Security of Wang-Li Threshold Signature Scheme

Lifeng Guo

Institute of Systems Science, Academy of Mathematics and System Sciences,
Chinese Academy of Sciences, Beijing 100080, P.R. China
E-mail address: lfguo@amss.ac.cn

Abstract. In 2003, Wang et al.[1] proposed a (t, n) threshold signature scheme without a trusted party based on the discrete logarithm problem. In this paper, according to [5]'s attacking method, we show that there are still some security leaks in that scheme, and give some methods of forgery attack. Moreover, we point out this scheme is vulnerable to universal forgery by an insider attacker under reasonable assumptions.

Keywords threshold signature; secret sharing; trusted party

1 Introduction

In 1991, Desmedt and Frankel proposed a (t,n) threshold signature scheme based on RSA [2]. In [3], the author gives a threshold group signature scheme based on Discrete Logarithm. Harn showed a threshold group signature scheme based on ELGamal signature without a trusted party [4]. As under many specific applying environment, a trusted center which is trusted by all group members does not exist, the threshold group signature without a trusted center takes on attraction. In [1], the author uses secret sharing technique, all group members decide group public key and group members' secret key.

2 Review of Wang et al.'s Threshold Signature Schemes

Their scheme consists of three parts: group public key and secret shares generation phase, partial signature generation and verification phase, and group signature generation and verification phase.

Part 1: Group Public Key and Secret Shares Generation Phase

Let $A(|A| = n)$ be the set of all shareholders, B be any subset in A of size t $(|B| = t)$. The public parameters, (H, p, q, α), should be agreed by all shareholders in advance.

- a collision free one-way hash function H.
- p= a large prime modulus, where $2^{511} < p < 2^{512}$.
- q= a prime divisor of p-1, where $2^{159} < p < 2^{160}$.
- a positive integer $\alpha = h^{p-1/q} \ \ mod \ \ p$, where $1 \le h \le p-1$, and g is a generator with order q in $GF(p)$.

Each shareholders $i, i \in A$, randomly selects a $(t-1)$-th degree polynomial, $f_i(x)$, and an integer x_i associated with each shareholder i, where $x_i \in [1, q-1]$. Then he computes $\lambda_{i,j} = f_i(x_j) modq$ for other $n-1$ members, and sends $\lambda_{i,j}$ to U_j by broadcast. We notice $\lambda_{i,i} = f_i(x_i) modq$ and U_i keeps $\lambda_{i,i}$.

After every members finished above procedure, group member U_i computes $\lambda_i = \sum_{j=1}^{t} \lambda_{j,i} \ \ mod \ \ q$.That is, $\lambda_i = \sum_{j=1}^{t} f_j(x_i) \ \ mod \ \ q$. Now we define a new fuction $f(x) = \sum_{i=1}^{t} f_i(x) \ \ mod \ \ q$. Although U_i doesn't know $F(x)$, he easily knows $\lambda_i = F(x_i)$. U_i chooses a randomly number k_i in $[1, p-1]$. $X_i = \lambda_i k_i mod q$ is a $U_i's$ secret key and $y_i = g^{x_i} modp$ is his public key. Let $r_i = g^{k_i} modp$ U_i sends r_i to other members by broadcast.

Every member computes $R = \prod_{i=1}^{n} r_i \ \ mod \ \ p$. Because threshold value is t, t members can obtain $F(0)$ by using Lagrange interpolating polynomials to compute $F(0) = (\sum_{i=1}^{t} F(x_i) \cdot \prod_{j=1, j\neq i}^{t} \frac{-x_j}{x_i - x_j}) \ \ mod \ \ q$. Then $y = g^{F(0)} \times R \ \ mod \ \ p$ is group's public key and the corresponding group secret key x is $F(0) + \sum_{i=1}^{n} k_i \ \ mod \ \ q$.

Part 2: Partial Signature Generation and Verification Phase

At first, members decide which members participate group signature by arranging. Group members of participating group signature forms the set S. suppose $S = \{U_i | i = 1, 2, \cdots, n\}$. Then every member U_i chooses a new random number t_i in $[1, q-1]$. U_i computes the following equation:$T_i = g^{t_i} \ \ mod \ \ p$ and $z_i = g^{t_i \times (k_i)^{-1}} mod \ \ p$where k_i is $U_i's$ random number in secret key generating phase. U_i sends T_i and z_i to other members of participating singatures through a broadcast channel.

After receiving T_i and z_i from other members, U_i chooses frontal t members in S and form the set S_t. U_i computes $r = \prod_{u_j \in S_t} z_j \ \ mod \ \ p$. According to the following equation U_i solve s_i:

$$k_i s_i = (k_i \lambda_i C_i) \times h(m) - r \times t_i mod \ \ q \tag{1}$$

The above equation is equivalence to:

$$s_i = (\lambda_i C_i) \times h(m) - r \times t_i \times (k_i)^{-1} mod \ \ q \tag{2}$$

Where $C_i = \prod_{j=1, j\neq i}^{t} \frac{-x_j}{x_i - x_j}$.

Then, the messages $(m, r_i, s_i, y_i, r, T_i, i)$ are transmitted to a DC(Designated Combiner) who is only responsible for collecting and evaluating information. Note that the DC here is different from a mutually trusted center since he does not select any parameter for users. Here, the individual signature s_i is a partial signature of the message m. On receiving the messages $(m, r_i, s_i, y_i, r, T_i, i)$, the DC uses public key y_i to check whether the following equation is true:

$$r_i^{s_i} (T_i)^r \equiv^? (y_i)^{h(m) c_i} mod \ \ p \tag{3}$$

If the equation holds, the partial signature s_i of the message m received from U_i has been verified.

Part 3: Group Signature Generation and Verification Phase

Once all these t partial signature are verified by the DC, the DC can generate the group signature for the message m as $\{m, s, r, R\}$, where

$$s = \sum_{U_i \in S_t} s_i,$$

That is, $s = \sum_{U_i \in S_t} (\lambda_i C_i) h(m) - r \sum_{U_i \in S_t} (t_i \times k_i^{-1}) \ \ mod \ \ q$.

To verify the validity of the group signature $\{m, r, s, R\}$, the verifier has to compute the following equation:

$$g^s r^r \equiv (y \times R^{-1})^{h(m)}. \tag{4}$$

3 An exterior Attack on Wang et al.'s threshold signature schemes [1]

Unfortunately, the signature scheme is insecure. Given a message m , anyone can forge a signature that will be verified, as follows:

(1). Choose two random values $a \in z_q^*$ and $d \in z_q^*$.

(2).Compute $r_i' = y_i^a \ \ mod \ \ p$ and $T_i' = r_i'^d \ \ mod \ \ p$.

(3). By verifying equation3have

$$y_i^{as_i'} \cdot y_i^{adr} \equiv y_i^{h(m)C_i} \ \ mod. \ \ p \tag{5}$$

Then we have

$$s_i' = a^{-1}h(m)C_i - dr \tag{6}$$

(4). (r_i', s_i', r, T_i') is a valid signature of message m.

Because we have

$$r_i'^{s_i'}(T_i')^r \equiv y_i^{as_i'} \cdot y_i^{adr}$$

$$\equiv y_i^{as_i'+adr} \equiv (y_i)^{h(m)c_i} mod \ \ p. \tag{7}$$

So (m, r_i', s_i', r, T_i') is a valid partial signature. That shows $U_i's$ partial signature can be forged by attackers.

We compute $S' = \sum\limits_{i=1}^{t} s_i' \ \ mod \ \ q$.

By

$$g^{s'} r^r \equiv (y \times R'^{-1})^{h(m)}. \tag{8}$$

We have

$$R' \equiv \left(g^{s'} r^r\right)^{h(m)} \cdot y \ \ mod \ \ p \tag{9}$$

(m, S', r, R') is a valid group signature.

Because

$$(y \times R'^{-1})^{h(m)} \equiv (y \times (g^{s'} r^r)^{h(m)^{-1}} \cdot y^{-1})^{h(m)}$$

We have

$$(y \times R'^{-1})^{h(m)} \equiv g^{s'} r^r \ \ mod \ \ p. \tag{10}$$

Remark. In [1], the author mistakes R a signature. In fact, from constructing we can find R is a public key. If this case, the attack of [1] increases difficulty. The following is the attack after correcting.

4 An interior Attack on Wang et al.'s threshold signature schemes [1]

First the possible attacker model are described. In the group environment we can distinguish between an insider, an outsider and a DC attack. The DC attack can be active (he does not follow the protocol) or passive(he just reveals some parameters). In the following, our attack assumes that one insider attackers and the passive DC collude, while the overwhelming majority of signers, more precisely all except the insider, can be assumed to be honest.

Assume that an insider attacker 1, say Charley, wants his victims $2, \cdots, t$ to sign a message m' with him. They reject, but agree to sign the innocent message m with him.

Therefore, signer (and victim) i (for all $i \in \{2, 3, \cdots, n\}$) chooses a random number $k_i \in Z_q^*$ and signer $i(2 \le i \le t)$ chooses a random number $t_i \in Z_q^*$. They compute $r_i = g^{k_i}$,$T_i = g^{t_i}$, $z_i = g^{t_i \times (k_i)^{-1}} mod \ \ p$. U_i sends r_i to other members through a broadcast channel. U_i sends T_i to other members of participating signatures through a broadcast channel. Charley waits until he received $r_2, r_3, \cdots, r_t$. He randomly chooses $k_1 \in Z_q^*$.He computes $r_1 = g^{k_1}$,$T_1 = g^{t_1}$, $z_1 = g^{t_1 \times (k_1)^{-1}} mod \ \ p$ and $r = \prod\limits_{u_j \in S_t} z_j \ \ mod \ \ p$.Then he computes $d = h(m') \cdot h(m)^{-1} \;\; mod \;\; p, r' = r^d \;\; mod \;\; p$ and $r'_1 = r' \prod_{j=2}^{t} r_j^{-1} \;\; mod \;\; p$. Charley sends r'_1 instead of r_1 to other signers. Now the signer U_i computes

$$r' = r'_1 \cdot \prod_{j=2}^{t} r_j \;\; mod \;\; p, \tag{11}$$

$$s'_i = (\lambda_i C_i) \times h(m) - r' \times t_i \times (k_i)^{-1} mod \;\; q. \tag{12}$$

Then he sends s'_i to DC.The DC, who colludes with Charley, reveals $s'_2, s'_3, \cdots, s'_t$. Charley computes

$$s'_1 = (\lambda_1 C_1) \times h(m) - r' \times t_1 \times (k_1)^{-1} mod \;\; q. \tag{13}$$

Now Charley can compute $s' = d \cdot \sum s'_i \;\; (mod \;\; q)$. Then (m', r', s') is a valid signature of message m'. As

$$r' \equiv r^d \equiv g^{d \cdot \sum_{i=1}^{t} t_i k_i^{-1}} \tag{14}$$

$$\begin{aligned} g^{s'} &\equiv g^{d \cdot \sum_{i=1}^{t} s'_i} \\ &\equiv g^{d \cdot (\sum_{i=1}^{t} \lambda_i C_i \times h(m) - r' \times t_i \times (k_i)^{-1})} \\ &\equiv g^{\sum_{i=1}^{t} \lambda_i C_i \times d \cdot h(m) - d \cdot r' \times t_i \times (k_i)^{-1}} \\ &\equiv \left(y \times R^{-1}\right)^{d \cdot h(m)} \cdot r^{-d \cdot r'} \\ &\equiv \left(y \times R^{-1}\right)^{h(m')} \cdot r'^{-r'} \end{aligned}$$

5 Conclusion

By forging attack, we show that is not secure. Moreover, we point out this scheme is vulnerable to universal forgery by an insider attacker under reasonable assumptions.

References

[1] Bin Wang, Jianhua Li. (t, n) threshold signature schemes without trusted center . Journal of Computers, 2003, 26(11) : 1581-1584

[2] Desmedt Y. Frankel Y. Shared generation of authenticators. In:Proceedings of Crypto'91, Santa Barbara, California, USA, 1991,457-469

[3] Wang C T, Lin C H, Chang C C. Threshold signautre schemes with traceable signers in group communications. Computer Communications,1998,21(8): 771-776

[4] Harn L. Group-oriented (t, n) threshold digital signature scheme and digital multisignature. IEE Proceedings of Computers and Digital and Technique, 1994,141(5): 307-313

[5] M. Michels, P.Horser, On the risk of disruption in several multiparty signauture scheme, in: Advances in Cryptology-ASIACRYPT'96, 1997, pp. 334-345