量子科技产学研创新联盟
Quantum Innovation Consortium

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

QIC量子科技产学研创新联盟
QIAC中国信息协会量子信息分会

量子安全技术蓝皮书

QUANTUM SAFE

QIC量子科技产学研创新联盟 QIAC中国信息协会量子信息分会

2024年11月

量子科技产学研创新联盟
Quantum Innovation Consortium
QIAC 中国信息协会量子信息分会
Quantum Information Association of China

本蓝皮书由量子科技产学研创新联盟牵头编写，参与单位有：中国信息协会量子信息分会、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、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、上海交通大学、武汉大学、中山大学、中国工商银行、北京科技大学、北京鹮鸟科技有限公司等。

编写组

赵　勇	赵梅生	黄　强	孙林红
赵于康	李明翰	郁　昱	王后珍
孙仕海	徐兵杰	沈超建	武宏宇
马彰超	马春利	王　子	王素妍

QIC量子科技产学研创新联盟
QIAC中国信息协会量子信息分会

前言

近年来，量子计算在全球范围内已成为科技创新的热点，自2019年谷歌“悬铃木”量子计算机首先实现量子优越性后，我国成功研发的“九章”、“祖冲之”系列以及加拿大“北极光”等量子计算原型机不断更新着量子优越性的记录。目前，我国的“九章三号”光量子计算原型机保持着光量子计算技术水平和量子优越性的世界纪录。

量子计算研究的加速进展令现有密码体系面临的量子计算威胁与日俱增。能抵御量子计算威胁的量子安全技术逐步成为信息安全发展的重要趋势之一。特别是敏感数据面临现在被截获和存储等待将来被破译的安全风险，使得当下实践量子安全已具现实意义，量子安全已然形成量子信息的一个重要研究方向，并成为各国科技和产业竞争的热点领域。基于新型数学难题的抗量子计算密码算法（包括抗量子计算的对称密码算法和公钥密码算法等）和基于量子物理的量子密码（包括量子密钥分发等）是实现量子安全的主要技术手段。近年来，量子密钥分发等相关量子密码的国际、国内标准陆续发布，国家商用密码检测中心也对国内市场上主流量子密钥产品开展了检验检测；美国牵头的抗量子计算密码筛选和制标工作已完成首批三个算法标准的发布，并继续备选算法的研究；量子密码及抗量子计算密码算法的发展呈增速态势。如何部署和使用量子安全密码技术正成为管理部门及产业界研究探讨的焦点问题。

QIAC中国信息协会量子信息分会
量子科技产学研创新联盟

量子科技产学研创新联盟协同中国信息协会量子信息分会组织多家单位，在中国信息协会量子信息分会 2022 年发布的《量子安全技术白皮书（2022 年 1 月修订版）》基础上，于 2024 年经更新、修订推出本蓝皮书。本蓝皮书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。希望以此能促进关注信息安全、量子安全各界同仁的深入沟通交流。

蓝皮书第一章从密码系统特点和量子攻击原理出发整体阐述量子安全概念的由来、产生背景及其重要性、紧迫性；第二章分别阐述已知能实现量子安全的两种途径，即基于数学的抗量子计算密码算法与基于物理的量子密码的安全原理、主要特性与当前进展；第三章阐述量子安全融合应用及其实现模式；第四章是讨论当前信息系统向量子安全的迁移方式及其准备和部分垂直领域内实例；第五章对量子安全迁移方面的一些开放问题进行了总结与展望。

QIC量子科技产学研创新联盟 QIAC中国信息协会量子信息分会

目录

一、量子攻击催生量子安全 1
（一）密码技术作用与特性 1
1. 密码是信息安全保障的基础支撑 1
2. 密码提供的主要安全服务 4
3. 主要密码技术体制及用途 5
4. 密码系统安全性要素 6
（二）量子计算攻击威胁 9
1. 量子攻击效果及影响 9
2. 非对称密码抗量子攻击能力分析 18
3. 对称密码抗量子攻击能力及其应对措施 21
（三）量子安全的实现路径 23
1. 量子安全的实现途径 23
2. 量子安全的重要性及紧迫性 24
二、量子安全技术与进展 31
（一）基于数学困难问题的抗量子计算密码 31
1. 格密码 32
2. 基于编码理论的密码 35
3. 基于哈希函数的密码 37
4. 多变量密码 39
5. 其它类型 PQC 密码算法 42
6. 抗量子计算密码总体发展趋势和面临的挑战 44

QIC量子科技产学研创新联盟
QIAC中国信息协会量子信息分会

7. 抗量子计算密码产业生态现状 46
8. 国际抗量子计算密码算法征集和标准化活动 49
（二）基于量子物理的量子密码 56
1. 量子密钥分发 56
2. 其它量子密码方案 61
3. 量子密码面临的挑战 65
4. 量子密码技术研究进展 68
5. 量子密码产业生态现状 76
6. 量子密码标准化发展现状 80
三、量子安全综合应用技术 88
（一）量子安全的 PQC 与量子密码的融合方案 88
1. 现有工作分析 88
2. 方案设计目标和途径 89
3. 系统适用的密码密钥配置 90
（二）用户端量子安全技术应用模式 93
1. 身份认证的量子安全实现示例 93
2. 传输加密类应用协议实现量子安全示例 97
3. 对密码服务应用接口的算法敏捷性要求 99
（三）量子安全的密钥管理基础设施 101
1. 密钥管理功能实现模式 101
2. 量子安全密钥管理基础设施的组成 101
四、面向量子安全的迁移 105

QIC量子科技产学研创新联盟
QIAC中国信息协会量子信息分会

（一）现有密码系统向量子安全的迁移规划和评估 105
1. 量子安全的密码系统迁移相关研究工作 105
2. 量子安全的密码迁移规划一般过程 107
3. 量子安全系统的安全性评估需要整体视角 109
4. 向量子安全基础设施的迁移规划 110
（二）面向金融行业的量子安全迁移规划现状 112
1. 金融行业面临量子攻击威胁的场景 112
2. 抗量子计算密码算法的实践探索 113
3. 量子密钥分发技术的实践探索 114
（三）面向电力行业的量子安全迁移规划现状 115
1. 电力行业面临量子攻击威胁的场景 115
2. 电力行业量子安全迁移规划 117
3. 电力行业量子安全实践探索 118
（四）面向电信行业的量子安全迁移规划现状 119
1. 电信行业对量子安全威胁的评估 119
2. 电信行业量子安全迁移规划 120
3. 电信行业量子安全迁移实践探索 121
（五）区块链系统向量子安全迁移规划示例 122
1. 评估区块链面临的量子攻击风险 122
2. 区块链面向抗量子计算密码算法迁移的重点问题 123
3. 同时适用于向 PQC/QKD 迁移的区块链中节点间通信机制 124
五、向量子安全迁移：一些开放性问题 125

QIC量子科技产学研创新联盟
QIAC中国信息协会量子信息分会

（一）用户向量子安全迁移的最佳时机 125
（二）向量子安全迁移的最佳技术路线 127
（三）向量子安全迁移的最佳实践 131
（四）通向开放性问题答案的途径 133
附录 1 针对 QKD 实际安全性的攻击方案和防御措施 136
附录 2 缩略语 138
参考文献 143

QIC量子科技产学研创新联盟
QIAC中国信息协会量子信息分会

表目录

表 1 密码服务对应的密码体制 7
表 2 Shor 算法和 Grover 算法面向求解问题特征比较 17
表 3 量子计算机对经典密码的影响[23] 17
表 4 PQC 主要算法类型定性比较 46
表 5 NIST 对 PQC 标准化的进展和计划 51
表 6 NIST 对 PQC 标准化的第三轮入选算法 52
表 7 NIST 对 PQC 标准化的第三轮候补入选算法 53
表 8 NIST 的 PQC 标准化的第三轮算法筛选后拟制标算法 55
表 9 QKD 方案分发模式分类对照说明 57
表 10 QKD 方案调制模式分类对照说明 57
表 11 主要量子密钥分发协议分类 60
表 12 融合模式实现量子安全的密码应用服务方案特性 90
表 13 融合模式实现量子安全的密钥管理方案特性 90
表 14 2022 年来向量子安全迁移主题的技术报告汇总 106

QIC量子科技产学研创新联盟
QIAC中国信息协会量子信息分会

图目录

图 1 密码典型工作流程示意图 3
图 2 经典计算与使用量子 Shor 算法计算复杂度对比示意图 15
图 3 针对各种对称密码的量子计算攻击示意图 21
图 4 构建量子安全所需时间关系图[19] 25
图 5 实现信息安全手段与作用模式示意图 30
图 6 依据 OTS 一次签名算法和 Merkle 哈希树形成公钥原理图 38
图 7 单量子制备测量（BB84 协议）方案原理图 58
图 8 纠缠测量方案原理图 59
图 9 在星地 QKD 网络中实现的纠缠测量方案原理图 60
图 10 量子隐形传态主要流程示意图 64
图 11 量子通信应用发展展望[63] 69
图 12 全球量子通信领域专利申请人排名（2024 年 8 月统计） 76
图 13 量子保密通信产业链 79
图 14 CCSA 关于量子保密通信标准建设路线图进展情况 84
图 15 能满足用户间双向安全认证需求的量子安全密码应用服务示例流程 95
图 16 量子安全基础设施和应用示意图 102
图 17 国家广域量子骨干网络示意图 104

QIC量子科技产学研创新联盟
QIAC中国信息协会量子信息分会

一、量子攻击催生量子安全

量子安全是指面对量子计算的挑战也能得到保障的信息安全。2015 年，针对来自量子计算机对密码系统可能的攻击，量子安全（Quantum Safe）的概念就被提出了[1]。量子计算机的最新进展业已表明量子计算的确比经典计算具有优势，虽然这并不直接意味着现有的密码技术都能够被量子计算破解，但由于 RSA、ECC 等不具有量子安全特性的密码算法当前被广泛应用，这已经形成了巨大的信息安全风险。

随着量子计算研究的进步，能抵御量子计算挑战的信息安全——量子安全技术，已经是全球 ICT 行业和相关部门需要认真考虑采用的新的安全基线和应对措施。量子计算是否是密码学面临的终极威胁尚未可知，但它无疑激发与促进了人们对密码学更深入的理解，引起人们对信息安全、密码安全的更多关注，在很大程度上促进了密码学的新发展。

（一）密码技术作用与特性

1. 密码是信息安全保障的基础支撑

现代社会中信息与信息系统的应用无处不在，愈加深入，起到了显著的加速与推动作用，随之而来的信息安全问题也愈发凸显。信息安全涉及现代社会生产生活的方方面面，如国家安全、基础设施安全、公共安全、个人隐私保护等等。当前，随着安全威胁变得

QIC量子科技产学研创新联盟
QIAC中国信息协会量子信息分会

越来越复杂、乃至对防护方一定程度上具有未知性，信息安全从强调保密、强调技术防护为主的通信保密时代向综合防护、纵深防御的网络空间安全时代发展。

1.1 信息安全保障的关键要素

信息安全内涵丰富，一般认为，实现信息安全保障的关键要素包括几个方面：

（1）可用性（Availability），是指得到授权的实体在其期望时间内能够访问到所要求的数据和使用到所需信息服务，即使在突发事件下，如网络攻击、计算机病毒感染、系统故障、自然灾害等，依然能够保障数据和服务的正常使用。

（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。

QIC量子科技产学研创新联盟
QIAC中国信息协会量子信息分会

1.2 密码支撑实现信息安全保障

密码是指利用特定的算法、参数、密钥等,对数据进行保护或身份认证的技术（根据我国《密码法》）。在信息安全理念诞生以来，从人们应对安全威胁的漫长历程中可以明显的看到，密码学从未“缺席”，密码学为满足信息安全需求而产生，是信息安全的基础核心支撑，能够对信息的生成、传输、存储、处理全过程实施保护。从有窃密开始，为满足通信保密需求就诞生了以数据变换为主的古代密码学。密码的典型作用是对于输入信息进行保密编码或变换，过程如图 1 表示。

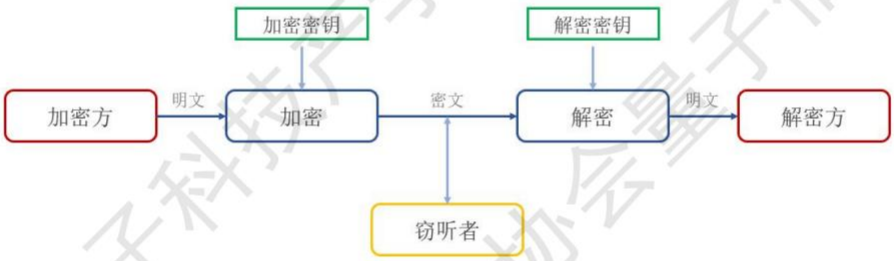


图 1 密码典型工作流程示意图

令 X 表示输入信息、Y 表示形成的密文，我们将使用密码算法进行的保密编码用函数简化表示为：

$$Y=H(X) \qquad (1)$$

需要指出，由于信息系统的复杂性和安全威胁的复杂性，并没有一种安全技术是“银弹”，是能据此就“安枕无忧”的。

QIC量子科技开学研创新联盟 QIAC中国信息协会量子信息分会

2. 密码提供的主要安全服务

密码系统通常是作为信息系统的子系统应用密码技术为信息系统提供安全服务。具体来说，针对信息安全的基本属性，密码系统可为信息安全保障提供以下四种安全服务。

2.1 机密性服务

用于保护数据防备以窃听为主的攻击。保护方式可依据通信关系（例如一对一或一对多）、保护范围等因素而不同。

2.2 完整性服务

用于保证接收方所接收的消息和发送方所发出的消息完全一致，未经插入、篡改、重排或重放，完整性服务和机密性服务一样，可应用于整个消息流、单个消息或一个消息的某一选定域。

2.3 真实性服务

用于保证通信内容、通信对象等通信要素的真实性。验证通信对象合法性，即验证发送者是真实的，而不是冒充的，称为身份认证；验证通信内容（即消息）的真实性，即验证消息来自可信发送方且在传输或存储过程中未被篡改、重放或延迟等，称为消息认证。

QIC量子科技产学研创新联盟
QIAC中国信息协会量子信息分会

2.4 不可否认服务

用于确保通信参与者不可否认或抵赖自己所做的行为，防止通信双方否认自己所传输的消息，实现信息安全可审查。

上述四种服务包含了基本安全属性中除可用性之外的所有安全属性（一般可用性不是密码所能直接提供的安全属性）。

3. 主要密码技术体制及用途

3.1 对称密码

对称密码指加密密钥和解密密钥相同的密码体制[2]。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。对称密码的代表性算法包括：AES、IDEA、SM4、ZUC 等。对称密码具备加密安全等级高，加解密效率高等特点，主要用于数据加密和认证。

3.2 非对称密码

非对称密码体制中，加密密钥和解密密钥不同且成对使用，又被称为公钥密码[2]，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），且在有限的计算资源和计算时间内基于公钥推算出私钥是不可行的，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性。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、椭圆曲线等。代

QIC量子科技产学研创新联盟
QIAC中国信息协会量子信息分会

表性公钥密码算法包括：RSA、ElGamal、ECC 等。公钥密码主要用于加解密、签名/认证等。

3.3 杂凑密码

杂凑密码又被称摘要算法（或 hash 函数、哈希函数等），它用于提供完整性安全服务。通常更多被使用的是不带密钥输入的杂凑函数，即输入为任意长度数据，输出为较短的固定长度（一般几十字节以内）的摘要值。设计良好的杂凑函数是定义域到值域上的压缩单向抗碰撞映射，不同的输入会散列成相同输出的概率要尽可能小。还有一类杂凑函数是带密钥输入的杂凑函数（又被称为消息认证码 HMAC），HMAC 算法一般用于接收方与发送方间对消息的认证，在验证 MAC 值时需要生成与验证双方共同持有的一个对称密钥的参与。

讨论各类密码体制都离不开讨论其安全性，而结合上述密码为信息安全提供的各类重要安全服务可见，密码不安全，则信息安全保障将失去基础，也就是说，密码安全是信息安全的生命线。

4. 密码系统安全性要素

4.1 不同密码体制组合应用形成完整的密码服务

单一的密码算法或密码体制一般难以满足现代 ICT 系统对安全保密的完整需求，因此，需要不同密码体制组合应用形成完整的密码服务。对称与公钥体制的密码技术可用于确保信息的机密性、真

实性、不可否认性、完整性等（如表 1 所示）[2]：机密性服务基于加解密的密码功能，主要采用对称密码，部分场景也采用公钥密码；真实性基于认证密码功能，主要采用对称密码、公钥密码和杂凑函数；不可否认性基于数字签名功能，主要采用公钥密码；完整性基于摘要密码功能，主要采用杂凑函数。

表 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	较少使用	-
真实性	认证	普遍使用	普遍使用	普遍使用
不可否认性	签名	-	普遍使用	-
完整性	摘要	-	-	普遍使用

在对称密码使用的场景中，常常要与公钥密码结合使用。例如在加解密过程中，首先需要在通信双方（或多方）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，密钥分发过程主要采用公钥密码，加解密过程主要采用对称密码，系统整体安全性依赖于密钥分发过程的安全性和加解密算法的安全性。

4.2 密钥与算法分离形成了密钥管理与密码应用的相对独立性

一般认为密码体系基本组成要素包括密码算法、密码协议以及密钥。算法的作用是使用密钥对明文进行转化，形成的密文对于不掌握密钥的破译者来说和随机数几乎无差别。密码协议规定参与方需要交互的数据、使用的密码算法、密钥以及交互步骤等，密码协议依托于具体应用场景产生和使用，应用场景为密码协议提供了具

体的设计要求、交互模式乃至参与方到环境的安全假设等，例如有按应用需求区分的各种密钥分发协议、身份认证协议、数据传输协议等，也可以按协议基于的具体密码体制分类，如基于公钥的认证协议、量子密钥分发协议、量子密码签名协议等，不一而足。

密钥管理是密码系统的必备基础功能，密钥管理基本内容包括：生成、注册、认证、注销、分发、安装、存储、归档、撤销、派生以及销毁等[3]。密码要素中，算法和密钥的关系尤为重要：现代密码学的基本原则是密钥与算法的独立；并且，现代密码学者的共识是，密码算法和协议不应当保密，最好是充分公开的，这样可以得到广泛的评估以保证其中无安全漏洞和缺陷，唯一需要保密的是密钥，“一切秘密蕴藏于密钥之中”[4]。因此公式（1）应扩展为如下的公式（2），其中 K 代表密钥。

$$Y=H(K, X) \qquad (2)$$

密钥管理是密码系统的必备基础功能，它对密码系统起到支撑作用，与密码应用同等重要。密钥管理是关键环节也容易成为薄弱环节和敌手攻击的切入点，密码的安全性首先取决于密钥的安全性，密码是信息安全的基础底线，而密钥管理是密码安全的基础底线，密码安全必须关注密钥管理的安全。

密钥管理服务的主要特点，一是其服务对象是密码系统内部各组件，而不是面向信息系统所有组件；二是由执行密钥管理服务的功能决定，它往往需要更加严格的安全保护，如较强的独立性要求。对密钥管理子系统，要求其相对具有独立性，也就是具有较高的隔

QIC量子科技先导研创新联盟
QIAC中国信息协会量子信息分会

离性，主要是指密钥管理应尽可能使用与数据保护不同的安全机制，保证密码应用系统如果被攻击不会连带攻击影响到密钥管理系统。

这一特性和密码系统是否满足量子安全特性紧密相关，例如，如果对称密码使用的密钥是基于公钥密码技术协商获得的，这种情况下即使对称密码算法本身是量子安全的，但由于密钥管理环节被破解、对称密钥可能已泄露而不再安全，整体的量子安全性也无法得到保证。这一结论也充分说明了考察密码系统安全问题上“唯密码算法”的观点是危险的，密钥管理上的防护不足、设计疏漏等各种原因都有可能导致密码系统被量子攻击攻破。

（二）量子计算攻击威胁

量子计算近年来的加速发展，对经典密码构成了直接、紧迫的破解威胁。在此先从量子攻击能力角度阐述量子计算对于传统密码的现实紧迫威胁，再从密码算法特性本身抵御量子攻击的能力上针对现用密码进行分析。

1. 量子攻击效果及影响

1.1 量子计算主要优势

量子计算是遵循量子力学的规律进行信息处理的新型计算模式[5]，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进行数学和逻辑运算、存储及处理量子信息。一般认为其优势源于以量子相干叠加和干涉来编码

QIC量子科技产学研创新联盟
QIAC中国信息协会量子信息分会

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进行变换相当于一次经典计算，所有叠加分量变换对应的经典计算可同时完成，并按一定的概率振幅叠加，给出量子计算输出结果。量子计算会带来以下的赋能效果：

（1）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）克服摩尔定律失效：量子计算能克服当前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。近年来，量子计算芯片的量子比特位数得到不断提升，其增长速度态势类似摩尔定律，也被称为“量子摩尔定律”。

量子计算机可基于多种不同物理体系实现，如超导电路体系、离子阱体系、线性光学体系、中性原子体系、半导体量子点体系、核磁共振体系、拓扑体系等。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，其它技术路线也有显著进展；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。

QIC量子科技产学研创新联盟 QIAC中国信息协会量子信息分会

1.2 量子计算总体发展现状及趋势

近年来，各主要国家和地区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不断加大投入。以 IBM、谷歌为代表的科技巨头间竞争激烈，开展了如火如荼的“量子计算大战”，并在生物医药、化学、人工智能等领域开展应用探索，推动了量子计算技术的快速发展。我国众多研究机构、高校和 IT 企业在量子计算领域也进行了大量投入和重点布局，部分技术成果处于国际领先水平。

（1） 总体发展趋势和当前所处阶段

量子计算机总体上仍处于技术验证和原理样机研制阶段，属于中等规模含噪量子（NISQ）计算阶段的初期，仍面临量子比特数量少、相干时间短、出错率高等诸多挑战。实现实用的通用量子计算机技术难度很大，是一个需要全球学界、产业界长期艰苦努力的任务[6]。

一般认为，第一个阶段是实现量子优越性（Quantum Advantage 或 Quantum Supremacy），即针对特定问题的计算能力超越经典计算机，达到这一目标需要约 50 个量子比特的相干操纵。这一阶段目标已在 2019 年由谷歌在其超导量子计算系统上率先实现[7]。2020 年、2021 年中国科学技术大学在其光量子计算原型机系统“九章”和超导量子计算原型机系统“祖冲之”上再次实现了量子优越性且性能显著提升，中国已成为世界上唯一一个在两个技术路线上实现量子优越性的国家[8][9][10]。

QIC量子科技产学研创新联盟
QIAC中国信息协会量子信息分会

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，即相干操纵几千个量子比特，可在组合优化、量子化学、机器学习等重要领域真实发挥效用。

第三个阶段是实现可编程可大规模纠错的通用量子计算机，即相干操纵至少数百万个量子比特。根据 IBM 于 2024 年发布的技术路线图[11]，到 2029 年将实现百万量子比特，未来随着量子比特数的增加，破解时间将指数级缩减。量子计算机对当前密码的威胁已经越来越近。

需要指出，量子计算与经典计算不是替代关系。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，其应用场景相对受限，亟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。量子计算本身需解决的退相干、量子纠错等关键技术问题也需进一步的研究。

（2） 不同量子计算技术路线发展现状

超导量子计算机近年来发展较快、受关注较多，超导量子比特主要基于约瑟夫森结，有较高的可控性、可扩展性和量子比特寿命，该路线代表企业有 IBM、谷歌等。2022 年 IBM 已实现 433 量子比特，2023 年谷歌宣布其最新量子计算机悬铃木二代仅用 6.18 秒，就完成了目前世界最快超级计算机 47.2 年的计算量。IBM 于 2023 年底发布了其 1121 量子比特的超导量子芯片，预计再用 3 年将突破 1 万

QIC量子科技产学研创新联盟 QIAC中国信息协会量子信息分会

量子比特，到 2029 年实现 100 万量子比特[11]。国内研发水平总体也处于第一梯队，2021 年中国科学技术大学构建了 66 比特可编程超导量子计算原型机“祖冲之二号”，实现了对量子随机线路取样任务的快速求解。计算复杂度比谷歌公开报道的 53 比特超导量子计算原型机“悬铃木”提高了 6 个数量级（“悬铃木”处理量子随机线路取样问题比经典超算快 2 个数量级）。是我国继光量子计算原型机“九章”后在超导量子比特体系首次达到“量子计算优越性”里程碑。

离子阱技术路线是利用离子阱陷住原子离子，并通过激光进行操作控制，能实现较高的保真度，国际上的代表企业有 IonQ 和 Honeywell 等。2021 年 Honeywell 宣布其离子阱量子计算机达到 10 个量子比特。2022 年因斯布鲁克大学和 AQT 公司联合发布了具备 8 个离子的 qudit 系统，并在此系统中展示了普适量子门集。2023 年，因斯布鲁克大学在一体化阱中实现了包含 105 离子的二维晶格的稳定囚禁。2024 年，Quantinuum 和 Microsoft 合作基于 QCCD 方案的离子阱芯片将量子线路的错误率降低为物理比特的 1/500 和 1/800，远超盈亏平衡点。国内方面，2024 年，清华大学段路明组在基于 4K 低温系统的一体化阱中实现了超过 500 个离子的稳定囚禁，并用 300 个离子实现了伊辛模型的量子模拟。

光量子计算路线利用光子作为量子比特载体，具有较强的容错性和抗干扰能力。2023 年，中国科学技术大学成功构建 255 个光子

QIC量子科技产学研创新联盟
QIAC中国信息协会量子信息分会

的量子计算原型机“九章三号”，刷新光量子信息的技术水平和量子计算优越性的世界纪录。

其它技术路线以及量子纠错等量子计算关键技术上，近期有突破性的进展。2023 年底，美国研究团队发布用中性原子体系研发的 48 个逻辑量子比特的量子计算原型机[12]。它使用 280 个物理量子比特和码距为 7 的纠错码，展现了中性原子体系进一步的可扩展性，也展现了用更少的物理量子比特构建容错量子计算的可能性。2023 年，我国研究团队通过对微波腔中的离散变量光量子比特进行实时反馈校正，超越了量子纠错的盈亏平衡点[13]。与同年谷歌团队采用不同技术路线均取得了量子纠错技术的突破。

1.3 量子攻击实现原理

（1） Shor 算法

很多量子计算攻击基于 Shor 算法[14]实现，Shor 算法基于量子傅里叶变换，比经典算法能更快速的进行质因数分解。傅里叶变换是通过一组特殊的正交基来实现时域到频域的变换，把时域序列转换到频域上以刻画其变化规律，当前我们在信息通信技术中通常使用的是快速傅里叶变换（Fast Fourier Transform, FFT），它是信息时代数据处理无处不在的基本工具。

量子傅里叶变换（Quantum Fourier Transform, QFT）是在量子计算机上实现傅里叶变换的算法。量子计算的模式适合于执行傅里叶变换：第一，基于量子相干性，QFT 通过构造合适的量子线路，

QIC量子科技产学研创新联盟 QIAC中国信息协会量子信息分会

对时域上有限长序列通过量子线路输入端形成的量子态进行测量，就可以高概率测出频域上体现的特征规律。第二，基于量子叠加性，QFT 算法处理单个数据流的速度虽然与经典 FFT 相同，但由于量子计算机允许一组量子比特同时对多种信息状态进行编码，可以一次将所有输入计算完成，由于 QFT 具有这样同时处理多个数据流的能力，因此理论上它的效率比 FFT 更高。由于量子傅里叶变换形成的加速效果，Shor 量子算法比经典算法有指数级的加速效果。

使用 Shor 算法解质因数分解问题的优势是能以多项式时间分解整数 N：也就是说它需要的时间是 $\log_2 N$ 的某个多项式这么长（这里 $\log_2 N$ 的意义恰好对应的是输入数字的二进制序列长度）。更精确的说，这个算法花费 $O((\log_2 N)^3)$ 的时间。比传统已知最快的因数分解算法——普通数域筛选法快出了指数级差异。因此可以对广泛使用的 RSA、ECC、DSA、ElGamal 等公钥密码算法进行快速破解。例如：分解一个 400 位的大整数，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。



图 2 经典计算与使用量子 Shor 算法计算复杂度对比示意图

QIAC量子科技先导研创制联盟 QIAC中国信息协会量子信息分会

近期诸多研究成果表明，破解主流的 2048 位 RSA 加密，在可预见的未来就可能实现。2019 年谷歌公司研究者发文认为量子计算机将在 8 小时内破解 2048 位 RSA 加密，但需要 2000 万个量子比特[15]。2021 年法国研究者发布的研究成果[16]表明，通过将量子存储器集成到量子计算机中（提出了设计方案但目前技术上还无法实现），13436 个量子比特耗费 177 天就能破解 RSA-2048，比此前所需的量子比特数减少了 3 个数量级。

（2） Grover 算法

除 Shor 算法外，其它量子算法也能攻击现用密码。1997 年 Lov Grover 发明的 Grover 量子算法[17]，也称为量子快速搜寻算法，它能从大量未分类的无序个体中快速寻找出某个特定的个体。Grover 算法先控制量子线路重复进行某些操作来改变待输出的量，使它刚好等于目标的概率增加到接近 1，再测量获得输出态。Grover 量子算法能够将非结构化数据或无序数据库的搜索时间降为经典算法的平方根时间。

举例来说，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（N+1）/2 次，而采用 Grover 算法的量子计算机采用并行处理，只需 $N^{1/2}$ 次。因此，Grover 算法可以有效地攻破 DES 或轻量级算法等密钥长度较短的对称密码。对于 DES 破译而言，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

QIC量子科技产学研创新联盟 QIAC中国信息协会量子信息分会

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。

比较 Shor 算法和 Grover 算法，其各自面向的求解问题的特征如表 2 所示。

表 2 Shor 算法和 Grover 算法面向求解问题特征比较

算法类别	Grover 算法	Shor 算法
数据周期规律	非周期问题	周期问题
数据变化规律	非线性问题	线性问题
求解问题类型	间接问题	直接问题
处理数据结构性	非结构性问题	结构性问题
数据规律变化	无规律问题	规律问题
排列是否有序	无序问题	有序问题
面向问题类型特征	不确定性问题	确定性问题
面向问题数据特征	随机性问题	非随机性问题

综上，如表 3 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。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。下面的 2、3 两节内容分别对其进行了详细分析。

表 3 量子计算机对经典密码的影响[23]

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，密钥协商与分发	不再安全
ECDSA, ECDH	公钥密码	数字签名，密钥协商与分发	不再安全
DSA	公钥密码	数字签名，密钥协商	不再安全

QIC量子科技产学研创新联盟 QIAC中国信息协会量子信息分会

2. 非对称密码抗量子攻击能力分析

2.1 公钥密码天然存在陷门性

为了达到保密，密码学家希望变换公式（1）中的函数 H 没有办法逆向求解，但 H 又不能使用杂凑函数这样的单向函数（否则将无法解密）。因此，对加密算法来说，公式（1）中的变换 H 需要具有“陷门性”，就是在变换 H 里隐藏一定的“结构”。

对公钥密码来说陷门性尤其重要。在此列举几种目前常用公钥密码中所构建的陷门性：

RSA：单向函数是大整数分解 n=p1p2…，退化为 n=p1p2 是陷门性要求。

DSA：单向函数是模整数的群中求离散对数，a=b 的 x 次方 mod n，已知 a,b 求 x；满足陷门性。

ECCDSA：单向函数是椭圆曲线点群中求离散对数，a=bx（椭圆曲线点群中数乘），已知 a,b 求 x；满足陷门性。

2.2 从可证明安全到启发式安全

(1) 可证明安全含义

可证明安全（Provable Security）的学术概念，是若能将破解某算法的难度归约化为寻找某个公认的数学困难问题的多项式时间复杂度求解算法，就称其为可证明安全的。典型的这类问题是 NP（Non-deterministic Polynomial）问题里面最难的 NPC 问题

QIC量子科技产学研创新联盟
QIAC中国信息协会量子信息分会

（Non-deterministic Polynomial Compelete，即非确定性多项式完全问题）。NPC 问题不多，也很难界定，只能独立的寻找和论证。一个 NPC 问题经过多项式时间的、不影响其困难性的变换可以形成一个问题族，要获得可证明安全的算法往往可以依此构造和选择。对此问题族来说，如果里面任意一个问题有了多项式的解，即找到一个破解算法，那么所有的问题都可以有多项式的解，也就是都被破解了。

相类似的量化定义有安全强度（Security strength），它是对密码方案安全性的量化指标，一般是将破解公钥算法的难度往熟知的某对称算法破解时间来度量。代表了攻破某密码方案所需的计算开销。公钥密码方案的安全强度与构建该方案所依赖的困难问题和具体的参数有关。随着抗量子计算密码学的发展，原先单一的安全强度评估标准产生了变化和扩充。

(2) 启发式安全含义

如果某个算法没有被验证是可证明安全的，那如何衡量其安全性呢？这就要引入学术上的计算安全（Computational Security）概念，它通过衡量攻破一个密码算法所需的计算开销来刻画其安全性。通俗的说，使用现有人们公认最好的算法破解某个密码算法所需的计算资源远远超出攻击者的既有能力时，可称其是计算安全的。

要验证可证明安全性需要从已知 NPC 问题出发进行转换、规约和严格证明，计算安全性需要定量计算。为便于理解，可以通俗的称由计算安全性获得的安全性为启发式安全或经验式安全。首先，

QIC量子科技发展创新联盟 QIAC中国信息协会量子信息分会

它不以已知的、公认的数学难解问题为基准；其次，这个定量计算的途径和方法是研究者各自想定的，是否会有更高效的破解算法尚不可知。

具备启发式安全特征的密码常见构造思路包括：随机函数发生器、伪随机函数发生器，通过小置换和小矩阵，横向扩散，纵向迭代等。例如，杂凑函数（如 SHA2）和分组密码（如 DES、AES）都是通过小置换和小矩阵，横向扩散、纵向迭代构建；后者是在迭代后要求整体是置换,为了能快速解密，还必须要求单轮是简单置换（如三角置换）。而序列密码（如 ZUC）是先设计一个质量不高的源序列，通过小置换和小矩阵，横向扩散、纵向迭代，输出序列；或者通过输出反馈模式，反复迭代。

2.3 当前公钥密码无法抵御量子攻击的原因

RSA 和 ECC 等公钥密码算法不是量子安全的，主要因为对其来说只是增加密钥长度还无法抵御未来量子计算机的攻击。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与 RSA 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[13]。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。基于上述公钥密码的

QIC量子科技专项创新联盟 QIAC中国信息协会量子信息分会

安全协议和系统都将受到量子计算的威胁。因此，需要用量子安全的技术手段代替这些密码算法才能抵御量子攻击。

3. 对称密码抗量子攻击能力及其应对措施

总体上也属于启发式安全的对称密码同样面临量子攻击风险，但由于对称密码算法一般不存在明显的数学结构，这种风险相对还较小。由于现用的杂凑密码总体上也是基于对称密码体制实现，我们将对称密码细化分为分组密码、序列密码和杂凑密码，如图 3 所示，分别对其量子计算攻击进行讨论。

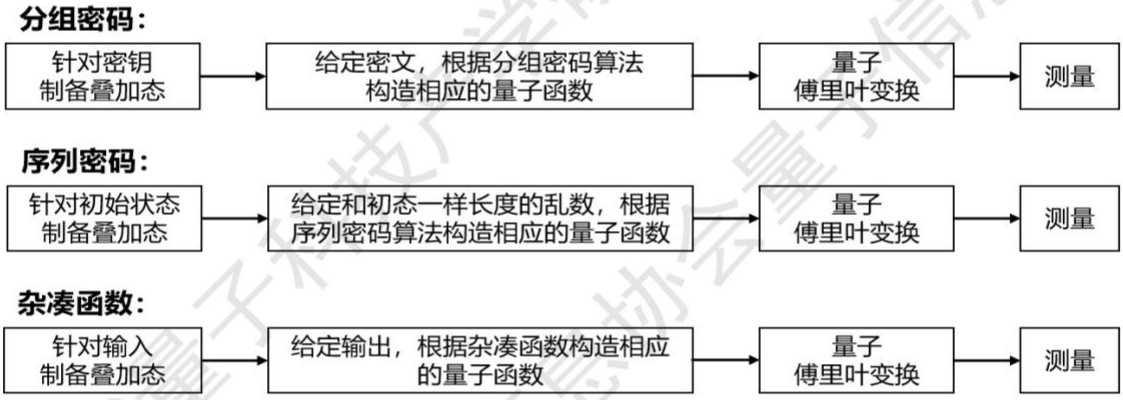


图 3 针对各种对称密码的量子计算攻击示意图

使用 Shor 算法挖掘对称密码算法的弱结构的成功概率和效率不如对公钥密码那样高。也就是一般情况下经过量子傅里叶变换输出后的规律比较微弱、不够显著，无法高概率测量。但如果通过对对称密码进行分析掌握一定的规律，依此进行针对性预处理再使用 Shor 算法，这种经典—量子混合的量子攻击可能成功概率更高。

对序列密码来说，一般情况下经过量子傅里叶变换输出后的规律会更微弱、更不够显著，所以更无法高概率测量。但如果对序列

QIC量子科技产学研创新联盟 QIAC中国信息协会量子信息分会

密码算法进行深入的分析，能掌握一定的规律，则对上述量子计算攻击有帮助。

对杂凑密码来说，一般情况下经过量子傅里叶变换输出后的规律会进一步更微弱和不够显著，所以也无法高概率测量。但如果对杂凑函数算法进行深入的分析，能掌握一定的规律，则对上述量子计算攻击有帮助。其它量子算法如 Grover 算法也可能对对称密码实施量子计算攻击。一般认为对称密码抵御量子攻击的应对措施是增加密钥长度或增加算法密文输出长度，具体的，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。

进一步的深入讨论，诸如 AES 等对称密码算法目前被认为是量子安全的，是依据计算复杂性理论，好的对称密码算法设计能在理论上等价于不可区分的伪随机数生成问题，而对于伪随机数的可区分性问题，一般认为又可以等价为无结构数据库的随机搜索问题求解这一问题，虽然使用量子计算机上的 Grover 算法比传统计算机效率更高，但这个加速不是指数级加速，而是平方级加速（当然对于具体对称密码算法其破解问题最终是否能够等价于一个无结构数据库随机搜索问题还需做针对性分析，例如若其等价于结构化数据库随机搜索问题，仍能找到具备指数级加速优势的量子算法）。根据这样的推论，通过将对称密码的密钥长度加倍就可以使其被量子计算机破解的难度与被传统计算机破解相当。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

QIC量子科技光学研创联盟 QIAC中国信息协会量子信息分会

和已知量子算法而言，AES-256 很难破解。因此 AES 被认为是量子安全的。

（三）量子安全的实现路径

1. 量子安全的实现途径

如何满足量子安全这一新出现的安全需求，一定程度上还存在不确定性，这促使人们开展深入研究去尽可能的、遍历的寻找量子安全所有可能的实现路径。在传统的基于数学的路径之外，从物理原理出发探索实现量子安全目标也已被证明是可行的路线。

2.1 延续数学原理实现量子安全的路径

目前人们认为，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，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。一般地，基于目前被认为是量子算法困难，并且也很有希望一直是量子困难的数学难题构造的经典密码算法，通常称为抗量子计算密码算法（Quantum Resist Cryptography，QRC）或后量子密码（Post Quantum Cryptography，PQC）——包括抗量子计算的对称密码算法和公钥密码算法，目前对抗量子计算密码算法的研究主要集中在公钥密码算法，故通常将 PQC 狭义的等同于抗量子计算的公钥密码算法（下文中 PQC 指代抗量子计算的公钥密码算法）。

QIC量子科技大学开创新联盟
QIAC中国信息协会量子信息分会

代表性 PQC 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、超奇异椭圆曲线密码等。需要注意的是，目前被认为是量子安全的算法在未来不再安全的可能性依然存在：从攻击角度看，对 PQC 的攻击可能来自新的量子破译算法，也可能来自新的经典密码分析技术；从密码算法自身构造来看，由于构造密码过程中引入陷门性等原因，PQC 算法的安全性与其基于的量子困难问题并不一定等价，因而，PQC 的安全性也有待长期检验。具体内容见第二章（一）部分。

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、密钥分发、数据加密都主要依赖于 RSA、ECC、DH 等现用公钥密码，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[18]的数字证书应用等。不仅如此，对于信息安全机密性有高级别要求，或者对保密时效有较长时间要求的内网运行环境中，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。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。一旦这个时刻到来，大部分现行公钥密码及其基础设施会丧失安全性；如上节所述，量子攻击也会削弱其它类如对称密码、杂凑等现

QIC量子科技先导研创新联盟 QIAC中国信息协会量子信息分会

有密码系统的安全性；更为严重的是，公钥密码在现代密码系统中通过完成密钥协商、密钥分发等功能大量扮演着密钥管理角色，基于公钥的密钥管理过程被攻破将意味着密钥管理系统被攻破。这都意味着所有信息系统使用者现在就需要规划将密码全面升级至量子安全级别。

关于量子攻击威胁留给我们的时间期限问题，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存多长时间，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，业界较为认可的是 XYZ 理论[19]。如图 4 所示，X 代表“数据需要保密的时间”，Y 代表“更新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”（依据主流推断，十年左右实现通用量子计算机）。如果 X+Y>Z，意味着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。

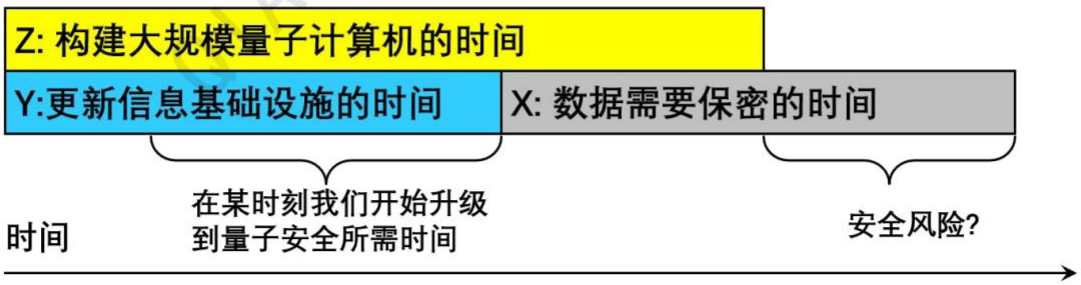


图 4 构建量子安全所需时间关系图[19]

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 5 年。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，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。

综上所述，量子安全不是指某一类技术或现有技术到新技术的演进，而是未来各类密码必须考虑满足的要求。量子安全的应用范畴也不限于现有各类数据安全场景，它也适合于、且必将应用于各类计算安全（如安全多方计算）场景。虽然目前大规模通用量子计算机时代还未到来，但对于对信息安全保障有需求的行业以及政策决策者而言，需要认识到这一重要性，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，以决定构建量子安全保障的最后期限，更为保险的做法是当下就要开始考虑升级到量子安全的信息通信系统和基础设施。正如 NIST（美国国家标准与技术研究院）2024 年 8 月正式发布首批 PQC 算法标准时所阐述的：量子计算技术发展迅速，可

QIC量子科技先锋创新联盟
QIAC中国信息协会量子信息分会

能在未来十年威胁到个人、组织和国家的安全及隐私。这给企业、政府机构及其供应商发出了明确信号——现在就要开始加强全球信息安全体系，以防范未来量子计算带来的安全威胁。

2.2 从物理原理探索实现量子安全的路径

从基本原理来说，基于物理上可信实体路径及方法、或基于物理原理实现信息安全的方式古已有之，例如，古人采用“蜡丸传书”、“虎符调兵”，现代，人们仍会使用“专人、专车、专程”的方式递送秘密信息，均属于此。为满足量子安全这一新出现的安全需求，人们自然也想到从物理原理探索实现。量子通信（Quantum Communication）是以量子态为信息载体，通过量子态传送实现量子信息或经典信息传送的技术，它是量子信息学的主要分支之一，利用量子通信中单量子不可分割、海森堡测不准原理、未知量子态不可复制、量子纠缠的非定域性等量子力学原理及其一些延伸技术如量子随机数发生器（QRNG），可以实现密码学的一系列目标，能够构建量子密码（Quantum Cryptography）用以提供各类安全服务、保护信息安全，量子密码具有内禀的量子安全特性或信息论安全特性，也被认为是能够抵抗未来量子计算攻击的一种有效方式，为实现抵御量子计算破解的密码提供了可行性。

量子密码中最具代表性和实用性的是量子密钥分发（Quantum Key Distribution，QKD），QKD 是指通信双方通过传送量子态的方法实现信息论安全的密钥生成和分发的方法和过程[20]。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。QKD 的功能是实现对称密钥的协商，与对称密码算法结合可实现加解密功能。与一次一密（OTP）结合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。

对于 QKD 这类基于物理原理的安全技术，安全性研究也重点在于物理安全问题。攻击者可能通过一些物理的技术手段利用 QKD 器件的特定脆弱性造成的“后门”，从而绕过 QKD 量子层面的防护攻击乃至破解 QKD。这种攻击被称为“量子黑客攻击”。例如，向 QKD 系统注入强光，以刺探 QKD 内部设置，或者改变 QKD 设备的工作状态。对于这些物理安全问题能否关闭，学界有不同看法。一种看法认为，为了达到更广泛的无条件安全，需要假设通过物理技术手段攻击的量子黑客具有无限强大的物理实现能力；此时将无法证明漏洞能被防御者穷尽，或者防御手段绝对有效，并因此否定 QKD 的实用价值。第二种看法是从被攻击系统角度来看，认为对于一个有限的物理系统，可利用的漏洞是有限的；经过充分的分析，这些漏洞总会被发现和弥补，最终可以达到有保障的安全性。近年来，关于 QKD 系统的量子黑客攻击研究并没有发现什么新类型的漏洞，这似乎支持第二种观点的适用性[21]。量子密码内涵丰富，包含 QKD 等各类用途的密码协议、以及与密码应用紧密相关的量子随机数发生器等，本书从量子安全角度对其具体展开的阐述内容见第二章（二）

QIC量子科技光学研创新联盟 QIAC中国信息协会量子信息分会

部分（也基于此，由于量子隐形传态能够实现量子安全，虽然一般将其归类于量子通信而非量子密码范畴，本书亦进行讨论）。

2.3 量子安全的实现途径将是数学方法和物理方法的融合

PQC 和 QKD 二者基于不同的科学原理：前者基于数学原理而后者基于量子物理。前者在目前并未从理论层面上完全解决量子安全威胁，未来投入实用中也会存在物理安全层面如侧信道攻击等的风险；后者虽然解决了量子安全威胁，却也引入了一些新的物理安全层面的风险。但 PQC 和 QKD 仍是目前从技术原理上和实践上都可行，且得到广泛认可的两种量子安全技术途径。

数学方法和物理方法从适用场景上有很大的不同，一般来说，用数学运算为主的方法处理数据由于实现方式成熟，具有速率高、灵活性强的特点。物理方法处理数据由于环节更复杂（例如需要进行信息的物理载体变换等原因），具有处理速度受物理规律所限、处理过程需物理设备参与的特性，同时也具备安全性基础更牢靠、不受数学算法破解威胁等特点。

针对现代信息系统处理信息方式复杂多样、数据存储、传输和处理量大等特点，对配套的密码子系统的要求也日趋复杂多样，需要细化讨论：对应用侧用户数据的处理具有速率高、灵活性强（如算法可替换）等要求，数学算法为主的方式总体上更适合于提供用户侧的、面向海量用户数据的密码服务。

QIC量子科技产学研创新联盟 QIAC中国信息协会量子信息分会

如前所述，密钥管理与密码应用有较大差异和相对独立性。针对密钥管理的高安全性要求，密钥需要充分隔离和强保护等，物理方法为主的方式更适合密钥生成、分发等管理环节，特别是核心部位。

对应到抵御量子攻击、实现量子安全目标，数学算法为主的方式总体上更适合于实现用户侧的、面向应用数据的密码服务。物理方法为主的方式如 QKD 更适合应用于密钥生成、分发、存储等密钥管理环节和子系统，特别是核心部位。如图 5 所示，是通过结合数学手段和物理手段实现信息安全的方式示意图，实线代表主要支持作用，虚线代表辅助支持作用，具体阐述见第三章。

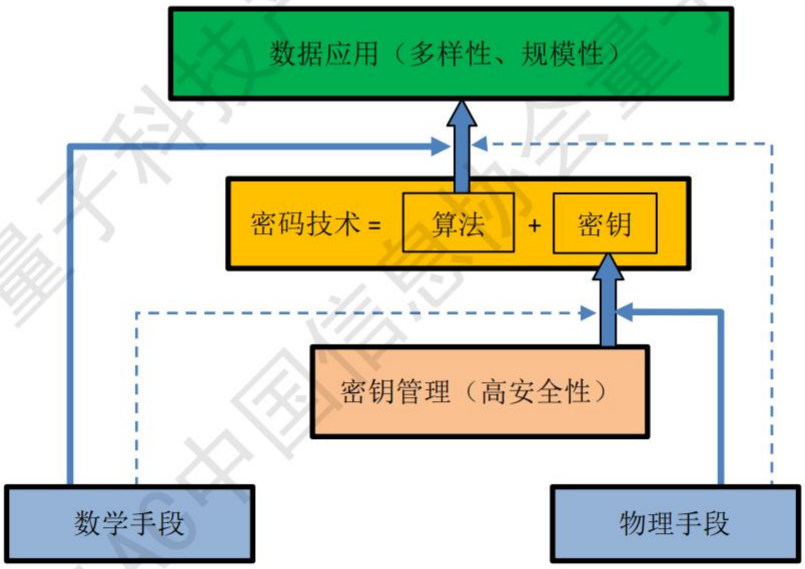


图 5 实现信息安全手段与作用模式示意图

QIC量子科技产学研创新联盟
QIAC中国信息协会量子信息分会

二、量子安全技术与进展

在量子计算对现有密码体系的威胁日趋严峻的背景下，信息安全即将整体进入量子安全时代。能抵御以量子计算为代表的新兴计算能力的挑战，成为了新一代密码技术的关键特征之一，也是当前国际激烈竞争的热点领域。研究者普遍认为，抗量子计算的密码包括抗量子计算的密码算法和量子密码。

（一）基于数学困难问题的抗量子计算密码

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抗量子计算的密码算法具有抗量子计算攻击的潜力[22][23]，以下以PQC来代表这些旨在抵御已知量子计算攻击和替代现用公钥密码的基于数学难题密码算法的统称。目前并无证据表明，量子计算能破解诸如格问题、非线性方程组求解问题、纠错码的一般译码等问题。于是，研究者基于这些困难问题设计密码算法，以期这些密码算法是具备抗量子攻击能力的，从而形成了格密码、基于编码理论的密码、基于哈希函数的密码、多变量密码、基于超奇异椭圆曲线密码、基于安全多方计算或其它技术的PQC类型。

QIC量子科技安全研创新联盟
QIAC中国信息协会量子信息分会

1. 格密码

1.1 基本原理

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。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[24]，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）的归约证明，为构建格密码算法奠定了基础。因此相对其它几类 PQC 来说，它在密码领域内经过了更长时间的理论研究，到目前为止并无证据表明量子计算能破解格问题。格密码中的困难问题主要是基于特定类型格如随机格（通过随机过程生成的格）中求最短向量或最近向量——如著名的 SVP 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，也因此被看好选入 PQC 的行列。从代数学的角度来看，SVP 问题可以归为二面体群中的隐藏子群问题（HSP）。对于所有阿贝尔群中的隐藏子群问题都具有多项式时间复杂度的量子算法，而二面体群属于非阿贝尔群，对于非阿贝尔群则尚未找到这样的量子算法，而计算复杂性理论的研究进展也倾向于认为可能不存在这样的量子算法。

QIC量子科技未来创新联盟 QIAC中国信息协会量子信息分会

1.2 发展历程

1997 年 Ajtai 和 Dwork[25]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。2009 年，Gentry 首次提出了基于格的全同态加密方案[26]，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[27][28][29]。

格密码一直被认为是 PQC 标准备选中最有力的竞争者。可以看到，在 NIST 每一轮抗量子算法候选和入选方案名单中，基于格的密码方案一直是占有重要地位的，2020 年第三轮筛选胜出的 7 个方案中，NTRU、Crystal-Kyber（以下简称 Kyber）、Saber、Crystal-Dilithium（以下简称 Dilithium）以及 Falcon 这 5 个方案均为格密码方案，前 3 个方案为密钥封装方案，后 2 个为数字签名方案。中国密码学会 2019 年举办的全国密码算法设计竞赛公钥密码组的 14 个最终获奖方案中，包含 11 个基于格的密码方案，获得一等奖的 3 个密码方案 Aigis-enc 密钥封装算法、Aigis-sig 数字签名算法、LAC.PKE 密钥封装算法均是基于格问题构造的。因此，格密码值得我们进一步深入研究。

QIC量子科技产学研创新联盟 QIAC中国信息协会量子信息分会

1.3 当前聚焦问题

格密码安全性主要是基于格上困难问题。具体的，格可分为非结构格（即其中不含特殊代数结构）和结构格。其中前者的安全性基于经典格上最坏情况下的困难问题，如经典格上的最短向量求解问题（SVP）——在格内找到最短的非零向量，这个问题在理论上是NP 困难问题。非结构格的一个关键特性是它们的“最坏情况”和“平均情况”问题之间的紧密联系。这意味着对于某些类型的非结构格问题，找到解决方案的平均难度接近于在最坏情况下的难度。也正因为如此，在格密码中我们可以将密码基于的求最短向量或最近向量问题趋近到近似最短向量，或近似最近向量，而认为破解难度没有明显变化。

NIST 比较看好的 LWE（容错学习，Learning With Error）和 NTRU 算法也正是基于 SVP 问题。对于 NTRU 密码体制，为满足陷门性，会将构造的随机格（随机格无结构的特点会造成无陷门）退化为理想格（循环格），对于 LWE 密码体制，对任意向量限定为小范数的向量。

目前针对格密码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）。

在实际构造中，结构格上的方案在密钥、签名尺寸、效率上具有绝对优势，因此其标准化进程也较快。2022 年，基于结构格问题

的 Kyber 密钥封装算法和 Dilithium 和 FALCON 两种数字签名算法都通过筛选成为了 NIST 的 PQC 算法标准化第三轮遴选后的拟制标算法。其中 FALCON 的密钥和签名尺寸上具有优势，而 Dilithium 则具有优秀的签名效率。因此 NIST 在第四轮的签名算法征集并不准备征集更多基于结构格的算法。

由于非结构格算法在效率上逊于基于结构格的算法，甚至也逊于很多基于其他假设的算法，因此尽管 NIST 新一轮的签名算法中也征集到了诸如 Squirrels、HuFu 的该类算法，但其在效率上不具备优势。

在 NIST 第四轮算法征集中，基于格的算法中，基于结构格的 HAETAE 算法具有一定的竞争性，Hawk 算法为基于全新的格同构问题签名算法其效率也较佳，而基于非结构格问题的算法未能展现出显著优势。

2. 基于编码理论的密码

2.1 基本原理

基于编码的公钥密码体制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（例如加入随机噪声），解密时运用私钥纠正错误也就是对带噪声编码进行解码恢复出明文，从而完成加解密或签名/验证功能。例如基于编码的公钥密码中的单向函数是大矩阵分解，D=ABC，由 D 求 A,B,C；为了满足陷门性，B 必须是纠错码，需要注意的是，在实际算法中都是使用了特殊的纠

QIC量子科技学研创新联盟
QIAC中国信息协会量子信息分会

错码。

2.2 发展历程

1978 年 Robert 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[30]。同年 Berlekamp 等人就证明了任意线性码的译码问题是 NP 完全问题[31]。随着量子攻击的出现，经典 McEliece 算法重新受到重视并入选 NIST 开展的 PQC 第三轮遴选，进入第四轮备选。

2.3 当前聚焦问题

McEliece 公钥密码的安全性高且加解密运算比较快，其密码方案经受了 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。其不足在于，通常基于编码的密码方案其公钥或密文值均长度较大。

在 NIST 第四轮签名算法征集中，征集到的基于编码的方案有 FuLeeca、Wave、LESS、MEDS、Enhanced pqsigRM 等算法。其中，FuLeeca 的公钥和签名尺寸都较小，但存在针对该算法的理论攻击。LESS、MEDS 算法其密钥、签名尺寸都不具备竞争性。而 Enhanced pqsigRM 算法为 NIST 之前征集到的 pqsigRM 算法的改进，由于 pqsigRM 算法受到了多次攻击，Enhanced pqsigRM 的安全性也有待验证。Wave 算法虽然具有较大的公钥尺寸，但也具有签名尺寸较小的独特优点。

QIC量子科技未来研创新联盟 QIAC中国信息协会量子信息分会

3. 基于哈希函数的密码

3.1 基本原理

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）。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。

从 Winternitz 一次签名方案开始，基于 Hash 函数的数字签名算法就形成了具备典型的启发式安全特征的公钥密码。这种公钥密码的陷门性表现不明显，而单向性由哈希函数的特征来体现和保障。

3.2 发展历程

1978 年 Rabin 首次提出了一次签名方案，该方案验证签名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。1989 年 Merkle 提出了 Merkle 认证树签名方案(MSS)[32]，如图 6 所示。Merkle 数字签

QIC量子科技产学研创新联盟 QIAC中国信息协会量子信息分会

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。

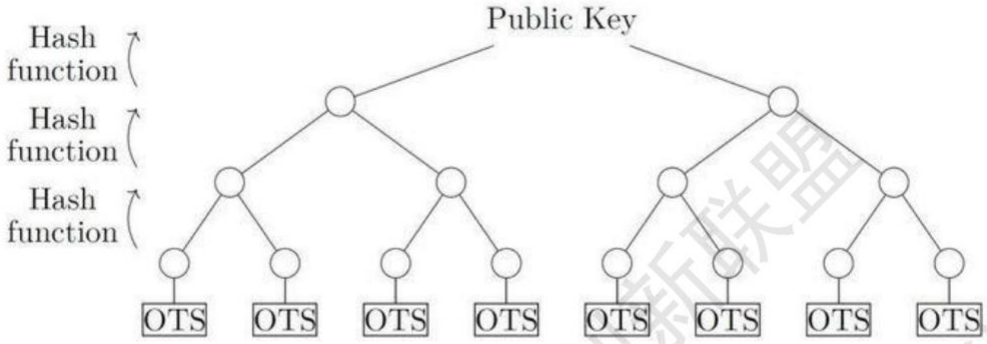


图 6 依据 OTS 一次签名算法和 Merkle 哈希树形成公钥原理图

在第三轮筛选后，NIST 已将基于哈希函数的 SPHINCS+作为数字签名 PQC 算法标准化正式制标的三种算法之一。

3.3 当前聚焦问题

基于哈希函数的密码算法的安全性仅取决于哈希函数本身，而不依赖其他困难问题假设。该类算法在签名、密钥尺寸及运行效率上并不占优势，但其安全假设成熟，这是其最大优势。对于 Merkle 签名方案来说，它具有明显的抗量子计算性质，并且签名和验证签名效率较高，缺点是签名值和密钥较长，产生密钥的代价较大。

目前，基于哈希函数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。

QIC量子科技产学研创新联盟 QIAC中国信息协会量子信息分会

在 NIST 的第四轮算法征集中，征集到了两个该类算法，即 Ascon-Sign 和 SPHINCS-α 。前者通过替换哈希函数改进了其运行效率。后者通过改进其单次签名的编码而改进了签名尺寸。

4. 多变量密码

4.1 基本原理

多变量（Multivariate-based）密码的基本原理基于多变量二次多项式。具体来说，它涉及到构造一个具有多个变量的二次多项式，这个多项式的系数是由接收者公开的，而其根是只有接收者和发送者知道的秘密。下面是此密码算法的基本原理步骤：

选择两个大素数 p 和 q，并计算它们的积 n=p*q。选择一个与 n 互素的整数 e，计算它的乘法逆元 d。选择一个二次多项式 f(x1, x2, ..., xm)随机生成，其系数在 Z/nZ 内。公开 n、e 和 f(x1, x2, ..., xm)。发送者生成消息 M，将其转化为 Z/nZ 内的元素。发送者计算 M 的 m 个坐标的乘积，得到一个在 Z/nZ 内的值。发送者用 d 对上述值进行加密，得到密文 C。发送者将 C 发送给接收者。接收者收到 C 后，用 e 进行解密，得到明文 M'。接收者验证 M'是否与原始消息 M 相同。如果相同，接收者接受该消息；否则拒绝该消息。

在这个过程中，只有发送者和接收者知道二次多项式的根，因此只有他们可以解密和验证消息。其他人即使知道公开的 n、e 和 f(x1, x2, ..., xm)，也无法解密消息。因此，这个密码体系提供了很好的安全性。

多变量二次多项式公钥密码体制（简称 MQ 公钥密码）的安全性基于有限域上多变量多项式方程组的求解问题（MQ 问题）。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。

多变量公钥密码中的单向函数是有限域上非线性多变量方程组求解，已知{f(x1,…,xt）=0}，求 x1,…,xt，为了满足陷门性，将 f 退化为简单函数（线性与特殊二次的复合）。

4.2 发展历程

目前基于多变量的公钥密码体制主要有：Matsumoto-Imai（MI）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。

1996 年 Patarin 针对 MI 算法的弱点提出了隐藏域方程 HFE 方案[33]。HFE 可看作为是对 MI 的实质性改进，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 的改进。

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。

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。

QIC量子科技产学研创新联盟 QIAC中国信息协会量子信息分会

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。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。

4.3 当前聚焦问题

多变量密码有验证速度快，签名值短的优点。其中 Rainbow 方案 2022 年也进入 NIST 的 PQC 标准第三轮评选（后继由于有公布的成功攻击而落选）。多变量密码是第四轮 NIST 签名算法征集中提交最多的种类，其中 SNOVA、DME-Sign、MAYO 效率较高。但其中也有部分算法已被指出存在成功攻击，包括 DME-Sign、Biscuit、HPPC、3WISE。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。多变量公钥密码的缺点还包括：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：

QIC量子科技产学研创新联盟 QIAC中国信息协会量子信息分会

(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. 其它类型 PQC 密码算法

基于超奇异椭圆曲线的数字签名算法典型的是 SIKE（超奇异同源密钥封装）算法。这类 PQC 算法基于的困难问题是寻找任意两条椭圆曲线之间的同源，其特性是有着非常小的公钥和签名大小，但是入选 NIST 公钥第四轮的 SIKE 算法被完全攻破，似乎使得研究人

QIC量子科技先导研创新联盟
QIAC中国信息协会量子信息分会

员对其丧失了信心。在第四轮 NIST 签名征集结果中仅有 SQIsign 一个算法。

另一类非占技术主流的新 PQC 算法是基于安全多方计算的抗量子计算密码，其源于 Yuval Ishai 等人提出的 MPC 脑中模拟（MPC in the head）技术，常被用于构造零知识证明、数字签名方案。该技术的基本思路是证明者模拟一个 N 方的安全多方计算，并对各方的视界（view）进行承诺，验证者通过打开其中部分承诺来完成验证。在第四轮征集中，征集到大量该类算法。其中，CROSS、RYDE 和 SDitH 算法基于故障（Syndrome）译码及其变种；MIRA、MiRitH 基于 MinRank 问题；MQOM 基于多变量问题的证明；PERK 基于置换核问题（Permuted Kernel Problem，简称 PKP）；AIMer 基于 AIM 单向函数；FAEST 则是基于 AES。其中 AIMer 和 FAEST 尽管被 NIST 分类为“基于对称的签名”，但其内部结构仍然遵守 MPC-in-the-head 技术路线。这些算法中，虽然没有算法能够在安全性或密钥、签名尺寸等方面优于 Dilithium，但 AIMer、FEAST、MIRA、RYDE、PERY 等算法都在保持一定签名、验证效率的情况下有效控制了密钥尺寸，从算法遴选应基于安全假设的多样性的原则上来看，都具备一定的价值。

在第四轮 NIST 签名算法征集结果中，还有 Preon 算法，它是基于 zk-SNARK 配合单向函数构造签名，其签名大小和时间都不具有竞争性。但除此不足外，目前针对 Preon 算法还未发布攻击成果或其它方面批评。

QIC量子科技产学研创新联盟 QIAC中国信息协会量子信息分会

6. 抗量子计算密码总体发展趋势和面临的挑战

6.1 从抗量子数学问题到可用密码算法的退化和折衷

如前所述，基于数学的密码算法构造过程中会引入陷门性，例如，为了实现密钥大小合适、加解密性能良好的具有使用价值的PQC 算法，实际的算法设计技术往往需要对其依据的原始计算困难问题进行改动，这种工程技术上的改动会使得得到的算法安全性上可能并不等价于数学上的困难问题，这些差异和妥协可能已经削弱了密码算法安全性。因此，PQC 算法的安全性还需要进一步探讨，从科学角度看现在就判定哪类 PQC 算法能抗量子计算攻击恐怕还为时过早。

6.2 PQC 算法安全性未来面临的挑战

另一方面，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。也就是说，PQC 的抗攻击能力到底如何？现在下结论恐怕为时尚早。PQC 作为新公钥算法，其安全性的评估是个复杂的问题：例如，PQC 算法同样也必须具备陷门；PQC 的抗量子计算攻击指抵御已知量子计算攻击，未来可能有新形式的量子攻击出现；为了抗量子攻击，PQC 设计上还可能“顾此失彼”即被有针对性的传统算法破解。近一两年来已经有多个 PQC 算法被传统方法破解的案例。2022 年 2 月，IBM 的专家发表论文宣称基于多变量密码（MQ）的 Rainbow 签名算法在其算

QIC量子科技产学研创新联盟 QIAC中国信息协会量子信息分会

法参数为安全等级为 1 的情况下，被一台笔记本电脑用 53 小时运行经典算法成功破解[34]。2022 年 4 月，以色列军方又发布了一份技术报告《错误学习问题（LWE）的安全性报告：改进的对偶格攻击方法》[35]，基于经典算法的改进成功地实现了对格密码中 LWE 算法的攻击。曾经入选 PQC 标准筛选结果中的 3 个算法(Kyber、Saber 和 Dilithium)会受该攻击方法影响。

6.3 PQC 算法应用和实施需关注的重点问题

由于 PQC 具有物理实现兼容于现有信息技术和工艺的优点，更易于实现标准化、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 算法的过程是一个较复杂的过程；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。

总体上看，PQC 算法实现标准化并经过实现正确性、安全性等方面的测试与评估验证后，PQC 的优势是能提供灵活性较高的各类用户端解决方案，以软件形式为主，适用于互联网等不依赖于专用硬件设备、软件升级适配方便的轻量级应用场景；当然也可以形成硬件解决方案。另外，各类 PQC 算法适用场景具有显著的差异性，其在密钥长度、运算速度和功能完善性上的粗略比较如表 4 所示。

QIC量子科技产学研创新联盟 QIAC中国信息协会量子信息分会

表 4 PQC 主要算法类型定性比较

密码类型	公钥大小	计算速度	主要功能
格密码	小	快	加密、签名、密钥交换等
基于编码理论的密码	大	较快	主要用于公钥加密
多变量密码	较大	较快	主要用于数字签名
基于哈希函数的密码	小	较快	用于数字签名
基于超奇异椭圆曲线的密码	很小	慢	用于数字签名

7. 抗量子计算密码产业生态现状

在过去的一两年中，抗量子计算密码的技术实现方面得到了稳步发展。以实现量子安全为出发点，各国政府、相关科研机构及商业机构非常重视，也在计划和加快部署抗量子计算密码技术的应用。

7.1 国际 PQC 产业发展

2023 年以来，抗量子计算密码的生态建设、产品发展与商业化应用发展迅速。2023 年 8 月，美国国家网络安全中心（NCCoE）发布了一份新的《向抗量子计算密码学迁移》白皮书。该文档简要概述了向抗量子计算密码学迁移项目的背景、目标、挑战、效益和工作流程，此外还列出了参与该项目的最新 28 家技术供应商名单。国际上 ICT 行业跨国公司如 IBM、微软、谷歌、亚马逊、思科、华为等都投都在 PQC 的研究上投入了力量并形成了相应研究成果。IBM 在该领域研究重点是格密码。微软参与了 FrodoKEM、SIKE、Picnic 等 PQC 项目的研究，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），

QIAC中国信息协会量子信息分会 量子科技产学研创新联盟

2018 年微软发布了开源项目 OpenVPN 下名为 PQCrypto-VPN 的分支项目，它在 OpenVPN 中实现了 PQC 算法。谷歌公司在对当前抗量子计算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。2023 年，谷歌公司宣布在其 Chrome 浏览器新版本上采用了 Kyber 密钥封装算法，用于在安全的 TLS 网络连接中安全的传输对称工作密钥，8 月谷歌又发布了首个开源的抗量子的 FIDO2 安全密钥实现，使用了 ECC/Dilithium 混合签名方案。2024 年，苹果公司在其即时通讯应用 iMessage 中引入了 Kyber 算法用于实现数字签名，以增强其通讯应用安全性，防止量子攻击威胁。

国际上也出现了一些面向 PQC 方向的初创公司。传统安全公司 Onboard Security 致力于面向格密码算法 NTRU 的研究。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，并从 2011 年起就发布了多种实现 NTRU 算法的软件库。

开源界也形成了 PQC 方向相关的开源社区，并开发了一些 PQC 开源项目。如“开放量子安全（Open Quantum Safe）”项目，目标是建立 PQC 算法的 C 语言库 liboqs，已被应用到开源安全软件 OpenSSL，类似的项目还有 NTRUOpenSourceProject 等。2023 年 9 月，移动通讯软件 Signal 宣布将其 X3DH(Extended Triple Diffie-Hellman)规范升级为称为 PQXDH(Post-Quantum Extended

Diffie-Hellman)的方法——它同时使用原 XD3H 的椭圆曲线密钥协商协议 X25519 和 PQC 类密钥封装算法 Kyber，融入了抗量子的工作密钥生成机制。

7.2 国内 PQC 产业发展

我国密码管理部门早在 2018 年就面向全国开展了抗量子计算密码算法设计竞赛活动，其中公钥算法部分征集到 38 个算法，并最终评出 14 个优胜算法，2019 年经第二轮筛选获得 12 个算法。并已经在积极推进 PQC 算法的标准化工作，基于 SM3 算法的抗量子公钥密码算法、量子安全的 ZUC-256 对称密码算法等已经提上标准化日程。华为公司计划尽早为密码协议引入安全的抗量子算法，以确保其产品的长期安全性，并计划在国内 PQC 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。

我国的密码科研团队一直是 PQC 公钥算法研究工作的重要力量之一，从客观审视的角度，普遍认为当前热门的 PQC 公钥算法的安全性尚待持续研究，对目前开展 PQC 公钥算法的标准化比较审慎。2024 年 1 月，中国抗量子密码战略与政策法律工作组成立，将对抗量子密码技术、产业、业务的现状和相关国内外政策、法律法规进行研究，发表抗量子密码相关研究成果，推动形成中国抗量子密码共识和行动方案。

QIC量子科技未来创新联盟 QIAC中国信息协会量子信息分会

8. 国际抗量子计算密码算法征集和标准化活动

8.1 国际有代表性的 PQC 标准化活动

2015 年欧盟率先启动抗量子计算密码算法 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，又开展了全球抗量子计算密码算法旗舰项目 PQCRYPTO。并于 2018 年开展了后续的 PROMETHEUS 项目，致力于打造新一代安全实用的抗量子计算密码方案。类似的还有日本的 CREST 项目也取得了较显著的成果。

欧洲电信标准化协会（ETSI）成立了 QSC 小组，专门负责 PQC 方面的标准制定和研究工作。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 ETSI GR QSC 001《量子安全算法框架》报告；2017 年 QSC 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》、《量子安全密钥交换》报告；2018 年 QSC 发布了《量子安全虚拟专用网》报告；2019 年 QSC 发布了《基于量子安全认证的加密》报告；2020 年，QSC 发布了《量子安全计划的迁移策略和建议》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。

国际标准化组织（ISO/IEC）中专门负责 PQC 相关工作的组织是 ISO/IECJTC1/SC27 下的 WG2 小组。2015 年，该小组开始了一项 PQC

QIC量子科技产学研创新联盟 QIAC中国信息协会量子信息分会

的调研工作，经过多轮讨论，在 2017 年 ISO 同意终止调研期并启动一项常设文件（WG2/SD8）的项目。

互联网产业方面权威的国际互联网工程任务组（IETF）也正在进行抗量子计算密码算法草案的设计。2023 年 1 月，IETF 启动了抗量子协议使用（PQUIP）工作组，其它代表性工作还包括制定了 IETF RFC 8391 《XMSS: eXtended Merkle Signature Scheme》。

美国电气和电子工程师协会（IEEE）制定了 IEEE 1363.1-2008《基于格上困难问题的公钥密码技术标准》。

2022 年，韩国也展开了抗量子计算密码标准化竞赛 KpqC，为其标准化工作做准备。在 KpqC 第一轮中，共征集到 7 个加密算法和 9 个签名算法。

我国于 2023 年 12 月成立了由国家密码管理局担任指导单位的中国抗量子密码战略与政策法律工作组，并发布了《中国后量子密码政策法律蓝皮书（2023）》。

总体上看，美、欧等传统发达国家处于抗量子计算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组织联合等方式开展了很多合作工作。

QIC量子科技产学研创新联盟
QIAC中国信息协会量子信息分会

8.2 NIST 抗量子计算密码算法标准化活动及制标情况

（1）NIST 的 PQC 算法征集活动

美国国家标准与技术研究院（NIST）早在 2009 年就发表了名为“Quantum Resistant Cryptography: A Survey”的学术报告，并

于 2012 年成立 PQC 项目组，2016 年发布抗量子计算密码算法标准化工作计划，开始向全球征集 PQC 密码算法。NIST 对 PQC 标准化的进展和计划如表 5 所示。从 NIST 征集抗量子计算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，进入 NIST 标准制标名单的算法多是西方国家团队共同研发的，较大程度上体现了国际合作，以及全球学术界、产业界对 NIST 标准化工作的认可度。

表 5 NIST 对 PQC 标准化的进展和计划

时间	工作阶段
2016 年 4 月	NIST 发布量子后密码学报告（编号 NISTIR 8105）
2016 年 12 月	正式提出征集算法呼吁提案
2017 年 11 月	第一轮算法征集的提交截止日期
2017 年 12 月	第一轮算法宣布（69 份提交被接受为"完整和正确"）
2018 年 4 月	召开首届 PQC 标准化会议
2019 年 1 月	第二轮候选算法公布（26 种算法）
2019 年 3 月	第二轮算法征集的更新提交截止日期
2019 年 8 月	召开第二届 PQC 标准化会议
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）
2020 年 10 月	第三轮更新提交包的截止日期
2021 年 6 月	召开第三届 PQC 标准化会议
2022 到 2024 年	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抗量子计算密码算法。其中基于格和编码构造的最多，主要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；基于哈希的构造方案只用于了数字签名算法。

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 抗量子计算密码标准征集工作。

2020 年 7 月，NIST 公布了 PQC 算法经第三轮筛选的 7 个最有希望入选、有望得到广泛应用的候选算法，其中公钥加密算法有 Classic McEliece、Kyber、NTRU、SABER；数字签名算法有 DILITHIUM、FALCON、Rainbow，如表 6 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，也作为候补算法入选：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 7 所示。本轮筛选中没有中国研究者提交的算法入围。

2021 年 NIST 在结束第三轮审查后，一方面正在开展第四轮抗量子签名算法征集活动；另一方面 NIST 对第三轮审查后上述 7 项决赛入围算法进行审查供制定标准参考。

表 6 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	—	—

QIC量子科技先导研创新联盟 QIAC中国信息协会量子信息分会

表 7 NIST 对 PQC 标准化的第三轮候补入选算法

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］	—

总体来看，NIST 对 PQC 算法遴选准则体现了筹划时间长、征集范围广、评审过程严的特点。从标准方案的选择上，NIST 希望其批准的算法具有多样性，也即依赖于尽可能不同的假设，对于第三轮入围的 BIKE、HQC、Classic McEliece 以及 SIKE 算法，进入第四轮备选。对于目前入选的具体算法，由于 KYBER、NTRU 和 SABER 都是基于格的方案，签名方案中的 CRYSTALS-DILITHIUM 和 FALCON 也是如此。一方面，体现了 NIST 倾向于认为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。另外一方面，为改善签名算法基于的安全假设单一性问题，第四轮征集也希望征集到基于结构格问题以外的算法。2023 年 7 月，NIST 公布其征集到的数十个算法，大致可以被分类为基于编码、基于格、基于安全多方计算、基于哈希函数、基于多变量、基于超奇异椭圆曲线以及基于其他问题几大类。

QIC量子科技实验室创新联盟
QIAC中国信息协会量子信息分会

（2）标准化过程中落选算法

基于多变量的 Rainbow 和 GeMMS 由于有公布的成功攻击而落选，而 Picnic 则与 SPHINCS+同样仅依赖对称组件，但由于其依赖的 LowMC 对称加密存在安全隐患而落选。

在 EUROCRYPT2023 会议中，出现了多篇对 SIKE 的攻击，SIKE 团队公开承认其算法已被破解。

在 CRYPTO2023 会议中，出现了对 BIKE 的解密失败概率的新的分析，利用这一点此文章对 128 比特版本的 BIKE 算法给出了一个 119.9 比特的攻击。

Saber、NTRU 和 NTRUprime 由于和 Kyber 在困难问题假设上相似， NIST 不计划批准多个基于结构格的方案而淘汰了上述三个方案。

Frodo 基于无结构化格，学术界公认无结构化格的安全性稍微高一点，但相比之下效率低。据称它是因为效率不足被淘汰，而德国等国家则出于自身的安全考虑，仍首选 Frodo。

（3）NIST 的 PQC 算法标准化制标情况

2022 年，NIST 批准了四个算法进入制标阶段，包括一个公钥加密（密钥封装）算法和三个数字签名算法。四个算法中有三个基于结构格，一个基于哈希。如表 8 所示。2023 年 8 月，NIST 发布了四种算法中三种算法的标准草案，只有第四种算法 FALCON 的标准草案被推迟发布（NIST 宣称将于 2024 年底发布 FALCON 的标准草案）。之后 NIST 就公布的这三个标准草案收集全球密码界反馈意见，2024

QIC量子科技产学研创新联盟 QIAC中国信息协会量子信息分会

年 8 月，NIST 正式发布了首批三个标准（FIPS 203、FIPS 204、FIPS 205），最终计划最迟于 2026 年左右形成其全套 PQC 标准。

表 8 NIST 的 PQC 标准化的第三轮算法筛选后拟制标算法

第三轮后	最终拟制标算法	
类别	公钥加密/密钥封装	公钥签名
基于格	KYBER [MLWE]	CRYSTALS-DILITHIUM [MLWE、Fiat-Shamir]
		FALCON[NTRU]
基于杂凑	—	SPHINCS+[杂凑]

制标的数字签名方案：数字签名标准 FIPS 204 规定的是基于 Module-LWE 困难问题的 Dilithium 算法；数字签名标准 FIPS 205 规定的是基于无状态哈希函数的 SPHINCS+算法；基于结构格问题的 Falcon 算法还未形成算法草案。Dilithium 和 Falcon 都具备较好的性能。尽管 SPHINCS+密钥、签名尺寸及签名、验证效率都较低，但其仅基于哈希函数的保守安全性得到了 NIST 的青睐。

制标的公钥加密/密钥封装方案：密钥封装标准 FIPS 203 规定的是基于 Module-LWE 困难问题的 Kyber 算法。NIST 最终是权衡效率、安全性基础等因素仅选择了 Kyber 算法作为标准。在 Kyber 与另一算法 Frodo 之间的最后选择有一些内部比较和争论——前者使用结构化格，后者使用无结构化格。NIST 认为，如果选 Frodo 而非 Kyber，这就向外界传递了美方对结构化格的方案信心有所不足，这马上就会影响到另一大类基于编码的方案。因此，NIST 决定将 Kyber 推出作为目前唯一的密钥封装正式制标算法。

QIC量子科技产学研创新联盟 QIAC中国信息协会量子信息分会

（二）基于量子物理的量子密码

现代的物理手段有：专人专程递送密件，设备出厂前预置固定密钥，基于量子物理原理的量子密码，基于信道物理特征的无线信道密钥分发技术等。无线信道密钥分发技术原理是基于无线信道的互易性，使得通信双方能够在公共信道中获得高度相关的信道特征。同时，信道环境的时间和空间变化性，为物理层密钥带来了一定的随机性和防窃听能力。

1. 量子密钥分发

量子密钥分发（QKD）基于物理原理，能够抗截获、抗窃听、抗破译地为通信双方分发具有信息理论安全性的对称密钥，从而从整体上提升密钥管理的安全性与独立性。

1.1 从分发模式区分的 QKD 方案类型

自 1984 年 Bennett 和 Brassard 提出第一个量子密钥分发方案以来，30 余年来学者们提出了多种量子密钥分发方案。关于量子密钥分发方案的分类，从分发模式上看主要可以分为制备-测量（prepare and measure）和纠缠测量（entanglement-based）两大类，由于纠缠测量方案实现难度大，又衍生出一种纠缠反演测量方案。表 9 比较了这三种分发模式中分发-测量量子态的特点和通过校验分析获得安全密钥的原理。

QIC量子科技产学研创新联盟
QIAC中国信息协会量子信息分会

表 9 QKD 方案分发模式分类对照说明

分发模式	量子态分发测量方式	安全校验内容	安全原理	设备可信要求
制备测量	A 发单量子，B 测量	A 和 B 比对收发结果，通过错误率分析评估窃听干扰情况	单量子测不准、不可复制，信道窃听必然留下痕迹	发送、测量设备均可信
纠缠测量	第三方分发纠缠，A 和 B 测量	A 和 B 比对测量结果，分析评估双方测量到最大纠缠的比例	最大纠缠没有第三方关联，第三方无法从中获取信息	设备无关（DI）
纠缠反演	A 和 B 发单量子，第三方测量	A 和 B 比对双方发送和第三方测量结果，分析在第三方测量时形成最大纠缠的比例		测量设备无关（MDI）

注：记分发密钥的双方为 A 和 B。A 和 B 使用的量子态分发或测量设备可能是不可信的，但是他们进行结果校验的行为是安全可信的。

1.2 从量子态载体及其调制方式区分的 QKD 方案类型

第二种分类方式是基于量子态载体及其调制方式上的分类，主要可以分为离散变量和连续变量两种。表 9 所列的三种分发模式均可以有离散变量和连续变量的实现方式，两种方式的调制特点和技术实现优缺点比较如表 10 所示。

表 10 QKD 方案调制模式分类对照说明

调制模式	调制物理量	信号载体	单量子实现	主要优势	主要劣势
离散变量	偏振、相位、角动量等离散量	单光子脉冲	单光子分析	1. 噪声分析简单，安全密钥提取比较简单； 2. 有限码长安全证明已完成； 3. 工作距离较远。	1. 高对比度脉冲调制速率低； 2. 单光子探测较连续变量方式效率低； 3. 成码速率较低。

QIC量子科技产学研创新联盟 QIAC中国信息协会量子信息分会

调制模式	调制物理量	信号载体	单量子实现	主要优势	主要劣势
连续变量	位置-动量等连续的共轭量	相干光压缩光	散粒噪声分析	1. 调制速率高； 2. 相干探测技术、器件成熟； 3. 短距离成码率高。	1. 噪声分析复杂，安全密钥提取运算要求高； 2. 有限码长安全证明还是开放问题； 3. 工作距离较短。

目前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实现了较大规模的商用。如图 7 所示的 BB84 协议方案实现量子密钥分发的工作流程包括：发送方制备编码（对离散变量常用偏振、相位、时间进行编码）单量子态、传输、接收方测量解码，然后双方通过经典通信进行筛选比对、误码检测和纠错、保密增强。



图 7 单量子制备测量（BB84 协议）方案原理图

单量子制备测量方案利用了单量子不可分割、不可复制、测不准等特性，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，均可被接收方察觉，从而杜绝了从信道上实施窃听的可能性。

测量设备无关（MDI）协议也属于制备测量方案的一种，是一种基于纠缠反演思想提出的新方案，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。设备无关协议的安全性不依赖于 QKD 设备工作状况，而是基于 Bell 不等式可以证明其安全性。

纠缠测量方案实现量子密钥分发的工作流程包括：在双方分享纠缠对的基础上（纠缠对可以由第三方提供），双方分别测量解码，然后双方通过经典通信进行纠缠校验、纠错、保密增强。如图 8 所示：

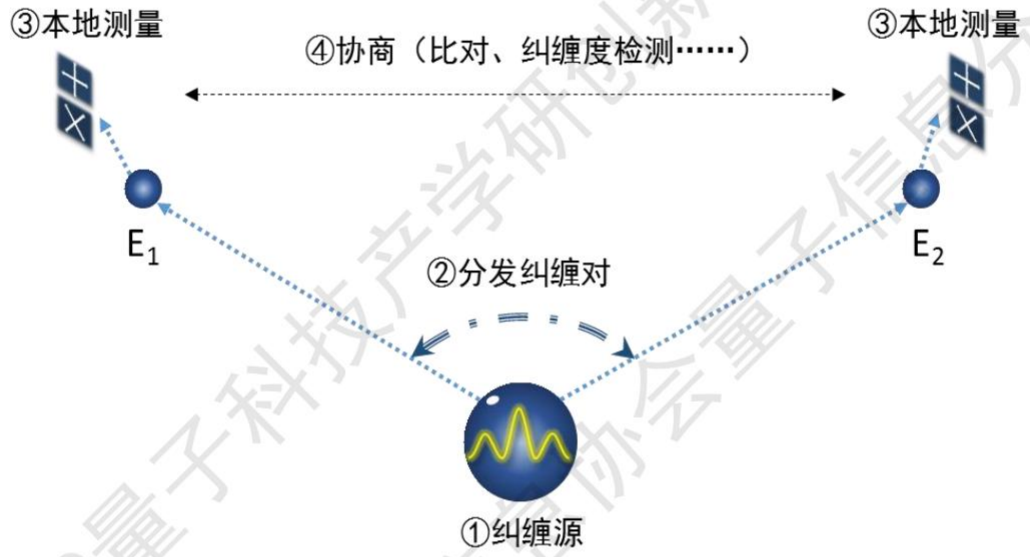


图 8 纠缠测量方案原理图

纠缠测量方案利用了两体最大纠缠态没有第三方关联、LOCC 操作（局域操作和经典通信）无法制造远程纠缠的特性，确保了纠缠制备方无法预知协商双方测量结果，本地测量装置也无法伪造纠缠，实现器件无关安全性。我国在基于“墨子号”卫星的星地一体的 QKD 网络中，已经实现了基于纠缠测量的量子隐形传态实验验证，如图 9 所示。

QIC量子科技产学研创新联盟 QIAC中国信息协会量子信息分会

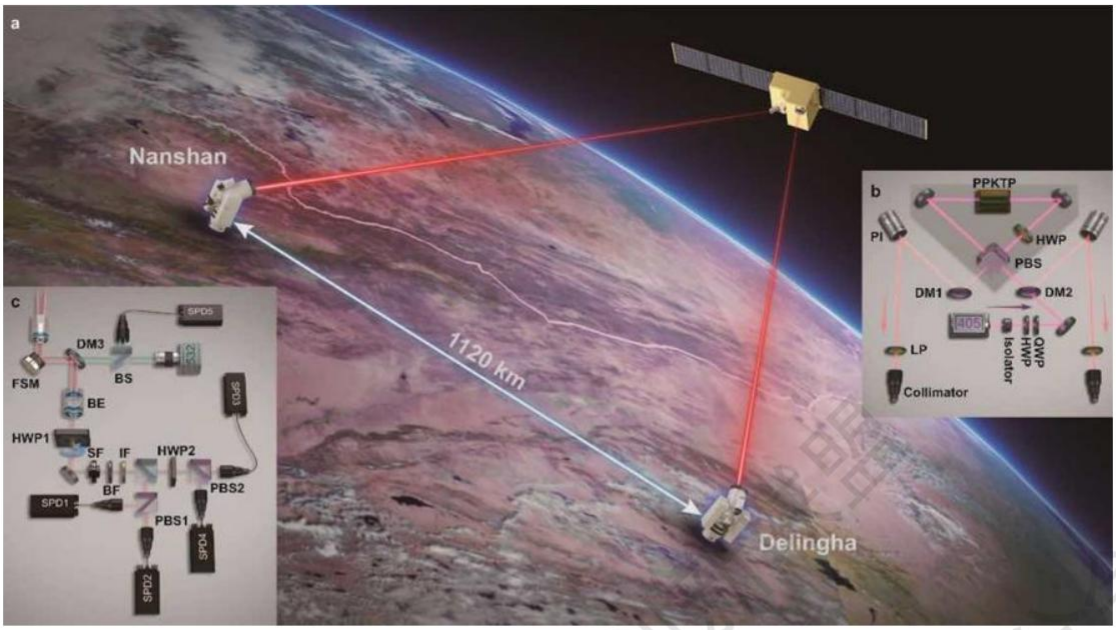


图 9 在星地 QKD 网络中实现的纠缠测量方案原理图

目前，已有的各类主要 QKD 协议说明如表 11 所示。

表 11 主要量子密钥分发协议分类

分发模式	调制方式	编码和探测方式	协议（年代）
制备测量	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)[36] 六态协议(1998)[37] SARG04(2004）[38] DecoyBB84(2005)[39][40][41]
		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，属一类易于调制的变形方案，单光子性还不严格，还没有严格理论安全证明能抗相干攻击	DPS(2002)[42] COW(2005)[43] RRDPS(2014)[44]
	连续变量	发送端编码时，对相干光或压缩光脉冲的两个共轭分量进行连续高斯调制，或对；接收端用平衡探测器对光脉冲进行探测。	GG02(2002)[45] QPSK(2009)[46]
纠缠测量	离散变量 连续变量	第三方分发或在收发双方间建立纠缠态，既可以是离散变量也可以是连续变量，双方进行纠缠检测。 目前以离散变量方案实验为主。	E91(1991)[47] B92/BBM92(1992)[48] DI(2007)[49]

分发模式	调制方式	编码和探测方式	协议（年代）
纠缠反演	离散变量 连续变量	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。 目前以离散变量方案实验为主。	MDI-QKD(2012)[50] PM-QKD(2018)[51] TF-QKD(2018)[52]

量子态制备测量方案可以看作是对纠缠测量方案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。而且，这两类量子密钥分发方案都需要通过经典协商才能完整地实现密钥分发，这是因为量子测量的结果具有随机性，通信双方只有首先比对筛选出落在相同基矢下的结果才能获得密钥。

2. 其它量子密码方案

2.1 量子数字签名

现用如第一章所述的公钥算法，其安全性的基础是大数分解等数学问题的复杂性假设，因此它是计算安全并且是启发式安全的，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。量子数字签名（QDS）可以实现认证对方身份真实性及验证信息完整性等传统数字签名的功能，也不依赖于其它安全假设，能提供信息理论层面的安全性。目前量子数字签名还需要面对实用化上工程技术问题的诸多挑战，但仍受到了颇为广泛的关注和研究。

QIC量子科技产学研创新联盟 QIAC中国信息协会量子信息分会

第一个量子数字签名方案于 2001 被年提出[53]，其原理是利用 n 个量子比特可以构成 2^n 个量子态，因此将一组 n 量子比特态构成的集合作为公钥，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，因此当前不具备实用性。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[54]，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，国内中科大团队[55]和国外团队[56]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。

QIC量子科技光学创新联盟 QIAC中国信息协会量子信息分会

2.2 量子随机数发生器

量子随机数发生器（QRNG）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，它制备的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。QRNG 可以广泛的应用于 ICT 行业中需要生成真随机数的仿真、密码、通信等多种应用领域。

根据不同的量子力学原理，量子随机数发生器方案可分为基于单光子检测的和基于宏观探测的两类。QRNG 研究开始于二十世纪五六年代。近年来，QRNG 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 QRNG 方案以解决实际设备缺陷导致的安全问题。

2.3 量子隐形传态

量子隐形传态（Quantum Teleportation）是指利用量子纠缠来直接传输微观粒子的量子状态即量子信息，而不用传输这个微观粒子本身。1993 年，Bennett 等人第一次提出了量子隐形传态的方案[57]，实现了未知量子态的远程传递。量子隐形传态技术原理是基于纠缠量子态实现的，实现原理如图 10 所示。

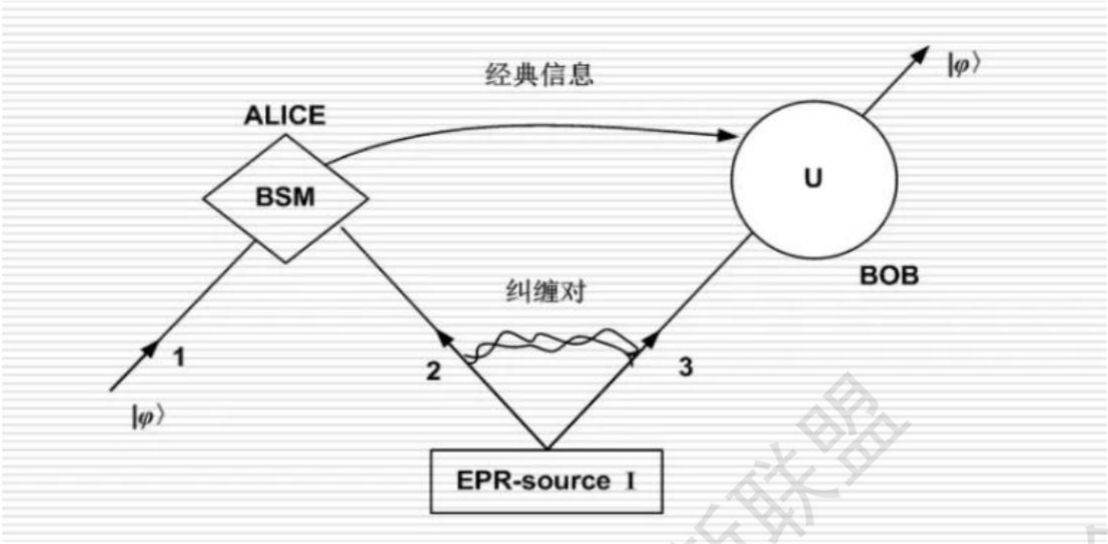


图 10 量子隐形传态主要流程示意图

（1）由 ERP 源生成一对处于纠缠状态的粒子 2 和粒子 3，其中粒子 2 传递给发送方 Alice，粒子 3 传递给接收方 Bob。

（2）发送方 Alice 将待传输的粒子 1 和粒子 2 进行联合测量（称为贝尔态测量或联合 Bell 基测量），由于量子纠缠非局域关联特性，测量后两个粒子的量子态将随机地塌缩到共同测量本征态中的一个，此时粒子 1 的量子态会作用于接收方 Bob 的粒子 3。

（3）发送方 Alice 通过经典信道将粒子 1 和粒子 2 的联合测量结果传输给 Bob，Bob 根据收到的结果对粒子 3 做相应的酉变换操作，使得粒子 3 的量子态与之前的粒子 1 完全相同，从而完成量子态的“转移”。

从 1997 年 Bouwmeester、潘建伟、Zeilinger 等第一次量子隐形传态实验成功[58]至今 20 多年，大体上可以分为验证传送能力、探索量子互联网功能两个阶段。在验证传送能力阶段，学者们先后实现了选择目的地传送、多光子复合传送、单光子多自由度传送、

QIAC中国信息协会量子信息分会 量子科技产学研创新联盟

光与原子间传送、远距离传送、高维态传送等基础传送功能。值得一提的是，这个阶段的大量验证实验都是我国学者基于多光子纠缠调控技术率先完成的，“墨子”号卫星也保持着千公里纠缠分发与隐形传态的纪录。探索量子互联网功能阶段起步不久，预计仍将持续多年，学者们已经实现了多种类型的量子纠缠源和量子存储器，也初步实现了将两者结合起来形成存储器纠缠、量子中继网络节点等，设计了一些基于小型纠缠网络的密码相关应用。

总体上，由于量子隐形传态需要制备和测量纠缠，相对于可以使用单光子的量子密钥分发有更高的实验技术要求，目前量子隐形传态还处于实验室研究阶段，但主流研究者认为未来量子隐形传态的应用前景非常广阔，量子通信进入量子互联网阶段将很大程度的利用量子隐形传态及其依赖的量子纠缠技术手段。安全是量子隐形传态的内禀性质，它同样可以实现量子安全的数据通信，而且可以实现密钥的安全协商，也可支撑量子数字签名、量子秘密共享等各种安全协议。

3. 量子密码面临的挑战

基于量子物理的密码技术总体上还处于起步阶段，无论是密码功能的完整实现还是关键量子技术的能力提升，都还有很大的上升空间。量子数字签名、量子秘密共享、量子多方安全计算等一系列量子安全协议还处在方案设计和原理试验阶段。QKD 是量子密码中发展最为成熟的分支，本节主要基于 QKD 进行讨论。

QC量子科技产业创新联盟
QIAC中国信息协会量子信息分会

3.1 QKD 进一步完善功能

由于 QKD 具有光通信系统的一般特征，随着传输距离增大，信号丢失、信噪比下降等情况会导致成码率下降，QKD 与传统光通信的核心差异在于使用量子态来保证安全性，代价是只能概率性地成功接收信号，数据传输速率受限。量子密码硬件设备的工程技术实现有一定的难度、目前成本还较高。

这些都要求量子相关器件和设备在成码距离、成码率、工程可靠、高性能、小型化等方面持续提升。具体体现在：高效率的单光子探测、高精度的物理信号处理、高信噪比的信号调制、光学/光电集成、制冷集成、高速高精度专用集成电路等。QKD 通过嵌入各类密码系统，将逐步具备支撑深度融合、大规模应用服务的能力。

3.2 提升 QKD 现实安全性的相关研究

经过全球学术界三十余年的共同努力，QKD 的理论安全性已经得到了证明[59][60]。在现实条件下，受器件加工工艺、设备成本等因素的影响，实际光电设备的性能参数和 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。这被称为 QKD 的现实安全性研究，其重要目标就是针对实际器件性能容差容错的安全性证明，以保障实际 QKD 系统的信息理论安全性。通过对现实物理设备建模并将其纳入安全性分析，以及进行新型协议的设计，现实条件下的安全性也已经建立起来了[61]。换而言之，QKD 所声称的信息理论安全性

QIC量子科技产学研创新联盟 QIAC中国信息协会量子信息分会

保障，并不仅仅局限于完全符合标准协议的理想系统。实际 QKD 系统采用的各个关键部件性能偏差对于安全性的影响，在 QKD 安全性研究的一系列进展中已经逐个得到分析。对 QKD 设备缺陷的安全性分析已经比较完善，能够通过一个综合安全模型分析几乎所有的源端缺陷和主要探测端的缺陷[62]，对于尚未纳入模型的缺陷也可以通过参数监控进行有效防御。实际的 QKD 系统能够在足够宽泛的程度上容忍部件性能的不理想，并仍然提供信息理论安全的密钥分发。这种容差和容错的能力还在随着 QKD 安全性研究的深入而逐渐提高，并使得制造 QKD 产品的工程难度逐步下降。

QKD 现实安全性的研究一直伴随 QKD 的产业化进程，早期主要针对光源偏离理想模型的不完美性，随着工艺的完善，这一问题目前已得到很好解决。QKD 的研究中还提出了多种有针对性的安全免疫方案，可以免疫关键部件如光源和探测器的安全漏洞。在光源端，最为显著的进展是清华大学王向斌教授[40]和国外 H.-K.Lo 教授[41]各自独立地发展了诱骗态方法以抵御光子数分离攻击，目前诱骗态方法已成为保证 DV-QKD 安全性的标准方法。在测量端防御的主要难度在于使用者一般难以控制测量端所可能接收的信号，利用 MDI-QKD 协议的测量设备无关特性，可以很好的抵御测量端的量子黑客攻击。

QIC量子科技产学研创新联盟 QIAC中国信息协会量子信息分会

4. 量子密码技术研究进展

4.1 发展总体趋势

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[63]，如图 11 所示。短期是量子保密通信阶段，应用量子密钥分发技术，为国防、政务、能源等用户提供高安全的数据传输和通信服务；中期是量子安全互联网阶段，以量子密钥分发技术为基础构建广泛的密钥管理网络，结合量子安全的密码算法，为金融、医疗、个人消费、云数据、电信服务等提供系统性的量子安全服务；远期是量子信息网络（即量子互联网）阶段，即随着量子中继、量子计算机、量子传感及测量等技术的成熟，应用量子隐形传态等量子通信技术手段，依托星地一体的广域量子通信网络，实现量子安全网络、量子云计算网络、量子传感网络等网络服务。欧洲量子旗舰工作规划中对量子互联网进行了详细阐述并于 2023 年成立了量子互联网联盟 QIA。目前在工程技术实现方面，我国已经进入了应用发展路线图的中期阶段，而预计再需要 10 年左右的时间，有望进入发展路线图的远期阶段。

QIC量子科技产学研创新联盟
QIAC中国信息协会量子信息分会

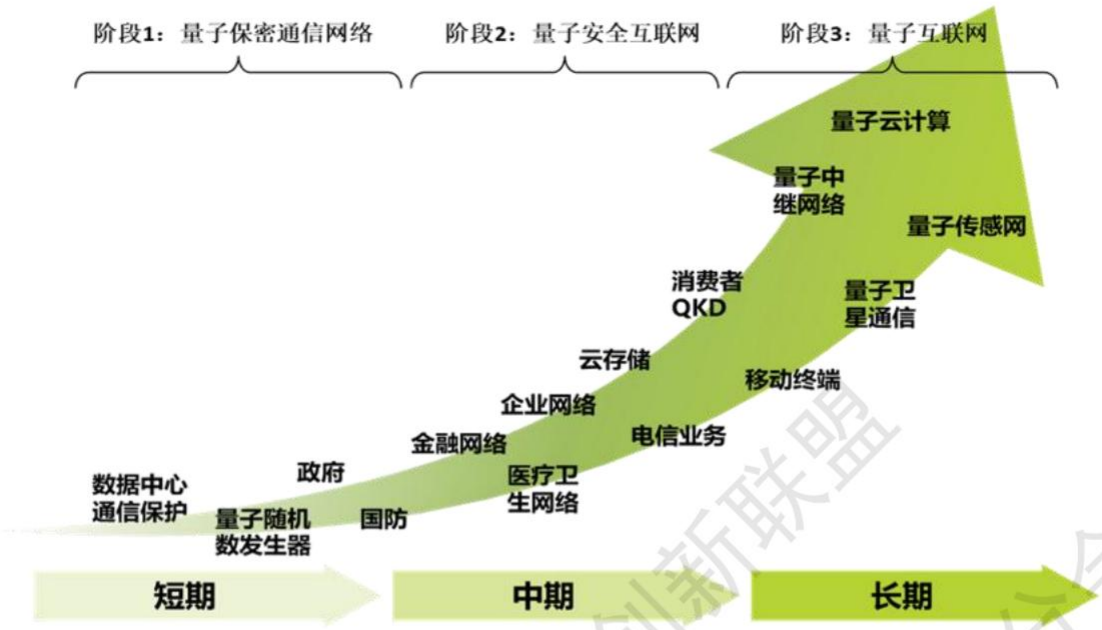


图 11 量子通信应用发展展望[63]

4.2 前沿技术成果

（1）高成码率/高速率 QKD 技术

2018 年，东芝（欧洲）剑桥研究实验室设计实现了高吞吐速率的 QKD 后处理模块，结合高速自差分探测器在背靠背连接条件下（插损约 2dB）实现了 13.72Mbps 的成码率[64]；

2020 年，瑞士日内瓦大学利用高带宽的数模驱动芯片实现了 5GHz 的高速 QKD 系统，成码率达 390kbps@100km[65]。

2023 年，中国科学技术大学实现 2.5GHz 高速 QKD，10 公里标准光纤信道下密钥率达到 115.8 Mb/s[66]。

（2）远距离 QKD 技术

2018 年，瑞士日内瓦大学实现单跨 421 公里光纤量子密钥分发世界纪录[67]；

QIC量子科技产学研创新联盟 QIAC中国信息协会量子信息分会

2018 年，中国和奥地利科学院应用“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[68]；

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 1120 公里两地间的量子密钥分发[69]；

2021 年，中国实现基于发送-不发送双场协议的 511 公里现场光纤量子密钥分发实验，成码率为 3.37bps@81.76dB[70]；

2021 年，东芝（欧洲）剑桥研究实验室实现了基于双场协议的实验室内 600 公里光纤量子密钥分发实验，成码率为 0.778bps@104.8dB[71]；

2021 年底，中国研究者基于改进的四相位调制双场协议实现了目前实验室内最远的基于光纤的 QKD 试验系统安全传输距离 833.8 公里[72]。

2023 年，中国科学技术大学实现了最远达 1002 km 的双场量子密钥分发，实验证明了 SNS-TF-QKD 协议通过超长光纤通道实现的可行性[73]。

（3）小型化 QKD 系统

2019 年，新加坡南洋理工大学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[74]；

2020 年，英国布里斯托大学实现基于 InP 芯片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 6×2mm^2 的 InP 芯片上，达到了 40dB 成码率 1bps[75]；

QIC量子科技发展创新联盟
QIAC中国信息协会量子信息分会

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 4.8×3mm^2 的硅光芯片上，并实验实现了 36dB 成码率 31bps[76]；

2021 年，东芝欧洲公司实现了 QKD 光学功能模块全部芯片化，并研制成功插拔光模块（编码、探测）的小型 QKD 终端产品[77]。

（4）量子中继和量子存储

2021 年，荷兰代尔夫特大学大学实现了多节点量子互联网原型实验，采用基于金刚石色心量子比特的三节点量子纠缠网络，演示了无需后选择建立三节点 GHZ 纠缠和通过中间节点执行纠缠交换[78]；

2021 年，德国马普所实现双原子腔量子存储并演示了量子中继和基于纠缠的设备无关量子密钥分发原理性实验，系统的误码率总计约 8%，预期可以在 30km（损耗约 7dB）线路上实现 10^{-5} 的成码率[79]；

2021 年，清华大学实现长时间量子存储的可扩展中继实验，采用原子系综量子存储器，存储时间达数十毫秒，支持按需纠缠交换并加快了纠缠连击率[80]；

2021 年，中国科学技术大学完成亚秒级光子-原子纠缠存储实验，通过环形腔的双重控制模式制备纠缠，使用三维光晶格延长存储时间，0.1 秒存储效率为 38%，1 秒存储后纠缠的 CHSH 值 S=2.36±0.14[81]；

QIC量子科技产学研创新联盟 QIAC中国信息协会量子信息分会

2021 年，荷兰代尔夫特大学实现了一种硅光芯片量子存储并实验演示了全功能量子中继，该量子存储器通过调控硅光晶体的自旋声子态和通信波段光子自旋态的光动力学耦合实现对光子的存储读写，存储时间大于 1 微秒，存储的效率和存储时间相对于金刚石色心有明显提升[82]。

2021 年，中国科学技术大学实现多模式复用的量子中继基本链路，并实现两个固态存储器的量子纠缠，为高速率、大尺度量子网络建设提供了新方案[83]。

2021 年，中国科学技术大学将长寿命冷原子量子存储技术与量子频率转换技术相结合，采用现场光纤在相距直线距离 12.5 公里的独立量子存储节点间建立纠缠[84]。

2023 年，中国科学技术大学利用冷原子系综实现了 25 维量子态的高效率存储，显示出对任意可编程量子态的兼容能力[85]。

（5）QRNG

量子随机数发生器的研发朝着无条件安全、芯片化方向发展。

2021 年中国科学技术大学团队实现了器件无关的量子随机数拓展实验[86]，在其前期实现“器件无关的量子随机数”生成实验基础上，通过提高探测效率和优化抽检方法，使随机数产生率高于纠缠检验所消耗的随机数。

2021 年 6 月，中国科大、浙江大学的研究人员研制成功基于芯片的高速随机数发生器，包含光源、调控光路、探测器的光芯片封

QIC量子科技奇智创新联盟
QIAC中国信息协会量子信息分会

装尺寸约 18×16mm^2，结合 FPGA 数据处理实现实时生成速率达 18.8Gbps[87]。

2023 年 7 月，清华大学实现基于雪崩光电二极管电子隧穿效应的无后处理量子随机数发生器，达到每秒 100 Mbps 的速率和 0.9872 bits/bit 的最小熵[88]。

4.3 主要产品

以 QKD 技术为核心的量子密码产品已经初步形成了从终端设备、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，用于星地通信的小型化量子卫星地面站产品也已投入使用；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。

QIC量子科技产学研创新联盟
QIAC中国信息协会量子信息分会

（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设备，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，例如光量子交换机、量子波分复用终端等；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，例如量子密钥管理机、密码交换机等；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，例如 QKD 集控站。还有一些具有拓展网络控制功能的量子加密设备，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。

（3）应用设备和软件

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，为了将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

QIC量子科技创新研究院 QIAC中国信息协会量子信息分会

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。QKD 用户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。这些拓展应用已经显著地体现了 QKD 密钥即时生成带来的管理便捷性和安全性。总体来看上层应用的研究属于刚刚起步，还有很大的发展空间。

4.4 技术专利

根据 2024 年 8 月 20 日对国际专利数据库的统计结果（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），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（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）如图 12 所示。其中，以科大国盾量子技术股份有限公司为代表的 9 家中国机构的专利数量约占前 10 位申请人的专利总量的 93%，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。

QIC量子科技产学研创新联盟
QIAC中国信息协会量子信息分会

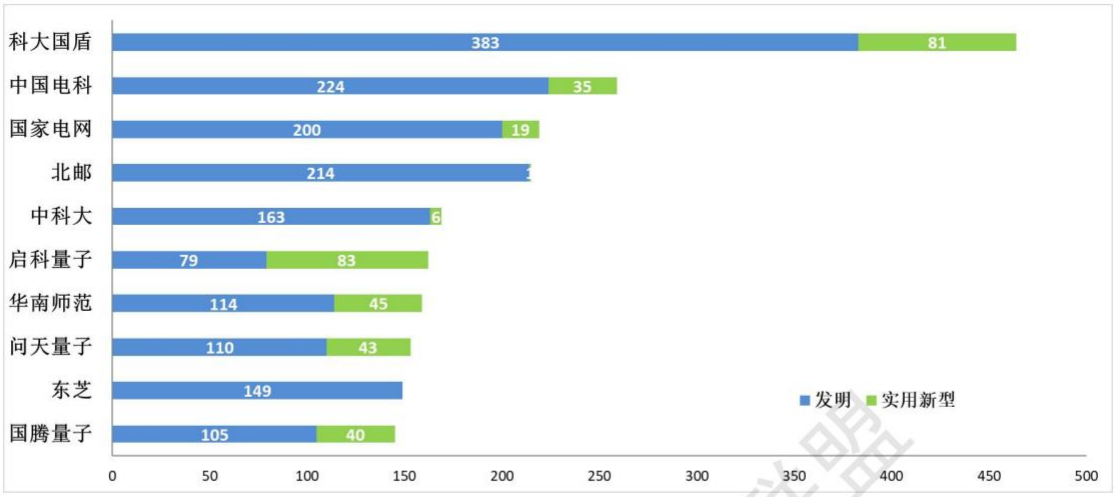


图 12 全球量子通信领域专利申请人排名（2024 年 8 月统计）

5. 量子密码产业生态现状

5.1 国际 QKD 产业发展

近年来，QKD 系统硬件设备已经可以从全球许多量子基础器件和核心设备厂商处购买到。国际产业界代表有瑞士 IDQuantique 公司（已被韩国 SKT 收购），德国 InfiniQuant 公司，美国 MagiQ 公司、QuantumXchange 公司和 Qubitekk 公司，澳大利亚 Quintessence Lab 公司等。国际深度参与 QKD 系统和网络建设的电信运营商包括韩国 SKT、韩国 KT、韩国 LGU+、英国电信、德国电信、西班牙电信等。此外，许多大型 ICT 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。

欧洲和日、韩等一直重点发展 QKD 技术，并加速相关基础设施建设。2021 年，欧盟组织 27 国启动建设“欧洲量子通信基础设施（EuroQCI）”，将建成全欧范围内含可信节点的光纤量子通信网络，计划于 2027 年实现运行。项目采用政产学研用多方参与、跨学科跨

QIC量子科技光学研创新联盟
QIAC中国信息协会量子信息分会

领域协同方式推进实施，聚集了一批来自量子信息、信息通信、信息安全等领域的企业和专家力量，并积极推动量子通信与 SDN、秘密共享等 ICT、信息安全等技术的融合发展。与此同时，欧盟计划于 2024 年开始发射低轨量子通信卫星，并逐步构建量子卫星星座。

日本以国家情报通信技术研究机构（National Institute of Information and Communications Technology，NICT）为主力，在高速 QKD 技术及应用研发方面非常活跃。韩国最大电信运营商之一 SKT 于 2018 年控股瑞士著名 QKD 企业 IDQ 之后，大力发展量子通信网络技术，开展量子通信与 5G 核心网络融合试点，开发了量子随机数芯片及量子安全网关、量子加密手机、量子 VPN 等终端产品，并为水力与核能电力公司、政府组织等能源、政务、金融等领域用户提供量子安全服务。韩国政府于 2020 年招标建设总长 2000 公里、覆盖全国 48 个政府部门的量子密钥分发网络。

协同创新是国际 QKD 产业链和生态发展的典型特征。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，该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。

QIC量子科技先导创新联盟
QIAC中国信息协会量子信息分会

5.2 国内 QKD 产业发展

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 13 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。

QIC量子科技产学研创新联盟 QIAC中国信息协会量子信息分会



图 13 量子保密通信产业链

QKD 系统硬件国内的代表性企业有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、上海循态量子科技有限公司等。

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芯片技术研究院、武汉光讯科技股份有限公司量产的雪崩管，赋同量子生产的超导纳米线单光子探测器（SNSPD），性能已能够媲美国外产品；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。国内电信运营商如中国电信、中国联通、中国移动等深度参与到 QKD 系统和网络建设，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。

6. 量子密码标准化发展现状

6.1 国际量子密码技术标准化成果

（1）国际电信联盟（ITU）标准

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，其下 SG11（协议和测试规范组）、SG13（未来网络组）和 SG17（安全组）研究组主要聚焦在 QKD 网络的协议、功能和安全性方面，已开展 40 余个相关标准制定项目。研究组已经定义了基于分层模型的典型 QKD 网络体系架构，并在此基础上，发布了 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。

2019 年，ITU-T 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。

QIC量子科技未来研创新联盟
QIAC中国信息协会量子信息分会

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。

目前，ITU-T 发布或通过的 QKD 网络相关国际标准或研究报告已有 20 余项，主要力量来自中日韩美欧，包括中国信通院、国科量子、科大国盾、北京邮电大学、韩国 SK Telecom/KT/ETRI/KAIST、瑞士 IDQ、日本 NICT/Toshiba/NEC、美国 Qubitekk 等。中国团队主导和参与 QKD 网络功能架构、QKD 节点防护安全要求、QKD 网络接口协议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。

2023 年 12 月，ITU-T 发布 5 项 QKD 网络协议相关标准，包括 QKD 网络的协议框架（Q.4160）、Ak 接口协议（密钥输出接口，编号 Q.4161）、Kq-1 接口协议（密钥请求输出接口，编号 Q.4162）、Kx 接口协议（密钥中继接口，编号 Q.4163）、Ck 接口协议（路由控制接口，编号 Q.4164），为实现 QKD 网络的互联互通提供了详细的消息格式参考。

QIC量子科技产业创新联盟
QIAC中国信息协会量子信息分会

（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，2019 年 2 月，该项目研究阶段工作获得 20 多国投票通过，正式进入标准起草阶段，开始编制国际标准 ISO/IEC 23837-1《量子密钥分发的安全要求、测试和评估方法 第 1 部分：安全要求》、ISO/IEC 23837-2《量子密钥分发的安全要求、测试和评估方法 第 2 部分：测试和评估方法》。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。项目的主要任务是阐明和规定 QKD 系统的安全要求和测试评估方法技术规范，为 QKD 系统的安全测评工作提供依据和指导，也是面向 QKD 安全领域推出的首个系统性地规范 QKD 安全检测要求的国际标准。该标准第 1 部分已于 2023 年 8 月发布，第二部分于 9 月发布。

（3）欧洲电信标准化协会（ETSI）标准

ETSI 于 2008 年发起了针对 QKD 技术的行业规范小组（Industry Specification Group on QKD，ISG-QKD）。ETSI ISG-QKD 开展的工作主要涉及 QKD 光学组件、模块、内部接口、应用程序接口以及现实安全性等方面，目前已发布了有关 QKD 的 10 项标准和 2 项研究报告，仍有 4 项标准和 2 项研究报告工作正在推进。另

QIC量子科技产学研创新联盟 QIAC中国信息协会量子信息分会

外，已经发布的应用接口、安全性证明、SDN 控制接口、安全轮廓、术语方面的标准及研究报告正在进行新版本的修订工作。

近期，ETSI 的卫星地面站和系统（SES）技术委员会下的卫星通信和导航（SCN）工作组，启动了《卫星量子密钥分发（S-QKD）卫星系统及相关光学地面站的技术规范》的标准制定工作。

6.2 国内量子密码标准化工作

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），下设量子通信工作组（WG1）和量子信息处理工作组（WG2），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，围绕量子保密通信标准体系正在开展一系列标准化工作。目前参与 ST7 的涵盖量子通信企业、电信运营商及高校的几十家会员单位，通过产学研用协调配合，国际国内标准联动推动量子通信标准工作开展。

QIC量子科技产学研创新联盟
QIAC中国信息协会量子信息分会

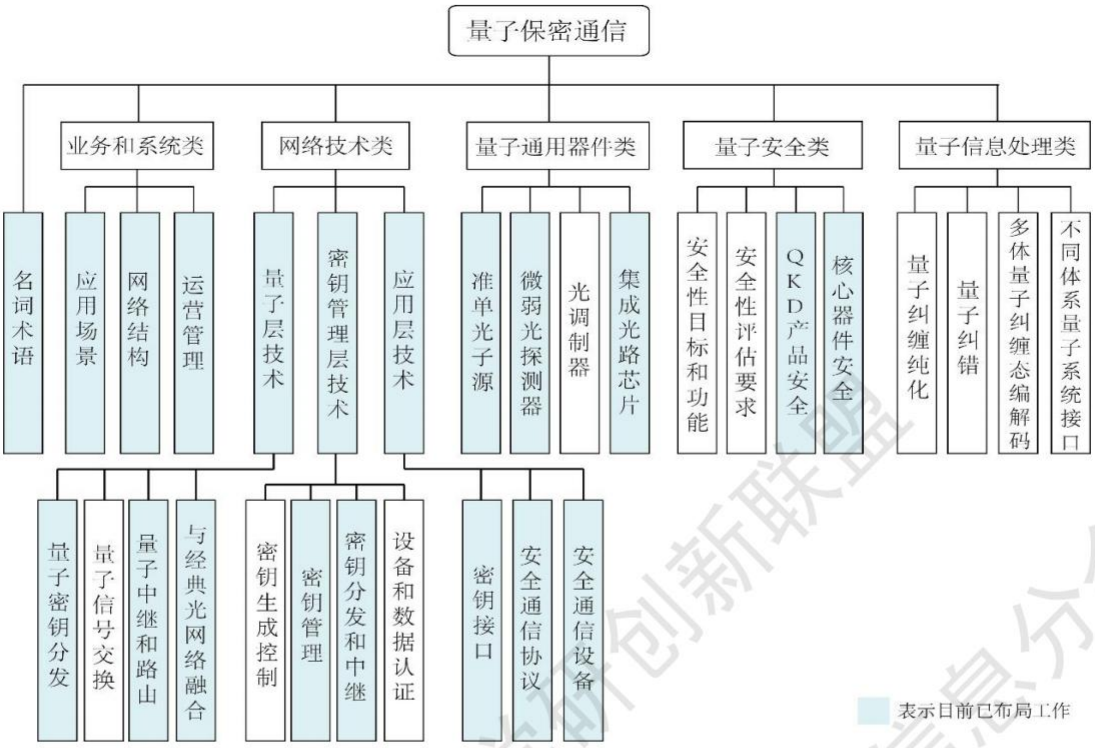


图 14 CCSA 关于量子保密通信标准建设路线图进展情况

图 14 为 CCSA 关于量子保密通信标准建设路线图，涵盖业务和系统、网络技术、量子通用器件、量子安全、量子信息处理等 6 类标准工作。目前 CCSA 已经在这些方向开展了 60 余个 QKD 相关标准研制项目，并发布了《量子保密通信技术白皮书》。2021 年，通信行业标准《量子密钥分发(QKD)系统技术要求 第 1 部分：基于诱骗态 BB84 协议的 QKD 系统》、《量子密钥分发(QKD)系统测试方法 第 1 部分：基于诱骗态 BB84 协议的 QKD 系统》和《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）》发布，填补了我国量子通信技术在通信行业标准上的空白。

2022 年，通信行业标准《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》和《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》由工信部发布。2023 年，《量子保密通信网络架构》、《量子密钥分发（QKD）网络 网络管理技术要求 第 1 部分：网络管理系统（NMS）功能》、《基于 IPSec 协议的量子保密通信应用设备技术规范》、《量子密钥分发与经典光通信共纤传输技术要求》、《量子密钥分发系统测试方法 第 2 部分：基于高斯调制相干态协议的 QKD 系统》五项量子保密通信相关的通信行业标准由工信部发布，规范了量子保密通信网络及其关键设备的设计、部署、管理等方面。2023 年 8 月，由中国通信标准化协会立项编研的国家标准《GB/T 42829-2023 量子保密通信应用基本要求》、《GB/T 43692-2024 量子通信术语和定义》由国家标准化管理委员会发布。目前，CCSA 归口/组织制定的量子通信相关国家标准、通信行业标准、团体标准及技术报告已达二十余项。并瞄准新研究领域如 QKD 与其它新密码/安全技术如 PQC 的融合应用、CV-QKD 等提前布局开展研究。

2016 年以来，密码行业标准化技术委员会（CSTC，以下简称“密标委”）组织开展了 10 余项量子密码相关标准研制工作，内容涵盖 QKD 技术规范、系统测评、应用接口、中继安全性等。2021 年，国家密码管理局公告发布了《诱骗态 BB84 量子密钥分配产品技术规范》、《诱骗态 BB84 量子密钥分配产品检测规范》两项密码行业标准，标志着 QKD 技术首次进入国家密码行业标准。

另外，作为 QKD 技术的重点应用领域，电力行业针对 QKD 在电力行业的应用规范开展了 3 个行业标准制定项目，并已发布。近年

QIC量子科技先导研创新联盟 QIAC中国信息协会量子信息分会

来，金融行业各单位如人民银行和组织如北京金融科技产业联盟也开展了多项 QKD 应用和管理方面团体标准的编研工作。

6.3 QKD 系统和网络测评方面标准化工作

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。潜在用户计划部署 QKD 网络或租用 QKD 服务时，需要知道该网络能否满足其可用性和安全性需求。测试和评估标准将为用户提供功能、性能和安全性方面的最终依据。测试和评估方面内容的标准化也是产业成熟的重要标志。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 工作组制定的 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的测评方法。ITU-T SG17 组研制的 QKD 密钥管理、QKD 节点防护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。

QIC量子科技产学研创新联盟
QIAC中国信息协会量子信息分会

三、量子安全综合应用技术

量子安全是新一代密码技术应具备的主要特性之一，基于数学和物理的两条实现路线（分别以 PQC 和 QKD 为代表）各具特性且有着不同适用场景，面向量子安全需求，两者在很大程度上是分工和互补的。本章第一部分介绍量子安全的 PQC 与量子密码的融合方案设计，第二和第三部分阐述基于此方案的用户端密码应用设计和管理端的密钥管理基础设施设计。

（一）量子安全的 PQC 与量子密码的融合方案

近年来，融合“量子”与“经典”的量子安全实现理念受到了越来越多的认同。早在 2020 年，欧洲量子旗舰工作规划中就宣称，尽管 PQC 和 QKD 原理和成熟度不同，两者是有各自不足及能够互补的优势的，近期和未来两者在量子安全领域是共存共用的，并规划在 2023-2026 年要部署融合 PQC 和 QKD 的安全解决方案[86]。韩国电信运营商 SKT 已经在开展 PQC+QKD 融合应用的系统布局，这些体现了欧洲和日韩在 QKD 技术上具备长期积累条件下，都坚持选择“PQC+QKD”路线。

1. 现有工作分析

目前公开发表的一些“融合”方案可分为两种，一是应用 PQC 为 QKD 网络的运行进行身份认证[90][91]，二是应用 PQC 的密钥封装算法与 QKD 的密钥进行混合使用[92]。

QIC量子科技产学研创新联盟
QIAC中国信息协会量子信息分会

第一种方式是指在一些面向应用的 QKD 系统中，密钥生成的安全水平与认证方法的安全水平是一致的[93]，通常使用预置共享密钥进行第一轮 QKD，然后使用 QKD 生成的部分密钥进行后续的认证，从而保障了 QKD 的信息论安全水平；而使用 PQC 进行身份认证，密钥生成的安全水平将降低到 PQC 的水平。

第二种方式是指在用户端到端生成密钥过程中，将 PQC 封装的密钥与 QKD 密钥进行混合使用，其目的在于通过“冗余”确保密钥的实际安全性不低于使用的 PQC 算法和 QKD 实际系统中安全性最高的一方，但系统的复杂性和用户使用成本均有所增加。

2. 方案设计目标和途径

方案设计目标是从密码算法应用和密钥管理两方面入手，在充分考虑数学手段和物理手段特征的前提下，通过技术“融合”实现密码所应提供的机密性、完整性、真实性和不可否认性安全服务，从而实现完善的量子安全体系。

如第一章所述，数学手段适用于实现密码应用服务，当前在数学手段方面，量子安全的公钥密码 PQC，其安全性目前尚不稳定；量子安全的对称密码主要是分组密码、序列密码、杂凑函数以及基于杂凑函数的签名算法等，其安全性已经过长时间检验，确定性高。目前可以提供的“核心稳定、服务全面”的以融合模式实现量子安全的密码应用服务解决方案如表 12 所示。

QIC量子科技产学研创新联盟 QIAC中国信息协会量子信息分会

表 12 融合模式实现量子安全的密码应用服务方案特性

用户安全性保障	对应的密码算法配用
机密性	对称密码算法/OTP
真实性	对称密码算法/PQC（如基于哈希的签名算法）
不可否认性	PQC（如基于哈希的签名算法）
完整性	杂凑算法

物理手段更适用于密钥管理服务，在物理手段方面，有量子技术也有经典技术。量子技术主要为 QKD，其安全性研究较为深入，目前确定性较高。其他的经典物理技术手段如“无线信道密码技术”可用于传递密钥，但其安全性、实用性等还需进一步研究；通过预置/人工递送密钥等方式也是常见的物理手段。目前可以提供的“核心稳定、服务全面”的量子安全系统解决方案如表 13 所示。

表 13 融合模式实现量子安全的密钥管理方案特性

核心基础设施适用的密钥分发模式	到用户侧适用的密钥分发模式
光纤/自由空间 QKD	[1]. 光纤/自由空间 QKD [2]. 预置密钥/人工递送 [3]. 基于无线信道物理特征的密钥传输技术 [4]. 基于 PQC 的密钥封装算法

3. 系统适用的密码密钥配置

系统配置的各类密码算法和这些算法配合的密钥生成、分发等各管理环节均具备量子安全性才能保障用户信息系统整体具备量子安全性，即只有在满足量子安全性的密钥管理服务支持下，密码应用整体才能满足量子安全性要求，否则很容易由于信息安全的“木桶原理”导致量子安全性在单点被突破。系统配置量子安全的算法

和密钥用以满足各类基础密码服务需求的方案可分别按以下四个方面阐述。

3.1 机密性密码服务

主要使用量子安全的对称密码算法实现对用户敏感数据的安全传输和安全存储，防止用户敏感数据泄露，此方案具有适用于传输加密和存储加密的多种场景、安全性强、加密速度快、密文与明文大小相比基本不变等优点。

机密性密码服务使用的密钥：机密性服务使用的对称密钥由量子安全的密钥管理基础设施提供，包括基于 QKD 技术的密钥核心网和多种技术的用户密钥接入网。

3.2 完整性密码服务

使用杂凑类密码算法验证用户数据完整性，保障数据或用户应用环境一致性与未受篡改。

完整性密码服务使用的密钥：使用杂凑类密码算法一般可不使用密钥；如使用带密钥的杂凑函数，则类似机密性服务，使用量子安全密钥管理基础设施提供的对称密钥。

3.3 真实性密码服务

使用量子安全的对称密码算法或带密钥的杂凑函数能够实现用户或数据的真实性验证。也可以使用PQC类非对称密码算法实现真实

QIC量子科技产学研创新联盟
QIAC中国信息协会量子信息分会

性密码服务，如基于基于哈希的签名算法生成用户公钥和对应的身份证书，可满足用户间双向安全认证、数据认证的安全需求。

真实性密码服务使用的密钥：在使用对称密码算法时，类似机密性服务，使用量子安全密钥管理基础设施提供的对称密钥；在使用PQC时，PQC公私钥对中的私钥可由QKD网络或其它物理方式生成/分发，对应公钥由私钥通过特定算法基于私钥生成。

3.4 不可否认性密码服务

一般认为不可否认性安全服务包括原发抗抵赖、交付抗抵赖、提交抗抵赖、传输抗抵赖等方面[94]，其认证使用的算法、密钥乃至认证过程与真实性认证都是相关的。使用PQC类非对称密码算法能够实现不可否认性的密码服务，能够防止信息发送方或生成者否认自己所传输的消息，实现信息的可追溯可审查。

不可否认性密码服务使用的密钥：使用PQC类非对称密码算法时，类似真实性服务，PQC公私钥对中的私钥可由QKD网络或其它物理方式生成/分发，对应公钥由私钥通过特定算法基于私钥生成。

QIC量子科技产学研创新联盟
QIAC中国信息协会量子信息分会

（二）用户端量子安全技术应用模式

1. 身份认证的量子安全实现示例

1.1 基于对称密码实现真实性和不可否认性服务

采用对称加密算法或 HMAC 算法，配合使用量子安全的对称密钥，如 QKD 系统提供的端端密钥，并增加密钥使用长度和哈希输出值长度，可实现端端的身份认证、消息认证等量子安全的真实性服务。

自上世纪八九十年代出现对实体和信息的真实性认证需求以来，基于对称密码实现真实性和不可否认性服务的密码方案就产生了。例如用户登录主机这类简单场景中采用的基于密钥 MAC 值比对的认证方式，以及广泛用于服务器-客户端等各应用场景的身份认证协议 Kerberos 支持的基于对称密码的认证方式等。这类方案的优势是安全性较强，基于对称密码的特性能够实现量子安全性；结合 QKD 等能够快速安全更新密钥的技术手段，前向安全性也有保障。

该类方案劣势是协议交互步骤较多、密钥分发量随用户数量增大而迅速增加，可能需要在线的可信第三方支持（具体方案可参见[95]等）。尤其是在实现不可否认性服务上，不可否认性服务要求验证消息的来源，并且信息的处理者不能否认其行为或者处理结果，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。而对称密码方案中双方使用相同的密钥来加密和解密消息，这意味着任何一方都可以声称是消息的发送者或接收者，若要基于对称密码实

现严格的不可否认性服务，则相应协议需要增加很多安全的交互步骤和时间戳等安全附加数据（如[95]）。

基于对称密码实现真实性和不可否认性服务的密码方案更适用于行业用户、专网用户等用户规模和角色均较固定且安全性要求较高的应用场景。而公钥密码相比较而言能更适用于变化多、规模大的用户场景如互联网环境下的实现真实性及不可否认性安全服务。

1.2 使用 PQC 算法实现真实性和不可否认性服务

依上节所述，采用 PQC 类公钥密码实现身份认证/不可否认性量子安全的密码服务适用于互联网等用户规模广、变动较频繁的应用场景。公钥密码由于有明确的公钥和私钥之分，并且每个参与者只有自己的私钥，从而可以更灵活地实现不可否认性安全服务。

使用格密码或基于杂凑的 PQC 如 MSS 等算法构造的量子安全密码，在应用流程上与当前广泛使用的基于 RSA 等算法的数字证书身份认证类似；不同之处在于调用的签名/验证算法和公钥长度等相关参数。使用 MSS 算法实现真实性和不可否认性服务的应用流程如图 15 所示。在准备阶段，各用户到身份认证中心申请各自的 MSS 身份证书，基于 MSS 机制的身份认证中心为各用户颁发证书。在使用阶段，用户 A 利用自己的 MSS 私钥做签名发给用户 B，用户 B 利用用户 A 的 MSS 身份证书进行验证，用户 B 利用自己的 MSS 私钥做签名发给用户 A，用户 A 利用用户 B 的 MSS 身份证书进行验证，完成双向的身份认证过程。

QIC量子科技产学研创新联盟 QIAC中国信息协会量子信息分会

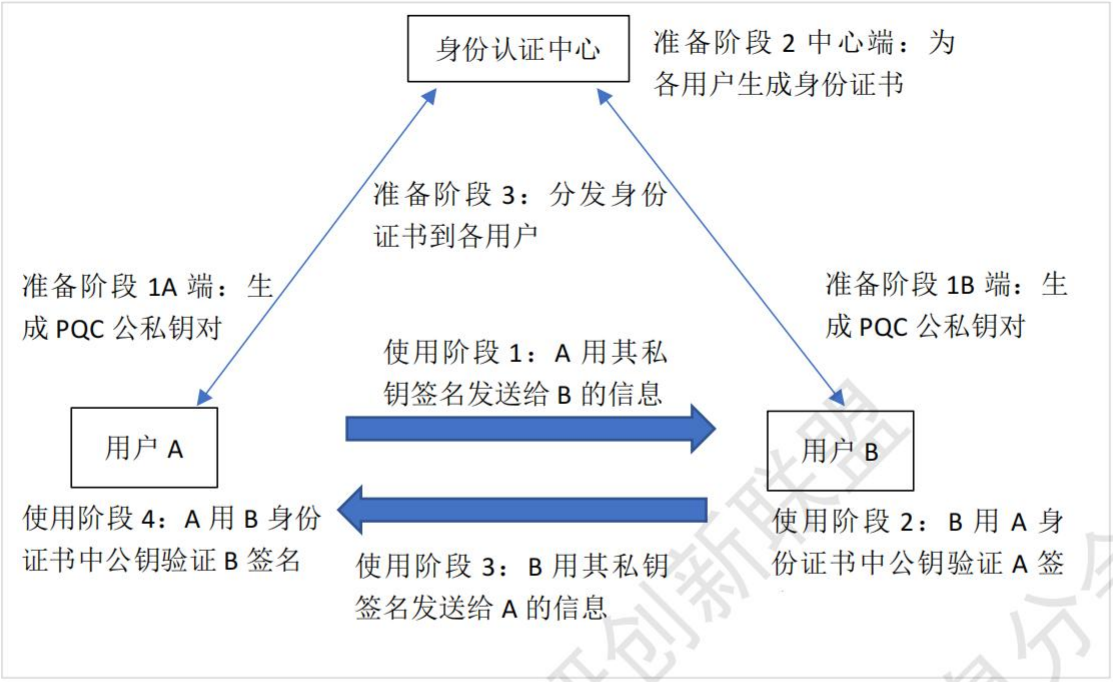


图 15 能满足用户间双向安全认证需求的量子安全密码应用服务示例流程

1.3 常用身份认证密码协议的改造示例

对于现用基于数字证书的身份认证协议（如 Kerberos 协议中基于数字证书认证的模式）来说，从证书结构上，X.509v3 格式是能兼容 PQC 的，不需要更改标准，数字证书格式中规定的对象标识 OID 域较灵活，支持自定义 PQC 类的新算法标识，而且其数据格式定义能够支持存储很长的公钥，所以对公钥长度较长的 PQC 算法也能兼容。基于数字证书的应用迁移到 PQC 算法既需要 CA 的调整，也需要各类基于证书的应用系统的改进，修改证书应用系统以防止在源代码中对证书长度限制过短，并让应用能根据新的算法标识验证签名。基于数字证书的认证协议需将签名/验证算法替换为新算法标识的 PQC 类签名/验证算法。

QIC量子科技大学研创新联盟 QIAC中国信息协会量子信息分会

再以用户端部署的相对结构较复杂的安全套接层协议举例，SSHv2 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，主要实现真实性认证和机密性服务。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，产生会话的唯一性标识 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、杂凑算法等参数。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。由于传输层子协议决定了之后所有流程使用的算法，所以执行传输层子协议时服务端和客户端双方都应使用量子安全算法。当前该协议认证过程使用的 RSA、DSA 或 ECDSA 公钥认证算法并不是量子安全的，需要替换为 PQC 类签名算法。

基于对称密码实现真实性和不可否认性服务的方案常见于早期如[95][96]等，典型的身份认证协议 Kerberos 最初就设计为使用对称密码实现开放网络中两个节点间进行安全通信的集中认证服务。Kerberos 认证服务器和客户端均使用对称密钥加密来生成安全票据（称为 Token）来确保认证过程中交互数据的安全性。所有的票据和消息都会被相应的密钥加密，只有拥有相应密钥的实体才能解密它们。这就保证了只有经过认证的实体才能获得和使用 Kerberos 票据。未来为实现实体认证的泛在量子安全性，可以选择使用对称密码模式。

QIC量子科技产学研创新联盟
QIAC中国信息协会量子信息分会

另一类具有代表性的身份认证场景可归纳为轻量级身份认证，广泛应用于物联网、工业控制系统等。其要求身份认证所需的的计算资源尽量少、传输和存储数据量要小、终端数量灵活可变等。目前一般使用轻量级数字证书或对称密码实现。现有物联网设备身份认证和数据安全存在量子安全性缺陷，会影响到工业控制网络和通信网络的安全，可使用量子安全的对称密码，需提高其认证模式的灵活性；若使用 PQC 类算法，则需要通过选用公钥长度小、认证速度快的签名验证算法从而严格限制轻量级数字证书的长度。

2. 传输加密类应用协议实现量子安全示例

常用传输加密协议如HTTPS、IPSEC VPN、SSL VPN等以实现数据的安全加密传输功能为主，在互联网中有广泛应用。这些密码协议常具备加密、认证等多功能（一般均设计为先认证成功后再加密传输数据的模式）。而量子安全的实现方案提现了可认证性与机密性是不同的。量子安全的认证功能上节已讨论，本节讨论量子安全的相关加密算法在传输加密类应用及密码协议中的配置、改造应用。

以 VPN 协议中的 IKE 子协议为例，IKE 协议常用于建立 VPN 通道时认证安全对端（SA）和协商密钥，实现认证服务和机密性服务，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。其修改方案是在该协议临时密钥生成的三次握手交

互中第一步和第三步交互不使用 DH 算法生成临时密钥，使用量子安全的密钥管理基础设施提供的端端对称密钥作为新的密钥协商生成方式。

传输层安全协议（TLS）协议的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，即主要实现认证服务和机密性服务。握手子协议使用基于 RSA 或基于 ECC 的密钥交换算法和 X.509 证书，这个过程不是量子安全的。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主要就是安全的生成和分发工作密钥：原不具有量子安全性的方案是客户端生成随机密钥，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。修改方案可分为两类：一是采用 PQC 类密钥封装算法替换现用公钥加密算法；二是由客户端和服务器双方采用量子安全的密钥管理基础设施提供的端端密钥作为工作密钥。由于 QKD 密钥更新频率高、前向安全性强，总体安全性上可能强于使用 PQC 类密钥封装算法的方案。在此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。

QIC量子科技先锋创新联盟
QIAC中国信息协会量子信息分会

再以安全套接层（SSH）协议为例，SSH 协议中原有不是量子安全的密钥协商机制可以由量子安全的密钥管理基础设施提供对称密钥来替换。当前 QKD 的密钥生成率很大程度上取决于距离和网络结构。由于当前的 SSH 安全参数建议每分钟或在传输每 1GB 数据后应更改密钥，因此当前商用的 QKD 设备完全可以满足相关需求。

3. 对密码服务应用接口的算法敏捷性要求

密码服务应用接口的算法敏捷性要求是密码应用软件设计和工程开发上的一项重要要求，要求密码服务应用接口具备标准化和可扩展性，能够适配广泛的、可能未来规划中增配的不同算法。在基于量子安全需求替换某种公钥密码算法时，应从应用需求、功能适用性、接口适配性、合规性等出发综合考虑从PQC算法库中查找并确定适用的量子安全替代算法，然后采用该适用算法进行替代。其中，由于PQC具备传统公钥密码对应的所有功能（主要包括公钥加密/签名），功能适用性相对容易确定，性能需求也容易依据具体应用场景明确，而接口适配是这些因素中值得讨论并体现了密码应用特点的需求，具体在此体现为接口适配上对可能应用的不同算法的敏捷性要求。

算法敏捷性概念的由来是密码学家和从业者认识到，算法安全性长期来看都可能会随时间推移而减弱甚至丧失（包括PQC），因此密码算法存在敏捷替换、持续升级的需求，若算法调用接口与特定算法硬绑定，则无法实现算法的按需快速替换。也就是说，算法敏

QIC量子科技产学研创新联盟 QIAC中国信息协会量子信息分会

捷性要求密码算法调用接口能够适应在未来灵活将现用算法替换为其它算法。若不具备算法敏捷性，则意味着不同密码算法的接口及参数均存在差异，当需要升级密码算法时，大量用户需要尽可能同时更换密码算法库、应用接口乃至具体调用参数，导致迁移过程复杂、工作量大、耗时长。

对量子安全迁移来说，具备较好的算法敏捷性则能够实现密码算法升级切换时，由密码管理员或密码协议的通信发起方通过调整算法参数，其他用户无需修改代码，即可快速从现用算法切换到量子安全的密码算法，或从某种量子安全的密码算法切换到另一种。因此，若用户端的密码应用软件或密码应用协议具备算法敏捷性，则可以方便的实现量子安全迁移。例如，SSH协议就是具备算法敏捷性的协议，它能够通过加入PQC软件库支持量子安全算法，不需要在代码层面做较多的修改。

应用系统要增加算法敏捷性这一特性，在编程实现层面大体分为两种实现思路：一是通信双方先协商本次通信使用的密码算法及密钥，选出双方都支持且优先级最高的算法，然后发送方基于协商结果对传输数据进行密码运算，接收方再基于相同算法及密钥进行处理。算法切换时，由发送方或接收方将新算法优先级调整为最高，另一方无需修改代码，协商时将自动选用新算法，从而实现密码算法切换；二是通信双方无需协商，而是由发送方在已加密处理的传输数据中增加使用的密码算法和密钥标识，接收方根据标识对数据进行相应处理。算法切换时，由发送方调整密码算法及密钥标识，

QIC量子科技先锋创新联盟
QIAC中国信息协会量子信息分会

接收方自动按新标识调用新算法进行处理，无需修改代码。

（三）量子安全的密钥管理基础设施

1. 密钥管理功能实现模式

面向密钥管理需求，需要建设量子安全的密钥管理基础设施：其中，核心基础设施可采用基于光纤和自由空间的QKD技术建设的密钥分发网络，并叠加相关技术以支撑各种密钥服务功能。在用户侧的密钥分发环节，可根据密级要求和使用场景，建设采用QKD、预置密钥、基于无线信道的密钥交换等技术的密钥接入网或使用PQC密钥封装算法分发密钥。提供的密钥管理功能包括：集中以及端端等模式的对称密钥生成、分发服务，PKI所需要的公私钥对生成、分发等服务。QKD作为密钥管理系统的功能“安全底座”，为密钥管理核心网络提供的量子密钥，可分别用于工作密钥、密钥加密密钥或PQC算法的公私钥对等不同用途。公私钥对及数字证书的分发可使用QKD生成的对称密钥进行保护。基于QKD较高的实时密钥更新频率，可使得密码系统获得很强的前向安全性，以及不同用途密钥之间很强的独立性。

2. 量子安全密钥管理基础设施的组成

量子安全密钥管理基础设施通过量子密钥管理、分发和保护手段，为各类应用系统提供量子安全的密码服务，由 QKD 网络、量子安全密钥管理系统、量子安全服务平台等组成。QKD 网络负责广域

量子密钥分发，按照分层分域理念，划分为骨干网、城域网和接入网，实现 QKD 网络深度覆盖；量子安全密钥管理系统负责实现量子安全密钥端到端配对和调度，对密钥的生成、注册、认证、注销、分发、安装、存储、归档、撤销、派生以及销毁的全生命周期进行管理。量子安全服务平台负责提供量子安全密钥应用接口和身份认证、数字签名、加解密等量子安全密码服务。

在密钥分发层面，通过 QKD 网络提供广域端到端量子安全密钥，充分发挥量子密钥长效安全性的优势，为密码系统和应用提供量子安全性保障。

在“最后一公里”安全接入方面，通过在遵循量子安全原则要求的基础上，采用 QKD、预置/人工递送密钥、基于无线信道物理特征的密钥传输、基于 PQC 密钥封装算法等密钥分发技术，根据应用场景和安全级别需要实现量子安全密钥的端端服务。



图 16 量子安全基础设施和应用示意图

图 16 是量子安全基础设施及应用于通信网络和其应用的示意图。通过部署 QKD 骨干、城域和接入网络，实现量子安全基础设施与固定、移动通信网络的全覆盖；通过量子安全密钥管理系统，实现端

到端的量子安全密钥分发。通过量子安全服务平台，为云、网、管、端等层面的各类终端、设备、网络及应用等提供量子安全的密钥分发服务。既能应用于通信网络基础设施的安全，如量子安全的对称加密算法+量子安全密钥保护云计算（数据中心）的数据传输安全，与数据加密算法结合保护数据存储安全；又能通过融合 PQC 算法+量子安全密钥，为物联网、云计算、分布式系统等各类 ICT 系统安全和应用安全提供量子安全认证服务等。

目前我国已经初步建成国际领先的量子安全密钥基础设施的雏形。2022 年我国新一代信息基础设施“国家广域量子保密通信骨干网络”（图 17）全线贯通并通过验收，地面干线总里程超过 10000 公里，覆盖京津冀、长江经济带、粤港澳等国家重要战略区域，并与“墨子号”、量子微纳卫星互联，具备全球密钥投送能力。同时，我国在合肥、武汉、上海、北京、南京、成都、重庆等 10 多个城市建成量子城域网络并提供服务。

QIC量子科技先导创新联盟
QIAC中国信息协会量子信息分会

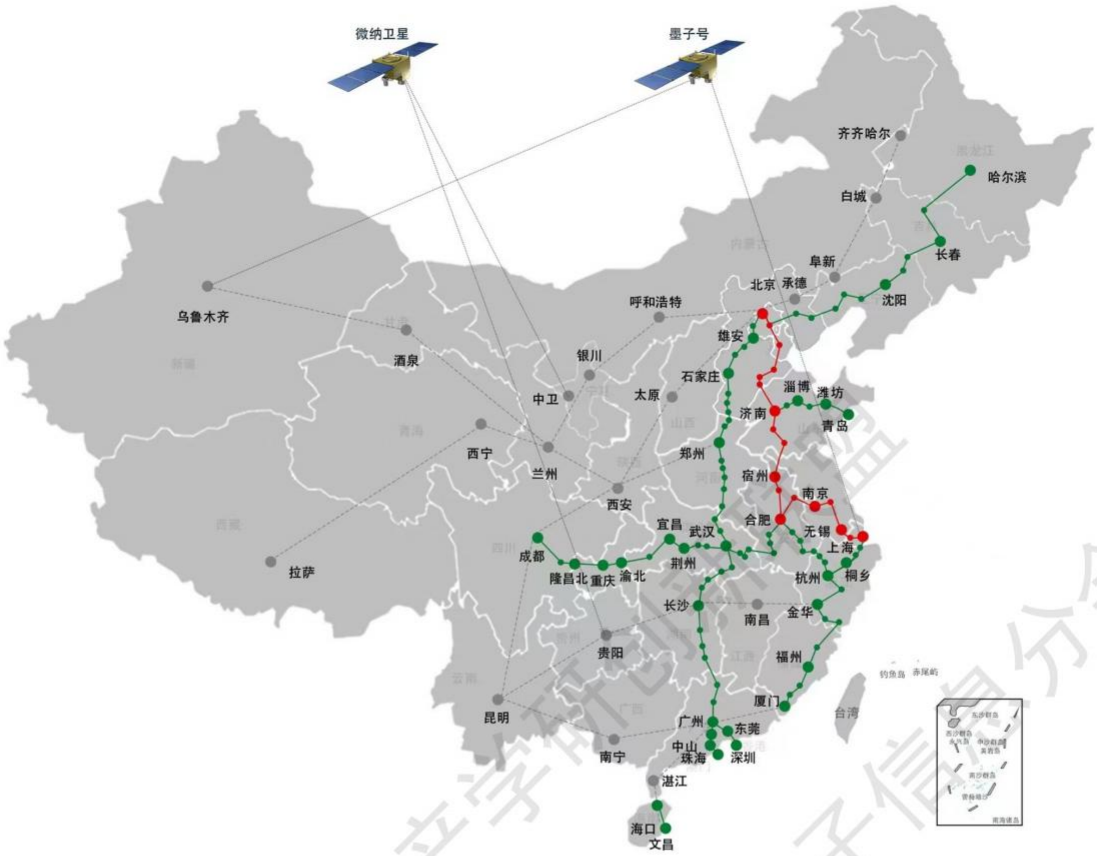


图 17 国家广域量子骨干网络示意图

QIC量子科技产学研创新联盟
QIAC中国信息协会量子信息分会

四、面向量子安全的迁移

（一）现有密码系统向量子安全的迁移规划和评估

将现有密码系统向能够抵御量子计算攻击的抗量子计算密码系统迁移是一项重要且紧迫的任务。除了采用量子安全的对称密码和PQC类公钥算法替换当前不符合量子安全要求的对应算法以外，还面临许多技术、标准化乃至政策上的复杂问题。涉及密码算法、协议、硬件设备和网络基础设施等多个方面，需要密切关注量子计算技术的发展，并与密码学研究人员、行业和标准化组织、系统设计团队、工程实现团队等密切合作，迁移过程需要谨慎规划和逐步实施，以确保安全性和平滑过渡。

1. 量子安全的密码系统迁移相关研究工作

2022年，随着量子计算发展加速和NIST发布PQC标准化阶段性成果等因素影响，国外量子安全相关政策和规划展望报告频繁发布。北约网络安全中心发声也提到了需要越来越重视应对“现在存储，以后解密”（Store-Now-Decrypt-Later，SNDL）的量子安全威胁，认为这是包括北约在内的所有组织都面临的威胁。美国总统拜登2022年12月签署了《量子计算网络安全防范法案》，以法律形式推进美国应对量子攻击的各种准备。2022年内，NIST、NSA、MIT等国外信息安全管理部门和研究机构都公开发布了预警量子攻击威

胁及向量子安全迁移路线图等相关主题的技术报告，主要情况汇总如表 14 所示。

表 14 2022 年来向量子安全迁移主题的技术报告汇总

发布机构	文档名称	重点关注内容和输出观点
NIST（美国国家标准与技术研究院）	为抗量子计算密码做好准备：采用抗量子算法的挑战	内容简洁、侧重举例，提到 IETF、ISO/IEC、ANSI/INCITS、TCG 等组织需制定迁移计划
MIT（麻省理工）	从今天起，直面明天的量子黑客	面向科普、面向行业和企业用户观点，混合应对及转换方法
Nature 杂志	成为向 PQC 迁移的组织	密码敏捷性，区分优先级策略，混合算法
世界经济论坛/德勤	量子准备工具包：构建量子安全的经济	倡议企业和组织着手构建基于新技术的量子安全体系，采用全球、跨产业的方法来处理网络安全和治理量子风险
NIST（美国国家标准与技术研究院）	向 PQC 迁移：考虑实施和应用量子安全的密码	可落地的实施向导，涉及到代码依存性、网络传输协议（QUIC, TLS, SSH, X.509 证书等的改造）及用户应用侧代码
ENISA（欧盟网络安全局）	抗量子计算密码——整合	双重加密/双重签名方法
European Quantum Flagship（欧洲量子旗舰）	量子旗舰战略研究和产业议程	双重加密/双重签名方法
美国咨询公司兰德/国土安全部	为抗量子时代关键基础设施做准备	强调详细评估的重要性
ITU-T	使用量子安全密码技术的身份验证和授权	使用量子安全密码实现 QKDN 中的认证和授权
美国量子经济发展联盟（QED-C）	机构量子安全指南	量子威胁时间线上的阐述，量子与数学的混合解决方案
全球移动通信联盟	抗量子电信网络影响评估白皮书	全球各国 PQC 发展现状，云、5G 网、端设备到 SIM 卡各应用场景的 PQC 适配

2023 年 8 月，美国网络安全和基础设施安全局（CISA）、国家安全局（NSA）和国家标准与技术研究院（NIST）联合发布了《量子准备：向抗量子加密技术的迁移》（Quantum-Readiness:

Migration to Post-Quantum Cryptography）的报告，概述了组织如何准备加密清单，与技术供应商合作，以及评估其供应链对系统和资产中易受量子攻击的加密技术的依赖。

2023 年底，NIST 又发布了两份特别出版物草案，分别为：《迁移到抗量子计算密码-量子准备：密码学发现》[97]以及《迁移到抗量子计算密码-量子准备：测试标准草案》[98]。提出，量子计算的进步可能使当前广泛用于保护数字信息的许多加密算法受到破坏，概述了迁移到新的抗量子计算密码标准时可能出现的具体问题，并提供了潜在的解决方案。

2. 量子安全的密码迁移规划一般过程

一是在量子安全密码迁移前需对现有的密码系统进行脆弱性评估和分析，确定其在量子计算机攻击下的脆弱性，并设计出能够抵御量子攻击的替代方案。其中需关注的重点问题包括：迁移计划的制定、给出迁移的状态定义、评估现有密码系统算法敏捷性和给出迁移后的验证标准等。

在分析评估阶段，需要将密码系统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。总体上，目前重点行业对应对量子安全的规划还略显薄弱、行动不足，对实施量子安全的合理实施路径也还不够清晰。

二是在量子安全密码实际迁移前对抗量子计算密码算法和量子密码系统进行安全性评估，对算法、协议及系统实现进行标准化，

QIC量子科技产学研创新联盟 QIAC中国信息协会量子信息分会

将这些算法和协议准备到软件包发布状态，相关的设备和系统达到货架状态。

在迁移准备阶段，总体上看当前存在的问题是标准化进展落后于需求，一方面有对量子安全实施紧迫性认识不足的因素，也有PQC 算法的实际成熟度与标准化要求还有一定的距离等因素。

三是在具体应用场景下，将抗量子计算密码算法和协议与现有的密码产品或基础设施进行集成。传统公钥密码算法与抗量子计算密码算法相比较，在算法参数尺寸、运算效率、算法机制等方面存在较大差异；PQC 算法中目前没有一种算法能像传统公钥算法如 RSA、ECC 算法这样包含了全功能的密钥协商、签名、加密各子算法，因此，在不同的应用场景下，需要选用不同的抗量子公钥密码算法，而算法的选择和互通性会给迁移带来不小的挑战。

四是密钥管理基础设施的迁移，对比密钥管理基础设施和密码应用用户端两侧，从实现密钥管理安全性、隔离性考虑，优先考虑密钥管理基础设施向量子安全的迁移。总体上，迁移应遵循的原则为：管理对象上，从目前传统公钥密码管理为主、对称密码管理为辅、各自独立 转向以实现量子安全的综合密钥管理为目标，对称密码为主配合 PQC 类公钥密码。保护方式上，从以数学算法实现安全为主转向以物理手段实现安全为主。管理网络上，从传统光/电介质的无线/有线网络转向使用 QKD 作为基础设施主干核心网+多种有线/无线传输技术结合以解决终端便捷接入密管网络的架构。重点是在现有 QKD 网络基础上进一步扩展其覆盖范围和密钥管理功能。

QIC量子科技产学研创新联盟 QIAC中国信息协会量子信息分会

3. 量子安全系统的安全性评估需要整体视角

抗量子计算密码算法乃至量子安全的信息系统的安全性分析是复杂和需要整体性视角的，从密码分析学角度看，现有抗量子计算密码算法是针对防御已知的一部分类型的量子攻击而设计的，对于新发明的量子/经典攻击方式可能并不免疫。如 NIST 的 PQC 标准算法征集评估活动中发现，基于 LWE 问题的密码算法其设计目标是抵御量子选择明文攻击，对于量子选择密文攻击则不能抵御。同样，对于 NIST 征集的 PQC 标准算法中各种 NTRU 算法，最新的安全性分析表明，至少其中的一部分算法对于量子选择密文攻击也可能是脆弱的。各种物理攻击方式如侧信道攻击对于 PQC 的威胁也同样存在，只是 PQC 密码的物理实现可以较多的依赖现有 ICT 技术，对于传统侧信道攻击的防御技术也可以更多的传承和借鉴。

QKD 的安全性研究是一个比较专门和相对艰深的领域，这使得 QKD 所需要的安全性设计、标准化和评测具有较高的技术门槛。但这并不意味着，实际 QKD 系统达到相应的安全性目标具有不可逾越的障碍。QKD 现实条件下的安全性分析和对策是有章可循的[61]，它还是一个十分开放和活跃的领域，这将保障其研究的深入和充分性。

信息安全领域攻防相长的特点决定了密码，包括 PQC 或量子密码而非特定某一技术，都是在谨慎的安全设计与公开广泛的安全性分析二者的碰撞之间扬弃和发展，只是研究成熟程度、评估方法和安全基线等方面存在不同。除上述这些相对独立的各领域内研究的

热点问题外，从系统角度看，量子安全信息系统的各层面融合接口，如数学和物理方法的融合，公钥和对称密码的结合使用，都需要对这些融合接口、融合方法的安全性进行深入分析。综合来看，量子安全系统的安全性评估需要全面性和动态性的视角，对应的产品评估、系统评估、功能性能和可用性评估、以及相关标准规范研究还刚起步。

4. 向量子安全基础设施的迁移规划

向量子安全基础设施迁移建议分为三个阶段：

第一阶段：迁移准备阶段。在准备阶段的具体措施包括完善量子安全基础设施、提升量子安全能力和制定量子安全迁移路线图。在完善量子网络基础设施方面，具体措施包括：扩大广域量子骨干网络的覆盖范围，实现地级市一级的全部覆盖；地市建设量子城域网，同时充分利用我国光纤覆盖的优势，实现量子密钥分发到重点楼宇/园区等；通过量子安全密钥管理系统和量子安全服务平台，提供量子安全密钥分发到终端/应用及身份认证、加解密等密码服务等。在 QKD 网络暂未覆盖的区域，在遵循量子安全原则性要求的基础上，可综合采用预置密钥/人工递送、基于无线信道物理特征的密钥传输以及 PQC 密钥封装算法等密钥分发技术。

在提升量子安全能力方面，通过探索量子安全密码基础理论和应用技术，研究并突破量子密钥分发（QKD）协议实现安全模型和测试评估、身份认证与访问控制、量子计算场景下的新型密码组件、

QIC量子科技产学研创新联盟
QIAC中国信息协会量子信息分会

算法与协议设计、量子网络和设备安全防护、PQC 密码认证体系及密码迁移等关键技术，打造量子安全基础设施的防护体系，实现量子安全能力全面持续提升。

在制定量子安全迁移路线图方面，需对加密数据及资产和现有密码系统进行梳理来制定适合本组织的迁移路线。可依据前述第一章第三节“量子安全的重要性和紧迫性”的 XYZ 理论，通过对不同加密数据资产的重要性、数据资产故障的后果、数据资产被攻击的风险和可用资源等方面进行评估确定迁移顺序和时间表。当迁移顺序确认后，对已经确定迁移的加密数据/资产等，梳理其使用的加密算法、密码协议和密码组件等，选择适用的量子安全算法+量子安全密钥解决方案替换现有密码系统。

第二阶段：小规模实施改造和测试阶段。在本阶段的主要工作依据迁移优先次序选择代表机构和典型场景进行试点。重点一是逐步改造和替换现有密码基础设施，引入量子安全硬件，如量子加密路由器、量子加密光传输设备、量子加密终端等，并应用 PQC 对现有证书管理系统进行改造。二是该阶段需对密钥管理基础设施存储的使用不具有量子安全性算法加密的数据使用量子安全的算法进行重新封装，以保护密钥管理基础设施存储的数据，抵御“先存储后解密”攻击。三是改造完成后需对新系统进行功能和性能测试以验证是否实现迁移目标，以及是否符合用户对密码系统的总体要求。四是该阶段还需兼顾与解决与用户侧等处部署的现用密码系统的兼容性问题，可以采取先通过将现有密钥管理数据利用经典算法+量子

QIC量子科技大学创新联盟 QIAC中国信息协会量子信息分会

密钥加密保护的方式实现，以避免迁移过程中部分点位未配置 PQC 算法从而无法兼容的问题。

第三阶段：规模升级改造和应用阶段。依据第一阶段的量子安全迁移路线图和第二阶段小规模升级改造的经验，在行业监管单位的带头下，在各行业进行全面升级改造，以实现全面的量子安全迁移。

（二）面向金融行业的量子安全迁移规划现状

1. 金融行业面临量子攻击威胁的场景

密码算法是金融安全的基石。当前量子计算攻击主要威胁非对称密码算法的安全，该类算法在金融行业使用广泛，应用场景主要包括数据加密（含密钥协商）、数字签名两大类，前者使用非对称密码算法加密数据或交换密钥协商因子，目的是实现数据/密钥的机密性保护；后者使用私钥对数据进行签名，实现真实性、不可否认性安全服务。

由于数据加密场景保护的数据有保密期的概念，攻击者可以现在窃取已加密的密文并存储起来，待未来量子计算机可破解非对称密码算法后，再解密出明文数据，如果此时数据未过保密期，则会导致信息泄露。

对于数字签名场景，由于签名生成的签名值一般用于短期的认证过程，因此只要在量子计算机可破解公钥签名算法前升级到抗量子计算密码算法，并完成数字证书的重新签发及长期有效的签名数

QIC量子科技卓越创新联盟
QIAC中国信息协会量子信息分会

据的迁移，就可以避免量子计算攻击。

整体来看，数据加密场景面临的量子计算攻击威胁相对迫切，有必要优先部署抗量子计算攻击措施。当前金融行业正在开展量子安全技术的应用探索，主要包括基于量子密钥分发技术及抗量子计算密码算法的迁移。

2. 抗量子计算密码算法的实践探索

由于当前抗量子计算密码算法的标准还未正式发布，国内多家商业银行主要开展了 PQC 类算法的研究和验证。其主要工作是对主流抗量子计算密码算法进行技术验证，一是基于我国商密 SM2 算法与 PQC 算法混用的方案，在内部管理类应用开展了应用层传输加密、签名验签场景的试点验证；二是基于经典非对称密码算法与 PQC 算法混用的 TLS 协议，在办公园区的 VPN 路由器之间实现网络层数据传输加密。同时，针对密码算法升级复杂度高、周期长的挑战，还完成基础密码服务平台的敏捷性服务设计，通过将密码算法进行参数化配置，设计与具体密码算法无关的密码服务接口和报文格式，尽量降低应用系统与密码算法的耦合。未来升级密码算法时，在基础密码服务平台已支持新算法的情况下，调用方通过修改配置参数或少量代码修改，就可以实现密码算法升级，降低密码算法升级成本及周期。建设银行通过修改传输层安全协议流程，在现有基于经典公钥算法协商密钥因子流程的基础上，增加了基于 PQC 算法协商的新密钥因子，再基于多个密钥因子生成数据传输密钥，从而实现

QIC量子科技产学研创新联盟 QIAC中国信息协会量子信息分会

抵御经典计算和量子计算攻击的目的，并在内部应用进行了试点验证。

对于数字证书及签名数据的迁移，受限于相关标准目前还没有成型，目前金融行业尚未开展相关实践，密码产业界提出了以下思路：对于身份认证等签名数据仅需短期有效的场景，只需将旧证书撤销并基于抗量子计算密码算法颁发新证书即可。对于签名数据需要长期验证的场景，如果数据由单方签名并集中管理（如各类业务流程存档单据），则可以采取“重生”思路，即由原签名方使用抗量子计算密码算法对原始数据重新进行签名（此时包含新算法的签名值）；如果数据由多方签名（如长期险保单），则可以采取“续命”思路，即由其中一方或可信第三方使用抗量子计算密码算法再次签名（此时包含新旧算法的签名时间、签名值等信息），以证明相关数据是在旧算法被破解之前签署的。

3. 量子密钥分发技术的实践探索

自 2015 年起，国内主要大行已启动量子密钥分发技术的应用试点探索，在部分应用场景使用量子密钥分发技术代替传统非对称算法实现对称密钥的安全协商，再使用对称密码算法对敏感信息进行加密传输，进一步提升数据加密场景的安全性，并形成了一批典型示范案例。借助我国“京沪干线”等量子密钥分发骨干网及各地城域网的建设，各国有大行及股份制商业银行均已开展量子密钥分发技术的试点，在同城机房互联、异地数据中心互联、与合作方互联

QIC量子科技共创创新联盟 QIAC中国信息协会量子信息分会

等场景实现业务数据的量子安全加密传输。

2015 及 2017 年，国内主要大行基于量子密钥分发技术先后实现了同城及异地机房之间重要数据的加密传输；并于 2022 年，进一步探索了量子密钥分发技术的跨行业应用，实现了 ETC 交易数据的加密传输。2017 年，完成企业网银用例建设，将量子保密通信技术应用于金融企业网银用户的实时交易。并成功应用量子保密通信技术，实现了数字证书信息在徽商银行与中国金融认证中心（CFCA）之间的量子加密传输应用。在北京城域环网基于量子密钥分发技术实现总行、数据中心、业务处理中心等地的办公、生产和同城灾备数据的安全传输。2018 年，成功应用千公里级量子保密通信技术，实现京沪异地数据量子加密传输。2020 年，在济南分行中心机房与同城灾备机房间建立了量子保密通信网络，为中心机房与同城灾备机房间之间灾备数据及视频会议的传输提供量子安全加密保障。2021 年，在清算总中心开发并建设了量子密钥分发系统，实现了数据中心间密钥的安全分发。

（三）面向电力行业的量子安全迁移规划现状

1. 电力行业面临量子攻击威胁的场景

目前，电力系统基于自建光纤专网和合规现用商用密码构建的经典加密体系，是基于计算复杂度来保障敏感电网业务数据安全传输和设备管理的。随着计算能力的不断进步和各类密码破解算法的不断发展，特别是量子计算机的出现，经典密码体系被破解的风险

与日俱增，需要在经典密码体系的基础上融入新的技术，增强安全防护能力。

在数字化转型的大趋势下，很多新型业务，如大数据分析、大模型、人工智能、隐私计算等，都要求结合云服务实现分布式架构下多云及跨域的数据流转，这已经成为数据增值业务逻辑的基本要求。随着业务关联方多元化主体的不断引入，新业务间的交互方式呈多样化，以往隔离保护中的敏感数据需要面对流通共享、交叉访问、协同分析的需求，数据共享与隐私保护矛盾凸显。同时，以破坏业务可用性、获取或篡改数据为目的的内、外部系统侵入亦呈现递增趋势。

在明确安全管理责任的前提下，在涉及数据流转的关键环节如数据生成、数据隔离、数据处理、数据存储、数据共享等，实施统一的策略逻辑管理，屏避越权授权或越权数据操作，有效解决数据滥用、数据泄露等问题也变得越来越迫切。统一的策略实施建立在基于共享密钥保护的策略、指令下发和受密钥保护的独立策略比对运行环境基础上。而在实现共享密钥的流程中，基于 PKI 体系的 RSA、ECC 等算法受到量子计算能力日益提升的威胁。而另一种构成共享密钥的 DH 对称密钥交换协议也受到所谓“中间人攻击”的威胁；密钥共享的安全性直接涉及到策略实施的安全性。因此，在复杂国际环境背景下采用自主可控的安全技术以推动数据流转控制机制的实现已迫在眉睫。

QIC量子科技光学创新联盟 QIAC中国信息协会量子信息分会

2. 电力行业量子安全迁移规划

从实施量子安全体系出发，深入分析新型电力系统控制类、管理类、采集类业务安全防护需求与量子通信技术的结合点，有效借鉴前期研究和实践经验，引入先进、适用的量子通信技术，创新量子密钥分发网在异构网络、差异化业务中的应用技术、应用模式以及应用装备，实现新场景、新业务、新模式下的新型电力系统量子通信应用体系。

国家电网等电力企业对于量子安全迁移的布局总体规划上重视以量子密钥融入和强化现有电网安全加密体系：一是在密钥管理系统与分发传输网络上，基于前期已开展的量子通信技术研究，充分利用 QKD 网络在原理上无条件安全通信的优势，用以实现电网核心节点以及广域离散节点下生产控制类、管理采集类业务的安全可靠运行，作为电网运行管控过程中抵御各类计算破译的长效手段。二是在与现有业务场景的安全防护体系融合上，依托现有量子保密通信中光纤方式、无线方式的融合应用模式，构建面向配电、调度、电话电视会议等场景下的业务加密、通道加密、认证鉴权等量子密钥应用技术体系。三是在重点先期探索上，利用安全存储介质将量子密钥资源进一步向应用侧延伸，通过量子密钥的全生命周期安全管理和应用服务等扩展功能实现各类移动智能终端等的业务保护。

为满足电力行业量子安全需求，基于量子密钥分发网络（QKDN），融合经典密码应用技术，设计构造了一种新型的针对分布式业务或是分布式业务承载平台间数据流转策略的安全管控系统。

它可以在两点间安全联盟（或记录层协议）的协商阶段借助 QKDN 的对称密钥安全协商能力保护发起方及其响应方的（SA）安全载荷并提供双方发送的必要随机数，继而可以在业务安全逻辑协商（如 SSL 握手协议， IPSec SA 等）的第二阶段参与会话密钥的生成。在建立安全共享的会话密钥基础上，密码应用系统受业务控制逻辑的委托，可以辅助业务系统实现实现数据在多云或多业务结点间流转时的协同安全策略、认证、监管控制机制及数据处理环境的保护问题，适合于新型业务在多云服务环境下的数据生成、数据隔离，数据共享、数据处理和数据存储、策略逻辑等的协同管理。

3. 电力行业量子安全实践探索

国家电网有关单位与量子通信技术企业展开合作，已经开展了一系列的量子安全应用项目，从量子密钥生成、调度和应用维度开展研究，面向适配不同运营商的多种网络（4G、5G 硬切片），融入传统配电自动化安全防护系统，兼顾内容加密和通道加密，为各类配电终端建立安全可信的无线公网通信网络隧道，提升配电设备远程无线控制命令安全性能和架空线路电网资源掌控能力。

应用于电力系统配电自动化业务的基于 4G/5G 网络的量子安全应用平台，原理上以量子密钥生成技术为基础，将量子密钥生成与管理终端基于 BB84 协议生成的量子密钥，从光纤网络进一步延伸拓展，实现基于 4G/5G 网络的在线安全应用。平台部署实现了将量子密钥生成与管理终端，量子随机数两种量子技术的密钥生成源融合，

由安全服务平台统一调度、分发，实现了量子密钥源的云化部署，应用侧融合了电力业务系统的相关量子安全网关、量子安全 CPE 以及配电自动化终端设备，实现应用侧基于量子保密技术的业务加密通道建立。

应用于新型电力系统的基于 QKDN 的密码应用系统，既可以面向新型电力电力业务系统数据生成逻辑的策略控制、经典安全设备节点间的策略协同，也可以在新型电力业务承载平台和流量承载体系里发挥策略控制作用，从而构建了从虚拟化层资源管理、业务和数据处理中台含数据库，分布式业务封装，协议、I/O、路由与传输承载，调度，网络、设施、业务管理等从底层到上层基于量子密码应用的一体化协同密钥控制体系，为构建自主可控的 ICT 主动防御体系和以数据为核心的管控体系奠定了基础。

（四）面向电信行业的量子安全迁移规划现状

1. 电信行业对量子安全威胁的评估

电信行业对量子攻击暴露的攻击面广泛存在，量子安全需求广泛存在，例如电信网络基础设施加密，云计算、大数据、物联网等依托数据中心和泛在网络的应用安全防护，各类用户智能终端设备的加密与认证等。其中，电信行业优先考虑的重点是：由于物理基础设施——光纤电缆可被窃听，不加密、加密措施不具备量子安全性等，都易造成可能的敏感数据泄露。因此，数据在通过网络，包括互联网骨干网、广域网、城域网等，从一个位置到另一个位置的

QIC量子科技先导研创联盟 QIAC中国信息协会量子信息分会

整个传输过程中都必须受到保护，即保障数据完整性、机密性或真实性的密码技术保护。在此，结合量子安全的对称密码算法和基于QKD分发的对称密钥，可以实现此目标。

随着国家量子信息领域一系列战略性项目的实施，我国已建设总长超过1万公里的量子通信地面光纤网络，为QKD作为密钥管理基础设施的广泛应用奠定了必要基础。但也存在如下问题：一是基于专有光纤的QKD网络难以广泛满足有线、无线通信场景下网络、设备及业务系统的安全接入、加密传输等安全需求。二是通信和信息系统中存在海量、异构的安全机制、安全协议和安全应用，这些机制、协议和应用在量子安全赋能的过程中，会因为QKD网络层的功能相对单一而难以灵活适配。三是当前通过安全存储介质离线分发量子密钥只是对密钥资源的有限利用，仅能满足小范围内的业务应用需求。如何充分发挥QKD网络的增益效能是现阶段应对量子安全威胁的关键问题之一。解决方案是对于面向未来的规模化、多样化业务应用，应当通过整合QKD网络及量子密钥的安全能力，形成可提供包括加解密、认证/鉴权等通用功能的量子安全服务平台，将密钥生成管理与多样、复杂的应用场景解耦，从而为用户提供更全面、更可靠、更便捷的量子安全服务，最大限度地发挥QKD基础设施的作用。

2. 电信行业量子安全迁移规划

电信运营商量子安全迁移规划的重点是：一是将QKD网络作为

抗量子计算密码体系中密钥管理的基础设施，通过结合 PQC、对称密码等传统密码构建自主可控的量子安全体系，在云、网、管、端等层面与 ICT 体系相融合，从而实现更加丰富的安全业务应用，为用户提供更广泛的服务。二是在量子安全体系与 ICT 体系融合实践中，为解决 QKD 网络承载能力较弱、难以灵活适配，难以简单高效地满足规模化、多样化的应用需求等问题。研究与规划在底层 QKD 网络与上层用户网络之间新增量子密钥应用服务层，以 QKD 为核心，结合各种密码算法和应用服务，形成面向应用统一界面的量子密钥应用服务平台。三是建设统一规划的量子密码服务中心，将量子密钥分发干线、量子密钥分发网络、经典通信网络等都有机地联系起来，形成高效的量子密码应用服务系统，为各类系统、设备、网络、终端及应用等提供服务，进一步扩大 QKD 网络的应用范围，实现局域、城域及广域量子安全服务体系。

3. 电信行业量子安全迁移实践探索

国内运营商开展了量子密码应用服务系统的研究，特别是在用户网络层与 QKD 网络之间构建应用服务层方面，研究将用户网络与 QKD 网络解耦，并基于应用服务层中的量子密钥服务中心对 QKD 网络产生的量子密钥实现统一管理，从而增强 QKD 网络工程应用的灵活性。它一方面支持离线/在线、单端/双端的密钥获取方式，降低传统安全业务应用使用量子密钥的难度，使 QKD 更易与现有 ICT 系统相适配；另一方面，通过统一的服务接口及服务设备，增强了量

QIC量子科技先导研创新联盟
QIAC中国信息协会量子信息分会

子保密通信应用系统对并发业务的支持能力，满足用户规模化发展的需要，推动量子保密通信与 ICT 体系的融合发展。

目前，国内电信行业量子安全迁移的规划和探索体现在“云网管边端”的多层面和对内管理运维/对外客户服务的多类型。并已形成了丰富的应用场景，应用于运营商的骨干网、接入网等。在商用业务方面，中国电信已经推出了 VoLTE、VoIP 量子安全加密通话等的商用产品，并开展了规模化的量子安全业务尝试。

（五）区块链系统向量子安全迁移规划示例

本节从另一个层面——ICT 新应用模式中的区块链应用为例，阐述区块链系统向量子安全迁移规划的现有尝试。国际著名公有链项目组织以太坊基金会于 2024 年公布了以太坊项目抵御量子威胁的 EIP7560 提案，旨在通过在交易过程中不泄露用户私钥来保护交易免受量子攻击。蚂蚁链等国内企业也已有抗量子计算密码应用于联盟链的实践，针对区块链应用的交易、共识、节点间通信三个场景，进行区块链全流程的抗量子计算密码能力建设。

1. 评估区块链面临的量子攻击风险

用户对部署和运营区块链系统需考虑的一类主要底层安全风险是来自区块链中涉及公钥密码的风险：区块链目前得到广泛应用来自于它给不同诉求方间的协作带来新的信任基础，而这种信任基础建立在底层密码学所提供的安全性保障之上。这其中涉及到公钥密

码的用法可粗略分为：链上交易防篡改使用的数字签名机制，以及节点间通信使用的安全传输协议。交易过程中公钥签名算法的作用是：用户对交易信息签名，发送交易请求到客户端后，客户端构造一笔有效交易并广播到链上的所有节点上。由于用户的公钥注册在链上，链上的各个节点都可以通过公钥验证这笔交易的合法性，交易合法才被允许上链。

受 Shor 算法的影响，上述公钥密码在使用上的安全性无法得到有效保障。在考虑专用密码破译量子计算机大规模应用所需时间的同时，还需考虑存储在区块链上的数据需要保存多长时间以及现有区块链系统升级到量子安全级别的时间。如果后两者相加的时间和大于前者，那么区块链上的数据就会受到量子计算带来的严重安全威胁。

2. 区块链面向抗量子计算密码算法迁移的重点问题

在选择适配区块链应用的抗量子计算密码算法方面，将现有区块链使用的 ECC 等公钥密码算法升级为量子安全的抗量子计算密码算法，并针对当前抗量子计算密码签名尺寸问题，结合特定场景进行升级优化。具体优化工作需要考虑以下因素。一是要求密钥小且签名短：区块链上的每笔交易都会包含签名信息，而验证任意一笔交易的公钥也存储在链上。若密钥以及签名尺寸过大，都将大大加剧区块链的存储成本以及通信开销。二是计算效率要求高：区块链运行时每一时间段可处理的交易数量很大程度上与算法的运行时间

QIC量子科技发展创新联盟 QIAC中国信息协会量子信息分会

有关，特别是签名验签算法。算法更快的计算效率可以更好地支持高性能的区块链应用。

对于区块链这种分布式系统，迁移需要做到目前运行传统签名算法的客户端，可与运行抗量子计算密码签名算法的客户端兼容共存，并且预留出抗量子计算密码算法的可扩展可插拔接口，以此快速应对未来抗量子计算密码标准化的任何变化。

3. 同时适用于向 PQC/QKD 迁移的区块链中节点间通信机制

区块链中节点间通信机制一般使用了 TLS 协议增强其安全性，由于区块链的特性，节点既是客户端又是服务器。公钥密码算法在 TLS 通信上的使用范围集中在 TLS 的握手阶段。以 TLS1.3 为例，握手阶段主要包含两部分：密钥交换和认证。密钥交换方面，客户端和服务器通过询问得到通信双方支持的密码套件，以及使用密钥交换协议生成的预主密钥；认证方面，客户端和服务端会根据实际的认证需要，对对方的证书信息进行验证。因此，对于量子安全区块链的迁移应用，一方面要关注对 TLS 现用签名算法的迁移，这点与上述交易同理，二要关注密钥协商算法的迁移，对联盟链这种可配置 QKD 节点的，可不需要使用 PQC 类密钥封装算法，对于公链，可以使用 PQC 的密钥封装算法来实现改造升级。

QIC量子科技产学研创新联盟 QIAC中国信息协会量子信息分会

五、向量子安全迁移：一些开放性问题

当前，量子信息科技以其创造人类福祉和威胁既有密码安全的双面性而广受关注，业已成为全球主要国家发展战略和安全战略的关注焦点，该领域的全球性竞争已经展开。作为融合量子物理、信息技术以及密码技术的交叉创新科技，量子安全不仅是量子信息科技中的重要领域，也已经成为新一代密码技术发展的重要方向。量子安全已经开始从理论、原理性技术向实践转化，在技术标准、产品、解决方案等各方面都已完成了初步的准备。但与此同时，向量子安全迁移仍存在值得关注的一些开放性问题。

（一）用户向量子安全迁移的最佳时机

安全总是相对的，信息安全也不例外。在实际构建信息安全保障时，用户必然也必须去考虑安全威胁的程度、技术措施有效性以及成本之间的平衡。原理上，向量子安全迁移的最佳时机就在这一平衡刚好建立的时刻。然而，这一平衡究竟应当在何种程度上达成，却取决于用户对于安全的认知程度。而对于量子安全的认知又更加受到诸多主观和客观因素的制约，这使得最佳时机的选择变成了不存在标准答案的开放性问题。

就当前而言，用户想要加深对于量子安全的认识，仍然存在一些客观的困难。由于量子科技仍然是一个在快速发展的领域，基于已有的有限的知识很难对量子计算带来的安全威胁做出恰如其分的估计。另一方面，在量子计算的发展中，存在着一些研究者的言过

QIAC中国信息协会量子信息分会
QIC量子科技产学研创新联盟

其实和产业人士的肆意炒作，使得情况更加复杂。例如，前两年一时轰动的新闻，我国某团队声称发现了一种在现有的量子计算机上就可以运行并有效地破解 RSA 公钥密码的新量子算法。然而很快这个声称被发现是过分夸张的，该团队在论文中自己承认这种算法并不会稳定收敛，因此也并不清楚是否具有量子加速能力。

这些泡沫的破裂。反过来又带来如“量子计算实现永远在下一个十年”之类的讥诮，让一部分人错误地坚信量子计算不会对现有密码带来实际性的威胁。作为一个极端的低估量子计算安全威胁的示例：在不到十年之前，一种彻底否定量子计算对传统公钥密码存在威胁的观点指出，由于 Shor 算法破解 RSA 等公钥的计算复杂度是输入长度的 3 次方量级，因此当公钥的长度达到 1Tbit 时，破解 RSA 的量子计算机需要的量子比特的数目将是一个天文数字。可以估算出这个数字大约相当于一颗小行星里的原子总数。而此时，公钥密码的加解密大概只需要几十台服务器工作 1 年。这样，在这种观点看来，向量子安全迁移的最佳时间当然是在接近于无穷远的未来。然而，近年来的新的研究表明，假如有足够好的量子存储器，那么运行 Shor 算法的量子计算机的量子总数并不需要达到输入长度的 3 次方量级，而仅仅是输入长度的 1.5 次方。这样的话，即使公钥长度达到 1Tbit，所需的量子总数也大约只相当于一滴水中的原子总数。建造这样的量子计算机来破解 RSA 看起来仍是人类能力所及的范围。

QIC量子科技先导研究创新联盟
QIAC中国信息协会量子信息分会

围绕量子安全问题，虚假的炒作只能造成类似量子计算进展这样忽左忽右，忽而激进忽而激退的信息淆乱，让大多数用户更加难以准确地认识量子计算对信息安全的威胁程度。

（二）向量子安全迁移的最佳技术路线

一般地说，向量子安全迁移的技术路线可以大致地分为三大类，基于数学的 PQC 路线、基于物理的 QKD 路线以及融合 PQC 和 QKD 的路线。实际上，PQC 路线还可以进一步地细分，一类是基于单向函数的签名认证算法。单向函数是一类不可逆的操作，例如杂凑函数，从输入可以确定性地知道输出，而从输出却只能概率性地反推出输入。而另一类是基于数学上 NP 问题的公钥密码算法。

NP 问题是指目前不清楚是否能在多项式计算复杂度内算出正确答案，但可以在多项式计算复杂度内验证给定的答案是否正确的一类问题。与之对应则有 P 问题，也就是能够在多项式计算复杂度内算出正确答案的问题。如果 NP≠P，也就是说问题确实不能在多项式计算复杂度内得到答案，那么它就可以用来构造可靠的公钥密码。再考虑 NPC 问题和 NP-hard 问题。所有的 NP 问题都可以归约为 NPC 问题，也就是说，任何一个 NP 问题可以通过某种多项式复杂度的算法，转化为求解某一个 NPC 问题。因此 NPC 问题是最有可能确实不能在多项式计算复杂度内求解的。而 NP-hard 问题甚至都不清楚是否能在多项式计算复杂度内验证答案，并不能用于构造公钥密码。

QIC量子科技发明创新联盟 QIAC中国信息协会量子信息分会

是否能证明 NP≠P？也就说是不是所有的 NP 问题都找不到多项式计算复杂度的解法？这本身是一个开放性问题。但这并不妨碍密码学家利用 NPC 问题来构造公钥密码。因为的确还没有被公认为 NPC 问题的难题已经被找到多项式复杂度的解法。大多数研究计算复杂度理论的专家，包括数学家和计算机科学家们，都相信 NP≠P；在他们看来，证明 NP≠P 的过程比结果更重要。这句话隐含的意思是，他们认为 NP 一定不等于 P，证明 NP≠P 只是为了在这个过程中发现新的数学和计算理论。

量子力学的引入，为计算复杂度理论研究带来一些新的变化，但尚不足以解决 NP 是否等于 P 这样的问题。量子 Shor 算法能够破解 RSA 公钥密码所依赖的大整数分解问题，这是一个重大的理论进展。但这一点不表明量子计算机能解决 NP 问题。因为大整数分解问题并不是一个 NP 问题。在目前的计算复杂度理论中，将量子计算机能够在多项式复杂度内解决的问题归类为 BQP（bounded-error quantum polynomial time，有界误差量子多项式时间）问题，并认为 BQP 问题包含 P 问题和 BPP（Bounded-error Probabilistic Polynomial time，有界误差概率多项式时间）问题（BPP 问题被认为是经典计算能以多项式复杂度求解的所有问题）。这也就是说，量子计算机应该比经典计算机强一些。但也没有明确的证明，再回到大整数分解问题这个著名的例子，它的确是一个 BQP 问题，但也不知道它是不是一个 BPP 问题。如果它是一个 BPP 问题，那么破解大数分解问题就不能用来证明量子计算机比经典计算机强。

QIC量子科技先导研创新联盟 QIAC中国信息协会量子信息分会

BQP 和 NP 问题的关系仍然并不清楚这个事实，是密码学家们利用 NPC 问题来构造抗量子公钥密码背后的勇气。换而言之，量子计算机能不能在多项式复杂度内解决 NP 问题并不清楚，而计算复杂度专家们的答案应该倾向于不能。因此，密码学家相信可以利用 NPC 问题设计抗量子公钥密码算法。但还需要指出的是，严格地从一个 NP 问题出发构造密码也不是轻而易举的事情，尤其是在考虑到计算速度、计算资源等实用性问题带来的条件限制之后。在一个实际可用的密码算法中，必须对原始的 NPC 问题进行特殊化，这一特殊化过程的安全性往往难以证明和保障。这也是为什么在 NIST 征集 PQC 标准的过程中，不断有候选算法被曝出存在安全隐患而被淘汰的原因。实际上，在欧洲，也有很多密码学研究专家认为 PQC 不具备长期安全性——不具备长期安全性是“迟早会被破解”的一种书面而委婉的表达。总体而言，当前这些名义上以 NPC 困难问题为基础的公钥，我们既不能肯定地说它是可证明的量子安全，也不好说它是经验式的量子安全，其抗攻击能力的理论保证和实践结论，或许还需要进一步的观察。

QKD 路线面临的局面和 PQC 则完全不同。QKD 的安全性在理论上有完备的证明，所面临的挑战则完全来自于物理层面，主要是两个方面：QKD 的物理实现是否严格符合理论要求，或者说需要在多高的精度内符合理论要求？如何应对物理攻击以保证 QKD 设备在工作时仍然处于符合理论要求的状态？第一个方面关系到两个问题，一是如何精确量化分析误差对于安全性的影响？二是制造技术能否满

QIC量子科技奖学术创新联盟
QIAC中国信息协会量子信息分会

足相应的精度要求？QKD 业界认为，对于前者，这样的方法框架已经建立，并正在不断地改进以提高分析方法的紧致程度；对于后者，则不存在原理上的困难。第二个方面的问题更加开放一些，特别是如果对于攻击者实施物理攻击的能力不做任何限定的话。但是，对于 QKD 来说幸运的是，物理攻击终归要受到一定的物理规则的束缚，通过攻击改变设备工作状态也必定需要留下痕迹。因此，在实践中，原理上总是可以发现攻击，并相应地进行保护。因此，QKD 的理论安全性，以及这一理论安全的实际实现的可保障性，是 QKD 业界将 QKD 技术实用化的底气。然而，QKD 的功能仅是实现密钥分发，利用 QKD 可以建设新型的密钥基础设施，如何有效地利用这一设施以实现安全功能？利用“一次一密”的方式可以实现信息论安全的加密和认证。这是安全性最好的方式，但 QKD 的密钥分发速度目前还难以支持大带宽的“一次一密”加密通信。结合对称密码，可以解决加密带宽的问题，但也使得加密的强度下降到经验式的量子安全。另一方面，如何用量子方式来实现安全的数字签名？这一方面的研究还处于非常初步的阶段，尽管原理上可行，能否有效地应用于实际场景或者说如何改进方案以应用于实际场景，还需要进一步研究。

融合 QKD 和 PQC 是一种折衷的技术路线。PQC 用于解决签名认证问题，而 QKD 解决密钥分发问题。但是从安全逻辑的自洽性上来说，并非所有 PQC 都可以用来和 QKD 融合，至少我们需要 PQC 具有经验式的量子安全。在这一前提下，QKD 和 PQC 的融合系统才具有至少经验式的量子安全保障能力。此外，还需要说明，前文提到的

QIC量子科技产业创新联盟 QIAC中国信息协会量子信息分会

一种 QKD 和 PQC 融合的方式，是将 PQC 用于 QKD 系统组网时的设备认证。这一方案的安全逻辑是，由于在 QKD 设备完成认证后，后续产生的密钥安全性就不再依赖于初始的认证公私钥安全性，因此，假定量子计算破解 PQC 需要的时间大于 QKD 组网时设备认证需要的时间，则整个 QKD 系统就是量子安全的。这种融合只是用来简化 QKD 组网的复杂性，而不是直接用于用户业务，需要注意加以区别。

如果仅从安全性保障这一个角度来衡量“最佳”，或许“向量子安全迁移的最佳路线”这一问题并不那么开放。实际上，这一问题的开放性是由于我们不得不从多个角度，至少需要从安全性和可用性这两个角度来衡量“最佳”。如果还需要考虑到需求匹配程度、安全威胁预期、实施安全的成本等等，“最佳”将更加难以衡量，也使得我们的开放性问题转变为下一个问题——什么是“向量子安全迁移的最佳实践”？

（三）向量子安全迁移的最佳实践

如前所述，被量子算法破解的 RSA 公钥密码所依赖的大整数分解问题并不是一个 NP 问题，也不知道是不是一个 BPP 问题，但的确是一个 BQP 问题。破解 RSA 的量子 Shor 算法在 1994 年就已经被提出。巧合的是，也是在 1994 年由 RSA 颁发了据说是第一张 SSL 数字证书。仅仅在第一张 SSL 数字证书颁发两年后的 1996 年，基于格问题的 NTRU 算法被提出，格问题被认为是一个 NPC 问题，而这一算法的改进版 Falcon 算法也在近期入选了 NIST 的 PQC 标准。为什么是

QIC量子科技发展创新联盟 QIAC中国信息协会量子信息分会

RSA 公钥密码在之前的 30 年内被广泛接纳成为密码系统和基础设施的核心？而似乎一直没有人担忧过这个核心密码的算法的设计仅仅是基于一个从未被确信为 NP 问题的数学“难”题。这实际上正反映出密码系统的发展和信息安全实践中的复杂性，对“最佳”实践的判定和选择严重依赖于判决者对安全需求和技术能力的认知深度，也是十分困难的。

对于量子安全，关系到“最佳”实践判定的因素也毫不例外地复杂：对量子计算威胁紧迫性和危害性的认识、解决方案和需求的适配度、部署和运维成本都会影响到使用者对于“最佳”的判断。

对于量子计算威胁紧迫性，认识上的困难我们已在第一个问题中做了解释。对于其危害性的认识，目前实际上也存在不甚清晰之处。特别是，尽管可能越来越多的人开始了解到“先存储、后攻击”的方式使得量子计算攻击对于需要长期保密的数据具有格外严重的威胁。然而对于每个用户而言长期究竟是多长？究竟那些数据需要长期保密？已经产生的数据中是否存在需要长期保密的数据？面临的风险如何？这些问题，即便资深专业人士目前可能也难以确切地给出答案。

对于特定的安全需求来说，如何判断解决方案的适配度也存在一定的困难。这种困难很大一部分来自于技术自身的不确定性。例如，当前这些名义上基于 NP 问题的 PQC 所提供的安全保障期到底有多长？是否足够保护信息的安全？QKD 是否能够及时发现物理攻击，并保证输出的密钥不受影响？

QIC量子科技先导研创新联盟
QIAC中国信息协会量子信息分会

在部署成本和运维成本方面，目前而言，对于无论是部署 PQC 还是 QKD，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；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，还涉及密钥管理基础设施的对应迁移；此外，无论使用哪一种技术，或许还要多考虑一些技术迭代升级的风险。一般地说，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。而究竟哪一种方案的迁移的全生命周期成本更高？目前也并没有非常清晰的答案。

（四）通向开放性问题答案的途径

向量子安全迁移中存在的这些开放性问题，答案不会一下子就清晰，但通向答案的途径并非茫然无迹。这需要整个业界的共同努力：

1）净化环境，尽力杜绝炒作，尽早挤去技术泡沫，使产业界和用户了解到真实准确的技术进展，深入理解量子安全的底层原理和安全基础，从而建立科学、客观的量子安全共识。

2）深化开展量子安全技术的攻防演练、测试评估等工作，用深入、精准的评测推动我国量子安全密码能力建设及相关标准化工作，建立体系化的技术标准。

QIC量子科技产学研创新联盟
QIAC中国信息协会量子信息分会

3）深入开展量子安全系统的评估研究，以详实、客观的测试数据为基础，对量子安全系统的效能和全生命周期成本进行评估，并能用易于理解的方式展示评估结果。

4）加快推动量子技术的发展，发展量子中继、共纤复用、芯片化技术等，拓展 QKD 网络的覆盖能力，进一步加强量子密码以及自主化 PQC 密码研究，深入开展量子安全的应用场景研究，在此基础上形成差异化的解决方案。

我们坚信，只要坚持相信科学、实事求是的态度，前文所述的开放性问题，其答案必然会得到澄清，向量子安全迁移的趋势是不可逆转的。

量子技术是我国少有的和国际强国同时起跑又始终并驾齐驱的科技领域。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。在 QKD 与 PQC 融合应用方向上，中国的科研和产业化团队已经迈出了他们的步伐。毫无疑问，量子安全的全球“最佳”实践已在中国践行。

未来，我国宜继续发挥在量子技术方面的领先优势，基于“密码技术是密码算法和密钥管理有机整体”的科学认识，实施以“量

QIC量子科技先导研创新联盟 QIAC中国信息协会量子信息分会

子安全的密码算法”结合“量子密钥分发为核心的密钥管理系统”为基础，形成自主可控的量子安全密码方案，从机密性、完整性、真实性、不可否认性等方面全面实现密码功能的量子安全升级，从而实现量子安全的信息安全体系。通过对量子安全技术发展中一个个挑战的应对和困难的攻关，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必将得到长足的发展，服务国家，造福社会。

QIC量子科技产学研创新联盟
QIAC中国信息协会量子信息分会

附录 1 针对 QKD 实际安全性的攻击方案和防御措施

附录表 1-1：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	发布时间	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
激光种子攻击	源	激光器	实验	2019	光隔离/光强监控
通风口木马攻击	源	调制器	实验	2020	光隔离
脉冲致盲攻击	探测	单光子探测器	实验	2020	光电流监控

表注：上表中“安全性分析”是指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 1-2： 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	发布时间	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
功率分析攻击	源	调制器	理论	2021	降低功耗/制备功率随机化

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

QIAC中国信息协会量子科技分会 量子科技产学研创新联盟

附录 2 缩略语

英文简称	英文全称	中文名称
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	BKW 算法，主要用于解决 LWE 问题
BQP	bounded-error quantum polynomial time	有界误差量子多项式时间
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
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 D-H 密钥交换算法
ECDSA	Elliptic Curve Digital Signature	椭圆曲线数字签名算法

英文简称	英文全称	中文名称
	Algorithm	
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
HSP	Hidden Sub-group Problem	隐藏子群问题
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	因特网密钥交换协议
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
LOCC	Local Operations and Classical Communications	局域操作和经典通讯
LPN	Learning Parity with Noise	带噪声奇偶学习

英文简称	英文全称	中文名称
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	带舍入的模学习
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	MI 算法，是一种基于多变量的公钥密码体制算法。
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
NCSC	National Cyber Security Centre	英国国家网络安全中心
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	签名、完整性和加密的欧洲新方案方案
NISQ	Noisy Intermediate-Scale Quantum	中等规模含噪量子
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
NPC	Non-deterministic Polynomial Compelete	非确定性多项式完全
NSS	NTRU Signature Scheme	一种签名算法
NTRU	Number Theory Research Unit	一种公钥加密算法
NTT	Nippon Telegraph & Telephone	日本电报电话公司
OID	Object Identifier	对象标识
OSI	Open System Interconnection Reference Model	开放系统互联参考模型
OTN	Optical Transport Network	光传送网
OTP	One-time pad	一次性密码本
OTS	One-time Digital Signature	一次性数字签名
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

英文简称	英文全称	中文名称
PQC	Post Quantum Cryptography	抗量子计算密码
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
QDS	Quantum Digital Signature	量子数字签名
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	安全关联
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
SVP	Shortest Vector Problem	最短向量求解问题
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	双场量子密钥分发
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	驯化变换法
TTS	Tamed Transformation Signature	驯化变换签名
UOV	Unbalanced Oil and Vinegar	不平衡油醋

英文简称	英文全称	中文名称
VoLTE	Voice over Long-Term Evolution	长期演进语音承载
VPN	Virtual Private Network	虚拟专用网
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

QIC量子科技产学研创新联盟
QIAC中国信息协会量子信息分会

参考文献

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

[2]. 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.

[3]. 中华人民共和国国家质量监督检验检疫总局. GB/T 17901.1-2020 信息技术 安全技术 密钥管理. 2020.

[4]. 徐汉良. 商用密码知识与政策干部读本.人民出版社,2017.

[5]. 中华人民共和国国家质量监督检验检疫总局. GB/T 42565-2023量子计算 术语和定义. 2016.

[6]. 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, 2019.09.

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

[8]. Han-Sen Zhong et al., Phase-Programmable Gaussian Boson Sampling Using Stimulated Squeezed Light. Phys. Rev. Lett. 127, 180502 – Published 25 October 2021.

[9]. Yulin Wu, et al., Strong quantum computational advantage using a superconducting quantum processor. Phys. Rev. Lett. 127, 180501, https://arxiv.org/abs/2106.14734.

[10]. HAN-SEN ZHONG, et al., Quantum computational advantage using photons. SCIENCE, Dec 2020, Vol 370, pp. 1460-1463, DOI: 10.1126/science.abe8770.

[11]. https://www.ibm.com/quantum/assets/IBM_Quantum_Development_&_Innovation_Roadmap.pdf

[12]. Bluvstein, et al. Logical quantum processor based on reconfigurable atom arrays. Nature 2023.

[13]. Ni, Z., Li, S., Deng, X. et al. Beating the break-even point with a discrete-variable-encoded logical qubit. Nature 616, 56–60 (2023). https://doi.org/10.1038/s41586-023-05784-4

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

[15]. Craig Gidney, Martin Ekerå. How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. Quantum 5, 433 (2021).arXiv:1905.09749v3

[16]. ÉlieGouzien, Nicolas Sangouard. Factoring 2048-bit RSA Integers in 177 Days with 13 436 Qubits and a Multimode Memory. Phys. Rev. Lett. 127, 140503, September 2021. https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.127.140503.

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

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

[19]. 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).

[20]. 中华人民共和国国家质量监督检验检疫总局. GB/T 42829-2023 量子保密通信应用基本要求. 2023

[21]. Valerio Scarani, HelleBechmann-Pasquinucci, Nicolas J. Cerf, et al. The security of practical quantum key distribution, Reviews of Modern Physics, 81, 1301(2009).
[22]. 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.
[23]. Lily Chen, Stephen Jordan, Yi-Kai Liu, et al. Report on Post-Quantum Cryptography. NIST.IR.8015(2016).
[24]. AjtaiM,Generating hard instances of lattice problems.Proc. of ACM Symposium on Theory of Computing 1996,New York:ACM, p99-108(1996).
[25]. AjtaiM,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).
[26]. Gentry C.Fully homomorphic encryption using ideal lattices.Proc. of ACM Symposium on T heory of Computing 2009,New York:ACM, p169-178(2009).
[27]. 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).
[28]. 王小云, 刘明洁. 格密码学研究.密码学报,1(1):13-27(2014).
[29]. Peikert C, A decade of lattice cryptography． Foundations and Trends in Theoretical Computer Science,10(4):283-424(2016).
[30]. McEliece, R., A public key cryptosystem based on algebraic coding theory. DSN progress report, 42-44:114-116 (1978).
[31]. 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).
[32]. Merkle, R.C., A certified digital signature. Advances in Cryptology-CRYPTO1989 Proceedings, Lecture Notes in Computer Science, 435:218-238(1989).
[33]. 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).
[34]. Ward Beullens. Breaking Rainbow Takes a Weekend on a Laptop. https://eprint.iacr.org/2022/214.pdf
[35]. MATZOV IDF. Report on the Security of LWE: Improved Dual Lattice Attack. https://doi.org/10.5281/zenodo.6493704
[36]. Bennett, C. H., Brassard, G., QUANTUM CRYPTOGRAPHY: PUBLIC KEY DISTRIBUTION AND COIN TOSSING, Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing(IEEE, New York, 1984):175-179(1984).
[37]. Dagmar Bruß, Optimal Eavesdropping in Quantum Cryptography with Six States, Physical Review letters, 81(14):3018-3021(1998).
[38]. 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).
[39]. Won-Young Hwang, Quantum key distribution with high loss: toward global secure communication, Physical Review Letters, 91(5): 057901(2003).
[40]. Xiang-Bin Wang, Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography, Physical Review letters, 94(23):230503(2005).
[41]. Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen, Decoy State Quantum Key Distribution, Physical Review letters, 94(23):230504(2005).
[42]. Kyo Inoue, Edo Waks, and Yoshihisa Yamamoto, Differential Phase Shift Quantum Key Distribution, Physical Review letters, 89(3):037902(2002).

[43]. Damien Stucki, Nicolas Brunner, Nicolas Gisin, et al. Fast and simple one-way quantum key distribution, Applied Physics Letters, 87:194108(2005).
[44]. Toshihiko Sasaki, Yoshihisa Yamamoto, and Masato Koashi, Practical quantum key distribution protocol without monitoring signal disturbance, Nature, 509:475-478(2014).
[45]. Frédéric Grosshans and Philippe Grangier, Continuous Variable Quantum Cryptography Using Coherent States, Physical Review letters, 88(5):057902(2002).
[46]. A. Leverrier and P. Grangier, Unconditional Security Proof of Long-Distance Continuous-Variable Quantum Key Distribution with Discrete Modulation, Phys. Rev. Lett. 102, 180504 (2009).
[47]. Artur K. Ekert, Quantum cryptography based on Bell's theorem, Physical Review letters, 67(6):661(1991).
[48]. Charles H. Bennett, Quantum cryptography using any two nonorthogonal states, Physical Review letters, 68(21):3121(1992).
[49]. A Acin, N Brunner, N Gisin, S Massar, S Pironio, V Scarani. Device-Independent Security of Quantum Cryptography against Collective Attacks. Physical review letters, 2007, 98(23):p.230501.1-230501.4.
[50]. Hoi-Kwong Lo, Marcos Curty, and Bing Qi, Measurement-Device-Independent Quantum Key Distribution, Physical Review letters, 108(13):130503(2012).
[51]. Xiong-Feng Ma, Pei Zeng, and Hong-Yi Zhou, Phase-Matching Quantum Key Distribution, Physical Review X, 8(3): 031043(2018).
[52]. 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).
[53]. Daniel Gottesman, Isaac Chuang, Quantum Digital Signatures, arXiv: quant-ph/0105032(2001).
[54]. Petros Wallden, VedranDunjko, Adrian Kent, Quantum Digital Signatures with Quantum-Key-Distribution Components, Physical Review A, 91(4):042304(2015).
[55]. Hua-Lei Yin, Yao Fu, Hui Liu, et. al., Experimental quantum digital signature over 102 km, Physical Review. A, 95(3): 032334(2017).
[56]. G. L. Roberts, M. Lucamarini, Z. L. Yuan, et. al., Experimental measurement –device - independent quantum digital signatures, Nature Communications, 8:1098(2017).
[57]. Vaidman L. Teleportation of Quantum States.1993.DOI:10.1103/PhysRevA.49.1473.
[58]. Bouwmeester D, Pan J W, Mattle K, et al. Experimental quantum teleportation. Nature, 1997, 390(6660):575–579.
[59]. Valerio Scarani, HelleBechmann-Pasquinucci, Nicolas J. Cerf, et al., The security of practical quantum key distribution, Reviews of Modern Physics, 81: 1301(2009).
[60]. Xiang-Bin Wang, Jing-Tao Wang, Ji-Qian Qin, et al., Guessing probability in quantum key distribution, npj Quantum Information, 6: 45(2020).
[61]. 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).
[62]. Shihai Sun, Feihu Xu. Security of quantum key distribution with source and detection imperfections. New Journal of Physics, Volume 23, February 2021.
[63]. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/564946/gs-16-18-quantum-technologies-report.pdf.
[64]. Yuan, Z.; Murakami, A.; et al., 10-Mb/s Quantum Key Distribution. Journal of Lightwave

Technology, 2018, 36, 3427-3433.

[65]. Grünenfelder, F.; Boaron, A.; Rusca, D.; Martin, A. &Zbinden, H. Performance and security of 5GHz repetition rate polarization-based quantum key distribution. Applied Physics Letters, 2020, 117, 144003.

[66]. Li, W., Zhang, L., Tan, H. et al. High-rate quantum key distribution exceeding 110 Mbs–1. Nat. Photon. 17, 416–421 (2023). https://doi.org/10.1038/s41566-023-01166-4

[67]. 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).

[68]. Sheng-Kai Liao, Wen-Qi Cai, Wei-Yue Liu, et al. Satellite-to-ground quantum key distribution. Nature 549, 43–47 (2017).

[69]. Juan Yin, Yu-Huai Li, Sheng-Kai Liao, et al. Entanglement-based secure quantum cryptography over 1,120 kilometres. Nature, 582: 501-505 (2020).

[70]. Chen, J.-P.; Zhang, C.; Liu, Y.; Jiang, C.; Zhang, W.-J.; Han, Z.-Y.; et al., Twin-field quantum key distribution over a 511 km optical fibre linking two distant metropolitan areas. Nature Photonics, 2021, 15, 570-575.

[71]. Pittaluga, M.; Minder, M.; Lucamarini, M.; Sanzaro, M.; Woodward, R. I.; Li, M.-J.; Yuan, Z. & Shields, A. J. 600-km repeater-like quantum communications with dual-band stabilization. Nature Photonics, 2021, 15, 530-535.

[72]. Shuang Wang, Zhen-Qiang Yin, De-Yong He, et al., Twin-field quantum key distribution over 830-km fibre. Nature Photonics, Nat. Photon. (2022). https://doi.org/10.1038/s41566-021-00928-2.

[73]. Yang Liu, Wei-Jun Zhang, et, al. Experimental Twin-Field Quantum Key Distribution Over 1000 km Fiber Distance. https://doi.org/10.48550/arXiv.2303.15795

[74]. 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).

[75]. Henry Semenenko, Philip Sibson, Andy Hart, et al., Chip-based measurement-device-independent quantum key distribution. Optica, 7: 238-242 (2020).

[76]. 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).

[77]. Paraïso, T. K.; Roger, T.; Marangon, D. G.; Marco, I. D.; Sanzaro, M.; Woodward, R. I.; Dynes, J. F.; Yuan, Z. & Shields, A. J. A photonic integrated quantum secure communication system. Nature Photonics, 2021, 15, 850-856.

[78]. Pompili, M.; Hermans, S. L. N.; Baier, S.; Beukers, H. K. C.; Humphreys, P. C.; Schouten, R. N.; Vermeulen, R. F. L.; Tiggelman, M. J.; dos Santos Martins, L.; Dirkse, B.; Wehner, S. & Hanson, R. Realization of a multinode quantum network of remote solid-state qubits. Science, 2021, 372, 259-264.

[79]. Langenfeld, S.; Thomas, P.; Morin, O. & Rempe, G. Quantum Repeater Node Demonstrating Unconditionally Secure Key Distribution. Physical Review Letters, 2021, 126, 230506.

[80]. Pu, Y.-F.; Zhang, S.; Wu, Y.-K.; Jiang, N.; Chang, W.; Li, C. & Duan, L.-M. Experimental demonstration of memory-enhanced scaling for entanglement connection of quantum repeater segments. Nature Photonics, 2021, 15, 374-378.

[81]. Wang, X.-J.; Yang, S.-J.; Sun, P.-F.; Jing, B.; Li, J.; Zhou, M.-T.; Bao, X.-H. & Pan, J.-W. Cavity-Enhanced Atom-Photon Entanglement with Subsecond Lifetime. Physical Review

Letters, 2021, 126, 090501.

[82]. Fiaschi, N.; Hensen, B.; Wallucks, A.; Benevides, R.; Li, J.; Alegre, T. P. M. &Gröblacher, S. Optomechanical quantum teleportation. Nature Photonics, 2021, 15, 817-821.

[83]. Liu, X., Hu, J., Li, ZF. *et al.* Heralded entanglement distribution between two absorptive quantum memories. Nature 594, 41–45 (2021). https://doi.org/10.1038/s41586-021-03505-3

[84]. Luo, X.-Y., Yu, Y., Liu, J.-L. et al. Postselected Entanglement between Two Atomic Ensembles Separated by 12.5 km. Physical Review Letters, 129(5), 050503

[85]. Dong, M. X., Zhang, W. H., Zeng, L. et al. Highly efficient storage of 25-dimensional photonic qudit in a cold atom-based quantum memory. Physical Review Letters, 131, 240801 – Published 15 December 2023

[86]. Li, M.-H.; Zhang, X.; Liu, W.-Z.; Zhao, S.-R.; Bai, B.; Liu, Y.; Zhao, Q.; Peng, Y.; Zhang, J.; Zhang, Y.; Munro, W. J.; Ma, X.; Zhang, Q.; Fan, J. & Pan, J.-W. Experimental Realization of Device-Independent Quantum Randomness Expansion. Physical Review Letters, 2021, 126, 050503.

[87]. Bai, B.; Huang, J.; Qiao, G.-R.; Nie, Y.-Q.; Tang, W.; Chu, T.; Zhang, J. & Pan, J.-W. 18.8 Gbps real-time quantum random number generator with a photonic integrated chip. Applied Physics Letters, 2021, 118, 264001.

[88]. Yu-Xuan Liu, Ke-Xin Huang, Yu-Ming Bai et al. A High-Randomness and High-Stability Electronic Quantum Random Number Generator without Post Processing. 2023 Chin. Phys. Lett. 40 070303

[89]. European Quantum Flagship. Strategic Research and Industry Agenda. https://qt.eu//app/uploads/2020/04/Strategic_Research-_Agenda_d_FINAL.pdf

[90]. Yong-Hua Yang, Pei-Yuan Li, Shi-Zhao Ma, et al., All optical metropolitan quantum key distribution network with post-quantum cryptography authentication. Optics Express Vol. 29, Issue 16, pp. 25859-25867(2021). https://doi.org/10.1364/OE.432944

[91]. 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).

[92]. Max Brauer, Rafael J. Vicente, et al., Linking QKD testbeds across Europe. Entropy 2023, 1, 0.https://doi.org/

[93]. ISO. Security requirements, test and evaluation methods for quantum key distribution Part 1: requirements. ISO/IEC 23837-1.

[94]. 中华人民共和国国家质量监督检验检疫总局. GB/T 17903.1-2008 信息技术 安全技术 抗抵赖 第 1 部分：概述.

[95]. 中华人民共和国国家质量监督检验检疫总局. GB/T 17903.2-2008 信息技术安全技术 抗抵赖 第2部分：采用对称技术的机制.

[96]. 中华人民共和国国家质量监督检验检疫总局. GB/T 15843.4-2008 信息技术 安全技术 实体鉴别 第4部分：采用密码校验函数的机制.

[97]. NIST. Migration to Post-Quantum Cryptography Quantum Readiness: Cryptographic Discovery. https://www.nccoe.nist.gov/sites/default/files/2023-12/pqc-migration-nist-sp-1800-38b-preliminary-draft.pdf

[98]. NIST. Migration to Post-Quantum Cryptography Quantum Readiness: Testing Draft Standard. https://www.nccoe.nist.gov/sites/default/files/2023-12/pqc-migration-nist-sp-1800-38c-preliminary-draft.pdf