ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.17, No.7, July 2006, pp.1627−1632
DOI: 10.1360/jos171627

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

对一种多重密钥共享认证方案的分析和改进*

王贵林[1,3]，卿斯汉[2+]

[1](计算机科学重点实验室(中国科学院 软件研究所),北京 100080)

[2](中国科学院 信息安全技术工程研究中心,北京 100080)

[3](资讯通信研究院,新加坡 119613)

Analysis and Improvement of a Multisecret Sharing Authenticating Scheme

WANG Gui-Lin[1,3], QING Si-Han[2+]

[1](Laboratory of Computer Science (Institute of Software, The Chinese Academy of Sciences), Beijing 100080, China)

[2](Engineering Research Center for Information Security Technology, The Chinese Academy of Sciences, Beijing 100080, China)

[3](Institute for Infocomm Research, Singapore 119613, Singapore)

+ Corresponding author: Phn: +86-10-62635150, Fax: +86-10-62635150, E-mail: qsihan@ercist.iscas.ac.cn

Wang GL, Qing SH. Analysis and improvement of a multisecret sharing authenticating scheme. *Journal of Software*, 2006,17(7):1627−1632. http://www.jos.org.cn/1000-9825/17/1627.htm

Abstract: In a (*t*,*n*) secret sharing scheme, a dealer splits a secret into *n* shares and sends a share to each of *n* participants. If necessary, any *t* members can provide their secret shares together and recover the secret by using a publicly specified algorithm. Multisecret sharing schemes allow a dealer to share multiple secrets among a group of participants securely and efficiently. In recent, Shi proposed an efficient multisecret sharing authenticating scheme. In his scheme, not only the shares held by the participants are reusable, but also the shares distributed by the dealer and the shadow shares provided by the participants are verifiable. This paper analyzes the security of Shi's scheme. It first points out a design error in his scheme, and then demonstrates an attack to show that both of his share-authenticating and shadow-key-authenticating methods are insecure. Specifically, using the attacks, a dishonest dealer can distribute false shares to participants, and malicious participants can easily forge false shadow shares such that the authenticating equality is satisfied. The result is that honest participants will be cheated and misled to believe that the recovered secret is correct. In addition, improvements are provided to avoid the identified design error and attacks.

Key words: secret sharing; multisecret sharing; cryptography; information security

摘 要: 在(*t*,*n*)密钥共享方案中,密钥管理者将一个秘密密钥分成 *n* 个子密钥,然后让 *n* 个成员中的每个成员保存一个子密钥.当需要恢复秘密密钥时,任意 *t* 个成员拿出他们持有的子密钥后,就可以按既定的公开算法恢复出所需密钥.而多重密钥共享使得密钥管理者可以安全且有效地共享多个密钥.Shi 给出了一种高效率的多重密

* Supported by the National Natural Science Foundation of China under Grant Nos.60083007, 60573042 (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)); the Beijing Natural Science Foundation of China under Grant No.4052016 (北京市自然科学基金)

Received 2005-01-10; Accepted 2005-10-19

钥共享认证方案.在其方案中,不仅成员持有的子密钥能够重复使用,而且管理者分发的子密钥和成员提供的影子子密钥也都是可认证的.对 Shi 方案的安全性进行了分析:首先指出该方案的一个设计错误;然后给出两个攻击,以表明该方案中的子密钥和影子子密钥认证方法实际上都是不安全的.准确地说,利用所提出的攻击,不诚实的管理者可以将假的子密钥分发给成员;而不良成员可以很容易地伪造假的但能满足认证等式的影子子密钥,从而欺骗诚实成员,使得诚实成员误以为他们恢复出的密钥是正确的.另外,还给出了改进方法,以避免上述设计错误和攻击.

关键词: 密钥共享;多重密钥共享;密码学;信息安全
中图法分类号: TP309 文献标识码: A

密钥共享(secret sharing)是一种分发、保存、恢复秘密密钥(或其他秘密信息)的方法:密钥管理者将秘密密钥拆分成一系列相互关联的秘密信息(称为子密钥),然后将子密钥分发给某群体中的各个成员;使得某些小组(授权集)中的各成员拿出他们的子密钥后,就可以利用既定的方法恢复该秘密密钥,而其他小组(非授权集)则无法恢复该密钥.密钥共享也称为密钥分存、秘密共享或秘密分存.在现实环境下的信息系统中使用密钥共享,可以防止系统密钥的遗失、损坏和来自敌方的攻击,减小密钥持有者(个人或服务器)的责任,同时还可以降低敌手破译密钥的成功率.

密钥共享首先由著名密码学家 Shamir[1]和 Blakley[2]提出.Shamir 的方案简单、实用,得到了广泛的应用和重视.Shamir 的方案属于(t,n)门限密钥共享方案,即任何不少于 t 个成员的小组都可以恢复秘密密钥.虽然 Shamir 门限方案是完善的密钥共享,但该方案存在两个问题[3,4]:(1) 管理者的诚实性问题:为防止管理者将假的子密钥分发给部分或全部成员,各成员如何验证管理者发送来的子密钥是正确的(即与其他密钥一致,从而可用来恢复秘密密钥);(2) 成员的诚实性问题:在恢复秘密密钥阶段,若某些恶意成员提供了假的子密钥,其他成员如何鉴别.

多重密钥共享研究的主要内容是密钥管理者如何安全且有效地共享多个密钥[5−7].文献[8]给出了一种高效率的多重密钥共享认证方案.此方案不仅密钥管理者能够方便地共享多个密钥,成员拥有的子密钥可以重复使用,而且管理者分发的子密钥和成员提供的影子子密钥都是可认证的.本文对此方案的安全性进行分析:首先指出该方案的一个设计错误;然后给出两个攻击,以表明该方案中所给出的子密钥和影子子密钥认证方法实际上都是不安全的.准确地说,利用我们的攻击,不诚实的管理者可以将假的子密钥分发给成员;而不良成员可以很容易地伪造假的但能满足认证等式的影子子密钥,从而欺骗诚实成员,使得诚实成员误以为他们恢复出的密钥是正确的.另外,我们还给出了改进方法,以避免上述设计错误和攻击.

本文第 1 节回顾 Shi 的多重密钥共享认证方案.第 2 节给出安全性分析并提出改进方法,以避免我们所发现的设计错误和攻击.第 3 节是结束语.

1 文献[8]方案简介

多重密钥共享认证方案[8]分为 4 个阶段:初始化、子密钥的生成、密钥分存和密钥恢复.前 3 个阶段由密钥管理者完成,而第 4 个阶段由 n 个成员中的任意 t 个合作完成.

(1) 初始化阶段:密钥的管理者 D 拥有一个电子公告牌 NB,用于公开信息、存储和认证影子子密钥.每个系统成员都可以读取公告牌 NB 中的内容,但只有管理者 D 可以修改、删除或添加.D 选取两个安全大素数 $p=2p'+1$ 和 $q=2q'+1$,其中 p'和 q'也是素数;置 $N=pq,R=p'q'$;选取 Z_N 的 R 阶生成元 g;产生 RSA 密钥对(e,d),使得 $ed=1 \bmod \Phi(N)$.最后,D 在 NB 中公开(N,g,e),将(d,R)作为秘密保存,同时删除素数 p 和 q.

(2) 子密钥的生成阶段:假定 $S=\{S_i|i=1,2,\ldots,m\}$是要共享的密钥集,而共享 S 中 m 个密钥的 n 个成员所构成的集合是 $G=\{U_j|j\in A=\{1,2,\ldots,n\}\}$,$ID_j$ 是成员 U_j 的标志符(一个公开的数值).管理者 D 随机选取一个$(t-1)$阶的多项式 $f(x)=a_0+a_1x+\ldots+a_{t-1}x^{t-1}\in Z_R[x]$(即随机选取各个系数 a_k 使得 $a_k\in Z_R,k=0,1,\ldots,t-1$).随后,D 在 NB 中公开对各系数 a_k 的承诺 V_k:

$$V_k = g^{a_k} \bmod N,\quad k=0,1,\ldots,t-1 \tag{1}$$

另外,对每个 $j\in\{1,2,\ldots,n\}$,D 计算如下的 x_j 和 y_j:

$$x_j = f(ID_j)\cdot P_j^{-1} \bmod R,\ y_j = g^{x_j} \bmod N \tag{2}$$

其中的 $P_j = \prod_{k\in A\setminus\{j\}}(ID_j - ID_k) \bmod R$.

这之后,管理者 D 经安全信道将 $\{g^{P_j} \bmod N, x_j\}$ 发送给 U_j,而将 y_j 作为公开信息放入 NB.为了检验管理者是否进行了欺骗,U_j 可以根据下面的子密钥认证等式来验证 x_j 的正确性:

$$(g^{P_j})^{x_j} \equiv \prod_{k=0}^{t-1}(V_k)^{ID_j^k} \bmod N \tag{3}$$

(3) 密钥分存阶段:为了将密钥集 S 中的 m 个密钥在 n 个成员中分存,D 选取 $2m$ 个随机数 $r_i\in Z_R, T_i\in Z_N, i=1,2,\ldots,m$.然后,针对每个许可证 T_i,按下面的式子计算一个凭证 C_i 和一个变换值 h_i:

$$C_i = g^{-d+r_i}\cdot(T_i)^{2d+r_i+1} \bmod N \tag{4}$$

$$h_i = (T_i^{a_0} - S_i)\cdot(C_i)^{-a_0} \bmod N \tag{5}$$

最后,D 把所有四元对$\{r_i,T_i,C_i,h_i\}$放入 NB.

(4) 密钥恢复阶段:若有 t 个成员 $U_j(j\in w, w\subseteq A$ 且$|w|=t)$想恢复密钥 $S_i\in S$,则每个成员 $U_j\in w$ 先从 NB 中获得$\{r_i,T_i,C_i,h_i\}$,然后利用他的秘密子密钥 x_j 按如下公式计算影子子密钥 A_{ij} 和相应的认证信息 B_{ij}:

$$A_{ij} = (T_i)^{x_j} \bmod N,\quad B_{ij} = (C_i)^{x_j} \bmod N \tag{6}$$

随后,U_j 将(A_{ij},B_{ij})送给 w 中的其他成员.利用 NB 中的公开信息 y_j,w 中的任何成员都可用下面的影子子密钥认证等式来验证(A_{ij},B_{ij})的有效性:

$$(B_{ij})^e \equiv (y_j)^{er_i-1}\cdot(A_{ij})^{2+e(r_i+1)} \bmod N \tag{7}$$

若 t 个(A_{ij},B_{ij})对都被认证,则 w 中的成员可以利用下式恢复出密钥 S_i:

$$S_i = \prod_{j\in w}(A_{ij})^{\Delta_j} - h_i\cdot\prod_{j\in w}(B_{ij})^{\Delta_j} \bmod N \tag{8}$$

上式中的Δ_j 由下式给出(注:Δ_j 在整数环 Z 计算,指标集 $A=\{1,2,\ldots,n\}$):

$$\Delta_j = \prod_{k\in w-\{j\}}(-ID_k)\cdot\prod_{k\in A-w}(ID_j - ID_k) \tag{9}$$

2 文献[8]方案的安全性分析及改进

文献[8]提到:文中所提方案不仅可以防止密钥管理者分发假的子密钥,还可以防止不良成员在密钥恢复阶段提供假的影子子密钥.进一步地,文献[8]还得出结论:Shi 方案的安全性取决于整数因子分解和离散对数两大数学难题的困难性.但我们发现,在 Shi 方案中,无论是管理者还是成员都可以轻而易举地进行作弊,以欺骗诚实成员.换句话说,子密钥认证等式(3)和影子子密钥认证等式(7)实际上都是不安全的.另外我们还发现,即使管理者和所有成员都是诚实的,t 个成员仍然可能无法按式(8)恢复出正确的密钥.这说明 Shi 方案有设计错误,原因在于管理者不能将 T_i 取为 Z_N 中的随机数,而应将其取为循环群$\langle g\rangle$中的随机数.下面分小节来详细分析这些安全缺陷,并加以改进.

2.1 文献[8]方案的设计错误

利用 Lagrange 插值公式,Shi 方案中证明了如下结果:

$$a_0 = \sum_{j\in w}(x_j\cdot\Delta_j) \bmod R \tag{10}$$

由此,文献[8]认为下面的两个式子成立,从而根据式(5)即知密钥恢复公式(8)成立:

$$\prod_{j\in w}(A_{ij})^{\Delta_j} = (T_i)^{\sum_{j\in w}(x_j\cdot\Delta_j)} = (T_i)^{a_0} \bmod N \tag{11}$$

$$\prod_{j\in w}(B_{ij})^{\Delta_j}=(C_i)^{\sum_{j\in w}(x_j\cdot\Delta_j)}=(C_i)^{a_0}\ \bmod\ N \tag{12}$$

我们发现,虽然式(10)是正确的,但对于随机选取的 $T_i\in Z_N$,式(11)和式(12)却不一定成立.为方便起见,记 $a=\sum_{j\in w}x_j\cdot\Delta_j$.也就是说,A 是所有 $x_j\cdot\Delta_j(j\in w)$作为整数相加的结果.那么,由式(10)成立可知:存在整数 l,使得 $a=l\cdot R+a_0$.所以我们有 $(T_i)^a=(T_i)^{l\cdot R+a_0}\ \bmod\ N$. 这说明,式(11)成立当且仅当$(T_i)^{l\cdot R}=1 \bmod N$.由于 $\gcd(T_i,N)\neq 1$ 的概率可以忽略,所以可以认为随机数 $T_i\in Z_N^*$.但 T_i 的阶可以是 $1,2,p',q',2p',2q',p'q'$和 $2p'q'$中的任何一个(参考文献[9]中的 Proposition 1).所以,当 T_i的阶含有因子 2 而 l 又是奇数时,等式$(T_i)^{l\cdot R}=1 \bmod N$ 不成立.在这种情况下,即使所有成员诚实地拿出他们所持有的影子子密钥,也无法按式(8)恢复出密钥 S_i.改进的方法很简单,密钥管理者随机选取一个数 $t_i\in Z_R^*$,然后置 $T_i=g^{t_i}\bmod N$ 即可.经过这一改进后,T_i 的阶是 $R(=p'q')$,于是有 $T_i^R=(g^R)^{t_i}=1\bmod N$,从而式(11)成立.同理,由式(4)可知 $C_i^R=1\bmod N$,所以式(12)也成立.

2.2 密钥管理者的欺骗

文献[8]提到:只要 Shi 方案中的密钥管理者 D 给成员 U_j 分发假的子密钥 $\bar{x}_j\neq x_j$,U_j 就可以通过子密钥认证等式(3)发现 D 的欺骗行为.实际上,D 仍可欺骗各个成员,方法如下:D 先按式(2)计算出 x_j 和 P_j,然后选取随机数 $x\in Z_R^*$ 并计算如下的 $\bar{x}_j$, $\bar{y}_j$ 和 $\bar{P}_j$:

$$\bar{x}_j=x_j\cdot x \bmod N,\quad \bar{y}_j=g^{\bar{x}_j}\bmod N,\quad \bar{P}_j=P_j\cdot x^{-1}\bmod R \tag{13}$$

这之后,管理者 D 将 $\{g^{\bar{P}_j}\bmod N,\bar{x}_j\}$ 安全地发送给 U_j,而将 $\bar{y}_j$ 作为公开信息放入 NB.容易看出:由于 $\bar{P}_j\bar{x}_j=P_jx^{-1}x_jx \bmod R=P_jx_j \bmod R$,所以 $\{g^{\bar{P}_j}\bmod N,\bar{x}_j\}$ 满足式(3),故 U_j 不能检验出他收到的 $\bar{x}_j$ 实际上是假的子密钥.这样,当某个或某些持有假子密钥的成员参加密钥恢复时,即使所有人都诚实地按照式(6)计算(A_{ij},B_{ij}),他们按式(8)恢复出来的密钥将不是 S_i 而是某个假的密钥 $\bar{S}_i$.其原因在于:此时式(10)不再成立(因为某些 x_j 被替换成了 $\bar{x}_j$).

下面的方法可以克服上述管理者欺骗问题.D 仍按式(2)计算 x_j 和 y_j,并将 x_j 秘密传送给 U_j 而将 y_j 公开.U_j 在接到 x_j 后,先在整数环中计算 $P_j=\prod_{k\in A\setminus\{j\}}(ID_j-ID_k)$,然后检查:

$$y_j\equiv g^{x_j}\bmod N,\quad (g^{x_j})^{P_j}\equiv\prod_{k=0}^{t-1}(V_k)^{ID_j^k}\bmod N \tag{14}$$

若上面的两个恒等式都成立,则认为 D 是诚实的;否则,U_j 提出抱怨.

2.3 成员的欺骗

文献[8]提到:不良成员 U_j 想要提供假的影子子密钥 $\bar{A}_{ij}$ 和相应的认证信息 $\bar{B}_{ij}$,使得 $(\bar{A}_{ij},\bar{B}_{ij})$ 满足影子子密钥认证等式(7),取决于他知道 d 或 R,而要获取 d 或 R 就得求解因子分解问题.但我们发现,U_j 根本不必知道 d 或 R 的值,更不必分解 N,就可以轻松地伪造一对假的 $(\bar{A}_{ij},\bar{B}_{ij})$ 使得式(7)满足.方法如下:U_j 首先按式(6)计算出正确的(A_{ij},B_{ij}),然后选取一个随机数 $r\in Z_N$,并按下式计算 $(\bar{A}_{ij},\bar{B}_{ij})$:

$$\bar{A}_{ij}=A_{ij}\cdot r^e \bmod N,\quad \bar{B}_{ij}=B_{ij}\cdot r^{2+e(r_i+1)}\bmod N \tag{15}$$

由于(A_{ij},B_{ij})满足式(7),因此我们有

$$\begin{aligned}(\bar{B}_{ij})^e&=(B_{ij})^e\cdot(r^{2+e(r_i+1)})^e \bmod N\\&=(y_j)^{er_i-1}\cdot(A_{ij})^{2+e(r_i+1)}\cdot(r^e)^{2+e(r_i+1)}\bmod N\\&=(y_j)^{er_i-1}\cdot(A_{ij}\cdot r^e)^{2+e(r_i+1)}\bmod N\\&=(y_j)^{er_i-1}\cdot(\bar{A}_{ij})^{2+e(r_i+1)}\bmod N\end{aligned} \tag{16}$$

这说明,U_j 按式(15)伪造出的 $(\bar{A}_{ij},\bar{B}_{ij})$ 也满足影子子密钥认证等式(7).所以,当 U_j 提供了假的 $(\bar{A}_{ij},\bar{B}_{ij})$ 时,其他合作者无法根据式(7)检查出 U_j 是作弊者.由此导致的结果是,诚实成员恢复出的是假的密钥 $\bar{S}_i$.而利用诚实

成员提供的正确的影子子密钥和自己的影子子密钥(A_{ij},B_{ij}),不良成员 U_j 却可以恢复出正确的密钥 S_i.

现在,我们可以给出一个非交互式的知识证明协议,以确保不良成员 U_j 无法作弊.我们所给出的协议使得 U_j 能向其他成员证明:他知道一个秘密 x_j 满足以下 3 个离散对数等式,但不泄漏 x_j 的值到底是多少:

$$\log_g y_i = \log_{T_i} A_{ij} = \log_{C_i} B_{ij} (= x_j) \tag{17}$$

先引入几个记号.记 l_g=|R|,即 g 的阶 R 是一个 l_g 比特长的整数(若取 N 为 1024 比特长的整数,则 l_g=|R|=1022).假设安全参数 k 是 Hash 函数的输出长度,而ε控制统计零知识证明的紧度(一般可取 k=160,ε=9/8).又设 $H(\cdot)$是一个公开的安全 Hash 函数 $H(\cdot)$:$\{0,1\}^* \to \{0,1\}^k$.

定义 **1**. 一个满足 $c_{ij} \equiv H(g \| T_i \| C_i \| y_j \| A_{ij} \| B_{ij} \| g^{s_{ij}} y_j^{c_{ij}} \| T_i^{s_{ij}} A_{ij}^{c_{ij}} \| C_i^{s_{ij}} B_{ij}^{c_{ij}} \| M)$ 的二元对$(c_{ij},s_{ij}) \in \{0,1\}^k \times \pm\{0,1\}^{\varepsilon(l_g+k)+1}$对称为 3 个离散对数 $\log_g y_i$, $\log_{T_i} A_{ij}$ 和 $\log_{C_i} B_{ij}$ 相等的、依赖于消息 M 的知识签名(signature of knowledge).

对于知道秘密 x_j 的成员 U_j,他可以先选取一个随机数 $t \in \pm\{0,1\}^{\varepsilon(l_g+k)}$,然后按如下公式计算出知识签名$(c_{ij},s_{ij})$: $c_{ij} = H(g \| T_i \| C_i \| y_j \| A_{ij} \| B_{ij} \| g^{s_{ij}} y_j^{c_{ij}} \| T_i^{s_{ij}} A_{ij}^{c_{ij}} \| C_i^{s_{ij}} B_{ij}^{c_{ij}} \| M)$,$s_{ij}$=$t$–$c_{ij}x_j$.这里的 s_{ij} 是在整数环 Z 中计算的.容易验证:如此产生的(c_{ij},s_{ij})满足定义 1.另外,式(18)中的消息 M 可以包含产生知识签名的日期、时间、要恢复密钥的 S_i 的序列号等,但也可以将 m 取为空消息.

实际上,上述的知识协议只是文献[9]中 Definition 5 的简单推广.采用文献[9,10]的记号,可以将这一知识签名协议简记为

$$SPK\{(x_j): y_j = g^{x_j} \wedge A_{ij} = T_i^{x_j} \wedge B_{ij} = C_i^{x_j}\}(M) \tag{18}$$

根据文献[9–11]的研究结果,在强 RSA 假设下,上述知识签名协议在随机预言模型下(the random oracle model)[12]是安全的,即该协议既是可模拟的(simulatable),又是对于适应性选择消息攻击存在性不可伪造的(existentially unforgeable against adaptive chosen message attacks).这说明,对于不知道秘密 x_j 的攻击者,即使他知道 U_j 所产生的多个知识签名对,他能产生新的、满足定义 1 的知识签名的成功概率也是可以忽略的.同时,对于不满足等式(17)的对(A_{ij},B_{ij}),U_j 想要产生一个知识签名对(c_{ij},s_{ij})满足定义 1 的概率也是可以忽略的.也就是说,在我们给出的上述影子子密钥认证协议中,任何一个提供了假的影子子密钥的成员,在现实中一定会被其他成员(验证者)发现.

事实上,知识签名是一种具有广泛应用范围的知识证明协议,可用于构造可公开可验证密钥共享[13,14]、群签名[9,10]、门限签名[15]以及门限不可否认签名方案[16]等.

3 结束语

密钥共享[1–8,17]是现代密码学的一个重要工具.在现实系统中使用密钥共享,有利于保护系统密钥,减小密钥持有者的责任,降低敌手破译密钥的成功率.Shi 给出的一种高效的多重密钥共享认证方案[8]不仅成员持有的子密钥能重复使用,而且管理者分发的子密钥和成员提供的影子子密钥都是可认证的.本文对 Shi 方案的安全性进行了分析:首先指出该方案的一个设计错误;然后给出两个攻击,以表明该方案中的子密钥和影子子密钥认证方法实际上都是不安全的.另外,为了避免上述设计错误和攻击,我们还给出了有效的改进方法.

References:

[1] Shamir A. How to share a secret. Communications of the ACM, 1979,22(11):612–613.

[2] Blakley GR. Safeguarding cryptographic keys. In: Proc. of the National Computer Conf. AFIPS Conf. proc. AFIPS Press, 1979,48: 313–317.

[3] Tompa M, Woll H. How to share a secret with cheaters. Journal of Cryptology, 1988(1):133–138.

[4] Stadler M. Publicly verifiable secret sharing. In: Maurer UM, ed. Proc. of the EUROCRYPT'96. LNCS 1070, Berlin: Springer-Verlag, 1996. 190–199.

[5] He J, Dawson E. Multistage secret sharing based on one-way function. Electronics Letters, 1994,30(19):1591–1592.

[6] He J, Dawson E. Multisecret-Sharing scheme based on one-way function. Electronics Letters, 1995,31(2):93−95.

[7] Harn L. Efficient sharing (broadcasting) of multiple secrets. IEE Computers and Digital Techniques, 1995,142(3):237−240.

[8] Shi RH. A multisecret sharing authenticating scheme. Chinese Journal of Computers, 2003,26(5):552−556 (in Chinese with English abstract).

[9] Ateniese G, Camenisch J, Joye M, Tsudik G. A practical and provably secure coalition-resistant group signature scheme. In: Bellare M, ed. Proc. of the CRYPTO 2000. LNCS 1880, Berlin: Springer-Verlag, 2000. 255−270.

[10] Camenisch J, Stadler M. Efficient group signature schemes for large groups. In: Jr Kaliski BS, ed. Proc. of the CRYPTO'97. LNCS 1294, Berlin: Springer-Verlag, 1997. 410−424.

[11] Pointcheval D, Stern J. Security arguments for digital signatures and blind signatures. Journal of Cryptology, 2000,13(3):361−396.

[12] Bellare M, Rogaway P. Random oracles are practical: A paradigm for designing efficient protocols. In: Proc. of the 1st ACM Conf. on Computer and Communications Security. New York: ACM Press, 1993. 62−73.

[13] Schoenmakers B. A simple publicly verifiable secret sharing scheme and its application to electronic voting. In: Michael J, Wiener MJ, eds. Proc. of the CRYPTO'99. LNCS 1666, Berlin: Springer-Verlag, 1999. 148−164.

[14] Wang GL, Qing SH, Ma HT. Security proof to a publicly verifiable secret sharing scheme. In: Zhang HG, Wang LN, eds. Proc. of the 3rd Chinese Conf. of Information and Communications Security—CCICS 2003. Beijing: Sciences Press, 2003. 268−276 (in Chinese with English abstract).

[15] Shoup V. Practical threshold signatures. In: Preneel B, ed. Proc. of the EUROCRYPT 2000. LNCS 1807, Berlin: Springer-Verlag, 2000. 207−220.

[16] Wang G, Qing S, Wang M, Zhou Z. Threshold undeniable RSA signature scheme. In: Qing S, Okamoto T, Zhou J, eds. Proc. of the Information and Communications Security (ICICS 2001). LNCS 2229, Berlin: Springer-Verlag, 2001. 221−232.

[17] Liu HP, Hu MZ, Fang BX, Yang YX. A dynamic secret sharing scheme based on one-way function. Journal of Software, 2002,13(5):1009−1012 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/13/1009.pdf

附中文参考文献:

[8] 施荣华.一种多重密钥共享认证方案.计算机学报,2003,26(5):552−556.

[14] 王贵林,卿斯汉,马恒太.一个可公开验证秘密共享方案的安全性证明.见:张焕国,王丽娜,编.第 3 届中国信息和通信安全学术会议论文集——CCICS 2003.北京:科学出版社,2003.268−276.

[17] 刘焕平,胡铭曾,方滨兴,杨义先.基于单向函数的动态密钥分存方案.软件学报,2002,13(5):1009−1012. http://www.jos.org.cn/1000-9825/13/1009.pdf

王贵林(1968－),男,云南漾濞人,博士,主要研究领域为密码学基础及应用.

卿斯汉(1939－),男,研究员,博士生导师,CCF 高级会员,主要研究领域为信息系统安全理论和技术.