IoT時代はデータ漏えいの危険がいっぱい…
ワンチップCortex-Mでここまで!

マイコン内蔵最新セキュリティ機能の研究

第2回　暗号化通信に欠かせない! 乱数生成器RNG

中森 章

今回は，暗号化通信などで欠かせない乱数生成器を紹介します．いい乱数値を得るのは，意外と簡単ではありませんので，半導体メーカの腕の見せどころです．（編集部）

乱数生成器とは

乱数生成器RNG（Random Number Generator）は，その名の通り乱数を生成できます．乱数は予測不可能な値の生成が必要な以下のような用途に使えます．

- 暗号鍵の種となるデータ生成
- 個人認証用のユニークなIDとして利用
- より乱雑さの高い乱数を生成する種（エントロピー生成）
- シミュレーションや暗号用の初期値生成
- シミュレーション実験のランダムなデータ生成（モンテカルロ・シミュレーション）
- 法則性/規則性を伴わない現象の将来予測
- 膨大な資料からの無作為なデータ抽出（確率的に発生する値生成，代表値生成）
- キャンペーンやプロモーションでの利用（抽選番号）

本連載のターゲット・マイコンKinetis（フリースケール・セミコンダクタ）におけるRNGモジュールの正式名称はRNGA（Random Number Generator Accelerator：乱数生成の加速装置）といいます．ディジタル署名のための連邦情報処理標準（Digital Signature Standard）で定義された暗号鍵の元になる乱数を生成します．乱数は32ビット長です．

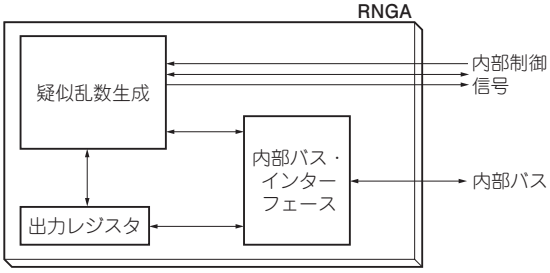

図1　その1：簡易乱数生成器RNGAの内部ブロック

● ホントの乱数を得るのはかなりムズい

乱数はリング・オシレータからのクロックで動作するシフト・レジスタから生成されます．リング・オシレータの周波数は不安定なので，それによって生成されるシフト値はそれなりにいい値（適度にばらつく）になるそうです．しかし，こうやって作られる乱数は再現しやすい（攻撃を受けやすい）ので，米国の国立標準技術研究所（National Institute of Standards and Technology：NIST）で認められた疑似乱数の種（シード）にすることが推奨されています．これは，DESやSHA-1で乱数をさらに暗号化することであると考えられます．

また，別の乱雑さ（エントロピー）を生成する資源と共にRNGを使って疑似乱数の種を生成することも推奨されています．たとえば，時計の時刻，マウスやキーボード（タッチパネル）の移動距離などをエントロピーとして与えて乱数生成を行うことができます．

● 乱数生成の基本動作

リセット後，シフト・レジスタはシフト動作を開始しますが，RNGA制御レジスタのGOビットがセットされるまでは，RNGA出力レジスタへの出力は行われません．GOビットがセットされた後は，システム・クロックの256サイクルごとにRNGA出力レジスタが更新されます（シフト・レジスタからの転送）．ただし，RNGA出力レジスタを読み出すまでは新たな更新は行われません．また，RNGAエントロピー・レジスタに適切な値を書き込むことで生成される乱数の品質を向上させます．RNGAエントロピー・レジスタが存在するかどうかは実装依存です．

なお，実装によっては，RNGA出力レジスタは最大255段のFIFOに構成できます．しかし，通常は1段のみのサポートのようです．

Kinetisマイコンの乱数生成器

● その1：簡易乱数生成器RNGA

RNGAの内部回路ブロックを**図1**に，レジスタ一覧