ATECC508A 概要版数据手册

特性

- 具有基于硬件的安全密钥存储功能的密码协处理器
- 执行高速公钥（PKI）算法
  - ——ECDSA：FIPS186-3 椭圆曲线数字签名算法
  - ——ECDH：FIPS SP800-56A 椭圆曲线 Diffie-Hellman 算法
- NIST 标准 P256 椭圆曲线支持
- 带有 HMAC 选项的 SHA-256 哈希算法
- 主机和客户端操作
- 256 位密钥长度
- 存储最多 16 个密钥
- 两个高耐擦写单调计数器
- 有保证的惟一 72 位序列号
- 内部高质量 FIPS 随机数发生器（Random Number Generator，RNG）
- 用于密钥、证书和数据的 10 Kb EEPROM 存储器
- 用于消耗记录和一次写入信息的多个选项
- 外部防篡改开关的入侵锁存器或上电片选功能。多个 I/O 选项：
  - ——高速单引脚接口，带一个 GPIO 引脚
  - ——1 MHz 标准 I^2C 接口
- 2.0V 至 5.5V 电源电压范围
- 1.8V 至 5.5V IO 电平
- <150 nA 的休眠电流
- 8 焊点 UDFN、8 引脚 SOIC 和 3 引脚触点式封装

应用

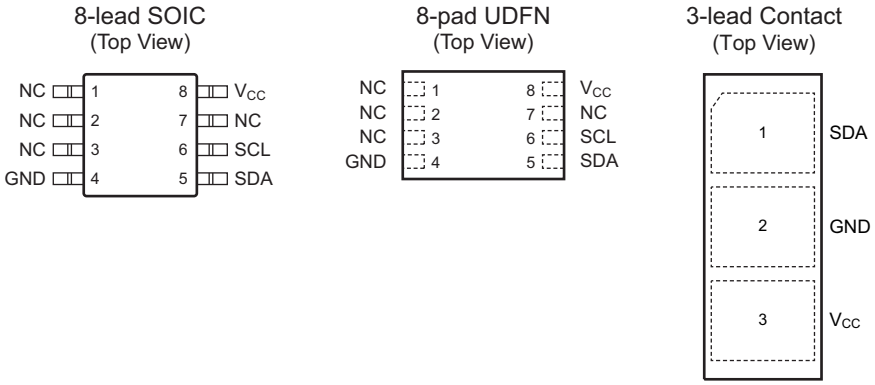
- 物联网节点安全和 ID
- 安全下载和启动
- 生态系统控制
- 报文安全
- 反克隆

封装类型

表 1. 引脚配置

引脚	功能
NC	无连接
GND	地
SDA	串行数据
SCL	串行时钟输入
V_{CC}	电源

图 1. 封装类型



目录

1. 简介

1.1 应用

ATECC508A 器件属于 Microchip CryptoAuthentication™ 系列加密引擎身份验证器件，具有基于硬件的高度安全密钥存储功能。

ATECC508A 器件具有灵活的命令集，可在许多应用中使用，其中包括：

- **网络/物联网节点保护**——验证节点 ID，确保报文的完整性，并支持密钥协议以创建用于报文加密的会话密钥。
- **防伪**——验证可移除、可更换或可消耗的客户端是否可信。客户端的示例可以是系统配件、电子子卡或其他备件。此器件也可用于验证软件/固件模块或存储器存储元件。
- **保护固件或介质**——在启动时验证存储在闪存中的代码以防止未经授权的修改，将下载的程序文件作为普通广播进行加密或者将代码映像单独加密为仅在单个系统上可用。
- **存储安全数据**——将加密加速器使用的机密信息密钥存储在标准微处理器中。进行加密/验证的读取和写入操作时，可实现可编程保护。
- **检查用户密码**——验证用户输入的密码而不让预期值变为已知，将可存储的密码映射到随机数上，并与远程系统安全地交换密码值。

1.2 器件特性

ATECC508A 包括 EEPROM 阵列，此阵列可用于存储最多 16 个密钥、证书、其他读/写内容、只读或机密数据、消耗记录和安全配置。可通过不同方式限制对存储器各个部分的访问，并可随后锁定配置以防止更改。

ATECC508A 具有多种专门设计的防御机制，可防止对器件本身的物理攻击，或对器件和系统之间传输的数据的逻辑攻击。密钥的使用或生成方式上设有硬件限制，这可为某些方式的攻击提供进一步的防御。

通过标准 I^2C 接口访问器件，速度最高 1 Mbps。此接口与标准串行 EEPROM I^2C 接口规范兼容。此器件还支持单线接口（Single-Wire Interface，SWI），可减少系统处理器上所需的 GPIO 数量，并且/或者减少连接器上的引脚数。如果使能单线接口，剩下的引脚可用作 GPIO、验证输出或篡改输入。

使用 I^2C 或单线接口时，多个 ATECC508A 器件可共用同一总线，从而减少处理器 GPIO 在多客户端（例如，不同颜色的墨水罐或多个备件）系统中的使用。

每个 ATECC508A 都附带一个有保证的惟一 72 位序列号。通过使用器件支持的加密协议，主机系统或远程服务器可以验证序列号的签名来证明序列号真实可信而非副本。序列号通常存储在标准串行 EEPROM 中；但这些序列号很容易复制，主机无法了解序列号是真实可信还是复制品。

ATECC508A 可以生成高质量的 FIPS 随机数，并将其用于任何目的，包括作为器件加密协议的一部分。由于可保证每个随机数本质上不同于本机或任何其他设备上生成的所有数字，因此将其包含在协议计算中可确保重放攻击（即重新传输先前成功的事务）始终失败。

由于具备宽电源电压范围（2.0V 至 5.5V）和超低休眠电流（<150 nA）的特性，系统集成非常简单。有关完整直流参数的信息，请参见 2. 电气特性部分。提供多种封装选项（见 产品标识体系和 5. 封装图部分）。

有关 Microchip ATSHA204A 和 ATECC108A 器件兼容性的信息，请参见 3. 兼容性部分。

1.3 加密操作

ATECC508A 实现了一种基于椭圆曲线加密技术和 ECDSA 签名协议的完整非对称（公/私）密钥加密签名解决方案。此器件提供 NIST 标准 P256 素曲线的硬件加速，并支持从高品质私钥生成到 ECDSA 签名生成、ECDH 密钥协议和 ECDSA 公钥签名验证的完整密钥生命周期。

硬件加速器实现此类非对称加密操作的速度可达到标准微处理器上运行软件的十倍到一千倍，没有标准微处理器所特有的常见高密钥暴露风险。

此器件用于安全地存储多个私钥及其关联的公钥和证书。签名验证命令可以使用任何存储的或外部 ECC 公钥。存储在器件中的公钥可以配置为需要通过证书链进行验证，以加快随后的器件验证速度。

器件内部支持随机私钥生成，确保器件外部始终不会获知私钥。对应于所存储私钥的公钥始终在生成密钥时返回，可选择稍后再计算。

ATECC508A 还支持基于哈希算法的标准质询-响应协议，以简化编程。在最基本的实例中，系统向器件发送一个质询，器件通过 MAC、HMAC 或 SHA 命令将质询与机密信息密钥组合，然后将响应发送回系统。器件使用 SHA-256 加密哈希算法来实现此组合，这样总线上的观察者便无法得出机密信息密钥的值，但通过对接收者系统上存储的机密信息副本执行相同的计算来保留接收者验证此响应是否正确的能力。

由于 ATECC508A 具有灵活的命令集，这些基本操作集（即，ECDSA 签名、ECDH 密钥协议和 SHA-256 质询-响应）可通过多种方式扩展。使用 GenDig 命令时，其他槽中的值可以包含在响应摘要或签名中，这提供了一种有效方式来证明所读取的数据确实来自器件，而不是由中间人攻击者插入。此命令可用于将两个密钥与质询相结合，这在要执行多层验证时十分有用。

在主机（例如手机）需要验证客户端（例如 OEM 电池）的主机-客户端配置中，需要将机密信息存储在主机中以验证来自客户端的响应。此 CheckMac 命令允许器件将机密信息安全地存储到主机系统中，并隐藏来自引脚的正确响应值，仅向系统返回 yes 或 no 回答。

最后，质询和机密信息密钥的哈希组合可保存在器件上，并与槽中的内容进行异或运算以实现加密 Read 命令，此组合也可以与加密的输入数据进行异或运算以实现加密 Write 命令。

所有哈希函数均采用行业标准的 SHA-256 安全哈希算法实现，此算法是各政府机构和密码专家推荐的最新一代高安全性加密算法的一部分。ATECC508A 采用完整大小的 256 位机密信息密钥来防止任何形式的穷举攻击。

1.4 命令

ATECC508A 是一款基于命令的器件，它从系统接收命令，执行这些命令，然后返回结果或错误代码。在本文档中，使用以下命名法来描述各种命令：

- **安全命令：**这组命令通常用于访问 EEPROM 空间和/或执行加密计算。这些命令在本文档中用特殊字体表示（例如，GenDig）并可从所有接口获得。
- **加密命令：**此安全命令子集包含访问硬件 ECC 加速器的所有 ECC 命令（GenKey、Sign、ECDH 和 Verify）以及访问硬件 SHA 加速器的 SHA 命令（CheckMac、DeriveKey、GenDig、HMAC、MAC、SHA 和 Nonce）。

2. 电气特性

2.1 绝对最大值

工作温度	-40°C 至+85°C
存储温度	-65°C 至+150°C
最大工作电压	6.0V
直流输出电流	5 mA
任一引脚上的电压	-0.5V 至（V_{CC} + 0.5V）

注： 如果器件的工作条件超过上述“绝对最大值”，可能对器件造成永久性损坏。上述数值仅是工作条件最大值，我们建议不要使器件工作在最大值甚至超过最大值的条件下。器件长时间工作在绝对最大值条件下，其可靠性可能受到影响。

2.2 可靠性

ATECC508A 采用 Microchip 公司具有极高可靠性的 CMOS EEPROM 制造技术制作。

表 2-1. EEPROM 可靠性

参数	最小值	典型值	最大值	单位
+85°C 下的耐写入次数（每个字节）	400,000			写周期
+55°C 下的数据保持时间	10			年
+35°C 下的数据保持时间	30	50		年
耐读取次数	无限制			读周期

2.3 交流参数：所有 I/O 接口

图 2-1. 交流时序图：所有接口

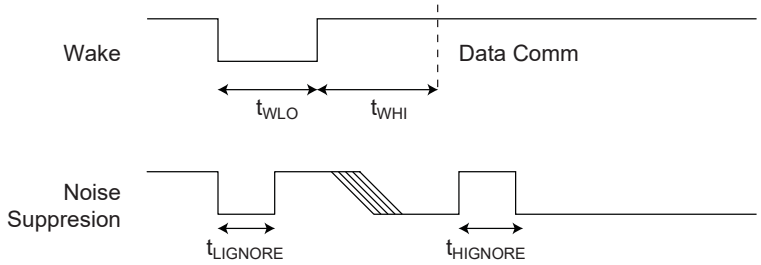


表 2-2. 交流参数：所有 I/O 接口

参数（注）	符号	方向	最小值	典型值	最大值	单位	条件
上电延时	t_{PU}	至加密验证	100		—	µs	从 V_{CC} > V_{CC} min 到测量 t_{WLO} 的最短时间。
唤醒为低电平的持续时间	t_{WLO}	至加密验证	60		—	µs	
唤醒为高电平到数据通信的延时	t_{WHI}	至加密验证	1500			µs	SDA 在整个过程中应保持稳定的高电平状态。
上桥臂毛刺滤波器激活时间	$t_{HIGNORE\_A}$	至加密验证	45（注）			ns	无论激活时的状态如何，宽度短于此时间的脉冲都将被器件忽略。
下桥臂毛刺滤波器激活时间	$t_{LIGNORE\_A}$	至加密验证	45（注）			ns	无论激活时的状态如何，宽度短于此时间的脉冲都将被器件忽略。
下桥臂毛刺滤波器休眠时间	$t_{LIGNORE\_S}$	至加密验证	15（注）			µs	处于休眠模式时，宽度短于此时间的脉冲将被器件忽略。
看门狗超时	$t_{WATCHDOG}$	至加密验证	0.7	1.3	1.7	s	从唤醒到强制器件进入休眠模式的最长时间。

注： 这些参数为特性值，但未经测试。

2.3.1 交流参数：单线接口

图 2-2. 交流时序图：单线接口

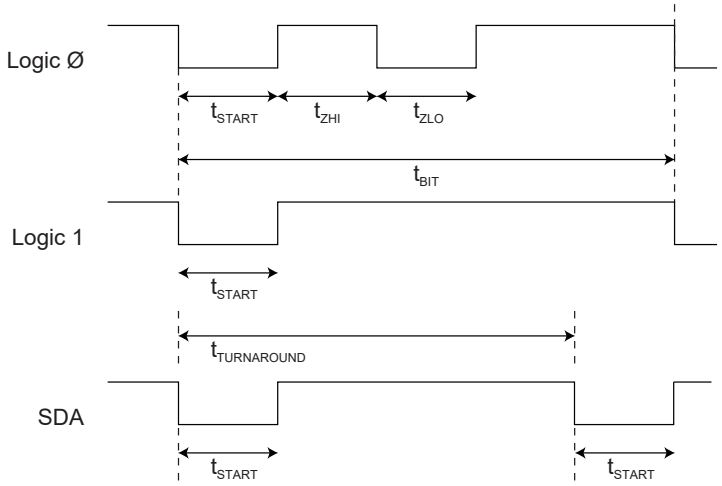


表 2-3. 交流参数：单线接口

除非另外说明，否则适用条件为：T_A = -40°C 至+85°C，V_{CC} = +2.0V 至+5.5V，CL =100 pF。

参数	符号	方向	最小值	典型值	最大值	单位	注
启动脉冲持续时间	t_{START}	至加密验证	4.10	4.34	4.56	µs	
		自加密验证	4.60	6	8.60	µs	
零传输高电平脉冲	t_{ZHI}	至加密验证	4.10	4.34	4.56	µs	
		自加密验证	4.60	6	8.60	µs	
零传输低电平脉冲	t_{ZLO}	至加密验证	4.10	4.34	4.56	µs	
		自加密验证	4.60	6	8.60	µs	
位时间（注）	t_{BIT}	至加密验证	37	39	—	µs	如果位时间超过 $t_{TIMEOUT}$，则 ATECC508A 可能进入休眠模式。
		自加密验证	41	54	78	µs	
周转延时	$t_{TURNAROUND}$	自加密验证	64	96	131	µs	在传输标志最后一位的起始脉冲的初始下降沿之后的这段时间间隔后，ATECC508A 将启动第一个低电平转换。
		至加密验证	93			µs	在 ATECC508A 传输组的最后一位后，系统必须等待此段时间间隔，之后才能发送标志的第一位。此时间从 ATECC508A 所传输最后一位的起始脉冲的下降沿开始测量。
IO 超时	$t_{TIMEOUT}$	至加密验证	45	65	85	ms	如果总线处于非活动状态的时间超过此持续时间，则 ATECC508A 可能转换为休眠模式。

注： START、ZLO、ZHI 和 BIT 设计为与发送和接收都以 230.4 Kbaud 速率运行的标准 UART 兼容。UART 应设置为 7 个数据位、无奇偶校验和 1 个停止位。

2.3.2 交流参数：I²C 接口

图 2-3. I²C 同步数据时序

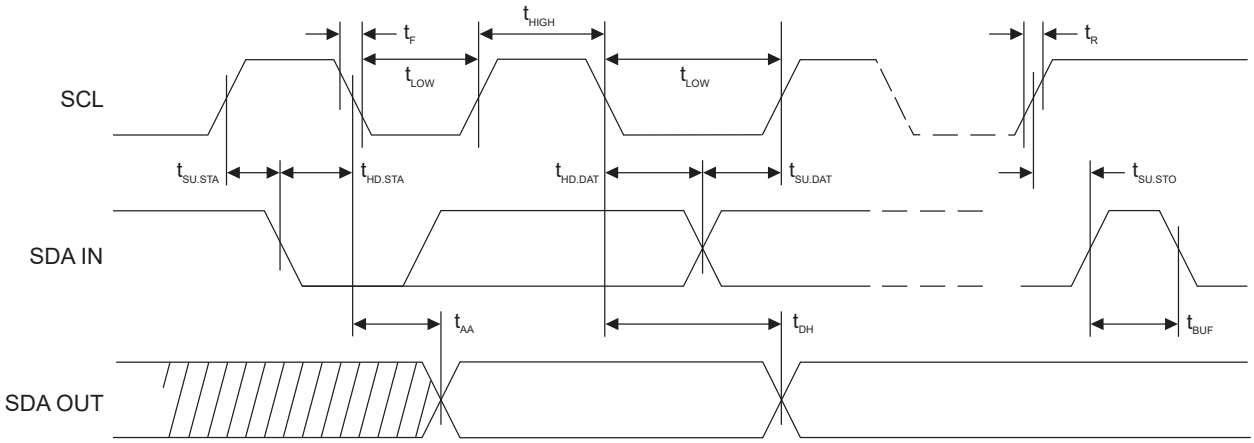


表 2-4. I²C 接口的交流特性

除非另外说明，否则适用的推荐工作范围为：T_A = -40°C 至+ 85°C，V_{CC} = +2.0V 至+5.5V，CL = 1 TTL 栅极和 100 pF。

参数	符号	最小值	最大值	单位
SCK 时钟频率	f_{SCK}	0	1	MHz
SCK 高电平时间	t_{HIGH}	400		ns
SCK 低电平时间	t_{LOW}	400		ns
启动条件建立时间	$t_{SU.STA}$	250		ns
启动条件保持时间	$t_{HD.STA}$	250		ns
停止条件建立时间	$t_{SU.STO}$	250		ns
数据输入建立时间	$t_{SU.DAT}$	100		ns
数据输入保持时间	$t_{HD.DAT}$	0		ns
输入上升时间(1)	t_R		300	ns
输入下降时间(1)	t_F		100	ns
时钟低电平到数据输出有效的时间	t_{AA}	50	550	ns
数据输出保持时间	t_{DH}	50		ns
SMBus 超时延时	$t_{TIMEOUT}$	25	75	ms
在新传输开始前时间总线必须保持空闲的时间。（1）	t_{BUF}	500		ns

注：

1. 上述值均为特性值，未经测试
2. 交流测量条件：
   - ——RL（连接 SDA 和 V_{CC}）：1.2 kΩ（对于 V_{CC} + 2.0V 至 + 5.0V）
   - ——输入脉冲电压：0.3 V_{CC} 至 0.7 V_{CC}
   - ——输入上升和下降时间：≤ 50 ns
   - ——输入和输出时序参考电压：0.5V_{CC}

2.4 直流参数：所有 I/O 接口

表 2-5. 所有 I/O 接口上的直流参数

参数	符号	最小值	典型值	最大值	单位	条件
环境工作温度	T_A	-40	—	85	°C	
电源电压	V_{CC}	2.0	—	5.5	V	
电源工作电流	I_{CC}	—	3	6	mA	在 I/O 传输期间或执行非 ECC 命令期间等待 I/O。
		—	—	16	mA	在 ECC 命令执行期间。
空闲电源电流	I_{IDLE}	—	800	—	µA	当器件处于空闲模式时，V_{SDA} 和 V_{SCL} < 0.4V 或> V_{CC} – 0.4
休眠电流	I_{SLEEP}	—	30	150	nA	当器件处于休眠模式时，$V_{CC} \le 3.6V$，V_{SDA} 和 V_{SCL} < 0.4V 或> V_{CC} – 0.4，$T_A \le +55°C$
		—	—	2	µA	当器件处于休眠模式时。
输出低电压	V_{OL}	—	—	0.4	V	当器件处于工作模式时，V_{CC} = 2.5 - 5.5V
输出低电流	I_{OL}	—	—	4	mA	当器件处于工作模式时，V_{CC} = 2.5 - 5.5V，V_{OL} = 0.4V
Theta JA	Θ_{JA}	—	166	—	°C/W	SOIC（SSH）
		—	173	—	°C/W	UDFN（MAH）
		—	146	—	°C/W	RBH

2.4.1 V_{IH} 和 V_{IL} 规范

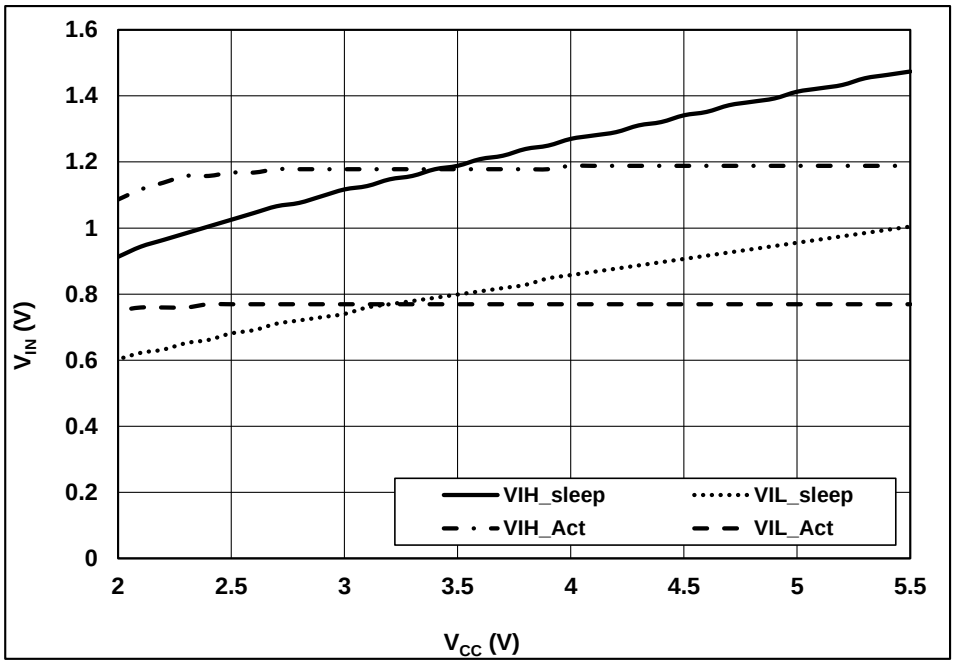
器件的输入电平将根据器件的模式和电压而变化。休眠或空闲模式下的输入电压阈值取决于 V_{CC} 电平，如图 2-4 所示。在休眠或空闲模式下时，TTLenable 位不起作用。

器件处于工作状态（即不处于休眠或空闲模式）时，输入电压阈值取决于 EEPROM 配置区域中的 ChipMode 字节中 TTLenable（bit 1）的状态。如果 ATECC508A 的 V_{CC} 引脚的供电电压与输入上拉电阻所连接的系统电压不同，系统设计人员可以选择将 TTLenable 设置为 0，从而使能一个固定的输入阈值（如图 2-4 中的曲线 VIL_ACT 和 VIH_ACT 所示）。 表 2-6 仅在器件处于工作状态时适用，其中给出了在该模式下工作时确保的工作电压。

表 2-6. 所有 I/O 接口上的 V_{IL} 和 V_{IH}（TTLenable = 0 时）

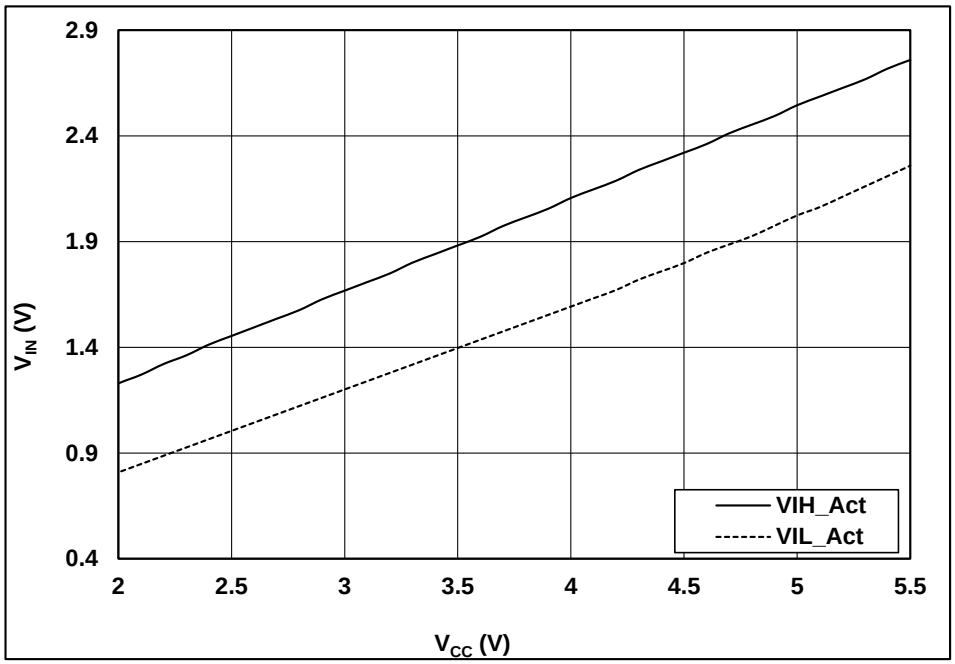
参数	符号	最小值	典型值	最大值	单位	条件
输入低电压	V_{IL}	-0.5		0.5	V	当器件处于工作状态且配置存储器中的 TTLenable 位为 0 时；否则请参见上文。
输入高电压	V_{IH}	1.5		V_{CC} + 0.5	V	当器件处于工作状态且配置存储器中的 TTLenable 位为 0 时；否则请参见上文。

图 2-4. 所有 I/O 接口上的 V_{IH} 和 V_{IL}（休眠或空闲模式下或者 TTLenable = 0 时）



当公共电压用于 ATECC508A V_{CC} 引脚和输入上拉电阻时，TTLenable 位应设置为 1，从而允许输入阈值跟踪电源，如图 2-5 所示。

图 2-5. 所有 I/O 接口上的 V_{IH} 和 V_{IL}（工作模式下且 TTLenable = 1 时）



3. 兼容性

3.1 Microchip ATSHA204A

ATECC508A 与 ATSHA204 和 ATSHA204A 器件完全兼容。如果配置正确，则它可在目前采用 ATSHA204 或 ATSHA204A 的所有情况下使用。由于 Configuration 区域较大，因此在对 ATSHA204 或 ATSHA204A 进行个性化设置时，必须更新器件的个性化步骤。要获得正确的兼容性，应注意包含与 ATSHA204 或 ATSHA204A 序列一起使用的密钥的 KeyType、ReqRandom 和 ReqAuth 槽。

3.2 Microchip ATECC108A

ATECC508A 设计为与 ATECC108 和 ATECC108A 器件完全兼容。如果配置正确，则可在目前采用 ATECC108 的所有情况下使用。在许多情况下，ATECC508A 也可以在不做更改的情况下用于 ATECC108 应用。新版本提供了下列显著优势：

- **ATECC508A 相比于 ATECC108A 的其他特性**
  - ECDH 命令
  - 高耐擦写单调计数器
  - 通过证书实现公钥失效
- **少量更改**
  - GenDig 命令用于验证生成传输密钥时是否使用随机临时值
  - Info 命令 DevRev 模式现在将为 ATECC108A 返回 0x1005，为 ATECC508A 返回 0x5000。由于此值将随每个次要版本而变化，因此不应在软件中使用。

4. 封装标识信息

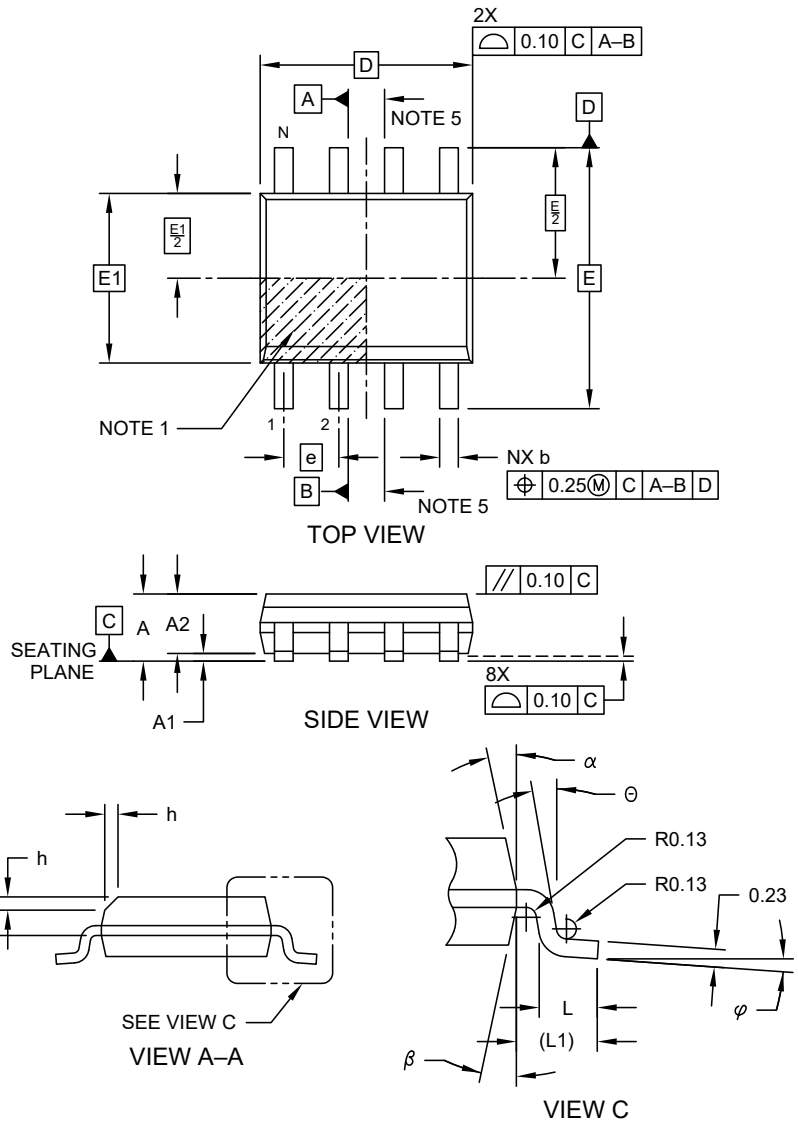
作为 Microchip 整体安全功能的一部分，所有加密器件的器件标识都有意进行了模糊处理。封装顶部的标识不提供有关器件的实际类型或制造商的任何信息。封装上的字母数字代码提供制造信息，并随装配批次变化。封装标识不应作为即将进行的任何检查步骤的一部分。

5. 封装图

5.1 8 引脚 SOIC

8-Lead Plastic Small Outline - Narrow, 3.90 mm (.150 In.) Body [SOIC]
Atmel Legacy

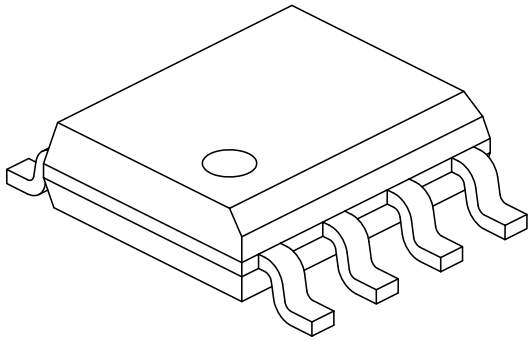
Note:	For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



Microchip Technology Drawing No. C04-057-Atmel Rev D Sheet 1 of 2

8-Lead Plastic Small Outline - Narrow, 3.90 mm (.150 In.) Body [SOIC]
Atmel Legacy

Note: For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



Units		MILLIMETERS		
Dimension Limits		MIN	NOM	MAX
Number of Pins	N		8	
Pitch	e		1.27 BSC	
Overall Height	A	-	-	1.75
Molded Package Thickness	A2	1.25	-	-
Standoff §	A1	0.10	-	0.25
Overall Width	E		6.00 BSC	
Molded Package Width	E1		3.90 BSC	
Overall Length	D		4.90 BSC	
Chamfer (Optional)	h	0.25	-	0.50
Foot Length	L	0.40	-	1.27
Footprint	L1		1.04 REF	
Foot Angle	φ	0°	-	8°
Lead Thickness	c	0.17	-	0.25
Lead Width	b	0.31	-	0.51
Mold Draft Angle Top	α	5°	-	15°
Mold Draft Angle Bottom	β	5°	-	15°

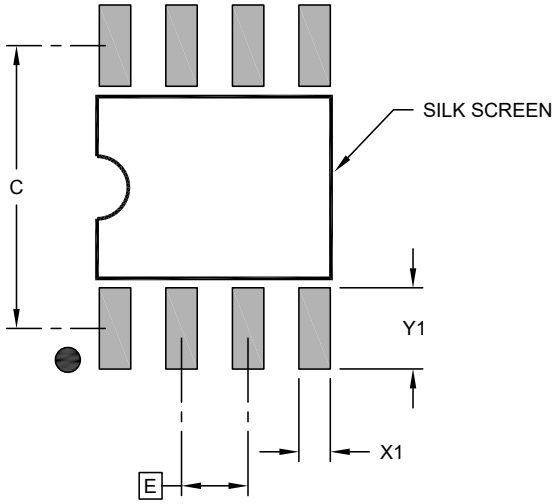
Notes:

1. Pin 1 visual index feature may vary, but must be located within the hatched area.
2. § Significant Characteristic
3. Dimensions D and E1 do not include mold flash or protrusions. Mold flash or protrusions shall not exceed 0.15mm per side.
4. Dimensioning and tolerancing per ASME Y14.5M
   BSC: Basic Dimension. Theoretically exact value shown without tolerances.
   REF: Reference Dimension, usually without tolerance, for information purposes only.
5. Datums A & B to be determined at Datum H.

Microchip Technology Drawing No. C04-057-OA Rev D Sheet 2 of 2

8-Lead Plastic Small Outline - Narrow, 3.90 mm (.150 In.) Body [SOIC]
Atmel Legacy

Note:	For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



RECOMMENDED LAND PATTERN

Units		MILLIMETERS		
Dimension Limits		MIN	NOM	MAX
Contact Pitch	E		1.27 BSC	
Contact Pad Spacing	C		5.40	
Contact Pad Width (X8)	X1			0.60
Contact Pad Length (X8)	Y1			1.55

Notes:

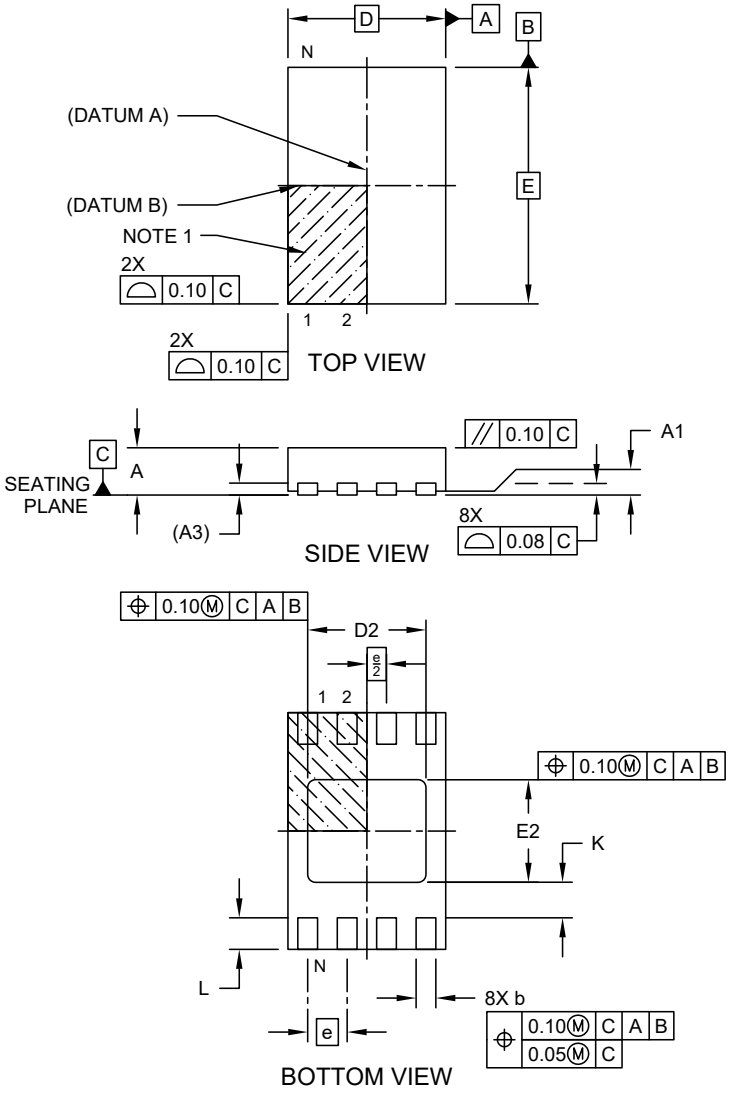
1. Dimensioning and tolerancing per ASME Y14.5M
   BSC: Basic Dimension. Theoretically exact value shown without tolerances.

Microchip Technology Drawing C04-2057-M6B Rev B

5.2 8 焊点 UDFN

8-Lead Ultra Thin Plastic Dual Flat, No Lead Package (Q4B) - 2x3 mm Body [UDFN]
Atmel Legacy YNZ Package

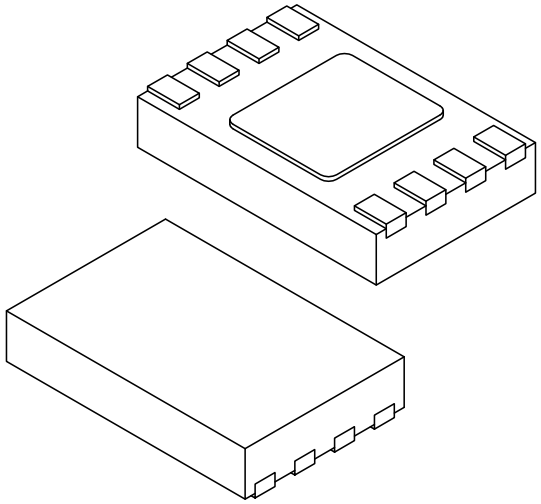
Note:	For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



Microchip Technology Drawing C04-21355-Q4B Rev A Sheet 1 of 2

8-Lead Ultra Thin Plastic Dual Flat, No Lead Package (Q4B) - 2x3 mm Body [UDFN]
Atmel Legacy YNZ Package

Note: For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



Units		MILLIMETERS		
Dimension Limits		MIN	NOM	MAX
Number of Terminals	N		8	
Pitch	e		0.50 BSC	
Overall Height	A	0.50	0.55	0.60
Standoff	A1	0.00	0.02	0.05
Terminal Thickness	A3		0.152 REF	
Overall Length	D		2.00 BSC	
Exposed Pad Length	D2	1.40	1.50	1.60
Overall Width	E		3.00 BSC	
Exposed Pad Width	E2	1.20	1.30	1.40
Terminal Width	b	0.18	0.25	0.30
Terminal Length	L	0.35	0.40	0.45
Terminal-to-Exposed-Pad	K	0.20	-	-

Notes:

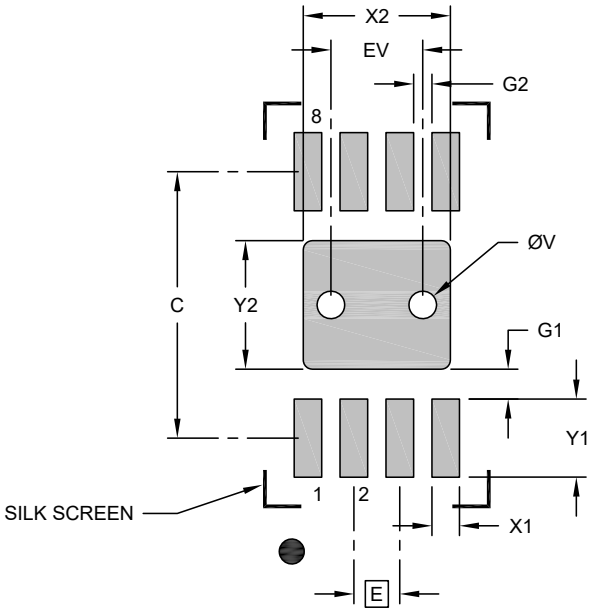
1. Pin 1 visual index feature may vary, but must be located within the hatched area.
2. Package is saw singulated
3. Dimensioning and tolerancing per ASME Y14.5M

BSC: Basic Dimension. Theoretically exact value shown without tolerances.
REF: Reference Dimension, usually without tolerance, for information purposes only.

Microchip Technology Drawing C04-21355-Q4B Rev A Sheet 2 of 2

8-Lead Ultra Thin Plastic Dual Flat, No Lead Package (Q4B) - 2x3 mm Body [UDFN]
Atmel Legacy YNZ Package

Note: For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



RECOMMENDED LAND PATTERN

Units		MILLIMETERS		
Dimension Limits		MIN	NOM	MAX
Contact Pitch	E		0.50 BSC	
Optional Center Pad Width	X2			1.60
Optional Center Pad Length	Y2			1.40
Contact Pad Spacing	C		2.90	
Contact Pad Width (X8)	X1			0.30
Contact Pad Length (X8)	Y1			0.85
Contact Pad to Center Pad (X8)	G1	0.20		
Contact Pad to Contact Pad (X6)	G2	0.33		
Thermal Via Diameter	V		0.30	
Thermal Via Pitch	EV		1.00	

Notes:

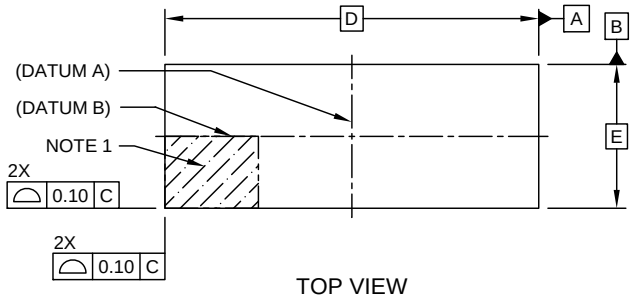
1. Dimensioning and tolerancing per ASME Y14.5M
   BSC: Basic Dimension. Theoretically exact value shown without tolerances.
2. For best soldering results, thermal vias, if used, should be filled or tented to avoid solder loss during reflow process

Microchip Technology Drawing C04-21355-Q4B Rev A

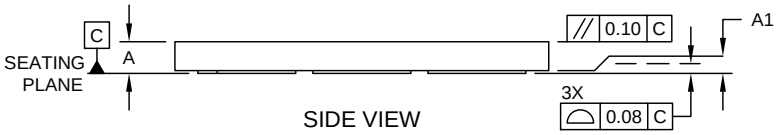
5.3 3 引脚触点式

3-Lead Contact Package (LAB) - 6.54x2.5 mm Body [Contact]
Atmel Legacy Global Package Code RHB

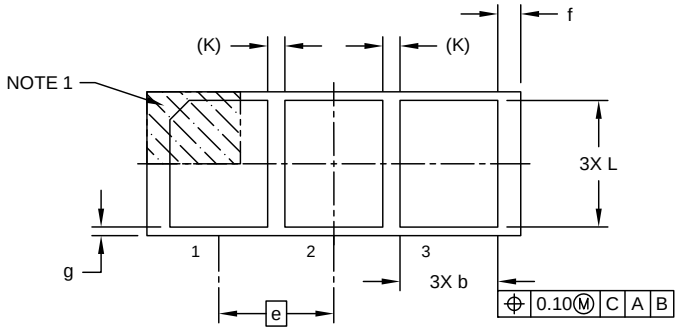
Note:	For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



TOP VIEW



SIDE VIEW

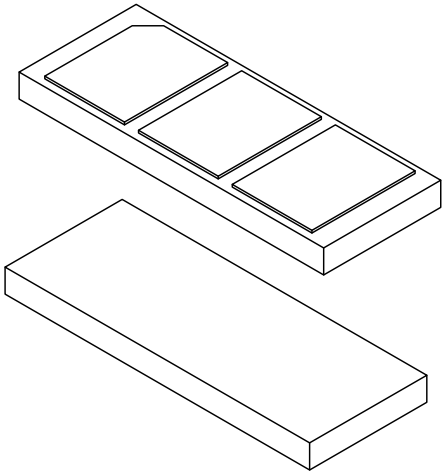


BOTTOM VIEW

Microchip Technology Drawing C04-21303 Rev A Sheet 1 of 2

3-Lead Contact Package (LAB) - 6.54x2.5 mm Body [Contact]
Atmel Legacy Global Package Code RHB

Note: For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



Units		MILLIMETERS		
Dimension Limits		MIN	NOM	MAX
Number of Terminals	N		3	
Pitch	e		2.00 BSC	
Overall Height	A	0.45	0.50	0.55
Standoff	A1	0.00	0.02	0.05
Overall Length	D		6.50 BSC	
Overall Width	E		2.50 BSC	
Terminal Width	b	1.60	1.70	1.80
Terminal Length	L	2.10	2.20	2.30
Terminal-to-Terminal Spacing	K		0.30 REF	
Package Edge to Terminal Edge	f	0.30	0.40	0.50
Package Edge to Terminal Edge	g	0.05	0.15	0.25

Notes:

1. Pin 1 visual index feature may vary, but must be located within the hatched area.
2. Dimensioning and tolerancing per ASME Y14.5M
   BSC: Basic Dimension. Theoretically exact value shown without tolerances.
   REF: Reference Dimension, usually without tolerance, for information purposes only.

Microchip Technology Drawing C04-21303 Rev A Sheet 2 of 2

6. 版本历史

版本 A（2017 年 12 月）
本文档的初始版本

该版本自 2016 年 3 月 8 日起取代 Atmel 文档修订版 8923FX

Microchip 网站

Microchip 网站 http://www.microchip.com/为客户提供在线支持。客户可通过该网站方便地获取文件和信息。只要使用常用的互联网浏览器即可访问，网站提供以下信息：

- **产品支持**——数据手册和勘误表、应用笔记和示例程序、设计资源、用户指南以及硬件支持文档、最新的软件版本以及归档软件
- **一般技术支持**——常见问题（FAQ）、技术支持请求、在线讨论组以及 Microchip 顾问计划成员名单
- **Microchip 业务**——产品选型和订购指南、最新 Microchip 新闻稿、研讨会和活动安排表、Microchip 销售办事处、代理商以及工厂代表列表

变更通知客户服务

Microchip 的变更通知客户服务有助于客户了解 Microchip 产品的最新信息。注册客户可在他们感兴趣的某个产品系列或开发工具发生变更、更新、发布新版本或勘误表时，收到电子邮件通知。

欲注册，请登录 Microchip 网站 http://www.microchip.com/。在“支持”（Support）下，点击“变更通知客户”（Customer Change Notification）服务后按照注册说明完成注册。

客户支持

Microchip 产品的用户可通过以下渠道获得帮助：

- 代理商或代表
- 当地销售办事处
- 应用工程师（FAE）
- 技术支持

客户应联系其代理商、代表或应用工程师（FAE）寻求支持。当地销售办事处也可为客户提供帮助。本文档后附有销售办事处的联系方式。

也可通过以下网站获得技术支持： http://www.microchip.com/support

产品标识体系

欲订货或获取价格、交货等信息，请与我公司生产厂或各销售办事处联系。

PART NO.	-XXX	XX	-X
Device	Package	I/O Type	Tape and Reel

器件：	ATECC508A：具有基于硬件的安全密钥存储功能的密码协处理器	
封装选项	SSH	= 8S1，8 引脚（主体宽 0.150”）塑封鸥翼小外形封装（JEDEC SOIC）
	MAH	= 8MA2，8 焊盘（主体 2 x 3 x 0.6 mm）增强散热型塑封超薄双列扁平无脚封装（UDFN）
	RBH	= 3RB，3 引脚（主体 2.5 x 6.5 mm，间距 2.0 mm）触点式封装（Sawn）。
I/O 类型	CZ	= 单线接口
	DA	= I^2C 接口
卷带式选项	B	= 管装
	T	= 大卷盘（尺寸因封装类型而异）
	S	= 小卷盘（仅适用于 MAH）

示例：

- ATECC508A-SSHCZ-T：单线，卷带式，每卷盘 4,000 个，8 引脚 SOIC 封装
- ATECC508A-SSHCZ-B：单线，管装式，每管 100 个，8 引脚 SOIC 封装
- ATECC508A-SSHDA-T：I^2C，卷带式，每卷盘 4,000 个，8 引脚 SOIC 封装
- ATECC508A-SSHDA-B：I^2C，管装式，每管 100 个，8 引脚 SOIC 封装
- ATECC508A-MAHCZ-T：单线，卷带式，每卷盘 15,000 个，8 焊盘 UDFN 封装
- ATECC508A-MAHDA-T：I^2C，卷带式，每卷盘 15,000 个，8 焊盘 UDFN 封装
- ATECC508A-MAHCZ-S：单线，卷带式，每卷盘 3,000 个，8 焊盘 UDFN 封装
- ATECC508A-MAHDA-S：I^2C，卷带式，每卷盘 3,000 个，8 焊盘 UDFN 封装
- ATECC508A-RBHCZ-T：单线，卷带式，每卷盘 5,000 个，3 引脚触点式封装
- ATECC508A-RBHCZ-B：单线，管装式，每管 56 个，3 引脚触点式封装

注：

1. 卷带式标识符仅出现在产品目录的部件编号描述中。该标识符用于订货目的，不会印刷在器件封装上。关于包装是否提供卷带式选项的信息，请咨询当地的 Microchip 销售办事处。
2. 可提供小型封装选项。有关小型封装可用性的信息，请访问 http://www.microchip.com/packaging 或联系您当地的销售办事处。

Microchip 器件代码保护功能

请注意以下有关 Microchip 器件代码保护功能的要点：

- Microchip 的产品均达到 Microchip 数据手册中所述的技术指标。
- Microchip 确信：在正常使用的情况下，Microchip 系列产品是当今市场上同类产品中最安全的产品之一。
- 目前，仍存在着恶意、甚至是非法破坏代码保护功能的行为。就我们所知，所有这些行为都不是以 Microchip 数据手册中规定的操作规范来使用 Microchip 产品的。这样做的人极可能侵犯了知识产权。
- Microchip 愿意与关心代码完整性的客户合作。
- Microchip 或任何其他半导体厂商均无法保证其代码的安全性。代码保护并不意味着我们保证产品是“牢不可破”的。

代码保护功能处于持续发展中。Microchip 承诺将不断改进产品的代码保护功能。任何试图破坏 Microchip 代码保护功能的行为均可视为违反了《数字器件千年版权法案（Digital Millennium Copyright Act）》。如果这种行为导致他人在未经授权的情况下，能访问您的软件或其他受版权保护的成果，您有权依据该法案提起诉讼，从而制止这种行为。

法律声明

本出版物中所述的器件应用信息及其他类似内容仅为您提供便利，它们可能由更新之信息所替代。确保应用符合技术规范，是您自身应负的责任。Microchip 对这些信息不作任何明示或暗示、书面或口头、法定或其他形式的声明或担保，包括但不限于针对其使用情况、质量、性能、适销性或特定用途的适用性的声明或担保。Microchip 对因这些信息及使用这些信息而引起的后果不承担任何责任。如果将 Microchip 器件用于生命维持和/或生命安全应用，一切风险由买方自负。买方同意在由此引发任何一切伤害、索赔、诉讼或费用时，会维护和保障 Microchip 免于承担法律责任，并加以赔偿。除非另外声明，否则在 Microchip 知识产权保护下，不得暗中或以其他方式转让任何许可证。

商标

Microchip 的名称和徽标组合、Microchip 徽标、AnyRate、AVR、AVR 徽标、AVR Freaks、BeaconThings、BitCloud、CryptoMemory、CryptoRF、dsPIC、FlashFlex、flexPWR、Heldo、JukeBlox、KeeLoq、KeeLoq 徽标、Kleer、LANCheck、LINK MD、maXStylus、maXTouch、MediaLB、megaAVR、MOST、MOST 徽标、MPLAB、OptoLyzer、PIC、picoPower、PICSTART、PIC32 徽标、Prochip Designer、QTouch、RightTouch、SAM-BA、SpyNIC、SST、SST 徽标、SuperFlash、tinyAVR、UNI/O 和 XMEGA 是 Microchip Technology Incorporated 在美国和其他国家或地区的注册商标。

ClockWorks、The Embedded Control Solutions Company、EtherSynch、Hyper Speed Control、HyperLight Load、IntelliMOS、mTouch、Precision Edge 和 Quiet-Wire 为 Microchip Technology Incorporated 在美国的注册商标。

Adjacent Key Suppression、AKS、Analog-for-the-Digital Age、Any Capacitor、AnyIn、AnyOut、BodyCom、chipKIT、chipKIT 徽标、CodeGuard、CryptoAuthentication、CryptoCompanion、CryptoController、dsPICDEM、dsPICDEM.net、Dynamic Average Matching、DAM、ECAN、EtherGREEN、In-Circuit Serial Programming、ICSP、Inter-Chip Connectivity、JitterBlocker、KleerNet、KleerNet 徽标、Mindi、MiWi、motorBench、MPASM、MPF、MPLAB Certified 徽标、MPLIB、MPLINK、MultiTRAK、NetDetach、Omniscient Code Generation、PICDEM、PICDEM.net、

ISBN： 978-1-5224-2857-2

DNV 认证的质量管理体系

ISO/TS 16949

Microchip 位于美国亚利桑那州 Chandler 和 Tempe 与位于俄勒冈州 Gresham 的全球总部、设计和晶圆生产厂及位于美国加利福尼亚州和印度的设计中心均通过了 ISO/TS-16949:2009 认证。Microchip 的 PIC® MCU 和 dsPIC® DSC、KEELOQ®跳码器件、串行 EEPROM、单片机外设、非易失性存储器和模拟产品严格遵守公司的质量体系流程。此外，Microchip 在开发系统的设计和生产方面的质量体系也已通过了 ISO 9001:2000 认证。

全球销售及服务网点

美洲

公司总部 Corporate Office
2355 West Chandler Blvd.
Chandler, AZ 85224-6199
Tel: 1-480-792-7200
Fax: 1-480-792-7277
技术支持：
http://www.microchip.com/support
网址：www.microchip.com

亚特兰大 Atlanta
Duluth, GA
Tel: 1-678-957-9614
Fax: 1-678-957-1455

奥斯汀 Austin, TX
Tel: 1-512-257-3370

波士顿 Boston
Westborough, MA
Tel: 1-774-760-0087
Fax: 1-774-760-0088

芝加哥 Chicago
Itasca, IL
Tel: 1-630-285-0071
Fax: 1-630-285-0075

达拉斯 Dallas
Addison, TX
Tel: 1-972-818-7423
Fax: 1-972-818-2924

底特律 Detroit
Novi, MI
Tel: 1-248-848-4000

休斯敦 Houston, TX
Tel: 1-281-894-5983

印第安纳波利斯 Indianapolis
Noblesville, IN
Tel: 1-317-773-8323
Fax: 1-317-773-5453
Tel: 1-317-536-2380

洛杉矶 Los Angeles
Mission Viejo, CA
Tel: 1-949-462-9523
Fax: 1-949-462-9608
Tel: 1-951-273-7800

罗利 Raleigh, NC
Tel: 1-919-844-7510

纽约 New York, NY
Tel: 1-631-435-6000

圣何塞 San Jose, CA
Tel: 1-408-735-9110
Tel: 1-408-436-4270

加拿大多伦多 Toronto
Tel: 1-905-695-1980
Fax: 1-905-695-2078

亚太地区

中国 - 北京
Tel: 86-10-8569-7000

中国 - 成都
Tel: 86-28-8665-5511

中国 - 重庆
Tel: 86-23-8980-9588

中国 - 东莞
Tel: 86-769-8702-9880

中国 - 广州
Tel: 86-20-8755-8029

中国 - 杭州
Tel: 86-571-8792-8115

中国 - 南京
Tel: 86-25-8473-2460

中国 - 青岛
Tel: 86-532-8502-7355

中国 - 上海
Tel: 86-21-3326-8000

中国 - 沈阳
Tel: 86-24-2334-2829

中国 - 深圳
Tel: 86-755-8864-2200

中国 - 苏州
Tel: 86-186-6233-1526

中国 - 武汉
Tel: 86-27-5980-5300

中国 - 西安
Tel: 86-29-8833-7252

中国 - 厦门
Tel: 86-592-238-8138

中国 - 香港特别行政区
Tel: 852-2943-5100

中国 - 珠海
Tel: 86-756-321-0040

台湾地区 - 高雄
Tel: 886-7-213-7830

台湾地区 - 台北
Tel: 886-2-2508-8600

台湾地区 - 新竹
Tel: 886-3-577-8366

亚太地区

澳大利亚 Australia - Sydney
Tel: 61-2-9868-6733

印度 India - Bangalore
Tel: 91-80-3090-4444

印度 India - New Delhi
Tel: 91-11-4160-8631

印度 India - Pune
Tel: 91-20-4121-0141

日本 Japan - Osaka
Tel: 81-6-6152-7160

日本 Japan - Tokyo
Tel: 81-3-6880-3770

韩国 Korea - Daegu
Tel: 82-53-744-4301

韩国 Korea - Seoul
Tel: 82-2-554-7200

马来西亚 Malaysia - Kuala Lumpur
Tel: 60-3-7651-7906

马来西亚 Malaysia - Penang
Tel: 60-4-227-8870

菲律宾 Philippines - Manila
Tel: 63-2-634-9065

新加坡 Singapore
Tel: 65-6334-8870

泰国 Thailand - Bangkok
Tel: 66-2-694-1351

越南 Vietnam - Ho Chi Minh
Tel: 84-28-5448-2100

欧洲

奥地利 Austria - Wels
Tel: 43-7242-2244-39
Fax: 43-7242-2244-393

丹麦 Denmark - Copenhagen
Tel: 45-4450-2828
Fax: 45-4485-2829

芬兰 Finland - Espoo
Tel: 358-9-4520-820

法国 France - Paris
Tel: 33-1-69-53-63-20
Fax: 33-1-69-30-90-79

德国 Germany - Garching
Tel: 49-8931-9700

德国 Germany - Haan
Tel: 49-2129-3766400

德国 Germany - Heilbronn
Tel: 49-7131-67-3636

德国 Germany - Karlsruhe
Tel: 49-721-625370

德国 Germany - Munich
Tel: 49-89-627-144-0
Fax: 49-89-627-144-44

德国 Germany - Rosenheim
Tel: 49-8031-354-560

以色列 Israel - Ra'anana
Tel: 972-9-744-7705

意大利 Italy - Milan
Tel: 39-0331-742611
Fax: 39-0331-466781

意大利 Italy - Padova
Tel: 39-049-7625286

荷兰 Netherlands - Drunen
Tel: 31-416-690399
Fax: 31-416-690340

挪威 Norway - Trondheim
Tel: 47-7289-7561

波兰 Poland - Warsaw
Tel: 48-22-3325737

罗马尼亚 Romania - Bucharest
Tel: 40-21-407-87-50

西班牙 Spain - Madrid
Tel: 34-91-708-08-90
Fax: 34-91-708-08-91

瑞典 Sweden - Gothenberg
Tel: 46-31-704-60-40

瑞典 Sweden - Stockholm
Tel: 46-8-5090-4654

英国 UK - Wokingham
Tel: 44-118-921-5800
Fax: 44-118-921-5820