Applied Mechanics and Materials Vols. 284-287 (2013) pp 3444-3448

doi:10.4028/www.scientific.net/AMM.284-287.3444

Improved on Date Attachable Electronic Cash

Jung-Wen Lo[1,a], Hung-Miao Lu[2,b], Tsuei-Hung Sun[3,c] and Min-Shiang Hwang[4,d]

[1]Department of Information Management, National Taichung University of Science and Technology, Taichung, 404, Taiwan

[2]Department of Information Management, Overseas Chinese University, Taichung, 407, Taiwan

[3]Department of Management Information Systems, National Chung Hsing University, Taichung, 402, Taiwan

[4]Department of Computer Science & Information Engineering, Asia University, Taichung, 413, Taiwan

[a]asalo@nutc.edu.tw, [b]lu@ocu.edu.tw, [c]njpth24121@gmail.com,
[d]Corresponding author: mshwang@asia.edu.tw

Keywords: Security in digital systems, Cryptography, Blind signature, Electronic cash, RSA cryptosystem.

Abstract. Electronic cash (E-cash) is widely used due to the electronic commerce being in vogue. The date attached E-cash can apply for some services such as interest calculation, expired date processing, etc. In this paper, we propose two E-cash schemes with date attachable: the basic scheme with a better efficiency and the advanced scheme with an extensible date. The most remarkable contribution is that the advanced scheme can express any readable date with the relative year concept and still has a marvelous efficiency improvement as well as the basic scheme has.

Introduction

The emergence of World Wide Web causes the electronic commerce appearance and then makes the electronic cash (E-cash) widespread use. After Chaum et al. proposed the concept of untraceable E-cash in 1982 [2], lots papers was proposed [1, 3, 4, 5, 6, 11, 15].

Most of E-cash schemes are based on blind signature [7, 8, 9, 10, 12, 13, 14, 16, 17, 18]. An on-line E-cash scheme has three kinds of participants: a bank, a group of merchants and a group of clients, and four stages: initializing, withdrawing, unblinding and depositing. In the initializing stage, the bank chooses its RSA-like public key pair. In the withdrawing stage, a client withdraws a temporal E-cash from bank. In the unblinding stage, the client unblinds the temporal E-cash to get the signed E-cash. In the depositing stage, the merchant deposits the E-cash into its account after receiving the E-cash from the client.

In 1996, Abe-Fujisaki proposed an embedded date concept based on the partially blind signature [1], but the efficiency of their scheme is not good. Therefore, Fan et al. proposed a readable date E-cash scheme with hash function computation. Nevertheless, their scheme needs 572 hash function executions and limits the term of validity of an E-cash in a period of one hundred years. To improve the efficiency, we proposed a basic scheme which reduces the number of hash operations to 212 times. To express a date, we use the relative year concept instead of the absolute year concept which is used in Fan et al.'s scheme. The main contribution of the advanced scheme not only extends the date but also has the same efficiency as the basic scheme.

This paper is organized as follows. In Section 2, the improved basic and advanced schemes were proposed. In Section 3, the discussion of long period E-cash and the analysis of performance and security are stated. Finally, the conclusion of this paper is given in Section 4.

The Improved schemes

In this section, we introduce the improved schemes which the main idea is the same as Fan et al.'s scheme. The basic scheme is to limit the date period of an E-cash in a decade instead of a century in Fan et al.'s scheme. It is suitable for most E-cash system. If the attaching date of E-cash is more than the basic scheme can express or a specific date should be attached, the advanced scheme is used.

The basic scheme

Now, we use Chaum's untraceable electronic cash scheme to demo the proposed basic scheme as Fan et al. stated in their paper [5].

Initialing stage: Firstly, the bank chooses two large prime number p and q, and computes $n = p \cdot q$ and $\varphi(n) = (p - 1) \cdot (q - 1)$. Then, it takes a large random number e where $GCD(e, \varphi(n)) = 1$, and finds another number d such that $e \cdot d \equiv 1 \bmod \varphi(n)$. Finally, the bank keeps its private key d in secret and publishes its public key (e, n) and one way hash function H where $H^0(m) = m$ and $H^i(m) = H(H^{i-1}(m))$ for $i > 0$.

Withdrawing stage: A client Cindy randomly chooses a blind factor r and six messages x_1, x_2, x_3, x_4, x_5, and x_6, and then delivers α to the bank where $\alpha = r^e \bullet H(m) \bmod n$ and Eq. (1). After computing $t = \alpha^d \bmod n$, the bank returns t to Cindy and deducts w dollars which is the worth of the E-cash from Cindy's account.

$$m=H^{10}(x_1)||H^{10}(x_2)||H^{12}(x_3)||H^{12}(x_4)||H^{31}(x_5)||H^{31}(x_6) \tag{1}$$

Unblinding stage: The client Cindy computes $s = r^{-1} \cdot t \bmod n$ and checks the correctness of the equation $s^e = H(m) \bmod n$. If the validation is passing, she can use the signed E-cash s later.

Depositing stage: Firstly, the client Cindy has to attach the date into the E-cash, so she sets three parameters year a, month b and day c. For example, if the present day is May 20, 2004, Cindy chooses the unit digit of the year 4 as a, month 5 as b and day 20 as c. Secondly, she separately computes $\beta_1 = H^a(x_1)$, $\beta_2 = H^{10-a}(x_2)$, $\beta_3 = H^b(x_3)$, $\beta_4 = H^{12-b}(x_4)$, $\beta_5 = H^c(x_5)$, $\beta_6 = H^{31-c}(x_6)$, and then sends these six parameters β_i for $i = 1 \cdots 6$, the date (a, b, c) and the signed E-cash s to the merchant. After verifying the data with Eq. (2), the merchant forwards all data to the bank for depositing. The bank also verifies the data as the merchant does and deposits the w dollars into the merchant's account if the verification is passed.

$$s^e = H(H^{10-a}(\beta_1)||\ H^a(\beta_2)||H^{12-b}(\beta_3)||H^b(\beta_4)||H^{31-c}(\beta_5)||H^c(\beta_6))\ mod\ n \tag{2}$$

The advanced scheme

The main idea of the advanced scheme is the concept of relative date. Because the Fan et al.'s scheme and our basic scheme are using the concept of absolute year, the presentation of absolute year limits the day which can be presented. With the idea of a based year, the E-cash can be extended the date in any date. The scheme is stated as follows.

Initialing stage: The bank creates its RSA key pair as mentioned in the basic scheme.

Withdrawing stage: A client Cindy randomly chooses a blind factor r, six messages x_1, x_2, x_3, x_4, x_5, and x_6 and a based year y which she plans to apply, e.g. year 2200, and then delivers α to the bank where $\alpha = r^e \bullet H(m) \bmod n$ and Eq. (3). After computing $t = \alpha^d \bmod n$, the bank returns t to Cindy and deducts w dollars which is the worth of the E-cash from Cindy's account.

$$m=H^{10}(x_1)||H^{10}(x_2)||H^{12}(x_3)||H^{12}(x_4)||H^{31}(x_5)||H^{31}(x_6)||y \tag{3}$$

Unblinding stage: Cindy unblinds the signed message t to obtain the signed E-cash s as mentioned in the basic scheme.

Depositing stage: When Cindy decides the date she wants to attach such as March 20, 2204. She sets three parameters year a = (real year) − (based year), month b and day c where $a = 2204 - 2200 = 4$, $b = 3$ and $c = 20$ now. Next, she separately computes $\beta_1 = H^a(x_1)$, $\beta_2 = H^{10-a}(x_2)$, $\beta_3 = H^b(x_3)$, $\beta_4 = H^{12-b}(x_4)$, $\beta_5 = H^c(x_5)$, $\beta_6 = H^{31-c}(x_6)$, and then sends these six parameters β_i for $i = 1 \cdots 6$, the date (a, b, c), the signed E-cash s and the based year y to the merchant. After verifying the data with Eq. (4), the merchant passes all data to the bank for depositing. The bank also verifies the data as the merchant does and deposits the w dollars into the merchant's account if the verification is correct.

$$s^e = H(H^{10-a}(\beta_1)||H^a(\beta_2)||H^{12-b}(\beta_3)||H^b(\beta_4)||H^{31-c}(\beta_5)||H^c(\beta_6)||y) \bmod n \quad (4)$$

Discussions and analyses

In this section, we discuss Fan et al.'s scheme and our schemes, and analyze the efficiency between them.

Discussions

Because the main idea of the proposed schemes is the same as Fan et al.'s scheme, we make more precise explanations between them in this subsection. There are two major differences, one is the format of date presentation of the E-cash and the other is the concept of absolute or relative date in the E-cash.

The date presentation: About the term of year presentation, Fan et al. supposed an E-cash has a hundred years period to use. However, a bill used in a real world may not over 10 years, so we think a decade term is enough for most of E-cash systems. To denote the year a, Fan et al.'s scheme uses (1 + (the two least significant digits of a year)) and our schemes use (the least significant digit of a year). For example, the present date is May 20, 2014, the date of E-cash (a, b, c) is (15, 5, 20) in Fan et al.'s scheme, (4, 5, 20) in our basic scheme or (4, 5, 20) with based year $y = 2010$ in our advanced scheme. When decoding the year of date, Fan et al.'s scheme should subtract 1 from the year parameter a, the basic scheme just use the year parameter a and the advanced scheme should add the based year y to year parameter a. As the previous example, to decode the real year of Fan et al.'s scheme is $a - 1 = 15 - 1 = 14$, of the basic scheme is $a = 4$ and of the advanced scheme is $y + a = 2010 + 4 = 2014$. Obviously, our advanced scheme can present the precise year.

The relative year presentation: The basic idea of Fan et al. is to use the two least significant digits of a year to present the year of an E-cash but it results in a problem. For example, in December 31, 2098, the client Cindy can set (a, b, c) as (99, 12, 31), but she cannot use this E-cash in the next day, January 1, 2099. The reason is the date will be set as (00, 1, 1) and this presentation is the same as to set the attached date January 1, 1998. In other words, they set down an absolute day among a centurial period in their E-cash system. Nevertheless, our advanced scheme uses the relative date concept which attached a based year with an index year of ten years period. This proposed scheme can extend the date to more than a century, or any valid day. For example, a client Cindy gives an E-cash to her grandchild and wants to set one hundred years after now, e.g. 2104. In our advanced scheme, she can set the based year $y = 2100$ and year parameter $a = 4$ as an index year. Nevertheless, it is impossible to set the exact year 2104 in Fan et al.'s scheme. Also, with the ten year period for adjusting, the proposed advanced scheme is more flexible then Fan et al.'s scheme.

In addition, the other useful application is the term of validity of E-cash. As our assumption, an E-cash should have an expired date for using, such as defined in our scheme with ten years. Only our advanced scheme can easier reach the goal. For example, the bank defines the term of validity of E-cash is ten years from the date withdrew. Therefore, the bank directly sets the based year parameter with the present year, such as 2004, and the client only sets the date triple (a, b, c) what she desires, such as (9, 12, 30). No matter both banks and client are whether synchronization or not, they should have the same year. Therefore, the client can set any day from the January 1 of the based year, 2004 now, and no longer than the December 31 of year $y + 9$, 2013 in this example. In the worst case, the

E-cash has at least nine years life time in our scheme when a client withdraws on December 31, but only one day in Fan et al.'s scheme when a client set the date on December 31 of two least significant digit of year is 98. As the above reasons, our advanced scheme offers a better solution in deal with the expired date proceeding.

Analyses

Efficiency analysis: The number of the hash function computing is $4 \times (100 + 12 + 31) = 572$ times in Fan et al.'s scheme and $4 \times (10 + 12 + 31) = 212$ times in our schemes. If desiring to present a chiliad period, Fan et al.'s scheme needs $4 \times (1000 + 12 + 31) = 4172$ times of hash executions but ours still keeps 212 times. If presenting a precise year, Fan et al.'s scheme needs $4 \times (10000+12+31) = 40172$ times of hash executions but ours still keeps 212 times. It is obvious that our scheme reduce 63% computing amount in a century period, 95% computing amount in a chiliad period and 99% computing amount in a thousand years period. The extra load is the advanced scheme has an additional parameter y transmitting in the network, but it is trivial.

Properties analysis: The properties of the E-cash are still existent because the proposed schemes are based on the Fan et al.'s scheme [5]. Therefore, we do not state them again, but just explain the difference. These three schemes are based on a partially blind signature [8]. The extra parameter, based year y, in the advanced scheme is also the information of the partially blind signature so it does not affect the properties of the E-cash system.

Security analysis: Due to our assumption, the term of validity of an E-cash is limited in a term of ten years, so any E-cash cannot allow being used over a term. In other words, an E-cash is only valid inside a term. If an attacker got the whole information flowing in the network, he still cannot break the data protected by the one way hash function. Also, an attacker cannot forget any E-cash, because all E-cashes should be signed by bank and are protected by the hash chain pair well. In addition, the double spending will be detected by bank due to the on-line checking system. In summary, the proposed schemes are secure.

Conclusions

The proposed schemes are based on the Fan et al.'s scheme, so they also inherit the readable date in an E-cash, the properties of the E-cash and the security of the scheme. However, there are too many hash function executions in Fan et al.'s scheme, and the absolute year limits the expired date of the E-cash. Therefore, the improved schemes not only have better efficiency improved than Fan et al.'s scheme but also extend the date which can be presented.

In the previous section, we had shown our useful idea, the relative concept in the date attachment, for date extension using or expired date design even a long future date expressing. Besides, the remarkable improvement of the efficiency is stated and the security of the proposed schemes is analyzed. Therefore, the proposed schemes are efficient and secure. Especially, the advanced scheme is more powerful in the readable date expression.

Acknowledgments

This study was supported by the National Science Council of Taiwan under grant NSC 98–2221–E–005–050- MY3. The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] M. Abe, E. Fujisaki, K. Kim and T. Matsumoto, How to Date Blind Signatures, Proceedings of the 2nd International Conference on the Theory and Applications of Cryptology and Information Security: Advances in Cryptology, Kyongju, Korea, 1996, pp. 244-251.

[2] D. Chaum, D. Chaum, R. L. Rivest and A. T. Sherman, Blind Signatures for Untraceable Payments, Proceedings of Crypto '82: Advances in Cryptology, California, USA, 1982, pp. 199-203.

[3] D. Chaum, A. Fiat and M. Naor, Untraceable Electronic Cash, Proceedings of Crypto '88: Advances in Cryptology, California, USA, 1988, pp. 319-327.

[4] C.-I. Fan and C.-L. Lei, Low-computation Partially Blind Signatures for Electronic Cash, IEICE Trans. Fundamentals E81-A(5) (1998) pp. 818-824.

[5] C.-I. Fan, W.-K. Chen and Y.-S. Yeh, Date attachable electronic cash, Comput. Commun 23(4) (2000) 425-428.

[6] M.-S.Hwang, I.-C. Lin and L.-H. Li, A Simple Micro-payment Scheme, J. Syst. Software 55(3) (2001) 221-229.

[7] M.-S. Hwang, C.-C. Lee and Y.-C. Lai, Traceability on Low-Computation Partially Blind Signatures for Electronic Cash, IEICE Trans. Fundamentals E85-A(5) (2002) 1181-1182.

[8] M.-S. Hwang, C.-C. Lee and Y.-C. Lai, Traceability on RSA-Based Partially Signature with Low Computation, Appl. Math. Comput. 145(2) (2003) 465-468.

[9] M.-S. Hwang, C.-C. Lee and Y.-C. Lai, Traceability on Stadler et al.'s Fair Blind Signature Scheme, IEICE Trans. Fundamentals E86-A(2) (2003) 513-514.

[10] M.-S. Hwang, C.-C. Lee and Y.-C. Lai, An Untraceable Blind Signature Scheme, IEICE Trans. Fundamentals E86-A(7) (2003) 1902-1906.

[11] S. Kim and H. Oh, Efficient Anonymous Cash Using the Hash Chain, IEICE T. Commun. E86-B(3) (2003) 1140-1143.

[12] C.-C. Lee, M.-S. Hwang and W.-P. Yang, Untraceable Blind Signature Schemes Based on Discrete Logarithm Problem, Fund. Inform. 55(3-4) (2003) 307-320.

[13] C.-C. Lee, M.-S. Hwang and W.-P. Yang, A New Blind Signature Based on the Discrete Logarithm Problem for Untraceability, Appl. Math. Comput. 164(3) (2005) 837-841.

[14] J. Li and S, Wang. New Efficient Proxy Blind Signature Scheme Using Verifiable Self-certified Public Key, International Journal of Network Security 4(2) (2007) 193-200.

[15] J.-W Lo, M.-S Hwang and Y.-P Chu, An Exchangeable E-Cash Scheme by E-mint, the proceedings of the 8th International Conference on Intelligent Systems Design and Applications 3(2008) 246-251.

[16] N. A. Moldovyan and A. A. Moldovyan, Blind Collective Signature Protocol Based on Discrete Logarithm Problem, International Journal of Network Security 11(2010) 44-48.

[17] N. A. Moldovyan, Blind Signature Protocols from Digital Signature Standards, International Journal of Network Security 13(1) (2011) 202-205.

[18] G. K. Verma, Probable Security Proof of a Blind Signature Scheme over Braid Groups, International Journal of Network Security 12(2) (2009) 118-124.