

量子密码卡

产品型号：SM-GM019



(图片仅供参考, 请以实物为准)

作为基于量子随机数发生器模组和支持国密密码芯片设计的一款高速量子密码卡，量子密码卡符合国家密码管理局关于PCIe密码卡的相关技术规范，支持国密算法和后量子密码算法，能够为可信计算等各类安全平台提供多线程、多进程和多卡并行处理的高速密码运算服务，可满足数字签名/验证、非对称/对称加解密、数据完整性校验、量子随机数生成、密钥生成和管理等功能要求，保证了敏感数据的机密性、真实性、完整性和抗抵赖性。

功能特性：

采用量子随机数

满足GM/T 0062 - 2018《密码产品随机数检测要求》、GB/T 32915 - 2016《信息安全技术二元序列随机性检测方法》、YD/T 3907.3 - 2021《基于BB84协议的量子密钥分发（QKD）用关键器件和模块第3部分：量子随机数发生器（QRNG）》、《NIST 800-90A/B/C》以及国密局《两类量子随机数生成器检测要求（修订稿）》等标准要求

国密算法库支持

用户态接口参考GM/T 0018-2012《密码设备应用接口规范》，支持该规范中的用户应用程序调用接口。内核态驱动支持调用国密算法接口

高性能

支持SM1、SM2、SM3、SM4和SM9等国密算法和后量子密码算法，SM4算法性能>10G

产品特点：

高度安全性

➢ 利用由国家密码局批准的多随机源生成量子随机数，从而提高了密码学算法的安全性和不可预测性。

兼容国家密码标准

➢ 符合国密标准，满足国家对信息安全的要求，方便在政务、金融等领域的应用。

集成度高

➢ 将量子随机数生成器集成到密码卡中，提高了设备的集成性和便携性。

支持多种算法

➢ 支持多种加密算法，满足不同的安全需求。

后量子密码

➢ 支持后量子密码，可抵御量子计算攻击。

量子密码卡

应用场景：

量子密码卡是基于量子随机数、国产密码与后量子密码的高安全性硬件设备，主要应用于对通信安全要求高的领域，能够有效抵御传统计算攻击和未来量子计算的威胁。其核心原理是利用量子物理原理，提高了密钥和密码算法的安全性和不可预测性。其应用场景广泛覆盖政务、国防、金融、医疗、能源、交通等重要行业和领域，通过量子密码技术保护重要数据传输、业务安全通信等，确保信息在传输过程中即使被截获也无法解密，可作为抵御量子计算攻击的关键基础设施。

量子密码卡通过与信创、商用密码等技术相结合，为未来网络提供了量子安全的底层支撑，成为保障国家战略安全和用户核心数据的重要技术手段。

客户价值：

- 全国产化量子密码安全组件，符合国家密码局标准规范要求，可满足国密改造应用需求
- 基于量子物理原理的安全防护，有效抵御传统计算攻击和未来量子计算威胁
- 支持多种算法的高性能国密加密，构建面向抗量子攻击的未来安全防护体系
- 提供标准服务接口，对接方式高可用、高易用，为业务应用对接提供保障服务
- 可满足业务应用的高等级安全需求，为行业客户提供面向未来的安全解决方案



浙江之江数安量子科技有限公司

电话：0571-85361889

官网：www.zjquantum.cn

地址：浙江省杭州市余杭区仓前街道文一西路1378号E幢1903室