RESEARCHERID
THOMSON REUTERS

[Porkodi* 6(7): July, 2019]ISSN 2349-4506

Impact Factor: 3.799

Global Journal of EngineeringScience and ResearchManagement

ELLIPTIC CURVE BASED UNTRACEABLE OFF-LINE ELECTRONIC CASH SYSTEM

Dr.C.Porkodi*, Dr.R.Arumuganathan[1]

*Associate Professor, [1]Professor, Department of Mathematics, PSG College of Technology, Coimbatore, India 642128

DOI: 10.5281/zenodo.3345117

KEYWORDS:e-cash, Elliptic curves, Elgamal Cryptosystem, homomorphic encryption, Elliptic curve discrete logarithm problem (ECDLP).

ABSTRACT

Electronic commerce (e-commerce) is a promising and continuously changing field of business management and information technology. The digital cash transfer system is the modern technology used to carry out the financial transactions electronically in banking sectors in a successful way. In this paper an elliptic curve based untraceable off-line electronic cash system is proposed. The popular cryptographic algorithm ECC providing high level security with smaller key size is used in the system. The scheme satisfies the requirements of a digital cash scheme and in particular preserves dual customer detection, anonymity and provides commanding fraud control facilities. ECC is considered to be best suitable for devices with less memory and so that the portability is guaranteed.

1. INTRODUCTION

The efficient electronic payment system is a significant requirement. One of the important issues for an enterprise is to provide attractive services on the Internet in order to keep the attention of new customers and maintain the existing one for e-commerce. In an electronic payment scheme three parties namely: a bank, a customer (the payer), and a shop (the payee) are involved and a sequence of protocols carried out between the parties. It permits a client to debit e-coins from his/her bank account, and then to credit the same into a merchant' account preferably without communicating with the bank or a trusted party in a secured way. Three distinct stages namely: (i) a withdrawal phase relating the bank and the customer (ii) a payment phase linking the customer and the shop (iii) a deposit phase concerning the shop on-line system and the bank. In an on-line system each of these phases occurs separately. The security requirements also vary for Bank, shop and customer. The bank must confirm that for every account credited there is an account has been debited. The merchant, in receipt of a payment, needs to be guaranteed that the bank credits the received amount in its account. Lastly the customer needs to confirm that the cash he/she has debited will be accepted for a payment.

The basic requirements of an e-cash scheme are

Anonymous payment: The person who spends the money must be confidential. It should not be possible to identify a connection between two expenditure protocols or between an expenditure protocol and a withdrawal protocol.

Unreusability: As the electronic data can be replicated, the prevention of dual spending must be incorporated in the e-cash system.

Unforgeability: Only the authorized parties must have the rights to create digital coins.

Off-line Payment: No communication with the centre is needed during the transaction.

Transferability: In on-line or off-line transactions electronic coins can be distributed to people.

Divisibility: Denomination of digital cash can be done.

Portability: Usage of digital cash and security are independent of location.

In almost every field, the rapid growth of computing and communication, the wired communication with the computers is replaced by wireless communication with smaller handheld embedded devices. There is always a demand for data protection and authentication in real time applications like, mobile banking, healthcare of a patient, connecting office networks on travel and so on. ECC [14] provides the trusted solution for security and effective implementation on resource constrained devices like mobiles and so on.

In this paper, with the scheme proposed by Ziba Eslami [16] as base work, an untraceable off-line e-cash scheme using elliptic curves is developed. To achieve dual customer detection, elliptic curve ElGamal signature scheme is employed so that if a coin is used up more than once, the customer's identity is disclosed efficiently. The computational hard problem ECDLP provides the security for the proposed scheme.

The paper is organized as, in section 2 existing approaches on e-cash is reviewed, in section 3 the proposed scheme is summarized, security and complexity of the scheme is analyzed in section 4, and finally conclusion is done.

2. LITERATURE REVIEW

Nowadays, the research on e-cash made a great attention to design security protocols involving cryptographic mechanisms. The progress in this field is achieved by developing such protocols fulfilling all basic requirements based on complicated mathematics concepts.

Chaum [5] suggested the first electronic cash system in 1982 in which the blind signature was used to guarantee the privacy. D. Chaum et al in [6] proposed cut and choose technology to prevent dual spending. Anonymity revocation protocols used payment systems were proposed by Camenisch et al in [3]. Brands [2] recommended an untraceable off-line electronic cash scheme based on El Gamal and blind signatures that maintain anonymity, dual customer detection strong fraud control capabilities. RSA-based partially blind signature scheme satisfying unforgeability and blindness was established by Cao et al [4]. Fan.C [8], developed a scheme in which an ownership affixed e-cash is formed by affixing the identities of a chosen payee and a corresponding transaction to the blinded e-cash. Fan C. Chen et al [9] proposed a common blind signature scheme with dual hashed messages to resolve the problem in electronic cash namely the cache owner to prove his/her ownership of his/her case.

Gang [12] proposed an anonymous off-line payment scheme involving multiple authorities, in which more than one issuer have the control over the e-coins and the issuers can be selected from the current available issuers list by the customer. Liu et al [13] developed an off line e-cash system which provides recoverability and untraceability. Y. Baseri et al [1] designed an untraceable electronic cash scheme in which the expiration date and the identity of the customer onto the coin are injected and the identity in the case of double spending is detected. ECC based online electronic cash system satisfying the basic requirements, namely customer anonymity, coin tracing, owner tracing, and double spending is developed by Porkodi et al [15]. Cryptography Varadharajan et.al [16] incorporated fairness into the RSA-based e-cash by setting up a set of servers that preserve a threshold cryptosystem such that the servers stay on-line when some error happens and the servers are assumed to preserve user anonymity. Ziba Eslami [17] proposed an untraceable off-line electronic cash scheme with strong fraud control capabilities providing anonymity and dual customer detection.

3. PROPOSED SCHEME

In this section the four phases related to the proposed electronic cash system, namely, the initialization phase, the withdrawal protocol, the payment protocol, deposit protocol are discussed in detail.

3.1 Initialization Phase

In this phase central authority CA initialize some common parameters used in all protocols and certify the public keys of the parties, namely the customer, the merchant and the bank. At any instant, if any enquiry for is made authentication each party must be able to show its digital certificate.

Step 1. **The Central Authority CA:**

1.1 Chooses a large prime field F_p and an elliptic curve $E(F_p)$: $y^2 \equiv x^3+ax+b \pmod p$

1.2 Selects the base point P∈ $E(F_p)$ of order q.
1.3 Selects three public hash functions H, H_0, H_1. The input for H is a 3-tuple of integers and the output is an integer mod q. The input H_0 is a 5-tuple of integers and the output is an integer (mod q).
1.4 Publishes $E(F_p)$, P, q, H, H_0, H_1.

Step 2. **The Bank B:**
2.1 Selects the e_B, d_B from Z_q^* such that $e_B\, d_B \equiv 1(\text{ mod } q)$
2.2 Selects a secret identity $x \in Z_q^*$ and computes the public key Z=xP
2.3 Publishes Z = xP

Step 3. **The Customer S:**
3.1 Selects the e_S, $d_S \in Z_q^*$ such that $e_S\, d_S \equiv 1(\text{ mod } q)$
3.2 Selects a point M ∈ $E(F_p)$ and assumes the X co-ordinate of M as its secret identity m.
3.3 Selects $r_m \in Z_q^*$ randomly and computes the hash value $I \equiv (H_1(m\|(r_mP)_x\ ,\ (e_BM))$, where $(r_mP)_x$ denotes the X-coordinate of the point r_mP
3.4 Sends (I, r_mP) to the Bank

Step 4. **The Bank B:**
4.1 Computes $d_B(I)$ to get the identity m. Also to confirm the integrity of message m it computes the hash value $H_1(m\|(r_mP)_x)$ and checks whether it is equal to the hash value sent by the customer.
4.2 Stores m and r_mP with the customer's identity details (e.g., name, address, etc) in its database.
4.3 Selects an integer $k \in Z_q^*$ randomly and computes

- s= (m||k) (mod q)
- V=sP
- R=xV

4.4 Stores s, k, V, R in its database
4.5 Sends (e_SV, e_SR) to the Customer

Step 5. **The Merchant M** chooses an identification number $ID_M \in Z_q^*$ and registers it with the bank.
In view of Bank, the customer's identity is composed of m and r_mP, where r_m is known to the customer alone. Thus I is a function of m and r_mP only. To validate client's identity by a zero knowledge proof and to prevent impersonation attack, r_m will be used in exchange protocol and in fraud control procedure respectively.

3.2 Withdrawal Protocol
The bank and the customer carry out the with drawal protocol given in Fig 1 to construct the coin. The Customer places a request for a coin from the Bank. The Bank is in need of the proof of identity similar to the withdrawal of traditional money from an account. All e-coins in the proposed scheme are equal and is denoted by (U, P, A, r, A^{11}, t) where U, P, A, A^{11} are points on $E(F_p)$, $r \in Z_q^*$ and t the expiration date of the coin. The elements of the coin are computed by the following steps.

Step 1: **The Customer S:**
1.1 uses his/her private key d_S to recover V and R as $d_S(\ e_SV) = V$ and $d_S(\ e_SR) = R$.
1.2 Selects e, β_1, β_2, and y $\in Z_q^*$ and L from $E(F_p)$
1.3 Calculates

- U = yP
- w = $(R_x\|e)$
- G = wP
- A = $\beta_1 V + \beta_2 P$
- c = $\beta_1^{-1} H(U_x, G_x, A_x)$ (mod q)
- P_1= (A+ e_BL)

1.4 Sends (P_1, c) to the Bank.

Step 2: **The Bank B:**

2.1 Selects the coin's expiration date t = (Date || Time)

2.2 uses its secret identity x to compute

- $c^1 \equiv (cx+s) \pmod q$
- $A^1 = d_B H_1(t)\ P_1 = d_B H_1(t)\ (A + e_B\ L) = d_B H_1(t)A + H_1(t)L$

2.3 Sends (A^1, c^1, t) to the Customer.

Step 3: **The Customer S:**

Computes the coin (U, G, A, r, A^{11}, t) where, $r \equiv \beta_1 c^1 + \beta_2 \pmod q$ and $A^{11}=A^1 - H_1(t)L$

The coin is (U, G, A, r, A^{11}, t).

Fig 1. Withdrawal Protocol

Bank	Customer
	1. gets V and R from ($e_S V$, $e_S R$) sent by the bank 2. Selects e, β_1, β_2, and y $\in Z_q^*$ and L from $E(F_p)$ 3. Computes U=yP w=(R_x‖e) G=wP A= $\beta_1 V+\beta_2 P$ c=$\beta_1^{-1} H(U_x, G_x, A_x) \pmod q$ P_1= (A+ $e_B L$)
← (P_1, c)	
1. Selects expiration date t = (Date || Time) 2. Computes $c^1 \equiv (cx+s) \pmod q$ $A^1=d_B H_1(t)\ P_1$	
→ (A^1, c^1, t)	
	4. Computes $r \equiv \beta_1 c^1 + \beta_2 \pmod q$ $A^{11}=A^1 - H_1(t)L$

Lemma 1: The following equations are satisfied by the coin (U, G, A, r, A^{11}, t) created in withdrawal protocol

(i) $H_1(t)A=e_B A^{11}$

(ii) $rP= H(U_x, G_x, A_x)Z+A$

Proof of (i):

In the coin (U, P, A, r, A^{11}, t) the value of A^{11} is computed as $A^{11} = A^1 - H_1(t)L$. In the communication protocol between the bank and the Customer, the Bank computes $A^1=d_B H_1(t)A + H_1(t)L$. Thus, $e_B(A^{11}) = e_B(A^1 - H_1(t)\ L) = e_B(d_B H_1(t)A + H_1(t)L) - e_B H_1(t)\ L = H_1(t)A$

Proof of (ii): $rP = H(U_x, G_x, A_x)Z+A$

Consider, $H(U_x, G_x, A_x)Z+A = H(U_x, G_x, A_x)\,xP + \beta_1 V+\beta_2 P$ (since $Z=xP$ and $A= \beta_1 V+\beta_2 P$)

$= H(U_x, G_x, A_x)\,xP +\beta_1 sP+ \beta_2 P$ (since $V= sP$) (1)

Consider, $rP = (\beta_1 c^1 + \beta_2)P$ (since $r \equiv \beta_1 c^1 + \beta_2 \pmod q$)

$= (\beta_1(cx + s)+ \beta_2)P$ (since $c^1 \equiv (cx+s) \pmod q$)

$= H(U_x, G_x, A_x)\,xP + \beta_1 sP+ \beta_2 P$ (since $c=\beta_1^{-1} H(U_x, G_x, A_x) \pmod q$) (2)

From (1) and (2), $rP = H(U_x, G_x, A_x)Z+A$

3.3 Payment Protocol

In the payment protocol the parties, namely Customer and Merchant are involved and is given in Fig 2.

Step 1: **The Customer** sends the coin (U, G, A, r, A^{11}, t) to the Merchant.

Step 2: **The Merchant**

2.1 Verifies the date of expiry of the coin

2.2 Validates whether $rP = H(U_x, G_x, A_x)Z+A$ and $H_1(t)A=e_B A^{11}$

Thus the Merchant conforms that the coin is valid. But to prevent double spending some more steps to be performed.

2.3 Computes $d = H_0(U_x, P_x, ID_M, \text{Date}\|\text{Time})$, where H_0 is the initialization phase hash function. Here the transaction date and time are represented as Date|| Time.

2.4 Sends d to the Customer.

Step 3. **The Customer:**

3.1 Computes γ such that $wU_x+y\,\gamma \equiv d \pmod q$

3.2 Sends γ to the Merchant

Step 4. **The Merchant** accepts the coin, if $U_xG + \gamma U= dP$

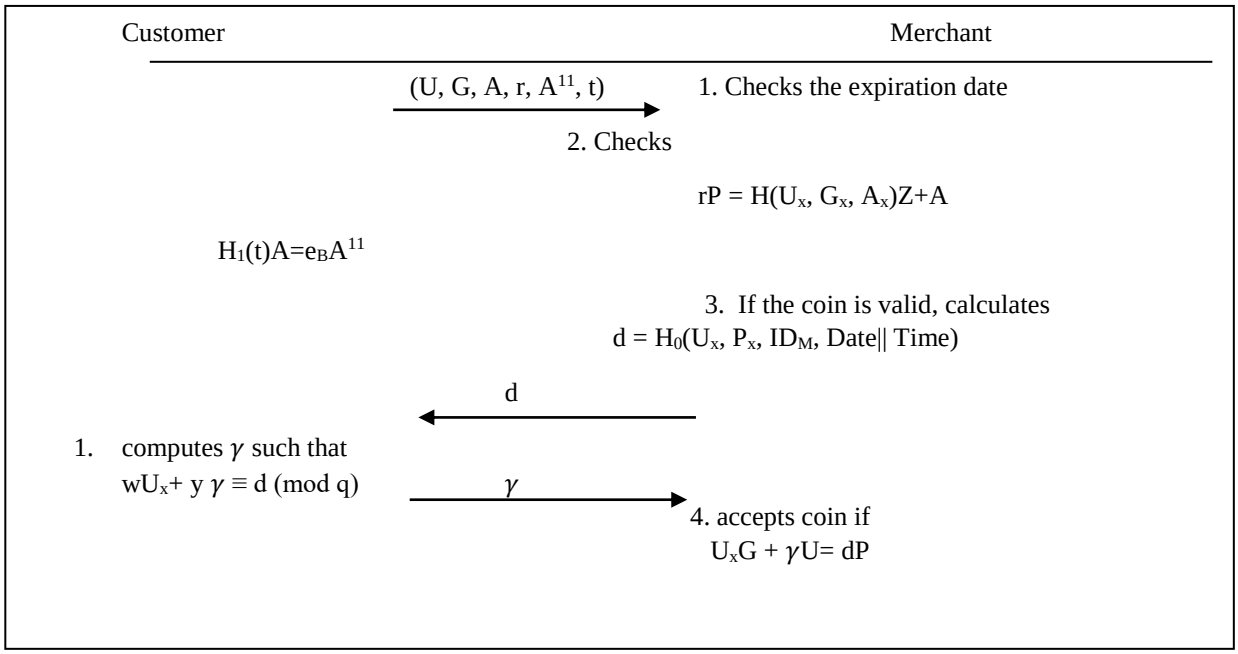

Fig 2. Payment protocol

Result 1: $U_xG + \gamma U= dP$

Proof:

Consider $U_xG + \gamma U = U_xwP+ ((d- wU_x)\,y^{-1})yP$ (since $wU_x+y\,\gamma \equiv d \pmod q$ and $U= xP$)

$= U_xwP+ (d- wU_x)P$

$= dP$

3.4 Deposit Protocol

The Merchant and the bank are involved in the deposit protocol depicted in Fig 3.

Step 1: **The Merchant** sends the coin (U, G, A, r, A^{11}, t) along with (d, γ) to the Bank.

Step 2: **The Bank:**

2.1 Skips to fraud control procedure, if (U, G, A, r, A^{11}, t) exists either in the Deposit information table 1 or in the Exchange information table 2 given below.

2.2 If not, verifies the validity of the coin through the equation $rP = H(U_x, G_x, A_x)Z+A$ and $H_1(t)A=e_BA^{11}$ and the bank stores (U, G, A, r, A^{11}, t), d, γ into the Deposit table and credit cash to the Merchant's account.

Table 1. Deposit Information

Coin information	**ID of the Depositer**	**Date**
(U_1, G_1, A_1, r_1, A_1^{11}, t_1, d_1, γ_1)	ID_1	date 1
(U_2, G_2, A_2, r_2, A_2^{11}, t_2, d_2, γ_2)	ID_2	date 2
…	...	…
(U_n, G_n, A_n, r_n, A_n^{11}, t_n, d_n, γ_n)	ID_n	date n

Table 2. Exchange Information

Coin information	**ID of the Depositer**	**Date**
(U_1, G_1, A_1, r_1, A_1^{11}, t_1)	ID_1	date 1
(U_2, G_2, A_2, r_2, A_2^{11}, t_2)	ID_2	date 2
...	…	…
(U_n, G_n, A_n, r_n, A_n^{11}, t_n)	ID_n	date n

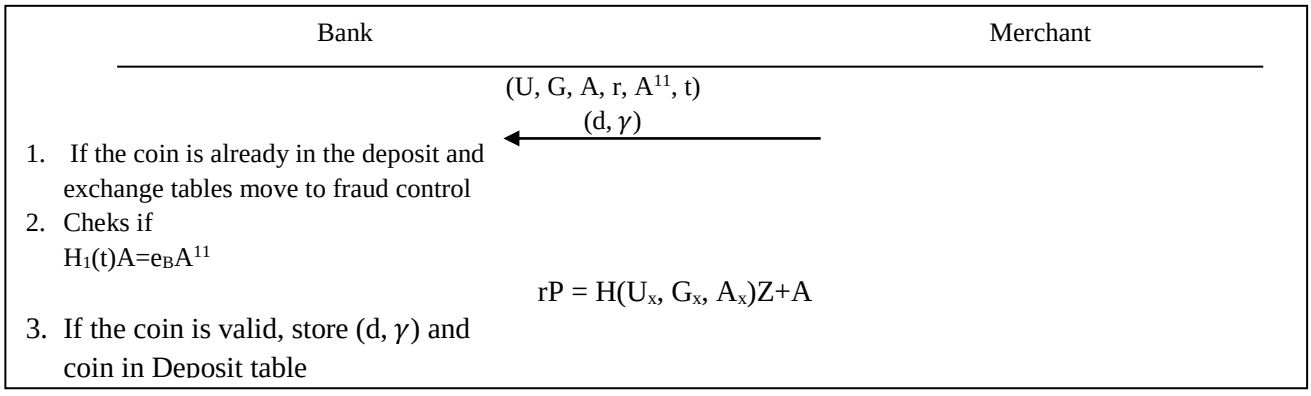

Fig 3.Deposit Protocol

3.5 Exchange Protocol

In this phase, the Bank exchanges only outdated coins which are not in the Deposit Table or Exchange Table. The owner of such coins can submit the coin to the Bank and collect a new coin with the updated expiration date. The protocol is described below.

Step 1. The Owner submits his/her outdated coin together with the hash value I to the Bank. The Bank verifies whether the Owner has the knowledge of the corresponding secret random number r_m involved in hashing by using zero knowledge technique and whether the coin is a valid one according to Lemma 2. A new coin can be created.

Step 2. The Owner performs steps 1.3 and 1.4 of the withdrawal protocol.

Step 3. The Bank performs steps 2.1, 2.2 and 2.3 of the withdrawal protocol.

Step 4. The Owner performs step 3 of the withdrawal protocol to get a complete coin.
The Bank updates the new coin in the Exchange table. It can be noted that when a coin enters this table, then it is treated as invalid and no further transaction on it is carried out.

4. SECURITY ANALYSIS AND COMPLEXITY

Anonymous, unforgeable and detection of double spending are the important security aspects relevant to the digital cash. The proposed scheme satisfies these aspects and is discussed in detail below.

4.1 Anonymous payment

A payment protocol is anonymous if and only if the identity of the customer is not exposed after completion of withdrawal phase. To show the proposed method provides anonymity, an experiment $Exprt_{Adv}^{eav}$ in the form of a game between eavesdropping adversary *Adv* and an imaginary challenger is defined for a probabilistic polynomial time. An imaginary challenger is interested to find whether an *Adv* is successful in exposing the the coin owner's identity.

Also if the *Adv* had the knowledge of all identity information of a specific customer S, it is not feasible to discriminate the coins produced by S from a entirely random coin. Thus in the proposed scheme the owners and the coins created are not linkable and is discussed below.

1. The withdrawal protocol of the proposed scheme is performed for a customer S with an identity I. The messages Trans = {(P_1, c), (A^1, c^1, t)} are exchanged between the Customer and the Bank. Also the coin $Coin_1$= (U_1, G_1, A_1, r_1, A_1^{11}, t) is produced.
2. A bit b is selected at random. If b = 0, then a valid random coin namely $Coin_0$ = (U_0, G_0, A_0, r_0, A_0^{11}, t) is produced.
3. The $Coin_b$= ($\widehat{U}$, $\widehat{G}$, $\widehat{A}$, $\widehat{r}$, $\widehat{A^{11}}$, t), Trans and customer's identity details Id_S is given to the *Adv*.
4. *Adv* produces a bit b^1.
5. If b = b^1, then the output is defined as $Exprt_{Adv}^{eav}$ = 1 and otherwise $Exprt_{Adv}^{eav}$= 0.

The adversary *adv* is successful when $Exprt_{Adv}^{eav}$ = 1

Anonymous of the scheme is broken by the adversary, if it correctly determines whether the $Coin_b$ is the original coin of customer S obtained by executing the protocol, or if $Coin_b$ is a randomly produced coin. If the probability of success of the adversary is atmost (½ + ε), where ε is a negligible value then the proposed scheme achieves anonymity.

To prove this, it can be noted that Prob [b=0] = Prob [b=1] =1/2. *Adv* gets (Trans, Id_S, $Coin_b$), with original coin $Coin_b$, if b=1, or a randomly generated $Coin_b$ if b= 0. Discriminating these two possibilities is same as associating a coin to its customer.

Thus,

$$\text{Prob}[Exprt_{Adv}^{eav} = 1] = \frac{1}{2}\text{Prob}[Exprt_{Adv}^{eav} = 1/\ b=1] + \frac{1}{2}\text{Prob}[Exprt_{Adv}^{eav} = 1/\ b=0]$$
$$= \frac{1}{2}\text{Prob}[Adv\ (\text{Trans, Id}_S, \text{Coin}_1) = 1] + \frac{1}{2}\text{Prob}[Adv\ (\text{Trans, Id}_S, \text{Coin}_0) = 0]$$
$$= \frac{1}{2}\text{Prob}[Adv\ (\text{Trans, Id}_S, \text{Coin}_1) = 1] + \frac{1}{2}(1\text{-Prob}[Adv\ (\text{Trans, Id}_S, \text{Coin}_0) = 1])$$
$$\leq \frac{1}{2} + \frac{1}{2}\{\text{Prob}[Adv\ (\text{Trans, Id}_S, \text{Coin}_1) = 1] - \text{Prob}[Adv\ (\text{Trans, Id}_S, \text{Coin}_0) = 1]\}$$

In view of everyone except the Customer, the values $\widehat{U}$, $\widehat{G}$, and $\widehat{A}$ in $Coin_b$ seems to be random. The remaining elements of the coin are $\widehat{r} = \beta_1 c^1 + \beta_2$ (mod q) and $\widehat{A^{11}} = \widehat{A^1} - H_1(t)L$ where β_1, β_2, L are randomly chosen by the Customer. Also, $c = \beta_1^{-1} H(\widehat{U_x}, \widehat{G_x}, \widehat{A_x})$ (mod q), $P_1 = (\widehat{A} + e_B L)$. Thus, *Adv* obtains different values for β_1 and L from the values of (P_1, c) in Trans, and $\widehat{U}$, $\widehat{G}$, and $\widehat{A}$ in (U_1, G_1, A_1, r_1, A_1^{11}, t) or (U_0, G_0, A_0, r_0, A_0^{11}, t). The values of β_1 and L occur with the same probability. {Prob[*Adv* (Trans, Id_S, $Coin_1$) = 1] - Prob[*Adv* (Trans, Id_S, $Coin_0$) = 1]}$\leq \varepsilon$, where ε is negligible. Thus, Prob[$Exprt_{Adv}^{eav}$ = 1] $\leq \frac{1}{2} + \varepsilon$.

4.2. Unforgeable

If the bank is the only source of producing e-coins then the payment protocol is said to be unforgeable. To produce an unauthorized coin, an attacker has to find (U, G, A, r, A^{11}, t) such that the components satisfy the equations $H_1(t)A = e_B A^{11}$ and $rP = H(U_x, G_x, A_x)Z + A$. As the Bank's blind signature A^{11} on A is unforgeable, A^{11}

cannot be generated by an attacker. Also computing r that satisfies $rP= H(U_x, G_x, A_x)Z+A$ is equivalent to solving the computational hard ECDLP.

4.3. Dual-spending detection

A payment protocol identifies dual-expenditure if and only if the e-coin can be utilized exactly once. If the customer uses the coin twice, once with M, and once with V. i.e, if the customer, with M deposits his/her coin along with (d, γ) and with V deposits his/her coin along with (d^1, γ^1), the Bank finds out the existence of the coin in its database. Also such a customer can be identified by the Bank by computing the value of y satisfying the equation $y(\gamma - \gamma^1) \equiv (d - d^1) \pmod q$. Using this value of y the bank can obtain w by using the equation $wU_x+y\ \gamma \equiv d \pmod q$ and recognize the customer.

4.4. Fraud control

The possible ways to cheating in the proposed scheme and how to control such frauds are discussed below.

1. The Merchant attempts to submit the coin twice, once with the valid pair $(d, \gamma)$and second time with a fake pair (d^1, γ^1). Such an attempt cannot be done by a Merchant; creating such numbers is equivalent to solving the computational ECDLP. i.e. computing $d^1, \gamma^1$from the equation $U_xG + \gamma^1U= d^1P$.
2. The malicious merchant MM may get a customer's coin and attempt to spend the coin along with the legitimate Merchant by depositing in the bank. MM provides the coin to the legitimate Merchant, who computes $d^1 \neq d$. MM is not aware of w, y but he/she must find out γ^1 such that $U_xG + \gamma^1U= d^1P$, which is equivalent to ECDLP. Since $d \neq d^1$, the Merchant detects that $U_xG + \gamma^1U \neq d^1P$.
3. An employee of the Bank may attempt to create a fake coin. He/she has the knowledge of the parameters s, V, R, d_B, and thus he/she can produce a coin satisfying $H_1(t)A=e_BA^{11}$ and $rP= H(U_x, G_x, A_x)Z+A$. But the Customer's secret parameters w, y are unknown to the person, he/she will not be able to find a suitable γ. Thus the coin cannot be spent by him/her.
4. A cheater may attempt to spend a coin by stealing from a customer. But he/she is unaware of the secret parameters w, y of the customer even the verification equations are satisfied. Thus, by the hardness of the ECDLP the cheater is unable to create γ such that $U_xG + \gamma U= dP$.
5. The malicious customer MS may spend the coin in the final day of its expiration date with merchant M1, then exchange the coin and spend the Exchanged coin with merchant M2. There are two possibilities:
    - First M1 deposits the coin. Since the coin exist in the Exchange Table, it is taken as invalid and the exchanged client MS can be found from Exchange Table. But, since exchanged coin does not exist in any of the tables, then M2 can deposit it safely.
    - First M2 deposits exchanged coin. Since exchanged coin does not exist in any of the tables, then M2 can safely deposit it. But, when M1 deposits the coin since it exists in the Exchange Table, it is taken as invalid and the client MS who has exchanged it is found.
6. Any person E may steal the coin from the Customer and attempt to exchange it. With respect to exchange protocol, it is feasible only if a coin is not already in Deposit Table or Exchange Table. Also, E's identity must be provided to spend the coin. If E is successful in exchanging it for exchanged coin, he/she can spend and deposit the new coin. But, as E's identity is stored in the Exchange Table corresponding to the coin, the legitimate transactions on the coin will make E to be guilty one.

4.5 Complexity of the proposed scheme

In this section the computation and complexity of the proposed e-cash scheme is discussed. Let M be the computation time of one modular multiplication in a 160-bit modulo, and EM is the computation time of one elliptic curve scalar multiplication operation in a 160-bit modulo the output size of secure one-way hash functions as 160 bits, H is the computation time of one hashing operation. The performance of the proposed scheme in view of the following aspects are represented by the table 3

Table 3 Complexity of the proposed e-cash scheme

Aspects	Proposed Scheme
C_1- Computation cost of withdrawing and spending for the spender	5EM+ 9M+1H
C_2- Computation cost of withdrawing for the Bank	1EM+ 2M+1H
C_3- Computation cost for the verification of e-coin for the Merchant	6EM+3M+2H
C_4- Computation cost of withdrawing an e-coin in bits	160
C_5- the need for an untraceable e-mail system	No
C_6- the need for smart card	No
C_7- transaction mode	Off-line
C_8- the hard problem of the security of e-cash	ECDLP

Currently cryptographic protocols apply asymmetric algorithms such as RSA and ECC because of their flexibility and enhanced ability to manage keys. Table 4 compares the key sizes of RSA cryptosystem with elliptic curve cryptosystem to encryption for comparable levels of security against brute-force attacks. From the table, it is obvious that the elliptic curve cryptosystem requires a considerably shorter key and offer the same level of security as RSA which need much larger keys.

Table 4. A comparison of key sizes of RSA and ECC

Elliptic curve Cryptosystem	RSA Cryptosystem	Key size ratio
160	1024	1:6
224	2048	1:9
256	3072	1:12
384	7680	1:20
512	15360	1:30

Recently most of the cryptographic protocols utilize ECC because it is considered to be best suitable for embedded devices cost wise and performance wise. The proposed electronic scheme is based on ECC and thus the proposed scheme is efficient than the exponentiation based electronic schemes.

CONCLUSION

In this paper, an off-line untraceable electronic cash system providing anonymity, double spender detection and fraud control capabilities is proposed. The produced coin contains the expiration date, the proposed scheme provides the bank to maintain the database in an easy and inexpensive way. The underlying security of the scheme lies on the computational hard elliptic curve discrete logarithm problem. Since ECC requires significantly smaller key size, the computations can be done fast, less storage space is needed and it is ideal for small devices like mobiles. Thus the computational overhead is less for the proposed e-cash scheme when compared to exponentiation based e-cash schemes.

REFERENCES

1. Y. Baseri, B. Takhtaei, J. Mohajeri, Secure untraceable off-line electronic cash system, Scientia IranicaD 20(3), pp. 637–646, 2013.
2. Brands, S. Untraceable off-line cash in wallets with observers. In Advances in Cryptology – Crypt'93 Proceedings. Lecture Notes in Computer Science, Vol. 773, Springer, Berlin, 1993, 302–318.
3. Camenisch, J., Maurer, U., and Stadler, M. Digital payment systems with passive anonymity-revoking trustees. In Computer Security – ESORICS'96 Proceedings. Lecture Notes in Computer Science, Vol. 1146, Springer, Berlin, 1996, 31–43.
4. Cao, T., Lin, D., and Xue, R. A randomized RSA-based partially blind signature scheme for electronic cash. Computers and Security, 2005, 44–49.
5. D. Chaum, Blind signature for untraceable payments. Proceedings of Eurocrypt'82, Plenum Press. Pp.199-203, 1983.
6. D. Chaum, A. Fiat, M. Naor, Untraceable electronic cash, Proceedings of the Crypto'88, pp. 319-327, Springer-Verlag Berlin Heidelberg, 1990.

7. C. Chang, and Y. Lai., A flexible date- attachment scheme on e-cash, Computers and Security, pp. 160-166, 2003.
8. Fan, C. Ownership-attached unblinding of blind signatures for untraceable electronic cash. Information Sciences, 176, 2006, 263–284.
9. Fan, C., Chen, W., and Yeh, Y. Blind signatures with double-hashed messages for fair electronic elections and ownership claimable digital cash. In J. Filipe (ed.), Enterprise Information Systems, Kluwer Academic, Dordrecht, 2000, pp. 197-203.
10. Ferguson, N. Extensions to single term off-line coins. In Advances in Cryptology – CRYPTO'93 Proceedings, Springer, 1994, 292–301.
11. Ferguson, N. Single term off-line coins. In T. Helleseth (ed.), Advances in Cryptology – EUROCRYP'93 (LNCS 765)765), Springer-Verlag, Berlin, 1994, pp.318–328
12. Juang, W. A practical anonymous off-line multi-authority payment scheme. Electronic Commerce Research and Applications, 2005, 240–249.
13. Liu, K., Tsang, P., and Wong, S. Recoverable and untraceable e-cash. In Second European PKI Workshop: Research and Applications, LNCS 3545, Springer, New York, 2005, 206–214.
14. N. Koblitz, "Elliptic Curves Cryptosystems", Mathematics of Computation, 48 (1987), pp. 203- 209.
15. C.Porkodi and K.Sangavai, An Online Electronic Cash System based on Elliptic Curve Cryptography, International Journal of Computer Sciences and Engineering, Vol.6, Iss.6, 2018, pp. 1043-1047.
16. Varadharajan, v., Nguyen, K. Q., and Mu, Y. On the design of efficient rsa-based offline electronic cash schemes. Theoretical Computer Science, 226, 1999, pp. 173-184.
17. Ziba Eslami, Mehdi Talebi, A new untraceable off-line electronic cash system, Electronic Commerce Research and Applications 10, 2011, pp. 59–66.