对一种向前安全群签名体制的密码学分析

鲁荣波[1],杨兴萍[2],何大可[3]
LU Rong-bo[1],YANG Xing-ping[2],HE Da-ke[3]

1.吉首大学 数学与计算机科学学院,湖南 吉首 416000
2.吉首大学 网络中心,湖南 吉首 416000
3.西南交通大学 信息安全与国家计算网格实验室,成都 610031
1.College of Math. and Computer Science,Jishou University,Jishou,Hunan 416000,China
2.Center of Network,Jishou University,Jishou,Hunan 416000,China
3.Laboratory of Information Security and National Computing Gird,Southwest Jiaotong University,Chengdu 610031,China
E-mail:lurongbo8563@163.com

LU Rong-bo,YANG Xing-ping,HE Da-ke.Cryptanalysis of efficient revocable group signature scheme with forward security.Computer Engineering and Applications,2008,44(15):124-126.

Abstract: The efficient revocable group signature scheme with forward security proposed by Chen Shao-Zhen et al is analyzed. First,its shortage in the module and there is redundancy data in the scheme,so,it is low in efficiency.At the same time,it is insecure.The group manager can forge group signatures that can be verified by a verifier.
Key words: group signature;forward security;revocable;cryptanalysis;redundant data

摘 要:对陈少真等提出的一种有效取消的向前安全群签名方案进行了密码学分析,首先指出该群签名体制存在错误的模运算及冗余数据,效率不高。其次,指出该群签名体制是不安全的,群管理员可以伪造能够通过验证的群签名。
关键词:群签名;向前安全;可取消性;密码学分析;冗余数据
DOI:10.3778/j.issn.1002-8331.2008.15.040 **文章编号**:1002-8331(2008)15-0124-03 **文献标识码**:A **中图分类号**:TP309

1 引言

群签名最早是 Chaum 和 Heyst 在 1991 年提出来的[1]。群成员允许任何群成员代表群进行匿名的签名,如发生争执,群管理员可以(或者借助一个第三方)揭示签名者的身份。由于群签名很好地为签名者(群成员)提供隐私保护,群签名在不同的领域越来越得到广泛的应用,如电子货币、电子选举、电子拍卖等,目前,人们已经提出了若干不同类型的群签名方案[2-4],这些方案中的相当一部分都在标准的密码学假设之下得到了安全性证明。但是,这些方案的群公钥/群签名的长度大都与群体中成员的个数呈线性关系,因此只能应用于较小的群体。直到 1997 年,J.Camenishj 和 M.Stadler 在文献[2]中提出了第一个效率相对较高且适用于大群体的群签名方案(简称为 CS97 方案)。该方案是第一个群公钥长度、群签名长度与群成员个数无关的群签名方案。其另一个优点是当有新成员加入群体时,无需改变群公钥。然而,CS97 方案在抵抗联合攻击方面是有弱点的。G.ATENIESE 等人在文献[4]中指出,CS97 方案的成员证书形式$(a^x+1)^d$并不安全,如果有 3 个群成员串通就可以成功地发动联合攻击。因此建议将 CS97 方案的成员证书形式修改,G.ATENIESE 等人在文献[5]中又进一步指出,在 CS97 方案的成员证书修改形式$(a^x+r)^d$中,r必须是随机选取的。特别是,如果以 a 为底 r 的离散对数是已知的,则 3 个串通的群成员仍然有可能成功地发动联合攻击。1998 年 J.CAMENISH 和 M.MICHELS 在文献[6]中提出了一个更为高效的群签名方案(简称为 CM98 方案)。该方案的安全性建立在强 RSA 假设以及 Diffie-Hellman 判定问题假设之上,而且其抵抗联合攻击的安全性已经在强 RSA 的假设下得到了证明。2000 年,ATENIESE 等人提出了一个新的群签名方案(简称为 ACJT 方案)[5]。在安全性方面,ACJT 方案的成员加入协议关于新成员所选取的秘密值满足统计上的零知识,且已得到证明可以抵抗自适应的攻击者所发动的联合攻击。ACJT 方案是目前较为理想的方案。

一般而言,一个安全有效的群签名需要满足以下安全性需求:

基金项目:国家自然科学基金(the National Natural Science Foundation of China under Grant No.60503005);湖南省自然科学基金(the Natural Science Foundation of Hunan Province of China under Grant No.07JJ6110);湖南省教育厅资助项目(the Research Project of Department of Education of Hunan Province of China under Grant No.07C522)。
作者简介:鲁荣波(1970-),男,副教授,博士,主要研究方向信息安全、电子支付;杨兴萍(1958-),女,高级实验师,主要研究方向信息理论与信息技术、网络信息安全;何大可,教授,博士生导师,主要研究方向网络安全、信息安全、电子支付、并行计算。
收稿日期:2007-11-05 **修回日期**:2007-12-24

(1)可验证性:利用公开的信息,一个合法的群成员按照签名算法产生的群签名一定能够通过验证算法。

(2)不可伪造性:非群成员要产生一个通过验证算法的群签名在计算上是不可能的。

(3)匿名性:给定对任意消息的一个群签名,除了群管理员外,决定该签名是由哪个群成员产生在计算上是不可能的。

(4)不可否认性:群管理员总能确定合法签名者的身份。并且群管理员还能向其他实体(比如法官)证明:给定的文档是由哪个成员签署的,同时不会泄露此成员以前或将来可能签署的消息的匿名性。

(5)可追踪性:一个正确的签名可以被群管理员揭开签字者的身份。

(6)抗联合勾结性:任何多个群成员勾结或与群管理员勾结都不能伪造其他群成员的签名。

(7)不可关联性:除群管理员外的任何人不能判定两个不同的签名是否由同一个成员所为。

(8)抗陷害攻击:群中没有任何子集(包含群管理员)能代表群中其他成员签署消息。即群中任何子集都不能"陷害"不属于该子集的其他成员。

(9)防止滥用性:群成员不能使用群成员证书进行除合法的群签名外的任何活动,如果发生误用甚至滥用,安全有效的群签名必须具备追究群成员责任的能力。

向前安全和有效取消是群签名体制所面临的两个重要问题,使用前向安全的概念可以减轻群签名密钥暴露的危害,即即使群签名密钥被泄露,以前产生的群签名依然有效而无须重新签署。前向安全的概念是 R.Anderson 在 1997 年首次提出[7],前向安全签名就是把整个签名有效时间分成若干个时段,在每个签名时段使用不同的签名密钥产生签名,而签名验证公钥则在整个签名有效时间内不变。即使当前签名时段的签名密钥被泄露,也并不影响此签名时段前签名的有效性,从而大大地减少了由于签名密钥泄露而带来的影响。同时,一个理想的群签名体制应该还支持动态的群成员流动,实际中群成员可以加入、离开或在任何时间被群取消。以前的大部分群签名体制可以支持群成员的有效加入,但很少有支持群成员的取消。

最近,文献[8]提出了设计向前安全和有效取消的群签名体制的思想,并设计了一个具有向前安全和可追溯的公开可取消的群签名体制,分析表明,一方面该体制存在错误的模运算以及冗余数据,另一方面该体制存在安全缺陷:群管理员可以伪造通过验证过程的群签名。

2 文献[8]方案介绍

2.1 建立

群管理员 GM 选择 4 个大素数 p,q,p',q',满足 $p=2p'+1$,$q=2q'+1$,设 $n=pq$ 是 RSA 模,取 $G=\langle g\rangle$ 为 Z_n^* 的奇数阶循环子群。GM 随机选择 $x\in Z_n^*$,计算 $y=g^x \bmod n$,存储(p,q,x)为秘密密钥,并把公钥有效的时间分为 T 个时间段公开。$h(x)$为单向无碰撞的 Hash 函数,$(r,s)=PK\{\gamma:y=g^\gamma\}(m)$表示知识签名,GM 公开$(n,g,h(x),y,T)$作为群管理员的公钥信息。

2.2 加入

一个用户 U 要加入群,U 和 GM 之间执行如下协议:

第 1 步 U:随机选择 $x_u\in Z_n^*$ 作为秘密密钥,计算其公钥 $y_u=g^{x_u} \bmod n$ 和知识签名$(r,s)=PK\{\gamma:y=g^\gamma\}(m)$,把$(y_u,(r,s))$发送给 GM。

第 2 步 GM:首先验证签名(r,s),若正确,则接收并存储$(y_u,(r,s))$。

第 3 步 GM:随机选择 $e_u\in Z_n^*$,计算 $c_{u,0}=(g^{e_u}y_u y)^{1/2^T} \bmod n$,秘密发送$(c_{u,0},e_u)$作为 U 的初始群成员资格证书。

第 4 步 U:验证:$(g^{e_u}g^{x_u}y)=c_{u,0}^{2^T} \bmod n$,若成立,将$(c_{u,0},e_u,x_u)$作为自己的群签名密钥。

2.3 演化

假定 U 在时间段 i 拥有群签名密钥$(c_{u,i},e_u,x_u)$,则在时间段 i+1 他的群密钥演变为$(c_{u,i+1},e_u,x_u)$,其中 $c_{u,i+1}=c_{u,i}^2 \bmod n$。

2.4 签名

假定 U 在时间段 i 拥有群签名密钥$(c_{u,i},e_u,x_u)$,他对消息 m 在时间段 i 进行签名,首先随机选择 $k_1\in Z_n^*$,计算:

$u_1=g^{k_1} \bmod n$,$u_2=h(u_1,m)$,

$r_1=c_{u,i}^{u_2} \bmod n$,$r_2=k_1+(e_u+x_u)u_2r_1 \bmod n$

将(u_1,u_2,r_1,r_2,m,i)作为对消息 m 在时间段 i 的签名。

2.5 验证

验证者收到群签名(u_1,u_2,r_1,r_2,m,i),计算:$u_1=g^{r_2}r_1^{-r_1 2^{T-i}}y^{u_2r_1} \bmod n$,$u_2=h(u_1,m)$。如成立,群签名有效。

$w=(ID_C r y_G^{rh(ID_B)}ID_B)^{-d} \bmod n$

2.6 打开

给定一个群签名(u_1,u_2,r_1,r_2,m,i),GM 首先通过验证阶段检查签名的有效性,然后计算:$\eta=1/(u_2r_1)\bmod\varphi(n)$,$u_1'=g^{r_2}r_1^{-r_1 2^{T-i}}\cdot y^{u_2r_1} \bmod n$ 通过验证等式 $y_u=(g^{r_2}/u_1')^\eta/g^{e_u} \bmod n$,确定签名者的身份。

2.7 取消

当一个群成员 U 在时间段 i 用他的群签名密钥$(c_{u,i},e_u,x_u)$对消息 m 进行签名,除了基本的签名过程外,还须做以下工作:U 随机选择 $k_2\in Z_n^*$,计算 $u_3=g^{k_2} \bmod n$ 和 $c=u_3^{c_{u,i}} \bmod n$,将(u_3,c)作为签名的一部分,称为"验证取消展示"。U 通过离散对数知识签名 $PK\{(k_2,c_{u,i}):u_3=g^{k_2}\wedge c=u_3^{c_{u,i}}\}(m)$证明 u_3 和 c 是正确形式。当一个用户 U 在时间段 j 从群中被取消,取消记号为$(c_{u,j},j)$将公布在取消表 CRL 中,假定一个验证者拥有在时间段 i 的签名,他不仅要验证原有的签名部分,还要验证"验证取消展示"(u_3,c)的正确性,当他在 CRL 中查到取消记号$(c_{u,j},j)$,计算 $c_{u,i}$(利用演化算法)并验证等式 $c'=u_3^{c'_{u,i}} \bmod n$。如果等式成立,表明签名者已经取消。

3 对文献[8]方案的密码学分析

3.1 该方案存在错误的模运算

用户 U 在时间段 i 对消息 m 在时间段 i 进行签名时,签名数据 r_2 是通过式 $r_2=k_1+(e_u+x_u)u_2r_1 \bmod n$ 计算出来的,由于这里进行了模 n 的运算,因此,正确的签名数据(u_1,u_2,r_1,r_2,m,i)是不能通过验证过程的,这是因为在计算 $u_1=g^{r_2}r_1^{-r_1 2^{T-i}}y^{u_2r_1} \bmod n$ 时,r_2 处于指数位置,因此 $g^{r_2}=g^{(k_1+(e_u+x_u)u_2r_1)\bmod n}\neq g^{k_1+(e_u+x_u)u_2r_1}$,进一步有:由于在验证过程中用到了

$u_1'=g^{r_2}r_1^{-r_1 2^{T-i}}y^{u_2r_1} \bmod n=g^{(k_1+(e_u+x_u)u_2r_1)\bmod n}r_1^{-r_1 2^{T-i}}y^{u_2r_1}\neq$

$$g^{k_1+(e_u+x_u)u_2r_1}r_1^{-r_1 2^{T-i}}y^{u_2r_1}=g^{k_1} \bmod n=u_1$$

故 $u_1'\neq u_1$,即按照文献[8]方案生成的群签名永远无法通过该方案的验证过程。

实际上计算 r_2 时,只要不进行模 n 运算,即 $r_2=k_1+(e_u+x_u)u_2r_1$,就能保证验证过程的正确性(在以下的安全性分析中假设 $r_2=k_1+(e_u+x_u)u_2r_1$)。

3.2 该方案存在冗余步骤

由于在群签名的验证阶段所用到的 u_1 是通过等式 $u_1=g^{r_2-r_1 2^{T-i}}r_1^{u_2r_1}y^{u_2r_1} \bmod n$ 计算出来的,因此群签名 (u_1,u_2,r_1,r_2,m,i) 中的数据 u_1 实际上是一个冗余数据。

3.3 群管理员的伪造攻击

文献[8]分析了该群签名的安全性和向前安全性,并在其不可伪造性分析中指出即使是群管理员也不能伪造有效的群签名,但该安全结论并不成立,事实上,群管理员可以按照以下步骤伪造一个能够通过验证的群签名:

第 1 步,群管理员:随机选择 $c\in Z_n^*$,计算 $c_{u,0}=(g^c y)^{1/2^T} \bmod n$。在时间段 i+1 令:$c_{u,i+1}=c_{u,i}^2 \bmod n$。

第 2 步,群管理员在时间段 i 对消息 m 进行签名:

首先随机选择 $k_1\in Z_n^*$,计算:

$u_1=g^{k_1} \bmod n, u_2=h(u_1,m)$

$r_1=c_{u,i}^{u_2} \bmod n, r_2=k_1+cu_2r_1$

将 (u_1,u_2,r_1,r_2,m,i) 作为对消息 m 在时间段 i 的签名。

则 (u_1,u_2,r_1,r_2,m,i) 一定能通过群签名的验证过程。这是因为:

$$u_1=g^{r_2-r_1 2^{T-i}}r_1^{u_2r_1}y^{u_2r_1}=g^{k_1+cu_2r_1-r_1 2^{T-i}u_2r_1}g^{k_1}g^{cu_2r_1}c_{u,i}^{-u_2r_1 2^{T-i}}y^{u_2r_1}=$$

$$g^{k_1}y^{-u_2r_1}y^{u_2r_1}=g^{k_1} \bmod n$$

则 $u_2=h(u_1,m)$ 成立。

这样,群管理员就伪造了一个有效的群签名 (u_1,u_2,r_1,r_2,m,i)。

4 结束语

向前安全和有效取消是群签名所面临的两个重要问题,文献[8]提出了设计这类群签名体制的思想,还给出了一种具体的群签名体制。但是,一方面该群签名体制存在错误的模运算及冗余数据,另一方面该群签名体制也是不安全的,群管理员可以生成一个能够通过验证的群签名,该群签名体制存在的这些缺陷都影响了该体制的可执行性和执行效率,如何设计向前安全和有效取消的群签名仍然是值得研究的问题。

参考文献:

[1] Chaum D,Heyst V E.Group signatures[C]//Proceedings of EUROCRYPT'91.Berlin:Springer-Verlag,1991:2257-2651.

[2] Camenishj J,Stadler M.Efficient group signatures for large groups[C]//Proceedings of CRYPTO97.Berlin:Springer-Verlag,1997:410-4241.

[3] Ateniese G,Camensh J,Tsudik M G.A practical and provably secure coalition-resistant group signature scheme[C]//Proceedings of Crypto's 2000.Berlin:Springer-Verlag,2000:255-270.

[4] Ateniese G,Tsudik G.Some open issues and direction in group signature[C]//Proceedings of in Financial Cryptology's 99.Berlin:Springer-Verlag,1999:225-237.

[5] Ateniese G,Joye M,Tsudis G.On the difficulty of coalition-resistant group signature schemes[C]//In the Second Workshop on Security in Communication Network(SCN'99).Berlin:Springer-Verlag,1999:16-17.

[6] Camenish J,Michels M.A group signature scheme based on RSA-variant,Rs-98-27 BRICS[R].University of Aarhus,1998-11.

[7] Anderson R.Two remarks on public key cryptology[C]//Proc of the Fourth ACM Computer and Communication Security,1997.

[8] 陈少真,李大兴.有效取消的向前安全群签名体制[J].计算机学报,2006,29(6):998-1003.

(上接 96 页)

优化问题。采用了最小路集的概念,将原始问题的约束条件大大减少,将原问题分解为两步解决。本文还提出了一个多目标遗传算法解决上述问题。通过实例验证并与 NSGA-II 算法的比较,提出的算法能够很好地解决随机流量网络上流量分配的多目标优化问题。该问题还可以进一步扩展,比如假设网络中有多种类型的流在流动时如何进行流量分配优化,或者当节点有存储功能时如何控制资源流。

参考文献:

[1] Lin Yi-Kuei.Evaluate the performance of a stochastic-flow network with cost attribute in terms of minimal cuts[J].Reliability Engineering & System Safety,2006,91(5):539-45.

[2] Yan Zhou,Qian Meng.Improving efficiency of solving d-MC problem in stochastic-flow network[J].Reliability Engineering & System Safety,2007,92(1):30-39.

[3] Kobayashi K,Yamamoto H.A new algorithm in enumerating all minimal paths in a sparse network[J].Reliability Engineering and System Safety,1999,65:11-15.

[4] Lin Yi-Kuei.Study on the system capacity for a multicommodity stochastic-flow network with node failure[J].Reliability Engineering & System Safety,2002,78(1):57-62.

[5] Yeh Weiwe-Chang.A simple MC-based algorithm for evaluating reliability of stochastic-flow network with unreliable nodes[J].Reliability Engineering & System Safety,2004,83(1):47-55.

[6] Lin Yi-Kuei.Using minimal cuts to study the system capacity for a stochastic-flow network in two-commodity case[J].Computers & Operations Research,2003,30(11):1595-1607.

[7] Hsieh Chung-Chi,Lin Ming-Hsien.Reliability-oriented multi-resource allocation in a stochastic-flow network[J].Reliability Engineering & System Safety,2003,81(2):155-161.

[8] Lin Yi-Kuei.Extend the quickest path problem to the system reliability evaluation for a stochastic-flow network[J].Computers & Operations Research,2003,30(4):567-575.

[9] Lin Yi-Kuei.Two-commodity reliability evaluation for a stochastic-flow network with node failure[J].Computers & Operations Research,2002,29(13):1927-1939.

[10] Lin Yi-Kuei.An algorithm to evaluate the system reliability for multicommodity case under cost constraint[J].Computers & Mathematics with Applications,2004,48(5-6):805-812.

[11] Al-Ghanim A M.A heuristic technique for generating minimal paths and cut sets of a general network[J].Computers and Industrial Engineering,1999,36:45-55.

[12] Deb K,Pratap A,Agarwal S,et al.A fast and elitist multi-objective genetic algorithm:NSGA-II[J].IEEE Transactions on Evolutionary Computation,2006,6(2):182-197.