International Journal of Security and Its Applications
Vol. 3, No. 4, October, 2009

A Novel Fair Tracing E-Cash System based on Elliptic Curve Discrete Logarithm Problem

Jayaprakash Kar[1] and Banshidhar Majhi[2]

[1]Department of Information Technology
Al Musanna College of Technology
Sultanate of Oman
[2]Department of Computer Science & Engineering
National Institute of Technology
Rourkela,INDIA
Jayaprakashkar@yahoo.com[1], bmajhi@nitrkl.ac.in[2]

Abstract

In this paper we have designed a fair e-cash system using Schnorr's one-time signature and Okamoto-Schnoor blind signature. In addition, the proposed e-cash system is constructed using elliptic curve cryptosystems (ECC) under the limited-storage environment for mobile devices such as smart cards, PDA etc able to efficiently store the coin streams. Furthermore, this system prevents criminal's activities by means of the two common cryptographic techniques double-spending detection and fair tracing.

Keywords*: Blind Signature, ECDLP, e-cash, fair-tracing*

1. Introduction

There have been many electronic cash (e-cash) protocols proposed with rapid improvement of information technologies and widespread diffusion of communication networks. David Chaum [1] proposed in 1982 the first electronic payment system based on the technique of blind signatures in order to guarantee the privacy of customers. This complete anonymity of electronic cash system can be used for blackmailing or money laundering. The cryptographic technique of blind signature based on RSA was proposed for protecting the customer's privacy. The blind signature is a protocol that the verifier can obtain a signature from the signer with out revealing the message, so that the signer can not link the signature to which he had signed. As a result, in the e-cash system the bank can not link the e-coins to their owner both in payment and deposit. Additionally, the e-coin is un-forged due to the signature is secure (in fact, there are not any efficient methods to forge a signature) .Therefore, the e-cash system with anonymity and un forge ability properties makes on-line business realizable Von Solms and Naccache showed in [2] 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 [3] and Stadler [5]. 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). In this paper, we propose a new fair off-line electronic cash system. 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. A secure and efficient e-cash system plays an important role to support ecommerce safely as a trustful payment over the Internet. In e-cash system, there are three basic entities, customer, bank and merchant. And there are also three activities, withdrawal, payment and deposit. A customer withdraws electronic coins from bank and pays the coins to a merchant in the off-line or on-line manner.
Finally, the merchant deposits the paid coins to a bank. In this process, there are many requirements which are anonymity, anonymous revocation, double spending prevention, off-line usage, transferability, divisibility and so on. We present a new fair-tracing off line electronic cash system based entirely on Elliptic Curve Discrete Logarithms. [15] [16].
Currently, along with the tremendous growth of the Internet, e-commerce for short brings business probability and riches. Especially in on-line business, the vendors can provide real/ electronic good sand services, and then the customers pay for them via the Internet. This means that making a transaction in the digital world is not a day dream any more. However, it is hard to realize online business due to the lack of convenient and secure methods. For example, image that the interaction between the physical customers and the Internet-based vendors could be monitored and recorded by some persons who use this information for direct marketing technique , determination of their credit -worthiness , and other legit-mate/illegitimate works . This unpleasant scenario is all ways arise repeatedly. More over, the e-coin may be intercepted, copied, and forged when being transmitted via the Internet. It is terrible that the economy of a country is suffered seriously if there are not any secure methods for transmitting coins. This paper is organized as follows. In section -2, we present the background where we brief overview of Elliptic Curve over finite field, Elliptic Curve Discrete Logarithm Problem (ECDLP), Fair Tracing and Double spending prevention .In section -3 and 4 present about the Off Line Electronic Cash System and the cryptographic requirement of an ideal e-cash system respectively. Section - 5 and 6 describes the Schnorr's One time Signature scheme and Okamoto-Schnorr Blind signature scheme respectively. In section -7 we present our proposed scheme. Furthermore, we discuss the security of this system in section-8. Finally, we conclude
the work of this paper in the last.

2. Background

In this section we brief overview of Elliptic Curve over finite field, Elliptic Curve Discrete Logarithm Problem, Fair Tracing and Double Spending prevention.

2.1 The finite field F_P

Let p be a prime number. The finite field F_P is comprised of the set of integers $0,1,2.....p-1$ with the following arithmetic operations [12] [13] [14]:

1. Addition: If $a,b \in F_p$ then $a+b=r$, where r is the remainder when $a+b$ is divided by p and $0 \le r \le p-1$. This is known as addition modulo p .
2. Multiplication: If $a,b \in F_p$ then $a.b=s$, where s is the remainder when $a.b$ is divided by p and $0 \le s \le p-1$.. This is known as multiplication modulo p .
3. Inversion: If a is a non-zero element in F_P , the inverse of a modulo p , denoted a^{-1} , is the unique integer $c \in F_p$ for which $a.c=1$.

2.2 Elliptic Curve over F_P

Let $p \geq 3$ be a prime number. Let $a, b \in F_p$ be such that $4a^3 + 27b^2 \neq 0$ in F_P. An elliptic curve E over F_P defined by the parameters a and b is the set of all solutions $(x, y), x, y \in F_p$, to the equation $y^2 = x^3 + ax + b$, together with an extra point O, the point at infinity. The set of points $E(F_p)$ forms a abelian group with the following addition rules [9]:

1. Identity: $P + O = O + P = P$, for all $P \in E(F_p)$.
2. Negative : if $P(x, y) \in E(F_p)$ then $(x, y) + (x, -y) = O$, The point $(x, -y)$ is dented as $-P$ called negative of P.
3. Point addition: Let $P(x_1, y_1), Q(x_2, y_2) \in E(F_p)$, then $P + Q = R \in E(F_p)$ and coordinate (x_3, y_3) of R is given by $x_3 = \lambda^2 - x_1 - x_2$ and $y_3 = \lambda(x_1 - x_3) - y_1$ where $\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$
4. Point doubling : Let $P(x_1, y_1) \in E(F_p)$ where $P \neq -P$ then $2P = (x_3, y_3)$ where $x_3 = (\dfrac{3x_1^{\ 2} + a}{2y_1})^2 - 2x_1$ and $y_3 = (\dfrac{3x_1^{\ 2} + a}{2y_1})(x_1 - x_3) - y_1$

2.3 Elliptic Curve Discrete Logarithm Problem (ECDLP)

Given an elliptic curve E defined over a finite field F_p ,a point $P \in E(F_p)$ of order n, and a point $Q \in (P)$, find the integer $l \in [0, n-1]$ such that $Q = l.P$. The integer l is called discrete logarithm of Q to base P, denoted $l = \log_p Q$ [16].

2.4 Fair Tracing

To protect the privacy of customers, each payment should be anonymous and it can be achieved by blind signature.However von Solms and Naccache [4] have shown that unconditional anonymity may be misused for untraceable blackmailing of customers, which is also called perfect crime. Furthermore, unconditional anonymity makes ease money laundering, illegal purchase, and bank robbery. Due to these anonymity related problems, tracing of payment systems with revocable anonymity [5], [7] have been invented. There are two types of tracing mechanism: Coin tracing and Owner tracing. This mechanism of e-cash is better feature compared with physical cash. Because coin and owner tracing is almost impossible in real world. But these two tracing mechanisms have one common problem, called the fair-tracing-problem: No one is able to control the legal usage of tracing, leading to the possibility of illegal tracing. Kugler and Vogt proposed a new kind of tracing mechanism [11]which guarantees stronger privacy than any other known approaches, although their fair coin tracing can be carried out by the bank without any help of trusted third parties. They

called their withdrawal-based scheme as optimistic fair tracing, which means that the decision whether the coins should be traceable or not must be made at their withdrawal. This protocol cannot prevent illegal tracing, but can detect it afterwards by the traced person. If it turns out to be illegal, then he can prove it to a judge and the tracer (bank) will be prosecuted. However, we propose a withdrawal based real fair tracing protocol and show that it has an enhanced computational complexity.

2.5 Double Spending prevention

Off-line digital cash systems are more preferable than on-line cash systems, since in off-line digital cash systems banks do not need to be involved in payment process. There have always been two major concerns for off-line systems double spending and customer's privacy. In particular, double-spending is a serious threat for off-line schemes [8]. In on-line e-cash system, double spending prevention mechanism can be achieved easily. While spending, the coins are securely transferred to the merchant. The merchant verifies the coins by sending them to the bank. After ascertaining that the coins are not double spent, the bank credits the merchants account and the coin is destroyed. If the coin is double spent, the bank sends an appropriate message to abort the transaction [9]. Our protocol focused on anonymity and its revocation functions. Basically, our coin stream is blinded and anonymous. So, using only this coin stream, bank cannot differentiate each coin without revealing its anonymity. So, it is hard for bank to prevent double spending.

3. Off Line Electronics Cash System

3.1 Overview

An e-cash system is a set of parties with their interactions, exchanging money and goods. A typical e-cash system has three parties:

- Customer: purchases goods or services from merchant using e-cash.
- Merchant: sells goods or services to customer, and deposits e-cash to bank.
- Bank: issues e-cash and maintains bank account for customers and merchants.

And there are also three activities, withdrawal, payment and deposit. A customer withdraws electronic coins from bank and pays the coins to a merchant. Finally, the merchant deposits the paid coins to the bank.

3.2 Anonymity Problem

It is often believed that electronic cash systems cannot simultaneously offer privacy for the users as well as security for the banks and shops. Many of the systems that are nowadays in use completely lack anonymity of users and in addition are on line in order for shops to be able to check the credibility of payers With the advent of public key cryptography techniques have been developed that show that this belief is unjustified These techniques initialized by allow the construction of off line electronic cash systems that are secure albeit under certain intractability assumptions for the bank yet at the same time honest users of the system are guaranteed to remain completely anonymous. This holds in a very strong sense the security of banks is not compromised even if all users and shops collaborate in such an attempt and the

privacy of honest users cannot be violated in any cryptanalytic way even under adversarial behavior of the bank in coalition with all the shops the fact that such systems can be off line reduces a lot of the overhead expenses and inflexibility of on line cash systems. In 1982, Chaum [1] showed how to build anonymous electronic cash system by devising blind signature schemes. Chaums scheme is provably anonymous: even an all powerful agent that collaborates with the bank and any coalition of the customers can not link payments to withdrawals, i.e. customers enjoy unconditional anonymity. In 1992 von Solms and Naccache [4] discovered a serious attack on Chaums payment system. Blackmailers could commit a perfect blackmailing crime by using anonymous communication channels and anonymous e-cash. Following that, further concerns were raised, e.g., it was argued that the ability to move money around anonymously at the speed of light may facilitate money laundering activities and tax evasion. Due to these anonymity problems, e-cash with revocable anonymity has been requested by governments and banks, and tracing methods have been invented, where the withdrawal and the deposit of coins can linked by two complementary tracing mechanisms [5] .

- Coin tracing: Is the withdrawn coin is deposited?
- Owner tracing: Who is the withdrawer of this deposited coin?

Tracing mechanism of e-cash can be achieved effectively by introducing trusted third party [7]. But that is a big assumption to realize of e-cash system, and that causes additional costs. To make matters worse, the achieved level of anonymity is uncertain and any misuse of tracing by TTP can not be detected. Recent one example of them is escrowed cash system. In this system, payment transactions look anonymous from the outside (to customers, merchants, banks), while Trustees are able to revoke the anonymity of each individual payment transaction. But in this scheme, criminals may still be able to hide their suspicious activities in an escrowed system in a way that is hard to detect. Sander and Ta-Shma [17] argue that escrowed cash is not a natural solution to some of the major attacks on electronic cash systems (blackmailing and bank robbery) that are caused not by the anonymity feature but rather stem from the fact that 7 most anonymous cash systems are implemented using signature based schemes. Therefore, recent approaches are not use TTP tracing [18] [10]. But they only protect against blackmailing and lack support for coin and owner tracing. And these payment systems require the bank to be on-line at payment. Kugler and Vogt [11] proposed offline payment system without TTP using marking mechanism. X. Chen et.al tried an off-line scheme using group blind signature [19]. In this thesis, we analyze the Kuglers mechanism and propose a true fair tracing mechanism of e-cash. Fair tracing means that legal tracing is always possible, but illegal tracing is inhibited. In here, if the tracing has been permitted by judge or withdrawer (customer), then that tracing is legal, otherwise illegal.

4. Cryptographic Requirements

An ideal e-cash system must satisfy the following properties:

- Unforgeability : the valid e-cash cannot forged.
- Anonymity: anyone cannot trace e-cash owner and cannot know what the customer bought.
- Anonymous revocation: legal coin or owner tracing is possible to prevent crimes.
- Double spending prevention: the same e-cash must not allow spending twice.

- Off-line: when a customer gives e-cash to a merchant, it is not need to connect to the bank on-line.
- Transferability: when a customer receives an e-cash in a transaction, he may spend it without depositing the coin first and getting a new e-cash issued from bank.
- Divisibility: we can divide money into arbitrary part/fractions.

Some of these requirements is not absolute condition for use some kind of e-cash. For example, un-forgeability and double spent prevention are essential conditions, but off-line is not. Depending on the payment method in e-commerce, the requirements are changed. For example, credit-based electronic money, anonymity is not allowed.

5. Schnorr's One-time Signature

We have used Schnoor's One-time Signature scheme in our system. The security of the scheme depends on the difficulty of solving Elliptic Curve Discrete Logarithms Problem (ECDLP). To sign a message M the signer proceeds as follows:

Each user generates a secret signing key s_k at random and such that $0 < s_k < p$, Public key is $P_k = s_k.P$.

- Signer chooses a random ephemeral key: $0 < \delta < p$.
- Signer computes $\widetilde{P} = \delta.P$
- Signer computes one-way hash $\widetilde{c} = H(\widetilde{P} \parallel M)$.
- Finally, signer computes $d = (\delta + \widetilde{c}.s_k) \bmod p$.

The signature on M is the pair $(\widetilde{c}, d)$.
To verify the signature $(\widetilde{c}, d)$ on message M under public key P_k, the verifier proceeds as follows:

- The Verifier computes $\widetilde{P} = d.P - \widetilde{d}.P_k$, so that the signature is valid we have $\widetilde{P} = (\delta + \widetilde{c}.s_k).P - s_k.\widetilde{c}.P$.
- So the Verifier accepts signature if and only if $\widetilde{c} = H(\widetilde{P} \parallel M)$.

6. Okamoto-Schnorr Blind Signature

Schnorr blind signature scheme was first introduced in (Okamoto,1992). The protocol requires three round of interaction between signer and recipients' i.e in our e-cash system between the Bank and Customer. Chaum [1] proposed the notion of blind digital signatures as a key tool for constructing various anonymous electronic cash instruments. Informally, a blind digital signature scheme may be thought of as an abstract game between a customer and a bank. A customer has a secret document for which she needs to get the signature from a bank. She should be able to obtain this signature without revealing to the bank anything about her document except its length. On the other hand, the security of the signature scheme

should guarantee that it is difficult for the customer to forge a signature of any additional document, even after getting from the bank a number of blind signatures. Since the scheme is based on Elliptic Curve Discrete Logarithm Problem (ECDLP), the security depends on the difficulty of solving ECDLP.

Let's assume that the sender A (the customer) does not want the signer B (the bank) to be capable of associating a postiori message m and a signature $Sig_B(m)$ to a specific instance of the protocol. This may be important in electronic cash applications where a message m might represent a monetary value which A can spend. When and $Sig_B(m)$ are presented to B for payment, B is unable to deduce which party was originally given the signed value. This allows remaining anonymous so that spending patterns cannot be monitored. A blind signature protocol required the following components [6]:

1. A digital signature mechanism for signer B. $Sig_B(X)$ denotes the signature of B on X.
2. Function f and g (known only to the sender) such that $g(Sig_B(f(m))) = Sig_B(m)$. f is called a blinding function, g an un-blinding function and $f(m)$ a blinded message.

Let the elliptic curve E defined over the finite field F_p and the parameters p and q are the prime factors of $p-1$. Let Q and R be any two points in $E(F_p)$. The private key of the bank (Signer) for blind signature is the pair (s_1, s_2), where $s_1, s_2 \in Z_q$. Bank's Public key is (Q, R, V), where $V = s_1.Q + s_2.R$. The scheme follows the following steps.

- Bank (Signer) picks random numbers $k_1, k_2 \in Z_q$, computes $X = k_1.Q + k_2.R$, and sends X to the Customer.
- Customer picks random numbers $\beta, \gamma, \delta \in Z_q$ and computes $L = X + \beta.Q + \gamma.R + \delta.V$ and $e = H(m \parallel L) - \delta$. Customer sends e to the Bank. Here m is a message to be signed.
- Bank computes $\alpha_1 = k_1 - e.s_1 \bmod q$ and $\alpha_1 = k_2 - e.s_2 \bmod q$ sends the pairs (α_1, α_2) to the Customer.
- Customer compute $\rho = \alpha_1 + \beta \bmod q, \sigma = \alpha_2 + \gamma \bmod q.(L, \sigma, \rho)$ is the Bank's signature.

Verification of signature is to be checked by the following equation.

$$L = \rho.Q + \sigma.R + H(m \parallel L).V \quad (1)$$

Verification: $\rho.Q + \sigma.R + H(m \parallel).V$

$$= (\alpha_1 + \beta).Q + (\alpha_2 + \gamma).R + H(m \| L).V$$
$$= (k_1 - e.s_1).Q + \beta.Q + (k_2 - e.s_2).R + \gamma.R + H(m \| L).V$$
$$= X + \beta.Q + \gamma.R + (H(m \| L) - e.V = L$$

7. Proposed Scheme

In this section we describe our scheme and combines Schnorrs one-time signature and Okamoto-Schnorr blind signature in order to make a more practical e-cash system. We consider 3-parties, customer, merchant and bank. Bank and customer can trace the coin to block blackmailing and kidnapping. Revealing of modified undeniable signature has no impact on Okamoto- Schnorr blind signature. We use one-time signature to prevent coin double spending in payment stage.

The system is composed of a set of protocols in which the three participants a customer, a merchant and a bank are involved that we have described in above section. The three protocols are withdrawal protocol involving the customer and the bank, payment protocol involving the customer and the merchant and deposit and verification protocol involving the merchant and the bank. Our payment protocol add trusted third party and two more protocols acted between the bank and the trusted third party that are Fair tracing protocol and Double Spending protocol.

7.1 System parameters

Let $p \geq 3$ be a prime number. Let $a, b \in F_p$ be such that $4a^3 + 27b^2 \neq 0$ in F_P. An elliptic curve E over F_P defined by the parameters a and b is the set of all solutions $(x, y), x, y \in F_p$, to the equation $y^2 = x^3 + ax + b$, together with an extra point O, the point at infinity.

1. The Bank :
   The Bank executes the following set up his parameters.
   - Select random secret s_1 and s_2 from the interval $[1, n-1]$.
   - Bank's blind signature private key is (s_1, s_2) .
   - Bank's Public key is (Q, R, V), where $V = s_1.Q + s_2.R$.
2. The Customer:
   - Select the random secret key s_k from the interval $[1, n-1]$.
   - Compute $P_k = s_k.P$.
   - The Public key of the Customer is P_k.
   - The Private key is s_k.
3. The Trusted Third Party:

The trusted third party executes the following to set up his parameters:
   - Select the random secret key u_t from the interval $[1, n-1]$.
   - Compute $P_t = u_t.P$.
   - The Public key of the trusted third party is P_t.

- The private key is u_t.

3. A one-way Hash function H such as SHA-1 or $MD5$.

7.2 Withdrawal Protocol

The withdrawal protocol involves the Customer and Bank in which the Customer withdraw an electronic coin from the Bank. In this protocol Customer receives the expiration date of validity time T_v, create a coin message $\tilde{m}$ and take the blind signature from the bank. Finally Customer generates a coin stream. So the Customer performs the following sub-protocol with the Bank.

1. Bank selects random number r from $[1, n-1]$, compute $U = r.R$ and sends it to the Customer.
2. For every coin, Customer selects a random number δ from $[1, n-1]$ and calculates $\tilde{U} = \delta.U$.
3. Bank selects random numbers k_1 and k_2 from $[1, n-1]$ and compute $T = k_1.Q + k_2.U$. Also fix the expiration date of validity time T_v and signed on it. Then sends $T, T_v, Sig_{bank}(T_v)$ to Customer.
4. Customer generate coin message $\tilde{m} = m \parallel T_v \parallel Sig_{bank}(T_v) \parallel ID$, where ID is the identity of the Customer .Selects random numbers $(\beta_1, \beta_2, \gamma)$ from the interval $[1, n-1]$. Calculate $\tilde{T} = T + \beta_1.Q + \beta_2.U + \gamma.V$ and $\tilde{c} = H(\tilde{m}, \tilde{U}, \tilde{T})$ and $c = \tilde{c} - \gamma$.
   Then Customer sign the coin message element c using the following signature scheme of Schonner.

   - Customer selects random ephemeral key: $0 < \delta < p$.
   - Computes $\tilde{P} = \delta.P$.
   - Computes $d = (\delta + \tilde{c}.s_k) \bmod p$.

   Signature on the coin message element c is the pair $(d, \tilde{P})$. Then Customer sends the the signature $(d, \tilde{P})$ to the Bank. Bank checks that the following equation holds.

   $$\tilde{P} = d.P - \tilde{c}.P_k \qquad (2)$$

5. Then Bank generate blind signature using Okamoto-Schnorr Blind Signature scheme. The sub-protocol which is performed by both the Bank and the Customer is as follows:

   - The Bank Computes $\alpha_1 = k_1 - c.s_1 \bmod p$, $\alpha_2 = k_2 - c.s_2.r^{-1} \bmod p$ and send the pair (α_1, α_2) to the Customer.
   - Customer calculates $\tilde{\alpha}_1 = \alpha_1 + \beta_1 \bmod p$ and $\tilde{\alpha}_2 = \delta^{-1}.\alpha_2 + \beta_2 \bmod p$
   - The Bank computes $C_{ID} = x_1 \bmod p$ where $T = (x_1, y_1)$.

- The Bank store (ID, C_{ID}) in his database.
- Finally generate the stream $(\tilde{m}, \tilde{T}, \tilde{\alpha}_1, \tilde{\alpha}_2, \tilde{U})$.

The reliance of the coin can be achieved by blind signature verification. In this step all necessary values are needed for verification can be extracted from the stream $(\tilde{m}, \tilde{T}, \tilde{\alpha}_1, \tilde{\alpha}_2, \tilde{U})$ and Bank's public key (Q, R, V). For verification any one can check by the following equation.

$$\tilde{T} = \tilde{\alpha}_1.Q + \tilde{\alpha}_2.\tilde{U} + \tilde{c}.V \quad (3)$$

$\tilde{c}$ can be calculated from the following equation

$$\tilde{c} = H(\tilde{m}, \tilde{U}, \tilde{T}) \quad (4)$$

Verification:-

$$\begin{aligned}
&\tilde{\alpha}_1.Q + \tilde{\alpha}_2.\tilde{U} + \tilde{c}.V \\
&= (\alpha_1 + \beta_1).Q + (\delta^{-1}.\alpha_2 + \beta_2).\tilde{U} + \tilde{c}.V \\
&= \alpha_1.Q + \beta_1.Q + \delta^{-1}.\alpha_2.\tilde{U} + \beta_2.\tilde{U} + \tilde{c}.V \\
&= \alpha_1.Q + \beta_1.Q + \alpha_2.U + \beta_2.\tilde{U} + \tilde{c}.V \\
&= (k_1 - c.s_1).Q + \beta_1.Q + (k_2 - c.s_2.r^{-1}).U + \beta_2.\tilde{U} + \tilde{c}.V \\
&= k_1.Q - c.s_1.Q + \beta_1.Q + k_2.U - c.s_2.r^{-1}.U + \beta_2.\tilde{U} + \tilde{c}.V \\
&= T + \beta_1.Q + \beta_2.\tilde{U} + \tilde{c}.V - c.s_1.Q - c.s_2.r^{-1}.U \\
&= T + \beta_1.Q + \beta_2.\tilde{U} + \tilde{c}.V - c.s_1.Q - c.s_2.R \\
&= T + \beta_1.Q + \beta_2.\tilde{U} + (c + \gamma).V - c.s_1.Q - c.s_2.R \\
&= T + \beta_1.Q + \beta_2.\tilde{U} + c.V + \gamma.V - c.V \\
&= T + \beta_1.Q + \beta_2.\tilde{U} + \gamma.V \\
&\tilde{T}
\end{aligned}$$

The Customer has to perform the following sub-protocol with the trusted third party:

1. The Customer sends the stream $(\tilde{m}, \tilde{T}, \tilde{\alpha}_1, \tilde{\alpha}_2, \tilde{U})$ with T to the trusted third party.
2. The trusted third party verifies the signature of the blinded coin by equation- (2). If the equation does not hold then the sub-protocol fails. Otherwise, the trusted third party will accept the signature.
3. The trusted third party generate the signature as follows:

- Select random ephemeral key $0 < \eta < p$.
- Compute $P' = \eta.P$.
- Compute $s = (\eta + \tilde{c}.u_t) \bmod p$.

4. The trusted third party sends the signature pair (P', s) to the Customer.
5. The trusted third party calculate $C_{ID} = x_1 \bmod p$ and stores C_{ID} and the stream $(\tilde{m}, \tilde{T}, \tilde{\alpha}_1, \tilde{\alpha}_2, \tilde{U})$. The coin stream or e-cash is represented by $(\tilde{m}, \tilde{T}, \tilde{\alpha}_1, \tilde{\alpha}_2, \tilde{U}, P', s)$.

7.3 Payment Protocol

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

1. The Customer sends the Coin $(\tilde{m}, \tilde{T}, \tilde{\alpha}_1, \tilde{\alpha}_2, \tilde{U}, P', s)$ to the Merchant.
2. The Merchant verifies the blind signature by equation-(2) extracting the parameters that are needed for verification.
3. Finally the Merchant will verify the truth of one-time signature i.e the signature pair (P', s) by the following equation.

$$P' = s.P - \tilde{c}.P_t \tag{5}$$

7.4 Deposit Protocol

This protocol involves the Merchant and the Bank. Here Merchant will send the coin to the Bank. But some time, one more interaction can be performed for tracing or double spending prevention. For this the following two protocols Fair Tracing and Double Spending can be performed.

1. The Merchant send the coin $(\tilde{m}, \tilde{T}, \tilde{\alpha}_1, \tilde{\alpha}_2, \tilde{U}, P', s)$ to the Bank.
2. The Bank check the expiration date T_v each coin has a time limit for usage.
   So, all coin must be deposited to the Bank by expiration date T_v. And Bank will maintain the spent coin until T_v.
3. The Bank checks the validity of the e-coin by verifying the one-time signature of the trusted third party by equation-(5) and the blind signature of the bank by equation-(3).
4. The Bank verifies 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.

7.5 Fair Tracing protocol

The Fair 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:

- The bank sends the e-coin $(\tilde{m}, \tilde{T}, \tilde{\alpha}_1, \tilde{\alpha}_2, \tilde{U}, P', s)$ and $T = (x_1, y_1)$ to the trusted third party.
- The trusted third party verifies the validity of the coin using the equation- (4). Computes $C_{ID} = x_1 \bmod p$ and send C_{ID} to the bank. Note that C_{ID} is linked with the customer's identity in the database of the bank.
- The Bank can find the corresponding customer from his database which has been saved in the withdrawal protocol.

7.6 Double Spending Protocol

The double spending protocol involves the Bank and the trusted third party. This protocol determines the e-coin in case when the black mailing occurs. The black mailing can be prevented in this protocol. Further each coin has a time limit for usage. So, all coin must be deposited to the bank by expiration date T_v. And bank will maintain the spent coin until T_v. In on-line e-cash system, when a merchant received a coin, he can request to the bank whether the coin is already on spent coin list or not. If the coin is in the spent list, the merchant will abort the transaction. So, merchant need not request the one-time signature of customer to the trusted third party. In off-line system, real time double spending prevention is impossible, but detection is possible using the same mechanism of on-line system through depositing coins on expiration date T_v. One-time signature can be a solution for this problem. In previous stage, customer chooses unique one-time random number δ for each coin, and received the banks blind signature. So, δ is a important blinding factor and combined with blind signature. So, if customer uses it more than once for different coin message $\tilde{m}$ customers secret key will be exposed. So, customer will not try to use a coin more than once. Otherwise, on final date T_v, double spending can be detected, and bank can reveal the criminal in cooperation with the trusted third party. The double spending protocol is as follow:

1. The customer sends his identity ID to the bank.
2. The bank sends $T = (x_1, y_1)$ to the trusted third party.
3. The trusted third party computes $C_{ID} = x_1 \bmod p$ and finds the corresponding coin stream $(\tilde{m}, \tilde{T}, \tilde{\alpha}_1, \tilde{\alpha}_2, \tilde{U}, P', s)$ and then sends the coin to the bank. Note that C_{ID} is linked with the coin in the trusted third party database.
4. The Bank can reject the coin or check for double spending.

8. Security Analysis

We will analyze the security of the proposed fair off-line electronic cash system in this section. The security of our system is based on Elliptic curve Discrete Logarithm Problem (ECDLP).

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 $(\tilde{\alpha}_1, \tilde{\alpha}_2)$ from the Public key (Q, R, V) of Bank .That is the intruder intends to break

the signature schemes, he (she) has to solve the Elliptic Curve Discrete Logarithm Problem. An attacker intends to reveal the secret keys (s_1, s_2) and generate the part $(\widetilde{\alpha}_1, \widetilde{\alpha}_2)$ of the valid coin stream by knowing the public keys (Q, R, V) . For that he has to solve Elliptic Curve Discrete Logarithm Problem which is computationally infeasible. We can say that forge ability of the coin is impossible.

Theorem 2 *The proposed fair off-line electronic cash system can protect the Customer's privacy and keep the system anonymous.*

Proof: Since the Okamoto-Schnorr blind signature $(\widetilde{T}, \widetilde{\alpha}_1, \widetilde{\alpha}_2)$ can not give any information for the coin, 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.

9. Conclusion

E-cash system is going to be important issue and application in current E-commerce. Obviously due to requirement of being similar to analog money and protecting some illegal crime, a revocable e-cash system is discussed and recommended.

We propose a new fair off-line e-cash system with anonymity revoking trustee .The security of our system is based on Elliptic Curve Discrete Logarithm Problem (ECDLP). The primary reason for the attractiveness of ECC over systems such as RSA and DSA is that the best algorithm known for solving the underlying mathematical problem (namely, the ECDLP) takes fully exponential time. In contrast, sub-exponential time algorithms are known for underlying mathematical problems on which RSA and DSA are based, namely the integer factorization (IFP) and the discrete logarithm (DLP) problems. This means that the algorithms for solving the ECDLP become infeasible much more rapidly as the problem size increases than those algorithms for the IFP and DLP. For this reason, ECC offers security equivalent to RSA and DSA while using far smaller key sizes. The attractiveness of ECC will increase relative to other public-key cryptosystems as computing power improvements force a general increase in the key size. The benefits of this higher-strength per-bit include higher speeds, lower power consumption, bandwidth savings, storage efficiencies, and smaller certificates. Since our proposed e-cash system is constructed using elliptic curve cryptosystems (ECC) it is more efficient than the other e-cash system which are based on IFP or DLP.

References

[1] D. Chum "Blind signatures for untraceable payments",Crypto 82,pp.199203, 1982.
[2] B. von Solms, D. Naccache "On blind signatures and perfect crimes", Computers and Security, 11(6), pp. 581- 583, 1992.
[3] Trustee-based tracing E. Brickell, P. Gemmel, and D. Kravitz, extensions to anonymous cash and the making of anonymous change, Proceedings of The 6th ACM-SIAM, pp. 457-466, 1995.
[4] B. Von Solms and D. Naccache "On blind signatures and perfect crimes", Computers and Security 11(6), pp.581583, 1992.
[5] M. Stadler, J. M. Piveteau and J. Camenisch "Fair blind signatures, Advances in Cryptology - EUROCRYPT 95, LNCS 921,Springer-Verlag, pp.209219, 1995.
[6] A.J. Menezes, P. v. Oorschot and S.Vanstone "Handbook of Applied Cryptography", CRC press LLC, pp.475, 1996.

[7] G. Davida, Y. Frankel Y. Tsiounis and M. Yung, ”Anonymity control in e-cash systems”, Financial Cryptography - FC97, LNCS 1318, Springer-Verlag,pp.116,1997.
[8] K. Q Nguyen, Y. Mu, and V. Varadharajan ”One-Response Off-Line Digital Coins”, Proceedings of SAC 97, 1997.
[9] R. Sai Anand and C. E. Veni Madhavan ”An Online, Transferable E-Cash Payment System”, INDOCRYPT 2000, LNCS1997, pp.93-103, 2000.
[10] B. Pfitzmann and A. R. Sadeghi ”Slef-escrowed cash against user blackmailing”, Financial Cryptography - FC 2000, LNCS 1962,Springer-Verlag ,pp.4252, 2001
[11] D. Kugler and H. Vogt”Fair tracing without trustees”, Financial Cryptography FC 2001, Preproceedings, 2001.
[12] N. Koblitz. A course in Number Theory and Cryptography, 2nd edition Springer-Verlag-1994
[13] K. H Rosen ”Elementary Number Theory in Science and Communication”, 2nd ed., Springer-Verlag, Berlin, 1986.
[14] A.Menezes, P. C Van Oorschot and S. A Vanstone Handbook of applied cryptography. CRC Press, 1997.
[15] D. Hankerson, A .Menezes and S.Vanstone. Guide to Elliptic Curve Cryptography, Springer Verlag, 2004.
[16] ”Certicom ECC Challenge and The Elliptic Curve Cryptosystem” available :http://www.certicom.com/index.php.
[17] T. Sander and A. Ta-Shma ”On Anonymous Electronic Cash and Crime”,ISW, pp.202206, 1999.
[18] T. Sander and A. Ta-Shma, ”Auditable, Anonymous Electronic Cash”,CRYPTO 99, LNCS 1648, Springer-Verlag, pp.555572,1999
[19] X. Chen, F. Zhang and Y. Wang ”A New Approach to Prevent Blackmailing in E-Cash” available from http://eprint.iacr.org/2003/055/, 2003.

Authors

Jayaprakash Kar has completed his M.Sc and M. Phil. in Mathematics from Sambalpur University, M.Tech in Computer Science from Utkal University, and pursuing Ph.D at Utkal University, Bhubaneswar, India. He has 5 years of industry experience in Bharat Earth Movers Limited in EDP department. He has completed 6 years of teaching in Engineering College and IGNOU Study center to MCA and BCA students. Mr. Kar is presently working as a Lecturer at Department of Information Technology, Al Musanna College of Technology, Ministry of manpower, Sultanate of Oman. His research areas are on Cryptography & Network Security, Biometrics and Web Security.

Prof. Banshidhar Majhi is currently working as a professor and head of the Department of Computer Science and Engineering at National Institute of Technology, Rourkela, India. He has completed his M.Tech and Ph.D. from Sambalpur University. He has 15 Journal papers and 60 Conference articles to his credit. His research interests include image processing, cryptography and network security, soft computing.