中国信息协会量子信息分会
Quantum Information Association of China

量子安全技术白皮书

（2020）

中国信息协会量子信息分会

（2020 年 12 月）

版权声明

编写人员

赵　勇[1,4]

戚　巍[2,5]　徐兵杰[3,6]

赵梅生[4]　黄　强[1]　马彰超[2,5,7]　郁　昱[8]　王后珍[9]

赵　波[9]　孙仕海[10]　马家骏[1]　秦　灏[5]　赵于康[4]

王留军[11]　姜　艳[4]　武宏宇[4]　姜　聪[12]　余　庆[4]

1 中国信息协会量子信息分会，2 中国通信标准化协会量子通信与信息技术特设任务组，3 中国电子学会量子信息分会，4 科大国盾量子技术股份有限公司，5 国科量子通信网络有限公司，6 中国电子科技网络信息安全有限公司，7 北京科技大学，8 上海交通大学，9 武汉大学国家网络安全学院，10 中山大学，11 云南大学，12 济南量子技术研究院

前言

随着信息通信技术的快速发展，社会的信息化程度日新月异，国家、机构、个人的信息安全需求与日俱增。密码技术作为信息安全技术的基石在保障信息的机密性、真实性、完整性和不可抵赖性方面发挥着核心作用。得益于数学的支撑，现代密码学构建了较完善的体系，而与其相生相克的密码破解技术却也一直在挑战和刺激着密码学的不断演进。特别是以量子计算为代表的计算能力飞跃发展，已经对基于大数分解、离散对数等数学难题的公钥密码体系带来了前所未有的挑战。于此同时，基于量子物理的量子密码技术（以基于量子通信的量子密钥分发为代表）和基于新型数学难题的抗量子计算公钥密码算法担负起了抵御量子计算挑战的重任，并在国际上催生了新的安全概念——量子安全。虽然距离第一台能破解典型公钥密码的量子计算机出现可能还需十年甚至二十年时间，但国家、机构甚至个人的核心数据保密年限需求也会达到数十年之久，其将面临诸如：现在被截获和存储，将来被破译等安全风险。因此，实践量子安全保障已具现实意义。

当前，量子密钥分发技术日臻成熟、商业产品已经投入实践；抗量子计算密码算法也正在广泛征集、快速发展。量子安全已成为国际热点与创新前沿。我国在量子通信及抗量子计算密码方面积累深厚、自主可控，并走在世界前列。本白皮书将围绕什么是量子安

全技术、如何实现量子安全技术，如何在信息系统中使用量子安全技术等方面凝聚学术界和产业界共识，并立足当下、面向未来探讨量子信息技术和新型密码技术如何在新一代信息技术基础设施中发挥作用，形成战略性新兴产业，服务社会民生。

本白皮书由中国信息协会量子信息分会牵头，中国通信标准化协会量子通信与信息技术特设任务组、中国电子学会量子信息分会联合组织编写。编写组人员分别来自科大国盾量子技术股份有限公司、国科量子通信网络有限公司、中国电子科技网络信息安全有限公司、北京科技大学、上海交通大学、武汉大学国家网络安全学院、中山大学、云南大学、济南量子技术研究院等 9 家单位。

本白皮书在编写过程中还得到了清华大学王向斌教授、中国科学技术大学张军教授、中国科学技术大学聂友奇博士等专家的帮助和指导，在此向他们表示诚挚的谢意。

目录

一、概述

（一）信息安全和密码技术

1. 从传统信息安全到网络空间安全

传统概念上的信息安全指信息生成、存储、传输等处理过程的安全。信息安全概念产生于防御以窃取敏感信息为主要方式的早期信息攻击。其一般特点我们可以总结为强调技术，强调防护。

现代社会中由于信息的使用无处不在，信息系统应用深入、广泛，对社会发展起到了加速器的重要作用，随之而来的信息安全问题也愈发凸显。社会生产生活涉及到的信息安全几乎包含了现代社会的各行各业和方方面面，如国家安全、基础设施安全、公共医疗与卫生、个人隐私保护、虚假信息甄别、突发事件应急响应等。与此同时，信息安全也正从传统理念向网络空间安全理念发展。网络空间安全理念更强调应对防御上的综合性与主动性，安全体系建设上的全程性。在网络空间安全时代，面对安全威胁的复杂性乃至一定程度的未知性，讨论信息安全问题时我们应该有体系意识和边界意识，没有一种安全技术、安全体制对信息安全威胁是“银弹”，是包打天下的。

2. 信息安全保障的关键要素

对信息安全保障的关键要素一般理解如下：

（1）可用性（Availability），是指即使在突发事件下，依然能够保障数据和服务的正常使用，如网络攻击、计算机病毒感染、系统崩溃、战争破坏、自然灾害等。

（2）机密性（Confidentiality），是指能够确保敏感或机密数据的传输和存储不遭受未授权的浏览，甚至可以做到不暴露保密通信的事实。

（3）完整性（Integrity），是指能够保障被传输、接收或存储的数据是完整的和未被篡改的，在被篡改的情况下能够发现篡改的事实或者篡改的位置。

（4）可认证性（Authentication），也称真实性，是指能够确保实体（如人、进程或系统）身份或信息、信息来源的真实性。

（5）不可否认性（Non-repudiation），是指能够保证信息系统的操作者或信息的处理者不能否认其行为或者处理结果，这可以防止参与某次操作或通信的一方事后否认该事件曾发生过。

3．密码技术在保障信息安全中的作用

密码是信息安全的基础、核心和支撑，是信息安全体系结构中最“硬核”的底线，又与信息有最直接、最“亲密”的保护关系。

具体来说，可以总结为密码技术为信息安全提供四种安全服务：

- **保密性服务**

保护数据以防窃听为主的被动攻击。保护方式可依据通信关系（一对一还是一对多）、保护范围等因素而不同。

- **完整性服务**

和保密性服务一样，完整性服务也能应用于整个消息流、单个消息或一个消息的某一选定域。用于保证所接收的消息未经插入、篡改、重排或重放，因此和所发出的消息是完全一样的。

- **认证服务**

用于保证通信的真实性。在单向通信的情况下，认证服务的功能是使接收者相信消息确实是由它自己所声称的那个信源发出的。在双向通信的情况下，在连接开始时，认证服务则使通信双方都相信对方是真实的（即的确是它所声称的实体）。

- **不可否认业务**

用于防止通信双方中的某一方对所传输消息的否认，接收方收到消息后，能够证明这一消息的确是由通信的另一方发出的。

（二）量子计算及其对于密码技术的威胁

1. 对称密码技术和非对称密码技术

1.1 对称体制

对称密码指加密密钥和解密密钥相同的密码体制[1]。其安全性取决于两点：一，密钥的安全性，一切秘密寓于密钥之中，密钥管理至关重要；二，加解密算法的安全性。对称密码包括两个主要分支：流密码，对明文消息按字符逐位进行加密；分组密码，将明文消息分组并逐组进行加密。代表性对称密码算法包括：AES、IDEA、SM4、ZUC

等。对称密码体制安全等级高，加解密效率高，可通过低成本芯片高效实现，主要用于数据加密和消息认证。

1.2 非对称体制

非对称体制下的密码即公钥密码[1]，其基本思想是：密钥成对出现，一个为加密密钥（公开的，故称公钥），一个为解密密钥（秘密的，故称私钥），且从公钥推算出私钥在有限的计算资源和计算时间内是不可行的。其安全性取决于公钥算法所依赖的数学困难问题的计算复杂度。最具代表性的应用于公钥密码设计的数学困难问题包括质因数分解、离散对数、椭圆曲线问题等。代表性公钥密码包括：RSA、El Gamal、ECC 等。公钥密码主要用于加解密、密钥分发、数字签名、认证等。

1.3 对称与非对称体制的比较与配合

对称与非对称体制的密码技术可确保信息的机密性、真实性、不可抵赖性、完整性等（如表 1-1 所示）[1]：机密性基于加解密密码功能，主要依赖于对称密码，部分场景可采用公钥密码；真实性基于认证密码功能，主要依赖于对称密码、公钥密码和杂凑函数；不可抵赖性基于签名密码功能，主要依赖于公钥密码；完整性基于摘要密码功能，主要依赖于杂凑函数。

在加解密等应用场景中，公钥与对称密码需结合使用。加解密系统中首先需要在通信双方间建立一致的、安全的密钥（即密钥分发过

程），然后再基于该密钥实现加解密，系统整体安全性依赖于密钥交换过程的安全性和加解密算法的安全性。其中，密钥分发过程主要依赖于公钥密码，其安全性主要基于质因数分解、离散对数、椭圆曲线等数学困难问题的计算复杂度，加解密过程主要依赖于对称密码。

表 1-1 密码服务对应的密码体制

信息安全属性	所需密码功能	对称密码	公钥密码	杂凑函数
机密性	加密	普遍使用	使用不普遍	-
真实性	认证	普遍使用	普遍使用	普遍使用
不可抵赖性	签名	-	普遍使用	-
完整性	摘要	-	-	普遍使用

2. 量子计算的原理和应用

2.1 量子计算基本原理

量子计算是一类遵循量子力学规律进行高速数学和逻辑运算、存储及处理量子信息，解决各类问题的技术，量子计算机是实现这一技术的物理装置。量子计算以量子比特为基本单元，通过量子态的受控演化实现数据的存储和计算，具有经典计算无法比拟的信息携带和并行处理能力。其优势源于以量子相干叠加和干涉来编码和处理信息而引入的量子并行性。量子计算对量子相干叠加态的每一个叠加分量实现的变换相当于一种经典计算，所有这些经典计算同时完成，并按一定的概率振幅叠加，给出量子计算输出结果，此即量子并行计算。量子计算的主要能力如下：

（1）**克服摩尔定律失效：**量子计算能克服晶体管特征尺寸减小引起的热耗效应和量子效应对现有计算机进一步发展的制约，解决经典计算机制造中面临的摩尔定律失效问题，是下一代计算机的重要发展方向。

（2）计算力飞跃：利用量子叠加效应实现量子并行计算，极大地提高计算速度和信息处理效率。量子计算被证明能指数或多项式量级加速某些有重要应用价值的计算问题的求解。

2.2 量子计算发展现状及趋势

（1）发展现状简介

近年来，各主要发达国家都大力投入量子计算研究。美国已形成政府、科研机构、产业和投资力量多方协同攻关局面，英国、欧盟、日本、加拿大、澳大利亚、中国等也在量子计算领域紧密跟随，不断加大对量子计算的投入。以 IBM、Google、英特尔为代表的科技巨头间竞争激烈，开展了如火如荼的“量子比特大战”，积极开发原型产品，推动了量子计算技术的快速发展。近年来，量子计算芯片的量子比特位数得到不断提升（目前正在向 128 量子比特发展），其增长速度基本符合摩尔定律，故也被称为“量子摩尔定律”。我国中国科学技术大学、中国科学院、阿里巴巴、腾讯、百度和华为等高校、科研院所和商业公司为代表在量子计算领域进行了大量布局，部分技术成果处于国际先进水平。

量子计算机可基于多种不同物理体系实现[2]，如离子阱体系、超导量子电路体系、半导体量子点体系、腔量子电动力学体系、核磁共振体系、线性光学体系、拓扑体系等。量子计算机总体上仍处于技术验证和原理样机研制阶段，目前处于中型含噪量子计算（NISQ）阶段（例如谷歌的 Sycamore），仍面临量子比特数量少、相干时间短、出错率高等诸多挑战。目前，超导和离子阱技术路线的研究相对较多、组成的量子线路规模相对较大，但总体而言尚无任何一种路线能完全满足实用化要求并趋向技术收敛。

（2）发展趋势

实现实用的通用量子计算机技术难度很大，是一个长期任务[2]：第一个阶段是实现量子优越性（或量子霸权），即针对特定问题的计算能力超越经典超级计算机，这一阶段目标已在 2019 年由 Google 公司在其超导量子计算系统上率先实现[3]，在 2020 年由中国科学技术大学在其光量子计算系统再次实现[4]；第二个阶段是实现具有实际应用价值的专用量子模拟系统，可在组合优化、量子化学、机器学习等方面发挥效用；第三个阶段是实现可编程的通用量子计算机。上述目标的实现还需要全世界学术界、工业界的长期艰苦努力。

然而，量子计算不是万能的，不能完全取代经典计算。目前量子计算已在大数分解、无序数据搜索、求解线性方程、组合优化等重要问题上被证明有优势，需探索更多有用的量子算法。量子计算究竟能多大程度解决多少有重要实际应用价值的计算问题仍需进一步探索。

2.3 量子计算的应用领域

量子计算技术所带来的算力飞跃，有可能成为未来科技加速演进的“催化剂”，一旦取得突破，可在生物医学、材料学、化学、密码破译、气象预报、空气动力学计算、武器研制、人工智能、能源与大数据等多个方面得到应用，为先进材料制造和新能源开发等奠定科学基础，对提升国家综合竞争力有战略意义。

3. 量子计算对经典密码安全性的威胁

密码是信息安全的核心，现有的信息安全是建立在经典密码技术之上的，包括对称体制和非对称体制。然而，量子计算技术和量子算法的不断进步，为密码破译提供了更有力、更致命的攻击方法。著名的 Shor 量子算法和 Grover 量子算法对经典密码体制安全性构成威胁。

Shor 量子算法可以在多项式时间内分解大整数和求解离散对数等复杂数学问题，因此可以对广泛使用的 RSA、ECC、DSA、ElGamal 等公钥密码体制进行快速破解。例如：分解一个 400 位的大数，经典计算机约需要 5×10^{22} 次操作，而量子计算机约需要 6×10^{7} 次操作，量子计算机所需操作数仅为经典计算机的 80 万亿分之一！

Grover 量子算法能够将无序数据库的搜索时间降为平方根时间。例如，当需要从 N 个未分类的客体中搜索出某个特定客体时，经典计算机需要一个个查询，直到找到所要的客体，平均要查 N/2 次，找到的几率为 1/2，而采用 Grover 算法的量子计算机采用并行处理，只

需 $N^{1/2}$ 次，找到的几率接近 100%。例如，Grover 算法可以有效地攻破以 DES 等为代表的对称密码，其本质就是从 2^{56} 个可能的密钥中寻找正确密钥。若以每秒 10^6 次的运算速率，经典计算机要花 1000 年，而采用 Grover 算法的量子计算机所需时间低于 4 分钟。

综上，如表 1-2 所示，Grover 量子算法同时适用于对称密码和公钥密码破译，其能力等价于将等效密钥长度减半。应对措施是将对称密码算法使用的密钥长度加倍；对于无密钥参与的哈希函数,应将哈希函数输出长度加倍。Shor 量子算法对基于大整数分解和离散对数问题的公钥密码产生了严重威胁，需要考虑采用新的密码算法加以应对。

表 1-2 量子计算机对经典密码的影响(来源于 NIST IR 8105[5])

密码算法	类型	功能用途	量子计算影响
AES	对称密码	加解密	需增加密钥长度
SHA-2, SHA-3	杂凑	哈希散列函数	需增加输出长度
RSA	公钥密码	数字签名，密钥分发	不再安全
ECDSA, ECDH	公钥密码	数字签名，密钥分发	不再安全
DSA	公钥密码	数字签名，密钥分发	不再安全

（三）量子安全的内涵

1. 量子安全的概念

对应于量子计算的攻击，量子安全（quantum safe）的概念也被相应的提出[6]。顾名思义，量子安全是指即使面对量子计算的挑战也能得到保证的信息安全。而与之相关的量子安全密码学是指寻找和

确认可抵御经典计算机和量子计算机攻击的算法和协议，即使在大型量子计算机出现之后也能确保信息资产的安全。

如前所述，目前并非所有的经典安全协议和密码算法都容易受到量子计算的攻击，部分算法被认为是量子安全的，另一部分则被认为是不能免疫量子攻击的。如果某种算法或协议在经过充分研究后，表明其可以抵御所有已知的量子算法攻击，同时在没有证据表明其易受量子攻击前，就可以认为其是量子安全的。当然，在经过深入研究后，目前被认为是量子安全的算法在未来未必安全的可能依然存在。

诸如 AES 之类的对称密码算法可以被认为是量子安全的。因为对于对称密码而言，虽然使用运行 Grover 算法[7]的量子计算机可以比传统计算机更快地破解对称算法，但是，通过将对称密码的密钥长度加倍，可以使量子计算机进行破解的难度与传统计算机相当。例如，目前的研究显示，对于经典计算机而言，AES-128 是难以破解的，而对于量子计算机和已知量子算法而言，AES-256 却很难破解。因此 AES 被认为是量子安全的。但 RSA 和 ECC 这样的公钥密码算法不是量子安全的，因为它们无法通过增加密钥长度来超越量子计算的发展速度。例如，研究表明，攻击 RSA 算法所需的量子比特数与 RSA 密钥的长度大致成线性比例关系，所需的量子门操作次数和 RAS 密钥的长度成多项式关系；也就是说，RSA 算法无法通过增加密钥长度来抵御量子计算的指数加速攻击[8]。 目前受量子计算攻击影响最大的是建立在整数分解和离散对数等计算复杂性上的公钥密码体系，包括 RSA，DSA，DH，ECDH，ECDSA 以及基于这些密码的其他变体。从这些公钥密码中

获取安全性的安全协议和系统都将受到量子计算的威胁。然而，目前的安全产品和协议中几乎所有公钥密码都需要使用这些类型的密码算法。因此，需要用量子安全密码代替这些密码算法才能抵御量子攻击。此外，对称密码通常使用公钥密码技术来进行对称密钥交换，即使对称密码本身是量子安全的，但由于对称密钥不安全，整体的量子安全性也无法得到保证。

实现量子安全的方式主要分为两类：一类是可以抵御已知量子计算攻击的经典密码算法，该类密码算法的安全性同样依赖于计算复杂度，这类算法或协议通常称为抗量子计算密码（Quantum Resist Cryptography，QRC）或后量子密码（Post Quantum Cryptography，PQC）。其中主要包括基于哈希的密码、格密码、基于编码理论的密码、多变量密码、超奇异椭圆曲线以及大部分对称密钥密码。如前所述，这些后量子密码能抵御已知的量子攻击，对于新出现的攻击可能并不免疫。同时即使是已知攻击，其安全性同样是基于计算困难性。

另一类量子安全的密码则是以量子物理原理为依托的量子密码（Quantum Cryptography），其最具代表性的协议是量子密钥分发（Quantum Key Distribution，QKD）[9]。QKD 具备信息论安全性，意味着 QKD 即使在攻击者拥有无限强的计算资源下也仍然安全，这其中自然也包含了面对经典和量子计算的安全性。 “信息论安全”在密码学领域也被称为“无条件安全”，这里的“条件”特指计算能力的限制，即安全性没有基于攻击者计算能力的假设。QKD 的功能是实现对称密钥的协商，需要与应用对称密码的算法结合以实现加解密功

能。QKD 结合“一次一密”可实现信息加密的信息论安全性，而结合量子安全的对称密码算法实现的是量子安全。当然，量子密码能够实现的密码功能不限于密钥协商，还可以实现数字签名、秘密共享等密码功能，而其中 QKD 的实用化进展目前是最快的。

2. 量子安全的重要性及紧迫性

当前以互联网为代表的公共网络基础设施，其用户认证、数据加密都主要依赖于 Diffie-Hellman、RSA、ECC 等公钥密码，例如我们浏览网站以及各类互联网应用程序常用的 HTTPS 协议、VPN 软件和设备、基于 X.509 标准[10]的数字证书应用等。对于信息安全保密性有高级别要求，或者对保密时效有较长时间要求的领域，其中可能包括军队中的军事通讯、政府传输机密文件、工业和商用领域传输的核心技术和数据、金融领域传输的金融数据、医疗行业传输的医疗记录个人信息等，也在大量使用公钥密码。正如上文所述，这些现有公钥密码系统具有易被量子计算攻击的弱点，在未来会被攻破已经成为密码行业、信息安全行业和量子计算专家公认的事实，普遍认为它将影响大部分现行公钥密码及其基础设施——可能会导致它们全部失效，同时也会削弱其它类如对称密码、杂凑等现有密码系统的安全性。这意味着所有信息系统使用者都将需要将密码全面升级至量子安全级别。

更重要的问题可能是我们何时需要量子安全。关于这一问题，仅考虑建造大规模量子计算机的时间是不够的。还需要同时考虑信息需要保持多长时间，以及将现有通信基础设施更新至量子安全将花费的

时间。关于这些时间的关系，加拿大滑铁卢大学量子计算研究所的 Mosca 教授给出了业界较为认可的 XYZ 理论（如图 1-1 所示）[11]。具体而言，X 代表“数据需要保密的时间”，Y 代表“更新我们的通信基础设施至量子安全所需要的时间”， Z 代表“建造大规模量子计算机所需要的时间”。如果 X+Y>Z，那么传递的信息就可能存在较大安全风险，因为这意味着在重新部署具有量子安全的基础设施和信息安全需要持续的时间之和大于建造大型量子计算机的时间 Z，那么在 X+Y-Z 这段时间内加密的信息将不再安全，攻击者可以利用量子计算轻易破解加密信息。反之如果 X+Y<Z, 攻击者不会得到利用量子计算机破解加密信息的机会。

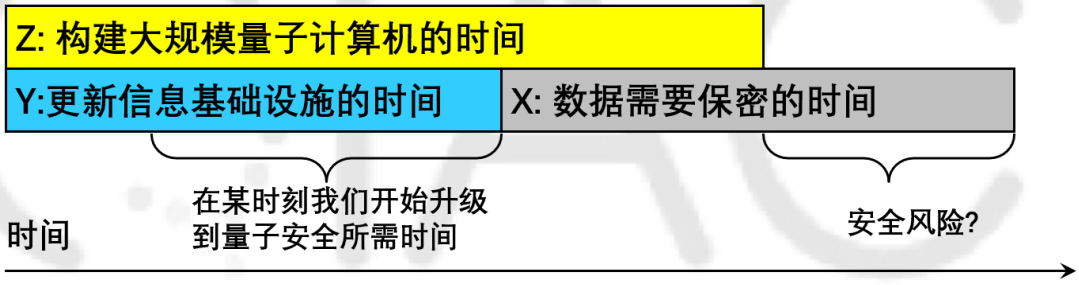

图 1-1 构建量子安全所需时间关系图[11]

在实际应用中，需要结合具体行业和场景考虑 X 的大小。一个重要的问题是 X 年后，某类信息成为公共信息的后果是什么？尤其是涉及到敏感信息的情况下，决定 X 的值需要非常谨慎，例如绝密的军事信息，政府的秘密文件等。欧美情报机构通常要求保密文件的保密时间 X>30 年。对于公众领域，X 的值可以适当放宽，但也需要考虑具体的场景和要求，例如个人的信用卡信息可能只需要 X<5 年，因为信用卡的有效期一般低于 X。而对于个人的身份证信息可能至少需要 X>10 年。再例如，随着技术的发展，诸如指纹、面部、基因等个人生物信

息的长期保密需求也变得紧迫，这时 X 可能就需要取决于每个人的生命年限。定义 X 的值并不容易，需要综合应用、技术发展、需求等进行深入研究，并进行风险分析和建模。

如前所述，学术界和工业界对于量子计算可能带来的威胁已经有比较清晰的认识。虽然目前大规模量子计算机还未到来，但是对于对信息安全需要有保障的行业以及政策决策者而言，需要进行前瞻性分析和思考，综合考虑量子计算机建造时间，信息需要保护的时间，升级基础设施需要的时间等因素，来决定何时需要量子安全。而最为保险的做法当然是尽快就开始考虑升级到量子安全的信息通信系统和基础设施。

量子安全不是指某一类技术或现有技术到新技术的演进，而是未来各类密码需要考虑满足的要求，从密码技术发展的攻防对抗特性上，从国家安全战略的前瞻性上，需要认识到这一重要性。而由于现代密码学内涵丰富、涉及软硬件模块与系统众多；量子密码随着量子信息科技的快速发展其本身也处于蓬勃发展当中；后量子密码算法本身又包含多种不同原理、不同类型的算法，所有这些技术上高度的专业性、复杂性导致 ICT 行业从业者、信息系统用户乃至密码和信息安全行业内部都有可能对此认识存在滞后和不足之处。而且，也正是由于这些技术、产业及政策上的复杂因素存在，应当将密码实现量子安全这一整体必达目标分解细化为一系列具体小目标和可行的实现路径和路线图。例如，目前阶段要实现量子安全就需要替换易受量子计算攻击的现用公钥密码算法。

二、量子安全技术

（一）基于数学问题的密码技术

基于已知量子算法无法多项式时间求解的数学困难问题设计的后量子密码体制（PQC）[12]，具有抗量子计算攻击的潜力，可实现量子安全。后量子密码技术相信，量子计算有优势，必然也有劣势，有其擅长计算的问题，也有其不擅长计算的问题。基于量子计算不擅长计算的数学问题构造密码，便可以抵御量子计算的攻击。虽然量子计算在大数分解等问题上能实现指数加速，但目前并无证据表明，量子计算擅长计算诸如非线性方程组求解问题、纠错码的一般译码问题。于是，研究者基于这些困难问题设计密码（主要指公钥密码体制），并称这些密码算法是抗量子计算的。

1. 格密码

格代数结构最早是作为一种密码分析工具被引入密码领域的，如1982 年，Shamir 采用格理论攻击背包公钥密码算法。基于格问题设计密码算法始于 Ajtai 的早期工作，1996 年他首次提出了基于格的单向陷门函数的思想[13]，并开创性地给出了格中某些困难问题的 worst-case（最坏情形）到 average-case（平均情形）的规约证明，从而为格密码体制的可证明安全奠定了基础。1997 年 Ajtai 和

Dwork[14]构造了第一个格密码体制。随后涌现出一批基于格的密码算法。其中比较著名如 1998 年 Hoffstein、Pipher 和 Silverman 提出 NTRU (Number Theory Research Unit)公钥密码体制[15]。NTRU 密码除了具有抗量子计算的性质外，与 RSA、ECC、ElGamal 密码相比还具有很大优点，相同安全性条件下，NTRU 算法的运行速度要快许多倍，密钥生成也更快且需要更小的存储空间。然而，NTRU 密码也存在不足，最主要的问题是其作为基于格的密码却没有严格的基于格问题的安全证明。

NTRU 作为最快速的公钥密码之一，引起了人们极大的研究兴趣。然而，基于 NTRU 的数字签名方案却并不十分成功。2000 年 Hoffstein 等利用 NTRU 格提出了 NSS 签名体制[16]，这个体制在签名时泄露了私钥信息，导致了一类统计攻击，后来被证明是不安全的。2001 年设计者改进了 NSS 体制，提出了 R-NSS 签名体制，不幸的是它的签名仍然泄露部分私钥信息，Gentry 和 Szydlo 结合最大公因子方法和统计方法，对 R-NSS 作了有效的攻击。2003 年设计者提出较有影响的 NTRUSign 数字签名体制[17]，该算法较前面两个方案做了很大的改进，在签名过程中增加了对消息的扰动，大大减少签名中对私钥信息的泄露，但却极大地降低了签名的效率，且密钥生成过于复杂。针对未加扰动的 NTRUSign 方案的缺陷，2008 年胡予濮提出了一种新的 NTRU 签名方案。但这些签名方案都不是零知识的，也就是说，签名值会泄露私钥的相关信息。

另外，2009 年，Gentry 首次提出了基于格的全同态加密方案[18]，再一次掀起了格密码的研究热潮，在此之后，在格的数学基础、格上数学问题以及格密码设计方面涌现出一批研究成果，包括基于格的零知识证明、格公钥加密/签名方案、以及密钥交换协议等，这些研究进展可以参见格密码综述文章[19-21]。

2015 年美国国家标准技术研究所（NIST），发布了 PQC 密码报告，并开始在全球范围内公开征集 PQC 密码算法标准，这项工作极大推动了 PQC 密码的研究工作，其中格密码被认为是最有力的竞争者。目前，NIST 的 PQC 密码标准候选算法中格密码占主导地位，因此，格密码值得我们进一步深入研究。

2. 基于编码理论的密码

纠错编码公钥密码体制可理解为：把纠错的方法作为私钥，加密时对明文进行纠错编码并主动加入一定数量的错误，解密时运用私钥纠正错误，恢复出明文。1978 年 McEliece 利用 Goppa 码有快速译码算法的特点，提出了第一个基于纠错编码的 McEliece 公钥密码体制[22]。1978 年，Berlekamp 等人证明了任意线性码的译码问题是 NP 完全问题[23]。McEliece 密码方案的原始版本经受了 40 多年来的广泛密码分析，被认为是目前安全性最高的公钥密码体制之一。Gibson 证明了加密变换中存在多个等价陷门，任何一个陷门都可用于解密，但要找到其中一个在计算上是不可行的[24]。虽然 McEliece 公钥密码的安全性高且加解密运算比较快，但该方案也有它的弱点，其一是

它的公钥尺寸太大，其二是信息扩展了多倍。由于这些原因，该方案一直以来并没有引起人们太多的关注。

1986 年 Niederreiter 提出了另一个基于纠错码的公钥密码体制[25]。与 McEliece 公钥不同的是它隐藏的是 Goppa 码的校验矩阵。我国学者李元兴、王新梅等在 1994 年证明了 Niederreiter 公钥与 McEliece 公钥密码体制在安全性上是等价的[26]。当然，也可采用其它具有快速译码算法的线性分组码如 BCH 码、RS 码等来构造公钥密码体制，但其安全性要比采用 Goppa 码低，主要原因是同一参数的其它码的数量要比 Goppa 码少。2009 年 Misoczki 等针对 McEliece 体制密钥量大的弱点，提出了一种改进方案[27]，但该方案被 Faugere 等在 2010 年欧密会上利用代数攻击攻破[28]。

与其它公钥密码体制(如 RSA 等)不同，McEliece 公钥以及 Niederreiter 公钥密码只能用于加密，但却不具备数字签名功能，其原由是，用 hash 算法所提取的待签消息摘要一般来说都不在给定的码空间中，从而导致解码失败。1990 年王新梅提出了第一个基于纠错编码的数字签名方案－Xinmei 方案[29]。1992 年 Harn 等对 Xinmei 方案进行了攻击和改进。Alabhadi 和 Wieker 于 1992 年提出了另一种攻击方法，其选择明文攻击的复杂度较低，这种攻击方法对 Harn 的改进方案同样有效，为了抵抗这种攻击，他们于 1993 年又提出了 AW 方案。2000 年王新梅对原始 Xinmei 方案进行了修正，得到了比 AW 方案更为简单的修正 Xinmei 方案。我国学者张振峰、冯登国和戴宗铎于 2003 年对 AW 方案进行有效的分析，仅利用公钥便能构造出等价

的私钥，并指出利用大矩阵分解的困难性很难构造出安全性较高的数字签名体制[30]。除此之外，1991 年李元兴等构造了一类同时具有签名、加密和纠错能力的公钥体制。目前，国际上公认安全的纠错码签名方案是 2001 年 Courtois 等人提出的 CFS 签名方案[31]，除了密钥量大的缺点外，该方案的签名效率较低。因此，如何用纠错码构造一个安全高效具有纠错能力的签名体制、以及既能加密又具有签名功能的密码体制，是一个相当困难但却非常有价值的开放课题。

3. 基于哈希函数的密码

基于 hash 的数字签名(主要指 Merkle 签名方案)源于一次签名方案(OTS)。1978 年 Rabin 首次提出了一次签名方案，该方案验证签名需要时需要与签名者交互。次年，Lamport 提出了一个更为有效的一次签名方案，它不要求与签名者交互；Diffie 将其推广，建议用 Hash 函数替代基于数学难题的单向函数以提高该机制的效率，因此，常称之为 Lamport-Diffie 一次签名方案(LD-OTS)。随后，又相继出现了一些改进方案，如 Bos-Chaum 方案、Winternitz 方案等。大多数一次签名方案具有签名生成和验证高效的优点。一次签名方案可应用在某些特殊环境比如芯片卡中，它们具有较低的计算复杂度。

在一次签名方案中，每个密钥对仅能签署一条消息；否则签名将以很高的概率暴露更多的私钥信息，因此很容易伪造针对新消息的签名。每次签署消息都需更新公钥，这相当于“一次一密”，虽然具有

较高的安全性，但却缺乏实用性。当一次签名与认证技术结合时，多次签名就成为可能。

1989年Merkle提出了Merkle认证树签名方案(MSS)[32]。Merkle数字签名方案中，没有太多的理论假设，它的安全性仅仅依赖于hash函数的安全性，目前在量子计算机模型下还没有一般hash函数的有效攻击方法，因此，Merkle签名方案具有抗量子计算性质。与基于数学困难性问题的公钥密码相比，Merkle 签名方案不需要构造单向陷门函数，给定一个单向函数(通常采用 hash 函数)便能构造一个Merkle签名方案，一般来说，在密码学上构造一个单向函数要比构造一个单向陷门函数容易的多，因为设计单向函数不必考虑隐藏求逆的思路，从而可以不受限制地运用置换、迭代、循环、反馈等简单编码技巧的巧妙组合，以简单的计算机指令或廉价的逻辑电路实现高度复杂的数学效果。

Merkle 数字签名方案的优点是签名和验证签名效率较高；缺点是签名和密钥较长，产生密钥的代价较大。在最初的Merkle签名方案中，需要签名的数量与需要构造的二叉树紧密相关，能够签名的数量越大，所需要构造的二叉树越大，同时消耗的时间和空间代价也就越大。因此该方案的签名数量是受限制的。近年来，许多学者对此作了广泛的研究，提出了一些修改方案大大地增加了签名的数量，如CMSS方案、GMSS方案、DMSS方案等[33-35]。Buchmann, Dahmen等提出了XOR树算法[36]，只需要采用抗原像攻击和抗第二原像攻击的hash函数，便能构造出安全的签名方案。而在以往的Merkle树签名

方案中，要求 hash 函数必须是抗强碰撞的。这是对原始 Merkle 签名方案的有益改进。上述这些成果，在理论上已相当完善，在技术上已基本满足工程应用要求，一些成果已经应用到了 Microsoft OutLook 以及移动代理路由协议中。

目前，基于 hash 的数字签名的研究仍处于初步阶段，仍有许多开放性课题如增加签名的次数、减小签名和密钥的尺寸、优化认证树的遍历方案以及实现相比其它公钥体制所不具备的功能(如基于身份的认证)等。

4. 多变量密码

多变量二次多项式公钥密码体制，简称 MQ 公钥密码，其安全性基于有限域上的多变量二次方程组的难解性。如何构造具有良好密码性质的非线性可逆变换是 MQ 公钥密码设计的核心，据此划分，目前基于多变量的公钥密码体制主要有：Matsumoto-Imai 体制、隐藏域方程(HFE)体制、不平衡油醋(UOV)体制及三角形(TTS)体制。

1988 年 Matsumoto 和 Imai 运用“大域-小域”的原理设计了第一个 MQ 方案，即著名的 MI 算法[37]，当时该方案受到了日本政府的高度重视，被确定为日本密码标准的候选方案。1995 年 Patarin 利用线性化方程方法成功攻破了原始的 MI 算法[38]。然而，这个体制是多变量公钥密码发展的一个里程碑，为该领域带来了一种全新的设计思想，并且得到了广泛地研究和推广。改进的 MI 算法实例如 SFLASH 签名体制[39]，最终在 2003 年被 NESSIE 项目收录，用于低廉智能卡

的标准算法，该标准签名算法在 2007 年美密会上被 Fouque、Granboulan 和 Stern 彻底攻破[40]。此外，2009 年 Clough 等提出了奇特征域上 SQUARE 方案[41]，它本质上也是 MI 算法的变种，2009 年亚密会上 Billet 等人成功攻破了该方案。

1996 年 Patarin 针对 MI 算法的弱点提出了隐藏域方程 HFE 方案[42]。HFE 可看作为是对 MI 的实质性改进。2003 年 Faugere 利用 F5 算法成功破解 HFE 体制的 Challenge-1。该体制主要有两种改进算法，一是 HFEv-体制，它是结合了醋变量方法和减方法改进而成，特殊参数化 HFEv-体制的 Quartz 签名算法，也是 NESSIE 工程的候选算法，因为效率等原因落败于 SFLASH 算法；二是 IPHFE 体制，这是丁津泰等人结合内部扰动方法对 HFE 的本质改进。这两种多变量体制至今还未发现有效的攻击方法。

油醋(Oil-Vinegar)体制是 Patarin 在 1997 年利用线性化方程的原理，构造的一种 MQ 公钥密码体制。产生签名时需解一个关于油变量的线性方程组。油醋签名体制主要分为三类：1997 年 Patarin 提出的平衡油醋(Oil-Vinegar)体制，1999 年欧密会上 Kipnis、Patarin 和 Goubin 提出的不平衡油醋(Unbalanced Oil and Vinegar)体制[43]以及丁津泰在 ACNS2005 会议上提出的彩虹(Rainbow)体制[44]。平衡油醋体制中，油变量和醋变量的个数相等。但平衡油醋体制并不安全，1998 年 Kipnis 和 Shamir 利用二次型矩阵方法有效地构造出与原私钥等价的密钥。不平衡油醋体制中，醋变量的个数大于油变量的个数，即使不使用线性变换，UOV 也具有非常可靠的最低安全性。彩虹体制

是一种多层的油醋体制，即每一层都是油醋多项式，而且该层的所有变量都是下一层的醋变量，它也是目前被认为是相对安全的多变量公钥密码之一。

三角形体制是现有多变量公钥密码体制中较为特殊的一类，它的签名效率比 MI 和 HFE 还快，而且均是在较小的有限域上进行。这种构造的源头可以追溯到 Fell 和 Diffie 的工作，不过他们并没有找到高效而安全的三角形体制。Shamir 在 1993 年提出的双有理结构在一定程度上也属于三角形体制。1999 年 T.T.Moh 基于 Tame 变换提出了 TTM 密码体制，并在美国申请了专利，丁津泰等人指出当时所有的 TTM 实例均满足线性化方程，T.T.Moh 等随后又提出了一个新的 TTM 实例，这个新的实例被胡磊、聂旭云等人利用高阶线性化方程成功攻破[45]，目前，还没有安全的 TTM 实例。T.T.Moh 等引入了锁多项式(lock polynomials)来隐藏中心映射中的线性多项式，以避免线性化方程攻击，既便如此，单独使用这种顺序解映射仍是不安全的，目前三角形体制的设计主要是围绕锁多项式的构造、结合其它增强多变量密码安全性的方法如加减(plus-minus)模式以及其它的代数结构如有理映射等。目前相对安全的三角形体制主要有 TTS、TRMS、Rainbow 等，但这些体制的安全性分析仍旧是一个开放问题。

MQ 公钥密码的安全性是基于有限域上多变量多项式方程组的求解问题，即 MQ 问题。1979 年 Micheal、Garey 和 Johnson 证明了 *GF(2)* 上的 MQ 问题是 NP 完全问题，1997 年 Patarin 和 Goubin 证明了任意域上的 MQ 问题也是 NP 完全问题。同时，为构造单向陷门函数，还需

利用多项式同构问题，即 IP 问题。1996 年 Patarin 证明了 IP 问题也是 NP 完全问题。确切地说，目前还没有一种公认安全的 MQ 公钥密码体制。实践证明，MQ 问题、IP 问题的难解性并不能完全保证 MQ 密码算法的安全性。在分析 MQ 公钥密码时，往往并不是直接解公钥方程来恢复明文或是从公钥中求解陷门，而是根据其内部构造结构中蕴含的特殊代数性质，以寻求明密文之间的关系或构造同解方程来伪造签名。目前多变量公钥密码的主要缺点是：只能签名，不能加密(加密时安全性降低)；公钥较长；很难设计出既安全又高效的多变量公钥密码体制。MQ 公钥密码领域中的一些亟待解决的开放性问题主要有：(1) 寻找有限域上具有良好密码性质的可逆二次多元多项式，用于构造多变量公钥密码的中心映射，这也是设计 MQ 公钥密码的核心；(2) 寻找新的结构用于构造多变量公钥密码的单向陷门函数，近年来，各种有效的多变量攻击方法显示，IP 问题的困难性并不能很好地保证陷门的安全；(3) 研究有限域上非线性代数方程组的求解技术，目前求解 MQ 问题的算法如 F4/F5 算法、XL 算法等，其效率仍然比较低；(4) 寻找新的用于增强多变量公钥密码的安全模式，如减方法“-”以及丁津泰近年提出的内部扰动方法等；(5) 将 MQ 问题与其它问题组合起来建立可证明安全的公钥密码体制；(6) 构造特殊应用需求的多变量密码体制，以用于低廉智能卡、无线传感器、RFID 等；(7)与基于纠错码的公钥密码一样，MQ 公钥密码也存在等价密钥问题。

5. 后量子密码小结

上述 PQC 算法之所以被视作抗量子计算攻击的，主要是由于其基于的困难性问题尚未找到高效的量子算法。以基于格密码问题为例，目前格密码可以基于底层的最坏意义的格困难问题，这些问题已经被数学家研究了几十甚至上百年，主流的看法是这些问题不存在高效的（多项式时间的)解法，因此是困难问题。目前针对 PQC 算法的攻击，也主要是经典算法攻击，如格密码（包括理想格）的三类攻击（Primal 攻击、代数攻击、BKW 算法）和基于对 LPN 问题的 BKW 算法，量子算法相对于经典算法在解决这类问题上并不具有太多优势（加速局限于多项式范围内）。其它方面，各 PQC 算法在密钥长度、运算速度和功能完善性上的粗略比较如表 2-1 所示。

表 2-1 PQC 算法定性比较

密码类型	公钥大小	计算速度	功能多样性
格密码	小	快	很好
基于编码理论的密码	较小	较快	好
多变量密码	大	较快	较好
基于哈希函数的密码	大	较快	有限

PQC 能提供具有量子安全特性的各类应用解决方案，其优势在于在密码领域内经过了较长时间的理论研究，处于算法的标准化研究阶段，安全性上预期能够抵御已知的量子攻击，由于其物理实现兼容于现有信息技术和工艺的优点，较 QKD 和量子密码来说，更易于集成化、

芯片化、小型化、低成本。但由于 PQC 在密钥长度、算法构造等方面与现有密码存在的差异较多，与应用系统的接口也相比 QKD 来讲更多，从现有公钥算法迁移到 PQC 算法的过程是一个复杂和漫长的过程；另一方面用户也在等待 PQC 算法的标准化，算法标准化将很大程度上促进 PQC 的推广使用。以发展的眼光看，PQC 依赖的数学难题未来是否依然难解，算法安全性是否长期有效仍是一个开放的问题；新类型 PQC 算法的发现，乃至提升 PQC 系统的实际安全性等，还需要研究者持续不断的深入研究。

（二）基于量子物理的密码技术

量子物理带来的传统密码学安全风险，也可以在量子物理中找到解决办法。单量子不可分割、不可克隆、测不准和量子纠缠等量子特性，为实现免疫计算破解的信息论安全的密码协议提供了可行性。

1. 量子密钥分发

量子密钥分发是指以量子为信息载体进行远程密钥分发。其中处理量子的手段主要有两大类：一类是对单量子进行编码、传输和解码测量，另一类是对量子纠缠进行分发、提纯和探测。两类手段相比，前者可以看作是对后者纠缠中的一个量子先进行了测量，而对剩下的一个量子进行传输和解码测量，因此两者在理论模型上具有等效性。单量子的不可分割、不可复制和测不准特性，使得任何来自于信道的窃听，要么导致量子信号丢失，要么导致量子信号发生可观测的变化，

因此量子密钥分发双方可以根据双方的有效结果进行安全密钥提炼。即便窃听者控制了传输信道，只要窃听者没有掌握能攻入双方设备内部的侧信道，量子密钥分发依然可以实现双方共享安全的密钥。学术界将这种安全性称之为“信息理论安全”。

值得注意的是，两类量子密钥分发手段都需要通过经典协商才能完整地实现密钥分发，主要的原因是量子测量的结果具有随机性而密钥应当是确定和一致的。量子测量的随机性包括制备和测量基矢选择的随机性、单量子成功探测的随机性等，这种随机性使得一方面密钥分发的双方必须筛选出一致的制备测量基矢，另一方面密钥分发的双方并不会提前预知最终产生的量子密钥。

量子密钥分发技术自提出至今已有 30 余年，第一个量子密钥分发方案是由查尔斯·贝内特（Charles Bennett）与吉勒·布拉萨（Gilles Brassard）于 1984 年提出的 BB84 协议，其后学者们也提出了多种不同的协议，不断地改进编解码的易实现性、效率、抗干扰和安全性等能力。量子密钥分发协议可以细分为多种方案：根据承载编码的量子态（物理量）来区分，量子密钥分发方案包括离散变量和连续变量两类，其中离散变量常用偏振、相位、时间位等；根据具体的编码和解码探测方式来区分，量子密钥分发方案包括 BB84 及诱骗态 BB84、分布式相位参考（DPR）、测量设备无关（MDI）和设备无关（DI）协议等。主要协议的分类说明如下表所示。其中离散变量方案中的诱骗态 BB84 协议是安全论证成熟、应用最广泛的协议，基于该协议的光纤量子密钥分发设备已经较大规模商用，可以达到百公里每

秒分发约 10kb 密钥的能力；测量设备无关方案是一种基于纠缠反演思想新提出的方案，在安全性方面不受测量设备物理缺陷的影响，同时还有助于提高密钥安全分发的总距离，目前光纤量子密钥分发最远距离的纪录就是由该类协议实现，其中基于独立相干光源实现的双场协议和相位匹配协议均已经突破 500 公里[46],[47]。

量子密钥分发实现了直连光纤/空间链路上的密钥分发，结合光纤链路切换、密钥交换等手段可以实现路由和距离拓展，从而组建各种拓扑、规模的量子密钥分发网络，为网络中各用户端点提供的双方共享或多方共享的安全密钥。这种分发密钥的功能可以和经典通信网络有效融合，利用对称加密技术为数据链路层、网络层、传输层、应用层等提供保密传输支撑。

表 2-2 量子密钥分发协议

类型	编码和探测方式	协议（年代）
离散变量	发送端编码时，对单光子或者弱光脉冲的偏振、时间、相位等自由度进行离散调制；接收端用单光子探测器对单光子进行探测。	BB84（1984）[48] E91（1991）[49] B92、BBM92（1992）[50] 六态协议（1998）[51] SARG04（2004）[52] Decoy BB84（2005）[53，54]
连续变量	发送端编码时，对弱光脉冲的两个正交分量进行连续调制；接收端用平衡探测器对光脉冲进行探测。	GG02（2002）[55]

类型	编码和探测方式	协议（年代）
分布式相位参考	发送端编码时，对弱光脉冲的时间模式和相邻时间模式之间的相位自由度进行离散调制；接收端用单光子探测器对弱光脉冲进行探测。	DPS（2002）[56] COW（2005）[57] RRDPS（2014）[58]
测量设备无关	两个异地光源以相干的方式向中间探测节点发送光信号，既可以是离散变量也可以是连续变量，中间探测节点进行纠缠检测。	MDI-QKD（2012）[59] PM-QKD（2018）[60] TF-QKD（2018）[61]

量子密钥的对称属性，也决定了其应用限于对称密码的范畴，无法直接结合非对称体制密码的应用诸如广泛使用的基于公钥的“数字签名”，因此发展量子版本的数字签名等技术需要另辟蹊径。

2. 量子随机数发生器

量子随机数发生器利用量子力学过程产生随机数。相比于传统的伪随机数发生器方案，量子随机数发生器并不依赖于复杂的数学问题，因此随机数的安全性具备信息论意义的安全性。这意味着掌握无限计算能力的攻击者都无法预测产生的随机数。另一方面，相比于基于传统物理噪声的随机数发生器，量子随机数发生器对熵源的建模和估计更加精细准确，最大限度地保证信息熵来源于较为可靠的量子力学随机性。

根据不同的量子力学原理，可以设计出各种不同的量子随机数发生器方案。量子随机数发生器早在二十世纪五六年代开始有人研究。近年来，量子随机数发生器的速率快速提升，达到 GHz 量级，并在低成本，小型化，芯片化方面取得重要突破。与此同时，人们提出了设

备无关和半设备无关的量子随机数发生器方案，用于一劳永逸地解决实际设备缺陷引发的侧信道安全问题。在不久的将来，量子随机数发生器有望应用于信息技术的各个方面。

3. 量子数字签名

目前广泛使用的数字签名是基于公钥的，其安全性的基础是大数分解等数学问题的复杂性假设，因此它是计算安全，而不是信息理论安全的。尤其是，我们已知量子计算机可以破解目前基于大数分解和离散对数问题的数字签名算法。因此，人们开始研究更为安全的替代方案，特别是信息理论安全的数字签名方案。原理上来说，基于经典手段也可以设计信息理论安全的数字签名方案，但它们都依赖于一些不易实现的假设，例如需要难以完全追溯的认证广播信道和认证私密信道[62]，或者需要安全可信的第三方[63]。量子数字签名（QDS）可以不依赖于这些额外假设的资源而提供信息理论安全的安全性，因此受到了广泛的关注和研究。

第一个量子数字签名方案于 2001 年提出[64]，其原理是利用 n 个量子比特可以构成 2^n 个量子态，因此将一个 n 量子比特态的多个拷贝作为公钥而制备方法作为私钥时，根据量子态的有限个拷贝（公钥）并不能推导出该量子态的完整构成（私钥），当公布制备方法时却可以验证，从而构成了信息论安全的签名方案。该方案依赖于对光脉冲的非破坏性测量、长时间量子存储等尚未实现的技术，因此不具备实用性。随后，人们提出了一系列改进方案，不断增强量子数字签

名方案的实用性，其中最具有实用意义的是基于量子密钥分发过程实现的量子数字签名[65]，其原理是当发送方编码发出一个量子比特序列（作为公钥）但不透露编码基矢（作为私钥），接收方根据自己的测量结果并不能反推出该序列，但公布编码方案时又可以验证该序列是否可以产生该测量结果，从而实现了数字签名。2017 年，中科大团队[66]和英国东芝剑桥实验室团队[67]分别完成了测量设备无关的量子数字签名实验，标志着该技术的实用化进程推进了一大步。这两个实验均采用了一种将测量设备无关量子密钥分发技术与经典通信协议结合的方案。方案可行性相对较高，技术成熟度几乎等同于测量设备无关的量子密钥分发网络。由于量子数字签名涉及多方通信，因此其实用化依赖于未来较大规模量子通信网络基础设施的构建。

4. 量子密码与量子密钥分发小结

量子密码学源于它独特的基于量子物理提供的安全基础，为构建量子安全的密码开辟了一条新的道路。QKD 只是量子密码科技当前发展最为成熟、最为人所熟知的一个分支。除了数字签名外，研究者也已经提出了一系列实现秘密共享、多方安全计算等各种功能的量子安全协议。随着量子器件、量子设备以及量子安全协议的研究取得进展，以发展的眼光看，量子密码将不只能够承担密钥分发的任务，而且能够实现可认证性、保护隐私性，例如基于量子数字签名实现认证，基于量子隐形传态实现数据安全传输等功能。

QKD 当前只解决安全分发密钥的难题，但大规模的、安全的密钥分发从来就是密码学的重要任务和挑战。而且 QKD 能够与现有密码系统、密码协议及应用系统更直接的以模块化方式结合，实现“即插即用”，这方面相较 PQC 具备一定的优势。在增强 QKD 的适用性和实用性，以及丰富应用场景方面，我国通过多年的科学实验和工程项目进行了验证，积累了大量工程和实用经验。

QKD 嵌入各类密码系统的集成和改造方案日臻成熟，但需要增配量子密码硬件设备，量子设备的工程技术实现难度还较大、成本较高；而且，量子器件及设备制造工艺的不完美会对 QKD 设备的安全性带来影响，需要针对 QKD 设备实际安全性的研究形成相关的标准和规范，甚至是新的 QKD 实现方案。此外，QKD 系统需要与经典系统结合应用，诸如可信节点等环节的安全性影响除了通过标准化和规范设计来解决，还需要 QKD 系统在成码距离和成码率等方面性能的持续提升。从长期安全性上考虑，全量子化的密码系统具备最强的抗量子攻击能力。

三、量子安全技术应用

量子安全是新一代密码技术应具备的主要特性之一，PQC 和 QKD，是转换到量子安全的必要工具。基于数学原理的 PQC 与基于物理原理的 QKD 看似有着一定的竞争关系，其实有着不同的发展路径，面向不同的应用场景，还可以合作搭配、互为增长。

本章结合国内外研发与应用情况，针对重要应用场景，在阐述网络信息系统面临的量子计算攻击风险的同时，从技术架构和行业领域应用两个维度分别对一系列典型和示例性应用场景中的量子安全技术应用场景与需求进行分析和探讨。

（一）量子安全应用方案

1. 后量子密码应用方案

总体上看,后量子密码应用方案能获得大规模推广的前置条件是需要 PQC 各类算法实现标准化和工程化，以及建设形成基于 PQC 的密码基础设施。PQC 能为用户提供灵活性较高的各类解决方案，以软件形式为主，如适用于各类如安全网站浏览、物联网等不依赖于专用硬件设备、便于软件升级的轻量级应用场景；当然也可以形成硬件解决方案。以下细化讨论 PQC 应用方案，先明确 PQC 与传统密码功能的对

应关系,再依据 PQC 在 ICT 系统各类常用密码协议的应用场景分开进行讨论。

1.1 后量子密码与传统密码的功能对应关系

后量子密码 PQC 按照基于的困难性假设分类，主要可以分为基于格的密码、基于编码理论的密码、基于哈希函数的密码、多变量密码等几类。PQC 具备传统密码的几乎所有功能，除了例如基于格的单向置换等少数特例，大部分关键的传统密码原语（如非交互零知识证明、抗碰撞哈希函数、公钥加密方案等）都有对应的后量子版本，而且后量子密码可以实现对应传统密码算法如 RSA、DH 不具备的功能（如全同态加密）。后量子密码中的格密码基于格上困难问题，对其安全假设的研究充分，功能多样，为主流的技术路线；基于编码的方案的困难性假设则是基于纠错编码问题，相对也比较成熟；基于哈希函数的后量子密码功能比较受限，目前主要用于构造后量子安全的数字签名方案；还存在其它方案，如基于超奇异椭圆曲线的 PQC 方案，用于构建后量子安全的 DH 密钥交换等。以下从传统密码功能及 PQC 支持实现的密码学新功能的维度进行分类阐述。

（1）传统密码方案的后量子安全版本:主要是传统密码方案的后量子版本，包括公钥加密/签名、哈希函数、零知识证明等。这些后量子版本的方案功能完善，理论上可以替代传统密码方案，实际应用中也可以满足现实需求，根据需求可以选择不同程度的后量子安全模型（标准模型、QROM 等）。

（2）全同态加密：全同态加密主要基于格的后量子密码方案，被称为密码学的圣杯。从现实可行的全同态加密方案来看，格密码是唯一成熟的候选方案，目前较直接和实际的应用场景是外包计算，例如隐私保护的机器学习。

（3）基于格的多方安全计算相关技术：多方安全计算的核心组件秘密分享的后量子版本是完全可以构造出的，因此功能性上，PQC下的多方安全计算是完全可行的，但是相比传统密码体制外，PQC 密码有如下几个值得注意的点：

a. 基于格可以构造出同态秘密分享。该部件可以用于构造新的多方安全计算协议，例如两轮交互多方安全计算协议。

b. 可以通过同态加密来进行安全多方计算，从而将通信轮数降到极低。

（4）功能加密(FE)和基于属性加密（ABE）的方案也可以基于格来构造。

1.2 基于后量子密码的常用密码协议改造方案

密码协议均是基于密码学原语构造的，因此基于PQC的密码学原语可构造量子安全的密码协议。而由于密码学原语的改变、算法原理不同、流程不同，乃至一些PQC算法与对应的传统密码算法在参数上就不兼容，必然导致密码协议需要做相应的改变，根据协议和更换算法的不同，改造方案差异很大。有的协议可以平滑的过渡升级，能够完全做到不改动现有协议格式与流程；有的需要升级协

议，改动协议的基本数据结构；有的涉及对传统密码基础设施如CA和使用协议的应用系统进行升级改造。对于密码系统开发者和用户，有必要在此进一步细化讨论，以下（1）—（5）内容参考了[6]。

（1）X.509 格式的数字证书相关应用：

用于 web 浏览安全认证所用的 SSL/TLS 网络安全协议，S/MIME 安全邮件协议，Web Service 架构使用的 XML 文件数字签名包括代码签名等都是基于 X.509v3 格式的数字证书实现的。证书由可信第三方证书认证中心（CA）颁发，证书中含有签名、公钥等多个与算法相关的敏感字段。当前商用 CA 颁发的证书还没有使用后量子算法，从证书结构上,X.509v3 格式是能兼容量子安全密码的,不需要更改标准，其规定的对象标识 OID 域较灵活，支持自定义 PQC 类的新算法标识。引入 PQC 算法后，需要修改读取证书的应用系统，让应用能根据新的算法标识验证签名。因此，迁移到量子安全不仅是 CA 业界需要考虑的，同时也是 IT 业界需要考虑的问题。迁移还应区分考虑是长生命周期的证书还是短生命周期的证书：对于前者为证书安全考虑更需要尽早迁移到使用量子安全的算法和相应标识；对于后者如果能预期在实现量子计算破解之前证书就已经失效的话，没有必要进行升级。X.509 证书的数据格式能够存储很长长度的公钥，所以对公钥长度较长的 PQC 算法不存在证书格式不兼容的问题，但是应用开发商则需要考虑相应的改动升级，防止在源代码中对证书长度进行了限制。

（2）IKEv2 协议：

IKEv2 协议用于建立 VPN 通道时认证安全对端(SA)和协商密钥，现在其使用的密码算法种类很有限，也都不是量子安全的。由于 IKEv2 协议的应用场景中其保护的网络传输敏感数据可能被敌手所截获保存用于以后通过量子计算进行破解，所以 IKEv2 协议应具备量子安全特性以抵御这类攻击。该协议典型流程需经过三次握手交互，第一次交互时使用了 DH 密钥交换算法生成一对工作密钥，第二次交互时双方会使用证书或预先分发的认证密钥对此工作密钥进行验证，第三次交互时使用 DH 算法再次生成一对新的加密/认证 IP 包数据使用的工作密钥。IKEv2 协议没有 DH 算法的替代算法，由于 DH 算法不是量子安全的，所以需使用预先分发的认证密钥方式才可能做到量子安全。

IKE 协议设计理念上力争达到完美的前向安全性，即每次建立新的安全连接都是基于新生成的、只使用一次的密钥。并且 IKE 协议每次连接都是可认证的，认证基于 RSA、DSS 或 MAC（MAC 会使用预先分发的密钥）算法实现，一般认为拥有合适的密钥长度和 MAC 值长度的 MAC 算法是量子安全的，而 RSA、DSS 算法不是量子安全的，但这里使用 MAC 算法存在不足之处：一方面在大规模网络中预分发密钥工作量大、需分发密钥数量大、速度慢会导致密钥管理变得复杂，另一方面全网共享密钥随着网络规模增大、泄露的安全风险也增大了，容易导致单点失败。因此 IKE 协议必须进行修改才能实现量子安全，修改方案包含以下两部分：

1）在第一步和第三步交互中不使用 DH 算法而是替换为使用新的能达到速度指标要求的量子安全算法，学术界研究者据此提出了几种算法替换方案，但目前还没有出现一种被业内普遍认可的新算法。

2）第二步交互中替换目前使用的 RSA 或 DSS 认证算法为量子安全的新算法，这样就可以消除上文所述的使用 MAC 认证算法存在的不足之处。

（3）TLSv1.2 协议：

TLSv1.2 协议是原 SSL 协议的更新版本，用以在服务器和客户端间建立保护应用数据包的安全通道。TLS 协议应用非常广泛，包括 Web 浏览、FTP 文件下载、SMTP 协议的电子邮件等，其握手子协议用于实现服务器对客户端的认证（也可用于实现反向认证），还用于生成两端间共享密钥，该共享密钥后续会用于应用数据的加密与认证。握手子协议使用 RSA 公钥密码算法和 X.509 证书，这个过程不是量子安全的。TLS 协议的实现不依赖于特定密码算法，它允许双方协商要使用的密码功能套件也就是要使用密码算法的集合，当然双方需具备同样的密码功能套件才可能达成协商一致。密码功能套件使用 DH 算法以实现前向安全性，套件中也包含对称密码等非公钥密码，一般认为 Grover 算法的搜索能力对暴力破解这些非公钥算法是有效的，这些非公钥算法需要扩展到之前密钥长度的二倍才能抵御量子攻击。

因此，TLSv1.2 协议标准必须进行修改才能实现量子安全，TLSv1.2 协议的握手子协议和密码功能套件中需改造的两个流程以及修改方案如下：

1）客户端生成随机密钥时，使用服务器的公钥对其进行加密，将密文发送给服务器,服务器用私钥解密获得随机密钥,这个基于RSA加密的密钥传输过程不是前向安全的，如果服务器私钥泄露，则所有随机密钥都会泄露。修改方案可以分两步，为尽量减少修改工作量，短期阶段内可以仍使用RSA算法,但将密钥生成过程替换为具备前向安全性的过程，并扩展对称密码密钥长度以抵御量子攻击，这种“混合”的密钥生成方式结合抗量子攻击的密钥生成过程和不抗量子攻击的签名认证过程，但由于它具备前向安全性，仍然可以抵御未来的量子攻击。第二步再用抗量子攻击的公钥签名算法替换现用完成认证功能的公钥算法。

2）服务器和客户端使用DH算法协商生成临时公私钥对，再用临时公私钥通过双方交互生成共享密钥,对临时公私钥对的认证是基于数字证书完成的。这整个过程是具备完善的前向安全性的，但TLS密码功能套件中提供的传统 DH 算法或基于椭圆曲线的 DH 算法都不是量子安全的。改进方案仍然可以分两步走完成,在短期内使用“混合”模式,即混合使用抗量子攻击的密钥协商算法和不抗量子攻击的密钥协商算法（如椭圆曲线 DH 算法），这种混合模式可以使用户密码系统达到量子安全标准的同时让用户能继续利用现有密码组件提供的安全基础，符合现有的例如FIPS这样的安全标准规范要求。

对该协议的修改方案仍处在学术研究阶段,产生了若干个基于量子安全密码学原语的密钥交换协议,研究表明量子安全的TLS协议在运行效率上能达到与基于椭圆曲线的密码功能套件相近似。

需要注意如果采用公钥及签名值长度较长的 PQC 算法可能需要对该协议做更多的修改:例如 TLS 数据分块的最大长度限制是 16KB，证书最大长度是 16MB，这种最大长度未来可能就需要增大。

（4）S/MIME 安全电子邮件协议

S/MIME 安全电子邮件协议基于公钥签名和加密算法实现安全的收发电子邮件。S/MIME 协议以及类似的 OpenPGP 电子邮件系统都实现了从邮件自发送者到接收者的全过程包括在发送者及接收者的电子邮件服务器上都是加密的。相比较，基于 TLS 的 SMTP 协议和基于 TLS 的 IMAP/POP3 协议就只是保护了电子邮件服务器之间邮件传输的安全而没有做到端到端的机密性与完整性保护。S/MIME 和 OpenPGP 在协议层面很相似，差别在于 S/MIME 依赖数字证书和 PKI 基础设施完成密钥分发，邮件接收者都必须持有合法证书才能接收邮件；而 OpenPGP 依赖于各参与节点都需要是可信赖的。因此 S/MIME 更为政务和商务 IT 系统所应用，这些大型机构的用户都会拥有合法证书。

在 S/MIMEv3.2 安全电子邮件协议中使用最低 1024 位长度的公钥签名算法保证邮件递送的保密性、完整性、抗伪造性。使用的具体算法是 DSA、RSA、RSA-PSS 三者之一（配套使用的摘要算法均为 SHA-256），SHA-256 算法是量子安全的，公钥算法就需要进行替换以实现量子安全性。S/MIME 协议使用的对称加密算法如 AES 可以认为是量子安全的，但预先生成对称加密所使需工作密钥的算法不是量子安全的，也需要替换。S/MIME 协议设计上也支持升级签名算法或扩展密钥长度。

S/MIME 协议实现的是称为 CMS(Cryptographic Message Syntax)的数据保护封装格式，算法、密钥这些安全参数也是依据 CMS 封装作为 CMS 的一部分。CMS 允许自定义算法参数，称为 S/MIME 能力属性的数据定义了签名算法、邮件内容加密、密钥加密所使用的算法种类，它是灵活可扩展的，新增加自定义的算法种类不影响原有算法的使用。不同版本的 S/MIME 实现应遵循的互操作性规范都定义在了 CMS 文档里，其中规定如果 S/MIME 协议在基于弱密码算法运行时就应该为用户生成警告信息，在 S/MIME 协议格式中定义了一个相应标识参数，应用代理基于此参数判断是否在使用弱密码算法，从而提示用户。可以利用此参数标识算法是否是量子安全的。但要注意，S/MIMEv3.1 协议及更早版本的协议会存在后向互操作兼容性问题，基于这种老版本协议实现的应用可能只包含了 RSA 算法从而无法达到量子安全要求。老版本协议格式存储的密钥长度有限，也不支持扩展的密钥长度，从而会出现基于老版本协议实现的客户程序与扩展成量子安全算法的新版本程序无法正常通信的情况，除非双方都使用老版本协议能识别的弱密码算法。

（5）SSHv2 协议

SSH 协议广泛的应用于在互联网等广域通用网络上安全的传输信息，它基于客户端—服务器应用模式设计，最初为远程安全登录目的设计，后来随着功能的完善适用于用户登录、发送命令、传输文件等各类不同应用场景。例如，基于此协议实现的 OpenSSH 能够为用户建立完善的加密 VPN 访问通道，SSH 还能用于构建成本低廉的 WLAN 局

域网，构建客户与云服务间的安全连接等各类需要远端客户安全访问服务端的场景中。

SSH 协议由三个子协议构成：传输层协议、用户认证协议、连接协议。这三个子协议运行于不同网络协议层，可以独立的使用各种密码算法。传输层协议为服务端认证客户端构建安全通道，保护所传输数据的机密性和完整性。它运行于 TCP/IP 协议之上，负责产生此次会话的唯一性标识 ID,协商服务端与客户端要使用的对称密码算法、消息认证算法、杂凑算法等若干参数。与 S/MIME 协议情况类似，当前该协议使用的 DH 类密钥交换和 RSA、DSA 或 ECDSA 公钥认证算法并不是量子安全的，需要替换。

用户认证子协议使用传输层定义的会话 ID 完成服务端对客户端的认证，该过程使用依据传输层子协议中经过双方协商达成一致的算法完成。

连接子协议使用传输层子协议建立的加密安全通道并扩展通道至数个以完成登录访问，代理运行其它扩展协议，通过安全通道执行 TCP/IP 协议或 X11 协议访问服务端其它安全子系统等任务，该子协议运行于传输层协议和用户认证协议之上。类似的，该过程使用依据传输层子协议中经过双方协商达成一致的算法完成。

SSH 协议设计上支持选择密码算法，允许服务端和客户端对要使用的摘要算法、加密算法、认证算法和密钥协商算法类型进行协商，因此基础的 SSH 协议支持量子安全算法不需要做大量修改。由于传输层子协议决定了之后所有流程使用的算法，并且双方开始密钥协商时

会使用双方共同拥有的第一个可用算法完成，所以传输层子协议中服务端和客户端双方协商的各类算法就应该包含其可能用到的量子安全算法。否则一旦双方使用了不安全的算法，会导致后续其它所有过程都是不安全的。SSH 协议中需改造的流程以及修改方案如下：

1）DH 密钥协商算法需要被替换为量子安全的、能够快速生成密钥且具有前向安全性的密钥协商算法。

2）服务端认证使用的 RSA、DSA 或 ECDSA 公钥认证算法需要被替换为量子安全的签名算法或者使用基于预先分发共享对称密钥的 MAC 算法。

要注意由于 SSH 协议运行的位置决定，即使进行了上述替换工作形成量子安全的 SSH 协议，在 SSH 协议客户端作为安全代理运行其它外部协议（如 SMTP、HTTP 等）的应用场景下，如果这些外部协议不是量子安全的，整体仍然不是量子安全的。SSH 提供的量子安全特性无法确保它所代理运行的其它安全协议具有这一性质，这显示了量子安全的实现是综合性的——一旦用了弱密码会使本来足够安全的密码协议失效，多层协议栈传输数据决定了一旦其中有一层安全协议被量子计算攻破，即使其它层协议是量子安全的，也会导致主机被攻破、安全机制失效的后果。

2. 量子密码应用方案

量子密码的应用方案可以从量子密码与传统密码相结合，以及量子密码与应用系统相结合两个维度进行介绍。

2.1 量子密码的总体应用模式

从量子密码与传统密码的结合上，并相应考虑结合方案的技术成熟度，首先给出量子密码应用的各类应用模式。

（1）量子密钥分发配合特定算法实现信息论安全

当前技术条件已经能够基于 QKD 配合使用一次一密（OTP）密码算法在 QKD 网络的端到端之间实现信息论安全的加密（在明文数据传输速率不高于 QKD 密钥分发速率情况下，如电话语音加密），这是 QKD 技术的特有优势。实现信息论安全的密码系统具备长期抗量子攻击的能力。在未来 QKD 网络密钥分发速率能够有大幅提高的前提下，这种模式可以应用于更广泛的其它多种场景。

（2）量子密钥分发配合各类现有对称加密算法实现长期安全

将 QKD 与现有的加密算法结合使用，与现有基于数学算法的密钥分发模式配合现有加密算法相比，能够达到密钥更新和分发实时性更强、更安全，大幅提升密钥更新速率的特性，实现能支持大带宽高速加密、移动安全应用等当前 ICT 系统多样化业务需求的实用化量子保密通信系统。由于这种应用方案大大降低了密钥分发方面受到量子攻击的风险，可以认为是确保了密钥的安全性及密码系统的前向安全性，因此在现有对称加密算法（例如 AES-256）能够实现长期安全性的前提下，整体加密系统也能够实现长期安全性。

（3）纯量子密码解决方案实现量子安全

随着未来量子密码算法的逐步实用化，量子设备制造技术更加成熟，量子密码的功能将更加完善。可基于 QKD、量子密码算法和量子密码协议实现纯量子密码解决方案。密钥分发及主要密码算法均由量子密码功能实现，适用于高安全等级需求、各类专用网络，优势是在抗未来量子攻击方面能力更强。

2.2 QKD 在 ICT 系统的主要应用模式

在以上内容列举的三种应用模式中可见，目前阶段 QKD 配合现有密码算法的应用模式具有相对较广泛的应用前景。下面就 QKD 在 ICT 系统中的各种可行的应用模式做举例介绍。

（1）用于传输通道加密提供量子安全传输通道方案。使用 QKD 技术，建立量子安全传输通道，实现终端与业务系统间、业务系统与第三方对接系统间重要敏感信息的加密传输。比如：在 IP 层 VPN 系统中用 QKD 技术生成对称密钥对实现 VPN 通道加密等。如图 3-1 所示。

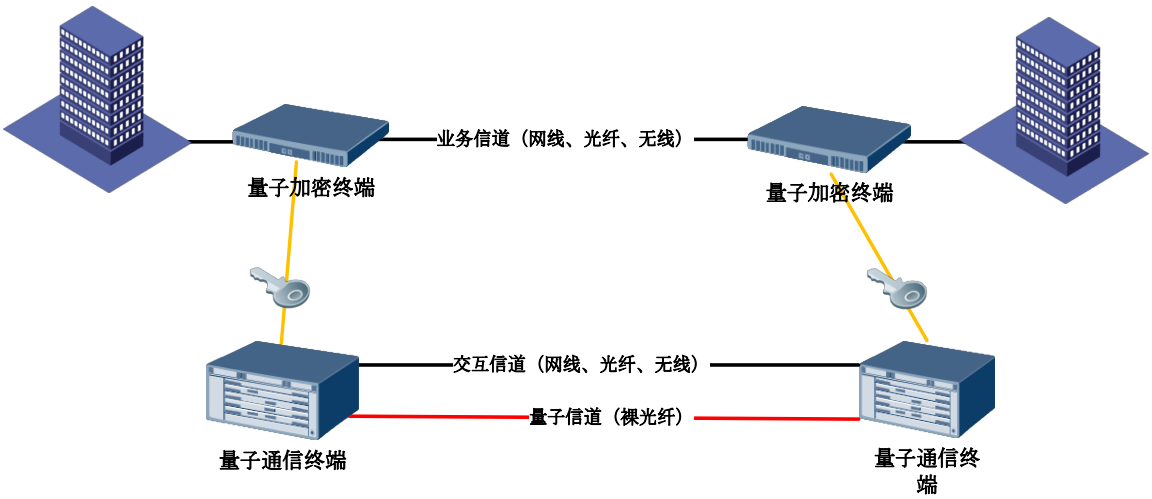

图 3-1 QKD+VPN 量子安全传输通道

（2）用于数据加密和密钥管理，提供密钥生成、端到端加解密、加密存储、加密密钥管理等方面的量子安全方案。例如：使用 QKD 技术，在各类端到端的通信过程中，对敏感的远程参数设置、控制命令等交互数据采用 QKD 技术的量子安全对称算法进行应用层加密，以保证数据的机密性。或者是使用 QKD 技术强化安全策略，对信息系统所使用的各种密钥进行全生命周期的安全管理。

（3）用于消息认证码 HMAC 的生成，提供保护数据真实性、完整性的量子安全方案。在使用消息认证码的信息系统中，可以利用 QKD 实时产生用于计算生成消息认证码所需的双方共有的对称密钥，比使用固定预分配对称密钥的传统方案更能提高认证过程的安全性。

2.3 QKD 在 TCP/IP 协议中的应用

在上一节讨论了 ICT 系统与 QKD 的模块化结合方式后，本节讨论从通信协议栈的角度，QKD 与现用的通信系统相结合，通信协议栈需要进行怎样的改造。QKD 与密码学中的密钥分发算法类似，能够与信息通信系统常用的 TCP/IP 参考模型中的数据链路层、网络层、传输层和应用层等分别进行结合应用，如图 3-2 所示[68]。

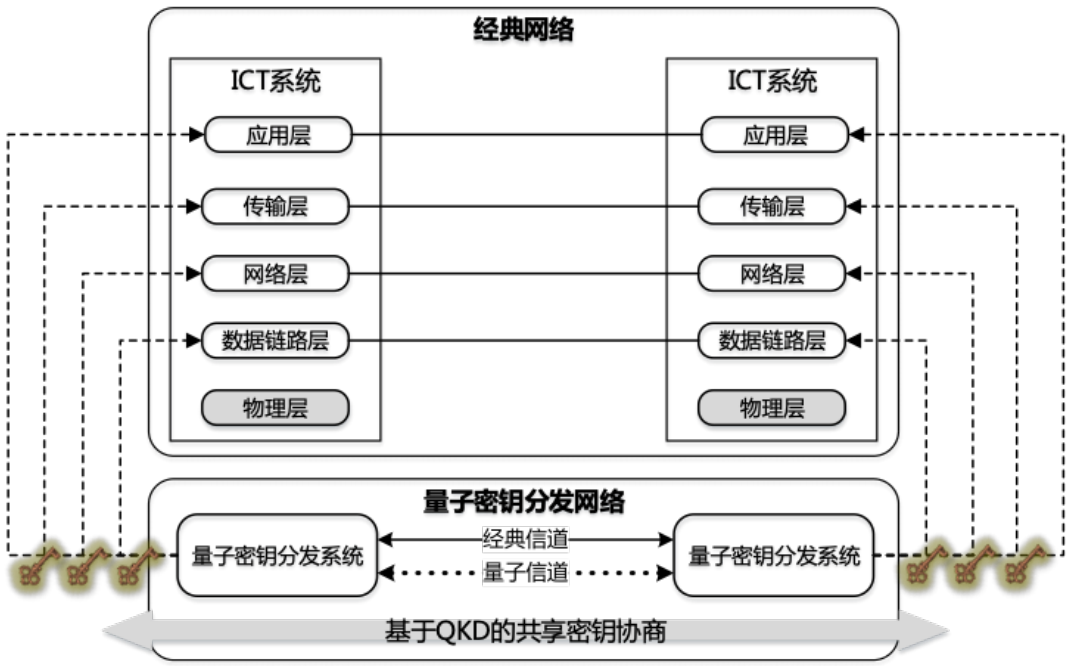

图 3-2 QKD 在 ICT 系统中的应用示意图

（1）数据链路层集成应用

目前的 QKD 系统通常是由点对点链路上的一对通过量子信道连接的设备组成。因此，将 QKD 与传统的链路加密机进行集成，构成基于 QKD 的量子链路加密机成为一种直观、合理的结合方案。该方案对对网络来说是透明的。这种用于点对点链路加密的 QKD 应用，也可称为基于 QKD 的虚拟专用网（VPN）隧道技术。 链路加密机可通过 QKD 产生对称密钥，作为对称分组加密算法使用的工作密钥，也可用于流加密算法（例如可实现最高安全性的 OTP，即一次性密码本），对光纤信道上承载的数据流量进行加密。注意这里 QKD 链路加密机既可用于在网络上相邻部署的两个节点之间的保密通信，也可以作为链路层的 VPN 隧道为跨网络的节点之间提供端到端的通信保护。

考虑具体的数据链路层协议，QKD 可与如下两类协议进行集成：

1）QKD 可以与 PPP（Point to Point Protocol）协议进行集成应用。PPP 协议工作在数据链路层，广泛用于网络中两组节点之间的连接。PPP 协议中的加密功能是通过加密控制协议（ECP）来实现的，用于在 PPP 的数据帧中实现加密算法。QKD 可作为 PPP 协议的一种新型密钥交换协议来进行结合。

2)QKD 还可用于另一种二层协议,即 IEEE 802.1 所定义的 MACsec 协议。MACsec 协议用于提供一种无连接的服务，支持为单个局域网或互联的局域网中的授权系统提供数据机密性、完整性和真实性服务。QKD 也可作为一种密钥交换技术在 MACsec 协议中集成应用。

（2）网络层集成应用

互联网安全协议（IPSec）是用于保障 IP 协议通信安全的一组协议套件。IPSec 工作在 OSI 模型的第三层，可实现对数据流中的 IP 数据包鉴权和加密。IPSec 协议簇中的互联网密钥交换协议（IKE）负责建立安全的网络连接。IKE 协议使用 DH 密钥交换协商算法建立共享会话密钥用于数据加密，在通信双方的认证鉴权方面，IKE 可以采用公钥方式，也可以采用预置密钥的方式。

QKD 作为新型密钥交换技术，可与 IKE 协议进行很好的融合。通过 IKE 协议的改进，可调用 QKD 生成的共享密钥为 IPSec 协议的载荷提供加解密功能。基于 QKD 所提供的共享密钥，可根据安全等级需求，既可以使用传统的分组加密算法，也可以采用一次性密码本（OTP）算法进行加密。目前已有不少集成 QKD 的 IPSec 应用案例，通常用于构建采用 IPSec 协议的 VPN 及路由器解决方案.

（3）传输层集成应用

TLS 及其前身 SSL 是工作在传输层的安全协议，用于在传输层为网络通信提供端到端的安全服务。它通常使用公钥密码交换技术来建立会话密钥，用来保护敏感信息的传输，例如电子商务交易中的信用卡信息。在 QKD 与 TLS 结合使用的场景中，QKD 产生的密钥可以用于替换 TLS 中的会话密钥，也可以用于进行一次性密码本方式的加密传输。另外，QKD 生成的密钥还可以用于实现消息认证，替换 TLS 协议中消息认证码（HMAC）或 SSL 协议中伪随机数函数的相应功能。

（4）应用层集成应用

在 OSI 模型传输层之上的应用层中，QKD 也可以与各类应用程序进行灵活的集成，例如加密语音/视频通话或会议、即时通信等业务。这些应用利用 QKD 为通信收发两端提供的对称共享密钥，既可以用于进行用户的身份认证或鉴权，也可以用于实现传输载荷的加密传输。

3. 量子密码与后量子密码融合应用方案

在当前以及近未来的技术条件下，可以将 QKD 与后量子密码相结合。后量子密码能应用于 QKD 网络中实现设备间的签名认证，即 QKD 网络协议执行需要待交互的设备间完成了可信认证作为前提，除通过预置密钥认证的方式外，结合使用 PQC 的公钥认证方法是较完善的量子安全解决方案。QKD 技术能够为后量子密码系统生成所需要的成对临时密钥或工作密钥，通过 QKD 不断更换加密密钥，可获得很强的前

向安全性。这种“QKD+PQC”类型的应用方案使密码系统整体能够应对量子攻击。

（二）量子安全典型技术领域应用

ICT 行业的主要应用场景，如各类终端设备，连通各设备的网络连接，云计算等运营模式的数据中心，以及区块链为代表的各类新兴密码应用，都存在被量子计算攻击的广泛可能性，因此，各类应用场景都具有量子安全技术的应用需求。

1. 终端设备加密与认证

这里的终端设备包括含义较为广泛,既包括用户用来与网络应用交互的有线/移动终端类硬件设备，如个人计算机、移动电话、类似 ATM 机的固定/移动智能终端，也包括基于嵌入式系统的物联网节点设备。终端设备加密与认证是指通过使用密码算法和安全协议使未授权方无法读取设备存储或传输的敏感内容，以防止各类未授权的数据访问，并基于此能够具备一定的抵御各类恶意攻击的能力。

终端设备加密与认证上存在的安全风险在于：即使通过全盘加密手段对终端设备的内容都进行了加密，如果设备使用的加密算法不是量子安全的，仍易被量子计算攻破从而被解密；即使磁盘加密是采用一般被认为量子安全的对称密钥算法实现，但如果密钥生成使用了非量子安全的公钥密码或密钥协商协议，例如 DSA（用于 AES 加密），RSA（用于三重 DES 加密）或 ECDSA，则整体加密方式仍然是抵抗不了

量子攻击的。这样量子计算对终端设备安全性就形成了以下各种潜在威胁：

一、攻击者若劫持了经过身份验证的终端设备，就可以使用与合法用户相同的端口、设备、网络，并访问相应的信息类别。也可以进行证书劫持，或者安装、执行 rootkit 等恶意软件。

二、攻击者可能借由被攻击设备利用安全远程访问协议（例如使用非量子安全算法的 SSH 协议）中的漏洞进行进一步的攻击，例如在设备间自己建立非授权安全隧道，用以在企业内网中攻击破坏更多的节点。

三、攻击者非法访问中央服务器或网络节点（通过恶意 SSH 隧道或类似的访问点）进而破坏整个网络，可以达到由特定用户或设备来控制读/写/复制/文件传输访问权限，以及哪个移动载体能够被允许访问网络；或者篡改或删除系统中的安全控制参数，从而使从内网中获取敏感内容变得更加容易。

四、攻击者还可以让终端设备伪装显示出符合安全访问控制策略的数据，例如伪造显示出具备策略所要求的防病毒软件和系统补丁，并将恶意软件渗透进入企业网络。这些受攻击的终端设备还可能导致由于违反信息安全法律被处罚。

终端设备加密与认证方面量子安全技术的目前可选用的应用方案模式是：

- 设备内部加密使用 QKD/QRNG 生成的对称密钥进行加密；
- 设备间端到端加密使用 QKD 分发的成对对称密钥完成；

- 设备间使用基于 QKD/QRNG 实时生成的成对密钥进行认证；
- 设备间使用 PQC 算法实现签名认证，设备间使用 PQC 算法实现密钥协商。

2. 网络基础设施加密

网络基础设施加密是指数据在整个网络基础设施传输中依赖网络自身实施加密以保护数据完整性、机密性、真实性。包括互联网主干网，大部分主要互联网通信通过互联网主干网在互联网的多个网络之间传播；互相连接的企业数据中心或云计算中心之间的加密，这些中心之间可能是互联网骨干网的一部分，也可能是内部网络；以及用于跨城域的广域网（WAN）的加密。

目前，并非所有在互联网上传输的数据都是经过加密的，因此易受到攻击，量子计算机破解的威胁意味着所有使用不抗量子计算的加密算法所加密的信息都可能受到损害。如果使用非量子安全的算法对网络基础设施进行加密，则通过该网络传输的所有数据都容易受到拥有量子计算机的对手立即或稍后解密的攻击。而且值得注意的是，敌手可以将现在的加密密文一直存储等待数年直到量子计算机能够破解加密算法。

例如，用于对 Web 浏览数据流量进行加密的最常用方法之一是安全超文本传输协议 HTTPS，除加密外，它还提供客户端和服务器间的身份验证。它使用 RSA 公钥算法进行服务器身份验证，使用 DH 算法进行密钥协商，这两种方法都容易受到 Shor 量子算法的攻击。因此，

拥有量子计算机的敌手即可解密在服务器和客户端 Web 浏览器之间发送的所有流量。

又例如，当前运营商或用户自身等机构基于专用加密硬件或网络设备实现的 OSI 第 2 层（以太网）或 OSI 第 3 层（IP）上的加密通信。当前没有广泛用于第 2 层加密的标准化协议，厂商一般使用自定义的加密协议，大多数厂商都依赖 RSA 算法或 DH 密钥交换协议，该类解决方案就容易受到量子计算机的攻击。当前已经出现了具有量子安全能力的第 2 层加密货架产品，其中包括一个专为第 2 层加密设备提供加密密钥的量子密钥分发系统。第 3 层加密通常基于 IPsec 协议，IPsec 协议使用 IKE 协议进行密钥协商，IKE 不是量子安全的，这就意味着可以使用量子计算机对通过这些网络的通信进行解密。

网络基础设施加密方面量子安全技术的目前可选用的应用方案模式是：

- 基于 PQC 算法实现核心网设备间和用户设备间的身份认证，核心网设备和用户设备均可使用 PQC 算法实现密钥协商和公钥加密算法；
- 基于 QKD 技术保障核心 IP 网交换信令数据传输安全，防范外部 IP 网络攻击；
- 基于 QKD 网络保护 5G 前传/中传网络的加密安全；
- 基于 QKD 技术保障类似移动通信网中 VoLTE 加密语音系统等通信业务系统的密钥分发安全；

- 基于 QKD 技术保护主数据中心和备份数据中心间敏感数据流的安全。

3. 云计算、大数据与人工智能

云计算、大数据与人工智能作为 IT 行业当前热门应用，都是将计算以服务形式为用户提供。基于高性能网络、硬件虚拟化技术的成熟以及计算和存储设备成本的下降，云服务已变得无处不在。云计算具有许多优势，包括可从多个设备/位置进行访问，减少企业自身 IT 应用投资，以及优化利用分布在许多用户和企业中的计算能力。但使用云计算的一个主要问题就是由于这些服务是由许多用户共享的，而且通常不是通过专用网络提供的，因此加密更是必不可少的。

量子安全云计算的实现涉及量子安全服务器，端设备和网络基础设施。如上文提到的要实现量子安全，所使用的 HTTPS 等安全协议的密钥协商不应再使用 RSA，DSA 或 ECDSA 算法。云计算的特殊之处在于其安全管理系统由云架构决定也会是集中式、跨业务和面向应用的，因此可以更方便的过渡到量子安全协议。由于云存储的远程访问需求，数据会穿越用户和云之间的公共网络,共享基础设施类型的不同且互不信任的众多用户群体会进一步强化对数据保密性的需求。

云计算、数据中心加密方面量子安全技术目前可选用的应用方案模式是：

- 基于 PQC 算法实现云存储、人工智能、大数据等新型应用系统服务端与客户端之间的身份认证，基于 PQC 算法实现服务端与客户端之间的密钥协商和公钥加密算法；
- 基于 QKD 技术实现云存储、人工智能、大数据等新型应用系统的密钥安全分发。

4. 区块链

区块链由于其安全性基于公钥密码而受到来自量子计算的严重安全威胁，此外它还有私钥安全存储等特殊安全问题。开源软件界已经认识到需要做这一必要工作，发起了“抗量子账簿(QRL)”项目。有研究者提出了一种基于 QKD 的量子安全区块链解决方案。主要思想是将基于 PoW 的共识机制替换为基于拜占庭算法的共识机制。这一共识机制不需要公钥密码进行身份验证，而是依靠 QKD 为区块链网络内的成对节点实现信息论上的安全身份验证。由于放弃了公钥算法，因此可以认为它是量子安全的区块链。还有厂商提出了一种量子密钥管理解决方案，利用 QKD 和 QRNG 来增强区块链的安全性，其利用 QRNG 生成真随机数作为密钥种子，并使用 Shamir 密钥共享算法将密钥拆分为多个元素，然后使用 QKD 将密钥元素安全地分发到分布式的远程密钥存储节点。

区块链领域量子安全技术总体应用模式是将现有区块链系统中不具备量子安全特性的公钥签名、公钥加密和密钥协商算法替换为对

应的 PQC 类算法以实现区块链系统的量子安全；而应用 QKD 的方式尚待研究。

（三）量子安全典型垂直行业应用

在涉及国计民生的政务、金融、通信、能源等领域量子安全技术具有广阔的应用前景。

1. 金融服务信息安全

银行和金融服务部门在运营中严重依赖信息技术，因此广泛使用加密技术来保证所处理信息的机密性、真实性、完整性和不可抵赖性。例如，需要保护其内部网络或数据中心间的信息传输、灾备数据流量、内部敏感通信等。这些系统可能是硬件或软件形式加密的，但只要是基于现有公钥密码实现密钥分发的，都易受到量子攻击。

用于银行间转移支付功能的基于 SWIFT 银行结算系统（也称为环球同业银行金融电讯协会）完成跨行间财务信息传递功能，它能够实现全球不同银行之间的统一标准化加密交易。SWIFT 自身具备公钥基础设施，通过 SWIFT 网络发送的消息都是进行数字签名和加密的，这些算法需要迁移到量子安全形式的数字签名和加密以保持其安全性。

信用卡信息受国际标准《支付卡行业数据安全标准》（PCIDSS）的保护。在被传输到银行之前，在零售机构持卡人数据就应该被加密。这种加密本身是利用对称密码完成，但这个过程就需要使用量子安全替代方案进行密钥协商以确保长期安全性。

金融业要实现安全的数据存储和灾备，存储设备中数据由金融公司负责加密，这种解决方案可能是基于硬件 AES 算法加密的，也必须实现量子安全。

在线银行业务通常依靠 TLS 协议来保护网络流量，使用 X.509 证书和 RSA 公钥进行服务器身份验证以及会话密钥协商，因此，容易受到量子攻击的影响，必须实现量子安全。

量子计算给金融业带来了巨大的安全性挑战。金融行业的客户数据这种类型的信息必须确保其长期安全性，电子交易数据本身价值极高，量子计算的现实威胁产生后，金融行业极有可能被首先锁定为目标，因为攻击者可以直接从攻击中获得经济利益。在针对金融服务行业的密码技术实现细节上，需要考虑对速率和信息有效负载等问题的特殊要求，金融业对在线交易完成速度的要求很高，解决方案提供商须仔细评估量子安全方案的密钥生成速度、加解密速度这些关键指标。

2. 政务网络信息安全

对于政务网络中运行的内部办公应用、电子政务、对外便民服务等类型的信息系统，确保其安全高效运行至关重要。我国在《“十三五”国家政务信息化工程建设规划》中就已要求：全面推进安全可靠产品及商用密码应用，提高自主保障能力，切实保障政务信息系统的安全可靠运行。电子政务系统一般均是基于其自建公钥密码基础设施实现身份认证与密钥协商，其使用的密码算法如果不具备量子安全特

性，当前生成的具敏感性的政务信息，在未来都可能被量子计算机所破解，因此政务领域需要应用具备长期安全性的密码算法。

例如对于电子证照系统，可考虑基于 QKD 技术建立数据库与数据接收终端设备间，数据接收终端设备与办事中心系统间加密传输通道，以确保参数设置、控制命令等数据的机密性、完整性等，并提升系统整体安全等级。

3. 工业互联网信息安全

以工业控制用途的远程监视和控制系统（Supervisory Control And Data Acquisition,SCADA)为例，其对资源开采和分配(如石油、天然气、采矿等）、国家公用事业和基础设施（如电网、铁路和交通系统控制、水处理及自来水系统等）、制造和建造业等都非常重要。不加密保护的 SCADA 系统为攻击者提供了远程接管工厂、石油管道、电网、机场、采矿业和电力供应的机会。在这些情况下造成破坏的可能性是不言而喻的，可能造成的损失会也是无法计量的。

从历史上看，由于 SCADA 系统最初都是专网专用的，对其安全性的研究很少，由于新的、网络化工业控制模式的出现，安全性上的模糊不清就不可接受了。在发生震网(Stuxnet)蠕虫事件之后几年中，渗透测试揭示了这些系统的安全性整体上非常不乐观。尽管后 Stuxnet 时代有些系统的部分环节是使用量子安全的算法加密的（例如使用 AES 算法），但系统安全模型中的任何薄弱环节都容易受到量子计算的攻击。须进一步研究来识别 SCADA 系统信息流中易受攻击的

环节，并应用标准的量子安全技术。当前的发展趋势是在大型分布式控制系统中使用卫星，在智能远程监控中普遍利用物联网，因此SCADA系统的设计人员和管理员必须重视加密系统向量子安全过渡这一重要需求。

物联网设备到设备（Machine to Machine,M2M)传感器是具有远程连接能力的嵌入式设备，用于远程监控资产并与上层服务器进行通讯，它具有普遍的适用性，例如电表、自动售货机、运输集装箱、医疗监控设备均是此类。这些设备要么使用专用无线网络，要么从运营商处接入移动公网。对其安全性的要求和相关监管已经被提上了日程，它的加密密钥管理需求有一些独特特征，例如资源受限、远程独立工作等，量子安全的要求在这里同样适用，有厂商已推出针对物联网终端实施量子安全密钥管理的产品。

时间敏感网络（Time Sensitive Network,TSN）是IEEE开发的一种广泛应用的通信标准，它用以满足工业环境中严格精确的延迟和定时要求，是工业控制系统的通信基础协议之一。确保TSN安全是一项重要要求，针对TSN不便于使用需要很多人工操作的预置共享密钥方式，也不便使用需要占用更多计算资源的公钥密码交换方式，有研究者提出QKD能够作为TSN的一种较好的密钥分发解决方案，实现高效实时安全的密钥分发。

4. 交通信息安全

专用用途如车队物流、公共安全应用、远程信息处理的具有信息互联能力的车辆，以及大众用途的新兴的车对车通信、车联网，以及交通信息基础设施的信息传输与控制等应用场景中，都需要确保通信的机密性、真实性。

例如智能网联汽车在传统汽车的基础上引入了大量的智能化设备和系统，可借助于网络通信技术远程对汽车进行更多的智能控制，如远程分析、远程检修、远程寻车、实时路况预警、自动驾驶、自动躲避、自动预警、自动更新等，并可将智能终端(如智能手机、平板电脑)与车载系统方便的建立连接，控制车载系统，提高驾驶的安全性和舒适度，增强驾车体验。但“特斯拉”等网联汽车被攻击事件的曝光，表明智能网联汽车信息安全问题日益严重。相关安全问题不仅会造成个人隐私暴露、企业经济损失，甚至还能造成车毁人亡的严重后果。据统计有大部分消费者认为信息安全和隐私保护将成为未来购车时主要考虑的因素，智能网联汽车信息安全已经成为汽车产业甚至社会关注的热点。

在终端接入、用户认证、控制指令下发、补丁包升级等关键环节上，需要通过密码技术实现身份可信、数据保密、数据不可篡改和来源可信，而这些密码算法如果不是量子安全的，将导致这些信息系统中的敏感数据被窃取，甚至系统被攻击者所控制造成更大的破坏和混乱。

5. 能源设施信息安全

能源设施是现代社会正常运行必须的基础设施。典型的是在电力系统中，发电、输电、变电、配电及供电部门都需要通过专门的调度环节，对电能量进行调度指挥、监督和管理。电力调度环节是电网电能量调配的核心环节，任何安全问题都可能导致灾难性后果，带来不可估量的损失。所采取的安全解决方案一般是建立基于公钥密码基础设施的专用电力调度证书系统，为电力调度生产及管理系统、调度数据网用户、关键网络设备、服务器等提供数字证书服务。结合专用的上下级间纵向加密认证装置，建立完整的安全保障体系。这一体系中使用的密码算法如果不是量子安全的，敌手可以基于量子计算攻击发动用户仿冒、控制数据伪造等各种形式、防不胜防、安全防护体系自身难以察觉和抵御的攻击行为，严重影响电力系统的运行安全。

6. 医疗健康信息安全

当前，区域范围乃至国家性的公共卫生信息网络和集中维护患者记录的医疗信息系统的使用日益普遍。保护患者的机密性、隐私性数据变得越来越重要。许多国家的法律要求由于安全措施不足而导致患者数据泄露的医疗机构须承担法律责任。量子计算对医疗机构信息系统造成的威胁包括：

- 由于工作人员终端设备加密不当或区域网络内医疗中心之间的通信加密不当，导致涉及患者信息的医疗数据泄露。

- 由于隐私性数据未经量子安全的加密，导致其在医疗网络中被未授权的数据挖掘行为获取。
- 通过伪造身份认证欺诈获取患者文件。
- 导致存储在临床计算机上的敏感性科研信息泄露。

使用量子安全解决方案保护与医学和医疗保健相关的信息尤为重要，因为此类信息通常需要长期保密，至少应等于患者的预期寿命，并在数据有遗传需求的情况下甚至可能超出此范围。这些要求通常会被一些国家整合到立法中，例如德国法律规定，即使患者死亡，医疗数据也必须保持保密性。

四、量子安全技术发展现状

（一）后量子密码技术的发展现状

1. 后量子密码技术的政策和规划

2015 年 1 月，欧盟率先启动后量子密码算法 SAFECRYPTO 应用项目，在对称加密、对称授权、公钥加密以及公钥签名系统领域都提出了相关标准化建议。同年 3 月，欧洲多所高校和科技企业联合开展了全球后量子密码算法旗舰项目 PQCRYPTO，并将其纳入欧盟地平线 2020 计划。2018 年又开展了后续的 PROMETHEUS 项目，致力于打造新一代安全实用的后量子密码方案。类似的还有日本的 CREST 项目也取得了较显著的成果。

2015 年，美国密码和信息安全领域最权威的管理和研究机构国家安全局（NSA）公开宣布由于面临量子计算的威胁，其计划将联邦政府各部门目前使用的 ECC/RSA 算法体系向后量子算法进行迁移。美国负责标准制定的美国国家标准与技术研究院（NIST）在 2016 年 4 月发布了“后量子密码学”的研究报告，并在同年启动了“后量子密码算法标准化”工作计划，面向全球征集后量子密码标准，其中包括公钥密码、数字签名以及密钥交换算法。NIST 计划利用 3-5 年时间

分析这些建议并发布相关分析报告，最终的标准拟制工作也将耗时 1-2 年。预计在 2022-2023 年完成 PQC 算法的起草与发布。

我国密码管理部门也于 2018 年面向全国开展了后量子密码算法设计竞赛活动并在推进 PQC 算法的标准化工作，2019 年经第二轮筛选获得 12 个算法。

总体上看，欧、美、日这些传统发达国家处于后量子密码研究和应用领域的领先地位。而且各国之间通过各类国际性组织联合等方式开展了很多合作工作，较少体现出对抗。欧洲电信标准化协会（ETSI）开展了量子安全计划的研究，国际标准化组织（ISO/IEC）开展了后量子密码算法研究项目的研究，互联网产业方面最权威的以美国为主导的国际互联网工程任务组（IETF）也正在进行后量子密码算法草案的设计，国际安全组织云安全联盟（CSA）于 2018 年也发布了后量子密码发展现状的研究报告。

2. 后量子密码技术标准化情况

近年来，各国密码管理部门对 PQC 研究也开始重视和推进，由于目前尚未实现算法标准化，还未发展到实际系统研发和基础设施推广建设阶段，主要的表现是国际产业界和标准化组织以及各国密码管理部门都在积极推进 PQC 密码的标准化工作。

2.1 欧洲

ETSI 在 CYBER 技术机构下成立了 QSC 小组，专门负责 PQC 方面的标准制定和研究工作。在 2016 年，QSC 发布了《量子安全密码和安全：介绍、优势、推动因素和挑战》白皮书；同年，QSC 发布了《量子安全算法框架》小组报告；2017 年 2 月和 3 月，QSC 分别发布了《案例研究和部署方案》、《受限于量子计算的对称密钥长度》、《量子安全威胁评估》小组报告；2017 年 10 月，QSC 发布了《量子安全密钥交换》技术报告；2018 年 9 月，QSC 发布了《量子安全虚拟专用网》技术报告；2019 年 12 月，QSC 发布了《基于量子安全认证的加密》技术报告；2020 年 6 年，QSC 发布了《量子安全计划的迁移策略和建议》技术报告。目前正在进行的工作程序有五项，其中两项已形成最终版本，一项已形成稳定版本。

ISO 中专门负责 PQC 相关工作的组织是 ISO/IEC JTC 1/SC 27 下的 WG 2 小组。2015 年，该小组开始了一项 PQC 的调研工作，经过多轮讨论，在 2017 年 11 月的柏林会议上，ISO 同意终止调研期并启动一项常设文件（WG2/SD8）的项目。

2.2 美国

美国 NIST 对 PQC 标准化的进展和计划如表 4-1 所示。从 NIST 征集后量子密码算法工作过程可以清晰的看到 PQC 算法研究受到了全球密码学界的高度重视，体现了很大程度的国际合作。

表 4-1 NIST 对 PQC 标准化的进展和计划

	时间	工作阶段
1	2016 年 4 月	NIST 发布量子后密码学报告（编号 NISTIR 8105）
2	2016 年 12 月	正式提出征集算法呼吁提案
3	2017 年 11 月	第一轮算法征集的提交截止日期
4	2017 年 12 月	第 1 轮算法宣布（69 份提交被接受为"完整和正确"）
5	2018 年 4 月	召开首届 PQC 标准化会议
6	2019 年 1 月	第二轮候选算法公布（26 种算法）
7	2019 年 3 月	第二轮算法征集的更新提交截止日期
8	2019 年 8 月	召开第二届 PQC 标准化会议
9	2020 年 7 月	第三轮算法征集候选算法公布（7 名入围者和 8 名候补候选人）
10	2020 年 10 月	第三轮更新提交包的截止日期
11	2022/2024	提供标准草案

2017年第一轮征集结束,NIST共收到来自全球的候选算法82份。在进行初步筛选后，NIST 公布了69个“完整且适合”的草案，包括基于格、编码、多变量、哈希以及其他方法构造的后量子密码算法。其中基于格和编码构造的最多，且主要被用于构造公钥加密算法；由于基于多变量的陷门构造相对更为可行和高效，因此主要集中于数字签名方案，公钥加密方案较少；而基于哈希的构造方案中树状结构的使用，目前只有数字签名的构造，缺少公钥加密算法。在后继2018年开展的第二轮征集和筛选中审查入围的有26种候选算法。数个来自中国的研究团队也参加了NIST后量子密码标准征集工作。

2020年7月，NIST公布了PQC算法第三轮筛选的7个最有希望入选、有望得到广泛应用的候选算法，分别是：公钥加密算法有Classic McEliece、CRYSTALS-KYBER、NTRU、SABER；数字签名算法有CRYSTALS-DILITHIUM、FALCON、Rainbow，如表4-2所示。此外，以下8种算法也被认为是具有发展前途、有希望被标准化的，需要更多的时间来发展成熟，也将进入候选：公钥加密算法有BIKE、FrodoKEM、HQC、NTRU Prime、SIKE；数字签名算法有GeMSS、Picnic、SPHINCS+，如表4-3所示。本轮筛选中没有中国研究者提交的算法入围。

表 4-2 NIST 对 PQC 标准化的第三轮入选算法

第三轮	**最终入选算法**	
类别	公钥加密/密钥封装	公钥签名
基于格	CRYSTALS-KYBER [MLWE]	CRYSTALS-DILITHIUM [MLWE、Fiat-Shamir]
	NTRU	FALCON[NTRU 及杂凑-签名]
	SABER [MLWR]	—
基于编码	Classic McEliece [Goppa 码]	—
基于多变量	—	Rainbow[UOV]
基于杂凑	—	—

表 4-3 NIST 对 PQC 标准化的第三轮后补入选算法

第三轮	**候补入选算法**	
类别	公钥加密/密钥封装	公钥签名
基于格	FrodoKEM [LWE]	—
	NTRU Prime [NTRU]	
基于编码	BIKE [QC-MDPC]	—
	HQC [Reed-Muller 和 Reed-Solomon 码]	
基于多变量	—	GeMSS [HFE]
基于杂凑	—	Picnic [ZKP+杂凑+分组密码]
		SPHINCS+ [杂凑]
其他	SIKE[超奇异椭圆曲线]	—

第三轮审查结束后，NIST 将继续对上述 7 项决赛入围算法进行审查，供下一步制定标准参考。由于 CRYSTALS-KYBER、NTRU 和 SABER

都是基于格的方案，NIST 计划最多选择一个作为标准。签名方案中的 CRYSTALS-DILITHIUM 和 FALCON 也是如此。在 NIST 看来，这些基于格上困难问题的方案是公钥加密和数字签名方案中最有前途的通用算法。预计第三轮的评价和审查将持续 12-18 个月。NIST 计划在 2021 年召开第三届 NIST PQC 标准化会议，在 2022 年发布后量子密码的初始标准。

3. 后量子密码技术产业生态

根据 Inside Quantum Technology 的一份最新报告，到 2029 年，后量子密码（PQC）软件和芯片的市场将增至 95 亿美元。PQC 功能将嵌入到众多设备和环境中，其中 80%以上的收入将来自网络浏览器、物联网、机床和网络安全行业本身。

国际上 ICT 行业大型跨国公司如 IBM、微软、谷歌、华为等都投入了力量在 PQC 的研究上并形成了相应研究成果。IBM 在该领域研究重点是格密码。微软参与到了 FrodoKEM、SIKE、Picnic、qTESLA 四个用于签名和密钥交互的 PQC 项目的研究中，PQC 库的开发和安全协议集成也是其重点投入的工作。2016 年微软公司发布了基于格密码库（Lattice Crypto），2018 年微软发布了著名开源项目 OpenVPN 的一个名为 PQCrypto-VPN 的分支项目，这个项目在 OpenVPN 中实现了 PQC 算法，并可以在 VPN 中测试 PQC 算法的功能和性能。谷歌公司在对当前后量子密码技术发展进行调查后，也提出了基于环上带误差学习问题的密钥交换协议，还对运行于浏览器的 PQC 算法进行了实验。

华为计划尽早为密码协议引入安全的后量子算法，以确保其产品的长期安全性，华为正在关注后量子算法的各种标准化活动，并计划在标准化工作结束之前将一些候选算法试验性地引入他们的产品中。

国际上也出现了一些面向 PQC 方向的初创公司和安全行业公司，传统安全公司 Onboard Security，研究方向面向格密码算法 NTRU，初创公司 Duality Technologies 提供基于量子安全的同态密码隐私保护解决方案。美国安全创新公司（Security Innovation）注册并拥有 NTRU 算法的专利，其提供两种授权选项：开源 GNUGPL v2 授权以及商业授权。从 2011 年起，该公司发布了多种实现 NTRU 算法的软件库，其中包括安全套接字协议层（SSL）和 ARM7/9 处理器库等。

开源界也形成了 PQC 方向相关的开源社区，并开发了一些 PQC 方面开源项目。如“开放量子安全(Open Quantum Safe)”项目[69]，目的是打造名为 liboqs 的抗量子破解加密算法的 C 语言库，该项目已经被应用到著名的开源安全软件 OpenSSL 上。类似的项目还有 NTRUOpenSourceProject 等。

（二）量子密码技术的发展现状

1. 量子密码技术的政策和规划

量子密码作为量子信息技术中最先进入实用化阶段的技术，其受到世界各国在量子信息整体战略布局和项目上的支持。

1.1 欧洲

欧盟委员会 2016 年发布《量子宣言》，提出欧洲量子技术旗舰计划[70]，计划 3 年左右建设低成本量子城域网并建立量子通信设备和系统的认证及标准，6 年左右利用可信中继、高空平台或卫星实现城际量子保密通信网络建设，10 年左右建成量子互联网。2017 年 10 月，多家欧洲研究机构发起成立量子互联网联盟（QIA），目标是通过开发、集成和演示所有功能性硬件和软件子系统，为基于纠缠的泛欧量子互联网制定蓝图[71]。2018 年 10 月，欧洲量子技术旗舰计划开始施行，预算为 10 亿欧元[72]。

2020 年 3 月，欧洲量子技术旗舰计划发布了一份战略研究报告[73]，给出了切实可行的短期及中长期建议。短期目标（3 年愿景）包括：基于欧洲量子通信基础设施（EuroQCI）端到端安全的考虑，开发用例和商业模型，开发用于城市间和城市内的经济高效且可扩展的设备和系统；开发可信节点网络的功能，提升光纤、自由空间和卫星链路之间的互操作性；利用 QKD 协议和具有可信节点的网络，开发用于全球安全密钥分发的基于卫星的量子密码；与 ETSI 等主要欧洲标准组织合作开展标准制定工作，制定用于 QRNG 和 QKD 的认证方法；进一步发展 QKD、QRNG 和量子安全认证系统，应表明其为用于关键基础设施、物联网和 5G 做好了技术准备；实现欧盟国家间可信节点上的端到端安全通信等。中长期目标（6～10 年愿景）包括：演示一系列物理距离遥远（至少 800 公里）的量子中继器；演示至少 20 个量子比特的量子网络节点；演示设备无关的 QRNG 和 QKD 等。

此外，英国、德国、俄罗斯等欧洲国家也制定了自己的量子战略，发展量子信息技术，实践量子保密通信等量子密码技术的应用试验示范[74]-[78]。

1.2 美国

2018 年 12 月，美国发布《国家量子计划法案》，计划未来十年内向量子研究注入 12 亿美元资金，由美国能源部、商务部国家标准与技术研究院和美国国家科学基金会配合联邦政府共同落实量子计划项目。2019 年 12 月，美国国防部（DoD）国防科学委员会公开《量子技术应用》研究报告的内容摘要版，其中列举了对量子传感、量子计算、量子通信三大领域共 24 条核心观点。报告指出， QKD 提供信息理论的密码安全性，但在产业化方面还存在挑战，并希望继续了解和跟踪 QKD 在其他国家的开发和使用。2020 年 2 月，美国发布《量子网络战略构想》[79]，提出了面向未来的两个具体目标：一是在未来的 5 年中，演示量子网络的基础科学和关键技术，从量子互联、量子中继器、量子存储器到高通量量子信道和探索跨洲际距离的天基纠缠分发；二是在未来 20 年里，量子互联网链路将利用网络化量子设备实现经典技术无法实现的新功能。2020 年 5 月，美国智库哈德森（Hudson）研究所发布《高管量子密码学指南：后量子世界中的安全性》报告，对 QKD 技术原理、应用场景和发展情况进行了简述。其中指出，面对量子计算的威胁，一种解决方案是抗量子计算破解密码学，另一种方案是使用量子技术提供的工具，包括 QKD 和 QRNG。未来，随

着 QKD 技术的发展和成熟，将形成包括空间网络在内的全球量子通信网络的基础。

1.3 中国

近年来，我国发布了一系列支持量子通信和量子密钥分发技术发展的政策。如，在 2016 年 3 月第十二届全国人民代表大会第四次会议发布《国民经济和社会发展第十三个五年规划纲要》中，在 2016 年 11 月国务院发布的《“十三五”国家战略性新兴产业发展规划》中，在 2017 年 5 月在国家发改委发布的《十三五国家技术创新工程规划》中，在 2018 年 1 月国务院发布的《国务院关于全面加强基础科学研究的若干意见》中，在 2019 年 12 月中共中央、国务院《长江三角洲区域一体化发展规划纲要》中，以及在 2020 年 3 月科技部发布《关于科技创新支撑复工复产和经济平稳运行的若干措施》中，都提到加强量子信息技术或量子通信技术的发展。

2020 年 10 月，中央政治局集中学习量子科技研究和应用前景。习近平总书记指出，要系统总结我国量子科技发展的成功经验，借鉴国外的有益做法，深入分析研判量子科技发展大势，找准我国量子科技发展的切入点和突破口，统筹基础研究、前沿技术、工程技术研发，培育量子通信等战略性新兴产业，抢占量子科技国际竞争制高点，构筑发展新优势。

在量子密码技术的实践方面，从 2009 年开始到 2020 年的 11 年间，通过国家科技部、中国科学院、国家发改委、教育部、工信部等，

以及各地方政府的科技创新及成果转化项目的支持下，我国通过在量子保密通信城域光纤网、城际光纤网以及星-地自由空间网络方面进行的技术攻关和应用试验示范，在国际上率先实现了星-地一体的广域量子保密通信网络路线图，并积累了丰富的工程和实践经验，推动了量子通信产业化的进程。

1.4 其他

日本政府近年来对量子密码、量子卫星、量子计算、量子传感等量子信息技术的研发都有计划项目支持[80]，将量子技术置于和人工智能、生物科技同等重要的位置。2020 年度日本政府预算中有关量子技术研发的费用比 2019 年度翻了一番，达到约 300 亿日元（约合 20 亿元人民币）[81]。日本政府将在 2020 年度起的 5 年里完善量子技术的研发体制，并在包括量子安全技术在内的 8 个领域建立核心研发基地。

韩国于 2016 年启动量子通信为期 8 年的中长期技术开发项目。2020 年 9 月，韩国科学与信息技术部发布旨在后疫情时代创造未来增长引擎的“数字新政”计划（Digital new deal），计划投资约 58 万亿韩元（约 425 亿欧元）支持人工智能、5G、量子技术等领域[82]。2020 年 11 月，韩国内务和安全部招标建设总长 2000km，覆盖全国 48 个政府部门的 QKD 网络，其将是目前中国之外建设规模最大的 QKD 网络[83]。

印度于 2020 年提出一项新国家量子任务，计划未来 5 年投入 800 亿卢比（11.2 亿美元），推动量子技术的发展。新国家量子任务旨在加速印度量子通信、量子计算、量子材料开发和密码学等量子技术的发展步伐[84]。

2. 量子密码技术、产品和专利

2.1 前沿技术成果

量子密钥分发是目前量子密码的主要体现，也是量子通信技术实用化的重要体现。英国政府科学办公室发布“量子时代的机会”研究报告中描绘了量子通信应用发展趋势[85]，如图 4-1 所示。量子密钥分发技术将随着量子通信技术的发展，从保密通信网络阶段逐步提升到量子互联网阶段，从利用可信节点组网阶段逐步提升到量子中继组网阶段，从而实现端到端的全量子安全网络。自 2007 年我国完成诱骗态协议量子密钥分发的首次实验验证[86]后，量子密钥分发技术进入了快速发展阶段，城域网、城际干线和星地量子密钥分发试验示范的依次完成，标志着量子密钥分发进入广域网络发展阶段。当前，量子密钥分发技术前沿技术的主要研究方向是：高速率、远距离、集成化、低成本、器件无关的量子密钥分发技术，以及量子中继、远距离量子纠缠分发及量子隐形传态技术等。近年来一些代表性成果如下：

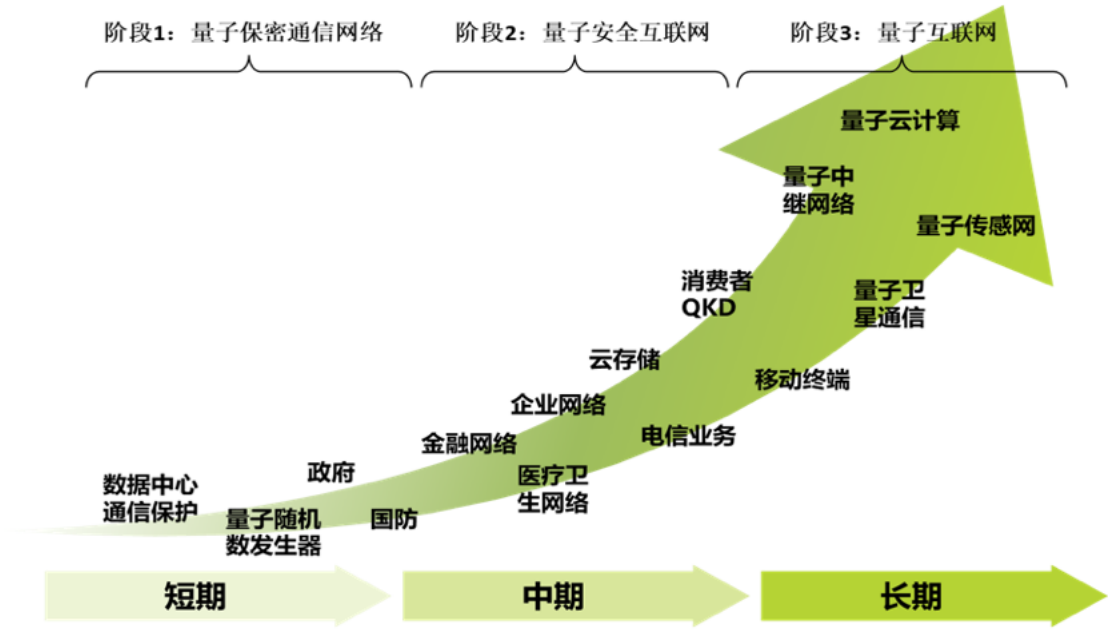

图 4-1 量子通信应用发展展望

（1）2016 年，中国研究人员提出 4 强度诱骗态优化协议[87]，结合长时间稳定的双光子干涉技术、国产化高效低噪声超导纳米线单光子探测器等，实现超过 400 公里的测量设备无关量子密钥分发，这也是当时远距离量子通信的世界纪录[88]；

（2）2016 年，中国成功发射“墨子号”量子科学实验卫星，实现了在从卫星到地面的最大 1200 公里的诱骗态 QKD 实验，并达到了 kbps 的成码率[89]；

（3）2017 年，中国实验实现了百公里光纤纠缠交换[90]；

（4）2017 年，奥地利、美国联合实现单跨 421 公里光纤量子密钥分发世界纪录[91]；

（5）2018 年，中国和奥地利应用“墨子号”卫星实现了洲际 QKD 实验，在相距 7600 公里的中国和奥地利地面站之间进行 QKD 实验并利用安全密钥完成了文本和视频的加密传输[92]；

（6）2019 年，中国实现了 3 方纠缠存储[93]、3 维量子隐形传态（中国、奥地利联合）[94]、22/50km 纠缠存储[95]；

（7）2019 年，中国实现了 300 公里真实环境光纤中的双场量子密钥分发(TF-QKD)实验，密钥生成率达到 2016 年实验的 50 倍[96]；

（8）2019 年，奥地利实现 50km 光与存储纠缠[97]；

（9）2019 年，新加坡实现了基于芯片化终端的 100 公里光纤连续变量量子密钥分发[98]；

（10）2020 年，法国实现高效率量子纠缠制备与存储[99]；

（11）2020 年，中国应用“墨子号”量子科学实验卫星，实现基于纠缠光子的，相距 1120km 两地间的量子密钥分发[100]；

（12）2020 年，中国实现基于发送-不发送双场协议[101]的 509 公里量子密钥分发[46]和基于相位匹配双场协议的 502 公里光纤量子密钥分发[47]，再次获得无中继光纤量子密钥分发世界纪录[102]；

（13）2020 年，英国实现基于 InP 芯片化终端的光纤测量器件无关量子密钥分发，将 250MHz、时间编码的光源组件集成在 6×2 mm^2 的 InP 芯片上，估计了 40dB 成码率 1bps[103]；

（14）2020 年，中国实现了基于硅光芯片的高速测量器件无关量子密钥分发，将 1.25GHz、偏振编码的光源组件全部集成在 4.8 × 3 mm^2 的硅光芯片上，并实验实现了 36dB 成码率 31bps[104]。

在 QKD 与 PQC 结合方面，2020 年，由中国科学技术大学、上海交通大学、国科量子通信网络有限公司、科大国盾量子技术股份有限公司等单位组成的联合团队，提出并验证了 PQC+QKD“混合型”量子

安全密码具体解决方案[105]。该方法结合成熟的公钥基础设施（PKI）可以方便地实现对 QKD 经典信道的认证，并保证了认证过程具有 PQC 算法的抗量子计算安全性。实验中成功验证了基于 PQC 算法的认证在 QKD 中继网络和全通网络的应用，并最终实现了基于 PQC 认证的 10 用户 QKD 网络的演示。

在量子随机数研究领域，2015 年 6 月，中国科学技术大学团队实验实现了 68 Gbps 的高速量子随机数发生器[106]，创造了当时的世界最快量子随机数产生记录。2017 年 12 月，中国网安刷新了这一纪录，极限速率突破 117 Gbps[107]。2018 年 9 月，中国科学技术大学团队在国际上首次成功实现“器件无关的量子随机数”生成[108]。这项突破性成果将在数值模拟和密码学等领域得到广泛的应用，有望形成新的随机数国际标准。

2.2 主要产品

经过十几年的产业化发展，以 QKD 技术为核心的量子密码产品已经初步形成了终端设备、网络设备、应用设备到应用软件等的产品体系。

（1）QKD 终端

QKD 终端用于建立点对点的量子密钥分发链路，以使用诱骗态 BB84 协议的设备最为成熟。经过几代发展已经实现多方面的应用指标：在距离上，既有满足城域通信的经济型终端，也有满足干线部署需求的百公里级高速终端；在可靠性方面，最成熟的商用产品已经达

到平均无故障时间大于 2 万小时；在安全性方面，由学术界、企业和行业测评机构联合研究的安全测评理论和工具逐渐完备；在可用性方面，与经典通信光纤的复用融合已经实现，小型化适合集成的终端已经形成原型机，特别是 2020 年实现了芯片化终端验证的突破，中国科学技术大学和科大国盾量子技术股份有限公司联合实现了 MDI-QKD 系统的发射终端芯片，在 4.8×3 平方毫米硅光子芯片上集成了 QKD 所需的所有光学调制组件并完成了百公里试验验证[109]。

（2）网络设备

量子密钥分发网络设备主要用于将点对点的 QKD 链路连接、交换构成网络。目前主要有 3 种设备：第一种是对量子信道进行交叉连接的光交换，通过波分复用器或者光开关实现，这种交换不影响 QKD 密钥的安全性，主要应用于短距离、小范围的交换；第二种是对密钥链路进行中继或交换，通过“一次一密”的密钥中继实现，并且通过即时中继、网络隔离、物理防护等手段保障密钥的安全性，主要用于长距离骨干线路的拓展和交换；第三种是将两种方案融合，结合网络控制、路由控制和服务策略，显著提升多终端汇聚接入的经济性和灵活性。实际上还有一些拓展的特殊网络设备，例如量子加密路由器，它将量子密钥与经典网络设备融合，同时实现了经典通信的加密和路由交换功能，这种设备已经投入应用；又例如基于 MDI-QKD 的星型网络中，其探测节点构成了网络的交叉连接中心，但由于技术不够成熟，主要还在实验研究中。

（3）应用设备

基于 QKD 网络生成的对称密钥可以实现高速加密通信，由此形成了一系列应用设备。最基础的应用设备是结合 QKD 终端实现的加密通话/视频通话、电报、传真等设备，同时也有和特殊业务结合的应用设备，例如量子安全金融密码机、量子安全 VPN 等，这些应用设备在 QKD 的支持下，通过快速更换密钥提升了原有业务的安全性。另外，为了安全性保障拓展到移动应用场景，目前也发展出了基于密钥存储携带的拓展应用模式和设备，包括便携的密钥存储器如量子密钥 U 盾/TF 卡/SIM 卡、移动加密终端如量子安全手机、密钥充注设备和后台的密钥安全服务系统。在这些拓展应用中，很明显地体现了 QKD 密钥即时生成带来的管理便捷性和安全性。

（4）应用软件

在加密通信的基础上，下游行业也已经开展了一些上层应用的探索和尝试。例如针对云和数据中心场景，已经研究了针对海量数据存储、云上业务处理等的安全解决方案和应用软件系统，已经部分用于阿里巴巴等的若干数据中心。另外，在医疗大数据领域的应用、与区块链/PQC 等结合的应用也正在研究中。总体来看，上层应用的研究属于刚刚起步，还有巨大的想象和发展空间。

2.3 技术专利

根据 2020 年 11 月 11 日对国际专利数据库的统计结果[1]，全球量子通信领域公开的同族专利数量排名前十位的专利申请人[2]如图 4-2 所示。其中，以科大国盾量子技术股份有限公司为代表的 7 家中国机构的专利数量约占前 10 位申请人的专利总量的 73%，说明我国在量子通信领域的创新能力和技术竞争实力较强。前 10 位专利申请人还包括日本东芝公司、日本电气株式会社（NEC）和日本电报电话公司（NTT）。其中，日本东芝公司的专利数量位居第二，是我国量子通信领域相关企业在国际上的主要竞争对手。

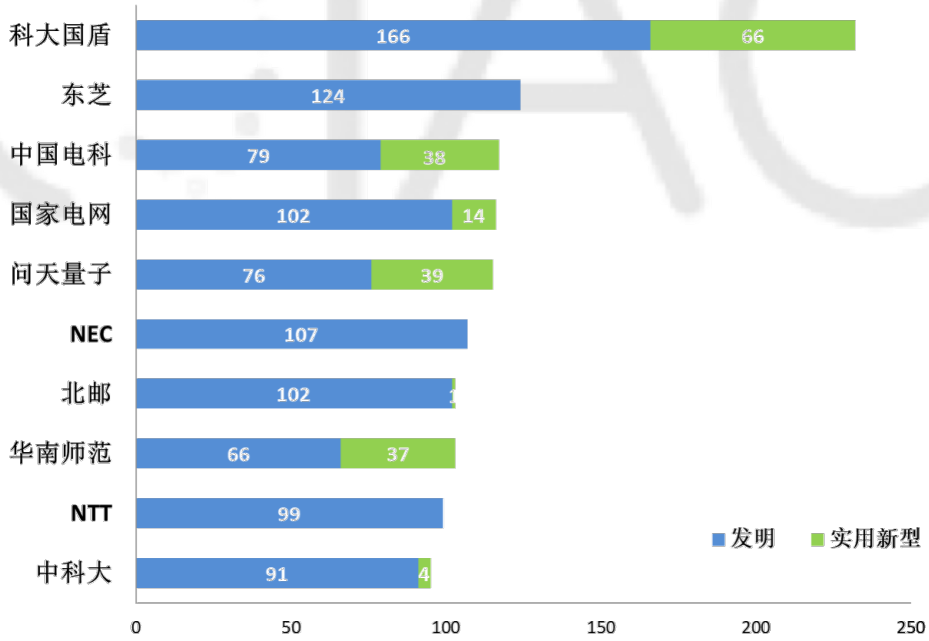

图 4-2 全球量子通信领域专利申请人排名

[1]通过关键词结合中国科学技术大学德温特数据库手工代码进行检索统计，仅供趋势性参考。
[2] 对申请人及其全资和控股子公司的专利数量进行了合并统计，专利数量相同的申请人按发明专利数量进行排序。

3. 量子密码技术的标准和测评

3.1 国际电信联盟（ITU-T）标准

联合国下属的国际电信联盟电信标准化部门（ITU-T）从 2018 年开始对 QKD 进行标准研究和制定工作。SG13 和 SG17 工作组已启动有关 QKD 网络方面和安全性方面的 19 个工作项目，如附录 1.1 所示。工作组已经定义了基于分层模型的典型 QKD 网络体系架构，此外，QKD 网络的密钥管理、网络控制、网络管理、网络安全要求等一系列标准化工作也正在进行。目前 ITU-T 已发布或通过的国际标准已有 8 项，中国团队主导和参与 QKD 网络功能架构、QKD 可信中继安全要求等多项重要标准研制，是 ITU-T QKD 网络标准化工作的重要推动力量。

2019 年 9 月，国际电信联盟电信标准局成立了“面向网络的量子信息技术”焦点组（Focus Group on Quantum Information Technology for Networks，FG-QIT4N），由中、美、俄三国专家共同担任联合主席。它是国际上首个涵盖量子计算、量子通信、量子精密测量、量子信息网络的量子信息技术标准研究组。焦点组的主要任务是研究量子计算、量子通信等量子信息技术如何服务于网络，特别是推动 QKD、量子计算等量子信息技术与信息通信技术（ICT）领域的融合发展及未来量子网络的演进等。其主要目标是组织和协调国际电联内部标准化研究工作，并协调其他标准化组织，构建全球量子信息标准化开放平台，推动标准化工作高效、有序开展。自成立开始，焦点组已召开 6 次会议，吸引了来自全球的量子信息相关领域技术专

家，在量子计算、QKD 网络、量子精密测量等方面产出了丰富的研究成果。ITU-TFG-QIT4N 的相关标准化项目情况参见附录 1.1。

3.2 国际标准化组织/国际电工协会（ISO/IEC）标准

2017 年，中国信息安全测评中心、科大国盾量子技术股份有限公司、中国科学技术大学等联合在 ISO/IEC JTC 1/SC 27 WG3 工作组发起了针对 QKD 设备安全测评技术的标准研究工作。经过一年的标准预研，WG3 工作组认可了该项工作的重要性，并于 2019 年正式立项量子密钥分发安全要求、测试和评估方法的标准项目，如附录 1.2 所示。该项目由中国牵头，担任标准主编，英国、新加坡、卢森堡等国参与，担任联合主编。项目的主要任务是编制 QKD 系统的安全要求和测评评估方法技术规范，为 QKD 系统的安全测评工作提供依据和指导。

3.3 欧洲电信标准协会（ETSI ISG-QKD）标准

ETSI 于 2008 年发起了有针对 QKD 技术的行业规范小组（Industry Specification GrouponQKD，ISG-QKD）。到 2019 年为止，ETSI ISG-QKD 已发布了 9 项有关 QKD 的规范，仍有 5 项标准工作项目正在推进，如附录 1.3 所示。 ISG-QKD 开展的工作主要研究 QKD 光学组件、模块、内部和应用程序接口以及实用安全性等。近期，ETSI 开始了对 QKD 网络体系结构和安全测评方面的研究，启动了《QKD 网络架构研究报告》和《基于通用评估标准（Common Criteria）的 QKD 安全防护行规（Protection Profile）》两项标准研制工作。

3.4 国内标准化工作

中国通信标准化协会（CCSA）于 2017 年成立了量子通信与信息技术特设任务组（ST7），对量子通信技术与量子通信网络、与量子通信相关的量子计算技术以及通用量子信息关键器件展开研究。到目前为止，CCSA 已经开展了 32 个 QKD 标准项目。国家标准《量子保密通信应用场景与需求》以及《量子密钥分发(QKD)系统测试方法》、《量子密钥分发(QKD)系统技术要求 第 1 部分:基于 BB84 协议的 QKD 系统》、《基于 BB84 协议的量子密钥分发（QKD）用关键器件和模块第 3 部分：量子随机数发生器（QRNG）》等三项行标已通过并进入报批阶段，已完成 8 项研究报告，包括《量子保密通信网络架构研究》、《量子密钥分发安全性研究》、《量子保密通信系统测试评估研究》、《量子密钥分发与经典光通信系统共纤传输研究》、《量子随机数制备和检测技术研究》等，详见附录 1.4。此外，密码行业标准化技术委员会也展开了 8 项 QKD 标准项目研究，内容涵盖 QKD 系统检测、量子保密通信中继安全、QKD 技术规范等等，其中 2 项已结题，见附录 1.5。作为 QKD 技术的潜在应用领域，电力行业对 QKD 展开了 3 个标准研究项目，已经发布了 2 项与电力量子保密通信系统相关的技术标准，见附录 1.6。

3.5 QKD 系统和网络测评

测试和评估对于新兴技术的市场营销和产业发展至关重要。当潜在用户计划购买点对点的 QKD 系统或部署 QKD 网络时，他们需要知道

该网络将满足其可用性和安全性需求。测试和评估工作将为用户提供功能、性能和安全性方面的 QKD 系统和 QKD 网络验证。这是连接系统供应商和最终用户以建立完整的产业链的重要链接。

测试和评估需要标准化的支持。技术规范标准可以为市场上不同类型的 QKD 系统提供基本的功能、性能和安全性要求。测评技术标准可以提出统一的测试环境，测试步骤以及通过/失败标准，以评估上述要求是否得到满足。因此，对 QKD 系统和网络进行标准化研究对于促进测试和评估工作的发展及其产业发展将具有重要意义。

ISO/IEC JTC 1/SC 27 WG3 工作组正在编制的 ISO/IEC 23837 标准对 QKD 系统的安全测评技术提供了严格的通用框架和方法。该标准基于国际上广泛使用的 Common Criteria（CC）模型，详细描述了 QKD 系统所需要具备的安全要求，并提出了相应的测试和评估方法。基于该通用框架，测评机构可以对运行不同协议的 QKD 系统制定针对性的测试方法，从而使得最终的测评方案可行且有效。

密钥管理等 QKD 网络其他方面的测评可以主要参考传统密码和通信技术和的测评方法。ITU-T SG17 组研制的 QKD 密钥管理、可信中继等技术的安全要求标准也提供了丰富的技术指导，可以作为测评依据。随着相关标准日渐完善和 QKD 测评工作经验的不断积累，QKD 测评技术将趋于成熟。

4. 量子密码攻防技术

经过全球学术界三十余年的共同努力，QKD 的理论安全性[110，111]和现实条件下的安全性都已经建立起来[112]。

在现实条件下，受器件加工工艺、设备成本等因素的影响，实际设备的性能参数和 QKD 理论安全模型的要求之间存在一定的偏差，这些设备非理想性所导致的偏差就为攻击者实施量子黑客攻击提供了可能。事实上，量子攻防的研究一直伴随 QKD 的产业化进程。黑客攻防的研究最早可以追溯到 1992 年的第一个 QKD 实验[113]，当时受器件的影响，不同探测器响应不同偏振态时会发出不同的声音，此时攻击者就可以通过“声音”这一侧信道来实现密钥的获取。随着探测器工艺的完善，这一问题目前已被很好的解决。随后，2000 年左右，研究者又发现 QKD 系统所采用的弱激光脉冲可能存在光子数分离攻击[114，115]（弱激光脉冲中存在多光子脉冲，攻击者就可以分离一个光子，然后待通信双方公布经典数据后再进行测量），随后清华大学王向斌教授和多伦多大学的 H.K.Lo 教授独立发展了诱骗态方法[53，54]，从而很好的解决了该问题，目前诱骗态方法已经是保证 DV-QKD 安全性的标准方法。

通过多年的研究，研究者已经发现了一系列针对实际 QKD 系统的量子黑客攻击方案，同时也对这些量子黑客攻击提出了相应的防御措施来提高 QKD 的实际安全性，附录表 2-1 和附录表 2-2 分别列出了目前主要的量子黑客攻击方案以及对应的防御措施。因此，量子黑客攻击的主要目标不仅仅是发现 QKD 系统的潜在安全性漏洞，更重要的是

研究如何通过系统参数监控或方案修改来提高 QKD 系统在实际条件下的安全性，同时为 QKD 测评标准的建立提供重要的参考和支撑。

5. 量子密码技术的产业生态

经过多年的技术积累和项目实践，我国已经形成了以 QKD 技术为核心的较为完整的量子保密通信产业链（如图 4-3 所示），自上而下分为基础器件、核心量子设备研制、量子应用设备研制、集成及应用技术、建设及运营服务、行业用户六个部分。其中，基础器件包括量子光源、单光子探测器件、频率转换器件、光学调制器件、电子学调制器件、量子随机数发生器等关键器件；核心设备包括 QKD 终端、光量子交换机、信道复用设备、量子密钥管理机、可信中继器、量子中继器等等；量子应用设备包括量子安全 VPN、量子安全路由器、量子安全 OTN、量子安全加密机等；集成及应用技术包括量子安全传输、量子安全认证、量子安全存储等解决方案；建设及运营服务包括量子保密通信网络建设、量子保密通信网络管理、量子保密通信网络运营等方面；行业用户涵盖国防、金融、政务、能源、电网等等。

近几年来，QKD 系统硬件已经可以从全球许多供应商处购买到。其中的代表性企业有中国的科大国盾量子技术股份有限公司、安徽问天量子科技股份有限公司、上海循态信息科技有限公司、浙江九州量子信息技术股份有限公司、北京中创为量子通信技术股份有限公司等，瑞士的 IDQuantique 公司，德国的 InfiniQuant 公司，美国的 MagiQ 公司和 Qubitekk 公司，澳大利亚的 Quintessence Lab 公司，以及英

国的东芝欧洲研究有限公司等。此外，许多大型公司也有活跃的 QKD 研发小组，例如日本 NTT、NEC、富士通、三菱电机等。

同时，量子保密通信产业链的上下游生态也逐渐健全起来。上游关键器件等我国已经基本实现自主可控。例如单光子探测器件的核心近红外单光子雪崩二极管，由于我国 QKD 技术领域的提前布局攻关，目前已经有一些单位如中国电子科技集团重庆声光电有限公司、武汉光讯科技股份有限公司等能够量产性能媲美国外产品的雪崩管；光学调制器件的研发生产、芯片化集成基本上也处于国际先进水平；还存在一定差距的主要是极高性能集成电路，虽然短期内还没有成为瓶颈，但产业链上游仍需要尽早布局。中下游领域的发展国内外都是方兴未艾。国内外电信运营商如中国电信、中国联通、中国移动、韩国 SKT、韩国 KT、韩国 LGU+、英国电信、德国电信、西班牙电信等，以及新兴量子网络公司如我国的国科量子通信网络有限公司、美国的 QuantumXchange 等都在量子保密通信基础设施建设、应用试点示范以及技术标准化方面积极发力。平台服务企业、终端服务企业和行业用户也已经开始应用模式的研究和实践，云和大数据服务、政务信息保护、金融业务加密、电力安全保障等已经率先试水并推出相关产品，围绕量子技术的安全产业生态已初露端倪。

协同创新是产业链和生态发展的核心关键。例如欧洲学术界、工业及初创企业联合提出 OPENQKD 计划，合作在欧洲各地部署开放测试基地，促进产业界对 QKD 技术的认识和参与。这个庞大计划建设的平台覆盖了光纤和星地网络基础设施、云和数据中心场景、电信网络融

合架构、B2B 网络中的 5G 融合、攻防与测评、信息安全理论和认证、各应用行业模式规范等；其他典型的协同创新如韩国 SKT、三星与瑞士 IDQ 等合作研发的基于量子随机数芯片的量子安全手机等。

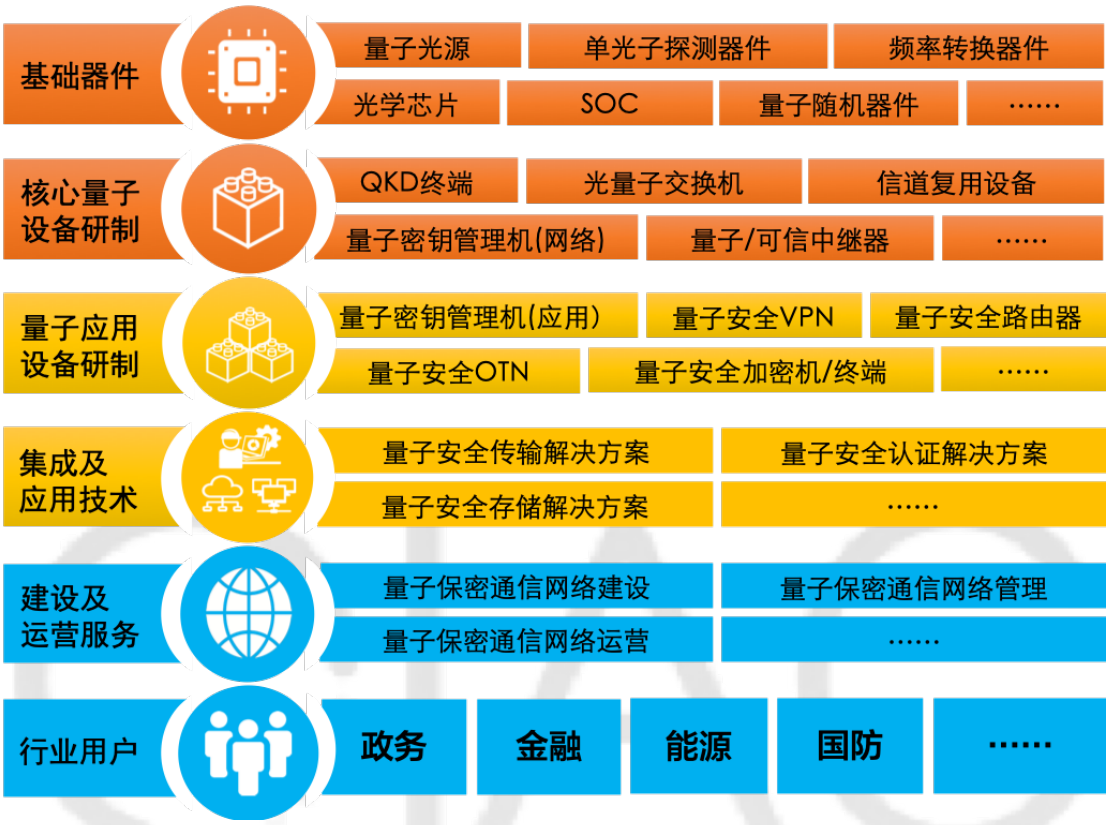

图 4-3 量子保密通信产业链

五、量子安全技术面临的挑战

从 1994 年 Peter Shor 发现能够快速分解大数质因子的量子算法以来，量子信息技术就一直以其创造人类福祉和威胁既有信息安全的双面性而广受关注。当前，量子信息技术已经成为全球主要国家发展战略和安全战略的关注焦点，围绕该技术领域的全球性竞争也已经展开。可以说，量子信息技术受重视程度之高、发展速度之快前所未有。量子安全技术是量子信息技术发展中的重要领域，也是新一代密码技术发展的重要方向。它是量子物理和信息技术以及密码技术的融合和创新。受益于人类量子调控能力的进步，今日，在量子信息领域所取得理论和技术进展，已经使得人们开始确切地感受到信息安全面临的“量子威胁”。这为量子安全技术的发展带了重大的机遇。然而，量子安全技术本身还面临着一些艰巨的挑战。

1. 量子安全技术的可信度

到目前为止，量子安全技术还没有经受实战的考验。对于 PQC 而言，NIST 的标准征集工作是一次发展契机。经过 NIST 遴选的 PQC 方案将受到一定程度的安全分析和攻防验证，原则上将具有较好的可信度；而未通过 NIST 遴选的 PQC 方案，其发展则可能受到挫折。然而，仍然需要指出，即便是从经典密码分析角度而言，对于 PQC 的安全性

理解仍然是任重道远。从另一个方面上来说，相比于从事经典密码分析专家的数量，具有密码分析的经验，又能够深入理解量子计算的专家十分稀缺。因此，对于 PQC 算法的量子攻击分析也许也并不充分。严格地说，PQC 算法的抗量子性是基于格和编码等底层数学问题的量子困难性假设，这一假设还有待时间的检验。

对于 QKD 等量子密码技术而言，关于其安全性诸如信息论安全性、长期的前向和后向安全性的理论证明较为完备，安全可信度问题主要存在于具体实现技术上物理安全的检验验证。目前，对于物理器件性能偏差或缺陷所导致的 QKD 安全漏洞的攻防研究和实际演练已经展开，但相关的评估、评测研究以及标准化还不够充分，尚需进一步的工作。

2. 量子安全技术的效能和成本

无论是使用 PQC 还是 QKD 技术，都存在从现有系统迁移到新系统的成本问题。使用 QKD 技术，意味着要新建一套 QKD 系统、全面更换加密设备或者更新加密设备的接口以使用 QKD 分发的密钥。而使用 PQC 技术，则需要对于原有密码系统进行全面的软件更新和硬件更换。如果迁移成本过高，就会遏制用户使用量子安全技术的愿望。这个问题对于 QKD 技术来说较为明显，因为目前的 QKD 系统远比用于实现 PQC 的硬件设备昂贵。同时，QKD 系统的维护涉及到的技术领域要比仅基于电子元器件的密码机设备多，维护的技术难度和成本也可能更高一些。

3. 单一解决方案的完整性

量子安全技术中单独的某一项技术有时不能构成完整的信息安全解决方案。这一问题对于 QKD 较为明显。因为 QKD 技术作为对称密码技术目前能比较好地解决加密和认证问题，基于一些对称密码签名技术，QKD 可以解决一部分应用场景下的签名问题。但是，对于最广泛的数字签名应用场景，目前 QKD 仍然没有好的解决途径。这一问题对于某些 PQC 算法也同样存在，例如，部分基于纠错码的 PQC 只能加密而不能签名，一些多变量 PQC 只能签名而不能加密。

4. 应用适应性

原则上说，要保障量子安全就必须在整个信息系统上都应用量子安全技术。因此，量子安全技术如何适配全系统中不同场景和不同设备形态并进行应用，也是需要解决的问题。对于 QKD 技术而言，这一问题更为明显。主要困难有三点：1）QKD 如何融合在电信网络中，实现中继和组网；2）QKD 如何适应无线通信，实现无线分发；3）QKD 如何小型化，以便适配各类终端设备。对于 PQC 技术而言，困难主要集中在如何减小算法复杂度和密钥规模，以便集成在轻量化设备中。

5. 国际化竞争

对于我国的量子安全技术发展而言，如何参与乃至把握国际竞争是一个重要的问题。这一问题在目前的形势下，格外复杂。这是由于地缘政治因素干预到了技术的竞争。相对而言，QKD 技术的国际竞争

形势要稍好一些。我国的 QKD 研究界和工业界在国际标准化组织中占据了一定的发言权，但也有被孤立的风险和倾向。对于 PQC 而言，这一问题比较严重。在国际标准化方面，我国的话语权较弱，存在被完全孤立的风险。

针对量子安全技术所面对的这些挑战，解决途径是明确的。解决途径包括：1)推动开展量子安全技术的攻防演练、测试评价等工作，建立体系化的技术标准；2)从完善产业链条出发，推动量子安全技术产品制造和使用成本的大幅减低；3）综合使用量子安全技术，建立异构化的完整技术解决方案；4）深入和加快推动量子技术的发展，发展量子中继、芯片化产品、共纤复用技术等拓展 QKD 的应用范围；发展和改进 PQC 算法，实现轻量化；5）加快量子安全技术应用，立足“大循环”和“双循环”，以市场引导标准，加强国际竞争力。

我们看到，近年来，我国在 QKD 技术的远距离、高速率、小型化、安全攻防以及标准化方面，在量子隐形传态、量子中继等面向未来量子网络的核心技术方面取得了一系列重大成果，在国际上处于暂时领先的地位；在与光通信基础设施及密码应用融合方面也在积极探索，并初步形成产业生态。在 PQC 领域，我国密码算法设计竞赛和标准化工作已经展开，除了大学和研究机构加大投入，一批致力于 PQC 应用的创新创业团队也在积极作为。我们也看到在 QKD 与 PQC 相结合的方向上，中国的科研和产业化团队已经迈出了他们的步伐。我们相信，通过对量子安全技术发展中一个个挑战的攻关，我国的量子信息技术、

密码技术以及新一代信息技术和相关产业将得到长足的发展，服务国家、造福社会。

附录 1 量子密钥分发技术标准化情况

附 1.1 国际电信联盟（ITU-T）标准

附录表 1-1. ITU-T QKD 标准项目

标准编号	标题	状态	工作组
Y.3800	支持量子密钥分发的网络概述 Overview on networks supporting quantum key distribution	2019 年 10 月通过，正式发布	SG13
Y.3801	量子密钥分发网络-功能要求 Functional requirements for quantum key distribution networks	2020 年 4 月通过，正式发布	SG13
Y.3802	量子密钥分发网络-功能架构 Quantum key distribution networks - Functional architecture	2020 年 12 月通过，待发布	SG13
Y.3803	量子密钥分发网络-密钥管理 Quantum key distribution networks - Key management	2020 年 12 月通过，待发布	SG13
Y.3804	量子密钥分发网络-控制与管理 Quantum Key Distribution Networks - Control and Management	2020 年 9 月通过，预发布	SG13
Y.QKDN_SDNC	量子密钥分发网络-软件定义网络控制 Software Defined Network Control for Quantum Key Distribution Networks	2021 年 7 月计划结项	SG13
Y.QKDN_BM	量子密钥分发网络-商业模型 Business role-based models in Quantum Key Distribution Network	2021 年 7 月计划结项	SG13
Y.QKDN_frint	量子密钥分发网络与安全网络基础设施融合框架 Framework for integration of QKDN and secure network infrastructures	2021 年 7 月计划结项	SG13
Y.QKDN-qos-req	量子密钥分发网络-服务质量保障要求 Requirements for QoS Assurance of the Quantum Key Distribution Network	2021 年 10 月计划结项	SG13
Y.QKDN-qos-gen	量子密钥分发网络-服务质量总体 General Aspects of QoS on the Quantum Key Distribution Network	2021 年 10 月计划结项	SG13
Y. QKDN-qos-arc	量子密钥分发网络-服务质量保障功能架构 Functional architecture of QoS assurance for quantum key	2021 年 12 月计划结项	SG13

标准编号	标题	状态	工作组
	distribution networks		
Y.QKDN-qos-ml-req	量子密钥分发网络-基于机器学习的服务质量保障要求 Requirements of machine learning based QoS Assurance for quantum key distribution networks	2022 年 7 月计划结项	SG13
X.1702	量子噪声随机数发生器架构 Quantum noise random number generator architecture	2019 年 11 月通过，正式发布	SG17
X.1710	量子密钥分发网络-安全框架 Security framework for quantum key distribution networks	2020 年 10 月通过，预发布	SG17
X.1714	量子密钥分发网络-密钥组合和加密密钥提供 Key combination and confidential key supply for quantum key distribution networks	2020 年 10 月通过，预发布	SG17
X.sec-QKDN-km	量子密钥分发网络-安全要求-密钥管理 Security requirements for quantum key distribution networks - key management	2021 年 1 月计划结项	SG17
X.sec-QKDN-tn	量子密钥分发网络-安全要求和设计-可信节点 Security requirements and designs for quantum key distribution networks - trusted node	2021 年 9 月计划结项	SG17
X.sec_QKDN_intrq	量子密钥分发网络与安全网络基础设施融合的安全要求 Security requirements for integration of QKDN and secure network infrastructures	2021 年 9 月计划结项	SG17
TR.sec-qkd	量子密钥分发网络的安全考虑研究报告 Security considerations for quantum key distribution network	2020 年 3 月通过，正式发布	SG17

附录表 1-2. ITU-T 面向网络的量子信息技术焦点组（FG-QIT4N）QKD 研究项目

编号	标题	状态
D2.1	量子密钥分发网络术语 QIT4N terminology part 2: quantum key distribution network	2021 年 12 月计划结项
D2.2	量子密钥分发网络应用 Technical report on the QIT4N use case part 2: quantum key distribution network	2021 年 12 月计划结项
D2.3	量子密钥分发网络协议 Technical report on QKDN protocols	2021 年 12 月计划结项

编号	标题	状态
D2.4	量子密钥分发网络传输技术 Technical report on QKDN transport technologies	2021 年 12 月计划结项
D2.5	量子密钥分发网络标准展望 Technical report on QIT4N standardization outlook and technology maturity part 2: quantum key distribution network	2021 年 12 月计划结项

附 1.2 国际标准化组织/国际电工协会（ISO/IEC）标准

附录表 1-3. ISO/IEC JTC1/SC 27 QKD 标准项目

标准编号	标题	状态
ISO/IEC 23837-1	Security requirements, test and evaluation methods for quantum key distribution Part 1: requirements	草案
ISO/IEC 23837-2	Security requirements, test and evaluation methods for quantum key distribution Part 2: test and evaluation methods	草案

附 1.3 欧洲电信标准协会（ETSI ISG-QKD）标准

附录表 1-4. ETSI QKD 标准项目

标准编号	标题	状态
GS QKD 002	Quantum Key Distribution (QKD); Use Cases	已发布
GR QKD 003	Quantum Key Distribution (QKD); Components and Internal Interfaces	已发布
GS QKD 004	Quantum Key Distribution (QKD); Application Interface	已发布
GS QKD 005	Quantum Key Distribution (QKD); Security Proofs	已发布
GR QKD 007	Quantum Key Distribution (QKD); Vocabulary	已发布
GS QKD 008	Quantum Key Distribution (QKD); QKD Module Security Specification	已发布

标准编号	标题	状态
GS QKD 010	Quantum Key Distribution (QKD); Implementation security: protection against Trojan horse attacks in one-way QKD systems	草案
GS QKD 011	Quantum Key Distribution (QKD); Component characterization: characterizing optical components for QKD systems	已发布
GS QKD 012	Quantum Key Distribution (QKD) Device and Communication Channel Parameters for QKD Deployment	已发布
GS QKD 013	Quantum Key Distribution (QKD); Characterisation of Optical Output of QKD transmitter modules	草案
GS QKD 014	Quantum Key Distribution (QKD); Protocol and data format of key delivery API to Applications;	已发布
GS QKD 015	Quantum Key Distribution (QKD); Quantum Key Distribution Control Interface for Software Defined Networks	草案
GS QKD 016	Common Criteria Protection Profile for QKD	草案
GR QKD 017	QKD Network Architectures	草案

附 1.4 中国通信行业标准

附录表 1-5. CCSAQKD 标准项目

标准编号	标题	状态	工作组
20181791-T-339	量子通信术语和定义	重新征求意见	ST7/WG1
20181799-T-339	量子保密通信应用场景和需求	工信部公示	ST7/WG1
2018-1646T-YD	量子密钥分发(QKD)系统技术要求 第 1 部分：基于 BB84 协议的 QKD 系统	工信部公示	ST7/WG1
2018-1739T-YD	量子密钥分发(QKD)系统测试方法	工信部公示	ST7/WG1
2018-1647T-YD	量子密钥分发(QKD)系统应用接口	重新征求意见	ST7/WG1
2019-1286T-YD	量子保密通信网络架构	起草阶段	ST7/WG1
2019-1287T-YD	量子密钥分发与经典光通信共纤传输技术要求	起草阶段	ST7/WG1& TC6 WG1

标准编号	标题	状态	工作组
2019-1283T-YD	基于 BB84 协议的量子密钥分发（QKD）用关键器件和模块 第 1 部分：光源	起草阶段	TC6/WG4&ST7/WG2
2019-1284T-YD	基于 BB84 协议的量子密钥分发（QKD）用关键器件和模块 第 2 部分：单光子探测器	起草阶段	TC6/WG4&ST7/WG2
2019-1285T-YD	基于 BB84 协议的量子密钥分发（QKD）用关键器件和模块 第 3 部分：量子随机数发生器（QRNG）	提交报批稿	ST7/WG2
2020-0581T-YD	量子密钥分发(QKD)设备安全要求 第 1 部分：基于诱骗态 BB84 协议的 QKD 设备	起草阶段	ST7/WG2
2020-0580T-YD	量子密钥分发（QKD）网络 密钥管理单元与 QKD 设备间接口要求	起草阶段	ST7/WG1
H-2020530181	基于 IPSec 协议的量子保密通信应用设备技术要求	起草阶段	ST7/WG1
H-2020530191	量子密钥分发网络 网络管理系统技术要求	起草阶段	ST7/WG1
2017-YDB-09	支持量子波道的 WDM 系统技术要求	通过标准征求意见稿	TC6 WG1&ST7/WG1
2018B68	连续变量量子密钥分发技术研究	重新征求意见	ST7/WG1
2018B67	量子保密通信网络可信中继节点技术研究	重新征求意见	ST7/WG1
2019B37	空间量子保密通信技术研究	重新征求意见	ST7/WG1
2019B39	基于诱骗态方法的优化协议研究	通过征求意见稿	ST7/WG2
2019B36	量子保密通信组网关键技术研究	起草阶段	ST7/WG1
2020B80	连续变量量子密钥分发系统测评研究	起草阶段	ST7/WG1
2018B69	软件定义的量子密钥分发网络研究	完成报批稿	ST7/WG1
2020B81	量子时间同步技术的演进及其在通讯网络中的应用研究	起草阶段	ST7/WG2
2019B38	量子保密通信网络中 MPLS 专线承载加密数据要求的研究	起草阶段	ST7/WG1
CCSA-SR 285-2019	量子随机数制备和检测技术研究	已发布，待印刷	ST7/WG2
2018B40	量子保密通信网络管理研究	通过送审稿	ST7/WG1

标准编号	标题	状态	工作组
CCSA-SR 284-2019	量子密钥分发安全性研究	已发布，待印刷	ST7/WG2
2017B66	量子保密通信网络架构研究	通过送审稿	ST7/WG1
CCSA-SR 244-2018	量子保密通信系统测试评估研究	已发布，待印刷	ST7/WG1
2017B64	量子密钥分发与经典光通信系统共纤传输研究	通过送审稿	ST7/WG1&TC6 WG1
2016B72	量子密钥分发技术及应用研究	完成报批稿	TC6 WG4
CCSA-SR 262-2019	量子密钥分发关键器件和模块技术要求研究	已发布，待印刷	TC6 WG4

附 1.5 中国密码行业标准

附录表 1-6. 密标委 QKD 标准项目

标准编号	标题	状态
暂无	诱骗态 BB84 量子密钥分发系统检测规范	预提交征求意见稿
暂无	基于量子密钥分发的加密通信技术体系框架研究	预提交征求意见稿
暂无	量子随机数制备和测试技术研究	预提交征求意见稿
暂无	量子保密通信中继安全性研究	预提交征求意见稿
暂无	基于量子密钥分配的网络密码机技术规范研究	结题
暂无	诱骗态 BB84 量子密钥分发系统测评规范研究	结题
暂无	诱骗态 BB84 量子密钥分配技术规范	结题
暂无	USB 接口安全保护技术规范研究	预提交征求意见稿

附 1.6 中国电力行业标准

附录表 1-7. 电力行业 QKD 标准项目

标准编号	标题	状态	工作组
TCSEE 0087.2—2018	电力量子保密通信系统 第 2 部分：VPN 网关设备	已发布	中国电机工程学会
TCSEE 0087.3—2018	电力量子保密通信系统 第 3 部分：网络工程验收	已发布	中国电机工程学会
暂无	电力量子保密通信系统密钥交互接口技术规范	起草阶段	电力行业标准化技术委员会（DL/TC 27）

附录 2 针对 QKD 实际安全性的攻击方案和防御措施

附录表 2-1：主要 DV-QKD 量子黑客攻击方案和防御措施

攻击名称	攻击目标	攻击器件	理论/实验	年份	防御措施
光子数分离攻击	源	多光子脉冲	理论	2000	诱骗态方法
探测荧光	探测	单光子探测器	理论	2001	光隔离器/光强监控
伪态攻击	探测	单光子探测器	理论	2005	光电流监控/安全性分析
特洛伊木马攻击	源/探测	器件背向反射	理论/实验	2006	光隔离器/光强监控/安全性分析
时间侧信道	探测	时间信息	实验	2007	安全性分析
时移攻击	探测	单光子探测器	实验	2007	信号监控/安全性分析
相位重映射	源	相位调制器	实验	2010	时序监控/调制门宽设置
探测器致盲	探测	单光子探测器	实验	2010	光电流监控
探测器致盲	探测	单光子探测器	实验	2011	光电流监控
探测器致盲	探测	超导探测器	实验	2011	光电流监控
法拉第镜	源	法拉第镜	理论	2011	修改光路结构
波长攻击	探测	分束器	实验	2011	光隔离滤波/安全性分析
死时间攻击	探测	探测器	实验	2011	死时间设置
信道标定	探测	探测器	实验	2011	标定流程监控
强度攻击	源	强度调制器	实验	2012	光强监控
相位随机化	源	相位随机化	实验	2012	主动相位调制/相位监控
存储攻击	探测	经典存储器	理论	2013	信号监控/安全性分析
激光损伤	探测	探测器	实验	2014	光强监控
激光注入	源	激光器	实验	2015	光隔离/光强监控
隐信道攻击	探测	经典存储器	理论	2017	安全性分析
码型效应	源	强度调制器	实验	2018	安全性分析

注：上表中“安全性分析”是设备的缺陷参数能够被纳入 QKD 安全模型中予以解决。

附录表 2-2：主要 CV-QKD 量子黑客攻击方案和防御措施

攻击名称	攻击目标	攻击器件	理论/实验	年份	防御措施
非理想光源攻击	源	态制备	理论	2013	调制修正
本振光波动攻击	探测	本振光	理论	2013	本振光监控/本地本振
本振光校准攻击	探测	本振光	理论	2013	本振光监控/本地本振
波长攻击	探测	探测器	理论	2013	波长监控/安全性分析
特洛伊木马攻击	源	调制器	理论	2014	光隔离/光强监控/安全性分析
零差探测器饱和攻击	探测	平衡探测器	实验	2016	光电流监控/数据分布检测
参考脉冲攻击	探测	本振光	理论	2017	本振光监控/本地本振
偏振攻击	探测	本振光	理论	2018	本振光监控/本地本振
零差探测器致盲攻击	探测	探测器	实验	2018	光电流监控/数据分布检测
激光器种子攻击	源	激光	理论	2019	光隔离器/光强监控
光衰减攻击	源	衰减器	理论	2019	光隔离器/光强监控

注：上表中“安全性分析”是设备的缺陷参数能够被纳入 QKD 安全模型中予以解决。

附录 3 缩略语

简称	全称	中文含义
ABE	Attribute-Based Encryption	基于属性加密
AES	Advanced Encryption Standard	高级加密标准
ATM	Automated Teller Machine	自动取款机
AW	Alabbadi and Wicker	一种基于 hash 函数的签名方案
B92	Bennett 1992	B92 协议
BB84	Bennett and Brassard 1984	BB84 协议
BBM92	Bennett, Brassard and Mermin 1992	BBM92 协议
BCH	Bose, Ray-Chaudhuri and Hocquenghem	一种纠错编码方法
BKW	Blum，Kalai，and Wasserman	人名首字母缩写组合
CA	Certificate Authority	认证中心
CC	Common Criteria	通用评估准则
CCSA	China Communications Standards Association	中国通信标准化协会
CFS	Courtois, Finiasz, and Sendrier	一种基于纠错码的签名方案
CMS	Cryptographic Message Syntax	加密消息语法
COW	Coherent One Way	相干单向
CV-QKD	Continuous-Variable QKD	连续变量量子密钥分发
DH	Diffie-Hellman	Diffie-Hellman 密钥协商算法的简称
DoD	United States Department of Defense	美国国防部
DPR	Distributed Phase Reference	分布式相位参考
DPS	Differential phase shift	差分相移
DSA	Digital Signature Algorithm	数字签名算法
DSS	Digital Signature Standard	数字签名标准，美国政府指定的数字签名算法的一种标准
DV-QKD	Discrete-Variable QKD	离散变量量子密钥分发
E91	Ekert 91	E91 协议
ECC	Elliptic Curve Cryptography	椭圆曲线密码算法
ECDH	Elliptic Curve Diffie–Hellman	椭圆曲线密钥交换
ECDSA	Elliptic Curve Digital Signature Algorithm	椭圆曲线数字签名算法

简称	全称	中文含义
ECP	Encryption Control Protocol	加密控制协议
ETSI	European Telecommunications Standards Institute	欧洲电信标准化协会
EuroQCI	the European Quantum Communication Infrastructure	欧洲量子通信基础设施
FE	Functional Encryption	功能加密
FG-QIT4N	Focus Group on Quantum Information Technology for Networks	“面向网络的量子信息技术”焦点组
FIPS	Federal Information Processing Standard	美国联邦信息处理标准
FTP	File Transfer Protocol	文件传输协议
GG02	Grosshans and Grangier, 2002	GG02 协议
HFE	Hidden Field Equations	隐藏域方程
HMAC	Hash-based Message Authentication Code	基于杂凑的消息认证码算法
HTTP	Hypertext Transport Protocol	超文本传输协议
HTTPS	Hyper Text Transfer Protocol over SecureSocket Layer	超文本传输安全协议
ICT	Information and Communications Technology	信息通信技术
ID	Identity Document	身份标识号
IDEA	International Data Encryption Algorithm	国际数据加密算法
IEC	International Electrotechnical Commission	国际电工协会
IEEE	Institute of Electrical and Electronics Engineers	电气和电子工程师协会
IKE	Internet Key Exchange	网络密钥交换协议
IP	Isomorphism of Polynomials	多项式同构
IPSec	Internet Protocol Security	互联网安全协议
IPHFE	Internal Perturbation of HFE	内部扰动隐藏域方程
ISG-QKD	Industry Specification Group on QKD	针对 QKD 技术的行业规范小组
ISO	International Organization for Standardization	国际标准化组织
ITU	International Telecommunication Union	国际电信联盟
LD-OTS	Lamport-Diffie OTS	Lamport-Diffie 一次签名方案
LPN	Learning Parity with Noise	带噪声奇偶学习

简称	全称	中文含义
LWE	Learning With Errors	错误学习问题
MAC	Message Authentication Codes	消息认证码
MDI-QKD	Measurement Device Independent QKD	测量设备无关量子密钥分发
MLWE	Module Learning With Errors	模错误学习问题
MLWR	Module Learning With Rounding	深度模学习？
MQ	Multivariate Quadratic	多变量二次多项式方程组
MSS	Merkle Signature Scheme	Merkle 认证树签名方案
MI	Matsumoto-Imai	人名首字母缩写
MIME	Multipurpose Internet Mail Extensions	多用途互联网邮件扩展类型
M2M	Machine to Machine	机器对机器
NSA	National Security Agency	美国国家安全局
NEC	Nippon Electronic Company	日本电气株式会社
NESSIE	New European Schemes for Signature, Integrity and Encryption	欧洲新的签名、完整性和加密方案
NISQ	Noisy Intermediate-Scale Quantum	中型含噪量子计算
NIST	National Institute of Standards and Technology	美国国家标准与技术研究院
NP	Non-deterministic Polynomial	非确定性多项式
NSS	NTRU Signature Scheme	一种签名算法
NTRU	Number Theory Research Unit	一种公钥加密算法
4562NTT	Nippon Telegraph & Telephone	日本电报电话公司
OID	Object Identifier	对象标识
OSI	Open System Interconnection Reference Model	开放互联系统
OTN	Optical Transport Network	光传送网
OTP	One-time-pad	一次性密码本
OTS	One-time Digital Signature	一次性签名方案
PCIDSS	Payment Card Industry Data Security Standard	支付卡行业数据安全标准
PKI	Public Key Infrastructure	公钥基础设施
PM-QKD	Phase Matching QKD	相位匹配量子密钥分发
PoW	Proof of Work	工作量证明
PPP	Point to Point Protocol	点对点协议

简称	全称	中文含义
PQC	Post Quantum Cryptography	后量子密码
PSS	Probabilistic Signature Scheme	概率签名方案
QC-MDPC	Quasi-Cyclic Moderate Density Parity-Check Codes	准循环中密度奇偶校验码
QIA	Quantum Internet Alliance	量子互联网联盟
QKD	Quantum Key Distribution	量子密钥分发
QRC	Quantum Resist Cryptography	抗量子计算密码
QRL	The Quantum Resistant Ledge	抗量子账簿
QRNG	Quantum Random Number Generators	量子随机数发生器
QROM	Quantum Random Oracle Model	量子随机预言机模型
QSC	Quantum Safe Cryptography	量子安全密码
RFID	Radio Frequency Identification	射频识别
RRDPS	round-robin DPS	循环差分相移
RS	Reed-Solomon	一种前向纠错的信道编码方案
RSA	Ron Rivest, Adi Shamir, Leonard Adleman (algorithm)	RSA 算法
SA	Security Association	安全联盟
SARG04	Scarani, Acin, Ribordy, and Gisin 2004	SARG04 协议
SCADA	Supervisory Control And Data Acquisition	数据采集与监控系统
SIKE	Supersingular Isogeny Key Encapsulation	超奇异同源密钥封装
SMTP	Simple Mail Transfer Protocol	简单邮件传输协议
SSH	Secure Shell	安全外壳协议
SSL	Secure Sockets Layer	安全套接层
SWIFT	Society for Worldwide Interbank Financial Telecommunications	环球同业银行金融电讯协会
TCP/IP	Transmission Control Protocol/Internet Protocol	传输控制协议/互联协议
TF-QKD	Twin-field QKD	孪生场量子密钥分发
TLS	Transport Layer Security	传输层安全协议
TSN	Time Sensitive Network	时间敏感网络
TTM	Tamed Transformation Method	一种多变量公钥加密方案
TTS	Tamed Transformation Signature	一种多变量公钥加密方

简称	全称	中文含义
		案
UOV	Unbalanced Oil and Vinegar	不平衡油醋
VoLTE	Voice over Long-Term Evolution	长期演进语音承载
VPN	Virtual Private Network	虚拟专网
WAN	Wide Area Network	广域网
WLAN	Wireless Local Area Network	无线局域网
XL	eXtended Linearization	扩展线性化
ZUC	ZUC stream cipher algorithm	祖冲之流密码算法

参考文献

[1]. 道格拉斯 R.斯廷森著,冯登国译.密码学原理与实践（第三版），北京：电子工业出版社，2016.

[2]. 量子信息和量子技术白皮书（合肥宣言）.新兴量子技术国际会议,中国合肥, 2019.9.

[3]. Frank Arute, Kunal Arya, Ryan Babbush, et al., Quantum supremacy using a programmable superconducting processor, Nature, 574: 505-510(2019).

[4]. Han-Sen Zhong, Hui Wang, Yu-Hao Deng, et al., Quantum computational advantage using photons, *Science*, 10.1126/science.abe8770(2020).

[5]. Lily Chen, Stephen Jordan, Yi-Kai Liu, et al. Report on Post-Quantum Cryptography. NIST.IR.8015(2016).

[6]. Matthew Campagna, Lidong Chen, Dr Özgür Dagdelen, et al. Quantum Safe Cryptography and Security: An introduction, benefits, enablers and challenges. *ETSI White Paper* No.8，2015.6.

[7]. Grover, L., A fast quantum mechanical algorithm for database search, 28th ACM Symposium on the Theory of Computing p. 212-219(1996).

[8]. Shor, P., Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, *SIAM Journal of Computing,* 26(5):1484-1509(1997).

[9]. Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, et al. The security of practical quantum key distribution, *Reviews of Modern Physics*, 81, 1301(2009).

[10]. Information technology–Open Systems Interconnection–The Directory: Public-key and attribute certificate frameworks.Recommendation ITU-T X.525 (2019) | ISO/IEC 9594-8(2019).

[11]. M. Mosca, Setting the Scene for the ETSI Quantum-safe Cryptography Workshop, e-proceedings of “1st Quantum-Safe-Crypto Workshop”, Sophia Antipolis, Sep 26-27(2013).

[12]. 张焕国，王后珍等译. 抗量子计算密码. 北京：清华大学出版社, 2015.02.

[13]. Ajtai M,Generating hard instances of lattice problems.Proc. of *ACM Symposium on Theory of Computing 1996*,New York:ACM, p99-108(1996).

[14]. Ajtai M,Dwork C,A public-key cryptosystem with worst-case/ average-case equivalence.Proc. of *ACM Symposium on Theory of Computing 1997*. New York:CM, p284-293(1997).

[15]. Hoffstein J, Pipher J, and Silverman J H.NTRU:A ring-based public key cryptosystem.LNCS 1423: Proc. of *International Algorithmic Number Theory Symposium*.Berlin:Springer, p267-288(1998).

[16]. Hoffstein, J., Pipher, J., and Silverman, J.H. NSS: An NTRU Lattice-Based Signature Scheme. I*n Advances in Cryptology-ENCRYPT*, 2045:211–228(2001).

[17]. Hoffstein, J., Graham, N.A.H., Pipher, J., Silverman, J.H., Whyte, W.NTRUSIGN: Digital signatures using the NTRU lattice. In Proc. of CT-RSA, *Lecture Notes in Compuer Science*, 2612: 122-140 (2003).

[18]. Gentry C.Fully homomorphic encryption using ideal lattices.Proc. of *ACM Symposium on T heory of Computing 2009*,New York:ACM, p169-178(2009).

[19]. 张平原，蒋瀚等. 格密码技术近期研究进展.*计算机研究与发展*, 54(10):2121-2129(2017).

[20]. 王小云，刘明洁. 格密码学研究. *密码学报*,1(1):13-27(2014).

[21]. Peikert C, A decade of lattice cryptography． *Foundations and Trends in Theoretical Computer Science*,10(4):283-424(2016).

[22]. McEliece, R., A public key cryptosystem based on algebraic coding theory. *DSN progress report*, 42-44:114-116 (1978).

[23]. Berlekamp, E., McEliece, R., and van Tilborg, H., On the inherent intractability of certain coding problems. *IEEE Transactions on Information Theory*, 24(3):384–386 (1978).

[24]. Gibson, K., Equivalent Goppa codes and trapdoors to McEliece's public key cryptosystem. In D.W. Davies, editor, Advances in Cryptology-Eurocrypt 1991, *Lecture Notes in Computer Science*, 547: 517-521 (1991).

[25]. Niederreiter, H., Knapsack-type cryptosystems and algebraic coding theory. *Problems of Control and Information Theory*, 15:19-34 (1986).

[26]. Xing-LiYuan,R.H.Deng,Xin-Mei Wang, The equivalence of McEliece's and Niederreiter's public-key cryptosystems. *IEEE Transactions on Information Theory*, 40: 271-273 (1994).

[27]. R. Misoczki and P. S. L. M. Barreto. Compact McEliece keys from Goppa codes. In Selected Areas in Cryptography (SAC 2009), Calgary, Canada, 2009.08.13-14.

[28]. Jean-Charles Faugere, Ayoub Otmani, Ludovic Perret, et al., Algebraic cryptanalysis of McEliece variants with compact keys. http://crypto.rd.francetelecom.com/ events/eurocrypt2010/papers

[29]. Xin-Mei Wang, Digital signature scheme based on error-correcting codes. *Electronics Letters*, 26(13):898–899 (1990).

[30]. Zhen-Feng Zhang, Deng-Guo Feng, Zong-Duo Dai, Cryptanalysis on AW digital signature scheme based on error-correcting codes. *Science in China (Series F)*, 5: 397-400(2002).

[31]. Courtois, N., Finiasz, M., and N.Sendrier, How to achieve a McEliece-based digital signature scheme. *In Advances in Cryptology-ASIACRYPT 2001*, 2248: 157-174 (2001).

[32]. Merkle, R.C., A certified digital signature. Advances in Cryptology-CRYPTO1989 Proceedings, *Lecture Notes in Computer Science,* 435:218-238(1989).

[33]. Buchmann, J., Coronado, C., Dahmen, E, et al., CMSS-an improved Merkle signature scheme. In Progress in Cryptology- INDOCRYPT2006, *Lecture Notes in Computer Science,* 4329: 349–363(2006).

[34]. Buchmann, J., Dahmen, E., Klintsevich, E., et al., Merkle signatures with virtually unlimited signature capacity. In Applied Cryptography and Network Security - ACNS 2007, *Lecture Notes in Computer Science*, 4521: 31-45(2007).

[35]. Buchmann, J., Dahmen, E., Schneider, M., Merkle tree traversal revisited. 2nd International Workshop on Post-Quantum Cryptography - PQCrypto 2008, *Lecture Notes in Computer Science,* 5299: 63-77(2008).

[36]. Dahmen, E., Okeya, K., Takagi, T., et al., Digital Signatures out of Second-Preimage Resistant Hash Functions. 2nd International Workshop on Post-Quantum Cryptography-PQCrypto 2008, *Lecture Notes in Computer Science* 5299: 109–123(2008).

[37]. Matsumoto T, Imai H, Public Quadratic Polynomial-tuples for efficient signature verification and message encryption, Proceedings of Eurocryp 1988, Berlin: Springer, p419-453(1988).

[38]. Patarin J, Cryptanalysis of the Matsumoto and Imai Public Key Scheme of Eurocrypt 1988, Proceedings of Crypto1995, Berlin: Springer-Verlag, p248-261(1995).

[39]. Akkar M, Courtois N, A fast and secure implementation of SFLASH, Proceedings of PKC 2003, Berlin: Springer, p267-278(2003).

[40]. Dubois V, Fouque P A, Shamir A, et al. Practical Cryptanalysis of SFLASH, Proceedings of Crypto 2007, Berlin: Springer-Verlag, p1-12(2007).
[41]. Crystal Clough, John Baena, Jin-Tai Ding, et al., Square, a New Multivariate Encryption Scheme. CT-RSA 2009, *Lecture Notes in Computer Science,* 5473: 252-264(2009).
[42]. Patarin J. Hidden field equations (HFE) and isomorphisms of polynomials (IP): two new families of asymmetric algorithms, Proceedings of Eurocrypt 1996, Berlin: Springer, p33-48(1996).
[43]. Kipins A, Pararin J, Goubin L, Unbalanced oil and vinegar signature schemes, Proceedings of EUROCRYPT 1999, Berlin: Springer, p206-222(1999).
[44]. Jin-Tai Ding, Schmidt D, Rainbow, a new multivariate public key signature scheme, Proceedings of ACNS 2005, Berlin: Springer, p164-175(2005).
[45]. Jin-Tai Ding，Lei Hu，Xu-Yun Nie, et al., High Order Linearization Equation (HOLE) Attack on Multivariate Public Key Cryptosystems, Proceedings of PKC 2007, Berlin: Springer, p233-248(2007).
[46]. Jiu-Peng Chen, Chi Zhang, Yang Liu, et al., Sending-or-Not-Sending with Independent Lasers: Secure Twin-Field Quantum Key Distribution over 509 km, *Physical Review letters,* 124(7):070501(2020).
[47]. Xiao-Tian Fang,Pei Zeng,Hui Liu, et al., Implementation of quantum key distribution surpassing the linear rate-transmittance bound.Nature Photonics, 14:422-425 (2020).
[48]. Bennett, C. H., Brassard, G., QUANTUM CRYPTOGRAPHY: PUBLIC KEY DISTRIBUTION AND COIN TOSSING, P*roceedings of IEEE International Conference on Computers, Systems, and Signal Processing(IEEE, New York, 1984)*:175-179(1984).
[49]. Artur K. Ekert, Quantum cryptography based on Bell's theorem, *Physical Review letters*, 67(6):661(1991).
[50]. Charles H. Bennett, Quantum cryptography using any two nonorthogonal states, *Physical Review letters*, 68(21):3121(1992).
[51]. Dagmar Bruß, Optimal Eavesdropping in Quantum Cryptography with Six States, *Physical Review letters,* 81(14):3018-3021(1998).
[52]. Valerio Scarani, Antonio Acín, Grégoire Ribordy, et al., Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations, *Physical Review letters*, 92(5):057901(2004).
[53]. Xiang-Bin Wang, Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography, Physical Review letters, 94(23):230503(2005).
[54]. Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen, Decoy State Quantum Key Distribution, Physical Review letters, 94(23):230504(2005).
[55]. Frédéric Grosshans and Philippe Grangier, Continuous Variable Quantum Cryptography Using Coherent States, *Physical Review letters*, 88(5):057902(2002).
[56]. Kyo Inoue, Edo Waks, and Yoshihisa Yamamoto, Differential Phase Shift Quantum Key Distribution, *Physical Review letters*, 89(3):037902(2002).
[57]. Damien Stucki, Nicolas Brunner, Nicolas Gisin, et al. Fast and simple one-way quantum key distribution, *Applied Physics Letters*, 87:194108(2005).
[58]. Toshihiko Sasaki, Yoshihisa Yamamoto, and Masato Koashi, Practical quantum key distribution protocol without monitoring signal disturbance, *Nature*, 509:475-478(2014).

[59]. Hoi-Kwong Lo, Marcos Curty, and Bing Qi, Measurement-Device-Independent Quantum Key Distribution, *Physical Review letters*, 108(13):130503(2012).
[60]. Xiong-Feng Ma, Pei Zeng, and Hong-Yi Zhou, Phase-Matching Quantum Key Distribution, *Physical Review X,* 8(3): 031043(2018).
[61]. M. Lucamarini, Z. L. Yuan, J. F. Dynes, et al., Overcoming the rate–distance limit of quantum key distribution without quantum repeaters, *Nature,* 557：400-403（2018）.
[62]. Chaum D., Roijakkers S., Unconditionally-Secure Digital Signatures. *In Advances in Cryptology|CRYPTO'90: Proceedings, Springer: Berlin*, 537:206-214(1991).
[63]. Hanaoka G., Shikata J., Zheng Y., Imai H., Unconditionally Secure Digital Signature Schemes Admitting Transferability, *Advances in Cryptology, Proceedings of the ASIACRYPT 2000, Springer: Berlin*, 1976:130-142(2000).
[64]. Daniel Gottesman, Isaac Chuang, Quantum Digital Signatures, arXiv: quant-ph/0105032(2001).
[65]. Petros Wallden, Vedran Dunjko, Adrian Kent, Quantum Digital Signatures with Quantum-Key-Distribution Components, *Physical Review A*, 91(4):042304(2015).
[66]. Hua-Lei Yin, Yao Fu, Hui Liu, et. al., Experimental quantum digital signature over 102 km, *Physical Review. A*, 95(3): 032334(2017).
[67]. G. L. Roberts, M. Lucamarini, Z. L. Yuan, et. al., Experimental measurement –device - independent quantum digital signatures, *Nature Communications*, 8:1098(2017).
[68]. 量子保密通信技术白皮书，中国通信标准化协会(2018).
[69]. https://openquantumsafe.org/
[70]. Quantum Manifesto: a new era of technology. 2016-05. http://qurope.eu/system/files/u7/93056_Quantum%20Manifesto_WEB.pdf.
[71]. http://quantum-internet.team/
[72]. https://ec.europa.eu/commission/presscorner/detail/en/IP_18_6205
[73]. https://qt.eu//app/uploads/2020/04/Strategic_Research-_Agenda_d_FINAL.pdf
[74]. https://www.mynewsdesk.com/uk/pressreleases/testing-begins-on-uks-ultra-secure-quantum-network-link-ukqntel-between-research-and-industry-2851900.
[75]. https://qt.eu/news/german-government-allocates-650-million-euros-for-quantum-technologies
[76]. https://www.bundesfinanzministerium.de/Content/DE/Standardartikel/Themen/Schlaglichter/Konjunkturpaket/2020-06-03-eckpunktepapier.pdf?__blob=publicationFile&v=9
[77]. https://www.telecompaper.com/news/itmo-university-to-design-quantum-network-for-russian-railways--1337193
[78]. https://tass.com/economy/1158951
[79]. A STRATEGIC VISION FOR AMERICA'S QUANTUM NETWORKS. THE WHITE HOUSE NATIONAL QUANTUM COORDINATION OFFICE, 2020.2. https://www.whitehouse.gov/wp-content/uploads/2017/12/A-Strategic-Vision-for-Americas-Quantum-Networks-Feb-2020.pdf
[80]. https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2019060507/Documents/Akihisa_Tomita_Presentation.pdf
[81]. http://m.cankaoxiaoxi.com/world/20191007/2392432_4.shtml
[82]. https://www.idquantique.com/id-quantique-and-sk-broadband-selected-to-build-a-pilot-qkd-infrastructure-in-public-medical-and-industrial-sectors-in-korea/
[83]. https://www.idquantique.com/id-quantique-and-sk-broadband-selected-for-the-construction-of-the-first-nation-wide-qkd-network-in-korea/
[84]. https://www.nature.com/articles/d41586-020-00288-x

[85]. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/564946/gs-16-18-quantum-technologies-report.pdf
[86]. Cheng-Zhi Peng, Jun Zhang, Dong Yang, et al., Experimental Long-Distance Decoy-State Quantum Key Distribution Based on Polarization Encoding, *Physical Review letters*, 98(1): 010505(2007).
[87]. Yi-Heng Zhou, Zong-Wen Yu, and Xiang-Bin Wang, Making the decoy-state measurement-device-independent quantum key distribution practically useful, *Physical Review A,* 93(4): 042324(2016).
[88]. Hua-Lei Yin, Teng-Yun Chen, Zong-Wen Yu, et. al., Measurement-Device-Independent Quantum Key Distribution Over a 404 km Optical Fiber, *Physical Review letters,* 117(19): 190501(2016).
[89]. Sheng-Kai Liao, Wen-Qi Cai, Wei-Yue Liu, et al. Satellite-to-ground quantum key distribution. *Nature 549*, 43–47 (2017).
[90]. Qi-Chao Sun, Yang-Fan Jiang, Ya-Li Mao, et al. Entanglement swapping over 100 km optical fiber with independent entangled photon-pair sources, *Optica* 4, 1214-1218 (2017).
[91]. Alberto Boaron, Gianluca Boso, Davide Rusca, et al. Secure quantum key distribution over 421 km of optical fiber. *Physical Review Letters,* 121(19): 190502 (2018).
[92]. Sheng-Kai Liao, Wen-Qi Cai, Johannes Handsteiner, et al., Satellite-Relayed Intercontinental Quantum Network, *Physical Review Letters,* 120(3): 030501 (2018).
[93]. Bo Jing, B., Xu-Jie Wang, Yong Yu, et al. Entanglement of three quantum memories via interference of three single photons. *Nature Photonics*, 13:210–213 (2019)
[94]. Yi-Han Luo, Han-Sen Zhong, Manuel Erhard, et al., Quantum teleportation in high dimensions. *Physical Review Letters*, 123(7): 070505 (2019).
[95]. Yong Yu,Fei Ma, Xi-Yu Luo. et al. Entanglement of two quantum memories via fibres over dozens of kilometres. *Nature*, 578:240–245 (2020).
[96]. Yang Liu, Zong-Wen Yu, Wei-Jun Zhang, et al., Experimental Twin-Field Quantum Key Distribution through Sending or Not Sending, *Physical Review letters,* 123(10): 100505(2019).
[97]. Krutyanskiy, V., Meraner, M., Schupp, J. et al. Light-matter entanglement over 50 km of optical fibre. *npj Quantum Information*, 5:72 (2019).
[98]. Gong Zhang, Jing-Yan Haw, H Cai, et al. An integrated silicon photonic chip platform for continuous-variable quantum key distribution. *Nature Photonics*, 13: 839–842 (2019)
[99]. Mingtao Cao, Félix Hoffet, Shuwei Qiu, et al., Efficient reversible entanglement transfer between light and quantum memories. *Optica*, 7: 1440-1444 (2020)
[100]. Juan Yin, Yu-Huai Li, Sheng-Kai Liao, et al. Entanglement-based secure quantum cryptography over 1,120 kilometres. *Nature*, 582: 501-505 (2020).
[101]. Xiang-Bin Wang, Zong-Wen Yu, and Xiao-Long Hu, Twin-field quantum key distribution with large misalignment error, *Physical Review A,* 98,062323 (2018
[102]. Zeng, Pei, et al. Implementation of repeaterless quantum key distribution over 502 km fibers. 2020 IEEE Photonics Conference (IPC). IEEE.
[103]. Henry Semenenko, Philip Sibson, Andy Hart, et al., Chip-based measurement-device-independent quantum key distribution. *Optica*, 7: 238-242 (2020).
[104]. Ke-Jin Wei, Wei Li, Hao Tan, et al. High-Speed Measurement-Device-Independent Quantum Key Distribution with Integrated Silicon Photonics. *Physical Review X*, 10(3): 031030 (2020).
[105]. Liu-Jun, Wang, Kai-Yi Zhang, Jia-Yong Wang, et al. Experimental Authentication of Quantum Key Distribution with Post-quantum Cryptography. *arXiv:*2009.04662 (2020).

[106]. You-Qi Nie, Leilei Huang, Yang Liu, et al., The generation of 68 Gbps quantum random number by measuring laser phase fluctuations. *Review of Scientific Instruments*, 86: 063105 (2015).

[107]. Jinlu Liu, Jie Yang, Zheng-Yu Li, et al., 117 Gbits/s Quantum Random Number Generation With Simple Structure. *IEEE Photonics Technology Letters*, 29(3):283-286(2017).

[108]. Yang Liu, Qi Zhao, Ming-Han Li, et al. Device-independent quantum random-number generation. *Nature*, 562:548-551(2018).

[109]. Kejin Wei, Wei Li, Hao Tan, et. al., High-Speed Measurement-Device-Independent Quantum Key Distribution with Integrated Silicon Photonics. *Physical Review X*, 10(3): 031030(2020).

[110]. Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, et al., The security of practical quantum key distribution, *Reviews of Modern Physics*, 81: 1301(2009).

[111]. Xiang-Bin Wang, Jing-Tao Wang, Ji-Qian Qin, et al., Guessing probability in quantum key distribution, *npj Quantum Information*, 6: 45(2020).

[112]. Fei-Hu Xu, Xiong-Feng Ma, Qiang Zhang, et al., Secure quantum key distribution with realistic devices, *Reviews of Modern Physics,* 92(2): 025002(2020).

[113]. Charles H. Bennett, François Bessette, Gilles Brassard, et al., Experimental quantum cryptography, *Journal of Cryptology*, 5: 3-28(1992).

[114]. Norbert Lütkenhaus, Security against individual attacks for realistic quantum key distribution, *Physical Review A*, 61:052304(2000).

[115]. Gilles Brassard, Norbert Lütkenhaus, Tal Mor, et al., Limitations on Practical Quantum Cryptography. *Physical Review Letters*, 85: 1330(2000).