早稲田大学大学院情報生産システム研究科

# 博士論文概要

## 論文題目

# Study on Low Energy True Random Number Generator with Latch-based Core and von Neumann-based Post-Processing for Hardware Security

申　請　者
Ruilin Zhang

情報生産システム工学専攻
ディペンダブル情報システム研究

2022 年　3　月

Information security has become a critical issue in the IoT era due to a large number of edge devices communicating with servers and each other in an environment where human involvement is weak. That requires embedded cryptographic systems to protect confidential data. And true random number generator (TRNG) is an essential component of it. TRNG utilizes random physical phenomenon to generate unpredictable true random numbers, which can be used as secure keys, nonce, and so on.

There have been some requirements in TRNG. First, for a cryptographic application, TRNG must have high randomness output under PVT (process, voltage, and temperature) variations. Robustness against intentional attacks is also required. Second, the energy-constrained IoT devices motivate low energy TRNG. Therefore, this work targets to design low energy TRNG with high randomness and robustness.

Typically, a TRNG consists of a TRNG core and a post-processing block. The TRNG core utilizes physical noise and generates raw $n$ bits with defects. Then the post-processing block is applied to remove these defects and generate $m$ bits with high randomness. The extraction efficiency (*ExE*) is defined as $m/n$. The total energy of TRNG ($E_{\mathrm{TRNG}}$) is calculated as: $E_{\mathrm{CORE}}/ExE+E_{\mathrm{POST}}$, where $E_{\mathrm{CORE}}$ and $E_{\mathrm{POST}}$ are the energy of TRNG core and post-processing, respectively. Therefore, in order to design a low energy TRNG, both low $E_{\mathrm{CORE}}$ and $E_{\mathrm{POST}}$, and high *ExE* are required.

For low energy and high *ExE* post-processing, N-bits von Neumann (VN_N) is a candidate. It can potentially reduce the dynamic power by processing N-bits at the same time. As the N value increases, its *ExE* is increased. But the mapping table complexity increases exponentially ($2^{N}$), which has been an obstacle for hardware implementation.

In the field of TRNG core, latch-based TRNG potentially provides low energy solution, thanks to the simple structure and only one-time voltage transition for data generation. However, it suffers mismatch-induced entropy drop, which requires complex calibration and feedback circuits. Or 256 latches are needed for obtaining 1-bit output. Both of them consumes a lot of energy.

Based on these considerations, in this dissertation, high *ExE* and low energy post-processing based on VN_N approach, and feedback control free low energy latch-based TRNG core are studied.

As for the post-processing, the mapping table complexity in VN_N is solved in three levels: At the algorithm level, a waiting strategy is proposed. By gathering two newly introduced waiting flags and generating output bits, high *ExE* with a small N value is achieved. At the architecture level, a Hamming weight-based structure is proposed to reconstruct the large table using smaller tables based on Hamming weight. At the logic level, an input-symbol-based code assignment using input codes as outputs is proposed for logic reduction. An 8-bit von Neumann with waiting (VN_8W, 62.21% *ExE*) is designed and confirmed in real chip.

As for the TRNG core, a low energy and high robustness latch-based TRNG core is proposed. It removes the calibration and feedback circuits by two novel methods: mismatch self-compensation and random noise enhancement. The mismatch self-compensation is realized by placing the initial state point close to the metastable point using newly added gate capacitance. In contrast with the conventional fixed initial state point, the proposed initial state point follows the metastable point, which changes position in response to mismatch variations. For noise enhancement, damped oscillation using large resistor is applied for the first time.

Finally, VN_8W is combined with the latch-based TRNG core to build a total TRNG. The performance of the total TRNG is verified by real chip.

The dissertation contains five Chapters as follows:
Chapter 1 briefly introduces the security issues in the IoT era and the random number generators in hardware security.

Chapter 2 shows the TRNG design requirement with introduction of previous works on post-processing and TRNG core. Then, the motivation and concept of this research are presented.

Chapter 3 describes the proposed N-bit von Neumann post-processing with high *ExE* and low energy. First, a light-weight 4-bit von Neumann (VN_4) using input-symbol based code assignment is presented. The logic complexity is roughly reduced to 2/16 times than the conventional code assignment. Then, the concept of waiting strategy is shown. VN_4 with waiting (VN_4W) achieved 46.88% *ExE*, which is higher than conventional 6-bit von Neumann (VN_6, 41.67% *ExE*). Targeting more than 50% *ExE*, hardware implementation of VN_8W with 62.21% *ExE* is presented. Using the Hamming weight-based structure, the conventional $2^8$ complexity mapping table is rebuilt with two identical 4 Bits Logic ($2^4$ complexity) and an 8 Bits Logic ($5^2$ complexity). Therefore, the mapping table complexity is roughly improved 4.5 times.

Fabricated in 130-nm CMOS, combined with the clock gating technique, VN_8W achieves low energy of 0.18 pJ/bit at 0.45 V, 1 MHz. Compared with previous work based on iterated von Neumann, it achieves more than 20% energy reduction at identical supply voltage.

Chapter 4 shows the proposed low energy latch-based TRNG. The TRNG core features mismatch self-compensation and random noise enhancement. First, the proposed entropy source latch circuit is described. Then, the mismatch self-compensation is introduced. It is achieved by placing the initial state point close to the metastable point, and 63.3% mismatch is self-compensated by newly added gate capacitance. The noise enhancement in damped oscillation mode by introducing RC delay in the feedback loop of each inverter is presented. The noise is 3 times enhanced by the newly added large resistor. As a result, the TRNG core exhibits 6σ robustness against process variations with only 4 entropy source latches. This is 1/64 times smaller than the conventional work (256 latches).

The total TRNG, including VN_8W, is verified with chips fabricated in 130-nm CMOS. It operates across a wide voltage (0.3-1.0V) and temperature (-20-100 ℃ ) range. Cryptographic-grade randomness is verified by NIST SP 800-22 and 800-90B IID tests. Power noise injection resilience is also demonstrated. An aging test reveals the equivalent 11-year life of the TRNG. It achieves the state-of-the-art minimum energy consumption of 0.186 pJ/bit at 0.3 V. These measurement results demonstrate that the TRNG has high randomness under PVT variations and low energy consumption, suitable for energy-constrained IoT devices.

Chapter 5 concludes the dissertation.