文章编号:2096-1472(2024)01-0014-05
DOI:10.19644/j.cnki.issn2096-1472.2024.001.004

基于区块链的量子密钥分发在云存储的应用研究

孙 羽,党 仁,周 虎,朱德新

(长春大学网络安全学院,吉林 长春 130022)

✉ 353130273@qq.com; 441721899@qq.com; 291253464@qq.com; 38925023@qq.com

摘 要:针对当前量子密钥分发技术在实际应用中存在建设成本极高和难以实现远距离的量子密钥分发等问题,提出了一种基于区块链的量子密钥分发方案。将该方案应用于云存储的数据隐私保护中,利用量子密钥对数据进行加密存储,实现量子密钥的扩展应用。实验结果表明,利用区块链技术能够实现安全且高效的量子密钥分发,相较于传统的量子密钥分发技术,该方案在实际应用中具有显著的优势。

关键词:区块链;量子密钥;云存储

中图分类号:TP311 **文献标志码**:A

Research on the Application of Blockchain-based Quantum Key Distribution in Cloud Storage

SUN Yu, DANG Ren, ZHOU Hu, ZHU Dexin

(*School of Cyber Security, Changchun University, Changchun* 130022, *China*)

✉ 353130273@qq.com; 441721899@qq.com; 291253464@qq.com; 38925023@qq.com

Abstract: A blockchain-based quantum key distribution solution is proposed to address the problems of extremely high construction cost and difficulty in realizing long-distance quantum key distribution that exist in the practical application of the current quantum key distribution technology. This solution is applied to the data privacy protection of cloud storage, and the quantum key is used for encrypting and storing the data to realize the extended application of quantum key. The experimental results show that the use of blockchain technology can realize secure and efficient quantum key distribution. Compared to traditional quantum key distribution technology, the proposed solution has significant advantages in practical use.

Key words: blockchain; quantum key; cloud storage

0 引言(Introduction)

作为一种新兴的数据存储方式,云存储在数据存储量、可靠性、成本等方面的优势使其逐步取代了传统的存储方式,为解决海量电子数据存储难题提供了全新的解决方案。尽管云存储技术发展繁荣,但在云环境中存储数据仍存在一些机密性、可用性和完整性方面的安全问题[1]。针对云存储数据的隐私问题,研究人员提出了不同的密码技术,确保云存储数据的隐私安全[2-4]。考虑到传统的加密技术存在一定的安全隐患,本文采用量子加密技术加密数据,确保数据存储安全[5]。目前,已经得到实用化的量子密钥分发技术是由 BENNETT 和 BRASSARD 在 1984 年提出的 BB84 协议,该协议通过传输光子并测量光子的偏振态实现对称的量子密钥,但是其依赖于光纤网络,并且单光子的探测设备成本较高,能实现的传输距离极短,因此限制了其应用范围[6]。区块链技术具有分布式存储、可信赖、透明性、防篡改、去中心化以及可追溯的特性。本文利用区块链技术实现量子密钥的扩展应用,提升量子密钥分发的安全性和实用性。

1 相关知识(Related technologies)

1.1 区块链技术

区块链是一种融合多种现有技术的新型分布式计算和存储范式,它利用分布式共识算法生成和更新数据,并利用对等网络进行节点间的数据传输,结合密码学原理和时间戳等技术的分布式账本保证存储数据的不可篡改性,利用自动化脚本代码或智能合约实现上层应用逻辑[7]。与传统的数据库相比,区块链相当于一种分布式的数据库,采用去中心化的设计思想,使得数据的存储和处理不依赖于中心化机构而是由全网的节

收稿日期:2023-05-11

点共同维护,使得数据具有更高的安全性和透明性。

1.2 可搜索加密

可搜索加密技术是近年研发的一种技术,针对云服务器上存储的加密数据,采用可搜索加密算法在密文上进行关键字搜索。2004 年,BONEH 等[8] 提出了第一个公钥可搜索加密方案。公钥可搜索加密(PEKS)算法如下。

(1)$KenGen$:令 G_1 和 G_2 为两个阶为素数 p 的乘法循环群,双线性映射 $e:G_1\times G_1\rightarrow G_2$,构建哈希函数 $H_1:\{0,1\}^*\rightarrow G_1$ 和 $H_2:G_2\rightarrow\{0,1\}^{\log p}$。选择随机元素 $\alpha\in Z_p^*$ 和 G_1 的生成元 g。输出 $A_{pub}=[g,h=g^{\alpha}]$ 和 $A_{priv}=\alpha$。

(2)$PEKS(A_{pub},W)$:计算 $t=e(H_1(W),h^r)\in G_2,r\in Z_p^*$。输出 $PEKS(A_{pub},W)=[g^r,H_2(t)]$。

(3)$Trapdoor(A_{priv},W)$:输出 $T_W=H_1(W)^{\alpha}\in G_1$。

(4)$Test(A_{pub},S,T_W)$:令 $S=[A,B]$。测试是否 $H_2(e(T_w,A))=B$。如果是,则输出"yes";如果不是,则输出"no"。

1.3 量子密钥分发技术

量子密码是一门新型的交叉学科,是量子理论、信息科学和计算机科学相结合的产物。量子密钥分发(Quantum Key Distribution, QKD)是量子通信技术中应用最广泛的成熟技术,QKD 的安全性来自量子力学的两个特性:一是量子世界本质的真随机性,这是产生真随机密钥的关键;二是承载有非正交信息的单量子态不可以被完美复制[9]。量子密钥分发过程既可以通过光纤通信网络实现,也可以在无线空间或其他介质中实现,主要取决于采用的量子密钥分发协议。QKD 协议主要有基于离散变量类协议和基于连续变量类协议。

2 系统模型(System model)

本节介绍结合量子密钥和区块链的安全云存储模型和基于区块链事件监听机制的量子密钥分发模型。

2.1 结合量子密钥和区块链的安全云存储模型

本文提出了结合量子密钥和区块链的安全云存储方案,云存储系统模型图如图 1 所示。方案涉及多种技术的结合应用:使用量子密钥加密数据;利用可搜索加密实现数据密文的安全检索。采用云存储服务器和区块链结合的方式,云存储服务器用于存储原始数据密文,区块链用来存储数据的索引信息及量子密钥分发的标记信息,并且利用事件监听机制实现对称量子密钥的分发。云存储服务器可以存储各种形式的数据,本文以存储文件数据为例,对方案模型进行介绍。

2.1.1 模型参与实体

模型中的主要参与实体包括区块链、量子密钥云服务器、云存储服务器、后台服务器、客户端及用户。

区块链(BC):模型中的区块链类型为联盟链。区块链账本记录文件的索引信息及量子密钥分发的标记信息。

云存储服务器(FCS):FCS 负责存储原始文件的密文,存储成功后将文件密文存储地址返回,并响应用户的文件下载请求。

量子密钥云服务器(QKCS):QKCS 部署在云上,由高速时间相位编码技术生成量子密钥,并且负责提供量子密钥,生成量子密钥分发的标记信息,利用部署在其上的区块链软件开发工具包(Software Development Kit,SDK)调用交易以及进行区块链链码事件的监听。

后台服务器(BS):BS 中部署的服务端应用程序包含 RSA

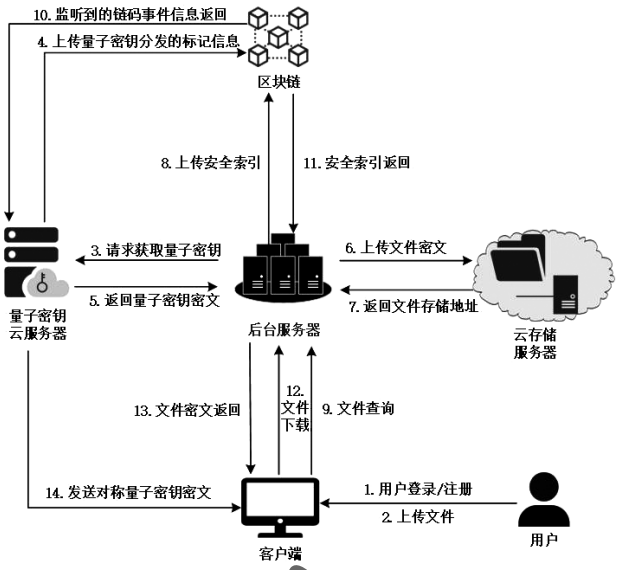

图 1　云存储系统模型图

Fig. 1 Diagram of cloud storage system model

密钥管理模块、AES 加密打包模块、用户信息管理模块、文件信息管理模块、公私钥管理模块、量子密钥 SDK 模块、区块链 SDK 模块和可搜索加密模块等。文件信息管理模块负责产生原始文件的 Hash 值,使用量子密钥对文件进行加密,并将文件密文上传到云存储服务器,将安全索引上传到区块链。用户信息管理模块的作用是管理用户信息。公私钥管理模块产生 BS 的公钥和私钥,管理合法客户端用户的公钥文件。量子密钥 SDK 模块用于连接量子密钥云服务器实时获取量子密钥。区块链 SDK 模块用于连接搭建的区块链网络,操作和管理区块链分布式数据库。可搜索加密模块负责对文件提取出的关键字进行加密,从而形成安全索引,在文件检索时为用户产生关键字搜索陷门,并匹配安全索引中的关键字密文。

客户端(CS):CS 部署的客户端应用程序是用户正常访问系统的平台,包含文件解密模块、公私钥管理模块、更改用户密码模块、量子密钥 SDK 模块、区块链 SDK 模块等。量子密钥 SDK 模块用于连接量子密钥云服务器,获取量子密钥云服务器发送的量子密钥密文。文件解密模块的作用是将来自后台服务器的加密文件利用量子密钥进行解密,然后计算解密后文件的 Hash 值,并将其与从区块链中查询出的文件 Hash 值进行比较。公私钥管理模块生成 CS 的私钥和公钥,管理后台服务器端的公钥文件。

用户(U):U 可以使用系统提供的云存储服务。

2.1.2 方案具体流程

(1)系统初始化,后台服务器应用程序进行全局公共参数设置,生成系统公共参数 $params=\{g,G_1,G_2,e,p,H_1,H_2,H_3\}$。

(2)量子密钥云服务器注册成为联盟链用户,联盟链为 QKCS 生成公私钥对,即 $\{pk_q,sk_q\}$,BS 的公私钥管理模块根据 $params$ 生成 BS 的公钥和私钥对 $\{pk_a,sk_a\}$。

(3)用户 U 登录客户端注册身份,CS 的公私钥管理模块根据 $params$ 生成 U 的公钥和私钥对 $\{pk_u,sk_u\}$,U 通过 CS 上传文件 F 并设置搜索文件的关键字 W。

(4)BS 中量子密钥 SDK1 模块根据量子密钥云服务器的下载服务地址请求获取文件加密量子密钥 k，QKCS 使用 BS 的公钥 pk_a 将 k 加密为 $\hat{k}=RSA_{pk_a}(k)$，通过经典信道发送给 BS 中的文件信息管理模块，同时量子密钥云服务器将发送的量子密钥 k 在数据库的密钥 ID 和量子密钥 k 的 Hash 值与用户 ID 构成键值对{用户 ID，量子密钥 ID+Hash 值}上链存储。

(5)BS 的文件信息管理模块对文件 F 进行哈希运算后生成 Hash 值 H_F，使用后台服务器的私钥 sk_a 解密量子密钥 k，$k=RSA_{sk_a}(\hat{k})$。利用 AES 加密算法 $\hat{F}=AES_k(F)$，得到加密文件 $\hat{F}$，并上传至云存储服务器，同时云存储服务器返回文件密文的存储地址 $Addr$。

(6)可搜索加密模块执行可搜索加密生成算法，将文件关键字 W 加密为关键字密文 $\hat{W}$，然后将关键字密文 $\hat{W}$、文件密文存储地址 $Addr$、用户 ID 以及 H_F 等信息组成安全索引 $Index=\{\hat{W},Addr,ID,H_F\}$ 数据结构并存储于 BC。

(7)U 需要访问包含某关键字 W 的文件时，利用客户端发起文件共享请求，可搜索加密模块为该请求产生搜索陷门 TD，利用搜索陷门向区块链发起查询交易，匹配含关键字 W 的文件索引，并返回安全索引 $Index$，在客户端展示检索到的文件基本信息。

(8)客户端收到文件查询请求阶段反馈的索引 $Index$ 信息时，在量子密钥云服务器中设置的区块链 SDK2 也利用监听器获取索引 $Index$ 信息。根据 $Index$ 信息中的用户 ID，区块链 SDK2 可以获取已经存储在区块链账本中用户 ID 标识的量子密钥 ID，再根据量子密钥 ID 从量子密钥数据库中获取相应的量子密钥 k。

(9)U 通过客户端下载搜索到的文件时，量子密钥云服务器使用用户的公钥加密得到量子密钥，然后将密文发送到客户端，利用 U 的私钥解密量子密钥 k。客户端通过索引中文件地址信息从云存储服务器拿到文件密文并利用 AES 解密算法 $F=AES_k(\hat{F})$，解密得到明文 F。

2.2 基于区块链事件监听机制的量子密钥分发模型

为了实现结合量子密钥和区块链的安全云存储方案中量子密钥的运用，设计了基于区块链事件监听机制的量子密钥分发模型(图 2)。

(1)Alice、Bob 和量子密钥云服务器注册成为区块链的用户，区块链为用户生成对应的公钥和私钥。

(2)Alice 根据量子密钥下载服务地址，向量子密钥云服务器发送量子密钥下载请求。

(3)量子密钥云服务器从区块链获取到 Alice 的公钥，用 Alice 公钥将一串长度为 256 bit 的量子密钥加密成密文，然后通过经典信道发送给 Alice，Alice 用自己私钥解密，获得量子密钥明文。量子密钥云服务器将发送的量子密钥在数据库的密钥 ID 和量子密钥的 Hash 值标识为 Alice 上链存储，此为量子密钥分发标记信息。

(4)Bob 向区块链发起查询 Alice 所用量子密钥的交易。此时，区块链链码状态发生变化，触发链码中定义的事件，然后调用区块链事件通知机制，将事件类型和相关数据通知区块链链码事件监听器，其中相关数据是指 Bob 所发起交易的

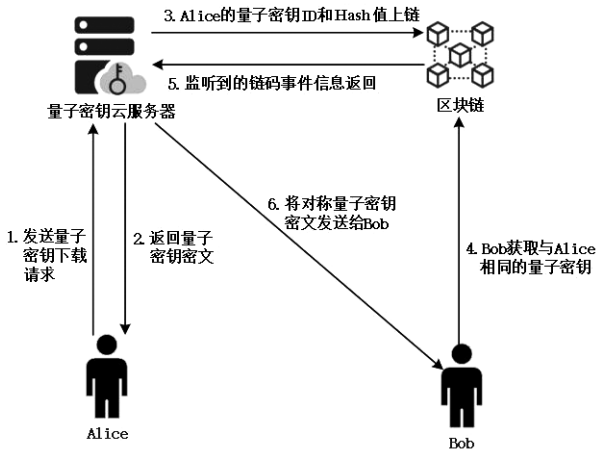

图 2 基于区块链事件监听机制的量子密钥分发模型

Fig. 2 Quantum key distribution model of event monitoring mechanism based on blockchain

payload 内容，即 Alice 的量子密钥分发标记信息。

(5)量子密钥云服务器所设置的区块链链码事件监听器监听到 Bob 发起交易产生的链码事件，获取 Bob 交易的信息，根据 Alice 的量子密钥 ID 从量子密钥数据库中获取相应的量子密钥，利用 Bob 的公钥加密生成量子密钥密文，然后通过经典信道发送给 Bob。

(6)Bob 收到量子密钥密文后，根据自己的私钥解密量子密钥明文，并计算量子密钥 Hash 值，并与从区块链中查询到的标识为 Alice 的量子密钥 Hash 值进行比对，若相同，则 Bob 获取到了未被篡改且与 Alice 相同的对称量子密钥，至此量子密钥分发完成。

3 安全性与隐私性分析(Security and privacy analysis)

半可信的云服务器存储的是文件密文，本文中使用量子密钥作为 AES 算法的加密密钥进行文件加密。有研究表明：对于高级加密标准(AES-256)这样的对称加密算法，适用于大量数据快速加密，并且使用量子密钥这种完全随机的高度安全密钥作为初始密钥，可以保证即使在量子攻击的情况下，仍然是安全的，保证了数据的机密性[10]。文件的 Hash 值记录在区块链账本中，区块链自身具备的特性保证了区块链账本数据难以被篡改，同时可以验证云服务器中存储的文件数据是否是完整的。

量子密钥云服务器上链存储的量子密钥标记信息仅包含量子密钥在数据库的存储 ID 和哈希摘要值，由于 ID 值不包含有效信息，而且哈希函数具有单向性，因此不会从量子密钥标记信息获取敏感信息。保证在量子密钥云服务器向用户发送量子密钥时，量子密钥服务器使用用户公钥对量子密钥进行加密，此过程的安全性由 RSA 算法[11]的安全性保障。综上，本系统兼顾安全性与隐私性。

4 实验与性能分析(Experiment and performance analysis)

4.1 实验环境

对本文提出的方案进行数值模拟实验，实验环境如表 1 所示。

表1　实验环境表

Tab.1 Table of experimental environment

实验环境	名称
开发平台	Windows 11
后端框架	Spring
前端框架	Vue
编程语言	Java,Golang
处理器	Inter Core i5
内存	16 GB
区块链开发平台	Ubuntu16.04
区块链环境	Hyperledger Fabricv 2.4.1

4.2　区块链性能测试

本文提出的方案是基于区块链技术实现的,而区块链交易的更新和查询时间开销是系统性能的关键因素。在整个方案中,文件的安全索引和量子密钥分发的标记信息均存储到区块链上,并在必要时进行查询追溯。由于安全索引在区块链交易中是属于数据量最大的,因此本文开展的实验以安全索引的交易为代表,通过测试联盟链网络交易的更新和查询操作的吞吐量以及平均时延评估本方案的性能。

通过 Caliper 工具分别发送从 1 000 次到 10 000 次的查询和更新文件安全索引交易至 Fabric 联盟链网络,每次实验测试 10 次,计算交易吞吐量和时延的平均值,结果如图 3 和图 4 所示。

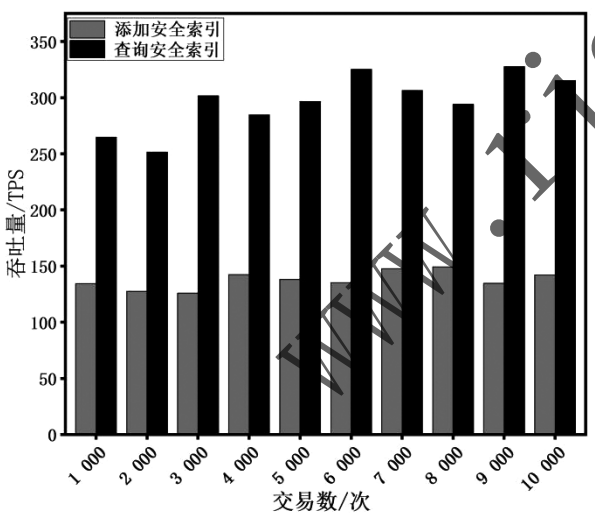

图 3　区块链添加和查询索引的吞吐量

Fig. 3 Throughput for adding and querying indexes in blockchain

从图 3 和图 4 可以看出,区块链添加安全索引时,随着交易数量的变化,成功的交易基本维持在每秒 135～150 次,并且时间延迟也基本保持在 0.15～0.23 s。区块链查询安全索引时,随着交易次数的增加,区块链交易始终维持着较高的吞吐量和较低的时间延迟;即使有很高的交易数量,例如 10 000 次交易,也能达到约 0.018 s 的低时间延迟和每秒 315 次成功交易的高吞吐量。因此得出,本系统构造的区块链并不适合过高并发交易,但是在较低并发的交易情况下,区块链能够发挥不错的效果。

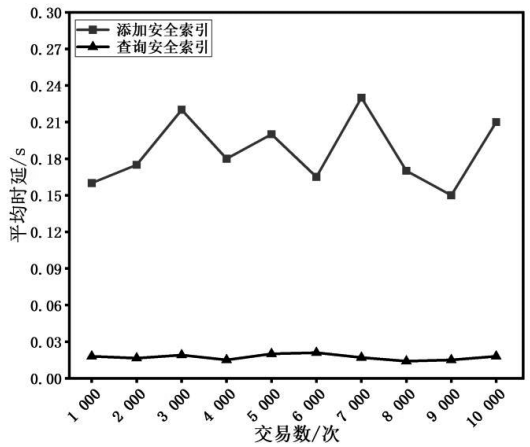

图 4　区块链添加和查询索引的平均时延

Fig. 4 Average latency for adding and querying index in blockchain

4.3　系统效率测试

为验证本文方案的可行性和效率,通过实际部署的区块链和量子密钥云服务器以及量子密钥分发网络进行实验分析。量子密钥云服务器 QKCS 采用 DELL Power Egde R740,CPU 型号为 Intel(R) Xeon(R) Silver 4110 CPU @2.10 GHz,内存为 32 GB,硬盘大小为 4 TB。量子密钥分发设备基于诱骗态 BB84 量子密钥分发协议,采用时间相位编码技术,集成千兆级工作频率的量子信号发射模块。

在云存储的应用场景下评估系统的性能。用户上传文件,后台服务器从 QKCS 获取量子密钥,将量子密钥加密文件储存在云存储服务器中。用户下载文件,经过量子密钥分发,获取文件密文解密量子密钥,解密出文件明文。通过测试文件上传获取加密量子密钥花费的时间和下载文件获取解密量子密钥的时间,分析方案的效率。

对于后台服务器获取加密文件量子密钥的消耗时间和客户端接收对称解密量子密钥的消耗时间,本文进行了 10～100 次的测试,将得到的数据进行归纳整理,得到结果如图 5 所示。

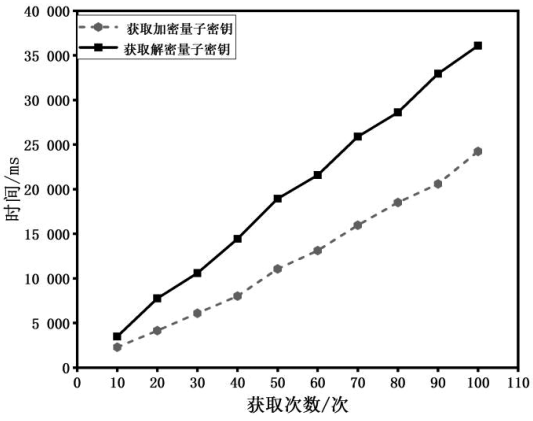

图 5　获取对称量子密钥消耗时间

Fig. 5 Consumption time of obtaining symmetric quantum keys

本文不考虑量子密钥的生成过程,仅对存储于云存储服务器的量子密钥做扩展运用,以测试本文设计的量子密钥分发方案的实际表现,评估系统性能。从图 5 可以看出,在网络环境稳定的情况下,客户端获取解密量子密钥花费的时间会比后台

服务端获取加密量子密钥花费的时间稍长，这是进行区块链交易需要消耗一些时间导致的。从图5展示的实验数据可以看出，后台服务端每次获取加密量子密钥的平均时间约为242 ms，客户端每次获取解密量子密钥的平均时间约为360 ms，因此对称量子密钥分发实现了较高的分发效率，满足实际的使用场景。

5 结论(Conclusion)

本文提出了一种基于区块链的量子密钥分发方案，并将此方案实际运用于云存储环境中。首先，考虑到经典的量子密码体系虽然具有绝对的安全性，但是其建设成本极高且通常只适用于两端通信，因此利用区块链技术设计了实用性较高的对称量子密钥分发方法。其次，本文充分利用量子密钥的特征和优势，将其与经典加密方式融合应用到云存储中的数据加密上，实现了量子密钥的扩展运用。最后，对本文提出的整体方案进行了安全性分析，并对方案进行模拟实验，测试区块链性能和对称量子密钥分发效率，分析方案的综合性能，确认了本方案具有良好的安全性和实用性。

参考文献(References)

[1] BENTAJER A, HEDABOU M, ABOUELMEHDI K, et al. CS-IBE: a data confidentiality system in public cloud storage system[J]. Procedia computer science, 2018, 141: 559-564.

[2] LAN C H, LI H F, YIN S L, et al. A new security cloud storage data encryption scheme based on identity proxy re-encryption[J]. International journal of network security, 2017, 19: 804-810.

[3] SERMAKANI A M, PAULRAJ D. Effective data storage and dynamic data auditing scheme for providing distributed services in federated cloud[J]. Journal of circuits, systems and computers, 2020, 29(16): 2050259.

[4] HUANG C Y, WEI S J, FU A M. An efficient privacy-preserving attribute-based encryption with hidden policy for cloud storage[J]. Journal of circuits, systems and computers, 2019, 28(11): 1950186.

[5] MAVROEIDIS V, VISHI K, ZYCH M D, et al. The impact of quantum computing on present cryptography[J]. International journal of advanced computer science and applications, 2018, 9(3): 405-414.

[6] 张文卓. 信息安全与量子加密解决方案将紧密结合[J]. 中国信息安全, 2021(z1): 197.

[7] 曾诗钦, 霍如, 黄韬, 等. 区块链技术研究综述: 原理、进展与应用[J]. 通信学报, 2020, 41(1): 134-151.

[8] BONEH D, DI CRESCENZO G, OSTROVSKY R, et al. Public key encryption with keyword search[C]//Springer. Proceeding of the International Conference on the Theory and Applications of Cryptographic Techniques. Berlin, Heidelberg: Springer, 2004: 506-522.

[9] 韩家伟. 量子密钥分发与经典加密方法融合关键技术研究[D]. 长春: 吉林大学, 2018.

[10] RAHMAN M, ZHOU L, CHAKRABARTTY S. SPoT-KD: a protocol for symmetric key distribution over public channels using self-powered timekeeping devices[J]. IEEE transactions on information forensics and security, 2022, 17: 1159-1171.

[11] RIVEST R L, SHAMIR A, ADLEMAN L. A method for obtaining digital signatures and public-key cryptosystems[J]. Communications of the ACM, 1978, 21(2): 120-126.

作者简介:

孙 羽(1997-)，男，硕士生。研究领域：区块链应用，隐私保护。

党 仁(1997-)，男，硕士生。研究领域：区块链应用，量子通信。

周 虎(1998-)，男，硕士生。研究领域：区块链应用，身份认证。

朱德新(1982-)，男，硕士，讲师。研究领域：区块链，量子密码技术。

(上接第13页)

参考文献(References)

[1] 张幕. 蜂窝车联网技术标准与应用概述[J]. 网络新媒体技术, 2023, 12(2): 48-54.

[2] 陈利红. 基于车联网技术的交叉口交通信号控制系统研究[J]. 计算机时代, 2019(1): 9-12.

[3] 邱彬, 李广友. 智能网联汽车数据安全管理研究[J]. 汽车工程学报, 2022, 12(3): 307-313.

[4] 张勇. 智能网联汽车数据安全认识与思考[J]. 时代汽车, 2022, 19(9): 7-9.

[5] 李克强, 李家文, 常雪阳, 等. 智能网联汽车云控系统原理及其典型应用[J]. 汽车安全与节能学报, 2020, 11(3): 261-275.

[6] XU W C, ZHOU H B, CHENG N, et al. Internet of Vehicles in Big Data Era[J]. 自动化学报(英文版), 2018, 5(1): 19-35.

[7] 段杰文. 智能网联汽车云平台和大数据分析[J]. 汽车电器, 2020, 61(6): 8-9.

[8] 李业伟. 基于车联网大数据的交通路况预测研究[J]. 信息通信技术, 2017, 11(6): 74-78.

[9] YANG F C, WANG S G, LI J L, et al. An overview of internet of vehicles[J]. 中国通信(英文版), 2014(10): 1-15.

[10] 梁雪辉. 基于车联网的大数据应用研究[J]. 电子测试, 2016, 23(9): 74, 86.

[11] 时瑞浩, 宋文明, 霍广. 基于车联网大数据的车辆智能辅助驾驶功能分析与实时告警系统设计[J]. 汽车周刊, 2022, 14(11): 72-73.

[12] 高新宇, 刘璐. 智能网联汽车云控系统原理及应用分析[J]. 汽车测试报告, 2022, 19(12): 62-64.

[13] 王琳. 汽车智能网联系统中远程启动技术的应用研究[J]. 时代汽车, 2023, 20(5): 13-15.

[14] 郭戈, 岳伟. 智能交通系统中的车辆协作控制[M]. 北京: 机械工业出版社, 2016: 13.

[15] 崔正杰, 刘南杰, 赵海涛. 基于管-云-端结构的汽车远程实时监控系统设计[J]. 微型机与应用, 2014, 33(24): 91-94.

作者简介:

陈建国(1987-)，男，硕士，工程师。研究领域：信息化项目管理，软件开发。