ISSN 1000-9825 Journal of Software 软件学报 2000,11(10):1326~1332

几个门限群签名方案的弱点*

王贵林 卿斯汉

(中国科学院软件研究所信息安全国家重点实验室 北京 100080)
(中国科学院信息安全技术工程研究中心 北京 100080)
E-mail: qsihan@yahoo.com; glwang@ercist.iscas.ac.cn

摘要 门限群签名是一类重要的数字签名,但现有的门限群签名方案几乎都有缺点.首先给出良好的门限群签名所应具备的性质,随后详细分析了3个门限群签名方案的弱点.其中最主要的弱点是:部分成员可以合谋得到系统的秘密参数,从而伪造群签名,甚至彻底攻破签名系统.

关键词 数字签名,群签名,门限群签名,密码学.
中图法分类号 TP309

毫无疑问,数字签名是现代密码学的一项重要发明.数字签名也是保证数据完整性、实现网络认证以及开展现代电子商务的重要工具.使用普通的数字签名时,无论是产生签名还是验证签名,都只有一个用户参与.但随着网络应用的蓬勃发展,普通的数字签名技术已经不能满足许多应用的要求.近10年来,众多研究者提出了许多特殊的数字签名.群签名、门限群签名、非否认群签名和多方签名就是其中的4种.群签名方案首次由Chaum和Heyst提出[1].在群签名方案中,每个成员都可以代表整个群体签名.在群签名方案中引入秘密分存[2],就形成门限群签名方案[3~8],使得群体中的某些给定子集可以代表整个群体签名.在非否认群签名中,签名的验证需要签名者的合作.而在多方签名方案中,各签名成员的身份是公开的,且在验证签名时一般需要各成员的公钥.在门限群签名方案中,门限群签名是由参加签名的各个成员所签署的部分数字签名按某种方式结合后产生的.根据分存秘密的分发方式的不同,现有的门限群签名方案可以分为两种类型:带有秘密分发中心的门限群签名方案[4,7,8]和分布式分发分存秘密的门限群签名方案[5~7].从目前的研究来看,我们认为良好的门限群签名应该具备以下一些性质:

(1) 群签名特性:只有群体中的成员才可以生成有效的部分签名,非群体成员无法伪造有效的部分签名;
(2) 门限特性:只有当签名人数不少于门限时,才可以产生有效的门限群签名;
(3) 防冒充性:任何小组不能假冒其他小组生成群签名;
(4) 验证简单性:签名的验证者可以方便而简单地验证签名是否有效;
(5) 匿名性:签名的验证者不知道该签名是群体中哪些成员签署的;
(6) 可追查性:事后发生纠纷时,可以追查出签名者的身份;
(7) 强壮性:恶意成员大于等于门限时仍然无法获取系统秘密参数;
(8) 系统稳定性:在剔除违规成员或加入新成员时,无须或只需少量改变系统参数和老成员参数.

按这8条性质去检查,现有的门限群签名方案几乎都有缺点.Desmedt和Frankel首次提出基于RSA的门限群签名方案[4],但是文献[9]发现文献[4]中指出的恶意成员大于或等于门限时,他们合谋能以高概率获取系统秘密(群秘密密钥),进而可不负责任地伪造其他成员的群签名.Langford在文献[10]中指出:文献[5,6]和文

* 本文研究得到国家自然科学基金(No. 19931010)和国家重点基础研究发展规划项目(No. G199035810)资助.作者王贵林,1968年生,博士生,主要研究领域为协议分析,信息安全基础.卿斯汉,1939年生,研究员,博士生导师,主要研究领域为信息安全理论和技术.

本文通讯联系人:卿斯汉,北京 100080,中国科学院软件研究所

本文2000-05-31收到原稿,2000-06-30收到修改稿

献[7]中的密钥生成协议有问题.对文献[11]所提出的门限群签名方案,文献[12]指出了对该方案的两个攻击:攻击者根据已有的群签名可伪造出关于其他消息的群签名.

本文主要分析文献[11]、文献[4]和文献[13]所提出的3个群门限签名的弱点.其中最主要的缺点是强壮性和防伪造性:t或$(t+1)$个成员可以合谋得到(至少是以高概率得到)系统的秘密参数,从而可以伪造群签名,甚至由此彻底攻破签名系统.同时,我们还分析了这3个方案在可追查性和匿名性方面的缺点.对于文献[11]和文献[4]提出的方案,我们的攻击不仅与文献[9]和文献[12]中所发现的攻击不同,而且我们的攻击更彻底,成功的概率更高,具有更强的实践性.

为方便起见,下面把文献[11]、文献[4]和文献[13]所提出的3个群门限群签名方案分别简称为WLC,DY,Xu门限群签名方案(或WLC,DY,Xu方案).这3个方案都是(t,N)门限群签名方案,其中t是门限,N是成员的个数,并用$IN=\{0,1,\ldots,N-1\}$表示指标集.系统中全部N个成员的真实身份构成集合$U=\{u_i|i\in IN\}$,而他们的化名身份构成集合$X=\{x_i|i\in IN\}$.对指标子集$I\subseteq IN$,记$U(I)=\{u_i|i\in I\}$,$X(I)=\{x_i|i\in I\}$.下面,我们一般用I表示IN的t元或$(t+1)$元指标子集,而$X(I)$可以是签署某消息的成员小组,也可以是进行合谋的某个恶意成员小组.另外,用$d\in_R D$表示从集合D中随机、均匀地选择元素d.

1 WLC门限群签名方案及其弱点

1.1 WLC门限群签名方案简介

WLC门限群签名方案由可信任的秘密分发中心SDC(share distribution center)选择系统参数和分发秘密分存.整个方案由初始化、部分签名的生成及验证和群签名的生成及验证这3个阶段组成.

1.1.1 初始化阶段

SDC选择、计算以下参数:

(1) 选择3个大素数p,p',q,使得$p'|(p-1),q|(p'-1)$;

(2) 选择$GF(p)$中阶为p'的元素g以及$GF(p')$中阶为q的元素α;

(3) 选择单向Hash函数H;

(4) 选择一个$(t-1)$次多项式$f(x)=a_0+a_1x+\ldots+a_{t-1}x^{t-1} \bmod q$,其中$a_i\in_R[1,q-1]$;

(5) 将$\alpha_0=f(0)$,$Y=g^{\alpha^{f(0)}}$分别作为群秘密种钥和群公开密钥;

(6) 为各成员u_i选择化名$x_i\in_R[1,q-1]$,并计算成员u_i的秘密密钥$\alpha^{f(x_i)}$和公开密钥$y_i=g^{\alpha^{f(x_i)}}$;

(7) 最后,SDC公开p,p',q,g,α,Y,H和$(y_i,x_i),i=0,1,\ldots,N-1$,并向各成员秘密发送$\alpha^{f(x_i)}$.

1.1.2 部分签名的生成及验证

若t个成员构成的小组$X(I)(I\subseteq IN\wedge|I|=t)$同意对某消息$m$进行签名,则每个成员$x_i(i\in I)$选择、计算以下各数,以生成部分签名:

(1) $r_i=\alpha^{k_i} \bmod p'$,其中$k_i\in_R[1,q-1]$;

(2) $s_i=\alpha^{k_i\cdot f(x_i)}\cdot H(m)\cdot r_i \bmod p'$,其中插值系数$c_{i,I}=\prod_{j\in I\setminus\{i\}}(0-x_j)/(x_i-x_j)$;

(3) $r'_i=g^{k'_i} \bmod p$,其中$k'_i\in_R[1,p'-1]$;

(4) $s'_i=k_i^{-1}(s_i-r'_i\cdot\alpha^{f(x_i)}) \bmod p'$;

(5) 发送部分签名$(y_i,m,r_i,s_i,r'_i,s'_i)$给预定的签名合成者DC(designated combiner).

DC按下式是否成立来判定各部分签名是否有效:

$$g^{s_i}\equiv y_i^{r'_i}\cdot r'^{s'_i}_i \bmod p. \tag{1}$$

1.1.3 群签名的生成及验证

如果DC收到的t份部分签名都是有效的,则他按如下步骤生成群签名:

(1) 计算$R=\prod_{i\in I}r_i \bmod p'$和$S=\prod_{i\in I}s_i \bmod p'$;

(2) 计算身份确定函数$h_I(y)=\sum_{i\in I}\left(x_i\cdot\prod_{j\in I\setminus\{i\}}(y-y_j)/(y_i-y_j)\right)$;

(3) $(m,R,S,h_I(y))$就是对消息 m 的门限群签名.

验证者可以通过下式确定门限群签名是否有效:

$$g^S \equiv Y^{H(m)^t \cdot R} \bmod p. \tag{2}$$

另外,验证者可通过计算 $h_I(y_i)$是否为 x_i 来了解某个化名成员 x_i 是否参加了此次群签名.

1.2 WLC 门限群签名方案的弱点

文献[12]指出了对 WLC 门限群签名方案的两个攻击:攻击者由已知的有效群签名可伪造出关于其他消息的群签名.在此我们指出一个攻击:在不知道任何有效群签名的情况下,t 个成员合谋可以获取大部分系统秘密,并由此伪造群签名.另外,WLC 方案还有不具备可追查性和强壮性,且系统稳定性差的缺点.

1.2.1 WLC 方案不具备防冒充性

在没有任何有效的群签名时,t 个成员构成的小组 $X(I)$通过合谋可以伪造有效的群签名,方法如下.

(1) 各成员 $x_i(i\in I)$把 $\alpha^{f(x_i)}$发送给某个成员 T,则 T 可生成多项式 $F(x)$:

$$F(x)\triangleq \prod_{i\in I}(\alpha^{f(x_i)})^{c_{i,I}(x) \bmod q} \bmod p' = \alpha^{\sum_{i\in I} f(x_i)\cdot c_{i,I}(x) \bmod q} \bmod p' = \alpha^{f(x)} \bmod p'. \tag{3}$$

其中,插值系数多项式

$$c_{i,I}(x)=\prod_{j\in IN\setminus I}(x-x_j)/(x_i-x_j).$$

(2) 于是,成员 T 可计算:

$$F(0)=\alpha^{f(0)} \bmod p',\ F(x_j)=\alpha^{f(x_j)} \bmod p',\quad j\in IN\setminus I.$$

(3) 由此,这 t 个成员掌握了其他所有成员的秘密密钥 $\alpha^{f(x_j)}(j\in IN\setminus I)$以及秘密参数 $\alpha^{f(0)}$.加之(y_j,x_j)是公开的,于是他们就可以任意选择 $R\in_R[1,p'-1]$和 t 元指标子集 I',伪造 $X(I')$对任何消息 m 的签名$(m,R,S,h_I(y))$.其中 S 由下式计算:

$$S=F(0)\cdot H(m)^t\cdot R \bmod p'(=\alpha^{f(0)}\cdot H(m)^t\cdot R \bmod p'). \tag{4}$$

根据式(2)容易验证,由式(4)计算出的群签名是有效的.

1.2.2 WLC 方案不具备可追查性和强壮性,且系统稳定性差

由于验证者只能通过计算 $h_I(y_i)$判断 x_i 是否参加了群签名,而化名成员 x_i 和真实成员 u_i 间的对应关系只有 SDC 知道,所以 WLC 方案具备匿名性.若事后发生纠纷,SDC 可以通过公开 x_i 和 $u_i(i\in I)$间的对应关系揭露签署群签名$(m,R,S,h_I(y))$的所有真实成员身份集合 $U(I)$.但$(y_j,x_j)(j\in IN)$是公开的(至少对于系统中的各个成员),那么对于一个有效的群签名$(m,R,S,h_I(y))$,任何人(至少各成员)都可以把 $h_I(y)$篡改为 $h_{I'}(y)$,使得验证者相信该签名的签署成员集是 $X(I')$,而不是 $X(I)(|I|=|I'|=t)$.于是,SDC 根据 $X(I')$追查出的真实成员集就是 $U(I')$,而不是 $U(I)$.所以,WLC 方案实际上不具备可追查性.在第 1.2.1 节中已经说明,t 个成员合谋可以获取许多系统秘密参数.所以 WLC 方案不也不具备强壮性.

容易知道,要在 WLC 方案中加入新成员 u_i,SDC 只需为其选择化名身份值 x_i,并将秘密密钥 $\alpha^{f(x_i)}$和公开密钥

$$y_i=g^{f(x_i)}$$

发送给他即可,而与系统和老成员相关的参数不必改动.但是,剔除旧成员时会出现问题.假如有$(t-1)$个旧成员已退出系统,而某个成员购买了他们的秘密密钥,那么这个成员就可以采用第 1.2.1 节中的办法,获取系统秘密,伪造签名.这是因为,在 WLC 方案中,只要系统参数不变,被剔除成员的秘密密钥就对破解系统秘密有用.

2 DY 门限群签名方案及其弱点

2.1 DY 门限群签名方案简介

在 DY 方案中,SDC 选择 $n=pq$.其中 p 和 q 都是安全大素数,即存在大素数 p'和 q',使得 $p=2p'+1$ 和 $q=2q'+1$.随机选择秘密密钥 d,使 $\gcd(d,\lambda(n))=1(\lambda(n)=2p'q')$,并由此计算满足 $ed\equiv 1 \bmod \lambda(n)$的公开密钥 e.然后,选择一个次数为$(t-1)$的多项式 $f(x)=a_0+a_1x+\ldots+a_{t-1}x^{t-1}$,使 $f(0)=a_0=d-1$.SDC 只公开 n 和 e,

而将其他参数保密.之后,SDC 向各成员 x_i 秘密分发由下式计算出来的 K_i:

$$K_i=f(x_i)/2\cdot\Big(1/2\cdot\prod_{j\in IN\setminus\{i\}}(x_i-x_j)\Big)^{-1}\bmod p'q', \tag{5}$$

要求其中所有的 x_i 为奇数,所有的 $f(x_i)$ 为偶数.

当 $X(I)$ 中的 t 个成员同意对消息 m 签名时,各成员 $x_i(i\in I)$ 先计算 $a_{i,I}$,再生成部分签名 $S_{i,I}$:

$$a_{i,I}=K_i\cdot\Big(\prod_{j\in IN\setminus I}(x_i-x_j)\prod_{j\in I\setminus\{i\}}(0-x_j)\Big),$$
$$S_{i,I}=m^{a_{i,I}}\bmod n. \tag{6}$$

各成员 $x_i(i\in I)$ 将他们的部分签名发送给签名合成者 DC,于是 DC 计算 S:

$$S=m\cdot\prod_{i\in I}S_{i,I}\bmod n\Big(=m\cdot m^{\sum_{i\in I}a_{i,I}}\bmod n\Big), \tag{7}$$

则关于消息 m 的群签名就是 (m,S). 由于

$$f(x)=\sum_{i\in I}K_i\prod_{j\in IN\setminus I}(x_i-x_j)\prod_{j\in I\setminus\{i\}}(x-x_j)\bmod\lambda(n),$$

所以由式(6),我们有

$$d-1=f(0)=\sum_{i\in I}a_{i,I}\bmod\lambda(n). \tag{8}$$

由式(7)、式(8)容易知道,验证者可根据以下等式是否成立来判定群签名是否有效:

$$m\equiv(S)^e\bmod n\Big(=\big(m\cdot m^{\sum_{i\in I}a_{i,I}}\big)^e\bmod n=(m^d)^e\bmod n\Big).$$

2.2 DY 门限群签名方案的弱点

在 DY 方案中,保护系统秘密参数 $p,q,p',q',\lambda(n)$ 和 $p'q'$ 是很关键的. 文献[9]指出了两个攻击,$(t+1)$ 或 t 个成员合谋可以高概率地获取系统秘密 $p'q'$. 这里,我们指出一个新的攻击:在这一攻击中,$(t+1)$ 个成员合谋不仅能以高概率获取 $p'q'$,而且可以进一步获取 $f(x)$. 由此,这 $(t+1)$ 个成员就得到了系统和所有成员的全部秘密,从而可以冒充其他小组进行签名而不必承担任何责任. 另外,我们还指出 DY 方案不具备可追查性和强壮性,且系统稳定性差.

2.2.1 DY 门限群签名方案不具备防伪造性

为方便起见,设这 $(t+1)$ 个成员就是前 $(t+1)$ 个成员,他们构成集合 $X(I)(I=\{0,1,\ldots,t\})$. $X(I)$ 中各成员将各自的 K_i 发送给攻击者 T,则 T 可计算出 $(t+1)$ 个多项式 $F_l(x)$.

$$F_l(x)\triangleq\sum_{i\in I_l}\Big(K_i\cdot\prod_{j\in IN\setminus I_l}(x-x_j)\prod_{j\in I_l\setminus\{i\}}(x-x_j)\Big)\Big(=f(x)\bmod p'q'\Big)\ (\forall\, l\in I), \tag{9}$$

其中 $I_l=I-\{l\}$,$l\in I$. T 将 $F_l(x)$ 改写为

$$F_l(x)=a_{l,0}+a_{l,1}x+\ldots+a_{l,(t-1)}x^{t-1}\Big(=f(x)\bmod p'q'\Big)\ (\forall\, l\in I). \tag{10}$$

由此,攻击者 T 可得出 t 个方程组:

$$\begin{cases}a_{0,0}=a_0\bmod p'q'\\ a_{1,0}=a_0\bmod p'q'\\ \cdots\\ a_{t,0}=a_0\bmod p'q'\end{cases},\quad\begin{cases}a_{0,1}=a_1\bmod p'q'\\ a_{1,1}=a_1\bmod p'q'\\ \cdots\\ a_{t,1}=a_1\bmod p'q'\end{cases},\quad\ldots,\quad\begin{cases}a_{0,(t-1)}=a_{t-1}\bmod p'q'\\ a_{1,(t-1)}=a_{t-1}\bmod p'q'\\ \cdots\\ a_{t,(t-1)}=a_{t-1}\bmod p'q'\end{cases}.$$

也就是说,$p'q'$ 整除所有 $(a_{l,j}-a_{0,j})(1\leqslant l\leqslant t,0\leqslant j\leqslant t-1)$,于是 T 可计算:

$$b_j\triangleq\gcd(a_{1,j}-a_{0,j},a_{2,j}-a_{0,j},\ldots,a_{t,j}-a_{0,j}),\ 0\leqslant j\leqslant t-1.$$

于是,$p'q'$ 整除所有 b_j. 所以与文献[9]中的攻击原理类似,T 将以高概率获得系统秘密 $p'q'$. 一旦获得 $p'q'$,攻击者随意选取一个 $F_l(x)$,就可根据下式得出 $f(x)$.

$$f(x)=F_l(x)\bmod p'q'.$$

既然已知 $f(x)$ 和 $p'q'$,而 x_j 又是公开的,所以攻击者 T 就可以像 SDC 一样,根据式(5)计算出所有成员的 K_i. 随后,T 就可伪造关于任何消息的签名.

注:必要时,攻击者 T 还可以利用以下事实破解 $p'q'$(其中 c 是任选的整数):

$$p'q' \mid \gcd(F_1(c)-F_0(0)(c), F_2(c)-F_0(c), \ldots, F_t(c)-F_t(c)).$$

2.2.2 DY门限群签名方案的其他弱点

在DY方案中,任何t个成员对同一消息的群签名是完全相同的.也就是说,群签名完全隐藏了签名者的身份信息,就算事后发生纠纷,SDC也无法根据群签名追查出实际参与该签名的成员身份.所以,DY方案是不可追查的.如前所述,$(t+1)$个成员合谋能以高概率获取系统秘密,所以DY方案也不具备强壮性.另外,与WLC方案类似,剔除成员的秘密信息仍然有效,所以DY方案的系统稳定性差.

3 Xu门限群签名方案及其弱点

3.1 Xu门限群签名方案简介

与DY方案类似,Xu门限群签名方案也是基于RSA密码体制的.在系统设置阶段,SDC的任务如下:

(1) 选择模数$n=pq$(p,q是安全大素数)、满足$de=1 \bmod \varphi(n)$的秘密密钥d和公开密钥e以及单向Hash函数h;

(2) 随机选取$(t-1)$次多项式$f(x)=a_0+a_1+\ldots+a_{t-1}x^{t-1}$,其中$a_i \in_R [1,\varphi(n)-1], i=1,2,\ldots,t-1$,而且$f(0)=a_0=d$;

(3) 选取较小的数$x_i \in [1,\varphi(n)-1]$作为U中成员u_i的化名,并保证各x_i互异,然后计算$y_i=f(x_i) \bmod \varphi(n), i \in IN$;

(4) 公开h,n,e,x_i,并将y_i秘密地发送给成员x_i.

$X(I)$中的t个成员要对消息m签名,则签名过程如下:

每个成员$x_i(i \in I)$先计算部分签名$S_{i,I}=h(m)^{y_i} \bmod n$,然后将$(x_i,S_{i,I})$发送给签名合成者DC,DC先在整数环上计算$\pi$和$\alpha_{i,I}$:

$$\pi = \prod_{i,j \in I \setminus I, i>j} (x_i - x_j), \quad \alpha_{i,I}=\pi \cdot c_{i,I}, \quad \forall i \in I. \tag{11}$$

其中$c_{i,I}=\prod_{j \in I \setminus \{i\}} (0-x_j)/(x_i-x_j)$,且易知$\alpha_{i,I}$为整数,然后再计算$S$:

$$S=\prod_{i \in I} S_{i,I}^{\alpha_{i,I}} \bmod n. \tag{12}$$

至此,DC生成对消息m的群签名(m,S).而验证者根据下式是否成立得知群签名(m,S)是否有效:

$$h(m)^\pi \equiv S^e \bmod n. \tag{13}$$

验证等式(13)的正确性由Lagrange插值公式来保证.

3.2 Xu门限群签名方案的弱点

首先,Xu门限方案中的群签名形式是(m,S),其中不包含签署成员的化名身份集$X(I)$,也不包含化名身份确定函数,所以,验证者根本不能计算π,也就不能验证签名是否有效.这是设计者的疏忽.下面讨论Xu方案的防伪造性、强壮性和系统稳定性.

3.2.1 Xu门限群签名方案的防伪造性差

仍假设前$(t+1)$个成员合谋破解系统秘密,他们构成集合$X(I)(I=\{0,1,\ldots,t\})$.$X(I)$中的各个成员将各自的y_i发送给攻击者T,则T可计算出$(t+1)$个多项式$F_l(x)$.

$$F_l(x) \triangleq \sum_{i \in I \setminus \{l\}} y_i \cdot \alpha_{i,I}(x) (= \pi_l \cdot f(x) \bmod \varphi(n)), \quad \forall l \in I. \tag{14}$$

其中

$$\pi_l = \prod_{i,j \in I \setminus \{l\}, i>j} (x_i - x_j), \quad \forall l \in I.$$

所以,对于任意的$l,l' \in I (l \neq l')$,有

$$F_{l,l'}(x) \triangleq \pi_{l'} \cdot F_l(x) - \pi_l \cdot F_{l'}(x) = 0 \bmod \pi_l \pi_{l'} \varphi(n).$$

这样,$F_{l,l'}(x)$作为整数环上的多项式,其各系数都是$\pi_l \pi_{l'} \varphi(n)$的倍数,它在任意一点上的函数值也都是$\pi_l \pi_{l'} \varphi(n)$的倍数.所以,类似于破解DY方案的办法,通过求这些系数、函数值的最大公因子,攻击者将以高概率破解系统

秘密 $\varphi(n)$.一旦得知 $\varphi(n)$,攻击者即可根据式(14)得到系统秘密 $f(x)$.之后,攻击者由公开的 x_i 可计算 y_i.至此,攻击者彻底攻破了签名系统,于是可以冒充任何小组对任何消息进行签名.

注:在选择 $F_{t,t'}(x)$ 时,攻击者要尽量选择既有正系数又有负系数的 $F_{t,t'}(x)$.若能从 $F_{t,t'}(x)$ 中获得长度接近 $\pi_t\pi_{t'}n$ 的系数或函数值,则攻击者已经成功.因为这表明,攻击者已经得到了 $\pi_t\pi_{t'}\varphi(n)$ 的小倍数,从而可以很容易地得到 $\varphi(n)$.

3.2.2 Xu 门限群签名方案的其他缺点

如前所述,$(t+1)$ 个成员合谋能以高概率获取系统秘密 $\varphi(n)$ 和 $f(x)$,所以,Xu 方案的强壮性差.另外,与前两个方案类似,剔除成员的秘密信息仍然有效,所以 DY 方案的系统稳定性差.

4 结束语

通过本文的分析,我们发现 WLC,DY 以及 Xu 门限群签名方案都有许多弱点.其中最大的弱点是:部分成员合谋可以获取(至少是以高概率获取)系统秘密,并由此伪造群签名,甚至彻底攻破系统.事实上,设计一个性能优良的门限群签名方案是当前密码学中的一个公开问题.

参考文献

1 Chaum D, Heyst E van. Group signatures. In: Davies D W ed. Advances in Cryptology——Eurocrypt'91 Proceedings. Berlin: Springer-Verlag, 1992. 257~265

2 Shamir A. How to share a secret. Communication of ACM, 1979,22(11):612~613

3 Desmedt Y. Society and group oriented cryptography. In: Pomerance C ed. Advances in Cryptology——Crypto'87 Proceedings. Berlin: Springer-Verlag, 1988. 120~127

4 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

5 Harn L, Yang S. Group-Oriented undeniable signature schemes without the assistance of a mutually trusted party. In: Seberry J, Zheng Y eds. Advances in Cryptology——Auscrypt'92 Proceedings. Berlin: Springer-Verlag, 1992. 133~142

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

7 Li C, Hwang T, Lee N. Threshold-Multisignature schemes where suspected forgery implies traceability of adversarial shareholders. In: Santis A D ed. Advances in Cryptology—— Eurocrypt'94 Proceedings. Berlin: Springer-Verlag, 1995. 194~204

8 Lu Lang-ru, Zhao Ren-jie. $A(t,n)$ threshold group signature scheme. In: Pei Ding-yi, Zhao Ren-jie, Zhou Jin-jun eds. Advances in Cryptology——Chinacrypt'96. Beijing: Science Press, 1996. 177~184
(Lu Lang-ru, Zhao Ren-jie. $A(t,n)$ threshold group signature scheme. 见:裴定一,赵仁杰,周锦君编.密码学进展——Chinacrypt'96.北京:科学出版社.1996. 177~184)

9 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, 1993. 413~419

10 Langford S K. Weakness in some threshold cryptosystems. In: Koblitz N ed. Advances in Cryptology——Crypto'96 Proceedings. Berlin: Springer-Verlag, 1996. 74~82

11 Wang C T, Lin C H, Chang C C. Threshold signature schemes with traceable signers in group communications. Computer Communications, 1998,21(8):771~776

12 Tseng Y M, Jan J K. Attacks on threshold signature schemes with traceable signers. Information Processing Letters, 1999,71(1):1~4

13 Xu Qiu-liang. A modified threshold RSA digital signature scheme. Chinese Journal of Computers, 2000,23(5):449~453
(徐秋亮.改进门限 RSA 数字签名体制.计算机学报,2000,23(5):449~453)

Weaknesses of Some Threshold Group Signature Schemes

WANG Gui-lin QING Si-han

(State Key Laboratory of Information Security Institute of Software The Chinese Academy of Sciences Beijing 100080)
(Engineering Research Center for Information Security Technology The Chinese Academy of Sciences Beijing 100080)

Abstract Threshold group signature is an important kind of signatures, but all of the existing threshold group schemes have weaknesses. Several properties are proposed to define a good threshold group scheme. Then, the weaknesses of three threshold group schemes are analyzed. The most serious weakness is that part of members can conspire to get system secret parameters and then forge a valid signature. In the worst situation, the total system is broken.

Key words Digital signature, group signature, threshold group signature,