标准模型下固定长度的基于身份环签名方案

葛爱军[1)] 马传贵[1)] 张振峰[2)] 陈少真[1)]

[1)](信息工程大学信息工程学院信息研究系 郑州 450002)

[2)](中国科学院信息工程研究所信息安全国家重点实验室 北京 100190)

摘 要 针对现有基于身份环签名方案签名长度过长、安全性不高等问题,利用椭圆曲线双线性对技术,文中提出了一种新的基于身份环签名方案,在标准模型下证明了其能抵抗适应性选择消息攻击,并且具有无条件匿名性.新方案签名长度达到了固定值,并且算法只需要三个双线性对运算.与现有的标准模型下基于身份环签名方案相比,该方案占用通信带宽低,计算效率高,安全性强,因此能更好地满足应用要求.

关键词 基于身份环签名;匿名性;双线性对;标准模型

中图法分类号 TP309 **DOI号**: 10.3724/SP.J.1016.2012.01874

Identity-Based Ring Signature Scheme with Constant Size Signatures in the Standard Model

GE Ai-Jun[1)] MA Chuan-Gui[1)] ZHANG Zhen-Feng[2)] CHEN Shao-Zhen[1)]

[1)](*Department of Information Research, Institute of Information Engineering, Information Engineering University, Zhengzhou* 450002)

[2)](*State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing* 100190)

Abstract Aiming at the efficiency and security weaknesses that exist in the identity-based ring signature schemes, using the method of bilinear pairing, this paper propose a new construction of identity-based ring signature scheme. This scheme is existentially unforgeable against adaptive chosen message attacks in the standard model, and can achieve unconditional anonymity. The new scheme, with constant size signatures, only needs three pairing operations. Compared with other existing schemes, this construction can provide better efficiency in terms of the communication cost and computation cost as well as the security guarantee, thus it can more satisfy the application requirements.

Keywords identity-based ring signature; anonymity; bilinear pairing; standard model

1 引 言

为解决传统的基于公钥基础设施(PKI)密码体制使用公钥证书产生的存储和管理开销过大的问题,最早由Shamir[1]提出了基于身份的公钥密码体制,其基本思想是用户采用自己的身份信息(如电子邮箱地址、身份证号码等)作为公钥,用户的私钥由一个称为私钥生成器(PKG)的可信第三方产生.在基于身份公钥密码体制中,PKG无需保存所签发的证书列表,而用户只需存储PKG的系统参数,而不是其他用户的证书数据库.2001年,Boneh和Frank-

收稿日期:2012-05-09;最终修改稿收到日期:2012-07-16.本课题得到国家自然科学基金(61170278,91118006)、河南省重点科技攻关项目(092101210502)和信息安全国家重点实验室开放课题(01-02-8)资助.**葛爱军**,男,1985年生,博士研究生,主要研究方向为公钥加密和数字签名.E-mail: geaijun@163.com. **马传贵**(通信作者),男,1962年生,博士,教授,博士生导师,中国计算机学会(CCF)会员,研究领域为密码协议以及信息安全.E-mail: chuanguima@sina.com. **张振峰**,男,1972年生,博士,研究员,博士生导师,研究领域为密码学和信息安全. **陈少真**,女,1967年生,博士,教授,博士生导师,研究领域为密码学.

lin[2]首次将椭圆曲线上双线性对引入到公钥密码体制，并构造了第一个实用的基于身份加密体制. 由于双线性对在密码学中具有良好的性质，因此得到了广泛的关注.

Rivest 等人[3]在研究如何匿名泄露秘密的背景下首次提出了环签名这一概念，并且因为其签名按一定规则首尾相接可组成一个环状而得名. 自环签名的概念被提出后，引起了各国学者的广泛关注，一系列高效的环签名方案相继被提出[4-6]. 环签名可以让用户以一种完全匿名的方式对消息进行签名. 任何验证者只能确信这个签名来自环中的某个成员，但却不能确认真实签名者的身份. 与群签名[7]相比，环签名可以实现无条件匿名性，并且具有更强的灵活性：没有群管理员，不需要预先建立群组以及撤销环成员等阶段，签名者只要知道某个用户的公钥，不需要对方同意或者合作就可以将其加入到环中进而对消息签名. 环签名的这些性质，使得其在电子现金、电子选举、Ad hoc 网络等匿名身份认证领域有着广泛的应用.

基于身份环签名[8-11]，作为环签名与基于身份密码体制的结合，已成为近年来的热点研究问题. 由于环签名中签名算法要使用环中所有成员的公钥，导致环签名的长度往往与环成员的个数线性相关，因此这类签名只适合于环成员规模较小的情况. 王玲玲等人[10]利用累加器技术，提出一种签名长度固定的基于身份环签名方案，但是他们的方案要求环成员固定不变，并且只能在随机预言模型下证明安全性. 然而，随机预言机模型把 Hash 函数作为一个完全随机的理想模型，而真正的 Hash 函数与随机预言机的问答模式是有区别的，近年来也有学者指出某些在随机预言机模型下可证安全的方案在 Hash 函数实例化后并不安全[12]. 因此在不借助于随机预言机的标准模型下设计固定长度的基于身份环签名方案更有意义.

利用 Waters 基于身份的签名技术[13]，Au 等人[9]首次给出了一个签名长度固定的基于身份环签名方案，并且在标准模型下证明了其安全性. 但是该方案存在两个问题：(1) 安全性较弱，不能抵抗适应性选择消息攻击；(2) 用户的私钥长度为 $(n+1)(n+2)$ 个群元素，其中 n 为环成员的最大数目，导致用户的存储代价过高. 通过在私钥中嵌入系统公开参数的方法，本文提出了一种新的签名长度固定的基于身份环签名方案，满足无条件匿名性，在标准模型下证明了其对适应性选择消息攻击是存在性不可伪造的，并且私钥长度缩短至 $(n+1)$ 个群元素，从而在提高安全性的同时，有效地减少了存储量.

本文第 2 节介绍环签名相关的背景知识，包括双线性映射、困难问题假设以及基于身份环签名的定义；第 3 节给出环签名的安全模型；第 4 节提出新的标准模型下安全的固定长度的基于身份环签名方案；第 5 节给出方案的安全性分析；最后，第 6 节总结全文.

2　预备知识

2.1　双线性映射

设 G_1，G_2 是阶为素数 p 的乘法群，g 是 G_1 的生成元，若一个映射 $e:G_1\times G_1\to G_2$ 满足以下 3 条性质，我们称这个映射为双线性映射：

(1) 双线性性. 对于任意的 $a,b\in\mathbb{Z}_p^*$，都有 $e(g^a,g^b)=e(g,g)^{ab}$.

(2) 非退化性. $e(g,g)\neq 1$.

(3) 可计算性. 对于任意的 $g,h\in G_1$，存在一个高效的算法来计算 $e(g,h)$ 的值.

2.2　复杂性假设

下面介绍本文环签名方案安全性所基于的复杂性假设：计算性 n-DHE 问题，这是基于 2005 年欧密会提出的困难问题：双线性计算 n-DHE 问题[14]的一个变型. 可以证明，如果计算性 n-DHE 问题解决，很容易解决双线性计算 n-DHE 问题[14]，因此本文环签名方案所基于的计算性 n-DHE 困难问题是比双线性计算 n-DHE[13]还要弱的困难问题假设，也即本文的困难问题假设是合理的.

定义 1.　双线性计算 n-DHE(Computation n-Bilinear Diffie-Hellman Exponentiation)问题[14]. 设 G_1 是阶为素数 p 的乘法群，且存在双线性映射 $e:G_1\times G_1\to G_2$，给定 $2n+1$ 元组 $(g,h,g^{\alpha},g^{\alpha^2},\cdots,g^{\alpha^n},g^{\alpha^{n+2}},\cdots,g^{\alpha^{2n}})\in G_1^{2n+1}$，其中 α 未知，要求计算 $e(g,h)^{\alpha^{n+1}}$ 的值.

定义 2.　计算性 n-DHE(Computation n-Diffie-Hellman Exponentiation)问题. 设 G_1 是阶为素数 p 的乘法群，g 是 G_1 的一个生成元，给定 $2n$ 元组 $(g,g^{\alpha},g^{\alpha^2},\cdots,g^{\alpha^n},g^{\alpha^{n+2}},\cdots,g^{\alpha^{2n}})\in G_1^{2n}$，其中 α 未知，要求计算 $g^{\alpha^{n+1}}$ 的值.

如果敌手不能在时间 t 内以一个不可忽略的概率 ε 计算出 $g^{\alpha^{n+1}}$ 的值，则称在 G_1 内 (t,ε) 计算性 n-DHE 假设成立.

2.3　基于身份环签名方案的一般化模型

根据文献[8]，一个基于身份环签名体制一般是

由如下 4 个多项式时间算法组成：

(1) 系统建立(Setup). 该算法是由 PKG 完成的概率多项式时间算法，输入安全参数 λ，输出主密钥 s 和系统公开参数 $params$.

(2) 密钥提取(Extract). 该算法亦是由 PKG 完成的概率多项式时间算法，输入一个用户的身份 ID，主密钥 s 和系统公开参数 $params$，算法输出对应 ID 的私钥 sk_{ID}，并通过秘密信道安全地传送给该用户.

(3) 签名算法(Sign). 该算法是由用户完成的概率多项式时间算法，输入系统公开参数 $params$、消息 M、构成环的用户身份集合 R 以及真实签名者的私钥 sk_{ID}(要求用户 ID 在环 R 中，即 $ID\in R$)，输出环 R 关于消息 M 的签名 σ.

(4) 验证算法(Verify). 该算法是由验证者完成的确定性多项式时间算法，输入系统公开参数 $params$、消息 M、环 R 以及对消息 M 的签名 σ，输出判断值“接受”或者“拒绝”.

3 基于身份环签名体制的安全模型

基于身份环签名方案必须满足两方面的安全性要求，一个是不可伪造性，即敌手只有知道环中公钥所对应的私钥时才能生成一个有效的环签名；另外一个是无条件匿名性，即便敌手拥有无限的计算能力并获取所有可能签名者的私钥，其仍然无法确定签名究竟是环中哪个成员所签署. 安全模型我们参照了文献[5,8].

3.1 不可伪造性

我们提出的基于身份环签名方案在选择环及适应性选择消息攻击下是存在性不可伪造的(EUF-sR-CMA)，其正式定义用如下一系列游戏来刻画，这些游戏分别由敌手 $\mathcal{A}$ 和挑战者 $\mathcal{C}$ 共同进行：

(1) 初始化(Init). 敌手 $\mathcal{A}$ 首先声明一个他要攻击的环 R^*，此环 R^* 即为在伪造环签名中要使用到的环成员身份列表.

(2) 系统建立(Setup). 接收到敌手 $\mathcal{A}$ 的挑战环 R^* 之后，挑战者 $\mathcal{C}$ 输入安全参数 λ，运行系统建立算法并得到主密钥 s 和系统公开参数 $params$，挑战者 $\mathcal{C}$ 发送公开参数 $params$ 给敌手 $\mathcal{A}$，并秘密保存主密钥 s.

(3) 询问阶段(Query). 敌手 $\mathcal{A}$ 可以进行多项式次数的适应性私钥提取询问和签名询问，挑战者 $\mathcal{C}$ 利用自己掌握的主密钥 s 相应地回答.

私钥提取询问：敌手 $\mathcal{A}$ 任意选择用户的身份 ID，要求 $\mathcal{C}$ 挑战者输出对应 ID 的私钥 sk_{ID}；

签名询问：敌手 $\mathcal{A}$ 任意选择一个消息 M 及包含 n 个身份的集合 $R=\{ID_1,\cdots,ID_n\}$，要求挑战者输出环 R 关于消息 M 的签名 σ.

(4) 伪造阶段(Forgery). 最后，敌手 $\mathcal{A}$ 输出一个对应消息 M^* 及环 R^* 的签名 σ^*，并且满足以下条件：

① 对于任意 $ID\in R^*$，敌手 $\mathcal{A}$ 没有对 ID 进行过私钥提取询问.

② 敌手 $\mathcal{A}$ 对 (M^*,R^*) 没有进行过签名询问.

③ σ^* 是满足环 R^* 对消息 M^* 的有效签名，即 (M^*,R^*,σ^*) 能通过验证算法.

我们定义敌手 $\mathcal{A}$ 的优势 $Adv_{\mathrm{IDR},\mathcal{A}}^{\text{sR-CMA-EUF}}$ 为在上述游戏中它能赢得游戏的概率.

定义 3. 不可伪造性. 如果一个敌手 $\mathcal{A}$ 能够在时间 t 内最多进行了 q_K 次私钥提取询问，q_S 次签名询问后能伪造上述签名的优势 $Adv_{\mathrm{IDR},\mathcal{A}}^{\text{sR-CMA-EUF}}$ 至少是 ε，我们就称该基于身份环签名方案可以被敌手 (t,q_K,q_S,ε) 攻破. 如果基于身份环签名算法对于任意多项式 t,q_K,q_S 以及不可忽略值 ε 都不能被敌手 (t,q_K,q_S,ε) 攻破，则称其对适应性选择消息攻击是存在性不可伪造的.

3.2 无条件匿名性

为了保证签名者无条件匿名性，基于身份环签名要求验证者只能确信环中某签名者签署该消息，但不泄露真实签名者的身份信息，正式定义如下.

定义 4. 签名者无条件匿名性. 对于任意包含 n 个身份的集合 $R=\{ID_1,\cdots,ID_n\}$ 以及对消息 M 的签名 σ，如果任何敌手 $\mathcal{A}$ 识别出实际签名者的优势不大于随机猜测，也即输出实际签名者的概率不会大于 $1/n$，我们就称该基于身份环签名方案达到了无条件匿名性.

4 固定长度的基于身份环签名方案

本节我们提出了一种有效的基于身份环签名方案，并且签名长度达到了常数值，具体构造如下：

系统建立(Setup). 设 G_1,G_2 都是阶为素数 p 的乘法群且 G_1 的生成元为 g，双线性映射 $e:G_1\times G_1\rightarrow G_2$，密钥生成中心 PKG 从 G_1 中随机选择 $n+2$(n 为系统允许的环成员最大数目)个元素 $\boldsymbol{G}=(g_0,g_1,\cdots,g_n,g_{n+1})$，$m+1$ 个元素 $\boldsymbol{U}=(u',u_1,u_2,\cdots,u_m)$，其中 m 为待签名消息的长度. 取随机数 $x\in\mathbb{Z}_p^*$，令 $Z=e(g,g)^x$. 公开参数 $params=(g,Z,\boldsymbol{G},\boldsymbol{U})$，系统主密钥为 $msk=g^x$.

密钥提取(Extract). 给定用户的身份$ID\in\mathbb{Z}_p^*$，PKG 随机选择 $r_{ID}\in\mathbb{Z}_p^*$，计算用户的私钥 $sk_{ID}=(K_{ID},L_{ID},K_{ID,1},\cdots,K_{ID,n})$，其中 $K_{ID}=g^{x}(g_0)^{r_{ID}}$，$L_{ID}=g^{r_{ID}}$，$\{K_{ID,i}=(g_{i+1}(g_1)^{-(ID)^i})^{r_{ID}}\}_{i=1,2,\cdots,n}$.

签名算法(Sign). 令 $R=(ID_1,ID_2,\cdots,ID_k)$为环签名中所包含的 $k(k\leq n)$个身份列表，假定真实签名者身份为 IDs，对消息 $M=(M_1,M_2,\cdots,M_m)\in\{0,1\}^m$进行签名如下：

(1) 签名者 IDs 首先对私钥 sk_{IDs}进行随机化：随机选择 $t'\in\mathbb{Z}_p^*$ 并计算

$K'_{IDs}=K_{IDs}(g_0)^{t'}$，$L'_{IDs}=L_{IDs}g^{t'}$，

$\{K'_{IDs,i}=K_{IDs,i}(g_{i+1}(g_1)^{-(IDs)^i})^{t'}\}_{i=1,2,\cdots,k}$.

注. 私钥随机化算法可以在签名之前完成，也即此时签名者可以预计算.

(2) 设环 R 对应的多项式为 $f_R(X)=\prod_{i=1}^{k}(X-ID_i)=\sum_{i=1}^{k+1}y_iX^{i-1}$，签名者随机选 $r\in\mathbb{Z}_p^*$，计算签名：$\sigma_1=K'_{IDs}\left(\prod_{i=1}^{k}(K'_{IDs,i})^{y_{i+1}}\right)\left(u'\prod_{i=1}^{m}u_i^{M_i}\right)^r$，$\sigma_2=L'_{IDs}$，$\sigma_3=g^r$.

(3) 输出对消息 M 的签名 $\sigma=(\sigma_1,\sigma_2,\sigma_3)$.

验证算法(Verify). 给定某签名者代表环 $R=(ID_1,ID_2,\cdots,ID_k)$对消息 $M=(M_1,M_2,\cdots,M_m)\in\{0,1\}^m$的签名 $\sigma=(\sigma_1,\sigma_2,\sigma_3)$，验证者计算环 R 对应的多项式为 $f_R(X)=\prod_{i=1}^{k}(X-ID_i)=\sum_{i=1}^{k+1}y_iX^{i-1}$，并验证如下等式是否成立：

$$e(g,\sigma_1)=Z\cdot e(g_0\prod_{i=1}^{k+1}g_i^{y_i},\sigma_2)\cdot e(u'\prod_{i=1}^{m}u_i^{M_i},\sigma_3).$$

5　方案的安全性分析

5.1　方案的正确性

正确性验证如下：

因为

$$\begin{aligned}\sigma_1&=K'_{IDs}\left(\prod_{i=1}^{k}(K'_{IDs,i})^{y_{i+1}}\right)\left(u'\prod_{i=1}^{m}u_i^{M_i}\right)^r\\&=g^x(g_0)^{(t'+r_{IDs})}\left(\prod_{i=1}^{k}(g_{i+1}(g_1)^{-(IDs)^i})^{(t'+r_{IDs})\cdot y_{i+1}}\right)\left(u'\prod_{i=1}^{m}u_i^{M_i}\right)^r\\&=g^x(g_0)^{(t'+r_{IDs})}\left(\prod_{i=1}^{k}((g_1)^{-(IDs)^iy_{i+1}})^{t'+r_{IDs}}\right)\cdot\\&\quad\left(\prod_{i=1}^{k}(g_{i+1})^{(t'+r_{IDs})\cdot y_{i+1}}\right)\left(u'\prod_{i=1}^{m}u_i^{M_i}\right)^r\\&=g^x(g_0(g_1)^{-\sum_{i=1}^{k}((IDs)^iy_{i+1})}\left(\prod_{i=1}^{k}(g_{i+1})^{y_{i+1}}\right)^{(t'+r_{IDs})}\left(u'\prod_{i=1}^{m}u_i^{M_i}\right)^r.\end{aligned}$$

又 IDs 是 $f_R(X)=\prod_{i=1}^{k}(X-ID_i)=\sum_{i=1}^{k+1}y_iX^{i-1}=0$ 的一个根，故 $-\sum_{i=1}^{k}((IDs)^iy_{i+1})=y_1$. 则

原式

$$\begin{aligned}&=g^x\left(g_0(g_1)^{y_1}\left(\prod_{i=1}^{k}(g_{i+1})^{y_{i+1}}\right)\right)^{(t'+r_{IDs})}\left(u'\prod_{i=1}^{m}u_i^{M_i}\right)^r\\&=g^x\left(g_0\prod_{i=1}^{k+1}(g_i)^{y_i}\right)^{(t'+r_{IDs})}\left(u'\prod_{i=1}^{m}u_i^{M_i}\right)^r.\end{aligned}$$

故

$$\begin{aligned}e(g,\sigma_1)&=e\left(g,g^x\left(g_0\prod_{i=1}^{k+1}(g_i)^{y_i}\right)^{(t'+r_{IDs})}\left(u'\prod_{i=1}^{m}u_i^{M_i}\right)^r\right)\\&=e(g,g^x)e\left(g_0\prod_{i=1}^{k+1}(g_i)^{y_i},g^{(t'+r_{IDs})}\right)e\left(\left(u'\prod_{i=1}^{m}u_i^{M_i}\right),g^r\right)\\&=Z\cdot e\left(g_0\prod_{i=1}^{k+1}(g_i)^{y_i},\sigma_2\right)\cdot e\left(\left(u'\prod_{i=1}^{m}u_i^{M_i}\right),\sigma_3\right).\end{aligned}$$

5.2　方案的安全性

定理 1.　如果在 G_1 内(t',ε')计算性 n-DHE 假设成立，并且假设攻击者最多 q_K 次私钥提取询问，q_S次签名询问，那么本文提出的基于身份环签名方案在选择环模型下对适应性选择消息攻击是(t,q_K,q_S,ε)存在性不可伪造的，其中 $\varepsilon'\geq\varepsilon/(4kq_S+2)$，$t'=t+O((q_K+q_S)n\rho)+O((q_K+q_S)n\tau)$，$\rho$ 和 τ 分别是 G_1 上乘法和幂指数运算时间.

证明.　设敌手 $\mathcal{A}$ 能以 ε 的优势攻击成功本文方案，给定挑战者 $\mathcal{C}$ 一个计算性 n-DHE 问题实例 $(g,h_1=g^{\alpha},h_2=g^{\alpha^2},\cdots,h_n=g^{\alpha^n},h_{n+2}=g^{\alpha^{n+2}},\cdots,h_{2n}=g^{\alpha^{2n}})$，以下我们将演示 $\mathcal{C}$ 如何利用 $\mathcal{A}$ 来计算出 $h_{n+1}=g^{\alpha^{n+1}}$，进而解决计算性 n-DHE 问题.

攻击者 $\mathcal{A}$ 首先给出要攻击的环成员身份列表 $R^*=(ID_1^*,ID_2^*,\cdots,ID_k^*)$. $\mathcal{C}$ 计算 $R^*=(ID_1^*,ID_2^*,\cdots,ID_k^*)$对应的多项式为 $f_{R^*}(X)=\prod_{i=1}^{k}(X-ID_i^*)=\sum_{i=1}^{k+1}y_i^*X^{i-1}$. 令 $g_0=g^{\beta_0}\cdot\prod_{i=1}^{k+1}h_i^{-y_i^*}$ $g_i=g^{\beta_i}h_i$ $(1\leq i\leq n)$，$\mathcal{C}$ 再定义 $u'=h_n^{a_0}g^{b_0}$，$u_j=h_n^{a_j}g^{b_j}$ $(1\leq j\leq m)$，其中 $\beta_i(0\leq i\leq n)$，$a_j,b_j(0\leq j\leq m)$都是 $\mathcal{C}$ 随机从 $\mathbb{Z}_p^*$ 中选取的. 令 $Z=e(g,g)^{\alpha^{n+1}}=e(h_1,h_n)$，则主密钥 $msk=g^x=g^{\alpha^{n+1}}$（$\mathcal{C}$ 未知），公开参数 $params=(g,Z,\boldsymbol{G}=(g_0,g_1,\cdots,g_n),\boldsymbol{U}=(u',u_1,\cdots,u_m))$.

假设待签名的消息 $M=(M_1,M_2,\cdots,M_m)\in\{0,1\}^m$，为了方便理解，参照 Waters[13] 的思想，我们首先定义两个函数：$F(M)=p-kt+a_0+\sum_{i=1}^{m}a_i^{M_i}$；$J(M)=b_0+\sum_{i=1}^{m}b_i^{M_i}$，$t=4q_S$. 如果 $a_0+\sum_{i=1}^{m}a_i^{M_i}=$

$0 \bmod(t)$，定义 $F(M)=0$，否则定义 $F(M)=1$. $\mathcal{C}$ 与 $\mathcal{A}$ 进行如下交互：

(1) 私钥提取询问. 假设 $\mathcal{A}$ 最多 q_K 次私钥提取询问，$\mathcal{A}$ 任意选择一个用户的身份 ID 满足 $ID \notin R^*$，$\mathcal{A}$ 要求挑战者 $\mathcal{C}$ 输出 ID 对应的私钥. $\mathcal{C}$ 计算私钥如下：

随机选 $t' \in \mathbb{Z}_p^*$，令 $t=t'+\left(\sum_{i=0}^{n-1}(ID^j \alpha^{n-j})/f_{R^*}(ID)\right)$，输出私钥 $sk_{ID}=(K_{ID}, L_{ID}, K_{ID,1}, \cdots, K_{ID,n-1})$，其中 $K_{ID}=g^x (g_0)^t$，$L_{ID}=g^t$，$\{K_{ID,i}=(g_{i+1}(g_1)^{-(ID)^i})^t\}_{i=1,2,\cdots,n-1}$.

注. 因为 ID 不是 $f_{R^*}(X)=\prod_{i=1}^{k}(X-ID_i^*)=\sum_{i=1}^{k+1} y_i^* X^{i-1}=0$ 的根，故 $f_{R^*}(ID)\neq 0$. 可以验证，计算私钥 sk_{ID} 不需利用到 $g^{\alpha^{n+1}}$ 的值，这是因为 K_{ID}，$\{K_{ID,i}=(g_{i+1}(g_1)^{-(ID)^i})^t\}_{i=1,2,\cdots,n-1}$ 相应的 α^{n+1} 的系数全为 0，详细信息如下：在计算 $K_{ID}=g^x (g_0)^t$ 时，$(g_0)^t$ 中含 $g^{\alpha^{n+1}}$ 的项为 $g^{-f_{R^*}(X)^{-1}\sum_{i=1}^{k+1}(y_i^* X^{i-1})\alpha^{n+1}}=g^{-f_{R^*}(X)^{-1}f_{R^*}(X)\alpha^{n+1}}=g^{-\alpha^{n+1}}$ 恰好与 $g^x=g^{\alpha^{n+1}}$ 约去；而在计算 $K_{ID,i}=(g_{i+1}(g_1)^{-(ID)^i})^t$ 时，其含 $g^{\alpha^{n+1}}$ 的项为 $g^{f_{R^*}(ID)^{-1}((ID)^i\alpha^{n+1}-(ID)^i\alpha^{n+1})}$ 恰好为 $g^0=1$. 因此对于挑战者 $\mathcal{C}$ 来说，其只需知道 $(g^\alpha, g^{\alpha^2}, \cdots, g^{\alpha^n}, g^{\alpha^{n+2}}, \cdots, g^{\alpha^{2n}})$ 而无需 $g^{\alpha^{n+1}}$ 即可完美模拟用户的私钥.

(2) 签名询问. $\mathcal{A}$ 可以任意选择一个包含 k' $(k' \leq n)$ 个身份列表 $R'=(ID_1, ID_2, \cdots, ID_{k'})$ 以及消息 $M=(M_1, M_2, \cdots, M_m) \in \{0,1\}^m$，要求挑战者 $\mathcal{C}$ 输出一个有效的环签名：

① 若 R' 不是 R^* 的子集，即存在某个 $ID \in R'$ 但 $ID \notin R^*$，此时可以通过(1)私钥提取询问获得该 ID 对应的私钥，进一步利用私钥来生成一个有效的环签名.

② 若 R' 是 R^* 的子集，即 $R' \subseteq R^*$，此时 $\mathcal{C}$ 不能通过询问私钥的方法获得一个有效的环签名，但是只要 $F(M)\neq 0$，$\mathcal{C}$ 仍然可以通过如下方法输出一个有效的签名 $\sigma=(\sigma_1, \sigma_2, \sigma_3)$：

$\mathcal{C}$ 随机选 $s, t' \in \mathbb{Z}_p$，计算 $R'=(ID_1, ID_2, \cdots, ID_{k'})$ 对应的多项式 $f_{R'}(X)=\prod_{i=1}^{k'}(X-ID_i)=\sum_{i=1}^{k'+1} y_i Z^{i-1}$，并令 $t=t'-(\alpha/F(M))$，可计算签名

$$\sigma_1=g^x\left(g_0\prod_{i=1}^{k'+1} g_i^{y_i}\right)^s\left(u'\prod_{i=1}^{m} u_i^{M_i}\right)^t$$

$$=\left(g_0\prod_{i=1}^{k'+1} g_i^{y_i}\right)^s (h_n^{F(M)} g^{J(M)})^{t'} h_1^{-\frac{J(M)}{F(M)}};$$

$$\sigma_2=g^s;\ \sigma_3=g^t=g^{t'-(\alpha/F(M))}=g^{t'}h_1^{-(1/F(M))}.$$

伪造. 模拟结束后，最终攻击者 $\mathcal{A}$ 输出一个对应环 $R^*=(ID_1^*, ID_2^*, \cdots, ID_k^*)$ 对消息 $M^*=(M_1^*, M_2^*, \cdots, M_m^*)$ 的一个有效签名 $\sigma^*=(\sigma_1^*, \sigma_2^*, \sigma_3^*)$，如果 $a_0+\sum_{i=1}^{m} a_i^{M_i^*}\neq 0 \bmod(t)$(即 $F(M^*)\neq 0$)，则算法 $\mathcal{C}$ 返回失败；否则，按如下方法 $\mathcal{C}$ 可解决该计算性 n-DHE 困难问题：

因为 $\mathcal{A}$ 伪造的签名能通过验证，必然有

$$\sigma^*=(\sigma_1^*, \sigma_2^*, \sigma_3^*)$$

$$=\left(g^x\left(g_0\prod_{i=1}^{k+1} g_i^{y_i^*}\right)^s (h_n^{F(M^*)} g^{J(M^*)})^t, g^s, g^t\right),$$

可计算得

$$g^{\alpha^{n+1}}=g^x=\sigma_1^*/\left(\left(g^{\beta_0}\prod_{i=1}^{k+1} g^{\beta_i y_i^*}\right)^s (g^{J(M^*)t})\right)$$

$$=\sigma_1^*/((\sigma_2^*)^{\beta_0+\sum_{i=1}^{k+1}\beta_i y_i^*}(\sigma_3^*)^{J(M^*)}).$$

概率分析. 上述过程成功，即 $\mathcal{C}$ 解决计算性 n-DHE 问题的成功概率分析如下：

假定攻击者至多进行了 q_S 次签名询问，输入的消息分别是 $M_i (1\leq i\leq q_S)$，记 $\mathcal{C}$ 成功的概率为 $Pr(\mathcal{C})$，则 $Pr(\mathcal{C})\geq \varepsilon \cdot Pr(F(M_1\neq 0)\bigcap F(M_2\neq 0)\bigcap\cdots\bigcap F(M_{q_S}\neq 0)\bigcap F(M^*=0))$.

记 $Pr(E)=Pr(F(M_1\neq 0)\bigcap F(M_2\neq 0)\bigcap\cdots\bigcap F(M_{q_S}\neq 0)\bigcap F(M^*=0))$，又因为 $Pr(\bar{E})\leq Pr(F(M^*\neq 0))+\sum_{i=1}^{q_S} Pr(F(M^*=0)\bigcap F(M_i=0))$，可计算得 $Pr(E)\geq 1/(4kq_S+2)$.

因此如果攻击者 $\mathcal{A}$ 能够以不可忽略的优势 ε 攻击成功本文提出的基于身份环签名方案，那么就可以构造一个算法 $\mathcal{C}$，并以 $\varepsilon'=\varepsilon/((4kq_S+2))$ 的优势解决计算性 n-DHE 问题. 证毕.

定理 2. 本文提出的基于身份环签名方案满足签名者无条件匿名性.

证明. 本文方案输出的环签名 $\sigma=(\sigma_1, \sigma_2, \sigma_3)$ 中，显然 $\sigma_3=g^r$ 是随机生成的，没有提供实际签名者的任何信息. 另外，$\sigma_2=g^{r_{ID}}g^{t'}$，其中 r_{ID} 是由 PKG (与实际签名者独立的)随机生成的，t' 是由实际签名者随机选择的，因此 σ_2 的分布也是随机的. 最后我们考虑 $\sigma_1=g^x\left(g_0\prod_{i=1}^{k+1} g_i^{y_i}\right)^s\left(u'\prod_{i=1}^{m} u_i^{M_i}\right)^r$，其中指数部分 s 和 r 都是随机的，g^x 是主密钥，所有这些都没有提供任何有关实际签名者的信息. 所以对于敌手

来说，给定环签名 $\sigma=(\sigma_1,\sigma_2,\sigma_3)$ 仍然等同于暴力猜测，因此本文提出的基于身份环签名方案满足签名者无条件匿名性. 证毕.

5.3 性能比较

在本节我们主要通过计算开销和通信开销两方面来综合分析本方案的性能，并将我们的方案与已有的标准模型下的基于身份环签名方案进行了性能对比. 其中，计算开销主要由签名运算及验证运算两部分组成，通信开销为签名长度. 此外，我们还对私钥长度进行了比较，具体如表 1 所示.

表 1　与现有的标准模型下的基于身份环签名方案的性能比较

方案	签名长度	签名算法复杂度	验证算法复杂度	私钥长度
文献[11]方案	$(k+1)G_1$	$(2k+2)E$	$(k+1)P+1E$	$2G_1$
文献[12]方案	$(k+1)G_1$	$(k+3)E$	$(k+1)P+1E$	$2G_1$
文献[9]方案	$2G_1$	$(2k+3)E$	$2P+(k+1)E$	$(n+1)(n+2)G_1$
本文方案	$3G_1$	$(k+2)E$	$3P+(k+1)E$	$(n+1)G_1$

不失一般性，在性能比较中，我们仅考虑最耗时的双线性对运算(用 P 表示一个双线性对运算时间)和次耗时的幂指数运算(用 E 表示一个幂指数运算所花费的时间). 在表 1 中，设 $k(1\leq k\leq n)$ 为环签名中环的成员个数，n 表示系统所支持的环成员的最大个数. 通过表 1 可以看出，考虑到预计算，本文方案在签名算法只需 $(k+2)$ 个指数运算，具有最高的计算效率. 此外，文献[11-12]中的方案签名长度以及验证算法所需双线性对运算的个数都与环成员个数 k 成线性关系，而本文方案签名长度达到了固定值，并且只需要 3 个双线性对运算，通信量和计算效率都有了很大改进. 与文献[9]方案相比，本文方案签名虽然增加了一个群元素，但是私钥长度由 $(n+1)(n+2)$ 缩短至 $(n+1)$ 个群元素，从而有效地减少了存储量. 此外，文献[9]方案不能抵抗适应性选择消息攻击，而本文方案可以证明在适应性选择消息攻击性仍然是存在性不可伪造的，安全性也有明显提高.

6 总　结

在基于身份环签名体制中，验证者只能确信环中某成员签署了消息，但不能确定真实签名者的身份信息，这使得基于身份环签名在匿名认证及隐私保护中有着广泛的应用. 本文提出的基于身份环签名方案，在标准模型下基于计算性 n-DHE 困难假设证明了其对适应性选择消息攻击是存在性不可伪造的. 新方案签名长度达到了固定值，并且方案只需三个双线性对运算，具有极高的运算效率. 与现有的标准模型下基于身份环签名方案相比，本文方案无论在通信量还是计算量和安全性上都有了较大改善，具有一定优势.

通过在私钥中嵌入系统公开参数的方法，本文签名长度达到了固定值，但是本文方案私钥长度较大，即牺牲用户存储代价来降低通信带宽，提高运算效率. 在网络环境中，系统的通信带宽往往会成为瓶颈，这是因为计算机的处理速度、存储容量服从摩尔定律，而要提高系统的通信带宽往往需要很高的代价. 如何在 n-DHE 困难假设下，尽量缩短私钥的长度，是我们下一步要继续研究的问题.

参　考　文　献

[1] Shamir A. Identity-based cryptosystems and signature schemes//Proceedings of the CRYPTO 1984. Santa Barbara, California, USA. LNCS 196. Berlin: Springer-Verlag, 1984: 47-53

[2] Boneh D, Franklin M. Identity-based encryption from the weil pairing//Proceedings of the CRYPTO 2001. Santa Barbara, California, USA. LNCS 2139. Berlin: Springer-Verlag, 2001: 213-229

[3] Rivest R, Shamir A, Tauman Y. How to leak a secret//Proceedings of the ASIACRYPT 2001. Gold Coast, Australia. LNCS 2248. Berlin: Springer-Verlag, 2001: 552-562

[4] Shacham H, Waters B. Efficient ring signatures without random oracles//Proceedings of the PKC 2007. Beijing, China. LNCS 4450. Berlin: Springer-Verlag, 2007: 166-180

[5] Bender A, Katz J, Morselli R. Ring signature: Stronger definitions and constructions without random oracles. Journal of Cryptology, 2009, 22(1): 114-138

[6] Melchor A, Cayrel C, Gaborit P, Laguillaumie F. A new efficient threshold ring signature scheme based on coding theory. IEEE Transactions on Information Theory, 2011, 57(7): 4833-4842

[7] Chaum D, Heyst E V. Group signatures//Proceedings of the EUROCRYPT 1991. Brighton, UK. LNCS 547. Berlin: Springer-Verlag, 1991: 257-265

[8] Chow S, Yiu S, Hui L. Efficient identity based ring signature//Proceedings of the ACNS 2005. New York, NY, USA. LNCS 3531. Berlin: Springer-Verlag, 2005: 499-512

[9] Au M H, Josph K L, Yuen T H et al. ID-based ring signature scheme secure in the standard model//Proceedings of the IWSEC 2006. Kyoto, Japan. LNCS 4266. Berlin: Springer-Verlag, 2006: 1-16

[10] Wang Ling-Ling, Zhang Guo-Yin, Ma Chun-Guang. An identity-based ring signature scheme with constant-size signature. Journal of Electronics & Information Technology, 2007, 29(11): 2645-2648(in Chinese)
(王玲玲，张国印，马春光. 一种签名长度固定的基于身份环签名方案. 电子与信息学报，2007，29(11)：2645-2648)

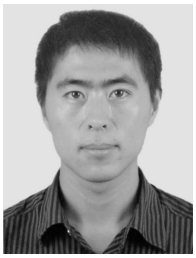
[11] Liu Zhen-Hua, Hu Yu-Pu, Mu Ning-Bo, Ma Hua. New identity-based ring signature in the standard model. Journal of Electronics & Information Technology, 2009, 31(7): 1727-1731(in Chinese)
(刘振华，胡予濮，牟宁波，马华. 新的标准模型下基于身份环签名方案. 电子与信息学报，2009，31(7)：1727-1731)

[12] Canetti R, Goldreich O, Halevi S. The random oracle methodology, revisited. Journal of the ACM, 2004, 51(4): 557-594

[13] Waters B. Efficient identity-based encryption without random oracles//Proceedings of the EUROCRYPT 2005. Aarhus, Denmark. LNCS 3494. Berlin: Springer-Verlag, 2005: 114-127

[14] Boneh D, Boyen X, Goh E. Hierarchical identity based encryption with constant size ciphertext//Proceedings of the EUROCRYPT 2005. Aarhus, Denmark. LNCS 3494. Berlin: Springer-Verlag, 2005: 166-180

[15] Zhang Ming-Wu, Yang Bo, Yao Jin-Tao, Zhang Wen-Zheng. Cryptanalysis and design of signature schemes with identity ambiguity in the standard model. Journal of Communications, 2011, 32(5): 40-46(in Chinese)
(张明武，杨波，姚金涛，张文政. 标准模型下身份匿名签名方案分析与设计. 通信学报，2011，32(5)：40-46)



GE Ai-Jun, born in 1985, Ph. D. candidate. His current research interests include public key encryption and digital signatures.

MA Chuan-Gui, born in 1962, Ph. D., professor, Ph. D. supervisor. His research interests include cryptology protocols and wireless communications.

ZHANG Zhen-Feng, born in 1972, Ph. D., professor, Ph. D. supervisor. His research interests focus on cryptology and information security.

CHEN Shao-Zhen, born in 1967, Ph. D., professor, Ph. D. supervisor. Her research interests include cryptology protocols and information security.

Background

A ring signature scheme allows a signer to sign on behalf of a group of users, that so called ring, on his own choice, and group members can be totally unaware of being conscripted in the group. Any verifier can be convinced that the signature has been generated by one of the ring members, but the actual signer cannot be discovered. Ring signatures provide signer anonymity in a very stronger sense. In contrast to group signatures, the anonymity of the signer cannot be revoked. At the same time, ring signature schemes are very flexible as no central management is needed. Ring signature schemes could be used for whistle blowing, anonymous member ship authentication for ad-hoc groups and many other applications which do not want complicated group formation stage but require signer anonymity.

Identity-based (ID-based) ring signatures, combining the property of ring signature and ID-based signature, are first formally introduced by Zhang Fang-Guo and Kim King in 2002, and several constructions of ID-based ring signatures have been proposed. Recent advances in this area focus on the design of scheme where the signatures have constant length. Wang Ling-ling et al. proposed the first ID-based ring signature scheme using the technology of accumulator. However, their construction is only secure in the random oracle model. Bellare et al. proved that some cryptosystems previously proved secure in the random oracle model are actual provably insecure when the random oracle is instantiated by any real world Hashing functions. Thus, it is natural to design a practical scheme provably secure without requiring random oracle, that is, secure in the standard model.

Independent of Wang Ling-Ling et al.'s work, Au Man Ho et al. also presented a constant size ID-based ring signature scheme which is secure in the standard model. The main drawback in their construction is that this scheme is only secure in a much weaker security model: the selective identity, selective chosen message attack model. In addition, the private key size in their scheme is also very large.

This paper proposed a constant size ID-based ring signature, which is existentially unforgeable against adaptive chosen message attacks, and can achieve unconditional anonymity. Compared with other existing schemes, this construction can provide better efficiency in terms of the communicational cost and computational cost, thus it can more satisfy the application requirements.

This work is supported by National Natural Science Foundation of China (Nos. 61170278, 91118006), Key Scientific and Technological Project of Henan Province (No. 092101210502) and the Open Foundation of the State Key Laboratory of Information Security (No. 01-02-8).