存在可实施强制签名特权集的门限群签名方案 *

陈道伟, 施荣华, 樊翔宇
(中南大学 信息科学与工程学院, 长沙 410075)

摘 要: 对存在特权集的门限群签名方案而言,要产生有效的群签名,必须要达到多个门限条件,只要其中有一个门限条件未达到群签名就不能产生,这大大降低了该类方案的灵活性。针对这一问题,利用 ELGamal 加密方法,提出了一种既可实施普通签名又可实施强制签名的解决方案。分析结果表明,该方案灵活性高、实用性强且具有可追踪性、匿名性等多种特性。另外,分析证明该方案在离散对数假设前提下是安全的。

关键词: 门限群签名; 特权集; 强制签名; 离散对数
中图分类号: TP309 **文献标志码**: A **文章编号**: 1001-3695(2012)01-0319-03
doi:10.3969/j.issn.1001-3695.2012.01.088

Threshold group signature scheme with mandatory signature privilege subsets

CHEN Dao-wei, SHI Rong-hua, FAN Xiang-yu
(*School of Information Science & Engineering, Central South University, Changsha* 410075, *China*)

Abstract: To the threshold group signature schemes with privilege subsets, if it want to produce effective group signature, it must achieve multiple threshold conditions, as long as one of the threshold conditions did not reach the group signature cannot produce, which greatly reduces the flexibility of this scheme. To solve the problem, made use of ELGamal encryption method, this paper put forward a signature scheme which could be either mandatory to implement or common to implement. The analysis results show that the theme has high flexibility, practicability and satisfies the properties of traceability, anonymity and so on. In addition, this paper analyzed the security of this scheme and proved that this scheme was secure in discrete logarithm assumption premise.

Key words: threshold group signature; privilege subsets; mandatory signature; discrete logarithm

门限群签名是指群中任意 t 个成员可以代表群组实施签名,而少于 t 个成员则不能产生有效的群签名。其首先由 Desmedt 等人[1]提出,随后门限群签名迅速发展。然而现有的一般门限群签名方案中签名成员权限都是相同的。针对这一问题,2005 年 Chen Wei-dong 等人[2]在 Shi Yi 等人方案[3]的基础上,详细论述了存在特权集的门限群签名问题,提出了一类 $(t_1,n_1;t,n)$ 门限签名方案。此后依据特权集思想多种方案相继被提出[4~6]。然而对于存在多个特权集 $(t_1,n_1;t_2,n_2;\cdots;t_m,n_m;t,n)$ 的门限签名模型,要产生一个有效的门限群签名需达到 $m+1$ 个门限条件,即 $(t_1,t_2,\cdots,t_m,t)$,这大大增加了产生门限群签名的难度,很容易导致签名"难产",降低了方案的实用性。因此在一定的条件下(如某一个或几个特权集3/4 以上成员同意),采用强制签名的方法来产生门限群签名就变得很有必要。强制签名的概念首先在文献[7]中提及,然而其采用的是 RSA 密码体制来实现强制签名,且方案不能有效抵抗内部用户的合谋攻击。

最近,文献[8,9]分别指出了文献[2]存在的错误和不足,并提出了改进方案增强原有方案的安全性。本文分析和研究了当特权集门限签名条件不能全部达到时,某一个或几个特权集可强制签名的情况,结合文献[8,9]的安全性分析和强制签名的思想,基于 ELGamal 密码体制,首次提出一种将普通签名与强制签名相结合起来的门限群签名方案。方案的基本设计思想是当满足普通签名门限条件时,实施普通签名,若不能满足普通签名的条件,但却满足强制签名特权集门限条件时则可实施强制签名。

1 方案描述

设有一签名群 G 由 n 个签名用户组成,有 m 个不相交的特权子集 $G_1,G_2,\cdots,G_m$,每个子集有 n_i 个成员。若要生成对某消息的有效签名,则要求 n_i 中至少要有 t_i 个签名用户同意,且同意签名用户总数至少为 t(即前述的 $m+1$ 个门限条件)。这种签名称为普通的存在特权集的门限签名,简称普通签名。由前述可知,普通签名很容易由于某一个门限条件不能达到而导致整个签名失败。而强制签名是指 m 个特权子集中有 m' 个特权集 $(m'\leqslant m)$ $G_1',G_2',\cdots,G_{m'}'$ 可实施强制签名,只要其中每个特权集同意签名用户数至少为 t_i'(一般来说 t_i' 要大于等于 t_i 才能体现出强制特性)且签名用户总数仍要达到 t 时就能实施强制签名,这种签名简称为强制签名。强制签名只需要达到 $m'+1$ 个门限条件,当 m' 远小于 m 时产生签名门槛将大为降低。

1.1 系统初始化

a) KAC(可信密钥认证中心)选取安全强素数 p 和 q 且满足 $q|p-1$,一个 $GF(q)$ 中阶为 q 的本原元 g 和一个强单向 hash 函数 $h(\cdot)$。

b) 秘密随机选择一个 $t-1$ 次多项式 $f(x)\in_R F[x]$ 和 m 个

收稿日期: 2011-05-13; **修回日期**: 2011-06-20 **基金项目**: 教育部国家大学生创新性实验计划国家级资助项目(LA10004)

作者简介:陈道伟(1989-),男,江西上饶人,本科,主要研究方向为通信网络与安全(daoweic@qq.com);施荣华(1964-),男,教授,博导,硕士,主要研究方向为计算机通信保密与信息安全;樊翔宇(1984-),男,博士研究生,主要研究方向为计算机网络安全.

次数为 t_i-1 的多项式 $g_i(x)\in {}_RF[x](i=1,2,\cdots,m)$。

c)KAC 为各个签名用户分配一个身份标志符(U_i,j,k)。其中 $i=1,2,\cdots,n;j=0,1,2,\cdots,m;k=0,1,\cdots,m'$($j$ 表示该用户属于哪个特权子集,当 $j=0$ 表示为普通用户;k 表示该用户属于某个可实施强制签名特权集,当 $k=0$ 时表示该集合用户不能实施强制签名)。KAC 保密签名用户的真实身份以便事后出现争议时追查。

d)公开$(p,q,g,h(\cdot))$和身份标志符(U_i,j,k)。

1.2 群密钥及秘密碎片生成阶段

本文借鉴文献[2]的双重秘密共享方案来产生群密钥和秘密钥,依靠的理论基础是 shamir 秘密共享原理。

普通签名群秘密钥:$x=f(0)+\sum_{j=1}^{m}g_j(0)\bmod q$

普通签名群公钥:$z=g^x\bmod p$

强制签名群秘密钥:$x_1=f(0)+\sum_{j=1}^{m'}g_j(0)\bmod q$

强制签名群公钥:$z_1=g^{x1}\bmod p$

用户秘密碎片分配:KAC 随机选择控制参数 $d\in Z_q^*$,若 U_i 是普通用户,则得到秘密碎片 $\delta_i=(f(U_i)-d)\bmod q$,并由 KAC 公开 $z_i=g^{f(U_i)}\bmod p$;若 U_i 是特权用户,并且属于特权集 j,则得到对应的秘密碎片有两份,一份是 $\delta_i=(f(U_i)-d)\bmod q$,另一份是 $\gamma_{ij}=(g_j(U_i)-d)\bmod q$,KAC 公开 $z_i=g^{f(U_i)}\bmod p$ 和 $z_{ij}=g^{(g_j(U_i))}\bmod p$,$D=g^d\bmod p$。

1.3 门限群签名的生成阶段

按照下面所述的步骤选取真正参与签名的用户:

a)如果参与签名用户的总人数小于 t,则签名失败,否则进行下一步。

b)按顺序选出满足各个特权子集门限值的特权签名用户。若能够成功选出,则选取 $t-\sum_{i=1}^{t}t_i$ 个剩余用户,实施普通签名(其中必有 $t\geqslant\sum_{i=1}^{t}t_i$,否则将与门限群签名的要求相矛盾);若选不出,则重新按照身份标志符从小到大的顺序选取满足强制签名特权集门限值的签名用户,若成功则实施强制签名,若选不出则本次签名彻底失败。

下面介绍具体签名生成过程:

设要签名的消息为 M。每个用户 U_i 为自身选择 $x_i\in Z_q^*$ 作为自己的私钥,同时公开对应的公钥 $y_i=g^{x_i}\bmod p$。

签名用户 U_i 秘密随机选择 $k_i\in Z_q^*$,计算 $r_i=g^{k_i}\bmod p$,并向其他签名用户和签名收集者(设为 SC)广播(U_i,j,r_i)。各签名用户在收到所有的组值后,根据上述步骤,选取真正参与签名的用户。若是符合普通签名条件则转入 1)执行,若符合强制签名条件则转入 2)执行,最后各签名用户和 SC 都计算 $r=\prod_{i=1}^{t}r_i$ 和 $Y=\prod_{i=1}^{t}y_i$。

1)普通签名

a)若 U_i 是普通用户,则计算:

$$s_i=(\lambda_i\delta_i+x_i)h(M\parallel r\parallel Y)-k_ir(\bmod q)$$

若 U_i 是特权用户,则计算:

$$s_i=(\lambda_i\delta_i+\gamma_{ij}\mu_i+x_i)h(M\parallel r\parallel Y)-k_ir(\bmod q)$$

其中:$\lambda_i=\prod_{j=1,j\neq i}^{t}\frac{0-U_j}{U_i-U_j}$ 和 $\mu_i=\prod_{j=1,j\neq i}^{t_c}\frac{0-U_{cj}}{U_{ci}-U_{cj}}$ 分别是用户在(t,n)秘密共享方案和(t_c,n_c)秘密共享方案(特权子集 c,其中 $c\in[1,m]$)的 Lagrange 恢复系数(可公开计算)。签名用户 U_i 将(s_i,r,Y)发送给签名服务机构 SC。

b)SC 收到 s_i 后,若 U_i 是特权用户,则计算 Lagrange 系数 λ_i 和 μ_i,若 U_i 是普通用户则只需计算 λ_i 而取 $\mu_i=0$;然后验证:

$$g^{s_i}r_i^rD^{(\lambda_i+\mu_i)h(M\parallel r\parallel Y)}=(z_i^{\lambda_i}z_{ij}^{\mu_i}y_i)^{h(M\parallel r\parallel Y)}\quad(1)$$

若等式成立,则接受签名并且 SC 计算 $s=\sum_{i=1}^{t}s_i\bmod q$。

然后 SC 将$(r,s,Y,h(x))$作为消息 M 的普通门限群签名安全发送给签名接收者,其中 $h(x)=\prod_{i=1}^{t}(x-U_i)$ 为签名用户的身份识别追踪函数。

2)强制签名

a)若 U_i 是普通签名用户,则计算:

$$s_{i1}=(\lambda_{i1}\delta_i+x_i)h(M\parallel r\parallel Y)-k_ir(\bmod q)$$

若 U_i 是可实施强制签名特权集用户,则计算:

$$s_{i1}=(\lambda_{i1}\delta_i+\gamma_{ij}\mu_{i1}+x_i)h(M\parallel r\parallel Y)-k_ir(\bmod q)$$

其中:$\lambda_{i1}=\prod_{j=1,j\neq i}^{t}\frac{0-U_j}{U_i-U_j}$ 和 $\mu_{i1}=\prod_{j=1,j\neq i}^{t_a'}\frac{0-U_{aj}}{U_{ai}-U_{aj}}$ 分别是用户在(t,n)秘密共享方案和(t_a',n_a')秘密共享方案(可强制签名特权集 a,其中 $a\in[1,m']$)的 Lagrange 恢复系数。签名用户 U_i 将(s_{i1},r,Y)安全发送给签名服务机构 SC。

b)SC 收到 s_{i1} 后,若 U_i 是特权用户,则计算 Lagrange 系数 λ_{i1} 和 μ_{i1},若 U_i 是普通用户则只需计算 λ_{i1} 而取 $\mu_{i1}=0$,然后验证等式 $g^{s_{i1}}r_i^rD^{(\lambda_{i1}+\mu_{i1})h(M\parallel r\parallel Y)}=(z_i^{\lambda_{i1}}z_{ij}^{\mu_{i1}}y_i)^{h(M\parallel r\parallel Y)}$。若等式成立,则接受签名并且 SC 计算 $s_1=\sum_{i=1}^{t}s_{i1}\bmod q$。

然后 SC 将$(r,s_1,Y,h_1(x))$作为消息 M 的强制门限群签名安全发送给签名接收者,其中 $h_1(x)=\prod_{i=1}^{t}(x-U_i)$ 为参与签名用户的身份识别追踪函数。

1.4 签名的验证阶段

任何签名接收人在收到签名后,验证签名的有效性。若签名是普通签名$(r,s,Y,h(x))$则验证等式:

$$g^sr^rD^{\sum_{i=1}^{t}(\lambda_i+\mu_i)h(M\parallel r\parallel Y)}=(zY)^{h(M\parallel r\parallel Y)}\quad(2)$$

如果签名是强制签名$(r,s_1,Y,h_1(x))$则验证等式 $g^{s1}r^rD^{\sum_{i=1}^{t}(\lambda_{i1}+\mu_{i1})h(M\parallel r\parallel Y)}=(z_1Y)^{h(M\parallel r\parallel Y)}$,若最终等式成立则证明签名有效接受签名,反之则拒绝签名。

如果事后需要追查出哪些人参与真正的签名,只需要将身份标志符 U_i 代入追踪函数 $h(x)$ 或 $h_1(x)$ 即可。若 $h(U_i)=0$ 或 $h_1(U_i)=0$ 则证明该用户参与了签名,再由 KAC 保存用户信息,可查出 U_i 的真实身份。

2 方案分析

2.1 正确性分析

由于强制签名是普通签名的一个特例,故本小节只对普通签名作分析,强制签名的分析类似。

a)SC 可以通过验证式(1)验证收到的单个签名 s_i 是否有效,证明如下:

$$g^{s_i}r_i^rD^{(\lambda_i+\mu_i)h(M\parallel r\parallel Y)}=g^{(\lambda_i\delta_i+\gamma_{ij}\mu_i+x_i)h(M\parallel r\parallel Y)-k_ir}g^{k_ir}$$

$$g^{d(\lambda_i+\mu_i)h(M\parallel r\parallel Y)}=g^{(\lambda_jf(U_i)+\mu_jf(U_i)+x_i)h(M\parallel r\parallel Y)}=(z_i^{\lambda_i}z_{ij}^{\mu_i}y_i)^{h(M\parallel r\parallel Y)}$$

b)签名验证者可以通过式(2)确认收到的签名是否有效,若等式成立,则证明签名有效。证明如下:

$$g^sr^rD^{\sum_{i=1}^{t}(\lambda_i+\mu_i)h(M\parallel r\parallel Y)}=g^{\sum_{i=1}^{t}s_i}(\prod_{i=1}^{t}r_i)^rg^{d\sum_{i=1}^{t}(\lambda_i+\mu_i)h(M\parallel r\parallel Y)}$$

$$g^{\sum_{i=1}^{t}(\lambda_i\delta_i+\gamma_{ij}\mu_i+x_i)h(M\parallel r\parallel Y)-k_ir}g^{\sum_{i=1}^{t}k_ir}g^{d\sum_{i=1}^{t}(\lambda_i+\mu_i)h(M\parallel r\parallel Y)}=$$

$$g^{\sum_{i=1}^{t}(\lambda_jf(U_i)+\mu_ig_j(U_i)+x_i)h(M\parallel r\parallel Y)}=g^{(f(0)+\sum_{j=1}^{m}g_j(0)+\sum_{i=1}^{t}x_i)h(M\parallel r\parallel Y)}=$$

$$(zY)^{h(M\|r\|Y)} \bmod p$$

证毕。

2.2 安全性分析

1)可以抵抗各种伪造攻击

这里只对普通签名作分析,强制签名的分析类似。首先考虑外部敌手的伪造攻击,要伪造签名$(r,s,Y,h(x))$,必须伪造出r、s。而伪造r面临求解离散对数的数学难题;伪造s需要知道用户的秘密碎片,在系统安全的情况下秘密碎片不能获得。通过求解$z=g^x$获得群私钥$x=f(0)+\sum_{j=1}^{m}g_j(0) \bmod q$,以便伪造群签名在离散对数假设安全的前提下是不能成功的。接着考虑内部$t-1$个成员的伪造攻击,这里指出在离散对数假设和可证明安全理论的前提下是不能成功的,具体参见文献[2]给出的分析。最后考虑 KAC 的伪造攻击,假设 KAC 被敌手攻破实施伪造攻击,在已知δ_i、γ_{ij}的前提下还必须知道签名人的私钥x_i,而由$y_i=g^{x_i} \bmod p$求x_i在离散对数假设下是不可行的,故 KAC 不能伪造签名。

2)可以抵抗内部t个用户的合谋攻击

文献[9]指出 Chen Wei-dong 等人的方案安全隐患之一在于无法抵抗内部用户的合谋攻击。本文借鉴其设计方法加入随机控制参数d,克服了内部t个用户的合谋攻击带来的风险,具体分析参见文献[9]的安全性分析。

3)具有可追踪签名人真实身份的特性

在本方案中采用身份标志符来代替签名人的真实身份,隐藏了签名用户的真实身份有利于保护签名人的权益,实现了匿名性。另外追踪签名用户的真实身份也很容易,只需要将身份标志符代入追踪函数$h(x)$即可。若$h(U_i)=0$,则证明该用户参与了签名,最后可由 KAC 查出该用户的真实身份。另外文献[8]证明了对追踪函数的攻击是不可行的,所以追踪函数的安全性是有保证的。

4)具有门限特性

本方案既可实施普通签名又可实施强制签名,灵活易用。而且两种签名方案都必须达到特定的签名门限值,否则不能恢复群私钥,同时签名验证方程也将不能通过。

3 结束语

本文提出了一种新的门限签名方案,解决了一般存在特权集的门限签名方案中签名容易"难产"且安全性弱的问题,进一步完善了存在特权集的门限群签名方案。

参考文献:

[1] DESMEDT Y,FRANKEL Y. Shared generation of authenticators and signatures[C]//Proc of the 11th Annual International Compotology Conference on Advances in Cryptology. London: Springer-Verlag, 1992:457-469.

[2] CHEN Wei-dong,FENG Deng-guo. A group of threshold group signature schemes with privilege subsets [J]. Journal of Software,2005, 16(7):1289-1295.

[3] 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. Beijing: Science Press, 2000:156-159.

[4] 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.

[5] XUE Ming-wang, YU Rong-dong. Threshold group signature scheme with privilege subjects based on ECC[C]//Proc of ICCIIS. 2010:84-87.

[6] 杨长海,唐西林. 具有多种特性的门限多代理多签名方案[J]. 计算机工程,2009,35(13):160-162.

[7] 贾晓芸. 面向群体的数字签名体制研究[D]. 北京:北京邮电大学,2008.

[8] 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.

[9] 王勇兵,王际川. 对存在特权集的门限群签名方案的安全性分析[J]. 计算机工程与应用,2010,46(9):80-82.

(上接第 318 页)引入了节点连接度差异性导致感染率不同的恶意软件扩散模型。该模型能够较真实地反映实际环境中如骨干节点、sink 网关节点等连接度大的节点常常受管理人员关注而具有较强安全性的特点,提出了节点感染率并不与连接度简单成正比的观点。实验证明此二维元胞自动机模型能够更准确地描述恶意软件在无线传感网络环境下的传播行为,具有重要的研究价值。

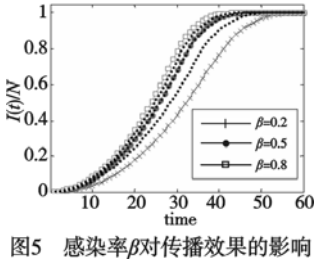

图5　感染率β对传播效果的影响

参考文献:

[1] STAN I S, PAXSON V, WEAVER N. How to own the Internet in your spare time[C]//Proc of the 11th USENIX Security Symposium. 2002:149-167.

[2] ZOU C C, TOWSLEY D, GONG W B. Modeling and simulation study of the propagation and defense of Internet e-mail worms[J]. IEEE Trans on Dependable and Secure Computing, 2007, 4(2):105-118.

[3] ZOU C C, GONG W, TOWSLEY D. Code red worm propagation modeling and analysis[C]//Proc of the 9th ACM Conference on Computer and Communications Security. 2002:138-147.

[4] PASTOR-SATORRAS R, VESP I I A. Epidemic spreading in scale free networks [J]. Physical Review Letters, 2001, 86(14):3200-3203.

[5] NEWMAN M E J, FORREST S, BALTHROP J. E-mail networks and the spread of computer viruses [J]. Physical Review E, 2002, 66(3):35101.

[6] KHAYAM S A, RADHA H. Using signal processing techniques to model worm propagation over wireless sensor networks [J]. IEEE Signal Processing Magazine, 2006, 23(2):164-169.

[7] DE P, LIU Y, DAS S K. Modeling node compromise spread in wireless sensor networks using epidemic theory[C]//Proc of International Symposium on World of Wireless, Mobile and Multimedia Networks. 2006:237-243.

[8] TANACHAIWIWAT S, HELMY A. Encounter-based worms: analysis and defense[J]. Ad hoc Networks, 2009, 7(7):1414-1430.

[9] OLINKY R, STONE L. Unexpected epidemic thresholds in heterogeneous networks [J]. Physical Review E, 2004, 70(3):30902.

[10] 宋玉蓉,蒋国平. 节点抗攻击存在差异的无尺度网络恶意软件传播研究[J]. 物理学报,2010,59(2):705-711.