Security Evaluation of RNGs – The Updated Evaluation Guidelines AIS 20 and AIS 31

Werner Schindler

Federal Office for Information Security (BSI),
Bonn, Germany

Marcoux, June 21, 2012

Outline

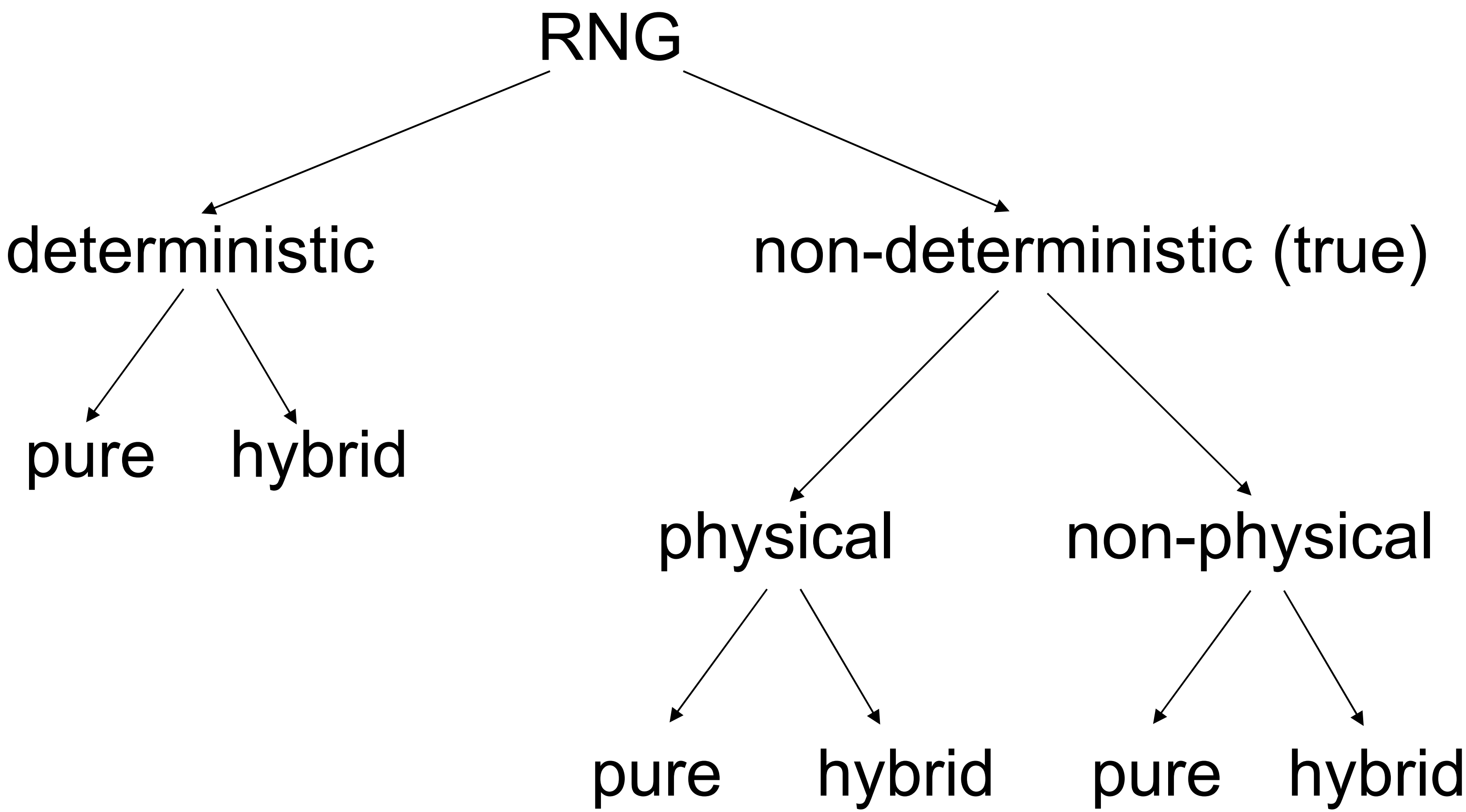
- Introduction and motivation
- Goals of a security evaluation
- Stochastic model
- New AIS 20 and AIS 31

Ideal RNGs

- Even with maximum knowhow, most powerful technical equipment and unlimited computational power an attacker has no better strategy than “blind” guessing (brute force attack).
- Guessing n random bits costs 2^{n-1} trials in average.
- The guess work remains invariant in the course of the time.
- An ideal RNG is a mathematical construct.

Federal Office for Information Security

Classification of ‘real-world’ RNGs



Abbreviations

- **DRNG**: Deterministic Random Number Generator
- **PTRNG**: Physical Random Number Generator
- **NPTRNG**: Non-Physical Non-Deterministic Random Number Generator (Example: /dev/random (Linux))

Security Requirements (I)

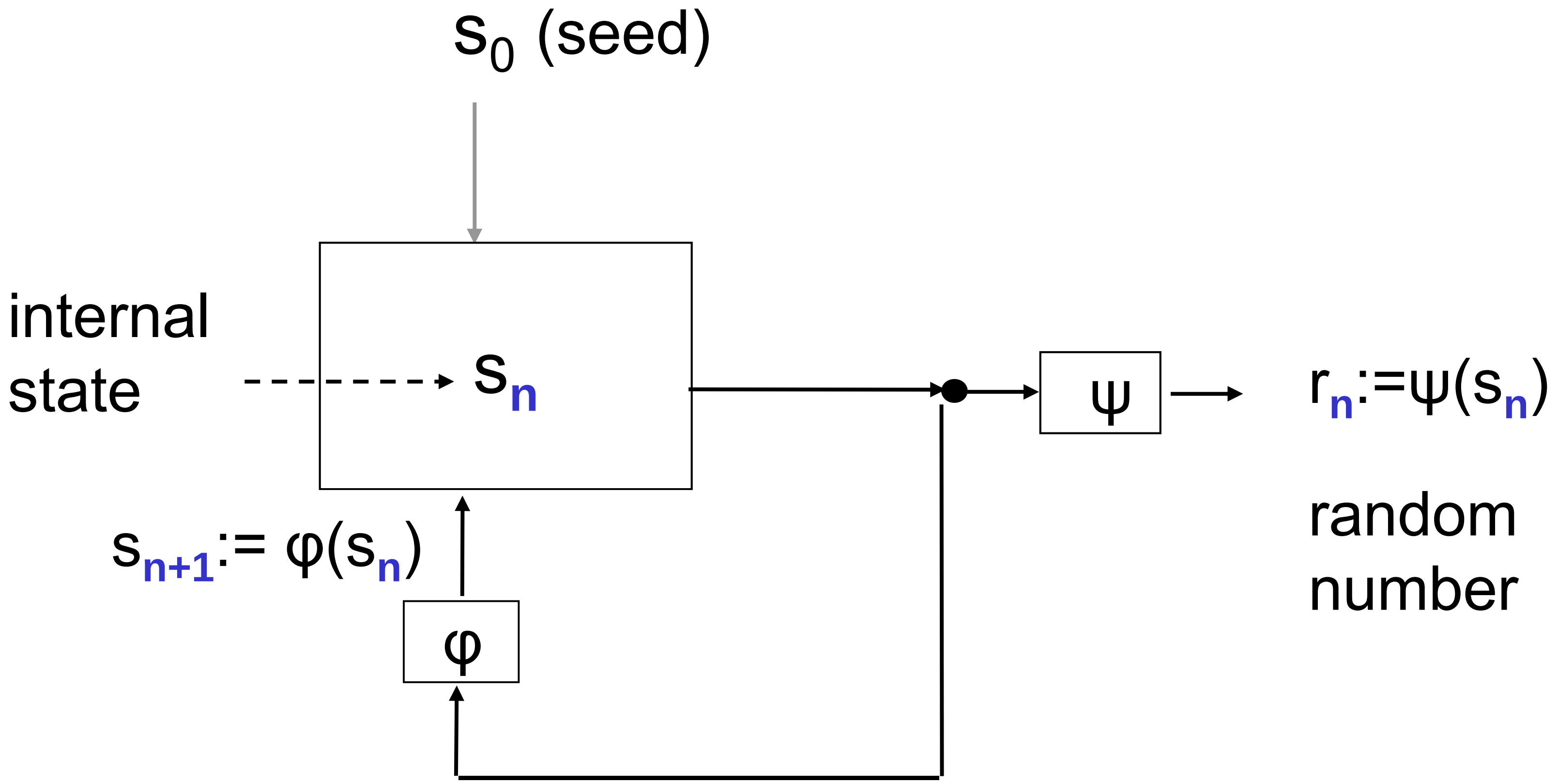
- **R1**: The random numbers should not show any statistical weaknesses.
- **R2**: The knowledge of sub-sequences of random numbers shall not allow to *practically* compute predecessors or successors or to guess them with non-negligibly larger probability than without knowledge of these sub-sequences. (backward secrecy and forward secrecy)

Security Requirements (II)

- **R3**: It shall not be *practically feasible* to compute preceding random numbers from the internal state or to guess them with non-negligibly larger probability than without knowledge of the internal state. (enhanced backward secrecy)
- **R4**: It shall not be *practically feasible* to compute future random numbers from the internal state or to guess them with non-negligibly larger probability than without knowledge of the internal state. (enhanced forward secrecy)

<ins>NOTE</ins>: R3 and R4 are DRNG-typical requirements.

Pure DRNG (schematic design)



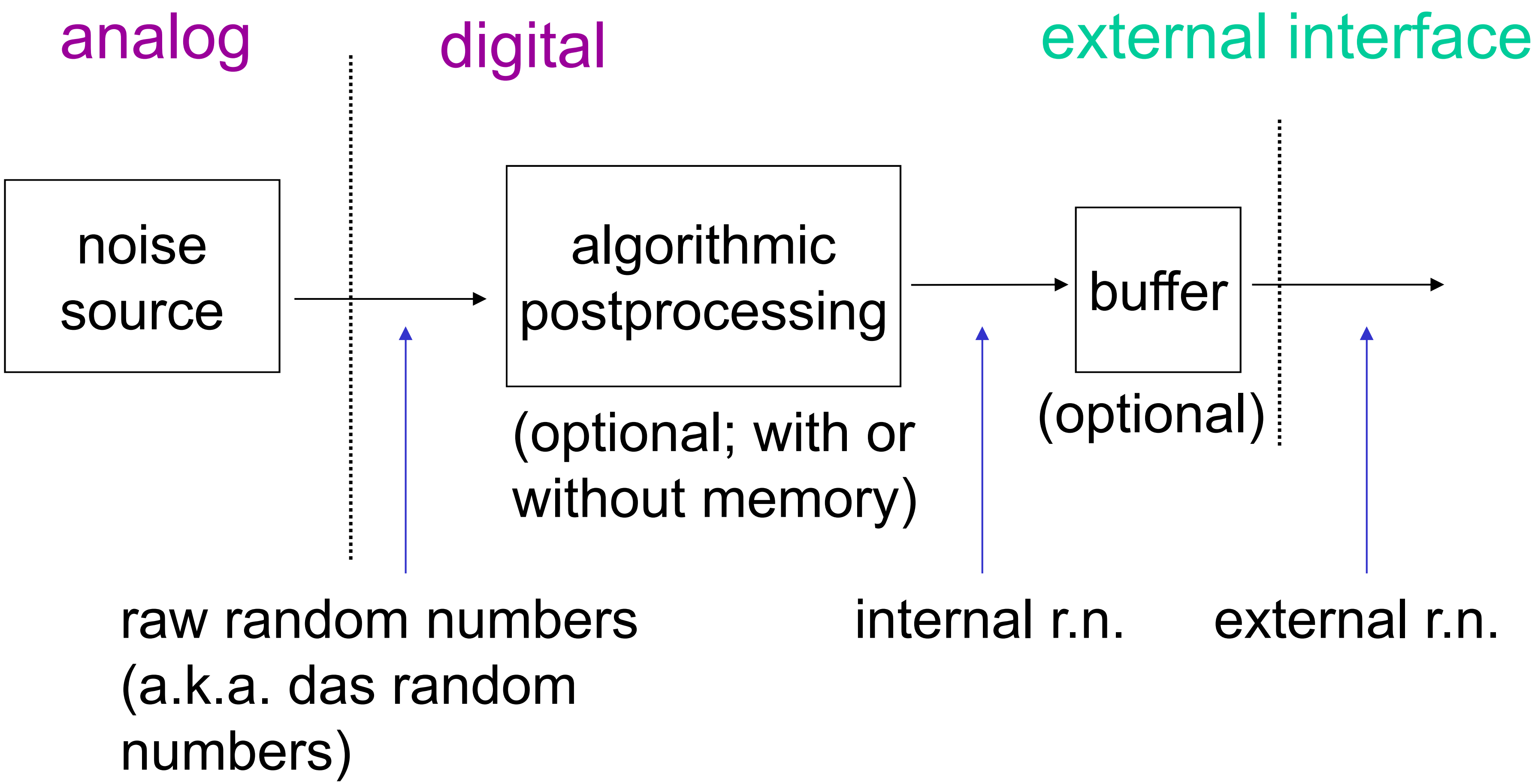
φ : state transition function

ψ : output function

Security aspects

- DRNGs can only provide computational security, which might get lost in the course of the time.
- The state transition function and the output function are usually composed of cryptographic primitives.
- The security of a DRNG grounds on the cryptographic properties of its primitives.

Physical RNG (schematic design)



Evaluation of the PTRNG design

- Goal: Estimate the entropy per internal random bit
- Note: Entropy is a property of random variables and not of the values that are assumed by these random variables (here: random numbers).
- In particular, entropy cannot be measured as temperature, voltage etc.
- General entropy estimators do not exist.

Stochastic model (I)

- Ideally, a stochastic model specifies a family of probability distributions that contains the true distribution of the internal random numbers.
- At least, the stochastic model should specify a family of distributions that contain the distribution
  - of the raw random numbers or
  - of ‚auxiliary' random variables

  if this allows to estimate the increase of entropy per internal random number.
- The specified family of probability distributions may depend on one or on several parameters.

Example 1: Coin tossing (I)

- **PTRNG:** A single coin is tossed repeatedly.
  "Head" (H) is interpreted as 1, "tail" (T) as 0.
- **Stochastic model:**
  - The observed sequence of random numbers (here: heads and tails) are interpreted as values that are assumed by random variables $X_1,X_2,\ldots$.
  - The random variables $X_1,X_2,\ldots$ *are assumed to be independent and identically distributed.* (Justification: Coins have no memory.)
  - $p := \mathrm{Prob}(X_j = H) \in [0,1]$ with unknown parameter p

Example 1: Coin tossing (II)

Entropy estimation (based on the stochastic model)

- Observe a sample $x_1, x_2, \ldots, x_N$
  Set $\tilde{p} := \#\{j \leq N \mid x_j = H\} / N$
- To obtain an estimate $\tilde{H}(X_1)$ for $H(X_1)$
  substitute p into the entropy formula:
  $\tilde{H}(X_1) = - (\tilde{p} * \log_2 (\tilde{p}) + (1-\tilde{p}) * \log_2(1-\tilde{p}))$

Stochastic model (II)

- For physical RNGs the justification of the stochastic model is usually more difficult and requires more sophisticated arguments. Ideally, it should be confirmed by experiments.
- The parameter(s) are estimated first, and out of it an entropy estimate is computed (cf. Example 1).

PTRNG in operation: Security measures

	goal
tot-test	shall detect a total breakdown of the noise source (almost) immediately; r.n.'s, which have been generated after that instant, shall not be output
startup test	shall ensure the functionality of the physical RNG when it is started
online test	shall detect non-tolerable weaknesses of the random numbers sufficiently soon

Security evaluation

A trustworthy security evaluation should verify the suitability of

- the RNG design
- the online test, the tot test and the startup test.

Common Criteria (CC)

- provide evaluation criteria for IT products which shall permit the comparability between independent security evaluations.
- A product or system that has successfully been evaluated is awarded with an internationally recognized IT security certificate.
- The Common Criteria and the corresponding evaluation manuals *do not* specify evaluation criteria for random number generators.

AIS 20 and AIS 31 (I)

In the German evaluation and certification scheme the evaluation guidance documents

AIS 20: Functionality Classes and Evaluation Methodology for Deterministic Random Number Generators
AIS 31: Functionality Classes and Evaluation Methodology for Physical Random Number Generators

have been effective for more than 10 years.

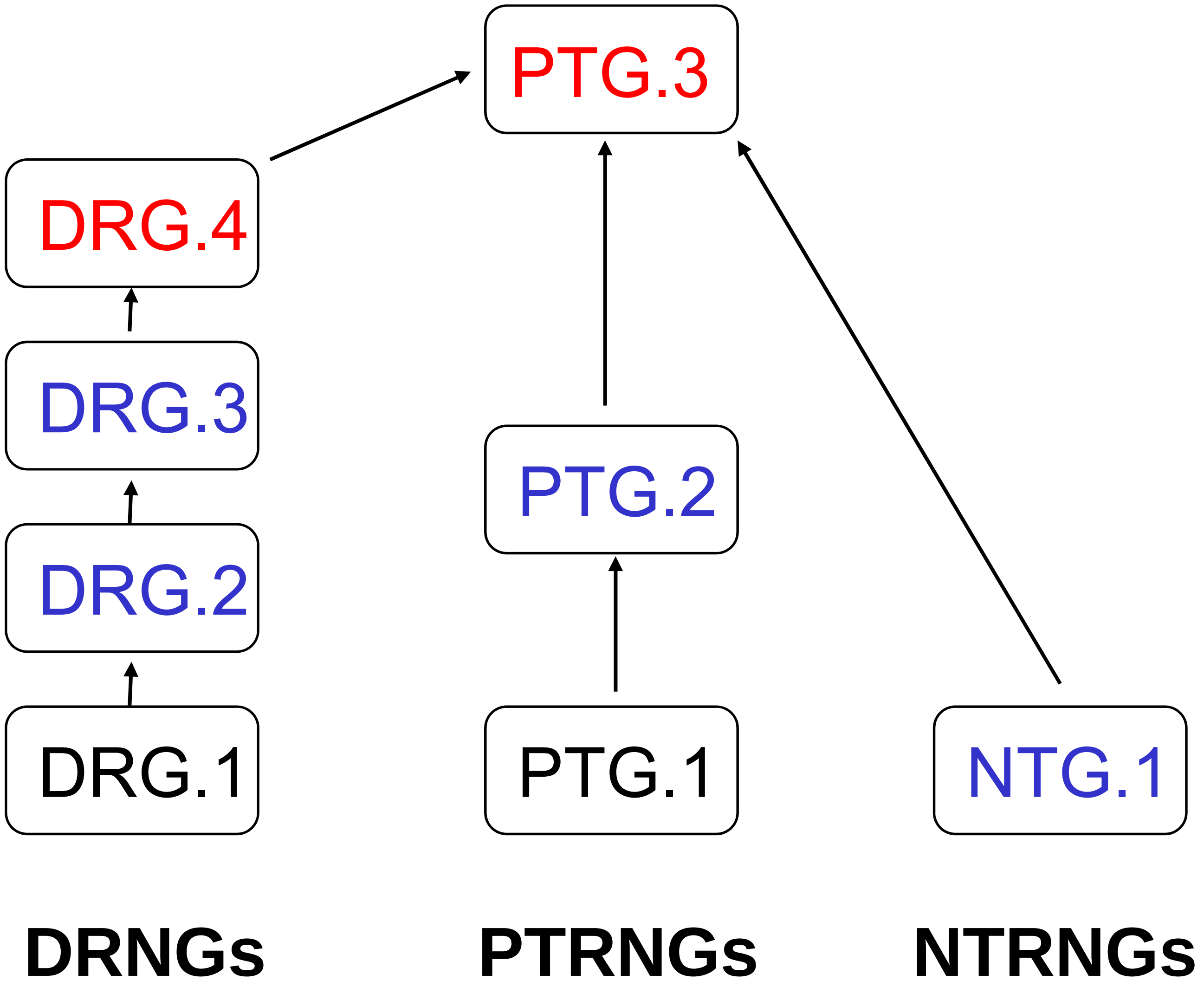
AIS 20 and AIS 31 (II)

- AIS 20 and AIS 31 are technically neutral. They define several functionality classes of RNGs.
- The applicant for a certificate has to give evidence that the RNG meets the specified requirements.
- The AIS 20 and AIS 31 have been well-tried in many product evaluations.
- A reference implementation of the applied statistical tests can be found on the BSI website.

AIS 20 and AIS 31 (III)

- In 2011 the mathematical-technical references of AIS 20 and AIS 31 have been updated.
- Some new functionality classes have been introduced.
- The mathematical background is explained, and several examples are discussed.

Functionality classes



AIS 20 and AIS 31:
Old and New (a coarse comparison)

New functionality classes	Old functionality classes
DRG.1	K2 + forward secrecy
DRG.2	K3
DRG.3	K4
DRG.4	no pendant
PTG.1	P1
PTG.2	P2
PTG.3	no pendant
NTG.1	no pendant

New AIS 20 + AIS 31 (DRNGs)

Functionality class DRG.2

- Goals: good statistical properties, backward secrecy, forward secrecy

Generic Requirements (simplified)

- large seed entropy
- cryptographic state transition function and output function

New AIS 20 + AIS 31 (DRNGs)

Functionality class DRG.3

- Goals: good statistical properties, backward secrecy, forward secrecy, enhanced backward secrecy

Generic Requirements (simplified)

- large seed entropy
- cryptographic state transition function and output function
- The state transition function is one-way

DRG.2 vs. DRG.3 (I)

- The functionality class DRG.3 ensures the secrecy of old random numbers even if the internal state has been compromised.
- This is an additional security measure, which relevant if the DRNG is operated in a potentially insecure environment.
- DRG.3 demands a one-way state transition function, which may be costly (e.g., for smart cards)

DRG.2 vs. DRG.3 (II)

- If
  - the previous random numbers need not be protected (zero-knowledge proofs, openly transmitted challenges etc.),
  - the device is operated in a secure environment, or
  - if one trusts unconditionally in the security of the device ($\rightarrow$ protection of the internal state)

it might be an option to use a DRG.2-conformant DRNG .

New AIS 20 + AIS 31 (DRNGs)

Functionality class DRG.4

- Goals: good statistical properties, backward secrecy, forward secrecy, enhanced forward secrecy, enhanced forward secrecy

Generic Requirements (simplified)

- large seed entropy
- cryptographic state transition function and output function
- The state transition function is one-way
- supply of fresh entropy (regularly, upon request, …)

DRG.3 and DRG.4

- Compared to DRG.3 the class DRG.4 provides an additional security anchor.

New AIS 20 + AIS 31 (PTRNGs)

Functionality class PTG.2

- Goals: good statistical properties, entropy per internal random number is sufficiently large
- Generic Requirements (simplified):
  - internal random numbers pass statistical tests
  - stochastic model of the noise source
  - effective online tests

New AIS 20 + AIS 31: PTRNGs

Functionality class PTG.3

- Goals: good statistical properties, entropy per internal random number is sufficiently large, computational security even after a total breakdown of the noise source
- Generic Requirements (simplified):
  - internal random numbers pass statistical tests
  - stochastic model of the noise source
  - effective online tests
  - cryptographic postprocessing with memory (DRG.3-conformance with cryptographic output function)

PTG.2

- The internal random numbers may have a small entropy defect (bias, correlation).
- For many applications this should not play a role: symmetric session keys, challenges etc.
- For certain applications an attacker might (at least theoretically) be able to combine information on several random numbers (e.g., for ephemeral keys for DSA or ECDSA), preventing at least information-theoretical security statements.
- Even if no concrete attacks are known it seems to be recommendable to use PTG.3-conformant RNGs (at least) for those applications.

PTG.3

- PTG.3-conformant RNGs provide two security anchors (unlike PTG.2- RNGs or DRG.3-RNGs).
- The cryptographic postprocessing algorithm ensures computational security even after a total breakdown of the noise source (provided that the noise source has worked for at least some period).
- PTG.3 is the highest functionality class. PTG.3-conformant RNGs are appropriate for all cryptographic applications.

DRG.4 and PTG.3

- Unlike PTG.3 the class DRG.4 allows to ‘extend’ entropy.
- (PTG.3) One may expect that the combination of an analog part and the cryptographic postprocessing algorithm provides stronger resistance against side-channel attacks and fault attacks than purely physical or purely deterministic RNGs.

New AIS 20 + AIS 31: NPTRNGs

Functionality class NTG.1

- Goal: good statistical properties, entropy per internal random number is sufficiently large
- Generic Requirements (simplified) :
  - internal random numbers pass statistical tests
  - reliable entropy estimator for the raw bit strings
  - postprocesing algorithm with memory, one-way property

Contact

Federal Office for Information Security (BSI)

Werner Schindler
Godesberger Allee 185-189
53175 Bonn, Germany

Tel: +49 (0)228-9582-5652
Fax: +49 (0)228-10-9582-5652

Werner.Schindler@bsi.bund.de
www.bsi.bund.de
www.bsi-fuer-buerger.de