IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.-6, Issue-6, June 2018 E-ISSN: 2347-2693

An Online Electronic Cash System based on Elliptic Curve Cryptography

C. Porkodi[1*], K. Sangavai[2]

[1*, 2]Department of Mathematics, PSG College of Technology, Coimbatore, India

**Corresponding Author cpg.maths@psgtech.ac.in*

Available online at: www.ijcseonline.org

Accepted: 03/Jun/2018, Published: 30/Jun/2018

***Abstract*—** Electronic commerce is an emerging area and one of the technological innovations of business management and information technology. A fair online electronic cash system with double spending tracing based on elliptic curve cryptography is presented in this paper. The security of the protocols is based on the computational hard elliptic curve discrete logarithm problem. In the proposed scheme, the anonymity of the user is maintained and is revocable by an on-line trusted third party under certain conditions. Dual spending of the same coin by the user is traced out by the bank. The proposed scheme is illustrated using Matlab 7.1

***Keywords*—** Cryptography, electronic cash system, elliptic curve, anonymity, unforgeability, double spending tracing

I. Introduction

Electronic commerce is an emerging and constantly changing area of banking and finance. Electronic cash (e-cash) transfer systems refer to the technological breakthrough that performs financial transactions electronically. In a digital cash system, the money transferred from one account to another in a secured way is known as e-coin or e-cash. In the simple electronic cash system customers and merchants have accounts at banks and the money is transferred from the customer's account to the merchant's account by using three cryptographic protocols:

- a withdrawal protocol - coins are withdrawn by the customer from his/her account at the bank
- a payment protocol - coins are paid by the customer to the merchant
- a deposit protocol – coins are deposited by the merchant to the bank

There are two types of electronic cash system, namely

- Online electronic cash system – The transaction can be done in online. i.e all the three parties are involved at the same time.
- Offline electronic cash system – The transaction can be done offline, meaning no communication with the central bank is needed during the transaction.

The simple electronic cash is system shown in Figure 1.1.

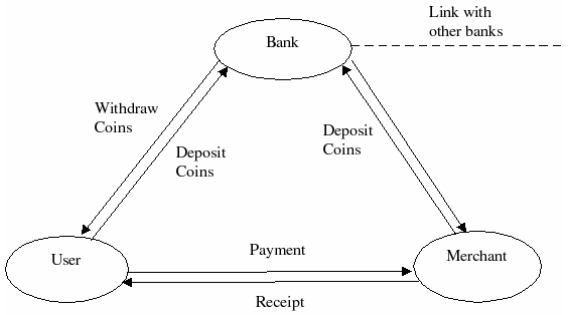

Fig. 1.1 Simple Electronic Cash System

Generally, an e- cash must satisfy the following properties:

- Unforgeability: Only legal signer can generate valid signatures. It means that only bank can issue electronic coins and only legal user can withdraw electronic coins from his account and deposit electronic cash into his account.
- Unlinkability: It is very hard to decide whether two different valid signatures were computed by the same signer. It means that it is difficult for the bank to determine whether any pair of payments is executed by the same customer, unless the payments cause over spending.
- Anonymously payment: Given a valid signature, it is computationally infeasible to find the identity of the signer without knowing the secret key. It means that the bank has no way of tracing electronic coin.
- Protect double spending: Spending of electronic coin more than once from the users or from the bank is prohibited. In our proposed e-cash system, the traceability is done when the coin is spent by the user more than once. In such a case of dual spending user's private key is revealed by the bank.

Furthermore, the user anonymity is maintained by the bank when the user spends a determined coin only once. Also this coin is unforgeable because it is difficult to find a user private key from his/her public key.

The structure of the paper is as follows: Introduction and related work of electronic cash system are presented in section 1 and 2 respectively. Elliptic curve cryptography concepts are given in section 3. An online electronic cash system protocol based on ECC is developed in section 4. The security analysis is also done in section 4, the proposed protocol is justified numerically in section 5, and finally the conclusion is made.

II. Related Work

The first e-cash scheme was proposed in 1982 by Chuam [2], and many research articles on electronic cash have been published. A good electronic cash must provide user's anonymity and untraceability. Double spending is an important issue in e-cash, that the user spends the coin more than one time. The technique to protect double spending by using cut and choose technology is proposed first by D. Chaum et al [3, 4]. However, their scheme is not efficient because the double spending is protected after the occurrence and this scheme was improved by S. Brands [1] including all benefits of Chuam's scheme. In Brands' scheme, the user cannot be traced by the bank if the user did not spend the coin twice. Khalid O Elaalim and Shoubao Yang [9, 10] improved this scheme by facilitating the user to make use of two secret keys, one for double spending and the other cannot be revealed unless double spending occurred. The advantage of this scheme is that the user need not open account again. In most of the electronic schemes, the requirements anonymity and unlinkability are provided, when the coin is spent once by the user. X. Hue [5, 6] introduced an electronic cash model in which the traceability of coins is done, when there is a double spending. The first off-line electronic cash system has introduced by Chaum *et al.* (1990) and then developed further Popescu [11, 12] and Ziba Eslami and Mehdi Talebi [13].

Koblitz introduced elliptic curve public key cryptosystem [7, 8], which offers the same level of security with considerably shorter key as other asymmetric algorithms with much larger keys. This security level due to elliptic curve discrete logarithm problem appears to be much harder than the discrete logarithm problem in DSA and RSA. For example, an elliptic curve cryptosystem with public key size of 160 bits is as secure as RSA and DSA cryptosystems with the public key of size 1024 bits.

III. Elliptic Curve Cryptography

In this section the basic definition of elliptic curves, point addition, Elliptic curve discrete logarithm problem are discussed.

3.1 Elliptic Curve

Let K be a field of characteristic $\neq 2$, 3, then an elliptic curve over K is the set of points (x, y) with $x, y \in K$ satisfying equation $E: y^2 = x^3 + ax + b$, provided $4a^3 + 27b^2 \neq 0$ together with a single element O_E, called point at infinity.

3.2 Addition of points on elliptic curve

Let $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ be two points on an elliptic curve E, then the sum of the points P_1 and is P_2 denoted by $P_3 = P_1 + P_2 = (x_3, y_3) \in E$ and is computed as follows.

$$P_1 + P_2 = \begin{cases} O_E \; if \;\; x_1 = x_2, \; y_1 = -y_2 \\ (x_3, y_3), \;\; otherwise \end{cases}$$

Where, $(x_3, y_3) = (\lambda^2 - x_1 - x_2, \lambda(x_1 - x_3) - y_1)$

and $\lambda = \begin{cases} \frac{3x_1^2 + a}{2y_1} if \; P_1 = P_2 \\ \frac{y_2 - y_1}{x_{2-x_1}} \;\; otherwise \end{cases}$

The notation nP stands for the addition of the point P+P+…n times. A point P on the elliptic curve is said to be of order n, if n is the smallest positive integer such that $nP = O_E$.

3.3 Elliptic curve discrete logarithm problem

Suppose Q = xP represents that the point P on the elliptic curve $E(F_p)$, then the elliptic curve discrete logarithm problem is to determine x given P and Q . It is relatively easy to calculate Q given x and P, but it is hard to determine x given Q and P.

3.4 Analogue of the Elliptic Curve ElGamal Encryption

The communication between two parties A and B is done as follows:

- A and B select $E(F_p)$ and a base point P of order q randomly.
- A and B choose secret keys as the random integers r_a and r_b respectively. The corresponding public keys of A and B are r_aP and r_bP.
- To send a message point m to B, A chooses a random integer k and sends the pair of points $(m + k(r_b\text{P}), \text{kP})$.
- To read m, B computes $m + k(r_b\text{P}) - r_b(\text{kP}) = \text{m}$.

IV. Electronic Cash System

A coin is a bit string that is (blindly) signed by the bank. The proposed scheme is restricted to a single denomination of coins and the extension to multiple denominations is straight forward, with the bank using a separate key pair for each denomination. In a fair electronic cash system, under certain

well defined conditions the tracing of a coin and the revoking of the customer's anonymity must be possible. For example, anonymity may be revoked by a trusted third party, the trusted center to track the forgery person who gets a payment as electronic cash.

4.1 System Setup

Let E (F_p): $y^2 \equiv x^3+ax+b \pmod p$, a, b $\in F_p$, be an elliptic over the prime field F_p and P be base point of the elliptic curve E (F_p) of order q. Let P, P_1, P_2 be randomly and independently selected base points of E(F_p). The security of the scheme is based on the elliptic curve discrete logarithm problem. Let h: $\{0, 1\}^* \rightarrow F_q^*$ be a collision resistant hash function.

1. The bank selects a secret key $x \in Z_q^*$ at random and publishes $y = xP$.
2. The trusted center T selects a secret key $x_T \in Z_q^*$ at random and publishes $y_T = x_T P_2$.
3. The customer Alice has the randomly chosen secret key $x_C \in Z_q^*$ and the public key $y_C = x_C P_1$.
4. The shop's secret key is $x_S \in Z_q^*$ and the public key is $y_S = x_S P_1$.

4.2 Opening an Account

To open an account, the customer Alice has to prove her identity by executing the protocol ProofLog (P_1, y_C) discussed in Protocol 4.2.1 with the bank.

Protocol 4.2.1: ProofLog (P_1, y_C)

1. Alice randomly selects $r \in Z_q^*$, computes $a = rP_1$ and send it to the Bank.
2. The bank chooses a challenge $k \in Z_q^*$, at random and sends it to Alice.
3. Alice computes $b := r - kx_c$ and sends it to the Bank.
4. The bank accepts the proof if $a = bP_1 + ky_c$; otherwise rejects it.

Since, $bP_1 + ky_c = (r - kx_c)P_1 + ky_c$
$= rP_1 - kx_cP_1 + ky_c$
$= rP_1 - ky_c + ky_c$
$= rP_1 = a$

The bank opens an account and stores y_C in Alice's entry in the account database.

4.3 The Online Electronic Cash System

The trusted center T is involved in every withdrawal transaction, and the bank is involved in every payment. The customer Alice has to authenticate herself to the bank by proving that she has the knowledge of the secret key $x_c = log_{p1}(y_c)$ by executing the above challenge response protocol. To get a coin which is essentially a signature of the empty string blindly issued by the bank, Alice executes the withdrawal protocol with the bank.

4.3.1 The withdrawal Protocol

1. The bank randomly selects $\bar{r} \in Z_q^*$, computes $\bar{a} = \bar{r}P$ and sends $\bar{a}$ to Alice.
2. Alice selects $u, v, w \in Z_q^*$, at random and computes $a = u\bar{a} + vP + wy$ and $c = h(a_x)$, $\bar{c} = (c - w)u^{-1} (mod\ q)$. Here a_x denotes the X-coordinate of the point a. Alice sends (u, v, w) encrypted with the trusted center's public keyy_T and $\bar{c}$ to the bank.
3. The bank sends $\bar{a}$ and $\bar{c}$ and the encrypted (u, v, w) to the trusted center ***T***.
4. T checks whether $u\bar{c} + w = h((u\bar{a} + vP + wy)_x)$, and sends the result to the bank. Here $(u\bar{a} + vP + wy)_x$ denotes the X-coordinate of the point $(u\bar{a} + vP + wy)$.
5. If the result is correct, the bank computes $\bar{b} = \bar{r} - \bar{c}x$ and sends it to Alice. Alice's account is debited.
6. Alice verifies whether $\bar{a} = \bar{b}P + \bar{c}y$, computes $b = u\bar{b} + v$ and gets as the coin the signature $\sigma = (c, b)$ of the empty message.

4.3.2 Payment and Deposit

In online payment, the shop must be connected to the bank when the customer spends the coin. Payment and deposit are done in one transaction. Alice spends a coin by sending it to a shop. The shop verifies the coin by checking $c = h((bP + cy)_x)$. If the coin is valid, it passes the coin to the bank. The bank also verifies the coin and then compares it with all previously spent coins which are stored in the database. If the coin is new, the bank accepts it and adds it into the database. The shop's account is credited.

Proposition 1. During the payment protocol, the shop can accept the coin, if $c = h((bP + cy)_x)$.

Proof:

bP + cy = $(u\bar{b} + v)P + cy$
$= [u(\bar{r} - \bar{c}x) + v]P + cy$
$= u\bar{r}P - u\bar{c}xP + vP + cy$
$= u\bar{a} - u\bar{c}y + vP + (\bar{c}u + w)y$
$= u\bar{a} - u\bar{c}y + vP + \bar{c}uy + wy$
$= u\bar{a} + vP + wy$
$= a$

$h[(bP + cy)_x] = h(a_x) = c$

4.3.3 Coin and Owner Tracing

The coin (c, b) is generated by binding the secret parameters $\bar{r}, x$ of the bank and the secret parameters u, v, w of the customer Alice. Trusted center computes u, v, w using its secret key. With the support of the values $(\bar{a}, \bar{c})$ received in the withdrawal protocol, the trusted center can link coin (c, b) and its owner. This link enables coin and owner tracing. The link is achieved by verifying $c = h\ (u\bar{a} + vP + wy)_x$ and $bP = u\bar{a} + vP$

4.3.4 Customer Anonymity

The anonymity of the customer is based on the fact that the used signature scheme is blind and on the security of the encryption algorithm used to encrypt the blinding factors *u*, *v* and *w*. In this scheme only the bank knows the identity of the e-cash, which is confidential to the merchant. In the payment protocol, the merchant receives e-cash from the user. The merchant can only verify the validity of the signatures, but could not determine the identity of the signer.

4.3.5 Double spending

If Alice spends a coin twice (at different shops, or at the same shop but different times), she produces signatures of two different messages. Both signatures are computed with the same commitment c# (the coin number). This reveals the signer's secret, which is the blinding exponents in our scheme.

4.4 Security Analysis

In the opening protocol, the customer Alice sends a= rP_1 by hiding the secret r. Because of the computationally hard ECDLP, from the known value of a, it is computationally infeasible for an attacker to recover the secret challenge "r". Thus, it is impossible for an attacker to impersonate as a legitimate customer. Similarly, because of the hardness of ECDLP is involved in the withdrawal protocol from the publicly known $\bar{a} = \bar{r}P$ it is computationally infeasible to compute the bank's secret $\bar{a} = \bar{r}P$. Thus the proposed scheme is resistant against any attacker.

V. Numerical Illustration

In this section, the proposed protocol is justified numerically using Matlab 7.1.

5.1 System setup

Consider the prime field F_{211} and the elliptic curve $E(F_{211})$: $y^2 = x^3 - 4(mod\ 211)$ over F_{211}. Here $a = 0, b = -4$. The point P = (94, 57) is observed to be a base point of $E(F_{211})$ and its order is $q = 241$. The points $P_1 = (5, 11)$, $P_2 = (2, 2)$ on $E(F_{211})$ are also selected.

1. The bank selects the secret key $x = 3 \in F_{241}$ and publishes the public key $y = xP = (13,\ 37)$.
2. The trusted center ***T*** selects the secret key $x_T = 7 \in F_{241}$ and publishes the public key $y_T = x_T P_2 = (179, 199)$.
3. The customer Alice randomly selects the secret key $x_C = 5 \in F_{241}$ and computes the public key $y_C = x_C P_1 = (75, 121)$.
4. The shop's secret key $x_S = 11 \in F_{241}$ and its public key is $y_S = x_S P_1 = (84, 1)$.

5.2 Opening an Account

To open an account, the customer Alice has to prove her identity by executing the challenge response protocol.

Protocol: ProofLog (P_1, y_C)

1. Alice selects $r = 17$, computes $a = rP_1 = (95, 17)$ and send it to the Bank.
2. The bank chooses a challenge $k = 3$, at random and sends it to Alice.
3. Alice computes $b := r - kx_c = 2$ and sends it to the bank.
4. The bank accepts the proof if $a = bP_1 + ky_c$
$= (95, 17) = a$

5.3 Withdrawal Protocol

1. The bank randomly selects $\bar{r} = 13$, computes $\bar{a} = \bar{r}P = (20, 191)$ and sends $\bar{a}$ to Alice.
2. Alice selects $u = 3, v = 5, w = 7$, at random and computes $a = u\bar{a} + vP + wy = (120, 180)$

It is assumed that the hash value of a_x as $c = h(a_x) = 19$,

Now, $\bar{c} = (c - w)u^{-1}(mod q) = 4$

Alice encrypts the secret (u, v, w) using the trusted center's public key y_T and sends the cipher text along with $\bar{c}$ to the bank.

3. The bank sends $\bar{a}$, $\bar{c}$ and the cipher text of (u, v, w) to the trusted center T.
4. T computes (u, v, w) by decrypting the cipher text of (u, v, w) using its secret key x_T. Also to check the authenticity and data integrity of the received values from the bank, T verifies the equation $u\bar{c} + w = h((u\bar{a} + vP + wy)_x) = h[a_x] = c = 19$ and sends the same result to the bank.
5. After receiving the correct hash value, the bank computes $\bar{b} = \bar{r} - \bar{c}x = 13 - 4(3) = 1$ and sends it to Alice. Then Alice's account is debited.
6. Alice verifies $\bar{b}P + \bar{c}y = (20, 191) = \bar{a}$ and gets the coin the signature $\sigma = (c, b) = (19, 8)$ of the empty message by computing $b = u\bar{b} + v = 8$.

5.4 Payment and Deposit

During the payment protocol, the shop can accept the coin, if $c = h((bP + cy)_x)$.

Proof: bP + cy = $(u\bar{b} + v)P + cy$

$= 8(94, 57) + 19(137, 37)$

$= (14, 29) + (93, 134)$

$= (120, 180) = a$

$h[(bP + cy)_x] = h(a_x) = c$

Conclusion

In this paper, a fair online electronic cash system based on elliptic curve cryptography is developed. The proposed scheme satisfies the basic requirements, namely customer anonymity, coin tracing, owner tracing, and double spending. Customer's anonymity can be revoked by proceeding owner tracing and coin tracing with the cooperation of the bank and the trusted third party. The security of the proposed system relies on the computational hard elliptic curve discrete logarithm problem. The protocol is numerically justified

using Matlab 7.1. Our future enhancement is to develop a fair offline electronic cash system based on elliptic curve cryptography.

References

[1] Brands S, "Untraceable off-line cash in wallets with observers", Advances in Cryptology: Proceedings of Crypto '93, Lecture Notes in Computer Science, Springer-Verlag, (1994) pp. 302-318.

[2] Chaum D, " Blind Signature for untraceable Payments", Advances in Cryptology-Crypto' 82, (1982) 199-203.

[3] Chaum D, Fiat A and Naor M, "Untraceable Electronic Cash" Advances in Cryptology CRYPTO '88, LNCS 403, Springer Verlag,(1988) 319-327.

[4] Chaum D , "Online Cash Checks" Advances in Cryptology-EUROCRYPT'89, LNCS 434, Springer-Verlag, (1989) 288-293.

[5] Hou X, Tan C H , "A New Electronic Cash Model",Proceedings of the International Conference on Information Technology, Coding and Computing (ITCC'05).

[6] Hou X, Tan C H, "On Fair Traceable Electronic Cash", Proceedings of the 3rd Annual Communication Networks and Services Research Conference (CNSR'05).

[7] Hankerson D, Menezes A and Vanstone S, "Guide to Elliptic Curve Cryptography", Springer Verlag New York, Inc,2004.

[8] Hans Delfs and Helmut Knebl, "Introduction To Cryptography, Principles and Applications",Springer ,(1998),91-109.

[9] Khalid O Elaalim and Shoubao Yang, "Secure Electronic Cash Using Elliptic Curve Cryptography Based On Zero Knowledge Proof", International Journal Of Cryptology Research ,3(1) : (2011) 15-26.

[10] Khalid O Elaalim and Shoubao Yang, "Electronic Cash System With Double Spending Tracing Based On Elliptic Curve Cryptography", Journal Of Computational Information Systems 6:9(2010), 2949-2957.

[11] Popescu C, "A Fair Off-line Electronic Cash System Based On Elliptic Curve Discrete Logarithm Problem", Studies in Informatics and Control, Vol. 14, No. 4,(2005) 291-298.

[12] Popescu C, " A Secure E-cash Transfer System based on the Elliptic Curve Discrete Logarithm Problem", Informatica, Vol.22, No. 3,(2011) 395-409.

[13] Ziba Eslami and Mehdi Talebi, "A New Fair Untraceable Off-Line Electronic Commerce Research and Applications , 10(2011) 59-66.

Authors Profile

Dr. C. PORKODI received her M.Sc. degree in Mathematics from Bharathiar University, Coimbatore, Tamil Nadu, India in 1992, and M.Phil degree in Mathematics from Madurai Kamaraj University, Madurai, Tamil Nadu, India in 2002. She is a rank holder in BSc and M.Sc degree courses. She completed her Ph.D degree in Mathematics with specialization "Cryptography", from Anna University, Chennai India in 2010. She has been serving as a faculty member in the Department of Mathematics, PSG College of Technology, India since 2000. Her research interest includes Number theory, Cryptography, and Wireless Sensor Networks.

Dr. K.SANGAVAI received her M.Sc. degree in Mathematics from Bharathidasan University, Trichy Tamil Nadu, Indiain 1992 and M.Phil degree in Mathematics from Anna University, Chennai, Tamil Nadu, India in 1993. She completed her Ph.D degree in Applied Mathematics with specialization "Graph Theory", from Bharathiar University, Coimbatore, Tamil Nadu, India in 2012.She is a rank holder in M.Sc degree course. She has been serving as a faculty member in the Department of Mathematics, PSG College of Technology, India, since 1999. Her research interest includes Graph Theory, Networks and Algorithms, Applications of Graph Theory and Statistics in Wireless Sensor Network.

