Fail-Stop Blind Signature Scheme Based on the Integer Factorization

Lin-Chuan Wu[1], Chun-I Fan[2], Yi-Shiung Yeh[1] and Tsann-Shyong Liu[3]

[1] Department of Computer Science and Information Engineering
National Chiao Tung University
Hsinchu, Taiwan 300, R.O.C.

[2] Department of Computer Science and Engineering
National Sun Yat-Sen University
Kaoshing, Taiwan, R.O.C.

[3] Telecommunication Laboratories
Chunghwa Telecom Co., Ltd.
12, Lane 551, Min-Tsu Road Sec. 5
Yang-Mei, Taoyuan, Taiwan 326, R.O.C.

Abstract*-In this paper, we proposed the first fail-stop blind signature scheme based on the integer factorization to obtain unforgeability and anonymity properties. It can be applied in more critical system like electronic payment systems which need higher security against more powerful forger and can preserve participants' anonymity.*

Keywords: Fail-Stop Signature, Blind Signature, RSA cryptosystem, Cryptography, Information Security.

1. Introduction

A digital signature can provide analogous to ordinary hand-written signature for achieving non-repudiation property. Diffie and Hellman [4] introduced the concept of digital signature in 1976, and then Rivest, Shamir, and Adleman [7] proposed the first digital signature scheme in 1978. RSA public-key cryptosystem is based on the integer factoring problem and the security of the cryptosystem relies on that computational assumption. However, such signatures are only computationally secure for the signer because a forger may forge a signature with unlimited computational power. This means that there is no mechanism to protect a signer against a forged signature which has succeeded in signature verification. Namely, if a signed message succeeds in signature verification it is assumed to be generated by the owner of the private key.

To overcome this kind of attack, Waidner and Pfitzmann [9] proposed the first fail-stop signature. Fail-stop signature can protect a signer against a forger even with unlimited computational power because the possibility of finding the signer's right private key in the fail-stop signature is negligible. The signer can use "proof of forgery" algorithm to prove the signature is forgery. It achieves "proof of forgery" by showing that the underlying computational assumption has been broken. The signer can stop the system if a forgery occurs – hence named fail-stop signature scheme. The signer is unconditionally secure and the recipient is cryptographically secure in the fail-stop signature scheme. One important application of the fail-stop signature is electronic payment system [6]. The anonymity of participants is very important in electronic payment systems. However, it cannot be achieved in the fail-stop signature.

Chaum [3] introduced the concept of a blind signature scheme which can protect the anonymity of participants. The blind signature scheme allows a user to obtain a message signed by the signer without revealing message and the signer cannot link any message-signature pair later. The blind signature scheme can be used in electronic payment systems to preserve participants' anonymity.

In this paper, we propose the first fail-stop blind signature scheme which is based on RSA-based fail-stop signature scheme presented by Susilo, Safavi-Naini and Pieprzyk [8]. Our scheme can provide "proof of forgery" for signers and guarantee "anonymity" for participants. We will give sufficient proof to show that the proposed scheme satisfies the conditions of fail-stop signature and blind signature. It can provide more secure cryptographic primitive for applying in electronic payment systems.

This paper is organized as follows. RSA-based fail-stop signature scheme will be reviewed in Section 2. In Section 3, we propose a fail-stop blind signature scheme based on the integer factorization problem. In Section 4, we show that the proposed scheme satisfies the conditions of fail-stop signature and blind signature. Finally, we give brief conclusions in Section 5.

2. RSA-based Fail-Stop Signature

Susilo, Safavi-Naini and Pieprzyk [8] presented two RSA-based fail-stop signature schemes (with or without a trusted dealer). We only consider the scheme with trusted dealer here for simplicity. Actually, the signer and the receiver can instead of trusted dealer to perform the initialization phase by using Boneh-Franklin's algorithm [2]. There are three kinds of participants, which are the trusted dealer, the sender and the receiver in the Susilo et al.'s scheme with trusted dealer. A forged signature can be proved by using Miller's [5] and Bach's [1] methods to reveal non-trivial factors for the signer. The detailed scheme is described as follows.

(1) Initialization phase : The two large prime numbers p and q are chosen by D, such that $p = 2p'+1$ and $q = 2q'+1$, where p' and q' are also prime [2]. Then, D computes $n = pq$ and $\phi(n) = (p-1)(q-1)$. Next, D selects d_D as her/his private key and computes $e_D = d_D^{-1} \bmod \phi(n)$, where $GCD(d_D, \phi(n)) = 1$. Then, D selects a random number $\alpha \in Z_n^*$ and computes $\beta = \alpha^{d_D} \bmod n$. Finally, D publishes his public key (α, n) and sends (e_D, β) to S securely.

(2) Key generation phase : S selects four random numbers, which are k_1, k_2, k_3 and k_4 as the private key, where $k_i \in Z_n^*$, $1 \le i \le 4$. Next, 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, he publishes his public key $(\beta_1, \alpha_1, \alpha_2)$.

(3) Signature generation phase : S computes $y_1 = k_1 x + k_2$ and $y_2 = k_3 x + k_4$, where $x \in Z_n^*$ is a message. Then, he publishes the signature (y_1, y_2) on message x.

(4) Signature verification phase : R can verify the signature by checking the formula $\alpha^{y_2}\beta_1^{y_1} = \alpha_1{}^x\alpha_2 \bmod n$. If it is true, this signature is a valid one.

(5) Proof of forgery phase : If a forged signature (y_1', y_2') on message x succeeds in signature verification phase, S can prove that a forgery has occurred by executing the following steps.

1. To construct the right signature (y_1, y_2) on message x.

2. To compute $Z_1 = (y_1' - y_1)$ and $Z_2 = (y_2 - y_2')$.

3. To compute $\gamma = e_D(Z_2 - k_4 Z_1) - k_3 Z_1 = c\phi(n)$

4. To find non-trivial factors of n by using Miller's [5] and Bach's [1] methods.

5. The non-trivial factors of n is the proof of forgery.

3. Fail-Stop Blind Signature Scheme

The fail-stop blind signature scheme combines the advantages of both fail-stop signature and blind signature. Our proposed scheme is a modification of Susilo et al.'s scheme with trusted dealer. There are seven phases (1) Initialization, (2) Key generation, (3) Blinding, (4) Signing, (5) Unblinding, (6) Verification and (7) Proof of forgery in the fail-stop blind signature scheme. The three kinds of participants in our scheme are the same as the section 2. The detailed scheme is described bellow.

(1) Initialization phase : Initially, the trusted dealer D chooses two large primes p and q such that $p = 2p'+1$ and $q = 2q'+1$, where p' and q' are also prime. D computes $n = pq$ and $\phi(n) = (p-1)(q-1)$. Next, e_D and d_D are chosen by the trusted dealer such that $e_D d_D \equiv 1 \bmod \phi(n)$. Then, D chooses a integer $\alpha \in Z_n^*$ randomly and computes $\beta = \alpha^{d_D} \bmod n$. Finally, D publishes his public key (α, n), keeps his private key d_D secretly and sends (e_D, β) to S via secure channel.

(2) Key generation phase : The signer S randomly chooses his private key (k_1, k_2, k_3, k_4), where $k_i \in Z_n^*$ and 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 publishes his(her) public key $(\beta_1, \alpha_1, \alpha_2)$ and a one-way hash function H.

(3) Blinding phase : For a message m, the receiver R selects a random numbers r in Z_n^*. R computes $\tilde{m} = rH(m) \bmod n$ with a blinding factor r, where $H(m)$ is the hashed value of message m. Then, R sends the blinded message $\tilde{m}$ and $x = H(r) \bmod n$ to S.

(4) Signing phase : In this phase, S computes $\tilde{s}_1 = \tilde{m}(k_1 x + k_2)$ and $\tilde{s}_2 = \tilde{m}(k_3 x + k_4)$. S sends the blinded signature $(\tilde{s}_1, \tilde{s}_2)$ on blinded message $\tilde{m}$ to R.

(5) Unblinding phase : After R obtains the blinded signature $(\tilde{s}_1, \tilde{s}_2)$, he(she) performs the unblinding operation by computing $s_1 = r^{-1}\tilde{s}_1$ and $s_2 = r^{-1}\tilde{s}_2$. Then, (s_1, s_2) is the signature on hashed message $H(m)$.

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

(7) Proof of forgery phase : This phase is similar to Susilo et al.'s scheme in section 2. The signer can prove that a forgery has occurred by revealing the non-trivial factors of n.

4. Security Analysis

A secure fail-stop blind signature scheme must satisfy four conditions as follows.

(1) The forger is nearly impossible to forge a signature even with unlimited computational power.

(2) The signer can use a polynomial-time algorithm to prove that a forgery has occurred.

(3) The polynomial-bounded signer cannot forge a signature and prove it a forgery later.

(4) The signer is computationally infeasible to link the message he actually signed and the corresponding signature for verification later.

Lemma 1: *There equally like exists $\phi(n)^2$ matching private keys for each public key, such that different private key generate different signature on the same message.*

Lemma 2: *The signer can prove that a forgery has occurred by factorizing n if a forged signature (s_1', s_2') on a message m succeeds in verification phase.*

Lemma 3: *The signer can prove that a forgery has occurred by the probability $\frac{\phi(n)-1}{\phi(n)}$.*

The detailed proofs of **Lemma 1, 2** and **3** are described in Susilo et al. [8]. The second condition of a secure fail-stop blind signature is satisfied by **Lemma 2**. **Theorem 1** shows that a forger even with unlimited computational power, still there exists $\phi(n)$ possible private keys for that signature.

Theorem 1: *The forger even with unlimited computational power still existing $\phi(n)$ possible private keys for that blinded signature $(\tilde{s}_1, \tilde{s}_2)$ on the blinded message $\tilde{m}$ together with corresponding public key.*

Proof: To Assume the forged blinded signature on the blinded message $\tilde{m}$ is $(\tilde{s}_1', \tilde{s}_2')$ and the public key of the signer is $(\beta_1, \alpha_1, \alpha_2)$. If a forger with unlimited computational power can solve the discrete logarithm and factorization problem successfully, he can obtain these equations as follows.

$$\tilde{s}_1' = (k_1 x + k_2)\tilde{m} \bmod \phi(n)$$
$$\tilde{s}_2' = (k_3 x + k_4)\tilde{m} \bmod \phi(n)$$
$$c_1 = (k_3 + wk_1) \bmod \phi(n)$$
$$c_2 = (k_4 + wk_2) \bmod \phi(n)$$

Where $\tilde{m} = rH(m)$, $x, c_1, c_2 \in Z_n^*$ and $w = \log_\alpha \beta_1 = k_4 + d_D k_3$. Then, a forger can rewrite these equations by using matrix representation.

$$\begin{bmatrix} x\tilde{m} & \tilde{m} & 0 & 0 \\ 0 & 0 & x\tilde{m} & \tilde{m} \\ w & 0 & 1 & 0 \\ 0 & w & 0 & 1 \end{bmatrix} \begin{bmatrix} k_1 \\ k_2 \\ k_3 \\ k_4 \end{bmatrix} = \begin{bmatrix} \tilde{s}_1' \\ \tilde{s}_2' \\ c_1 \\ c_2 \end{bmatrix}$$

The above matrix's rank is 3 because $x\tilde{m}r_3 - wr_1 - r_2 + \tilde{m}r_4 = 0$, where r_i is the i-th row of the matrix. There are $\phi(n)$ possible private keys for that blinded signature since the solutions of equations are $\phi(n)$. □

Lemma 4: *The forger even with unlimited computational power cannot generate the blinded signature on a new message.*

Theorem 2: *The polynomial-bounded signer cannot generate a valid signature and prove it a forgery later.*

Proof: The polynomial-bounded signer must have another private key (k_1', k_2', k_3', k_4') which can match the corresponding public key $(\beta_1, \alpha_1, \alpha_2)$ to deny a generated valid signature, such that $\alpha_1 = \alpha^{k_3'} \beta_1^{k_1'} \bmod n$ and $\alpha_2 = \alpha^{k_4'} \beta_1^{k_2'} \bmod n$. The difficulty to find another private key (k_1', k_2', k_3', k_4') is equivalent to solve the discrete logarithm problem. Moreover, it is difficult to find d_D without knowing $\phi(n)$ since the difficulty of integer factorization. Hence, the proposed scheme satisfies the third condition of a secure fail-stop blind signature by **Theorem 2**. □

Theorem 3: *There exists a unique private key corresponding to the public key, the blinded signature* $(\tilde{s}_1, \tilde{s}_2)$ *on the blinded message* $\tilde{m}$ *and a valid blinded signature* $(\tilde{s}_1', \tilde{s}_2')$ *on the blinded message* $\tilde{m}'$, *where* $\tilde{m} \neq \tilde{m}'$.

Proof: From **Theorem 1**, the forger even with unlimited computational power still existing $\phi(n)$ possible private keys for the blinded signature on the blinded message corresponding the public key. The signer can organize these equations as follows.

$$\tilde{s}_1 = (k_1 x + k_2)\tilde{m} \bmod \phi(n)$$
$$\tilde{s}_2 = (k_3 x + k_4)\tilde{m} \bmod \phi(n)$$
$$\tilde{s}_1' = (k_1 x + k_2)\tilde{m}' \bmod \phi(n)$$
$$\tilde{s}_2' = (k_3 x + k_4)\tilde{m}' \bmod \phi(n)'$$
$$c_1 = (k_3 + wk_1) \bmod \phi(n)$$
$$c_2 = (k_4 + wk_2) \bmod \phi(n)$$

Where $\tilde{m} = rH(m)$, $x, c_1, c_2 \in Z_n^*$ and $w = \log_\alpha \beta_1 = k_4 + d_D k_3$. The matrix representation of above equations can rewrite as follows.

$$\begin{bmatrix} x\tilde{m} & \tilde{m} & 0 & 0 \\ 0 & 0 & x\tilde{m} & \tilde{m} \\ x\tilde{m}' & \tilde{m}' & 0 & 0 \\ 0 & 0 & x\tilde{m}' & \tilde{m}' \\ w & 0 & 1 & 0 \\ 0 & w & 0 & 1 \end{bmatrix} \begin{bmatrix} k_1 \\ k_2 \\ k_3 \\ k_4 \end{bmatrix} = \begin{bmatrix} \tilde{s}_1 \\ \tilde{s}_2 \\ \tilde{s}_1' \\ \tilde{s}_2' \\ c_1 \\ c_2 \end{bmatrix}$$

Since $\tilde{m} \neq \tilde{m}'$, The above coefficient matrix's rank is 4. Hence, the private key is unique corresponding to the public key. We prove that the first condition of a secure fail-stop blind signature is satisfied from **Theorem 3**. □

Theorem 4: *The signer computationally cannot link the blinded message* $\tilde{m}$ *he actually signed and the corresponding signature* (s_1, s_2) *for verification later.*

Proof: In the signing phase, the signer can obtain the blinded message $\tilde{m} = rH(m)$ and $x = H(r) \bmod n$. The signer can obtain the signature (s_1, s_2) in the verification phase, where

$$s_1 = r^{-1}\tilde{s}_1 = (k_1 x + k_2)H(m)$$
$$s_2 = r^{-1}\tilde{s}_2 = (k_3 x + k_4)H(m)$$

The signer is computationally infeasible to link the blinded message and the signature for verification later since a blinding factor is chosen randomly by the receiver. The last condition of a secure fail-stop blind signature is satisfied by **Theorem 4**. □

5. Conclusions

Waidner and Pfitzmann presented the first fail-stop signature that can provide a signer to prove the signature is forgery. In this paper, we propose the first fail-stop blind signature scheme and give sufficient proof to prove that it satisfies the conditions of fail-stop signature and blind signature. It is suitable to be applied in untraceable electronic payment systems which need higher security against an unlimited forger and can preserve the anonymity of participants.

References

[1] E. Bach, "Discrete Logarithm and Factoring," *Report no. UCB/CSD 84/186, Comp. Sc. Division (EECS)*, University of California, Berkeley, 1984.

[2] D. Boneh and M. Franklin, "Efficient Generation of Shared RSA keys," *Advances in Cryptology - CRYPTO '97*, LNCS Vol. 1294 (1997), Springer-Verlag, pp. 425-439.

[3] D. Chaum, "Blind Signatures for Untraceable Payments," *Advances in Cryptology - CRYPTO '82*, Plenum Press (1983), pp. 199-203.

[4] W. Diffie and M. Hellman, "New Directions in Cryptography," *IEEE Trans. Information Theory*, Vol. IT-22 (1976), pp. 644-654.

[5] G. L. Miller, "Riemann's Hypothesis and Tests for Primality," *Journal of Computer and System Sciences*, Vol. 13 (1976), pp. 300-317.

[6] B. Pfitzmann and M. Waidner, "Fail-Stop Signatures and Their Applications," *SECURICOM P1*, Paris (1991), pp. 145-160.

[7] R. L. Rivest, A. Shamir, and L. M. Adleman, "A Method for Obtaining Digital Signatures and Public-key Cryptosystems," *Communications of the ACM*, Vol. 21 (1978), pp. 120-126.

[8] W. Susilo, R. Safavi-Naini, and J. Pieprzyk, "RSA-based Fail-Stop Signature Schemes," *International*

Workshop on Security, IEEE Computer Society Press (1999), pp. 161-166.

[9] M. Waidner and B. Pfitzmann, “The Dining Cryptographers in the Disco : unconditional sender and recipient untraceability with computationally secure serviceability,” *Advances in Cryptology - EUROCRYPT '89,* LNCS Vol. 434 (1989), Springer-Verlag, pp. 690.