Chair of Security in Information Technology
TUM Department of Electrical and Computer Engineering
Technical University of Munich

Seminar

How to Build a TRNG Model

High quality true random number generators are crucial for the security of many cryptographic protocols. The BMBF provides in the AIS 31 quality criteria for the certification of TRNGs. In this context it is required to provide a model the TRNG.
For this seminar topic, the methodology for building a statistical TRNG model that fulfills the requirements of the AIS 31 should be summarized and examples for such a model building should be provided. The student might start research with the references below.

References:

- https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_31_Fun
- W. Killmann and W. Schindler; A Design for A Physical RNG with Robust Entropy Estimators; CHES 2008

Contact

Request Topic

Advisors

Michael Pehl