On the Privacy of "User Efficient Recoverable Off-Line E-Cash Scheme with Fast Anonymity Revoking"

Yalin Chen[1] and Jue-Sam Chou[2]
(Corresponding author: Jue-Sam Chou)
Institute of information systems and applications, National Tsing Hua University, Taiwan[1]
Department of Information Management, Nanhua University, Taiwan[2]
No. 55, Sec. 1, Nanhua Rd., Dalin Township, Chiayi County 62249, Taiwan (R.O.C.)
(Email: jschou@mail.nhu.edu.tw)
(Received Dec. 3, 2014; revised and accepted Apr. 16 & May 26, 2015)

Abstract

Recently, Fan et al. proposed a novel e-cash scheme which allows a user to recover the e-cash he lost. They claimed their e-cash possesses properties of anonymity, unlinkability (i.e. untraceability), bank-off-line payment, double-spending detection, and anonymity revocation. The e-cash untraceability is greatly related to users' privacy and indicates that no one including the issuer bank can link e-cash to any user when the e-cash is legally spent. Although, the authors have formally proved the unlinkability of their scheme, we still found a loophole to compromise user's privacy. That is, an issuer bank or an attacker who intrudes the issuer bank's system can link e-cash to a user by collecting e-cash withdrawal and deposit transaction messages. This may make the user's shopping behaviors or location information exposed.

Keywords: Anonymity revocation, digital signatures, electronic commerce and payment, off-Line E-Cash, recoverable, RSA

1 Introduction

With the advances of technology, people are paying through diverse payment tools or systems [2, 8, 16, 18], for example credit cards, debit cards, PayPal, account transfer, Short-Message-Service (SMS) payment, mobile phone payments, electronic transportation toll, and etc. Most of the payment tools or systems are named payments which make the payers' identities exposed to the brokers or intermediaries. In the case of the globally widespread credit card payments, card-issuing banks are aware of the contents of the cardholder's all spending, such as the cardholder went somewhere to buy something at some time, visited some restaurant to have dinner, or travelled to some gas station, and so forth. To prevent personal privacy exposure to the payment intermediaries, electronic cash (e-cash) which holds the anonymity property like dollar bill can make the payer not to be aware of and not to be tracked. There have been many cryptographic scientists working within the field of e-cash system design [1, 3, 4, 5, 6, 7, 9, 10, 11, 17] since Chaum first proposed the concept of e-cash in 1982. From the viewpoint of control, e-cash systems fall into two categories: bank-controlled e-cash systems, ex. Mondex, and P2P (peer-to-peer)-distributed e-cash systems, ex. Bitcoin.

Mondex [15] developed by National Westminster Bank in the U. K. and had big success in 1990s. It has the advantage of absolute anonymity but opens a perfect way for criminals to illegally transfer funds with untraceability. While Bitcoin [13, 19] kills the role of the central bank or authority, reduces the expensive bank-processing cost, and prevails over the cyberspace and the real world. All activities including coin mintage, coin validness check, double-spending check are done through the cooperation of the peer nodes on the Bitcoin P2P network. By just generating a public/private key pair, a user can join the Bitcoin network, and he/she uses this public key as a his/her pseudonym to mine, exchange, buy, and pay the Bitcoin without revealing his/her real identity and location. However, some privacy issues exist since all Bitcoin transactions are public. One may trace sensitive transactions or de-anonymize social network data using network topology, thus violating users' privacy [12, 14].

For a sound cash system, some essential properties should be focused.

Verifiability. The validness of e-cash can be publicly examined.

Unforgeability. E-cash should be only issued through defined procedures. No one including banks can forge e-cash by other ways.

Anonymity. It indicates that a user need not present his/her real identity when paying.

Untraceability or Unlinkability. It means that no one including the banks can know the owner of the e-cash when it is legally used. Specially, although the bank provides e-cash withdrawal service to her account holder, it cannot link any e-cash to her account holder.

Double-spending detection. An e-cash system should prevent e-cash to be spent twice. If it happens, the system should efficiently catch the cheater.

Anonymity revocation. When e-cash is used for illegal purposes such as money laundering and tax evading, the system should disclose the owner identity of the e-cash.

Recently, Fan et al. [3] proposed a bank-off-line e-cash scheme with fast anonymity revoking. Bank-off-line e-cash indicates that e-cash in a payment transaction need not an online bank to examine its validness. Fan et al. claimed that each user possessed anonymity and unlinkability, 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 Trust Third Party (TTP). Moreover, TTP can revoke the anonymity of the e-cash owner when illegal transaction occurs. Additionally, Fan et al. scheme allows the police to trace a specific user. However, after examining their scheme, we found that it does not have anonymity and unlinkability.

2 Review of Fan et al.'s Scheme

Fan et al.'s e-cash scheme [3] applies the concepts of Chaum's blind signature and the chameleon hashing function. It consists of two main protocols, the withdrawal protocol and the payment protocol, and four entities user, bank, shop and the judge. The bank publishes $\{n_b, e_b\}$ as RSA public key, H as one-way hash function, and $\{p, q, g\}$ as the parameters of chameleon hashing function h_{Hk}. The judge generates public and private key pair $\{pk_j, sk_j\}$, and embeds $\{pk_j, sk_j, H, h_{Hk}, n_b, e_b\}$ into a tamper-resistant device. In the below, we first describe Fan et al.'s withdrawal and payment protocols and show their weaknesses then.

2.1 E-cash Withdrawal

In an e-cash withdrawal process, Fan et al.'s scheme assumes that the bank authenticates her account holder through a secure channel first. The bank and the user then perform the following e-cash withdrawal protocol.

1) User → Bank: $E_{pk_j}(k, m, r)$.
The user randomly chooses three random strings $\{k, m, r\}$ and he then sends $E_{pk_j}(k, m, r)$ to the bank, where $E(\cdot)$ is a public key encryption algorithm and k is a secret session key to be shared with the judge's device embedded in the bank system.

2) Bank → Judge's device: $\{E_{pk_j}(k, m, r), \mu\}$.
After the bank authenticates the user, she knows the user's identity ID_u. She then sends $E_{pk_j}(k, m, r)$ and $\mu = ID_u$ to the judge's device.

3) Judge's device → Bank: $\{\beta, E_k(x, x', c, k, \delta)\}$.
On receiving $\{E_{pk_j}(k, m, r), \mu\}$, the judge's device uses the stored private key sk_j to decrypt $E_{pk_j}(k, m, r)$ and obtain $\{k, m, r\}$. Then, it randomly chooses three strings $\{r_1, r_2, c\}$, and computes

$$\begin{aligned} x &= (\mu||r_1), \\ x' &= x^{-1} (\mathrm{mod} q), \\ \delta &= E_{pk_j}(\mu, r_2), \\ y &= g^x (\mathrm{mod} p), \\ \beta &= (c^{-1})^{e_b} h_{Hk}(m, r) H(\delta||y) (\mathrm{mod} n_b), \end{aligned}$$

where $h_{Hk}(m, r) = g^m y^r (\mathrm{mod} q)$, and outputs $\{\beta, E_k(x, x', c, k, \delta)\}$ to the bank system. Note that $h_{Hk}(\cdot)$ is a chameleon hashing function with the secret key Hk; given $h_{Hk}(m, r)$ one can easily find a preimage (m', r') such that $h_{Hk}(m', r') = h_{Hk}(m, r)$ if he knows the secret key Hk.

4) Bank → User: $\{t, E_k(x, x', c, k, \delta)\}$
On receiving the device response, the bank system returns $\{t = \beta^{d_b}, E_k(x, x', c, k, \delta)\}$ to the user (where d_b is the bank's RSA signing key), and stores $\{ID_u, E_{pk_j}(k, m, r), E_k(x, x', c, k, \delta)\}$ in her database.

5) User unblinding e-cash On receiving $\{t, E_k(x, x', c, k, \delta)\}$, the user decrypts $E_k(x, x', c, k, \delta)$ and parses the 4th parameter in the decryption result as k'. Then he checks whether $k' = k$. If it holds, he computes $\sum = ct (\mathrm{mod} n_b)$. At last, the user obtains an e-cash as $\{\sum, y, m, r, \delta\}$.

2.2 E-cash Paying and Deposit

A user in Fan et al.'s e-cash system allows to pay his cash to an Internet shop in the bank-offline manner as follows.

1) Shop → User: $\{m'\}$.
On receiving the user's payment request, the shop sends a challenge $m' = (ID_s r_s)$ to the user, where ID_s is the shop's identity and r_s is a random string.

2) User → Shop: $\{\sum, y, r', \delta\}$
On receiving the shop's challenge m', the user computes $r' = x'(m + xr - m') (\mathrm{mod} q)$ and answers the shop $\{\sum, y, r', \delta\}$.

3) Shop → Bank: $\{\sum, y, m', r', \delta\}$ On receiving the user's response, the shop verifies if the following equation holds.

$$\sum^{e_b} = h_{Hk}(m', r') H(\delta||y) (\mathrm{mod} n_b).$$

If it holds, the shop accepts the e-cash and stores the e-cash transcript $\{\sum, y, m', r', \delta\}$. In the clear time, the shop sends the bank the e-cash transcript.

4) Bank: acceptance or rejection. On receiving the e-cash transcript for deposit from the shop, the bank first verifies the e-cash by checking if the equation in 3) holds and if data $\{\sum, y, \delta\}$ has not existed in bank's database. If both are true, the bank stores the e-cash transcript $\{\sum, y, m', r', \delta\}$ in the database and credits the shop's account. Otherwise, the bank rejects the shop's deposit request.

3 A Loophole of Users' Privacy

An attacker can collect the transmitted messages of withdrawal, payment and deposit transactions in Fan et al.'s e-cash system, and obtain information as follows:

1) From a withdrawal transaction, the attacker can know the values, μ, β, and t. Notice that the user in the end of the transaction privately produces the e-cash $\{\sum, y, m, r, \delta\}$ which is not known to any other ones including the attacker.

2) From an off-line payment transaction, the attacker can know the e-cash, $\{\sum^*, y^*, m^*, r^*, \delta^*\}$ from the communication.

He then launches an offline attack by the following steps.

1) Computes $c^* = \sum^* t^{-1} (\mathrm{mod} n_b)$.

2) Computes to see if $\beta \stackrel{?}{=} h_{Hk}(m^*, r^*) H(\delta^* || y^*)$.

If the equation in 2) holds, the attacker links the e-cash $\{\sum^*, y^*, m^*, r^*, \delta^*\}$ to the user whose identity is $\mu (= IDu)$. Thus, the features of anonymity and unlinkability are broken.

4 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. This may result in e-cash user's shopping behaviors and movement information exposed to banks or attackers.

References

[1] M. Z. Ashrafi, S. K. Ng, "Privacy-preserving e-payments using one-time payment details", *Computer Standards & Interfaces*, vol. 31, no. 2, pp. 321–328, 2009.

[2] L. Aszalós, A. Huszti, "Payment approval for PayWord", in *Information Security Applications*, pp. 161–176, 2012.

[3] Y. Baseri, B. Takhtaei, and J. Mohajeri, "Secure untraceable off-line electronic cash system", *Scientia Iranica*, vol. 20, no. 3, pp. 637–646, 2013.

[4] J. Camenisch, U. Maurer, M. Stadler, "Digital payment systems with passive anonymity-revoking trustees", *Journal of Computer Security*, vol. 5, no. 1, pp. 69–89, 1997.

[5] D. Chaum, "Blind signatures for untraceable payments", in *Advances in Cryptology (Crypto'82)*, LNCS 82, pp. 199–203, 1983.

[6] D. Chaum, A. Fiat, M. Naor, "Untraceable electronic cash", in *Advances in Cryptology (Crypto'88)*, pp. 319–327, 1988.

[7] Y. Chen, J. S. Chou, H. M. Sun, M. H. Cho, "A novel electronic cash system with trustee-based anonymity revocation from pairing", *Electronic Commerce Research and Applications*, vol. 10, no. 6, pp. 673–682, 2011.

[8] K. K. R. Choo, "New payment methods", *Computers & Security*, vol. 36, pp. 12–26, 2013.

[9] Z. Eslami, M. Talebi, "A new untraceable off-line electronic cash system", *Electronic Commerce Research and Applications*, vol. 10, no. 1, pp. 59–66, 2011.

[10] C. I. Fan, V. S. M. Huang, Y. C. Yu, "User efficient recoverable off-line e-cash scheme with fast anonymity revoking", *Mathematical and Computer Modelling*, vol. 58, no. 1-2, pp. 227–237, 2012.

[11] W. S. Juang, "D-cash: A flexible pre-paid e-cash scheme for date-attachment", *Electronic Commerce Research and Applications*, vol. 6, no. 1, pp. 74–80, 2007.

[12] I. Miers, C. Garman, M. Green, A. D. Rubin, "Zerocoin: Anonymous distributed e-cash from bitcoin", in *IEEE Symposium on Security and Privacy*, pp. 397–411, 2013.

[13] M. E. Peck, "The cryptoanarchists' answer to cash", *IEEE Spectrum*, vol. 49, no. 6, pp. 50–56, 2012.

[14] F. Reid, M. Harrigan, "An analysis of anonymity in the bitcoin system", in *Security and Privacy in Social Networks*, pp. 197–223, 2013.

[15] F. Stalder, "Failures and successes: Notes on the development of electronic cash", *The Information Society: An International Journal*, vol. 18, no. 3, pp. 209–219, 2002.

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

[17] H. Wang, J. Cao, Y. Zhang, "A flexible payment scheme and its role-based access control", *IEEE Transactions on Knowledge and Data Engineering*, vol. 17, no. 3, pp. 425–436, 2005.

[18] Q. Wang, J. Zhu, "Study on the Electronic Payment Technology in E-Commerce", in *Proceedings of the 2nd International Conference on Green Communications and Networks (GCN'12)*, pp. 95–100, 2013.

[19] G. Zorpette, "The beginning of the end of cash", *IEEE Spectrum*, vol. 49, no. 6, pp. 27–29, 2012.

Yalin Chen received his Ph.D. degree in the Institute of Information Systems and Applications from National Tsing Hua University (NTHU) in Hsinchu, Taiwan, ROC. She now hosts the C & C Information Security Laboratory with Dr. Jue-Sam Chou in Chiayi, Taiwan. She now is also a contributing editor of Journal of Computer Science. Her primary research interests are Information Security, Cryptographic Protocols, Data security and Privacy, Authentication, Key Agreement, Electronic Commerce Security, E-commerce Protocols, Ad-Hoc Network Security, Sensor Network Security, RFID Authentication Protocol, Electronic Cash, Electronic Voting.

Jue-Sam Chou received his Ph.D. degree in the department of computer science and information engineering from National Chiao Tung Univ. (NCTU) in Hsinchu, Taiwan,ROC. He is an associate professor and teaches at the dept. of Infomation Management of Nanhua Univ. in Chiayi, Taiwan. He is now editors of two journals: Journal of computer science and International Journal of Cognitive Research in Science and Engineering and Education (IJCRSEE). His primary research interests are Information Security, Cryptographic Protocols, Data security and Privacy, Authentication, Key Agreement, Electronic Commerce Security, E-commerce Protocols, Ad-Hoc Network Security, Sensor Network Security, RFID Authentication Protocol, Electronic Cash, Electronic Voting.