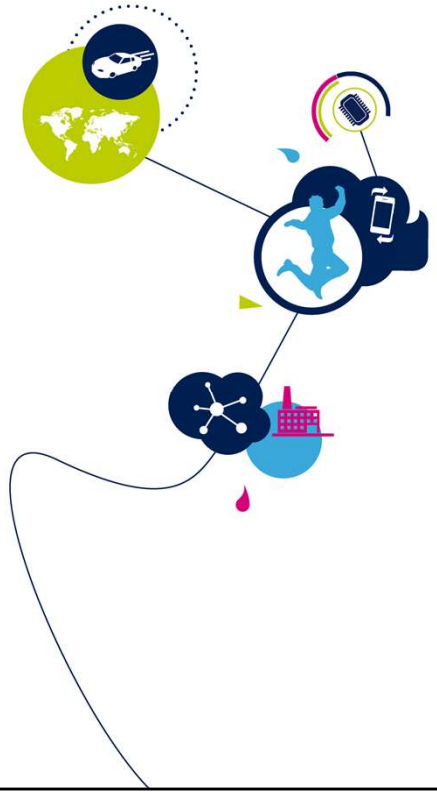
STM32H7 - CRYP

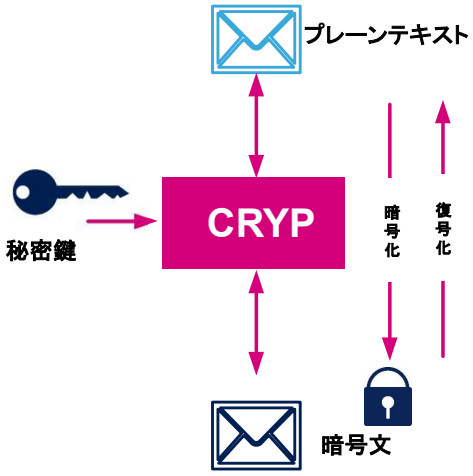
暗号プロセッサ：DES、トリプルDES、AESエンジン
1.0版



life.augmented

STM32H7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

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

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。
STM32H7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機能は、当事者間の共有鍵を含む対称暗号化に適しています。

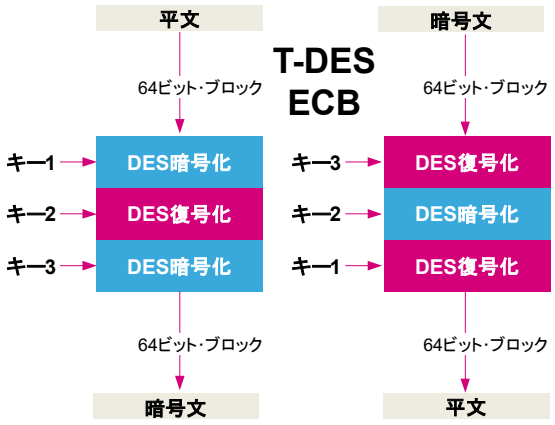
主な機能

- 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、256ビットキーをサポート
  - 1、8、16および32ビット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56ビットキーを使用し、より堅牢であるAESでは128ビット、192ビット、256ビット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64ビット・データ・ブロックに基づく
    元のメッセージは64ビットの連続したブロックに分けられる
  - キー長は56ビット（+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る
- 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

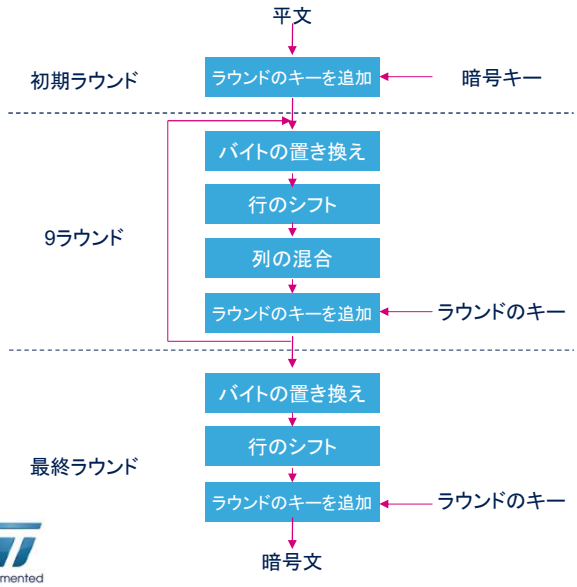
life.augmented

データ暗号化標準は、64ビットのデータブロックで動作します。入力データは同じ56ビット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64ビット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64ビット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。

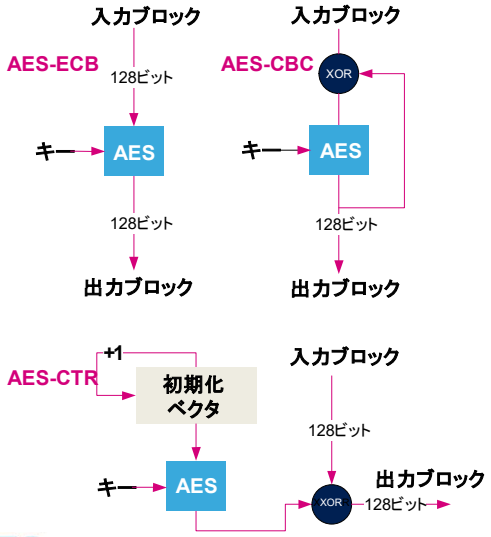
高度な暗号化標準



- AES暗号ブロック
  - 128ビット･ブロックのサイズ処理
  - 128、192、または256ビットのキー長
  - 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、128ビットのブロックで動作します。128、192、または256ビットのキーを使用して、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、128ビットキーを使用した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。

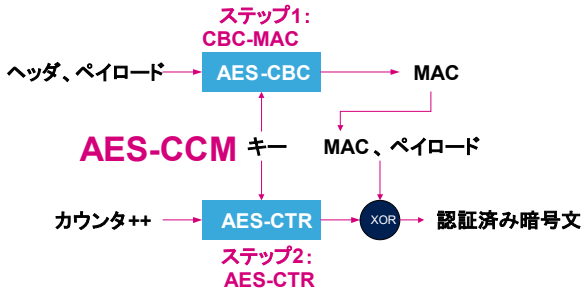
ECB、CBC、CTRの動作モード



- 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
- 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）される
  - ECBと比較して全体的な堅牢性が高まる
- カウンタモード（CTR）
  - AESブロックは、入力ブロックに注入される連続したランダムベクトルを生成(XOR-ed)
  - このモードはストリーム暗号エンジン(乱数注入)と同等

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エンジンがランダムストリームジェネレータとして使用されます。結果のランダム・ストリームは、入力メッセージと排他的OR操作と混合されます。CBCに関しては、CTRは暗号化セッションごとに異なる初期化ベクトルを必要とします。

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る
      認証と暗号化を行うペイロードと、認証のみのヘッダ
  - 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る
    - 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る
  - ガロア／カウンタモード（GCM）
    - 機密性はCTRモードのバリエーションによって与えられ、認証メカニズムはバイナリ·ガロア·フィールド内の乗算を特徴とする特定のハッシュ関数に依存
    - GCMはCCMより高速で、オンザフライで処理可能

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、各ペイロードブロックにAESエンジンのパスを1つだけ必要とするため、CCMよりも高速です。さらに、ペイロードメッセージは、マルチパス処理のために保存することなく、その場で処理することができます。

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
  - 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
  - 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）に準拠

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

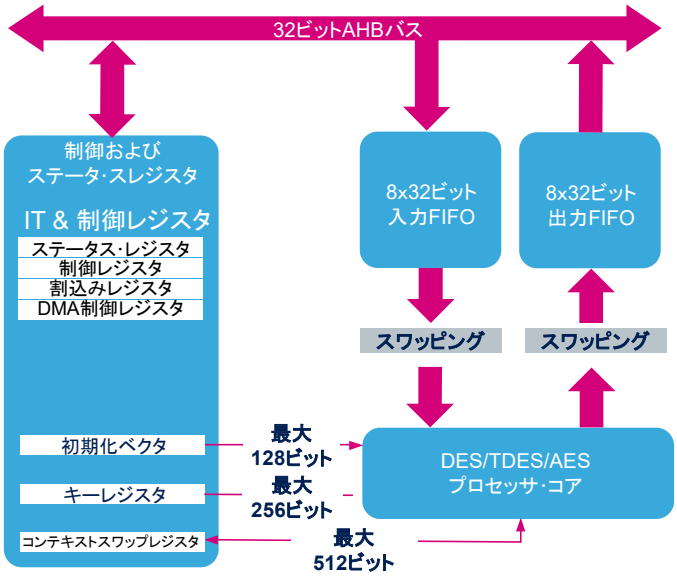
キー長	ECB、CBC、CTR	キー準備(*)	GCM				CCM			
			初期化	ヘッダ	ペイロード	MAC	初期化	ヘッダ	ペイロード	MAC
128b	14	12	24	10	14	14	12	14	25	14
192b	16	13	28	10	16	16	14	16	29	16
256b	18	14	32	10	18	18	16	18	33	18

life.augmented

(*)AESECB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、64ビットブロックに基づいており、AESは128ビット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128ビット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(4x32ビット)未満ある場合にセット
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

- 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
  - 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
    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る

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	アクティブ ペリフェラルの割込みにより、デバイスはSLEEPモードを終了
STOP	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 ペリフェラルは、STANDBY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ご参照ください。
  - 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）

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トレーニングをご参照ください。
さらに暗号化エンジンを使いたい場合は、ハッシュトレーニングをご参照ください。

参照

- 詳細および追加情報については、次の文書をご参照ください。
  - アプリケーションノートAN4230:STM32F2xx, STM32F4xx NIST Statistical Test Suiteを用いた乱数生成の検証
  - 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ご参照ください。