



# QKDN-ICT融合密码应用 助力数据安全自主可控



# 背景介绍

## 量子计算威胁临近RSA的安全性受到威胁

### 目前公钥主要基于三大数学困难性问题:

- 大整数分解数学困难性问题: RSA, Paillier 等;
- 有限域离散对数困难性问题: Elgamal, DH, DSA 等;
- 椭圆曲线群离散对数困难性问题: ECDH, ECDSA, SM2 等。

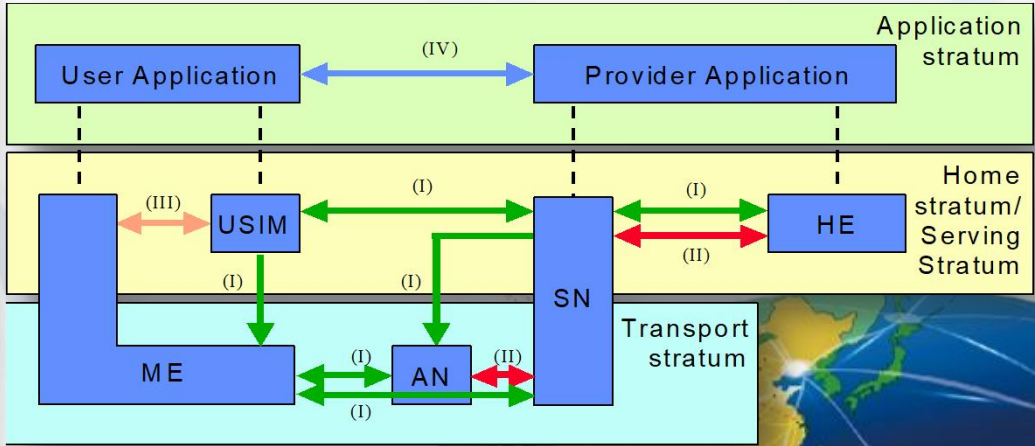
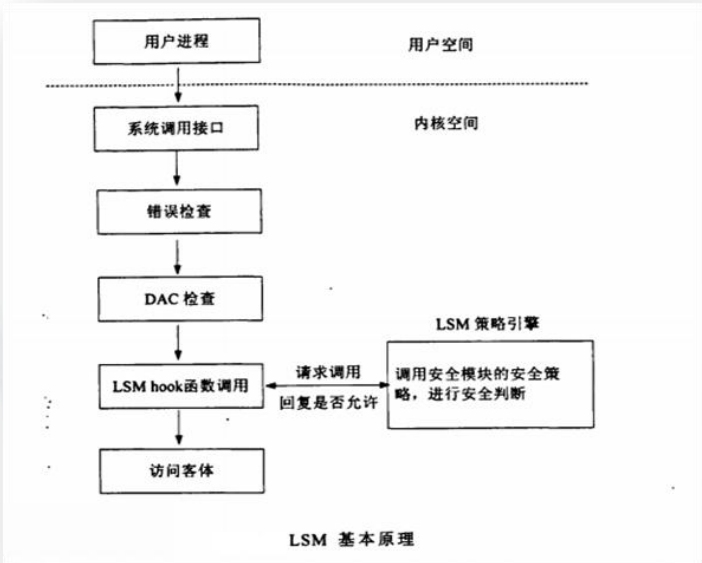
这三大问题在图灵计算模型下尚未发现有效的攻击算法



经典密码破译

1994年, P.W.Shor 给出了一种量子算法, 在量子计算模型下可在多项式时间内解决上述三大数学困难性问题。这意味着基于上述数学困难性问题的公钥密码算法在量子计算模型下已不再安全。

## 信息安全的上游逻辑: 安全层通过控制协议成为业务逻辑及可靠性逻辑的必要环节



# 数据时代来临：共性资源平台化、逻辑定义个性化

## — 平台/网络对应客户和商务模式



## 无法规避云原生安全



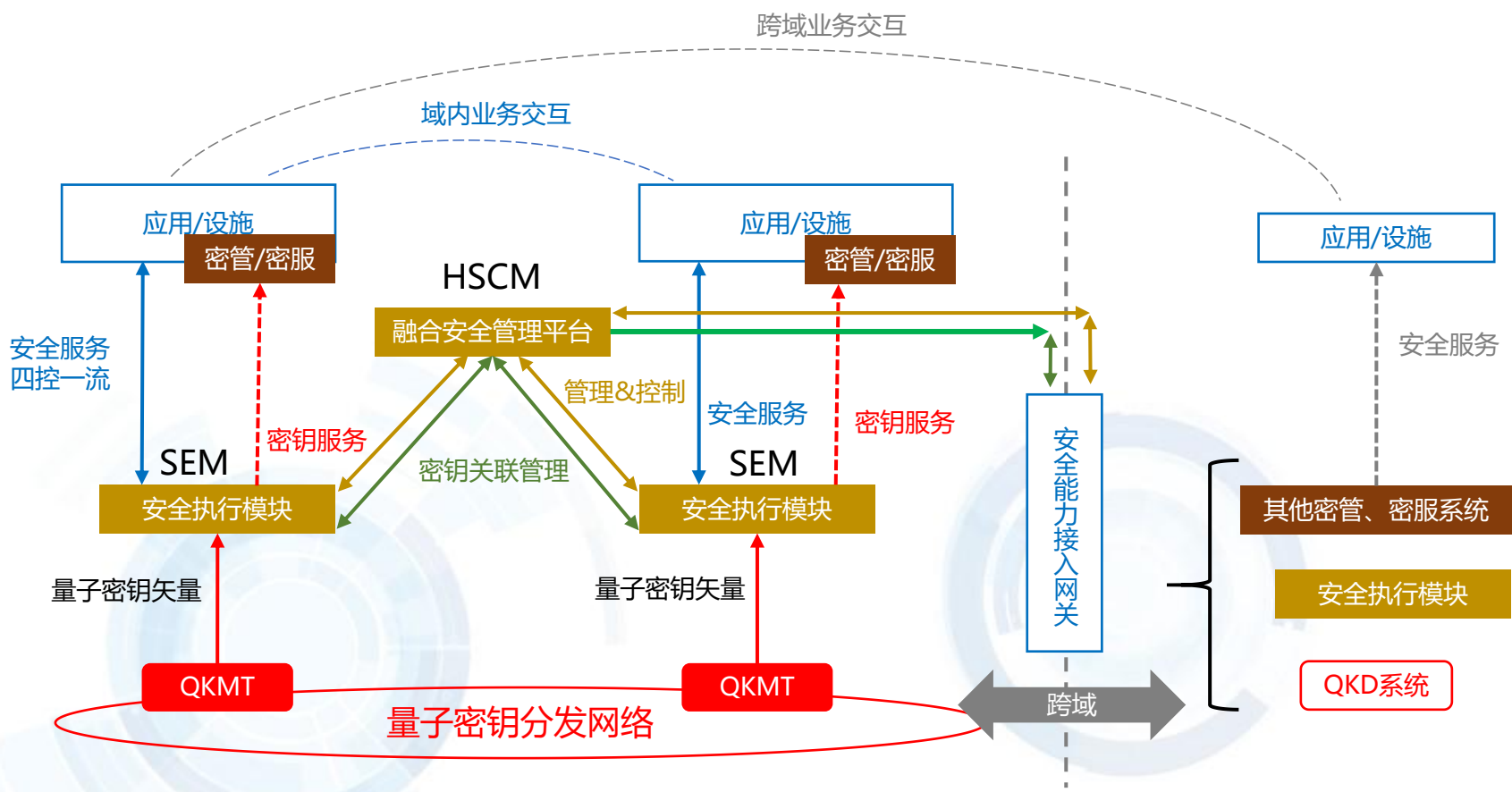




# 结合QKDN能力的融合密码应用体系

## — 基于量子密钥分发网络的密码应用系统（安全责任上收、跨域密钥矢量转移）

当业务和数据在多云、多点环境流转时，利用QKDN（量子密钥协商网络）的密钥矢量协商共享能力，实现特征密钥更新，支持密码应用系统结合业务（包括安全业务、平台和数据等），利用API实现独立的认证、数据和参数保护、策略保护及关键进程保护，构建可控数据执行存储环境，将量子密钥应用作为业务逻辑和可靠性逻辑的必要环节，并为介入管理和新型增值业务提供支撑。



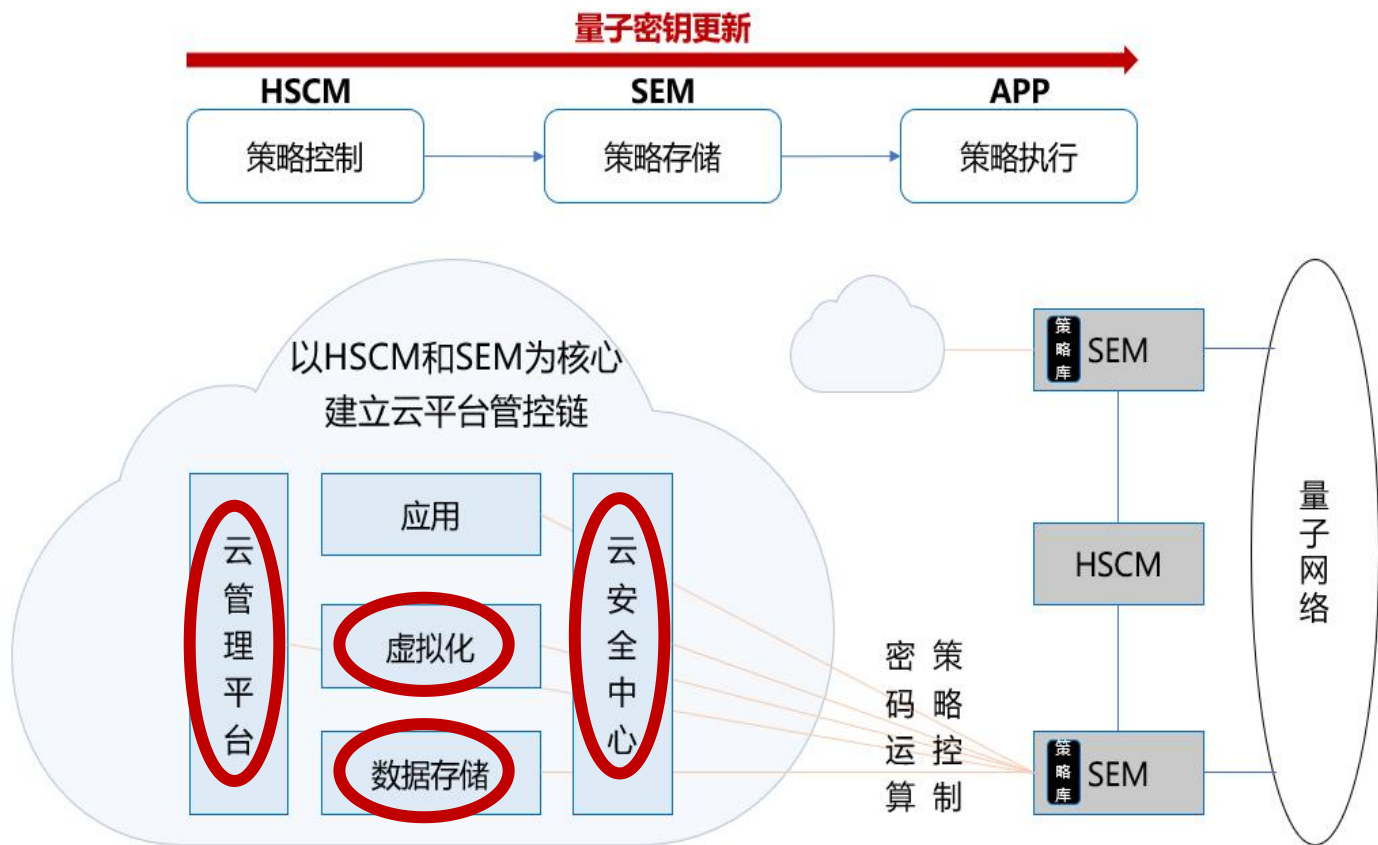
- 安全互控、流量控制、密钥生命周期管理、管理KPI和用户广义流量:
- 认证
  - 关键进程启动
  - 数据与参数保护
  - 虚拟化层保护
  - 策略保护/介入保护

基于量子密钥分发网络的密码应用系统（Q-HSCS）由融合安全管理平台（HSCM）和安全执行模块（SEM）两部分组成。



# QKDN-ICT融合密码应用场景

## — 融合量子通信技术的自主可控云平台（独立策略管控）



基于QKD安全机制的自主可控云平台，覆盖了传统云的所有功能，在为用户提供基于量子密钥安全增强的计算、存储、网络等虚拟化资源同时，通过定义云内组件编码和密钥派生规则、建立统一策略库、量子密钥更新和供给控制、受控闭锁异常处理机制，实现对虚拟化、数据存储、云管平台、云平台软件等方面的策略管控。

数据管控（数据访问和应用运行策略）：

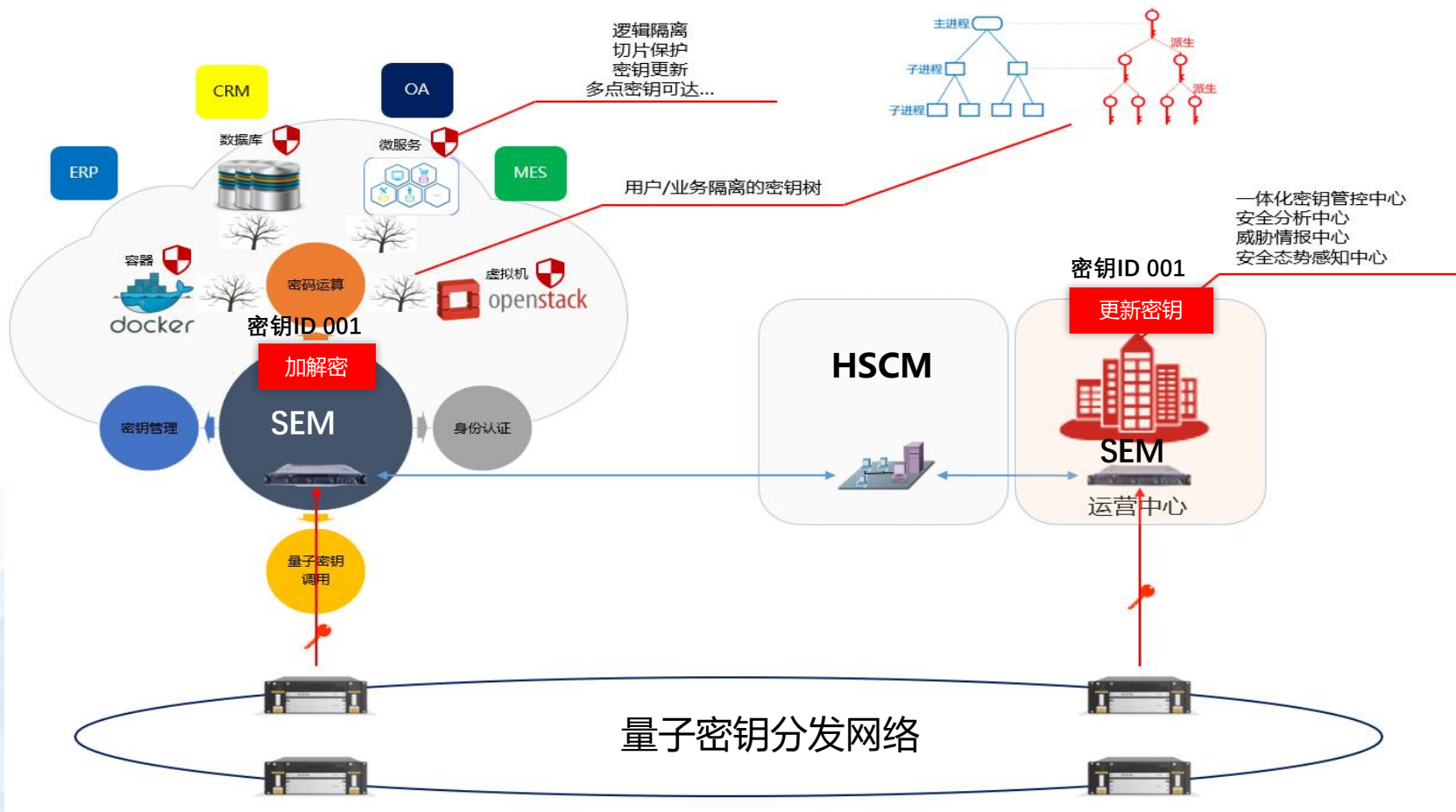
- 虚拟化：虚拟机可信启动、虚拟机运行时保护
- 数据存储：虚拟机镜像文件加密
- 云管平台：身份认证
- 云平台软件：服务进程启动、敏感参数保护
- 云安全资源池：安全策略访问



# QKDN-ICT融合密码应用场景

## — 融合ICT基础设施与应用

Q-HSCS通过与ICT基础设施和应用的融合，构建自主可控的数据执行存储环境，将量子密码应用成为ICT基础设施和应用业务流程的必要环节。同时为监管方的介入管理提供技术手段，为培育新型数据增值业务提供平台支撑。

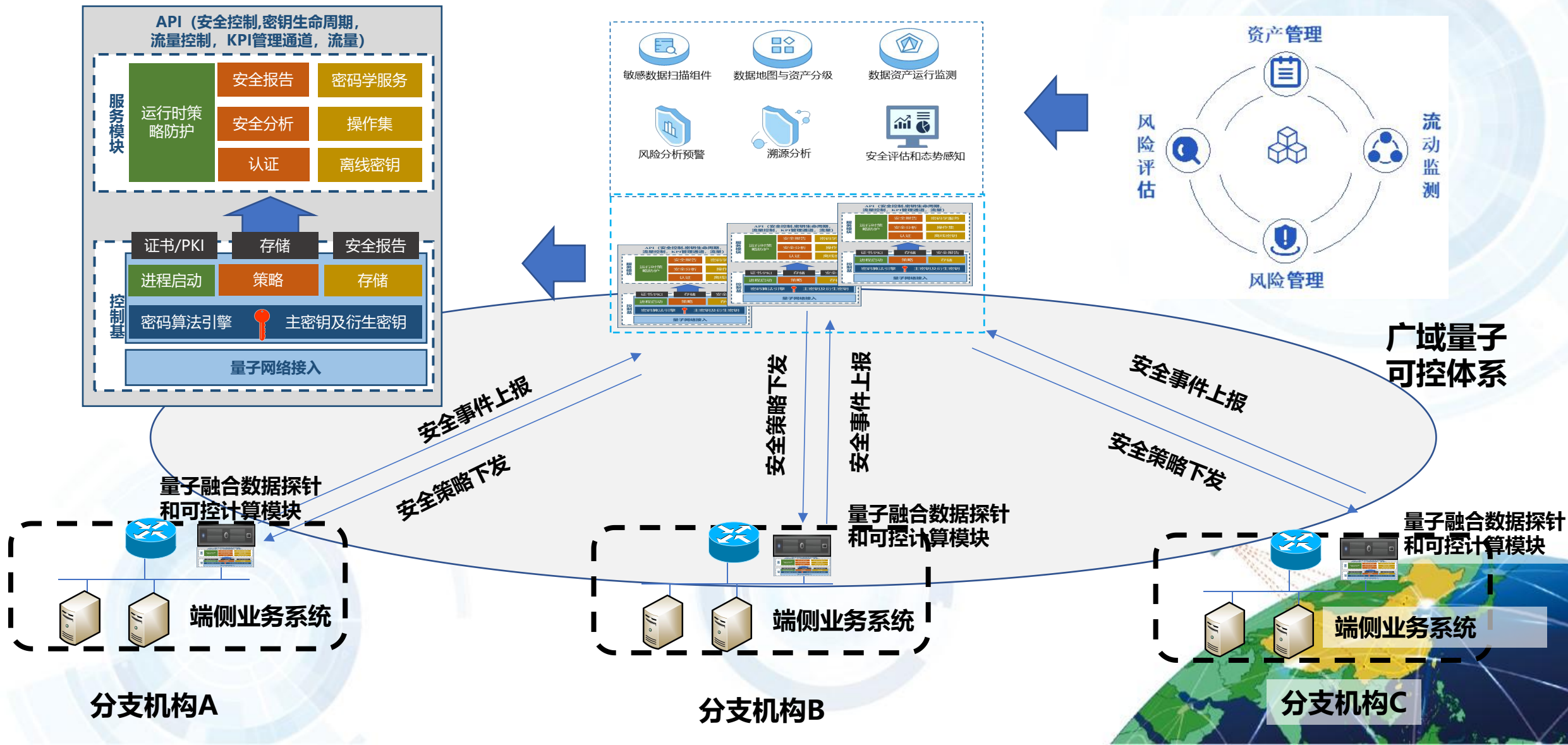




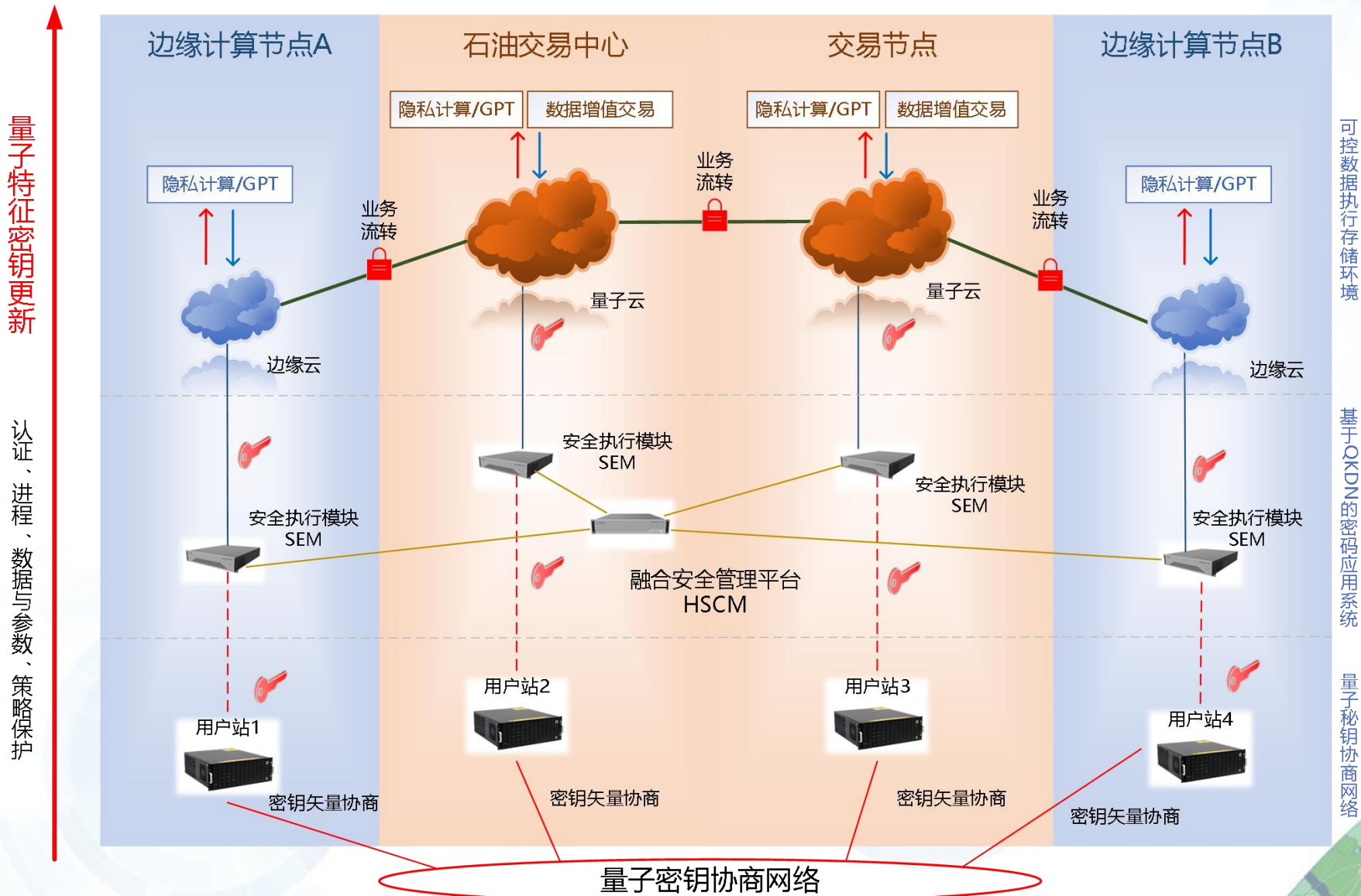


# QKDN-ICT融合密码应用场景

## — 基于量子通信技术的网络安全管理

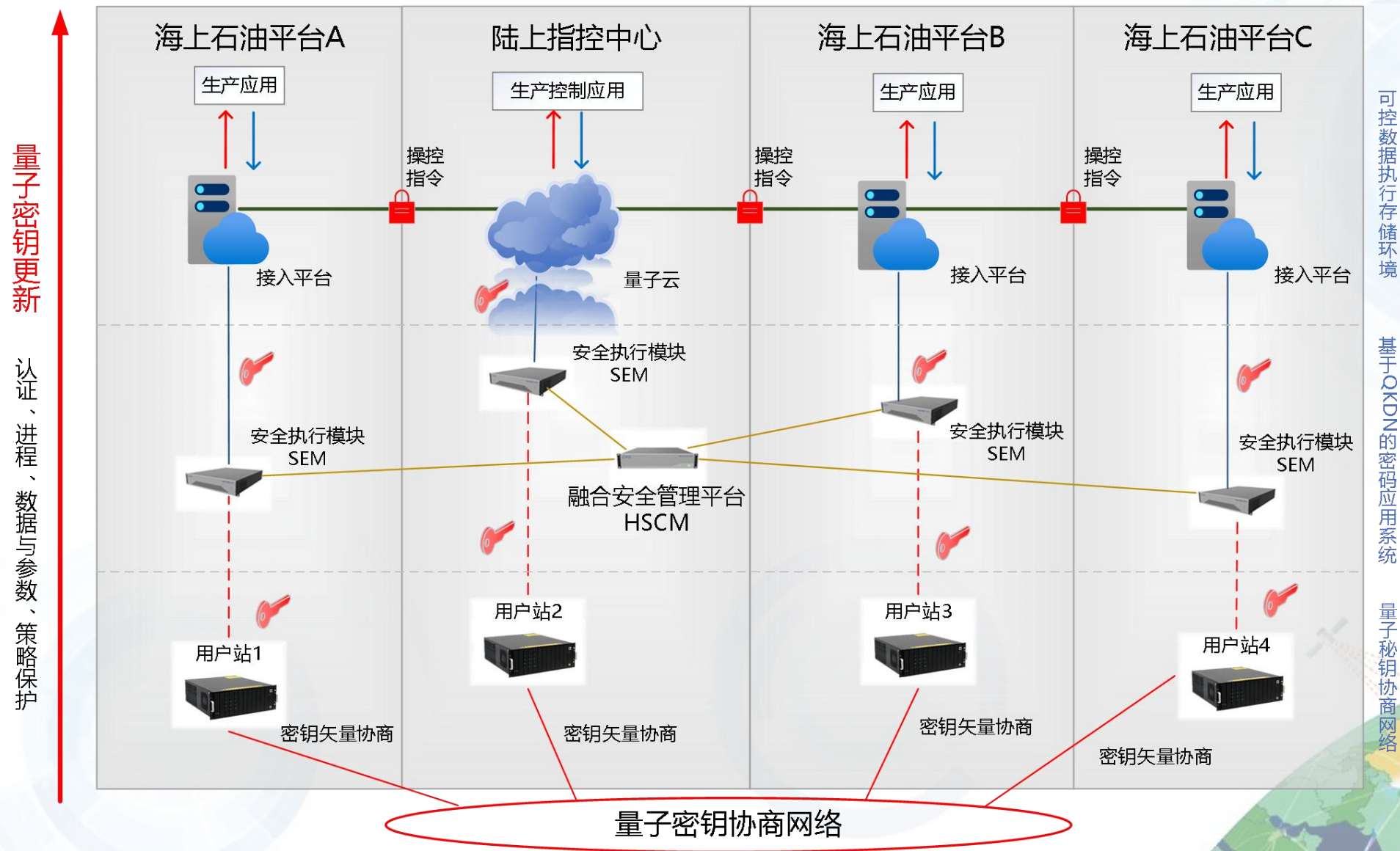


# 应用案例：多云、多点架构下数据流转的统一安全管控





# 应用案例：远程操控场景下的指令安全保护





**谢谢!**

---

2023年7月