光子盒
GUANGZIHE

量子通信&安全系列报告

# 后量子密码（PQC）

## ——未来安全的风暴热点

光子盒研究院

2022 年 5 月

# 前言

## Foreword

从2量子比特到127量子比特，量子计算正在飞速发展。由于量子计算的并行计算能力预计未来可为众多需要大规模计算的难题提供解决方案，因此成为各国争相布局的技术前沿。但是，量子计算能力的提高同时将对当前经典密码体系下的信息安全造成巨大威胁。为了抵御未来量子计算实用化对当前密码体系的潜在冲击，几乎所有的加密算法都需要进行改进甚至必须进行迁移。由此，全球正在开展保护数据和加密通信的研究，其中包括2006年以来研究的后量子密码学（Post-quantum cryptography，PQC），又称抗量子密码学（Quantum-resistant cryptography），包括更新密码协议和标准等措施。

在美国，PQC的研究和实施活动得到多个政府机构的支持，包括NIST（国家标准与技术研究院）、NSF（国家科学基金会）、DOD（国防部）、DHS（国土安全部）和NSA（国家安全局）。此外，欧洲、日本、中国在PQC研究中也迅速崛起，力争在PQC标准中占据一席之地。在推进PQC技术标准的过程中，影响力最大的是NIST面向全球征集技术方案。

PQC能否成为抵御“量子之矛”（量子计算机）的“量子之盾”？这可能还需很长一段时间去验证，在没有开发出完全可用的量子计算机的情况下，难以真正衡量一个PQC算法的强度。即使如此，提前研究PQC并做好相应部署，仍十分必要。

# 声明

## Declaration



光子盒引用其他资料的目的在于呈现信息，并不代表光子盒赞同其全部观点，不对其真实性、时效性负责。

本报告具有一定的时效性，仅表达截至发稿时的情况，不代表未来情况。在任何情况下，本报告中的信息或所表述的意见均不构成投资建议。

# 目录

# 表目录



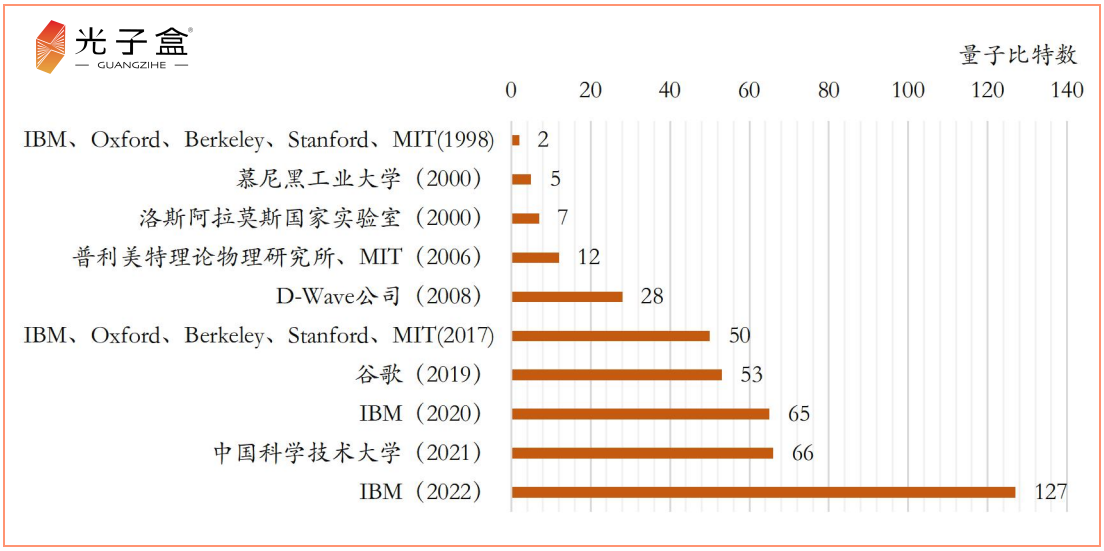
# 图目录

# 一、PQC 恰逢其时

## （一）经典密码体系面临危机

随着量子计算技术不断取得突破，算力大幅提升，特别是以 Shor 算法为典型代表的量子算法的提出，相关运算操作在理论上可以实现从指数级别向多项式级别的转变。目前看来，量子计算机有潜力将破解速度从经典计算机的 1 万年，变为“一个响指”的时间。这意味着，在量子计算机面前，传统加密方式的信息被偷听窃密的可能性急剧增加。量子计算对公钥密码的潜在威胁是不容忽视的，有潜力完全攻破目前广泛使用的公钥密码算法，即便是增加参数长度也是无效的，因此，需要 PQC 作为新的解决方案。

图 1 量子计算能力演进图




注：尽管量子比特数不是衡量量子计算性能的唯一参数（还有保真度、相干时间、连接性等），但作为重要指标可以反映量子计算发展速度。

## （二）PQC 应运而生

为了应对量子计算对公钥密码算法的威胁，PQC 应运而生。PQC 是能够抵抗量子计算对现有密码算法攻击的新一代密码算法，旨在研究密码算法在量子环

境下的安全性，并设计在经典和量子环境下均具有安全性的密码系统。

对于对称密码算法，尽管量子计算机可能降低现有算法的安全性，从 k-bit 降低为 k/2-bit，但增大参数的长度对维护安全性是有效的。因此，PQC 的研究重点是非对称密码算法。PQC 与近些年发展迅速的量子密钥分发（主要包括 QKD）有所差异，量子密码学涉及利用量子物理特性的密码算法，PQC 关注的是可在经典计算机上运行的算法，这类算法即使用量子计算机也无法被破坏。

**表 1 量子计算能力对当前经典密码系统的影响**

| 密码算法 | 类型 | 作用 | 潜在量子计算能力威胁造成的冲击 |
|---|---|---|---|
| AES | 对称密钥 | 加密 | 增大密钥长度 |
| SHA-2、SHA-3 | — | 哈希功能 | 输出长度增加 |
| RSA | 公钥密码 | 数字签名<br>密钥建立 | 丧失安全性 |
| ECDSA、ECDH | 公钥密码 | 数字签名<br>密钥交换 | 丧失安全性 |
| DSA | 公钥密码 | 数字签名<br>密钥交换 | 丧失安全性 |

来源：Report on Post-Quantum Cryptography[1]、光子盒研究院

**表 2 经典密码、QKD 和 PQC 比较**

| 保密类型 | 技术基础 | 专用设备 | 出发点 | 关注点 | 安全性 | 现存问题 |
|---|---|---|---|---|---|---|
| 经典密码 | 数学原理 | 无需专用硬件设备 | 解析数学难题 | 密钥的保密性 | 不能抵御量子计算机攻击 | 不能抵御量子计算机攻击 |
| QKD | 物理原理 | 需专用硬件设备 | 一次一密加密体制 | 解决密钥分配问题 | 量子环境下，理论绝对安全 | 成本高、有硬件要求、应用场景有限 |
| PQC | 数学原理 | 无需专用硬件设备 | 解析数学难题 | 非对称密码系统 | 量子环境下，理论绝对安全 | 未经过充分验证 |

来源：光子盒研究院

[1] https://csrc.nist.gov/publications/detail/nistir/8105/final

# 二、PQC 算法方案与标准

## （一）主要方案及对比

PQC 算法目前有四种主流方案：基于哈希（Hash-based）的公钥密码学、基于编码（Code-based）的公钥密码学、基于多变量（Multivariate-based）的公钥密码学、基于格（Lattice-based）的公钥密码学。

**1.基于哈希的方案**

基于哈希的签名算法由 Ralph Merkel 提出，被认为是传统数字签名（RSA、DSA、ECDSA 等）的可行代替算法之一[2]。基于哈希的签名算法由一次性签名方案演变而来，并使用 Merkle 的哈希树认证机制。哈希树的根是公钥，一次性的认证密钥是树中的叶子节点。基于哈希的签名算法的安全性依赖哈希函数的抗碰撞性。由于没有有效的量子算法能快速找到哈希函数的碰撞，因此（输出长度足够长的）基于哈希的构造可以抵抗量子计算机攻击。此外，基于哈希的数字签名算法的安全性不依赖某一个特定的哈希函数。即使目前使用的某些哈希函数被攻破，还可用更安全的哈希函数直接代替被攻破的哈希函数。

**2.基于编码的方案**

基于编码的算法使用错误纠正码对加入的随机性错误进行纠正和计算。一个著名的基于编码的加密算法是 McEliece[3]。McEliece 使用随机二进制的不可约 Goppa 码作为私钥，公钥是对私钥进行变换后的一般线性码。Courtois、Finiasz 和 Sendrier 使用 Niederreiter 公钥加密算法构造了基于编码的签名方案[4]。基于编码的算法（例如 McEliece）的主要问题是公钥尺寸过大。基于编码的算法包括加密、密钥交换等。基于多变量（Multivariate-based）的方案，被认为是能够抵御基于量子计算机攻击的新型公钥密码体制之一。

---

[2] Merkle R C, Charles R, et al. Secrecy, authentication, and public key systems[J]. 1979.
[3] Mceliece R J. A public-key cryptosystem based on algebraic[J]. Coding Thv, 1978, 4244:114–116.
[4] Courtois N T, Finiasz M, Sendrier N. How to achieve a McEliece-based digital signature scheme[C]. Proceedings of International Conference on the Theory and Application of Cryptology and Information Security. Springer, 2001. 157–174.

**3.基于多变量的方案**

基于多变量的算法使用有限域上具有多个变量的二次多项式组构造加密、签名、密钥交换等算法[5]。多变量密码的安全性依赖于求解非线性方程组的困难程度，即多变量二次多项式问题。该问题被证明为非确定性多项式时间困难。目前没有已知的经典和量子算法可以快速求解有限域上的多变量方程组。与经典的基于数论问题的密码算法相比，基于多变量的算法的计算速度快，但公钥尺寸较大，因此适用于无需频繁进行公钥传输的应用场景，例如物联网设备等。

**4.基于格的方案**

格（Lattice）是一种数学结构，定义为一组线性无关的非 0 向量（称作格基）的整系数线性组合。格密码的主要数学基础是格中的两个困难问题：格的最短矢量问题（SVP）和格的最近矢量问题（CVP）。SVP 是对于给定的一组基,找出其所生成的格中欧氏距离（两点之间的距离）最小的非零向量。即在格上找到一个非零向量 v，满足对格上的任意非零向量 u,均有$\|v\| \leq \|u\|$。CVP 是对于给定的格及任一向量,找出格中与该向量距离最近的向量。即在格上找到一个向量 v,满足对格上的任意非零向量 u,均有$\|v-y\| \leq \|u-y\|$。格是一个困难的问题，并且难度还能控制，满足了成为密码学算法核心的必要条件。

PQC 算法中，对格的研究是最活跃、最灵活的。基于格的算法在安全性、公私钥大小[6]、计算速度上可达到较好的平衡。第一，基于格的算法可以实现加密、数字签名、密钥交换、属性加密、函数加密、全同态加密等各类功能的密码学构造。第二，基于格的算法的安全性依赖于求解格中问题的困难性。这些问题在达到相同的安全强度时，基于格的算法的公私钥大小比上述其他三种方案更小，计算速度更快，且能被用于构造多种密码学原语，更适用于真实世界中的应用。因此，基于格的算法被认为是最有前景的 PQC 算法之一[7]。

---

[5] Ding J, Gower J E, Schmidt D S. Multivariate public key cryptosystems[M], volume 25. Springer Science & Business Media, 2006.

[6] 注：公私钥大小是常见说法，指密钥长度，如 2014 位、2048 位。

[7] Nejatollahi, H. , Shahhosseini, S. , Cammarota, R. , & Dutt, N. . (2021). Exploring energy efficient architectures for rlwe lattice-based cryptography. Journal of Signal Processing Systems, 1-10.

表 3 四类 PQC 方案优缺点比较

| PQC 方案分类 | 优点 | 缺点 |
|---|---|---|
| 基于哈希算法签名 | 安全要求是最小的 | 只能用于量子签名方案（签名/验签） |
| 基于编码密码 | 加解密速度快 | 大型公钥大小（100KBS-MBS），签名/验签成本大 |
| 基于多变量方程式密码 | 与基于哈希的签名方案相比，签名较短，效率较高 | 与传统的 RSA、ECC 等系统相比，公钥量大；安全性不确定 |
| 基于格密码 | 可证明安全：基于最坏情况的强安全性证明；相对高效的实现；非常简单；多用途，许多先进的密码体制的提出都是基于格密码，例如：IBE、ABE、FHE | 暂无（未经过充分验证） |

来源：光子盒研究院

## （二）标准研究和制定

近年来，多国密码管理部门对 PQC 研究开始重视和推进，由于目前尚未实现算法标准化，还未发展到实际系统研发和基础设施推广建设阶段。当前主要是标准化组织、各国密码或安全管理部门、产业界推进 PQC 密码的标准化。从全球算法征集和标准制定角度来看，欧洲、美国和中国走在国际前沿。

表 4 PQC 标准研究及制定

| 地区/区域 | 相关机构 | 标准工作 |
|---|---|---|
| 欧洲 | 欧洲电信标准化协会（ETSI） | 成立小组专门负责 PQC 方面的标准制定和研究工作[8] |
| | 欧盟（EU） | 启动“PQCRYPTO”后量子加密技术项目，开发新的加密系统[9] |
| 美国 | 国家标准与技术研究院（NIST） | 面向全球启动后量子密码标准竞选，已完成三轮竞选，预计 2024 年确立后量子公钥密码标准[10] |
| 中国 | 中国密码学会（CACR） | 面向中国举办后量子密码算法竞赛[11] |
| 总部在美国 | 国际互联网工程组织（IETF） | 在 RFC 8391 中标准化 XMSS[12] |

[8] https://www.etsi.org/committee/1393-cyber
[9] https://www.fmprc.gov.cn/ce/cebe/chn/kjhz/kjdt/t1591743.htm
[10] https://csrc.nist.gov/news/2016/public-key-post-quantum-cryptographic-algorithms
[11] https://sfjs.cacrnet.org.cn/site/content/309.html
[12] https://tools.ietf.org/id/draft-irtf-cfrg-xmss-hash-based-signatures-10.html

来源：光子盒研究院

## （三）PQC 算法的硬件实现

目前，大多数 PQC 算法还处在审查阶段，研究重点更多地是专注算法层面的安全性、成本和性能的评估和优化，在 PQC 算法的硬件实现方面相关研究还较少。PQC 算法在硬件实现上主要面临两个挑战，一是算法规范的数学复杂性，此类规范通常是由密码学家编写的，关注的重点是其安全性而非实现的效率；二是在硬件实现上需要存储大型公钥、私钥和内部状态，这可能会导致不能实现真正的轻量级，而且会影响硬件实现的效率。目前后量子加密算法的硬件实现方式包括 PQC 硬件应用程序编程接口（API）的开发、基于 HLS（HTTP Live Streaming）的抽象实现和基于 FPGA/ASIC 平台的硬件实现。

API 满足后量子密码系统的各种需求，包括最低遵从标准、接口、通信协议和 PQC 核支持的时间特性。PQC 核接口由六大数据总线组成：公共数据输入、私密数据输入、随机数据输入、公共数据输出、私密数据输出和外部内存输入输出。

基于 HLS 的抽象实现是将 HLS 应用于 PQC 加速器设计或利用 HLS 为 PQC 算法提供面积优化和速度优化的解决方案，从而保证硬件的安全性，防止定时侧通道攻击。

利用 FPGA 技术，实现基于大容量 FPGA 的 PQC 算法硬件平台，并进行进行 PQC 算法的综合、验证和物理实现，可提高密钥生成和签名生成的速度。

# 三、PQC 应用体系

## （一）PQC 主要应用

目前，PQC 算法中的热点研究可以直接代替现有的公钥加密、数字签名、密钥交换算法，包括 RSA 加密/签名、Diffie-Hellman 密钥交换、椭圆曲线加密/签名等。与现有的公钥密码算法一样，PQC 可以被应用于更高层次一些的协议/应用，包括 HTTPS（TLS）、数字证书（PKI）、SSL、VPN、IPSec、比特币等数字货币、U 盾、移动操作系统等各个领域和应用中。现在用到公钥密码算法的应用，基本可以使用 PQC 算法进行代替。

表 5 PQC 技术的应用栈

| | |
|---|---|
| **应用** | 网络浏览器、证书、数字货币、软件更新、操作系统 |
| **协议** | SSL，TLS，IPSec（IKE） |
| **密码学** | PQC：公钥加密；数字签名；密钥交换<br>混合模式（PQC+经典） |
| **基础层面** | 库（GMP，NTL）<br>分组密码（AES）<br>哈希函数<br>RNGs<br>硬件支持维护基于哈希算法的签名 |

来源：光子盒研究院

PQC 应用领域主要包括民政、军事、情报和国家安全、电信、数据中心、灾难恢复、金融服务和其他。

图 2 PQC 主要应用领域


## （二）PQC 应用时间

对于许多公司来说，PQC 时代已经开始。例如，越来越多的联网车辆将需要满足高安全标准，以保护用户在使用寿命内的安全和隐私。尽管当前使用和存储的大多数数据不会受到影响，但海量数据、关键系统和旗舰产品的安全性仍处于危险之中。

对于相关企业来说，何时开始采取措施，采取怎样的措施因行业和企业而异。在确定何时开始采取量子缓解措施时，企业需要考虑高优先级资产的两个关键特征——数据保质期以及系统生命周期和开发周期。

一般来说，银行、保险、公共管理部门具有较长的数据保质期和系统生命周期，可能在 2025 年之前就会面临风险；生命科学类具有较长数据生命周期和较短系统生命周期的行业，以及先进产业、全球能源和材料等具有较短数据保质期和较长系统生命周期的行业可能在 2025 年至 2030 年开始面临风险，而电信、媒体、信息技术、旅行、物流、消费类电子产品等行业具有较短的数据保质期和系统生命周期，可能在 2030 年之后才会面临风险。

# 四、PQC 面临的潜在威胁与挑战

## （一）威胁

PQC 通过数学理论保证了算法的安全性，但在具体实现和应用中易受侧信道攻击（Side-channel attack）。侧信道攻击能够利用密码算法在密码芯片上运行时泄露出来的侧信息，分析并恢复出密钥或加密信息，是密码算法物理安全的主要威胁手段，这严重威胁到 PQC 的安全性。

侧信道攻击从目标密码系统在平台运行中获取侧信息，与其他形式的密码分析形成了对比，在其他形式的密码分析中，一般都是攻击算法及其底层的计算问题，所有的电子设备都会以多种方式泄露信息，侧信道攻击通过来自目标设备泄露的这些信息来查找与密钥相关的信息，这些可能是设备内部操作的时间或功率轨迹，或者是设备产生的错误输出。

侧信道攻击可分为以下几类：时间攻击、能量分析攻击、故障注入攻击等。其中，能量分析一直是主要攻击手段，其作用途径是：密码设备的功耗可以提供有关发生的操作和相关参数的大量信息，通过这些功耗信息可以获取与功耗相关的操作和数据信息。针对能量分析的防护手段主要是随机化和掩码[13]。对于不同类型密码系统，攻击点也有所不同。

## （二）挑战

PQC 解决方案的应用仍面临一些挑战。一是成本较高，PQC 解决方案目前仅占全球密码学市场的 2%左右，成本高于传统的密码学解决方案，初创企业很难获得深度渗透和规模效应。二是难以测试，由于 PQC 解决方案仍处于新生状

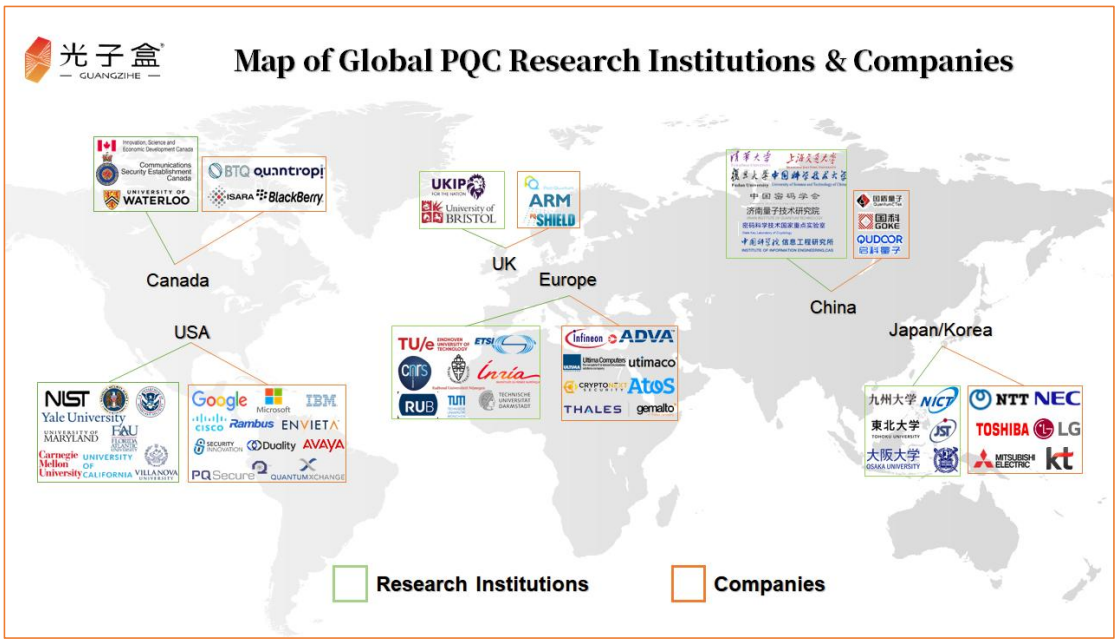
[13] BartheG，BelaïdS，EspitauT，FouquePA，GrégoireB，RossiM，TibouchiM.MaskingtheGLPlattice-basedsignatureschemeatanyorder.In：NielsenJB，RijmenV.Proc.oftheAdvancesinCryptology—EUROCRYPT2018.Cham：SpringerInt'lPublishing，2018.354–384.

态，无法量子计算机上进行测试，因此尚不能最终证明它们确实可以提供免受量子甚至传统威胁的保护。三是计算能力和延迟时间的高要求，与现有标准相比，目前可用的 PQC 解决方案需要显著的额外计算能力和更高的延迟时间。虽然，目前的 PQC 解决方案可能足以满足延迟要求较低的应用程序，例如非紧急、简单的银行转账或保险合同的转让。但对于运行高价值边缘计算和云计算应用程序（需要大量数据在本地节点和分散的计算能力来源之间快速流动）的相关主体，目前的 PQC 解决方案难以应用。

# 五、全球竞争与应对

目前，全球已有众多国家关注未来量子攻击对网络安全的潜在威胁，也已采取必要的行动和相关部署以应对此威胁。PQC 涉及到密码体系的建立，即标准化的建立，因此，越来越多的国际参与者加入到研究中，但在激烈的竞争中，也体现出各国应对潜在信息安全危机的态度。投资者对信息安全行业和量子计算行业的兴趣不断增加是市场扩张的主要原因。目前，PQC 全球最具实力的市场参与者主要分布在北美和欧洲，例如，北美的公司有 Google（美国）、IBM（美国）、Microsoft（美国）、PQSecure（美国）、Cisco（美国）、Envieta（美国）、ISARA（加拿大）、Quantropi（加拿大）等，欧洲的公司有 PQShield（英国）、Infineon（德国）、Thales（法国）、CrypotoNext（法国）、Gemalto（荷兰，2019 年被 Thales 收购）等。这些公司是提供芯片设计、数字信息安全和量子安全综合解决方案这三大类服务的科技企业。此外，还有一些顶尖大学和研究院所参与 PQC 研究，例如，慕尼黑工业大学（德国）、佛罗里达大西洋大学（美国）、清华大学（中国）。

图 3 全球后量子密码学市场的主要参与者




以下选取了几个具有代表性的国家或地区，阐述其 PQC 的简要发展情况：

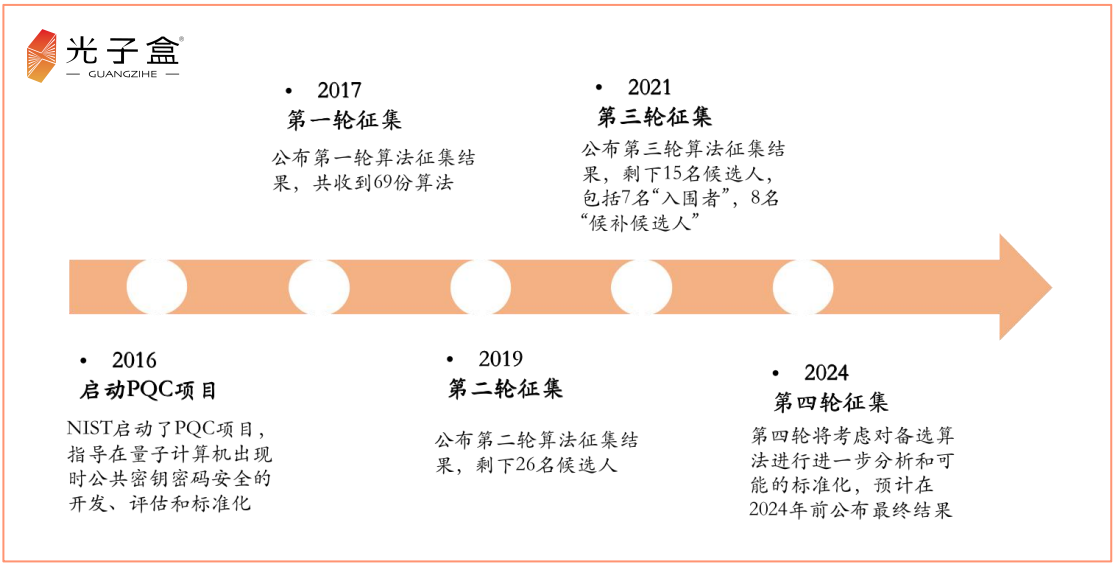
## （一）美国

### 1.NIST 开展新一代公钥密码算法征集

2016 年 4 月，Report on Post-Quantum Cryptography（NISTIR 8105）发布，标志着 NIST 开始启动 PQC 项目，正式在全球范围征集 PQC 标准协议。评估工作分为三轮进行，每轮 18 个月左右，预计 2024 年前完成。

2017 年 12 月，NIST 公布后量子密码学标准协议的第一轮预选协议。2019 年 1 月，NIST 再次发布第二轮的标准方案，从第一轮标准方案以及最新研究成果中遴选出 26 个进入第二轮，其中包括 17 个公钥加密和密钥交换方案及 9 个数字签名方案。26 个候选算法中包括 12 个格密码，7 个基于编码的密码，4 个多变量密码，2 个基于散列（分组码）的密码，1 个同源密码。2021 年 1 月，NIST 公布的第三轮的 7 个决赛方案和 8 个备选方案，包括数字签名和公钥加密。

图 4 NIST-PQC 项目时间线




在 NIST 公布的 7 个决赛方案中，有 5 个为格密码，这说明当前格密码占据较大的优势，是未来最有望标准化的算法。

表 6 NIST 公布的第三轮决赛方案

| 方案名称 | 安全假设 | 方案类型 | 技术路线 |
|---|---|---|---|
| 经典 McEliece | McEliece 假设 | 公钥加密 | 编码密码 |

| | | | |
|---|---|---|---|
| CRYSTALS-KYBER | M-LWE 假设 | 公钥加密 | 格密码 |
| NTRU | NTRU 假设 | 公钥加密 | 格密码 |
| SABER | M-LWR 假设 | 公钥加密 | 格密码 |
| CRYSTALS-DILITHIUM | M-LWE/SIS 假设 | 数字签名 | 格密码 |
| Falcon | NTRU/M-SIS 假设 | 数字签名 | 格密码 |
| Rainbow | MQ 假设 | 数字签名 | 多变量密码 |

来源：光子盒研究院

决赛方案主要是通用算法，在很大程度上是可以得到广泛的应用。备选方案虽然应用可能性不大，但这些算法仍有希望被标准化。

表 7 NIST 公布的第三轮备选方案

| 方案名称 | 安全假设 | 方案类型 |
|---|---|---|
| BIKE | QC-MDPC 假设 | 公钥加密 |
| FrodoKEM | LWE 假设 | 公钥加密 |
| HQC | c-QCSD 假设 | 公钥加密 |
| NTRUPrime | QuotientNTRU 假设 | 公钥加密 |
| SIKE | SIDH 假设 | 公钥加密 |
| GeMSS | MQ 假设 | 数字签名 |
| Picnic | 哈希函数+LowMC | 数字签名 |
| SPHINCS+ | 哈希函数 | 数字签名 |

来源：光子盒研究院

目前，第三轮已经进入尾声，但一些算法仍需进一步研究，NIST 第四轮会议讨论是否还有其他算法需要标准化，预计最终标准将在 2024 年前公布。

### 2.美国将抗量子算法纳入国家安全备忘录

2022 年 1 月，美国总统签署了关于提高国家安全、国防部和情报社区系统网络安全的备忘录（Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems）[14]，该文件是国家安全机构在当前的联邦网络安全计划中，首个特别提到抗量子算法（Quantum Resistant Algorithms）的文件，并指示美国国家安全局应当向公司首

[14] https://www.reuters.com/world/us/biden-administration-sets-new-requirements-us-secure-networks-2022-01-19/

席信息官发布任何与“后量子协议以及必要时计划使用后量子密码”相关的文件。2022 年 5 月，美国总统又签署了关于促进美国在量子计算领域的领导地位同时降低易受攻击的密码系统风险的国家安全备忘录（National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems），该文件启动了联邦政府与私营部门之间的合作，指示 NIST 在国家网络安全卓越中心建立一个“后量子密码技术迁移项目”，并与业界建立一个开放的工作组，对量子弹性密码标准和技术进行研究。同时，该备忘录为联邦机构设定更新密码系统的要求，考虑到完全过渡到抗量子加密标准过程复杂性以及时间等成本，备忘录中提供了 IT 系统建设路线图，帮助联邦机构有效保护网络[15]。

### 3.后量子迁移受到美国政府重视，并发布过渡路线图

2021 年 8 月，国家标准技术研究院国家网络安全卓越中心（NIST NCCoE）正式启动 PQC 迁移工程。2021 年 10 月，DHS 与 NIST 合作发布了应对量子技术风险的路线图[16]，旨在帮助企业保护其数据和系统，降低量子技术发展相关的风险。

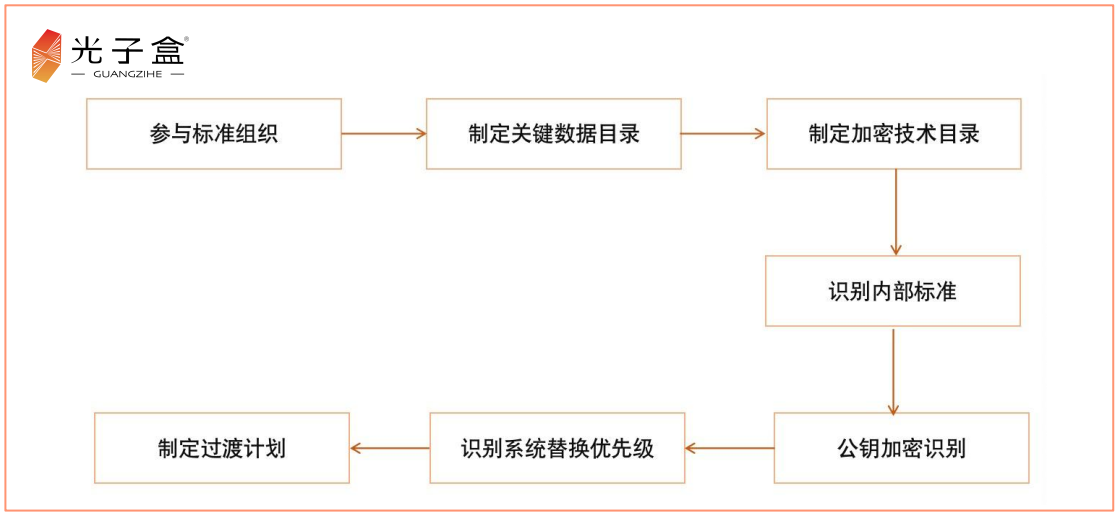
图 5 DHS&NIST 合作发布“应对量子技术风险的路线图”


来源：Preparing for Post-Quantum Cryptography: Infographic、光子盒研究院

NIST 发布的“应对量子技术风险的路线图”中，详细阐述了七个步骤指导企业开展 PQC 迁移工作。

[15] https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/fact-sheet-president-biden-announces-two-presidential-directives-advancing-quantum-technologies/
[16] https://www.dhs.gov/publication/preparing-post-quantum-cryptography-infographic

图 6 “应对量子技术风险的路线图”的七个步骤




来源：Preparing for Post-Quantum Cryptography: Infographic、光子盒研究院

**4.国家科学基金会为包括后量子安全在内的下一代技术投资**

NSF 将投资超过 3700 万美元用于下一代网络和计算机系统的学术研究[17]。例如，耶鲁大学[18]和卡内基梅隆大学[19]研究的“后量子密码学的硬件体系结构”，以及 PQSECURE 的“资源受限设备中的后量子加密”[20]获得了 NSF 的补助金。佛罗里达大西洋大学研究的“大规模系统的后量子密码学”和“智能手持嵌入式设备上的抗量子算法的设计、实现和分析”[21]获得了 NSF 的资金支持。

**5.美国科技巨头已开展 PQC 研究及应用测试**

Microsoft（微软）、Google（谷歌）、IBM 是美国乃至全球信息科技巨头，以下为这三家公司开展的 PQC 相关研究情况：

微软参与了 FrodoKEM、SIKE、Picnic、qTESLA 这四个用于签名和密钥交互的 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。此外，微软还发布了基于格密码库（LatticeCrypto）和项目 PQCrypto-VPN，并在 OpenVPN 中实现了 PQC 算法，可在 VPN 中测试 PQC 算法的功能和性能。微软研究院与许多科技公司、大学以及研究机构进行后量子密码学合作，共同开发

[17] https://www.fedscoop.com/nsf-partnership-next-gen-networks/
[18] https://www.nsf.gov/awardsearch/showAward?AWD_ID=1716541&HistoricalAwards=false
[19] https://www.nsf.gov/awardsearch/showAward?AWD_ID=1717146
[20] https://www.nsf.gov/awardsearch/showAward?AWD_ID=1853095&HistoricalAwards=false
[21] https://www.nsf.gov/awardsearch/showAward?AWD_ID=1661557&HistoricalAwards=false

了 Supersingular Isogeny Key Encapsulation（SIKE）密钥交换协议的后量子密钥封装机制。此外，微软研究院与许多科技公司、大学以及研究机构进行合作，共同开发了 qTESLA 后量子数字签名方案，其安全性基于带错误的决策环学习（R-LWE）问题的硬度。

谷歌于 2016 年宣布涉足 PQC，在 Chrome 浏览器的 Canary 测试版本中使用名为 New Hope 的后量子密钥交换算法的实验。开展后量子密码技术的测试活动，开始应用基于环上带误差学习问题密钥交换协议“新希望”。2019 年 1 月，谷歌宣布将部署一种新的 TLS 密钥交换方法，称为 CECPQ2（组合椭圆曲线和后量子密钥交换）。2019 年 6 月，谷歌和 Cloudflare 合作探索 PQC 如何在实践中击败 HTTPS 连接。此外，谷歌母公司 Alphabet 剥离出来的量子技术开发部门成立了初创公司 SandboxAQ，其主要研究目标之一是创建后量子密码系统和相关的隐私增强技术。

IBM Research 于 2019 年联合一些大学开发了新的量子安全算法，作为 CRYSTALS 格密码学套件的一部分，该算法已开源，并将其提交给 NIST 进行标准化。同年，IBM 已在 IBM TS1160 磁带驱动器原型上成功测试了 CRYSTALS，该原型使用 Kyber 和 Dilithium 并结合对称 AES-256 加密，以实现世界上第一个量子计算安全磁带驱动器。2022 年 4 月，IBM 发布首个量子安全系统—IBMz16，该系统基于格密码理论来研发并优化加密算法和数字签名技术。

## （二）英国

**后量子加密产品及技术服务需求显现，相关企业已展开测试及应用**

PQShield 公司在 2022 年 1 月获得 2000 万美元的 A 轮融资。公司目前产品有 PQSoC（嵌入式设备的后量子加密硬件）、PQSlib（嵌入式设备的后量子加密固件）、PQSDK（用于移动喝服务器技术的加密 SDK）、PQE2E（消息平台喝应用程序的加密解决方案），面对的市场主要为关键基础设施、物联网、OEM 行业。

Post-Quantum Solution 公司自 2009 年进行 PQC 相关深入研发，公司目前产

品为 PQ Chat、Hybrid PQ VPN、Nomidio Identity，针对的主要行业有银行与金融服务、国防与国家安全、关键国家基础设施。2022 年，北约网络安全中心（NCSC）使用了 Post-Quantum 提供的虚拟专用网络（VPN）进行了安全通信流的测试。

## （三）中国

### 1.中国涉足 PQC 研究，并参与 NIST 的 PQC 算法征集

中国目前开展 PQC 研究的单位有两大类，一类是偏数学算法方面的，例如清华大学、复旦大学、上海交通大学等；另一类是偏硬件融合的，例如中国科学技术大学、国盾量子、启科量子等。

NIST-PQC 算法征集中，中国后选团队是偏数学算法方面的，具体情况如下：

表 8 NIST-PQC 项目中的中国候选算法

| 算法 | 所在机构/单位 | 团队/个人 |
|---|---|---|
| Lepton | 密码科学技术国家重点实验室 | 张江 |
| KCL | 复旦大学 | 赵运磊、金正中、巩博儒 |
| LAC | 中国科学院信息工程研究所<br>信息安全国家重点实验室 | 路献辉、刘亚敏、贾仃仃、<br>薛海洋、贺婧楠 |
| | Algorand[22] | 张振飞 |

来源：NIST、光子盒研究院

### 2.中国展开“QKD+PQC”融合应用验证

中国科学技术大学、国盾量子、国科量子、济南量子技术研究院与上海交大等单位组成的联合团队完成了国际首次 QKD 和 PQC 融合可用性的现网验证。该研究证明了“PQC+QKD”的融合方案能够有效适应规模网络的交互通信条件，在实际应用中具有可行性，为 QKD 设备大规模认证提供了一种便利的新型手段。

### 3.中国设计出通用型 PQC 硬件架构

清华大学的科研团队提出一种低计算复杂度的快速数论转换与逆变换方法

[22] Algorand 是一家领先的区块链技术公司，由图灵奖得主、密码学先驱 Silvio Micali 教授创建

[23]，设计了一款具有普适的通用性的后量子密码硬件架构，能降低一类基于格的后量子密码算法的计算复杂度，还能在提高算法执行速度的同时减少了硬件资源开销。实验结果表明，与最先进的方法相比，该设计在计算速度上快了 2.5 倍以上，同时面积延时积（ATP）减小了 4.9 倍。

**4.中国开展后量子密码标准征集工作**

中国在后量子密码标准的征集方面也做了不少工作。但中国目前尚未向全球征集密码算法。自 2019 年，中国密码学会开始举办后量子密码算法竞赛的征集，至今连续举办三次。该项密码竞赛仅面向中国的密码学者。这场竞赛是中国在后量子密码算法标准制定的预赛，意味着中国也开始了后量子密码标准的制定征程。

## （四）欧洲

**1.欧洲深度参与 NIST-PQC 算法征集**

欧洲研究团队为 NIST-PQC 算法征集的贡献了最多的来源，在 NIST 发布的第二轮 26 个标准方案中，欧洲主导和参与的达 20 多个。除欧洲、美国、加拿大之外，其他进入第二轮的仅有中国科学院数据与通信保护研究教育中心设计的 LAC 算法。

**2.欧盟启动 PQCrypto & SafeCrypto 项目**

欧盟于 2015 年相继启动 SafeCRYPTO 和 PQCrypto 两个项目以应对纠错量子计算时代到来的潜在风险。PQCrypto 项目主要致力于后量子密码学研究，开发新的加密系统，研究了保护嵌入式设备（如手机、打印机等）防止黑客入侵的方法，并把高安全性的后量子加密技术集成到互联网中。同时，该项目还研究了云服务加密，可为存储在云服务中的文件提供 50 年的保护。PQCrypto 开发的算法服务于 Google 的服务器。PQCrypto 项目总预算近 400 万欧元，参与国家和地区

[23] 相关论文发表在《采用低复杂度快速数论变换和逆变换技术在 FPGA 上高效实现 NewHope-NIST 算法的硬件架构》

包括荷兰、比利时、丹麦、法国、德国、以色列和中国台湾。SafeCrypto 项目则聚焦格问题，将格问题作为计算难度的来源开发新的公钥加密方案。

**3.欧洲在后量子加密芯片和密钥交换方案上取得重要成果**

2021 年，慕尼黑工业大学研究人员已开发出实现后量子密码学的芯片，并展示其阻止黑客使用量子计算机解密通信的能力。该芯片是首个完全基于硬件/软件协同设计方法的后量子密码设备。与完全基于软件解决方案的芯片相比，使用 Kyber（PQC 最有希望的候选者之一）加密时的速度大约快 10 倍，其使用的能量大约减少 8 倍，并且几乎同样灵活。该芯片包含的专门设计的硬件加速器，不仅支持如 Kyber 等基于格的后量子密码算法，还可以与需要更多计算能力的 SIKE 算法配合使用。德国公司英飞凌在安全 IC 上的量子抗加密和认证能力处于领先地位，在一种商用非接触式智能卡芯片上成功实施一种后量子密钥交换方案。法国公司 Thales 在开发抗量子密码解决方案的竞赛中快速起步，参与了法国和欧洲的多个研究项目。目前公司已经开发了用于后量子加密的 Thales 公司 TCT CRYPTO 敏捷解决方案，具备快速修改底层加密原语的能力与灵活的可升级技术，使用户能够通过在其基础设施中使用经典加密和抗量子加密的混合方法。

## （五）日韩

**1.日本推出 CREST 密码数学项目**

JST CREST 项目“下一代密码学数学建模”专注于为下一代加密系统的数学建模奠定基础，从而解决密码分析的最新进展带来的风险，特别是量子计算和对加密设备的物理攻击（例如，功率分析）。CREST 项目每年举办后量子安全相关会议，已成为日本后量子密码学研究者的重要成果交流平台。

**2.日本参与 NIST-PQC 算法征集**

在 NIST-PQC 算法征集中，中国参与 NIST 的后量子密码标准征集工作主要有以下研究团队：

表 9 NIST-PQC 项目第三轮的日本参与者

| 算法 | 所属机构/单位 | 团队/个人 |
|---|---|---|
| NTRU | 日本电报电话公司 | T.Saito，K.Xagawa，T.Yamakawa |
| Classic McEliece | 大阪大学 | T.Chou |

来源：NIST，光子盒研究院

**3.日本密码研究与评估委员会（CRYPTREC）进行 PQC 过渡**

CRYPTREC 列出三个密码清单，分别是电子政务推荐密码清单、候选推荐密码清单、监控密码清单。其中，电子政务推荐密码清单中，PQC 未被罗列其中，但他们将启动 WG 制定的 PQC 指南。因此，PQC 不在列表中，但在指南中。

**4.日本在软硬件中实现 PQC 物理安全性研究**

NTT 社会信息学实验室（高级研究员 Keita Xagawa 和高级研究员 Junko Takahashi）和东北大学联合研究在软件和硬件中实现 PQC 的物理安全性。结果表明 NIST 国际标准的九分之八的公钥加密候选者具有物理漏洞。该团队对此进行了实验，以评估使用此漏洞盗窃解密密钥等攻击的可行性。此外，该团队制定并验证了实施措施，以防止这些脆弱性。

**5.韩国推出全球首个后量子密码专线**

韩国移动运营商 LG Uplus（LGU+）于 2022 年推出韩国首个 PQC 商业服务，可防御对量子计算机的黑客攻击，这也是世界上第一个后量子密码专线服务。目前，该线路已经过电信技术协会（TTA）的测试和验证。

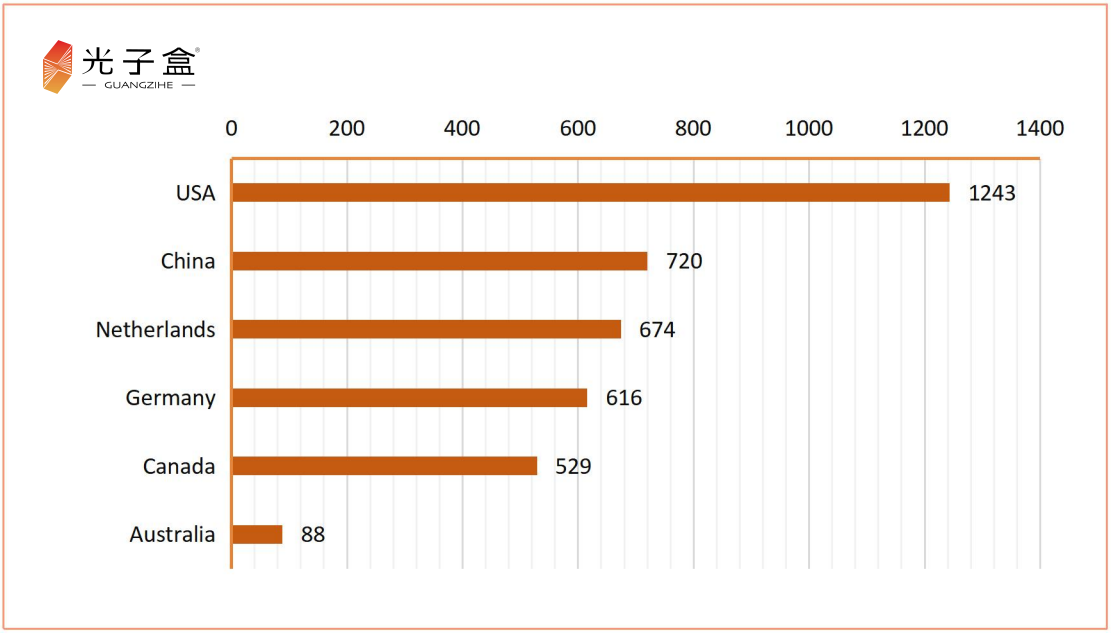
## （六）国际比较

**1.研究影响（RI）**

根据澳大利亚的关键技术政策协调办公室（CTPCO）发布的数据，美国在 PQC 方面的研究影响力最高，其次是中国。已发表研究的总量以每年 33%左右

的速度增长。在 2016-2020 年，31%的研究涉及国际合作。

图 7 2016-2020 年 PQC 相关出版物数量总和



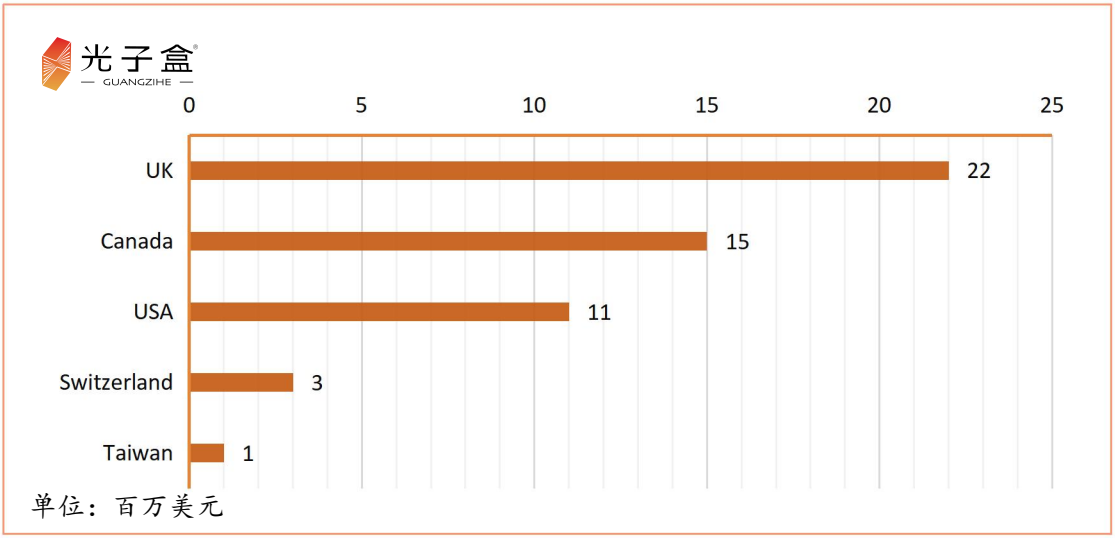

注：研究影响提供了一个国家或机构生产力的指标。在这里，生产力被假设为以出版物数量作为学术产出的指标。

数据来源：CTPCO

**2.风险投资**

根据 Crunchbase 发布的统计数据，英国在 2016-2020 年间的 PQC 方面获得的风险投资额最高，领先于加拿大和美国。2016-2020 年，全球风险投资对后量子密码学的投资增长了约 37%。

图 8 2016-2020 年 PQC 相关风险投资综合

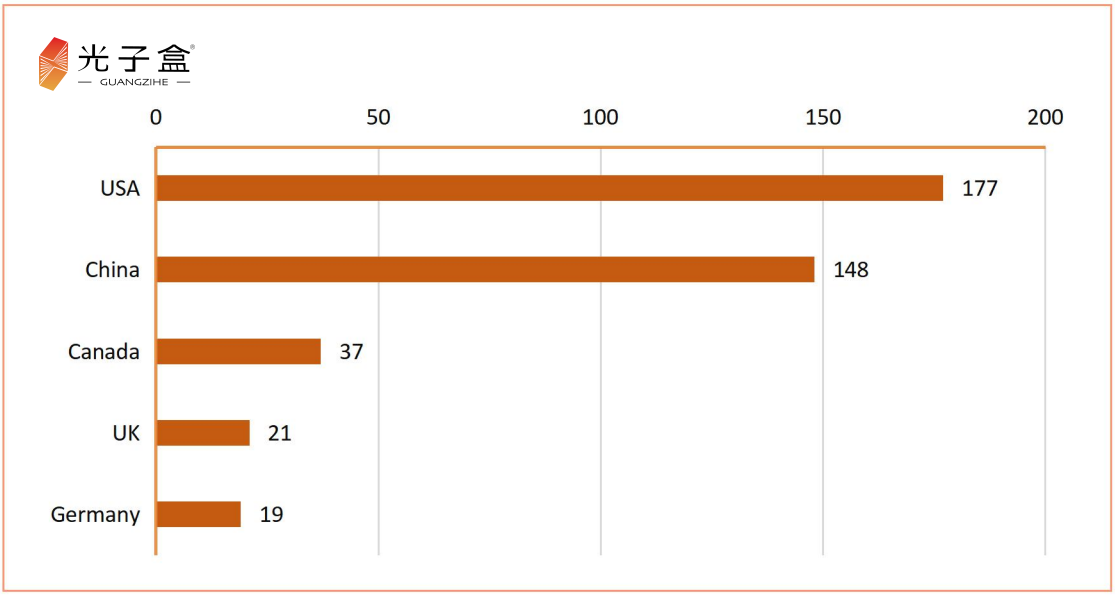


数据来源：Crunchbase

**3.技术专利**

2016-2020 年，PQC 领域的大部分专利是由美国的申请人或发明人申请的，其次是中国。2016 年-2020 年，总体专利申请以每年 40%的速度增长。

图 9 2016-2020 年 PQC 相关专利数量总和




数据来源：CTPCO

## （七）小结

世界许多主要国家都已意识到量子计算对信息安全领域带来的潜在威胁，诸多科技大国已开展 PQC 研究。其中，欧洲、美国、中国、日本等国家和地区的研究程度较深。美国在 PQC 方面处于领先地位，拥有最大的后量子生态系统。但欧洲也有机会成为全球领导者，在七名 NIST 决赛“选手”中，除一个外，其他加密系统都有大多数欧洲科学家参与其开发。欧洲在后量子密码算法方面的策略是全力配合美国 NIST 的算法征集，并基于 NIST 的算法推动后量子密码迁移工作，若能抓住 PQC 人才及团队优势，极有可能实现后量子密码技术的全球超越。

# 六、PQC 发展趋势预测

## （一）PQC 逐步向全同态加密等更高级应用演变

目前 NIST 等机构正在标准化的 PQC 算法仅包括公钥加密和数字签名等常见的密码算法，这些算法已趋于成熟，优化改进的空间较小。但其实基于格困难问题不仅能用于公钥加密和数字签名，还能构造全同态加密（Fully Homomorphic Encryption/FHE）、不可区分混淆等高级密码算法。其中，能支持任意计算操作的同态加密被称为全同态加密。传统加密算法只能保护数据在存储和传输过程中的静态安全性。数据加密后，对密文能做的唯一有效操作是解密。同态加密允许在没有解密密钥的情况下对密文进行有意义的计算操作，最终输出加密的计算结果，整个计算过程不泄露原始数据和计算结果的任何有效信息。同态加密已取得较大进步，逐步从理论走向应用，目前几乎所有的全同态加密都是基于格困难问题。随着 PQC 技术不断发展，同态加密这一更高级别的密码学应用有望逐步实现。

## （二）公钥密码系统向 PQC 系统过渡仍有很大困难

当前，为了抵御对传统计算的攻击，NIST 已建议从提供 80 位安全性的密钥大小和算法过渡到提供 112 位或 128 位安全性的密钥大小和算法。而为了提供抵御量子攻击的安全性，未来还需要进行一个过渡，即把公钥密码系统过渡到新的 PQC 系统。为了应对未来量子计算机攻击的出现，新的 PQC 算法有望成为未来全球加密与数字签名新标准。为此，PQC 算法也要融合多领域密码知识，包括编码密码、网格密码、多变量密码、散列密码，以及超通用椭圆曲线同源密码等。此外，标准的完善及实际应用普及也会对过渡进程产生影响。因此，公钥密码系统向 PQC 系统过渡这一实现过程仍有许多问题亟待解决。

## （三）短期内仍以多种密码体系混搭为主

经典密码无法抵抗全面纠错量子计算机的威胁，量子密码（如 QKD）面临技术与工程方面、标准与认证、成本与应用等方面的挑战。PQC 面临的困难也在于成本和应用。要想替换 RSA 等已经非常成熟和应用普及的密码体系，新的密码体系应用的成本必需大幅度下降。同时，具备密码敏捷性以增强应用场景的广泛性。考虑到这些问题，很可能未来能够大规模应用的 PQC 技术，要与传统安全密码技术结合起来，形成一种“混搭”模式以适用更多的需求。此外，QKD 与 PQC 可以应用在不同场景，各有利弊，相互补充。QKD 偏重于高价值、高安全等级资产（如骨干网）的保护，PQC 则可以像 RSA 一样，普及应用在现有的信息基础设施各个方面。

## （四）金融机构将加快 PQC 评估和相关部署

量子计算机有潜力改变现有的金融系统，因为它们可以比最强大的经典计算机更快、更准确地解决许多问题。但量子计算这一双刃剑也会带来前所未有的威胁。金融机构因其加密货币、比特币等可为黑客带来巨额获益而更可能面临网络安全挑战。因此，金融机构相比于其他行业，可能会更早地采取相应的措施为新的加密系统过渡做准备，需要全面评估量子计算机的未来和追溯风险，清点金融机构加密算法（尤其是公钥），建立加密敏捷性，以提高金融机构整体网络安全弹性。

## （五）企业将是推动 PQC 落地的主要力量

新的密码体系的成熟离不开不断地与各行各业进行测试应用。在 PQC 应用方面，企业能够通过新型密码产品的商业化推广使用活动，不断积累和分析用户数据，促进 PQC 系统安全性能和运行效应的提升，推动密码企业与垂直行业相关用户供需对接和技术攻关，促进 PQC 应用适配研发，推动研制实用性高的 PQC 密码产品及服务，持续推动 PQC 应用相关测试验证服务优化、创新。

## （六）与 PQC 配套的硬件市场增长有望，更多芯片及安全公司入局

PQC 的重点发展方向在算法方面，但依然离不开一些硬件的辅助实现。对于一些嵌入式系统，搭配硬件的实现方法是一种有效的安全解决方案。目前，已经有一些企业使用 ASIC 芯片或 FPGA 来实现算法，例如，英飞凌已开发了一种实现 NewHope 算法的非接触式智能卡芯片，Utimaco 公司（德国）硬件安全模块（HSM）可使用户能够生成加密密钥并将其安全存储。许多顶尖芯片设计公司、网络信息安全解决方案公司已经将 PQC 列入公司业务的重要发展方向之一。因此，预计在 PQC 的硬件实现市场上，将会有较为乐观的增长潜力和发展前景。

# 关于我们

光子盒
GUANGZIHE

光子盒（GUANGZIHE）创立于 2020 年 2 月，名称来自于在 1930 年第六届索尔维会议（Solvay Conference）上，爱因斯坦（Albert Einstein）在其与玻尔（Niels Bohr）的争论（Bohr-Einstein debate）中提出的一项光子盒实验（photon box experiment）。

光子盒定位为量子科技产业服务平台，通过推送量子科技前沿新闻、科普量子知识、解读量子技术、发布年度和专题报告等形式，致力成为中国量子科技产业最值得信赖的服务机构。截至 2022 年 5 月，光子盒已公开发布了 40 余份量子科技领域的专题报告，并且为 10 余家中国量子科技领军企业提供量子行业咨询和数据服务等。

2021 年 5 月，光子盒作为协办方，与主办方中国电子科技集团公司电子科学研究院、社会安全风险感知与防控大数据应用国家工程实验室和中国工程科技发展战略安徽研究院，在安徽合肥成功举办了“2021 中国量子科技产业‘双循环’高峰论坛”。

光子盒正在不断扩充自有量子科技产业数据库的广度与深度，建立多维量子产业数据信息，提供客观、专业、深入及具有时效性的量子行业报道与咨询服务。光子盒未来还将承办量子科技领域的论坛，提供更为丰富的主题和内容，联合量子产业科技公司、金融行业投资公司、国家/省级量子相关科研院所、政策战略研究单位等共同促进量子产业持续向好发展。

# 联系我们

**如您有任何问题，欢迎咨询光子盒**

**请发送邮件至：gzh.marketing@quantumchina.com**

**更多精彩内容，请关注：**

光子盒官网

光子盒微信公众号

量子通信&安全系列报告

光子盒
GUANGZIHE
专注量子领域的咨询机构
WWW.QUANTUMCHINA.COM

# 后量子密码（PQC）
# ——未来安全的风暴热点