高效可撤销成员的不可链接的群盲签名方案*)

刘文远　宋春梅
(燕山大学信息科学与工程学院　秦皇岛 066004)

摘　要　在 ACJT 方案的基础上实现了一成员可撤销的群盲签名方案。借鉴陈的成员撤销思想，对签名过程进行了改进，将原方案的两个零知识证明减少为一个，减少了模指数运算，缩短了签名长度，同时将 C. Popescu 的群盲签名思想加入到签名过程中，使改进的成员可撤销的群签名增加了盲性，改进后同时解决了 C. Popescu 提出的群盲签名方案可链接性的缺陷。实现的成员可撤销的不可链接的群盲签名方案，可应用于多银行电子现金系统中，用来实现成员可撤销的多银行电子现金系统，使电子现金系统更接近现实金融系统。

关键词　成员可撤销，ACJT 方案，效率，群盲签名

New Efficient Group Blind Signature Scheme with Membership Revocation and Unlinkability

LIU Wen-yuan　SONG Chun-mei
(Institute of Information Science and Engineering , Yanshan University, Qinhuangdao 066004, China)

Abstract　A new efficient group blind signature scheme with membership revocation on the basis of ACJT group scheme was provided. Drawing on the thought of the membership revocation of Chen , in the process of signature, it only uses a random number to decrease two zero-knowledge proofs of the original program to one, and decreases the mode index operation, thus shortens the length of signatures, while the group blind signature thinking proposed by C. Popescu is joined in the signature process, increases blind to the improved group signature with the membership revocation, and the program has also effectively addressed the flaw of linkability of the group blind signature programs proposed by C. Popescu. The new efficient group blind signature scheme with membership revocation and unlinkability can be applied to multi-bank electronic cash system, used to realize the multi-bank electron cash system which can abolish the group members, enables the electronic cash system to conform to the application of the real financial system.

Keywords　Members revocation, ACJT scheme, Efficiency, Group blind signature

1　引言

群签名最早是由 Chaum 和 Heyst[1] 在 EUROCRYPT'91 上提出的。在群签名方案下，群体中的任意一个成员可以代表群体进行匿名签名，验证者只能验证该签名是否由群体中的成员所签，而不能确定是哪个成员。当然，群成员的匿名性是可撤消的。在发生争执时，群管理者可以打开签名来揭露签名者的身份，使得签名者不能否认。1997 年，J Camenisch 和 M Stadler[2] 首次提出适用于大群体的群签名方案，该方案是第一个群公钥长度、群签名长度与群成员个数无关的群签名方案，并且当有新成员加入时无需更改群公钥。这个方案的提出标志着对群签名的研究进入了一个新的阶段，研究的焦点集中到如何有效地撤消成员，如何提高打开及验证算法的效率，以及寻找新的安全高效的群签名算法等几个方面。2000 年，G Ateniese[3] 等人提出了一个新的群签名方案（简称 ACJT 方案），该方案被证明在强 RSA 假设和 Diffie-Hellman 假设下能够抵抗联合攻击，同时又具有不错的效率，因此很受关注 。后来国内外许多学者在此基础上提出了许多成员撤销方案，大多数效率都不是很高，群签名中签名和验证算法的计算量要么依赖于当前的群成员个数，要么依赖于被撤消的成员个数。2005 年，陈泽文[4] 等提出一个新的撤消方案，与以前的方案相比，该方案较为高效，因为该方案签名长度固定，撤消一个成员，群管理者只需做一次乘法运算来更新群公钥，而以前方案需要做多次的指数运算，签名和验证算法均独立于目前的成员个数和撤消的成员个数，但缺陷是签名验证过程中用到了两个知识证明，计算量很大。

1998 年，A. Lysyanskaya 和 Z. Ramzan[5] 在国际金融密码会议（FC98）上首次将群签名和盲签名的概念有机地结合起来，设计了第一个群盲签名方案——Lys98 方案，并用该群盲签名方案构造了一个在线的、匿名的电子现金系统；但是该方案采用计算量很大的双重离散对数知识签名和离散对数次根知识签名，所以签名特别长，群盲签名中数据传输量也特别大，从而使系统的效率很低，并且后来被发现方案不能抵抗联合攻击。2003 年，C. Popescu[6] 提出的群盲签名方案是以 G Ateniese[3] 等的有效的可抗合谋攻击的群签名方案为基础，但该方案具有可链接性。

本文借鉴了陈的成员撤销的思想，在签名过程中将原方案的两个知识证明减为一个，缩短了签名长度，同时将 C. Popescu 提出的群盲签名思想加入到签名过程中，使改进的群签名增加了盲性，并且方案同时还有效解决了 C. Popescu

*)基金项目：国家科技部高新技术计划项目（2005EJ000017），国家电子信息发展基金及河北省信息产业发展计划项目（2005035025），河北省自然科学基金（F2005000368）资助。**刘文远**　博士生导师，研究方向为电子商务、信息安全、智能计算；**宋春梅**　硕士研究生，研究方向为电子商务、信息安全、密码学。

提出的群盲签名方案的可链接性的缺陷，最后实现了一个成员可撤销且不可链接的群盲签名方案。

2 预备知识

设 $G=\langle g\rangle$ 是有限循环群，其阶 $\#G$ 未知，但阶的最大二进制长度 l_G 是公开的，$y\in G$，对 g 的离散对数是满足 $y=g^x$ 的整数，$x\in Z$。有一个无碰撞的 hash 函数 $H:\{0,1\}^*\rightarrow\{0,1\}^k$，该函数把任意长度的二进制串映射为一个 k-bit 的 hash 值。

2.1 困难性假设

假设 1(强 RSA 假设) 存在一个概率算法 T，使得对所有的概率多项式时间的算法 A，所有的多项式 $p(\cdot)$ 和所有充分大的 lg：$Pr[z=u^e\mid(G,z):=T(1^{lg}),(u,e>1):=A(G,z)]<1/p(lg)$。

假设 2(Diffie-Hellman 假设) 不存在这样的概率多项式时间算法，该算法能以不可忽略的概率区分出分布 D 和 R，这里，$D=(g,g^x,g^y,g^z)$，$x,y,z\in_R Z_{\#G}$，$R=(g,g^x,g^y,g^{xy})$，$x,y\in_R Z_{\#G}$。

平方剩余群 QR(n) 令 $n=pq$ 为一个 RSA 体制的模数，$p=2p'+1$，$q=2q'+1$ 且 p,p',q,q' 均为素数。全体模 n 的平方剩余在模乘运算下构成群 Z_n^* 的一个循环子群，记为 $QR(n)$。已知 $QR(n)$ 的阶为 $p'q'$，通常认为在循环群 $QR(n)$ 上，强 RSA 假设成立。

3 改进的成员可撤销的群盲签名方案

设 $\varepsilon>1$，k 和 l_p 为安全参数，定义两个整数区间 $\Delta=[2^{\lambda_1}-2^{\lambda_2},2^{\lambda_1}+2^{\lambda_2}]$，$\Gamma=[2^{\gamma_1}-2^{\gamma_2},2^{\gamma_1}+2^{\gamma_2}]$

这里，$\lambda_1>\varepsilon(\lambda_2+k)+2$，$\lambda_2>4l_p$，$\gamma_1>\varepsilon(\gamma_2+k)+2$，$\gamma_2>\lambda_1+2$

1)初始化

a) 群管理者 GM 随机地秘密选择 l_p 比特的素数 p',q'，使得 $p=2p'+1$，$q=2q'+1$ 为素数。令 $n=pq$，$H()$ 是一个抗合谋攻击的散列函数

b)GM 随机选择 a，a_0，g，$h\in_R QR(n)$

c)GM 随机地秘密选择 $x\in Z_{p'q'}$，令 $y=g^x \bmod n$

d)群公钥为 $Y=(n,a,a_0,y,g,h)$

e)GM 的私钥为 $S=(p',q',x)$

2)成员加入

a)成员 U_i 产生一秘密值 $\tilde{x}_i\in[0,2^{\lambda_1}]$，一个随机整数 $\tilde{r}\in[0,n^2]$，计算 $C_1=g^{\tilde{x}_i}h^{\tilde{r}}$ 并将 C_1 发送给 GM，并证明 C_1 的正确性。

b)GM 检查 $C_1\in QR(n)$，若成立，则随机选择 α_i 和 $\beta_i\in[0,2^{\lambda_1}]$，将 α_i 和 β_i 传给成员 U_i。

c)成员 U_i 计算，$x_i=2^{\lambda_1}+(\alpha_i\tilde{x}_i+\beta_i \bmod 2^{\lambda_2})$，将 $C_2=a^{x_i} \bmod n$ 传给 GM，同时向 GM 证明：C_2 对 a 的离散对数在 Δ 内；知道 u,v,w 使得 u 在 $[-2^{\lambda_1},2^{\lambda_1}]$ 内；u 等于 $C_2/a^{2^{\lambda_1}}$ 对 a 的离散对数；$C^{\alpha_i\beta_i}$ 等于 $g^u(g^{2^{\lambda_2}})^v h^w$。

d)GM 检查 $C_2\in QR(n)$，若成立且上述证明正确，则 GM 选择一素数 $e_i\in\Gamma$，计算 $A_i=(C_2a_0)^{1/e_i}$，并发给用户 U_i 的成员证书 $[A_i,e_i]$。

e)U_i 验证 $a^{x_i}a_0=A_i^{e_i} \bmod n$。

3)成员撤销

假设 $E_{delete}:=\{U_1,U_2,\cdots,U_m\}$ 为现有撤消成员集合，群管理者计算 $E:=e_{u_1}\cdots e_{u_m}$ 并公布，其中 e_{U_i} 是对应成员 U_i 证书的素数。当有一些成员要被撤消，令 E' 是欲被撤消成员的 e_{U_j} 的乘积，群管理者通过计算 $E=E'E$ 来更新群公钥，并在一个公共的目录上公布最新的 E，当前的时间 t 和所有撤消成员的 e_{U_i}。

4)签名过程

签名者首先根据群管理者公布的当前时间 t 的成员撤销验证公钥 E，利用 GCD 算法计算 $A'e_i+B'E=1$ 中的 A' 和 B'，保持 (A',B') 直到 E 发生变化。签名者对签名接收的消息 m 签名如下：

(1)签名者选一随机数 $w\in\{0,1\}^{2l_p}$，并用证书秘钥 (A',B')，并计算

$\tilde{A}=A_iy^w \bmod n$，$\tilde{B}=g^w \bmod n$

$\tilde{D}=g^{e_i}h^w \bmod n$，$\tilde{F}=\tilde{D}^{A'}h^{we_i} \bmod n$

$\tilde{G}=(g^E)^{B'}h^{-we_i} \bmod n$，$\tilde{K}=h^{-A'w} \bmod n$

选择随机数 $\tilde{r}_1\in\pm\{0,1\}^{\varepsilon(\gamma_2+k)}$，$\tilde{r}_2\in\pm\{0,1\}^{\varepsilon(2l_p+k)}$，$\tilde{r}_3\in\pm\{0,1\}^{\varepsilon(\gamma+2l_p+k+1)}$，$\tilde{r}_4,\tilde{r}_5,\tilde{r}_6,\tilde{r}_7,\tilde{r}_8\in\pm\{0,1\}^{\varepsilon(2l_p+k)}$ 并计算

$\tilde{t}_1=\tilde{A}^{\tilde{r}_1}/(a^{\tilde{r}_2}y^{\tilde{r}_3})$，$\tilde{t}_2=\tilde{B}^{\tilde{r}_1}/g^{\tilde{r}_3}$

$\tilde{t}_3=g^{\tilde{r}_4}$，$\tilde{t}_4=g^{\tilde{r}_1}h^{\tilde{r}_4}$

$\tilde{t}_5=h^{\tilde{r}_5}$，$\tilde{t}_6=\tilde{D}^{\tilde{r}_7}h^{\tilde{r}_3}$

$\tilde{t}_7=(g^E)^{\tilde{r}_8}h^{\tilde{r}_6}$

将 $(\tilde{A},\tilde{B},\tilde{D},\tilde{F},\tilde{G},\tilde{K},\tilde{t}_1,\tilde{t}_2,\tilde{t}_3,\tilde{t}_4,\tilde{t}_5,\tilde{t}_6,\tilde{t}_7)$ 传送给签名接收者。

(2)签名接收者随机选择 $\alpha_1,\alpha_2,\alpha_3,\alpha_4,\alpha_5,\alpha_6,\alpha_7,\alpha_8,\delta\in_R\{0,1\}^{\varepsilon(l_p+k)}$ 并计算

$t_1=a_0^{\delta}\tilde{t}_1\tilde{A}^{\alpha_1-\delta 2^{\gamma_1}}/(a^{\alpha_2-\delta 2^{\lambda_1}}y^{\alpha_3})$

$t_2=\tilde{t}_2\tilde{B}^{\alpha_1-\delta 2^{\gamma_1}}/g^{\alpha_3}$，$t_3=\tilde{t}_3\tilde{B}^{\delta}g^{\alpha_4}$

$t_4=\tilde{t}_4\tilde{D}^{\delta}g^{\alpha_1-\delta 2^{\gamma_1}}h^{\alpha_4}$，$t_5=\tilde{t}_5\tilde{K}^{\delta}h^{\alpha_5}$

$t_6=\tilde{t}_6\tilde{F}^{\delta}\tilde{D}^{\alpha_7}h^{\alpha_3}$，$t_7=\tilde{t}_7\tilde{G}^{\delta}(g^E)^{\alpha_8}h^{\alpha_6}$

$C=H(t\|E\|m\|g\|h\|y\|a_0\|a\|\tilde{A}\|\tilde{B}\|\tilde{D}\|\tilde{F}\|\tilde{G}\|\tilde{K}\|t_1\|t_2\|t_3\|t_4\|t_5\|t_6\|t_7)$

$\tilde{C}=C-\delta$

将 $\tilde{C}$ 发给签名者。

(3)签名者收到后计算

$\tilde{S}_1=\tilde{r}_1-\tilde{C}(e_i-2^{\gamma_1})$，$\tilde{S}_2=\tilde{r}_2-\tilde{C}(x_i-2^{\lambda_1})$

$\tilde{S}_3=\tilde{r}_3-\tilde{C}we_i$，$\tilde{S}_4=\tilde{r}_4-\tilde{C}w$

$\tilde{S}_5=\tilde{r}_5+\tilde{C}A'w$，$\tilde{S}_6=\tilde{r}_6+\tilde{C}we_i$

$\tilde{S}_7=\tilde{r}_7-\tilde{C}A'$，$\tilde{S}_8=\tilde{r}_8-\tilde{C}B'$

发送 $(\tilde{S}_1,\tilde{S}_2,\tilde{S}_3,\tilde{S}_4,\tilde{S}_5,\tilde{S}_6,\tilde{S}_7,\tilde{S}_8)$ 给签名接收者。

(4)签名接受者收到后计算

$S_i=\tilde{S}_i+\alpha_i(1\leqslant i\leqslant 8)$，

$A=\tilde{A}^{H(C\|S_1\|S_2\|S_3\|S_4)} \bmod n$

$B=\tilde{B}^{H(C\|S_1\|S_2\|S_3\|S_4)} \bmod n$

$D=\tilde{D}^{H(C\|S_1\|S_2\|S_3\|S_4\|A\|B)} \bmod n$

$F=\tilde{F}^{H(C\|S_4\|S_5\|S_6\|S_7\|S_8)} \bmod n$

$G=\tilde{G}^{H(C\|S_4\|S_5\|S_6\|S_7\|S_8)} \bmod n$

$K=\tilde{K}^{H(C\|S_4\|S_5\|S_6\|S_7\|S_8)} \bmod n$

最后得到关于 m 的群盲签名 $(t,C,S_1,S_2,S_3,S_4,S_5,S_6,S_7,S_8,A,B,D,F,G,K)$。

5)验证过程

验证者根据签名时间 t 找出当时的撤销验证公钥 E 并计算

$b_1=1/H(C\|S_1\|S_2\|S_3\|S_4)$

$b_2=1/H(C||S_1||S_2||S_3||S_4||A||B)$

$b_3=1/H(C||S_4||S_5||S_6||S_7||S_8)$

$t'_1=(a_0{}^C A^{b_1(S_1-C2^{\gamma_1})}/(a^{S_2-C2^{\lambda_1}}y^{S_3}))\bmod n$

$t'_2=(B^{b_1(S_1-C2^{\gamma_1})}/g^{S_3})\bmod n$

$t'_3=B^{b_1C}g^{S_4}\bmod n$

$t'_4=D^{b_2C}g^{S_1-C2^{\gamma_1}}h^{S_4}\bmod n$

$t'_5=K^{b_3C}h^{S_5}\bmod n$

$t'_6=D^{b_2S_7}F^{b_3C}h^{S_3}\bmod n$

$t'_7=G^{b_3C}h^{S_6}(g^E)^{S_8}\bmod n$

$C=H(t||E||m||g||h||y||a_0||a||A^{b_1}||B^{b_1}||D^{b_2}||F^{b_3}||G^{b_3}||K^{b_3}||t'_1||t'_2||t'_3||t'_4||t'_5||t'_6||t'_7)$

验证 $C=?\ \tilde{C}$，若成立，则计算验证 $F^{b_3}G^{b_3}K^{b_3}\bmod n=?\ g$，若成立则接受此群盲签名。

(6)打开

①群管理者进行和步(5)一样的验证过程检验签名的有效性。

②用自己的私钥计算 $A_i=(A/B^x)^{b_1}$，其中 $b_1=1/H(C||S_1||S_2||S_3||S_4)$

即可找到签名者的身份，同时给关于自己私钥的证明 $SPK\{(x):y=g^{x\wedge}A/A_i^{1/b_1}=B^x\}$

4 性能分析

4.1 正确性

方案中群盲签名过程中，签名者利用自己选取的随机数 w 及自己的签名证书 $[A_i,e_i]$，使用群管理员的公钥 y 利用 ELGamal 来加密 A_i，用户和签名者交互生成群盲签名。

$$t'_1=(a_0{}^C A^{b_1(S_1-C2^{\gamma_1})}/(a^{S_2-C2^{\lambda_1}}y^{S_3}))\bmod n$$
$$=(a_0{}^{\delta}\tilde{A}^{(a_1-\delta 2^{\gamma_1})}/(a^{a_2-\delta 2^{\lambda_1}}y^{a_3})*\tilde{t}_1)\bmod n=t_1$$

$$t'_2=(B^{b_1(S_1-C2^{\gamma_1})}/g^{S_3})\bmod n$$
$$=([\tilde{B}^{(\tilde{S}_1-\tilde{C}2^{\gamma_1})}/g^{\tilde{S}_3}]*[\tilde{B}^{(a_1-\delta 2^{\gamma_1})}/g^{\delta_3}])\bmod n$$
$$=(\tilde{t}_2*[\tilde{B}^{(a_1-\delta 2^{\gamma_1})}/g^{\delta_3}])\bmod n=t_2$$

$$t'_3=\tilde{B}^{b_1C}g^{S_4}\bmod n=\tilde{B}^{\tilde{C}+\delta}g^{\tilde{S}_4+\alpha_4}\bmod n$$
$$=\tilde{B}^{\delta}g^{\alpha_4}\tilde{B}^{\tilde{C}}g^{\tilde{S}_4}\bmod n=\tilde{B}^{\delta}g^{\alpha_4}\tilde{t}_3\bmod n=t_3$$

$$t'_4=D^{b_2C}g^{S_1-C2^{\gamma_1}}h^{S_4}\bmod n$$
$$=\tilde{D}^{\delta}g^{a_1}h^{a_4}(g^{e_i}h^{w})^{\tilde{C}}g^{(\tilde{S}_1-(\tilde{C}+\delta)2^{\gamma_1})}h^{\tilde{S}_4}\bmod n$$
$$=\tilde{D}^{\delta}g^{a_1}h^{a_4}g^{(e_i\tilde{C}+\tilde{S}_1-\tilde{C}2^{\gamma_1}-\delta 2^{\gamma_1})}h^{\tilde{S}_4+\tilde{C}w}\bmod n$$
$$=\tilde{D}^{\delta}g^{a_1}h^{a_4}\tilde{t}_4\bmod n=t_4$$

$$t'_5=K^{b_3C}h^{S_5}\bmod n=\tilde{K}^{\tilde{C}+\delta}h^{\tilde{S}_5+\alpha_5}\bmod n$$
$$=\tilde{K}^{\delta}h^{a_5}h^{\tilde{r}_5+\tilde{C}Aw}h^{-\tilde{C}Aw}\bmod n$$
$$=\tilde{K}^{\delta}h^{a_5}h^{\tilde{r}_5}\bmod n=t_5$$

$$t'_6=D^{b_2S_7}F^{b_3C}h^{S_3}\bmod n$$
$$=\tilde{D}^{\tilde{S}_7+\alpha_7}h^{\tilde{S}_3+\alpha_3}\tilde{F}^{\tilde{C}+\delta}\bmod n$$
$$=(\tilde{F}^{\delta}\tilde{D}^{a_7}h^{a_3}*\tilde{D}^{\tilde{r}_7}h^{\tilde{r}_3}(D^Ah^{e_iw})^{-\tilde{C}}\tilde{F}^{\tilde{C}})\bmod n$$
$$=\tilde{F}^{\delta}\tilde{D}^{a_7}h^{a_3}*\tilde{t}_6\bmod n=t_6$$

$$t'_7=G^{b_3C}h^{S_6}(g^E)^{S_8}\bmod n$$
$$=\tilde{G}^{\tilde{C}+\delta}h^{\tilde{S}+\alpha_6}(g^E)^{S_8+\alpha_8}\bmod n$$
$$=((g^E)^{a_8}h^{a_6}\tilde{G}^{\delta}*(g^E)^{\tilde{r}_8-\tilde{C}B}h^{\tilde{r}_6+\tilde{C}we_i}\tilde{G}^{\tilde{C}})\bmod n$$
$$=((g^E)^{a_8}h^{a_6}\tilde{G}^{\delta}*\tilde{t}_7)\bmod n=t_7$$

4.2 盲性

假设签名者能遵循该签名协议，并且拥有无限的计算能力，但是也无法得到任何有关消息 m 与最终得到的群盲签名 $(t,C,S_1,S_2,S_3,S_4,S_5,S_6,S_7,S_8,A,B,D,F,G,K)$ 之间的信息。

证明：首先由于签名过程中签名者并没有得到消息及其相关变形，因此他不可能知道具体的内容。签名者得到 m 和最终的签名 $(t,C,S_1,S_2,S_3,S_4,S_5,S_6,S_7,S_8,A,B,D,F,G,K)$ 后，虽然能够验证其合法性，但是由于签名中的各个元素都经过了盲化处理，并不能将它们与自己曾计算过的参数联系起来，因此他不可能知道该签名是他签署的。

4.3 安全性分析

本文的群盲签名方案的安全性等同于 Ateniese 和 Camenisch 等人[3]提出的群签名体制的安全性。方案的安全性证明是建立在随机预言机模型和强 RSA 以及判定 Difile-Hellman 假设之上。依照 Camenisch 和 Stadle [2]有关离散对数知识签名的表示形式，签名者的签名可表述为

$$SPK\{(\alpha,\beta,\gamma,\theta,\zeta):\tilde{A}=\zeta y^{\theta}\hat{}\ \tilde{B}=g^{\theta}\hat{}\ \tilde{D}=g^{\alpha}h^{\theta}\hat{}\ \tilde{F}=$$
$$\tilde{D}^{\beta}h^{\theta\alpha}\hat{}\ \tilde{G}=(g^E)^{\gamma}h^{-\theta\alpha}\hat{}\ \tilde{K}=h^{\beta\theta}\hat{}\ \tilde{F}\tilde{G}\tilde{K}=g\hat{}\ \alpha\in\Gamma\}$$

类似文献[3]中引理 1 知，在强 RSA 假设下，能给出上述知识签名的人必须拥有一个与 E 互素的数。类似文献[3]中定理 1 知，在强 RSA 假设下，上述的 SPK 交互协议是一个关于证明者知道数 α 和 E 互素的统计零知识证明 。

①不可伪造性：在强 RSA 假设下，上述群盲签名方案中的交互式协议是关于证明者知道成员证书和相应的签名密钥的统计零知识的知识证明。只有合法群成员才能代表群体进行群盲签名。

②不可链接性：因为在签名过程中没有泄漏有用信息，每次签名时签名者都随机选取数 w，与签名绑定在一起，使得判断两个不同群盲签名是否来自同一个签名者在计算上是困难的，即使当一个成员被撤消后，即他的 e_i 被公开，其他成员也不能把他跟他过去的签名链接在一块。假设有两个不同的签名 $(t,C,S_1,S_2,S_3,S_4,S_5,S_6,S_7,S_8,A,B,D,F,G,K)$ 和 $(\bar{t},\bar{C},\bar{S}_1,\bar{S}_2,\bar{S}_3,\bar{S}_4\bar{S}_5,\bar{S}_6,\bar{S}_7,\bar{A},\bar{B},\bar{D},\bar{F},\bar{G},\bar{K})$，当 e 公开时，其他人可能知道 A' 和 B'，使 $A'e_i+B'E=1$。若他们想确定这两个签名是否为同一个成员产生，他们必须确定 $\log_y(A^{b_1}/\bar{A}^{b_1})$，$\log_g(B^{b_1}/\bar{B}^{b_1})$ 跟 $\log_h(D^{b_2}/\bar{D}^{b_2})$，$\log_h(K^{b_3}/\bar{K}^{b_3})*(1/(-A'))$ 是否相等或 $\log_h(F^{b_3}/\bar{F}^{b_3})$ 跟 $\log_h(G^{b_3}/\bar{G}^{b_3})$ 是否相等，在 Diffie-Hellman 假设下，这是不可能的。

③匿名性：因为在签名过程中没有泄漏有用信息，所以想从公共参数中获得成员证书中的秘密值相当于求解离散对数。当一个成员的 e_i 被泄漏时，类似不可链接性的分析，可以知道匿名性仍然满足。

④可跟踪性：群管理员可根据情况随时打开一个群成员的签名，确定该成员的身份。

⑤抗陷害性：群成员和群管理者都不能代表其他成员进行签名。由于证书仅能由群管理者生成签发，群成员不能代表其他群成员进行签名，其次，群管理者没有成员的密钥 x_i，因此群管理员也不能产生有效签名。

⑥可撤销性：对一个拥有证书 (A_i,e_i) 的被撤消的成员来说，他有两种可能的方式来证明其是合法用户：(1) 另外选择一个与 e_i 不同且与 E 互素的 e 来证明成员资格，由于证书仅能由群管理者生成签发，因此这是无法实现的，(2)还用原来的 e_i 来证明成员资格，在强 RSA 假设下，知识证明签名仅能由某个使用与 E 互素的数的人给出，并且由于不可伪造性也决定伪造签名的不可行性，因此这也是无法实现的。

(下转第 206 页)

表 3　小波域水印嵌入前后图像特征变化量

图像 \ 属性	△Y = $Y_{前} - Y_{后}$				
	△V	△RGB	△I	△G	△T
a	0k	(0,0,0)	0.03	0-0	−0.0008
b	0k	(0,0,0)	−0.57	1-0	−0.0035
c	0k	(0,0,0)	−0.57	0-0	0.0046
d	0k	(0,0,0)	−0.25	0-0	−0.0062

表 4　两种算法的 PSNR 值

属性 \ 图像		a	b	c	d
PSNR	小波域	34.7052	51.3835	39.9574	37.4089
	空间域	35.4039	35.7251	36.1554	31.2821

抗攻击实验是验证水印鲁棒性的有力手段，一个好的水印算法必须经过各种攻击测试才能对其作出客观的评价。攻击方法包括添加椒盐噪声、JPEG 压缩、剪切、中值滤波、锐化等。经过各种攻击后提取出的水印如图 4 所示。

图 4　各种攻击后提取出的水印图

由图 4 可以看出，从总体上说，小波域算法的数字水印在上述 5 种攻击的情况下，提取出的水印大部分能够较清晰的辨认，但对剪切攻击和中值滤波的抗攻击性较差些，而对 JPEG 压缩和锐化的抗攻击性较好。

结束语　基于人眼视觉系统（HVS）的图像数字水印技术已成为了当前数字水印领域研究的一个热点，该技术利用图像的局部特性，结合人眼视觉系统的特性来解决数字水印的鲁棒性和不可见性之间的矛盾，在保证嵌入的水印有足够强鲁棒性的前提下同时满足视觉不可感知性的要求。

本文提出了一种改进的基于人眼视觉特性和小波变换的彩色图像数字水印算法。该算法采用 YIQ 色彩空间进行水印的嵌入，水印信息为有意义的二值水印图像，为了提高安全性与抗干扰性，水印嵌入前采用 Arnold 变换对其进行三次随机置乱处理。在嵌入过程中，利用视觉系统的亮度掩蔽、纹理掩蔽、边缘掩蔽等特性将 Y 分量的小波系数进行分类，计算 JND 阈值并对小波系数进行量化，然后将置乱后的三个水印序列以不同强度嵌入到不同方向的小波系数中。本文对此算法在 Matlab 下进行实验，首先进行水印的嵌入，结果表明隐蔽性较好；采取一些攻击测试，包括噪声、剪切、滤波、JPEG 压缩等，实验结果证明，该算法具有很好的不可见性，且对常见的攻击具有较好的鲁棒性。

参 考 文 献

[1] Kwon S G, Ban S W. Highly Reliable Digital Watermarking Using Successive Subband Quantization and Human Visual System. IEEE Tans. on Image Processing, 1999, 7(1): 74-92

[2] 江波. 李峰. 一种基于离散小波变换和 HVS 的彩色图像数字水印算法微型机与应用, 2004, 3

[3] Liu Huajian, Kong Xiangwei, Kong Xiang dong, et al. Content based color image adaptive watermarking scheme. IEEE, 2001: 41-44

[4] Parisis A, Carre P, Fernandez-Maloigne C. Color image watermarking with adaptive strength of insertion. IEEE, 2004: 85-88

[5] 肖亮, 韦志辉, 吴慧中. 一种利用人眼视觉掩盖的小波域数字水印. 通信学报, 2002, 3(23): 100-106

[6] 李明, 廖晓峰. 结合混沌的小波变换数字水印技术. 计算机科学, 2007, 34(8): 245-247

（上接第 62 页）

4.4　效率分析

陈泽文等方案的签名长度包括原 ACJT 方案的签名长度和为了成员撤消增加一个知识签名两个部分，原方案签名中增加了 8 次模乘运算，改进后的方案将两个知识签名减为一个知识签名，签名过程中签名者仅增加了 3 次模乘运算，签名长度也缩短了，对应的验证过程计算量也减少，同时本文改进后有效解决了 C. Popescu 提出的群盲签名可以链接的缺陷，使该群盲签名既具有成员可撤销性，又具有不可链接性。

结束语　文中基于 ACJT 群签名方案对陈的撤销方案进行了改进，结合 C. Popescu 提出的群盲签名思想，实现了更高效的成员可撤销的不可链接的群盲签名方案。该方案可应用于多银行电子现金系统中实现具有成员撤销功能的多银行电子现金系统，使电子现金系统更符合现实应用，更加接近现实中的金融系统 。

参 考 文 献

[1] Chaumd, Heyst F. Group signature // Advance in Cryptology-Eurocrypt'91, LNCS. Berlin: Springer-verlag, 1992, 547: 257-265

[2] Camenisch J, Stadler M. Effient Group Signature Schemes for Large Groups [C]// Proceedings of CRYPTO 1997. Berlin: Springer-Verlag, 1997: 410-424

[3] Ateniese G, Camenisch J, Joye M, et al. A Practical and Provably Secure Coalition Resistant Group Signature Scheme [C]// Proceedings of CRYPTO 2000. Berlin: Springer-Verlag, 2000: 255-270

[4] 陈泽文, 王继林, 黄继武, 等. ACJT 群签名方案中成员撤消的高效实现. 软件学报, 2005, 1(1): 151-157

[5] Lysyanskaya A, Ramzan Z. Group blind digital signatures: A scalable solution to electronic cash // Financial Cryptography (FC'98). Lecture Notes in Computer Science. Vol 1465, Springer-Verlag, 1998: 184-197

[6] Popescu C. A Secure and Efficient Group Blind Signature Scheme[J]. Studies in Informaties and Control Journal, 2003 (12): 269-276