后量子时代数据加密安全方案研究

Research on Data Encryption Security Schemes in Post-Quantum Era

黄建康，侯玉华，齐　霄，田　嘉（中讯邮电咨询设计院有限公司，北京 100048）
Huang Jiankang, Hou Yuhua, Qi Xiao, Tian Jia (China Information Technology Designing & Consulting Institute Co., Ltd., Beijing 100048, China)

摘　要：
首先以量子技术和量子计算机发展为背景介绍了后量子时代现有密码体系的安全性问题，然后对量子密钥分发和抗量子加密算法2种技术方案进行分析。最后提出基于目前技术现状以及未来发展趋势的后量子安全方案演进升级路线，包括量子密钥分发与抗量子加密融合、国密与抗量子算法融合等。同时针对一些典型场景进行详细的分析介绍，包括车辆网系统中身份认证和移动支付身份认证协议的后量子安全升级方案。

关键词：
抗量子；QKD；身份认证；数据安全
doi：10.12045/j.issn.1007-3043.2025.10.007
文章编号：1007-3043（2025）10-0036-06
中图分类号：TN914
文献标识码：A
开放科学（资源服务）标识码（OSID）：

Abstract:
Firstly, based on the background of the development of quantum technology and quantum computers, the security issues of the existing cryptographic systems in the post-quantum era are introduced. Then, two technical solutions, namely QKD and PQC are analyzed. Finally, a roadmap for the evolution and upgrading of quantum security solutions based on current technological status and future development trends is proposed, including the integration of QKD and PQC, as well as the integration of national encryption and quantum-resistant algorithms, etc. In addition, it conducts detailed analysis and introduction for some typical scenarios, including the post-quantum security upgrade schemes for identity authentication and mobile payment identity authentication protocols in the vehicle network system.

Keywords:
PQC; QKD; Identity authentication; Data security

引用格式：黄建康，侯玉华，齐霄，等. 后量子时代数据加密安全方案研究[J]. 邮电设计技术，2025（10）：36-41.

0 引言

量子计算技术的迅猛发展正在对传统密码学体系构成前所未有的威胁。根据Shor算法原理，量子计算机能够在多项式时间内破解广泛使用的RSA、Diffie-Hellman和椭圆曲线密码体制（ECC），这使得当前保护数字通信的大多数加密方法面临失效风险[1]。Grover算法则将对对称密钥加密的攻击复杂度从O（2^n）降低到O（$2^{n/2}$），进一步削弱了传统加密的安全性。面对这种迫在眉睫的威胁，全球密码学界提出了2种主要应对策略：基于量子物理原理的量子密钥分发（QKD）和基于数学难题的抗量子密码算法（PQC）[2]。

本文将分析量子计算背景下数据安全方案的演进路径，对比量子密钥分发和抗量子密码算法2种技术路线的优劣与适用场景，重点探讨抗量子密码算法与现有加解密算法及CA证书体系、TLS协议等融合方案及实现平滑迁移的策略建议，最后介绍了在私有协议和定制化场景中可以更快实现PQC安全升级的方案以及典型案例。

1 后量子安全技术原理与发展现状

1.1 量子密钥分发（QKD）

收稿日期：2025-08-01

量子密钥分发（QKD）是一种基于量子力学原理的安全通信方法，它利用量子态的特性来检测窃听行为，从而保证密钥分发的安全性。QKD的核心原理是量子不可克隆定理和海森堡测不准原理：前者确保任何未知量子态无法被完美复制，后者则保证任何测量量子系统的行为都会扰动系统状态。这意味着一旦有窃听者试图拦截量子信道，通信双方就能够通过误差率分析检测到窃听行为。

目前主流的QKD技术主要包括基于光纤的连续变量QKD和基于自由空间的离散变量QKD。光纤QKD适合城市范围内的安全通信，而自由空间QKD则为星地量子通信提供了可能性。近年来，QKD技术取得了显著进展，研究人员成功实现了一定规模的纠缠光子分发，将偏振纠缠光子对通过光纤和自由空间光学链路组合分布到三节点网络中。我国在QKD技术的研究、标准制定和产业化方面都处于国际领先水平[3]。

QKD技术已经在多个领域得到实际应用，特别是在高安全需求的场景中。然而，QKD技术也存在一些固有局限性。首先，它通常需要专用设备（如量子随机数生成器、单光子探测器和量子光源）和专用光纤链路，这导致部署成本较高；其次，QKD的传输距离受到限制，虽然通过中继器可以扩展范围，但中继器本身可能需要信任，这引入了潜在的安全风险；最后，QKD通常只保护密钥分发过程，而不是端到端的加密，数据加密仍然需要与传统加密算法结合使用。例如电信运营商的量子密话业务，依赖QKD的密钥分发只局限于特定量子网络专线，而终端设备只能依赖线下的密钥注入把分发的密钥注入到安全载体中[4]。

表1为主要QKD协议的比较。

1.2 抗量子密码算法（PQC）

抗量子密码算法（PQC）是通过数学方法构造能够抵抗量子计算攻击的密码算法，它不需要专门的量子设备，可以在现有数字基础设施上运行。PQC是基于那些被认为在经典计算机和量子计算机上都难以解决的数学难题构造的，主要包括格子密码、编码密码、多变量密码和哈希密码等几种类型。

表1　主要QKD协议的比较

协议名称	编码方式	最大传输距离	密钥速率	技术特点
BB84	偏振编码	100 km（光纤）	中等	第1个QKD协议，理论成熟
E91	纠缠编码	150 km（光纤）	较低	基于量子纠缠，安全性更高
CV-QKD	连续变量	80 km（光纤）	较高	使用标准光通信组件
TF-QKD	时间频率	400 km以上	中等	超长距离传输

后量子密码学也称为抗量子密码学，是指能够抵抗量子计算攻击的新一代密码算法。与量子密钥分发不同，PQC不需要专门的量子设备，而是在传统数字基础设施上运行，通过数学方式保障安全。美国国家标准与技术研究院（NIST）在2016年启动了PQC标准化项目，最终选定了CRYSTALS-Kyber用于密钥封装以及CRYSTALS-Dilithium用于数字签名。这些算法基于被认为能够抵抗量子计算攻击的数学难题，为未来数据安全提供了坚实基础[5]。

PQC算法主要包括如下几种。

a）格密码（Lattice-based cryptography）。它是目前最受关注的PQC方向，基于格的最短向量问题（SVP）和最近向量问题（CVP）等难题。NIST选定的密钥封装机制（CRYSTALS-Kyber）和数字签名（CRYSTALS-Dilithium）算法均属于格密码。这类算法具有较短的密钥长度、较高的效率以及强大的安全证明，适合大多数应用场景。

b）编码密码（Code-based cryptography）。它是基于纠错码解码问题的困难性构造的，Classic McEliece是NIST选定的另一个密钥封装算法，其优势是已有数10年的抗密码分析历史，但主要缺点是公钥尺寸非常大（达到几MB），限制了其在某些场景的应用。

c）多变量密码（Multivariate cryptography）。它是基于多元多项式方程组的求解困难性构造的，可用于数字签名方案（如Rainbow）。然而，一些多变量密码算法已被攻破，其安全性需要被进一步评估。

d）哈希密码（Hash-based cryptography）。它是基于哈希函数的抗碰撞特性构造的，适用于数字签名（如SPHINCS+）。这类方案的安全性依赖于哈希函数的安全性，但签名尺寸较大，适合特殊应用场景。

NIST的PQC标准化工作始于2016年，经过多轮评估，NIST于2022年公布了第1批入选算法。2024年，NIST又公布了额外的签名算法方案。目前，NIST PQC标准主要包括[2]：

a）密钥封装机制：CRYSTALS-Kyber（主选算法）、Classic McEliece（备用算法）。

b）数字签名：CRYSTALS-Dilithium（主选算法）、Falcon（主选算法）、SPHINCS+（备用算法）。

值得注意的是，不同国家和地区可能采用不同的

PQC标准。我国也在积极推进自己的PQC标准制定工作，2024年在3GPP和CCSA已有相关标准立项。

1.3 QKD与PQC的对比分析：优势、劣势与适用场景

虽然QKD和PQC都旨在应对量子计算威胁，但它们在技术原理、安全假设和适用场景上存在显著差异。下面从多个维度对这2种技术进行对比分析。

QKD的安全性基于物理定律，如量子不可克隆定理和海森堡测不准原理，任何窃听行为都会引入可检测的扰动，从而保证密钥分发的安全。这种安全性是基于量子物理特性的安全，不依赖于攻击者的计算能力假设。然而，QKD的实际安全性受到设备缺陷和实施漏洞的影响，这可能被旁道攻击利用。

PQC的安全性基于数学难题的计算复杂性，即便使用量子计算机，解决某些数学问题也是计算上不可行的。这种安全性是计算安全，依赖于攻击者的计算能力假设。在最初公布的多种PQC算法中已经发现安全问题并删除其中一些算法，但其余算法是否存在尚未发现的安全漏洞仍是不可预知的。PQC的优势在于它提供端到端的安全性，而不仅仅是密钥分发的安全。

QKD需要专用设备和基础设施（如专用光纤链路），部署成本较高，适合点对点的高安全性通信场景。它主要用于高安全需求的环境，如政府通信、金融交易和电力基础设施保护。OTN量子加密专线就是一个典型例子。

PQC则可以通过软件或固件更新部署在现有数字设备上，无需专用硬件（尽管专用硬件可以提高性能），部署成本相对较低。PQC适用于大多数现有应用场景，包括TLS/SSL、VPN、数字签名、安全电子邮件等。特别是PQC可以轻松集成到现有公钥基础设施（PKI）中，支持大规模部署。

QKD与PQC技术对比如表2所示[6]。

表2　QKD与PQC技术对比

对比维度	量子密钥分发（QKD）	抗量子密码（PQC）
安全基础	物理定律	数学难题
安全性性质	量子物理特性安全	计算安全
保护范围	密钥分发	端到端安全
部署需求	专用设备与链路	软件/固件更新
部署成本	较高	较低
传输距离	受限（需中继）	无限制
标准化进度	国内CCSA、国际ITU-T	以NIST为主导
适用场景	高安全专线/专网	通用互联网应用

值得注意的是，QKD和PQC并不相互排斥，是可以互补和融合的。我国在积极推进QKD产业化的同时，也高度重视PQC标准的制定与产业应用。从长远来看，预计PQC会替代传统加密算法，将QKD与PQC技术融合，构建更全面的量子安全防护体系。

我国在QKD技术的研究、标准制定和产业化方面都处于国际领先水平。相关产品已经发布，产品布局也具备一定的规模，但由于技术设备等限制仍限于特定的高安领域。PQC技术标准的研究起步相对较晚，这也是近年发展的重点。而且PQC技术的应用会带来更广泛的影响，为整个互联网带来一次全面的安全升级。接下来本文重点介绍PQC技术在未来的发展与应用。

2 PQC与现有技术的融合方案

本章将从PQC与现有算法的融合策略入手，进一步探讨其在PKI体系中的集成方案，并以TLS协议为例说明如何实现平滑迁移。

2.1 PQC与现有算法标准的融合

当前NIST已经公布了PQC算法标准，我国也正在制定相关算法标准。但由于PQC算法本身的安全性及对现有密码系统中算法的替换升级或者兼容问题，现有算法与PQC算法的融合会是近期考虑的重点。

对于签名算法而言，可以同时保留2个算法，使用各自独立的签名密钥，签名过程也相互独立，这为不同算法的替换或者算法兼容带来很大便利。唯一不足之处在于签名过程的算力消耗相比现有单一签名算法会有成倍增加。但这也是为保证安全强度不可避免的问题。

图1所示为国密SM2和PQC算法融合签名方案示意。对于数据加密算法，算法融合问题会更加复杂。因为使用各自独立密钥加密后，一旦其中一种加密算法被破解，使用另一种加密算法加密的结果也就没有了意义。而使用双重加密，又无法抵抗简单的密文攻击。安全领域当前比较主流的方案是使用双重密钥因子生成加密密钥来保证数据加密的安全性[7]。

图2所示为使用国密SM2和PQC算法融合加密方案示意。这种混合加密方案虽然保证了密钥的安全性，但也存在无法和现有加密方式兼容的问题。而且同样在算法的算力消耗方面也会有成倍的增加。所以现在一些类似网关产品的加密协议升级时只对签名算法做了抗量子和融合升级。未来随着PQC标准

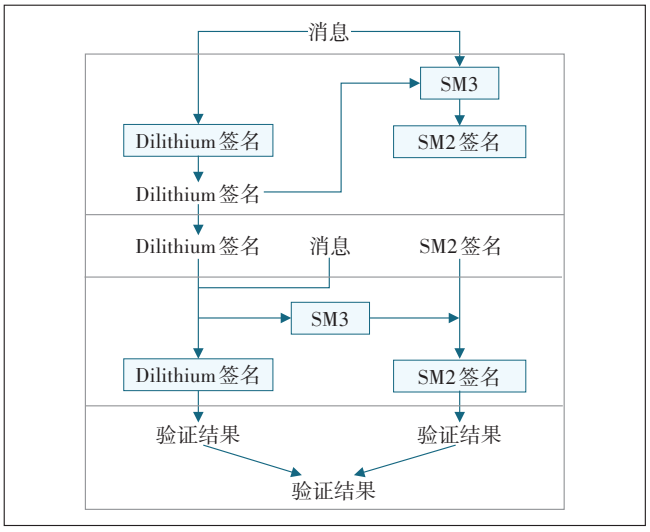

图1　国密SM2和PQC算法融合签名方案示意

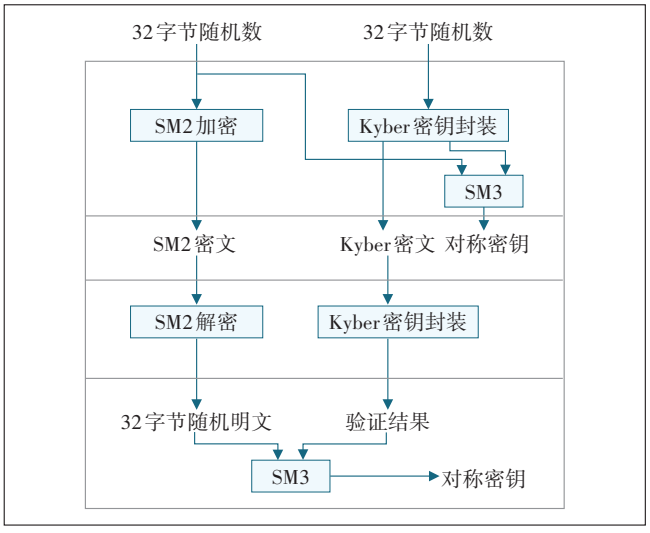

图2　所示为使用国密SM2和PQC算法融合加密方案示意

的发布，这一问题将得到一定程度的解决。

2.2 PQC与现有PKI体系的融合方案

公钥基础设施（PKI）作为现代互联网身份认证技术的基础，在众多通信协议中有着广泛的使用。随着后量子密码学的发展，如何将PQC整合到现有的数字证书体系和公钥基础设施（PKI）中成为一个关键问题。现有的CA证书体系基于传统密码算法（如RSA和ECC），需要平滑过渡到抗量子算法，同时保持向后兼容性[8]。

数字证书是PKI的核心组成部分，用于绑定实体身份与其公钥。目前将PQC集成到数字证书中有以下几种方式。

a）混合证书。同时包含传统公钥和PQC公钥，使用双重签名（传统签名和PQC签名）。这种方式确保了与旧系统的兼容性，同时提供了量子安全性。例如，证书可以同时包含RSA公钥和Dilithium公钥，并用2种算法分别生成签名。

b）PQC-only证书。只包含PQC公钥，仅使用PQC算法进行签名。这种方式提供了纯净的量子安全解决方案，但可能无法与不支持PQC的系统兼容。

c）证书链组合。使用PQC算法签发传统证书，或使用传统算法签发PQC证书，形成混合证书链。这种方式允许逐步迁移，不同部分可以在不同时间过渡到PQC。

为了平衡安全性和兼容性，许多组织建议采用双栈实施策略，即同时运行传统密码算法和PQC算法。例如，在TLS握手过程中，可以同时执行RSA和Kyber密钥交换。这种方法的优点是即使一种算法被攻破，系统仍然受到另一种算法的保护。同时，它允许根据客户能力逐步过渡，而不是强制突然切换[8]。

表3给出了混合证书格式示意。

表3　混合证书格式示意

字段	内容	说明
版本	v3	X.509证书版本
序列号	01:23:45:67	唯一标识符
签名算法	SHA256WithRSAandDilithium	混合签名算法
颁发者	CN=Example CA	证书颁发者标识
有效期	20250101-20251231	证书有效期
主体	CN=Example.com	证书主体标识
公钥信息	RSA-2048 + Kyber768	双公钥嵌入
扩展信息	基本约束、密钥用法等	标准X.509扩展
签名值	RSA签名 + Dilithium签名	双重签名

将PQC集成到现有PKI体系也面临诸多挑战。首先，算法敏捷性是关键要求，系统需要支持多种算法并能轻松替换算法。其次，性能考虑也很重要，因为许多PQC算法（尤其是签名算法）可能比传统算法更慢或产生更大的签名。这可能会影响证书验证速度和网络带宽。最后，标准与互操作性是成功集成的关键。不同厂商和组织可能需要时间来实现和支持相同的PQC标准。标准化工作有助于解决这个问题，但过渡期间可能会出现互操作性问题。

2.3 PQC在TLS协议中的集成方案

TLS（Transport Layer Security）传输层安全性协议是互联网上最重要的安全协议之一，诸多上层的安全协议如Https、sftp、VPN等都是基于TLS实现的。将

PQC集成到TLS协议中是后量子迁移的核心挑战之一[9]。

目前国际开源组织已经在这方面做了一些工作，在TLS 1.3协议中，可以通过多种方式集成PQC[10]。

a）混合密钥交换。结合传统密钥交换（如ECDHE）和PQC密钥交换（如Kyber），同时从两者派生共享密钥。即使其中一种算法被攻破，结合后的密钥仍然安全。NIST已经制定了混合模式的规范，确保其安全性和互操作性。

b）PQC签名算法。使用PQC签名算法（如Dilithium或Falcon）进行服务器身份验证。这需要服务器证书包含PQC公钥，并使用PQC算法进行签名。

c）双栈实现。客户端和服务器可以协商使用传统密码套件或PQC密码套件，取决于双方的支持能力。这种方案允许逐步部署，而不破坏与旧客户端的兼容性。

以下是一个混合TLS 1.3握手流程的示例，结合了传统算法和PQC算法。

a）ClientHello。客户端发送支持的算法列表，包括传统算法（如RSA-2048）和PQC算法（如Kyber512）。

b）ServerHello。服务器选择确认使用的算法组合。

c）密钥交换。执行混合密钥交换，结合传统算法和PQC算法。

d）会话密钥派生。使用HKDF从2个共享密钥（传统算法和PQC算法）派生会话密钥。

e）应用数据加密。使用派生出的会话密钥（如AES-256-GCM）加密通信数据。

这种混合方法确保了即使未来量子计算机攻破了传统算法，今天的通信仍然受到PQC算法的保护，防止“先收集后解密”（HNDL）攻击。

3 私有协议或定制化场景中的PQC应用

在后量子迁移过程中，私有协议和定制化场景相比公共互联网服务具有独特优势。如第2章所述PKI体系和TLS协议，它们的升级改造影响范围广泛，需要考虑对现有使用的升级兼容性，以及不同用户或设备的梯度升级等。但一些私有协议或者定制业务场景通常不必考虑这些问题，能够更快速地集成PQC解决方案。

3.1 私有协议或定制化部署场景的特点

私有协议或定制化部署场景（如仅在特定领域使用的私有协议、公司内部网络、工业控制系统）具有以下特点，使其更适合早期部署PQC。

a）可控的环境。组织对终端设备、网络基础设施和安全策略有完全控制权，可以统一部署PQC解决方案，而不需要担心与外部实体的互操作性问题。

b）定制化硬件。许多私有化场景已经使用专用安全设备（如硬件安全模块、密码卡），可以更容易地升级以支持PQC算法。

c）较高的安全需求。这些场景通常处理高价值资产或关键基础设施，有更强的动机尽早采用量子安全解决方案。

d）较少的兼容性约束。由于不面向公共互联网，这些场景可以更自由地选择算法和协议，不需要保持与大量外部实体的兼容性。

3.2 终端设备身份认证协议PQC算法升级

随着移动互联网的发展和普及，终端设备上各种身份认证也有许多成熟的解决方案。接下来以FIDO（Fast IDentity Online）协议为例，展示在FIDO身份认证过程中如何集成和使用PQC算法来实现后量子的安全升级。这很好地体现了在这些相对独立的协议中可以快速地完成PQC算法升级，而与此同时整个系统对接的其他相关服务无需做相应的调试，平滑地完成安全升级[11]。

图3所示为FIDO认证系统框架。

PQC算法集成升级方案的协议流程修改（以WebAuthn为例）如下。

a）注册（Attestation）阶段。

（a）客户端（浏览器/认证器）：在生成传统的ECC

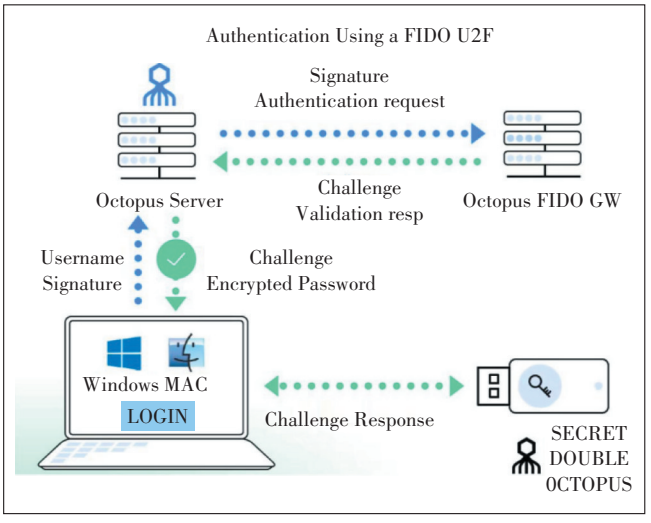

图3 FIDO认证系统框架

密钥对（sk_ecc，pk_ecc）的同时，也生成一个PQC密钥对（sk_pqc，pk_pqc）。认证器应支持PQC算法运算。

（b）客户端→服务端：在发出的attestation响应中，除了包含现有的attestationObject（内含pk_ecc和ECC签名），新增一个扩展字段（例如pqcAttestation），该字段包含pqcPublicKey（pk_pqc的编码）、pqcSignature〔使用sk_pqc对同一个挑战（challenge）和同一组客户端数据（clientDataJSON）生成的签名〕和使用的PQC算法标识符（OID）（可选字段）。

（c）服务端：像往常一样验证ECC的签名和挑战，同时使用收到的pk_pqc验证PQC签名和同一个挑战，仅当2个签名都验证成功时，注册才完成。服务端将用户的credentialId与2个公钥（pk_ecc和pk_pqc）关联存储。

b）认证（Assertion）阶段。

（a）客户端：在生成传统的ECC签名sig_ecc的同时，使用sk_pqc对同样的认证数据（authenticatorData）和客户端数据（clientDataJSON）生成第2个签名sig_pqc。

（b）客户端→服务端：在发出的assertion响应中，新增一个扩展字段（例如pqcAssertion），该字段包含pqcSignature（sig_pqc）和PQC算法标识符（可选字段）。

（c）服务端：根据credentialId查找对应的pk_ecc和pk_pqc，像往常一样使用pk_ecc验证sig_ecc，同时使用pk_pqc验证sig_pqc，仅当2个签名都验证成功时，认证才通过。

目前FIDO联盟组织已经制定了PQC算法的升级路线图，在PQC算法标准发布后可以启动算法升级。而对于一些私有化部署的系统，这部分工作可以更快地被完成。尤其当前很多金融类应用都使用了FIDO协议，它们对安全往往有更高的要求，也有更强烈的升级意愿。另外我国也有类似FIDO的身份认证协议，如腾讯牵头制定的SOTER协议或者IFFA组织制定的认证协议。相信随着我国PQC算法标准的发布，相关组织很快会发布升级计划。

4 总结

从长远来看，面对量子计算带来的安全威胁，QKD和PQC技术势必会融合，而不是作为孤立解决方案存在。国内QKD技术已经有了一定的积累沉淀，同时对PQC的研发投入也在逐步加大。结合物理安全性和数学安全性的混合方案，为不同场景提供最佳安全保证。

向后量子密码学的迁移不是可选而是必然。然而，这种迁移不是一夜之间能够完成的，而是需要精心规划和执行的多年度转型过程。同时后量子密码学的发展仍在进行中，算法可能会随着密码分析进展而演变。相关组织应持续关注标准发展，并适时调整其策略。通过谨慎规划、分阶段实施和持续监控，共同构建能够抵抗量子计算威胁的数字未来。

参考文献：

[1] MOSCA M. Cybersecurity in an era with quantum computers：will we be ready?[J]. IEEE Security & Privacy，2018，16(5)：38-41.

[2] CHEN L D，JORDAN S P，LIU Y K，et al. Report on post-quantum cryptography[EB/OL]. [2025-02-17]. https://www.nist.gov/publications/report-post-quantum-cryptography.

[3] 3GPP. Security architecture and procedures for 5G system：3GPP TS 33.501[S/OL]. [2025-02-17]. ftp://ftp.3gpp.org/Specs/.

[4] ZHANG L. Post-quantum cryptography for 5G networks[J]. IEEE Communications Magazine，2023，61(12)：32-38.

[5] National Institute of Standards and Technology (NIST). Post-quantum cryptography [EB/OL]. [2025-02-17]. https://csrc. nist.gov/projects/post-quantum-cryptography.

[6] PIRANDOLA S，ANDERSEN U L，BANCHI L，et al. Advances in quantum cryptography[J]. Advances in quantum cryptography，2020，12(4)：1012-1236.

[7] GIRON A A，CUSTÓDIO R，RODRÍGUEZ-HENRÍQUEZ F. Post-quantum hybrid key exchange：a systematic mapping study[J]. Journal of Cryptographic Engineering，2023，13(1)：71-88.

[8] HOANG K. Post-quantum cryptography for public key infrastructure [EB/OL]. [2025-02-17]. https://www. theseus. fi/bitstream/handle/10024/802390/Thesis-official.pdf?sequence=2.

[9] RESCORLA E. The transport layer security (tls) protocol version 1.3：RFC 8446[S/OL]. [2025-02-17]. https://www.rfc-editor.org/rfc/rfc8446.

[10] ETSI. Quantum-safe cryptography (QSC)；quantum-safe migration recommendations：ETSI GR QSC 005[S/OL]. https://www.etsi.org/standards.

[11] 高峰，张翼，赵烨昕. 快速身份认证系统CFCA FIDO+[J]. 网络空间安全，2019，10(2)：101-107.

作者简介：
黄建康，毕业于吉林大学，主要从事移动安全应用开发和密码技术应用工作；侯玉华，毕业于沈阳工业大学，高级工程师，硕士，主要研究方向为移动信息安全、终端操作系统；齐霄，毕业于北京交通大学，高级工程师，硕士，主要从事移动安全相关研究工作；田嘉，毕业于中国人民大学，工程师，硕士，主要从事移动信息安全相关研究工作。