



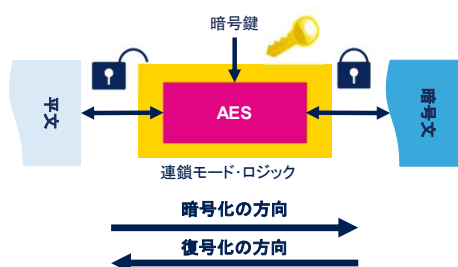
# STM32G4 – AES

Advanced Encryption Standard ハードウェア・アクセラレータ

1.0版



STM32 の Advanced Encryption Standard ハードウェアアクセラレータのプレゼンテーションによろこそ。ここでは、暗号アプリケーションで広く使用されている AES インタフェイスの機能の説明を行います。



- 平文と呼ばれる元のテキストを暗号文と呼ばれる読取り不能テキストにセキュアな暗号鍵を用いて変換
  - CPUまたはDMAIによって使用されるハードウェア・アクセラレータとして設計
- 多くの標準動作モードと2種類の鍵サイズ(128bitまたは256bit)に対応

### アプリケーション側の利点

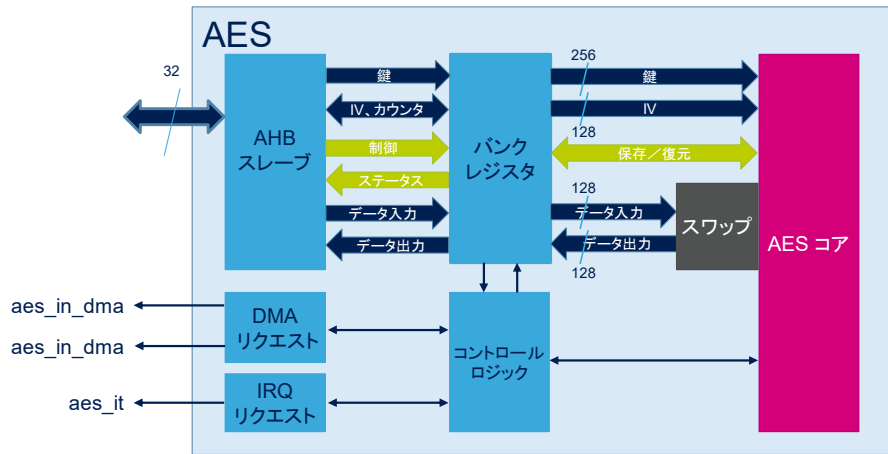
- データの機密性と真正性を保護
- CPU処理時間の低減

AES アルゴリズムは、128bit 長か 256bit 長の秘密暗号鍵を用いて情報の暗号化と復号化を行うための対称ブロック暗号です。暗号化では、暗号文と呼ばれる判読不能なフォーマットにデータを変換し、復号化では、平文と呼ばれる元のフォーマットに暗号文を変換します。

AES ペリフェラルには、AES アルゴリズムが NIST FIPS 197 準拠で実装されており、処理時間についてはソフトウェアライブラリよりも高効率です。AES ペリフェラルは複数の連鎖モードに対応しており、モードに応じて、データの機密性またはデータの機密性および真正性を保護します。

## AES ブロック図

3



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によって、AES コアの中で暗号化と復号化の処理が行われ、CPU の負荷が軽減されます。

AES ブロックは AHB スレーブの1 つです。CPU が AES ブロックにデータ、鍵、初期化ベクトルをメモリマップドレジスタに書き込んだ後に読出して結果を取得するか、2 本の DMA チャンネル(1 本は AES へのデータの書き込み、もう1 本は結果の読出し)によってデータの移動が保証されます。

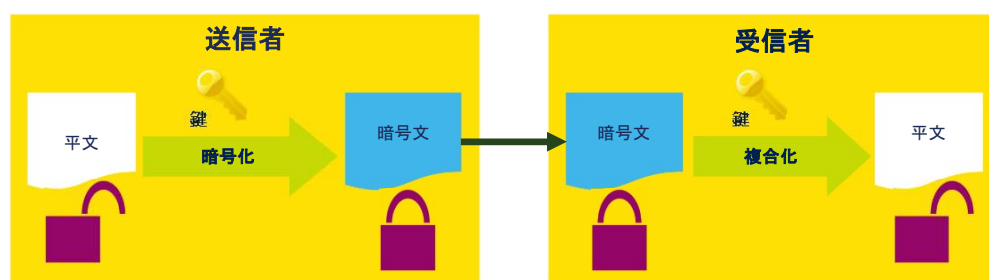
AES がより優先順位の高い別メッセージを処理する必要がある場合は、ソフトウェアで元のメッセージをサスペンドする事が可能で、その後レジュームする事が出来ます。

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、32bit データのスワッピングに対応しています。内部データパスは、データと初期値には 128bit 幅、鍵には 256bit 幅です。128bit 鍵にも対応しています。

# AESを用いた機密性保護

4

- 暗号化とは、平文と呼ばれる元データを、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の目的: データの機密性の保護

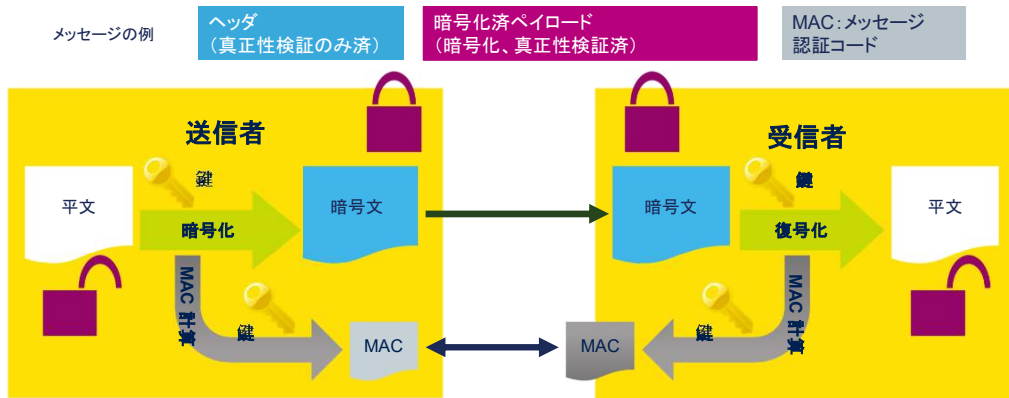


AES の暗号化と復号化のアルゴリズムは、セキュアネットワークルータ、ワイヤレス通信、ならびに、セキュアスマートカード、セキュアビデオ監視システム、セキュア電子会計トランザクションを含む暗号化データストレージなどのさまざまなアプリケーションに適しています。

送信者は、秘密鍵を用いて平文メッセージを暗号化します。受信者は、同じ秘密鍵を用いてその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おり、同じ鍵が暗号化と復号化の両方に使用されます。

# AESを用いた認証済み暗号化

- メッセージの機密性の保護に加えて、受信者は、メッセージが本物であり転送中に変更されていないかどうかについても知りたいケース
  - これは、メッセージ認証コード (MAC) 計算と呼ばれる追加処理で達成



暗号文にメッセージ認証コードを追加することにより、受信者は、そのメッセージが期待される送信者が元となっていることの確認が可能となります。  
AES ブロックは、データ暗号化の中で MAC の生成が可能です。

- NIST FIPS 197に準拠したAESアルゴリズムの実装
- NIST によって標準化された6種類のAES連鎖モード：
  - 128bit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128bitである必要は無い)
    - 3) カウンタ・モード(CTR)
  - MAC 計算を用いた特殊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)



米国標準技術研究所(NIST)は、暗号化規格を規定する連邦情報処理規格(FIPS)広報物を発行しています。

ブロック暗号モードは、暗号化するデータがバッファに格納されている場合に有益です。

ストリーム暗号モードは、(ブロックレベルでは無く)ビットレベルで効率的にデータの暗号化や復号化を行うために便利です。このモードには鍵のスケジューリングが不要です。

認証済みモードは、(有効化されている場合に)暗号化されたデータとともにメッセージ認証コード(MAC)を生成するために用いられます。

- 3種類のAES動作モード:
  - モード 1:暗号化
  - モード 2:暗号化のための鍵導出(ECBとCBCのみ)
  - モード 3:復号化



AES は 3 種類の動作モードを特徴としています。

- 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)の暗号化鍵連鎖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化する前に、AES キーレジスタに格納された値に基づいて、新しい鍵が鍵導出によって導出されます。
- モード 3:暗号文復号化

- 128、256bitキーと128bitデータ・ブロックの処理に対応
  - メッセージ・サイズがブロック・サイズの倍数ではない場合に、ECBモードとCBCモードでは ciphertext stealingテクニックをソフトウェアによって実装する必要あり
- 1、8、16、32bit 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チャンネル(1チャンネルは受信データ、1チャンネルは送信データ用)



AES キーの長さは 128bit か 256bit です。  
データスワッピングは、128bit データブロック内の 1、8、16、32bit 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(128bit)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 特別広報 800-38A の付録に記載されているものなどの ciphertext stealing テクニックを実装する必要があります。

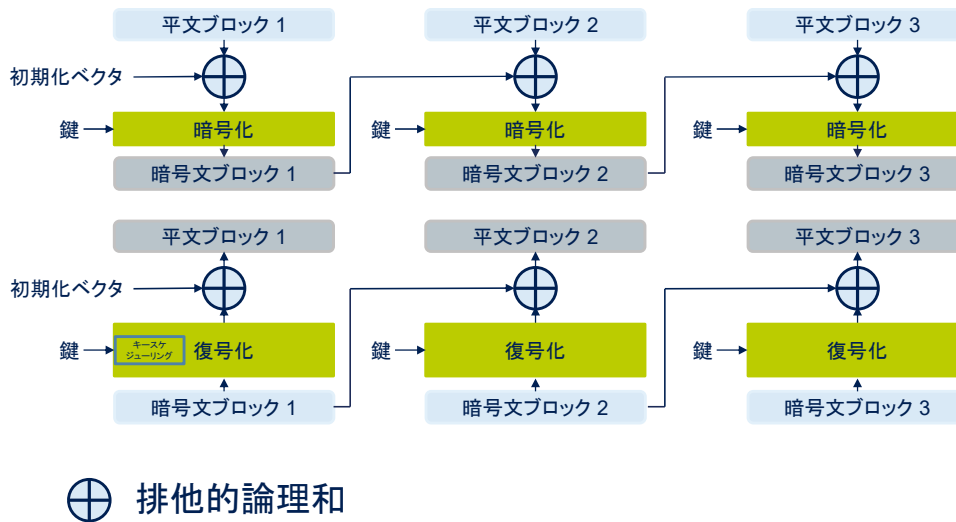


# ECB(電子コード・ブック)



ECB は最も単純な動作モードです。連鎖操作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カギを、暗号化の最終ラウンドの鍵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。

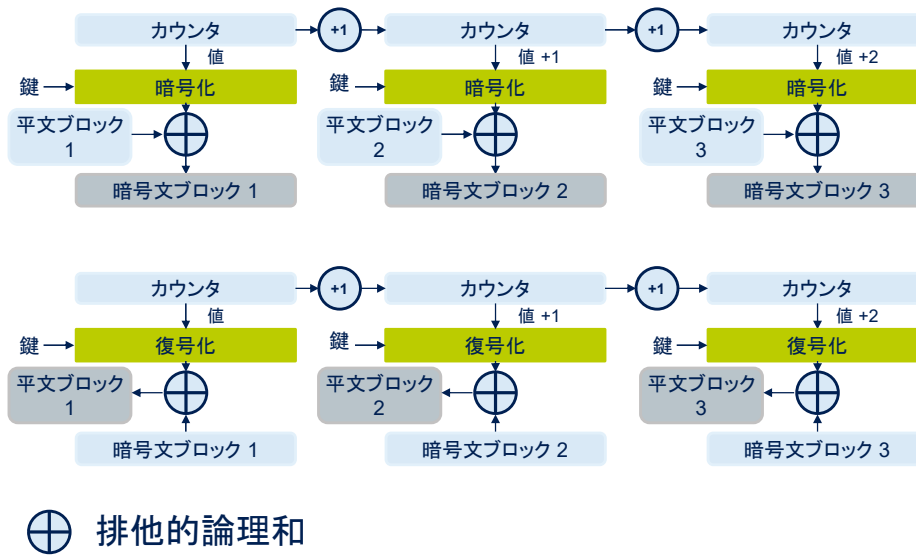
# 暗号ブロック連鎖 (CBC) モード



CBC モードでは、平文の各ブロックが前の暗号文ブロックと XOR され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鍵を、暗号化の最終ラウンドの鍵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

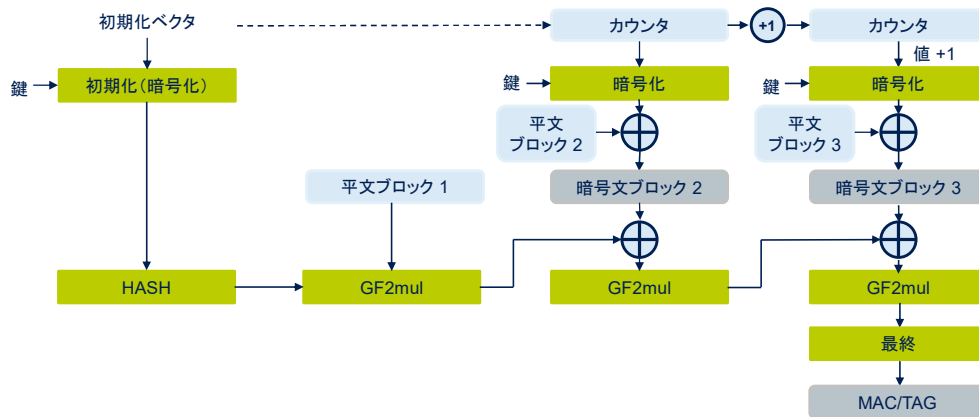


カウンタ(CTR)モードでは、AES コアを使用してキーストリームを生成します。鍵は、その後平文との排他的論理和をとって暗号文を得ます。

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 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)

12



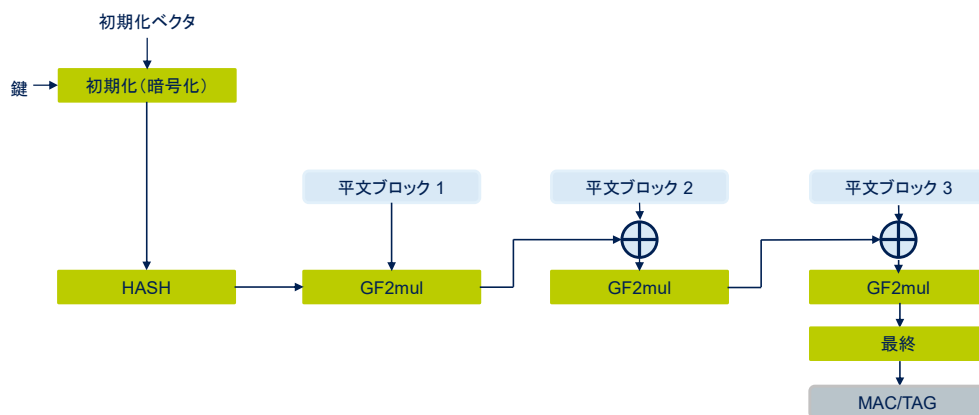
⊕ 排他的論理和



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 (認証タグともいいます) が生成されます。AES の機密性のあるカウンターモードをベースとして、加算と乗算を繰り返しタグを生成します。最初に初期化ベクトルが必要です。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

13



$\oplus$  排他的論理和



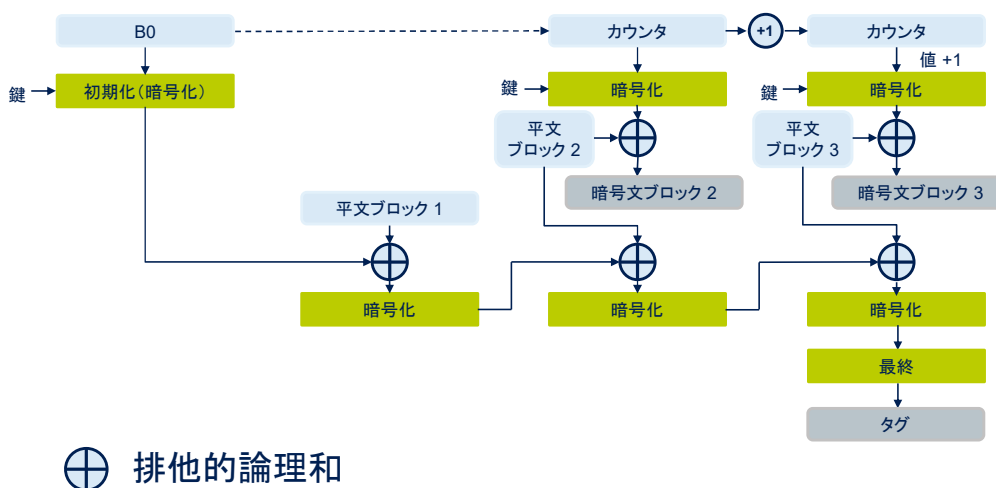
ガロアメッセージ認証コード (GMAC) を使用すると、メッセージの認証と、対応するメッセージ認証コード (MAC) の生成が可能となります。

平文の認証済みヘッダのみが含まれるメッセージ (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

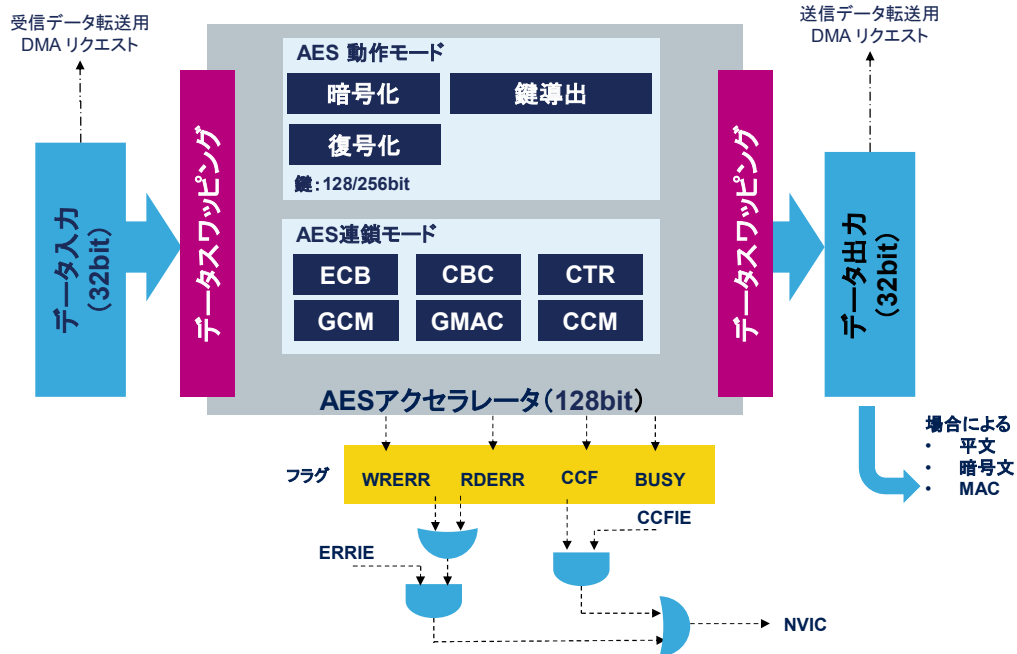
14



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、AESの機密性のあるカウンターモードをベースとして、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 規格では、最初の認証ブロック(規格では B0 と呼ぶ)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)に適用することもできますが、こうすることは NIST が推奨していません。CCM をこのように使用することは CMAC とは呼ばれない(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単純化されたブロック図には、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を使用して、または使用せずに、128bit または 256bit 長の暗号化キーを用いて 128bit 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 種類のフラグを介して AES アクセラレータの動作をチェックします。

計算フェーズまたは入力フェーズ中に予期しない読み出し操作が検出されたときに、AES ステータスレジスタに読み出しエラーフラグ (RDERR) がセットされます。

出力フェーズまたは計算フェーズ中に予期しない書き込み操作が検出されたときに、AES ステータスレジスタに書き込みエラーフラグ (WRERR) がセットされます。

AES 制御レジスタのエラー割込み有効 (ERRIE) ビットが事前にセットされていた場合、これら 2 種類のエラーフラグの 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) ビットは、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 割込みイネーブルビットが事前にセットされていた場合、割込みが生成されます。

BUSY フラグは GCM モードのみで使用され、暗号化モードの場合に、優先順位の高いメッセージが GCM ペイロードフェーズ中に現在のメッセージに割り込めることを示します。

# AES処理時間(1/2)

16

- 処理時間

(AHB クロック・サイクル・ユニットの128bit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
128bit	モード 1: 暗号化	ECB, CBC, CTR	9	38	4	51
	モード 2: 鍵導出	-	-	59	-	59
	モード 3: 復号化	ECB, CBC, CTR	9	38	4	51
256bit	モード 1: 暗号化	ECB, CBC, CTR	13	58	4	75
	モード 2: 鍵導出	-	-	82	-	82
	モード 3: 復号化	ECB, CBC, CTR	13	58	4	75



ここには、各種の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)

17

- 処理時間

(AHBクロック・サイクル・ユニットの128bitデータ・ブロック当たり)

- 注: ヘッダ内に1データ・ブロック、ペイロード内に1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
128bit	モード 1: 暗号化	GCM	64	35	51	59	209
	モード 3: 復号化	CCM	63	55	114	58	290
	-	GMAC	64	35	-	59	158
256bit	モード 1: 暗号化	GCM	88	35	75	75	273
	モード 3: 復号化	CCM	87	79	162	82	410
	-	GMAC	88	35	-	75	198



ここには、各種の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。

割り込みイベント	説明
AES 計算完了フラグ	計算が完了したときにセット
AES 読出しエラー・フラグ	(計算フェーズまたはデータ入力フェーズで)AES Data Outレジスタからの予期しない読出し操作が検出されたときにセット
AES 書込みエラー・フラグ	(計算フェーズまたはデータ出力フェーズで)AES Data Inレジスタへの予期しない書込み操作が検出されたときにセット

- DMA機能: 2チャンネル(1チャンネルは受信データ、1チャンネルは処理済みの送信データ用)
  - 入力用DMAリクエストチャンネル: INPUTフェーズ中、AES Data In (AES\_DINR)レジスタにワードを書き込む必要があるたびに、AESはDMAリクエスト(AES\_IN)を開始
  - 出力用DMAリクエスト・チャンネル: OUTPUTフェーズ中、AES Data Out (AES\_DOUTR)レジスタからワードを読み出す必要があるたびに、AESはDMAリクエスト(AES\_OUT)を開始



ここでは、ネスト化されたベクタ割り込みコントローラで割り込みをトリガ可能なイベントである、AES 計算完了、AES 読出しエラー、AES 書込みエラーの概要を示します。

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の両方に対して内部で生成されます。DMA チャンネルは、32bit データサイズで、メモリからペリフェラルモードまたはペリフェラルからメモリモードに設定する必要があります。

モード	説明
RUN	有効
SLEEP	RCC で無効
低電力 RUN	有効
低電力 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持
STANDBY	パワーダウン状態 ペリフェラルは、STANDBYモード終了後に再初期化する必要あり
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あり



ここでは、各低電力モードにおける 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 モードのときには、AES の動作はできません。

- このペリフェラルに関連した以下のペリフェラル・トレーニングを参照してください。
  - 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。

- 詳細と追加情報については、以下を参照してください。
  - 米国標準技術研究所(NIST)
    - SP800-38A: Ciphertext Stealing for CBC Mode
    - SP800-38A: Recommendation for Block Cipher Modes of Operation
    - SP800-38D: Galois/Counter Mode (GCM) and GMAC
    - SP800-38C: CCM Mode for Authentication and Confidentiality
    - AES Algorithm Validation Suite (AESAVS)
  - UM0586: STM32 暗号ライブラリ



詳細については、弊社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。