第 35 卷 第 9 期 计 算 机 工 程 2009 年 5 月
Vol.35 No.9 Computer Engineering May 2009
·安全技术· 文章编号：1000—3428(2009)09—0150—03 文献标识码：A 中图分类号：TN918

具有特殊成员的门限签名方案安全性分析

王勇兵，门玉梅，姬龙涛
(河北师范大学附属民族学院，石家庄 050091)

摘 要：门限数字签名是数字签名领域的重要研究内容。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，通过安全性分析，发现它是不安全的，容易受到 3 种伪造攻击。在保持原方案基本属性的基础上对其进行了改进。新方案可以克服 3 种伪造攻击，限制 SDC 的权限，保护签名人的利益，相对于原方案更安全有效。

关键词：门限签名；特殊成员；伪造攻击

Security Analysis of Threshold Signature Scheme with Special Member

WANG Yong-bing, MEN Yu-mei, JI Long-tao
(Nationalities College of Hebei Normal University, Shijiazhuang 050091)

【Abstract】Threshold signature is an important part of digital signature. Through the security analysis of a new(t, n) threshold signature scheme with a special member presented by Miao at the tenth youth communication conference, this paper proposes three kinds of forgery attacks, malicious SDC and the signaturer can forge a valid signature. An improved scheme based on the property of original scheme is proposed and the security weakness of Miao scheme is overcome. In the new scheme, the power of SDC is limited and the benefit of signaturer is protected, so it is more safety and efficient.

【Key words】threshold signature; special member; forgery attack

1 概述

在当今信息化社会中，信息的安全性是至关重要的，密码技术为信息安全提供了重要保证。作为密码学重要组成部分的数字签名在电子商务和电子政务中应用广泛，日益受到人们的关注。数字签名体制的安全性取决于签名密钥，签名密钥的泄露意味着签名安全性的丧失[1]。数字签名与秘密共享[2]结合便产生了门限签名的思想，将签名密钥以门限方式分散给多人管理，可以有效解决密钥的泄露和遗失问题，提高系统的安全性。在(t, n)门限签名方案[3-4]中，群体的签名密钥被 n 个成员共享，使得任意不少于 t 个成员的子集可以代表群体产生签名，而任意少于 t 个成员的子集不能代表群体产生签名。

文献[5]提出了一个有特殊成员的(t, n)门限签名方案(Miao 方案)，它具有“在任意不少于 t 个成员中必须有某个特殊成员的参与才能生成有效签名”的特性，然而笔者发现该方案是不安全的，完全丧失了门限签名思想和有特殊成员参与签名的特性，秘密分发中心可以单独或与签名者(包括特殊成员)合谋产生有效的门限签名，本文提出了 3 种有秘密分发中心参与的伪造攻击，分析了该方案不安全的实质原因并对其进行了改进，分析表明新方案可以抵抗本文提出的各种伪造攻击，有效限制了秘密分发中心的权限，充分保护了签名人的利益。

2 Miao 方案简介

Miao 方案参与者包括秘密分发中心(SDC)，签名团体 $G_S=\{U_1,U_2,\cdots,U_n\}$ 和特殊成员 U_k；整个方案由参数产生、个体签名产生和认证、门限签名产生和认证 3 个阶段组成。

2.1 参数产生阶段

SDC 选择、计算以下参数：

(1)选择 2 个安全的大素数 p 和 q，并且 $p|q-1$；

(2)选择 Z_p^* 中阶为 q 的元素 g；

(3)选择公开的 Hash 函数 $H(.)$；

(4)选择控制参数 $\delta\in_R Z_p^*$，并秘密传送给 U_k，U_k 保密 δ；

(5)选择一个 t-1 次多项式 $f(x)=a_0+\delta+a_1x+\cdots+a_{t-1}x^{t-1} \bmod q$，其中，$a_i\in_R Z_P^*, i=1,2,\cdots,t-1$；

(6)将 $e=a_0$，$d=Y_{G_s}=g^{a_0} \bmod p$ 分别作为签名团体的私钥和公钥；

(7)根据 U_i 的身份标识符 id_i 计算成员私钥 $f(id_i)$ 和公钥 $Y_{U_i}=g^{f(id_i)} \bmod p$。

2.2 个体签名产生和认证阶段

团体中的 t 个签名者 $D=\{U_1,U_2,\cdots,U_k,\cdots,U_t\}$ 用完成以下步骤产生个体签名：

(1) U_i 选取 $t_i\in_R Z_q^*$，计算 $K_i=g^{t_i} \bmod p$，并发送 K_i 给 D 中的其他成员；

(2) U_i 计算 $K=\prod_{i=1}^{t}K_i$，$S_i=t_i-f(id_i)\ L_iH(K,m) \bmod q$，其

基金项目：河北师大附属民族学院科研基金资助重点项目
作者简介：王勇兵(1981－)，男，硕士，主研方向：密码学，信息安全；门玉梅，讲师；姬龙涛，助教
收稿日期：2008-09-30 **E-mail：**wyb723@yahoo.com.cn

中，$L_i=\prod_{j=1,j\neq i}^{t}\frac{-id_i}{id_i-id_j}\bmod q$，并发送 S_i 给 U_k；

(3) U_k 验证 $K_i\overset{?}{=}g^{S_i}Y_{U_i}{}^{L_iH(K,m)}$。

2.3 门限签名的产生和认证阶段

所有个体签名 S_i 被确认后，U_k 计算 $S=\sum_{i=1}^{t}S_i+\delta H(K,m)$，从而产生门限签名 (K,S)，签名验证者可以由以下等式验证签名的有效性：$K=g^{S}Y_{U_i}{}^{H(K,m)}$。

3 伪造攻击

攻击 1 SDC 可以伪造任意消息 m 的有效门限签名。

证明：SDC 自己选择随机数 a_0,δ，利用 $t-1$ 次多项式产生签名人的密钥 $f(id_i)$，$f(id_i)$ 和 δ 对 SDC 来说是已知的，他可以通过以下步骤伪造有效签名：

(1)选择 $t_1,t_2,\cdots,t_t\in_R Z_q^*$，计算 $K_i=g^{t_i}\bmod p$；

(2)计算 $K=\prod_{i=1}^{t}K_i$，$S_i=t_i-f(id_i)\ L_iH(K,m)\bmod q$；

(3)计算 $S=\sum_{i=1}^{t}S_i+\delta H(K,m)$，$(K,S)$ 将是消息 m 的有效签名。很明显 (K,S) 可以通过 $K=g^{S}Y_{U_i}{}^{H(K,m)}$ 的验证。

攻击 2 SDC 可以与特殊成员合谋伪造任意消息 m 的有效门限签名。

证明：他们可以采取和攻击 1 相同的手段伪造有效的门限签名，只需要特殊成员一个人就能产生有效签名，这样违背了“不少于 t 个成员的子集可以代表群体产生签名，而任意少于 t 个成员的子集则不能代表群体产生签名”门限签名的初衷，从而该方案丧失了门限签名的特性。

攻击 3 SDC 可以和签名团体中的任意 t 个普通成员合谋伪造任意消息 m 的有效门限签名。

证明：SDC 可以把特殊成员的控制参数 δ 泄露给 t 个普通成员任何一个人(比如 U_j)，t 个普通成员可以通过以下步骤伪造有效的门限签名：

(1) U_i $(i=1,2,\cdots,t)$ 选取 $t_i\in_R Z_q^*$，计算 $K_i=g^{t_i}\bmod p$，并发送 K_i 给 t-1 个其他成员；

(2) U_i $(i=1,2,\cdots,t)$ 计算 $K=\prod_{i=1}^{t}K_i$，$S_i=t_i-f(id_i)\ L_iH(K,m)\bmod q$，并发送 S_i 给 U_j；

(3) U_j 验证 $K_i\overset{?}{=}g^{S_i}Y_{U_i}{}^{L_iH(K,m)}$，计算 $S=\sum_{i=1}^{t}S_i+\delta H(K,m)$，产生有效的门限签名 (K,S)。同样，(K,S) 可以通过等式 $K=g^{S}Y_{U_i}{}^{H(K,m)}$ 的验证。

攻击 1~攻击 3 充分表明 Miao 方案的安全性是很脆弱的，不适合在开放的网络环境中应用，其中的原因有 3 点：(1)若秘密分发中心是人为操作机构，靠人为自律不如靠方案的绝对安全性，而在现实中也很难找到一个绝对值得信任的机构。若秘密分发中心是网络中的服务器，就很容易成为攻击焦点和通信瓶颈，因为攻破此服务器就意味着可以伪造有效的门限签名。(2)签名人(包括特殊成员)缺少自我保护措施，他们签名的密钥完全依赖 SDC 产生，没有任何签名人自己的相关信息，这就给各种伪造攻击创造了机会，必然损害签名人的利益。(3)签名 (K,S) 没有任何关于签名人的信息，这在一定程度上给攻击者有可乘之机，也不利于仲裁机构解决签名纠纷。

下面从限制秘密分发中心的权限和加强签名人的自我保护 2 个角度对 Miao 方案进行改进，新方案在保持原方案特性的基础上，克服了原方案的安全缺陷。

4 Miao方案的改进

改进方案由原方案的一个 SDC 增加到 m($m\geq 2$)个 SDC，每个 SDC 独立分发密钥，签名人在获得所有 SDC 发送过来的密钥后签名，整个方案由系统初始化、密钥分发、门限签名产生和验证 3 个阶段组成。

4.1 系统初始化

(1)SDC 选择 2 个安全的大素数 p 和 q，并且 $p|q-1$；

(2)SDC 选择 Z_p^* 中阶为 q 的元素 g；

(3)SDC 选择公开的安全 Hash 函数 $H(.)$；

(4)签名人 U_i $(i=1,2,\cdots,t)$ 选取 $k_i\in_R Z_q^*$ 作为私钥，计算相应公钥 $Y_i=g^{k_i}\bmod p$。

4.2 密钥分发

(1)第 i 个 SDC 选择控制参数 $\delta_i\in_R Z_q^*$，并秘密传送给 U_k，U_k 计算 $\delta=\sum_{i=1}^{m}\delta_i$，并保密 δ；

(2)第 i 个 SDC 选择一个 $t-1$ 次多项式 $f_i(x)=a_{i0}+\delta_i+a_{i1}x+\cdots+a_{i(t-1)}x^{t-1}\bmod q$，其中，$a_{ij}\in_R Z_P^*$；

(3)将 $e=\sum_{i=1}^{m}a_{i0}$，$d=Y_{G_s}=g^{e}\bmod p$ 分别作为签名团体的私钥和公钥；

(4)计算成员 U_i $(i=1,2,\cdots,t)$ 的私钥 $f(id_i)=\sum_{j=1}^{m}f_j(id_i)$ 和公钥 $Y_{U_i}=g^{f(id_i)}\bmod p$。

4.3 门限签名产生和验证

设 t 个签名人集合为 $D=\{U_1,U_2,\cdots,U_k,\cdots,U_t\}$，$ASID=\{id_1,id_2,\cdots,id_k,\cdots,id_t\}$ 为实际签名人的标识符，签名消息为 m，具体签名和验证协议如下：

(1) U_i 选取 $t_i\in_R Z_q^*$，计算 $K_i=g^{t_i}\bmod p$，并发送 K_i 给 D 中的其他成员；

(2) 收到所有 K_j $(j=1,2,\cdots,t)$，U_i 计算 $K=\prod_{i=1}^{t}K_i$，$S_i=t_iK-f(id_i)L_i+k_ih(m,AISID)\bmod q$，并发送 S_i 给 U_k；

(3)收到 S_i 后 U_k 验证：

$$K_i{}^{K}Y_i{}^{H(m,ASID)}\overset{?}{=}g^{S_{ii}}Y_{U_i}{}^{L_i} \tag{1}$$

(4)在所有个体签名 S_i 确认后，U_i 计算 $S=\sum_{i=1}^{t}S_i+\delta$，将 $(m,K,S,ASID)$ 作为消息 m 的门限签名；

(5)验证者在收到签名 $(m,K,S,ASID)$ 后，可以用以下等式验证签名的有效性：

$$K^{K}(\prod_{i=1}^{t}Y_i)^{H(m,ASID)}=g^{S}Y_{G_S} \tag{2}$$

5 方案分析

5.1 正确性分析

定理 1 特殊成员 U_k 可以由式(1)验证个体签名 S_i 的有效性。

证明：

$$g^{S_i}Y_{U_i}{}^{L_i}=g^{t_iK-f(id_i)L_i+k_iH(m,ASID)}g^{f(id_i)L_i}=g^{t_iK+k_iH(m,ASID)}=K_i{}^{K}Y_i{}^{H(m,ASID)}$$

定理 2 验证者可以由式(2)验证门限签名 $(m,K,S,ASID)$ 的有效性。

证明：由式(1)易知

$$g^{\sum_{i=1}^{t}S_i}\ g^{\sum_{i=1}^{t}f(id_i)} = g^{\sum_{i=1}^{t}S_i}\ g^{e+\delta} = g^{S-\delta}g^{e+\delta} = g^{S}Y_{G_S} = K^{K}(\prod_{i=1}^{t}Y_i)^{H(m,ASID)}$$

5.2 安全性分析

多个 SDC 可以提高系统强安全性。原方案借助一个 SDC 分发密钥，理想状态下 SDC 是值得信赖的，但实际应用中就不一定了，SDC 可以轻而易举伪造签名；改进的方案由一个 SDC 增加至多个 SDC，单个 SDC 要伪造签名是不可能的，因为签名者私钥和特殊成员控制参数均有 m 个部分组成，若多个 SDC 中有一个 SDC 是可信的，就可以防止 SDC 的勾结，提高了系统的安全性；若 SDC 为网络中的服务器，多个 SDC 的存在分散了攻击者的攻击力度，攻击者即使攻破某几个 SDC，对伪造签名毫无帮助；另外，若只需要确保方案一般安全性，可以继续使用一个 SDC，无须修改。

该方案可以抵抗本文提出的 3 种伪造攻击。新方案在采用多个 SDC 基础上重新使用了签名者的私钥 k_i，保证了签名人的合法权利。由式(2)知签名 S_i 使用了 t_i，$f(id_i)$ 和 k_i 3 个秘密信息，即使所有 SDC 联合起来也只能知道 $f(id_i)$，而不知道 t_i，k_i；同理，SDC 和某几个签名人合谋也不能伪造，系统外的攻击者伪造签名就更不可能了。

方案可以有效解决签名纠纷。签名中嵌入了签名人的身份信息 *ASID*，并且 *ASID* 不能修改或伪造，它受安全 Hash 函数保护，在出现签名纠纷时，仲裁机构根据 *ASID* 可以很容易找到实际签名人，从而解决纠纷.

方案保证了 t 个签名人中有特殊成员的特性。原方案中 SDC 可以和 t 个普通签名人合谋产生有效门限签名，避开了特殊成员的参与，丧失了有特殊成员参与签名的特性，此与 Miao 方案的设计初衷相违背，新方案可以抵抗 SDC 发起的各种伪造攻击，保证了 t 个签名人中有特殊成员。

5.3 效率分析

对改进方案签名生成和验证阶段的计算复杂度和门限签名长度分析可知，它们均与签名人的个数有关，适合 t 较小的应用，对于门限值人 t 较大的情况，可以在确保特殊成员参与的基础上采用“代表中选代表”的方式使得最后参与签名的人数 t 不是很大。

计算复杂度和签名长度分别见表 1、表 2。

表 1 计算复杂度

运算名称	幂运算	模乘运算	加减运算	Hash 运算
签名生成	$5t$	$5t$-3	$3t$	$2t$+1
签名验证	4	T+1	0	1

表 2 签名长度

门限签名	签名长度
(*m*, *K*, *S*, *ASID*)	$\|m\|+p+q+t$

6 结束语

文献[5]的(t,n)门限签名方案在股份制公司中股东对某文件进行表决时，往往每次表决都需要控股最多的股东(特殊成员)参与，否则表决无效。本文对 Miao 方案进行密码学分析，发现其只具有理想状态下的安全性，容易受到由 SDC 发起的各种伪造攻击，在保持其原有特性基础上对其进行了改进，新方案克服了原方案的安全缺陷，保证了有特殊成员参与签名，有效限制了 SDC 的权限，充分保护了签名人的利益，从而新方案更安全、有效、实用。Miao 方案只有一个特殊成员，在实际应用中有一定的局限性，如何设计有多个特殊成员参与的(t,n)门限签名方案是值得进一步研究的问题。

参考文献

[1] Mehta M, Harn L. Efficient One-time Proxy Signature[J]. IEE Proceedings of Communication, 2005, 152(2): 129-133.

[2] 马春波，何大可. 基于秘密共享的代理多重签名方案[J]. 计算机工程, 2006, 32(2): 40-41, 90.

[3] 王贵林，卿斯汉. 几个门限群签名方案的弱点[J]. 软件学报, 2000, 11(10): 1326-1332.

[4] 谢 琪. 两种门限签名方案的密码学分析及其改进[J]. 通信学报, 2005, 26(7): 123-128.

[5] 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.

编辑 张正兴

（上接第 149 页）

[5] Jha S, Sheyner O, Wing J. Two Formal Analyses of Attack Graphs[C]//Proceedings of the 15th IEEE Computer Security Foundations Workshop. Cape Breton, Nova Scotia, Canada: IEEE Computer Society, 2002: 49-63.

[6] Noel S, Jajodia S, O'Berry B, et al. Efficient Minimum-cost Network Hardening via Exploit Dependency Graphs[C]// Proceedings of the 19th Annual Computer Security Applications Conference. Las Vegas, Nevada, USA: [s. n.], 2003.

[7] Ritchey R, O'Berry B, Noel S. Representing TCP/IP Connectivity for Topological Analysis of Network Security[C]//Proceedings of the 18th Annual Computer Security Applications Conference. Las Vegas, Nevada, USA: [s. n.], 2002.

[8] Ou Xinming, Boyer W F, McQueen M A. A Scalable Approach to Attack Graph Generation[C]//Proceedings of the 13th ACM Conference on Computer and Communications Security. [S. 1.]: ACM Press, 2006: 336-345.

[9] Ou Xinming, Govindavajhala S, Appel A W. MulVAL: A logic-based Network Security Analyzer[C]//Proceedings of the 14th USENIX Security Symposium. Baltimore, MD, USA: [s. n.], 2005.

[10] Li Wei. An Approach to Graph-based Modeling of Network Exploitations[D]. Florida, USA: Department of Computer Science and Engineering, Mississippi State University, 2005.

[11] Lippmann R, Ingols K. An Annotated Review of Past Papers on Attack Graphs[Z]. MIT Lincoln Laboratory, 2005-03.

编辑 索书志