Application Note

CC23xx AESCTRDRBG 驱动符合 NIST SP 800-90A 标准

Sam Hachem, Achyut Ray *Automotive Connectivity Solutions*

摘要

本应用手册介绍 TI SimpleLink™ 安全驱动包中随 CC23xx 器件系列配套发布的基于高级加密标准 (AES) 计数器模式 (CTR) 的确定性随机比特生成器 (AESCTRDRBG) 驱动，并展示由 TI 验证套件生成的符合 NIST SP 800-90A 标准的合规证明材料。本手册同时阐释，评估 CC23xx 所搭载的确定性随机比特生成器 (DRBG) 时，适用规范依据为 NIST SP 800-90A，而非 NIST SP 800-22 Rev. 1a 规定的输出统计检测套件，并说明其原因。

内容

商标

1 简介

CC23xx SimpleLink 系列提供基于 AES CTR 的确定性随机位生成器 (AESCTRDRBG) 驱动，可为系统集成商提供确定性随机位生成服务。本文档介绍了终端客户和 OEM 利益相关者要求的三个方面：

- CC23xx AESCTRDRBG 驱动和 NIST SP 800-90A 规范之间的映射
- 根据 NIST CAVP CTR_DRBG 测试向量验证驱动的方法
- 2025 年 4 月 4 日执行的验证套件的完整通过/失败结果

2 详细说明

2.1 范围

本手册适用于 CC23xx 系列的 TI 安全驱动库中的 AESCTRDRBG 驱动。本手册仅介绍确定性机制。物理熵源表征 (NIST SP 800-90B) 和 RBG 结构 (NIST SP 800-90C) 不在本文档的范围内。

2.2 标准选择：SP 800-22 与 SP 800-90A

SP 800-22 针对 RNG 的比特流输出定义了十五项统计测试。确定性 DRBG（如 CC23xx AESCTRDRBG 驱动等）适用的规范标准为 NIST SP 800-90A 修订版 1，而不是 SP 800-22，原因如下：

1. SP 800-90A 规定了机制结构（CTR_DRBG，Hash_DRBG，HMAC_DRBG）。SP 800-90A 是驱动实施的规范，同时也是验证合规性所需依据的标准。
2. NIST 的加密模块验证程序 (CMVP) 根据 FIPS 140-3 标准对 DRBG 进行了 SP 800-90A/90B 验证。SP 800-22 未在验证过程中使用（请参阅 FIPS 140-3 实施指南）。
3. SP 800-22 评估输出流的统计属性。通过 SP 800-22 全套检测仅为必要非充分判定依据：存在密码学层面存在缺陷的随机数生成器可通过该全套检测。同行评审分析 (Saarinen，PQShield，2022) 在随 SP 800-22 一起提供的参考生成器上证明了这一点。
4. CC23xx AESCTRDRBG 驱动为确定性生成机制，可接收外部输入的种子值。已知答案测试 (KAT) 可根据 NIST CAVP CTR_DRBG 向量验证驱动的正确性，该机制是 SP 800-90A 通过验证的。

因此，本说明中的验证依据采用基于 NIST CAVP CTR_DRBG 向量完成的 SP 800-90A 合规性验证结果。

2.3 受测器件和驱动

条目	值
器件系列	CC23xx（SimpleLink 蓝牙®低功耗无线 MCU）
驱动器	AESCTRDRBG（安全驱动包）
机制	CTR_DRBG，符合 NIST SP 800-90A 修订版 1，第 10.2 节
分组密码/密钥大小	AES-128
SDK	包含在 SimpleLink CC23xx SDK 9.20 中（并通过补丁反向移植到 9.11）
待测 TF-M 配置	tfm_disabled

2.4 NIST SP 800-90A 特性映射

下表将 SP 800-90A 特性映射到 CC23xx AESCTRDRBG 驱动。其中明确标识了此处介绍的确定性用例不需要的可选功能。

NIST SP 800-90A 特性	驱动支持	注释
机制	仅 CTR_DRBG	未实现 Hash_DRBG 和 HMAC_DRBG。
推导函数 (df)	否	可选，依据 SP 800-90A 第 10.2.1 节。
预测电阻	否	驱动不实现 PR。因此，CAVP PR 真向量集不适用于此配置。
个性化字符串	是	依据 SP 800-90A 第 8.7.1 节。
重播种时附加熵输入	是	依据 SP 800-90A 第 9.2 节。
生成时附加数据输入	否	依据 SP 800-90A 第 9.3 节。
重播种间隔	可配置，强制	通过专用测试进行验证（请参阅第 7 节）。

2.5 测试方法

验证基础架构基于 NIST CAVP DRBG 验证系统 (DRBGVS) 规范构建。测试向量是公开发布的 CAVP CTR_DRBG 向量。这些向量会在 RTOS、工具链和返回行为的所有受支持组合中，针对驱动的每个公开 API 执行。

2.5.1 已应用向量集

用于测试的向量集可以在这里找到:

- CTR_DRBG，未重播种 (drbgvectors_no_reesed)。
- CTR_DRBG，在没有预测电阻的情况下重播种 (drbgvectors_pr_false)。
- 具有预测电阻的 CTR_DRBG (drbgvectors_pr_true)：不适用 — 驱动不实现 PR；已被设计排除。

2.5.2 已执行构建矩阵

轴	值
RTOS	NoRTOS、FreeRTOS
工具链	IAR、GCC、Clang/LLVM
返回行为	阻塞、轮询
密钥大小	AES-128
TF-M	tfm_disabled（密钥库路径单独跳过和验证）

2.6 测试覆盖范围

各项测试覆盖 AESCTRDRBG 驱动全部公开的 API：

表 2-1. 来源：tests/secure_drivers/aesctrdrbg/general/tests/test_aesctrdrbg_general.py in the secure_drivers 存储库。

测试	用途
test_getRandomBytes	根据 CAVP KAT 验证原始随机字节输出
test_getBytes	验证字节级生成路径
test_generateKey	验证源自 DRBG 的 AES 密钥生成
test_generateKeyWithKeyStore	密钥库集成路径（需要启用 TF-M；在此轮中跳过）
test_reseed_interval	依据 SP 800-90A 第 9.3.1 节验证已配置的重播种间隔的实施情况

2.7 结果

汇总结果，报告生成日期：2025 年 4 月 4 日：

结果	数量
通过	48
未通过	0
误差	0
已跳过（根据设计，TF-M 关闭）	12
总计	60

跳过的十二个测试都是 test_generateKeyWithKeyStore 变体。跳过测试的原因是“tfm_disabled 配置中不支持密钥库 API”，并在启用 TF-M 时通过单独执行来涵盖这些测试。在矩阵中的每个（RTOS、工具链、返回行为）组合内，所有未跳过的测试都为通过。

2.7.1 各轴摘要

RTOS	工具链	阻塞已通过	轮询通过
NoRTOS	IAR	5/5	5/5
NoRTOS	GCC	5/5	5/5
NoRTOS	LLVM	5/5	5/5
FreeRTOS	IAR	5/5	5/5
FreeRTOS	GCC	5/5	5/5
FreeRTOS	LLVM	5/5	5/5

2.8 蓝牙 SIG 认证相关说明

蓝牙 SIG 认证测试规范不强制要求对控制器层或主机层进行 RNG 熵统计测试。蓝牙 SIG 明确表示 RNG 适合芯片制造商。此文档提供了 TI 的 CC23xx 芯片组符合 SP 800-90A 安全标准的官方证明。

3 测试向量文件映射

CAVP DRBG 测试向量分发包为包含若干 .rsp 文件的 zip 压缩包。下面列出了针对 AESCTRDRBG 驱动应用的子集。pythest 线束将执行完整的预期和实际比较。任何 KAT 上的不匹配都会导致报告中出现 FAIL 结果。

压缩包	适用文件	已应用？
drbgvectors_no_reseed.zip	CTR_DRBG.rsp（AES-128，无 df）	是
drbgvectors_pr_false.zip	CTR_DRBG.rsp（AES-128，无 df，重播种）	是
drbgvectors_pr_true.zip	CTR_DRBG.rsp（AES-128，PR）	否（未实现功能）
drbgvectors_*	Hash_DRBG.rsp，HMAC_DRBG.rsp	否（未实现机制）

4 总结

CC23xx AESCTRDRBG 驱动在所有受支持的 RTOS/工具链/返回行为组合中，通过了根据其公共 API 执行的每个适用 NIST CAVP CTR_DRBG 测试向量。对于节 2.4 中所述的功能集，该驱动符合 NIST SP 800-90A 修订版 1 中指定的 CTR_DRBG 机制。这满足低功耗蓝牙平台中使用的确定性 DRBG 的适用标准化合规性基础。

5 参考资料

1. NIST SP 800-90A 修订版 1，使用确定性随机比特生成器生成随机数的建议，2015 年 6 月。https://doi.org/10.6028/NIST.SP.800-90Ar1
2. NIST SP 800-90B，建议用于随机位生成的各向异性源，2018 年 1 月。https://doi.org/10.6028/NIST.SP.800-90B
3. NIST SP 800-22 修订版 1a，用于加密应用的随机和伪随机数生成器的统计测试套件，2010 年 4 月。NIST 规划说明 2022 年 04 月 19 日：出版物正在修订中。https://csrc.nist.gov/publications/detail/sp/800-22/rev-1a/final
4. NIST CAVP DRBG 验证系统 (DRBGVS)。https://csrc.nist.gov/CSRC/media/Projects/Cryptographic-Algorithm-Validation-Program/documents/drbg/DRBGVS.pdf
5. NIST CAVP DRBG 测试向量。https://csrc.nist.gov/CSRC/media/Projects/Cryptographic-Algorithm-Validation-Program/documents/drbg/drbgtestvectors.zip
6. FIPS 140-3，加密模块的安全要求，2019 年 3 月。https://doi.org/10.6028/NIST.FIPS.140-3
7. M-J. O. Saarinen。SP 800-22 和 GM/T 0005-2012 测试：明显过时，可能有害。PQShield Ltd.，2022 年

重要通知和免责声明

TI“按原样”提供技术和可靠性数据（包括数据表）、设计资源（包括参考设计）、应用或其他设计建议、网络工具、安全信息和其他资源，不保证没有瑕疵且不做出任何明示或暗示的担保，包括但不限于对适销性、与某特定用途的适用性或不侵犯任何第三方知识产权的暗示担保。

这些资源可供使用 TI 产品进行设计的熟练开发人员使用。您将自行承担以下全部责任：(1) 针对您的应用选择合适的 TI 产品，(2) 设计、验证并测试您的应用，(3) 确保您的应用满足相应标准以及任何其他安全、安保法规或其他要求。

这些资源如有变更，恕不另行通知。TI 授权您仅可将这些资源用于研发本资源所述的 TI 产品的相关应用。严禁以其他方式对这些资源进行复制或展示。您无权使用任何其他 TI 知识产权或任何第三方知识产权。对于因您对这些资源的使用而对 TI 及其代表造成的任何索赔、损害、成本、损失和债务，您将全额赔偿，TI 对此概不负责。

TI 提供的产品受 TI 销售条款)、TI 通用质量指南 或 ti.com 上其他适用条款或 TI 产品随附的其他适用条款的约束。TI 提供这些资源并不会扩展或以其他方式更改 TI 针对 TI 产品发布的适用的担保或担保免责声明。 除非德州仪器 (TI) 明确将某产品指定为定制产品或客户特定产品，否则其产品均为按确定价格收入目录的标准通用器件。

TI 反对并拒绝您可能提出的任何其他或不同的条款。

最后更新日期：2025 年 10 月