Offline and online testability of Random Number Generators

Marco Bucci, Raimondo Luzzi, Admir Alihodzic
Infineon Technologies AG, Austria

Abstract

In this work, the offline and online testability of Random Number Generators (RNG's) and entropy sources is discussed. It is pointed out that, despite this is commonly accepted, the evaluation method used for pseudo-RNG's is not applicable to RNG's where the focus must be on the actual entropy. It is shown that the min-entropy, which is proposed as a quality figure for entropy sources, is not really a conservative estimation of the actual entropy but, in most of the cases, just a misleading quantity which can also result in an over estimation. On the other side, it is shown that, provided that the sequence under test features a relatively short memory, the actual Shannon entropy can be straightforwardly and correctly evaluated. Surprisingly, if the digital post-processing of an RNG is properly designed, this method can be also applied after post-processing, thus assessing whether or not the RNG features (a practically) maximal entropy. Finally, feasibility, costs and robustness of online tests is compared vs the usage of redundant (i.e. multiple) entropy sources. It is shown that redundancy provides a better security coverage while, online tests, can even be exploited for mounting attacks.