1998 International Computer Symposium
Workshop on Cryptology and Information Security
December 17-19, 1998, N.C.K.U., Tainan, Taiwan, R.O.C.

Digital Multisignature Scheme Giving Message Recovery Using RSA-based Self-Certified Public Keys

Yuh-Shihng Chang, Tzong-Chen Wu and Jung-Hui Chiu*

Department of Information Management
National Taiwan University of Science and Technology
Taipei, Taiwan 106, Republic of China
E-mail:{D8309002, tcwu}@cs.ntust.edu.tw

*Department of Electronic Engineering
National Taiwan University of Science and Technology
Taipei, Taiwan 106, Republic of China
E-Mail: jhchiu@et.ntust.edu.tw

ABSTRACT

The authors propose a new digital multisignature scheme giving message recovery using RSA-based self-certified public keys. Any group of signers can sign a message giving message recovery without or with signer-anonymity. For the purpose of verifying the authenticity of the public key(s), no additional certificate is required. Besides, the processes of verifying a multisignature, recovering the message from the multisignature, and verifying the authenticity of the signer's public key can be accomplished at a time.

1.Introduction

Most previously proposed digital signature schemes not giving message recovery (e.g., [1-4]) or giving message recovery (e.g., [5-11]) are vulnerable to the active attacks, such as the substitution of a fake public key to a genuine one in a key directory or during key delivery [12, 13]. These active attacks also threaten the multisignature schemes developed from Diffie-Hellman [14] or RSA [3] public key system. In order to avoid the active attacks, the verifier of a signature/multisignature should verify the signer's public key before using it. That is, the satisfaction of verifying a signature/multisignature absolutely depends on the satisfaction of verifying the signer's public key.

Recently, Girault [12] introduced a new public key system, referred to the *self-certified public key system*, to resolve the public key verification problem. In Girault's system, no additional certificate for verifying the public key is required. User's secret key is randomly chosen by himself, whereas the corresponding public key is computed by the system authority (SA) without revealing the user's secret key. Girault's self-certified public key system has two features: (1) the user can use the own secret key to verify the public key distributed by SA, and (2) in digital signature applications, the processes of verifying a signature and verifying the authenticity of the signer's public key can be accomplished at a time.

By integrating the merits inherent in both the signature scheme giving message recovery proposed by Nyberg and Rueppel [8-9] and the RSA-based self-certified public key system designated by Girault [12], we will propose a new multisignature scheme giving message recovery. In the proposed scheme, any set of users can dynamically form a group and sign a message giving message recovery without or with signer-anonymity. The proposed scheme provides the feature that the processes of verifying a multisignature, recovering the message from the multisignature, and verifying the authenticity of the signers' public keys (without signer-anonymity) or the group's public key (with signer-anonymity) can be accomplished at a time. We also show that the proposed scheme can withstand the active attacks.

2. The Proposed Scheme

The proposed scheme works in a computer network system that consists of an SA and several users. SA takes the responsibilities for defining system's parameters and accepting user/group registration. Any registered user possesses a secret key randomly chosen by himself and a self-certified public key generated by SA. Any user's public key is regarded as the signature of the own secret key. Our system model also needs a clerk (CLK) whose tasks are to verify the personal signatures generated by all participant signers and to construct a multisignature from verified personal signatures. Any signer or the first signer who is trusted by all participant co-signers may also act as CLK. We describe the proposed scheme by the following four phases: system initialization, user registration, multisignature generation and message recovery.

2.1 System Initialization

As in Girault's scheme [12], SA first selects two large primes p and q, where $p \geq 2^{350}$ and $q \geq 2^{350}$, and computes $N = p \cdot q$. Afterwards, SA chooses a generator α with maximal order in the multiplicative group $(Z/_N Z)^*$, and generates a pair of RSA keys (e, d) such GCD(e, $\varphi(N)$) = 1 and $e \cdot d = 1(\bmod\, \varphi(N))$, where φ is Euler's totient function. Additionally, SA also chooses an available one-way hash function h, which accepts a variable-length input and produces a fixed-length (e.g., 128 bits or 160 bits as suggested in literature [15]) output. After that, SA makes N, e, α and h public, while keeping d secret.

2.2 User Registration

When a user U_i with a distinct identity ID_i registers with the system, he first randomly chooses a 150-bit integer x_i as the own secret key and sends $\{ID_i$, $v_i = \alpha^{-x_i} \bmod N\}$ to SA. Notice that v_i is computed by using the Extended Euclidean algorithm [15], since $\varphi(N)$ is unknown. Then, SA computes U_i's public key $y_i = (v_i - ID_i)^d \bmod N$, and distributes it to U_i. Subsequently, U_i can verify y_i by checking that

$$y_i{}^e + ID_i \doteq v_i = \alpha^{-x_i} (\bmod N) \qquad (1)$$

2.3 Multisignature Generation

Let $G = \{U_1, U_2, ..., U_n\}$ be the dynamically-formed group of users that want to sign a message M, where the bit-length of $M \| h(M)$ is less than that of N. If the signing policy is with signer-anonymity, all users in G should first determine a distinct group identity GID and then each U_i sends $\{GID$, $v_i = \alpha^{-x_i} \bmod N\}$ to SA for generating G's public key $Y = ((\prod_{U_i \in G} v_i) - GID)^d \bmod N$. Subsequently, all users in G can individually verify Y by checking that

$$Y^e + GID = \prod_{U_i \in G} v_i = \prod_{U_i \in G} (y_i{}^e + ID_i)(\bmod N) \qquad (2)$$

After that, all users in G cooperatively sign the message M as follows:

(i) Each $U_i \in G$ randomly chooses an integer $w_i \in Z_N$ and broadcasts $\{r_i = \alpha^{-w_i} \bmod N\}$ to CLK and all other co-signers. Afterwards, CLK and each participant signer computes $R = (M \| h(M)) \cdot \prod_{U_j \in G} r_j \bmod N$.

(ii) Each $U_i \in G$ broadcasts $\{r_i$,

$s_i = w_i + x_i \cdot h(R)$ } to CLK and all other co-signers. Here, $(r_i,\ s_i)$ is regarded as the personal signature of M signed by U_i.

(iii) CLK (or any participant signer in G) verifies each $(r_i,\ s_i)$ by checking that

$$r_i \cdot \alpha^{s_i} \cdot (y_i{}^e + ID_i)^{h(R)} = 1(\text{mod}\ N)\,.\quad(3)$$

If eqn. 3 is not satisfied, then terminate the procedure.

(iv) When all $(r_i,\ s_i)$'s have been successfully verified, CLK computes $S = \sum_{U_j \in G} s_j$ and transmits $\{(R, S), (ID_1,\ y_1), (ID_2,\ y_2), \ldots, (ID_n,\ y_n)\}$ to the verifier if the signing policy is without signer-anonymity, otherwise transmits $\{(R, S), (GID, Y)\}$ to the verifier. Here, (R, S) is the multisignature of M for G.

2.4 Message Recovery

According to the pre-determined signing policy, the verifier computes

$$M \| h(M) = \begin{cases} R \cdot \alpha^S \cdot (\prod\limits_{U_i \in G} (y_i{}^e + ID_i))^{h(R)} \bmod N \\ \qquad\qquad\qquad \text{(without signer - anonymity)} \\ R \cdot \alpha^S \cdot (Y^e + GID)^{h(R)} \bmod N \\ \qquad\qquad\qquad \text{(with signer - anonymity)} \end{cases} \quad (4)$$

and obtain M by eliminating $h(M)$. The recovered M can be further verified by checking that its hashed value is identical to $h(M)$ obtained by eqn. 4.

2.5 Correctness of the Scheme

The verification of the public keys, i.e., y_i and Y, and personal signature, i.e., $(r_i,\ s_i)$, can be easily derived from eqns. 1, 2 and 3, respectively. From eqns. 2 and 3, we have

$$\begin{aligned} &\prod_{U_i \in G} (r_i \cdot \alpha^{s_i} \cdot (y_i{}^e + ID_i)^{h(R)}) \\ &= \prod_{U_i \in G} r_i \cdot \alpha^{\sum\limits_{U_i \in G} s_i} \cdot \prod_{U_i \in G} (y_i{}^e + ID_i)^{h(R)} (\text{mod}\ N) \\ &= R \cdot (M \| h(M))^{-1} \cdot \alpha^S \cdot \prod_{U_i \in G} (y_i{}^e + ID_i)^{h(R)} (\text{mod}\ N) \\ &= 1(\text{mod}\ N) \end{aligned}$$

which implies eqn. 4. Thus, the verifier can successfully recover the message from the received multisignature in the message recovery phase by following the pre-determined signing policy.

3. Security Analysis

It is to see that the security of SA's secret key d, any user U_i's secret key x_i, and any dynamically-formed group G's secret key X is based on the factorization problem as in RSA scheme [3]. In the following, we discuss some potential forgery attacks (including forging a personal signature and a group signature) and the active attacks against the proposed scheme.

Forgery attack 1: The adversary tries to forge a valid personal signature for U_i without knowing U_i's secret key x_i.

Analysis: Once R is determined (which implies that the adversary should determine r_i in advance), the adversary should compute s_i satisfying eqn. 3. However, as discussed in [12], the adversary will face the difficulty of computing discrete logarithm modulo N to solve s_i from eqn. 3 without knowing x_i and $\varphi(N)$.

Forgery attack 2: The adversary tries to forge a valid multisignature (R, S) for a chosen message M without knowing all participant signers' secret keys or the group's secret key.

Analysis: If M is first fixed, then finding a multisignature (R, S) satisfying eqn. 4 is based on the difficulty of computing discrete logarithm modulo N. On the other side, If a multisignature (R, S) is first fixed, then the adversary can easily compute the result $M \| h(M)$ from eqn. 4. However, based on the non-inverse property of one-way hash function h, it is infeasible to determine such M.

Active attack 1: The adversary tries to substitute U_i's public key y_i with a fake y_i'

for universally forging a valid personal signature on any given message.

Analysis: If the adversary can substitute the public key y_i with a fake y_i' that satisfying $\alpha^{x_i'} = y_i'^e + ID_i (\bmod N)$, where $x_i' \in Z_N$ is randomly chosen, then he can universally forge any valid personal signature on any given message by using x_i' as U_i's secret key. However, the adversary cannot compute such y_i' unless he knows *d*, which is protected by the RSA assumption. On the other side, the adversary might first fix y_i' and then compute the corresponding secret key x_i' satisfying $\alpha^{x_i'} = y_i'^e + ID_i (\bmod N)$. Again, finding such x_i' is based on the difficulty of computing discrete logarithm modulo *N*.

Active attack 2: The adversary tries to substitute *G*'s public key *Y* with a fake Y' for universally forging a valid multisignature on any given message.

Analysis: If the adversary can compute a pair $(X', \quad Y' \neq Y)$ satisfying $\alpha^{X'} = Y'^e + GID (\bmod N)$, then he can universally forge a multisignature on any given message by using X' as *G*'s secret key. Similar to Active attack 1, first fixing X' then computing Y' is based on the RSA assumption, and first fixing Y' then computing X' is based on the difficulty of computing discrete logarithm modulo *N*.

4. Conclusions

We have presented a multisignature scheme with message recovery using RSA-based self-certified public key system. In the proposed scheme, any set of users can dynamically form a group to sign a message without/with signer-anonymity. The main feature of the proposed scheme is that the processes of verifying a multisignature, recovering the message from the multisignature, and verifying the authenticity of the public key(s) can be accomplished at a time. The proposed scheme requires smaller communication bandwidth as compared to previously developed multisignature schemes without using self-certified public keys. Moreover, the proposed scheme can withstand the active attacks.

5. References

[1] T. ELGAMAL, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, **IT-31**, (4), pp. 469-472, 1985.

[2] L. HARN, "New digital signature scheme based on discrete logarithm," *Electronics Letters*, **30**, (5), pp. 396-398, 1994.

[3] R.L. RIVEST, A. SHAMIR and L. ADLEMAN, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, **21**, (2), pp. 120-126, 1978.

[4] A. SHAMIR, "Identity-based cryptosystems and signature schemes," *Advances in Cryptology-CRYPTO'84*, (Springer-Verlag), pp. 47-53, 1985.

[5] P. HOSTER, M. MICHELS and H. PETERSON, "Authenticated encryption schemes with low communication costs," *Electronics Letters*, **30**, (15), pp. 147-157, 1994.

[6] P. HOSTER, M. MICHELS and H. PETERSON, "Meta-message recovery and meta-blind signature schemes based on the discrete logarithm problem and their applications," *Advances in Cryptology-ASIACRYPTO'94*, (Springer-Verlag), pp. 224-237. , 1995

[7] W.B LIN and C.C. CHANG, "Authenticated encryption scheme without using a one-way function," *Electronics Letters*, **31**, (19), pp. 147, 1995.

[8] K. NYBERG and R.A. RUEPPEL, "A new signature scheme based on the DSA giving message recovery," *1st ACM Conference on Computer and Communications Security*, Fairfax, Virginia, 1993.

[9] K. NYBERG and R.A. RUEPPEL,

"Message recovery for signature scheme based on the discrete logarithm problem," *Designs, Codes and Cryptography*, 7, (1/2), pp. 61-81, 1996.

[10] R.G.E. PINCH, "Comment: new signature with message recovery," *Electronics Letters*, **30**, (11), pp. 852, 1994.

[11] J.M. PIVETEAU, "New signature with message recovery," *Electronics Letters*, 29, (25), pp. 2185, 1993.

[12] M. GIRAULT, "Self-certified public keys," *Advances in Cryptology-EUROCRYPT'91*, (Springer-Verlag), pp. 491-497, 1991.

[13] M. MICHELS and P. HORSTER, "On the risk of disruption in several multiparty signature schemes," *Advances in Cryptology-ASIACRYPT'96*, (Springer-Verlag), pp. 334-345, 1996.

[14] W. DIFFIE and M.HELLMAN, "New directions in cryptography," *IEEE Transactions on Information Theory*, **IT-22**, (6), pp. 644-654, 1976.

[15] D.R. STINSON, *Gryptography: Theory and Practice*, CRC Press, Inc. 1995.