C*Core Technology Co.,Ltd.

2024年国芯科技
量子安全芯片和模组技术与产品
白皮书

苏州国芯科技股份有限公司

2024年11月

目录

1. 企业介绍

国芯科技（股票代码：688262）是一家聚焦于国产自主可控嵌入式 CPU 技术研发和产业化应用的芯片设计公司。公司致力于服务安全自主可控的国家战略，为国家重大需求和市场需求领域客户提供 IP 授权、芯片定制服务和自主芯片及模组产品，主要产品应用于信创和信息安全、汽车电子和工业控制、人工智能和先进计算三大关键领域。公司已成功实现基于“PowerPC 指令集”、“RISC-V 指令集”和“M*Core 指令集”的 8 大系列 40 余款 CPU 内核，实现了多发射乱序执行、多核总线一致性架构、多核锁步以及多级 Cache 等主流架构设计，并同步研发了软件集成开发与调试工具链，实现对多种嵌入式操作系统的支持。公司在国内首先实现累计上百万颗、上千万颗和上亿颗应用，并于 2022 年 1 月 6 日登陆上交所科创板。

在信创和信息安全领域，公司重点发展云安全芯片、RAID 存储控制芯片、量子安全芯片和端安全芯片，覆盖云计算、大数据、物联网、智能存储、工业控制和金融电子等关键领域，以及智能终端、服务器等重要产品，信创和信息安全芯片累计出货超 2 亿颗。

国芯科技将信创和信息安全芯片与量子技术相结合，基于参股公司合肥硅臻芯片技术有限公司研发的量子随机数发生器开发了量子安全芯片、终端应用量子安全模组及服务器和云应用量子安全模组，可广泛应用于电力、通信、金融、安防、政务等领域和智能终端、网关、服务器等产品中。

公司先后承担和完成了多项国家重大科技项目，包括“核高基”国家科技重大专项、国家 863 计划，国家高技术产业发展项目、国家技术创新项目和工信部工业转型升级项目等数十项，获得国家科技进步二等奖等。

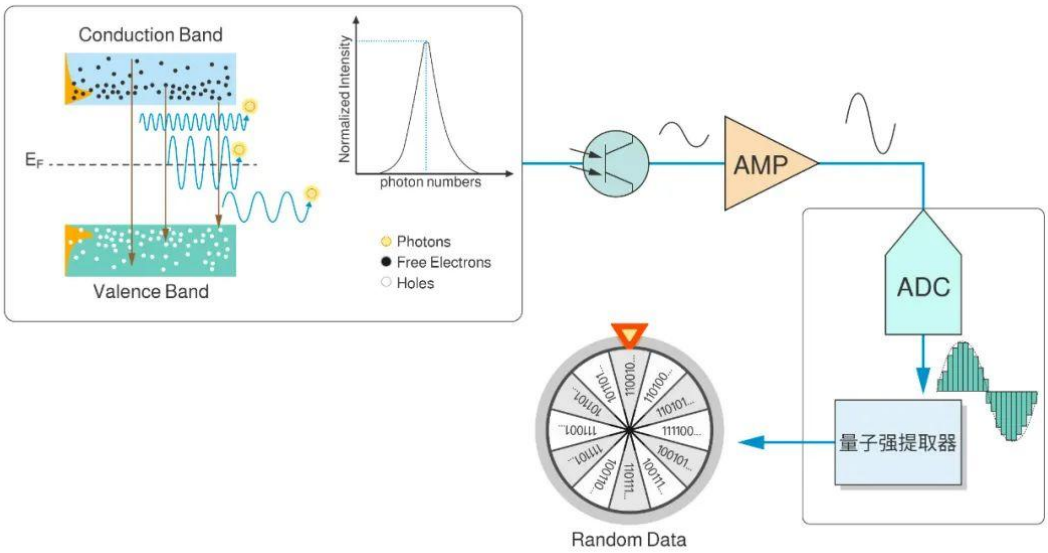
公司担任江苏省集成电路设计产业联盟副理事长、江苏省商用密码产业协会副理事长和苏州市半导体行业协会会长等。

2. 量子随机数发生器

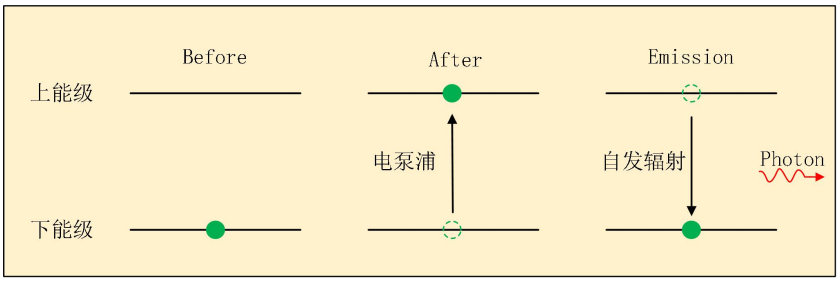
随机数是信息安全系统生成密钥的核心，是每一款信息安全产品的必要组成部分，随机数的随机性直接决定了信息安全系统的可靠性。

随机数分为伪随机数和物理随机数，根据发生器的不同又可将物理随机数分为基于经典噪声的随机数和基于量子噪声的随机数。相比于伪随机数发生器和经典噪声随机数发生器，量子随机数发生器的优势体现在其基于量子力学的理论可证的不可预见性上。量子随机数发生器是依据量子力学的概率性本质设计运行的，目前在理论上被严格证明能产生完全不可预知随机序列。

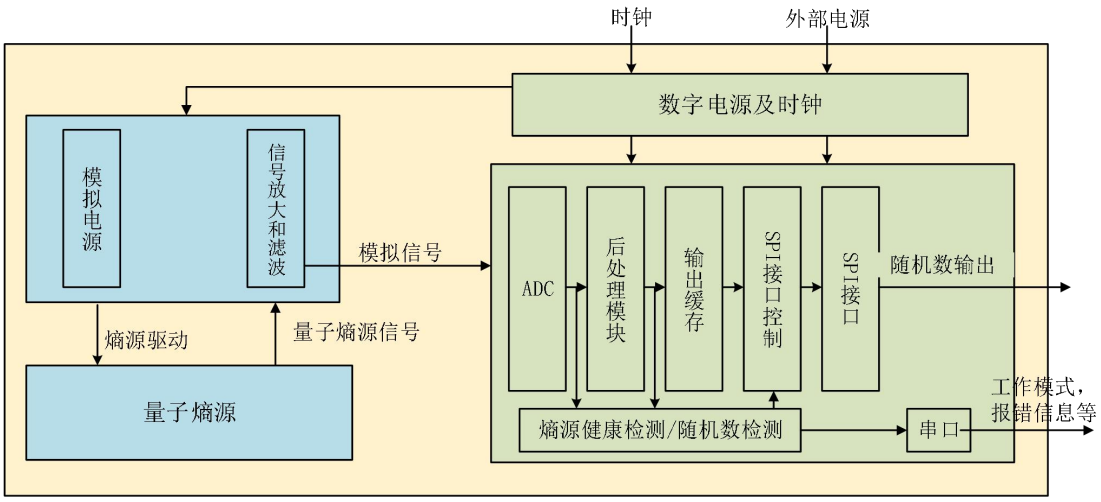
国芯科技的参股公司合肥硅臻芯片技术有限公司研发的量子随机数发生器，基于量子力学原理提供超高质量的随机数，其随机性源于放大自发辐射原理，具有可证明的内禀随机性。量子熵源选用自发辐射光源结构作为量子光源，同时采用高灵敏度光电探测器去对自发辐射光束中的量子散粒噪声进行探测和量化。另外，量子信号采集与提取模块集成了后处理计算核心以及熵源健康检测核心和随机数检测核心等保证和监控随机数生成质量的数字电路。



量子光源中半导体材料里电子在外部能量泵浦下，由基态跳跃到激发态，由于激发态是不稳定的一种能级状态，在未来某个时间点，电子会由激发态回到基态，此时发生出一个光子。由于光子发生时间是随机的，所以在单位时间内对光子数进行统计时，会得到一个随机的光子数分布。



熵源健康检测核心通过对量子熵源输出的原始随机信号进行实时检测，保证熵源工作正常，同时随机数检测核心则按照相关标准对最终输出的随机数进行检测，保证其满足相关随机性要求。



3. 量子安全芯片 A5Q

作为信息安全产品的核心部件，安全芯片自身的安全直接影响信息安全产品的安全，所以安全芯片应具有安全存储、安全版图、入侵检测、算法安全和权限管理等特性，可有效抵御旁路、物理、故障和软件等攻击手段。将安全芯片与量子随机数发生器相结合，可进一步提升安全芯片的安全防护等级。

A5Q 芯片是由公司端安全芯片 A5、光信号处理芯片 AGC001 和两颗光量子噪声源芯片采用多芯片封装技术合封而成，其中 AGC001 和光量子噪声源芯片为公司参股公司合肥硅臻芯片技术有限公司产品。可以代替传统的 SE 芯片，应用到各类信息安全终端上。该芯片按照 GM/T 0008《安全芯片密码检测准则》第二级要求设计，具有低功耗、高性能、多功能及高安全性等特点。

■ **功能特点**

- ✓ CPU：国芯自主 32 位安全内核 CSO
- ✓ 工作频率：典型 100MHz
- ✓ 通信接口：SPI/USB/SD/UART
- ✓ 接口电平：3.3V/1.8V
- ✓ 存储资源：256KB SRAM，1280KB EFLASH
- ✓ 随机数：量子随机数发生器
- ✓ 加密算法：DES/AES/SM4 对称算法，RSA/ECC/SM2 非对称算法， SHA/SM3 哈希算法
- ✓ 封装：LGA36
- ✓ 尺寸：5.5*5.5*1mm
- ✓ 工作温度：-40℃~85℃

4. 终端应用量子安全模组

终端应用量子安全模组通过硬件加密、物理防护、密钥管理、身份认证机制、数据传输加密等多种手段来保障产品安全性，依托于量子随机数发生器生成的量子密钥，进行数据加解密保护，使数据存储访问更加安全。量子安全模组按照 GM/T 0027《智能密码钥匙技术规范》和 GM/T 0028《密码模块安全技术要求》第二级要求设计，适用于 Windows、Linux 等多种操作系统，可广泛应用在 PKI 认证、数字签名、数据加解密等方面。

4.1 量子 USBKEY CCUMU2Q01

■ **功能特点**

- ✓ 主控芯片：国芯 CCM3310S-T 安全芯片
- ✓ 通信接口：USB2.0 高速接口

- ✓ 用户空间：128K 字节
- ✓ 随机数：量子随机数发生器
- ✓ 加密算法：DES/AES/SM4 对称算法，RSA/ECC/SM2 非对称算法， SHA/SM3 哈希算法
- ✓ 算法性能：SM2 签名 110 次/秒，验证 80 次/秒；SM3 运算 90Mbps；SM4 加解密 70Mbps

4.2 高速量子 USBKEY CCUMU3Q02

- ■ **功能特点**
- ✓ 主控芯片：国芯 CCM3305S 安全芯片
- ✓ 通信接口：USB2.0/3.0 高速接口
- ✓ 用户空间：256K 字节
- ✓ 随机数：量子随机数发生器
- ✓ 加密算法：DES/AES/SM4 对称算法，RSA/ECC/SM2 非对称算法， SHA/SM3 哈希算法
- ✓ 算法性能：SM2 签名 1100 次/秒，验证 800 次/秒；SM3 运算 350Mbps；SM4 加解密 450Mbps

5. 服务器和云应用量子安全模组

服务器和云应用量子安全模组依托于高速量子随机数发生器生成的量子密钥，满足数字签名/验证、非对称/对称加解密、数据完整性校验、密钥生成和管理等功能需求，保证敏感数据的安全性、真实性、完整性和抗抵赖性。量子安全模组按照《PCI 密码卡技术规范》、GM/T 0018《密码设备应用接口规范》和 GM/T 0028《密码模块安全技术要求》第二级/三级要求设计，其中《密码模块安全技术要求》第三级要有更强的物理安全机制，以进一步防止外界对密码模块内敏感数据的非授权访问。量子安全模组支持 Windows、Linux 以及麒麟、UOS 等系统，适配龙芯、飞腾、兆芯、海光等多种平台。为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。

5.1 量子 Mini PCI-E 密码卡 CCUPM2Q04

■ **功能特点**

✓ 主控芯片：国芯 CCM3305S 安全芯片

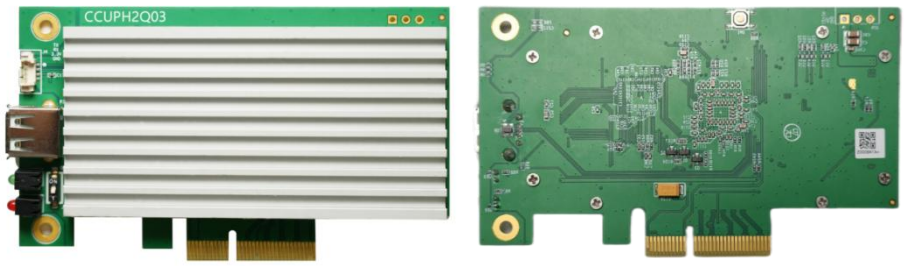
✓ 通信接口：Mini PCI-E2.0

✓ 随机数：量子随机数发生器

✓ 加密算法：DES/AES/SM4 对称算法，RSA/ECC/SM2 非对称算法，SHA/SM3 哈希算法

✓ 算法性能:SM2 签名 1100 次/秒,验证 800 次/秒;SM3 运算 330Mbps;SM4 加解密 430Mbps

5.2 量子 PCI-E 密码卡 CCUPH2Q03



■ **功能特点**

✓ 主控芯片：国芯 CCP907T 安全芯片

✓ 通信接口：PCI-E3.0

✓ 随机数：量子随机数发生器

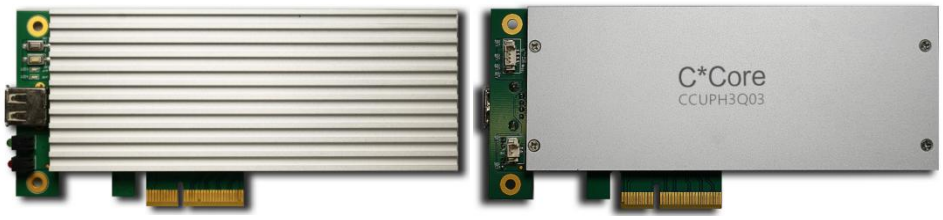
✓ 加密算法：DES/AES/SM4 对称算法，RSA/ECC/SM2 非对称算法，SHA/SM3 哈希算法

✓ 算法性能：SM2 签名 36000 次/秒，验证 35000 次/秒；SM3 运算 20Gbps；SM4 加解密

20Gbps；

- ✓ 安全特性：按照 GM/T 0028《密码模块安全技术要求》第二级要求设计

5.3 量子 PCI-E 密码卡 CCUPH3Q03



- ■ **功能特点**

- ✓ 主控芯片：国芯 CCP907T 安全芯片
- ✓ 通信接口：PCI-E3.0
- ✓ 随机数：量子随机数发生器
- ✓ 加密算法：DES/AES/SM4 对称算法，RSA/ECC/SM2 非对称算法，SHA/SM3 哈希算法
- ✓ 算法性能：SM2 签名 36000 次/秒，验证 35000 次/秒；SM3 运算 20Gbps；SM4 加解密 20Gbps；
- ✓ 安全特性：按照 GM/T 0028《密码模块安全技术要求》第三级要求设计
  - 防拆卸、防钻孔探测的安全屏蔽盖
  - 基于身份的鉴别机制
  - 提供非入侵式攻击缓解技术的有效性证据和测试方法
  - 有效防止电压、温度超出模块正常运行范围对密码模块安全性的破坏

6. 量子安全产品的应用

量子安全芯片和量子安全模组在多个领域有着广泛的应用场景，其不仅可以提供强大的数据保护能力，还可以支持复杂的身份认证和访问控制机制。

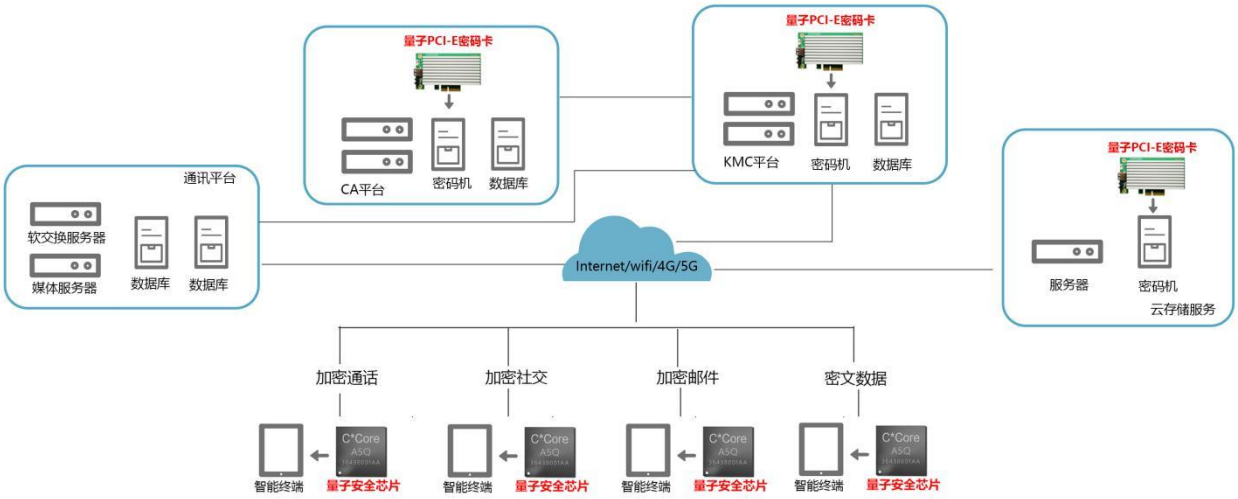
量子安全芯片结合量子安全技术赋能传统密码体系，助力各类终端产品信息安全技术的全面升级。

量子 Mini PCI-E 密码卡可用于 VPN 安全网关、身份认证网关、安全交换机、防火墙，量子 PCI-E 密码卡可用于签名验签服务器、数据库加密机、云安全服务器、服务器密码机等产品中，进一步提升安全产品的安全防护等级。

国芯科技量子安全芯片和量子安全模组可用于如下典型应用场景。

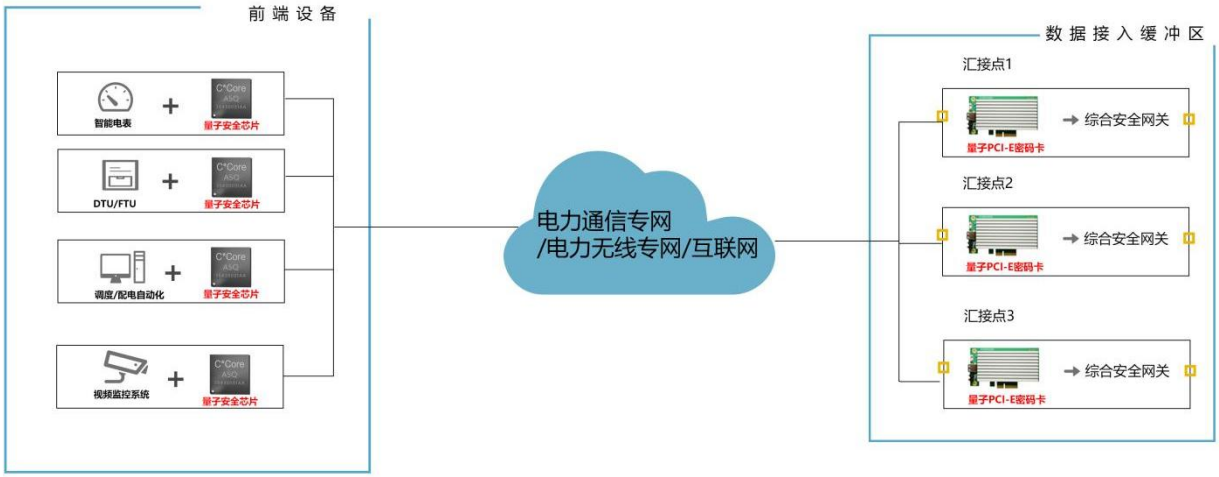
6.1 智能终端应用

随着移动互联网的发展，智能终端已成为人们日常生活和工作中不可或缺的一部分。然而，智能终端的通信信息及存储的如个人隐私、金融账户、商务信息等数据面临着被泄露或窃取的风险。将量子安全芯片应用于智能终端，同时量子 PCI-E 密码卡应用于 CA、KMC 及云存储平台，可实现通信安全、数据安全、金融安全、系统安全和云安全。



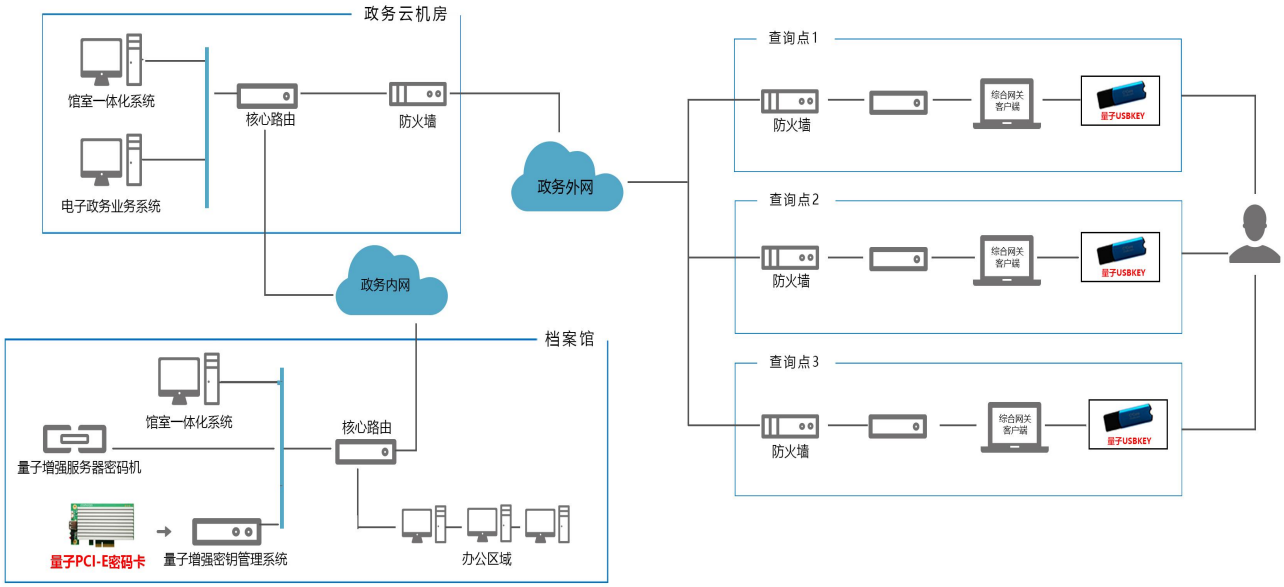
6.2 电力应用

电力系统是国家关键基础设施的重要组成部分，随着电力系统的智能化和信息化程度不断提高，电力系统面临的安全威胁也日益增加。量子安全产品在电力系统中的应用具有重要意义，可实现用电数据的加密传输和校验、电力控制的权限管理、设备的安全接入等，可显著提升电力系统的安全性和可靠性。



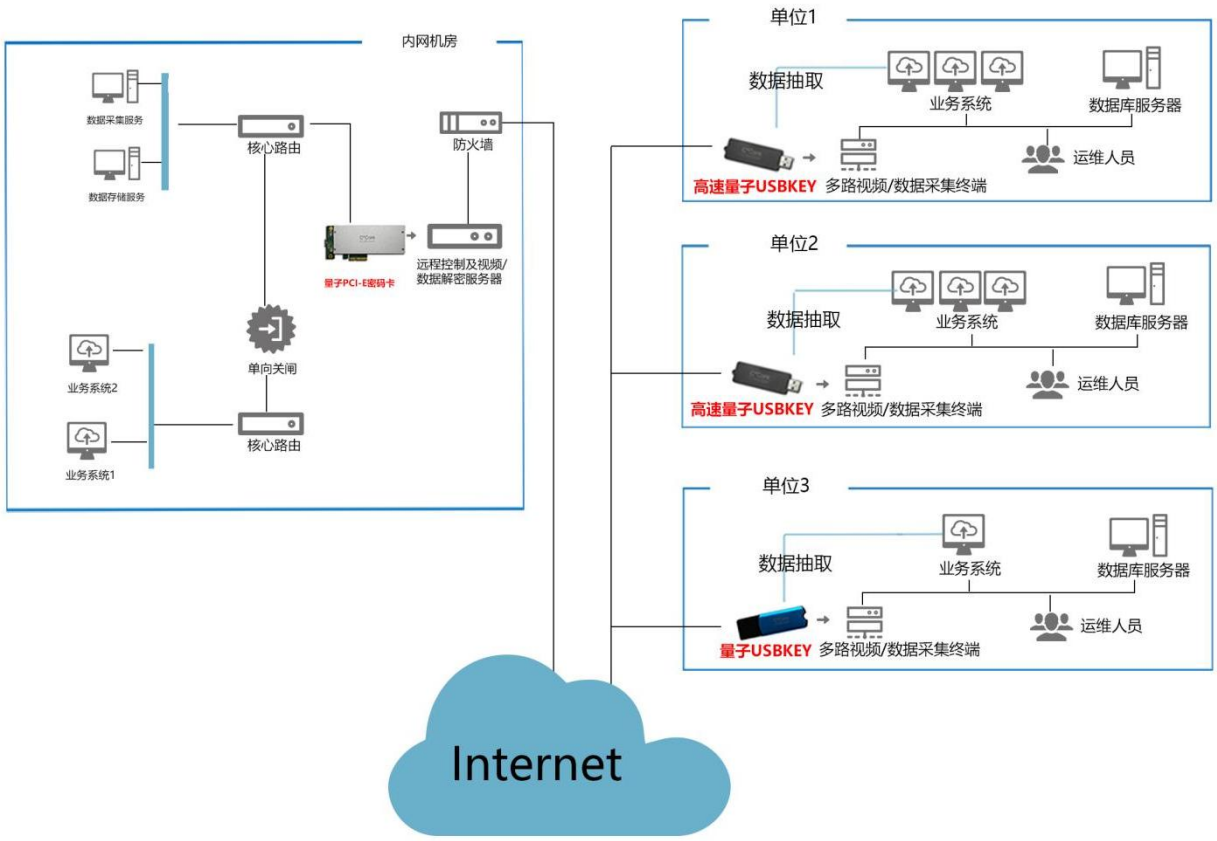
6.3 电子政务

量子安全产品在电子政务领域的应用可实现身份认证、安全隔离、信息加密、完整性保护及抗抵赖性等功能，协助保护政府数据和信息系统免受各种威胁，保障电子政务服务的正常运行和公众信任。



6.4 视频监控系统

在现有视频监控系统的基础上，根据国家信息安全领域内的相关法规，应用 PKI 体系的密码技术，使视频监控系统具备前端设备身份认证、用户身份认证、平台身份认证、视频加密解密、控制信令的完整性验证等功能。



7. 展望

随着集成电路设计水平、封装材料和封装工艺的进步，量子随机数发生器向着更小体积和更高性能发展，这为满足更多行业应用的量子安全芯片和量子安全模组的设计创造了条件。国芯科技将抓住量子安全带来的历史机遇，持续推出系列化量子安全芯片及量子安全模组，满足更多的应用场景，为更多领域赋能量子安全。

C*Core Technology Co.,Ltd.

官网

微信公众号

苏州国芯科技股份有限公司