

文章编号: 2096-1618(2022)05-0515-05

基于国密化区块链平台的量子密钥全生命周期管理系统

林雨生, 昌 燕, 侯麒麟, 谢汶廷, 王 玮, 陈天肃
(成都信息工程大学网络空间安全学院, 四川 成都 610225)

摘要:针对传统通信系统中密钥存在的密钥易泄露、密钥管理可信度低等安全性问题,提出一个基于国密化区块链平台的量子密钥全生命周期管理及追溯系统。有保密通信需求的两个机构,将量子密钥替换传统通信系统中的主密钥,在通信过程中,量子密钥生成、分发、使用、更新和销毁的相关操作信息由两个机构管理员及用户实时上传至区块链平台。对 Fabric 联盟链进行国密化改造,保证算法的自主可控,并用于量子密钥的全生命周期管理。当联盟链管理员对保密通信过程中发生的安全事件进行追溯追责时,利用联盟链去中心化、不可篡改、身份验证等特点,可以实现量子密钥全生命周期管理和追溯过程的透明可信,保证量子密钥在通信系统中的安全使用与有效监管。

关键词:量子密钥,国密化 Fabric 联盟链,保密通信,管理及追溯系统

中图分类号:P751.1

文献标志码:A

doi:10.16836/j.cnki.jcui.2022.05.005

0 引言

传统通信系统中,保证密钥的安全性是用户进行保密通信的前提。密钥的安全性问题主要分为两个方面:(1)密钥生成时不是真随机的序列,并且在密钥分发时,由于计算能力的提高,密钥泄露的可能性越来越大;(2)密钥管理缺乏可信度,当发生安全事件时,管理员无法进行有效及可信赖的追溯追责。

量子通信^[1-3]利用量子力学特征,使量子密钥分发时具有无条件安全性,并且产生的量子密钥是真随机的序列。因此,量子通信能够有效解决传统通信系统中密钥生成与分发的安全性问题。目前,量子通信在保密通信中应用越来越广泛,赖俊森等^[4]分析了量子保密通信的发展前景,并提出了相应的策略;曹原等^[5]分析了目前量子通信网络的研究进展,提出量子通信网络体系架构;郑炜能^[6]将量子通信应用于实现多节点的路由功能;查振兴等^[7]则将量子通信应用于 VPN 网络中密钥的传输;吴佳楠等^[8]将量子密钥应用于文件加密系统中;熊英等^[9]将量子通信应用于保护移动办公的安全中。以上研究保证了量子密钥生成、分发的安全性,但没有解决量子密钥使用及管理时存在的安全性问题。

联盟链^[10]是区块链的一种,由多个私有链组成,只有联盟内部的机构及其用户才能访问数据,达成共识容易。目前,联盟链应用于保密通信中量子密钥管理的研究较少,已有的研究中,姚英英等^[11]提出使用区块链应用于物联网场景下的身份认证以及密钥管理

方案;石润华等^[12]利用区块链技术解决了物联网中密钥分发困难的问题,并且使用量子随机数提高密钥的安全性。以上研究使用公有链进行密钥管理,不能进行实时更新,并且公有链的数据隐私性较弱。

针对目前研究中存在的问题,本文结合区块链技术与量子通信技术,提出一个基于国密化区块链平台的量子密钥全生命周期管理系统,具有以下特点:将量子密钥应用于传统保密通信中,并使用一次一密的思想,保证量子密钥生成、分发、使用时的安全性;将国密化算法替换国际通用密码算法,构建国密化 Fabric 联盟链管理系统用于量子密钥的全生命周期管理;联盟链管理员可以对量子密钥的全生命周期中发生的安全事件进行追溯追责。本文提出的系统,可以实现对量子密钥的可信、有效监管,并能对保密通信时发生的安全事件进行追溯追责,解决了经典通信系统中密钥存在的安全性问题。

1 系统设计

1.1 业务设计

系统的业务包括两个机构成员间的保密通信、国密化 Fabric 联盟链平台搭建与管理、量子密钥操作日志信息上链、联盟链管理员对安全事件的追溯追责。具体开发逻辑如下。

(1)两个机构间的保密通信业务。根据两个机构间的保密通信需求,构建 C/S 模式的保密通信网络。该业务包含 3 个方面:两个机构量子设备管理员首先通过量子密钥分发产生对称密钥池,然后进一步协商量子密钥编号规则以及选取量子密钥的长度;两个机

构成员向各自管理员申请量子密钥用于保密通信;在保密通信时使用 CA 证书、公钥体系和对称密码技术保证安全性。

(2)国密化 Fabric 联盟链开发业务。将现有 Fabric 联盟链进行国密化改造,建立 Fabric 平台。以两个机构中两个成员进行保密通信为例,配置有两个机构的组织,并且在每个组织的节点上写入链码。

(3)量子密钥操作日志信息上链。在两个机构成员间进行保密通信的整个过程中,有关量子密钥全生命周期的操作日志文件由两个机构的管理员或用户上传到 Fabric 平台中,最后由联盟链管理员进行管理。

(4)安全事件的追溯追责。当两个机构成员进行保密通信时或保密通信后,若发生安全事件,则由联盟链管理员根据发生安全事件时的量子密钥 ID 进行追溯追责。

1.2 架构设计

系统的架构主要包括国密化 Fabric 联盟链平台、基于 C/S 模式的保密通信网络、Web 服务器端的管理与追溯追责,见图 1。

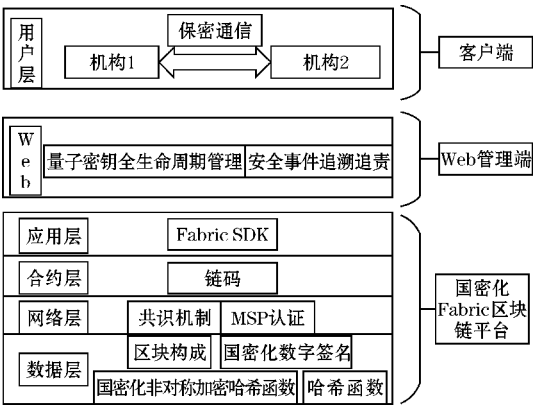


图 1 系统架构

其中客户端为两个机构中的成员及管理员。该客户端保密通信网络采取 C/S 模式,当两个机构成员或管理员操作量子密钥时,实时记录并上传相关量子密钥操作日志文件到联盟链中。

Web 管理端使用 Vue 框架进行编写,为联盟链管理员对安全事件进行管理与追溯追责,是系统的核心。当联盟链管理员登录 Web 后端后,可以查询客户端用户上传时的交易 ID,并以量子密钥的全生命周期过程进行分类,查询所有交易 ID 的交易信息进行分类展示。若对安全事件进行追溯追责时,则查询发生安全事件的量子密钥 ID,展示该量子密钥 ID 对应量子密钥的全生命周期过程中的交易信息,再由管理员进行逐一排查,最终确定安全事件的责任方。

国密化 Fabric 联盟链平台包括数据层、网络层等,其功能是对机构用户或管理员上传的量子密钥操作日

志信息进行存储。其中数据层是联盟链的核心部分,能将机构用户或管理员的量子密钥日志操作文件上传到联盟链中;网络层保证了 Fabric 联盟链中的信息传输,主要有共识机制和数据验证机制等;合约层含有 Fabric 联盟链的智能合约,也称为链码,是在 Fabric 联盟链上进行存储等操作的一段代码,并且能与 Fabric 网络进行交互;最外层是应用层,包含了 Fabric SDK 模块,能实现 Fabric 联盟链与后端服务的连接。

2 系统实现

2.1 国密化联盟链平台

为实现联盟链平台算法的自主可控,则需用国密算法替换 BCCSP 模块^[13]中的哈希算法、对称密码算法以及非对称密码算法。目前,曹琪等^[14]已经对如何嵌入国密化算法到联盟链平台中有一定研究,本文构建的国密化区块链平台则借鉴其思想将国密 SM2、SM3、SM4 算法替换 SHA 算法、AES 算法、RSA 算法等,并根据使用量子密钥的保密通信机构设置节点等信息,以便用于量子密钥全生命周期的管理与安全事件的追溯。

2.1.1 国密化联盟链环境搭建

系统将联盟链搭建在 Ubuntu 环境下,使用 Golang 编辑器运行代码,然后安装联盟链环境的依赖程序以及 Fabric 的系统文件,再运行 Fabric 文件中的 bootstrap 脚本完成其余文件的配置,随后将国密化算法接口嵌入到上层应用中,实现对国密算法调用的支持,最后根据保密通信中含有的机构数量创建组织节点,构建证书、数据文件和通道,同时打开 orderer 和 peer 节点,当通道创建后,将节点逐个加入,则完成国密化联盟链环境部署。本系统创建的两个组织的相关信息见表 1。

表 1 组织信息

机构名	组织号	组织 ID
机构 1	Org1	User1
机构 2	Org2	User2

当完成通道创建后,添加节点和对所构建的节点进行测试见图 2~3。

```
Creating network "net_byfn" with the default driver
Creating volume "net_orderer.example.com" with default driver
Creating volume "net_peer0.org1.example.com" with default driver
Creating volume "net_peer1.org1.example.com" with default driver
Creating volume "net_peer0.org2.example.com" with default driver
Creating volume "net_peer1.org2.example.com" with default driver
Creating peer1.org1.example.com ... done
Creating peer0.org1.example.com ... done
Creating orderer.example.com ... done
Creating peer1.org2.example.com ... done
Creating peer0.org2.example.com ... done
Creating cli ... done
```

图 2 创建节点

```

===== peer0.org: joined channel 'mychannel' =====

+ peer channel join -b mychannel.block
+ res=0
+ set -x

bcsp gm keyimport pk is *sm2.PublicKeyBcsp gm keyimport pk is *sm2.PublicKeyBcsp gm keyimport pk is *sm2.PublicKeySM3
SM3

2021-11-08 09:01:15.845 UTC [channelCmd] InitCmdFactory -> INFO 001 Endorser and orderer connections initialized
2021-11-08 09:01:19.918 UTC [channelCmd] executeJoin -> INFO 002 Successfully submitted proposal to join channel
===== peer1.org: joined channel 'mychannel' =====

+ peer channel join -b mychannel.block
+ res=0
+ set -x

bcsp gm keyimport pk is *sm2.PublicKeyBcsp gm keyimport pk is *sm2.PublicKeyBcsp gm keyimport pk is *sm2.PublicKeySM3
SM3

2021-11-08 09:01:18.948 UTC [channelCmd] InitCmdFactory -> INFO 001 Endorser and orderer connections initialized
2021-11-08 09:01:19.918 UTC [channelCmd] executeJoin -> INFO 002 Successfully submitted proposal to join channel

```

图3 测试节点

File Explorer window showing the contents of the file `161_A1_recommended_key22.txt`. The file is located in the `target` folder. The contents of the file are as follows:

```

1 161_A1_recommended_key22.txt
2 2A1_A1_recommended_key22.txt
3 161_A1_recommended_key22.txt
4 161_A1_recommended_key22.txt
5 161_A1_recommended_key22.txt
6 161_A1_recommended_key22.txt
7 161_A1_recommended_key22.txt
8 161_A1_recommended_key22.txt
9 161_A1_recommended_key22.txt
10 161_A1_recommended_key22.txt
11 161_A1_recommended_key22.txt
12 161_A1_recommended_key22.txt
13 161_A1_recommended_key22.txt
14 161_A1_recommended_key22.txt
15 161_A1_recommended_key22.txt
16 161_A1_recommended_key22.txt
17 161_A1_recommended_key22.txt
18 161_A1_recommended_key22.txt
19 161_A1_recommended_key22.txt
20 161_A1_recommended_key22.txt
21 161_A1_recommended_key22.txt
22 161_A1_recommended_key22.txt
23 161_A1_recommended_key22.txt
24 161_A1_recommended_key22.txt
25 161_A1_recommended_key22.txt
26 161_A1_recommended_key22.txt
27 161_A1_recommended_key22.txt
28 161_A1_recommended_key22.txt

```

图4 量子密码本

2.1.2 国密化联盟链链码开发

在保密通信过程中,为实现两方机构管理员和用户的量子密钥日志文件进行实时上传,Fabric 联盟链需要进行相应链码的开发及封装,主要方法见表2。

表2 链码方法

方法名	状态	功 能
CreateInfo	PutState	日志信息上链
historyForKeyId	Getstate	查询历史信息
queryBlockByTxId	Getstate	查询交易 ID
queryInfoByTxId	Getstate	根据交易 ID 查询
queryInfoByKeyId	Getstate	根据量子密钥 ID 查询
updateInfo	PutState	更新信息上链

2.2 保密通信网络

本系统以经典通信为基础,使用 java 语言进行编程,采取 C/S 通信模式,将量子密钥融入到经典通信网络中,保证通信密钥的真随机性及不可窃取。保密通信网络包含:两个机构管理员进行量子密钥传输及协商量子密码本;两个机构成员使用量子密钥进行保密通信;两个机构管理员及成员上传量子密钥日志文件到区块链中。

2.2.1 协商量子密码本

两个机构间需要进行保密通信时,首先需要两方机构管理员间使用量子设备产生对称量子密钥池,借助 DH 密钥协商的思想,两个机构管理员利用公私钥体系保护协商内容及 CA 证书进行身份认证,再确定所取量子密钥长度以及每个量子密钥的编号规则,最终产生对称的量子密码本保存在本地。本系统以两个机构管理员协商的编号规则为 k +递增,选取的量子密钥长度为 128 位,则两方机构管理员最终形成的量子密码本见图 4。

2.2.2 保密通信

当两个机构成员需要进行保密通信时需要如下步骤:

(1)各个机构成员需向各自管理员申请量子密钥,由管理员使用公私钥体系将量子密钥进行内网传输到指定成员,并记录此次操作保包含的日志信息,以便后续上传至区块链中,其管理员分发量子密钥后展示界面见图5。

用户名	用户IP地址	用户端口号	密钥ID	密钥状态	时间
admin1	/127.0.0.1	52594		null	Tue Nov 09 11:04:20 CST 2021
bob	/127.0.0.1	52611		null	Tue Nov 09 11:04:26 CST 2021
bob	/127.0.0.1	52611	k19358	RECEIVE	Tue Nov 09 11:05:24 CST 2021

图5 管理员界面展示

(2) 机构成员接收到量子密钥后首先存储在本地密码本中,并在成员界面展示密钥相关信息,然后将其作为 AES-128 算法的密钥种子产生一级密钥,再将该一级密钥加密随机数 R 产生会话密钥,最后用于加密通信内容,并使用公私钥体系将加密通信内容、量子密钥 ID、随机数 R 等发送至另一机构接收方,同时记录此次量子密钥相关日志信息,其发送方用户界面展示见图 6。

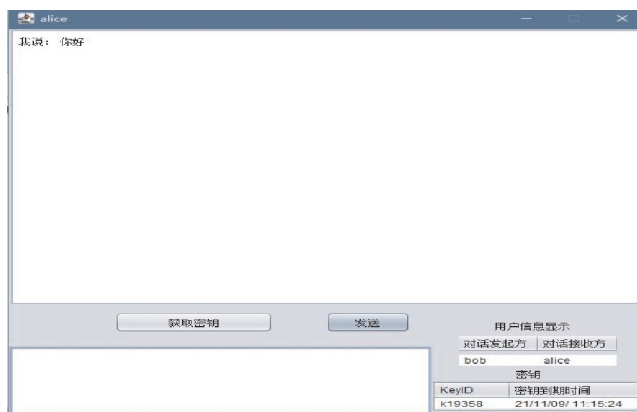


图 6 发送方界面

(3)接收方利用公私钥体系进行解密数据包,首先查询是否含有量子密钥 ID 对应的量子密钥,若没有则与步骤(2)申请量子密钥操作一致,然后还原出会话密钥解密通信内容,并记录此次量子密钥相关日志信息。以上步骤则称为完成两个机构间的保密通信。

2.2.3 上传量子密钥日志文件

为实现对量子密钥全生命周期的管理与发生安全事件时的追溯追责,两方机构管理员与成员在对量子密钥进行相关操作时,都需要将量子密钥日志文件以 json 格式实时上传至区块链中。在量子密钥全生命周期中,两方机构管理员或用户对量子密钥的操作信息见表 3。

表 3 量子密钥日志信息字段

名称	含义
Index	上传索引
Keyid	量子密钥 ID
Status	量子密钥状态
Username	操作者名称
Targetname	目标用户名称
Rule	量子密钥编号规则
Summary	量子密钥文件摘要
DestoryObject	量子密钥销毁者
Createdate	量子密钥生成时间
Distributedate	量子密钥分发时间
Receivedate	量子密钥接收时间
Usedate	量子密钥使用时间
Destroydate	量子密钥销毁时间

当两方机构管理员或用户操作量子密钥并形成日志文件时,管理员或用户只需使用 GRPC 远程调用区块链封装的方法即可,其主要的调用方法见表 4。

表 4 上链调用方法

调用方法	功能
Createinfo	将日志信息上链
getMessage	获取上链操作信息
getTxid	获取本次交易 ID
getData	获取本次交易数据

2.3 量子密钥管理及追溯平台

当保密通信过程中或通信后发生安全事件时,区块链管理员可登录管理后台,查询相关量子密钥 ID 全生命周期过程中所记录的日志信息,并根据量子密钥全生命周期的不同阶段逐步追溯安全事件的责任人以及时间段。其中量子密钥管理及追溯平台采用 Vue 框架,并与区块链平台进行实时查询交易信息并展示。

2.3.1 量子密钥全生命周期管理

量子密钥的全生命周期包括密钥生成、分发、使用、销毁阶段,根据保密通信过程中两方机构管理员或用户上传的量子密钥日志信息进行分类,使得区块链管理员可以实时查看每个阶段的量子密钥相关信息,以便及时发现安全事件。以量子密钥生成阶段为例,区块链管理员查看的信息展示见图 7。



图 7 量子密钥管理界面

2.3.2 安全事件追溯追责

当区块链管理员或保密通信用户发现安全事件时,则由区块链管理员首先排查安全事件发生的阶段以及责任方。区块链管理员根据发生安全事件时使用的量子密钥 ID 查询其所有的日志信息,并以量子密钥全生命周期不同阶段进行展示;然后由管理员对比每个阶段参与者的日志信息是否不一致,若发现有问题的阶段则点击错误按钮,再进入下一个阶段,直到判别完该量子密钥的全生命周期所有阶段的日志信息则结束;最后则完成追溯,并展示出错的阶段以及该阶段的参与者,随后再联合相关参与者判定此次安全事件的责任人。安全事件追溯及追溯结果展示见图 8、图 9。



图 8 安全事件追溯展示



图 9 安全事件追溯结果

3 结束语

本文针对经典保密通信中存在的密钥易泄露、密钥不真随机等问题,将量子密钥用于经典保密通信中,并构建国密化区块链平台对量子密钥的全生命周期进行管理,实现量子通信与区块链的结合应用。当发生安全事件时,由于区块链具有去中心化、数据不可篡改等特点,区块链管理员可以对安全事件进行可靠、可信的追溯追责,保证了保密通信过程中量子密钥全生命周期的安全性,并能对量子密钥使用者进行一定程度上的威慑,使之不能随意进行破坏。

致谢:感谢成都市科技项目(2019-YF05-02028-GX)对本文的资助

参考文献:

- [1] BENNETT CH, BRASSARD G. Quantum Cryptography: Public Key Distribution and Coin Tossing [C]. IEEE. International Conference on Computers Systems and Signal Processing, September 12, 1984, Baialore, India. New York: IEEE, 1984: 175-179.
- [2] ELKOUSS D, MARTINEZ-MATEO J, CIURANA A, et al. Secure Optical Networks Based on Quantum Key Distribution and Weakly Trusted Repeaters[J]. Journal of Optical Communications & Networking, 2013, 5(4): 316-328.
- [3] LO HK, CHAU HF. Unconditional Security of Quantum Key Distribution over Arbitrarily Long Dis-

- tances[J]. Science, 1999, 283(5410): 2050-2056.
- [4] 赖俊森, 赵文玉, 张海懿. 量子保密通信技术进展及应用趋势分析[J]. 信息通信技术与政策, 2020(12): 64-69.
- [5] 曹原, 赵永利. 量子通信网络研究进展[J]. 激光杂志, 2019, 40(9): 1-7.
- [6] 郑祎能. QKD 网络量子信道管理关键技术研究[J]. 计算机科学, 2018, 45(S1): 369-376+404.
- [7] 查振兴, 高泉, 李强, 等. 基于量子密钥分发的 IPsec VPN 密码机: CN 108173652 A[P]. 2018.
- [8] 吴佳楠, 唐祁, 贺曼丽, 等. 融合量子密钥的内网文件加密系统[J]. 重庆大学学报, 2020, 43(11): 45-55.
- [9] 熊英, 唐小康, 陈娟. 一种利用量子密钥提升移动办公系统安全性的方法: CN 109756325 A[P]. 2019.
- [10] Linux. Hyperledger Fabric [EB/OL]. <https://www.hyperledger.org/>. 2020-09-15.
- [11] 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]. 信息安全与技术, 2019, 010(6): 33-39.
- [12] 石润华, 石泽. 基于区块链技术的物联网密钥管理方案[J]. 信息安全, 2020, 20(8): 1-8.
- [13] hyperledger-fabric/docs documentation [EB/OL]. <https://hyperledger-fabric.readthedocs.io/zh-CN/latest/>. 2020-01-29.
- [14] 曹琪, 阮树骅, 陈兴蜀, 等. Hyperledger Fabric 平台的国密算法嵌入研究[J]. 网络与信息安全学报, 2021, 7(1): 65-75.

Full Life Cycle Management of Quantum Keys based on State Secret Blockchain Platform

LIN Yusheng, CHANG Yan, HOU Qiyu, XIE Wenting, WANG Wei, CHEN Tiansu
(College of Cyberspace Security, Chengdu University of Information Technology, Chengdu 610225, China)

Abstract: Aiming at the security problems such as easy key leakage and low management reliability in traditional communication systems, this paper proposes a quantum key full life cycle management and traceability system based on the state secret blockchain platform. Two institutions with a need for secure communication replace the master key in traditional communication systems with quantum keys. During the communication process, the relevant operation information of quantum key generation, distribution, use, update and destruction is uploaded to the blockchain platform in real time by the administrators and users of the two institutions. In this paper, the state secret transformation of the Fabric alliance chain is carried out to ensure that the algorithm is autonomous and controllable, and it is used for the full life cycle management of quantum keys. When the consortium chain administrator traces the security incidents that occur in the confidential communication process, the use of the consortium chain's features of decentralization, non-tampering, and identity verification can realize the transparency and reliability of the quantum key full life cycle management and traceability process. It ensures the safe use and effective supervision of quantum keys in communication systems.

Keywords: quantum key; state secret fabric alliance chain; confidential communication; management and traceability system