I.J. Wireless and Microwave Technologies, **2011, 6, 65-72**
Published Online December 2011 in MECS (http://www.mecs-press.net)
DOI: 10.5815/ijwmt.2011.06.10

Available online at http://www.mecs-press.net/ijwmt

A Structured Multi-signature Scheme Against Forgery Attack

Wenjun Luo[a], Changying Li[b]

Department of Computer Science and Technology, Chongqing University of Posts and Telecommunications, Chongqing, China

Abstract

There are some classic structured multi-signature programs, such as Burmester's, Harn's and Lin's schemes that can not resist inside attack and outside attack. In this paper, we briefly review Burmester's program and relate safety analysis, Burmester's scheme vulnerable to forgery attack. Then we propose a structured multi-signature scheme against forgery attack. In the new scheme, we increase the signature parameter verification to improve security.

Index Terms: Structured multi-signature; ElGamal; forgery attack; Discrete logarithm problem

1. Introduction

Digital signature is one of the important problems of cryptography, it is a simulation of traditional handwritten signatures, and can realize sign electronic news. General digital signature scheme includes three processes: system initialization procedures, signature generating process and signature verification process. Signature algorithm is the cornerstone of digital signature system. Currently there are three kinds effective digital signature algorithm: (1) based on big integer factor decomposition problem; (2) based on discrete logarithm problem (DLP) of finite field, (3) based on elliptic curve discrete logarithm problem (ECDLP).

Digital signature is the important tool which realize network identity authentication, data integrity protection and non-repudiation service basics, also develop e-commerce and sign electronic contract. Using common digital signature, each signer has a respective key to generate signature and validate the signature, there are only a signer participation. let multiple users cooperate to sign one message, in many cases, it is important and necessary, the result that Generation of the multi-signature, the length of signature is irrelevant to the number of signature. In this special digital signature, each signer processes information by using their deposited secret respectively, then synthesis the results of treatment as the entire group signature; when the verifier of signature know the unique public keys of this group, and can validate that the signature is valid. In multi-signature

This material is based upon work supported by the National Natural Science Foundation under Grants NO.60963023 and Chongqing University Posts and Telecommunications Talent Introduction Foundation of China [2009].

* Corresponding author.
E-mail address: [a]luowj@cqupt.edu.cn; [b]changying1030@163.com

scheme, part of the signer's signature means the members sign some messages by using their own deposited secret, and all the signer's part signature is group multi-signature.

According to the different signature process, multi-signature [1] can be divided into orderly multi-signature and broadcasting multi-signature. Orderly multi-signature is a serial signature, it requires the signer according to certain order to sign message, each signer firstly validates the effectiveness of the signature what he received, if effective, it continues to signatures, then send to the next signer; if the signature is invalid, it declines to the signature and terminates the entire signature. And broadcast multi-signature is parallel, all signers can simultaneously sign message and send signature to signature collector, then signature collector collates all signature into a multi-signature. So-called structured multi-signature [2] means signature group has the predetermined signature structure, the structure is orderly or broadcast, also can both union.

Multi-signature was first pointed out in 1983 by Itakura.J K [3]. Burmester pointed out a structured based on ElGamal variant of the sequential multi-signature scheme [4], it makes that the signer can sign structured signature with serial and parallel combination. In 2000, Miyaji and Mitomi pointed out two multi-signature schemes, one was based on the DLP, another was based on RSA problem [5]. In 2003, Kawauehi and Tada pointed out improvement scheme on the basis of literature [5], and demonstrated its safety [6]. In 2004, L.Harn etc put forward respectively based on RSA and two ElGamal of multi-signature algorithm [7].

The rest of this paper is organized as follows: In section 2, I briefly review of Burmester's scheme. In section 3, the paper put forward a structured multi-signature scheme prevent forgery attack. In section 4 is safety analysis of the new scheme. Finally, I draw our conclusions in Section 5.

2. Briefly Review of Burmester's Scheme

2.1. System Initialization

Put U_1 to the sender, U_v for signature verification, U_i for message signer, supposed $(U_1, U_2, \cdots, U_n)$ are the signature order. Selecting big primes p, q is $p-1$ a large prime factor, let g be the primitive-root of the cyclic group $GF(p)$, h () is a one-way hash function. Each signer U_i $(i = 1,2,\cdots,n)$ randomly choose an integer as their private keys $x_i \in Z_q^*$. Then compute their public keys as follows: $y_1 = g^{x_1} \bmod p$, $y_i = (y_{i-1} g)^{x_i} \bmod p$. Opening system parameters (p, q, g, h), Signers open their public keys, and preserve their private key.

2.2. Signature Process

1). Signature Parameters R Generation

(1) Signer U_1 randomly selects an integer $k_1 \in Z_q^*$ and computes $r_1 = g^{k_1} \bmod p$, then broadcast r_1 to next signer.

(2) For $i \in (2,3,\cdots,n)$, U_i randomly selects an integer $k_i \in Z_q^*$ and computes his signature parameters $r_i = (r_{i-1})^{x_i} \cdot g^{k_i} \bmod p$, then broadcast to next signer.

(3) When the last signer U_n generates his signature Parameter r_n, they compute $R = r_n$.

2). Generation of signature

(1) The first signer U_1 computes $s_1 = x_1 + k_1 Rh(R, M) \bmod q$, and sends (s_1, M) to next signer.

(2) For $i \in (2,3,\cdots,n)$, the signer U_i verifies that $g^{s_{i-1}} \stackrel{?}{=} y_{i-1} \cdot Rh(R, M) \bmod p$, then computes $s_i = (s_{i-1} + 1)x_i + k_i Rh(R, M) \bmod q$ and sends (s_i, M) to next signer.

2.3. Signature Verification

When all the signers have finished signing the message M, the last signer U_n sends (s_n, M) to the signature verifier U_v, U_v verifies $g^{s_n} \stackrel{?}{=} y_n \cdot R^{Rh(R,M)} \bmod p$. If the equations establish, it is that the signature is valid, else judge invalid and reject the signature.

Literature [8] shows that Burmester's scheme is unsafe. If the attacker is the signature signer, he can forge some certain messages by forging his own public key, signature parameter and signature. If the attacker is not the signature signer, he can forge some certain messages by forge signature parameters.

3. A New Structured Multi-Signature Scheme

The new scheme adds a signature verifier to check the signers' signature parameters in signature process, which can resist forgery attack. When the signers finish generating their signature parameters, then they generate a parameter according to their signature parameters, after that they send the parameter to the signature verifier to check whether their signature parameters is valid. In this way, the improved scheme can resist forgery attack.

The new scheme is divided into three phases: system initialization, signature process and signature verification.

3.1. System Initialization

(1) The system choose a big prime p, q is $p-1$ a large prime factor, let g be the primitive-root of the cyclic group $GF(p)$, and adopting a safety one-way hash function $h()$.

(2) The signer $(U_1, U_2, \cdots, U_n)$ respectively choose $(x_1, x_2, \cdots, x_n) \in Z_q^*$ randomly as their private keys, and compute their public keys sequentially as follow: $y_1 = g^{x_1} \bmod p$, $y_i = y_{i-1} g^{x_i} \bmod p$.

(3) Signers open system parameters and their public keys, meanwhile, preserve their private keys.

3.2. Signature Process

1). Signature Parameters R Generation

The signature verifier U_v randomly chooses an integer $k_v \in Z_q^*$ and computes his signature parameters $r_v = g^{k_v} \bmod p$, then publish r_v to all the signers.

For $(i=1,2,\cdots,n-1)$, U_i randomly selects their own integer $k_i \in Z_q^*$, and computes their signature parameters sequentially as follows: $r_1 = g^{k_1} \bmod p$, $r_i = r_{i-1} \cdot g^{k_i} \bmod p$. Then broadcast to all of the users (signers and verifier). The last signer U_n computes the signature parameters $R = r_n$.

When the signer U_i completes generating his signature parameters r_i, then he computes $w_i = r_v^{k_i} \bmod p$ and sends w_i to the system verifier U_v to verify whether his signature parameters is forgery.

2). Signer's Signature Parameters Verification

In this process, the system verifier U_v verifies all of the signers' signature parameters are forgery or not. If someone's signature parameters is fake, then signature system is unsafe. Because the inside and outside attacker can forge an unauthorized message by forge his signature parameters. So, all signers' signature parameters through verifying, this scheme can resist forgery attack. The method as follow:

When system verifier U_v received the signer U_i's w_i, he verifys:

$$\begin{cases} w_i \stackrel{?}{=} (r_i \cdot r_{i-1}^{-1})^{k_v} \bmod p \\ r_i^{k_v} \bmod p \neq 1 \bmod p \end{cases}$$

If the one of two equations are not verify, it is means that the signer U_i's signature parameters is forgery, so the signer verifier must suspend the next signer U_{i+1} to generate his signature parameters and let U_i generate his signature parameters again until the signer U_i's signature parameters is valid. If all of the signers' signature parameters are valid, the process of signature parameters verification completed.

3). Generation of signature

If the signer is U_1, take the following step:

Firstly he computes the signature $s_1 = x_1 + k_1 Rh(R, M) \bmod q$, then sends (s_1, M) to the next signer.

If the signer is $U_i (i = 2,3,\cdots,n)$, take the following steps:

(1) Verifying $g^{s_{i-1}} \stackrel{?}{=} y_{i-1} r_{i-1}^{Rh(R,M)} \bmod p$, if the equations establish, it is means that the structured multi-signature is valid, or reject the signature and judge the signature invalid.

(2) Firstly he computes the signature $s_i = s_{i-1} + x_i + k_i Rh(R, M) \bmod q$, then sends (s_i, M) to the next signer.

3.3. Generation of signature

When all of the signers have finished signing the message M, the last signer sends (s_n, M) to system verifier U_v.

Firstly, U_v computes $R = r_n$, then verifies the equations that $g^{s_n} = y_n \cdot R^{Rh(R,M)} \bmod p$ establish or not. If the equations establish, it is means that the signature is valid, else judge the signature invalid, and terminate the signature.

4. Cryptanalysis of the new Structured Mgulti-signature Scheme

4.1. The New Scheme Correctness Testify

The method of compute public keys y_i as follow:

$$\begin{cases} y_1 = g^{x_1} \bmod p \\ y_i = y_{i-1} \cdot g^{x_i} \bmod p = g^{x_1+x_2+\cdots+x_i} \bmod p \end{cases}$$

The method of compute public keys y_i as follow:

$$\begin{cases} r_1 = g^{k_1} \bmod p \\ r_i = r_{i-1} \cdot g^{k_i} \bmod p = g^{k_1+k_2+\cdots+k_i} \bmod p \end{cases}$$

The value of s_{i-1} as follow:

$$\begin{cases} s_{i-1} = s_{i-2} + x_{i-1} + k_{i-1}Rh(R,M) \bmod q \\ s_{i-2} = s_{i-3} + x_{i-2} + k_{i-2}Rh(R,M) \bmod q \\ \vdots\vdots\vdots \\ s_2 = s_1 + x_2 + k_2 Rh(R,M) \bmod q \\ s_1 = x_1 + k_1 Rh(R,M) \bmod q \end{cases}$$

$$\begin{aligned} & s_{i-1} + s_{i-2} + \cdots + s_2 + s_1 = s_{i-2} + s_{i-3} + \cdots + s_2 \\ & + s_1 + (x_{i-1} + x_{i-2} + \cdots + x_2 + x_1) + Rh(R,M) \cdot \\ & (k_{i-1} + k_{i-2} + \cdots + k_2 + k_1) \bmod q \Rightarrow \sum_{j=1}^{i-1} s_j = \sum_{j=1}^{i-2} s_j \\ & + \sum_{j=1}^{i-1} x_j + Rh(R,M) \cdot \sum_{j=1}^{i-1} k_j \Rightarrow s_{i-1} = \sum_{j=1}^{i-1} x_j + R \cdot \\ & h(R,M) \cdot \sum_{j=1}^{i-1} k_j \end{aligned}$$

(1) Verify: $g^{s_{i-1}} \stackrel{?}{=} y_{i-1} r_{i-1}^{Rh(R,M)} \bmod p$:

$$g^{s_{i-1}} = g^{(x_i+x_2+\cdots+x_{i-1})+Rh(R,M)\cdot(k_1+k_2+\cdots+k_{i-1})} =$$

$$g^{(x_1+x_2+\cdots+x_{i-1})} \cdot (g^{(k_1+k_2+\cdots+k_{i-1})})^{Rh(R,M)} =$$
$$y_{i-1} \cdot r_{i-1}^{Rh(R,M)} \bmod p$$

If the signer before U_{i-1} sign the message with the supplied condition, the equation $g^{s_{i-1}} \stackrel{?}{=} y_{i-1} r_{i-1}^{Rh(R,M)} \bmod p$ will validate. If all the signers sign the message with the supplied condition, the equation $g^{s_n} = y_n \cdot R^{Rh(R,M)} \bmod p$ will validate.

(2) Verify:

$$\begin{cases} w_i \stackrel{?}{=} (r_i \cdot r_{i-1}^{-1})^{k_v} \bmod p \\ r_i^{k_v} \bmod p \neq 1 \bmod p \end{cases}$$

When Signature Process, the signer verifier verify signer's signature parameters by equation $w_i \stackrel{?}{=} (r_i \cdot r_{i-1}^{-1})^{k_v} \bmod p$. Signer's signature parameters verification as follow:

$$w_i = y_v^{k_i} = (g^{k_v})^{k_i} = (g^{k_i})^{k_v} = (g^{(k_i+k_{i-1}+\cdots+k_1)} /$$
$$g^{(k_{i-1}+k_{i-2}+\cdots+k_1)})^{k_v} \bmod p = (r_i / r_{i-1})^{k_v} \bmod p$$
$$= (r_i \cdot r_{i-1}^{-1})^{k_v} \bmod p$$

4.2. Resist Inside Forgery attack

If a dishonest signer U_f wanted to forge himself on news signature, let $y_f = y_t \cdot g^{x_f} \bmod p$, $r_f = r_t \cdot g^{k_f} \bmod p$, $s_f = s_t + x_f + k_f Rh(R,M) \bmod q$. Although, verified that $g^{s_{f-1}} = y_{f-1} r_{f-1}^{Rh(R,M)} \bmod p$, the equations establish, but it can not pass signature parameters validation. Because the signature parameters of all signers are not passing verifying the equations

$$\begin{cases} w_f = (r_f \cdot r_{f-1}^{-1})^{k_v} \bmod p \\ r_f^{k_v} \bmod p \neq 1 \bmod p \end{cases}$$

before signature verification. The method as follow:

(1) Signer U_f forges his signature parameters $r_f = r_t \cdot g^{k_f} \bmod p$.

(2) The attacker set $y_f = y_t \cdot g^{x_f} \bmod p$ and $s_f = s_t + x_f + k_f Rh(R, M) \bmod q$.

Verify： $w_f \neq \left(r_f \cdot r_{f-1}^{-1}\right) \bmod p$

$$\left(r_f \cdot r_{f-1}^{-1}\right)^{k_v} = \left(r_t g^{k_f} \cdot r_{f-1}^{-1}\right)^{k_v} \bmod p = \left(r_t \cdot r_{f-1}^{-1}\right)^{k_v} \cdot g^{k_f \cdot k_v} \bmod p$$
$$= \left(r_t \cdot r_{f-1}^{-1}\right) \cdot \left(g^{k_v}\right)^{k_f} \bmod p = \left(r_t \cdot r_{f-1}^{-1}\right) \cdot r_v^{k_f} \bmod p =$$
$$\left(r_t \cdot r_{f-1}^{-1}\right) \cdot w_f \bmod p \neq w_f$$

In this way, the dishonest signer can not forge some certain messages by forge signature parameters. So the new scheme can resist inside forgery attack.

4.3. Resist Outside Forgery attack

Literature [8] have achieved the external forgery attack on Burmester's scheme as follows: If outside forger want to forge some certain messages by forge signature parameters, let all the signers ally to forge $R = g^t$, the attacker satisfy h(R,M')= h(R,M)+a (a is an integer) and set $s_n^{'} = s_n + tRa \bmod q$. Although, verified that $g^{s_{i-1}} = y_{i-1} r_{i-1}^{Rh(R,M)} \bmod p$, the equations establish, but it can not pass signature parameters validation. The reason as with subsection 4.1, therefore, the attacker can not sign some illegal messages by that all the signers ally to forge $R = g^t$. In this way, the new scheme can resist outside forgery attack.

5. Conclusions

This paper briefly review that the classic structured multi-signature scheme such as Burmester's scheme is not secure. Then the paper points out a structured multi-signature scheme against forgery attack and shows that the new scheme can resist inside and outside forgery attack by verifying signature parameters. Based on security of the new scheme, we believe that the signature occasions need more than one signer to sign a message, it is effective and practical.

References

[1] Wanli Lü, Cheng Chung. The Analysis Of Digital Signature Scheme[J] in chinese. Journal of Guangxi Academy of Sciences, 2002,18(4):161-164.

[2] Lin CY, Wu TC, Zhang FG. A structured multi-signature scheme from the Gap Diffie-Hellman Group[R]. Cryptology ePrint Archive, 2003.

[3] Itakura K, Nakamura K.A public key cryptosystem suitable for digital multi-signature[J].NEC Res and Develop, 1983, 71(10): 1- 8.

[4] Burmester M, Desmedt Y, Doi H, et a1. A structured ElGamal type multisignature scheme [C]. In: Proceedings of PKC 2000, LNCS 1751.466 - 483.

[5] Mitomi S, Miyaji A. A muhisignature scheme with message flexibility, order flexibility and order verifiability[C]. In: Proceedings of ACISP 2000, LNCS 1841,298 – 312.
[6] Kawauchi K, Tada M. On the exact security of multi-signature schemes based on RSA [C]. Safavi-Naini R, Seberry J(Eds.), ACISP 2003, LNCS 2727, 336 – 349.
[7] Harn L, LN CY, WU TC. Structured multisignature algorithms[J]. IEE Proceedings Computers and Digital Techniques, 2004, 153(3):231-234.
[8] Jun Zhang. Cryptographic analysis of the two structured multi-signature schemes[J]. Journal of Computational Information Systems 2010, 6(9):3127 - 3135.