ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 2, No 5, May 2013

Security Analysis of Fair E-cash Payment System

Thae Nu Nge

***Abstract*— In e-commerce, e-payment is one of the most essential research areas. Properly combining the payment protocol with a fair exchange procedure, the payment system allows the consumer and the merchant to fairly exchange their money and merchandise. This paper analysis and addresses the security flaws in a fair e-cash payment system which is based on DSA signature with message recovery and proposes a solution that would ensure user authentication and data integrity. The improved system also defences against threats and misbehaviors related to unfairness and repudiation coming from insiders parties of the transaction.**

***Index Terms*— e-commerce, fairness, security, offline, e-cash**

I. INTRODUCTION

The more business is conducted over the Internet, the greater the fair exchange problem is. The fairness has been described with a lot of definitions. The fair exchange ensures no parties gains advantage over the other party by misbehaving [2]. In other words, an exchange is said to be fair if at the end of transaction, each participant receives the expected item or neither dishonest participant receives any valuable information about the other's item [11,14]. During the last decade, the researches proposed e-cash systems with fairness between consumer and merchant. Integrating fair exchange procedure with the payment protocol, the fair e-cash system, allows the consumer and merchant to exchange fairly their money and merchandise [2].

According to the participation of trusted third party (or bank), electronic cash systems can be classified into two types: online and offline. In an online e-cash system, the issuing bank should play a part in the payment protocol to verify the e-cash [12]. Although it is a simple way to ensure of the validity of payments, it can lead to the bottle-neck of a transaction and become network congestion. An off-line system can enhance performance [5] in which the bank is not involved during the payment procedure.

The fairness of the e-cash scheme can be maintained with the help of an offline trusted third party (offline TTP or bank). That is, the consumer and the merchant can exchange their desired items without TTP's participation. However, only when a party misbehaves, honest party can request the TTP to resolve the problem and ensure the fairness of the transaction.

Numerous mechanisms have been proposed for offline e-cash system in the last decade. Most of these systems assumed that the banks and other third authorities are trustworthy and they did not consider the insider attacks by untrusted authorities [6]. In paper [1] proposed an efficient e-cash system based on DSA multi-signature in which there is no withdrawal stage and e-cash is produced by consumer. It is very efficient because of not only reducing communication cost but also avoiding the storage and lose problem [1,7,8]. However, from the view point of preventing crimes, the security of e-cash system is weak. The scheme does not satisfy the unforgeable property since an adversary can fake a signature for the customer after the exchange phase. This paper addresses the issue of the security of e-cash system based on DSA signature with message recovery feature and adopts the concept of public key cryptosystem to e-cash procedure while still maintaining the efficiency but enhancing e-cash security.

The paper is organized as follows. Briefly introduce the concept of the DSA signature with message recovery feature in Section 2. In Section 3, a brief description of fair e-cash scheme based on DSA multi- signature is shown. In Section 4, improved payment system that satisfies the designed properties is proposed. Finally, the conclusion is described in Section 5.

II. DSA SIGNATURE FOR MESSAGE RECOVERY FEATURE

This section briefly describes the concept of the message recovery feature of DSA signature [3,4,9,10,15]. Let p be a large prime, q be a large integer factor of $p-1$ and an element $g \in Z_p^*$ whose order is q. Let x is the private key, $y = g^x \bmod p$ is the public key, k is random number $k \in Z_q$. The signature (r , s) of a message m is

$$r = m\, g^k \pmod p,\ r' = r \pmod q,$$
$$s = k - r'x \pmod p$$

The public key y is verified by recovering the message m from signature (r , s). That is, $m = g^s y^{r'} r \pmod p$.

III. REVIEW OF FAIR E-CASH PAYMENT SCHEME

In this section, a brief description of fair e-cash payment scheme based on DSA signature is presented. The basic scheme consists of three participants and four processes: set up process, exchange process, deposit process and dispute resolution process.

A. Setup Process

In setup process, national bank generates (x_B , y_B) and publish public key. National bank issues certification for the other branch bank i , $CA_{Bi} = E_{xB}(y_{Bi})$ to prove the branch bank's validity. (x_{Bi} , y_{Bi}) are the secret key and public key of branch bank i.

Manuscript received May, 2013.
Thae Nu Nge, *Faculty of Information and Communication Technology, University of Technology Yatanarpon Cyber City, Pyin Oo Lwin, Myanmar.*

The consumer generates p, q, g, x, x_1, $y = g^x$ and $y_1 = g^{x1}$, and publishes p, q, g. For an exchange information m, consumer computes e-cash (denote as $\delta = (r, s)$) $r = mg^k \pmod p$, r' = r (mod q), s = $k - r'x \pmod p$ and commitment (denote as$\delta_1 = (r_1, s_1)$) , $r_1 = m\, g^k \pmod p$, $r_1' = r_1 \pmod q$, $s_1 = k - r_1' x_1 \pmod p$.

Consumer contacts bank i to get the public key y certified. The arbitration key x_2 is used by bank to make a fair dispute resolution when there is a dissension between user and merchant. The consumer sends y , y_1 , δ, δ_1 , x_2, m, ID_c to bank i.

Bank i checks $m = g^s y^{r'} r \pmod p$, $m = g^s y_1^{r1'} r_1 \pmod p$, $s = s_1 + r_1' x_2 \pmod p$ is valid. After verifying the validity of all items, bank i issues a signed certificate CA_c and an overdraft credit voucher V_c to consumer, where

$V_c = Sig_{Bi} (y_1 \,||\, N \,||\, E_\psi (x_2 || ID_c))$,

$CA_c = (E_{xBi} (y) \,||\, CA_{Bi})$, $CA_{Bi} = E_{xB} (y_{Bi})$

N stipulates the largest value of an e-cash which consumer can overdraft based on credit. After the setup process, consumer has (x, y), (x_1, y_1), x_2, V_c, CA_c, and bank i has his secret arbitration key x_2, and y, y_1, V_c , CA_c.

B. Exchange Process

When the consumer wants to purchase the digital merchandise, consumer and merchant cooperate to do the following steps. Where C represents consumer and M represents merchant.

1. C ⟶ M : V_c , CA_c , δ_1
2. C ⟵ M : $E_r(u)$
3. C ⟶ M : δ

Firstly, the consumer choose a number k randomly and compute $\delta_1(r_1, s_1)$ on the purchase information m and sends δ_1 , V_c and CA_c to merchant.

Second, merchant can verify the bank's public key y_{Bi} and consumer public key y using the national bank' public key y_B from CA_c . From V_c , he obtains public key y_1 and checks N. If all items are valid, merchant sends the encrypted merchandise $E_r(u)$ to consumer. Otherwise, merchant does not send the merchandise, and stops the protocol.

Finally, if consumer satisfies the merchandise, he computes the e-cash δ and sends it to merchant. Otherwise, consumer stops the protocol.

After receiving e-cash δ, Merchant verifies δ using y. If it is valid, merchant ends the protocol. Otherwise, merchant requests bank i to resolve the dispute.

C. Deposit Process

Merchant sends the e-cash δ and CA_c to merchant's bank j. If e-cash δ is valid, bank i transfer financing from consumer's accounts to bank j.

D. Dispute Resolution Process

If consumer does not sends the e-cash δ, or if δ is invalid, merchant performs these process.

1. M ⟶ B : V_c , CA_c , δ_1 , $E_r(u)$, $E_{yBi}(r)$
2. M ⟵ B : δ

Merchant sends V_c , CA_c , δ_1, $E_r(u)$ and the encrypted session key $E_{yBi}(r)$ to bank i.

Bank i use his private key x_{Bi} to decrypts $E_{yBi}(r)$ and then recover u using r. Next, he verifies δ_1 using the system parameters and keys from CA_c and V_c. If everything is valid, bank i generates the e-cash using δ_1 and his secret arbitration key x_2 as follow: $r = r_1$, $r_1' = r_1 \bmod q$, $s = s_1 + r_1' x_2 \bmod p$.

The e-cash δ and encrypted merchandise is sent to merchant and consumer respectively. Otherwise, if bank i checks the invalid of the received item, bank i sends nothing to either party.

E. Security Analysis

The DSA signature with message recovery feature is vulnerable to existential forgery attacks, that is, given a valid signature of a known message, an adversary can forge a valid signature of another different message without the knowledge of the secret key [3,13,15]. Let A be the signer and an adversary gets A's signature (r , s) for a message m. Then, the adversary can compute a signature (r' , s') for a message m' without the knowledge of A's secret key by the following procedure. The adversary computes $r_1' = (mr^{-1})\, g^{-1} = r_1\, g^{-1} = g^{k-1} \pmod p$.

Then, sets a message

$m' = m\, g^{-1} \pmod p$, $r' = r$ and $s' = s\text{-}1$.

Sends (r', s') as a signature of m', (r' , s') is a valid signature of m' since

$$\begin{aligned} g^{s'} y^r r &= g^{s-1} y^r r \\ &= g^s y^r r\, g^{-1} \\ &= m\, g^{-1} \\ &= m' \pmod p \end{aligned}$$

By this procedure, an adversary can make the signature on a message mg^{-1} and also can generate a signature for any message in a subset $S_{m,g} = \{mg^{-n} | n \in Zq\}$, within one time known-message attack.

It is obvious that an adversary can forge consumer's e-cash after he got the real e-cash after the exchange process. Hence, the faked e-cash can be verified successfully and there is no evidence that whether merchant makes deposit with the consumer's real e-cash or not. Moreover, malicious merchant can make the illegal purchase with V_c , CA_c and fake e-cash. It may cause a great financial loss to the business partners and dissatisfy the fairness of the exchange. In addition, a malicious bank can forge a fact of honest merchant's double deposit [6].

IV. Improved Fair E-cash Payment Scheme

This section presents the improved fair e-cash payment scheme in order to solve the above flaws. The proposed solution is straightforward and it should not require to much modifications in the overall system. In addition to certified public key y, consumer applies another certified public key e to encrypt e-cash in payment process.

Before registration process, the consumer needs to select two large prime numbers: p and q. Modulus n is : $n = p \times q$. A number e is chosen that is $0 < e < (p-1) \times (q-1)$ and also co-prime: gcd (e; [$(p-1) \times (q-1)$]) = 1. The public key is: **(** n, e**)**. Private key d is $d = e^{-1} \pmod{(p-1) \times (q-1)}$.

A. Setup Process

The registration process is the same procedure as the above protocol except the consumer submits the public key **(n , e)** to bank i .

For an exchange information m, consumer computes e-cash (denote as $\delta = (r , s)$) and commitment (denote as $\delta_1 = (r , s)$) as follow.

$r = m\, g^k \pmod p$, $r' = r \pmod q$, $s = k - r'x \pmod p$

$r_1 = m\, g^k \pmod p$, $r_1' = r_1 \pmod q$, $s_1 = k - r_1'x_1 \pmod p$.

After computing e-cash and commitment signature, the consumer encrypts them using his private key d. That is, e-cash δ:(r,s) is encrypted as δ':(c_r , c_s) as follow.

$c_r = r^d \bmod n$, $c_s = s^d \bmod n$

The encrypted commitment δ_1':(c_{r1}, c_{s1}) is computed as follow.

$c_{r1} = r_1^{\,d} \bmod n$, $c_{s1} = s_1^{\,d} \bmod n$

Next, consumer sends y, y_1 , e , δ':(c_r, c_s), δ_1':(c_{r1}, c_{s1}), x_2, m, ID_c to bank i. Bank i recover the e-cash δ:(r, s) and commitment signature δ_1 :(r_1, s_1) using public key (n,e) as follow.

$r = c_{r1}^{\,e} \bmod n$, $s = c_s^{\,e} \bmod n$

and

$r_1 = c_{r1}^{\,e} \bmod n$, $s_1 = c_{s1}^{\,e} \bmod n$

After that, Bank i checks $m = g^s y^{r'} r \pmod p$, $m = g^s y_1^{\,r1'} r_1 \pmod p$, $s = s_1 + r_1' x_2 \bmod p$ is valid.

After verifying the validity of all items, bank i issues a signed certificate CA_c and an overdraft credit voucher V_c to consumer, where

$V_c = Sig_{Bi}(y_1 \,||\, N \,||\, E_\psi (x_2 || ID_c))$,

$CA_c = (E_{xBi} (y \,||\, e) \,||\, CA_{Bi})$, $CA_{Bi} = E_{xB} (y_{Bi})$

After the setup process, consumer has (x, y), (x_1, y_1), x_2, (e,d), V_c , CA_c and bank i has his authentic public key e and y, y_1, x_2, V_c , CA_c .

B. Exchange Process

When the consumer want to purchase the digital merchandise, the consumer and the merchant cooperate to do the following steps.

1. C ⟶ M : V_c , CA_c , δ_1'
2. C ⟵ M : $E_r (u)$
3. C ⟶ M : δ

At first, the consumer picks a number k randomly, and computes δ_1:(r_1, s_1) for the purchase information m (which might contain consumer's unique identity, merchant's unique account number, price, description and date of transaction). To prevent the signature δ_1:(r_1, s_1) modified or forged, the consumer encrypts commitment signature using his private key d,

$c_{r1} = r_1^{\,d} \bmod n$, $c_{s1} = s_1^{\,d} \bmod n$

and sends δ_1':(c_{r1}, c_{s1}), V_c and CA_c to merchant.

Secondly, merchant can verify consumer's public key y and e using CA_c. Merchant can recover the commitment δ_1:(r_1, s_1) from δ_1':(c_{r1}, c_{s1}) using consumer's authentic public key e as follow.

$r_1 = c_{r1}^{\,e} \bmod n$, $s_1 = c_{s1}^{\,e} \bmod n$

Then verifies the signature

$m = g^{s1} y_1^{\,rl'} r_1 \pmod p$

If all items are valid, merchant sends encrypted merchandise to consumer.

Finally, receiving expected merchandise, consumer computes e-cash δ:(r,s) and encrypts as δ':(c_r, c_s) as follow and sends it to merchant.

$c_r = r^d \bmod n$, $c_s = s^d \bmod n$

Merchant checks the validity of δ' using e and y as follow.

$r = c_r^{\,e} \bmod n$, $s = c_s^{\,e} \bmod n$

$m = g^s y^{r'} r \pmod p$

If both of them are valid, merchant ends the protocol. Otherwise, merchant performs the dispute resolution process.

C. Deposit Process

Merchant sends the e-cash δ' and CA_c to merchant's bank j. Bank j verifies CA_{Bi} using y_B, verifies CA_c using y_{Bi} . Bank j recovers the e-cash δ from δ' using consumer' authentic public key e and verifies e-cash using y. If merchant has not deposit e-cash before, bank j deposits it in her account.

D. Dispute Resolution Process

If consumer does not sends the e-cash, or if e-cash is invalid, merchant performs these processes.

1. M ⟶ B : V_c , CA_c , δ_1' , $E_r(u)$, $E_{yBi} (r)$
2. M ⟵ B : δ

After receiving V_c , CA_c , δ_1' , $E_r(u)$, $E_{yBi} (r)$ from merchant, bank i decrypts $E_{yBi} (r)$ using his private key x_{Bi}, and uses r to recover u. Next, he verifies δ_1 using the system parameters and keys from CA_c and V_c.

Bank i recovers the δ_1 from δ_1' using consumer' authentic public key e and verifies δ_1 using y.

If everything is valid, bank i generates the e-cash using δ_1 and his secret arbitration key x_2 as follow: $r = r_1$, $r_1' = r_1 \bmod q$, $s = s_1 + r_1' x_2 \bmod p$.

The e-cash and encrypted merchandise is sent to merchant and consumer respectively. Otherwise, if bank i checks the invalid of the received item, bank i sends nothing to either party.

E. Security Analysis

In this section, the security issues with respect to the proposed system will be discussed.

Authentication analysis: In improved system, part of e-cash is encrypted using public and private key pair (e,d), e-cash is still produced by consumer. During the exchange process, the consumer must prove the merchant that he is the owner of e-cash. Upon receiving δ_1':(c_{r1}, c_{s1}), the merchant compute $r_1 = c_{r1}^{\,e} \bmod n$, $s_1 = c_{s1}^{\,e} \bmod n$. Even if someone can get CA_c , V_c and fake signature, he can't prove that he is the holder of CA_c and V_c because he can't produce δ_1':(c_{r1}, c_{s1}), without obtaining d. During the deposit process, the bank verifies the e-cash using public key e also ensures that e-cash is a valid one generated by consumer, not a modified one by merchant.

The previous proposed system can't hold this property because an adversary can make use of CA_c, V_c and fake signature in another purchases as described in session 3.5. Therefore, encrypting the e-cash using key pair (e, d) makes the e-cash secure and ensures authentication of the system processes.

Non-repudiation analysis: After the exchange phase, consumer cannot deny that he had spent the e-cash because only the consumer who knows the private key *d* could perform the computation of δ_1':(c_{r1}, c_{s1}),. As a result, the improved scheme gives the evidence of origin and fulfills non-repudiation.

Integrity analysis: Because producing δ_1':(c_{r1}, c_{s1}), results that the e-cash is a valid one generated by the consumer. Although an adversary can successfully produce the forge e-cash, he can't encrypt it without knowing consumer's private key *d*. If an adversary deposits forged or modified e-cash (r',s'), bank can check immediately. Thus, the adversary can't make a deposit with the forge e-cash. Clearly, it also prevents the dishonest merchant initiating the dispute resolution process with a fake e-cash. For this reason, the improved scheme prevents the effects of existential forgery attack and confirms that data integrity is not violated.

Impersonation analysis: Because the consumer's private key is not stored in the database of the bank, the malicious bank employee can't produce e-cash from the honest consumer's account by impersonating the consumer with the secret key. Therefore, this incomplete information (for the bank) enhances security against the impersonation by the malicious bank [6].

Also, malicious bank cannot issue a consumer's e-cash without the consumer's agreement. In addition, a malicious bank cannot forge a fact of honest merchant's double deposit.

V. CONCLUSION

This paper addresses the security issue of e-cash system based on DSA signature with message recovery feature and shows the weakness of that system. The improved scheme encrypts the e-cash using public key cryptosystem during the exchange phase that prevents the effects of existential forgery attack and overcomes the weakness. The proposed solution is straightforward and it should not require to much modifications in the overall system. Hence, integrating authentic public key for e-cash verification satisfies the two basic requirements: authenticity and integrity and makes the fair offline e-cash payment systems securely workable. In the future, it needs to formalize both the protocol and the security requirements that it needs to meet, and then verify that the requirements are met indeed using one of the formal verification methods such as AVISPA.

ACKNOWLEDGMENT

I would like to thank my supervisor and all of my teachers for their helpful comments in improving our manuscript.

REFERENCES

[1] Zhaoxia, Wang Shaobin, Nu Shuwang , "A DSA Multi-Signature Protocol and Applying in E-Bank and E-Voting", IEEE 978-1-4244-5895-0, 2010.

[2] C-H Wang and W-M Chiang, "The Design of a Novel E-cash System with the Fairness Property and Its Implementation in Wireless Communications", Department of Computer Science and Information Engineering National Chiayi University , *Journal of Computers* Vol.18, No.2, July 2007.

[3] Atsuko Miyaji, "Weakness in Message recovery signature scheme based on discrete logarithm problems 1", *IEICE Japan Tech. Rep.*, ISEC95-11, 1994.

[4] Y.-M. Tseng, "Digital signature with message recovery using self-certified public keys and its variants", *Applied Mathematics and Computation* 136 (2003) 203–214.

[5] C. Popescu, "A Secure E-Cash Transfer System based on the Elliptic Curve Discrete Logarithm Problem", *INFORMATICA*, vol. 22, No. 3, 395–409, 2011.

[6] T.Nishide, S.Miyazaki, K.Sakurai, "Security Analysis of Offline E-cash Systems with Malicious Insider", *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, vol. 3, number: 1/2, pp. 55-71.

[7] Lei Hu, "Fair E-cash Payment Model on Credit O", 2006 *IEEE Asia-Pacific Conference on Services Computing* (APSCC 06), 12/2006.

[8] Guohua Cui, "A fair e-cash payment scheme based on credit", *in Proc. 7th international conference on Electronic commerce* - ICEC 05 ICEC 05, 2005.

[9] Gao, C. zhi, D. Xie, J. Li, B. Wei, and H. Tian. "Deniably Information-Hiding Encryptions Secure against Adaptive Chosen Ciphertext Attack", *Fourth International Conference on Intelligent Networking and Collaborative Systems*, 2012.

[10] Tseng, Y.M.,"Digital signature with message recovery using self-certified public keys and its variants", *Applied Mathematics and Computation*, 20030315.

[11] Xian Zhu. "Optimistic fair-exchange protocols based on DSA signatures", *IEEE International Conference on Services Computing* 2004 (SCC 2004) Proceedings 2004, 2004

[12] Al-Fayoumi, Mohammad. "Practical E-Payment Scheme", *International Journal of Computer Science Issues* (IJCSI)/16940784, 20100501

[13] Zichen Li. "A new forgery attack on message recovery signatures", *Journal of Electronics* (China), 07/2000

[14] Xinmei Wang. "Fair Exchange Signature Schemes", 22nd International Conference on Advanced Information Networking and Applications - Workshops (aina workshops 2008), 03/2008

[15] Kaisa Nyberg. "Message recovery for signature schemes based on the discrete logarithm problem", Lecture Notes in Computer Science, 1995

Thae Nu Nge received Master degree in Information Technology from Mandalay Technological University, Myanmar in 2009. Now she is currently pursuing Ph.D degree in security protocols and electronic payments systems. Research interests include cryptography, network security, security protocols and electronic payment systems.