Multiple output bits ROPUF design for TRNG

Filip Kodýtek, Róbert Lórencz, Jiří Buček and Simona Buchovecká
Czech Technical University
Faculty of Information Technology
Prague, Thákurova 9
Email: { kodytfil | lorencz | bucekj | buchosim }@fit.cvut.cz

Abstract

In this contribution we propose method of generating random numbers utilizing the circuit primarily designed as PUF based on ring oscillators (ROs). The ROPUF proposed in [1] is based on selecting suitable part (multiple bits) of the counter value, whose value is derived from the ratio of 2 frequencies of 2 ROs in a pair. These bits from the counter value are selected according to their statistical properties, such as stability and entropy, because we need both of these properties to be met in order to generate unique and stable PUF outputs.

To generate random numbers, we need to use the bits with high entropy and low stability. For this purpose, the bits close to the least significant bit of the counter value appear to be suitable source of randomness.

We tested single bits from the counter values obtained from various RO pairs for randomness using the statistical tests in NIST SP 800-22. Based on the results, we selected bits that can be used for TRNG to generate random sequences of bits. To improve the statistical properties of the generated random sequences, we used post-processing techniques. As in the case of PUF, where we extracted multiple bits from each counter value for the PUF output, we obtained multiple bits from the same counter values for the random sequence generated by the same circuit. Therefore, for a single challenge to this circuit, we can generate both the PUF output and a random sequence.

References

[1] Kodýtek, F.; Lórencz, R. Proposal and Properties of Ring Oscillator-Based PUF on FPGA. In *Journal of Circuits, Systems and Computers.* 2015, 1640016.