基于 ISRSAC 数字签名算法的适配器签名方案

张艳硕[1,2]，刘宁[1]，袁煜淇[1]，杨亚涛[3]

（1. 北京电子科技学院密码科学与技术系，北京 100070；
2. 杭州师范大学浙江省密码技术重点实验室，浙江 杭州 311121；
3. 北京电子科技学院电子与通信工程系，北京 100070）

摘 要：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，并已在实践中得到广泛应用。以改进的安全 RSA 密码系统（ISRSAC）数字签名算法为基础构造了一个新的适配器签名方案。在证明所提方案满足预签名的正确性、不可伪造性、预签名的可适配性、证据的可提取性和签名方案的安全性后，将其与基于 SM2 数字签名算法的适配器签名方案、基于 Schnorr 的适配器签名方案和基于 ECDSA 的适配器签名方案在时间开销、主要计算量等方面进行对比分析。分析结果表明，所提方案在时间开销上与其他方案相差不多，但所提方案扩展了 ISRSAC 算法在当前环境中的应用场景，且 ISRSAC 算法和适配器签名技术的结合使适配器签名的选择更具灵活性，应用范围更广。

关键词：适配器签名；ISRSAC；数字签名；安全；不可伪造性

中图分类号：TN918.1

文献标志码：A

DOI: 10.11959/j.issn.1000−436x.2023056

Adaptor signature scheme based on ISRSAC digital signature algorithm

ZHANG Yanshuo[1,2], LIU Ning[1], YUAN Yuqi[1], YANG Yatao[3]

1. Department of Cryptology Science and Technology, Beijing Electronic Science & Technology Institute, Beijing 100070, China
2. Key Laboratory of Cryptography of Zhejiang Province, Hangzhou Normal University, Hangzhou 311121, China
3. Department of Electronic and Communication Engineering, Beijing Electronic Science & Technology Institute, Beijing 100070, China

Abstract: The adapter signature scheme can provide good properties of atomic exchange in the block chain, and has been widely used in practice. A new adapter signature scheme was constructed based on a digital signature algorithm for improved security of RSA cryptosystem (ISRSAC). After proving that the proposed scheme satisfied the correctness of the pre-signature, unforgeability, adaptability of the pre-signature, extractability of the evidence and the security of the signature scheme, it was compared with the adapter signature scheme based on the SM2 digital signature algorithm, the Schnorr-based adapter signature scheme and the ECDSA-based adapter signature scheme. And these schemes were analyzed in terms of time overhead and main calculation amount. The analysis results show that the proposed scheme is similar to other schemes in terms of time overhead, but the proposed scheme expands the application scenarios of ISRSAC algorithm in the current environment, and through the combination of ISRSAC algorithm and adapter signature technology, the selection of adapter signature is more flexible and can have a wider range of applications.

Keywords: adapter signature, ISRSAC, digital signature, safety, unforgeability

收稿日期：2022−10−24；**修回日期：**2023−01−04

基金项目：中央高校基本科研业务费专项资金资助项目（No.328202226）；浙江省密码技术重点实验室基金资助项目（No.ZCI21009）；国家自然科学基金资助项目（No.62002003）

Foundation Items: The Fundamental Research Funds for the Central Universities (No.328202226), Zhejiang Provincial Key Laboratory of Cryptography (No.ZCI21009), The National Natural Science Foundation of China (No.62002003)

0　引言

1976 年，Diffie 等[1]首次提出了数字签名技术的概念。数字签名技术发展至今，已经从最初的一个数学概念，发展到基于计算复杂性问题的具体实现、扎实的安全模型定义、安全性可证明的高效构造、满足各类差异化需求的特性签名技术[2]。近几年，随着区块链技术的不断发展，在标准数字签名基础上扩展而来的适配器签名开始受到密码学者的广泛关注。

适配器签名是在无脚本脚本概念的基础上形式化定义的。该签名通过使用 Schnorr 签名[3]在链下执行智能合约的方法，在很多区块链应用程序中都是重要的组成部分[4]，例如，支付通道[5-8]、支付通道网络中的支付路由[9-10]和原子交换[11-12]。该签名的主要优势在功能、隐私和效率方面。在功能方面，增加了比特币智能合约的范围和复杂性；在隐私性方面，使用 Schnorr 签名将易暴露的智能合约移出链，避免当智能合约本身在链上被泄露时，包括隐私在内的许多细节被泄露；在效率方面，通过将智能合约移至链下，最大限度地减少了需要在网络验证和存储的数据量。这些优势使参与者的开销更少，用户的交易费用更低，从而实现了双赢。

近几年，先后有学者构造了相关的适配器签名方案。Malavolta 等[13]基于单向同态函数构建了适配器签名方案，并给出了将适配器签名方案用于构建支付通道网络的方法；Tairi 等[14]给出了将适配器签名方案用于构建支付通道集线器的方法。Aumayr 等[15]在形式化定义了适配器签名后，提出了 Schnorr、椭圆曲线数字签名算法（ECDSA）构造，并在此基础上构建了通用支付通道。此外，为了对抗量子技术不断发展所带来的计算威胁，Esgin 等[16]设计了第一个基于标准格的适配器签名（LAS）方案；Tairi 等[17]设计了第一个基于同源的适配器签名（IAS）方案。Erwig 等[4]构建了具有可聚合公钥的两方适配器签名方案，并且提出了构造适配器的通用方法；Qin 等[18]提出了基于身份鉴别协议的适配器签名的第一个通用构造，并构建了盲适配器签名和可链接环适配器签名；Aumayr 等[19]再次形式化定义了状态通道，并构造了基于 Schnorr 的适配器签名方案和基于 ECDSA 的适配器签名方案；Thyagarajan 等[20]为 BLS（Boneh-Lynn-Shacham）签名的特例设计了一个高效的 PCN 协议；彭聪等[21]构造了基于 SM2 数字签名算法的适配器签名方案，但尚未发现基于改进的安全 RSA 密码系统（ISRSAC）数字签名算法的适配器签名方案。

ISRSAC[22]是在 2017 年由 Varalakshmi 和 Thangavel 提出的。相比 RSA 算法，ISRSAC 算法通过加强大整数 n 的分解难度和增加随机数，提高了算法的破解难度和安全性。Varalakshmi 和 Thangavel[22]也证实了 ISRSAC 算法的安全性要高于 RSA 算法。由此可见，ISRSAC 算法是一种安全性高于传统 RSA 算法的新型算法。由于适配器签名具有以上优势，且 ISRSAC 算法是一种安全性高于传统 RSA 算法的新型算法，故本文构造了基于 ISRSAC 数字签名算法的适配器签名方案。

以 ISRSAC 数字签名算法为基础构造的适配器签名方案，不仅扩宽了 ISRSAC 算法的应用场景，而且使适配器签名有了更多可供选择的方案，更具灵活性，能更好地满足当前环境下的应用需要。

1　预备知识

本节依次介绍基于 ISRSAC 算法的数字签名和困难关系的定义。

定义 1　基于 ISRSAC 算法的数字签名。基于 ISRSAC 的数字签名由三阶段构成[23]：密钥生成算法、签名生成算法和签名验证算法。

具体算法流程介绍如下。

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

① 随机选取 2 个大素数 p 和 q，其中 $p \neq q, p>3, q>3$。

② 计算 $n=pq(p-1)(q-1)$，$m=pq$。

③ 随机选取一个整数 r，满足 $p>2^r$ 且 $q>2^r$，生成 $\alpha(n)=\dfrac{(p-1)(q-1)(p-2^r)(q-2^r)}{2^r}$。

④ 随机选取一个数 e，同时满足 $1<e<\alpha(n)$ 和 $\gcd(e,\alpha(n))=1$。

⑤ 计算 d，满足 $de \equiv 1(\mathrm{mod}\,\alpha(n))$。

通过上述计算，确定公钥 $\mathrm{pk}=(e,m)$ 和私钥 $\mathrm{sk}=(d,n)$。

2) 签名生成算法($S \leftarrow \mathrm{Sign}_{\mathrm{sk}}(M)$)

在考虑到算法的性质后，在选择哈希算法时，选用密码散列函数标准 SM3[24]。

本文假设原文为 M，哈希函数为 H，明文 M 的哈希值为 $H(M)$。为了对 $H(M)$ 进行签名，在加入

私钥 d 和 n 后进行签名，生成 $S \equiv H(M)^d \bmod m$。

3) 签名验证算法($b \leftarrow \mathrm{Vrfy}_{\mathrm{pk}}(M;\sigma)$)

为验证签名 S，在计算出 M 的哈希值 $H(M)$ 后，加入公钥 e 和 m，验证方程 $H(M) \equiv S^e \bmod m$ 是否正确。如果正确则输出 $b=1$，否则输出 $b=0$。

定义 2 困难关系。给定一个二元关系 Ψ，$L_\Psi = \{Y \mid \exists y,(Y,y) \in \Psi\}$，其中，$Y$ 为困难关系状态，y 为困难关系证据。若 Ψ 满足以下 3 个性质，则称这种二元关系 Ψ 是一种困难关系[21]。

① 在一个概率多项式时间内可以成功地生成一组例子，记为 $(Y,y) \leftarrow \mathrm{Gen}\,\Psi(1^\lambda)$，其中 λ 为系统的安全系数。

② 生成的二元关系 (Y,y) 可以在一个确定性的多项式时间内被验证是否属于 Ψ。

③ 在 Y 已知的情况下，能够在任意的多项式时间内正确求出 y 的概率是忽略不计的。

困难关系是构造适配器签名方案的一个重要关系，将会在构建相关模型和适配器签名方案中起重要作用。

2 适配器签名的一般模型

本节根据文献[19]和文献[21]中的系统模型和安全模型，建立了相应的系统模型和安全模型，这些模型将用于第 3 节和第 4 节构造基于 ISRSAC 数字签名算法的适配器签名方案及正确性等相关性质的证明。

2.1 系统模型

适配器签名的系统模型即对适配器签名的形式化定义。下面给出其形式化定义，作为构造基于 ISRSAC 数字签名算法的适配器签名方案的基础。

定义 3 适配器签名。适配器签名算法主要包括预签名生成算法 $\mathrm{pSign}_{\mathrm{sk}}(M,Y)$、预签名验证算法 $\mathrm{pVrfy}_{\mathrm{pk}}(M,Y;\tilde{\sigma})$、适配算法 $\mathrm{Adapt}(\tilde{\sigma},y)$ 和提取算法 $\mathrm{Ext}(\sigma,\tilde{\sigma},Y)$ 4 个算法。4 个算法的具体描述如下。

1) 预签名生成算法 $\mathrm{pSign}_{\mathrm{sk}}(M,Y)$，即输入困难关系状态 Y、消息 M 和私钥 sk，输出预签名值 $\tilde{\sigma}$。

2) 预签名验证算法 $\mathrm{pVrfy}_{\mathrm{pk}}(M,Y;\tilde{\sigma})$，即输入困难关系状态 Y、消息 M、公钥 pk 和预签名值 $\tilde{\sigma}$，输出 $b \in \{0,1\}$，其中 $b=1$ 表示预签名成功，$b=0$ 表示预签名失败。

3) 适配算法 $\mathrm{Adapt}(\tilde{\sigma},y)$，即输入困难关系证据 y 和预签名值 $\tilde{\sigma}$，输出真正签名值 σ。

4) 提取算法 $\mathrm{Ext}(\sigma,\tilde{\sigma},Y)$，即输入预签名值 $\tilde{\sigma}$、签名值 σ 和困难关系状态 Y，输出使 $(Y,y) \in \Psi$ 成立的困难关系证据 y 或失败符号 $\perp$。

2.2 安全模型

适配器签名的安全模型即适配器签名一般为保证安全需要满足性质的形式化定义，本节参考文献[19]和文献[21]分别给出相关定义。

定义 4 预签名的正确性。适配器签名方案是预签名正确的，即对于任意困难关系状态 Y 和消息 M，都有

$$\Pr\left[\mathrm{pVrfy}_{\mathrm{pk}}(M,Y;\tilde{\sigma})=1 \wedge \mathrm{Vrfy}_{\mathrm{pk}}(M;\sigma)=1 \wedge (Y,y') \in \Psi \,\middle|\, (\mathrm{sk},\mathrm{pk}) \leftarrow \mathrm{Gen}(1^\lambda), \tilde{\sigma} \leftarrow \mathrm{pSign}_{\mathrm{sk}}(M,Y), \sigma = \mathrm{Adapt}(\tilde{\sigma},y), y' = \mathrm{Ext}(\sigma,\tilde{\sigma},Y)\right] = 1$$

预签名的正确性是在保证传统数字签名正确性的基础上进一步验证 $\mathrm{pVrfy}_{\mathrm{pk}}(M,Y;\tilde{\sigma})$ 的正确性。

定义 5 预签名的可适配性。适配器签名方案是预签名可适配的，即对于任意的困难关系状态 Y、消息 M、公钥 pk 和预签名值 $\tilde{\sigma}$，使用困难关系证据 y 可以得到正确有效的签名值 σ，表示为

$$\Pr\left[\mathrm{Vrfy}_{\mathrm{pk}}(M;\sigma)=1 \,\middle|\, \mathrm{pVrfy}_{\mathrm{pk}}(M,Y;\tilde{\sigma})=1, \sigma = \mathrm{Adapt}(\tilde{\sigma},y)\right] = 1$$

定义 6 不可伪造性。适配器签名方案满足不可伪造性，即在任意多项式时间内攻击者 A 能取得游戏 $\mathrm{aSigForge}^A_{\Xi_{\Sigma,\Pi}}$ 胜利的可能性是可忽略不计的，表示为

$$\Pr\left[\mathrm{aSigForge}^A_{\Xi_{\Sigma,\Pi}}=1\right] < \varepsilon(\lambda)$$

游戏 $\mathrm{aSigForge}^A_{\Xi_{\Sigma,\Pi}}$ 的具体步骤如下。

1) 模拟器 S 初始化一个空消息询问列表 Q_{M}。

2) 模拟器 S 产生困难关系实例 (Y,y)，将困难关系状态 Y 和公钥 pk 一起发送给攻击者 A。

3) 攻击者 A 自主选择消息 $M_i \in \{0,1\}^*$，分别询问签名预言机 $O_{\mathrm{s}}(M)$ 和预签名预言机 $O_{\mathrm{ps}}(M,Y)$ 得到对应的签名值。

4) 攻击者 A 自主选择挑战消息 $M^* \in \{0,1\}^*$ 后询问得到关于 M^* 和 Y 的预签名值 $\tilde{\sigma}$。

5) 攻击者 A 可以选择性地对 M^* 进行 $O_{\mathrm{s}}(M)$ 和 $O_{\mathrm{ps}}(M,Y)$ 询问。

6) 攻击者 A 输出签名值 σ^*，若 σ^* 满足 $\mathrm{Vrfy}_{\mathrm{pk}}(M;\tilde{\sigma})=1$ 并且产生 σ^* 的 $M^* \notin Q_{\mathrm{M}}$，则攻击者 A 赢得游戏胜利，否则游戏失败。

定义 7 证据的可提取性。适配器签名方案是证据可提取的，即在任意的多项式时间内攻击者 A

能够取得游戏 $\mathrm{aWitExt}^{A}_{\Xi_{\Sigma,\Pi}}$ 胜利的可能性是可忽略不计的，表示为

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

游戏 $\mathrm{aWitExt}^{A}_{\Xi_{\Sigma,\Pi}}$ 的具体步骤如下。

1) 模拟器 S 初始化一个空消息询问列表 Q_{M}。

2) 模拟器 S 产生困难关系实例 (Y,y)，将困难关系状态 Y 和公钥 pk 一起发送给攻击者 A。

3) 攻击者 A 自主选择消息 $M_i\in\{0,1\}^*$，分别询问签名预言机 $O_{\mathrm{s}}(M)$ 和预签名预言机 $O_{\mathrm{ps}}(M,Y)$ 得到对应的签名值。

4) 攻击者 A 自主选择挑战消息 $M^*\in\{0,1\}^*$ 后询问得到关于 M^* 和 Y 的预签名值 $\tilde{\sigma}$。

5) 攻击者 A 可以选择性地对 M^* 进行 $O_{\mathrm{s}}(M)$ 和 $O_{\mathrm{ps}}(M,Y)$ 询问。

6) 攻击者 A 输出一个签名值 σ^*。

7) 模拟器 S 利用 $\mathrm{Ext}(\sigma^*,\tilde{\sigma},Y)$ 得到对应的 y'。

8) 若 $\mathrm{Vrfy}_{\mathrm{pk}}(M;\tilde{\sigma})=1$、$M^*\notin Q_M$ 并且 $(Y,y')\notin\Psi$，则攻击者 A 赢得游戏胜利，否则游戏失败。

定义 8　适配器签名的安全性。一个适配器签名方案若同时满足预签名的正确性、预签名的可适配性、签名的不可伪造性和证据的可提取性，就称该适配器签名方案是安全的。

3　基于 ISRSAC 的适配器签名方案

为了能够扩展 ISRSAC 算法在当前环境中的应用场景以及适配器签名技术的应用范围，本节结合困难关系和ISRSAC签名算法，设计了基于ISRSAC数字签名算法的适配器签名方案，并对其预签名的正确性进行了证明。

3.1　适配器签名方案设计

本节基于 ISRSAC 数字签名设计基于 ISRSAC 数字签名算法的适配器签名方案，主要分为预签名生成算法、预签名验证算法、适配算法和提取算法 4 个部分。在该方案中，假设困难关系 Ψ 是大整数分解问题上的困难关系，其中，$(Y,y)\subseteq Z_m^*\times Z_m^*$，$Y=y^{-e}(\mathrm{mod}\,m)$，sk、pk 等参数均源自 ISRSAC 数字签名方案。

算法 1　预签名生成算法 $(\mathrm{pSign}_{\mathrm{sk}}(M,Y))$

1) 输入消息 $M\in\{0,1\}^*$、困难关系状态 Y 和私钥 sk；

2) 计算 $r=H(M\,\|\,Y)$；

3) 计算 $\tilde{s}=r^d\bmod m$；

4) 输出预签名值 $\tilde{\sigma}=(r,\tilde{s})$。

算法 2　预签名验证算法 $\left(\mathrm{pVrfy}_{\mathrm{pk}}(M,Y;\tilde{\sigma})\right)$

1) 输入消息 $M\in\{0,1\}^*$、困难关系状态 Y、公钥 pk 和预签名值 $\tilde{\sigma}$；

2) 计算 $r'=H(M\,\|\,Yr^{-1}\tilde{s}^e)$；

3) 验证是否 $r'\equiv r$，若 $r'\equiv r$，输出 $b=1$；否则输出 $b=0$。

算法 3　适配算法 $\left(\mathrm{Adapt}(\tilde{\sigma},y)\right)$

1) 输入困难关系证据 y 和预签名值 $\tilde{\sigma}$；

2) 计算 $s=\tilde{s}y^{-1}$；

3) 得到签名值 $\sigma=(r,s)$；

4) 输出签名值 σ。

算法 4　提取算法 $\left(\mathrm{Ext}(\sigma,\tilde{\sigma},Y)\right)$

1) 输入困难关系状态 Y、预签名值 $\tilde{\sigma}$ 和签名值 σ；

2) 计算 $y'=\tilde{s}s^{-1}$；

3) 验证是否 $(Y,y')\in\Psi$，若验证成功输出 y'，否则输出 $\perp$。

3.2　正确性分析

定理 1　基于 ISRSAC 数字签名算法的适配器签名方案满足预签名正确性。

证明　在基于 ISRSAC 数字签名算法的适配器签名方案中，当给定私钥 sk、公钥 pk 时，根据 $\mathrm{pSign}_{\mathrm{sk}}(M,Y)$ 算法、$\left(\mathrm{pVrfy}_{\mathrm{pk}}(M,Y;\tilde{\sigma})\right)$ 算法及 $\mathrm{Adapt}(\tilde{\sigma},y)$ 算法可以推出

$$\begin{aligned}&r'=H(M\,\|\,Yr^{-1}\tilde{s}^e)=\\&H\left(M\,\|\,Yr^{-1}(r^d\bmod m)^e\right)=\\&H\left(M\,\|\,Yr^{-1}(r^{ed}\bmod m)\right)\end{aligned}$$

设 $\mu=\dfrac{1}{2^r}$，可得

$$\begin{aligned}&r^{ed}(\mathrm{mod}\,m)=\\&r^{1+\mu\left((p-1)(q-1)(p-2^r)(q-2^r)\right)}\bmod m=\\&rr^{\mu\left((p-1)(q-1)(p-2^r)(q-2^r)\right)}\bmod m=\\&rr^{(p-1)(q-1)\mu(p-2^r)(q-2^r)}\bmod pq\end{aligned}$$

根据费马小定理，可以进一步推出

$$\begin{aligned}&r^{ed}(\mathrm{mod}\,m)=\\&rr^{(p-1)(q-1)\mu(p-2^r)(q-2^r)}\bmod pq=\\&r1^{\mu(p-2^r)(q-2^r)}\bmod pq=r\end{aligned}$$

故有

$$r' = H\left(M \| Yr^{-1}(r^d \bmod m)^e\right) =$$
$$H(M \| Yr^{-1}r) =$$
$$H(M \| Y) = r$$

则成功推导出

$$r' = H\left(M \| Yr^{-1}(r^d \bmod m)^e\right) = r$$

即 $\mathrm{pVrfy}_{\mathrm{pk}}(M, Y; \tilde{\sigma}) = 1$ 成立。

当 $\mathrm{pVrfy}_{\mathrm{pk}}(M, Y; \tilde{\sigma}) = 1$ 且 $\sigma = \mathrm{Adapt}(\tilde{\sigma}, y)$ 时，$s = \tilde{s}y^{-1}$、和 $Y = y^{-e} \bmod m$ 均成立，则可以推出

$$r' = H\left(M \| Yr^{-1}\tilde{s}^e\right) =$$
$$H\left(M \| Yr^{-1}(sy)^e\right) =$$
$$H\left(M \| y^{-e}r^{-1}s^e y^e\right) =$$
$$H(M \| r^{-1}s^e)$$

因此得知 σ 是关于消息 M 和公钥 pk 的有效签名，即 $\mathrm{Vrfy}_{\mathrm{pk}}(M; \sigma) = 1$。

此外，根据 $\mathrm{Adapt}(\tilde{\sigma}, y)$ 算法可知 $\tilde{\sigma} = (r, \tilde{s})$，$\sigma = (r, s)$，$y' = \tilde{s}s^{-1}$，可以进一步推出

$$\mathrm{Ext}((r,s),(r,\tilde{s}),Y) =$$
$$\tilde{s}s^{-1} =$$
$$\tilde{s}\left(\tilde{s}y^{-1}\right)^{-1} =$$
$$\tilde{s}\tilde{s}^{-1}\left(y^{-1}\right)^{-1} = y$$

证得 y' 与困难关系状态 Y 之间有 $(Y, y') \in \Psi$。故可得

$$\Pr\left[\mathrm{pVrfy}_{\mathrm{pk}}(M, Y; \tilde{\sigma}) = 1 \wedge \mathrm{Vrfy}_{\mathrm{pk}}(M; \sigma) = 1 \wedge (Y, y') \in \Psi \,\middle|\, (\mathrm{sk}, \mathrm{pk}) \leftarrow \mathrm{Gen}(1^\lambda), \tilde{\sigma} \leftarrow \mathrm{pSign}_{\mathrm{sk}}(M, Y), \sigma = \mathrm{Adapt}(\tilde{\sigma}, y), y' = \mathrm{Ext}(\sigma, \tilde{\sigma}, Y)\right] = 1$$

成立。证毕。

4 安全性分析

适配器签名方案为保证安全，除满足预签名的正确性外，还需满足签名的不可伪造性、预签名的可适配性和证据的可提取性，本节依次给出证明。

定理 2 如果在任意的多项式时间内攻击者 A 能够取得游戏 $\mathrm{aSigForge}^{A}_{\Xi_{\Sigma,\Pi}}$ 胜利的可能性是可忽略不计的，那么基于 ISRSAC 数字签名算法的适配器签名方案是不可伪造的。

证明 假设攻击者 A 和模拟器 S 一起参与游戏 $\mathrm{aSigForge}^{A}_{\Xi_{\Sigma,\Pi}}$，在这个游戏中攻击者 A 能够对模拟器 S 发出预签名询问 O_{ps}、签名询问 O_{s} 和哈希询问 $H(\cdot)$，模拟器 S 能够对攻击者 A 的询问进行响应。$\mathrm{aSigForge}^{A}_{\Xi_{\Sigma,\Pi}}$ 的具体步骤如下。

1) 模拟器 S 初始化一个空消息询问列表 Q_{M} 和一个空哈希询问列表 Q_{H}。

2) 模拟器 S 产生困难关系实例 (Y, y)，将困难关系状态 Y 和公钥 pk 一起发送给攻击者 A。

3) 攻击者 A 自主选择消息 $M_i \in \{0,1\}^*$，在进行哈希询问 $H(x)$ 后，分别询问签名预言机 $O_{\mathrm{s}}(M)$ 和预签名预言机 $O_{\mathrm{ps}}(M, Y)$，得到对应的签名值。

其中，模拟器 S 对哈希询问 $H(x)$ 的具体响应是：当攻击者 A 发起对 x 的 $H(x)$ 询问后，模拟器 S 首先查询 Q_{H} 列表中是否有对应的消息对，如果存在则直接将对应的消息对输出并返回给攻击者 A；如果不存在则产生对应的 $H(x)$，并将对应的消息对 $(x, H(x))$ 更新到 Q_{H} 列表中。对签名预言机 $O_{\mathrm{s}}(M)$ 的具体响应是：当攻击者 A 询问消息 M_i 的签名值时，模拟器 S 直接通过 O_{s} 得到有关消息 M_i 的签名值 σ，并将签名值 σ 返回给攻击者 A。对预签名预言机 $O_{\mathrm{ps}}(M, Y)$ 的具体响应是：当攻击者 A 询问消息 M_i 和困难关系状态 Y 的预签名值时，模拟器 S 首先通过 O_{s} 得到有关消息 M_i 的签名值 σ，接着将产生签名值的消息 M_i 存入消息列表 Q_{M}，随后计算 $\tilde{s} = sy$，最后将生成的预签名值 $\tilde{\sigma} = (r, \tilde{s})$ 返回给攻击者 A。

4) 攻击者 A 自主选择挑战消息 $M^* \in \{0,1\}^*$ 后询问关于消息 M_i 和困难关系状态 Y 的预签名值 $\tilde{\sigma}$，模拟器 S 通过 $O_{\mathrm{ps}}(M^*, Y)$ 对攻击者 A 的询问进行响应。

5) 攻击者 A 可以自主选择是否再次循环步骤 3)。

6) 攻击者 A 输出签名值 σ^*，当模拟器 S 收到 σ^* 后，验证是否 $\sigma^* \equiv \mathrm{Adapt}(\tilde{\sigma}, y)$，若成立则说明出现了不属于 Q_{M} 中的消息 M^* 的合法签名值 σ^*，系统进行报错处理，攻击者 A 获得游戏胜利。

整个游戏过程中，A 只有可能在步骤 6)中出现游戏胜利的情况，但在这种情况下，攻击者 A 能够成功通过 σ^* 和 $\tilde{\sigma}$ 在提取算法中得到困难关系证据 y 的可能性是可以忽略不计的。那么能够取得游戏胜利的概率也是可以忽略不计的，故证得 $\Pr\left[\mathrm{aSigForge}^{A}_{\Xi_{\Sigma,\Pi}} = 1\right] < \varepsilon(\lambda)$ 成立。证毕。

定理 3 基于 ISRSAC 数字签名算法的适配器签名方案满足预签名可适配性。

证明 在定理 1 中已经证得 σ 是关于消息 M 和公钥 pk 的有效签名，即 $\mathrm{Vrfy}_{\mathrm{pk}}(M; \sigma) = 1$，故

$$\Pr\left[\mathrm{Vrfy}_{\mathrm{pk}}(M;\sigma)=1 \middle| \mathrm{pVrfy}_{\mathrm{pk}}(M,Y;\tilde{\sigma})=1,\ \sigma=\mathrm{Adapt}(\tilde{\sigma},y)\right]=1$$

成立。证毕。

定理 4　如果在任意的多项式时间内攻击者 A 能够取得游戏 $\mathrm{aWitExt}^{A}_{\Xi_{\Sigma,\Pi}}$ 胜利的可能性是可忽略不计的，那么基于 ISRSAC 数字签名算法的适配器签名方案是满足证据可提取性的。

证明　假设攻击者 A 和模拟器 S 一起参与游戏 $\mathrm{aWitExt}^{A}_{\Xi_{\Sigma,\Pi}}$，在这个游戏中攻击者 A 能够对模拟器 S 发出预签名询问 O_{ps}、签名询问 O_{s} 和哈希询问 $H(\cdot)$，模拟器 S 能够对攻击者 A 的询问进行响应。$\mathrm{aWitExt}^{A}_{\Xi_{\Sigma,\Pi}}$ 的具体步骤如下。

1) 模拟器 S 初始化一个空消息询问列表 Q_{M} 和一个空哈希询问列表 Q_{H}。

2) 模拟器 S 产生困难关系实例 (Y,y)，将困难关系状态 Y 和公钥 pk 一起发送给攻击者 A。

3) 攻击者 A 自主选择消息 $M_i\in\{0,1\}^*$，先进行哈希询问 $H(x)$，然后分别询问签名预言机 $O_{\mathrm{s}}(M)$ 和预签名预言机 $O_{\mathrm{ps}}(M,Y)$ 得到对应签名值。

其中，模拟器 S 对哈希询问 $H(x)$ 的具体响应是：当攻击者 A 发起对 x 的 $H(x)$ 询问后，模拟器 S 首先查询 Q_{H} 列表中是否有对应的消息对，如果存在则直接将对应的消息对输出并返回给攻击者 A；如果不存在则产生对应的 $H(x)$，并将对应的消息对 $\left(x,H(x)\right)$ 更新到 Q_{H} 列表中；对签名预言机 $O_{\mathrm{s}}(M)$ 的具体响应是：当攻击者 A 询问消息 M_i 的签名值时，模拟器 S 直接通过 O_{s} 得到有关消息 M_i 的签名值 σ，并将签名值 σ 返回给攻击者 A。对预签名预言机 $O_{\mathrm{ps}}(M,Y)$ 的具体响应是：当攻击者 A 询问消息 M_i 和困难关系状态 Y 的预签名值时，模拟器 S 首先通过 O_{s} 得到消息 M_i 的签名值 σ，接着计算出 $\tilde{s}=sy$，$y'=\tilde{s}s^{-1}$，判断是否 $(Y,y')\in\Psi$，如果 $\left(Y,y'\right)\notin\Psi$，则游戏结束，攻击者 A 获得游戏胜利；否则将消息 M_i 存入 Q_{M} 中并输出预签名值 $\tilde{\sigma}=(r,\tilde{s})$ 给攻击者 A。

4) 攻击者 A 自主选择是否挑战消息 $M^*\in\{0,1\}^*$ 后询问关于消息 M_i 和困难关系状态 Y 的预签名值 $\tilde{\sigma}$，模拟器 S 通过 $O_{\mathrm{ps}}(M^*,Y)$ 对攻击者 A 的询问进行响应。

5) 攻击者 A 可以自主选择是否再次循环步骤 3)。

6) 攻击者 A 输出签名值 σ^*。

整个游戏过程中，A 只有可能在步骤 3)中的 $O_{\mathrm{ps}}(M,Y)$ 询问中出现游戏胜利的情况，但这种情况出现的可能性是可以忽略不计的，即能够取得游戏胜利的概率也是可以忽略不计的，故证得 $\Pr\left[\mathrm{aWitExt}^{A}_{\Xi_{\Sigma,\Pi}}=1\right]<\varepsilon(\lambda)$ 成立。证毕。

定理 5　当基于 ISRSAC 数字签名算法的适配器签名方案满足预签名的正确性、不可伪造性、预签名的可适配性和证据可提取性时，基于 ISRSAC 数字签名算法的适配器签名方案是安全的。

证明　根据定理 1~定理 4 可知，基于 ISRSAC 数字签名算法的适配器签名方案满足预签名的正确性、不可伪造性、预签名的可适配性和证据可提取性，即基于 ISRSAC 的适配器签名方案是安全的。证毕。

5　方案对比分析

本节将本文方案与文献[21]中的基于 SM2 的方案及文献[19]中的基于 Schnorr 的方案和基于 ECDSA 的方案在时间开销、安全性等方面进行比较。

5.1　效率对比分析

在对各方案效率进行对比分析前，先将本节所需的必要符号进行说明，如表 1 所示。

表 1　符号及定义

符号	含义
T_{mul}	Z_m^*或Z_q^* 中执行一次模乘的耗时
T_{add}	Z_m^*或Z_q^* 中执行一次模加的耗时
T_{inv}	Z_m^*或Z_q^* 中执行一次模逆的耗时
T_{exp}	Z_m^* 中执行一次模指数的耗时
T_{h}	一次哈希运算的耗时
T_{pm}	群 G 中一次点乘的耗时
T_{pa}	群 G 中一次点加的耗时
T_{ZP}	零知识证明中运行一次生成算法耗时
T_{ZV}	零知识证明中运行一次验证算法耗时

下面将各方案不同算法部分的时间开销分别进行对比分析，如表 2 所示。

在密钥生成算法中，本文方案的时间开销为 $7T_{\mathrm{mul}}+2T_{\mathrm{inv}}$，相比其他 3 种方案时间开销略多。

在预签名生成算法中，本文方案的时间开销为 $T_{\mathrm{h}}+T_{\mathrm{exp}}$，与基于 SM2 的方案相比多了 T_{exp} 的耗时，但少了 $2T_{\mathrm{pm}}+T_{\mathrm{pa}}+2T_{\mathrm{mul}}+T_{\mathrm{inv}}+3T_{\mathrm{add}}+T_{\mathrm{ZP}}$ 的耗时；与

表 2 各方案不同算法部分的时间开销

方案	密钥生成算法	预签名生成算法	预签名验证算法	适配算法	提取算法
基于 SM2 的方案	T_{mul}	$2T_{\text{pm}}+T_{\text{pa}}+T_{\text{h}}+2T_{\text{mul}}+T_{\text{inv}}+3T_{\text{add}}+T_{\text{ZP}}$	$2T_{\text{pm}}+T_{\text{pa}}+T_{\text{h}}+2T_{\text{mul}}+3T_{\text{add}}+T_{\text{ZV}}$	T_{add}	T_{add}
基于 Schnorr 的方案	T_{mul}	$T_{\text{pm}}+T_{\text{pa}}+T_{\text{h}}+T_{\text{mul}}+T_{\text{add}}$	$2T_{\text{pm}}+2T_{\text{pa}}+T_{\text{h}}$	T_{add}	T_{add}
基于 ECDSA 的方案	T_{mul}	$2T_{\text{pm}}+T_{\text{inv}}+T_{\text{h}}+T_{\text{mul}}+T_{\text{add}}+T_{\text{ZP}}$	$3T_{\text{pm}}+T_{\text{inv}}+T_{\text{h}}+2T_{\text{mul}}+T_{\text{ZV}}$	$T_{\text{inv}}+T_{\text{mul}}$	$T_{\text{inv}}+T_{\text{mul}}$
本文方案	$7T_{\text{mul}}+2T_{\text{inv}}$	$T_{\text{h}}+T_{\text{exp}}$	$T_{\text{h}}+2T_{\text{mul}}+T_{\text{inv}}+T_{\text{exp}}$	$T_{\text{inv}}+T_{\text{mul}}$	$T_{\text{inv}}+T_{\text{mul}}$

基于 Schnorr 的方案相比多了 T_{exp}，但少了 $T_{\text{pm}}+T_{\text{pa}}+T_{\text{mul}}+T_{\text{add}}$ 的耗时；与基于 ECDSA 的方案相比多了 T_{exp} 的耗时，但少了 $2T_{\text{pm}}+T_{\text{inv}}+T_{\text{mul}}+T_{\text{add}}+T_{\text{ZP}}$ 的耗时。

在预签名验证算法中，本文方案的时间开销为 $T_{\text{h}}+2T_{\text{mul}}+T_{\text{inv}}+T_{\text{exp}}$，与基于 SM2 的方案相比多了 $T_{\text{inv}}+T_{\text{exp}}$ 的耗时，但少了 $2T_{\text{pm}}+T_{\text{pa}}+3T_{\text{add}}+T_{\text{ZV}}$ 的耗时，优于基于 SM2 的方案；与基于 Schnorr 的方案相比多了 $2T_{\text{mul}}+T_{\text{inv}}+T_{\text{exp}}$ 的耗时，但少了 $2T_{\text{pm}}+2T_{\text{pa}}$ 的耗时；与基于 ECDSA 的方案相比多了 T_{exp} 的耗时，但少了 $3T_{\text{pm}}+T_{\text{ZV}}$ 的耗时。

由于 T_{exp} 的实际耗时取决于指数运算具体应用何种方式进行运算，例如，当 $a^b \bmod c$ 用最直接的方式转化为模乘运算，则可以变形为 $a^b \bmod c = a(\bmod c)\times\cdots\times a(\bmod c)$，即进行 $b-1$ 次模乘运算；当应用二进制算法进行时，模乘次数转变为 $\sum_{i=0}^{\rho-1} b_i - 1$，其中，$\sum_{i=0}^{\rho-1} b_i$ 表示指数 e 的二进制表示中 1 的个数，故优秀的方式会使 T_{exp} 的实际耗时很低。

在适配算法和提取算法中，本文方案使用了乘法构造法，使适配算法和提取算法的时间开销均为 $T_{\text{inv}}+T_{\text{mul}}$，与使用乘法构造法的基于 ECDSA 的方案时间开销相同，与基于 SM2 的方案和基于 Schnorr 的方案相比时间开销略高。

5.2 安全性能对比分析

为了更清晰地了解本文方案与其他方案的区别和联系，本节从主要计算量和安全性方面对几种方案进行对比分析，具体结果如表 3 所示。

从表 3 中可以看到，在安全性方面，4 种方案均从预签名正确性、预签名可适配性、aEUF-CMA 安全性、证据可提取性方面进行了分析。在主要计算量方面，本文方案主要基于模乘和模加运算以及哈希运算，其他 3 种方案除了基于模乘和模加运算以及哈希运算外，还有对群 G 中点乘和点加运算或零知识证明算法的运算。

通过对上述方案的对比分析可知，本文方案在时间开销上相比其他方案并无明显优势，但在主要计算量上涉及更少类型，更简便且易实现，且本文的主要目的也并非设计更高计算效率的适配器签名方案，而是要构造基于 ISRSAC 算法的适配器签名方案，扩展 ISRSAC 算法在当前环境中的应用场景并且使适配器签名的选择更具灵活性，可以应用到更多的领域。

6 结束语

本文以 ISRSAC 数字签名算法为基础构造了适配器签名方案，然后证明了该方案满足预签名的正确性、不可伪造性、预签名的可适配性、证据的可提取性和签名方案的安全性。此外，本文还将本文方案与基于其他算法的适配器签名方案在时间开销、安全性以及主要计算量等方面进行了对比分析，分析结果表明，本文方案在时间开销上相比其他适配器签名方案并无明显优势，但在主要计算量方面涉及种类少，更简便且易实现。

以 ISRSAC 数字签名算法为基础构造的适配器

表 3 名方案主要计算量和安全性对比

方案	主要计算量	安全性
基于 SM2 的方案	群 G 中点乘和点加运算、模乘和模加运算、哈希运算、零知识证明算法运算	预签名正确性、预签名可适配性、aEUF-CMA 安全性、证据可提取性
基于 Schnorr 的方案	群 G 中点乘运算、模乘运算、哈希运算	aEUF-CMA 安全性、预签名可适配性、预签名正确性、证据可提取性
基于 ECDSA 的方案	群 G 中点乘和点加运算、模乘运算、哈希运算、零知识证明算法运算	aEUF-CMA 安全性、预签名可适配性、预签名正确性、证据可提取性
本文方案	模乘和模加运算、哈希运算	预签名正确性、不可伪造性（即 aEUF-CMA 安全性）、预签名的可适配性、证据的可提取性

签名方案，扩展了 ISRSAC 算法在当前环境中的可应用场景，并且 ISRSAC 算法和适配器签名方案的结合可以使适配器签名的选择更具灵活性，可以应用到更多的领域，有更广的应用空间。

参考文献：

[1] DIFFIE W, HELLMAN M. New directions in cryptography[J]. IEEE Transactions on Information Theory, 1976, 22(6): 644-654.

[2] 程朝辉. 数字签名技术概览[J]. 信息安全与通信保密, 2020, 18(7): 48-62.
CHENG C H. Overview of digital signature technology[J]. Information Security and Communications Privacy, 2020, 18(7): 48-62.

[3] SCHNORR C P. Efficient signature generation by smart cards[J]. Journal of Cryptology, 1991, 4(3): 161-174.

[4] ERWIG A, FAUST S, HOSTÁKOVÁ K, et al. Two-party adaptor signatures from identification schemes[C]//IACR International Conference on Public-Key Cryptography. Berlin: Springer, 2021: 451-480.

[5] TANG W Z, WANG W N, FANTI G, et al. Privacy-utility tradeoffs in routing cryptocurrency over payment channel networks[C]//Proceedings of the ACM on Measurement and Analysis of Computing Systems. New York: ACM Press, 2020: 1-39.

[6] DECKER C, WATTENHOFER R. A fast and scalable payment network with bitcoin duplex micropayment channels[C]//Symposium on Self-Stabilizing Systems. Berlin: Springer, 2015: 3-18.

[7] ERDIN E, CEBE M, AKKAYA K, et al. A scalable private bitcoin payment channel network with privacy guarantees[J]. Journal of Network and Computer Applications, 2021: doi.org/10.1016/j.jnca.2021.103021.

[8] CLA B, NING M D, XUN W, et al. Rapido: scaling blockchain with multi-path payment channels[J]. Neurocomputing, 2020, 406: 322-332.

[9] RYU K, KIM W, LEE E K. PayGo: incentive-comparable payment routing based on contract theory[J]. IEEE Access, 2020, 8: 70095-70110.

[10] MILLER A, BENTOV I, KUMARESAN R, et al. Sprites and state channels: payment networks that go faster than lightning[J]. arXiv Preprint, arXiv: 1702.05812, 2017.

[11] DESHPANDE A, HERLIHY M. Privary-preserving cross-chain atomic swaps[C]//Financial Cryptography and Data Security. Berlin: Springer, 2020: 540-549.

[12] HOENISCH P, PINO L S D. Atomic swaps between bitcoin and monero[J]. arXiv Preprint, arXiv: 2101.12332, 2021.

[13] MALAVOLTA G, MORENO-SANCHEZ P, SCHNEIDEWIND C, et al. Anonymous multi-hop locks for blockchain scalability and interoperability[C]//Proceedings of 2019 Network and Distributed System Security Symposium. Reston: Internet Society, 2019: 10168773.

[14] TAIRI E K, MORENO-SANCHEZ P, MAFFEI M. A2L: anonymous atomic locks for scalability in payment channel hubs[C]//Proceedings of 2021 IEEE Symposium on Security and Privacy (SP). Piscataway: IEEE Press, 2021: 1834-1851.

[15] AUMAYR L, ERSOY O, ERWIG A, et al. Generalized bitcoin compatible channels[J]. IACR Cryptology ePrint Archive, 2020(2020):476.

[16] ESGIN M F, ERSOY O, ERKIN Z. Post-quantum adaptor signatures and payment channel networks[C]//Proceedings of the 25th European Symposium on Research in Computer Security. Berlin: Springer, 2020: 378-397.

[17] TAIRI E K, MORENO-SANCHEZ P, MAFFEI M. Post-quantum adaptor signature for privacy-preserving off-chain payments[C]//International Conference on Financial Cryptography and Data Security. Berlin: Springer, 2021: 131-150.

[18] QIN X, CUI H, YUAN T H. Generic adaptor signature[J]. IACR Cryptology ePrint Archive, 2021(2021):161.

[19] AUMAYR L, ERSOY O, ERWIG A, et al. Generalized channels from limited blockchain scripts and adaptor signatures[C]//Lecture Notes in Computer Science. Berlin: Springer, 2021: 635-664.

[20] THYAGARAJAN S A K, MALAVOLTA G. Lockable signatures for blockchains: scriptless scripts for all signatures[C]// Proceedings of 2021 IEEE Symposium on Security and Privacy (SP). Piscataway: IEEE Press, 2021: 937-954.

[21] 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.

[22] VARALAKSHMI P, THANGAVEL M. Improved secure RSA cryptosystem for data confidentiality in cloud[J]. International Journal of Information Systems and Change Management, 2017, 9(4): 261-277.

[23] YANG T, ZHANG Y S, XIAO S, et al. Digital signature based on ISRSAC[J]. China Communications, 2021, 18(1): 161-168.

[24] 田椒陵. SM3 算法界面设计及安全性分析[J]. 信息安全与技术, 2014, 5(5): 24-26, 33.
TIAN J L. SM3 algorithm interface design and safety analysis[J]. Information Security and Technology, 2014, 5(5): 24-26, 33.

[作者简介]

张艳硕（1979– ），男，陕西宝鸡人，博士，北京电子科技学院副教授、硕士生导师，主要研究方向为密码理论及其应用。

刘宁（1999– ），女，山西忻州人，北京电子科技学院硕士生，主要研究方向为密码学。

袁煜淇（2000– ），女，江西南昌人，北京电子科技学院硕士生，主要研究方向为密码学。

杨亚涛（1978– ），男，河南平顶山人，博士，北京电子科技学院教授、博士生导师，主要研究方向为信息安全、同态加密、密码协议和算法。