SP 800-90B Entropy Source Validation Workshop

Tim Hall (NIST)

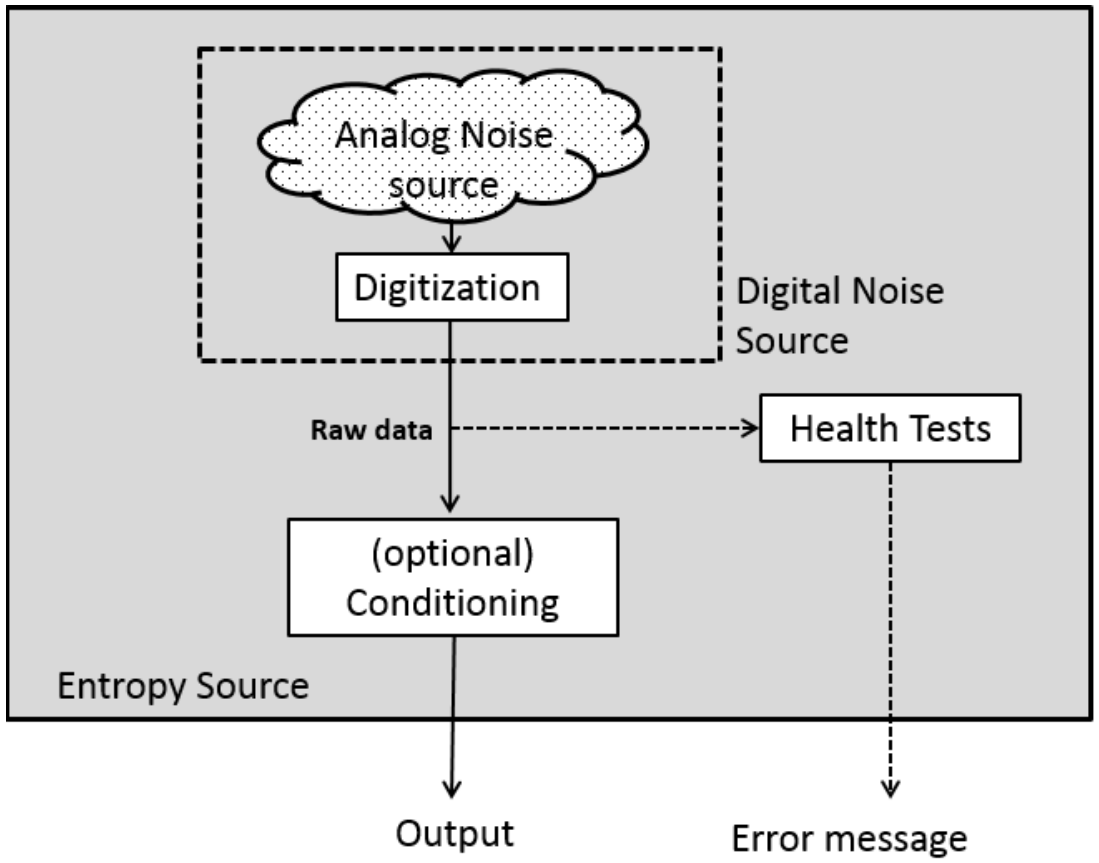
27 April 2021

Why this workshop?

NIST SP 800-90B

"*Recommendation for the Entropy Sources Used for Random Bit Generation*" published January 2018

Figure 1 (right) shows the entropy source model



SP 800-90B: *min-entropy* of output samples

Support claim with a statistical estimate

- estimators run on collected raw noise bits

Sec. 6 *Estimating Min-Entropy*:

> "This section describes generic estimation methods that will be used to test the noise source and also the conditioning component, when non-vetted conditioning components are used. It should be noted that the entropy estimation methods described in this section rely on some statistical assumptions that may not hold for all types of noise sources."

SP 800-90B: *min-entropy* of output samples

…***and*** justification of how noise source produces claimed entropy

(heuristic or mathematical model of noise source)

Sec 3.2.2 *Requirements on the noise source*:

> "Documentation **shall** provide an explicit statement of the expected entropy provided by the noise source outputs and provide a technical argument for why the noise source can support that entropy rate. To support this, documentation **may** include a stochastic model of the noise source outputs, and an entropy estimation based on this stochastic model **may** be included."

Transition to NIST SP 800-90B

Until November of 2020, there was another option:

> "There was no NIST standard for entropy estimation prior to January 2018. When entropy estimation is required (according to an applicable scenario of IG 7.14), testers have used the ***rather loose guidelines of IG 7.15*** to review the properties of an entropy source and to estimate the amount of generated entropy.
>
> Since the amount of the generated entropy is the most critical component of an estimate of the overall security of the module's cryptographic operations, it is **necessary to transition to full compliance with the SP 800-90B standard**."
>
> [excerpt from FIPS 140-2 IG 7.18]

Transition to NIST SP 800-90B

07 November 2020*: All entropy sources in a cryptographic module submitted for validation to FIPS 140 must meet requirements of SP 800-90B.

- New requirements
- More rigor
- Just *new…*

*Always a requirement for FIPS 140-3 validation

What are we doing to support this transition?

Supporting the transition

Conducted a CMVP pre-review program (concluded)

- Accredited labs could submit partial or complete entropy reports
- One-pass review by CMVP reviewers and SMEs, comments returned to lab

Developing an Entropy Source Validation Testing System (ESVTS)

- Automated workflow for submission and management of entropy reports
  - completeness, correctness, consistency of submissions
- Validation authority runs min-entropy estimators on collected noise source outputs

Establishing a separate validation scope for entropy sources

- Decouples entropy source validation from module validation
- Validate entropy source once*, reference from many places

Supporting the transition

…and this workshop

- Bring the community together
- Authors and reviewers speak
- Hear from you

Agenda for Day 1 – Tue, 27 April 2021

Morning sessions – Day 1

10:00 am EDT [15]	Workshop Introduction *Tim Hall (NIST)*
10:15 am EDT [45]	SP 800-90 Series Update *Meltem Sonmez Turan (NIST)*
11:00 am EDT [30]	IG 7.19 and Draft IG 7.20 *Alex Calis (NIST) and Allen Roginsky (NIST)*
11:30 am EDT [30]	Data Collection *Alex Calis (NIST) and Allen Roginsky (NIST)*
12:00 pm EDT [30]	30 min break

Afternoon sessions – Day 1

12:30 pm EDT [30]	Heuristic and Mathematical Models *John Kelsey (NIST)*
1:00 pm EDT [30]	Health Tests *John Kelsey (NIST)*
1:30 pm EDT [60]	Open Q & A with Panel *Day 1 speakers, moderator: Kim Schaffer (NIST)*
2:30 pm EDT	***End Day 1***

Agenda for Day 2 – Wed, 28 April 2021

Morning sessions – Day 2

10:00 am EDT [60]	Panel – Lessons Learned from Pre-reviews *Alex Calis (NIST), Jonathan Ng Cheng Hin (CCCS), Erin McAfee (CCCS), Allen Roginsky (NIST)* *moderator: Tim Hall (NIST)*
11:00 am EDT [60]	Demo of ESV Server and Architecture *Chris Celi (NIST)*
12:00 pm EDT [30]	30 min break

Afternoon sessions – Day 2

12:30 pm EDT [30]	BSI Update *Werner Schindler (BSI)*
1:00 pm EDT [30]	iid vs non-iid sources *Allen Roginsky (NIST), Meltem Sonmez Turan (NIST)*
1:30 pm EDT [60]	Open Q & A with Panel *Day 2 speakers,* *moderator: Kim Schaffer (NIST)*
2:30 pm EDT	***End Day 2***

Agenda for Day 3 – Thu, 29 April 2021

Morning sessions – Day 3

10:00 am EDT [30]	Physical Entropy Sources *John Kelsey (NIST), Chris Celi (NIST)*
10:30 am EDT [30]	Non-Physical Entropy Sources *Tim Hall (NIST)*
11:00 am EDT [30]	Conditioning Components *Tim Hall (NIST)*
11:30 am EDT [30]	Current Process vs New Process from a Submitter Perspective *Chris Celi (NIST)*
12:00 pm EDT [30]	30 min break

Afternoon sessions – Day 3

12:30 pm EDT [30]	New Validation Scope for Entropy Sources *Brad Moore (NIST), Chris Celi (NIST)*
1:00 pm EDT [30]	Impact on CMVP Review and Certification Process *Carolyn French (CCCS)*
1:30 pm EDT [60]	Open Q & A with Panel *Day 3 speakers,* *moderator: Kim Schaffer (NIST)*
2:30 pm EDT	***End Day 3***

To get the most out of the workshop…

- Use the agenda to prepare
- Participate and ask questions
- *Clarify guidance and interpretation in writing*

let’s get started!