素数阶群上基于非对称对的身份基环签名

侯红霞[1]，张明瑞[2]，赵艳琦[1]，董晓丽[1,3]

（1. 西安邮电大学网络空间安全学院，陕西 西安 710121；
2. 陕西师范大学计算机科学学院，陕西 西安 710061；
3. 广西密码学与信息安全重点实验室，广西 桂林 541004）

摘 要：针对已有身份基环签名的安全性证明难以在标准模型下实现的问题，提出标准模型下可证明安全的身份基环签名方案。首先，给出了身份基环签名安全模型和敌手模型的形式化定义。然后，基于素数阶群上的非对称对构造了一个具体的身份基环签名方案。最后，给出了该方案的安全性分析和性能分析。安全性分析结果表明，所提方案通过采用对偶系统加密技术实现了标准模型下的可证明安全性。性能分析结果表明，所提方案有效提升了方案中各算法的运行效率，与已有的基于对偶系统的身份基环签名方案相比，产生签名和验证签名的时间更短。

关键词：环签名；对偶系统加密；非对称对；标准模型；素数阶群

中图分类号：TP309

文献标识码：A

DOI: 10.11959/j.issn.1000−436x.2021159

ID-based ring signature on prime order group from asymmetric pairing

HOU Hongxia[1], ZHANG Mingrui[2], ZHAO Yanqi[1], DONG Xiaoli[1,3]

1. School of Cyberspace Security, Xi'an University of Posts and Telecommunications, Xi'an 710121, China
2. School of Computer Science, Shaanxi Normal University, Xi'an 710061, China
3. Guangxi Key Laboratory of Cryptography and Information Security, Guilin 541004, China

Abstract: For the problem that the security proof was difficult to be realized under the standard model in the existing ID-based ring signature schemes, an ID-based ring signature scheme proven secure in the standard model was proposed. Firstly, the formal definitions of security model and adversary model of ID-based ring signature were given. Then, a specific ID-based ring signature scheme was constructed on the prime order groups from asymmetric pairings. Finally, the security analysis and performance analysis were given. The results of security analysis show that the proven security of the proposed scheme is achieved under the standard model by using the dual system encryption technique. The results of performance analysis show that the operation efficiency of each algorithm in the proposed scheme is improved effectively, compared with existing ID-based ring signature schemes from dual system, it is shorter to take the time in generating and verifying signature.

Keywords: ring signature, dual system encryption, asymmetric pairing, standard model, prime order group

---

收稿日期：2021−05−08；**修回日期**：2021−07−23

基金项目：国家自然科学基金资助项目（No.62072369, No.62072371, No.61802303, No.61772418）；广西密码学与信息安全重点实验室研究课题基金资助项目（No.GCIS201923）；陕西省重点研发计划基金资助项目（No.2021ZDLGY06-02, No.2020ZDLGY08-04, No.2019KW-053）；陕西省创新能力支持计划基金资助项目（No.2020KJXX-052, No.2017KJXX-047）；青海省基础研究计划基金资助项目（No.2020-ZJ-701）

Foundation Items: The National Natural Science Foundation of China (No.62072369, No.62072371, No.61802303, No.61772418), Guangxi Key Laboratory of Cryptography and Information Security (No.GCIS201923), The Key Research and Development Program of Shaanxi (No.2021ZDLGY06-02, No.2020ZDLGY08-04, No.2019KW-053), The Innovation Capability Support Program of Shaanxi Province (No.2020KJXX-052, No.2017KJXX-047), The Basic Research Program of Qinghai Province (No.2020-ZJ-701)

1 引言

环签名的概念是由 Rivest 等[1]于 2001 年提出的。在环签名中，环中的任意成员都能代表整个环对消息进行签名，签名验证者仅知道签名来自环，但却不能确定具体的签名者。环签名中没有管理员，没有环的建立和撤销过程，因此真实的签名者对于验证者而言是无条件匿名的。

为了简化传统公钥基础设施中的证书管理问题，Shamir[2]于 1984 年引入了身份基公钥密码体制。在身份基密码体制中，用户的公钥可以是标识该用户身份的任意二进制串，比如 E-mail 地址等；对应的私钥则是由一个可信任的私钥生成中心（PKG, private key generator）根据该用户的身份生成的。因此，PKG 不需要保存已发布的证书列表，每个用户仅需保存系统参数而不需要保存其他用户的公钥证书。

身份基环签名将身份基公钥密码体制和环签名技术相融合，既实现了匿名性、不可伪造性，又避免了用户证书的管理。作为实现匿名性的一个重要的密码学原语，身份基环签名在许多场合（如电子选举、电子现金、区块链技术、车联网等[3-8]）中有重要的应用。

自从 Zhang 等[9]正式给出身份基环签名的概念后，许多身份基环签名方案及其变种被相继提出[10-16]。然而，这些方案的安全性都是在随机预言机模型下证明的。在随机预言机模型中，哈希函数被作为一个完全随机的理想化模型，这是一个非常强的假设。已有文献[17]表明，在随机预言机模型下被证明安全的方案在实际应用中可能并不安全。因此，设计标准模型下可证明安全的身份基环签名方案更具实际意义。2006 年，Au 等[18]在标准模型下提出了 2 个身份基环签名方案，但遗憾的是，这 2 个方案后来被证明并不能满足环签名的安全需求。此后，有许多工作致力于构造标准模型下高效安全的身份基环签名方案。文献[19-20]从节约通信成本和提高计算效率的角度出发，分别在标准模型下提出了改进的身份基环签名方案，但遗憾的是，这 2 个方案之后被证明不安全。2012 年，文献[21]给出了一个标准模型下具有固定签名长度的身份基环签名方案，但该方案被指出有漏洞。2013 年，通过分析分层身份基加密方案与身份基环签名方案之间的联系，Au 等[22]在标准模型下提出了一个身份基环签名方案。2018 年，基于 Au 等[22]方案，赵艳琦等[23]在标准模型下构造了一个新的身份基环签名方案。方案[22-23]在安全性证明时都采用了对偶系统加密技术，从而在标准模型下都达到了全安全性和完全匿名性。对偶系统加密技术为安全性归约证明开辟了一条新思路。然而，这 2 个方案都是在合数阶双线性群上构造的，因而实现效率都很低。已有文献[24]指出，阶数 n 为 160 bit 的素数阶群具有与阶数 n 为 1 024 bit 的合数阶群同样的安全水平，合数阶群上的双线性对运算要比素数阶群上的对运算慢许多。因此，在素数阶群上设计高效安全的环签名方案具有重要的实际意义。文献[22]也将此作为一个公开问题提出。

Ramanna 等[25]在非对称双线性对环境中提出了一些 Waters 对偶系统原语[26]的变形机制。许多研究结果[27-29]已表明，相比于对称双线性对运算，非对称双线性对运算更加快速和紧致。基于文献[22-23,25]的工作，本文给出了一种在素数阶群上构造身份基环签名方案的方法。在素数阶群上基于非对称双线性对构造了一个高效的身份基环签名方案。该方案可以抵抗适应性选择身份攻击和适应性选择消息攻击。通过采用对偶系统加密技术，该方案的安全性被归约到素数阶群上非对称对环境中的 3 个困难性假设。实验结果表明，与已有的基于对偶系统的身份基环签名方案相比较，本文方案在效率方面更具优势。

2 预备知识

2.1 符号说明

本文中，κ 表示安全参数，negl(κ) 表示一个关于 κ 的可忽略函数，$x \xleftarrow{R} \mathcal{X}$ 表示 x 均匀随机地取自集合 $\mathcal{X}$，$|R|$ 表示集合 R 的基，$[n]$ 表示集合 $\{1,2,\cdots,n\}$，ε 表示一个可忽略的参数。

2.2 非对称双线性对

令(G_1, G_2, G_T)分别是 3 个阶为素数 p 的循环群，其中 $G_1 = \langle P_1 \rangle$ 和 $G_2 = \langle P_2 \rangle$ 分别表示由 P_1 和 P_2 生成的加法群，G_T 是乘法群。

双线性对 $e: G_1 \times G_2 \to G_T$ 是满足以下性质的映射。

1) 双线性。对于 $P_1, Q_1 \in G_1$ 和 $P_2, Q_2 \in G_2$，有

$$e(P_1, P_2 + Q_2) = e(P_1, P_2)e(P_1, Q_2)$$

$$e(P_1 + Q_1, P_2) = e(P_1, P_2)e(Q_1, P_2)$$

2) 非退化性。$e(P_1, P_2) \neq 1 \in G_T$。

3) 有效可计算性。对于任意的 $P \in G_1$ 和 $Q \in G_2$，存在一个有效的算法计算 $e(P,Q)$。

当 $G_1 = G_2$ 时，双线性映射被称为对称或类型 1 双线性映射，否则被称为非对称双线性映射。非对称双线性映射进一步可分为类型 2 和类型 3 非对称双线性映射。类型 2 非对称双线性映射是指由 G_1 到 G_2 或由 G_2 到 G_1 存在一个有效的可计算同构，而类型 3 非对称双线性映射则不存在这样的同构。对于 $S_1 \in G_1$ 和 $S_2 \in G_2$，文中用 $S_1 \sim S_2$ 表示 S_1（以 P_1 为底）和 S_2（以 P_2 为底）具有相同的离散对数。

2.3 复杂性假设

判定性 Diffie-Hellman（DDH, decision Diffie-Hellman）假设[25]。令 P_1, P_2 分别是群 G_1, G_2 的随机生成元，$x_1, x_2, c \xleftarrow{R} Z_p, Y_1 \xleftarrow{R} G_1$。

G_1 中的 DDH 问题（记为 DDH1）是指给定 $(P_1, x_1P_1, x_2P_1, P_2, Z_1 = (x_1x_2 + c)P_1)$，判定 $c = 0$ 还是 $c \xleftarrow{R} Z_p$。

令 $\mathcal{B}$ 是一个输出为 0 或 1 的多项式时间（PPT, probabilistic polynomial time）算法。定义 $\mathcal{B}$ 解决 DDH1 问题的优势为

$$\mathrm{Adv}^{\mathcal{B}}_{\mathrm{DDH1}} = |\Pr[\mathcal{B}(P_1, x_1P_1, x_2P_1, P_2, x_1x_2P_1) = 1] - \Pr[\mathcal{B}(P_1, x_1P_1, x_2P_1, P_2, Y_1) = 1]|$$

如果对于任意敌手 $\mathcal{B}$，其运行时间至多为 t，解决 DDH1 问题的优势为 $\mathrm{Adv}^{\mathcal{B}}_{\mathrm{DDH1}} \leqslant \varepsilon$，则称 (ε, t)-DDH1 假设成立。

G_2 中的 DDH 假设（记为 DDH2）定义类似。

DDH2v 假设[25]。令 P_1, P_2 分别是群 G_1, G_2 的随机生成元，$x_1, x_2, d, z, c \xleftarrow{R} Z_p$，$Y_2 \xleftarrow{R} G_2$。

DDH2v 问题是指给定 $(P_1, dP_1, dzP_1, zx_1P_1, P_2, dP_2, x_1P_2, x_2P_2, Z_2 = (x_1x_2 + c)P_2)$，判定 $c = 0$ 还是 $c \xleftarrow{R} Z_p$。

令 $\mathcal{B}$ 是一个输出为 0 或 1 的 PPT 算法。定义 $\mathcal{B}$ 解决 DDH2v 问题的优势为

$$\mathrm{Adv}^{\mathcal{B}}_{\mathrm{DBDH}} = |\Pr[\mathcal{B}(P_1, dP_1, dzP_1, zx_1P_1, P_2, dP_2, x_1P_2, x_2P_2, x_1x_2P_2) = 1] - \Pr[\mathcal{B}(P_1, dP_1, dzP_1, zx_1P_1, P_2, dP_2, x_1P_2, x_2P_2, Y_2) = 1]|$$

如果对于任意敌手 $\mathcal{B}$，其运行时间至多为 t，解决 DDH2v 问题的优势为 $\mathrm{Adv}^{\mathcal{B}}_{\mathrm{DDH2v}} \leqslant \varepsilon$，则称 (ε, t)-DDH2v 假设成立。

判定性双线性 Diffie-Hellman（DBDH, decision bilinear Diffie-Hellman）假设[25]。令 P_1, P_2 分别是群 G_1, G_2 的随机生成元，$x_1, x_2, x_3, c \xleftarrow{R} Z_p$，$Y_T \xleftarrow{R} G_T$。

DBDH 问题是指给定 $(P_1, x_1P_1, x_2P_1, x_3P_1, P_2, x_1P_2, x_2P_2, x_3P_2, Z_3)$，判定 $Z_3 = e(P_1, P_2)^{x_1x_2x_3}$ 还是 $Z_3 \xleftarrow{R} G_T$。

令 $\mathcal{B}$ 是一个输出为 0 或 1 的 PPT 算法。定义 $\mathcal{B}$ 解决 DBDH 问题的优势为

$$\mathrm{Adv}^{\mathcal{B}}_{\mathrm{DBDH}} = |\Pr[\mathcal{B}(P_1, x_1P_1, x_2P_1, x_3P_1, P_2, x_1P_2, x_2P_2, x_3P_2, e(P_1, P_2)^{x_1x_2x_3}) = 1] - \Pr[\mathcal{B}(P_1, x_1P_1, x_2P_1, x_3P_1, P_2, x_1P_2, x_2P_2, x_3P_2, Y_T) = 1]|$$

如果对于任意敌手 $\mathcal{B}$，其运行时间至多为 t，解决 DBDH 问题的优势为 $\mathrm{Adv}^{\mathcal{B}}_{\mathrm{DBDH}} \leqslant \varepsilon$，则称 (ε, t)-DBDH 假设成立。

2.4 安全模型

定义 1　一个 $(1, n)$ 身份基环签名方案由以下 4 个 PPT 算法组成。

Setup。该算法由 PKG 运行，输入一个安全参数 κ，输出主密钥 MSK 和系统公开参数 Params。

Extract。对于身份 ID，该算法输入主密钥 MSK，输出身份 ID 所对应的私钥 $\mathrm{SK}_{\mathrm{ID}}$。

Sign。输入系统公开参数 Params、身份集 $\mathrm{Ring} = \{\mathrm{ID}_1, \cdots, \mathrm{ID}_n\}$、消息 m 以及用户私钥 $\{\mathrm{SK}_{\mathrm{ID}} \mid \mathrm{ID} \in \mathrm{Ring}\}$，输出一个 $(1, n)$ 身份基环签名 σ。

Verify。输入系统公开参数 Params、n 个用户的身份集 $\mathrm{Ring} = \{\mathrm{ID}_1, \cdots, \mathrm{ID}_n\}$、消息 m 以及环签名 σ，输出 Valid 或 Invalid。

一个安全的 $(1, n)$ 身份基环签名方案应满足不可伪造性和匿名性。

定义 2　不可伪造性。如果没有多项式时间敌手能以不可忽略的优势赢得以下游戏，一个 $(1, n)$ 身份基环签名方案在适应性选择消息攻击和适应性选择身份攻击下是不可伪造的。

该游戏在敌手 $\mathcal{A}$ 与挑战者 $\mathcal{C}$ 之间进行。

1) 输入安全参数 κ，挑战者 $\mathcal{C}$ 运行 Setup 算法，然后将系统公开参数 Params 发送给敌手 $\mathcal{A}$。

2) 通过访问下述预言机，敌手 $\mathcal{A}$ 在多项式时间内适应性地向挑战者 $\mathcal{C}$ 发起以下询问。

密钥提取预言机（EO, extraction oracle）：输入身份 ID，$\mathrm{SK}_{\mathrm{ID}} \leftarrow \mathrm{Extract(params, ID)}$ 被返回给敌手 $\mathcal{A}$。

签名预言机（SO, signing oracle）：敌手 $\mathcal{A}$ 选取一个身份集 $\mathrm{Ring} = \{\mathrm{ID}_1, \cdots, \mathrm{ID}_n\}$ 和消息 m，签名预

言机会返回一个有效的 $(1,n)$ 身份基环签名 σ 给 $\mathcal{A}$。此过程中，签名预言机可以询问密钥提取预言机。

3) 最后，$\mathcal{A}$ 输出 $(\text{Ring}^*,m^*,\sigma^*)$，且 (Ring^*,m^*) 没有在之前的签名询问中出现过，同时对于环 Ring^* 中的任意身份 $\text{ID}\in\text{Ring}^*$，不允许 $\mathcal{A}$ 做密钥提取询问。

如果 $\text{Verify}(\text{Ring}^*,m^*,\sigma^*)$ 的输出结果为 Valid，则 $\mathcal{A}$ 赢得该游戏。定义敌手 $\mathcal{A}$ 的获胜优势为 $\text{Adv}_{\mathcal{A}}=\Pr[\mathcal{A}\ \text{succeeds}]$。

定义 3 匿名性。当且仅当以下条件被满足，一个 $(1,n)$ 身份基环签名方案是无条件匿名的。

给定任意身份集 $\text{Ring}=\{\text{ID}_1,\cdots,\text{ID}_n\}$，消息 m 以及环签名 σ，即使以无限的计算能力，任意敌手都不能以优于随机猜测的概率识别出真实的签名者。换句话说，敌手 $\mathcal{A}$ 仅能以不高于 $1/n$ 的概率输出真实签名者的身份。

2.5 敌手模型

存在 2 种类型的签名和密钥：正常类型，记为 type-N；半功能类型，记为 type-S。type-S 类型的签名和密钥仅在安全性证明中使用，并不会出现在真实的签名方案中。

根据签名的类型可将敌手划分为 2 种类型。

type-S 伪造者：如果敌手为 type-S，这种情况下，模拟器仅输出 type-N 签名和密钥。

type-N 伪造者：如果敌手为 type-N，这种情况下，模拟器需要使用 game-hopping 技术在敌手未察觉的情况下将签名和密钥逐步由 type-N 转变为 type-S。

3 基于非对称对的身份基环签名方案

3.1 方案构造

Setup。令 $e:G_1\times G_2\to G_T$ 是一个类型 3 非对称双线性映射，其中 $G_1=\langle P_1\rangle$ 和 $G_2=\langle P_2\rangle$ 都是阶为素数 p 的加法群。随机选取参数 $a,v,v'\xleftarrow{R}Z_p$，使 $V_2=vP_2$，$V_2'=v'P_2$，$\tau P_2=V_2+aV_2'$（$\tau=v+av'$）。$H_0:\{0,1\}^*\to Z_p$，$H_1:\{0,1\}^*\times\{0,1\}^*\to Z_p$ 是 2 个抗碰撞哈希函数。PKG 随机选取 $\alpha\in Z_p$，$Q_1,W_1,U_1\in G_1$，$Q_2,W_2,U_2\in G_2$ 且 $Q_1\sim Q_2$，$W_1\sim W_2$，$U_1\sim U_2$。系统主密钥为 $\text{MSK}=\alpha P_2$，系统公开参数为 $\text{Params}=\{P_1,aP_1,\tau P_1,Q_1,W_1,U_1,e(P_1,P_2)^{\alpha},H_0,H_1\}$。

Extract。为了生成身份 $\text{ID}\in\{0,1\}^{\ell}$ 的用户私钥，该算法随机选取 $r\xleftarrow{R}Z_p$ 和标签 $\text{ktag}_{\text{ID}}\xleftarrow{R}Z_p$，计算

$$\begin{aligned}&\text{id}=H_0(\text{ID})\\&A_{\text{ID}}=\alpha P_2+rV_2\\&B_{\text{ID}}=rV_2'\\&C_{\text{ID}}=r(\text{id}Q_2+\text{ktag}_{\text{ID}}W_2+U_2)\\&D_{\text{ID}}=rP_2\end{aligned}$$

算法输出 $\text{SK}_{\text{ID}}=(A_{\text{ID}},B_{\text{ID}},C_{\text{ID}},D_{\text{ID}})$ 作为身份 ID 的用户私钥，并秘密发送 SK_{ID} 和 $\{\text{ktag}_{\text{ID}},P_2,V_2,V_2',Q_2,W_2,U_2\}$ 给用户 ID。

Sign。令环 $\text{Ring}=\{\text{ID}_1,\cdots,\text{ID}_n\}$ 为包含 n 个身份的身份集。假设环 Ring 中的一个用户 ID，不失一般性，假设 ID 是环 Ring 的第 π 个用户（$\pi\in[n]$），即 $\text{ID}_{\pi}=\text{ID}$。为了生成消息 $m\in\{0,1\}^*$ 的环签名，该算法分别计算 $\text{id}_i=H_0(\text{ID}_i)$（$i\in[n]$）以及 $M=H_1(m,\text{Ring})$，然后执行以下步骤。

1) 随机选取 $\lambda_i,r_i,\text{ktag}_i\xleftarrow{R}Z_p$（$i\in[n]$，令 $\text{ktag}_{\pi}=\text{ktag}_{\text{ID}}$）使其满足限制 $\sum_{i=1}^{n}\lambda_i=0$ 和 $\sum_{i=1}^{n}r_i=\bar{r}$。

2) 对于 $i\in[n]$，有以下结论成立。

当 $i\neq\pi$ 时，有

$$\begin{aligned}&A_i=\lambda_iP_2+r_iV_2\\&B_i=r_iV_2'\\&C_i=r_i(\text{id}_iQ_2+\text{ktag}_iW_2+U_2)\\&D_i=r_iP_2\end{aligned}$$

当 $i=\pi$ 时，有

$$\begin{aligned}&A_{\pi}=A_{\text{ID}_{\pi}}+\lambda_{\pi}P_2+r_{\pi}V_2+MP_2=\\&\alpha P_2+MP_2+\lambda_{\pi}P_2+(r_{\pi}+r)V_2\\&B_{\pi}=B_{\text{ID}_{\pi}}+r_{\pi}V_2'=(r_{\pi}+r)V_2'\\&C_{\pi}=C_{\text{ID}_{\pi}}+r_{\pi}(\text{id}_{\pi}Q_2+\text{ktag}_{\pi}W_2+U_2)=\\&(r_{\pi}+r)(\text{id}_{\pi}Q_2+\text{ktag}_{\pi}W_2+U_2)\\&D_{\pi}=D_{\text{ID}_{\pi}}+r_{\pi}P_2=(r_{\pi}+r)P_2\end{aligned}$$

3) 输出签名 $\sigma=\{A_i,B_i,C_i,D_i,\text{ktag}_i\}_{i=1}^{n}$。

Verify。在收到消息 m 的环签名 $\sigma=\{A_i,B_i,C_i,D_i,\text{ktag}_i\}_{i=1}^{n}$ 后，验证者先计算 $\text{id}_i=H_0(\text{ID}_i)$（$i\in[n]$）和 $M=H_1(m,\text{Ring})$；然后随机选取 s，$\text{ctag}_1,\cdots,\text{ctag}_n\xleftarrow{R}Z_p$（其中 $\text{ctag}_i\neq\text{ktag}_i$，$i\in[n]$）并计算 $T_1=sP_1$，$T_2=asP_1$，$T_3=-s\tau P_1+$

$sW_1, T_{4,i} = s(\mathrm{id}_i Q_1 + \mathrm{ctag}_i W_1 + U_1)$；最后验证者检验式(1)是否成立。

$$\prod_{i=1}^{n} e(T_1, A_i)e(T_2, B_i)e(T_3, D_i) = e(P_1, P_2)^{\alpha s} e(P_1, P_2)^{Ms} \prod_{i=1}^{n} \left(\frac{e(T_{4,i}, D_i)}{e(T_1, C_i)} \right)^{\frac{1}{\mathrm{ctag}_i - \mathrm{ktag}_i}} \quad (1)$$

3.2　正确性

方案的正确性成立，是因为

$$\prod_{i=1}^{n} e(T_1, A_i)e(T_2, B_i)e(T_3, D_i) = e(sP_1, \alpha P_2)e(sP_1, MP_2)e(sP_1, \lambda_\pi P_2) \cdot e(sP_1, (r + r_\pi)V_2)e(saP_1, (r + r_\pi)V_2') \cdot e(-s(v + av')P_1 + sW_1, (r + r_\pi)P_2) \cdot \prod_{i=1, i\neq\pi}^{n} e(sP_1, \lambda_i P_2)e(sP_1, r_i V_2)e(saP_1, r_i V_2') \cdot e(-s(v + av')P_1, r_i P_2)e(sW_1, r_i P_2) = e(P_1, P_2)^{\alpha s} e(P_1, P_2)^{Ms} e(W_1, P_2)^{s\left(\sum_{i=1}^{n} r_i + r\right)} = e(P_1, P_2)^{\alpha s} e(P_1, P_2)^{Ms} e(W_1, P_2)^{s(\bar{r} + r)}$$

$$\prod_{i=1}^{n} \left(\frac{e(T_{4,i}, D_i)}{e(T_1, C_i)} \right)^{\frac{1}{\mathrm{ctag}_i - \mathrm{ktag}_i}} = \left(\frac{e(T_{4,\pi}, D_\pi)}{e(T_1, C_\pi)} \right)^{\frac{1}{\mathrm{ctag}_\pi - \mathrm{ktag}_\pi}} \cdot \prod_{i=1, i\neq\pi}^{n} \left(\frac{e(T_{4,i}, D_i)}{e(T_1, C_i)} \right)^{\frac{1}{\mathrm{ctag}_i - \mathrm{ktag}_i}} = e(W_1, P_2)^{s(r + r_\pi)} \prod_{i=1, i\neq\pi}^{n} e(W_1, P_2)^{sr_i} = e(W_1, P_2)^{s\left(\sum_{i=1}^{n} r_i + r\right)} = e(W_1, P_2)^{s(\bar{r} + r)}$$

4　安全性证明

本文方案的安全性采用对偶系统加密技术进行证明，为此需定义 2 个额外的结构，即半功能密钥和半功能签名，半功能密钥和半功能签名不会出现在真实的签名方案中，仅用于方案的安全性证明。

半功能密钥。若身份 ID 的正常密钥为 $\mathrm{SK}_{\mathrm{ID}} = (\mathrm{A}'_{\mathrm{ID}}, \mathrm{B}'_{\mathrm{ID}}, \mathrm{C}'_{\mathrm{ID}}, \mathrm{D}'_{\mathrm{ID}})$，则其半功能密钥被设置为 $\mathrm{SK}_{\mathrm{ID}} = (A_{\mathrm{ID}} = A'_{\mathrm{ID}} - a\gamma P_2, B_{\mathrm{ID}} = B'_{\mathrm{ID}} + \gamma P_2, C_{\mathrm{ID}} = C'_{\mathrm{ID}}, D_{\mathrm{ID}} = D'_{\mathrm{ID}})$，其中 $\gamma \xleftarrow{R} Z_q$。

半功能签名。对于环 $\mathrm{Ring} = \{\mathrm{ID}_1, \cdots, \mathrm{ID}_\pi, \mathrm{ID}_n\}$，若签名算法输出的正常签名为 $\sigma' = \{A'_i, B'_i, C'_i, D'_i, \mathrm{ktag}'_i\}_{i=1}^{n}$，则其半功能签名 σ 设置为 $A_\pi = A'_\pi - a\gamma P_2$，$B_\pi = B'_\pi + \gamma P_2$，其余元素与 σ' 中的元素相同，即

$$\sigma = (A_\pi, B_\pi, \{A_i = A'_i, B_i = B'_i\}_{i=1, i\neq\pi}^{n}, \{C_i = C'_i, D_i = D'_i, \mathrm{ktag}_i = \mathrm{ktag}'_i\}_{i=1}^{n})。$$

定理 1　若假设 DDH1、DDH2v 和 DBDH 成立，则 3.1 节所构造的方案是不可伪造的。

证明　为了证明本文方案在 type-S 伪造者和 type-N 攻击下是不可伪造的，考虑下面 2 种情况。

情况 1　若敌手 $\mathcal{A}$ 能输出一个 type-S 的伪造，则可构造一个能利用敌手 $\mathcal{A}$ 的能力攻破假设 DDH1 的模拟器 $\mathcal{B}$。

换句话说，模拟器 $\mathcal{B}$ 的目的是在收到一个 DDH1 实例 $(P_1, sP_1, aP_1, P_2, Z_1 = (as + c)P_1)$ 后，判定 c 是否等于 0。为此，模拟器 $\mathcal{B}$ 与敌手 $\mathcal{A}$ 执行以下游戏。

系统建立　模拟器 $\mathcal{B}$ 随机选取 $\alpha, y_v, y_{v'}, y_q, y_w, y_u \xleftarrow{R} Z_q$，并设置参数

$$Q_1 = y_q P_1,\ W_1 = y_W P_1,\ U_1 = y_u P_1,$$
$$Q_2 = y_q P_2,\ W_2 = y_W P_2,\ U_2 = y_u P_2,$$
$$V_2 = y_v P_2,\ V'_2 = y_{v'} P_2$$

这里相当于隐式地令 $\tau = y_v + a y_{v'}$，则 $\tau P_1 = y_v P_1 + y_{v'}(aP_1)$。接着模拟器 $\mathcal{B}$ 利用 α 计算其余参数，然后选取 2 个哈希函数 H_0, H_1，发送系统公开参数给敌手 $\mathcal{A}$

$$\mathrm{PK} = \{P_1, aP_1, \tau P_1, Q_1, W_1, U_1, e(P_1, P_2)^\alpha, H_0, H_1\}$$

询问　由于模拟器 $\mathcal{B}$ 知道系统主密钥，因此能正确回答所有来自敌手 $\mathcal{A}$ 的密钥询问。

伪造　当敌手 $\mathcal{A}$ 输出一个关于环 Ring 和消息 m 的伪造环签名 $\sigma^* = \{A_i^*, B_i^*, C_i^*, D_i^*, \mathrm{ktag}_i^*\}_{i=1}^{n}$ 后，模拟器 $\mathcal{B}$ 首先计算 $M = H_1(m, \mathrm{Ring})$，$\mathrm{id}_i = H_0(\mathrm{ID}_i)$（$i \in [n]$），然后随机选取 s'，$\mathrm{ctag}_1, \cdots, \mathrm{ctag}_n \xleftarrow{R} Z_p$，（其中 $\mathrm{ctag}_i \neq \mathrm{ktag}_i$，$i \in [n]$），计算 $T_1 = s'P_1$，$T_2 = s'aP_1$，$T_3 = -s'\tau P_1 + s'W$，$T_{4,i} = s'(\mathrm{id}_i Q_1 + \mathrm{ctag}_i W_1 + U_1)$，于是有

$$\prod_{i=1}^{n} e(T_1, A_i^*) e(T_2, B_i^*) e(T_3, D_i^*) =$$

$$e(P_1, P_2)^{\alpha s'} e(P_1, P_2)^{Ms'} \prod_{i=1}^{n} \left(\frac{e(T_{4,i}, D_i^*)}{e(T_1, C_i^*)} \right)^{\frac{1}{\text{ctag}_i - \text{ktag}_i}} \tag{2}$$

因为敌手 $\mathcal{A}$ 输出的是一个 type-S 伪造，所以一定存在 π，使 $A_\pi^* = A_\pi^{*\prime} - a\gamma P_2$，$B_\pi^* = B_\pi^{*\prime} + \gamma P_2$。利用这一点，模拟器 $\mathcal{B}$ 便可判定 c 是否等于 0，具体如下。

模拟器 $\mathcal{B}$ 可设置 $T_1 = sP_1$，$T_2 = Z_1$，$T_3 = -y_v(sP_1) - y_v' Z_1 + y_w(sP_1)$，$T_{4,i} = (\text{id}_i y_q + \text{ctag}_i y_w + y_u)(sP_1)$，然后验证式(3)是否成立。

$$\prod_{i=1}^{n} e(T_1, A_i^*) e(T_2, B_i^*) e(T_3, D_i^*) \stackrel{?}{=}$$

$$e(T_1, P_2)^{\alpha} e(T_1, P_2)^{M} \prod_{i=1}^{n} \left(\frac{e(T_{4,i}, D_i^*)}{e(T_1, C_i^*)} \right)^{\frac{1}{\text{ctag}_i - \text{ktag}_i}} \tag{3}$$

如果 $c = 0$，则式(3)成立；否则，式(3)不成立，因为会有额外的一项 $e(P_1, P_2)^{\gamma c} \neq 1$。

情况 2 这部分证明中，假设敌手 $\mathcal{A}$ 的伪造为 type-N。进一步，假设敌手 $\mathcal{A}$ 共做了 L 次密钥提取询问和签名询问。该部分证明是通过一系列游戏的 game-hopping 技术来完成的，这一系列游戏记为 $\text{Game}_0, \text{Game}_1, \cdots, \text{Game}_L$。

Game_0：真实的不可伪造性游戏。

Game_k：对于每个 $k \in [L]$，游戏 Game_k 如同 Game_0，除了返回给敌手 $\mathcal{A}$ 的第 k 个密钥和签名为 type-S。

对于每个 $k \in [L]$，Game_{k-1} 与 Game_k 的不可区分性可归约到 DDH2v 困难性假设上。

换句话说，模拟器 $\mathcal{B}$ 的目的是在收到一个 DDH2v 实例 $(P_1, dP_1, dzP_1, zx_1P_1, P_2, dP_2, x_1P_2, x_2P_2, Z_2 = (x_1x_2 + c)P_2)$ 后，判定 c 是否等于 0。为此，模拟器 $\mathcal{B}$ 与敌手 $\mathcal{A}$ 执行以下游戏。

系统建立 模拟器 $\mathcal{B}$ 随机选取 $a, \alpha, \mu, \xi, y_v', y_q, y_u, y_w \xleftarrow{R} Z_q$，并设置参数 $Q_2 = -\mu(dP_2) + y_q P_2$，$U_2 = -\xi(dP_2) + y_u P_2$，$W_2 = (dP_2) + y_w P_2$，$Q_1 = -\mu(dP_1) + y_q P_1$，$U_1 = -\xi(dP_1) + y_u P_1$，$W_1 = (dP_1) + y_w P_1$，$V_2 = -a(x_1P_2)$，$V_2' = x_1P_2 + y_u' P_2$。

令 $\tau = ay_v'$，则 $\tau P_1 = ay_{v'} P_1$。同样，Q_1, W_1, U_1 也可由 dP_1 类似地计算而得。其余的公开参数以及困难问题中的其他元素均可由 a 和 α 计算得到，然后模拟器 $\mathcal{B}$ 选取 2 个哈希函数 H_0, H_1，将以下公开参数发送给敌手 $\mathcal{A}$

$$\text{PK} = \{P_1, aP_1, \tau P_1, Q_1, W_1, U_1, e(P_1, P_2)^{\alpha}, H_0, H_1\}$$

询问 对于第 j 次询问，模拟器 $\mathcal{B}$ 需根据 $j \in [L]$ 的值给敌手返回 type-S 或 type-N 的密钥或签名。

如果 $j > k$，则模拟器 $\mathcal{B}$ 利用主密钥和秘密参数生成一个 type-N 的密钥或签名。

如果 $j < k$ 且第 j 次询问是针对身份 ID 的一个密钥提取询问，则模拟器 $\mathcal{B}$ 首先生成一个正常密钥 $\text{SK}_{\text{ID}}' = (A_{\text{ID}}', B_{\text{ID}}', C_{\text{ID}}', D_{\text{ID}}')$，然后随机选取 $\gamma \xleftarrow{R} Z_p$，计算得到一个半功能密钥 $\text{SK}_{\text{ID}} = (A_{\text{ID}} = A_{\text{ID}}' - a\gamma P_2, B_{\text{ID}} = B_{\text{ID}}' + \gamma P_2, C_{\text{ID}} = C_{\text{ID}}', D_{\text{ID}} = D_{\text{ID}}')$。

如果 $j < k$ 且第 j 次询问是针对环 $\text{Ring} = \{\text{ID}_1, \cdots, \text{ID}_n\}$ 和消息 m 的一个签名询问，则模拟器 $\mathcal{B}$ 首先生成一个正常签名 $\sigma' = \{A_i', B_i', C_i', D_i', \text{ktag}_i'\}_{i=1}^n$，然后随机选取 $\gamma \xleftarrow{R} Z_p$，计算得到一个半功能签名 $\sigma = \{A_i, B_i, C_i, D_i, \text{ktag}_i\}_{i=1}^n$ 如下。

对于 $i \in [n]$，有以下结论成立。

当 $i \neq \pi$ 时，有 $A_i = A_i'$，$B_i = B_i'$，$C_i = C_i'$，$D_i = D_i'$，$\text{ktag}_i = \text{ktag}_i'$；

当 $i = \pi$ 时，有 $A_\pi = A_\pi' - a\gamma P_2$，$B_\pi = B_\pi' + \gamma P_2$，$C_\pi = C_\pi'$，$D_\pi = D_\pi'$，$\text{ktag}_\pi = \text{ktag}_\pi'$。

如果 $j=k$ 且第 j 次询问是针对身份 ID 的一个密钥提取询问，则模拟器 $\mathcal{B}$ 首先生成一个正常密钥 $\text{SK}_{\text{ID}}' = (A_{\text{ID}}', B_{\text{ID}}', C_{\text{ID}}', D_{\text{ID}}')$，并令 $\text{ktag}_{\text{ID}} = \mu\text{id} + \xi$（其中 $\text{id} = H_0(\text{ID})$），然后计算身份 ID 的私钥

$$A_{\text{ID}} = A_{\text{ID}}' - aZ_2$$

$$B_{\text{ID}} = B_{\text{ID}}' + Z_2 + y_{v'}(x_2P_2)$$

$$C_{\text{ID}} = C_{\text{ID}}' + (y_q\text{id} + y_w\text{ktag}_{\text{ID}} + y_u)(x_2P_2)$$

$$D_{\text{ID}} = D_{\text{ID}}' + x_2P_2$$

这里隐式地设置 $r = r' + x_2$。如果 $Z_2 = x_1x_2P_2$，则身份 ID 的私钥是正常密钥，否则 $Z_2 = (x_1x_2 + c)P_2$，身份 ID 的私钥就是一个 $\gamma = c$ 的半功能密钥。

如果 $j=k$ 且第 j 次询问是针对环 $\text{Ring} = \{\text{ID}_1, \cdots, \text{ID}_n\}$ 和消息 m 的一个签名询问，则模拟器 $\mathcal{B}$ 首先利用主密钥生成一个正常密钥 $\text{SK}_{\text{ID}_\pi} = (A_{\text{ID}_\pi}', B_{\text{ID}_\pi}', C_{\text{ID}_\pi}', D_{\text{ID}_\pi}')$（$\pi \in [n]$），选取满足 $\sum_{i=1}^{n} \lambda_i = 0$ 和 $\sum_{i=1}^{n} r_i = \bar{r}$ 限制的随机数 $\lambda_i, r_i \xleftarrow{R} Z_p$，选

取 $\text{ktag}_i \xleftarrow{R} Z_p$（其中 $i \in \{1,\cdots,\pi-1,\pi+1,\cdots,n\}$），$\text{ktag}_\pi = \mu \text{id}_\pi + \xi$。然后模拟器 $\mathcal{B}$ 回答第 j 次签名询问如下。

对于 $i \in [n]$，有以下结论成立。

当 $i \neq \pi$ 时，有

$$A_i = \lambda_i P_2 + r_i V_2$$
$$B_i = r_i V_2'$$
$$C_i = r_i(\text{id}_i Q_2 + \text{ktag}_i W_2 + U_2)$$
$$D_i = r_i P_2$$

当 $i = \pi$ 时，有

$$A_\pi = \lambda_\pi P_2 + MP_2 + r_\pi V_2 + A'_{\text{ID}_\pi} - aZ_2$$
$$B_\pi = r_\pi V_2' + B'_{\text{ID}} + Z_2 + y_{v'}(x_2 P_2)$$
$$C_\pi = r_\pi(\text{id}_\pi Q_2 + \text{ktag}_\pi W_2 + U_2) + C'_{\text{ID}} + (y_q \text{id} + y_w \text{ktag}_{\text{ID}} + y_u)(x_2 P_2)$$
$$D_\pi = r_\pi P_2 + D'_{\text{ID}} + x_2 P_2$$

最后输出签名 $\sigma = \{A_i, B_i, C_i, D_i, \text{ktag}_i\}_{i=1}^n$。这里隐式地设置 $r = r' + x_2$。如果 $Z_2 = x_1 x_2 P_2$，则签名时正常的，否则 $Z_2 = (x_1 x_2 + c)P_2$，签名是一个 $\gamma = c$ 的半功能签名。

伪造　当敌手 $\mathcal{A}$ 输出一个关于环 Ring 和消息 m 的伪造环签名 $\sigma^* = \{A_i^*, B_i^*, C_i^*, D_i^*, \text{ktag}_i^*\}_{i=1}^n$ 后，模拟器 $\mathcal{B}$ 首先计算 $M = H_1(m, \text{Ring})$，$\text{id}_i = H_0(\text{ID}_i)$（$i \in [n]$），然后随机选取 $s, \text{ctag}_1, \cdots, \text{ctag}_n \xleftarrow{R} Z_p$，于是有

$$\prod_{i=1}^n e(sP_1, A_i^*) e(saP_1, B_i^*) e(-s\tau P_1 + sW_1, D_i^*) = e(P_1, P_2)^{\alpha s} e(P_1, P_2)^{Ms} \cdot \prod_{i=1}^n \left(\frac{e(s(\text{id}_i Q_1 + \text{ctag}_i W_1 + U_1), D_i^*)}{e(sP_1, C_i^*)} \right)^{\frac{1}{\text{ctag}_i - \text{ktag}_i}} \tag{4}$$

在上述模拟过程中，如果 $c = 0$，则模拟器 $\mathcal{B}$ 与敌手 $\mathcal{A}$ 执行游戏 Game_{k-1}；否则，执行游戏 Game_k。如果敌手 $\mathcal{A}$ 在这 2 个游戏中获胜的概率有差异，则模拟器 $\mathcal{B}$ 利用这点差异就可以解决 DDH2v 问题。然而，如果敌手 $\mathcal{A}$ 的伪造由 type-N 转变为 type-S，$\mathcal{A}$ 在这 2 个游戏中获胜的概率有可能保持不变。因此，模拟器 $\mathcal{B}$ 不得不检测 $\mathcal{A}$ 输出的伪造是否仍然是 type-N。为此，$\mathcal{B}$ 随机选取 $s' \xleftarrow{R} Z_p$，对于每一个 $i \in [n]$，设置 $\text{ctag}_i = \mu \text{id}_i + \xi$，并计算

$$T_1 = s'P_1 + zx_1 P_1$$
$$T_2 = as'P_1 + a(zx_1 P_1) + dzP_1$$
$$T_3 = -\tau s'P_1 + s'W_1 - ay'_v(zx_1 P_1) + y_w(zx_1 P_1) - y'_v(dzP_1)$$
$$T_{4,i} = s'(\text{id}_i Q_1 + \text{ctag}_i W_1 + U_1) + (y_q \text{id}_i + \text{ctag}_i y_w + y_u)(zx_1 P_1)$$

这里隐式地设置 $s = s' + zx_1$。然后 $\mathcal{B}$ 验证式(5)是否成立。

$$\prod_{i=1}^n e(T_1, A_i^*) e(T_2, B_i^*) e(T_3, D_i^*) = e(P_1, P_2)^{\alpha s'} e(zx_1 P_1, P_2) e(P_1, P_2)^{Ms'} \cdot \prod_{i=1}^n \left(\frac{e(T_{4,i}, D_i^*)}{e(T_1, C_i^*)} \right)^{\frac{1}{\text{ctag}_i - \text{ktag}_i}} \tag{5}$$

如果伪造为 type-N，则式(5)成立；否则，式(5)不成立，因为会产生额外的一项 $e(P_1, P_2)^{dz\gamma}$。

因此，如果敌手 $\mathcal{A}$ 能够区分 Game_{k-1} 和 Game_k，模拟器 $\mathcal{B}$ 就能利用敌手 $\mathcal{A}$ 的能力攻破 DDH2v 假设。

最后，本文证明如果敌手 $\mathcal{A}$ 在游戏 Game_L 中输出一个 type-N 的伪造，模拟器 $\mathcal{B}$ 就能利用敌手 $\mathcal{A}$ 的能力攻破 DBDH 假设。

系统建立　给定 $(P_1, xP_1, aP_1, sP_1, P_2, xP_2, aP_2, sP_2, Z_3)$，模拟器 $\mathcal{B}$ 的目的是判定 Z_3 是否等于 $e(P_1, P_2)^{xas}$。为此，模拟器 $\mathcal{B}$ 随机选取 $a, y_v, y'_v, y_q, y_u, y_w \xleftarrow{R} Z_q$ 和 2 个哈希函数 H_0, H_1，设置参数 $V_2 = y_v P_2$，$V_2' = y'_v P_2$，$Q_1 = y_q P_1$，$W_1 = y_w P_1$，$U_1 = y_u P_1$，$Q_2 = y_q P_2$，$W_2 = y_w P_2$，$U_2 = y_u P_2$，$\tau P_1 = y_v P_1 + y'_v(aP)$，$e(P_1, P_2)^\alpha = e(xP_1, aP_2)$，这里隐式地令 $\alpha = xa$，$\tau = y_v + ay'_v$。然后，$\mathcal{B}$ 发送公开参数给 $\mathcal{A}$。

密钥提取询问　为了回答身份 ID 的密钥提取询问，模拟器 $\mathcal{B}$ 首先随机选取 $\gamma', r, \text{ktag}_{\text{ID}} \xleftarrow{R} Z_p$，一定存在 $\gamma \xleftarrow{R} Z_p$，隐式地有 $\gamma' = x - \gamma$；然后 $\mathcal{B}$ 计算身份 ID 的半功能密钥如下。

$$A_{\text{ID}} = \gamma'(aP_2) + rV_2 = (x - \gamma)(aP_2) + rV_2 = xaP_2 + rV_2 - a\gamma P_2 = \alpha P_2 + rV_2 - a\gamma P_2$$
$$B_{\text{ID}} = rV_2' - \gamma' P_2 + xP_2 = rV_2' - (x - \gamma)P_2 + xP_2 = rV_2' + \gamma P_2$$
$$C_{\text{ID}} = r(\text{id} Q_2 + \text{ktag}_{\text{ID}} W_2 + U_2)$$
$$D_{\text{ID}} = rP_2$$

这里需要注意的是，由于 $\mathcal{B}$ 并不知道 α，因此仅能生成半功能密钥给 $\mathcal{A}$。

签名询问 为了回答签名询问，模拟器 $\mathcal{B}$ 首先利用米主要生成签名者 ID_π 的一个半功能密钥 $\mathrm{SK}_{\mathrm{ID}_\pi}=(A_{\mathrm{ID}_\pi},B_{\mathrm{ID}_\pi},C_{\mathrm{ID}_\pi},D_{\mathrm{ID}_\pi})$，选取满足 $\sum_{i=1}^{n}\lambda_i=0$ 和 $\sum_{i=1}^{n}r_i=\bar{r}$ 限制的随机数 $\lambda_i,r_i,\mathrm{ktag}_i\xleftarrow{R}Z_p$，然后回答签名询问如下。

对于 $i\in[n]$，有以下结论成立。

当 $i\neq\pi$ 时，有

$$A_i=\lambda_iP_2+r_iV_2$$

$$B_i=r_iV_2'$$

$$C_i=r_i(\mathrm{id}_iQ_2+\mathrm{ktag}_iW_2+U_2)$$

$$D_i=r_iP_2$$

当 $i=\pi$ 时，有

$$A_\pi=\lambda_\pi P_2+MP_2+r_\pi V_2+A_{\mathrm{ID}_\pi}=$$
$$\alpha P_2+\lambda_\pi P_2+MP_2+(r_\pi+r)V_2-a\gamma P_2$$

$$B_\pi=r_\pi V_2'+B_{\mathrm{ID}_\pi}=(r_\pi+r)V_2'+\gamma P_2$$

$$C_\pi=r_\pi(\mathrm{id}_\pi Q_2+\mathrm{ktag}_\pi W_2+U_2)+C_{\mathrm{ID}_\pi}=$$
$$(r_\pi+r)(\mathrm{id}_\pi Q_2+\mathrm{ktag}_\pi W_2+U_2)$$

$$D_\pi=r_\pi P_2+D_{\mathrm{ID}_\pi}=(r_\pi+r)P_2$$

最终得到一个 type-S 的签名。

伪造 当敌手 $\mathcal{A}$ 输出一个关于环 Ring 和消息 m 的伪造环签名 $\sigma^*=\{A_i^*,B_i^*,C_i^*,D_i^*,\mathrm{ktag}_i^*\}_{i=1}^n$ 后，模拟器 $\mathcal{B}$ 首先计算 $M=H_1(m,\mathrm{Ring})$，$\mathrm{id}_i=H_0(\mathrm{ID}_i)$（$i\in[n]$），对于任意的 $s',\mathrm{ctag}_1,\cdots,\mathrm{ctag}_n\xleftarrow{R}Z_p$（$\mathrm{ctag}_i\neq\mathrm{ktag}_i,i\in[n]$），有

$$\prod_{i=1}^{n+1}e(s'P_1,A_i^*)e(s'aP_1,B_i^*)e(-s'\tau P_1+s'W_1,D_i^*)=$$
$$e(P_1,P_2)^{\alpha s'}e(P_1,P_2)^{Ms'}\cdot$$
$$\prod_{i=1}^{n+1}\left(\frac{e(s'(\mathrm{id}_iQ_1+\mathrm{ctag}_iW_1+U_1),D_i^*)}{e(s'P_1,C_i^*)}\right)^{\frac{1}{\mathrm{ctag}_i-\mathrm{ktag}_i}}\tag{6}$$

接着，$\mathcal{B}$ 随机生成 $\delta',t,\mathrm{ctag}_1,\cdots,\mathrm{ctag}_n\xleftarrow{R}Z_p$（$\mathrm{ctag}_i\neq\mathrm{ktag}_i,i\in[n]$），并计算

$$e(P_1,P_2)^{\alpha s}=\frac{\prod_{i=1}^{n}e(sP_1,A_i^*)e(\delta'P_1,B_i^*)e(-y_v(sP_1)-\delta'y_v'P_1+y_w(sP_1),D_i^*)}{\prod_{i=1}^{n}\left(\frac{e((y_q\mathrm{id}_i+y_w\mathrm{ctag}_i+y_u)(sP_1),D_i^*)}{e(sP_1,C_i^*)}\right)^{\frac{1}{\mathrm{ctag}_i-\mathrm{ktag}_i}}e(sP_1,P_2)^M}\tag{7}$$

这里，模拟器 $\mathcal{B}$ 隐式地设置 $\delta'=\delta+as$，其中 $\delta\xleftarrow{R}Z_p$。然后 $\mathcal{B}$ 通过检验 $e(P_1,P_2)^{\alpha s}=Z_3$ 是否成立攻破 DBDH 假设。

定理 2 匿名性。3.1 节给出的环签名方案是无条件匿名的。

证明 签名 $\sigma=\{A_i,B_i,C_i,D_i,\mathrm{ktag}_i\}_{i=1}^n$ 中，由于 $\{\lambda_i,r_i,\mathrm{ktag}_i\}_{i=1}^n$ 是由真实签名者随机生成的，因此 $\{A_i,B_i,C_i,D_i,\mathrm{ktag}_i\}(i\in[n]\setminus\{\pi\})$ 是均匀分布的。另一方面，由于 αP_2 是主密钥，r 和 ktag_π 是由 PKG 随机生成的，与真实签名者无关，因此 $\{A_\pi,B_\pi,C_\pi,D_\pi,\mathrm{ktag}_\pi\}$ 也是均匀分布的。因此，整个签名过程中，有关真实签名者的信息没有被泄露。敌手想要通过签名 $\sigma=\{A_i,B_i,C_i,D_i,\mathrm{ktag}_i\}_{i=1}^n$ 确定真实签名者身份的概率不会优于从环 $\mathrm{Ring}=\{\mathrm{ID}_1,\cdots,\mathrm{ID}_n\}$ 中随机猜测真实签名者身份的概率。故 3.1 节给出的环签名方案是无条件匿名的。

5 性能比较

本节将本文方案与已有的基于对偶系统的身份基环签名方案[22-23]进行性能比较。

为了比较方案在各个阶段的运行效率，本文使用 Java 语言编程实现 3 个方案，通过调用 JPBC 密码库实现相关的密码运算，基于 PC 端开发，主要运行环境如下。中央处理器：AMD Ryzen 7-4800H；内存：16 GB；硬盘：240 GB；操作系统：Windows 10 专业版。

图 1~图 4 是本文方案与文献[22-23]中各算法运行时间的对比曲线。由图 1~图 4 可以看出，由于本文方案在素数阶群上构造，因此在效率方面具有很大优势。

表 1 列出了当环大小为 $n=150$ 时 3 个方案中各个算法的操作时间，相较于文献[22-23]方案，本文方案中各算法运行时间更短，这主要是因为文献[22-23]方案是基于合数阶群上的对称对构造的，而本文方案是基于素数阶群上的非对称对构造的。对运算是

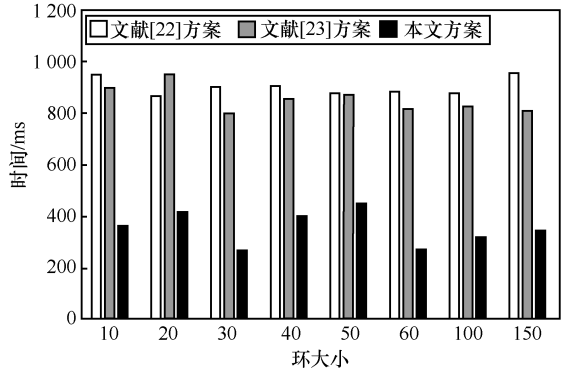

图 1　各方案 Setup 算法的性能比较

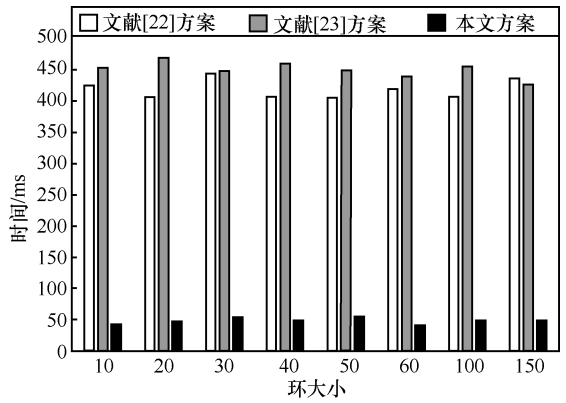

图 2　各方案 Extract 算法的性能比较

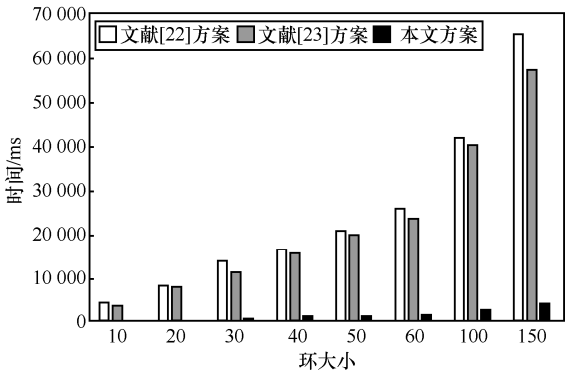

图 3　各方案 Sign 算法的性能比较

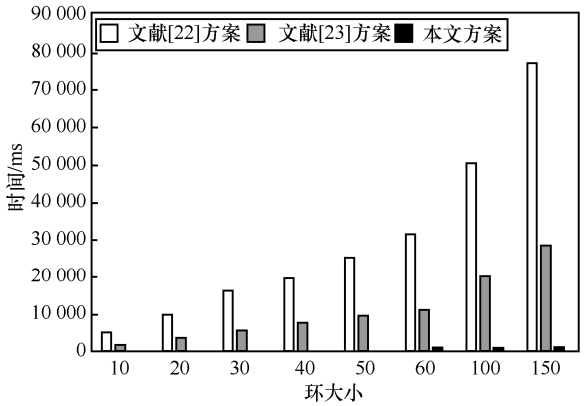

图 4　各方案 Verify 算法的性能比较

各个算法中最耗时的运算，而合数阶群上的对运算要比素数阶群上的对运算慢许多。相比于对称对，非对称对在实现时也更快更紧致。

表 1　环大小为 $n=150$ 时的计算效率比较

方案	Setup/ms	Extract/ms	Sign/ms	Verify/ms
文献[22]方案	960	438	65 816	77 238
文献[23]方案	814	428	57 687	28 894
本文方案	350	51	4 683	1 531

6　结束语

环签名中，环中任意成员都能以一种完全匿名的方式对消息进行签名。这一性质被称为环签名的无条件匿名性，可用于保护签名者的隐私。因在隐私保护等方面的重要应用，身份基环签名已成为一个热门的研究方向。然而，大多数已有的身份基环签名方案的安全性证明不是基于随机预言机模型就是使用了公共参考串模型。本文提出了一个基于素数阶群上非对称对的身份基环签名方案。基于对偶系统加密技术，该方案被证明在标准模型下是不可伪造和无条件匿名的。与文献[22-23]方案相比，本文方案更高效。然而，本文方案中签名大小仍然会随着环成员个数的增长而呈线性增长。因此，在素数阶群上基于对偶系统加密技术构造标准模型下，可证明安全的具有常量大小的身份基环签名方案是笔者今后研究的主要方向。

参考文献：

[1] RIVEST R L, SHAMIR A, TAUMAN Y. How to leak a secret[C]//Proceedings of the 7th International Conference on the Theory and Application of Cryptology and Information Security. Berlin: Springer, 2001: 552-565.

[2] SHAMIR A. Identity-based cryptosystems and signature schemes[C]//International Cryptology Conference. Berlin: Springer, 1984: 47-53.

[3] CHOW S S M, LIU J K, WONG D S. Robust receipt-free election system with ballot secrecy and verifiability[C]//Proceedings of Network and Distributed System Security Symposium. Piscataway: IEEE Press, 2008: 81-94.

[4] TSANG P P, WEI V K. Short linkable ring signatures for E-voting, E-cash and attestation[C]//Proceedings of the 1th Information on Security Practice and Experience. Berlin: Springer, 2005: 48-60.

[5] QIU C, ZHANG S B, CHANG Y, et al. Electronic voting scheme based on a quantum ring signature[J]. International Journal of Theoretical Physics, 2021, 60(4): 1550-1555.

[6] 李旭东, 牛玉坤, 魏凌波, 等. 比特币隐私保护综述[J]. 密码学报, 2019, 6(2): 133-149.
LI X D, NIU Y K, WEI L B, et al. Overview on privacy protection in bitcoin[J]. Journal of Cryptologic Research, 2019, 6(2): 133-149.

[7] 陈思吉, 翟社平, 汪一景. 一种基于环签名的区块链隐私保护算法[J]. 西安电子科技大学学报, 2020, 47(5): 86-93.
CHEN S J, ZHAI S P, WANG Y J. Blockchain privacy protection algorithm based on ring signature[J]. Journal of Xidian University, 2020, 47(5): 86-93.

[8] 宋婷婷. 车联网环境下环签名方案的研究[D]. 兰州: 西北师范大学, 2020.
SONG T T. Research on ring signature scheme in the environment of Internet of vehicles[D]. Lanzhou: Northwest Normal University, 2020.

[9] ZHANG F G, KIM K. ID-based blind signature and ring signature from pairings[C]//Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security. Berlin: Springer, 2002: 533-547.

[10] CHOW S S M, HUI L C K, YIU S M. Identity based threshold ring signature[C]//Proceedings of the 7th International Conference on Information Security & Cryptology. Berlin: Springer, 2004: 218-232.

[11] CHOW S S M, YIU S M, HUI L C K. Efficient identity based ring signature[C]//Proceedings of the Third international conference on Applied Cryptography and Network Security. Berlin: Springer, 2005: 499-512.

[12] CHEN Y Q, SUSILO W, MU Y. Identity-based anonymous designated ring signatures[C]//Proceeding of the 2006 International Conference on Communications and Mobile Computing. New York: ACM Press, 2006: 189-194.

[13] ZHOU C, CUI Z, GAO G. Efficient identity-based generalized ring signcryption scheme[J]. KSII Transactions on Internet and Information Systems, 2016, 10(12): 6116-6134.

[14] 邓伦治, 高岩, 高荣海, 等. 一个高效的基于身份的环签名方案[J]. 贵州师范大学学报(自然科学版), 2021, 39(1): 1-8.
DENG L Z, GAO Y, GAO R H, et al. An efficient identity-based ring signature scheme[J]. Journal of Guizhou Normal University (Natural Sciences), 2021, 39(1): 1-8.

[15] 贾小英, 何德彪, 许芷岩, 等. 格上高效的基于身份的环签名体制[J]. 密码学报, 2017, 4(4): 392-404.
JIA X Y, HE D B, XU Z Y, et al. An efficient identity-based ring signature scheme over a lattice[J]. Journal of Cryptologic Research, 2017, 4(4): 392-404.

[16] 赵艳红, 陈晓玲. 基于身份及 RSA 的简短代理环签名方法[J]. 沈阳大学学报(自然科学版), 2018, 30(4): 302-310.
ZHAO Y H, CHEN X L. A short proxy ring signature scheme based on identity and RSA[J]. Journal of Shenyang University (Natural Science), 2018, 30(4): 302-310.

[17] CANETTI R, GOLDREICH O, HALEVI S. The random oracle methodology, revisited[J]. Journal of the ACM, 2004, 51(4): 557-594.

[18] AU M H, LIU J K, YUEN T H, et al. ID-based ring signature scheme secure in the standard model[C]//Advances in Information and Computer Security. Berlin: Springer, 2006: 1-16.

[19] 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 Y Y, LI H, WANG Y M. Identity-based ring signature scheme under standard model[J]. Journal on Communications, 2008, 29(4): 40-44.

[20] 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 Z H, HU Y P, MU N B, et al. New identity-based ring signature in the standard model[J]. Journal of Electronics & Information Technology, 2009, 31(7): 1727-1731.

[21] 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 A J, MA C G, ZHANG Z F, 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.

[22] AU M H, LIU J K, SUSILO W, et al. 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.

[23] 赵艳琦, 来齐齐, 禹勇, 等. 标准模型下基于身份的环签名方案[J]. 电子学报, 2018, 46(4): 1019-1024.
ZHAO Y Q, LAI Q Q, YU Y, et al. ID-based ring signature in the standard model[J]. Acta Electronica Sinica, 2018, 46(4): 1019-1024.

[24] FREEMAN D M. Converting pairing-based cryptosystems from composite-order groups to prime-order groups[C]//Proceedings of the 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2010: 44-61.

[25] RAMANNA S C, CHATTERJEE S, SARKAR P. Variants of waters' dual system primitives using asymmetric pairings[C]//Proceedings of the 15th International Conference on Practice and Theory in Public Key Cryptography. Berlin: Springer, 2012: 298-315.

[26] WATERS B. Dual system encryption: realizing fully secure IBE and HIBE under simple assumptions[C]//Proceedings of the 29th Annual International Cryptology Conference. Berlin: Springer, 2009: 619-636.

[27] CHATTERJEE S, MENEZES A. On cryptographic protocols employing asymmetric pairings—The role of Ψ revisited[J]. Discrete Applied Mathematics, 2011, 159(13): 1311-1322.

[28] GALBRAITH S D, PATERSON K G, SMART N P. Pairings for cryptographers[J]. Discrete Applied Mathematics, 2008, 156(16): 3113-3121.

[29] SMART N P, VERCAUTEREN F. On computable isomorphisms in efficient asymmetric pairing-based systems[J]. Discrete Applied Mathematics, 2007, 155(4): 538-547.

[作者简介]

侯红霞（1980− ），女，山西朔州人，博士，西安邮电大学副教授，主要研究方向为应用密码学。

张明瑞（1996− ），男，陕西西安人，陕西师范大学硕士生，主要研究方向为密码学与信息安全。

赵艳琦（1992− ），男，吉林双辽人，博士，西安邮电大学副教授，主要研究方向为密码学与区块链安全。

董晓丽（1982− ），女，山西阳曲人，博士，西安邮电大学讲师，主要研究方向为信息安全和密码学。