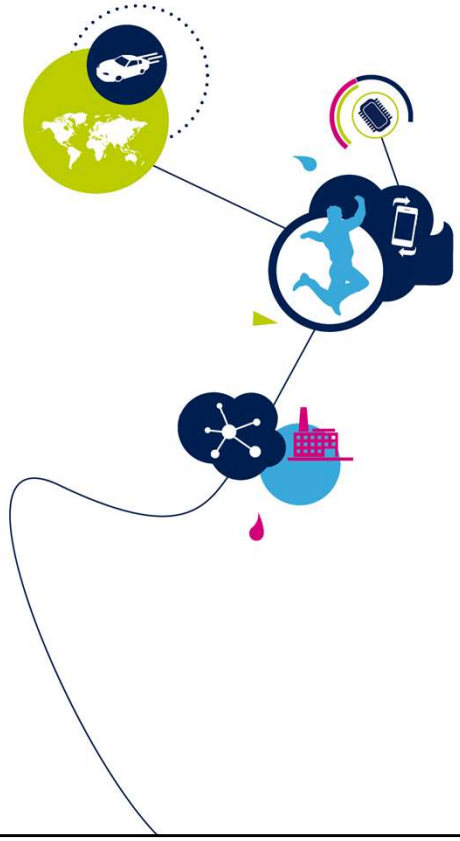
STM32H7 - HASH

ハッシュ・プロセッサ：SHA-1、SHA-2、MD5エンジン
1.0版

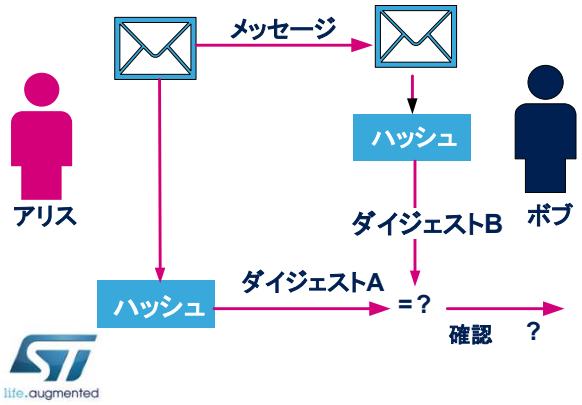


life.augmented

STM32H7ハッシュプロセッサのプレゼンテーションにようこそ。

概要

- ハッシュ処理
  - メッセージから固定長のダイジェストを計算
  - メッセージはダイジェストから取得できない
  - 同じダイジェストで2つのメッセージを発見することは実質不可能（衝突）



アプリケーション側の利点

- 次を保証してトランザクションを保護するために使用される
  - メッセージ整合性（HASH）
  - メッセージ認証（HMAC）
- CPU の処理時間が低減

ハッシュペリフェラルは、メッセージダイジェストの効率的な計算を実行します。
ダイジェストとは、入力メッセージから計算される固定長の値です。ダイジェストは一意で、同じダイジェストで2つのメッセージを発見することは実質不可能です。元のメッセージはダイジェストから取得できません。
ハッシュダイジェストとハッシュベースメッセージ認証コード（HMAC）は、転送の整合性と認証を保証するために使用されるため、通信で広く使用されています。

主な機能

- ハッシュプロセッサは次のものをサポート
  - 次のハッシュ関数の高速計算
    - MD5
    - SHA-1
    - SHA-224およびSHA-256
  - シンプルなハッシュ・ダイジェストやハッシュ・ベースのメッセージ認証コード（HMAC）の計算
  - ビッグエンディアンおよびリトルエンディアンに準拠する自動バイト・スワッピング
  - 入力されたビット列をモジュロ512（16×32ビット）のメッセージ・ダイジェスト演算に合わせて自動でパディングする機能
  - 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

life.augmented

ハッシュプロセッサは、メッセージダイジェスト5（MD5）、セキュアハッシュアルゴリズムSHA-1、224ビットと256ビットのダイジェスト長バージョンを持つさらに新しいSHA-2を含め、広く使用されるハッシュ関数をサポートしています。
ハッシュを秘密鍵で生成して、メッセージ認証コード（MAC）を生成することもできます。
このプロセッサは、ビット、バイト、およびハーフワードスワッピングをサポートしています。また、ブロック配置での入力データの自動パディングもサポートしています。
このプロセッサは、自動プロセッサ供給を実現するためにDMAと組み合わせて使用できます。

ハッシュ関数

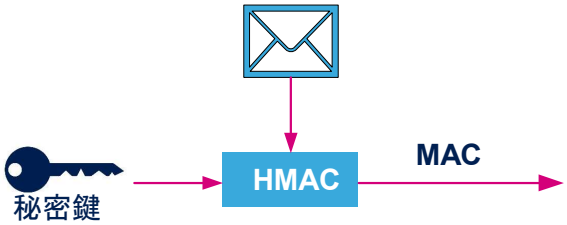
- ブロック･ベース･アルゴリズム
  - サポートされるハッシュ関数は、512ビットのデータ･ブロックで動作
    元のメッセージは、必要に応じてパディングされた後、512ビットの連続したブロックに分けられる
  - 内部演算は32ビット･ワードで行われる
  - 攻撃に対する堅牢性は、ダイジェスト長で上がる

ハッシュ関数		ダイジェスト（ビット）	強度（衝突）
MD5		128	2^64
SHA-1		160	2^80
SHA-2	SHA-224	224	2^112
	SHA-256	256	2^128

すべてのサポートされるハッシュ関数は、512ビットのデータブロックで動作します。入力メッセージは、ハッシュプロセッサに供給するために必要な数に分けられます。連続したブロックが順番に計算されます。
MD5は、わずか128ビットダイジェストの堅牢性の低い関数です。
SHA標準には、SHA-1と、224ビットと256ビットのダイジェスト長バージョンを持つさらに新しいSHA-2の2バージョンがあります。

メッセージ認証コードのためのHMAC鍵付きハッシング

- H-MAC
  - 整合性に加えて、メッセージの認証も保証
  - 送信側と受信側の両方で共有される秘密鍵が含まれる
- このアルゴリズムは2つのネストされたハッシュ操作で構成
  - HMAC(message) = Hash[((key | pad) ⊕ 0x5C) | Hash(((key | pad) ⊕ 0x36) | message)]
  - ハッシュ関数は、ペリフェラルによってサポートされるうちのいずれかになる



life.augmented

ハッシュベースのメッセージ認証コード（HMAC）は、メッセージの認証と整合性の確認に使用されます。HMAC関数は、送信側と受信側の両方で共有される秘密鍵がある2つのネストされたハッシュ関数で構成されます。
HMAC計算に含まれるハッシュ関数は、ペリフェラルによってサポートされるものに設定できます。MD5、SHA-1、SHA-2のいずれかです。

標準

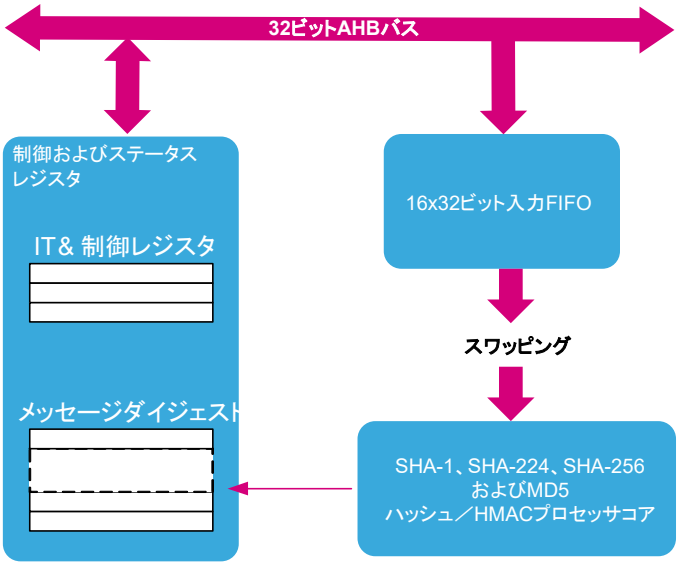
標準の準拠

- このハッシュプロセッサはデータ認証アプリケーションに適しており、次の標準に準拠
  - セキュアハッシュ標準スペック（SHA-1、SHA-224およびSHA-256）ではFIPS PUB 180-2（連邦情報処理規格公報180-2）
  - IETF RFC 1321（インターネット技術タスクフォースRFC1321）メッセージ･ダイジェスト･アルゴリズム（MD5）の仕様について
  - 鍵付きハッシュ･メッセージ認証コード（HMAC）に関するFIPS PUB 198-1

life.augmented

ハッシュプロセッサは、セキュアハッシュアルゴリズム（SHA）、メッセージダイジェストアルゴリズム（MD5）、ハッシュメッセージ認証コード（MAC）の国際標準に準拠しています。

ブロック図



life.augmented

こちらのハッシュプロセッサの簡略化されたブロック図には、基本的なデータフローと制御モジュールを示しています。
ハッシュプロセッサは、512ビットデータブロックを処理して、アルゴリズムに応じて最大256ビットのダイジェストを生成します。
入力データは、コアユニットに移行し、そこで処理されてシンプルなハッシュやメッセージ認証コード（MAC）を生成する前にスワッピングできます。

割込みおよびDMA

割込みイベント	説明
ハッシュダイジェスト計算完了	ダイジェストがレディになったとき（メッセージ全体が処理済）にセット
ハッシュデータ入力レディ	入力バッファが512ビットの新しいブロックを取得する準備ができたときにセット（空き領域が16か所）

- DMA機能：メモリからの入力データ用のチャネル1個のみ
  - ハッシュプロセッサが、512ビットのデータ･ブロック1個をすべてロードするためにDMAリクエスト（HASH_IN）を発生
  - DMAの転送完了割込みをデータ･フロー制御に使用可能

life.augmented

ネスト化されたベクタ割込みコントローラ（NVIC）での割込みは、ハッシュダイジェストの計算が完了したとき、またはハッシュプロセッサが新しいデータブロックを受け入れる準備ができたときにトリガされます。

ダイレクトメモリアクセス（DMA）モードでは、入力データに対するリクエストが内部で生成されます。DMAチャネルは、512ビットのデータサイズでメモリからペリフェラルモードに設定する必要があります。

パフォーマンス

- ハッシュのパフォーマンス
  - メッセージの中間ブロック(512ビット)の計算については
    - SHA-1では66HCLKクロック・サイクル
    - SHA-224では50HCLKクロック・サイクル
    - SHA-256では50HCLKクロック・サイクル
    - MD5では50HCLKクロック・サイクル
    - ブロックの16ワードをプロセッサにロードするのに必要な時間も考慮されている
      (512ビットのブロックでは少なくとも16クロック・サイクル)
  - このペリフェラルによって、速度が上がり、アルゴリズムのソフトウェア・バージョンと比較して電力が削減される

life.augmented

これらは、選択したアルゴリズムに応じて1つのデータブロックの処理にかかる時間です。
HCLKはCPUクロックで、216MHzハイにできます。
ハードウェアアクセラレータの主なメリットは、速度が上がり、ハッシュ関数の完全ソフトウェア実装と比較して電力が削減されるということに注意してください。

低電力モード

モード	説明
RUN	アクティブ
SLEEP	アクティブ ペリフェラル割り込みにより、デバイスがスリープ·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、STANBY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ハッシュプロセッサのステータス概要を示します。
デバイスがSTOPモードの場合、ハッシュ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ペリフェラルのトレーニングをご参照ください
  - CRYP
  - DMA

これは、ハッシュプロセッサに関連するペリフェラルの一覧です。暗号エンジンについて詳しく知りたい方は、CRYPペリフェラルのトレーニングを参照してください。ハッシュチャンネルの設定方法については、DMAペリフェラルの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
  - UM0586：STM32暗号ライブラリ

詳細については、弊社ウェブサイトで利用できるユーザマニュアルをご参照ください。