ICS 35.030

CCS M30

T/ZRIA

团 体 标 准

T/ZRIA 001—2024

电网巡检机器人的量子加密5G通信技术规范

Quantum-encrypted 5G communication specifications for distribution network inspection robots

2024－03－12 发布 2024－03－27 实施

浙江省机器人产业发展协会 发 布

目录

前　言

本文件按照GB/T 1.1－2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本标准由浙江省机器人产业发展协会提出并解释。

本标准由浙江省机器人产业发展协会归口。

本标准起草单位：国网浙江省电力有限公司宁波供电公司、宁波永耀电力投资集团有限公司、上海循态量子科技有限公司、杭州申昊科技股份有限公司、浙江国自机器人技术股份有限公司、杭州国辰机器人科技有限公司、杭州蓝芯科技有限公司、杭州云深处科技有限公司。

标准主要起草人：安磊、刘鹏、李建刚、马丽军、俞红生、吴笑、章立伟、任赟、鲍聪颖、喻琰、邵淦、费武、吴昊、曹建敏、曹雅素、邹翔、张文博、王轩楷、林相成、李典泽、吴忠平、赵萌、周颖明、李华生、黄镇涛、吴海腾、田少华、马超、裴翔、郑超、孙昭龙、陈申红、吴清梅。

本标准首次发布。

面向配电网巡检机器人的量子加密 5G 通信技术规范

1 范围

本文件规定了面向配电网巡检机器人（以下简称巡检机器人）的量子加密 5G 通信技术的应用场景、功能要求和技术要求等。

本文件适用于使用量子加密 5G 通信技术的配电网巡检机器人的设计、开发与应用。应用类似技术的其他机器人，可参考使用。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 2423.10-2008 电工电子产品环境试验 第 2 部分： 试验方法 试验 Fc：振动（正弦）

GB/T 3797-2016 电气控制设备

GB/T 17626.2-2018 电磁兼容 试验和测量技术 静电放电抗扰度试验

GB/T 17626.3-2016 电磁兼容 试验和测量技术 射频电磁场辐射抗扰度试验

GB/T 17626.8-2006 电磁兼容 试验和测量技术 工频磁场抗扰度试验

GB/T 32915-2016 信息安全技术 二元序列随机性检测方法

GB 5226.1-2008 机械电气安全 机械电气设备 第 1 部分：通用技术条件

GB 50169-2016 电气装置安装工程接地装置施工及验收规范

GB/Z 19397-2003 工业机器人 电磁兼容性试验方法和性能评估准则 指南

YD/T 3618-2019 5G 数字蜂窝移动通信网 无线接入网总体技术要求（第一阶段）

YD/T 3834.1-2021 量子密钥分发（QKD）系统技术要求第 1 部分：基于诱骗态 BB84 协议的 QKD 系统

YD/T 3834.2-2022 量子密钥分发（QKD）系统技术要求第 1 部分：基于高斯调制相干态协议的 QKD 系统

YD/T 3835.1-2021 量子密钥分发（QKD）系统测试方法第 1 部分：基于诱骗态 BB84 协议的 QKD 系统

YD/T 3835.2-2022 量子密钥分发（QKD）系统测试方法第 1 部分：基于高斯调制相干态协议的 QKD 系统

YD/T 4011-2022 5G 网络管理技术要求 总体要求

Q/GDW 11513.1—2016 变电站智能机器人巡检系统技术规范 第 1 部分：变电站智能巡检机器人

Q/GDW 11513.2—2016 变电站智能机器人巡检系统技术规范 第 2 部分：监控系统

3 术语和定义

下列术语和定义适用于本文件。

3.1

配电网巡检机器人 inspection robot for distributive network

由移动载体、通信设备和检测设备等组成，采用遥控或全自主运行模式，用于配电网巡检作业的移动巡检装置。

3.2

量子密钥分发设备 quantum key distribution equipment

实现量子密钥分发协议的设备或系统，包括量子密钥发送端（Alice）、量子密钥接收端（Bob）和量子通道传输模块（如光纤电缆或自由空间通信模块）等组件。实现量子态的生成、传输和检测，进而生成安全密钥。

3.3

量子密钥管理设备 quantum key management equipment

管理量子密钥的设备或系统，由存储、传输和更新量子密钥等软硬件组件构成，包括量子密钥存储器、密钥分发模块、密钥更新模块和密钥分发协议管理模块等。

3.4

量子密钥充注设备 quantum key injection device

向量子通信系统中充注新量子密钥的设备，由注入新量子密钥的硬软件组件构成，包括注入新量子密钥、管理密钥注入过程的安全性、监控充注操作的完整性等功能。

3.5

量子安全透明网关 quantum-safe transparent gateway

保护传统通信网络受未来量子计算攻击的安全设备，利用量子安全技术，保护通信数据免受量子计算的攻击，通常作为网络的边界设备，位于通信网络的传入和传出点，实现量子安全的通信通道。

3.6

5G CPE 5G customer premises equipment

5G网络中的客户端设备，连接无线和有线通信，包括数据传输、流量管理、安全控制和网络接入等功能。

4 符号、代号和缩略语

下列符号、代号和缩略语适用于本文件。

MEC：边缘计算（Mobile Edge Computing）

QKD：量子密钥分发（Quantum Key Distribution）

5G CPE: 5G 客户端设备（5G Customer Premises Equipment）

5 应用场景描述

本标准使用量子密钥分发技术，定义了典型的巡检机器人量子加密 5G 通信技术规

范配电网应用场景，拓扑如图 1 所示：

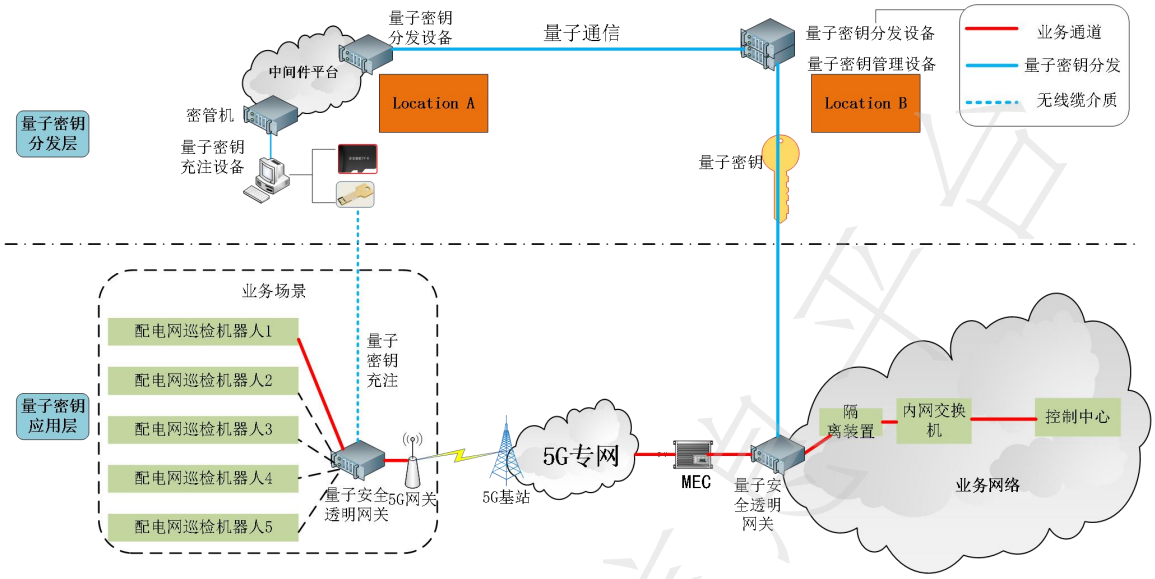

图 1 面向配电网巡检机器人的量子加密 5G 通信技术方案拓扑图

面向配电网巡检机器人的量子加密5G通信技术方案可以分为两层，分别是量子密钥分发层以及量子密钥应用层。在量子密钥分发层中有量子保密通信设备，包括量子密钥分发设备、密管机、量子密钥管理设备、量子密钥充注设备。量子密钥分发设备通过量子信道对密钥进行生成和分发，量子密钥管理设备负责对量子密钥进行管理和销毁，密管机和量子密钥充注设备实现量子密钥的充注。量子密钥应用层中有配电网巡检机器人、量子安全透明网关、5G基站、MEC等设备，其中量子安全透明网关使用量子密钥对业务数据进行量子加解密，并将加密后的数据传输到5G专网中进行传输，具体的业务流程如下：

第一步：由通信传输网络和配电自动化业务汇聚的两个核心节点两侧的量子密钥分发设备分发量子密钥；

第二步：通过量子密钥充注设备，利用移动量子技术将密钥充注至量子安全透明网关，结合配电自动化三遥业务信息生成密文；

第三步：通过5G网关，将密文通过5G专网无线网络传输至配网主站；

第四步：利用量子安全透明网关利用分发的密钥解密接收到的密文。

6 功能要求

6.1 巡检机器人要求

6.1.1 通信性能要求

a) 配电网巡检机器人的最大遥控距离应不小于 1km，工作应可靠。
b) 两台或两台以上巡检机器人在同一地点工作时，其控制信号不应相互干扰。
c) 控制中心可通过监控系统能实时地、可靠地接收巡检机器人采集的图像、语音、数据等信息并进行转发或处理。

6.2 5G CPE 要求

6.2.1 网络接入要求

应支持 802.11 b/g/n 标准的通信，支持 WEP/WPA/WPA2 等加密，支持 5G、Wi-Fi、有线互为备份。

6.2.2 安全要求

数据传输应支持 IPsec VPN、L2TP、PPTP、OPEN VPN、GRE、CA 证书，支持 SPI 全状态检测、Secure Shell（SSH）、入侵保护（Ping）、DDos 攻击、攻击防御、IP-MAC 绑定网络安全功能。

6.2.3 软件功能

网络接入应支持 APN VPND,接入认证支持 CHAP/PAP 认证,网络模式支持 GSM/GPRS/EDGE LTE/5G；LAN 协议支持 ARP，Ethernet；WAN 协议支持静态 IP，DHCP，PPPoE，PPP；IP 应用支持 Ping、Trace、DHCP Server、DHCP Relay、DHCP Client、DNS relay、DDNS、Telnet；支持 IP 路由功能；支持网络地址转换。

6.2.4 网络管理功能

网络管理应支持带宽限速、IP 限速；配置方式应支持 telnet、web、ssh 和 console。

6.2.5 日志功能

应支持本地系统日志、远程日志、串口输出日志。

6.2.6 网管功能

应支持 SNMP v3，支持 SNMP TRAP 功能。

6.2.7 流量管理

应支持流量阈值设定，支持流量统计和流量告警功能。

6.2.8 预警功能

应支持系统重启，LAN 端口上下线、流量告警、sim 卡故障警告。

6.2.9 状态查询功能

应支持查询系统状态，modem 状态，网络连接状态，路由状态。

6.3 量子保密通信设备要求

6.3.1 密钥一致性要求

a) 通过 CV-QKD 上位机将发送端和接收端在同一时间段内生成的密钥文件导出，密钥文件≥1Gbit。
b) 利用密钥一致性测试工具对密钥文件一致性进行测试，即二进制文件内容比对。
c) 发送端与接收端密钥一致。

6.3.2 密钥随机性要求

生成的密钥应能够通过 GB/T32915-2016 标准的随机性检测。

6.3.3 密钥安全成码率要求

使用 OTDR（或光源+光功率计）标定系统光纤链路长度和损耗。通过 QKD 系统网管或上

位机记录密钥成码率，并统计一小时内密钥平均成码率。在标称光纤链路损耗（8dB/10dB/12dB/14dB/16dB/18dB）下的密钥成码率小时平均值满足标称值。

6.3.4 数据加解密速率要求

加解密速率200M。

6.3.5 密钥存储大小要求

根据所使用的UKEY的安全存储区的大小配置，目前使用的最大密钥存储量为3000个，单个密钥长度16字节（bytes）。

7 技术要求

7.1 整体要求

7.1.1 巡检机器人

在如下环境条件下应能正常工作：

a) 环境温度：-20℃～+40℃；
b) 相对湿度：（5%～80%）RH；
c) 最大风速：20m/s。

7.1.2 5G CPE

在如下环境下应能正常工作：

a) 工作温度：0℃～+25℃；
b) 存储温度：-25℃～+70℃；
c) 存储湿度：（5%—80%）RH。

7.1.3 量子保密通信设备

在如下环境下应能正常工作：

a) 工作电压：5V；
b) 工作温度：0℃～+25℃；
c) 工作湿度：（20%～90%）RH；
d) 存储温度：-10℃～80℃；
e) 存储湿度：（10%～95%）RH。

7.2 结构外观要求

7.2.1 5G CPE 设备

a) 外壳防护等级应满足IP30；
b) EMC 各项等级指标达3级；
c) 以太网口支持1.5kV隔离变压保护；
d) 宽压支持：（9—36）V。

7.2.2 量子保密通信设备

a) 外壳防护等级应满足IP30；
b) USB接口应满足USB 2.0或USB 3.0。

7.3 电磁兼容要求

7.3.1 静电放电抗扰度

巡检机器人应能承受 GB/T 17626.2 第 5 章规定的严酷等级为 4 级的静电放电抗扰度试验。

7.3.2 射频电磁场辐射抗扰度

巡检机器人应能承受 GB/T 17626.3 第 5 章规定的严酷等级为 2 级的射频电磁场辐射抗扰度试验。

7.3.3 工频磁场抗扰度

巡检机器人应能承受 GB/T 17626.8 第 5 章规定的严酷等级为 4 级的工频磁场抗扰度试验。

7.4 电气化要求

电气化设计应符合 GB/T 2423.10-2008、GB/T 3797-2016、GB 5226.1-2008、GB 50169-2016 和 GB/Z 19397-2003 的规定。

7.5 接口要求

7.5.1 硬件接口

7.5.1.1 巡检机器人

a) WAN 口：1 个 100M WAN 口；
b) LAN 口：1 个（10M/100M 自适应 MDI/MDIX 口）；
c) USB 接口：1 个 USB2.0 或 USB3.0；
d) 天线接口：1 个 5G 天线，1 个 2.4G 天线；
e) 电源端子：1 个；
f) 控制口：1 个。

7.5.1.2 5G CPE

a) WAN 口：1 个 100M WAN 口；
b) LAN 口：4 个（10M/100M 自适应 MDI/MDIX 口）；
c) USB 接口：1 个 USB2.0 或 USB3.0；
d) 天线接口：4 个 5G 天线，2 个 2.4G 天线；
e) 电源端子：1 个；
f) 控制口：1 个。

7.5.1.3 量子保密通信设备

7.5.1.3.1 中心解密网关

a) WAN 口：2 个 1000M WAN 口 ；
b) USB 接口：1 个 USB2.0 或 USB3.0；
c) 控制口：1 个。

7.5.1.3.2 密钥充注设备

a) WAN 口：1 个 1000M WAN 口 ；
b) USB 接口：4 个 USB2.0 或 USB3.0；
c) 控制口：1 个；
d) TF 卡：一个 TF 卡槽。

7.5.2 软件接口

7.5.2.1 密钥充注

接口调用过程流程如下：

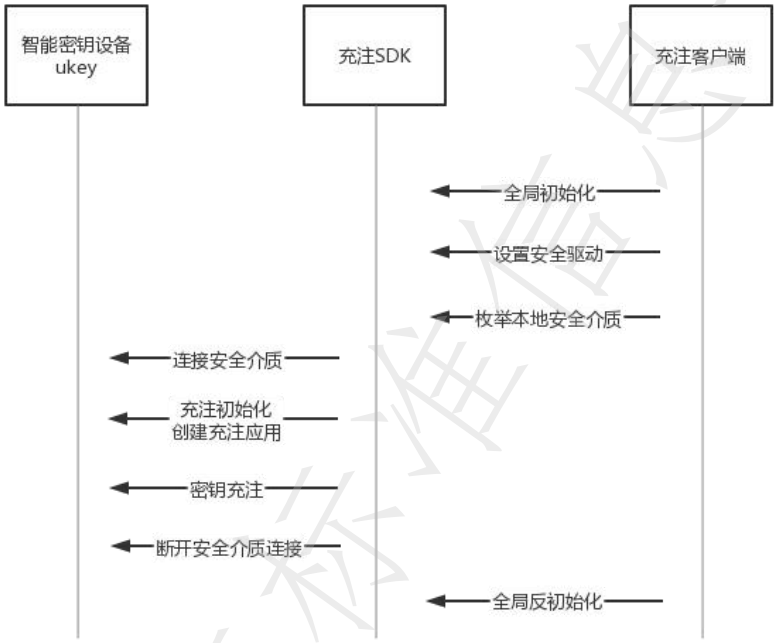

图 2 接口调用过程流程图

密钥充注由密钥充注客户端实现。充注时，需在密钥充注客户端上插入一个或多个需要被充注的用户设备，并调用量子安全 SDK 将密钥信息依次写入用户设备中，具体 API 接口函数说明见附录 A。

7.5.2.2 密钥使用

接口调用过程：客户端和服务端程序在初始化连接方面都经历了一系列步骤。首先，两端均调用全局初始化，确保满足日志、链表等初始化条件。随后，程序配置适配对应厂商的安全驱动，并对本地插入的安全介质进行枚举。一旦成功枚举，程序将安全介质的序列号存储到链表中，并建立与枚举到的安全介质的连接。

客户端首先通过接口从安全介质中获取初始向量，并随机选择一条充注密钥。使用所选的充注密钥，客户端申请量子加强密钥。

客户端的申请量子加强密钥接口返回了量子加强密钥和 token 值。该 token 值包含初始向量和充注密钥的索引值。客户端在成功申请后，将 token 发送到服务端。

服务端接收到 token 值后，调用获取量子加强密钥的接口，提取对应索引的充注密钥，并通过 token 中的初始向量对密钥进行增强，最终得到对称的量子加强密钥。

完成以上交互后，两端程序断开与安全介质的连接，并调用全局反初始化接口，释放所分配的内存。

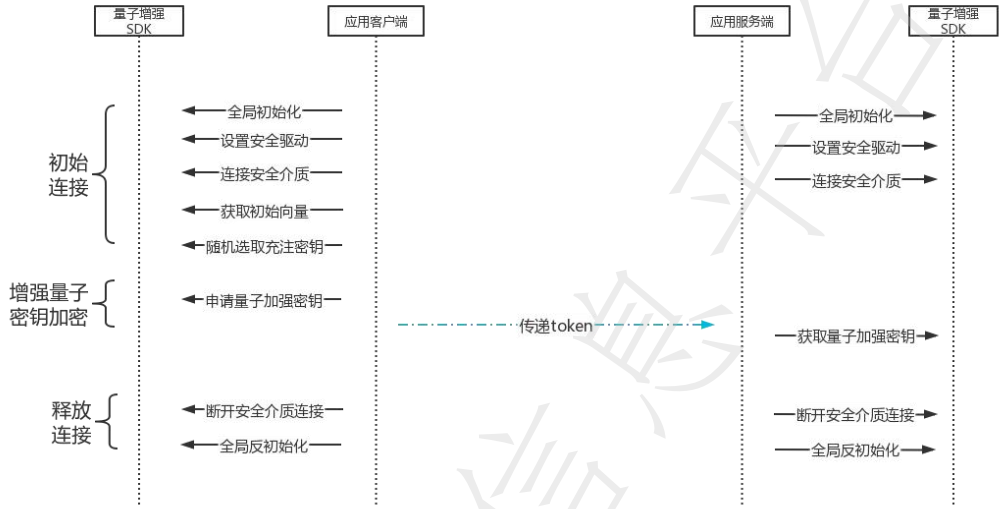

图 3 密钥使用过程流程图

附　录　A（规范性）

充注过程 API 接口函数说明

a)　全局初始化

接口名称	int XTQS_Init(void)
功能描述	全局初始化
参数	无
返回值	成功：返回 0 不成功返回 NULL
备注	

b)　设置安全介质驱动

接口名称	XTQS_LoadDevDriver(const char *devDriverName)
功能描述	设置安全介质驱动
参数	[IN] devDriverName: 安全介质驱动的全路径文件名
返回值	成功：返回 0（不成功返回值）
备注	使用中的介质驱动为最后设置的介质驱动

c)　枚举本地安全介质设备

接口名称	void XTQS_EnumDev(dev_names_t *pDevNames)
功能描述	枚举本地计算机上的安全介质设备
参数 返回值	[OUT] pDevNames: 本地计算机上的安全介质设备列表 成功：pDevNames->amout > 0
备注	

d)　连接安全介质设备

接口名称	void* XTQS_ConnectDev(const char *devName)
功能描述	连接安全介质设备
参数	[IN] devName: 待连接的安全介质设备序列

	号
返回值	成功：返回设备句柄 失败：返回 NULL
备注	

e) 设置安全介质设备标签

接口名称	Int XTQS_SetLabel(void *hDev, const char *labelName)
功能描述	设置安全介质设备设备信息中的标签
参数	[IN] hDev: 待修改的安全介质设备句柄 [IN] labelName: 标签
返回值	成功：返回 0 不成功返回 NULL
备注	

f) 获取安全介质设备信息

接口名称	int XTQS_GetDevInfo(void *hDev, dev_info_t *pDevInfo)
功能描述	获取安全介质设备设备信息
参数	[IN] hDev: 待查询的安全介质设备句柄 [OUT] pDevInfo: 安全介质设备信息结构体
返回值	成功：返回 0 不成功返回 NULL
备注	

g) 断开安全介质设备连接

接口名称	int XTQS_DisconnectDev(void *hDev)
功能描述	断开安全介质设备连接
参数	[IN] hDev: 待断开的安全介质设备句柄
返回值	成功：返回 0 不成功返回 NULL
备注	

h) 全局反初始化

接口名称	void XTQS_DeInit(void)
功能描述	全局反初始化
参数	无
返回值	无
备注	

i) 安全介质应用清除

接口名称	int XTQS_DeleteKeyApp(void *hDev)
功能描述	安全介质应用清除
参数	[IN] hDev: 待清除应用的安全介质设备句柄
返回值	成功：返回 0 不成功返回 NULL
备注	

j) 安全介质应用创建

接口名称	int XTQS_CreateKeyApp(void *hDev)
功能描述	安全介质应用创建
参数	[IN] hDev: 待创建应用的安全介质设备句柄
返回值	成功：返回 0 不成功返回 NULL
备注	

k) 安全介质密钥充注

接口名称	int XTQS_ChargeKey(void *hDev, XTQS_KEY_FILE_E keyfileType, const char *keyFileName)
功能描述	安全介质密钥充注
参数	[IN] hDev: 待充注应用的安全介质设备句柄 [IN] keyfileType: 待充注应用的安全介质设备类型 [IN] keyFileName: 待充注的密钥文件路径
返回值	成功：返回 0 不成功返回 NULL
备注	

附　录　B（规范性）

密钥使用过程 API 接口函数说明

a)　全局初始化

接口名称	int XTQS_Init(void)
功能描述	全局初始化
参数	无
返回值	成功：返回 0 不成功返回 NULL
备注	

b)　设置安全介质驱动

接口名称	XTQS_LoadDevDriver(const char *devDriverName)
功能描述	设置安全介质驱动
参数	[IN] devDriverName: 安全介质驱动的全路径文件名
返回值	成功：返回 0 不成功返回 NULL
备注	使用中的介质驱动为最后设置的介质驱动

c)　枚举本地安全介质设备

接口名称	void XTQS_EnumDev(dev_names_t *pDevNames)
功能描述	枚举本地计算机上的安全介质设备
参数	[OUT] pDevNames: 本地计算机上的安全介质设备列表
返回值	成功：pDevNames->amout > 0
备注	

d)　连接安全介质设备

接口名称	void* XTQS_ConnectDev(const char *devName)
功能描述	连接安全介质设备
参数	[IN] devName: 待连接的安全介质设备序列号
返回值	成功：返回设备句柄 失败：返回 NULL

备注	

e) 设置安全介质设备标签

接口名称	Int XTQS_SetLabel(void *hDev, const char *labelName)
功能描述	设置安全介质设备设备信息中的标签
参数	[IN] hDev: 待修改的安全介质设备句柄 [IN] labelName: 标签
返回值	成功：返回 0 不成功返回 NULL
备注	

f) 获取安全介质设备信息

接口名称	int XTQS_GetDevInfo(void *hDev, dev_info_t *pDevInfo)
功能描述	获取安全介质设备设备信息
参数	[IN] hDev: 待查询的安全介质设备句柄 [OUT] pDevInfo: 安全介质设备信息结构体
返回值	成功：返回 0 不成功返回 NULL
备注	

g) 断开安全介质设备连接

接口名称	int XTQS_DisconnectDev(void *hDev)
功能描述	断开安全介质设备连接
参数	[IN] hDev: 待断开的安全介质设备句柄
返回值	成功：返回 0 不成功返回 NULL
备注	

h) 全局反初始化

接口名称	void XTQS_DeInit(void)
功能描述	全局反初始化
参数	无
返回值	无
备注	

i) 获取安全介质初始向量

接口名称	int XTQS_GetInitializationVector(void *hDev, int ivIndex, u_char *iv, int ivLen)
功能描述	获取安全介质初始向量
参数	[IN] hDev: 待查询的安全介质设备句柄 [IN] ivIndex: 待查询的初始向量索引 [OUT] iv: 初始向量 [IN]ivLen: 传入的初始向量缓冲区长度
返回值	成功：返回 0 不成功返回 NULL
备注	

j) 获取安全介质原始密钥

接口名称	int XTQS_GetKey(void *hDev, int *keyIndex, u_char *key, int keyLen)
功能描述	获取安全介质原始密钥
参数	[IN] hDev: 待查询的安全介质设备句柄 [IN, OUT] keyIndex: 密钥索引指针 当*keyIndex <0, 则意为随机取密钥，接口调用后修改*keyIndex 为实际取用的密钥索引； 当*keyIndex>=0, 则按*keyIndex 取，接口不会对 keyIndex 进行修改 [OUT] key: 原始密钥 [IN]keyLen: 传入的原始密钥缓冲区长度
返回值	成功：返回 0 不成功返回 NULL
备注	

k) 申请量子增强密钥

接口名称	int XTQS_ApplyQuantumEnhancedKey(void *hDev, u_char *qkey, int *pQKeyLen, u_char *token, int *pTokenLen)
功能描述	申请量子增强密钥
参数	[IN] hDev: 待查询的安全介质设备句柄 [OUT] qkey: 量子增强密钥 [OUT] pQKeyLen: 量子增强密钥长度

	[OUT] token: 会话 token [OUT]pTokenLen: 会话 token 长度
返回值	成功：返回 0 不成功返回 NULL
备注	

l) 获取量子增强密钥

接口名称	int XTQS_GetQuantumEnhancedKey(void *hDev, const u_char *token, int tokenLen, u_char *qkey, int *pQKeyLen)
功能描述	获取量子增强密钥
参数	[IN] hDev: 待查询的安全介质设备句柄 [IN] token: 会话 token [IN]tokenLen: 会话 token 长度 [OUT] qkey: 量子增强密钥 [OUT] pQKeyLen: 量子增强密钥长度
返回值	成功：返回 0 不成功返回 NULL
备注	