基于格签名算法的抗量子区块链数据加密方法

龙草芳 [1,2]
LONG Caofang

摘 要 为提升抗量子区块链数据加密的安全性，提出基于格签名算法的抗量子区块链数据加密方法。利用密钥矩阵生成区块链数据密钥，对部分数据分散处理，利用格签名算法对区块链数据签名，将签名与密钥整合生成区块链数据加密数字证书，利用证书对数据加密处理，以此实现基于格签名算法的抗量子区块链数据加密。实验证明，设计方法应用下抗量子区块链数据一致程度平均为 97%，平均数据加密速率为 3 115.15 byte/s，具有一定的应用价值。

关键词 格签名算法；抗量子；区块链；数据加密；安全比特；密钥矩阵

doi：10.3969/j.issn.1672-9528.2024.01.015

0 引言

区块链中存储了大量的敏感数据，包括个人身份信息、交易记录等。但因为互联网具有分布式、开放性以及随意性等特性，一些不法分子利用网络漏洞或者区块链漏洞，攻击者可能篡改数据或伪造交易，破坏区块链的可靠性和信任 [1]，造成严重的社会损失和经济损失，因此抗量子区块链数据安全问题越来越受到人们的重视与关注。数据加密作为保证数据安全的重要手段，通过对抗量子区块链中数据加密、数字签名、签名验证以及解密等一系列操作，确保抗量子区块链中数据信息的完整性、安全性以及隐私性 [2]。文献 [3] 提出基于策略隐藏的 CP-ABE 方案将访问策略隐藏，并通过区块链存储交易来保护访问控制策略的隐私性。引入分布式文件系统和区块链技术构建分布式数据存储机制，确保用户数据的完整性。当用户满足访问策略时，系统生成并发送相应的证明交易至区块链，以供验证和审计。文献 [4] 提出通过优化存储器接脚组成结构和选择 Cortex-M3 芯片作为核心处理器，构建基

1. 三亚学院信息与智能工程学院 海南三亚 572022
2. 三亚学院容淳铭院士工作站 海南三亚 572022
[基金项目] 海南省教育厅项目资助，项目编号 Hnky2023ZD-14；三亚市高校及医疗机构专项科技计划项目，项目编号 2021GXYL53；三亚学院重大专项课题（USY22XK-04）；海南省重点研发项目 (ZDYF2023GXJS007)

[7] 肖鹏，王柯强，黄振林．基于 IABC 和聚类优化 RBF 神经网络的电力信息网络安全态势评估 [J]. 智慧电力，2022, 50(6):100-106.
[8] 杨杰，郭逸豪，郭创新，等．考虑模型与数据双重驱动的电力信息物理系统动态安全防护研究综述 [J]. 电力系统保护与控制，2022,50(7):176-187.
[9] 陆孝锋，李鹏，高莲，等．基于 DKPCA 的电力信息系统虚假数据注入攻击检测方法 [J]. 电子测量技术，2022, 45(2): 91-97.
[10] 刘瑞环，陈晨，刘菲，等．极端自然灾害下考虑信息 - 物理耦合的电力系统弹性提升策略：技术分析与研究展望 [J]. 电机与控制学报，2022,26(1):9-23.
[11] 赵彦旻，袁绍山，陈宇，等．基于大数据分析的园区能源互联网电力信息管理系统设计 [J]. 自动化与仪器仪表，2021(10): 169-173.
[12] 逯宝中，李庚银，王剑晓，等．计及监测与控制功能的电力信息物理系统关键输电线路辨识方法 [J]. 中国电机工程学报，2022,42(7):2556-2566.
[13] 丁斌，袁博，郑焕坤，等．基于大数据分析的电力信息系统安全状态监测技术研究 [J]. 电测与仪表，2021,58(11):59-66.
[14] 张艺伟，刘文霞，刘耕铭，等．考虑拓扑相关和双重耦合的电力信息物理系统建模与脆弱性分析 [J]. 中国电机工程学报，2021,41(16):5486-5500.
[15] 胡怡霜，丁一，朱忆宁，等．基于状态依存矩阵的电力信息物理系统风险传播分析 [J]. 电力系统自动化，2021, 45(15):1-10.

【作者简介】

李晓龙（1978—），男，吉林长春人，本科，工程师，研究方向：电力市场。

（收稿日期：2023-09-20）

于区块链技术的一体化供应平台信息加密系统。使用 PAFT 算法对原始数据进行区块划分，并结合同态加密算法构建支持局部修复的数据加密方法。然而，上述方法的计算量较大，导致数据加密效率较低。因此，本文提出了基于格签名算法的抗量子区块链数据加密方法，以解决这些问题。

1 生成抗量子区块链数据加密密钥

采用由密钥 + 同态签名混合的加密体系，将生成的密钥与同态签名整合为数字证书，抗量子区块链数据接收者通过数字证书验证身份，获取到数据信息 [2]。因此首先需要生成抗量子区块链数据加密密钥，密钥采用密钥矩阵生成，密钥矩阵设计是否合理直接关系到数据加密质量，为了使抗量子区块链数据参量的传输速率能够大幅度提高，在对密钥编码过程中使用的密钥模板以矩阵的状态保持 [3]。密钥矩阵由横向定义系数与纵向定义系数组成，两个系数之间始终满足以下关系：

$$\begin{cases} x=\dfrac{\lambda\cdot R}{E} \\ y=\dfrac{\sqrt{R\cdot E}}{\lambda^2} \end{cases} \tag{1}$$

式中：x 表示密钥矩阵横向定义系数，该系数表示抗量子区块链数据的横向传输能力；λ 表示已编码信息的查询系数；R 表示任意一个密钥指标的数据信息编码特征；E 表示抗量子区块链数据单位传输量均值；y 表示密钥矩阵纵向定义系数，该系数表示抗量子区块链数据的纵向传输能力 [4]。假设密钥矩阵的横向定义系数与纵向定义系数同为属于大于零的数，则用于生成密钥的密钥矩阵可以表示为：

$$\boldsymbol{P}=\left(s_{\max}-s_{\min}\right)^2\begin{bmatrix} S_{11} & S_{12} & \cdots & S_{i1} \\ S_{12} & S_{22} & \cdots & S_{i2} \\ \vdots & \vdots & \ddots & \vdots \\ S_{1y} & S_{2y} & \cdots & S_{xy} \end{bmatrix} \tag{2}$$

式中：$\boldsymbol{P}$ 表示用于生成抗量子区块链数据加密密钥的密钥矩阵；$S_{\max}$ 表示数据加密主机所能分辨的数据传输向量最大值；$S_{\min}$ 表示数据加密主机所能分辨的数据传输向量最小值 [5]。将以上生成的密钥矩阵代入到加密模板中，生成数据加密密钥：

$$K=P\frac{\sqrt{g^2-z^2}}{\left(\gamma\cdot\left|\Delta A\right|\right)-h} \tag{3}$$

式中：K 表示抗量子区块链数据加密密钥；g 表示任意编码进度下加密数据文本编码信息；z 表示抗量子区块链数据加密文本的初始编码信息；γ 表示密码文本传输系数；ΔA 表示密码文本在单位时间内的传输量数值；h 表示数据加密权限值 [6]。利用生成的密钥对待传输部分区块链数据分散处理，将该部分数据信息设定为不公开信息，其余数据为公开信息。

2 基于格签名算法的数据线性签名

考虑到仅对数据进行部分加密，当抗量子区块链数据遭到攻击，攻击者可以利用一些解密技术同样可以获取到数据信息，因此在上述基础上，利用格签名算法对待传输数据进行线性签名，该签名用于对数据接收者身份验证，确保抗量子区块链数据的私密性 [7]。格签名算法是将一组线性无关的向量组成签名，一个格为一个向量空间，用公式表示为：

$$L=L(B)=\left\{\sum b_i\in X\right\} \tag{4}$$

式中：L 表示格向量；$L(B)$ 表示基向量，由于格的基是一组线性无关的向量组成，因此格可以由不同的基向量表示；b_i 表示元模格，即格中的一个子格；X 表示向量组 [8]。签名者从高斯离散分布中采样离散向量，即格向量，格向量值表示为：

$$e_L=ad_1+d_2 \tag{5}$$

式中：e_L 表示格向量值；a 表示签名者随机选择的一个数值，该数为正整数；d_1、d_2 分别为从高斯离散分布采样的两个离散向量 [9]。将其与密钥作为格签名算法的输入向量，生成数据签名，用公式表示为：

$$U=\left(e_L,K\right) \tag{6}$$

式中：U 表示抗量子区块链数据签名 [10]。在签名中 e_L 是根据高斯离散分布的向量，所以生成的签名需要满足以下条件：

$$\frac{1}{2}D_{er}=1\Big/\left(M\exp\left(-\frac{\left\|e_L\right\|^2}{2K}\right)\right) \tag{7}$$

式中：D_{er} 表示高斯离散分布；M 表示格签名算法的迭代期望值 [11]。利用上述公式对生成的数据签名进行检验，如果不满足以上条件，则生成新的签名，再对其进行检验，直到满足公式（7）条件为止；如果满足以上条件，则算法输出签名，以此实现抗量子区块链数据签名。

3 抗量子区块链数据加密处理

将以上生成的密钥与签名整合为数字证书，证书格式采用 FG.151 国际标准，数字证书包含密钥、签名以及密文，用公式表示为：

$$F=\left(K,U,Y,W\right) \tag{8}$$

式中：F 表示用于抗量子区块链数据加密的数字证书；Y 表示待传输数据信息密文；W 表示数字证书序列号，该序列号为数字证书所有域的信息哈希摘要。利用以上生成的数字证书对区块链数据加密处理，当数据接收者接收到签发的数字证书后，即可表示该用户合法拥有数据密钥，但是数据接收者想要获取证书中的明文时，则需要提取数字证书中的签名，对身份进行验证，验证运算为：

$$c = F\left(\bmod 2q, U\right) \tag{9}$$

式中：c 表示数据哈希值；q 表示验证密钥[12]。当上述公式计算到的数据哈希值 c 与数字证书中的哈希摘要相等，则验证成功，用户身份是可信的，即可提取到数字证书中的密文，利用密钥对密文进行解密，获取到数据明文；如果计算到的数据哈希值 c 与数字证书中的哈希摘要不相等，则验证失败，表示用户为非法用户，无法获取到抗量子区块链数据密文，以此实现基于格签名算法的抗量子区块链数据加密。

4 实验论证

4.1 实验准备与环境

以下将对本文设计方法进行实验分析，将设计方法与传统方法 A（文献 [3] 方法）、传统方法 B（文献 [4] 方法）加密效果进行对比，分析本文设计方法在实际应用中加密效果，对设计方法可行性与可靠性进行验证。选择抗量子区块链数据为实验对象，数据总量为 12.41 GB，利用本文设计方法对区块链数据加密，考虑到提出方法在运行过程中产生的数据相对比较大，为了使提出方法可以正常运算，对实验环境设计为：选择型号为 KFAAG-A4F8 的 PC 机，搭配 Intel Corei5-46948（vPro）（CORE23.15 GHz）处理器，操作系统选择专业版 Windows2010，内存为 32 GB，格签名算法开发语言为 Python，开发工具选用 PyCharm+Aakastha3（64 bit）。实验使用 JKHFA 软件模拟网络攻击，入侵抗量子区块链数据库，网络攻击频率为 15.26 GHz。操作系统 Ubuntu 20.04，编程语言 Python 3.8，加密库 pycryptodome，格签名算法库 PQCrypto-SIDH。选择包含敏感交易信息的区块链数据为实验对象，数据总量为 12.41 GB，需要对其进行加密保护。数据分为发送方和接收方两部分。原始数据 Transaction Amount100 units, Sender Alice, Receiver Bob，公钥用于加密数据，公开可见，私钥用于解密数据，保密存储。按照上述流程生成抗量子区块链数据加密签名，具体如图 1 所示。

```
66.  75.  24.  57.  57.  62.   6.  87. 102.  98.  75. 100.  40.  89.  93.  38.  10.  92.
91.  54.  12.  86.   2.  44. 105.  81.  42.  46.  33.  80.  11.  86.  36.   5.  86.  55.
28.   6.  42.  87.  91.  21.  50.  20.  92. 102.  68.  72.  86.  22.  79.  46.  47.  46.
41.  94.  37.  30.  54.  45.  24.  39.  98.  94.   4.  31.   9.  43.  81.  31.   2.  21.
88.  86. 103.  43.  16.  85.  40.  42.  35.   2.  98.  25.  39. 101.   6.  43.  31.   3.
12.  46.  36.  92.  97.  42.  21.  43.  97.  83.  45.  94.  38.  54.  24.  62. 103.  60.
104.  39.  56.  85.  17.   4.   7.  11.  68.  92.  81.  26.  41.  90.  77.  86.  80.  79.
95. 100.  37.  69.   2.  46.  61.  55.  16.  30.  72.  17.   0.  13.  95.   3.  10.  65.
```

图 1 抗量子区块链数据加密签名

对产生的签名按照验证条件进行验证，对签名进行线性计算，才能通过对签名的验证，验证结果如图 2 所示。

图 2 抗量子区块链数据签名验证

本文设计方法基本可以完成抗量子区块链数据加密任务，以下对具体加密效果进行评定。

4.2 实验结果与讨论

通过分析量子攻击模拟的结果，评估加密算法在量子攻击下的表现，检验攻击下加密效果是否能够保持在较高的安全比特值。数据安全比特可以反映出抗量子区块链数据安全性，安全比特值越高，则表示数据安全性越高，加密效果越好。实验在抗量子区块链中随机选择 10 个子区块，对数据加密处理后，使用 IHFAR 软件测算每个子区块数据安全比特，使用电子表格对实验数据记录，具体数据如表 1 所示。

表 1 三种方法应用下区块链数据安全比特对比

单位：bits

子区块序号	设计方法	传统方法 A	传统方法 B
1	186.15	124.16	124.15
2	176.59	135.42	111.22
3	185.42	124.17	125.32
4	186.16	112.56	100.24
5	194.25	125.36	102.31
6	195.63	132.12	104.26
7	199.52	133.33	112.32
8	187.52	121.41	112.42
9	186.32	115.26	111.48
10	188.52	123.41	101.23

从表 1 中数据可以看出，三种方法在数据安全比特方面表现出明显的差异，在设计方法应用下抗量子区块链数据安全比特平均值为 186.48 bits，说明设计方法加密后数据安全性良好。而在传统方法 A 应用下平均安全比特值为 121.46 bits，传统方法 B 应用下平均安全比特值为 112.41 bits，因此通过以上分析可以证明在安全性方面设计方法更佳。

模拟数据传输过程，将加密后的数据传输给接收方，接收方使用相应的解密算法和密钥对收到的密文进行解密，将解密后的数据与原始数据进行比对，确保解密结果与原始数据一致，验证数据的完整性。以一致程度（%）为指标，验证抗量子区块链数据安全性，一致程度越高，则表示数据安

全性越高，加密效果越好。结果如图 3 所示。

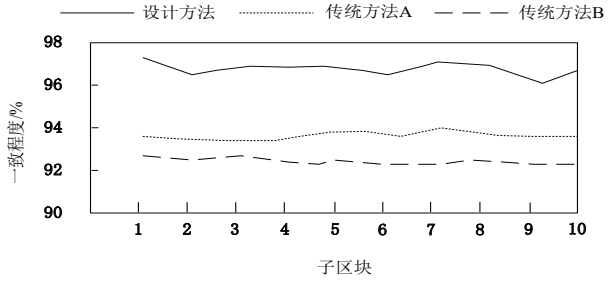

图 3 区块链数据解密一致程度

分析图 3 可知，三种方法在数据安全性方面表现出明显的差异，在设计方法应用下抗量子区块链数据一致程度平均为 97%，而传统方法 A 和传统方法 B 应用下的一致程度平均为 93.7% 和 92.1%，表明本文方法下区块链数据在加密和解密过程中的安全性更高，可以有效保障数据安全及完整性。

对三种方法加密速率进行对比，实验随机抽取十种规格的数据包，数据包容量各相差 50 byte 数据，使用电子表格记录不同数据量下三种方法加密速率，具体数据如表 2 所示。

表 2 三种方法加密速率对比

数据量 /byte	设计方法 /(byte·s^{-1})	传统方法 A /(byte·s^{-1})	传统方法 B /(byte·s^{-1})
1450	3 145.62	1 134.16	1 024.46
1500	3 015.28	1 058.56	1 024.18
1550	3 105.46	1 225.15	1 023.64
1600	3 152.46	1 095.63	1 000.25
1650	3 024.61	1 066.53	1 051.56
1700	3 142.45	1 056.14	1 048.52
1750	3 125.64	1 032.62	1 025.78
1800	3 125.47	1 024.15	1 047.76
1850	3 124.11	1 000.23	1 124.61
1900	3 023.24	1 001.15	1 124.56

分析表 2 可知，三种方法在加密速率方面也表现出明显的差异，设计方法平均加密速率为 3 115.15 byte/s，而传统方法 A 平均加密速率为 1 105.15 byte/s，传统方法 B 平均加密速率为 1 024.16 byte/s，均远低于设计方法。这是因为设计方法采用了格签名算法对数据签名，生成的签名长度比较短、尺寸比较小，从而在一定程度上提升了数据加密速率。因此通过以上对比实验数据证明，无论是在安全性方面还是在加密速率方面，设计方法均表现出明显的优势，相比较两种传统方法更适用于抗量子区块链数据加密。

5 结语

格签名算法作为一种具有抗量子计算攻击特征的数据加密算法，此次结合该算法优势，将其应用到抗量子区块链数据加密中。经过实验验证，提出方法具有更短的加密签名长度和密钥长度，有效提高抗量子区块链数据加密速率，并且采用了签名 + 数字证书混合加密体系，有效提高了抗量子区块链数据安全比特水平，为数据加密实践提供了有力的理论支撑，同时也为该方面研究提供了参考依据，提高抗量子区块链数据加密技术水平。

参考文献：

[1] 李宗维 , 孔德潮 , 牛媛争 , 等 . 基于人工智能和区块链融合的隐私保护技术研究综述 [J]. 信息安全研究 , 2023,9(6):557-565.

[2] 景旭 , 蒋炎 . 集群式农产品供应链区块链密文策略可验多部门监管方案 [J]. 农业工程学报 , 2023,39(3):227-236.

[3] 巴阳 , 陈越 , 胡学先 , 等 . 基于区块链与属性基加密的数据共享方案 [J]. 信息工程大学学报 , 2022,23(4):443-451.

[4] 迟小华 . 基于区块链技术的一体化供应平台信息加密系统 [J]. 自动化与仪器仪表 , 2022(7):180-184.

[5] 李容嵩 , 彭凌烟 , 蒋成 , 等 . 基于区块链和属性加密的工程检测数据安全共享技术研究 [J]. 湖南电力 ,2022,42(3):65-72.

[6] 李懿 , 王劲松 , 张洪玮 . 基于区块链与函数加密的隐私数据安全共享模型研究 [J]. 大数据 , 2022,8(5):33-44.

[7] 吉斌 , 昌力 , 朱丽叶 , 等 . 区块链系统节点私钥泄露的电力数据防篡改方法与验证机制设计 [J]. 电力自动化设备 , 2021, 41(12):87-94.

[8] 段新华 . 基于同态加密的区块链交易数据隐私保护系统设计 [J]. 信息与电脑 (理论版), 2021,33(13):68-70.

[9] 杨亮 . 基于区块链技术的机器人数据加密传输控制系统设计 [J]. 计算机测量与控制 ,2021,29(6):119-122+163.

[10] 芦效峰 , 付淞兵 . 属性基加密和区块链结合的可信数据访问控制方案 [J]. 信息网络安全 ,2021,21(3):7-14.

[11] 段平 . 基于区块链及分层加密技术的数据传输控制系统设计 [J]. 计算机测量与控制 ,2020,28(10):76-80.

[12] 郭瑞雪 . 基于区块链技术的网络数据隐私保护方法研究 [J]. 现代信息科技 , 2020,4(13):164-166.

【作者简介】

龙草芳（1983—），女，江西抚州人，硕士，副教授，研究方向：计算机网络与分布式数据库、数字信息安全。

（收稿日期：2023-08-03）