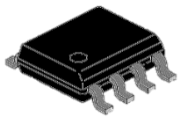
汉芝电子股份有限公司
iMQ Technology Inc.

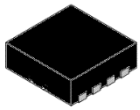
# SQ7131/SQ7133/SQ7135

**低功耗安全加密芯片, ECC-256/384, ECDSA, ECDH, AES-128/AES-256, SHA-256,TRNG**

- **基本信息**
  - 工作电压范围: 2.0V ~ 5.5V
  - 工作温度范围: -40°C ~ 85°C
- **低功耗平台**
  - 低功耗设计支持运作(operation)与深眠(Deep Sleep)模式
  - 深眠模式功耗 300nA
- **安全加密防护功能**
  - NIST CAVP认证
  - NIST标准之非对称式硬件加速器
    - NIST P256 /P384椭圆曲线
    - ECDSA : FIPS186-4椭圆曲线数字签名
    - ECDH: FIPS SP800-56A 密钥合意协议(Key Agreement)
  - NIST标准之硬件对称式加密算法
    - FIPS 180-4 SHA-256 & FIPS 198-1 HMAC 哈希算法
    - FIPS-197 AES-128/256 : 加密/解密, Galois Field Multiply for GCM
  - 支持网络密钥管理
    - TLS 1.2 & 1.3 PRF/HKDF 计算
    - ECDHE 密鑰交換協定
  - 高质量TRNG设计，兼容SP800-22标准
  - 防篡改(Anti-Tamper)保护，对企图入侵进行监测并做出反应
  - 差分功耗分析旁路攻击保护(SPA/DPA : simple/differential power analysis)
  - 独立内部时钟、防止外部Glitch攻击
  - 128位唯一标识符 (UID)
- **封装形式**



SOP8



**8-Lead DFN (3mm x 3mm)**

- **安全存储**
  - 芯片加扰加密技术
  - 安全存储区–密钥、X.509证书、数据
  - 大容量User Data : 5.6KB
- **通讯接口**
  - SQ7131具标准I2C接口(最高传输速度1Mbps)
  - SQ7133具标准SPI接口(最高传输速度10MHz@ MODE 3)
  - SQ7135支持SWI(Single Wire Interface)界面(230.4Kbps)
- **应用项目**
  - 配件认证、耗材认证
  - 系统反仿冒
  - 加密电子锁、指纹锁
  - 对话密钥交换 (Session Key Exchange)
  - 连网装置安全识别或认证
  - 敏感数据加密、加密通讯
  - 上位机软件、版权保护
  - 嵌入式系统固件(Firmware)保护
  - 安全传输TLS1.2与TLS 1.3
  - AIoT 装置安全认证
  - 安全启动/安全远程更新