On the security of oscillator-based random number generators

David Lubicz

Abstract

Physical random number generators (a.k.a. TRNGs) appear to be critical components of many cryptographic systems. Yet, such building blocks are still too seldom provided with a formal assessment of security, in comparison to what is achieved for conventional cryptography. In this talk, we present a comprehensive statistical study of TRNGs based on the sampling of an oscillator subject to phase noise (a.k.a. phase jitters). This classical layout, typically instantiated with a ring oscillator, provides a simple and attractive way to implement a TRNG on a chip. Our mathematical study allows one to evaluate and control the main security parameters of such a random source, including its entropy rate and the biases of certain bit patterns, provided that a small number of physical parameters of the oscillator are known. In order to evaluate these parameters in a secure way, we also provide an experimental method for filtering out the global perturbations affecting a chip and possibly visible to an attacker. Finally, from our mathematical model, we deduce specific statistical tests applicable to the bit stream of a TRNG. In particular, in the case of an insecure configuration, we show how to recover the parameters of the underlying oscillator.