On the Way to Monitor Random Number Generation

Patrick Haddad, Florent Bernard, Viktor Fischer

Abstract

The jitter present in oscillators is an analog phenomenon observable also in digital integrated circuits. This phenomenon is often used as a source of entropy in true random number random generators (TRNG).

Many works in the community showed the possibility to bias a TRNG output sequence, thereby creating significant vulnerabilities in many cryptographic systems. Therefore, it is important for security reasons to maintain every time statistical properties of the generated bitstream and its unpredictability, but also to guarantee its robustness against intentional or unintentional variations of the environment.

After the study of the intrinsic behavior of the jitter, we propose a new approach for securing TRNG design by implementation of generator-specific embedded tests. The tests are aimed at detecting harmful degradations of the entropy caused by environmental disturbances.

In this presentation, we will introduce this approach and we will present advancement of its implementation in hardware.