对存在特权集的门限群签名方案的安全性分析

王勇兵,王际川
WANG Yong-bing,WANG Ji-chuan

河北师范大学 附属民族学院,石家庄 050091
Nationalities College of Hebei Normal University,Shijiazhuang 050091,China
E-mail:wyb723@yahoo.com.cn

WANG Yong-bing,WANG Ji-chuan.Cryptanalysis of threshold group signature schemes with privilege subsets.Computer Engineering and Applications,2010,46(9):80-82.

Abstract: Feng Deng-guo suggests a problem called threshold group signature scheme with privilege.In 2005,Chen Wei-dong presented a group of threshold group signature schemes with privilege subsets.Through cryptanalysis of it,KAC or KAC with others can froge signature,and it is not provided with distinguishability and traceability.Furthermore,it can not resist conspiratorial attack.An improved scheme is proposed and the security drawbacks of original scheme are overcome.In the new scheme,the interests of signer are protected and storage space is reduced,so it is more secure and efficient.

Key words: threshold group signature;privilege subsets;frogery attack;conspiratorial attack

摘 要:针对冯登国提出的"存在特权集的门限群签名"问题,2005 年,陈伟东提出了一类存在特权集的门限群签名方案(C-F 方案),分析发现它容易受到可信密钥认证中心发起的三种伪造攻击,不具有签名的可区分性和事后身份追踪的特性,也无法抵抗内部成员的合谋攻击。提出了一种改进方案,新方案克服了 C-F 方案的安全隐患,保护了签名人的合法权益,节省了系统存储空间,是一个安全有效的签名方案。

关键词:门限群签名;特权集;伪造攻击;合谋攻击
DOI:10.3778/j.issn.1002-8331.2010.09.023 **文章编号**:1002-8331(2010)09-0080-03 **文献标识码**:A **中图分类号**:TN918

1 概述

随着计算机知识的普及和宽带网的深入,信息安全日益成为人们关注的问题。数字签名是一种被广泛应用、提供认证服务的有效机制,是实现信息安全的重要手段。门限群签名是一种特殊的数字签名,最早是由 Desmedt 和 Frankel[1]于 1991 年提出,群成员中任意 t 个可以代表群组进行数字签名,而少于 t 个则不能生成有效的群签名。近年来此方面的研究很多,但是它们均有一个局限性:各签名方的权限是等同的。在第十届全国青年通信学术会议上,苗澎锋提出了一个有特殊成员的(t,n)门限签名方案[2],文献[3]指出它是不安全的,容易受到 3 种伪造攻击,并提出了相应的改进方案。然而,文献[2-3]签名成员只局限于一个特权者, 不适合具有多个特权者的签名方案的应用。石怡等[4]针对实际生活中签名人的权限不等的问题,提出了一种新型的门限群签名方案,多个特权签名人可以作为一个特权子集参与签名。文献[5]指出文献[4]的方案并不十分理想,协议过分复杂,签名长度较长,而且存在安全隐患,利用成熟的单签名方案和双重秘密分割的方法设计了一类存在特权集的门限群签名方案。文献[6]指出文献[5]的方案在设计时存在一个错误, 签名过程过于简单和确认签名方的身份算法效率不高,并提出了一个改进方案。然而文献[5-6]的安全性仍然很脆弱,容易受到密钥认证中心发起的 3 种伪造攻击,签名不具有可区分性和事后身份追踪的特性, 也无法抵抗内部成员的合谋攻击。从保护签名方的合法权益出发,提出了一种改进方案,新方案克服了文献[5-6]方案的安全隐患,保护了签名人的合法权益,节省了系统存储空间,是一个安全有效的签名方案。

2 C-F 方案简介

文献[5]利用 EIGmal 类型签名方案,结合门限群签名方案,采用对秘密密钥"双重"分割的方法,设计了一个$(t_1,n_1;t,n)$门限群签名方案和一个具有消息恢复性质的$(t_1,n_1;t,n)$门限群签名方案,安全性分析发现两个方案都是不安全的,下面仅对第一个方案作如下简述并对其安全性作详细分析,参与者包括可信中心 KAC,n 个签名人组成的群体 G,签名服务机构 SC 和特权子集 G_1;整个方案由系统设置、群密钥及秘密密钥碎片产生、门限群签名产生、群签名的验证和事后身份追踪 4 个部分。方案设计过程如下:

2.1 系统设置阶段

KAC 选择两个安全素数 p,q,满足 $q|p-1$;秘密随机选择两

基金项目:河北师大附属民族学院科研基金资助项目。
作者简介:王勇兵(1981-),男,助教,研究方向为密码学与信息安全;王际川(1976-),男,讲师,研究方向为计算机科学与技术。
收稿日期:2009-08-07 **修回日期**:2009-10-09

个次数分别为(t-1)和(t_1-1)的多项式$f(x)$,$g(x)$;取α为F_q的本原元,公开(p,q,α)和x_i,$y_i\in_R Z_q[x]$。

2.2 群密钥及秘密密钥碎片产生

KAC产生群密钥:$(f(0)+g(0))\bmod q$,群公钥:$z=\alpha^{(f(0)+g(0))\bmod q}\bmod p$,秘密钥碎片分发:如果$i$是普通用户,则得到对应秘密碎片$f(x_i)$,并由KAC公开$z_i=\alpha^{\lambda_i f(x_i)}\bmod p$;如果$i$是特权用户,则得到对应碎片$f(x_i)$,$g(y_{ij})$公开$z_i=\alpha^{\lambda_i f(x_i)+u_i g(y_{ij})\bmod q}\bmod p$,其中$\lambda_i$,$u_i$是Lagrange恢复系数。

2.3 门限群签名的产生和身份追踪

设t个人参加签名,恰为1,2,…,t,被签署的消息为m。$\forall i$秘密随机选取$k_i\in Z_p^*$,计算$r_i=\alpha^{k_i}\bmod p$,并广播r_i,每个用户i可以计算$r=\prod_{i=1}^{t} r_i\bmod p$,若$i$是普通用户,则计算$s_i=(f(x_i)\lambda_i h(m)-k_i r)\bmod q$;若$i$是特权用户,则计算$s_i=(f(x_i)\lambda_i h(m)+g(y_{ij})u_i h(m)-k_i r)\bmod q$,$s_i$被发送给签名服务机构SC。SC验证$\alpha^{s_i}r_i^{r}=z_i^{h(m)}$,若成立,则是合法的单签名。如果SC收到所有$s_i$后计算$s=\sum_{i=1}^{t} s_i\bmod q$,输出($r$,$s$)作为消息$m$的群签名。SC根据需要来追踪签名人的身份。

3 C-F方案安全性分析

(1)可信密钥认证中心(KAC)权力过大。在现实中找到一个义务和权力不对称的完全理想化的可信中心是很难的,即使用网络中的服务器代替,虽然可以代避免人为因素的操作,但它很容易成为通信的瓶颈和攻击的焦点,一旦服务器瘫痪或被攻破,系统将完全丧失安全性。签名的密钥完全依赖于KAC,没有加入签名人的任何相关信息,无法抵抗KAC发起的各种伪造攻击,不能保护签名人的利益。

定理1 KAC可以冒充签名人生成有效签名。KAC随机选择t个$k_j\in Z_p^*(j=1,2,\cdots,t)$,计算$r_j=\alpha^{k_j}\bmod p$,并计算$r=\prod_{j=1}^{t} r_j\bmod p$,并计算$t_1$个特殊用户的签名$s_i=(f(x_i)\lambda_i h(m)+g(y_{ij})u_i h(m)-k_i r)\bmod q$和$t-t_1$个普通用户的签名$s_i=(f(x_i)\lambda_i h(m)-k_i r)\bmod q$,将$s_i$发送给SC,很明显$s_i$可以通过$\alpha^{s_i}r_i^{r}=z_i^{h(m)}$验证。

定理2 KAC和SC联合可以冒充签名人签名。伪造可以分成两种情况:一是KAC和SC共同参与伪造签名;二是KAC可以将签名人密钥$f(x_i)$和$g(y_{ij})$泄露给SC,SC单独实施伪造签名。这两种伪造攻击具体过程类似定理1的攻击。

定理3 KAC可以和任何一个签名人一起伪造有效签名。KAC可以把密钥碎片$f(x_i)$,$g(y_{ij})$与任一签名人共享,这样KAC就可以和签名人一起产生有效签名。若签名人是特权用户,方案不具有门限签名的特性;若签名人是普通用户,方案不具有门限签名的特性,也缺少特权用户的参与。

(2)SC追踪签名人的身份是不可行的。SC要实现对签名人身份的追踪,在收到每一个单签名s_i时就必须将s_i与用户i的一些信息对应起来存入数据库,为事后追踪签名人身份,用户信息需要长期保存,这样数据库将越来越大,必将耗费大量的存储空间和维护成本。另外,用户i的签名密钥$f(x_i)$和$g(y_{ij})$中没有加入签名人的任何信息,完全由KAC掌握,KAC可以单独或联合其他人伪造有效签名,这样SC无法辨认KAC冒充的签名和签名人的正常签名,因此,SC将s_i确定为用户i的签名是不合理的。

(3)方案无法抵抗内部成员的合谋攻击。参与签名的t个人可以一起出示自己的密钥碎片,根据$\sum_{i=1}^{t} f(x_i)\lambda_i=f(0)$和$\sum_{i=1}^{t_1} g(y_{ij})u_i=g(0)$联合恢复出群私钥$f(0)+g(0)\bmod q$可以冒充其他成员产生任何消息的签名。具体操作如下:选取$k_i\in Z_p^*$,计算$r_i=\alpha^{k_i}\bmod p$,并计算$r=\prod_{i=1}^{r} r_i\bmod p$;对任何消息$m'$可以计算签名$s=h(m')(f(0)+g(0))-r\sum_{i=1}^{t} k_i$,得到消息$m'$的签名($r$,$s$),很显然($r$,$s$)可以通过$\alpha^{s}r^{r}=z^{h(m')}$验证,因此,($r$,$s$)为消息$m'$的有效签名。

4 C-F方案的改进

改进方案在签名私钥中嵌入了签名人的私钥,保护了签名人的利益;并且签名中增加了身份识别函数,使得事后身份追踪更具有可操作性。每个签名人$i(i=1,2,\cdots,n)$选取$t_i\in_R Z_q^*$作为私钥,对应的公钥为$T_i=\alpha^{t_i}\bmod p$,x_i为签名人i的化名身份。整个方案群密钥及秘密密钥碎片分发、门限群签名和群签名的验证和事后追踪3个阶段组成。

4.1 群密钥及秘密密钥碎片分发

KAC产生群密钥:$(f(0)+g(0))\bmod q$,群公钥:$z=\alpha^{(f(0)+g(0))\bmod q}\cdot\bmod p$,并选择随机控制参数$d\in Z_q^*$,如果$i$是普通用户,则得到秘密碎片$w_i=(f(x_i)-d)\bmod q$,并由KAC公开$z_i=\alpha^{\lambda_i f(x_i)}\bmod p$;如果$i$是特权用户,则得到碎片$w_i=(f(x_i)-d)\bmod q$和$v_{ij}=(g(y_{ji})-d)\bmod q$,公开$z_i=\alpha^{\lambda_i f(x_i)+u_i g(y_{ij})\bmod q}\bmod p$,$D=\alpha^{d}\bmod p$,其中$\lambda_i$,$u_i$是Lagrange恢复系数可以公开计算。

4.2 门限群签名

(1)每个签名人i秘密随机选取$k_i\in Z_p^*$,计算$r_i=\alpha^{k_i}\bmod p$,并广播r_i,每个用户i可以计算$r=\prod_{i=1}^{t} r_i\bmod p$以及$T=\prod_{i=1}^{t} T_i\bmod p$;

(2)若i是普通用户,则计算$s_i=((w_i\lambda_i+t_i)h(m\parallel r\parallel T)-k_i r)\bmod q$;若$i$是特权用户,则计算$s_i=((w_i\lambda_i+v_{ij}u_i+t_i)h(m\parallel r\parallel T)-k_i r)\bmod q$,用户发送($r$,$s_i$,$T$)给签名服务机构SC;

(3)SC验证$\alpha^{s_i}r_i^{r}D^{\lambda_i h(m\parallel r\parallel T)}=(z_i T_i)^{h(m\parallel r\parallel T)}$,若验证成立,则接受签名,并计算$s=\sum_{i=1}^{t} s_i\bmod q$和签名人身份识别多项式$h(x)=\prod_{i=1}^{t}(x-x_i)$,输出($r$,$s$,$T$,$h(x)$)作为消息$m$的群签名。

4.3 群签名的验证和事后追踪

验证人收到签名(r,s,T,$h(x)$)后,验证$\alpha^{s}r^{r}D^{\sum_{i=1}^{t}\lambda_i h(m\parallel r\parallel T)}=(zT)^{h(m\parallel r\parallel T)}$,若验证等式成立,则($r$,$s$,$T$,$h(x)$)为消息$m$的有效签名,否则无效。事后如果出现签名纠纷,需要知道哪些人参加了签名,只需要将签名人i的化名身份x_i代入身份识别函数$h(x)=\prod_{i=1}^{t}(x-x_i)$中,若$h(x_i)=0$,则签名人$i$参与了签名,这样实现了事后对实际签名人的追踪。

5 方案分析

5.1 正确性分析

定理 4 SC 可以通过 $\alpha^{s_i r_i} D^{\lambda_i h(m\|r\|T)}=(z_i T_i)^{h(m\|r\|T)}$ 验证单签名 s_i 的有效性。

证 $\alpha^{s_i r_i} D^{\lambda_i h(m\|r\|T)}=\alpha^{(w_i\lambda_i+t_i)h(m\|r\|T)-k_i r}\alpha^{k_i r}\alpha^{d\lambda_i h(m\|r\|T)} \bmod q=\alpha^{(f(x_i)\lambda_i+t_i)h(m\|r\|T)} \bmod q=(z_i T_i)^{h(m\|r\|T)} \bmod q$。

定理 5 验证人可以由 $\alpha^{s r} D^{\sum_{i=1}^{t}\lambda_i h(m\|r\|T)}=(zT)^{h(m\|r\|T)}$ 来验证门限群签名 $(r,s,T,h(x))$ 的有效性。

证 $\alpha^{s r} D^{\sum_{i=1}^{t}\lambda_i h(m\|r\|T)}=\alpha^{\sum_{i=1}^{t}s_i}\left(\prod_{i=1}^{t} r_i\right)^{r} D^{\sum_{i=1}^{t}\lambda_i h(m\|r\|T)}=\left(\prod_{i=1}^{t} z_i T_i\right)^{h(m\|r\|T)}=\left(\alpha^{f(0)+g(0)}\prod_{i=1}^{t} T_i\right)^{h(m\|r\|T)}=(zT)^{h(m\|r\|T)}$。

5.2 安全性分析

(1)方案可以抵抗 KAC 发起的各种伪造攻击。C-F 方案中 KAC 权力过大,签名密钥完全依赖于它,这是 C-F 方案不安全的根源,在改进方案中,签名密钥依赖于 KAC 分发的秘密碎片 w_i,v_{ij} 和签名人的私钥 t_i,嵌入了签名人的信息,KAC 要伪造签名虽然 w_i,v_{ij} 已知,还必须知道签名人的私钥 t_i,而由 $T_i=\alpha^{t_i} \bmod p$ 计算出 t_i 将面临离散对数问题,因此 KAC 权力得到了一定的限制,无法伪造有效签名,这也充分保护了签名人的权益。

(2)方案可以抵抗内部成员的合谋攻击。t 个人一起出示自己的密钥碎片,根据拉格朗日插值公式无法恢复出群私钥 $(f(0)+g(0)) \bmod q$,因为 $w_i=(f(x_i)-d) \bmod q$ 和 $v_{ij}=(g(y_{ji})-d) \bmod q$ 中包含了随机的控制参数 d,任何签名人都无法获得,内部成员合谋攻击是不可行的。与以往的许多方案相比,随机控制参数的使用使得此方案可以使用多次,每次只需改变控制参数即可。

(3)事后签名人身份追踪很方便。虽然改进方案的签名 $(r,s,T,h(x))$ 相对 C-F 方案的签名 (r,s) 中增加了 $T=\prod_{i=1}^{t} T_i \bmod p$ 和 $h(x)=\prod_{i=1}^{t}(x-x_i)$ 使得签名长度变长,但是身份识别函数 $h(x)$ 追踪实际签名人是很方便的,不需要系统存储大量的签名人的信息,这样节省了系统的成本。

(4)新方案和原方案一样具有门限签名和有特权用户参与的特性。

6 结束语

考虑到签名人的权限不同,陈伟东提出了一类存在特权集的门限群签名方案,分析发现它容易受到 KAC 发起的各种伪造攻击和系统内部成员的合谋攻击,并且事后追踪签名人的身份是不可行的,对其进行了改进,设计了安全有效的新方案。在实际应用中,代理签名人的权限一般也不等[7],如何设计安全有效的存在特权集的代理签名方案是值得进一步思考和研究的问题。

参考文献:

[1] Desmedt Y,Frankel Y.Shared generation of authenticators and signatures[C]//Advances in Cryptology-CRYPTO'91.Berlin:Springer-Verlag,1992:457-469.

[2] 苗澎锋.一个有特殊成员的(t,n)门限签名方案[C]//2005 通信理论与技术新进展——第十届全国青年通信学术会议论文集.北京:北京邮电大学出版社,2005:1003-1005.

[3] 王勇兵,门玉梅,姬龙涛.具有特殊成员的门限签名方案安全性分析[J].计算机工程,2009,35(9):150-152.

[4] Shi Yi,Feng Deng-guo.The design and analysis of a new group of (t_j,t,n)threshold group-signature scheme[C]//Proc of the China-CRYPT 2000.Beijing:Science Press,2000:156-159.

[5] 陈伟东,冯登国.一类存在特权集的门限群签名方案[J].软件学报,2005,16(7):1289-1295.

[6] 王泽成,斯桃枝,李志敏.安全增强的存在特权集的门限群签名方案[J].计算机工程与应用,2007,43(9):151-153.

[7] 王天芹.存在特权集的门限代理群签名方案[J].计算机应用研究,2008,25(7):2146-2147.

(上接 50 页)

[3] Hu X,Eberhart R.Solving constrained nonlinear optimization problems with swarm optimization[C]//Proceedings of the 6th World Multiconference on Systemics,Cybernetics and Informatics(SCI2002),Orlando,USA,2002.

[4] Kocis G R,Grossmann I E.A modeling and decomposition strategy for the MINLP optimization of process flowsheets[J].Cmputers & Chemical Engineering,1989,13(7):797-819.

[5] Costa L,Oliveira P.Evolutionary algorithm to the solution of mixed integer non-linear programming problems[J].Computers and Chemical Engineering,2001,25(2/3):257-266.

[6] Kitayama S,Arakawa M,Yamazaki K.Penalty function approach for the mixed discrete nonlinear problems by particle swarm optimization[J].Structural and Multidisciplinary Optimization,2006,32(3):191-202.

[7] Sandgren E.Nonlinear integer and discrete programming in mechanical design[J].ASME Journal Mechanical Design,1990,112(2):223-229.

[8] Cardoso M F,Salcedo R L,de Azevedo S F,et al.A simulated annealing approach to the solution of MINLP problems[J].Computers and Chemical Engineering,1997,21(12):1349-1364.

[9] Special issue on mixed integer programming and it's application to engineering[J].Grossmann I E,Sahinidis N V.Optm Eng.Netherlands:Kluwer Academic Publishers,2002,3(4).

[10] 袁亚湘,孙文瑜.最优化理论与方法[M].北京:科学出版社,2003.

[11] 贺益君,陈德钊.适于混合整数非线性规划的混合粒子群优化算法[J].浙江大学学报:工学版,2008,5(5):747-751.