both systems.

For key generation, **B** generates two RSA secure Sophie Germain primes p', q' where

$$p = 2p' + 1, \quad q = 2q' + 1 \tag{1}$$

are primes as well. Then RSA modulus n and Euler totient function ϕ are computed

$$n = pq,\ \ \phi(n) = 4p'q' = \phi. \tag{2}$$

According to Paillier and RSA algorithms [1], **B** computes his private key PrK and public key PuK in the form

$$PrK = (d, \phi),\ \ PuK = (n, e) \tag{3}$$

where $ed \equiv 1\, mod\, \phi(n)$ and e is RSA exponent.

The encryption and signing procedures are the following:

Let $m\, \epsilon\, \mathbb{Z}_n$ be a message to be encrypted. Then random number $r\, \epsilon\, \mathbb{Z}_n^*$ is selected and ciphertext c is computed using Paillier encryption function $Enc_{Pai}()$ in the following way

$$c = Enc_{Pai}(m) = (1+n)^m \cdot r^n mod\ n^2, c\, \epsilon\, \mathbb{Z}_{n^2}^*. \tag{4}$$

RSA signature s on c is computed using $Sig_{RSA}()$ function

$$s_c = Sig_{RSA}(c) = c^d mod\ n, s_c\, \epsilon\, \mathbb{Z}_n^*.$$

Signature s_c verification on c is performed in an ordinary manner with verification function $Ver_{RSA}()$

$$Ver_{RSA}(s_c, c) = \begin{cases} True,\ if\ s_c^e\, mod(n) = c \\ \quad False,\ otherwise \end{cases} \tag{5}$$

According to Paillier algorithm, ciphertext c is decrypted with private key ϕ using decryption function $Dec_{Pai}()$ by the formula

$$m = Dec_{Pai}() = (c^{\phi(n)} mod\big(n^2\big) - 1) \cdot n^{-1} \cdot \phi^{-1} modn, m\, \epsilon\, \mathbb{Z}_n \tag{6}$$

Both Paillier encryption and RSA signature have the following homomorphic properties [1]. Let $m = m_1 + m_2$, then

$$Enc_{Pai}(m_1) \cdot Enc_{Pai}(m_2) = Enc_{Pai}((m_1 + m_2) mod(n)) = Enc_{Pai}(m) = c, c\, \epsilon\, \mathbb{Z}_n^* \tag{7}$$

Let $c = c_1 \cdot c_2$, then

$$Sig_{RSA}(c_1) \cdot Sig_{RSA}(c_2) = Sig_{RSA}\big((c_1 \cdot c_2) mod\big(n^2\big)\big) = Sig_{RSA}(c) = s_c,\ s_c\, \epsilon\, \mathbb{Z}_n^* \tag{8}$$

The security proof of this textbook RSA signature in combination with Paillier encryption is presented in Sect. 6.

3 E-money System

In this section, we present a methodology for e-wallet construction by considering registration, e-cash withdrawal, payment and deposit protocols.

3.1 Registration Protocol

The electronic license is issued by the **B** to **P** during the registration protocol. This protocol is performed once per purchaser, typically when the purchaser opens an account, using secure and authenticated communications between **B** and **P**.

1. **P** appeals to **B** to open his e-cash account for his e-wallet;
2. **B** supplies **P** with his public key $PuK = (n, e)$;
3. **B** assigns an identification Id for **P**, encrypts and signs it by computing $C_{Id} = Enc_{Pai}(Id)$, $S_{Id} = Sig_{RSA}(C_{Id})$;
4. **B** generates random number R, encrypts and signs it by computing $C_R = Enc_{Pai}(R)$ and $S_R = Sig_{RSA}(C_R)$. R represents a random decimal number providing randomness of every transaction.
5. **B** sends to **P** the following registration data D_R using secure and authenticated communication channel;

$$D_R = [n, e, Id, C_{Id}, S_{Id}, R, C_{\mathrm{R}}, S_{\mathrm{R}}] \tag{9}$$

6. **P** forms e-wallet data structure D with the data received from **B**. D structure is represented by a decimal number, satisfying relation

$$D = Id + R + void_1 + void_2, \tag{10}$$

where all decimal positions of added numbers are different and do not intersect, $void_1$ is an empty position for placing maximal amount M of money **B** allows **P** to spend and $void_2$ is an empty position for a decimal number representing e-cash to be paid during payment protocol (Fig. 1).

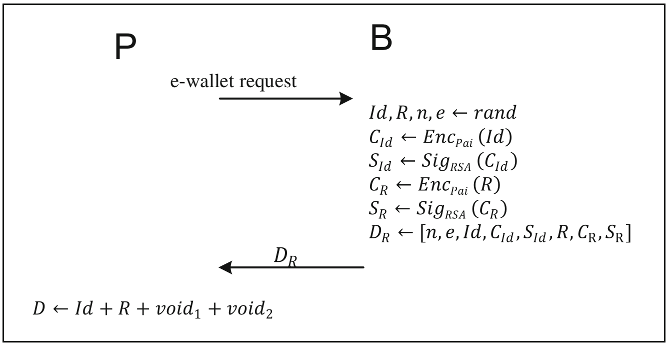
P
B
e-wallet request
$Id, R, n, e \leftarrow rand$
$C_{Id} \leftarrow Enc_{Pai}(Id)$
$S_{Id} \leftarrow Sig_{RSA}(C_{Id})$
$C_R \leftarrow Enc_{Pai}(R)$
$S_R \leftarrow Sig_{RSA}(C_R)$
$D_R \leftarrow [n, e, Id, C_{Id}, S_{Id}, R, C_{\mathrm{R}}, S_{\mathrm{R}}]$
D_R
$D \leftarrow Id + R + void_1 + void_2$

Fig. 1. Registration protocol

3.2 Withdrawal Protocol

After the registration protocol, withdrawal protocol can be executed.

1. **P** sends money request to **B**;
2. **B** defines maximal amount M of e-cash **P** is allowed to spend. **B** encrypts M and signs encrypted value obtaining $C_M = Enc_{Pai}(M)$ and $S_M = Sig_{RSA}(C_M)$. **B** supplies **P** with signed banknotes of several nominal values. For example, we use banknotes with nominal values $m_0 = 0{,}01€$, $m_{10} = 0{,}1€$, $m_{100} = 1€$. **B** encrypts banknotes obtaining $c_0 = Enc_{Pai}(m_1)$, $c_{10} = Enc_{Pai}(m_{10})$, $c_{100} = Enc_{Pai}(m_{100})$ and signs encrypted values computing $s_0 = Sig_{RSA}(c_1)$, $s_{10} = Sig_{RSA}(c_{10})$, $s_{100} = Sig_{RSA}(c_{100})$;
3. **B** sends **P** the following withdrawal data

$$D_W = [M, C_M, S_M, m_0, m_{10}, m_{100}, c_0, c_{10}, c_{100}, s_0, s_{10}, s_{100}] \tag{11}$$

E-wallet data D_{E-W} consists of the union of D_R and D_W data, i.e.

$$D_{E-W} = [n, e, Id, C_{Id}, S_{Id}, R, C_{\mathrm{R}}, S_{\mathrm{R}}, M, C_M, S_M, m_0, m_{10}, m_{100}, c_0, c_{10}, c_{100}, s_0, s_{10}, s_{100}] \tag{12}$$

This data is used to form e-cash and perform a payment (Fig. 2).

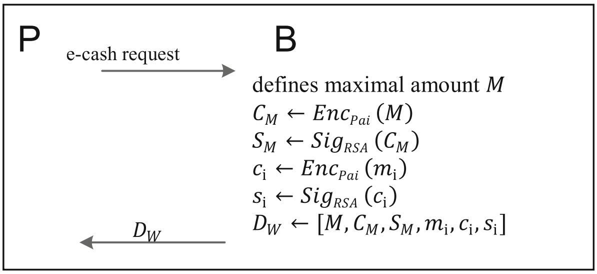
P
e-cash request
B
defines maximal amount M
$C_M \leftarrow Enc_{Pai}(M)$
$S_M \leftarrow Sig_{RSA}(C_M)$
$c_{\mathrm{i}} \leftarrow Enc_{Pai}(m_{\mathrm{i}})$
$s_{\mathrm{i}} \leftarrow Sig_{RSA}(c_{\mathrm{i}})$
D_W
$D_W \leftarrow [M, C_M, S_M, m_{\mathrm{i}}, c_{\mathrm{i}}, s_{\mathrm{i}}]$

Fig. 2. Withdrawal protocol

3.3 Payment Protocol

Say **P** wants to pay the sum $M_1 < M$ to **V**. **P** takes banknotes m_0, m_{10}, m_{100} and forms the required sum

$$M_1 = a_0 m_0 + a_2 m_{10} + a_3 m_{100} \tag{13}$$

where a_0, a_2, a_3 is a quantity of corresponding banknotes.

1. **P** encrypts M_1, using $PuK = (n)$, obtaining C_{M_1} and then computes S_{M_1} on C_{M_1}

$$Enc_{Pai}(M_1) = C_{M_1}, S_{M_1} = s_0^{a_0} \cdot s_{10}^{a_2} \cdot s_{100}^{a_3} \tag{14}$$

2. **P** randomizes its payment by randomly choosing integer α and computing

$$R_1 = \alpha \cdot R, C_{R_1} = C_R^{\alpha} \tag{15}$$

   P computes ciphertext and common signature on $Id_P + \alpha R$

$$C_{IdR_1} = C_{Id} \cdot C_{R_1}, S_1 = S_{Id} \cdot S_R^{\alpha} \cdot S_M \cdot S_{M_1} \tag{16}$$

3. **P** sends **V** the following payment data: $D_P = [M, M_1, C_{IdR_1}, S_1]$.
4. **V** verifies, if $M_1 < M$, and if *Yes*, performs the following computation

$$C_{M_1} = Enc_{Pai}(M_1),\ C_M = Enc_{Pai}(M),\ C_1 = C_{IdR_1} \cdot C_M \cdot C_{M_1} \tag{17}$$

   V verifies signature S_1 on C_1 and if $Ver_{RSA}(S_1, C_1) = True$, then e-cash with nominal value M_1 is accepted from **P** (Fig. 3).

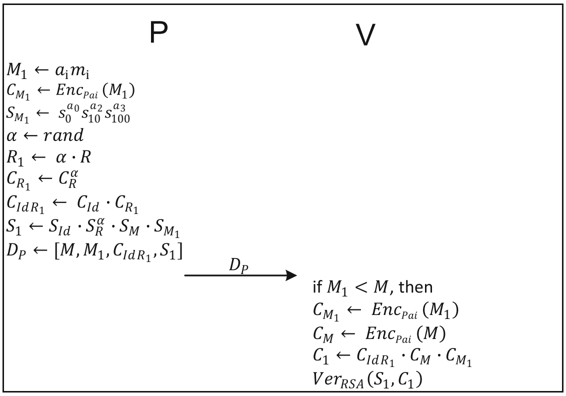
P
V
$M_1 \leftarrow a_i m_i$
$C_{M_1} \leftarrow Enc_{Pai}(M_1)$
$S_{M_1} \leftarrow s_0^{a_0} s_{10}^{a_2} s_{100}^{a_3}$
$\alpha \leftarrow rand$
$R_1 \leftarrow \alpha \cdot R$
$C_{R_1} \leftarrow C_R^{\alpha}$
$C_{IdR_1} \leftarrow C_{Id} \cdot C_{R_1}$
$S_1 \leftarrow S_{Id} \cdot S_R^{\alpha} \cdot S_M \cdot S_{M_1}$
$D_P \leftarrow [M, M_1, C_{IdR_1}, S_1]$
D_P
if $M_1 < M$, then
$C_{M_1} \leftarrow Enc_{Pai}(M_1)$
$C_M \leftarrow Enc_{Pai}(M)$
$C_1 \leftarrow C_{IdR_1} \cdot C_M \cdot C_{M_1}$
$Ver_{RSA}(S_1, C_1)$

Fig. 3. Payment protocol

3.4 Deposit Protocol

After the payment protocol, **V** sends **B** data $D_D = [M_1, C_1]$ for deposition.

1. **B** decrypts ciphertext $Dec_{Pai}(C_1) = (Id + \alpha \cdot R + M + M_1) = D$;
2. Firstly, **B** checks **P** status according to Id. If it is ok, then **B** confirms e-cash validity to **V**; In this stage, **B** can trace all previous **P's** payments and if total sum exceeds limited sum M, then overpayment is detected (Fig. 4).

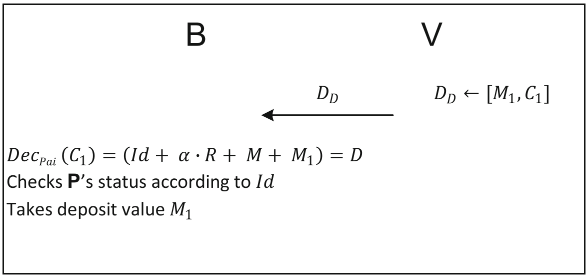
B
V
D_D
$D_D \leftarrow [M_1, C_1]$
$Dec_{Pai}(C_1) = (Id + \alpha \cdot R + M + M_1) = D$
Checks **P**'s status according to Id
Takes deposit value M_1

Fig. 4. Deposit protocol

4 E-cash Data Format

In our construction, e-cash is a decimal number $D = (Id + \alpha \cdot R + M + M_1)$ consisting of separated numbers $Id, \alpha \cdot R, M, M_1$, placed in different decimal positions. A certain amount of decimal digits is assigned to all positions in D to represent the values of these numbers. Format of D is shown below, in Table 1.

Table 1. E-cash data format

	Positions in e-cash	Multiplier
Id	10	10^{35}
$\alpha \cdot R$ or R	20	10^{15}
M	9	10^{6}
M_1	6	1

In this table, for Id we provide 10 decimal digits, for random number $\alpha \cdot R$ - 20 decimal digits and so on. For example, for $Id = 1234567890$, $\alpha \cdot R = 10203040506070809011$, $M = 10000$ € and $M_1 = 345$ €, we obtain

$$D = 1234567890 \cdot 10^{35} + 10203040506070809011 \cdot 10^{15} + 10000 \cdot 10^{6} + 345$$

5 Comparison with Several Existing Schemes

The comparison of proposed system with traditional e-cash systems such as CFN [23], Brands [10] and CHL [11] is presented in Table 2.

As we can see from Table 2, we have prevented Chaum's declared drawback [15] of e-cash data growth property, sacrificing off-line deposit and anonymity against bank.

Table 2. Proposed e-cash system functionality comparison with three common existing systems

Property	Our system	CFN, Brand's and CHL systems
Off-line payment	Yes	Yes
Off-line deposit	No	Yes
Full traceability	Yes by Bank	No
Anonymity against Vendor	Yes	Yes
Anonymity against Bank	No	Yes
Over spending prevention	Yes	Yes
Money divisibility	Yes	Yes
E-cash data grows in size	No	Yes

6 Security Proof

Security of proposed e-wallet methodology relies on the security of combination of Paillier encryption scheme and RSA textbook signature scheme. According to our construction, message m is encrypted obtaining ciphertext c which is then signed by RSA, obtaining signature s.

We assume, that Paillier scheme is an indistinguishable encryption under a chosen-plaintext attack if random encryption number r in (4) is chosen as random element in $\mathbb{Z}_n^*$. We assume, that in this case Paillier encryption is performed correctly and we will follow this assumption. Then ciphertext c corresponding to the message m is uniformly distributed in $\mathbb{Z}_{n^2}^*$ if r is uniformly distributed in $\mathbb{Z}_n^*$.

It is known, e.g. in [1], that RSA textbook signature scheme is existentially forgeable under an adaptive chosen message attack.

In [28], authors introduced RSA Full-Domain-Hash (FDH) function, which can be applied for signing with RSA signature scheme. It was shown in [28, 29] that this scheme is provably secure, i.e. existentially unforgeable under adaptive chosen-message attacks in the random oracle model, assuming that inverting RSA is hard, i.e. extracting a root modulo a composite integer, is hard.

Proposition. If Paillier encryption and RSA signature have the same modulus n and message m is in $\mathbb{Z}_n$, then RSA signature $s = Sig_{RSA}(c)$ on ciphertext c is existentially unforgeable under adaptive chosen-message attacks in the random oracle model.

Proof. Firstly, we should show that ciphertext $c = Enc_{Pai}(m)$ obtained by Paillier encryption taken modulo n, is in RSA domain, i.e. $c\ mod\ n = z\mathbb{Z}_n^*$. It is clear, that $z\mathbb{Z}_n^*$, since $\gcd(h, n) = 1$ if $\gcd(h, n^2) = 1$. Let f be a function of $modn$, i.e. $f(c) = c\ mod\ n = z$. Hence, the composition $f \circ Enc_{Pai}$ of function f and Enc_{Pai} represents the following mapping

$$f \circ Enc_{Pai} : \mathbb{Z}_n \times \mathbb{Z}_n^* \to \mathbb{Z}_n^*$$

and the range of this composition coincides with RSA domain.

We must show that if Paillier encryption is correct, then for any $m\mathbb{Z}_n$, value z is randomly distributed in $\mathbb{Z}_n^*$ for distinct uniform values of r in (4).

For all z in $\mathbb{Z}_n^*$, the set of elements $f^{-1}(z)$ is $\{z, nz, 2nz, \ldots, (n-1)nz\}$ and consists exactly of n elements. Enc_{Pai} is an isomorphism $\mathbb{Z}_n \times \mathbb{Z}_n^* \to \mathbb{Z}_{n^2}^*$. Since $\mathbb{Z}_{n^2}^*$ has $\phi \cdot n$ elements and $\mathbb{Z}_n^*$ has ϕ elements, where ϕ is defined in (2), the function f is n-to-1 mapping: $\mathbb{Z}_{n^2}^* \to \mathbb{Z}_n^*$ and hence, the composition $f \circ Enc_{Pai}$ can be interpreted as a H-function and as a conditional random oracle if number r in correct Paillier encryption scheme can be treated as random.

This implies that element z as a function of r is strongly universal as defined by Wegman and Carter in [31]. In [30], Vaudenay defines this property as a perfect 1-wise decorrelation. Vaudenay showed, that in this case our scheme is secure against chosen plaintext attack (CPA) and chosen ciphertext attack (CCA) respectively (Theorem 7 in [30]). Then, according to [28, 29], textbook RSA signature on Paillier ciphertext c is existentially unforgeable under adaptive chosen-message attacks in the random oracle model. **End of proof**.

6.1 Anonymity Against Vendor

During the payment protocol, **P** randomizes his *Id* by adding it to a product $\alpha \cdot R$ of two numbers, where α is a random number chosen by **P** and r – random number received from **B**. Hence, **P** hides his *Id* for every payment by choosing different α every time.

6.2 Over Spending Prevention

Overspending prevention is achieved by **B** during deposit protocol. After the decryption of current payment data D, **B** extracts **P's** *Id* and is able to trace all previous payments of **P** using his database.

7 Discussion and Conclusions

Most of divisible, anonymous, off-line, traceable e-cash systems have a common issue – data grows in size when transferring e-cash. We proposed a methodology, avoiding this drawback and the example of its realization. E-cash placed in e-wallet can be transferred to other users without growing in size. It is achieved by sacrificing such e-cash properties as off-line deposit and anonymity against bank.

We assume that the proposed realization is a step towards the creation of e-cash which would be (1) provably secure based on well understood assumptions, (2) efficient and (3) conceptually easy, which coincides with requirements presented in [26].

In the proposed methodology, bank represents trusted third party – TTP, which is able to trace all users' transactions. It provides us with several benefits in the sense of money laundering and forensic of other financial crimes.

For further research, we intend to improve our scheme by providing it with off-line deposit option.

References

1. Katz, J., Lindell, Y.: Introduction to Modern Cryptography. Chapman and Hall/CRC, Washington (2008)
2. Paillier, P.: Public-key cryptosystems based on composite degree residuosity classes. In: Stern, J. (ed.) EUROCRYPT 1999. LNCS, vol. 1592, pp. 223–238. Springer, Heidelberg (1999). doi:10.1007/3-540-48910-X_16
3. Rosenberg, B.: Handbook of Financial Cryptography and Security. Chapman and Hall/CRC, Washington (2011)
4. Pfitzmann, A., Köhntopp, M.: Anonymity, unobservability, and pseudonymity - a proposal for terminology. In: Federrath, H. (ed.) Designing Privacy Enhancing Technologies. LNCS, vol. 2009, pp. 1–9. Springer, Heidelberg (2001). doi:10.1007/3-540-44702-4_1
5. Okamoto, T.: An efficient divisible electronic cash scheme. In: Coppersmith, D. (ed.) CRYPTO 1995. LNCS, vol. 963, pp. 438–451. Springer, Heidelberg (1995). doi:10.1007/3-540-44750-4_35
6. Eng, T., Okamoto, T.: Single-term divisible electronic coins. In: De Santis, A. (ed.) EUROCRYPT 1994. LNCS, vol. 950, pp. 306–319. Springer, Heidelberg (1995). doi:10.1007/BFb0053446
7. Fan, C., Sun, W.Z., Hau, H.T.: Date Attachable Offline Electronic Cash Scheme, Department of Computer Science and Engineering, National Sun Yat-sen University, Kaohsiung, Taiwan (2014)
8. Pointcheval, D., Sanders, O., Traoré, J.S.: Cut Down the Tree to Achieve Constant Complexity in Divisible E-Cash (2015)
9. Canard, S., Pointcheval, D., Sanders, O., Traoré, J.: Divisible e-cash made practical. In: Katz, J. (ed.) PKC 2015. LNCS, vol. 9020, pp. 77–100. Springer, Heidelberg (2015). doi:10.1007/978-3-662-46447-2_4
10. Brands, S.: An efficient off-line electronic cash system based on the representation problem. Technical Report CS-R9323 1993, Centrum voor Wiskunde en Informatica (1993)
11. Camenisch, J.L., Hohenberger, S., Lysyanskaya, A.: Compact e-cash. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 302–321. Springer, Heidelberg (2005). doi:10.1007/11426639_18
12. Catalano, D., Gennaro, R., Howgrave-Graham, N.: The bit security of paillier's encryption scheme and its applications. In: Pfitzmann, B. (ed.) EUROCRYPT 2001. LNCS, vol. 2045, pp. 229–243. Springer, Heidelberg (2001). doi:10.1007/3-540-44987-6_15
13. Paillier, P.: Paillier encryption and signature schemes. In: van Tilborg, H. (ed.) Encyclopedia of Cryptography and Security, p. 453. Springer, Heidelberg (2005)
14. Asokan, N., Janson, P.A., Steiner, M., Waidner, M.: The state of the art in electronic payment systems, pp. 28–35 (1997)
15. Chaum, D., Pedersen, T.P.: Transferred cash grows in size. In: Rueppel, R.A. (ed.) EUROCRYPT 1992. LNCS, vol. 658, pp. 390–407. Springer, Heidelberg (1993). doi:10.1007/3-540-47555-9_32
16. Hanatani, Y., Komano, Y., Oht, K., Kunihiro, N.: Provably secure untraceable electronic cash against insider attacks. IEICE Trans. **90-A**(5), 980–991 (2007)
17. Baseri, Y., Takhtaei, B., Mohajeri, J.: Secure untraceable off-line electronic cash system. Scientia Iranica **20**(3), 637–646 (2013)
18. Wang, F., Chang, C.-C., Lin, C.: Security analysis on "secure untraceable off-line electronic cash system". Int. J. Netw. Secur. **18**(3), 454–458 (2016)

19. Canard, S., Gouget, A., Traoré, J.: Improvement of efficiency in (Unconditional) anonymous transferable e-cash. In: Tsudik, G. (ed.) FC 2008. LNCS, vol. 5143, pp. 202–214. Springer, Heidelberg (2008). doi:10.1007/978-3-540-85230-8_19
20. Baldimtsi, F., Chase, M., Fuchsbauer, G., Kohlweiss, M.: Anonymous transferable e-cash. In: Katz, J. (ed.) PKC 2015. LNCS, vol. 9020, pp. 101–124. Springer, Heidelberg (2015). doi:10.1007/978-3-662-46447-2_5
21. Chase, M., Kohlweiss, M., Lysyanskaya, A., Meiklejohn, S.: Malleable signatures: new definitions and delegatable anonymous credentials. In: IEEE Computer Security Foundations Symposium (2014)
22. Canard, S., Gouget, A.: Divisible e-cash systems can be truly anonymous. In: Naor, M. (ed.) EUROCRYPT 2007. LNCS, vol. 4515, pp. 482–497. Springer, Heidelberg (2007). doi:10.1007/978-3-540-72540-4_28
23. Chaum, D., Fiat, A., Naor, M.: Untraceable electronic cash. In: Goldwasser, S. (ed.) CRYPTO 1988. LNCS, vol. 403, pp. 319–327. Springer, Heidelberg (1990). doi:10.1007/0-387-34799-2_25
24. Rabin, M.O.: Digitalized Signatures, in Foundations of Secure Computation. Academic Press, New York (1978)
25. Tsiounis, Y.S.: Efficient electonic cash: new notions and techniques. Ph.D. thesis, Northeastern University, Boston, Massachusetts (1997)
26. Frankel, Y., Tsiounis, Y., Yung, M.: Fair off-line e-cash made easy. In: Ohta, K., Pei, D. (eds.) ASIACRYPT 1998. LNCS, vol. 1514, pp. 257–270. Springer, Heidelberg (1998). doi:10.1007/3-540-49649-1_21
27. Brands, S.: Untraceable off-line cash in wallets with observers. In: Stinson, D.R. (ed.) CRYPTO 1993. LNCS, vol. 773, pp. 302–318. Springer, Heidelberg (1994). doi:10.1007/3-540-48329-2_26
28. Bellare, M., Rogaway, P.: The exact security of digital signatures - how to sign with RSA and rabin. In: Maurer, U.M. (ed.) EUROCRYPT 1996. LNCS, vol. 1070, pp. 399–416. Springer, Heidelberg (1996)
29. Coron, J.-S.: On the exact security of full domain hash. In: Bellare, M. (ed.) CRYPTO 2000. LNCS, vol. 1880, pp. 229–235. Springer, Heidelberg (2000). doi:10.1007/3-540-44598-6_14
30. Vaudenay, S.: Decorrelation: a theory for block cipher security. J. Cryptology **16**(4), 249–286 (2003)
31. Wegman, M.N., Carter, J.L.: New hush functions and their use in authentication and set equality. J. Comput. Syst. Sci. **22**, 265–279 (1981)