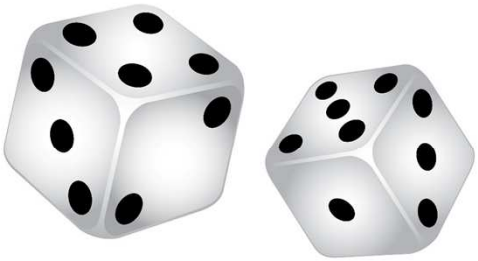
こんにちは、STM32乱数ジェネレータのプレゼンテーションへようこそ。
このプレゼンテーションでは、乱数を提供するために広く使用できる周辺装置の機能を説明します。

概要



- 乱数の提供
  - 予測不可能な結果を生み出す時に使われる

アプリケーションの利点

- 数の無作為性を増やす
- 値を推測する可能性を減少させる

予測不可能な結果を生み出したい時に、STM32マイコン製品の中で統合された乱数ジェネレータ（RNG）が、乱数を提供します。
アプリケーションは、数の無作為性を増大させるか、または一定の値を推測する可能性を減少させるために、RNGは有効です。

主な特徴

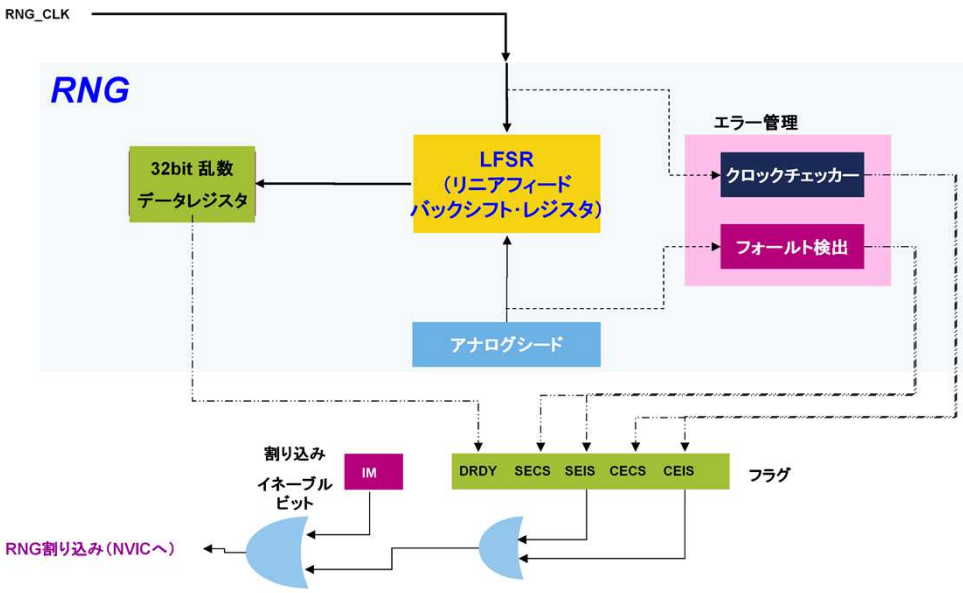
3

- ノイズソースをベースにした32bit 乱数発生器
  - 32bit 乱数はAHB/54の平均的周波数で生成可能。
  - 電力消費量を減らすために無効化が可能。
- 次の場合に、3つのフラグでトリガを掛けることが可能
  - 有効なランダムなデータは用意できた時。
  - 異常シーケンスがシード(初期値)上で発生した時(同じ値を持つ64を超える連続的なビット、または、0と1を32回連続的交替する時).
  - 周波数エラーは、PLL48 RNGクロックソースを使う時に検出
- 1割り込み
  - エラー表示のため(異常なシードまたは周波数エラー)。

life.augmented

RNG周辺装置は、後で詳細に説明されるランダムな32bit値を提供する連続的なアナログノイズに基づいています
RNGは、AHB/54の平均的な周波数で32bit乱数を生成することができます。
新しいランダムなデータが用意できて、確認済みの時には、フラグがデータレジスターにセットされます。
RNGは、提供されたデータの無作為性を確認します;
もし64を超える連続的なビットが同じ価値(0または1)を持っているか、または32より多く0と連続的交互1があるならば、シードのエラーカレントステータスフラグがセットされます。
PLL48 RNGクロックソースが使われる時は、もし、HCLKが32で割られるよりPLL48クロック周波数が小さいならば、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。
割込みソースで、異常なシードシーケンスまたは周波数エラーを示めさせることは可能です。

ブロック図



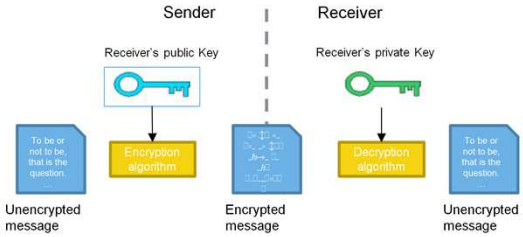
life.augmented

RNGのブロック図は、その基本機能 とコントロールモジュールを示します。
乱数ジェネレータは、いくつかのリング発振器で作られたアナログ回路に基づきます、その出力は、32bit乱数を生み出すためにリニアのフィードバックシフトレジスタに供給するシードを発生させるXORさせる回路です。
リニアのフィードバックシフトレジスタは専用のRNGクロックシグナルで動作するので、乱数の品質はHCLK周波数から独立しています。
シードの重要な数がLFSレジスターに導入された時に、リニアのフィードバックシフトレジスタの内容がデータレジスターに変えられます。
並行して、もしPLL48ソースが使われるならば、エラー管理ブロックはRNGソースクロック周波数と正しいシードの振る舞いとを比較確認します。
ステータスビットは設定されていて、もし異常なシーケンスがシードに検出されるか、または、PLL48 RNGクロックの周波数

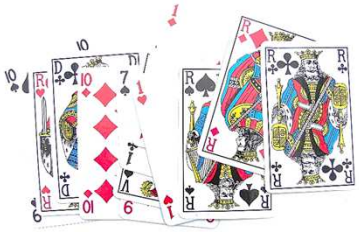
が低すぎる場合は、割り込みが引き起こされます。

使用例

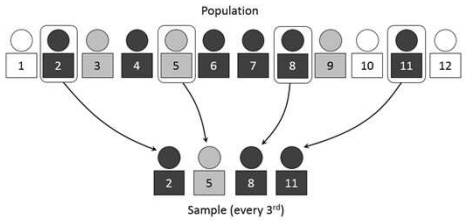
- 暗号化



- ゲーム



- 統計のサンプリング



life.augmented

RNGは、暗号、ゲーム、および統計のサンプリングを含む様々なアプリケーションに使うことができます。
例えば、暗号アルゴリズムのすべてのセキュリティは、キー値を推測しなければならないため、乱数のキー値は解読を不可能性にしています。
キーが乱数でないと、ハッカーがキー値を推測できてしまいます。

関連する周辺機能

- RNGと関連する周辺機能
  - RCC（RNGクロックコントロール、RNG 有効/リセット）
  - 割り込み（RNG 割り込みマップ）

life.augmented

これは、乱数ジェネレータと関連した周辺装置のリストです。
もし必要ならば、これらの周辺機能のより多くの情報が記載されているトレーニング 資料を参照してください。

参考

AN4230: STM32F2xx, STM32F4xx random number generation validation using the NIST statistical test suite.

- AN4230は、STM32F2またはSTM32F4に内蔵された乱数発生器確認するガイドラインです。これは、アメリカ国立標準技術研究所（NIST）統計テストスイート（STS）SP 800-22（2010年4月）に基づいています。
- NISTテストスイートは、STM3220G-EVAL.rev.BとSTM3240G-EVAL.rev.Bボードにおいて実行されています。結果はファームウェアフォルダ『NIST_Test_Suite_OutputExample』において提供されます。

life.augmented

詳細については、STM32F2とSTM32F4 MCUにより生成された乱数を有効にするためにNIST統計テストスイートを使用することについて書かれているアプリケーションノートAN4230を参照してください。