基于量子计算的加密方法及抗量子攻击算法的理论研究

张尚哲
黑龙江大学 黑龙江 150080

摘要:本文探讨了量子计算对现代信息安全技术的影响,特别是对传统加密方法的威胁。量子计算的并行处理能力和 Shor 算 法使得传统加密方法面临被破解的风险。为应对这一挑战,本文介绍了基于量子计算的新型加密方法,包括量子行走(QW) 和基于量子纠缠的加密方案,以及抗量子攻击的加密算法(PQC)。详细讨论了 NTRUEncrypt 和 Lattice-based 加密算法的计算 原理和优缺点,并分析了这些新型加密方法在信息安全中的应用和前景。

关键词:量子计算;量子加密;抗量子攻击算法;信息安全

Theoretical Research on Encryption Methods Based on Quantum Computing and Quantum-Resistant Attack Algorithm

Zhang Shangzhe
Heilongjiang University, Heilongjiang 150080 China

Abstract This paper explores the impact of quantum computing on modern information security technologies, especially the threat to traditional encryption methods. The parallel processing capability of quantum computing and Shor algorithm make traditional encryption methods face the risk of being cracked. To address this challenge, this paper introduces novel cryptographic methods based on quantum computing, including quantum walking (QW) and quantum entanglement based cryptographic schemes, as well as quantum attack-resistant cryptographic algorithms (PQC). The computing principles, advantages and disadvantages of NTRUEncrypt and Lattice-based encryption algorithms are discussed in detail, and the application and prospect of these new encryption methods in information security are analyzed.

keyword quantum computing; Quantum encryption; Anti-quantum attack algorithm; Information security

1 引言

加密技术是现代信息安全的基石，广泛应用于数据传输、存储和通信中。随着计算能力的提升，特别是量子计算的出 现，传统加密方法如 RSA 和 AES 面临着前所未有的破解风 险。量子计算的并行处理能力和 Shor 算法使得这些传统方法 可能在量子计算机面前不堪一击[1]。因此，探索基于量子计算 的新型加密方法成为亟待解决的重要课题。

2 量子计算的基本原理

量子计算利用量子比特 (Qubits) 进行计算。与传统比特不同，量子比特可以同时处于多个状态，这使得量子计算具 有强大的并行处理能力。量子计算的两个重要特性——叠加 和纠缠，使其能够解决许多传统计算无法有效处理的问题。 量子算法如 Shor 算法和 Grover 算法正是基于这些特性，能 够显著提升计算效率，同时也使得量子计算在解决某些特定 问题时表现出极

大的优势。

(1) 叠加原理 量子叠加原理是量子力学的核心概念之一。它描述了量子系统可以同时处于多个状态的特性。这与经典物理学中的 概念完全不同。在经典物理中，一个系统只能处于一种确定 的状态，但在量子力学中，一个量子系统可以同时处于多个 状态的叠加态。量子叠加原理允许量子比特处于多个状态的组合，而不仅仅是 0 或 1 的单一状态。这一特性使得量子计 算机可以同时处理大量数据，从而提高计算效率。例如，一个 n 个量子比特的系统可以同时表示 2^n 个状态。

(2) 纠缠原理

量子纠缠是指两个或多个量子系统在相互作用后，即使 它们相隔很远，依然表现出高度相关的量子态。这种纠缠态 无法用经典物理学来解释。量子纠缠揭示了两个或多个量子 比特之间存在的一种特殊关联，使得其中一个量子比特的状 态变化会立即影响到其他纠缠量子比特的状态，无论它们之 间的距离有多远。这一特性被用来设计高效的量子通信和计 算协议，是量子加密技术的重要基础。

3 基于量子计算的加密方法

量子计算基于量子位的叠加态和纠缠态，能够在并行计 算和非线性问题上表现出强大的计算能力。加密方法利用这 些特性，可以执行在经典计算机上无法实现的复杂计算。在 加密计算方面，量子计算可以在不泄露任何信息的情况下，对加密的量子数据执行任意的量子计算。在图像加密方面，量子计算可以利用量子行走 (Quantum Walks) 的非线性混沌 特性进行图像加密，比传统方法具有更高的安全性 [2]。在密钥 分发方面，量子加密结合了量子算法和传统的对称加密算法，这种优势使其可以实现更高效的密钥分发和管理。

4 基于量子纠缠的加密方法

量子纠缠态可以用于实现更加复杂的加密方案。通过量子纠缠，双方可以共享一个纠缠态对，当一方对其量子比特 进行测量时，另一方的量子比特状态也会相应确定。这种特 性可以用于设计高效的量子加密通信协议，确保通信过程的 安全性和隐私性。在此方面，主要使用 Ekert(E91) 协议。 Ekert 协议由 Artur Ekert 在 1991 年提出，利用量子纠缠和贝 尔不等式来保证密钥分发的安全性。协议中，Alice 和 Bob 共 享一对纠缠态光子，分别对其进行测量。由于纠缠态的特性，测量结果之间存在关联，这种关联被用于生成共享密钥。窃 听者的干预会破坏纠缠态的关联，从而被检测到 [3]。

5 抗量子攻击的加密算法

为了应对量子计算的威胁，研究者们提出了多种抗量子攻击的加密算法 (PQC)。这些算法主要基于数学问题，如格 问题和多变量多项式问题，目前尚未被量子算法有效破解 [4]。NTRUEncrypt 和 Lattice-based 加密方法是其中较为典型的例 子，这些方法利用复杂的数学结构提供高安全性，并且在传统计算机上仍然保持较高的计算效率 [5][6]。

5.1 NTRUEncrypt

NTRUEncrypt 是一种基于格理论的公钥加密算法，其安全性依赖于在格上找到短向量的困难性。NTRUEncrypt 具有计算效率高、密钥生成速度快等优点，且目前尚无有效的量 子算法能够破解这一问题。

NTRUEncrypt 算法依赖于多项式环和卷积的概念。其核心是对多项式进行模多项式的运算，这种结构可以有效地提 供安全性和效率。

多项式环 :NTRUEncrypt 使用一个多项式环 R，其中的 多项式系数取模一个整数 q。

卷积积 : 多项式的卷积用于加密和解密过程。这种运算 提供了一种混淆机制，使得破解密文变得极为困难。

NTRUEncrypt 加密算法的具体流程如下 : (1) 密钥生成

选择两个小多项式 f 和 g，其中 f 应具有逆元 fp 和 fq; 计算 fp * f ≡ 1 mod p 和 fq * f ≡ 1 mod q;

计算公钥 h = fq g mod q;

公钥为 h，私钥为 (f，fp);

(2) 加密算法

选择一个随机的小多项式 r 作为随机化因子 ; 明文消息 m 编码为一个多项式 ;

计算密文 e = r * h + m mod q;

(3) 解密算法

计算 a = f * e mod q;

将 a 的系数限制在 [-q/2，q/2] 范围内，得到 a’ ; 计算明文 m=fp *a’ modp; 下面将通过使用一个简单的参数集来更详细地阐述

LWE 加密算法 :

第一步 : 选择参数 N = 5，q = 32，p = 3; 第二步 : 选择多项式 f=1+x+ x2 - x3，g=1–x- x2+ x4;

第三步 : 计算公钥 h = fq * g mod q;

第四步 : 选择随机多项式 r=1–x+ x2; 第五步 : 编码消息 m = 1 + x;

第六步 : 加密得到 e = r * h + m mod q; 第七步 : 计算 a=f*emodq，然后解密得到 m=fp *amod p;

5.2 Lattice-based

加密算法 基于格理论的加密算法利用格问题的复杂性来提供安全性。常见的格问题包括短整数解问题 (SIS) 和学习带误差问 题 (LWE)。这些问题在量子计算机上仍然难以解决，因此 被认为是抗量子攻击的有效方法。

LWE 加密算法的具体流程如下 :

(1) 密钥生成

选择一个随机矩阵 A ∈ Zn x m; q 选择一个随机向量 s ∈ Zn 作为私钥；q 计算公钥 b= ATs+emodq，其中 e 是一个小误差向量；

(2) 加密算法

第一步：选择参数 q = 257，n = 4，m = 6；

第二步：选择随机矩阵 $A=\begin{pmatrix}3&4&1&5&6&2\\1&3&5&7&2&4\\6&5&4&3&2&1\\7&2&5&4&1&3\end{pmatrix}$；

第三步：选择私钥向量 $s=\begin{pmatrix}1\\2\\3\\4\end{pmatrix}$；

第四步：计算公钥 $b = A^T s + e \bmod q$，其中 e 是小误差向量；

第五步：选择随机向量 $r=\begin{pmatrix}2\\3\\1\\4\\5\\6\end{pmatrix}$；

第六步：编码消息 $m=\begin{pmatrix}1\\0\\1\\0\\1\\0\end{pmatrix}$；

第七步：加密得到 c = Ar + m mod q;

第八步：计算 m' = c – br mod q，然后取模 p 得到明文；

6 量子加密算法的比较与分析

6.1 NTRUEncrypt 加密算法的优缺点

NTRUEncrypt 基于格理论的复杂性，具有抵抗量子计算 攻击的能力。相比传统的公钥加密算法，如 RSA 和 ECC，NTRUEncrypt 在加解密速度方面表现出色，尤其在嵌入式系统和移动设备上更为高效。这主要归功于其独特的数学结构，能够在相对较低的计算资源消耗下完成复杂的加解密操作。

NTRUEncrypt 对量子计算攻击具有显著的抗性。传统加密算法在量子计算机面前可能变得脆弱，但 NTRUEncrypt 由于其基于格的结构，在理论上能够抵御量子计算机的 Shor 算法攻击。这使得 NTRUEncrypt 成为未来抗量子加密的有力候选者之一。此外，NTRUEncrypt 的密钥大小相对较小，在资源受限的环境中（如智能卡和物联网设备等）非常实用，这进一步提升了其应用价值 [7]。

然而，NTRUEncrypt 也存在一些缺点。其数学基础较为复杂，理解和实现起来可能比其他加密算法更具挑战性。这 种复杂性可能导致在实际应用中出现错误，从而影响系统的 安全性。此外，NTRUEncrypt 曾经受到专利保护，这限制了 其在某些应用中的自由使用。尽管一些专利已经过期，但历 史上的专利问题仍可能影响一些开发者的选择。

6.2 Lattice-based 加密算法的优缺点

Lattice-based 加密算法的安全性同样基于格问题的计算复杂性，能够抵御量子计算攻击。尤其是 LWE 相关算法在实际使用中表现其高效性，尤其适合在资源受限的环境中使用，如嵌入式设备和物联网。传统的公钥加密算法，如 RSA 和 ECC，依赖于整数分解和离散对数问题，这些问题可以通过 Shor 算法在量子计算机上有效解决。然而，格问题如最短向 量问题 (SVP) 和误差学习问题 (LWE) 被认为在量子计算机 上也难以解决，这使得 lattice-based 加密算法在未来量子计算 机出现时仍能保持安全 [8]。

此外，Lattice-based 加密算法具有高度的理论安全性。它们的安全性通常基于最坏情况难度假设，这意味着破解这些 加密算法在最坏情况下是极其困难的。这一特性为这些算法 提供了强大的安全保障，并使其在面对未知攻击时更具鲁棒 性。Lattice-based 加密算法具有灵活性和多功能性。它们不仅 可以用于传统的加密和签名，还可以用于更复杂的应用，如 完全同态加密，这种加密允许在密文上执行计算而无需解密，从而在云计算和数据隐私保护中具有重要应用前景 [9]。

然而，Lattice-based 加密算法也面临一些挑战。首先是实现复杂性和效率问题。尽管在理论上这些算法具有高效性，但在实际实现中，尤其是在硬件和嵌入式系统中，实现高效 且安全的格基加密仍然是一个技术难题。需要仔细优化算法 和硬件架构以平衡安全性和性能。此外，Lattice-based 算法的 密钥和密文的大小也是一个重要问题。与传统的公钥加密算 法相比，Lattice-based 算法往往需要更大的密钥和密文存储空 间，这在资源受限的环境中可能成为一个瓶颈。

6.3 基于量子行走的加密技术的优缺点

基于量子行走的加密技术具有显著的优缺点。在安全性 方面，量子行走加密技术利用量子力学的基本原理，如测不 准原理和不可克隆定理，使其在对抗潜在攻击方面具有天然 优势。研究表明，量子行走可以生成更难以破解的加密密钥，从而增强安全性。此外，传统的加密方法在大型量子计算机 面前将不堪一击，而基于量子行走的加密方法能抵御量子计 算机的攻击，为未来提供安全保障。量子行走还能提高量子 密钥分发的效率，优化密钥生成过程，使其更加快速且安全。 量子行走的非线性特性使其在生成加密密钥和设计加密算法 方面非常强大，有助于构建更复杂和安全的加密协议。

然而，这种技术在实际应用中也存在一些显著的缺点。 首先，量子行走加密技术的实现复杂度较高，需要先进的量 子计

算硬件和技术支持，这对当前的技术水平提出了很高的 要求。此外，要实现量子行走加密，需要高质量的量子通信网 络和相关基础设施，这对广泛应用仍具有挑战性。量子行走 算法的复杂性可能导致实际计算中的资源消耗大，尤其是在 大规模应用中，可能需要大量的计算资源和时间。

6.4 Ekert(E91) 协议的优缺点

E91 协议的一个显著优点是其利用了纠缠态的特性，这意味着 Alice 和 Bob 可以通过测量纠缠态粒子来生成共享的 密钥，而不必直接传输密钥本身。这种方法使得窃听者 Eve 无法在不被发现的情况下截获和复制量子态，因为任何对量子 态的观察都会不可避免地引入扰动并改变其状态，从而暴露 窃听行为。通过测量 Bell 不等式，Alice 和 Bob 可以检测到 任何试图窃听的行为，如果 Bell 不等式被破坏，则说明存在 窃听者，密钥的安全性得到了保证。

但是，E91 协议的实现也面临一些技术挑战。生成和维持纠缠态在现实中是复杂的，尤其是在存在噪声和衰减的通信 信道中。已有研究表明，去极化噪声和广义幅度阻尼是主要 的影响因素，去极化噪声比广义幅度阻尼更容易解纠缠，这 表明 E91 协议对广义幅度阻尼更为鲁棒。

E91 协议在噪声环境下的安全性分析也非常重要。已有 研究表明，在集体旋转噪声环境中，E91 协议可以有效检测到 窃听行为，尽管噪声水平接近 0.5 时，窃听者可能获取约 50% 的密钥，但总体上协议仍然保持安全 [10]。除此之外 E91 协议 具有自检能力。研究者提出了一种公平采样测试方案，旨在 检测使用偏差样本来模拟 Bell 不等式表观违反的窃听企图。 该测试是本地和非破坏性的，可以在密钥生成过程中随时由 Alice 或 Bob 单独执行。

7 结束语

量子计算的快速发展对传统加密技术提出了严峻挑战，但也为新型加密方法的发展提供了契机。本文探讨了量子计 算对传统加密方法的影响，并分析了几种基于量子计算的新 型加密方法。尽管量子加密技术尚处于发展初期，但其无条 件安全性和抗量子攻击能力为未来的信息安全提供了新的方 向。随着量子计算技术的不断进步，量子加密技术有望在未 来的数字时代中发挥至关重要的作用。

参考文献：

[1] 刘安航，李浩昱，关佳，等 . 基于量子计算原理的 Shor 算法优越性验证 [J]. 物理实验，2022，42(04):7−12.
[2] 刘升，张雄，赵春柳 . 基于量子行走的彩色多图像加密 [J]. 中国计量大学学报，2024，35(01):129−136+151.
[3] 张雨欣 . 量子密集编码的安全性分析 [D]. 北京邮电大学，2020.
[4] 尹安琪，汪定，郭渊博，等 . 可证明安全的抗量子高效 口令认证密钥交换协议 [J]. 计算机学报，2022，45(11):2321− 2336.
[5] 王焰 . 基于 NTRUEncrypt 的安全两方多项式数据计算 的研究 [D]. 杭州电子科技大学，2023.
[6]WANG X，XU G，YU Y .Lattice−Based Cryptography: A Survey[J].Chinese Annals of Mathematics，Series B，2023，44(06):945−960.
[7] 贺婧楠，张振飞 . 基于 NTRU 的加密及签名算法研究 [J]. 信息安全学报，2019，4(02):29−36.
[8]S. E M，V. A K，A. S N，et al.Post−Quantum Cryptosystems:Open Problems and Solutions. Lattice−Based Cryptosystems[J].Journal of Applied and Industrial Mathematics，2024，17(4):767−790.
[9]Li J，Yan M，Peng J，et al.A lattice−based efficient certificateless public key encryption for big data security in clouds[J].Future Generation Computer Systems，2024，158255− 266.
[10]Naik，Peterson，White，et al.Entangled state quantum cryptography:eavesdropping on the ekert protocol[J].Physical review letters，2000，84(20):4733−6.