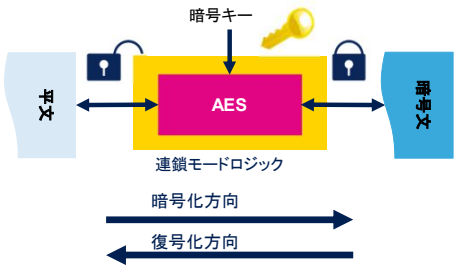
STM32 高度暗号化標準ハードウェアアクセラレータのプレゼンテーションへようこそ。このハードウェアアクセラレータは、暗号化機能を含め、STM32G0 アクセスラインのデバイス（STM32G08x マイクロコントローラ）に搭載されています。ここでは、暗号化アプリケーションに幅広く使用される AES インタフェースの機能について説明します。

概要



- 安全な暗号化キーを使用して、平文と呼ばれる元のテキストを暗号文と呼ばれる解読不能なテキストに変換
  - ハードウェア・アクセラレータとして設計され、CPUまたはDMAで使用
- 多くの標準動作モードと2つのキー・サイズ（128または256ビット）に対応

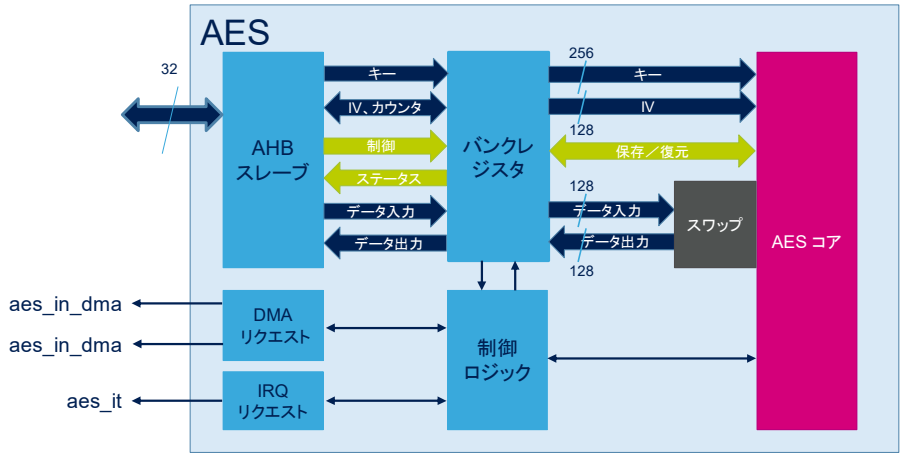
アプリケーション側の利点

- データの機密性および／または認証性を保護
- CPU処理時間を短縮

life.augmented

AES アルゴリズムは、128 または 256 ビット長の秘密の暗号化キーを使用して、情報を暗号化および復号化するために使用される対称ブロック暗号です。暗号化はデータを暗号文という解読できないフォーマットに変換します。一方、復号化は暗号文を変換して、平文という元のフォーマットに戻します。
AES ペリフェラルは、AES アルゴリズムの NIST FIPS 197 に準拠した実装で、処理時間の点ではソフトウェアライブラリよりも効率的です。AES ペリフェラルは複数の連鎖モードをサポートし、モードに応じて、データの機密性やデータの機密性と認証性を保護します。

AESブロック図



平文データを暗号文に暗号化したり、その反対に暗号文を平文に復号化したりするには、すべてをソフトウェアで行うと大きな負荷となる集中的な演算が必要となります。AES ハードウェアアクセラレータは、AES コアで暗号化／復号化処理を実行することにより、STM32G08x CPU の負荷を軽減します。

AES ブロックは AHB スレーブの 1 つです。CPU がデータ、キー、初期化ベクタをメモリマップレジスタに書き込んで AES ブロックに渡した後にレジスタを読み出して結果を取得することも、2 つの DMA チャネル（AES へのデータの書込みと結果の読出しの 2 つのチャネル）によってデータの移動を確保することもできます。

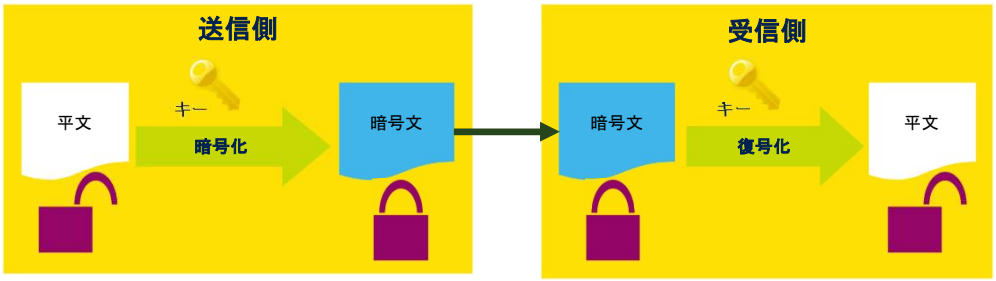
AES がより優先順位の高い別メッセージを処理する必要がある場合は、ソフトウェアでメッセージをサスペンドしてから元のメッセージのレジュームができます。

AES コアはデータ処理を担当するユニットです。そのロジックは 1、8、16、32 ビットデータスワッピングに対応しています。

内部データパスは、データと初期化値については 128 ビット幅、キーについては 256 ビット幅です。128 ビットキーもサポートしています。

AESを使用した機密性の保護

- 暗号化は、平文またはクリア･テキストと呼ばれる元のデータを、暗号文と呼ばれる、ランダムで読取り不能に見える形式に変換する方法。
- 第1の目標：データの機密性の保護

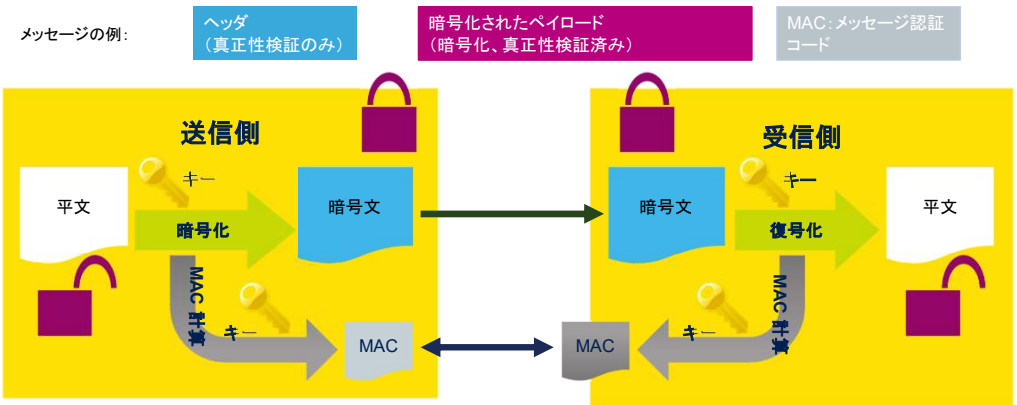


life.augmented

AES の暗号化および復号化アルゴリズムは、セキュアなネットワーキングルータ、無線通信、暗号化データストレージなどの各種アプリケーションに適しています。これには、セキュアスマートカード、セキュアビデオ監視システム、セキュア電子金融取引などが含まれます。
送信側は秘密鍵を使用して平文メッセージを暗号化します。受信側は同じ秘密鍵を使用してメッセージを復号化します。
したがって、AES は対称鍵に基づいています。つまり、同じ鍵が暗号化と復号化の両方に使用されます。

AESを使用した認証済み暗号化

- メッセージの機密性の保護だけでなく、受信側では、メッセージが本物であり、送信中に変更が加えられていないことを確認したい場合がある
  - それには、メッセージ認証コード（MAC）計算と呼ばれる追加の処理を実行する



メッセージ認証コードを暗号文に追加すると、受信側では、メッセージの送信元が想定どおりの送信者であることを確認できます。
AES ブロックはデータ暗号化とともに、MAC を生成できます。

AESの機能(1/3)

- NIST FIPS 197に準拠した高度暗号化標準(AES)アルゴリズムの実装。
- NISTによって標準化された6つのAES連鎖モード:
  - 128ビット・ブロックを処理する「ブロック」暗号モード
    - 1) 電子コード・ブック(ECB)
    - 2) 暗号ブロック連鎖(CBC)
  - あらゆるデータ・サイズを処理する「ストリーム」暗号モード(メッセージがモジュロ128ビットである必要はない)
    - 3) カウンタ・モード(CTR)
  - MAC計算を使用した特殊なストリーム暗号である「認証済み」暗号モード
    - 4) ガロア・カウンタ・モード(GCM)
    - 5) GCMの1種であるガロア・メッセージ認証コード・モード(GMAC)
    - 6) CBC-MAC付きカウンタ(CCM)

life.augmented

米国国立標準技術研究所(NIST)は、暗号化標準を規定する、連邦情報処理規格(FIPS)公報を作成しています。
ブロック暗号モードは、暗号化されるデータがバッファに格納されている場合に有用です。
ストリーム暗号モードは、ビットレベルで(ブロックレベルではない)データを効率的に暗号化または復号化する場合に有用です。このモードではキースケジューリングは不要です。
認証済みモードは、メッセージ認証コード(MAC)と暗号化データ(有効化されている場合)の生成に使用されます。

AESの機能(2/3)

- 3つのAES動作モード:
  - モード1:暗号化
  - モード2:復号化のためのキー派生(ECBおよびCBCのみ)
  - モード3:復号化

life.augmented

AES には次の 3 つの動作モードがあります。

- モード 1:平文暗号化
- モード 2:電子コードブック(ECB)または暗号ブロック連鎖(CBC)復号化キー派生。ECB または CBC の連鎖モードでモード 3 を選択する前に使用する必要があります。AES アクセラレータを有効にする前に、AES キーレジスタに格納されている値に基づいて、新しいキーがキー派生によって生成されます。
- モード 3:暗号文の復号化

AESの機能(3/3)

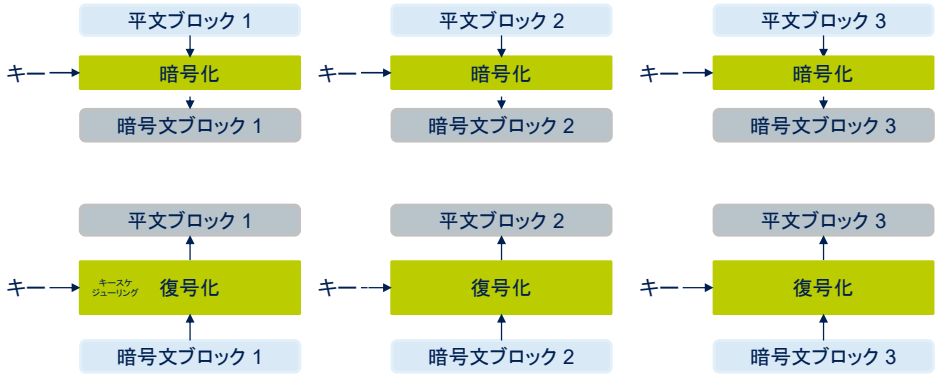
- 128および256ビット・キー(書込み専用*)をサポート
- 128ビット・データ・ブロックの処理
  - メッセージ・サイズがブロック・サイズの倍数でない場合は、ECBおよびCBCモードではソフトウェアを使用して暗号文借用(ciphertext stealing)技術を実装する必要がある
- 1、8、16、32ビット・データをサポートするデータ・スワッピング・ロジック
- 優先順位の高い別のメッセージを処理する必要がある場合に、メッセージをサスペンド
- DMA 機能:2つのチャネル(1つは受信データ用、もう1つは送信データ用)

(*) G0 128K 460 および 64K 466

life.augmented

AES キーは 128 または 256 ビット長です。
データスワッピングは、128 ビットデータブロック内の 1、8、16、または 32 ビットのスワッピングに対応しています。
サスペンド／レジュームメカニズムによって、処理するメッセージの優先度に応じたプリエンプションが可能です。
サイズがブロックサイズ(128 ビット)の倍数ではないメッセージを管理する場合、ソフトウェアは、NIST 特別公報 800-38A の付録に記述されているような暗号文借用(ciphertext stealing)技術を実装する必要があります。

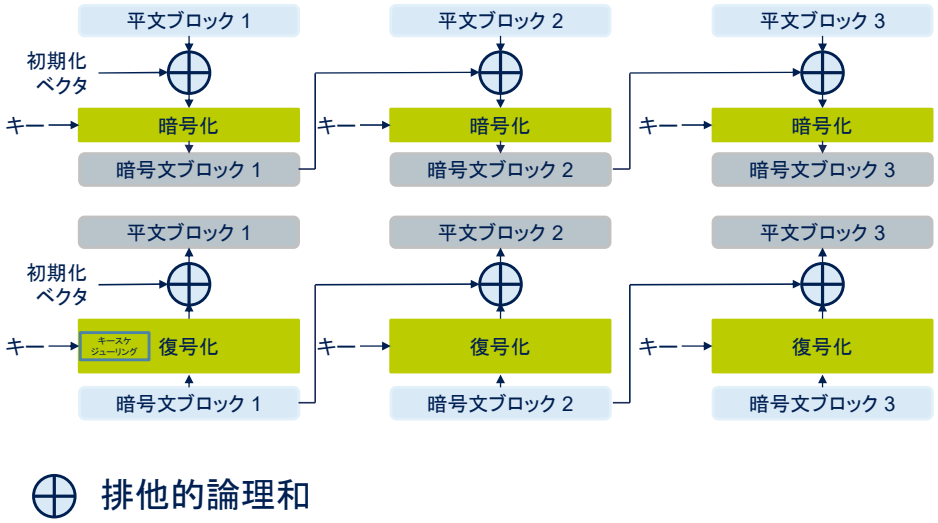
ECB（電子コード・ブック）



life.augmented

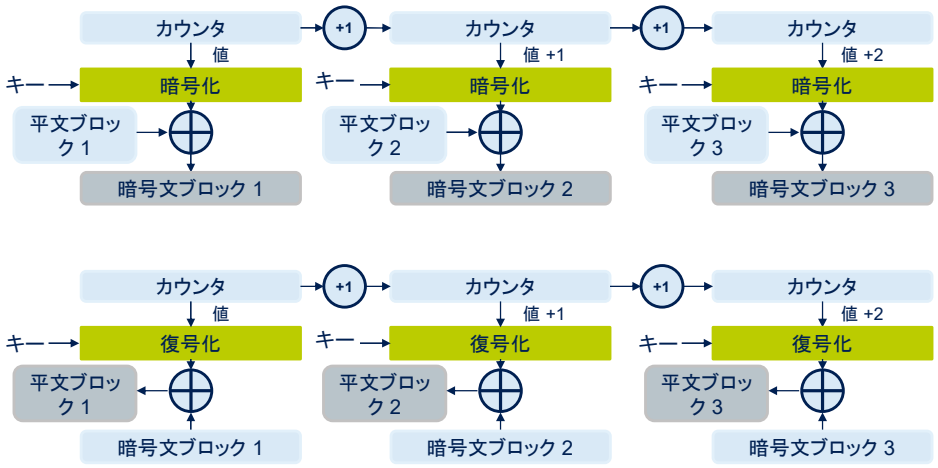
ECB は最も単純な動作モードです。連鎖処理も、特別な初期化ステージもありません。メッセージはブロックに分割され、各ブロックが個別に暗号化または復号化されます。
ECB の復号化では、最初のラウンドの復号化のキーを、暗号化の最終ラウンドのキーから導出する必要があります。これは、復号化を行う前に、暗号化の完全なキースケジュールが必要となるためです。

暗号ブロック連鎖（CBC）モード



CBC モードでは、プレーンテキストの各ブロックが前の暗号テキストブロックとの排他的論理和をとってから暗号化されます。各メッセージを一意にするために、最初のブロック処理時に初期化ベクタが使用されます。
CBC の復号化では、最初のラウンドの復号化のキーを、暗号化の最終ラウンドのキーから導出する必要があります。これは、復号化を行う前に、暗号化の完全なキースケジュールが必要となるためです。

カウンタ(CTR)モード

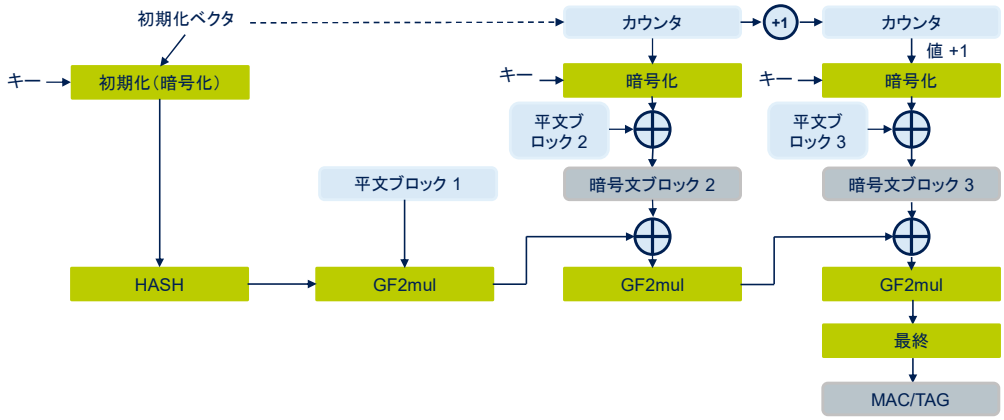


life.augmented

⊕ 排他的論理和

カウンタ(CTR)モードでは、AES コアを使用してキーストリームを生成します。キーは、その後平文との排他的論理和をとって暗号文を得ます。
この連鎖スキームでは、キーストリームまたはカウンタブロックの生成に AES コアが暗号化モードで必ず使用されるため、ECB モードや CBC モードとは異なり、CTR モードでの復号化にキースケジューリングは必要ありません。

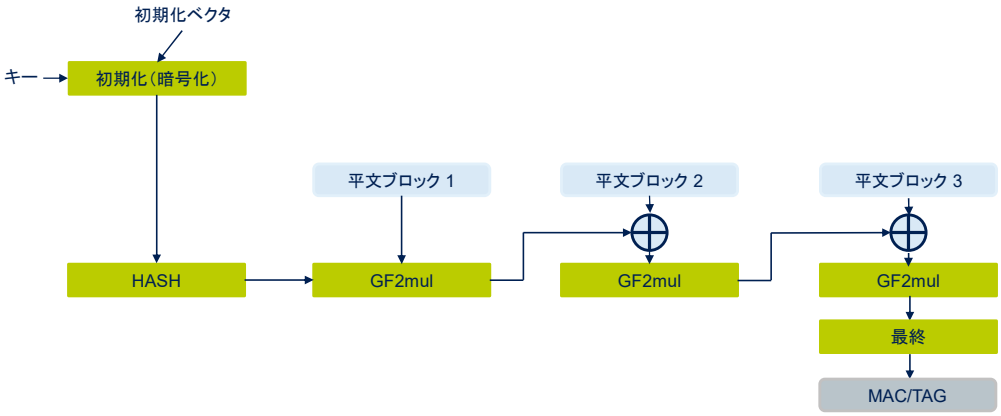
ガロア／カウンタ·モード（GCM）



⊕ 排他的論理和

ガロア／カウンタモード（GCM）では、平文メッセージが暗号化されている間に、並列でメッセージ認証コード（MAC）が計算され、対応する暗号文とその MAC（認証タグとも言います）が生成されます。機密性のために AES のカウンタモードに基づいており、固定の有限フィールドに乗算器を使用してタグを生成します。最初に初期化ベクタが必要です。
GCM メッセージの一部（ここではブロック 1）は暗号化されないことがあります（認証済みヘッダと呼ばれます）。

ガロア･メッセージ認証コード（GMAC）モード

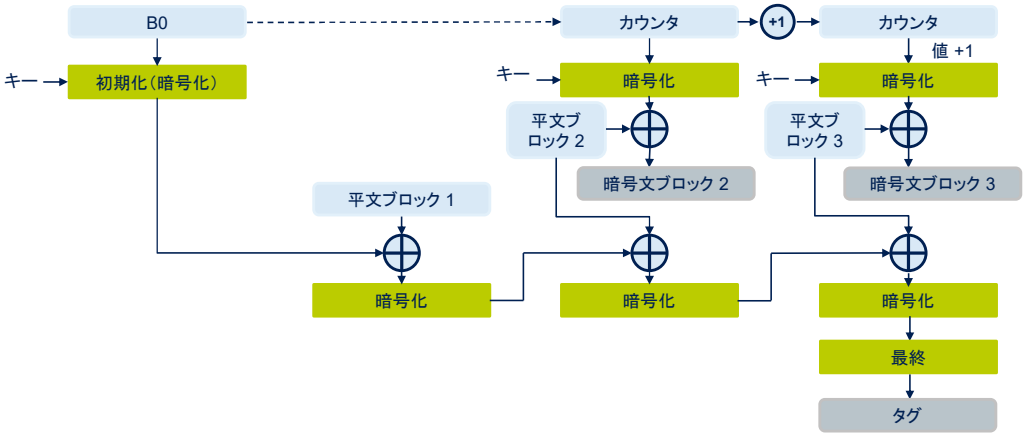


⊕ 排他的論理和

life.augmented

ガロアメッセージ認証コード（GMAC）を使用すると、メッセージの認証と、対応するメッセージ認証コード（MAC）の生成が可能となります。
平文の認証済みヘッダのみで構成されたメッセージ（すなわち、ペイロードなし）に適用されることを除けば、GMAC は GCM と似ています。
ペイロードフェーズが使用されないことを除くと、手順と設定は GCM とすべて同じです。

CBC-MAC付きカウンタ(CCM)モード



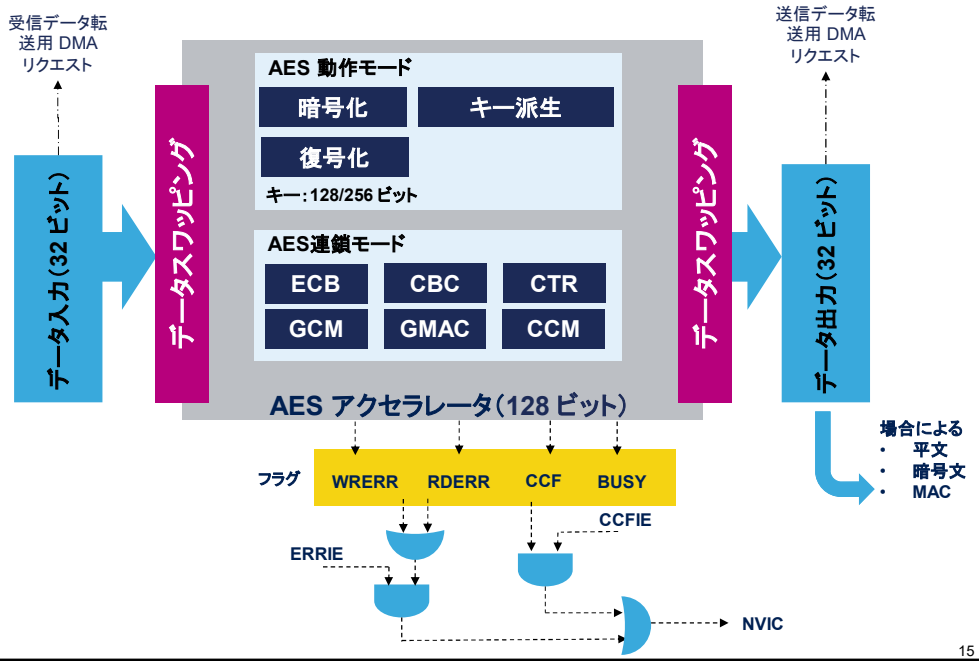
暗号ブロック連鎖-メッセージ認証コード付きカウンタ(CCM)モードでは、平文メッセージのペイロード部が暗号化されている間に、並列でそのメッセージ全体に対するメッセージ認証コード(MAC)が計算され、対応する暗号文と対応する MAC(タグとも言います)が生成されます。

CCM モードは、機密性のためにカウンタモードの AES に基づいており、CBC を使用してメッセージ認証コードを計算します。初期値が必要です。

CCM 規格は、最初の認証ブロック(標準では B0 と呼ばれる)に対して特定の暗号化規則を定義しています。具体的に言うと、最初のブロックにはフラグ、ノンス、ペイロード長(単位:バイト)が含まれています。

CCM 連鎖モードは、GCM のように平文の認証済みデータのみで構成されたメッセージ(すなわち、ヘッダのみでペイロードなし)に適用できます。ただし、これは NIST では推奨されていません。CCM のこのような使用方法は CMAC と呼ばれない(GCM/GMAC とは異なります)ことに注意してください。CMAC は SP800-38B に規定されている別種の NIST モードです。

AESアクセラレータ·ブロック図



AES アクセラレータのこの簡易ブロック図には、左側のデータ入力から右側のデータ出力へのデータパスが示されています。
AES アクセラレータは、データスワッピングオプションの使用に関係なく、128 ビットまたは 256 ビット長の暗号化キーを使用して、128 ビットデータブロックを処理します。
エラーフラグブロックは、次の 2 種類のフラグを使用して AES アクセラレータの動作を確認します。
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にセットされます。
書込みエラーフラグ(WRERR)は、出力フェーズまたは計算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にセットされます。
AES 制御レジスタのエラー割込み有効化(ERRIE)ビットが事前にセットされていた場合、これら 2 つのエラーフラグの 1 つがセットされたときに割込みを生成できます。
計算完了フラグ(CCF)は、計算が完了したときに、ハードウェアによってセットされます。CCF 割込み有効化ビットが以前にセットされていた場合は、割込みが生成されます。
ビジーフラグは GCM モードでのみ使用され、暗号化モードの場合に、GCM ペイロードフェーズ中に優先順位の高いメッセージが現在のメッセージに割込みできることを示します。

AES処理時間(1/2)

- 処理時間(AHBクロック・サイクル・ユニットの128ビット・データ・ブロック当たり)

キー長	動作モード	アルゴリズム	入力フェーズ	計算フェーズ	出力フェーズ	合計
128 ビット	モード 1:暗号化	ECB、CBC、CTR	9	38	4	**51**
	モード 2:キー派生	-	-	59	-	**59**
	モード 3:復号化	ECB、CBC、CTR	9	38	4	**51**
256 ビット	モード 1:暗号化	ECB、CBC、CTR	13	58	4	**75**
	モード 2:キー派生	-	-	82	-	**82**
	モード 3:復号化	ECB、CBC、CTR	13	58	4	**75**

life.augmented

ここには、各種キーサイズとアルゴリズムに対する処理時間が示されています。

AES処理時間(2/2)

- 処理時間(AHBクロック·サイクル·ユニットの128ビット·データ·ブロック当たり)
  - 注:ヘッダに1つのデータ·ブロック、ペイロードに1つのデータ·ブロック(GCM、CCM)

キー長	動作モード	アルゴリズム	初期フェーズ	ヘッダフェーズ	ペイロードフェーズ	タグフェーズ	合計
128 ビット	モード 1:暗号化 モード 3:復号化	GCM	64	35	51	59	**209**
		CCM	63	55	114	58	**290**
	-	GMAC	64	35	-	59	**158**
256 ビット	モード 1:暗号化 モード 3:復号化	GCM	88	35	75	75	**273**
		CCM	87	79	162	82	**410**
	-	GMAC	88	35	-	75	**198**

life.augmented

ここには、各種キーサイズとアルゴリズムに対する処理時間が示されています。

割込みおよびDMA

割込みイベント	説明
AES計算完了フラグ	計算が完了したときにセットされる。
AES読出しエラーフラグ	AESデータ出力レジスタからの予期しない読出し操作が 検出された場合にセットされる(計算フェーズまたはデータ入力フェーズ中に)。
AES書込みエラーフラグ	AESデータ入力レジスタへの予期しない書込み操作が検出された場合にセットされる (計算フェーズまたはデータ出力フェーズ中に)。

- DMA機能:2チャネル。1つは受信データ用、もう1つは処理済みの送信データ用。
  - 入力用DMAリクエスト・チャネル:AESはINPUTフェーズ中、AESデータ入力(AES_DINR)レジスタにワードを書き込む必要があるたびに、DMAリクエスト(AES_IN)を開始する。
  - 出力用DMAリクエストチャネル:AESはOUTPUTフェーズ中、AESデータ出力(AES_DOUTR)レジスタからワードを読み出す必要があるたびに、DMAリクエスト(AES_OUT)を開始する。

life.augmented

ここでは、ネスト化されたベクタ割込みコントローラで割込みをトリガできるイベント(AES 計算完了、AES 読出しエラー、および AES 書込みエラー)をまとめて示しています。
ダイレクトメモリアクセスリクエストは、受信データと送信データ両方に対して内部で生成されます。DMA チャネルは、32 ビットデータサイズで、メモリからペリフェラルへの転送モードまたはペリフェラルからメモリへの転送モードに設定する必要があります。

低消費電力モード

モード	説明
RUN	アクティブ。
SLEEP	RCCで無効。
低消費電力RUN	アクティブ。
低消費電力SLEEP	RCCで無効。
STOP 0/STOP 1	停止。ペリフェラルレジスタの内容は保たれる。
STANDBY	パワーダウン状態です。ペリフェラルは、STANBYモード終了後に再初期化する必要があります。
SHUTDOWN	パワーダウン状態。ペリフェラルは、SHUTDOWNモード終了後に再初期化する必要がある。

life.augmented

ここでは、各低消費電力モードでの AES アクセラレータのステータスの概要を示します。
デバイスが STOP モードの場合は、AES の動作は不可能です。

関連ペリフェラル

- 次のペリフェラルに関連するペリフェラルトレーニングを参照
  - RCC（AESクロック制御、AESイネーブル／リセット）
  - 割込み（NVIC）
  - ダイレクト・メモリ・アクセス（DMA）コントローラ

これは、AES アクセラレータに関連したペリフェラルのリストです。詳細については、必要に応じてこれらのペリフェラルトレーニングを参照してください。

参照

- 詳細および追加情報については、以下を参照:
  - 米国国立標準技術研究所(NIST)
    - SP800-38A:Ciphertext Stealing for CBC Mode(CBC モード用暗号文借用)
    - SP800-38A:Recommendation for Block Cipher Modes of Operation(ブロック暗号の推奨動作モード)
    - SP800-38D:Galois/Counter Mode (GCM) and GMAC(ガロア／カウンタ・モード(GCM)およびGMAC)
    - SP800-38C:CCM Mode for Authentication and Confidentiality(認証および機密性のためのCCM モード)
    - AES Algorithm Validation Suite(AESAVS)
  - UM0586:STM32暗号ライブラリ

life.augmented

詳細については、弊社 Web サイトで入手可能なこれらの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。