Update of the AIS 20 / 31

Matthias Peter, **Werner Schindler**
Bundesamt für Sicherheit in der Informationstechnik (BSI)
Bonn, Germany

April 28, 2021

AIS 20 and AIS 31

Matthias Peter, Werner Schindler
Bundesamt für Sicherheit in der Informations-technik (BSI)

- The AIS 20 and AIS 31
  - are evaluation guidelines for RNGs that are used in cryptographic applications.
  - have been effective in the German certification scheme (Common Criteria) since 1999, resp. since 2001.
  - refer to a joint mathematical-technical reference
    - often itself briefly denoted as AIS 20, AIS 31, or AIS 20/31 (depending on the context)
- The latest version of the mathematical-technical reference has been effective since 2011.

AIS 20 and AIS 31

Matthias Peter, Werner Schindler
Bundesamt für Sicherheit in der Informationstechnik (BSI)

- The mathematical-technical reference AIS 20/31 is currently being updated.
- BSI and NIST have aimed to harmonize AIS20/31 and SP 800-90[A,B,C].
- BSI and NIST have had several meetings with fruitful discussions on that topic.

Classification of RNGs

Matthias Peter, Werner Schindler
Bundesamt für Sicherheit in der Informationstechnik (BSI)

- **DRNGs** deterministic RNGs
  - a.k.a. pseudorandom number generators
  - (pure and hybrid) DRNGs
- **PTRNGs** physical (true) RNGs
  - the noise source (a.k.a. entropy source; notation is not unique) consists of dedicated hardware or exploits physical experiments
  - usually run on smart cards
- **NPTRNGs** non-physical true RNGs
  - noise source: no dedicated hardware
  - typically, entropy is gained from system data (timing values, RAM data, etc.) or user's interaction (mouse movement, key strokes, etc.)
  - usually run on PCs, servers, etc.

Functionality classes

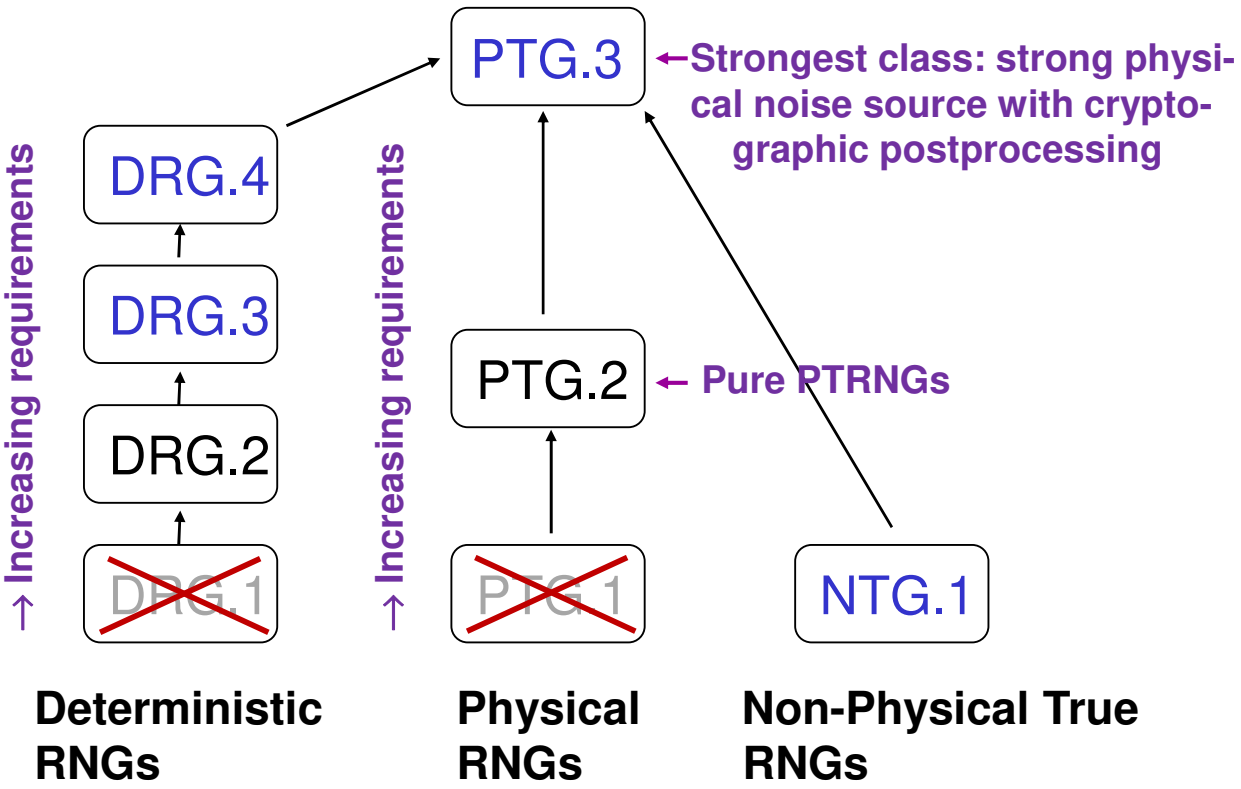
Matthias Peter, Werner Schindler
Bundesamt für Sicherheit in der Informationstechnik (BSI)

- The AIS 20 and the AIS 31 are technically neutral. They do not specify approved designs.
- Instead, functionality classes are defined.
- The applicant for a certificate (usually the developer) and an accredited evaluation lab have to give evidence that the RNG meets the class-specific requirements.

New AIS 20 / 31 — Functionality classes

Update of the AIS 20 / 31

Matthias Peter, Werner Schindler
Bundesamt für Sicherheit in der Informationstechnik (BSI)



DRNG: functionality classes

Matthias Peter, Werner Schindler
Bundesamt für Sicherheit in der Informationstechnik (BSI)

- Three functionality classes with increasing security requirements exist.
- Roughly speaking, the classes ensure
  - DRG.2: backward secrecy and forward secrecy
  - DRG.3: + enhanced backward secrecy
  - DRG.4: + enhanced forward secrecy

Updated AIS 20: 90A-compliant designs

Matthias Peter, Werner Schindler
Bundesamt für Sicherheit in der Informationstechnik (BSI)

- In the updated AIS 20 the definitions of the functionality classes are modified (requests are introduced).
  - The 90A-approved designs will be compliant to AIS 20 (to DRG.3 or DRG.4) if a suitable TRNG is used for seeding / reseeding, and for high-entropy input.
  - The mathematical-technical reference will contain conformity proofs of the approved designs (algorithmic requirements).
  - Sufficient conditions for seeding / reseeding (DRG.3) and for the generation of high-entropy additional input (DRG.4) are specified.
  - An applicant for a certificate (usually the developer) may refer to these proofs.

PTRNG: Functionality class PTG.2

Matthias Peter, Werner Schindler
Bundesamt für Sicherheit in der Informationstechnik (BSI)

- 'pure' PTRNG
- usually applies mathematical postprocessing (e.g. XOR), 'no postprocessing' and cryptographic postprocessing are allowed
- Recommended applications:
  - DRNGs: seeding, reseeding, (high-entropy) additional input
  - PTRNGs: 'core' of a PTG.3-compliant PTRNG
  - random numbers should not be used 'directly' to generate cryptographic keys etc.

PTRNG: Functionality class PTG.3

Matthias Peter, Werner Schindler
Bundesamt für Sicherheit in der Informationstechnik (BSI)

- Physical RNG with cryptographic postprocessing
  - cryptographic postprocessing algorithm with memory
  - If the postprocessing algorithm runs autonomously it can viewed as a DRG.3-compliant DRNG.
- Typical design: Random numbers from a PTG.2-compliant PTRNG are the input of the postprocessing algorithm
  - The evaluation can be split into two independent steps:
    - PTG.2-compliance
    - (possibly at a later date): PTG.3-compliance (does not require the knowledge of details of the PTG.2-compliant PTRNG)

Stochastic model

Matthias Peter, Werner Schindler
Bundesamt für Sicherheit in der Informations-technik (BSI)

- The evaluation of physical RNGs (PTG.2, PTG.3) must be based on a stochastic model.
- The stochastic model specifies a class of distributions in which the true distribution of the raw random numbers is contained.
- The raw random numbers shall be stationary distributed.
- (PTG.2) The impact of the postprocessing algorithm (if existent) on the entropy has to be considered.
- (PTG.2) With the stochastic model a lower entropy bound per random bit shall be verified.

Stochastic model (II)

Matthias
Peter, Werner
Schindler
Bundesamt
für Sicherheit
in der
Informations-
technik
(BSI)

- The stochastic model shall be tailored to the noise source.
  - The applicant has to give evidence that the stochastic model is appropriate. Usually, this is supported by engineering or physical arguments, by findings from the literature, by test data etc.

Online test and total failure test

Matthias Peter, Werner Schindler
Bundesamt für Sicherheit in der Informationstechnik (BSI)

- The online test shall detect non-tolerable weaknesses sufficiently soon.
  - The online test shall be tailored to the stochastic model.
- The total failure test shall detect total failures of the noise source very fast.
  - The output of weak random numbers (worst case: entropy 0!) must be prevented.
  - justification shall be supported by engineering arguments (failure analysis)

Evaluation of PTG.2 + PTG.3: Central objectives

Matthias
Peter, Werner
Schindler
Bundesamt
für Sicherheit
in der
Informations-
technik
(BSI)

- verification and analysis of the stochastic model
- verification that the online test and the total failure test are effective

PTG.3

Matthias Peter, Werner Schindler
Bundesamt für Sicherheit in der Informations-technik (BSI)

- Data compression rate of the cryptographic postprocessing algorithm:
  - today: compression rate ≥ 1 (the certificate does not mention the compression rate)
  - update: still data compression rate ≥ 1 but data compression rate > 1 shall explicitly be mentioned in the certificate

NPTRNGs

Matthias Peter, Werner Schindler
Bundesamt für Sicherheit in der Informationstechnik (BSI)

- Main differences to PTRNGs
  - non-physical noise sources (no dedicated hardware)
  - designer / evaluator cannot control the environment where the NPTRNG is operated (typically run on PCs, servers, etc.)
  - does not allow precise stochastic modelling
  - has to be compensated by conservative entropy estimates and a large compression rate
    - goal: derive a trustworthy lower entropy bound under conservative assumptions on the entropy source and the abilities of potential attackers
    - BSI has initiated a permanent study on Linux /dev/random several years ago (see BSI website, conducted by atsec information security GmbH (Stefan Müller))

New AIS 20 / 31

Matthias Peter, Werner Schindler
Bundesamt für Sicherheit in der Informationstechnik (BSI)

1. Introduction
2. AIS 20 and AIS 31 — scope, limits, RNG classes, concepts [informative]
3. Functionality classes
4. Mathematical Background
   [mainly informative, provides info for Chaps. 3 and 5]
5. Examples
   [mainly informative, discusses examples and explains how to verify the class requirements]
6. Glossary

   Appendix [informative] with cross-glossary to the terminology of SP 800-90[A,B,C]

Update of the AIS 20 and AIS 31

Matthias Peter, Werner Schindler
Bundesamt für Sicherheit in der Informationstechnik (BSI)

- A draft of the mathematical-technical reference AIS 20/31 will be published in the third quarter 2021.
- Comments will be appreciated!

Contact

Bundesamt für Sicherheit in der Informationstechnik (BSI),
Bonn, Germany

Werner Schindler

P.O. Box 200363, 53133 Bonn, Germany
Tel.: +49 (0)228-9582-5652

Werner.Schindler@bsi.bund.de
https://www.bsi.bund.de