Optoelectronics 光电子, 2023, 13(3), 84-91
Published Online September 2023 in Hans. https://www.hanspub.org/journal/oe
https://doi.org/10.12677/oe.2023.133010

Hans汉斯

基于低成码率的量子密钥存储和使用方案

许子豪[1]，朱向冰[1]，卢　萍[1,2]，刘　云[2]

[1]安徽师范大学物理与电子信息学院，安徽　芜湖
[2]安徽问天量子科技股份有限公司，安徽　芜湖

收稿日期：2023年8月15日；录用日期：2023年9月11日；发布日期：2023年9月19日

摘　要

为了解决现有量子保密通信中安全密钥成码率过低带来的安全隐患，提出了一种基于低成码率的量子密钥存储和使用方案。构建量子加密设备硬件架构，改进量子密钥的存储方式与使用机制。将密钥池分为现役池与备用池，现役池中密钥用来加密和解密数据，备用池用来接收安全密钥。对现役池中的量子密钥进行分组及编号，随机选择密钥进行加密，根据密钥内部的二进制数来选择不同的加密方式，增加了破解密钥的难度。这种方案不仅能保证量子加密的高安全性，还可提高量子密钥的使用效率。

关键词

量子保密通信，量子密钥，加密，存储

A Quantum Key Storage and Utilization Scheme Based on Low Coding Rate

Zihao Xu[1], Xiangbing Zhu[1], Ping Lu[1,2], Yun Liu[2]

[1]School of Physical and Electronic Information, Anhui Normal University, Wuhu Anhui
[2]Anhui Qasky Quantum Science and Technology Co., Ltd., Wuhu Anhui

Received: Aug. 15th, 2023; accepted: Sep. 11th, 2023; published: Sep. 19th, 2023

Abstract

In order to solve the security risks caused by the low code rate of the security key in the existing quantum secure communication, a quantum key storage and use scheme based on low code rate is proposed. The hardware architecture of the quantum encryption device is constructed to improve the storage method and utilization mechanism of the quantum key. The key pool is divided into an active pool and a standby pool, where the keys in the active pool are used to encrypt and decrypt data, and the standby pool is used to receive security keys. The quantum keys in the active pool

文章引用: 许子豪, 朱向冰, 卢萍, 刘云. 基于低成码率的量子密钥存储和使用方案[J]. 光电子, 2023, 13(3): 84-91.
DOI: 10.12677/oe.2023.133010

are grouped and numbered, the keys are randomly selected for encryption, and different encryption methods are selected according to the binary number inside the key, which increases the difficulty of cracking the key. This scheme not only ensures high security of quantum encryption, but also improves the efficiency of quantum key usage.

Keywords

Quantum Secure Communication, Quantum Key, Encryption, Storage

1. 引言

随着分布式计算的成熟和量子计算机概念的提出，使得许多基于计算复杂度的经典密码体制的安全性受到质疑。在依托量子计算机强大算力的 Shor 量子算法提出后，经典密码中基于离散对数、大数分解问题的公钥密码体制变得不再安全；而 Grover 搜索算法的提出则极大地缩减了搜索时间，这使得经典加密算法的安全性面临巨大的威胁[1] [2]。

为了保障通信安全、应对量子计算的威胁，各国都在积极投入资源研究量子保密通信，量子密钥分发(Quantum Key Distribution, QKD)能够为合法的通信方实时的建立安全的密钥，结合“一次一密”算法可以实现信息论上的无条件安全[3]，但量子通信中也存在一些问题。例如，量子密钥分发与经典密码应用融合时，量子密钥的成码率太低，导致有效的密钥的数量严重不足，不得不多次采用相同的密钥进行加密，安全性得不到保障[4] [5]。

针对可用密钥数不足的问题，现有的研究主要是改进 QKD 协议[6]与提升有限密钥的使用效率。相较于前者，不涉及量子原理的高效密钥使用方案操作简单，更具备实际的使用价值。例如，文献[7]通过使用固定密钥池提前存储密钥，设计了一种两阶段密钥池共享方案实现了量子密钥资源的高效调配；文献[8]通过对密钥进行拆分再组合的方式，在密钥总数不变的情形下提高了密钥的使用效率。

本文结合量子密钥分发技术和密码通信的特点，设计了一种基于低成码率下的量子密钥存储和使用方案。该方案将密钥池分为现役池与备用池，随机选取现役池内的密钥进行加密，同时根据密钥内部的二进制数来选择加密方式，增加了破解难度，在保证量子高安全性的同时，解决了量子密钥数量不足带来的安全性下降的问题。

2. 量子密码现状分析

2.1. 量子密码的优势与局限

与传统通信技术相比，量子技术具有高安全性的特点，当被用于安全密钥分发系统时，由于量子具有不确定性与不可复制的特性，一旦有窃听行为发生便会被发现，攻击者无法获取密钥。因此，量子密钥分发技术相较传统密钥分发机制有着不可比拟的优势，同时也是目前实用化程度最高的量子技术。

虽然量子密码有着极高的安全性，相关的理论研究与设备研发也都在逐步完善，但仍然存在一些问题。首先是量子密钥分发协议的安全性与可行性上存在缺陷，需要进一步验证与完善[9] [10]，其次是由于量子通信本身的物理特性，量子通道是通过光纤传送微弱单光子信号，容易受到距离长度与复杂环境

的影响，使得量子密钥的成码率较低[11]。如何在实际生产中更加高效的利用量子密码，就需要解决上述的问题。因此，需要使用一套更为高效的量子密钥存储与使用方案，来提高量子通信中低成码率下的密钥的使用效率，进而实现安全性和实用性的提升。

2.2. 密钥生成的分析

在量子密钥分发的过程中，需要通过量子态制备、传输、量子态探测、基矢比对、纠错和保密放大过程，最终生成双方共享的安全密钥。安全密钥指的是量子密钥分发设备形成的最终的双方共享的密钥。安全码率是每秒生成的安全密钥量，又称“安全密钥成码率”。现有的量子通信技术存在的主要缺陷表现为安全密钥成码率太低。

以 50 MHz 相位型 QKD 系统在电力架空环境(环回的光纤总长度约 1.973 km，衰减器为 14.73 dB)为例，安全密钥成码率约 1700 bps，当气温降到 0 摄氏度以下时成码率降到 1500 bps。使用中继的方式可以有效地延长通信距离，由于传输距离长(达到数千公里)，沿途可能会遇到各种极端的环境甚至人为攻击和破坏，安全密钥成码率将会进一步降低[12]。

经典信道的传输速度比较快，可以达到数十 Mbps，而量子密钥的成码率太低，不超过 2 Kbps，导致有效的密钥的数量严重不足，不得不多次采用相同的密钥和同一种加密方法进行加密，安全性得不到保障[13]。在需要不断地传输大量的信息通信网络中，明文中也存在着很多重复的内容，如电力系统中大多数调度指令和遥测指令的主要部分是相同的，只有一些参数不一样[14]，由于明文信息的相似性，导致密钥更容易被破解，给系统的运行带来了隐患。

因此，为了能够更加充分地利用量子密码系统，需要使用一套更为有效的量子密钥存储与使用方案来提升密钥使用效率。

3. 密钥存储与使用方法

3.1. 系统架构

在多个行业中需要使用量子通信技术提高安全性，都存在着“安全密钥成码率太低导致的安全性下降”的问题，本文从密钥的分配和使用等方面突破该技术难题。图 1 为本文提出的量子加密设备硬件架构，包含几个模块：1) 量子密钥的接收和存储模块，根据电力系统远程通信的特点，存储模块的容量要足够大，并实现对密钥的动态管理；2) 与电脑之间传输文件的模块，通过 USB 接口与电脑进行通信；3) 数据加密解密模块，为了保障加密速度，计划通过硬件实现加密算法；4) 网络接口模块，通过以太网实现远程数据的交换；5) 中央控制模块，负责控制其他的模块的运转并响应按键。在硬件模块的基础上编写程序实现本文的量子密钥存储和使用协议。

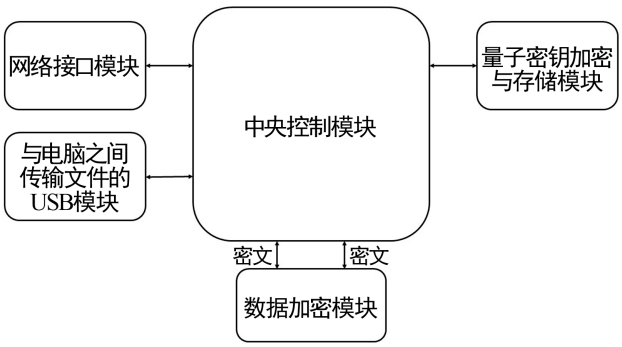

Figure 1. Hardware structure of encryption and decryption device
图 1. 加密和解密装置硬件结构

3.2. 密钥交互机制

本文提出了量子密钥的存储与交互机制。参考图 2，发送方和接收方都有两个密钥池，分别是现役池和备用池，所有密钥池的容量相同。现役池中的密钥用来加密和解密数据；备用池用来存放量子密钥分发系统传递的安全密钥，即双方共享的密钥。

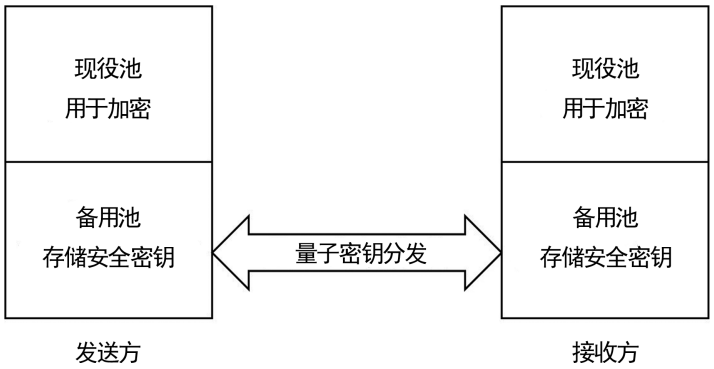

Figure 2. Key storage structure for sender and receiver
图 2. 发送方和接收方的密钥存储结构

当备用池存满后，将备用池转为现役池，原先的现役池变为备用池，旧的密钥全部废弃，备用池接收量子密钥分发系统传递的新的安全密钥，当备用池存满新的安全密钥后，再将备用池和现役池互换。

按照文献 10 中电力系统量子通信的密钥成码率约为 1500 bps 来估算，每天 24 小时连续传递密钥，每天得到的 123.6 Mbit 的密钥，备用池和现役池密钥容量都是 128 Mbit，它们都可以存储 128 Mbit 的密钥。正常情况下，密钥池内的更新周期小于 36 小时。如果量子密钥分发系统出现故障，备用池中的密钥将停止更新，只有等到故障恢复后，备用池才能转换成现役池。现役池中始终有 128 Mbit 的密钥，即使量子密钥分发系统出现问题导致安全密钥成码率非常低，也始终有足够多的密钥，不影响对信息的加密。

通信双方对密钥进行分组；图 3 为对密钥分组的过程。通信双方各自按照同样的方式将自己的现役池中的密钥分成多组，根据二进制数的排列顺序进行分组，最前面的二进制数是第 1 组密钥，接着的二进制数是第 2 组密钥，依次类推，直到第 n 组密钥，图 3 中每组密钥的长度是 128 bit，得到 1 M 组密钥。

每组密钥的组号就是编号，在图 3 中，第 1 组密钥的编号为 1，第 2 组密钥的编号为 2，……，第 k 组密钥的编号就是 k。

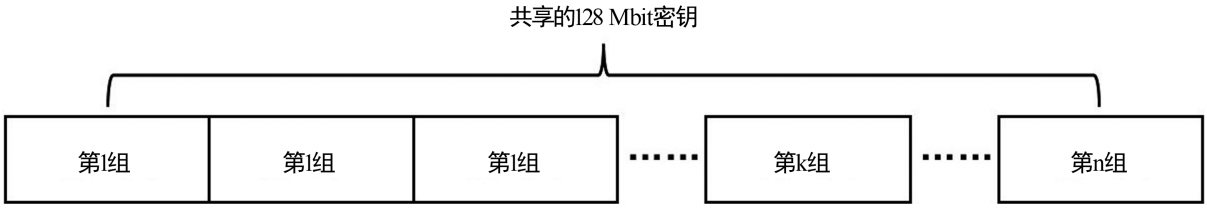

Figure 3. The grouping and numbering of quantum keys
图 3. 量子密钥的分组及编号方式

通信双方使用每组密钥中一些二进制位作为标志位，参考图 4，使用第 1 个二进制位、第 3 个二进制位、第 5 个二进制位作为标志位，这三位二进制数排列在一起，可以得到 8 种结果，对应的十进制数是 0、1、2、3、4、5、6、7，在图 4 中得到的是 110，对应的 10 进制数是 6。

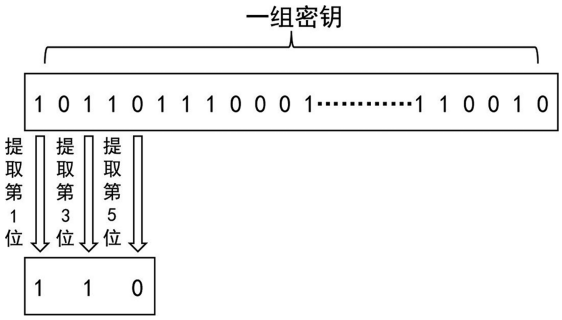

Figure 4. Sign bit selection for quantum keys
图 4. 密钥的标志位选取

十进制数 0 到 7 分别对应不同加密算法：0 对应 AES 算法，仅使用 AES 算法进行加密，只加密一次；1 对应 SM4 算法，仅使用 SM4 算法进行加密，只加密一次；2 对应 ZUC 算法，仅使用 ZUC 算法进行加密，只加密一次；3 对应 ZUC + SM4，先使用 ZUC 算法加密一次得到中间结果，再使用 SM4 算法对中间结果做一次加密运算，将最终结果作为密文；4 对应的算法是 AES + SM4，先使用 AES 算法加密一次得到中间结果，再使用 SM4 算法对中间结果加密一次，将最终结果作为密文；5 对应 AES + ZUC，先使用 AES 算法加密一次得到中间结果，再使用 ZUC 算法对中间结果加密一次，将最终结果作为密文；6 对应 XOR + AES，先使用密钥对明文进行 XOR 运算，然后再用 AES 算法加密；7 对应 XOR + ZUC，先使用密钥对明文进行 XOR 运算，然后再用 ZUC 算法加密。

图 5 是工作过程，发送方得到一组明文信息；发送方随机选择现役池中的一组密钥，读取标志位，根据标志位确定加密算法；使用密钥按照该加密算法对该组明文信息进行加密，得到一组密文。

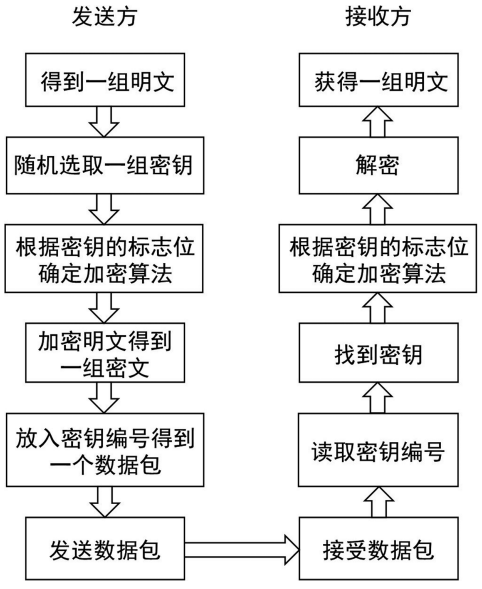

Figure 5. Encryption and decryption and the process of sending and receiving
图 5. 文件加密解密及收发流程

发送方将密钥的编号和该组密文放在一起得到一个数据包。如图 6，密钥池中有 1 M 组密钥，使用 24 位二进制数(3 个字节)表示密钥编号，将密钥编号的前 2 个字节的二进制数放在密文的前部，密钥编号的最后一个字节放在密文的后面，得到一个数据包。

Figure 6. Data package
图 6. 数据包

发送方将数据包通过经典信道传递给接收方。接收方接收数据包，读取数据包中的密钥编号，根据密钥编号找到对应的密钥，根据标志位得到加密算法，对密文进行解密，得到一组明文；参考图 5 中右侧的部分。

不同的密钥采用不同的加密方式，各数据包的加密方式不一样，即便攻击者知道密钥的编号，但是不知道密钥的具体内容，因而不知道加密方式，攻击者需要尝试多种加密算法，极大地增加了破解的难度；能够有效提高网络通信的安全性。

4. 硬件

根据前文所述，量子密钥的成码率较低，不超过 2 Kbps，考虑到成本、开发时间等因素，量子密钥的接收和存储模块采用 RS232 通信协议完成，在标准的 RS232 通信协议中，电压值较高，本文使用改进后的通信协议，将电压值降到与中央控制模块(3.3 V)一致。密钥池的总容量是 256 Mbit，为了与现有的网络密码机相适应，采用 SD 卡来存储密钥，同时也用来存储密文和明文。SD 卡模块使用 Class 10 级别的 MicroSD。

采用 USB 通信的方式与电脑之间传输文件，在现阶段使用 FT232 芯片作为 USB 的 PHY 层。FT232 芯片在内部完成了 USB 硬件接口差分电平转换，还封装了 USB 的相关协议，留出了数据交互接口。相比与市面上其它的芯片，FT232H 有着官方提供的工具软件“FT_Prog”，可以直接在 UI 界面进行模式配置，而不需要编写模式配置的相关代码，减少了开发的时间。

数据加密解密模块和中央控制模块使用 Xilinx Artix 7 系列 XC7A35T 芯片，FPGA 芯片能高速运算设计的多种加密算法。

网络接口中 PHY (物理层)芯片使用 YT8511，YT8511 是一个千兆以太网物理层收发器，支持 1000/100/10 Mbps 通信速率，其内部参数通过 MDIO 接口进行配置。上位机通过 RJ45 接口连接网线实现全双工网络通信功能。

5. 实验与测试

本文对系统的硬件和软件分别进行了实验测试，制作成样机后，通过实验获取软件所需要的数据，测试各模块功能是否满足要求。

首先进行量子密钥的接收和存储模块的测试，由于串口通信是以数据包的形式发送，测试使用 1 位起始位、8 位数据位和 1 位停止位来构成 10 bit 的数据包，按量子密钥的成码率为 1700 bps 来计算，最接近的 RS232 通信速率是 2400 bps，设备间实际通信的波特率最终选择 2400 bps，考虑到 SD 卡每一扇区的存储空间为 512 Bytes，为便于测试，使用计算机模拟密钥分发设备，先向样机发送完 512 Bytes 的数据后，样机将这些数据写入 SD 卡，再从样机的 SD 卡中读出数据，传回计算机，通过对比两者数据是否一致来检测样机的密钥接受存储功能。经测试，计算机发送与接收的数据完全一致。再通过计算机发送和接受 128 M 的数据，并进行比对，测试中样机的密钥接受存储功能正常。

在量子密钥的接收和存储功能测试后，本文对数据加密模块进行了相应的测试，量子密钥分发设备

分发设定的密钥数据给样机，根据数据加密模块的功能，当有明文需要加密时，会从 SD 卡中读取一段 128 bit 的密钥数据，并对其分组编号、读取标志位来确定加密方式，测试根据发送的密钥数据计算出数据包的理论数据，并编写一段测试代码来获取数据加密完成后的数据包数据，通过对比理论与实际结果来判断加密功能的实现情况。表 1 为测试使用的几组密钥以及所对应的编号、标志位和加密算法。

Table 1. Key for testing and corresponding information
表 1. 测试的密钥及对应信息

密钥	组数	标志位	加密方式	对应算法
100000…0	1	100	4	AES + SM4
010000…0	2	000	0	AES
001000…0	3	010	2	ZUC
000100…0	4	000	0	AES
000010…0	5	001	1	SM4

测试结果如表 2 所示。经过大量测试后，加密后所得数据包数据与理论的结果完全一致，测试证明，将明文加密成数据包的过程符合要求。

Table 2. Comparison of packet data
表 2. 数据包数据对比

密钥	数据包理论值	数据包实际值
100000…0	00wvuBVScwoEthAvEZFtSU+Re49qcZZQz0zKD16uNnvZw=1	00wvuBVScwoEthAvEZFtSU+Re49qcZZQz0zKD16uNnvZw=1
010000…0	00z6U9FjNpiUb4Ri0kfUzsLw==2	00z6U9FjNpiUb4Ri0kfUzsLw==2
001000…0	009eaba81532e77a40e0b6b318f5f9668a3	009eaba81532e77a40e0b6b318f5f9668a3
000100…0	00jNGeQ7cRqj7DJq6ZcA8kZA==4	00jNGeQ7cRqj7DJq6ZcA8kZA==4
000010…0	00rPgs0TLWzxgzwu2XPZf5Yw==5	00rPgs0TLWzxgzwu2XPZf5Yw==5

本文对量子加密设备进行解密功能的测试，通过对比上位机传输的明文与解密后的结果来判断系统整体功能的实现。如表 3 所示，展示了几组典型的测试结果，测试证明，明文与解密结果保持完全一致，验证了系统整体功能可以达到预期结果的结论。

Table 3. Comparison of plaintext and decryption results
表 3. 明文与解密结果对比

密钥	明文	解密结果
100000…0	1111	1111
010000…0	1111	1111
001000…0	1111	1111
000100…0	1111	1111
000010…0	1111	1111

6. 结论

在信息时代保护信息的安全是至关重要的，量子密码正是在计算机运算能力得到迅速提升、传统的密码系统备受挑战的背景下，以其在物理性质上的安全性另辟蹊径，在通信安全领域取得了广泛的关注与研究。然而，受限于现阶段的技术，量子分发设备的密钥生成速率较低，如何更加高效地去使用量子密钥是一个亟待解决的问题。本文提出了一种基于低成码率下的量子密钥存储和使用方案，匹配量子加密设备的成码率与通信系统数据安全性需求，可以解决量子加密通信中密钥数量不足的技术难题。我们也将探索如何在严酷的自然环境中提高量子密钥的成码率，以提高通信的安全性。

基金项目

芜湖市科技计划项目(2021hg04)。

参考文献

[1] 赖俊森, 吴冰冰, 汤瑞. 量子保密通信标准化现状与发展分析[J]. 电信科学, 2018, 34(1): 1-7.

[2] 蒋庆庆. 实用化量子密钥分发系统设计与实现[D]: [硕士学位论文]. 南京: 南京邮电大学, 2023.

[3] 刘东. 量子密码实际安全性与应用研究[D]: [博士学位论文]. 合肥: 中国科学技术大学, 2014.

[4] 冯雁, 刘念, 谢四江. 一种量子密钥池的双向使用方案[J]. 信息网络安全, 2020, 20(12): 40-46.

[5] 李大伟. 量子密钥分配实际安全性思考[J]. 信息安全与通信保密, 2022(9): 57-64.

[6] 叶子豪. 量子城域网密钥管理和端到端通信方法仿真研究[D]: [硕士学位论文]. 西安: 西安电子科技大学, 2021.

[7] Wang, L.C., Wang, D.S., Gao, J., *et al*. (2019) Research on Multi-Source Data Security Protection of Smart Grid Based on Quantum Key Combination. 2019 *IEEE* 4*th International Conference on Cloud Computing and Big Data Analysis* (*ICCCBDA*), Chengdu, 12-15 April 2019, 449-453. https://doi.org/10.1109/ICCCBDA.2019.8725680

[8] Tang, Z.F., Qin, Y.Y., Jiang, Z.M., *et al*. (2021) Quantum-Secure Microgrid. *IEEE Transactions on Power Systems*, **36**, 1250-1263. https://doi.org/10.1109/TPWRS.2020.3011071

[9] 黄安琪, 高彬舞, 石惟旭. 面向量子密钥分发的量子攻防技术及安全评估[J]. 国防科技, 2022, 43(6): 1-7.

[10] 胡倩倩, 冯宝, 李冬. 基于量子随机数发生器的量子密钥分发系统[J]. 计算机应用与软件, 2023, 40(4): 324-328.

[11] 刘宏伟. 实际量子通信系统及其安全性的实验研究[D]: [博士学位论文]. 北京: 北京邮电大学, 2019.

[12] 马茹昕. 电力量子保密通信系统测试技术研究[D]: [硕士学位论文]. 北京: 华北电力大学, 2019.

[13] 韩冰洋, 朱玉坤, 陈文伟. 基于密钥自演化的电力业务量子密钥分配方案[J]. 电子设计工程, 2019, 27(10): 128-132.

[14] 王东山, 李温静, 苑佳楠, 等. 面向电力通信接入网的量子密钥交互机制[J]. 供用电, 2019, 36(8): 36-40, 90.