Random Number Generators and Physical Unclonable Functions

David Lubicz

Organized by:
DGA, CEA, Institut Fourier, Hubert Curien Laboratory, IETR, TIMA, Creach Labs

Introduction

Random Number Generators (RNGs) and Physical Unclonable Functions (PUFs) are crucial components for the security of cryptographic systems. Typical usages include:

- RNG: generation of cryptographic keys (RN), initialization vectors, nonces, and masks in countermeasures against side-channel attacks;
- PUF: generation of fingerprints of electronic circuits and of the hardware-related local security key.

Design hardware-based RNGs and PUFs with a proved level of security is still a challenge.

General methodology for the RNG design

In the simple case of a RNG, one has to

- Identify (analog) random noise serving as a source of randomness, have a statistical model for it, prove that it is stable, non manipulable by an attacker;
- Make it possible to measure random noise parameters;
- Design a circuitry serving to extract randomness, which use the random noise to produce unpredictable bit sequences;
- Use a statistical model of the whole TRNG to verify the level of security of the RNG;
- Design the total failure test(s) and online test(s) to check the good operation of the device and protect it against attacks;
- Take into account certification and industrial processes.

and PUF design...

The approach for designing a PUF is even more difficult – we have to

- Quantify technological variability,
- Use error correcting codes, compute the mutual information of two random phenomenons...

The aim of this conference is to address all these challenges.

Next, we explain how the contributions fit in the whole picture.

Part 1: RNG & PUF design and evaluation guidelines

In this part, we will discuss standards and procedures aimed at the design and evaluation of TRNGs and PUFs including:

- Guidelines for designers to guarantee security and reliability of the RNG;
- Streamline evaluation and certification process.

Part 1: Contributions

Talks:

- Werner Schindler, BSI: "New AIS 20/31";
- John Kelsey, NIST: "An overview of SP 800_90";
- Florian Pebay Peyroula, CEA: "OpenTRNG: an open-source initiative for ring-oscillator based TRNGs".

Posters:

- Florian Pebay-Peyroula, CEA-Leti: "OpenTRNG: an open-source initiative for ring-oscillator based TRNGs";
- David Lubicz, DGA: "DGA's design and evaluation recommandations for RNG".

Part 2: Design and model of the physical source

This part will include:

- Identification of random phenomenon in electronic circuits;
- Identification of variation in physical microstructure;
- Design statistical models, measurements methods, security metrics.

Part 2: Contributions

Talks:

- Marco Bucci, Infineon Technologies: "Chaotic Entropy Sources";
- Onur Günlü, Linkoping University "PUF: Signal Processing and Information-theoretic Aspects";
- Maciej Skorski, Hubert Curien Laboratory, University of Warsaw: "On Jitter Transfer in Ring Oscillators and Comprehensive Modelling of 1/f Noises ";
- Florent Bernard, Hubert Curien Laboratory: "Low cost and precise jitter measurement method".

Posters:

- Maciej Skorski, Hubert Curien Laboratory, University of Warsaw: "Comprehensive Modelling of 1/f Noises ".

Part 3: RNG and PUF architectures

This part will include:

- General architecture of RNG and PUF;
- Digitizers, entropy post-processing;
- Online tests.

Part 3: Contributions

Talks:

- Nicola Massari, Bruno Kessler Institute: "SPAD-based QRNGs";
- Benjamin Malthiery, 3D-OXides: "PUF based multifunctional oxide thin films";
- Torsten Schuetze, Rohde-Schwartz: "Digitization and mathematical post-processing";
- Johannes Mittmann, BSI: "Post-processing algorithms for Markov chain models";
- Milos Grujic, KU Leven: "Advancing Secure Randomness: Challenges and Innovations in TRNG and PUF Design".

Part 3: contributions

Posters:

- Antoine Levotre, Institut Fourier: "Proposal for an enhanced autocorrelation test for random number generators";
- Licinius Benea, CEA-Leti, "TRNG research topic at CEA-leti".

Part 4: RNG and PUF implementation

This part will include:

- Implementation on a given technology, compatibility with industrial processes;
- Certification process, standards compliance;
- Attacks on RNG.

Part 4: Contributions

Talks:

- Grégoire Gimenez, Icalps: "Some pitfalls to consider when designing a TRNG";
- Lucile Quatravaux, Thales: "High-grade security TRNG";
- Kevin Layat, ID Quantique: "ID quantique's QRNG";
- Sylvain Guilley, Secure-IC: "Entropy and Reliability of the Loop-PUF";
- Raimondo Luzzi, Infineon Technologies: "A Reliable Low-area Low-power PUF-based Key Generator";
- Patrick Haddad, Rambus: "Random numbers for security applications in industrial context".

Part 4: contributions

Poster:

- Eloise Delolme, Hubert Curien Laboratory: "Beyond Total Locking: Demonstrating and Measuring Mutual Influence on a RO-Based TRNG on an FPGA".