Varchola, Michal; **Drutarovsky, Milos**

New high entropy element for FPGA based true random number generators. (English)

Zbl 1434.94079

Mangard, Stefan (ed.) et al., Cryptographic hardware and embedded systems – CHES 2010. 12th international workshop, Santa Barbara, USA, August 17–20, 2010. Proceedings. Berlin: Springer. Lect. Notes Comput. Sci. 6225, 351-365 (2010).

Summary: We demonstrate a new high-entropy digital element suitable for True Random Number Generators (TRNGs) embedded in Field Programmable Gate Arrays (FPGAs). The original idea behind this principle lies in the randomness extraction on oscillatory trajectory when a bi-stable circuit is resolving a metastable event. Although such phenomenon is well known in the field of synchronization flip-flops, this feature has not been applied for TRNG designs. We propose a new bi-stable structure – Transition Effect Ring Oscillator (TERO) where oscillatory phase can be forced on demand and be reliably synthesized in FPGA. Randomness is represented as a variance of the TERO oscillations number counted after each excitation. Variance is highly dependent on the internal noise of logic cells and can be used easily for reliable instant inner testing of each generated bit. Our proposed mathematical model, simulations and hardware experiments show that TERO is significantly more sensitive to intrinsic noise in FPGA logic cells and less sensitive to global perturbations than a ring oscillator composed from the same elements. The experimental TERO-based TRNG passes NIST 800-22 tests.

For the entire collection see [Zbl 1193.68012].

MSC:

94A62 Authentication, digital signatures and secret sharing
94A17 Measures of information, entropy

Keywords:

True Random Number Generators (TRNGs); Field Programmable Gate Arrays (FPGAs); oscillatory metastability; randomness extraction; inner testability

Full Text: DOI