紧安全的环签名构造

邱 添[1,2], 唐国锋[3], 林东岱[1,2]

[1] 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 中国 100093
[2] 中国科学院大学网络空间安全学院 北京 中国 100049
[3] 中国科学院软件研究所可信计算与信息保障实验室 北京 中国 100190

摘要 对于一个密码方案而言, 如何在安全证明中降低归约损失、实现紧归约是一个重要的问题。因为一般来说归约损失越大, 就需要更大的参数来保证方案的理论安全强度, 而在部署一个紧安全的密码方案的时候, 则不需要牺牲效率来弥补归约损失。在这篇文章中, 我们关注紧安全的环签名构造。环签名在 2001 年由 Rivest 等人首次提出, 它允许用户在隐藏自己身份的同时进行签名, 任何人都不能破坏环签名的匿名性, 同时敌手不能冒充任意一个环成员生成相应的有效签名。虽然目前已有多种环签名的构造方案, 但证明过程中的归约损失是高效实现的一大阻碍。

在本文中, 我们基于 DDH 假设在随机预言机模型下提出了一种环签名方案, 其中安全证明的归约损失仅为常数, 因此称为紧安全的环签名构造。在构造中, 我们令每个用户的公钥由两个子公钥构成, 用户私钥为其中一个子公钥对应的子私钥, 再基于 Goh 与 Jarecki 提出的紧安全的 EDL 签名方案, 我们利用标准的 CDS 变换构造了一个 1/N-DDH 非交互零知识证明系统, 从而证明用户拥有有效的私钥, 得到相应的环签名方案。得益于这种特殊的构造, 在安全证明中我们不必使用分叉引理, 也不必猜测敌手的目标公钥, 从而实现了紧安全归约。此外, 我们的方案可以用来构造附加其他性质的环签名方案, 如可链接环签名, 同时对于其他匿名签名方案的紧安全设计也具有启发意义。

关键词 环签名; 可证明安全; 紧安全归约; DDH 假设
中图法分类号 TP309.7 DOI 号 10.19363/J.cnki.cn10-1380/tn.2022.05.03

Tightly-secure Ring Signature Construction

QIU Tian[1,2], TANG Guofeng[3], LIN Dongdai[1,2]

[1] State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
[2] School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China
[3] Trusted Computing and Information Assurance Laboratory, Institute of Software Chinese Academy of Sciences, Beijing 100190, China

Abstract In real-world cryptography, reducing security loss and achieving tight security are increasingly gaining importance, as larger reduction loss must be compensated by larger parameters if we want to choose these parameters in a theoretically-sound way. However, when we implement a tightly-secure cryptographic scheme, there is no need to sacrifice efficiency. In this paper, we focus on the constructions of tightly-secure ring signature. Ring signature was introduced by Rivest et. al. in 2001. It allows users to sign messages anonymously. Nobody could break this anonymity and the adversary cannot forge a valid ring signature. Although there are many ring signature constructions, their reduction loss hinders efficient implementations.

In this paper, we propose a tightly-secure ring signature scheme in the random oracle model based on the DDH assumption and the reduction loss is just a constant factor in the security proof. In our construction, user's public key consists of two base public keys and the secret key consists of a random secret key for one of two base public keys. Then we design a 1/N-DDH non-interactive zero-knowledge proof system by applying standard CDS transformation (CRYPTO'94) on the tightly secure EDL signature scheme proposed by Goh and Jarecki (EUROCRPYPT'03). Using this proof system, users prove the ownership of one of N secret keys and we obtain a ring signature scheme. Due to this special construction, we do not use forking lemma and do not need to guess adversary's targeted public key, thus we achieve tight security. In addition, our scheme can be used to construct other ring signature schemes with additional properties such as linkable ring signature, and it is an important inspiration to design other privacy-preserving signature schemes.

Key words ring signature; provable secure; tight secure reduction; Decisional Diffie-Hellman(DDH) assumption

通讯作者: 邱添, 硕士, Email: qiutian@iie.ac.cn。
本课题得到国家自然科学基金 (No. 61872359, No. 61936008)资助。
收稿日期: 2019-10-16; 修改日期: 2020-02-24; 定稿日期: 2022-03-15

1 引言

1976 年, Diffie 与 Hellman 发表了文章《密码学的新方向》[1], 标志着公钥密码学的建立。此后众多公钥密码算法相继被提出, 并应用到人们的日常生活当中, 如密钥交换算法、公钥加密算法、数字签名算法等等。

评价一个公钥密码算法主要从以下三点出发: 效率, 密码学假设以及安全归约。前两点比较直观, 它要求密码方案的实现是高效的, 底层困难假设是标准的且已被广泛研究; 然而安全归约较为复杂, 因为它涉及具体的证明方法。一般来说, 在论证密码方案安全性的时候, 我们构造一个归约, 把破坏密码方案的有效敌手 $\mathcal{A}$ 转换为解决某个特定底层困难问题的挑战者 $\mathcal{B}$, 如大整数分解问题, 离散对数问题, 格上的最短整数解问题等等。在归约过程中, 如果 $\mathcal{B}$ 的运行时间和成功概率与敌手 $\mathcal{A}$ 的相近, 或者相差一个常数因子, 我们就称归约是紧的。通常归约构造的敌手 $\mathcal{B}$ 的运行时间与敌手 $\mathcal{A}$ 的相近 $t_{\mathcal{B}} \approx t_{\mathcal{A}}$, 但成功概率会有差距 $\varepsilon_{\mathcal{B}} \geqslant \varepsilon_{\mathcal{A}} / Q$。我们称 Q 为归约损失, 特别地, 只有当 Q 为某个常数时, 我们称归约是紧的。在实际应用中, 为了使密码方案在理论上达到特定的安全级别, 我们按照安全证明来选择参数。如果归约损失 Q 很大, 那么方案所需的安全参数就要越大, 相应地效率就会降低。为了使得密码方案有最优的参数选取, 我们需要安全证明是一个紧归约, 相应的密码方案为紧安全的密码方案。

然而紧归约的实现一般比较困难, 主要体现在两个方面, 一是证明方法, 比如基于离散对数假设的 Schnorr 签名[2], 它本质上是由一个 Σ-协议通过 Fiat-Shamir 变换[3]得到的, 在该方案的安全证明中, 挑战者通过重绕敌手得到针对于同一个承诺值的两次伪造, 从中提取出离散对数的解。由分叉引理[4]可知这个归约并不紧, 且损失因子与敌手询问随机预言机的次数有关。尽管有很多紧安全的基于离散对数的签名构造, 但它们或者损失了效率[5], 或者需要更强的假设[6-8]。另一方面是应用场景, 比如在多用户的场景中[9], 挑战者需要猜测敌手的目标用户公钥, 猜对了才能解决底层困难问题, 成功概率一般与用户的个数有关, 因此多用户场景也会引起归约损失。为了使密码方案在理论上达到特定的安全级别, 部署方案时就需要过大的安全参数, 因此降低效率。作为一类典型的多用户签名方案, 环签名就是这样一个例子。

1.1 相关工作

环签名(Ring Signature, RS)这一概念[10]由 Rivest、Shamir 和 Tauman 于 2001 年提出。一个环签名方案中可以有多个用户, 每个用户可以任意选取多个其他用户的公钥构成一个环, 在签名算法中签名者只需证明自己是环中的一个成员, 从而隐藏自己的身份, 匿名性保证验证者可以检查签名的有效性, 但不知道签名是由环中的哪一个成员所签。不可伪造性保证敌手不能冒充任意一个环成员伪造出一个有效的签名。目前已有众多环签名方案, 它们或者以提高效率为目的[11-16], 或者增加了新的功能[17-20]。除了 Rivest 等人的工作, Bender 等人[11]对环签名提出了严格的安全定义, 并在标准模型下给出了理论上的构造。

在效率提升方面, Shacham 等人[12]在标准模型中基于双线性群首次给出了高效的构造, 但签名尺寸仍与环规模(即环成员个数)呈线性关系。同年, Chandran 等人[13]在标准模型下给出了次线性的环签名方案, 即签名尺寸与环规模 n 成次线性关系 $O(\sqrt{n})$。在随机预言机模型下, Groth 等人[15]基于离散对数假设给出了对数签名尺寸的环签名构造。Libert 等人[16]也给出了基于格的对数尺寸环签名方案, 但以上两个环签名方案[17-18]都存在着很大的归约损失。

就功能性而言, 具有额外属性的环签名方案也相继被提出, 如可链接环签名[17], 基于身份的环签名[18-19], 唯一环签名[20]等等。

1.2 主要难点

在本文中, 我们考虑随机预言机模型下紧安全的环签名构造。事实上, 在环签名不可伪造性的证明中实现紧归约非常具有挑战性, 一般来讲, 它的归约损失主要受两个因素的影响: 敌手询问注册预言机的次数 q_j 和敌手询问随机预言机的次数 q_h。

具体地, 在定义的安全模型中, 假设敌手最多可以询问 q_j 次注册预言机, 得到 q_j 个用户公钥, 对于其中任意的某些公钥, 敌手可以询问对应的私钥, 也可以询问任意消息、任意环对应的环签名。最终, 如果敌手输出一个新的消息, 以及此消息对应的一个合法环签名, 并且敌手不知道环中每个用户的私钥, 那我们便认为敌手成功地破坏了环签名方案的不可伪造性。为了利用敌手的伪造能力, 挑战者需要在归约中猜测敌手的目标公钥, 并将底层困难问题的输入嵌入到这个公钥中, 这种证明方法自然会导

致一个损失因子 q_j。除此之外, 如果归约使用了重绕技术, 那么损失因子还与随机预言机的询问次数 q_h 有关。

1.3 主要贡献与技术

在本文中, 我们构造了一个紧安全的环签名方案, 归约损失仅为常数 2。受 Gjøsteen 和 Jager 的工作[21]的启发, 令每个用户的公钥包含两个子公钥 $pk=(pk^{(0)},pk^{(1)})$, 用户的私钥包含一个随机比特 $b\leftarrow_{\$}\{0,1\}$, 以及一个子私钥 $sk^{(b)}$, 对应于子公钥 $pk^{(0)}$ 或者 $pk^{(1)}$。挑战者知道每个用户的私钥, 可以为敌手模拟攻击环境, 但挑战者不知道 $sk^{(1-b)}$, 因此, 如果敌手的伪造目标是 $pk^{(1-b)}$, 我们便可以构造归约, 使挑战者能从关于 $pk^{(1-b)}$ 的伪造中提取出困难问题的解。

其次, 基于 Goh 与 Jarecki 提出的 EDL 签名方案[6], 我们利用标准的 CDS 变换[22]构造了一个 1/N-DDH 非交互零知识证明系统。我们把 CDH 问题的输入嵌入到公钥和哈希值中, 利用敌手的一次伪造, 挑战者便能得到 CDH 问题的解, 从而归约成功。利用 CDS 变换, 我们将这个 Σ-协议扩展成一个 1/N 版本。

基于我们的环签名构造, 还可以得出具有其他附加性质的环签名方案, 譬如可链接环签名[17]。此外, 我们的工作对于在匿名情境下设计紧安全的签名方案还具有启发意义, 如群签名[23]、可追踪签名[24]等。

在本文第二章节中我们介绍了与本方案有关的预备知识和相关概念; 在第三章中介绍了 1/N-DDH 零知识证明系统, 以此为底层协议, 我们在第四部分给出了环签名的具体方案并在随机预言机模型下证明其安全性, 证明过程中的归约损失仅为常数; 第五章总结本文并提出未来的研究方向。

2 预备知识

在本文中, 用 $\mathbb{N}$ 表示自然数集合, 对于非零自然数 $n\in\mathbb{N}$, 定义 $[n]=\{1,2,...,n\}$。用 $\mathbb{Z}$ 表示整数集合, $\mathbb{Z}_q$ 表示模 q 的整数集, 其中 q 为素数, 即 $\mathbb{Z}_q=\{0,1,...,q-1\}$。对于任意集合 A, 用 $s\leftarrow_{\$}A$ 表示从 A 中均匀随机抽取一个元素 s。

2.1 Diffie-Hellman 困难问题假设

定义 1.(Diffie-Hellman 集合.) 令 $\mathbb{G}$ 为一个 q 阶的循环群, q 为素数, g 为 $\mathbb{G}$ 的一个生成元。令 $\mathcal{DDH}$ 为 DDH 数组 $\{(g^a, g^b, g^{ab})|a, b\in\{0,1,\ldots,q-1\}\}$ 的集合。

定义 2.(判定 Diffie-Hellman 问题, DDH.) 对于概率多项式时间(Probabilistic Polynomial Time, PPT)的敌手, 给定两个数组(g^a, g^b, g^{ab})和(g^a, g^b, g^c), 令其判断其中哪一个是 DDH 数组。

定义 3.(计算 Diffie-Hellman 问题, CDH.) 对于概率多项式时间(Probabilistic Polynomial Time, PPT)的敌手, 给定数组(g, g^a, g^b), 令其计算 g^{ab}。

定义 4.(m-DDH 问题.) 令 $\mathcal{A}$ 是一个输出为 0 或 1 的算法, $\mathcal{A}$ 能够询问预言机, 输入为整数 $i\in[m]$, 预言机返回三个群元素。令 $\mathcal{O}_0$ 是一个这样的预言机, 返回随机选取的 DDH 数组, 而另一个 $\mathcal{O}_1$ 预言机返回的是随机选取的 3 个群元素。那么解决 m-DDH 问题的算法 $\mathcal{A}'$ 的优势为

$$\mathbf{Adv}_{\mathcal{A}'}^{\mathbf{m\text{-}DDH}}=\left|\Pr[\mathcal{A}^{\mathcal{O}_0}=0]-\Pr[\mathcal{A}^{\mathcal{O}_1}=0]\right|.$$

定理 1.(m-DDH 问题.) 令 $\mathcal{A}'$ 是解决 m-DDH 问题的算法, 那么存在解决 DDH 问题的算法 $\mathcal{B}$ 满足:

$$\mathbf{Adv}_{\mathcal{A}'}^{\mathbf{m\text{-}DDH}}\leqslant\mathbf{Adv}_{\mathcal{B}}^{\mathbf{DDH}}+\frac{1}{q}.$$

定理 1 的证明可参见文献[9]。

2.2 Σ-协议

定义 5.(Σ-协议.) Σ-协议是一种特殊的三轮交互证明协议, 证明者先公开一则断言 x, 发送初始消息 a 给验证者, 验证者返回一条随机挑战 e, 证明者再对这个挑战进行回应 r, 最后验证者根据交互过程产生的副本(x, a, e, r)来决定接受或者拒绝证明者的断言。作为一类特殊的交互证明系统, 除了完美完备性和合理性之外, Σ-协议还具有以下特殊性质:

(1) 特殊合理性: 对于任意断言 x 和关于 x 的一对可接受副本(a, e, r)和(a, e', r'), 只要 $e\neq e'$, 验证者就能计算出与 x 对应的证据 w。

(2) 特殊诚实验证者零知识性: 对于断言 x, 给定一个随机挑战 e, 就一定存在一个 PPT 模拟器 $\mathcal{S}$, 尽管没有证据 w, 但它仍然能够输出一个可接受的副本 (a, e, r), 并且此副本与真实交互产生的副本是不可区分的。

下面我们给出一个 DDH 问题的 Σ-协议的例子。其中 $\mathbb{G}$ 为一个 q 阶的循环群, q 为素数, g 为 $\mathbb{G}$ 的一个生成元。令 $y,h,z\in\mathbb{G}$ 满足 $y=g^x$ 并且 $z=h^x$, 基于 DDH 假设可以构造证明 $\log_g y=\log_h z$ 的 Σ-协议, 如图 1 所示。

此协议具有特殊诚实验证者零知识性, 即存在模拟器 $\mathcal{S}$ 以公共输入 (y,h,z) 以及挑战值 c 为输入, 可以产生一个可接受的交互副本 (u,v,c,s), 且它与诚实证明者和诚实验证者之间的真实交互所产生的

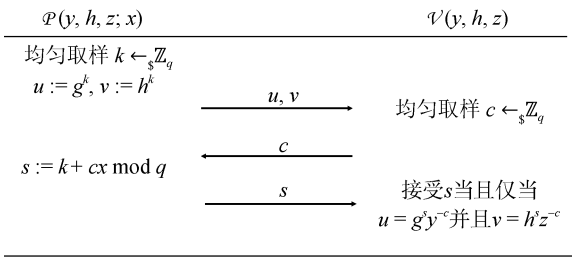

图 1 DDH 问题的 Σ-协议

Figure1 Σ-protocol of DDH problem

副本是完美不可区分的, 此算法记为 $\mathrm{ZSim}_1(y,h,z;c)$: 模拟器均匀随机选择 $s \leftarrow_{\$} \mathbb{Z}_q$, 计算 $u = g^s y^{-c}$ 以及 $v = h^s z^{-c}$, 输出 (u,v,c,s)。

利用标准的 Fiat-Shamir 变换, 我们可以将上述 Σ-协议转换成一个非交互的零知识证明系统, 此时证明者只需利用随机预言机 $\mathcal{H}$ 自己产生挑战值 $c = \mathcal{H}(u,v)$。

2.3 环签名

一个环签名方案由以下 4 个算法构成(初始化, 密钥生成, 签名, 验证):

初始化 Setup(1^κ): 以安全参数 1^κ 为输入, 输出公共参数 pp, 假设这个公共参数是以下算法的默认输入。

密钥生成 KeyGen(pp): 以公共参数 pp 为输入, 输出私钥 sk 和公钥 pk。

签名 Sign(M,R,sk): 以私钥 sk, 签名消息 M 和一个公钥集合 R 为输入, 输出环签名 σ。

验证 Vrfy(M,R,σ): 以公钥集合 R, 消息签名对 (M,σ) 为输入, 输出 1 或 0 分别代表验证通过或不通过。

正确性: 对于安全参数 1^κ, $\{pk_i, sk_i\}_{i\in[N]}$ 是由密钥生成算法产生的公私钥对集合, 如果对于任何 $\pi \in [n]$ 和消息 M 满足 $\mathbf{Vrfy}(R, M, \mathbf{Sign}(sk_\pi, M, R)) = 1$, $R = \{pk_i\}_{i\in[n]}$, 我们就称这个环签名方案是正确的。

我们用以下三个预言机来刻画敌手能力:

注册预言机 $pk \leftarrow \mathcal{JO}$: $\mathcal{JO}$ 生成一个新成员的公钥并返回公钥 pk;

私钥预言机 $sk \leftarrow \mathcal{CO}(pk)$: 输入 $\mathcal{JO}$ 产生的公钥 pk, $\mathcal{CO}$ 输出相应的私钥 sk;

签名预言机 $\sigma \leftarrow \mathcal{SO}(R, M, pk_\pi)$: 输入公钥集合 R, 消息 M 和签名者的公钥 $pk_\pi \in R$, 此预言机返回一个关于 M 和 R 有效的签名 σ。

匿名性: 我们通过以下敌手 $\mathcal{A}$ 与挑战者 $\mathcal{CH}$ 的游戏来描述这一性质:

(1) 初始化阶段: $\mathcal{CH}$ 运行初始化算法, 并将公共参数发送给 $\mathcal{A}$;

(2) 询问阶段: $\mathcal{A}$ 被允许自适应性地询问注册预言机 $\mathcal{JO}$, 私钥预言机 $\mathcal{CO}$, 签名预言机 $\mathcal{SO}$;

(3) 挑战阶段: $\mathcal{A}$ 选出一个公钥集合 R, 两个身份 $i_0, i_1 \in [n]$ 和消息 M 并发送给 $\mathcal{CH}$, 要求 $\mathcal{A}$ 没有询问过 i_0, i_1 的私钥。$\mathcal{CH}$ 从 i_0, i_1 中选出 i_b 并运行签名算法, 将签名发给 $\mathcal{A}$;

(4) 输出阶段: $\mathcal{A}$ 输出一个猜测 b'。

如果 $b' = b$, 则 $\mathcal{A}$ 胜利, 我们定义 $\mathcal{A}$ 的优势为 $\mathbf{Adv}_{\mathcal{A}}^{\mathrm{anon}} = \left|\Pr[b' = b] - 1/2\right|$

定义 6.(匿名性.) 对于任意无限计算能力的敌手 $\mathcal{A}$, 如果 $\mathcal{A}$ 在匿名性游戏中的优势 $\mathbf{Adv}_{\mathcal{A}}^{\mathrm{anon}}$ 关于安全参数是可忽略的, 那么就称环签名方案满足无条件匿名性。

不可伪造性: 敌手 $\mathcal{A}$ 与挑战者 $\mathcal{CH}$ 的不可伪造性游戏定义如下:

(1) 初始化阶段: $\mathcal{CH}$ 运行初始化算法, 并将公共参数发送给 $\mathcal{A}$;

(2) 询问阶段: $\mathcal{A}$ 被允许适应性地询问注册预言机 $\mathcal{JO}$, 私钥预言机 $\mathcal{CO}$ 和签名预言机 $\mathcal{SO}$;

(3) 输出阶段: $\mathcal{A}$ 输出一个伪造 $\left(M^*, \sigma^*, R^*\right)$。

如果这个伪造能够通过验证算法的验证, R^* 中的公钥都是 $\mathcal{JO}$ 预言机的输出, 而且 R^* 中的公钥都未作为 $\mathcal{CO}$ 的输入, 敌手也从未就 $\left(M^*, R^*\right)$ 询问过 $\mathcal{SO}$, 则称 $\mathcal{A}$ 伪造成功, 其成功的概率即为不可伪造性的优势, 记为 $\mathbf{Adv}_{\mathcal{A}}^{\mathrm{uf}}$。

定义 7.(不可伪造性.) 对于 PPT 的敌手 $\mathcal{A}$, 如果 $\mathcal{A}$ 在的优势 $\mathbf{Adv}_{\mathcal{A}}^{\mathrm{uf}}$ 关于安全参数是可忽略的, 那么就称环签名方案满足不可伪造性。

3 1/N -DDH 零知识证明

基于 DDH 问题的 Σ-协议, 我们可以利用标准的 CDS 变换构造一个 1/N-DDH 非交互零知识证明系统 $\mathsf{ZP}_{1/N}$, 用来证明 N 组 $\{y_i, h_i, z_i\}_{i\in[N]}$ 中至少有一组 $l \in [N]$ 满足等式 $\log_g y_l = \log_{h_l} z_l$。证明者拥有证据 (l, x_l), 我们把证明者产生此类非交互证明 $\Pi_{1/N}$ 的算法记作 $\mathbf{ZPrv}_{1/N}(\{y_i, h_i, z_i\}_{i\in[N]}; l, x_l)$, 验证者验证 $\Pi_{1/N}$ 的算法记为 $\mathbf{ZVfy}_{1/N}(\{y_i, h_i, z_i\}_{i\in[N]}; \Pi_{1/N})$。

生成证明的 $\mathrm{ZPrv}_{1/N}(\{y_i,h_i,z_i\}_{i\in[N]};l,x_l)$ 算法按以下步骤进行:

1. 承诺: 对于任意的 $i\in[N]$, 且 $i\neq l$, 证明者均匀随机选择 $c_i\leftarrow_{\$}\mathbb{Z}_q$, 调用模拟算法 $\mathbf{ZSim}_1(y_i,h_i,z_i;c_i)$, 模拟器均匀随机选择 $s_i\leftarrow_{\$}\mathbb{Z}_q$, 计算 $u_i=g^{s_i}y^{-c_i}$ 以及 $v_i=h_i^{s_i}z_i^{-c_i}$,输出 (u_i,v_i,c_i,s_i). 对于 $i=l$, 证明者均匀随机选择 $k_l\leftarrow_{\$}\mathbb{Z}_q$, 计算 $u_l=g^{k_l}$ 以及 $v_l=h_l^{k_l}$, 因此承诺阶段的所有承诺值为 $\{u_i,v_i\}_{i\in[N]}$;

2. 挑战: 证明者计算挑战值 $c=\mathcal{H}(\{u_i,v_i\}_{i\in[N]})$;

3. 响应: 证明者计算 $c_l=c-\sum_{i\in[N]\setminus\{l\}}c_i \bmod q$, $s_l=k_l+c_lx_l \bmod q$, 得到响应值为 $\{c_i,s_i\}_{i\in[N]}$, 证明者发送证明 $\Pi_{1/N}=\{c_i,s_i\}_{i\in[N]}$ 给验证者。

对于证明 $\Pi_{1/N}$, 验证者运行算法 $\mathbf{ZVfy}_{1/N}(\{y_i,h_i,z_i\}_{i\in[N]};\Pi_{1/N})$: 验证者接受 $\Pi_{1/N}$ 并输出 1 当且仅当 $\mathcal{H}\left(\{u_i,v_i\}_{i\in[N]}\right)=\Sigma_{i\in[N]}c_i$, 其中对于所有 $i\in[N]$, $u_i=g^{s_i}y_i^{-c_i}$, $v_i=h_i^{s_i}z_i^{-c_i}$。否则, 输出 0。

在随机预言机模型下, 证明系统 $\mathbf{ZP}_{1/N}$ 具有完美完备性, 合理性, 特殊诚实验证者零知识性, 以及证据不可区分性。这些性质的定义已在第 2.2 节中给出, 我们接下来将分别进行证明。

完美完备性: 对于 $i\neq l$, 模拟算法 ZSim_1 中证明者计算 $u_i=g^{s_i}y_i^{-c_i}$, $v_i=h_i^{s_i}z_i^{-c_i}$。对于 $i=l$, 证明者计算 $u_l=g^{k_l}$ 以及 $v_l=h_l^{k_l}$, 并且 k_l 在响应阶段满足 $k_l=s_l-c_lx_l$, 即满足 $u_l=g^{s_l}y_l^{-c_l}$, $v_l=h_l^{s_l}z_l^{-c_l}$, 其中证明者求得 $c_l=\mathcal{H}(\{u_i,v_i\}_{i\in[N]})-\Sigma_{i\in[N]\setminus\{l\}}c_i \mod q$, 因此诚实证明者产生的证明 $\Pi_{1/N}=\{c_i,s_i\}_{i\in[N]}$ 一定满足 $\mathcal{H}(\{g^{s_i}y_i^{-c_i},h_i^{s_i}z_i^{-c_i}\}_{i\in[N]})=\Sigma_{i\in[N]}c_i$, 一定会被验证者接受。

合理性: 如果对于任意的 $i\in[N]$, $x_i=\log_g y_i$ 与 $x_i'=\log_{h_i} z_i$ 不相等, 那么证明者 $\mathcal{P}^*$ 可以设置每个承诺值 $u_i=g^{k_i}$, $v_i=h_i^{k_i'}$, 产生的证明 $\Pi_{1/N}^*=\{c_i^*,s_i^*\}_{i\in[N]}$ 可以通过验证, 需要满足 $s_i^*=k_i+c_i^*x_i=k_i'+c_i^*x_i'$, 因此 $\mathcal{P}^*$ 只能选择挑战值 $c_i^*=(k_i-k_i')/(x_i'-x_i)$。验证通过还需要满足 $\sum_{i\in[N]}c_i^*=\mathcal{H}(\{u_i,v_i\}_{i\in[N]})$, 但这个事件发生的概率不超过 $1/q$, 因此以下定理成立。

定理 2. 在随机预言机模型中, 假设任意无限计算能力的敌手 $\mathcal{P}^*$ 最多可以询问 q_h 次随机预言机, 输出 $S=\{y_i,h_i,z_i\}_{i\in[N]}$ 以及一个 $\mathbf{ZP}_{1/N}$ 证明 $\Pi_{1/N}$。其中对于任意 $i\in[N]$, $S_i=\{y_i,h_i,z_i\}\notin\mathcal{DDH}$, 那么 $\Pi_{1/N}$ 是可接受的概率不超过 q_h/q, 如下式所示:

$$\mathbf{Pr}[(S;\Pi_{1/N})\leftarrow\mathcal{P}^{*\mathcal{H}},\forall S_i\notin\mathcal{DDH},$$
$$\mathbf{ZVfy}_{1/N}(S;\Pi_{1/N})=1]\leqslant q_h/q$$

特殊诚实验证者零知识性: 在随机预言机模型中, 存在一个模拟器 $\mathcal{S}$ 以 $S=\{y_i,h_i,z_i\}_{i\in[N]}$ 为输入, 输出一个可接受的证明副本, 此算法记为 $\mathbf{ZSim}_{1/N}(S)$, 过程如下:

1. 对于每一个 $i\in[N]$, 均匀随机取样 $c_i,s_i\leftarrow_{\$}\mathbb{Z}_q$, 并计算 $u_i=g^{s_i}y_i^{-c_i}$, $v_i=h_i^{s_i}z_i^{-c_i}$。

2. 重编程随机预言机 $\mathcal{H}(\{u_i,v_i\}_{i\in[N]})=\Sigma_ic_i$, 输出证明 $\Pi_{1/N}=\{c_i,s_i\}_{i\in[N]}$.

利用以上模拟算法, 我们可得到如下定理:

定理 3. 对于任意无限计算能力的敌手 $\mathcal{V}^*$, 公共输入 $S=\{y_i,h_i,z_i\}_{i\in[N]}$ 满足 $\log_g y_l=\log_{h_l} z_l=x_l$,

$$|\mathbf{Pr}[\Pi_{1/N}\leftarrow\mathbf{ZPrv}_{1/N}(S;l,x_l),\mathcal{V}^{*\mathcal{H}}(S;\Pi_{1/N})=1]$$
$$-\mathbf{Pr}[\Pi_{1/N}\leftarrow\mathbf{ZSim}_{1/N}(S),\mathcal{V}^{*\mathcal{H}}(S;\Pi_{1/N})=1]|\leq q_h/q^2$$

其中 q_h 为敌手询问随机预言机 $\mathcal{H}$ 的次数。

证明. 在模拟中, c_i,s_i 取自均匀分布, 与真实的证明分布一样。模拟器 $\mathcal{S}$ 需要重编程 $\mathcal{H}(\{g^{s_i}y_i^{-c_i},h_i^{s_i}z_i^{-c_i}\}_{i\in[N]})=\Sigma_ic_i$, 使得模拟的证明可以通过验证。敌手 $\mathcal{V}^*$ 无法区分, 除非它在此之前恰巧询问过这一点的随机预言机。但对于一个最多询问 q_h 次随机预言机的敌手, 这个事件发生的概率不超过 q_h/q^2。

4 紧安全的环签名方案

4.1 方案描述

在本节中将给出环签名方案的具体描述, 特别地, 在签名阶段我们调用了第 3 章的 $\mathrm{ZPrv}_{1/2n}$ 算法来产生一个非交互零知识证明。

初始化 Setup(1^κ): 对于安全参数 κ, 以 1^κ 为输入, 选择循环群 $\mathbb{G}$, 其阶为素数 q, 生成元为 g, 选择哈希函数 $H:\{0,1\}^*\to\mathbb{G}$, 输出公共参数 $pp:=(\mathbb{G},q,g,H)$。

密钥生成 KeyGen(pp): 以公共参数 pp 为输入, 均匀随机取样 $b \leftarrow_{\$} \{0,1\}$, $x^{(b)} \leftarrow_{\$} \mathbb{Z}_q$ 以及 $y^{(1-b)} \leftarrow_{\$} \mathbb{G}$。计算 $y^{(b)} = g^{x^{(b)}}$, 输出私钥 $sk = \left(b, x^{(b)}\right)$, 公钥 $pk = \left(y^{(0)}, y^{(1)}\right)$。为了避免混淆, 注意这里$(b)$仅表示记号, 并不是指数运算。

签名 Sign(M, R, sk_π): 以消息 M, 环 $R = (pk_1, \cdots, pk_n)$ 以及私钥 sk_π 为输入, 其中 $pk_i = \left(y_i^{(0)}, y_i^{(1)}\right)$ 对于所有 $i \in [n]$, $sk_\pi = \left(b_\pi, x_\pi^{(b_\pi)}\right)$ 对于 $\pi \in [n]$, 操作如下:

(1) 均匀随机取样 $r \leftarrow_{\$} \{0,1\}^{n_r}$, 计算 $h = H(M, r)$;

(2) 对于所有的 $i \in [n] \setminus \{\pi\}$, 均匀随机取样 $z_i^{(0)}, z_i^{(1)} \leftarrow_{\$} \mathbb{G}$。对于 $i = \pi$, 均匀随机选择 $z_\pi^{(1-b_\pi)} \leftarrow_{\$} \mathbb{G}$, 特别地计算 $z_\pi^{(b_\pi)} = h^{x_\pi^{(b_\pi)}}$。记 $\{y_j\}_{j\in[2n]} = \{y_i^{(0)}, y_i^{(1)}\}_{i\in[n]}$, $\{z_j\}_{j\in[2n]} = \{z_i^{(0)}, z_i^{(1)}\}_{i\in[n]}$, 其中 $y_{2i+b_i} = y_i^{(b_i)}$, $z_{2i+b_i} = z_i^{(b_i)}$;

(3) 记 $S := \{y_j, h, z_j\}_{j\in[2n]}$, $l := 2\pi + b_\pi$, 调用算法 $\mathbf{ZPrv}_{1/2n}$ 产生一个非交互零知识证明, 用来证明 S 中至少有一组满足 DDH 的等式关系, $\mathbf{ZPrv}_{1/2n}(S; (l, x_\pi^{(b_\pi)})) \to \{c_j, s_j\}_{j\in[2n]}$;

(4) 输出签名 $\sigma := (r, \{z_j, c_j, s_j\}_{j\in[2n]})$。

验证 Vrfy(M, R, σ): 以消息 M, 环 $R = (pk_1, \cdots, pk_n)$ $= \{y_j\}_{j\in[2n]}$ 以及签名 $\sigma = (r, \{z_j, c_j, s_j\}_{j\in[2n]})$ 为输入, 首先计算 $h = H(M, r)$, 令 $S = \{y_j, h, z_j\}_{j\in[2n]}$, 调用 $\mathbf{ZP}_{1/2n}$ 的验证算法 $\mathbf{ZVfy}_{1/2n}(S; \{c_j, s_j\}_{j\in[2n]}) \to b'$。如果 $b' = 1$, 则输出 1; 否则, 输出 0。

4.2 安全性分析

我们称一个环签名方案是安全的, 如果它满足匿名性和不可伪造性。这两个性质我们在第 2.3 节中已经给出了定义, 在本节中将通过以下两个定理分别证明 4.1 节中给出的环签名方案满足这两个性质, 从而说明此方案是安全的。

定理 4. 任意无限计算能力的敌手 $\mathcal{A}$ 破坏匿名性的优势不超过

$$\mathbf{Adv}_{\mathcal{A}}^{\text{anon}} \leqslant \mathbf{Adv}_{\mathcal{B}}^{DDH} + \frac{1}{q} + \frac{(q_s+1)q_h}{2^{n_r}} + \frac{(q_s+1)q_h}{q^2},$$

其中 q_h 是哈希询问的次数, q_s 是签名询问的次数。

证明. 如果存在一个敌手 $\mathcal{A}$ 可以破坏我们环签名构造的无条件匿名性, 那我们可以构造另一个敌手 $\mathcal{B}$ 区分 DDH 问题, 敌手 $\mathcal{B}$ 以 $(y, h, z) \in \mathbb{G}^3$ 为输入, 判断是否 $(y, h, z) \in \mathcal{DDH}$。具体构造如下:

(1) 初始化阶段: 给定参数 $(\mathbb{G}, q, g)$, $\mathcal{B}$ 选择一个哈希函数 $H: \{0,1\}^* \to \mathbb{G}$。$\mathcal{B}$ 把系统参数 $pp := (\mathbb{G}, q, g, H)$ 发送给敌手 $\mathcal{A}$;

(2) 询问阶段: 敌手 $\mathcal{A}$ 可以自适应地询问注册预言机, 签名预言机以及随机预言机。

注册预言机 $\mathcal{JO}$: $\mathcal{B}$ 均匀随机选择 $b \leftarrow_{\$} \{0,1\}$, $a, x \leftarrow_{\$} \mathbb{Z}_q$, 计算 $y^{(b)} = g^x$, $y^{(1-b)} = y^a$。令公钥 $pk = \left(y^{(0)}, y^{(1)}\right)$, 私钥 $sk = (b, x)$。$\mathcal{B}$ 把公钥 pk 发送给敌手 $\mathcal{A}$, 并把 $\left(y^{(1-b)}, a\right)$ 记录到表 $\mathcal{T}$ 中。

私钥预言机 $\mathcal{CO}$: $\mathcal{A}$ 询问关于公钥 pk 的私钥, $\mathcal{B}$ 返回私钥 $sk = (b, x)$。

签名预言机 $\mathcal{SO}$: 收到一个公钥集合 $R = (pk_1, \cdots, pk_n) = (\{y_i^{(0)}, y_i^{(1)}\}_{i\in[n]})$, 一个消息 M 以及 R 中的某一个公钥 pk_π, $\mathcal{B}$ 需要返回关于 M 的环签名给敌手 $\mathcal{A}$, 操作如下:

a. $\mathcal{B}$ 均匀随机选择 $r \leftarrow_{\$} \{0,1\}^{n_r}$, $\xi \leftarrow_{\$} \mathbb{Z}_q$, 编程随机预言机 $H(M, r) = g^\xi$;

b. 对于所有的 $i \in [n] \setminus \{\pi\}$, 均匀随机取样 $z_i^{(0)}, z_i^{(1)} \leftarrow_{\$} \mathbb{G}$。对于 $i = \pi$, $\mathcal{B}$ 计算 $z_\pi^{(0)} = (y_\pi^{(0)})^\xi$, $z_\pi^{(1)} = (y_\pi^{(1)})^\xi$。记 $\left\{y_j\right\}_{j\in[2n]} = \left\{y_i^{(0)}, y_i^{(1)}\right\}_{i\in[n]}$, $\left\{z_j\right\}_{j\in[2n]} = \left\{z_i^{(0)}, z_i^{(1)}\right\}_{i\in[n]}$;

c. $\mathcal{B}$ 运行 $\mathbf{ZSim}_{1/2n}(\{y_j, g^\xi, z_j\}_{j\in[2n]})$ 模拟产生一个证明 $\Pi_{1/2n} = (\{c_j, s_j\}_{j\in[2n]})$;

d. $\mathcal{B}$ 发送签名 $\sigma = (r, \{z_j, c_j, s_j\}_{j\in[2n]})$ 给敌手 $\mathcal{A}$, 并把 (M, r, g^ξ) 记录到表 $\mathcal{L}$ 中。

(3) 挑战阶段: 收到 $\mathcal{A}$ 的挑战 (M, i_0, i_1, R), 其中包括挑战消息 M, 挑战环 $R = (\{y_i^{(0)}, y_i^{(1)}\}_{i\in[n]}) = \{y_j\}_{j\in[2n]}$, 以及环中两个成员 $i_0, i_1 \in [n]$。首先, $\mathcal{B}$ 均匀随机选择 $r \leftarrow_{\$} \{0,1\}^{n_r}$, $d \leftarrow_{\$} \mathbb{Z}_q$, 编程随机预言机 $H(M, r) = h^d$。$\mathcal{B}$ 选择

$b \leftarrow_{\$} \{0,1\}$, 记 $\pi = i_b$, $\mathcal{B}$ 知道 R 中第 π 个成员的私钥为 (b_π, x_π), 并找到表 $\mathcal{T}$ 中的记录 $\left(y_\pi^{(1-b_\pi)}, a_\pi\right)$, 设定 $z_l = z_\pi^{(1-b_\pi)} = z^{a_\pi d}$ 其中 $l = 2\pi + 1 - b_\pi$。对于所有的 $j \in [2n] \setminus \{l\}$, $z_j \leftarrow_{\$} \mathbb{G}$。$\mathcal{B}$ 运行 $\mathsf{ZSim}_{1/2n}(\{y_j, h^d, z_j\}_{j\in[2n]})$ 模拟产生一个证明 $\Pi_{1/2n} = (\{c_j, s_j\}_{j\in[2n]})$, 发送挑战签名 $\sigma = (r, \{z_j, c_j, s_j\}_{j\in[2n]})$ 给敌手 $\mathcal{A}$。

(4) 输出阶段: $\mathcal{A}$ 输出 $b' \in \{0,1\}$, 如果 $b' = b$, 则 $\mathcal{B}$ 输出 1。

我们首先说明 $\mathcal{B}$ 成功模拟了敌手 $\mathcal{A}$ 的攻击环境。对于注册预言机, 与真实执行过程不同的是 $\mathcal{B}$ 设置 $y^{(1-b)} = y^a$ 而不是均匀随机选择 $y^{(1-b)} \leftarrow_{\$} \mathbb{G}$, 由于 $a \leftarrow_{\$} \mathbb{Z}_q$ 是随机均匀抽取, 因此 $y^{(1-b)} = y^a$ 与真实执行环境中 $y^{(1-b)} \leftarrow_{\$} \mathbb{G}$ 的分布是不可区分的。在签名预言机模拟中, $(y_\pi^{(0)}, g^\xi, z_\pi^{(0)}) \in \mathcal{DDH}$ 以及 $(y_\pi^{(1)}, g^\xi, z_\pi^{(1)}) \in \mathcal{DDH}$, 然而在真实的签名算法中, 只有 $(y_\pi^{(b_\pi)}, H(M,r), z_\pi^{(b_\pi)}) \in \mathcal{DDH}$, 但如果敌手 $\mathcal{A}$ 可以发现这个区别, 我们可以构造一个 q_s-DDH 区分器。其中模拟随机预言机 $H(M,r) = g^\xi$ 失败的概率不超过 $q_s q_h / 2^{n_r}$。在签名询问中, 敌手 $\mathcal{A}$ 并不能从中获得用户私钥的信息。

在生成挑战签名过程中, $\mathcal{B}$ 并没有计算 $z_\pi^{(b_\pi)} = H(M,r)^{x_\pi^{(b_\pi)}}$, 而是编程 $H(M,r) = h^d$, 利用 $\left(y^{a_\pi}, h^d, z^{a_\pi d}\right)$ 来代替 $(y_\pi^{(b_\pi)}, H(M,r), z_\pi^{(b_\pi)}) \in \mathcal{DDH}$。其中, 编程失败的概率不超过 $q_h / 2^{n_r}$。

如果给定的输入 $(y,h,z) \notin \mathcal{DDH}$, 那么 $\left(y^{a_\pi}, h^d, z^{a_\pi d}\right) \notin \mathcal{DDH}$, 此时 $(y_j, h^d, z_j) \notin \mathcal{DDH}$ 对于所有的 $j \in [2n]$, 因此, 敌手 $\mathcal{A}$ 从挑战签名中并不能获得任何关于比特 b 信息, 在这种情况下, 敌手 $\mathcal{A}$ 成功输出 $b' = b$ 的概率为 1/2。

如果给定的输入 $(y,h,z) \in \mathcal{DDH}$, 那么 $\left(y^{a_\pi}, h^d, z^{a_\pi d}\right) \in \mathcal{DDH}$, 其中 y^{a_π} 对应于第 $\pi = i_b$ 个用户的子公钥 $y_\pi^{(1-b_\pi)}$, 而在真实的签名中, $(y_\pi^{(b_\pi)}, H(M,r), z_\pi^{(b_\pi)}) \in \mathcal{DDH}$。因为敌手 $\mathcal{A}$ 没有询问过用户 i_0, i_1 的私钥, 同时敌手 $\mathcal{A}$ 不能从签名询问中获得用户 i_0, i_1 的私钥信息, 因此敌手 $\mathcal{A}$ 没有比特 b_π 的信息。再结合**定理 3** 中零知识证明系统 $\mathsf{ZP}_{1/2n}$ 的零知识性, 如果 $(y,h,z) \in \mathcal{DDH}$, $\mathcal{B}$ 模拟产生的挑战签名与真实执行签名算法产生的挑战签名是计算不可区分的。在这种情况下, 如果敌手 $\mathcal{A}$ 可以成功地输出 $b' = b$ 以大于 1/2 不可忽略的优势, 那么 $\mathcal{B}$ 可以借助敌手 $\mathcal{A}$ 的能力来判断是否满足 $(y,h,z) \in \mathcal{DDH}$。

综上所述, 如果敌手 $\mathcal{A}$ 成功破坏匿名性, 我们可以构造一个敌手 $\mathcal{B}$ 解决 q_s+1-DDH 问题, 结合**定理 1** 其优势满足

$$\mathbf{Adv}_{\mathcal{A}}^{\text{anon}} \leqslant \mathbf{Adv}_{\mathcal{B}}^{\text{DDH}} + \frac{1}{q} + \frac{(q_s+1)q_h}{2^{n_r}} + \frac{(q_s+1)q_h}{q^2}。$$

定理 5. 在随机预言机模型下, 如果存在一个敌手 $\mathcal{A}$ 可以成功地伪造一个环签名, 假设它最多可以询问 q_h 次随机预言机, q_s 次签名预言机, 那我们可以构造敌手 $\mathcal{B}$ 和 $\mathcal{C}$ 分别解决 CDH 和 DDH 问题, 满足

$$\mathbf{Adv}_{\mathcal{A}}^{\text{uf}} \leqslant 2\mathbf{Adv}_{\mathcal{B}}^{\text{CDH}} + \mathbf{Adv}_{\mathcal{C}}^{\text{DDH}} + \frac{1}{q} + \frac{q_h}{q} + \frac{q_s q_h}{2^{n_r}} + \frac{q_s q_h}{q^2}$$

证明. 给定 y, h, $\mathcal{B}$ 的目标是调用敌手 $\mathcal{A}$ 来计算 z 满足 $(y,h,z) \in \mathcal{DDH}$, 具体操作如下:

(1) 初始化阶段: 给定公共参数 $pp = (\mathbb{G}, q, g)$, $\mathcal{B}$ 选择一个哈希函数 $H: \{0,1\}^* \to \mathbb{G}$, H 被模型化为随机预言机模型。$\mathcal{B}$ 把系统参数 pp 发送给敌手 $\mathcal{A}$。

(2) 询问阶段: 敌手 $\mathcal{A}$ 可以自适应地询问注册预言机, 签名预言机, 私钥预言机以及随机预言机。

注册预言机 $\mathcal{JO}$: $\mathcal{B}$ 均匀随机选择 $b \leftarrow_{\$} \{0,1\}$, $a, x^{(b)} \leftarrow_{\$} \mathbb{Z}_q$, 计算 $y^{(b)} = g^{x^{(b)}}$, $y^{(1-b)} = y^a$。令公钥 $pk = \left(y^{(0)}, y^{(1)}\right)$, 私钥 $sk = \left(b, x^{(b)}\right)$。$\mathcal{B}$ 把公钥 pk 发送给敌手 $\mathcal{A}$, 并把 $\left(y^{(1-b)}, a\right)$ 记录到表 $\mathcal{T}$ 中。

私钥预言机 $\mathcal{CO}$: $\mathcal{A}$ 询问关于公钥 pk 的私钥, $\mathcal{B}$ 返回私钥 $sk = \left(b, x^{(b)}\right)$。

签名预言机 $\mathcal{SO}$: 收到一个公钥集合 $R = (pk_1, \cdots, pk_n) = (\{y_i^{(0)}, y_i^{(1)}\}_{i\in[n]})$, 一个消息 M 以及 R 中的某一个公钥 pk_π, $\mathcal{B}$ 需要返回关于 M 的环签名给敌手 $\mathcal{A}$, 操作如下:

a. $\mathcal{B}$ 均匀随机选择 $r \leftarrow_{\$} \{0,1\}^{n_r}$, $\xi \leftarrow_{\$} \mathbb{Z}_q$, 编程随机预言机 $H(M,r) = g^\xi$;

b. 于所有的 $i \in [n] \setminus \{\pi\}$, 均匀随机取样

$z_i^{(0)}, z_i^{(1)} \leftarrow_{\$} \mathbb{G}$。对于 $i=\pi$，$\mathcal{B}$ 计算 $z_\pi^{(0)}=(y_\pi^{(0)})^{\xi}$，$z_\pi^{(1)}=(y_\pi^{(1)})^{\xi}$。记 $\{y_j\}_{j\in[2n]}=\{y_i^{(0)}, y_i^{(1)}\}_{i\in[n]}$，$\{z_j\}_{j\in[2n]}=\{z_i^{(0)}, z_i^{(1)}\}_{i\in[n]}$;

c. $\mathcal{B}$ 运行 $\mathbf{ZSim}_{1/2n}(\{y_j, g^{\xi}, z_j\}_{j\in[2n]})$ 模拟产生一个证明 $\Pi_{1/2n}=(\{c_j, s_j\}_{j\in[2n]})$;

d. $\mathcal{B}$ 发送签名 $\sigma=(r, \{z_j, c_j, s_j\}_{j\in[2n]})$ 给敌手 $\mathcal{A}$，并把 (M, r, g^{ξ}) 记录到表 $\mathcal{L}$ 中。

随机预言机 H: 以消息 M 以及比特字符串 r 为输入，$\mathcal{B}$ 首先查看表 $\mathcal{L}$ 中是否有记录 $(M, r, \cdot)$，如果存在，则将对应的结果返回给 $\mathcal{A}$。如果没有，则随机均匀选择 $d \leftarrow_{\$} \mathbb{Z}_q$，编程 $H(M, r)=h^d$，返回 h^d 给 $\mathcal{A}$，并将 (M, r, h^d) 记录下来;

(3) 输出阶段：收到 $\mathcal{A}$ 的伪造结果 $(M^*, R^*=(\{pk_i^*\}_{i\in[n]})=(\{y_j^*\}_{j\in[2n]}), \sigma^*)$，满足 $\mathbf{Vrfy}(M^*, R^*, \sigma^*)=1$，$\mathcal{A}$ 没有询问过关于消息 M^* 和环 R^* 的签名，也没有询问过 R^* 中任意一个公钥所对应的私钥，并且 R^* 中的每一个公钥均来自于注册预言机。$\mathcal{B}$ 操作如下:

a. 首先把签名拆开 $\sigma^*=(r^*, \{z_j^*, c_j^*, s_j^*\}_{j\in[2n]})$，敌手 $\mathcal{A}$ 一定询问过随机预言机 $H(M^*, r^*)$，找到表 $\mathcal{L}$ 中相应的记录，记作 (M^*, r^*, h^{d^*})，则 $H(M^*, r^*)=h^{d^*}$;

b. 签名 σ^* 的合法性说明 $\Pi_{1/2n}^*=\{c_j^*, s_j^*\}_{j\in[2n]}$ 是关于 $S=\{y_j^*, h^{d^*}, z_j^*\}_{j\in[2n]}$ 的一个可接受的证明副本，进而由零知识证明系统 $\mathbf{ZP}_{1/2n}$ 的合理性，我们知道公共输入 S 中至少有一组 $\{y_l^*, h^{d^*}, z_l^*\}\in\mathcal{DDH}$，其中 $l\in[2n]$;

c. 记 $\pi=\lfloor l/2\rfloor\in[n]$，如果 $l=2\pi+b_\pi$，则游戏停止；如果 $l=2\pi+(1-b_\pi)$，则表 $\mathcal{T}$ 中存在记录 (y_l^*, a_π^*)，满足 $y_l^*=y^{a_\pi^*}$，在这种情况下，$(y^{a_\pi^*}, h^{d^*}, z_l^*)\in\mathcal{DDH}$ 可以推导出 $(y, h, (z_l^*)^{1/(a_\pi^*\cdot d^*)})\in\mathcal{DDH}$，$\mathcal{B}$ 输出 $z=(z_l^*)^{1/(a_\pi^*\cdot d^*)}$，解决了 CDH 问题。

下面我们说明 $\mathcal{B}$ 成功地为敌手 $\mathcal{A}$ 模拟了攻击环境。首先在注册预言机模拟中，与真实执行过程不同的是 $\mathcal{B}$ 设置 $y^{(1-b)}=y^a$ 而不是均匀随机选择 $y^{(1-b)}\leftarrow_{\$}\mathbb{G}$，由于 $a\leftarrow_{\$}\mathbb{Z}_q$ 是随机均匀抽取，因此 $y^{(1-b)}=y^a$ 与真实执行环境中 $y^{(1-b)}\leftarrow_{\$}\mathbb{G}$ 的分布是不可区分的。在签名预言机模拟中，$(y_\pi^{(0)}, g^{\xi}, z_\pi^{(0)})\in\mathcal{DDH}$ 以及 $(y_\pi^{(1)}, g^{\xi}, z_\pi^{(1)})\in\mathcal{DDH}$，然而在真实的签名算法中，只有 $(y_\pi^{(b_\pi)}, H(M, r), z_\pi^{(b_\pi)})\in\mathcal{DDH}$，但如果敌手 $\mathcal{A}$ 可以发现这个区别，我们可以构造一个 q_s-DDH 区分器。其中模拟随机预言机 $H(M, r)=g^{\xi}$ 失败的概率不超过 $q_sq_h/2^{n_r}$。除此之外，$\mathcal{B}$ 运行 $\mathbf{ZSim}_{1/2n}$ 模拟产生证明 $\Pi_{1/2n}=(\{c_j, s_j\}_{j\in[2n]})$，而不是调用算法 $\mathsf{ZPrv}_{1/2n}$ 真实地产生一个证明，基于**定理 3**，敌手能够区分这个变化的优势不超过 q_sq_h/q^2。

如果 $\mathcal{A}$ 成功地破坏了环签名的不可伪造性，输出了 $(M^*, R^*, \sigma^*=(r^*, \{z_j^*, c_j^*, s_j^*\}_{j\in[2n]}))$，那么 $\mathcal{A}$ 一定没有询问过 $\mathcal{SO}(R^*, M^*, \cdot)$，进而 $H(M^*, r^*)=h^{d^*}$ 成立，其中 d^* 是 $\mathcal{B}$ 在某一次随机预言机模拟中均匀随机选择的。如果 $\{y_j^*, h^{d^*}, z_j^*\}\notin\mathcal{DDH}$ 对于所有的 $j\in[2n]$，那么敌手就破坏零知识证明系统 $\mathsf{ZP}_{1/2n}$ 的合理性。由**定理 2** 可知，此概率不超过 q_h/q。假设有一组 $\{y_l^*, h^{d^*}, z_l^*\}\in\mathcal{DDH}$，其中 $l\in[2n]$，如果 $\pi=\lfloor l/2\rfloor\in[n]$，则 y_l^* 是用户 π 公钥的一部分，敌手 $\mathcal{A}$ 不知道 b_π，那么至少有 1/2 的概率 $l=2\pi+(1-b_\pi)$，也就是说 $\mathcal{B}$ 不知道 y_l^* 对应的离散对数。在注册预言机模拟中，$\mathcal{B}$ 把 y_l^* 设置为 $y^{a_\pi^*}$，其中 a_π^* 服从 $\mathbb{Z}_q$ 上的均匀分布。那么 $\mathcal{B}$ 可以通过计算 $z=(z_l^*)^{1/(a_\pi^*\cdot d^*)}$ 来解决给定输入 y, h 的 CDH 问题。总结来看，敌手 $\mathcal{A}$ 成功破坏我们环签名方案的不可伪造性的概率满足下面的式子:

$$\mathbf{Adv}_{\mathcal{A}}^{\mathbf{uf}}\leqslant 2\mathbf{Adv}_{\mathcal{B}}^{\mathbf{CDH}}+\mathbf{Adv}_{\mathcal{C}}^{q_s\text{-}\mathbf{DDH}}+\frac{q_h}{q}+\frac{q_sq_h}{2^{n_r}}+\frac{q_sq_h}{q^2}。$$

再由**定理 1** 即 $\mathbf{Adv}_{\mathcal{C}}^{q_s\text{-}\mathbf{DDH}}\leqslant\mathbf{Adv}_{\mathcal{C}}^{\mathbf{DDH}}+1/q$ 可知

$$\mathbf{Adv}_{\mathcal{A}}^{\mathbf{uf}}\leqslant 2\mathbf{Adv}_{\mathcal{B}}^{\mathbf{CDH}}+\mathbf{Adv}_{\mathcal{C}}^{\mathbf{DDH}}+\frac{1}{q}+\frac{q_h}{q}+\frac{q_sq_h}{2^{n_r}}+\frac{q_sq_h}{q^2}。$$

4.3 性能分析

如上表所示，本文方案的通讯复杂度以及计算复杂度均为 $O(n)$。和 Groth 等人[25]的典型环签名构造相比，虽然该方案的通讯复杂度为 $O(\log n)$，但其

表 1 现有工作对比

Table 1 Efficiency comparison

	公钥尺寸	签名尺寸	签名计算量	验证计算量
本文方案	$2n\cdot G$	$4n\cdot\|q\|+2n\cdot G$	$8n-1^{*}$	$8n^{*}$
文献[15]方案	$n\cdot G$	$(3\log n+1)\cdot\|q\|$ $+4\log n\cdot G$	$(n+7)\log n^{*}$	$(n+6)\log n^{*}$

(注: G 是指表示循环群 $\mathbb{G}$ 中元素的比特位数; n 指环中成员个数; q 指循环群 $\mathbb{G}$ 的阶数($G\geqslant|q|=\lceil\log_2 q\rceil$); “*” 表示指数运算的次数)

计算复杂度为 $O(n\cdot\log n)$, 而且它的安全规约存在巨大损失 $\varepsilon_{\mathcal{B}}\approx\varepsilon_{\mathcal{A}}^{\log n}/(q_j\cdot q_h)$, 举一个例子: 假设 $n=2^{10}$, $q_j=q_h=2^{30}$, 如果我们希望安全级别达到 128 bit, 那么安全参数就要取 $\kappa=1340$, 降低了方案效率。然而对于本文的紧归约方案来说, 安全参数的选取几乎不受影响。

5 结论

本文中我们基于DDH假设提出了一个紧安全的环签名方案, 安全证明过程中的归约损失仅为常数。在设计中, 我们令用户的公钥包含两个子公钥, 从而避免了猜测敌手目标所带来的归约损失; 基于EDL 签名方案, 我们构造了一个 1/N-DDH 非交互零知识证明系统, 从而证明用户拥有有效的私钥, 得到相应的环签名方案。得益于这种构造方式, 在证明过程中我们没有使用重绕技术, 最终的归约损失仅为常数。

下一步, 我们可以从两个方面继续我们的研究工作, 一是基于我们的设计构造具有其他性质的环签名方案, 如可链接环签名。文献[25]提出可以利用一个环签名方案和一个一次签名方案来构造可链接环签名, 基于我们的构造虽然可以降低可链接环签名方案的归约损失, 但并不能直接得到紧安全的可链接环签名方案, 仍需进一步的研究。另一方面, 可以探究如何利用我们的思想和技术来设计其他隐私保护签名方案, 如紧安全的群签名、可追踪签名等等。

参考文献

[1] Diffie W, Hellman M. New Directions in Cryptography[C]. *IEEE Transactions on Information Theory*, 1976: 644-654.

[2] Blazy O, Kakvi S A, Kiltz E, et al. Tightly-Secure Signatures from Chameleon Hash Functions[C]. *Public-Key Cryptography-PKC 2015*, 2015: 256-279.

[3] Fiat A, Shamir A. How to Prove Yourself: Practical Solutions to Identification and Signature Problems[C]. *Advances in Cryptology - CRYPTO' 86*, 1987: 186-194.

[4] Pointcheval D, Stern J. Security Arguments for Digital Signatures and Blind Signatures[J]. *Journal of Cryptology*, 2000, 13(3): 361-396.

[5] Fischlin M. Communication-Efficient Non-Interactive Proofs of Knowledge with Online Extractors[C]. *Advances in Cryptology-CRYPTO 2005*, 2005: 152-168.

[6] Goh E J, Jarecki S. A Signature Scheme as Secure as the Diffie-Hellman Problem[C]. *Advances in Cryptology-EUROCRYPT 2003*, 2003: 401-415.

[7] Katz J, Wang N. Efficiency Improvements for Signature Schemes with Tight Security Reductions[C]. *The 10th ACM conference on Computer and communications security*, 2003: 155-164.

[8] Chevallier-Mames B. An Efficient CDH-Based Signature Scheme with a Tight Security Reduction[C]. *Advances in Cryptology-CRYPTO 2005*, 2005: 511-526.

[9] Bellare M, Boldyreva A, Micali S. Public-Key Encryption in a Multi-User Setting: Security Proofs and Improvements[C]. *Advances in Cryptology — EUROCRYPT 2000*, 2000: 259-274.

[10] R. Rivest, A. Shamir, Y. Tauman. How to leak a secret[C]. *In proc. Asian Cryptology Conference*, 2001: 552-565.

[11] Bender A, Katz J, Morselli R. Ring Signatures: Stronger Definitions, and Constructions without Random Oracles[J]. *Journal of Cryptology*, 2009, 22(1): 114-138.

[12] Shacham H, Waters B. Efficient Ring Signatures without Random Oracles[J]. *IACR Cryptology EPrint Archive*, 2006: 289.

[13] Chandran N, Groth J, Sahai A. Ring Signatures of Sub-Linear Size without Random Oracles[C]. *Automata, Languages and Programming*, 2007: 423-434.

[14] Wang F H, Hu Y P, Wang C X. A Lattice-Based Ring Signature Scheme from Bonsai Trees[J]. *Journal of Electronics & Information Technology*, 2010, 32(10): 2400-2403.
(王凤和, 胡予濮, 王春晓. 格上基于盆景树模型的环签名[J]. *电子与信息学报*, 2010, 32(10): 2400-2403.)

[15] Groth J, Kohlweiss M. One-out-of-many Proofs: Or how to Leak a Secret and Spend a Coin[C]. *Advances in Cryptology - EUROCRYPT 2015*, 2015: 253-280.

[16] Libert B, Ling S, Nguyen K, et al. Zero-Knowledge Arguments for Lattice-Based Accumulators: Logarithmic-Size Ring Signatures and Group Signatures without Trapdoors[C]. *Advances in Cryptology-EUROCRYPT 2016*, 2016: 1-31.

[17] Liu J K, Wei V K, Wong D S. Linkable Spontaneous Anonymous Group Signature for Ad Hoc Groups[C]. *Information Security and Privacy*, 2004: 325-335.

[18] Chow S S M, Lui R W C, Hui L C K, et al. Identity Based Ring Signature: Why, how and what next[C]. *Public Key Infrastructure*,

2005: 144-161.

[19] 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.
(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.)

[20] Franklin M, Zhang H B. Unique Ring Signatures: A Practical Construction[C]. *Financial Cryptography and Data Security*, 2013: 162-170.

[21] Gjøsteen K, Jager T. Practical and Tightly-Secure Digital Signatures and Authenticated Key Exchange[C]. *Advances in Cryptology -CRYPTO 2018*, 2018: 95-125.

[22] Cramer R, Damgård I, Schoenmakers B. Proofs of Partial Knowledge and Simplified Design of Witness Hiding Protocols[C]. *Advances in Cryptology-CRYPTO '94*, 1994: 174-187.

[23] D. Chaum, E. van Heyst. Group Signatures[C]. *In Proc. European Cryptology Conference*, 1991: 257-265.

[24] K. Aggelos, Y. Tsiounis, M. Yung. Traceable Signatures[C]. *In Proc. European Cryptology Conference*, 2004: 571-589.

[25] Wang X L, Chen Y, Ma X C. Adding Linkability to Ring Signatures with One-Time Signatures[C]. *Information Security*, 2019: 445-464.

邱添 于 2016 年在西安电子科技大学统计学专业获得理学学士学位。现在中国科学院信息工程研究所信息安全国家重点实验室攻读硕士学位。研究领域为密码算法。研究兴趣包括: 群签名、环签名、格密码。Email: qiutian@iie.ac.cn

唐国锋 于 2016 年在中国石油大学信息与计算科学专业获得理学学士学位。现在中国科学院软件研究所可信计算与信息保障实验室攻读博士学位。研究领域为密码算法与安全协议。研究兴趣包括: 格密码、数字签名。 Email: guofeng2016@iscas.ac.cn

林东岱 于 1990 年在中国科学院系统科学研究所获得博士学位。现为中国科学院信息工程研究所信息安全国家重点实验室研究员。主要研究领域为密码理论与技术。Email: ddlin@iie.ac.cn