【9】

氏名	天木 健彦（あまき たけひこ）
博士の専攻分野の名称	博士（情報科学）
学位記番号	第 25846 号
学位授与年月日	平成25年3月25日
学位授与の要件	学位規則第4条第1項該当 情報科学研究科情報システム工学専攻
学位論文名	A Study on Oscillator-based True Random Number Generator Robust to Environmental Fluctuation （環境変動にロバストなオシレータベース真性乱数生成回路に関する研究）
論文審査委員	（主査） 教授 尾上 孝雄 （副査） 教授 今井 正治　准教授 三浦 克介　准教授 橋本 昌宜

論文内容の要旨

This thesis discusses an oscillator-based true random number generator (TRNG) which is robust to environmental fluctuation. Random number generated from physical random sources is a key component of a security system, such as cryptography and authentication, because of its unpredictability, and many instruments for random number generation have been studied. This thesis focuses on an oscillator-based TRNG, which utilizes random jitter of the oscillator as a random source, since it is easily implemented on silicon and it is inherently robust to deterministic noise compared to a direct amplification method. However, it is difficult to design an oscillator-based TRNG with circuit simulations, because ordinary simulators do not take the jitter into account directly. An efficient design methodology tailored to the oscillator-based TRNG is demanded. In addition, the amount of jitter is generally insufficient while the randomness of output bit stream depends on the jitter amount. Frequency dividers help accumulate the jitter, but they reduce the throughput of the TRNG. Thus, an oscillator which has large jitter yet operates at high frequency is required. Bias of output bits is another critical issue for the TRNG. Probability of '1' occurrence depends on duty cycle of an internal oscillator of the TRNG, whereas the duty cycle fluctuates by environmental variations. Consequently, post-silicon online tuning of duty cycle is indispensable.

This thesis firstly presents a design methodology for the oscillator-based TRNG based on a stochastic behavior model. The model is used to evaluate the randomness of the TRNG. Measurement results of a prototype TRNG fabricated in a 65 nm CMOS process show that the proposed model well reproduces the behavior of the TRNG. The stochastic model also enables a worst-case-aware design of the TRNG. This thesis analytically confirms that the worst case the methodology considers results in the lowest randomness of

outputs. The proposed worst-case-aware design methodology determines design parameters according to the worst χ value of a poker test under deterministic noise. Experimental results with a noise-aware gate-level simulator implemented for validation purpose verifies the efficiency of the worst χ evaluation. Also, a design example is presented to exemplify the proposed worst-case-aware methodology.

Secondly, this thesis proposes an architecture of a jitter amplifier to improve the randomness of the oscillator-based TRNG. Jitter of an oscillating signal is intensified by changing a propagation delay of a latency-controllable (LC) buffer. Two types of LC buffer, viz. two-voltage LC buffer and single-voltage LC buffer are presented. This thesis also derives an expression to estimate the gain of the jitter amplifier, and analyzes sufficient conditions for proper amplification. The oscillator-based TRNGs with the jitter amplifiers are implemented with a 65 nm CMOS process. Area of the amplifier with the two-voltage LC buffer is 3,300 μm^2, while the amplifier with the single-voltage LC buffer occupies 1,700 μm^2. Measured jitter gain of the jitter amplifier with the two-voltage LC buffer is 8.4, and that with the single-voltage LC buffer is 2.2. The jitter amplification enhances the entropy of bit streams, and makes the output random bits pass the all tests of the NIST test suite. The proposed jitter amplifier attains higher throughput per area than frequency dividers in most cases.

Finally, this thesis describes a system that self-calibrates duty cycle to remove the biasing. In the proposed system, a duty cycle monitor measures the duty cycle of an oscillating signal, and a duty cycle corrector adjusts the duty cycle according to the measured value. A TRNG with the proposed monitor and the corrector is fabricated in a 65 nm CMOS process. The duty cycle monitor measures the duty cycle with a resolution of 0.16 % and the duty cycle corrector achieves 0.11 % of resolution in average at 20 ℃. In addition, the monitor reduces the necessary time for estimating duty cycle to be 3,500 times smaller than output bit sampling. Employing the self-calibration system, the variation of probability of '1' occurrence due to the temperature fluctuation becomes 1/18 times smaller.

Integrating these accomplishments, this thesis realizes generation of highly random numbers even under environmental fluctuation, and contributes to development of highly secure systems.

論文審査の結果の要旨

本論文は、環境変動にロバストなオシレータベース真性乱数生成回路に関する研究の成果をまとめたものであり、以下の主要な結果を得ている。

1. 動作モデルを用いたワーストケース設計手法の提案

オシレータベース真性乱数生成回路(TRNG)の設計において、SPICE等の一般的な回路シミュレータを用いて設計パラメータを探索することは困難である。特にセキュリティ向けTRNGの設計においては、決定性雑音の影響を考慮する必要がある。本論文では、オシレータベースTRNGの動作モデルを構築し、モデルを用いて乱数品質を評価することで設計パラメータを効率的に探索する手法を提案した。また、決定性雑音下におけるワーストケースを考慮して乱数品質を評価する手法を提案した。提案設計手法を用いてTRNGを設計することにより、決定性雑音下においても十分な乱数品質を保証することができる。

2. 低速オシレータ向けゆらぎ増幅回路の提案

オシレータの周期ゆらぎはオシレータベースTRNGのランダム源であるが、十分な乱数品質を達成するために必要なゆらぎ量を得ることは困難である。本論文では、低速オシレータのゆらぎ量を増幅することで、乱数品質を改善する回路を提案した。65nmプロセスを用いて提案回路を実装し、最大8.4倍のゆらぎ利得を達成した。また、ゆらぎ利得の見積もり式を解析的に導出し、実測結果と良く一致していることを確認した。さらに、ゆらぎ増幅による品質改善効果により、NISTテストに合格し、2Mbpsのスループットを達成するTRNGを実現した。

3. 環境変動下におけるデューティ比自動調整機構の提案

TRNGの出力における"1"出現確率は温度変化の影響を受けて劣化する。本論文では、高速オシレータのデューティ比を自律的に調整することで温度変化への耐性を実現する機構を提案した。65nmプロセスを用いて、デューティ比モニタ回路およびデューティ比調整回路から構成される提案調整機構を実装した。デューティ比モニタ回路は、従来手法と比較して 3,500倍高速に"1"出現確率を推定できることを確認した。また、提案調整機構により、温度が5～60℃ と変化した場合の"1"出現確率の変動量を1/18に抑制できることを確認した。

以上のように、環境変動にロバストなオシレータベース真性乱数生成回路に関する研究は、温度変化や決定性雑音のある劣悪な環境の下でも高品質な乱数を生成するという点において非常に有用である。これにより、乱数を用いるセキュリティシステムの信頼性向上に貢献するものと期待できる。従って、博士(情報科学)の学位論文として価値のあるものと認める。