ATSHA204A

ATSHA204A Microchip CryptoAuthentication™ 数据手册

特性

- 具有基于受保护硬件的密钥存储功能的加密元件
- 采用对称加密的验证设备主机和客户端操作
- 具有报文验证代码（Message Authentication Code，MAC）和哈希报文验证代码（Hash-Based Message Authentication Code，HMAC）选项的优异 SHA-256 哈希算法
- 一流的 256 位密钥长度；最多可存储 16 个密钥
- 有保证的惟一 72 位序列号
- 内部高质量随机数发生器（Random Number Generator，RNG）
- 用于存储密钥和数据的 4.5 kb EEPROM
- 用于固定信息的 512 位可一次性编程（One Time Programmable，OTP）位
- 多个 I/O 选项
  - 兼容 UART 的高速单线接口
  - 1 MHz I^2C 接口
- 2.0V 至 5.5V 电源电压范围
- 1.8V 至 5.5V 通信电压范围
- <150 nA 的休眠电流
- 安全下载和启动
  - 生态系统控制
  - 报文安全
  - 反克隆
- 8 引脚 SOIC、8 引脚 TSSOP、3 引脚 SOT23、8 焊盘 UDFN 和 3 引脚触点式封装

应用

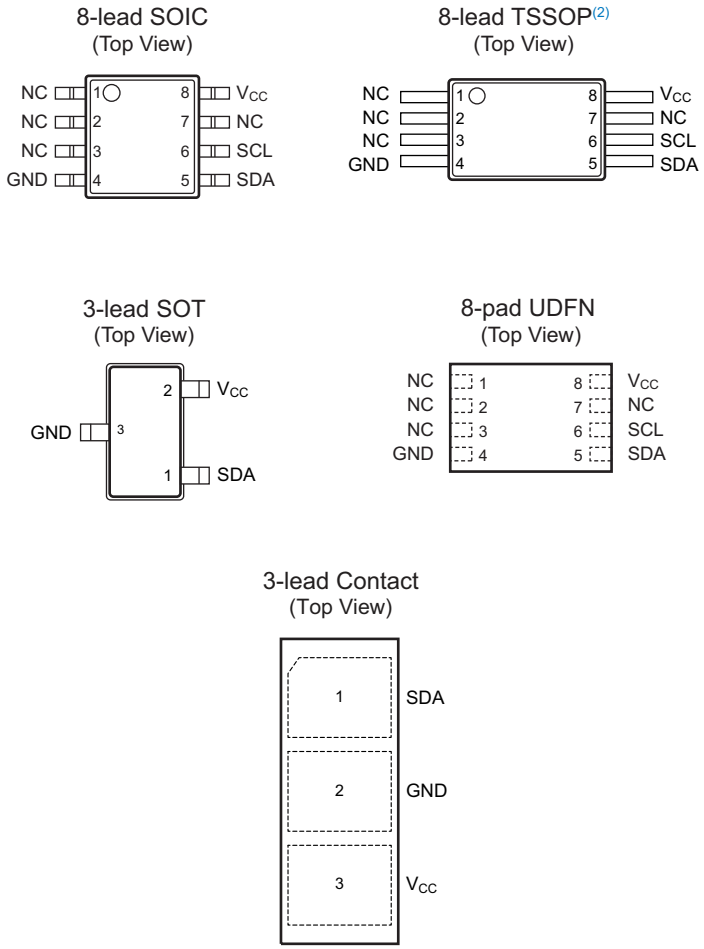
- 安全下载和启动
- 生态系统控制
- 反克隆
- 报文安全

封装类型

表 1. 引脚配置

引脚名称	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. 引脚布局(1)



注：

1. 封装图未按比例显示。
2. 不建议用于新产品设计。

目录

1. 简介

以下各章节对 Microchip ATSHA204A 加密元器件的特性和功能进行了介绍。

1.1 应用

ATSHA204A 属于 Microchip CryptoAuthentication™ 系列高安全性硬件验证器件。它具有灵活的命令集，可在许多应用中使用，其中包括：

- **防伪**

  验证可移除、可更换或可消耗的客户端是否可信。例如，客户端可以是打印机墨盒、电子子卡、一次性医疗用品或备件。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（这也被称为安全启动），对下载的媒体文件进行加密，并将代码映像单独加密为仅可在单个系统上使用。
- **交换会话密钥**

  在系统微处理器中安全、方便地交换加密/解密引擎使用的数据流加密密钥，以管理机密通信通道、已加密的下载和类似项。
- **安全地存储数据**

  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。它还可用于存储配置、校准、ePurse 值、消耗数据或其他机密所需的少量数据。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，将简单密码映射到复杂密码，并与远程系统安全地交换密码值。

1.2 器件特性

ATSHA204A 器件包括一个电可擦除的可编程只读存储器（Electrically Erasable Programmable Read-Only Memory，EEPROM）阵列，此阵列可用于密钥存储、其他读/写数据、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。有关详细信息，请参见 **EEPROM 构成**一节。

ATSHA204A 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，有关详细信息，请参见**安全功能**一章。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。有关详细信息，请参见 **I^2C 接口**一章。此接口符合 I^2C 接口规范。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。有关更多详细信息，请参见**单线接口**一章。

使用单线接口时，多个 ATSHA204A 器件可共用同一总线，从而减少处理器 GPIO 在多客户端（例如，不同颜色墨盒或多个备件）系统中的使用。有关实现方式的详细信息，请参见**共用接口**和 **Pause 命令**一节。

每个 ATSHA204A 都附带一个有保证的惟一 9 字节（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证明序列号是真实可信而非副本。序列号通常存储在标准串行 EEPROM 中，可轻松复制，主机无法了解序列号是真实可信还是复制品。必须使用完整的序列号来保证惟一性。

ATSHA204A 可以生成高质量的随机数，并将其用于任何目的，包括作为此器件的加密协议的一部分。由于每个 32 字节（256 位）随机数均独立于之前在此器件或任何其他器件上生成的数字，因此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。请参见**随机数发生器（RNG）**和 **Random 命令**章节。

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**电气特性**一章，本章还介绍了多种封装选项，其中包括尺寸仅为 2.0 mm x 3.0 mm 的小型 UDFN 封装。有关更多详细信息和订购代码，请参见**封装图**一章。

有关 Microchip ATSHA204 兼容性的信息，请参见**兼容性**一章。

1.3 加密操作

ATSHA204A 支持标准的质询-响应协议，以简化编程。在最基本的实例中，主机系统向客户端器件发送一个质询（例如一个数字），此器件通过来自系统的报文验证代码（MAC）命令将此质询与机密信息密钥组合（如 **MAC 命令**一节所述），然后将此响应发送回系统。此器件使用加密哈希算法来实现此组合（也称为摘要）。使用哈希算法可防止总线上的观察者获取机密信息密钥的值，同时允许接收者使用存储的机密信息副本执行相同的计算（即，将质询与机密信息组合以创建摘要）来验证响应是否正确。

由于 ATSHA204A 具有灵活的命令集，这种基本操作可通过多种方式扩展。通过使用 GenDig 命令（**GenDig 命令**一节），其他槽中的值可以包含在响应摘要中，这提供了一种有效的方式来证明所读取数据确实来自器件，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。

DeriveKey 命令（**DeriveKey 命令**一节）实现了密钥滚动方案。根据命令模式参数，所得到的操作可类似于诸如在远程控制的车库门开启装置中实现的操作。每次使用密钥时，密钥的当前值都会以加密方式与特定于此系统的值组合，此结果随后会构成下一个加密操作的密钥。即使攻击者获得一个密钥的值，此密钥也会在下次使用时永久消失。

DeriveKey 还可用于生成新的随机密钥，这些密钥可能仅针对特定主机 ID、特定时间段或某个其他受限条件有效。每个生成的密钥都不同于在任何器件上生成的任何其他密钥。通过以这种方式在现场“激活”主机-客户端对，单个客户端的克隆将无法作用于任何其他主机。

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（**CheckMac 命令**一节）允许主机器件安全地存储客户端的机密信息，并隐藏来自引脚的正确响应值，仅向系统返回 yes/no 回答。

需要用户输入的密码时，CheckMac 命令还提供了一种在不将密码公开在通信总线上的情况下验证密码以及将密码映射到可具有更高熵的存储值的方法。有关详细信息，请参见**密码检查**一节。

最后，质询和机密信息密钥的哈希组合（例如摘要）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读取（**Read 命令**一节），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写入（**Write 命令**一节）。

其中的每个操作均可受到防重放攻击保护，方法是将随机临时值（**Nonce 命令**一节）包含在计算中。

所有安全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。有关算法的详细信息，请参见 **SHA-256** 一节。必要时，SHA-256 算法还可包含在 HMAC 序列中（见 **HMAC 命令**一节）。ATSHA204A 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。

2. 器件构成

器件包含以下存储块：

- EEPROM
- SRAM

2.1 EEPROM 构成

EEPROM 共有 664 字节（5312 位），分为以下几个区域：

表 2-1. ATSHA204A 区域

区域	说明	命名法
数据	512 字节（4 Kb）的区域分为 16 个 32 字节（256 位）的通用只读或读/写存储器槽，每个槽可用于存储密钥、校准数据、型号或其他通常与 ATSHA204A 器件所连接的项有关的信息。每个数据槽的访问策略由编程到相应配置值中的值确定。但是，策略仅在设置 LockValue 字节时生效。	槽<YY> = 存储在数据区域的槽 YY 中的全部内容。
配置	包含序列号和其他 ID 信息以及访问数据存储器各槽权限信息的 88 字节（704 位）EEPROM 区域。编程到配置区域中的值可确定每个数据槽响应方式的访问策略。配置区域锁定（LockConfig 设置为!=0x55）之前可进行修改。为了使能访问策略，必须设置 LockValue 字节。（见上文）	SN<a:b> = 配置区域中的字段内的字节范围。
可一次性编程（OTP）	OTP 位的 64 字节（512 位）区域。在锁定 OTP 区域之前，可以使用标准 Write 命令自由写入相应位。OTP 区域可用于存储只读数据或单向熔丝型消耗记录信息。	OTP<bb> = OTP 区域内的一个字节，而 OTP<aa:bb>表示一个字节范围。

本文档中讨论的术语具有以下含义：

表 2-2. 文档术语

术语	含义
模块	特定存储区域的单个 256 位（32 字节）区域。工业 SHA-256 文档使用术语“块”来表示报文输入的 512 位片段。此外，本文档的 I/O 部分使用术语“块”来表示在系统和器件之间传输的长度可变的聚合元素。
槽	对于数据区域，术语“块”和“槽”可以互换使用。对于 OTP 和配置区域，有多个块（每个块 32 个字节）。
param<b>	表示参数或字节字段的一位。
SRAM	包含输入和输出缓冲区以及状态存储单元。请参见**静态 RAM（SRAM）**一节

从 Microchip 发货时，EEPROM 包含可用于固定值电路板测试的出厂测试数据。在锁定器件的配置和/或数据部分之前，此数据必须用所需内容覆盖。关于包含特定交付值的文档，请访问 **Microchip 网站**。

2.1.1 EEPROM 数据区域

数据区域为 512 字节（4 kb），是 EEPROM 阵列的一部分，可用于安全存储目的。

在锁定配置区域（通过使用 Lock(Config)）之前，数据区域不可访问，既不能读取也不能写入。完成配置锁定后，可使用 Write 命令对整个数据区域进行写操作。如果需要，可以加密要写入的数据。

在下表中，“字节地址”表示数据区域内用于相应槽中的第一个字节的字节地址。由于 ATSHA204A 的所有 Reads 和 Writes 操作均以字（4 字节或 32 字节）为单位执行，因此下表中的字地址应当用于传送至 Read 和 Write 命令的地址参数。

表 2-3. 数据区域槽

槽	字节地址（十六进制）	字地址（十六进制）	槽	字节地址（十六进制）	字地址（十六进制）
0	0x0000	0x0000	8	0x0100	0x0040
1	0x0020	0x0008	9	0x0120	0x0048
2	0x0040	0x0010	10	0x0140	0x0050
3	0x0060	0x0018	11	0x0160	0x0058
4	0x0080	0x0020	12	0x0180	0x0060
5	0x00A0	0x0028	13	0x01A0	0x0068
6	0x00C0	0x0030	14	0x01C0	0x0070
7	0x00E0	0x0038	15	0x01E0	0x0078

2.1.2 配置区域

配置区域中的 88 字节（704 位）包含制造标识数据、常规设备和系统配置以及数据区中槽的访问限制控制值。这些字节的值始终可使用 Read 命令获得。此区域的字节排列如下表所示。

表 2-4. 配置区域

字	字节 0	字节 1	字节 2	字节 3	默认值	写访问	读访问
0x00	SN<0:3>				01 23 xx xx	从不	始终
0x01	RevNum				xx xx xx xx	从不	始终
0x02	SN<4:7>				xx xx xx xx	从不	始终
0x03	SN<8>	保留	I2C_Enable	保留	EE 55 xx 00	从不	始终
0x04	I2C_Address	CheckMacConfig	OTP 模式	选择器模式	C8 00 55 00	Config 解锁时	始终
0x05	SlotConfig 0		SlotConfig 1		8F 80 80 A1	Config 解锁时	始终
0x06	SlotConfig 2		SlotConfig 3		82 E0 A3 60	Config 解锁时	始终
0x07	SlotConfig 4		SlotConfig 5		94 40 A0 85	Config 解锁时	始终
0x08	SlotConfig 6		SlotConfig 7		86 40 87 07	Config 解锁时	始终
0x09	SlotConfig 8		SlotConfig 9		0F 00 89 F2	Config 解锁时	始终
0x0A	SlotConfig 10		SlotConfig 11		8A 7A 0B 8B	Config 解锁时	始终
0x0B	SlotConfig 12		SlotConfig 13		0C 4C DD 4D	Config 解锁时	始终
0x0C	SlotConfig 14		SlotConfig 15		C2 42 AF 8F	Config 解锁时	始终
0x0D	UseFlag 0	UpdateCount 0	UseFlag 1	UpdateCount 1	FF 00 FF 00	Config 解锁时	始终
0x0E	UseFlag 2	UpdateCount 2	UseFlag 3	UpdateCount 3	FF 00 FF 00	Config 解锁时	始终
0x0F	UseFlag 4	UpdateCount 4	UseFlag 5	UpdateCount 5	FF 00 FF 00	Config 解锁时	始终

.....（续）

字	字节 0	字节 1	字节 2	字节 3	默认值	写访问	读访问
0x10	UseFlag 6	UpdateCount 6	UseFlag 7	UpdateCount 7	FF 00 FF 00	Config 解锁时	始终
0x11	LastKeyUse 0	LastKeyUse 1	LastKeyUse 2	LastKeyUse 3	FF FF FF FF	Config 解锁时	始终
0x12	LastKeyUse 4	LastKeyUse 5	LastKeyUse 6	LastKeyUse 7	FF FF FF FF	Config 解锁时	始终
0x13	LastKeyUse 8	LastKeyUse 9	LastKeyUse 10	LastKeyUse 11	FF FF FF FF	Config 解锁时	始终
0x14	LastKeyUse 12	LastKeyUse 13	LastKeyUse 14	LastKeyUse 15	FF FF FF FF	Config 解锁时	始终
0x15	UserExtra	选择器	LockValue[1]	LockConfig	00 00 55 55	仅通过 UpdateExtra 命令	始终

注：

1. LockValue 之前称为 LockData。

2.1.2.1 I2C_Enable

Bit 7-1： 忽略，由 Microchip 设置。

Bit 0： 0 = 单线接口模式。

1= I^2C 接口模式。

2.1.2.2 I2C_Address

I^2C 模式 I2C_Enable<0> = 1

Bit 7-1： I^2C 器件地址

Bit 3： TTL 使能（双用途位）

I^2C 地址的一部分，设置阈值。

0 = 输入电平使用固定参考。

1 = 输入电平使用 V_{CC} 作为参考。

Bit 0： 忽略。

单线模式 I2C_Enable<0> = 0

Bit 7-4： 忽略。

Bit 3： TTL 使能

0 = 输入电平使用固定参考。

1 = 输入电平使用 V_{CC} 作为参考。

Bit 2-0： 忽略。

2.1.2.3 CheckMacConfig

此字节仅适用于 CheckMac、Read 和 Write 命令：

- **Read 和 Write：**CheckMacConfig<0>控制槽 0 和 1，CheckMacConfig<1>控制槽 2 和 3，依此类推。如果 TempKey.SourceFlag 中的值与此字节中的相应位不匹配，则任何加密 Read 或 Write 命令都将失败。对于明文读取和写入，此字节被忽略。
- **CheckMac：** CheckMacConfig<0>控制槽 1，CheckMacConfig<1>控制槽 3，依此类推。只有在目标槽对应的 CheckMacSource 值与 CheckMac 命令的 Mode bit 2 的值匹配时才会使能复制功能。如果 Mode bit 2 与 TempKey.SourceFlag 不匹配，则此命令将失败，因此这相当于要求此字节中的相应位与 TempKey.SourceFlag 匹配。

2.1.2.4 OTP 模式

0xAA（只读模式）= 当 OTP 区域锁定时，禁止写操作，允许所有字的读操作。

0x55（消耗模式）= 当 OTP 区域锁定时写入 OTP 区域会导致位仅从 1 转换为 0。允许读取所有字。

0x00（传统模式）= 当 OTP 区域锁定时，禁止写操作，并会禁止字 0 和 1 的读操作以及 32 字节读操作。

所有其他模式均保留。

2.1.2.5 选择器模式

如果为 0x00，将用 UpdateExtra 更新 Selector。

如果为其他值，将只允许 Selector 在值为零时更新。

2.1.2.6 槽配置

请参见表 **SlotConfig 位（每个槽）**。

2.1.2.7 UseFlag

用于“限制使用的槽”。“1”位的数量表示在禁止前槽 0 至 7 可使用的次数。

2.1.2.8 UpdateCount

表示槽 0 至 7 已用 DeriveKey 更新的次数。

2.1.2.9 LastKeyUse

用于控制槽 15 的限制使用次数。每个“1”位表示槽 15 的一次剩余使用次数。仅适用于 SlotConfig<5> LimitedUse 置 1 的情况。

2.1.2.10 UserExtra

对于一般的系统使用，可通过 UpdateExtra 命令进行修改。

2.1.2.11 选择器

选择哪个器件将在执行 Pause 命令后保持工作模式。

2.1.2.12 LockValue

控制数据和 OTP 区域是否解锁、可自由写入但不能读取。

0x55 = 数据和 OTP 区域已解锁，且具有写访问权限。

0x00 = 数据和 OTP 区域已锁定，并采用配置区域中定义的访问策略。数据区域中的槽只能根据相应的 WriteConfig 字段进行修改。OTP 区域只能根据 OTP 模式进行修改。

2.1.2.13 LockConfig

配置区域访问。

0x55 = 配置区域具有写访问（已解锁）。

0x00 = 配置区域没有写访问（已锁定）。

2.1.2.14 SlotConfig（字节 20 至 51）

使用 16 个 SlotConfig 元素为 ATSHA204A 中的 16 个槽中的各个槽配置访问保护。每个配置元素由16 个位组成，它们控制特定槽或密钥的使用和访问。当数据区域锁定时，SlotConfig 字段根据下表进行解析。当数据区域解锁时，这些限制不适用，所有槽均可自由写入，但不能读取。

表 2-5. SlotConfig 位（每个槽）

Bit	名称	说明
15-12	WriteConfig	请参见有关用途的详细功能定义。
11-8	WriteKey	要用于验证加密写操作的密钥的槽。
7	IsSecret	**0 =** 槽并非机密信息槽，允许明文读取、明文写入，无 MAC 检查且无 Derivekey 命令 **1 =** 槽为机密信息槽。读操作和写操作（如果允许）必须进行加密。
6	EncryptRead	**0 =** 允许明文读取。 **1 =** 要求槽为机密信息槽，并以加密读取的方式进行访问。
5	LimitedUse(1)	**0 =** 密钥可使用的次数无限制。 **1 =** 根据槽的 UseFlag（或 LastKeyUse）对密钥的使用次数进行限制。
4	CheckOnly	**0 =** 此槽可用于所有加密命令。 **1 =** 此槽只能用于 CheckMac 以及后跟 CheckMac 的 GenDig 命令。
3-0	ReadKey	要用于加密读取的密钥的槽。 如果为 0x0，则此槽可用作 CheckMac/Copy 命令的源槽。

注：

1. LimitedUse 位之前称为 SingleUse。

表 2-6. 写配置位——Derivekey 命令

Bit 15	Bit 14	Bit 13	Bit 12	源密钥(1)	说明
0	X	1	0	目标	DeriveKey 命令可在未授权 MAC 的情况下运行（滚动）。
1	X	1	0	目标	DeriveKey 命令需要授权 MAC（滚动）。
0	X	1	1	父项	DeriveKey 命令可在未授权 MAC 的情况下运行（创建）。
1	X	1	1	父项	DeriveKey 命令需要授权 MAC（创建）。
X	X	0	X	—	在 WriteConfig 字段中具有此值的槽不可用作 DeriveKey 命令的目标。

注：

1. DeriveKey 命令所执行计算的源密钥可以是在 Param2（“目标”）中直接指定的密钥或者是在 slotConfig<Param2>.WriteKey（“父项”）中的密钥。有关更多详细信息，请参见**密钥值**一节。

表 2-7. 写配置位——Write 命令

Bit 15	Bit 14	Bit 13	模式名称	说明
0	0	0	始终	始终允许对此槽进行明文写入。设置为“始终”的槽始终不应用来存储密钥。可以向此槽写入 4 个或 32 个字节。
X	0	1	从不	始终不允许使用 Write 命令写入此槽。设置为“从不”的槽仍可用来存储密钥。
1	0	X	从不	始终不允许使用 Write 命令写入此槽。设置为“从不”的槽仍可用来存储密钥。
X	1	X	加密	写入此槽的内容需要一个正确计算的 MAC，并且输入数据必须由系统通过 WriteKey 使用 Write 命令说明（8.5.18 Write 命令）中记录的加密算法进行加密。禁止对此槽进行 4 字节写入。

4 位 WriteConfig 字段由表写配置位—Write 命令所示的 Write 命令解析，其中“X”表示无关。

这些表有重叠。例如，代码 0b0110 表示可以用 Write 命令以加密形式写入的槽，也可以是将目标作为来源的未授权 DeriveKey 命令的目标。

对于读取和/或写入必须加密或完全禁止的槽而言，IsSecret 位控制这些槽正确实现安全性所必需的内部电路。它还必须针对所有要用作密钥的槽置 1，包括通过 DeriveKey 创建或修改的槽。具体来说，为了使器件能够正常工作，除非 WriteConfig 为“始终”，否则此位必须置 1。对于此位置 1 的槽而言，禁止对其进行四字节访问。

用于存储密钥值的槽应始终将 IsSecret 设置为 1，并将 EncryptRead 设置为 0（禁止读取）以获得最大的安全性。对于固定密钥值，WriteConfig 应设置为“从不”。如果以这种方式配置，则在数据区域锁定之后无法读取或写入密钥，只能用于加密操作。

一些安全策略要求机密信息不时更新。ATSHA204A 通过以下方式支持此功能：

- 特定槽的 WriteConfig 应设置为“加密”，SlotConfig.WriteKey 应通过将 WriteKey 设置为槽 ID来指回相同槽。之后，可使用标准 Write 命令向此槽写入一个新值，前提是使用旧的（即当前）密钥值来计算验证 MAC。

2.1.2.15 配置区域中的特殊存储器值（字节 0 至 12）

ATSHA204A 中包含了各种固定信息，无论锁定位的状态如何，在任何情况下都不能写入，但始终可以读取。

- **SerialNum**
  9 个字节（SN<0:8>），一起形成 CryptoAuthentication 系列中任何器件都不会重复的惟一值。序列号分为两组：
  1. **SN<0:1>和 SN<8>**
     在 ATSHA204A 的大多数版本中，这些位的值是在制造时固定的。其默认值为（0x01 0x23 0xEE）。这 24 位始终包含在 ATSHA204A 所执行的 SHA-256 计算中。
  2. **SN<2:7>**
     这些位的值由 Microchip 在制造过程中编程，对于每个芯片均有所不同。这 6 个字节（48 位）可视情况包含在 ATSHA204A 所执行的一些 SHA-256 计算中
- **RevNum**
  Microchip 用来提供制造版本信息的 4 字节信息。这些字节可以自由读取为 RevNum<0:3>，但始终不应被系统软件使用，因为它们可能会因芯片版本发生变化。

2.1.3 可一次性编程（OTP）区域

64 字节（512 位）的 OTP 区域是 EEPROM 阵列的一部分，可用于只读存储。

在锁定配置区域（通过使用 Lock(LockConfig)）之前，OTP 区域不可访问，既不能读取也不能写入。在配置锁定之后，但在锁定 OTP 区域（使用 Lock(LockValue)）之前，可以使用 Write 命令写入整个 OTP 区域。如果需要，可以加密要写入的数据。解锁后，不能读取 OTP 区域。

OTP 区域锁定后，配置区域中的 OTP 模式字节将控制此区域的访问权限，具体如下：

- **只读模式**

数据无法修改，将用于存储固定型号、校准信息、制造历史和/或其他始终不应改变的数据。 Write 命令将始终返回错误，使存储器保持未修改状态。OTP 区域中的全部 64 字节始终可通过 4 字节或 32 字节读取方式进行读取。

- **消耗模式**

这些位用作单向熔丝，可用于跟踪 ATSHA204A 所连接项的消耗或使用情况。例如，在电池中，它们可能被用来跟踪充电周期或使用时间；在打印机墨盒中，它们可能会跟踪所消耗的油墨量；在医疗设备中，它们可能会跟踪限制使用项目的允许使用次数。在此模式下，Write 命令只能使相应位从 1 变为 0。在逻辑上，这意味着输入参数列表中的数据值将与字中的当前值进行“与”运算，并将结果写回存储器。例如，写入值 0xFF 将导致字节不发生任何变化，写入值 0x00 将导致存储器中的字节变为 0，而不管先前的值为何。一旦某个位转换为 0，便始终无法再转换为 1。

- **传统模式**

OTP 区域的操作与 Microchip ATSA102S 上的熔丝阵列一致。字 0 和 1 始终禁止读取，而其余 14 个字始终允许读取。只允许 4 字节（32 位）读取操作，任何尝试执行 32 字节（256 位）读取的操作都将返回错误代码。禁止对 OTP 区域的所有写操作。有关 Microchip ATSA102S 兼容性的更多详细信息，请参见 9. 兼容性一章。

从 Microchip 工厂发货时，所有 OTP 区域位的值均为 1。

表 2-8. OTP 区域

字（十六进制）	地址（十六进制）	默认值
0x00	0x00	0xFFFFFFFF
0x01	0x04	0xFFFFFFFF
0x02	0x08	0xFFFFFFFF
0x03	0x0C	0xFFFFFFFF
0x04	0x10	0xFFFFFFFF
0x05	0x14	0xFFFFFFFF
0x06	0x18	0xFFFFFFFF
0x07	0x1C	0xFFFFFFFF
0x08	0x20	0xFFFFFFFF
0x09	0x24	0xFFFFFFFF
0x0A	0x28	0xFFFFFFFF
0x0B	0x2C	0xFFFFFFFF
0x0C	0x30	0xFFFFFFFF
0x0D	0x34	0xFFFFFFFF
0x0E	0x38	0xFFFFFFFF
0x0F	0x3C	0xFFFFFFFF

2.1.4 器件锁定

此器件有两个独立的锁定字节：

- 一个用于锁定配置区域（由字节 87 LockConfig 控制）。
- 一个用于锁定数据区域和 OTP 区域（由字节 86 LockValue 控制）。这样可根据槽配置为数据区域中相应的槽使能访问策略。

这些锁定存储在配置区域中的单独字节内，只能通过 Lock 命令进行修改。存储器区域锁定后，便无法解锁。锁定数据/OTP 区域并不意味着无法修改槽。可以根据槽配置定义的访问策略修改槽。

器件应在系统制造商处通过所需配置信息完成个性化设置，之后，应锁定配置区域。完成此锁定后，在适当情况下，对 EEPROM 槽执行的所有必要公共和机密信息写入操作均应采用加密写入操作的形式。完成对数据区域和 OTP 区域的写入后，数据区域和 OTP 区域应写入 LockValue 字节。

在将包含器件的系统发布到现场之前，必须将 LockValue 字节设置为锁定，以便保护存储在数据区域和 OTP 区域中的数据。未能锁定这些区域可能会允许修改任何密钥，并且可能导致其他安全问题。

在锁定配置区域之前，任何尝试读取或写入数据区域或 OTP 区域的操作都将使器件返回错误。

请与 Microchip 联系以获取可选的安全个性化服务。

2.1.4.1 配置区域锁定

无论 LockConfig 的状态如何，配置区域内的某些字节都不能进行修改。使用配置区域中的 LockConfig 字节来控制区域内其余字节的访问，如下表所示。在本文档中，如果 LockConfig 为 0x55，则认为配置区域处于解锁状态；否则，处于锁定状态。

表 2-9. 配置区域锁定

锁定状态	读访问	写访问
LockConfig == 0x55（解锁）	读	写
LockConfig != 0x55（锁定）	读	<从不>

2.1.4.2 数据和 OTP 区域锁定

在本文档中，如果 LockValue 为 0x55，则认为数据区域和 OTP 区域处于解锁状态；否则，处于锁定状态。

在锁定配置区域之前，不会对数据区域和 OTP 区域进行读写访问。

表 2-10. 数据区域和 OTP 区域的访问限制

锁定状态	读访问	写访问
LockValue == 0x55（解锁）	<从不>	写
LockValue != 0x55（锁定）	读(1)	写(1)

注：

1. 基于给定槽的槽配置。

2.1.4.3 OTP 区域锁定

OTP 区域的读写操作取决于配置区域中 LockConfig、LockValue 和 OTP 模式字节的状态。

2.2 静态 RAM（SRAM）

此器件包括用于存储输入命令或输出结果、中间计算值和/或临时密钥的 SRAM 阵列。每当器件进入休眠模式或断电时，此寄存器的全部内容便始终无效。临时密钥名为 TempKey，可用作 MAC、HMAC、

CheckMac、GenDig 和 DeriveKey 命令的输入，也可用作 Read 和 Write 命令的数据保护（加密或解密）密钥。请参见 **TempKey** 一节。

2.2.1 TempKey

TempKey 是 SRAM 阵列中的一个存储寄存器，可用于通过 Nonce、GenDig、CheckMac 或 SHA 命令存储临时结果值。此寄存器的内容始终不能从器件读取（尽管器件本身可以在内部读取和使用内容）。

此寄存器包含下表所示的元素：

表 2-11. TempKey 存储寄存器

名称	位长度	说明
TempKey	256（32 字节）	临时值（来自 Nonce 命令）或摘要（来自 GenDig 命令）。
SlotID	4	如果 TempKey 由 GenDig 生成（见 GenData 和 CheckFlag 位），则这些位指示在其计算中使用哪个密钥。这 4 位表示数据区域的其中一个槽。
SourceFlag	1	TempKey 中随机性的来源： **0 =** 内部生成的随机数（Rand）。 **1 =** 仅输入种子，未生成内部随机数（Input）。
GenData	1	**0 =** TempKey.SlotID 无意义，被忽略。 **1 =** TempKey 的内容是由 GenDig 使用数据区中的一个槽生成的（TempKey.SlotID 是有意义的）。
CheckFlag	1	**0 =** TempKey 内容是使用 Nonce、SHA 或 GenDig 生成的，没有 CheckMac 密钥限制。 **1 =** TempKey 的内容是由 GenDig 命令生成的，并且此生成过程中使用的密钥至少有一个被限制为 CheckMac 命令（SlotConfig.CheckOnly 为 1）。
有效	1	**0 =** TempKey 中的信息无效。 **1 =** TempKey 中的信息有效。

在本规范中，名称“TempKey”是指 32 字节（256 位）数据寄存器的内容。其余的位字段称为 TempKey.SourceFlag、TempKey.GenData 等。

在以下任一情况下，TempKey.Valid 位均将清零：

- 上电、休眠、掉电、看门狗过期或篡改检测。不过，当器件进入空闲模式时，TempKey 的内容将保留不变。
- 在执行除 Nonce 或 GenDig 之外的任何命令后，而无论命令是否成功执行。除非成功复制，否则可能由 CheckMac 命令清零。如果存在通信问题（通过循环冗余校验（Cyclic Redundancy Check，CRC）错误证明），则不会清零。
- 解析或执行 GenDig 和/或 Nonce 命令时出错。
- 执行 GenDig 会将之前的 Nonce 命令输出替换为 GenDig 命令的输出。同样，执行 Nonce 命令会替换之前的 GenDig 命令输出。

3. 安全特性

3.1 物理安全

ATSHA204A 集成了许多物理安全功能，旨在保护 EEPROM 的内容免于未经授权的暴露。安全措施包括：

- 部件主动屏蔽保护
- 内部存储器加密
- 安全测试模式
- 毛刺保护
- 电压篡改检测
- 温度篡改检测

存储在 ATSHA204A 上的预编程传输密钥的加密方式可确保使用外部分析来获取其值非常困难。

逻辑时钟和逻辑电源电压均在内部产生，从而防止使用器件引脚对这两个信号进行直接攻击。

3.2 随机数发生器（RNG）

ATSHA204A 包含一个高质量的 RNG，它将 32 字节随机数返回到系统。此器件将生成的这一数字与单独的输入数字组合起来，构成一个存储在器件的 TempKey 中的临时值，以供后续命令使用。

系统可以将此 RNG 用于任何用途。其中一个常见的用途是，作为单独 CryptoAuthentication 器件中 MAC 命令的输入质询。为此，器件提供了一个特殊的 Random 命令，不会影响内部存储的临时值。

为简化系统测试，在配置区域锁定前，RNG 始终返回以下 32 字节值：

0xFF FF 00 00 FF FF 00 00 ···

其中 0xFF 是从器件中读取的第一个字节，用于 SHA 报文。

为了防止与 ATSHA204A 之间传送的加密数据遭受重放攻击，器件要求包含新的内部生成的临时值，将其作为用于保护正在读取或写入的数据的加密序列的一部分。为实现此要求，在创建临时值时，由 GenDig 生成且供 Read 或 Write 命令使用的数据保护密钥必须使用内部 RNG。

随机数由硬件 RNG 的输出和内部种子值的组合生成，内部种子值无法从外部访问。内部种子存储在 EEPROM 中，通常在每次上电或休眠/唤醒周期后更新一次。更新后，如果器件进入休眠模式或断电，则此种子值将保留在器件的已失效的 SRAM 寄存器中。

4. 通用 I/O 信息

与 ATSHA204A 的通信通过两种不同协议（I²C 或单线）之一来实现，具体根据订购的器件进行选择：

- **单线接口**
  在连接到器件 SDA 引脚的系统微处理器上使用单个 GPIO 连接。此方法可将最少数量的连接器引脚连接到任何可移动或可替换的实体上。比特率最高 25.6 kbps，与标准 UART 信令兼容。
- **I²C 接口**
  此模式与 Microchip AT24C16 串行 EEPROM 接口兼容。需要串行数据（SDA）和串行时钟（SCL）这两个引脚。I²C 接口支持最高 1 Mbps 的比特率。

单线接口和 I²C 接口章节介绍了最低级别的 I/O 协议。在 I/O 协议级别之上，两个接口将完全相同的字节传入和传出器件以实现加密命令和错误代码，如安全命令一章所述。

此器件实现了一个故障保护内部看门狗定时器，无论当前活动如何，此定时器都会在一定的时间间隔后强制器件进入极低功耗模式。系统编程必须考虑到这一点。有关详细信息，请参见看门狗故障保护一节。

4.1 字节和位顺序

CryptoAuthentication 器件针对字节以及本文档中数字和阵列的表示方式使用了一种通用的排序方案：

- 所有多字节聚合元素都视为字节阵列，并按索引 #0 在前的接收或发送顺序进行处理。
- 2 字节（16 位）整数（通常为 Param2）首先出现在总线的 LSB 上。

位顺序有所不同，具体取决于使用的 I/O 通道：

- 在单线接口上，数据首先在总线上传入/传出 ATSHA204A 的 LSb。
- 在 I²C 接口上，数据首先在总线上传入/传出 ATSHA204A 的 MSb。

4.1.1 输出示例

以下字节将按照此顺序在总线上通过对配置区域（输入地址为 0x0000）进行 32 字节读操作来返回：
SN<0>、SN<1>、SN<2>、SN<3>、RevNum<0>、RevNum<1>、RevNum<2>、RevNum<3>、SN<4>、SN<5>、SN<6>、SN<7>、SN<8>、reserved、I2C_Enable、reserved、I2C_Address、OTPmode、SelectorMode、SlotConfig<0>.Read、SlotConfig<0>.Write、SlotConfig<1>.Read、SlotConfig<1>.Write、SlotConfig<2>.Read、SlotConfig<2>.Write、SlotConfig<3>.Read、SlotConfig<3>.Write、SlotConfig<4>.Read、SlotConfig<4>.Write、SlotConfig<5>.Read、SlotConfig<5>.Write

4.1.2 MAC 报文示例

以下字节将使用 0x71 模式值和槽 x 的 SlotID 传送至用于 MAC 命令的 SHA 引擎。在下面的示例中，K<x>表示数据区域中槽 x 的 SlotID，K<0>是在总线上对此槽读写的第一个字节。OTP<0>表示在总线上从 OTP 区域（地址 0）读取的第一个字节，依此类推。
K<0>、K<1>、K<2>、K<3> … K<31>、TempKey<0>、TempKey<1>、TempKey<2>、TempKey<3> … TempKey<31>、Opcode（=0x08）、Mode（=0x71）、Param2（LSB = 0xYY）、Param2（MSB = 0x00）、OTP<0>、OTP<1>、OTP<2>、OTP<3>、OTP<4>、OTP<5>、OTP<6>、OTP<7>、OTP<8>、OTP<9>、OTP<10>、SN<8>、SN<4>、SN<5>、SN<6>、SN<7>、SN<0>、SN<1>、SN<2>、SN<3>。
有关 MAC 报文的更多详细信息，请参见 MAC 命令一节。

5. 单线接口

在单线接口模式下，与 ATSHA204A 之间的通信通过 SDA 引脚（一条异步定时线路）进行，SCL 引脚被忽略。

仅当 SCL 引脚保持低电平或未连接时，才能保证休眠电流规范值。

整个通信结构采用层级形式：下表所示为用于单线接口和标准 RS-232 端口的令牌。主机 UART 端口应设置为 7 位数据字和 230.4 kBaud 数据速率。

表 5-1. 唤醒和 I/O 令牌

令牌类型	令牌值	启动(1)	唤醒令牌 LSb: MSb							停止(1)
			b0	b1	b2	b3	b4	b5	b6	
唤醒(2)	0x00	0	0	0	0	0	0	0	0	1
逻辑 0 (3)	0x7D	0	1	0	1	1	1	1	1	1
逻辑 1 (3)	0X7F	0	1	1	1	1	1	1	1	1

注：

1. 所有令牌必须以低电平启动脉冲开头以同步数据捕捉，并以高电平停止值结束。
2. 唤醒令牌创建一个足以唤醒器件的低电平脉冲。
3. 逻辑 0 和逻辑 1 I/O 令牌表示单个数据位。创建单个字节的数据需要 8 个 I/O 令牌。

I/O 标志——标志由 8 个令牌（位）组成，这些令牌（位）可以传送下一组位（如果存在）的方向和含义。标志始终先发送 LSb。

块——在命令和传输标志后的数据块。它们包含一个字节计数和一个校验和，以确保正确的数据传输。

数据包——形成块核心的字节数据包（减去字节数和 CRC）。它们是 CryptoAuthentication 命令的输入或输出参数或来自 ATSHA204A 的状态信息。

5.1 I/O 令牌

有许多 I/O 令牌可通过单线接口传输：

- **输入**（至 ATSHA204A）
  - Wake：将器件从休眠或空闲状态唤醒。
  - Zero：从系统向器件发送一个值为 0 的位。
  - One：从系统向器件发送一个值为 1 的位。
- **输出**（自 ATSHA204A）
  - ZeroOut：从器件向系统发送一个值为 0 的位。
  - OneOut：从器件向系统发送一个值为 1 的位。

任一方向上的波形都是相同的。不过基于以下预期，时序将有一些不同：主机具有非常精确且一致的时钟，但由于正常制造和环境波动的影响，ATSHA204A 的内部时钟发生器在不同器件间存在明显不同。

位时序的设计允许标准 UART 以 230.4kBaud 的速度高效发送和接收令牌。UART 发送或接收的每个字节对应于器件接收或发送的单个位。UART 需要配置为 7 位数据，`0x7F` 对应于逻辑 `1`，`0x7D` 对应于逻辑 `0`。

Wake 令牌是特殊的，因为它需要 SDA 引脚上的 t_{WLO} 超长低电平脉冲（见表交流参数——所有 I/O 接口），此脉冲不能与数据令牌（即 Zero、One、ZeroOut 或 OneOut）期间出现的较短低电平脉冲混淆。处于空闲或休眠状态的器件将忽略所有数据令牌，直到收到合法的 Wake 令牌为止。不要将 Wake 令牌发送至唤醒的器件，否则它们将失去同步，因为波形可被解析为既非合法 1 也非合法 0 的值。有关重新获得同步的程序，请参见同步程序一节。

5.2 I/O 标志

系统始终是总线主器件；因此在任何 I/O 事务之前，系统必须向器件发送 1 个 8 位标志来指示随后将执行的 I/O 操作，如下表所示。

表 5-2. I/O 标志

名称	值	含义
休眠（低功耗）	0xCC	ATSHA204A 进入低功耗休眠模式，忽略所有后续的 I/O 转换，直到下一个唤醒标志。器件的整个易失性状态将复位。
空闲	0xBB	ATSHA204A 进入空闲状态，忽略所有后续的 I/O 转换，直到下一个唤醒标志。TempKey 和 RNG Seed 寄存器的内容将保留。
命令	0x77	将后续字节写入输入命令缓冲区中的连续地址。
保留	所有其他值	这些标志不应发送到器件。
发送	0x88	通知器件等待一段总线周转时间，然后开始将其响应发送到先前传输的命令块。当有效数据位于输出缓冲区中时，可以重复将传输标志发送给器件，以将缓冲区中的内容重新发送到系统。
唤醒	请参见“接口”	将器件从低功耗模式唤醒，并复位看门狗计数器。

5.2.1 传输标志

传输标志用于总线周转，以便 ATSHA204A 可以将数据发送回系统。器件返回系统的字节取决于器件的当前状态，可能包括状态、错误代码或命令结果。

当器件忙于执行命令时，它会忽略 SDA 引脚和系统发送的所有标志。有关每个命令类型在器件中的执行延时，请参见命令操作码、简要说明和执行时间一节。在发送命令之后，系统必须遵循这些延时，然后再尝试与器件进行通信。

5.3 同步

由于通信协议是半双工的，因此系统和 ATSHA204A 彼此间可能会失去同步。为了加快恢复速度，器件会在某些情况下实施超时，强制其进入休眠状态。

5.3.1 I/O 超时

在接收到任何数据令牌的先导转换后，ATSHA204A 将期望器件在 $t_{TIMEOUT}$ 间隔内正确接收到令牌的其余位。未能发送足够的位，或传输非法令牌（超过 t_{ZLO} 的低电平脉冲）将导致器件在 $t_{TIMEOUT}$ 间隔后进入休眠状态。

在传输命令块期间，同样的超时适用。传输合法命令标志后，I/O 超时电路将使能，直到收到最后一个预期的数据位。

注： 超时计数器在每个合法令牌之后复位，传输命令的总时间可能会超过 $t_{TIMEOUT}$ 间隔，而两个位的时间间隔可能不会。

当器件忙于执行命令时，I/O 超时电路将禁止。

5.3.2 同步程序

如果系统发送传输标志时器件不忙，则器件应在 $t_{TURNAROUND}$ 内响应。如果还未超过 t_{EXEC} 时间，器件可能很忙，系统应轮询或等待最大 t_{EXEC} 时间结束。如果器件在 $t_{TURNAROUND}$ 内仍未响应第二个传输标志，则它可能失去同步。此时，系统可以采取以下步骤来重新建立通信：

1. 等待 $t_{TIMEOUT}$。
2. 发送传输标志。
3. 如果器件在 $t_{TURNAROUND}$ 内响应，则系统可继续执行更多命令。
4. 发送 Wake 令牌。
5. 等待 t_{WHI}。
6. 发送传输标志。
7. 器件应在 $t_{TURNAROUND}$ 内以 0x11 状态响应，在此期间，系统可继续执行命令。

当系统和器件失去同步时，I/O 缓冲区中的任何命令结果都可能丢失。

5.4 共用接口

多个 CryptoAuthentication 器件可共用同一接口，如下所示：

1. 系统发出 Wake 令牌（**看门狗故障保护**一节）唤醒所有器件。
2. 系统发出 Pause 命令将除其中一个器件之外的所有器件都置于空闲模式。剩余的惟一器件随后将获知系统发送的任何命令。当系统完成与一个活动器件的通信时，它将发送一个空闲标志（空闲器件将忽略），但会将其余的活动器件置于空闲模式。有关更多详细信息，请参见 **Pause 命令**一节。

对于线路上的每个器件，重复步骤 1 和步骤 2。如果系统已完成与最终器件的通信，则应唤醒所有器件，然后使所有器件进入休眠状态以降低总功耗。

器件使用配置区域内的 Selector 字节来确定哪个器件保持唤醒状态。只有 Selector 值与 Pause 命令的输入参数匹配的器件将保持唤醒状态。为便于后期配置使用多器件共用模式的系统，支持 Selector 字节的下列三种更新功能：

1. **无限制更新**

可随时执行 UpdateExtra 命令来向配置区域的 Selector 字段写入值。要使能此模式，请将配置区域中的 SelectorMode 字节设为零。

2. **一次性现场更新**

如果将 SelectorMode 字节设为非零值，并且在锁定配置区域之前将 Selector 字节设为零值，则在配置区域锁定后的任意时间，均可一次性使用 UpdateExtra 命令将 Selector 设为非零值。UpdateExtra 命令不受 LockValue 字节的影响。

3. **固定 Selector 值**

如果 SelectorMode 和 Selector 均设为非零值，则在配置区域锁定后，始终不可修改 Selector 字节。UpdateExtra 命令将始终返回错误代码。

5.5 事务示例

唤醒（单线）		
主机		器件
唤醒	→	
发送	→	

.....（续）		
唤醒（单线）		
	←	数据

示例（单线）		
主机		器件
唤醒	→	
发送	→	
	←	数据
命令	→	
数据	→	
发送	→	
	←	数据
空闲/休眠	→	

表 5-3. 示例（单线）

	Wake 令牌 0x00								发送 0x88								计数 0x04								状态 0x11							
主机									0	0	0	1	0	0	0	1																
设备																	0	0	1	0	0	0	0	0	1	0	0	0	1	0	0	0
	CRC-16 0x33								CRC-16 0x43								命令 0x77								计数							
主机																	1	1	1	0	1	1	1	0								
设备	1	1	0	0	1	1	0	0	1	1	0	0	0	0	1	0																
	操作码								Param1								Param2								Param2							
主机																																
设备																																
	数据（0 – N）								发送 0x88								计数								数据（1 – N）							
主机									0	0	0	1	0	0	0	1																
设备																	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	CRC-16								CRC-16								空闲															
主机																	1	1	0	1	1	1	0	1								
设备	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X																

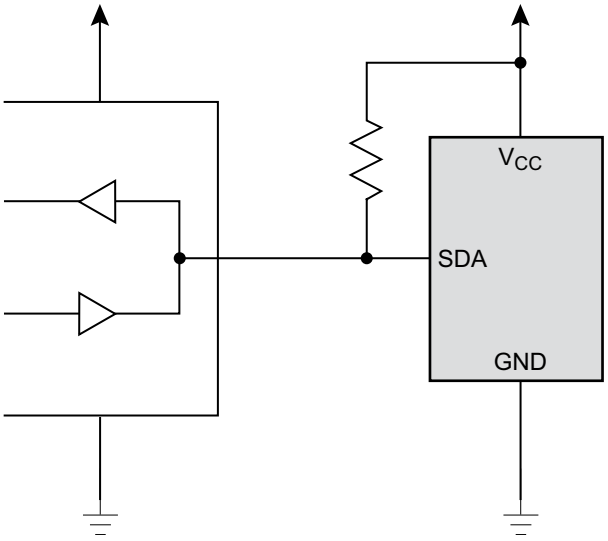
5.6 单线接口的接线配置

单线接口可以通过单个 SDA 引脚将 ATSHA204A 连接到主机，以双向传输数据。此接口不使用 SCL 引脚。如果回送到电源的电源和接地信号的阻抗较低，则 ATSHA204A 在此配置中接线时不需要旁路电容。Microchip 建议始终使用旁路电容以获得最佳可靠性。

为了防止正向偏置内部二极管以及在系统的电源层之间消耗电流，SDA 引脚上的上拉电阻应连接到与 V_{CC} 引脚或低电压轨相连的同一电源。

如果 SDA 的信号电平与 V_{CC} 电压不同，请参见本文档的参数规范部分，以确保信号电平使休眠模式下的过量泄漏电流降至最低。如果 ATSHA204A 器件在物理上远离总线主器件，或者总线主器件的电源电压与 ATSHA204A 的电源电压不同，则可能出现这种情况。

图 5-1. 单线接口的 3 线配置



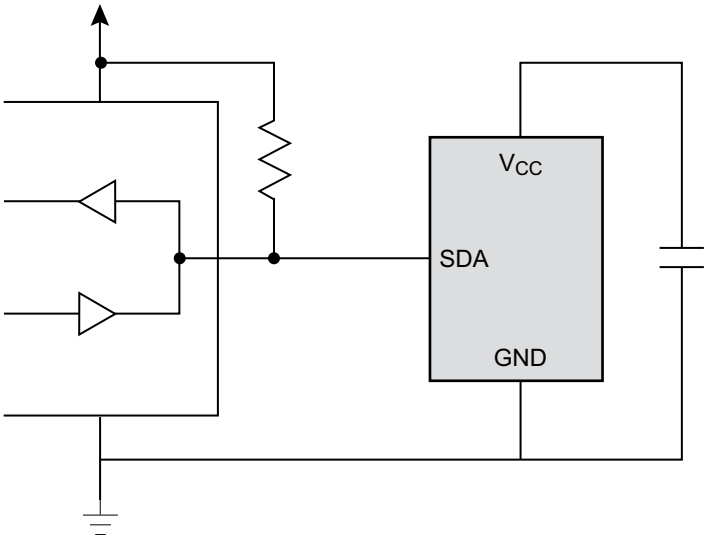
5.6.1 2 引脚配置

器件内部有一个门控开关，其连接在 SDA 和 V_{CC} 引脚之间，可允许 ATSHA204A 从 SDA 引脚获取电能并将其存储在旁路电容中。在这种情况下，V_{CC} 引脚无需连接至主机的电源。此配置允许包含 ATSHA204A 和旁路电容的电路板仅使用两个引脚（即 SDA 和 GND）即可连接至主机的微处理器。

如果系统电源电压至少为 3V，则上拉电阻应不大于 1K，电容应不小于 0.03 μF。此器件将正常运行，使 V_{CC} 保持在等于或高于 2V 的规范级别。有关更多配置信息，请联系 Microchip。

在 2 引脚配置中，必须使用一个能够在任一命令执行的整个过程中提供 I_{CC} 的有效驱动器，将 SDA 引脚驱动为高电平 V_{CC}，并应使用一个图腾柱型驱动器向器件发送数据。在将数据从 ATSHA204A 发送到系统时，SDA 线应仅依赖于上拉电阻。

图 5-2. 单线接口的 2 引脚配置



6. I²C 接口

I²C 接口使用 SDA 和 SCL 引脚来指示 ATSHA204A 的各种 I/O 状态。此接口设计为在协议级别与工作在高达 1 MHz 下的其他 I²C 器件兼容。

由于 ATSHA204A 的输出引脚上仅包含一个开漏驱动器，因此 SDA 引脚必须使用外部上拉电阻拉高。总线主器件可能是开漏型或图腾柱型，在后一种情况下，当 ATSHA204A 在总线上驱动结果时应该是三态的。SCL 引脚为输入，必须始终由外部器件或上拉电阻驱动为高电平和低电平。

6.1 I/O 条件

ATSHA204A 器件响应以下**器件休眠**和**器件唤醒**章节中所述的 I/O 条件。

6.1.1 器件休眠

当器件休眠时，它将忽略除唤醒状态以外的所有状态。

- **唤醒**：如果 SDA 保持低电平的时间超过 t_{WLO}，此器件将退出低功耗模式，并且在 t_{WHI} 的延时后，它将准备好接收 I²C 命令。当器件空闲或休眠时，在 t_{WLO} 期间，器件将忽略 SCL 引脚上的任何电平或转换。在 t_{WHI} 期间的某个时刻，将使能 SCL 引脚，并且将遵循**器件唤醒**一节中列出的条件。

唤醒条件要求系统处理器手动将 SDA 引脚驱动为低电平并持续 t_{WLO}，或者以足够低的时钟速率传输 0x00 数据字节以使 SDA 的低电平时间持续最短周期 t_{WLO}。当器件唤醒时，正常的处理器 I²C 硬件和/或软件可用于器件通信，直至包括所需的 I/O 序列，从而使器件回到低功耗（例如休眠）模式。

当总线上有多个 ATSHA204A 器件时，I²C 接口运行在 133 KHz 或更低频率下，传输某些数据类型（例如 0x00）将导致总线上的所有 ATSHA204A 器件唤醒。由于沿总线传输的后续器件地址将只匹配所需的器件，因此未使用的器件将保持无效，不会引起任何总线冲突。

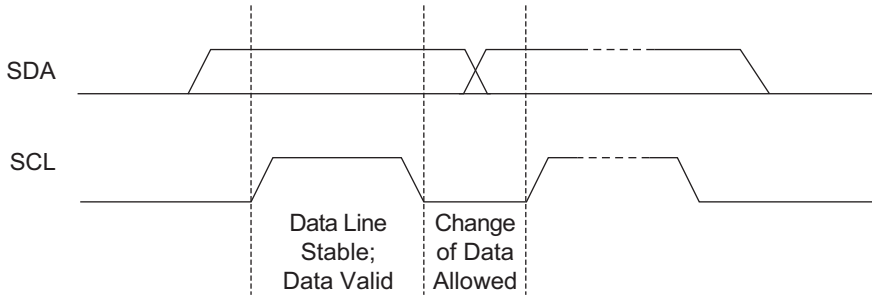
在 I²C 模式下，器件将忽略器件已经唤醒时发送的唤醒序列。

6.1.2 器件唤醒

当器件唤醒时，它将遵循下列条件：

- **数据 0**：如果 SDA 为低电平且保持稳定，而 SCL 由低电平变为高电平再变为低电平，则将在总线上传输一个 0 位。当 SCL 为低电平时，SDA 可发生变化。
- **数据 1**：如果 SDA 为高电平且保持稳定，而 SCL 由低电平变为高电平再变为低电平，则将在总线上传输一个 1 位。当 SCL 为低电平时，SDA 可发生变化。

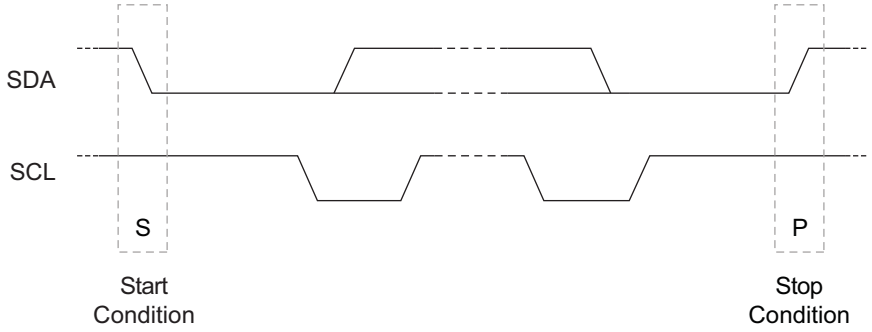
图 6-1. I²C 接口上的数据位传输



- **启动条件**：必须将 SDA 从高电平转换为低电平且 SCL 为高电平作为优先于所有命令的启动条件。
- **停止条件**：SDA 线从低电平转换为高电平且 SCL 为高电平为停止条件。器件收到此条件后，当前的 I/O 事务结束。在输入端，如果器件有足够的字节来执行命令，则器件转换到繁忙状态并开始执行。

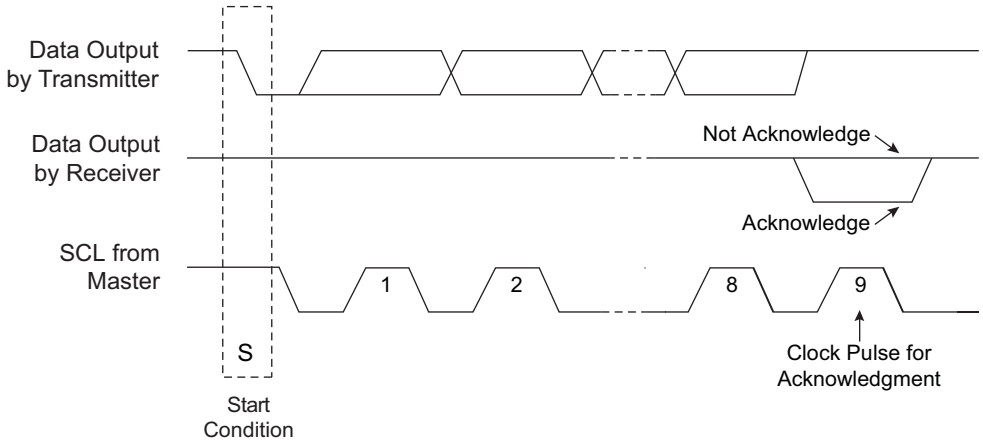
Microchip 建议在将任一数据包发送到器件后发送停止条件，尽管可能并非始终需要这样做。当接收到正确的字节数时，器件将启动。如果总线出错，器件将基于看门狗定时器复位。

图 6-2. I²C 接口上的启动和停止条件



- **应答（ACK）**：在每个地址或数据字节传输后的第 9 个时钟周期，接收器将拉低 SDA 引脚以确认正确接收字节。
- **无应答（NACK）**：在每个地址或数据字节传输后的第 9 个时钟周期，接收器也可使 SDA 引脚保持高电平，以指示接收字节时出现问题，或者此字节完成块传输。

图 6-3. I²C 接口上的 NACK 和 ACK 条件



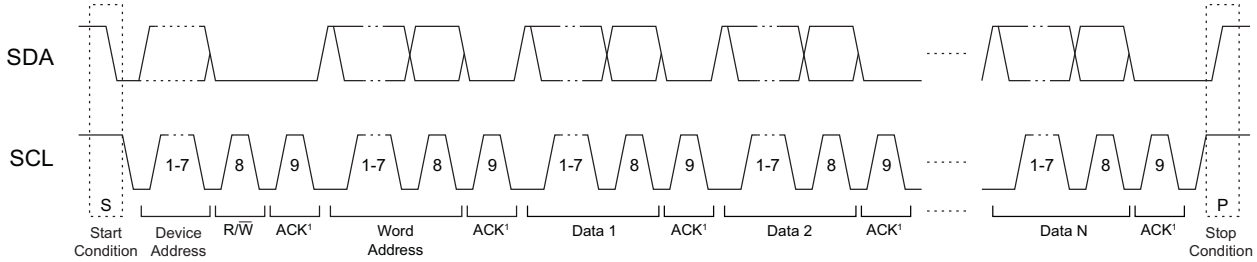
如果 I2C_Address 字节针对总线上的每个器件以不同方式编程，则多个 ATSHA204A 器件可共用同一 I²C 接口。由于器件地址的 6 个位可编程，因此 ATSHA204A 还可将 I²C 接口与任何标准 I²C 器件（包括串行 EEPROM）共用。Bit 3（也称为 TTL 使能）必须根据所需输入阈值进行编程，并且在特定应用中为固定设置。

6.2 到 ATSHA204A 器件的 I²C 传输

下图总结了从系统到 ATSHA204A 的数据传输。传输顺序如下：

1. 启动条件
2. 器件地址字节
3. 字地址字节
4. 可选数据字节（1 至 N）
5. 停止条件

图 6-4. 到 ATSHA204A 的正常 I²C 传输



注： ATSHA204A 在 ACK 周期内将 SDA 驱动为低电平

下表标记了 I/O 事务的字节。“I²C 名称”列提供了 AT24C16 数据手册中所描述字节的名称。

表 6-1. 到 ATSHA204A 的 I²C 传输

ATSHA204A	I²C 名称	方向	说明
器件地址	器件地址	至从器件	此字节选择 I²C 接口上的特定器件。如果此字节的 bit 1 至 bit 7 与配置区域中的 I2C_Address 字节的 bit 1 至 bit 7 匹配，则选择 ATSHA204A。此字节的 bit 0 是标准 I²C R/W 位，并且应为 0 以指示写操作（器件地址后的字节从主器件传输到从器件）。
数据	数据 1,N	至从器件	输入块。

由于器件将命令输入缓冲区视为 FIFO，因此输入块可通过一个或多个 I²C 命令块发送到器件。发送到器件的第一个字节是计数，所以在器件接收到相应数量的字节之后，它将忽略随后接收的任何字节，直到执行完成。

系统必须在最后一个命令字节后发送一个停止条件，以确保 ATSHA204A 将启动命令的计算。未能发送停止条件可能最终导致同步丢失（有关恢复程序，见 **I²C 同步**一节）。

6.2.1 字地址值

在 I²C 写数据包期间，ATSHA204A 会将发送的第二个字节解释为字地址，表示数据包功能，如下表所述。

表 6-2. 字地址值

名称	值	说明
复位	0x00	复位地址计数器。下一个读取或写入事务将从 I/O 缓冲区起始处开始。
休眠（低功耗）	0x01	ATSHA204A 进入低功耗休眠模式，忽略所有后续的 I/O 转换，直到下一个唤醒标志。器件的整个易失性状态将复位。
空闲	0x02	ATSHA204A 进入空闲状态，忽略所有后续的 I/O 转换，直到下一个唤醒标志。TempKey 和 RNG Seed 寄存器的内容将保留。
命令	0x03	将后续字节写入输入命令缓冲区中先前写入内容之后的连续地址。这是正常操作。
保留	0x04-0xFF	这些地址不应发送到器件。

6.2.2 命令完成轮询

完整的命令发送到 ATSHA204A 后，器件将一直处于繁忙状态，直到命令计算完成。对于此延时，系统有两个选项：

- **轮询**
  系统应等待 t_{EXEC}（典型值），然后发送一个读序列（见**来自 ATSHA204A 器件的 I²C 传输**一节）。如果器件未确认器件地址，则它仍处于繁忙状态。系统可延迟一段时间，也可立即发送另一个读取序列，再次在未确认状态下循环。在总延时 t_{EXEC}（最大值）后，器件将完成计算并返回结果。
- **单次延时**
  系统应等待 t_{EXEC}（最大值），之后器件将完成执行，并且可以使用正常读序列从器件读取结果。

6.3 自 ATSHA204A 器件的 I²C 传输

当 ATSHA204A 唤醒且不繁忙时，总线主器件可以使用 I²C 读取从器件中获取当前缓冲区内容。如果有效的命令结果可用，则返回的块大小由已经运行的特定命令决定（见**安全命令**一章）；否则，块大小（以及返回的第一个字节）将始终为 4：计数、状态/错误和 2 字节 CRC。总线时序如图 **I²C 同步数据时序**所示。

表 6-3. 自 ATSHA204A 的 I²C 传输

名称	I²C 名称	方向	说明
器件地址	器件地址	至从器件	此字节选择 I²C 接口上的特定器件，如果此字节的 bit 1 至 bit 7 与配置区域中的 I2C_Address 字节的 bit 1 至 bit 7 匹配，则选择 ATSHA204A。此字节的 bit 0 是标准 I²C R/W 引脚，并且应为 1 以指示器件地址后的字节从从器件传输到主器件（读操作）。
数据	数据 1,N	至主器件	由计数、状态/错误字节或输出数据包（后跟 2 字节的 CRC）组成的输出块，请参见第 8.2 节。

主器件可以重复读取状态、错误或命令输出。每次 Read 命令沿 I²C 接口发送到 ATSHA204A 时，器件均会发送输出缓冲区中的下一个连续字节。有关器件如何处理地址计数器的详细信息，请参见后续章节。

如果 ATSHA204A 处于繁忙、空闲或休眠状态，它将不会确认读序列上的器件地址。如果部分命令已发送至器件，则它将不会确认器件地址，但在数据间隔期间会使总线悬空。

6.4 地址计数器

通过 I²C 接口写入和/或读取 ATSHA204A I/O 缓冲区时假设器件为 FIFO。可使用 I²C 字节或块写入/读取协议。每个块序列传输的字节数不影响器件的操作。

发送给器件的第一个字节视为计数字节。如果尝试发送的字节多于此字节数，或者尝试写入的字节超过 I/O 缓冲区（84 字节）的末尾，则将导致 ATSHA204A 不确认这些字节。

在主机向输入缓冲区写入一个命令字节之后，将禁止主机向器件发出 Read 命令，直到器件完成命令执行。尝试在发送最后一个命令字节之前读取器件将导致确认总线上除全 1（0xFF）以外的器件地址。如果主器件在执行命令时尝试向器件发送一个读取字节，则器件将不会确认器件地址。

在以下三种条件下可以从器件读取数据：

- 上电后，可以在 4 字节块中读取单个字节 0x11（见**命令操作码、简要说明和执行时间**一节）。
- 如果器件接收到完整的数据块，但在解析或执行命令时发生任何错误，则可以使用一个字节的错误代码（也位于 4 字节块中）。
- 命令执行完成后，可以在 4 到 35 字节的块内读取 1-32 字节的命令结果。

如果尝试读取超出有效输出缓冲区结尾的数据，则将向系统返回 0xFF，地址计数器不会返回到缓冲区的起始处。

在某些情况下，系统可能希望重新读取输出缓冲区，例如当 CRC 校验显示错误时。在这种情况下，主器件应向 ATSHA204A 发送一个双字节序列，此序列包括正确的器件地址和字地址 0x00（复位，见表 6-2），然后是停止条件。这将导致地址计数器复位为 0，并允许向（或从）器件重新写入（或重新读取）数据。如果在序列执行之前 I/O 缓冲区中有数据可供读取，则此地址复位序列不禁止后续的读取操作。

在为获取命令执行的结果而进行一次或多次读取操作之后，第一次写入操作会将地址计数器复位到 I/O 缓冲区的起始处。

6.5 I²C 同步

系统可能会由于系统复位、I/O 噪声或其他某个条件而失去与 ATSHA204A I/O 端口的同步。在这种情况下，ATSHA204A 可能不会按预期响应，可能处于休眠状态，也可能在系统期望发送数据的时间间隔期间传输数据。当系统和器件失去同步时，I/O 缓冲区中的任何命令结果都可能丢失。要重新同步，应按照以下步骤操作：

1. 为了确保 I/O 通道复位，系统应发送标准 I²C 软件复位序列，具体如下：
   - 启动条件。
   - 9 个 SCL 周期，SDA 保持高电平。
   - 另一个启动条件。
   - 停止条件。

   然后应当可以发送一个读序列，如果同步正确完成，ATSHA204A 将确认器件地址。在数据周期内，器件可能返回数据，也可能使总线悬空（系统会将其解释为数据值 0xFF）。

   如果器件确认了器件地址，系统应复位内部地址计数器，强制 ATSHA204A 忽略可能已发送的任何部分输入命令。这可以通过将一个写序列发送到字地址 0x00（复位），然后再发送一个停止条件来实现。
2. 如果器件不通过 ACK 来响应器件地址，则它可能处于休眠状态。在这种情况下，系统应发送一个完整的 Wake 令牌并在上升沿后等待 t_{WHI}。系统随后可以发送另一个读序列，如果同步完成，器件将确认器件地址。
3. 如果器件仍不通过 ACK 来响应器件地址，则它可能忙于执行命令。系统应等待最长 t_{EXEC}（最大值），然后发送读取序列，这将由器件确认。

6.6 事务示例

表 6-4. 唤醒（I²C）

唤醒（I²C）		
主机		器件
启动	→	
唤醒	→	
停止	→	
启动	→	
从器件地址/R	→	
	←	数据
停止	→	

表 6-5. 事务示例

示例（I²C）		
主机	→	器件
启动	→	
唤醒	→	
停止	→	
启动	→	
从器件地址/R	→	
	←	数据
停止	→	
启动	→	
从器件地址/W	→	
命令	→	
数据	→	
停止	→	
启动	→	
从器件地址/R	→	
	←	数据
停止	→	
启动	→	
从器件地址/W	→	
空闲/休眠	→	
停止	→	

7. 电气特性

7.1 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	5.0 mA
任一引脚上的电压	0.5V 至（V_{CC} + 0.5V）
ESD 额定值：	
人体模型（Human Body Model，HBM）ESD	>4kV
充电器件模型（Charge Device Model，CDM）ESD	>1kV

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。上述值仅代表本规范规定的极限工作条件，不代表器件在上述极限值或超出极限值的情况下仍可正常工作。器件长时间工作在最大值条件下，其可靠性可能受到影响。

7.2 可靠性

ATSHA204A 采用 Microchip 公司具有极高可靠性的 CMOS EEPROM 制造技术生产。

表 7-1. EEPROM 可靠性

参数	最小值	典型值	最大值	单位
耐写入次数（25°C 时每个字节）	100,000			写周期
数据保持时间（55°C 时）	10			年
数据保持时间（35°C 时）	30	50		年
耐读取次数	无限			读周期

7.3 交流参数——所有 I/O 接口

图 7-1. 交流时序图——所有 I/O 接口

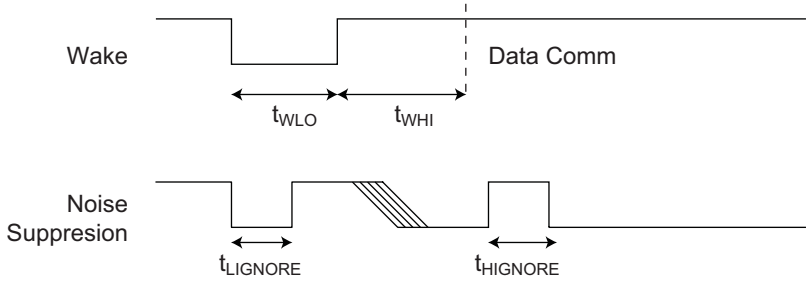


表 7-2. 交流参数——所有 I/O 接口

参数	符号	方向	最小值	典型值	最大值	单位	注
唤醒为低电平的持续时间	t_{WLO}	至加密验证	60		—	µs	在延长的休眠间隔内，SDA 可以稳定在高电平或低电平。
上电延时	t_{PU}	至加密验证	100(1)			µs	从 V_{CC} > V_{CC} min 到测量 t_{WLO} 的最短时间。
唤醒为高电平到数据通信的延时	t_{WHI}	至加密验证	2.5			ms	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			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			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。
上桥臂毛刺滤波器休眠时间	$t_{HIGNORE\_S}$	至加密验证	15			µs	处于休眠模式时，宽度短于此时间的脉冲将被器件忽略。
下桥臂毛刺滤波器休眠时间	$t_{LIGNORE\_S}$	至加密验证	15			µs	处于休眠模式时，宽度短于此时间的脉冲将被器件忽略。
看门狗复位	$t_{WATCHDOG}$	至加密验证	0.7(1)	1.3	1.7	s	从唤醒到强制器件进入休眠模式的最长时间（见**看门狗故障保护**一节）。

注：

1. 这些参数为特性值，但未经测试。

7.3.1 交流参数——单线接口

图 7-2. 交流时序图——单线接口

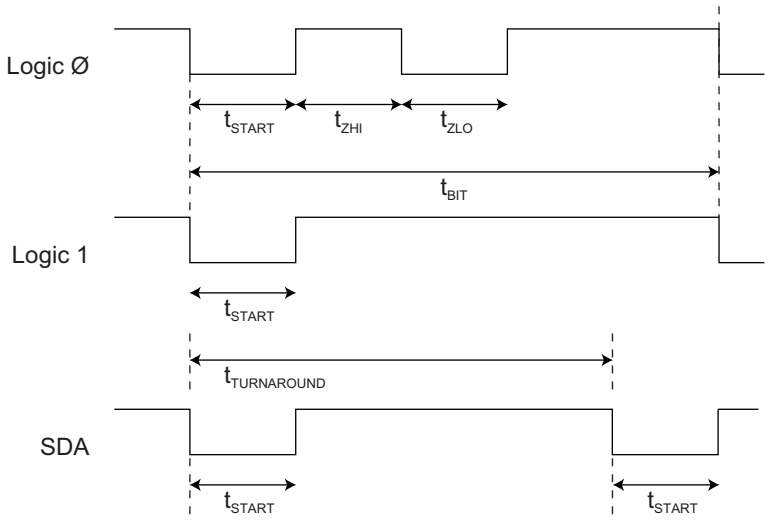


表 7-3. 交流参数——单线接口

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(1)	t_{START}	至加密验证	4.10	4.34	4.56	µs	
		自加密验证	4.60	6.00	8.60	µs	
零传输高电平脉冲(1)	t_{ZHI}	至加密验证	4.10	4.34	4.56	µs	
		自加密验证	4.60	6.00	8.60	µs	
零传输低电平脉冲(1)	t_{ZLO}	至加密验证	4.10	4.34	4.56	µs	
		自加密验证	4.60	6.00	8.60	µs	
位时间(1)	t_{BIT}	至加密验证	37	39	—	µs	如果位时间超过 $t_{TIMEOUT}$，则 ATSHA204A 可能会进入休眠状态。有关特定详细信息，请参见 **I/O 超时** 一节。
		自加密验证	41	54	78	µs	
周转延时	$t_{TURNAROUND}$	自加密验证	64	80	131	µs	在传输标志最后一位（t_{BIT}）起始后的这段时间间隔之后，ATSHA204A 将启动第一个低电平转换。
		至加密验证	93			µs	在 ATSHA204A 传输块的最后一位后，系统必须等待此段时间间隔，之后才能发送标志的第一位。
I/O 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 ATSHA204A 可能转换到休眠状态。有关特定详细信息，请参见 **I/O 超时** 一节。

注：

1. t_{START}、t_{ZLO}、t_{ZHI} 和 t_{BIT} 设计为与发送和接收都以 230.4K 波特运行的标准 UART 兼容。UART 应设置为 7 个数据位、无奇偶校验和 1 个停止位。

7.3.2 交流参数——I²C 接口

图 7-3. I²C 同步数据时序

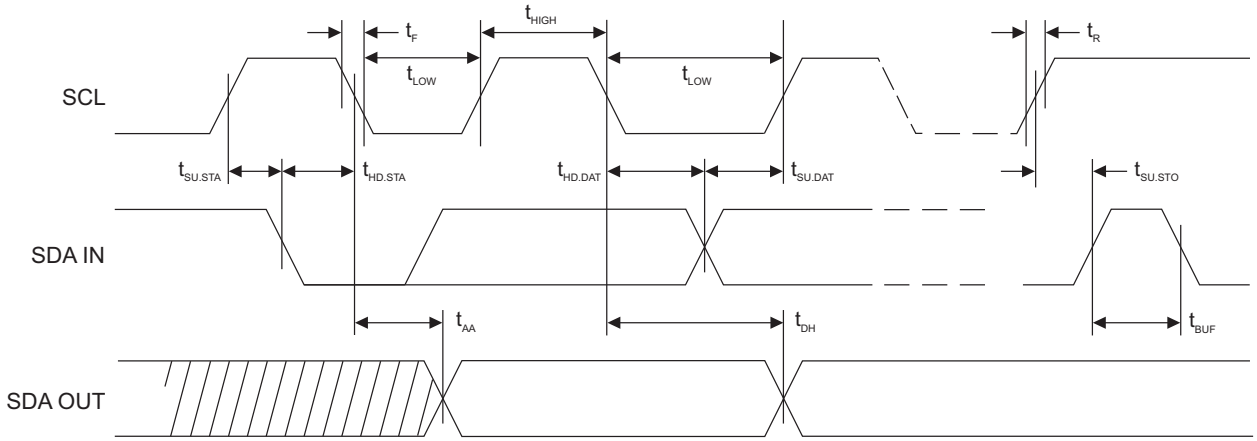


表 7-4. I²C 接口的交流特性

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。

符号	参数	最小值	最大值	单位
f_{SCK}	SCK 时钟频率		1000	kHz
	SCK 时钟占空比	30	70	%
t_{HIGH}	SCK 高电平时间	400		ns
t_{LOW}	SCK 低电平时间	400		ns
$t_{SU.STA}$	启动条件建立时间	250		ns
$t_{HD.STA}$	启动条件保持时间	250		ns
$t_{SU.STO}$	停止条件建立时间	250		ns
$t_{SU.DAT}$	数据输入建立时间	100		ns
$t_{HD.DAT}$	数据输入保持时间	0		ns
t_R	输入上升时间(1)		300	ns
t_F	输入下降时间(1)		100	ns
t_{AA}	时钟低电平到数据输出有效的时间	50	550	ns
t_{DH}	数据输出保持时间	50		ns
t_{BUF}	在新传输开始前时间总线必须保持空闲的时间。(1)	500		ns

注：

1. 上述值均为特性值，但未经测试。
   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：$0.3V_{CC}$ 至 $0.7V_{CC}$
   - 输入上升和下降时间：≤ 50 ns
   - 输入和输出时序参考电压：$0.5V_{CC}$

7.4 直流参数——所有 I/O 接口

表 7-5. 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	注
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}		500		μA	0°C → +70°C，V_{CC} = 3.3V。
			—	2	mA	-40°C → +85°C，V_{CC} = 5.5V。

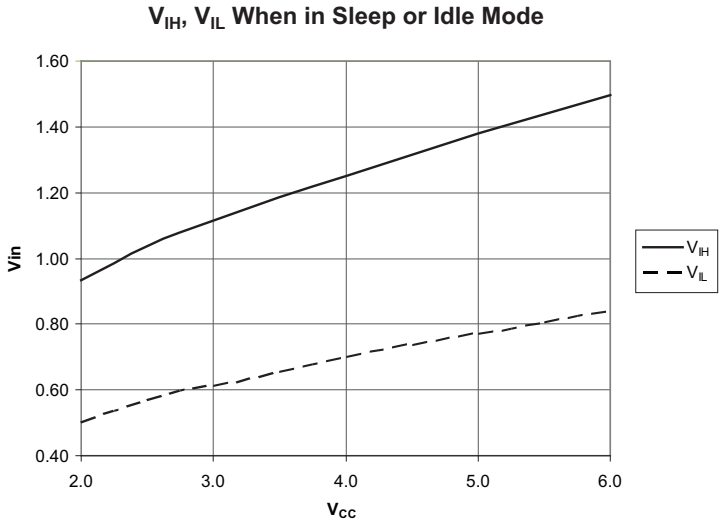
.....（续）

参数	符号	最小值	典型值	最大值	单位	注
电源空闲电流	I IDLE		200		μA	当器件处于空闲模式时，V_{CC} = 3.3V，V_{SDA} 和 V_{SCL} < 0.3V 或> > V_{CC}-0.3。
休眠电流	I SLEEP		30	150	nA	当器件处于休眠模式时，$V_{CC} \leq$ 3.6V，V_{SDA} 和 V_{SCL} < 0.3V 或 > V_{CC}-0.3，$T_A \leq$ 55°C
				2	μA	当器件处于休眠模式时；所有工作条件。
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。

7.4.1 V_{IH} 和 V_{IL} 规范

休眠或空闲模式下的输入电压阈值取决于 V_{CC} 电平，如下图“休眠或空闲模式下的 V_{IH} 和 V_{IL}”所示。

图 7-4. 休眠或空闲模式下的 V_{IH} 和 V_{IL}



器件处于工作状态（例如，不处于休眠或空闲模式）时，输入电压阈值取决于存储在 EEPROM 配置区域中的 I2C_Address 字节内 TTLenable（bit 3）的状态。当公共电压用于 ATSHA204A V_{CC} 引脚和输入上拉电阻时，该位应设置为 1，从而允许输入阈值跟踪电源，如图 7-5 所示。

如果 ATSHA204A 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，输入信号必须满足表 7-6 所示的阈值。

图 7-5. 所有 I/O 接口上的 TTLenable = 1 时的 V_{IH} 和 V_{IL}

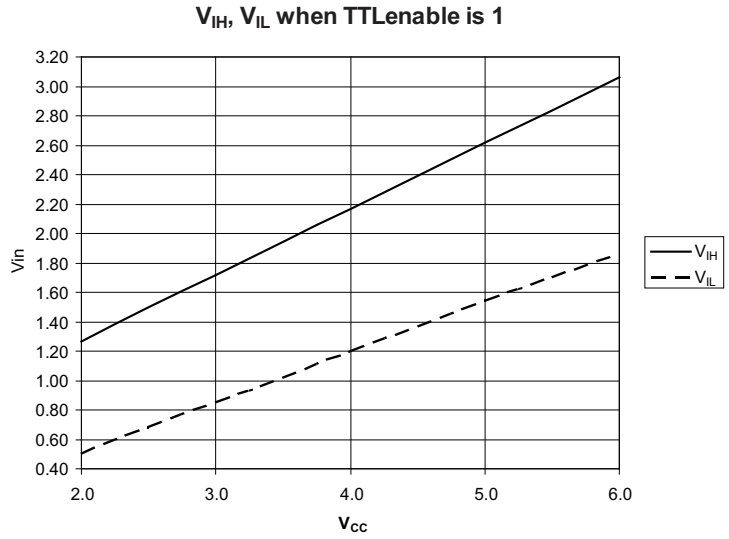


表 7-6. 所有 I/O 接口上的 TTLenable = 0 时的 V_{IL} 和 V_{IH}

参数	符号	最小值	典型值	最大值	单位	注
输入低电压	V_{IL}	GND - 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。

8. 安全命令

8.1 I/O 块

无论所使用的 I/O 协议（例如单线还是 I²C）如何，都会向器件发送命令，并会从按以下方式构建的块中接收到器件的响应：

表 8-1. 块

字节	名称	含义
0	Count	数据包大小。包括计数、数据和校验和。
1 至 N-2	Data	如果是器件输入，则为命令和参数。如果是器件输出，则为器件基于正在调用的命令的响应。
N-1 至 N	Checksum	CRC-16。CRC 多项式为 0x8005。

ATSHA204A 的设计应使输入块中的计数值与命令参数中指定的大小要求一致。如果计数值与数据包内的命令操作码和/或参数不一致，则 ATSHA204A 将根据具体的命令以不同的方式响应。响应可能包含错误指示，也可能默默忽略一些输入字节。

8.1.1 状态/错误代码

器件没有专用的状态寄存器，因此状态、错误和命令结果共用输出 FIFO。器件的所有输出均作为完整的块返回至系统。

器件接收到输入命令块的第 1 个字节后，系统将无法读取器件中的任何内容，直到系统将所有字节发送给器件。

在唤醒后和执行命令后，器件的输出寄存器中会有错误、状态或结果字节，可通过系统获取。当此数据块的长度是 4 个字节时，返回的代码详见下表。有些命令执行成功时会返回超过 4 个字节。得到的数据包说明在下面的“命令”部分列出。

CRC 错误始终在任何其他类型的错误之前返回。它们表明发生了某种 I/O 错误，并且此命令可重新发送给器件。如果一条命令同时包含解析错误和执行错误，则无需遵循特定的优先顺序，因此执行错误既可能发生在解析错误之前，也可能发生在解析错误之后。

表 8-2. 4 字节块中的状态/错误代码

状态说明	错误/状态	说明
命令执行成功	0x00	命令执行成功。
Checkmac 不匹配	0x01	CheckMac 命令已正确发送到器件，但输入客户端响应与预期值不匹配。
解析错误	0x03	命令已正确接收，但长度、命令操作码或参数非法，而与 ATSHA204A 的状态（易失性和/或 EEPROM 配置）无关。 命令位的值必须在重新尝试之前进行更改。
执行错误	0x0F	命令已正确接收，但无法由器件在当前状态下执行。 器件状态或命令位的值必须在重新尝试之前进行更改。
在唤醒之后、第 1 条命令之前	0x11	指示 ATSHA204A 已收到适当的 Wake 令牌。

.....（续）		
状态说明	错误/状态	说明
CRC 或其他通信错误	0xFF	命令未由 ATSHA204A 正确接收，应由系统中的 I/O 驱动器重新发送。 未尝试解析或执行命令。

8.2 休眠序列

系统完成使用 ATSHA204A 后，应发出休眠序列，使器件进入低功耗模式。通过使用 I^2C 接口，此序列包含正确的器件地址，接着是休眠标志，然后是停止条件。这种到低功耗状态的转换会导致器件的内部命令引擎和输入/输出缓冲区完全复位。当器件唤醒且不忙时，此序列可随时发送到器件。

8.3 空闲序列

如果所需命令的总序列超过 $t_{WATCHDOG}$，则器件将自动进入休眠状态，并丢失存储在易失性寄存器中的任何信息。在看门狗时间间隔完成之前将器件置于空闲状态可防止此操作。当器件收到 Wake 令牌时，它将重新启动看门狗定时器，并继续执行。

通过使用 I^2C 接口，此空闲序列包含正确的器件地址，接着是值 0x02（作为字地址），然后是停止条件。当器件唤醒且不忙时，此序列可随时发送到器件。

如果 TempKey 是因 CheckMac 命令的副本模式而创建，则在器件进入空闲状态时不会保留。

8.4 看门狗故障保护

ATSHA204A 收到 Wake 令牌后，器件内的看门狗计数器将启动。在 $t_{WATCHDOG}$ 之后，无论正在进行某种 I/O 传输还是正在执行命令，器件都会进入休眠模式。除了将器件置于休眠或空闲模式，然后再将其唤醒之外，无法复位计数器。

看门狗定时器是作为一种故障保护机制实现的，因此无论系统侧或器件内部出现何种情况（包括任何 I/O 同步问题），功耗均会自动下降到超低休眠水平。

当器件转换到休眠状态时，它将复位存储在 SRAM 和内部状态寄存器中的值；但是，如果器件通过适当的 I/O 序列明确地进入空闲模式，则器件将保留 2 个 SRAM 寄存器（例如，TempKey 和 RNG Seed）的内容。

通常，对于所有命令序列而言，如果它们需要存储在 SRAM 寄存器中的状态，则必须在 $t_{WATCHDOG}$ 内完成。系统软件可以在各命令之间使用这种空闲模式机制来实现比单个看门狗时间间隔内可完成的序列更长的命令序列。

8.5 命令序列

8.5.1 命令数据包

下表对命令数据包进行了分解。

表 8-3. 命令数据包

字节编号	名称	含义
0	Command	命令标志（有关 I²C 工作模式的信息，请参见**字地址值**，有关单线接口模式的信息，请参见 **I/O 标志**）。不包括在计数或 CRC 字段中。
1	Count	数据包大小：包括计数、操作码、Param1、Param2、数据和 CRC。不包括命令标志。
2	Opcode	ATSHA204A 正在调用的操作。
3	Param1	第一个参数。始终存在一个字节。
4-5	Param2	第二个参数。始终存在两个字节。
	Data	基于正在调用的命令的可选数据。
N-1 至 N	Checksum	CRC-16。CRC 多项式为 0x8005。包括计数、操作码、Param1、Param2 和数据。不包括命令标志。

在 ATSHA204A 接收到块中的所有字节之后，器件将转换到繁忙状态并尝试执行命令。当器件繁忙时，无法从其中读取状态和结果。在此期间，无论选择哪个 I/O 接口，器件的 I/O 接口都会忽略所有 SDA 转换。**数据区域中的读操作**一节中列出了命令执行延时。

如果器件处于单线模式时未向其中发送足够数量的字节，则器件会在 $t_{TIMEOUT}$ 间隔后自动转换到低功耗休眠状态。在 I²C 模式下，器件将继续等待其余字节，直到达到看门狗定时器限值 $t_{WATCHDOG}$，或者器件接收到启动/停止条件。

在表 8-8 至表 8-41 的各个命令说明中，大小列描述了每个特定行中记录的参数中的字节数。如果特定命令的输入块大小不正确，则器件将根据命令做出不同的响应。任何情况下都不会返回错误指示（见**状态/错误代码**一节）。

8.5.2 命令操作码、简要说明和执行时间

在解析参数和随后执行正确接收的命令期间，器件将处于繁忙状态，不响应引脚的转换。器件处于繁忙状态的时间间隔取决于命令及其参数值、器件状态、环境条件以及其他因素，如下表所示。

在大多数情况下（但不是所有情况下），失败的命令都会在典型执行时间之前相对迅速地返回。

表 8-4. 命令操作码、简要说明和执行时间

命令	操作码	说明	典型执行时间(1)（ms）	最大执行时间(2)（ms）
DeriveKey	0x1C	从目标密钥或父密钥得出目标密钥值。	14	62
DevRev	0x30	返回器件版本信息。	0.4	2
GenDig	0x15	通过随机或输入种子和密钥生成数据保护摘要。	11	43
HMAC	0x11	使用 HMAC/SHA-256 计算密钥和其他内部数据的响应。	27	69
CheckMac	0x28	验证在另一个 Microchip CryptoAuthentication 器件上计算的 MAC。	12	38
Lock	0x17	防止进一步修改器件的某个区域。	5	24
MAC	0x08	使用 SHA-256 计算密钥和其他内部数据的响应。	12	35

.....（续）

命令	操作码	说明	典型执行时间(1)（ms）	最大执行时间(2)（ms）
Nonce	0x16	生成一个 32 字节的随机数和一个内部存储的临时值。	22	60
Pause	0x01	选择性地仅将共用总线上的一个器件置于空闲状态。	0.4	2
Random	0x1B	生成一个随机数。	11	50
Read	0x02	从器件读取 4 个字节，可以使用或不使用身份验证和加密。	0.4	4
SHA	0x47	计算 SHA256 摘要以用于系统中的任一功能。	11	22
UpdateExtra	0x20	配置区域锁定后，更新配置区域内的字节 84 或 85。	8	12
Write	0x12	向器件写入 4 个或 32 个字节，可以使用或不使用身份验证和加密。	4	42

注：

1. 典型的执行时间代表执行命令的持续时间，假设没有错误条件，采用最快的模式设置，无可选内部操作（例如，限制使用的密钥）且在有利的环境条件下。为获得最佳性能，请延迟此时间间隔，随后开始轮询以确定实际命令完成的时间。
2. 最长的执行时间代表在扩展的统计和环境条件下成功执行命令的最长持续时间（所有模式和内部操作均使能）。在极端情况下，执行时间可能会超出这些值。

8.5.3 区域编码

用于 Read 命令和 Write 命令的 Param1 中的值控制命令将访问的区域。欲了解各区域“锁定”和“解锁”状态的控制因素的更多信息，请参见**配置区域锁定**一节。所有其他区域的值均保留，不得使用。

表 8-5. 区域编码（Param1）

区域名称	Param1 的值	大小	读	写
配置	0	704 位 88 字节 3 个槽	始终支持。	解锁时，部分支持。 锁定时，始终不支持。 始终不加密。
OTP	1	512 位 64 字节 2 个槽	解锁时，始终不支持。锁定时始终支持，传统模式除外。 请参见**可一次性编程（OTP）区域**一节。	LockConfig 解锁时不允许。 LockConfig 锁定且 LockValue 解锁时，均可写。 LockValue 锁定时由 OTPmode 控制。 请参见**可一次性编程（OTP）区域**一节。
数据	2	4096 位 512 字节 16 个槽	解锁时，始终不支持；其他情况下，由 IsSecret 和 EncryptRead 控制。	LockConfig 解锁时不允许。 LockConfig 锁定且 LockValue 解锁时，均可写。 LockValue 锁定时由 WriteConfig 控制。 请参见**器件锁定**一节。

8.5.4 地址编码

Param2 包含一个地址，表示要访问的存储器。所有读操作和写操作均以字（4 字节）为单位。合法 ATSHA204A 地址的最高有效字节始终为 0。所有未使用地址位均应始终设为 0。地址中的低位描述了块/槽内要访问的第一个字的偏移量，而高位指定了槽号，如下表所示：

表 8-6. 地址编码（Param2）

区域	字节 0（总线上的第 1 个字节）								字节 1							
	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
数据	0	模块				偏移量			0	0	0	0	0	0	0	0
配置	0	0	0	模块		偏移量			0	0	0	0	0	0	0	0
OTP	0	0	0	0	模块	偏移量			0	0	0	0	0	0	0	0

每个区域内有不同的访问限制，如下表所示：

表 8-7. 合法块/槽值

区域	合法块/槽（包括上下限值）	注
数据	0-15	所有槽中的所有偏移量均可供读写使用。 仅当 S槽lotConfig.IsSecret 为 0 时，才允许在特定槽上进行 4 字节访问。
配置	0-2	始终不可读取高于 16（块 2，偏移量 6）的字。 读取和写入高于 10（块 2，偏移量 0）的字时必须采用字（4 字节）模式。 始终不可写入低于 04（块 0，偏移量 4）和高于 15（块 2，偏移量 5）的字。
OTP	0-1	当 OTPmode 为只读模式时，两个块中的所有偏移量都可与 4 字节和 32 字节读取一起使用。 如果 OTPmode 为消耗模式，还允许对所有偏移量进行写操作。如果 OTPmode 为传统模式，请参见**可一次性编程（OTP）区域**一节。

8.5.5 CheckMac 命令

CheckMac 命令可计算 CryptoAuthentication 器件上生成的 MAC 响应，然后将 MAC 响应与特定输入值进行比较。它会返回一个布尔结果来指示比较成功还是失败。

在运行此命令之前，可能已选择性地运行 Nonce 和/或 GenDig 命令以在 TempKey 中创建和加载密钥或临时值。模式参数确定“密钥”（SHA 报文的前 32 个字节）和“质询/临时值”（SHA 报文的第 2 组 32 个字节）的来源。

如果 TempKey 是计算值的一部分，则使用 Mode<2>控制对随机临时值的要求。如果 Mode<2> = 1，则必须使用 Nonce(Fixed) 生成 TempKey；如果 Mode<2> = 0，则必须使用 Nonce(Random) 生成 TempKey。

在某些情况下，将 Mode<2>置 1 会使能重放攻击。

如果比较匹配，则目标槽值可复制到 TempKey 中。如果 SlotID 为偶数，则目标槽为 SlotD+1，否则目标槽为 SlotID。要实现复制，以下条件必须为真。如果不全为真，则 ATSHA204A 将返回比较结果，但不会复制密钥值。

1. CheckMac 的模式参数值必须为 0x01 或 0x05。
2. 目标密钥的 SlotConfig.ReadKey 必须为 0。
3. Config.CheckMacSource 中对应于密钥槽的位值必须与 Mode<2>匹配。

表 8-8. 输入参数

	名称	大小	注
Opcode	CheckMac	1	0x28
Param1	Mode	1	**Bit 7-6：** 必须为 0。 SHA 报文的 8 个字节。 **Bit 5：** 0：0 1：OTP 区域 **Bit 4-3：** 必须为 0。 **Bit 2：** 如果使用 TempKey，则此位必须与 TempKey.SourceFlag 的值匹配。 SHA 报文的前 32 字节的来源。 **Bit 1：** 0：Slot<SlotID> 1：TempKey SHA 报文的第二组 32 字节的来源。 **Bit 0：** 0：ClientChal 参数 1：TempKey
Param2	SlotID	2	将用于生成响应的内部槽。仅使用 bit 3-0。
Data1	ClientChal	32	发送到客户端的质询。（必须显示在输入流中）。
Data2	ClientResp	32	客户端生成的响应。
Data3	OtherData	13	响应计算所需的剩余常量数据。

表 8-9. 输出参数

名称	大小	注
Result	1	如果 ClientResp 与内部计算的摘要匹配，则返回值为 0 的单个字节；如果不匹配，则为 1。

使用 SHA-256 算法进行哈希运算的报文由以下信息组成：

32 字节	key<SlotID>或 TempKey（具体取决于模式）
32 字节	ClientChal 或 TempKey（具体取决于模式）
4 字节	OtherData<0:3>
8 字节	OTP<0:7>或 0（具体取决于模式）
3 字节	OtherData<4:6>
1 字节	SN<8>
4 字节	OtherData<7:10>
2 字节	SN<0:1>

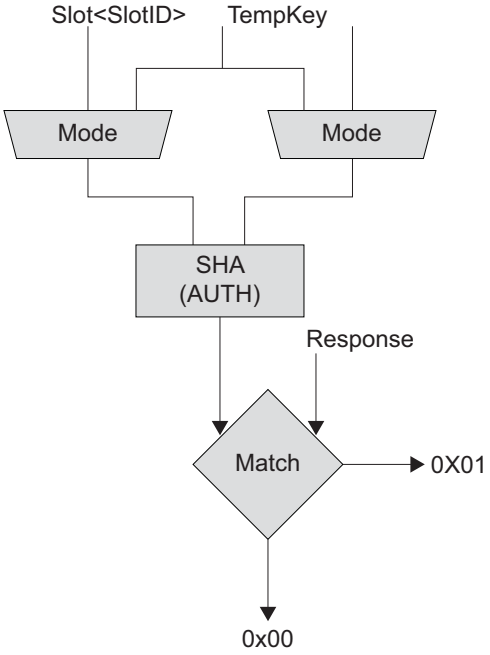
2 字节	OtherData<11:12>

OtherData 用于构建 SHA-256 报文，此报文将与用于生成 ClientResp 的 MAC 报文完全匹配。通过比较用于 MAC 命令的 SHA-256 的报文，OtherData 解析如下：

表 8-10. OtherData

大小	CheckMac	MAC	注
1	OtherData<0>	OpCode	MAC 操作码 = 0x08
1	OtherData<1>	Mode	用于 MAC 命令的模式。
2	OtherData<2:3>	SlotID	用于 MAC 命令的 SlotID。
3	OtherData<4:6>	OTP<8:10>	用于 MAC 命令的 OTP<8:10>。（适用于传统模式。）
4	OtherData<7:10>	SN<4:7>	用于 MAC 命令的 SN<4:7>。（对于每个客户端惟一。）
2	OtherData<11:12>	SN<2:3>	用于 MAC 命令的 SN<2:3>。（对于每个客户端惟一。）

图 8-1. 用于 CheckMac 命令的数据流



8.5.6 DeriveKey 命令

器件使用 SHA-256 将密钥的当前值与存储在 TempKey 中的临时值组合，并将结果放入目标密钥槽中。SlotConfig<TargetKey>.Bit13 必须置 1，否则 DeriveKey 将返回错误。

如果 SlotConfig<TargetKey>.Bit12 为 0，则与 TempKey 组合的源密钥是命令行（滚动密钥操作）中指定的目标密钥。如果 SlotConfig<TargetKey>.Bit12 为 1，则源密钥是 SlotConfig<TargetKey>.WriteKey（创建密钥操作）中的目标密钥的父密钥。

在执行 DeriveKey 命令之前，必须已运行 Nonce 命令，才能在 TempKey 中创建有效的临时值。根据输入模式的第二位的状态，此临时值可能已通过内部 RNG 创建，或者已被修复。

如果 SlotConfig<TargetKey>.Bit15 置 1，则输入 MAC 必须存在并且已按如下方式计算：

SHA-256（ParentKey，Opcode，Param1，Param2，SN<8>，SN<0:1>）
其中，ParentKey ID 始终为 SlotConfig<TargetKey>.WriteKey。

如果 SlotConfig<TargetKey>.Bit12 或 SlotConfig<TargetKey>.Bit15 置 1，且 SlotConfig<ParentKey>.LimitedUse 也置 1，`DeriveKey` 将在 UseFlag<ParentKey>为 `0x00` 时返回错误。如果 SlotConfig<TargetKey>.Bit12 和 SlotConfig<TargetKey>.Bit15 均为 0，则 `DeriveKey` 会忽略目标密钥的 LimitedUse 和 UseFlag。

仅针对槽 0 至 7，如果输入解析和可选 MAC 检查成功，则 UseFlag<TargetKey>置为 `0xFF`，且 UpdateCount<TargetKey>递增。如果 UpdateCount 当前值为 0xFF，则它会绕回至零。如果命令因任何原因而失败，这些字节将无法更新。如果在执行 `DeriveKey` 期间断电，则 UpdateCount 值可能会损坏。

注： 当源密钥和目标密钥相同时，如果电源在写入操作期间中断，则存在密钥值永久丢失的风险。如果配置位允许，则可以使用经过认证和加密的写入操作基于父密钥来恢复密钥槽。

表 8-11. 输入参数

	名称	大小	注
操作码	DeriveKey	1	0x1C
Param1	Random	1	**Bit 7-3：** 必须为 0。 **Bit 2：** 此位的值必须与 TempKey.SourceFlag 中的值相匹配，否则命令将返回错误。 **Bit 1-0：** 必须为 0。
Param2	TargetKey	2	要写入的密钥槽。
数据	Mac	0 或 32	用于验证操作的可选 MAC。

表 8-12. 输出参数

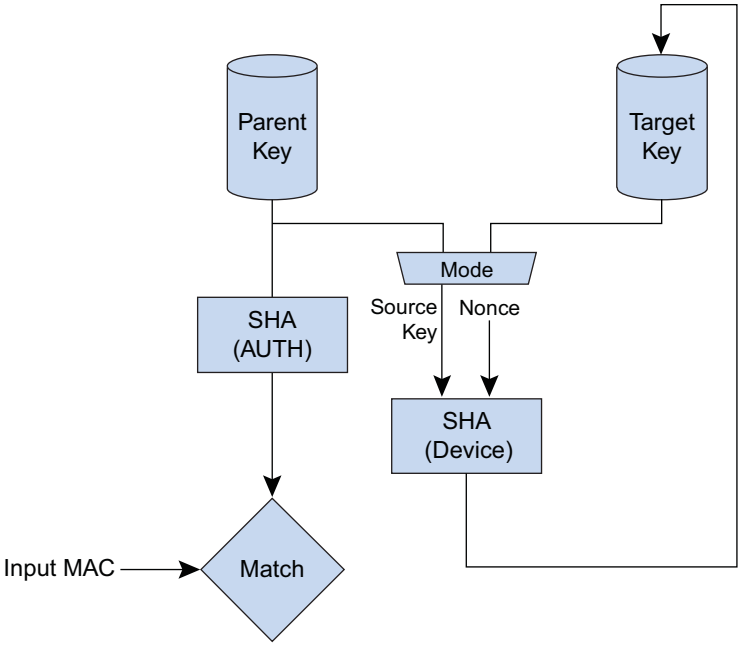
名称	大小	注
Success	1	成功完成后，ATSHA204A 将返回值 0。

写入目标槽的密钥是以下报文的 SHA-256 的结果：

32 字节	目标密钥或父密钥（具体取决于 SlotConfig Bit12）
1 字节	操作码
1 字节	Param1
2 字节	Param2
1 字节	SN<8>
2 字节	SN<0:1>
25 字节	0
32 字节	TempKey.value

此命令的数据流如下图所示：

图 8-2. DeriveKey 命令的数据流



8.5.7 DevRev 命令

DevRev 命令返回表示器件版本号的单一 4 字节字。软件不应依赖于此值，因为它可能会不时发生更改。

表 8-13. 输入参数

	名称	大小	注
操作码	DevRev	1	0x30.
Param1	Mode	1	必须为 0。
Param2	—	2	必须为 0。
数据	—	0	—

表 8-14. 输出参数

名称	大小	注
Success	4	当前器件版本号。

8.5.8 GenDig 命令

GenDig 命令使用 SHA-256 将存储的值与 TempKey 的内容相结合，这些内容在执行此命令之前必须有效。存储的值可以来自其中一个数据槽、任一 OTP 页、配置区域前两页的任意一页，也可以来自硬件传输密钥阵列。得到的摘要保留在 TempKey 中，可以通过以下三种方式之一使用：

1. 它可以作为 MAC、CheckMac 或 HMAC 命令使用的报文的一部分包含在内。由于 MAC 响应输出结合了 GenDig 计算中使用的数据与 MAC 命令的机密信息密钥，因此将用于验证数据和/或 OTP 区域中存储的数据。
2. 后续 Read 或 Write 命令可以使用摘要来为数据提供认证和/或加密，在这种情况下，相应摘要称为数据保护摘要。

3. 可以使用此命令通过传输密钥阵列中的值进行安全个性化。得到的数据保护摘要将供 Write 命令使用。

如果区域为 2（数据），并且 SlotID 小于等于 15，则 GenDig 命令会将 TempKey.GenData 设置为 1，将 TempKey.SlotID 设置为输入 SlotID；否则，TempKey.GenData 将设置为 0。

无论如何计算得到的摘要，都不能从器件读取摘要。

如果 TempKey.Valid 无效，则此命令将返回错误。在命令完成时，TempKey.Valid 位置 1，表明摘要已加载并且可以使用。当执行下一个命令时，TempKey.Valid 位将清零。有关详细信息，请参见**静态 RAM（SRAM）**一节。

对于所有小于 0x8000 的 SlotID 值，器件将使用 SlotID 的低 4 位来确定从其中获得 EEPROM 数据区域中密钥值的槽编号。大于 0x8000 的 SlotID 值将引用设计的掩码中存储的密钥。在任何情况下，作为器件输入的所有 16 位 SlotID 均用作 SHA-256 计算中的 Param2。

如果区域参数指向配置区域，则在配置区域解锁时，此命令会返回错误。

当 GenDig 输入上所指定密钥的 CheckOnly 位置 1 时，可使用 GenDig 来生成与使用 DeriveKey 命令在客户端 CryptoAuthentication 器件上生成的密钥相匹配的临时密钥。CheckOnly 位置 1 的密钥表示器件充当主机的情况。在这种情况下，通常会包含在 SHA 计算中的操作码和参数字节将替换为来自输入流的字节。

表 8-15. 输入参数

	名称	大小	注
操作码	GenDig	1	0x15
Param1	Zone	1	如果为 0x00（配置），则使用 SlotID 指定配置区域的第 1 个（SlotID = 0）或第 2 个（SlotID = 1）256 位块。 如果为 0x01（OTP），则使用 SlotID 指定 OTP 区域的第 1 个或第 2 个 256 位块。 如果为 0x02（数据），则 SlotID 指定数据区域中的槽或硬件阵列中的传输密钥。所有其他值都被保留，且不能使用。
Param2	SlotID	2	要使用的密钥的标识号，或 OTP 块的选择。
数据	OtherData	4 或 0	当使用 CheckOnly 密钥时，SHA 计算使用 4 字节数据；其他情况将被忽略。

表 8-16. 输出参数

名称	大小	注
Success	1	成功执行后，ATSHA204A 将返回值 0。

如果区域为“数据”且 SlotConfig<SlotID>.CheckOnly 为 1，则用于创建所得到的全新 TempKey 的 SHA-256 报文内容由以下字节组成：

32 字节	Slot<SlotID>
4 字节	OtherData
1 字节	SN<8>
2 字节	SN<0:1>
25 字节	0

32 字节	TempKey.value

在所有其他情况下，用于创建 TempKey 的报文均如下所示：

32 字节	Config<SlotID>、OTP<SlotID>、Data.slot<SlotID>或 TransportKey<SlotID>
1 字节	操作码
1 字节	Param1
2 字节	Param2
1 字节	SN<8>
2 字节	SN<0:1>
25 字节	0
32 字节	TempKey.value

8.5.9 HMAC 命令

HMAC 命令为存储在器件中的密钥、质询和器件上的其他信息计算 HMAC/SHA-256 摘要。此命令的输出是通过此密钥和报文计算的 HMAC 算法的输出。如果报文包含器件的序列号，则此响应是“多样化的”。

使用此命令的正常命令流程如下所示：

1. 运行 Nonce 命令以加载输入质询，并视情况将其与生成的随机数组合。此操作的结果是在器件内部存储的一个临时值。
2. 视情况运行 GenDig 命令，将器件中的一个或多个存储 EEPROM 单元与临时值组合。结果存储在器件内部。
3. 运行此 HMAC 命令，将步骤 1（以及步骤 2，需要时）的输出与 EEPROM 密钥组合，以生成输出响应。

步骤 2 处理了多个使用模型。如果 EEPROM 中的数据是密钥，则 GenDig 具有使用多个机密信息密钥对质询进行验证的作用。此外，如果槽的内容是数据（甚至不一定是机密），则 GenDig 具有验证存储在此单元的值的作用。

表 8-17. 输入参数

	名称	大小	注
操作码	HMAC	1	0x11。
Param1	Mode	1	控制器件中的哪些字段用于报文。
Param2	SlotID	2	将用于生成响应的密钥。 Param2<3:0>仅用于选择一个槽，而 HMAC 报文中将使用全部 16 位。
数据	—	0	—

表 8-18. 输出参数

名称	大小	注
Response	32	HMAC 摘要

将 SlotID 中的密钥作为 HMAC 密钥为包含以下信息的报文计算 HMAC 摘要：

32 字节	0

32 字节	TempKey
1 字节	操作码（始终为 0x11）
1 字节	Mode
2 字节	SlotID
8 字节	OTP<0:7>或 0（见下表）
3 字节	OTP<8:10>或 0（见下表）
1 字节	SN<8>
4 字节	SN<4:7>或 0（见下表）
2 字节	SN<0:1>
2 字节	SN<2:3>或 0（见下表）

有关包含如何使用 SHA-256、HMAC 密钥和相应填充计算各摘要的完整说明的管理文档，请参见 **HMAC/SHA-256** 一节。

表 8-19. 模式编码

位	含义
7	必须为 0。
6	**0 =** 对应于 SN<2:3>和 SN<4:7>的 48 个位设置为 0。 **1 =** 报文中包含 48 位 SN<2:3>和 SN<4:7>
5	**0 =** 对应于 OTP<0>至 OTP<7>的 64 个位设置为 0。 **1 =** 报文中包括前 64 个 OTP 位（8 字节）OTP<0>至 OTP<7>。 如果 Mode<4>置 1，则此模式位的值将被忽略。
4	**0 =** 对应于 OTP<0>至 OTP<10>的 88 个位（11 个字节）设置为 0。 **1 =** 报文中包括前 88 个 OTP 位（11 字节）OTP<0>至 OTP<10>。
3	必须为 0。
2	此位的值必须与 TempKey.SourceFlag 中的值相匹配，否则命令将返回错误。
1-0	必须为 0b00。

8.5.10 Lock 命令

将 LockConfig 或 LockValue 写为 0x00，以更改指定区域中的权限。

如果指定区域已锁定，则此命令失败。

在锁定器件前，ATSHA204A 使用 CRC-16 算法来生成指定区域的摘要。此计算使用与为输入和输出块计算的 CRC 相同的算法。

- **配置区域：**CRC 是针对所有 88 个字节计算得出的。
- **数据和 OTP 区域：**其内容按相应顺序连接以创建 CRC 算法的输入。

如果输入摘要与器件上计算的摘要不匹配，则会返回错误，此时应重复个性化过程。

表 8-20. 输入参数

	名称	大小	注
操作码	Lock	1	0x17。
Param1	Zone	1	**Bit 7：** 0 = 区域锁定时检查 CRC。 1 = 无论存储器的状态如何，都将忽略 CRC 的检查并锁定区域。Microchip 建议不要使用此模式。 **Bit 6-1：** 所有位必须为 0。 **Bit 0：** 0 = 配置区域 1 = 数据和 OTP 区域
Param2	Summary	2	指定区域的摘要，如果 Zone<7>置 1，则应为 0x0000。
数据	—	0	—

表 8-21. 输出参数

名称	大小	注
Success	1	成功执行后，ATSHA204A 将返回值 0。

8.5.11 MAC 命令

MAC 命令为存储在器件中的密钥、质询和器件上的其他信息计算 SHA-256 摘要。此命令的输出为此报文的摘要。如果报文包含器件的序列号，则此响应是“多样化的”。

使用此命令的正常命令流程如下所示：

1. 运行 Nonce 命令以加载输入质询，并视情况将其与生成的随机数组合。此操作的结果是在器件的 tempkey 内存储的一个临时值。
2. 视情况运行 GenDig 命令，将器件中的一个或多个存储 EEPROM 单元与临时值组合。结果存储在器件内部的 tempkey 中。此功能允许将 2 个或多个密钥用作响应生成的一部分。
3. 运行此 MAC 命令，将步骤 1（以及步骤 2，需要时）的输出与 EEPROM 密钥组合，以生成一个输出响应（或摘要）。

表 8-22. 输入参数

	名称	大小	注
操作码	MAC	1	0x08。
Param1	Mode	1	控制器件中的哪些字段用于报文。
Param2	SlotID	2	将用于生成响应的内部密钥。 Bit 3-0 仅用于选择一个槽，而 SHA-256 报文中将使用全部 16 位。
数据	质询	0 或 32	要提取摘要的报文的输入部分，Mode<0>为 1 时忽略。

表 8-23. 输出参数

名称	大小	注
Response	32	SHA-256 摘要。

使用 SHA-256 算法进行哈希运算的报文由以下信息组成：

32 字节	key<SlotID>或 TempKey（见下表）
32 字节	质询或 TempKey（见下表）
1 字节	操作码（始终为 0x08）
1 字节	Mode
2 字节	Param2
8 字节	OTP<0:7>或 0（见下表）
3 字节	OTP<8:10>或 0（见下表）
1 字节	SN<8>
4 字节	SN<4:7>或 0（见下表）
2 字节	SN<0:1>
2 字节	SN<2:3>或 0（见下表）

表 8-24. 模式编码

位	含义
7	必须为 0。
6	**0 =** 将对应于 SN<2:3>和 SN<4:7>的位设置为 0。 **1=** 报文中包含 48 位 SN<2:3>和 SN<4:7>。
5	如果 Mode<4>置 1，则此模式位的值将被忽略。 **0 =** 将相应 64 个 OTP 位设置为 0。 **1 =** 报文中包括前 64 个 OTP 位（OTP<0>至 OTP<7>）。
4	**0 =** 将相应 88 个 OTP 位设置为 0。 **1 =** 报文中包括前 88 个 OTP 位（OTP<0>至 OTP<10>）。
3	必须为 0。
2	如果 Mode<0>或 Mode<1>置 1，则 Mode<2>必须与 TempKey.SourceFlag 中的值相匹配，否则命令将返回错误。
1	**0=** SHA 报文的前 32 个字节从其中一个数据槽加载。 **1 =** 前 32 个字节用 TempKey 填充。
0	**0 =** SHA 报文的第 2 组 32 字节取自输入质询参数。 **1 =** 第 2 组 32 字节用 TempKey 中的值填充。建议将此模式用于所有用途。

8.5.12 Nonce 命令

Nonce 命令通过将内部生成的随机数与来自系统的输入值相组合来生成临时值，以供后续 GenDig、MAC、HMAC、Read 或 Write 命令使用。得到的临时值在内部存储到 TempKey 中，生成的随机数则返回到系统。

输入值设计为防止对主机进行重放攻击，且必须由系统外部生成并使用此命令传入器件。它可以是任何一个不断变化的值，例如非易失性计数器、当前的实时时间等，也可以是外部生成的随机数。

要为随后的加密命令提供一个临时值，需根据下列信息将输入数和输出随机数进行哈希运算。得到的摘要（临时值）始终存储在 TempKey 寄存器中，TempKey.Valid 置 1，并且 TempKey.SourceFlag 设置为“Rand”。临时值可由后续 GenDig、Read、Write、HMAC 或 MAC 命令使用，因此系统必须在外部计算此摘要值并将其存储在外部才能完成这些命令的执行。

或者，如果后续命令需要固定的临时值，也可以在直接传递模式下运行此命令。在这种情况下，输入值必须为 32 个字节长，并在不进行修改的情况下直接传送给 TempKey。不执行 SHA-256 计算，并将 TempKey.SourceFlag 设置为“Input”。TempKey 中的临时值可能不适用于 Read 或 Write 命令。如果在此模式下运行并且具有重复的输入数字值，则器件不会提供防止重放攻击的保护。

在配置区域锁定之前，RNG 会生成 32 字节值 0xFF FF 00 00 FF FF 00 00...以方便测试。此测试值以上述方式与输入值组合。

表 8-25. 输入参数

	名称	大小	注
操作码	Nonce	1	0x16。
Param1	Mode	1	控制内部 RNG 和种子更新的机制。
Param2	Zero	2	必须为 0x0000。
数据	NumIn	20,32	来自系统的输入值。

表 8-26. 输出参数

名称	大小	注
RandOut	1 或 32	RNG 的输出，如果 Mode<0:1>为 3，则为具有 0 值的单个字节。

如果 Mode<1:0>为 0b00 或 0b01，则输入 NumIn 参数的长度必须为 20 个字节，用于创建 TempKey 内部存储的临时值的 SHA-256 报文包含以下内容：

32 字节	RandOut
20 字节	来自输入流的 NumIn
1 字节	操作码（始终为 0x16）
1 字节	Mode
1 字节	Param2 的 LSb（应始终为 0x00）

完成此命令后，TempKey.SourceFlag 将设置为“Rand”。

如果 Mode<1:0>为 0b11，则此命令将在直接传递模式下运行，输入参数（NumIn）必须为 32 个字节长，TempKey 将加载 NumIn。不执行 SHA-256 计算，不会向系统返回数据，TempKey.SourceFlag 将设置为“Input”。

如果 Mode<1:0>为 0b01，则将抑制自动种子更新。有关更多详细信息，请参见**随机数发生器（RNG）**一节。Microchip 建议将 Mode<1:0>设置为 0b00 以实现最高安全性。

表 8-27. 模式编码

位	含义
7-2	必须为 0。
1-0	**00 =** 将新随机数与 NumIn 组合，存储到 TempKey 中。在随机数生成之前，仅在必要时自动更新 EEPROM 种子。建议采用此设置以获得最高安全性。 **01 =** 将新随机数与 NumIn 组合，存储到 TempKey 中。使用现有的 EEPROM 种子生成随机数，不更新 EEPROM 种子。 **10 =** 无效状态 **11 =** 在直接传递模式下运行，并将 NumIn 写入 TempKey。（应为 32 字节）。

8.5.13 Pause 命令

总线上配置 Selector 字节与输入 Selector 参数不匹配的所有器件都将进入空闲状态。此命令用于防止多个 ATSHA204A 器件共用同一总线的系统中出现总线冲突。

Pause 命令与空闲标志/序列的不同之处在于，单个引脚总线上的各个器件可以有选择地进入空闲状态，而空闲标志将导致总线上的所有 CryptoAuthentication 器件均进入空闲状态。

如果 EEPROM Selector 字节与输入 Selector 参数不匹配，则器件将立即进入空闲状态。如果输入 Selector 参数与配置 Selector 字节匹配，则器件将返回成功代码 0x00。

Pause 命令不能用于使器件进入休眠状态。

表 8-28. 输入参数

	名称	大小	注
操作码	Pause	1	0x01。
Param1	Selector	1	与此值不匹配的所有器件都将进入空闲状态。
Param2	Zero	2	必须为 0x0000。
数据	—	0	—

表 8-29. 输出参数

名称	大小	注
Success	1	如果命令指示某个其他器件应空闲，则 ATSHA204A 将返回值 0x00。 如果此器件进入空闲模式，则不返回任何值。

8.5.14 Random 命令

Random 命令生成一个随机数，以供系统使用。

随机数由硬件 RNG 的输出和存储在 EEPROM 或 SRAM 中的内部种子值的组合生成。生成随机数（Nonce 或 Random 命令的执行过程的一部分）之前，外部系统可以选择更新内部存储的 EEPROM 种子值。为实现最高安全性，Microchip 建议始终更新 EEPROM 种子。

Random 命令不提供将输入数与内部存储的种子集成的机制。如果需要此功能，则系统应使用 Nonce 命令并忽略生成的临时值。

在配置区域锁定之前，RNG 会生成 32 字节值 0xFF, 0xFF, 0x00, 0x00, 0xFF, 0xFF, 0x00, 0x00...以方便测试。

Nonce 和 Random 命令使用相同的内部存储种子。必要时，使用 Mode<0>以确保更新 EEPROM。

表 8-30. 输入参数

	名称	大小	注
操作码	Random	1	0x1B。
Param1	Mode	1	控制内部 RNG 和种子更新的机制。
Param2	Zero	2	必须为 0x0000。
数据	—	0	—

表 8-31. 输出参数

名称	大小	注
RandOut	32	RNG 的输出。

表 8-32. 模式编码

位	含义
7-1	必须为 0。
0	0 = 在随机数生成之前，仅在必要时自动更新 EEPROM 种子。 建议采用此设置以获得最高安全性。 1 = 使用现有的 EEPROM 种子生成随机数；不更新 EEPROM 种子。

8.5.15 Read 命令

Read 命令从器件的一个存储区域读取字（一个 4 字节字或一个 32 字节的 8 字块）。数据可以在返回到系统之前选择性地进行加密。有关数据区域字节和字寻址的信息，请参见 **EEPROM 数据区域**一节。

如果读取 SlotConfig.EncryptRead 置 1 的槽，GenDig 命令必须在执行此命令之前已运行，才能生成供加密使用的密钥。如果槽编号是偶数，或者，如果对应于此槽的 CheckMacSource 位为 0，则 GenDig 的输入临时值必须是随机数。最后，GenDig 计算中必须已使用 SlotConfig.ReadKey 中指定的密钥。

器件通过将从 EEPROM 中读取的每个字节与来自 TempKey 的相应字节进行异或运算来加密要读取的数据。不允许对配置区域和/或 OTP 区域进行加密读取。

在传送到器件之前，要读取的字节地址应除以 4（丢弃低 2 位）。如果正在读取 32 个字节，则将忽略输入地址的低 3 位。如果地址超出指定区域的末尾，则将导致错误。

以下限制适用于下列三个区域：

- **数据**
  如果数据区域解锁，则此命令将返回错误；否则，相应的 SlotConfig 字中的值将用于控制对数据槽的访问。如果 SlotConfig.IsSecret 置 1 并尝试四字节读取操作，则器件将返回错误。如果

EncryptRead 置 1，则此命令将按照上述内容加密数据。如果 IsSecret 置 1 且 EncryptRead 清零，则此命令将返回错误。如果 IsSecret 清零且 EncryptRead 清零，则此命令将明文返回所需槽。

- **配置**

  无论 LockConfig 的值如何，此区域中的字始终可使用此命令读取。

- **OTP**

  如果 OTP 区域解锁，则此命令将返回错误。锁定后，如果 OTP 模式未设置为传统模式，则可读取所有字。如果 OTP 模式为传统模式，则只允许四字节读取操作，而 0 或 1 的地址将返回错误。

表 8-33. 输入参数

	名称	大小	注
操作码	Read	1	0x02
Param1	Zone	1	**Bit 7：** 0 = 读取 4 字节。 1 = 读取 32 字节。在传统模式下，从 OTP 区域读取时必须为 0。 **Bit 6-2：** 所有位必须为 0。 **Bit 1-0：** 在 Config、OTP 或 Data 中进行选择。请参见区域编码一节。
Param2	Address	2	区域内要读取的第一个字的地址。请参见地址编码一节。
数据	—	0	—

表 8-34. 输出参数

名称	大小	注
Contents	4 或 32	指定存储单元的内容。

8.5.15.1 数据区域中的读操作

数据区域中的读操作由 IsSecret 和 EncryptRead 的状态决定，如下表所示：

表 8-35. 读操作权限

IsSecret	EncryptRead	说明
0	0	始终允许从此槽进行明文读取。 设置为此状态的槽始终不应用来存储密钥。一 次可以读取 4 个或 32 个字节。
0	1	禁止。使用此代码的槽不能保证安全性。
1	0	始终不允许从此槽进行读取。 设置为此状态的槽仍可用来存储密钥。
1	1	从此槽中读取的内容使用 Read 命令描述（见 **Read 命令**一节）中记录的加密算法进行加密。 加密密钥位于由 ReadKey 指定的槽中。禁止 4 字节读写操作。

如果读取数据区域并且相应 SlotConfig 字中的 EncryptRead 位置 1，则会采取以下操作来加密数据：

- 所有的 TempKey 寄存器位必须按如下正确设置，否则此命令将返回错误：

```
TempKey.Valid == 1

TempKey.GenData == 1
```

```
TempKey.SlotID == SlotConfig.ReadKey
```

- 如果读取的槽编号是偶数，则 TempKey.SourceFlag 必须为“RAND”。
- 如果槽编号是奇数，则 TempKey.SourceFlag 必须与槽对应的 Config.CheckMacSource 中的值匹配。
- 将存储区域内的数据与 TempKey 进行异或运算。以“Contents”形式返回。

8.5.16 SHA 命令

SHA 命令用于计算系统通用的 SHA-256 摘要。可容纳任何报文长度。系统负责基于最后一个块发送填充字节和长度字节。
摘要的计算分以下两个步骤：

1. **初始化**
   通过用初始化常量覆盖 TempKey 的当前值来设置 SHA-256 计算引擎。强制 TempKey 标志匹配在 Nonce(Fixed) 命令后所处的状态。此模式不接受任何报文字节。
2. **计算**
   在此模式下，可通过多次调用命令为报文添加字节。此模式的每次迭代都必须包含 64 字节的报文。输出缓冲区始终包含摘要，必要时可忽略。此摘要还被载入 TempKey 中。

SHA(Init) 命令必须先运行，然后才能接受 SHA(Compute) 命令。系统可根据需要运行多个 SHA(Compute) 命令来计算所需摘要。如果在“Init”迭代和最后一个“Compute”迭代之间运行除 SHA 之外的任何命令，则会返回错误。如果 Mode 字节的值不是 0x00 或 0x01，则此命令还返回一个解析错误。

如果器件进入休眠模式或看门狗定时器超时，则存储在 TempKey 中的中间摘要将失效。系统软件必须确保在单个唤醒/看门狗时间间隔内将整个报文发送到器件，或确保在 SHA 命令之间插入合适的空闲序列。

表 8-36. 输入参数

	名称	大小	注
操作码	SHA	1	0x47
Param1	Mode	1	**Bit 7-1：** 必须为 0。 **Bit 0：** 0 =（初始化）：使用 SHA-256 的初始化值加载 TempKey。不接受任何报文字节（长度必须为 0）。 1 =（计算）：将报文参数中的 64 个字节添加到 SHA 上下文中并返回摘要。
Param2	Param2	2	必须为 0x0000。
数据	Message	0 或 64	要包含在哈希运算中的 64 字节数据。如果 Mode<0>为 0，则忽略。

表 8-37. 输出参数

名称	大小	注
Response	1 或 32	Mode<0> = 1 时，为 SHA-256 摘要；否则为 0x00（成功时）或错误代码。

8.5.17 UpdateExtra 命令

UpdateExtra 命令用于在配置区域锁定后更新配置区域内的 2 个额外字节（存储单元 84 和 85）的值。它还可用于在适当的情况下快速递减与密钥相关联的使用计数器。

如果 Mode<1>置 1，则此命令会使可能与特定密钥相关联的有限使用计数器实现快速递减。如果“NewValue”参数指定的槽不包含实现或使能了有限使用的密钥，则此命令将以静默方式返回而不采取

任何操作。如果指示的槽包含一个没有剩余使用次数的有限使用密钥，则此命令将返回错误；否则，其中的一个剩余使用次数位将清零。此命令不会修改相关槽的 Config.UpdateCount。

如果模式参数指示地址 84 处的 UserExtra：

- 如果 UserExtra（配置区域的字节 84）中的当前值为 0，则 UpdateExtra 将向此字节写入 NewValue 的 LS 字节并返回成功信息。
- 如果 UserExtra 中的当前值不为 0，则此命令将返回执行错误。

如果模式参数指示地址 85 处的 Selector：

- 如果 SelectorMode（配置区域的字节 19）不为 0 并且 Selector（配置区域的字节 85）为 0，则此命令将向 Selector 写入 NewValue 的 LSB 并返回成功信息。写入非零值后，将会被锁定，无法进一步更新。
- 如果 SelectorMode 的值为 0，则表示不应检查当前 Selector，此命令将始终更新 Selector 并且始终成功。

表 8-38. 输入参数

	名称	大小	注
操作码	UpdateExtra	1	0x20。
Param1	Mode	1	**Bit 7-2：** 必须为 0。 **Bit 1：** 0 =更新配置字节 84 或 85 1 =忽略 bit 0，使与“NewValue”槽中的密钥相关的限制使用计数器递减。 **Bit 0：** 如果为 0，则更新配置字节 84。 如果为 1，则更新配置字节 85。
Param2	NewValue	2	**LSB：** 可选择性写入配置区域中的存储单元 84 或 85 的值。 **MSB：** 必须为 0x00。
数据	—	0	—

表 8-39. 输出参数

名称	大小	注
Success	1	如果存储器字节已更新，则此命令将返回值 0x00；否则，它将返回执行错误。

8.5.18 Write 命令

Write 命令向器件上的一个 EEPROM 区域写入一个 4 字节字或一个 32 字节的 8 字块。根据此槽的 WriteConfig 字节的值，数据发送到器件之前可能需要由系统进行加密。

以下限制适用于使用此命令向区域内写入的情况：

- **数据区域**：如果配置区域锁定且数据区域解锁，则所有区域中的所有字节都可以通过 32 字节写操作用纯文本或加密数据写入。数据区域锁定后，WriteConfig 字节中的值控制对数据槽的访问。如果此槽的 WriteConfig 位设置为“始终”，则输入数据应明文传送到器件。如果 SlotConfig<14>设置为 1，则应加密输入数据并计算输入 MAC。

- **配置区域**：如果配置区域锁定或 Zone<6>置 1，则此命令将返回错误；否则字节将按要求写入。如果尝试写入任何永久禁止写操作的字节（见 **EEPROM 数据区域**一节），则会导致命令错误，而不对 EEPROM 进行任何修改。
- **OTP 区域**：如果 OTP 区域解锁，则所有字节均可使用此命令写入。如果 OTP 区域锁定并且 OTPmode 字节为只读或传统模式，则此命令将返回错误；否则，OTP 模式应为消耗模式并且此命令会将 OTP 区域中对应于输入参数值中 0 位的位设置为 0。当 OTP 区域锁定时，无论 OTP 模式如何，始终不允许对其执行加密写操作。

只有以下四个条件均满足时，数据区域和 OTP 区域中才允许进行 4 字节写操作：

- SlotConfig.IsSecret 必须为 0。
- SlotConfig.WriteConfig 必须为“始终”。
- 输入数据不能加密。
- 数据/OTP 区域必须锁定。

在所有其他情况下，4 字节写操作均会返回错误。

Param2 的低 3 位（Address<2:0>）表示块内的字，如果写入整个 32 字节块，则它们将被忽略。Address<6:3>包含写入数据区域的槽编号或配置区域和 OTP 区域的块编号。如果地址值超出指定区域的大小，则将导致命令返回错误。

如果尝试在配置区域锁定之前写入 OTP 和/或数据区域，则将导致器件返回错误代码。

8.5.18.1 输入数据加密

可通过加密输入数据防止个性化或系统操作期间在总线上发生侦听。系统应通过将纯文本与 TempKey 中的当前值进行异或运算来加密数据。接收后，器件将使输入数据与 TempKey 进行异或运算，以在写入 EEPROM 之前恢复纯文本。

只要加密输入数据，在写入输入区域时就始终需要授权输入 MAC。此 MAC 的计算如下：

SHA-256（TempKey，操作码，Param1，Param2，SN<8>，SN<0:1>，<25 个字节的 0>，PlainTextData）

在锁定 OTP/数据区域之前，Zone<6>用于向器件指示输入数据是否加密。在锁定 OTP/数据区域之后，将忽略 Zone<6>，并且仅使用对应于所写入槽的 SlotConfig<14>来确定输入数据是否加密。

如果指示了数据加密，则在调用此命令之前，TempKey 必须有效，且必须是 `GenDig` 的结果。具体来说，这意味着 TempKey.Valid 和 TempKey.GenDig 都必须设置为 1。在数据锁定之前，可以使用任何密钥来生成 TempKey。锁定后，存储在 TempKey.SlotID 中且由 `GenDig` 用来创建 TempKey 的最后一个槽必须与 SlotConfig.WriteKey 中的槽相匹配。如果写入的槽编号是偶数，则 TempKey.SourceFlag 必须为“RAND”。如果槽编号是奇数，则 TempKey.SourceFlag 必须与槽对应的 Config.CheckMacSource中的值匹配。

表 8-40. 输入参数

	名称	大小	注
操作码	Write	1	0x12

.....（续）

	名称	大小	注
Param1	Zone	1	**Bit 7：** 0 = 4 字节数据写入指定的区域。 1 = 32 字节数据写入指定的区域。 **Bit 6：** 0 = 数据以明文写入。 1 = 输入数据必须加密。 如果数据/OTP 区域锁定，则必须为 0。 **Bit 5-2：** 必须为 0。 **Bit 1-0：** 在 Config、OTP 或 Data 中进行选择。请参见区域编码一节。
Param2	Address	2	区域内要写入的第一个字的地址。请参见地址编码一节。
Data_1	Value	4 或 32	要写入区域的信息；可进行加密。
Data_2	Mac	0 或 32	用于使地址和数据生效的报文验证代码。

表 8-41. 输出参数

名称	大小	注
Success	1	成功完成后，ATSHA204A 将返回值 0x00。

9. 兼容性

ATSHA204A 经过专门设计，可与 ATSHA204 完全兼容，适用于所有主机、客户端和个性化操作。请注意对 ATSHA204A 进行的以下重要改进：

- 有功功耗较低。
- 支持两线连接模式，无需外部二极管。
- 新的 SHA 命令允许对 SHA 摘要进行一般计算，而无需主机中的加密软件。
- 在个性化过程中的写操作始终要求将 MAC 传送至器件，以防中间人攻击。（某些版本的 ATSHA204 在数据区域解锁的条件下忽略了写操作时的 MAC。）
- UpdateExtra 命令现可用于在需要多步计数时快速递减限制使用计数器。
- CheckMac 命令的副本模式现可使用固定临时值运行，这简化了受保护安全启动验证和其他相关任务的实现。
- OTP 区域的新消耗模式提供了额外的使用情况跟踪功能。
- 当配置区域锁定且 OTP 区域和数据区域解锁时，对 OTP 区域或数据区域进行的写操作需要 32 个字节。对于此锁定状态，ATSHA204 允许 4 字节 Write 命令。

10. 机械信息

10.1 引脚分配

此器件提供多种封装：

- 8 焊点 UDFN
- 3 引脚 SOT23
- 8 引脚 SOIC
- 8 引脚 TSSOP（注）
- 3 引脚触点式，用于机械、非焊接式连接。

引脚分配如下：

表 10-1. 封装引脚分配

名称	3 引脚 SOT23	8 引脚 SOIC、8 引脚 TSSOP（注）和 8 焊点 UDFN	3 引脚触点式
SDA	1	5	1
SCL	—	6	—
V_{CC}	2	8	3
GND	3	4	2
NC	—	1、2、3 和 7	—

注： 不建议用于新产品设计。

11. 封装标识信息

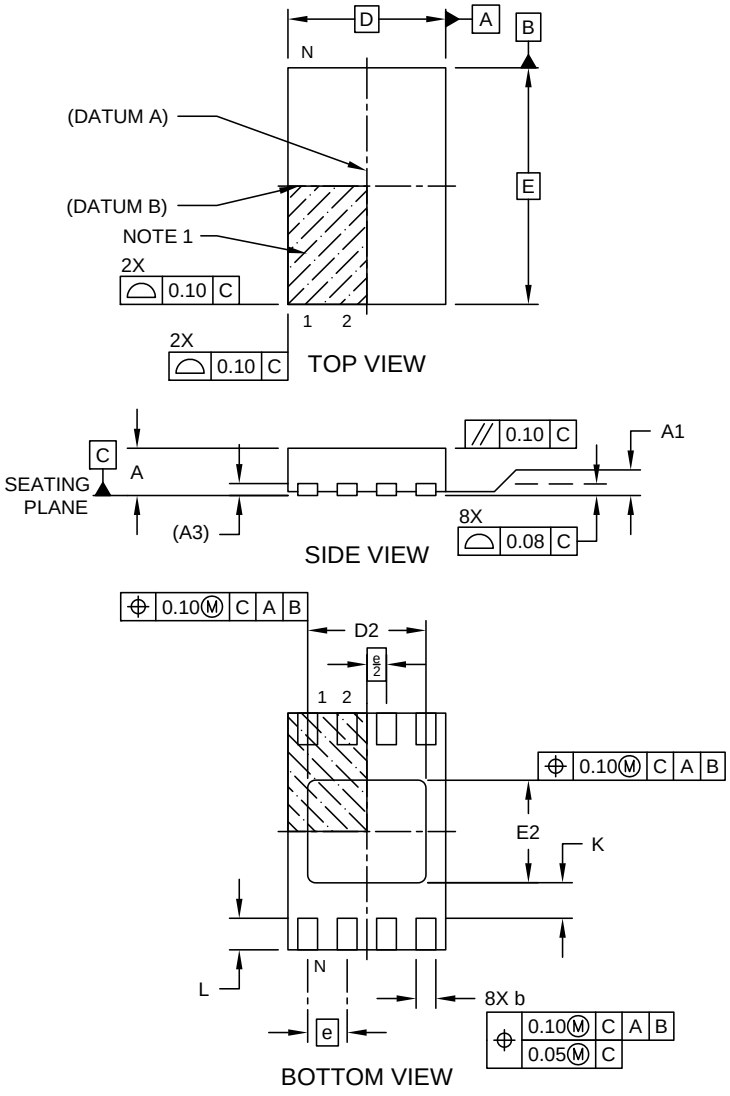
作为 Microchip 整体安全功能的一部分，所有加密器件的器件标识都有意进行了模糊处理。封装顶部的标识不提供有关器件的实际类型或制造商的任何信息。封装上的字母数字代码提供制造信息，并随装配批次变化。封装标识不应作为即将进行的任何检查步骤的一部分。

12. 封装图

12.1 8 焊点 UDFN

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

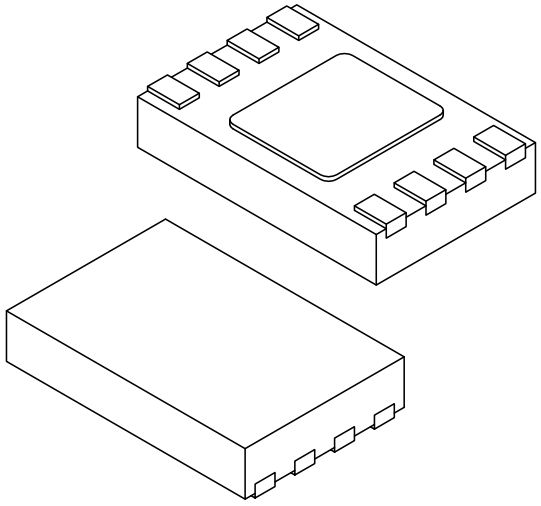
Note:	For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



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:

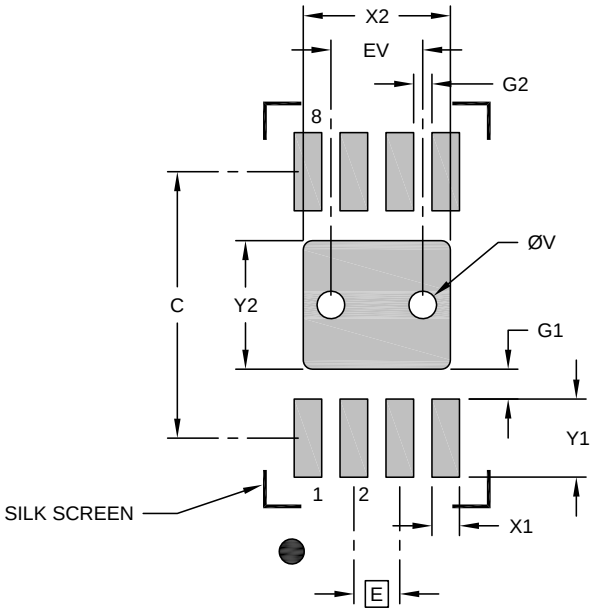
1. Pin 1 visual index feature may vary, but must be located within the hatched area.
2. Package is saw singulated
3. Dimensioning and tolerancing per ASME Y14.5M

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:

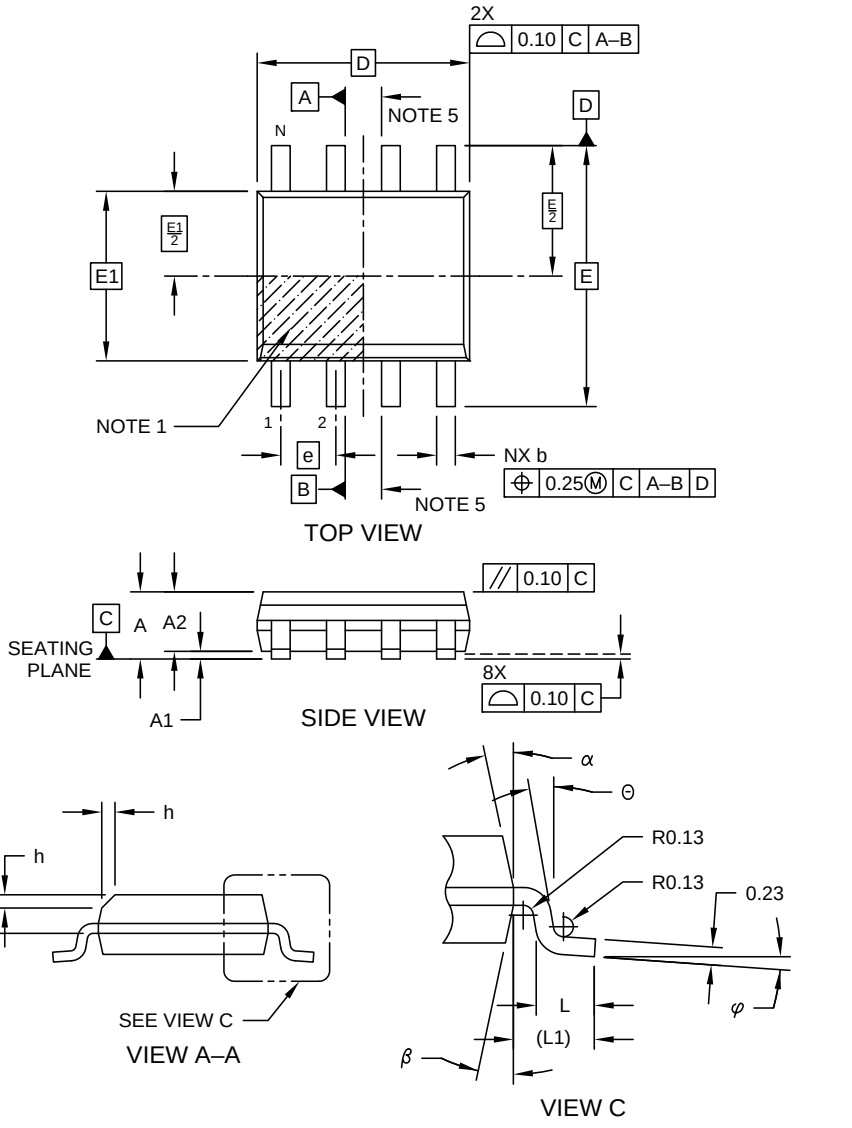
1. Dimensioning and tolerancing per ASME Y14.5M
   BSC: Basic Dimension. Theoretically exact value shown without tolerances.
2. For best soldering results, thermal vias, if used, should be filled or tented to avoid solder loss during reflow process

Microchip Technology Drawing C04-21355-Q4B Rev A

12.2 8 引脚 SOIC

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

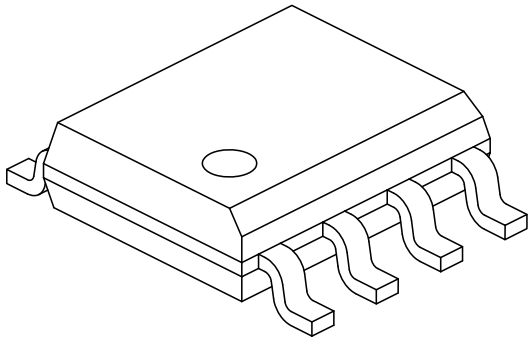
Note:	For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



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°

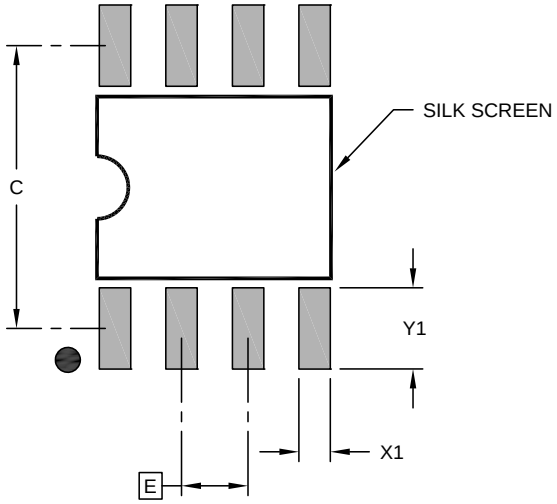
Notes:

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:

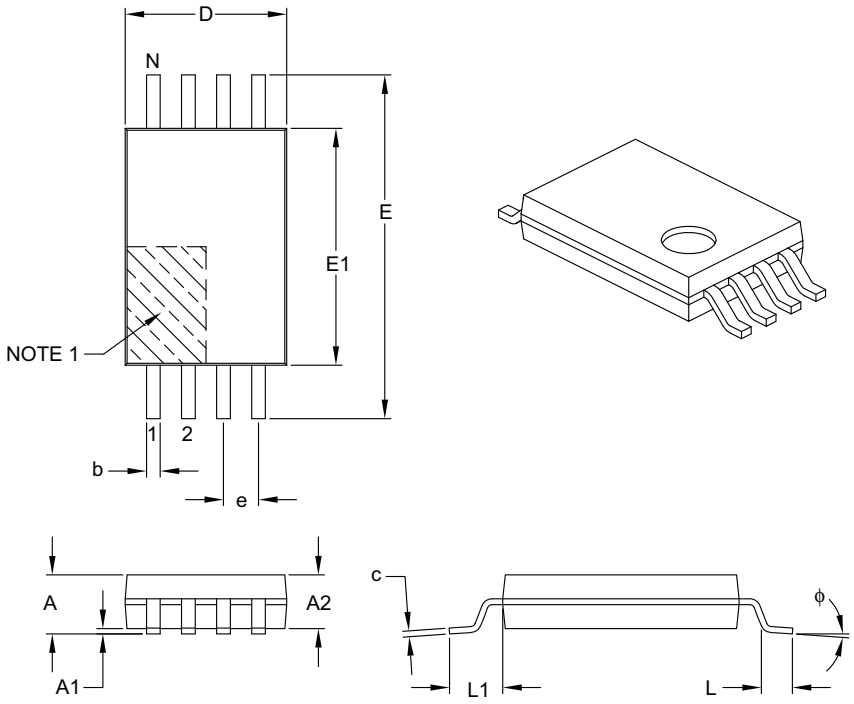
1. Dimensioning and tolerancing per ASME Y14.5M
   BSC: Basic Dimension. Theoretically exact value shown without tolerances.

Microchip Technology Drawing C04-2057-M6B Rev B

12.3 8 引脚 TSSOP

8-Lead Plastic Thin Shrink Small Outline (ST) – 4.4 mm Body [TSSOP]

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



Unit		MILLIMETERS		
Dimension Limits		MIN	NOM	MAX
Number of Pin	N		8	
Pitch	e		0.65 BSC	
Overall Height	A	–	–	1.20
Molded Package Thickness	A2	0.80	1.00	1.05
Standoff	A1	0.05	–	0.15
Overall Width	E		6.40 BSC	
Molded Package Width	E1	4.30	4.40	4.50
Molded Package Length	D	2.90	3.00	3.10
Foot Length	L	0.45	0.60	0.75
Footprint	L1		1.00 REF	
Foot Angle	ϕ	0°	–	8°
Lead Thickness	c	0.09	–	0.20
Lead Width	b	0.19	–	0.30

Notes:

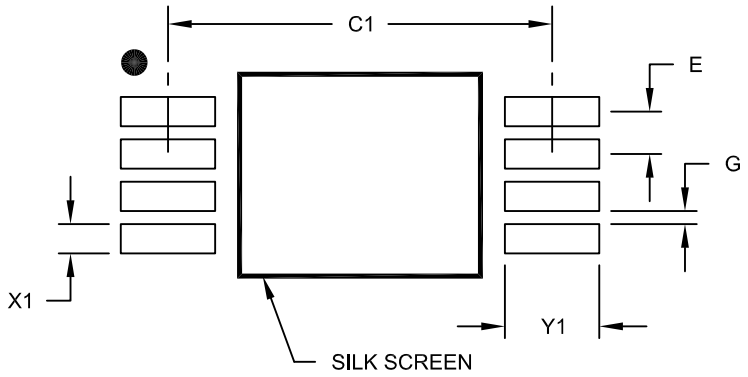
1. Pin 1 visual index feature may vary, but must be located within the hatched area.
2. Dimensions D and E1 do not include mold flash or protrusions. Mold flash or protrusions shall not exceed 0.15 mm per side.
3. Dimensioning and tolerancing per ASME Y14.5M.

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

Microchip Technology Drawing C04-086B

8-Lead Plastic Thin Shrink Small Outline (ST) - 4.4 mm Body [TSSOP]

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		0.65 BSC	
Contact Pad Spacing	C1		5.90	
Contact Pad Width (X8)	X1			0.45
Contact Pad Length (X8)	Y1			1.45
Distance Between Pads	G	0.20		

Notes:

1. Dimensioning and tolerancing per ASME Y14.5M

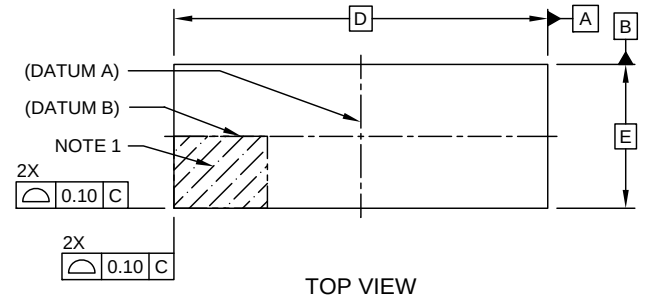
BSC: Basic Dimension. Theoretically exact value shown without tolerances.

Microchip Technology Drawing No. C04-2086A

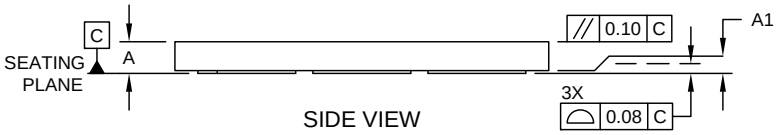
12.4 3 引脚触点式

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

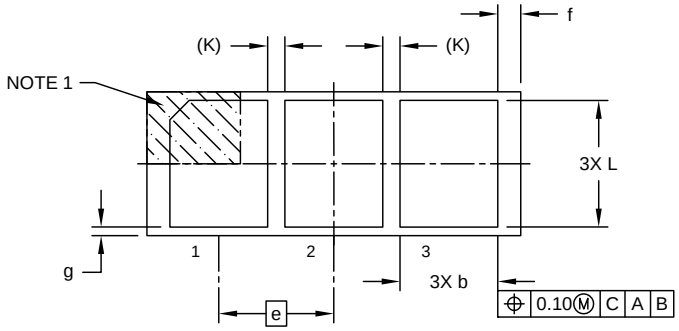
Note:	For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



TOP VIEW



SIDE VIEW

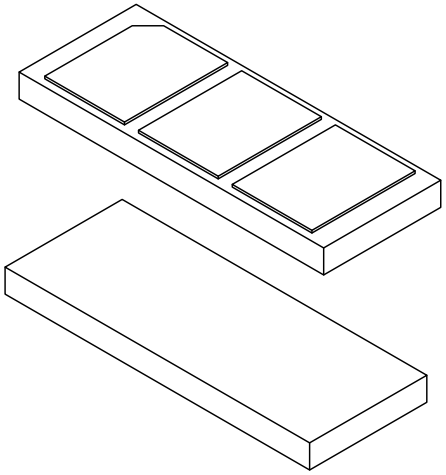


BOTTOM VIEW

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:

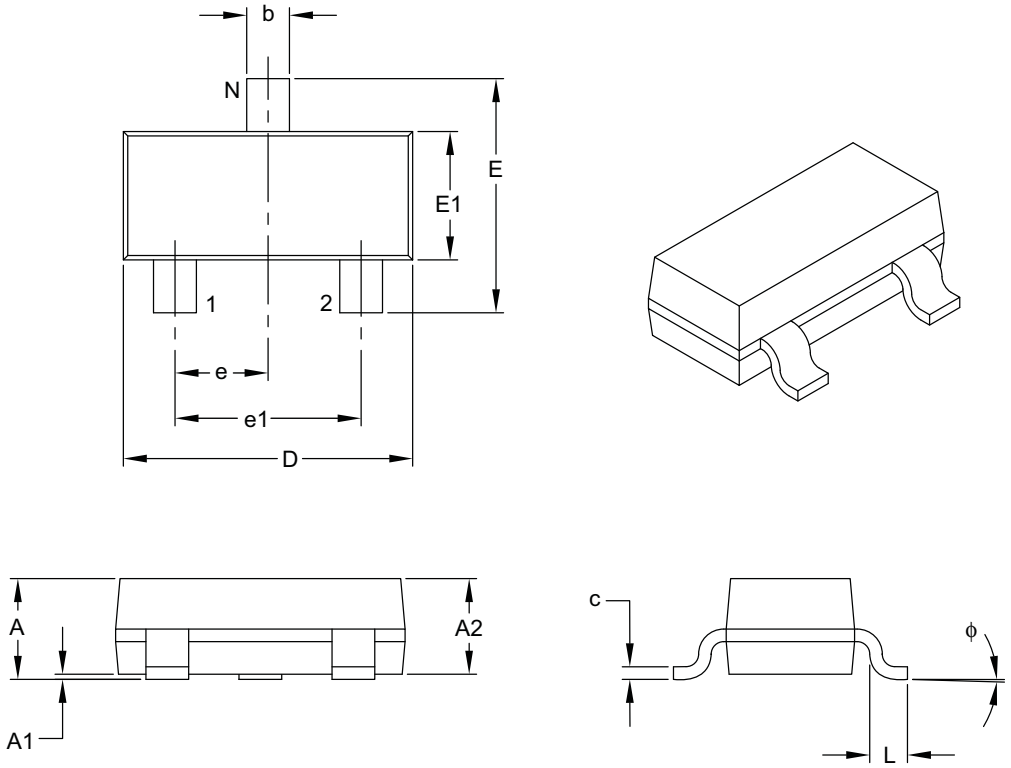
1. Pin 1 visual index feature may vary, but must be located within the hatched area.
2. Dimensioning and tolerancing per ASME Y14.5M
   BSC: Basic Dimension. Theoretically exact value shown without tolerances.
   REF: Reference Dimension, usually without tolerance, for information purposes only.

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

12.5 3 引脚 SOT23

3-Lead Plastic Small Outline Transistor (NB) [SOT-23]

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		3	
Lead Pitch	e		0.95 BSC	
Outside Lead Pitch	e1		1.90 BSC	
Overall Height	A	0.89	–	1.12
Molded Package Thickness	A2	0.79	0.95	1.02
Standoff	A1	0.01	–	0.10
Overall Width	E	2.10	–	2.64
Molded Package Width	E1	1.16	1.30	1.40
Overall Length	D	2.67	2.90	3.05
Foot Length	L	0.13	0.50	0.60
Foot Angle	ϕ	0°	–	10°
Lead Thickness	c	0.08	–	0.20
Lead Width	b	0.30	–	0.54

Notes:

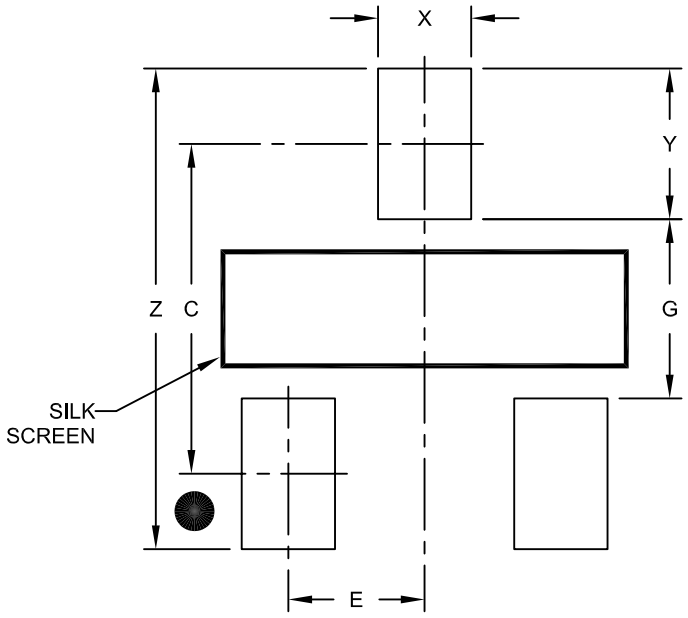
1. Dimensions D and E1 do not include mold flash or protrusions. Mold flash or protrusions shall not exceed 0.25 mm per side.
2. Dimensioning and tolerancing per ASME Y14.5M.

BSC: Basic Dimension. Theoretically exact value shown without tolerances.

Microchip Technology Drawing C04-104B

3-Lead Plastic Small Outline Transistor (NB) [SOT-23]

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	0.95 BSC		
Contact Pad Spacing	C		2.30	
Contact Pad Width (X3)	X			0.65
Contact Pad Length (X3)	Y			1.05
Distance Between Pads	G	1.25		
Overall Width	Z			3.35

Notes:

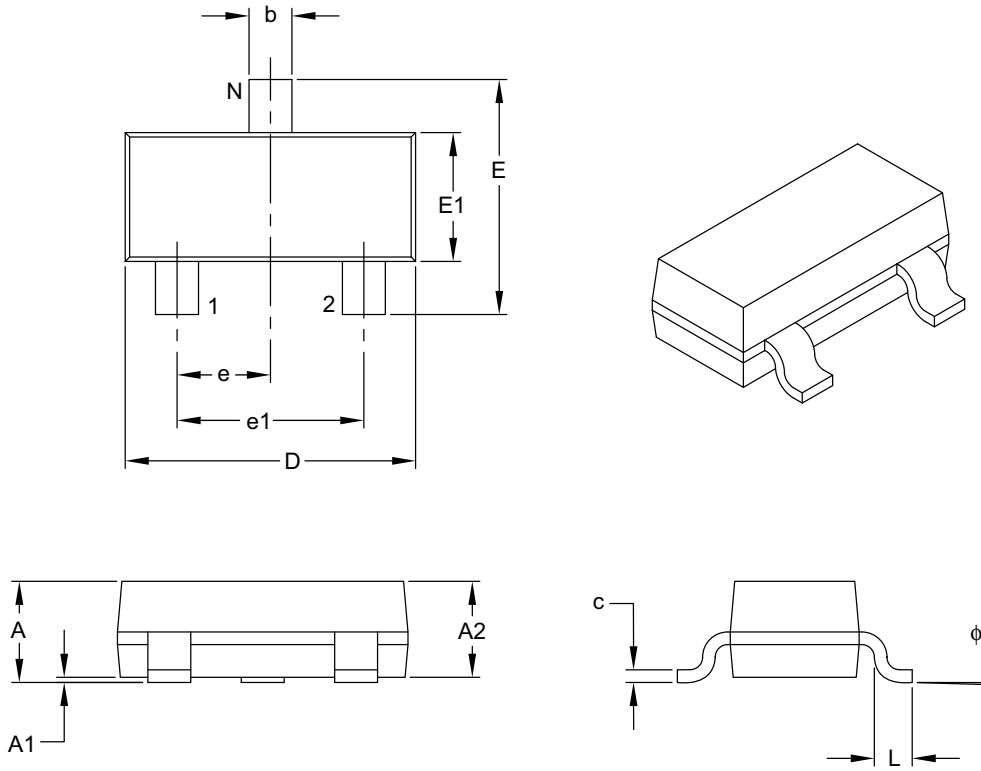
1. Dimensioning and tolerancing per ASME Y14.5M

BSC: Basic Dimension. Theoretically exact value shown without tolerances.

Microchip Technology Drawing No. C04-2104A

3-Lead Plastic Small Outline Transistor (TT) [SOT-23]

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



Unit		MILLIMETERS		
Dimension Limits		MIN	NOM	MAX
Number of Pin	N		3	
Lead Pitch	e		0.95 BSC	
Outside Lead Pitch	e1		1.90 BSC	
Overall Height	A	0.89	–	1.12
Molded Package Thickness	A2	0.79	0.95	1.02
Standoff	A1	0.01	–	0.10
Overall Width	E	2.10	–	2.64
Molded Package Width	E1	1.16	1.30	1.40
Overall Length	D	2.67	2.90	3.05
Foot Length	L	0.13	0.50	0.60
Foot Angle	ϕ	0°	–	10°
Lead Thickness	c	0.08	–	0.20
Lead Width	b	0.30	–	0.54

Notes:

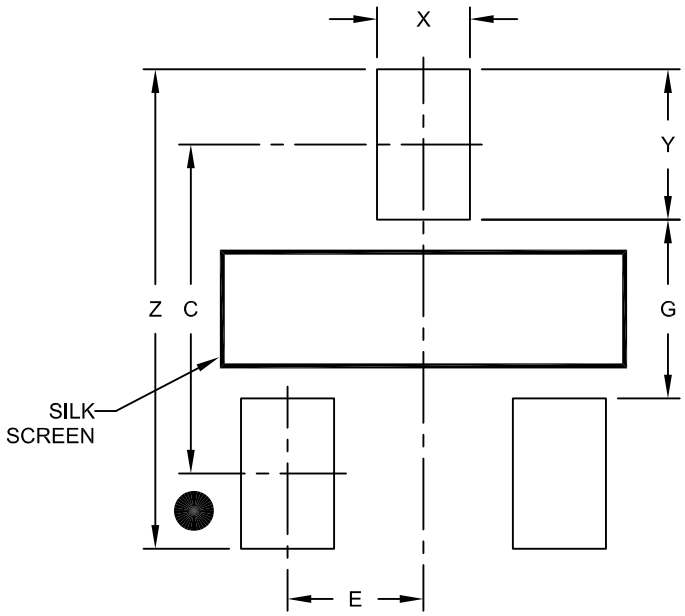
1. Dimensions D and E1 do not include mold flash or protrusions. Mold flash or protrusions shall not exceed 0.25 mm per side.
2. Dimensioning and tolerancing per ASME Y14.5M.

BSC: Basic Dimension. Theoretically exact value shown without tolerances.

Microchip Technology Drawing C04-104B

3-Lead Plastic Small Outline Transistor (TT) [SOT-23]

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		0.95 BSC	
Contact Pad Spacing	C		2.30	
Contact Pad Width (X3)	X			0.65
Contact Pad Length (X3)	Y			1.05
Distance Between Pads	G	1.25		
Overall Width	Z			3.35

Notes:

1. Dimensioning and tolerancing per ASME Y14.5M

BSC: Basic Dimension. Theoretically exact value shown without tolerances.

Microchip Technology Drawing No. C04-2104A

13. 参考和应用笔记

ATSHA204A 使用 SHA-256 或 HMAC/SHA-256 实现了质询-响应协议，详细信息如下所述。响应始终是一个 256 位摘要。

Nonce 命令（见 **Nonce 命令**一节）接受来自系统的输入质询，并视情况将其与内部生成的随机数组合，以生成用于计算的临时值（例如，仅使用一次的数字）。此组合为种子，随后与一个机密信息密钥组合，共同作为任一加密命令（例如，MAC、HMAC、Read、Write 或 GenDig）的认证计算的一部分。输入质询也可直接传送至 MAC 命令。

只有当器件在计算中包含其 RNG 的输出时，器件才能保证临时值的惟一性；这是因为系统输入可能惟一，也可能不惟一。与之前的所有临时值相比，每个随机临时值实际上都保证具有惟一性，以便确保每个事务始终惟一。

13.1 SHA-256

ATSHA204A MAC 命令计算与质询或临时值连接的密钥的摘要。它可以视情况包含报文摘要中存储在器件上的各种其他信息片段。

ATSHA204A 根据以下网址记录的算法计算 SHA-256 摘要：

http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf

命令描述中针对使用此算法的每个命令列出 ATSHA204A 处理的完整 SHA-256 报文。此算法的大多数标准软件实现自动将适当数量的填充和长度位添加到此报文，以匹配器件在内部执行的操作。

ATSHA204A 还可使用 SHA 命令计算 SHA-256 摘要。调用程序负责将填充字节和长度字节发送至报文。报文大小必须是 64 字节的倍数，包括填充字节。

SHA-256 算法用于加密，方法是将哈希算法的输出摘要与纯文本数据进行异或运算以生成密文。解密是反向操作，即密文与摘要进行异或运算来生成纯文本。

13.2 HMAC/SHA-256

对质询的响应也可以使用 HMAC 算法基于以下网址记录的 SHA-256 来计算：

http://csrc.nist.gov/publications/fips/fips198/fips-198a.pdf

由于计算复杂度增加，HMAC 命令不如 MAC 命令灵活，HMAC 的计算时间有所延长。虽然 HMAC 序列对于确保摘要的安全性不是必需的，但是为了与各种软件包兼容，仍将其包括在内。

13.3 密钥值

SHA204A 中的所有密钥的长度均为 256 位。ATSHA204A 使用这些密钥作为报文的一部分，这类报文使用 MAC、CheckMac、HMAC 和 GenDig 命令进行哈希运算。EEPROM 数据区域中的任一槽均可用于存储密钥，但只有在 SlotConfig（包括 IsSecret 位）内正确设置了读写权限时，相应值才是加密的。

除了 GenDig 命令，在确定密钥数据的源时，都将忽略除 SlotID 参数的低 4 位之外的所有内容。仅使用低 4 位来选择数据区域的一个槽。有关 GenDig 如何使用其他 SlotID 值的信息，请参见**传输密钥**一节。

在使用 Param2 执行 SHA-256 计算的所有情况下，整个 16 位 SlotID 都将作为输入包含在报文中。

13.3.1 多样化密钥

如果主机或验证实体有能够安全存储密钥的位置，则可通过使用嵌入在器件中的序列号（SN<0:8>）对 EEPROM 槽中存储的密钥值实现多样化。凭借这种方式，每个客户端器件均可获得惟一密钥，此密钥可提供针对已知明文攻击的额外保护，能够将遭到破坏的序列号识别出来并列入黑名单。

为了实现此操作，需使用某种加密算法在个性化过程中将根机密信息与器件序列号外部组合，并将结果写入 ATSHA204A 密钥槽。

ATSHA204A `CheckMac` 命令提供了一种机制，能够安全地生成和比较多样化密钥，从而消除主机系统的这种要求。

有关详细信息，请参见以下应用笔记：

http://ww1.microchip.com/downloads/en/appnotes/doc8666.pdf

13.3.2 滚动密钥

为避免重复使用相同的密钥值，ATSHA204A 支持密钥滚动。通常情况下，使用一定次数（可能只有一次）后，当前密钥值将替换为其当前值与一些偏移量组合后的 SHA-256 摘要，可能是一个常数、与当前系统有关的事物（例如，序列号或型号）或随机数。

此功能通过使用 `DeriveKey` 命令实现。在执行 `DeriveKey` 命令之前，必须运行 `Nonce` 命令以将偏移量加载到 TempKey 中。每次在槽 0 到槽 7 上执行滚动操作时，此槽的 UpdateCount 字段都将递增。

此功能的一个用途是永久删除器件中的原始密钥，并将其替换为仅在特定环境中有用的密钥。在密钥发生滚动之后，没有办法获取旧值，这提高了系统的安全性。

如果在滚动模式下执行 `DeriveKey` 命令时发生电源中断，则可能导致密钥或 UpdateCount 具有未知值。如果使用 SlotConfig 的 bit 14 使能槽写入操作，则可以通过 `Write` 命令以加密和验证格式写入这些密钥。或者，也可以将密钥的多个副本存储在多个槽中，以防单个槽的故障使系统无法工作。

13.3.3 创建的密钥

为支持每个客户端的惟一临时密钥，ATSHA204A 还支持密钥创建。利用这种机制，“父”密钥（由 slotConfig.writeKey 指定）可与固定值或随机阵列组合创建一个惟一密钥，以随后用于任何加密目的。

如果父密钥存在使用限制，则创建惟一密钥的功能尤其有用（见下面的 13.3.4 节**有限使用的密钥**和 13.3.5 节**有限使用的密钥（编号 15）**）。在此模式下，可以使用有限使用的父密钥来创建无限制使用的子密钥。因为子密钥只对此特定主机-客户端对有用，所以对其值的攻击价值不大。

此功能也可通过使用 `DeriveKey` 命令实现。在执行 `DeriveKey` 命令之前，必须通过运行 `Nonce` 命令将临时值加载到 TempKey 中。每次在槽 0 到槽 7 上执行创建操作时，此槽的 UpdateCount 字段都将递增。

13.3.4 有限使用的密钥

对于与 EEPROM 数据部分中的槽 0 至 7 对应的 SlotID 值，可以严格限制存储在槽中的密钥的重复使用。如果 SlotConfig 字段中的 LimitedUse 位置 1，则使能此功能。对于槽 8 到 14，将忽略 LimitedUse 位。剩余使用次数作为一个位映射存储在对应于相关槽的 UseFlag 字节中。

在执行任何使用此槽作为密钥的加密命令之前，会出现以下情况：

- 如果 SlotConfig<SlotID>.LimitedUse 置 1 且 UseFlag<SlotID>为 0x00，则器件会返回错误。
- 从 UseFlag<SlotID>的 bit 7 起，将第一个当前为 1 的位清零。

实际上，此过程允许 LimitedUse 密钥在每次使用 DeriveKey 命令执行“刷新”之前使用八次。对于引用使能了此功能的密钥的任何命令，如果在执行期间断电，则即使命令未完成，UseFlag 的其中一个使用位
也仍可被清零。为此，Microchip 建议密钥只使用一次，其他位会产生安全隐患。
在正常情况下，全部 8 个 UseFlag 字节均应初始化为 0xFF。如果要允许某个特定密钥的使用次数少于 8 次，则应将这些字节初始化为 0x7F（使用 7 次）、0x3F（使用 6 次）、0x1F（使用 5 次）、0x0F（使用 4 次）、0x07（使用 3 次）、0x03（使用 2 次）或 0x01（使用 1 次）。禁止初始化为除这些值或 0xFF 以外的任何其他值。
Read、Write 和 DeriveKey 命令的工作方式稍有不同，如下所述：

- **Read 和 Write**

  这些命令忽略 LimitedUse 位的状态，并且 UseFlag 字节不会因执行这些命令而改变。尽管槽中的值不能用作加密命令的密钥，但 UseFlag 被占用的 LimitedUse 槽（值为 0x00）仍然可被读取或写入（受相应 SlotConfig 限制的影响）。

  如果槽 X 的 SlotConfig.WriteKey 指回 X，但 UseFlag<X>被占用，则对槽进行的加密写操作将始终不会成功，因为之前的 GenDig 命令将因使用限制而返回错误。读操作和 ReadKey 存在类似的情况。用作密钥的槽不应将 IsSecret 设置为 0，或将 WriteConfig 设置为“始终”。

- **DeriveKey**

  如果父密钥用于身份验证或用作源，则在 LimitedUse（针对父密钥）置 1 且 UseFlag（同样针对父密钥）为 0x00 时，DeriveKey 命令将返回错误。对于目标密钥，LimitedUse 和 UseFlag位被忽略。成功执行后，DeriveKey 始终为目标密钥将 UseFlag 复位为 0xFF。这是复位 UseFlag 位的惟一机制。

  DeriveKey 命令的使用是可选项。只有在此槽的 WriteConfig<13>置 1 时，才能合法运行此命令。在某些情况下，仅配有一个可以使用八次的密钥是有利的。在这种情况下，其他加密命令将逐一将 UseFlag 中的位清零，直到所有位均清零，此时会禁止密钥。

13.3.5 有限使用的密钥

如果 Slot<15>.LimitedUse 置 1，则将通过与上述一次性限制（仅适用于槽 0 至 7）不同的机制来限制密钥编号 15 的使用。

在通过加密命令使用密钥 15 之前，将发生以下情况：

- 如果 LastKeyUse 中的所有字节均为 0x00，则将返回错误。
- 从 LastKeyUse 的第一个字节（配置区域中的字节 68）的 bit 7 开始，将第一个当前为 1 的位清零。如果字节 68 为 0x00，则检查字节 69 的第 7 位，依此类推，直到字节 83。在使用密钥 15 之前，每次只将 1 位清零。

此限制没有复位机制；在使用 128 次（或个性化时 LastKeyUse 中置 1 的位数）之后，将永久禁止密钥 15。此功能不易受电源中断的影响。即使在执行命令期间电源中断，LastKeyUse 中只有 1 位是未知的；LastKeyUse 中的所有其他位将保持不变，并且此密钥将保持不变。

如果密钥 15 的使用次数需少于 128，则此阵列中的一些字节不应初始化为 0xFF。对于 UseFlag，此字段中字节的惟一合法值（0xFF 除外）为 0x7F、0x3F、0x1F、0x0F、0×07、0x03、0×01 或 0x00。设置为 1 的总位数表示使用次数。

示例：有限使用的次数设置为 16。

```
0xFF, 0xFF, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00
```

LimitedUse 位会被 Read 和 Write 命令忽略，并且 LastKeyUse 不会因执行这些命令而改变。LimitedUse 位会被 CheckMac 命令的复制功能忽略。LimitedUse 位会受 DeriveKey 命令中的父密钥遵从，但会被目标密钥忽略。

13.3.6 密码检查

许多应用程序要求用户输入密码以使能功能，解密存储的数据或实现其他用途。通常情况下，预期密码必须存储在存储器中的某个位置，因此容易发现。ATSHA204A 可以安全地存储预期密码并对其执行一些有用的操作。密码始终不会明文传送给器件，且无法从器件读取。密码传送给器件之前，将在系统软件中使用随机数进行哈希运算。使用传输密钥时，必须始终使用内部 RNG 生成 TempKey 中的临时值。

CheckMac 命令的副本功能可使能以下类型的密码检查选项：

1. CheckMac 将与预期的密码进行内部比较，并向系统返回布尔值以指示密码是否正确输入。
2. 如果器件确定输入了正确的密码，则密码的值可以与存储的值或临时值组合使用，以创建一个密钥，供系统用于数据保护。
3. 如果器件确定已经输入了正确的密码，则器件可以根据这一事实来选择性地释放次级高随机性机密信息，此机密信息可用于数据保护，而没有穷举字典攻击的风险。
4. 如果密码已丢失，则获知了父密钥值的实体可以选择性地将新密码写入槽中。当前值也可以用父密钥加密并从器件读取。

密码应存储在偶数编号的槽中。如果要将密码映射到次级值（使用上面的第三步），则包含此值的目标槽将采用下一个更高的槽编号（密码的槽编号加 1）；否则，目标槽与密码槽相同。

目标槽的 ReadKey 必须设置为 0x0，才能使能此功能。为了防止欺诈或意外使用此功能，请勿将任何槽的 ReadKey 设置为 0x0，除非此 CheckMac/Copy 功能是特别需要的。特别是，不要假定特定槽的配置字中的其他位将覆盖由 ReadKey = 0x0 指定的此功能的使能操作。

仅当 CheckMac 的模式参数的值为 0x01 或 0x05，且 TempKey.SourceFlag 与 Mode<2>匹配时，才使能此功能。

注： 使用 Mode 0x05 时应小心，因为系统会受到重放攻击；不过，这种分配对于某些系统配置可能是有利的。

- SHA-256 报文的前 32 个字节存储在 EEPROM 的数据槽中（密码）。
- SHA-256 报文的第二组 32 个字节必须是 TempKey 寄存器中随机生成的临时值。

如果满足上述条件，并且输入响应与内部生成的摘要匹配，则目标密钥的内容将复制到 TempKey。其他 TempKey 寄存器位的设置如下：

- SourceFlag 设置为 1（非随机）。
- GenData 设置为 0（不是由 GenData 命令生成的）。
- CheckFlag 设置为 0（TempKey 不受限于 CheckMac 命令）。
- Valid 设置为 1。

13.3.7 传输密钥

ATSHA204A 器件包括一个内部硬件密钥阵列（传输密钥），用于在锁定数据部分之前实现安全个性化。硬件密钥的值是保密的，只有符合要求的客户才能向 Microchip 申请。这些密钥只能用于 GenDig 命令，由大于或等于 0x8000 的 SlotID 值指示。

对于 GenDig 和所有其他命令，小于 0x8000 的 SlotID 值始终引用存储在 EEPROM 数据区域中的密钥。在这些情况下，只有 SlotID 的低 4 位用于确定槽编号，而整个 16 位 SlotID 作为输入在任意 SHA-256 报文计算中使用。

14. 版本历史

版本 A（2018 年 4 月）
本文档的 Microchip 格式初始版本。

该版本自 2015 年 11 月起取代 Atmel 文档修订版 8885H。

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：	ATSHA204A：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：

- ATSHA204A-SSHCZ-T: 单线，卷带式，每卷盘 4,000 个，8 引脚 SOIC 封装
- ATSHA204A-SSHCZ-B：单线，管装式，每管 100 个，8 引脚 SOIC 封装
- ATSHA204A-SSHDA-T：I^2C，卷带式，每卷盘 4,000 个，8 引脚 SOIC 封装
- ATSHA204A-SSHDA-B：I^2C，管装式，每管 100 个，8 引脚 SOIC 封装
- ATSHA204A-MAHCZ-T：单线，卷带式，每卷盘 15,000 个，8 焊盘 UDFN 封装
- ATSHA204A-MAHDA-T：I^2C，卷带式，每卷盘 15,000 个，8 焊盘 UDFN 封装
- ATSHA204A-MAHCZ-S：单线，卷带式，每卷盘 3,000 个，8 焊盘 UDFN 封装
- ATSHA204A-MAHDA-S：I^2C，卷带式，每卷盘 3,000 个，8 焊盘 UDFN 封装
- ATSHA204A-RBHCZ-T：单线，卷带式，每卷盘 5,000 个，3 引脚触点式封装
- ATSHA204A-RBHCZ-B：单线，管装式，每管 56 个，3 引脚触点式封装
- ATSHA204A-STUCZ-T：单线，卷带式，每卷盘 5000 个，3 引脚 SOT-23 封装
- ATSHA204A-XHDA-T：I^2C，卷带式，每卷盘 5000 个，8 引脚 TSSOP 封装
- ATSHA204A-XHCZ-T：单线，卷带式，每卷盘 5000 个，8 引脚 TSSOP 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、Adaptec、AnyRate、AVR、AVR 徽标、AVR Freaks、BesTime、BitCloud、chipKIT、chipKIT 徽标、CryptoMemory、CryptoRF、dsPIC、FlashFlex、flexPWR、HELDO、IGLOO、JukeBlox、KeeLoq、Kleer、LANCheck、LinkMD、maXStylus、maXTouch、MediaLB、megaAVR、Microsemi、Microsemi 徽标、MOST、MOST 徽标、MPLAB、OptoLyzer、PackeTime、PIC、picoPower、PICSTART、PIC32 徽标、PolarFire、Prochip Designer、QTouch、SAM-BA、SenGenuity、SpyNIC、SST、SST 徽标、SuperFlash、Symmetricom、SyncServer、Tachyon、TempTrackr、TimeSource、tinyAVR、UNI/O、Vectron 及XMEGA 均为 Microchip
Technology Inc.在美国和其他国家或地区的注册商标。
APT、ClockWorks、The Embedded Control Solutions Company、EtherSynch、FlashTec、Hyper Speed Control、HyperLight Load、IntelliMOS、Libero、motorBench、mTouch、Powermite 3、PrecisionEdge、ProASIC、ProASIC Plus、ProASIC Plus 徽标、Quiet-Wire、SmartFusion、SyncWorld、Temux、TimeCesium、TimeHub、TimePictra、TimeProvider、Vite、WinPath 和ZL 均为 Microchip Technology Inc.在美国的注册商标。

ISBN：978-1-5224-4714-6

质量管理体系

有关Microchip 质量管理体系的更多信息，请访问**www.microchip.com/quality**

全球销售及服务网点

美洲	亚太地区	亚太地区	欧洲
公司总部 2355 West Chandler Blvd. 钱德勒，亚利桑那州 85224-6199 电话：480-792-7200 传真：480-792-7277 技术支持： http://www.microchip.com/support 网址： www.microchip.com 亚特兰大 德卢斯，佐治亚州 电话：678-957-9614 传真：678-957-1455 奥斯汀，德克萨斯州 电话：512-257-3370 波士顿 韦斯特伯鲁，马萨诸塞州 电话：774-760-0087 传真：774-760-0088 芝加哥 艾塔斯卡，伊利诺伊州 电话：630-285-0071 传真：630-285-0075 达拉斯 阿迪森，德克萨斯州 电话：972-818-7423 传真：972-818-2924 底特律 诺维，密歇根州 电话：248-848-4000 休斯顿，德克萨斯州 电话：281-894-5983 印第安纳波利斯 诺布尔斯维尔，印第安纳州 电话：317-773-8323 传真：317-773-5453 电话：317-536-2380 洛杉矶 米慎维荷，加利福尼亚州 电话：949-462-9523 传真：949-462-9608 电话：951-273-7800 罗利，北卡罗来纳州 电话：919-844-7510 纽约，纽约州 电话：631-435-6000 圣何塞，加利福尼亚州 电话：408-735-9110 电话：408-436-4270 加拿大 - 多伦多 电话：905-695-1980 传真：905-695-2078	澳大利亚 - 悉尼 电话：61-2-9868-6733 中国 - 北京 电话：86-10-8569-7000 中国 - 成都 电话：86-28-8665-5511 中国 - 重庆 电话：86-23-8980-9588 中国 - 东莞 电话：86-769-8702-9880 中国 - 广州 电话：86-20-8755-8029 中国 - 杭州 电话：86-571-8792-8115 中国 - 香港特别行政区 电话：852-2943-5100 中国 - 南京 电话：86-25-8473-2460 中国 - 青岛 电话：86-532-8502-7355 中国 - 上海 电话：86-21-3326-8000 中国 - 沈阳 电话：86-24-2334-2829 中国 - 深圳 电话：86-755-8864-2200 中国 - 苏州 电话：86-186-6233-1526 中国 - 武汉 电话：86-27-5980-5300 中国 - 西安 电话：86-29-8833-7252 中国 - 厦门 电话：86-592-2388138 中国 - 珠海 电话：86-756-3210040	印度 - 班加罗尔 电话：91-80-3090-4444 印度 - 新德里 电话：91-11-4160-8631 印度 - 浦那 电话：91-20-4121-0141 日本 - 大阪 电话：81-6-6152-7160 日本 - 东京 电话：81-3-6880- 3770 韩国 - 大邱 电话：82-53-744-4301 韩国 - 首尔 电话：82-2-554-7200 马来西亚 - 吉隆坡 电话：60-3-7651-7906 马来西亚 - 槟榔屿 电话：60-4-227-8870 菲律宾 - 马尼拉 电话：63-2-634-9065 新加坡 电话：65-6334-8870 台湾地区 - 新竹 电话：886-3-577-8366 台湾地区 - 高雄 电话：886-7-213-7830 台湾地区 - 台北 电话：886-2-2508-8600 泰国 - 曼谷 电话：66-2-694-1351 越南 - 胡志明市 电话：84-28-5448-2100	奥地利 - 韦尔斯 电话：43-7242-2244-39 传真：43-7242-2244-393 丹麦 - 哥本哈根 电话：45-4450-2828 传真：45-4485-2829 芬兰 - 埃斯波 电话：358-9-4520-820 法国 - 巴黎 电话：33-1-69-53-63-20 传真：33-1-69-30-90-79 德国 - 加兴 电话：49-8931-9700 德国 - 哈恩 电话：49-2129-3766400 德国 - 海尔布隆 电话：49-7131-72400 德国 - 卡尔斯鲁厄 电话：49-721-625370 德国 - 慕尼黑 电话：49-89-627-144-0 传真：49-89-627-144-44 德国 - 罗森海姆 电话：49-8031-354-560 以色列 - 若那那市 电话：972-9-744-7705 意大利 - 米兰 电话：39-0331-742611 传真：39-0331-466781 意大利 - 帕多瓦 电话：39-049-7625286 荷兰 - 德卢内市 电话：31-416-690399 传真：31-416-690340 挪威 - 特隆赫姆 电话：47-72884388 波兰 - 华沙 电话：48-22-3325737 罗马尼亚 - 布加勒斯特 电话：40-21-407-87-50 西班牙 - 马德里 电话：34-91-708-08-90 传真：34-91-708-08-91 瑞典 - 哥德堡 电话：46-31-704-60-40 瑞典 - 斯德哥尔摩 电话：46-8-5090-4654 英国 - 沃金厄姆 电话：44-118-921-5800 传真：44-118-921-5820