AN2237

从 ATECC608A 移植到 ATECC608B

简介

作者：James Boomer——Microchip Technology Inc.

随着时间的推移，试图损害安全系统的攻击能力不断增强，安全领域内的安全功能和预期也在不断提高。认识到这些变化后，Microchip 开发了 ATECC608A 的安全增强版本，称为 ATECC608B。器件中实现的安全更改主要在后台进行，无法在正常工作期间直接观察到。ATECC608B 的设计支持从 ATECC608A 轻松移植，同时可改善总体安全性。

对于新设计，建议用户直接使用 ATECC608B 开始设计。对于正在经历升级或修订的设计，建议升级部分包含 ATECC608B。对于其他设计，用户必须进行全面的安全评估，确定相关设计是否需要移植到 ATECC608B。

ATECC608B 延续了安全产品线，作为 Microchip CryptoAuthentication™高安全性加密器件系列的一部分进行开发。这些器件将世界一流的基于硬件的密钥存储与硬件加密加速器相结合，以实现各种身份验证和加密协议。ATECC608B 还支持 ATECC608A 之前支持的所有应用和用例。

应用总结

- **网络/物联网（Internet of Things，IoT）节点端点安全**——管理节点身份验证以及会话密钥的创建和管理，并支持包括 TLS 1.2 和 TLS 1.3 等多种协议的临时会话密钥生成流程。
- **固件验证（安全引导）**——通过验证代码摘要并可选择在安全引导成功时使能通信密钥来支持单片机（MCU）主机的安全引导。此外，还提供了多种配置以提升性能。
- **短小报文加密**——通过硬件高级加密标准（Advanced Encryption Standard，AES）引擎加密和/或解密短小报文或数据，如个人可识别信息（Personally Identifiable Information，PII）。该器件直接支持 AES-ECB 模式，在主机的帮助下还可支持其他 AES 模式。附加 Galois 域乘法（Galois Field Multiply，GFM）计算功能支持 AES Galois 计数器模式（AES-GCM）。
- **安全无线（Over-the-Air，OTA）更新**——支持为已下载映像生成本地保护密钥。既支持将一个映像广播到多个系统（每个系统都具有相同的解密密钥），也支持点对点下载每个系统的独特映像。
- **配件/一次性用品认证**——验证系统或组件的真伪。系统中包含一次性组件时，通常使用该功能。

目录

1. 器件差异

ATECC608B 的整体架构与 ATECC608A 相同。ATECC608B 未引入任何新的配置位，其数据槽数与 ATECC608A 相同。所有命令和命令模式仍受支持。该器件支持 I²C 和 SWI 接口 I/O 协议。8 引脚 SOIC 和 UDFN 封装的引脚分配保持不变。

以下部分将介绍 ATECC608A 和 ATECC608B 器件之间的差异。

低频 I²C 问题

ATECC608A 的 I²C 电路存在错误，以下条件下器件可能错误响应：

- 多个 I²C 器件与 ATECC608A 处于同一总线上。
- ATECC608A 器件处于空闲模式。
- I²C 工作频率 ≤ 300 kHz。
- ATECC608A 将 I²C 总线上其他器件的数据模式解析为唤醒脉冲。

在上述条件下，ATECC608A 会唤醒且可能损坏发送到总线上其他器件的数据。数据是否损坏取决于工作频率和发送的实际数据。

ATECC608B 器件已通过修改 I²C 电路消除了这一问题。请注意，ATECC608B 仍可在低频下唤醒，但不会响应或引起数据损坏。

器件版本（DevRev）差异

Microchip 安全器件上的封装标识不指示器件类型。因此，该封装标识无法用于标识 ATECC608B。标识器件的惟一方式是使用器件版本。可使用 `Info` 命令的版本模式（0x00）来读取器件的硬件器件版本。每个器件的 `Info` 命令的输出响应如下：

表 1-1. 版本响应

器件	版本响应
ATECC608A	0x00 0x00 0x60 0x02
ATECC608B	0x00 0x00 0x60 0x03（注）

注： 第四个字节的值可随时间变化，但产品最初发布时为 0x03。

重要： 版本模式响应的值与器件配置区域中的 4 字节 RevNum（Byte[4:7]）不同。只有版本模式响应可用于器件标识。

执行时间差异

实现安全增强功能导致一些命令的执行时间发生变化。这种变化取决于实际的时钟分频比模式以及特定工作模式。下表列出了一些命令和预期的执行时间差异。

CAUTION **注：** 有关执行时间的更多详细信息，请参见完整的数据手册。

表 1-2. ATECC608A 和 ATECC608B 的执行时间差异

命令	变化说明
`Verify`	• `Verify` 命令执行时间的延长不超过 10%。实际变化可能取决于特定命令模式。 • 所有三种时钟分频比模式的执行时间都将延长。

.....（续）	
命令	**变化说明**
SecureBoot	• SecureBoot 命令包含验证操作。执行时间的延长由该命令的验证部分引起。 • SecureBoot 命令执行时间的延长不超过 10%。实际变化可能取决于特定命令模式。 • 所有三种时钟分频比模式的执行时间都将延长。
Read	• 读取时间的延长取决于读取的内容。 • 配置区域中 32 字节的读取时间大约延长了 50%（0.8 ms 到 1.2 ms）。 • 数据区域中 32 字节的读取时间大约延长了一倍（0.9 ms 到 1.8 ms）。 • 这不适合读回命令响应。该时间将保持相同。 • 执行时间的延长不会随时钟分频比模式而变化。
Lock	• 配置区域或数据区域的最长锁定时间大约延长了 30%。 • 由于量产器件以锁定状态交付，这并不会影响器件正常工作，只需由用户在原型设计或开发阶段观察。 • 执行时间的延长不会随时钟分频比模式而变化。

增强型温度范围

ATECC608A 可在-40°C 至+85°C 的工业温度范围内达到规定性能。

ATECC608B 可在-40°C 至+85°C 的标准工业范围和-40°C 至+100°C 的扩展范围内达到规定性能，适合需要环境温度上限值 > +85°C 的用户。增强型温度范围器件具有惟一订购代码，该代码位于器件数据手册中。

全新封装

ATECC608B 现采用 3 引脚 RBH 触点式封装。这是对已有 8 引脚 SOIC 和 UDFN 封装的补充。该封装之前用于 ATSHA204A 和 ATECC508A CryptoAuthentication™器件。RBH 封装仅适用于 SWI 接口模式的器件。

RBH 封装是触点式封装，常用的安装方式是通过外露信号焊盘将封装粘合到外壳上。当一次性器件连接到主机系统时，通常通过弹簧针将触点连接到焊盘。

2. ATECC608B 移植

ATECC608B 的外形、装配和功能与 ATECC608A 相同。封装和引脚分配、器件结构以及命令和命令结构均相同。因此，ATECC608B 在功能上可直接替代 ATECC608A。如果用户使用 Microchip 的软件库（CryptoAuthLib）实现其设计，这将进一步简化移植过程。

必须额外考虑的一个因素是 ATECC608A 和 ATECC608B 对于特定设计而言的时序差异。这实际取决于软件的实现方式。需要考虑以下两种情况：

固定时序实现

如果编写代码时假定的是硬接线时序参数，则必须仔细分析以评估从 ATECC608A 更改为 ATECC608B 所带来的影响。采用这种方法时，在发出命令后，单片机需要先等待一段固定时间，之后才能读回响应数据。如果 ATECC608B 所需的延时明显长于 ATECC608A，则该命令可能失败。将针对 ATECC608A 的旧版本 CryptoAuthLib 或客户生成的库用于 ATECC608B 可能导致一些时序错误。采用最新版本的 CryptoAuthLib 可正确更新时序信息，只需重新编译代码和刷新单片机即可校正时序问题。通常，固定时序所采用的参数都有较大余量，和实际最坏情况下的值相距甚远，因此，可能都不会成为问题。如 **1. 器件差异**所述，ATECC608B 和 ATECC608A 的时序差异相对较小。此外，这些是特定命令模式的代表性时间，还存在其他项（如数据手册所述），可能导致这些值的差异扩大。

如果时序存在问题，可以考虑以下解决方案：

1. 移植代码以使用最新版本的 CryptoAuthLib 库。
2. 移植代码以使用轮询时序。请参见下面的 **2. 轮询时序实现部分**。
3. 如果使用具有固定时序的自定义库，请更新 ATECC608B 所需的库时序参数。
4. 通过在接收到指示响应尚未就绪的失败代码后尝试再次读回数据来实现冗余。

轮询时序实现

当使用 CryptoAuthLib 库时，轮询时序设置为默认工作模式。如果编写代码时使用轮询，则移植到 ATECC608B 将不存在问题。在这种情况下，单片机将轮询 ATECC608B 以确定何时可读取数据。少量时序差异通过轮询命令消除。这些差异可由 ATECC608B 器件完全消除，因为命令的执行时间并不存在明显差异。

2.1 I^2C 低频 ATECC608B 移植

移植必须处理低频 I^2C 问题的 ATECC608A 设计无需更改任一硬件或固件。为确保 ATECC608A 正确工作而实现的更改不会导致经过修正的 ATECC608B 出现问题。

用户必须考虑取消为更正 ATECC608A 问题而实现的固件更改是否有利于系统运行。取消这些更改很可能会减小固件大小并改善系统性能。是否值得出于这些原因修改工作代码取决于实施者。

3. 结论

由于 ATECC608B 的外形、装配和功能与 ATECC608A 几乎相同，移植任务通常十分轻松。器件间的少量时序差异通常不会引起问题，即使引起问题也可轻松修正。补充的全新 RBH 封装和增强型温度范围还可扩大 ATECC608B 安全元件的市场空间。

ATECC608B 实现的更改主要用于提高器件安全性，很大程度上对用户透明。若要采用新的系统设计以及刷新现有系统，强烈建议转换为 ATECC608B 来提高总体系统安全性。

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。

Microchip 器件代码保护功能

请注意以下有关 Microchip 产品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。

商标

ISBN：978-1-5224-9148-4

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