山西大学学报(自然科学版)47(4):815—822,2024
Journal of Shanxi University(Nat. Sci. Ed.)

DOI:10.13451/j.sxu.ns.2024038

面向数字政府的量子安全加密通信框架

盛佃清[1,2]

(1.山西省人大常委会民族宗教侨务外事工作委员会,山西 太原 030600;
2.山西省信息技术应用创新工程研究中心,山西 太原 030060)

摘 要:随着数字政府建设的推进,数据安全和通信的保密性显得尤为重要。传统加密技术如非对称加密(Rivest-Shamir-Adleman,RSA)和椭圆曲线密码学(Elliptic Curve Cryptography,ECC)面临被破解的风险,特别是量子计算机上的Shor算法。因此量子密码学研究探索适用于数字政府的量子安全加密通信算法满足政府通信的特点,如大规模数据传输、多种通信参与者以及高安全性要求。本文提出了一套针对数字政府特定需求的量子威胁应对策略,包括对现有数字政府加密体系的威胁评估及定制化适应性策略;开发了新型的量子安全加密通信框架,并设计了量子加密协议(Quantum Enhanced Secure Communication Protocol,QESCP)。该框架考虑到政府通信的特点,如大规模数据传输、多种通信参与者以及高安全性要求,融合了量子密钥分发和特定的量子密码技术。通过仿真验证,算法在模拟的噪声环境下的通信效率达到了92.5%,同时对抗量子计算机攻击显示出了较高的安全性。

关键词:数字政府;量子安全;量子密钥分发;加密通信;量子通信应用
中图分类号:G203 **文献标志码**:A **文章编号**:0253-2395(2024)04-0815-08

A Quantum Secure Encrypted Communication Framework for Digital Government

SHENG Dianqing[1,2]

(1. *Standing Committee on Ethnic and Religious Overseas Chinese Affairs and Foreign Affairs, Shanxi Provincial People's Congress, Taiyuan* 030600*, China;*
2. *Innovative Engineering Research Center of Information Technology Application of Shanxi Province, Taiyuan* 030060*, China*)

Abstract: With the development of digital government progresses, the importance of data security and the confidentiality of communications cannot be overstated. Traditional encryption methods, including Rivest-Shamir-Adleman (RSA) and Elliptic Curve Cryptography (ECC), are increasingly vulnerable, particularly to the Shor algorithm on quantum computers. In response, research into quantum cryptography is advancing, focusing on developing quantum-secure encryption algorithms tailored to the unique requirements of digital government. These requirements include the need for large-scale data transmission, accommodation of numerous communication participants, and stringent security demands. This paper introduces a comprehensive set of strategies to counter quantum threats tailored to the specific needs of digital governments. These strategies encompass an assessment of the vulnerabilities in current digital government encryption systems and the development of bespoke adaptive measures. We also present a pioneering quantum-secure cryptographic communication framework and outline the Quantum Enhanced Secure Communication Protocol (QESCP). This framework leverages quantum key distribution and bespoke quantum cryptography techniques, designed with government communication needs in mind—highlighting large-scale data transmission, multiple participant engagement, and high security.

收稿日期:2023-10-18;**接受日期**:2024-02-27
基金项目:山西省科技战略研究专项(202204031401179;2021040313023)
作者简介:盛佃清(1963-),男,山西大同人,博士,正高级工程师,研究方向为云计算、量子安全、大数据技术。E-mail:yjyhzcx@sxctc.net
引文格式:盛佃清 . 面向数字政府的量子安全加密通信框架[J]. 山西大学学报(自然科学版),2024,47(4):815-822. DOI:10.13451/j.sxu.ns.2024038

Our simulation tests confirm the algorithm's efficacy, achieving a 92.5% communication efficiency in a simulated noisy environment and demonstrating robust security against quantum computer attacks.

Key words: digital government; quantum security; quantum key distribution; encrypted communications; quantum communication applications

0 引言

《中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要》提出要提升大数据等现代技术手段辅助治理能力,加快实现国家治理体系和治理能力现代化,推动全体人民共同富裕取得更为明显的实质性进展。随着信息技术和互联网的普及,数字化已经成为全球政府的一个核心战略,目标是通过电子方式为公众提供更加高效、透明和参与性的公共服务[1]。这一趋势被称为"数字政府"。数字政府是数字中国的重要建设内容,加强数字政府建设是创新政府治理理念和方式的重要举措,对加快转变政府职能,建设法治政府、廉洁政府、服务型政府意义重大。

然而,随着这种数字政府的推进,数据安全和通信的保密性变得越来越重要。传统的加密技术,如非对称加密(Rivest-Shamir-Adleman,RSA)和椭圆曲线密码学(Elliptic Curve Cryptography,ECC)等,长期以来为信息安全提供了坚固的保障[2]。然而,近年来,量子计算技术的突破性进展使得这些传统的密码体制可能会在不久的将来被破解。Shor算法是量子计算中的一个重要算法,特别是对于加密和信息安全领域,因为它提供了一种在多项式时间内破解RSA和ECC等公钥密码体制的方法。Shor算法可以在量子计算机上有效地破解RSA和ECC等公钥密码体制。这对全球数字政府的建设提出了巨大的安全挑战[3-4]。

量子计算利用量子叠加和纠缠等原理,从而在某些特定的计算任务上大大超越经典计算机的性能[5]。RSA和ECC等密码体制的安全性是基于某些数学问题的困难性,如大数分解和椭圆曲线离散对数问题。这些问题在传统的计算机上是非常困难的。但是,Shor算法利用量子计算机的特性,能够在可行的时间内解决这些问题,从而破解相关的密码。随着数字化进程的推进,政府越来越依赖于加密技术来确保信息的机密性、完整性和可用性。这不仅包括公民数据,还涉及国家安全、经济、健康和多种其他领域。因此,量子计算机的潜在威胁不能被忽视。为了应对这些威胁,研究人员和机构正在开展"量子密码学"的研究,以设计新的加密方案,这些方案即使在量子计算机出现的情况下也是安全的。这些新的密码体制基于一些被认为是对Shor算法和其他量子攻击方法安全的数学问题[6]。与已有的工作不同,大多数现有的量子安全研究侧重于广泛的信息安全领域,而本文专门针对数字政府的特定需求,如大规模数据传输、多种通信参与者和高安全性要求。在量子安全算法的研究中,常常需要在安全性和效率之间寻找平衡。本文提出的框架旨在确保在保持高度安全性的同时,还能够满足数字政府的实时、高效通信需求。

数字政府的通信安全需要应对潜在的量子计算威胁,确保公民数据和关键信息的安全。主要存在以下两点关键科学问题:(1)量子威胁与现有体系的适应性:在现有的数字政府通信架构中,哪些部分是最容易受到量子计算威胁的?需要评估不同的密码算法在面对量子攻击时的脆弱性,并确定哪些算法或部分需要紧急改进或替换。(2)量子安全算法的适用性与效率:在众多的量子安全算法中,哪些最适合数字政府的通信需求?考虑到数字政府的通信特性,如大数据量、多参与者和高安全需求,需要设计一个既高效又安全的量子安全通信框架。

为此,本研究旨在探索一种适用于数字政府的量子安全加密通信算法,不仅要考虑量子计算的威胁,还要满足政府通信的特点,如大规模数据传输、多种通信参与者以及高安全性要求。在面对量子计算日益增长的威胁,尤其是Shor的算法对传统公钥密码体制如RSA和ECC的潜在攻击能力,本研究针对数字政府的通信系统进行了深入探讨。首先,对现有的数

字政府加密体系进行了全面的威胁评估,明确了那些最容易受到量子计算威胁的部分,并为此提出了适应性策略。进一步研究了各种量子密码算法,目的是找到那些最能满足政府大规模、多参与者、高安全性要求的通信场景。为了解决效率问题,本文提出了一种量子密钥分发和加密通信算法,确保在维护上的高度安全性。本文的主要贡献和创新之处包括:

(1)提出了一套针对数字政府特定需求的量子威胁应对策略。这包括对现有数字政府加密体系的全面威胁评估,以及基于这些评估结果,针对量子计算挑战的定制化适应性策略;

(2)开发了新型的量子安全加密通信算法,设计一个概念性的量子加密协议(Quantum Enhanced Secure Communication Protocol ,QESCP);

(3)文章不仅研究了量子密钥分发的理论基础,还考虑了数字政府的特点,如高数据量、多样化的参与者和对高安全性的需求。

1 相关工作

1.1 量子威胁评估与现有体系的适应性策略

为了深入理解量子计算对数字政府通信体系的潜在影响,需要详尽的威胁评估。基于这些评估结果,可以对最容易受到量子威胁的部分制定策略,并提出适应性修改和建议[7-8]。其中包括混合加密策略的引入,以及对关键交换和证书生成机制的更新,确保它们在潜在的量子攻击面前仍然保持其安全性。对于量子威胁评估与现有体系的适应性,近年来已有众多的研究工作针对此进行了探索。Shor 在 1994 年提出了一种能够在量子计算机上有效地分解大整数的算法,这使得 RSA 加密可能会被破解。该算法的提出促使了对量子计算威胁的深入研究[9]。除了 Shor 算法,还有其他的研究关注于利用量子计算机破解其他加密方法。李婷等[10]提出了一种可外包解密的高效密文策略的属性基加密方案,郭丽峰等[11]对云存储中可验证的完全外包的属性基加密进行了研究。

尽管大规模的、能够破解现有密码的量子计算机还没有建成,但小规模的量子计算机已被用于模拟某些加密攻击,以评估实际的威胁。国际标准化组织和政府机构如美国国家标准与技术研究院(National Institute of Standards and Technology,NIST)正在进行后量子密码的标准化工作,确保选择的算法既安全又实用。为了对抗量子威胁,某些研究提出了混合使用经典和抗量子密码技术的策略,即在一个系统中同时使用两种密码技术。考虑到大规模量子计算机的建设还需要时间,某些建议进行逐步迁移,先在关键部分使用量子密码,然后逐渐扩展到整个系统。Yi 等[12]利用量子算法的对策来保护免受量子计算机攻击,提出了一种量子安全方案。为了保持保密性,提出了一种后量子非对称密钥加密方案,用生成的会话密钥加密信息。Kuang 等[13]探索了 QPP 量子实现的工作原理与对称加密和解密方案的工作原理,揭示了量子对量子和量子对量子之间的量子安全通信是可能的。

1.2 量子密码算法的选择与效率优化

针对数字政府的特定通信需求,需要深入研究各种量子密码算法,以确定哪些算法最适合这种场景。需要对算法进行详细的比较和评估,而且还需要一系列算法加速和优化技术,确保所选择的算法能够在保持高度安全性的同时满足大规模、多参与者的通信效率要求[14-15]。量子密码算法的选择与效率优化是后量子密码学研究的关键组成部分。随着量子计算机技术的逐渐成熟,该领域的研究也日趋活跃。格基密码学(Lattice-based Cryptography)是目前最有前景的后量子密码方案之一,它具有高效和理论上的安全性[16]。例如,Learning With Errors(LWE)和其变种,Ring-LWE 和 Module-LWE,是格基密码的核心问题。码基密码学(Code-based Cryptography)算法如 McEliece 和 Niederreiter 密码系统,基于线性码的困难性问题[17-18]。多变量多项式(Multivariate Polynomial Cryptography)基于多变量多项式方程的困难性问题,例如 Quadratic (MQ)问题。哈希基密码学(Hash-based Cryptography)主要基于哈希函数的一些困难性质,例如 Merkle 签名方案。为了了解实际应用中的性能,研究者对不同的后量子密码算法进行了实际测试,包括在各种硬件和软件平台上的实现[19-20]。例如,使用专用集成电路(ASIC)或可编程逻辑门阵列(FPGA)来实现

加密和解密操作,提供更高的吞吐量。

2 量子安全加密通信算法

面向数字政府的量子安全加密通信算法框架旨在适应未来量子计算的威胁,同时满足数字政府在大规模数据传输、多通信参与者和高度安全性方面的需求。该框架替换传统的公钥基础设施,引入量子公钥基础设施以支持量子安全的证书和密钥管理。此外,它还利用抗量子密码技术进行安全的密钥交换和会话建立,并实现基于这些技术的安全数据传输层。为了在安全性与效率之间找到平衡,该框架专注于算法选择、并行处理、硬件优化和算法参数调整。持续的量子威胁情报收集和框架的定期更新也是其关键组成部分,确保加密通信始终处于安全状态。该算法框架图如图1所示。

2.1 需求分析

数字政府通常涉及大量的数据交换,这可能包括从简单的公共服务申请到复杂的行政数据、公共健康数据、税务记录等。为了确保公共服务的高效运行,数据需要快速传输,这对加密算法的性能提出了要求。与一次性的数据交换不同,数字政府的数据传输往往是持续的,并需要长期的安全支持。与一个单一的机构或企业不同,数字政府的通信参与者可能包括各种政府部门、公民、企业和其他外部实体。参与者的身份和角色可能会随时间变化,需要一个动态的身份验证和授权系统。鉴于涉及敏感数据和公共利益,确保通信双方的真实性和合法性是至关重要的。高安全性要求政府通常持有大量的敏感数据,如公民个人信息、税务记录、健康记录等,这些数据的泄露可能导致重大的负面后果。鉴于政府数据的持久性和重要性,所选的加密方案不仅需要对抗目前的威胁,还需要考虑未来可能出现的威胁,如量子计算攻击。

2.2 核心组件

如图1所示,量子公钥基础设施是框架的基础,确保所有的密钥和证书管理在量子计算环境下都是安全的。量子公钥基础设施包括密钥交换机制组件、数据传输安全层组件、动态身份验证与授权组件和量子密码算法组件。安全的密钥交换机制考虑到数字政府涉及多种通信参与者,一个稳健和安全的密钥交换机制是必要的。此组件利用抗量子密码技术确保即使在量子计算环境下,密钥交换也是安全的。数

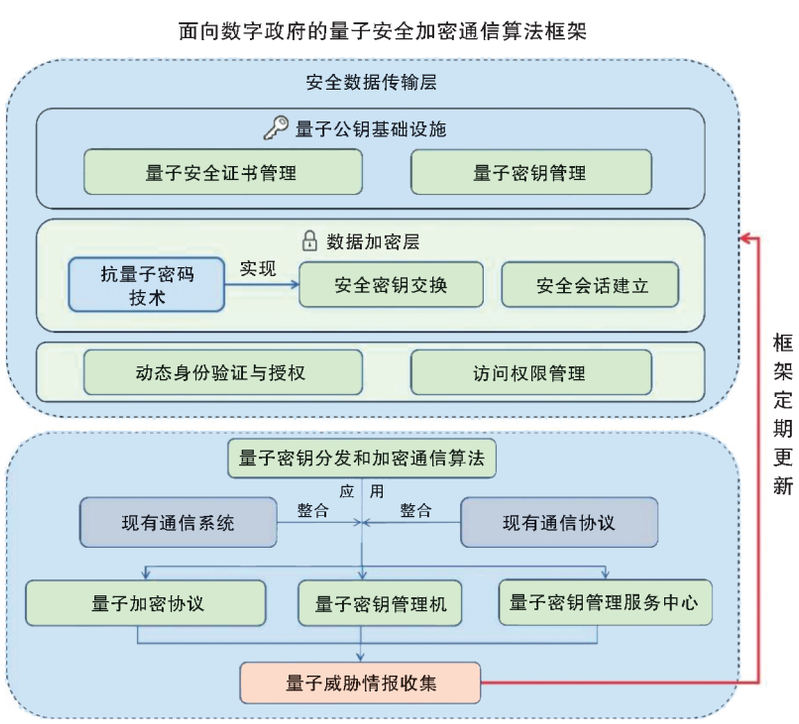

图1 面向数字政府的量子安全加密通信算法框架

Fig. 1 A quantum secure cryptographic communication algorithmic framework for digital government

据传输安全层组件提供了一个加密层,确保所有在数字政府中传输的数据都得到了适当的保护。这意味着无论数据是怎样的或传输给谁,都有一个统一和安全的标准来处理。动态身份验证与授权鉴于数字政府的通信参与者是动态变化的,这一组件确保了所有的参与者都被正确地验证和授权。此外,它还提供了一种机制来管理和撤销访问权限,确保只有合适的实体可以访问数据。考虑到性能和安全性需求,算法选择与优化框架应能支持量子密码算法组件,并根据实际需要进行选择和优化。

2.3 量子密钥分发和加密通信算法

核心组件要求集成量子密码算法到标准的通信协议和应用中,如传输层安全(Transport Layer Security, TLS)/安全套接字层(Secure Sockets Layer, SSL)、虚拟专用网络(Virtual Private Network, VPN)和其他政府专用通信系统。本文设计了一种新的算法评估准则,综合考虑安全性S衡量算法抵抗量子和传统攻击的能力,效率E算法执行的速度和所需的资源,兼容性C算法是否能与现有系统和技术平滑地集成,综合评分函数为

$$F(a)=w_1\times S(a)+w_2\times E(a)+w_3C(a),\quad(1)$$

其中$F(a)$是算法a的总评分,w_1,w_2和w_3是权重因子,其值反映了各准则在决策中的重要性。根据以上评估准则设计一个概念性的量子加密协议(Quantum Enhanced Secure Communication Protocol, QESCP)。这个协议包括量子密钥分发、量子加密通信以及错误检测和纠正隐私放大。

量子密钥分发阶段使用BB84协议来分发密钥,A随机选择一个二进制字符串和一个对应的基集来发送量子比特。B随机选择基来测量接收到的量子比特。通过公共信道比较基,并保留匹配基的比特作为原始密钥。

准备和发送量子比特,A随机生成两个长度为n的字符串:$a\in\{0,1\}^n$(比特字符串),$b\in\{0,1\}^n$(基字符串)。对于每个i,A准备量子比特$|q_i\rangle$,按照下列规则:如果$b_i=0$并且$a_i=0$,发送$|0\rangle$;如果$b_i=0$并且$a_i=1$,发送$|1\rangle$;如果$b_i=1$并且$a_i=0$,发送$(|0\rangle+|1\rangle)/2=|+\rangle$;如果$b_i=1$并且$a_i=1$,发送$(|0\rangle-|1\rangle)/2=|-\rangle$。

产生纠缠对,A使用一个量子纠缠源生成一对纠缠的量子比特(qubit)。通过下面的Bell态来实现:

$$|\Psi^-\rangle=\frac{1}{\sqrt{2}}(|0_A1_B\rangle-|1_A0_B\rangle),\quad(2)$$

其中A和B分别代表A和B的qubit。

执行量子门操作,A对它的qubit执行一系列的量子门操作(例如Hadamard门和X门)来改变其状态。设H是Hadamard门,X是X门,则操作可以表示为:

$$H(|\Psi^-\rangle)=\frac{1}{\sqrt{2}}(|0_A\rangle H|1_B\rangle-|1_A\rangle H|0_B\rangle),\quad(3)$$

$$X(|\Psi^-\rangle)=\frac{1}{\sqrt{2}}(|X|0_A\rangle|1_B\rangle-X|1_A\rangle|0_B\rangle)。\quad(4)$$

接收和测量量子比特,B随机生成一个长度为n的字符串$c\in\{0,1\}^n$作为基字符串。对于每个i,B使用基c_i来测量量子比特$|q_i\rangle$,得到结果r_i。

基的比较和密钥提取,A和B通过经典公开信道比较它们的基字符串b和c。对于每个i,如果$b_i=c_i$,则保留$a_i(A)$和$r_i(B)$作为原始密钥的一部分。

$$K_{\text{raw}}=\{a_i|b_i=c_i\}(A),\{r_i|b_i=c_i\}(B)。\quad(5)$$

这个过程保证了即使量子通道受到监听,由于不确定性原理,窃听者也不能准确得知密钥信息,从而确保了密钥的安全性。

量子加密通信阶段,使用Cascade协议来检测和纠正错误:划分子块假设A和B的原始密钥分别为$K_{A,\text{raw}}$和$K_{B,\text{raw}}$,它们首先将这两个密钥分成m个子块,每个子块包含k个比特。

$$K_{A,\text{raw}}=(A_1,A_2,\cdots,A_m),\quad(6)$$

$$K_{B,\text{raw}}=(B_1,B_2,\cdots,B_m),\quad(7)$$

其中$A_i,B_i\in\{0,1\}^k$。

计算并比较奇偶校验,A和B分别计算每个子块的奇偶校验比特:

$$P_{A,i}=\bigoplus_{j=1}^{k}A_{ij},\quad(8)$$

$$P_{B,i}=\bigoplus_{j=1}^{k}B_{ij},\quad(9)$$

其中$\oplus$是异或操作,A_{ij}和B_{ij}是子块A_i和B_i的第j个比特。A和B通过公开信道比较奇偶校验比特$P_{A,i}$和$P_{B,i}$。

错误定位与纠正,如果$P_{A,i}=P_{B,i}$,子块i被

认为是正确的。如果$P_{A,i}\neq P_{B,i}$,则执行以下操作:A和B进一步将子块A_i和B_i分成更小的子块并重复步骤2,直到找到错误的比特位置。一旦找到错误的比特,B翻转相应的比特来纠正错误。

合并纠正后的密钥,合并所有经过纠正的子块以获得最终的密钥:

$$K_A=A_1\|A_2\|\cdots\|A_m, \tag{10}$$

$$K_B=B_1\|B_2\|\cdots\|B_m, \tag{11}$$

其中‖表示连接操作。使用通用哈希函数来进行隐私放大,A和B选择一个通用哈希函数h。使用h来从纠正后的密钥中派生出最终的密钥。$K=h(K')$,这里K'是纠正后的密钥,K是最终的密钥。

3 仿真及分析

3.1 仿真设置

为了模拟真实的量子传输,使用高级量子模拟器QuTiP,这是一个在量子信息领域广泛使用的工具,能够精确模拟量子状态、操作和测量的演化。计算设备主要配置为:Intel Core i7-9700K(3.60 GHz)CPU,32 GB内存和2 TB固态硬盘,符合计算密集型的量子模拟的资源要求。模拟一个有噪声的量子信道,误码率设置为0.02,即每100个量子比特中有2个受到噪声的影响。噪声类型包括位翻转和相位翻转。密钥长度选择256比特,512比特和1 024比特三种长度,以测试在不同长度下算法的性能。传输次数每种长度的密钥分别传输100次,以获得可靠的统计数据。

3.2 比较方法

为验证本文提出的量子密钥分发和加密通信算法QESCP的有效性,比较了以下3个经典加密算法:

(1)RSA加密算法[21]。RSA算法是一种非对称加密算法,由Ron Rivest, Adi Shamir和Leonard Adleman提出,公钥和私钥是一对互补的密钥,公钥用于加密信息,而私钥用于解密信息。

(2)ECC加密算法[22]。ECC算法是一种应用椭圆曲线数学理论建立的公钥密码体制。它被广泛应用于现代密码学和信息安全领域。与传统的RSA算法相比,ECC提供了更高的安全级别和更高效的性能。

(3)LBC算法[23]。Lattice-Based Cryptography(格基密码学)是一种加密算法范式,它是基于格问题的困难性构建的,是量子抗性密码学的一个重要分支。

3.3 量子密钥分发和加密通信仿真结果

本文比较了RSA、ECC、LBC和QESCP算法在模拟的噪声环境下的通信效率,结果如表1所示。QESCP量子密钥分发中,发送端生成一个256位的随机二进制序列作为原始密钥,并使用BB84协议通过量子信道发送对应的量子比特。接收端接收并测量这些量子比特,然后与发送端通过经典信道进行信息交换,以便正确地重构出原始密钥。仿真结果表明,在模拟的噪声环境下,量子密钥分发依然能够以高成功率进行,表明绝大多数情况下接收端能够成功地重构出与发送端相同的密钥。本文提出的方法QESCP相比较RSA、ECC和LBC算法通信效率较基准方法分别提高了12.2%,7.1%和5.5%。RSA算法在密钥生成和加密过程中相对效率较低,ECC和LBC算法在密钥生成和加密过程中效率更高。QESCP在保持高安全性的同时,展现出最优的效率。仿真结果显示,尽管模拟的量子信道中存在一定的误码率,但BB84协议依然能够在大多数情况下成功地进行密钥分发。

表1 RSA、ECC、LBC和QESCP算法在模拟的噪声环境下的通信效率结果

Table 1 Communication efficiency results of RSA, ECC, LBC and QESCP algorithms in a simulated noisy environment

不同方法	RSA	ECC	LBC	QESCP
通信效率	80.3%	85.4%	87.0%	**92.5%**

本文利用奇偶校验和Shor代码相结合的方法进行错误纠正,不同纠错轮数下分发准确率变化图如图2所示,不同纠错轮数由1增加到8时分发准确率由89.1%提高到92.5%。由此可见,通过应用量子纠错代码,大多数的量子比特错误得以成功纠正,显示了高效和稳定的错误检测与纠正能力。仿真结果表明,即使在面临人为错误和信道噪声的情况下,系统也能够保持较高的密钥分发正确性。虽然还存在小部

分无法纠正的错误,但通过进一步优化错误纠正代码和增加纠错轮数,有望进一步提高错误纠正的成功率。在实际应用中,选择合适的纠错轮数是一个平衡效率和准确性的过程。纠错过程会消耗额外的时间和资源,因此增加纠错轮数可能会降低通信的整体效率。在对通信效率有较高要求的应用中,可能需要在保持一定准确率的同时,尽量减少纠错轮数。纠错过程通常需要额外的计算资源和存储资源。如果应用场景对数据传输的实时性有严格要求,过多的纠错轮数可能会导致不可接受的延迟。在这种情况下,需要在保证实时性和准确性之间找到平衡点。综上所述,实际应用中选择合适的纠错轮数需要综合考虑通信效率需求、实时性要求和系统资源限制等因素。

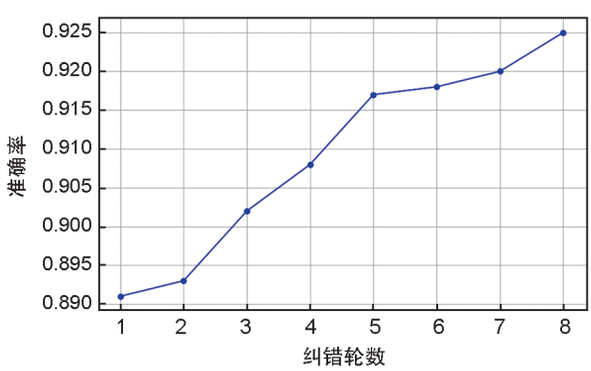

图2 不同纠错轮数下分发准确率变化图

Fig. 2 Plot of distribution accuracy variation with different number of error correction rounds

4 结论

随着量子计算技术的不断发展,量子威胁的规模和复杂性也将进一步增加。通过分析量子计算的威胁和量子安全加密通信的特点,本文提出了一个综合的量子密钥分发和错误检测与纠正方案。仿真结果显示,该方案能够有效地对抗量子计算的威胁,实现高效、稳定和安全的密钥分发,错误检测和纠正机制也表现出良好的性能和可靠性。总的来说,本文的未来工作将致力于进一步提升量子安全加密通信算法的性能和安全性,以满足数字政府建设中不断增长的安全通信需求。未来可以探索和研究更为高效和安全的量子密钥分发协议,以实现更快速和更可靠的密钥分发。还可以研究量子通信安全的多层防护机制和策略,以便从多个层面保障量子通信的安全性。

参考文献:

[1] 赵放, 刘雨佳. 中国数字经济的联系强度、空间结构与发展策略[J]. 山西大学学报(哲学社会科学版), 2021, **44**(4): 99−108. DOI: 10.13451/j. cnki. shanxi. univ(phil. soc.).2021.04.014.
ZHAO F, LIU Y J. The Connection Strength, Spatial Structure and Development Strategy of China's Digital Economy[J]. *J Shanxi Univ Philos Soc Sci Ed*, 2021, **44**(4): 99−108. DOI: 10.13451/j. cnki. shanxi. univ(phil. soc.).2021.04.014.

[2] PANAGIOTOPOULOS P, KLIEVINK B, CORDELLA A. Public Value Creation in Digital Government[J]. *Gov Inf Q*, 2019, **36**(4): 101421. DOI: 10.1016/j. giq.2019.101421.

[3] JANSSEN M, RANA N P, SLADE E L, *et al*. Trustworthiness of Digital Government Services: Deriving a Comprehensive Theory Through Interpretive Structural Modelling[J]. *Public Manag Rev*, 2018, **20**(5): 647−671.

[4] 高飞, 郭奋卓, 温巧燕, 等. 重新审视量子对话和双向量子安全直接通信的安全性[J]. 中国科学(G辑:物理学力学 天文学), 2008, **38**(5): 477−484.
GAO F, GUO F Z, WEN Q Y, *et al*. Re-examine the Security of Quantum Dialogue and Two-way Quantum Secure Direct Communication[J]. *Sci China Ser G Phys Mech Astron*, 2008, **38**(5): 477−484.

[5] 匡畅, 郑晓毅. 基于类GHZ态的受控量子安全直接通信[J]. 量子电子学报, 2019, **36**(6): 714−718. DOI: 10.3969/j.issn.1007-5461.2019.06.012.
KUANG C, ZHENG X Y. Controlled Quantum Secure Direct Communication Based on GHZ-like State[J]. *Chin J Quantum Electron*, 2019, **36**(6): 714−718. DOI: 10.3969/j.issn.1007-5461.2019.06.012.

[6] 周贤韬, 江英华, 郭晨飞, 等. 基于GHZ态粒子和单光子混合的量子安全直接通信协议[J]. 量子电子学报, 2022, **39**(5): 768−775. DOI: 10.3969/j. issn. 1007-5461.2022.05.010.
ZHOU X T, JIANG Y H, GUO C F, *et al*. Quantum Secure Direct Communication Protocol Based on Mixture of GHZ Particles and Single Photon[J]. *Chin J Quantum Electron*, 2022, **39**(5): 768−775. DOI: 10.3969/j.issn.1007-5461.2022.05.010.

[7] KUANG R, BARBEAU M. Quantum Permutation Pad for Universal Quantum-safe Cryptography[J]. *Quantum Inf Process*, 2022, **21**(6): 211. DOI: 10.1007/s11128-022-03557-y.

[8] SLIWA J, WRONA K, SHABANSKA T, *et al*. Lightweight Quantum-safe Cryptography in Underwater Scenarios[C]//2023 IEEE 48th Conference on Local Computer Networks (LCN). Florida: IEEE, 2023: 1−6. DOI: 10.1109/LCN58197.2023.10223321.

[9] SHOP P W. Algorithms for Quantum Computation: Discrete Logarithms and Factoring[C]//Proceedings 35th Annual Symposium on Foundations of Computer Science. Santa Fe: IEEE, 1994: 124−134. DOI: 10.1109/SFCS.1994.365700.

[10] 李婷, 常利伟. 一种可外包解密的高效密文策略的属性基加密方案[J]. 山西大学学报(自然科学版), 2022, **45**(2): 387−392. DOI: 10.13451/j.sxu.ns.2020164.
LI T, CHANG L W. An Efficient Ciphertext-policy Attribute-based Encryption Scheme with Outsourcing Decryption[J]. *J Shanxi Univ Nat Sci Ed*, 2022, **45**(2): 387−392. DOI: 10.13451/j.sxu.ns.2020164.

[11] 郭丽峰, 王倩丽. 云存储中可验证的完全外包的属性基加密[J]. 山西大学学报(自然科学版), 2021, **44**(2): 262−268. DOI: 10.13451/j.sxu.ns.2020102.
GUO L F, WANG Q L. Verifiable Fully Outsourcing Attribute-based Encryption in Cloud Storage[J]. *J Shanxi Univ Nat Sci Ed*, 2021, **44**(2): 262−268. DOI: 10.13451/j.sxu.ns.2020102.

[12] YI H B. A Post−quantum Secure Communication System for Cloud Manufacturing Safety[J]. *J Intell Manuf*, 2021, **32**(3): 679−688. DOI: 10.1007/s10845−020−01682−y.

[13] KUANG R, PEREPECHAENKO M. Quantum Encryption with Quantum Permutation Pad in IBMQ Systems[J]. *EPJ Quantum Technol*, 2022, **9**(1): 26. DOI: 10.1140/epjqt/s40507−022−00145−y.

[14] 靳文京, 郑学欣, 孟玉飞. 基于不同密码算法的MAVSec安全协议性能研究[J]. 信息安全研究, 2023, **9**(8): 771−776. DOI: 10.12379/j.issn.2096-1057.2023.08.08.
JIN W J, ZHENG X X, MENG Y F. Research on Performance of MAVSec Security Protocol Based on Different Cryptographic Algorithms[J]. *J Inf Secur Res*, 2023, **9**(8): 771−776. DOI: 10.12379/j. issn. 2096-1057.2023.08.08.

[15] 奚宇航, 黄一平, 苏检德, 等. 基于国密算法的即时通信加密软件系统的设计与实现[J]. 计算机应用与软件, 2020, **37**(6): 303−308. DOI: 10.3969/j. issn. 1000-386x.2020.06.052.
XI Y H, HUANG Y P, SU J D, *et al*. Design and Implementation of Instant Messaging Encryption \rsoftware System Based on National Secret Algorithm [J]. *Comput Appl Softw*, 2020, **37**(6): 303−308. DOI: 10.3969/j.issn.1000-386x.2020.06.052.

[16] HEINZ D, PÖPPELMANN T. Combined Fault and DPA Protection for Lattice-based Cryptography[J]. *IEEE Trans Comput*, 2023, **72**(4): 1055−1066. DOI: 10.1109/TC.2022.3197073.

[17] SAJIMON P C, JAIN K, KRISHNAN P. Analysis of Post-quantum Cryptography for Internet of Things[C]//2022 6th International Conference on Intelligent Computing and Control Systems (ICICCS). Madurai: IEEE, 2022: 387−394. DOI: 10.1109/ICICCS53718.2022.9787987.

[18] ZHOU L, SHENG Y B, LONG G L. Device-Agnostic Quantum Secure Direct Communication Resilient Against Joint Attacks[J]. Sci Bull, 2020, 65(1): 12-20. DOI: 10.1016/j.scib.2019.10.025.

[19] 李西明, 吴嘉润, 吴少乾, 等. 基于生成对抗网络的抗泄露加密算法研究[J]. 计算机工程与应用, 2020, 56(10): 69−74. DOI: 10.3778/j.issn.1002−8331.1902−0062.
LI X M, WU J R, WU S Q, et al. Key Resilient Encryption Algorithm Based on Generative Adversarial Networks[J]. Comput Eng Appl, 2020, 56(10): 69−74. DOI: 10.3778/j.issn.1002−8331.1902−0062.

[20] LOHACHAB A, LOHACHAB A, JANGRA A. A Comprehensive Survey of Prominent Cryptographic Aspects for Securing Communication in Post-quantum IoT Networks[J]. *IoT*, 2020, **9**: 100174. DOI: 10.1016/j.iot.2020.100174.

[21] MOHAMMED S J, TAHA D B. Performance Evaluation of RSA, ElGamal, and Paillier Partial Homomorphic Encryption Algorithms[C]//2022 International Conference on Computer Science and Software Engineering (CSASE). Madurai: IEEE, 2022: 89−94. DOI: 10.1109/CSASE51777.2022.9759825.

[22] WANG J, LIU Y, RAO S Y, *et al*. Enhancing Security by Using GIFT and ECC Encryption Method in Multi-tenant Datacenters[J]. *Comput Mater Continua*, 2023, **75**(2): 3849−3865. DOI: 10.32604/cmc.2023.037150.

[23] D'ANVERS J P, VAN BEIRENDONCK M, VERBAUWHEDE I. Revisiting Higher-order Masked Comparison for Lattice-based Cryptography: Algorithms and Bit-sliced Implementations[J]. *IEEE Trans Comput*, 2023, **72**(2): 321−332. DOI: 10.1109/TC.2022.3197074.