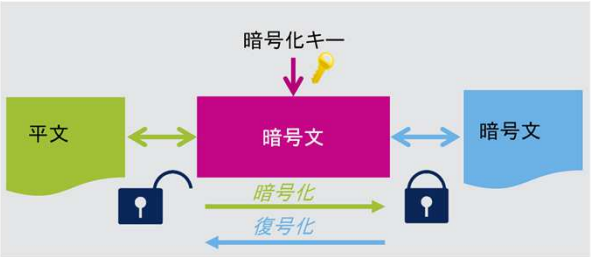
こんにちは、STM32高度暗号化標準ハードウェア·アクセラレータのプレゼンテーションへようこそ。
これは、AESの機能をカバーする暗号化のアプリケーションのために広く使われているインタフェースです 。

概要



- 安全性の高い暗号化キーを使って、平文と呼ばれるオリジナルのテキストを、暗号文と呼ばれる解読できないテキストに変換
  - 幅広い設定が可能
  - 多くの標準の操作モードおよび種々のキーサイズに適用可能

アプリケーションの利点

- データの機密を保護
- CPU処理時間の低減

life.augmented

AESアルゴリズムは、128または256bit の長さである秘密の暗号法キーを使って、情報を暗号化または復号化する対称のブロック暗号文です。
暗号化により、データは、暗号文と呼ばれる解読しにくいフォーマットに変換されます：暗号文を暗号解読することによって、データをそのオリジナルのフォーマットの平文逆変換します。
アプリケーションは、短時間処理だけでなくデータの機密を保護するために、AESアルゴリズムのNIST FIPS 197に準拠したインプリメンテーションを行うという利点もあります。

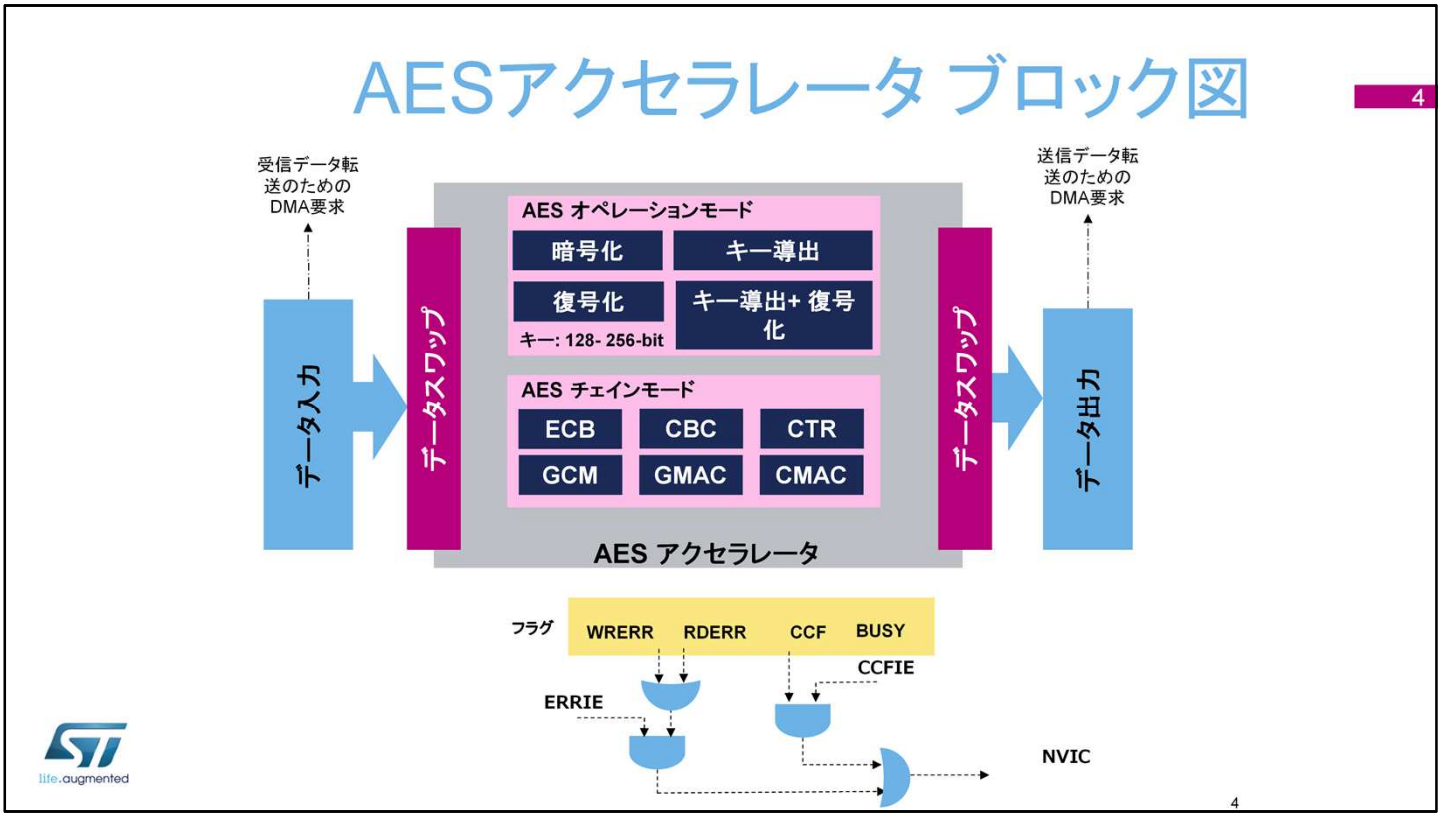
主な特徴

AESのNIST FIPS 197準拠のインプリメンテーション

- AESは以下のオペラーションモード適用可能:
  - 暗号化
  - キーの導出
  - 復号化
  - キーの導出+ 復号化
- AESは、128または256bit のキー長を用いたアルゴリズム適用可能:
  - **E**lectronic **C**ode**B**ook (ECB)
  - **C**ipher **B**lock **C**haining (CBC)
  - **C**oun**T**e**R** mode (CTR)
  - **G**alois **C**ounter **M**ode (GCM)
  - **G**alois **M**essage **A**uthentication **C**ode mode (GMAC)
  - **C**ipher **M**essage **A**uthentication **C**ode mode (CMAC)

life.augmented

AESアクセラレータは4つの操作モードをサポートします：暗号化、キーの導出、復号化、キーの導出＋復号化。
128または256bit の長さである暗号キーを使って、128bitデータブロックを処理します。それは、次のスライドに示されるように、選択されたチェインモードに基づいています。



AESのブロック図は、基本的機能とコントロールモジュールを示します。
AESアクセラレータは、データのスワッピングオプションの有り/無しで、256bit または128bit の長さの暗号キーを使って128bit データブロックを処理します。

AESアクセラレータには4つのオペレーションモードがあります:
・モード1:AESキーレジスタにストアーされている暗号キーを使った暗号化です。
・モード2:AESアクセラレータを有効にする前に、AESキーレジスタにストアした値に基づいた新しいキーを導出します。このモードは、AESチェインモード選択から独立しています。
・モード3:AESキーレジスタにストアーされている、与えられた(あらかじめ計算された)暗号解読キーを使った複合化です。
・モード4:キー導出+AESキーレジスタにストアーされている暗号化キーを使った複合化です(チェインアルゴリズム のため

のカウンターモードにおいてAESが設定される時には使われない）。

AESアクセラレータは、6つのチェインアルゴリズムまたはモードをサポートします：

Electronic codebook (ECB)→これは初期値のモードです。このモードはAES_IVRレジスタを使いません。チェインオペレーションはありません。
メッセージはブロックに分けられて、個々のブロックは別々に暗号化されます。

Cipher block chaining (CBC)→ 暗号化される前に、平文の個々のブロックが、前の暗号文ブロックとのXORになります。個々のメッセージをユニークにするために、最初のブロックを処理する時に、初期設定ベクトルが使われます。

Counter mode (CTR)→ 32bit カウンターが、XOR演算のノンス値（使い捨てのランダムな値)に加えて、暗号文または平文に使われる。

Galois counter mode (GCM)→ 対応した暗号文とTAGを生成して平文を暗号化し、認証するために使用されます（また、メッセージ認証コードまたはメッセージの完全性チェックとして知られています）。それは機密保持のためのAESのカウンターモードに基づき、TAGを生成するための固定された有限のフィールドの上の係数を使います。それは最初に初期設定ベクトルを必要とします。

Galois message authentication code mode (GMAC)→ GMACは、ヘッダーだけにより構成されているメッセージに適用されたGCMと同じです。すべてのステップと設定は、ペイロードフェーズが使われない事を除いて同じです。

Cipher message authentication code mode (CMAC).→ CMACは、平文を認証するために使用され、対応したTAGを生成します。メッセージはヘッダーフェーズとタグフェーズだけで構成されます。CCM標準は最初の認証ブロックのための具体的なエンコーディング規則を定義します（標準の中でB0と呼ばれるものです ）。特に最初のブロックはフラグ、ノンス、バイトで表現されたペイロード長さを含みます。

エラーフラグブロックは2種の異なるフラグ経由で、AESアクセラレータの振る舞いをチェックします：計算フェーズまたはインプットフェーズの間に、予想外の読出しオペレーションが検出される時には、AESステータスレジスタの読みだしエラーフラグ（RDERR）がセットされます。
アウトプットフェーズまたは計算フェーズの間に予想外の書込みオペレーションが検出された時には、AESステータスレジスタの書込みエラーフラグ（WRERR）がセットされます。
もし、その前にAESコントロールレジスタのエラー割込み有効化（ERRIE）ビットが設定されたならば、これらの2つのエラーフラグのうちのどちらか1つがセットされる時に、割込み発生します。

現在のオペレーションのステータスを与えるために、2つの特別なフラグがAESアクセラレータで利用可能です：計算が完了した時には、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。もし、その前にCCF割込み有効化ビットが設定されるならば、割込みが生成されます。
ビジーフラグ〈GCMモードだけで使用される〉は、暗号化モードのためのGCMペイロードフェーズの間に、より高いプライオリティメッセージが現在のメッセージに割り込むことができることを示します。

AES 処理時間 (1/3)

Processing time (in clock cycle)

Mode of operation	Input phase	Computation phase	Output phase	Total
Mode 1: Encryption	8	202	4	214
Mode 2: Key derivation	-	80	-	80
Mode 3: Decryption	8	202	4	214
Mode 4: Key derivation + decryption	8	276	4	288

life.augmented

以下のスライドは、選択されたチェインモードに従ったオペレーションモードのうちのそれぞれの処理時間です。

AES 処理時間 (2/3)

Processing time (in clock cycle) for ECB, CBC and CTR

Key size	Mode of operation	Algorithm	Input phase	Computation phase	Output phase	Total
128-bit	Mode 1: Encryption	ECB, CBC, CTR	8	202	4	214
	Mode 2: Key derivation	-	-	80	-	80
	Mode 3: Decryption	ECB, CBC, CTR	8	202	4	214
	Mode 4: Key derivation + decryption	ECB, CBC	8	276	4	288
256-bit	Mode 1: Encryption	ECB, CBC, CTR	8	286	4	298
	Mode 2: Key derivation	-	-	109	-	109
	Mode 3: Decryption	ECB, CBC, CTR	8	286	4	298
	Mode 4: Key derivation + decryption	ECB, CBC	8	380	4	392

life.augmented

ここでは、キーサイズとアルゴリズムに依存する処理時間です

AES 処理時間 (3/3)

Processing time (in clock cycle) for GCM and CMAC

Key size	Mode of operation	Algorithm	Init Phase	Header phase	Payload phase	Tag phase
128-bit	Mode 1: Encryption/ Mode 3: Decryption	GCM	215	67	202	202
	-	GMAC	215	67	-	202
	-	CMAC	-	206	-	202
256-bit	Mode 1: Encryption/ Mode 3: Decryption	GCM	299	67	286	286
	-	GMAC	299	67	-	286
	-	CMAC	-	290	-	286

life.augmented

ここでは、GCMアルゴリズムのための処理時間です。

割込みとDMA

割り込みイベント	説明
AES 計算完了フラグ	計算が完了するとセット
AES 読出しエラーフラグ	レジスタの外のAESデータからの予期せぬ読出しオペレーションが検出される時に設定される（計算またはデータインプットフェーズの期間）。
AES 書込みエラー	レジスタのAESデータへの予期せぬ書込みオペレーションが検出される時に設定されます（計算またはデータアウトプットフェーズの期間）

- DMA機能: 2チャンネル、受信データ用、および処理された送信データ用
  - 入力用のDMA要求チャンネル:AESデータレジスタ（AES_DINR）に、書込みが要求されると、AESはINPUTフェーズの間にDMA要求（AES_IN）を開始。
  - 出力用のDMA要求チャンネル: AESデータアウト（AES_DOUTR）レジスタからから読出しが要求されると、AESはOUTPUTフェーズの間にDMA要求（AES_OUT）を開始。

life.augmented

NVICの割込みを引き起こすイベント：AESの計算完了、AES読みだしエラー、AES書込みエラー
DMAアクセス要求は受信と送信データ用に内部で発生します。
DMAチャンネルは、メモリー-周辺装置または周辺-メモリーモードにおいて32bit データサイズで設定されなければなりません。

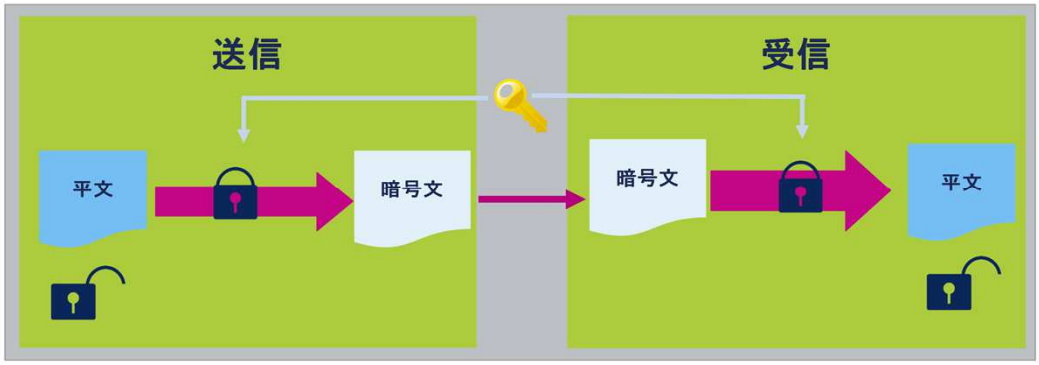
低消費電力モード

Mode	Description
Run	動作
Sleep	動作、周辺の割込みでデバイスのSleepモードから復帰
Low-power run	動作
Low-power sleep	動作、周辺の割込みでデバイスのLow-power sleepモードから復帰
Stop 1	停止、周辺機能のレジスタ内容は保持
Stop 2	停止、周辺機能のレジスタ内容は保持
Standby	パワーダウン、Standbyモードから復帰後は再初期化が必要.
Shutdown	パワーダウン、**Shutdown**モードから復帰後は再初期化が必要.

life.augmented

低消費電力モードの時の、AESアクセラレータのステータスの概要です。
デバイスがStopモードの時は、AESオペレーションは不可です。

アプリケーション例 (1/2)

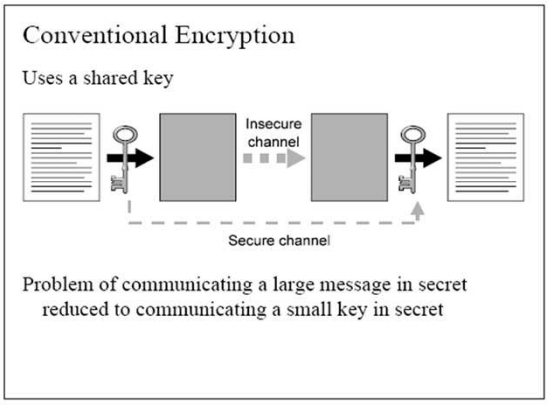


AESの共通オペレーション

AES暗号化と復号化アルゴリズムは、セキュリティネットワーキングルータ、無線通信、セキュリティスマートカード、セキュリティ監視テレビ装置、セキュリティ電子金融取引などを含む暗号化されたデータストレージなどの各種のアプリケーションに適しています。
送信側は、秘密キーで暗号化された平文を送り、受信側は同じ秘密のキーのメッセージを復号化します。

アプリケーション例(2/2)

- 例
  - AES-128, -256
- 利点
  - 通常のプロセッサをしても簡単/高速処理が可能で、コプロセッサを使うともっと、もっと高速になる。
- 難点
  - キーの配布
    - 他の暗号化を使って送られるが使われる
    - セキュリーティハードウェアで送られる
    - キー操作



life.augmented

関連する周辺機能

- これらの周辺機能に関連する周辺機能のトレーニング資料をご参照ください
  - RCC (AES クロック制御、AES 有効化 / リセット)
  - 割込み (AES 割込みマッピング)

life.augmented

参考

- より詳しい内容、追加情報は以下を参照してください。:
  - AN4230: STM32F2xx, STM32F4xx Random Number Generation Validation using NIST Statistical Test Suite.
  - AN4023 & AN4024: STM32 Secure Firmware Update(SFU)
  - UM0586: STM32 Cryptographic Library

life.augmented

詳細については、STのウェブサイトから入手可能なアプリケーションノートとユーザマニュアルを参照してください。