

基于SM2数字签名算法的环适配器签名方案

许馨月^{1,2}, 徐淑奖^{1,2}, 王连海^{1,2}, 张淑慧^{1,2}, 邵蔚^{1,2}, 王启正^{1,2}

(1. 齐鲁工业大学(山东省科学院)山东省计算中心(国家超级计算济南中心),

算力互联网与信息安全教育部重点实验室, 山东 济南 250014;

2. 山东省基础科学研究中心(计算机科学), 山东省工业网络与信息系统安全重点实验室, 山东 济南 250014)

摘 要: 适配器签名能够在不依赖可信第三方的情况下保障跨链交易的原子性, 但大多数适配器签名算法无法保障用户身份的隐私性。尤其是多数方案并非基于国产密码算法设计, 这些方案自主可控性差。针对上述问题, 提出了基于SM2数字签名算法的环适配器签名方案。签名者首先利用环签名生成预签名; 预签名验证通过后, 将预签名与一个秘密值结合, 进而适配为完整签名; 任何拥有预签名及其完整签名的用户可以提取出秘密值。该环适配器签名方案在预签名阶段利用环签名的性质保障签名者身份的隐私性, 同时利用适配器签名保障交易的原子性, 兼具身份隐私保护及交易原子性的优异特性。其安全性可规约到离散对数困难问题。在随机预言机模型下, 证明了该方案满足预签名可适配性、预签名正确性、选择消息攻击下的存在不可伪造性、证据可提取性和匿名性。理论分析表明, 该环适配器签名方案与现有环适配器签名方案的时间开销及通信开销相当。该方案极大地拓展了国密签名算法在环适配器签名领域的应用, 尤其适用于跨链支付等隐私保护领域。

关键词: 区块链; SM2数字签名; 环适配器签名

中图分类号: TP309

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2026003

Ring adaptor signature scheme based on SM2 digital signature algorithm

Xu Xinyue^{1,2}, Xu Shujia^{1,2}, Wang Lianhai^{1,2}, Zhang Shuhui^{1,2}, Shao Wei^{1,2}, Wang Qizheng^{1,2}

1. Key Laboratory of Computing Power Network and Information Security, Ministry of Education, Shandong Computer Science Center (National Supercomputer Center in Jinan), Qilu University of Technology (Shandong Academy of Sciences), Jinan 250014, China

2. Shandong Provincial Key Laboratory of Industrial Network and Information System Security, Shandong Fundamental Research Center for Computer Science, Jinan 250014, China

Abstract: Adaptor signature can guarantee the atomicity of cross-chain transactions without relying on trusted third parties, but most adaptor signature algorithms fail to protect the privacy of user identities. Moreover, most of these

收稿日期: 2025-03-04; 修回日期: 2025-09-23

通信作者: 徐淑奖, xsj@qlu.edu.cn

基金项目: 山东省重点研发计划 (No.2025CXPTWZ003, No.WSR2024004); 泰山学者项目 (No.tsqn202312231); 山东省自然科学基金 (No.ZR2024MF104, No.ZR2023QF129); 济南市新高校二十条项目 (No.202228017); 齐鲁工业大学(山东省科学院)科教产融合创新试点工程项目 (No.2024ZDZX08)

Foundation Items: The Shandong Provincial Key Research and Development Program (No.2025CXPTWZ003, No.WSR2024004), The Taishan Scholars Program (No.tsqn202312231), The Shandong Natural Science Foundation of China (No.ZR2024MF104, No.ZR2023QF129), The New 20 Project of Higher Education of Jinan, China (No.202228017), The Pilot Project for Integrated Innovation of Science, Education, and Industry of Qilu University of Technology (Shandong Academy of Sciences) (No.2024ZDZX08)

schemes are not based on domestic cryptographic algorithms, resulting in poor autonomy and controllability. To address these issues, a ring adaptor signature scheme based on the SM2 digital signature algorithm was proposed. The signer first generates a pre-signature using a ring signature; after the pre-signature is verified, it is combined with a secret value to adapt to a complete signature; any user with the pre-signature and its complete signature can extract the secret value. This ring adaptor signature scheme uses the properties of ring signatures to protect the privacy of the signer's identity in the pre-signature stage, while using adaptor signatures to ensure the atomicity of transactions, and combines the excellent characteristics of both identity privacy protection and transaction atomicity. Its security can be reduced to the discrete logarithm problem. Under the random oracle model, it was proved that the proposed scheme satisfies pre-signature adaptability, pre-signature correctness, existential unforgeability under chosen message attacks, witness extractability, and anonymity. Theoretical analysis shows that the time and communication overhead of this ring adaptor signature scheme is comparable to that of existing ring adaptor signature schemes. This scheme greatly expands the application of domestic cryptographic signature algorithms in the field of ring adaptor signatures, which is especially pertinent to the field of privacy protection in cross-chain payments.

Keywords: blockchain, SM2 digital signature, ring adaptor signature

0 引言

数字化时代, 区块链技术凭借去中心化、不可篡改、可追溯等特性, 正在深刻改变传统的支付与交易模式, 有望重塑货币支付体系^[1]。随着异构区块链网络的不断涌现, 跨链交易需求日益增长。然而, 若跨链交易无法在涉及的所有链上实现同步成功或失败, 将导致资产状态不一致、数据不完整, 进而面临资产丢失或双重支付等风险, 给用户带来重大经济损失并引发信任危机^[2]。因此, 保障跨链交易的原子性至关重要^[3]。

为满足区块链系统对交易原子性的迫切需求, Poelstra^[4]于2017年首次在区块链社区中提出适配器签名(又称无脚本脚本)这一密码学原语。作为传统数字签名的扩展, 适配器签名将数字签名算法与困难关系的状态—证据对相结合, 兼具签名验证和证据提取功能^[5]。签名者使用私钥对消息及其对应的困难关系进行预签名, 只有持有困难关系证据的用户, 才能将预签名转换为有效的完整签名。此外, 用户可以依据预签名及其对应的完整签名, 反向提取出该困难关系的证据。适配器签名的提出, 为网络交易提供了一种无须依赖可信第三方即可实现原子交换的技术路径^[6-7]。得益于关键步骤在链下完成, 适配器签名突破了区块链脚本语言的固有限制, 具有较强的兼容性, 且已被证实可以应用于支付通道网络, 提升了区块链的可扩展性^[8-11]。

在适配器签名的研究演进中, 相关方案不断迭代优化。2019年, Malavolta等^[12]基于单向同态函数设计了适配器签名方案, 并将其应用于支付通道网络的构建。2021年亚洲密码学年会上, Aumayr等^[13]从理论层面系统地规范了适配器签名的形式化定义和标准安全模型, 该模型此后成为构造适配器签名方案和开展安全证明的通用框架。同年, 彭聪等^[14]将SM2数字签名算法扩展为SM2适配器签名方案。2023年, Bao等^[15]基于IEEE P1363标准中基于身份的签名算法, 设计了一种基于身份的适配器签名方案。

为保证签名信息的隐私性, Qin等^[16]于2023年提出盲适配器签名和灵活盲条件签名, 并实例化了基于椭圆曲线数字签名算法(ECDSA)算法的盲适配器签名方案。2024年, 胡小明等^[17]设计了盲适配器签名系统模型和安全模型, 并构造了基于SM2签名算法的盲适配器签名方案。

尽管现有方案在签名隐私性上有所突破, 但仍未能充分解决交易过程中用户身份隐私保护问题。身份隐私是指用户的真实身份与区块链交易地址之间的关联关系^[18]。由于区块链上的所有交易记录均公开可查, 攻击者可以通过分析交易数据挖掘交易地址之间的关联性, 进而推断出用户的真实身份。现有适配器签名方案通常要求签名者公开其公钥。例如, 在签名验证阶段, 签名者的公钥直接与签名绑定。这种机制使得签名者的身份具有可追踪性, 存在个人信息泄露风险。对于高度重视隐私保护的应用场景而言, 这无疑

构成了重大安全隐患。身份隐私保护旨在将实际交易用户隐匿于无关用户群体中,在不泄露参与者真实身份的前提下,确保可以验证交易的有效性。为弥补适配器签名在匿名性上的缺陷,环适配器签名被提出。其具有匿名性和不可伪造性,能够有效实现身份隐私保护。2022年, Sui等^[19]利用可验证连续单向函数生成系列状态-证据对,进而提出连续适配器签名的通用构造方法。2024年, Wang等^[20]提出可链接环适配器签名的通用结构,并构造了匿名增强型多跳锁。

然而,现有环适配器签名大多是基于非国产数字签名算法设计的,难以实现自主可控,存在安全隐患。针对这一问题,本文提出一种基于国密SM2算法^[21]的环适配器签名方案,并在预言机模型下完成了方案安全性和匿名性的证明。理论分析结果表明,该方案在时间和通信开销方面与现有环适配器签名方案处于同一水平。本文方案采用国密算法构建,具有较好的自主可控性,在区块链等领域具有广阔的应用前景,尤其适用于对隐私保护要求较高且需要采用国产密码算法的场景。

1 预备知识

本节给出本文所用符号的说明,并介绍方案设计涉及的相关理论基础。

1.1 符号说明

为便于后续算法描述,本节首先给出本文涉及的符号描述。

p : 大素数。

F_p : 有限域。

$E(F_p)$: 定义在 F_p 上的椭圆曲线。

$\mathbb{G}$: $E(F_p)$ 上的点构成的加法循环群。

q : 加法循环群 $\mathbb{G}$ 的阶。

G : 加法循环群 $\mathbb{G}$ 的基点。

$\Pi_{\mathbb{G}}$: 加法循环群 $\mathbb{G}$ 上的困难关系, $\Pi_{\mathbb{G}} \subseteq \mathbb{G} \times \mathbb{Z}_q$, 满足 $\Pi_{\mathbb{G}} := \{(Y, y) | Y = y \cdot G\}$ 。

I_Y : 困难关系 $\Pi_{\mathbb{G}}$ 的实例。

y : 困难关系证据。

Y : 困难关系状态。

λ : 安全参数。

$H_1(\cdot)$: 安全的哈希函数, $H_1: \{0,1\}^* \rightarrow Z_q^*$ 。

d_i : 环成员用户 i 私钥, $d_i \in Z_q^*$, 其中 $i = (1, 2, \dots, n)$ 。

P_i : 环成员用户 i 公钥, $P_i = d_i \cdot G$, 其中 $i = (1, 2, \dots, n)$ 。

L : 环群组公钥, $L = \{P_1, P_2, \dots, P_{t-1}, P_t, P_{t+1}, \dots, P_{n-1}, P_n\}$, 签名者为第 t 个用户 ($1 \leq t \leq n$)。

d_t : 签名者私钥。

$\tilde{\sigma}$: 预签名, $\tilde{\sigma} = (c_1, \tilde{s}_1, \tilde{s}_2, \dots, \tilde{s}_n, Q_1, Q_2, \dots, Q_n, \pi)$ 。

σ : 正式签名, $\sigma = (c_1, s_1, s_2, \dots, s_n)$ 。

m : 消息, $m \in \{0,1\}^*$ 。

π : 非交互式零知识证明。

$P_Y(\cdot)$: 非交互式零知识证明生成算法。

$V_Y(\cdot)$: 非交互式零知识证明验证算法。

$K(\cdot)$: 非交互式零知识证明提取算法。

1.2 签名算法

数字签名 $\Sigma = (\text{Gen}, \text{Sign}, \text{Vrfy})$ 包含 3 种算法, 分别是密钥生成算法 Gen、签名生成算法 Sign 和签名验证算法 Vrfy。

(1) 密钥生成算法 Gen: $(\text{sk}, \text{pk}) \leftarrow \text{Gen}(1^\lambda)$

以安全系数 1^λ 作为输入, 经过密钥生成算法 Gen, 输出公/私钥对 (sk, pk) 。

(2) 签名生成算法 Sign: $\sigma \leftarrow \text{Sign}(m, \text{sk})$ 。

以消息 $m \in \{0,1\}^*$ 和私钥 sk 作为输入, 经过签名生成算法 Sign, 输出签名 σ 。

3) 签名验证算法 Vrfy: $b \leftarrow \text{Vrfy}(m, \sigma, \text{pk})$

以消息 $m \in \{0,1\}^*$ 、签名 σ 和签名者公钥 pk 作为输入, 经过签名验证算法 Vrfy, 输出结果 $b \in \{0,1\}$ 。若 $b = 1$, 签名有效, 验证通过; 否则签名被视为无效。

1.3 困难关系

定义二元关系 Π , 描述该二元关系的语言为 L_Π , $L_\Pi = \{Y | \exists y \text{ s.t. } (Y, y) \in \Pi\}$, 若 Π 满足以下 3 个性质, 则称 Π 为一种困难关系。

1) 存在一个效率为概率多项式时间的算法, 该算法可以输出满足条件的实例对 $(Y, y) \leftarrow \text{GenR}(1^\lambda)$, (Y, y) 属于 Π 。

2) 存在一个效率为确定性多项式时间的验证算法, 该算法能够有效判断任意二元组 (Y, y) 是否满足 Π 。

3) 对于任意多项式时间的挑战者, 在给定输入 Y 时, 能够计算出对应 y 的成功概率小于等于 $\text{negl}(\lambda)$ 。

在困难关系 (Y, y) 中, Y 为困难关系状态, y 为对应的困难关系证据。

1.4 非交互式零知识证明

非交互式零知识 (NIZK) 证明是零知识证明的重要变体, 其显著特征在于省略了传统零知识证明中的多次信息交互, 仅通过一次交互就能够完成证明。对于一组困难关系状态-证据对, 非交互式零知识证明能够在不泄露任何有用信息的情况下, 使其他用户相信证明者拥有该困难关系证据。

非交互式零知识证明包含以下两种算法。

1) 证明生成算法 $P_Y(\cdot)$: 输入困难关系状态及其对应证据, 输出证明 π 。

2) 证明验证算法 $V_Y(\cdot)$: 输入证明和困难关系状态, 输出 1 (接受) 或 0 (拒绝)。

零知识证明应满足以下 3 个性质。

1) 完备性: 对于任意一对满足困难关系 Π_G 的实例 (Y, y) , 均能够通过证明验证算法的检验, 即 $V_Y(Y, P_Y(Y, y)) = 1$ 。

2) 可靠性: 若实例 (Y, y) 不属于困难关系 Π_G , 则任意敌手使验证者接受无效证明的概率是可以忽略的。

3) 零知识性: 对于任意的一对困难关系实例 $(Y, y) \in \Pi_G$, 存在一个多项式时间模拟器 S , 能为其模拟生成一个证明。

2 适配器签名的一般模型

本节阐述适配器签名的形式化系统模型, 并给出其安全模型的定义。

2.1 系统模型

适配器签名将困难关系 Π 嵌入数字签名 $\Sigma = (\text{Gen}, \text{Sign}, \text{Vrfy})$ 中, 包括 4 种算法: 预签名生成算法 pSign 、预签名验证算法 pVerify 、适配算法 Adapt 、证据提取算法 Ext , 系统模型表示为

$\Xi_{\Sigma, \Pi} = (\text{pSign}, \text{Adapt}, \text{pVerify}, \text{Ext})$ 。

(1) 预签名生成算法 pSign : $\tilde{\sigma} \leftarrow \text{pSign}(m, \text{sk}, Y)$

该算法接收消息 $m \in \{0, 1\}^*$ 、私钥 sk 、困难关系状态 Y , 经过预签名生成算法 pSign , 输出预签名 $\tilde{\sigma}$ 。

(2) 预签名验证算法 pVerify : $b \leftarrow \text{pVerify}(m, \tilde{\sigma}, \text{pk}, Y)$

该算法接收消息 $m \in \{0, 1\}^*$ 、预签名 $\tilde{\sigma}$ 、公钥 pk 、困难关系状态 Y , 经过预签名验证算法 pVerify , 输出结果 $b \in \{0, 1\}$ 。若 $b = 1$, 则表示签名有效; 若 $b = 0$, 则表示签名无效。

(3) 适配算法 Adapt : $\sigma \leftarrow \text{Adapt}(m, \tilde{\sigma}, \text{pk}, y)$

该算法以消息 $m \in \{0, 1\}^*$ 、预签名 $\tilde{\sigma}$ 、公钥 pk 、困难关系证据 y 作为输入, 经过适配算法 Adapt , 输出完整签名 σ 。

(4) 证据提取算法 Ext : $y \leftarrow \text{Ext}(\sigma, \tilde{\sigma}, Y)$

该算法以完整签名 σ 、预签名 $\tilde{\sigma}$ 、困难关系状态 Y 作为输入, 经过证据提取算法 Ext , 输出困难关系证据 y (y 满足条件 $(Y, y) \in \Pi$) 或失败符号 $\perp$ 。

2.2 安全模型

适配器签名须满足以下性质。

定义 1 预签名正确性

若对于任意消息 m 和 $(Y, y) \in \Pi_G$, 都满足式(1), 则称环适配器签名满足预签名正确性。

$$\Pr \left[\begin{array}{l} \text{pVerify}(m, \tilde{\sigma}, L, Y) = 1 \wedge \\ \text{Vrfy}(m, \sigma) = 1 \wedge \\ (Y, y') \in \Pi_G \end{array} \middle| \begin{array}{l} \text{Gen}(1^\lambda) \leftarrow (d, P_t) \\ \text{pSign}(m, L, d, Y) \rightarrow \tilde{\sigma} \\ \text{Adapt}(\tilde{\sigma}, y) \rightarrow \sigma \\ \text{Ext}(\sigma, \tilde{\sigma}, Y) \rightarrow y' \end{array} \right] = 1 \quad (1)$$

预签名正确性是数字签名方案中的一个重要的性质。该性质确保预签名能够被正确地验证为有效, 从而保证签名的真实性和有效性。

定义 2 预签名可适配性

对于任意由消息 m 、 $(Y, y) \in \Pi_G$ 和环群组公钥 L 生成的有效预签名 $\tilde{\sigma}$, 若通过正确的困难关系证据 y 适配后得到的签名 σ 是有效的, 则称该环适配器签名满足预签名可适配性。

$$\Pr \left[\text{Vrfy}(m, \sigma) = 1 \mid \begin{array}{l} \text{pVerify}(m, \tilde{\sigma}, L, Y) = 1 \\ \text{Adapt}(\tilde{\sigma}, Y) \rightarrow \sigma \end{array} \right] = 1 \quad (2)$$

在适配器签名方案中, 通过定义预签名的适配性, 能够确保在正确的困难问题证据下, 有效的预签名能够被适配为有效的完整签名。这一过程不仅验证了签名方案的正确性, 也为其安全性提供了理论基础。

定义 3 选择消息攻击下适配器签名的存在不可伪造性 (existential unforgeability under chosen message attack for adaptor signature, aEUF-CMA)

若对于任意的概率多项式时间 (probabilistic polynomial time, PPT) 敌手 $\mathcal{A}$, 其赢得游戏 aSignForge 的概率是可以忽略的, 则称该环适配器签名是 aEUF-CMA 安全的。aSignForge 游戏是用于形式化这一属性的实验模型, 其定义如图 1 所示。

aSignForge	$O_s(m)$
$Q = \emptyset$	$\sigma \leftarrow \text{Sign}(d_p, m, L)$
$(d_p, P_p) \leftarrow \text{Gen}(1^\lambda)$	$Q = Q \cup \{m\}$
$(Y, y) \leftarrow \text{GenR}(1^\lambda)$	return σ
$m \leftarrow A^{O_s(\cdot), O_{ps}(\cdot)}(P_p, L, Y)$	$O_{ps}(m, Y)$
$\tilde{\sigma} \leftarrow \text{pSign}(m, L, d_p, Y)$	$\tilde{\sigma} \leftarrow \text{pSign}(m, L, d_p, Y)$
$\sigma \leftarrow A^{O_s(\cdot), O_{ps}(\cdot)}(\tilde{\sigma}, Y)$	$Q = Q \cup \{m\}$
return $(m \notin Q \wedge \text{Vrfy}(m, \sigma))$	return $\tilde{\sigma}$

图 1 aSignForge 游戏定义

aEUF-CMA 安全性确保了即使攻击者可以自由选择消息并获取对应的签名, 他们也无法利用这些信息伪造出其他消息的有效签名。该属性为签名系统提供了关键的安全保证, 能够有效抵御伪造攻击。

定义 4 证据可提取性

如果一个环适配器签名方案能够使任意 PPT 敌手 $\mathcal{A}$ 在 aWitExt 游戏中获胜的概率是可以忽略的, 那么该方案被认为具备证据可提取性。aWitExt 游戏是用于形式化这一属性的实验模型, 其定义如图 2 所示。

证据可提取性保证用户能够从有效的预签名及其完整签名中, 提取到对应的困难关系证据。

aWitExt	$O_s(m)$
$Q = \emptyset$	$\sigma \leftarrow \text{Sign}(d_p, m, L)$
$(d_p, P_p) \leftarrow \text{Gen}(1^\lambda)$	$Q = Q \cup \{m\}$
$(Y, y) \leftarrow \text{GenR}(1^\lambda)$	return σ
$(m, Y) \leftarrow A^{O_s(\cdot), O_{ps}(\cdot)}(P_p, L)$	$O_{ps}(m, Y)$
$\tilde{\sigma} \leftarrow \text{pSign}(m, L, d_p, Y)$	$\tilde{\sigma} \leftarrow \text{pSign}(m, L, d_p, Y)$
$\sigma \leftarrow A^{O_s(\cdot), O_{ps}(\cdot)}(\tilde{\sigma}, Y)$	$Q = Q \cup \{m\}$
$y' \leftarrow \text{Ext}(\sigma, \tilde{\sigma}, Y)$	$Q = Q \cup \{m\}$
return $(m \notin Q \wedge (y', Y) \notin \Pi_{\mathbb{G}} \wedge \text{Vrfy}(m, \sigma))$	return $\tilde{\sigma}$

图 2 aWitExt 游戏定义

3 基于 SM2 的环适配器签名方案

3.1 挑战与应对

基于 SM2 数字签名设计具备身份隐私保护功能的环适配器签名方案, 主要面临以下 3 个方面的技术挑战。

(1) 兼容性挑战: SM2 算法与环签名及适配器签名的结构融合

作为国密标准算法, SM2 数字签名算法是基于椭圆曲线离散对数难题设计的。在椭圆曲线框架下构造环适配器签名, 需要将适配器签名的签名机制嵌入 SM2 签名流程中, 同时保持可适配性与证据可提取性等密码学特性, 从而确保签名的有效性。

(2) 安全性证明挑战: 确保环适配器签名的安全性可归约到离散对数困难问题

环适配器签名方案的安全性证明较复杂, 需要建立包含预签名可适配性、预签名正确性、选择消息攻击下的存在不可伪造性、证据可提取性及匿名性等属性的增强型安全模型。本文将在随机预言机模型下将其安全目标规约至椭圆曲线上的离散对数难题。在 SM2 现有的安全基础上, 引入模拟器和提取器完成安全性规约, 确保所有安全属性均得到满足。

(3) 隐私保护挑战: 平衡身份隐私性与可验证性

环适配器签名方案需要在保护签名者身份隐私的同时, 确保能够对签名的有效性进行验证。其难点在于设计一种验证机制, 使验证者能够在不知晓签名者身份的情况下, 确认该签名确实由环内合法成员生成。为此, 本文引入非交互式零

知识证明技术，实现在不泄露任何私密信息的情况下对签名有效性进行验证。

3.2 方案设计

本节设计了一种基于SM2数字签名算法的环适配器签名方案。

设 $\Pi_{\mathbb{G}} \subseteq \mathbb{G} \times \mathbb{Z}_q$ 是群 $\mathbb{G}$ 上的困难关系，满足 $\Pi_{\mathbb{G}} := \{(Y, y) | Y = y \cdot G\}$ ， I_Y 表示困难关系 $\Pi_{\mathbb{G}}$ 中的一个状态实例。

该方案的算法实现流程描述如下。

算法1 系统初始化算法 setup : $\text{params} \leftarrow \text{setup}(1^\lambda)$

算法 $\text{setup}(1^\lambda)$

输入 安全参数 λ

输出 $\text{params} = \{p, F_p, E(F_p), \mathbb{G}, G, q, H_1\}$

- 1) 选择大素数 p ，并确定有限域 F_p
- 2) 选择椭圆曲线 $E(F_p)$ ，确定曲线参数
- 3) 设置加法循环群 $\mathcal{G}$ 的基点 G 和群阶 q
- 4) 选择安全的哈希函数 $H_1: \{0, 1\}^* \rightarrow \mathbb{Z}_q^*$
- 5) 返回 params

算法2 密钥生成算法: $\text{Gen}(1^\lambda) \leftarrow (d_i, P_i)$

用户 i 从 $\mathbb{Z}_q^*$ 中均匀选取私钥 d_i ，计算公钥 $P_i = d_i \cdot G$ 。

算法 $\text{Gen}(1^\lambda)$

输入 params

输出 (d_i, P_i)

- 1) 随机选择 $d_i \in \mathbb{Z}_q^*$
- 2) 计算 $P_i = d_i \cdot G$
- 3) 返回 (d_i, P_i)

算法3 预签名生成算法: $\tilde{\sigma} \leftarrow \text{pSign}(m, L, d_i, Y, y)$

签名者利用私钥和环群组公钥，生成嵌入困难关系的预签名，并附带NIZK证明。

算法 $\text{pSign}(m, L, d_i, Y, y)$

输入 消息 $m \in \{0, 1\}^*$ 、环群组公钥 L 、签名者私钥 d_i 和困难关系 (Y, y)

输出 $\tilde{\sigma} = (c_1, \tilde{s}_1, \tilde{s}_2, \dots, \tilde{s}_n, Q_1, Q_2, \dots, Q_n, \pi)$

1) 签名者选择环内 $(n-1)$ 个辅助成员，确定环群组公钥 $L = \{P_1, P_2, \dots, P_{t-1}, P_t, P_{t+1}, \dots, P_{n-1},$

$P_n\}$ ，签名者的位置为 $t(1 \leq t \leq n)$

2) 计算 $Q_t = (1 + d_t) \cdot Y$

3) 随机选择 $k_t \in \mathbb{Z}_q^*$

4) 计算 $c_{t+1} = H_1(L, m, k_t \cdot G + Q_t)$

5) 对 $i = t + 1, \dots, n, 1, \dots, t - 1$

a) 随机选择 $\tilde{s}_i \in \mathbb{Z}_q^*$

b) 计算 $Z_i = \tilde{s}_i \cdot G + (\tilde{s}_i + c_i) \cdot P_i$

c) 计算 $Q_i = Y + y \cdot P_i$

d) 计算 $c_{i+1} = H_1(L, m, Z_i + Q_i)$ ，其中 $c_1 =$

c_{n+1}

6) 计算 $\tilde{s}_t = ((1 + d_t)^{-1} \cdot (k_t - c_t \cdot d_t)) \bmod q$ ，

使环签名满足闭环条件

7) 生成NIZK证明 $\pi = P_Y((P_t, Q_t), d_t)$

8) 输出预签名 $\tilde{\sigma} = (c_1, \tilde{s}_1, \tilde{s}_2, \dots, \tilde{s}_n, Q_1, Q_2, \dots, Q_n, \pi)$

算法4 预签名验证算法 pVerify : $b \leftarrow \text{pVerify}(m, \tilde{\sigma}, L, Y)$

验证预签名的有效性与NIZK证明的正确性。

算法 $\text{pVerify}(m, \tilde{\sigma}, L, Y)$

输入 消息 $m \in \{0, 1\}^*$ 、预签名 $\tilde{\sigma} = (c_1, \tilde{s}_1, \tilde{s}_2, \dots, \tilde{s}_n, Q_1, Q_2, \dots, Q_n, \pi)$ 、环群组公钥 L 和困难关系状态 Y

输出 $b = \{0, 1\}$

- 1) 检查 c_1 和 $\tilde{s}_i (1 \leq i \leq n)$ 是否属于 $\mathbb{Z}_q^*$
- 2) 若有任一条件不满足，返回 $b = 0$
- 3) 否则

a) 验证 $b_Y = V_Y((P_t, Q_t), \pi)$

b) 对 $i = 1, 2, \dots, n$

i) 计算 $Z_i' = \tilde{s}_i \cdot G + (\tilde{s}_i + c_i') \cdot P_i$

ii) 计算 $c_{i+1}' = H_1(L, m, Z_i' + Q_i)$

c) 若 $c_1 = c_{n+1}'$ ，返回 $b_c = 1$

d) 否则，返回 $b_c = 0$

e) $b = b_Y \wedge b_c$

4) 返回 b

算法5 适配算法 Adapt : $\sigma \leftarrow \text{Adapt}(\tilde{\sigma}, y)$

使用困难关系证据 y 将预签名 $\tilde{\sigma}$ 适配为完整签名 σ 。

算法 Adapt($\tilde{\sigma}, y$)

输入 预签名 $\tilde{\sigma}$, 证据 y

输出 完整签名 σ

1) 对 $i = 1, 2, \dots, n$

计算 $s_i = \tilde{s}_i + y$

2) 返回完整签名 $\sigma = (c_1, s_1, s_2, \dots, s_n)$

算法 6 签名验证算法 Vrfy: $b \leftarrow \text{Vrfy}(m, \sigma)$

检查完整签名是否有效, 确认其由环内某一成员的密钥生成, 且满足 SM2 环签名的正确性。

算法 Vrfy(m, σ)

输入 消息 $m \in \{0, 1\}^*$ 和签名 $\sigma = (c_1, s_1, s_2, \dots, s_n)$

输出 $b = \{0, 1\}$

1) 检查 c_1 和 $\tilde{s}_i (1 \leq i \leq n)$ 是否属于 Z_q^*

2) 若任一条件不满足, 返回 $b = 0$

3) 否则

a) 对 $i = 1, 2, \dots, n$:

i) 计算 $Z_i' = s_i \cdot G + (s_i + c_i') \cdot P_i$

ii) 计算 $c_{i+1}' = H_1(L, m, Z_i')$

b) 若 $c_1 = c_{n+1}'$, 返回 $b = 1$

c) 否则, 返回 $b = 0$

4) 返回 b

算法 7 证据提取算法 Ext: $y \leftarrow \text{Ext}(\sigma, \tilde{\sigma}, Y)$

给定预签名及其对应的完整签名, 提取困难关系证据 y 。

算法 Ext($\sigma, \tilde{\sigma}, Y$)

输入 预签名 $\tilde{\sigma}$ 、完整签名 σ 和困难关系状态 Y

输出 困难关系证据 y 或失败符号 $\perp$

1) 对 $i = 1, 2, \dots, n$

计算 $y_i' = s_i - \tilde{s}_i$

2) 若提取出的 y_i' 一致

a) 若 $(Y, y) \in \Pi_{\mathbb{G}}$, 返回困难关系证据 y'

b) 否则, 返回失败符号 $\perp$

3) 否则, 返回失败符号 $\perp$

基于 SM2 数字签名算法的环适配器签名方案如图 3 所示。

4 安全性证明

本节将依次证明方案的预签名可适配性、预签名正确性、选择消息攻击下的存在不可伪造

性、证据可提取性及匿名性。

4.1 预签名可适配性

定理 1 基于 SM2 数字签名算法的环适配器签名满足预签名可适配性。

证明 基于 SM2 数字签名算法的环适配器签名方案满足预签名可适配性。若 $\text{pVerify}(m, \tilde{\sigma}, L, Y) = 1$, 则有 $c_{n+1}' = H_1(L, m, \tilde{s}_n \cdot G + (\tilde{s}_n + c_n') \cdot P_n + Q_n) = c_1$ 。

根据适配算法 $\sigma \leftarrow \text{Adapt}(\tilde{\sigma}, y)$, 对于 $i = 1, 2, \dots, n$, 令 $\tilde{s}_i = s_i - y$, 得到:

$$\begin{aligned} \tilde{s}_i \cdot G + (\tilde{s}_i + c_i') \cdot P_i + Q_i &= \\ (s_i - y) \cdot G + ((s_i - y) + c_i') \cdot P_i + Q_i &= \\ s_i \cdot G - Y + (s_i + c_i') \cdot P_i - y \cdot P_i + Y + y \cdot P_i &= \\ s_i \cdot G + (s_i + c_i') \cdot P_i & \quad (3) \end{aligned}$$

因此, 完整签名 σ 是有效签名。

4.2 预签名正确性

定理 2 基于 SM2 数字签名算法的环适配器签名满足预签名正确性。

证明 验证者根据预签名 $\tilde{\sigma} = (c_1, \tilde{s}_1, \tilde{s}_2, \dots, \tilde{s}_n, Q_1, Q_2, \dots, Q_n, \pi)$, 依次计算 $Z_i' = \tilde{s}_i \cdot G + (\tilde{s}_i + c_i') \cdot P_i$ 和 $c_{i+1}' = H_1(L, m, Z_i' + Q_i)$, 显然, 当 $i \neq t$ 时, $c_i' = c_i$; 当 $i = t$ 时,

$$\begin{aligned} Z_t' &= \tilde{s}_t \cdot G + (\tilde{s}_t + c_t') \cdot P_t = \\ (1 + d_t)^{-1} \cdot (k_t - c_t \cdot d_t) \cdot (G + P_t) + c_t \cdot P_t &= \\ (k_t - c_t \cdot d_t) \cdot G + c_t \cdot d_t \cdot G &= \\ k_t \cdot G, \end{aligned}$$

$$c_{t+1}' = H_1(L, m, Z_t' + Q_t) = H_1(L, m, k_t \cdot G + Q_t) =$$

c_{t+1} 满足 $c_1 = c_{n+1}'$ 。由 NIZK 证明的完备性可以证明 $V_Y((P_t, Q_t), \pi) = 1$, 因此可以证明 $\text{pVerify}(m, \tilde{\sigma}, L, Y) = 1$ 。

根据定理 1, 当 $\text{pVerify}(m, \tilde{\sigma}, L, Y) = 1$ 且 $y = \text{Ext}(\sigma, \tilde{\sigma}, Y)$ 时, 可以证明 $\text{Vrfy}(m, \sigma) = 1$ 。

由于 $s_i = \tilde{s}_i + y$, 因此 $\text{Ext}(\sigma, \tilde{\sigma}, Y)$ 得到的 y' 满足 $(Y, y) \in \Pi_{\mathbb{G}}$ 。

4.3 选择消息攻击下的存在不可伪造性

定理 3 若 SM2 环签名方案满足选择消息攻击下的存在不可伪造性, 且 $\Pi_{\mathbb{G}}$ 是一个困难关系, 则基于 SM2 数字签名算法的环适配器签名方案满足选择消息攻击下适配器签名的存在不可

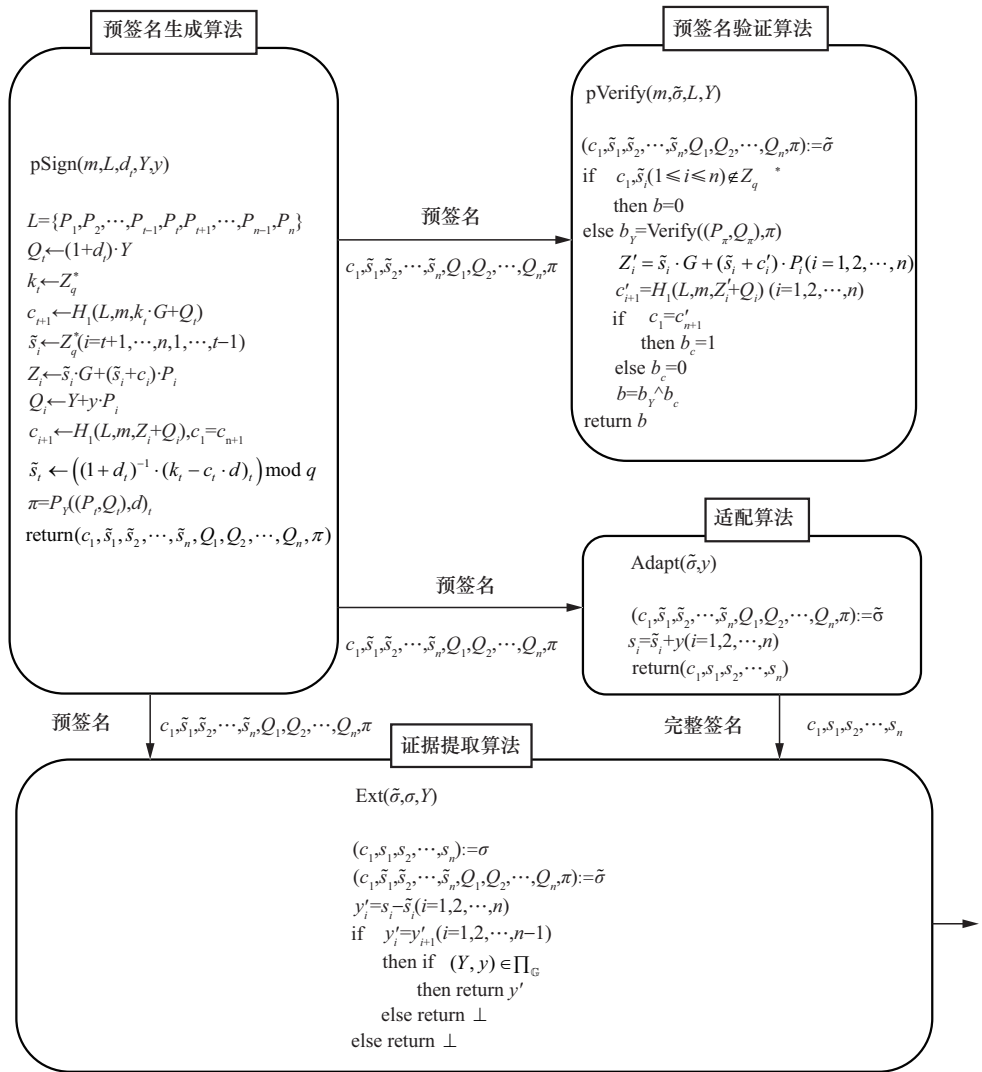


图3 基于SM2数字签名算法的环适配器签名方案

伪造性。

证明 对于任意 PPT 敌手 $\mathcal{A}$ ，敌手 $\mathcal{A}$ 与模拟器 S 进行 aSignForge 游戏，若敌手 $\mathcal{A}$ 赢得游戏的概率是一个可忽略的函数，则称适配器签名满足选择消息攻击下适配器签名的存在不可伪造性。

本节定义了 GAME0、GAME1、GAME2 和 GAME3，各游戏在分布上是不可区分的。此外，模拟器 S 能够完美模拟 GAME3。

GAME0: 该游戏即为原始 aSignForge 游戏。

GAME1: 在 aSignForge 游戏中，敌手 $\mathcal{A}$ 可以访问签名预言机 O_S 和预签名预言机 O_{ps} ，生成挑战消息 m^* 的一个有效伪造。在预言机模型下，GAME1 与 GAME0 的区别是敌手 $\mathcal{A}$ 可以额

外访问随机预言机 $H(x)$ ，且 $\Pr[\text{GAME1} = 1] = \Pr[\text{aSignForge} = 1]$ 。GAME1 的定义如图4所示。

GAME1	$O_S(m)$	$O_{ps}(m, Y)$
$Q = \emptyset$	$\sigma \leftarrow \text{Sign}(d, m, L)$	$\tilde{\sigma} \leftarrow \text{pSign}(m, L, d, Y)$
$(d, P_t) \leftarrow \text{Gen}(1^t)$	$Q = Q \cup \{m\}$	$Q = Q \cup \{m\}$
$(Y, y) \leftarrow \text{GenR}(1^t)$	return σ	return $\tilde{\sigma}$
$m \leftarrow A^{O_S(\cdot), O_{ps}(\cdot)}(P_t, L, Y)$	$H(x)$	
$\tilde{\sigma} \leftarrow \text{pSign}(m, L, d, Y)$	if $H(x) = \perp$	
$\sigma \leftarrow A^{O_S(\cdot), O_{ps}(\cdot)}(\tilde{\sigma}, Y)$	$H(x) \leftarrow Z_q^*$	
return($m \notin Q \wedge \text{Vrfy}(m, \sigma)$)	return $H(x)$	

图4 GAME1 定义

GAME2: 该游戏与 GAME1 的区别在于，当敌手 $\mathcal{A}$ 输出伪造的签名 σ^* 时，GAME2 检查使

用困难关系证据 y 适配预签名的结果是否为 σ^* ，若 $\text{Adapt}(\tilde{\sigma}, y) = \sigma^*$ ，则 GAME2 终止。GAME2 的定义如图 5 所示。

GAME2	$O_s(m)$	$O_{ps}(m, Y)$
$Q = \emptyset$	$\sigma \leftarrow \text{Sign}(d_p, m, L)$	$\tilde{\sigma} \leftarrow \text{pSign}(m, L, d_p, Y)$
$(d_p, P_p) \leftarrow \text{Gen}(1^\lambda)$	$Q = Q \cup \{m\}$	$Q = Q \cup \{m\}$
$(Y, y) \leftarrow \text{GenR}(1^\lambda)$	return σ	return $\tilde{\sigma}$
$m \leftarrow A^{O_s(\cdot), O_{ps}(\cdot)}(P_p, L, Y)$		
$\tilde{\sigma} \leftarrow \text{pSign}(m, L, d_p, Y)$		
$\sigma \leftarrow A^{O_s(\cdot), O_{ps}(\cdot)}(\tilde{\sigma}, Y)$	$H(x)$	
if $\text{Adapt}(\tilde{\sigma}, y) = \sigma$	if $H(x) = \perp$	
Abort	$H(x) \leftarrow Z_q^*$	
return($m \notin Q \wedge \text{Vrfy}(m, \sigma)$)	return $H(x)$	

图5 GAME2 定义

GAME3: 该游戏与 GAME2 的区别是，敌手 $\mathcal{A}$ 在选定挑战消息 m^* 后，模拟器 S 通过修改完整签名 σ 得到预签名 $\tilde{\sigma}$ ，将其发送给敌手 $\mathcal{A}$ 。具体而言， S 首先生成困难关系状态-证据对，然后通过签名预言机得到挑战消息 m^* 的完整签名 σ ，最后利用 $\text{Adapt}(\sigma, -y)$ 生成预签名 $\tilde{\sigma}$ （即计算 $\tilde{s}_i = s_i - y$ ）。GAME3 的定义如图 6 所示。

GAME3	$O_s(m)$	$O_{ps}(m, Y)$
$Q = \emptyset$	$\sigma \leftarrow \text{Sign}(d_p, m, L)$	$\sigma \leftarrow \text{pSign}(d_p, m, L)$
$(d_p, P_p) \leftarrow \text{Gen}(1^\lambda)$	$Q = Q \cup \{m\}$	$\tilde{\sigma} \leftarrow \text{Adapt}(\sigma, -y)$
$(Y, y) \leftarrow \text{GenR}(1^\lambda)$	return σ	$Q = Q \cup \{m\}$
$m \leftarrow A^{O_s(\cdot), O_{ps}(\cdot)}(P_p, L, Y)$		return $\tilde{\sigma}$
$\tilde{\sigma} \leftarrow \text{pSign}(m, L, d_p, Y)$		
$\sigma \leftarrow A^{O_s(\cdot), O_{ps}(\cdot)}(\tilde{\sigma}, Y)$	$H(x)$	
if $\text{Adapt}(\tilde{\sigma}, y) = \sigma$	if $H(x) = \perp$	
Abort	$H(x) \leftarrow Z_q^*$	
return($m \notin Q \wedge \text{Vrfy}(m, \sigma)$)	return $H(x)$	

图6 GAME3 定义

在 GAME3 中，模拟器 S 生成困难关系状态-证据对，应用困难关系证据 y 模拟预签名预言机，生成相应的预签名值，因此 GAME2 与 GAME3 在本质上是无法区分的，即 $\Pr[\text{GAME2} = 1] = \Pr[\text{GAME3} = 1]$ 。

推论 1 设 Bad1 是 GAME2 的终止事件，则

$\Pr[\text{Bad1}] \leq n_1(v)$ ， $n_1(v)$ 是可忽略函数。

证明 本证明通过将问题归约到困难关系的困难性上来证明该推论。构造一个模拟器 S ，使得若敌手 $\mathcal{A}$ 能够以不可忽略的概率赢得 GAME0，则 S 可以打破困难关系。

模拟器 S 在获得挑战 Y^* 后，模拟敌手 $\mathcal{A}$ 在 GAME1 中对随机预言机 H 、预签名预言机 O_{ps} 和签名预言机 O_s 的询问。当收到敌手 $\mathcal{A}$ 的挑战消息 m^* 时， S 计算预签名值并将其返回给敌手 $\mathcal{A}$ ，敌手 $\mathcal{A}$ 输出完整签名 σ^* 。

假设 Bad1 发生，即敌手 $\mathcal{A}$ 利用困难关系证据 y 和预签名适配出的完整签名与伪造签名相同，那么 S 可以利用提取算法 $\text{Ext}(\sigma, \tilde{\sigma}, Y)$ 提取困难关系证据 y^* ，使 $Y^* = y^* \cdot G$ ，从而打破困难关系。因此， S 打破困难关系的概率与敌手 $\mathcal{A}$ 赢得 GAME2 的概率相同，且该概率是可忽略的。除非 Bad1 发生，否则 GAME1 和 GAME2 是等价的，即 $|\Pr[\text{GAME1} = 1] - \Pr[\text{GAME2} = 1]| \leq n_1(v)$ 。

因此，从初始的 aSignForge 游戏（即 GAME0）到 GAME3 的转换过程是不可区分的。

构造模拟器 S 以模拟 GAMA3，并在其中赢得 aSignForge 游戏的具体方式如下。

1) 哈希询问：当敌手 $\mathcal{A}$ 询问某个消息的哈希值时，模拟器 S 检查 $H(x)$ 是否已存在于哈希询问列表中。若存在，则直接返回 $H(x)$ 给敌手 $\mathcal{A}$ ；若不存在，则查询 $H_{\text{SM2-RSign}}$ ，并将结果返回给敌手 $\mathcal{A}$ 。

2) 签名询问：当敌手 $\mathcal{A}$ 向签名预言机 O_s 询问消息 m 的签名时，模拟器 S 利用 $O_{\text{SM2-RSign}}$ 获得签名，并将签名转发给敌手 $\mathcal{A}$ 。

3) 预签名询问：模拟器 S 接收到敌手 $\mathcal{A}$ 对 O_{ps} 的查询 (m, Y) 时，先询问 $O_{\text{SM2-RSign}}$ 获得关于消息 m 的签名 σ ，再利用困难关系证据 y 计算 $\tilde{s}_i = s_i - y$ ，输出预签名 $\tilde{\sigma}$ 返回给敌手 $\mathcal{A}$ 。

4) 挑战阶段：模拟器 S 接收到敌手 $\mathcal{A}$ 选定的挑战消息 m^* 后，首先执行困难关系生成算法 $\text{GenR}(1^\lambda) \rightarrow (Y, y)$ 以生成困难关系状态-证据对，接着运行签名预言机得到完整签名，并计算 $\tilde{s}_i = s_i - y$ ，然后将生成的预签名 $\tilde{\sigma}$ 返回给敌手 $\mathcal{A}$ 。当敌手 $\mathcal{A}$ 输出一个伪造的签名值 σ^* 时，模拟器 S 将输出 (m^*, σ^*) 作为自己的伪造。

推论2 (m^*, σ^*) 是 aSignForge 的有效伪造。

证明 为证明 (m^*, σ^*) 的有效性，需证明 (m^*, σ^*) 此前未被 O_S 输出过。这意味着，在挑战阶段之前，敌手 $\mathcal{A}$ 没有向预言机 O_S 或 O_{ps} 提交过 m^* 的查询，即向 $O_{SM2-RSign}$ 提交的挑战信息 m^* 查询仅在挑战阶段进行。根据 GAME2 的规则，敌手 $\mathcal{A}$ 生成的伪造签名 σ^* 与 $O_{SM2-RSign}$ 输出的完整签名 σ 一致的概率极低，是一个可忽略的函数。由此可以推断出 $O_{SM2-RSign}$ 从未对消息 m^* 输出过相应的签名，因此伪造签名 σ^* 在 aSignForge 游戏环境中是有效的。

综上所述，模拟器 S 准确地再现了 GAME3。通过对 GAME0 到 GAME3 的逐步分析，得到结果 $\Pr[\text{GAME0} = 1] \leq \Pr[\text{GAME3} = 1] + n_1(v)$ 。

敌手 $\mathcal{A}$ 在 aSignForge 游戏中的优势为：

$$\text{Adv}_{\text{aSignForge}}^{\mathcal{A}} \leq \text{Adv}_{\text{RSM2-EUF-CMA}}^S + n_1(v) \quad (4)$$

因此其赢得游戏的概率是可忽略的。这表明基于 SM2 数字签名算法的环适配器签名满足选择消息攻击下的存在不可伪造性。

4.4 证据可提取性

定理4 若 SM2 环签名方案满足选择消息攻击下的存在不可伪造性，且 Π_G 是一个困难关系，则基于 SM2 数字签名算法的环适配器签名方案满足证据可提取性。

证明 对于任意在多项式时间内运行的敌手 $\mathcal{A}$ ，若敌手 $\mathcal{A}$ 与模拟器 S 在 aWitExt 游戏中获胜的概率是一个可忽略的函数，则认为基于 SM2 数字签名算法的环适配器签名方案具备证据可提取性。

与 aSignForge 游戏不同，在 aWitExt 游戏的挑战阶段，由敌手 $\mathcal{A}$ 运行困难关系生成算法生成困难关系状态-证据对，从而导致模拟器 S 无法直接得到困难关系证据 y 。然而，由于所采用的非交互式零知识证明满足直线可提取性，存在一个多项式时间的在线提取器 K ，它能够通过访问随机预言机的查询列表，在观察到敌手 $\mathcal{A}$ 生成的有效证明后，恢复出相应的困难关系见证。因此，模拟器 S 可以依赖提取器 K 完成预签名的模拟。

具体而言，提取器 K 的存在性依赖于所用 NIZK 证明的特殊可提取性。对于任意一个有效

的零知识证明 π ， K 能够在多项式时间内对 π 进行分析，并输出与之对应的困难关系状态及其见证 (Y, y) ，其中 $(Y, y) \in \Pi_G$ 。该提取过程不依赖敌手的内部状态，而仅依赖于其与随机预言机的交互记录。因此，可以保证提取器 K 的存在性和可实现性。

本节定义了 GAME0 和 GAME1，各游戏在分布上是不可区分的，且模拟器 S 能够完美模拟 GAME1。

GAME0：该游戏与 aWitExt 游戏行为相同。

GAME1：该游戏在挑战阶段使用直线证据提取器 K 获得困难关系证据 y ，通过访问 $O_{SM2-RSign}$ ，获得签名 σ ，计算 $\tilde{s}_i = s_i - y$ ，返回预签名 $\tilde{\sigma}$ 。

构造模拟器 S 以模拟 GAME1 的具体方式如下。

1) 哈希询问：当敌手 $\mathcal{A}$ 询问某消息的哈希值时，模拟器 S 首先检查 $H(x)$ 是否已存在于哈希询问列表中。若存在，则直接返回 $H(x)$ 给敌手 $\mathcal{A}$ ；若不存在，则查询 $H_{SM2-RSign}$ ，并将结果返回给敌手 $\mathcal{A}$ 。

2) 签名询问：当敌手 $\mathcal{A}$ 向签名预言机 O_S 询问消息 m 的签名时，模拟器 S 查询 $O_{SM2-RSign}$ 获取结果，并将结果转发给敌手 $\mathcal{A}$ 。

3) 预签名询问：当模拟器 S 接收到敌手 $\mathcal{A}$ 向 O_{ps} 查询的 (m, Y) 时，先询问 $O_{SM2-RSign}$ 获得关于消息 m 的签名 σ ，再利用直线证据提取器提取困难关系证据 y ，计算 $\tilde{s}_i = s_i - y$ ，输出预签名 $\tilde{\sigma}$ 并将其返回给敌手 $\mathcal{A}$ 。

4) 挑战阶段：模拟器 S 接收到敌手 $\mathcal{A}$ 选定的挑战消息 m^* ，首先利用直线证据提取器提取困难关系证据 y ，然后运行签名预言机得到完整签名，并计算 $\tilde{s}_i = s_i - y$ ，最后返回预签名 $\tilde{\sigma}$ 给敌手 $\mathcal{A}$ 。当敌手 $\mathcal{A}$ 输出一个伪造的签名值 σ^* 时，模拟器 S 将输出 (m^*, σ^*) 作为自己的伪造。

推论3 GAME0 和 GAME1 是不可区分的。

证明 在挑战阶段，模拟器 S 可以利用非交互式零知识证明的直线证据提取性，以非忽略概率成功提取出满足 $(Y, y) \in \Pi_G$ 的困难关系证据 y ，通过调用签名预言机获得完整签名，并据此计算出预签名。因此，GAME1 中敌手 $\mathcal{A}$ 的观察分布与 GAME0 完全一致，二者在本质上无法区分，

即 $|\Pr[\text{GAME1} = 1] - \Pr[\text{GAME2} = 1]| \leq n_1(v)$ 。

综上所述, 模拟器 S 可以完美模拟 GAME1 , 敌手 $\mathcal{A}$ 在游戏 aWitExt 中的优势

$$\begin{aligned} \text{Adv}_{\text{aWitExt}}^{\mathcal{A}} &= \Pr[\text{GAME0} = 1] \leq \\ \Pr[\text{GAME1} = 1] &+ n_2(v) = \\ \text{Adv}_{\text{RSM2-EUF-CMA}}^S &+ n_2(v) \end{aligned}$$

是可以忽略的。

4.5 匿名性

定理 5 若 SM2 环签名方案满足匿名性和选择消息攻击下的存在不可伪造性, 且 $\Pi_{\mathbb{G}}$ 是一个困难关系, 则基于 SM2 数字签名算法的环适配器签名方案满足匿名性。

证明 需要证明由任何一个成员生成的环适配器签名在分布上是不可区分的, 从而推导出环适配器签名的无条件匿名性。

假设敌手 $\mathcal{A}$ 指定消息 m^* 及环群组公钥 L , 并发送给模拟器 S , 模拟器 S 在环成员集合 $\{1, 2, \dots, n\}$ 中随机选取一个索引 l , 并假设环群组成员 A_l 为签名者, 计算出关于消息 m^* 的有效签名。对于任意 $i \in [1, n]$, 若选择索引 i 作为签名者, 则模拟器 S 从 Z_q^* 中均匀随机选取随机数 k_i , 并计算满足 $\tilde{s}_i = \left((1 + d_i)^{-1} \cdot (k_i - c_i \cdot d_i) \right) \bmod q$ 的响应值, 以生成环适配器签名。由此得到的签名分布与索引 i 的取值无关, 因为非签名者位置上的随机数均服从独立均匀分布。

因此, 在环内生成签名的过程中, 对于每个成员 i , 其被选为签名者的条件概率均为 $\Pr[\text{Signer} = i] = \frac{1}{n}$ 。

进一步地, 设模拟器 S 在生成过程中构造 $(n-1)$ 个不同的签名对 $(c_j, \tilde{s}_j)$, 其中 $i \neq j$, 则每个签名对被选中的概率为 $\frac{1}{q-1}$, 不同选择之间的联合概

率为 $\frac{1}{q-1} \cdot \frac{1}{q-2} \cdot \dots \cdot \frac{1}{q-n+1}$, 并且该概率分布不依赖真实签名者的索引。由此可见, 敌手 $\mathcal{A}$ 无法区分环内哪个成员是实际签名者。

综上, 敌手 $\mathcal{A}$ 在匿名性实验中能够区分出真实签名者的概率不超过 $\frac{1}{n}$, 由此证明基于 SM2 数字签名算法的环适配器签名方案满足匿名性。

5 性能分析

本节将评估基于 SM2 数字签名算法的环适配器签名方案的效率, 分析其时间开销、通信开销及安全性, 并与现有的环适配器签名方案进行对比。

5.1 时间开销

表 1 对比了 3 种环适配器签名方案的时间开销。其中, n 表示环成员用户数量, T_{pm} 、 T_{pa} 分别表示点乘运算及点加运算的时间开销, T_{e} 表示幂指数运算的时间开销, T_{mul} 、 T_{add} 、 T_{inv} 分别表示模乘、模加及模逆运算的时间开销, T_{p} 、 T_{v} 分别表示非交互式零知识证明的生成算法及验证算法的时间开销, T_{h} 表示哈希运算的时间开销。

1) 预签名生成算法: 与 Schnorr 可链接环适配器签名方案相比, 本文方案的时间开销额外增加 $T_{\text{pm}} + (2n-2)T_{\text{pa}} + T_{\text{mul}} + T_{\text{inv}} + T_{\text{p}}$, 但计算开销减少 $(4n-1)T_{\text{e}} + T_{\text{add}}$; 与 GQ 可链接环适配器签名方案相比, 本文方案的时间开销额外增加 $T_{\text{pm}} + (2n-2)T_{\text{pa}} + T_{\text{mul}} + T_{\text{inv}} + T_{\text{p}}$, 计算开销减少 $4nT_{\text{e}} + T_{\text{h}}$ 。

2) 预签名验证算法: 与 Schnorr 和 GQ 可链接环适配器签名方案相比, 本文方案的时间开销额外增加 $nT_{\text{pa}} + T_{\text{v}}$, 计算开销减少 $4nT_{\text{e}}$ 。

3) 适配算法和提取算法: 本文方案与 Schnorr 和 GQ 可链接环适配器签名方案的时间开销相等, 均为 nT_{add} 。

表 1 3 种环适配器签名时间开销对比

方案	预签名生成算法	预签名验证算法	适配算法	提取算法
本文方案	$(3n-1)T_{\text{pm}} + (2n-2)T_{\text{pa}} + nT_{\text{h}} + 2T_{\text{mul}} + T_{\text{inv}} + T_{\text{p}}$	$2nT_{\text{pm}} + nT_{\text{pa}} + nT_{\text{h}} + T_{\text{v}}$	nT_{add}	nT_{add}
Schnorr 可链接环适配器签名方案	$(3n-2)T_{\text{pm}} + (4n-1)T_{\text{e}} + nT_{\text{h}} + T_{\text{mul}} + T_{\text{add}}$	$3nT_{\text{pm}} + 4nT_{\text{e}} + (n+1)T_{\text{h}}$	nT_{add}	nT_{add}
GQ 可链接环适配器签名方案	$4nT_{\text{e}} + (3n-2)T_{\text{pm}} + (n+1)T_{\text{h}} + T_{\text{mul}}$	$3nT_{\text{pm}} + 4nT_{\text{e}} + (n+1)T_{\text{h}}$	nT_{add}	nT_{add}

5.2 通信开销

表2对3种环适配器签名方案的通信开销进行了对比。其中, $|q|$ 表示大素数 q 所占的比特位数, $|G|$ 表示循环群所占的比特位数。所有方案均采用相同的安全参数: $|q|=256$ bit, $|G|=512$ bit。

表2 3种环适配器签名方案通信开销对比

方案	预签名值大小	签名值大小
本文方案	$(n+3) q + n G $	$(n+1) q $
Schnorr可链接环适配器签名	$(n+1) q + G $	$(n+1) q + G $
GQ可链接环适配器签名	$(n+1) q + G $	$(n+1) q + G $

本文方案预签名 $\tilde{\sigma} = (c_1, \tilde{s}_1, \tilde{s}_2, \dots, \tilde{s}_n, Q_1, Q_2, \dots, Q_n, \pi)$ 产生的预签名值大小为 $(n+3)|q| + n|G|$, 签名值大小为 $(n+1)|q|$ 。

5.3 仿真实验

为全面评估本文所提的环适配器签名方案的性能, 研究人员开展了仿真实验。仿真实验的硬件环境为搭载16.0 GB RAM的联想移动端主机和13th Gen Intel Core i7-13700H CPU @ 2.40 GHz的中央处理器。操作系统版本为64位Windows 11 Home Chinese Edition。开发环境为Pycharm, 编程语言为Python 3.12.5, 并使用gmssl库, 椭圆曲线参数遵循GM/T 0003-2012标准。

表3展示了本文签名方案中各算法在不同环成员数量下的时间开销, 数据来源于实验测量(保留3位小数)。仿真结果数据是某一轮1 000次运行结果的平均值。实验结果表明, 预签名生成算法的时间开销与预签名验证算法的时间开销随环成员数量的增加而上升, 意味着其计算复杂度与环成员数量呈正比, 这与环签名方案的特性一致。相比之下, 适配算法与提取算法的时间开销变化微小。

表3 不同环成员数量下各算法的时间开销

环成员数量	预签名生成算法/ms	预签名验证算法/ms	适配算法/ms	提取算法/ms
$n=1$ 个	23.454	21.505	0.001	0.001
$n=5$ 个	112.638	100.008	0.002	0.002
$n=10$ 个	239.112	225.385	0.003	0.003
$n=20$ 个	515.972	465.160	0.005	0.004
$n=50$ 个	1 308.940	1 198.694	0.011	0.011

图7对比了3种方案预签名生成算法的执行时间随环成员数量的变化趋势。Schnorr可链接环适配器签名方案因具有线性同态性质, 通常被视为高效的环适配器签名代表, 将其与本文方案对比, 可验证本文方案在主流技术框架下的实用性。实验结果显示, 3种方案的执行时间均随环成员数量增加而显著上升, 但本文方案的增长速度更缓。尤其是当环成员超过10个时, 本文方案的执行时间少于另外两种方案。

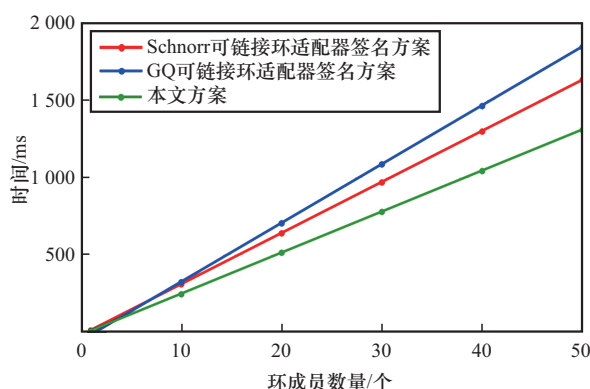


图7 3种方案预签名生成算法时间开销对比

图8展示了3种方案预签名验证算法的时间开销随环成员数量变化情况, 从中可以看出, 本文方案的预签名验证时间整体上显著少于Schnorr和GQ可链接环适配器签名方案。尤其是在环成员数量较多时, 优势更加明显。结合表1的数据可知, 本文方案在预签名生成与验证阶段均具有更短的时间开销。这些结果表明, 本文方案在运行效率方面优于其他两种环适配器签名方案。

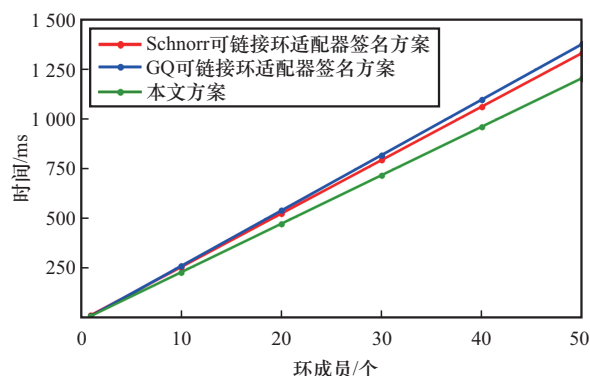


图8 3种方案预签名验证算法时间开销对比

5.4 安全性对比

在安全性方面, 本文方案与其他数字签名方

案的对比结果见表 4。基于 SM2 的环签名方案在安全方面不具备可适配性和可提取性，而基于 SM2 的适配器签名方案则缺乏匿名性。本文提出的方案具备可适配性、可提取性与匿名性。

表 4 签名方案安全性对比

方案	可适配性	可提取性	匿名性
基于 SM2 的环签名方案	×	×	√
基于 SM2 的适配器签名方案	√	√	×
本文方案	√	√	√

5.5 与类 Monero 环适配器签名方案的对比

本文方案与类 Monero 的环适配器签名方案在设计上存在以下区别。

(1) 密码学基础结构差异

本文方案基于国密算法 SM2 和环签名技术构建，采用 GM/T 0003-2012 标准规定的椭圆曲线参数，其安全性建立在 SM2 椭圆曲线离散对数难题及国密特定参数集的安全性假设之上。文献[20]中提出的 Monero 类方案采用通用的密码原语组合架构，默认采用 Schnorr 签名或 GQ 签名等标准化算法，通常使用 secp256k1 等国际通用椭圆曲线，其安全模型建立在不同椭圆曲线群上的计算性 Diffie-Hellman 假设基础之上。因此，二者在椭圆曲线密码算法的数学基础和安全假设上存在本质差异。

(2) 功能特性差异

本文方案通过 SM2 环签名实现了条件支付场景下的身份隐私保护与交易原子性，并兼容跨链协议中的哈希时间锁操作。类 Monero 环适配器签名方案专门为实现强匿名性支付通道网络而设计，通过可链接环签名技术实现交易输入与输出的完全匿名化，并支持多跳支付路径的锁定与解锁机制。因此，该方案能够在保持监管合规的前提下实现身份隐私保护，而 Monero 类方案更强调交易的完全匿名性。

综上所述，本文方案融合国产密码算法 SM2、环签名与适配器签名技术，在保障身份隐私的同时实现了密码算法的自主可控；在功能上

兼顾身份隐私与交易原子性，尤其适用于电子政务、跨境数据监管、金融合规审查等对密码自主可控性要求较高的场景，并在跨链隐私保护中展现出独特的应用潜力。类 Monero 环适配器签名通过多跳锁定与强隐私保护机制，在支付通道网络中具有较好的实用性。

6 结束语

本文提出了一种基于国密算法 SM2 的环适配器签名方案，在保证交易原子性的同时，能够实现用户身份隐私保护。该方案通过环签名生成预签名，将其与秘密值结合生成完整签名，从而隐藏签名者身份信息；同时，支持用户通过完整签名和预签名提取秘密值，不仅保障了交易原子性，还保障了签名者身份的隐私性。在随机预言机模型下，该环适配器签名方案的安全性可归约到离散对数困难问题。在时间开销和通信开销方面，本文方案与现有环适配器签名方案相当，甚至部分性能表现更佳。本文方案基于国密算法设计，既保障了环适配器签名算法的自主可控性，又扩展了国产签名算法在环适配器签名领域的应用，特别适用于跨链交易等对身份隐私保护要求较高的场景。

与具有线性特征的 Schnorr 数字签名算法不同，SM2 数字签名算法涉及椭圆曲线点运算等复杂的非线性数学结构，因此本文方案须借助额外的椭圆曲线点将困难关系嵌入预签名中，导致预签名尺寸有所增加。未来研究将重点围绕在保证安全性的前提下优化预签名结构展开，具体方向包括设计适用于 SM2 的聚合或批量验证算法、重构困难关系嵌入机制，以提升算法性能。

参考文献：

- [1] 曾诗钦, 霍如, 黄韬, 等. 区块链技术研究综述: 原理、进展与应用[J]. 通信学报, 2020, 41(1): 134-151.
- Zeng S Q, Huo R, Huang T, et al. Survey of blockchain: principle, progress and application[J]. Journal on Communications, 2020, 41(1): 134-151.
- [2] Thyagarajan S A K, Malavolta G. Lockable signatures for blockchains: scriptless scripts for all signatures[C]//Proceedings of the 2021 IEEE Symposium on Security and Privacy (SP). Piscataway:

- IEEE Press, 2021: 937-954.
- [3] 郭朝, 郭帅印, 张胜利, 等. 区块链跨链技术分析[J]. 物联网学报, 2020, 4(2): 35-48.
- Guo Z, Guo S Y, Zhang S L, et al. Analysis of cross-chain technology of blockchain [J]. Chinese Journal on Internet of Things. 2020, 4(2): 35-48.
- [4] Poelstra A. Scriptless script[EB]. 2017.
- [5] Erwig A, Faust S, Hostáková K, et al. Two-party adaptor signatures from identification schemes[C]//Proceedings of IACR International Conference on Public-key Cryptography. Cham: Springer International Publishing, 2021: 451-480.
- [6] Thyagarajan S A K, Malavolta G, Moreno-Sanchez P. Universal atomic swaps: secure exchange of coins across all blockchains[C]//Proceedings of the 2022 IEEE Symposium on Security and Privacy (SP). Piscataway: IEEE Press, 2022: 1299-1316.
- [7] Fournier L. One-time verifiably encrypted signatures aka adaptor signatures[EB]. 2019.
- [8] 涂彬彬, 陈宇. 支持批量证明的SM2适配器签名及其分布式扩展[J]. 软件学报, 2024, 35(5): 2566-2582.
- Tu B B, Chen Y. SM2-based adaptor signature with batch proofs and its distributed extension[J]. Journal of Software, 2024, 35(5): 2566-2582.
- [9] Tairi E, Moreno-Sanchez P, Maffei M. Post-quantum adaptor signature for privacy-preserving off-chain payments[C]//Proceedings of the International Conference on Financial Cryptography and Data Security. Berlin: Springer, 2021: 131-150.
- [10] Deshpande A, Herlihy M. Privacy-preserving cross-chain atomic swaps[C]//Proceedings of the International Conference on Financial Cryptography and Data Security. Cham: Springer International Publishing, 2020: 540-549.
- [11] Hoenisch P, Del Pino L S. Atomic swaps between bitcoin and Monero[PP]. arXiv preprint, 2021, arXiv: 2101.12332.
- [12] Malavolta G, Moreno-Sanchez P, Schneidewind C, et al. Anonymous multi-hop locks for blockchain scalability and interoperability[C]//Proceedings of the 2019 Network and Distributed System Security Symposium. Reston: Internet Society, 2019: 1-15.
- [13] Aumayr L, Ersoy O, Erwig A, et al. Generalized channels from limited blockchain scripts and adaptor signatures[C]//Proceedings of the Advances in Cryptology-ASIACRYPT 2021: 27th International Conference on the Theory and Application of Cryptology and Information Security, Berlin: Springer International Publishing, 2021: 635-664.
- [14] 彭聪, 罗敏, 何德彪, 等. 基于SM2数字签名算法的适配器签名方案[J]. 计算机研究与发展, 2021, 58(10): 2278-2286.
- Peng C, Luo M, He D B, et al. Adaptor signature scheme based on the SM2 digital signature algorithm[J]. Journal of Computer Research and Development, 2021, 58(10): 2278-2286.
- [15] Bao Z, He D, Peng C, et al. An identity-based adaptor signature scheme and its applications in the blockchain system[J]. IEEE Open Journal of the Computer Society, 2023, 4: 231-242.
- [16] Qin X R, Pan S M, Mirzaei A, et al. BlindHub: bitcoin-compatible privacy-preserving payment channel hubs supporting variable amounts[C]//Proceedings of the 2023 IEEE Symposium on Security and Privacy (SP). Piscataway: IEEE Press, 2023: 2462-2480.
- [17] 胡小明, 陈海婵. 可证明安全的SM2盲适配器签名方案[J]. 网络与信息安全学报, 2024, 10(2): 59-68.
- Hu X M, Chen H C. Proven secure blind adaptor signature scheme based on the SM2[J]. Chinese Journal of Network and Information Security, 2024, 10(2): 59-68.
- [18] 谢晴晴, 杨念民, 冯霞. 区块链交易隐私保护技术综述[J]. 计算机应用, 2023, 43(10): 2996-3007.
- Xie Q Q, Yang N M, Feng X. Survey on privacy-preserving technology for blockchain transaction[J]. Journal of Computer Applications, 2023, 43(10): 2996-3007.
- [19] Sui Z, Liu J K, Yu J, et al. Monet: a fast payment channel network for scriptless cryptocurrency Monero[C]//Proceedings of the 2022 IEEE 42nd International Conference on Distributed Computing Systems (ICDCS). Piscataway: IEEE Press, 2022: 280-290.
- [20] Wang X, Lin C, Huang X, et al. Anonymity-enhancing multi-hop locks for Monero-enabled payment channel networks[J]. IEEE Transactions on Information Forensics and Security, 2024, 19: 2438-2453.
- [21] 范青, 何德彪, 罗敏, 等. 基于SM2数字签名算法的环签名方案[J]. 密码学报, 2021, 8(4): 710-723.
- Fan Q, He D B, Luo M, et al. Ring signature schemes based on SM2 digital signature algorithm[J]. Journal of Cryptologic Research, 2021, 8(4): 710-723.

[作者简介]



许馨月 (2001-), 女, 辽宁辽阳人, 齐鲁工业大学 (山东省科学院) 硕士生, 主要研究方向为数据安全、区块链。



徐淑奖 (1979-), 男, 山东临沂人, 齐鲁工业大学 (山东省科学院) / 山东省计算中心 (国家超级计算济南中心) 研究员, 主要研究方向为数据安全、区块链。



王连海 (1969-), 男, 山东潍坊人, 齐鲁工业大学 (山东省科学院) / 山东省计算中心 (国家超级计算济南中心) 研究员, 主要研究方向为数据安全、区块链、计算机取证。



邵蔚 (1994-), 女, 山东济南人, 齐鲁工业大学 (山东省科学院) / 山东省计算中心 (国家超级计算济南中心) 研究员, 主要研究方向为区块链、隐私保护。



张淑慧 (1981-), 女, 山东济宁人, 齐鲁工业大学 (山东省科学院) / 山东省计算中心 (国家超级计算济南中心) 研究员, 主要研究方向为数据安全、区块链、计算机取证。



王启正 (1993-), 男, 山东济南人, 齐鲁工业大学 (山东省科学院) / 山东省计算中心 (国家超级计算济南中心) 研究员, 主要研究方向为隐私保护、人工智能。