A New Robust True Random Numbers Generator Using Self-Timed Rings

Abdelkarim Cherkaoui[1,2], Viktor Fischer[1], Laurent Fesquet[2], and Alain Aubert[1]

[1] Hubert Curien Laboratory, UMR CNRS 5516, Saint-Etienne, France
[2] TIMA Laboratory, UMR CRNS 5159, Grenoble, France

Abstract. Self-Timed Rings (STR) are oscillating structures derived from asynchronous design techniques. Contrary to Inverter Ring Oscillators (IRO), several events can evolve simultaneously in a STR: a handshake request and acknowledge protocol prevents them from colliding. The major feature of STRs is their ability to auto-regulate timings between the events, allowing a very precise control of the relative phase in each ring stage. In addition, recent studies revealed that STRs provide a high quality random jitter suitable for TRNG applications. In this talk, we present a novel TRNG principle using Self-Timed Rings and a probabilistic model for computing bias and entropy boudaries at the TRNG output. The proposed design provides high quality, provably random bit sequences passing NIST SP 800-22 and FIPS 140-1 statistical tests with a high throughput (10 MBps).

Keywords: Self-Timed Rings, Entropy, TRNG, Applied Cryptography