On the Security of Huang-Chang Multi-signature Schemes

Jianhong Zhang[1,2] and Wei Zou[2]
(Corresponding author: Jianhong Zhang)

College of Science, North China University of Technology, Shijingshan District[1]
Beijing 100041, P. R. China. (Email: jhzhang@ncut.edu.cn)
Institute of Computer & Technology, Peking University, Haidian District[2]
Beijing 100871, P. R. China. (Email: ww@ncut.edu.cn)

(Received Nov. 04, 2005; revised and accepted Dec. 10, 2005 & Jan. 27, 2006)

Abstract

Recently, based on RSA and discrete logarithm with composite modulus, Huang and Chang proposed two multisignature schemes with distinguished signing authority and claimed that their scheme can resist forgery attack. Unfortunately, in this works, we show that their schemes have forgery attack by security analysis of Huang-Chang multi-signature schemes. Given a multisignature of certain a document, arbitrary one can forge a multisignature. To overcome the weakness of the schemes, we proposed an improved scheme.

Keywords: Attack, forgery attack, multisignature, security analysis

1 Introduction

A digital signature scheme is a method which allows one party, the signer, to sign messages (documents) in such a way that everyone can verify the validity of authentic signatures, but no one can forge signatures of other messages. The secret key is held by the signer and can't be known by anyone in any way. However, in some group-oriented applications, the message might demand all the group members to generate a signature together [1, 2, 3, 5, 10]. Conventionally, in these schemes, all group members sign the messages; we call these schemes as multisignature scheme.

A multisignature scheme is a signature scheme, in which plural signers jointly generate a signature for an identical message or several messages. The multisignature schemes are divided into two classes according to distinguishable signing authority: one is the multisignature with undistinguished signing authorities, note that all group members hold the same responsibility for signing the signature; the other is the multi-signature with distinguished signing authorities, note that each group member is responsible for a partial group message. There exist much less multi-signature schemes up to now.

Recently, Huang and Chang [4] propose two multisignature schemes with distinguished signing authority based on RSA [8] and the discrete logarithm with composite modulus [6]. One scheme is suitable for sequential architecture and the other is for the broadcasting one. They claim that two multi-signature schemes can resist the forgery attack. Unfortunately, we show that two schemes exist the forging attack by security analysis and give the corresponding attack way. To overcome the flaws of Huang-Chang multisignature schemes, we give an improved scheme and show that the scheme is secure in random oracle model. For the convenience of the following description, we briefly claim the proposed schemes by H.F.Huang and C.C.Chang as Huang-Chang scheme.

The organization of this paper is shown as follows. In Section 2, we review Huang-Chang multisignature schemes. In Section 3, we give security analysis to Chang et al scheme. Our improved digital signature scheme is presented in Section 4. Finally, we draw some conclusions.

2 Reviews of Huang-Chang Scheme

In this section, we only brief describe the broadcasting multisignature scheme. The idea of the sequential multisignature is similar to one of the broadcasting multisignature. The scheme consists of three phases: the initialization phase, the multi-signature generation phase and multisignature verification phase. With loss of the generality, supposed that the group $G = \{U_1, U_2, \ldots, U_n\}$ and the message m_1 be the partial message that U_i is responsible for. The whole processes of the scheme are as follows.

The Initialization Phase:
The Setup of the system parameters is produced by the

following steps:

1) The system authority chooses two safe large primes p, q, which satisfy $p = 2p_1 + 1$ and $q = 2q_1 + 1$, where p_1 and $q1$ are also prime numbers. Let $N = p \cdot q$ and $\phi(N) = 4p_1 \cdot q_1$ where $\phi(N)$ is called Euler's function.

2) select an integer g with the order p_1q_1 in $GF(N)$. Note that $g^{p_1q_1} = 1 \bmod N$.

3) For each group member U_i, the system authority computes a secret key $s_i = g^{d_i^{-1}} \bmod N$ for $i = 1, 2, L, n$, where $d_i < min(p_1, q_1)$ is the identity of U_i and $d_i \cdot d_i^{-1} = 1 \bmod p_1q_1$, then secretly send the secret key s_i to the group member U_i(the signer U_i) by a secure channel.

4) The system authority randomly chooses an integer $v \in Z_{\phi(N)}$ as a fixed parameter and which satisfies $v < d_i$ for $i = 1, 2, L, n$.

5) Finally, the system keep p_1, q_1, p and q secret and publish N, g, v and a secure collision-resistant hash function $h(\cdot)$.

The Multisignature Generation Phase:
Assumed that $m = \{m_1, m_2, L, m_n\}$ is the document in which the partial message m_i is signed by Ui for $i = 1, 2, L, n$. Each signer U_i signs the partial message m_i by the following steps:

1) Each signer U_i randomly selects a number k_i and computes a partial signature $t = \prod_{i=1}^{n} d_i$, $r_i = s_i^{h(m_i)} g^{k_i v} \bmod N$ and $y_i = g^{k_i t} \bmod N$ for the partial message m_i. Then U_i broadcast $\{r_i, y_i, m_i\}$ to collector (or all other signers).

2) the collector (or all other signers) verifies the valid partial signature (r_i, y_i) of m_i by checking the following equality:

$$r_i^t = (s_i^{h(m_i)} g^{k_i v}) = g^{t_i h(m_i)} y_i^v \bmod N,$$

when $t_i = \prod_{j=1, j\neq 1}^{n} d_i = \frac{t}{d_i}$ and d_i is the identity of the signer U_i.

3) if the above checking holds for $i = 1, 2, L, n$, then the multisignature for the document $m = \{m_1, m_2, L, m_n\}$ IS (r, y) where $r = \prod_{i=1}^{n} \bmod N$ and $y = \prod_{i=1}^{n} y_i \bmod N$.

The Multi-Signature Verification Phase:
When a verifier obtains the multi-signature (r, y) of the document $m = \{m_1, m_2, L, m_n\}$, he carries out the following checking steps:

1) compute $t = \prod_{i=1}^{n} d_i$ and $t_i = \prod_{j=1, j\neq 1}^{n} d_i = \frac{t}{d_i}$ for $i = 1, 2, L, n$.

2) compute $R = \sum_{i=1}^{n} t_i h(m_i)$.

3) check $r^t = g^R y^v \bmod N$.

If Step 3 holds, the verifier concludes that (r, y) is the multi-signature of the document $m = \{m_1, m_2, L, m_n\}$.

3 Security Analysis of the Huang-Chang Scheme

In this section, we give an analysis to Huang-Chang multi-signature schemes and show that their schemes exist forgery attack. In the following, we only consider the attack on the broadcasting multi-signature scheme; similarly, the way also mount to the sequential multisignature scheme.

According to the above the multi-signature generation phase of the signer U_i, we know that a signature of the partial message m_i is (r_i, y_i) and satisfies $r_i = s_i^{h(m_i)} g^{k_i v} \bmod N$ and $y_i = g^{k_i t} \bmod N$. Thus an adversary can forge as follows:

1) randomly choose a number $\alpha \in Z_n$.

2) compute $r_i' = r_i \cdot g^{\alpha v} \bmod N$.

3) then (r_i', y_i') is also the partial signature of message m_i.

Because

$$\begin{aligned} (r_i')^t &= (r_i \cdot g^{\alpha v})^t = r_i^t \cdot g^{\alpha v t} = g^{t_i h(m_i)} y_i^v g^{\alpha v t} \\ &= g^{t_i h(m_i)} (y_i g^{\alpha t})^v = g^{t_i h(m_i)} (y_i')^v. \end{aligned}$$

Then given a multisignature (r, y) of a document m, we can forge a multisignature (r', y') by randomly choosing a number $\beta \in_R Z_N$ to compute $r' = r \cdot g^{\alpha v} \bmod N$ and $y' = y \cdot g^{\beta t} \bmod N$.

The attack way can also mount to the sequential multisignature scheme of Huang-Chang schemes.

4 An Improved Scheme

In this section, we propose an improved multisignature scheme. The system parameters are similar to one of Huang-Chang multisignature in our proposed scheme. The differences are only multisignature generation and verification. The describe procedures are as follows.

The Multisignature Generation Phase:
Assumed that $m = \{m_1, m_2, L, m_n\}$ is the document in which the partial message m_i is signed by U_i for $i = 1, 2, L, n$. Each signer U_i signs the partial message m_i by the following steps:

1) Each signer U_i randomly selects a number k_i and computes a partial signature $t = \prod_{i=1}^{n} d_i$, $y_i = g^{k_i t} \bmod N$ and $r_i = s_i^{h(m_i \| y_i)} g^{k_i v} \bmod N$ for the partial message m_i. Then U_i broadcasts $\{r_i, y_i, m_i\}$ to collector (or all other signers).

2) the collector (or all other signers) verifies the valid partial signature (r_i, y_i) of m_i by checking the following equality:

$$r_i^t = (s_i^{h(m_i \| y_i)} g^{k_i v})^t = g^{t_i h(m_i \| y_i) y_i^v \bmod N}.$$

What $t_i = \prod_{j=1,j\neq i}^{n} d_i = \frac{t}{d_i}$ and d_i is the identity of the signer U_i.

3) if the above checking holds for $i = 1, 2, L, n$, then the multisignature for the document $m = \{m_1, m_2, L, m_n\}$ is (r, y_1, y_2, L, y_n) where $r = \prod_{i=1}^{n} r_i \bmod N$.

The Multi-Signature Verification Phase:
When a verifier obtains the multi-signature (r, y_1, y_2, L, y_n) of the document $m = \{m_1, m_2, L, m_n\}$, he verifies as follows:

1) compute $t = \prod_{i=1}^{n} d_i$ and $t_i = \prod_{j=1,j\neq i}^{n} d_i = \frac{t}{d_i}$ for $i = 1, 2, L, n$.

2) compute $R = \sum_{i=1}^{n} t_i h(m_i \parallel y_i), y = \prod_{i=1}^{n} y_i$.

3) check $r^t = g^R y^v \bmod N$.

If all checking equation hold, it mean that this multisignature is valid. Such way can also extend to the sequential multisignature scheme. Here we don't describe it for limited space.

To overcome our attack, we revise $r_i = s_i^{h(m_i)}\ g^{k_i v} \bmod N$ into $r_i = s_i^{h(m_i \| y_i) g^{k_i v}} \bmod N$ in our proposed scheme, so that the adversaries can change y_i. The improved scheme efficiently resists our forgery attack above. In the following, we will show that the improved scheme is secure in random oracle model and the security of the scheme is relative to the difficulty of solving the RSA problem. From the above scheme, we know that the collector's function checks the validation of individual signature (partial signature) and he doesn't participate in the generation of multisignature. In each individual signature, the signature algorithm is similar each other. Then if the individual signature scheme is secure, it denotes that our multisignature scheme is secure.

Theorem 1. *There exists an adversary A for an adaptively chosen message attack to our individual signature scheme with running time t in non- negligible probability* $\varepsilon \geq 10(q_s+1)(q_h+1)/n$, *then the private key* $s_i = g^{d_i^{-1}}$ *can be solved within expected time* t', *where* q_h, q_s *denote the maximum number of queries to random oracle* $h(\cdot)$ *and Sign oracle asked by A, respectively. It is in contradiction to the RSA problem.*

Proof. Let us recall the private key generation of the group member U_i, the system authority first chooses two safe large primes p, q, which satisfy $p = 2p_1 + 1$ and $q = 2q_1 + 1$. And computes secret key $s_i = g^{d_i^{-1}} \bmod N$, where $d_i < \min(p_1, q_1)$ is the identify of U_i. If an adversary can solve his private s_i of group member U_i, then it will be contradiction to the RSA problem.

To show the proof, we assume there is polynomial algorithm A that can generate a valid individual signature for a message m without the private key s_i of member U_i. The algorithm A accepts the identity d_i of member U_i, the system parameters N, v, g and a message m, and it outputs a valid individual signature (r_i, y_i) of m, where

$$Pr[verification(m, (r_i, y_i), d_i) = accept] = 1.$$

By forking lemma [7], we can obtain two signatures on the same message m, then we can obtain the private key s_i of member U_i by the above two signatures. In the following, we will show that there exists an algorithm $\tilde{A}$, which use this algorithm A as subroutine, to solve the private key s_i of member U_i. More concretely, the algorithm is described as follows. Firstly, the algorithm $\tilde{A}$ selects two random numbers $a, a' \in Z_{|h(\cdot)|}$, which satisfies $a - a' = 1$. Then, $\tilde{A}$ will control A as follows.

First Round:
h-Hash Query: when A requests the value of $h(m \parallel y_i)$, for the targeted parameters, $\tilde{A}$ responds with a. Otherwise, responds with the list that he has generated.

- Signature Query: when A requests the signature of message m_i, $\tilde{A}$ checks whether the hash value of $(m_i, *)$ is responded, if the hash value has been responded, he rejects it; otherwise, he responds as follows:

  1) Firstly he computes $t = d_1 \cdot d_2 L d_n$ and $t_i = \prod_{j=1,j\neq i}^{n} d_i$,
  2) then randomly choose a number k_i and compute $y_i = g^{k_i t} \bmod N$.
  3) Set the hash value of (m_i, y_i) as $h(m_i \parallel y_i) = d_i \beta_i = h_i$ where β_i is a random number.
  4) Set $r_i = g^{\beta_i + v k_i}$ and return individual signature (r_i, y_i, h_i).

- Output: Eventually, the output of the first round is (r^*, y^*, h^*) of the message m.

Second Round:
h-Hash Query: when A requests the value of $h(m \parallel y_i)$, for the targeted parameters, $\tilde{A}$ responds with a'. Otherwise, responds with the list that he has generated.

- Signature Query: the signature query is the same as ones of first round in this round.

- Output: Eventually, the output of the first round is (r'^*, y^*, h'^*) of the message m.

It is obvious that the two signatures (r'^*, y^*, h'^*) and (r^*, y^*, h^*) satisfy

$$\begin{aligned} r^*)^t &= g^{t_i h^*} (y^*)^v \bmod N \quad \text{and} \\ (r'^*)^t &= g^{t_i h'^*} (y^*)^v \bmod N. \end{aligned}$$

Thus, we obtain

$$\begin{aligned}(\frac{r^*}{r'^*})^t &= \frac{g^{t_i h^*}}{g^{t_i h'^*}} \bmod N \\ &= g^{t_i(h^*-h'^*)} \bmod N \\ &= g^{t_i(a-a')} \bmod N \\ &= g^{t_i} \bmod N \\ &= (s_i)^t \bmod N.\end{aligned}$$

It denotes that the private key of member U_i is $s_i = r^*(r'^*)^{-1}$. In other words, it means that the algorithm $\tilde{A}$ can solve the private key of member U_i without the factoring of N. It is in contradiction to the RSA problem. □

5 Conclusion

Recently, Huang and Chang proposed two efficient multisignature schemes and claim that their schemes can resist forgery attack. However, in this works, we give a security analysis of Huang-Chang multi-signature schemes and show that their schemes have forgery attack. Arbitrary one can forge a multisignature provided that he knows a multisignature of certain a document. Finally, to overcome our attack, we propose an improved scheme.

Acknowledgements

The author would like to thank the anonymous referees for their valuable comments and suggestions that improve the presentation of this paper. And this work is supported by the Doctor Research starting and Scientific Research Common Program of Beijing Municipal Commission of Education (KM200610009011).

References

[1] T. Hardjono and Y. Zheng, "A practical digital multisignature scheme based on discrete logarithms", in *AUSCRYPT'92*, pp. 16-21, Berlin, Springer, 1992.

[2] L. Harn, "Group-oriented (t, n) threshold signature and multisignature", *IEE-Proceedings Computation Digital Techniques*, vol. 141, no. 5, pp. 307-313, 1994.

[3] L. Harn, "Digital multisignature with distinguished signing authorities", *Electronics Letters*, vol. 35, no. 4, pp. 294-295, 1999.

[4] H. F. Huang C. C. Chang, "Multisignature with distinguished signing authorities for sequential and broadcasting architectures", *Computer Standards & Interfaces*, vol. 27, pp. 169-176, 2005

[5] C. H. Lim and P. J. Lee, "Modified Maurer-Yacobi's scheme and its application", in *AUSCRYPT'92*, pp. 308-323, Berlin, Springer, 1992.

[6] M. McCurley, "A key distribution system equivalent to factoring", *Journal of Cryptology*, vol. 2, pp. 95-105, 1988.

[7] D. Pointcheval and J. Stern, "Security arguments for digital signatures and blind signatures", *Journal of Cryptography*, vol. 13, no. 3, pp. 361-396, 2000.

[8] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", *Communications of the ACM*, vol. 21, no. 2, pp. 120-126, 1978.

[9] A. Shamir, "Identity-based cryptosystems and signature schemes", in *CRYPTO'84*, pp. 47-53, Berlin, Springer, 1984.

[10] T. S. Wu and C. L. Hsu, "ID-based multisignatures with distinguished signing authorities for sequential and broadcasting architectures", *Applied Mathematics and Computation*, vol. 131, no. 2, pp. 349-356, 2002.

Jianhong Zhang received the M.Sc. and Ph. D degree in 2001 and 2004, respectively. Currently he is lecture in North China University of Technology. His area of interest is Public key cryptography based on elliptic curve and digital signature.

Wei Zou is currently a professor in Institute of Computer science & Technology of Peking University. His research interests include design and analysis of networking security protocol, mobile computing , secure electronic commerce, cryptography and network security.