メタスタビリティを利用した真性乱数生成回路の FPGA による実装

指導教員：市川 周一　　学籍番号：043732　畑 尚志

1　はじめに

多くのセキュリティ技術は安全性の根拠を乱数に依存している．そのためハードウェアによる真性乱数生成器 (True Random Number Generator; TRNG) は, セキュリティの基盤技術として重要である. 熱雑音など物理乱数を利用した TRNG が実用化されているが, 実装にアナログ回路が必要であるため論理 LSI への集積が難しい.

デジタル回路で実装可能な TRNG として発振器のジッタを利用した方法とメタスタビリティを利用する回路が提案されている. Sunar ら [2] は奇数のインバータで構成されるリングオシレータ (RO) を利用した TRNG を提案した. Sunar らの実装では Free run の RO が複数必要になるため消費電力が大きくなる. 一方, メタスタビリティを利用した TRNG は実装が難しくカスタム LSI で実装された例がほとんどである [1].

本研究では RS ラッチのメタスタビリティを利用した TRNG (ラッチ型 TRNG) を FPGA (Field Progarammable Gate Array) で実装し, その乱数品質と生成速度を報告する. FPGA は RAM (LUT) とスイッチで構成される回路で, 配線遅延等の調整に制限がある. そのため, FPGA で実装可能であればカスタム LSI でも実装可能である. また, FPGA は近年広く利用されているため, FPGA で実装可能であることはそれ自体が実用的価値が高い.

2　RS ラッチによる乱数生成

一般に，ラッチのセットアップ時間やホールドタイム違反が起こると，メタスタビリティが発生する．例として，RS ラッチの R 入力と S 入力を同時にアサートする回路を図 1(a) に示す．図 1(a) の回路は，TRNG CLK=0 では出力 $(Q, \bar{Q}) = (1, 1)$ で安定状態となるが，TRNG CLK=1 では $(Q, \bar{Q}) = (0, 1)$ あるいは $(1, 0)$ で安定となる．実際には，ラッチは TRNG CLK の立ち上がりエッジでメタステーブル状態 (準安定状態) になり，その後，いずれかの安定状態へ遷移する．これは (理想的には) コインストスにより 1 bit の乱数を得ることに相当する．安定状態への遷移時間は一定でなく，確率分布をもつ.

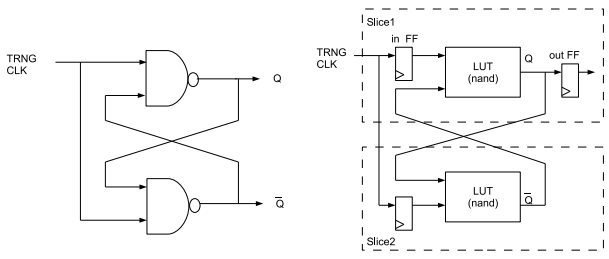
上に述べた TRNG の動作原理は単純であるが，実際に高品質の乱数を生成することは容易でない．例えば TRNG CLK 信号にスキューがある場合，ラッチの出力が 0 もしくは 1 に偏る可能性がある．2 つの NAND ゲートのドライブ能力に差がある場合も同様である．スキューやドライブ能力差がない場合でも，前回の出力に応じて Q,$\bar{Q}$ 間に電位差がある場合に出力に偏りが生じうる.

RS ラッチを FPGA に実装するために nand ゲートを LUT に置き換える. FPGA で実装可能なラッチ (LUT latch) を図 1(b) に示す. 図 1(b) の回路では入力側に Flip-Flop (FF) を挿入し配線遅延を小さくすることでスキューを小さくしている. さらに, 出力に FF を挿入して $Q, \bar{Q}$ の配線負荷を均衡化している.

乱数品質を上げるためにゲートのドライブ能力の均衡をとる必要があるが, FPGA ではこれを是正することは出来ない. そのため LUT latch を複数実装し XOR をとることで偏りを補正する. 以後, LUT latch が n 個の構成の TRNG を LUT latch n と表記する.

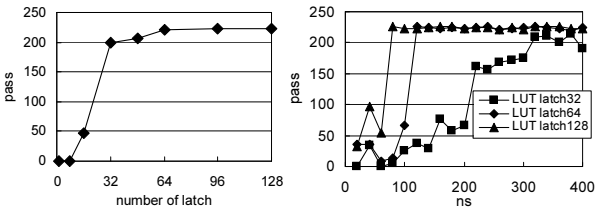
3　TRNG の実装と評価

実装評価には，Xilinx Virtex4 FX20 (XC4VFX20) を搭載する Xilinx ML405 ボードを使用した．CAD は Xilinx ISE 10.1.03 を使用し，パラメータはデフォルトで使用した．乱数の取得は，FPGA に搭載されている PowerPC 405 に TRNG を周辺回路として接続して行う．クロックは PowerPC が 300MHz，バスクロックが



(a) RS ラッチによる乱数生成　　(b) FPGA に実装するラッチ

図 1: LUT latch



(a) LUT latch の数と乱数品質　(b) サンプリング周期と乱数品質

図 2: Diehard テストでの評価

表 1: 回路規模と乱数生成速度

Design	Slice	Mbps
LUT latch 64	145	3.8
LUT latch 128	290	8.3
LUT latch 256	580	12.5

100MHz である.

TRNG はバッファ(1 MB SRAM) を介して PowerPC 405 に接続されている．動作開始後，TRNG はバッファを満たすまで出力を行い，バッファが満たされると停止する. 1 MB 以上の出力を生成する場合は，1 MB の計測を複数回繰り返す.

乱数の評価には Diehard テストと NIST テスト [3] を使用する. Diehard テストは Marsaglia が提案した乱数テストセットである. 本研究では Diehard v0.2 beta[4] の乱数テストを使用した. 乱数の評価は p value によって行われる. p value は理想的な乱数ならば [0,1] の間に一様分布する値で,Diehard テストでは 10 MB の乱数を入力すると 229 個の p value を出力する. p value の評価基準は設けられていないため, 本研究では 0.01 <p value< 0.99 の範囲に収まる値がいくつあるかで評価した．理想的な乱数ならば 225 個前後の p value がテストに合格するはずである. Diehard テストはデータ量が小さく短時間でテストできるため TRNG の簡易評価に使用した.

NIST テストは National Institute of Standards and Technology が提案する乱数検定で, 15 種類のテストから構成されている. 本研究ではバージョン 1.8 を使用し，データ量は 10^9 bit，パラメータはデフォルトとした．p value の評価は NIST の評価基準に準じて行い，15 種類のテストすべてに合格した場合に NIST テストに合格したと判定する．NIST テストは乱数の最終的な評価に使用する.

Diehard テストでの評価結果を図 2 に示す. 図 2(a) はサンプリング周期を 320ns 固定とし, LUT latch の数を変えた場合である. Diehard テストでの評価では LUT latch は 64 個以上必要になる. 図 2(b) では LUT latch が 32, 64, 128 個の時のサンプリング周期を評価している. LUT latch の数が増えるとサンプリング周期を短く出来ることがわかる.

最後に NIST テストで合格することを確認し, 乱数生成速度を評価した (表 1) .

4　おわりに

本研究でラッチ型 TRNG の基本動作は確認したが実応用には更なる検討が必要である. まず, 電源電圧や温度変化に対する乱数品質の評価が必要である. また, XC4VFX20 以外のデバイスでも検証する必要がある. ラッチ型 TRNG はシンプルな回路構成で, ラッチ数の変更により乱数品質を調整することが可能なため条件が変わっても実装可能であると考えられる.

参考文献

[1] 市川周一, 畑尚志, “RS ラッチのメタスタビリティを利用した真性乱数生成回路,” Proc. SCIS 2009, 2F1-5, 2009. (CDROM)

[2] B. Sunar, W.J. Martin, and D.R. Stinson, “A provably secure true random number generator with built-in tolerance to active attacks,” IEEE Trans. Comput, vol.56, no.1, pp.109–119, 2007.

[3] NIST, “Statistical test suite,” `http://csrc.nist.gov/groups/ST/toolkit/rng/documentation_software.html`, 2008.

[4] “Diehard Battery of Tests of Randomness v0.2 beta,” `http://i.cs.hku.hk/~diehard/`, 2008.