

基于 SM2 的两方协作盲签名协议

白雪, 秦宝东, 郭瑞, 郑东

(西安邮电大学网络空间安全学院, 陕西 西安 710121)

摘要: SM2 是我国于 2010 年发布的椭圆曲线公钥密码标准, 由于其具有比 RSA 签验速度快、存储空间小和运算复杂度低的特点被广泛应用于金融、社保等领域。随着国密算法的推广应用, 密钥安全和数据隐私问题备受关注。单密钥签名模式的签名权力过于集中, 无法满足分布式环境的应用需求, 密钥泄露将威胁整个密码系统的安全, 密钥的安全存储和合理利用问题亟待解决。此外, 标准 SM2 数字签名算法无法实现消息内容的隐私保护功能, 国密算法的签名消息的隐私保护有待进一步探究。针对签名算法的密钥安全和数据隐私问题, 已有对 SM2 的协作签名研究和盲签名研究, 然而, 没有对 SM2 盲签名的协作设计, 提出一种两方协作的盲签名协议, 允许除用户以外的两方执行签名操作, 签名过程无须恢复完整私钥, 不会泄露部分私钥和秘密数的信息, 密钥分散存储提升密钥安全性, 盲签名性质保护消息隐私。在安全性方面, 协议满足不可伪造性和不可链接性; 在效率方面, 使用 C 语言进行仿真测试, 系统中各个参与者在本地的运行耗时均在可承受范围内, 在签名者诚实执行协议的情况下, 协作签名阶段中各个实体的时间损耗与执行一次轻量级的 SM2 盲签名的时间损耗基本一致。因此, 该协议在功能和效率上具备一定的实用前景。

关键词: SM2; 协作盲签名; 密钥安全; 隐私保护

中图分类号: TP309.2

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2022081

Two-party cooperative blind signature based on SM2

BAI Xue, QIN Baodong, GUO Rui, ZHENG Dong

School of Cyberspace Security, Xi'an University of Posts & Telecommunications, Xi'an 710121, China

Abstract: SM2, issued by China in 2010, is a public key cryptography standard based on elliptic curves. It has been widely used in finance, social security and other fields thanks to its advantages of improved signature efficiency, decreased storage space and computing complexity than RSA. With the popularization and application of SM2, the issues of its key security and data privacy are of great concern. The single-key mode inhibits the potential

收稿日期: 2022-02-02; 修回日期: 2022-06-22

通信作者: 秦宝东, qinbaodong@xupt.edu.cn

基金项目: 国家自然科学基金 (61872292); 青海省基础 Research 计划项目 (2020-ZJ-701)

Foundation Items: The National Natural Science Foundation of China (61872292), Basic Research Program of Qinghai Province (2020-ZJ-701)

引用格式: 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.

Citation Format: 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.

application in multi-user settings, and the leakage of the key will threaten the security of the entire cryptosystem due to the centralization. The problem of secure storage and reasonable utilization of keys needs to be solved urgently. In addition, the SM2 digital signature algorithm cannot guarantee the message privacy. Aiming at the issues of key security and data privacy of the signature algorithm, many researchers have proposed the idea of cooperative signature and blind signature for SM2. However, there isn't SM2 collaborative blind signature scheme proposed. Then a two-party cooperative blind signing protocol based on SM2 was proposed in this paper, which allowed two parties to sign except the user. The signing process did not require recovering the complete private key, while not revealing the information of the partial private key and secret number. The key was stored separately to improve the security of the key, while the blind signature protected the privacy of the message. In terms of security, the protocol satisfied unforgeability and unlinkability. The protocol was implemented using C to demonstrate the efficiency of each participant's local operation. In the honest model, the time cost of each entity in the cooperative signature phase was similar as that of executing a lightweight SM2 blind signature. Overall, the proposed protocol has certain advantages in terms of function and efficiency.

Keywords: SM2, two-party blind signature, key security, privacy protection

0 引言

SM2^[1]是国家密码管理局于 2010 年 12 月 17 日颁布的基于椭圆曲线的公钥密码标准,该标准包括数字签名算法、密钥交换协议和公钥加密算法,其中,SM2 数字签名算法于 2018 年被正式发布在 ISO/IEC14888-3:2018 中。该算法改善了 RSA 面临的安全威胁,使用较短的密钥即可与 RSA 达到同等的安全级别^[2]。为了实现我国密码基础建设的安全可控,国家密码管理局计划用 SM2 逐步替换 RSA,完成信息行业国密算法的升级改造^[3],至此,国产密码的应用引起了国内外学者的广泛关注,现已产生了较多关于 SM2 算法的研究成果^[4-6]。

在数字签名技术中,一方面,考虑到密钥作为用户身份的凭证,可确保用户具有相关权限,密钥一旦泄露,攻击者可伪装成合法用户威胁整个系统的安全^[7],并且,签名权力的集中不利于多方参与决策的公平性,密钥的安全存储和合理利用问题亟待解决;另一方面,传统签名模式中的待签名消息对签名者完全公开,签名者可以对消息进行追溯^[8],这不适用于对消息内容有隐私保护需求的应用,如电子交易、电子竞拍和匿名选举等^[9]。

针对 SM2 数字签名算法中的密钥安全^[10]问题,国内外学者相继提出了基于 Shamir^[11]秘密分享原理、Paillier^[12]同态加密和安全两方计算的协

作签名思想,即密钥分散存储,至少两个参与者共同执行签名操作。前者属于 (t, n) 门限密码范畴,在 n 个参与者中允许 t 个及以上用户生成最终签名结果,有效提升了密钥安全性和系统稳健性,但由于 SM2 数字签名的特殊结构,现有方案^[13-15]使用零秘密共享、乘法秘密共享、点乘秘密共享和求逆秘密共享的方法,存在交互次数多、效率较低的问题。Ding 等^[16]提出 SM2 协作签名和群签名方案,通过秘密分享密钥、添加随机数的方式减少了签名交互。2020 年,Zhang 等^[17]提出了可证明安全的 SM2 两方协作签名方案,参与者使用本地私钥协商生成签名验证公钥,在签名阶段借助 Paillier 同态性质交互一次完成签名操作。侯等^[18]采用零知识证明、比特承诺技术设计了两方签名方案,较文献[17]的方案减少了一次同态加密操作。之后,为解决移动互联网环境中,用户计算资源和存储空间受限的问题,冯吟雪等^[19]采用改进的 SM2 签名形式,简化私钥求逆运算,设计了轻量级的安全两方签名协议。苏等^[20]使用参与者的部分私钥验证中间计算结果的正确性,无须零知识证明辅助,通过预计算的方式提升了签名效率。2022 年,Tang 等^[21]利用椭圆曲线上的 Diffie-Hellman 密钥交换变体设计实现了两方 SM2 协作签名方案,同样在无须零知识证明的辅助下保证了中间结果的一致性。

针对数字签名算法中的消息隐私保护研究,有效的方式是设计盲签名方案^[22-23],即用户令签

名者对盲化的消息进行签名, 用户可消除盲因子得到原始消息的签名, 签名者无法预知消息内容, 有效保证了消息隐私。在现有的 SM2 盲签名方案中, He 等^[24]提出将原始 SM2 签名结构中的随机数拆分为两部分, 采用 Paillier 同态加密性质盲化消息, 但同样由于使用开销较大的同态加密, 方案效率较低, 2020 年, Zhang 等^[25]对其改进, 采用随机数盲化消息的通用构造, 设计了轻量级的 SM2 盲签名方案, 是目前较为高效的可证明安全的盲签名方案。2022 年, 唐卫中等^[26]提出一种 SM2 无证书盲签名方案用以满足通信带宽和存储资源受限环境下的应用需求。但以上方案中的签名私钥由唯一的签名者持有, 依然存在签名权力集中、单个密钥泄露导致的系统安全问题。

综上, 现有方案可单独实现基于 SM2 的两方协作签名功能或实现基于 SM2 的盲签名功能, 前者无法满足消息隐私保护需求, 后者无法满足两方参与者决策的应用。本文考虑到盲签名方案中的密钥安全问题, 提出一种基于 SM2 的两方协作盲签名协议, 允许除用户以外的两个参与者执行签名操作。对用户而言, 待签名消息对签名者保密, 对两个签名者而言, 签名过程不会暴露各自的私钥信息, 在提升 SM2 签名密钥安全性的同时实现消息隐私保护。此外, 本文对协议进行了性能评估, 结果表明在诚实模型下, 协议的计算代价较小, 具备一定的应用价值。

1 预备知识

1.1 SM2 数字签名算法

定义 λ 为安全参数, $E(F_q)$ 是定义在有限域 F_q 上的椭圆曲线, 其方程表示为 $y^2 = x^3 + ax + b$, q 是有限域上的元素数目, 定义 P 是椭圆曲线上阶为素数 n 的一个基点, 其坐标表示为 $P = (x_p, y_p)$ 。 H_{256}^* 表示输入任意长度的字符串, 输出为 256 bit 的安全哈希函数, H_v^* 表示输入任意长度的字符串, 输出为 v bit 的安全哈希函数。在本文中, 符号 “ $\cdot$ ” 表示椭圆曲线上的点乘运算, “ $\parallel$ ” 表示字符串的拼接, SM2 数字签名算法包含以下 4 个阶段。

1) 系统参数建立 (Setup): 输入安全参数 λ , 输出椭圆曲线系统参数 $\text{params} = \{E(F_q), P, n\}$ 。

2) 密钥生成 (KenGen): 输入系统参数 params , 签名者随机选择一个秘密数 $d \in Z_n^*$ 作为私钥, 计算签名验证公钥 $PK = d \cdot P = (x_k, y_k)$, 输出 (PK, d) 作为签名密钥对。

3) 签名生成 (Sign): 输入系统参数 params 、待签名消息 M 和私钥 d , 签名者按以下步骤执行。

① 计算 $Z = H_{256}(\text{LEN} \parallel \text{ID} \parallel a \parallel b \parallel x_p \parallel y_p \parallel x_k \parallel y_k)$, 其中 ID 是长度为 LEN 的签名者可辨别标识。

② 计算 $e = H_v(Z \parallel M)$ 。

③ 随机选择 $k \in Z_n^*$, 计算 $R = k \cdot P = (R_x, R_y)$ 。

④ 计算 $r = (e + R_x) \bmod n$, 若 $r = 0$ 或 $r + k = 0$, 则重新执行步骤③。

⑤ 计算 $s = (1 + d)^{-1}(k - rd) \bmod n$, 若 $s = 0$, 则重新执行步骤③。

⑥ 输出签名 $\sigma = (r, s)$ 。

4) 签名验证 (Verify): 输入系统参数 params 、签名验证公钥 PK 、消息 M 及其对应的签名 $\sigma = (r, s)$, 验证者按以下步骤执行。

① 检验 $r, s \in Z_n^*$ 是否成立, 若不成立, 则签名无效。

② 计算 $e' = H_v(Z \parallel M)$ 。

③ 计算 $t' = (r + s) \bmod n$, 若 $t' = 0$, 则签名无效。

④ 计算 $R = s \cdot P + t' \cdot PK = (R'_x, R'_y)$, $r' = (e' + R'_x) \bmod n$ 。

⑤ 检验 $r = r'$ 是否成立, 若成立, 则签名通过, 输出 1, 否则签名无效, 输出 0。

特别地, 签名 $s = (1 + d)^{-1}(k - rd) \bmod n$ 等价于改进形式 $s = ((1 + d)^{-1}(k + r) - r) \bmod n$, 本文方案采用改进形式进行设计。

SM2 数字签名算法的安全性: SM2 属于椭圆曲线公钥密码算法, 其安全性建立在求解椭圆曲线离散对数问题 (ECDLP) 的困难性之上。文献[27]证明若哈希函数 H_v 是均匀且抗碰撞的, 则 SM2 数字签名算法在通用群模型^[28]中对适应性选择消息攻击具有存在不可伪造性 (EU-CMA)。

1.2 盲签名协议

盲签名协议由用户和签名者参与执行, 协议

包含以下 4 个阶段,

1) 系统参数建立 (Setup): 输入安全参数 λ , 输出签名所需系统公开参数 params 。

2) 密钥生成 (KenGen): 输入系统参数 params , 签名者生成签名密钥对 (sk, pk) 。

3) 盲签名生成 (B_Sign): 输入系统参数 params 、待签名消息 M 和签名私钥 sk , 用户和签名者按以下步骤执行。

① 用户盲化待签名消息 M 得到 M' , 将 M' 发送给签名者。

② 签名者接收到 M' , 使用私钥 sk 对 M' 进行签名得到 σ' , 将 σ' 发送给用户。

③ 用户接收到 σ' , 消除盲因子, 输出消息 M 的签名 σ 。

4) 签名验证 (Verify): 输入系统参数 params 、签名验证公钥 pk 、消息 M 及其对应的签名 σ , 执行验证算法, 若签名有效, 则输出 1, 否则输出 0。

1.3 知识提取假设

1991 年, Damgård 等^[29]提出知识提取假设 (简称 KEA), 用于密码方案的安全性证明。该假设也被苏吟雪等^[20]用于证明其设计的基于 SM2 的协作签名协议, 该假设的定义如下。

定义 1 (知识提取假设 KEA)。假设 P 和 Q 是有限循环群中的两个元素, T 是任意多项式时间算法, 输入 (P, Q) , 输出 (kP, kQ) , 其中 k 是算法 T 选择的。那么, 存在另一个多项式时间算法 T^* , 当算法的输入与 T 相同, 且使用与 T 相同的随机纸带, 那么算法 T^* 将以压倒性的优势 $1-\epsilon$ 输出 (k, kP, kQ) , 其中 ϵ 是一个可忽略量。

2 两方协作盲签名协议

2.1 系统模型

本文提出的两方协作盲签名协议的系统模型如图 1 所示。

该模型包含以下 3 个实体。

1) 用户 U : 待签名消息的持有者。将消息进行盲化处理后, 利用第一签名者和第二签名者获取原始消息的签名。

2) 第一签名者 S_1 : 签名协议的部分私钥持有者, 通过与第二签名者协作完成对用户消息的签名。

3) 第二签名者 S_2 : 与第一签名者类似, 持有签名协议的部分私钥, 并通过与第一签名者共同执行协议完成对用户消息的签名。

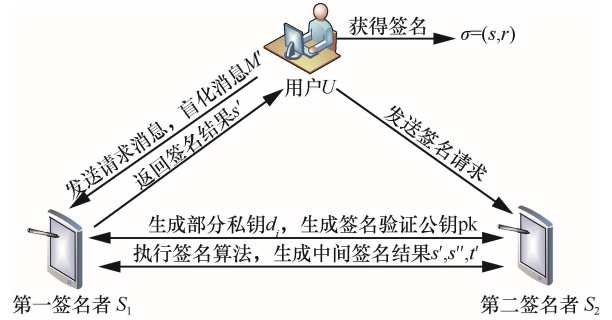


图 1 两方协作盲签名协议的系统模型
Figure 1 The model of two-party cooperative blind signature

2.2 协议设计

基于苏吟雪等^[20]两方协作 SM2 签名协议, 本文提出 SM2 的两方协作盲签名协议, 如图 2 所示。协议的具体执行过程如下。

1) 系统参数建立: 本阶段与 SM2 数字签名系统参数建立一致, 即输入安全参数 λ , 输出椭圆曲线系统参数 $\text{params} = \{E(F_q), P, n\}$ 。

2) 密钥生成: 本阶段由 S_1 和 S_2 参与执行, 给定系统参数 params , 执行以下步骤。

① S_1 随机选择一个秘密数 $d_1 \in Z_n^*$ 作为部分私钥, 计算部分公钥 $\text{pk}_1 = d_1 \cdot P$, 将 pk_1 发送给 S_2 。

② S_2 接收到 pk_1 , 随机选择一个秘密数 $d_2 \in Z_n^*$ 作为部分私钥, 计算部分公钥 $\text{pk}_2 = d_2 \cdot P$, 将 pk_2 发送给 S_1 , 计算验证公钥 $\text{pk} = d_2 \cdot \text{pk}_1 - P$ 。

③ S_1 接收到 pk_2 , 计算 $\text{pk} = d_1 \cdot \text{pk}_2 - P$, 并公布 pk 。

3) 盲签名生成: 本阶段由 U 、 S_1 和 S_2 参与执行, 假设 U 的待签名消息为 M , 执行以下步骤。

① S_1 随机选择 $k_1 \in Z_n^*$, 计算 $R_1 = k_1 \cdot P$, $R'_1 = k_1 \cdot \text{pk}_2$, 将 R_1 和 R'_1 发送给 S_2 。

② S_2 接收到 R_1 和 R'_1 , 计算并验证 $R'_1 = d_2 \cdot R_1$ 是否成立, 若不成立, 则中止协议, 否则随机选择 $k_2 \in Z_n^*$, 计算 $R_2 = k_2 \cdot P$, $R'_2 = k_2 \cdot \text{pk}_1$, 将 R_2 和 R'_2 发送给 S_1 。

③ S_1 接收到 R_2 和 R'_2 , 计算并验证

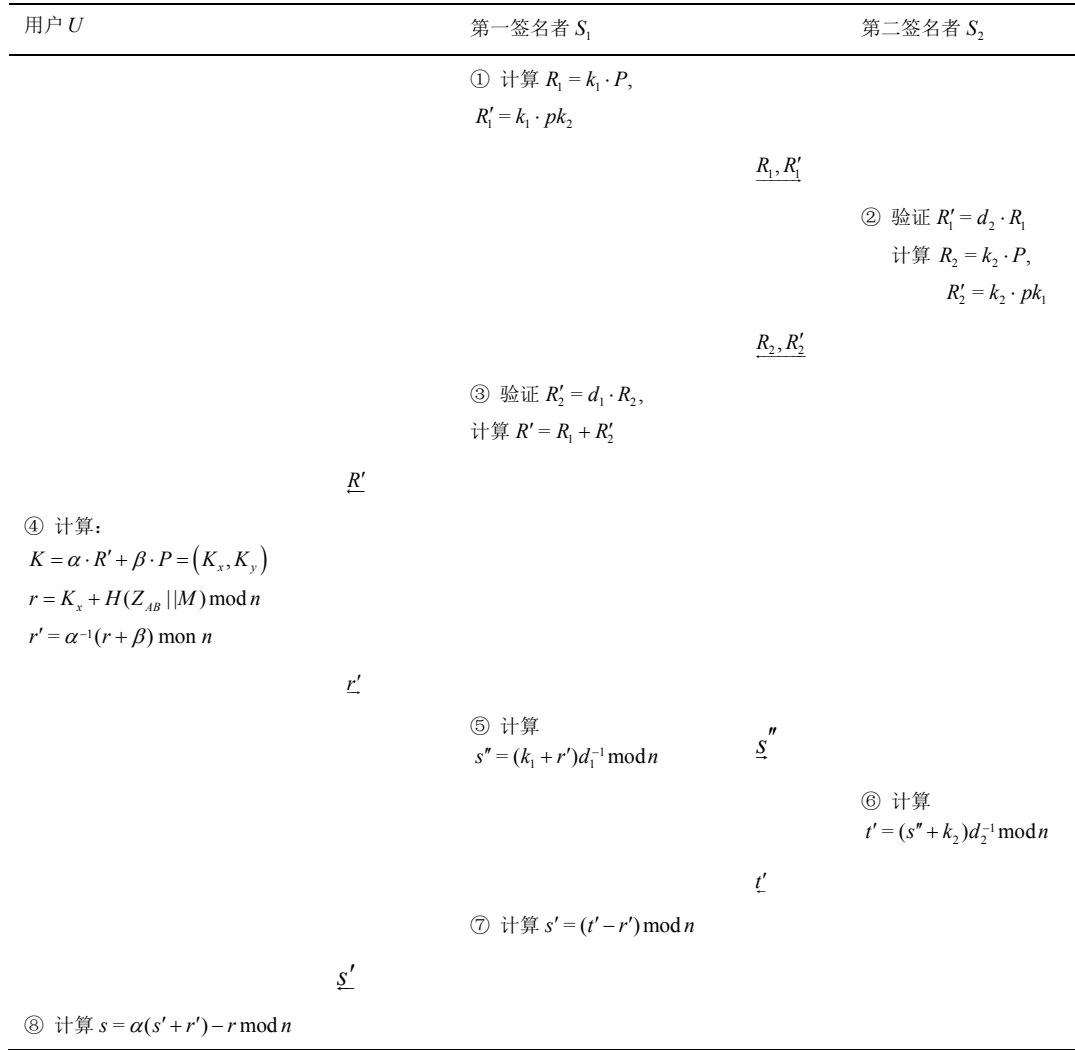


图2 基于 SM2 的两方协同盲签名协议
Figure 2 A two-party blind signature protocol based on SM2

$R'_2 = d_1 \cdot R_2$ 是否成立, 若不成立, 则中止协议, 否则计算 $R' = R_1 + R'_2$, 将 R' 发送给 U 。

④ U 接收到 R' , 随机选择 $\alpha, \beta \in Z_n^*$, 计算 $K = \alpha \cdot R' + \beta \cdot P = (K_x, K_y)$, 计算 $r = K_x + H(Z_{AB} || M) \bmod n$, $r' = \alpha^{-1}(r + \beta) \bmod n$, 若 $r = 0$ 或 $r' = 0$, 则重复步骤④。最后, 将 r' 发送给 S_1 , 其中 Z_{AB} 表示 S_1 和 S_2 身份标识的并接。

⑤ S_1 接收到 r' , 计算 $s'' = (k_1 + r')d_1^{-1} \bmod n$, 将 s'' 发送给 S_2 。

⑥ S_2 接收到 s'' , 计算 $t' = (s'' + k_2)d_2^{-1} \bmod n$, 将 t' 发送给 S_1 。

⑦ S_1 接收到 t' , 计算 $s' = (t' - r') \bmod n$, 将 s' 发送给 U 。

⑧ U 接收到 s' , 计算 $s = \alpha(s' + r') - r \bmod n$, 输出签名 $\sigma = (r, s)$ 。

4) 签名验证 (Verify): 本阶段与 SM2 数字签名验证一致。

协议分析: 在盲签名生成阶段的步骤①中, 计算 R'_1 是为了令 S_2 验证 S_1 是否诚实执行了协议, 并生成了随机秘密数 k_1 , 同理, 步骤②中计算 R_2 是为了令 S_1 验证 S_2 是否诚实执行了协议并生成了随机秘密数 k_2 , 以此保证中间消息的一致性。若 S_1 和 S_2 均能诚实地执行协议, 则无须检验中间信息的一致性, 可以进一步减少步骤①中 R'_1 和步骤②中 $d_2 \cdot R_1$ 、 R_2 以及步骤③中 $d_1 \cdot R_2$ 所涉及的 4 次标量乘法运算, 签名效率可进一步提高。

2.3 正确性分析

由密钥生成阶段可知:

$$pk = d_2 \cdot pk_1 - P = (d_1 d_2 - 1) \cdot P$$

由签名生成阶段可知:

$$\begin{aligned} s &= \alpha(s' + r') - r = \\ &\alpha(k_1 + \alpha^{-1}(r + \beta))d_1^{-1}d_2^{-1} + \alpha k_2 d_2^{-1} - r = \\ &(\alpha k_1 + r + \beta + \alpha k_2 d_1)d_1^{-1}d_2^{-1} - r = \\ &(\alpha(k_1 + k_2 d_1) + \beta + r)((d_1 d_2 - 1) + 1)^{-1} - r \end{aligned}$$

本协议的签名形式与 SM2 签名改进形式一致, 即 s 是私钥 $(d_1 d_2 - 1)$ 和随机数 $\alpha(k_1) + k_2 d_1 + \beta$ 对消息 M 的签名, 签名正确性得证。

3 安全性分析

3.1 安全模型定义

类似传统的盲签名方案, 协同盲签名方案应该同时满足不可伪造性和不可链接性(盲性)。在协同盲签名的系统模型中, 假设参与协议的 3 个实体都是诚实且好奇的参与者, 即用户、第一签名者和第二签名者都会按照协议的要求执行协议。在该假设下, 给出协同盲签名协议的不可伪造性和不可链接性的形式化定义。

定义 2 (不可伪造性)。给定一个协同盲签名协议 $\Pi = (\Pi_U, \Pi_{S_1}, \Pi_{S_2})$, 其中 U 、 S_1 和 S_2 分别是协议的 3 个诚实参与者, Π_I 表示参与者 $I \in \{U, S_1, S_2\}$ 在协议中执行的过程。假设 $\mathcal{A}$ 是一个概率多项式时间攻击者, 并最多可能腐化一个诚实参与者 $I \in \{U, S_1, S_2\}$ 。通过如下攻击者与挑战者的攻击游戏, 定义协同盲签名协议的不可为伪造性攻击实验 $\text{Exp}_{(\mathcal{A}, \Pi)}^{\text{EU-CMA}}(\lambda)$ 。

1) 系统初始化: 挑战者运行协议的参数建立算法 $\text{Setup}(\lambda)$, 生成系统参数 params , 以及协同密钥生成算法 $\text{KeyGen}(\text{params})$ 生成第一签名者和第二签名的公私钥对 (pk_1, d_1) 和 (pk_2, d_2) 以及系统公钥 pk 。挑战者将系统参数 params 和公钥 pk_1 、 pk_2 、 pk 发送给攻击者。

2) 腐化询问: 攻击者选择一个腐化参与者 $I \in \{U, S_1, S_2\}$, 若 $I = S_1$ (或 $I = S_2$), 则挑战者将私钥 d_1 (或 d_2) 返回给攻击者; 若 $I = U$, 则挑战者不返回任何信息。

3) 签名询问与伪造: 攻击者可以同挑战者交互执行盲签名协议 m 次, 并输出 $m+1$ 个消息-签名 $(M_1, \sigma_1), \dots, (M_{m+1}, \sigma_{m+1})$ 。

4) 输出: 对于任意 $i, j \in \{1, \dots, m+1\}$, 若 $M_i \neq M_j$, $\text{Verify}(pk, M_i, \sigma_i) = 1$, 则返回 1, 否则返回 0。

在上述实验中, 若返回 1, 则代表攻击者通过 m 次协议交互, 得到了 $m+1$ 个合法签名, 即攻击者至少成功伪造了 1 个签名。攻击者在实验 $\text{Exp}_{(\mathcal{A}, \Pi)}^{\text{EU-CMA}}(\lambda)$ 中的成功概率定义为

$$\text{Adv}_{(\mathcal{A}, \Pi)}^{\text{EU-CMA}}(\lambda) = \Pr[\text{Exp}_{(\mathcal{A}, \Pi)}^{\text{EU-CMA}}(\lambda) = 1]$$

若概率 $\text{Adv}_{(\mathcal{A}, \Pi)}^{\text{EU-CMA}}(\lambda)$ 是可忽略的, 则称协同盲签名协议 Π 满足存在不可伪造性。

定义 3 (不可链接性)。给定一个协同盲签名协议 $\Pi = (\Pi_U, \Pi_{S_1}, \Pi_{S_2})$, 假设 $\mathcal{A}$ 是一个概率多项式时间攻击者, 并可以腐化第一签名者和第二签名者。通过如下攻击者与挑战者的攻击游戏, 定义协同盲签名协议的不可链接性攻击实验 $\text{Exp}_{(\mathcal{A}, \Pi)}^{\text{Unlink}}(\lambda)$ 。

1) 系统初始化: 挑战者运行协议的参数建立算法 $\text{Setup}(\lambda)$, 生成系统参数 params , 以及协同密钥生成算法 $\text{KeyGen}(\text{params})$ 生成第一签名者和第二签名的公私钥对 (pk_1, d_1) 和 (pk_2, d_2) 以及系统公钥 pk 。挑战者将系统参数 params 和公钥 pk_1 、 pk_2 、 pk 发送给攻击者。

2) 挑战阶段: 攻击者选择两个消息 M_0 和 M_1 发送给挑战者。挑战者随机选择一个比特 $b \in \{0, 1\}$, 通过与攻击者交互执行协作盲签名协议分别获得消息 M_b 和 M_{1-b} 的签名 (M_b, σ_b) 和 (M_{1-b}, σ_{1-b}) 发送给攻击者。

3) 猜测阶段: 攻击者最终输出一个比特 b' 作为对比特 b 的猜测结果。

4) 输出阶段: 若 $b' = b$, 则返回 1, 否则返回 0。定义攻击者在上述实验中成功的概率为

$$\text{Adv}_{(\mathcal{A}, \Pi)}^{\text{Unlink}}(\lambda) = \Pr[\text{Exp}_{(\mathcal{A}, \Pi)}^{\text{Unlink}}(\lambda) = 1] - \frac{1}{2}$$

若概率 $\text{Adv}_{(\mathcal{A}, \Pi)}^{\text{Unlink}}(\lambda)$ 是可忽略的, 则协同盲签名协议 Π 满足存在不可链接性(盲化性)。

3.2 安全性证明

定理 1 (不可伪造性)。设 $\mathcal{A}$ 是一个概率多

项式时间算法, 若 $\mathcal{A}$ 能够以概率 ϵ 成功攻击图 2 中两方协作盲签名协议的不可伪造性, 那么存在一个仿真算法 Sim 能够以至少 $\epsilon/(3e)$ 的概率成功攻击 SM2 签名算法的不可伪造性, 其中 e 是自然对数的底。

证明 为了给出定理 1 的证明, 假设协议的参与者 $I \in \{U, S_1, S_2\}$ 是诚实可信的。通过仿真算法模拟协议的执行过程, 使攻击者看到的协议运行环境与实际实验环境不可区分。

1) 系统参数: 仿真算法 Sim 随机猜测攻击者要攻击的参与者 $I \in \{U, S_1, S_2\}$ 。根据猜测结果, Sim 模拟构造协议的公开参数以及第一签名者和第二签名者的密钥, 具体过程如下。

① 仿真算法 Sim 请求 SM2 签名算法的挑战者获取系统参数 params 和一个挑战 SM2 公钥 pk^* 。

② 当 $I = S_1$ 时, Sim 随机选择 $d_1 \in Z_n^*$ 作为 S_1 的私钥并计算其公钥 $\text{pk}_1 = d_1 \cdot P$ 。令 S_2 的公钥为 $\text{pk}_2 = d_1^{-1}(\text{pk}^* + P)$ 。假设 SM2 的私钥为 d^* , 则 pk_2 对应的私钥为 $d_2 = d_1^{-1}(d^* + 1) \bmod n$ 。 d^* 是随机选取的, 所以 S_2 的公钥和私钥分布与实际选取方式一致。这里, Sim 并不知道 S_2 私钥的真实值。当 $I = S_2$ 时, 类似前一种情况, Sim 随机选择 $d_2 \in Z_n^*$ 并计算 $\text{pk}_2 = d_2 \cdot P$ 作为 S_2 的私钥和公钥。同时, Sim 计算 $\text{pk}_1 = d_2^{-1}(\text{pk}^* + P)$ 作为 S_1 的公钥。当 $I = U$ 时, Sim 可以按照第一种或第二种情况设置第一签名者和第二签名者的密钥。

③ Sim 将系统参数 params 和公钥 pk_1 、 pk_2 、 pk^* 发送给挑战者。

2) 腐化询问: 攻击者选择一个腐化对象 I' 。

若 $I' \neq I$, 则 Sim 终止游戏; 否则, Sim 将相应的部分签名私钥发送给攻击者。

由 Sim 选取系统参数和公钥的方式, 可知该过程与不可伪造性实验初始化系统的方式是一致的, 并且该过程与攻击者的视角完全独立。因此, Sim 猜对攻击者腐化对象的概率, 即 $I' = I$ 的概率至少为 $1/3$ 。

3) 签名询问与伪造: 根据 I' 的不同情况, 分别讨论 Sim 仿真协议的执行过程。

① 当 $I' = S_1$ 时, 对于攻击者的任意签名询问 M_i , 仿真算法 Sim 模拟第二签名者和用户与攻

击者进行协议交互。首先, Sim 询问 SM2 签名算法的挑战者, 获取消息 M_i 的签名 $\sigma_i = (r_i, s_i)$ 。利用签名 σ_i 计算临时(随机)群元素 $R_i = s_i \cdot P + (r_i + s_i) \cdot \text{PK}$ 。

当 Sim 收到攻击者发送的信息 R_i 和 R'_i 后, Sim 随机选择 $\alpha, \beta \in Z_n^*$ 并计算

$$\begin{aligned} R'_2 &= \alpha^{-1}(R_i - \beta \cdot P) - R_1 \\ R_2 &= d_1^{-1} \cdot R'_2 \end{aligned}$$

由 R_i 的随机性可知, R_2 和 R'_2 通过实际协议中随机选择 $k_2 \in Z_n^*$, 计算 $R_2 = k_2 \cdot P$, $R'_2 = k_2 \cdot \text{pk}_1$ 的分布完全一致, 且 k_2 等价于 $k_2 = \alpha^{-1} \cdot (s_i + (r_i + s_i) \cdot d^* - \beta) - k_1 \bmod n$ 。 Sim 将 R_2 和 R'_2 发送给攻击者。

当 Sim 收到 R' 后, 计算

$$K = \alpha \cdot R' + \beta \cdot P = (K_x, K_y)$$

若攻击者正确地计算 $R' = R_1 + R'_2$, 由 R'_2 的选取方式可知

$$K = R_i$$

$$r = K_x + H(Z_{AB} || M_i) \bmod n = r_i$$

Sim 计算 $r' = \alpha^{-1}(r + \beta) \bmod n$, 将 r' 发送给攻击者。

当 Sim 收到攻击者发送的信息 s'' 后, 计算 $t' = \alpha^{-1} \cdot (s_i + r) \bmod n$, 将 t' 发送给攻击者。由 k_2 和 d_2 的形式可知, t' 与通过 $(s'' + k_2) d_2^{-1} \bmod n$ 计算的结果一致。

当 Sim 收到 s' 后, 计算

$$s = \alpha \cdot (s' + r') - r \bmod n$$

若攻击者正确地计算 s' , 即 $s' = t' - r'$, 则 $s = s_i$ 。

最后, Sim 将消息 M_i 的签名结果返回给攻击者。由于 $\sigma = (r, s) = (r_i, s_i)$, 所以 σ 是 M_i 的一个有效签名。

② 当 $I' = S_2$ 时, 对于攻击者的任意签名询问 M_i , 仿真算法 Sim 模拟第一签名者和用户与攻击者进行协议交互。同情况①一样, Sim 首先询问 SM2 签名算法的挑战者, 获取消息 M_i 的签名 $\sigma_i = (r_i, s_i)$ 。利用签名 σ_i 计算临时(随机)群元素 $R_i = s_i \cdot P + (r_i + s_i) \cdot \text{PK}$ 。

仿真算法随机选择 $k_1 \in Z_n^*$, 计算 $R_1 = k_1 \cdot P$, $R'_1 = k_1 \cdot \text{pk}_2$, 并将 R_1 和 R'_1 发送给攻击者。

当 Sim 收到攻击者发送的信息 R_2 和 R'_2 后, 将攻击者看作知识提取假设中的算法 T , 其输入为 (P, pk_1) , 输出为 $(k_2 \cdot P, k_2 \cdot \text{pk}_1)$ 。根据知识提取假设 KEA, 存在一个算法 T^* , 以 (P, pk_1) 为输入, 以 $(k_2, k_2 \cdot P, k_2 \cdot \text{pk}_1)$ 为输出, 从而得到 k_2 。若该过程失败, 则说明攻击者没有诚实地按照协议生成 R_2 和 R'_2 , Sim 终止实验, 否则, Sim 计算 $R' = R_1 + R'_2$, 随机选择 $\alpha \in Z_n^*$ 并令 $K = R_i$ 。这相当于随机选择了 $\beta \in Z_n^*$ 使得 $\beta \cdot P = K - \alpha \cdot R'$ 。由于 $K = (K_x, K_y) = \alpha \cdot R' + \beta \cdot P = R_i$, 所以

$$r = K_x + H(Z_{AB} || M_i) \bmod n = r_i$$

Sim 计算 $s'' = \alpha^{-1} \cdot d_2 \cdot (r_i + s_i) - k_2 \bmod n$ 并将 s'' 发送给攻击者。

当 Sim 收到攻击者发送的信息 t' 后, Sim 计算 $s = \alpha \cdot t' - r_i \bmod n$, 若攻击者正确地计算 t' , 则 $s = s_i \bmod n$ 。

最后, Sim 将消息 M_i 的签名结果返回给攻击者。由于 $\sigma = (r, s) = (r_i, s_i)$, 所以 σ 是 M_i 的一个有效签名。

③ 当 $I' = U$ 时, 按照情况①的方式构造第一签名者和第二签名者的公钥和私钥。Sim 知道第一签名者的私钥 d_1 , 但不用发送攻击者。同时, Sim 要与攻击者(即用户)交互模拟协议的签名过程。在诚实用户模型下, 将不可伪造性攻击实验的模型做如下改动: 当攻击者提出对消息 M_i 的签名请求时, 对于任意选定的 R_2 和 R'_2 , 以及 α 和 β , Sim 随机选择一个群元素 R , 并令

$$\begin{aligned} R_1 &= \alpha^{-1} (R - \beta \cdot P) - d_1 \cdot R_2 \\ R'_1 &= d_1 \cdot R_1 \end{aligned}$$

由 R 的随机性可知, R_1 和 R'_1 的分布与实际选取方式完全一样。因此, 在改动的实验模型中, 攻击者成功的概率与原始模型一致。

特别地, 当 Sim 通过询问 SM2 签名算法的挑战者获得消息 M_i 的签名 $\sigma_i = (r_i, s_i)$ 时, 若令 $R = s_i \cdot P + (r_i + s_i) \cdot \text{PK}$, 则 $R = k_i \cdot P$, 其中 k_i 是 SM2 签名算法选取的随机数。此时, 对于攻击者来说, R 依然是随机选取的。Sim 计算 $R' = R_1 + R'_2$ 并返回给攻击者。

当 Sim 收到攻击者的消息 r' 后, 计算 $s' = \alpha^{-1} \cdot (r_i + s_i) - r'$ 并返回给攻击者。

最终, 攻击者将获得消息 M_i 的签名 (r, s) 。由 R 的选取方式, 可得 $(r, s) = (r_i, s_i)$ 。

4) 输出: 若攻击者通过上述方式进行了 m 次协议询问, 输出 $m+1$ 个消息的合法签名 (M_i, σ_i) 且对于任意不同的 $i, j \in \{1, \dots, m+1\}$, $M_i \neq M_j$, 其中假设 $(M_1, \sigma_1), \dots, (M_m, \sigma_m)$ 是攻击者通过协议询问获取的合法消息-签名对, 则仿真算法 Sim 将 (M_{m+1}, σ_{m+1}) 返回给 SM2 签名算法的挑战者。

通过仿真算法 Sim 对实验环境的模拟过程可以看出, 若 Sim 在模拟过程中不终止游戏, 那么 Sim 将以与攻击者相同的概率成功伪造一个 SM2 签名。下面分析 Sim 终止游戏的事件及其概率。

令 E_1 表示事件“ $I' \neq I$ ”, E_2 表示事件“情况②中的知识提取算法运行失败”。令 $E = E_1 + E_2$ 。当事件 E 不发生时, Sim 成功输出一个伪造签名的概率与攻击者攻击协作盲签名协议成功的概率一样。由于 $\Pr[E_1] = 1/3$, $\Pr[E_2] = (1 - \epsilon_{\text{KEA}})^m$, 所以

$$\Pr[\bar{E}] = \Pr[\bar{E}_1 \cdot \bar{E}_2] \geq \frac{1}{3} \cdot (1 - \epsilon_{\text{KEA}})^m \approx \frac{1}{3e}$$

其中, e 为自然对数的底。由此, 可得

$$\begin{aligned} \Pr[\text{Sim成功}] &= \Pr[\text{Sim成功} \wedge E] + \\ &\Pr[\text{Sim成功} \wedge \bar{E}] \geq \\ &\Pr[\text{Sim成功} | \bar{E}] \cdot \Pr[\bar{E}] \geq \frac{1}{3e} \cdot \epsilon \end{aligned}$$

定理 1 证毕。

定理 2 (不可链接性)。图 2 中的两方协作盲签名协议满足不可链接性。

证明 假设攻击者按照协议的方式生成系统参数 params 、第一签名者和第二签名者的私钥 d_i 和公钥 $\text{pk}_i = d_i \cdot P$ ($i=0,1$), 以及系统公钥 $\text{pk} = (d_1 d_2 - 1) \cdot P$ 。令 $d = d_1 d_2 - 1$ 。攻击者选择两个消息 M_0 和 M_1 发送发给挑战者后, 挑战者通过与攻击者交互执行协作盲签名协议, 获取消息 M_0 和 M_1 的两组签名, 记作

$$(M_0, r[0], s[0]) \text{ 和 } (M_1, r[1], s[1])$$

在签名过程中, 攻击者能够获得的两组临时

信息为 $(R'[0], r'[0], s'[0])$ 和 $(R'[1], r'[1], s'[1])$ 。

根据协议, 若 (R', r', s') 是协议生成签名 (M, r, s) 时产生的临时信息, 则应存在 α 和 β , 满足

$$\begin{cases} r = r' \cdot \alpha - \beta \bmod n \\ s = s' \cdot \alpha + \beta \bmod n \end{cases} \quad (1)$$

$$s \cdot P + (r + s) \cdot \text{pk} = \alpha \cdot R' + \beta \cdot P \quad (2)$$

为了证明协议满足不可链接性, 只需要证明, 对于任意的合法签名 (M, r, s) 及临时信息 (R', r', s')

$$\begin{aligned} (M, r, s) &\in \{(M_0, r[0], s[0]), (M_1, r[1], s[1])\} \\ (R', r', s') &\in \{(R'[0], r'[0], s'[0]), (R'[1], r'[1], s'[1])\} \end{aligned}$$

都存在 α 和 β , 使得方程(1)和方程(2)同时成立。

根据协议, 由于 $r[b] + s[b] \neq 0$ 且 $\alpha[b] \neq 0$, 所以 $r'[b] + s'[b] \neq 0$ 。因此, 方程(1)中的系数组成的行列式值不为零, 即 $r'[b] + s'[b] \neq 0$ 。故, 对于任意的合法签名 (M, r, s) 及临时信息 (R', r', s') , 方程(1)都存在一组解 α 和 β 。下面分两种情况证明 α 和 β 同时满足方程(2)。

1) (R', r', s') 本来就是合法签名 (M, r, s) 的临时信息, 根据协议的正确性, 从方程(1)中计算出来的 α 和 β 显然满足等式(2)。

2) (R', r', s') 不是合法签名 (M, r, s) 的临时信息, 不妨假设

$$(M, r, s) = (M_0, r[0], s[0])$$

$$(R', r', s') = (R'[1], r'[1], s'[1])$$

根据方程(1)得

$$\alpha = \frac{r[0] + s[0]}{r'[1] + s'[1]} \bmod n$$

$$\beta = \frac{r[0] + s[0]}{r'[1] + s'[1]} \cdot r'[1] - r[0] \bmod n$$

令 $\alpha[1]$ 和 $\beta[1]$ 为签名 $(M_1, r[1], s[1])$ 生成过程中用户选取的两个临时随机数, 则

$$\alpha[1] \cdot R'[1] + \beta[1] \cdot P = s[1] \cdot P + (r[1] + s[1]) \cdot \text{pk}$$

由此可知

$$R'[1] = \frac{s[1] + (r[1] + s[1]) \cdot d - \beta[1]}{\alpha[1]} \cdot P$$

将 α 、 β 和 $R'[1]$ 的取值代入式 $\alpha \cdot R'[1] + \beta \cdot P$ 中, 可得

$$\begin{aligned} \alpha \cdot R'[1] + \beta \cdot P &= \left(\frac{r[0] + s[0]}{r'[1] + s'[1]} \cdot \frac{s[1] + (r[1] + s[1]) \cdot d - \beta[1]}{\alpha[1]} \right) \cdot P + \\ &\left(\frac{r[0] + s[0]}{r'[1] + s'[1]} \cdot r'[1] - r[0] \right) \cdot P \end{aligned}$$

由于 $r[1]$ 和 $s[1]$ 满足如下形式

$$r[1] = \alpha[1] \cdot r'[1] - \beta[1]$$

$$s[1] = \alpha[1] \cdot s'[1] + \beta[1]$$

所以

$$\begin{aligned} \alpha \cdot R'[1] + \beta \cdot P &= \left(\frac{r[0] + s[0]}{r'[1] + s'[1]} \cdot \frac{s'[1] + (r'[1] + s'[1]) \cdot d}{1} \right) \cdot P + \\ &\left(\frac{r[0] + s[0]}{r'[1] + s'[1]} \cdot r'[1] - r[0] \right) \cdot P = \\ &(s[0] + (r[0] + s[0]) \cdot d) \cdot P = \\ &s[0] \cdot P + (r[0] + s[0]) \cdot \text{pk} \end{aligned}$$

因此, 对于情况 2), α 和 β 依然满足等式(2)。

通过上述分析可见: 攻击者掌握的两组临时信息 $(R'[0], r'[0], s'[0])$ 和 $(R'[1], r'[1], s'[1])$ 与任意一组合法签名 $(M_b, r[b], s[b])$ 都是完美匹配的。因此, 攻击者从掌握的临时信息中无法关联到用户的实际签名信息。

定理 2 证毕。

4 性能分析

本节主要对第 2 节提出的两方协作盲签名协议进行性能评估, 理论分析了协议执行过程中的主要计算开销, 并对协议进行了实验评测。

为全面评估协议性能, 选取何德彪等^[24]基于 Paillier 同态加密技术的 SM2 盲签名方案以及 Zhang 等^[25]设计的轻量级的 SM2 盲签名方案作为对比, 为保持形式一致, 令其中的用户表示为 U ,

签名者表示为 S_1 。

表 1 统计了各个协议在盲签名阶段运行过程中用户 U 、第一签名者 S_1 和第二签名者 S_2 的理论计算开销。表 2 列出了各个协议的安全性对比。其中, Ha 表示执行一次哈希运算, Mul 表示执行一次椭圆曲线上的标量乘运算, Inv 表示执行一次大整数求逆运算, Eh 表示执行一次 Paillier 加密运算, Dh 表示执行一次 Paillier 解密运算, Exp 表示执行一次 Paillier 同态乘运算。

表 1 理论计算开销
Table 1 Theoretical computational overhead

方案	U	S_1	S_2
何德彪等 ^[24]	1Mul+2Eh+1Dh+1Ha	1Mul+2Exp+1Inv	—
Zhang 等 ^[25]	2Mul+1Ha+1Inv	1Mul+1Inv	—
本文协议	2Mul+1Ha+1Inv	3Mul+1Inv	3Mul+1Inv
本文协议 (无须验证)	2Mul+1Ha+1Inv	1Mul+1Inv	1Mul+1Inv

表 2 协议的安全性对比
Table 2 Comparison of protocol security

方案	消息盲化	两方协作	存在性不可伪造
何德彪等 ^[24]	√	×	√
Zhang 等 ^[25]	√	×	√
本文协议	√	√	√
本文协议 (无须验证)	√	√	√

综合表 1、表 2 可以看出, 理论上本文协议中 S_1 和 S_2 承担的计算开销基本相等, 签名阶段用户的计算开销较小。本文协议在满足消息盲化的同时实现了两方协作签名的功能。

对用户而言, 本协议无须同态加密的协助, 比何德彪等方案减少了 2 次 Paillier 加密运算和 1 次 Paillier 解密运算, 本文协议与 Zhang 等方案的用户开销基本一致。

对签名者而言, 本文协议由于增加了一个签名者, 因此与何德彪等和 Zhang 等方案相比, 各个签名者需要多计算 2 次椭圆曲线上的标量乘运算, 但与何德彪等方案相比本文协议无须 Paillier 同态乘法计算, 并且协议在实现协作签名的同时, 确保了签名消息的隐私性。此外, 考虑不同环境下的安全需求, S_1 和 S_2 诚实执行协议时无须验证

对方随机数的正确性, 签名者只需计算 1 次开销较大的椭圆曲线上的标量乘运算。

为了更系统地评估协议中 U 、 S_1 和 S_2 的执行效率, 本文使用 C 语言调用 Miracl 密码库在一台 PC 端进行仿真测试, 主要环境如下。

操作系统: 64 位 Windows10 家庭中文版。

中央处理器: Intel i5-8250 @ 1.6 GHz。

硬盘: 1 T。

内存: 8 GB。

实验中采用“GM/T 003.5-2012”标准中附录 A 推荐的椭圆曲线参数作为系统参数, 采用国密 SM3 密码杂凑算法作为协议中的安全哈希函数。

对于固定 414 B 大小的消息, 本文将协议运行 1 000 次取平均值, 测试了协议各个阶段运行时间, 对比如表 3 所示。

表 3 协议各个阶段运行时间对比
Table 3 Comparison of running time for each phase

单位: ms

方案	密钥生成	盲签名			验证
		U	S_1	S_2	
何德彪等 ^[24]	355.97	573.98	77.76	—	22.26
Zhang 等 ^[25]	9.44	12.70	8.98	—	21.05
本文协议	24.62	12.50	26.55	26.64	19.68
本文协议 (无须验证)	25.10	12.98	8.98	8.93	21.33

在密钥生成阶段, 何德彪等方案的密钥生成过程与标准 SM2 相同, 本协议需要预先进行密钥协商, 在该阶段的耗时为 24.62 ms, 但与何德彪等方案相比, 本协议无须生成 Paillier 密钥, 可节省约 331.35 ms 的时间成本; 在盲签名阶段, 由表 3 盲签名一栏中各个实体的耗时求和可得, 何德彪等方案的签名耗时为 651.74 ms, Zhang 等方案的签名耗时为 21.68 ms, 本文协议的签名耗时为 65.69 ms。本文协议无须 Paillier 同态加密协助, 较何德彪等方案节省 586.05 ms 的时间成本。在无须一致性检验的情况下, 本协议的签名耗时为 30.89 ms, 可在原设计的基础上进一步减少约 35 ms 的时间损耗, 并且本文协议在盲签名基础上增加实现了协作签名功能, 同时, 协议各个实

体在本地的耗时与 Zhang 等设计的轻量级 SM2 盲签名的耗时基本一致; 在签名验证阶段, 何德彪等和 Zhang 等方案均使用原 SM2 签名验证公钥进行验证, 本文协议使用协商的密钥进行验证, 验证算法均与标准 SM2 验证算法一致, 表 3 中签名验证的耗时受系统运行影响略有差异, 但整体与 SM2 验证耗时相近, 协议具有良好的兼容性和一定的实用性。

此外, 本文进一步评测了盲签名生成阶段的运行时间, 如图 3 所示, 其中, $step_i$ 表示执行盲签名生成阶段的第 i 步, 分别对应图 2 中的各个步骤。对比可看出, U 执行第④步和第⑧步操作, 共耗时 12.504 ms, S_1 执行第①、③、⑤、⑦步操作, 共耗时 26.551 ms, S_2 执行第②步和第⑥步操作, 共耗时 26.64 ms, 用户计算开销最小, 各阶段运行耗时与理论分析一致。

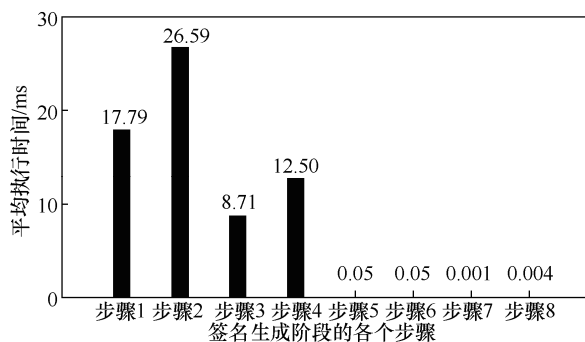


图3 签名阶段运行时间
Figure 3 Time costs of signing phase

图4是 SM2 数字签名算法与两方协作盲签名算法分别对长度为 1 B、1 KB、10 KB、100 KB 和 1 MB 消息进行签名的效率对比, 可以看出, 签署长度在 1 B 至 100 KB 范围内的消息对签名效率的影响不显著, 签署长度超过 100 KB 时, 签名耗时增加幅度较大, 主要与哈希函数压缩不同大小消息所消耗的时间有关。如表 4 所示, 对于 1 MB 大小的消息, SM2 签名运行时间 119.38 ms, 两方协作签名运行时间 176.56 ms, 二者运行时间变化趋势一致, 符合理论分析。

进一步地, 在诚实通信的前提下, 签名者无须进行验证运算, 如 2.2 节协议分析所述, 每次执行协作盲签名可减少 4 次耗时较大的点乘运算, 效率可得到进一步的提高。

表4 运行时间对比
Table 4 Comparison of running time

单位: ms

算法	1 B	1 KB	10 KB	100 KB	1 MB
SM2	10.76	10.83	12.68	21.06	119.38
Ours	65.37	68.67	67.05	76.52	176.56

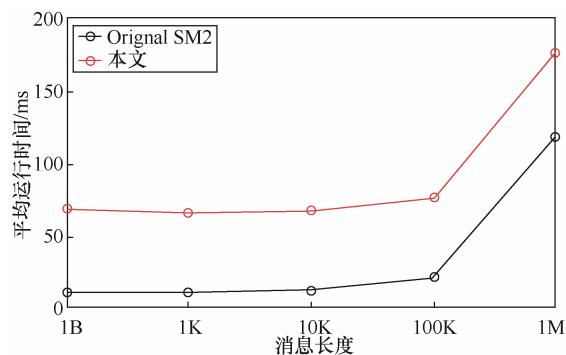


图4 签署不同长度消息的运行时间对比
Figure 4 Time costs for signing messages of different sizes

5 结束语

针对 SM2 数字签名的消息隐私保护和密钥安全问题, 本文提出一种基于 SM2 的两方协作盲签名协议, 通过传统盲签名系统中增添签名参与者的方式, 一方面将密钥分散存储, 提升密钥的安全性, 另一方面签名者均无法预知待签名消息内容, 实现了两方分布式环境中的协同盲签名操作。实验表明, 系统中各个参与者在本地运行耗时均在可承受范围内, 协议具备一定的实用性。

参考文献:

- [1] 国家密码管理局. GM/T2003—2012 SM2 椭圆曲线公钥密码算法[S]. 北京: 中国标准出版社, 2010.
State Cryptography Administration. GM/T2003—2012 public key cryptographic algorithm SM2 based on elliptic curves [S]. Beijing: Standards Press of China, 2010.
- [2] 冯泽宇, 巩博儒, 赵运磊. 基于离散对数的数字签名标准对比研究[J]. 计算机工程, 2016, 42(1): 145-149.
FENG Z Y, GONG B R, ZHAO Y L. Comparative study of digital signature standards based on discrete logarithm[J]. Computer Engineering, 2016, 42(1): 145-149.
- [3] 贾冀芳, 张立新, 廖明耀. 基于 OpenSSL 的 SM2 与 RSA 自动切换算法的设计[J]. 计算机工程与应用, 2018, 54(3): 74-81.
JIA J F, ZHANG L X, LIAO M Y. Design of automatic switching algorithm between SM2 and RSA based on OpenSSL[J]. Computer

- Engineering and Applications, 2018, 54(3): 74-81.
- [4] TIAN H B, SU Y X, LIANG Z Q. A provable secure server friendly two-party SM2 signing protocol for blockchain IoT[C]//2019 IEEE Globecom Workshops (GC Wkshps). 2019: 1-5.
- [5] LI W, LI R, WU K, et al. Design and implementation of an SM2-based security authentication scheme with the key agreement for smart grid communications[J]. IEEE Access, 2018, 6:71194-71207.
- [6] LONG Y H, CHENG M Y. Secret sharing based SM2 digital signature generation using homomorphic encryption[C]//2019 15th International Conference on Computational Intelligence and Security (CIS). 2019: 252-256.
- [7] 涂彬彬, 陈宇. 门限密码系统综述[J]. 密码学报, 2020, 7(1):1-14.
- TU B B, CHEN Y. A survey of threshold cryptosystems[J]. Journal of Cryptologic Research, 2020, 7(1): 1-14.
- [8] CHAUM D. Blind signatures for untraceable payments[C]// Advances in Cryptology. 1983: 199-203.
- [9] KREMER S, RYAN M, SMYTH B. Election verifiability in electronic voting protocols[C]//European Symposium on Research in Computer Security. 2010: 389-404.
- [10] CUI H D, QIN X R, CAI C L, et al. Security on SM2 and GOST signatures against related key attacks[C]//2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). 2021: 155-163.
- [11] SHAMIR A. How to share a secret[J]. Communications of the ACM, 1979, 22(11): 612-613.
- [12] PAILLIER P. Public-key cryptosystems based on composite degree residuosity classes[C]//Advances in Cryptology - EUROCRYPT '99, International Conference on the Theory and Application of Cryptographic Techniques. 1999:223-238.
- [13] 涂彬彬, 王现方, 张立廷. 两种分布式 SM2/9 算法应用[J]. 密码学报, 2020, 7(6): 826-838.
- TU B B, WANG X F, ZHANG L T. Two distributed applications of SM2 and SM9[J]. Journal of Cryptologic Research, 2020, 7(6): 826-838.
- [14] 尚铭, 马原, 林璟铨, 等. SM2 椭圆曲线门限密码算法[J]. 密码学报, 2014, 1(2): 155-166.
- SHANG M, MA Y, LIN J Q, et al. A threshold scheme for SM2 elliptic curve cryptographic algorithm[J]. Journal of Cryptologic Research, 2014, 1(2): 155-166.
- [15] YAN J, LU Y, CHEN L Y, et al. A SM2 elliptic curve threshold signature scheme without a trusted center[J]. KSII Transactions on International and Information Systems. 2016, 2(10): 897-913.
- [16] DING F, LONG Y H, WU P L. Study on secret sharing for SM2 digital signature and its application[C]//2018 14th International Conference on Computational Intelligence and Security (CIS). 2018: 205-209.
- [17] ZHANG Y D, HE D B, ZHANG M W, et al. A provable-secure and practical two-party distributed signing protocol for SM2 signature algorithm[J]. Frontiers of Computer Science, 2020, 14(3): 1-14.
- [18] 侯红霞, 杨波, 张丽娜, 等. 安全的两方协作 SM2 签名算法[J]. 电子学报, 2020, 48(1): 1-8.
- HOU H X, YANG B, ZHANG L N, et al. Secure two-party SM2 signature algorithm[J]. Acta Electronica Sinica, 2019, 48(1): 1-8.
- [19] 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.
- FENG Q, HE D B, LOU M, et al. Efficient two-party SM2 signing protocol for mobile internet[J]. Journal of Computer Research and Development, 2020, 57(10): 2136-2146.
- [20] 苏吟雪, 田海博. 基于 SM2 的双方共同签名协议及其应用[J]. 计算机学报, 2020, 43(4): 701-710.
- SU Y X, TIAN H B. A two-party SM2 signing protocol and its application[J]. Chinese Journal of Computers, 2020, 43(4): 701-710.
- [21] TANG G, ZHANG Z. Two-party signing for ISO/IEC digital signature standards[J]. The Computer Journal, 2022: 1-15.
- [22] RÜCKERT M. Lattice-based blind signatures[C]//International Conference on the Theory and Application of Cryptology and Information Security. 2010: 413-430.
- [23] HE D B, CHEN J H, ZHANG R. An efficient identity-based blind signature scheme without bilinear pairings[J]. Computers & Electrical Engineering, 2011, 37(4): 444-450.
- [24] 何德彪, 张韵茹, 谢翔, 等. 盲签名的获取方法、装置和服务器. 中国专利[P]. CN109818730A, 2019-03-06.
- HE D B, ZHANG Y R, XIE X, et al. Method and system for generating blind signature[P]. CN 109818730A, 2019-03-16.
- [25] ZHANG Y D, HE D B, ZHANG F G, et al. An efficient blind signature scheme based on SM2 signature algorithm[C]// International Conference on Information Security and Cryptology. 2020: 368-384.
- [26] 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.
- [27] ZHANG Z F, YANG K, ZHANG J, et al. Security of the SM2 signature scheme against generalized key substitution attacks[C]// International Conference on Research in Security Standardisation. 2015: 140-153.
- [28] SHOUP V. Lower bounds for discrete logarithms and related problems[C]//International Conference on the Theory and Applications of Cryptographic Techniques. 1997: 256-266.
- [29] DAMGÅRD I. Towards practical public key systems secure against chosen ciphertext attacks[C]//Annual International Cryptology Conference. 1991: 445-456.

[作者简介]



白雪（1996- ），女，陕西榆林人，西安邮电大学硕士生，主要研究方向为国密算法、公钥密码学。



郭瑞（1984- ），男，河南洛阳人，西安邮电大学副教授，主要研究方向为区块链安全。



秦宝东（1982- ），男，江苏徐州人，西安邮电大学教授，主要研究方向为公钥密码学。



郑东（1964- ），男，山西翼城人，西安邮电大学教授、博士生导师，主要研究方向为信息安全。