2021 年度 卒業研究発表 梗概

電気学科

学籍番号 氏　名	V18033　大矢 龍聖	指導教員	藤枝 直輝
題　目	高位合成による乱数検定回路の実装と評価		

1　序論

システムのセキュリティにおいて真性乱数は重要である。真性乱数は、ハードウェアの物理現象を利用して生成され、原理上次の出力が予測不可能である。これを生成する回路や機器を真性乱数生成器 (TRNG) とよぶ。TRNG の乱数品質は動作条件によって変動するので、制御する必要がある。乱数品質は乱数検定によって判定できるが、乱数検定は基本的にソフトウェア上で行い、大量の乱数データが必要であるため、即時性に欠ける。乱数検定をハードウェア上で扱えれば、再利用性や即時性があるものとして使える。しかし、高い演算精度を保とうとすると大量のハードウェアが必要となる。解消するには固定小数点演算を使用して演算精度を落とす必要がある。

本研究の目的は、この乱数検定をハードウェア化するための演算精度の検討、および高位合成 (HLS) を使用した乱数検定のハードウェア化とその評価である。

2　関連研究

岸部らは、乱数検定のテストスイートである diehard の 18 種類のテストによって、ラッチ型 TRNG で生成した乱数の品質を評価している [1]。diehard テストの中で、2 つの count the 1's(stream と specific byte) は、論理が簡単でオンライン制御に向いており、おおむね diehard テスト全体の結果を示すことが分かった。このことから、本研究でハードウェア化の対象とする乱数検定は count the 1's(stream) とした。

3　演算精度の検討

本研究では、まず、count the 1's のハードウェア化に向けて、TC-TERO 型 TRNG [2] というパラメータを変更することで動作条件を変更できる TRNG を用いて、diehard テストの予備評価を行った。TRNG のパラメータは 1〜100 とした。その結果、diehard に合格しない乱数列は、count the 1's において、合格だと判定する値からかけ離れた評価値を示すことが分かった。そのため、count the 1's において、明らかに失敗と判断できる場合は、計算途中で打ち切るようにする。具体的には、χ^2 値の計算途中の値によって打ち切りを決め、閾値を超えた場合、その時点で計算を打ち切り、テスト不合格とした。

固定小数点演算での精度を保つために、各計算時において、小数部分のビット数とテスト結果との関係を評価する。パラメータ 0〜500 のうち、count the 1's に合格した 17 個のパラメータを使用する。計算時に使用する値の小数部分のビット数を変更し、合否の判断に影響するかどうかを調べる。全ての計算でビット数を同一にした場合、ビット数を 16 以上にした場合、全てのパラメータで合格と判断された。減算処理以外は 16 ビットにし、減算処理のビット数のみを変更した場合、ビット数を 3 以上としたときに合格と判断された。これらのことから、小数部分のビット数は、減算処理の値は 3 ビット、その他の値では 16 ビットとする。

4　ハードウェア化と評価

3 節の検討結果に従い、変更したプログラム (固定小数点演算) と変更を加えていないプログラム (浮動小数点演算) の 2 つをハードウェア化する。HLS プラグマを使用して、回路のインターフェイスを作成し、ループ処理をパイプラインとした。これらを高位合成した後、TC-TERO 型 TRNG で乱数を生成しつつ、ハードウェアの count the 1's に乱数を入力するようなシステムを作成する。

作成したシステムにおいて、ハードウェア処理とソフトウェア処理のテスト結果は全て一致した。論理合成後のハードウェア量は、浮動小数点演算と比べて、LUT(Look-up Table) 数で 57%、FF(Flip-flop) 数で 47% 削減された。今後の課題として、さらなるハードウェア量の減少がある。

参考文献

[1] 岸部 仁美, 市川 周一, 藤枝 直輝: "ラッチ型 TRNG の軽量実装に関する検討," 電気学会研究会資料 IIS-21-012, 2021

[2] N.Fujieda: "On the feasibility of TERO-based true random number generator on Xilinx FPGAs," in FPL 2020, pp. 103-108, 2020.