乱数品質を保証したオンチップハードウェア乱数発生器の開発（102107008）

Development of quality-assured on-chip hardware random number generator

研究代表者
橋本昌宜　大阪大学
Masanori Hashimoto　Osaka University

研究分担者
なし

研究期間　平成 22 年度～平成 24 年度

概要
電源などの外乱(他回路からのノイズや意図的な悪意有る攻撃)に一定の耐性を持つオシレータサンプリング方式を基本方式として採用し、チップ内の小さなランダム雑音を増幅する回路を開発して、乱数品質向上や外乱耐性向上を実現した。さらに、製造ばらつきや環境変動・意図的な攻撃による乱数品質の劣化を検出する機構を開発し、自己調整(回路パラメータ調整や後処理方式の変更)により品質劣化要因を克服した。以上により品質が保証された乱数生成を達成した。

１．まえがき

社会基盤の電子化に伴い、情報セキュリティ、特に暗号の重要性が増している。暗号化には予測不可能性を持つハードウェア乱数が必要であるが、現在は疑似乱数生成器を用いて乱数が生成されており、予測不可能性が達成できていない。本研究は、オンチップに搭載可能な小型ハードウェア乱数発生器を開発し、予測不可能なハードウェア乱数が暗号の鍵生成などに容易に利用できる環境を提供し、情報セキュリティの強化を達成することを目的に実施した。

２．研究開発内容及び成果

研究開発成果の目標:

本研究では、暗号の鍵生成に容易に利用可能なオンチップ搭載可能ハードウェア乱数生成器を開発した。これまでハードウェア乱数生成器が普及しなかった主な原因として、乱数品質の保証がなかったことがあげられ、将来的には耐タンパー性への配慮がないことが問題視されると考えられる。本研究では、回路の簡潔さや電源ノイズに対する耐性等の好ましい性質を持つオシレータサンプリング方式に着目し、下記の 4 つの特徴を持つハードウェア乱数生成器方式を開発してその動作を実機にて確認する。

(1) 容易なオンチップ搭載　　専用デバイスを必要としない簡易なデジタル回路で構成
(2) 乱数品質の保証　　乱数出力を常に監視し、回路の自己調整により品質低下を防止
(3) 柔軟なスループット　　乱数品質とのトレードオフにより柔軟なスループットを実現
(4) 耐タンパー性　　意図的な電源ゆらぎ攻撃に対する耐性を実現

研究開発のアプローチ:

本研究では、容易なオンチップ搭載を考え、他回路からの電源ノイズや電源を通じた意図的な悪意有る攻撃に一定の耐性を持つオシレータサンプリング方式を基本方式として採用した。チップ内で得られる時間ゆらぎが小さい問題に対し、小さな時間ゆらぎを増幅する回路を開発して、乱数品質向上や外乱耐性向上を実現した。さらに、製造ばらつきや環境変動・意図的な攻撃による乱数品質の劣化を検出する機構を開発し、自己調整(回路パラメータ調整や後処理方式の変更)により品質劣化要因を克服した。以上により品質が保証された乱数生成を達成した。

図 1(a)にオシレータサンプリング方式乱数生成器の回路構造を示す。速度差のある二つのオシレータがあり、高速オシレータの発振信号をデータ、低速オシレータの発振信号をクロックとし、D フリップフロップでサンプリングすることで乱数列を得る。図 1(b)に二つのオシレータの発振波形を示す。低速オシレータ内の回路内雑音により発振周期にゆらぎが生じるため、発振波形の立ち上がりタイミングにもゆらぎが生じる。D フリップフロップはクロックの立ち上がりタイミング時のデータの 0/1 にしたがってビット列を出力するため、ゆらぎによって 0/1 が変化する。このように回路内部のランダムな雑音から乱数列を得ることができる。

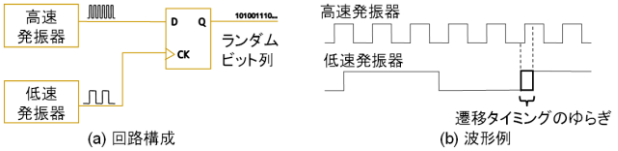

図 1: オシレータサンプリング方式

以上の研究開発を実施するため、以下の研究項目を実施した。研究相関図を図 2 に示す。

[1] インジェクションロッキングの影響評価
[2] 動作モデルを用いたワーストケース設計手法の開発
[3] ゆらぎ増幅回路の開発
[4] デューティ比モニタ回路およびデューティ比自己構成機構の開発

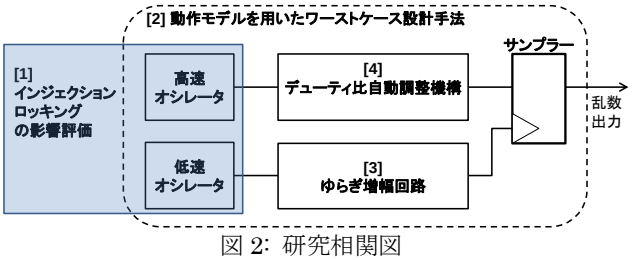

図 2: 研究相関図

なお、上記の研究項目と研究開発研究目標との関係は以下のように整理される。

(1) 容易なオンチップ搭載
チップ内の熱雑音を中心とするノイズをランダム源とし、簡潔な構成であるオシレータサンプリング方式を採用

(2) 乱数品質の保証　　研究項目[1][2][3][4]
[1]でインジェクションロッキングによる最悪のゆらぎ削減効果を評価し、ゆらぎ量が最大に削減された状態でも、十分なランダム性が達成できるワーストケース設計を[2]で実現する。乱数品質の向上に重要な、ゆらぎ量は[3]で増幅し、デューティ比は[4]で一定に固定する。
(3) 柔軟なスループット　　研究項目[2]
[2]を用いた設計パラメータと乱数品質の高速な評価により、低速オシレータの分周率を変化させて、乱数品質とスループットを柔軟に調整する。
(4) 耐タンパー性　　研究項目[1][2][3][4]
[1]の評価を通じて、オンチップではインジェクションロック攻撃が難しいことを示す。たとえ最悪のロッキングが起こっても乱数品質が達成できるワーストケース設計を[2]で実現する。ゆらぎ量を増幅することで、外乱への耐性を向上させる[3]。さらに、環境変動の変化による 0/1 比率の変化は[4]で調整する。

開発した真性乱数生成器

真性乱数生成器にとって、出力の 0/1 出現確率の偏りをなくすことは極めて重要である。動的な温度変化に対応するためには、高速オシレータのデューティ比をオンラインで調整する必要がある。
本研究では、オシレータベース真性乱数生成器向けのデューティ比自己校正機構を考案した。図 3 に開発した自己校正機能を有するオシレータベース真性乱数生成器を示す。本機構は、デューティ比モニタ回路とデューティ比調整回路からなる。環境の変化によってデューティ比が変化した場合、提案のモニタ回路が観測したデューティ比の情報をデューティ比調整回路に送る。デューティ比調整回路は高速オシレータのデューティ比を調整し、0/1 比の偏りを解消する。

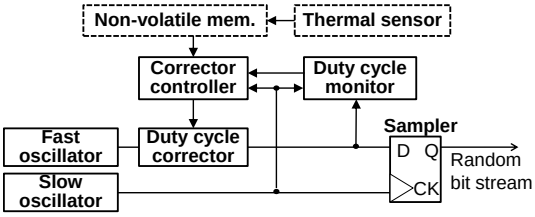

図 3: 自己校正機能を搭載した真性乱数生成器

提案自己校正機構を含む真性乱数生成器を 65nm プロセスで試作した。チップ写真を図 4 に示す。チップ面積は 6,500um² である。提案モニタ回路は 70 倍高精度に見積もることができること、自己校正が乱数品質向上に大きく寄与していることを実測で確認した。
乱数生成器の出力を NIST ならびに DIEHARD テストを用いて評価した。提案乱数生成器は 7.5Mbps のスループットですべてのテストをクリアし、乱数品質の高さを実証した。

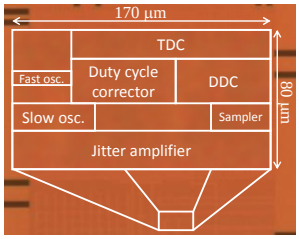

図 4: 65nm プロセスで試作した真性乱数生成器

最後に他文献との性能比較を表 1 に示す。提案回路は、後処理無く NIST テスト等をクリアした乱数生成器の中で最も小面積である。さらに、表には示されていないが、提案乱数生成器は環境変動に耐性を持っており、他文献の乱数生成器とは一線を画している。

表 1: 他文献との比較

	Bucci2003[11]	Bucci2008[3]	Pareschi2010[12]	Srinivasan2010[2]	This work
Principal	Direct amp.	Oscillator-based	Chaos-based	Metastable-based	Oscillator-based
Technology	180 nm	90 nm	180 nm	45 nm	65 nm
Area	25,000 μm^2	13,000 μm^2	126,000 μm^2	4,004 μm^2	6,670 μm^2
Area normalized to 45nm	1,563 μm^2	3,250 μm^2	7,875 μm^2	4,004 μm^2	3,335 μm^2
Throughput	40 Mbps	1.74 Mbps	80 Mbps	2.4 Gbps	7.5 Mbps
Randomness Assessment	FIPS140-1 Knuth	AIS31 Entropy eval.	NIST SP800-22	NIST SP800-22 Entropy eval. Autocorrelation eval. Run length eval.	NIST SP800-22 DIEHARD
Post processing	XOR	LSFR	-	-	-

３．今後の研究開発成果の展開及び波及効果創出への取り組み

本研究により、これまで疑似乱数を用いてきた通信回路やプロセッサにおいても、ハードウェア乱数が利用できる環境が整いつつある。さらに乱数の後処理の検討も加えて、実用化を進めたい。これらを通じて、より安全性の高い暗号鍵生成を実現し、高いセキュリティの達成、ひいては安心・安全の社会構築に貢献できるよう、さらに研究活動を進めたい。

４．むすび

本研究では、乱数品質の保証と容易なオンチップ搭載を考え、他回路からの電源ノイズや電源を通じた意図的な悪意有る攻撃に耐性を持つオシレータサンプリング方式を基本方式とした真性乱数生成器を開発した。チップ内で得られる時間ゆらぎが小さい問題に対し、小さな時間ゆらぎを増幅する回路を開発して、乱数品質向上や外乱耐性向上を実現した。製造ばらつきや環境変動・意図的な攻撃による乱数品質の劣化を検出する機構を開発し、自己調整(回路パラメータ調整や後処理方式の変更)により品質劣化要因を克服する機構を開発した。以上により品質が保証された乱数生成を達成し、65nm プロセスによる試作チップにより、乱数品質の高さと環境変動への耐性を実証した。

【誌上発表リスト】

[1] T. Amaki, M. Hashimoto, Y. Mitsuyama, and T. Onoye, ``A Worst-Case-Aware Design Methodology for Noise-Tolerant Oscillator-Based True Random Number Generator with Stochastic Behavior Modeling," IEEE Transactions on Information Forensics and Security, vol. 8, no. 8, pp. 1331--1342, August 2013.
[2] T. Amaki, M. Hashimoto, and T. Onoye, ``Jitter Amplifier for Oscillator-Based True Random Number Generator," IEICE Trans. on Fundamentals of Electronics, Communications and Computer Sciences, vol. E96-A, no. 3, pp. 684--696, March 2013.
[3] T. Amaki, M. Hashimoto, and T. Onoye, ``A Process and Temperature Tolerant Oscillator-Based True Random Number Generator with Dynamic 0/1 Bias Correction," Proceedings of IEEE Asian Solid-State Circuits Conference (A-SSCC), 発表予定.

【申請特許リスト】

[1] 橋本昌宜、天木健彦、ゆらぎ増幅装置及び真性乱数生成器、日本、2011/1/24