两个代理签名方案的密码学分析*)

明 洋 王育民

(西安电子科技大学综合业务网络国家重点实验室 西安 710071)

摘 要 最近,戴等人提出了一种指定接收人的代理签名方案和一种消息保密的代理签名方案。在本文中,给出了这两个代理签名方案的安全分析,指出它们是不安全的,都不能抵抗原始签名者的伪造攻击。

关键词 代理签名,伪造攻击,安全分析

Cryptanalysis of Two Proxy Signatures Schemes

MING Yang WANG Yu-Min

(State Key Lab. of Integrated Service Networks, Xidian Univ. Xi'an 710071)

Abstract Recently, Dai et al. propose a designated-receiver proxy signature scheme and a proxy signature scheme with privacy protection. In this paper, we give security analysis of the two proxy signature schemes. The schemes are all insecure against the original signer's forgery attack.

Keywords Proxy signature, Forgery attack, Security analysis

1 引言

1996年Mambo等人提出代理签名的概念[1]。在这种签名中,原始签名者把他或她的签名能力授权给一个代理签名者。然后,代理签名者能够代表原始签名者签发一定的消息。当接收到某一个消息的代理签名后,一个验证者能够通过给定的步骤来验证有效性,从而可以相信这个消息的签名是原始签名者同意和授权的。代理签名被建议了许多的应用,尤其是在权力委托的情况下及在分配计算中使用,在电子现金系统、电子商务的移动代理、移动交互、网格计算等均有使用。

一个代理签名应满足下面的安全需求[1]:

(1)可验证性:任何人能够验证代理签名的有效性,并且根据有效的代理签名可以确认原始签名者承认签署的文件。

(2)不可伪造性:除了指定的代理签名者外,任何其他人都不能生成代表原始签名者的有效的代理签名。

(3)可识别性:任何验证者都能够从代理签名中确定代理签名者的身份。

(4)不可否认性:一旦代理签名者代替原始签名者产生了有效的代理签名,他就不能向任何人否认他所签署的有效的代理签名。

最近,为了防止代理签名权力的滥用,戴等人结合Schnorr签名方案[2]和指定接收人签名方案[3],提出一种指定接收人的代理签名方案[4],方案声称满足代理签名方案的安全性需求。为了保护原始签名人的隐私,戴等人基于Elgamal加密和盲Nyberg-Rueppel签名方案[5],提出一种消息保密的代理签名方案[6],同样声称满足代理签名的安全性需求。

本文中,我们给出戴等人所提出方案的安全性分析,指出这两个方案都不能抵抗原始签名者的伪造攻击,即原始签名者能够伪造出代理签名,并且声称是代理签名者生成的。这一点不能满足代理签名的安全性需求。

2 戴等人的一种指定接收人的代理签名方案

为了防止代理签名权力的滥用,戴等人结合Schnorr签名方案和指定接收人方案,提出指定接收人的代理签名方案,下面给出这个方案的描述,具体的细节可以看参考文[4]。

2.1 系统的安全参数

p,q是两个大素数且满足$q|p-1$,g是Z_p^*中q阶乘法子群的生成元,$h(\cdot)$是安全的单向hash函数,(x_A,y_A)表示原始签名者A的私钥和公钥对,满足$y_A=g^{x_A} \bmod p$。(x_B,y_B)表示代理签名者B的私钥和公钥对,满足$y_B=g^{x_B} \bmod p$,(x_C,x_C)表示接收者C的私钥和公钥对,满足$y_C=g^{x_C} \bmod p$。M表示待签名的消息。

2.2 代理授权

原始签名者A选取$k_A\in_R Z_p^*$,计算$r_A=g^{k_A} \pmod p$,$e_A=H(M,y_C,r_A,)$,$s_A=x_Ae_A+k_A \pmod p$。原始签名者A把代理授权(M,s_A,r_A,y_C,y_A)秘密的传给代理签名者B。

2.3 代理授权的验证

代理签名者B收到(M,s_A,r_A,y_C,y_A)后,验证$g^{s_A}=y_A^{H(M,y_C,r_A)}r_A \pmod p$是否成立,如果成立,则代理签名者$B$接受$(M,s_A,r_A,y_C,y_A)$为有效的授权,否则$B$拒绝。

2.4 代理签名的生成

代理签名者B计算代理签名密钥对$x_p=s_A+x_B \pmod q$,$y_P=g^{x_P}=y_A^{H(m,y_C,r_A)}r_Ay_B \pmod p$。

代理签名者B生成代理签名如下:随机选取$R,r\in Z_q^*$,并计算$K=g^{R-r} \pmod p$,$D=y_C^R \pmod p$,$e_B=H(y_C,K,D,M)$,$s=r-x_p\cdot e_B \pmod q$。则(M,r_A,K,D,s,y_A,y_B)为代理签名并发送给接收者C。

2.5 代理签名的验证

接收者C收到签名(M,r_A,K,D,s,y_A,y_B)后,首先计算$e_A=H(M,y_C,r_A)$,$e_B=H(y_C,K,D,M)$,检验$(g^s(y_P)^{e_B}K)^{x_C}$

*)基金项目:国家自然科学基金资助项目(60473072)。明 洋 博士生,主要研究方向为密码学理论,电子商务。王育民 教授,博士生导师,主要研究方向为信息论,密码,编码。

$=(g^{s'}(y_A^{r'_A}r_A y_B)^{\epsilon'_B}K)^{x_C}=D(\mathrm{mod}\ p)$是否成立，如果成立，则接收者接受这个签名。

3 对指定验证者代理签名方案的密码学分析

我们给出戴等人的指定验证者代理签名方案的安全性分析，得出该方案不能抵抗原始签名者的伪造攻击。

原始签名者 A 伪造攻击如下：

原始签名者 A 随机选取 $a,R',r'\in Z_q^*$

计算 $r'_A=y_B^{-1}g^a(\mathrm{mod}\ p)$

$e'_A=H(M,y_C,r'_A)$

$K'=g^{R'-r'}(\mathrm{mod}\ p)$

$D'=y_C^{R'}(\mathrm{mod}\ p)$

$e'_B=H(y_C,K',D',M)$

$s'=r'-(x_A\cdot H(M,y_C,r'_A)+a)\cdot H(y_C,K',D',M)$
$(\mathrm{mod}\ q)=r'-(x_A\cdot e'_A+a)\cdot e'_B(\mathrm{mod}\ q)$

则$(M,r'_A,K',D',s',y_A,y_B)$是一个有效的代理签名，因为

$$(g^{s'}(y_P)^{\epsilon'_B}K')^{x_C}=(g^{s'}(y_A^{r'_A}r'_A y_B)^{\epsilon'_B}K')^{x_C}$$
$$=(g^{r'-(x_A\cdot e'_A+a)\cdot e'_B}(g^{x_A\cdot e'_A}\cdot y_B^{-1}g^a\cdot y_B)^{e'_B}g^{R'-r'})^{x_C}=(g^{R'})^{x_C}=(g^{x_C})^{R'}=y_C^{R'}=D'(\mathrm{mod}p)$$

由上式可以得出原始签名者伪造的代理签名(M,r'_A,K',D',s,y_A,y_B)满足代理签名的验证方程，所以对这个方案伪造攻击成功。

4 戴等人的一种消息保密的代理签名方案

戴等人基于 Elgamal 加密和盲 Nyberg-Rueppel 签名方案，提出一种消息保密的代理签名方案。首先给出这个方案的描述，具体的细节可以看参考文[6]。系统的参数如上。

4.1 代理授权

原始签名者 A 随机选取$k\in Z_q^*$，计算 $a=g^k(\mathrm{mod}\ p)$，$b+My_C^k(\mathrm{mod}\ p)$，$s_A=x_AH(a,k,y_C)+k(\mathrm{mod}\ q)$，$A$ 把代理授权(a,b,y_C,y_A,s_A)秘密的传给代理签名者 B。

4.2 代理授权的验证

代理签名者 B 接收到(a,b,y_C,y_A,s_A)后，验证 $g^{s_A}=y_A^{H(a,b,y_C)}a(\mathrm{mod}\ p)$是否成立，如果成立，则 B 接受(a,b,y_C,y_A,s_A)为有效的授权。

4.3 代理签名的产生

代理签名者 B 生成代理签名密钥对 $x_P=s_A+x_B(\mathrm{mod}\ q)$，$y_P=g^{x_P}=y_A^{H(a,b,y_C)}\cdot a\cdot y_B(\mathrm{mod}\ p)$。

代理签名者 B 使用x_P 和盲 Nyberg-Rueppel 签名方案产生签名：

1)B 随机选择$\tilde{k}\in Z_q^*$，计算 $\tilde{r}=g^{\tilde{k}}(\mathrm{mod}\ p)$，把$(a,b,y_A,y_B,\tilde{r})$给指定接收者 C。

2)签名的接收者 C 使用密钥 x_C 恢复出消息 M，即$\frac{b}{a^{x_C}}=M(\mathrm{mod}\ p)$。

随机选择 $a,\beta\in Z_q^*$，计算 $r=mg^a\tilde{r}^{\beta}(\mathrm{mod}\ p)$，$\tilde{M}=r\beta^{-1}(\mathrm{mod}\ q)$。

检查$\tilde{M}\in Z_q^*$，如果成立，则把 $\tilde{M}$ 发送给代理签名者 B，否则重新计算 $\tilde{M}$。

3)代理签名者 B 计算$\tilde{s}=\tilde{M}x_P+\tilde{k}(\mathrm{mod}\ q)$，并把 $\tilde{s}$ 发送给指定接收者 C。

4)指定接收者 C 计算$s=\tilde{s}\beta+a(\mathrm{mod}\ q)$，则$(a,b,y_A,y_B,r,s)$为消息 M 的签名。

4.4 签名的验证

指定接收者 C 验证$g^{-s}y_P^r r=g^{-s}(y_A^{H(a,b,y_C)}\cdot a\cdot y_B)^r r=M(\mathrm{mod}\ p)$是否成立，如果成立，则此签名是有效的。

5 对消息保密代理签名方案的密码学分析

我们给出戴等人的消息保密代理签名方案的安全性分析，得出该方案不能抵抗原始签名者的伪造攻击。

原始签名者伪造攻击如下：

随机选择 $a,\bar{k}\in Z_q^*$

令 $\bar{a}=y_B^{-1}g^a(\mathrm{mod}\ p)$，$\bar{b}=My_C^{\bar{k}}(\mathrm{mod}\ p)$

计算 $\bar{x}_p=x_AH(\bar{a},\bar{b},y_C)+a(\mathrm{mod}\ q)$，$\bar{y}_p=g^{\bar{x}_p}(\mathrm{mod}\ p)$

则$(\bar{x}_p,\bar{y}_p)$是一个有效的代理签名密钥对，因为

$$\bar{y}_p=y_A^{H(\bar{a},\bar{b},y_C)}\bar{a}y_B\ \mathrm{mod}\ p$$
$$=g^{x_AH(\bar{a},\bar{b},y_C)}y_B^{-1}g^a y_B\ \mathrm{mod}\ p$$
$$=g^{x_AH(\bar{a},\bar{b},y_C)+a}\mathrm{mod}\ p$$
$$=g^{\bar{x}_p}\ \mathrm{mod}\ p$$

所以签名$(\bar{a},\bar{b},y_A,y_B,r,s)$是消息 M 的有效签名。并且伪造签名满足签名的验证方程，所以对这个方案的伪造攻击成功。

结论 本文分析了戴等人提出的指定接收人的代理签名方案和消息保密的代理签名方案，指出这两个方案都不安全，都不能抵抗原始签名者的伪造攻击。

参 考 文 献

1 Mambo M, Usuda K, Okamoto E. Proxy signature for delegating signing operation. In: Proc. of the 3. th ACM Conf. on Computer and Communications Security, New Dehli, India, New York: ACM Press, 1996. 48～57

2 Schnorr C P. efficient identification and signatures for smart cards [A]. Advances in cryptology-Crypto'89, LNCS1435. Berlin: Springer-verlag, 1990. 239～252

3 Kim S J, Park S J, Won D H. Zero-knowledge nominative signature. In: Proc. of Pragocrypt'96, Int. conf. on the theory and applications of cryptology, 1996. 380～392

4 戴佳筑，杨小虎，董金详. 一种指定接收人的代理签名方案[J]. 浙江大学学报(工学版)，2004,38(11):1422～1425

5 Camenisch L J, Piveteau M J, Stadler A M. Blind signatures based on the discrete logarithm problem[A]. Advances in Cryptology'92. Berlin:Springer-verlag,1995. 428～432

6 戴佳筑，杨小虎，董金详. 一种消息保密的代理签名方案[J]. 浙江大学学报(工学版)，2005,39(5):701～704