Cryptanalysis on “Secure untraceable off-line electronic cash system”

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, Baseri et al. proposed a secure untraceable off-line electronic cash system. They claimed that their scheme could achieve security requirements of an e-cash system such as, untraceability, anonymity, unlinkability, double spending checking, un-forgeability, date-attachability, and prevent forging coins. They further prove the un-forgeability security feature by using the hardness of discrete logarithm problems. However, after cryptanalysis, we found that the scheme cannot attain the security feature, untraceability. We, therefore, modify it to comprise this desired requirement, which is very important in an e-cash system.

Keywords: digital signatures, discrete logarithm problem, cryptanalysis, RSA, electronic commerce and payment

1. Introduction

There have been many cryptographic scientists working within the field of e-cash system design [1-33] since Chaum first proposed the concept of e-cash and its paper cash-like properties of anonymity, verifiability, and unforgeability (Chaum 1982) in 1982 [11]. 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, Baseri et al. [27] pointed out that Eslami et al.’s untraceable off-line electronic cash system [17] is flawed. It suffers three attacks, double spender detection attack, expiration date forgery, and frauds on exchange protocol. They also proposed an excellent untraceable off-line e-cash scheme system and claimed that their scheme contains anonymity, double spending

detection, un-forgeability, date attachability properties, and forgery prevention. Meanwhile, they also show the reasons why their scheme immune to the three faults that Eslami et al.'s scheme suffers. However, after examining their scheme, we found that it does not have the untraceability property. We, therefore, for enhancing its security, modify it to comprise this feature, which is very important in an e-cash system. We demonstrate it in this article.

2. Review of Baseri et al.'s scheme

Baseri et al.'s e-cash scheme [27] consists of four participants in the scheme: a central authority, the bank, the spender, and the merchant. It contains five phases: initialization, withdrawal, payment, deposit, and the exchange. Meanwhile, they use Chaum's signature to design the scheme and take advantage of RSA-based method to attach the time to the structure of the signature. 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 central authority sets some public parameters, including two publicly known elements, g_1, g_2, and the bank's two RSA public/private key pairs $(((e_B, n), 1/e_B))$ and $((e_B^{'}, n), 1/e_B^{'})$ such that $e_B \geq e_B^{'}$. Before withdrawing and asking for a coin, the spender should provide his ownership of the account to the bank. The spender should prove his identity in a similar way to the withdrawal of classical cash from an account. In addition, the bank periodically publishes the fresh time by two parameters, t and $e_B * t \pmod{\phi(n)}$, where t is constant during the period and used to synchronize customers and $e^b * t$ plays the role of a public key for the bank and is chosen in such a way that its reverse exists. The coin is represented by a five touple (A', B, s_1, s_2, s_3). The withdrawal protocol is depicted as follows.

Step 1. The spender S:

(a) Chooses three random numbers, $x_1, x_2 \in_R Z_{e_B^{'}}^*$ and $s \in_R Z_n^*$, and two blinding factors, $b_1, b_2 \in Z_n^*$

(b) Computes: $A' = A^s \pmod{n}$, $B = g_1^{x_1} g_2^{x_2} \pmod{n}$, $w_1 = B b_1^{e_B^{'}} \pmod{n}$, $w_2 = (A^{'} + B) b_2^{e_B * t} \pmod{n}$,

(c) Sends w_1, w_2, t to the bank.

Step 2. The bank B:

(a) Checks the validity of the Date/Time slip.

(b) Signs w_1, w_2 by computing:

$$O_2 = w_1^{1/e_B'} (\mathrm{mod}\, n) \quad , \quad O_3 = w_2^{1/(e_B * t)} (\mathrm{mod}\, n)$$

(c) Sends O_2 and O_3 to the spender.

Step 3. The spender S:

(a) Verifies the signatures of the bank on A, w_1, w_2.

(b) Obtains the signatures of the bank on A', B and $A' + B$, which are signed with private keys $1/e_B$, $1/e_B'$, and $(1/(e_B * t))$, respectively:

$s_1 = O_1^s (\mathrm{mod}\, n) = \mathrm{sign}_B(A')$, $s_2 = O_2 / b_1 (\mathrm{mod}\, n) = \mathrm{sign}_B(B)$,

$s_3 = O_3 / b_2 (\mathrm{mod}\, n) = \mathrm{sign}_B(A' + B)$.

The Coin is $(A', B, s_1, s_2, s_3, t)$.

2.2 The off-line payment protocol

The off-line payment protocol is described as follows.

Step 1. The spender S:

(a) Sends $(A', B, s_1, s_2, s_3, t)$ to the merchant M.

Step 2. The merchant M:

(a) Verifies whether $A' \neq 0$.

(b) Checks the coin's expiration date.

(c) Verifies the signatures, s_1, using the public key, e_B, s_2 using the public key, e_B', and s_3 using the public key $(e_B * t)$.

(d) Computes:

The challenge d = H($A', B, ID_M, date \,||\, time$), where H is the hash function determined in the initializeation phase, ID_M is the merchant's identity and $date \,||\, time$ represents the transaction's date and time.

(e) Sends d to the spender.

Step 3. The spender S:

(a) Computes:

$r_1 = dus + x_1 (\mathrm{mod}\ e_B)$,

$r_2 = ds + x_2 (\mathrm{mod}\ e_B)$.

(b) Sends r_1 and r_2 to the merchant.

Step 4. The merchant M:

(a) Accepts the coin if $g_1^{r_1} g_2^{r_2} = A'^{dB}$.

3. The weakness

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

(1) From the messages in one of the withdrawal protocol executions, the attacker can know the values, w_1, w_2, t, O_2 , and O_3 .

(2) From the messages in the off-line payment protocol, the attacker can know the coin, $(A', B, s_1, s_2, s_3, t)$.

Assuming that the attacker has gathered all m (with $m \le 2^q$, where q is the security parameter, e.g., q=80) coins $(A_i', B_i, s_{i1}, s_{i2}, s_{i3}, t_i)$, for i=1 to m, he then can launch an offline attack for the m coins using the following ways.

(1) Computes $O_2^{e_B'} = w_1 = Bb_1^{e_B'} (\mathrm{mod}\, n)$. From this equation, he knows $b_1^{e_B'} = O_2^{e_B'} / B (\mathrm{mod}\, n)$. Although, he cannot have the right value of B, with the help of m observed coins $(A_i', B_i, s_{i1}, s_{i2}, s_{i3}, t_i)$, he can compute $b_{i1}^{e_B'} = O_2^{e_B'} / B_i (\mathrm{mod}\, n)$, for i=1 to m. Then, he randomly chooses $a, f \in z_n^*$, forms the value $w_{i1} = a^{e_B'} b_{i1}^{e_B'} (\mathrm{mod}\, n)$, and executes the withdrawal protocol by sending w_{i1}, f, t to the bank for acquiring $O_2' = w_1^{d_B'} = ab_{i1}, O_3' = f^{d_{e_B * t}}$. He is able to deduce b_{i1} using the value $a^{-1} (\mathrm{mod}\, n)$.

(2) Computes to see if $O_2 = s_{i2} \cdot b_{i1}$.

If the equation in (2) holds, the insider knows that the e-cash $(A_i', B_i, s_{i1}, s_{i2}, s_{i3}, t_i)$ is related to the parameters w_1, w_2, t, O_2 , and O_3 in a specific withdraw protocol. Else, he continues through the rest of each of the m-1 coins. Definitely, he will find one coin satisfying the equation. Thus, the feature of untraceability is violated. Even if $m \ge 2^q$, the attacker can use the parameter t, observed in the withdraw protocol, to sieve the coins which have the same time t, and then launch the two-step attack shown above.

4. Modification

From the weakness found in section 3, we see that the key point is that the insider can use $b_{i1}^{e_B'} (= O_2^{e_B'} / B_i (\mathrm{mod}\, n))$ to produce $w_{i1} (= a^{e_B'} b_{i1}^{e_B'} (\mathrm{mod}\, n))$ for sending to the bank to obtain b_{i1} , and then check to see if $O_2 = s_{i2} \cdot b_{i1}$ holds. To further blur the relation

between O_2 and s_{i2} , we introduce two other parameters $b_3 \in z_n, x_1 \in z_n^*$, and modify $w_1 = b_3 B b_1^{e_B'}$, form $w_{11} = (b_3 b_1^{e_B'}) x_1^{e_B'}$, and let the spender send w_1, w_{11}, w_2, t to the bank. Thus, the bank will return O_2, O_{22}, and O_3. O_2 from the bank will become $w_1^{1/e_B'} (\mathrm{mod}\, n) = (b_3 B)^{1/e_B'} b_1$ and $O_{22} = b_3^{1/e_B'} b_1 x_1$. After this, the spender can use $x_1^{-1} \bmod n$ to acquire $O_{22-x_1} = b_3^{1/e_B'} b_1$ from O_{22}, and then take advantage of it to obtain $s_2 = B^{1/e_B'} = O_2 \cdot O_{22-x_1}^{-1}$. Accordingly, if an attacker launches the above attack on our modification; although, he knows O_{22}, without $x_1^{-1} \bmod n$, he cannot have O_{22-x_1} to form the value $w_{i1} = a^{e_B'} O_{22-x_1}^{e_B'} (\mathrm{mod}\, n)$, and executes the withdrawal protocol by sending w_{i1}, *f*, *t* to the bank for breaking the untraceability.

5. Conclusion

In this paper, we showed that Baseri et al.'s untraceable off-line e-cash's scheme is flawed. It suffers from traceability. We, therefore, for enhancing its security, modified it to avoid this weakness. From the analysis shown in section 4, we see that we have reached the goal of the security promotion.

References

[1] Choo, K. K. R. (2013). New payment methods: A Review of 2010-2012 FATF Mutual Evaluation Reports. *Computers & Security*, 36, 2013, 12-26.

[2] Wang, Q., & Zhu, J. (2013, January). Study on the Electronic Payment Technology in E-Commerce. In *Proc. of the 2nd International Conference on Green Communications and Networks 2012 (GCN 2012): Vol.*4 (pp. 95-100). Springer Berlin Heidelberg.

[3] Aszalós, L., & Huszti, A. (2012). Payment approval for PayWord. In *Information Security Applications* (pp. 161-176). Springer Berlin Heidelberg.

[4] Tan, G. W. H., Ooi, K. B., Chong, S. C., & Hew, T. S. (2013). NFC Mobile Credit Card: The Next Frontier of Mobile Payment?. *Telematics and Informatics*, 31, 2014, pp. 292–307.

[5] Žilka, R., Matyáš, V., & Kyncl, L. (2012). Four authorization protocols for an electronic payment system. In *Mathematical and Engineering Methods in Computer Science* (pp. 205-214). Springer Berlin Heidelberg.

[6] Hossein Pour, M. M., Husin, A. R. C., & Dahlan, H. M. (2012, May). BESTCASH: A new e-cash for micropayment. In *Innovation Management and Technology Research (ICIMTR), 2012 Intl Conference on* (pp. 580-584). IEEE.

[7] Hinterwälder, G., Zenger, C. T., Baldimtsi, F., Lysyanskaya, A., Paar, C., & Burleson, W. P. (2013, January). Efficient E-Cash in Practice: NFC-Based Payments for Public Transportation Systems. In *Privacy Enhancing Technologies* (pp. 40-59). Springer Berlin Heidelberg.

[8] Tiwari, M., Kumar, R., Jindal, S., & Sharma, P. (2013). An Efficient and Secure Micro-payment Transaction Using Shell Cryptography. In *Quality, Reliability, Security and Robustness in Heterogeneous Networks* (pp. 461-469). Springer Berlin Heidelberg.

[9] Hinterwälder, G., Paar, C., & Burleson, W. P. (2013). Privacy preserving payments on computational RFID devices with application in intelligent transportation systems. In *Radio Frequency Identification. Security and Privacy Issues* (pp. 109-122). Springer Berlin Heidelberg.

[10] Rahman, B. A., Azlina, N., Shajaratuddur Bt Harun, K., & Bt Yusof, Y. (2013, March). SMS banking transaction as an alternative for information, transfer and payment at merchant shops in Malaysia. In *Information Technology and e-Services (ICITeS), 2013 3rd International Conference on* (pp. 1-6). IEEE.

[11] Chaum, D. (1982, August). Blind Signatures for Untraceable Payments. In *Crypto* (Vol. 82, pp. 199-203).

[12] Chaum, D., Fiat, A., & Naor, M. (1990, January). Untraceable electronic cash. In *Advances in Cryptology—CRYPTO'88* (pp. 319-327). Springer New York.

[13] Brands, S. (1994, January). Untraceable off-line cash in wallet with observers. In *Advances in Cryptology—CRYPTO'93* (pp. 302-318). Springer Berlin Heidelberg.

[14] Brickell, E., Gemmell, P., & Kravitz, D. (1995, January). Trustee-based tracing extensions to anonymous cash and the making of anonymous change. In *Proceedings of the sixth annual ACM-SIAM symposium on Discrete algorithms* (pp. 457-466). Society for Industrial and Applied Mathematics.

[15] Camenisch, J., Maurer, U., & Stadler, M. (1997). Digital payment systems with passive anonymity-revoking trustees. *Journal of Computer Security*, *5*(1), 69-89.

[16] Fujisaki, E., & Okamoto, T. (1997, January). Practical escrow cash systems. In*Security Protocols* (pp. 33-48). Springer Berlin Heidelberg.

[17] Eslami, Z., & Talebi, M. (2011). A new untraceable off-line electronic cash system. *Electronic Commerce Research and Applications*, *10*(1), 59-66.

[18] Frankel, Y., Tsiounis, Y., & Yung, M. (1998, January). Fair off-line e-cash made easy. In *Advances in Cryptology—ASIACRYPT'98* (pp. 257-270). Springer Berlin Heidelberg.

[19] Wang, H., Cao, J., & Zhang, Y. (2005). A flexible payment scheme and its role-based access control. *Knowledge and Data Engineering, IEEE Transactions on*, *17*(3), 425-436.

[20] Fuchsbauer, G., Pointcheval, D., & Vergnaud, D. (2009). Transferable constant-size fair e-cash. In *Cryptology and Network Security* (pp. 226-247). Springer Berlin Heidelberg.

[21] Gaud, M., & Traoré, J. (2003, January). On the anonymity of fair offline e-cash systems. In *Financial Cryptography* (pp. 34-50). Springer Berlin Heidelberg.

[22] Hufschmitt, E., & Traoré, J. (2007). Fair blind signatures revisited. In *Pairing-Based Cryptography–Pairing 2007* (pp. 268-292). Springer Berlin Heidelberg.

[23] Juang, W. S. (2007). D-cash: A flexible pre-paid e-cash scheme for date-attachment. *Electronic Commerce Research and Applications*,*6*(1), 74-80.

[24] Ashrafi, M. Z., & Ng, S. K. (2009). Privacy-preserving e-payments using one-time payment details. *Computer Standards & Interfaces*, *31*(2), 321-328.

[25] Chen, Y., Chou, J. S., Sun, H. M., & Cho, M. H. (2011). A novel electronic cash system with trustee-based anonymity revocation from pairing. *Electronic Commerce Research and Applications*, *10*(6), 673-682.

[26] Fan, C. I., Huang, V. S. M., & Yu, Y. C. (2012). User efficient recoverable off-line e-cash scheme with fast anonymity revoking. *Mathematical and Computer Modelling*, 58(1-2), 227-237.

[27] Baseri, Y., B. Takhtaei, and J. Mohajeri (2013). Secure untraceable off-line

electronic cash system, *Scientia Iranica*, *20* (3), 637–646.

[28] Stalder, F. (2002). Failures and successes: notes on the development of electronic cash. Inf Soc18(3),209–219

[29] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.*Consulted*, *1*, 2012. Available: http://www.bitcoin.org/bitcoin.pdf.

[30] Zorpette, G. (2012). The beginning of the end of cash. *Spectrum*, *IEEE*, *49*(6), 27-29.

[31] Peck, M. E. (2012). The cryptoanarchists' answer to cash. *Spectrum*, *IEEE*, *49*(6), 50-56.

[32] Miers, I., Garman, C., Green, M., & Rubin, A. D. (2013). Zerocoin: Anonymous Distributed E-Cash from Bitcoin. In *IEEE Symposium on Security and Privacy*.

[33] Reid, F., & Harrigan, M. (2013). An analysis of anonymity in the bitcoin system. In *Security and Privacy in Social Networks* (pp. 197-223). Springer New York.