休閒運動管理學刊
第二期 93 頁-97 頁
民國一〇四年九月

Journal of Leisure and Sports Management
No.2 pp.93~97
September 2015

Remark on the design of secure digital blind signature schemes and their applications

Chun-Te Lee Huna-Mei Chu

Cheng Shiu University

Abstract

Over nearly 30 years, digital signature has been developed under the assumption t hat both attackers and attackees are equipped with exactly identical computing facilitie s [1-7, 9, 11]. If this is not the case, in practical E commerce applications, there exis ts a risk that passwords of attackees could be cracked by attackers who use fake iden tities to commit many types of crime on the internet. As a consequence, the entire E commerce environment holds threats. For this sake, a blind signature scheme [12] was proposed, while such proposal is found against the fundamentals of a fail stop schem e, not as it claims to be. Accordingly, a novel fail stop scheme is presented in this w ork as an effective way to make a secure E-commerce environment against any sort o f attack.

Key Words: Untraceability, Fail-stop Signature, Blind Signature, Network Security, Information Security

1 Introduction

The initial use of passwords to prevent unintended releases of confidential messages can be dated back to 1000 years ago. These days, applications of cryptotography can be found ubiquitously in many aspects such as the military, commerce, technology, daily life, etc. Taking the popular E commerce nowadays as an instance, there is a growing demand for transactions over internet, including communication, money transfer, document deliveries, virtual book stores, online shopping, even online banks, etc. The applications of cryptotography are thus seen more important as the number of network crimes rises.

The strength of a crypotographic algorithm is measured as the time required to crack an encrypted code on the condition that the computing facilities on an attacker side are identical to those on an attackee side. Accordingly, a long period of time required indicates a high security level of such algorithm, and vice versa. In case a crime group is of a high performance computing facility, passwords can be cracked within an extremely limited time frame and fake identities are employed by hackers to access business secrets. Consequently, there is a tremendous loss in the credit of attackees and online transactions. Under such circumstance, attackees must find a way to prove their innocence, and enterprises must ensure clients a well secure network system in order that online business transactions can be resumed as expected. For this sake, proposed in 2004 by Katja Schmidt-Samoa, an improved version of [8], presented in 2000, is developed based on a fail stop scheme [10, 11], requiring factorization. Albeit such scheme is proven able to clear the attackees of charges, the price paid is the disclosure of the information on $n = p \times q$. For safety concern, system parameters must be replaced, leading to a negative effect on the network operation for enterprise's sake.

The point is to find an effective way to recognize a forgery and prevent attackers from denial of forgery while keeping $n = p \times q$ secret. In light of this, a novel fail stop scheme is proposed against [12] due to the inherent disadvantages thereof. This work is outlined as follows: section II is devoted to a literature review, the novel signature scheme is described in section III, and this work is concluded at the end with futuristic research directions.

2 Literature Review

The work [12] is stated in brevity as follows.

Initialization: As the first step, a trusted dealer D chooses two large prime numbers p and q such that $p = 2p'+1$ and $q = 2q'+1$, where p' and q' are both prime numbers as well. Computing $n = pq$ and $\varphi(n) = (p-1)(q-1)$, e_D and d_D are then chosen by the trusted dealer D so as to satisfy $e_D d_D \equiv 1 \bmod \varphi(n)$. Subsequently, an integer $\alpha \in z_n^*$ is randomly selected and $\beta = \alpha^{d_D} \bmod n$ is evaluated. Finally, publishing a public key (α, n) thereof, D keeps a private key d_D secret, sending (e_D, β) to a signer S via a secure channel.

Key generation: Randomly choosing a private key (k_1, k_2, k_3, k_4), where $k_i \in Z_n^*$, the signer S computes $\beta_1 = \alpha^{k_4}\beta^{k_3} \bmod n$, $\alpha_1 = \alpha^{k_3}\beta_1^{k_1} \bmod n$ and $\alpha_2 = \alpha^{k_4}\beta_1^{k_2} \bmod n$. Finally, S has her/his public key$(\beta_1, \alpha_1, \alpha_2)$ and a one-way hash function H published.

Blinding: Given a message m, a receiver R selects a random number r out of z_n^*. R computes $\widetilde{m} = rH(m) \bmod n$ with a blinding factor r, where $H(m)$ denotes the hashed value of the message m. Then, R sends a blinded message $\widetilde{m}$ and $x = H(r) \bmod n$ to S.

Signing: In this phase, computing blinded signatures $\widetilde{s}_1 = \widetilde{m}(k_1 x + k_2)$ and $\widetilde{s}_2 = \widetilde{m}(k_3 x + k_4)$, S sends $(\widetilde{s}_1, \widetilde{s}_2)$, with which the blinded message $\widetilde{m}$ is signed, to R.

Unblinding: Following the reception of the blinded signature $(\widetilde{s}_1, \widetilde{s}_2)$, an unblinding operation is performed by the receiver R through $s_1 = r^{-1}\widetilde{s}_1$ and $s_2 = r^{-1}\widetilde{s}_2$. Then, (s_1, s_2) is evaluated as the signature on the hashed message $H(m)$.

Verification: Anyone can verify the message-signature $(H(m)$, x, s_1, $s_2)$ by checking whether $\alpha^{s_2}\beta_1^{s_1} = \alpha_1^{H(m)}\alpha_2 \bmod n$ holds true.

Proof of forgery: This phase is similar to the scheme proposed by Susilo et al. The signer can identify a forgery by revealing non-trivial factors of n .

3 The weakness of the design of secure digital blind signature schemes and their applications

A fail stop scheme is applied to a case where an attacker is of a superior computing facility relative to an attakee, that is, the attacker is able to find an easy way to crack the private key associated with a public key released by the attackee. Consequently, attakcers, using fake identities, take illegal action on the internet. For this sake, there have been a number of research works addressing this issue [1, 8, 10], among which [8, 10] are treated as representative pieces particularly. The work [12] can be said to be an original proposal in terms of non fail stop schemes. Unfortunately, during the initialization stage, an attacker can find out a pubic key pair (α,n), key generation ($\beta_1, \alpha_1, \alpha_2$), blind signature ($\tilde{m}$,x = H(r) mod n) of a trusted dear D. Since the attacker acquires high performance computing facilities, m can be derived from x, following which $\tilde{m}'$ can be forged for taking attack.

4 Our Proposal

A large prime number p_1 is selected by a system center to satisfy $n \mid p_1 - 1$, where n represents the product of two large prime numbers p and q. subsequently, a number g with a modulo p_1 and an order p is chosen by system center 2, represented as

$$g^{\frac{1}{2}p-1} \equiv -1 (\bmod p_1) \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

The open public keys released by the system center are p_1, g and n, while the associated private keys are p and q.

4.1 Registration Phase

A user A selects two distinct numbers x_1, $x_2 \in z_n^*$, evaluating

$$y_i \equiv g^{x_i} (\bmod p_1) , \quad 1 \le i \le 2 \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (2)$$

The user A, holding $\{y_1, y_2\}$ as the public keys, signs up in the system center, while the private keys x_i, $1 \le i \le 2$, are kept secret.

4.2 Signature Phase

In the event that A has an intention to send B an digitally signed message m , the following procedure must be performed.

(1) Evaluate

$$a \equiv mx_1 + x_2 (\bmod n) \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (3)$$

$$s_1 \equiv g^a (\bmod p_1) \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (4)$$

$$s_2 \equiv g_1^a (\bmod p_1) \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (5)$$

(2) Select three distinct numbers $k_i \in z_m^*$, $1 \le i \le 3$, and evaluate

$$r_1 \equiv g^{k_1} (\bmod p_1) \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (6)$$

$$r_2 \equiv g_1^{k_2} (\bmod p_1) \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (7)$$

$$s_1 \equiv ar_1 + k_1 b_1 (\bmod n) \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (8)$$

$$s_2 \equiv ar_2 + k_2 b_2 (\bmod n) \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (9)$$

(3) Send $\{r_i, b_i, s_j\}$, $1 \le i \le 3$, $1 \le j \le 2$, to a user B.

4.3 Verification Phase

Following the reception of all the relevant information, B evaluates

$$s_1 \equiv y_1^m y_2 (\bmod p_1) \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(10)$$

$$g^{s_1} \equiv s_1^{r_1} r_1^{b_1} (\bmod p_1) \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(11)$$

$$g_1^{s_2} \equiv s_2^{r_2} r_2^{b_2} (\bmod p_1) \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(12)$$

In case all the above equations are satisfied, *m* is accepted. Otherwise, it gets rejected.

4.4 Dispute handling Phase

Suppose that the message sent from B to A is forged into $\{r_i^{'}, b_i^{'}, s_j^{'}\}$, $1 \le i \le 3$, $1 \le j \le 2$. After all the steps listed in the signature phase are performed by A, B then repeats those in the verification phase. There exists a $(1-q^{-1})$ probability that $s_1 \ne s_2^{'} (\bmod n)$ as an evidence that a message has been forged.

5 Discussion and Future Research Directions

A novel fail stop scheme is proposed in this work to prevent attackers from denial of forgery without revealing the information on $n = p \times q$. A great number of research activities have been done toward building secure E-commerce systems over the internet. To this end, this work is proposed as an effective means to render a secure signature scheme. A number of futuristic research directions are suggested as follows.

(1) Build up the security of signature schemes on the basis of this work.

(2) reduce the CPU time and the number of parameters required.

(3) build a blind signature scheme based upon a fail stop scheme.

References

1. N. Bari’c and B. Pfitzmann. Collision-free accumulators and fail-stop signatures without trees.advances in Cryptology – Eurocrypt ’97, Lecture Notes in Computer Science 1233, pages 480-494, 1997.
2. J.J.R. Chen and Y. Liu , A Traceable Group Signature Scheme, Mathematical and Computer Modelling 31, 147-160, 2000.
3. W. Diffie and M. Hellman. New directions in cryptography. IEEE IT, 22:644-654, 1976.
4. T. ELGamal, A public-key cryptosystem and a signature scheme based on discrete logarithms, IEEE Trans. On Information Theory II-31 (4), 469-472, 1985.
5. Niven, H.S. Zuckerman and H.L. Montgomery, An Introduction to the Theory of Numbers, John Wiley and Sons, 1991.
6. M.O. Rabin, Digitalized signatures and public-key functions as intractable as factorization, Technical Report LCS/TR 212, MIT, Cambridge, MA, 1979.
7. R.L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. Comm. Of the ACM, 21, no. 2:120-126, 1978.
8. Katja Schmidt-Samoa. Factorization-based Fail-Stop Signatures Revisited. In: Information and Communications Security (ICICS 2004), LNCS 3269, pp. 118-131.Springer-Verlag, 2004.
9. D. R. Stinson. Cryptography: Theory and Practice. CRC Press, Boca Raton, New York, 1995.
10. Willy Susilo, Rei Safavi-Naini, Marc Gysin, and Jennifer Seberry. A new and efficient fail-stop signature scheme. The Computer Journal, 43(5):430–437, 2000.
11. Willy Susilo, Rei Safavi-Naini, Pieprzyk, J., RSA-based fail-stop

signature schemes, 1999 International Workshop on Parallel Processing, 161-166, 1999.
12. L.-C. Wu, The Design of Secure Digital Blind Signature Schemes and Their Applications, 2005 Thesis for doctor of Science Department of Computer Science and Engineering National Chiao Tung University