一种基于身份信息无可信中心无随机预言的群签名

蔡永泉,刘 岩
(北京工业大学计算机学院,北京 100124)

摘 要: 本文提出了一种标准模型下基于身份的无可信中心的群签名方案,解决了群签名的前向安全性,并分析了新方案的正确性和安全性. 分析结果表明,合法的群成员可以代表群得到有效群签名,仲裁者可以打开签名,且可以判断群管理者是否伪装成合法的群成员. 本文还利用对时间段信息的管理实现了该签名的前向安全性,以抵抗密钥泄漏等情况.

关键词: 基于身份群签名; 无随机预言; 无可信中心; 前向安全; 双线性映射
中图分类号: TP309 **文献标识码**: A **文章编号**: 0372-2112 (2009) 4A-087-05

An ID-based Group Signature Scheme Without Trusted PKG or Random Oracles

CAI Yong-quan, LIU Yan
(College of Computer Science and Technology, Beijing University of Technology, Beijing 100124)

Abstract: In a group signature scheme, any legal member of this group can sign on behalf of this group, and no one can find out which member is the actual signer except the group manager. The focus of this paper is to design a new ID-based group signature without trusted PKG (group manager) or random oracles, and the security of the scheme, such as forward security. According to the analysis result, legal group members can sign on behalf of the group; an arbiter (OM) can open a legal signature to find out the actual signer, and he can also point out that whether the group manager is legal or not. So this is a scheme without trusted PKG without random oracles. Besides, this paper takes advantage of the information of time section to implement the forward security of this scheme in case of key exposure or revocation of group members.

Key words: identity-based group signature; without random oracle; without trusted PKG; forward security; Bilinear pairing

1 引言

群签名是普通的数字签名的扩展,由 Chaum 和 van Heyst[1]提出,允许群成员代表群进行有效的签名,但不对外泄漏签名者的任何身份信息,广泛应用于电子现金、电子投标、电子拍卖等电子商务应用方面.

基于身份的群签名机制是群签名研究的热点问题之一. 1984 年, Shamir 第一次提出基于身份的加密、签名、认证的设想[2],身份可以是用户的姓名、身份证号码、电子邮件地址等,优势在于每个人的公钥都可以直接通过身份信息计算出来,密钥生成中心再根据公钥计算出相应私钥,用户不再需要公钥证书,提高了密钥管理及证书撤销的效率. 2001 年 Boneh 和 Franklin 利用椭圆曲线双线性对(Weil 对或 Tate 对)的性质[3]提出了一个有效且可证明安全的基于身份的密码方案[4],之后基于身份的群签名受到了广泛的关注[5~8]. Chen Xiaofeng 等人研究了一种基于身份信息的群签名技术[5],仲裁者拒绝接受群管理者伪装成合法群成员进行的签名. CASTELLUCCIA 和 POPESCU[6,7]的思路都是由用户生成一对非对称密钥对(如 RSA/DSA),在进行群签名时先作一次 RSA/DSA 签名以防止群管理员冒充,但相当于进行了两次签名,消耗大且产生的签名长度较长,效率不高. 张培清等给出了一个基于身份的签名向群签名的转换过程[8],并在文献[6,7]的基础上,构造两个无法合谋的管理者来防止管理者伪造用户签名. 但使用了求逆操作,效率较低. 文献[5]和[8]都是在随机预言的模型下,假设 Hash 函数是理想的,但实际中,这种理想的 Hash 函数并不存在. 且有研究表明,存在在随机预言模型中安全,但在标准模型下不安全的协议[9];且他们都没有实现群签名的前向安全性,这是解决密钥泄漏等问题的一个重要性质.

本文将在文献[5]的密钥托管的方法的基础上,研究无随机预言下的基于身份信息的群签名,实现在标准模型下具有前向安全性的群签名.

收稿日期:2008-09-11;修回日期:2008-12-20
基金项目:国家 973 重点基础研究发展规划(No. 2007CB311100)

2 相关背景

(1) 群签名

群签名是为隐藏某个团体或组织的内部结构而创建的数字签名方案,因此不像一般的数字签名.群签名直接与签名者的利益与责任挂勾.群签名关系到整个组织或团体的利益.

群签名应当满足以下安全方面的需求[5,10,11]:

(a) 正确性.合法群成员的任何签名必须都是正确有效的.

(b) 不可伪造性.只有合法的群成员才可以签名.

(c) 匿名性.给定一个群签名,除群管理者之外的任何人确定签名者的身份是计算困难的.

(d) 不可联系性.除群管理者之外没有人能判断两个签名是否是同一个成员签署.

(e) 可追踪性.群管理者总是可以打开一个有效的签名来判定签名者的真实身份.

(f) 开脱性(防陷害性).群管理者或者群成员合伙甚至联合起来,均不能以另一个成员的名义签名,即无陷害.

(g) 抗联合攻击.群成员合伙甚至全部成员联合起来也不能阻止一个有效签名的打开,即使一些群成员联合也不能产生有效的不被跟踪的群签名.

(2) 双线性映射

设 G_1 和 G_2 分别为阶同为素数 p 的加法和乘法循环群,g 为 G_1 生成元,双线性映射 $e: G_1 \times G_1 \rightarrow G_2$ 具有如下性质的映射:

(a) 线性性:对于所有的 $u, v \in G_1$, $a, b \in Z_p$,都有 $e(u^a, v^b) = e(u, v)^{ab}$.

(b) 非退化性:$e(g, g) \neq 1$.

(c) $e(u, v) = e(v, u)$.

根据以上性质可得:

(a) 对任意的 $u \in G_1$, $v_1, v_2 \in G_2$,满足 $e(u, v_1 v_2) = e(u, v_1) \cdot e(u, v_2)$.

(b) 对任意 $u, v \in G_1$,满足 $e(u, \psi(v)) = e(v, \psi(u))$.

(3) Hellman 问题

(a) DLP(Discrete Logrithm Problem)离散对数问题:给定 $P \in G_1$, $Q \in G_1$,找出整数 n,使得 $P = nQ$ 成立.群 G_1 上的 DLP 问题是难以解决的.

(b) DDH(Diffe-Hellman)问题:给定一个四元组$\langle P, xP, yP, zP\rangle \in G_1$, $P \in G_1$, $x, y, z \in Z_p$,寻找 z 满足 $z = xy \bmod q$

(c) CDH(Computational Diffe-Hellman)问题:随机给定一个三元组$\langle P, xP, yP\rangle \in G_1$, $P \in G_1$,其中 x, y 是从 Z_p 中均匀随机选择的,寻找元素 xyP.

3 无随机预言下基于身份信息的前向安全的群签名方案

在一个基于身份的密码系统中,每个用户的公钥用他们唯一的身份信息表示,私钥由可信的密钥发行中心 PKG 统一生成,任意两个用户都可以安全通信而不需要交换公钥证书,不必保存公钥证书列表,也不必使用在线的第三方,只需一个 PKG 为每个第一次接入系统的用户分配一个对应其公钥的私钥即可.如何解决密钥托管问题实现无可信 PKG,则是基于身份的群签名机制首先需要解决的问题.本文借鉴了文献[5]的密钥托管的方法,研究无随机预言下的基于身份信息的群签名,实现在标准模型下具有前向安全性的群签名.

在基于身份信息的群签名中,群管理者即为密钥分发中心 PKG;OM 为群打开者和仲裁者.传统的群签名机制将群签名的打开功能也赋予群管理者,造成群管理者若不可信,导致打开签名的正确性无法保证.出于安全性方面的考虑,引入一个第三方判断机构(仲裁者):第一,利用打开私钥打开一个群签名找到签名的群成员,除了掌握打开私钥的仲裁者有权打开签名,任何人无法打开签名;第二,对一个签名进行仲裁,若同一个签名在同一个时间段内对应两个随机签名私钥,则该签名是由不可信 *PKG* 通过伪装得到的,拒绝该签名.

由上述内容,构造本文的一个签名结构模型如图 1:

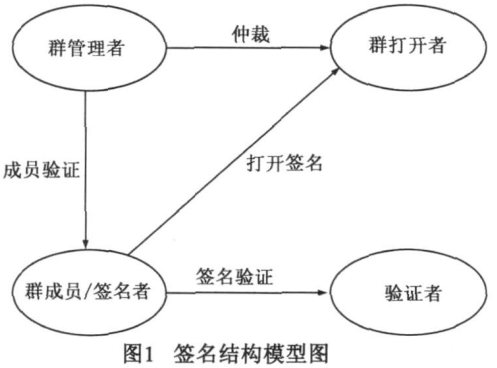

图1 签名结构模型图

安全性方面,前向安全性首先由 Anderson 提出[12].无前向安全性的群签名机制中,群成员的密钥在其生命阶段并不改变,因此无法满足以下两方面要求:首先,若群成员离开群,群成员离开群之前的签名仍然有效且匿名;其次,若群成员密钥泄漏被群管理者删除,该成员之前的签名同样应当有效且匿名.因此,引入时间段信息解决群签名的前向安全性,根据时间段随时更新群成员的密钥信息,并删除过期的密钥.

本文提出的群签名方案分为初始化、密钥提取、新成员加入、密钥更新、签名、验证和打开签名几个步骤.具体过程如下:

3.1 初始化

群管理者 PKG 选择生成元 $P \in G_1$,选择 $s \in Z_q$ 作为系统私钥,计算 $P_{pub} = sP$ 为系统公钥,选择 $H:\{0,1\}^* \rightarrow \{0,1\}^n$, n 是固定的安全系数. 定义函数 $f(S) = u' \prod_{i \in S} u_i$,其中 $\forall S \subseteq \{1, \cdots, n\}$, $u' \in G_1$, $u_i \in G_1$[13]. 定义双线性对 $e = G_1 \times G_1 \rightarrow G_2$. H 为无随机预言下的抗冲突的散列函数. OM 随机选择 x_R 作为打开私钥,并计算 $Y_R = x_R P$ 作为打开公钥. 假设 PKG 和 OM 是完全互不干扰的. PKG 公开 $P, P_{pub}, H, G_1, G_2, e, Y_R, u', u_i$. 因此群的公共信息为 $P, P_{pub}, H, G_1, G_2, e, Y_R, f, u', u_i$.

3.2 密钥提取

用户加入群时,首先确定其总的有效时间段,记作 T(用户的生命周期,用二进制形式表示),并将其按照一定规则分作 k 个不同的单位 $T_j (0 \leq j \leq k)$ (如按照每天为一个单位). 加入时,用户选择 $r_0 \in Z_q$ 作为自己初始的秘密私钥(r_0 表示用户存在的整个生命周期内第一个时间段,即用户刚加入群时的私钥, r_0 随着时段将不断的更新 $r_0 \cdots r_k$ 直至生命周期结束),并计算 $R = r_0 P$ 发送给 PKG 和 OM. PKG 计算 $q_0 = H(ID \| T_0)$ (ID 为用户的身份信息,用二进制表示),令 $q[id] \subseteq \{1, \cdots, n\}$ 为计算得出的 $q_0[id] = 1$ 的下标的集合[13],简记为 q_0(q_0 随着时段的更新而更新), $Q_{ID} = q_j \cdot R$ 作为用户公钥, ID 为用户的身份信息,用二进制表示, T_j 指的是成员在它的生命阶段 T 中对应的一个时间段,相应的密钥是 r_j(在第 j 个时段, r_j 为 T_j 时对应的私钥,因此时段 T_j,相应得到 $Q_{ID} = q_j \cdot r_j P$). PKG 计算 $S_{ID} = sQ_{ID}$ 并通过安全信道发给用户,OM 计算 $R_{ID} = x_R P_{pub}$ 也通过安全信道发给用户,实际的用户私钥为 (r_j, S_{ID}),公钥为 $(r_j P, Q_{ID})$,用户的密钥对随着时段 T 的更新而更新.

3.3 新成员加入

群成员加入不但需要进行上述密钥提取阶段的过程,此外,加入过程也是用户与群管理者之间相互通信的过程. 这里,我们建立两个列表:群成员列表和成员撤销列表,分别保存有效的群成员的信息和已撤销的群成员的信息. 在时段 T_0 用户 i 加入群,用户随机选择 xi,计算 $r_0 P, xiP$ 和 $r_0 xiP$,发送给 OM,并与 $ID(i$ 的身份信息) 和 S_{ID} 一起发送给群管理者[5];管理者验证 $S_{ID} = sq \cdot r_0 P$ 和 $e(r_0 xiP, P) = e(xiP, r_0 P)$ 是否相等来判断成员加入过程是否正确,成员是否属于这个群. 若相等,群管理者发送 $S_i = sf(T_0)\, r_0 xiP$ 给用户,否则终止退出;用户得到它的成员证书 $(S_i, r_0 xiP)$,最终用户的群签名私钥是 $(S_i, r_0 xi)$, S_{ID} 是用户进行普通签名的私钥. 最后将 $r_0 P, xiP, r_0 xiP$ 和 ID 加入到群成员列表中. 群成员列表只有群管理者 PKG 可修改和更新,群仲裁者 OM 可访问.

3.4 密钥更新

为了实现签名的前向安全性,需要注意 $S_{ID} = sq \cdot r_0 P$ 是初始时计算得到的,随着密钥更新, S_{ID} 随着 r_0 的改变而改变($r_0, \cdots, r_k$). 成员在时刻 T_j 的密钥为 r_j,用户刚加入群为用户的初始时刻,初始密钥为 r_0, $r_j = H(r_{j-1} \| T_j)$,更新得到新的密钥后,删除前一个密钥,同时成员的密钥对要同时更新,包括 q, S_i, Q_{ID} 和 S_{ID},并修改成员列表中的相应信息. 这些均由群管理者 PKG 进行操作.

3.5 群成员撤出

可利用撤销树实现成员的撤销. 群成员的撤出不是本文的重点,只给出简单的分析. 每次群成员撤出时,群管理者首先应当将该成员从成员列表中删除. 然而这并不足够,删除的成员可能仍然保管之前掌握的群的信息,或如果删除的成员被攻击者攻击而将身份信息及密钥信息泄漏,仍然有可能代表群得到签名. 因此需要判断成员是否仍然是合法成员. 将已撤出的成员信息加入成员撤销表 RL (Revocation List) 中. 签名验证时遍历撤销表,若该成员信息在已撤销成员内,则证明该成员已被撤除群无法继续签名.

3.6 签名

假设待签名信息为 m,首先计算 $m' = H(m \| T_j)$,其中时段为 $j = 1, \cdots, k$. 令 $\{m'\} \subseteq \{1, \cdots, n\}$ 为计算得出的 $m'[id] = 1$ 的下标的集合,简记为 m'.签名成员 i 随机选择 $a \in Z_q$,得到相应的公私钥如密钥提取阶段所述.

接着签名成员进行下列计算:

$$A = (r_j xi P)^a \qquad B = r_j xi (f(m') r_j xi P)^a$$

$$d = f(m')(A + B) \qquad E = dS_i^a$$

$$F = R_{ID} P_{pub}$$

最后 m 的签名为 $(A, B, E, F, T_j, r_j xiP, m)$.

3.7 验证

验证者接收到签名 $(A, B, E, F, T_j, r_j xiP, m)$ 后,首先计算 $f(m')$, $d = f(m')(A + B)$ 和 $f(T_j)$. 接着进行判断:若 $e(B, P) = e(f(m') r_j xiP, A)$ 且 $e(E, P) = e(d, P)\, e(f(T_j) A, P_{pub})$,则接受签名,否则拒绝该签名.

3.8 打开签名

对于有争议的有效签名,由 OM 执行打开操作找到签名者. OM 利用 $r_j xiP$ 确定签名者的身份 ID. 为了保证除了 OM 外没有人能够打开签名信息,OM 首先验证 $e(F, P) = e(P_{pub}, Y_R)\, e(P_{pub}, P)$ 是否相等,不相等则终止操作. OM 同时可通过判断 $e(r_j xiP, P) = e(xiP, r_j P)$ 和 $e(S_{ID}, P) = e(qr_j P, P_{pub})$ 来防止签名者抵赖.

4 安全性分析

4.1 正确性

利用双线性对的性质,并且通过验证过程可以得到下面的等式证明签名的正确性,

$$e(B,P)=e(r_jxi(f(m\|r_jxiP)^a,P)$$
$$=e((f(m\|r_jxiP)^a,r_jxiP)$$
$$=e(f(m\|r_jxiP,(r_jxiP)^a)$$
$$=e(f(m\|r_jxiP,A)$$
$$e(E,P)=e(dS_i^a,P)=e(d,P)e(S_i^a,P)$$
$$=e(d,P)e(S_i,P^a)$$
$$=e(d,P)e(sf(T_j)r_jxiP,P^a)$$
$$=e(d,P)e(f(T_j)sP,r_jxiP^a)$$
$$=e(d,P)e(f(T_j)P_{pub},A)$$
$$=e(d,P)e(f(T_j)A,P_{pub})$$

4.2 不可伪造性

由于 H 为标准模型下抗冲突的散列函数,且只有群成员才能拥有群签名私钥及群成员证书(s,S_i),所以任何群外的成员都无法伪造群签名. 群成员的签名私钥是随机选择的,群私钥也只有群管理者知道,假设攻击者 A 截取了成员列表获得成员证书(S_i,r_jxiP),要获得群成员的签名密钥和群私钥 s,攻击者 A 只有通过解决数学难题 $e(abP,P)=e(aP,bP)$,其中 $S_i=abP$, $qr_jxiP=aP$, $P_{pub}=bP$, $e(S_i,P)=e(sqr_jxiP,P)=e(qr_jxiP,sP)=e(qr_jxiP,P_{pub})$.

4.3 匿名性

由于打开密钥只有 OM 知道,并且是通过安全信道发送给用户,因此除了 OM 外,没有人能够打开签名,即使群管理者也是一样,因此本方法满足匿名性.

$$e(F,P)=e(R_{ID}P_{pub},P)=e(R_{ID},P)e(P_{pub},P)$$
$$=e(x_RP_{pub},P)e(P_{pub},P)=e(P_{pub},Y_R)e(P_{pub},P)$$

4.4 不可联系性

给定两个签名,虽然可以由签名直接得到 r_jxiP 和 $r_jxi'P$,但私钥 xi 和 xi' 是用户签名时随机选择的,那么就无法知道 xiP 和 $xi'P$ 的值,也就无法知道这两个签名是否是属于同一个 r_jP,即是否属于同一个群成员的,即除群管理者 PKG 和群打开者 OM 外,任何用户都无法确定给定的两个签名是否具有相同的成员 ID,因此签名具有不可联系性.

4.5 可追踪性

显而易见,群签名是可追踪的. 掌握打开密钥的打开者 OM 可以识别具体的签名者,即群签名具有可追踪性.

4.6 开脱性(防陷害性)

要证明方法具有防陷害性,就需要证明在同一时刻不可能有两个不同的签名者对同一相同信息进行签名. 这里假设群管理者伪装成合法的群成员,在时段 j 进行签名,待签名信息 m 经过哈西运算得到 m'. 首先,群管理者随机选择 $r_j'\in Z_q$ 作为秘密私钥,并计算 $S_{ID}'=sQ_{ID}'=sq\cdot R'=sq\cdot r_j'P$. 接着,群管理按照上述签名过程进行签名,得到签名结果为:$A'=(r_j'xiP)^b$

$B'=r_j'xi(f(m\|r_j'xiP)^b$

$d'=f(m\|(A'+B\|$ $E=(b+d\|S_i^b$

最后得到 m 的签名为$(A',B',E',F,T_j,r_j'xiP,m\|)$.

由验证过程可知,该签名可以通过验证,PKG 伪装了一个合法成员的有效签名. 因此要判断该签名的有效性,需要进行仲裁.

仲裁时,首先由群管理者 PKG(在仲裁者 OM 和验证者来看 PKG 现在是合法的群成员) 发送 S_{ID}'给 OM,OM 随机选择 $y\in Z_q$ 并计算 $e(S_{ID}',yP)$,若满足 $e(S_{ID}',yP)=e(sQ_{ID}',yP)=e(Q_{ID}',P_{pub})^y=e(q\cdot r_j'P,P_{pub})^y$,则可以得出,签名的成员 ID 在时段 j 可以利用 $r_j'P(r_j'\in Z_q)$ 进行合法的签名. 接着,被 PKG 伪装的用户将自己当前时段 j 的密钥 r_jP 发送给 OM,OM 随机选择 y',并计算 $e(S_{ID},y'P)=e(sQ_{ID},y'P)=e(Q_{ID},P_{pub})^{y'}=e(q\cdot r_jP,P_{pub})^{y'}$,若等式成立,可知,在时段 j 签名 ID 也可以利用 $r_j\in Z_q$ 进行合法的签名. 而且 PKG 可告诉 OM 它知道成员证书 S_{ID},如 $e(S_{ID},P)=e(sQ_{ID},P)=e(Q_{ID},P_{pub})=e(q\cdot r_jP,P_{pub})$.

可以看出,在同一个时间段 j,同一个成员 ID 对应了两个不同的签名私钥 $r_j'P$ 及 r_jP. 因此,可以推断出其中一个签名是伪造的,而且这必定是群管理者进行的,因为只有群管理者才知道群私钥 s 而计算出 S_{ID}.

由上述的仲裁过程,可以证明群管理者不可信,并且拒绝其得到的签名信息.

4.7 抗联合攻击

联合攻击包括无群管理者参加的多个群成员的联合攻击以及包括群管理者在内的多个成员的联合攻击. 由于群成员的签名密钥有两部分,一是由群管理者分发的密钥,一是签名者随机选择的密钥,群成员的成员证书包括这两种私钥. 因此对于第一种情况,即使有多个成员合谋,也无法猜到另一群成员的私钥,而无法得到他的合法成员证书,因此无法伪装成他进行签名;在有群管理者参与的情况下,由不可伪造性和开脱性可知,即使多个成员与群管理者合谋,签名也将被仲裁者最终检测出为不合法的而拒绝. 因此,签名满足抗联合攻击性.

4.8 前向安全性

只有在某个时段有效的成员可以进行合法签名. 由群成员加入过程和验证过程可知,若某成员在某个时段已经撤出,该成员必然在撤销成员列表中,那么即使它继续代表该群进行签名也无法通过验证;若某成员在某个时段密钥泄漏并被管理员删除,由于该成员在该时段之前时段对应的密钥已经删除,因此之前的

签名依旧有效具有匿名性,且无法被攻击者攻击,仲裁者也可以打开之前的签名找到成员列表中的签名者,但之后该成员已无法代表群进行群签名.因此,具有前向安全性.

综上,群签名是安全的.

5　效率分析

与文献[5]相同,本文介绍的基于身份信息且无可信中心的群签名中,群公钥及群签名的长度均与群成员的个数无关,应用于动态群时,不但提高了效率,而且还可以应用于较大的群;且打开者 OM 可以直接通过 $r_j x_i P$ 找到签名群成员.

对于数字签名来说,签名的效率主要决定于签名和验证的过程,这里的签名过程包括了 3 次指数运算,3 次点乘运算,2 次数乘运算,1 次加法和两次哈西函数运算;验证过程包括 3 次点乘运算,1 次加法运算,3 次函数运算和 5 次双线性计算.本文与在随机预言下实现的基于身份信息的群签名相比,减少了哈西函数的计算量,如文献[5];本文也没有像文献[8]那样使用求逆操作,因此提高了效率.

6　结论

本文提出了一种无随机预言下基于身份的前向安全的群签名方案,由仲裁者代替群管理者打开群签名,分担了群管理者的部分工作,更具有安全性.与文献[5]相比,本文还实现了在无随机预言的模型下的无可信中心的群签名,比文献[5]进一步深入.与以往的签名方案相比,本文具有前向安全性,且提高了效率.

参考文献:

[1] D Chaum, E van Heyst. Group signatures[A]. Proc of EUROCRYPT'91[C]. Berlin: Springer-Verlag, 1991. 547: 257 - 265.

[2] SHAMIR A. Identity-based cryptosystems and signature schemes[A]. Advances in Cryptology 1985[C]. Berlin: Springer-Verlag, 1985. 196: 47 - 53.

[3] K G Paterson. ID-based signatures from pairings on elliptic curves[J]. United Kingdom: IEE Electronics Letters, 2002, 38(18): 1025 - 1026.

[4] D Boneh, M Franklin. Identity based encryption from the weil pairing[A]. Advances in Cryptology-Crypto of 2001[C]. Berlin: Springer-Verlag, 2001. 2139: 213 - 229.

[5] Chen Xiaofeng, Zhang Fangguo, Kwangjo Kim. New ID-based group signature from pairings[J]. China: Journal of Electronics (China), 2006, 11, 23(6): 892 - 900.

[6] Castelluccia C. How to convert any ID-based signature scheme into a group signature scheme[OL]. http://eprint.iacr.org/, 2002/116.

[7] Popescu C. An efficient ID-based group signature scheme[J]. Studia Univ: Babes-Bolyai, Informatica, 2002, Volume XLVII(2): 29 - 36.

[8] 张培清,胡磊. 一种基于身份的群签名方案[J]. 成都:计算机应用研究,2007,24(5):122 - 124.
Zhang Pei-qing, Hu Lei. ID-based group signature scheme[J]. Chengdu: Application Research of Computers, 2007, 24(5): 122 - 124. (in Chinese)

[9] Mihir Bellare, Phillip Rogaway. Minimizing the use of random oracles in authenticated encryption schemes[A]. Information and Communications Security[C]. Berlin: Springer-Verlag, 1997. 1334: 1 - 16.

[10] 李敏,王尚平,马晓静,秦慧. 分级群签名[J]. 计算机应用研究,2006,(9):88 - 91.
Li Min, Wang Shang-ping, Ma Xiao-jing, Qin Hui. Rank group signature[J]. Chengdu: Application Research of Computers, 2006, (9): 88-91. (in Chinese)

[11] 吴克力,孙抗毒,朱保平,刘凤玉. 一种动态群签名方案[J]. 计算机应用与软件,2007,24(9):26 - 29.
Wu Ke-li, Sun Kang-du, Zhu Bao-ping, Liu Feng-yu. A dynamic group signature scheme[J]. Shanghai: Computer Applications and Software, 2007, 24(9): 26 - 29. (in Chinese)

[12] R Anderson. Invited lecture[R]. The 4th ACM Conf on Computer and Communications Security, Zurich, 1997.

[13] Jian Weng, Shengli Liu, Kefei Chen, Changshe Ma. Identity-based key-insulated signature without random oracles[A]. Computational Intelligence and Security[C]. Berlin: Springer-Verlag, 2007, 4456: 470 - 480.

作者简介:

蔡永泉　男,1956 年出生于安徽,博士、教授、博士生导师.主要研究方向为信息安全、计算机网络.
E-mail: cyq@bjut.edu.cn

刘　岩　女,1984 年出生于山西大同,硕士研究生,主要研究方向为信息安全.