两种群签名方案的安全性分析

陈艳玲　　陈鲁生　　符方伟
(南开大学数学科学学院　天津　300071)

摘　要：群签名允许群成员以匿名的方式代表整个群体对消息进行签名。而且，一旦发生争议，群管理员可以识别出签名者。该文对 Posescu (2000)群签名方案和 Wang-Fu (2003)群签名方案进行了安全性分析，分别给出一种通用伪造攻击方法，使得任何人可以对任意消息产生有效群签名，而群权威无法追踪到签名伪造者。因此这两个方案都是不安全的。

关键词：群签名，伪造攻击，不关联性
中图分类号：TN918　　**文献标识码**：A　　**文章编号**：1009-5896(2005)02-0235-04

Security Cryptanalysis of Two Group Signature Schemes

Chen Yan-ling　　Chen Lu-sheng　　Fu Fang-wei
(*College of Mathematical Science, Nankai University, Tianjin* 300071, *China*)

Abstract　Group signature schemes allow a group member to anonymously sign on group's behalf. Moreover, in case of anonymity misuse,a group manager can recover the issuer of a signature. This paper analyzes the security of two group signature schemes recently proposed respectively by Posescu (2000) and Wang Xiaoming (2003), and shows that both schemes are universally forgeable, that is, anyone (not necessarily a group member) is able to produce a valid group signature on an arbitrary message, which cannot be traced by the group manager. So both schemes are insecure.

Key words　Group signature, Forgery attack, Unlinkability

1　引言

1991 年，Chaum 和 Heyst[1]首次提出了群签名(group signature)的概念。在这个特殊的数字签名中，群体中的任意一个合法成员可以以匿名的方式代表整个群体对消息进行签名。与其他数字签名一样，群签名是可以公开验证的，而且可以只用单个群公钥进行验证。一旦发生争议,签名者能被群成员一起或群权威被识别出来。所以一个群签名方案必须满足以下 3 条性质：(1)只有群成员才能对消息进行签名。(2)签名的接受者可以验证该签名是否为该群的有效签名，但不能识别出是群中哪个成员签的名。(3)一旦以后对签名发生争议，群权威能根据该签名识别出签名者。由于群签名能为群签名人提供很好的匿名性，同时在必要的时候又可以通过权威机构来撤销匿名性，再加上其他性能，使得群签名在诸如电子商务中的电子支付系统，电子拍卖系统，电子彩票系统等方面有着广泛的应用前景，因此一个群签名的安全性便显得越发的重要。

在分析前人提出的方案的优缺点的基础上，1998 年，Tseng 和 Jan[2]提出来一个基于标志符(ID)的群签名方案(T-J 群签名方案一)。与此同时，Lee 和 Chang[3]提出了一个高效的群签名方案(Lee-Chang 方案)。但这两个方案都是不安全的。1999 年，Tseng 和 Jan[4]对 Lee-Chang 方案进行改进,改进的方案(T-J 群签名方案二)满足了不相关性，但仍然不能抵抗伪造攻击。2000 年，Popescu[5]对 TJ 群签名方案一进行分析，并提出了改进方案(Posescu 群签名方案)，其安全性基于 e 次方根问题和离散对数问题。2003 年，王晓明和符方伟[6]对 T-J 群签名方案二进行了安全性分析，提出来一个新的群签名方案(Wang-Fu 群签名方案)，并声称方案是安全的。本文对 Posescu 群签名方案和 Wang-Fu 群签名方案进行分析并得出如下结论：它们不满足群签名的性质(1)和(3)，在这两个方案中，任何人可以对任意消息产生有效签名，而群权威无法追踪伪造签名者，因此这两个方案仍然都是不安全的。

2　群签名基本知识

定义 1　一个群签名方案是包含如下过程的数字签名方案:

(1) 创建　一个用以产生群公钥和私钥的多项式时间概率算法。该算法的输入是包含安全参数在内的一些公共参数，输出为群公钥和相关私钥。

(2) 加入　一个用户和群管理人之间的使用户成为群成员的交互式协议。执行该协议可产生群成员的私钥和成员证

2003-10-09 收到，2004-03-09 改回
国家自然科学基金（60172060）资助课题

书, 并使群管理人得到群成员的秘密的成员管理钥。

(3) 签名 一个概率算法,当输入一个消息, 群公钥, 群成员证书和相关私钥后, 输出对消息的签名。

(4) 验证 一个在输入对消息的签名及群公钥后确定签名是否有效的算法。

(5) 打开 一个在给定一个消息签名对和群私钥的条件下确定签名人身份的算法。

定义 2 一个好的群签名应满足以下的安全性要求:

(1) 正确性 一个由签名算法生成的群签名必须能被验证算法所接受。

(2) 匿名性 给定一个消息的群签名后, 除了群权威外对任何人来说, 确定签名者的身份在计算上是不可行的。

(3) 不关联性 在不打开签名的情况下,任意给定几个对同一消息或不同消息的群签名, 确定这几个签名是否为同一个群成员所签署在计算上是不可行的。

(4) 防伪造性 只有群成员才能生成被验证算法所接受的有效签名。

(5) 防陷害攻击 包括群管理人在内的任何人都不能以其他群成员的名义产生合法的群签名。

(6) 可追踪性 群权威在必要时总可以打开有效签名以确定出签名人的身份, 而且签名人不能阻止一个合法签名的打开。

(7) 抗联合攻击 即使一些群成员串通在一起也不能产生一个合法的不能被追踪的群签名。

定义 3 一个群签名方案的效率主要依赖于以下参数:

(1) 群公钥的大小; (2) 群签名的长度; (3) 群签名算法和验证算法的效率; (4) 创建、加入以及打开过程的效率。

3 Posescu 群签名方案的介绍和分析

3.1 Posescu 群签名方案的介绍

(1) 群创建 (a) 可信中心(Trusted Authority,TA)选取两个大素数 p, q, 满足 $(p-1)/2,(q-1)/2$ 为奇数且互素。令 $n=pq$, 使 Jacobi 符号 $2/n=-1$, 以使 TA 易求模 p 和 q 的离散对数。(b) TA 选取大整数 e 满足 $(e,\varphi(n))=1$, 并计算 d 满足 $ed\equiv 1(\mathrm{mod}\varphi(n))$。(c) TA 选取 $g\in Z_n^*$, 其阶很大, 使得 Z_n^* 上以 g 为底的离散对数问题难解。(d) TA 选取安全的 Hash 函数 h, 公开 h。(e) 群权威(Group Manager, GM)选择 $x\in Z_q^*$ 作为私钥, 计算 $y=g^x \bmod n$ 作为公钥。

群的公开参数为 (n,e,g,y), 秘密参数为 (p,q,x)。

(2) 新成员加入 当 U_i (假设其识别信息为 ID_i)想成为群的一个成员,需进行如下步骤: (a) TA 计算 $s_i=\mathrm{ID}_i^d \bmod n$。

(b) GM 计算 $x_i=(\mathrm{ID}_i+eg)^x \bmod n$。

用户 U_i 的成员证书为 (s_i,x_i)。

(3) 群签名的产生 设待签消息为 m, U_i 选取随机数 r_1,r_2, 并计算: $A=y^{r_2 e} \bmod n$, $B=x_i y^{s_i+r_1} \bmod n$, $C=x_i y^{r_2} \bmod n$, $D=s_i h(m\|A)+r_1 h(m\|A)$。消息 m 的签名为 (A,B,C,D)。

(4) 群签名的验证 验证同余式 $C^{eh(m\|A)}y^{eD}\equiv B^{eh(m\|A)}\cdot A^{h(m\|A)}(\mathrm{mod}\,n)$ 是否成立。若上式成立,则签名为有效签名。

(5) 识别签名者 一旦发生争议,需要打开某一个群签名, 则对每一个群成员 U_i, 这里 $i=1,2,\cdots,k$。k 是群成员个数, 群权威 GM 检验 U_i (其身份信息为 ID_i)是否满足同余式:

$$(\mathrm{ID}_i+eg)^{xe}\equiv C^e A^{-1}(\mathrm{mod}\,n)$$

使上述同余式成立的 ID_i 即为签名者的身份信息。

3.2 Posescu 群签名方案的安全性分析

3.2.1 匿名性不关联性的分析 对每个群成员 U_i, 其成员证书为 (s_i,x_i)。若他以群的名义对消息 m 产生的群签名为 (A,B,C,D), 则由 $A=y^{r_2 e} \bmod n$, $C=x_i y^{r_2} \bmod n$, 易得出: $x_i^e\equiv C^e A^{-1}(\mathrm{mod}\,n)$。

显然, 同一签名者对两个不同消息 m_1, m_2 的群签名 (A_1,B_1,C_1,D_1), (A_2,B_2,C_2,D_2) 满足 $x_i^e\equiv C_1^e A_1^{-1}\equiv C_2^e A_2^{-1}(\mathrm{mod}\,n)$, 即 $C_1^e A_2\equiv C_2^e A_1(\mathrm{mod}\,n)$。

更精确地,由 $D=s_i h(m\|A)+r_1 h(m\|A)=(s_i+r_1)h(m\|A)$, 可得 $(s_i+r_1)=D/h(m\|A)$。而 $B=x_i y^{s_i+r_1} \bmod n=x_i y^{D/h(m\|A)}\cdot \bmod n$, 则有 $x_i=B(y^{D/h(m\|A)})^{-1} \bmod n$。从而对任意两个不同的消息签名对 m_1, (A_1,B_1,C_1,D_1) 和 m_2, (A_2,B_2,C_2,D_2) 有

$$B_1(y^{D_1/h(m_1\|A_1)})^{-1} \bmod n=x_i$$

$$B_2(y^{D_2/h(m_2\|A_2)})^{-1} \bmod n=x_j$$

显而易见, 当 $x_i=x_j$ 时, 这两个群签名由同一个群成员所签署。

可以看出, 攻击者很容易由签名者识别阶段建立 x_i^e 和 ID_i 的一一对应表。由于争议发生, 被 GM 公开的签名者 ID_i 其在公开之前和公开之后所签署的群签名都可以很容易被识别出来。从而群签名的匿名性不被满足。而且, 同一签名者的任意两个不同的群签名有着直接的关联关系, 任何人一旦得到一个签名者的群签名, 那么该签名者的任何其它群签名都可以通过上述关联关系被识别出来。显然群签名的不关联性也不被满足, 即 Posescu 群签名方案不满足群签名定义 2: 安全性要求中的(1)和(3): 匿名性和不关联性。

3.2.2 对 Posescu 群签名方案的伪造攻击 用这种攻击方法, 任何人都能对任意消息产生有效的群签名, 而且群权威无法追踪到签名者。假设攻击者为 Alice, 产生有效的群签名过程如下:

Alice 任意选取随机数 x_i,k,b,d, 令 $a=ke$。计算: $A=y^a \bmod n$, $B=x_i y^b \bmod n$, $C=x_i y^d \bmod n$, $D=(b-d+$

$k)h(m\|A)$。消息 m 的签名即为 (A,B,C,D)。

上述伪造的群签名是有效的，能通过验证算法的验证。这是因为

$$\begin{aligned}C^{eh(m\|A)}y^{eD} &\equiv x_i^{eh(m\|A)}y^{deh(m\|A)}y^{e(b-d+k)h(m\|A)}(\mathrm{mod}\,n)\\ &\equiv x_i^{eh(m\|A)}y^{beh(m\|A)+keh(m\|A)}(\mathrm{mod}\,n)\\ &\equiv (x_iy^b)^{eh(m\|A)}y^{keh(m\|A)}(\mathrm{mod}\,n)\\ &\equiv B^{eh(m\|A)}y^{ah(m\|A)}(\mathrm{mod}\,n)\\ &\equiv B^{eh(m\|A)}A^{h(m\|A)}(\mathrm{mod}\,n)\end{aligned}$$

伪造签名满足验证方程，所以 (A,B,C,D) 是一个有效的群签名。

3.2.3　可追踪性的分析　一旦发生争议，伪造签名需被打开时，群权威 GM 对每一个群成员 U_j (其身份信息为 ID_j)检验式子 $(\mathrm{ID}_j+eg)^{xe}\equiv C^eA^{-1}(\mathrm{mod}\,n)$ 是否成立。而此时有

$$C^eA^{-1}\equiv x_i^{\,e}y^{de}y^{-ke}\equiv x_i^{\,e}y^{(d-k)e}(\mathrm{mod}\,n)$$

由于 x_i,d,k 都是随机选取的，同一个签名伪造者在多次伪造签名时，可以选取不同的 x_i,d,k，从而得到不同的值 $C^eA^{-1}\,\mathrm{mod}\,n$。从这个角度看，即使是同一个签名伪造者伪造的多个消息签名对，打开时满足识别方程所需的身份信息也不相同，很可能，每一个群成员的身份信息 ID_j 均不满足上述识别方程。

若对每一个群成员 U_j，其对应身份信息 ID_j 都不满足识别方程，则显然群权威 GM 不能确定出签名者的身份，从而 Posescu 群签名不能满足群签名定义 2：安全性要求中的(6)可追踪性。若存在某个群成员 U_j，其对应身份信息 ID_j 满足识别方程，则此时相当于签名伪造者以群成员 U_j 的名义产生合法签名，让 U_j 百口莫辩。而这时群权威 GM 识别出的签名者却并非真正的签名者。所以，Posescu 群签名既不满足群签名定义 2：安全性要求中的(4)和(6)：防伪造性和可追踪性，(5)防陷害攻击也不能得到保障。

4　Wang-Fu 群签名方案的介绍和分析

4.1　Wang-Fu 群签名方案的介绍

(1) 群创建　(a) p,q 为两个大素数，且 $q|(p-1)$，g 是 GF(p) 中阶为 q 的生成元。公开 p,q,g。

(b) 安全的 Hash 函数 h，公开 h。

(c) 群权威 GM 选择 $x_T\in Z_q^*$ 作为私钥，计算 $y_T=g^{x_T}\,\mathrm{mod}\,p$ 作为公钥。

(d) 群中的每一个成员选择随机数 $x_i\in Z_q^*$ 作为私钥，计算 $y_i=g^{x_i}\,\mathrm{mod}\,p$ 作为公钥。

(2) 新成员加入　当 U_i 想成为群的一个成员，需进行如下步骤：(a) GM 随机选取 $k_i\in Z_q^*$，并计算 $r_i=g^{-k_i}y^{k_i}\,\mathrm{mod}\,p$，$s_i=(k_i-r_ix_T)\,\mathrm{mod}\,q$，GM 秘密送 (s_i,r_i) 给 U_i，并存储 (s_i,r_i,k_i)。

(b) U_i 接到 (s_i,r_i) 后，验证同余式 $g^{s_i}y_T^{\,r_i}r_i\equiv(g^{s_i}y_T^{\,r_i})^{x_i}(\mathrm{mod}\,p)$ 是否成立。如上式成立，U_i 接收 (s_i,r_i)。(s_i,r_i) 即为群成员 U_i 的签名钥。

(3) 群签名的产生　设待签消息为 m，U_i 随机选取 $a,t,b,d\in Z_q^*$，并计算：

$$C=(r_ia-d)\,\mathrm{mod}\,q,\quad A=y_i^{\,b}\,\mathrm{mod}\,p,\quad D=g^b\,\mathrm{mod}\,p$$

$$E=r_i^{\,a}(1+g^{-s_ia}y_T^{-r_ia})^{x_i}\,\mathrm{mod}\,p,\quad F=y_T^d\,\mathrm{mod}\,p$$

$$B=(s_ia-bh(A\|C\|D\|E\|F)+bh(E\|D\|F))\,\mathrm{mod}\,q$$

$$\alpha_i=(D^{h(E\|D\|F)}+g^By_T^CFD^{h(A\|C\|D\|E\|F)})\,\mathrm{mod}\,p$$

$$R=\alpha_i^{\,t}\,\mathrm{mod}\,p,\quad S=t^{-1}(h(m\|R)-x_iR)\,\mathrm{mod}\,q$$

U_i 将 (S,R,A,B,C,D,E,F,m) 送给签名验证人。

(4) 群签名的验证　群签名验证人首先计算：

$$\alpha_i=(D^{h(E\|D\|F)}+g^By_T^CFD^{h(A\|C\|D\|E\|F)})\,\mathrm{mod}\,p$$

$$\delta_i=A^{h(E\|D\|F)}(\alpha_iD^{-h(E\|D\|F)}-1)E\,\mathrm{mod}\,p$$

(b) 验证同余式 $\alpha_i^{\,h(m\|R)}\equiv\delta_i^{\,R}R^S(\mathrm{mod}\,p)$ 是否成立。如果上式成立，则 (S,R,A,B,C,D,E,F,m) 是 U_i 对消息 m 的有效签名。

(5) 识别签名者　(a) 群权威 GM 已存有每一个群成员的 (s_i,r_i,k_i)，GM 可以预先计算：$v_i=s_i^{-1}k_i\,\mathrm{mod}\,q$，$w_i=g^{v_i}\cdot\mathrm{mod}\,p$，并将 (v_i,w_i) 与 (s_i,r_i,k_i) 一起存储。

(b) 一旦发生争议，需要打开某一个群签名，GM 可以查询已存的 (s_i,r_i,k_i,v_i,w_i)，这里 $i=1,2,\cdots,n$，n 是群成员个数，判断哪个群成员对应的 (v_i,w_i) 满足

$$\begin{aligned}&g^By_T^CFD^{h(A\|C\|D\|E\|F)}\\ &\equiv w_i^{\,B}D^{h(A\|C\|D\|E\|F)v_i-h(E\|D\|F)v_i+h(E\|D\|F)}(\mathrm{mod}\,p)\end{aligned}\qquad(1)$$

这样 GM 就能确定签名人的身份。

(6) 群成员的注销　如果要注销某个群成员，群权威 GM 查询出要注销群成员对应的 w_i,v_i，并公布 w_i,v_i 为注销群成员。当签名验证人收到群签名时，首先从公布的注销群成员名单中取出 w_i,v_i，判断是否满足式(1)。若式(1)成立，则此签名无效。若式(1)不成立，继续验证群签名的有效性。从而实现了群成员的注销。

4.2　Wang-Fu 群签名方案的安全性分析

4.2.1 对 Wang-Fu 群签名方案的伪造攻击　用这种攻击方法，任何人都能对任意消息产生有效的群签名，而且群权威无法追踪到签名者。假设攻击者为 Alice，产生有效的群签名过程如下：

(1) Alice 任意选取随机数 $x_i,d\in Z_q^*$，$k\in Z_p^*$ 且满足 $1+k$ 的阶为 q，计算：$D=g^d\,\mathrm{mod}\,p$，$A=D^{x_i}\,\mathrm{mod}\,p$，$E=k^{-1}(1+k)^{x_i}\cdot\mathrm{mod}\,p$。其中 k^{-1} 是 k 模 p 的逆。

(2) 任意选取 C,$t\in Z_q^*$ 计算

$$F=ky_T^{-C}\,\mathrm{mod}\,p$$

$$B=(d(h(E\|D\|F)-h(A\|C\|D\|E\|F)))\,\mathrm{mod}\,q$$

$$\alpha_i=(D^{h(E\|D\|F)}+g^By_T^CFD^{h(A\|C\|D\|E\|F)})\,\mathrm{mod}\,p$$

$$R=\alpha_i^{\,t}\,\mathrm{mod}\,p$$

$$S=t^{-1}(h(m\|R)-x_iR)\,\mathrm{mod}\,q$$

签名即为 (S,R,A,B,C,D,E,F,m)。

上述伪造的群签名能通过验证算法的验证,因为

$$\begin{aligned}\alpha_i &= (D^{h(E\|D\|F)} + g^B y_T{}^C F D^{h(A\|C\|D\|E\|F)}) \bmod p \\ &= (D^{h(E\|D\|F)} + D^{h(E\|D\|F)} y_T^C F) \bmod p \\ &= D^{h(E\|D\|F)}(1 + y_T^C F) \bmod p \\ &= D^{h(E\|D\|F)}(1+k) \bmod p\end{aligned}$$

$$\begin{aligned}\delta_i &= A^{h(E\|D\|F)}(\alpha_i D^{-h(E\|D\|F)} - 1)E \bmod p \\ &= A^{h(E\|D\|F)} g^B y_T^C F D^{h(A\|C\|D\|E\|F)-h(E\|D\|F)} E \bmod p \\ &= A^{h(E\|D\|F)} y_T^C F E \bmod p \\ &= D^{x_i h(E\|D\|F)} k E \bmod p \\ &= D^{x_i h(E\|D\|F)}(1+k)^{x_i} \bmod p \\ &= (D^{h(E\|D\|F)}(1+k))^{x_i} \bmod p \\ &= (\alpha_i)^{x_i} \bmod p\end{aligned}$$

而由 k 的选取可知, $1+k$ 的阶为 q ,又 g 的阶为 q 且 $D = g^d \bmod p$, 而 $\alpha_i = D^{h(E\|D\|F)}(1+k) \bmod p$, 于是 α_i 的阶也为 q。再由 S 的计算式可知: $h(m \| R) \equiv tS + x_i R (\bmod q)$。从而以下同余式成立:

$$\alpha_i{}^{h(m\|R)} \equiv \alpha_i{}^{tS} \alpha_i{}^{x_i R} \equiv R^S \delta_i{}^R (\bmod p)$$

即伪造的群签名能通过验证算法的验证。所以 (S,R,A,B,C,D,E,F,m) 是一个有效的群签名。

4.2.2 可追踪性的分析 一旦发生争议, 需要打开由上述伪造方法产生的群签名时, 同样地, 群权威 GM 查询已存的 (s_j,r_j,k_j,v_j,w_j) , 判断哪个群成员对应的 (v_j,w_j) 满足式(1)识别方程。从而确定签名人的身份。

很可能每一个群成员对应的 (v_j,w_j) 均不能满足识别方程, 这种情况下, 很显然群权威 GM 不能确定出签名者的身份。若存在某个群成员对应的 (v_j,w_j) 满足识别方程, 则此时相当于签名伪造者以 (v_j,w_j) 对应的群成员的名义产生合法签名, 这时群权威 GM 识别出的签名者并非真正的签名者。所以, Wang-Fu 群签名既不满足群签名定义 2: 安全性要求中的(4)和(6): 防伪造性和可追踪性, (5)防陷害攻击也不能得到保障。

4.2.3 对注销算法的讨论 Wang-Fu群签名方案与T-J群签名方案二相比, 除了对原方案进行改进外, 还增加了可注销群成员的特性。然而这个注销方案可能会引发一定的安全性问题。

在群成员(设 U_i)被注销后, 用其签名钥 (s_i,r_i) 无法再生成有效的群签名, 而其他群成员和公钥不用改变, 仍然可以生成有效的群签名, 且保持匿名性和不关联性。然而 U_i 在被注销前生成的有效的签名不再有效, 且不再具备匿名性和不关联性。任何人可以根据公开的注销成员表, 得到任一被注销成员所签署的所有群签名。而且, 当群比较大时, 随着被注销成员的增加, 由于验证算法计算量与被注销成员个数成正比, 整个方案的效率将下降。故而, 这个方案中的注销算法效率不高且不能提供较理想的安全性。

5 结论

本文对 Posescu 群签名方案和 Wang-Fu 群签名方案进行安全性分析, 并分别给出一种伪造攻击方法, 使得任何人可以对任意消息产生有效群签名。由于本文提出的两种攻击方法任何人对任何消息都可以实施, 而群权威 GM 识别签名者时仅对群成员进行检验, 所以一旦争议发生, 在识别阶段, 群权威无法识别签名者。从而两个方案都不能满足群签名定义安全性要求中的防伪造性和可追踪性, 防陷害攻击也得不到保障。而且, 前者方案还不具备不关联性和匿名性, 不能充分保护签名者的身份。后者方案中提出的注销方法使得验证的计算量与被注销成员个数成正比, 使整个方案效率降低, 而且使得被注销成员在注销之前的签名全部无效, 且不满足匿名性和不相关性。因此这两个方案仍然都是不安全的。

参 考 文 献

[1] Chaum D, van Heijst. Group signatures. In Advances in Cryptology——EUROCRYPT'91, LNCS 547, Springer-Verlag, 1991: 257 – 265.

[2] Tseng Yuh-Min, Jan Jinn-Ke. A novel ID-based group signature. In T. L. Hwang and A. K. Lenstra, editors, 1998 International Computer Symposium, Workshop on Cryptology and Information Security, Tainan, December 17 – 19, 1998: 159 – 164.

[3] Lee Wei-Bin, Chang Chin-Chen. Efficient group signature scheme based on the discrete logarithm. *IEE Proc. Comput. Digit. Tech.*, 1998, 145(1): 15 – 18.

[4] Tseng Yuh-Min, Jan Jinn-Ke. Improved group signature scheme based on discrete logarithm problem. *Electronics Letters*, 1999, 35(1): 37 – 38.

[5] Popescu C. A modification of the Tseng-Jan group signature scheme. *Studia Universitatis Babes-Bolyai Informatica*, 2000, XLV(2): 36 – 40.

[6] 王晓明, 符方伟. 一个安全的群签名方案. 电子与信息学报, 2003, 25(5): 657 – 663.

陈艳玲: 女, 1979 年生, 硕士生, 研究方向为密码学和有限域等.

陈鲁生: 男, 1962 年生, 教授, 主要从事密码学和编码理论等方面的研究和教学工作.

符方伟: 男, 1963 年生, 教授, 博士生导师, 长期从事信息论、密码学、编码理论和数字通信原理等方面的研究和教学工作.