融合PQC与QRNG的移动通信量子安全方案研究

Research on Quantum Security Solutions for Mobile Communications Integrating PQC and QRNG

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

摘　要：
随着量子技术的不断进步，移动通信领域正面临着前所未有的重大安全挑战与威胁。针对移动通信的量子安全风险，提出“应用加密层+硬件安全层”双层量子安全方案。应用层采用“国密+抗量子密码（PQC）”混合架构，实现抗量子通信；硬件层通过SIM卡集成量子随机数发生器（QRNG），解决随机数质量不足与密钥存储安全问题。该方案可抵御现有及未来的量子计算攻击，核心算法攻击成本远超现有物理极限，与现有国密体系、SIM卡硬件兼容，部署成本低，为移动通信量子安全提供了可靠的技术路径。

关键词：
移动通信；量子安全；抗量子密码；量子随机数发生器
doi：10.12045/j.issn.1007-3043.2025.10.008
文章编号：1007-3043（2025）10-0042-06
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：
With the continuous advancement of quantum technology，the field of mobile communication is facing unprecedented major security challenges and threats. In response to the quantum security risks in mobile communication，a dual-layer quantum security scheme consisting of an “application encryption layer + hardware security layer” is proposed. The application layer adopts a hybrid architecture of “national cryptography + post-quantum cryptography（PQC）” to achieve quantum-resistant communication. The hardware layer integrates a quantum random number generator（QRNG）through a SIM card to address the issues of insufficient random number quality and key storage security. This scheme can withstand existing and future quantum computing attacks，with the cost of attacking the core algorithm far exceeding current physical limits. It is compatible with the existing national cryptography system and SIM card hardware，with low deployment costs，providing a reliable technical path for quantum security in mobile communication.

Keywords：
Mobile communication；Quantum security；Post-quantum cryptography；Quantum random number generator

引用格式：田嘉，旷炜，侯玉华，等. 融合PQC与QRNG的移动通信量子安全方案研究[J]. 邮电设计技术，2025（10）：42-47.

1 概述

量子计算的快速发展，对现有的公钥密码体系构成了前所未有的威胁。量子计算机利用量子力学现象可以求解传统计算机难以解决的数学问题，从而可以攻破当前许多正在使用的公钥加密系统。例如，Shor算法可在多项式时间内分解大整数、求解离散对数问题，直接破解RSA、ECC、国密SM2等主流非对称密码[1]；Grover算法可将对称密码的暴力攻击复杂度降至平方级，对AES、国密SM4等算法构成加速威胁。

量子威胁不仅局限于理论层面。目前，已经有研究使用量子计算机实现了RSA的现实攻击能力，大幅提升了量子技术的现实威胁性[2]。同时，已有攻击者开始收集和存储重要数据，准备在未来使用量子计算

收稿日期：2025-09-02

机进行破解以获取敏感信息。这种“现在存储，以后解密”的攻击方式[3]，使得移动通信在量子计算机技术还未完全成熟的当下，已经对量子安全升级产生了迫切的需求。

2 量子安全核心技术原理

本章介绍了主流的抗量子攻击和利用量子力学的安全保密技术，包括抗量子密码（PQC）、量子密钥分发（QKD）以及量子随机数发生器（QRNG），并探讨了这些技术在移动通信中的应用场景。

2.1 抗量子密码（PQC）技术

抗量子密码（PQC）技术是一种为抵抗量子计算机攻击而设计的加密技术[4]。PQC基于在量子计算能力下难以解决的数学问题，包括基于格（lattice）、基于编码理论、多变量多项式和基于哈希函数等理论，构建密码体系，提供了一种在量子时代保护信息安全的新途径。

2024年8月13日，NIST正式发布了全球首批3个抗量子加密标准[5]，其中Kyber密钥封装算法与Dilithium数字签名算法性能优、安全性高。

PQC可以与现有的密码算法混合使用，这种混合部署方法提供了针对传统和潜在量子对手的分层防御[6]。混合算法同时采用2种算法，确保整个系统至少与混合算法中使用的最强算法一样安全。

2.1.1 Kyber算法：抗量子密钥封装

Kyber基于Module-Learning With Errors（MLWE）问题设计，核心原理是“高维格空间中寻找短向量的计算复杂性”。算法通过多项式环上的加法、乘法运算，将密钥协商过程转化为MLWE问题求解。即使借助量子计算，攻击Kyber-512仍需2^{70}次量子门操作、1.9×10^{12} PB内存，远超现有超级计算机2.8 PB的存储极限，且计算时间远超宇宙年龄（见表1）。

表1　主流算法攻击成本对比

算法	经典攻击门操作数/次	量子混合攻击门操作数/次	内存需求/PB
Kyber-512	2^{143}	2^{70}（Grover加速）	1.9×10^{12}
Dilithium-2	2^{141}	2^{70}	3.2×10^{12}
AES-128（基准）	2^{86}	-	2.8（当前极限）

在移动通信中，Kyber主要用于密钥封装。接收方生成Kyber公私钥对，发送方用公钥封装随机数生成“预密钥”，双方通过预密钥推导会话密钥，满足选择密文攻击下的不可区分性（IND-CCA2）安全。

2.1.2 Dilithium算法：抗量子数字签名

Dilithium同样基于MLWE问题，通过“格空间中生成短向量签名、验证时校验短向量合法性”实现身份认证。该算法的签名过程需生成多个短向量并进行哈希压缩，验证过程需验证短向量的范数约束。攻击Dilithium-2需2^{70}次量子门操作、3.2×10^{12} PB内存，其安全性显著高于AES-128（见表1）。

在移动通信中，Dilithium用于服务端身份验证和客户端签名验证，防止中间人攻击与数据篡改。

2.2 量子密钥分发（QKD）技术

量子密钥分发（QKD）是一种利用量子力学原理来实现2个通信方之间安全密钥共享的技术[7]。QKD的核心思想是利用量子态传输密钥信息，一方面海森堡测不准原理量子态的密钥信息难以被准确测量，另一方面任何对量子态的复制和测量行为都会改变量子态的状态，这使得任何对量子系统的窃听行为都会被通信双方所察觉，所有的干扰都可以被通信双方检测到，从而保障了密钥的安全性。

QKD在有线信道下的应用较为成熟，特别是在光纤通信中[8]。然而，在无线信道下应用QKD则面临更多挑战。无线信道的不稳定性、信号衰减使QKD在无线环境下的实现更为复杂和困难[9]。在成本及改造量方面，QKD的部署需要特定的量子通信设备，如量子信号发射和接收模块以及密钥存储管理模块，在现有的通信基础设施中，这些设备的集成和部署需要较大的改造和成本投入。

对于移动通信而言，虽然QKD理论上可以提供无条件的安全性，但这与移动通信广覆盖、无线传输、终端移动性的特点存在本质矛盾：无线信道容易受干扰、遮挡的影响，无法满足语音、视频等实时通信需求；终端侧QKD模块体积大、功耗高，难以集成至手机、物联网终端；跨运营商、跨区域的QKD网络互联成本极高，短期内无法规模化部署。

2.3 量子随机数发生器（QRNG）技术

量子随机数发生器（QRNG）是一种利用量子力学原理产生随机数的技术[10]。量子随机数发生器的核心优势在于其生成的随机数具有内禀的随机性，这种随机性源自量子力学的不确定性原理，即量子态的测量结果具有本质上的随机性，无法被任何的算法或模型精确预测。随着技术的进步，量子随机数发生器的集成度和生成速率的提升[11]，以及小型化芯片的快速

发展,这项技术也更加实用化[12]。

在移动通信中,在终端侧,QRNG主要可用于生成SM2/PQC密钥对、会话密钥随机参数;在服务端侧,QRNG可用于生成服务端PQC公私钥、密钥封装随机数,实现端到端随机数安全。

3 移动通信系统量子安全风险分析

结合移动通信的特点,其量子安全风险[13-17]可归纳为4类。

3.1 传统密码体系的量子脆弱性

移动通信当前采用"身份认证(SM2)+数据加密(SM4)+传输安全(TLS)"体系。其中,SM2基于椭圆曲线离散对数问题,可被Shor算法破解;TLS1.3默认采用ECC密钥协商,同样面临量子威胁。这些脆弱性使得攻击者可以窃取SIM卡SM2私钥、破解TLS传输数据,实现用户身份伪造、通信内容窃听。

3.2 无线信道的开放性与中间人攻击

移动通信数据通过无线信道传输(如4G LTE的PDCP层、5G的SDAP层),信道完全开放且易被监听。攻击者可通过"伪基站"伪装服务端,拦截客户端与服务端的密钥协商过程;即使采用TLS传输层加密,若服务端公钥被篡改(中间人攻击),加密数据仍可被破解。现有TLS证书体系依赖RSA/ECC签名,量子计算可伪造证书,这导致中间人攻击成功率大幅提升。

3.3 密钥存储与运算的安全隐患

移动通信密钥管理存在密钥存储风险、密钥明文暴露等隐患。若密钥存储在移动终端本地而非硬件安全模块,攻击者可通过root权限读取私钥;若密钥存储在SIM卡中,根据国密GM/T0016-2012规范的要求,SM2私钥无法导出SIM卡,但SM4会话密钥需从SIM卡导出至手机内存,以明文形式参与运算,易被恶意程序窃取。密钥泄露将直接导致加密失效,攻击者可冒充合法用户登录、解密历史通信数据。

3.4 随机数质量不足的连锁风险

现有移动通信终端及服务端主要采用伪随机数(PRNG)或者物理噪声源的方式生成随机数。随机数来源存在明显缺陷:伪随机数基于确定性算法,若初始种子泄露,所有随机数均可被预测;物理噪声源易受温度、电磁干扰的影响,随机性不足且可被操控。随机数是密码算法的"安全基石",随机数质量不足会导致密钥生成不安全、签名参数可预测,攻击者可通过分析随机数规律破解密码系统。

4 融合PQC与QRNG的双层量子安全方案

针对上述风险,本文提出"应用加密层+硬件安全层"双层防护方案,其核心思路是应用层解决抗量子通信,硬件层保障安全根基。

a)应用加密层。基于国密+PQC混合算法,用于密钥协商、数据加密与身份认证,实现抗量子通信。

b)硬件安全层。终端以SIM卡为硬件安全根,集成QRNG芯片,实现高质量随机数同步生成,为密码算法提供安全种子,同时提供密钥安全存储与权限控制。

4.1 应用加密层设计:抗量子通信的核心

应用加密层的核心是不改动传输层加密,在应用层实现国密+PQC混合加密,避免现有网络架构的大规模改造,同时抵御量子攻击与中间人攻击。

4.1.1 "Kyber+SM2"混合密钥封装方案

密钥封装的目标是安全推导会话密钥,本方案结合了Kyber的抗量子性与SM2的经典安全性。

"Kyber+SM2"混合密钥封装算法的流程如下(见图1)。

a)生成32字节的随机明文,并使用SM2算法公钥进行加密运算,得到SM2密文。

b)生成32字节的随机数,使用Kyber公钥对其进行密钥封装运算,得到Kyber密文和32字节的预密钥K。

c)拼接32字节的随机明文和K作为SM3算法的输入,得到32字节的对称密钥。

"Kyber+SM2"混合密钥解封装算法的流程如下(见图1)。

a)使用SM2算法私钥对SM2密文进行解密运算,得到32字节的随机明文。

b)使用Kyber私钥对Kyber密文进行密钥解封装运算,得到32字节的预密钥K。

c)拼接32字节的随机明文和K作为SM3算法的输入,得到32字节的对称密钥。

"Kyber+SM2"混合密钥封装方案的安全优势如下。

a)抗量子性。Kyber算法抵御量子计算攻击,即使SM2被破解,攻击者仍无法推导会话密钥。

b)前向安全性。每次会话生成新的随机明文及预密钥,历史会话密钥无法通过私钥泄露进行推导。

c)IND-CCA2安全(选择密文攻击下的不可区分

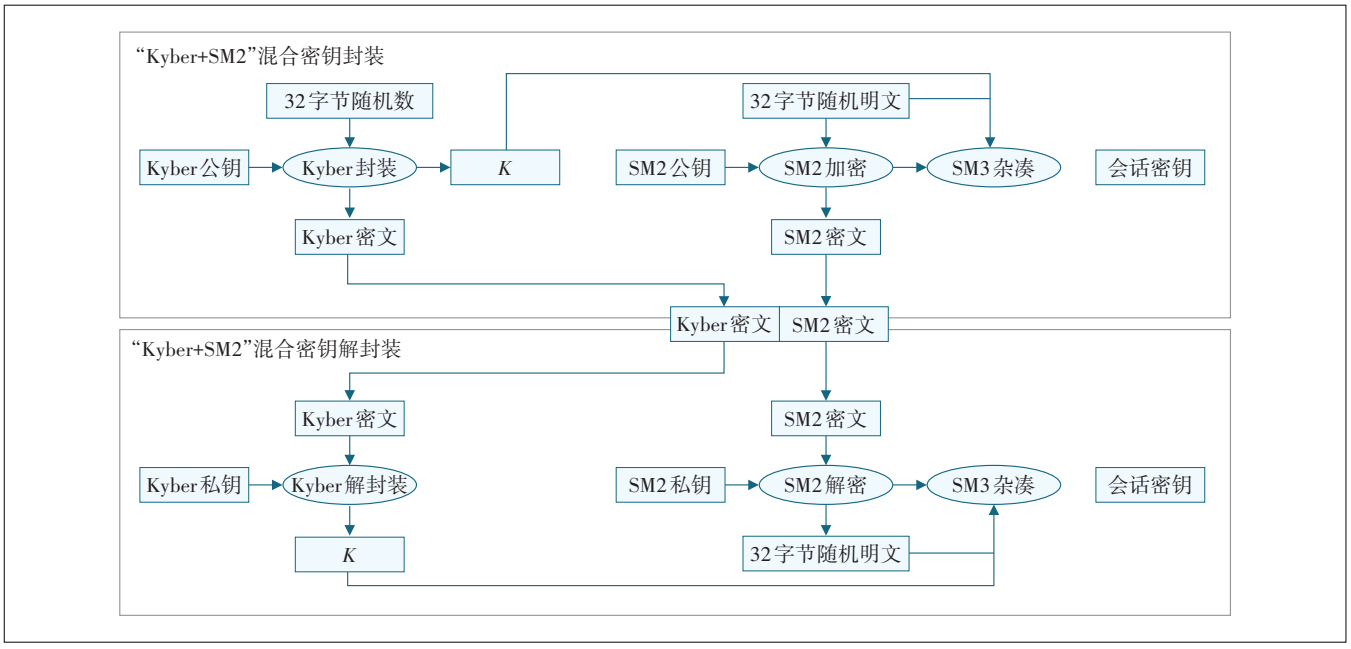

图1　“Kyber+SM2”混合密钥封装以及解封装示意

性）。混合算法中的Kyber算法通过FO转换实现密钥封装，满足IND-CCA2。

4.1.2 “Dilithium+SM2”混合签名方案

签名的目标是验证身份合法性，防止中间人攻击，本方案通过双重签名实现“经典+量子”双重安全。

“Dilithium+SM2”混合签名算法的流程如下（见图2）。

a）使用SM2私钥对消息进行签名运算，得到SM2签名。

b）使用Dilithium私钥对消息进行签名运算，得到

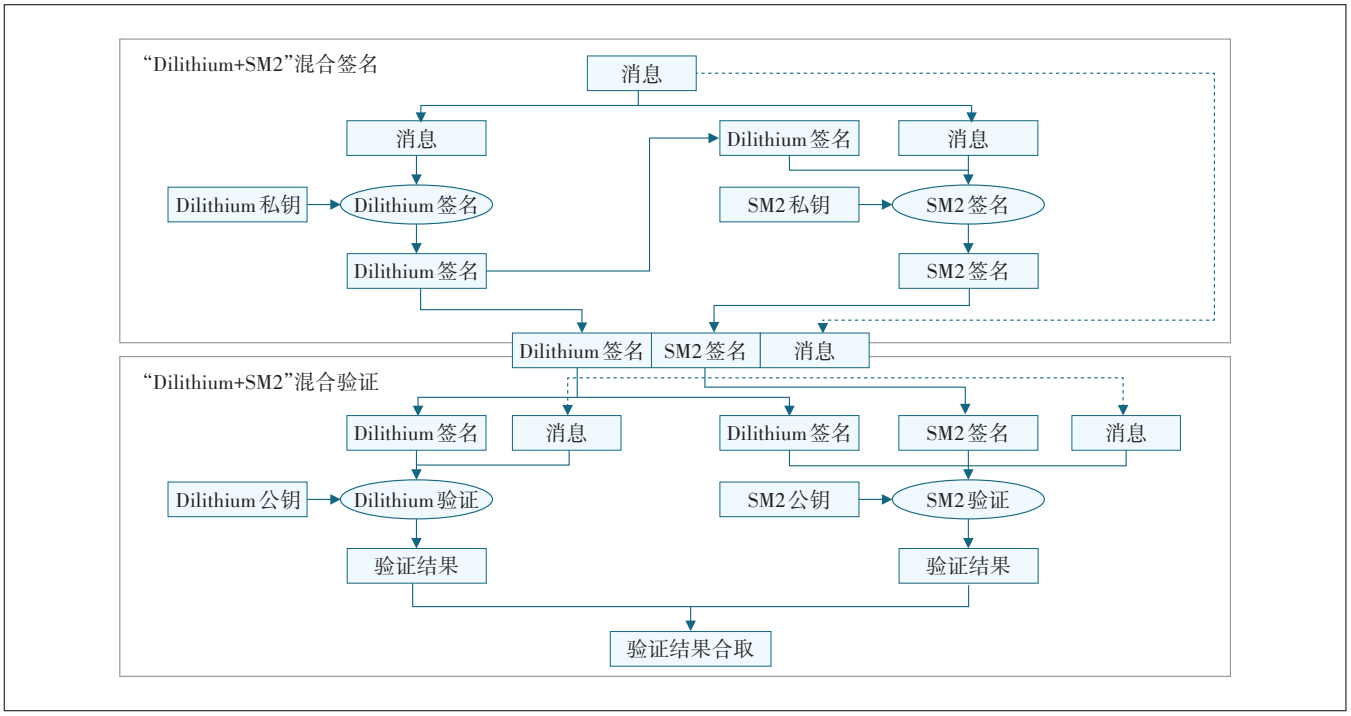

图2　“Dilithium+SM2”混合签名以及验证示意

Dilithium签名。

c)最终签名即为SM2签名||Dilithium签名。

“Dilithium+SM2”混合验证算法的流程如下(见图2)。

a)使用SM2公钥对SM2签名进行验证,得到验证结果。

b)使用Dilithium公钥对Dilithium签名进行验证,得到验证结果。

c)最终签名验证结果即为2个签名验证结果的合取。

“Dilithium+SM2”混合签名方案安全优势如下。

a)抗中间人攻击。即使量子计算伪造SM2签名,仍无法伪造Dilithium签名。

b)兼容性。SM2签名保障了当前经典环境下的验证效率,Dilithium签名保障了量子环境下的安全。

4.1.3 应用层通信流程

应用层的混合加密避免了对传输层的大规模改造,同时提供了端到端的安全防护。基于上述国密+PQC混合算法,客户端和服务端保护通信数据的交互流程如下。

a)客户端向服务端发送通信请求,并发送自己的SM2+Kyber混合公钥。

b)服务端使用客户端用户的SM2+Kyber公钥进行密钥封装运算,计算得到封装密文和会话密钥。

c)服务端构造请求响应,请求响应中包含封装密文,并使用自己的SM2+Dilithium私钥对响应进行签名。

d)服务端向客户端发送请求响应。

e)客户端使用内置的服务端的SM2+Dilithium公钥对响应签名进行校验,完成对服务端的身份验证。

f)客户端使用自己的SM2+Kyber混合私钥对封装密文进行解封装,得到与服务端一致的会话密钥。

g)后续客户端与服务端通信的应用数据均使用该会话密钥以及其派生出来的密钥进行加密。

4.2 硬件安全层设计:安全根基的保障

硬件安全层以SIM卡为核心,集成QRNG芯片实现高质量随机数同步生成,为密码算法提供安全种子,同时提供密钥安全存储与权限控制,解决密钥存储安全、随机数质量问题。

4.2.1 SIM卡集成QRNG芯片

使用SIM卡作为移动通信终端的硬件安全根,具有物理防解剖、防探测的特性。本方案在SIM卡内集成微型QRNG芯片,基于“光子偏振测量”生成真随机数,为国密和PQC密钥生成、会话密钥参数提供安全种子。相较于物理噪声源,SIM卡集成QRNG具有更强的抗干扰性与安全性,可防止攻击者通过干扰随机数生成过程破解密码系统。

4.2.2 密钥安全存储与权限控制

本方案中SIM卡采用分区存储+权限控制机制,保障SM2、SM4、PQC密钥的安全,避免明文暴露与未授权访问。

根据GM/T0016-2012规范,SM2密钥存储于SIM卡的密钥容器中,SM2私钥无法导出、防解剖读取,存储的安全性较高,不存在容易被攻击的安全隐患;SM4密钥生成后存储于SIM卡内部,仅在运算时通过加密通道而非明文传输至客户端。

对于PQC密钥,由于手机系统的存储环境较为复杂,容易遭受到恶意攻击,导致密钥泄露,所以PQC算法的密钥像SM2算法密钥一样存储在SIM卡内部。由于SIM卡无PQC密钥的标准容器,为了与SM2算法的权限要求保持一致,本方案将PQC算法的公钥和私钥分别存储在不同权限的文件中,借助SIM卡中应用的权限机制保证密钥的读写安全性;对私钥进行加密存储能够防止物理性探测攻击,PQC算法密钥在SIM卡中存储的安全性与SM2密钥相同。

使用SIM卡作为终端密钥载体的优势如下。

a)物理安全。SIM卡采用防解剖、防探测设计,私钥无法通过物理手段进行读取。

b)权限隔离。不同密钥对应不同权限。

5 方案安全性与可行性验证

5.1 风险应对验证

针对第3章所述的移动通信系统的4类量子安全风险,本方案实现了全维度覆盖(见表2)。

5.2 算法安全性验证

方案核心算法的安全性如下。

a)算法抗攻击性保障。核心采用抗量子算法Kyber/Dilithium,其安全性基于MLWE问题的计算复杂性,即便借助量子计算资源,攻击所需门操作数(2^{70}量级)与内存需求(10^{12} PB)远超现有物理极限,形成理论安全屏障。

b)混合加密机制。采用“Kyber+SM2”混合密钥封装与“Dilithium+SM2”混合签名架构,实现了前向安全性(国密算法抵御经典算力攻击)和抗量子保障(抗量

表2　移动通信系统量子安全风险应对说明

风险类型	方案应对说明
传统密码量子脆弱性	“Kyber/Dilithium+SM2”混合算法，其中Kyber/Dilithium抵御量子攻击，SM2保障经典安全，形成双重防护
无线信道中间人攻击	应用层实施“Dilithium+SM2”混合签名，客户端需同时验证2种签名，通过后才能确认服务端身份，杜绝中间人冒充，提供了端到端的安全防护
密钥存储与运算隐患	SIM卡提供硬件级防护，SM2私钥存储于密钥容器，PQC私钥经SM2加密存储；SM4会话密钥通过加密通道传输，运算后即时销毁
随机数质量不足	终端SIM卡集成QRNG芯片，满足随机性检测标准，确保密钥生成不可预测

子密码算法防御未来量子计算威胁）。

5.3 工程可行性验证

方案在移动通信场景中的可行性主要体现在以下3个方面。

a）性能适配性。采用轻量级抗量子密码算法，密钥封装与签名操作的耗时能够满足实时通信的交互需求，确保用户性能体验。

b）硬件兼容性。通过SIM卡集成量子随机数生成模块，在保持现有终端硬件架构的基础上实现安全增强。该设计兼顾了硬件成本控制与能效优化，符合移动终端对低功耗、小型化的核心要求。

c）部署便捷性。方案采用应用层加密改造策略，完全兼容现有4G/5G网络传输协议，无需升级基站、核心网等基础设施，大幅降低了运营商网络改造的实施难度和商业成本。

6 结束语

针对移动通信的量子安全需求，本文提出了“应用加密层+硬件安全层”双层方案，通过“国密+PQC”混合算法解决抗量子通信问题，通过SIM卡集成QRNG解决安全根基问题。该方案保证了安全性、可行性和兼容性，可抵御现有及未来量子计算攻击；适配移动通信的无线传输、终端资源受限特点，部署成本低；与现有国密体系、SIM卡硬件兼容，无需大规模改造现有网络。

参考文献：

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

[2] 王潮，王启迪，洪春雷，等. 基于D-Wave Advantage的量子退火公钥密码攻击算法研究[J]. 计算机学报，2024，47(5)：1030-1044.

[3] 赖俊森，赵文玉，张海懿. 量子计算信息安全威胁与应对策略分析[J]. 信息通信技术与政策，2024，50(7)：24-29.

[4] DAM D T, TRAN T H, HOANG V P. A survey of post-quantum cryptography: start of a new race[J]. Cryptography, 2023, 7(3): 40.

[5] NIST. NIST releases first 3 finalized post-quantum encryption standards [EB/OL]. [2024-08-13]. https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards.

[6] JOSEPH D, MISOCZKI R, MANZANO M, et al. Transitioning organizations to post-quantum cryptography[J]. Nature, 2022, 605(7909): 237-243.

[7] BENNETT C H, Brassard B. Quantum cryptography: Public key distribution and coin tossing[C]//Proc of IEEE International Conference on Computers, Systems and Signal Processing. Bangalore: IEEE, 1984: 175-179.

[8] SHARMA P, AGRAWAL A, BHATIA V, et al. Quantum key distribution secured optical networks: a survey[J]. IEEE Open Journal of the Communications Society, 2021, 2: 2049-2083.

[9] TSAI C W, YANG C W, LIN J, et al. Quantum key distribution networks: challenges and future research issues in security[J]. Applied Sciences, 2021, 11(9): 3767.

[10] SCHMIDT H. Quantum-mechanical random-number generator[J]. Journal of Applied Physics, 1970, 41(2): 462-468.

[11] BAI B, HUANG J Y, QIAO G R, et al. 18.8 Gbit/s real-time quantum random number generator with a photonic integrated chip[J]. Applied Physics Letters, 2021, 118(26): 264001.

[12] 宋晨. 量子随机数发生器技术现状及其应用[J]. 华东科技(综合)，2021(1)：1.

[13] 国家密码管理局. SSL VPN技术规范：GM/T 0024-2014[S]. 北京：国家密码管理局，2014.

[14] SHANNON C E. Communication theory of secrecy systems[J]. The Bell System Technical Journal, 1949, 28(4): 656-715.

[15] 李兴新，郭晓花，侯玉华，等. 新形势下移动终端安全需求和对策[J]. 邮电设计技术，2021(6)：88-92.

[16] 旷炜，侯玉华，齐霄，等. 新一代保密通信网络架构研究[J]. 邮电设计技术，2023(4)：17-19.

[17] 李路曼，旷炜，侯玉华，等. 基于量子密钥的移动终端保密通信方案研究[J]. 邮电设计技术，2023(11)：40-43.

作者简介：

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的研究工作；旷炜，毕业于清华大学，高级工程师，硕士，主要从事安全平台相关的研究工作；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的研究工作；黄建康，毕业于吉林大学，高级工程师，学士，主要从事移动安全及密码算法相关的研究工作；杨华新，毕业于长安大学，高级工程师，硕士，主要从事安全通信、数字化转型相关研究工作。