一个群签名方案的安全性分析与改进

张兴兰

(北京工业大学计算机学院 北京 100124)

摘 要 最近陈少真等人提出了一种具有前向安全和有效撤销成员性质的群签名方案,该方案通过在签名中增加一个验证取消展示实现对成员的撤销。分析了陈方案设计的缺陷,给出了一种改进的成员撤销算法。在强RSA和离散对数假设下,证明了改进方案的有效性和安全性。

关键词 群签名,成员撤销,可跟踪性

中图法分类号 TP309 **文献标识码** A

Security Analysis and Improvement of a Group Signature Scheme

ZHANG Xing-lan

(College of Computer Science, Beijing University of Technology, Beijing 100124, China)

Abstract Recently, Chen, et al. presented a membership revocation algorithm of a group signature scheme, verifiable revocation procedure was invoked to show whether a member is revoked. By analyzing Chen's design, a limitation was pointed. At the same time, another improved membership revocation algorithm was proposed. Under the assumption of stronger RSA and Discrete Logarithm problem, the efficiency and the security of the new group signature scheme were proven.

Keywords Group signature, Membership revocation, Traceability

1 引言

群数字签名概念由 D. Chaum 和 E. van Heyst[1]首先提出。在一个群签名方案中,群成员可以代表群体进行匿名签名,而验证者并不能确定其个体身份。当发生争执时,群管理员可以打开签名来揭露签名人的个体身份,使签名人不可否认自己的签名。这些安全性质,使群签名方案在管理、军事及经济等领域有着许多应用的前景,受到研究者的广泛关注。但直到2000年,G. Ateniese 等人才提出了一个比较好的群签名方案(简称为 ACJT 方案[4]),使群签名方案在安全性和有效性方面取得了重大进展。ACJT 方案的成员加入协议是关于新成员所选取的秘密值在统计上的零知识证明,且已证明可以抵抗自适应的攻击者所发动的联合攻击。然而,ACJT 方案本身并没有提供成员撤销的解决方法。为了适应群组的动态变化性,许多研究者对群成员撤销问题进行了研究[2,3,5,6]。

最近,陈少真等人[7]分析了成员撤销方法的设计原则,提出一个新的撤消方法——验证取消展示。该方法通过对部分签名密钥做零知识证明,然后用取消列表中的值进行合法性验证。本文指出其验证取消展示的密钥由于没有和签名进行绑定,成员撤销方法实质上是无效的,并使群签名方案失去可跟踪性和抗陷害性。基于此,本文否定了陈方案关于成员撤销的设计方法2,并基于成员的签名密钥与群公钥之间的整除关系改进了群签名的成员撤销算法。在强 RSA 假设下,证明了改进方案的有效性和安全性。

2 陈少真等人的方案

本节对陈少真等人提出的群签名方案进行必要的描述。陈方案仅存在两个实体:群管理员和群成员。群管理员(GM)负责建立整个系统,为每个群成员生成证书,并在必要的时候打开一个合法的签名,确定签名者的身份。

2.1 系统建立

GM 随机地秘密选择 l_p 比特的素数 p',q'使得 $p=2p'+1$,$q=2q'+1$ 仍为素数。令 $n=pq$ 为 RSA 的模。取 $G=\langle g\rangle$ 为 Z_n^* 的奇数阶循环群。GM 随机地秘密选择 $x\in Z_{p'q'}$,计算 $y=g^x \bmod n$,存储(p,q,x)作为秘密密钥,y 为 GM 的公开密钥。GM 将系统的有效时间划分为 T 个时间段。设 $H(x)$为一个单向无碰撞的 Hash 函数。最后,GM 公布$(n,g,H(x),y,T)$作为其公钥信息。

2.2 加入

如果成员 U 想加入群,U 和 GM 之间执行一个交互协议。首先成员 U 选择一个随机值 $x_u\in Z_n^*$ 作为自己的秘密密钥,计算公钥 $y_u=g^{x_u} \bmod n$ 和知识签名$(r,s)=PK\{x_u:y_u=g^{x_u} \bmod n\}(m)$,发送$(r,s,y_u)$给 GM。GM 收到签名信息后,验证签名的有效性。如果通过验证,GM 随机选择一个不同的素数 $e_u\in_R Z_n^*$,计算 $C_{u,0}=(g^{x_u}y_u y)^{\frac{1}{2^T}} \bmod n$,并将$[C_{u,0}$,

到稿日期:2009-06-03 返修日期:2009-09-07 本文受国家高新技术研究发展计划八六三项目(2006AA01Z440),国家重点基础研究发展计划九七三项目(2007CB311100)资助。

张兴兰(1970—),女,博士,副教授,CCF 会员,研究方向为密码学与可信计算,E-mail:zhangxinglan@bjut.edu.cn。

e_u]作为初始证书发送给成员 U。成员 U 验证 $C_{p,0}{}^{2^T}=g^{e_u}g^{x_u}y \bmod n$，如果等式成立，则将$(C_{u,0},e_u,x_u)$作为自己的签名密钥。

2.3 演化

成员 P 通过密钥更新算法 $C_{u,i}=C_{u,i-1}^2 \bmod n$，计算任何时间段 $j(j\geqslant 1)$的签名密钥$(C_{u,j},e_u,x_u)$。显然 $C_{u,i}{}^{2^{T-j}}=g^{e_u}g^{x_u}y \bmod n$ 始终成立。

2.4 签名

设在时间段 j 成员 U 的密钥为$(C_{u,j},e_u,x_u)$，对消息 m 签名过程为：随机选取 $k\in Z_n^*$，计算 $u_1=g^k \bmod n$，$u_2=H(u_1,m)$，$r_1=C_{u,j}{}^{u_2} \bmod n$，$r_2=k+(e_u+x_u)u_2r_1 \bmod n$。签名为$(j,u_1,u_2,r_1,r_2)$。

2.5 验证

对签名(j,u_1,u_2,r_1,r_2)，验证者计算 $u_1=g^{r_2}r_1^{-r_1{}^{2^{T-j}}}y^{u_2r_1} \bmod n$，验证 $u_2=H(u_1,m)$。如果通过验证，则接受此签名。

2.6 打开

对一个通过验证的签名(j,u_1,u_2,r_1,r_2)，GM 计算 $y_u=(g^{r_2}/u_1)^{1/r_1u_2}(1/g^{e_u}) \bmod n$，确定签名者的身份。

2.7 取消

取消过程是通过扩展上述签名体制实现的。当一个群成员 U 在时间段 j 用他的群签名密钥$(C_{u,j},e_u,x_u)$签署一个消息时，除了一个基本的签名过程外，U 还做以下工作：U 随机选取 $k_2\in Z_n^*$，计算 $u_3=g^{k_2} \bmod n$，$c=u_3^{C_{u,j}} \bmod n$，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 $PK\{(k_2,C_{u,j}):u_3=g^{k_2} \bmod n \wedge c=u_3^{C_{u,j}} \bmod n)\}(m)$，证明$(u_3,c)$为正确的形式。若一个成员 U 在时间段 j 从群中取消，取消记号$(C_{u,j},j)$将公布在取消表 CRL 中。假定一个验证者拥有成员 U 在时间段 j 的签名(j,u_1,u_2,r_1,r_2)及验证取消展示(u_3,c)，他不仅要验证原有的签名部分，而且要验证“验证取消展示”(u_3,c)的正确性。于是他在 CRL 中查到取消记号$(C_{u',i},i)$，$i\leqslant j$(为了检查签名者是否已被取消，验证者利用演化算得到时间段 j 的签名密钥 $C_{u,j}$)，并验证等式 $c'=u_3^{C_{u',j}} \bmod n$。如果等式成立，则表明签名已被取消。

3 安全性分析

上述方案的安全性是基于强 RSA 和离散对数问题假设的。下面给出对上述方案的攻击形式，从而证明这些基本假设对该方案是无效的。

为了说明攻击的有效性，首先给出一个基本的事实：如果一个合法成员 U 仅仅泄露了密钥 $C_{u,j}$，根据强 RSA 假设和离散对数假设，攻击者计算 U 的其他密钥成分(x_u,e_u)是困难的。

1)攻击 1：不可撤销性

一个攻击者 U'(可能是被撤销成员本人，也可能是其他攻击者)任意选择一个 $C<n$，且 $C\notin\{C_{u,j}\mid(C_{u,j},j)\in CRL,0\leqslant j\leqslant T\}$。$U'$一定可以构造一个基于离散对数的知识签名 $PK\{(k_2,C_{u,j}):u_3=g^{k_2} \bmod n\wedge c=u_3^C \bmod n)\}(m)$来证明$(u_3,c)$为正确的形式，即$(u_3,c)$作为签名的“验证取消展示”部分不能检验出签名的合法性。因此，原方案的撤销算法无效。

2)攻击 2：攻击者得到合法用户时间段 i 的一个签名，就可以任意构造该用户在时间段 i 的合法签名。

设攻击者获得一个合法用户时间段 i 的一个签名(i,u_1,u_2,r_1,r_2)，与上述攻击相同，选择任意一个满足条件的 $C(<n)$计算出签名的“验证取消展示”(u_3,c)。此时，(i,u_1,u_2,r_1,r_2)和新计算的(u_3,c)一起作为一个完整的签名一定可以通过有效性和合法性检验，但该签名并非合法用户签发。因此，原方案破坏了群签名的可跟踪性和抗陷害性。

特例：设一个被撤销成员 U'收买某合法成员 U，得到其密钥 $C_{u,j}$。因为 U 知道，即使 U'知道了 $C_{u,j}$也不可能伪造他的签名，从而 U 泄露密钥所付出的代价是很低的。如果 U'用自己的签名密钥完成签名部分，而用合法成员的 $C_{u,j}$计算验证取消展示，则所得签名是可以通过检验的。

4 一个改进方案

基于以上分析，本节给出一个改进方案。在改进的方案中将撤销算法中所使用的密钥与签名过程中的密钥进行了绑定。设系统建立和打开算法都与原方案同。为了节约篇幅，下面只给出群签名方案的成员加入与撤销、签名和验证算法。

成员加入与撤销：假设 $E_{\text{add}}:=\{G_1,G_2,\cdots,G_m\}$为当前群成员的集合。群管理者除了为新加入的成员计算其群证书外，还计算一个群公钥 $E=e_{G_1}\cdots e_{G_m}$，其中 e_{G_i}是对应成员 G_i 证书中的素数。在系统运行的某个时间段 t，不妨设 E'是当时所有被撤销成员的 e_{G_j}的乘积，而 E''是当时所有加入成员的 e_{G_j}的乘积。群管理者为新加入成员计算群证书，并通过计算 $E:=E''E/E'$实时更新群公钥 E(在一个公开的目录上公布最新的 E 和更新的时间段 t)。

签名：一个合法群成员 U 想对消息 m 签名，则必须做两个证明：1)必须证明拥有成员证书$(C_{u,j},e_u,x_u)$，这可以通过原方案得到；2)通过公共目录得到当前最新的公开值 E，并证明成员证书$(C_{u,j},e_u,x_u)$中的 e_u 是 E 的因子。下面是新的签名过程：

1)计算 a，其中 $ae_u=E$；

2)随机选取 $k,k_1\in Z_n^*$，计算

$u_1=g^k \bmod n$，$u_2=H(u_1,m)$，$u_3=u_1^a g^{k_1} \bmod n$，$r_1=C_{u,j}^{u_2} \bmod n$

$r_2=k+(e_u+x_u)u_2r_1$，$r_3=a(k+x_uu_2r_1)+k_1$，$r_4=k_1(e_u+x_u)u_2r_1$

签名为$(j,m,u_1,u_2,u_3,r_1,r_2,r_3,r_4)$。

验证：找到与时间段对应的群公钥 E，计算 $u_1=g^{r_2}r_1^{-r_1{}^{2^{T-j}}}y^{u_2r_1} \bmod n$。验证 $u_2=H(u_1,m)$和 $u_3{}^{r_2}=u_1^{Eu_2r_1+r_3}g^{r_4} \bmod n$ 的正确性。如果通过验证，则接受签名；否则，签名无效。

第一个验证关系与原方案同，用来证明拥有成员证书$(C_{u,j},e_u,x_u)$。第二个验证关系是用来证明签名者知道 a 使得 $ae_u=E$ 成立。

在上述方案中，群管理者只需做一次整数除法运算就可以撤销一个成员，且签名和验证算法与群成员个数和被撤销成员的个数无关。此外，由于改进方案的群公钥长度与被撤销成员个数无关，因此管理者可以自由地实施对成员的撤销而不影响方案的执行效率。

(下转第 90 页)

研究[J]. 计算机科学,2009,36(4):112-115
[9] 窦军,曾华燊,汪海鹰. NGI/NGN 体系结构及其服务质量保障机制研究[J]. 计算机科学,2008,35(3):31-33
[10] Dou Jun, Zeng Huaxin, Wang Haiying. Single User-Plane Architecture and its QoS Provisioning Mechanisms in Signaling and Management (S&M) Planes[C]// The 5th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT 04). Singapore, Dec. 2004:429-440
[11] 赵君,高雨. SUPANET 中 QoS 协商流程研究[J]. 计算机科学,2004,31(8 增刊):21-24
[12] Zeng Huaxin, Gao Yu, Xia Yu. On NGN architecture and evolution strategy[C]// First ITU-T Kaleidoscope Academic Conference-Innovations in NGN: Future Network and Services. Geneva: IEEE press, May 2008:337-342
[13] Gao Yu, Zeng Huaxin. A New Mechanism supporting QoS and Mobility in SUPANET[C]// 2008 International Symposium on Computer Science and Computational Technology (ISCSCT 2008). Vol. 1, Shanghai: IEEE press, December 2008:771-776
[14] Johnson D, Perkins C, Arkko J. Mobility Support in IPv6 RFC 3775 [DB/OL]. [2004-6-10]. http://www.ietf.org/rfc/rfc3775.txt
[15] Gao Yu, Zeng Huaxin, Wang Haiying. Research on Mobility Management in DDQP Mechanism of SUPANET[C]// 2009 International Conference on Communications and Mobile Computing (CMC 2009). Kunming: IEEE press, January 2009:216-221

(上接第 76 页)

5 改进方案的安全性和性能分析

在 BSZ 模型中[5],将理想的动态群签名方案应满足的安全特性归纳为 4 点:1)正确性。群成员所生成的签名验证有效,打开算法能正确地揭示签名者的身份并且给出可接受的证明;2)匿名性。对于一个指定消息的签名,如果敌手不能判定是由他所选择的两个成员中哪一个成员所签署,则方案满足匿名性;3)可跟踪性。敌手若不能生成一个 GM 就不能揭示其身份的签名,或者 GM 可以揭示其身份但是不能给出一个可接受的证明;4)抗陷害性。如果一个成员没有生成某个签名,敌手就不能给出一个证明来认定该成员生成了此签名。基于此安全模型,对改进方案的安全性分析如下。

正确性:$u_1=g^{r_2}r_1^{-r_1 2^{T-j}}y^{u_2 r_1} \bmod n$ 的正确性由原方案保证。而 $u_3^{r_2}=u_1^{[k+(e_u+x_u)u_2r_1]}g^{k_1[k+(e_u+x_u)u_2r_1]}=u_1^{Eu_2r_1+a[k+x_uu_2r_1]+k_1}u_1^{-k_1}g^{k_1[k+(e_u+x_u)u_2r_1]}=u_1^{Eu_2r_1+a[k+x_uu_2r_1]+k_1}g^{-kk_1}g^{k_1[k+(e_u+x_u)u_2r_1]}=u_1^{Eu_2r_1+r_3}g^{r_4} \bmod n$。

匿名性:首先,在强 RSA 问题和离散对数假设下,从两个不同的签名出发,判断密钥 e_u 的相关性等同于求解离散对数问题 $C_{p,0}^{2^T}=g^{e_u}g^{x_u}y \bmod n$,判断 $C_{u,j}$ 的相关性等同于求解强 RSA 问题 $C_{u,i}=C_{u,i-1}^2 \bmod n$。其次,由于随机值 k_1 和 k 分别通过 $r_2=k+(e_u+x_u)u_2r_1$,$r_4=k_1(e_u+x_u)u_2r_1$ 和 $r_3=a(k+x_uu_2r_1)+k_1$ 对密钥成分 (e_u+x_u) 和 x_u 进行了随机化,任何对密钥成分 (e_u+x_u) 和 x_u 的求解或比较也是不可行的。因此,在改进方案中,不仅签名 $(u_1,u_2,u_3,r_1,r_2,r_3,r_4)$ 的每一成分都与随机数进行了绑定,而且任何对密钥成分的求解和比较是不可行的,从而改进方案的匿名性仍然成立。

可跟踪性:由于打开算法与原方案同,方案的可跟踪性仍然成立。

抗陷害性:在离散对数和强 RSA 问题假设下,由方案的匿名性求解签名密钥是不可行的。而如果签名密钥是安全的,攻击者选择满足条件的参数 (r_1',r_2',r_3',r_4'),设 $u_1'=g^{r_2'}r_1'^{-r_1'2^{T-j}}y^{u_2'r_1'} \bmod n$,$u_3'^{r_2'}\equiv u_1'^{Eu_2'r_1'+r_3'}g^{r_4'} \bmod n$,$u_2'=H(u_1',m)$。在离散对数和强 RSA 问题假设下,求解 u_1',u_2',u_3' 是不可行的,因此攻击者不能伪造一个合法的群签名。

可撤销性:(u_3,r_3,r_4) 可以作为"e_u 整除当前 E 值"的知识证明。由于验证 (u_3,r_3,r_4) 的合法性密钥 e_u 和签名使用的密钥 e_u 是一致的(利用了同一参数 r_2),并且两个验证关系相互绑定,如果成员 U 被撤销,则他此后的签名也只能使用自己的密钥成分 e_u 做合法性检验,而此时的密钥 e_u 一定不满足 $ae_u=E$。

结束语 在大量的群签名方案的设计中,成员撤销问题的解决备受关注。本文分析了陈少真等人提出的群签名方案中成员取消算法的缺陷,否定了文献[7]给出的第 2 种群成员撤销方法,并在陈方案的基础上给出了一个可撤销成员的改进方案。新方案中群管理者只需做一次除法运算就可以撤销一个成员,而成员密钥不需要改变,且签名和验证过程独立于现有的成员个数和撤销成员个数。因此,改进方案克服了原方案存在的安全缺陷,提高了群签名协议的执行效率,是一个实用的群签名方案。

参 考 文 献

[1] Chaum D, van Heyst E. Group signatures[C]// Advances in Cryptology—EUROCRYPT '91. Berlin: Springer-Verlag, 1991:257-265
[2] Ateniese G, Tsudik G. Some open issues and new directions in group signature schemes[C]// Financial Cryptography (FC'99). Berlin: Springer-Verlag, 1999:196-211
[3] Song D X. Practical forward secure group signature schemes[C]// Proc. of the 8th ACM Conf on Computer and Communications Security (CCS 2001). New York: ACM Press, 2001:225-234
[4] Atenies G, Camenisch J, Joye M, et al. A practical and provably secure coalition-resistant group signature scheme[C]// Advances in Cryptology—CRYPTO 2000. Berlin: Springer-Verlag, 2000:255-270
[5] Bellare M, Shi H, Zhang C. Foundations of group signatures: research interests are cryptography and the case of dynamic groups[C]// CT2RSA 2005. Berlin: Springer-Verlag, 2005:136-153
[6] Camenisch J, Lysyanskaya A. Dynamic accumulators and application to efficient revocation of anonymous credentials[C]// Proc. of Crypto 2002. Berlin: Springer Verlag, 2002:61-76
[7] 陈少真,李大兴. 有效取消的向前安全群签名体[J]. 计算机学报,2006,29(6):998-1003
[8] 陈泽文,王继林,黄继武,等. ACJT 群签名方案中成员撤消的高效实现[J]. 软件学报,2005,16(1):151-157