

基于SM3的变色龙哈希函数及其应用

赵宪鑫¹, 马金花¹, 严笑天¹, 许胜民^{1,2}

(1. 福建师范大学计算机与网络空间安全学院, 福建 福州 350117;

2. 区块链应用监管教育部工程研究中心(东南大学), 江苏 南京 211189)

摘要: 区块链的不可篡改性使得数据一经上链即无法修改, 致使上链的不良信息将持续带来严重的负面影响。为保障链上数据合理可控, 可修订区块链的概念被提出, 其关键密码技术为变色龙哈希函数。然而, 现有的变色龙哈希函数方案缺乏国密算法理论支撑, 不符合区块链核心技术自主可控的需求。因此, 基于国密体系构建可修订区块链成为亟待解决的关键问题。基于 I -SDH 困难问题, 构造了一种基于 SM3 的变色龙哈希函数, 并证明该方案在随机谕言机模型下是安全的。通过系统的实验评估, 验证了所提方案在实现可修订功能的同时, 仅引入了可接受的计算开销, 具有良好的实用性。该研究有助于丰富国产密码算法的应用体系, 并推动区块链关键密码技术的国产化进程。

关键词: SM3 哈希函数; 变色龙哈希函数; 可修订区块链; 区块链

中图分类号: TP311

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2025057

Chameleon hash function based on SM3 and its applications

ZHAO Xianxin¹, MA Jinhua¹, YAN Xiaotian¹, XU Shengmin^{1,2}

1. College of Computer and Cyber Security, Fujian Normal University, Fuzhou 350117, China

2. Engineering Research Center of Blockchain Application, Supervision and Management (Southeast University),
Ministry of Education, Nanjing 211189, China

Abstract: The immutability of blockchain technology was known to ensure that once data was added to the chain, it could not be altered, which meant that any harmful information uploaded would continue to exert serious negative impacts. To ensure that on-chain data remained reasonable and controllable, the concept of a redactable blockchain was proposed, with the chameleon hash function identified as the key cryptographic technology. However, existing chameleon hash function schemes were found to lack the theoretical foundation of national crypto-

收稿日期: 2025-02-21; 修回日期: 2025-07-24

通信作者: 马金花, jinhua@fjnu.edu.cn

基金项目: 国家重点研发计划(2023YFB3106200); 国家自然科学基金(62572123, 62402109); 教育部开放课题(K1-2024-03-01)

Foundation Items: The National Key R&D Program of China (2023YFB3106200), The National Natural Science Foundation of China (62572123, 62402109), The Engineering Research Center of Blockchain Application, Supervision and Management (Southeast University), Ministry of Education (K1-2024-03-01)

引用格式: 赵宪鑫, 马金花, 严笑天, 等. 基于 SM3 的变色龙哈希函数及其应用[J]. 网络与信息安全学报, 2025, 11(5): 162-171.

Citation Format: ZHAO X X, MA J H, YAN X T, et al. Chameleon hash function based on SM3 and its applications[J]. Chinese Journal of Network and Information Security, 2025, 11(5): 162-171.

graphic algorithms, failing to meet the strategic need for autonomous and controllable core blockchain technologies. Therefore, the construction of a redactable blockchain based on national cryptographic standards was recognized as a critical issue that urgently needed to be addressed. A chameleon hash function based on the national cryptographic algorithm SM3 was constructed, and its security was proven under the random oracle model, relying on the hardness of the l -SDH problem. Through systematic experimental evaluation, the proposed scheme was demonstrated to support data redaction functionality with only modest computational overhead, indicating good practical applicability. This research was considered to contribute to the enrichment of the application framework of national cryptographic algorithms and to promote the localization of core cryptographic technologies in blockchain systems.

Keywords: SM3 hash function, chameleon hash function, redactable blockchain, blockchain

0 引言

区块链是一种去中心化、不可篡改的分布式账本技术,已被广泛应用于物联网、数字金融、智能制造等领域。其中,不可篡改性是区块链的核心安全特性之一。该特性由链式结构与哈希算法共同保障:每个区块包含前一个区块的哈希值,一旦区块内的数据发生变动,其哈希值将随之改变,继而破坏后续所有区块的哈希链。这种机制使得任何用户都无法擅自修改或删除链上数据,从而有效防止数据被恶意篡改。

然而,在隐私保护与法律合规领域,不可篡改性面临着新的挑战。区块链上的数据在写入区块链之后不可删除,与《通用数据保护条例》^[1]中提出的“被遗忘权”、《中华人民共和国个人信息保护法》^[2]中提出的“删除权”等存在冲突。一旦敏感信息、非法内容或错误数据被记录在链上,将永久存储,难以满足用户的数据更正、删除等合法诉求。这种技术与合规之间的矛盾,促使研究者探索更加灵活的数据处理机制。

为实现区块链系统在保持结构完整前提下的数据修改,Ateniese等^[3]提出了可修订区块链的概念,允许授权的修订者删除、修改原始区块链中的数据内容,并使得修订后的区块链仍能通过公开验证。其具体构造主要利用基于公钥的加密算法与变色龙哈希函数,结合安全多方计算,实现了基于区块层的粗粒度修订授权技术。变色龙哈希函数是一种具备可控碰撞特性的哈希函数,给定一个消息及对应的哈希原像,普通用户无法找到该消息的哈希碰撞,但

陷门持有者可通过私钥计算出对应碰撞,从而对已生成的哈希原像进行修订而不影响区块链结构。这使得可修订区块链能够在不破坏原有哈希链完整性的前提下,支持链上数据的更新、纠错与合规调整。

然而,目前国内尚缺乏对国密算法体系下可修订区块链的系统性研究。以SM3为代表的国密哈希函数虽然在安全性方面经过广泛验证,但其本身不具备可控碰撞能力,难以直接应用于变色龙哈希函数构造。因此,如何在不破坏SM3核心安全属性的基础上,拓展其功能以支持可控碰撞,成为构建基于国密算法的可修订区块链的关键问题。

为推进可修订区块链技术的国产化进程,满足信息安全自主可控的需求,本文在SM3哈希函数^[4]的基础上,结合Gennaro^[5]提出的承诺机制,设计了一种具备可控碰撞能力的变色龙哈希函数。该函数保留了SM3原有的安全特性,同时允许陷门持有者灵活修改哈希原像。基于 l -SDH困难问题,本文在随机预言机模型下证明了所提方案的抗碰撞性安全。

实验评估表明,在生成哈希值并保持可控碰撞能力的前提下,所提方案相比原始SM3哈希函数仅增加约10.9 ms的计算时间,具有良好的效率表现。该方案不仅实现了可修订区块链在国密算法体系中的功能拓展,而且提升了链上数据修订的安全性与实用性。

本文为丰富国产密码算法体系、推动区块链关键密码技术的自主发展提供了新的思路,也为隐私保护、数据纠错与法律合规等实际应用场景提供了技术支撑。

1 相关工作

1.1 变色龙哈希函数

2000 年, Krawczyk 和 Rabin^[6]首次提出变色龙哈希函数的概念, 分别给出了基于离散对数和因式分解的变色龙哈希函数的具体构造, 并利用变色龙哈希函数设计了变色龙签名。然而, 这种早期构造存在一个显著的安全性问题——陷门暴露风险。当执行一次碰撞算法后, 攻击者可能利用公开信息恢复陷门, 从而危及系统的安全性。2004 年, Ateniese 等^[7]提出了基于身份的变色龙哈希函数, 简化了密钥管理, 提升了计算效率。2005 年, Ateniese 等^[8]利用 Gennaro^[5]提出的承诺方案, 在双线性群上构造了一种基于 l -SDH 困难问题的变色龙哈希函数, 该方案通过引入标签, 有效解决了陷门暴露问题; Chen 等^[9]基于计算 Diffie-Hellman (CDH) 困难问题设计了抗密钥泄露的变色龙哈希函数方案。2017 年, Camenisch 等^[10]提出了带有即时陷门的变色龙哈希 (chameleon-hashes with ephemera trapdoors, CHET) 函数, 并给出了 3 种构造方案。其中一种构造方案为黑盒构造, 通过结合两个变色龙哈希函数间接实现 CHET, 两个哈希函数的陷门分别对应长期陷门和临时陷门, 数据的修改需要同时持有两者, 其余两种方案分别基于离散对数和因式分解困难问题并结合零知识证明, 直接实现 CHET 的构造。2018 年, Krenn 等^[11]提出了具有双重长期陷门的变色龙哈希函数。该构造中, 计算哈希的一方可以决定生成新陷门或者复用现有陷门, 进一步增强了变色龙哈希函数的灵活性。2020 年, Derler 等^[12]研究了不同变色龙哈希函数的抗碰撞性之间的关系, 提出了完全抗碰撞变色龙哈希函数的黑盒构造。2024 年, Li 等^[13]提出了基于格的变色龙哈希函数, 为变色龙哈希函数在抗量子计算场景中的应用提供了理论支撑。此外, 变色龙哈希函数的研究不断扩展到密钥管理^[14]、车联网^[15]、电子政务系统^[16]等领域。

1.2 可修订区块链

2017 年, Ateniese 等^[3]提出了可修订区块链的概念, 并利用变色龙哈希函数、安全多方计算和零知识证明等技术构造了第一个可修订区

块链系统, 但该方案的构造过于复杂, 导致巨额的通信开销。此外, 该方案构造仅支持粗粒度的区块级数据修订, 并不实用。为实现高效的细粒度的数据修订, 2019 年, Derler 等^[17]结合密文策略属性基加密^[18]和 CHET, 提出了基于策略的变色龙哈希 (policy-based chameleon-hashes, PCH) 函数, 并给出了具体构造。该构造要求计算碰撞的密钥均需满足访问策略, 利用 PCH 代替底层哈希函数, 实现了对区块链的交易级重写, 进一步提升了数据管理的精细度。2019 年, Deuber 等^[19]基于共识投票机制提出了一种全新的设计方案。该方案允许任何用户提出数据修订请求, 并通过区块链网络的共识投票决定是否执行修订操作, 摆脱了对单一授权中心的依赖。然而, 在去中心化的同时, 该方案的效率和安全性仍需进一步优化, 尤其是在处理大量修订请求时所面临的通信开销大和共识时延高等问题。在单授权中心的可修订区块链系统中, 授权中心通常被假设为完全可信, 这种设计容易导致单点失效问题, 授权中心也可能成为攻击者的主要目标。为解决这一问题, 2022 年, Ma 等^[20]提出了去中心化的 PCH, 并基于此设计了多授权中心的可修订区块链系统。该方案通过多个授权中心分散修订权限, 结合访问策略管理机制, 显著提升了系统的安全性和可靠性。2020 年, Tian 等^[21]提出了具有黑盒问责机制的 PCH, 当某一区块修改后发生争议时, 任何用户都可以通过与黑盒交互追溯到该区块的修改者。2021 年, Xu 等^[22]基于 RSA 困难问题提出了可撤销的 PCH (revocable policy-based chameleon hash, RPCH), 为可修订区块链提供了一种撤销陷门持有者的重写权限的方法。2022 年, Jia 等^[23]提出了一种在去中心化环境下具有可追溯性的高效可修订区块链。2023 年, Tian 等^[24]基于离散对数困难问题构造了效率更高的 RPCH。2024 年, Duan 等^[25]提出了 T-Times 变色龙哈希 (t-times chameleon hash, T-CH) 函数, 并基于 T-CH 设计了一个不依赖可信机构的可修订区块链系统。该方案允许对区块链中的数据执行最多 T 次修订操作, 通过限制修订次数, 有效防止了特权滥用问题。同时, T-CH 的

设计进一步强化了去中心化特性，为可修订区块链的实际应用提供了新的解决思路。自可修订区块链概念提出以来，便迅速成为国内外研究热点方向之一，并广泛应用于物联网^[26-27]、电子医疗记录^[28]、移动网络^[29]等场景。此后，研究人员针对可修订区块链进行更为深入的研究，然而目前基于国密算法的可修订区块链相关研究尚且不足。

1.3 SM3

SM3是国家密码管理局于2010年12月公布的商用密码杂凑算法（征求意见稿），2012年形成行业标准GM/T 0004-2012，2016年进一步升级为国家标准GB/T 32905-2016。该算法在SHA-256的基础上进行了改进，其每轮迭代处理2个消息字的机制使其在一定程度上具备比SHA-256更强的安全性。自SM3发布以来，已受到密码学界的广泛关注，并在文件完整性检测^[30]、恶意软件检测^[31]、智能电网^[32]等应用场景中得到实际应用。此外，SM3在数字签名领域也得到了重要应用。2023年，孙思维等^[33-34]基于SM3哈希函数，分别提出了无状态数字签名方案和后量子数字签名方案，为解决传统签名在资源约束设备和量子计算威胁下的安全问题提供了新思路；陈学雷等^[35]提出了基于单指令多数据（single instruction multiple data, SIMD）寄存器SM3并行算法的快速SM2-KDF实现方法，大幅提升了计算效率。SM3的应用研究非常广泛，但目前尚未见基于SM3的变色龙哈希函数构造的相关研究的报道。本文提出首个基于SM3的变色龙哈希函数，进一步完善国密算法生态体系，有效助推国产密码算法在国际金融、电子政务领域的创新实践。

2 预备知识

2.1 参数说明

设 $\mathbb{N}$ 是所有自然数的集合，用 $\lambda \in \mathbb{N}$ 表示安全参数。设 Z_q 为模 q 的整数群。若无特殊说明，输入的消息为任意长度且所有算法均为多项式时间内的算法。

设 $\text{SM3}(\cdot)$ 表示SM3哈希函数（杂凑算法），参数说明如表1所示。

表1 SM3算法参数说明

Table 1 SM3 algorithm parameter description

符号	描述
$ABCDEFGH$	8个字寄存器值的串联
$B^{(i)}$	第 i 个消息分组
CF	压缩函数
FF_j	布尔函数，随 j 改变
GG_j	布尔函数，随 j 改变
IV	压缩函数的初始值
P_0	压缩函数中的置换函数
P_1	消息扩展中的置换函数
T_j	常量，随 j 改变
m	消息
m'	填充后的消息
mod	模运算
$\wedge$	32比特与运算
$\vee$	32比特或运算
$\oplus$	32比特异或运算
$\neg$	32比特非运算
$+$	mod ³² 算术加运算
$\ll k$	循环左移 k 比特运算
$\leftarrow$	左向赋值运算符

2.2 双线性群

设 $\mathbb{G}_1, \mathbb{G}_2$ 为(加法)循环群， $\mathbb{G}_T$ 为(乘法)循环群，阶为素数 q ，群元素 $g_1 \in \mathbb{G}_1, g_2 \in \mathbb{G}_2$ 为生成元。 e 表示双线性对映射 $e: \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ ，该映射满足以下性质。

1) 双线性。对于任意的 $a, b \in Z_q$ ，均有 $e(ag_1, bg_2) = e(g_1, g_2)^{ab}$ 成立。

2) 非退化性。对于任意的生成元 $g_1 \in \mathbb{G}_1$ 和 $g_2 \in \mathbb{G}_2$ ，均有 $e(g_1, g_2) \neq 1$ 。

3) 可计算性。双线性对映射 e 可以在多项式时间内计算。

双线性群分为对称和非对称双线性群两类，若群 $\mathbb{G}_1$ 和 $\mathbb{G}_2$ 相同或者群 $\mathbb{G}_1$ 和 $\mathbb{G}_2$ 之间存在同态映射，则称为对称双线性群；若群 $\mathbb{G}_1$ 和 $\mathbb{G}_2$ 不同且群 $\mathbb{G}_1$ 和 $\mathbb{G}_2$ 之间不存在任何同态映射，则称为非对称双线性群。本文令 $\mathbb{G} = \mathbb{G}_1 = \mathbb{G}_2$ ， $\mathcal{BP} = (\mathbb{G}, \mathbb{G}_T, e, q)$ 表示对称双线性群^[36-37]。

2.3 困难问题假设

本文方案的安全性基于 l -SDH困难问题^[38]，设 $\mathbb{G}$ 为一般循环群，生成元为 $g \in \mathbb{G}$ ，则 l -SDH问题的定义如下。

参数 1^l 。输出公私钥对 (pk, sk) 。

$(ch, k) \leftarrow \text{CHash}(pk, m, L)$ ，变色龙哈希算法输入公钥 pk ，消息 m 和标签 L 。输出变色龙哈希值 ch 和随机值 k 。

$\{0, 1\} \leftarrow \text{CHCheck}(pk, m, k, L, ch)$ ，哈希验证算法输入公钥 pk 、消息 m 、随机值 k 、标签 L 和变色龙哈希值 ch 。若 ch 对 (m, k, L) 有效，则输出 1；否则输出 0。

$k' \leftarrow \text{CHColl}(pk, sk, m, k, L, m')$ ，哈希碰撞算法输入公钥 pk 、私钥 sk 、消息对 (m, k) 、标签 L 、消息 m' 和变色龙哈希值 ch ，输出哈希碰撞 k' 。

定义2 正确性。对于本文所有正确计算的输出 $(pk, sk) \leftarrow \text{Setup}(1^l)$ ， $(ch, k) \leftarrow \text{CHash}(pk, m, L)$ ， $k' \leftarrow \text{CHColl}(pk, sk, m, k, L, m')$ ，均有 $\text{CHCheck}(pk, m, k, L, ch) = \text{CHCheck}(pk, m', k', L, ch) = 1$ 。

3.2 安全模型

本文构造的变色龙哈希函数需满足抗碰撞性 (collision resistance, CR)，其定义如下。

定义3 抗碰撞性。假设给定消息对 (m, k, m') ，不存在多项式时间内的算法能够计算 (m, k, m') 在标签 L 下哈希碰撞 k' 。

抗碰撞性安全模型通过挑战者 C 和敌手 A 之间的交互游戏定义。该游戏分为4个阶段，具体定义如下。

1) 初始化。挑战者 C 执行 Setup 算法获取公私钥 (pk, sk) ，挑战者 C 将公钥 pk 发送给敌手 A 。然后敌手 A 将其挑战的消息对 (m, k, m', ch) 发送给挑战者 C 。

2) 哈希询问。在此阶段，敌手自适应选择标签 L_i 向挑战者 C 发起询问，挑战者 C 返回 L_i 的哈希值给敌手。

3) 碰撞询问。敌手 A 向挑战者 C 询问 (m, k, m', ch) 在标签 L_i 下的哈希碰撞，挑战者 C 执行 CHColl 算法计算碰撞 k'_i ，并返回给 A 。

4) 伪造。敌手 A 伪造在标签 L 下关于消息对 (m, k, m', ch) 的哈希碰撞 k' ，并发送给挑战者 C ，其中 L 未被询问过。挑战者 C 执行 CHCheck 算法检验 k' ，若有效，敌手赢得游戏，否则敌手失败。

假设 k' 是消息对 (m, k, m') 敌手在标签 L 下的伪造碰撞，则定义敌手赢得该游戏的优势为： $\text{Adv}_{\mathcal{A}}^{\text{CR}}(1^l) = \Pr[\text{CHCheck}(pk, m', k', L, ch) = 1]$ 。

若对于任意多项式时间内的敌手，该优势可忽略，则称本文方案满足抗碰撞性。

3.3 具体构造

基于 SM3 的变色龙哈希函数方案共 4 个算法，为方便描述，下文所有算法中，令 $s = \text{SM3}(L)$ ，且所有 SM3 的哈希值都默认对 q 取模。该算法具体构造如下。

1) Setup ：算法输入安全参数 1^l 。初始化双线性群 $\mathcal{BP} = (\mathbb{G}, \mathbb{G}_T, e, q)$ ，生成元为 $g \in \mathbb{G}$ ；随机选择 $x \in Z_q$ ，计算 $h = g^x$ 。输出公私钥对 $(pk, sk) = (h, x)$ 。

2) CHash ：算法输入公钥 pk 、消息 m 和标签 L 。随机选择 $r \in Z_q$ 并计算 $k = g^r$ 、 $ch = g^{\text{SM3}(m)}(g^s h)^r$ ，最后输出变色龙哈希值 ch 和随机值 k 。

3) CHCheck ：算法输入公钥 pk 、消息 m 、随机值 k 、标签 L 和变色龙哈希值 ch 。该算法验证消息对 (m, k) 在标签 L 下与变色龙哈希值 ch 是否匹配。计算 $F = ch/g^{\text{SM3}(m)}$ ，若 (k, hg^s, F) 满足配对运算 $e(k, hg^s) = e(g, F)$ ，则输出 1，否则输出 0。

4) CHColl ：算法输入公钥 pk 、私钥 sk 、消息对 (m, k) 、标签 L 和消息 m' 。设 (m, k) 和 (m', k') 在标签 L 下的变色龙哈希值相等，其中 $k = g^r$ ，且存在一个随机数 $r' \in Z_q$ 满足 $k' = g^{r'}$ ，根据 CHash 计算：

$$g^{\text{SM3}(m)}(g^s h)^r = g^{\text{SM3}(m')}(g^s h)^{r'}$$

进一步计算

$$g^{r'} = g^r g^{(\text{SM3}(m) - \text{SM3}(m'))/(x + s)}$$

即

$$k' = k g^{(\text{SM3}(m) - \text{SM3}(m'))/(x + s)}$$

最后输出哈希碰撞 k' 。

3.4 正确性分析

假设 Setup 、 CHash 、 CHCheck 和 CHColl 算法均正确执行，且消息对 (m, k, m', k', ch) 在传递过程中没有被篡改，则方案的正确性可通过以下式子推导出：算法正确执行有 $(h, x) = \text{Setup}(1^l)$ ， $(ch, k) = \text{CHash}(pk, m, r, L)$ ， $k' = \text{CHColl}(pk, sk, m, k, L, m')$ 。计算 $F' = ch/g^{\text{SM3}(m')}$ 和 $s = \text{SM3}(L)$ ，设存在 $r' \in Z_q$ 满足 $k' = g^{r'}$ ，故有

$$e(k', hg^s) = e(g^{r'}, hg^s) =$$

$$e(g, (hg^s)^{r'}) = e(g, F')$$

成立。因此，本文方案满足正确性要求。

3.5 安全性分析

本文方案的抗碰撞性基于 l -SDH 困难问题，

安全性分析如下。

定理 1 若 l -SDH 问题在双线性群 $\mathbb{G}$ 上是困难的, 则该方案满足抗碰撞性。

证明 假设存在一个敌手 $\mathcal{A}$ 能在时间 t 内以 ϵ 的概率攻破本文方案, 则可以构造一个模拟器 $\mathcal{B}$ 解决 l -SDH 困难问题。给定一个双线性群 $\mathbb{G}$ 上的困难问题实例 $(g, g^a, g^{a^2}, \dots, g^{a^l})$, 模拟器 $\mathcal{B}$ 扮演安全模型中的挑战者, 并控制随机谕言机 $\mathcal{H}$ 。敌手和模拟器进行以下操作。

1) 初始化。初始化挑战消息对 (m, k, m', ch) 。模拟器 $\mathcal{B}$ 随机选择 l 个整数 $w_1, w_2, \dots, w_l \in Z_q$, 设 $g^{\text{SM3}(m) - \text{SM3}(m')} = g^{(a+w_1)(a+w_2)\dots(a+w_l)}$, 公钥为 $h = g^a$, 其对应私钥为 a 。

2) 哈希询问。敌手在此阶段向模拟器 $\mathcal{B}$ 询问所选标签的哈希值。在敌手开始询问之前, 模拟器 $\mathcal{B}$ 随机选择整数 $i^* \in [1, q_H]$ 和 $w^* \in Z_q$ 。然后, 模拟器 $\mathcal{B}$ 建立一个哈希列表记录所有的询问和应答, 哈希列表初始为空。

当敌手 $\mathcal{A}$ 自适应选择标签 L_i 向模拟器 $\mathcal{B}$ 发起询问时, 若哈希列表中已经有 L_i 对应的项, 则模拟器 $\mathcal{B}$ 根据哈希列表应答该询问。否则, $\mathcal{B}$ 计算:

$$\mathcal{H}(L_i) = \begin{cases} w_i, i \neq i^* \\ w^*, i = i^* \end{cases}$$

然后将 $(L_i, \mathcal{H}(L_i))$ 记作该询问的应答, 并加入哈希列表。

3) 碰撞询问。敌手在此阶段向模拟器 $\mathcal{B}$ 询问消息对 (m, k, m') 在标签 L_i 下的哈希碰撞。若 L_i 是在哈希列表中第 i^* 个询问的标签, 则终止; 否则, 计算 $k'_i = kg^{(a+w_1)\dots(a+w_{i-1})(a+w_{i+1})\dots(a+w_l)}$ 。根据 CHColl 函数定义有:

$$k'_i = kg^{(\text{SM3}(m) - \text{SM3}(m'))/(a+w_i)} = kg^{(a+w_1)\dots(a+w_{i-1})(a+w_{i+1})\dots(a+w_l)}$$

最后模拟器 $\mathcal{B}$ 将 k'_i 返回给敌手 $\mathcal{A}$ 。

4) 伪造。敌手 $\mathcal{A}$ 伪造在标签 L_i^* 下关于消息对 (m, k, m') 的哈希碰撞 k' , 并发送给模拟器 $\mathcal{B}$ 。若 L_i^* 不是哈希列表中第 i^* 个询问的标签, 则终止; 否则, 由 $\mathcal{H}(L_i^*) = w^*$ 可以计算:

$$k' = kg^{\frac{(a+w_1)(a+w_2)\dots(a+w_l)}{a+w^*}}$$

设 $f(a)$ 为 $l-1$ 次多项式, d 为一个非零整数, 模拟器 $\mathcal{B}$ 可以计算:

$$g^{\frac{f(a) + \frac{d}{a+w^*}}{a+w^*}} = \frac{k'}{k}$$

进一步计算:

$$\left(\frac{g^{\frac{f(a) + \frac{d}{a+w^*}}{a+w^*}}}{g^{f(a)}} \right)^{\frac{1}{d}} = g^{\frac{1}{a+w^*}}$$

最后输出 $(w^*, g^{\frac{1}{a+w^*}})$ 作为 l -SDH 困难问题的解。

由于真实攻击和模拟攻击是不可区分的, 假设敌手向随机谕言机询问 q_H 次后, 敌手能在时间 t 内以 ϵ 的概率攻破本文方案, 则解决 l -SDH 问题的优势为 ϵ/q_H 。令 T_s 为模拟的时间成本, 则模拟器 $\mathcal{B}$ 在时间 $t + T_s$ 内解决 l -SDH 困难问题的优势为:

$$\text{Adv}_{\mathcal{A}}^{l\text{-SDH}}(1^\lambda) = \frac{\epsilon}{q_H}$$

由于 l -SDH 问题是困难的, 因此证明本文方案是安全的。

4 应用

在可修订区块链中, 允许特定授权实体 (如监管机构或管理员) 对区块链中的数据进行合法修改, 而无需重新计算整个链的哈希值。因此, 可修订区块链在电子政务与法律合规、跨境金融等领域具有实际应用价值。例如, 电子政务系统存储大量敏感数据, 如公民身份信息、政府公告等。可修订区块链能够在不影响整体数据结构的情况下, 允许监管机构对错误或敏感信息进行合法修订, 确保数据合规性。

基于本文构造的变色龙哈希函数, 结合比特币的区块结构作为基础语法, 对可修订区块链中的区块修订操作进行讨论。如图 1 所示, 对于可修订区块链中的每个区块, 均包含 4 部分: Pre_H 表示前一个区块的哈希; TS 表示时间戳, 记录区块生成的时间信息; Root 表示 Merkle 树的根哈希值; Nonce 表示随机值, 用于区块链系统的工作量证明机制。假设存在一个管理员持有陷门, 用户仅持有公钥, 而管理员能够利用陷门修改区块事务。以本文方案代替底层哈希函数, $H(\cdot)$ 表示一般哈希函数。区块链中的每个区块存储一组事务的哈希值, 即 Merkle 树的根哈希, 它累计了一个区块中的所有事务。考虑对于区块 i 包含 4 个事务, 分别为 $T_{i,1}$ 、 $T_{i,2}$ 、 $T_{i,3}$ 、

$T_{i,4}$, 对应的哈希值为 A 、 B 、 C 、 D 。以变色龙哈希值 ch 代替事务 $T_{i,1}$, 则 $A = H(ch)$, $(ch, k) = CHash(pk, T_{i,1}, L)$, 其中 k 作为事务的非哈希部分存储。若管理者要求将事务 $T_{i,1}$ 修改为 $T'_{i,1}$, 则利用私钥 sk 计算随机值 $k' = CHColl(pk, sk, m, k, L, m')$, 新的随机值 k' 代替初始的随机值 k 存储在区块链中。在修改事务之后, A 的哈希值并未发生改变。

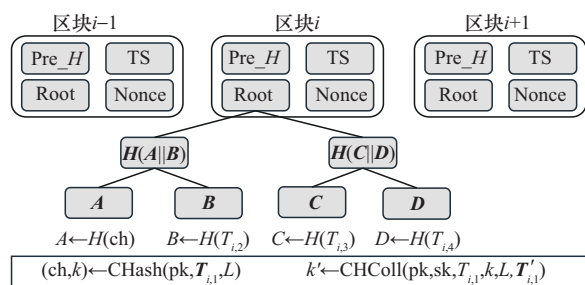


图1 区块修订

Figure 1 Block redaction

5 实验

5.1 算法分析

本节从理论上分析基于SM3的变色龙哈希方案的计算开销, 由于与对比方案的系统初始算法 Setup 计算开销相当, 因此本节只对比除 Setup 算法以外的其他3种算法的计算开销。CHash为变色龙哈希算法, 该算法计算过程中需要计算两次哈希值和3次指数级运算, 指数运算实现过程中利用了快速指数算法提高运行效率。CHColl为碰撞算法, 该算法执行过程中需要计算3次哈希、一次指数运算和一次乘法逆元(扩展欧几里得算法)。CHCheck为哈希验证算法, 该算法的时间开销与CHash相比多两次配对运算。该方案与利用SHA-256、MD5哈希算法实现的变色龙哈希算法和哈希碰撞算法效率对比见表2。

表2 算法效率

Table 2 Algorithm efficiency

算法	运行时间/ms
MD5-CHash	38.3
SHA256-CHash	55.9
本文CHash	95.8
MD5-CHColl	66.5
SHA256-CHColl	96.4
本文CHColl	170.1

5.2 实验分析

本节简单说明代码的实现, 并通过实验分析方案的可行性。本文方案使用Python编程语言实现, 版本为Python3.11, 代码主要利用hashlib、PairingGroup库实现。其中hashlib库内置了MD5、SM3和SHA-256哈希算法, 用于计算消息的哈希值, PairingGroup库用于计算配对, 并生成 q 阶对称双线性群。本文方案的算法效率实验所使用的设备配置为: Ubuntu5.4.0-150-generic, Intel Core i7-10700 CPU @ 2.90 GHz, 2 GB内存, 64位操作系统。每组数据测试运行15次取平均值作为结果, 以保证实验数据的准确性。

由图2和图3可知, 本文方案基于SM3的变色龙哈希函数, 时间效率低于基于SHA-256和MD5的实现。这主要是因为: ①哈希值长度不同, MD5的哈希值长度为128比特, 而SM3和SHA-256的哈希值长度均为256比特, 导致SM3和SHA-256的计算开销更高; ②算法复杂度不同, 虽然SM3与SHA-256的哈希值长度相同, 但SM3算法的安全性更高, 其设计更为复杂。例如, SM3的压缩函数每一轮迭代使用两个消息字, 这显著增加了计算时间。当消息长度为 2.5×10^7 bit时, 本文方案与SHA-256算法实现的变色龙哈希函数的时间开销相差约50.1 ms。对比哈希碰撞算法时, 本文方案的时间开销比SHA-256实现的变色龙哈希函数多73.7 ms。尽管SM3算法的时间开销略高于SHA-256和MD5, 但其在安全性上具有明显优势。本文方案在时间效率上的性能损耗在可接受范围内, 为可修订区块链提供了一个高效、安全的底层构造。

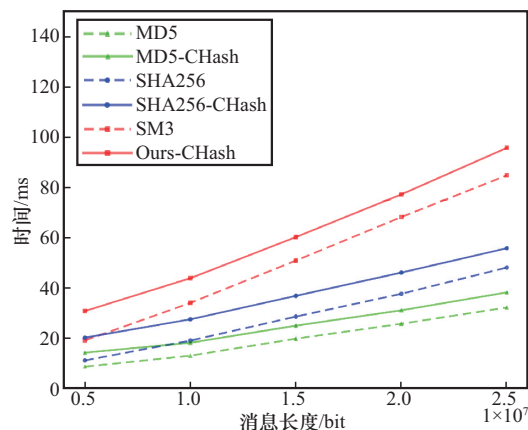


图2 哈希算法时间开销对比

Figure 2 Comparison of time overhead CHash algorithms

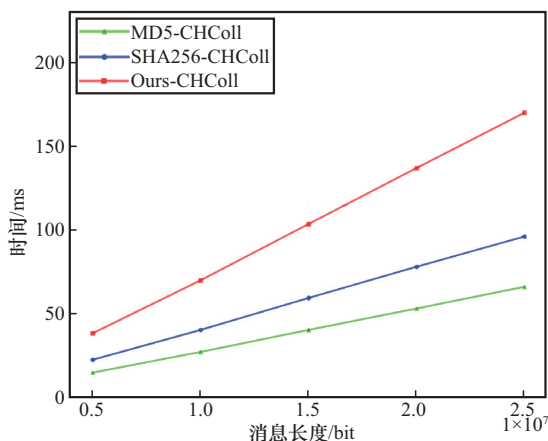


图3 哈希碰撞算法时间开销对比

Figure 3 Comparison of time overhead CHColl algorithms

6 结束语

本文提出了一种基于SM3的变色龙哈希函数，并在*l*-SDH困难问题假设下证明了方案的安全性。实验结果表明，本文方案在实现可修订功能过程中引入的额外时间开销是合理可控的。该方案的提出为可修订区块链提供了基于国密算法的密码学底层原语设计，加速了区块链关键技术国产化进程，对区块链核心技术自主创新发展及国密算法的推广应用具有重要意义。

参考文献:

- [1] VOIGT P, VON DEM BUSCHE A. The EU general data protection regulation (GDPR): a practical guide[M]. 1st ed. Cham, Switzerland: Springer, 2017.
- [2] 新华社. 中华人民共和国个人信息保护法[EB]. 2021 Xinhua News Agency. Personal information protection law of the People's Republic of China [EB]. 2021.
- [3] ATENIESE G, MAGRI B, VENTURI D, et al. Redactable blockchain - or - rewriting history in bitcoin and friends[C]//Proceedings of the 2nd IEEE European Symposium on Security and Privacy. Paris, Washington: IEEE, 2017: 111-126.
- [4] 国家密码管理局. GM/T 0004—2012: SM3 密码杂凑算法[S]. 北京: 中国标准出版社, 2012. State Cryptography Administration. GM/T 0004-2012: SM3 cryptographic Hash algorithm[S]. Beijing: China Standards Press, 2012.
- [5] GENNARO R. Multi-trapdoor commitments and their applications to proofs of knowledge secure under concurrent man-in-the-middle attacks[C]//Advances in Cryptology-CRYPTO 2004. Berlin: Springer, 2004: 220-236.
- [6] KRAWCZYK H, RABIN T. Chameleon hashing and signatures[C]//Proceedings of the the 26th Network and Distributed System Security Symposium. Reston VA: The Internet Society, 2000.
- [7] ATENIESE G, DE MEDEIROS B. Identity-based chameleon hash and applications[M]//Financial Cryptography. Berlin: Springer, 2004: 164-180.
- [8] ATENIESE G, DE MEDEIROS B. On the key exposure problem in chameleon hashes[C]//Security in Communication Networks. Berlin, Springer, 2005: 165-179.
- [9] CHEN X F, ZHANG F G, KIM K. Chameleon hashing without key exposure[C]//Information Security. Berlin: Springer, 2004: 87-98.
- [10] CAMENISCH J, DERLER D, KRENN S, et al. Chameleon-hashes with ephemeral trapdoors: and applications to invisible sanitizable signatures[C]//Public-Key Cryptography-PKC 2017. Berlin: Springer, 2017: 152-182.
- [11] KRENN S, PÖHLS H C, SAMELIN K, et al. Chameleon-hashes with dual long-term trapdoors and their applications[C]//Progress in Cryptology-Africacrypt 2018. Cham: Springer, 2018: 11-32.
- [12] DERLER D, SAMELIN K, SLAMANIG D. Bringing order to chaos: the case of collision resistant chameleon-Hashes[C]//Proceedings of the 23rd International Conference on Practice and Theory of Public-Key Cryptography, Amsterdam Netherlands. Berlin: Springer, 2020: 462-492.
- [13] LI Y M, LIU S L. Tagged chameleon hash from lattices and application to redactable blockchain[C]//Proceedings of the 27th International Workshop on Practice and Theory in Public Key Cryptography. Berlin: Springer, 2024: 288-320.
- [14] WANG Z W, LAN L W, YIU S. Chameleon hash based efficiently updatable oblivious key management[J]. IEEE Transactions on Services Computing, 2023, 16(6): 4503- 4513.
- [15] GUO S, ZENG D Z, XIANG Y. Chameleon hashing for secure and privacy-preserving vehicular communications[J]. IEEE Transactions on Parallel and Distributed Systems, 2014, 25(11): 2794 2803.
- [16] KUMAR R, BHALAJI N. Blockchain based chameleon hashing technique for privacy preservation in e-governance system[J]. Wireless Personal Communications, 2021, 117(2): 987-1006.
- [17] DERLER D, SAMELIN K, SLAMANIG D, et al. Fine-Grained and controlled rewriting in blockchains: chameleon-hashing gone attribute-based[C]//Proceedings of the 26th Network and Distributed System Security Symposium. Reston VA: The Internet Society, 2019.
- [18] BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-policy attribute-based encryption[C]//Proceedings of the 28th IEEE Symposium on Security and Privacy. Washington: IEEE Computer Society, 2007: 321-334.
- [19] DEUBER D, MAGRI B, THYAGARAJAN S A K. Redactable blockchain in the permissionless setting[C]//Proceedings of the 2019 IEEE Symposium on Security and Privacy (SP). Piscataway: IEEE Press, 2019: 124-138.
- [20] MA J H, XU S M, NING J T, et al. Redactable blockchain in decentralized setting[J]. IEEE Transactions on Information Forensics and Security, 2022, 17: 1227-1242.
- [21] TIAN Y, LI N, LI Y, et al. Policy-based chameleon hash for blockchain rewriting with black-box accountability[C]//Proceedings of the Annual Computer Security Applications Conference. New York: ACM, 2020: 813-828.
- [22] XU S M, NING J T, MA J H, et al. Revocable policy-based chameleon hash[C]//Proceedings of the 26th European Symposium on Re-

- search in Computer Security. Berlin: Springer, 2021: 327-347.
- [23] JIA M, CHEN J, HE K, et al. Redactable blockchain from decentralized chameleon Hash functions[J]. IEEE Transactions on Information Forensics and Security, 2022, 17: 2771-2783.
- [24] TIAN Y G, MIYAJI A, MATSUBARA K, et al. Revocable policy-based chameleon Hash for blockchain rewriting[J]. The Computer Journal, 2023, 66(10): 2365-2378.
- [25] DUAN J K, WANG W, WANG L C, et al. Controlled redactable blockchain based on T-times chameleon hash and signature[J]. IEEE Transactions on Information Forensics and Security, 2024, 19: 7560-7572.
- [26] GAO W, CHEN L Q, RONG C M, et al. Security analysis and improvement of a redactable consortium blockchain for industrial Internet-of-things[J]. The Computer Journal, 2022, 65(9): 2430-2438.
- [27] LU Y S, TANG X J, LIU L, et al. Speeding at the edge: an efficient and secure redactable blockchain for IoT-based smart grid systems[J]. IEEE Internet of Things Journal, 2023, 10(14): 12886-12897.
- [28] ZHANG T S, WU Q, MU Y, et al. Redactable block-chain-enabled hierarchical access control framework for data sharing in electronic medical records[J]. IEEE Systems Journal, 2023, 17(2): 1962-1973.
- [29] XU J, XUE K P, TIAN H Y, et al. An identity management and authentication scheme based on redactable blockchain for mobile networks[J]. IEEE Transactions on Vehicular Technology, 2020, 69(6): 6688-6698.
- [30] 杨中皇, 何便便. 基于SM3的Android文件完整性检测系统[J]. 西安邮电大学学报, 2019, 24(6): 22-26.
YANG C H, HE B B. Android file integrity detection tool based on SM3[J]. Journal of Xi'an University of Posts and Telecommun, 2019, 24(6): 22-26.
- [31] 郑东, 赵月. 基于SM3与多特征值的Android恶意软件检测[J]. 信息网络安全, 2020, 20(6): 17-25.
ZHENG D, ZHAO Y. Android malware detection based on SM3 and multi-feature[J]. Netinfo Security, 2020, 20(6): 17-25.
- [32] 区永通, 陈重辰, 谭浩彬, 等. 基于SM3算法的智能配电网报文安全认证方法[J]. 机电工程技术, 2024, 53(2): 263-266.
QU Y T, CHEN Z C, TAN H B, et al. SM3-based intelligent distribution network message security authentication method[J]. M&E Engineering Technology, 2024, 53(2): 263-266.
- [33] 孙思维, 刘田雨, 关志, 等. SPHINCS+-SM3: 基于SM3的无状态数字签名算法[J]. 密码学报, 2023, 10(6): 1266-1278.
SUN S W, LIU T Y, GUAN Z, et al. SPHINCS+-SM3: SM3-based stateless digital signature scheme[J]. Journal of Cryptologic Research, 2023, 10(6): 1266-1278.
- [34] 孙思维, 刘田雨, 关志, 等. 基于杂凑函数SM3的后量子数字签名[J]. 密码学报, 2023, 10(1): 46-60.
SUN S W, LIU T Y, GUAN Z, et al. SM3-based post-quantum digital signature schemes[J]. Journal of Cryptologic Research, 2023, 10(1): 46-60.
- [35] 陈学雷, 付勇, 王美琴. 基于SM3并行实现的SM2-KDF快速实现算法[J]. 密码学报, 2023, 10(4): 813-822.
CHEN X L, FU Y, WANG M Q. Optimized implementation of SM2-KDF based on parallel SM3[J]. Journal of Cryptologic Research, 2023, 10(4): 813-822.
- [36] JOUX A, NGUYEN K. Separating decision Diffie-Hellman from computational Diffie-Hellman in cryptographic groups[J]. Journal of Cryptology, 2003, 16(4): 239-247.
- [37] BONEH D, LYNN B, SHACHAM H. Short signatures from the Weil Pairing[J]. Journal of Cryptology, 2004, 14(4): 297-319.
- [38] BONEH D, BOYEN X. Short signatures without random oracles[C]// Proceedings of the 2004 International Conference on the Theory and Applications of Cryptographic Techniques, IBM Zurich Research Laboratory. Berlin: Springer, 2004: 56-73.

[作者简介]



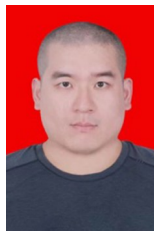
赵宪鑫 (1999-), 男, 河南安阳人, 福建师范大学硕士生, 主要研究方向为密码学、应用密码学。



马金花 (1990-), 女, 江苏新沂人, 博士, 福建师范大学讲师, 主要研究方向为密码学、应用密码学。



严笑天 (2000-), 男, 浙江绍兴人, 福建师范大学硕士生, 主要研究方向为密码学、应用密码学。



许胜民 (1989-), 男, 山东荣成人, 博士, 福建师范大学教授、博士生导师, 主要研究方向为密码学、应用密码学。