Analysis of a Known Offline E-Coin System

Sattar J. Aboud
Department of Computer Science and Technology
University of Bedfordshire, UK

Ammar Aggoun
Department of Computer Science and Technology
University of Bedfordshire, UK

ABSTRACT
In 2012, Fan *et al*. presented the user recoverable offline e-coin system with rapid anonymity revoking. The authors claimed that their system can accomplish the security needs of e-coin scheme such as unlinkability, over-spending checking, anonymity control and rapid anonymity revoking on over-spending. They added prove unforgeability characteristic. But, in this paper we demonstrate that a system cannot reach the two proven security characteristics, unlinkability and anonymity. So, we adjust the scheme to contain these two characteristics which are vital in any e-coin scheme.

General Terms
Information Security

Keywords
Digital signatures, discrete logarithm problem, cryptanalysis, RSA, e-commerce and payment

1. INTRODUCTION
E-cash system permits secure e-payments by giving similar security and anonymity as hand cash. The general e-cash idea illustrates a communication between three kinds of participants, customer, bank and merchant. Financial value is denoted by e-cash, which are pieces of information blindly signed by a bank. A bank is the only participant capable to create e-cash. It releases e-cash to the customer, who uses them to pay in the supermarket. In e-cash its serial number with an identity of its customer is encrypted in blinded method. Then the merchant deposits the cash that collected from customers in his bank account. Through or after the deposit process a bank verifies if the deposited e-cash had been deposited previously, if the merchant deposited the same coin twice, or if the customer over-spent the coin, by any case his identity will be disclosed. The vital characteristic of certain e-coin system is that they support the encoding of customers characteristics into coins such as customer age or address. This is suitable for two aims. It lets a collection of important customer information in order to study and enhance a scheme in the privacy protecting way and it permits applying extra characteristics in a scheme such as variable cost to decreased charges for senior users.

The e-coin scheme usually includes three protocols. These are withdrawal protocol, payment protocol, and deposit protocol. In a designing scheme, a user identity must not be disclosed, to secure the purchasing. On the other hand, it can be revealed if over-spending or unauthorized transaction happens. In the offline e-coin system, a bank cannot obstruct over-spending online. So, it should have a capability to revoke anonymity of a user who spent twice the e-coins.

2. RELATED WORKS
In 1982, Chaum [1] was a first to present a thought of e-coin scheme that lets anonymous, unlikable payments, which is anti-over-spending in an offline case. After Chaum idea many systems were introduced [2]. For example, 1n 1993 Brands [3] introduced a scheme that its efficiency measured during spending. But, official proof of security has by no means provided it and recently illustrated that it cannot be shown secure in a Random Oracle model [4]. In 2001 Masayuki Abe presented the three-move blind signature scheme [5] which can be lengthened to e-coin, though is less efficient compared with Brands system but has the security proof in a Random Oracle. In 2003 Abe discovered with Ohkubo the proof suffered from limitations, because it was merely applicable for a hacker with great success likelihood, and they provided another proof in a generic model [6]. In 2006, Heydt-Benjamin *et al*. [7] presented another improves in anonymous credentials to construct offline payment scheme. They use the hybrid scheme with two types of e-tickets, passive RFID transponders and embedded schemes for example mobile phones. In 2007, Clemente-Cuervo *et al*. [8] introduced the PDA execution of the offline e-coin system which relied on Brands, and accomplishes the implementation with time of second for withdrawal.

In 2009 Blass *et al.* [9] presented RFID-typed, e-ticket system for transit uses which are restricted to defend user confidentiality versus stranger not anti-transportation authority. In 2010, Batina *et al*. are proposed the execution of anonymous credentials on Java [10]. In 2011, Derler *et al.* [11] executed NFC-typed mobile ticketing scheme, which is relied on Brands private credential system. Implementation times of some seconds are reached. In 2012, Baldimtsi and Lysyanskaya introduced anonymous credentials light [12], which widens Abe system to let encoding of properties into cash whereas maintaining its efficiency. But, their proof of security goes in as they constraint their idea to trail composition only. Also, in 2012 Pirker *et al*. explained the use of particular hardware abilities of certain mobile phones to construct the secure NFC-typed and prepaid payment scheme [13], but a scheme needs devices accepting the payment online in any time. Also in 2012, Fan *et al*. [14] presented a great offline e-coin system with rapid anonymity revoking. They claimed that every user can overcome anonymity and unlinkability, if spending e-coin in the system and a user is allowable to get back his e-coin if missing. Also, a bank can discover over-spending and effectively obtain an identity of a user, without any assist from a trusted authority. Also, trusted authority can revoke anonymity of e-coin holder if unauthorized transaction happens. Furthermore, their system permits a monitor to trace the certain user. But, after investigative the system, we discovered that the system is not containing anonymity and unlinkability. So, to increase its security, we adjust it to include the two characteristics which are significant of e-coin scheme.

3. NOTATIONS USED
The notations used in this paper are as follows:

C : Customer

B : Bank
J : Judge
S : Shop
Id_C : Identity of the customer
p, q : The prime numbers
p_B, q_B : Prime numbers for the bank
$||$: Concatenation
n_B : Composite modulus for the bank
$\theta(n_B)$: The Theta for the bank
gcd : Greater common divisor
e_B : Public key for the bank
d_B : Private Key for the bank
e_j : Public key for judge
d_j : Private Key for judge
g : The generator
h : Secure one-way hash function
z : The chameleon hash function
l_k : Security key represents the bit length of a session key.
l_r : Security key represents the bit length of a random string.

4. DESCRIPTION OF FAN *ET AL.* SYSTEM

Fan *et al*. e-coin system contains three protocols, the withdrawal protocol, the payment protocol and the recovery protocol. Also, the scheme has four participants, customer, bank, shop and judge. Also, they use Chaum signature and a secure hashing function to construct their system. In this paper, we will describe these protocols to show their system drawbacks.

4.1 Initialization

The steps of the initialization phase are as follows:

Step 1: The Bank B

1. Chooses randomly two large primes (p_B, q_B)
2. Find $n_B = (p_B q_B)$
3. Find $\theta(n_B) = (p_B - 1)(q_B - 1)$
4. Pick arbitrarily an integer e_B with $\gcd(\theta(n_B), e_B) = 1$ and $1 < e_B < \theta(n_B)$
5. Find d_B where $e_B d_B \equiv 1 \bmod \theta(n_B)$
6. Select arbitrarily a secure prime p
7. Select an integer k
8. Picks a generator $g \in Z_p^*$ of order q, with $p = kq + 1, q$ is a prime,
9. Pick a secure one-way hash function h
10. Determine (n_B, e_B, p, q, g, h) with (p, q, g) is a public key of a chameleon hash function.

Step 2: The Judge J

1. Create public-private key (e_j, d_j)
2. Determine the public key and inserts $(e_j, d_j, h, h', n_B, e_B)$ into a temper-resistant device
3. Send $(e_j, d_j, h, h', n_B, e_B)$ to a bank

4.2 The Withdrawal protocol

The description of withdrawal protocol is as follows.

Step 1: The Customer C

1. Select arbitrarily three integers (k, m, r), with $k \in (0,1)^{l_k}$, and $m, r \in Z_q^*$.
2. Post $e_j(k, m, r)$ to a bank.

Step 2: The Bank B

1. Verify a customer, by a customer identity Id_C.
2. Find $a = Id_C$
3. Key $e_j(k, m, r)$ and a into a judge machine.

Step 3: The Judge Machine J

1. Use d_j to decrypt $e_j(k, m, r)$ and obtains (k, m, r)
2. Select arbitrarily three integers (r_1, r_2, c), with $r_1, r_2 \in (0,1)^{l_r}$ and $c \in Z_{n_B}^*$
3. Find $x = (a || r_1)$
4. Find $i = x^{-1} \bmod q$
5. Find $b = e_j(a, r_2)$
6. Find $y = g^x \bmod p$
7. Find $f = (c^{-1})^{e_B}(g^m y^r) \bmod p$
8. Find $h(b || y) \bmod n_B = (c^{-1})^{e_B} z(m, r) h(b || y) \bmod n_B$
9. Post $(f, o(x, i, c, k, b))$ to a bank.

Step 4: The Bank B

1. Find $t = f^{d_B} \bmod n_B$
2. Send $(t, o(x, i, c, k, b))$ to a customer.
3. Save $(Id_C, e_j(k, m, r), o(x, i, c, k, b))$ for e-coin tracing.

Step 5: The Customer C

1. Decrypt $o(x, i, c, k, b)$
2. Determine k'.
3. Verify $k' = k$. If yes,
    1. Find $w = ct \bmod n_B$
    2. Get e-coin (w, y, m, r, b).

4.3 The Payment Protocol

The description of the offline payment protocol is as follows.

Step 1: The Shop S

When the customer wants to pays to the shop. The shop should do the following:

1. Select arbitrarily integer r_s
2. Find $v = (Id_S || r_s)$, with $v \in Z_q^*$, and Id_s is a shop identity.
3. Pass v to a customer

Step 2: The Customer C

1. Find $r' = i(m + xr - v) \bmod q$ (1)
2. Post (w, y, r', b) to a shop

Step 3: The Shop S

1. Check $w^{e_B} \equiv z(v, r') h(b || y) \bmod n_B$, with $z = (p, q, g, y)$

2. If it is yes, accepts coin (w, y, v, r', b) and saves it
3. Deposit e-coin (w, y, v, r', b) in a bank

Step 4: The Bank B

1. Check if $w^{e_B} = z(v, r')h(b \| y) \bmod n_B$ and (w, y, b) has not in a database.
2. If both are correct, save e-coin (w, y, v, r', b) in database and deposits it into shop account.

4.4 The Recovery Protocol

If the customer with identity a, lost his e-coin, he can make a recovery protocol, which is illustrated below to retrieve an e-coin. Previous to running the following protocol, a user should authenticated by a bank and achieve a recovery protocol under the protected channel.

Step 1: The User U

The user has to inform a bank that he desires to recover an e-coin which had been withdrawn by certain time period t_p as follows:

1. Pick arbitrarily $k' \in (0,1)^{l_k}$
2. Pass $(t_p, e_j(k'))$ to a bank

Step 2: The Bank B

Suppose that a bank recover j withdrawal records $(e_j(k_i, m_i, r_i), e_{k_i}(x_i, i_i, c_i, k_i, b_i))$ such records made for a user during a period t_p and $i \in (1,\ldots,j)$. It keys $(e_j(k'),$ $(e_j(k_i, m_i, r_i), e_{k_i}(x_i, i_i, c_i, k_i, b_i), a)$ to a judge device.

Step 3: The Judge Device J

1. Recover $e_j(k')$
2. Recover $e_j(k_i, m_i, r_i)$,
3. Recover $e_{k_i}(x_i, i_i, c_i, k_i, b_i)$,
4. Find $y_i = g^{x_i} \bmod p$
5. Find $f_i = (c_i^{-1})^{e_B} h'(m_i, r_i)h(b_i \| y_i) \bmod n_B$
6. Send $(f_i, e_{k'}(x_i, i_i, c_i, k', b_i, m_i, r_i)$ to a bank.

Step 4: The Bank B

1. Find $t_i = f_i^{d_B} \bmod n_B$
2. Post $(t_i, e_{k'}(x_i, i_i, c_i, k', b_i, m_i, r_i))$ to the user

Step 5: The User U

1. Decrypt $(t_i, e_{k'}(x_i, i_i, c_i, k', b_i, m_i, r_i))$ by k'
2. Find $w_i = ct \bmod n_B$ for $i \in (1,\ldots,j)$
3. Get the e-coin $(w_i, y_i, m_i, r_i, b_i)$

5. THE DRAWBACK

Note that if there is any e-coin of $(w_i, y_i, m_i, r_i, b_i)$ has been spent by a user and he does not remember which ones had been spent, he can deposit all of these e-coin into a bank and execute a withdrawal protocol again. But, he will lose the privacy of those spent e-coin. Therefore, a hacker can gather transmitted messages on an Internet, and get the data as follows:

From steps 2, 3, and 4 in a withdrawal protocol, a hacker can recognize the values, a, f, t

From step 3 in an offline payment protocol, a hacker can recognize the values (w', y', v, r', b'). Then start offline attack by the following methods.

1. Find $c' = w' t^{-1} \bmod n_B$
2. Find $f \equiv ((c')^{-1})^{e_B} z(v, r')h(b' \| y')$ if yes. It means that the hacker knows the e-coin (w, y, m', r', b) owner is $a = Id_C$. So, properties of anonymity and unlinkability are broken.

Anonymity and unlinkability: are the basic requirements for each e-cash scheme. Anonymity means that if an e-cash is shown, no one can know who withdrew this e-cash. Whereas Unlinkability means that both the bank and merchant cannot trace a user's consumption behavior. Due to anonymity and unlinkability, the user can maintain his privacy in an e-cash scheme. Table one illustrates the differences between four e-cash offline schemes including Fan *et al* scheme, we compare Fan *et al*. scheme with [15–17] in anonymity and unlinkability

Table 1. Table comparisons between four e-cash offline schemes

Scheme	Anonymity	Unlinkability
Fan *et al*	No	No
Liu *et al* [15]	Yes	Yes
Qiu [16]	No	No
Hou and Tan [17]	Yes	No

6. DEVELOPMENT

From a drawback found in section 5, we see a key point is a and t in messages 2 and 4 of a withdrawal protocol were not unseen from a hacker. This causes it suffer from the above attack. To improve, we conceal the two keys $e_j(k, m, r)$ and $o(x, i, c, k, b)$ into $e_j(k, m, r, a)$ and $o(x, i, c, k, b, t)$ respectively. But, if a hacker starts the above attack on the modification; and he knows f without known t, he cannot break the unlinkability; also without a value of a the anonymity is certain.

7. CONCLUSION

Fan *et al*. claimed that in their scheme each user possesses anonymity and unlinkability if spending e-cash. They also stated that their scheme allows the user to reclaim his lost e-cash. If the user over-spends his e-cash, the bank can find out and efficiently obtain the identity of the user without any help from trusted authority. In addition, if an e-cash has been spent in an illegitimate transaction and reported to trusted authority, trusted authority can frustrate the anonymity of the owner of the e-cash. Also, they stated that their e-cash scheme allows the police to trace the specific user. Accordingly, their offline e-cash scheme means has anonymity, unlinkability, recoverability.

But, in this paper we demonstrate that Fan *et al*. scheme cannot achieve the two security requirements, unlinkability and anonymity. But, to enhance its security and to avoid the drawbacks in section 5, the solution is illustrated in section 6. Therefore, we have reached the objective of this paper.

8. ACKNOWLEDGMENTS

The authors wish to thank the University of Bedfordshire, department of Computer science and Technology for its support us.

9. REFERENCES

[1] Chaum, D. 1982, Blind Signatures for Untraceable Payments, CRYPTO82, pp. 199–203, Plenum Press, New York.

[2] Tan, Garry Wei-Han, 2014, NFC Mobile Credit Card: The Next Frontier of Mobile Payment, Telematics and Informatic, 31, pp. 292–307.

[3] Brands, S. 1993, Untraceable Off-line Cash in Wallets with Observers, CRYPTO93, volume 773 of Lecture Notes in Computer Science, pages 302-318, Springer.

[4] Baldimtsi, F. and Lysyanskaya, A. 2012, On the Security of One-Witness Blind Signature Schemes, IACR Cryptology ePrint Archive, 2012:197.

[5] Abe, M. 2001, A Secure Three-Move Blind Signature Scheme for Polynomial Many Signatures, EUROCRYPT2001, volume 2045 of Lecture Notes in Computer Science, pp. 136–151, Springer.

[6] Ohkubo, M. and Abe, M. 2003, Security of Three-move Blind Signature Schemes Reconsidered, SCIS03, Symposium on Cryptography and Information Security, Japan.

[7] T Heydt-Benjamin, Chae, H. Defend, B. and Fu, K. 2006, Privacy for Public Transportation, Privacy Enhancing Technologies, volume 4258, Lecture Notes in Computer Science, pp. 1–19, Springer.

[8] Clemente-Cuervo, E. Rodríguez-Henríquez, F. Arroyo, D. and Ertaul, L. 2007, A PDA Implementation of an Off-line e-Cash Protocol, Security and Management, pp. 452–458, CSREA Press.

[9] Blass, E. Kurmus, A. Molva, R. and Strufe, T. 2009, private and secure payment with RFID, WPES, pp. 51–60, ACM.

[10] Batina, L. Hoepman, J. Jacobs, B. Mostowski, W. and Vullers, P. 2010, Developing Efficient Blinded Attribute Certificates on Smart Cards via Pairings, volume 6035 of Lecture Notes in Computer Science, pages 209–222, Springer.

[11] Derler, D. Potzmader, K. Winter, J. and Dietrich, K. 2011, Anonymous Ticketing for NFC-Enabled Mobile Phones, INTRUST, volume 7222 of Lecture Notes in Computer Science, pages 66–83, Springer.

[12] Baldimtsi F. and Lysyanskaya, A. 2012, Anonymous Credentials Light, IACR Cryptology ePrint Archive, 2012:298.

[13] Pirker M. and Slamanig, D, 2012, A Framework for Privacy-Preserving Mobile Payment on Security Enhanced ARM TrustZone Platforms", TrustCom, pp. 1155–1160, IEEE Computer Society.

[14] CI Fan, VSM Huang, and YC Yu, 2012, User Efficient Recoverable Off-line E-cash Scheme with Fast Anonymity Revoking, Mathematical and Computer Modeling, Vol.58, No. 1-2, pp.227-237.

[15] Liu, J.K. Tsang, P.P., and Wong, D.S. 2005, Recoverable and Untraceable E-cash, in: Euro PKI 2005, in: Lecture Notes in Computer Science, vol. 3545, Springer-Verlag, pp. 206–214.

[16] Qiu, W. 2007, A Fair Off-line Electronic Payment System, in: Studies in Computational Intelligence, Springer-Verlag, pp. 177–195.

[17] Hou, X. and Tan, C.H. 2004, Fair traceable off-line electronic cash in wallets with observers, in: Advanced Communication Technology, IEEE Computer Society, Phoenix Park, Korea, 2004, pp. 595–599.