219-0022; Rev 0; 12/12
备有评估板

DS28EL25

DeepCover安全认证器，带有1-Wire SHA-256和4Kb用户EEPROM

概述

DeepCover®嵌入式安全方案采用多重先进的物理安全机制保护敏感数据，提供业内最高等级的密钥存储安全保护。Deepcover安全认证器(DS28EL25)将强加密、双向、安全质询–应答安全认证功能与符合FIPS 180-3安全散列算法(SHA-256)的方案结合在一起。4Kb用户可编程EEPROM阵列为应用数据提供了非易失存储空间，具有附加保护的存储器存储SHA-256操作的密码和用户存储器控制设置。每片器件都拥有唯一的64位ROM识别码(ROM ID)，由工厂写至芯片。唯一的ROM ID用作加密运算的基本输入参数，也作为应用中的电子序列号。双向安全模型允许主机系统和嵌入式从DS28EL25之间的双向安全认证。主机系统采用从至主安全认证，安全验证连接或嵌入式DS28EL25的真实可靠性。主至从安全认证用于保护DS28EL25用户存储器不被非法主机更改。DS28EL25产生的SHA-256信息验证代码(MAC)根据用户存储器中的数据、片上密码、主机随机质询及64位ROM ID计算得到。DS28EL25通过单触点1-Wire®总线进行高速通信，通信符合1-Wire协议，在多器件的1-Wire网络中，ROM ID作为节点地址。

应用

联网器械的安全认证

打印机墨盒ID/安全认证

许可管理参考设计

系统知识产权保护

传感器/配件识别和校准

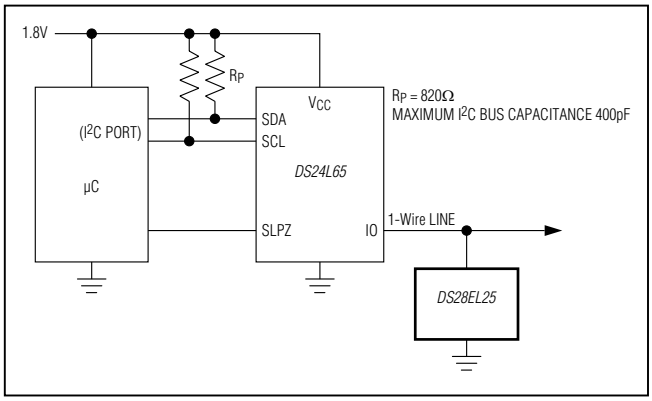
可配置系统的安全功能设置

加密系统的密码发生和交换

特性

- 基于SHA-256的对称加密双向安全认证模型
- 专用的硬件SHA加速引擎产生SHA-256 MAC
- 利用高位计数、用户可编程密码及输入质询进行有效的安全认证
- 4096位用户EEPROM存储器，分为16页，每页256位
- 用户可编程、不可擦除EEPROM保护模式，包括：安全认证、读/写保护以及OTP/EPROM仿真
- 唯一的工厂编程64位识别码
- 单触点1-Wire接口与主机通信，速度可达76.9kbps
- 工作范围：1.8V ±5%，-40°C至+85°C
- 5µA (典型值)低待机功耗
- ±8kV人体模式ESD保护(典型值)
- 6引脚TDFN封装

典型应用电路



定购信息在数据资料的最后给出。

1-Wire和DeepCover是Maxim Integrated Products, Inc.的注册商标。

相关型号以及配合该器件使用的推荐产品，请参见：china.maximintegrated.com/DS28EL25.related。

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.maximintegrated.com。

ABSOLUTE MAXIMUM RATINGS

IO Voltage Range to GND..... -0.5V to 4.0V
IO Sink Current.....20mA
Operating Temperature Range ..... -40°C to +85°C
Junction Temperature .....+150°C
Storage Temperature Range..... -55°C to +125°C
Lead Temperature (soldering, 10s) .....+300°C
Soldering Temperature (reflow) .....+260°C

Stresses beyond those listed under "Absolute Maximum Ratings" may cause permanent damage to the device. These are stress ratings only, and functional operation of the device at these or any other conditions beyond those indicated in the operational sections of the specifications is not implied. Exposure to absolute maximum rating conditions for extended periods may affect device reliability.

ELECTRICAL CHARACTERISTICS

(T_A = -40°C to +85°C, unless otherwise noted.) (Note 1)

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
IO PIN: GENERAL DATA						
1-Wire Pullup Voltage	V_{PUP}	(Note 2)	1.71		1.89	V
1-Wire Pullup Resistance	R_{PUP}	V_{PUP} = 1.8V ±5% (Note 3)	300		750	Ω
Input Capacitance	C_{IO}	(Notes 4, 5)		1500		pF
Input Load Current	I_L	IO pin at V_{PUP}		5	19.5	µA
High-to-Low Switching Threshold	V_{TL}	(Notes 6, 7)		0.65 x V_{PUP}		V
Input Low Voltage	V_{IL}	(Notes 2, 8)			0.3	V
Low-to-High Switching Threshold	V_{TH}	(Notes 6, 9)		0.75 x V_{PUP}		V
Switching Hysteresis	V_{HY}	(Notes 6, 10)		0.3		V
Output Low Voltage	V_{OL}	I_{OL} = 4mA (Note 11)			0.4	V
Recovery Time	t_{REC}	R_{PUP} = 750Ω (Notes 2, 12)	5			µs
Time-Slot Duration	t_{SLOT}	(Notes 2, 13)	13			µs
IO PIN: 1-Wire RESET, PRESENCE-DETECT CYCLE						
Reset Low Time	t_{RSTL}	(Note 2)	48		80	µs
Reset High Time	t_{RSTH}	(Note 14)	48			µs
Presence-Detect Sample Time	t_{MSP}	(Notes 2, 15)	8		10	µs
IO PIN: 1-Wire WRITE						
Write-Zero Low Time	t_{W0L}	(Notes 2, 16)	8		16	µs
Write-One Low Time	t_{W1L}	(Notes 2, 16)	1		2	µs
IO PIN: 1-Wire READ						
Read Low Time	t_{RL}	(Notes 2, 17)	1		2 - δ	µs
Read Sample Time	t_{MSR}	(Notes 2, 17)	t_{RL} + δ		2	µs
EEPROM						
Programming Current	I_{PROG}	V_{PUP} = 1.89V (Notes 5, 18)			1	mA
Programming Time for a 32-Bit Segment or Page Protection	t_{PRD}	(Note 19)			10	ms
Programming Time for the Secret	t_{PRS}	(Note 20)			200	ms
Write/Erase Cycling Endurance	N_{CY}	T_A = +85°C (Notes 21, 22)	100k			—
Data Retention	t_{DR}	T_A = +85°C (Notes 23, 24, 25)	10			Years

ELECTRICAL CHARACTERISTICS (continued)

(T_A = -40°C to +85°C, unless otherwise noted.) (Note 1)

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
SHA-256 ENGINE						
Computation Current	I_{CSHA}	V_{PUP} = 1.89V (Notes 5, 18)			1	mA
Computation Time	t_{CSHA}	(Notes 5, 26)			3	ms

Note 1: Limits are 100% production tested at T_A = +25°C and/or T_A = +85°C. Limits over the operating temperature range and relevant supply voltage range are guaranteed by design and characterization. Typical values are not guaranteed.
Note 2: System requirement.
Note 3: Maximum allowable pullup resistance is a function of the number of 1-Wire devices in the system and 1-Wire recovery times. The specified value here applies to systems with only one device and with the minimum 1-Wire recovery times.
Note 4: Typical value represents the internal parasite capacitance when V_{PUP} is first applied. Once the parasite capacitance is charged, it does not affect normal communication.
Note 5: Guaranteed by design and/or characterization only; not production tested.
Note 6: V_{TL}, V_{TH}, and V_{HY} are a function of the internal supply voltage, which is a function of V_{PUP}, R_{PUP}, 1-Wire timing, and capacitive loading on IO. Lower V_{PUP}, higher R_{PUP}, shorter t_{REC}, and heavier capacitive loading all lead to lower values of V_{TL}, V_{TH}, and V_{HY}.
Note 7: Voltage below which, during a falling edge on IO, a logic-zero is detected.
Note 8: The voltage on IO must be less than or equal to V_{ILMAX} at all times when the master is driving IO to a logic-zero level.
Note 9: Voltage above which, during a rising edge on IO, a logic-one is detected.
Note 10: After V_{TH} is crossed during a rising edge on IO, the voltage on IO must drop by at least V_{HY} to be detected as logic-zero.
Note 11: The I-V characteristic is linear for voltages less than 1V.
Note 12: Applies to a single device attached to a 1-Wire line.
Note 13: Defines maximum possible bit rate. Equal to $1/(t_{W0LMIN} + t_{RECMIN})$.
Note 14: An additional reset or communication sequence cannot begin until the reset high time has expired.
Note 15: Interval after t_{RSTL} during which a bus master can read a logic 0 on IO if there is a DS28EL25 present. The power-up presence detect pulse could be outside this interval. See the *Typical Operating Characteristics* for details.
Note 16: ε in Figure 11 represents the time required for the pullup circuitry to pull the voltage on IO up from V_{IL} to V_{TH}. The actual maximum duration for the master to pull the line low is $t_{W1LMAX} + t_F - \varepsilon$ and $t_{W0LMAX} + t_F - \varepsilon$, respectively.
Note 17: δ in Figure 11 represents the time required for the pullup circuitry to pull the voltage on IO up from V_{IL} to the input-high threshold of the bus master. The actual maximum duration for the master to pull the line low is $t_{RLMAX} + t_F$.
Note 18: Current drawn from IO during the EEPROM programming interval or SHA-256 computation. The pullup circuit on IO during the programming and computation interval should be such that the voltage at IO is greater than or equal to V_{PUPMIN}. A low-impedence bypass of R_{PUP} activated during programming and computation is the recommended way to meet this requirement.
Note 19: Refer to the full data sheet.

Note 20: Refer to the full data sheet.

Note 21: Write-cycle endurance is tested in compliance with JESD47G.
Note 22: Not 100% production tested; guaranteed by reliability monitor sampling.
Note 23: Data retention is tested in compliance with JESD47G.
Note 24: Guaranteed by 100% production test at elevated temperature for a shorter time; equivalence of this production test to the data sheet limit at operating temperature range is established by reliability testing.
Note 25: EEPROM writes can become nonfunctional after the data retention time is exceeded. Long-term storage at elevated temperatures is not recommended.

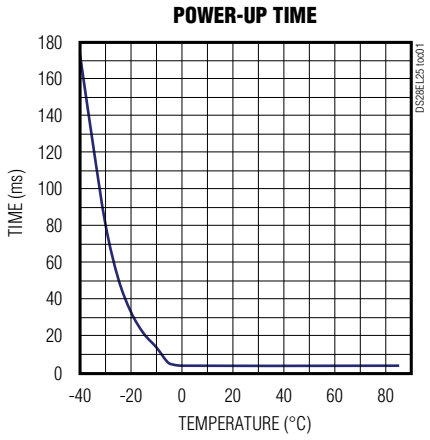
ELECTRICAL CHARACTERISTICS (continued)

(T_A = -40°C to +85°C, unless otherwise noted.) (Note 1)

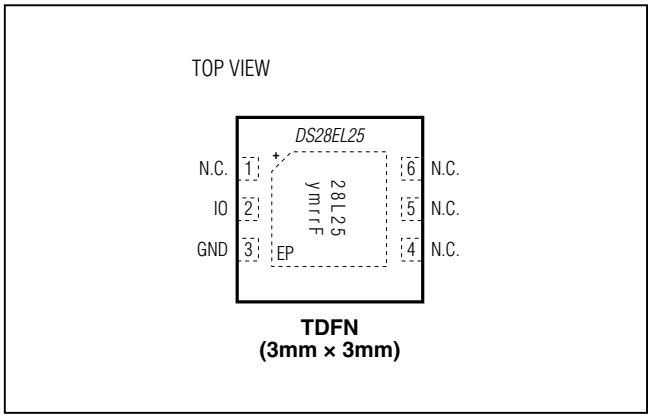
Note 26: Refer to the full data sheet.

典型工作特性

(V_{PUP} = 1.71V, V_{IL} = 0.3V)



引脚配置



TDFN
(3mm × 3mm)

引脚说明

引脚	名称	功能
3	GND	地基准。
2	IO	1-Wire总线接口。开漏信号，需要外部上拉电阻。
1, 4, 5, 6	N.C.	无连接。
—	EP	裸焊盘。均匀焊接至电路板的接地区域以确保正常工作。更多信息请参见应用笔记3273：*Exposed Pads:A Brief Introduction*。

DS28EL25

DeepCover安全认证器，带有1-Wire SHA-256和4Kb用户EEPROM

注意：该文件是完整数据资料的缩略版。其他产品信息仅在完整版的数据资料中。如需申请完整版，请浏览china.maximintegrated.com/DS28EL25并点击**申请数据资料全文**。

定购信息

器件	温度范围	引脚–封装
DS28EL25Q+T	-40°C至+85°C	6 TDFN-EP* (2.5k pcs)

+表示无铅(Pb)/符合RoHS标准的封装。
T = 卷带包装。
**EP = 裸焊盘。*

封装信息

如需最近的封装外形信息和焊盘布局(占位面积)，请查询china.maximintegrated.com/packages。请注意，封装编码中的“+”、“#”或“–”仅表示RoHS状态。封装图中可能包含不同的尾缀字符，但封装图只与封装有关，与RoHS状态无关。

封装类型	封装编码	外形编号	焊盘布局编号
6 TDFN-EP	T633+2	21-0137	90-0058

DS28EL25

DeepCover安全认证器，带有1-Wire SHA-256和4Kb用户EEPROM

修订历史

修订号	修订日期	说明	修改页
0	12/12	最初版本。	—

Maxim北京办事处
北京8328信箱 邮政编码100083
免费电话：800 810 0310
电话：010–6211 5199
传真：010–6211 5299