Bundesamt
für Sicherheit in der
Informationstechnik

Use of Stochastic Models in RBG Standards

Johannes Mittmann

Bundesamt für Sicherheit in der Informationstechnik (BSI), Germany

NIST Random Bit Generation Workshop 2023

What is a stochastic model?

Stochastic model in a nutshell

A stochastic model

- provides a mathematical description of a noise source using random variables,
- allows the verification of an entropy lower bound for the output data,
- is based on and justified by the understanding of the noise source.

Physical vs. non-physical noise sources

Physical noise sources

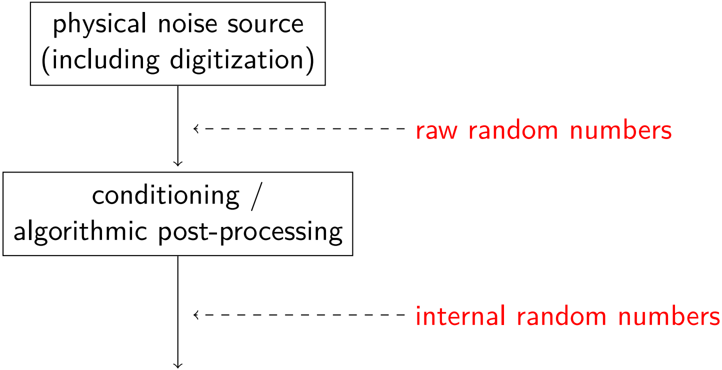
- exploit physical phenomena or physical experiments,
- use dedicated hardware designs.

Non-physical noise sources

- exploit system data or user interaction,
- use general-purpose hardware,
- may run in a variety of operational environments.

→ Stochastic models are only feasible for physical noise sources in general.

Entropy source schematic



Bundesamt
für Sicherheit in der
Informationstechnik

Mathematical definition

- Random numbers are interpreted as realizations of random variables.
- A stochastic model consists of a family of probability distributions that contains the true distribution of the raw random numbers (ideal case).
- This family of distributions usually has 1 to 3 parameters.

- The raw random numbers shall be (time-locally) stationarily distributed.

Stochastic model validation

The stochastic model of a noise source shall be

- substantiated using arguments from physics or electrical engineering,
- validated using empirical data and tailored statistical tests.

Entropy estimation

- The stochastic model shall be used to derive an entropy lower bound per internal random bit (depending on the parameters of the model).
- A set of good parameters for the targeted entropy bound shall be determined.
- The parameters of the noise source shall be estimated under relevant environmental conditions.

Health testing

An online test / health test shall

- detect non-tolerable entropy defects sufficiently soon,
- be tailored to the stochastic model,
- use the raw random numbers, because they contain more information than the internal random numbers.

Stochastic models in RBG standards

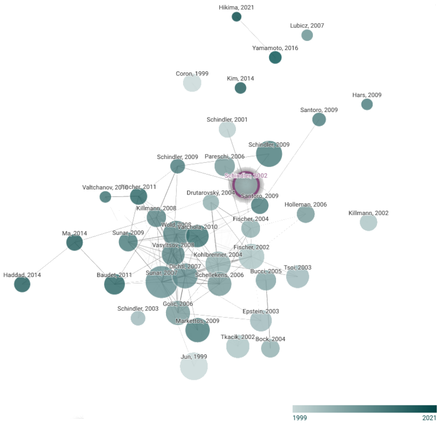
- AIS 20/31: Stochastic model mandatory for certification of physical noise sources in the German Common Criteria scheme since 2001 (functionality classes PTG.2, DRG.4, and PTG.3).
- ISO/IEC 20543: Stochastic model required for evaluation of physical noise sources.
- NIST SP 800-90B: Stochastic model recommended as entropy justification for physical noise sources. NIST intends to make stochastic models mandatory.

Stochastic models in the scientific literature

Stochastic models

- have become the state of the art in the analysis of physical noise sources,
- have influenced the design of physical noise sources.

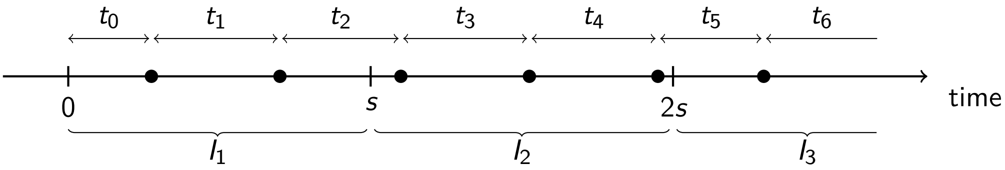
→ Stochastic model should already be considered at the design stage.



Source: `https://www.connectedpapers.com`

Example: Counting random events

Counting random events

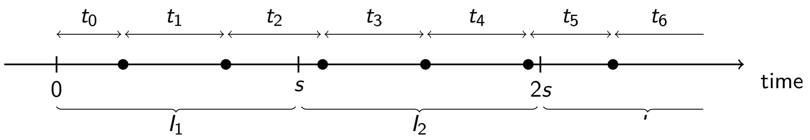


- Intermediate times between events ($\bullet$): $t_0, t_1, t_2, \ldots$
- Time intervals ($\vdash\!\!\dashv$): $I_n = \big((n-1)s, ns\big]$ with fixed length s

- Raw random numbers: $r_n = \#\big\{\text{events occuring in } I_n\big\}$
- Internal random numbers: $y_n = r_n \bmod 2$

Bundesamt
für Sicherheit in der
Informationstechnik

Example: Noisy diodes



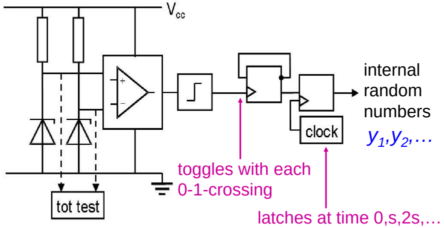


Figure: Two noisy diodes: schematic design (Killmann & Schindler, CHES 2008)

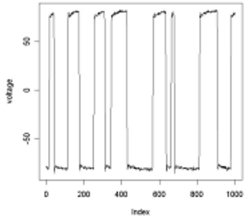


Figure: Random event: Up-crossing of amplified voltage.

Further examples of random events

- Rising edges of a ring oscillator.
- Photons emitted from an LED.
- Decays of a radioactive source.

Stochastic model (generic)

- The intermediate times $t_1, t_2, \ldots$ are interpreted as realizations of iid non-negative random variables $T_1, T_2, \ldots$
- The time intervals $I_n = ((n-1)s, ns]$ have fixed length s.
- The raw random numbers are $R_n = \#\{\text{events occuring in } I_n\}$.
- The internal random numbers are $Y_n = R_n \bmod 2$.

- This model is analyzed in AIS 20/31 draft 2022.
- If $s \gg \mathrm{E}(T_j)$, the iid-assumption can be relaxed ($\rightarrow$ noisy diodes).

- A stochastic model for a real-world physical noise source has to be substantiated and validated.

Stochastic model (normal distribution)

From now on:

- The intermediate times $T_1, T_2, \ldots$ are iid $\mathcal{N}(\mu, \sigma^2)$-distributed.
- The time intervals $I_n = ((n-1)s, ns]$ have fixed length $s \gg \mu$.
- The raw random numbers are $R_n = \#\{\text{events occuring in } I_n\}$.
- The internal random numbers are $Y_n = R_n \bmod 2$.

- The parameters of this model can be taken as

$$\frac{s}{\mu} \qquad \text{(expected number of events in } I_n\text{)}$$

$$\frac{\sigma}{\mu} \qquad \text{(coefficient of variation of } T_j\text{)}$$

Statistical properties of the raw random numbers

- The raw random numbers $R_1, R_2, \dots$ are stationary.
- Their mean is

$$E(R_n) = \frac{s}{\mu}\,.$$

- Their variance can be (well) approximated as

$$\mathrm{Var}(R_n) \approx \left(\frac{\sigma}{\mu}\right)^2 \frac{s}{\mu} + \frac{1}{6} + \frac{1}{2}\left(\frac{\sigma}{\mu}\right)^4 .$$

- Their covariances can be (well) approximated as

$$\mathrm{Cov}(R_n, R_{n+1}) \approx -\frac{1}{12} - \frac{1}{4}\left(\frac{\sigma}{\mu}\right)^4$$

and $\mathrm{Cov}(R_n, R_{n+k}) \approx 0$ for $k \geq 2$.

Entropy of the internal random numbers

- We require an entropy lower bound for the internal random numbers $Y_1, Y_2, \dots$
- We consider the (worst-case) conditional min-entropy

$$\mathrm{H}_\infty(Y_n \mid Y_{n-1}) = -\log_2 \max_{y_n, y_{n-1} \in \{0,1\}} \Pr(Y_n = y_n \mid Y_{n-1} = y_{n-1}) .$$

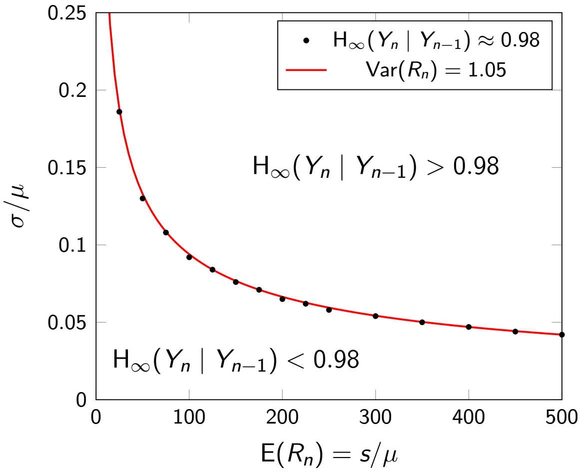
- We want to find parameters for which $\mathrm{H}_\infty(Y_n \mid Y_{n-1}) \geq 0.98$.

Entropy estimation by simulation

The cond. min-entropy $H_\infty(Y_n \mid Y_{n-1})$

- increases with s/μ (more events per time interval),
- increases with σ/μ (more variation per event),
- is determined by $\mathrm{Var}(R_n)$.

$\rightarrow$ Online test / health test should be based on $\mathrm{Var}(R_n)$.



Bundesamt für Sicherheit in der Informationstechnik

Wrap-up

Summary

Stochastic models

- help to understand physical noise sources,
- enable to derive entropy lower bounds,
- enable effective and lean health tests,
- are mandatory in German CC certifications according to AIS 31 since 2001,
- are recommended as justification of entropy estimates in SP 800-90B validations,
- should be considered already at the design stage.

Thank you for your attention!

Questions?

Contact:

- https://www.bsi.bund.de/dok/randomnumbergenerators
- ais-20-31@bsi.bund.de
- johannes.mittmann@bsi.bund.de