

基于区块链与国密 SM9 的抗恶意 KGC 无证书签名方案

唐飞¹, 甘宁¹, 阳祥贵², 王金洋¹

(1. 重庆邮电大学网络空间安全与信息法学院, 重庆 400065; 2. 江西昌河航空工业有限公司工程技术部, 江西 景德镇 333002)

摘要: 无证书密码体制能同时解决证书管理和密钥托管问题, 但其安全模型中总是假设 Type II 敌手 (恶意密钥生成中心 (KGC)) 不会发起公钥替换攻击, 这一安全性假设在现实应用中具有一定的局限性。国密 SM9 签名方案是一种高效的标识密码方案, 它采用了安全性好、运算速率高的 R-ate 双线性对, 但需要 KGC 为用户生成和管理密钥, 存在密钥托管问题。针对以上问题, 基于区块链和国密 SM9 签名方案提出一种抗恶意 KGC 无证书签名方案。所提方案基于区块链的去中心化、不易篡改等特性, 使用智能合约将用户秘密值对应的部分公钥记录在区块链上, 在验签阶段, 验证者通过调用智能合约查询用户公钥, 从而保证用户公钥的真实性。用户私钥由 KGC 生成的部分私钥和用户自己随机选取的秘密值构成, 用户仅在首次获取私钥时由 KGC 为其生成部分私钥来对其身份标识符背书。随后可以通过更改秘密值及其存证于区块链的部分公钥实现私钥的自主更新, 在此过程中身份标识保持不变的, 为去中心化应用场景提供密钥管理解决方法。区块链依靠共识机制来保证分布式数据的一致性, 用户部分公钥的变更日志存储在区块链中, 基于区块链的可追溯性, 可对恶意公钥替换攻击行为进行溯源, 从而防止恶意 KGC 发起替换公钥攻击。基于实验仿真和安全性证明结果, 所提方案签名与验签的总开销仅需 7.4 ms, 与同类无证书签名方案相比, 所提方案能有效抵抗公钥替换攻击, 且具有较高的运算效率。

关键词: 无证书签名方案; 抗恶意 KGC; 区块链; SM9 签名

中图分类号: TP309

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2022073

Anti malicious KGC certificateless signature scheme based on blockchain and domestic cryptographic SM9

TANG Fei¹, GAN Ning¹, YANG Xianggui², WANG Jinyang¹

1. School of Cyber Security and Information Law, Chongqing University of Posts and Telecommunications, Chongqing 400065, China

2. Department of Engineering Technology, Jiangxi Changhe Aviation Industry CO.,LTD, Jingdezhen 333002, China

Abstract: The certificateless cryptosystem can solve the problems of certificate management and key escrow at the

收稿日期: 2022-07-20; 修回日期: 2022-09-30

通信作者: 唐飞, tangfei@cqupt.edu.cn

基金项目: 国防基础科研计划 (JCKY2020205C013)

Foundation Item: The National Defense Basic Research Program (JCKY2020205C013)

引用格式: 唐飞, 甘宁, 阳祥贵, 等. 基于区块链与国密 SM9 的抗恶意 KGC 无证书签名方案[J]. 网络与信息安全学报, 2022, 8(6): 9-19.

Citation Format: TANG F, GAN N, YANG X G, et al. Anti malicious KGC certificateless signature scheme based on blockchain and domestic cryptographic SM9[J]. Chinese Journal of Network and Information Security, 2022, 8(6): 9-19.

same time, but its security model always assumes that Type II adversary (named malicious KGC) will not launch public key replacement attacks. This security assumption has certain limitations in real-world applications. As an efficient identity-based cryptographic scheme, SM9 signature scheme adopts R-ate bilinear pairing which has good security and high computational efficiency. However, it requires KGC to generate and manage keys for users, so it has the problem of key escrow. In view of the above problems, a certificateless signature scheme against malicious KGC was constructed based on blockchain and SM9 signature algorithm. Based on the properties of decentralization and tamper-proof of blockchain, the proposed scheme used the smart contract to record part of the public key corresponding to the user's secret value on the blockchain. Then, the verifier can revoke the smart contract to query the user's public key during the signature verification stage. Therefore, the proposed scheme ensured the authenticity of the user's public key. The user's private key consisted of the partial private key generated by KGC and a secret randomly chosen by the user. The user required the partial private key generated by KGC to endorse his identity identifier when the user generates the private key for the first time. Subsequently, the private key can be independently updated by changing the secret and the corresponding partial public key. During this process, the identity remains unchanged, which provided a viable solution for key management in decentralized application scenarios. The blockchain relied on the consensus mechanism to ensure the consistency of the distributed data. Based on the traceability of the blockchain, the change log of user's partial public key was stored in the blockchain, which can trace the source of malicious public key replacement attacks and thereby prevent malicious KGC from launching public key replacement attacks. According to the experimental simulation and security proof results, the total overhead of signature and verification of the proposed scheme is only 7.4ms. Compared with similar certificateless signature schemes, the proposed scheme can effectively resist public key replacement attacks and has higher computational efficiency.

Keywords: certificateless signature, anti malicious KGC, blockchain, SM9 signature

0 引言

数字签名具有不可伪造、不可否认和保护消息完整性等特点, 可对数据内容的完整性和数据源的真实性进行检测, 是保证数据安全的核心技术之一, 在电子政务、电子商务、数字化医疗等领域有广泛用途。传统数字签名需要证书机构 (CA, certification authority) 为用户公钥颁发证书, 以确保公钥的真实性, 从而存在复杂的公钥证书管理问题。基于身份的签名方案将密钥生成中心 (KGC, key generation center) 视为可信中心, 虽然解决了证书管理的问题, 但存在单点故障和密钥托管问题。

Al-Riyami 等^[1]在 2003 年提出了由 KGC 和用户联合生成用户密钥的无证书公钥密码体制。无证书公钥密码体制能同时解决证书管理和密钥托管问题, 增强系统的安全性, 这使得它成为密码学研究的热点之一。夏峰等^[2]提出一种公钥不可替换无证书签名方案; 王圣宝等^[3]提出一个无双

线性配对的无证书签名方案; 王亚飞等^[4]指出文献[3]提出的方案是不安全的并提出改进方案; 但樊爱宛等^[5]和李艳琼等^[6]对文献[4]进行分析后指出其所提方案难以抵抗恶意但被动的 KGC (MKGC, malicious-but-passive KGC) 攻击, 并针对此安全缺陷提出了新方案; 汤永利等^[7]给出针对文献[5]的公钥替换攻击的伪造流程, 并提出了 9 个新方案; 王菁等^[8]分析汤永利等^[7]提出的 9 个无证书签名方案, 发现其中 5 个签名方案不能抵抗公钥替换攻击。Hung 等^[9]设计了一个强不可伪造的无证书签名方案; 吴涛等^[10]指出文献[9]无法抵抗 MKGC 攻击, 并提出改进方案; 杨小东等^[11]发现文献[10]的方案不满足不可伪造性且不能抵抗 MKGC 攻击。文献[12]指出文献[13]中的无证书签名方案不安全, 并提出了一种抗 MKGC 攻击的安全无证书签名方案。

分析现有无证书方案不难发现, 用户私钥包括 KGC 生成的部分私钥和用户随机选取的秘密值。然而, 在实际应用中, 恶意 KGC 只需随机选取一个新的秘密值, 再结合先前为用户生成的

部分私钥,就能伪造出该用户的一对有效公私钥,这使得恶意 KGC 具备发起公钥替换攻击的能力。但是,在传统无证书公钥密码方案的安全模型中,总是假设 Type II 敌手(恶意 KGC)不会发起公钥替换攻击,这一安全性假设在现实应用中具有一定的局限性。针对无证书公钥密码这一局限性,文献[2,5,7,12]做了相关研究。文献[2]提出由 KGC 为用户公钥签名,只要同一个用户有两对有效公私钥,就能证明 KGC 是恶意的,但在无证书签名方案中,验证者并不能判断签名者当前是否拥有两个有效公钥。文献[5]采用公告板公示用户公钥,但这个公告板仅由 KGC 维护,所以 KGC 仍然可以更改用户公钥,这样并不能有效约束 KGC。文献[7]指出文献[5]的方案存在安全性问题并给出改进方案,但文献[7]提出的方案中用户公钥与 KGC 公钥间存在线性关系,普通敌手可通过消去 KGC 公钥来实现公钥替换攻击。文献[12]通过校验用户公钥信息的哈希值验证用户公钥的有效性,由于哈希值是公开计算的,恶意 KGC 能伪造出可以通过验证的用户公钥,所以并不能及时发现恶意 KGC 的攻击行为。上述分析表明,现有无证书签名方案不能及时发现并阻止恶意 KGC 的公钥替换攻击行为。

针对上述问题,本文主要工作如下。

- 1) 基于区块链技术和 SM9 标识密码算法^[14]提出了一个抗恶意 KGC 公钥替换攻击的签名方案。
- 2) 基于可证明安全理论,证明了所提方案在适应性选择消息和标识攻击模型下具有不可伪造性;基于区块链的不易篡改性,采用区块链存证用户部分公钥,保证用户公钥的真实性,并且能够及时发现恶意 KGC 的公钥替换攻击行为。
- 3) 实验结果表明,采用区块链存证用户部分公钥的本文方案是可行的,方案签名与验签总开销约为 7.4 ms;与同类无证书签名方案对比,所提方案能更好地抵抗恶意 KGC 发起的公钥替换攻击,且具有更高的计算效率和较短的签名长度。

1 预备知识

1.1 双线性对与复杂性假设

设 G_1 、 G_2 是阶为大素数 N 的加法循环群, P_1 、 P_2 是 G_1 、 G_2 的生成元。设 G_T 是阶为 N 的

乘法循环群,记其单位元为 1。若 $x \in Z_N$, $[x]P_i$ 代表 x 个生成元 P_i 相加,其中, $i \in \{1, 2\}$ 。

定义 1 如果一个二元函数 $e: G_1 \cdot G_2 \rightarrow G_T$ 是一个双线性对,则其满足如下性质。

- 1) 双线性性: 对 $\forall a, b \in Z_N$, 满足 $e([a]P_1, [b]P_2) = e([b]P_1, [a]P_2) = e(P_1, P_2)^{ab}$ 。
- 2) 非退化性: $\exists R \in G_1, Q \in G_2$, 使得 $e(R, Q) \neq 1$ 。
- 3) 可计算性: 对 $\forall R \in G_1, Q \in G_2$, 存在有效算法能高效计算双线性对 $e(R, Q)$ 。

假设 1 椭圆曲线离散对数 (ECDL) 问题: 给定椭圆曲线上的群 (G_1, P_1, N) , 随机选择 $R \in G_1$, 求出 $x \in Z_N$, 使之满足 $R = [x]P_1$, 其中 P_1 为 G_1 的生成元。

假设 2 强 Diffie-Hellman (q -SDH) 问题: 已知 $(G_1, G_2, G_T, P_1, P_2, N)$ 和正整数 q , 给定 $q+2$ 个元素 $(P, Q, [a]Q, [a^2]Q, \dots, [a^q]Q) \in G_1 \cdot G_2^{q+1}$, 其中 a 未知, 找到 $\left(c, \left[\frac{1}{c+a}\right]P\right)$, $c \in Z_N^*$ 。

若 ECDL 问题在多项式时间内可解的概率是可忽略的,则称 ECDL 假设成立;同理,若 q -SDH 问题在多项式时间内可解的概率是可忽略的,则称 q -SDH 假设成立。

1.2 国密 SM9

SM9^[14]是我国自主研发的标识密码即基于身份的密码 (IBC, identity-based cryptography), 于 2016 年被认定为国家商用密码行业标准 (GM/T0044—2016), 并于 2018 年 11 月纳入国际标准。两项国家标准 GB/T 38635.1—2020《信息安全技术 SM9 标识密码算法 第 1 部分: 总则》、GB/T 38635.2—2020《信息安全技术 SM9 标识密码算法 第 2 部分: 算法》于 2020 年正式发布。SM9 方案推荐采用的椭圆曲线方程为 $y^2 = x^3 + 5$, 其安全性建立在 q -SDH 假设成立的基础上。

作为基于身份的密码方案, SM9 受到越来越多的关注。近年来,国内学者基于 SM9 密码方案开展大量研究工作,证明了 SM9 签名具有 EUF-CMIA 安全性^[15], 基于 SM9 提出了聚合签名^[16]、可搜索加密^[17]、聚合签名^[18]、部分盲签名^[19]、环签名^[20]、可追踪属性签名^[21]以及群签名^[22]等方案,另外, SM9 广泛应用于区块链、电子邮件、物

联网、车联网和跨域协同等场景中的隐私保护^[23-24]、身份认证^[25-26]、密钥管理^[27-29]等方向。

1.3 无证书签名方案的形式化定义

无证书签名方案^[1]中用户完整密钥对 (sk_{ID}, pk_{ID}) 的结构如图 1 所示。

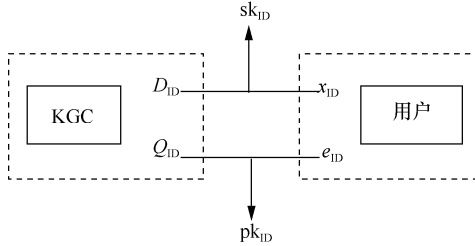


图 1 无证书密码方案中用户完整密钥对的结构
Figure 1 User complete key pair structure in certificateless signature scheme

一个无证书签名方案由以下 7 个算法构成。

1) $CL \cdot Setup(1^k)$: 给定安全参数 k , 初始化无证书密码系统, 并返回系统参数 pp 和主密钥对 (mpk, msk) 。系统参数包括消息空间 M 和签名空间 S 等。

2) $CL \cdot PartialPrivateKeyExtract(pp, msk, ID)$: 以 pp 、主密钥对 msk 和用户的标识符 ID 作为输入, 返回部分私钥 D_{ID} 和对应的部分公钥 Q_{ID} 。

3) $CL \cdot SetSecretValue(pp, ID)$: 以 pp 和用户的标识符 ID 作为输入, 输出用户的秘密值 x_{ID} 和对应的部分公钥 e_{ID} 。

4) $CL \cdot SetPrivateKey(D_{ID}, x_{ID})$: 以部分私钥 D_{ID} 和秘密值 x_{ID} 作为输入, 返回完整私钥 sk_{ID} 。

5) $CL \cdot SetPublicKey(pp, sk_{ID}, Q_{ID}, e_{ID})$: 以 pp 、完整私钥 sk_{ID} 、部分公钥 Q_{ID} 、 e_{ID} 作为输入, 并由此构造用户的完整公钥 pk_{ID} 。

6) $CL \cdot Sign(pp, m, sk_{ID})$: 以 pp 、待签名的消息 $m \in M$ 和私钥 sk_{ID} 作为输入, 输出签名 $s \in S$ 。

7) $CL \cdot Verify(pp, m, pk_{ID}, s)$: 以 pp 、消息 m 、公钥 pk_{ID} 、待验证签名 s 作为输入, 输出验签结果。

无证书签名算法对应的安全模型^[1]包括两个方面, 分别对应两类不同的攻击者。① 攻击者 $\mathcal{A}_I$ 是外部敌手, 他试图冒充被攻击者获得其秘密值和更换其公钥, 但他不知道系统主私钥。② 攻击者 $\mathcal{A}_{II}$ 是诚实且好奇的 KGC, 他试图在不留痕迹的情况下冒充某个被攻击者, 他知道系统主密钥

但不能更换任何用户的公钥。其中, 由敌手 $\mathcal{A}_I$ 发起的攻击被称为公钥替换攻击。无证书签名算法安全性可用以下两个攻击游戏来模拟。

(1) 游戏 1: 攻击者 $\mathcal{A}_I$

初始化: 挑战者运行初始化算法, 生成主密钥 msk 和系统参数 pp , 并将 pp 发送给 $\mathcal{A}_I$, 同时保存 msk 。

攻击: 挑战者模拟签名方案中算法, 应答 $\mathcal{A}_I$ 进行的用户公钥询问、部分私钥询问、秘密值询问、公钥替换询问、签名询问等。

伪造: $\mathcal{A}_I$ 输出 $(ID^*, P_{ID}^*, m^*, \sigma^*)$, 当输出满足以下 3 个条件时, 攻击者获胜。① σ^* 是公钥为 P_{ID}^* 的用户 ID^* 对消息 m^* 的有效签名; ② $\mathcal{A}_I$ 没有询问过 ID^* 的部分私钥; ③ $\mathcal{A}_I$ 没有询问过公钥为 P_{ID}^* 的用户 ID^* 对消息 m^* 的有效签名。

(2) 游戏 2: 攻击者 $\mathcal{A}_{II}$

初始化: 挑战者运行初始化算法, 生成主密钥 msk 和系统参数 pp , 并将 pp 和 msk 发给 $\mathcal{A}_{II}$ 。

攻击: 挑战者模拟签名方案中算法, 应答 $\mathcal{A}_{II}$ 进行的公钥询问、秘密值询问、签名询问等。由于 $\mathcal{A}_{II}$ 是不能进行公钥替换攻击的恶意 KGC, 可以计算用户部分私钥, 故用户部分私钥、公钥替换询问都无须进行。

伪造: $\mathcal{A}_{II}$ 输出 (ID^*, m^*, σ^*) , 当输出满足以下 3 个条件时, 攻击者获胜。① σ^* 是公钥为 P_{ID} 的用户 ID^* 对消息 m^* 的有效签名; ② $\mathcal{A}_{II}$ 没有询问过用户 ID^* 的秘密值或替换用户的公钥 P_{ID} ; ③ $\mathcal{A}_{II}$ 没有询问过用户 ID^* 对消息 m^* 的有效签名。

1.4 区块链

区块链是比特币的底层技术^[30], 以数据区块为单位存储数据, 每个区块中记录一批交易信息, 其本质是一个无中心的账本数据库。区块结构如图 2 所示。

区块链结合共识算法、密码学等相关技术, 能让分布式节点达成数据一致性共识, 使得账本信息不被恶意篡改。区块链具有去中心化、不易篡改、维护成本低、安全性强等特性, 适用于解决信任管理、可靠溯源与可信监管等问题。

1.5 KGC 信任等级

Girault^[31]在 1991 年把可信中心 (本文指

KGC) 划分为 3 个信任等级。

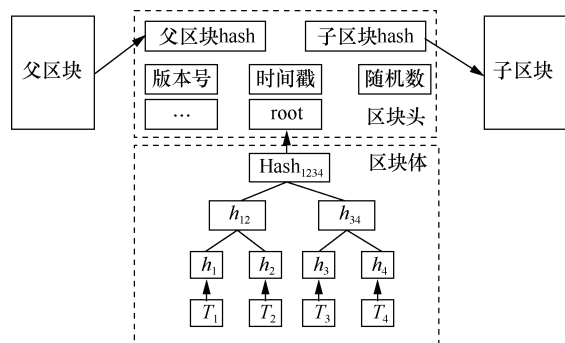


图2 区块结构
Figure 2 block structure

等级 1: KGC 知道任意合法用户的密钥, 即 KGC 可以伪造任意用户对任意消息的签名而不被发现。

等级 2: KGC 不知道任意合法用户的密钥, 但可以伪造出“合法”的假密钥, 且能使用假密钥伪造签名而不被发现。

等级 3: KGC 不知道任意合法用户的密钥, 且若 KGC 伪造密钥, 用户可以发现且提供证据证明该密钥是伪造的。

满足等级 3 的无证书签名方案意味着方案中的 KGC 不能通过改变为用户生成的部分私钥来模拟用户, 即 KGC 不能为同一个公钥提供不同的部分私钥。

2 抗恶意 KGC 无证书签名方案

2.1 基于区块链的无证书签名定义

基于区块链的 KGC 无证书签名方案由以下一系列算法构成。

$CL \cdot Setup(1^\lambda) \rightarrow pp$: 由 KGC 运行, 初始化系统参数与区块链系统参数。

$CL \cdot SetSecretValue(pp) \rightarrow (x, P_A)$: 由签名者执行, 选定秘密值 x , 并将秘密值证明 P_A 上链存证。

$CL \cdot PartialPrivateKeyExtract(pp, ks, id_A, P_A) \rightarrow D_A$: 由 KGC 与区块链联合执行, 为签名者生成部分私钥 D_A 。

$CL \cdot SetPrivateKey(D_A, x) \rightarrow ds_A$: 由签名者执行, 生成完整私钥 ds_A 。

$CL \cdot SetPublicKey(pp) \rightarrow id_A$: 由签名者执行,

公开其公钥 id_A 。

$CL \cdot Sign(pp, m, ds_A) \rightarrow \sigma$: 由签名者执行, 用私钥 ds_A 对消息 m 签名。

$CL \cdot Verify(pp, m, P_A, \sigma) \rightarrow 0/1$: 由验证者执行, 通过区块链校验 P_A 的有效性, 并验证签名 σ 的有效性, 输出 1 为有效, 输出 0 为无效。

本文考虑敌手 $\mathcal{A}$ 为能进行公钥替换攻击的恶意 KGC, 即敌手同时具备敌手 $\mathcal{A}_I$ 与敌手 $\mathcal{A}_{II}$ 的攻击能力, 也就是说, $\mathcal{A}$ 可以自适应地初始化系统参数, 且能在不被察觉的情况下替换被攻击者公钥, 但不能获得被攻击者的秘密值。由于用户公钥和区块链记录是公开的, 且 $\mathcal{A}$ 可以计算用户部分私钥, 所以攻击者 $\mathcal{A}$ 无须进行公钥询问、用户部分私钥询问等攻击过程。

攻击者 $\mathcal{A}$ 的攻击游戏模拟过程如下。

初始化: 挑战者运行初始化算法, 生成主密钥 msk 和系统参数 pp , 并将 pp 和 msk 发给 $\mathcal{A}$ 。

攻击: 挑战者模拟签名方案中算法, 应答 $\mathcal{A}$ 进行公钥替换询问、秘密值询问、公钥替换询问、签名询问等。

伪造: $\mathcal{A}$ 输出 (id^*, m^*, σ^*) , 当输出满足以下 3 个条件时, 攻击者获胜。① σ^* 是公钥为 P_{id^*} 的用户 id^* 对消息 m^* 的有效签名; ② $\mathcal{A}$ 没有询问过用户 id^* 的秘密值; ③ $\mathcal{A}$ 没有询问过用户 id^* 对消息 m^* 的有效签名。

2.2 方案构造

本节给出基于区块链与 SM9 的抗恶意 KGC 无证书签名方案的具体构造。方案设计采用 SM9 标识密码算法中的符号, 具体描述如下。

(1) $CL \cdot Setup(1^\lambda) \rightarrow pp$

1) 参数生成。给定安全参数 λ , KGC 首先选择一个双线性群 $BP = (G_1, G_2, G_T, e, N)$, $N > 2\lambda$ 。并选择群 G_1 和群 G_2 的生成元 P_1 和 P_2 。选定密码杂凑函数 $H_1(\{0,1\}^* \cdot N \rightarrow Z_N^*)$ 和 $H_2(\{0,1\}^* \cdot N \rightarrow Z_N^*)$ 。KGC 选择随机数 $ks \in [1, N-1]$ 作为系统主私钥, 计算群 G_2 中的元素 $P_{pub} = [ks]P_2$ 作为系统主公钥, 接着选择一个字节 hid 表示私钥生成函数识别符。系统公开参数 $pp = \{BP, P_1, P_2, P_{pub}, H_1, H_2, hid\}$ 。

2) 区块链系统初始化。先初始化区块链节点公私钥及区块链系统参数; 然后事先部署智能合

约——全局管理智能合约 (GMSC, global manage smart contract) 并将其作为区块链中的全局合约, 记录区块链中部署的智能合约, 包括身份记录智能合约 (IRSC, identity record smart contract)、身份查询智能合约 (IQSC, identity query smart contract), 从而实现上链和查询功能。智能合约框架如图 3 所示。

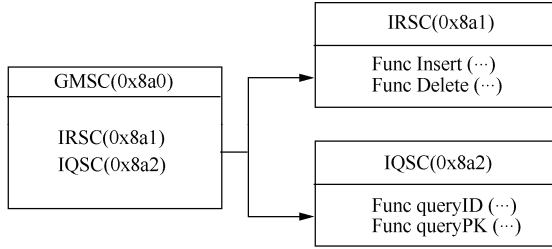


图 3 智能合约框架

Figure 3 Smart contract framework

(2) $CL \cdot SetSecretValue(pp, id_A) \rightarrow (ka, P_A)$

签名者 A 选择随机数 $ka \in [1, N-1]$ 作为用户秘密值, 计算 $P_A = [ka]P_2$ 作为用户秘密值证明, 将 (id_A, P_A) 发给区块链。

(3) $CL \cdot PartialPrivateKeyExtract(pp, ks, id_A, P_A) \rightarrow C_A$

部分私钥生成算法由区块链与 KGC 协作完成, 如算法 1 所示。首先, 区块链调用智能合约查询签名者 A 的标识符及其选定的用户秘密值证明当前是否在使用中, 若未在使用中, 将 (id_A, P_A) 发给 KGC; 然后, KGC 先校验用户标识符 id_A 是否有效, 若有效则为签名者 A 生成部分私钥, 再用 Elgamal 加密算法加密部分私钥, 并将部分私钥密文发给区块链; 最后, 区块链将用户秘密值证明上链, 将用户部分私钥密文 C_A 与秘密值证明上链状态 $status$ 反馈给签名者 A 。

算法 1 部分私钥生成

输入 (ks, id_A, P_A)

输出 $(C_A, status)$

执行智能合约:

- 1) **if** $IQSC(id_A) = P_A$ // P_A 在使用中
- 2) $status = 0$
- 3) **return** $(nil, status)$
- 4) **else** // P_A 未在使用中
- 5) $send(id_A, P_A)$ to KGC

6) **end if**

执行 KGC:

7) **if** $IdentityAuthentication(id_A) = \text{true}$

// id_A 为有效身份标识

8) $D_A = [H_1(id_A \parallel hid, N) + ks]^{-1} P_1$

9) $status = 1$

10) $C_A = ElgamalEnc(D_A)$ with P_A

11) $send(C_A, status)$ to Blockchain

12) **else** // id_A 为无效身份标识

13) $status = -1$

14) **end if**

执行智能合约:

15) **if** $status = 1$

16) $IRSC(P_A, id_A, status)$

17) **end if**

18) **return** $(C_A, status)$

(4) $CL \cdot SetPrivateKey(C_A, status, x_A) \rightarrow ds_A$

签名者 A 收到 $(C_A, status)$, 当 $status = -1$ 时, 返回算法 $CL \cdot SetSecretValue$; 当 $status = 0$ 时, 说明 id_A 在使用中, 无法生成关于 id_A 的密钥; 当 $status = 1$ 时, 签名者 A 用秘密值 ka 解密获得 D_A , 生成完整私钥 $ds_A = [ka]D_A$ 。

(5) $CL \cdot SetPublicKey(pp) \rightarrow id_A$

签名者 A 生成完整私钥后, 设置公钥为其身份标识 id_A 。

(6) $CL \cdot Sign(pp, m, ds_A) \rightarrow \sigma$

给定消息 m , 签名者 A 对其进行签名。具体步骤如下: 计算 $g = e(P_1, P_A)$; 随机选择 $r \in [1, N-1]$, 计算 $w = g^r$; 计算 $h = H_2(M \parallel w, N)$; 计算 $l = (r - h) \bmod N$, 若 $l = 0$, 则重新选取随机数 r ; 计算 $S = [l]ds_A$; 输出签名 $\sigma = (h, S)$ 。

(7) $CL \cdot Verify(pp, m, P_A, \sigma) \rightarrow 0/1$

若验证者 B 初次收到来自签名者 A 的签名 $\sigma' = (h', S')$ 之后, 先通过 h' 校验消息的完整性, 再通过秘密值证明查询算法 (如算法 2 所示) 向区块链发起查询申请。

算法 2 秘密值证明查询

输入 id_A

输出 P_A

执行智能合约:

```

1) if IQSC(idA) = nil //idA 不存在
2) return nil
3) else if exist(PA) and status = 1
//PA 处于有效状态
4) return PA
5) else
6) return nil
7) end if

```

若区块链返回给验证者 P_A ，说明用户 id_A 当前有效秘密值证明为 P_A ；反之， id_A 当前没有有效秘密值证明，签名无效。在收到 P_A 之后，验证者 B 继续根据如下步骤验证签名的有效性。判断 $h' \in [1, N-1]$ 、 $S' \in G_1$ 是否成立，若不成立，输出 0；计算 $g = e(P_1, P_A)$ ；计算 $t = g^{h'}$ ；计算 $P = [H_1(\text{id}_A \parallel \text{hid}, N)]P_2 + P_{\text{pub}}$ ；计算 $u = e(S', P)$ ；计算 $w' = u \cdot t$ ；判断 $h'' = H_2(M \parallel w', N)$ 与 h' 是否相等，若相等，输出 1，否则输出 0。

2.3 正确性与可验证性分析

(1) 正确性

在签名验证阶段，验证者最终需要验证计算出的 h'' 与来自签名者签名中的 h' 是否相等，因为 $h'' = H_2(M \parallel w', N)$ ， $h' = H_2(M \parallel w, N)$ ，验证二者是否相等等价于验证 w' 与 w 是否相等，验证过程如下：

$$\begin{aligned}
u &= e(S', P) = e([r-h]ds_A, P) = \\
&= e([r-h]ds_A, [H_1(\text{id}_A \parallel \text{hid}, N)]P_2 + P_{\text{pub}}) = \\
&= e([r-h][ka \cdot t_1^{-1}]P_1, [t_1]P_2) = \\
&= e([r-h]P_1, [ka]P_2) = \\
&= e([r-h]P_1, P_2)^{ka} = g^{r-h}
\end{aligned}$$

又因为 $w' = u \cdot t$ ， $u = g^{r-h}$ ， $h = h'$ ，所以 $w' = g^{r-h} \cdot g^{h'} = g^{r-h} \cdot g^h = g^r = w$ ，验证通过，方案的正确性得证。

(2) 可验证性

1) 对 D_A 来源于 KGC 的验证。签名者 A 通过式(1)验证部分私钥来源于 KGC 且正确，若验证不通过，签名者 A 可向区块链反馈，要求 KGC 重新生成。

$$e(D_A, [H_1(\text{id}_A \parallel \text{hid}, N)]P_2 + P_{\text{pub}}) = e(P_1, P_2) \quad (1)$$

2) 对用户秘密值正确性的验证。区块链记录具有不易篡改的特性，且通过 status 状态值标识 P_A 的有效性，若验证者 B 通过区块链查询到签名者的用户秘密值证明 P_A ，则说明用户 id_A 当前的有效秘密值证明为 P_A 。进一步地，在验证过程中验证 P_A 的正确性，验证计算如式(2)所示。

$$e(S, P) \cdot e(P_1, P_A)^h = w \quad (2)$$

2.4 安全性分析

(1) 抗公钥替换攻击

本文的无证书签名方案满足可验证性，签名者可以通过式(1)验证 KGC 生成的部分私钥，使得攻击者无法通过改变部分私钥的方式实现公钥替换攻击，削弱了攻击者替换公钥的能力。另外，本文方案将签名者选取秘密值放在 KGC 生成部分私钥之前，使签名者设置的秘密值成为 KGC 产生部分私钥的前置条件，有效地约束了 KGC 的行为。

签名者所选秘密值对应的部分公钥（用户秘密值证明）由区块链存证，且签名者更换秘密值时的日志由区块链记录。区块链存储与传统的分布式存储不同，区块链的每个节点都按照块链式结构存储完整的数据，且每个节点存储都是独立且地位等同的。区块链依靠共识机制保证存储的一致性，没有任何一个节点可以单独记录账本数据，有效避免出现记假账的行为。基于区块链数据存储去中心化、不易篡改、可追溯的特性，如果敌手用伪造秘密值证明替换用户原本的秘密值证明，恶意替换的行为就会暴露；一旦恶意 KGC 伪造密钥，用户就能及时发现并提供证据证明该密钥是伪造的。

因此，本文方案属于 KGC 信任等级 3，不仅可以很好地抵御恶意 KGC 的公钥替换攻击，还能保证签名者秘密值的确定性，进而有效保证签名的不可抵赖性。

(2) 不可伪造性

本文方案在自适应选择消息攻击下具有不可伪造性。下面在随机预言机模型下进行不可伪造性的证明。

定理 1 在随机预言机模型下，对于基于区块链与国密 SM9 的抗恶意 KGC 无证书签名方案，如果存在一个多项式时间攻击者 $\mathcal{A}$ 在安全假设下以不可忽略优势攻击该方案成功，则存在一个多项式时间的模拟算法 $\mathcal{B}$ 可以求解 ECDL 问题。

证明 假设在适应性选择消息和标识攻击下的不可伪造性安全模型中存在多项式时间概率攻击算法 $\mathcal{A}$ ，在询问 q_{H_1} 次随机预言机 $H_1(i=1,2)$ 、 q_x 次秘密值询问后，能以不可忽略的优势 ε 成功伪造签名。可构造一个多项式时间概率模拟算法 $\mathcal{B}$ 与 $\mathcal{A}$ 交互后，能以 ε/q_x 的概率解决 ECDL 问题。已知 $\mathcal{B}$ 以一个 ECDL 问题的实例 (P_2, P_{id^*}) 为输入， $P_1 \in G_2$ 且 $P_{id^*} \in G_2$ ，其中 G_2 的阶为大素数 N 。 $\mathcal{B}$ 的目标是找到元素 x^* ，使得 $P_{id^*} = [x^*]P_2$ ，其中 $x^* \in Z_N^*$ 。为描述方便，证明中忽略密码杂凑函数 $H_i(i=1,2)$ 中 hid 和 N 的输入，因为这对方案的安全性证明没有影响。

1) 初始化阶段。 $\mathcal{B}$ 首先选定系统参数，包括系统主私钥 a 和公共参数 $pp = \{BP, P_1, P_2, P_{pub}, H_1, H_2, hid\}$ ，其中双线性群 $BP = (G_1, G_2, G_T, e, N)$ ， $N > 2\lambda$ ， P_1 和 P_2 是群 G_1 、 G_2 的生成元， $H_1(\{0,1\}^* \cdot N \rightarrow Z_N^*)$ 、 $H_2(\{0,1\}^* \cdot N \rightarrow Z_N^*)$ 为两个密码杂凑函数，并将系统参数和主私钥全部发给 $\mathcal{A}$ 。

2) 随机预言机询问阶段。 H_1 -询问：已知标识 id_i ， $\mathcal{B}$ 为 H_1 询问建立列表 L_1 ，表中元素以二元组 (id, y) 的形式存储。若询问的 id_i 在 L_1 中，则返回相应的 y_i ；否则，记 id_i 为第 i 个新标识的询问。 $\mathcal{B}$ 随机选择 $y_i \in Z_N^*$ ，设 $H_1(id_i) = y_i$ ，把 y_i 发送给 $\mathcal{A}$ ，同时 $\mathcal{B}$ 将 (id_i, y_i) 存入列表 L_1 。 H_2 -询问：已知二元组 (M_i, w_i) ， $\mathcal{B}$ 为 H_2 询问建立列表 L_2 ，表中元素以三元组 (M, w, h) 的形式存储。若询问的 (M_i, w_i) 在 L_2 中，则返回相应的 h_i ；否则，记 id_i 为第 i 个新标识的询问。 $\mathcal{B}$ 随机选择 $h_i \in Z_N^*$ ，设 $H_2(M_i, w_i) = h_i$ ，把 h_i 发给 $\mathcal{A}$ ，同时 $\mathcal{B}$ 将 (M_i, w_i, h_i) 存入列表 L_2 。

3) 秘密值询问阶段。已知标识 id_i ， $\mathcal{B}$ 为秘密值询问建立列表 L_3 ，表中元素以二元组 (id, x) 的形式存储。若询问的 id_i 在 L_3 中，则返回相应的 x_i ；否则，记 id_i 为第 i 个新标识的询问。当 $id_i = id^*$ 时， $\mathcal{B}$ 输出模拟失败；否则， $\mathcal{B}$ 随机选择 $x_i \in Z_N^*$ 作为用户 id_i 的秘密值，把 x_i 发给 $\mathcal{A}$ ，同时 $\mathcal{B}$ 将 (id_i, x_i) 存入列表 L_3 。

4) 公钥替换询问阶段。已知标识 id_i ， $\mathcal{B}$ 为

秘密值询问建立列表 L_4 ，表中元素以二元组 (id, P_{id}) 的形式存储。若询问的 id_i 在 L_4 中，则返回相应的 P_{id} ；否则，由秘密值询问可知 $id_i \neq id^*$ ，否则 $\mathcal{B}$ 输出模拟失败，此时， $\mathcal{B}$ 查询列表 L_3 获得 id_i 对应的秘密值 x_i ，计算 $P_{id_i} = [x_i]P_2$ ，把 P_{id_i} 发给 $\mathcal{A}$ ，同时 $\mathcal{B}$ 将 (id_i, P_{id_i}) 存入列表 L_4 。

5) 签名询问阶段。记第 i 个消息标识对为 (M_i, id_i) ，若 $id_i \neq id^*$ ，则 $\mathcal{B}$ 可以通过随机预言机询问和秘密值询问获得对应的签名私钥 $ds_{id_i} = [x_i(y_i + a)^{-1}]P_1$ ，并根据签名算法生成有效的签名。若 $id_i \neq id^*$ ， $\mathcal{B}$ 随机选择 $k \in Z_N^*$ 和 $h \in Z_N^*$ ，令 $S = [k]P_1 \in G_1$ ， $h = H_2(M_i, w_i)$ ，再计算 $P^* = [y_i]P_2 + P_{pub}$ 和 $w = e\{S, P^*\}e(P_1, P_{id^*})^{h_1}$ ，然后 $\mathcal{B}$ 把 (h, S) 作为签名发给 $\mathcal{A}$ 。若 (M, w) 被询问过， $\mathcal{B}$ 输出模拟失败，但该事件发生的概率为 $\frac{q_{H_2} + q_s}{2^\lambda}$ ，是可忽略的，其中 q_s 是签名询问次数。

6) 伪造阶段。若 $\mathcal{A}$ 输出伪造签名 (σ^*, M^*, id^*) ，其中 $\sigma^* = (h^*, S^*)$ 。若 $id_i \neq id^*$ ， $\mathcal{B}$ 停止模拟并输出失败。当 $id_i = id^*$ 时，根据分叉引理^[15,32]，设方案的签名是 (M, w, h, S) ，其中 w, h, S 是一个 3 次交互零知识协议。存在一个 CMA 的攻击算法 $\mathcal{A}$ 能在时间 t 内以 $\varepsilon > \frac{10(q_s + 1)(q_s + q_h)}{2^\lambda}$ 的概率成功伪造签名，其中

q_s 和 q_h 分别为签名询问和随机预言机的次数。如果 (M, w, h, S) 是在不知道相应签名私钥情况下伪造的，则存在一个图灵机 $\mathcal{A}'$ 通过 $\mathcal{A}$ 的帮助，以相同的输入 (x, M, id) 在时间 $t' < 120686q_h \frac{t}{\varepsilon}$ 内输出两个有效的签名 (M, w, h_1, S_1) 和 (M, w, h_2, S_2) ，其中 $h_1 \neq h_2$ ， $S_1 \neq S_2$ 。因此， $\mathcal{B}$ 可以通过运行算法 $\mathcal{A}'$ 获得关于 (x^*, id^*) 的有效签名 (h_1^*, S_1^*) 和 (h_2^*, S_2^*) ，其中， $S_1^* = [k_1^*]P_1$ ， $S_2^* = [k_2^*]P_1$ ，且满足等式： $e(S_1^*, [H_1(id^*)]P_2 + P_{pub})e(P_1, P_{id^*})^{h_1^*} = e(S_2^*, [H_1(id^*)]P_2 + P_{pub})e(P_1, P_{id^*})^{h_2^*}$ 。

化简得： $e([x^*]^{-1}(h_1^* - h_2^*)^{-1})(S_1^* - S_2^*), [y_i + a]P_2) = e(P_1, P_2)$ 。

亦可得， $x^* = (h_1^* - h_2^*)^{-1}(y_i + a)(k_1^* - k_2^*)$ 。

之后, 模拟算法 $\mathcal{B}$ 输出 x^* 作为 ECDL 问题实例的解。

7) 概率计算。由以上证明可知, 在伪造阶段, 若 $id_i = id^*$, 则 $\mathcal{A}$ 未获得 id^* 的签名私钥, 此事件的概率为 $1/q_x$, q_x 为秘密值询问次数, 所以 $\mathcal{B}$ 成功模拟的概率为 $1/q_x$ 。因此, 若 $\mathcal{A}$ 能以不可忽略的优势 ε 成功伪造签名, 则 $\mathcal{B}$ 与 $\mathcal{A}$ 交互后能以 ε/q_x 的概率求解 ECDL 问题。

2.5 对比分析

(1) 区块链存证开销

本文基于 Hyperledger Fabric 2.2.5, 在 Ubuntu 22.04 中借助 Docker 搭建了本地测试环境, 并用 go 语言编写链码, 进行上链和查询的测试, 时间消耗如表 1 所示。

表 1 上链与查询时间
Table 1 invoke and query time

Peer 节点个数	上链时间/s	查询时间/ms
2	2.083 3	9.407 8
4	2.097 3	13.477 7
8	2.291 7	43.750 7

由表 1 可以看出, 在节点个数小于 8 时, 区块链上链存在开销约为 2 s, 查询开销不到 50 ms。采用区块链存储签名者的用户秘密值证明这一开销仅发生在用户注册阶段或者用户密钥更新阶段, 对签名方案的签名过程和验证过程没有影响。另外, 本文方案需要验证者 V 在签名验证阶段做一次区块链查询操作, 但这在实际应用中无须每次验签都通过区块链查询操作查询 P_A , 验证者 V 只需在第一次收到来自签名者 A 的签名时通过区块链查询, 之后查询本地记录即可; 如果签名者 A 更换了用户秘密值证明, 则可通过调用智能合

约提醒相应的验证者更新本地记录。

(2) 效率分析与安全性比较

定义双线性对运算开销为 B ; G_T 指数运算开销 E , G_T 中乘法运算开销 M ; 群 $G_i (i=1,2)$ 标量乘运算开销为 S_i ; 映射到 Z_N^* 的哈希运算开销 $hash$, Z_N 上的逆运算为 inv 。本文对方案的计算开销进行测试。实验测试平台为 ASUS FL5900U, 处理器为 Intel i7-7500U, 主频为 2.70 GHz, 内存为 12 GB, 操作系统为 Windows 10, 编程语言是 go1.15.2。方案测试代码采用 Go 语言编写, 由 Go 语言工具 benchmark 进行基准测试得出实验结果。经测试发现, $hash$ 与 inv 的效率极高, 其时间消耗可以忽略不计。 S_1 、 S_2 、 B 、 E 和 M 的运算效率如表 2 所示。

表 2 基本运算效率对比
Table 2 Comparison of basic operation efficiency

运算	效率/ms
S_2	0.276 8
S_1	0.088 3
B	1.449 1
E	1.364 1
M	0.007 0

表 3 列出了本文方案与文献[10-13,33]中方案计算开销与安全性的比较。其中, n_u 和 n_m 是固定值, 分别表示文献[12]、文献[13]中对应方案中两个哈希函数的输出长度; $|G_1|$ 、 $|G_T|$ 分别表示群 G_1 、 G_T 中元素大小, $|H_2|$ 表示 SM9 中密码杂凑函数 H_2 的哈希值长度。表 4 为本文方案与区块链无证书相关方案的安全性比较。表 3、表 4 中类型 I 表示外部敌手发起的公钥替换攻击, 类型 II 表示诚实且好奇的 KGC 发起的伪造攻击, 恶意

表 3 方案计算开销与安全性比较
Table 3 Computational costs and security comparison of different schemes

方案	签名方案	验证方案	总开销/ms	签名长度	类型 I	类型 II	恶意 KGC	信任等级
文献[10]	$6E$	$4B + 2E$	16.709 2	$3 G_1 $	×	×	×	2
文献[11]	$3E$	$5B + E$	12.709 1	$3 G_1 $	√	√	×	2
文献[12]	$3E + (2n_m + 3)S_1$	$3B + 3S_2 + (n_u + 2n_m + 1)S_1$	> 9.811 7	$3 G_1 $	√	√	×	3
文献[13]	$5E + (n_u + n_m + 5)S_1$	$4B + E + 3S_2 + (n_u + n_m + 1)S_1$	> 15.906 7	$3 G_1 $	×	×	×	2
文献[33]	$B + 2S_1 + E + M$	$3B + E$	9.085 2	$ G_1 + G_T $	√	√	×	2
本文	$B + E + S_1$	$2B + E + S_2 + M$	7.447 6	$ G_1 + H_2 $	√	√	√	3

KGC 表示 KGC 发起的公钥替换攻击; × 表示方案不能抵抗该类型的敌手攻击, √ 表示方案能够抵抗该类型的攻击。

表 4 基于区块链的方案安全性比较
Table 4 Security comparison of
blockchain-based schemes

方案	签名类型	类型 I	类型 II	恶意 KGC	信任等级
文献[22]	群签名	√	√	×	1
文献[34]	可截取签名	√	√	×	2
文献[35]	聚合签名	√	√	×	2
文献[36]	聚合签名	√	√	×	2
本文	—	√	√	√	3

从表 3 可知, 本文方案具有更短的签名长度和更高的效率, 更重要的是, 结合表 4 的比较分析, 本文方案满足可信中心信任等级 3 且能抵抗恶意 KGC 公钥替换攻击, 具有更高安全性。

3 结束语

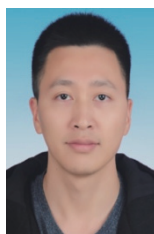
本文提出一种基于区块链和 SM9 的抗恶意 KGC 的无证书签名方案, 并证明了其安全性。通过区块链记录用户部分公钥, 可保证用户部分公钥的真实有效性, 有效防止用户公钥被恶意替换, 可以抵抗恶意 KGC 公钥替换攻击。

参考文献:

- [1] AI-RIYAMI S S, PATERSON K G. Certificateless public key cryptography[C]//Proceedings of 9th International Conference on the Theory and Application of Cryptology. 2003: 452-473.
- [2] 夏峰, 杨波. 公钥不可替换无证书签名方案[J]. 计算机科学, 2012, 39(8): 92-95.
XIA F, YANG B. Certificateless signature scheme without public key replaced[J]. Computer Science, 2012, 39(8): 92-95.
- [3] 王圣宝, 刘文浩, 谢琪. 无双线性配对的无证书签名方案[J]. 通信学报, 2012, 33(4): 93-98.
WANG S B, LIU W H, XIE Q. Certificateless signature scheme without bilinear pairings[J]. Journal on Communications, 2012, 33(4): 93-98.
- [4] 王亚飞, 张睿哲. 强安全无对的无证书签名方案[J]. 通信学报, 2013, 34(2): 94-99.
WANG Y F, ZHANG R Z. Strongly secure certificateless signature scheme without pairings[J]. Journal on Communications, 2013, 34(2): 94-99.
- [5] 樊爱宛, 杨照锋, 谢丽明. 强安全无证书签名方案的安全性分析与改进[J]. 通信学报, 2014, 35(5): 118-123.
FAN A W, YANG Z F, XIE L M. Security analysis and improvement of strongly secure certificate less signature scheme[J]. Journal on Communications, 2014, 35(5): 118-123.
- [6] 李艳琼, 李继国, 张亦辰. 标准模型下安全的无证书签名方案[J]. 通信学报, 2015, 36(4): 189-198.
LI Y Q, LI J G, ZHANG Y C. Certificateless signature scheme without random oracles[J]. Journal on Communications, 2015, 36(4): 189-198.
- [7] 汤永利, 王菲菲, 叶青, 等. 改进的可证明安全无证书签名方案[J]. 北京邮电大学学报, 2016, 39(1): 112-116.
TANG Y L, WANG F F, YE Q, et al. Improved provably secure certificateless signature scheme[J]. Journal of Beijing University of Posts and Telecommunications, 2016, 39(1): 112-116.
- [8] 王菁, 李祖猛. 几个无证书签名方案的伪造攻击[J]. 网络与信息安全学报, 2020, 6(3): 108-112.
WANG J, LI Z M. Forgery attacks on several certificate less signature schemes[J]. Chinese Journal of Network and Information Security, 2020, 6(3): 108-112.
- [9] HUNG Y H, HUANG S S, TSENG Y M, et al. Certificateless signature with strong unforgeability in the standard model[J]. Informatica, 2015, 26(4): 663-684.
- [10] 吴涛, 景晓军. 一种强不可伪造无证书签名方案的密码学分析与改进[J]. 电子学报, 2018, 46(3): 602-606.
WU T, JING X J. Cryptanalysis and improvement of a certificateless signature scheme with strong unforgeability[J]. Acta Electronica Sinica, 2018, 46(3): 602-606.
- [11] 杨小东, 王美丁, 裴喜祯, 等. 一种标准模型下无证书签名方案的安全性分析与改进[J]. 电子学报, 2019, 47(9): 1972-1978.
YANG X D, WANG M D, PEI X Z, et al. Security analysis and improvement of a certificateless signature scheme in the standard model[J]. Acta Electronica Sinica, 2019, 47(9): 1972-1978.
- [12] YANG W, WANG S, WU W, et al. Top-level secure certificateless signature against malicious-but-passive KGC[J]. IEEE Access, 2019, 7: 112870-112878.
- [13] SHIM K A. A new certificateless signature scheme provably secure in the standard model[J]. IEEE Systems Journal, 2019, 13(2): 1421-1430.
- [14] 国家市场监督管理总局, 国家标准化管理委员会. GB/T38635.2-2020 信息安全技术 SM9 标识密码算法 第 2 部分: 算法[S]. 中国标准出版社, 2020.
State Administration of Market Supervision and State Standardization Administration Committee. GM/T 38635.2-2020 Information security technology—Identity-based cryptographic algorithms SM9—Part 2: algorithms[S]. China Standards Press, 2020.
- [15] 赖建昌, 黄欣沂, 何德彪, 等. 国密 SM9 数字签名和密钥封装算法的安全性分析. 中国科学: 信息科学, 2021, 51: 1900-1913.
LAI J C, HUANG X Y, HE D B, et al. Security analysis of SM9 digital signature and key encapsulation (in Chinese). Scientia Sinica Informations, 2021, 51: 1900-1913.
- [16] 唐飞, 凌国玮, 单进勇. 基于国密 SM2 和 SM9 的加法同态加密方案[J]. 密码学报, 2022, 9(3): 535-549.
TANG F, LING G W, SHAN J Y. Additive homomorphic encryption schemes based on SM2 and SM9[J]. Journal of Cryptologic Research, 2022, 9(3): 535-549.
- [17] 张超, 彭长根, 丁红发, 等. 基于国密 SM9 的可搜索加密方案[J]. 计算机工程, 2022: 1-10.
ZHANG C, PENG C G, DING H F, et al. Searchable encryption scheme based on china state cryptography standard SM9[J]. Computer Engineering, 2022: 1-10.
- [18] 安涛, 马文平, 刘小雪. VANET 中基于 SM9 密码算法的聚合签名方案[J]. 计算机应用与软件, 2020, 37(12): 280-284.
AN T, MA W P, LIU X X. Aggregate signature scheme based on SM9 cryptographic algorithm in VANET[J]. Computer Applications

- and Software, 2020, 37(12): 280-284.
- [19] 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 algorithm based on SM9[J]. Chinese Journal of Network and Information Security, 2021, 7(4): 147-153.
- [20] 彭聪, 何德彪, 罗敏, 等. 基于 SM9 标识密码算法的环签名方案[J]. 密码学报, 2021, 8(4): 724-734.
PENG C, HE D B, LUO M, et al. An identity-based ring signature scheme for SM9 algorithm[J]. Journal of Cryptologic Research, 2021, 8(4): 724-734.
- [21] 唐飞, 凌国玮, 单进勇. 基于国产密码算法 SM9 的可追踪属性签名方案[J]. 电子与信息学报, 2022, 44: 1-8.
TANG F, LING G W, SHAN J Y. Traceable attribute-based signature scheme based on domestic cryptographic SM9 algorithm[J]. Journal of Electronics and Information, 2022, 44: 1-8.
- [22] 杨亚涛, 蔡居良, 张筱薇, 等. 基于 SM9 算法可证明安全的区块链隐私保护方案[J]. 软件学报, 2019, 30(6): 1692-1704.
YANG Y T, CAI J L, ZHANG X W, et al. Privacy preserving scheme in block chain with provably secure based on SM9 algorithm[J]. Journal of Software, 2019, 30(6): 1692-1704.
- [23] 郭阳楠, 蒋文保, 叶帅. 可监管的区块链匿名交易系统模型[J]. 计算机应用, 2022: 1-10.
GUO Y N, JIANG W B, YE S. Supervisable blockchain anonymous transaction system model[J]. Computer Applications, 2022: 1-10.
- [24] 闻庆峰, 杨文捷, 张永强. SM9 及其 PKI 在电子政务邮件系统中的应用[J]. 计算机应用与软件, 2017, 34(4): 105-109.
WEN Q F, YANG W J, ZHANG Y Q. Application of SM9 and PKI in e-government e-mail system[J]. Computer Applications and Software, 2017, 34(4): 105-109.
- [25] 马晓婷, 马文平, 刘小雪. 基于区块链技术的跨域认证方案[J]. 电子学报, 2018, 46(11): 2571-2579.
MA X T, MA W P, LIU X X. A cross domain authentication scheme based on blockchain technology[J]. Acta electronica Sinica, 2018, 46(11): 2571-2579.
- [26] 邱帆, 胡凯雨, 左黎明, 等. 基于国密 SM9 的配电网分布式控制身份认证技术[J]. 计算机应用与软件, 2020, 37(9): 291-295.
QIU F, HU K Y, ZUO L M, et al. Distributed control identity authentication technology based on SM9[J]. Computer Applications and Software, 2020, 37(9): 291-295.
- [27] 姚英英, 常晓林, 甄平. 基于区块链的去中心化身份认证及密钥管理方案[J]. 网络空间安全, 2019, 10(6): 33-39.
YAO Y Y, CHANG X L, ZHEN P. Decentralized identity authentication and key management scheme based on blockchain[J]. Cyberspace Security, 2019, 10(6): 33-39.
- [28] 许盛伟, 任雄鹏, 袁峰, 等. 一种关于 SM9 的安全密钥分发方案[J]. 计算机应用与软件, 2020, 37(1): 314-319.
XU S W, REN X P, YUAN F, et al. A secure key issuing scheme for SM9[J]. Computer Applications and Software, 2020, 37(1): 314-319.
- [29] 吴俊青, 彭长根, 谭伟杰, 等. FaceEncAuth: 基于 FaceNet 和国密算法的人脸识别隐私安全方案[J]. 计算机工程与应用, 2022: 1-7.
WU J Q, PENG C G, TAN W J, et al. FaceEncAuth: face recognition privacy security scheme based on FaceNet and SM algorithms[J]. Computer engineering and application, 2022: 1-7.
- [30] NAKAMOTO S. Bitcoin: A peer-to-peer electronic cash system[J]. Decentralized Business Review, 2008: 21260.
- [31] GIRAULT M. Self-certified public keys[C]//Workshop on the Theory and Application of Cryptographic Techniques. Springer, 1991, 547(1): 490-497.
- [32] POINTCHEVAL D, STERN J. Security arguments for digital signatures and blind signatures[J]. Journal of Cryptology, 2000, 13(3): 361-396.
- [33] 叶胜男, 陈建华. 一个强安全的无证书签名方案的分析和改进[J]. 计算机科学, 2021, 48(10): 272-277.
YE S N, CHEN J H. Security Analysis and improvement of strongly secure certificateless digital signature Scheme[J]. Computer Science, 2021, 48(10): 272-277.
- [34] LIU J, LI X, YE L, et al. BPDS: a blockchain based privacy-preserving data sharing for electronic medical records[C]//Proceedings of 2018 IEEE Global Communications Conference (GLOBECOM). 2018: 1-6.
- [35] ALI I, GERVAIS M, AHENE E, et al. A blockchain-based certificateless public key signature scheme for vehicle-to-infrastructure communication in VANETs[J]. Journal of Systems Architecture, 2019, 99: 101636.
- [36] BENIL T, JASPER J. Cloud based security on outsourcing using blockchain in E-health systems[J]. Computer Networks, 2020, 178: 107344.

[作者简介]



唐飞 (1986-), 男, 重庆垫江人, 博士, 重庆邮电大学副教授、博士生导师, 主要研究方向为公钥密码、隐私保护、区块链等。



甘宁 (1998-), 女, 重庆綦江人, 重庆邮电大学硕士生, 主要研究方向为区块链、公钥密码。



阳祥贵 (1985-), 男, 江西宜春人, 江西昌河航空工业有限公司高级工程师, 主要研究方向为信息化、数字化、智能制造。



王金洋 (1998-), 男, 重庆渝北人, 重庆邮电大学硕士生, 主要研究方向为区块链、公钥密码。