汉芝电子股份有限公司
iMQ Technology Inc.

SQ7101/SQ7103

低功耗安全加密芯片, 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 250nA

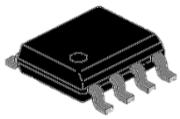
◆ 安全加密防护功能

- NIST CAVP认证
- AES-128/AES-256硬件加解密算法
- SHA-256硬件哈希算法
- 真随机数生成器(true random number generator, TRNG)
- 物理上使用强力密封和防篡改电路，提高密钥和敏感数据保護能力
- 差分功耗分析旁路攻击保护(SPA/DPA : simple/differential power analysis)
- 独立的内部时钟、可防止外部Glitch攻击
- 128位唯一识别码 (UID)
- 内建 16个monotonic 计数器、防止replay 攻击及中间人(man in the middle)攻击

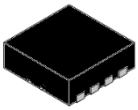
◆ 安全存储

- 支持16个128-bit 或8个256-bit 密钥
- 256 Bytes 用户数据(User Data)
- 768 Bytes Small Zone

◆ 封装形式



SOP8



8-Lead DFN (3mm x 3mm)

◆ 通讯接口

- SQ7101具标准I2C接口(最高传输速度400Kbps)
- SQ7103具标准SPI接口(最高传输速度5MHz)

◆ 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
- 崁入式系统韧体(Firmware)保护