ECC608-TFLXWPC

ECC608-TFLXWPC CryptoAuthentication™数据手册

简介

ECC608-TFLXWPC是ATECC608A产品系列的预配置型号。TrustFLEX安全元件属于Microchip通用配置安全器件系列。器件配置旨在满足无线充电联盟（Wireless Power Consortium，WPC）Qi® 1.3版本标准的身份验证要求。

按照定义，ECC608-TFLXWPC 配置满足提供身份验证的Qi发射器的基本身份验证需求。如果需要，可以实现双WPC证书槽。此外，还支持用户提供专有扩展以实现WPC基础架构产品的TLS身份验证或提供安全引导功能。其中一些数据槽具有指定用途，其余数据槽均可灵活用于其他应用。在订购ECC608-TFLXWPC器件之前，这些槽的访问策略将由Trust Platform Design Suite工具设置。

本数据手册提供了ECC608-TFLXWPC特有的槽和密钥配置信息。该信息定义了每个数据区域槽的访问策略。其中仅包含相关命令和I/O工作信息。此外，应用部分介绍了可帮助开发应用程序的Microchip软硬件工具及其下载链接。

特性

- JIL高评级——经验证符合JIL Application of Attack Potential to Smartcards and Similar Devices（版本3.1）
- 指定的配置区，具有有限的可选选项
- 具有可一次性更改I²C地址的I²C接口
- 支持WPC Slot 0制造证书颁发机构（Certification Authority，CA）和量产器件证书
  - WPC制造证书颁发机构（CA）——压缩证书和公钥
  - WPC量产器件压缩证书
  - WPC量产器件P-256椭圆曲线加密（Elliptic Curve Cryptography，ECC）私钥
- 可选择支持WPC Slot 1、WPC Slot 2或WPC Slot 3专有扩展
- 支持WPC槽摘要，以便对发射器快速进行WPC重新身份验证
- 支持TLS身份验证
  - 适用于Google Cloud™、Amazon Web Services（AWS®）和Microsoft® Azure Cloud Services等
  - TLS签名人——压缩证书和公钥
  - TLS器件压缩证书
  - TLS器件P-256 ECC私钥
- I/O保护密钥槽，用于保护I²C通信
- 使用制造时可定制的安全引导公钥使能安全引导
- 采用8引脚UDFN和8引脚SOIC封装，量产为2k件

应用

- WPC Qi 1.3身份验证
- 安全IoT TLS 1.2和1.3连接
- 安全引导/安全固件更新

© 2022 Microchip Technology Inc.
及其子公司

目录

简介.....1

特性.....1

应用.....1

1. 引脚配置和引脚分配.....5

2. 无线充电联盟.....6

2.1. 无线充电联盟术语.....6

3. EEPROM存储器和数据区域访问策略.....8

3.1. ECC608-TFLXWPC配置区域.....9

3.1.1. 可修改的配置区域字节.....9

3.2. 数据区域和访问策略.....10

3.2.1. 数据区域数据类型.....10

3.2.1.1. 私钥.....10

3.2.1.2. ECC公钥.....10

3.2.1.3. 证书存储.....11

3.2.1.3.1. TLS证书存储.....11

3.2.1.3.2. WPC证书存储.....12

3.2.1.4. WPC槽摘要.....12

3.2.1.5. 安全引导.....13

3.2.1.6. I/O保护密钥.....13

3.2.1.7. 通用数据存储.....13

3.2.2. 槽配置术语.....13

3.2.3. ECC608-TFLXWPC槽配置汇总.....14

3.2.4. ECC608-TFLXWPC详细槽访问.....15

3.3. ECC608-TFLXWPC EEPROM一次性编程（OTP）区域.....22

4. 器件命令.....23

4.1. 常规器件命令.....24

4.1.1. Counter命令.....24

4.1.2. Info 命令.....24

4.1.3. Lock命令.....24

4.1.4. Nonce 命令.....24

4.1.5. Random 命令.....25

4.1.6. Read 命令.....25

4.1.7. SelfTest命令.....25

4.1.8. SHA命令.....25

4.1.9. UpdateExtra命令.....25

4.1.10. Write命令.....25

4.2. 非对称加密命令.....25

4.2.1. ECDH命令.....26

4.2.2. GenKey命令.....26

4.2.3. SecureBoot命令.....26

4.2.4. Sign命令.....26

4.2.5. Verify命令 26
4.3. 对称加密命令 27
4.3.1. GenDig命令 27
4.3.2. MAC命令 27

5. I²C接口 28
5.1. I/O条件 28
5.1.1. 器件休眠 28
5.1.2. 器件唤醒 29
5.2. I²C至ECC608-TFLXWPC的I2C传输 30
5.2.1. 字地址值 31
5.2.2. I²C同步 31
5.3. 休眠序列 32
5.4. 空闲序列 32
5.5. SMBus超时 32
5.6. 自ECC608-TFLXWPC的I²C传输 32

6. 应用信息 34
6.1. WPC相关信息 34
6.2. 用例 35
6.3. 开发工具 35
6.3.1. 可信平台设计套件 35
6.3.2. 硬件工具 35
6.3.3. CryptoAuthLib 36

7. 电气特性 38
7.1. 绝对最大值 38
7.2. 可靠性 38
7.3. 交流参数： 所有I/O接口 38
7.3.1. 交流参数：I²C接口 39
7.4. 直流参数：所有I/O接口 40
7.4.1. V_{IH}和V_{IL}规范 41

8. 封装图 43
8.1. 封装标识信息 43
8.2. 8焊盘UDFN 44
8.3. 8引脚SOIC 47

9. 版本历史 50

Microchip网站 51

产品变更通知服务 51

客户支持 51

产品标识体系 52

Microchip 器件代码保护功能 52

法律声明 52

商标.....53

质量管理体系.....53

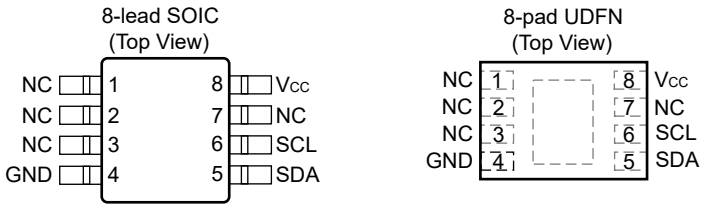
全球销售及服务网点.....54

1. 引脚配置和引脚分配

表 1-1. 引脚配置

引脚	I²C 器件功能
NC	无连接
GND	地
SDA	I²C串行数据
SCL	I²C串行时钟输入
VCC	电源

图1-1. UDFN和SOIC引脚分配



注： 建议将UDFN背面焊盘连接到GND。

2. 无线充电联盟

无线充电联盟定义了一个完整的生态系统，用于为移动设备部署无线充电。从Qi规范的版本1.3开始，身份验证便被定义为充电器以高于5W的功率充电时必须满足的一项要求。该规范的版本1.3允许以最高15W的功率为移动设备充电。所有充电器最初以5W功率充电时都无需身份验证。当充电功率超过5W后，必须进行身份验证。
为了适应这些变化，信任链被定义为Qi生态系统的一部分。该信任链分为三个级别：

1. WPC根证书——包括根私钥和根证书。
2. WPC制造证书——包括由根证书的私钥签名的制造证书。
3. WPC量产器件证书——包括由WPC制造证书的私钥签名的量产器件证书。

WPC证书遵循X.509格式。对于WPC Slot 0和1，证书格式是固定的。对于WPC Slot 2和3，格式未定义，允许专有使用这些证书链槽。

要参与WPC无线充电生态系统，必须成为无线充电联盟的成员。有关标准和联盟的更多信息，请访问WPC网站：www.wirelesspowerconsortium.com/.

2.1 无线充电联盟术语

本数据手册中使用的以下术语旨在帮助理解WPC Qi身份验证标准的相关项。本节旨在反映WPC标准中的信息，但在所有情况下都应以标准本身为准。

电源接收器	由电源发射器充电并与其通信以进行身份验证或控制充电的器件。
电源发射器	用于与电源接收器通信并向其供电的器件。安全存储子系统位于电源发射器内。
Qi	WPC针对与移动设备无线充电相关的标准使用的标识符。
撤销顺序标识符（RSID）	RSID是WPC器件证书中存储的惟一标识符，用于惟一标识给定发射器以及出于不合规原因而撤销电源发射器的高功率或完整操作应用。
安全存储子系统（SSS）	用于存储对无线电源发射器进行身份验证所使用的安全信息的器件，可视为安全元件或安全加密器件。
WPC制造商	获得WPC许可生产经认证的WPC电源发射器的公司或实体。所有WPC制造商都必须签署WPC制造商协议。
WPC制造CA	获得WPC许可生产经认证的WPC电源发射器中使用的安全存储子系统的公司。Microchip就是一家获得许可的制造CA。
无线充电联盟	负责定义与Qi标准相关的所有无线充电规范以及许可和认证Qi认证产品的标准机构。生产符合Qi标准的电源发射器或接收器需要成为WPC的成员。有关WPC的更多信息，请访问以下网站：www.wirelesspowerconsortium.com/。
WPC根颁发机构	WPC根颁发机构是WPC证书链的关键。所有WPC制造证书都将由WPC根颁发机构签名。

WPC槽

WPC身份验证规范将槽定义为存储WPC证书链的元素。WPC身份验证规范定义了四个可能的槽（Slot 0-3），但只需要使用Slot 0，并且其中必须存储WPC证书链。如果使用Slot 1，则此槽也保留用于存储WPC证书链。Slot 2和3的格式未定义，这两个槽保留用于可选专有扩展。在本文档中，提及WPC证书链时将始终使用术语“WPC槽”，以便与用于表示ECC608-TFLXWPC器件中的数据槽的术语“槽”区分开来。

WPC槽摘要

存储在WPC槽中的整个证书链的32字节摘要。

3. EEPROM存储器和数据区域访问策略

EEPROM存储器共有1400字节，分为以下几个区域：

表 3-1. ECC608-TFLXWPC EEPROM区域

区域	说明	命名
配置	128字节（1024位）EEPROM区域，包含： • 器件配置 • 槽访问策略信息 • 计数器值 • 器件序列号 • 锁定信息 LockConfig字节已设置。无法向该区域直接写入任何内容。始终可读取该区域。	Config[a:b] = 配置区域某个字段内的字节范围
数据	1208字节（9.7 Kb）区域，分为16个通用只读或读/写存储器槽。配置区域字节定义的访问策略信息决定了每个槽的访问方式。ECC608-TFLXWPC器件中每个数据槽的访问策略已设置并且配置区域定义的槽访问策略完全有效。取决于槽访问策略，有些可以被读写，而有些则不能。	Slot[YY] = 存储在数据区域的Slot YY中的全部内容
一次性编程（OTP）	64字节（512位）区域，分为两个块，每个块32字节。对于ECC608-TFLXWPC，该区域预装了一个预定义值。该区域无法修改，但可以随时读取。有关更多信息，请参见3.3 ECC608-TFLXWPC EEPROM一次性编程（OTP）区域。	OTP区域内的一个字节，而OTP[aa:bb]表示一个字节范围

表 3-2. 文档术语

本文档中讨论的术语具有以下含义：

术语	含义
块	特定存储区域的单个256位（32字节）区域。工业标准SHA-256文档还使用术语“块”来表示报文输入的512位片段。在本文档内，仅当描述哈希输入报文时使用此约定。
KeyID	KeyID相当于指定为保存密钥值的槽的编号。Key1（有时称为key[1]）存储在Slot[1]中，依此类推。当全部16个槽均可保存密钥时，配置为允许明文读取的槽通常不会被加密命令用作私钥或机密信息密钥。
mode[b]	表示参数模式的bit（b）。
SRAM	包含输入和输出缓冲区以及内部状态存储单元。用户无法直接访问该存储器。
Word	从块读取或写入块的单个4字节数据字。字是数据访问的最小单位。
LSB/MSB	最低有效字节/最高有效字节。
LSb/MSb	最低有效位/最高有效位。

3.1 ECC608-TFLXWPC配置区域

ECC608-TFLXWPC配置在很大程度上是固定的，客户无法进行修改。使用Microchip可信平台设计套件时，工具会考虑所有配置信息。有关如何配置器件的信息显示在下方或槽信息中。

器件配置信息

- 每个器件的序列号都是惟一的，存储在byte[0:3，8:12]中。Byte[0:1]为0x01 0x23，Byte[8]为0x01。所有其他字节都是惟一的。默认的7位I²C地址为0x38。可使用`UpdateExtra`命令改写I²C地址。

重要：ECC608-TFLXWPC的默认I²C地址与通用未配置ATECC608A器件不同。

- I/O电压设置为固定参考电压；因此，主机处理器可以在低于ECC608-TFLXWPC器件电压的电压下工作。
- 看门狗定时器（WDT）设置为1.3s的最大超时。
- 存储在Slot 6中的密钥可用作I/O保护密钥。
- 对于ECC608-TFLXWPC，以下各个槽可以单独配置为锁定或不锁定：Slot 3-6和8-15。
- 对于 ECC608-TFLXWPC，FullStore摘要模式支持SecureBoot。
- 单调计数器可供系统使用，并且未关联到任何密钥。
- 无论何时因运行状况测试失败而导致命令失败后，运行状况测试失败位都会清零。如果失败征兆是暂时的，则在第二次运行时，命令可能会通过。

3.1.1 可修改的配置区域字节

由于配置区域已锁定，因此不能直接写入配置区域中的任何字节。但是，仍然可以使用其他命令来修改某些字节。

SlotLocked位

对于ECC608-TFLXWPC，可单独配置以下各槽为锁定或不锁定：Slot 3-6及8-15。通过使用Trust Platform Design Suite工具，可在生产时将这些槽设置为固定或锁定。Slot 10-12 及Slot 9、13或14必须始终以同样的方法设置。这些槽可通过`Lock`命令的SlotLock模式锁定。每个使能了此功能的槽只能被单独锁定一次。一旦槽被锁定，将无法对其进行修改或解锁，但仍可根据为该槽定义的访问策略进行使用。

Byte 88和89用于存储SlotLocked字节。最初，这些字节中的所有位均设置为值1。对于已锁定的槽，相应位的值将设置为值0。

I²C地址重新定义

此器件已经过相应配置，以便可重新定义一次I²C地址。`UpdateExtra`命令可用于将配置区域的byte 85重新写入新I²C地址。当该字节设置为非零值时，器件配置将byte 85用作其I²C地址 ，而非使用默认地址。重新写入该字节后，器件必须先掉电或置于休眠模式，之后此更改才会生效。

重要：如果无需更改I²C地址，则必须使用默认I²C地址写入该存储单元。

UserExtra字节
UserExtra字节可用于任何所需用途。该字节只能用`UpdateExtra`命令更新一次。UserExtra字节位于配置区域的byte 84。

Counter[0,1]
尽管该器件未使用计数器，但不会将其禁止。如有必要，系统可使用单调计数器。请注意，计数器被初始化为零，并且可以计数到最大值2,097,151。计数器值可递增或通过使用`Counter`命令读取。该计数器的使用方式严格遵循系统要求，与器件上的其他任何事物无关。计数器值可使用`Counter`命令读取或更新。

3.2 数据区域和访问策略

以下各节介绍了与每个槽关联的详细访问策略信息。实际访问策略信息存储在EEPROM配置区域的槽和密钥配置段中。每个数据区域槽都具有与其关联的2个槽配置字节和2个密钥配置字节。这4个字节一起为每个槽创建访问策略。存储在槽中的数据的实际类型由该槽的访问策略确定。

3.2.1 数据区域数据类型

以下部分提供了ECC608-TFLXWPC数据槽中能够存储的各种数据类型的更多详细信息。

3.2.1.1 私钥

ECC私钥是ECC安全性的基本构件。这些密钥是私密的，并且对于每个器件都是惟一的，始终无法读取。ECC私钥由HSM在配置期间随机生成，并安全地保存在配置为ECC私钥的槽中。

TLS IoT私钥
这是用于IoT连接的主身份验证密钥。该密钥是永久性的，不能更改。每个器件都有自己惟一的私钥。

该密钥可用于：

- 用于身份验证的ECDSA签名
- 用于密钥协议的ECDH。如果需要对ECDH输出进行加密，则需要先设置I/O保护密钥。有关设置的详细信息，请参见3.2.1.6 I/O Protection Key。

该私钥是生成相应公钥和IoT TLS X.509证书的基础。

WPC Slot 0和Slot 1私钥
这些是用于WPC器件身份验证的主ECC密钥。通常，只会使用WPC Slot 0中的密钥。

该密钥可用于：

- 用于身份验证的ECDSA签名

该私钥是分别为WPC Slot 0和WPC Slot 1的WPC X.509量产器件证书生成相应公钥的基础。

3.2.1.2 ECC公钥

公钥始终与ECC私钥相关联。每个ECC私钥将具有自己的惟一公钥。公钥可以存储在器件中，如果器件的给定槽进行了相应配置，也可以使用`GenKey`命令重新生成。对于ECC608-TFLXWPC，可以使用或生成7种公钥：

- 器件Slot 0和Slot 1包含与WPC Slot 0和WPC Slot 1证书链关联的WPC量产器件证书的ECC私钥。对于其中每一个私钥，始终可以生成对应的公钥并将其用于验证操作。
- 器件Slot 2包含用于TLS IoT身份验证的ECC私钥。对于该私钥，始终可以生成对应的公钥并将其用于验证操作。
- 器件Slot 9包含WPC Slot 0制造X.509证书的ECC公钥。
- 器件Slot 8包含WPC Slot 1制造X.509证书的ECC公钥。该公钥存储在槽的前72个字节中。如果未使用WPC Slot 1，则该密钥可能有其他用途，也可能没有。
- Slot 11包含X.509 IoT TLS签名人证书信息中的ECC公钥。
- Slot 15包含可用于安全引导操作的ECC公钥。

3.2.1.3 证书存储

ECC608-TFLXWPC 可支持针对不同用例应用的多个证书链，最多支持三个X.509证书链。由于X.509证书的大小通常比单个ECC608-TFLXWPC器件槽大，因此使用压缩格式。该技术更应被称为部分证书，因为它在器件上存储动态证书信息，并施加了一些限制。动态信息是可以随器件更改的证书内容（例如，公钥和有效日期等）。而静态数据是在所有器件上都保持不变的证书内容。固件的证书定义中应包含模板，以便针对具体用例完全重建每个X.509证书。完整的证书由动态数据和静态数据组合而成

ECC608-TFLXWPC提供两种X.509证书来分别支持IoT TLS用例和WPC身份验证用例。每一种都采用不同的X.509格式，因此ECC608-TFLXWPC将具有不同的压缩证书格式。如果未使用WPC Slot 1并且在WPC Slot 2或WPC Slot 3中使用了专有扩展，则可能需要其他类型的证书链。

3.2.1.3.1 TLS证书存储

TLS X.509证书链与用于Microchip Trust&GO和TrustFLEX TLS产品的证书链相同，具体来说是ATECC608B-TNGTLS和ATECC608B-TFLXTLS。

以下应用笔记记录了压缩证书格式：《压缩证书定义》。

CryptoAuthLib库还包含用于处理TLS压缩证书的atcacert模块。

器件证书
件证书包含与实际ECC608-TFLXWPC器件关联的信息。

签名人证书
签名人证书包含与用于签名器件证书的签名人证书颁发机构相关的信息。此外，还需要添加签名人公钥来重新编译完整的签名人证书。

签名人公钥
签名人公钥用于验证签名人和与签名人压缩证书关联的信息。

下表列出了与ECC608-TFLXWPC中的证书关联的所有槽：

表3-3. 证书槽

槽	说明
3	主私钥。在模式 = 0x00时，可使用`GenKey`命令随时生成公钥。
10	器件证书。以压缩格式存储在此处。
11	签名人公钥。

.....续

槽	说明
12	签名人证书。以压缩格式存储。

对于ECC608-TFLXWPC量产器件，这些槽可配置为永久锁定或槽可锁定。为了便于初期开发，对于原型器件将Slot 10-12设置为槽可锁定。

3.2.1.3.2 WPC证书存储

WPC X.509证书链记录在WPC 1.3.0身份验证规范中。该规范仅限WPC的注册成员使用。Microchip针对WPC X.509证书使用的压缩格式是以前针对Microchip定义的TLS X.509证书使用的压缩格式的变型。

WPC证书使用的命名法反映了WPC身份验证规范使用的命名法。

CryptoAuthLib库还包含用于处理WPC压缩证书的atcawpccert模块。

量产器件证书
量产器件证书包含与安全存储子系统关联的信息。量产器件证书与为TLS身份验证用例指定的器件证书等效。

制造商证书
制造商证书包含与制造商证书颁发机构关联的信息，用于对量产器件证书进行签名。制造商证书与为TLS身份验证用例指定的签名人证书等效。

制造商公钥
制造商公钥用于验证制造商和与制造商压缩证书关联的信息。制造商公钥与为TLS身份验证用例指定的签名人公钥等效。

下表列出了与ECC608-TFLXWPC中的WPC证书关联的所有槽：

表 3-4. 证书槽

WPC Slot 0	WPC Slot 1	说明
0	1	主WPC私钥。在模式 = 0x00时，可使用`GenKey`命令随时生成公钥。
4	8	制造商或量产器件证书所需的额外数据
5	8	量产器件证书所需的RSID
13	8	量产器件证书。以WPC压缩格式存储。
9	8	签名人公钥。
14	8	制造商证书。以WPC压缩格式存储。

对于ECC608-TFLXWPC量产器件，这些槽可配置为永久锁定或槽可锁定。为了便于初期开发，对于原型器件将Slot 4、5、8、9、13和14设置为槽可锁定。

3.2.1.4 WPC槽摘要

除了使用证书进行完整身份验证之外，还可以使用WPC身份验证规范进行快速身份验证，具体来说只需要比较与WPC Slot 0或WPC Slot 1相关联的摘要（如果已相应定义）即可。要使用此方法，必须事先完成完整的身份验证，并且必须计算和存储WPC槽的摘要。

摘要值是一个32字节的值，通过对整个WPC槽进行SHA-256哈希运算得出。该规范允许为每个已定义的WPC证书槽计算摘要。>ECC608-TFLXWPC可存储两个摘要。器件Slot 3用于WPC Slot 0。WPC Slot 1摘要存储在Slot 8[288:319]中。

3.2.1.5 安全引导

ECC608-TFLXWPC支持 `SecureBoot` 命令。此功能支持系统在执行完全引导之前先通过自举程序以加密方式验证其固件，还可用于在装载新固件映像之前对其进行验证。

安全引导功能需要建立P-256固件签名密钥才能使用。私钥将由固件开发人员持有，用于对固件映像进行签名。公钥需要写入安全引导公钥槽，然后通过锁定槽使公钥变成永久性的。

对于ECC608-TFLXWPC，还可以使能以下功能：需经过有效安全引导后才能获得授权使用TLS主私钥以及WPC Slot 0和WPC Slot 1 ECC密钥。有关如何使能此功能的信息，请参见3.2.4 安全引导选项。

有关完整的详细信息，请参见 .2.3 SecureBoot 命令。

要实现安全引导，需要多个数据槽。

安全引导摘要
安全引导摘要是基于固件应用程序代码计算的32字节SHA-256摘要。每次更新固件时都需要更新此摘要。对于ECC608-TFLXWPC，摘要存储在Slot 7中。

安全引导公钥
安全引导公钥用于验证安全引导摘要和签名的验证功能。安全引导公钥存储在Slot 15中。

3.2.1.6 I/O保护密钥

`Verify`、`ECDH`、`SecureBoot`和`KDF`命令还可选择使用I/O保护功能来加密某些参数并（通过MAC）验证一些响应。这有助于防止物理 I^2C总线上出现中间人攻击。但是，为了能够使用该功能，MCU和ECC608-TFLXWPC 需要事先生成并保存惟一的I/O保护密钥，实际上是将MCU和ECC608-TFLXWPC器件彼此配对。配对过程必须在首次引导时进行。

I/O保护密钥生成：

1. MCU使用随机命令来生成一个随机的32字节I/O保护密钥。
2. MCU将I/O保护密钥保存在其内部闪存中。
3. MCU将I/O保护密钥写入I/O保护密钥槽中。
4. MCU槽锁定该槽以使I/O保护密钥具有永久性。

作为配对检查，MCU可以使用`MAC`命令向I/O保护密钥发出质询，并验证闪存中存储的I/O保护密钥是否与ECC608-TFLXWPC中的密钥匹配。

3.2.1.7 通用数据存储

所有槽都有指定的用途，但并非所有用途都是必需的。如果不需要WPC Slot 1信息，Slot 4和Slot 8可用于存储通用数据。如果不需要TLS身份验证用例，Slot 10-12也可用于存储通用数据。这些槽既可以在配置期间写入数据，也可以保持锁定状态，之后在现场写入数据。

3.2.2 槽配置术语

以下部分提供了一组用于讨论配置选项的术语。

术语	说明
AES密钥	槽可用作`AES`命令的密钥源。ECC608-TFLXWPC的AES密钥为128位长。

术语	说明
始终写入	可以使用Write命令以明文方式写入槽。
明文读取	槽视为公共（非机密）的，可以使用Read命令以明文方式读取其内容。
ECDH	椭圆曲线Diffie Hellman。私钥可与ECDH命令一起使用。
加密写入	只能使用加密写入基于指定的写密钥写入槽。
外部签名	私钥可用于对外部（任意）报文进行签名。
内部签名	私钥可用于对GenKey或GenDig命令生成的内部报文进行签名。用于证明器件的内部密钥和配置。
可锁定	槽可以在将来的某个时间锁定。锁定后，槽内容将无法更改（仅供读取/使用）。
不可读取	槽被视为机密，无法使用Read命令读取其内容。私钥和对称机密信息必须始终配置为“不可读取”。
不可写入	无法使用Write命令更改槽。
永久	私钥是永久的/不可更改。它是出厂配置期间在内部生成的。
可更新	私钥稍后可以改写为内部生成的全新随机私钥。其初始值是出厂配置期间在内部生成的。
经验证	父公钥使公钥生效后，公钥只能与Verify命令一起使用。

3.2.3 ECC608-TFLXWPC槽配置汇总

ECC608-TFLXWPC有16个槽，可以针对不同的用例进行配置。下表汇总了ECC608-TFLXWPC的这些槽及其配置以及建议的用例：

表3-5. 槽配置

槽	用例	说明	主要配置
0	WPC Slot 0 身份验证	WPC Slot 0主ECC身份验证密钥	永久，外部签名，不可读，可选安全引导使能
1[1]	WPC Slot 1 身份验证	WPC Slot 1主ECC身份验证密钥	永久，外部签名，不可读，可选安全引导使能
2	TLS身份验证	主TLS ECC身份验证密钥	永久，外部签名，ECDH，不可读，可选安全引导使能
3	WPC Slot 0 身份验证	WPC Slot 0证书链摘要	永久或者可写入且槽可锁定，明文读取（具体取决于访问策略）
4	WPC Slot 0 身份验证	WPC Slot 0额外信息	永久或者可写入且槽可锁定，明文读取（具体取决于访问策略）
5	WPC Slot 0 身份验证	WPC Slot 0额外信息	永久或者可写入且槽可锁定，明文读取（具体取决于访问策略）
6	I/O保护密钥	用于保护某些命令的I^2C总线通信（I/O）的密钥。使用前需要进行设置。	永久或者可写入且槽可锁定，永不读取（具体取决于访问策略）

.....续

槽	用例	说明	主要配置
7	安全引导	安全引导摘要的存储位置。这是一个内部功能，因此不使能读写操作。	不可读取，不可写入
8[2]	WPC Slot 1 身份验证	存储WPC Slot 1信息公钥、证书和槽摘要	明文读取，可写入或可锁定（具体取决于访问策略）
9	WPC Slot 0 身份验证	WPC Slot 0制造商公钥	永久，明文读取，不可写入或可写入（具体取决于访问策略）
10	TLS身份验证	CryptoAuthentication™ 压缩格式的TLS器件压缩证书	永久，明文读取，不可写入或可写入（具体取决于访问策略）
11	TLS身份验证	已对器件证书进行签名的CA（签名人）的TLS公钥	明文读取，不可写入或可写入（具体取决于访问策略）
12	TLS身份验证	CryptoAuthentication™压缩格式器件证书的CA（签名人）证书的TLS证书	明文读取，不可写入或可写入（具体取决于访问策略）
13	WPC Slot 0 身份验证	WPC Slot 0压缩器件证书	永久，明文读取，不可写入或可写入（具体取决于访问策略）
14	WPC Slot 0 身份验证	WPC Slot 0压缩制造商证书	永久，明文读取，不可写入或可写入（具体取决于访问策略）
15	安全引导	安全引导公钥	永久或者可写入且可锁定，明文读取

注：
1. 此槽始终为ECC私钥保留。如果不需要WPC Slot 1，此槽也可以存储用于WPC Slot 2或其他用途的私钥。
2. 如果应用中未使用WPC Slot 1，则此槽可用于存储WPC Slot 2或3的信息。如果此槽用于存储公钥或证书信息，建议将其锁定。如果不需要其他WPC槽，则此槽可用于存储通用数据。

3.2.4 ECC608-TFLXWPC详细槽访问策略

ECC608-TFLXWPC的默认WPC配置仅使用与WPC Slot 0关联的信息。与WPC Slot 0关联的器件槽中的所有信息都是身份验证过程或证书链的必需部分，但存储在Slot 3中的WPC Slot 0摘要除外。

注： 在使用默认WPC Slot 0配置之外的功能之前，请与Microchip核实，因为并非所有功能最初都已在预配置系统中实现。

ECC608-TFLXWPC在以下两个方面提供灵活性：
1. 槽永久锁定还是槽可锁定。
2. 安全引导是否已连接到密钥和持久锁存位。

槽锁定选项
槽锁定选项针对各个槽调用，将属于以下两种类型之一：

槽可锁定 槽锁定选项置1的槽允许最终用户在初始制造阶段之后的将来某个时候锁定槽。这可以用来在Microchip之外的最终制造步骤中或由最终用户设置密钥。可使用Lock命令锁定槽。槽一旦锁定，就无法再对其中的数据进行修改。

永久锁定	永久锁定的槽在离开Microchip制造厂后将永远无法更新。在配置这些器件之前，必须将正确的数据或密钥提供给Microchip。

安全引导选项
安全引导访问策略提供了一个选项，用于限定成功执行安全引导之前要运行的命令或提供无限的命令访问。可以将Slot 0、Slot 1和Slot 2中的ECC私钥设置为需要先进行安全引导，然后才能授权这些密钥用于大多数命令。要使用该功能，需要更改安全引导配置设置和密钥配置值。这些配置更改将在成功进行安全引导后设置持久锁存位。Slot 0的槽访问策略更改将密钥的使用与设置的持久锁存位连接到一起。

持久锁存位操作
即使在空闲和休眠模式下，持久锁存位也将保持其状态。这允许单次安全引导操作在初始上电后仅运行一次。如果器件电源电压低于最小允许值，则持久锁存位将复位，并且需要执行新的安全引导操作。

原型器件
原型器件具有无法更改的特定默认配置。默认配置将所有槽选项设置为“槽可锁定”。在开发软件以通过应用程序重新编程密钥时，这可提供极大的灵活性。最终配置不需要按这种方式设置。原型器件不支持安全引导选项。只能为已量产器件选择该选项。原型器件仅支持I^2C接口。

详细槽配置
下表更加详细地说明了器件上各个已配置槽的槽配置和密钥配置设置。其中包括适用于各个已配置槽的相关命令和命令模式。该表中按槽提供了适用于ECC608-TFLXWPC器件的所有允许密钥和槽配置值。

表3-6. Slot 0配置信息

槽	配置值	已使能功能的说明
0	**选项1：不连接到持久锁存位**	
	密钥：	**WPC Slot 0 ECC私钥** • 包含P-256 NIST ECC私钥 • 始终可以生成相应的公钥 • 需要随机nonce
	槽：	• 槽是机密的 • 可对外部报文进行签名
	选项2：连接到持久锁存位	
	密钥：	同上，另外还有一点： • 必须先运行安全引导，然后才能使用该密钥
	槽：	同上

表3-7. Slot 1配置信息

槽	配置值	已使能功能的说明
1	**选项1：不连接到持久锁存位**	
	密钥：	**WPC Slot 1 ECC私钥** • 包含P-256 NIST ECC私钥 • 始终可以生成相应的公钥 • 需要随机nonce
	槽：	• 槽是机密 • 可对外部报文进行签名
	选项2：连接到持久锁存位	
	密钥：	同上： • 必须先运行安全引导，然后才能使用该密钥
	槽：	同上

表 3-8. Slot 2配置信息

槽	配置值	已使能功能的说明
2	**选项1：不连接到持久锁存位**	
	密钥：	**TLS会话私钥** • 包含P-256 NIST ECC私钥 • 始终可以生成相应的公钥 • 需要随机nonce
	槽：	• 槽是机密的 • 可对外部报文进行签名 • 可与ECDH命令一起使用
	选项2：连接到持久锁存位	
	密钥：	• 与选项1相同 • 使能持久禁止选项
	槽：	• 与选项1相同

表3-9. Slot 3配置信息

槽	配置值	已使能功能的说明
3	**选项1：永久锁定**	

.....续

槽	配置值	已使能功能的说明
	密钥:	**WPC Slot 0摘要** • 包含WPC Slot 0证书链的32字节摘要 • 该槽永久锁定
	槽:	• 始终可采用明文形式读取 • 永久锁定
	选项2：槽可锁定且可写	
	密钥:	• 槽可锁定
	槽:	• 槽可采用明文形式写入 • 槽始终可读取

表 3-10. Slot 4 配置信息

槽	配置值	已使能功能的说明
4	**选项1：永久数据**	
	密钥:	**WPC槽其他数据** • 用于存储WPC Slot 0其他数据 • 槽永久锁定
	槽:	• 始终可采用明文形式读取 • 永久锁定
	选项2：槽可锁定且可写	
	密钥:	• 用于存储WPC Slot 0其他数据 • 槽可写
	槽:	• 始终可采用明文形式读取 • 槽可锁定

表 3-11. Slot 5 配置信息

槽	配置	已使能功能的说明
5	**选项1：永久数据**	
	密钥:	**WPC Slot 0其他数据（续）** • 用于存储WPC Slot 0其他数据 • 槽永久锁定
	槽:	• 始终可采用明文形式读取 • 永久锁定
	选项2：槽可锁定且可写	
	密钥:	• 用于存储WPC Slot 0其他数据 • 槽可写
	槽:	• 始终可采用明文形式读取 • 槽可锁定

表 3-12. Slot 6 配置信息

槽	配置值	已使能功能的说明
6	**选项1：槽可锁定**	
	密钥：	**I/O保护密钥** • 可包含SHA-256对称密钥或其他数据。如果未使用I/O保护密钥，则该槽可用于其他数据。 • 使用该密钥时，需要随机nonce • 该槽可以单独锁定
	槽：	• 数据可采用明文形式写入 • 该槽的内容是机密信息，无法读取 • 槽不能用于`CheckMac Copy`命令
	选项2：永久锁定	
	密钥：	• 与选项1相同，但槽永久锁定。
	槽：	• 与选项1相同，但槽无法写入

重要：通常，必须使Slot 6中存储的I/O保护密钥保持“槽可锁定”状态。在大多数情况下，I/O保护密钥对于每个器件通常都是惟一的。如果对于某些用例，所有器件的I/O保护密钥均相同，则可以选择永久锁定选项。

表 3-13. Slot 7 配置信息

槽	配置值	已使能功能的说明
7	密钥：	**安全引导摘要** • 该槽专门用于其他数据
	槽：	• 该槽无法直接写入或读取 • 该槽是机密的，无法通过`MAC`命令使用 • 该槽不能用于`CheckMac Copy`命令

表 3-14. Slot 8 配置信息

槽	配置值	已使能功能的说明
8	**选项1：槽可锁定**	
	密钥：	**WPC Slot 1数据** • 该槽专门用于WPC Slot 1数据 • 槽可锁定
	槽：	• 允许对该槽进行明文写入和读取 • 槽不能用于`CheckMac Copy`命令
	选项2：永久锁定	
	密钥：	• 与选项1相同，但槽永久锁定。
	槽：	• 与选项1相同，但槽无法写入

表 3-15. Slot 9 配置信息

槽	配置值	已使能功能的说明
9	**选项1：永久锁定<**	
	密钥：	**WPC Slot 0公钥** • 槽针对ECC密钥定义 • ECC密钥为公钥
	槽：	• 数据无法覆盖 • 数据可采用明文形式读取
	选项2：槽可锁定 *注：该配置用于原型器件*	
	密钥：	• 选项1所示的所有功能 • 槽可锁定
	槽：	• 与选项1相同，但槽可写入

表 3-16. Slot 10 配置信息

槽	配置值	已使能功能的说明
10	**选项1：永久锁定**	
	密钥：	**器件压缩证书** • 槽定义为存储其他数据
	槽：	• 数据无法覆盖 • 数据可采用明文形式读取
	选项2：槽可锁定 *注：该配置用于原型器件*	
	密钥：	• 选项1所示的所有功能 • 槽可锁定
	槽：	• 与选项1相同，但槽可写入

表 3-17. Slot 11 配置信息

槽	配置值	已使能功能的说明
11	**选项1：永久锁定**	
	密钥：	**签名人公钥** • 槽针对ECC密钥定义 • ECC密钥为公钥
	槽：	• 数据无法覆盖 • 数据可采用明文形式读取
	选项2：槽可锁定 *注：该配置用于原型器件。*	
	密钥：	• 选项1所示的所有功能 • 槽可锁定
	槽：	• 与选项1相同，但槽可写入

表 3-18. Slot 12 配置信息

槽	配置值	已使能功能的说明
12	**选项1：永久锁定**	
	密钥:	**签名人压缩证书** • 槽定义为存储其他数据
	槽:	• 数据无法覆盖 • 数据可采用明文形式读取
	选项2：槽可锁定 *注：该配置用于原型器件*	
	密钥:	• 选项1所示的所有功能 • 槽可锁定
	槽:	• 与选项1相同，但槽可写入

表 3-19. Slot 13 配置信息

槽	配置值	已使能功能的说明
13	**选项1：永久锁定**	
	密钥:	**WPC Slot 0器件压缩证书** • 槽定义为存储其他数据
	槽:	• 数据无法覆盖 • 数据可采用明文形式读取
	选项2：槽可锁定 *注：该配置用于原型器件*	
	密钥:	• 选项1所示的所有功能 • 槽可锁定
	槽:	• 与选项1相同，但槽可写入

表3-20. Slot 14 配置信息

槽	配置值	已使能功能的说明
14	**选项1：永久锁定**	
	密钥:	**WPC Slot 0 MFG压缩证书** • 槽定义为存储其他数据
	槽:	• 数据无法覆盖 • 数据可采用明文形式读取
	选项2：槽可锁定 *注：该配置用于原型器件*	
	密钥:	• 与选项1相同，但槽可写入 • 槽可锁定
	槽:	• 与选项1相同，但槽可写入

表 3-21. Slot 15配置信息

槽	配置值	已使能功能的说明
15	**选项1：槽可锁定**	
	密钥：	**安全引导公钥** • 槽针对ECC密钥定义 • 槽可锁定
	槽：	• 除非锁定，否则始终可写 • 槽始终可读取
	选项2：永久锁定	
	密钥：	• 与选项1相同，但槽永久锁定。
	槽：	• 与选项1相同，但槽无法写入

3.3 ECC608-TFLXWPC EEPROM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，用于只读存储。它分为2个块，每个块32字节。对于ECC608-TFLXWPC，OTP区域出厂时已预先锁定，其中包含以下信息：

I^2C器件版本

```
60 1B 1E 85 3B 13 C7 75 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

写入OTP区域的数据字节值始终可通过4字节或32字节读取方式进行读取，但始终不可进行修改。

重要：OTP区域中的字节可能会随时间变化。这些值不得在任何加密计算中使用。

4. 器件命令

下部分详细介绍了ECC608-TFLXWPC中允许的基于命令模式细分的所有命令，具体分为以下三类：

1. **常规器件命令**
   此类命令分为两类：
   - 常规器件访问命令，用于将数据发送到器件或检索数据，但通常不执行任何加密功能
   - 常规加密命令，可由器件或系统使用，但通常不会用于特定数据槽
2. **非对称加密命令**
   这些命令执行非对称加密操作，例如密钥生成、报文签名和报文验证（使用ECC公钥或私钥）。这些命令仅限用于ECC数据区域槽。
3. **对称加密命令**
   这些命令执行对称加密功能，例如生成摘要或MAC、密钥派生或AES加密和解密。

所有命令的输入参数

除非另有说明，否则输入参数表中的多字节输入参数以大尾数值的形式（MSB在前）显示。请注意，ECC608-TFLXWPC器件实际上希望数据以小尾数形式（LSB在前）发送。

表 4-1. 命令操作码、简要说明和命令类别

命令	说明	命令类别
Counter	读取或递增单调计数器之一	常规器件命令
ECDH	使用存储的私钥和输入公钥生成ECDH预主机密信息。	非对称加密命令
GenKey	生成ECC公钥。也可以生成ECC私钥	非对称加密命令
Info	返回器件状态信息	常规器件命令
Lock	防止进一步修改器件的某个区域或槽	常规器件命令
Nonce	生成一个32字节的随机数和一个内部存储的Nonce	常规器件命令
Random	生成一个随机数	常规器件命令
Read	从器件读取4个或32个字节，可以使用或不使用身份验证和加密	常规器件命令
SecureBoot	上电时验证代码签名或代码摘要	非对称加密命令
SelfTest	测试各种内部加密计算元素	常规器件命令
Sign	ECDSA签名计算	非对称加密命令
SHA	计算系统通用的SHA-256或HMAC摘要	常规器件命令
UpdateExtra	配置区域锁定后，更新配置区域内的byte 84或85	常规器件命令

.....续

命令	说明	命令类别
Verify	ECDSA验证计算	非对称加密命令
Write	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	常规器件命令

4.1 常规器件命令

下表总结了常规器件命令：

表4-2. 常规器件命令

命令名称	说明
Counter	递增并读取单调计数器
Info	用于从器件中读取版本和状态信息
Lock	用于锁定器件中的各个可锁定槽
Nonce	用于为器件生成或传递仅使用一次的数字
Random	用于生成供系统使用的32字节随机数
Read	用于读取器件的各个区域
SelfTest	测试各种内部加密计算元素
SHA	计算系统通用的SHA-256或HMAC摘要
UpdateExtra	配置区域锁定后，更新配置区域内的byte 84或85
Write	配置区域锁定后，更新配置区域内的byte 84或85

4.1.1 Counter命令

Counter命令在配置区域内读取器件上2个单调计数器之一的二进制计数值。此计数器可达到的最大值为2,097,151。尝试计数超出此值将导致错误代码。此计数器的设计可确保即使计数操作期间电源中断，也始终不会丢失计数。在某些电力损失的情况下，计数器可能会以超过1的值递增。

对于ECC608-TFLXWPC，计数器未关联到任何密钥，但仍可供系统使用。每个计数均设置为其默认值，并且可以计数到最大值。

4.1.2 Info命令

Info命令用于读取器件的状态。该信息对于确定错误或使用各种命令很有用。

4.1.3 Lock命令

对于ECC608-TFLXWPC，配置区域已锁定，并且数据区域的访问策略已设置。但是，仍然可以通过使用其他命令来更新几个数据槽。如有需要，可以使用Lock命令的槽锁定模式将其中一些槽永久锁定，以避免未来的更新。

4.1.4 Nonce命令

Nonce命令通过将随机数（可在内部或外部生成）与来自系统的输入值相组合来生成nonce（使用一次的数字），以供后续命令使用。得到的nonce在内部存储在三个可能的缓冲区中：TempKey缓冲区、报文摘要缓冲区和备用密钥缓冲区。如有必要，可将值传递给器件，而不是生成nonce。

4.1.5 Random命令

Random 命令生成一个随机数，以供系统使用。随机数通过内部NIST 800-90 A/B/C随机数发生器生成。该命令始终在总线上输出32字节数字。该数字不能存储在任何数据槽或SRAM单元中。

4.1.6 Read命令

Read命令可用于访问ECC608-TFLXWPC器件的任何EEPROM区域。基于为每个槽设置的访问策略，数据区域访问将受到限制。如果设置了特定的访问策略，则只能在数据区域槽上进行加密读取。

4.1.7 SelfTest命令

SelfTest命令对ECC608-TFLXWPC芯片中的一个或多个加密引擎执行测试。将根据输入模式参数测试部分或全部算法。

对于ECC608-TFLXWPC器件，SelfTest命令已被禁止，以避免在上电或唤醒事件后自动运行。但是，如有需要，可以通过系统执行该命令。无需运行该测试。

如果任何自检失败，则无论是在上电和唤醒时自动调用还是通过此命令调用，芯片都将进入故障状态，芯片操作将受限。存储的故障状态始终在唤醒或掉电再上电后清除。

4.1.8 SHA命令

SHA命令用于计算主机系统通用的SHA-256或HMAC/SHA摘要。SHA计算在ECC608-TFLXWPC内部存储器中的一个特殊区域（上下文缓冲区）执行，该区域不能被任何其他命令读取或写入。任意命令都可以穿插在SHA命令的各个阶段之间，而不会出现问题。此SHA上下文在上电和唤醒时无效。大多数情况下，如果在执行SHA命令的过程中发生错误，上下文保持不变。

4.1.9 UpdateExtra命令

UpdateExtra 命令用于更新UpdateExtra和UpdateExtraAdd字节（分别为配置区域中的byte 84和85）。这些字节只能通过此命令进行更新。这些字节是可一次性更新的字节，只能在当前值为0x00时更新。如果值不为0x00，则尝试更新此字节将导致错误。

对于ECC608-TFLXWPC器件，UpdateExtraAdd字节（byte 85）已配置为备用I^2C地址。

4.1.10 Write命令

对于ECC608-TFLXWPC，配置区域和OTP区域为锁定状态，无法更新这些区域。根据每个槽的访问策略，数据区域上的写入能力有限。该命令的子模式中描述了可写入的槽。

4.2 非对称加密命令

非对称加密命令集由专门用于生成或使用ECC密钥的命令组成。密钥通常存储在数据区域槽中，但对于某些命令，也可以存储在SRAM阵列中。

表 4-3. 非对称加密命令

命令名称	说明
ECDH	使用存储的私钥和输入公钥生成ECDH预主机密信息
GenKey	生成ECC私钥，也可选择通过存储的私钥生成ECC公钥
SecureBoot	上电时验证代码签名或代码摘要
Sign	使用ECC私钥和ECDSA签名计算对内部或外部报文摘要进行签名
Verify	使用ECC公钥和ECDSA验证计算对内部或外部报文摘要进行验证

4.2.1 ECDH命令

ECDH命令用于生成两个器件之间的共用机密信息。通过传递另一个器件中的ECC公钥并将其与存储在槽中的ECC私钥或存储在TempKey中的临时密钥进行组合，然后在另一个器件上执行相反的操作，即可让两个器件生成相同的共用预主机密信息。该机密信息随后可以进一步与双方的其他公共数据相结合，以生成两个器件之间的共用会话密钥。KDF命令通常与TLS会话一起使用，以进一步实现共用机密信息的多样化。

4.2.2 GenKey命令

GenKey命令用于生成ECC私钥，通过私钥生成ECC公钥，或者生成公钥摘要。此命令仅适用于被指定为ECC私钥或公钥的槽。在非ECC槽上运行此命令将产生错误。

4.2.3 SecureBoot命令

SecureBoot命令用于为外部MCU或MPU的安全引导提供支持。一般方法如下：系统内的引导代码将使用ECC608-TFLXWPC来协助验证随后要执行的应用程序代码。ECC608-TFLXWPC器件配置为在安全引导和存储摘要模式下工作。摘要将存储在Slot 7中，而验证安全引导所需的公钥将存储在Slot 15中。可选择将器件配置为使用持久锁存。安全引导是否与上电关联取决于选择的选项。请参见3.2.4 安全引导选项。

可以选择通过写入TempKey的nonce、IO保护机密信息和各种其他数据（具体取决于命令的模式）代替返回代码来生成MAC，以防止篡改主机与ECC608-TFLXWPC之间的线路。

4.2.4 Sign命令

Sign命令使用ECDSA算法生成签名。由KeyID指定的槽中的ECC私钥用于生成签名。该器件可提供多种模式，具体取决于要签名的内容。

4.2.5 Verify命令

Verify命令用于获取ECDSA[R,S]签名并验证其是否正确生成（给定输入报文摘要和公钥）。在所有情况下，签名都是命令的输入。

可选择让Verify命令返回MAC来防御所有中间人攻击。如果验证计算结果表明已通过输入摘要正确生成签名，则将根据存储在TempKey中的输入nonce与存储在ECC608-TFLXWPC和主机MCU中的I/O保护机密信息值计算MAC。MAC输出只能在外部和存储模式下生成。必须使能I/O保护功能才能计算MAC。

4.3 对称加密命令

对称加密命令集代表与生成或使用对称密钥有关的命令。密钥通常存储在数据区域槽中，但对于某些命令，也可以存储在SRAM存储单元中。

表 4-4. 对称加密命令

命令名称	说明
GenDig	通过随机或输入种子和存储的值生成数据摘要
MAC	使用SHA-256计算密钥和其他内部数据的摘要（响应）

4.3.1 GenDig命令

GenDig 命令使用SHA-256哈希运算将存储的或输入的值与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、配置区域、任一OTP页或单调计数器。器件的具体模式决定了GenDig计算中将包含的数据。

在某些情况下，在执行一些命令之前，需要先运行GenDig该命令可运行多次，以在执行给定命令前在摘要中包含更多数据。得到的摘要保留在TempKey中，可以通过以下四种方式之一使用：

1. 它可以作为MAC、Sign或CheckMac 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身份验证和/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写操作使用。
4. 输入值（通常是远程器件中的nonce）与当前TempKey值相结合以创建共用nonce，其中两个器件均可以证明包含RNG。

4.3.2 MAC命令

报文身份验证代码（MAC）命令用于为由存储在器件中的密钥、质询和器件上的其他信息组成的报文生成SHA-256摘要。此命令的输出为此报文的摘要。
使用此命令的正常流程如下所示：

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命令一次或多次，将器件中的存储EEPROM单元与nonce组合。结果存储在器件内部。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（即摘要）。

或者，可以通过相同的GenDig机制将任何槽中的数据（不必是机密信息）累积到响应中。其作用是验证存储在相应单元的值。

5. I²C接口

I²C接口使用SDA和SCL引脚来指示ECC608-TFLXWPC的各种I/O状态。此接口设计为在协议级别与工作在1 MHz下的Microchip AT24C16串行EEPROM兼容。

注：与AT24C16相比，这两款器件之间存在许多差异（例如，默认I²C 地址不同）；因此，设计人员必须仔细阅读相应的数据手册。

由于ECC608-TFLXWPC从器件的输出引脚上仅包含一个开漏驱动器，因此SDA引脚通常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 ECC608-TFLXWPC在总线上驱动结果时必须是三态的。SCL引脚为输入，必须始终由外部器件或电阻驱动为高电平和低电平。

注意事项： 对于I²C标准中使用的术语“Master”和“Slave”，本文档的英文版中使用了与之等效的Microchip术语“Host”和“Client”。

5.1 I/O条件

器件响应以下I/O条件：

5.1.1 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——当SDA保持低电平的时间 ≥ t_{WLO}后，器件将在SDA的上升沿退出低功耗模式。在t_{WHI}的延时后，器件将准备好接收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5.1.2 器件唤醒中列出的条件。

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，可使用正常的处理器I²C硬件和/或软件进行器件通信，其中包括使器件重新进入低功耗（即休眠）模式所需的I/O序列。

提示：以100 kHz的频率发送字节0x00即可轻松生成唤醒脉冲。后续命令可采用更高的频率运行。

在I²C模式下，器件将忽略器件已经唤醒时发送的唤醒序列。

总线上有多个器件

当总线上有多个器件并且I²C接口以低于~300 kHz的速度运行时[1]，传输某些数据模式将使总线上的ECC608-TFLXWPC器件唤醒。频率越低，器件唤醒的概率就越高。由于沿总线传输的后续器件地址只匹配所需的器件，因此ECC608-TFLXWPC不会作出响应，但会唤醒。在以较低频率与另一个器件通信后，建议发出休眠或空闲序列以使ECC608-TFLXWPC 返回已知状态。

[1] 给定器件的实际频率将随过程和环境因素而变化。该值被认为在所有条件下都是安全的。

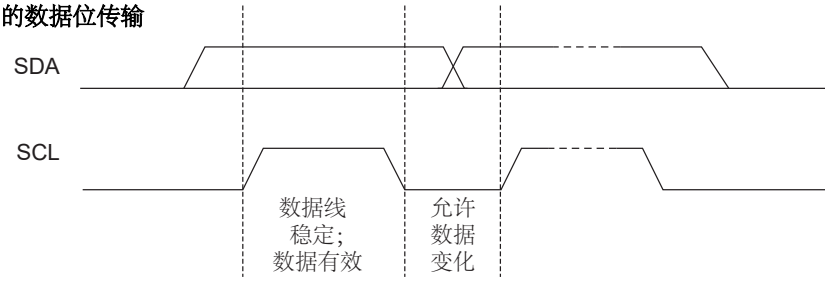
重要：t_{WLO}是系统为确保ECC608-TFLXWPC在所有制造和环境条件下都能够唤醒而必须提供的最短时间。实际上，器件可能会以较小的脉冲宽度唤醒。

5.1.2 器件唤醒

当器件唤醒时，它将遵循下列条件：

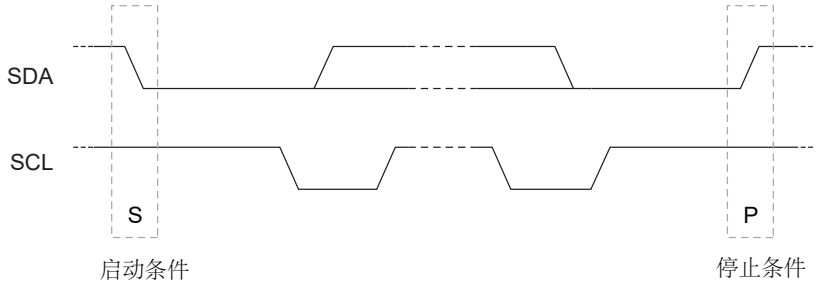
- 数据0：如果SDA为低电平且保持稳定，而SCL由低电平变为高电平再变为低电平，则将在总线上传输一个0位。当SCL为低电平时，SDA可发生变化。
- 数据1：如果SDA为高电平且保持稳定，而SCL由低电平变为高电平再变为低电平，则将在总线上传输一个1位。当SCL为低电平时，SDA可发生变化。

图5-1. I²C接口上的数据位传输



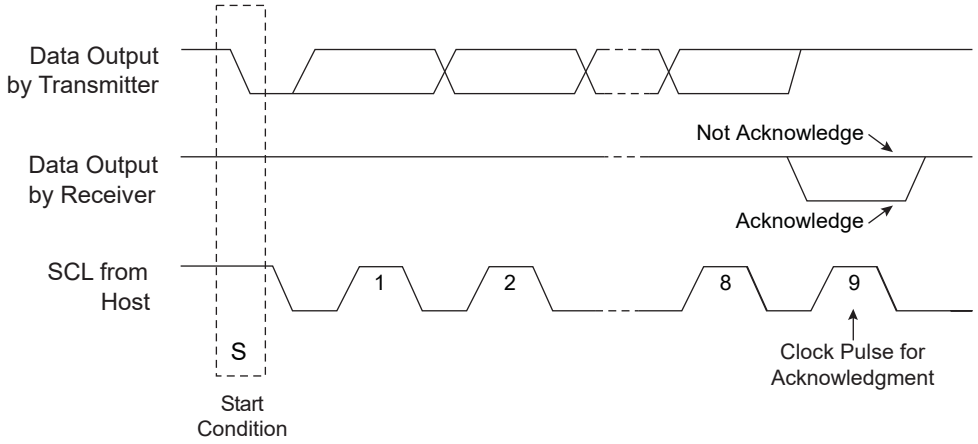
- **启动条件：**必须将SDA从高电平转换为低电平且SCL为高电平作为优先于所有命令的启动条件。
- **停止条件：**SDA线从低电平转换为高电平且SCL为高电平为停止条件。器件收到此条件后，当前的I/O事务结束。在输入端，如果器件有足够的字节来执行命令，则器件转换到繁忙状态并开始执行。务必在发送到器件的任何数据包的末尾发送停止条件。

图5-2. 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，或者此字节完成组传输。

图5-3. I²C接口上的NACK和ACK条件



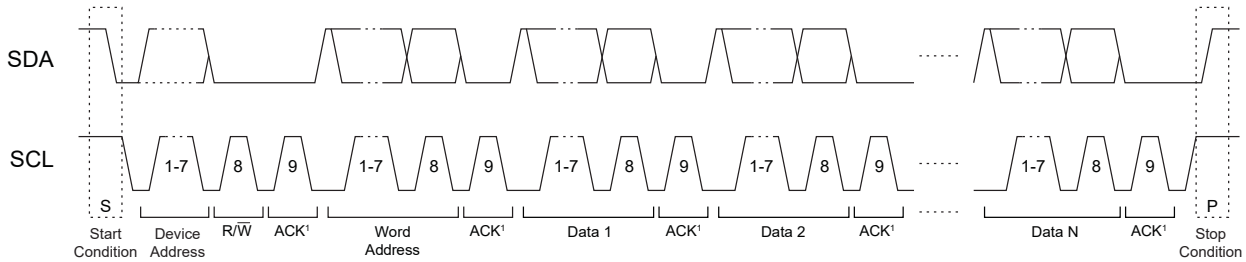
如果配置区域中的I2C_Address字节针对总线上的每个器件以不同方式编程，则多个ECC608-TFLXWPC器件可轻松共用同一I²C接口信号。由于器件地址的全部7个位均可编程，因此ECC608-TFLXWPC还可将I²C接口与任何I²C器件（包括任何串行EEPROM）共用。

5.2 至ECC608-TFLXWPC的I²C传输

下图总结了从系统到ECC608-TFLXWPC的数据传输。传输顺序如下：

- 起始条件
- 器件地址字节
- 字地址字节
- 可选数据字节（1至N）
- 停止条件

图5-4. 至ECC608-TFLXWPC的正常I²C传输



ACK周期将SDA驱动为低电平。

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

表5-1. 到ECC608-TFLXWPC的I²C传输

名称	I²C名称	说明
器件地址	器件地址	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ECC608-TFLXWPC。此字节的bit 0是标准I²C R/W位，必须为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）。
字地址	字地址	要正常工作，此字节的值必须为0x03。

.....续		
名称	I²C 名称	说明
命令	数据1，N	由计数、命令数据包和2字节CRC组成的命令组。CRC通过大小和数据包字节计算。

由于器件将命令输入缓冲区视为FIFO，因此输入组可通过一个或多个I²C命令组发送到器件。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ECC608-TFLXWPC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，请参见 5.2.2 I2C同步。

相关链接

5.2.1 字地址字节

5.2.1 字地址值

在I²C写数据包期间，ECC608-TFLXWPC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5-2. 字地址值

名称	值	说明
复位	0x00	复位地址计数器。下一个I²C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	ECC608-TFLXWPC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	ECC608-TFLXWPC进入空闲模式，忽略所有后续的I/O转换，直到下一个唤醒标志。TempKey、MessageDigestBuffer和备用密钥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	这些地址不得发送到器件。

5.2.2 I²C同步

系统可能会由于系统复位、I/O噪声或其他条件而失去与ECC608-TFLXWPC I/O端口的同步。在这种情况下，ECC608-TFLXWPC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。要重新同步，可按照以下步骤操作：

1. 为了确保I/O通道复位，系统必须发送标准 I²C软件复位序列，具体如下：
   - 一个启动位条件
   - 九个SCL周期，通过系统上拉电阻使SDA保持高电平
   - 另一个启动位条件
   - 一个停止位条件

然后可能可以发送一个读序列，如果同步正确完成，ECC608-TFLXWPC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，系统必须复位内部地址计数器，强制ECC608-TFLXWPC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，系统必须发送一个完整的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。系统必须等待最长t_{EXEC}（最大值），然后发送读取序列，这将由器件确认。

5.3 休眠序列

建议让系统在使用完ECC608-TFLXWPC后发出休眠序列，以将器件置于低功耗模式。此序列包含正确的器件地址，接着是值0x01（作为字地址），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。

5.4 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模式可防止此操作。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。

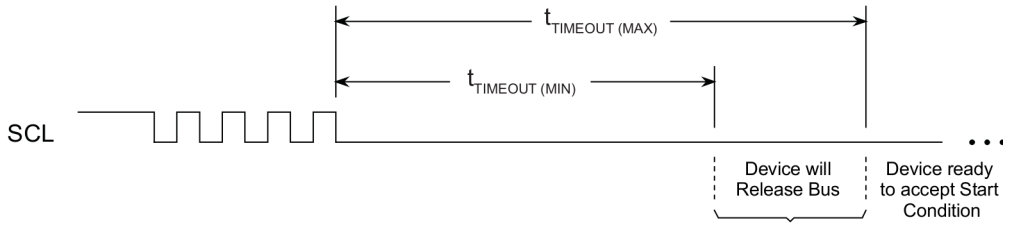
此空闲序列包含正确的器件地址，接着是值0x02（作为字地址），然后是停止条件。当器件唤醒且不忙时，此序列可随时发送到器件。

5.5 SMBus超时

ECC608-TFLXWPC支持SMBus超时功能，如果SCL引脚保持低电平的时间超过最小$t_{TIMEOUT}$规范值，ECC608-TFLXWPC将复位其串行接口并释放SMBus（即，停止驱动总线并使SDA悬空为高电平）。

当达到$t_{TIMEOUT}$时，器件将进入休眠模式。一旦最大$t_{TIMEOUT}$结束，ECC608-TFLXWPC将准备接受新的唤醒序列，然后是启动条件。

图 5-5. SMBus 超时



5.6 自ECC608-TFLXWPC的I²C传输

当ECC608-TFLXWPC唤醒且不繁忙时，主器件可以使用I²C读取从器件中获取当前输出缓冲区内容。如果有效的命令结果可用，则返回的组大小由已经运行的特定命令决定。否则，组大小（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。

表5-3. 自ECC608-TFLXWPC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字节的bit 1至bit 7匹配，则将选择ECC608-TFLXWPC。此字节的bit 0是标准I²C R/W引脚，必须为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）组成的输出组。

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ECC608-TFLXWPC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ECC608-TFLXWPC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。如果部分命令已经发送到器件，并且读取序列`[Start + DeviceAddress(R/W == R)]`发送到器件，则ECC608-TFLXWPC将不会确认器件地址以指示没有数据可供读取。

相关链接

7.3.1 AC参数：I2C接口

6. 应用信息

ECC608-TFLXWPC是Microchip Trust CryptoAuthentication™产品系列的成员。TrustFLEX 产品使用方便，易于实现，甚至允许小批量生产的用户在其最终系统中实现安全性，同时可利用Microchip的专业知识和基础架构进行安全配置。

ECC608-TFLXWPC器件旨在省去为符合Qi标准的无线充电发射器增加安全性时的猜测工作。该产品经过预先配置，可轻松存储一个或两个WPC槽证书链。如果未使用WPC Slot 1证书链，则可用于存储与WPC Slot 2关联的专有证书链。

此外，与ATECC608B-TFLXTLS和ATECC608B-TNGTLS产品一样，ECC608-TFLXWPC器件也支持无缝连接到IoT Cloud。这样，便可以在餐厅和酒店等行业的基础设施应用中部署无线充电连接。如果需要，还可以使用器件中支持的安全引导功能在连接到云端之前对无线充电发射器中的单片机进行固件检查。

除了实际的安全器件之外，Microchip还开发了一系列工具，这些工具可与其硬件器件无缝集成，从而为开发整个安全解决方案提供一种简便途径。当开发人员使用Microchip的软件安全工具时，可以消除其自行设置基础架构的复杂性，并且能够快速地实现初始原型设计和生产。

6.1 WPC相关信息

所有公司都必须先成为无线充电联盟的成员才能销售Qi认证产品。所有打算以Qi认证名义销售的产品都必须通过Qi验证、测试和认证程序。如果产品未通过适当的验证和测试程序，则不可声称符合Qi标准或通过Qi认证。Qi认证产品的制造商必须在无线充电联盟中具有良好的信誉。

对于需要身份验证的Qi 1.3产品，还需要额外的措施。如果实体希望生产具有身份验证的产品，必须获得作为Qi认证制造商的许可。需要进行身份验证的产品必须配备可安全存储ECC P-256私钥的安全存储子系统（SSS）。提供SSS的公司必须是经过WPC Qi许可的制造证书颁发机构。Microchip有多种产品满足SSS的要求，ECC608-TFLXWPC就是其中一种。Microchip是经过Qi认证的制造CA。

请注意，制造商负责从经过Qi认证的供应商处挑选SSS，而制造商CA负责验证制造商在WPC中是否具有良好的信誉。

安全生产配置流程

以下是WPC量产器件的典型配置流程：

1. 客户使用ECC608-TFLXWPC着手开发工作。
2. 客户为配置的SSS提交Microchip Sales Force支持ticket。
3. 客户通过支持ticket系统向Microchip提供PTMC和Qi ID。
4. Microchip与WPC共同验证PTMC和Qi ID以确认所有权。
5. 验证后，Microchip会生成适当的证书并设置证书签名请求，以便WPC根CA对制造证书进行签名。（注：可能发生这种情况时，请与WPC联系。）
6. 签名过程完成后，Microchip将生成数量有限的验证器件供客户评估。评估包括验证器件是否正确编程以及是否满足客户的所有要求。
7. 客户通知Microchip验证器件被接受。
8. 客户继续完成WPC认证测试。
9. 成功完成后，客户可以申请满负荷量产器件和相应数量。

6.2 用例

ECC608-TFLXWPC定义为专门满足WPC Qi充电市场的身份验证需求。Microchip是WPC的授权制造CA。除了安全IC之外，Microchip还为无线充电市场提供了带和不带身份验证的完整电源接收器和电源发射器解决方案。

安全TLS连接
ECC608-TFLXWPC允许使用多种协议创建安全的TLS连接。此应用超出了WPC身份验证要求的规范，但它被视为Qi发射器得以在Qi基础设施市场激增的重要因素。

安全引导
保护单片机或微处理器的引导映像是许多供应商关注的问题。通过提供一种机制来验证正在运行的代码真实且未被修改，可以维护系统的整体完整性。已配置为允许通过将系统的代码摘要存储在器件的数据槽中来实现安全引导。最初执行代码后，系统可以通过系统固件重新生成摘要，并将其与存储在ECC608-TFLXWPC中的摘要进行比较，验证固件未遭到篡改。此外，在安全引导发生之前，可以根据器件配置阻止对TLS或WPC发射器的身份验证。

通用数据存储
有时需要为给定系统存储少量的其他信息。可以使用ECC608-TFLXWPC来实现此目的，即使用数据可随时读写的数据槽。这样便无需添加额外的EEPROM存储器件来存储数据。

6.3 开发工具

ECC608-TFLXWPC受多种软硬件工具以及后端服务支持，可快速开发应用程序。初始开发可以从一系列易于使用的Trust Platform Design Suite工具开始。这些工具以图形方式来实现您的用例，最终会输出实现应用程序所需的C代码。

如果预定义的Trust Platform Design Suite工具无法提供您所需要的应用程序，则可以使用CryptoAuthLib或Python®版本的CryptoAuthLib和CryptoAuthTools来开发应用程序。CryptoAuthLib同时也是Trust Platform Design Suite工具所输出的代码的主干。

可以结合使用硬件工具和ECC608-TFLXWPC器件样片来全面验证您的应用程序。器件的访问策略已设置，因此，重点仅围绕开发系统级代码。

当应用程序开发完毕后，即可访问Microchip直销网站订购ECC608-TFLXWPC器件。

6.3.1 可信平台设计套件

为了简化实现过程，Microchip开发了一套基于Web的可信平台设计套件工具，可引导开发人员按照流程从概念阶段过渡到生产阶段。借助这些工具，可以在ECC608-TFLXWPC的配置和所定义访问策略的限制下开发和构建实现特定应用程序所需的事务图和代码。

注：有关这些工具的更多信息，请访问Microchip的可信平台信息页面。

6.3.2 硬件工具

使用ECC608-TFLXWPC进行开发时，有多种硬件工具可为用户提供帮助。关于此处未提及的其他工具的可用性信息，请访问Micochip网站。特定用例示例还会提及特定工具。

DM320118——CryptoAuthentication可信平台
DM320118是一款紧凑的开发系统，其中包含ATSAMD21单片机（ATECC608B-TNGTLS、ATECC608B-TFLXTLS 和ATECC608B-TCSTM可信器件各一个）、USB集线器、mikroBUS连接器和板上调试器。该工具包旨在与Trust Platform Design Suite工具搭配使用，后者用于实现与各种可信器件关联的各种用例。该工具包可与MPLAB® X或Microchip Studio Design环境搭配使用，以开发其他应用程序。通过使用mikroBUS附加板，该工具包可与ECC608-TFLXWPC配合使用。

DM320109——CryptoAuthentication入门工具包
DM320109由ATSAMD21-XPRO开发板组成，该开发板预编程了可与CryptoAuthentication器件搭配使用的固件。该工具包随附AT88CKSCKTSOIC-XPRO插座板，但您需要获得该插座板的UDFN版本才能与当前仅以UDFN封装提供的器件样片搭配使用。ECC608-TFLXWPC的特定样片需要单独获取。

AT88CKSCKTUDFN(SOIC)-XPRO
AT88CKSCKTUDFN-XPRO和AT88CKSCKTSOIC-XPRO是通用的CryptoAuthentication插座工具包，可与任何具有XPRO接口的单片机开发板搭配使用。必须获取ECC608-TFLXWPC的特定样片才能与这些工具包搭配使用。

Microchip无线电源解决方案
我们还提供基于dsPIC®数字信号控制器的完整无线功率发射器和接收器。Microchip解决方案包括需要身份验证的Qi 1.3解决方案、Qi 1.2解决方案以及其他专有解决方案。有关所有Microchip无线电源解决方案的更多信息，请访问www.microchip.com/en-us/solutions/power-management-and-conversion/intelligent-power/wireless-power。

6.3.3 CryptoAuthLib

CryptoAuthLib是一个支持Microchip CryptoAuthentication器件系列的软件库。Microchip建议在使用ECC608-TFLXWPC进行开发时使用该库。该库实现了执行本数据手册中详述的命令所需的API调用。

该库实现后可以很容易地与多款Microchip单片机配合使用，但也可通过硬件抽象层（Hardware Abstraction Layer，HAL）轻松扩展为支持其他单片机，包括其他供应商生产的单片机。

有关这些工具的更多详细信息，请查看以下信息：

- CryptoAuthLib – Web Link
- CryptoAuthLib – GitHub

API调用
数据手册中的每个命令都有一个或多个与其关联的API调用。通常，命令有一个基本的API调用，可以在其中指定所有输入参数。命令和各小节中显示的参数可与该命令一起使用。每个API调用还有多种模式变体。下表列出了命令和基本API调用的示例。有关最准确的API信息，请参见GitHub信息。

表6-1. CryptoAuthLib API调用的示例命令

器件命令	API调用	备注
Info	atcab_info_base()	
Write	atcab_write()	
Read	atcab_read_zone()	
SHA	atcab_sha_base()	
Sign	atcab_sign_base()	
Random	atcab_random()	

.....续		
器件命令	API 调用	备注
Verify	atcab_verify()	

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
任何 **-0.5V**至 **(V_{CC} + 0.5V)** 引脚的电压	-0.5V至(V_{CC} + 0.5V)
ESD 额定值:	
人体模型（**Human Body Model**，**HBM**）**ESD**	>4 kV
充电器件模型（**Charge Device Model**，**CDM**）**ESD**	>1 kV

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

ECC608-TFLXWPC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
+85°C时的耐写入次数（每个字节）	400,000	—	—	写周期
+55°C时的数据保持时间	10	—	—	年
+35°C的数据保持时间	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

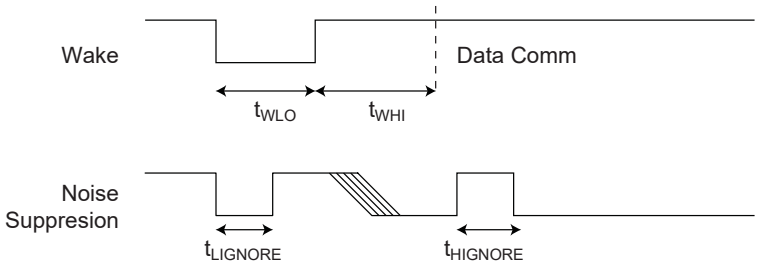


表 7-2. 交流参数：所有I/O接口

参数	符号	方向	最小值	典型值	最大值	单位	条件
上电延时[2]	t_{PU}	至加密器件	100	—	—	µs	从VCC > VCC min到t_{WLO}开始的最短时间。
唤醒为低电平的持续时间	t_{WLO}	至加密器件	60	—	—	µs	—
唤醒为高电平到数据通信的延时	t_{WHI}	至加密器件	1500	—	—	µs	除非实现了轮询，否则建议使SDA在整个过程中保持稳定的高电平状态。上电时不使能自检。
使能自检时唤醒为高电平的延时	t_{WHIST}	至加密器件	20	—	—	ms	除非实现了轮询，否则建议使SDA在整个过程中保持稳定的高电平状态。
上桥臂毛刺滤波器激活时间	$t_{HIGNORE_A}$	至加密器件	45[1]	—	—	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	$t_{LIGNORE_A}$	至加密器件	45[1]	—	—	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	$t_{LIGNORE_S}$	至加密器件	15[1]	—	—	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	$t_{WATCHDOG}$	至加密器件	0.7	1.3	1.7	s	从唤醒到强制器件进入休眠模式的时间（Config.ChipMode[2]为0时）。

注：
1. 这些参数为特性值，但未经生产测试。
2. 如果在配置区中使能了上电自检，则上电延时将显著延长。

7.3.1 交流参数：I²C接口

图7-2. I²C同步数据时序

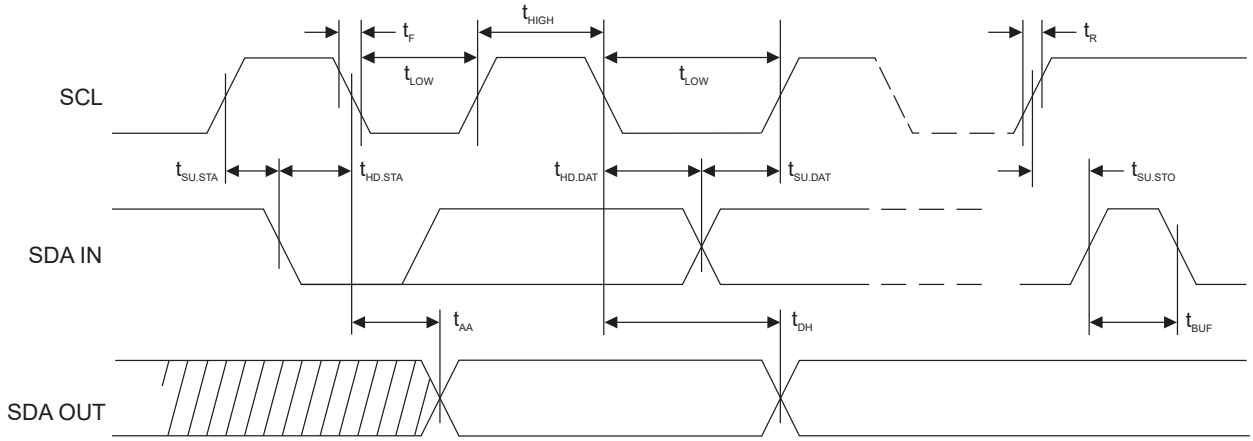


表 7-3. I²C接口的交流特性(2)

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，C_L = 1 TTL栅极和100 pF。

参数	符合	最小值	最大值	单位
SCL时钟频率	f_{SCL}	0	1	MHz
SCL高电平时间	t_{HIGH}	400	—	ns
SCL低电平时间	t_{LOW}	400	—	ns
启动建立时间	$t_{SU.STA}$	250	—	ns
启动保持时间	$t_{HD.STA}$	250	—	ns
停止建立时间	$t_{SU.STO}$	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	35	ms
在新的传输启动之前总线必须保持空闲的时间[1]	t_{BUF}	500	—	ns

注：

1. 相关值均为表征值，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：0.3V_{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 7-4. 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	标准工业级温度范围
电源电压	V_{CC}	2.0	—	5.5	V	—
电源工作电流	I_{CC}	—	2	3	mA	在I/O传输或非ECC命令执行期间等待I/O。与时钟分频值无关。
		—	—	14	mA	在ECC命令执行期间。时钟分频比 = 0x0
电源空闲电流	I_{IDLE}	—	800	—	µA	当器件处于空闲模式时， VSDA和VSCL < 0.4V或 > VCC – 0.4
休眠电流	I_{SLEEP}	—	30	150	nA	当器件处于休眠模式时，VCC ≤ 3.6V， VSDA和VSCL < 0.4V或 > VCC – 0.4，TA ≤ +55°C
		—	—	2	µA	当器件处于休眠模式时。 在整个VCC和温度范围内。

.....续

参数	符号	最小值	典型值	最大值	单位	条件
输出低电平电压	V_{OL}	—	—	0.4	V	当器件处于工作模式时，V_{CC} = 2.5至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至5.5V，V_{OL} = 0.4V
热阻JA	Θ_{JA}	—	166	—	°C/W	SOIC（SSH）
		—	173	—	°C/W	UDFN（MAH）

7.4.1 V_{IH}和V_{IL}规范

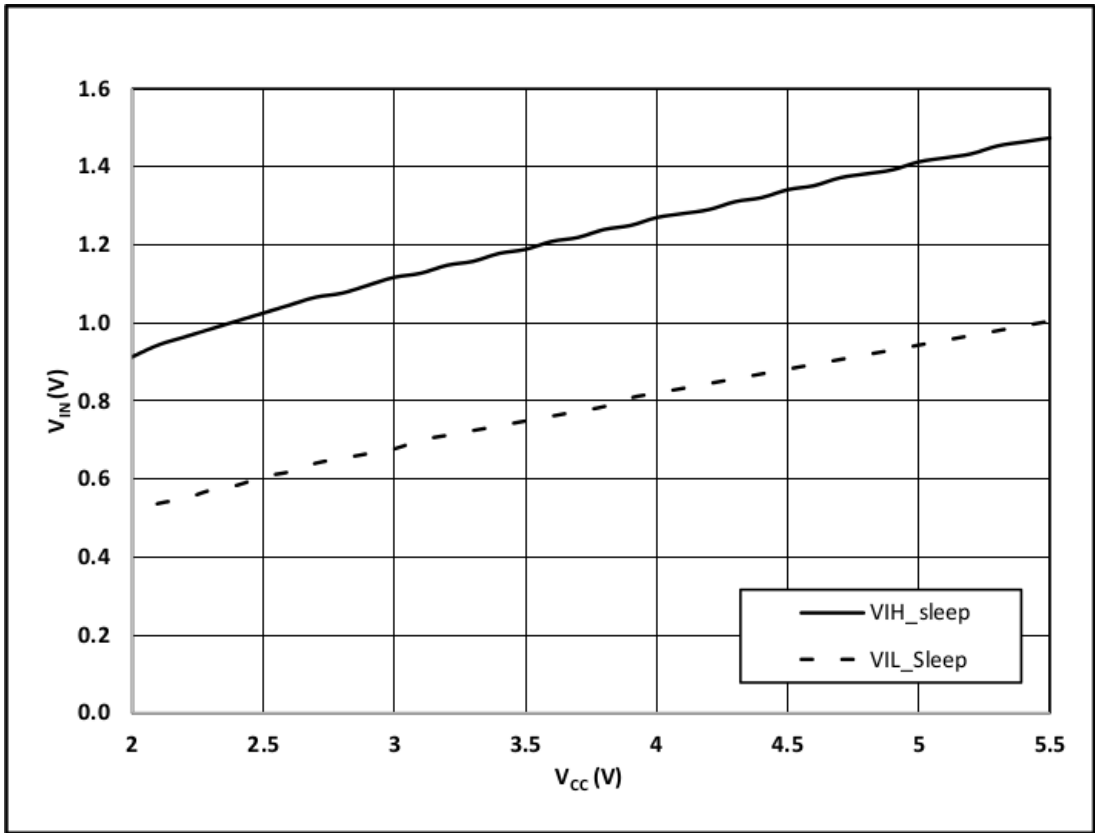
器件的输入电平将根据器件的模式和电压而变化。处于休眠或空闲模式时的输入电压阈值取决于VCC电平，如图7-3所示。在休眠或空闲模式下，TTLenable位没有任何作用。

ECC608-TFLXWPC的有效输入电平是固定的，不随V_{CC}电平而变化。传输到器件的输入电平必须符合下表。

表 7-5. 所有I/O接口上的V_{IL}和V_{IH}（TTLenable = 0）

参数	符号	最小值	典型值	最大值	单位	条件
输入低电平电压	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。
输入高电平电压	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 **7-3.**休眠和空闲模式下的V_{IH}和V_{IL}



8. 封装图

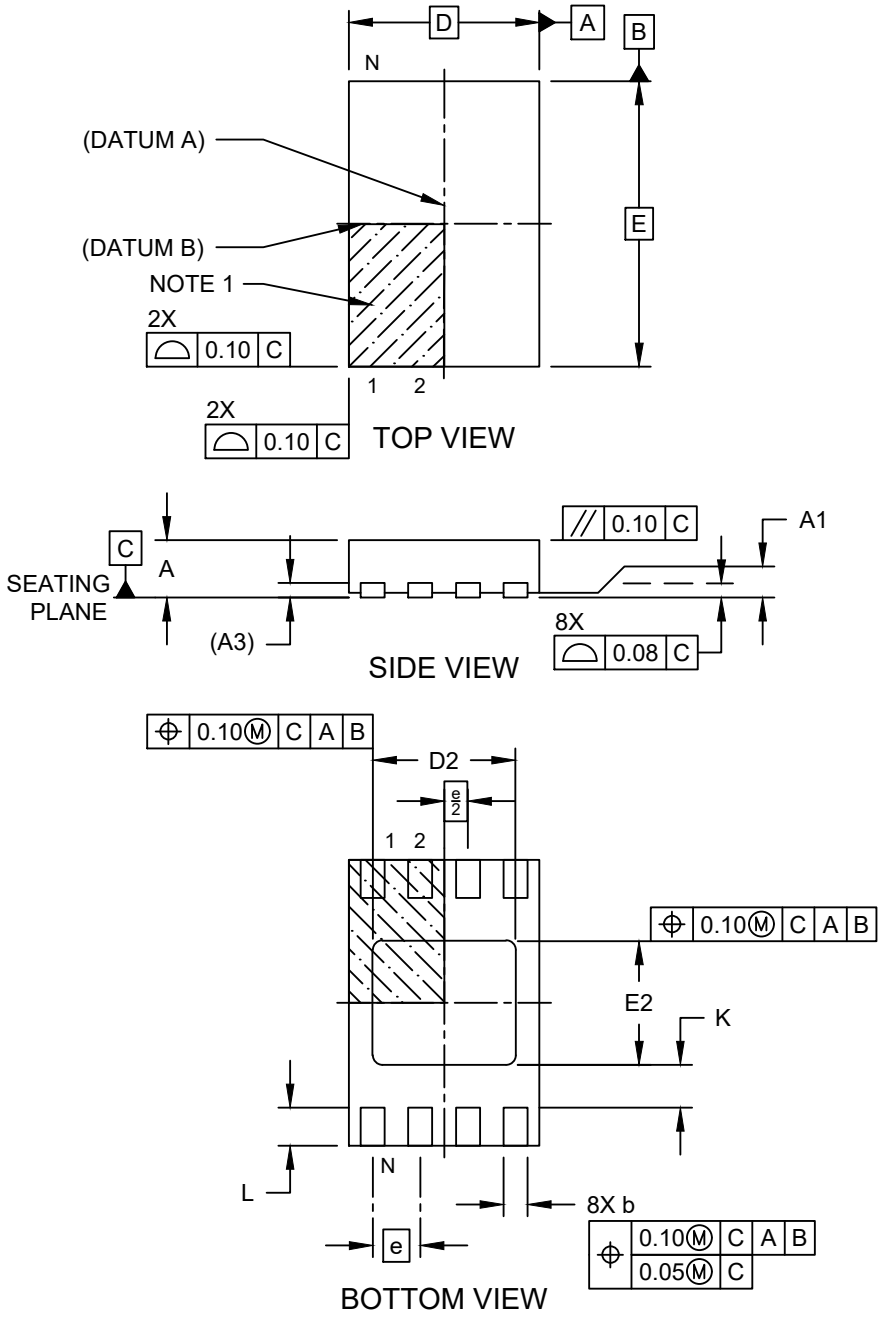
8.1 封装标识信息

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。建议不要将封装标识作为即将进行的任何检查步骤的一部分。

8.2 8焊盘UDFN

8引脚超薄塑封双列扁平无引线封装（Q4B）——主体2x3 mm [UDFN]
原Atmel全球封装代码YNZ

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

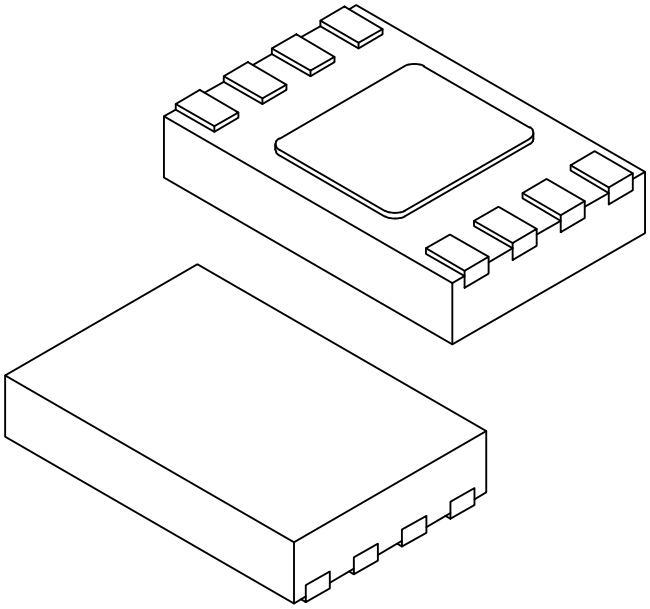


Microchip Technology Drawing C04-21355-Q4B Rev B Sheet 1 of 2

© 2017 Microchip Technology Inc.

8引脚超薄塑封双列扁平无引线封装（Q4B）——主体2x3 mm [UDFN]
原Atmel全球封装代码YNZ

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:

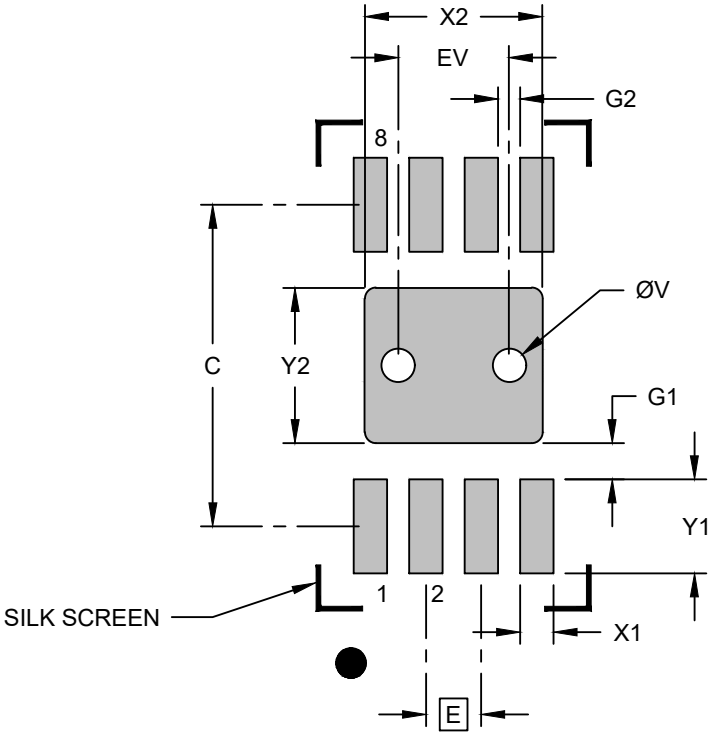
1. Pin 1 visual index feature may vary, but must be located within the hatched area.
2. Package is saw singulated
3. Dimensioning and tolerancing per ASME Y14.5M
   BSC: Basic Dimension. Theoretically exact value shown without tolerances.
   REF: Reference Dimension, usually without tolerance, for information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

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

© 2017 Microchip Technology Inc.

8引脚超薄塑封双列扁平无引线封装（Q4B）——主体2x3 mm [UDFN]
原Atmel全球封装代码YNZ

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	0.33		
Contact Pad to Contact Pad (X6)	G2	0.20		
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

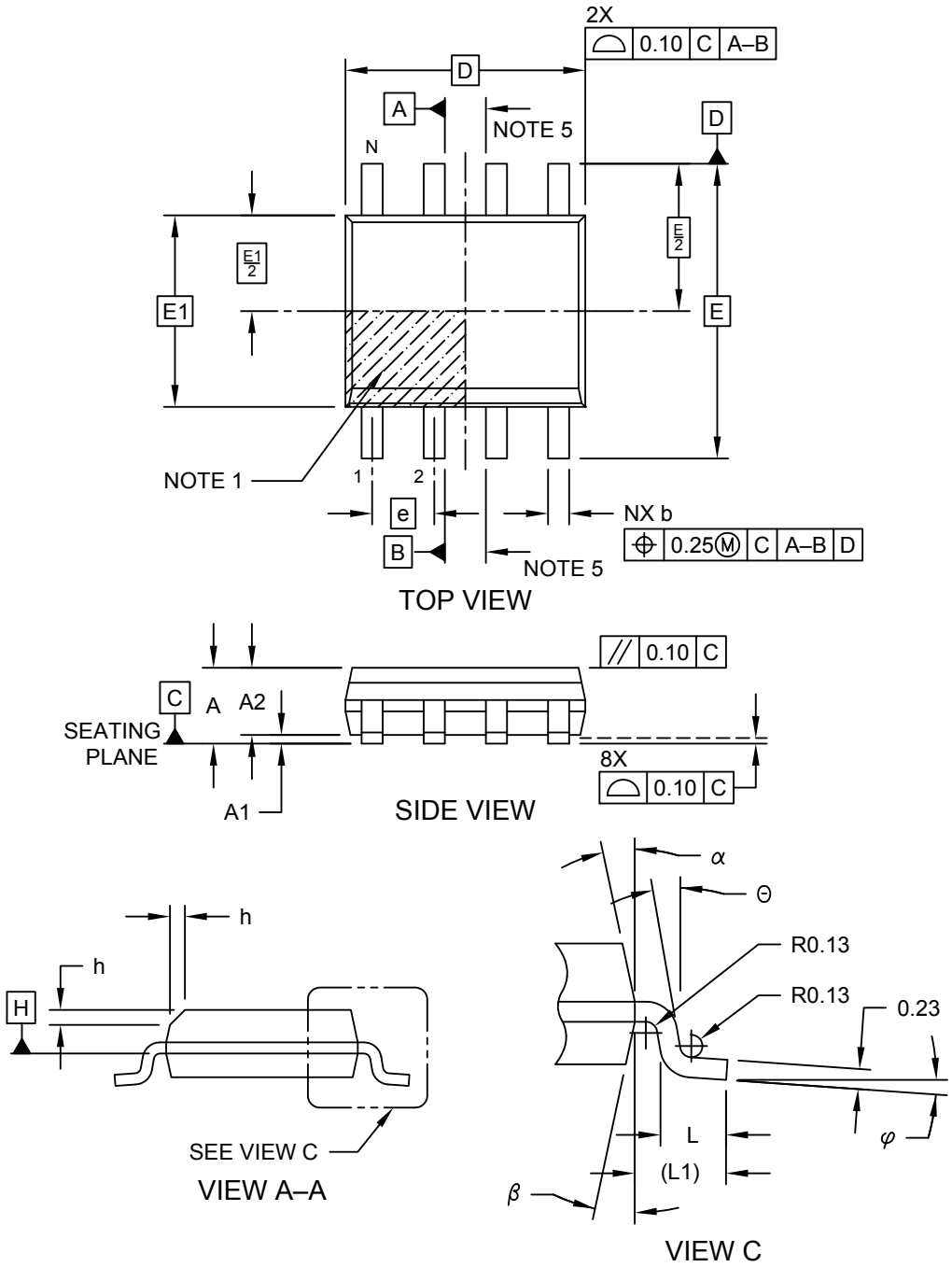
Microchip Technology Drawing C04-23355-Q4B Rev B

© 2017 Microchip Technology Inc.

8.3 8引脚SOIC

8引脚塑封窄条小外形封装，主体3.90 mm（0.150英寸）[SOIC]
原Atmel全球封装代码SWB

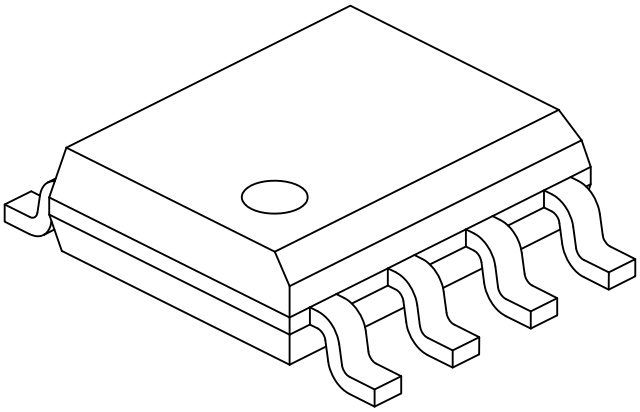
Note:	For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



Microchip Technology Drawing No. C04-057-SWB Rev E Sheet 1 of 2

8引脚塑封窄条小外形封装，主体3.90 mm（0.150英寸）[SOIC]
原Atmel全球封装代码SWB

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°

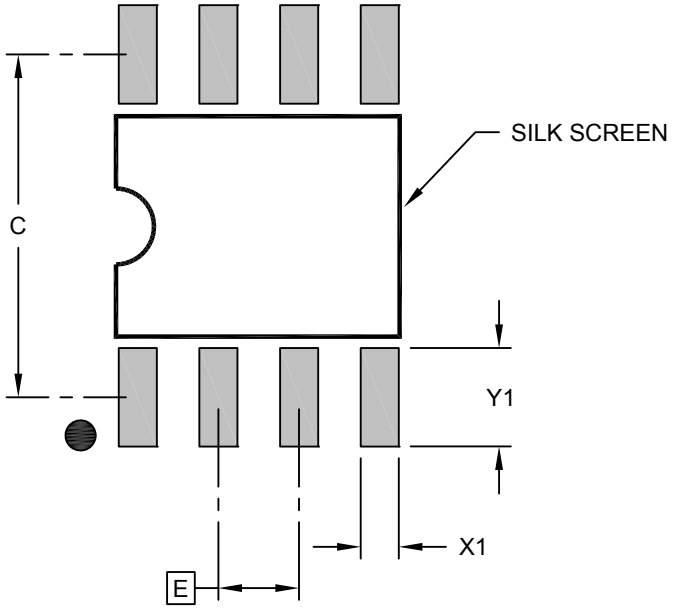
Notes:

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-SWB Rev E Sheet 2 of 2

8引脚塑封窄条小外形封装，主体3.90 mm（0.150英寸）[SOIC]
原Atmel全球封装代码SWB

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-SWB Rev E

9. 版本历史

版本A （2021年9月）
本文档的初始版本。

Microchip 网站

Microchip 网站（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。我们的网站提供以下内容：

- **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**——常见问题解答（FAQ）、技术支持请求、在线讨论组以及 Microchip 设计伙伴计划成员名单
- **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

产品变更通知服务

Microchip 的产品变更通知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，请访问 www.microchip.com/pcn，然后按照注册说明进行操作。

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（ESE）
- 技术支持

客户应联系其代理商、代表或 ESE 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 www.microchip.com/support 获得网上技术支持。

产品标识体系

欲订货或获取价格、交货等信息，请与工厂或当地销售办事处联系。

部件编号	X	-X
器件	封装类型	卷带式

器件：	ECC608-TFLXWPC：具有基于硬件的安全密钥存储功能的预配置加密协处理器	
封装选项	U	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引线封装（UDFN）
	S	8引脚（主体宽0.150”）塑封鸥翼小外形封装（JEDEC® SOIC）
卷带式选项		2k卷盘
	PROTO	每批10件——原型器件

示例：

- ECC608-TFLXWPCU：TrustFLEX TLS，预配置，8-UDFN，2K卷盘MOQ和I²C接口
- ECC608-TFLXWPCU-PROTO：TrustFLEX TLS，预配置原型，8-UDFN，每批10件，SWI或I²C接口
- ECC608-TFLXWPCS：TrustFLEX TLS，预配置，8-SOIC 2K卷盘MOQ和I²C接口
- ECC608-TFLXWPCS-PROTO：TrustFLEX TLS，预配置原型，8-SOIC，每批10件，I²C接口

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。

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规范。
- Microchip 确信：在正常使用且符合工作规范的情况下，Microchip 系列产品非常安全。
- Microchip 注重并积极保护其知识产权。严禁任何试图破坏 Microchip 产品代码保护功能的行为，这种行为可能会
- 违反《数字千年版权法案》（Digital Millennium Copyright Act）。
- 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。

法律声明

提供本文档的中文版本仅为了便于理解。请勿忽视文档中包含的英文部分，因为其中提供了有关 Microchip 产品性能和使用情况的有用信息。Microchip Technology Inc.及其分公司和相关公司、各级主管与员工及事务代理机构对译文中可能存在的任何差错不承担任何责任。建议参考 Microchip Technology Inc.的英文原版文档。

本出版物及其提供的信息仅适用于 Microchip 产品，包括设计、测试以及将 Microchip 产品集成到您的应用中。以其他任何方式使用这些信息都将被视为违反条款。本出版物中的器件应用信息仅为您提供便利，将来可能会发生更新。如需额外的支持，请联系当地的 Microchip 销售办事处，或访问 https://www.microchip.com/en-us/support/design-help/client-supportservices。

Microchip“按原样”提供这些信息。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，包括但不限于针对非侵权性、适销性和特定用途的适用性的暗示担保，或针对其使用情况、质量或性能的担保。

在任何情况下，对于因这些信息或使用这些信息而产生的任何间接的、特殊的、惩罚性的、偶然的或间接的损失、损害或任何类型的开销，Microchip 概不承担任何责任，即使 Microchip 已被告知可能发生损害或损害可以预见。在法律允许的最大范围内，对于因这些信息或使用这些信息而产生的所有索赔，Microchip 在任何情况下所承担的全部责任均不超出您为获得这些信息向 Microchip 直接支付的金额（如有）。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损害、索赔、诉讼或费用时，会维护和保障 Microchip 免于承担法律责任。除非另外声明，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 和 XMEGA 均为 Microchip Technology Incorporated 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、Precision Edge、ProASIC、ProASIC Plus、ProASIC Plus 徽标、Quiet-Wire、SmartFusion、SyncWorld、Temux、TimeCesium、TimeHub、TimePictra、TimeProvider、Vite、WinPath 和 ZL 均为 Microchip Technology Incorporated 在美国的注册商标。

Adjacent Key Suppression、AKS、Analog-for-the-Digital Age、Any Capacitor、AnyIn、AnyOut、BlueSky、BodyCom、CodeGuard、CryptoAuthentication、CryptoAutomotive、CryptoCompanion、CryptoController、dsPICDEM、dsPICDEM.net、Dynamic Average Matching、DAM、ECAN、EtherGREEN、In-Circuit Serial Programming、ICSP、INICnet、Inter-Chip Connectivity、JitterBlocker、KleerNet、KleerNet 徽标、memBrain、Mindi、MiWi、MPASM、MPF、MPLAB Certified 徽标、MPLIB、MPLINK、MultiTRAK、NetDetach、Omniscient Code Generation、PICDEM、PICDEM.net、PICkit、PICtail、PowerSmart、PureSilicon、QMatrix、REAL ICE、Ripple Blocker、SAM-ICE、Serial Quad I/O、SMART-I.S.、SQI、SuperSwitcher、SuperSwitcher II、Total Endurance、TSHARC、USBCheck、VariSense、ViewSpan、WiperLock、Wireless DNA 和 ZENA 均为 Microchip Technology Incorporated 在美国和其他国家或地区的商标。

SQTP 是 Microchip Technology Incorporated 在美国的服务标记。

Adaptec 徽标、Frequency on Demand、Silicon Storage Technology 和 Symmcom 为 Microchip Technology Inc.在其他国家或地区的注册商标。

GestIC 是 Microchip Technology Inc.的子公司 Microchip Technology Germany II GmbH & Co. KG 在除美国外的国家或地区的注册商标。

在此提及的所有其他商标均为各持有公司所有。

© 2022，Microchip Technology Incorporated. 版权所有。

ISBN：978-1-6683-1232-2

质量管理体系

有关 Microchip 的质量管理体系的信息，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. Chandler, AZ 85224-6199 电话：480-792-7200 传真：480-792-7277 技术支持： 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：45-4485-5910 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