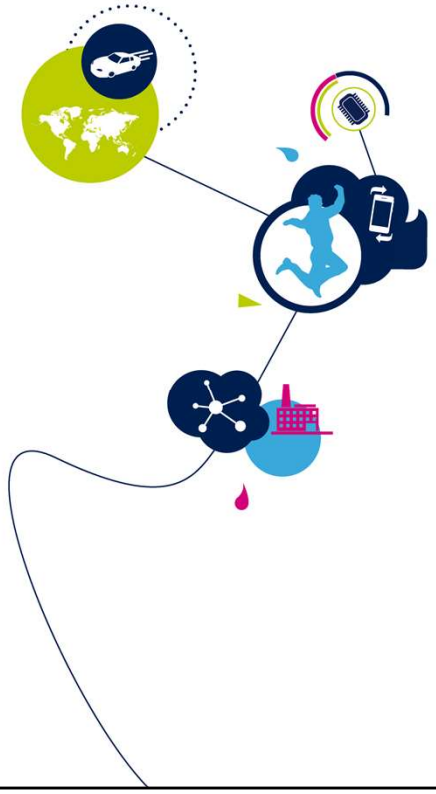
STM32MP1 - CRYP

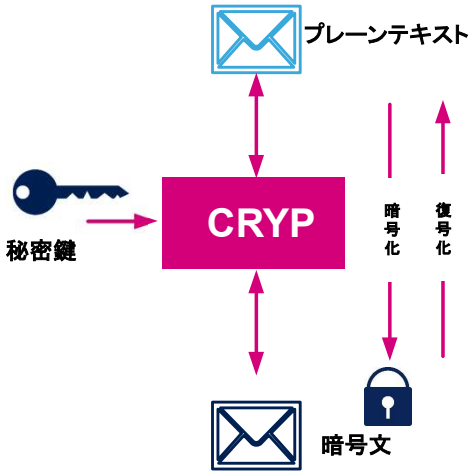
暗号プロセッサ：DES、トリプル DES、AES エンジン
1.0 版



life.augmented

STM32MP1 暗号プロセッサのプレゼンテーションにようこそ。このペリフェラルは、複数の動作モードでデータ暗号化標準（DES）、トリプル DES、高度暗号化標準（AES）をサポートしています。

概要



- 暗号プロセッサ
  - よく使われる DES および AES 標準のハードウェアアクセラレータ、対称暗号化用のブロックベースアルゴリズム
  - 複数の動作モードをサポート
- 2 つのインスタンス：CRYP1 および CRYP2

アプリケーション側の利点

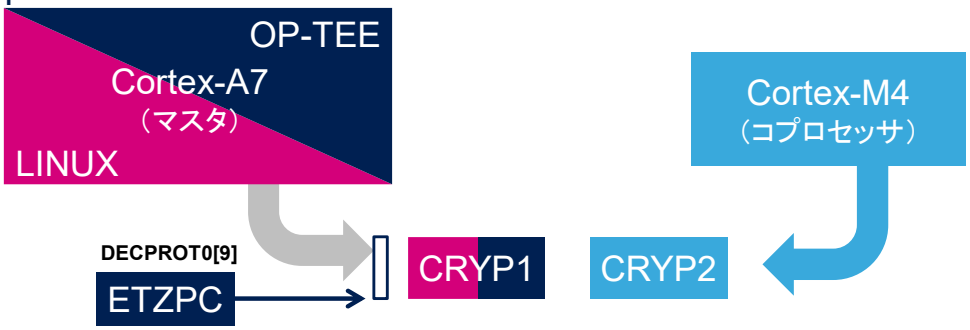
- データの機密性を保護
- CPUにおける大規模の計算処理タスクから解放

life.augmented

ほとんどの通信チャネルにおいて、認証と機密性は必須となります。そこで、暗号化は広く使われていますが、CPU の処理という点で非常に要件の厳しいものとなります。
STM32MP1 マイクロコントローラには、ブロックベースアルゴリズムの DES と AES を効率よく計算するためのハードウェアアクセラレータが組み込まれています。
よく知られているこれらの標準は、当事者間の共有鍵を含む対称暗号化に適しています。

CRYP の使用と関連するソフトウェア

- STM32MP1 デバイスには、Arm® コアや関連するセキュリティモードの違いに応じて複数のランタイムコンテキストが存在します。
  - Cortex®-A7 セキュア（Trustzone）は、セキュアモニタや OP-TEE のようなセキュア OS で動作します。
  - Cortex-A7 非セキュアは、Linux で動作します。
  - Cortex-M4（非セキュア）は、STM32Cube で動作します。
- サポートされる CRYP ペリフェラル割当て:



CRYP1 はセキュアペリフェラルです（ETZPC_DECPROT0 bit 9 で ETZPC 制御下）。
CRYP2 は非セキュアペリフェラルです。
CRYP1 インスタンスは、次に対して割り当てられます。

- CRYP OP-TEE ドライバによって OP-TEE で制御する Arm Cortex-A7 セキュアコア
- Linux 暗号化フレームワークを搭載した Linux® で使用するための Arm Cortex-A7 非セキュアコア

CRYP2 インスタンスは、STM32Cube CRYP ドライバによって STM32Cube MPU パッケージで制御する Arm Cortex-M4 コアに割り当てられます。

CRYP1 は、まず ROM コードによって初期化され、認証プロセスに使用されます。また、認証プロセス中にアプリケーションのセキュアブート（TF-A）によっても使用されます（ROM コードサービス使用時）。

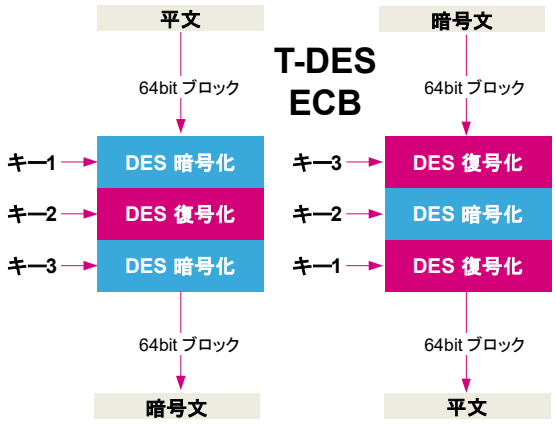
主な機能

- 暗号プロセッサは次のものをサポート
  - ECB および CBC 動作モードでデータを暗号化および復号化するための DES 標準およびトリプル DES 標準
  - AES 標準
    - ECB、CBC、CTR、GCM、CCM の動作モードでのデータの暗号化および復号化
    - GCM モードと CCM モードでのメッセージ認証コード（MAC）の生成
    - 128、192、256bit キーをサポート
  - 1、8、16 および 32bit ワードの自動スワッピング
  - ダイレクトメモリアクセス（DMA）をサポートする自動データフロー制御

暗号プロセッサは、以降のスライドで説明する複数の動作モードでデータ暗号化標準（DES）、トリプル DES、高度暗号化標準（AES）をサポートしています。
両標準は、ブロック暗号アルゴリズムファミリの一部です。
DES では 56bit キーを使用し、より堅牢である AES では 128bit、192bit、256bit のキーを使用できます。
ダイレクトメモリアクセスコントローラ（DMA）によって、データフロー全体を自動化できます。

DES およびトリプル DES

データ暗号化標準およびトリプル DES



- DES
  - 処理は 64bit データブロックに基づきます。元のメッセージは 64bit の連続したブロックに分けられます。
  - キー長は 56bit（+ 8 個のパリティビット）
- トリプル DES
  - トリプル DES は、キーのセットが異なる 3 つの連続した DES 処理ステップをつなげたもので構成されます。
- サポートされる動作モード：
  - 電子コードブック（Electronic Code Book(ECB)）：直接的で基本的な実装
  - 暗号ブロック連鎖（Cipher Block Chaining (CBC)）：ECB より堅牢で初期化ベクタ（IV）が必要

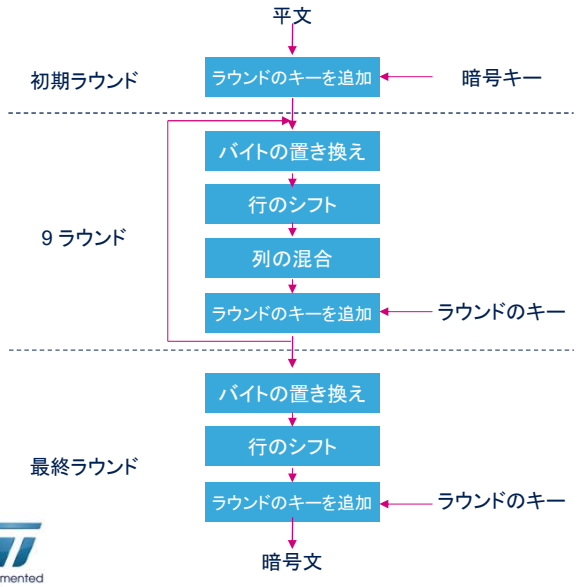
データ暗号化標準は、64bit のデータブロックで動作します。入力データは同じ 56bit キーで暗号化または復号化されます。

大きいメッセージは 64bit の複数のブロックに分けられ、次の 2 種類の動作モードのいずれかに従って連鎖します。 電子コードブック（ECB）または暗号ブロック連鎖（CBC）です。
ECB は、互いに依存関係のないブロックの後につながる直接実装ブロックです。小さいメッセージでは安全に使用できます。大きいメッセージの場合、暗号化出力を効率的にランダム化できるため、CBC が推奨されます。

図に示されているトリプル DES は、同じキーまたは 3 つの異なるキーを持つ 64bit の同じブロックに対して 3 つの連続した DES 操作を連鎖させて構成されています。DES のように、ブロックの連鎖は ECB または CBC に従います。

AES

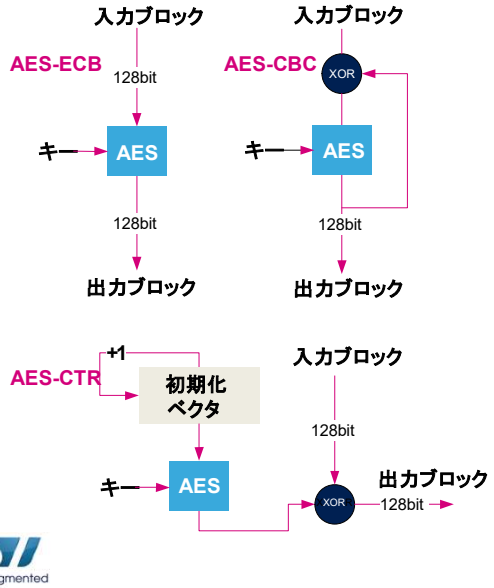
Advanced Encryption Standard



- AES 暗号ブロック
  - 128bit ブロックのサイズ処理
  - 128、192、または 256bit のキー長
  - 置き換え／並べ替えの複数のラウンドを構成する処理
- 動作モードで連続したデータのブロックの暗号化方法を定義
  - 電子コードブック（ECB）
  - 暗号ブロック連鎖（CBC）
  - カウンタモード（CTR）
  - ガロア／カウンタモード（GCM）
  - CBC-MAC付きカウンタ（CCM）

高度暗号化標準は、128bit のブロックで動作します。128、192、または 256bit のキーを使用して、暗号化や復号化を実行できます。
ブロック操作は、複数の置き換えと並べ替えで構成されています。この図では、128bit キーを使用した AES 暗号化の操作を示しています。
連続するブロックは、次のスライドで説明する複数の動作モードに従って連鎖できます。

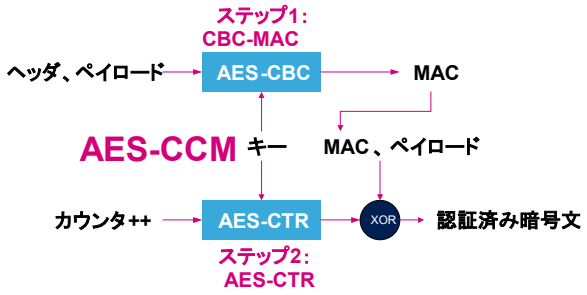
ECB、CBC、CTR の動作モード



- 電子コードブック（ECB）
  - 連続したブロック間に依存関係がない基本的な AES の実装です。
- 暗号ブロック連鎖（CBC）
  - 出力ブロックは、次の AES ステップにインジェクト（XOR）されます。
  - ECB と比較して全体的な堅牢性が高まります。
- カウンタモード（CTR）
  - AES ブロックが、各データブロックに 1 つずつ実装された初期化ベクタを暗号化します。疑似乱数出力は、入力データブロックに対してXORをとります。
  - このモードでは、AES がストリーム暗号エンジンとして使用されます。

DES の操作については、電子コードブック（ECB）および暗号ブロック連鎖（CBC）がサポートされます。
ECB は小さいメッセージ（数ブロック）にのみ安全に使用できます。
CBC モードでは、図に示すように最初の操作の出力が次のブロック操作の入力でインジェクトされます。最初のラウンドでは、初期化ベクタが必要です。
3 番目の動作モードは、カウンタモード（CTR）です。このモードでは、AES エンジンがストリーム暗号として使用され、限定の論理和操作で入力メッセージと混合された疑似乱数キーストリームを生成します。セキュリティ上の理由で、CTR では指定したキーを持つ各暗号化セッションで異なる初期化ベクタが必要になります。

CCM モードと GCM モード



- 認証済み暗号化
  - 次の 2 種類の動作モードは整合性、認証、機密性を提供
    - メッセージは 2 つの部分に分けられます。認証と暗号化を行うペイロードと、認証のみのヘッダです。
  - CBC-MAC 付きカウンタモード(CCM)
    - 暗号化の AES-CTR モードと、メッセージ認証コード(MAC)計算の AES-CBC モードを組み合わせます。
    - MAC がまず CBC モードで平文から計算されてから、CTR モードのペイロードで暗号化されます。
  - ガロア/カウンタモード(GCM)
    - 暗号化の AES-CTR モードと、メッセージ認証コード(MAC)計算の特定のハッシュ関数を組み合わせます。
    - GCM は CCM より高速です。

life.augmented

このスライドで説明する 2 種類の動作モードでは、機密性に認証と整合性が加わります。
認証メカニズムが、暗号化されるペイロードメッセージと、認証のみを必要とする追加データにも適用されます。この最後の部分はヘッダと呼ばれます。

1 つ目のモードは、「CBC メッセージ認証コード付きカウンタ」(CCM)です。このモードは、認証タグ計算(MAC)に AES-CBC モードの最初のパスを組み合わせます。そして、MAC がもう 1 つの AES-CTR パスのペイロードで暗号化されます。
同じキーが、CTR パスと CBC パスの両方に使用されます。

2 つ目の認証暗号化モードは、ガロアカウンタモード(GCM)です。
データの機密性が CTR モードで提供され、機密データの認証はバイナリガロアフィールドで定義される汎用ハッシュ関数で提供されます。
GCM は、認証計算にかかるサイクル数が少ないため、CCM より高速になります(汎用ハッシュ関数は 10サイクルですが、AES ラウンドは 14サイクルです)。

標準の準拠

- この暗号プロセッサは、次の標準に完全に準拠しています。
  - 連邦情報処理規格公報（FIPS：Federal Information Processing Standards Publication）（FIPS PUB 46-3, 1999 October 25）によって規定されているデータ暗号化標準（DES：Data EncryptionStandard）およびトリプル DES（TDES）。米国規格協会（ANSI：American National StandardsInstitute ）の X9.52 規格に準拠しています。
  - 連邦情報処理規格公報（FIPS PUB 197, 2001 November 26）によって規定されている高度暗号化標準（AES：Advanced Encryption Standard）、ならびに以下に準拠しています。
    - NIST 特別公報 800-38A『ブロック暗号の推奨動作モード』に定義された CTR 連鎖
    - NIST 特別公報 800-38D『ブロック暗号の推奨動作モード - ガロア／カウンタモード（GCM）および GMAC』に定義された GCM および GMAC 連鎖
    - NIST 特別公報 800-38C『ブロック暗号の推奨動作モード - 認証および機密性のための CCM モード』に規定された CCM 連鎖

life.augmented

暗号プロセッサは、データ暗号化標準と高度暗号化標準に準拠しています。これらの標準は、連邦情報処理規格公報の下で発行されています。

パフォーマンス

- DES
  - DES では 16サイクルで 1 つの 64bit ブロックを処理
  - TDES では 48サイクルで 1 つの 64bit ブロックを処理
- AES
  - この表で 1 つの 128bit ブロックの処理に必要なサイクル数を指定

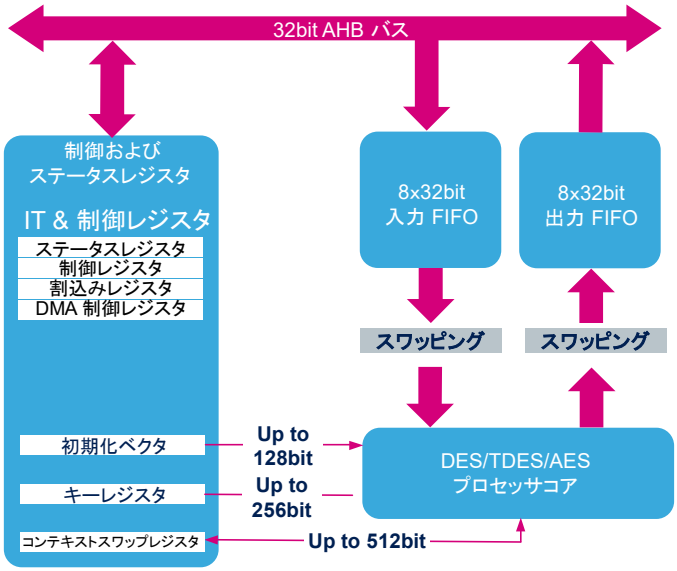
キー長	ECB、CBC、CTR	キー準備 (*)	GCM				CCM			
			初期化	ヘッダ	ペイロード	MAC	初期化	ヘッダ	ペイロード	MAC
128b	14	12	24	10	14	14	12	14	25	14
192b	16	13	28	10	16	16	14	16	29	16
256b	18	14	32	10	18	18	16	18	33	18

life.augmented

(*) AES ECB 復号化および CBC 復号化に必要

処理時間は、ブロック操作に対して指定されています。DES およびトリプル DES の操作は、64bit ブロックに基づいており、AES は 128bit ブロックに基づいています。
トリプル DES は、明らかに単純な DES の 3 倍の処理時間がかかります。
AES の時間は表に示されています。複数の 128bit ペイロードブロックの大きいメッセージでは、GCM が CCM より効率的であることがわかります。

ブロック図



暗号プロセッサのブロック図を、このスライドに示します。ペリフェラルは複数のハードウェアモジュールで構成されます。

- 1 つの AES または DES ブロック操作を担うプロセッサコア
- バスの相互接続に接続された入出力 FIFO
- 制御レジスタおよびステータスレジスタが組み込まれたモジュール

割込みおよび DMA

割込みイベント	説明
入力 FIFO サービス割込み	この FIFO に 4 ワード(4x32bit)未満ある場合にセットされます。
出力 FIFO サービス割込み	出力 FIFO に最低 1 つのデータがあり、読み出す準備ができている場合にセットされます。

- DMA 機能:2 個のリクエストチャネル(データ入力用と送信データ処理用)
  - シングルリクエストと最大 4 ワードのバーストリクエスト転送をサポートしています。
  - 入力(CRYP_IN)と出力(CRYP_OUT)のストリームが、同じ DMA ストリームリクエスト番号を共有します。入力 FIFO が一杯になる前に、DMA コントローラが出力 FIFO を空にできるように、CRYP_OUT に高い優先度を付与する必要があります。

life.augmented

2 つの機能割込みがペリフェラルに対して定義されます。1 つは入力 FIFO がデータを受け取る準備ができたときにセットされ、もう 1 つは出力データが CPU または DMA で一掃する準備ができたときにセットされます。
DMA には、暗号プロセッサに接続された 2 つのストリームがあります。これらの 2 つのストリームは同じチャネル(#2)を共有します。出力ストリームの優先度は入力ストリームより高くなります。

低電力モード

モード	説明
RUN	アクティブ
SLEEP	オプションで RCC では無効です。
STOP	停止。ペリフェラルレジスタの内容は保たれます。
LP-Stop	
LPLV-Stop	
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。

life.augmented

ここでは、各低電力モードでの暗号プロセッサのステータス概要を示します。
デバイスが STOP モードおよび STANDBY モードの場合、暗号操作は実行できません。

関連するペリフェラル

- 次のペリフェラルに関するトレーニングを参照してください。
  - CRYP1 用のマスタダイレクトメモリアクセスコントローラ（MDMA）
  - CRYP2 用のダイレクトメモリアクセスコントローラ（DMA）
  - ハッシュプロセッサ（HASH）

life.augmented

これは、暗号プロセッサに関連するペリフェラルの一覧です。
暗号チャネル設定に関する詳細については、DMA トレーニングを参照してください。
また、暗号エンジンについて知りたい場合は、ハッシュ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、次の文書を参照してください。
  - ユーザマニュアル UM0586：STM32 暗号ライブラリ

life.augmented

詳細については、弊社ウェブサイトで利用できるこれらの関連資料を参照してください。