参考資料

Application Note

CC23xx AESCTRDRBG ドライバの NIST SP 800-90A 準拠

Sam Hachem, Achyut Ray *Automotive Connectivity Solutions*

概要

このアプリケーション ノートでは、CC23xx デバイス ファミリ向けの TI SimpleLink™ Secure Drivers パッケージに搭載されている高度暗号化標準 (AES) カウンタ ベース (CTR ベース) 決定論的乱数生成器 (AESCTRDRBG) ドライバについて説明するとともに、TI の検証スイートによって生成された NIST SP 800-90A への準拠の根拠を提示しています。また、CC23xx に実装されているような決定論的乱数生成器 (DRBG) を評価する際に、NIST SP 800-22 Rev. 1a で規定されている統計的出力テスト スイートではなく、NIST SP 800-90A が適用される規範的根拠となっている理由についても説明します。

目次

商標

1 はじめに

CC23xx SimpleLink ファミリは、AES CTR ベースの決定論的乱数生成サービスをシステム インテグレータに提供する決定論的乱数生成器 (AESCTRDRBG) ドライバを備えています。このドキュメントは、最終顧客と OEM 関係者が必要とする 3 つの項目をまとめたものです。

- CC23xx AESCTRDRBG ドライバと NIST SP 800-90A 仕様との間のマッピング
- NIST CAVP CTR_DRBG テスト ベクトルに対してドライバを検証するために使用される手法
- 2025 年 4 月 4 日に実行された検証スイートの合格 / 不合格の全結果

2 詳細説明

2.1 範囲

この注記は、CC23xx ファミリ向けの TI Secure Drivers リポジトリにある AESCTRDRBG ドライバに適用されます。この注記は、決定論的機構についてのみ説明しています。物理的なエントロピー ソースの特性評価 (NIST SP 800-90B) と RBG 構造 (NIST SP 800-90C) は、このドキュメントでは対象外です。

2.2 標準の選択肢：SP 800-22 と SP 800-90A の比較

SP 800-22 では、RNG のビット ストリーム出力に関する 15 の統計テストを定義しています。CC23xx AESCTRDRBG ドライバなど、決定論的 DRBG に適用される規範的基準は、以下の理由から、SP 800-22 ではなく NIST SP 800-90A Rev. 1 です。

1. SP 800-90A は、機構の構造 (CTR_DRBG、Hash_DRBG、HMAC_DRBG) を規定します。SP 800-90A はドライバが実装する仕様であり、適合性を実証する必要がある仕様です。
2. NIST の暗号モジュール検証プログラム (CMVP) は、FIPS 140-3 下の DRBG を SP 800-90A/90B に対して検証します。SP 800-22 は、その検証プロセスでは使用されません (FIPS 140-3 実装ガイダンスを参照)。
3. SP 800-22 は、出力ストリームの統計的プロパティを評価します。SP 800-22 テスト スイートに合格することは必要条件ではあるが十分条件ではありません：暗号学的に破綻した生成器であっても、このテスト スイートに合格可能で、実際に合格しています。ピア レビュー分析 (Saarinen、PQShield、2022 年) は、SP 800-22 に付属のリファレンス生成器でこれを実証しています。
4. CC23xx AESCTRDRBG ドライバは、外部から供給されるシードを受け入れる決定論的な機構です。ドライバの正確性は、NIST CAVP CTR_DRBG ベクトルに対する既知の回答テスト (KAT) によって検証可能です。これは、SP 800-90A が検証された機構です。

したがって、このノートに記載されているエビデンスは、NIST CAVP CTR_DRBG ベクトルによる SP 800-90A 適合性を使用しています。

2.3 テスト対象のデバイスとドライバ

項目	値
デバイス ファミリ	CC23xx (SimpleLink Bluetooth® Low Energy ワイヤレス MCU)
ドライバ	AESCTRDRBG (Secure Drivers パッケージ)
機構	NIST SP 800-90A Rev. 1、セクション 10.2 に準拠の CTR_DRBG
ブロック暗号 / キーのサイズ	AES-128
SDK	SimpleLink CC23xx SDK 9.20 に付属 (また、パッチで 9.11 に逆移植)
テスト中の TF-M 構成	tfm_disabled

2.4 NIST SP 800-90A 機能マッピング

以下の表は、SP 800-90A の機能を CC23xx AESCTRDRBG ドライバにマッピングしています。ここで記載されている決定論的な使用事例では、不要なオプション機能が明示的に特定されています。

NIST SP 800-90A の機能	ドライバ サポート	注
機構	CTR_DRBG のみ	Hash_DRBG および HMAC_DRBG は実装されていません。
導出関数 (df)	なし	SP 800-90A セクション 10.2.1 に従い任意選択。
予測抵抗性	なし	ドライバは PR を実装していません。このため、CAVP PR-true ベクトル セットは、この構成には適用されません。
パーソナライズ文字列	有	SP 800-90A セクション 8.7.1 に従う。
再シード時の追加エントロピー入力	有	SP 800-90A セクション 9.2 に従う。
生成時の追加データ入力	なし	SP 800-90A セクション 9.3 に従い任意選択。

NIST SP 800-90A の機能	ドライバ サポート	注
再シード間隔	設定可能、強制	専用テストにより検証済み (セクション 7 を参照)。

2.5 テスト方法

検証インフラストラクチャは、NIST CAVP DRBG 検証システム (DRBGVS) の仕様に基づいて構築されています。テストベクトルは、一般に公開されている CAVP CTR_DRBG ベクトルです。ベクトルは、ドライバの公開 API に対して実行されるほか、RTOS、ツールチェーン、リターン挙動など、サポート対象のすべての組み合わせにわたっています。

2.5.1 適用されるベクトル セット

テストに使用するベクトル セットは、このページにあります。

- CTR_DRBG、再シードなし (drbgvectors_no_reseed)。
- CTR_DRBG、予測抵抗性なしの再シード (drbgvectors_pr_false)。
- 予測抵抗性ありの CTR_DRBG (drbgvectors_pr_true):適用せず — ドライバは PR を実装しておらず、設計により除外されます。

2.5.2 実行されたビルド マトリクス

軸	値
RTOS	NoRTOS、FreeRTOS
ツールチェーン	IAR、GCC、Clang/LLVM
リターン挙動	ブロッキング、ポーリング
キーのサイズ	AES-128
TF-M	tfm_disabled (キーストア パスがスキップされ、個別に検証されます)

2.6 テスト範囲

テストでは、AESCTRDRBG ドライバの公開 API 全範囲を検証します。

表 2-1. 出典:secure_drivers リポジトリの tests/secure_drivers/aesctrdrbg/general/tests/test_aesctrdrbg_general.py。

テスト	目的
test_getRandomBytes	CAVP KAT に対してランダムな未加工バイト出力を検証します
test_getBytes	バイト レベルの生成パスを検証します
test_generateKey	DRBG から導出された AES 鍵生成を検証します
test_generateKeyWithKeyStore	キーストア統合パス (TF-M が有効になっている必要があります。この実行ではスキップされます)
test_reseed_interval	SP 800-90A セクション 9.3.1 に従って設定された再シード間隔の適用を検証します

2.7 結果

2025 年 4 月 4 日に生成されたレポートの集計結果。

結果	カウント
合格	48
不合格	0
エラー	0
省略済み (設計により、TF-M オフ)	12
合計	60

省略された 12 のテストは、すべて test_generateKeyWithKeyStore のバリエーションです。テストは「tfm_disabled 構成ではサポートされていないキーストア API」という理由で省略され、TF-M が有効になっている場合は個別の検証で網羅されます。省略されていないすべてのテストは、マトリクス内のすべて (RTOS、ツールチェーン、リターン挙動) の組み合わせで合格しました。

2.7.1 軸ごとの概要

RTOS	ツールチェーン	成功したブロッキング	成功したポーリング
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 Bluetooth SIG 認証の背景情報

Bluetooth SIG 認証テスト仕様は、コントローラ層またはホスト層の RNG エントロピー統計テストを義務付けていません。Bluetooth SIG は、シリコン メーカーに RNG 適合性を明示的に委任しています。この資料は、TI の CC23xx チップ セットが SP 800-90A セキュリティ規格に適合しているという公式な証拠を提示します。

3 テスト ベクトル ファイルのマッピング

CAVP DRBG のテスト ベクトル配布は、.rsp ファイルの zip アーカイブです。AESCTRDRBG ドライバに対して適用されるサブセットを以下に示します。予測値と実測値の完全な比較は、pytest ハーネスによって実行されます。いずれかの KAT に不一致があると、レポートに「FAIL」と表示されます。

アーカイブ	対象ファイル	適用の有無
drbgvectors_no_reseed.zip	CTR_DRBG.rsp (AES-128、導出関数なし)	有
drbgvectors_pr_false.zip	CTR_DRBG.rsp (AES-128、導出関数なし、再シード)	有
drbgvectors_pr_true.zip	CTR_DRBG.rsp (AES-128、予測耐性)	無 (機能は実装されていません)
drbgvectors_*	Hash_DRBG.rsp、HMAC_DRBG.rsp	無 (機構は実装されていません)

4 まとめ

CC23xx AESCTRDRBG ドライバは、サポート対象のすべての RTOS / ツールチェーン / リターン挙動の組み合わせにわたって、その公開 API に対して実行された、該当するすべての NIST CAVP CTR_DRBG テスト ベクトルに合格しています。このドライバは、セクション 2.4 に記載されている機能セットについて、NIST SP 800-90A Rev. 1 で規定されている CTR_DRBG 機構に準拠しています。これにより、Bluetooth Low Energy プラットフォームで使用される決定論的 DRBG に対して適用される規範的適合要件を満たしていることになります。

5 参考資料

1. NIST SP 800-90A Rev. 1、Recommendation for Random Number Generator Using Deterministic Random Bit Generator、2015 年 6 月。https://doi.org/10.6028/NIST.SP.800-90Ar1
2. NIST SP 800-90B、Recommendation for the Entropy Sources Used for Random Bit Generation、2018 年 1 月。https://doi.org/10.6028/NIST.SP.800-90B
3. NIST SP 800-22 Rev. 1a、A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications、2010 年 4 月。NIST Planning Note 2022-04-19：改訂中の出版物。https://csrc.nist.gov/publications/detail/sp/800-22/rev-1a/final
4. NIST CAVP DRBG Validation System (DRBGVS)。https://csrc.nist.gov/CSRC/media/Projects/Cryptographic-Algorithm-Validation-Program/documents/drbg/DRBGVS.pdf
5. NIST CAVP DRBG test vectors。https://csrc.nist.gov/CSRC/media/Projects/Cryptographic-Algorithm-Validation-Program/documents/drbg/drbgtestvectors.zip
6. FIPS 140-3、Security Requirements for Cryptographic Modules、2019 年 3 月。https://doi.org/10.6028/NIST.FIPS.140-3
7. M-J. O. Saarinen。SP 800-22 および GM/T 0005-2012 Tests：明らかに廃版、おそらくためにならず。PQShield Ltd.、2022 年

重要なお知らせと免責事項

TI は、技術データと信頼性データ (データシートを含みます)、設計リソース (リファレンス デザインを含みます)、アプリケーションや設計に関する各種アドバイス、Web ツール、安全性情報、その他のリソースを、欠陥が存在する可能性のある「現状のまま」提供しており、商品性および特定目的に対する適合性の黙示保証、第三者の知的財産権の非侵害保証を含むいかなる保証も、明示的または黙示的にかかわらず拒否します。

これらのリソースは、TI 製品を使用する設計の経験を積んだ開発者への提供を意図したものです。(1) お客様のアプリケーションに適した TI 製品の選定、(2) お客様のアプリケーションの設計、検証、試験、(3) お客様のアプリケーションに該当する各種規格や、その他のあらゆる安全性、セキュリティ、規制、または他の要件への確実な適合に関する責任を、お客様のみが単独で負うものとします。

上記の各種リソースは、予告なく変更される可能性があります。これらのリソースは、リソースで説明されている TI 製品を使用するアプリケーションの開発の目的でのみ、TI はその使用をお客様に許諾します。これらのリソースに関して、他の目的で複製することや掲載することは禁止されています。TI や第三者の知的財産権のライセンスが付与されている訳ではありません。お客様は、これらのリソースを自身で使用した結果発生するあらゆる申し立て、損害、費用、損失、責任について、TI およびその代理人を完全に補償するものとし、TI は一切の責任を拒否します。

TI の製品は、 TI の販売条件 、 TI の総合的な品質ガイドライン 、 ti.com または TI 製品などに関連して提供される他の適用条件に従い提供されます。TI がこれらのリソースを提供することは、適用される TI の保証または他の保証の放棄の拡大や変更を意味するものではありません。 TI がカスタム、またはカスタマー仕様として明示的に指定していない限り、TI の製品は標準的なカタログに掲載される汎用機器です。

お客様がいかなる追加条項または代替条項を提案する場合も、TI はそれらに異議を唱え、拒否します。

最終更新日：2025 年 10 月