文章编号: 1000-5013(2008)02-0213-05

Cryptanalysis of Threshold Signature Scheme for Group Communication

HAN Jin-guang[1], KANG Bao-yuan[2], WANG Qing-ju[3]

(1. College of Sciences, Hohai University, Nanjing 210098, China;
2. College of Mathematics Science and Computing Technology, Central South University, Changsha 410075, China;
(3. Department of Mathematics, Shaoxing College of Artand Science, Shaoxing 312000, China)

Abstract: Recently, Chang proposed a (t, n) threshold signature with (k, l) threshold-shared verification to be used in agroup-oriented cryptosystem without a shared distribution center (SDC). In their scheme, any t participants can represent a group (signing group) to sign a message, and any k participants can represent another group (verifying group) to verify the signature. In this paper, we will argue that Chang's scheme is vulnerable to the impersonation attack, and violates the basic definition requirement of (t, n) threshold signature with (k, l) threshold-shared verification.

Keywords: cryptanalysis; impersonation attack; proxy signature; threshold cryptosystem
CLC Namber: TP 309 **Document Code:** A

In 1991, Desmedt and Frankel proposed the concept of (t, n) threshold signature scheme[1]. Since then, many threshold signature scheme are proposed[2-14]. In 2000, Wang brought up a new idea that the (t, n) threshold signature on behalf of the signing group should be able to be verified by (k, l) threshold-shared verification on behalf of the verifying group[2]. In 2002, however, Hsu pointed that any adversary can reveal the signing group's secret key from two valid threshold signature and then forge a threshold signature in Wang's scheme. And they proposed a improved scheme which can with stand the attack[3]. But Hus's improved scheme need a shared distribution center (SDC). Recently, Chang proposed a threshold signature scheme for group communications without a SDC[4]. In this paper, we will argue that Chang's scheme is vulnerable to the impersonation attack.

1 Review of Chang's Scheme

In this section, we will brieflyreview Chang's scheme. Chang's scheme is comprised of four phases. (1) Key generation phase. (2) Individual signature generation and verification. (3) Threshold signature generation and encrypting phase. (4) Decrypting and threshold signature verifying phase.

1.1 Key Generation Phase

In their scheme, they used the following notations: (1) G_s, $G_s = \{u_{s_1}, u_{s_2}, \cdots, u_{s_n}\}$ is defined as the signing group of signers; g_s, $g_s (|g_s| = t \leqslant n)$ is any subset of size t in G_s; G_v, $G_v = \{u_{v_1}, u_{v_2}, \cdots, u_{v_l}\}$ is defined a the verifying group of l verifers; $g_v (|g_v| = k \leqslant l)$ is any subset of size k in G_v; ID_{s_i}

收稿日期: 2007-06-26
作者简介: 韩金广(1979-),男,助教,硕士,主要从事密码学、数字签名和密钥协议的研究. E-mail: jghan22@yahoo.com.cn.
基金项目: 国家自然科学基金资助项目(10471152)

denotes the identity of u_{s_i}; ID_{v_j} denotes the identity of u_{v_j}; E_s/E_v two elliptic curves; p_s/p_v two odd-prime numbers; F_{p_s}/F_{p_v} finite field of p_s and p_v elements, respectively; α_s/α_v base points on E_s and E_v, respectively; q_s/q_v orders of α_s and α_v separately in E_s and E_v, which are odd primes.

Each u_{s_i} in G_s performs the following three steps.

(1) Randomly choose an integer d_{s_i}.

(2) Randomly choose a $(t-1)$th degree polynomial $f_{s_i}(x)$ over Z_{q_s} such that

$$f_{s_i}(x) = f_{s_i,0} + f_{s_i,1}x + \cdots + f_{s_i,t-1} \cdot x^{t-1},$$

where $f_{s_i,0}, f_{s_i,1}, \cdots, f_{s_i,t-1}$ are in Z_{q_s}, and $f_{s_i}(0) = f_{s_i,0} = d_{s_i}$. Then send $f_{s_i}(ID_{s_j})$ to $u_{s_j}(\forall j \neq i)$ in G_s over a secret channel and broadcast the check values $f_{s_i,l}\alpha_s (l = 1, 2, \cdots, t-1)$ to the other participants in G_s. After receiving $f_{s_i}(ID_{s_j})$ from u_{s_i}, each u_{s_j} verifies the validity of it by the following verification equation.

$$f_{s_i}(ID_{s_j})\alpha_s = \sum_{l=1}^{t-1} (ID_{s_j})^l (f_{s_i,l}\alpha_s). \tag{1}$$

(3) Compute his/her private key $k_{s_i} = \sum_{j=1}^{n} f_{s_j}(ID_{s_i})$.

(4) Compute G_s's public key $Q_s = \sum_{j=1}^{n} f_{s_j,0}\alpha_s$ and his/her public key $Q_{s_i} = k_{s_i}\alpha_s$.

Similarly, each u_{v_i} in G_v perform the above steps. The result of performing those steps is listed in the following, as

$$k_{v_i} = \sum_{j=1}^{l} f_{v_j}(ID_{v_i})$$

and $Q_{v_i} = k_{v_i}\alpha_v$ are separately u_{v_i}'s private key and public key; and $Q_v = \sum_{j=1}^{l} f_{v_j,0}\alpha_v$ is G_v's public key.

In summary, the system parameters are: (1) Public information of G_s and G_v: E_s/E_v, α_s/α_v, Q_s/Q_v, q_s/q_v; (2) Public information of u_{s_i} in G_s and u_{v_i} in G_v: Q_{s_i}/Q_{v_i}, ID_{s_i}/ID_{v_i}; (3) Secret information of u_{s_i} in G_s and u_{v_i} in G_v: k_{s_i}/k_{v_i}.

1.2 Individual Signature Generating and Verifying Phase

Assume that t participants $u_{s_1}, u_{s_2}, \cdots, u_{s_t}$ in g_s are to sign a message m. Each u_{s_i} performs the following four steps.

(1) Compute a value e_{s_i} as

$$e_{s_i} = k_{s_i}a_{s_i}. \tag{2}$$

where $a_{s_i} = \prod_{j \in G_s, j \neq i} (ID_{s_j}/(ID_{s_j} - ID_{s_i}))$.

(2) Randomly choose an integer ω_i, where $1 \leqslant \omega_i \leqslant q_s - 1$. Then, compute R_{s_i} as

$$R_{s_i} = \omega_i\alpha_s, \tag{3}$$

and broadcast it to the other participants in g_s.

(3) Compute a point (X, Y) as

$$(X, Y) = \sum_{i \in g_s} R_{s_i} = \sum_{i \in g_s} \omega_i\alpha_s. \tag{4}$$

(4) Compute the individual signature $\{r, s_i\}$ as

$$r = X - h(m) \bmod q_s, \qquad s_i = e_{s_i}r + \omega_i \bmod q_s. \tag{5}$$

To verify the correctness of the individual signature s_i, a participant may be randomly selected from G_s as a designated clerk. The clerk uses u_{s_i}'s public key Q_{s_i} and a base point α_s to verify the individual signature as

$$R_{s_i} = s_i\alpha_s - ra_{s_i}Q_{s_i}. \tag{6}$$

If equation (6) holds, the individual signature (r, s_i) on message m is valid.

1.3 Threshold Signature Generation and Encrypting Phase

In this phase, the clerk combines t valid individual signature $\{r, s_i\}$ into a threshold signature (r, s) and encrypts m by using the elliptic curve ElGamal cryptosystem as follow.

(1) Compute the signature s as

$$s = \sum_{i \in g_s} s_i \bmod q_s, \tag{7}$$

$\{r, s\}$ is a group signature on message m.

(2) Express m as the x-coordinate of a point P_m on E_v. Then, choose a random integer ω_i, where $1 \leqslant \omega_i \leqslant q_v - 1$.

(3) Compute B and the ciphertext C as

$$B = \omega_i \alpha_v \bmod q_v, \qquad C = P_m + \omega_i Q_v \bmod q_v. \tag{8}$$

(4) Transfer (r, s) and (B, C) to the verifying group G_v.

1.4 Decrypting and Threshold Signature Verifying Phase

Assume that each k participants $u_{v_1}, u_{v_2}, \cdots, u_{v_k}$ in g_v wants to use his/her own private key k_{v_i} to collaborate recover the message and authenticate the signature by performing the following three steps.

(1) Compute a value e_{v_i} as

$$e_{v_i} = B k_{v_i} a_{v_i}, \tag{9}$$

where $a_{v_i} = \prod_{j \in G_v, j \neq i} (\mathrm{ID}_{v_j} / (\mathrm{ID}_{v_j} - \mathrm{ID}_{v_i}))$. Next, transfer e_{v_i} to a clerk randomly selected from G_v.

(2) The clerk computes a point P_m as

$$P_m = C - \sum_{i \in g_v} e_{v_i}, \tag{10}$$

and recover m from the x-coordinate of P_m.

(3) Compute X-coordinate as

$$X = r + h(m) \bmod q_s, \tag{11}$$

and compute the corresponding Y-coordinate on E_s.

The signature can be verified by the signing group′s public key Q_s and the base point α_s as

$$(X, Y) = s\alpha_s - rQ_s. \tag{12}$$

If equation (12) holds, the signature $\{r, s\}$ on message m is valid.

2 Cryptanalysis of Chang′s Scheme

In this section, we shall show that Chang′s scheme cannot withstand the impersonation attack, and violates the basic definition requirement of the (t, n) threshold signature with (k, l) threshold-shared verification.

Suppose that t proxy signers $u'_{s_1}, u'_{s_2}, \cdots, u'_{s_t}$ in g'_s and k verifiers $u'_{v_1}, u'_{v_2}, \cdots, u'_{v_k}$ in g'_v want to cooperatively impersonate another t proxy signers $u_{s_1}, u_{s_2}, \cdots, u_{s_t}$ in g_s and k verifiers $u_{v_1}, u_{v_2}, \cdots, u_{v_k}$ in g_v to generate and authenticate a valid threshold signature for any message m'. They can execute the following twelve steps.

(1) Each u'_{s_i} can receive $f_{s_j}(\mathrm{ID}'_{s_i})$ from u_{s_j}, where ID'_{s_i} denotes the identity of u'_{s_i} for $j = 1, 2, \cdots, n$. Then t proxy signers $u'_{s_1}, u'_{s_2}, \cdots, u'_{s_t}$ can cooperatively reconstruct each $(t-1)$th degree polynomial $f_{s_j}(x)$ by Lagrange interpotlation formula, namely $f_{s_j}(x) = \sum_{i=1}^{t} f_{s_j}(\mathrm{ID}'_{s_i}) a'_{s_i}$, where $a'_{s_i} = \prod_{c \in g'_s, c \neq i} (x - \mathrm{ID}'_{s_i} / (\mathrm{ID}'_{s_c} - \mathrm{ID}'_{s_i}))$, for $j = 1, 2, \cdots, n$. So they can compute any proxy signer u_{s_j}′s private key $k_{s_j} = \sum_{i=1}^{n} f_{s_i}(\mathrm{ID}_{s_j})$ and his public key $Q_{s_j} = k_{s_i}\alpha_s$, for $j = 1, 2, \cdots, t$.

Similarly, k verifiers $u'_{v_1}, u'_{v_2}, \cdots, u'_{v_k}$ can cooperatively reconstruct each $(k-1)$ the degree polynomial $f_{v_j}(x)$ by Lagrange interpolation formula, namely $f_{v_j}(x) = \sum_{i=1}^{k} f_{v_j}(\mathrm{ID}'_{s_i}) a'_{v_i}$, where $a'_{v_i} = \prod_{c \in g'_v, c \neq i} (x - \mathrm{ID}'_{v_i} / (\mathrm{ID}'_{v_c} - \mathrm{ID}'_{v_i}))$, for $j = 1, 2, \cdots, l$. So they can compute any verifier u_{v_j}′s private key

$k_{v_j} = \sum_{i=1}^{l} f_{v_i}(\mathrm{ID}_{v_j})$ and his public key $Q_{v_j} = k_{v_j}\alpha_s$, for $j = 1, 2, \cdots, l$. (2) Each u'_{s_i} compute the value e_{s_j} as

$$e_{s_j} = k_{s_j} a_{s_j}, \qquad j = 1, 2, \cdots, t. \tag{13}$$

(3) Each u'_{s_i} randomly choose a integer ω'_i, where $1 \leqslant \omega'_i \leqslant q_s - 1$. Then, compute R'_{s_i} as $R'_{s_i} = \omega'_i \alpha_s$, and broadcast it to the other participants in g'_s.

(4) Compute a point (X', Y') as

$$(X', Y') = \sum_{i \in g'_s} R'_{s_i} = \sum_{i \in g'_s} \omega'_i \alpha_s. \tag{14}$$

(5) Compute the individual signature $\{r', s'_i\}$ as

$$r' = X' - h(m') \bmod q_s, \qquad s'_i = e_{s_i} r' + \omega'_i \bmod q_s. \tag{15}$$

Then u'_{s_i} sends the individual signature for message m' to the designated clerk. The clerk verifies the correctness of (r', s'_i) by the equation as

$$R'_{s_i} = s'_i \alpha_s - r' a_{s_i} Q_{s_i}. \tag{16}$$

So the clerk think that u_{s_i} want to take part in the threshold signature for the message m', because his private key k_{s_i} has been used to the generation of the individual signature (r', s'_i).

The clerk combines t valid individual signature (r', s'_i) into a threshold signature (r', s') and encrypts m' by using the elliptic curve ElGamal cryptosystem.

(6) Compute the signature s' as $s' = \sum_{i \in g'_s} s'_i \bmod q_s$, (r', s') is a group signature on message m'.

(7) Express m' as the x-coordinate of a point P'_m on E_v. Then, choose a random integer ω'_c, where $1 \leqslant \omega'_c \leqslant q_v - 1$.

(8) Compute B' and the ciphertext C' as

$$B' = \omega'_c \alpha_v \bmod q_v, \qquad C' = P'_m + \omega'_c Q_v \bmod q_v. \tag{17}$$

(9) Transfe (r', s') and (B', C') to the verifying group G_v.

(10) Each u'_{v_i} computes value e_{v_i} as

$$e'_{v_i} = B' k_{v_i} a_{vi}. \tag{18}$$

Next, transfer e_{v_i} to the designated clerk of G_v. The clerk think that u_{v_i} want to take part in the verifcation of the threshold signature for message m', because his private key k_{v_i} is used to compute the value e'_{v_i}.

(11) The clerk computes a point P'_m as

$$P'_m = C' - \sum_{i \in g'_v} e'_{v_i}, \tag{19}$$

and recover m' from the x-coordinate of P'_m.

(12) Computes X'-coordinate as

$$X' = r' + h(m') \bmod q_s, \tag{20}$$

and computes the corresponding Y'-coordinate on E_s.

The signature can be verifed by the signing group's public key Q_s and the base point α_s as

$$(X', Y') = s'\alpha_s - r'Q_s. \tag{21}$$

So the t proxy signers $u'_{s_1}, u'_{s_2}, \cdots, u'_{s_t}$ in g'_s and k verifiers $u'_{v_1}, u'_{v_2}, \cdots, u'_{v_k}$ in g'_v cooperatively impersonate another t proxy signers $u_{s_1}, u_{s_2}, \cdots, u_{s_t}$ in g_s and k verifers $u_{v_1}, u_{v_2}, \cdots, u_{v_k}$ in g_v to generate and authenticate a valid threshold signature. Because the private key k_{s_i} of u_{s_i} and the private key k_{v_i} of u_{v_i} are be used to generating the individual signature and authenticate the threshold signature.

3 Conclusion

In this paper, we have shown that Chang's scheme is vulnerable to impersonation attack. In their scheme, the participant u_{s_i}'s and u_{v_i}'s private key k_{s_i} and k_{v_i} is generated by the value of $\sum_{j=1}^{n} f_{s_j}(\mathrm{ID}_{s_i})$

and $\sum_{j=1}^{l} f_{v_j}(\mathrm{ID}_{v_i})$. However, the every value $f_{s_j}(\mathrm{ID}_{s_i})$ and $f_{v_j}(\mathrm{ID}_{v_i})$ is sent by u_{s_j} and u_{v_j}, namely u_{s_i}'s and u_{v_i}'s private key k_{s_i} and k_{v_i} is not relative to themselves. It is this reason that bring to impersonal attack to their scheme.

References:

[1] DESMEDT Y, FRANKEL Y. Shared generation ofanthentication[J]. Advaces in Cryptology, Proceedings of the CRYPTO′, 1991, 91: 457-469.

[2] WANG C T, CHANG C C, LIN C H. Generalization of threshold signature and authenticated encrytion for group communications[J]. IEICE Trans Fund, 2000, 83(6): 1228-1237.

[3] HSU C L, WU T S, WU T C. Improvments of threshold signature and authti cated encryption for group communication[J]. Iform Process Letter, 2002, 81(1): 41-45.

[4] CHANG T Y, YANG C C, HWANG M S. Athreshold signature scheme for group communications without a shared distribution center[J]. Future Generation Computer Systems, 2004, 20: 1013-1021.

[5] SUN H M. An efficient nonrepudiable threshold proxy signature scheme with known signers[J]. Comput Communications, 1999, 22: 717-722.

[6] HWANG M S, LIN L C, ERIC J L. Asecure nonrepudiable threshold proxy signature scheme with known signers [J]. Informatica, 2000, 11(2): 137-144.

[7] HWANG S L, CHEN C C. Cryptanalysis of nonrepudiable threshold proxy signature with known signers[J]. Information Security Conference, 2002, 5: 243-246.

[8] HWANG S J, CHEN C C. New multi-proxy multi-signature schemes[J]. Applied Mathematics and Computation, 2004, 147: 57-67.

[9] TZENG S F, YANG C Y, HWANG M S. A nonrepudiable threshold multi-proxy multi-signature scheme with shared verification[J]. Future Generation Computer Systems, 2004, 20: 887-893.

[10] HWANG S J, CHEN C C. New threshold-proxy threshold-signature schemes[J]. Computer and Electrical Engineering, 2005, 31: 69-80.

[11] HSU C L, WU T S, HE W H. New proxy multi-signature scheme[J]. Applied Mathematics and Computation, 2005, 162: 1201-1206.

[12] HSU C L, WU T S, WU T C. New nonrepudiable threshold proxy signature scheme with known singers[J]. The Journal of Systems and Software, 2001, 58: 119-124.

[13] TZENG S F, HWANG M S, YANG C Y. An improvement of nonrepudiable threshold proxy signature scheme with known signers[J]. Computers & Security, 2004, 23: 174-178.

[14] YANG C Y, TZENG S F, HWANG M S. On the efficiency of nonrepudiable threshold proxy signature scheme with known signers[J]. The Journal of Systems and Software, 2004, 73: 507-514.

面向群通信的门限签名方案的密码学分析

韩金广[1]，亢保元[2]，王庆菊[3]

(1. 河海大学 理学院，江苏 南京 210098；2. 中南大学 数学科学与计算技术学院，湖南 长沙 410075；
3. 绍兴文理学院 数学系，浙江 绍兴 312000)

摘要：　探讨 Chang 等提出的面向群通信的(t, n)门限签名$(k, 1)$门限验证的数字签名方案. 分析认为，由于方案不需要分发中心(SDC)，任何 t 个参与者可以代替一个群(签名群)对一个信息签名，并且任何 k 个参与者可代替另外一个群(验证群)对签名进行验证，因此，不能抵抗假冒攻击.

关键词：　密码分析；假冒攻击；代理签名；门限密码体制

(责任编辑：黄仲一　　英文审校：吴逢铁)