Li 等學者一般化代理簽章法的安全分析

Cryptanalysis of Li et al.'s Generalization of Proxy Signature Schemes

黃心嘉

Hwang, Shin-Jia

淡江大學資訊工程系

Department of Computer Science and Information Engineering,

TamKang University, Tamsui, Taipei Hsien, 251, Taiwan, R.O.C.

sjhwang@mail.tku.edu.tw

詹景中

Chan, Ching-Chung

淡江大學資訊工程系

Department of Computer Science and Information Engineering,

TamKang University, Tamsui, Taipei Hsien, 251, Taiwan, R.O.C.

791190027@s91.tku.edu.tw

摘要

近來 Li 等學者提出代理簽章的一般化簽署法，然而 Li 等學者提出方法具有一個共同的安全弱點。在 Li 等學者方法中，攻擊者事先攔截某一代理群為其所代理的原始簽章群所產生的代理簽章，攻擊者便可以偽造出相同於攔截訊息的代理簽章，讓偽造的代理簽章看起來像是該代理群為攻擊者所簽署的代理簽章。

關鍵詞：代理簽章法、代理門檻式簽章法、多人代理簽章法、代理多人簽章法、多人代理多人簽章法

Abstract

Recently, Li et al. proposed their generalization of proxy signature schemes. However, all of Li et al.'s schemes have a common security weakness. In Li et al.'s schemes, an adversary first intercepts a valid proxy signature generated by a proxy group on behalf of the proxy group G_P. From the intercepted proxy signature, the adversary can forge illegal proxy signatures being like generated by the proxy group on behalf of an adversary.

Keywords: Proxy signatures scheme, proxy threshold signature scheme, multi-proxy signature scheme, proxy multi-signature scheme, multi-proxy multi-signature scheme

1. Introduction

In 1996, Mambo et al. [8, 9] proposed the concept of proxy signature scheme. In the proxy signature scheme, an original signer can authorize a proxy signer to generate a proxy signature and become his deputy. There is a limitation that one original signer can authorize only one proxy signer.

Due to the group-oriented application, many group-oriented variants of proxy signature schemes are proposed. In the proxy multi-signature scheme [3, 10, 12], proxy certificates must be authorized by all of the original signers in the original group. In a multi-proxy signature scheme [6], the proxy signature should be generated by all proxy signers in the proxy group. In 2001, the multi-proxy multi-signature scheme [4] is proposed to integrate proxy multi-signature schemes and multi-proxy signature schemes. The threshold proxy signature schemes were discussed widely [1, 2, 5, 11]. In a (t, n) threshold proxy signature scheme, an original signer can authorize a proxy group with n proxy signers to generate a proxy signature on behalf of the original signer. Then only t or more proxy signers in the proxy group can cooperatively generate the proxy signatures.

In 2003, Li et al. proposed a generalization of proxy signature schemes [7] for these schemes mentioning above. The type of delegation in Li et al.'s scheme is delegation by war-

rant. However, the Li et al.'s schemes are not secure. In the following section, the Li et al.'s schemes are briefly reviewed. Section 3 is our cryptanalysis of Li et al.'s scheme. The final section is our conclusion.

2. Brief Review of Li et al.'s Schemes

Li et al.'s (t/n-t'/n') proxy signature scheme based on the discrete logarithm problem [7] is first reviewed. Their (t/n-t'/n') proxy signature scheme consists of three phases: The proxy share generation phase, the proxy signature generation phase, and the proxy signature verification phase.

In Li et al.' s (t/n-t'/n') proxy signature scheme, there are some system-wide parameters. The public parameters p and q are two large prime numbers such that q|(p-1). The parameter g is an element of order q in Z^*_p. The public function h(.) is a secure one-way hash function. Let G_O= {$U_{O,1}$, $U_{O,2}$, …, $U_{O,n}$} denote the original group and G_P= {$U_{P,1}$, $U_{P,2}$, …, $U_{P,n'}$} denote the proxy group. There are two designated clerks, C_O and C_P, for G_O and G_P respectively. Let M_W denote a proxy warrant that records the identities of the original signers in G_O the identities of the proxy signers in G_P, the parameters (t, n) and (t', n'), and the valid delegation period. Each original signer $U_{O,i}$ randomly selects a private key $x_{O,i} \in Z^*_q$ and computes a certificated public key $y_{O,i}= g^{x_{O,i}} \bmod p$. Similarly, each proxy signer $U_{P,i}$ has a private key $x_{P,i} \in Z^*_q$ and a certificated public key $y_{P,i}= g^{x_{P,i}} \bmod p$.

Proxy share generation phase

Suppose that the original group G_O wants to authorize G_P as their proxy group satisfying the following requirements. At least t original signers in G_O must reach an agreement on the proxy authorization such that proxy signatures should be generated by the cooperation of the t' or more proxy signers in G_P. Without losing generality, assume D_O= {$U_{O,1}$, $U_{O,2}$, …, $U_{O,T}$} is the group the T actual original signers with identities AOSID, where t≤ T ≤n. Each member $U_{O,i}$ in D_O selects a random integer $R_{O,i} \in Z^*_q$, computes $k_{O,i}= g^{R_{O,i}} \bmod p$, and broadcasts $k_{O,i}$ to other T-1 original signers in D_O and the clerk C_O. After receiving all the other $k_{O,j}$' s, each $U_{O,i}$ in D_O calculates $K=\prod_{i=1}^{T} k_{O,i} \bmod p$ and $\sigma_{O,i}= R_{O,i}K+ x_{O,i}y_{O,i}h(M_W, K, AOSID) \bmod q$, and sends $\sigma_{O,i}$ to C_O. After receiving all of $\sigma_{O,i}$' s, C_O computes $K=\prod_{i=1}^{T} k_{O,i} \bmod p$ and checks the correctness of $\sigma_{O,i}$ by adopting the equation $g^{\sigma_{O,i}} \equiv k_{O,i}^{K} y_{O,i}^{y_{O,i} h(M_W,K,AOSID)} \pmod p$. If all of $\sigma_{O,i}$' s are correct, C_O computes $\sigma_O= \sum_{i=1}^{T} \sigma_{O,i} \bmod q$. Then C_O broadcasts (M_W, K, σ_O, AOSID) to G_P. Each proxy signer $U_{P,i} \in G_P$ validates (M_W, K, σ_O, AOSID) by adopting the equation $g^{\sigma_O} \equiv K^K \prod_{i=1}^{T} y_{O,i}^{y_{O,i} h(M_W,K,AOSID)} \pmod p$. Finally, each $U_{P,j}$ owns σ_O as her/his proxy share.

Proxy signature generation phase

Without losing generality, assume D_P= {$U_{P,1}$, $U_{P,2}$, …, $U_{P,T'}$} is the group the T' actual proxy signers with identities APSID, where t'≤ T'≤ n'. Each actual proxy signer $U_{P,j}$ in D_P selects a random integer $R'_{P,j} \in Z^*_q$ and calculates $k'_{P,j}= g^{R'_{P,j}} \bmod p$. Each $U_{P,j}$ in D_P broadcasts $k'_{P,j}$ to the other T'-1 proxy signers and the designated clerk C_P. After receiving all $k'_{P,j}$'s, each $U_{P,j}$ in D_P calculates $R=\prod_{j=1}^{T'} k'_{P,j} \bmod p$, finds $s_{P,j}$ satisfying the equation

$$s_{P,j}=R'_{P,j}R+(\sigma_O T'^{-1}+x_{P,j}y_{P,j})h(M,R,APSID) \bmod q,$$

and sends $s_{P,j}$ to the clerk C_P. After computing $R=\prod_{i=1}^{T'} k'_{P,i} \bmod p$, the clerk C_P validates the correctness of all $s_{P,j}$'s by the equation

$$g^{s_{P,j}}= k'^{R}_{P,j}((K^K \prod_{i=1}^{T} y_{O,i}^{y_{O,i} h(M_W,K,AOSID)})^{T'^{-1}} y_{P,j}^{y_{P,j}})^{h(M,R,APSID)} \bmod p.$$

Then the clerk C_P computes $S= \sum_{j=1}^{T'} s_{P,j} \bmod q$.

In other words, $S= \sum_{j=1}^{T'} (RR'_{P,j}+ (\sigma_O T'^{-1}+$

$x_{P,j}y_{P,j})h(M, R, APSID)) \bmod q = R\sum_{j=1}^{T'} R'_{p,j}$

$+(\sigma_O+\sum_{j=1}^{T'} x_{P,j}y_{P,j})h(M, R, APSID) \bmod q.$

Finally, the proxy signature of the message M is (M_W, K, AOSID, M, (R, S), APSID).

Proxy signature verification phase

To validate the proxy signature (M_W, K, AOSID, M, (R, S), APSID), any verifier first obtains the certificated public keys of the actual proxy signers and actual original signers according to AOSID and APSID from the proxy warrant M_W. Then the verifier adopts the equation

$$g^S \equiv R^R(K^K \prod_{i=1}^{T} y_{O,i}^{y_{O,i}h(M_W,K,AOSID)} \prod_{j=1}^{T'} y_{P,j}^{y_{P,j})^{h(M,R,APSID)}} \pmod p$$

to validate the proxy signature (M_W, K, AOSID, M, (R, S), APSID).

3. Cryptanalysis of Li et al's Scheme

An attack on Li et al.'s (t/n-t'/n') proxy signature scheme is proposed. Supposes that an adversary, A, wants to forge proxy signatures generated by the group D_P such that G_P becomes his deputy. The adversary A first intercepts σ_O and a legal proxy signature (M_W, K, AOSID, M, (R, S), APSID) generated by D_P on behalf of G_O. First of all, the adversary A illegally authorizes the group G_P as his agent. The adversary A randomly selects an integer $R_A \in Z^*_q$ and computes $K_A = g^{R_A} \bmod p$. Then A uses his secret key x_A to generate σ' such that $\sigma' = R_AK_A + x_Ay_Ah(M'_W, K_A, ID_A) \bmod q$, where $AOSID = ID_A$ and M'_W is an illegal proxy warrant. The adversary A computes $\Delta = \sigma' - \sigma_O \bmod q$ and finds S' such that $S' = \Delta h(M, R, APSID)+S \bmod q$. Finally A forges an illegal proxy signature (M'_W, K_A, $AOSID=ID_A$, M, (R, S'), APSID) being like to be generated by the proxy group G_P on behalf of A. The following gives why the attack is success. In other words, the forged proxy signature (M'_W, K_A, $AOSID=ID_A$, M, (R, S'), APSID) can pass the verification equation $g^{S'} =$

$$R^R(K_A^{K_A}y_A^{y_Ah(M'_W,K_A,ID_A)} \prod_{j=1}^{T'} y_{P,j}^{y_{P,j})^{h(M,R,APSID)}} \bmod p$$

$$S' \equiv \Delta h(M, R, APSID)+S$$

$$\equiv (\sigma'-\sigma_O)h(M,R,APSID)+ S$$

$$\equiv (\sigma'-\sigma_O)h(M,R,APSID)+ R\sum_{j=1}^{T'} R'_{P,j}+ (\sigma_O + \sum_{j=1}^{T'} y_{P,j}x_{P,j})h(M,R,APSID)$$

$$\equiv R\sum_{j=1}^{T'} R'_{P,j}+ (\sigma'+\sum_{j=1}^{T'} y_{P,j}x_{P,j})h(M, R, APSID)$$

$$\equiv R\sum_{j=1}^{T'} R'_{P,j}+(K_AR_A+ y_Ax_Ah(M'_W,K_A,ID_A) + \sum_{j=1}^{T'} y_{P,j}x_{P,j})h(M,R,APSID) \pmod q.$$

4. Conclusions

An attack on Li et al.'s proxy signature schemes [7] is proposed to show that their schemes have security problem. By our attack, any adversary intercepts the proxy share and a valid proxy signature generated by a proxy group on behalf of an original group. Then the adversary can forge a proxy signature being like the one that is generated by the proxy group G_P on behalf of the adversary.

References

[1] Hsu, Chien-Lung, Wu, Tzong-Sun, and Wu, Tzong-Chen, "New nonrepudiable threshold proxy signature scheme with known signers," The Journal of Systems and Software, Vol. 58, pp. 119-124, 2001.

[2] Hwang, Min-Shiang, Lin, Iuon-Chang, and Lu, Jui-Lin Eric, "A secure nonrepudiable threshold proxy signature scheme with known signers," INFORMATICA, Vol. 11, No. 2, 2000, pp. 137-144.

[3] Hwang, Shin-Jia, and Chen, Chiu-Chin, "A New Proxy Multi-Signature Scheme," The 2001 International Workshop on Cryptology and Network Security, Taipei, Taiwan, R.O.C., Sep. 26-28, 2001, pp. 199-204.

[4] Hwang, Shin-Jia, and Chen, Chiu-Chin, "A New Multi-Proxy Multi-Signature Scheme," 2001 National Computer Symposium: Information Security, Taipei, Taiwan, R.O.C., Dec. 20-21, 2001, pp. F019-F026. Also appear in Applied Mathematics and Computation.

[5] Hwang, Shin-Jia, and Chen, Chiu-Chin, "Cryptanalysis of Nonrepudiable Threshold Proxy Signature Schemes with Known Signers," Journal of Informatica, Vol. 14, No. 2, 2003, pp. 205-212.

[6] Hwang, Shin-Jia and Shi, Chi-Hwai, "A simple multi-proxy signature scheme," Proceedings of the Tenth National Conference on Information Security, Taiwan, pp. 134-138, 2000

[7] Li, Li-Hua, Tzeng, Shiang-Feng, and Hwang, Min-Shiang, "Generalization of proxy signature-based on discrete logarithms," Computers & Security, Vol. 22, No. 3, pp. 245-255, 2003.

[8] MAMBO, Masahiro, USUDA Keisuke, and OKAMOTO, Eiji, "Proxy signatures: Delegation of the power to sign message," IEICE. Trans. Fundamentals, E79-A, 9, pp. 1338-1354, 1996.

[9] MAMBO, Masahiro, USUDA Keisuke, and OKAMOTO, Eiji, "Proxy signatures for delegation signing operation," Proc. 3rd ACM Conference on Computer and Communication Security, pp. 48-57, 1996.

[10] Sun, Hung-Min, "On proxy (multi-) signature schemes," 2000 International Computer Symposium, Chiayi, Taiwan, R.O.C., Dec. 6-8, 2000, pp. 65-72.

[11] Sun, Hung-Min, Lee N.-Y., and Hwang, T., "Threshold proxy signatures," IEE Proceedings-computers & Digital Techniques, Vol. 146, No. 5, pp. 259-263, September 1999.

[12] Yi, L. Bai, G., and Xiao, G., "Proxy multi-signature scheme: A new type of proxy signature scheme," Electronics Letters, Vol. 36, No. 6, pp.527-528, 2000.