Crypto-analyses on “user efficient recoverable off-line e-cashs scheme with fast anonymity revoking”

Yalin Chen[1] and Jue-Sam Chou*[2]

[1] Institute of information systems and applications, National Tsing Hua University

d949702@oz.nthu.edu.tw

[2] Department of Information Management, Nanhua University, Taiwan R.O.C

*: corresponding author: jschou@mail.nhu.edu.tw

Tel: 886+ (0)5+272-1001 ext.56536

Abstract

Recently, Fan et al. proposed a user efficient recoverable off-line e-cash scheme with fast anonymity revoking. They claimed that their scheme could achieve security requirements of an e-cash system such as, anonymity, unlinkability, double spending checking, anonymity control, and rapid anonymity revoking on double spending. They further formally prove the unlinkability and the un-forgeability security features. However, after crypto-analysis, we found that the scheme cannot attain the two proven security features, anonymity and unlinkability. We, therefore, modify it to comprise the two desired requirements which are very important in an e-cash system.

1. Introduction

There have been many cryptographic scientists working within the field of e-cash system design [1-21] since Chaum first proposed the concept of e-cash and its paper cash-like properties of anon*ymity*, *verifiability*, and *unforgeability* (Chaum 1982) in 1982 [1]. An e-cash system typically contains three roles: customer, bank, and the merchant, and three protocols: withdrawal protocol, payment protocol, and the deposit protocol. In the protocol design principle, the user’s identity cannot be revealed, to assure his purchasing privacy. Conversely, it can be disclosed when double spending or illegal transaction occurs. In an off-line e-cash scheme, the bank cannot prevent the double spending on-line. Therefore, it must have the ability to revoke the anonymity of the user who doubly spent his e-cash. In 2013, Fan et al. [16] proposed an excellent off-line e-cash scheme with fast anonymity revoking. They claimed that each user possessed anonymity and un-linkability, when spending e-cash in their scheme, and the user is allowed to recover his e-cash when lost. Besides, the bank can detect the double spending and efficiently derive the identity of the user, without any help of the TTP. Moreover, TTP can revoke the anonymity of the e-cash owner when illegal transaction occurs. Additionally, their scheme allows the police to trace a specific user. However, after examining their scheme, we found that it does not have anonymity and un-linkability. We, therefore, for enhancing its security, modify it to comprise these two features which are very important in an e-cash system. We demonstrate it in this article.

2. Review of Fan et al.'s IBS scheme

Fan et al.'s e-cash scheme [16] consists of two main protocols: the withdrawal protocol and the payment (and deposit) protocol, and four entities user, bank, shop and the judge. Meanwhile, they use Chaum's signature and the chameleon hashing functions to design the scheme. The used notations can be referred to the original article. Here, we only list the withdrawal protocol and the payment protocol to illustrate its weakness.

2.1 The withdrawal protocol

The scheme assumes that the bank can authenticate the user through a secure channel. They omit the design relating to this portion. The withdrawal protocol is depicted as follows.

1. User→Bank: $E_{pk\_j}(k,m,r)$.

   The user randomly chooses three strings *(k,m, r),* where k∈{0, 1}^{lk} and m, r∈ z_q^*.

   Then, he sends $E_{pk\_j}(k,m,r)$ to the bank.

2. Bank→The judge device: ($E_{pk\_j}(k,m,r)$, μ).

   After the bank authenticates the user, it knows the user's identity ID_u. It then sets $\mu = ID_u$, and inputs $E_{pk\_j}(k,m,r)$ and μ into the judge device.

3. The judge device→Bank: (β , $E_k(x,\bar{x},c,k,\delta)$)).

   After receiving $E_{pk\_j}(k,m,r)$ and μ, the judge device uses *sk_j* to decrypt $E_{pk\_j}(k,m,r)$ and gets *(k,m, r)*. Then, it randomly chooses three strings (r_1, r_2, c), where r$_1$, r$_2$∈ {0, 1}^{lr} and c∈ $z_{n_b}^*$ and computes $x=(\mu \parallel r_1) \in z_q^*$, $\bar{x} = x^{-1}$ mod q, $\delta = E_{pk\_j}(\mu, r_2)$, and $y = g^x \bmod p$. Finally, it computes $\beta = (c^{-1})^{eb} (g^m y^r \bmod p) H(\delta \parallel y) \bmod n_b = (c^{-1})^{e_b} h_{HK}(m,r) H(\delta \parallel y) \bmod n_b$ and outputs

(β, $E_k(x,\bar{x},c,k,\delta)$) to the bank, where *HK* = *(p, q, g, y)*.

4. Bank→User: (t, $E_k(x,\bar{x},c,k,\delta)$).

   After receiving (β, $E_k(x,\bar{x},c,k,\delta)$) from the judge device, the bank computes t = β^{d_b} mod n_b and returns (t, $E_k(x,\bar{x},c,k,\delta)$) to the user. Then the bank stores (ID_u, $E_{pk\_j}(k,m,r)$, $E_k(x,\bar{x},c,k,\delta)$) for e-cash tracing and recovery.

5. Unblinding: After receiving (t, $E_k(x,\bar{x},c,k,\delta)$), the user decrypts $E_k(x,\bar{x},c,k,\delta)$ and parses the 4th parameter in the decryption result as k'. Then he checks whether $k' = k$. If it's true, he computes $\Sigma = ct \bmod n_b$. At last, the user obtains an e-cash $(\Sigma, y, m, r, \delta)$.

2.2 The off-line payment protocol

The off-line payment protocol is described as follows.

1. Shop→User: (m').

   When a user makes a payment to a shop, the shop will randomly choose a string r_s and compute $m' = (ID_s \,||\, r_s)$, such that $m' \in z_q^*$, where ID_s is the shop's identity. Then the shop sends m' to the user.

2. User→Shop: (Σ, y, r', δ).

   After receiving m', the user computes $r' = \bar{x}(m + xr - m') \bmod q$. (1)

   Then, he sends (Σ, y, r', δ) to the shop.

3. Shop→Bank: $(\Sigma, y, m', r', \delta)$.

   After receiving (Σ, y, r', δ), the shop verifies if $\Sigma^{e_b} = h_{HK}(m', r')H(\delta \| y) \bmod n_b$, where *HK* = *(p, q, g, y)*. If it's true, shop accepts the e-cash and stores $(\Sigma, y, m', r', \delta)$. Later, the shop will send the bank the received e-cash.

4. Bank: acceptance or rejection.

   The shop deposits e-cash $(\Sigma, y, m', r', \delta)$ to the bank. The bank first verifies it by checking if $\Sigma^{e_b} = h_{HK}(m', r')H(\delta \| y) \bmod n_b$ and (Σ, y, δ) has not existed in the database. If both are true, the bank stores e-cash $(\sum, y, m', r', \delta)$ in the database and deposits tit into the shop's account.

3. The weakness

An attacker can collect the transmitted message on the Internet, and obtain some information as follows:

(1) From message 2, 3, and 4 in the withdrawal protocol, the attacker can know the values, μ, β , and *t*.

(2) From message 3 in the off-line payment protocol, the attacker can know the values, $(\sum', y', m', r', \delta')$.

He then can launch an offline attack by the following ways.

(1) Computes $c' = \sum' t^{-1} \bmod n_b$

(2) Computes to see if $\beta ?= [(c')^{-1}]^{e_b} h_{HK}(m', r')H(\delta' \| y')$.

If the equation in (2) he knows that the e-cash $(\sum, y, m', r', \delta)$ owner is μ *(= IDc)*. Thus, the features of anonymity and un-linkability are broken.

4. Modification

From the weakness found in section 3, we see that the key point is that μ and *t* in messages 2 and 4 of the withdrawal protocol were not hidden from the attacker. This makes it suffer from the above attack. To enhance, we hide the two parameters into $E_{pk\_j}(k, m, r)$ and $E_k(x, \bar{x}, c, k, \delta)$ to become $E_{pk\_j}(k, m, r, \mu)$ and $E_k(x, \bar{x}, c, k, \delta, t)$, respectively.

Accordingly, if an attacker launches the above attack on our modification; although, he knows β, without the value of *t*, he cannot break the un-linkability; and without the value of μ, the anonymity is assured.

5. Conclusion

In this paper, we showed that Fan et al.'s recoverable off-line e-cash's scheme is flawed. It suffers from linkability and identity leakage. We, therefore, for enhancing its security, modified it to avoid these two weaknesses. From the analysis shown in section 5, we see that we have reached the goal of the security promotion.

References

[1] D.Chaum, “Blind signatures for untraceable payments”, *Crypt’82*, Plenum, NY, 1983, pp. 199-203

[2] Wen-Shenq Juang, Horng-Twu Liaw, “A practical anonymous multi-authority e-cash scheme”, *Applied Mathematics and Computation*, Vol. 147, No. 3, 16 January 2004, pp. 699-711.

[3] Wen-Shenq Juang, “D-cash: A flexible pre-paid e-cash scheme for date-attachment”, *Electronic Commerce Research and Applications*, Vol. 6, No. 1, Spring 2007, pp. 74-80.

[4] Yu Yi Chen, Jinn Ke Jan, Chin-Ling Chen, “A novel proxy deposit protocol for e-cash systems”, *Applied Mathematics and Computation* , Vol. 163 , 2005 , pp. 869–877.

[5] H. Wang, Y. Zhang, “Untraceable off-line electronic cash flow in e-commerce”, *Computer Science Conference*, 2001. ACSC 2001. Proceedings. 24th Australasian 29 Jan-4 Feb 2001 pp. 191 – 198.

[6] C. Popescu, H. Oros, “An Off-line Electronic Cash System Based on Bilinear Pairings”, *Systems, Signals and Image Processing*, 2007 and 6th EURASIP Conference focused on Speech and Image Processing, Multimedia Communications and Services. 14th International Workshop on 27-30 June 2007, pp. 438 – 440

[7] Shangping Wang, Zhiqiang Chen, Xiaofeng Wang, “A new certificateless electronic cash scheme with multiple banks based on group signatures”, *IEEE International Symposium on Electronic Commerce and Security*, 2008.

[8] Yun Ling, Yiming Xiang, Xun Wang, “RSA-based Secure Electronic Cash Payment system”, *IEEE International Conference*, 2-4 December 2007, pp.1898 – 1902.

[9] Matthieu Gaud, Jacques Traore, “On the Anonymity of Fair Offline E-cash Systems”, *LNCS 2742*, 2003, pp. 34-50.

[10] Alfredo De Santis, Anna Lisa Ferrara, Barbara Masucci, “An attack on a payment scheme”, *Information Sciences*, Vol. 178, No. 5, 1 March 2008, pp. 1418-1421.

[11] Hua Wang, Jinli Cao, Yanchun Zhang, “A flexible payment scheme ant its role-based access control”, *IEEE Trans. Knowl. Data Eng*, 17 March 2005, pp. 425-436.

[12] Chun-I Fan, Shi-Yuan Huang, Pei-Hsiu Ho, Chin-Laung Lei, “Fair anonymous rewarding based on electronic cash”, *Journal of Systems and Software*, in press, Corrected Proof, Available online 13 February 2009.

[13] Mafruz Zaman Ashrafi, See Kiong Ng, “Privacy-preserving e-payments using one-time payment details”, *Computer Standards & Interfaces*, Vol. 31, Issue 2, February 2009, pp. 321-328.

[14] M.Franklin, M.Yung, “Secure and efficient off-line electronic digital money”, *Lecture Notes in Computer Science*, Vol. 700, 20th Int. Colloquium on Automata, Languages and Programming (ICALP), Springer Verlag, 1993, pp. 265-276.

[15] Stefan Brands, “Untraceable Off-line Cash in Wallets with Observers”, *CRYPTO’93*, *Lecture Notes in Computer Science*, Vol.773, Springer-Verlag, pp. 302-318.

[16] CI Fan, VSM Huang, and YC Yu, “User efficient recoverable off-line e-cash scheme with fast anonymity revoking”, *Mathematical and Computer Modelling*, Vol.58, No. 1-2, 2012, pp.227-237.

[17] Baseri, Y., B. Takhtaei, and J. Mohajeri. "Secure untraceable off-line electronic cash system", *Scientia Iranica*, 20 (3), 2013, pp.637－646.

[18] Choo, Kim-Kwang Raymond. "New payment methods: A Review of 2010-2012 FATF Mutual Evaluation Reports." *Computers & Security*, 3 6, 2013, pp. 1 2-2 6.

[19] Wei-Chen Wu, Horng-Twu Liaw. “Secure Anonymous Conditional Purchase Order Payment Mechanism.”, Computer Science and its Applications, *Lecture Notes in Electrical Engineering*, Volume 203, 2012, pp. 291-300

[20] Aszalós, László, and Andrea Huszti. "Payment approval for PayWord.", *Information Security Applications*. Springer Berlin Heidelberg, pp. 2012. 161-176.

[21] Tan, Garry Wei-Han, et al. "NFC Mobile Credit Card: The Next Frontier of Mobile Payment?.", *Telematics and Informatic* , 31, 2014, pp. 292－307.