工程与管理科学
Engineering and Management Science
第 8 卷◆第 7 期◆版本 1.0◆2026 年
文章类型：论文|刊号（ISSN）：2705-0637(P) / 2705-0645(O)

量子计算下保密通信技术研究

杨志成
华为技术有限公司　江苏南京　210012

DOI：10.32629/ems.v8i7.21176

［摘　要］保密通信，使用密码技术等手段，保证信息在传输的过程中，为信息提供了机密性、完整性、真实性保障（身份鉴别等），保密通信的安全依赖于所使用的现代密码算法及密钥的安全。但量子计算的发展给现代密码算法带来了严重威胁，给保密通信的安全性带来了严重挑战，本文介绍了量子威胁，以及保密通信抗量子计算攻击的技术路线及挑战。

［关键词］保密通信；密码算法；密钥；后量子密码算法；量子密钥分发

1.保密通信业务场景

保密通信是指在通信过程中采用了保密措施的一种通信方式，现在保密通信通常是指通信的通道保密或者通信内容保密。

通道保密通常是指采用密码算法进行加密的方式在网络中建立安全的通信通道，将信息在该通道中传输以保障信息的完全，而通信信息保密则是指对会用密码算法对通信内容先加密，然后再通道中传输的方式，通过通道保密或内容保密的方式，保障了通信内容的安全，即使攻击者或者窃听者获得了通信内容，也无法还原，或者需要极高的成本还原通信内容。两种通信方式可以单独使用，也可以结合使用，业务可根据保密级别或或者业务诉求进行选择。

在诸多场景中，需要使用保密通信保护通信内容，保密通信则广泛应用于政府部门（如机要文电）、军队（如军事指挥及情报传递）、银行金融（如网银、网上支付、保险、证券交易等）、商业、个人（如聊天内容加密），及工业控制（如设备指令、业务数据）等领域。

在保密通信的身份认证、数据加密等场景中广泛使用现代密码算法，包括对称密码算法、非对称密码算法及散列算法（Hash，也称为哈希）等。

2.计算的发展

计算是保密通信发展的推动力，加密是保密通信安全的保障，同时，计算的发展推动了加密算法的发展。

计算发展的本质是从手工计算、机械计算、电子计算（含智能计算）至量子计算的不断推进、不断提升计算速度、方式和能力的过程。计算的发展，快速推动了密码算法的发展，以保障保密通信的安全。

在手工（人工）计算阶段，移位密码、代换密码为主流，如著名的凯撒密码；在机械计算阶段出现了使用机器（机械，非电子计算机）进行密码计算，典型为恩尼格密码机（Enigma），属于典型的机电式密码机；电子计算时代，出现了电子计算机、大型计算中心，产生了现代密码，如 AES、RSA、SHA 等。

现在，量子计算成为新的计算方式与发展方向，量子计算是以量子比特为基本单元，利用量子叠加和量子纠缠实现并行计算的新型计算模式，计算能力可随量子比特数指数级增长，在特定问题上远超传统计算机，并对现有密码体系构成重大挑战。

各主要国家、厂商、高校等，如中国、美国，谷歌等，在重点投入量子计算及抗量子的密码算法研究，并制定自己的抗量子密码算法体系，以保障量子计算时代保密计算的安全。

当前，美国通过 NIST（National Institute of Standards and Technology，美国国家标准与技术研究院）在全球征集并发布首批抗量子密码算法（运行于电子计算机上），中国也启动了抗量子密码算法征集，各商业公司也在积极探索量子保密通信，如华为技术有限公司设计与开发后量子 Polar-LAC 算法并在路由器商用，并向国际标准组织 ISO/IEC、IETF 等提交量子密码算法相关提案。

3.现代密码学威胁

在保密通信中，现代密码算法应用广泛，典型场景包括身份认证、协议安全、传输安全、本地存储加密、完整性保护等，这些场景广泛使用了现代密码算法，均受到量子计算的威胁，需升级算法或增加密钥长度以支持抗量子，保障保密通信安全。

现代密码算法主要包括对称加密算法（如 AES 256，用于传输数据加密）、非对称加密算法（如 RSA4096、ECC，用于密钥传输）、哈希（如 SHA-256，用于保障数据的完整性）及密钥协商算法（如 DH、ECDH，用于通信构成中的密钥协商）等。

但随着量子计算的发展，量子比特的增加、计算方式的改变及算力的增强，则对现代密码算法产生了巨大的影响，量子计算对现在密码算法与数据的威胁分类说明如下：

1、可破解非对称密码算法：在具有 4000 个量子比特的量子计算机上运行 Shor 算法（可在多项式时间内完成大数分解），可在数小时内破解 RSA-2048。

同样，量子计算可破解密钥协商 DH、ECDH 密码交换算法等，RSA、DH 等非对称密码算法，需要升级到可以抗量子计算的密码算法。

2、可降低对称密码算法的强度：通过 Grover 算法，量

子计算机将对称密码算法的安全强度降低一半。因此，对称密码算法需通过增加密钥长度,如 AES 从 128 增加至 256 位，在量子计算下可保持安全性。

3、可降低散列（哈希）算法安全强度：量子计算机使用 Grover 算法可将哈希算法强度降低一半，需增加密钥长度保持哈希算法的安全性

4、数据囤积攻击:囤积攻击为 Store Now, Decrypt Later (SNDL/ HNDL)，即攻击者现在无法破解你使用的 RSA/ECC 等传统加密，但可以被动窃听、复制并长期存储所有加密数据（密文）。等到未来量子计算机成熟（能运行 Shor 算法），再用它回溯破解当年存储的所有数据，获取现在的敏感明文。

因此，需研究抗量子密码算法，并对现网运行的网络设备、服务器、计算资源等进行升级，保障数据以及计算、传输、存储时的安全。

4.保密通信抗量子攻击技术路线

密码算法支持抗量子的主流路线包括两类：

1、PQC（Post-Quantum Cryptography,后量子密码算法）：运行在经典计算机（电子计算机）上、基于不同的数学问题。这些算法的安全性，依赖于有没有可快速求解其底层数学问题或直接对算法本身的高效攻击计算法。

该路线可与传统网络对接，设别可通过算法演进，升级软件，应用于身份认证、密钥协商、数字签名等场景。

2、QKD（Quantum Key Distribution，量子密钥分发）：利用量子微观效应，在合法通信双方之间无条件安全地建立相同的经典密钥，其安全性来源于量子力学，不受量子计算的高算力威胁。

对于 QKD 路线，需构建新的 QKD 网络，需要升级的部分包括协议、密钥生成与中级软件，安全性高，但同时带来高的升级成本，可用于关键数据传输、保护，如政务数据、企业的商业数据。

4.1 后量子密码算法（PQC）

PQC：后量子密码算法（Post-Quantum Cryptography, PQC），是运行在电子计算网络体系下的抗量子密码算法，是能够抵御量子计算机攻击的密码学算法。

在量子计算场景下，现代密码算法体系中的公钥密码算法（包括非对称密码算法 RSA、椭圆曲线密码算法 ECC，以及哈希算法，如 SHA-1）面临被破解的威胁，量子计算机凭借其并行计算能力，可以破解非对称密码等算法，并将对称密码算法的安全性降低一半。

因此，世界主要国家、科研团队研究、推进迁移至 PQC，替换原本的公钥密码算法体系，已抵御量子计算机的攻击。

4.1.1 后量子密码算法解决的问题

4.1.1.1 抵御量子计算机对现有密码体系的攻击

现代密码算法体系的安全性基于计算意义上的困难问题，典型包括大整数因子分解问题、离散对数问题，对于电子计算机等传统计算机以及经典算法，这些困难问题几乎难以解决。

1994 年发明的 Shor 算法改变了该状态，通过构建足够大的量子计算机来运行 Shor 算法，可以有效、快速的分解大整数,进而是的公钥密码算法 RSA 和 DH 之类的相关算法被彻底攻破，不再安全。

这对互联网、政务网络等造成巨大的影响。许多数据（如政府机密、金融记录、医疗信息）需要长期保密，但当前加密的数据可能被量子计算机 “先窃取后解密”（即攻击者先截获数据并存储，待量子计算机成熟后破解）。

因此需要在电子计算时代，构建并迁移至可抵御量子计算攻击的密码算法，构建新的安全防御体系。

4.1.1.2 构建量子计算时代的安全通信基础

密码算法是安全通信的基础，在量子计算时代下安全通信面临如下关键问题需要解决：

1、通信加密：需构建抗量子的密钥交换协议，已替代现在密码算法体系中的密钥交换协议，如 DH、ECDH，以防范量子窃听；

2、通信内容完整性：现代密码算法防护体系数字签名、Hash 等会被量子计算破解，因此需提供抵御量子计算攻击的完整性算法，保护通信内容完整、真实。

抗量子算法迁移兼容性：互联网上当前使用的是公钥密码算法体系，在数据传输、数据处理及数据存储等方面大量使用，协议、算法等迁移至后量子密码算法体系时，需考虑兼容性部署，避免出现不兼容问题，导致通信安全真空。

4.1.2 后量子密码算法标准进展

为应对量子计算对通信安全带来的威胁与冲击，世界上各国家、地区都在制定抗量子密码算法及标准，如美国 NIST 于 2016 年启动后量子密码算法标准化项目,该项目成果也是当前可商用的密码算法。

当前，后量子密码算法基于不同的数学难题，主要包括如下几类：

1、基于格的密码算法（Lattice-based）：最为通用的一类，可以实现几乎所有的经典公钥密码功能柜，加密、签名、密钥交换均高度实用化，代表算法包括 Falcon（数字签名算法，用户替换 RSA、DSA、ECDSA 等签名算法）、Dilithium（非对称加密算法、密码要协商，用户替换 RSA、ECIES、DH、ECDH 等非对称算法）；

2、基于哈希（Hash）的密码，用于构造签名，安全性分析已较为透彻，代表算法包括 XMSS、LMS、SPHINCS+算法，主要应用于软件包、数据的签名与验签，支持数据的完整性与真实性；

3、基于编码 (Code-based)：最早出现于 1978 年，主要用于构造加密算法。代表算法为 McEliece；

4、基于多变量 (Multivariate-based)：最早出现于 1988 年，主要用于构造数字签名、加密、密钥交换等。代表算法为 Rainbow 。

4.1.3 后量子密码算法应用进展

各国家、机构与商业公司都在大力推进抗量子密码算法。当前，后量子密码算法（PQC）已从标准制定全面进入工程化、规模化部署的关键阶段。全球主要科技公司、运营商、金融机构与政府部门正加速将 NIST 标准算法（ML-KEM/Kyber、ML-DSA/Dilithium、Falcon、SPHINCS+、HQC）集成到 TLS、VPN、云、5G/6G、区块链与工业控制系统中，以抵御 Store Now, Decrypt Later 攻击。

微软、IBM、谷歌等企业已开始在云计算、浏览器等场景中测试后量子密码方案；金融和政府机构逐步规划后量子迁移路线图。

4.1.4 后量子密码算法应用挑战

对于后量子密码算法的应用，当前仍存如下关键挑战：

PQC 算法的安全性需进一步评估，在 PQC 算法的选择过程中，出现多种算法被破解的的问题，因此 PQC 算法的安全性、算法实现的安全性等需进一步评估。

协议支持抗量子缺少规范：对于身份认证、安全传输、协议安全等，大量使用了非对称密码算法，当前缺少支持抗量子的的协议规范。

后量子密码算法在密钥长度、加密数据长度等均增大，造成通信贷款增加、证书大小增加，会导致数据传输时需分片，增大了协商时间，因此，需在算法的硬化上做进一步研究。

现网如何支持密码算法的平滑升级、迁移，现网部署复杂、设备多样，如何平滑的迁移、对接、全网支持抗量子成为关键挑战。

4.2 量子密钥分发（QKD）

量子密钥分发（Quantum Key Distribution, QKD） 是一种利用量子力学原理（如量子叠加、量子纠缠、量子不可克隆定理）实现安全密钥协商的技术。

QKD 利用量子微观效应，在合法通信双方之间无条件安全地建立相同的经典密钥，其安全性来自量子力学，不受量子计算的高算力威胁，是量子安全密码（Quantum Safe Cryptography）的重要技术之一，是目前最可实用的量子通信技术。

4.2.1 量子密钥分发方案解决的问题

量子密钥分发的核心目标是解决传统密码学中密钥分发的安全性隐患，确保通信双方能够安全、可靠地共享加密密钥。

QKD 可以作为一种新的密钥分发功能组件，广泛应用与现有的 ICT（Information and Communications Technology：信息通信技术）系统。与经典密码学中的密钥分发算法类似，QKD 可以与 OSI 参考模型中的不同层的协议进行结合，解决使用各层协议进行数据传输时的量子威胁：

TCP/IP 协议栈主要安全协议包括应用层 SSH、传输层 TLS/DTLS、网络层 IPSec、物理层 MACSec，QKD 可以与各层安全协议集成，获取量子密钥，以解决量子计算威胁。

4.2.2 量子密钥分发应用场景

量子密钥分发可以应用于安全要求高的业务场景，典型包括金融政务、卫星通信、工业与物联网，详细包括

1、在金融与政务领域为银行转账、政府机密文件传输提供高安全级别的密钥分发，防止量子时代的“先窃取后解密”攻击。构建量子保密通信网络，构建安全的端到端量子密钥分发链路（如城域网、广域网）。通过卫星实现长距离量子密钥分发（如中国 “墨子号” 卫星已实现千公里级量子密钥分发），实现卫星通信抗量子攻击；对与工业与物联网，保护工业控制系统（ICS）、智能设备的通信密钥，抵御针对物联网设备的低算力量子攻击。

4.2.3 量子密钥分发应用面临的挑战

4.2.3.1 技术挑战

1、传输距离限制：当前技术限制在 80KM，光纤传输中光子会因损耗衰减，需依赖量子中继器（尚未成熟）延长距离。

2、环境干扰：自由空间传输易受天气、大气湍流影响，需高灵敏度单光子探测器。

3、设备国产化：核心器件（如单光子源、探测器）依赖进口，需突破自主可控技术。

4、QKD 组网：当前 QKD 多采用密钥注入的方式，需要研究能够自组网的能力，提升量子密钥分发技术的可应用性。

4.2.3.2 标准化与产业化

1、国际电信联盟（ITU-T）、中国通信标准化协会（CCSA）等组织正推动 QKD 标准制定。

2、中国已建成 “京沪干线” 量子保密通信骨干网，实现金融、政务等领域的商用试点；欧美企业（如 ID Quantique、MagiQ）也在布局 QKD 产品。

4.2.3.3 与后量子密码的协同

从上述分析可以看出，QKD 提供密钥分发的物理层安全，后量子密码（PQC）保障算法层安全，两者结合、协同使用，可构建 “量子 + 后量子” 的双重安全体系，已成为学术界、工业界研究的新热点。

5. 总结

随着量子计算机的快速发展，保密通信需加速抗量子能力，但技术规范、标准的建设以及现网敏捷迁移成为下一步工作的重点。

[参考文献]

[01]龙桂鲁，盛宇波，殷柳国. 量子通信研究进展与应用. 物理 47 卷(2018 年)7 期

[02]张晓枫，高新凯. 量子密钥分发驱动网络通信数据传输安全防护技术研究. 网络安全技术与应用，2026 (04) : 25-26