基于 RSA 公钥密码体制的可选择可转换关联环签名

张文芳[1),3)] 熊 丹[1),2)] 王小敏[1)] 陈 桢[1),3)] 刘旭东[1),3)]

[1)](西南交通大学信息科学与技术学院 成都 610031)

[2)](中国电子科技网络信息安全有限公司 成都 200233)

[3)](西南交通大学信息安全与国家计算网格四川省重点实验室 成都 610031)

摘 要 环签名因其无条件匿名性、自发性和灵活的群结构被广泛应用于电子现金、电子投票等强匿名认证领域.其中,关联环签名可以在不泄露真实签名者身份的前提下证明两个签名是否由同一人签发,因此可以在保障匿名性的前提下避免签名权滥用,如重复投票、电子现金重复花费等问题.然而,已有关联环签名的安全性大多数建立在离散对数困难问题基础上,且绝大多数方案因强关联性导致匿名性退化.为了克服上述问题,该文提出一个基于大整数分解难题和 RSA 公钥密码体制的可选择关联可转换环签名方案,并给出该类环签名的形式化安全模型.通过选择随机参数生成关联标签的方式,使得所提方案不仅具备强匿名性,而且环签名的关联性可由签名者自主决定.此外,签名者可以在不公开秘密随机参数的前提下将环签名转换为普通数字签名,能够抵抗可转换性攻击.在随机预言机模型下可证明该方案在适应性选择消息和选择公钥攻击下是存在性不可伪造的.此外,性能分析表明,该文方案与同类方案相比具有较高的运行效率.

关键词 RSA 公钥密码体制;环签名;选择关联性;强匿名性;可转换性

中图法分类号 TP309 **DOI 号** 10.11897/SP.J.1016.2017.01168

Selectively Linkable and Convertible Ring Signature Based on RSA Public Key Cryptosystem

ZHANG Wen-Fang[1),3)] XIONG Dan[1),2)] WANG Xiao-Min[1)] CHEN Zhen[1),3)] LIU Xu-Dong[1),3)]

[1)](*School of Information Science and Technology, Southwest Jiaotong University, Chengdu* 610031)

[2)](*China Electronic Technology Cyber Security Limited Company, Chengdu* 200233)

[3)](*Key Laboratory of Information Science and National Computing Grid, Southwest Jiaotong University, Chengdu* 610031)

Abstract Ring signatures are widely used in strong anonymous athentication environments such as electronic cash and electronic voting, because of their unconditional anonymity, spontaneity and flexible group structures. However, for some special purpose, we should discriminate if two signatures are signed by the same signer. For example, we should distinguish if a voter has cast mutiple ballots and the same e-cash has been repeatedly consumed. To solve the above mentiond problems, linkable ring signatures were proposed, by which any two signatures generated by the same person can be detected, with the premise of not disclosing the indentity of the real signer. However, most of the existing linkable ring signature schemes are based on discrete logarithm public key cryptosystems, and the vast majority of schemes only have the characteristics of weak anonymity and strong linkability. In this paper, a selectively linkable and convertible ring signature based on RSA public key cryptosystem was proposed, and a formal security model of

收稿日期:2015-12-29;在线出版日期:2016-10-29.本课题得到国家自然科学基金(61003245,61371098)、四川省科技厅应用基础研究基金(2015JY0182)、中央高校基本科研业务费专项基金(SWJTU11CX041)资助.**张文芳**,女,1978 年生,博士,副教授,主要研究方向为密码学、信息安全.E-mail:wfzhang@swjtu.edu.cn.**熊 丹**,女,1989 年生,硕士研究生,主要研究方向为信息安全、环签名.**王小敏**(通信作者),男,1974 年生,博士,教授,主要研究领域为信息安全、轨道交通安全工程.E-mail:xmwang@swjtu.edu.cn.**陈 桢**,男,1990 年生,硕士研究生,主要研究方向为信息安全、基于属性的密码体制.**刘旭东**,男,1990 年生,硕士研究生,主要研究方向为环签名、基于属性的密码体制.

this kind of ring signature was presented. The scheme is proven to be unconditionally anonymous, and the linkability of the signature can be decided by the signer through selecting random parameters to generate the linkable tag. Besides, in necessary occasions, the signer can convert the ring signature into an ordinary digital signature on the premise of not revealing secret parameters, so that he can prove himself as the real signer. It is proven that the proposed scheme can resist the convertable attack and is existentially unforgeable against the adaptive chosen plaintext attack and the chosen public-key attack under the random oracle model. Finally, the performance analysis shows that the proposed scheme has high operating efficiency.

Keywords　RSA public key cryptosystem; ring signature; selective linkability; strong anonymity; convertibility

1　引　言

2001 年，Rivest，Shamir 和 Tauman[1]首次提出了环签名的概念，因其按照一定规则首尾相连可组成一个环状结构而得名，签名验证者可以确定签名者来自环中的某一个成员，但无法确定真实签名者的身份. 不同于群签名的是，环签名可以任意选择一组成员作为可能的签名者，没有群的建立过程，也不需要群管理员，并且能够保证签名者身份的无条件匿名性，这些性质使环签名在电子现金、电子选举、Ad hoc 等匿名身份认证领域有着广泛应用. 随着环签名的提出，各种实现方案被先后提出，如 Dodis 等人[2]在 Eurocrypt2004 上利用 Fiat-Shamir 变换给出一个随机预言机模型下可证安全的环签名方案，Shacham 和 Waters[3]在 PKC2007 首次基于双线性映射提出一个高效环签名，2009 年 Bender 等人[4]给出第一个标准模型下可证安全的环签名. 随后，环签名的研究进入一个非常活跃的时期. 2015 年 Bose 等人[5]给出一个无需随机预言机假设的定长环签名方案，Shim[6]提出一个具有固定数量 Pairing 运算的高效环签名方案，Wang 等人[7]给出一个可引用(quotable)的环签名方案；2016 年 Gritti 等人[8]给出一个签名长度为 $O(\log_2 N)$ 的环签名方案. 除了上述利用大整数分解和离散对数等平均困难问题构造的环签名之外，为了抵抗量子计算攻击并降低计算复杂度，基于格、编码和多变量二次方程组(Multivariate Quadratic，MQ)难解问题的环签名也被先后提出. 2010 年 Brakerski 和 Kalai[9]提出第一个基于格中最坏问题(worst-case problem in lattice)的环签名方案，随后多个基于格中困难问题的环签名及门限环签名方案被提出[10-15]. 文献[16-17]基于 MQ 问题先后提出多变量公钥密码体制下(Multivariate Public Key Cryptosystem，MPKC)的环签名方案. 2007 年 Zheng 等人[18]基于综合解码问题给出一个环签名方案，Melchor 等人[19]和 Dallot 等人[20]则先后给出基于编码的门限环签名方案；2016 年，文献[21]给出一个基于 LDGM(Low-Density Generator-Matrix)码的环签名. 上述方案可以被看作后量子环签名方案. 此外，一系列具备不同特性的环签名方案也被先后提出，如门限环签名、可撤销匿名性的环签名、代理环签名和不可否认环签名等[22-26].

某些环境中，在保证匿名性的前提下，需要知道两个签名是否由同一签名者签发，如在电子投票中，既需要保护选民的隐私，又要避免重复投票. 为解决上述问题，Liu 等人[27]提出了关联环签名(Linkable Ring Signature)的概念：存在有效算法可以在不泄露真实签名者身份的前提下证明两个签名由同一签名者签发. 通过在环签名中添加关联标签，该文给出了第一个关联环签名方案——LSAG(Linkable Spontaneous Anonymous Group)，并用改造后的分叉引理证明了方案的安全性. 同时，作者指出关联环签名框架不具有无条件匿名性，如何设计一个具有强匿名性的关联环签名是一个尚待解决的问题[27]. 此后，不同的关联环签名框架被先后提出[28-35]. 如文献[28]利用双线性对构造了一种 GDH(Gap Diffie-Hellman)群上的关联环签名，签名之间的关联性由零知识协议保证；2005 年，Tsang 等人[29]将可分性和关联性同时应用于门限环签名，提出了可分关联门限环签名，并引入了指责关联性、“群体-指向”关联性和“事件-指向”关联性；文献[30-32]针对电子投票和电子现金中重复投票、重复花费等问题提出了简短关联环签名的形式化安全模型及实现方案.

然而,这些关联环签名框架均引入强关联标签实现同源签名间的相互关联,若环中其他成员合作,真实签名者的身份即会暴露,因此都不具备强匿名性特点.此外,如果签名者拒绝加入正确的关联标签,则整个签名无效,即签名的关联性不能由签名者自行决定.

针对上述问题,Liu 等人[36]提出了一种指定验证者的关联环签名,保证所有人都能验证签名的正确性,但只有指定的验证者才能验证签名的关联性.随后,Chow 等人[37]提出一个第三方托管的关联环签名方案,只有关联认证机构才能关联两个环签名.2008 年,Jeong 等人[38]提出了可选择关联环签名(Selective Linkable Ring Signature),签名者可以自行决定是否使其生成的不同环签名之间具备关联性,同时通过使用随机参数生成关联标签的方式实现了签名的强匿名性和弱关联性.虽然可选择关联环签名在一定程度上解决了普通关联环签名匿名性退化的问题,但现有方案大多借助离散对数困难问题进行构造,仅存在少部分基于其他 NP 困难问题的可选择关联环签名方案[39].

除可选择关联性外,在某些应用中(如需要为揭发者颁奖等场合),环签名还需要具备可转换性(Convertibility),即签名者在必要时能够将环签名转化为普通的数字签名,从而证明自己为签名者本人.基于不同体制的可转换环签名虽被先后提出[39-44],但多数方案无法抵抗可转换性攻击,即环中其他成员能够代替实际签名者进行签名转换[45].

本文针对现有可选择关联环签名大多建立在离散对数难题基础上,大部分方案由于引入强关联标签导致匿名性退化,以及可转换环签名无法抵抗可转换攻击等问题,提出一个基于大整数分解困难问题的可选择关联可转换环签名方案.与现有关联环签名大多依赖于单一困难问题不同,本文所提方案基于 RSA 公钥密码体制原型构建,其数学基础为大整数分解.本方案通过选择随机参数生成关联标签的方法,具备可选择关联性和强匿名性,同时签名者可以在不公开秘密随机参数的前提下将环签名转换为普通数字签名,能够抵抗可转换性攻击.本文给出该类可选择关联可转换环签名的形式化安全模型,并在随机预言机模型下证明所提方案在适应性选择消息和选择公钥攻击下是存在性不可伪造的.最后,将所提方案的性能与同类方案进行对比分析,仿真结果表明本文方案在保证匿名性的前提下具有很高的运算效率.

本文第 2 节介绍关联环签名的相关研究工作;第 3 节给出可选择关联可转换环签名方案的安全模型及其安全性的形式化定义;第 4 节提出一个基于 RSA 公钥密码体制的可选择关联可转换环签名方案;第 5 节对所提方案的正确性和安全性进行证明;第 6 节给出方案的性能分析和效率比较;第 7 节利用 WinNTL 和 OpenSSL 函数库给出方案的算法实现;最后对全文进行总结.

2 相关工作

环签名具备的匿名性(anonymity)主要分为两类:计算匿名性(computational anonymity)和无条件匿名性(unconditional anonymity).

(1)计算匿名性.是指方案的匿名性是基于某一数学困难问题(如离散对数问题、RSA 问题、大整数分解问题、Diffi-Hellman 问题等).如果存在一个敌手能够有效地求解这一困难问题,则匿名性将会被攻破.

(2)无条件匿名性.是指即便某一敌手拥有无限的计算能力和时间,依然无法获得签名者的真实身份,即匿名性仍然能够得到保证.

大多数传统的环签名都具备无条件匿名性,也有一些环签名方案提供计算匿名性.

然而关联环签名自提出以来一直只能提供计算匿名性.直到 2008 年,Jeong 等人[38]才提出了一个具备强匿名性的弱关联环签名,并将关联环签名的匿名性分为两类:强匿名性(strong anonymity)和弱匿名性(weak anonymity).

(1)弱匿名性.已知环签名中所有环成员的公钥,只要环中所有成员不揭露自己的身份,任何人都不可能获知此环签名的真实签名者身份.

(2)强匿名性.已知环签名中所有环成员的公钥,即便环中所有成员的私钥均被知晓,任何人依然无法得知此环签名的真实签名者身份.

目前绝大多数关联环签名只具备弱匿名性,仅有少数方案提供了强匿名性.下面对关联环签名的相关研究工作进行详细的分析和介绍.

关联环签名的概念由 Liu 等人[27]于 2004 年首次提出,主要用于一些既要保障签名者的匿名性又要避免签名者滥用签名权的场所,即关联环签名需要满足匿名性、自发性(spontaneity)和关联性(linkability)这 3 个基本性质.目前的研究主要通过在环签名中添加关联标签、指定关联验证者、引入第

三方权威机构等方式实现环签名的可关联性.

在第一类关联环签名方案中，签名者的私钥信息被嵌入关联标签中，验证者可以通过关联标签判断两个签名是否由同一个签名者产生，由于该类方案的关联标签包含了签名者私钥且签名的关联性可被任何人验证，因此具有强关联性和弱匿名性. LSAG 方案[27]即为此类关联环签名，在随机预言机模型下，该方案利用改造后的分叉引理证明其在抗适应性选择明文攻击和适应性选择密钥攻击下是不可伪造的. Liu 等人在文献[27]中还利用 LSAG 方案实现了可检测重复投票的电子投票协议，并进一步给出基于 LSAG 的(t,n)门限关联环签名方案，其时间复杂度和空间复杂度均为 $O(tn)$. 2006 年，Zheng 等人[28]指出 LSAG 方案[27]的安全性仅基于 DDH(Decisional Diffie-Hellman)假设，而 DDH 问题在 GDH 群上是可解的，因此将 LSAG 进一步扩展为 GDH 群上的关联环签名方案. 此外，Tsang 等人[29]于 2005 年提出可分(Separable)门限关联环签名及其安全模型，即使成员使用不同的密码元语和系统参数，仍能够自发组群产生有效的关联环签名，该方案的时间和空间复杂度均为 $O(n)$，同时文献[29]还对关联性进行了细化分类，引入了指责和非指责关联性、“群体-指向”关联性和“事件-指向”关联性. 具备“非指责”关联性是指方案只能检测两个环签名是否由同一人生成，但如果具备“指责”关联性则可以进一步输出两个同源环签名的签名者身份. “群体-指向”关联性指同一签名者利用同一群体对不同消息产生的签名之间具备关联性，“事件-指向”关联性则指签名者不论选取什么群体对事件进行签名，只要事件相同，其签名之间就具备关联性. 随后，Fujisaki 在文献[34]中首次提出了标准模型下可证明安全的关联环签名方案. 然而，上述方案均存在签名长度与群成员数量相关这一缺陷，当所选群成员数量较多时，必然导致签名长度过长，因此并不实用. 为了克服签名长度过长这一缺陷，Tsang 等人[30]利用文献[2]中的短环签名构造了签名长度固定的可关联环签名方案，其安全性基于 LD-RSA (Link Decisional RSA)假设，同时探讨了该短关联环签名在电子投票和电子现金中的应用. 但 Au 等人[31]通过研究指出文献[30]中关联环签名方案的安全模型存在缺陷并提出一个基于强 RSA 假设和强 DDH 假设的改进模型，给出了在新安全模型下可证明安全的签名长度固定的关联环签名方案. 随后，其又在文献[32]中首次给出可撤销关联(Revoke-iff-Linkability)环签名的定义和安全模型，提出一个基于身份(ID-Based)的签名长度固定的可撤销关联环签名方案，并在新安全模型下证明了该方案的安全性.

上述关联环签名由于加入强关联标签导致不具备强匿名性. 随后，研究者围绕弱关联性和强匿名性展开广泛的研究. 在指定验证者关联环签名中，只有指定的验证者才能将两个同源环签名进行关联，因此能够更好地保护签名者的匿名性，如文献[36]利用零知识证明和可验证秘密共享(Verifiable Secret Sharing，VSS)保证所有人都能验证签名的正确性，但只有指定群体中多于门限值的验证者合作才能重构出关联标签并验证签名的关联性，因此可有效约束普通签证者的关联权限，但这种方案需要较高的计算代价且签名长度较长. Chow 等人[37]于 2006 年提出“托管关联性”的概念，并利用基于身份的密码体制给出一个身份托管关联环签名方案，避免了 PKI 体制中复杂的公钥证书维护和管理问题. 所谓托管关联性，是指环签名的关联性只能被第三方托管机构验证，因此可进一步约束验证者的关联权限. 然而，该方案仍存在密钥托管问题并引入了计算量较大的双线性对运算. 随后，Tsang 等人给出一个无双线性对的基于身份关联门限环签名方案[33]及其相应的短签名方案[35]，其安全性基于随机预言机模型下的 DDH 假设.

上述方案虽然通过约束关联性的方式来增强匿名性，但仍然达不到强匿名性要求. 2008 年，Jeong 等人[38]首次提出“可选择”(Selective)关联环签名的概念，签名者可根据实际情况自主选择是否生成具有关联性的环签名，既可以直接生成关联环签名，也可以生成不具有关联性的普通环签名，且在不泄露身份的前提下签名者可以在事后将其生成的普通环签名进行关联. 该方案通过使用随机参数生成关联标签的方式实现了环签名的强匿名性和弱关联性. 可选择关联环签名对于保护举报者身份具有重要的应用价值. 例如，举报者利用可选择关联环签名先后揭发了两个秘密，且前一个秘密已被证实是可靠的，则举报者可在不泄露自己身份的前提下证明两个秘密之间的关联性，进而提高人们对后一个秘密的信任程度. 由于可选择关联环签名具备强匿名性，因此举报者的身份即使在权威机构的合作下也不会被暴露. 随后，文献[39]给出一个基于双线性映射的可选择关联环签名. 然而，已有的可选择关联环签名方案大多借助离散对数困难问题进行构造，如何构造基

于其他 NP 困难问题的可选择关联环签名是一个亟待研究的方向.

3 可选择关联可转换环签名方案安全模型

3.1 算法组成

定义 1. 可选择关联可转换环签名由以下 5 个多项式时间算法(G,S,V,LV,CV)组成.

(1)公私钥生成算法(G). $G(1^k)$是一个概率多项式时间算法(PPT),输入安全参数 k 后,输出私钥 sk 及其对应公钥 pk.

(2)签名算法(S). $S(1^k,m,L,sk)$是一个概率多项式时间算法(PPT),输入安全参数 k,消息 m,公钥集合 L 以及与 L 中某一公钥对应的私钥 sk 后,输出签名 σ.

(3)验证算法(V). $V(1^k,m,L,\sigma)$是一个概率多项式时间算法(PPT),输入安全参数 k,消息 m,公钥集合 L 和签名 σ 后,输出 1 或者 0,分别代表接受或者拒绝签名. 对于任意消息 m 和任意公钥集合 L,若想验证算法 $V(1^k,m,L,S(1^k,m,L,sk))=1$ 成立,要求公私钥对(sk,pk)必须是由 $G(1^k)$产生的,且 L 是由 pk 组成的公钥集合.

(4)关联性验证算法(LV). $LV(1^k,(L',m',\sigma'),(L'',m'',\sigma''))$是一个概率多项式时间算法$(PPT)$,当输入安全参数 k,两个公钥集合 L',L''和两对消息/签名对(m',σ')和(m'',σ'')后,输出 1 或者 0,分别代表满足关联性和不满足关联性. 对于任意两个公钥集合 L',L''和任意两对消息/签名对(m',σ')和(m'',σ''),若想验证算法 $LV(1^k,(L',m',\sigma'),(L'',m'',\sigma''))=1$ 成立,要求 L',L''是由 pk 组成的公钥集合,且(L',m',σ')和(L'',m'',σ'')分别满足 $V(1^k,m',L',\sigma')=1$ 和 $V(1^k,m'',L'',\sigma'')=1$.

(5)转换性验证算法(CV). $CV(1^k,m,L,\sigma)$是一个概率多项式时间算法(PPT),当输入安全参数 k,消息 m,公钥集合 L 和签名 σ 后,输出 1 或者 0,代表能够或不能确认签名 σ 为环中某一确定成员的合法签名. 对于任意消息 m 和任意公钥集合 L,若想验证算法 $CV(1^k,m,L,\sigma)=1$ 成立,要求 L 是由 pk 组成的公钥集合,且(m,σ)满足 $V(1^k,m,L,\sigma)=1$.

为简洁起见,在后续算法描述中省略了安全参数 k.

3.2 安全定义

定义 2. 若可选择关联可转换环签名满足以下性质,则称此方案是安全的.

(1)正确性. 若签名者按照正确的签名算法生成签名 σ,则 σ 通过验证算法 $V(1^k,m,L,\sigma)$的概率为 1.

(2)在适应性选择消息和选择公钥攻击下是存在性不可伪造. 设$(sk_i,pk_i)(i=1,2,\cdots,n)$是由 $G(1^{k_i})$生成的公私钥对,$k=\min(k_1,k_2,\cdots,k_n)$,$\hat{L}=\{pk_1,pk_2,\cdots,pk_n\}$,$SO(m',L')$为签名预言机. 当输入任意消息 m'和任意公钥集合 $L'\subseteq\hat{L}$,签名预言机输出一个签名 σ'满足 $V(m',L',\sigma')=1$. 如果对于任意一概率多项式时间算法 A 与签名预言机 SO 进行交互产生$(m,L,\sigma)\leftarrow A^{SO}(L)$满足$(m,L,\sigma)$没有在之前的询问-应答对中出现过,且 $V(m,L,\sigma)=1$ 概率在安全参数 k 下是可忽略的,其中 $L\subseteq\hat{L}$,则称可选择关联可转换环签名在抗适应性选择消息和选择公钥攻击下是存在性不可伪造的.

(3)强匿名性. 设$(sk_i,pk_i)(i=1,2,\cdots,n)$是由 $G(1^{k_i})$生成的公私钥对,$L=\{pk_1,pk_2,\cdots,pk_n\}$. 如果对于任意 L,任意消息 m 以及由 $S(1^k,m,L,sk)$生成的任意签名 σ,对于任意算法 A,输出 i 满足 $sk=sk_i(i=1,2,\cdots,n)$的概率仅为 $1/n$,则称方案具备强匿名性.

(4)关联性. 设$(sk_i,pk_i)(i=1,2,\cdots,n)$是由 $G(1^{k_i})$生成的公私钥对,$k=\min(k_1,k_2,\cdots,k_n)$,$\hat{L}=\{pk_1,pk_2,\cdots,pk_n\}$,$L',L''\subseteq\hat{L}$,任意两个消息$m',m''$的对应签名为$\sigma'\leftarrow S(1^k,m',L',sk_{\pi'})$,$\sigma''\leftarrow S(1^k,m'',L'',sk_{\pi''})$(其中,$\pi',\pi''\in\{1,2,\cdots,n\}$). 当签名 σ',σ''为同一用户所签时,则存在一个概率多项式时间(PPT)算法 F,能以不可忽略的概率得出 σ',σ''为同一人所签;而如果签名 σ',σ''不是由同一用户所签,则对任意概率多项式时间算法 F,得出签名为同一人所签的概率是可忽略的,则称此环签名方案是关联的.

(5)对非签名者的不可转换性. 对于非签名者,如其能成功将某一合法环签名 σ 转换为一个有效的普通数字签名的概率是可忽略的,则称方案对非签名者具备不可转换性,也即非签名者无法证明自己为真实签名者.

4 基于 RSA 公钥密码体制的可选择关联可转换环签名方案

4.1 初始化

对于 $i=1,2,\cdots,n$,每个用户 U_i 任意选择两个

大素数 p_i 和 q_i，计算

$$N_i=p_iq_i \text{ 和 } \varphi(N_i)=(p_i-1)(q_i-1).$$

随机选择整数 $e_i(1<e_i<\varphi(N_i))$，满足 $gcd(e_i,\varphi(N_i))=1$，计算整数 d_i，满足：

$$e_i\,d_i=1\bmod\varphi(N_i).$$

将 N_i 和 e_i 公布，并将 p_i，q_i 和 $\varphi(N_i)$ 保密.

选择安全哈希函数 $H_i:\{0,1\}^*\to Z_{N_i}$，用户 U_i 的公钥为 $pk_i=(N_i,e_i)$，私钥为 $sk_i=(p_i,q_i,d_i)$. $L=\{pk_1,pk_2,\cdots,pk_n\}$ 为 n 个用户的公钥集合.

4.2　签名生成

设消息 $m\in\{0,1\}^*$，公钥集合为 $L=\{(N_1,e_1),(N_2,e_2),\cdots,(N_n,e_n)\}$，签名者 U_k 私钥为 d_k，对应公钥为 (N_k,e_k)，其中 $1\le k\le n$，U_k 按如下步骤产生关联环签名.

(1) U_k 随机选择 a_k 和 r，满足 $1<a_k,r<\varphi(N_k)$，计算 a_k^{-1}，使得 $a_ka_k^{-1}=1\bmod\varphi(N_k)$，然后计算关联标签：$\tilde{e}=a_k^{-1}r\bmod\varphi(N_k)$.

(2) U_k 随机选择 $u,v\in Z_{N_k}$，计算：$c_{k+1}=H_{k+1}(L,\tilde{e},m,u,v)$.

(3) 对于 $i=k+1,k+2,\cdots,n-1,n,1,2,\cdots,k-1$，依次选择随机数 $s_i\in_R Z_{N_i}$ 和 $\tilde{s}_i\in_R Z_{N_i}$，然后计算：

$$c_{i+1}=H_{i+1}(L,\tilde{e},m,c_i+s_i^{e_i}\bmod N_i,c_i+\tilde{s}_i^{\tilde{e}}\bmod N_i).$$

注意：当 $i=n$ 时，令 $c_{i+1}=c_1$，$H_{i+1}=H_1$.

(4) 计算 r_k^{-1}，使得 $rr_k^{-1}=1\bmod\varphi(N_k)$，然后计算：$s_k=(u-c_k)^{d_k}\bmod N_k$，$\tilde{s}_k=(v-c_k)^{a_kr_k^{-1}}\bmod N_k$.

(5) 最后，输出签名：

$$\sigma_L(m)=(c_1,s_1,\cdots,s_n,\tilde{s}_1,\cdots,\tilde{s}_n,\tilde{e},r).$$

4.3　签名验证

验证者收到消息 m，签名 $\sigma_L(m)=(c_1,s_1,\cdots,s_n,\tilde{s}_1,\cdots,\tilde{s}_n,\tilde{e},r)$ 以及公钥集合 L 后按如下步骤验证签名的正确性：

首先，对于 $i=1,2,\cdots,n$，计算：

$$z_i=c_i+s_i^{e_i}\bmod N_i,\ \tilde{z}_i=c_i+\tilde{s}_i^{\tilde{e}}\bmod N_i.$$

然后，计算 $c_{i+1}=H_{i+1}(L,\tilde{e},m,z_i,\tilde{z}_i)(i\ne n)$.

最后，验证 $c_1=H_1(L,\tilde{e},m,z_n,\tilde{z}_n)$ 是否成立，若成立，则签名正确，否则签名无效.

4.4　关联性验证

签名者既能产生可关联的环签名，也能产生不可关联的环签名. 已知两个不同的环签名为

$$\sigma'_{L'}(m')=(c'_1,s'_1,\cdots,s'_n,\tilde{s}'_1,\cdots,\tilde{s}'_n,\tilde{e}',r'),$$

$$\sigma''_{L''}(m'')=(c''_1,s''_1,\cdots,s''_n,\tilde{s}''_1,\cdots,\tilde{s}''_n,\tilde{e}'',r'').$$

如果签名者 U_k 在两个签名中使用相同的 (a_k^{-1},r)，则这两个签名中的关联标签 $(\tilde{e},r)$ 相同，因此这两个环签名具备关联性. 如果签名者 U_k 在两个签名中使用不同的 $(a_k'^{-1},r')$ 和 $(a_k''^{-1},r'')$，则这两个签名中的关联标签 $(\tilde{e}',r')$ 和 $(\tilde{e}'',r'')$ 不相同，因此这两个环签名是不可关联的.

验证者只需验证两个签名中的关联标签 $(\tilde{e}',r')$ 和 $(\tilde{e}'',r'')$ 是否相同，便可验证签名是否具备关联性.

4.5　可转换性验证

在需要撤销匿名性的必要场合下，签名者 U_k 可以将环签名转换为普通的数字签名，从而证明自己为真实签名者.

假设 U_k 生成的签名为 $\sigma_L(m)=(c_1,s_1,\cdots,s_n,\tilde{s}_1,\cdots,\tilde{s}_n,\tilde{e},r)$，签名者 U_k 利用零知识协议 $Z=Proof[(d_k,a_k^{-1}):e_k=d_k^{-1}\bmod\varphi(N_k)\wedge\tilde{e}=a_k^{-1}r\bmod\varphi(N_k)]$，证明其拥有知识 (d_k,a_k^{-1})，从而将环签名 σ 转换成普通的数字签名. 验证者通过验证 Z 是否成立，便能确认签名 σ 是否为 U_k 所签.

5　安全性分析

定理 1.　正确性证明.

证明.　由签名过程可得

$$\begin{aligned}
c_{k+1}&=H_{k+1}(L,\tilde{e},m,u,v)\\
c_{k+2}&=H_{k+2}(L,\tilde{e},m,c_{k+1}+s_{k+1}^{e_{k+1}}\bmod N_{k+1},c_{k+1}+\tilde{s}_{k+1}^{\tilde{e}}\bmod N_{k+1})\\
&\vdots\\
c_n&=H_{n-1}(L,\tilde{e},m,c_{n-1}+s_{n-1}^{e_{n-1}}\bmod N_{n-1},c_{n-1}+\tilde{s}_{n-1}^{\tilde{e}}\bmod N_{n-1})\\
c_1&=H_1(L,\tilde{e},m,c_n+s_n^{e_n}\bmod N_n,c_n+\tilde{s}_n^{\tilde{e}}\bmod N_n)\\
c_2&=H_2(L,\tilde{e},m,c_1+s_1^{e_1}\bmod N_1,c_1+\tilde{s}_1^{\tilde{e}}\bmod N_1)\\
&\vdots\\
c_k&=H_{k-1}(L,\tilde{e},m,c_{k-1}+s_{k-1}^{e_{k-1}}\bmod N_{k-1},c_{k-1}+\tilde{s}_{k-1}^{\tilde{e}}\bmod N_{k-1}),
\end{aligned}$$

因为 $s_k=(u-c_k)^{d_k}\bmod N_k$，$\tilde{s}_k=(v-c_k)^{a_kr_k^{-1}}\bmod N_k$，$\tilde{e}=a_k^{-1}r\bmod\varphi(N_k)$，所以有

$$\begin{aligned}
c_{k+1}&=H_{k+1}(L,\tilde{e},m,c_k+s_k^{e_k}\bmod N_k,c_k+\tilde{s}_k^{\tilde{e}}\bmod N_k)\\
&=H_{k+1}(L,\tilde{e},m,c_k+(u-c_k)^{d_ke_k}\bmod N_k,\\
&\quad c_k+(v-c_k)^{a_kr_k^{-1}a_k^{-1}r}\bmod N_k)\\
&=H_{k+1}(L,\tilde{e},m,c_k+(u-c_k),c_k+(v-c_k))\\
&=H_{k+1}(L,\tilde{e},m,u,v).
\end{aligned}$$

而序列 $\{c_i\}$，$i=1,2,\cdots,n$ 在环签名的验证和产生过程中是一致的，因此 $c_1=H_1(L,\tilde{e},m,c_n+s_n^{e_n}\bmod N_n,c_n+\tilde{s}_n^{\tilde{e}}\bmod N_n)=H_1(L,\tilde{e},m,z_n,\tilde{z}_n)$ 成立.

所以,本文方案满足正确性. 证毕.

定理 2(适应性选择消息和选择公钥攻击下存在性不可伪造). 假设存在一个概率多项式时间(*PPT*)算法敌手 A,能对随机预言机 $H_i(i=1,2,\cdots,n)$最多进行 q_H次询问,对签名预言机 SO 最多进行 q_S次询问. 如果对某一消息 m 和某一公钥集合 L,A 能以不可忽略的概率 $\varepsilon>1/Q(k)$,在时间 τ 内伪造一个有效的签名 σ,满足 $V(m,L,\sigma)=1$(其中,Q 为一个多项式函数,k 为足够大的安全参数),即

$$\Pr(A(L)\rightarrow(m,\sigma):V(m,L,\sigma)=1)>\frac{1}{Q(k)}.$$

则存在一个 *PPT* 算法,在时间 $\eta\approx\tau$ 内,以不可忽略的概率 $\mu>\frac{1}{n(q_H+nq_S)Q(k)}$求解 RSA 困难问题.

证明. 设 $\hat{L}=\{pk_1,pk_2,\cdots,pk_n\}=\{(N_1,e_1),(N_2,e_2),\cdots,(N_n,e_n)\}$(见 3.1 节中的定义),$N=\min\{N_1,N_2,\cdots,N_n\}$. A 为一 *PPT* 敌手,能对随机预言机 $H_i(i=1,2,\cdots,n)$最多进行 q_H次询问,对签名预言机 SO最多进行q_S次询问. 假设 A 能以不可忽略的概率$\varepsilon>1/Q(k)$,在时间 τ 内伪造一个有效的签名 σ,即

$$\Pr(A(L)\rightarrow(m,\sigma):V(m,L,\sigma)=1)>\frac{1}{Q(k)},$$

其中:Q 为一多项式函数;q_H 和 q_S在安全参数 k 下仅能进行多项式次增长. 除了重复询问外,独立随机预言 H_i输出随机结果,SO 也能询问预言机 H_i,并且与 A 的询问输出保持一致.

通过调用黑盒子 A,*PPT* 仿真器 sim 能够仿真随机预言机,从而得到与每个 hash 函数 H_i和签名预言机 SO 一致的回答.

对于任一消息 m,任一公钥集合 $L\subseteq\hat{L}$,sim 通过模拟 SO,不用任何私钥,仅仅通过控制 H,便能按如下步骤生成一个有效的签名 σ.

(1)首先,sim 随机选择 $i\in_R\{1,2,\cdots,n\}$,$c_i\in_R N_i$.

(2)然后,随机选择 $b_k\in_R N/2$,$r\in_R N/2$,并计算 $\tilde{e}=b_k^{-1}r\bmod N_k/2$.

(3)接下来,对于 $i=k,k+1,k+2,\cdots,n-1,n,1,2,\cdots,k-1$,随机选择 $s_i\in_R Z_{N_i}$,$\tilde{s}_i\in_R Z_{N_i}$,计算 $z_i=c_i+s_i^{e_i}\bmod N_i$,$\tilde{z}_i=c_i+\tilde{s}_i^{\tilde{e}}\bmod N_i$,然后计算 $c_{i+1}=H_{i+1}(L,\tilde{e},m,z_i,\tilde{z}_i\bmod N_i)(i\neq k-1)$.

(4)然后,设置 $H_k(L,\tilde{e},m,z_{k-1},\tilde{z}_{k-1})=c_k$.

(5)最后,输出$(c_1,s_1,\cdots,s_n,\tilde{s}_1,\cdots,\tilde{s}_n,\tilde{e},r)$.

注意:当 $i=n$ 时,$H_{i+1}=H_1$,$c_{i+1}=c_1$. SO 像实际签名者为 U_k一样返回签名.

A 返回一个伪造签名,且同时对所有用于验证方程的 n 个随机预言询问均已询问过的概率不小于 $\frac{1}{Q(k)}-\frac{1}{q-q_H-nq_S}$,其中,$q$ 表示所有预言机应答的可能结果的个数,因为 $\frac{1}{q-q_H-nq_S}$值很小可忽略,所以 A 返回一个伪造签名,且同时对所有用于验证方程的 n 个随机预言询问均已询问过的概率不小于 $1/Q(k)$.

因此,当 A 伪造一个有效签名时,必定询问过与验证方程一致的 n 个对 H_i的询问,记这 n 个询问为 $X_{i_1},X_{i_2},\cdots,X_{i_n}$,$1\leq i_1<i_2<\cdots<i_n$. 当 SO 对 A 的询问生成签名时,SO 对 H_i的询问可忽略.

对于一个由 A 成功伪造的签名 σ,考虑被 A 询问过的所有用于验证的询问集合. 假设 $X_{i_1},X_{i_2},\cdots,X_{i_n}$为第一次出现满足验证的 n 个询问,其中 $1\leq i_1,i_2,\cdots,i_n$. 设 k 满足:

$$X_{i_k}\rightarrow H_k(L,\tilde{e},m,c_{k-1}+s_{k-1}^{e_{k-1}}\bmod N_{k-1},c_{k-1}+\tilde{s}_{k-1}^{\tilde{e}}\bmod N_{k-1}).$$

即 X_{i_k}对应于验证中对 H_k的询问. 称 k 为环签名 σ 的缺口.

如果 $i_1=l$,则记 A 伪造的签名 σ 为(l,k)-伪造签名,也即第一次出现与所有的验证相关的询问是第 l 次询问,且缺口等于 k. 在仿真开始时 sim 选择一对(l,k),其中 $1\leq l\leq q_H$,$1\leq k\leq n$,则 sim 能以不小于 $1/(n(q_H+nq_S)Q(k))$的概率确保自己的猜测是正确的,并且接收 $X_{i_k}\rightarrow H_k(L,\tilde{e},m,z_{k-1},\tilde{z}_{k-1})$,$X_{i_{k+1}}\rightarrow H_{k+1}(L,\tilde{e},m,z_k,\tilde{z}_k)$.

当询问 X_{i_k}发生时(询问 $X_{i_{k+1}}\rightarrow H_{k+1}(L,\tilde{e},m,c_k+s_k^{e_k}\bmod N_k,c_k+\tilde{s}_k^{\tilde{e}}\bmod N_k)=H_{k+1}(L,\tilde{e},m,z_k,\tilde{z}_k)$也已经发生,因为与验证相关的询问已经全部发生),sim 返回 c_k作为 $H_k(L,\tilde{e},m,z_{k-1},\tilde{z}_{k-1})$的值. 此时,由于 $c_k,z_k,\tilde{z}_k$均为已知,如果 A 能成功伪造环签名,则将输出满足关系式 $z_k=c_k+s_k^{e_k}\bmod N_k$和 $\tilde{z}_k=c_k+\tilde{s}_k^{\tilde{e}}\bmod N_k$的 s_k和 $\tilde{s}_k$,即 A 能够在不知道$(e_k,\tilde{e},N_k)$对应私钥 $\varphi(N_k)$的前提下从 $s_k^{e_k}\bmod N_k$和 $\tilde{s}_k^{\tilde{e}}\bmod N_k$中求解出 s_k和 $\tilde{s}_k$,这与 RSA 问题求解是困难的相矛盾. 因此,不可伪造性得证. 证毕.

定理 3(强匿名性). 本文方案具备强匿名性.

证明. 假设签名 $\sigma_L(m)=(c_1,s_1,\cdots,s_n,\tilde{s}_1,\cdots,\tilde{s}_n,\tilde{e})$是由签名者 U_k生成的一个合法签名. 由签名过程可知,$c_{k+1}=H_{k+1}(L,\tilde{e},m,u,v)$. $\tilde{e}$ 随机分布于

$(1,\varphi(N_K))$中，u 和 v 随机分布于 Z_{N_k} 中，且 H_k：$\{0,1\}^* \rightarrow Z_{N_k}$，所以 c_{k+1} 在 Z_{N_k} 中具有随机性. 对于 $i=k+1,k+2,\cdots,n-1,n,1,2,\cdots,k-1$，$c_{i+1}=H_{i+1}(L,\tilde{e},m,c_i+s_i^{e_i} \bmod N_i, c_i+\tilde{s}_i^{\tilde{e}} \bmod N_i)$，且 $s_i \in {}_RZ_{N_i}$，$\tilde{s}_i \in {}_RZ_{N_i}$，$H_i:\{0,1\}^* \rightarrow Z_{N_i}$，因此 c_{i+1} 也均匀随机分布于 $Z_{N_{i+1}}$ 中. 由上可知，对于所有的 $i=1,2,\cdots,n$，c_i 均随机分布于 Z_{N_i} 中. 所以签名 σ 中的 c_1 随机分布于 Z_{N_1} 中.

另外，对于签名 $\sigma_L(m)=(c_1,s_1,\cdots,s_n,\tilde{s}_1,\cdots,\tilde{s}_n,\tilde{e},r)$ 中的 s_i 和 $\tilde{s}_i$，除了 s_k 和 $\tilde{s}_k$ 是由计算所得外，其余 s_i 和 $\tilde{s}_i$ 都是从 Z_{N_i} 中随机选取的. 而 $s_k=(u-c_k)^{d_k} \bmod N_k$，$\tilde{s}_k=(v-c_k)^{a_k r_k^{-1}} \bmod N_k$，又因为 u,v 也是从 Z_{N_k} 中随机选择的，且上面已证得 $c_k \in {}_RZ_k$，所以 s_k 和 $\tilde{s}_k$ 也随机分布于 Z_{N_k} 中. 因此，对于任一固定的 (L,m)，$(s_1,s_2,\cdots,s_n)$ 和 $(\tilde{s}_1,\tilde{s}_2,\cdots,\tilde{s}_n)$ 分别有 $\prod_{i=1}^{n} N_i$ 种可能的解，且这些解具有等概性.

关联标签 $\tilde{e}=a_k^{-1} r \bmod \varphi(N_k)$，其中 $(1<a_k<\varphi(N_k),1<r<\varphi(N_k))$，且 a_k 和 r 均由签名者随机选取，所以 $(\tilde{e},r)$ 随机分布于 $(1,\varphi(N_K))$ 中.

综上可知，$\sigma_L(m)=(c_1,s_1,\cdots,s_n,\tilde{s}_1,\cdots,\tilde{s}_n,\tilde{e})$ 中的每一参数都具有随机性，所以对于任意算法 A，由签名信息 σ 输出某一 i，满足 $sk=sk_i$ $(i=1,2,\cdots,n)$ 的概率仅为 $1/n$，因此本方案具备强匿名性. 证毕.

定理 4(关联性). 对于某一签名 $\sigma_L(m)=(c_1,s_1,\cdots,s_n,\tilde{s}_1,\cdots,\tilde{s}_n,\tilde{e})$，若伪造者 A 能以不可忽略的概率产生与 $\sigma_L(m)$ 关联的环签名 $\sigma_L(m')=(c_1',s_1',\cdots,s_n',\tilde{s}_1',\cdots,\tilde{s}_n',\tilde{e})$，则存在一个 PPT 算法能以不可忽略的概率求解 RSA 困难问题.

证明. 定理 2 已证明，非环成员者不可能伪造合法环签名. 所以只需考虑环成员伪造与已知签名关联的环签名. 而环成员只拥有一个自己的私钥，而无法知道群中其他成员的私钥. 假设已知签名为 $\sigma_L(m)=(c_1,s_1,\cdots,s_n,\tilde{s}_1,\cdots,\tilde{s}_n,\tilde{e},r)$，$A$ 伪造的与 $\sigma_L(m)$ 关联的环签名为 $\sigma_L(m')=(c_1',s_1',\cdots,s_n',\tilde{s}_1',\cdots,\tilde{s}_n',\tilde{e},r)$. 因为 A 为环成员，所以其只知晓自己的私钥. 与定理 2 证明方法相同，假设 A 能成功伪造一个与 $\sigma_L(m)$ 关联的环签名 $\sigma_{L'}(m')$，则将输出 $\tilde{s}_k'$ 满足 $\tilde{z}_k=c_k+\tilde{s}_k'^{\tilde{e}} \bmod N_k$，其中，$\tilde{z}_k,c_k$ 均为已知，即 A 能够在不知道 $(\tilde{e},N_k)$ 对应私钥 $\varphi(N_k)$ 的情况下从 $\tilde{s}_k^{\tilde{e}} \bmod N_k$ 中求解出 $\tilde{s}_k$，这与 RSA 问题求解是困难的相矛盾. 因此，关联性得证. 证毕.

定理 5(对非签名者的不可转换性). 在随机预言模型下，若大数分解是困难的，则本方案对非签名者具备不可转换性.

证明. 假设某一合法签名为 $\sigma_L(m)=(c_1,s_1,\cdots,s_n,\tilde{s}_1,\cdots,\tilde{s}_n,\tilde{e},r)$，其中 $\tilde{e}=a_k^{-1} r$. 只有签名者可知 a_k^{-1} 的值，且 a_k^{-1} 随机分布于 $(1,\varphi(N_k))$ 中. 当签名者给出验证 $\Delta=Proof[(d_k,a_k^{-1}):e_k=d_k^{-1} \bmod \varphi(N_k) \wedge \tilde{e}=a_k^{-1} r \bmod \varphi(N_k)]$ 证明其拥有知识 (d_k,a_k^{-1}) 后，验证者验证 Δ 成立后，便能确认签名确实为 U_k 所签. 另外，在大整数分解难题下，由 $\tilde{e}$ 和 r 求解 a_k^{-1} 是困难的，所以对非签名者来说，证明其拥有知识 (d_k,a_k^{-1}) 是困难的，即将签名转换成普通签名的概率是可忽略的，因此本方案对非签名者具备不可转换性. 证毕.

6 性能及效率对比

本节通过与现有典型关联环签名方案的性能比较给出所提方案的运行效率评估. 表 1 对算法中用到的变量及运算符进行了定义.

表 1 相关变量及运算符定义

符号	定义
n	环成员总数
M	模乘运算的时间复杂度
I	模逆运算的时间复杂度
E	模指数运算的时间复杂度
EC_M	椭圆曲线上倍点运算的时间复杂度
EC_P	椭圆曲线上双线性映射运算的时间复杂度

表 2 给出本文方案与现有的典型关联环签名方案[27,29-31,33-34,36,38-39,43]的匿名性及效率比较结果.

为了更直观地对各个方案的计算量进行对比，此处根据文献[46]推算出的不同运算之间的等价换算关系对表 2 中的签名、验证以及总计算量进行换算. 根据文献[46]，假设 163 比特的椭圆曲线密码算法与 1024 比特的 RSA、DL 或 Diffi-Hellman 密码体制算法具有相同的安全强度. 则有 $E \approx 240M$，$E \approx 8.24EC_M$，$E \approx 3.2EC_P$，$I \approx 12M$. 可以推出 $E \approx 240M$，$EC_M \approx 29.13M$，$EC_P \approx 75M$，$I \approx 12M$. 对数据进行换算后的结果详见表 3 中的 $T(S)$ 估计值、$T(V)$ 估计值和 $T(S,V)$ 估计值.

为了更清晰地说明表中各方案的效率，取 $M=15\mu s$，$n'=20$，并将表 3 中的总时间复杂度显示于图 1 中.

从表 3 和图 1 可以看出，在签名及验证的总时间复杂度上，当环成员总数 n 较小时 $(n<8)$，本文方案效率仅次于文献[43]方案的效率，当 n 较大时

($n\geq 8$),本文方案效率也仅次于文献[30-31, 39, 43].其中文献[30]中的方案存在授权中心安全隐患,文献[30-31]中的方案仅能提供弱匿名性,文献[39,43]和本文方案则具备强匿名性,但文献[39]中,环中成员可以伪造跟其它环签名相关联的新环签名,存在安全隐患.对于签名长度,已有方案的环签名长度基本都是 $O(n)$,只有文献[30-31]提出的简短关联环签名长度为 $O(1)$,文献[34]为 $O(\sqrt{n})$,但这 3 个方案都只具备弱匿名性.特别的,本文算法在签名算法复杂度、验证算法复杂度和总时间复杂度均少于文献[34]算法,分别少$(n+4232\sqrt{n}+3820)M$,$(n+900\sqrt{n}+600)M$ 和$(2n+5132\sqrt{n}+4420)M$.而与文献[38]相比,本文算法在 n 较小时签名效率优势虽不明显,但由于验证算法复杂度比文献[38]算法少$(n+481)M$,因此总时间复杂度比文献[38]算法少$(2n+457)M$.

综合以上性能分析可知,本文方案在提供强匿名性的同时还具有很高的运算效率.

表 2 (1,n)关联环签名的匿名性及效率比较

方案	签名大小	匿名性	签名时间复杂度 $T(S)$	验证时间复杂度 $T(V)$	总时间复杂度 $T(S,V)$
文献[27]	$O(n)$	弱匿名性	$(4n-1)E+(2n-1)M$	$4nE+2nM$	$(8n-1)E+(4n-1)M$
文献[29]	$O(n)$	弱匿名性	$(6n-2)E+(2n-1)M$	$6nE+3nM$	$(12n-2)E+(5n-1)M$
文献[30]	$O(1)$	弱匿名性	$(n+13)E+7M$	$11E+7M$	$(n+24)E+14M$
文献[31]	$O(1)$	弱匿名性	$(n+13)E+7M$	$11E+7M$	$(n+24)E+14M$
文献[36]	$O(n)$	弱匿名性	$(4n+8n')E+(3n+n'-1)M$	$(4n+n')E+2nM$	$(8n+9n')E+(5n+n'-1)M$
文献[38]	$O(n)$	强匿名性	$2nE+(n+1)M$	$(2n+2)E+(n+1)M$	$(4n+2)E+(2n+2)M$
文献[43]	$O(n)$	强匿名性	$(2n-1)EC_P+(n+1)EC_M$	$2nEC_P+nEC_M$	$(4n-1)EC_P+(n+1)EC_M$
文献[33]	$O(n)$	弱匿名性	$(9n+4)E+4nM$	$10nE+5nM$	$(19n+4)E+9nM$
文献[34]	$O(\sqrt{n})$	弱匿名性	$(2n+17\sqrt{n}+16)E+(n+2\sqrt{n}+5)M+2\sqrt{n}EC_P$	$2nE+nM+(2n+12\sqrt{n}+8)EC_P$	$(4n+17\sqrt{n}+16)E+(2n+2\sqrt{n}+5)M+(2n+14\sqrt{n}+8)EC_P$
文献[39]	$O(n)$	强匿名性	$(4n-2)EC_M+M+I$	$2nEC_M+(n+1)EC_P$	$(6n-2)EC_M+(n+1)EC_P+M+I$
本文方案	$O(n)$	强匿名性	$2nE+M+2I$	$2nE$	$4nE+M+2I$

注:表中 n'为文献[36]中指定的可关联团体成员总数.

表 3 (1,n)关联环签名的匿名性及效率比较(评估值)

方案	签名大小	匿名性	签名时间复杂度 $T(S)$估计值	验证时间复杂度 $T(V)$估计值	总时间复杂度 $T(S,V)$估计值
文献[27]	$O(n)$	弱匿名性	$(962n-241)M$	$962nM$	$(1924n-242)M$
文献[29]	$O(n)$	弱匿名性	$(1442n-481)M$	$(1443n+240)M$	$(2885n-241)M$
文献[30]	$O(1)$	弱匿名性	$(240n+3127)M$	$2647M$	$(240n+5774)M$
文献[31]	$O(1)$	弱匿名性	$(240n+3127)M$	$2647M$	$(240n+5774)M$
文献[36]	$O(n)$	弱匿名性	$(966n+1921n'-1)M$	$(962n+240n')M$	$(1992n+2161n'-1)M$
文献[38]	$O(n)$	强匿名性	$(481n+1)M$	$(481n+481)M$	$(962n+482)M$
文献[43]	$O(n)$	强匿名性	$(179.13n-45.87)M$	$179.13nM$	$(358.26n-45.87)M$
文献[33]	$O(n)$	弱匿名性	$(2164n+960)M$	$2405nM$	$(4569n+960)M$
文献[34]	$O(\sqrt{n})$	弱匿名性	$(481n+4232\sqrt{n}+3845)M$	$(481n+900\sqrt{n}+600)M$	$(962n+5132\sqrt{n}+4445)M$
文献[39]	$O(n)$	强匿名性	$(114.2n-45.6)M$	$(133.24n+75)M$	$(247.44n+29.4)M$
本文方案	$O(n)$	强匿名性	$(480n+25)M$	$480nM$	$(960n+25)M$

注:表中 n'为文献[36]中指定的可关联团体成员总数.

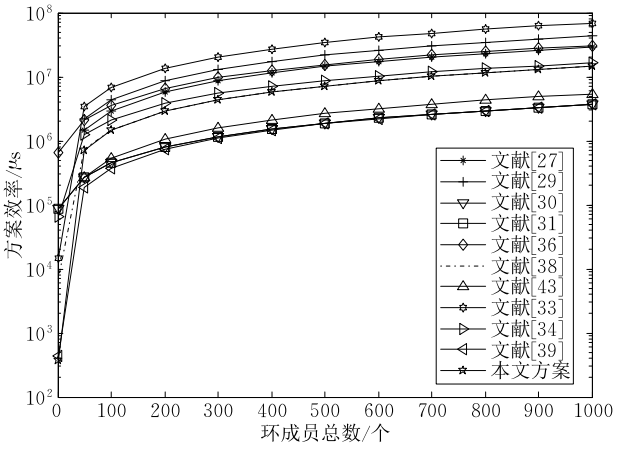


图 1 (1,n)关联环签名效率对比图

7 算法实现

本文所提方案可通过调用 WinNTL 和 OpenSSL 密码函数库利用 C++编程实现,各阶段算法如下.

算法 1. 初始化.

输入:用户$\{U_1,U_2,\cdots,U_n\}$

输出:用户公钥集合 $L=\{pk_i=(N_i,e_i)\}_{i=1,\cdots,n}$,哈希函数 H

begin

$L\leftarrow\varnothing$

select $H_i:\{0,1\}^*\rightarrow Z_{N_i}$

for $i=1$ to n do

select random p_i, q_i

$N_i = p_i \times q_i$

$\varphi(N_i) = (p_i - 1) \times (q_i - 1)$

select random e_i from 1 to $\varphi(N_i)$

$d_i = \mathrm{InvMod}(e_i, \varphi(N_k))$ //$d_i = e_i^{-1} \bmod \varphi(N_i)$

send $sk_i = (p_i, q_i, d_i)$ to U_i

$L \leftarrow L \cup pk_i = (N_i, e_i)$

output L, H

end

算法 2.　签名生成.

输入：消息 m，签名者 U_k，用户公钥集合 L

输出：签名 $\sigma_L(m)$

begin

$\sigma_L(m) \leftarrow \varnothing$

select random a_k, r from 1 to $\varphi(N_k)$

$a_k^{-1} = \mathrm{InvMod}(a_k, \varphi(N_k))$

$\tilde{e} = \mathrm{MulMod}(a_k^{-1}, r, \varphi(N_k))$//关联标签 $\tilde{e} = a_k^{-1} r \bmod \varphi(N_k)$

$\sigma_L(m) \leftarrow \sigma_L(m) \cup \tilde{e} \cup r$

select random u, v from 1 to $N_k - 1$

$c_{k+1} = H_{k+1}(L, \tilde{e}, m, u, v)$

$\sigma_L(m) \leftarrow \sigma_L(m) \cup c_{k+1}$

for $i = k+1$ to n do

select random $s_i, \tilde{s}_i$ from 1 to $N_i - 1$

$c_{i+1} = H_{i+1}(L, \tilde{e}, m, c_i + s_i^{e_i} \bmod N_i, c_i + \tilde{s}_i^{\tilde{e}} \bmod N_i)$

$\sigma_L(m) \leftarrow \sigma_L(m) \cup c_{i+1}$

$c_1 = c_{n+1}$, $H_1 = H_{n+1}$

for $i = 1$ to $k-1$ do

select random $s_i, \tilde{s}_i$ from 1 to $N_i - 1$

$c_{i+1} = H_{i+1}(L, \tilde{e}, m, c_i + s_i^{e_i} \bmod N_i, c_i + \tilde{s}_i^{\tilde{e}} \bmod N_i)$

$\sigma_L(m) \leftarrow \sigma_L(m) \cup c_{i+1}$

$r_k^{-1} = \mathrm{InvMod}(r, \varphi(N_k))$

$s_k = (u - c_k)^{d_k} \bmod N_k$

$\tilde{s}_k = (v - c_k)^{a_k^{r_k^{-1}}} \bmod N_k$

$\sigma_L(m) \leftarrow \sigma_L(m) \cup s_k \cup \tilde{s}_k$

output $\sigma_L(m) = (c_1, s_1, \cdots, s_n, \tilde{s}_1, \cdots, \tilde{s}_n, \tilde{e}, r)$

end

算法 3.　签名验证.

输入：消息 m，签名 $\sigma_L(m)$，用户公钥集合 L

输出：若签名有效，则输出 true，否则为 false

begin

for $i = 1$ to n do

$z_i = c_i + s_i^{e_i} \bmod N_i$, $\tilde{z}_i = c_i + \tilde{s}_i^{\tilde{e}} \bmod N_i$

if $i != n$ then $c_{i+1} = H_{i+1}(L, \tilde{e}, m, z_i, \tilde{z}_i)$

if $c_1 == H_1(L, \tilde{e}, m, z_n, \tilde{z}_n)$ then return(true)

else return(false)

end

算法 4.　关联性验证.

输入：消息 m_1，签名 $\sigma_L(m_1)$，消息 m_2，签名 $\sigma_L(m_2)$

输出：若两签名关联，则输出 true，否则为 false

begin

$\sigma_L(m_1) = (c_1', s_1', \cdots, s_n', \tilde{s}_1', \cdots, \tilde{s}_n', \tilde{e}', r')$,

$\sigma_L(m_2) = (c_1'', s_1'', \cdots, s_n'', \tilde{s}_1'', \cdots, \tilde{s}_n'', \tilde{e}'', r'')$

if $(\tilde{e}', r') == (\tilde{e}'', r'')$ then return(true)

else return(false)

end

8　结　论

关联环签名在电子现金、电子投票、Ad hoc 等领域有着重要的应用价值. 本文针对现有关联环签名方案均建立在离散对数困难问题基础上，且绝大多数方案仅具备强关联性和弱匿名性的问题，提出了一个基于大整数分解难题和 RSA 公钥密码体制的可选择关联可转换环签名方案，并在随机预言机模型下证明了其安全性. 方案不仅具备强匿名性，而且签名者可以自行选择所产生签名的关联性. 同时，在必要场合，又能够将环签名转化为普通的数字签名. 通过性能分析表明本文方案在保障上述安全特性的前提下具有较高的实现效率. 所提方案可用于设计安全高效的电子现金、电子投票和匿名揭发协议，并可扩展为基于 RSA 的可选择门限环签名方案. 如何在标准模型下构造该类方案是有待进一步研究和解决的问题. 此外，如何设计基于其他数学难题，如格、编码和多变量二次方程组的关联环签名方案也是值得研究的方向.

参　考　文　献

[1] Rivest R, Shamir A, Tauman Y. How to leak a secret// Proceedings of the Advances in Cryptology-ASIACRYPT 2001. Gold Coast, Australia, 2001: 552-565

[2] Dodis Y, Kiayias A, Nicolosi A, Shoup V. Anonymous identification in ad hoc groups//Proceedings of the Advances in Cryptology-EUROCRYPT 2004. Interlaken, Switzerland, 2004: 609-626

[3] Shacham H, Waters B. Efficient ring signatures without random oracles//Proceedings of the Public Key Cryptography 2007(PKC 2007). Beijing, China, 2007: 166-180

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

[5] Bose P, Das D, Chandrasekharan P. Constant size ring signature without random oracle//Proceedings of the 20th Australasian Conference on Information Security and Privacy (ACISP 2015). Queensland, Australia, 2015: 230-247

[6] Shim K. An efficient ring signature scheme from pairings. Information Sciences, 2015, 300: 63-69

[7] Wang K, Yi M, Susilo W. Identity-based quotable ring signature. Information Sciences, 2015, 321: 71-89

[8] Gritti C, Susilo W, Plantard T. Logarithmic size ring signatures without random oracles. IET Information Security, 2016, 10(1): 1-7

[9] Brakerski Z, Kalai Y T. A framework for efficient signatures, ring signatures and identity based encryption in the standard model. Iacr Cryptology ePrint Archive, 2010: 1-44

[10] Cayrel P, Lindner R, Rückert M, Silva R. A lattice-based thresh-old ring signature scheme//Proceedings of the Progress in Cryptology-LATINCRYPT 2010. Puebla, Mexico, 2010: 255-272

[11] Wang Feng-He, Hu Yu-Pu, Wang Chun-Xiao. A lattice-based ring signature scheme from bonsai trees. Journal of Electronics & Information Technology, 2010, 32(10): 2400-2403(in Chinese)
(王凤和, 胡予濮, 王春晓. 格上基于盆景树模型的环签名. 电子与信息学报, 2010, 32(10): 2400-2403)

[12] Wang J, Sun B. Ring signature schemes from lattice basis delegation. Information and Communications Security, 2011, 7043(1): 15-28

[13] Tian Miao-Miao, Huang Liu-Sheng, Yang Wei. Efficient lattice-based ring signature scheme. Chinese Journal of Computers, 2012, 35(4): 712-718(in Chinese)
(田苗苗, 黄刘生, 杨威. 高效的基于格的环签名方案. 计算机学报, 2012, 35(4): 712-718)

[14] Aguilar M C, Bettaieb S, Boyen X, et al. Adapting Lyubashevsky's signature schemes to the ring signature setting//Proceedings of the Progress in Cryptology—AFRICACRYPT 2013. Cairo, Egypt, 2013: 1-25

[15] Geontae N, Ji Y, Ik R. Strongly unforgeable ring signature scheme from lattices in the standard model. Journal of Applied Mathematics, 2014, 2014(1): 1-12

[16] Wang S, Ma R, Zhang Y, et al. Ring signature scheme based on multivariate public key cryptosystems. Computers & Mathematics with Applications, 2011, 62(10): 3973-3979

[17] Liu X, Zhao Y. Variant scheme of ring signature based on multivariate public key cryptosystems. Computer Engineering, 2015, 41(2): 96-99

[18] Zheng D, Li X, Chen K. Code-based ring signature scheme. Chinese Journal of Electronics, 2007, 16(3): 154-157

[19] Melchor C A, Cayrel P L, Gaborit P. A new efficient threshold ring signature scheme based on coding theory//Proceedings of the 2nd International Workshop on Post-Quantum Cryptography. Cincinnati, USA, 2008: 1-16

[20] Dallot L, Vergnaud D. Provably secure code-based threshold ring signatures//Proceedings of the 12th IMA Conference on Cryptography and Coding. Cirencester, England, 2009: 222-235

[21] Liu M, Han Y, Yang X. A ring signature based on LDGM codes. Communications in Computer and Information Science, 2016, (590): 155-162

[22] Xiong H, Chen Z, Li F. Bidder-anonymous English auction protocol based on revocable ring signature. Expert Systems with Applications, 2012, 39(8): 7062-7066

[23] Wang Hua-Qun, Qin Bo. Cryptanalysis and improvements of some ring signature and its extended signature schemes. Chinese Journal of Computers, 2012, 35(5): 1052-1058(in Chinese)
(王化群, 秦波. 一些环签名及其扩展签名方案的安全性分析及改进. 计算机学报, 2012, 35(5): 1052-1058)

[24] Deng L, Zeng J. Two new identity-based threshold ring signature schemes. Theoretical Computer Science, 2014, 535: 38-45

[25] Rajabzadeh Asaar M, Salmasizadeh M, Susilo W. A short identity-based proxy ring signature scheme from RSA. Computer Standards & Interfaces, 2015, 38: 144-151

[26] Rajabzadeh Asaar M, Salmasizadeh M, Susilo W. A provably secure identity-based proxy ring signature based on RSA. Security and Communication Networks, 2015, 8(7): 1223-1236

[27] Liu J, Wei V, Wong D. Linkable spontaneous anonymous group signature for ad hoc groups//Proceedings of the 9th Australasian Conference on Information Security and Privacy (ACISP 2004). Sydney, Australia, 2004: 325-335

[28] Zheng D, Wei V, Chen K. GDH group-based signature scheme with linkability. IEE Proceedings of Communications, 2006, 153(5): 639-644

[29] Tsang P, Wei V, Chan T, et al. Separable linkable threshold ring signatures//Proceedings of the Progress in Cryptology—INDOCRYPT 2004. Chennai, India, 2005: 384-398

[30] Tsang P, Wei V. Short linkable ring signatures for E-voting, E-cash and attestation//Proceedings of the 1st Information Security Practice and Experience (ISPEC 2005). Singapore, 2005: 48-60

[31] Au M, Chow S, Susilo W, Tsang P. Short linkable ring signatures revisited//Proceedings of the Public Key Infrastructure 2006. Turin, Italy, 2006: 101-115

[32] Au M, Liu J, Susilo W, Yuen T. Constant-size ID-based linkable and revocable-iff-linked ring signature//Proceedings of the Progress in Cryptology—INDOCRYPT 2006. Kolkata, India, 2006: 364-378

[33] Tsang P, Au M, Liu J, et al. A suite of non-pairing ID-based threshold ring signature schemes with different levels of anonymity//Proceedings of the 4th International Conference on Provable Security (ProvSec'10). Malacca, Malaysia, 2010: 166-183

[34] Fujisaki E. Sub-linear size traceable ring signatures without random oracles//Proceedings of the 11th International Conference on Topics in Cryptology (CT-RSA'11). San Francisco, America, 2011: 393-415

[35] Au M, Liu J, Susilo W, Yuen T. Secure ID-based linkable and revocable-iff-linked ring signature with constant-size construction. Theoretical Computer Science, 2013, 469: 1-14

[36] Liu J, Susilo W, Wong D. Ring signatures with designated linkability//Proceedings of the Advances in Information and Computer Security (IWSEC 2006). Kyoto, Japan, 2006: 104-119

[37] Chow S, Susilo W, Yuen T. Escrowed linkability of ring signatures and its applications//Proceedings of the Progress in Cryptology-VIETCRYPT 2006. Hanoi, Vietnam, 2006: 175-192

[38] Jeong I, Kwon J, Lee D. Ring signature with weak linkability and its applications. IEEE Transactions on Knowledge and Data Engineering, 2008, 20(8): 1145-1148

[39] Li Wei, Tang Ming-Wei, Fan Ming-Yu. Pairing-based linkable and convertible ring signature scheme without random oracle. Journal of Xihua University (Natural Science), 2013, 32(2): 1-4(in Chinese)
(李伟，唐明伟，范明钰. 标准模型下基于线性对的选择关联可转换环签名方案. 西华大学学报(自然科学版)，2013，32(2)：1-4)

[40] Lee K, Wen H, Hwang T. Convertible ring signature. IEEE Proceedings Communication, 2005, 152(4): 411-414

[41] Ren J, Ham L. Ring signature based on ElGamal signature//Proceedings of the 1st International Conference on Wireless Algorithms, Systems, and Applications (WASA 2006). Xi'an, China, 2006: 445-456

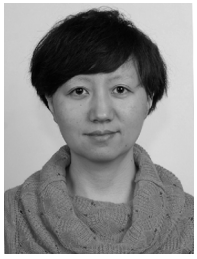
[42] Ren J, Ham L. Generalized ring signatures. IEEE Transactions on Dependable and Secure Computing, 2008, 5(3): 155-162

[43] Wang Shao-Hui, Zheng Shi-Hui, Zhan Tao. Identity-based linkable and convertible ring signature. Journal of Electronics & Information Technology, 2008, 30(4): 995-998 (in Chinese)
(王少辉，郑世慧，展涛. 基于身份的可链接和可转换环签名. 电子与信息学报，2008，30(4)：995-998)

[44] Hwang J, Chang K, Cho H, et al. Collusion-resistant convertible ring signature schemes. Science China Information Sciences, 2015, 58: 1-16

[45] Wang H, Zhang F, Sun Y. Cryptanalysis of a generalized ring signature schemes. IEEE Transactions on Dependable and Secure Computing, 2009, 6(2): 149-151

[46] Juang W S. RO-cash: An efficient and practical recoverable pre-paid offine e-cash scheme using bilinear pairings. Journal of Systems and Software, 2010, 83(1): 638-645



ZHANG Wen-Fang, born in 1978, Ph. D., associate professor. Her current research interests include cryptography and information security.

XIONG Dan, born in 1989, M. S. candidate. Her current research interests include information security and ring signatures.

WANG Xiao-Min, born in 1974, Ph. D., professor. His current research interests include information security and rail-trafic secure controlling.

CHEN Zhen, born in 1990, M. S. candidate. His current research interests include information security and attribute-based cryptosystems.

LIU Xu-Dong, born in 1990, M. S. candidate. His current research interests include ring signatures and attribute-based cryptosystems.

Background

As an important branch of group-oriented cryptosystems, ring signature schemes allow members of a group to sign messages on behalf of the group without any necessity to reveal their identities, i. e., providing unconditional signer anonymity. Applications of ring signature schemes include whistle blowing, anonymous membership authentication for ad hoc groups, perfect concurrent signature and et al. Linkable ring signatures were first proposed by Liu et al. in 2004. In this notion, the identity of the signer in a ring signature remains anonymous, but two ring signatures can be linked if they are signed by the same signer. Linkable ring signatures are suitable in many different practical applications, such as e-voting, in which linkability make it possible to allow the public to detect any signer who has produced two or more votes. Till now, there are a couple of tag-based linkable ring signature schemes having been proposed. However, most of

them are based on discrete logarithm public key cryptosystems, and the vast majority of schemes only have the characteristics of weak anonymity and strong linkability. In this paper, a selectively linkable and convertible ring signature based on RSA public key cryptosystem was proposed, and a formal security model of this kind of ring signature was presented. Our proposed scheme is proven to be unconditionally anonymous and existentially unforgeable against adaptive chosen plaintext and chosen public-key attacks under the random oracle model. Besides, in necessary occasions, the signer can convert the ring signature into ordinary digital signature to prove himself as a real signer on the premise of not revealing secret parameters. The performance analysis also shows that the proposed scheme has a high operating efficiency.

This paper is supported by the National Natural Science Foundation of China (Nos. 61003245, 61371098), the Basic Application Research Project of Sichuan Province of China (No. 2015JY0182), and the Fundamental Research Funds for the Central Universities of China (No. SWJTU11CX041). The research of these projects focuses on information security resolutions and the related cryptographic algorithms in large-scale distributed networks.

The authors have published a couple of related research works in Information Sciences, Security and Communication Networks, Telecommunication systems, Journal of Communications, Acta Electronica Sinica and et al.