量子计算在信息安全中的潜在应用与挑战

胡中平
（江苏省南京市建邺区人民武装部 南京 210000）

摘　要　文中旨在研究量子计算在信息安全中的潜在应用与挑战。通过分析量子计算的潜在应用以及量子计算对传统加密算法的影响，深入探索了量子计算时代的信息安全挑战，具体包括量子计算对云安全的潜在威胁、量子计算对区块链技术的影响以及量子计算对物联网（IoT）设备安全产生的影响，同时提出了应对这些挑战的对策。

关键词：量子计算；信息安全；量子计算危机
中图分类号　TP309

Potential Applications and Challenges of Quantum Computing in Information Security

HU Zhongping
（People's Armed Forces Department, Jianye District, Nanjing 210000, China）

Abstract　This paper aims to study the potential applications and challenges of quantum computing in information security. By analyzing the potential applications of quantum computing and the impact of quantum computing on traditional encryption algorithms, it deeply explores the information security challenges in the era of quantum computing, including the potential threats of quantum computing to cloud security, the impact of quantum computing on blockchain technology, and the security challenges posed by quantum computing on Internet of Things (IoT) devices, etc., and proposes countermeasures to address these challenges.

Keywords　Quantum computing, Information security, Quantum computing crisis

0　引言

随着科技的不断进步，量子计算作为一项颠覆性的技术正逐渐走进人们的视野。郭国平[1]指出，量子计算技术作为一种基于量子力学原理的计算方式，具有超越传统二进制计算的潜在能力。量子计算因其超高速计算和强大的并行处理能力，能在极短的时间内破解现有的安全加密算法，如 RSA 和椭圆曲线加密。因此，探索量子计算在信息安全领域中的潜在应用，并应对由此带来的挑战，成为业界的研究热点。

1　量子计算的潜在应用

量子计算的潜在应用领域众多，其中包括量子密钥分发（Quantum Key Distribution，QKD）、量子随机数生成（Quantum Random Number Generation，QRNG）、量子签名和认证（Quantum Signature and Authentication）、量子安全多方计算（Quantum Secure Multi-Party Computation）等。

1.1　量子密钥分发

量子密钥分发指利用量子力学原理来实现安全的密钥交换。通过量子比特的特性，通信双方可以在不被窃听的情况下共享密钥。这种方式保护了信息在传输过程中的安全性，避免了传统加密方法可能面临的被破解的风险。量子密钥分发的成功应用，将极大地提高互联网和通信系统的安全性[2]。

1.2　量子随机数生成

量子随机数生成利用了量子系统的不确定性特性，生成真正的随机数。传统的伪随机数生成方法大多基于特定的算法，而量子随机数生成则利用了量子比特的不可预测性。这些真正的随机数在密码学、模拟实验、大数据分析等领域具有广泛的应用，提供了更高层次的安全性和可靠性。

1.3　量子签名和认证

量子签名和认证是一种基于量子力学原理的安全验证机制。利用量子态的特性，这种方法可以确保信息的完整性，完成对发送者的身份验证。在数字签名和身份认证领域中，使用传统方法可能会受到量子计算的威胁，而量子签名和认证则提供了更加安全的替代方案，为信息交换提供了可靠的保障。

1.4　量子安全多方计算

量子安全多方计算允许多个参与方在不暴露各自输入

作者简介：胡中平（1971—），专科，研究方向为计算机信息技术。

的情况下进行联合计算。通过量子纠缠和量子叠加的性质，参与方可以共同完成计算任务，且不会泄露私密信息。这在金融、医疗数据分析等需要合作计算但又需要保护隐私的场景中具有巨大的潜力[3]。

2 量子计算对传统加密算法的挑战

2.1 传统加密算法的基本原理

传统加密算法大多基于数学问题的难解性来确保数据的安全传输。常见的传统加密算法包括 RSA（Rivest-Shamir-Adleman）加密算法、椭圆曲线加密（ECC）算法等。这些算法被广泛应用于现代通信和数据安全领域，但随着量子计算的发展，它们的安全性面临着严峻的挑战。

2.2 量子计算对 RSA 加密算法的影响

RSA 算法的安全性基于大整数分解的困难性。然而，量子计算中的 Shor 算法可以在多项式时间内解决大整数分解问题，从而破解 RSA 加密。通过分解大整数，攻击者可以获取 RSA 加密算法使用的私钥，进而窃取加密数据，威胁信息的机密性。

2.3 量子计算对椭圆曲线加密（ECC）的影响

椭圆曲线加密（ECC）是一种基于椭圆曲线数学问题的加密算法，具有较高的安全性和效率。然而，量子计算中的椭圆曲线算法攻击可以在较短时间内破解 ECC 加密。这种攻击威胁到了使用 ECC 加密的网络通信和数据存储，引发了对替代算法的需求。

2.4 其他加密算法受到的威胁

除 RSA 和 ECC 外，其他一些传统的加密算法也受到了量子计算的威胁。例如，基于离散对数问题的 Diffie-Hellman 密钥交换协议和椭圆曲线 Diffie-Hellman 密钥交换协议也容易受到量子计算攻击。此外，对称加密算法中的部分模式（如 Grover 算法），也会受到量子计算的影响，可能导致算法被快速破解[4]。

3 量子计算时代的信息安全挑战

3.1 量子计算对云安全的潜在威胁

随着量子计算技术的发展，云安全面临着前所未有的威胁。传统的加密算法（如 RSA 和 ECC），是云服务中常用的用户隐私保护工具。然而，量子计算中的 Shor 算法可以快速解决大整数分解和椭圆曲线离散对数等数学难题，这意味着传统加密算法的保护机制将被破解。恶意攻击者可以利用量子计算的优势，轻松窃取存储在云中的敏感信息，包括用户数据、金融记录等。这种威胁可能会导致个人隐私泄露、企业机密暴露等严重后果。

3.2 量子计算对区块链技术的影响

区块链技术的核心在于加密算法的不可逆转性，以确保交易的安全性和完整性。然而，随着量子计算技术的发展，传统区块链中的基础加密可能会受到威胁。量子计算中的 Grover 算法可以用来解决搜索问题，这意味着恶意攻击者可以更容易地找到区块链的哈希碰撞，破坏交易的唯一性，导致数据被篡改或被伪造。此外，量子计算还可能加速私钥的破解，进而导致交易过程中的非授权访问，损害区块链系统的安全性。

3.3 量子计算对物联网（IoT）设备的影响

物联网（IoT）设备通常具有低功耗、计算和存储资源有限的特点。传统加密算法在这些设备上的应用较为广泛，但量子计算技术的崛起使得这些设备的安全性受到了挑战。由于量子计算可以更高效地破解对称密钥和非对称密钥，物联网设备的通信可能变得易受窃听和伪装攻击。此外，物联网设备中的传感器数据可能包含个人隐私信息，一旦这些信息被泄露，就会导致严重的用户隐私泄露问题[5]。

4 应对策略及安全加固方案

4.1 加强对量子安全通信技术的研究与应用

面对快速发展的量子计算对信息安全造成的挑战，需要加强对量子安全通信技术的研究与应用。在量子密钥分发（QKD）技术的研发上，研究者们需要投入更多的资金和人力资源，不断加大研发力度，以提高 QKD 技术的安全性和稳定性。对于量子随机数生成（QRNG）技术，需要支持其商业化应用，促使其在各个领域得到广泛的应用，从而提高随机数的质量和可信度。在量子签名和认证技术的实际应用中，需要投入一定的研究资源，深入探索其在通信领域中的具体应用场景，确保通信数据的完整性和真实性。

4.2 推动量子安全算法的研究

量子安全算法在应对量子计算带来的信息安全威胁方面发挥着关键作用。在可以用来对抗量子计算攻击的密码学算法研究中，需要加强对新一代密码学技术的深入探索，确保这些算法在量子计算环境中的安全性。对于基于格的密码学算法，可以深入研究和推动其应用，因为这类算法在面对量子计算威胁时表现出色，提供了可靠的安全解决方案。对于基于哈希函数和码的新型加密方案，需要持续不断地投入资源，探索并设计具备创新性的加密技术，以加强传统加密算法在量子计算攻击下的抵抗能力。

4.3 建设量子计算安全生态系统

建设量子计算安全生态系统是应对量子计算信息安全挑战的重要措施之一。一方面，政府部门需要提供持续的政策支持和资金扶持，以促进本国量子计算产业的创新和发展。这意味着需要支持量子计算硬件和软件产业的发展，鼓励科研机构和企业进行深入的技术研究和开发，确保在量子计算领域的竞争力。另一方面，政府部门应制定相关政策，推动产业创新和标准化。例如，制定明确的规章制

度，推动量子计算产业的健康发展，推动产业标准化，提高整体水平，确保产品、服务的质量和安全性。同时，应积极加强国际合作，与其他国家和组织建立紧密的合作关系，共同分享安全经验和技术。这种国际间的合作不仅可以加速信息安全技术的创新，还能共同应对量子计算带来的全球性挑战，形成全球性的量子计算安全合作体系。

4.4 加固传统加密算法

为增强传统加密算法的安全性，应对量子计算攻击带来的挑战，应做好以下几点。(1)增强 RSA，ECC 等传统加密算法的密钥长度，以提高破解难度，提高信息的安全性。(2)应积极推动多因子身份验证(Multi-Factor Authentication)的普及，提倡和推广多因子身份验证方式，提高身份验证的复杂度，从而大幅增强信息的安全性。(3)建立并执行定期更新密钥的政策，确保定期更换加密密钥，降低因为长期不更新密钥而导致的风险，有效保障信息的持续性安全。

4.5 加强有关量子计算安全的教育和培训

加强有关量子计算安全的教育和培训，可以提高相关从业人员和公众的安全意识。(1)可以设计专门针对量子计算安全的培训课程，如量子计算的基础知识和安全应对策略等。(2)企业内部人员的量子安全意识培养也至关重要，通过定期的内部培训和演练，可以确保员工了解并提高应对潜在的量子计算威胁的能力。(3)推广量子计算知识，提高公众的安全意识，使人们在使用网络和传递信息的过程中更加警觉。

5 结语

量子计算在信息安全中的潜在应用主要集中在提供无条件安全的加密通信、增强随机数生成、确保数字签名和认证的完整性等领域。然而，它也导致了传统加密算法被破解、量子计算硬件的可靠性等挑战。因此，需要进行有针对性的战略调整，包括加强量子安全通信技术研究、推动量子安全算法创新等，确保信息安全的持续性与稳定性。

参考文献

[1] 郭国平.量子计算技术的产业变革与生态建构[J].人民论坛，2023(16)：13-17.
[2] 王敬，张萌，李芳，等.量子计算关键技术及应用发展分析[J].信息通信技术与政策，2023，49(7)：9-16.
[3] 王东，李春平，张淑荣.量子计算时代的安全加密算法研究[J].电脑与电信，2022(4)：85-88.
[4] 赵洋.后量子计算时代的信息安全[J].中国安防，2021(9)：106-112.
[5] 刘宏伟，石竑松.量子威胁及其应对技术[J].中国信息安全，2020(7)：30-32.

(上接第 119 页)

信息共享平台可以帮助医疗机构了解当前的网络威胁趋势，加强医疗机构之间的合作。通过共享攻击技术和恶意软件的信息，医疗机构可以更好地准备和防御潜在的攻击。在发生网络安全事件时，医疗机构可以共享信息，互相支持，并采取协调行动来应对事件。安全信息共享平台还可以提供匿名性保护，允许医疗机构分享信息而不暴露其身份。

4 结语

医保电子网络安全维护工作面临着重重困境，但通过合作与信息共享、借助新技术(如人工智能、区块链技术、云计算和大数据分析)，医疗机构可以更好地应对这些挑战。维护患者数据的隐私性和网络系统的安全性，这对提供高质量的医疗服务至关重要，应成为医疗机构的首要任务之一。因此，医疗机构应积极采取措施，不断提升医保电子网络安全的水平，以确保患者的信息得到妥善保护。

参考文献

[1] 国家医保局：加强网络安全和数据保护[J].医学信息学杂志，2021，42(4)：94.
[2] 严长春.医院电子医保凭证应用的实践与思考[J].信息系统工程，2021(11)：77-80.
[3] 张瑞娜."互联网＋"医保服务实施现状及对策研究[D].大连：东北财经大学，2021.
[4] 杨红燕.数字化时代的数字医保：内涵、价值、挑战与治理思路[J].华中科技大学学报(社会科学版)，2021，35(2)：17-24.
[5] 靳宏，李佳，高于峰，等.助力"医保控费"，中国人寿在政保合作服务中的 AI 技术探索与实践——以湖州地区为例[C]//浙江保险论文汇编 2020(上)，2020.