标准模型下基于身份的环签名方案

赵艳琦[1,2],来齐齐[1],禹 勇[1],杨 波[1,2],赵 一[1]
(1.陕西师范大学计算机科学学院,陕西西安 710062;
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 100093)

摘 要: 本文利用Waters提出的对偶系统加密技术,结合合数阶群上双线性运算的正交性,提出了一个基于身份的环签名方案.该方案在标准模型下是完全安全的,其安全性依赖于两个简单的静态假设.该方案借助分级身份加密(Hierarchical Identity-Based Encryption,HIBE)的思想,使得环签名满足无条件匿名性且具有较高的计算效率.

关键词: 对偶系统;基于身份的环签名;标准模型;分级身份加密;匿名性
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2018)04-1019-06
电子学报URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2018.04.033

ID-Based Ring Signature in the Standard Model

ZHAO Yan-qi[1,2],LAI Qi-qi[1],YU Yong[1],YANG Bo[1,2],ZHAO Yi[1]
(1. *School of Computer Science, Shaanxi Normal University, Xi'an, Shaanxi* 710062, *China*;
2. *State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing* 100093, *China*)

Abstract: In this paper, we propose an identity-based ring signature scheme based on Waters dual system encryption technology and the orthogonality property of composite order bilinear group operation. The scheme, relying on two simple static assumptions, is fully secure in the standard model. Due to the merit of Hierarchical identity-based encryption (HIBE), the proposed ring signature scheme achieves unconditional anonymity and has much higher computational efficiency.

Key words: dual system; identity-based ring signature; standard model; HIBE; anonymity

1 引言

环签名是由Rivest等人[1]首次提出,目的在于保证签名者能够以一种完全匿名的方式进行签名.签名者可以匿名选择签名组,而组成员完全不知道被包括在该组中.任何验证者只能确信这个签名来自群组中的某个成员,但不能确认真实签名者的身份.与群签名[2~5]相比,环签名没有群体建立的过程,也无特殊的管理者.不需要预先加入和撤出单个群体,群体的形成是根据需要在签名前由签名者自己指定.根据环签名的完全匿名性,在特殊环境中有不同应用.例如:电子投票[6],匿名电子举报[7,8],Ad Hoc网络认证[9]等.

基于身份的密码体制由Shamir首次提出[10],其中直接将用户的身份(如电话号码、身份证号等)作为公钥,不需要维护所签发的证书列表,因此得到广泛的实际应用.基于身份的环签名结合了环签名和身份签名的性质,由Zhang和Kim首次给出了构造[11].2006年Au等人在标准模型下提出了基于身份可证安全的环签名方案[12].近几年,标准模型下基于身份的环签名成为新的研究热点,提出了很多方案[13~16].2009年Waters[17]为解决分离式策略在HIBE安全性证明中的不足,首次提出对偶系统加密技术.在该技术中密文和密钥可分为两种计算不可区分的形式:正常的和半功能的.正常的密文和密钥在实际方案中使用,而半功能的密文和密钥只用在安全性证明中.并运用对偶系统加密技术构造了更紧的完全安全的HIBE方案.该方案的安全性是基于DBDH假设和判定性线性假设,但密文长度随着层数的增加呈线性递增.2010年Lewko和Waters[18]利用对偶系统加密技术构造了短密文的完全安全的HIBE方案.该方案的安全性是基于合数阶群和三个静态假设为对偶系统加密的实现提供了新方法.2011

收稿日期:2016-07-15;修回日期:2017-04-30;责任编辑:孙瑶
基金项目:国家自然科学基金(No.61572303,No.61772326);中国科学院信息工程研究所信息安全国家重点实验室开放课题(No.2017-MS-03);中央高校基本科研业务费项目(No.GK201603084,No.GK201702004);国家重点研发计划"网络空间安全"专项(No.2017YFB0802003,No.2017YFB0802004);"十三五"国家密码发展基金(No.MMJJ20170216)

年 Lewko 和 Waters[19] 提出无界的 HIBE 方案,该方案可以构造任意层数的 HIBE 而不需要在初始化阶段对层数进行限制. 2013 年 Au 等人利用 Lewko 和 Waters[19] 无界 HIBE 方案,构造了基于 HIBE 标准模型下完全安全身份环签名方案[20],但环签名长度随着环成员增加成线性增长,且计算效率较低.

本文受 Lewko 和 Waters 利用对偶系统可以构造完全安全 HIBE 的启发,结合 Au 等人所提基于 HIBE 身份环签名[20]结构,构造了一个新的基于 HIBE 的身份环签名方案. 该方案建立在标准模型下,通过使用对偶系统密码技术和合数阶双线性群系统的双线性运算,利用合数阶双线性运算的子群正交性删除了随机标签的介入,使得密钥和签名只包含 3 个子群元素. 该方案的安全性规约在简单的静态假设下,其安全性证明显示方案是存在性不可伪造的,且具有无条件匿名性. 与 Au 等人提出的方案相比,本文的计算效率更高.

2 预备知识

2.1 符号概念

本文中,$\mathcal{G}$ 表示一个算法,$\psi \leftarrow_R \mathcal{G}$ 表示 $\mathcal{G}$ 返回随机值 ψ. p_1,p_2,p_3 表示三个不同的素数,$N=p_1p_2p_3$,G 和 G_T 为 N 阶循环群,单位元记为 1,$g \leftarrow_R G$ 表示随机选取群 G 中元素 g. $\{0,1\}^*$ 表示任意长的 0,1 串. $\mathbb{Z}_N$ 表示模 N 的整数环,$x \leftarrow_R \mathbb{Z}_N$ 表示从 $\mathbb{Z}_N$ 中任取一个元素 x. 用户身份集合 $L=\{ID_1,\cdots,ID_n\}$. $M \in \{0,1\}^*$ 表示 M 为任意长的 0,1 串. $\{x_1,y_1,x_2,y_2,\cdots,x_n,y_n\}$ 表示 $2n$ 个不同元素,简记为 $\{x_i,y_i\}_{i=1}^n$.

2.2 合数阶双线性群

合数阶双线性群被首次使用在文献[21]中. 一个群生成算法 $\mathcal{G}$,输入安全参数 λ,输出双线性群 G. 构建群系统 $\psi=(N=p_1p_2p_3,G,G_T,e)$,其中 $e:G\times G\rightarrow G_T$ 是双线性映射,满足以下性质:

① 双线性性:$\forall u,v \in G, a,b \leftarrow_R \mathbb{Z}_N, e(u^a,v^b)=e(u,v)^{ab}$;

② 非退化性:$\exists\ g \in G$,使得 $e(g,g)$ 在 G_T 中阶为 N;令 G_{p_1},G_{p_2},G_{p_3} 分别表示 G 中阶为 p_1,p_2,p_3 的子群. 同时 $G_{p_ip_j}$ 表示 G 中阶为 p_ip_j 的子群. 当 $h_i \leftarrow_R G_{p_i}, h_j \leftarrow_R G_{p_j}$ 且 $i \neq j$ 时,$e(h_i,h_j)$ 是 G_T 中单位元,例如 $h_1 \leftarrow_R G_{p_1}, h_2 \leftarrow_R G_{p_2}$,满足 $e(h_1,h_2)=1$,我们称 G_{p_1},G_{p_2},G_{p_3} 的这一特性为正交性.

2.3 安全性假设

以下给出的安全性假设均为静态假设,这些假设在文献[18]中已经证明.

假设 1 给定群系统生成算法 $\mathcal{G}$,构建群系统:$\psi=(N=p_1p_2p_3,G,G_T,e) \leftarrow_R \mathcal{G}$,选取参数:$g,X_1 \leftarrow_R G_{p_1}, X_2,Y_2 \leftarrow_R G_{p_2}, X_3,Y_3 \leftarrow_R G_{p_3}$,已知 $D=(\psi,g,X_1X_2,X_3,Y_2Y_3)$,$T_1 \leftarrow_R G$ 和 $T_2 \leftarrow_R G_{p_1p_3}$ 是不可区分的.

其中 T_1 可以被唯一表示成 G_{p_1},G_{p_2} 与 G_{p_3} 中元素的乘积,称这些元素分别是 T_1 中的 G_{p_1} 部分,T_1 中的 G_{p_2} 部分和 T_1 中的 G_{p_3} 部分. 类似地,T_2 可以表示成 G_{p_1} 中和 G_{p_3} 中元素的乘积.

假设 2 给定群系统生成算法 $\mathcal{G}$,构建群系统:$\psi=(N=p_1p_2p_3,G,G_T,e) \leftarrow_R \mathcal{G}$,选取如下参数 $\alpha,s \leftarrow_R \mathbb{Z}_N, g \leftarrow_R G_{p_1}, X_2,Y_2,Z_2 \leftarrow_R G_{p_2}, X_3 \leftarrow_R G_{p_3}$. 已知 $D=(\psi,g,g^\alpha X_2,X_3,g^sY_2,Z_2)$,计算出 $T=e(g,g)^{\alpha s}$ 是困难的.

2.4 基于身份的环签名安全模型

一个安全的环签名方案需要同时满足不可伪造性和匿名性,详细安全模型见文献[14].

3 基于身份的环签名方案

3.1 身份环签名构造

环签名是在 LW10-HIBE 基于身份加密系统基础上构造的.

Setup:选择 N 阶双线性群 $G(N=p_1p_2p_3,p_1,p_2,p_3$ 为不同的素数),用哈希函数将任意长身份映射到 $\mathbb{Z}_N$,因此下文假定任一身份 $ID \in \mathbb{Z}_N$,$H_1:\{0,1\}^* \times \{0,1\}^* \rightarrow \mathbb{Z}_N$ 为抗碰撞的 hash 函数,选择 $\alpha \leftarrow_R \mathbb{Z}_N, g,u_1,u_2,h \in G_{p_1}, X_3 \leftarrow_R G_{p_3}$,$\alpha$ 为主密钥. 公开参数

$$\text{param}=\{N,g,u_1,u_2,h,X_3,H_1,e(g,g)^\alpha\}$$

Extract:生成身份 ID 对应的私钥,随机选取 $r \leftarrow_R \mathbb{Z}_N, R_3,R_3',\tilde{R}_3 \leftarrow_R G_{p_3}$,计算

$$d_{ID}=(g^\alpha(u_1^{ID}h)^rR_3,g^rR_3',u_2^r\tilde{R}_3)=(d_0,d_1,d_2) \quad (1)$$

Sign:$L=\{ID_1,ID_2,\cdots,ID_n\}$ 作为身份环签名的身份集合,我们假设实际签名者为 $ID_\pi (ID_\pi \in L)$,签名消息 $M \in \{0,1\}^*$,计算 $m=H_1(M,L)$,用 d_{ID_π} 执行以下步骤

① 签名者随机选取 $r_i,\lambda_i \leftarrow_R \mathbb{Z}_N, R_{3,i},R_{3,i}' \leftarrow_R G_{p_3}(i=1,\cdots,n)$,$\lambda_1+\lambda_2+\cdots+\lambda_n=0$

② $i=1,\cdots,n$

$$i \neq \pi\ A_i=g^{\lambda_i}(u_1^{ID_i}u_2^mh)^{r_i}R_{3,i} \quad (2)$$

$$B_i=g^{r_i}R_{3,i}' \quad (3)$$

$$\begin{aligned} i=\pi\ A_\pi &= d_0g^{\lambda_\pi}(u_1^{ID_\pi}u_2^mh)^{r_\pi}d_2^mR_{3,\pi} \\ &= g^{\alpha+\lambda_\pi}(u_1^{ID_\pi}u_2^mh)^{r+r_\pi}R_3\tilde{R}_3^mR_{3,\pi} \end{aligned} \quad (4)$$

$$B_\pi=d_1g^{r_\pi}R_{3,\pi}'=g^{r+r_\pi}R_3'R_{3,\pi}' \quad (5)$$

③ 输出环签名 $\sigma=\{A_i,B_i\}_{i=1}^n$.

Verify:给定身份集合 $L=\{ID_1,ID_2,\cdots,ID_n\}$ 关于消息 $M \in \{0,1\}^*$ 的环签名 $\sigma=\{A_i,B_i\}_{i=1}^n$,验证者计算 $m=H_1(M,L)$,随机生成 $s \leftarrow_R \mathbb{Z}_N$ 验证等式:

$$\prod_{i=1}^n \frac{e(g^s,A_i)}{e((u_1^{ID_i}u_2^mh)^s,B_i)} \stackrel{?}{=} e(g,g)^{\alpha s} \quad (6)$$

如果成立输出 Valid,否则输出 Invalid.

正确性:从下面的推导中很容易得出方案是正确的.

$$\prod_{i=1}^{n}\frac{e(g^s,A_i)}{e((u_1^{ID_i}u_2^m h)^s,B_i)}$$

$$=\frac{e\left(g^s,\prod_{i=1}^{n}A_i\right)}{\prod_{i=1}^{n}e((u_1^{ID_i}u_2^m h)^s,B_i)}$$

$$=e(g^s,g^\alpha)\left(\frac{e(g^s,(u_1^{ID_\pi}u_2^m h)^r)}{e((u_1^{ID_\pi}u_2^m h)^s,g^r)}\right)\left(\frac{e\left(g^s,\prod_{i=1}^{n}(u_1^{ID_i}u_2^m h)^{r_i}\right)}{\prod_{i=1}^{n}e((u_1^{ID_i}u_2^m h)^s,g^{r_i})}\right)$$

$$=e(g,g)^{\alpha s}\prod_{i=1}^{n}\left(\frac{e(g^s,(u_1^{ID_i}u_2^m h)^{r_i})}{e((u_1^{ID_i}u_2^m h)^s,g^{r_i})}\right)$$

$$=e(g,g)^{\alpha s} \tag{7}$$

3.2　安全性证明

定理 1　若假设 1,2 成立,我们构造的方案满足定义 1(方案是不可伪造的).

证明　签名类型分为两种:正常的和半功能的. 通过签名算法生成的合法签名 $\sigma=\{A_i,B_i\}_{i=1}^n$,称为正常签名. 若签名 $\sigma=\{A_i,B_i\}_{i=1}^n$ 中 $A_i,B_i(i=1,\cdots,n)$ 是由 G_{p_1},G_{p_2},G_{p_3} 中元素构成,则称为半功能签名.

密钥类型也分为两种:正常的和半功能的. 通过密钥算法生成的合法密钥 $d_{ID}=(d_0,d_1,d_2)$,称为正常密钥. 若(d_0,d_1,d_2)是由 G_{p_1},G_{p_2},G_{p_3} 中元素构成,则称为半功能密钥.

通过一系列不可区分的游戏来完成安全性证明. 第一个游戏是 $\mathrm{Game}_{\mathrm{real}}$不可伪造性游戏,返回给敌手 $\mathcal{A}$ 的密钥和签名都是正常的. 其次是 $\mathrm{Game}_{\mathrm{restricted}}$游戏,它与 $\mathrm{Game}_{\mathrm{real}}$的区别在于 $\mathcal{A}$ 询问的身份与挑战身份不能是模 p_2 相等的,比 $\mathrm{Game}_{\mathrm{real}}$中 $\mathcal{A}$ 询问的身份与挑战身份不能是模 N 相等的限制性更强. 同时 $\mathcal{A}$ 生成的哈希值,在 mod p_2 时也是可区分的(即 $\mathcal{A}$ 不能生成两个环身份集合和消息,$(L,M)\neq(L',M')$,但 $H_1(L,M)=H_1(L',M')\bmod p_2$),在后面的游戏中,将保留这个更加严格的限制. 其次是 Game_k 游戏,前 k 次询问回答是半功能的. 例如:第 j 次是密钥询问,$j<k$,返回给 $\mathcal{A}$ 的密钥为半功能的. 如果第 j 次询问为签名询问,$j<k$,返回给 $\mathcal{A}$ 的签名也为半功能的. 否则,返回密钥和签名都是正常的. 最后是游戏 $\mathrm{Game}_{q_E+q_S}$,返回给 $\mathcal{A}$ 的密钥和签名都为半功能的.

引理 1　如果存在一个敌手 $\mathcal{A}$ 使得 $\mathrm{Game}_{\mathrm{real}}\mathrm{Adv}_{\mathcal{A}}-\mathrm{Game}_{\mathrm{restricted}}\mathrm{Adv}_{\mathcal{A}}=\varepsilon$,模拟者 $\mathcal{S}$ 以 ε 的优势攻破假设 1.

证明　给定 g,X_1X_2,X_3,Y_2Y_3,$\mathcal{S}$ 和 $\mathcal{A}$ 模拟游戏 $\mathrm{Game}_{\mathrm{real}}$ 或 $\mathrm{Game}_{\mathrm{restricted}}$. 如果 $\mathcal{A}$ 能以 ε 的优势区分 $\mathrm{Game}_{\mathrm{real}}$和 $\mathrm{Game}_{\mathrm{restricted}}$,那么 $\mathcal{A}$ 就能找到两个身份 ID 和 ID^*,使得 $ID\neq ID^*\bmod N$,并且 p_2 整除 $ID-ID^*$,$\mathcal{S}$ 通过这些身份计算 $p=gcd(ID-ID^*,N)$得到 N 的一个非平凡因子. 设 $q=\frac{N}{p}$,考虑以下三种情况:

① p,q 中有一个为 p_1,另一个为 p_2p_3,通过测试 $(Y_2Y_3)^p$ 和$(Y_2Y_3)^q$ 中有一个为单位元,不失一般性的令 $p=p_1,q=p_2p_3$,$\mathcal{S}$ 通过检测 $e(T^p,X_1X_2)$是否为单位元,判断 T 中是否含有 G_{p_2}的成分,若是则 T 中不含有,否则含有.

②p,q 中有一个为 p_2,另一个为 p_1p_3,已经排除第一种可能,通过测试$(X_1X_2)^p$ 和$(X_1X_2)^q$ 中有一个为单位元,不失一般性的令 $p=p_1,q=p_1p_3$,$\mathcal{S}$ 通过检测 T^q 是否为单位元,判断 T 中是否含有 G_{p_2}的成分,若是则 T 中不含有,否则含有.

③ p,q 中有一个为 p_3,另一个为 p_1p_2,当 1,2 都不发生时情况 3 发生. 通过测试$(X_3)^p$,$(X_3)^q$ 为单位元,不失一般性的令 $p=p_3$,$\mathcal{S}$ 通过检测 $e(T^p,Y_2Y_3)$是否为单位元判断 T 中是否含有 G_{p_2}的成分,若是则 T 中不含有,否则含有.

引理 2　如果存在一个敌手 $\mathcal{A}$ 使得 $\mathrm{Game}_{k-1}\mathrm{Adv}_{\mathcal{A}}-\mathrm{Game}_k\mathrm{Adv}_{\mathcal{A}}=\varepsilon$,模拟者 $\mathcal{S}$ 以 ε 的优势攻破假设 1.

证明分为两部分,Part 1 中 $\mathcal{A}$ 进行 q_E 次密钥询问. Part 2 中 $\mathcal{A}$ 进行 q_S 次签名询问. 在进行签名询问时,因为敌手已经进行了 q_E 次密钥询问,得到的密钥都是半功能的,敌手只需进行 q_S 次签名询问,生成相应的签名. 设 j 是 Game_k 中 $\mathcal{A}$ 所做的密钥询问的次数,$\mathcal{S}$ 根据 j 和 k 的大小关系来返回密钥和签名是正常的或半功能的.

证明(Part 1)　当 $0<k<q_E$ 时,$\mathcal{A}$ 进行 q_E 次密钥询问.

Setup:$\mathcal{S}$ 构造 (g,X_1X_2,X_3,Y_2Y_3,T) 和 $\mathcal{A}$ 模拟 Game_{k-1}或 Game_k. 参数设置如下:随机选择 $\alpha,a_1,a_2,b\leftarrow_R\mathbb{Z}_N$,令 $g=g,u_1=g^{a_1},u_2=g^{a_2},h=g^b$,选择哈希函数 H_1,公共参数 $\mathrm{param}=\{N,g,u_1,u_2,h,H_1,e(g,g)^\alpha\}$ 发给 $\mathcal{A}$. $\mathcal{A}$ 收到的公开参数与实际公开参数的分布是相同的.

Extract Query:$\mathcal{A}$ 对于身份 ID 进行生成密钥询问,在游戏 Game_k 中 $0<k<q_E$,敌手进行第 j 次密钥生成询问.

$q_E>j>k$,$\mathcal{S}$ 使用 Extract 算法产生正常密钥,随机选择 $r,t,w,v\leftarrow_R\mathbb{Z}_N$,计算 $d_{ID}=(g^\alpha(u_1^{ID}h)^r X_3^w,g^r X_3^t,u_2^r X_3^v)$,对于 $\mathcal{A}$ 来说收到的密钥是正确的.

$0<j<k$,$\mathcal{A}$ 对身份 ID 进行第 j 次生成密钥询问,$\mathcal{S}$ 生成半功能密钥,随机选择 $r,z,t,v\leftarrow_R\mathbb{Z}_N$,计算

$$d_{ID}=(g^\alpha(u_1^{ID}h)^r(Y_2Y_3)^z,g^r(Y_2Y_3)^t,u_2^r(Y_2Y_3)^v) \tag{8}$$

对于 $\mathcal{A}$ 来说收到的密钥是正确的.

$j=k$,$\mathcal{A}$ 对身份 ID 进行第 j 次生成密钥询问,$\mathcal{S}$ 计算 $z_k=a_1ID+b$,随机选择 $w,v\leftarrow_R\mathbb{Z}_N$,计算 $d_{ID}=(g^{\alpha}T^{z_k}X_3^{w},T,T^{a_2}X_3^{v})$,如果 $T\leftarrow_R G$,生成的是半功能密钥,如果 $T\leftarrow_R G_{p_1p_3}$,生成的是正常密钥(g^r 为 T 中的 G_{p_1} 部分).

Signature Query:$\mathcal{A}$ 发起对群组成员 L 和消息 M 的签名询问. 对于某个身份 $ID\in L$,$\mathcal{S}$ 计算 $m=H_1(M,L)$,随机选取 $r_i,w_i,t_i,\lambda_i\leftarrow_R\mathbb{Z}_N,(i=1,\cdots,n),\lambda_1+\lambda_2+\cdots+\lambda_n=0$,运行 Sign 算法生成 L 和 M 的签名,计算:$i=1,\cdots,n$,

$$i\neq\pi,\quad A_i=g^{\lambda_i}(u_1^{ID_i}u_2^{m}h)^{r_i}X_3^{w_i}\tag{9}$$

$$B_i=g^{r_i}X_3^{t_i}\tag{10}$$

$$i=\pi,\quad A_{\pi}=g^{\alpha+\lambda_{\pi}}(u_1^{ID_{\pi}}u_2^{m}h)^{r_{\pi}+r}X_3^{w+w_{\pi}+vm}\tag{11}$$

$$B_{\pi}=g^{r+r_{\pi}}X_3^{t+t_{\pi}}\tag{12}$$

对于 $\mathcal{A}$ 来说收到的签名和实际签名是不可区分的.

证明(Part 2) 当 $q_E<k<q_E+q_S$ 时,$\mathcal{A}$ 进行 q_S 次签名询问.

Setup:$\mathcal{S}$ 构造 (g,X_1X_2,X_3,Y_2Y_3,T) 和 $\mathcal{A}$ 模拟 Game_{k-1} 或 Game_k. 参数设置如下:随机选择 $\alpha,a_1,a_2,b\leftarrow_R\mathbb{Z}_N$,令 $g=g,u_1=g^{a_1},u_2=g^{a_2},h=g^b$,选择哈希函数 H_1,公共参数 $\mathrm{param}=\{N,g,u_1,u_2,h,H_1,e(g,g)^{\alpha}\}$ 发给 $\mathcal{A}$. $\mathcal{A}$ 收到的公共参数与实际公开参数的分布是相同的.

Extract Query:$\mathcal{A}$ 对于身份 ID 进行第 j 次生成密钥询问,在游戏中 $\mathcal{A}$ 已经进行过 q_E 次密钥生成询问,生成密钥都为半功能的.

Signature Query:$\mathcal{A}$ 发起对群组成员 L 和消息 M 的签名询问. 在游戏 Game_k 中 $q_E<k<q_E+q_S$,$\mathcal{A}$ 对于身份 ID 进行第 j 次签名询问.

$q_E+q_S>j>k$,$\mathcal{S}$ 计算 $m=H_1(M,L)$,随机选取 $r_i,w_i,t_i,\lambda_i\leftarrow_R\mathbb{Z}_N,(i=1,\cdots,n),\lambda_1+\lambda_2+\cdots+\lambda_n=0$,运行 Sign 算法生成 L 和 M 的签名,计算正常签名:$i=1,\cdots,n$

$$i\neq\pi,\quad A_i=g^{\lambda_i}(u_1^{ID_i}u_2^{m}h)^{r_i}X_3^{w_i}\tag{13}$$

$$B_i=g^{r_i}X_3^{t_i}\tag{14}$$

$$i=\pi,\quad A_{\pi}=g^{\alpha+\lambda_{\pi}}(u_1^{ID_{\pi}}u_2^{m}h)^{r_{\pi}+r}X_3^{w+w_{\pi}+vm}\tag{15}$$

$$B_{\pi}=g^{r+r_{\pi}}X_3^{t+t_{\pi}}\tag{16}$$

$q_E<j<k$,$\mathcal{S}$ 计算 $m=H_1(M,L)$,随机选取 $r_i,w_i,t_i,\lambda_i\leftarrow_R\mathbb{Z}_N,(i=1,\cdots,n),\lambda_1+\lambda_2+\cdots+\lambda_n=0$,运行 Sign 算法生成 L 和 M 的签名,计算半功能签名:$i=1,\cdots,n$

$$i\neq\pi,\quad A_i=g^{\lambda_i}(u_1^{ID_i}u_2^{m}h)^{r_i}X_3^{w_i}\tag{17}$$

$$B_i=g^{r_i}X_3^{t_i}\tag{18}$$

$$i=\pi,\quad A_{\pi}=g^{\alpha+\lambda_{\pi}}(u_1^{ID_{\pi}}u_2^{m}h)^{r+r_{\pi}}(Y_2Y_3)^{z+vm}X_3^{w_{\pi}}\tag{19}$$

$$B_{\pi}=g^{r+r_{\pi}}(Y_2Y_3)^{t}X_3^{t_{\pi}}\tag{20}$$

$j=k$,$\mathcal{S}$ 计算 $m=H_1(M,L)$,随机选取 $r_i,w_i,t_i,\lambda_i\leftarrow_R\mathbb{Z}_N,(i=1,\cdots,n),\lambda_1+\lambda_2+\cdots+\lambda_n=0$,运行 Sign 算法生成 L 和 M 的签名:$i=1,\cdots,n$

$$i\neq\pi,\quad A_i=g^{\lambda_i}(u_1^{ID_i}u_2^{m}h)^{r_i}X_3^{w_i}\tag{21}$$

$$B_i=g^{r_i}X_3^{t_i}\tag{22}$$

$$i=\pi,\quad A_{\pi}=g^{\alpha+\lambda_{\pi}}(u_1^{ID_{\pi}}u_2^{m}h)^{r_{\pi}}T^{z_i+a_2m}X_3^{w_{\pi}}\tag{23}$$

$$B_{\pi}=g^{r_{\pi}}TX_3^{t_{\pi}}\tag{24}$$

如果 $T\leftarrow_R G_{p_1p_3}$,$\mathcal{S}$ 能够正确的模拟 Game_{k-1}. 如果 $T\leftarrow_R G$,$\mathcal{S}$ 能够正确的模拟 Game_k. $\mathcal{A}$ 能够区分出 Game_{k-1} 和 Game_k,因此,$\mathcal{S}$ 可以根据 $\mathcal{A}$ 输出值区分 T 的两种不同情况.

引理3 如果存在一个敌手 $\mathcal{A}$ 使得 $\mathrm{Game}_{\mathrm{real}}\mathrm{Adv}_{\mathcal{A}}-\mathrm{Game}_{q_E+q_S}\mathrm{Adv}_{\mathcal{A}}=\varepsilon$,模拟者 $\mathcal{S}$ 以 ε 的优势攻破计算性假设2.

证明 Setup:$\mathcal{S}$ 构造 $(g,g^{\alpha}X_2,X_3,g^{s}Y_2,Z_2,T)$ 和 $\mathcal{A}$ 模拟游戏 $\mathrm{Game}_{q_E+q_S}$. $\mathcal{S}$ 随机选择 $a_1,a_2,b\leftarrow_R\mathbb{Z}_N$,设置公共参数 $g=g,u_1=g^{a_1},u_2=g^{a_2},h=g^b,e(g,g)^{\alpha}=e(g^{\alpha}X_2,g)$,选择哈希函数 H_1,公开参数 $\mathrm{param}=\{N,g,u_1,u_2,h,H_1,e(g^{\alpha}X_2,g)\}$ 发给 $\mathcal{A}$.

Extract Query:$\mathcal{A}$ 对于身份 ID 进行第 j 次生成密钥询问,$\mathcal{S}$ 生成半功能密钥,随机选择 $c,r,w,z,t,v,q\leftarrow_R\mathbb{Z}_N$,计算

$$d_{ID}=(g^{\alpha}X_2Z_2^{c}(u_1^{ID}h)^{r}X_3^{w},g^{r}Z_2^{z}X_3^{t},u_2^{r}Z_2^{q}X_3^{v})\tag{25}$$

Signature Query:$\mathcal{A}$ 发起对群组成员 L 和消息 M 的签名询问. 对于某个身份 $ID\in L$,$\mathcal{S}$ 计算 $m=H_1(M,L)$,然后运行 Sign 算法生成 L 和 M 的半功能签名. $\mathcal{S}$ 随机选 $r_i,\lambda_i\leftarrow_R\mathbb{Z}_N,R_{3,i},R'_{3,i}\leftarrow_R G_{p_3}(i=1,\cdots,n)$,$\lambda_1+\lambda_2+\cdots+\lambda_n=0$,计算 $i=1,\cdots,n$

$$i\neq\pi,\quad A_i=g^{\lambda_i}(u_1^{ID_i}u_2^{m}h)^{r_i}R_{3,i}\tag{26}$$

$$B_i=g^{r_i}R'_{3,i}\tag{27}$$

$i=\pi$,

$$A_{\pi}=g^{\alpha}X_2Z_2^{c}(u_1^{ID_{\pi}}h)^{r}X_3^{w}g^{\lambda_{\pi}}(u_1^{ID_{\pi}}u_2^{m}h)^{r_{\pi}}(u_2^{r}Z_2^{q}X_3^{v})^{m}R_{3,\pi}\tag{28}$$

$$B_{\pi}=g^{r}Z_2^{z}X_3^{t}g^{r_{\pi}}R'_{3,\pi}\tag{29}$$

Forgery:$\mathcal{A}$ 输出环成员 L 和 M 的签名 $\sigma=\{A_i,B_i\}_{i=1}^{n}$,$\mathcal{S}$ 先计算 $m=H_1(M,L)$,对于任意的 $s\leftarrow_R\mathbb{Z}_N$,$\mathcal{S}$ 计算

$$\prod_{i=1}^{n}\frac{e(g^{s}Y_2,A_i)}{e((g^{s}Y_2)^{a_1ID_i+a_2m+b},B_i)}=e(g,g)^{\alpha s}\tag{30}$$

这样就计算出 $e(g,g)^{\alpha s}$,敌手 $\mathcal{A}$ 能够以不可忽略的优势 ε 攻击成功,那么模拟者 $\mathcal{S}$ 以 ε 的优势攻破计算性假设2.

由以上3个引理及一系列游戏得证,我们的方案满足定义1,即我们的方案是不可伪造的. 在不可伪造性证明中,敌手无需事先提交挑战身份,而是在密钥提取询问

后适应性选择攻击目标,故而本文方案是完全安全的.

定理 2　我们的方案满足定义 2(方案是无条件匿名的).

证明　通过模拟者 $\mathcal{S}$ 和敌手 $\mathcal{A}$ 之间游戏完成无条件匿名性证明. Game_0 游戏模拟对身份 ID_0 进行签名,Game_1 游戏模拟对身份 ID_1 进行签名. 如果敌手对两个游戏视图不可区分,那么我们的方案满足无条件匿名性.

Game_0 游戏:

(1) 系统参数设置:$\mathcal{S}$ 输入参数 λ,并运行 Setup 算法生成系统参数 param 和主密钥 α,选择 $\alpha \leftarrow_R \mathbb{Z}_N$,$g$,$u_1,u_2,h \in G_{p_1}$,$X_3 \leftarrow_R G_{p_3}$,选择哈希函数 H_1. 公开参数 param = $\{N,g,u_1,u_2,h,X_3,H_1,e(g,g)^{\alpha}\}$ 和主密钥发送给敌手 $\mathcal{A}$.

(2) $\mathcal{A}$ 输出消息 M,两个身份 ID_0,ID_1,身份集合 L ($ID_0,ID_1 \in L$) 给模拟者. 模拟者生成 ID_0 私钥 d_{ID_0} 并计算 $m = H_1(M,L)$,实际签名者 $ID_\pi = ID_0$,用 $d_{ID_\pi} = d_{ID_0}$ 执行以下步骤:

① 随机选取 $r_i,\lambda_i \leftarrow_R \mathbb{Z}_N$,$R_{3,i},R'_{3,i} \leftarrow_R G_{p_3}$,($i = 1,\cdots,n$),$\lambda_1 + \lambda_2 + \cdots + \lambda_n = 0$

② 对于 $i = 1,\cdots,n$

$$i \neq \pi,\quad A_i = g^{\lambda_i}(u_1^{ID_i}u_2^m h)^{r_i}R_{3,i} \tag{31}$$

$$B_i = g^{r_i}R'_{3,i} \tag{32}$$

$$i = \pi,\quad A_\pi = g^{\alpha+\lambda_\pi}(u_1^{ID_\pi}u_2^m h)^{r+r_\pi}R_3\tilde{R}_3^m R_{3,\pi} \tag{33}$$

$$B_\pi = d_1 g^{r_\pi}R'_{3,\pi} = g^{r+r_\pi}R'_3R'_{3,\pi} \tag{34}$$

$\mathcal{S}$ 生成签名 $\sigma_0 = \{A_i,B_i\}_{i=1}^n$,并发送给 $\mathcal{A}$.

Game_1 游戏和 Game_0 游戏的不同在于 $\mathcal{S}$ 生成 ID_1 私钥 d_{ID_1},实际签名者 $ID_\pi = ID_1$,模拟者用 d_{ID_1} 生成签名 $\sigma_1 = \{A_i,B_i\}_{i=1}^n$,并发送给 $\mathcal{A}$.

两个签名中存在随机化元素 $\mathcal{R}_0 = \{r_{i,0},\lambda_{i,0},R_{3,i,0},R'_{3,i,0}\}_{i=1}^n$,$\mathcal{R}_1 = \{r_{i,1},\lambda_{i,1},R_{3,i,1},R'_{3,i,1}\}_{i=1}^n$,$\mathcal{R}_0$ 和 $\mathcal{R}_1$ 是同分布的,生成签名 σ_0 和 σ_1 也是同分布的. 对于 $\mathcal{A}$ 视图 Game_0 和 Game_1 是不可区分的,$\mathcal{A}$ 识别出实际签名者的优势不大于随机猜测. 因此,环签名方案是无条件匿名的.

3.3　性能分析

下面从计算效率和所用技术把新方案与已有的标准模型下基于身份环签名方案进行对比. 用 n 表示环签名中群组的成员个数,文献[20]的签名长度为 $4n+4$,本文签名长度为 $2n$. 相比较文献[20]本文采用合数阶群下两个子群判定性假设(Subgroup),达到基于身份的存在性不可伪造(EUF-CMA). 在计算效率上主要对双线性对配对运算,群 G 中的幂指数运算和群 G_T 中的幂指数运算进行比较,具体的对比如表 1 所示,在性能比较中,用 P 表示一个双线性对运算时间,用 E 表示 G_T 中幂指数运算时间,用 F 表示 G 中幂指数运算时间. 通过比较可以看出相对于文献[20],本文在签名长度和计算效率得到了很大改进,并满足安全性要求.

表 1　与标准模型下基于身份的环签名方案对比

方案	基础方案	困难性假设	群的类型	不可伪造性	系统建立	私钥提取	签名	验证
文献[20]	LW11	Subgroup(4 个)	合数阶	EUF-CMA	$1P$	$7F$	$(7n+7)F$	$(4n+1)P+1E+(4n+6)F$
本文	LW10	Subgroup(2 个)	合数阶	EUF-CMA	$1P$	$5F$	$(4n+2)F$	$2nP+1E+(2n+2)F$

4　总结

本文在标准模型下提出了一个新的基于身份的环签名方案,该方案满足无条件匿名性,且满足存在性不可伪造. 与现有的基于身份环签名方案相比,新方案在标准模型下基于 HIBE 构造了完全安全的身份环签名,在计算效率和安全性上都有了较大改善. 我们把构造固定长度的标准模型下安全的基于身份的环签名方案作为下一步研究方向.

参考文献

[1] RIVEST R, SHAMIR A, TAUMAN Y. How to leak a secret[A]. The 7th International Conference on the Theory and Application of Cryptology and Information Security [C]. Gold Coast, Australia, 2001. 552 – 565.

[2] 张福泰,张方国,王育民. 群签名及其应用[J]. 通信学报,2001,22(1):77 – 85.
ZHANG Fu-tai, ZHANG Fang-guo, WANG Yu-min. Group signature and its applications[J]. Journal of Communications, 2001, 22(1): 77 – 85. (in Chinese)

[3] 陈泽文,张龙军,王育民,等. 一种基于中国剩余定理的群签名方案[J]. 电子学报,2004,32(7):1062 – 1065.
CHEN Ze-wen, ZHANG Long-jun, WANG Yu-min, et al. A group signature scheme based on Chinese remainder theorem[J]. Acta Electronica Sinica, 2004, 32(7): 1062 – 1065. (in Chinese)

[4] 张键红,伍前红,邹建成,等. 一种高效的群签名[J]. 电子学报,2005,33(6):1113 – 1115.
ZHANG Jian-hong, WU Qian-hong, ZOU Jian-cheng, et al. An efficient group signature scheme[J]. Acta Electronica Sinica, 2005, 33(6): 1113 – 1115. (in Chinese)

[5] 李继国,孙刚,张亦辰. 标准模型下可证安全的本地验证者撤销群签名[J]. 电子学报,2011,39(7):1618 – 1623.
LI Ji-guo, SUN Gang, ZHANG Yi-chen. Provably secure group signature scheme with verifier-local revocation in the

standard model[J]. Acta Electronica Sinica,2011,39(7):1618 – 1623. (in Chinese)

[6] CHOW S S M, SUSILO W, YUEN T H. Escrowed linkability of ring signtures and its applications[A]. First International Conference on Cryptology in Vietnam[C]. Hanoi, Vietnam, 2006. 175 – 192.

[7] 苗付友,王行甫,苗辉,等. 一种支持悬赏的匿名电子举报方案[J]. 电子学报,2008,36(2):320 – 324.
MIAO Fu-you, WANG Xing-Fu, MIAO Hui, et al. An anonymous E-prosecution scheme with reward support[J]. Acta Electronica Sinica, 2008, 36(2): 320 – 324. (in Chinese)

[8] 王化群,于红,吕显强,等. 一种支持悬赏的匿名电子举报方案的安全性分析及设计[J]. 电子学报,2009,37(8):1826 – 1829.
WANG Hua-qun, YU Hong, LÜ Xian-qiang, et al. Cryptanalysis and design of an anonymous E-prosecution scheme with reward support[J]. Acta Electronica Sinica, 2009, 37(8): 1826 – 1829. (in Chinese)

[9] YANG X, WEI W, JOSEPH K L, CHEN X F. Lightweight anonymous authentication for ad hoc group: a ring signature approach[A]. International Conference on Provable Security[C]. Kanazawa, Japan, 2015. 215 – 226.

[10] SHAMIR A. Identity-based cryptosystems and signature schemes[A]. The Workshop on the Theory and Application of Cryptographic Techniques[C]. California, USA, 1984. 47 – 53.

[11] ZHANG F G, KIM K. ID-based blind signature and ring signature from pairings[A]. International Conference on the Theory and Application of Cryptology and Information Security[C]. Queenstown, New Zealand, 2002. 533 – 547.

[12] AU M H, JOSPH K L, YUEN T H, et al. ID-based ring signature scheme secure in the standard model[A]. International Workshop on Security[C]. Kyoto, Japan, 2006. 1 – 16.

[13] 张跃宇,李晖,王育民. 标准模型下基于身份的环签名方案[J]. 通信学报,2008,29(4):40 – 44.
Zhang Yue-yu, LI Hui, WANG Yu-min. Identity-based ring signature scheme under standard model[J]. Journal of Communications, 2008, 29(4): 40 – 44. (in Chinese)

[14] 刘振华,胡予濮,牟宁波,等. 新的标准模型下基于身份的环签名方案[J]. 电子与信息学报,2009,31(7):1727 – 1731.
LIU Zhen-hua, HU Yu-pu, MU Ning-bo, et al. New identity-based ring signature in the standard model[J]. Journal of Electronics & Information Technology, 2009, 31(7): 1727 – 1731. (in Chinese)

[15] 张明武,杨波,姚金涛,等. 标准模型下身份匿名签名方案分析与设计[J]. 通信学报,2011,32(5):40 – 46.
ZHANG Ming-wu, YANG Bo, YAO Jin-tao, et al. Cryptanalysis and design of signature schemes with identity ambiguity in the standard model[J]. Journal of Communications, 2011, 32(5): 40 – 46. (in Chinese)

[16] 葛爱军,马传贵,张振峰,等. 标准模型下固定长度的基于身份环签名方案[J]. 计算机学报,2012,35(9):1874 – 1880.
GE Ai-jun, MA Chuan-gui, ZHANG Zhen-feng, et al. Identity-based ring signature scheme with constant size signatures in the standard model[J]. Chinese Journal of Computers, 2012, 35(9): 1874 – 1880. (in Chinese)

[17] WATERS B. Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions[A]. Advances in Cryptology-CRYPTO[C]. California, USA, 2009. 619 – 636.

[18] LEWKO A, WATERS B. New techniques for dual system encryption and fully secure HIBE with short ciphertexts[A]. Theory of Cryptography Conference[C]. Zurich, Switzerland, 2010. 455 – 479.

[19] LEWKO A, WATERS B. Unbounded HIBE and attribute-based encryption[A]. Annual International Conference on the Theory and Applications of Cryptographic Techniques[C]. Tallinn Estonia, 2011. 547 – 567.

[20] AU M H, JOSPH K L, SUSILO W, ZHOU Jian-ying. Realizing fully secure unrestricted ID-based ring signature in the standard model based on HIBE[J]. IEEE Transactions on Information Forensics and Security, 2013, 8(12): 1909 – 1922.

[21] BONEH D, GOH E-J, NISSIM K. Evaluating 2-DNF formulas on ciphertexts[A]. Theory of Cryptography Conference[C]. Cambridge, MA, USA, 2005. 325 – 341.

作者简介

赵艳琦 男,1992 年生于吉林双辽,陕西师范大学计算机科学学院硕士研究生,研究兴趣为数字签名及其应用.
E-mail: zhaoyq@snnu.edu.cn

杨 波(通信作者) 男,1963 年生于陕西富平. 教授、博士生导师,陕西省“百人计划”特聘教授. 研究方向为密码学、信息安全.
E-mail: byang@snnu.edu.cn