计算机科学
COMPUTER SCIENCE

基于多用户变色龙哈希的可修正联盟链方案设计

康重, 王卯宁, 马小雯, 段美姣

引用本文

康重, 王卯宁, 马小雯, 段美姣. 基于多用户变色龙哈希的可修正联盟链方案设计[J]. 计算机科学, 2024, 51(6A): 230600004-6.

KANG Zhong, WANG Maoning, MA Xiaowen, DUAN Meijiao. New Design of Redactable Consortium Blockchain Scheme Based on Multi-user Chameleon Hash [J]. Computer Science, 2024, 51(6A): 230600004-6.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.230600004

基于多用户变色龙哈希的可修正联盟链方案设计

康 重 王卯宁 马小雯 段美姣
中央财经大学信息学院 北京 102206
(kangzhong123@gmail.com)

摘 要 因存在缺乏数据监管策略、数据包含可疑或有害信息、数据上链后无法修改等问题,现有的区块链架构容易成为低成本网络犯罪的法外场所,因而限制了其可用性。可修正区块链方案被认为是解决这一问题的有效途径,但如何将这一理念与联盟链的优势相结合是一个尚未解决的技术问题。为此,所提方案扩展了变色龙哈希函数的概念到多用户情形,引入群组公钥,完善了单一用户持有密钥导致的修改权限中心化问题。在此基础上,提出了一种面向联盟链的可修正区块链方案,采用请求修改-修改验证的两阶段模式完成修改功能。在通用模型和随机预言模型下,基于离散对数问题困难假设,分别证明了所提方案是抗碰撞的和多用户安全的。仿真实验和对比分析论证了所提方案的有效性和可用性。

关键词:可修正区块链;变色龙哈希;联盟链;多用户;分叉引理;离散对数问题
中图分类号 TP309;TP311.13

New Design of Redactable Consortium Blockchain Scheme Based on Multi-user Chameleon Hash

KANG Zhong, WANG Maoning, MA Xiaowen and DUAN Meijiao
School of Information, Central University of Finance and Economics, Beijing 102206, China

Abstract Due to the lack of supervision strategies, the inclusion of suspicious or harmful information, and the inability to modify data after being uploaded to the chain, the existing blockchain architecture is likely to become an extrajudicial place for low-cost cybercrime, thus limiting its usability. The redactable blockchain scheme is considered to be an effective way to solve this problem, but how to combine this concept with the advantages of the consortium blockchain is an unresolved technical problem. To this end, in this paper, a new cryptographic scheme is put forward, which extends the concept of chameleon hash functions to multi-user scenarios by introducing the group key, and improves the solution to the problem of centralized modification rights caused by a single user holding the whole trapdoor key. On this basis, a consortium-oriented redactable blockchain scheme is proposed, which adopts a two-stage model of request-verification to complete the modification. Under the general model and random oracle model, based on the discrete logarithm assumption, it is proved that the scheme is collision-free and multi-user secure. Simulation experiments and comparative analysis also demonstrate the effectiveness and usability of the scheme.

Keywords Redactable blockchain, Chameleon hash, Consortium blockchain, Multi-user, Forking lemma, Discrete logarithm problem

1 引言

随着区块链技术应用领域的不断拓展[1-4],人们逐渐意识到,在保证用户数据安全的同时,区块链系统也存在着存储非法和虚假信息的可能性[5]。更进一步,区块链交易信息、智能合约、电子凭证等数据一经发布便无法修改。例如,2016年,在以太坊系统[6]中,THE DAO[7]智能合约出现了严重的程序漏洞,但未能及时修复,造成了巨大的经济损失和资源浪费。因此,为了防止虚假信息、恶意或者错误交易、合约漏洞给用户和系统造成巨大损失,区块链在得到普遍应用之前,应首先解决这一系列可能会遇到的问题。此时,可修正区块链作为一类潜在的解决方案,成为了近年来学者们研究的热点。

截至目前,较为实用的是Ateniese等[8]于2017年提出的基于变色龙哈希函数[9]的可修正区块链方案。利用变色龙哈希函数的特点,其在修改区块数据的同时保证哈希值不变,进而实现区块链的可编辑功能。随后,埃森哲(Accenture)公司进行了系统原型开发并已经获得与之对应的技术专利,其可用性得到了产业界认可。在此基础上,后续研究者基于可链接、审计与追责等变色龙哈希函数的扩展属性,不断进行功能完善[10-13]。但现有的研究往往针对公共区块链,而对于联盟链这一类具有用户准入机制的区块链架构,如何细粒度、分布式地控制区块修改权限是一个有待解决的技术问题。

基金项目:国家自然科学基金(61907042,61702570);北京市自然科学基金(4194090);四川省教育厅人文社会科学重点研究基地科技金融与创业金融研究中心课题(JR2018-2)
This work was supported by the National Natural Science Foundation of China(61907042,61702570), Natural Science Foundation of Beijing, China(4194090) and Project of Research Center for Science and Technology Finance and Entrepreneurship Finance, Key Research Base of Humanities and Social Sciences, Sichuan Provincial Department of Education(JR2018-2).
通信作者:王卯宁(13854139297@139.com)

因此，本文在原有的变色龙哈希函数基础上进行扩展与改进，引入群组公钥，通过离散对数密码体制中指数同态可加性实现单用户到多用户的转变，并应用于联盟链场景中，提出两阶段式区块修改方案，用户组中的每个用户都可以通过自身私钥对区块内容发起修改请求，实现了多用户的可修正区块链方案。更进一步，本文在通用模型和随机预言模型下对方案进行了形式化数学证明，论证其安全性；同时，进行了仿真实验以验证方案的有效性和可用性。最后对本文方案进行分析，并和现有其他方案进行对比分析。

2 相关知识

2.1 变色龙哈希函数

变色龙哈希函数是一种特殊类型的哈希函数，它可以利用陷门密钥信息构造哈希碰撞[9]。形式上，对于任意消息 m 和随机选择的参数 r，给定一个陷门密钥 sk，陷门拥有者可以找到消息对 (m,r) 和 (m',r') 构造变色龙哈希函数碰撞，即 $CH(m,r)=CH(m',r')$，其中 CH 代表变色龙哈希函数且 $m\neq m'$。

一个标准的变色龙哈希函数由 4 个多项式时间算法组成。

1) $Setup(1^k)\rightarrow\{params\}$：输入一元字符串 1^k，k 为安全参数，输出公共参数 $params$。

2) $KeyGen\rightarrow\{sk,pk\}$：一种概率算法，为每个用户输出私钥 sk 以及相应的公钥 pk。

3) $Single\text{-}Hash(pk,m,r)\rightarrow\{h\}$：算法输入公钥 pk、消息 m 和随机因子 r，输出哈希值 h。

4) $Single\text{-}Forge(sk,m,m',r)\rightarrow\{r'\}$：一种有效的概率算法输入消息 m、随机因子 r 和其他消息 m'，输出随机因子 r' 使得如下等式成立：$Single\text{-}Hash(pk,m,r)=Single\text{-}Hash(pk,m',r')$。

2.2 联盟链

联盟链是一种特殊的区块链网络[14]，它是由一组预选节点组成，这些节点需要经过授权才能参与到该网络中。与公共区块链不同，联盟链的参与者必须是经过身份验证和授权的实体，例如企业、政府机构或其他组织。相比公共区块链，联盟链更加适合于需要高度控制和保密的场景，例如银行、保险、供应链管理等领域。

由于联盟链的参与者需要进行身份验证和授权，因此该网络通常拥有更高的吞吐量和更快的交易确认速度。此外，联盟链还可以提供更高的隐私保护，因为参与者之间可以进行加密通信和数据共享，以保护敏感信息的安全。这些优势吸引越来越多企业和政府机构的关注和应用。

2.3 可修正区块链

目前可修正区块链方案的研究思路分为基于密码学[8,15-16]和基于非密码学[17]两种。本文主要关注 Ateniese 等提出的框架[8]，此类方案通常将区块链的内层哈希函数替换为变色龙哈希函数，在不改变内层哈希函数输出结果的前提下实现区块链的数据修改。具体来说，可修正区块链每个区块结构的描述如以下四元组所示：

$$B=\langle S,X,Ctr,R\rangle,S\in\{0,1\}^l,X\in\{0,1\}^*,Ctr\in\mathbb{N}$$

其中，S 为前一区块的哈希值，长度为 l；X 为当前区块的数据，它可以为任意长度值；Ctr 为当前区块共识过程中产生的随机数；R 为当前区块内层变色龙哈希函数中的随机值。当如下等式成立时，则称可修正区块 B 有效。

$$validblock_Q^D(B)=(H(Ctr,Ch.Hash(\bigcup_{i=1}^{n}\{pk_i\},\tau,(S,X),R)<D)\cap(Ctr<Q)$$

其中，$H:\{0,1\}^*\rightarrow\{0,1\}^l$ 为外层哈希函数，$Ch.Hash:\{0,1\}^*\rightarrow\{0,1\}^K$ 为内层哈希函数，该函数为变色龙哈希函数，同时内外层两个为抗碰撞的哈希函数。参数 $D\in\mathbb{N}$ 为区块链的当前困难层次（即生成新区块的哈希值范围），$Q\in\mathbb{N}$ 为当前限定时间最大哈希请求数。设可修正区块链 C 的链头为 $Head(C)=\langle S,X,Ctr,R\rangle$，若添加新的区块为 $B'=\langle S',X',Ctr',R'\rangle$，则区块 B' 满足 $S'=H(Ctr,Ch.Hash(\bigcup_{i=1}^{n}\{pk_i\},\tau,(S,X),R))$ 为前一区块的哈希值。更新之后的新区块链为 $C'=C\parallel B'$。

图 1 可修正区块链结构图

Fig. 1 Redactable blockchain structure

3 方案设计

3.1 多用户变色龙哈希函数

为了解决单一用户持有密钥导致的修改权限中心化问题，本文提出了多用户变色龙哈希函数方案，其基于群组密钥管理，允许任意合法群组中的成员代表请求区块修改。

具体来说，多用户变色龙哈希函数在 2.1 节所述单用户变色龙哈希函数 4 个多项式时间算法的基础上增加：

1) $Multi\text{-}Hash(\bigcup_{i=1}^{n}\{pk_i\},m,r)\rightarrow\{h\}$：算法输入 n 个用户公钥、消息 m 和随机因子 r，输出对应于输入参数的哈希值 h。

2) $Multi\text{-}Forge(\bigcup_{i=1}^{n}\{sk_i\},m,m',r)\rightarrow\{r'\}$：算法输入 n 个用户私钥、消息 m、不同于消息 m 的待碰撞消息 m'、哈希值 h 和随机因子 r，输出随机因子 r' 使得如下等式成立：$Multi\text{-}Hash(\bigcup_{i=1}^{n}\{pk_i\},m,r)=Multi\text{-}Hash(\bigcup_{i=1}^{n}\{pk_i\},m',r')$，等式中用户公钥和该用户私钥相对应。

Single-hash 和 *Single-Forge* 算法的安全要求与普通变色龙哈希函数相同。其中，语义安全性对应于哈希值的随机性，因此同样适用于 *Single-Hash* 和 *Multi-Hash* 算法。此外，*Multi-Hash* 和 *Multi-Forge* 算法还应该满足以下安全要求。

1) 抗碰撞性。输入给定的 n 个用户公钥 $\bigcup_{i=1}^{n}\{pk_i\}$、消息 m、随机因子 r 和消息 m'，在没有对应 n 个用户私钥的情况下，找到随机因子 r' 使得等式 $Hash(\bigcup_{i=1}^{n}\{pk_i\},m,r)=Hash$

$(\bigcup_{i=1}^{n}\{pk_i\},m',r')$成立在计算上是不可行的。

2)多用户安全性。对于至少存在1名诚实用户的变色龙哈希方案,一个输入仅是公开数据、能够多项式次访问随机预言机的概率多项式时间敌手,在不持有诚实用户私钥情况下,不能有效地找到一个能够通过验证的伪造碰撞。

3.2　具体方案

本节在3.1节所述的框架基础上,给出了一个基于离散对数困难问题的多用户变色龙哈希函数的具体构造。更进一步,基于其对多用户应用环境的满足性,将其扩展为面向联盟链的可修正区块链方案。该方案的正确性与安全性证明分别在4.1节、4.2节给出。

1)$Chameleon.Setup(1^K)\rightarrow\{params\}$:令 p 为 K 比特长度的安全素数,使得 $p=2q+1$ 成立,其中 q 也为素数。记 g 为阶为 q 的有限域 $\mathbb{Z}_p^*$ 的二次剩余类子群的生成元,此时 g 可以由 $\mathbb{Z}_p^*$ 的本原元取2次幂得到。预先给定一个哈希函数 H_e,它可以将任意长度的字符串输入映射到固定长度的字符串。

2)$Chameleon.KeyGen\rightarrow\{sk_i,pk_i\}$:用户私钥 sk_i 是从 $\{2,\cdots,q-1\}$ 随机选择出来的,对应的公钥 pk_i 为 g^{sk_i}。特别地,对应于单用户情形,记私钥 sk 对应的公钥为 $y=g^{sk}$。

3)$Chameleon.Single\text{-}Hash(pk,m,\tau,R)\rightarrow\{h\}$:记 $R=(r,s)\in\mathbb{Z}_q^2$,计算 $e=H_e(\tau,m,r)$ 和 $h=r-(y^e g^s \bmod p) \bmod q$。

4)$Chameleon.Single\text{-}Forge(sk,m,m',\tau,R)\rightarrow\{R'\}$:令 $h=Chameleon.Hash(m,\tau,R)$,其中 $e=H_e(\tau,m,r)$。用户从 $\{1,2,\cdots,q-1\}$ 随机选择 k',设修改的目标数据为 m',计算 $r'=h+(g^{k'} \bmod p) \bmod q$,$e'=H_e(\tau,m',r')$ 和 $s'=k'-e'sk \bmod q$,记 $R'=(r',s')$。

5)$Chameleon.Multi\text{-}Hash(\bigcup_{i=1}^{n}\{pk_i\},m,\tau,R)\rightarrow\{h\}$:每个用户 i 从 $\{1,2,\cdots,q-1\}$ 随机选择一个 k'_i,并计算 $g_i=g^{k'_i}$。记用户组的组公钥为 $y=\prod_{i=1}^{n}g^{sk_i}$,记 $R=(r,s)\in\mathbb{Z}_q^2$,计算 $h=r-(y^e g^s \bmod p) \bmod q$。

6)$Chameleon.Multi\text{-}Forge(\bigcup_{i=1}^{n}\{sk_i\},m,m',\tau,R)\rightarrow\{R'\}$:用户组中的任意用户收到这些 g_i 后,计算 $r'=h+\prod_{i=1}^{n}g_i \bmod p$ 和 $e'=H_e(\tau,m',r')$,进而每个用户 i 可以计算得到 $\phi_i=k_i'-e'sk_i \bmod q$。当用户组中的任意用户收到这些 ϕ_i 后,可以计算 $s'=\sum_{i=1}^{n}\phi_i \bmod q$。输出 $R'=(r',s')$。

3.3　两阶段联盟链修改

在区块链中,设区块 $B=\langle S,X,Ctr,R\rangle$ 和区块 $B'=\langle S',X',Ctr',R'\rangle$ 相互连接,两个区块的标识符分别为 τ 和 τ',满足 $S'=H(Ctr,Ch.Multi\text{-}hash(\bigcup_{i=1}^{n}\{pk_i\},\tau,(S,X),R))$。设联盟链中的合法用户组为 $P_1,P_2,\cdots,P_N$,每个用户节点可以通过构造变色龙哈希函数碰撞对区块内容进行修改,主要分为两个阶段。

1)请求修改阶段

(1)当联盟链中的用户 P_s,$s\in\{1,2,\cdots,N\}$ 需要进行修改时,用户发送更改请求 R_s,其中描述请求将联盟链中某一个历史区块的内容 X 修改为 X',同时用户使用私钥 sk_s 对修改请求进行签名得到 σ_s,然后广播 (R_s,σ_s) 给用户组中的其他用户,开启请求修改阶段。

(2)联盟链中其他用户监听到修改请求后,通过用户公钥 g^{sk_s} 和签名 σ_s 验证用户 P_s 是否是合法用户,若同意修改,则对请求 (R_s,σ_s) 签名并发回给用户 P_s。

(3)用户 P_s 收到所有用户返回签名并使用相应公钥验证后,即联盟链中所有用户节点都同意用户 P_s 的修改请求后,用户 P_s 广播这些表明其他用户节点同意修改的签名。

2)修改和验证阶段

(1)用户 P_s 和联盟链中其他节点进行如下交互:其他每个用户 i 计算 $g_i=g^{k_i'}$,其中 k_i' 从 $\{1,2,\cdots,q-1\}$ 随机选择,并将 g_i 发送给用户 P_s;用户 P_s 收到这些 g_i 后,计算 $r'=h+\prod_{i=1}^{n}g_i \bmod p$ 和 $e'=H_e(\tau,X',r')$,并将 (r',e') 广播给联盟链中的其他用户;进而每个用户 i 可以计算得到 $\phi_i=k'_i-e'sk_i \bmod q$,并将 ϕ_i 发送给用户 P_s;当用户 P_s 收到这些 ϕ_i 后,可以计算 $s'=\sum_{i=1}^{n}\phi_i \bmod q$,得出 $R_1'=(r',s')$,这意味着用户 P_s 生成的 R'_1 使得:$Ch.Multi\text{-}Hash(\bigcup_{i=1}^{n}\{pk_i\},\tau',(S',X'),R')=Ch.Multi\text{-}Hash(\bigcup_{i=1}^{n}\{pk_i\},\tau',(S',X'_1),R_1')$ 成立,也就是说通过构造变色龙哈希碰撞,用户 P_s 完成对区块内容的修改。

(2)用户 P_s 广播 (X',R_1')、其他用户节点监听到广播信息后,验证 X' 是否与第一阶段中请求 R_s 所描述内容一致。如果验证通过,则进一步验证内层变色龙哈希函数值是否相等。最后验证通过,用户节点记录更改后区块并将上一步用户 P_s 广播的所有内容进行标记。

如图2所示,可以看出用户 P_s 修改区块内容后根据伪造的 R' 计算哈希值,而内层哈希值保持不变,即通过内层变色龙哈希函数碰撞实现了可修正区块链方案。特别地,对于本方案,用户组中任意用户都可以修改当前区块的内容,修改后内层哈希值保持不变,实现了多用户的可修正区块链方案。

对于非法用户,根据多用户哈希函数的抗碰撞性,用户在不具有用户组中其他用户提供陷门信息情况下无法构造内层哈希函数碰撞,进而无法实现对区块的修改。

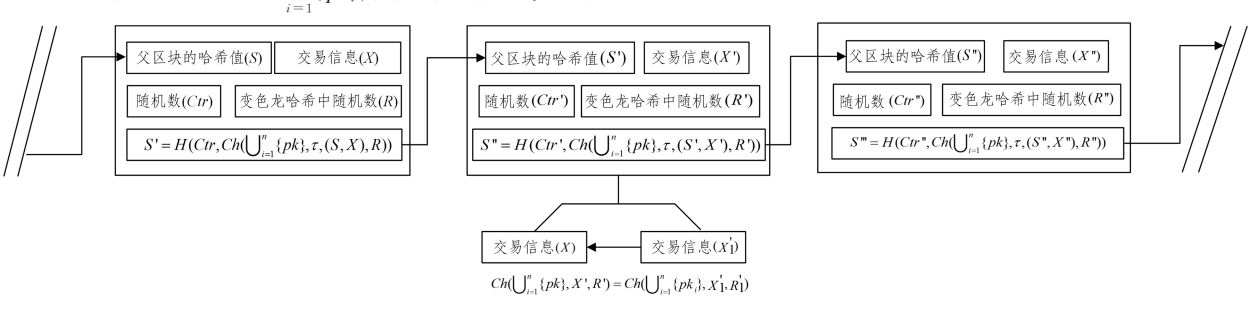

图2　可修正区块方案

Fig. 2　Redacable block scheme

4 安全性分析

本节首先分析了多用户可修正区块链方案的正确性，并在离散对数困难问题假设下对方案进行了形式化的安全性证明。

4.1 正确性验证

设构造的变色龙哈希碰撞值为h'，则有：

$$h'=r'-(y^{e'}g^{s'} \bmod p) \bmod q$$

$$=h+(\prod_{i=1}^{n} g_i \bmod p) \bmod q-(g^{\sum_{i=1}^{n} sk_i e'} g^{\sum_{i=1}^{n} \phi_i \bmod q} \bmod p) \bmod q$$

$$=h+(g^{\sum_{i=1}^{n} k_i'} \bmod p) \bmod q-(g^{\sum_{i=1}^{n} sk_i e'+\sum_{i=1}^{n} k_i'-\sum_{i=1}^{n} sk_i e'} \bmod p) \bmod q$$

$$=h+(g^{\sum_{i=1}^{n} k_i'} \bmod p-g^{\sum_{i=1}^{n} k_i'} \bmod p) \bmod q=h$$

综上，3.2 节提出的方案的正确性得到验证。

4.2 安全性证明

1)抗碰撞性

定理 1 在通用模型框架下[18-19]，单用户变色龙哈希方案碰撞安全性问题等价于关于 g 的离散对数困难问题。

证明：设编码函数 $\sigma(t)=g^t \bmod p(0\leqslant t\leqslant q-1)$，则在通用模型中关于 g 的离散对数困难问题等价于在安全序列 $\sigma((a_i+b_i x) \bmod q)$形式的线性组合中求出 x 的值。

对于给定安全序列$\{z_1,\cdots,z_n\}$，其中z_i为形如$g^{a_i+b_i x}$的元素，$x=sk$，敌手 F 返回 R 和 R'，分别对应哈希值 h 和 h'。对于此类通用型敌手 F，在 sk 为随机选取的前提下，(m,R)和(m',R')构成一对碰撞，即 $h=h'$的概率可忽略。证明过程如下。

(1)当 $s+ex,s'+e'x$ 中有一个和安全序列$\{z_1,\cdots,z_n\}$中的一个元素指数相同时，不妨设 $s+ex$ 与z_i相同，即$g^{s+ex}=g^{a_i+b_i x}$，此时 $x=(a_i-s)(e-b_i)^{-1} \bmod q$。已知 $p=2q+1$，可得出$z_i=(r-h \bmod q) \bmod p$ 或$((r-h) \bmod q+q) \bmod p$。由于 $h=r-z_i \bmod q$，则 $h=h'$的概率为$\frac{2}{p}$。

(2)当 $s+ex,s'+e'x$ 两个都出现在安全序列中，又 $i=j$ 时，即 $g^{s+ex}=g^{s'+e'x}=g^{a_i+b_i x}$。设 H_e 的碰撞概率为 $\frac{1}{q_H}$，即 $\Pr(e=e')=\frac{1}{q_H}$，此时概率$\frac{1}{q_H}$为可忽略大小。由于 $e=e'$时，只能 $s=s'$，则 $R=R'$，不满足变色龙哈希碰撞的条件，即不存在此类情况。

(3)当 $s+ex,s'+e'x$ 两个都出现在安全序列中时，又 $i\neq j$，即$g^{s+ex}=g^{a_i+b_i x}=z_i$，$g^{s'+e'x}=g^{a_j+b_j x}=z_j$。由于 $h=(r-z_i) \bmod q=(r'-z_j) \bmod q$，可得出$(z_i-z_j) \bmod q=r-r'$。因为 $r-r'$为固定值，$p=2q+1$，即z_i和z_j为满足上述等式条件的概率为$\frac{2}{n}$。安全序列中共有C_n^2对z_i和$z_j(i\neq j)$，即成功构造变色龙哈希碰撞的概率为 $O\left(\frac{2n^2}{p}\right)$。

上述证明过程对于多用户情形同样适用。

2)多用户安全性

定理 2 在随机预言模型下[20]，对于多用户变色龙哈希方案，如果该方案对多项式时间敌手 F 来说不安全，则存在一个多项式时间算法 A 可以违反离散对数困难问题假设。

证明：假设给定算法 A 一个离散对数问题实例 p,q,g,y，A 需要计算出一个$t\in[0,q-1]$使得$g^t\equiv y \bmod p$用于解决离散对数困难问题(DLP)。

利用敌手 F 来攻击 DLP 假设：假设算法 A 被给予一个关于的 DLP 的实例，即 p,q,g,y，同时用户 i 是用户组 S 中唯一不被算法 A 操控的用户，并使用户 i 的公钥$y_i=y$。然后，算法 A 运行敌手 F 并回复敌手 F 的变色龙哈希碰撞查询。

假设敌手 F 共对H_e进行q_H次哈希查询，每次查询结果都由算法 A 提前随机选择好，分别为$e_1,\cdots,e_{q_H}$。对于非用户 i 的其他用户，由于算法 A 知道其私钥信息，因此可以按正常计算过程回答敌手 F 所需碰撞值。接下来，为了回答敌手 F 对用户 i 的变色龙哈希碰撞查询，此时，算法 A 需要进行如下步骤：(1)在 1 到q_H中随机选择j_0；(2)随机选择 $\phi\in[0,q-1]$；(3)当收到敌手 F 发送的(τ,m,m',R)，其中 $R=(r,s)$时，算法 A 计算$g_i=y_i^{e_{j_0}} g^{\phi} \bmod p$，并将$(h+g_i,\varphi)$发送给敌手 F 作为变色龙哈希碰撞查询的结果。

假设敌手 F 输出一个关于消息m_0变色龙哈希碰撞(m_0',r_0',s_0')，进一步假设该碰撞是基于(τ_0,r_0,s_0,m_0)对哈希函数H_e的第j_0个哈希查询，该哈希查询结果为e_{j_0}。利用“分叉原理”技术：算法 A 保持第一次运行时的数重置敌手 F 并重新运行敌手 F，敌手 F 的第j_0次H_e哈希查询结果为新的随机数e'_{j_0}，其余的哈希查询结果不变。此时，由于敌手 F 使用相同的数重置并得到相同的哈希查询结果，当敌手 F 仍以相同的问答方式构造变色龙哈希碰撞，则前j_0-1次的H_e计算结果不变。如果敌手 F 再次输出一个关于消息m_1的变色龙哈希碰撞(m_1',r_1',s_1')，并且如果该伪造再次基于第j_0个哈希查询，则$m_1=m_0$，$r_1'=r_0'$以及

$$r_0'-(y'^{e_{j_0}} g^{s_0'} \bmod p) \bmod q=r'_1-(y'^{e'_{j_0}} g^{s_1'} \bmod p) \bmod q$$

$$y'^{e_{j_0}} g^{s_0'}=y'^{e'_{j_0}} g^{s_1'} \bmod p$$

$$y'^{e_{j_0}-e'_{j_0}}=g^{s_1'-s_0'} \bmod p$$

$$y'=g^{\frac{s_1'-s_0'}{e_{j_0}-e'_{j_0}}} \bmod p$$

由于$y'=\prod_{j=1}^{n} y_j \bmod p$，算法 A 为了从伪造用户组中提取用户 i 的公钥y_i对应的离散对数，需要除去其用户组 S 中的其他用户的公钥y_{i_j}的离散对数。由于用户组中的其他用户均为算法 A 提前设定，因此算法 A 知道其他用户的私钥信息，故能够分离出y_i，进而通过在$\frac{s_1'-s_0'}{e_{j_0}-e'_{j_0}}$中减掉其他用户私钥来计算其离散对数。定理得证。

5 实验与对比

5.1 仿真实验

方案的实验环境为 Windows11 操作系统，Intel(R)Core(TM) i7-10875H CPU@ 2.30GHz，内存为 16.00GB。基于联盟链的特点，实验设置 $N=100$ 个用户节点，对每种算法进行 20 次重复测试并记录实验结果，每次测试执行 100 次。对于 p,q，方案通过 python 中的 gmpy2 库生成 $\log n=512$ 比特长度的大素数。实验结果及其相对应的理论复杂度评估如表 1 所列，其中 Ge 和 Gm 分别表示$\mathbb{Z}_p$中的幂(exponentiation)和乘法(multiplication)运算，Mean 代表运行时间的平均值(单位为 ms)，Std 代表运行时间的标准差。

表 1　实验结果

Table 1　Experiment results

	Computational Cost	*Mean*	*Std*
KeyGen	$O(\log(\log n))Ge+O((\log n)^3)$	576.11	1068.50
SingleHash	$2Ge+Gm$	15.55	3.98
SingleForge	$3Ge+2Gm$	22.20	4.61
MultiHash	$N(2Ge+Gm)+2Ge+Gm$	1847.55	22.13
MultiForge	$NGm+2Ge+Gm$	46.75	5.71

根据实验结果可以看出,所提方案的运行时间主要在密钥生成和多用户哈希生成阶段。为了实现方案安全性,方案中 p,q 选取 $\log n=512$ 比特长度的大素数,对于素数检测具有一定的运算量要求。但由于 KeyGen 仅在系统建立初始进行一次运算,其计算量对系统整体影响可忽略。在多用户哈希生成阶段,由于多用户变色龙哈希函数需要用户组的公钥才能进行哈希生成。计算用户组的公钥时需要进行一定量的幂运算,因此占据了方案的主要运行时间。

实验进一步设置方案中的不同量级用户节点数量,并记录实验结果,如图 3 所示。

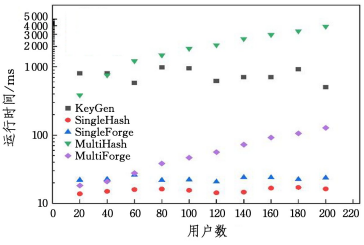

图 3　实验结果散点图

Fig. 3　Scatter plot of results

随着用户节点数量的增加,方案中的多用户哈希生成和伪造阶段的运行时间提升,主要运算仍在用户组的公钥运算上,其与用户规模增加幅度对应。实验结论表明,考虑用户计算与修改区块的平均时间,本文方案并未造成系统过多的额外负载;同时,考虑多用户总体计算量,在用户规模达到 200 级别时,本文方案的运行时间仍在 ms 数量级范围内,达到可用级别,因此本文方案具有实用性。

5.2　方案对比

相比 Ateniese[8] 最早提出的基于变色龙哈希函数的可修正区块链方案,以及近几年陆续提出的同类方案,本文方案通过改进基于离散对数困难问题的变色龙哈希函数,面向联盟链场景实现了多用户的可修正方案。本文方案具有以下优势:

方案适用于以联盟链为代表的多参与方区块链环境中,用户组中的任意合法参与者可以发起对区块进行修改的请求,实现了多用户的可修正区块链方案,避免了由单独一方持有密钥而导致的权限中心化问题。

方案中陷门密钥存在于用户组的各个实体中,修改者修改区块时只需和用户组中的其他实体进行信息交互,利用自己的私钥即可修改区块,不需要使用多方计算和密钥共享等复杂方式,计算简便、效率高且具有可扩展性。

方案中的变色龙哈希函数计算区块链中交易的哈希值,支持细粒度的修正方案。当修改者修改区块时,只需要重新改写相应的交易事务,而不是整个区块的内容,保证了区块链的完整性。

表 2　方案对比表

Table 2　Scheme comparison

方案	年份	困难问题	用户数	安全模型	编辑粒度	可扩展性
Ateniese 等[8]	2017	离散对数	单用户	通用群模型	区块级别	×
Camenisch 等[21]	2017	因子分解及离散对数	单用户	随机预言模型	区块级别	×
Derler 等[10]	2019	—	单用户	强不可区分模型	事务级别	×
Huang 等[22]	2019	计算性 Diffie-Hellman	单用户	—	区块级别	×
Xu 等[23]	2021	—	单用户	w-KE 安全模型	区块级别	√
Wu 等[24]	2021	格上(非齐次)小整数解	单用户	随机预言模型	区块级别	×
Gao[13]	2022	因子分解	单用户	随机预言模型	事务级别	√
本文方案	2023	离散对数	多用户	随机预言模型	事务级别	√

结束语　区块链由于其去中心化和不可篡改性而日益流行,它提供了一种在不受信任的环境中存储和共享数据的新方法。然而,不可篡改性成为一把双刃剑,由于在某些情况下会造成问题,阻碍了区块链的应用。为了解决这一问题,本文重点关注可修正区块链技术。具体来说,本文提出了一种面向多用户的可修正联盟链方案。该方案基于改进的变色龙哈希函数,在严格的数学语言下证明其安全性,进一步解决了单一用户持有密钥导致的中心化问题。与目前同类方案相比,结合了联盟链和可修正区块链的优势,具有支持细粒度、适用多用户、实用性强的特性。在后续的研究中,该方案所对应的系统开发及从应用层面验证其有效性和安全性是进一步的研究方向。此外,设计支持国密算法的自主可控方案也是未来的可行研究方向之一。

参 考 文 献

[1] NAKAMOTO S. Bitcoin: A peer-to-peer electronic cash system [EB/OL]. [2021-12-08]. https://bitcoin.org/bitcoin.pdf.

[2] LI B, XIANG H Y, ZHANG Y X, et al. Application Research of PBFT Optimization Algorithm for Food Traceability Scenarios [J]. Computer Science, 2022, 49(S1): 723-728.

[3] ZHANG B J, LI J, HU K, et al. Distributed Encrypted Voting System Based on Blockchain [J]. Computer Science, 2022, 49(S2): 211000212-6.

[4] LI B, WU H, HE X W, et al. Survey of Storage Scalability in Blockchain Systems [J]. Computer Science, 2023, 50(1): 318-333.

[5] MATZUTT R, HILLER J, HENZE M, et al. A quantitative analysis of the impact of arbitrary blockchain content on bitcoin [C]// International Conference on Financial Cryptography and Data Security. Berlin, Heidelberg: Springer Verlag, 2018: 420-438.

[6] WOOD G. Ethereum: A secure decentralized generalised transaction ledger [J]. Ethereum Project Yellow Paper, 2014, 151(2014): 1-32.

[7] BUTERIN V. Critical Update Re: DAO vulnerability [EB/OL]. https://blog.ethereum.org/2016/06/17/criticalupdate-re-dao-vulnerability/. June 17, 2016.

[8] ATENIESE G, MAGRI B, VENTURI D, et al. Redactable blockchain-or-rewriting history in bitcoin and friends[C]// 2017 IEEE European Symposium on Security and Privacy. IEEE, 2017: 111-126.

[9] KRAWCZYK H M, RABIN T D. Chameleon hashing and signatures: U. S. Patent 6, 108, 783[P]. 2000-08-22.

[10] DERLER D, SAMELIN K, SLAMANIG D, et al. Fine-Grained and Controlled Rewriting in Blockchains: Chameleon-Hashing Gone Attribute-Based[J]. IACR Cryptol. ePrint Arch., 2019: 406. NDSS 2019.

[11] LI P L, XU H X, MA T J, et al. Research on Modifiable Blockchain Technology [J]. Journal of Cryptography, 2018, 5(5): 501-509.

[12] TIAN Y, LI N, LI Y, et al. Policy-based chameleon hash for blockchain rewriting with black-box accountability[C]// Annual Computer Security Applications Conference. 2020: 813-828.

[13] GAO W, CHEN L Q, TANG C M, et al. One-Time Chameleon Hash Function and Its Application in Redactable Blockchain[J]. Journal of Computer Research and Development, 2021, 58(10): 2310-2318.

[14] DIB O, BROUSMICHE K L, DURAND A, et al. Consortium blockchains: Overview, applications and challenges[J]. International Journal On Advances in Telecommunications, 2018, 11(1&2): 51-64.

[15] CHENG L, LIU J, SU C, et al. Polynomial-based modifiable blockchain structure for removing fraud transactions[J]. Future Generation Computer Systems, 2019, 99: 154-163.

[16] GRIGORIEV D, SHPILRAIN V. Rsa and redactable blockchains[J]. International Journal of Computer Mathematics: Computer Systems Theory, 2021, 6(1): 1-6.

[17] LI X, XU J, YIN L, et al. Escaping from consensus: Instantly redactable blockchain protocols in permissionless setting[J]. IEEE Transactions on Dependable and Secure Computing, 2024.

[18] MAURER U, WOLF S. Lower bounds on generic algorithms in groups[C]// Advances in Cryptology—EUROCRYPT'98. Lecture Notes in Computer Science. Springer, Berlin, Heidelbeg, 1998.

[19] MA C, WENG J, LI Y, et al. Efficient discrete logarithm based multi-signature scheme in the plain public key model[J]. Designs, Codes and Cryptography, 2010, 54(2): 121-133.

[20] GUO F, SUSILO W, MU Y. Introduction to Security Reduction [M]. Springer, 2018.

[21] CAMENISCH J, DERLER D, KRENN S, et al. Chameleon-hashes with ephemeral trapdoors[C]// IACR International Workshop on Public Key Cryptography, (Amsterdam, The Netherlands). Springer, 2017: 152-182.

[22] HUANG K, ZHANG X, MU Y, et al. Building redactable consortium blockchain for industrial internet-of-things[J]. IEEE Transactions on Industrial Informatics, 2019, 15(6): 3670-3679.

[23] XU S, NING J, MA J, et al. K-time modifiable and epoch-based redactable blockchain[J]. IEEE Transactions on Information Forensics and Security, 2021, 16: 4507-4520.

[24] WU C, KE L, DU Y. Quantum resistant key-exposure free chameleon hash and applications in redactable blockchain[J]. Information Sciences, 2021, 548: 438-449.

KANG Zhong, born in 2000, postgraduate. His main research interests include blockchain and cryptography.

WANG Maoning, born in 1987, Ph. D, associate professor, is a member of CCF (No. 93508M). Her main research interests include cryptography, blockchain and digital currency.