



具有快速清零技术的 安全加密控制器

MAXQ1850

概述

MAXQ1850 是一款低功耗、32 位 RISC 器件，设计用于电子商务、银行及数据安全系统。该器件具有高性能、单指令周期、先进的防篡改检测技术和硬件加密，提供业内领先的数据安全和密钥保护。

物理安全机制包括环境传感器，可检测出超范围的电压或温度，检测到这种情况时会快速清除关键数据。提供四路自毁输入，用于响应其它篡改操作。内部硅片上的防护网可提供防探针保护。内部高速环形振荡器可阻止通过控制芯片时钟频率的攻击。为保护数据，MAXQ1850 集成了多个高速、抗解析的加密引擎。硬件支持的算法包括：AES (128、192 和 256 位)、DES、3DES (2 密钥和 3 密钥)、ECDSA (160、192 和 256 位密钥)、DSA、RSA (达 2048 位)、SHA-1、SHA-224 以及 SHA-256。MAXQ1850 先进的安全功能完全符合 ITSEC E3 高级、FIPS 140-2 3 级以及公共标准等最严格的安全认证要求。

MAXQ1850 包括 256KB 闪存及 8KB 电池备份的安全数据 SRAM。硬件引擎支持多种通信协议，包括：用于智能卡应用的 ISO 7816、USB (带有 4 级端点缓存的从机接口)、RS-232 通用同步/异步收发器(USART)、SPI™ 接口(支持主机或从机模式)以及多达 16 路的通用 I/O 引脚。MAXQ1850 的其它外设支持包括：真正的硬件随机数发生器(RNG)、实时时钟(RTC)、可编程看门狗定时器以及灵活的 16 位定时器，可支持捕获、比较及脉宽调制(PWM)操作。

应用

| | |
|---------|-------------|
| 电子商务 | 计次计时付费(PPP) |
| EMV® 银行 | 授权认证 |
| 安全门禁控制 | 电子签名发生器 |
| 安全数据存储 | |

特性

- ◆ 高性能、低功耗、32 位 MAXQ30 RISC 内核
- ◆ 3.3V 单电源供电，提供低功耗/灵活接口
- ◆ 在整个工作范围内，指令可运行在直流至 16MHz
- ◆ 65MHz 的加密引擎缩短处理时间
- ◆ 片上 2 倍/4 倍时钟倍频器
- ◆ 33 条指令
- ◆ 16 位指令字、32 位内部数据总线
- ◆ 16 x 32 位累加器
- ◆ 多达 16 路的通用 I/O 引脚
- ◆ 5V 兼容 I/O
- ◆ 不受限制的软件堆栈
- ◆ 经过优化的 C 编译器(高速/高密度代码)
- ◆ 存储器特性
- ◆ 安全特性
- ◆ 附加外设
- ◆ 低功耗

完整的特性信息请参见详细特性部分。

订购信息

| PART | TEMP RANGE | PIN-PACKAGE |
|---------------|----------------|-------------|
| MAXQ1850-BNS+ | -40°C to +85°C | 40 TQFN-EP* |
| MAXQ1850-LNS+ | -40°C to +85°C | 49 CSBGA |
| MAXQ1850-DNS+ | -40°C to +85°C | Bare die |

+ 表示无铅(Pb)/符合 RoHS 标准的封装。

*EP = 裸焊盘。

选型指南在数据资料的最后给出。

EMV 是 EMVCo, LLC 的注册认证标志。

SPI 是 Motorola, Inc. 的商标。

注意：该器件某些版本的规格可能与发布的规格不同，会以勘误表的形式给出。通过不同销售渠道可能同时获得器件的多个版本。欲了解器件勘误表信息，请点击：china.maxim-ic.com/errata。



本文是英文数据资料的译文，文中可能存在翻译上的不准确或错误。如需进一步确认，请在您的设计中参考英文资料。

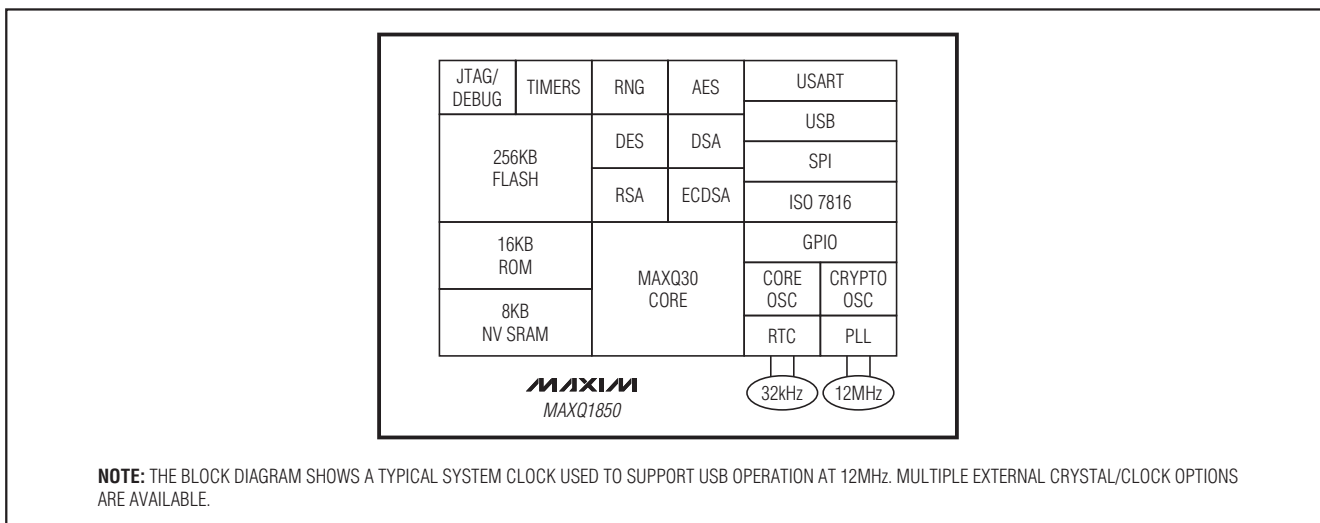
有关价格、供货及订购信息，请联络 Maxim 亚洲销售中心：10800 852 1249 (北中国区)，10800 152 1249 (南中国区)，或访问 Maxim 的中文网站：china.maxim-ic.com。

数据资料缩写本

具有快速清零技术的 安全加密控制器

MAXQ1850

方框图



详细特性

- ◆ 高性能、低功耗、32位 MAXQ30 RISC 内核
- ◆ 3.3V 单电源供电，提供低功耗/灵活接口
- ◆ 在整个工作范围内，指令可运行在直流至 16MHz
- ◆ 65MHz 的加密引擎缩短处理时间
- ◆ 片上 2 倍/4 倍时钟倍频器
- ◆ 33 条指令
- ◆ 3 个独立的数据指针，具有自动递增/递减功能，加速数据转移
- ◆ 16 位指令字、32 位内部数据总线
- ◆ 16 x 32 位累加器
- ◆ 多达 16 路的通用 I/O 引脚
- ◆ 5V 兼容 I/O
- ◆ 不受限制的软件堆栈
- ◆ 经过优化的 C 编译器(高速/高密度代码)
- ◆ 存储器特性
 - 256KB 闪存，划分为 512 字节扇区(每扇区 1K 擦除/写入周期)
 - 8KB 电池备份数据 SRAM
 - 专用密钥存储空间

◆ 安全特性

- 唯一 ID
- 篡改检测快速擦除密钥/数据
- 四路自毁输入
- 硬件 AES 和 DES 引擎
- 公钥加密加速器用于 DSA、ECDSA 和 RSA
- 支持 SHA-1、SHA-224 和 SHA-256 算法
- 真正的硬件 RNG 和 PRNG
- 硬件 CRC-32/16
- 不能更改的电池备份实时时钟

◆ 附加外设

- 电源失效报警
- 上电复位/电压跌落复位
- JTAG I/F 用于系统编程和访问片上调试器
- 带有四个端点缓存的 USB I/F
- 带有 FIFO 的 ISO 7816 智能卡 UART
- 四个 16 位定时器/计数器，其中两个具有 PWM 功能
- SPI 和 USART 通信端口
- 可编程看门狗定时器

◆ 低功耗

- 电池备份模式下，保持 8KB NV SRAM 和安全检测器有效工作时仅吸收 150nA 典型电流(RTC 有效工作时，电流为 460nA)

请读者注意：本文档是完整数据资料的缩写本，如需申请数据资料全文，请访问 china.maxim-ic.com/MAXQ1850 点击申请数据资料全文。