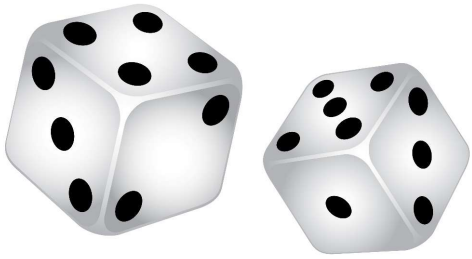
STM32乱数生成器のプレゼンテーションにようこそ。乱数の提供に広く使用されているこのペリフェラルについて、このプレゼンテーションで説明します。

概要



- 乱数の提供
  - 予測不可能な結果を生み出すことが望まれる場合に使用

アプリケーション側の利点

- 数のランダム性の向上
- 値の推測可能性を著しく減らす

life.augmented

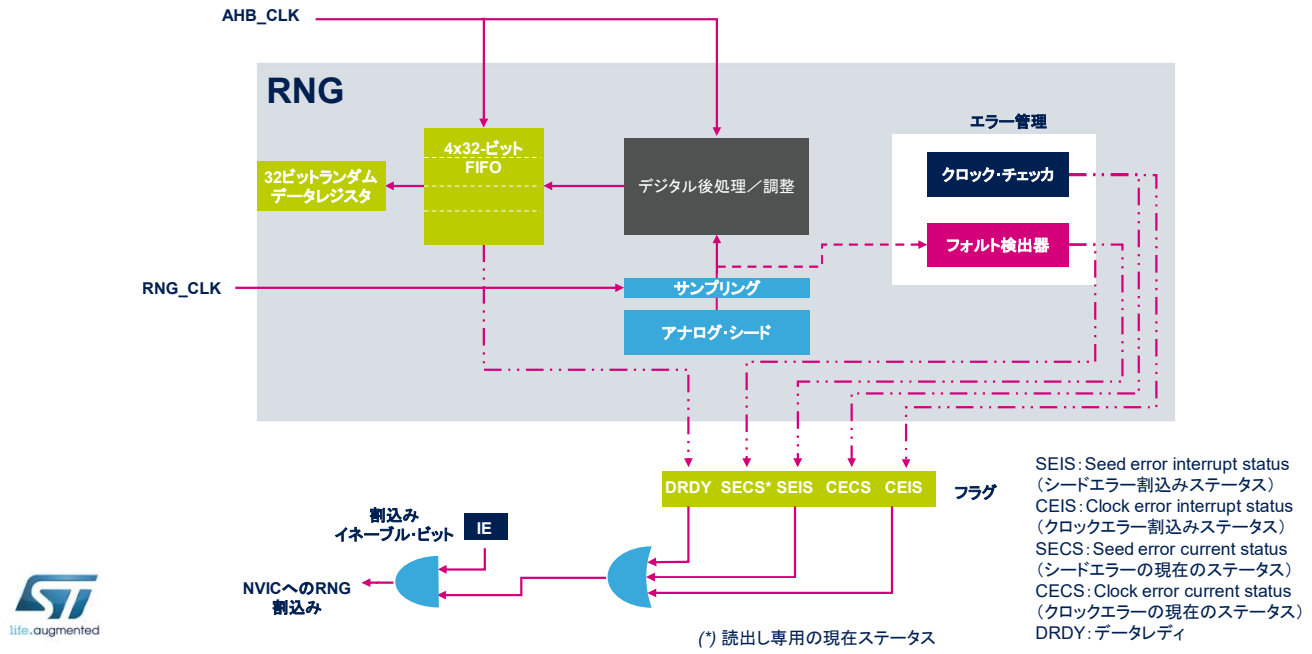
STM32製品の中に組み込まれている乱数生成器（RNG）は、予測不可能な結果を生み出すことが望まれる場合に使用される乱数を提供します。アプリケーションがRNGから得られる利点は、数のランダム性を上げたり、特定の値の推測可能性を下げたりすることです。

主な機能

- ノイズ･ソースに基づく32ビット乱数生成器
  - 213クロック･サイクルの最小周波数で、4個の32ビット乱数を生成可能
    - 実際の値（213よりも大きい場合）は、システムクロックとRNGサンプルクロックの比による*16 x f_{AHB} / f_{RNG}となる f_{AHB}=64MHzかつf_{RNG}=48MHzである場合、サンプルは57AHBサイクル毎に提供される*
  - 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のRNGEN=0）
- 以下の3種類のフラグがトリガ可能
  - DRDY:有効な乱数が準備済み
  - SECS:シードで異常なシーケンスが発生（64ビットを超える連続したビットが“0”あるいは“1”の同一値、または“01”あるいは“10”のビット･パターンが32回を超えて連続）
  - CECS:f_{RNG}周波数がf_{AHB}/32よりも低い（このチェックは無効化可能）
- 3種類の割込み
  - CEIS:クロック･エラーを示す
  - SEIS:シード･エラーを示す
  - DRDY:有効な乱数が準備済みであることを示す

RNGペリフェラルは、連続アナログノイズに基づいており、32ビットの乱数値を返します。RNGは、213システムクロックサイクルの最小周波数で、4個の32ビット乱数を生成できます。目安としては、RNGクロックが低いほど、サンプリングされたランダムソースのエントロピーが良くなります。
新しいランダムデータのセットが準備でき検証が終わると、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。このフラグは必ず使用する必要があります。
RNGは、提供されたデータのランダム性の基本検証を行います。たとえば、同一の値（0または1）が64ビットを超えて連続する場合や、32回を超えて連続的に0と1が交互に繰り返される場合には、シードエラーカレントステータスフラグがセットされます。
RNGクロックが32で分周されたHCLKクロックよりも小さい場合に、クロックエラーカレントステータスフラグがセットされます。
このチェックは、とりわけ、エントロピーを最大とするためにRNGクロックが低く初期化された場合に無効にできます。
また、割込みを有効にして、異常なシードシーケンスや周波数エラーを示すことができます。

ブロック図



このRNGが単純化されたブロック図には、その基本的な機能モジュールと制御モジュールが示されています。
乱数生成器は、複数のリングオシレータで構成されるアナログ回路に基づいています。サンプリングされたリングオシレータ出力の排他的論理和をとり、計算ラウンド当たり4個の32ビット乱数を生成可能なデジタル後処理ブロックに送り込むシードを生成します。
アナログシードのサンプリングは専用RNGクロック信号からクロック供給を受けますので、乱数の特性としてはHCLK周波数と無関係になります。
後処理ブロックの内容は、4ワードのFIFOを通じてデータレジスタに転送されます。FIFOがフルになるとすぐにデータレディフラグ（DRDY）がトリガされ、それ以上のデータをRNGから読み戻すことができなくなると、自動的にリセットされます。
並行して、エラー管理ブロックにより、正しいシード動作とRNGソースクロックの周波数が検証されます。
シードの中に異常シーケンスが検出されたり、RNG周波数が低過ぎたりした場合には、ステータスビットがセットされて割込みがトリガされます。
（品質上の理由などにより）RNGクロックがAHB_CLK/32未満に固定されている場合には、RNG周波数エラーチェックは無効にする必要があります。

低電力モード

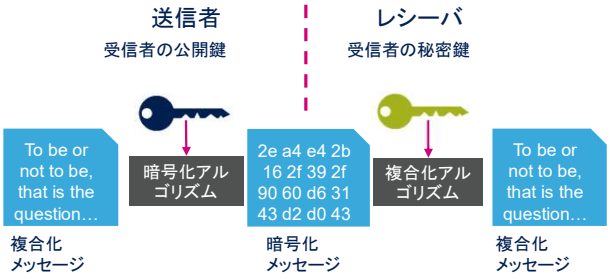
モード	RNGペリフェラルの説明
RUN	有効
SLEEP	RCCまたはRNGで無効化される（RNGEN=0） RNGを有効に保つと、RNG初期化時間のためのランダムサンプルが利用可能となるまでのレイテンシが解消される
低電力RUN	消費電力を最小とするためにRCCで無効化
低電力SLEEP	
STOP0/1	
STANDBY	STANDBYパワーダウン状態　ペリフェラルは、STANDBYモード終了後に再初期化する必要がある
SHUTDOWN	SHUTDOWNパワーダウン状態　ペリフェラルは、SHUTDOWNモード終了後に再初期化する必要がある

life.augmented

真性乱数生成器は、RUNモードでのみアクティブです。初期化時のレイテンシを回避するために、SLEEPモードで有効に保つことができます。その他の低電力モードでは無効化され、STANDBYモードとSHUTDOWNモードでは完全にパワーダウンされます。

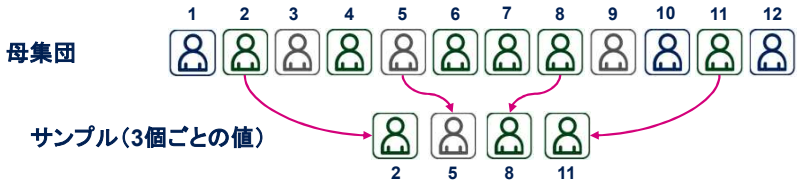
アプリケーション例

- 暗号化



- ゲーム

- 統計的サンプリング



life.augmented

RNGは、暗号、ゲーム、統計的サンプリングを含む幅広いアプリケーションに利用できます。たとえば、暗号化アルゴリズムのすべてのセキュリティは、キーの推測が不可能であることに結び付いています。そのためにキーは乱数である必要があり、そうしないと攻撃者による推測が可能です。

関連ペリフェラル

- RNGに関連したペリフェラル
  - RCC（RNGクロック制御、RNGイネーブル／リセット）
  - 割込み（RNG割込みマッピング）

これは、乱数生成器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トレーニングを参照してください。

参照

- AN4230: STM32 microcontrollers random number generation validation using NIST statistical test suite.
  - AN4230は、STM32マイクロコントローラ群に内蔵されている乱数生成器ペリフェラルによって生成される数のランダム性検証ガイドライン。この検証は、米国標準技術研究所（NIST）の統計テストスイート（STS）SP800-22（公開後、2010年4月にSP800-22rev1aとして更新）に基づく
  - NISTテストスイートは、RNGペリフェラルを搭載しているSTM32ボード群の上で実行
    その結果は、ファームウェア･フォルダ ‘NIST_Test_Suite_OutputExample’に格納されている

詳細については、STM32MCU群によって生成される乱数を検証するためのNIST統計テストスイートの使用に関するアプリケーションノートAN4230を参照してください。