Tailored RNGs for Low-Cost Devices

Werner Schindler

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185–189
53175 Bonn, Germany
Werner.Schindler@bsi.bund.de

Abstract

High-end smart cards and general purpose hardware (PC, server etc.) normally use RNGs, which allow the broadest possible range of applications. This is a very convenient feature but general purpose RNGs usually require substantial resources.

Low-cost devices usually apply resource-saving lightweight (or even ultra lightweight) cryptographic algorithms, which fit their applications. Consequently, it seems to be natural to tailor the RNG to the particular low-cost device and its application(s), too

In this talk we consider physical RNGs and deterministic RNGs. Depending on the application protection mechanisms against active or passive implementation attacks might be saved. For low output rates resource-saving designs of physical RNGs may exist. It seems to be difficult, however, to scale any requirements, which concern the entropy, or to facilitate the corresponding parts of the security evaluation adequately. Depending on the application one might consider saving the online test but this bears the risk of unnoticed use of weak random numbers. In the second part of the talk we consider deterministic RNGs. For deterministic RNGs both the security requirements and the security level of the algorithmic part can be adjusted to particular applications in a natural way.

The talk presents basic generic considerations but not elaborate results. The presentation may serve as a basis for discussions.