 DOI: https://doi.org/10.12349/iser.v5i11.3626

Research on Cryptographic Algorithms Based on Quantum Computing

Xiaofei Yin

Jiangsu Fuergan Technology Co., Ltd., Nanjing, Jiangsu, 210026, China

Abstract

In order to counter the quantum computing attacks that traditional cryptography algorithms may face, this paper studies cryptography algorithms based on quantum computing. Firstly, the basic principles and main characteristics of quantum algorithms are introduced in detail, and the threats that quantum computers may cause to existing cryptosystems in the future are analyzed. Secondly, a new cryptography algorithm based on quantum computing is designed and its effectiveness in improving information security is empirically studied. It is found that the new algorithm has great advantages in reducing the computational complexity and improving the difficulty of cryptography decryption, which is of great significance for improving the ability of cryptosystem to resist quantum attacks. The research in this paper provides a new theoretical support for the future research and development of cryptography in the quantum environment.

Keywords

quantum computing; cryptographic algorithm; quantum attack; information security; password system

基于量子计算的密码学算法研究

殷晓飞

江苏富而乾科技有限公司，中国 · 江苏 南京 210026

摘　要

为了对抗传统密码算法可能面临的量子计算攻击，论文进行了基于量子计算的密码学算法研究。首先，详细介绍了量子算法的基本原理和主要特征，并针对未来量子计算机可能对现有密码系统造成的威胁进行了分析；其次，设计了一种新型的基于量子计算的密码学算法，并对其在提高信息安全性方面的有效性进行了实证研究。研究发现，新算法在减小计算复杂度，提高密码解密难度方面展现出了较大优势，对于提高密码系统抵抗量子攻击的能力具有重要意义。论文的研究为未来密码学在量子环境下的研究发展提供了新的理论支持。

关键词

量子计算；密码学算法；量子攻击；信息安全性；密码系统

1 引言

量子计算机的出现和发展可能会破解我们现有的密码系统，像 RSA 和 ElGamal 等密码算法可能会被破解，这让我们面临信息安全的风险。所以，我们需要研究和创建新的基于量子计算的密码方法，来提高信息的安全性。本研究就是要先了解量子计算是怎么运作的，并探索它会给密码系统带来什么威胁。然后，我们还会设计一个新的基于量子计算的密码方法，来保护信息安全。这项研究的目标是希望在密码学和量子计算的领域里，填补我们现在还不了解的部分，并提供一些理论支持，帮助未来在量子环境下的密码学研究和应用得到发展。

【作者简介】殷晓飞（1972–），男，中国安徽芜湖人，硕士，工程师，从事计算机研究。

2 量子算法基本原理及其特性

2.1 量子算法的基本原理

量子算法基于量子力学的基本原理，主要包括叠加性、纠缠性和量子干涉等特性 [1]。通过这些特性，量子算法实现了传统计算无法企及的计算能力。量子力学的叠加原理允许量子比特（qubits）存在于多个状态，这与传统二进制系统中比特只能处于 0 或 1 的一种状态形成了鲜明对比。借助叠加性，量子计算能够并行处理大量信息，提高计算速度。

纠缠性是量子算法的另一核心特性。两个或多个量子比特通过纠缠现象，可以在空间上分离的情况下依然保持关联。当对一个量子比特实施测量时，纠缠比特的状态也会立即确定。这一性质在量子通信和量子密钥分发中展现出巨大的应用潜力，为实现安全的量子密码系统奠定了理论基础。

量子干涉原理则通过对量子态进行干涉来增强特定计算路径，使得无效路径相互抵消，最终提高计算结果的概率。

这一特性是诸如 Shor 算法和 Grover 算法得以高效执行的关键因素。Shor 算法在整数分解问题上，展示了远超传统算法的速度优势，对现有公钥密码体制构成潜在威胁。Grover 算法则通过提高无序数据库搜索的效率，降低了对称密钥密码体制的安全性 [2]。

2.2 量子算法的主要特性

量子算法的主要特性主要体现在其计算能力、并行处理和概率性等方面。量子算法利用量子力学的叠加性和纠缠性，使其能够处理多个计算路径，这显著提高了计算速度。例如，量子叠加允许量子比特在计算中存在于多个状态，这使得搜索和优化等问题能够在指定时间内完成。与经典算法相比，量子算法能够更高效地处理某些特定问题。

量子纠缠是另一特性，它增强了信息的传输和处理能力。纠缠使得多个量子比特之间存在非局域的联系，在进行量子计算时，量子比特之间相互影响，从而提升了算法的整体性能。量子算法的概率性表现在其计算结果是根据概率分布得出的，而不是确定性的，这就决定了量子算法的输出需要多次测量才能达到较高的置信水平。

这些特性在一定程度上赋予了量子算法在解决特定问题上的潜在优势，但也对算法设计和实现提出了更高要求。掌握和利用这些特性，将为开展更复杂的计算任务提供丰富的可能性。

2.3 量子计算机和传统计算机的对比

量子计算机与传统计算机在计算原理和信息处理能力上具有显著差异。传统计算机基于二进制系统，使用比特作为信息的最小单位，每个比特以 0 或 1 表示，从而进行串行处理。而量子计算机采用量子比特，其可以以 0 和 1 的叠加态存在，利用量子纠缠和量子叠加原理进行并行计算，这使得量子计算机在处理海量并行任务时展现出超越传统计算机的潜力。量子门的操作可以在较少步骤中完成复杂运算，提升计算速度。量子计算的这些特性使其在处理某些特定问题上具备显著的优势，对密码学中的因式分解和离散对数等问题表现尤为突出，这对现有的加密技术构成挑战。

3 量子计算对现有密码系统的威胁分析

3.1 量子计算的安全威胁

量子计算机作为新一代计算技术，其潜力强大的计算能力对现有密码系统构成重要安全威胁。量子计算能够通过许多传统计算机难以企及的方法进行复杂计算，其中最突出的是利用 Shor 算法对公钥密码系统的攻击能力。Shor 算法能够在多项式时间内分解大整数和计算离散对数，这一特性使得基于这些数学难题构建的密码系统（如 RSA 和 ECC）在量子计算机面前变得不再安全。这种攻击能力直接威胁到当前广泛使用的公共基础设施的安全性。

量子计算的另一种威胁表现在 Grover 算法对对称密码学的影响。Grover 算法可以将穷举搜索的时间复杂度从传统的 $O(2^n)$ 降低到 $O(2^{n/2})$，这意味着对于使用 n 位密钥长度的对称加密算法，在量子计算机上仅需约 $2^{n/2}$ 次运算即可破解。这对依赖密钥长度作为安全性度量的对称加密系统提出了更高的密钥长度要求。

量子计算不仅挑战了当前密码算法的基础，还促使对量子环境下信息安全的重新评估。这种威胁引发了对新型密码学算法的研究，以探索在量子计算背景下如何构建更为安全的系统。量子抗性密码学的出现，正是为了应对此类威胁，这一领域的研究正在为确保未来信息安全提供新的路径与方向。当前密码学界对量子计算威胁的关注，反映了在这一转折点上对密码安全的重新思考与布局。

3.2 传统密码学和量子密码学的对比

传统密码学与量子密码学在多个方面存在显著差异，主要体现在其抵御攻击能力和算法基础上。传统密码学依赖经典计算理论，其安全性通常基于数学难题的复杂性，如整数分解和离散对数问题。量子计算机能够通过量子算法，例如 Shor 算法，高效解决这些数学难题，直接威胁传统密码系统的安全性。

量子密码学则以量子物理原理为基础，特别是量子态表达和测量的不可克隆性，为信息的安全传输提供了全新的保障机制。量子密钥分发协议（如 BB84 协议）利用量子叠加性和测量坍缩性，实现了无条件安全的密钥交换。这种安全性并不依赖于计算复杂性，而是基于量子物理定律，从而在理论上抵御量子计算攻击 [3]。

在应用前景上，传统密码学由于其成熟度和计算效率，目前仍是主流。随着量子技术的发展，量子密码学被认为是前景广阔的基础科学领域。其发展不仅能提升安全保障能力，还可能引发整个密码学领域的革新。量子密码学有望在为传统密码学带来挑战为信息安全提供更坚实的保障和更广阔的发展空间。

3.3 对量子计算可能对现有密码系统威胁的深入分析

量子计算的快速发展对于现有的密码系统构成了重大威胁，尤其是经典加密算法在面对强大的量子计算机时可能失去其安全性。Shor 算法能够在多项式时间内对大整数进行分解，这直接影响了依赖大数分解难题的 RSA 加密算法的安全性。Grover 算法可以将对称加密算法的搜索空间从指数级缩小为平方级，使得使用量子计算机进行暴力破解成为现实威胁。量子计算所具备的并行计算能力和指数级速度提升，使得大多数传统密码在量子的背景下失去安全保证，提出了重新设计密码体系的迫切要求。

4 基于量子计算的密码学算法设计及有效性验证

4.1 基于量子计算的密码学算法设计

设计基于量子计算的密码学算法，须考虑量子计算的

独特性质，如叠加性和纠缠特性。在此基础上，一个有效的量子密码算法需运用这些特性，以确保在量子计算环境下的安全性。

该算法的设计框架从基本的量子电路模型出发，结合量子位（qubit）的操作。量子的比特不仅可以处在 0 和 1 的状态，还可以处在 0 和 1 的叠加状态，这为密码算法的设计提供了新的可能。采取的策略之一是利用 Shor 算法和 Grover 算法优化量子密钥分发机制。通过量子态的变化来加密信息，借助 Bell 态之类的量子纠缠态，可以保证信息在传输过程中的不可破解性。

量子态的叠加性可用于生成复杂的多态密钥，使得即使是量子计算机进行暴力破解攻击，所需的计算复杂度也会大幅增加。此类设计注重量子算法的可实现性，确保在现有或未来可预见的量子计算能力下，该密码学算法能提供足够的安全保障。

该设计需对抗现有破密手段，尤其是针对传统 RSA 和 ECC 算法的局限，通过量子抵抗特性设计更为复杂和难以预测的加密机制。还需考虑量子容错编码的实现，以最大化减少量子噪声对算法带来的影响，提高加密的鲁棒性和可靠性。通过设计这样的算法，可以更好地抵御量子计算带来的潜在威胁，为信息的安全保护建立坚固的防线。

4.2 提高信息安全性的研究

在量子计算环境下，提高信息安全性成为密码学研究的核心目标之一。研究表明，量子计算的巨大算力对现有加密方案构成严重威胁，开发具备抗量子攻击能力的加密算法至关重要。新型密码学算法通过量子计算特有的并行处理能力，实现了数据快速加密和解密，显著增加了密钥空间的复杂性，从而提高了破解难度。对算法的安全性进行评估时，使用量子信息论方法，确保其在理论上可以抵御当前已知的量子攻击方式。实验结果显示，新算法在数据加密过程中采用了随机量子态的生成与操作，增加了攻击者对密文进行分析和预测的困难，从而提升了信息的安全性。这不仅有效降低了量子计算可能带来的解密风险，还提升了整体密码系统的稳健性，为网络通讯及数据存储提供了更高级别的保护。通过结合量子计算和密码学理论，新设计的算法在信息安全性研究中显示出极强的适应性和长远价值，推动了密码学在新时代的进步和应用。

4.3 对新算法在提高密码解密难度和降低计算复杂度方面的评估

在评估新型基于量子计算的密码学算法时，重点在于其在增加密码解密难度和降低计算复杂度方面的表现。该算法通过利用量子叠加和纠缠性质，显著提高了潜在攻击者恢复密钥的难度。与经典算法相比，量子算法的复杂性增加，使得试图通过暴力破解的手段变得更加不可行。新算法体现出更低的计算复杂度，这主要归因于量子计算并行处理的能力，使得在空间内可处理的信息量大幅增加。量子计算的这种特性显著降低了加密和解密过程中所需的资源投入，并使实时信息处理成为可能。新算法在对抗量子计算威胁的，保证了较高的计算效率，为密码系统的安全性提供了强有力的支持。该评估结果表明，新算法不仅在安全性上具有优越性，而且在效率上也实现了突破性进展。

5 结语

论文以应对量子计算带来的挑战和威胁为出发点，对基于量子计算的密码学算法进行了一系列研究。研究首先系统阐述了量子算法的基本原理、主要特征，并对量子计算可能对密钥系统带来的威胁进行了详尽而深入的剖析。其次，论文设计并实证检验了一种新型的量子计算密码学算法，该算法在降低计算复杂度、提高密码解密难度等方面显示出了明显优越性，对保障信息安全以及对抗量子攻击能力的提升都起到了积极的推动作用。然而，需要注意的是，尽管这项研究取得了一些初步的成果，但量子计算密码学还处于起步阶段，许多理论和技术还需要进一步的研究和探索。特别是如何利用量子计算的特性更好地设计和优化密码系统，以及如何将其有效地应用在实际工作中，都是未来研究的重要课题。这项研究为密码学在量子计算环境下的理论研究和实践应用提供了新的启示和思路，对于密码学、信息安全以及量子计算的后续研究与探索具有重要的价值和指导意义。

参考文献

[1] 巫光福,江林伟.抗量子密码学综述[J].长江信息通信,2021,34(7):55-60.

[2] 阿德里安·丘.密码学家找到了免遭量子攻击的算法[J].世界科学,2019(10):12-13.

[3] S.皮兰多拉,U.L.安德森,L.班基.量子密码学进展[J].信息安全与通信保密,2020,18(11):56-79.