A Fair Off-line Electronic Cash System Based on Elliptic Curve Discrete Logarithm Problem

Constantin Popescu

Department of Mathematics and Computer Science

University of Oradea,

One Universitatii Street, Oradea

ROMANIA

Abstract: In this paper we present a new fair off-line electronic cash system based on Elliptic Curve Discrete Logarithm Problem. To achieve this, we employed the fair off-line electronic cash system based on discrete logarithm problem suggested by Popescu and Oros [17] and extended it on an elliptic curve over the finite field $GF(2^n)$. This naturally reduces the message size to 72% compared with the original scheme and makes it possible to handle a smart card. The anonymity of the system can be revokable under certain conditions by an off-line trusted third party.

Keywords: Cryptography, electronic cash system, blind signatures, elliptic curve discrete logarithm problem.

Constantin Popescu has received the Ph. D degree in 2001 in computer science (cryptography) at the Babes-Bolyai University, Cluj Napoca, Romania. Since April 2005 he is a Professor at the Department of Mathematics, University of Oradea, Romania. His current research interests include cryptography, network security, group signatures, security protocols, identification schemes, electronic payment systems.

1. Introduction

In some applications, it is necessary to protect the privacy of participants. Chaum [6] proposed in 1982 the first electronic payment system based on the technique of blind signatures in order to guarantee the privacy of customers. In an e-cash scheme there are three types of participants: the bank, merchants, and users. The users can withdraw coins from the bank and spend them at merchants. An e-cash scheme is online or offline. In the former case the bank is involved in every transaction, whereas in the second case payments can be performed without contacting the bank. Obviously offline schemes are preferable to online schemes. However, an electronic coin, being nothing but a string of numbers, can be copied and spent more than once, and in an offline scheme such double-spendings cannot be detected during the actual purchase. Rather than preventing double-spending, offline schemes are designed so that double-spenders are detected and identified. Privacy is a crucial ingredient of e-cash schemes. It is desirable that merchants cannot learn the identity of the user, or even determine whether two payments were made by the same user or not. Many schemes also provide the same privacy towards the bank. However, anonymity also works in favor of criminals using the scheme for illegal activities protected by the privacy offered. To protect against such events some schemes offer the possibility for trusted third parties to trace a payment. Most schemes require a merchant to deposit a coin after the purchase. A few schemes allow a coin to be transferred between users in several steps before it is deposited at the bank. Such schemes are said to have transferable coins. Another possible feature is divisibility, i.e., that a coin may be spent only in part.

The complete anonymity of electronic cash system can be used for blackmailing or money laundering. Von Solms and Naccache showed in [18] that anonymity could be used for blackmailing or money laundering by criminals without revealing their identities.

The concept of fair electronic cash system was put forth independently by Brickell [2] and Stadler [20]. It offers a compromise between the need of the privacy protection of customers and effectively preventing the misuse by criminals. On one hand, the bank and the merchant can not obtain the identities of customers by themselves. On the other hand, in the cases where there are suspect criminal activities (e.g. blackmailing or money laundering), the trusted third party, with the help of the bank, can revoke the anonymity of the customer or the coin.

Based on the system of Brands [1], Brickell proposed a fair electronic cash system [2], in which a trustee must be involved in the transactions. Camenisch extended his anonymous payment system [3] to be a fair payment system [5]. Frankel, Tsiounis and Yung proposed a fair off-line electronic cash system [7] which need more communication among the bank, the customers and the merchants.

Also, electronic payment systems with revokable anonymity have been proposed in [4], [8], [11], [15]. In these payment systems trusted third parties are able to revoke the anonymity of the customers in case of suspicious transactions. When illegal acts like blackmailing are disclosed, the trusted third party can block various attacks on payment systems by tracing the coins or the customer.

In this paper, we propose a new fair off-line electronic cash system based on elliptic curve discrete logarithm problem. The anonymity of users can be revoked in our double spending resistant system and our system has the ability to trace both the electronic coin and the owner of the electronic coin.

This paper is organized as follows. The next section presents elliptic curves over finite fields. In section 3, we present our fair off-line electronic payment system. Furthermore, we discuss the security and efficiency of this system in section 4. Finally, we conclude the work of this paper in the last section.

2. Elliptic Curves over Finite Fields

Many researchers have examined elliptic curve cryptosystems, which were firstly proposed by Miller [13] and Koblitz [9]. The elliptic curve cryptosystems which are based on the elliptic curve logarithm over a finite field have some advantages over other systems: the key size can be much smaller over the other schemes since only exponential-time attacks have been known so far if the curve is carefully chosen [10], and the elliptic curve discrete logarithms might be still intractable even if factoring and the multiplicative group discrete logarithm are broken.

Elliptic Curves over $GF(2^n)$: A non-supersingular elliptic curve E over $GF(2^n)$ can be written into the following standard form

$$E: \quad y^2 + xy = x^3 + ax^2 + b, \quad b \neq 0, a, b \in GF(2^n).$$

The points $P = (x, y)$, $x, y \in GF(2^n)$ that satisfy this equation, together with a "point at infinity" denoted O form an abelian group $(E, +, O)$ whose identity element is O.

Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be two different points on E and both P and Q are not equal to the infinity point. Addition law for E non-supersingular is as follow: For $2P = P + P = (x_3, y_3)$, if

$x_1 \neq 0$

$x_3 = \delta^2 + \delta + a$

$y_3 = (x_1 + x_3)\delta + x_3 + y_1, \quad where \quad \delta = x_1 + y_1/x_1.$

If $x_1 = 0$, $2P = O$. For $P + Q = (x_3, y_3)$, if $x_1 = x_2$, then $P + Q = O$. Otherwise,

$x_3 = \lambda^2 + \lambda + x_1 + x_2 + a$

$y_3 = (x_1 + x_3)\lambda + x_3 + y_1, \quad where\ \lambda = (y_1 + y_2)/(x_1 + x_2).$

Elliptic Curves over $GF(p^n)$: A non-supersingular elliptic curve E over $GF(p^n), \ p > 2$ can be written into the following standard form

$$E: \quad y^2 = x^3 + ax + b, \quad 4a^3 + 27b^2 \neq 0, a, b \in GF(p^n).$$

For the addition law, for the elliptic curve E over $GF(p^n)$, see more details in [12].

We give a definition of the elliptic curve discrete logarithm problem [16].

Definition 1. Let E be an elliptic curve defined over a finite field F_q and let $P \in E(F_q)$ be a point of order n. Given $Q \in E(F_q)$, the elliptic curve discrete logarithm problem is to find the integer $l, 0 \leq l \leq n-1,$ such that $Q = l \cdot P.$

3. The Proposed fair off-line Electronic Cash System

In this section, we propose a new fair off-line electronic cash system based on elliptic curve discrete logarithm problem.

An electronic cash system is composed of a set of protocols in which three participants are involved: a customer, a merchant and a bank. Basically, three protocols are included in an electronic cash system: withdrawal protocol involving the customer and the bank, payment protocol involving the customer and the merchant and deposit protocol involving the merchant and the bank. In our payment system will be added one more party, the trusted third party, and two more protocols acted between the bank and the trusted third party: customer tracing protocol and coin tracing protocol.

In Figure 1 we give the general model of an off-line electronic cash system.

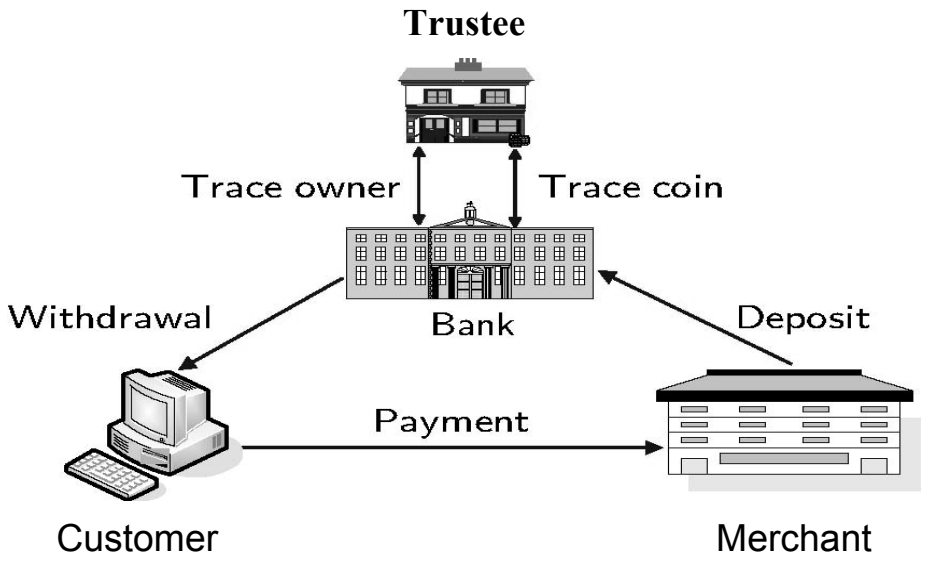

Figure 1: Off-line E-cash Model

3.1. System parameters

In this paper we use an elliptic curve E defined over a finite field F_q of characteristic p. The system parameters consist of:

1. a field size q, where q is a prime power (in practice, either $q = p$, an odd prime, or $q = 2^m$).
2. two field elements $a, b \in F_q$, which define the equation of the elliptic curve E over F_q (i.e., $y^2 = x^3 + ax + b$ in the case $p > 3$, where $4a^3 + 27b^2 \neq 0$).
3. two field elements x_p and y_p in F_q, which define a finite point $P = (x_p, y_p)$ of prime order in $E(F_q)$ ($P \neq O$, where O denotes the point at infinity).
4. the order n of the point P.
5. a one-way hash function, H, such as SHA-1 [14].

The Trusted Third Party:

The trusted third party executes the following to setup his parameters:

1. Select random secret x_t from the interval $[1, n-1]$.
2. Calculate the point $P_t = x_t \cdot P$
3. The public key of the trusted third party is P_t.
4. The corresponding secret key is x_t.

The Bank:
The bank executes the following to setup his parameters:

1. Select random secret x_b from the interval $[1, n-1]$.
2. Calculate the point $P_b = x_b \cdot P$
3. The public key of the bank is P_b.
4. The corresponding secret key is x_b.

The Customer:
The customer executes the next steps to setup his parameters:

1. Select random secret x_u from the interval $[1, n-1]$.
2. Calculate the point $P_u = x_u \cdot P$
3. The public key of the customer is P_u.
4. The corresponding secret key is x_u.

3.2. The Withdrawal Protocol

The withdrawal protocol involves the customer and the bank in which the customer withdraws an electronic coin from the bank.

The customer must to perform the following subprotocol with the bank:

1. The customer sends his electronic cash requirement:
   $m = H(withdrawalrequire \,||\, ID \,||\, time)$
   to the bank, where ID is the identity of the customer and H is a collision-resistant hash function. Then, the customer signs the message m using the elliptic curve signature scheme of Schnorr [19]:
   $$r_u = H(k_u \cdot P, m) \quad (1)$$
   $$s_u = k_u - r_u x_u (\mathrm{mod} n), \quad (2)$$
   where $k_u \in [1, n-1]$. The customer sends the signature (r_u, s_u) to the bank.
2. The bank checks that the following equality holds:
   $r_u = H(s_u \cdot P + r_u \cdot P_u, m).$
3. Then, the bank uses blind Schnorr signature [4] to sign the e-coin: selects $k' \in [1, n-1]$, computes the point $R = k' \cdot P = (x_1, y_1)$ and sends R to the customer.
4. The customer establishes a randomly coin c of 24 bit, randomly selects $\alpha, \beta \in [1, n-1]$, computes $R_b = R + \alpha \cdot P + \beta \cdot P_b$ and blind the e-coin by computing $c' = H(c, R_b) - \beta (\mathrm{mod} n)$. The customer sends the value c' to the bank.
5. The bank computes: $s' = k' - c' x_b (\mathrm{mod} n)$ and forwards s' to the customer.
6. The customer computes $s_b = s' + \alpha (\mathrm{mod} n)$. The pair (R_b, s_b) is a valid e-coin signature issued by the bank.
7. The bank computes $z_{ID} = x_1 (\mathrm{mod} n)$ and stores the pair (ID, z_{ID}) in his database.

The customer has to perform the following subprotocol with the trusted third party:

1. The customer sends (c, c', s', s_b, R, R_b) to the trusted third party.
2. The trusted third party verifies the signature of blinded coin:
   $$R = s' \cdot P + c' \cdot P_b. \quad (3)$$
   If the equality (3) does not hold, then the subprotocol fails. Otherwise, the trusted third party will accept the signature.
3. The trusted third party chooses a random number $k_t \in [1, n-1]$ and computes:
   $$r_t = H(k_t \cdot P, c) \quad (4)$$

$$s_t = k_t - x_t r_t (\mathrm{mod} n). \quad (5)$$

4. The trusted third party stores the pair (z_{ID}, c), where $z_{ID} = x_1 (\mathrm{mod} n)$ and x_1 is x-coordinate of R.
5. Finally, the trusted third party sends the pair (r_t, s_t) to the customer.

The e-cash is represented by the tuple $(c, r_u, s_u, s_t, r_t, s_b, R_b)$.

3.3. The Payment Protocol

The payment protocol involves the customer and the merchant in which the customer pays the electronic coin to the merchant.

1. The customer sends the tuple $(c, c', s', s_u, r_u, s_t, r_t, R, s_b, R_b)$ to the merchant.
2. The merchant verifies the validity of the signature (r_u, s_u) by checking that the following equality holds:
$$r_u = H(s_u \cdot P + r_u \cdot P_u, m). \quad (6)$$

From (1) and (2), we have:

$$r_u = H(k_u \cdot P - r_u x_u \cdot P + r_u x_u \cdot P, m) =$$
$$= H(k_u \cdot P, m) = r_u$$

3. The merchant verifies the validity of the signature (R_b, s_b) by checking that the following equality holds:
$$R = s' \cdot P + c' \cdot P_b. \quad (7)$$

We have:

$$R = s' \cdot P + c' \cdot P_b = (k' - c' x_b) P + c' x_b \cdot P =$$
$$= k' \cdot P - c' x_b P + c' x_b \cdot P = k' \cdot P = R$$

4. The merchant verifies the validity of the signature (r_t, s_t) by checking that the following equality holds:
$$r_t = H(s_t \cdot P + r_t \cdot P_t, c). \quad (8)$$

From (3) and (4), we have:

$$r_t = H(s_t \cdot P + r_t \cdot P_t, c) = H((k_t - x_t r_t) \cdot P + r_t x_t \cdot P, c) =$$
$$= H(k_t \cdot P - x_t r_t \cdot P + r_t x_t \cdot P, c) = H(k_t \cdot P, c) = r_t$$

If the equalities (6), (7) and (8) hold, then the merchant will accept the coin from the customer.

3.4. The Deposit Protocol

The deposit protocol involves the merchant and the bank as follows (the merchant deposits his electronic coins to the bank):

1. The merchant sends the e-cash $(c, r_u, s_u, s_t, r_t, s_b, R_b)$ to the bank.
2. The bank verifies the validity of the e-coin using the same operations as the merchant (see steps 2, 3 and 4 from subsection 3.3).
3. The bank checks whether the coin has been double spent. If the coin was not deposited before, the bank accepts the coin and will deposit the e-cash to the account of the customer. Then the merchant sends the goods to the customer.

If the coin was deposited before, then the bank requests the trusted third party that the identity of the dishonest customer to be revoked.

3.5. The Customer Tracing Protocol

The customer tracing protocol involves the bank and the trusted third party. This protocol is used to determine the identity of the customer in a specific payment transaction. Money laundering can be prevented from detecting the identity of the illegal customer in this protocol.
The customer tracing protocol is as follow:

1. The bank sends the e-coin $(c, r_u, s_u, s_t, r_t, s_b, R_b)$ and $R = (x_1, y_1)$ to the trusted third party.
2. The trusted third party verifies the validity of the e-coin using the same operations as the merchant (see steps 2, 3 and 4 from subsection 3.3), computes $z_{ID} = x_1 (\mathrm{mod} n)$ and sends z_{ID} to the bank. Note that z_{ID} is linked with the customer's identity in the database of the bank.
3. The bank can find the corresponding customer from his database (saved in the withdrawal protocol).

3.6. The Coin Tracing Protocol

The coin tracing protocol involves the bank and the trusted third party. This protocol determines the e-coin in the case when the blackmailing occurs. The blackmailing can be prevented in this protocol.

The coin tracing protocol is as follow:

1. The customer sends his identity, ID, to the bank.
2. The bank sends $R = (x_1, y_1)$ to the trusted third party.
3. The trusted third party computes $z_{ID} = x_1 (\mathrm{mod} n)$, finds the corresponding coin c and then sends the coin c to the bank. Note that z_{ID} is linked with the coin c in the trusted third party's database.
4. The bank can reject the coin c.

4. Security and Efficiency Analysis

In this section, we will analyze the security and efficiency of the proposed fair off-line electronic cash system.

Theorem 1. If the blind signature scheme is secure against forgery then the proposed e-cash system is secure against forgery of the coin.

Proof. If a dishonest customer tries to forge a valid e-coin, he must to generate a valid blind signature of the bank, (R_b, s_b). Since solving a elliptic curve discrete logarithm problem is infeasible (i.e. from the public key of the bank, $x_b \cdot P$, the customer can not compute the secret key of the bank, x_b we can say that the forgeability of the coin is impossible. □

Theorem 2. The anonymity of customers can be removed with the cooperation between the bank and the trusted third party in certain special cases.

Proof. The trusted third party records each pair (c, z_{ID}) in the withdrawal protocol and z_{ID} is linked with the identity of the customer. He can checks in his database the tracing information and provides it to the bank.

Theorem 3. The proposed fair off-line electronic cash system can protect the customer's privacy and keep the system anonymous.

Proof. Since the blind Schnorr signature (R_b, s_b) can not give any information for the coin c, the bank can not link the blind coin with the identity of the customer. Therefore, it is infeasible for the bank to trace honest customers without the help of the trusted third party. Also, in the payment protocol, the merchant can only verify the e-coin of the customer and the identity of the customer is anonymous. □

Our e-cash system increases an overall efficiency compared with the system in [17] in terms of the size of the message and the storage space. Assuming a prime modulus p and q in [17] to be 1024 bit and 160 respectively, we compare the system in [17] with our electronic cash system which has a point P of 160 and n of 160. The messages of payment phase $(c, \overline{r}, r_b, s_b, r_t, s_t)$ is 5144 bit in [17] and 1464 bit in our electronic cash system. Therefore, the proposed e-cash system has 72% reduction in the message size.

5. Conclusion

In this paper we proposed a new fair off-line electronic cash system with anonymity revoking trustee. Customer's anonymity can be removed by proceeding owner tracing and coin tracing under cooperating of the bank and the trusted third party. In our scheme the trusted third party verifies the bank's signature of the e-coin and then records the tracing information, which is different from conventional electronic cash system. The security of our system is based on the elliptic curve discrete logarithm problem.

REFERENCES

1. S. BRANDS, **Untraceable off-line cash in wallet with observers**, Advances in Cryptology-CRYPTO'93, Lecture Notes in Computer Science, vol. 773, Springer-Verlag, pp. 302-318, 1993.

2. E. BRICKELL, P. GEMMEL, and D. KRAVITZ, **Trustee-based tracing extensions to anonymous cash and the making of anonymous change**, *Proceedings of The 6th ACM-SIAM*, pp. 457-466, 1995.

3. J. CAMENISCH, J. PIVETEAU, M. STADLER, **An efficient payment system protecting privacy**, Proceedings of ESORICS'94, Lecture Notes in Computer Science, vol. 875, Springer-Verlag, pp. 207-215, 1994.

4. J. CAMENISCH, J. PIVETEAU, M. STADLER, **An efficient fair payment system**, Proceedings of ACM Conference on Computer and Communications Security, pp. 88-94, 1996.

5. J. CAMENISCH, U. MAURER, M. STADLER, **Digital Payment Systems with Passive Anonymity-Revoking Trustees**, Journal of Computer Security, vol. 5, number 1, IOS Press, 1997.

6. D. CHAUM, **Blind signatures for untraceable payments**, Proceedings of EUROCRYPT'82, pp. 199-203, 1983.

7. Y. FRANKEL, Y. TSIOUNIS, M. YUNG, **Indirect discourse proofs: Achieving efficient fair off-line e-cash**, Advances in Cryptology-ASIACRYPT'96, Lecture Notes in Computer Science, vol. 1163, Springer-Verlag, pp. 286-300, 1996.

8. A. JUELS, **Trustee tokens: Simple and practical anonynous digital coin tracing**, Lecture Notes in Computer Science, vol. 1648, Springer-Verlag, pp. 33-43, 1999.

9. N. KOBLITZ, **Elliptic curve cryptosystems**, Mathematics of Computation, 48, 1987, pp. 203-209.

10. N. KOBLITZ, **CM-Curves with Good Cryptographic Properties**, Proceedings of Crypto'91, 1992.

11. G. MAITLAND, C. BOYD, **Fair electronic cash based on a group signature scheme**, Proceedings of ICICS 2001, Lecture Notes in Computer Science, Springer-Verlag, pp. 461-465, 2001.

12. A. MENEZES, **Elliptic Curve Public Key Cryptosystems**, Kluwer Academic Publishers, 1993.

13. V. MILLER, **Uses of elliptic curves in cryptography**, Advances in Cryptology, Proceedings of Crypto'85, Lecture Notes in Computer Sciences, 218, Springer-Verlag, 1986, pp. 417-426.

14. National Institute of Standards and Technology, **Secure Hash Standard (SHS)**, FIPS Publication 180-1, 1995.

15. C. POPESCU, **An Off-line Electronic Cash System with Revokable Anonymity**, Proceedings of the 12th IEEE Mediterranean Electrotechnical Conference, Dubrovnik, Croatia, pp. 763-767, 2004.

16. C. POPESCU, **A Secure Key Agreement Protocol Using Elliptic Curves**, International Journal of Computers and Applications, vol. 27, 2005.

17. C. POPESCU, H. OROS, **A Fair Off-line Electronic Cash System with Anonymity Revoking Trustee**, Proceedings of the International Conference on Theory and Applications of Mathematics and Informatics, Thessaloniki, Greece, pp. 409-416, 2004.

18. B. VON SOLMS, D. NACCACHE, **On blind signatures and perfect crimes**, Computers and Security, 11(6), pp. 581-583, 1992.

19. C.P. SCHNORR, **Efficient signature generation for smart cards**, Journal of Cryptology, 4(3), 1991, 239-252.

20. M. STADLER, J.M. PIVETEAU, and J. CAMENISCH, **Fair blind signatures**, Proceedings of Eurocrypt'95, pp. 209-219, 1995.