SIM卡与量子技术融合在未来通信安全中的应用研究

Discussion on Application of SIM Card and Quantum Technology Integration in Future Communication Security

王海涛，衣莉莉，李佳俊，孙阳阳，王振宇（联通华盛通信有限公司，北京 100032）
Wang Haitao，Yi Lili，Li Jiajun，Sun Yangyang，Wang Zhenyu（Unicom Vsens Communications Co.，Ltd.，Beijing 100032，China）

摘　要：
量子计算对SIM卡依赖的经典密码体系构成现实威胁。分析了传统SIM卡、eSIM与iSIM的安全局限，阐述量子密钥分发（QKD）、量子随机数生成器（QRNG）与后量子密码（PQC）的原理与优势，提出由SIM卡安全存储QKD密钥、在SIM卡芯片内集成微型QRNG以及在安全执行环境中实现PQC算法3种融合方案，并讨论了部署模式及硬件小型化、功耗成本与标准化挑战。研究认为，量子SIM卡有望成为6G端点安全的信任根。

关键词：
SIM卡；量子密钥分发；量子随机数生成；后量子密码；移动通信安全
doi：10.12045/j.issn.1007-3043.2026.10.013
文章编号：1007-3043（2026）10-0077-05
中图分类号：TN918
文献标识码：A
开放科学（资源服务）标识码（OSID）：

Abstract：
Quantum computing poses a realistic threat to the classical cryptography on which SIM cards rely. The security limitations of conventional SIM, eSIM and iSIM are analyzed, and the principles and advantages of quantum key distribution (QKD), quantum random number generators (QRNG) and post-quantum cryptography (PQC) are outlined. Three integration schemes are proposed: secure storage of QKD keys in the SIM card, integration of a miniaturized QRNG into the SIM chip, and implementation of PQC algorithms in the secure execution environment. Deployment modes and the challenges of hardware miniaturization, power consumption, cost and standardization are further discussed. It is concluded that the quantum SIM card is expected to serve as the endpoint trust anchor for 6G security.

Keywords：
SIM card; Quantum key distribution; Quantum random number generation; Post-quantum cryptography; Mobile communication security

引用格式：王海涛，衣莉莉，李佳俊，等. SIM卡与量子技术融合在未来通信安全中的应用研究[J]. 邮电设计技术，2026（10）：77-81.

1 概述

1.1 移动通信安全挑战的演进

随着5G向6G演进，移动通信网络面临日益严峻的安全挑战。传统SIM（Subscriber Identity Module）卡依赖的经典密码算法在量子计算的威胁下安全性堪忧。Shor算法可破解RSA、ECC等公钥密码，威胁用户身份和通信内容安全[1]。物联网、边缘计算等新应用扩大了攻击面，SIM卡作为端点安全核心，亟需前瞻性安全方案来应对未来威胁。

1.2 量子技术在通信安全中的潜力

量子技术为通信安全带来了机遇。量子密钥分发（QKD）利用量子力学原理实现无条件安全密钥分发，任何窃听均可被察觉，提供信息论安全[2-3]。量子随机数生成器（QRNG）基于量子物理产生真随机数，提升密码学基础安全性。后量子密码（PQC）开发抗量

收稿日期：2026-08-18

子攻击的经典算法，为现有网络向量子安全过渡提供可行路径[4]。依据这些技术，可共同应对未来的量子威胁。

1.3 本文研究意义与结构

SIM卡作为移动通信信任根，与量子技术融合可提升其抗量子攻击能力，保障用户身份和通信数据安全，并为物联网等提供端点安全。本文探讨了SIM卡与量子技术融合的可行性、方案及挑战。其中，第2章回顾了SIM卡技术与安全局限；第3章阐述了QKD、QRNG、PQC原理；第4章提出融合方案；第5章对技术挑战与趋势进行了讨论；第6章对量子SIM卡前景进行了总结与展望。

2 SIM卡技术发展与安全机制现状

2.1 SIM卡的核心功能与演进历程

SIM卡作为移动通信终端与网络连接的桥梁，承载用户身份识别、鉴权、加密算法存储和用户数据管理等核心功能[5]。从2G到4G，其功能不断扩展，可支持更复杂的鉴权和更大的存储容量。5G时代，SIM卡功能扩展至支持切片网络、物联网等[6]，内部集成了微控制器和加密协处理器，成为高度安全的微型计算机系统和信任根。

2.2 现有SIM卡安全机制的局限性

SIM卡现有的安全机制面临量子计算威胁。SIM卡依赖AES、RSA、ECC等经典密码算法，这些算法的安全性基于计算复杂性。量子计算机的Shor算法可高效破解RSA和ECC，Grover算法可加速对称密钥的破解[1]，使SIM卡密钥和运算面临风险。此外，SIM卡多采用伪随机数生成器，存在被预测的风险，影响密钥安全。这些局限性表明SIM卡安全机制急需升级，以应对量子威胁。

2.3 eSIM和iSIM的兴起及其安全特性

eSIM（Embedded SIM）和iSIM（Integrated SIM）技术应物联网小型化、集成化和远程管理的趋势而生。eSIM直接焊接在主板上，支持远程配置运营商Profile，无须物理更换，提升物联网部署的灵活性[7-8]。iSIM将SIM功能集成到主处理器安全区域，进一步减小尺寸、降低功耗成本，增强防篡改能力，适用于受限物联网终端[9]。eSIM和iSIM的软件定义和高集成度特性，为SIM卡与量子技术融合提供了新契机，支持OTA更新PQC算法，并为芯片级集成QRNG或量子安全模块奠定了物理基础。SIM卡技术演进与安全特性对比如表1所示。

表1 SIM卡技术演进与安全特性对比

SIM类型	发展阶段	主要功能	安全特性	挑战
传统SIM卡	2G/3G/4G/5G	用户身份识别、鉴权、密钥存储、数据管理	物理防篡改、经典密码算法（AES/RSA/ECC）	易被物理移除、量子计算威胁
eSIM（嵌入式）	4G/5G/IoT	远程配置Profile、多Profile管理、用户鉴权	物理防篡改、经典密码算法、远程安全更新机制	仍依赖经典密码算法；远程配置链路基于经典PKI；焊装不可更换，量子硬件能力难以后期加装
iSIM（集成式）	5G/IoT/未来6G	SoC集成、超小型化、极低功耗、用户鉴权、数据加密	硬件级安全隔离、经典密码算法、更强防篡改能力	仍依赖经典密码算法、集成度高导致更新复杂性增加

3 量子安全通信技术原理

为应对量子计算对现有密码体系的潜在威胁，量子安全通信技术提供了3种主要路径，分别为量子密钥分发（QKD）、量子随机数生成器（QRNG）以及后量子密码（PQC）。

3.1 量子密钥分发（QKD）原理及其安全性

QKD利用量子力学原理实现密钥安全分发。任何窃听都会扰动量子态并被察觉，确保密钥分发的无条件信息论安全。BB84协议是经典QKD协议，Alice和Bob通过随机选择基编码和测量光子，并通过公开基选择来检测窃听，确保密钥安全[3]。QKD安全性基于物理定律，可抵御量子计算机攻击，是未来量子威胁的终极解决方案，但其面临传输距离、密钥速率和设备成本高体积大的挑战[10]。中国科学技术大学已在量子微纳卫星与可移动地面站间的实时星地量子密钥分发研究中取得突破，实现了低成本小型化诱骗态量子光源技术和实时密钥提取，为实用化卫星量子通信组网铺平了道路[2]。南京大学率先完成了基于无人机平台的量子密钥分发实验，验证了移动平台实现光量子信息任务的可行性。

3.2 量子随机数生成器（QRNG）

密码学中随机数至关重要。传统伪随机数生成器理论上可被预测，存在安全风险。QRNG利用量子力学固有随机性，如光子路径选择，产生真正不可预测的真随机数，安全性更高。QRNG提供不可预测、高熵值的真随机数，为密码学奠定基础。随着微型化，QRNG有望集成到SIM卡等终端设备上。

3.3 后量子密码（PQC）

PQC是抵御量子计算机攻击的经典密码算法，它基于数学难题，而非量子物理。NIST正推动PQC标准化，研究方向包括格基、多变量、哈希签名、编码和超奇异同源密码，旨在替代RSA、ECC等公钥体系[4,11]。PQC的优势在于可软件升级部署于现有网络，兼容性好。它与QKD互补，提供量子安全的数字签名和加密，适用于QKD无法覆盖或长距离传输场景。

量子安全技术在通信中的应用潜力如表2所示。

表2　量子安全技术在通信中的应用潜力

量子技术	核心原理	安全优势	适用场景	挑战
QKD	量子态不可克隆、测量扰动	信息论无条件安全、窃听可察觉	核心网密钥分发、数据中心互联、专网通信	传输距离、密钥速率、设备体积与成本、光纤依赖
QRNG	量子物理固有随机性	产生真随机数、不可预测、高熵值	密钥生成、协议初始化、认证、随机数池填充	小型化、功耗控制、集成度
PQC	数学难题（抗量子攻击）	软件升级兼容性好、可部署于现有网络、抵御量子攻击	数字签名、身份认证、数据加密、TLS/SSL替代	算法效率、密钥或签名长度、安全性仍基于计算假设

4 SIM卡与量子技术融合方案设计

将量子安全技术引入SIM卡，能够显著提升移动通信终端的安全性，使其能够有效抵御未来量子计算的威胁。

4.1 量子SIM卡（Q-SIM）概念与架构

量子SIM卡（Quantum-SIM，Q-SIM）指具备或利用量子安全能力的SIM卡，以SIM卡为信任根，集成或协同外部量子模块，实现量子级身份认证、密钥管理和数据保护。Q-SIM架构多样，从物理SIM到eSIM、iSIM。理想Q-SIM应具备量子密钥管理、QRNG、PQC算法支持及安全可信执行环境。中国电信已推出量子安全SIM卡，并获得国家密码管理局的商用密码产品认证证书[12]。中国移动也以超级SIM卡为核心载体，构建“超级SIM量子国密资源池”，实现量子密码服务与密钥存储分离，并已在多省落地应用[13-14]。

4.2 融合方案1：QKD密钥分发与SIM卡安全存储

本方案利用QKD网络分发密钥，SIM卡作为量子安全密钥的存储和管理载体。

本方案的工作原理如下。QKD设备可部署在核心网侧或基站侧，并通过量子信道完成密钥分发，经典信道负责纠错与隐私放大。生成的量子密钥统一由QKD密钥管理系统（QKMS）进行管理，可通过ETSI GS QKD 004标准定义的API接口（典型操作包括OPEN_CONNECT、GET_KEY、CLOSE）安全地提供给上层应用[15]。SIM卡通过运营商的OTA安全信道或与基站侧安全模块建立的接口，接收并注入量子密钥，并在内部防篡改安全存储区进行长期保存。在部署模式上，核心网侧集中部署便于统一管理和与现有安全体系的融合，适合大规模商用；基站侧分布式部署则能实现端到端低时延的量子密钥传递，适合对本地安全与实时性要求高的场景。两者可形成分层互补：核心网负责骨干级密钥管理，基站侧负责接入端安全，从而构建分层量子密钥分发体系。同时，业务链路与量子链路严格隔离，前者用于通信数据传输，后者仅承担密钥分发，以确保整体安全性。

该方案继承了QKD无条件安全，密钥保护达信息论安全级别；利用SIM卡防篡改、防克隆特性，可有效保护量子密钥；可逐步演进，通过网络侧QKD部署和SIM卡升级实现演进，无须大幅改变终端硬件。

本方案面临的挑战有：QKD网络须广泛部署以支持大规模终端，面临基础设施成本、远距离传输和中继挑战；高效安全地将QKD密钥分发至海量SIM卡并管理其生命周期，是系统级挑战；须定义SIM卡与QKD密钥管理系统间的安全接口和协议标准。

4.3 融合方案2：QRNG集成于SIM卡增强随机性

本方案通过在SIM卡芯片内部集成微型QRNG，提升SIM卡随机数质量和安全性。

本方案将基于量子噪声的微型QRNG芯片或模块直接集成到SIM卡芯片内部，QRNG模块利用量子物理过程产生原始真随机比特流，经处理后输出高质量真随机数。SIM卡加密协处理器在密钥生成、数字签名等密码学操作时，直接调用QRNG产生的真随机数。

本方案可提供物理层面的真随机性，杜绝伪随机数风险，显著提升依赖随机数的密码操作的安全性；QRNG集成在SIM卡内部，不依赖外部量子网络，部署灵活独立；QRNG技术小型化趋势使其具备集成到SIM卡芯片的可能性。

本方案面临的挑战有：将微型QRNG集成到SIM卡芯片中，面临尺寸、功耗和成本的工程制造难题；QRNG模块运行可能增加SIM卡功耗，需优化设计以适应低功耗要求；确保QRNG在SIM卡中稳定高效生成真随机数并控制成本，是商业化的关键。

4.4 融合方案3：PQC算法在SIM卡中的实现

本方案在SIM卡安全执行环境中实现PQC算法，以应对量子计算机对经典密码的威胁。

本方案的工作原理如下。将NIST标准化的PQC算法（如Kyber、Dilithium）移植到SIM卡芯片操作系统或安全应用中[11]；SIM卡利用硬件安全模块和安全执行环境，确保PQC算法计算和密钥安全，抵御信道攻击；SIM卡在认证、密钥协商、数据加密时优先使用PQC算法，如在5G AKA中引入PQC提供量子安全认证和会话密钥协商[6]。

本方案的优势包括：PQC算法通过软件或固件升级实现，对现有网络改动小，易部署；eSIM/iSIM的OTA更新能力支持PQC算法灵活升级；PQC算法旨在抵御量子计算机攻击，为SIM卡提供长期密码安全保障；可根据PQC标准化进程和性能，灵活选择和替换算法。

本方案面临的挑战有：部分PQC算法计算复杂度高、密钥签名长，挑战SIM卡计算和存储资源，须优化裁剪以适应资源限制；PQC算法标准化中，最终算法可能存在性能差异和漏洞，须持续关注更新；确保SIM卡PQC算法与网络侧模块互操作，须统一协议和标准。

3种量子SIM卡融合方案的对比如表3所示。

表3　量子SIM卡融合方案对比

融合方案	核心技术	SIM卡角色	安全提升	实施复杂性
QKD密钥存储型	QKD网络	量子密钥安全存储、管理、调用	密钥分发无条件安全、抵御量子攻击	依赖QKD网络覆盖、密钥管理系统复杂、需新标准
QRNG集成型	微型QRNG	内部真随机数生成器	密码学随机性增强、消除伪随机数风险	硬件集成难度高、功耗控制要求严、成本敏感度高
PQC算法型	PQC算法	执行PQC算法、量子安全认证与加密	抵御量子攻击、兼容现有网络、软件升级灵活	算法资源开销大、应用标准不统一、互操作性要求高

4.5 潜在的融合架构与部署模式

SIM卡与量子技术融合可采用多种架构和部署模式，适应不同的场景需求。

a）混合模式（Hybrid Mode）。结合经典与量子密码，如在现有协议引入PQC，同时QKD分发密钥，SIM卡支持双重算法，实现平滑过渡。

b）量子信任根（Quantum Trust Anchor）。将SIM卡升级为量子信任根，作为移动通信量子安全链的起点，所有相关安全操作优先采用量子机制。

c）网络—终端协同。QKD网络分发密钥至核心网/边缘节点，再安全传递给SIM卡；QRNG和PQC集成于SIM卡内部，提供端侧量子安全能力，最大化优势。

d）云—边—端一体化安全。将量子安全能力延伸至云、边、端（SIM卡），构建端到端量子安全通信体系；SIM卡作为终端代表，负责与边缘/核心网进行量子安全认证和密钥协商。

5 关键技术挑战与展望

尽管SIM卡与量子技术融合的前景广阔，但其在技术实现和产业化推广方面仍面临诸多挑战。

5.1 技术实现挑战

5.1.1 硬件集成与小型化

将QKD模块、QRNG芯片等量子器件集成到SIM卡微小芯片中是巨大挑战。QKD光学元件体积大、精度高，虽然芯片级技术有所发展，但超小型化和低成本仍需突破，如光子源集成、单光子探测器微型化和量子芯片量产。iSIM集成量子功能对芯片设计制造的要求更高。

5.1.2 功耗与成本

SIM卡需要极低功耗，但量子器件功耗较高，如何在保证性能的前提下控制功耗是个挑战。量子技术研发制造成本高，须显著降低成本以实现大规模商业化，初期或限于政府、金融等高安全领域。

5.1.3 兼容性与标准化

将量子安全引入SIM卡需要与现有移动通信标准深度融合，包括协议兼容性、接口定义、安全认证和PQC算法选择。

a）协议兼容性。在不破坏现有鉴权加密协议框架的前提下，引入量子密钥或PQC算法，并确保与网络侧的互操作性。

b）接口定义。须定义SIM卡与外部量子安全基础设施间的安全接口和数据传输协议。

c）安全认证。建立量子SIM卡安全评估认证体系，确保符合行业标准。

d）PQC算法选择。在PQC算法标准化中，选择适合SIM卡环境的PQC算法并确保其长期安全性，须持续研究验证。

特别是QKD网络与终端接口须符合国际标准，ETSI GS QKD 004提供了QKD密钥管理与应用之间的统一API定义，这是实现不同厂商设备互通的重要前提[5,15]。与此同时，核心网集中部署与基站侧分布式

部署模式如何平衡，也是标准化和产业化须重点解决的问题。

5.2 产业化与商业模式挑战

SIM卡与量子技术融合还面临产业化和商业模式的挑战。

a）产业链协同。芯片商、SIM卡商、运营商、设备商和量子技术公司须紧密合作，共同推动研发、标准和产品落地。

b）市场需求驱动。量子安全成本以及复杂性高，短期内难以普及，须明确其价值主张，率先在金融、电网、军事等高安全领域进行推广。

c）政策法规支持。政府对量子技术的投入和标准制定将推动量子SIM卡产业化。中国在量子通信领域进展显著，提供了良好的政策环境。

5.3 未来发展趋势与应用前景

尽管面临挑战，SIM卡与量子技术融合仍是未来移动通信安全的必然趋势。6G时代将是万物智联时代，量子SIM卡有望成为其设备认证和数据加密的量子安全基石，为物联网、沉浸式通信等提供强大安全保障。

a）量子安全物联网。集成QRNG或PQC的量子SIM卡可为物联网终端提供低成本、高效率量子安全能力，保护设备身份和数据传输，防范网络攻击。

b）数字经济安全。量子SIM卡可作为个人和企业数字身份的量子安全载体，保障数字资产和交易安全。

c）量子安全通信网络演进。未来，天地一体化量子通信网络将逐步形成，量子SIM卡可作为端点，实现端到端量子安全通信，构建数字信任基础设施。

6 结论

本文探讨了SIM卡与量子技术融合在未来移动通信安全中的应用前景与挑战。面对量子计算威胁，SIM卡作为核心安全组件，亟需融入量子抗攻击能力。研究表明，QKD密钥存储、QRNG集成和PQC算法实现是SIM卡与量子技术融合的可行方案，可从多维度提升SIM卡安全性，为移动通信网络提供强大端点安全保障。尽管面临硬件小型化、功耗、成本、标准化等挑战，但随着量子技术的成熟和产业投入，这些问题有望解决。eSIM和iSIM加速了量子能力集成。

此外，本文还对QKD网络与SIM卡之间的接口机制及核心网与基站侧的部署模式进行了分析，以增强方案的可实施性和与国际标准的契合度。

展望未来，SIM卡与量子技术融合将成为6G及未来移动通信网络安全基石，可有效抵御量子攻击，为物联网、数字经济等提供安全保障，推动移动通信安全进入量子时代，为构建安全、可信的数字基础设施奠定坚实基础。

参考文献：

[1] 崔富鑫，王韦，刘焱，等. 公钥密码的量子攻击研究现状与展望[J]. 网络安全与数据治理，2022，41(9)：3-12.
[2] 潘建伟. 量子信息科技的发展现状与展望[J]. 物理学报，2024，73(1)：2-9.
[3] 王吉鹏. 量子密钥分发技术的实验研究[D]. 北京：北京邮电大学，2022.
[4] 孙奥，何银，李海波，等. 后量子密码发展综述[J]. 信息安全与通信保密，2023(9)：27-35.
[5] ETSI TS 102.221 V17.4.0 Smart cards；UICC-terminal interface；physical and logical characteristics[S].
[6] 3GPP TS 33.501 V18.8.0 Security architecture and procedures for 5G System[S].
[7] 谭伦. 三大运营商重启eSIM业务市场前景广阔[N]. 中国经营报，2025-07-07(C02).
[8] GSMA. eSIM [EB/OL]. [2026-07-21]. https://www.gsma.com/solutions-and-impact/technologies/esim/.
[9] 郑海霞，郑崇恩，王东. ISIM标准及关键标识参数分析[J]. 电信网技术，2016(3)：68-72.
[10] Toshiba. Quantum key distribution：secure communications for the future[EB/OL]. [2026-07-21]. https://www.global.toshiba/solutions/security-ict/qkd.html.
[11] NIST. Post-quantum cryptography[EB/OL]. [2026-07-21]. https://csrc.nist.gov/projects/post-quantum-cryptography.
[12] 中国电信首发“量子高清密话”[J]. 智能建筑与智慧城市，2022(6)：4.
[13] 黄健文，黄首盛，徐诚率，等. 基于运营商号卡能力和量子国密资源池的数据要素可信通道构建[C]//第39次全国计算机安全学术交流会. 西安：中国计算机学会，2024：258-261.
[14] 马晓凯. 量子通信技术与超级SIM卡融合的研究与应用[J]. 通讯世界，2024，31(6)：31-33.
[15] ETSI GS QKD 004 V2.1.1 Quantum key distribution (QKD)；application interface[S].

作者简介：
王海涛，高级工程师，硕士，主要研究方向为信息安全与智能卡技术；衣莉莉，高级工程师，硕士，主要研究方向为智能卡技术管理与应用；李佳俊，高级工程师，博士，主要研究方向为无线通信网络与移动终端技术；孙阳阳，工程师，学士，主要从事智能卡研发及技术管理工作；王振宇，硕士，主要从事电信智能卡、信息安全等相关工作。