CONTACTLESS ELECTROMAGNETIC ACTIVE ATTACK ON RING OSCILLATOR BASED TRUE RANDOM NUMBER GENERATOR

Pierre Bayon[1], Lilian Bossuet[1], Alain Aubert[1], Viktor Fischer[1],
Francois Poucheret[2,3], Bruno Robisson[3], and Philippe Maurine[2]

[1] University of Lyon, Hubert Curien Laboratory, CNRS 5516, Saint-Etienne, France
[2] University of Montpellier 2, LIRMM Laboratory, CRNS 5506, Montpellier, France
[3] CEA-LETI, SESAM Laboratory, Centre Microelectronique de Provence, Gardanne, France

True random number generators (TRNGs) are ubiquitous in data security as one of basic cryptographic primitives. They are primarily used as generators of confidential keys, to initialize vectors, to pad values, but also as random masks generators in some side channel attacks countermeasures. As such, they must have good statistical properties, be unpredictable and robust against attacks. This paper presents a contactless and local active attack on ring oscillators (ROs) based TRNGs using electromagnetic fields. Experiments show that in a TRNG featuring fifty ROs, the impact of a local electromagnetic emanation on the ROs is so strong, that it is possible to lock them on the injected signal and thus to control the monobit bias of the TRNG output even when low power electromagnetic fields are exploited. These results confirm practically that the electromagnetic waves used for harmonic signal injection may represent a serious security threat for secure circuits that embed RO-based TRNG.