

可证明安全的SM2盲适配器签名方案

胡小明, 陈海婵

(上海第二工业大学计算机与信息工程学院, 人工智能研究院, 上海 201209)

摘要: 适配器签名是近年来出现的新密码学原语, 其基本思想是将签名过程与秘密值的揭示联系起来, 通过将预签名适配为正式签名, 使最终的签名结果和常规签名一致。预签名与正式签名可提取出一个秘密值, 因此具有原子性, 在区块链中拥有良好的应用前景。但是适配器签名不具有匿名性, 容易暴露交易参与者身份, 在电子支付等隐私需求高的应用场景具有一定的局限性。为了解决这一问题, 提出了新的盲适配器签名, 系统模型和安全模型, 在新系统模型的基础上提出了基于SM2签名算法的盲适配器签名方案, 并基于SM2签名方案的不可伪造性和困难关系证明了该方案的安全性满足新提出的安全模型要求, 即满足盲性、预签名可适配性、不可伪造性和证据可提取性。性能分析表明, 在计算开销上, SM2盲适配器签名方案的总时间仅比SM2适配器签名方案增加了5.91 ms, 与现有同类方案相比, 该方案盲性更强且具有自主可控性, 对于隐私要求高且需要采用国产密码算法的关键应用场景具有良好的应用价值。

关键词: SM2数字签名; 盲适配器签名; 原子性; 匿名性

中图分类号: TP309.7

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2024024

Proven secure blind adaptor signature scheme based on the SM2

HU Xiaoming, CHEN Haichan

School of Computer and Information Engineering, Institute for Artificial Intelligence,
Shanghai Polytechnic University, Shanghai 201209, China

Abstract: Adaptor signature (AS) is a novel cryptographic primitive that has gained prominence in recent years for its ability to link the signature process with the revelation of a secret value. The process involves adapting a pre-signature to a formal signature, ensuring that the final signature result aligns with conventional signatures. Both the pre-signature and the formal signature are capable of extracting a secret value, which endows AS with atomicity and suggests its promising application within blockchain technologies. However, the lack of anonymity in AS can lead to the exposure of transaction participants' identities, which may limit its application in scenarios demanding high privacy

收稿日期: 2023-10-23; 修回日期: 2024-03-12

通信作者: 胡小明, xmhu@sspu.edu.cn

基金项目: 上海市科委扬帆计划项目 (No.20YF1414400)

Foundation Item: Shanghai Sailing Program (No.20YF1414400)

引用格式: 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(02): 59-68.

Citation Format: 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(02): 59-68.

standards, such as electronic payments. To address this issue, a new blind adaptor signature system model and security model were proposed. Subsequently, a blind adaptor signature scheme was developed based on the SM2 signature algorithm, leveraging the new system model. The security of this new scheme, which was founded on the unforgeability and the hardness of the SM2 signature scheme, was demonstrated to meet the requirements of the newly proposed security model. Specifically, the scheme was proven to satisfy properties such as blindness, pre-signature adaptability, unforgeability, and witness extractability. Performance analysis indicates that the computational overhead of the SM2 blind adaptor signature scheme is minimal, with the total operation time of the signature process only increasing by a negligible 5.91ms compared to the SM2 adaptor signature scheme. Moreover, when compared to existing similar schemes, the SM2 blind adaptor signature scheme offers enhanced blindness and autonomy, making it particularly valuable for key application scenarios that necessitate high privacy requirements and the utilization of domestic cryptographic algorithms.

Keywords: SM2 digital signature, blind adaptor signature, atomicity, anonymity

0 引言

为了在不改变区块链结构和实现方式的情况下改善区块链的性能,允许区块链以更小的花费执行更大的应用程序,出现了一种称为适配器签名的新密码学原语。适配器签名由Poelstra提出的无脚本脚本(scritless script)演变而来,它将消息的身份验证和秘密值的揭露关联起来,由于其在不同应用程序(如原子交换^[1-2]和支付通道^[3-4])中具有广泛的应用,引起国内外学者的广泛关注,产生了很多关于适配器签名的研究成果。

Aumayr等^[5]最先基于区块链常用的Schnorr数字签名算法^[5]和将ECDSA^[6]扩展为了适配器签名方案。Erwig等^[7]提供了一种将两步式签名方案转换为适配器签名的通用方案。彭聪等^[8]构造了SM2适配器签名方案并进行了详细的安全性证明。王子瑞等^[9]基于双线性配对的优良性质构造了基于双线性配对的适配器签名。张艳硕等^[10]提出基于ISRSAC数字签名算法的适配器签名方案。后来,Erwig等^[11]提出了可重置随机密钥的适配器签名用于构造适配器钱包,涂彬彬等^[12]提出分布式SM2适配器签名并将其用于构建批量原子交换协议和支付通道网络,更好地满足了适配器签名的应用场景。

盲签名(blind signature, BS)^[13-14]是Chaum于1982年首次提出的密码学概念,允许用户获得签名者对消息的签名,同时不泄露有关消息内容的信息,即使将来签名者得到解盲后的消息-签名对,也无法将签名过程与最终的签名关联起来,

以此保证消息的隐私性。常亮等^[15]提出了基于椭圆曲线密码(elliptic curve cryptography, ECC)的同态加密盲签名方法。何德彪等^[16]设计了一种基于轻量级SM2盲签名生成方法和系统。唐卫中等^[17]基于SM2签名算法,在不需要双线性对操作的前提下,提出了一种高效无证书盲签名方案,该方案具有可证明的安全性。吕尧等^[18]提出基于SM9的部分盲签名方案,使签名具有可控性。

在盲签名的应用上,Chaum将盲签名应用于电子现金系统,Li等^[19]医疗数据匿名共享,白雪等^[20]提出一种基于SM2的两方协作盲签名协议,用盲签名性质保护用户隐私。在区块链的隐私保护中,Shentu等^[21]提出了一种集中式的盲混合算法,该算法不要求所有参与者同时在线,但是要求第三方使用盲签名保证混币的隐私安全。Yi等^[22]考虑了货币提供商向客户出售货币时,能够将其支付信息与其公钥地址联系起来,提出了与标准ECDSA签名兼容的盲签名。因此,盲签名是区块链隐私保护的重要技术手段之一。

为了在应用适配器签名的过程中更好地保护用户的隐私,Deshpande等^[23]以适配器签名为基础,设计了隐私保护的跨链原子交换方案,从而增强了跨链交易的隐私性和安全性。Qin等^[24]提出了盲适配器签名的定义和安全模型,并设计了基于ECDSA的实例。然而Qin等^[24]将盲适配器签名(bind adaptor signature, BAS)的盲性描述为弱盲性,即签名者无法知道被签名消息的具体内容,但在消息-签名对公开后,签名者能将签名过程与最终签名联系起来,其实际上不属于真

正的盲性。

综上所述，适配器签名虽然在交易的可验证性和原子性方面表现非常出色，但它却暴露了交易参与者的身份，不适用于电子支付等隐私需求高的应用场景。盲签名虽然具有良好的隐私保护能力，但是不具有原子性。针对这一问题，本文提出了新的盲适配器签名系统模型和安全模型，根据新的系统模型提出了基于SM2签名算法^[25]的盲适配器签名方案，基于SM2签名方案的不可伪造性和困难关系，证明了新方案的安全性符合新提出的安全模型要求。性能分析表明，该方案盲性比ECDSA盲适配器签名盲性强，测试环境中运行总时间比SM2适配器签名仅增加了5.91 ms。因此，本文方案具备良好的应用前景。

1 预备知识

本节介绍困难关系和SM2适配器签名方案。

符号定义： λ 为安全参数， Z_n^* 为以 n 为模的所有对模乘可逆元的集合， G 为一个阶为 n 的椭圆曲线点群， G 是其中的生成元， $H(\cdot)$ 为哈希函数， $f(\cdot): G \rightarrow Z_n$ 为取 G 中椭圆曲线点的 x 坐标， $R_G \subseteq G \times Z_n$ 为群 G 上的困难关系。

1.1 困难关系

设 R 是 (Y, y) 所满足的一个二元关系， L_R 是描述 R 关系的语言，记 $L_R = \{Y \mid \exists y \text{ s.t. } (Y, y) \in R\}$ ，如果以下3个性质成立，则称 R 是一种困难关系， y 为困难关系证据， Y 为困难关系状态。

(1) 在概率多项式时间内，存在一个即时抽样函数 GenR 生成 $(Y, y) \in R$ 。

(2) 在确定多项式时间内，存在一个算法能够判定 $(Y, y) \in R$ 是否成立。

(3) 对于任意时间敌手，给出 $Y \in L_R$ ，敌手计算出 y ，使得 $(Y, y) \in R$ 的概率是可忽略的。

1.2 SM2适配器签名方案

适配器签名方案一般包含预签名生成、预签名验证、适配和提取4个算法。

(1) 预签名生成 $\text{pSign}_{\text{sk}}(m, Y)$ ：给定私钥 sk 、消息 m 以及困难关系状态 Y ，签名者计算生成一个预签名值 δ' 。

(2) 预签名验证 $\text{pVrfy}_{\text{pk}}(m, Y; \delta')$ ：给定公钥

pk ，消息 m ，困难关系状态 Y 以及预签名值 δ' ，验证预签名的有效性，有效输出 true ，否则输出 false 。

(3) 适配 $\text{Adapt}(\delta', y)$ ：给定预签名值 δ' 和困难关系证据 y ，适配者计算生成一个签名值 δ 。

(4) 提取 $\text{Exact}(\delta', \delta, Y)$ ：给定预签名值 δ' 、签名值 δ 和困难关系状态 Y ，提取者提取一个秘密值 y ， y 与 Y 属于困难关系。

2 盲适配器签名的一般模型

本节提出了新的盲适配器签名的系统模型和安全模型，在后面的章节中将根据这些模型构造具体的SM2盲适配器签名方案并给出安全性证明。

2.1 系统模型

本文通过对文献[24]进行深入研究，并基于适配器签名的一般模型给出盲适配器签名的定义。

定义1 盲适配器签名。对于一个盲签名和一个困难关系 R ，盲适配器签名方案 $\text{SIG}_{R, \text{BS}}$ 主要包含7个算法：初始化算法 Setup ，消息盲化算法 $m\text{Blind}$ ，盲签名生成算法 $b\text{Sign}$ ，解盲算法 $u\text{Blind}$ ，预签名验证算法 $p\text{Vrfy}$ ，适配算法 Adapt 和提取算法 Exact 。

$\text{Setup}(\lambda)$ ：给定安全参数 λ ，生成困难关系对 (Y, y) ，密钥对 (pk, sk) ，临时密钥对 (T, t) ，计算承诺 A 等相关参数，初始化成功输出 true ，否则输出 false 。

$m\text{Blind}(m, T, A, \text{pk})$ ：给定待盲化的消息 m ，临时密钥 T ，承诺 A ，公钥 pk ，随机选择盲化因子 $\alpha, \beta \in Z_n^*$ ，输出盲化结果 (r, c) 。

$b\text{Sign}_{\text{sk}}(c, t)$ ：给定盲消息 c ，临时密钥 t ，私钥 sk ，输出盲签名 δ'' 。

$u\text{Blind}_{\alpha, \beta}(\delta'', r)$ ：给定盲签名 δ'' ，消息 r ，盲化因子 α 和 β ，输出预签名 δ' 。

$p\text{Vrfy}_{\text{pk}}(m, A, \delta')$ ：给定公钥 pk 、承诺 A 、签名消息 m 和预签名值 δ' ，输出一个 bool 值， true 为预签名有效， false 为预签名无效。

Adapt 和 Exact 算法与SM2适配器签名的适配和提取算法定义一致。

定义 2 预签名正确性。若对任意消息 m 和任意困难问题实例 Y ，均有：

$$\Pr \left[\begin{array}{l} \text{pVrfy}_{\text{pk}}(m, A, \delta') \\ \wedge \\ \text{Vrfy}_{\text{pk}}(m, \delta) \\ \wedge \\ (Y, y') \in R \end{array} \middle| \begin{array}{l} \text{params} \leftarrow \text{Setup}(\lambda) \\ (r, c) \leftarrow m\text{Blind}(m, T, A, \text{pk}) \\ \delta'' = \text{bSign}_{\text{sk}}(c, t) \\ \delta' = u\text{Blind}_{a,b}(\delta'', r) \\ \delta = \text{Adapt}(\delta', y) \\ y' = \text{Exact}(\delta, \delta', Y) \end{array} \right] = 1 \quad (1)$$

则称该盲适配器签名方案是预签名正确的。

2.2 安全模型

本文在文献[24]的研究工作基础上，提出盲适配器签名新的安全模型，包含：盲性、预签名可适配性、bEUF-CMA blind adaptor signature existential unforgeability under chose message attacks 安全性和证据可提取性。

定义 3 盲性。盲适配器签名的签名对于签名者具有盲性。若对任意概率多项式时间运行游戏 $\text{Blind}_{A, \text{SIG}(R, \text{BS})}(\lambda)$ ，敌手 A 赢得游戏的优势概率是可忽略的，即

$$\Pr[\text{Blind}_{A, \text{SIG}(R, \text{BS})}(\lambda) - 1/2] \leq \text{negl}(\lambda) \quad (2)$$

则称数字签名方案 $\text{SIG}_{R, \text{BS}}$ 具有盲性。

游戏 $\text{Blind}_{A, \text{SIG}(R, \text{BS})}(\lambda)$ 定义如下：设敌手 A 是签名者， U_0 和 U_1 是两个诚实的用户。

步骤 1 敌手 A 产生 2 个消息 m_0, m_1 ；

步骤 2 模拟器随机选择 $b \in (0, 1)$ ，将 m_b, m_{1-b} 分别发送给 U_0 和 U_1 ；

步骤 3 U_0 和 U_1 与敌手 A 交互，敌手对 m_b, m_{1-b} 进行盲签名， U_0 和 U_1 解盲并适配后得到 δ_b 和 δ_{1-b} ，将其发送给敌手 A ；

步骤 4 敌手 A 输出对 b 的猜测 b^* 。

若 $b^* = b$ ，则敌手 A 赢得游戏，敌手 A 赢得游戏的优势定义为： $\text{Adv}(A) = \Pr[b^* = b] - 1/2$ 。

定义 4 预签名可适配性。若对任意消息 m 、公钥 pk 和困难关系状态 Y 生成的合法预签名 δ' ，使用对应的困难关系证据 y 进行适配，若得到的全签名值是正确有效的，即

$$\Pr \left[\text{Vrfy}_{\text{pk}}(m; \delta) = 1 \middle| \begin{array}{l} \text{pVrfy}_{\text{pk}}(m, Y; \delta') \\ \delta = \text{Adapt}(\delta', y) \end{array} \right] = 1 \quad (3)$$

则称数字签名方案满足预签名可适配性。

适配器签名选择消息攻击下的存在不可伪造

性 (adaptor signature existential unforgeability under chose message attacks, aEUF-CMA) 是适配器签名最重要的定义，使得任何不具有证据 y 的敌手即使获得关于 m_i 的预签名，也难以伪造关于 m_i 的正式签名。另外，本文考虑敌手能获得关于 m_i 的合法盲签名值情况，允许敌手进行盲签名和预签名询问，获得关于 m_i 的盲签名和预签名，对于敌手选取的挑战消息 m^* ，允许敌手获得关于盲化因子 α, β 的盲签名和关于 Y 的预签名，那么，盲适配器签名的不可伪造性的要求就是敌手在不知道盲化因子和困难关系证据的情况下伪造一个合法正式签名的概率是可忽略的。

定义 5 bEUF-CMA 安全性。若对任意概率多项式时间运行游戏 $\text{bSigForge}_{A, \text{SIG}(R, \text{BS})}(\lambda)$ ，敌手 A 赢得游戏的概率是可忽略的，即

$$\Pr[\text{bSigForge}_{A, \text{SIG}(R, \text{BS})}(\lambda) = 1] \leq \text{negl}(\lambda) \quad (4)$$

则称数字签名方案 $\text{SIG}_{R, \text{BS}}$ 是 bEUF-CMA 安全的。

游戏 $\text{bSigForge}_{A, \text{SIG}(R, \text{BS})}$ 定义如下。

初始化阶段：模拟器 S 运行参数生成算法生成公私钥以及困难关系对，将公钥 pk 和困难关系状态 Y 交给敌手 A ，保留私钥 sk 以回答敌手的盲签名、预签名和签名询问。消息询问集合 Q_m 初始化为空。

盲签名询问阶段：敌手 A 可以选择任意盲消息 c_i 作盲签名询问，模拟器 S 运行 $\delta'' = \text{bSign}_{\text{sk}}(c, t)$ 算法，将 c_i 和对应盲签名发送给敌手。

预签名询问阶段：敌手 A 可以选择任意消息 m_i 作预签名询问，模拟器 S 将消息 m_i 加入消息询问集合 Q_m ，运行 $\delta' \leftarrow \text{pSign}_{\text{sk}}(m, Y)$ 交互协议，将 m_i 和对应预签名发送给敌手。

签名询问阶段：敌手可以选择任意消息 m_i 作签名询问，模拟器 S 将消息 m_i 加入消息询问集

合 Q_m , 产生一个签名值 $\delta \leftarrow \text{Sign}_{\text{sk}}(m_i)$, 将 m_i 和对应签名发送给敌手。

预签名伪造阶段：敌手 A 选择要挑战的消息 m^* 发送给模拟器 S , 模拟器将关于 (m^*, Y) 的盲签名 δ'' 发送给敌手 A , 敌手 A 给出针对消息 m^* 的伪造预签名。若伪造的预签名验证通过且 m^* 不属于 Q_m , 则敌手赢得游戏。

全签名伪造阶段：敌手 A 选择要挑战的消息 m^* 发送给模拟器 S , 模拟器将关于 (m^*, Y) 的预签名值 δ^* 发送给敌手 A , 敌手 A 给出针对消息 m^* 的伪造签名。若伪造的签名验证通过且 m^* 不属于 Q_m , 则敌手赢得游戏。

定义6 证据可提取性。当任意的多项式时间敌手赢得游戏 $\text{WitExact}_{A, \text{SIG}_{(R, \text{BS})}}(\lambda)$ 的概率是可忽略的, 即

$$\Pr[\text{WitExact}_{A, \text{SIG}_{(R, \text{BS})}}(\lambda) = 1] \leq \text{negl}(\lambda) \quad (5)$$

则称数字签名方案 $\text{SIG}_{R, \text{BS}}$ 是证据可提取的。

游戏 $\text{WitExact}_{A, \text{SIG}_{(R, \text{BS})}}(\lambda)$ 的定义如下。

初始化阶段：模拟器 S 和敌手 A 运行参数生成算法生成公私钥对 (pk, sk) 和困难关系对 (Y, y) , 模拟器将公钥 pk 和困难关系状态 Y 交给敌手 A , 保留私钥 sk 和困难关系证据 y 以回答敌手的预签名和签名询问。消息询问集合 Q_m 初始化为空。

预签名询问阶段：敌手 A 可以选择任意消息 m_i 进行预签名询问, 模拟器 S 将消息 m_i 加入消息询问集合 Q_m , 产生一个预签名值 $\delta' \leftarrow \text{pSign}_{\text{sk}}(m_i, Y)$, 将 m_i 和对应预签名发送给敌手。

签名询问阶段：敌手可以选择任意消息 m_i 作签名询问, 模拟器 S 将消息 m_i 加入消息询问集合 Q_m , 产生一个签名值 $\delta \leftarrow \text{Sign}_{\text{sk}}(m_i)$, 将 m_i 和对应签名发送给敌手。

签名伪造阶段：敌手 A 选择要挑战的消息 m^* 和状态发送给模拟器 S , 模拟器将关于 (m^*, Y^*) 的预签名值 δ'' 发送给敌手 A , 敌手 A 给出针对消息 m^* 的伪造签名 δ^* 。

证据提取阶段：模拟器 S 通过 Exact 算法提取 $y' = \text{Exact}(\delta^*, \delta'', Y^*)$ 。若签名验证通过, 同时 m^* 不属于 Q_m , 且 (Y^*, y') 不属于 R , 则敌手赢得游戏。

3 基于SM2的盲适配器签名方案

本节根据系统模型的定义构造基于SM2的盲适配器签名方案并给出预签名正确性证明。

3.1 方案构造

采用素数阶的椭圆曲线有限域, 符号定义与预备知识所定义的符号一致, 如图1所示, 基于SM2的盲适配器签名方案包含5个角色: 签名者、适配者、用户、验证者、提取者, 7个算法。

(1) 初始化算法 $\text{params} \leftarrow \text{Setup}(\lambda)$: 以安全参数 λ 为输入, 签名者生成密钥对 $(\text{pk}, \text{sk}) = (x, P)$, 临时密钥对 (T, t) , 公开公钥 pk , 临时密钥 T , 保密私钥 sk 和临时密钥 t ; 适配者生成困难关系对 (Y, y) , 计算承诺 $A_a = yP + Y$, 公开困难关系状态 Y 和承诺 A_a , 保密证据 y ; 签名者计算承诺 $A_s = (1 + x)Y$ 并公开; 用户验证 $A_a = A_s$ 是否成立, 若成立则 $A = A_a$, 则初始化成功输出 true , 否则输出 false 。

(2) 消息盲化算法 $(r, c) \leftarrow m\text{Blind}(m, T, A, \text{pk})$: 用户随机选择盲化因子 $\alpha, \beta \in Z_n^*$, 计算 $K = \alpha T + \beta G$, $r = H(m) + f(K + A)$, $c = \alpha^{-1}(r + \beta) \bmod n$, 发送 c 给签名者。

(3) 盲签名生成算法 $\delta'' = b\text{Sign}_{\text{sk}}(c, t)$: 签名者计算 $s'' = (1 + x)^{-1}(t - cx) \bmod n$, 令盲签名值 $\delta'' = (c, s'')$ 并将其发送给用户。

(4) 解盲算法 $\delta' = u\text{Blind}_{\alpha, \beta}(\delta'', r)$: 用户计算 $s' = (\alpha s'' + \beta)$, 令预签名值 $\delta' = (r, s')$ 。

(5) 预签名验证算法 $\text{pVrfy}_{\text{pk}}(m, A, \delta')$: 验证者验证 $A = A_a$ 是否成立, 若成立则计算 $K' = s' \cdot G + (r + s') \cdot P$, $r' = H(m) + f(K' + A)$, 验证 $r' = r$ 是否成立, 若成立输出 true , 否则输出 false 。

(6) 适配算法 $\delta = \text{Adapt}(\delta', y)$: 适配者计算 $s = s' + y$, 令签名值 $\delta = (r, s)$, δ 即为适配的正式签名值。

(7) 提取算法 $y' = \text{Exact}(\delta, \delta', Y)$: 提取者计算 $y' = s - s'$, 验证 $(Y, y') \in R_G$ 是否成立, 若成立, 则困难关系证据为 y' 。

3.2 预签名正确性

根据预签名正确性的定义, SM2盲适配器签

params $\leftarrow$ Setup (λ)	(r, c) $\leftarrow$ mBlind (m, T, A, pk)	pVrfy _{pk} (m, A, δ')
签名者: $x \leftarrow Z_n^*$ $P = xG$ $t \leftarrow Z_n^*$ $T = tG$ $sk = x$ $pk = P$ 适配者: $y \leftarrow Z_n^*$ $Y = yG$ $A_s = yP + Y$ 签名者: $A_s = (1+x)Y$ 用户: if $A_s = A_s$ then $A = A_s$ return true else return false	用户: $\alpha, \beta \leftarrow Z_n^*$ $K = \alpha T + \beta G$ $r = H(m) + f(K + A)$ $c = \alpha^{-1}(r + \beta) \bmod n$ return (r, c) send c to Signer $\delta'' = \text{bSign}_{sk}(c, t)$ 签名者: $s'' = (1+x)^{-1}(t - cx) \bmod n$ send (c, s'') to User $\delta'' = \text{uBlind}_{\alpha, \beta}(\delta'', r)$ 用户: $s' = (\alpha s'' + \beta)$ $\delta' = (r, s')$ return δ'	验证者: $\leftarrow \mathcal{I}$ $K' = s' \cdot G + (r + s') \cdot P$ $r' = H(m) + f(K' + A)$ if $r' = r$ then return true else return false $\delta = \text{Adapt}(\delta', y)$ 适配者: $s = s' + y$ $\delta = (r, s)$ return δ $y' = \text{Exact}(\delta, \delta', Y)$ 提取者: $y' = s - s'$ if $(Y, y') \in R_G$ then return y' else return false

图1 SM2盲适配器签名

Figure 1 Blind adaptor signature base on the SM2

名的预签名正确性证明如下。

定理1 基于SM2的盲适配器签名方案满足预签名正确性。

证明：给定私钥 x 、困难问题证据 y 和消息 m ，则有 $P = xG$ ， $Y = yG$ ， $A = yP + Y$ 。对于本方案产生的预签名值 $\delta' = (r, s')$ ，有

$$K^* = s'G + (r + s')P = \alpha T + \beta G \quad (6)$$

所以 $K^* = K$ ，即 $r^* = r$ 必然成立。根据适配算法的定义可知， s 和 s' 间只差一个 y ，那么

$$sG + (r + s)P = s'G + (r + s')P + A \quad (7)$$

由于 $A = yP + Y = (1+x)Y$ 在系统初始化时就经过用户的验证，所以通过提取算法提取到的 y' 必然是 Y 的证据，即 $(Y, y') \in R_G$ 。

4 安全性证明

本节根据第2节定义的安全模型，依次证明本文方案满足盲性、预签名可适配性、bEUF-CMA安全性和证据可提取性。

定理2 基于SM2的盲适配器签名方案具有盲性。

证明：构造模拟器 S 可随机产生一个比特 $b \in (0, 1)$ ，假设存在诚实用户 U_0 和 U_1 ，存在敌手 A 想要在多项式时间内赢得游戏 $\text{Blind}_{A, \text{SIG}(R, \text{BS})}(\lambda)$ ，

根据 $\text{Blind}_{A, \text{SIG}(R, \text{BS})}(\lambda)$ 定义，游戏交互过程如下。

消息产生阶段：敌手产生2个消息 m_0, m_1 。

比特选择阶段：模拟器随机选择 $b \in (0, 1)$ ，将 m_b, m_{1-b} 分别发送给 U_0 和 U_1 。

盲消息询问阶段： U_0 和 U_1 分别发起 m_b, m_{1-b} 的盲消息询问，模拟器返回盲化结果 c_b, c_{1-b} ， U_0 和 U_1 分别将盲化结果发送给敌手 A 进行盲签名。

敌手 A 分别计算 c_b, c_{1-b} 的盲签名，分别返回 (c_b, s''_b) 和 (c_{1-b}, s''_{1-b}) 给用户 U_0 和 U_1 。

解盲阶段： U_0 和 U_1 分别发起 (c_b, s''_b) ， (c_{1-b}, s''_{1-b}) 的解盲询问，模拟器解盲并适配后返回 $\delta_b = (r_b, s'_b)$ 、 (r_{1-b}, δ_{1-b}) 给 U_0 和 U_1 ， U_0 和 U_1 将 δ_b, δ_{1-b} 发送给敌手 A 。

比特猜测阶段：敌手 A 输出对 b 的猜测 b^* 。

若 $b^* = b$ ，则敌手 A 赢得游戏，假设敌手保存了 c_b, c_{1-b} ，但是由于敌手无法获得随机数 α, β ，也就无法从 c_b, c_{1-b} 与 r_b, r_{1-b} 中计算出 m_b, m_{1-b} ，即敌手只能以1/2的概率判定 b 的值，根据游戏的定义，攻击者赢得游戏的优势可忽略，所以本文方案具有盲性。

定理3 基于SM2的盲适配器签名方案满足预签名可适配性。

证明：对于任意的公钥 $P \in G$ ，困难关系实

例 $(Y, y) \in R_G$ 、消息 m 和预签名值 $\delta' = (r, s')$ ，如果 $\text{pVrfy}_{\text{pk}}(m, A, \delta') = 1$ 成立，则有

$$r = H(m) + f(s'G + (r + s')P + A) \quad (8)$$

根据适配算法的定义，有 $s = s' + y$ ，那么 $(s - y)G + (r + s - y)P + yP + Y = sG + (r + s)P$ 得到的签名 δ 是一个关于公钥和消息的有效签名。

定理4 如果SM2签名方案满足EUF-CMA安全性，且 R_G 是一个困难关系，则基于SM2的盲适配器签名方案满足bEUF-CMA安全性。

证明：构造一个模拟器S，假设存在敌手A想要在多项式时间内赢得游戏 $\text{bSigForge}_{A, \text{SIG}_{(R, \text{BS})}}$ ，按照游戏 $\text{bSigForge}_{A, \text{SIG}_{(R, \text{BS})}}$ 的定义，双方交互过程如下。

初始化阶段：模拟器S控制签名预言机生成密钥对 (pk, sk) 和困难关系对 (Y, y) ，将公钥 pk 和困难关系状态 Y 交给敌手A，保留私钥 sk 和困难关系证据 y 以回答敌手的盲签名、预签名和签名询问。消息询问集合 Q_m 、盲消息询问集合 Q_c 和哈希询问集合 Q_h 均初始化为空。

哈希询问阶段：当敌手A询问 m_x 的哈希值时，S先查询 Q_h 中是否存在 $H(m_x)$ ，若存在，则直接取出，否则产生 $H(m_x)$ ，并将 $(m_x, H(m_x))$ 并入 Q_h 集合中，最后返回 $H(m_x)$ 给A。

盲消息询问阶段：当敌手A自适应地选择消息 m_i 作盲化消息询问时，S先查询集合 Q_c 中是否存在 c_{m_i} ，若存在，则直接取出，否则根据盲化算法随机产生 $c_{m_i} \leftarrow \text{mBlind}(m_i, Y)$ 并将 (m_i, c_{m_i}) 并入 Q_c 集合中，最后返回 c_{m_i} 给敌手。

盲签名询问阶段：当敌手A自适应地选择消息 m_i 作盲签名询问时，模拟器S进行如下操作。

(1) 模拟器S发起关于 m_i 的盲消息询问获取盲化消息 c_{m_i} ；

(2) 计算 $s'' = (1 + x) - 1(t - (c_{m_i})x) \bmod n$ ；

(3) 输出盲签名值 $\delta'' = (c_{m_i}, s'')$ ；

(4) 模拟器S将 δ'' 返回给敌手A。

预签名询问阶段：当敌手A自适应地选择盲签名 s'' 作预签名询问时，模拟器S进行如下操作。

(1) 模拟器S发起关于 m_i 的盲签名询问获取

盲签名 $\delta'' = (c, s'')$ ；

(2) 计算 $s' = as'' + \beta$ ；

(3) 更新集合 $Q_m = Q_m \cup \{m_i\}$ ；

(4) 输出预签名值 $\delta' = (r, s')$ ；

(5) 模拟器S将 δ' 返回给敌手A。

签名询问阶段：当敌手A自适应地选择消息 m_i 作签名询问，模拟器S进行如下操作。

(1) 模拟器S发起关于 m_i 的预签名询问获取预签名值 $\delta' = (r, s')$ ；

(2) 计算 $s = s' + y$ ；

(3) 更新集合 $Q_m = Q_m \cup \{m_i\}$ ；

(4) 输出签名值 $\delta = (r, s)$ ；

(5) 模拟器S将 δ 发送给敌手A。

预签名伪造阶段：敌手A选择要伪造预签名的消息 m^* ，模拟器S运行 $\delta'' \leftarrow \text{bSign}_{\text{sk}}(m^*, Y)$ ，将关于 (m^*, Y) 的盲签名值 δ'' 发送给敌手A，敌手A给出针对消息 m^* 的伪造预签名 δ^* 。

全签名伪造阶段：敌手A自适应地选择盲消息 c_{m^*} ，模拟器S运行 $\delta' = \text{uBlind}_{\alpha, \beta}(\delta'', r)$ ，将关于 (m^*, Y) 的预签名值 δ' 发送给敌手A，敌手A给出针对消息 m^* 的伪造签名 δ^* 。

若预签名值 δ^* 是有效的且 m^* 未出现在集合 Q_m 中，或签名值 δ^* 是有效的且 m^* 未出现在集合 Q_m 中，则敌手成功伪造了签名。由于盲签名的计算引入了2个随机盲化因子，同时推测出2个随机盲化因子的概率是可忽略的，从盲签名入手伪造一个SM2预签名的概率也是可忽略的，即敌手从盲签名入手成功伪造全签名的概率是可忽略的。假定 (Y, y) 属于困难关系，敌手只可能通过Exact算法从预签名和全签名中获取证据 y ，伪造一个SM2签名的概率是可忽略的，所以敌手获取证据 y 的概率也是可忽略的，即敌手从预签名入手成功伪造全签名的概率是可忽略的。所以敌手赢得游戏 $\text{bSigForge}_{A, \text{SIG}_{(R, \text{BS})}}$ 的概率是可忽略的。

定理5 如果SM2签名方案满足EUF-CMA安全性，且 R_G 是一个困难关系，则基于SM2的盲适配器签名方案满足证据可提取性。

证明：构造一个模拟器S可以控制SM2签名预言机。假设存在敌手A想要在多项式时间内赢得游戏 $\text{WitExact}_{A, \text{SIG}_{(R, \text{BS})}}(\lambda)$ ，按照 $\text{WitExact}_{A, \text{SIG}_{(R, \text{BS})}}(\lambda)$

游戏的定义, 双方交互过程如下。

模拟器 S 控制签名预言机生成密钥对 (pk, sk) 和困难关系对 (Y, y) , 将公钥 pk 和困难关系状态 Y 交给敌手 A , 保留私钥 sk 和困难关系证据 y 以回答敌手的预签名询问和签名询问。消息询问集合 Q_m 和哈希询问集合 Q_h 均初始化为空。

哈希询问阶段: 与游戏 $bSigForge_{A, SIG_{(R, BS)}}$ 的哈希询问阶段一致。

预签名询问阶段: 当敌手 A 自适应地选择消息 m_i 作预签名询问时, 模拟器进行如下操作。

(1) 模拟器 S 发起关于 m_i 的签名询问, 获取签名值 $\delta = Sign_{sk}(m_i) = (r, s)$;

(2) 计算 $s' = s - y$;

(3) 更新集合 $Q_m = Q_m \cup \{m_i\}$;

(4) 输出预签名值 $\delta' = (r, s')$;

(5) 模拟器 S 将 δ' 返回给敌手 A 。

签名询问阶段: 敌手 A 自适应地选择消息 m_i 作签名询问, 模拟器 S 将消息 m_i 加入消息询问集合 Q_m , 模拟器 S 发起关于 m_i 的签名询问, 获取签名值 $\delta = Sign_{sk}(m_i)$ 并将其返回给敌手。

签名伪造阶段: 敌手 A 选择要伪造全签名的消息 m^* , 模拟器 S 运行 $\delta' \leftarrow pSign_{sk}(m^*, Y^*)$, 将关于 (m^*, Y^*) 的预签名值 δ' 发送给敌手 A , 敌手 A 给出针对消息 m^* 的伪造签名 δ^* 。

证据提取阶段: 模拟器 S 接收到伪造签名值 δ^* 后, 验证 $\delta^* = Adapt(\delta', y)$ 是否成立。

若签名验证通过, 同时 m^* 不属于 Q_m , 且 (Y^*, y) 不属于 R , 则敌手赢得游戏。如果敌手伪造的签名 δ^* 是有效的, 同时 $m^* \notin Q_m$, 意味着 (m^*, δ^*) 可以作为一个合法消息-签名对攻击 SM2 签名方案的不可伪造性, 其概率是可忽略的, 或者攻击者 A 从别处获取到困难关系证据, 适配的签名通过验证, 则 $(Y, y) \in R$ 一定成立, 且 A 从别处获取到困难关系证据的概率是可忽略的, 故敌手赢得游戏 $WitExact_{A, SIG_{(R, BS)}}(\lambda)$ 的概率是可忽略的。

5 性能分析

为评估新方案性能, 将本文方案与同类方案^[24]从计算时间、盲性和所基于数字签名算法几

方面进行性能理论对比分析。

在性能理论对比分析前, 先将所需的符号进行如下定义: T_{gm} 、 T_{ga} 和 T_{gs} 分别表示群 G 中点乘、点加和点逆的计算耗时, T_{inv} 、 T_{mul} 和 T_{add} 分别表示 Z_n 中模逆、模乘、模加的计算时间, T_h 表示一次哈希运算的计算时间, T_p 和 T_v 分别表示零知识证明生成与验证的计算时间。

表 1 ECDSA 盲适配器签名方案与本文方案性能对比
Table 1 Performance comparison between ECDSA blind adaptor signature scheme and the proposed scheme in this paper

方案名称	计算时间/ms	盲性	算法类型
ECDSA 盲适配器签名方案	$4T_{inv} + 6T_{mul} + 4T_{gm} + 2T_h + T_{add} + T_p + T_v$	弱盲	国外
本文方案	$2T_{inv} + 4T_{mul} + 6T_{gm} + 2T_h + 6T_{add} + 4T_{ga}$	盲性	国密

如表 1 所示, 与基于 ECDSA 盲适配器签名方案相比, 在计算开销上, 由于本文方案多了消息盲化和解盲的过程, 总计算时间为 $2T_{inv} + 4T_{mul} + 6T_{gm} + 2T_h + 6T_{add} + 4T_{ga}$, ECDSA 盲适配器签名方案只在 ECDSA 适配器签名方案基础上多了一次零知识证明生成和验证的过程, 总计算时间为 $4T_{inv} + 6T_{mul} + 4T_{gm} + 2T_h + T_{add} + T_p + T_v$, 本文方案比 ECDSA 盲适配器签名方案多 2 个点乘、4 个点加、5 个模加, 少 2 个模逆、2 个模乘、一个零知识证明生成和验证的计算时间。在盲性上, ECDSA 盲适配器签名只是将签名消息取了哈希给签名者, 使得签名者无法知道被签名消息的具体内容, 属于弱盲性。本文提出的 SM2 盲适配器签名方案引入了盲化因子 α, β , 签名者不仅无法知道被签名消息的具体内容, 即使最后消息-签名对被公开, 签名者也无法获得消息和签名过程的联系, 盲性相对而言较强。最后, ECDSA 盲适配器签名基于国外签名算法 ECDSA, 本文方案基于国密算法 SM2, 具有自主可控的优势。

本文实验环境如下。操作系统: ubuntu 20.04; 处理器: i9-12900H 2.50 GHz; 内存: 8 GB; 编程语言: Golang 1.17.13。

为了测试本文方案的运行效率, 在测试环境中, 对方案各算法的时间进行测试, 对一个比特币区块大小, 即 1M 的消息进行 1 000 次 SM2 盲

适配器签名, 分别计算系统初始化、消息盲化、盲签名、解盲、预签名验证、适配和提取的运行时间, 结果取1 000次测试的运行时间平均值, 测试结果如图2所示。

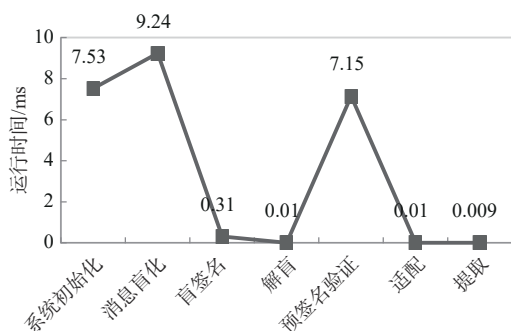


图2 本文方案各算法平均运行时间
Figure 2 Average operation time of the scheme

系统初始化时间为7.53 ms, 消息盲化时间9.24 ms, 盲签名、解盲、适配和提取时间均不到1 ms, 预签名验证时间7.15 ms。其中, 时间最长的是消息盲化算法, 但是系统初始化算法包含的密钥生成、临时密钥生成、困难关系对生成和承诺的计算都可以在签名前进行预计算, 因此, 本文方案的执行时间在正常签名运行时间范围内。

在测试环境中, 对方案整体运行过程时间进行测试, 分别对1 B、1 KB、10 KB、100 KB和1 MB的消息进行1 000次SM2适配器签名和1 000次SM2盲适配器签名, 计算方案整体运行时间, 结果取1 000次测试的运行时间平均值, 测试结果如表2所示。在对1 B、1 KB、10 KB、100 KB和1 MB的消息进行签名时, 本文方案比SM2适配器签名方案时间分别增加了4.87 ms、5.2 ms、7.37 ms、6.47 ms和5.66 ms, 平均增加了5.91 ms, 但本文方案增加了消息盲化和解盲过程, 所以签名阶段的时间有所增加是合理的。

表2 运行时间对比
Table 2 Comparison of running time

方案	单位: ms				
	1 B	1 KB	10 KB	100 KB	1 MB
SM2 AS	6.49	7.01	9.94	9.52	18.63
本文方案	11.36	12.21	17.31	15.99	24.29

6 结束语

针对适配器签名不具备匿名性问题, 本文提

出了新的盲适配器签名的系统模型和安全模型, 基于新的系统模型, 提出了一种基于SM2签名算法的盲适配器签名方案。基于SM2签名方案的EUF-CMA安全性和困难关系 R_G 证明了该新方案的安全性满足新提出的安全模型要求。性能分析表明, 与ECDSA盲适配器签名方案相比, 本文方案盲性更强且具有自主可控性, 与SM2适配器签名方案相比, 本文方案总时间仅增加了5.91 ms。在区块链隐私保护意识不断提升, 国密算法越来越受欢迎的大环境下, 本文方案在各种关键应用场景中都具有广泛的潜力和价值, 尤其是需要采用国产密码算法以确保重要信息安全的关键应用场景。下一步, 考虑将方案应用到实际应用中, 以发现并解决应用上的问题, 优化本方案的计算效率, 以扩大应用场景。

参考文献:

- [1] DESHPANDE A, HERLIHY M. Privacy-preserving cross-chain atomic swaps[M]//Financial Cryptography and Data Security. Cham: Springer International Publishing, 2020: 540-549.
- [2] GUGGER J. Bitcoin-Monero cross-chain atomic swap[J]. IACR Cryptology ePrint Archive, 2020: 1026.
- [3] AUMAYR L, ERSOY O, ERWIG A, et al. Generalized channels from limited blockchain scripts and adaptor signatures[M]. Cham: Springer International Publishing, 2021: 635-664.
- [4] MALAVOLTA G, MORENO-SANCHEZ P, SCHNEIDEWIND C, et al. Anonymous multi-hop locks for blockchain scalability and interoperability[C]//Proceedings 2019 Network and Distributed System Security Symposium. Reston, VA: Internet Society, 2019: 1-15.
- [5] SCHNORR C P. Efficient signature generation by smart cards[J]. Journal of Cryptology, 1991, 4(3): 161-174.
- [6] KERRY C F, GALLAGHER P D. Digital signature standard[S]. 2013.
- [7] ERWIG A, FAUST S, HOSTÁKOVÁ K, et al. Two-party adaptor signatures from identification schemes[C]//GARAY JA. IACR International Conference on Public-Key Cryptography. Cham: Springer, 2021: 451-480.
- [8] 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.
- [9] 王子瑞, 张驰, 魏凌波. 基于双线性配对的适配器签名方案[J]. 密码学报, 2022, 9(4): 686-697.
WANG Z R, ZHANG C, WEI L B. Adaptor signatures from bilinear pairings[J]. Journal of Cryptologic Research, 2022, 9(4): 686-697.

- [10] 张艳硕, 刘宁, 袁煜淇, 等. 基于 ISRSAC 数字签名算法的适配器签名方案[J]. 通信学报, 2023, 44(3): 178-185.
ZHANG Y S, LIU N, YUAN Y Q, et al. Adaptor signature scheme based on ISRSAC digital signature algorithm[J]. Journal on Communications, 2023, 44(3): 178-185.
- [11] ERWIG A, RIAHI S. Deterministic wallets for adaptor signatures[C]//European Symposium on Research in Computer Security. Cham: Springer, 2022: 487-506.
- [12] 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.
- [13] CHAUM D. Blind signatures for untraceable payments[C]//CHAUM D, RIVEST RL, SHERMAN AT. Advances in Cryptology. Boston, MA: Springer, 1983: 199-203.
- [14] RÜCKERT M. Lattice-based blind signatures[C]//International Conference on the Theory and Application of Cryptology and Information Security. Berlin, Heidelberg: Springer, 2010: 413-430.
- [15] 常亮, 韩同壮, 马仲博. 一种基于 ECC 的同态加密盲签名方法[J]. 通信技术, 2020, 53(8): 1983-1987.
CHANG L, HAN T Z, MA Z B. A blind signature method of based on ECC homomorphic encryption[J]. Communications Technology, 2020, 53(8): 1983-1987.
- [16] 何德彪, 张语获, 张方国, 等. 一种轻量级 SM2 盲签名生成方法及系统: CN110213048A[P]. 2019-09-06.
HE D B, ZHANG Y D, ZHANG F G, et al. A lightweight SM2 blind signature generation method and system[P]. 2019-09-06.
- [17] 唐卫中, 张大伟, 佟晖. 基于 SM2 的无证书盲签名方案[J]. 计算机应用研究, 2022, 39(2): 552-556.
TANG W Z, ZHANG D W, TONG H. Certificateless blind signature scheme based on SM2[J]. Application Research of Computers, 2022, 39(2): 552-556.
- [18] 吕尧, 侯金鹏, 聂冲, 等. 基于 SM9 算法的部分盲签名方案[J]. 网络与信息安全学报, 2021, 7(4): 147-153.
LYU Y, HOU J P, NIE C, et al. Partial blind signature scheme based on SM9 algorithm[J]. Chinese Journal of Network and Information Security, 2021, 7(4): 147-153.
- [19] LI C, JIANG B, GUO Y, et al. Efficient group blind signature for medical data anonymous authentication in blockchain-enabled IoMT[J]. Computers, Materials & Continua, 2023, 76(1).
- [20] 白雪, 秦宝东, 郭瑞, 等. 基于 SM2 的两方协作盲签名协议[J]. 网络与信息安全学报, 2022, 8(6): 39-51.
BAI X, QIN B D, GUO R, et al. Two-party cooperative blind signature based on SM2[J]. Chinese Journal of Network and Information Security, 2022, 8(6): 39-51.
- [21] SHENTU Q C, YU J P. A blind-mixing scheme for Bitcoin based on an elliptic curve cryptography blind digital signature algorithm[J]. Computer Science, 2015: 1510.
- [22] YI X, LAM K Y. A new blind ECDSA scheme for Bitcoin transaction anonymity[C]//Proceedings of the Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security. New York: ACM, 2019: 613-620.
- [23] DESHPANDE A, HERLIHY M. Privacy-preserving cross-chain atomic swaps[C]//International Conference on Financial Cryptography and Data Security. Cham: Springer, 2020: 540-549.
- [24] 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.
- [25] 国家密码管理局. SM2 椭圆曲线公钥密码算法[S]. 2010. OSCCA. Elliptic curve public key cryptography algorithm[S]. 2010.

[作者简介]



胡小明 (1978-), 女, 浙江慈溪人, 上海第二工业大学教授, 主要研究方向为密码学、区块链安全及隐私保护。



陈海婵 (1998-), 女, 广西贵港人, 上海第二工业大学硕士生, 主要研究方向为区块链隐私保护。