



Secure Cryptographic Controller with Rapid Zeroization Technology

MAXQ1850

General Description

The MAXQ1850 is a low-power, 32-bit RISC device designed for electronic commerce, banking, and data security systems. It combines high-performance, single-cycle processing, sophisticated tamper-detection technology, and advanced cryptographic hardware to provide industry-leading data security and secret key protection.

Physical security mechanisms include environmental sensors that detect out of range voltage or temperature conditions, responding with an instantaneous zeroization of critical data. Four self-destruct inputs are provided for additional tamper response. An internal shield over the silicon provides protection from microprobe attacks. A high-speed internal ring oscillator is provided to thwart attacks that rely on controlling the clock rate of the chip. To protect data, the MAXQ1850 integrates several high-speed, analysis-resistant encryption engines. Algorithms supported in hardware include AES (128-, 192-, and 256-bit), DES, triple DES (2-key and 3-key), ECDSA (160-, 192-, and 256-bit keys), DSA, RSA (up to 2048 bits), SHA-1, SHA-224, and SHA-256. The advanced security features of the MAXQ1850 are designed to meet the stringent requirements of regulations such as ITSEC E3 High, FIPS 140-2 Level 3, and the Common Criteria certifications.

The MAXQ1850 includes 256KB of flash memory and 8KB of secure, battery-backed data SRAM. Several communication protocols are supported with hardware engines, including ISO 7816 for smart card applications, USB (slave interface with four end-point buffers), an RS-232 UART, an SPI™ interface (master or slave mode support), and up to 16 general-purpose I/O pins. Other peripherals supported on the MAXQ1850 include a true hardware random-number generator (RNG), a real-time clock (RTC), a programmable watchdog timer, and flexible 16-bit timers that support capture, compare, and pulse-width modulation (PWM) operations.

Applications

- | | |
|-----------------------|---------------------------------|
| Electronic Commerce | Pay-per-Play |
| EMV™ Banking | Certificate Authentication |
| Secure Access Control | Electronic Signature Generation |
| Secure Data Storage | |

EMV is a trademark owned by EMVCo LLC.

SPI is a trademark of Motorola, Inc.

Note: Some revisions of this device may incorporate deviations from published specifications known as errata. Multiple revisions of any device may be simultaneously available through various sales channels. For information about device errata, go to: www.maxim-ic.com/errata.



For pricing, delivery, and ordering information, please contact Maxim Direct at 1-888-629-4642, or visit Maxim's website at www.maxim-ic.com.

Features

- ◆ High-Performance, Low-Power, 32-Bit MAXQ30 RISC Core
- ◆ Single 3.3V Supply Enables Low Power/Flexible Interfacing
- ◆ DC to 16MHz Code Execution Across Entire Operating Range
- ◆ Up to 65MHz Cryptography Engine Execution to Reduce Processing Time
- ◆ On-Chip 2x/4x Clock Multiplier
- ◆ 33 Instructions
- ◆ 16-Bit Instruction Word, 32-Bit Internal Data Bus
- ◆ 16 x 32-Bit Accumulators
- ◆ Up to 16 General-Purpose I/O Pins
- ◆ 5V Tolerant I/O
- ◆ Virtually Unlimited Software Stack
- ◆ Optimized for C-Compiler (High-Speed/Density Code)
- ◆ Memory Features
- ◆ Security Features
- ◆ Additional Peripherals
- ◆ Low-Power Consumption

See the Detailed Features section for complete list of features.

Ordering Information

PART	TEMP RANGE	PIN-PACKAGE
MAXQ1850-BNS+	0°C to +70°C	40 TQFN-EP*

Note: A chip-scale BGA (CSBGA) version of the MAXQ1850 is in development. Contact the factory for more information.

+Denotes a lead(Pb)-free/RoHS-compliant package.

*EP = Exposed pad.

Pin Configuration and Selector Guide appear at end of data sheet.

ABRIDGED DATA SHEET

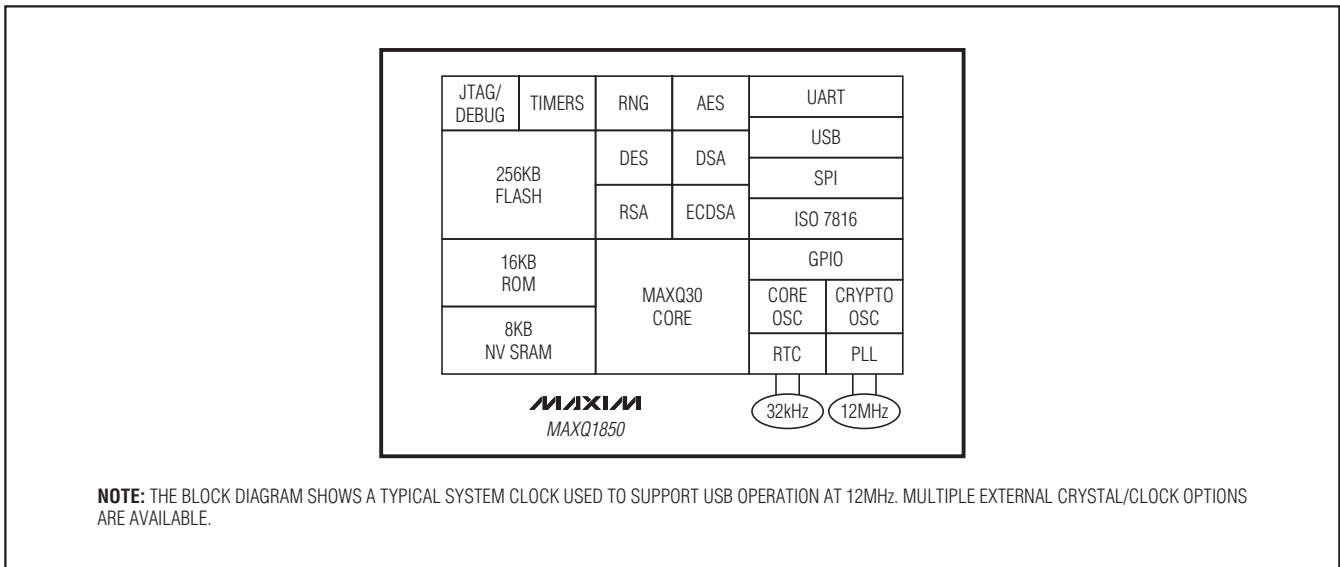
Secure Cryptographic Controller with Rapid Zeroization Technology

Typical Operating Characteristics

(T_A = +25°C, unless otherwise noted.)

Refer to the full data sheet.

Block Diagram



ABRIDGED DATA SHEET

Secure Cryptographic Controller with Rapid Zeroization Technology

MAXQ1850

Detailed Features

- ◆ **High-Performance, Low-Power, 32-Bit MAXQ30 RISC Core**
- ◆ **Single 3.3V Supply Enables Low Power/Flexible Interfacing**
- ◆ **DC to 16MHz Code Execution Across Entire Operating Range**
- ◆ **Up to 65MHz Cryptography Engine Execution to Reduce Processing Time**
- ◆ **On-Chip 2x/4x Clock Multiplier**
- ◆ **33 Instructions**
- ◆ **Three Independent Data Pointers Accelerate Data Movement with Automatic Increment/Decrement**
- ◆ **16-Bit Instruction Word, 32-Bit Internal Data Bus**
- ◆ **16 x 32-Bit Accumulators**
- ◆ **Up to 16 General-Purpose I/O Pins**
- ◆ **5V Tolerant I/O**
- ◆ **Virtually Unlimited Software Stack**
- ◆ **Optimized for C-Compiler (High-Speed/Density Code)**
- ◆ **Memory Features**
 - 256KB Flash, Composed of 512 Byte Sectors (1K Erase/Write Cycles per Sector)
 - 8KB Battery-Backed Data SRAM
 - Dedicated Cryptographic Memory Space
- ◆ **Security Features**
 - Unique ID
 - Tamper Detection with Rapid Key/Data Destruction
 - Four Self-Destruct Inputs
 - Hardware AES and DES Engines
 - Public Key Cryptographic Accelerator for DSA, ECDSA, and RSA
 - Real Hardware RNG and PRNG
 - Hardware CRC-32/16
 - Unalterable, Battery-Backed Real-Time Clock
- ◆ **Additional Peripherals**
 - Power-Fail Warning
 - Power-On Reset/Brownout Reset
 - JTAG I/F for System Programming and Accessing On-Chip Debugger

USB I/F with Four End-Point Buffers
ISO 7816 Smart Card UART with FIFO
16-Bit Programmable Timers/Counters with Prescaler, Capture/Compare, and PWM
SPI and UART Communication Ports
Programmable Watchdog Timer

◆ **Low-Power Consumption**

130nA Typical Current Draw in Battery-Backed Mode, Preserving 8KB NV SRAM and with Security Sensors Active (460nA with RTC Active)

Detailed Description

Refer to the full data sheet.

Note to readers: This document is an abridged version of the full data sheet. To request the full data sheet, go to www.maxim-ic.com/MAXQ1850 and click on **Request Full Data Sheet**.