计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2021.20210645
58(10):2278-2286,2021

# 基于SM2数字签名算法的适配器签名方案

彭 聪[1] 罗 敏[1] 何德彪[1] 黄欣沂[2]
[1](武汉大学国家网络安全学院 武汉 430072)
[2](福建师范大学计算机与网络空间安全学院 福州 350117)
(cpeng@whu.edu.cn)

# Adaptor Signature Scheme Based on the SM2 Digital Signature Algorithm

Peng Cong[1], Luo Min[1], He Debiao[1], and Huang Xinyi[2]
[1](*School of Cyber Science and Engineering, Wuhan University, Wuhan* 430072)
[2](*College of Computer and Cyber Security, Fujian Normal University, Fuzhou* 350017)

**Abstract** The adaptor signature scheme is an extension of the standard digital signature, which can create a "pre-signature" that implies the state of a hard relation (such as discrete logarithm problems) and can be transformed into a completed signature by the witness of the hard relation. The completed signature can be verified by the verification algorithm of a standard signature scheme. Intuitively, an adaptor signature has two properties: 1) only users who know the witness can transform the pre-signature into a completed signature; 2) any user may extract the witness through a pre-signature and a completed signature. Thus, the adaptor signature scheme can provide the atomic exchange property in the blockchain, and has been proved to be very widely used in practice. Based on the SM2 digital signature algorithm, a new adaptor signature scheme (SM2-AS) is constructed in this paper. This scheme can effectively match the SM2 signature scheme's key generation, signature generation and signature verification algorithms. Moreover, under the random oracle model, we prove that the SM2-AS scheme is secure, that is, it satisfies the pre-signature correctness, pre-signature adaptability, existential unforgeability under chosen plaintext attacks, and witness extractability. Through theoretical analysis and experimental test, the performance of the SM2-AS scheme is comparable to that of ECDSA-based adaptor signature scheme, but obviously weaker than that of the Schnorr-based adaptor signature scheme.

**Key words** blockchain technology; payment channel; SM2 signature; adaptor signature; atomic exchange

**摘 要** 适配器签名(adaptor signature)方案是标准数字签名的一种扩展形式,它可以创建一个隐含困难关系(例如离散对数)状态的"预签名",并通过困难关系证据将该预签名转换为一个完整签名,且转换

**收稿日期**:2021-06-11;**修回日期**:2021-07-30
**基金项目**:国家自然科学基金项目(61972294,61932016,62032005);山东省重点研发计划项目(2020CXGC010107);湖北省科技重大专项(2020AEA013);湖北省自然科学基金项目(2020CFA052);武汉市科技计划项目(2020010601012187)
This work was supported by the National Natural Science Foundation of China (61972294, 61932016, 62032005), the Key Research and Development Program of Shandong Province (2020CXGC010107), the Special Project on Science and Technology Program of Hubei Provience (2020AEA013), the Natural Science Foundation of Hubei Province (2020CFA052), and the Science and Technology Project of Wuhan Municipal (2020010601012187).
**通信作者**:罗敏(mluo@whu.edu.cn)

后的完整签名可通过一个标准签名方案的验证算法验证其有效性.直观地说,适配器签名应具备 2 个属性:1)只有知道困难关系证据的用户才能够将预签名转变为完整签名;2)任何用户可以通过预签名和完整签名提取困难关系证据.基于这 2 个性质,适配器签名方案能够在区块链中提供很好的原子交换性质,并已在实践中得以广泛应用.以 SM2 数字签名算法为基础,构造了一个新的适配器签名方案(记为 SM2-AS).该方案能够有效地衔接 SM2 签名方案的密钥生成、签名生成和签名验证算法.在随机预言模型下证明了 SM2-AS 方案是安全的,即满足预签名正确性、预签名可适配性、选择明文攻击下的存在不可伪造性和证据可提取性.理论分析和实验测试表明:SM2-AS 方案的性能虽然弱于 Schnorr 适配器签名方案,但与 ECDSA 适配器签名方案相当.

**关键词**　区块链技术;支付通道;SM2 签名;适配器签名;原子交换

**中图法分类号**　TP393.08

在过去几年中,区块链技术受到了学术界、产业界以及政府部门的高度关注,它能够在互不信任的分布式系统中实现安全支付、数据交易甚至更为普适的计算模式.它的核心是通过一个去中心化的共识协议,每个参与节点共同建立并维护一个存储所有交易的分布式账本.以比特币、以太坊为代表的数字货币均依赖于区块链系统,并基于区块链的脚本语言提供丰富的交易方式.虽然区块链上每笔交易记录具有公开可验证性,但它的交易吞吐量扩展问题也非常明显[1].例如,比特币每秒大约可以完成 10 笔交易,比信用卡网络低 3 个数量级[2].

为解决区块链交易扩容问题,研究人员提出了支付通道(payment channels)[3]的概念,即在不破坏交易安全性的前提下支持任意数量的线下交易,且仅将最终的交易状态上链,从而完成交易.比特币中的闪电网络(Lightning Network)[4]和以太坊中的雷电网络(Raiden Network)[5]均采用支付通道技术实现.然而,构建支付通道的一个关键点是如何撤销旧的交易状态.为此,以闪电网络为代表的支付通道采用了惩罚机制来让受骗方获取所有的货币(包括不诚实交易方的货币)[6].由于矿工收取的交易费用与每笔交易中包含的脚本大小以及矿工验证所需的计算量成正比,故需要尽可能的降低链上交易规模.一种有效的途径是在链下管理一些交易逻辑,即将交易逻辑编码为发送方和接收方之间的点对点协议,而不是直接在交易脚本中进行逻辑编码.由此出发,Polestra 引入了无脚本脚本(scriptless scripts)的概念[7],后来将其形式化为适配器签名(adaptor signature, AS)[8-9].

适配器签名方案是标准数字签名的一种扩展形式,它可以创建一个隐含困难关系(例如离散对数)状态的"预签名",并通过困难关系证据将该预签名可以转换为一个完整签名,且转换得到的完整签名可以由一个标准签名方案的验证算法验证有效性.直观地说,适配器签名应具备 2 个属性:1)只有知道困难关系证据的用户才能够将预签名转变为完整签名;2)任何用户可以通过预签名和完整签名提取困难关系证据.基于这 2 个性质,适配器签名方案能够在区块链中提供很好的原子交换性质,并已在实践中被证明应用非常广泛.例如,它可以构建链下支付应用程序,包括通用支付通道[8]、支付通道网络[10]、支付通道集线器[11]等,也可被实际的区块链协议采用,例如闪电网络、雷电网络等.

在本文中,我们以 SM2 数字签名算法为基础,构造了一个新的适配器签名方案,记为 SM2-AS.该方案能够有效地衔接 SM2 签名方案的密钥生成、签名生成和签名验证算法.我们在随机预言模型下证明了 SM2-AS 方案是安全的,即满足预签名正确性、预签名可适配性、选择明文攻击下的存在不可伪造性和证据可提取性.理论分析和实验测试表明,SM2-AS 方案的性能虽然弱于 Schnorr 适配器签名方案,但与 ECDSA 适配器签名方案相当.

## 1　相关工作

在 Polestra 提出无脚本脚本[7]的概念后,Aumayr 等人[8]设计了基于 Schnorr 签名和 ECDSA 签名的适配器签名方案,并将其用于通用支付通道的构建.Malavolta 等人[10]基于单向同态函数构建了适配器签名方案.同年,Moreno-Sanchez 等人[12]针对门罗币中的可链接环签名方案构造了一个新的适配器签名,以改进门罗币的交易脚本逻辑.此外,文献[10-11]分别给出了将适配器签名方案用于构建支付通道网络和支付通道集线器的方法.

随着量子计算威胁日益增强,以太坊和零币均开展了向抗量子攻击的密码学原语迁移的计划.为此,Esgin 等人[13-14]设计了第 1 个基于标准格的适配器签名方案 LAS.但 LAS 在正确性、通信开销和隐私性方面存在一些问题,即仅具备弱预签名可适配性、较大的预签名尺寸.随后,Tairi 等人[14]设计了第 1 个基于同源的适配器签名方案 IAS,该方案是基于 CSI-Fish 签名方案扩展而成的.另外,Qin 等人[15]给出了第 1 个基于身份鉴别协议的适配器签名通用构造方法,并验证该方法可支持离散对数形式、RSA 形式、格基形式的鉴别协议.并且,Qin 等人[15]给出了适配器盲签名和可链接适配器环签名的实例.

## 2 预备知识

本节我们给出本文的符号约定,并描述签名算法、困难关系和非交互式零知识证明的概念.

### 2.1 符号约定

本文中,我们用$\mathbb{Z}_n^*$表示整数集合$\{1,2,\cdots,n-1\}$,$x\leftarrow_{\$}\mathbb{Z}_n^*$表示从集合$\mathbb{Z}_n^*$均匀随机抽取一个整数.$\{0,1\}^*$表示任意长度的比特串.$\mathbb{G}$是一个阶为 $q$ 的椭圆曲线点群,$G$ 是$\mathbb{G}$的生成元,其群运算法则用$+$表示,标量运算用 $k\cdot G$ 表示($k\in\mathbb{Z}_q^*$ 为标量).$\lambda$ 表示系统安全参数,$\varepsilon(\cdot)$表示可忽略函数.

### 2.2 签名算法

一般而言,传统的数字签名方案 $\Sigma=(Gen,Sign,Vrfy)$包含 3 个算法:密钥生成算法 $Gen$、签名生成算法 $Sign$ 和签名验证算法 $Vrfy$.各算法的功能描述为:

1) $Gen(1^\lambda)$.该算法以系统安全参数 $\lambda$ 为输入,输出一对私钥 $sk$ 和公钥 $pk$.

2) $Sign_{sk}(m)$.该算法以私钥 $sk$ 和消息 $m\in\{0,1\}^*$ 为输入,输出一个签名值 $\sigma$.

3) $Vrfy_{pk}(m;\sigma)$.该算法以公钥 $pk$、消息 $m$ 和签名值 $\sigma$ 为输入,输出验证结果 $b\in\{0,1\}$.若 $b=1$,则表示签名有效;否则,签名无效.

从安全性角度而言,若一个数字签名方案是安全的,则必须满足 2 个性质:

1) 正确性.即对任意的消息 $m$ 和密钥对$(sk,pk)$,有 $Vrfy_{pk}(m;Sign_{sk}(m))=1$.

2) 选择明文攻击下的强存在不可伪造性.即对于任意的公钥 $pk$,敌手 $\mathcal{A}$ 即使可以访问 $pk$ 对应的签名预言机,也无法伪造任意消息 $m$ 的一个新的合法签名.

### 2.3 困难关系

令 $\Pi$ 是一种二元关系,$L_\Pi$ 是描述这种关系的语言,即 $L_\Pi:=\{Y\mid\exists y\ \text{s.t.}(Y,y)\in\Pi\}$.若 3 个性质成立,则称 $\Pi$ 是一种困难关系:

1) 存在一个概率多项式时间算法能够产生一组实例,记为$(Y,y)\leftarrow Gen\Pi(1^\lambda)$.

2) 存在一个确定性的多项式时间算法能够验证给定的$(Y,y)$是否属于关系 $\Pi$.

3) 对于任意的多项式时间敌手,通过 $Y$ 计算得到 $y$ 的概率是可忽略的.

一般称 $Y$ 为困难关系状态,$y$ 为困难关系证据.

### 2.4 非交互式零知识证明

对于某种给定的困难关系,当证据持有者需要向他人证明其所拥有的证据且不泄露证据的任何信息时,就需要用到零知识证明.非交互式零知识证明(NIZK)包括 2 个算法:证明生成算法 $P$ 和证明验证算法 $V$.其中,证明生成算法 $P(Y,y)$以状态 $Y$ 和证据 $y$ 为输入,产生一个有效的证明 $\pi$;证明验证算法 $V(Y,\pi)$以状态 $Y$ 和证明 $\pi$ 为输入,输出一个比特 $b\in\{0,1\}$表示该证明是否有效.若 $b=1$,则表示证明有效;否则,表示证明无效.在本方案中,所使用的零知识证明协议需要满足 3 个性质:

1) 完备性(completeness).即对任意的$(Y,y)\in\Pi$,均有 $V(Y,P(Y,y))=1$.

2) 零知识性(zero-knowledge).即存在一个多项式时间的模拟器 $S$,能够模拟产生任意困难关系实例$(Y,y)\in\Pi$ 的一个证明 $\pi$.

3) 在线提取器(online extractor).存在一个多项式时间的在线提取器 $K$ 能够访问随机预言机的询问列表,并能够提取任意状态 $Y$ 及其证明 $\pi$ 中的证据 $y$.

## 3 适配器签名基本概念

本节我们主要介绍适配器签名的系统模型和安全模型.

### 3.1 系统模型

本质上,适配器签名是一种两步式的签名算法:拥有私钥的签名者对一个消息和一个秘密值的承诺进行预签名,拥有秘密值的适配者可将预签名值适配为完整的签名值.具体而言,适配者首先产生一个困难关系$(Y,y)\leftarrow Gen\Pi(1^\lambda)$并公开状态 $Y$;签名者对给定的消息 $m$ 和状态 $Y$ 使用私钥 $sk$ 进行预签名,并将预签名值 $\tilde{\sigma}$ 发送给适配者;适配者对于给定的

预签名值 $\tilde{\sigma}$ 使用秘密值 $y$ 进行适配,得到完整的签名值 $\sigma$.此外,任何人获取到 $\sigma$ 和 $\tilde{\sigma}$ 时,可提取秘密值 $y$.适配器签名方案的形式化定义为:

**定义 1.** 适配器签名.对于一个数字签名方案 $\Sigma=(Gen,Sign,Vrfy)$ 和一个困难关系 $\Pi$,适配器签名方案 $\Xi_{\Sigma,\Pi}=(pSign,Adapt,pVrfy,Ext)$ 包含 4 个算法:预签名生成算法 $pSign$、预签名验证算法 $pVrfy$、适配算法 $Adapt$ 和提取算法 $Ext$.各算法的功能描述为:

1) $pSign_{sk}(m,Y)$.该预签名生成算法以一个私钥 $sk$、一个消息 $m$ 和一个困难问题状态 $Y$ 为输入,输出一个预签名值 $\tilde{\sigma}$.

2) $pVrfy_{pk}(m,Y;\tilde{\sigma})$.该预签名验证算法以一个公钥 $pk$、一个消息 $m$、一个困难问题状态 $Y$ 和一个预签名值 $\tilde{\sigma}$ 为输入,输出验证结果 $b\in\{0,1\}$.若 $b=1$,则表示签名有效;否则,签名无效.

3) $Adapt(\tilde{\sigma},y)$.该适配算法以一个预签名值 $\tilde{\sigma}$ 和一个困难问题证据 $y$ 为输入,输出一个签名值 $\sigma$.

4) $Ext(\sigma,\tilde{\sigma},Y)$.该提取算法以一个签名值 $\sigma$、一个预签名值 $\tilde{\sigma}$ 和一个困难问题状态 $Y$ 为输入,输出满足 $(Y,y)\in\Pi$ 的困难问题证据 $y$ 或者失败符号 $\perp$.

### 3.2　安全模型

相比普通数字签名方案而言,适配器签名方案需要满足 5 个定义性质.

**定义 1.** 预签名正确性(pre-signature correctness).一个适配器签名方案是预签名正确的,若对于任意消息 $m$ 和任意困难问题实例 $Y$,均有:

$$Pr\left[\begin{array}{c}(pVrfy_{pk}(m,Y;\tilde{\sigma})=1)\\ \wedge\\ (Vrfy_{pk}(m;\sigma)=1)\\ \wedge\\ ((Y,y')\in\Pi)\end{array}\middle|\begin{array}{l}(sk,pk)\leftarrow Gen(1^{\lambda}),\\ \tilde{\sigma}\leftarrow pSign_{sk}(m,Y),\\ \sigma:=Adapt(\tilde{\sigma},y),\\ y':=Ext(\sigma,\tilde{\sigma},Y)\end{array}\right]=1.$$

可见,定义 1 中隐含了数字签名方案 $\Sigma$ 的正确性,并对预签名过程和证据提取过程进行正确性约束.

**定义 2.** 预签名可适配性(pre-signature adaptability).对任意的关于公钥 $pk$、消息 $m$ 和困难问题实例 $Y$ 的有效预签名值 $\tilde{\sigma}$ 使用正确的困难问题证据 $y$ 进行适配,若得到的签名值是有效的,那么称该适配器签名方案是预签名可适配的,即

$$Pr\left[Vrfy_{pk}(m;\sigma)=1\middle|\begin{array}{l}pVrfy_{pk}(m,Y;\tilde{\sigma})=1,\\ \sigma:=Adapt(\tilde{\sigma},y)\end{array}\right]=1.$$

给出适配器签名方案的安全性定义.首先,延续选择消息攻击下的存在不可伪造性(existential unforgeability under chosen message attacks, EUF-CMA)的定义,考虑敌手能够访问签名预言机获取任意消息 $m_i$ 的合法签名值.其次,允许敌手能够访问预签名预言机获取任意消息 $m_i$ 和困难问题实例 $Y$ 的合法预签名值.最后,对于敌手选取的挑战消息 $m^*$,允许敌手可以获取消息 $m^*$ 的关于实例 $Y$ 的预签名值.那么,适配器方案的不可伪造性的要求就是即使敌手具备攻击能力,它在不知道困难问题证据的情况下成功伪造一个合法签名的概率是可忽略的.

**定义 3.** aEUF-CMA 安全性.一个适配器签名方案是 aEUF-CMA 安全的,当任意的多项式时间敌手 $\mathcal{A}$ 赢得 $aSigForge^{\mathcal{A}}_{\Xi_{\Sigma,\Pi}}$ 游戏的概率是可忽略的,即

$$Pr\left[aSigForge^{\mathcal{A}}_{\Xi_{\Sigma,\Pi}}(\lambda)=1\right]<\varepsilon(\lambda).$$

定义 3 中,$aSigForge^{\mathcal{A}}_{\Xi_{\Sigma,\Pi}}$ 游戏的定义为:

1) 模拟器 $\mathcal{S}$ 建立一个空的消息询问列表 $\mathcal{Q}_m$;

2) 模拟器 $\mathcal{S}$ 获取一个公钥 $pk$,产生困难问题实例 $(I_Y=(Y,\pi_Y),y)\leftarrow GenR(1^{\lambda})$,并将 $(pk,I_Y)$ 公布给敌手 $\mathcal{A}$;

3) 敌手 $\mathcal{A}$ 可选取任意的消息 $m_i\in\{0,1\}^*$,访问签名预言机 $\mathcal{O}_S(m_i)$ 或预签名预言机 $\mathcal{Q}_{pS}(m_i,I_Y)$,并获取相应的签名值;

4) 敌手 $\mathcal{A}$ 选取一个挑战消息 $m^*\in\{0,1\}^*$,并获取到关于 $m^*$ 和 $Y$ 的预签名值,即 $\tilde{\sigma}\leftarrow pSign_{sk}(m^*,Y)$;

5) 敌手 $\mathcal{A}$ 仍然可以选取消息 $m_i\in\{0,1\}^*$ 并访问 $\mathcal{O}_S(m_i)$ 或 $\mathcal{Q}_{pS}(m_i,Y)$;

6) 敌手 $\mathcal{A}$ 输出一个签名值 $\sigma^*$.若 $m^*\notin\mathcal{Q}_m$ 且 $Vrfy_{pk}(m;\sigma^*)=1$,则敌手 $\mathcal{A}$ 赢得游戏.

签名预言机 $\mathcal{O}_S(m_i)$ 的工作方式为:产生一个签名值 $\sigma\leftarrow Sign_{sk}(m_i)$,并将被签名的消息写入列表 $\mathcal{Q}_m:=\mathcal{Q}_m\cup\{m_i\}$,返回签名值 $\sigma$.

预签名预言机 $\mathcal{Q}_{pS}(m_i,Y)$ 的工作方式为:产生一个预签名值 $\tilde{\sigma}\leftarrow pSign_{sk}(m,Y)$,并将被签名的消息写入列表 $\mathcal{Q}_m:=\mathcal{Q}_m\cup\{m_i\}$,返回签名值 $\tilde{\sigma}$.

**定义 4.** 证据可提取性(witness extractability).一个适配器签名方案是证据可提取的,当任意的多项式时间敌手 $\mathcal{A}$ 赢得 $aWitExt^{\mathcal{A}}_{\Xi_{\Sigma,\Pi}}$ 游戏的概率是可忽略的,即

$$Pr\left[aWitExt^{\mathcal{A}}_{\Xi_{\Sigma,\Pi}}(\lambda)=1\right]<\varepsilon(\lambda).$$

定义 4 中,$aWitExt^{\mathcal{A}}_{\Xi_{\Sigma,\Pi}}$ 游戏的定义为:

1) 模拟器 $\mathcal{S}$ 建立一个空的消息询问列表 $\mathcal{Q}_m$;

2) 模拟器 $\mathcal{S}$ 获取一个公钥 $pk$ 和一个困难关系实例 $I_Y=(Y,\pi_Y)$,并将 $(pk,I_Y)$ 公布给敌手 $\mathcal{A}$;

3) 敌手 $\mathcal{A}$ 可选取任意的消息 $m_i \in \{0,1\}^*$，访问签名预言机 $\mathcal{O}_S(m_i)$ 或预签名预言机 $\mathcal{Q}_{pS}(m_i, I_Y)$，并获取相应的签名值；

4) 敌手 $\mathcal{A}$ 选取一个挑战消息 $m^* \in \{0,1\}^*$，并获取到关于 $m^*$ 和 $Y$ 的预签名值，即 $\tilde{\sigma} \leftarrow pSign_{sk}(m^*, Y)$；

5) 敌手 $\mathcal{A}$ 仍然可以选取消息 $m_i \in \{0,1\}^*$ 并访问 $\mathcal{O}_S(m_i)$ 或 $\mathcal{Q}_{pS}(m_i, Y)$；

6) 敌手 $\mathcal{A}$ 输出一个签名值 $\sigma^*$；

模拟器 $\mathcal{S}$ 通过 $Ext$ 算法提取 $y' := Ext(\sigma^*, \tilde{\sigma}, Y)$. 若 $m^* \notin \mathcal{Q}_m$ 且 $(Y, y') \notin \Pi$ 且 $Vrfy_{pk}(m; \sigma^*) = 1$，则敌手 $\mathcal{A}$ 赢得游戏.

显然，$aWitExt$ 游戏和 $aSigForge$ 游戏较为相似，但前者与后者的区别在于尽管敌手 $\mathcal{A}$ 可能成功伪造签名 $\sigma^*$，但 $Ext(\sigma^*, \tilde{\sigma}, Y)$ 提取的证据也可能不是 $Y$ 的证据.

**定义 5.** 安全适配器签名方案. 一个适配器签名方案是安全的，当它满足 aEUF-CMA 安全性、预签名可适配性和证据可提取性.

## 4 基于 SM2 的适配器签名

在本节中，我们首先回顾下 SM2 数字签名方案，再给出适用于 SM2 算法的适配器签名方案.

一般而言，标准的 SM2 数字签名方案[16-17]采用素数阶的椭圆曲线点群为基本的循环群结构. 不妨令 $\mathbb{G}$ 是一个阶为 $q$ 的椭圆曲线点群，$G$ 是 $\mathbb{G}$ 的生成元，函数 $f(\cdot): \mathbb{G} \to \mathbb{Z}_q$ 表示取 $\mathbb{G}$ 中椭圆曲线点的 $x$ 坐标，$H(\cdot)$ 是一个密码杂凑函数. 那么，SM2 签名算法 $\Sigma_{SM2} = (Gen, Sign, Vrfy)$ 的描述为：

1) 密钥生成算法 $(sk, pk) \leftarrow Gen(1^\lambda)$. 随机选取一个整数 $d \leftarrow_\$ Z_q^*$ 并计算 $P = d \cdot G \in \mathbb{G}$，输出私钥 $sk = d$ 和公钥 $pk = P$.

2) 签名生成算法 $\sigma \leftarrow Sign_{sk}(m)$. 对于消息 $m \in \{0,1\}^*$，随机选取一个整数 $k \leftarrow_\$ Z_q^*$，计算 $K = k \cdot G$，$r = H(m) + f(K) \bmod q$ 和 $s = (1+d)^{-1}(k - r \cdot d) \bmod q$，输出签名值 $\sigma = (r, s) \in \mathbb{Z}_q \times \mathbb{Z}_q$.

3) 签名验证算法 $b = Vrfy_{pk}(m; \sigma)$：对于消息 $m \in \{0,1\}^*$ 和签名值 $\sigma = (r, s) \in \mathbb{Z}_q \times \mathbb{Z}_q$，验证式子 $r = H(m) + f(s \cdot G + (r+s) \cdot P)$ 是否成立；若成立，则 $b = 1$；否则，$b = 0$.

显然，因为 $s \cdot G + (r+s) \cdot P = (s + (1+d)^{-1} \cdot (k \cdot d + r \cdot d)) \cdot G = k \cdot G$，SM2 数字签名方案的正确性是可以满足的.

假设 $\Pi_G \subseteq \mathbb{G} \times \mathbb{Z}_q$ 是群 $\mathbb{G}$ 上的困难关系，即 $\Pi_G := \{(Y, y) \mid Y = y \cdot G\}$，$I_Y$ 表示困难关系 $\Pi_G$ 中对于状态 $Y$ 的实例. 为将困难关系 $\Pi_G$ 嵌入到 SM2 签名方案中，我们设计了适配器签名方案：

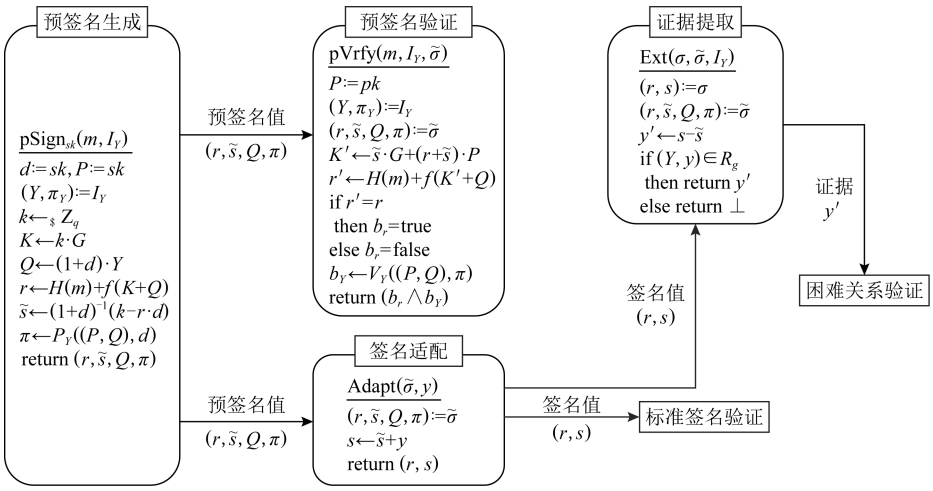


Fig. 1 SM2-based adaptor signature scheme

图 1 基于 SM2 的适配器签名方案

**算法 1.** 预签名生成算法 $\tilde{\sigma} \leftarrow pSign_{sk}(m, Y)$.

输入：私钥 $d$、消息 $m \in \{0,1\}^*$ 和困难关系状态 $Y$；

输出：预签名值 $\tilde{\sigma}$.

① 随机选取一个整数 $k \leftarrow_\$ Z_q^*$，计算 $K = k \cdot G$；

② 计算 $Q = (1+d) \cdot Y$，$r = H(m) + f(K+Q) \bmod q$ 和 $\tilde{s} = (1+d)^{-1}(k - r \cdot d) \bmod q$；

③ 产生零知识证明 $\pi = P_Y((P, Q), d)$；

④ 令预签名值 $\tilde{\sigma} = (r, \tilde{s}, Q, \pi)$.

**算法 2.** 预签名验证算法 $b = pVrfy_{pk}(m, Y; \tilde{\sigma})$.

输入:公钥 $P$、消息 $m\in\{0,1\}^*$、困难关系状态 $Y$、预签名值 $\tilde{\sigma}$;

输出:验证结果 $b$.

① 计算 $K'=\bar{s}\cdot G+(r+\bar{s})\cdot P$ 和 $r'=H(m)+f(K'+Q)$;

② 验证式子 $r'=r$ 是否成立;若成立,则 $b_r=1$;否则,$b_r=0$;

③ 验证 $b_Y=V_Y((P,Q),\pi)$;

④ 输出验证结果为 $b=b_r\wedge b_Y$.

**算法 3.** 适配算法 $\sigma:=Adapt(\tilde{\sigma},y)$.

输入:预签名值 $\tilde{\sigma}$ 和困难关系证据 $y$;

输出:签名值 $\sigma$.

① 计算 $s=\bar{s}+y$;

② 令签名值 $\sigma=(r,s)$.

**算法 4.** 提取算法 $y':=Ext(\sigma,\tilde{\sigma},Y)$.

输入:签名值 $\sigma$、预签名值 $\tilde{\sigma}$ 和困难关系状态 $Y$;

输出:证据 $y'$或失败符号 $\perp$.

① 计算 $y'=s-\bar{s}$;

② 验证 $(Y,y)\in\Pi_G$ 是否成立;

③ 若成立,则返回 $y'$;否则,返回 $\perp$.

## 5　安全性证明

本节我们将给出基于 SM2 算法的适配器签名方案的安全性证明.

**定理 1.** 基于 SM2 的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 $P\in\mathbb{G}$、困难关系实例 $(I_Y,y)\in\Pi_G$、消息 $m\in\{0,1\}^*$ 和预签名值 $\tilde{\sigma}=(r,\bar{s},Q,\pi)$,如果 $pVrfy_{pk}(m,Y;\tilde{\sigma})=1$ 成立,则有

$$r=H(m)+f(\bar{s}\cdot G+(r+\bar{s})\cdot P+Q)).$$

根据适配算法的定义,$\sigma:=Adapt(\tilde{\sigma},y)$ 中的 $s=\bar{s}+y$.那么,

$$s\cdot G-Y+(r+s-y)P+(1+d)\cdot Y=$$
$$s\cdot G+(r+s)P.$$

显然,适配得到的签名值 $\sigma$ 是一个关于公钥和消息的有效签名. 证毕.

**定理 2.** 基于 SM2 的适配器签名方案满足预签名正确性.

证明. 给定私钥 $d$、困难问题证据 $y$ 和消息 $m\in\{0,1\}^*$,则有 $P=d\cdot G$ 和 $Y=y\cdot G$.对于 $pSign_{sk}(m,Y)$ 产生的预签名值 $\tilde{\sigma}=(r,\bar{s},Q,\pi)$,有 $K'=\bar{s}\cdot G+(r+\bar{s})\cdot P=k\cdot G=K$,则 $r'=r$ 必然成立.又根据非交互式零知识证明的完备性,$V_Y((P,Q),\pi)=1$ 也成立.因此,$pVrfy_{pk}(m,Y;\tilde{\sigma})=1$.

根据定理 1,可知 $Vrfy_{pk}(m;\sigma)=1$.再根据适配算法的定义可知,$\bar{s}$ 和 $s$ 间只差一个 $y$.那么,通过提取算法还原的 $y'$必然是 $Y$ 的证据,即$(Y,y')\in\Pi_G$. 证毕.

**定理 3.** 如果 SM2 签名方案 $\Sigma_{SM2}$ 是 EUF-CMA 安全的,且 $\Pi_G$ 是一个困难关系,则基于 SM2 的适配器签名方案满足 aEUF-CMA 安全性.

证明. 假设敌手 $\mathcal{A}$ 与模拟器 $\mathcal{S}$ 进行 aSignForge 游戏,其中 $\mathcal{A}$ 会向 $\mathcal{S}$ 进行哈希询问($\mathcal{H}$)、签名询问($\mathcal{O}_S$)和预签名询问($\mathcal{O}_{pS}$),而 $\mathcal{S}$ 能够访问 SM2 签名方案的签名预言机 $\mathcal{O}_S(\cdot)$来响应询问,并控制随机预言机 $\mathcal{H}$ 和预签名预言机 $\mathcal{O}_{pS}$ 来响应询问.按照 aSignForge 游戏的定义,敌手 $\mathcal{A}$ 与模拟器 $\mathcal{S}$ 进行交互:

1) 模拟器 $\mathcal{S}$ 初始化一个空的消息询问列表 $\mathcal{Q}_m$ 和一个空的哈希询问列表 $\mathcal{Q}_H$;

2) 模拟器 $\mathcal{S}$ 询问 SM2 签名方案的签名预言机 $\mathcal{O}_S(\cdot)$获取公钥 $pk$,产生困难关系$(I_Y=(Y,\pi_Y),y)\leftarrow GenR(1^\lambda)$,并发送$(pk,I_Y)$给敌手 $\mathcal{A}$;

3) 敌手 $\mathcal{A}$ 自适应的选取消息 $m_i\in\{0,1\}^*$,进行哈希询问、签名询问和预签名询问,模拟器 $\mathcal{S}$ 的响应方式为:

哈希询问 $\mathcal{H}(x)$.当询问 $x$ 的哈希值时,$\mathcal{S}$ 先查询列表 $\mathcal{Q}_H$ 中是否存在 $H(x)$;若存在,则直接取出;否则,随机产生 $H(x)\leftarrow_{\$}\mathbb{Z}_q^*$,并将$(x,H(x))$存入列表中;最后,返回 $H(x)$给 $\mathcal{A}$;

签名询问 $\mathcal{O}_S(m_i)$:当询问 $m_i$ 的签名值时,$\mathcal{S}$ 直接向 $\mathcal{O}_S$ 发起关于 $m_i$ 的签名询问,并将获取的签名值 $\sigma$ 返回给 $\mathcal{A}$;

预签名询问 $\mathcal{Q}_{pS}(m_i,I_Y)$:当询问 $m_i$ 和 $I_Y$ 的预签名值时,$\mathcal{S}$ 按照步骤进行响应:

① 对 $\mathcal{O}_S$ 发起关于 $m_i$ 的签名询问,获取签名值 $\sigma=Sign_{sk}(m_i)$;

② 计算 $\bar{s}=s-y$ 和 $Q=Y+y\cdot P$;

③ 模拟零知识证明 $\pi_S=S((P,Q),1)$;

④ 更新列表 $\mathcal{Q}_m:=\mathcal{Q}_m\cup\{m_i\}$;

⑤ 输出预签名值 $\tilde{\sigma}=(r,\bar{s},Q,\pi_S)$.

之后,$\mathcal{S}$ 将 $\tilde{\sigma}$ 返回给 $\mathcal{A}$.

4) 敌手 $\mathcal{A}$ 选取一个挑战消息 $m^*\in\{0,1\}^*$,并询问关于 $m^*$ 和 $Y$ 的预签名值,$\mathcal{S}$ 按照预签名询问 $\mathcal{Q}_{pS}(m^*,I_Y)$进行响应;

5) 敌手 $\mathcal{A}$ 仍可自适应的选取消息 $m_i \in \{0,1\}^*$,进行 3)中的询问;

6) 敌手 $\mathcal{A}$ 输出一个签名值 $\sigma^*$.模拟器 $\mathcal{S}$ 收到 $\sigma^*$ 后,检查 $\sigma^* = Adapt(\tilde{\sigma}, y)$ 是否成立;若成立,则报错退出.

如果签名值 $\sigma^*$ 是有效的且 $m^*$ 未出现在列表 $\mathcal{Q}_m$ 中,那意味着 $\mathcal{S}$ 可以将 $(m^*, \sigma^*)$ 作为一个合法的消息-签名对攻击 SM2 签名方案的不可伪造性.

优势分析:由于模拟器只可能在步骤 6)中退出,且该情况发生时隐含敌手可通过 Ext 算法从 $\sigma^*$ 和 $\tilde{\sigma}$ 中获取证据 $y$,其概率是可忽略的.那么,敌手 $\mathcal{A}$ 的优势是 $Adv^{\mathcal{A}}_{\text{aSignForge}} = Adv^{\mathcal{A}}_{\text{SM2-EUF-CMA}} + \varepsilon(\lambda)$,也是可忽略的. 证毕.

**定理 4.** 如果 SM2 签名方案 $\Sigma_{\text{SM2}}$ 是 EUF-CMA 安全的,且 $\Pi_G$ 是一个困难关系,则基于 SM2 的适配器签名方案满足证据可提取性.

证明. 假设敌手 $\mathcal{A}$ 与模拟器 $\mathcal{S}$ 进行 aWitExt 游戏,其中 $\mathcal{A}$ 会向 $\mathcal{S}$ 进行哈希询问($\mathcal{H}$)、签名询问($\mathcal{O}_S$)和预签名询问($\mathcal{O}_{pS}$),而 $\mathcal{S}$ 能够访问 SM2 签名方案的签名预言机 $\mathcal{O}_S(\cdot)$来响应询问,并控制随机预言机 $\mathcal{H}$ 和预签名预言机 $\mathcal{O}_{pS}$ 来响应询问.按照 aSignForge 游戏的定义,敌手 $\mathcal{A}$ 与模拟器 $\mathcal{S}$ 进行交互:

1) 模拟器 $\mathcal{S}$ 初始化一个空的消息询问列表 $\mathcal{Q}_m$ 和一个空的哈希询问列表 $\mathcal{Q}_H$;

2) 模拟器 $\mathcal{S}$ 询问 SM2 签名方案的签名预言机 $\mathcal{O}_S(\cdot)$获取公钥 $pk$ 并发送给敌手 $\mathcal{A}$;同时,敌手 $\mathcal{A}$ 获取到困难问题实例 $I_Y = (Y, \pi_Y)$;

3) 敌手 $\mathcal{A}$ 自适应的选取消息 $m_i \in \{0,1\}^*$,进行哈希询问、签名询问和预签名询问,模拟器 $\mathcal{S}$ 的响应方式为:

哈希询问 $\mathcal{H}(x)$.当询问 $x$ 的哈希值时,$\mathcal{S}$ 先查询列表 $\mathcal{Q}_H$ 中是否存在 $H(x)$;若存在,则直接取出;否则,随机产生 $H(x) \leftarrow_{\$} \mathbb{Z}_q^*$,并将 $(x, H(x))$ 存入列表中;最后,返回 $H(x)$给 $\mathcal{A}$;

签名询问 $\mathcal{O}_S(m_i)$:当询问 $m_i$ 的签名值时,$\mathcal{S}$ 直接向 $\mathcal{O}_S$ 发起关于 $m_i$ 的签名询问,并将获取的签名值 $\sigma$ 返回给 $\mathcal{A}$;

预签名询问 $\mathcal{Q}_{pS}(m_i, I_Y)$:当询问 $m_i$ 和 $I_Y$ 的预签名值时,$\mathcal{S}$ 按照步骤进行响应:

① 通过 NIZK 方案的在线提取器获取证据 $y$,即 $y := \mathcal{K}(Y, \pi_Y, \mathcal{H})$;如果 $(Y, y) \notin \Pi_G$,则报错退出;

② 对 $\mathcal{O}_S$ 发起关于 $m_i$ 的签名询问,获取签名值 $\sigma = Sign_{sk}(m_i)$;

③ 计算 $\tilde{s} = s - y$ 和 $Q = Y + y \cdot P$;

④ 模拟零知识证明 $\pi_S = S((P, Q), 1)$;

⑤ 更新列表 $\mathcal{Q}_m := \mathcal{Q}_m \cup \{m_i\}$;

⑥ 输出预签名值 $\tilde{\sigma} = (r, \tilde{s}, Q, \pi_S)$.

之后,$\mathcal{S}$ 将 $\tilde{\sigma}$ 返回给 $A$.

4) 敌手 $\mathcal{A}$ 选取一个挑战消息 $m^* \in \{0,1\}^*$,并询问关于 $m^*$ 和 $Y$ 的预签名值,$\mathcal{S}$ 按照预签名询问 $\mathcal{Q}_{pS}(m^*, I_Y)$进行响应;

5) 敌手 $\mathcal{A}$ 仍可自适应的选取消息 $m_i \in \{0,1\}^*$,进行 3)中的询问;

6) 敌手 $\mathcal{A}$ 输出一个签名值 $\sigma^*$.

如果签名值 $\sigma^*$ 是有效的且 $m^*$ 未出现在列表 $\mathcal{Q}_m$ 中,那意味着 $\mathcal{S}$ 可以将 $(m^*, \sigma^*)$ 作为一个合法的消息-签名对攻击 SM2 签名方案的不可伪造性.

优势分析:由于模拟器只可能在 3)中①)退出,且该情况发生的概率是可忽略的.那么,敌手 $\mathcal{A}$ 的优势是 $Adv^{\mathcal{A}}_{\text{aWitExt}} = Adv^{\mathcal{A}}_{\text{SM2-EUF-CMA}} + \varepsilon(\lambda)$,也是可忽略的. 证毕.

**定理 5.** 如果 SM2 签名方案 $\Sigma_{\text{SM2}}$ 是 EUF-CMA 安全的,且 $\Pi_G$ 是一个困难关系,则基于 SM2 的适配器签名方案是安全的.

证明. 显然,根据定义 5 和定理 1~4 可知,基于 SM2 的适配器签名方案是安全的. 证毕.

## 6 效率分析

本节我们以计算开销和通信开销来评估基于 SM2 的适配器签名方案的效率,并将评估结果与文献[8]中的基于 Schnorr 的适配器签名方案和基于 ECDSA 签名方案进行比较.

### 6.1 计算开销分析

在计算开销方面,我们主要考虑预签名生成算法、预签名验证算法、适配算法和提取算法的计算开销.对于密钥生成算法而言,SM2,Schnorr 和 ECDSA 的密钥生成机制是一样的,故不作比较.表 1 给出了 3 种方案计算开销,其中 $T_{\text{P}}$ 和 $T_{\text{V}}$ 分别使用 NIZK 证明生成算法和验证算法的计算耗时,$T_{\text{pm}}$ 和 $T_{\text{pa}}$ 分别表示群 $\mathbb{G}$ 中点乘和点加运算的计算耗时,$T_{\text{inv}}$,$T_{\text{mul}}$ 和 $T_{\text{add}}$ 分别表示 $\mathbb{Z}_q^*$ 中模逆、模乘和模加运算的计算耗时,$T_{\text{h}}$ 表示一次杂凑运算的计算耗时.由于,$T_{\text{add}}$ 在 pSign 和 pVrfy 算法中的占比极低,故可忽略.另外,SM2 算法中的 $(1+d)^{-1}$ 可预计算,故该运算亦可忽略.

**Table 1　Comparisons of Computation Costs for Different Adaptor Signature Schemes**

**表 1　不同适配器签名方案的计算开销比较**

| 方案 | 预签名生成 | 预签名验证 | 适配算法 | 提取算法 |
|---|---|---|---|---|
| SM2 适配器签名 | $T_{\mathrm{P}}+2T_{\mathrm{pm}}+T_{\mathrm{pa}}+T_{\mathrm{h}}+2T_{\mathrm{mul}}$ | $T_{\mathrm{V}}+2T_{\mathrm{pm}}+T_{\mathrm{pa}}+T_{\mathrm{h}}+2T_{\mathrm{mul}}$ | $T_{\mathrm{add}}$ | $T_{\mathrm{add}}$ |
| Schnorr 适配器签名 | $T_{\mathrm{pm}}+T_{\mathrm{pa}}+T_{\mathrm{h}}+T_{\mathrm{mul}}$ | $2T_{\mathrm{pm}}+2T_{\mathrm{pa}}+T_{\mathrm{h}}$ | $T_{\mathrm{add}}$ | $T_{\mathrm{add}}$ |
| ECDSA 适配器签名 | $T_{\mathrm{P}}+2T_{\mathrm{pm}}+T_{\mathrm{h}}+T_{\mathrm{inv}}+T_{\mathrm{mul}}$ | $T_{\mathrm{V}}+2T_{\mathrm{pm}}+T_{\mathrm{pa}}+T_{\mathrm{h}}+T_{\mathrm{inv}}+2T_{\mathrm{mul}}$ | $T_{\mathrm{inv}}+T_{\mathrm{mul}}$ | $T_{\mathrm{inv}}+T_{\mathrm{mul}}$ |

对于预签名生成算法而言,SM2 适配器签名方案比 Schnorr 适配器签名方案多 1 个 NIZK 证明、1 个点乘和 1 个模乘,比 ECDSA 适配器签名方案多 1 个模乘、少 1 个模逆.从图 2 中可知,SM2 适配器签名方案的预签名生成耗时与 ECDSA 适配器签名方案相当,但是 Schnorr 适配器签名方案的 3.2 倍.

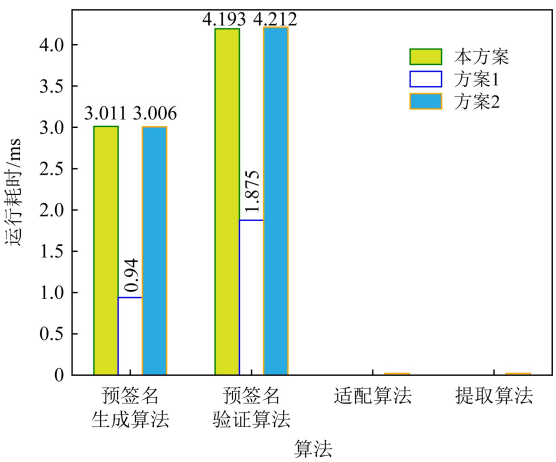


Fig. 2　Execution time of different adaptor signature schemes

图 2　不同适配器签名方案的运行耗时

对于预签名验证算法而言,SM2 适配器签名方案比 Schnorr 适配器签名方案多 1 个 NIZK 验证和 2 个模乘,少 1 个点乘,比 ECDSA 适配器签名方案少 1 个模逆.从图 2 中可知,SM2 适配器签名方案的预签名验证耗时与 ECDSA 适配器签名方案相当,但是 Schnorr 适配器签名方案的 2.3 倍.

对于适配算法和提取算法而言,SM2 适配器签名方案和 Schnorr 适配器签名方案均采用了加法形式构造,其所调用的模加/减运算几乎可以忽略不计.而 ECDSA 适配器签名方案采用乘法方式构造,需要调用 1 次模逆和 1 次模乘,其运算量远大于另外 2 个方案.

### 6.2　通信开销分析

在通信开销方面,我们主要考虑预签名值的尺寸.对于参与比较的 3 个适配器签名方案,其私钥、公钥和签名值尺寸是一样的.

如表 2 所示,SM2 适配器签名方案和 ECDSA 适配器签名方案的预签名值尺寸为 $4|\mathbb{Z}_q|+|\mathbb{G}|$ (192 B),其中 NIZK 证明需要 2 个$\mathbb{Z}_q$上的元素表示.Schnorr 适配器签名方案的预签名值尺寸为$2|\mathbb{Z}_q|$ (64 B).

**Table 2　Comparisons of Communication Costs for Different Adaptor Signature Schemes**

**表 2　不同适配器方案的通信开销比较**

| 方案 | 预签名值尺寸/B |
|---|---|
| SM2 适配器签名 | $4\|\mathbb{Z}_q\|+\|\mathbb{G}\|=192$ |
| Schnorr 适配器签名 | $2\|\mathbb{Z}_q\|=64$ |
| ECDSA 适配器签名 | $4\|\mathbb{Z}_q\|+\|\mathbb{G}\|=192$ |

SM2 适配器签名方案在计算和通信开销方面与 ECDSA 适配器签名方案相当,但在适配算法和提取算法的计算开销方面更优;SM2 适配器签名方案的运算性能约为 Schnorr 适配器签名方案的一半,且预签名值尺寸为 Schnorr 适配器签名方案的 3 倍.

## 7　结　　论

作为标准数字签名方案的一种扩展,适配器签名可以在签名逻辑中内联困难问题,并限制完整签名的获取条件.该功能已经成为了区块链系统中链下支付通道构建的关键模块.然而,现在的适配器签名方案均以国外算法为原型,缺少基于国家商用密码标准的适配器签名方案.为此,本文以 SM2 数字签名方案为基础,构造了一个新的适配器签名方案,并在随机预言模型下证明其满足适配器签名方案的安全要求.通过性能分析,可知所提出的适配器签名方案的性能与基于 ECDSA 的适配器签名方案相当,且在适配算法和提取算法的计算开销方面具有极大的优势.下一步,我们将以本文的方案为出发,试图构造基于 SM2 的指定提取者适配器签名方案、盲适配器签名方案和环适配器签名方案等.

## 参 考 文 献


[1] Yu Hui, Zhang Zongyang, Liu Jianwei. Research on scaling technology of bitcoin blockchain [J]. Journal of Computer Research and Development, 2017, 54(10): 2390-2403 (in Chinese)
(喻辉, 张宗洋, 刘建伟. 比特币区块链扩容技术研究[J]. 计算机研究与发展, 2017, 54(10): 2390-2403)

[2] Stress test prepares visanet for the most wonderful time of the year [OL]. [2021-05-28]. http://tinyurl.com/ya35s3uo

[3] Bitcoin Wiki. Payment Channels [OL]. [2021-05-28]. http://en.bitcoin.it/wiki/Payment channels

[4] Lightning Network. Lightning Network [OL]. [2021-05-28]. http://lightning.network/

[5] The Raiden Network. The Raiden Network [OL]. [2021-05-28]. http://raiden.network/

[6] Zhu Liehuang, Gao Feng, Shen Meng, et al. Survey on privacy preserving techniques for blockchain technology [J]. Journal of Computer Research and Development, 2017, 54(10): 2170-2186 (in Chinese)
(祝烈煌, 高峰, 沈蒙, 等. 区块链隐私保护研究综述 [J]. 计算机研究与发展, 2017, 54(10): 2170-2186)

[7] Poelstra A. Scriptless scripts [OL]. [2021-05-28]. http://download.wpsoftware.net

[8] Aumayr L, Ersoy O, Erwig A, et al. Generalized bitcoin-compatible channels [J]. IACR Cryptology ePrint Archive, 2020, 2020: 476

[9] Fournier L. One-time verifiably encrypted signatures aka adaptor signatures [OL]. [2021-05-28]. http://github.com/LLFourn/one-time-VES

[10] Malavolta G, Moreno-Sanchez P, Schneidewind C, et al. Anonymous multi-hop locks for blockchain scalability and interoperability [C/OL] //Proc of the 26th Annual Network and Distributed System Security Symp, NDSS 2019. The Internet Society, 2019: 10168773 [2021-05-28]. https://par.nsf.gov/servlets/purl/10168773

[11] Tairi E, Moreno-Sanchez P, Maffei M. A2L: Anonymous atomic locks for scalability in payment channel hubs [J]. IACR Cryptology ePrint Archive, 2019, 2019: No.598

[12] Moreno-Sanchez P, Blue A, Le D V, et al. DLSAG: Non-interactive refund transactions for interoperable payment channels in monero [C] //Proc of the 24th Int Conf on Financial Cryptography and Data Security. Berlin: Springer, 2020: 325-345

[13] Esgin M F, Ersoy O, Erkin Z. Post-quantum adaptor signatures and payment channel networks [C] //Proc of the 25th European Symp on Research in Computer Security. Berlin: Springer, 2020: 378-397

[14] Tairi E, Moreno-Sanchez P, Maffei M. Post-quantum adaptor signature for privacy-preserving off-chain payments [J]. IACR Cryptology ePrint Archive, 2020, 2020: 1345

[15] Qin X, Cui H, Yuen T H. Generic adaptor signature [J]. IACR Cryptology ePrint Archive, 2021, 2021: 161

[16] General Administration of Quality Supervision, Inspection and Quarantine of the People's Pepublic of China, Standardization Administration of the People's Republic of China. GB/T 32918—2016 Information security technology-public key cryptographic algorithm SM2 based on elliptic curves [S]. Beijing: Standards Press of China, 2016 (in Chinese)
(国家质量监督检验检疫总局, 中国国家标准化管理委员会. GB/T 32918—2016 信息安全技术 SM2 椭圆曲线 公钥密码算法[S]. 北京: 中国标准出版社, 2016)

[17] Feng Qi, He Debiao, Luo Min, et al. Efficient two-party SM2 signing protocol for mobile Internet [J]. Journal of Computer Research and Development, 2020, 57(10): 2136-2146 (in Chinese)
(冯琦, 何德彪, 罗敏, 等. 移动互联网环境下轻量级 SM2 两方协同签名[J]. 计算机研究与发展, 2020, 57(10): 2136-2146)



**Peng Cong**, born in 1989, PhD, associate professor. His main research interests include cryptography and information security, cryptography.
**彭 聪**, 1989 年生. 博士, 副研究员. 主要研究方向为信息安全和密码学.



**Luo Min**, born in 1974. PhD, associate professor. His main research interests include cryptography and information security, cryptography.
**罗 敏**, 1974 年生. 博士, 副教授. 主要研究方向为信息安全和密码学.



**He Debiao**, born in 1980. PhD, professor, PhD supervisor. Senior member of CCF. His main research interests include cryptography and information security, cryptography. (hedebiao@whu.edu.cn)
**何德彪**, 1980 年生. 博士, 教授, 博士生导师, CCF 高级会员. 主要研究方向为信息安全和密码学.



**Huang Xinyi**, born in 1981. PhD, professor, PhD supervisor. His main research interests include cryptography and information security. (xyhuang@fjnu.edu.cn)
**黄欣沂**, 1981 年生. 博士, 教授, 博士生导师. 主要研究方向为密码学和信息安全.