On a Threshold Group Signature Scheme and a Fair Blind Signature Scheme

Zhengjun Cao

Key Lab of Mathematics Mechanization, Academy of Mathematics and Systems Science,

Chinese Academy of Sciences, Beijing, P.R. China. 100080 zjcamss@hotmail.com

(Graduate School of Chinese Academy of Sciences)

Abstract In the paper, we analyze two signature schemes. The first is a (t_j, t, n) threshold group signature scheme proposed by Shi and Feng in [1]. The second is a fair blind signature scheme proposed by Feng in [2]. Our results show that both schemes are forgeable. Besides, we introduce a concept, i.e., suspended factor, to describe the common error in designing signature scheme, which means that some signature data lie at neither base position nor exponent position in verifying equation, instead lie at factor position solely .

Keywords threshold group signature scheme, fair blind signature scheme, universal forgeability, suspended factor.

1 Shi-Feng threshold group signature scheme

Group signatures, introduced by Chaum and Heyst[3], allow individual members to make signatures on behalf of the group. More formally, a secure group signature scheme must satisfy the following properties[4]: unforgeability, anonymity, unlinkability, exculpability, traceability, coalition-resistance. For more details, one can refer to [4].

In 2000, Shi and Feng proposed a **variant** group signature scheme, i.e., (t_j, t, n) threshold group signature scheme[1]. Here we omit the background and requirements of the model. We care naught for them, instead we care for its universal forgeability. We show the scheme is universally forgeable by a simple and direct attack.

1.1 Review of the threshold group signature scheme

The model consists of four entities: group manager (GM), signature compiler (DC), group members, verifier.

Setup

(1)

(a) GM picks a hash function $H(\cdot)$, p, q satisfying $2^{511} < p < 2^{512}$, $2^{159} < q < 2^{160}$ and $q|(p-1)$.

(b) Pick $h \in Z_p^*$, set $\alpha = h^{(p-1)/q}$ mod p, $(\alpha \neq 1)$. Hence, α is of order q.

(c) Choose $f_j(x) = a_{j0}+a_{j1}x+\cdots+a_{j,n_j-1}x^{n_j-1}$ mod q, satisfying $0 < a_{j,i} < q, j = 1, 2, \cdots, l, i \in [0, n_j - 1]$. Set $f_j^d(x) = f_j(x)$ mod x^d, where $d \in [1, n_j]$.

(d) Compute $Y = \prod_{j=1}^{l} \alpha^{f_j(0)}$ mod p.

(e) GM opens $\{H(x), p, q, \alpha, Y\}$, keeps h in secret, and sends $f_j(x)$ to DC.

(2)

Group member $U_i \in A_j$ chooses $c_i \in [1, q-1]$, computes $x_i = \alpha^{c_i}$ mod p, keeps c_i in secret, and sends $\{x_i, j\}$ to GM.

(3)

GM picks $l_i \in [1, q-1]$, computes

$$id_i = \alpha^{l_i x_i} \ mod \ p, \qquad y_i^d = \alpha^{f_j^d(id_i)} \ mod \ p$$

$$u_i^d = (l_i x_i + f_j^d(id_i)) \ mod \ q, \qquad F_j(x) = \prod_{i \in A_j} (x - id_i) \ mod \ q$$

GM keeps l_i in secret, sends $\{id_i, y_i^d, u_i^d\}$ to U_i, $F_j(x)$ to DC, and takes id_i as U_i's identity.

Sign

(1) Given a message m, if member U_i wants to sign it, then he picks $k_i \in [1, q-1]$, computes $r_i = \alpha^{k_i}$ mod p, sends the pre-signature $\{id_i, j, r_i\}$ to DC.

(2) DC checks $F_J(id_i) = 0$ mos q. If it holds, then DC collects pre-signatures of A_j, denoted by B_j, where B_j consists of T_j members, the number of pre-signatures denoted by T. DC checks $T_j \geq t_j, \ T \geq t$. If it holds, then computes:

$$R_j = \prod_{i \in B_j} r_i \ mod \ p, \quad E_j = H(m, R_j) \ mod \ q, \quad g_j(x) = \prod_{i \in B_j} (x - idi) \ mod \ q$$

(3) DC keeps R_j in secret, broadcasts $\{j, g_j(x), E_j\}$.

(4) Member U_i checks $g_j(id_i) = 0$ mod q. If it holds, then U_i computes:

$$d_j = \partial^0(g_j(x)), \quad G_{ji}(0) = (-(id_i g_j'(id_i))^{-1} g_j(0)) \ mod \ q, \quad s_i = (u_i^{d_j} G_{ji}(0) + k_i E_j) \ mod \ q$$

where $d_j = T_j$, $g_j^{'}(x)$ is the derivative of $g_j(x)$.

(4) U_i keeps $G_{ji}(0)$ in secret, sends his partial signature $\{id_i, s_i, y_i^{d_j}\}$ to DC.

(5) DC computes $G_{ji}(0)$, checks

$$\alpha^{s_i} = (id_i y_i^{d_j})^{G_{ji}(0)} r_i^{E_j} \ mod \ p$$

If it fails, DC rejects it.

(6) After DC collects partial signatures, he computes

$$S = \sum_{j=1}^{l} \sum_{i \in B_j} s_i \ modq, \quad ID = \prod_{j=1}^{l} \prod_{i \in B_j} id_i^{G_{ji}}(0) \ mod \ p, \quad g(x) = \prod_{j=1}^{l} g_j(x) \ mod \ q$$

sends the threshold group signature $\{S, ID, g(x), R_j, E_j | (j = 1, \cdots, l)\}$.

Verify

Verifier checks

$$\alpha^S = Y \times ID \times \prod_{j=1}^{l} R_j^{E_j} \quad mod\ p$$

Open

Given a valid threshold group signature $(m, \{S, ID, g(x), R_j, E_j|(j = 1, \cdots, l)\})$, GM only needs to find each id_i in the members' list for

$$g(id_i) = 0 \quad mod\ q$$

1.2 Analysis

The authors claim that the security of the signature scheme is based on DLP, but we find it is false. Here we present a simple and direct attack on it, only according to the verifying phase. As far as the possible faults in the whole description of algorithm (see [1]) and other possible attacks, we do care nought for them.

First, we observe that there are some redundant data $E_j|(j = 1, \cdots, l)$ among the signature data $\{S, ID, g(x), R_j, E_j|(j = 1, \cdots, l)\}$. In fact, the appropriate signature is of the form:

$$(m, \{S, ID, g(x), R_j|(j = 1, \cdots, l)\})$$

The appropriate verifying equation is of the form:

$$\alpha^S = Y \times ID \times \prod_{j=1}^{l} R_j^{H(m,R_j)} \quad mod\ p$$

Secondly, we introduce a simple and direct attack on it in the following.

Universal forgeability: Adversary only needs to randomly pick $\lambda_j \in Z_p^*$ $(j = 1, \cdots, l)$ and $\omega \in Z_q^*$, computes:

$$\begin{aligned} R_j &= \lambda_j \quad (j = 1, \cdots, l) \\ S &= \omega \\ ID &= \alpha^S (Y R_j^{H(m,R_j)})^{-1} \quad mod\ p \end{aligned}$$

where Y, α are public parameters of the group, m is a given message.

The correctness of the forged group signature is easy to check.

Now we introduce a concept **suspended factor** to describe the error which occurs in the verifying equation. For example, ID in above verifying equation does lie at neither base position nor exponent position. It lies at a factor position solely.

2 Feng fair blind signature scheme

Blind signature was introduced by Chaum in 1982. For more details of the model, one can refer to [5, 6, 7].

Feng proposed a fair blind signature scheme in [2]. The author's claim that the security of the scheme is equivalent to that of the scheme proposed by Camenisch et al.[6] is false. In the following, we first review the scheme. Then we point out some errors in the description. At last, we show that an attacker with the certificate authorized by the Trustable Center (TC) can directly forge blind signatures.

2.1 Review of Feng fair blind signature scheme

The scheme consists three entities: Signer, Requester and Trusted center (TC).

TC randomly picks large primes p, q such that $q|(p-1)$, an integer $\alpha \in Z_p^*$ of order q.

Signer randomly picks a secret key x, opens his public key $y = \alpha^x \ (mod\ p)$.

Register:

$$
\begin{array}{ccc}
\textbf{Requester} & & \textbf{TC} \\
 & & \frac{\text{pick} A_0 \in Z_q^*,\ \alpha_i \in Z_q^*}{(*)} \\
 & \text{(request)} \longrightarrow & \\
 & \longleftarrow (A_o, Sig_{TC}(A_0 \parallel 0)) & \alpha_i \neq \alpha_j, i \neq j \\
 & \longleftarrow (\alpha_i, Sig_T C(A_i \parallel i)) & A_i = A_0^{\alpha_i} \\
A_i = A_0^{\alpha_i} (1 \leq i \leq k) & \vdots & \\
 & \longleftarrow (\alpha_k, Sig_{TC}(A_k \parallel k)) & \text{record}(A_0, A_1, \cdots, A_k)
\end{array}
$$

Sign:

$$
\begin{array}{rcl}
\textbf{Requester} & & \textbf{Signer} \\
 & (A_0, Sig_{TC}(A_0 \parallel 0)) \longrightarrow & \text{check} Sig_{TC}(A_0 \parallel 0) \\
\alpha_i \in \{\alpha_1, \alpha_2, \cdots, \alpha_k\} & \longleftarrow \widetilde{z} & \widetilde{z} = A_0^x \\
Z = \widetilde{z}^{\alpha_i} & & \widetilde{k} \in_R z_q^* \\
a, b \in_R z_q^* & \longleftarrow (\widetilde{r}_1, \widetilde{r}_2) & \widetilde{r}_1 = \alpha^{\widetilde{k}}, \widetilde{r}_2 = A_0^{\widetilde{k}} \\
\widetilde{r} = \widetilde{r}_1 \widetilde{r}_2\ mod\ p & & \\
r_1 = \widetilde{r}_1^a \alpha^b\ mod\ p & & \\
r_2 = \widetilde{r}_2^{\alpha_i a} A_i^b\ mod\ p & & \\
r = r_1 r_2\ mod\ p & & \\
\widetilde{m} = a m r^{-1} \widetilde{r}\ mod\ q & \widetilde{m} \longrightarrow & \widetilde{s} = (x\widetilde{r} + \widetilde{k}\widetilde{m})\ mod\ q \\
\frac{s = (\widetilde{s} r \widetilde{r} + bm)\ mod\ q}{(**)} & \longleftarrow \widetilde{s} &
\end{array}
$$

The signature of message m is $(A_i, Sig_{TC}(A_i \parallel i), z, r, s)$.

Verify:

(a) Check $Sig_{TC}(A_i \parallel i)$,

(b) Check $(A_i\alpha)^s \stackrel{?}{=} (yz)^r r^m$. If it holds, accept the signature, otherwise reject it.

2.2 Analysis

An error in setup phase

The system parameter $A_0 \in Z_q^*$(see underlined part (*)) picked by TC is a fault. By the later verifying equation, we know that A_0 should be of same order with α, i.e., q.

Mend: TC chooses $A_0 \in Z_p^*$ such that A_0 is of order q.

Verifying equation does not hold

$$\begin{aligned}
\text{left} &= (A_i\alpha)^s = (A_i\alpha)^{\widetilde{s}r\widetilde{r}+bm} \\
&= (A_i\alpha)^{(x\widetilde{r}+\widetilde{k}\widetilde{m})r\widetilde{r}+bm} \\
&= (A_i\alpha)^{xr\widetilde{r}^2+\widetilde{k}am\widetilde{r}^2+bm} \quad (mod\ p)
\end{aligned}$$

$$\begin{aligned}
\text{right} &= (yz)^r r^m = (\alpha^x A_0^{\alpha_i x})^r (r_1 r_2)^m \\
&= (A_i\alpha)^{xr}(\widetilde{r_1}^a \alpha^b \cdot \widetilde{r_2}^{\alpha_i a} A_i^b)^m \\
&= (A_i\alpha)^{xr}((\widetilde{r_1}\widetilde{r_2}^{\alpha_i})(A_i\alpha)^b)^m \\
&= (A_i\alpha)^{xr+bm}(\widetilde{r_1}\widetilde{r_2}^{\alpha_i})^{am} \\
&= (A_i\alpha)^{xr+bm}(A_i\alpha)^{\widetilde{k}am} \\
&= (A_i\alpha)^{xr+bm+\widetilde{k}am} \quad (mod\ p) \\
&\neq \text{left}
\end{aligned}$$

Mend: Substitute

$$s = (\widetilde{s}r\widetilde{r}^{-1} + bm)\ mod\ q$$

for the underlined part(**).

Requester's attack

The author claimed the security of the scheme is equivalent to that of the scheme proposed by Carmenisch et al. in [6]. This is false. In a sense, two signature schemes have comparability of the form. But the new scheme has a more datum z which destroys the security of total protocol.

Given a message m, Requester U_i can forge blind signature after he obtains A_i from TC. He only needs to:

(a) pick $\omega_1, \omega_2 \in_R Z_q^*$,

(b) compute

$$z = y^{-1}(A_i\alpha)^{\omega_1}\ (mod\ p), \quad r = (A_i\alpha)^{\omega_2}\ (mod\ p), \quad s = \omega_1(A_i\alpha)^{\omega_2} + \omega_2 m\ (mod\ q)$$

The blind signature of message m is $(A_i, Sig_{TC}(A_i \parallel i), z, r, s)$.

Correctness:

Checking for $Sig_{TC}(A_i \parallel i)$ is obvious. We only need to check $(A_i\alpha)^s \stackrel{?}{=} (yz)^r r^m$. In fact,

$$(yz)^r r^m = [yy^{-1}(A_i\alpha)^{\omega_1}]^{(A_i\alpha)^{\omega_2}}[(A_i\alpha)^{\omega_2}]^m = (A_i\alpha)^{\omega_1(A_i\alpha)^{\omega_2}+\omega_2 m} = (A_i\alpha)^s \ (mod\ p)$$

3 Conclusion

In the paper, we analyze Shi-Feng threshold group signature scheme and Feng fair blind signature scheme. Our results show that both schemes are forgeable. Besides, we introduce a concept suspended factor to describe the common error in designing signature scheme, which means a signature datum lying at neither base position nor exponent position in verifying equation, instead at factor position solely. Incidently, as far as modifications of the two schemes, we care naught for them. We only care for that both two schemes are fragile.

References

[1] Shi Yi, Feng Dengguo. The Design and analysis of a new group of (t_j, t, n) threshold group signature scheme. ChinaCrypt'2000. PP.149-152.

[2] Feng Dengguo. Blind signature schemes based on DLP problem. Privacy of Communication (China) 1997 (1), pp. 31-34.

[3] D.Chaum, F.Heyst. Group Signatures. Proc. EUROCRYPT'91, 1992, pp.257-265.

[4] M. Bellare, D. Micciancio, B. Warinschi. Foundations of Group Signatures: Formal Definitions, Simplified Requirements, and a Construction Based on General Assumptions. EUROCRYPT 2003. LNCS 2656, pp.614-629, 2003.

[5] D. Chaum. Blind Signature for Untraceable Payments. In: Advances in cryptology, proc.crypto'82. New York, 1983. pp. 199-203.

[6] Carmenisch J L et al. Blind signatures based on the discrete logarithm problem. Rump session of Eurocrypt'94, Perugid: Italy, 1994.

[7] M. Stadler et al., Fair Blind Signatures. In: Advances in cryptology, proc. Eurocrypt'95. New York, 1995. pp. 209-219.