一种高效的可验证的门限签名方案*

甘元驹** 施荣华

(中南大学信息科学与工程学院 长沙 410075)

【摘要】针对现有的(t,n)门限签名方案中所存在的当群内任何t个或更多个秘密分享成员联合攻击，能暴露系统的秘密密钥的问题，设计了一种能抵制群内成员联合攻击的可证实的具有系统稳定性的门限签名方案。该方案的安全性是基于求离散对数和RSA大整数因式分解的困难，其群签名长度和群签名的验证时间只相当于一般个人签名。

关 键 词 门限群签名; 可验证性; 高效性; 离散对数; 因式分解问题

中图分类号 TP309 文献标识码 A

An Efficient and Verifiable Threshold signature Scheme

Gan Yuanju Shi Ronghua

(College of information science and engineering, Central South University ChangSha 410075)

Abstract Group oriented (t,n) threshold digital signature schemes have a problem in that the underlying signature schemes will be broken if any t or more shadowholders conspire together with each other,thus the group secret key will be revealed.The new scheme proposed by us can avoid the conspiracy attack.It is based on the difficulty of computing the discrete logarithm modulo for a composite number and the factorization problem of large integer.The size of the group signature and verification time of the group signature are equivalent to that of an individual signature.

Key words threshold group signature; verification; efficiency; discrete logarithm; factoring problem

文献[1]提出了一种基于RSA的(t,n)门限群签名方案，该方案仅有t个或更多个成员才能代表群签名，任何小于t个或更少个的参与者是不能伪造群签名。而Li[2]指出在这种方案中，当t个或更多个成员合谋就能得到系统秘密密钥，并还可进一步得到每个成员的秘密密钥。为了解决这种合谋攻击，在Li[3]所提出的方案中，在每个成员的私钥中附加了一个随机数，这样该方案就能防止合谋攻击。然而Michels[4]详细讨论了Li[3]方案中，(n–t+1)个成员如何合谋以伪造一个有效的群签名。同时Michels在该文中还分析了Harn[5]方案同样不能抵制合谋攻击和伪造签名攻击。Wang[6]指出Xu[7]的门限签名方案同样不能防止伪造签名，且系统强壮性和稳定性差等特点。为考虑对以上问题的研究，设计了一个基于RSA门限签名[2,7]与离散对数签名和门限签名[3,5]相结合的高效的可证实[8]能抵制群内成员联合攻击的(t,n)门限群签名方案。

1 新的门限群签名方案

新的(t,n)门限群签名方案的设计。假设有一个可信任的秘密分发中心SDC，由系统初始化、秘密影子的生成与验证、部分签名生成及验证和群签名的生成及验证，具体定义及四个阶段构成如下：

2002年9月3日收稿

* 国家自然科学基金资助项目，编号：60173041

** 男 28岁 硕士 讲师 主要从事电子商务安全、密码协议分析和网络安全方面的研究

定义1 可信任秘密分发中心SDC (Share Distribute Center)指将一个或多个秘密分给t个秘密分享者。可信任也就暗含了SDC一定能确保秘密信息不会泄露。

定义2 公告栏(NB)指存放公开参数或数据的媒介，系统各方均可访问公告栏上的内容，但只有SDC才能修改或更新公告栏上的内容。

1.1 系统初始化

不失一般性，假设一个群体中有n个成员，用A表示该群体的所有成员，该群体中任何t个或t个以上成员可代表该群体进行签名，用B表示，可知B是A的子集，且大小为t。

SDC选择参数如下：

$N=pq$，其中p和q都是安全大素数，即存在p'和q'，使$p=2p'+1$和$q=2q'+1$，且p'和q'也都是安全大素数；

一个Z_N^*中阶为$v=p'q'$的生成器g；

选择系统一公开数值e, 使$\gcd(e,v)=1$，且$ed=1 \bmod v$，d是系统的一个秘密数值；

一个强单向hash函数$h()$；一个次数为$t-1$的秘密多项式 $f(x)=c_{t-1}x^{t-1}+\cdots+c_1x+c_0 \bmod v$；

一个系统的密钥 $x=f(0) \bmod v$和系统公钥 $y=g^x \bmod N$。

于是SDC在公告栏上公布e, y, N, g和$h()$, 并将d, x, v, p, q, p'和q'保密。

1.2 秘密影子的生成与验证

对于各个成员U_i，SDC选择化名ID_i，并保证各个ID_i互异，保存U_i与ID_i之间的对应关系，以便可进行追踪。SDC并在公告栏上公布 $f_k=g^{c_k} \bmod N$ (其中$k=0,1,\cdots,t-1$)。然后分别按下面给出的方程计算每个U_i的私钥 $x_i=(g^{f(ID_i)})^d \bmod N$ 和公钥 $y_i=g^{f(ID_i)} \bmod N$。最后SDC利用一可靠信道把每一个人的私钥与公钥安全地送给其拥有者。对于每个参与者，可以验证方程 $y_i=x_i^e \bmod N, y_i=\prod_{j=0}^{t-1} f_j^{(ID_i^j)} \bmod N$, 是否成立及判别SDC给出是否为有效密钥。

定理1 如果方程 $y_i=x_i^e \bmod N, y_i=\prod_{j=0}^{t-1} f_j^{(ID_i^j)} \bmod N$ 成立，则分享者得到的为有效秘密影子。

证明 对于方程$y_i=x_i^e \bmod N$，验证x_i, y_i是否为一对合法的RSA私钥与公钥。

$$\prod_{j=0}^{t-1} f_j^{(ID_i^j)} \bmod N \equiv \prod_{j=0}^{t-1} (g^{c_j})^{(ID_i^j)} \bmod N \equiv$$

$$\prod_{j=0}^{t-1} g^{(ID_i^j)\cdot c_j} \bmod N \equiv g^{f(ID_i)} \bmod N = y_i$$ 证毕

1.3 部分签名生成与验证

若t个成员构成的小组B同意代表群体对消息m签名，那么每个成员U_i选择一个随机数k_i，并计算 $r_i=g^{k_i\cdot e} \bmod N$，将$r_i$通过广播信道发送出去，当每个$U_i$都收到其他成员的$r_i$后，$B$中的成员$U_i$计算 $R=\prod_{i\in B} r_i \bmod N$，然后$U_i$用自己的私钥$x_i$和随机数$k_i$对$m$签名：$s_i=(x_i)^{h(m,R,B)\prod_{j\in B, i\neq j}\frac{0-ID_j}{ID_i-ID_j}} g^{k_i} \bmod N$，$U_i$将$\{r_i,s_i\}$发送给一个既定的签名合成者DC(Designated Combiner)(该成员可由群内中的任何成员充当)，DC可根据下面方程是否成立来验证每个部分签名是否有效

$$s_i^e=(y_i)^{h(m,R,B)\prod_{j\in B, i\neq j}\frac{0-ID_j}{ID_i-ID_j}} r_i \bmod N \tag{1}$$

定理2 如果方程式(1)成立，那么U_i的部分签名$\{r_i,s_i\}$为有效签名。

证明 $$s_i^e \equiv (x_i)^{e\cdot h(m,R,B)\prod_{j\in B, i\neq j}\frac{0-ID_j}{ID_i-ID_j}} g^{k_i\cdot e} \bmod N \equiv (g^{f(ID_i)\cdot d})^{e\cdot h(m,R,B)\prod_{j\in B, i\neq j}\frac{0-ID_j}{ID_i-ID_j}} g^{k_i\cdot e} \bmod N \equiv$$

$$(g^{f(ID_i)})^{h(m,R,B)\prod_{j\in B, i\neq j}\frac{0-ID_j}{ID_i-ID_j}} r_i \bmod N \equiv (y_i)^{h(m,R,B)\prod_{j\in B, i\neq j}\frac{0-ID_j}{ID_i-ID_j}} r_i \bmod N$$ 证毕

1.4 群签名生成与验证

若所有的$\{r_i, s_i\}$，其中$i\in B$，都是有效签名，则DC生成消息m的群签名$\{R, S, B\}$，其中$S=\prod_{i\in B} s_i \bmod N$，要验证对消息$m$的群签名$\{R, S, B\}$是否有效时，验证者只需用群公钥$y$验证下面方程是否成立来确定群签名是

否有效

$$S^e \equiv y^{h(m,R,B)} R \bmod N \tag{2}$$

定理3 若方程式(2)成立，则群体对消息m的签名$\{R, S, B\}$为有效签名。

证明 $S^e \equiv (\prod_{i\in B} s_i)^e \bmod N \equiv \prod_{i\in B}(y_i)^{h(m,R,B)\prod_{i\in B, i\neq j}\frac{0-ID_j}{ID_i-ID_j}} r_i \bmod N \equiv$

$$\prod_{i\in B}(g^{f(ID_i)})^{h(m,R,B)\prod_{j\in B, i\neq j}\frac{0-ID_j}{ID_i-ID_j}} \prod_{i\in B} r_i \bmod N \equiv \prod_{i\in B}(g^{h(m,R,B)\cdot f(ID_i)\cdot\prod_{j\in B, i\neq j}\frac{0-ID_j}{ID_i-ID_j}}) R \bmod N \equiv$$

$$g^{h(m,R,B)\cdot\sum_{i\in B}(f(ID_i)\cdot\prod_{j\in B, i\neq j}\frac{0-ID_j}{ID_i-ID_j})} R \bmod N$$

由Lagrange插值公式得

$$S^e \equiv g^{f(0)\cdot h(m,R,B)} R \bmod N \equiv y^{h(m,R,B)} R \bmod N$$

证毕

由上面的定理可知，只要方程式成立，验证者相信群体对消息m的群签名$\{R, S, B\}$是有效签名。由于B中是U_i的化名，因而验证者并不知道签名者的真正身份，因而签名者对验证者是匿名的。当签名发生纠纷时，可由SDC追查出签名者的真实身份，因而该方案具有可追查性。

2 特性分析

2.1 安全性分析

上述方案的安全性是基于大整数分解和离散对数的困难性，因此在计算上安全。下面分析该方案的一些可能攻击：

攻击1 非群内成员的攻击者试图从群公钥y中得到群秘密密钥x

由于该攻击者是非群内成员，则得到x的最可能的途径是从方程$y=g^x \bmod N$求出x，这就意味着他将面对求解离散对数问题。

攻击2 群中任意t个成员合谋，试图得到群秘密密钥$x=f(0) \bmod v$

对于群内的每个成员U_i，都有相应的私钥$x_i = g^{f(ID_i)\cdot d} \bmod N$和公钥$y_i = g^{f(ID_i)} \bmod N$。$t$个成员可以生成一个有效的群签名，但为了获得群秘密密钥，将有可能采取从每个人的x_i或y_i中求出$f(ID_i)$，利用t个不同的$f(ID_i)$值求出$f(0)$；若要得到$f(ID_i)$的值，同攻击1一样，同样会面对求解离散对数问题。因此合谋是不可能得到系统秘密密钥x，可见该方案能有效防止群内成员合谋攻击。

攻击3 成员U_i，U_i'与DC合谋，将某成员U_i部分签名用U_i'的代替，使群签名$\{m,R,S,B\}$变为$\{m, R', S', B'\}$[4]，其中$U_i \in B, U_i' \notin B, B \subset A$, $R'=R$, $S'=S/s_i*s_i'$, $B'=B-U_i+U_i'$。

在这种情况下，验证者将会拒绝B'签名。因为$E=h(m,R,B)$包括子组B中签名者的信息，对于其他签名者，所签名的消息是$E=h(m,R,B)$。而对于验证者，计算的则是$E'=h(m,R',B')$，由于$E \neq E'$，因此$S'^e \equiv y^{E'} R' \bmod N$是不可能成立的。该方案能防止伪签名攻击，既防冒充性，又是任何小组不能假冒其他小组生成签名。

攻击4 DC或其他攻击者试图获取成员的私钥x_i

由于$x_i=(y_i)^d \bmod N$，要获取成员私钥，必须知道d的值。但是，攻击者是不可能从公布的e中算出d，除非DC或其他攻击者解决了大整数的因式分解难题。

2.2 稳定性分析

综上所述，在该方案中，加入新成员U_i，SDC只需要选择化名的身份值ID_i，并将秘密密钥$x_i = g^{f(ID_i)\cdot d} \bmod N$和公开密钥$y_i = g^{f(ID_i)} \bmod N$发送给他即可，而系统和老成员的相关参数不必改动。删除成员时，只需要将ID通知其他成员为无效ID。由于该方案具有强壮性和防冒充性，即使有$(t-1)$个旧成员已退出系统，而某个成员购买了秘密密钥，这个成员既不能伪造签名，也不能获取系统密密参数。

2.3 性能分析

在验证群签名的时间复杂性上，与Li[3]，Harn[8]以及Xu[7]的方案进行比较，结果如表1所示。

表1 方案对比

方案	乘法次数	求模指数次数	求逆次数
Ours cheme	1	2	—
Li	t+2	t+2	—
Harn	t	2t+3	t–1
Xu	t	2	—

综上所述，上述方案在群签名验证时间是很高效，基本上只相当于一般个人签名的验证时间。在存储空间上，每个成员由于只有一个公钥和私钥，其空间代价为2|*N*|，|*N*|表示整数*N*的位长。

3 结 束 语

本文所提出的(*t*,*n*)门限群签名方案，既是一种RSA和离散对数门限群签名的设计思想，也是一种具有良好特性的可验证门限群签名方案。该方案最大的特点是签名验证简单而且计算量少，并具有匿名性、可追踪性和系统稳定性等优点。并在安全和效率上都优于Li，Harn和Xu的方案。在实际运用中，该方案是一种很有前景的方案。

参 考 文 献

[1] Desmedt Y, Frankel Y. Shared generation of authenticators and signatures. In:Feigenbaum J ed. Advances in Cryptology—Crypto' 91 Proceedings. Berlin:Springer-Verlag, 1992: 457-469

[2] Li C, Hwang T, Lee N. Remark on the threshold RSA signature scheme. In:Stinson D R ed. Advances in Cryptology—Crypto'93 Proceedings. Berlin: Springer-Verlag, 1994: 413-419

[3] Li C, Hwang T, Lee N. Threshold-multisignature schemes where suspected forgery implies traceability of adversarial shareholders. In: SantisA D ed. Advances in Cryptology ——Eurocrypt'94 Proceedings. Berlin:Springer-Verlag, 1995: 194-204

[4] Michels M, Horster P. On the risk of disruption in several multiparty signature schemes. In:Feigenbaum J ed. Advances in Cryptology ——CRYPTO'96 Proceedings. Berlin:Springer-Verlag, 1997: 334-345

[5] Harn L. Group-oriented (t, n)threshold digital signature scheme and multisignature. IEE Proceedings, Computers and Digital Techniques, 1994, 141(5): 307-313

[6] 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): 1 326-1 332

[7] 徐秋亮. 改进门限RSA数字签名体制[J]. 计算机学报, 2000, 23 (5): 449-453

[8] Harn L. Digital signature with(t, n)shared verification based on discrete Logarithms. Electron Lett., 1995, 31 (3): 177-185

编 辑 刘文珍