STM32U5 対称暗号コプロセッサのプレゼンテーションへようこそ。ここでは、暗号化アプリケーションに広く使用されている AES および SAES モジュールの機能について説明します。

STM32U5 AES の機能リスト

- NIST FIPS197 準拠の AES 実装
- AES連鎖モード
  - 電子コードブック(ECB)
  - 暗号ブロック連鎖(CBC)
  - カウンタ(CTR)モード
  - ガロアカウンタモード(GCM)
  - ガロアメッセージ認証コード(GMAC)
  - CBC-MAC 付きカウンタ(CCM)モード
- 128 ビットデータブロック、128 または 256 ビットキーでの AES 動作モード
  - 暗号化、復号(関連するキー派生モード)
- **セキュア AES から共有鍵をロードできます**
- サスペンド/レジュームおよび DMA サポート付き AHB スレーブ(IN + OUT チャネル)
- 32 ビットデータワードスワッピングのサポート(ビット、バイト、またはハーフワード)
- **アトミックキーの書込み/ローディングの実施**

128 ビットブロックの処理に必要なサイクル数
クロック周波数= ペリフェラルの AHB クロック

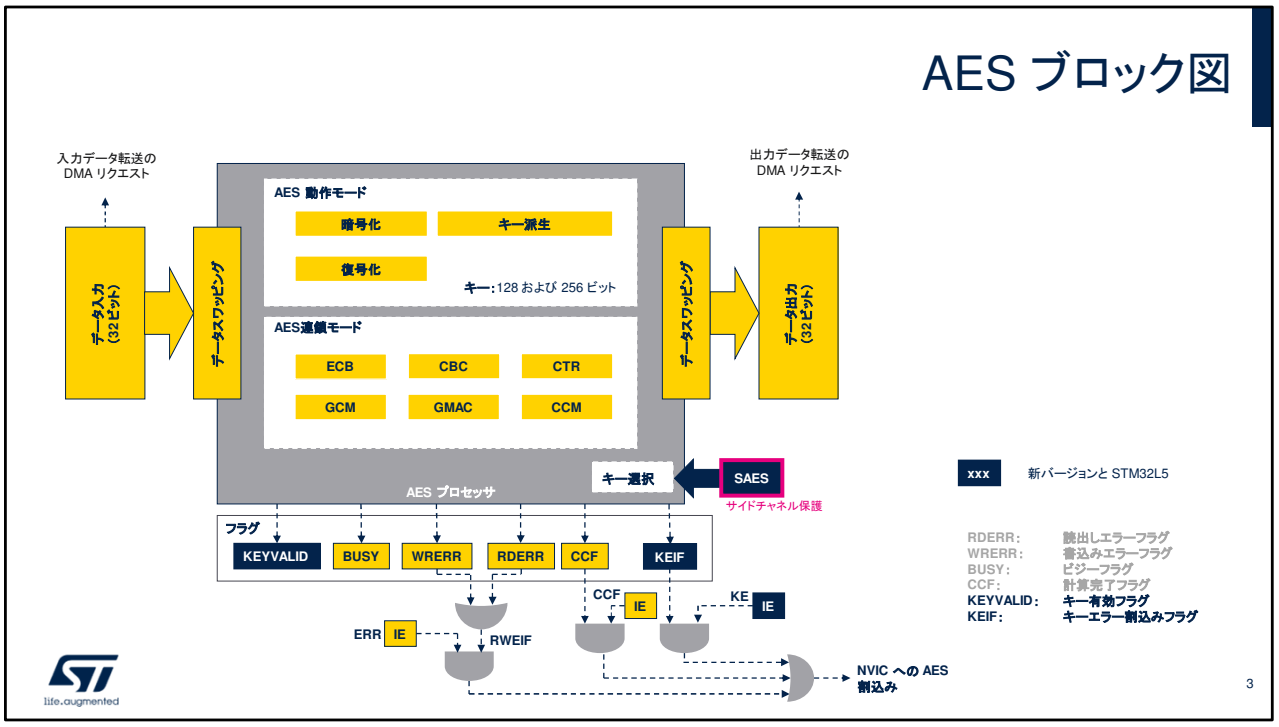
キー長	ECB	CBC	CTR	GCM				CCM			
				初期化	ヘッダ	ペイロード	タグ	初期化	ヘッダ	ペイロード	タグ
128 ビット	51(*)		51	64	35	51	59	63	55	114	58
256 ビット	75(*)		75	88	35	75	75	87	79	162	82

life.augmented

(*)復号化では、キー派生時間を 1 回追加する必要があります。

2

AES アクセラレータは、3 つの動作モードをサポートしています。
-暗号化
-復号化
-復号化のためのキー派生
選択された連鎖モードに応じて 128 または 256 ビット長の暗号化キーを使用して、128 ビットのデータブロックを処理します。
SAES ペリフェラルからの原子キー書込みおよびキーロードは、STM32U5 の新機能です。
キーロードシーケンスを開始すると、BUSY フラグがセットされ、KEYVALID フラグがクリアされます。
KEYSIZE で定義されたビット数が AES_KEYRx レジスタに転送されると、BUSY がクリアされ、KEYVALID がセットされ、EN ビットが書込み可能になります。
これにより、キーロード操作は正常に完了します。
この表には、連鎖モードとキー長に従って、データの 128 ビットブロックを処理するために必要なクロックサイクル数を示します。
AES モジュールでは、SAES モジュールから共有鍵をロードできます。この手順は、SAES で制御されます。



この AES ブロック図は、STM32L5 との比較で、STM32U5 でサポートされる新機能を示しています。

キー有効フラグとキーエラー割込みフラグは新機能です。

- KEYVALID は、有効なキーがキーレジスタにロードされたときにセットされます。
- KEYEIF は、キー情報がキーレジスタにロードできなかったときにセットされます。

STM32L5 にはそれ以外のフラグもあります。

- 読出しエラーフラグ(RDERR)は、計算フェーズまたは入力フェーズ中に予期しない読出し操作が検出されたときに、AES ステータスレジスタでセットされます。
- 書込みエラーフラグ(WRERR)は、計算フェーズまたは出力フェーズ中に予期しない書込み操作が検出されたときに、AES ステータスレジスタでセットされます。

AES 割込みイネーブルレジスタの読出しまたは書込みエラー割込みイネーブル(RWEIE)ビットが事前にセットされた場合に、これら 2 つのエラーフラグのいずれかがセットされているときに、割込みを生成できます。

AES アクセラレータが現在の動作のステータスを示すために、2 つの追加フラグを使用できます。

-計算完了時に、計算完了フラグ(CCF)がハードウェアによってセットされます。CCF 割込みイネーブルビットが事前にセットされた場合、割込みが生成されます。

- ビジーフラグ(BUSY)は、GCM モードでのみ使用され、暗号化モードの GCM ペイロードフェーズ中に、優先順位の高いメッセージにより現在のメッセージへの割込みが行えることを示します。

AES モジュールは、SAES によって制御されるサイドチャネル耐性 SAES ペリフェラルとのハードウェアキーの共有に対応しています(共有鍵モード)。

SAES 機能リスト（STM32U5 のみ）

- NIST FIPS197 準拠の AES 実装
- AES連鎖モード
  - 電子コードブック（ECB）
  - 暗号ブロック連鎖（CBC）
- **強化セキュアキーストレージ**
  - **ハードウェアキー（DHUK、BHK）**
    - **デバイス依存、DHUK を使用**
    - **アプリケーション依存、BHK を使用**
  - **ハードウェア秘密鍵の復号化（キーのアンラップ）**
  - **アトミックキーの書込み/ローディングの実施**
- 128 ビットデータブロック、128 または 256 ビットキーでの AES 動作モード
  - 暗号化、復号（関連するキー派生モード）
- キーモード：ノーマル、**ラップされて共有されるキー（より高速な AES エンジンによってロードされる）**
- サスペンド/レジュームおよび DMA サポート付き AHB スレーブ（IN + OUT チャネル）
- **サイドチャネル攻撃に対する耐性**

128 ビットブロックの処理に必要なサイクル数
➢ クロック周波数 = 48 MHz の監視不能クロック（SHSI）

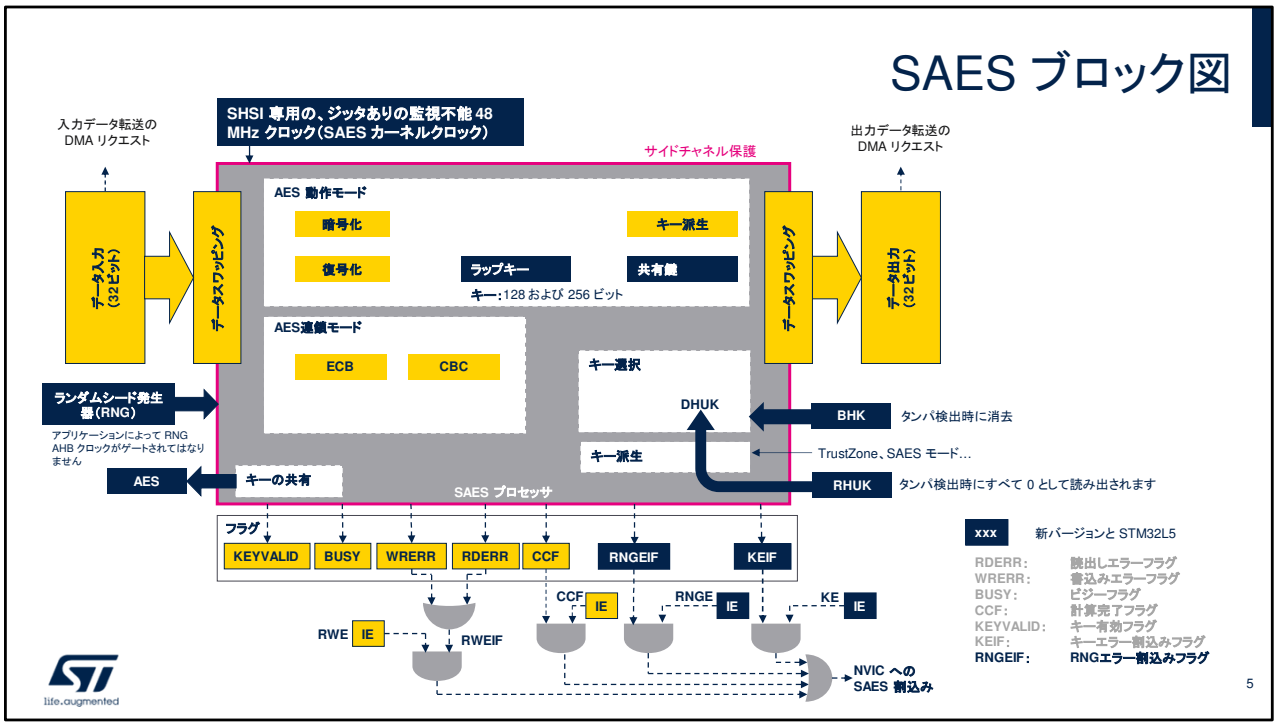
キー長	暗号化		復号化	
	ECB	CBC	ECB	CBC
128 ビット	528		528 [+200](*)	
256 ビット	743		743 [+324](*)	

(*) 復号化では、キー派生時間を 1 回追加する必要があります。

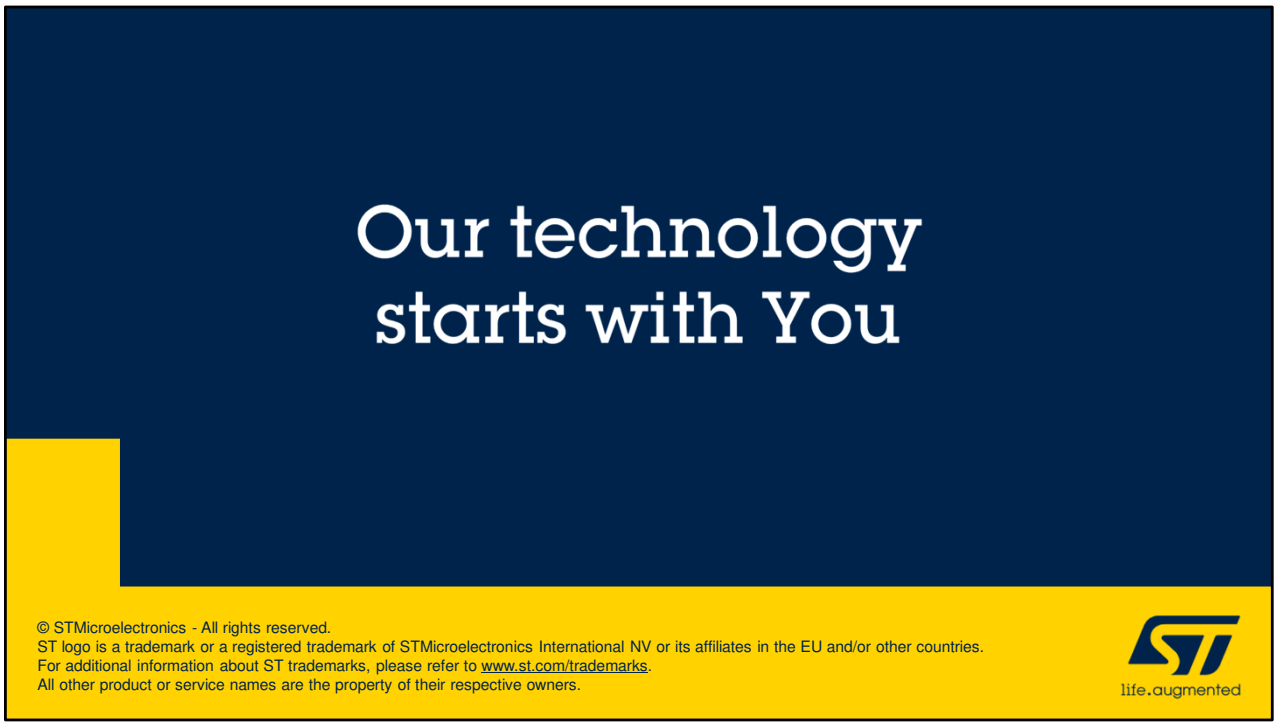
life.augmented

4

SAES は、AES モジュールと同様の機能を実装しています。それらは灰色で示しています。新機能は青色で示しています。
ECB および CBC の連鎖モードのみがサポートされます。
SAES は、ハードウェアによって秘密鍵（ブートハードウェアキー BHK および派生ハードウェア・ユニーク・キー DHUK）をロードすることができます。これらはアプリケーションで使用可能ですが、読出しはできません。
SAES ペリフェラルでは、アプリケーションキー BHK で排他的論理和を得るかどうかにかかわらず、これらのハードウェア秘密鍵 DHUK を使用してアプリケーションキーをラップ（暗号化）およびアンラップ（復号化）できます。
この機能により、プレーンテキストで（暗号化せずに）公開されることなく、AES キーをアプリケーションソフトウェアで使用できるようにすることができます。
SAES モジュールには、差動電力解析（DPA）などのサイドチャネル攻撃（SCA）に対する保護が組み込まれています。
この表は、連鎖モードとキー長に従って、128 ビットブロックのデータを処理するために必要なクロックサイクル数を示します。
性能は AES よりも低くなることに注意してください。
RCC によって提供される SHSI クロックの周波数は 48 MHz で、+/−15% のジッタが発生します。



この SAES ブロック図は、AES との比較で、SAES でサポートされる新機能を示しています。
まず、48 MHz のカーネルクロックは監視できません。これは外部からは確認できません。
その後、RCC でモジュールリセットがトリガされた後、SAES により RNG ペリフェラルから自動的に乱数がフェッチされます。
RNGEIF がセットされている場合、SAES は使用できません。RNG ペリフェラルから乱数をフェッチしているときに、不良エントロピーなどによりエラーが検出された場合、このフラグがセットされます。
SAES では、ハードウェアによって秘密鍵 DHUK および BHK をロードされる可能性があります。
これらのキーは、タンパが検出されたときにクリア/消去できるので、攻撃者はすべての機密情報を解読できません。
SAES キー共有機能が有効化されている場合、DHUK と BHK を除いて、SAES によって管理されるキーはすべて AES モジュールと共有できることに注意してください。



新しい強化セキュリティキーストレージ機能とラップ/共有鍵モードの詳細については、強化セキュアキーストレージのトレーニングモジュールを参照してください。