Random Number Generation: a potential target of electromagnetic emanation analysis?

Pierre Bayon, Lilian Bossuet, Alain Aubert
Laboratoire Hubert Curien, Saint-Etienne, France

Abstract

Although the random number generation in a cryptographic system is a key element of the security chain, bibliography dealing with attacks on this part is not really wide. However, among the large number of attacks targeting cyphers, the ones exploiting electromagnetic side channel (in near field) could be very effective against random number generators.
This presentation gives an insight on the first results of electromagnetic analysis performed on random number generators. The main idea is to evaluate if the tools elaborated to perform electromagnetic analysis on cyphers could be used on random number generators, too.