第34卷 第17期 计 算 机 工 程 2008年9月
Vol.34 No.17 Computer Engineering September 2008
·安全技术· 文章编号：1000—3428(2008)17—0147—02 文献标识码：A 中图分类号：TP309

抗合谋攻击的门限签名方案

侯整风，赵 香，杨 曦
(合肥工业大学计算机与信息学院，合肥 230009)

摘 要：门限签名是一种特殊而重要的数字签名。但在现有的门限签名方案中，合谋攻击一直是一个难以解决的问题。该文对现有抗合谋攻击门限签名方案进行了安全性分析，指出该方案存在的缺陷，并基于现有的门限签名体制，对如何抵抗合谋攻击给出了一些启发式的思想和方法。

关键词：密码学；门限签名；合谋攻击

Threshold Signature Scheme to Withstand Conspiracy Attack

HOU Zheng-feng, ZHAO Xiang, YANG Xi
(School of Computer and Information, Hefei University of Technology, Hefei 230009)

【Abstract】 Threshold signature is a kind of special and important digital signature. But in the existing threshold signature scheme, conspiracy attack is still a problem which is difficult to solve. This paper analyzes a threshold signature scheme to withstand conspiracy attack, analyzes its weakness and proposes some heuristic idea and methods to withstand conspiracy attack based on the existing threshold signature schemes.

【Key words】 cryptography; threshold signature; conspiracy attack

1 概述

(t,n)门限签名方案最早是由Desmedt和Frankel[1]提出的。该方案是指，n个成员共享群体密钥，当参与签名的成员数目大于或等于规定的门限值t时，就能代表群体产生签名，任何验证者都可以用群公钥验证签名的有效性。(t,n)门限签名自提出以来取得了很大的发展，但由于现有的门限签名方案都是基于Shamir(t,n)门限秘密共享体制的，因此，自从台湾学者Li C.M.[2]提出合谋攻击问题以来，合谋攻击就一直是门限签名中难以解决的问题。

合谋攻击是指，当群中 t 个或更多的恶意成员合谋时，就可以恢复群秘密多项式，从而获得群密钥和其他成员的私钥，因此群内的一组成员可以假冒另一组成员进行签名。许多学者对如何抵抗合谋攻击做了大量研究。1999 年 Jan 和 Tseng 提出了一个不可追踪的抗合谋攻击方案；Li Z.C.等人提出了 2 个没有附加秘密数的抗合谋攻击方案；王斌和李建华的基于联合秘密共享技术提出了一个无可信中心的抗合谋攻击方案等。这些方案都被证实不能抵抗合谋攻击。

最近，Jan和Gan[3]分别提出 2 个新的抗合谋攻击方案，方案使用了离散对数和RSA相结合的密钥体制，并加入签名者追踪机制。但是文献[4]给出了一个攻击算法证明他们的方案是不安全的，并给出了一个改进的抗合谋攻击方案。

2 文献[4]的方案

文献[4]的方案由 4 个部分组成：系统初始化阶段，秘密影子的分发和验证阶段，个体签名的产生和验证阶段，门限签名的产生和验证阶段。

(1)系统初始化阶段

可信中心负责选取参数如下：

随机选择 4 个大素数p,q,p',q'，满足$p=2p'+1$和$q=2q'+1$，计算 $N=p\cdot q$。设g是 Z_N^* 中阶为 $v=p'\cdot q'$ 的生成元，随机选择e使得$gcd(e,v)=1$，并由 $e\cdot d=1 \bmod v$ 计算出d。选择安全的单向哈希函数$h()$和一个$(t\text{-}1)$阶多项式 $f(x)=c_0+c_1x+\cdots+c_{t-1}x^{t-1} \bmod v$，$c_0,c_1,\cdots,c_{t-1}\in Z_v^*$。

可信中心计算 $f_k=g^{c_k} \bmod N, k=0,1,\cdots,t-1$。令群私钥 $x=f(0) \bmod v$，群公钥 $y=g^x \bmod N$。可信中心公布$\{e,y,N,g,f_k,h()\}$，保密$\{p,q,p',q',d,x,v\}$。

(2)秘密影子的分发和验证阶段

设$A=\{U_1,U_2,\cdots,U_n\}$是群中的n个成员，身份标识是ID_i。对于群中每个成员 $U_i\in A$，可信中心计算U_i的私钥 $x_i=(g^{f(ID_i)})^d \bmod N$ 和他的公钥 $y_i=g^{f(ID_i)} \bmod N$，并通过秘密通道把x_i发送给每个U_i，U_i可以通过等式 $x_i^e=\prod_{j=0}^{t-1} f_j^{ID_i^j} \bmod N$ 检查私钥的正确性。

(3)个体签名的产生和验证阶段

不失一般性，设t个成员$B=\{U_1,U_2,\cdots,U_t\}$要对消息m产生代表群的门限签名，则他们一起执行以下步骤：

Step1 选取随机数k_i，计算 $r_i=g^{k_i\cdot e} \bmod N$，并将$r_i$广播给$B$中的其他成员。

Step2 每个成员在收到t个r_i后，计算：

$$R=\prod_{i\in B} r_i \bmod N$$

$$s_i=x_i^{h(m,R)\prod_{j\in B,j\neq i}\frac{-ID_j}{ID_i-ID_j}}\cdot(g^{k_i})^R \bmod N$$

然后将个体签名$\{r_i,s_i\}$发送给签名合成者。

签名合成者通过等式 $(s_i)^e=(y_i)^{h(m,R)\prod_{j\in B,j\neq i}\frac{-ID_j}{ID_i-ID_j}}\cdot(r_i)^R \bmod N$

作者简介：侯整风(1958－)，男，教授，主研方向：网络与信息安全，数据库；赵 香、杨 曦，硕士研究生

收稿日期：2008-05-21 **E-mail：**yangxi830417@yahoo.com.cn

验证个体签名的正确性。

(4)门限签名的产生和验证阶段

签名合成者计算 $R=\prod_{i\in B} r_i \bmod N$ 和 $S=\prod_{i\in B} s_i \bmod N$，$\{R,S\}$ 即消息 m 的门限签名。

任何验证者都可以通过验证方程 $(S)^e = y^{h(m,R)}\cdot R^R \bmod N$ 验证签名的正确性。

文献[4]称：在这个方案中，恶意的t个成员B'合谋可以伪造B对消息m'的门限签名$\{R',S'\}$，但是，B'却不能伪造B中每个成员的个体签名$\{r_i',s_i'\}$，因为从验证等式 $(r_i')^{R'} = (s_i')^e((y_i)^{h(m',R')\prod_{j\in B,j\neq l}\frac{-ID_j}{ID_i-ID_j}})^{-1} \bmod N$ 求得 r_i' 是不可能的，这是R'次根问题，所以该方案可以抵抗合谋攻击，是安全的。

3 对文献[4]方案的分析

经分析，Xie的方案存在如下的安全性隐患：假设B'已经拥有B对消息m的签名，则B'不仅可以伪造B对消息m'的门限签名$\{R',S'\}$，而且可以避开R'次根问题，伪造出合法的个体签名$\{r_i',s_i'\}$。具体攻击步骤如下:

(1)对于每个 $U_i \in B'$，由于他们知道m,R,ID_j以及自己的私钥x_i，因此他们可以合谋计算出：

$$y^{h(m,R)d} = \prod_{i\in B'} x_i^{h(m,R)\prod_{j\in B',j\neq i}\frac{-ID_j}{ID_i-ID_j}} \bmod N$$

(2)任选随机数 $c\in Z_N$，计算：

$R' = y^{h(m,R)}\cdot g^{ce} R^R \bmod N$ ；

(3)B'合谋可以计算出：

$$y^{h(m',R')d} = \prod_{i\in B'} x_i^{h(m',R')\prod_{j\in B',j\neq i}\frac{-ID_j}{ID_i-ID_j}} \bmod N$$

(4)令 $S' = y^{h(m',R')d}(Sg^c)^{R'} \bmod N$，则门限签名$\{R',S'\}$生成。

显然，验证等式 $(S')^e = y^{h(m',R')}(R')^{R'} \bmod N$ 成立，其正确性证明见文献[4]，即B'能够合谋伪造出B对消息m'的门限签名$\{R',S'\}$。接下来证明B'能够伪造出B中每个成员的个体签名$\{r_i',s_i'\}$，其攻击步骤如下：

B'中的成员合谋，随机选择 $v_i \in Z_N^*$ (i=1,2,⋯,t-1)，使得 $S\cdot g^c = \prod_{i=1}^{t} v_i \bmod N$ 。

令 $r_i' = (v_i)^e \bmod N$，$s_i' = (v_i)^{R'}(x_i)^{h(m',R')\prod_{j\in B',j\neq l}\frac{-ID_j}{ID_i-ID_j}} \bmod N$;则伪造的个体签名$\{r_i',s_i'\}$生成。

显然，验证公式 $(s_i')^e = (y_i)^{h(m',R')\prod_{j\in B',j\neq l}\frac{-ID_j}{ID_i-ID_j}}\cdot(r_i')^{R'} \bmod N$ 成立，其正确性证明如下：

$$(s_i')^e = (v_i)^{R'e}((x_i)^{h(m',R')\prod_{j\in B',j\neq l}\frac{-ID_j}{ID_i-ID_j}})^e =$$
$$(v_i^e)^{R'}(x_i^e)^{h(m',R')\prod_{j\in B',j\neq l}\frac{-ID_j}{ID_i-ID_j}} =$$
$$(r_i')^{R'}(y_i)^{h(m',R')\prod_{j\in B',j\neq l}\frac{-ID_j}{ID_i-ID_j}} \bmod N$$

另外，该攻击方案还满足 2 个潜在的条件，即：$\prod_{i=1}^{t} r_i' = R'$ 和 $S' = \prod_{i=1}^{t} s_i' \bmod N$ 。证明如下：

$$\prod_{i=1}^{t} r_i' = \prod_{i=1}^{t}(v_i)^e = S^e\cdot g^{ce} = R' \bmod N$$

$$\prod_{i=1}^{t} s_i' = \prod_{i=1}^{t}(s_i)^{R'}(x_i)^{h(m',R')\prod_{j\in B',j\neq l}\frac{-ID_j}{ID_i-ID_j}} =$$

$$S^{R'}\cdot g^{cR'}\cdot y^{h(m',R')d} = S' \bmod N$$

因此，该方案既能伪造出满足签名验证等式的个体签名$\{r_i',s_i'\}$，又能满足 2 个前提条件，是一个有效的攻击方案。

4 抗合谋攻击方案的研究讨论

从对文献[4]的方案和以往研究的分析可知，人们虽然对抗合谋攻击做出了大量研究，但至今尚未出现一个被广泛认可的抗合谋攻击方案或策略。在此，分析几种在门限签名中常用的抗合谋攻击的方法和对应的攻击手段，并提出一些抗合谋攻击的思想和方法：

(1)从门限签名的特点可知，签名合成者(DC)在门限签名中具有特殊的地位。如果签名合成者和伪造者进行合谋，他们很容易伪造签名，如中断协议攻击[5]、伪造攻击等。因此，任何门限签名方案都应该考虑对签名合成者加以限制。徐秋亮、陈泽雄等人提出了签名发布密钥的思想，将门限签名的发布权限制于签名合成者一人。这样做虽然不能完全解决合谋问题，但可以防止签名合成者参与合谋。

(2)在签名合成者值得信赖的情况下，如何防止伪造个体签名将成为抗合谋攻击的关键。Li C.M.[6]利用添加随机数的方法隐藏成员私钥，并实现对内部成员的追踪以抵抗合谋，但Michels[5]证实，用加随机数的方法不能防止内部成员的伪造攻击，他们提出的改进思想是使用同步广播信道或对随机数r进行零知识证明，或者用Hash函数取代对r的一些运算。

(3)近来，又有一些新的抗合谋方案不断被提出，如胡迎松、徐鹏等人 2007 年在 Xie 签名方案基础上提出的一个基于消息源可识别数字签名的抗合谋方案。但是该方案忽略了伪造者可以恢复出被伪造者私钥的事实，从而伪造者同样可以伪造出合法的签名，因此该方案也没有完全解决合谋攻击问题。

综合以上分析，本文提出以下一些可以用于抵抗合谋攻击的思想和方法：

(1)采用责任集中或限制权利的协议，确保签名合成者诚实可靠。

(2)尽量不使用成员的公开信息作为成员身份标识或用于生成密钥。

(3)采用特权集的思想，设置部分特权成员，每次签名都必须有一些特权成员参与，其实质就是使抗合谋任务的分散到每个特权成员身上，这样可防止普通成员的合谋攻击。

(4)在每次签名中附加时间戳，防止中断协议攻击，并根据计算复杂度和系统安全性的需要，综合使用“ 添加随机数、消息源可识别数字签名 ”等方法，增加合谋攻击的难度。

5 结束语

本文对文献[4]中提出的门限签名方案进行了攻击，证明其不能满足抗合谋攻击的特性，最后通过对几种抗合谋攻击方法和对应攻击方法的分析总结，提出了抗合谋攻击的一些思想和策略。虽然说这些策略还不能完全实现抵抗合谋攻击，但对后续研究具有较好的参考价值。

参考文献

[1] Desmedt Y, Frankel Y. Shared Generation of Authenticators and Signatures[C]//Proc. of Advances in Cryptology-CRYPTO’91. Berlin, Germany: Springer, 1992: 457-469.

（下转第 152 页）