参考資料

Application Brief

CC27xx HSM タイミング ベンチマーク

Zhitao Wu

はじめに

CC27xx は、ハードウェア アクセラレーション形式の暗号化を実現するハードウェア セキュリティ モジュール (HSM) を内蔵した、テキサス インスツルメンツのワイヤレス マイコン デバイス ファミリです。この資料は、組込みファームウェア エンジニアやセキュリティ アーキテクトが、セキュリティとエネルギー効率の両方を重視する IoT、スマートハウス、産業オートメーション、ワイヤレス センサ アプリケーション向けのコネクテッド製品を設計する際に役立ちます。

この資料では、TI のワイヤレス マイコンである CC2745 のタイミング性能ベンチマーク測定の結果について説明します。この製品は、専用のハードウェア セキュリティ モジュール (HSM) を内蔵し、暗号処理を高速化します。HSM は、セキュリティ ワークロードをメイン CPU からオフロードします。

このテスト プロセスでは、AES-128、SHA-256、ECC-256 処理のタイミング データを測定しました。特に記述のない限り、すべてのタイミング テストは、テキサス インスツルメンツの SimpleLink™ Low Power F3 ソフトウェア開発キット (SDK) バージョン 9.20.00.81、HSM ファームウェア バージョン 3.4.5 を使用して PG2.0 シリコン上で実施しています。この資料には、テスト結果から得られた重要な推奨事項と、HSM ハードウェア アクセラレーションと MbedTLS ソフトウェアの比較結果が記載されています。

このデータにより、設計チームは適切な暗号パスを選択できるようになります。バルク スループットには HSM ハードウェア (ペイロードが大きい場合、最大 2.5 倍高速)、小さなパケットでレイテンシの影響を受けやすい用途にはソフトウェア フォールバックが適しています。

タイミングの比較:HSM ハードウェアと MbedTLS ソフトウェアの比較

測定は、PG2.0 シリコン上の SDK 9.20.00.81、HSM ファームウェア 3.4.5 で実施しました。その結果、ペイロードが大きい場合、HSM ハードウェアは MbedTLS ソフトウェアよりもはるかに優れたスループットを提供することが示されました。

表 1. AES-CBC-128

データ サイズ	暗号化			復号化		
	HSM HW (µs)	MbedTLS SW (µs)	SW/HW 比	HSM HW (µs)	MbedTLS SW (µs)	SW/HW 比
16 バイト	124	34	0.27 倍 (サイズが小さい場合は SW のほうが高速)	122	84.5	0.69 倍 (サイズが小さい場合は SW のほうが高速)
128 バイト	124	134.5	1.08 倍 (HW のうほうが高速)	123.5	204	1.65 倍 (HW のうほうが高速)
256 バイト	127	232.5	1.83 倍 (HW のうほうが高速)	125.5	328	2.61 倍 (HW のうほうが高速)

表 2. SHA-256

データ サイズ	HSM HW (µs)	MbedTLS SW (µs)	SW/HW 比
3 バイト	110.5	70	0.63 倍 (サイズが小さい場合は SW のほうが高速)
65 バイト	109	125.5	1.15 倍 (HW のうほうが高速)
252 バイト	110	279.5	2.54 倍 (HW のうほうが高速)

表 3. ECDSA- SECP-256

処理	HSM HW (ms)	MbedTLS SW (ms)	SW/HW 比
署名	23.63	1062	44.94 倍 (HW のうほうが高速)
検証	41.50	4017	96.8 倍 (HW のうほうが高速)

主な調査結果

CC2745 HSM は、ハードウェア アクセラレーション形式の暗号化処理を提供します。ベンチマーク データから、以下の調査結果が得られました。

- AES-128 の暗号化または復号のレイテンシは約 124 ～ 127µs で、これはドライバ インターフェイスではなく、HSM 処理がレイテンシに影響していることを示しています。SHA-256 でも同様のパターンが見られます。
- ECC-256 署名 (約 24ms) と検証 (約 41ms) は、最も負荷のかかる処理ですが、MbedTLS ソフトウェアよりも優れた性能を示しています。
- ペイロードが大きい場合、HSM ハードウェアは MbedTLS ソフトウェアよりも優れています。
  - AES-CBC 暗号化は、256 バイトで約 1.83 倍、復号は約 2.61 倍高速です
  - SHA-256 は、252 バイトで約 2.5 倍高速です
  - データ サイズが小さい場合 (約 30 バイト未満)、HSM では初期化でオーバーヘッドが発生するため、MbedTLS ソフトウェアのほうが高速になります。

全体として、HSM は、バルク暗号化スループットや、ECDSA ベースの署名と検証を必要とするアプリケーションに適しています。小さなデータ (16～30 バイト未満) でレイテンシの影響を受けやすい処理には、ソフトウェア フォールバックを実装できます。

参考資料

1. テキサス インスツルメンツ、『CC274xR-Q1, CC274xP-Q1 車載用 SimpleLink™ Bluetooth® Low Energy ワイヤレス マイコン』データシート

商標

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