

抗量子安全产品手册

构筑面向未来的『量子安全防线』

Quantum Security Product Manual



CONTENTS

目录

TABLE CONTENTS

量子计算对公钥密码体系的安全威胁	01
抗量子密码是应对量子计算攻击的关键路径	02
本源量子已形成量子计算攻防兼备能力	03
抗量子软件安全密码模块	04
抗量子密码卡	05
抗量子服务器密码机	07
抗量子安全网关	09
抗量子安全模组	11
抗量子安全U盾	12
抗量子安全TF卡	13
抗量子安全云桌面操作系统	14
抗量子安全手机	15
量子超级SIM卡	16

量子计算对公钥密码体系的安全威胁

数字经济的基础是构建在RSA、ECC、SM2等公钥密码体系之上。公钥密码安全性依赖传统计算机解决某些数学难题“超高耗时”，以目前常见的2048位RSA密钥为例,传统计算机破解通常需数百万年甚至更久,而量子计算机可能只需几小时甚至更短时间。

威胁目标	量子算法	威胁
非对称密码 (RSA/ECC/SM2)	Shor算法	如同“万能钥匙”，可快速破解,导致身份认证与数字签名彻底失效
对称密码与哈希 (AES/SM3)	Grover算法	将破解难度平方根降低,迫使密钥长度加倍 (如AES-256需升级至AES-512)

“先窃取,后解密”已成为现实威胁,攻击者通过截获并存储加密数据,待量子计算机成熟后解密。根据权威预测,对主流公钥密码的全面破解能力,可能在2030年代初就会到来。

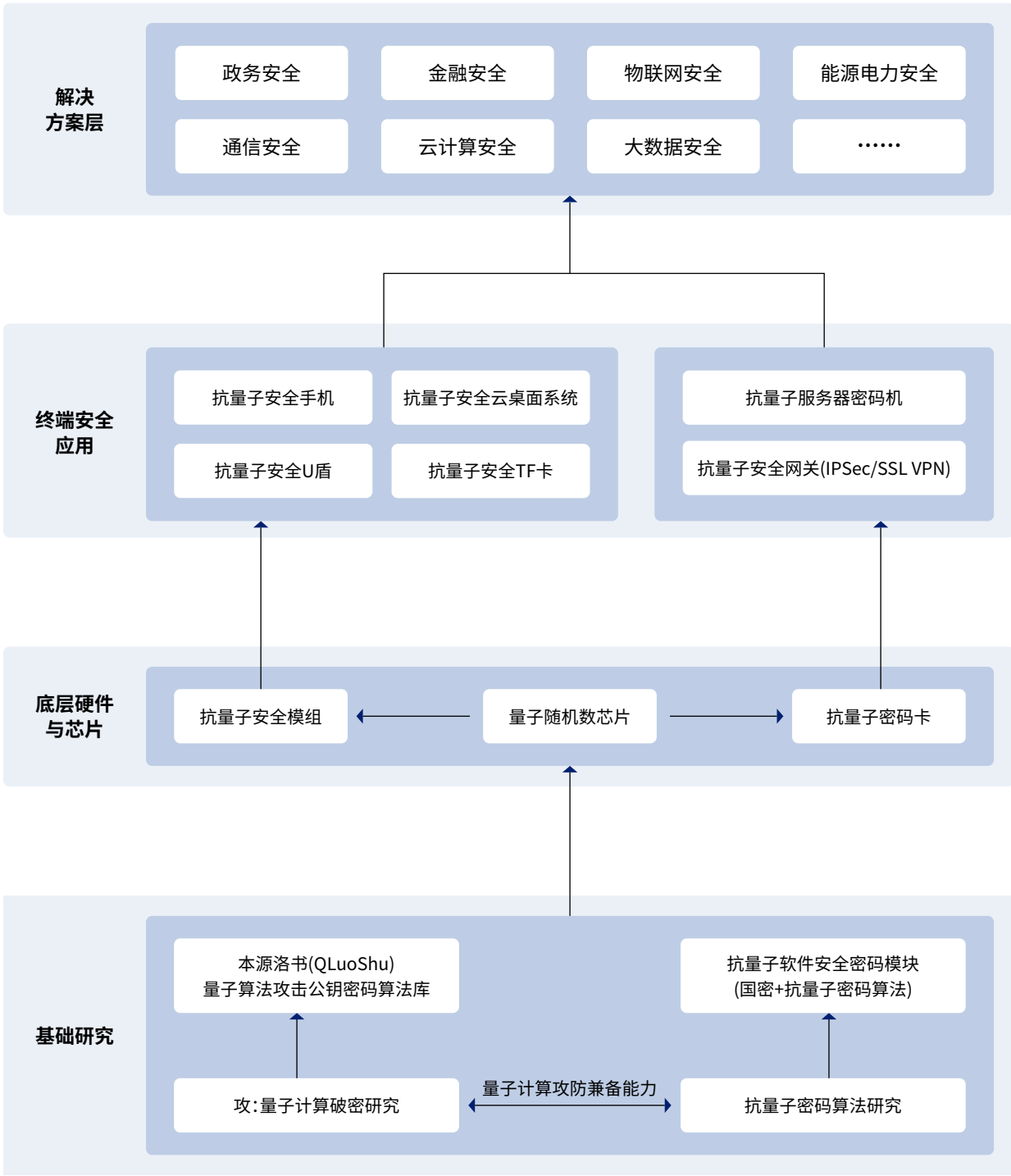
抗量子密码是应对量子计算攻击的关键路径

PQC和QKD是应对量子计算机攻击的两条主要技术路线。PQC因兼容性与经济性,成为国际公认主流的迁移方案。

技术路径	抗量子密码 (PQC)	量子密钥分发 (QKD)
技术原理	基于量子计算不能求解的数学困难问题	依赖于量子力学原理,通过量子信道建立两方之间的安全密钥交换
部署成本	低 (兼容通讯基础设施,对有线、无线网络传输质量无特别要求,网络可达性高)	高 (单光子源/专用光纤/中继)
安全性	抵御量子计算攻击	理论上无条件安全,但依赖物理链路无窃听
适用场景	大规模、广域网络 (互联网、移动通信、云服务)	专用、点对点高安全性专线
国际态势	主流路径, NIST已发布标准,欧美明确迁移路线与应用时间表	因工程化问题,尚未形成安全标准

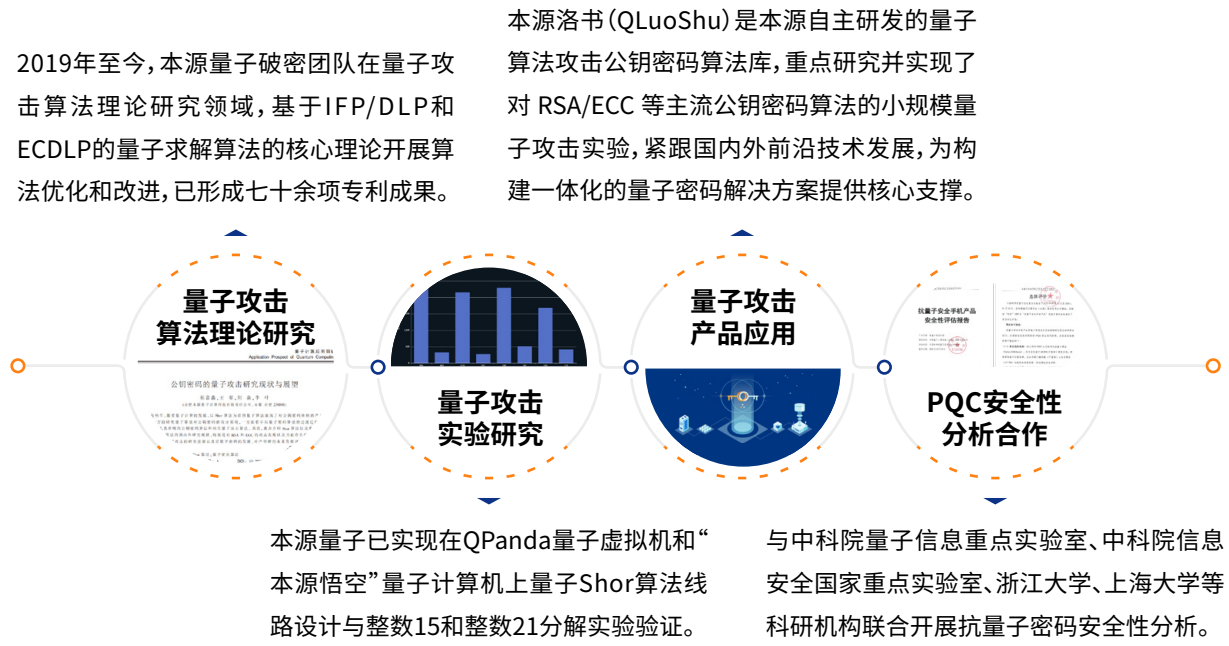
本源量子已形成量子计算攻防兼备能力

本源量子注重技术创新与产业创新融合发展,积极助力量子科技未来产业形成新质生产力,并已形成量子计算“攻防兼备”能力。产品覆盖从算法理论研究到安全产品实现、从安全芯片到网络传输、从数据中心到移动终端全方位安全需求,为抗量子技术从理论突破到产业落地提供全链条支撑。



◎ 量子计算“攻”的能力:前沿密码分析研究

本源基于“量-超-智”三算融合开展的量子破密研究在国内位居前沿。研究内容主要为整数分解 (IFP) 与离散对数 (DLP/ECDLP)等传统公钥密码算法困难问题及抗量子加密算法安全性分析。



◎ 抗量子“防”的实力:抗量子产品与生态

- **产品矩阵完备:**率先提出针对银行、通讯、政务等领域的“国密+抗量子加密+量子随机数”安全解决方案,并成功研发具有自主知识产权的抗量子密码卡、抗量子安全网关、抗量子安全模组等产品。
- **算法自主优化:**对主流抗量子算法进行优化改良,并使用国产自主可控“本源悟空”72bit第三代超导量子计算机开展量子算法攻击PQC算法底层数学问题相关工作。
- **深度参与标准制定:**作为唯一量子计算公司,参与国家《抗量子密码算法迁移》标准编制等工作。

Q U A N T U M C O M P U T I N G

抗量子软件安全密码模块

◎ 产品介绍

抗量子软件安全密码模块支持的密码算法包括国密SM系列算法、NIST标准PQC算法:ML-KEM、ML-DSA、SLH-DSA、国产PQC算法Scloud+、Aigis等。为终端应用提供快速、便捷的“国密+抗量子”加密算法调用能力,轻松实现软件层安全升级。

◎ 产品特点

- **双重安全保障:**支持SM2/SM3/SM4等国密算法,支持ML-KEM、ML-DSA、SLH-DSA等抗量子密码算法。
- **开箱即用:**提供原子接口,用户无需研究混合算法逻辑,可根据自身业务逻辑进行二次封装,减少业务开发周期,为现有业务提供国密算法+抗量子密码算法双重安全加密。
- **全栈兼容:**除适用于Windows, Linux, Android, IOS等主流平台系统外,还兼容银河麒麟和阿里龙蜥等国产操作系统,便于开展信创产品的开发。并且提供C/C++、Python、Java、JavaScript等不同开发语言版本,可快速集成至传统应用,移动互联网,物联网等领域应用。
- **无缝衔接,便于业务实现安全升级:**已实现同密码卡等硬件安全密码模块接口对齐,支持同安全硬件相互加密解密,签名验签等业务,从而实现业务安全升级,减少业务开发工作量。

◎ 典型应用场景

移动App加密、物联网终端通信、云原生应用、信创软件安全增强。

产品介绍

密码卡是 PKI(Public Key Infrastructure, 公钥基础设施)系统中的以 PCI、PCI Express 总线为接口的基础密码设备,具有密码运算功能、密钥管理功能、随机数产生功能和设备自身安全保护措施硬件加密设备。在密码安全应用场景,密码卡是信息安全系统中的重要的硬件保障。

本源磐石抗量子密码卡产品是本源量子自主研发的基础密码设备,能够适用于各类密码安全应用系统,提供高性能的密码运算和安全存储功能,可以满足应用系统数据的数字签名,数据加密的要求,保证传输信息的机密性、完整性和有效性,同时提供安全、完善的密钥管理机制。密码应用系统通过调用密码卡提供的标准接口函数来使用密码服务,接口函数符合《GM/T 0018-2023 密码设备应用接口规范》,通用性好,能够平滑接入各种系统平台,满足大多数应用系统的要求,在应用系统安全方面具有广泛应用前景。



产品特点

- **内嵌量子随机数发生器(QRNG):**QRNG是当前唯一一种可被证明真随机的随机数发生装置,其随机数具有不可被预测、不可被回溯以及无数字模式等随机特性,具备信息论安全性,是信息安全系统中面向未来的密钥源。
- **支持多种主流密码算法,满足不同安全需求:**支持国际主流密码算法RSA/AES,支持SM1/SM2/SM3/SM4等国产密码算法,支持ML-KEM(Kyber)/ML-DSA(Dilithium)等抗量子密码算法。
- **高速加解密运算:**采用高性能主控芯片及加密芯片,能够实现高速加密和解密运算。
- **高易用性:**支持Linux/Unix/FreeBSD等32位/64位操作系统,支持基于龙芯、飞腾、神威、海思、鲲鹏等国产处理器的操作系统。

技术参数

算法类型		性能指标
SM1加解密 (Mbps)		2300
SM2	密钥对生成 (Tps)	3.6万
	签名/验证 (Tps)	3.3万/2.5万
	加密/解密 (Tps)	2.5万/3.5万
SM3 (Mbps)		1900
SM4 (Mbps)		2300
抗量子算法性能		
算法类型		性能指标 (Tps)
Kyber512/768/1024	密钥对生成	32000/28000/21000
	密钥封装	36000/28600/22000
	密钥解封装	34600/25500/18800
Dilithium2/3/5	密钥对生成	28000/21000/13700
	签名	17900/8100/5500
	验证	28400/20000/13600
量子随机数生成 (Mbps)		20

典型应用

通用密码设备、身份认证设备、网络安全设备、存储加密设备。

抗量子服务器密码机

产品介绍

抗量子服务器密码机是由本源量子自主研发的高性能密码设备,支持抗量子密码算法(Post-Quantum Cryptography, PQC),量子随机数发生器,国密SM1、SM2、SM3、SM4等多种算法,可以满足应用系统数据的签名/验签,加密/解密的要求,保证信息的机密性、完整性和有效性,同时提供安全的密钥管理机制,自身具备较强的安全防护能力。抗量子服务器密码机符合国家密码管理局颁布的GM/T0030-2014《服务器密码机技术规范》、GM/T0028-2024《密码模块安全技术要求》、GM/T0018-2023《密码设备应用接口规范》。

产品特点

抗量子服务器密码机具有如下特征:

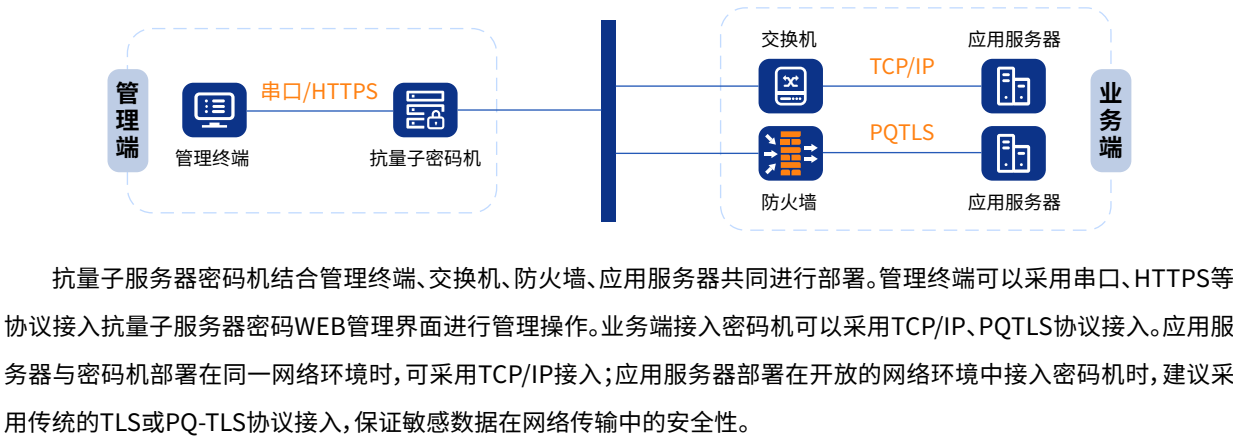
- 完善的算法支持**
 - 支持SM2等国密标准非对称算法;
 - 支持SM1、SM4等国密标准对称算法;
- 支持SM3等杂凑算法**
 - 支持ML-KEM512, ML-KEM768, ML-KEM1024等PQC密钥封装算法;
 - 支持ML-DSA44,ML-DSA65,ML-DSA87等PQC签名、验签、身份认证算法;
 - 支持量子随机数发生器生成真量子随机数。
- 完善的权限控制**
 - 具有完善的分级权限控制机制,分为管理员、审计员、操作员等不通的管理角色,密码机不同的管理操作需要相应管理角色操作;
 - 管理角色载体为USBKEY(智能密码钥匙);
 - 管理角色认证方式基于身份的认证。
- 高可用**
 - 可选配冗余电源,保证设备运行的持续性;
 - 网口支持主备模式绑定,保证网络冗余;
 - 负载由接口层实现,对上层应用透明,部署方式简单。
- 高可维护性**
 - 具备日志审计、状态监控、SNMP标准协议监控、SYSLOG外送日志、NTP时间同步等扩展功能,进一步提高服务器密码机的可维护性。
- 安全密钥存储**
 - 服务器密码机采用三级密钥保护接口,保证关键密钥在任何时候都不以明文形式出现在设备外,密钥备份文件受备份密钥加密保护。

- 安全的访问控制**
 - 具备IP白名单、连接口令等访问控制方式,授权接入的应用客户端请求;
 - 支持基于SM2、PQC的安全通道接入,确保数据传输的安全性。

产品规格

产品版本机型号	抗量子服务器密码机
外观类别	机架式2U
外观	前视图后视图
外观尺寸	560mmx440mmx89mm (长x宽x高)
工作电源	200V, 550W冗余电源
网络接口	2个千兆电口, 2个万兆光口
IPMI接口	1个IPMI口
USB接口	1个USB2.0, 1个USB3.0
密码实现模式	抗量子密码卡
MTBF	≥50000小时
工作环境	0°C~40°C
存储环境	-40°C~60°C
非凝结工作湿度	0%~90%

部署方式



抗量子安全网关

产品概述

抗量子安全网关是本源自主研发的高速网络安全设备，通过网络传输中构建“量子加密”隧道，保障数据在传输过程中的安全。产品部署简单，配置灵活，无需对现有网络进行改动，可广泛应用于政府、公安、能源、交通、税务、企业集团、商业连锁等领域。



产品特点

- 内嵌PCI-e高性能抗量子密码卡；
- 采用ML_KEM/Scloud+抗量子密钥封装算法及ML_KEM和SM2/Scloud+和SM2的混合密钥封装算法，实现IPSec、SSL协议；
- 采用高可靠性、工业级硬件平台，确保7×24小时不间断运行；支持IPSec断线重连，60秒内自动恢复可用；双机热备；负载均衡；
- 旁路部署方式，无缝接入原有网络以及原系统。

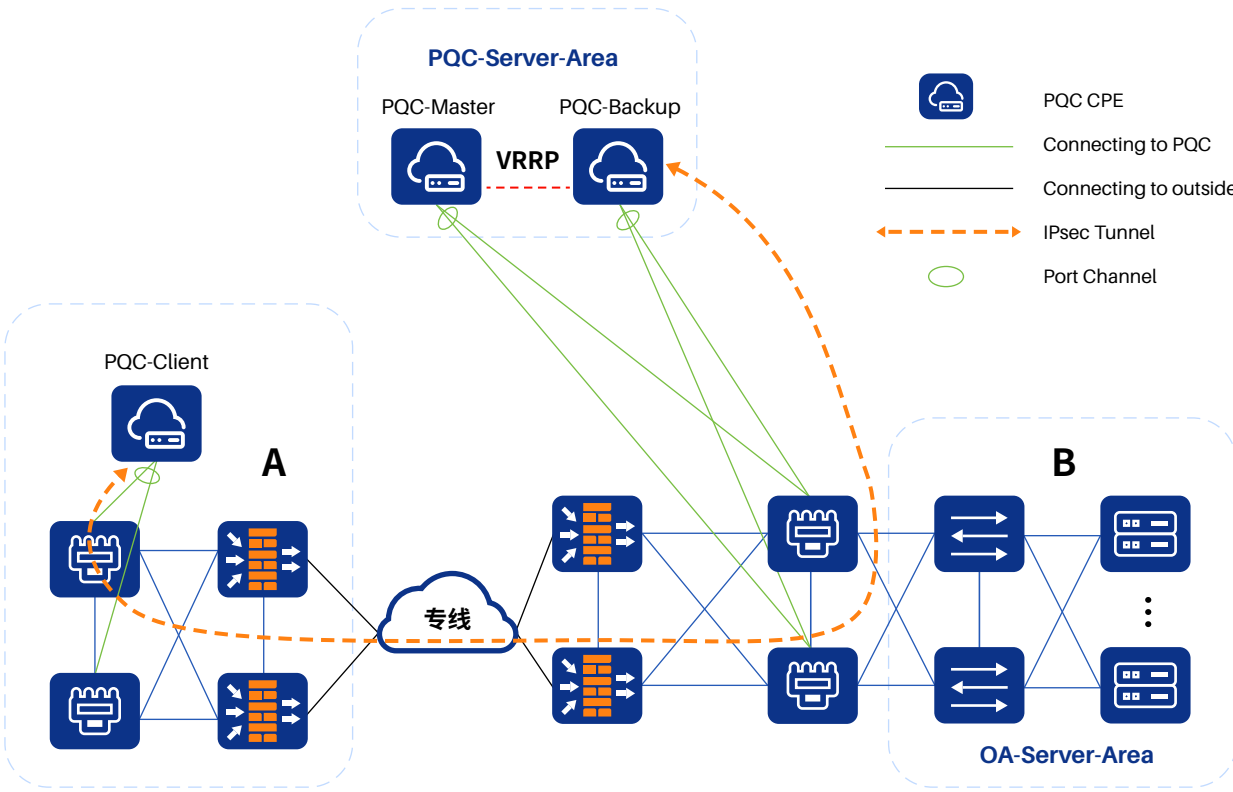
产品参数

类型	功能与参数	抗量子安全网关
硬件参数	外形尺寸	1U机架式
	网络接口	2.5G网口=6 10G光口=2
	电源	额定功率250w, 100-240V宽屏电压
	工作温度	0℃ 至 50℃
	存储温度	5℃ 至 90℃
	湿度	10% 至 90% 非凝结
	安全设备	支持本源量子自主知识产权的抗量子密码卡硬件(可选)

性能参数	抗量子算法性能	密钥生成速率>=20000Tps 密钥封装速率>=20000Tps 密钥解封装速率>=20000Tps 量子随机数生成速率>=20Mbps
	隧道数	>=1000
	吞吐量	>=2.0Gbps
	链路聚合吞吐量	单链路:2.35 Gbps 双链路:4.59 - 4.69 Gbps 三链路: 6.72 - 6.79 Gbps

应用案例

某医疗机构通过部署量子安全网关设备，构建了从运维办公区到数据中心的量子安全链路。在数据交互过程中，发送端的量子安全网关利用抗量子加密算法对数据进行实时加密处理，数据以密文形式安全传输至接收端。接收端部署的量子安全网关则通过配套解密算法解析密文，恢复数据并验证其完整性，利用端到端加密机制，有效抵御量子计算机威胁，保障医院关键数据在传输过程中的机密性与完整性，为医院信息提供安全可靠的防护。



抗量子安全模组

产品介绍

量子安全模组是一款融合量子技术与加密算法的高性能安全组件，旨在解决传统密码学面临的量子计算破解风险，同时满足当前数字系统对信息安全的合规性与可靠性需求，为金融、政务、物联网等领域提供“当下安全、未来抗量子”的双重防护支撑。

产品特点

- 内置量子随机数 (QRNG) 芯片，根源保障随机源安全
 - 双算法兼容，兼顾合规与抗量子能力
 - 支持国密算法：兼容 SM2 (非对称加密)、SM4 (对称加密)、SM3 (哈希函数) 等国内商用密码标准，完全符合政务、金融等领域的合规要求，可直接适配国内现有数字系统，无需大规模改造底层架构。
 - 集成抗量子加密算法：搭载 NIST 推荐的 ML-KEM (格基密码)、ML-DSA (数字签名) 等抗量子算法，可抵御未来量子计算机对传统密码学 (如 RSA、ECC、SM2) 的破解威胁，实现 “一次部署，长期安全”，避免因量子技术迭代导致的产品淘汰风险。
 - 轻量化设计，高灵活适配多载体
- 模组采用小型化封装 (尺寸可低至 [25] mm×[25] mm×[3] mm)，可无缝集成至 USB Key (身份认证密钥)、TF 卡 (移动存储加密)、智能终端 (如手机、物联网传感器)、服务器等多种载体，适配个人信息安全、移动办公加密、物联网终端接入等不同场景。支持标准化接口 (UART接口/SPI接口/USB接口)，集成周期短，降低企业应用成本。

典型应用场景

- 金融领域：交易与数据安全防护
- 集成至银行 UKey，通过 QRNG 生成交易密钥，结合抗量子算法实现转账签名、账户登录认证，防止量子计算机破解传统密钥导致的资金被盗风险；
- 政务领域：身份认证与公文加密
- 适配政务终端设备 (如政务电脑、移动执法终端)，通过国密算法完成公务员身份认证，结合抗量子算法加密传输电子公文、敏感政务数据，确保政务信息在传输、存储过程中的安全性与合规性，符合国家“量子安全政务”建设要求。

- 物联网领域：终端安全接入

集成至物联网传感器、智能设备，利用轻量化特性实现设备身份加密认证，通过抗量子算法保护设备间通信数据 (如工业物联网设备指令传输、智能家居数据交互)，解决物联网终端“数量多、算力弱、易被攻击”的痛点，构建抗量子的物联网安全生态。

抗量子安全U盾

产品介绍

量子安全U盾 (又称USBKey或USBToken)，是基于量子安全模组自主研发的新一代网络身份认证产品，实现国密与抗量子混合加密算法等高强度算法，达到金融安全级别，并支持主流内核浏览器，可实现网页安全登录、安全信息交互、VPN证书安全登录等。



产品特点

- 内嵌量子随机数 (QRNG) 芯片
- 支持多种通讯协议，包括：HID、CCID、USBMassStorage 以适应用户多种需求
- 支持Windows 10/Linux操作系统
- 支持中科方德/中标麒麟国产操作系统

应用场景



移动办公/作业



移动电子政务



终端数据保护

抗量子安全TF卡

产品介绍

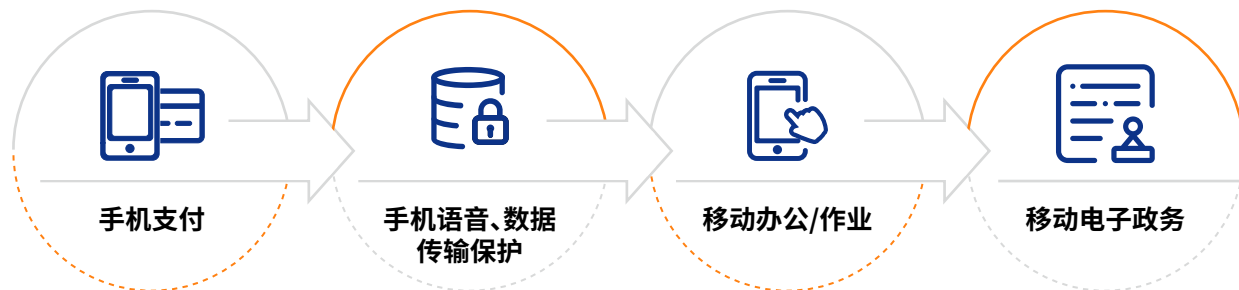
量子安全TF卡物理外观、接口和标准TF卡完全一致,内置量子安全模组,可将量子加密密钥方便的融入手机、PAD等移动通信终端,最大限度保护用户敏感数据及运算的安全性,并提供4G -16G 安全存储,在满足移动智能设备外扩存储需求的同时提供基于量子加密的移动安全服务。



产品特点

- 内嵌量子随机数 (QRNG) 芯片
- TF 接口
- 大容量安全数据存储区
- 支持GM/T 0016-2012 智能密码钥匙密码应用接口规范

应用场景



抗量子安全云桌面操作系统

产品介绍

由本源量子和中科方德联合研发的桌面操作系统,通过深度整合量子安全技术(PQC+QRNG)和云虚拟化技术,实现终端接入、数据传输、存储加密、身份认证的全链路量子安全防护,为政务、金融、能源等关键行业提供“量子免疫”级别的办公环境。



产品特点

- 量子增强安全身份认证
采用抗量子签名算法+QRNG等多因素认证机制。
- 全链路加密传输
结合量子安全网关产品,可实现数据传输的“量子级”安全加密。
- 系统高效兼容
支持海光、兆芯、飞腾、龙芯、申威、鲲鹏等国产CPU平台和Intel/AMD平台,支持台式机、笔记本、一体机等多种形态整机。
- 应用丰富、便捷易用
预装的方德软件中心应用软件丰富,良好支持金山WPS Office、永中Office、LibreOffice等办公套件。

应用场景

安全办公、远程运维或接入、终端设备固件签名

抗量子安全手机

◎ 产品介绍

中国联通与本源量子共同推出首款抗量子安全手机,由中国联通“量子要谈”APP和量子超级SIM卡两大核心产品构成,是针对政务场景推出的一款加密安全即时通信应用。



中国联通“量子要谈”APP

- 深度融合抗量子密码算法(PQC)与国密算法;
- 有效抵御量子计算攻击及网络窃听风险;
- 端到端加密通信能力,有力守护用户通信安全。



量子超级SIM卡

- 国密安全芯片+量子随机数生成芯片“双芯融合”架构;
- 实时生成符合量子力学原理的“真”随机密钥;
- 密钥安全存储、生成、分发、销毁。

◎ 产品优势

● 金融领域:交易与数据安全防护

抗量子算法与量子密钥协同构筑加密通信的双重防线。抗量子算法抵御量子计算攻击,保障数据安全;量子密钥“真随机”、无条件安全分发,确保密钥传输可靠。两者互相协作融合,有效应对量子时代安全挑战。

● 洞察需求,功能更丰富

中国联通“量子要谈”应用具备加密音/视频通话、多模态加密即时消息收发、文件加密传输、单聊/群聊、准入认证、防截屏/录屏等加密通信能力,还可根据客户需求定制设备管控、终端安全加固、企业内容定制等安全增强能力。

● 权威认证,安全有保障

产品的抗量子计算攻击的能力已通过中国科学院量子信息重点实验室权威评估,内嵌量子器件满足国标要求,量子超级SIM卡及量子要谈已获得公安部、工信部、国家密码管理局及信通院的权威认证。

量子超级SIM卡

◎ 产品介绍

采用在SIM卡中植入国密安全芯片与量子随机数芯片,国密芯片内嵌入SM2、SM3、SM4国密算法,量子随机数芯片用于产生真随机数,结合抗量子密码算法,并与自建CA或第三方CA系统对接,打造实名身份认证和量子国密安全能力,具备身份鉴别、安全加解密、数字签名、网络准入等功能,保障移动终端系统用户/设备身份的真实性和数据的机密性。

