
SAMD5x/E5x加密功能

简介

SAMD/E5x 系列器件中配有多个硬件模块用于支持通信和内部验证安全功能，以确保满足大量常用安全应用架构的要求。

目录

简介.....	1
1. 公钥加密控制器	3
2. 高级加密标准（AES）	4
3. 真随机数发生器	5
4. 完整性检查监视器.....	6
5. 安全位.....	7
6. 用例.....	8
7. 安全引导.....	9
8. 生成和验证 ECDSA 签名.....	10
Microchip 网站.....	11
变更通知客户服务.....	11
客户支持.....	11
Microchip 器件代码保护功能.....	11
法律声明.....	12
商标.....	12
DNV 认证的质量管理体系.....	13
全球销售及服务网点.....	14

1. 公钥加密控制器

公钥加密控制器（Public Key Cryptography Controller, PUKCC）是用于处理 RSA 或 ECC 计算的硬件模块。PUKCC 本身又带有一个集成库，即公共密钥加密库（Public Key Cryptography Library, PUKCL），该库存储在 SAMD/E5x ROM 中，可帮助提高应用的使用效率。

随着 PUKCC 和 PUKCL 的引入，嵌入式应用中处理非对称加密的速度得到了进一步提高。创建像 PUKCL 这样的密码库非常复杂，需要花费大量的时间来确保库的安全性达到既定的标准。

即使通过硬件和支持库提高了效率，RSA 或 ECC 最多也只能使用小于 256 字节（包括填充）的加密信封来加密 2048 位长度的密钥。如果要传输大量数据，使用非对称加密方案可能会非常耗时，并且需要大量的嵌入式系统资源。

2. 高级加密标准（AES）

AES 模块使用对称密钥方案实现加密和解密管理。AES 模块支持 128 位、192 位和 256 位密钥，并具有多种模式和策略。

与非对称加密方案相比，使用对称加密方案的加密和解密过程所需的时间和资源要少很多。这是由于非对称加密的计算复杂性所致。由于对称加密方案所需的复杂性降低，通常使用公钥（RSA 或 ECC）传输会话密钥和对称密钥，而大数据集的其余部分将使用 AES 传输。

3. 真随机数发生器

真随机数生成器（True Random Number Generator，TRNG）可满足 NIST 对播种确定性随机数发生器的要求。PUKCC 和 AES 模块都集成了可由 TRNG 播种的确定性随机数发生器。

4. 完整性检查监视器

完整性检查监视器（Integrity Check Monitor, ICM）支持身份验证服务中经常使用的多种安全哈希算法，可以监视 SAMD/E5x NVM 区域以防止存储器内容被篡改。

当 ICM 监视已定义的存储器区域并发现某个区域的相关哈希不匹配时，则发生中断。虽然依据加密标准这并不是一个安全特性，但可以设置 ICM 来监视存储公钥的存储器区域，并在发生篡改时向系统报警。这进而又可以确保对安全引导或安全固件更新等进程进行身份验证。建议在需要安全存储非对称或对称密钥的应用中使用类似于 ECC508 这样的器件。

5. 安全位

在所有 MicrochipSAM 器件中都可使用安全位，设置此位后，它将限制器件服务单元（Device Service Unit, DSU）对器件的访问。这意味着，通过调试访问端口（Debug Access Port, DAP）访问器件将受到限制，从而保护 NVM 内容。安全位不是 SAMD/E5x 的加密特性，但它提供了加密特性所依赖的安全环境。

清除安全位的唯一方法是通过 DAP 发出芯片擦除命令。芯片擦除命令将删除易失性和非易失性存储器中的全部内容。芯片擦除命令还将观察 BOOTPROT 位的状态，并保留 BOOTPROT 位定义的 NVM 区域。为了确保安全自举程序受到保护，不应设置 BOOTPROT 位。

6. 用例

如今，出于多种原因，应用中会使用嵌入式安全技术。有许多方法可以保护数据和 IP 不受外部源的影响，下面将重点介绍和讨论其中几种方法，以展示如何在这些模型中使用 SAMD/E5x 硬件。

7. 安全引导

在安全引导应用程序中，在每次关机后再开机或复位后都会对应用程序映像进行验证，以确保映像未被损坏。可以使用非对称密钥或对称密钥处理安全引导。

使用的模块：ICM、PUKCC 或 AES

通常，安全引导过程由自举程序处理，它将管理启动时的应用程序映像验证以杜绝任何可能的篡改行为。在允许应用程序启动之前，自举程序会先使用 ICM 模块对应用程序映像进行哈希校验，然后将该哈希值与签名证书中包含的哈希值进行比较。

在此过程中，会要求将来自 OEM 的公钥、与当前驻留在器件中的应用程序映像相关联的签名证书以及用于管理此过程的安全自举程序加载到 SAMD/E5x 中。

8. 生成和验证 ECDSA 签名

Atmel START 提供了一个示例程序 PUKCC ECDSA，用于逐步展示带有 PUKCC/PUKCL 功能的 ECC 用例。有关更多信息，请访问以下位置：<http://start.atmel.com/#examples/SAME54XplainedPro>。

项目文件夹中包含一个 PDF 文件，其中介绍了项目的功能以及如何使用集成的加密库。

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>

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，不得暗中以其他方式转让任何许可证。

商标

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

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

Adjacent Key Suppression、AKS、Analog-for-the-Digital Age、Any Capacitor、AnyIn、AnyOut、BodyCom、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、motorBench、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.、SQL、SuperSwitcher、SuperSwitcher II、Total Endurance、TSHARC、USBCheck、VariSense、ViewSpan、WiperLock、Wireless DNA 和 ZENA 为 **Microchip Technology Incorporated** 在美国和其他国家或地区的商标。

SQTP 为 **Microchip Technology Inc.** 在美国的服务标记。

Silicon Storage Technology 为 **Microchip Technology Inc.** 在除美国外的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。

© 2018, **Microchip Technology Incorporated** 版权所有。

ISBN: 978-1-5224-3501-3

DNV 认证的质量管理体系

ISO/TS 16949

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

全球销售及服务中心

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: 1-480-792-7200 传真: 1-480-792-7277 技术支持: http://www.microchip.com/support 网址: www.microchip.com 亚特兰大 德卢斯, 乔治亚州 电话: 1-678-957-9614 传真: 1-678-957-1455 奥斯汀, 德克萨斯州 电话: 1-512-257-3370 波士顿 韦斯特伯鲁, 马萨诸塞州 电话: 1-774-760-0087 传真: 1-774-760-0088 芝加哥 艾塔斯卡, 伊利诺伊州 电话: 1-630-285-0071 传真: 1-630-285-0075 达拉斯 艾迪生, 德克萨斯州 电话: 1-972-818-7423 传真: 1-972-818-2924 底特律 诺维, 密歇根州 电话: 1-248-848-4000 休斯敦, 德克萨斯州 电话: 1-281-894-5983 印第安纳波利斯 诺布尔斯维尔, 印第安纳州 电话: 1-317-773-8323 传真: 1-317-773-5453 电话: 1-317-536-2380 洛杉矶 米申维耶霍, 加利福尼亚州 电话: 1-949-462-9523 传真: 1-949-462-9608 电话: 1-951-273-7800 罗利, 北卡罗来纳州 电话: 1-919-844-7510 纽约, 纽约州 电话: 1-631-435-6000 圣何塞, 加利福尼亚州 电话: 1-408-735-9110 电话: 1-408-436-4270 加拿大 - 多伦多 电话: 1-905-695-1980 传真: 1-905-695-2078	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 - 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 - 香港特别行政区 电话: 852-2943-5100 中国 - 珠海 电话: 86-756-3210040 台湾地区 - 高雄 电话: 886-7-213-7830 台湾地区 - 台北 电话: 886-2-2508-8600 台湾地区 - 新竹 电话: 886-3-577-8366	澳大利亚 - 悉尼 电话: 61-2-9868-6733 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 - 檳榔嶼 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 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 - 海布隆 电话: 49-7131-67-3636 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 - 赖阿南纳 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: 47-7288-4388 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