The new AIS 20/31

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

European Cyber Week 2024 —
Génération d'aléa

Rennes

November 20, 2024

Outline

- Introduction and motivation
- New AIS 20/31: Overview and key features
- Harmonization with NIST
- Physical RNGs
  - Stochastic model
  - Functionality classes PTG.2 and PTG.3
  - Post-processing algorithms
- Takeaways

Random numbers in cryptography

- Many cryptographic applications need random numbers.
- Weak random number generators (RNGs) can decisively weaken strong cryptographic mechanisms.

Common Criteria (CC)

- provide evaluation criteria for IT products, which shall permit the comparability between independent security evaluations.
- A product or a system that has successfully been evaluated is awarded with an internationally recognised IT security certificate (up to particular assurance levels).
- The Common Criteria and the corresponding evaluation manuals do not specify evaluation criteria for random number generators.

AIS 20 and AIS 31

- The AIS 20 and AIS 31
  - are evaluation guidelines for RNGs for cryptographic applications.
  - have been effective in the German certification scheme (Common Criteria) since 1999, resp. since 2001.
  - are umbrella documents that refer to a joint mathematical-technical reference
    - for short usually also called AIS 20, AIS 31, or AIS 20/31 (depending on the context).
    - We follow this convention.
  - AIS 20/31 was first revised in 2011.

Mathematical-technical reference (AIS 20/31)

- The mathematical-technical reference AIS 20/31 was in an update process lasting several years.
  Authors: Matthias Peter, Werner Schindler

- In September 2024 a new version of AIS 20/31 has been published.
  - available at:
  `https://www.bsi.bund.de/dok/ais-20-31-appx-2024`

Harmonization with NIST

- BSI and NIST have been in an ongoing process of harmonizing AIS 20/31 and SP 800-90[A,B,C].
- In the last years, BSI and NIST have given several joint presentations at international conferences.
- New Joint BSI/NIST publication:
  NIST IR 8446 — Bridging the Gap between Standards on Random Number Generation: Comparison of SP 800-90 Series and AIS 20/31
  - compares the requirements of NIST and BSI
  - shall help vendors to comply with both standards in the same design
  - available at:
    `https://csrc.nist.gov/pubs/ir/8446/ipd`

John Kelsey: Overview of SP 800–90
13:30 – 14:25

'Natural' requirements

- Random numbers should assume all admissible values with equal probability.
- The assumed values should be independent from predecessors and successors.

- This characterizes an *ideal RNG*.
- Unfortunately, ideal RNGs do not exist in the real world!

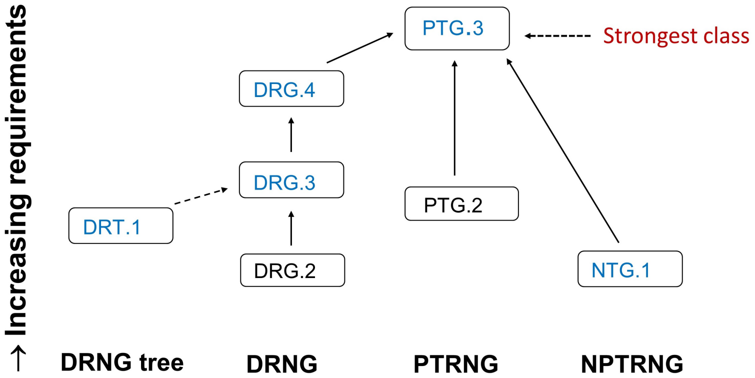
Classification of RNGs

- **DRNGs** deterministic RNGs
  - the random numbers depend on
    - the seed,
    - possibly: + on reseeding, + additional input
- **PTRNGs** physical true RNGs (short: physical RNGs)
  - physical noise source
    - exploits physical phenomena from dedicated hardware designs or from physical experiments
- **NPTRNGs** non-physical true RNGs
  - non-physical noise source
    - no dedicated hardware design
    - typically, exploits system data (timing values, RAM data, etc.) or user's interaction (mouse movement etc.)

AIS 20/31: Central features

- The AIS 20 and the AIS 31 are technology neutral.
- The AIS 20 and the AIS 31 do not specify approved designs.
- Instead, functionality classes are defined.
  - Security requirements are specified that RNGs shall fulfil in order to comply.
  - 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.

AIS 20/31 — Hierarchy of the functionality classes



DRT.1: DRNG trees

- important for software implementations.
  Example: Linux /dev/random, OpenSSL
- The initial randomness source provides the entropy for the whole DRNG tree.

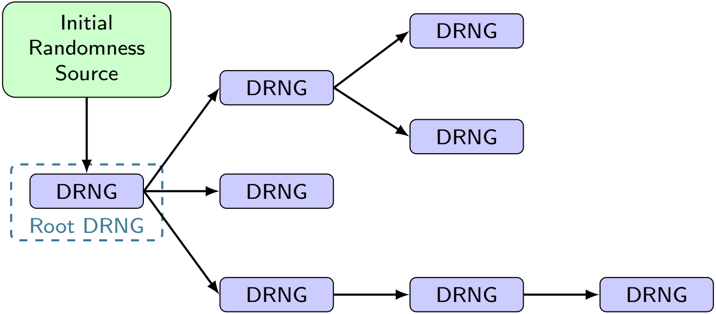


Abbildung: Example of a DRNG tree

DRNGs

- AIS 20/31 – harmonization with SP 800-90 series
  - notion of requests introduced to allow the standard-compliant use of SP 800-90 A approved designs.
  - contains conformity proofs for Hash_DRBG and HMAC_DRBG with the algorithmic requirements of functionality class DRG.3 (does not mean that the CTR_DRBG with AES-256 is not algorithmically compliant with DRG.3)
  - Class DRT.1 and RBGC constructions are very similar.
- effective internal state $\geq$ 248 bits,
  min-entropy (effective internal state) $\geq$ 240 bits
  (alternative Shannon entropy condition permitted)
  ($\rightarrow$ multi-target attacks, Grover's algorithm).

Stochastic model

- Passing blackbox test suites does not confirm that a PTRNG (physical RNG) is good!!!
- The stochastic model is the 'core' of each PTRNG evaluation (PTG.2, PTG.3).
- Random numbers are interpreted as realizations of random variables.
- Aim: Verification of a lower entropy bound per *internal random bit* (= output bit).

Stochastic model (II)

- A stochastic model provides a partial mathematical description (of the relevant properties) of a (physical) noise source using random variables. It allows the verification of a (lower) entropy bound for the output data during the lifetime of the physical RNG, even if the quality of the digitized data goes down.
- Ideally, a stochastic model consists of a family of probability distributions that contains the true distribution of the raw random numbers during the lifetime of the physical RNG.
- However, it may suffice to model parts of the entropy contributions if it can be shown that the neglected effects do not decrease the entropy.

Stochastic model (III)

- (AIS 31) The raw random numbers shall be (time-locally) stationarily distributed.
  - Slow drifts of the parameters are permitted as long as the entropy remains sufficiently large.

Stochastic model (IV): Toy example in a nutshell

- A coin is tossed N times; '1' $\cong$ 'head' and '0' $\cong$ 'tail'
  - outcome: $x_1, \ldots, x_N \in \{0, 1\}$
- $x_1, \ldots, x_N \cong$ realizations of random variables $X_1, \ldots, X_N$.
  - Coins have no memory.
  - $\Longrightarrow X_1, \ldots, X_N$ may be assumed to be independent and identically $B(1, p)$-distributed (Bernoulli distribution)
  - parameter $p := \mathrm{Prob}(X_j = 1)$ is unknown
- Stochastic model: $X_1, \ldots, X_N$ are independent and identically $B(1, p)$-distributed with $p \in [0, 1]$.
  - The stochastic model fits to other coins, too, and would tolerate drifts of p for the same coin in the course of time.
  - Estimate p on the basis of $x_1, \ldots, x_n$
  - Substitute its estimate $\tilde{p}$ into the (1-dimensional) entropy formula.

Stochastic model (V)

- The applicant has to give evidence that the stochastic model fits to the physical noise source (includes digitization).
  - The stochastic model shall be based on the understanding of the noise source.
  - The argumentation should be supported by engineering or physical arguments, by findings from the literature, by tests on empirical data etc.

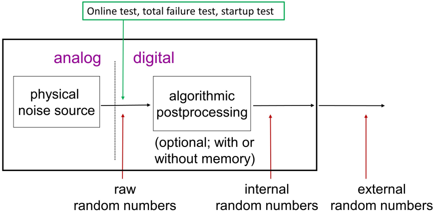
Stochastic model (VI)

- The AIS 20/31 discusses in detail several exemplary stochastic models of real-world physical noise sources.
    - PTRNG exploiting two noisy diodes
    - Analysis of two generic types of designs that exploit events whose intermediate times can be modelled by a renewal process.
    - Radioactive decay with non-ideal Geiger counter
    - PLL-based PTRNG
- These analyses shall support the developer and the lab in their tasks.

Online test and total failure test

- 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 must be prevented.
  - The justification shall be supported by engineering arguments (failure analysis).
- Online tests and total failure tests are treated in detail in AIS 20/31.

PTRNG: Functionality class PTG.2

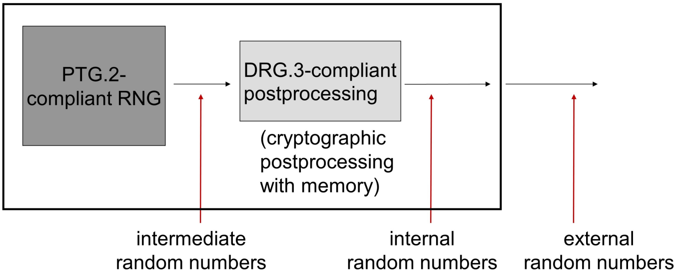


- 'Pure' PTRNG
  - algorithmic post-processing (e.g., XOR)
  - 'no post-processing', universal families of hash functions, and cryptographic post-processing are also permitted
- Entropy (one or both claims are possible [selection])
  - Shannon entropy / output bit ≥ 0.9998.
  - Min-entropy / output bit ≥ 0.98.
- Effective online test and total failure test, startup test

PTRNG: Functionality class PTG.3

- Physical RNG with
  - strong, well-understood physical noise source
  - effective online test and total failure test, startup test
  - cryptographic post-processing with memory (DRG.3-compliant, if run autononously)

PTG.3: typical design



- The evaluation can be split into two separate steps:
  - PTG.2-compliance of the 'inner' PTRNG
  - PTG.3-compliance of the entire RNG
    (possibly at a later date, with another applicant)
- Different companies can be involved in these evaluations.

PTG.3: entropy claims

- The applicant (developer) can apply for Shannon entropy, for min-entropy, or for both [selection].
- Maximum min-entropy claim per output bit: $1 - 2^{-32}$ (= 'full entropy' (SP 800-90))

> - At most 0.9998 bit Shannon entropy / 0.98 bit min-entropy can be claimed on the basis of the stochastic model.
> - Higher entropy claims require data compression.
> - Important special cases are discussed in AIS 20/31.

Post-processing algorithms

- Post-processing algorithms are applied to raw random numbers (PTG.2) or intermediate random numbers (PTG.3).
- Post-processing algorithm is bijective $\Longrightarrow$ (average) entropy / bit remains unchanged
- Only data compression can increase the entropy per bit.
- Task: Verify a lower bound for the entropy per output bit.

Algorithmic post-processing algorithms

- Example: XOR, modular addition, LFSR
- The analysis must consider the stochastic model of the raw random numbers.

> Johannes Mittmann:
> Post-processing algorithms for Markov chain models
> Thursday, 15:05 – 15:45

Cryptographic post-processing algorithms

- Example: Hash functions, HMAC, (cryptographic reseeding algorithm + output function)
- Usually, the exact impact of the cryptographic post-processing algorithm cannot be determined exactly.
- Instead, cryptographic post-processing algorithms can often be modelled by random mappings or the composition of random mappings.
- Usually, only the (min-)entropy of the input data is relevant but not the whole stochastic model.
- AIS 20/31 provides formulae and many illustrating examples.

Example

- 'typical' PTG.3-design:
  PTG.2-compliant PTRNG (with min-entropy claim, i.e. ≥ 0.98 bit of min-entropy per bit) $+$
  DRG.3-compliant post-processing
- The intermediate random numbers (PTG.2 output) and the internal state of the postprocessing algorithm are input into SHA-256 (can be modelled by a random mapping)
- ≥ 327 intermediate random bits $\rightarrow$
  256 output bits with min-entropy / output bit $\geq 1 - 2^{-32}$.

QRNGs

- QRNGs are treated as physical RNGs.
- Hence, functionality class PTG.2 or, if a suitable cryptographic post-processing algorithm with memory is applied, functionality class PTG.3 applies.

Impact of AIS 31 (I)

- Over the years, the AIS 31 has influenced the design of physical RNGs.
- AIS 31 has had significant influence on scientific research.
  - Many scientific papers and PhD theses studied physical RNGs and their conformance to the AIS 31 by analyzing stochastic models.
- ISO/IEC 20543: The evaluation of a physical RNGs must be based on a stochastic model.
- The NIST document SP 800-90 B requires that the entropy of noise sources is justified (a stochastic model is optional). With the next revision of SP 800-90 B NIST intends to demand stochastic models for the evaluation of physical RNGs.

Impact of AIS 31 (II)

- The AIS 31 has also been applied in the French certification scheme.
- Certificates that confirm the PTG.2-conformance have mutually been recognized between the BSI and ANSSI since 2015.

AIS 20/31

- The AIS 20/31 contains many informative parts that illustrate the class requirements.
- The document is about 300 pages long.
- **But you do NOT have to study everything to be able to use it.**
- Instead, depending on the RNG, the targeted functionality class, and on previous knowledge, applicants for a certificate (usually, the developers) and evaluation labs can select and concentrate on parts.

Takeaway

- AIS 20/31 is technology neutral and allows a lot of freedom. The applicant for a certificate and the evaluation lab have to give evidence that all requirements of the claimed functionality class are fulfilled.
- It is not necessary to study the whole document to use it.

Contact

Bundesamt für Sicherheit in der Informationstechnik (BSI),
Godesberger Allee 87,
53175 Bonn, Germany

Werner Schindler
Tel.: +49 (0)228-9582-5652

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