STM32U5 のハッシュプロセッサのプレゼンテーションへようこそ。

ハッシュキーの機能

- ハッシュプロセッサは、以下に対応します
  - 次のハッシュ関数の高速計算
  - 単純ハッシュダイジェストまたは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と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
  - 最小ダイジェストブロックサイズ（512 ビット）に合わせて入力ビット列を補完する自動パディング
  - 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
- ハッシュ性能
  - 右の表を参照してください

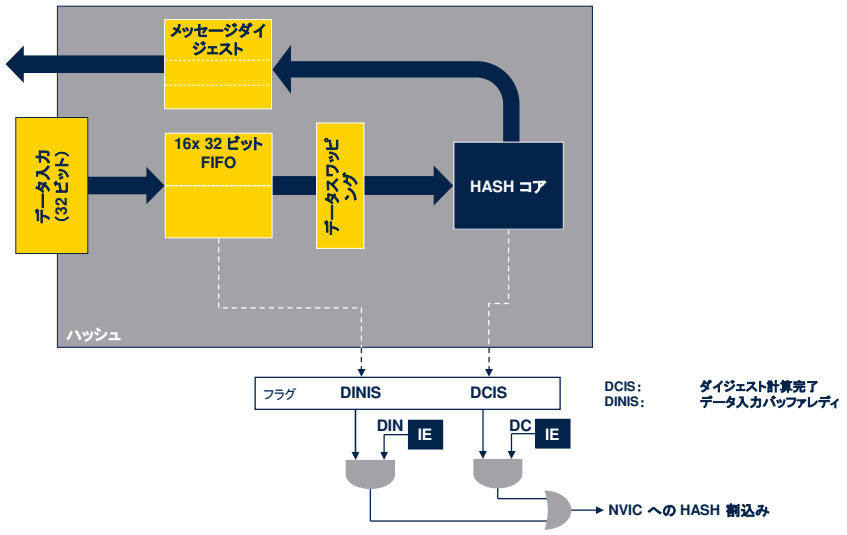
ハッシュ関数：		ダイジェストサイズ（ビット）
MD5		128
SHA-1		160
SHA-2	SHA-224	224
	SHA-256	256

512 ビットブロックの処理に必要なサイクル数				
モード	MD5	SHA-1	SHA-224	SHA-256
ノーマル	66	82	66	
HMAC	時間を以下まで増加させます ➢ x2.5（ショートキー） ➢ x5（ロングキー）			

life.augmented

ハッシュプロセッサは、広く使用されているハッシュ関数に対応しています。例えば、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 のほか、ダイジェスト長が 224 ビットおよび 256 ビットである最近の SHA-2 などがあります。
任意の長さのメッセージが入力として与えられた場合、ハッシュ処理コアでは、アルゴリズムに応じて、メッセージダイジェストと呼ばれる固定長の出力文字列が生成されます。上の表に、メッセージダイジェストのサイズを示します。
ハッシュは、メッセージ認証コード（MAC）を生成するための秘密鍵を使用して生成することもできます。
プロセッサは、ビット、バイト、ハーフワードのスワッピングに対応しています。ブロックアラインメントのために、入力データの自動パディングにも対応しています。
ハッシュプロセッサを DMA と組み合わせて使用することで、データの自動供給が可能になります。
1 つのデータブロックを処理するのにかかる時間は、選択したアルゴリズムによって異なります。
下の表には、各動作モードで中間ブロックの処理に必要な時間を示しています。
HMAC も生成される場合、これは 2.5 または 5 の係数で増加します。

HASH ブロック図

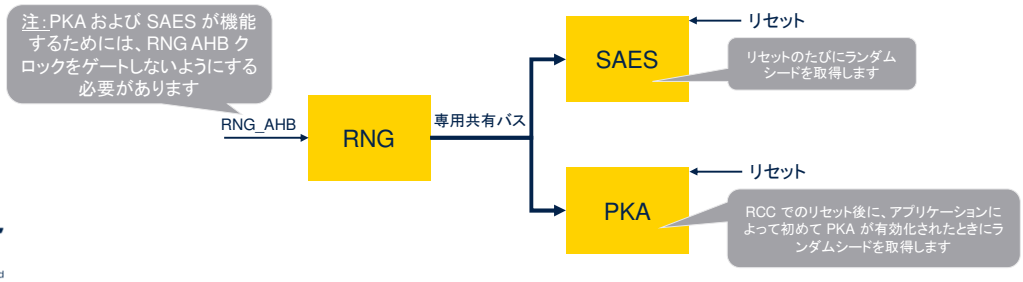


この簡略化されたブロック図は、メッセージが完全にロードされると、FIFO を介してハッシュプロセッサによってデータブロックが処理され、ダイジェストが生成されることを示しています。
入力データは、コアユニットに入る前にスワッピングできます。
ハッシュプロセッサでは、ダイジェスト計算完了（DCIS）またはデータ入力バッファレディ（DINIS）のイベントの際に、個別にマスク可能な 2 つの割込みソースが管理されます。

新バージョンと STM32L5

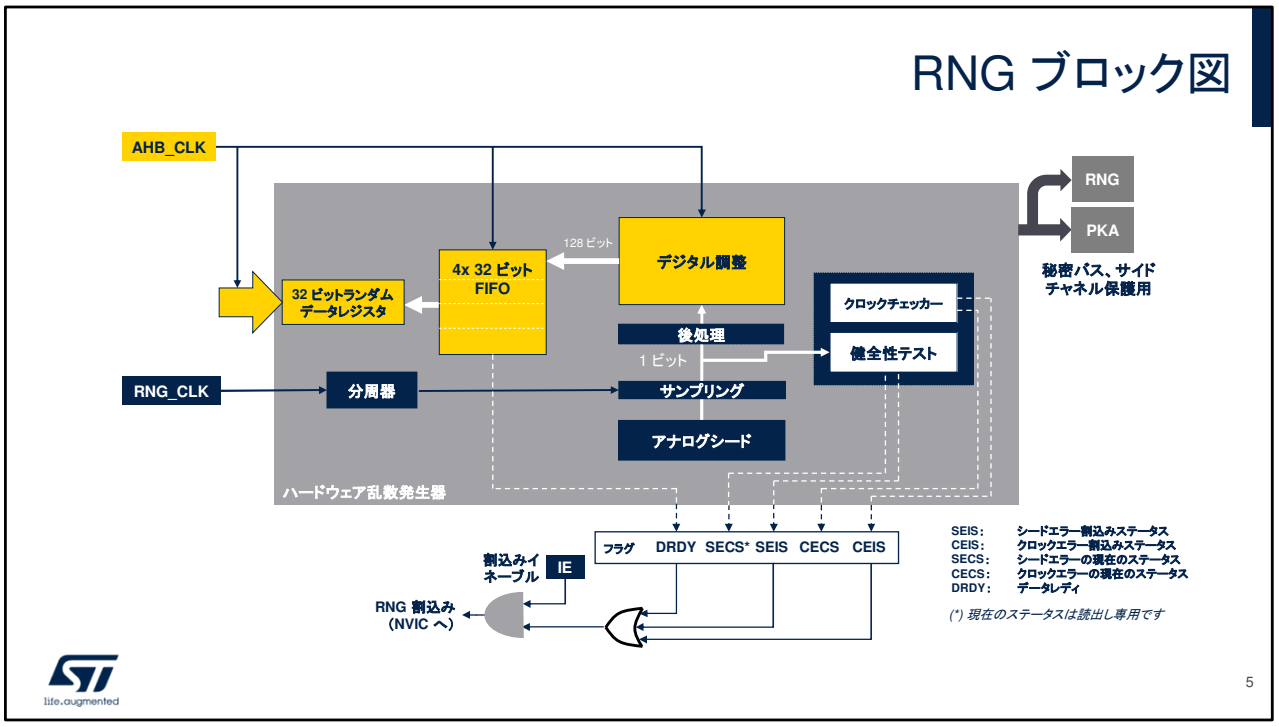
RNG キーの機能

- 32 ビット真の乱数発生器、NIST SP800-90B 認定
- NIST 設定では、RNG_AHB クロックが 1.2 MHz3 以上の場合、RNG により 341µs ごとに 16 バイトの真のランダムビットが供給されます。
- 本機能を無効にして消費電力を低減することができます（RNG_CR で RNGEN=0）
- PKA および SAES 耐サイドチャネルペリフェラルにランダムシードを供給するために使用されます



life.augmented

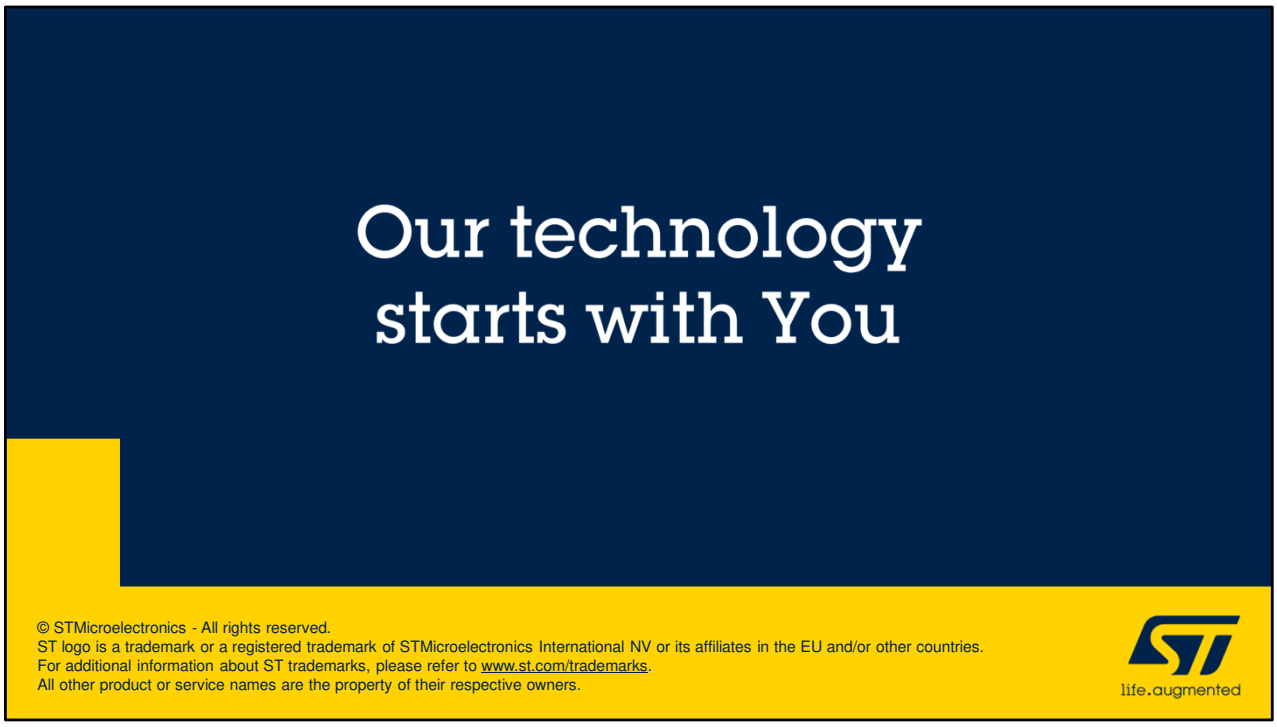
RNG ペリフェラルは、ランダム 32 ビット値を供給する連続アナログノイズに基づいています。これは NIST SP800-90B 認証可能であり、128 ビットのエントロピーが保証されています。この設定では、示されているように、RNG から 16 バイトの真のランダムビットが供給されます。
新しいランダムデータのセットがレディ状態で有効になると、ステータスレジスタのデータレディフラグがセットされます。これは常に使用する必要があります。
RNG では、ノイズソースに対する NIST SP800-90B 準拠の健全性テスト（エラーの場合、シードエラーの現在のステータスフラグがセットされます）が自動的に実行されます。
RNG クロックが HCLK クロックの 32 分周未満の場合、クロックエラーの現在のステータスフラグがセットされます。特にエントロピーを最大にするために RNG クロックがローに初期化される場合、このチェックは無効にできます。
割込みソースを有効にして、異常なシードシーケンスまたは周波数エラーを示すこともできます。
RNG を使用して、PKA と SAES がリセットから開放されるたびに、ランダムシードを PKA および SAES の耐サイドチャネルペリフェラルに供給します。



この RNG ブロック図は、NIST SP800-90B 仕様に従って、ペリフェラルで乱数が生成される方法を示しています。
RNG には 2 つのクロックドメインがあります。1 つはエントロピーのアナログソースのサンプリング用で、もう 1 つはこれらの元サンプルの調整および AHB バスを介した検索用です。
RNG および PKA ペリフェラルのサイドチャネル保護を初期化するために、秘密バスが追加されています。RNG カーネルクロックには、モジュール内に専用の分周回路があります。
データレディ(DRDY)フラグは、データ FIFO がフルになると直ちにトリガされ、RNG から読み出せるデータがなくなると自動的にリセットされます。
クロックチェッカーと NIST 準拠の健全性テストロジックは並行して実行され、シードで異常なシーケンスが検出された場合、または RNG 周波数が低すぎる場合には、専用のエラー信号がトリガされます。
TRNG ブロックは、次のシーケンスで正しく初期化する必要があります。

1) 条件付きソフトリセットビット CONDRST、および RNG_CR レジスタの正しい RNG の設定をセットします。
2) CONDRST ビットに 0 をセットし、割込みイネーブル(IE)ビットに 1 をセットし、RNG イネーブル(RNGEN)ビットに 1 をセットして、RNG_CR レジスタに 2 回目の書込みをします。

乱数の準備ができたとき、またはエラーが発生したとき、割込みが生成されるようになります。



このプレゼンテーションにご参加いただき、ありがとうございました。詳細と追加情報については、「ユーザマニュアル STM32 暗号ライブラリ」を参照してください。