计算机科学
COMPUTER SCIENCE

一种分散变色龙哈希函数的链上隐私数据编辑机制

黄寿孟, 杨博雄, 杨明

引用本文

黄寿孟, 杨博雄, 杨明. 一种分散变色龙哈希函数的链上隐私数据编辑机制[J]. 计算机科学, 2024, 51(6A): 240100157-5.

HUANG Shoumeng, YANG Boxiong, YANG Ming. Privacy Data Editing Mechanism Based on Distributed Chameleon Hash Function [J]. Computer Science, 2024, 51(6A): 240100157-5.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.240100157

一种分散变色龙哈希函数的链上隐私数据编辑机制

黄寿孟[1,2]　杨博雄[2]　杨　明[3]
1 三亚学院信息与智能工程学院　海南 三亚 572022
2 三亚学院陈国良院士团队创新中心　海南 三亚 572022
3 三亚学院容淳铭院士工作站　海南 三亚 572022

摘　要　随着区块链技术广泛应用于各个领域,数据安全及用户隐私出现了很多未知威胁和挑战。对于恶意携带用户隐私或者携带非法攻击代码的非法交易数据,通过属性策略、变色龙哈希算法,设计了基于多方监控的变色龙哈希碰撞数据编辑机制(DecPRB),该DecPRB机制是在变色龙哈希编辑机制的基础上,优化设计以方便管理的陷门哈希函数,通过计算哈希碰撞实现区块链历史数据编辑,即可将在区块链上公开的那些非法数据(特别是隐私数据或攻击代码)删除,当然在更新编辑过程中,所有修改权限由链上所有节点共同监控。最后通过安全性分析推理出DecPRB机制,既不改变区块链的安全属性,又具有很强的抗攻击能力,再通过仿真实验验证DecPRB机制具有一定的有效性,符合数据安全需求。该DecPRB机制在复杂的分布式网络环境中(特别是分布式的云计算和区块链系统)能有效保护数据安全和隐私问题,对数字经济时代的发展作出一定的贡献。

关键词:哈希函数;隐私数据;编辑机制;变色龙哈希
中图分类号　TP309

Privacy Data Editing Mechanism Based on Distributed Chameleon Hash Function

HUANG Shoumeng[1,2], YANG Boxiong[2] and YANG Ming[3]
1 School of Information & Intelligence Engineering, University of Sanya, Sanya, Hainan 572022, China
2 Academician Guoliang Chen Team Innovation Center, University of Sanya, Sanya, Hainan 572022, China
3 Academician Chunming Rong Workstation, University of Sanya, Sanya, Hainan 572022, China

Abstract　With the widespread application of blockchain technology in various fields, data security and user privacy are faced with many unknown threats and challenges. For illegal transaction data that maliciously carries user privacy or illegal attack code, a chameleon hash collision data editing mechanism (DecPRB) based on multi-party monitoring is designed through attribute strategy and chameleon hash algorithm. This DecPRB mechanism is based on the chameleon hash editing mechanism, optimized and designed with a trapdoor hash function that is easy to manage. By calculating hash collisions, blockchain historical data editing is achieved, illegal data (especially private data or attack code) that is publicly available on the blockchain can be deleted. Of course, during this update and editing process, all modification permissions are jointly monitored by all nodes on the chain. Finally, through security analysis, it is inferred that the DecPRB mechanism does not change the security attributes of the blockchain and has strong anti attack capabilities. Simulation experiments are conducted to verify the effectiveness of the DecPRB mechanism, which meets data security requirements. DecPRB mechanism can effectively protect data security and privacy issues in complex distributed network environments, especially distributed cloud computing and blockchain systems, and make a certain contribution to the development of the digital economy era.

Keywords　Hash function, Privacy data, Editing mechanism, Chameleon hash

1　引言

目前,以区块链技术为主的支付机制被广泛应用于交易业务,如数字金融、电子商务、知识版权、存储服务等,但它在交易记录中容易出现用户隐私信息,这是因为区块链交易自身可追溯性影响制约着交易双方的匿名性,攻击方通过溯源历史交易数据,寻找出交易方的真实身份及关联的地址信息,即将获取该用户的所有商业机密隐私。另外,区块链技术中节点的不可变性被攻击者滥用,攻击者在合法交易中携带恶意数据,如携带恶意代码、错误信息、隐私信息等非法数据,网络上一旦出现这些非法数据,就将产生重大的网络安全案例。如Matzutt等[1]发现了比特币交易业务中的一些非法数据,

基金项目:海南省自然科学基金(622RC735);海南省院士创新平台科研项目资金(YSPTZX202144,YSPTZX202145);三亚学院校级重大项目(USY22XK-04)
This work was supported by the Hainan Provincial Natural Science Foundation of China(622RC735), Specific Research Fund of the Innovation Platform for Academician of Hainan Province(YSPTZX202144, YSPTZX202145) and University of Sanya Major Project(USY22XK-04).
通信作者:黄寿孟(huang123888@126.com)

特别是大量与儿童性内容相关的数据；国际刑警在网络安全执法过程中发现了比特币交易系统中的 251768 号区块节点存储恶意攻击代码。那么保护交易双方的合法隐私和清除恶意非法数据是区块链技术研究的迫切需求，从现有的文献中找到解决这些问题的方案有 3 类应用设计可变区块链的编辑机制，第一类是基于元数据（Mate-Transaction）的编辑机制[2-3]，它主要是交易申请人在交易成功时更新可变区块链节点中的元数据，发布新版本消息，但它的历史记录是存在且可恢复的，还有一点是更新时间是受限制的；第二类是基于共识的编辑机制[4-5]，这种机制采用新的编辑块代替旧的编辑块，算力计算周期长、网络成本高、扩展效率低，无法执行多次更新请求，易出现分叉节点；第三类是基于变色龙哈希编辑机制[6-9]，该机制以密码学公式计算节点中的哈希函数碰撞值，从而实现数据更新，但是此时编辑策略的用户是受信任机构中心授予，这与区块链技术的去中心化理念相悖[10]，因此一旦该机构中心背叛，将对整个网络产生严重的安全威胁，甚至面临惨重的商业经济损失。针对这些缺陷，本文提出了一种多方监管（分散管理）的变色龙哈希函数的区块链数据编辑机制，该机制以基于变色龙哈希编辑机制为基础，优化设计方便管理的陷门哈希函数，通过挑战者和攻击者之间的内外碰撞分析解决数据安全性问题。

2 相关研究

2.1 基于元数据的编辑机制

基于元数据的编辑机制采用更新命令方式 $\mu chain$[2] 修改区块链上的交易数据，即当区块链节点收到交易申请时产生可变编辑的交易状态，并将这种交易更新状态来触发更新命令，让区块链节点实现编辑操作。当然这种更新命令有两种情况，一种扩展交易的更新命令，另一种替换交易的更新命令，这两种更新命令都要预先设置编辑策略（包括编辑者、被编辑者、时间窗等重要信息），整个区块链系统节点对这种可变交易进行验证仲裁，验证通过代表更新记录成功，否则编辑失败。该机制更新命令是为了隐藏交易记录，通过秘密共享进行密钥管理，机制实现算法如算法 1 所示。

算法 1 “基于元数据的编辑机制”实现算法

输入：更新前编辑链上的区块 C，交易状态的记录 Tx，当前编辑策略 P

输出：更新后的区块 C′

1. /* 更新请求 */
2. 发生一次元数据更新交易状态的记录 Tx^*，要求 Tx→Tx′；
3. /* 执行更新命令，先判断是否满足编辑策略，后更新编辑状态 */
4. if 当前状态满足编辑策略 P then
5. 验证是否符合 P，修改元数据交易状态的记录 Tx^* 和 Tx→Tx′；
6. 公开新交易 Tx′，更新节点记录状态，C→C′；
7. else 公开此次交易失败
8. end
9. /* 区块记录更新完成 */
10. 输出更新后的区块 C′

从算法 1 中可知，该机制的编辑实际上是改变交易视图来进行操作，或者说用户也可使用解密密钥将新视图重新修改回旧视图，因此基于元数据的编辑机制存在安全隐患，易受双花攻击和篡改攻击，并且该机制委托第三方可信认证，若第三方出于恶意目的编辑交易信息，将无法保证网络节点的同步编辑操作。

2.2 基于共识的编辑机制

基于共识的编辑机制是依赖区块链技术中的共识规则来实现交易编辑，新交易视图是链上的待编辑区块广播请求编辑消息，在一定周期内达到统一的共识 POW 权限，即可完成编辑机制。通用算法如算法 2 所示，这类机制不依赖第三方信任，完全由区块链的去中心化特征来确保系统的有效性和安全性，也能有效抵抗篡改攻击、双花攻击，但每次编辑会消耗一定交易费用，且需重新计算区块 POW 权限，因此执行成本高、编辑效率低、共识延迟显著，不适合频繁的编辑请求。

算法 2 “基于共识的编辑机制”实现算法

输入：编辑前链上的区块 C，区块高度|C|，编辑时间周期 t

输出：编辑后的区块 C′

1. /* 请求编辑消息 */
2. 公开编辑请求消息并将其广播于所有用户，请求 C 块用户 B 中的记录 Tx→Tx^*；
3. /* 执行编辑请求 */
4. 将用户 B 中的记录 Tx→Tx^*；
5. 统计 Tx^* 新区块 C′的 POW 权限；
6. /* 执行第三方投票信任 */
7. 公开新区块 C′验证操作；
8. while|C|≤t do
9. /* 判断投票信任的费用 */
10. if 区块 C′同时满足 POW 的一致性和有效性 then
11. 对区块 C′投票成功，累计赞成票数；
12. else
13. 投票无效，放弃区块 C′的编辑；
14. end
15. end
16. /* 链上的用户记录更新 */
17. if 赞成票数大于预定的阈值 then
18. 区块链节点用户公开编辑有效；
19. 更新 C′←C；
20. end
21. 输出更新后的区块 C′

2.3 基于变色龙哈希的编辑机制

哈希算法是一种数学函数，其作用是将任意长度的数据（如文件或消息）映射为固定长度的输出，称为哈希值。哈希算法是一种不可逆操作，即无法从哈希值还原出原始数据。本文设变色龙哈希函数为 CH，也可称 CH 为陷门抗碰撞哈希函数，只有公钥的用户能计算有效的碰撞值 Π_{CH}，若有密钥的用户也可计算出变色龙哈希碰撞值 $\Pi_{CH.CHash}$，如果没有密钥或公钥几乎不可能分析出变色龙哈希函数值 Π_{CH}。2017 年 Ateniese 等第一个提出基于标准变色龙哈希函数 $\Pi_{CH.CHash}$ 的编辑机制[11]，给 SHA256 哈希值的编辑公式 $SHA256(CHash(pk,BH,r))\leqslant Target$，其中 pk 为公钥，BH 为可编辑块，r 是随机数。当编辑请求合法时，将原记录 BH 更新为新记录 BH'，这样有密钥的用户能计算出相同的哈希值，即可表示为 $CHash(pk,BH,r)=CHash(pk,BH',r')$。通用算法如算法 3 所示，基于变色龙哈希的编辑机制是让编辑前后的节点数据能映射到同一哈希值上，从而保证主链的节点一致性，不用重新计算 POW 权限，因此计算成本

低，编辑效率高，可频率编辑。

算法 3 “基于变色龙哈希的编辑机制”实现算法

输入：编辑前链上的区块 C

输出：编辑后链上的区块 C′

1./* 构建密钥 */

2.构建生成算法密钥并关联到区块链上的用户；

3./* 生成要交易的记录 */

4.生成 CH 函数的交易记录并增加到区块 C 上；

5./* 发出修改请求 */

6.在链上广播修改消息，区块 C 上的用户交易 Tx→Tx′；

7./* 调用验证算法执行编辑消息 */

8.调用算法 $\Pi_{CH.CHAdapt}$，返回随机值 r′使得 $\Pi_{CH.CHash}(B, r) = \Pi_{CH.CHash}(B', r')$或$\Pi_{CH.CHash}(Tx, r) = \Pi_{CH.CHash}(Tx', r')$；

9.广播交易 Tx′和 r′；

10./* 链更新 */

11. if r′满足正确性 &B′(或交易 Tx′)有效 then

12. 区块 B′替换原始区块 B(或交易 Tx′替换原始交易 Tx)；

13. 更新 C 为链 C′；

14. end

2.4 现有机制评价指标分析

为了更好实现数据安全与隐私保护，本文对现有文献中的 3 类机制进行综合评价，评价指标包括有效性、一致性、兼容性、抗攻击性等 10 项指标，其中有效性指编辑申请成功接受；一致性指编辑后的节点视图保持与原链视图一致；兼容性指该编辑机制可应用于其他区块链系统；高效率指一次编辑请求有效接受的时间；安全属性指该编辑机制不改变原区块链的安全属性；篡改攻击指存在恶意编辑请求；双花攻击指同一编辑请求两次；拒绝服务攻击指攻击方频繁编辑请求使得系统过载瘫痪。具体评价情况如表 1 所列，其中基于元数据的编辑机制不满足的指标有 3 个，即安全属性、抗双花攻击、抗拒绝服务攻击；基于共识的编辑机制不满足的指标也有 3 个，即高效率、无需重新计算 POW、无共识延迟；只有基于变色龙哈希的编辑机制满足或部分满足表 1 中的所有评价指标。

表 1 3 类机制的评价指标情况表

Table 1 Evaluation indicators of three types of mechanism

评价指标	基于元数据	基于共识	基于变色龙哈希
有效性	◎	√	◎
一致性	◎	√	√
兼容性	◎	◎	◎
高效率	◎	×	√
安全属性	×	√	◎
抗篡改攻击	√	√	◎
抗双花攻击	×	√	◎
抗拒绝服务攻击	×	√	◎
无需重新计算 POW	◎	×	√
无共识延迟	◎	×	√

注：√：满足；◎：部分满足；×：不满足。

3 编辑机制

3.1 总体设计

从第 2 章中得知基于变色龙哈希函数的编辑机制的评价性能略高，为了更好地优化安全属性与抗攻击性，本文设计了一种分散变色龙哈希函数的链上隐私数据编辑机制，通过哈希密码学原理完成安全性对抗。该编辑机制有计算哈希碰撞(DACH)和隐私数据编辑(DecPRB)两大模块，其中 DACH 模块是一种分散的基于属性的变色龙哈希函数，能有效计算哈希碰撞，而 DecPRB 模块则是在 DACH 基础上实现抗攻击的区块链隐私可变编辑，也就是说 DACH 模块实现交易签名，DecPRB 实现创建原区块。首先，合法用户提出编辑申请，DACH 模块通过计算哈希碰撞性来验证申请合法性，完成 DACH 值签名，其次提交到 DecPRB 模块以创建新区块，将 DACH 值构建节点 Merkle 树，并确保编辑前后的数据映射到相同哈希值，从而实现编辑数据的更新。

3.2 分散控制

为了实现编辑权限的分散控制设计，本文采用基于属性的加密算法 DCP_ABE[12]，此算法可设计出分散的访问权限来监管陷门密钥，每个陷门密钥通过访问策略进行加密处理，共享于属性认证中心(Attribute Authorities Centrality, AAC)，并由认证中心 AAC 恢复陷门密钥(AA)。这样链上的数据编辑不是某个 AA 监管，而是由 AAC 一起监管，同时 DecPRB 中的 DACH 算法模块Π_{DACH}由 6 个子模块算法组成，具体描述如下。

1)$PPGen$ 算法

初始化算法，根据安全参数 k，初始化公共参数 $pp \leftarrow \{N, G, G_{p1}, g, e\}$，其中 pp 是五元组 $hash$ 算法的标识符，本质是将用五元组的值进行哈希运算所得的运算结果表示这个连接，通常表示成 $pp \leftarrow PPGen(1^k)$。

2)$AASetup$ 算法

陷门密钥 AA 生产算法，根据 pp 设置参数，产生公钥与私钥，计算公式表示为公钥 $pk \leftarrow (mpk, spk)$ 和私钥 $sk \leftarrow (msk, ssk)$，其中 $\{ssk, spk\} \leftarrow \Pi_{DCP\text{-}ABE.AAsetup}(pp)$，$\{msk, mpk\} \leftarrow \Pi_{RSA.RSAKGen}(pp)$，此算法通常表示为 $(pk, sk) \leftarrow AASetup(pp)$。

3)$DKGen$ 算法

密钥构建算法，根据$\{GID, sk, S\}$，即{全局身份，密钥，属性}，计算每个属性 $i \in S$ 构建对应的密钥SK_i，其中 $SK_i \leftarrow \Pi_{DCP\text{-}ABE.KGen}(GID, i, sk)$ 且 $SK_s = \{SK_i \mid i \in S\}$，结果表示为 $SK_i \leftarrow DKGen(GID, sk, i)$。

4)$DHash$ 算法

哈希函数算法，根据消息 m、公钥 pk 和访问结构 $A \subseteq 2^U$，得到哈希碰撞值 h、随机值 r 和更新值 ct，算法公式可表示为 $\{h, r, etd\} \leftarrow \Pi_{CHET.CHash}(pk, m)$，$ct \leftarrow \Pi_{DCP\text{-}ABE.Enc}(etd, A, pk)$，结果表示为 $(h, r, ct) \leftarrow DHash(pk, m, A)$。

5)$Dver$ 算法

检测算法，根据 pk, m, h, r，验证每个用户的 $b \in \{0, 1\}$ 与 h 的有效性，其中 $b \leftarrow \Pi_{CHET.CHVer}(pk, m, h, r)$，结果用公式 $b \leftarrow DVer(pk, m, h, r)$ 来表示。

6)$DAdapt$ 算法

碰撞验证算法，根据SK_s，m, h, r 以及用户的新消息 $m' \in M$，产生随机值 r'，计算碰撞值 $\{r', L\} \leftarrow \Pi_{CHET.CHAdapt}(sk, etd, m, h, r, m')$ 且 $\{etd, L\} \leftarrow \Pi_{DCP\text{-}ABE.Dec}(SK_s, ct)$，结果表示为 $\{r', L\} \leftarrow DAdapt(SK_s, m, h, r, ct, m')$。

下面说明分散控制 $DACH$ 算法满足数据的正确性，假设对于所有的 $k \in N$，$A \subseteq 2^U$，$s \in A$，$i \in S$，$pp \leftarrow PPGen(1^k)$，$(pk, sk) \leftarrow AASetup(pp)$，$GID \in \{0, 1\}^*$，$SK_s \leftarrow DKGen(GID, sk, S)$，$m \in M$，$m' \in M$，$(h, r, ct) \leftarrow DHash(pk, m, A)$，存在 $r' \leftarrow DAdapt(SKs, m, h, r, ct, m')$ 使得 $1 = Dver(pk, m, h, r) = DVer(pk, m', h, r')$ 成立，那么 $DACH$ 算法满足数据的正确性。

3.3 实现流程

在 DecPRB 机制中，用户指编辑申请者或交易发送者，AA 代表区块链系统中的编辑节点，N_B 是 AA 节点在主链上的编辑的区块数量，也可以说是 AA 节点对区块链系统的贡献值，N_R 是 AA 节点的有效编辑数量，那么 AA 节点的贡献值是 N_B 与 N_R 的加权和，可表示为 $PR_{AA}=\lambda N_B+\eta N_R$，$0\leqslant\lambda,\eta\leqslant 1$。DecPRB 机制的实现框架如图 1 所示，首先由某个 AA 节点提出编辑申请，构建可编辑的区块链，接着根据 Π_{DACH} 算法计算出哈希值 h 签名并广播于链上的所有用户，然后 AA 节点接收有效反馈交易 DACH 值以创建新块，最后用有效的 TX 修改新块的历史记录。

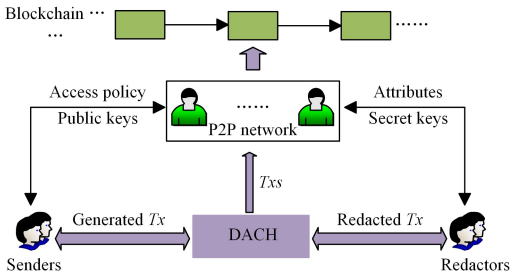

图 1 DecPRB 机制的实现框架

Fig. 1 Implementation framework of DecPRB mechanism

DecPRB 机制中的 AA 节点由 $PPGen$ 和 $AAsetup$ 算法初始化，编辑申请者采用算法 $(h,r,ct)\leftarrow DHash(pk,Tx,A)$，并计算哈希值 $h=H(m)r^e mod(nn')$；接着公开消息由加密算法计算，即 $ct\leftarrow\Pi_{DCP\text{-}ABE.Enc}(pk,m,A)$，$(n,q,p,e,d)\leftarrow RSAKGen(1^k)$，$(n',q',p',e',d')\leftarrow RSAKGen(1^k)$；接着对交易哈希值 h 进行签名验证（调用算法 $\{0,1\}\leftarrow DVer(pk,Tx,h,r)$ 来验证哈希值 h 的有效性）并广播交易到 P2P 网络中，调用算法 $\Pi_{DACH.DHash}$ 对交易 $\{tx0,tx1,\cdots\}$ 分别进行哈希计算，计算出交易哈希值 $\{h_0,h_1,\cdots h_n\}$，由 AA 节点集成到系统主链上的节点块 $\#i$ 结构的 Merkle 树中，Merkle 树内部结构如图 2 所示。若 DACH 算法满足数据的正确性，则编辑有效。假设请求交易 Tx，交易成功后为 Tx'。只有编辑者满足 $\{GID,S\}$ 时，调用算法 $DKGen$，结果 $SK_s=\{SK_i\}$ 反馈回编辑者。接着调用算法 $\{r',L\}\leftarrow DAdapt(SK_s,Tx,h,r,ct,Tx')$ 获取碰撞值 h'、随机值 r'，若满足属性策略，则反馈回陷门密钥 etd。接着将随机值 r' 和 Tx' 映射到哈希值 h。此时若 $DVer(pk,Tx',h,r')=1$ 则 r' 有效，满足 $DHash(pk,Tx,r)=DHash(pk,Tx',r')$。如果 $Dver()=1$ 且 $DAdapt()=r'$，则 r' 有效，这说明编辑者满足访问策略，此时节点编辑 $Tx'\rightarrow Tx$ 更新块 $\#i$ 的历史记录；否则 $DVer()=0$，r' 无效，撤消编辑，更新无效。

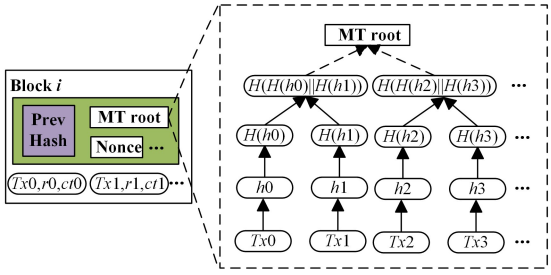

图 2 DecPRB 机制的 Merkle 树结构

Fig. 2 Merkle tree structure of DecPRB mechanism

4 性能分析

4.1 安全性分析

DecPRB 机制中的算法 $\Pi DACH.DAdapt$ 满足访问策略，则计算哈希碰撞值。假设给定 S 满足策略 (A,p)，$h\leftarrow DHsh(\cdot,m,\cdot)$，对于任意 $m'\neq m$，如果存在 $h'\leftarrow DHsh(\cdot,m',\cdot)$ 使得 $DVer(\cdot,m',h',r')=1$ 且 $h=h'$，那么可以对 S 中的属性运行 $DKGen$ 算法得到新的随机值 $r'=(hH_2(m')^{-1})^d \bmod (nn')$，其中 $ed\equiv 1 \bmod \varphi(nn')$。则可计算出哈希值 h'，即 $h'=H_2(m')r'^e$ 和 $h'=H_2(m')((hH_2(m)^{-1})^d)^e=h$，说明了 r' 可以使 $Dver(\cdot,m',h',r')=1$ 成立。因此，DACH 函数碰撞值有效，即 DecPRB 机制满足正确性，说明此机制满足设计合理的基本需求。

如果不能满足属性策略的用户恶意勾结，能否合谋出有效的碰撞值呢？假设属性策略由属性集 $S=\{S_1,S_2,\cdots,S_i\}$ 表示。存在一组全局身份为 $\{GID_1,\cdots,GID_j\}$ 的用户（且每个用户自身无法满足策略）相互合谋后收齐属性集 S，这时每个用户从 AA 处获取密钥 $\{SK_{s_i},GID_j\}$ 并计算 $\Pi_{DCP\text{-}ABE.Dec}(ct,SKs)$ 的结果是不同的，这说明不同用户的 $y_j=H_1(GID_j)$ 是不同的，则形成无效的碰撞值。因此，无法恢复出正确的陷门密钥，说明 DecPRB 机制是抗合谋攻击的。

4.2 有效性分析

算法的有效性指该算法的有效执行时间，本文为了验证 DecPRB 机制的有效性，采用仿真实验测试了 DACH 算法中的每个子算法的执行时间。仿真实验主机配置如下：CPU 为 2.6 GHz/i5、内存 RAM 为 8 GB、硬盘为 512 GB/SSD；仿真实验软件环境为 Python 语言；仿真实验数据主要来源于 Charm-Crypto[13] 提供代数运算的哈希函数和开源通信 OpenSSL 库[14]、GMP 库[15]、PBC 库[16]；实验过程采用曲线 SS512 和双线性对 512 位的测试方式，属性策略值分别取 2 的倍数。经过 3 次的测试分别取平均值，详细的实验结果如表 2 所列，其中 Setup 算法的数据是 PPGen 算法与 AASetup 算法的共同值，因为实验中无法单独测试 PPGen 算法与 AA-Setup 算法的执行时间，只能测试两者的共同执行时间。从表 2 中得到属性数量越来越多时，除了 DVer 算法执行时间相对稳定，其他 4 种子算法的执行时间也会越来越长，这是因为不管属性数量多少，DVer 算法只调用一次，所以 DVer 算法执行时间的变化不大。但是，从表 2 的仿真结果来说，DecPRB 机制中的 DACH 算法的执行时间是可接受的。

表 2 算法执行时间

Table 2 Algorithm execution time

(s)

属性数量	Setup	DKGen	DHash	DVer	DAdap
2	2.277	0.781	5.871	0.145	2.661
4	4.561	1.584	11.044	0.146	4.517
8	9.212	3.082	21.131	0.147	8.374
16	18.307	6.315	41.309	0.146	16.002
32	36.801	12.779	81.682	0.147	31.145

结束语 本文针对区块链系统中的携带用户隐私等非法交易数据，在现有链上数据编辑算法中，优化变色龙哈希函数，提出了一种分散的多方管理 DecPRB 编辑机制，在保护用户身份及交易金额隐私数据安全的情况下实现了区块链交易

数据的修改编辑，具有很强的抗攻击能力。然而，在 DecPRB 编辑过程中，非法交易记录是需要人为判定的，编辑更新后的交易记录除了 DecPRB 系统验证之外，也无法验证是否携带新的非法数据，也就是说刚刚编辑过的节点是否有新的攻击代码或携带非法交易数据，系统也无法判定。因此，今后研究 DecPRB 节点自身更新的合理机制，实现同步更新自身非法检测。

参 考 文 献

[1] ROMAN M，JENS H，MARTIN H，et al. A quantitative analysis of the impact of ar-bitrary blockchain content on bitcoin [C]// International Conference on FinancialCryptography and Data Security. 2018：420-438.

[2] IVAN P，ALEXANDRA D，SRDJAN C. uchain：How to forget without hard forks[J]. IACR Cryptology ePrint Archive，2017，20(1)：106-116.

[3] ALI D，SALIL S K，RAJA J. Mof-bc：A memory optimized and flexible blockchain for large scale networks[J]. Future Generation Computer Systems，2019，92：357-373.

[4] DOMINIC D，BERNARDO M，SRI A K T. Redactable blockchain in the permissionless setting[C]// 2019 IEEE Symposiumon Security and Privacy. 2019：124-138.

[5] SRI A K T，ADITHYA B，BERNARDO M，et al. Reparo：Publicly verifiable layer to repair blockchains [J]. arXiv：2001.00486，2020.

[6] GIUSEPPE A，BERNARDO M，DANIELE V，et al. Redactable blockchain ··c or ··c rewriting history in bitcoin and friends [C]// 2017 IEEE European Symposium on Security and Privacy. 2017：111-126.

[7] DAVID D，KAI S，DANIEL S，et al. Fine-grained and controlled rewriting in blockchains：Chameleon-hashing gone attribute-based[C]// 26th Annual Network and Distributed System Security Symposium. 2019：1-15.

[8] KE H，XIAO S Z，YI M，et al. Achieving intelligent trust-layer for internet-of-things via self-redactable blockchain[J]. IEEE Transactions on Industrial Informatics. 2020，16(4)：2677-2686.

[9] KE H，XIAO S Z，YI M，et al. Building redactable consortium blockchain for industrial internet-of-things[J]. IEEE Transactions on IndustrialInformatics. 2019，15(6)：3670-3679.

[10] ZHANG D. Research on key technologies of dataSecurity and privacy protection in distributed environment[D]. Chongqing：Southwest University，2021.

[11] LIAO X F，ZHANG D. Data privacy security based on redactable blockchain[J]. Journal of Guangzhou University(Natural Science Edition)，2021，20(3)：1-8.

[12] ALLISON L，BRENT W. Decentralizing attribute-based encryption[C]// Annual international conference on the theory and applications of cryptographic techniques. 2021：568-588.

[13] Charm-Crypto0. 5. [OL]. https：//github. com/JHUISI/charm. 2021-09-15

[14] OpenSSL[OL]. https：//www. openssl. org/. 2021-10-10.

[15] TheGNU Multiple Precision Arithmetic Library 6. 1. 2. [OL]. Available：https：//gmplib. org/. 2022-08-04.

[16] The Pairing-Based Cryptography Library 0. 5. 14. [OL]. Available：https：//crypto. stanford. edu/pbc/. 2022-10-27.

HUANG Shoumeng，born in 1975，master，associate professor. His main research interests inclue information technology and information security.