Evaluation Criteria for True (Physical) Random Number Generators Used in Cryptographic Applications

Werner Schindler[1], Wolfgang Killmann[2]

[1] Bundesamt für Sicherheit in der Informationstechnik (BSI)

Bonn, Germany

[2] T-Systems ISS GmbH

Bonn, Germany

Random numbers in cryptographic applications

Examples:

- random session keys
- RSA prime factors
- random numbers for DSS
- zero-knowledge-proofs
- challenge-response-protocols
- IV vectors
- ...

Random number generators

- **t**rue (physical) **r**andom **n**umber **g**enerators (**TRNG**s)

- **d**eterministic **r**andom **n**umber **g**enerators (**DRNG**s)
  (output completely determined by the seed)

- hybrid generators (refreshing their seed regularly;
  e.g. by exploiting user‘s interaction, mouse move-
  ment, key strokes or register values)

Requirements on random numbers

The requirements on the used random numbers depend essentially on the intended application!

R1: The random numbers should have good statistical properties

R2: The knowledge of subsequences of random numbers shall not enable to compute pre-decessors or successors or to guess them with non-negligible probability.

TRNGs vs. DRNGs

For sensitive applications requirement R2 is indispensable!

DRNGs rely on computational complexity („practical security“)

TRNGs: If the entropy per random number is sufficiently large this ensures theoretical security.

Objectives of a TRNG evaluation (I):

Verification of the general suitability

of the TRNG-design

at hand of

theoretical considerations and

carefully investigated prototypes

TRNGs in operation: General problems and risks

- total breakdown of the noise source
- aging effects
- tolerances of components

tot-test / startup test / online test

test	aim
tot-test	shall detect a total breakdown of the noise source very soon
startup test	shall ensure the functionality of the TRNG at the start
online test	shall detect non-tolerable weaknesses or deterioration of the quality of random numbers

Objectives of a TRNG evaluation (II):

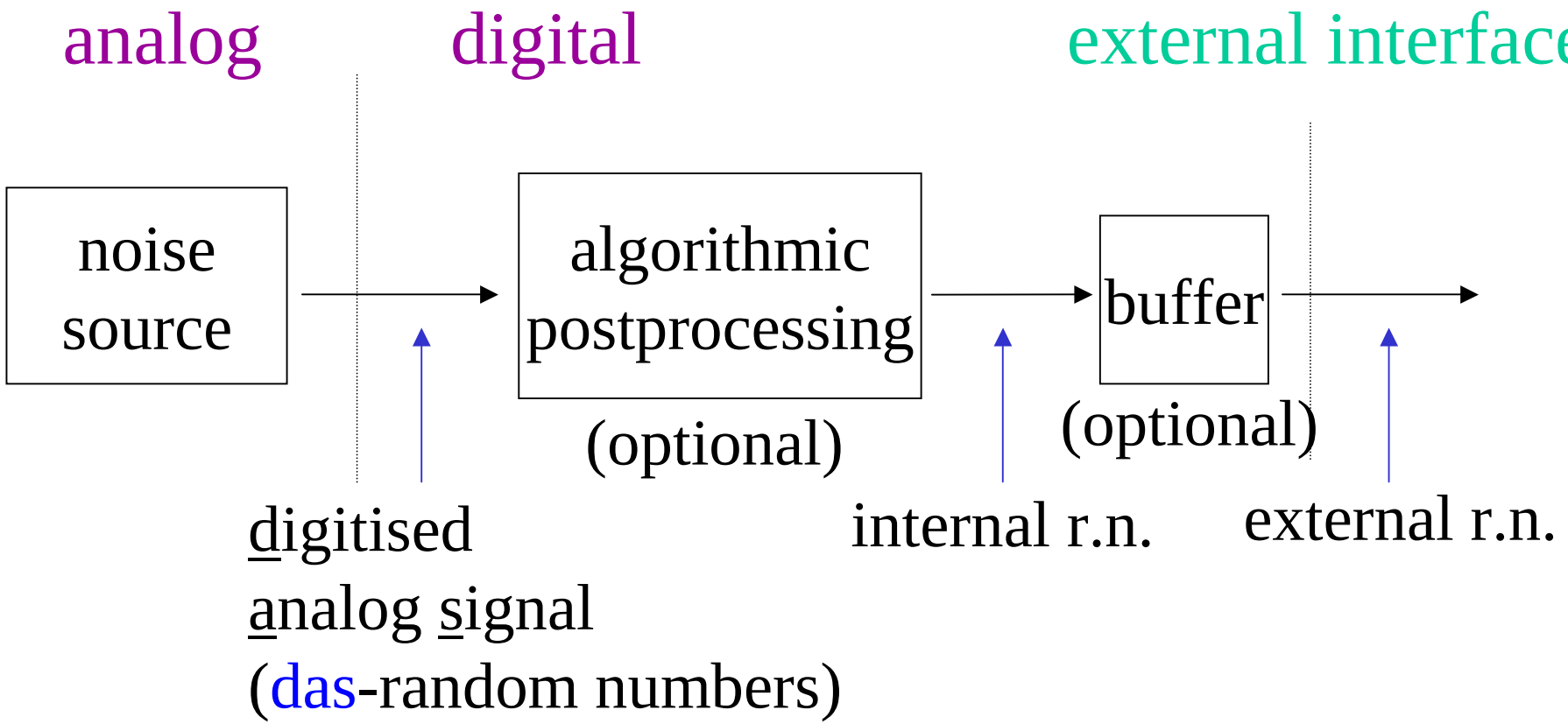
Verification of the suitability

of the tot-, startup- and online test

at hand of

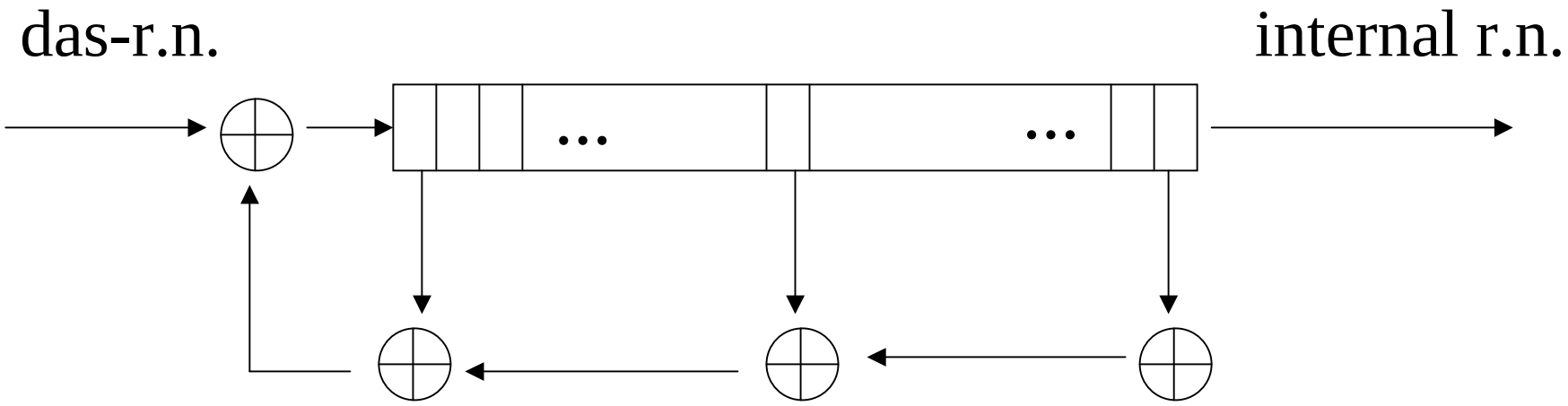
theoretical considerations

TRNG (schematic design)



Which random numbers should be tested? (I)

Example: linear feedback shift register



worst case scenario:

total breakdown of the noise sorce

→ das-r.n.s : constant, i.e. entropy /bit = 0 ... **but** ...

internal r.n.s: good statistical properties!!!

Which random numbers should be tested? (II)

Example (continued):

Statistical blackbox tests applied on the internal random numbers will **not** detect a total breakdown of the noise source (unless the linear complexity profile is tested).

The relevant property is the increase of entropy per random bit.

Entropy (I)

General demand (-> R2):

- **Entropy / random bit** should be sufficiently large

Fundamental problems:

- **Entropy is a property of random variables but not of observed random numbers!**
- „general“ entropy estimators do not exist

Consequences:

- Entropy cannot be measured as voltage etc.
- at least the distribution class of the underlying random variables has to be known

Entropy (II)

---

das-random numbers:

- may not be equidistributed
- may be dependent on predecessors
- but there should not be complicated algebraic long-term dependencies (-> math. model of the noise source)

Conclusion:

The das-random numbers should be tested.

ITSEC and CC

ITSEC (Information Technology Security Evaluation Criteria) and
CC (Common Criteria)

- provide evaluation criteria which **shall permit the comparability between independent security evaluations**.
- A product or system which has been successfully evaluated is awarded with an **internationally recognized IT security certificate.**

CC: Evaluation of Random Number Generators

ITSEC, CC and the corresponding evaluation manuals do not specify any uniform evaluation criteria for random number generators!

In the German evaluation and certification scheme the evaluation guidance document

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

has been effective since September 2001

AIS 31 (I)

- provides clear evaluation criteria for TRNGs
- distinguishes between two functionality classes

  P1 (for **less sensitive applications** as challenge-response mechanisms)

  P2 (for **sensitive applications** as key generation)

- no statistical blackbox tests for class P2
- discusses positive and negative examples

AIS 31 (II)

- does not favour or exclude any reasonable TRNG design; if necessary, the applicant has **give and to justify alternative criteria**

- mathematical-technical reference:
  W. Schindler, W. Killmann: A Proposal for: Functionality Classes and Evaluation Methodology for True (Physical) Random Number Generators

www.bsi.bund.de/zertifiz/zert/interpr/trngk31.pdf

AIS 31: Alternative Criteria (I)

P2-specific requirement P2.d)(vii):

Digitised noise signal sequences meet particular criteria or pass statistical tests intended to rule out features such as multi-step dependencies ...
... Tests and evaluation rules are specified in sub-section P2.i)

Aim of this requirement:

to guarantee a minimum entropy limit for the das-random numbers and, consequently, for the internal random numbers.

AIS 31: Alternative Criteria (II)

Case A): The das-random numbers do not meet these criteria. Using an appropriate (data-compressing) mathematical postprocessing the entropy of the internal r.n.s may yet be sufficiently large.

The applicant **has to give clear proof** that the entropy of the internal random numbers is sufficiently large, taking into account the mathematical postprocessing on basis of the empirical properties of the digitized noise signal sequence.

AIS 31: Alternative Criteria (III)

Case B): Due to construction of the TRNG there is no access to the das-random numbers possible.

The applicant **additionally has to give a comprehensible and plausible description** of a mathematical model of the noise source and of the das random numbers (specifying a distribution class!).

AIS 31: Reference Implementation

The AIS 31 has been well-tried in a number of product evaluations

A **reference implementation** of the applied statistical tests will be put on the BSI website in September

www.bsi.bund.de/zertifiz/zert/interpr/ais_cc.htm

Proposals and ideas

for improvement of the AIS 31

are always welcome!