一类存在特权集的门限群签名方案*

陈伟东[1,2+], 冯登国[3]

[1](信息安全国家重点实验室(中国科学院 研究生院),北京 100049)

[2](中国科学院 电子学研究所,北京 100080)

[3](信息安全国家重点实验室(中国科学院 软件研究所),北京 100080)

A Group of Threshold Group-Signature Schemes with Privilege Subsets

CHEN Wei-Dong[1,2+], FENG Deng-Guo[3]

[1](State Key Laboratory of Information Security (Graduate School, The Chinese Academy of Sciences), Beijing 100049, China)

[2](Institute of Electronics, The Chinese Academy of Sciences, Beijing 100080, China)

[3](State Key Laboratory of Information Security (Institute of Software, The Chinese Academy of Sciences), Beijing 100080, China)

+ Corresponding author: Phn: +86-10-66842704, Fax: +86-10-62645000, E-mail: zccwd@yahoo.com.cn, http://gscas.ac.cn

Received 2003-12-01; Accepted 2004-07-06

Chen WD, Feng DG. A group of threshold group-signature schemes with privilege subsets. *Journal of Software*, 2005,16(7):1289−1295. DOI: 10.1360/jos161289

Abstract: Feng Deng-Guo suggested a problem so called "threshold group-signature scheme with privilege subsets". This paper analyzes the security of such schemes at present and propose new schemes. Based on theory of finite fields, the authors firstly show there are some insufficiencies and potential hazard in the scheme proposed by Shi, et al. Secondly, using the idea of constructing group-signature scheme by individual signature scheme, a group of the ones with four variants of type of ElGamal are put fordward, which have some attractive properties, such as message recovery, shorter length of signature, etc. Finally, the security of the schemes is proved under the assumption that the respective individual signature schemes are secure.

Key words: threshold group-signature; secret sharing scheme; ElGamal cryptosystem; message recovery; provable security

摘 要: 针对冯登国提出的"存在特权集的门限群签名"问题,旨在分析现有解决方案的安全缺陷并给出新的解决方案.首先基于有限域理论分析指出石怡等人给出的一种实现方案存在不足和安全隐患.然后推广了利用单签名构造群签名的思想,提出了具有 4 个变形的一类 ElGamal 类型门限群签名方案,从而解决了以上问题.这类方案还具有消息恢复、签名长度短等许多良好性质.最后,基于单签名的安全性假设,证明以上方案是安全的.

关键词: 门限群签名方案;秘密共享方案;ElGamal 体制;消息恢复;可证明安全性

* Supported by the National Natural Science Foundation of China under Grant No.60253027 (国家自然科学基金); the National Grand Fundamental Research 973 Program of China under Grant No.G1999035802 (国家重点基础研究发展规划(973))

作者简介: **陈伟东**(1969－),男,内蒙古赤峰人,博士生,主要研究领域为密码学及其应用;**冯登国**(1965－),男,博士,研究员,博士生导师,主要研究领域为信息与网络安全方面的研究与开发.

中图法分类号: TP309 文献标识码: A

密码学的主要任务就是在充满敌意的环境中确保安全通信:各方在敌手控制的网络上传送数据,一般需要确保数据的隐秘性、认证性.在保密通信中提供认证功能与确保数据的隐秘性一样重要,数字签名就是一种被广泛应用、提供认证服务的有效机制.

一般的签名方案都是由一个签名方使用自己的私钥签名,验证方利用其公钥验证签名是否合法,本文称之为单签名.然而,在许多应用中,签名的责任需要被一个由多个签名方组成的签名方集合分享,一般要约定:n 个签名方中,至少要有 t(不大于 n)个签名方参与才能产生某消息的合法签名.因此提出多签名、门限群签名概念是很自然的思想:前者的验证一般需要多个公钥,后者只需群公钥即可验证,通常还要求签名方匿名.本文研究范围限于门限群签名(注意,这和一般的群签名概念有很大的不同),该思想最初由 Desmedt 和 Frankel 在 1991 年提出——主要是基于 RSA 构造了一个门限群签名方案[1];近年来,研究有了很大进展,参见文献[2~5]等.值得注意的是,文献[3,4]所提出的方案可以没有可信认证中心;文献[5]则从可证明安全性理论角度为群签名本原奠定了理论基础,但必须说明的是,文献[5]所涵盖的群签名概念与本文有很大区别——仅指群中任一成员可以代表团体签名.

目前,一般门限群签名方案的一个潜在问题是,各签名方的权限是等同的,但实际情形不总是这样.文献[6]提出了一个新的门限群签名问题(示例):一个公司包含两类董事,一类是任职董事(8 人),另一类不在公司任职(12 人);要通过一个提案时,除需半数以上董事同意(对提案签名)以外,为保证可操作性,还要求其中至少包括 6 名任职董事,同时要保证表决的匿名性,但事后在得到授权时应有办法查明表决情况.以上示例可以抽象成一个“存在特权集的门限群签名问题”:一个由 n 个签名方组成的群体 G,有 m 个不相交特权子集 $G_1,...,G_m$,每个子集有 n_i 人;要产生对某消息的合法群签名,至少需要 $G_i(i=1,2,...,m)$ 中有 t_i 人同意,且同意签名方总人数至少为 t,还要求具有匿名性和事后确认签名方身份等性质.

文献[6]还给出了解决上述问题的一个实现方案,最近两年来尚未见到有其他方案,但一些门限密钥管理方案借用了以上思想,不过多数是不安全的.

我们要说明的是,文献[6]所提出的方案并不十分理想,如协议过分复杂、签名长度较长,而且存在安全隐患.本文应用了利用单签名构造群签名的设计思想,提出了一类存在特权集的 EIGamal 类型门限群签名方案,具有许多良好的性质,诸如签名长度短、可以不设可信密钥认证中心、无须额外身份鉴别算法即可实现特权门限条件,协议步骤较简单等;共包括 4 个变形,其中两个还具有消息恢复性质,即由签名可恢复所签署的消息,这样的签名方案具有很大的应用优势,如节省带宽等;与文献[6]提出的方案相比,本文的方案实现起来也更为有效.以上的许多性质都是文献[1~4,6]等所不具备的,而且这些方案都未给出安全性证明,但我们用可证明安全性理论分析了所设计方案,在标准模型(假设单签名是安全的)中给出了安全性证明.

为了叙述简洁起见,我们不妨假设签名方群体 G 只有一个特权子集 G_1,下面会看到,推广到多个特权子集的情况是很容易的.

1 对一种存在特权集的门限群签名方案[6]的分析

文献[6]依据离散对数问题提出一种存在特权集的门限群签名方案,简称为 (t_j,t,n) -门限(群签名)方案.

其基本设计流程如下:

I. 初始化.IDC(可信的身份代码分配中心)与每个成员协同产生成员身份代码,且 IDC 还产生群的参数;执行结果(需要 12 步交互协议)是用户 i 得到 $\{id_i$, 2 个签名参数$\}$,DC(签名合成器,后面称为签名服务机构 SC)得到 $F_j(x)=\prod_{i\in G_j}(x-id_i)\bmod q$.

II. 签名.签名方和 DC 执行交互签名协议(12 步):主要是每个签名方先生成“预签名”(含身份代码 id_i),利用 $F_j(x)$ 是否为 0 判断签名方身份是否合法,然后判断是否符合“特权门限”条件;若符合,则在组内广播群签名参

数 $\{j, g_j(x), E_j\}$,这里, $g_j(x)$ 是 $F_j(x)$ 的因子——实际参与方的身份判别多项式.最后,DC 收集所有个人签名,并生成群签名 $\{ID, S, g(x), R_j, E_j \mid j=1,2,...,m\}$. 这里, $g(x)=\prod_{j=1}^{m} g_j(x) \bmod q$, 其余说明略.

III. 验证.略.

下面对以上方案作简要分析.首先,协议比较复杂,特别是签名长度较长,至少为 $(m+1)\log_2 p+(m+t+1)\log_2 q$ ($q \mid (p-1)$, q, p 都是大素数,m 是特权子集的个数).

更为重要的是,以上方案还存在安全隐患:由于匿名性要求,用户身份代码是保密的;群签名中的 $g(x)$ 是为事后 IDC 验证签名方身份而设置的,因此要求分解 $g(x)$ 是不可行的[6];但必须说明的是,有限域上(即使特征较大)的多项式分解是存在有效分解算法的,如 Berleknmp 算法及其改进算法[7].

2 一类(t_1,n_1;t,n)门限群签名方案

2.1 基本思想

采用文献[2]的设计思想:利用成熟的单签名方案,如 EIGamal 类型的签名方案,结合秘密共享方案构造门限群签名方案;与文献[2]不同的是,我们把特权条件要求与秘密共享思想结合起来,即采用对秘密钥的“双重”分割方法,设计一类具有 4 个变形、存在特权集的 EIGamal 类型门限群签名方案,特别是还构造出具有消息恢复性质的方案;与文献[2]一样,也可以不要求可信密钥认证中心 KAC 的存在.

2.2 初始化

所涉及的机构如下:

KAC:可信密钥认证中心,负责颁发密钥;

SC:签名服务机构,负责颁布签名;

G:n 个签名方组成的群体;

G_1:G 的子集,至少有其中的 t_1 方参与才可能产生合法群签名,称为特权子集.

KAC 执行如下操作:

(1) 选取安全素数 p, q ,满足 $q \mid (p-1)$;

(2) 在 F_q 上秘密随机选取 2 个多项式 $f(x), g(x)$,次数分别是 $(t-1)$ 和 (t_1-1) ;

(3) 取 α 是有限域 F_q 的本原元.公开 (p, q, α) 和 $x_i, y_j \in_R Z_q[x], i=1,2,...,n, j=1,2,...,n_1$.

2.3 群密钥及秘密钥碎片产生

基本工具采用 Shamir 秘密共享方案[8],记为 SSS.

群秘密钥:KAC 产生,亦即 $(f(0)+g(0)) \bmod q$.

群公钥: $z=\alpha^{(f(0)+g(0)) \bmod q} \bmod p$.

秘密钥碎片分发:采用“双重”SSS(分别是 (t, n) 和 (t_1, n_1)- 门限 SSS),即如果 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 是特权集中的用户(以后简称为特权用户),则得到对应碎片 $f(x_i), g(y_{ij})$ (不妨用 y_{ij} 表示第 2.2 节最后随机选取的某个 y_j ,各特权用户不重),公开 $z_i=\alpha^{\lambda_i f(x_i)+\mu_i g(y_{ij})} \bmod p$. 这里, λ_i, μ_i 是 SSS 所涉及的 Lagrange 恢复系数,是可以公开计算的,参见文献[8],以上过程实际上是建立了各用户的公私钥碎片.

2.4 (t_1,n_1;t,n)-门限群签名产生

基本流程与文献[2]类似,不妨假设只有 t 个人参加签名,且恰为 $1,2,...,t$, 具体步骤如下,设被签署消息为 m.

(1) 单个签名的产生和验证. $\forall i=1,2,...,t, i$ 秘密随机选取 $k_i \in Z_p^*$,计算 $r_i=\alpha^{k_i} \bmod p$,并在群内通过广播信道匿名广播 r_i; 于是每一用户 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 $s_i=(f(x_i)\lambda_i h(m)+g(y_{ij})\mu_i h(m)-k_i r)\bmod q$. 这里, λ_i,μ_i 是 SSS 所涉及的恢复系数,是可以公开计算的,参见文献[8], $h(\cdot)$ 是 hash 函数; s_i 被发送给签名服务机构 SC.SC 可以这样验证所提交子签名的合法性:对于用户 i(无论是普通用户还是特权用户),验证 $\alpha^{s_i}r_i^r=z_i^{h(m)}$ 是否成立,若成立,则接受单签名.

(2) 签名合成:如果SC接受所有提交的单签名,则计算 $s=(s_1+s_2+...+s_t)\bmod q$, 输出 (r,s) 作为消息 m 的群签名.

2.5 群签名的验证和(事后)身份追踪

不妨仍假设共有 t 个人参加签名,且恰为1,2,...,t, 且其中至少有 t_1 人属于特权子集.

显然, $s=h(m)\left(\sum_{i=1}^{t}f(x_i)\lambda_i+\sum_{i=1}^{t_1}g(y_{ij})\mu_i\right)-r\sum_{i=1}^{t}k_i=h(m)(f(0)+g(0))-r\sum_{i=1}^{t}k_i$, 因此有如下验证方程成立:

$$\alpha^s r^r=z^{h(m)}.$$

易见,如果不符合特权条件要求,则即使有 t 个以上人员参加签名, $g(0)$ 的恢复也是不可能的,从而得不到群秘密钥;而如果不足 t 个以上人员参加签名,即使 $g(0)$ 可以恢复,但却不可能恢复 $f(0)$.如果事后得到许可,需要调查是哪些人员参与签名,则由 SC 追踪签名方是平凡的.

2.6 存在任意多个特权集的门限群签名方案

前面已指出,一般情形如下:n 个签名方组成的群体 G,有 m 个不相交特权子集 $G_1,\ldots,G_m$,每个子集有 t_i 人;要产生对某消息的合法群签名,至少需要 G_i(i=1,2,…,m)中有 t_i 人同意,且同意签名方总人数至少为 t,其余说明同前.

上述问题可称为 $(t_1,n_1;...,t_m,n_m;t,n)$- 门限群签名问题.

$(t_1,n_1;t,n)$- 门限群签名方案易于推广到 $(t_1,n_1;...,t_m,n_m;t,n)$- 门限群签名方案:只需在初始化阶段选取 $m+1$ 个多项式 $f(x),g_1(x),...,g_m(x)$, 群秘密钥被选取为 $\left(\sum_{i=1}^{m}g_i(0)+f(0)\right)\bmod q$, 每个特权用户持有 $f(x_i)$ 及对应的一个 $g_i(y_{ij})$, 其余说明同前.

2.7 没有KAC存在的情况

与文献[4]一样,以上方案也可以不要求 KAC 存在.

基本方法是:各用户自己作自己的 KAC,即自行选择(ElGamal 类型)公私钥对 (x_i,y_{ij}); 群公钥为 $y=\prod_{i=1}^{n}y_i$, 类似前面的碎片分发,各用户采用“双重 SSS”方法,把自己的秘密钥碎片分给其余 $(n-1)$ 个用户,群签名的产生是类似的,限于篇幅,我们将另文讨论这个问题.

3 具有消息恢复性质的$(t_1,n_1,\ldots,t_m,n_m;t,n)$-门限群签名方案

主要考虑到效率因素,具有消息恢复性质(即由签名可以恢复被签署消息)的签名方案是很有吸引力的,下面沿用以上思想可以构造出具有消息恢复性质的 $(t_1,n_1;...,t_m,n_m;t,n)$- 门限群签名方案.与前面一样,仍以 $(t_1,n_1;t,n)$- 门限群签名方案为例说明.

3.1 一般ElGamal类型$(t_1,n_1;t,n)$-门限群签名方案的构造

问题:是否各种 ElGamal 类型的签名方案变形都可以用以上方法构造本文的门限群签名方案?对此,我们持谨慎态度,但可以肯定的是,如下 2 个单签名变形[9,10]

$$s=xr\pm kh(m)\bmod q, s=xh(m)\pm kr\bmod q$$

都可以(后一种情况就是第 2 节所依据的单签名方案),这里,均有 $r=g^k \bmod p$, 验证方程略.具体构造过程类似第 2 节.

值得注意的是,文献[9,10]给出了 6 个具有消息恢复性质的单签名方案,我们认为,如下 2 个变形可以用来构造本文的门限多签名方案:

$$s=-xr+k \bmod q, s=-x+kr \bmod q,$$

第 1 个签名分量均为 $r=R(m)g^{-k} \bmod p$. 这里, $R(\cdot)$ 是冗余(redundancy)函数,即把消息一一映射到所谓的 message-signing 空间 M_S; 注意,对冗余函数的基本要求是,像空间 M_R 在 M_S 中必须是"稀疏"的,否则易于遭受存在性伪造攻击[10];当用 hash 函数取代冗余函数时,便与普通签名方案一样,不再具有消息恢复特性;相应的验证方程分别为

$$R(m)=ry^r g^s \bmod p, R(m)=ry^{r^{-1}} g^{sr^{-1}} \bmod p.$$

下面以第 1 个变形为例,考虑 $(t_1,n_1;t,n)$-门限群签名方案的构造,一般情形的推广类似第 3 节.

3.2 $(t_1,n_1;t,n)$-门限群签名方案的构造

初始化和碎片分配与第 2 节类似.群公钥 z、各(特权或普通)用户公钥 z_i 的说明可类比推出.

不妨假设只有 t 个人参加签名(满足特权条件),且恰为 1,2,...,t, 具体步骤如下:

(1) 单个签名的产生和验证. $\forall i=1,2,...,t$, i 秘密随机选取 $k_i \in Z_p^*$, 计算 $r_i=R(m)\alpha^{-k_i} \bmod p$, 并在群内通过广播信道匿名广播 r_i; 每一用户 i 计算 $r=\dfrac{1}{R(m)^{t-1}}\prod_{i=1}^{t} r_i \bmod p$; 若 i 是普通用户,则计算 $s_i=(-f(x_i)\lambda_i r+k_i) \bmod q$,若 i 是特权用户,则计算 $s_i=(-(f(x_i)\lambda_i r+g(y_{ij})\mu_i)r+k_i) \bmod q$, s_i 被发送给 SC.

由第 3.1 节所述不难构造 SC 的验证方程:即检查 $R(m)=r_i\alpha^{s_i}z_i^r \bmod p$ 是否成立,若成立,则接受单签名.

(2) 签名合成.如果 SC 接受所有提交的单签名,则计算 $s=(s_1+,...,s_t) \bmod q$, 输出 (r,s). 作为消息 m 的群签名.

显然,签名验证方程是: $r\alpha^s z^r=R(m)$.

类似第 2 节,也可以在没有 KAC 的情况下构造具有信息恢复特性的 $(t_1,n_1;t,n)$-门限群签名方案;推广到 $(t_1,n_1;...;t_m,n_m;t,n)$-门限群签名方案的过程也是类似的.

4 分 析

不妨称第 2 节的方案为 $(t_1,n_1;t,n)$-门限群签名方案,称第 3 节构造的方案为 $MR-(t_1,n_1;t,n)$-门限群签名方案;它们各有 2 个变形,只以第 1 个为例来加以说明.

首先分析正确性.

定理 1. 如果各方遵从协议规则, $(t_1,n_1;t,n)$-门限群签名方案的验证方程 $\alpha^s r^r=z^{h(m)}$ 成立,则 $MR-(t_1,n_1;t,n)$-门限群签名方案的验证方程 $r\alpha^s z^r=R(m)$ 亦然.

证明:参见第 2、第 3 节相应论述,略. □

下面分析匿名性.显然,只有 SC 知道签名方身份,因为其他用户只通过广播信道得知了 $r_i=\alpha^{k_i} \bmod p$ 的值,并不能确定任何其他用户身份——亦即由最终群签名是不能(未经特许的情况下)追踪各签名方身份的,值得说明的是,这里我们并未像文献[6]那样设计一个身份识别算法;当然也有待改进之处,即各签名方知道有多少人参与了表决,但多数情况下这不会引起什么问题.

还应该说明,即使是 SC 本身也不能构造一个合法群签名,因为 SC 既不知道群私钥,而且部分签名 r 也是由用户产生的.

下面考虑上述签名方案的抗伪造攻击能力.

由前所述,两个签名方案是根据如下两个 ElGamal 变形单签名方案得到的:

$$r=\alpha^k \bmod p, s=xh(m)-kr \bmod q \quad (1)$$

$$r=R(m)\alpha^{-k} \bmod p, s=-xr+k \bmod q \quad (2)$$

验证方程分别是(1) $\alpha^s r^r=z^{h(m)}$;(2) $r\alpha^s z^r=R(m)$.

多年来的研究表明,以上 2 个单签名方案具有很好的抗伪造攻击能力,其安全性已得到公认,有关具体分析可参见文献[9,10]等.

如果利用常用的信息论分析方法分析以上门限群签名方案,我们易于证明:如果门限或特权条件不满足,则敌手(可能有一些签名方被收买)得不到群秘密钥的任何信息.但这并不能说明以上群签名方案具有抗伪造攻击性质.为此,我们采用复杂性理论方法(即可证明安全性理论[11]),假设单签名方案(1)、(2)是安全的,证明在此假设下上述门限群签名方案是安全的.下面规定签名方案敌手(亦即伪造者 F)都是概率多项式时间(PPT)算法.

我们先引入不可分辨和统计近似概念[12].

定义 1(计算不可分辨). 设 $\{X_n\}$ 和 $\{Y_n\}$ 是 2 个概率空间,称它们是(多项式)计算不可分辨的,如果对任意多项式 $p(\cdot)$,任意 PPT 算法(概率多项式算法)D 及所有辅助输入 $z\in\{0,1\}^{poly(n)}$, $|\Pr[D(X_n,1^n,z)=1]-\Pr[D(Y_n,1^n,z)=1]<1/p(n)$.

以上定义说明,不存在明显可区分概率空间 $\{X_n\}$ 和 $\{Y_n\}$ 的概率多项式算法,亦即在多项式时间内,使用任何 PPT 区分算法,成功概率是可忽略的;所谓可忽略概率是指,当 $n\to\infty$ 时,概率趋于 0 的速度比任何多项式函数的倒数的速度要"快".

定义 2(统计近似). 称 2 个概率空间 $\{X_n\}$ 和 $\{Y_n\}$ 是统计近似(statistical close)的,如果其统计差异(statistical difference)是可忽略的.这里,统计差异定义为 $\Delta(n)=1/2\sum_{\alpha}|\Pr[X_n=\alpha]-\Pr[Y_n=\alpha]|$.

引理 1. 如果 2 个概率空间 $\{X_n\}$ 和 $\{Y_n\}$ 是统计近似的,则必然计算不可分辨.

证明:参见文献[12]. □

ElGamal 类型签名 (r,s) 是随机的(由随机变量 k 决定),则分别记(1)、(2)决定的随机变量为 $(m,r(k),s(k,m))_1$ 和 $(m,r(k),s(k,m))_2$;类似可记 $(t_1,n_1;t,n)$-门限群签名方案、$MR-(t_1,n_1;t,n)$-门限群签名方案决定的签名随机变量分别为 $(m,\sigma(k_1,...,k_t),\tau(k_1,...,k_t,m))_1$, $(m,\sigma(k_1,...,k_t),\tau(k_1,...,k_t,m))_2$.

定理 2. 任意不满足门限特权条件的敌手在与诚实用户交互后,$(m,r(k),s(k,m))_i$ 和 $(m,\sigma(k_1,...,k_t),\tau(k_1,...,k_t,m))_i$ 是不可分辨的,这里,$i=1,2$.

证明:如果各签名方完全可信,显然结论成立.下面考虑最极端的情况(一般情况是类似的): $(t-1)$ 人不可信或不可信(即可能协同攻击),由 Shamir 秘密共享方案的性质可知,这种情况下已为敌手所知的密钥 Shares 和群私钥在信息论意义上是独立的,因此不妨以第 1 种情况为例加以证明,且假设这些签名方是 $1,2,...(t-1)$. 以(1)为例,注意,这时,$\sum_{i=1}^{t-1}k_i$ 已被被收买用户取定,但 k_t 仍是随机的,而任何常数与均匀随机变量 U 的和仍是 U,故随机变量 $\sum_{i=1}^{t-1}k_i+k_t=K$ 和 k 一样,都是(长为 $\log_2 p$ 的)均匀分布随机变量(即敌手不能分辨 K,k).综上可知,$r=\alpha^k$ 和 $\sigma=\alpha^K$ 是统计近似的,从而由引理 1 可知也是计算不可分辨的;又,对群签名而言,$\tau=h(m)(f(0)+g(0))-r\sum_{i=1}^{t}k_i$,该式中前一项和 s 完全相同(假设相应的群私钥和单签名私钥相同),易见 s,τ 也是不可分辨的.实际上 s,τ 的不可分辨由 $r=\alpha^k$ 和 $\sigma=\alpha^K$ 的不可分辨易于得到.对情形(2)的讨论类似,证毕. □

该定理说明,当敌手(至多控制 $(t-1)$ 个签名方)与诚实签名方(未被收买)交互时,得到的群签名和相应单签名是不可分辨的.

下面,我们考虑敌手和不诚实的签名方交互的情形,亦即敌手试图假冒合法签名方.简洁起见,假设敌手 A 已收买了全部 t 个参与方中的 $(t-1)$ 个签名方 $1,2,...,(t-1)$.

假设如下单签名方案:任意外部公开输入 r',公钥 $z_i=\alpha^{y_i}$.

$$r_i=\alpha^{k_i}\bmod p, r=r'r_i\bmod p, s_i=(y_ih(m)-k_ir)\bmod q \tag{3}$$

验证方程是 $\alpha^{s_i}r_i^r=z_i^{h(m)}$. 显然,该单签名方案就是 $(t_1,n_1;t,n)$-门限群签名方案的基础单签名方案.我们可以假设:如果敌手 A 不满足门限特权条件,则任意诚实方的如上单签名方案是安全的.根据定理 2,该假设是合理的.

定理 3. 在上述条件下,$(t_1,n_1;t,n)$-门限群签名方案抗积极敌手的伪造攻击.

证明:不失一般性,设共有 t 个签名方参加,其中 $1,2,...,t-1$ 已被收买且特权条件满足,只有 t 是诚实方.如果敌手 A 可以伪造群签名,易于证明 A 一定可以伪造 t 的单签名.设所伪造的群签名是 (σ,τ),设 $1,2,...,t-1$ 的相应单

签名是 (r_i, s_i),则易验证

$$r_t = \sigma / \prod_{i=1}^{t-1} r_i, s_t = \tau - \sum_{i=1}^{t-1} s_i$$

就是 t 的合法单签名,这与假设矛盾. □

References:

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

[2] Harn L. Group-Oriented (*t*,*n*)-threshold digital signature scheme based on discrete logarithms. IEEE Proc. Computers and Digital Techniques, 1994,141(5):307−313.

[3] Wang GL, Qing SH. A threshold undeniable signature scheme without a trusted party. Journal of Software, 2002,13(9):1758−1764 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/13/1758.pdf

[4] Takaragi K, Miyazaki K, Takahashi M. A threshold digital signature issuing scheme without secret communication. 1998. http://grouper.ieee.org/groups/1363/StudyGroup/Threshold.html

[5] Bellare M, Micciancio D, Warinschi B. Foundations of group signatures: Formal definitions, simplified requirements, and a constructions based on general assumptions. In: Biham E, ed. Proc. of the Advances in Cryptology—EUROCRYPT 2003. LNCS 2656, Berlin: Springer-Verlag, 2003. 614−629.

[6] Shi Y, Feng DG. The design and analysis of a new group of (t_j,*t*,*n*) threshold group-signature scheme. In: Wang EF, Yang WC, eds. Proc. of the CHINACRYPT 2000. Beijing: Science Press, 2000. 156−159 (in Chinese with English abstract).

[7] Shoup V. On the deterministic complexity of factoring polynomials over finite fields. Information Processing Letters, 1990,33: 261−267.

[8] Feng DG, Pei DY. Introduction to Cryptology. Beijing: Science Press, 1999. 235−236 (in Chinese).

[9] Nyberg K, Rueppel RA. Message recovery for signature schemes based on the discrete logarithm problem. In: De Santis A, ed. Advances in Cryptology—EUROCRYPT'94. LNCS 950, Berlin: Springer-Verlag, 1995. 182−193.

[10] Ateniese G, de Medeiros B. Efficient group signatures without trapdoors. 2002. http://eprint.iacr.org/2002/173/

[11] Bellare M. Practice-Oriented provable-security. In: Damgard I, ed. Advances in Cryptology—Eurocrypt'99. LNCS 1561, Berlin: Springer-Verlag, 1999. 221−231.

[12] Goldreich O. Foundations of Cryptography. Beijing: Publishing House of Electronics Industry, 2003. 103−107.

附中文参考文献:

[3] 王贵林,卿斯汉.不需要可信任方的门限不可否认签名方案.软件学报,2002,13(9):1758−1764. http://www.jos.org.cn/1000-9825/13/1758.pdf

[6] 石怡,冯登国.一类新型(t_j,*t*,*n*)-门限群签名方案的设计与分析.见:王鄂芳,杨伟成,编,密码学进展——ChinaCrypto 2000.北京:科学出版社,2000.156−159.

[8] 冯登国,裴定一.密码学导引.北京:科学出版社,1999.235−236.