Entropy Sources
Importance and testing

Tim Hall, John Kelsey, Meltem Sönmez Turan

Information Security and Privacy Advisory Board Meeting, October 26, 2022

National Institute of Standards and Technology
U.S. Department of Commerce

INFORMATION TECHNOLOGY LABORATORY

Overview of the talk

Part I: Overview of NIST standards on random bit generation

Part II: Entropy estimation

Part III: Validation process

Part I : Overview of NIST Standards on Random Bit Generation

Cryptographic random number generation

Security of cryptographic primitives relies of the assumption that *bits are generated uniformly at random and are unpredictable*.

Designing random bit generators (RBGs) is challenging.

- Finding a robust randomness source and correctly extracting randomness
- Difficult to know how unpredictable the outputs are (i.e., estimating entropy)
- Difficult to statistically model the process
- Difficult to understand the effects of outside parameters and environmental conditions (e.g., humidity, temperature) on the source

Validating RBGs is challenging.

- Expert knowledge on the randomness sources
- Difficult to verify some of the claims
- Practical constraints (e.g., time)

NIST SP 800 90 Series

- Provides guidelines on how to construct RBGs that can be validated through FIPS 140.
- Aims to improve the quality of RBGs by specifying design principles, requirements.

The series consists of three parts:

- SP 800 90A – Recommendation for Random Number Generation Using Deterministic Random Bit Generators (2015)
- SP 800 90B – Recommendation for the Entropy Sources Used for Random Bit Generation (2018)
- SP 800 90C – Recommendation for Random Bit Generator (RBG) Constructions (2022, 3rd draft)

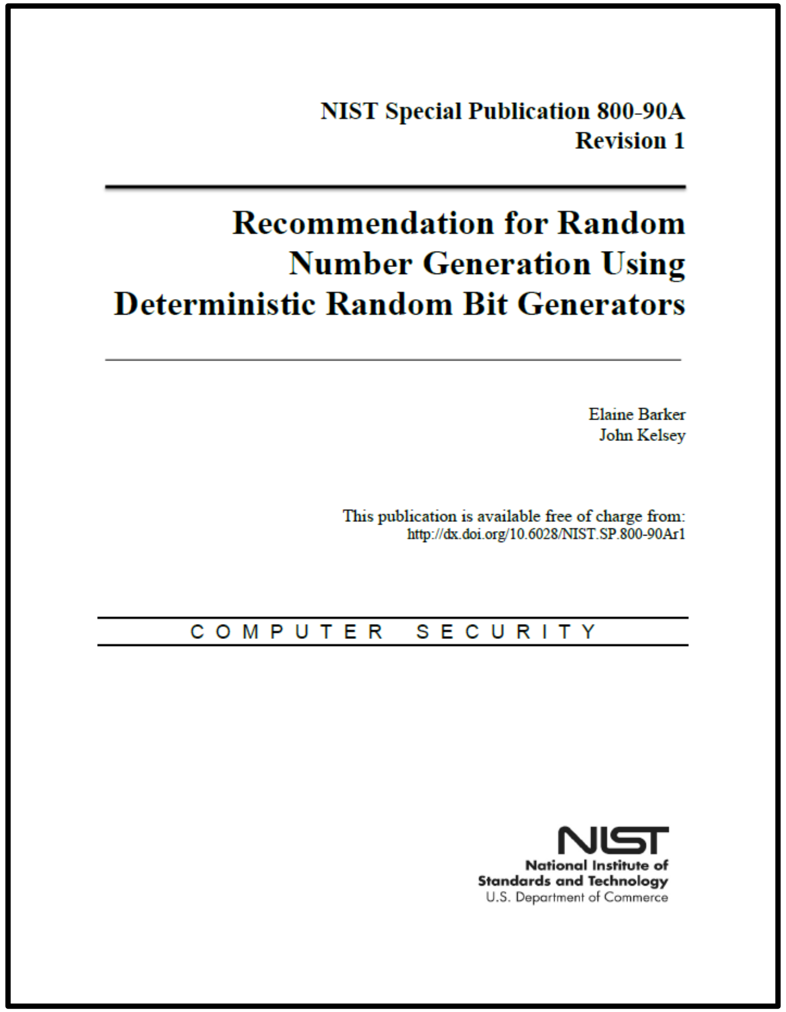
SP 800 90A (2015)

Recommendation for random number generation using Deterministic Random Bit Generators

- Specifies mechanisms for the generation of random bits using deterministic methods based on hash functions and block ciphers.

Earlier versions: January 2012 and June 2006

Next steps: NIST is working on a new revision to align with the new revision of 90C.



NIST Special Publication 800-90A
Revision 1

Recommendation for Random Number Generation Using Deterministic Random Bit Generators

Elaine Barker
John Kelsey

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-90Ar1

COMPUTER SECURITY

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

SP 800 90B (2018)

NIST

Recommendation for the Entropy Sources Used for Random Bit Generation

- Provides an entropy source definition and a model.
- Specifies design principles and requirements for entropy source components.
- Includes entropy estimation techniques.

Earlier versions: August 2012 and January 2016

Next steps: NIST is planning to revise the standard based on the lessons learned during the validation testing.

NIST Special Publication 800-90B

Recommendation for the Entropy Sources Used for Random Bit Generation

Meltem Sönmez Turan
Elaine Barker
John Kelsey
Kerry A. McKay
Mary L. Baish
Mike Boyle

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-90B

COMPUTER SECURITY

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

SP 800 90C (2022)

NIST

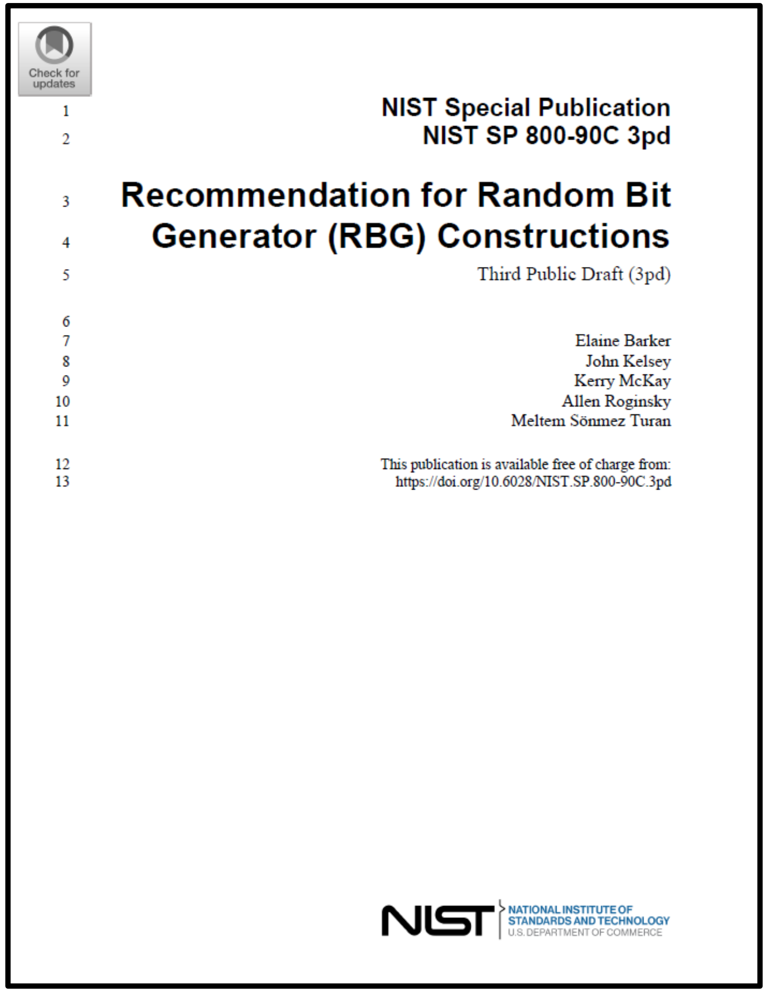
Recommendation for Random Bit Generator (RBG) Constructions

Describes three RBGs constructions:

- RBG1 provides random bits from a device that is initialized from an external RBG.
- RBG2 includes an entropy source that is available on demand.
- RBG3 includes an entropy source that is continuously accessed to provide output with full entropy.

Earlier versions: August 2012 and April 2016.

Next steps: Third draft is published in September 2022. *Public comments due*: December 7, 2022


Check for updates

NIST Special Publication
NIST SP 800-90C 3pd

Recommendation for Random Bit Generator (RBG) Constructions

Third Public Draft (3pd)

Elaine Barker
John Kelsey
Kerry McKay
Allen Roginsky
Meltem Sönmez Turan

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-90C.3pd

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

SP 800 22 (2010)

NIST

A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications

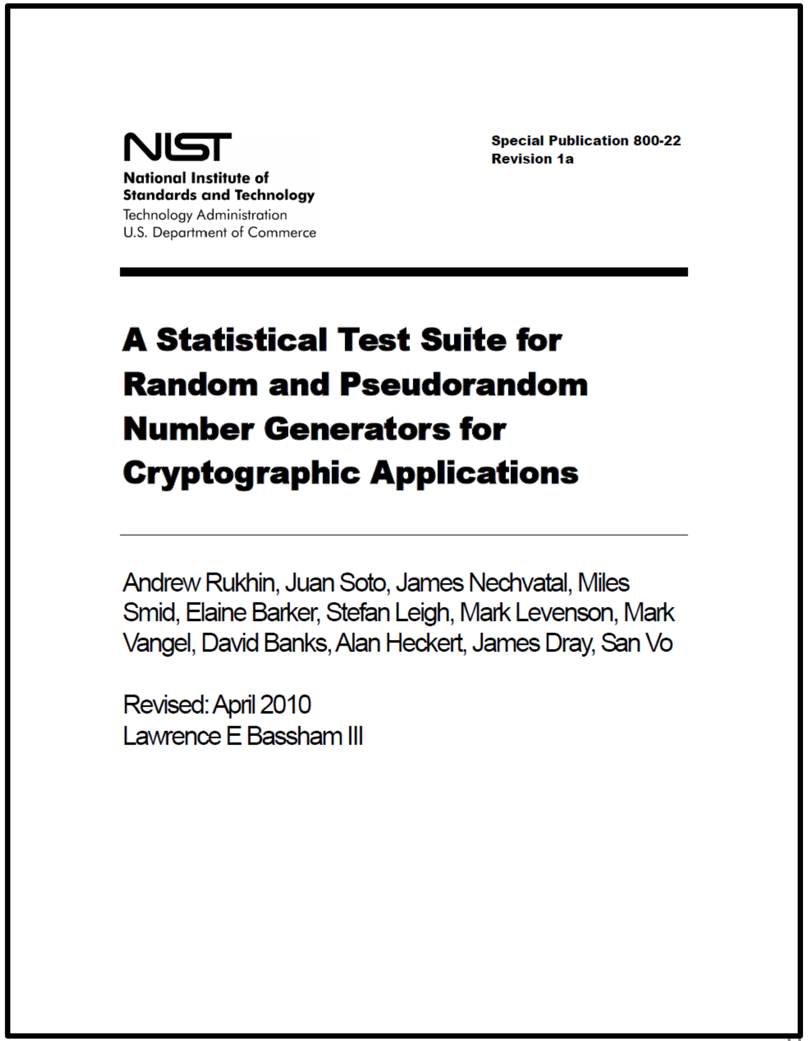
- *Specifies 15 statistical randomness tests and includes a software tool*

Earlier version: August 2008 and October 2000.

Next steps:

Crypto publication review board recently completed the review of SP 800-22 and proposed to revise the standard to align with SP 800 90 series and to make technical improvements.
NIST is working on Revision 2.

More info: https://csrc.nist.gov/projects/crypto-publication-review-project/completed-reviews



NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Special Publication 800-22
Revision 1a

A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications

Andrew Rukhin, Juan Soto, James Nechvatal, Miles Smid, Elaine Barker, Stefan Leigh, Mark Levenson, Mark Vangel, David Banks, Alan Heckert, James Dray, San Vo

Revised: April 2010
Lawrence E Bassham III

Aligning NIST and BSI standards

BSI (Germany) also has standards on random number generation:

- AIS 20: Functionality classes and evaluation methodology for deterministic random number generators
- AIS 31: Functionality classes and evaluation of physical random number generators

There are differences in the BSI’s and NIST’s validation process in terms of definitions, requirements, modeling and evaluation process.

NIST and BSI are jointly working to align the RBG standards, will publish a joint NIST-BSI report to explain the process.

Part II : Entropy Estimation

What do we mean by "entropy?"

We commonly use "entropy" to mean two things:

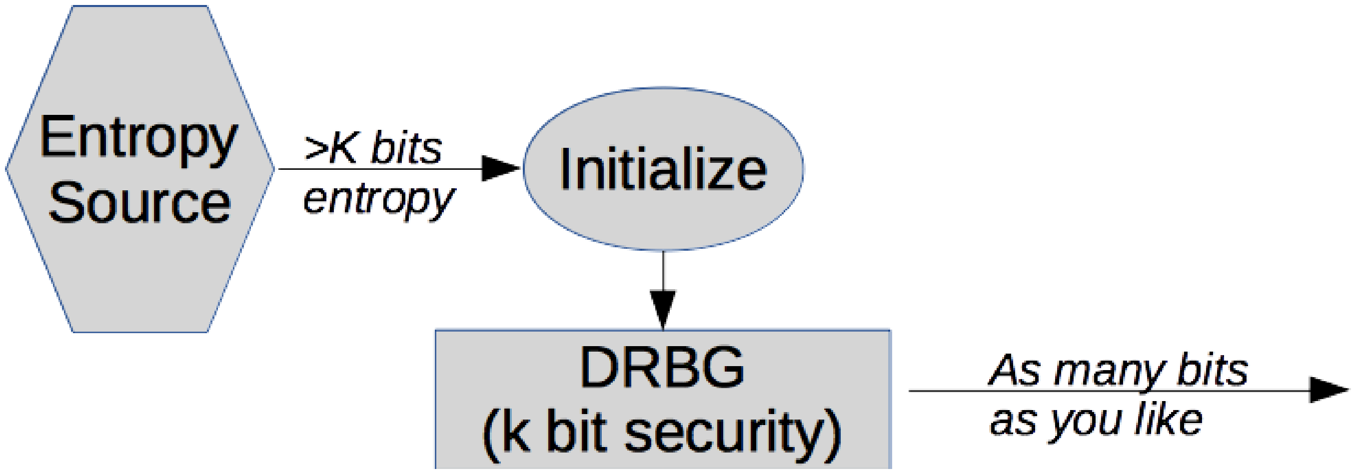
- A string of unpredictable bits
- A measure of how unpredictable the bits are

- We measure unpredictability by min-entropy
  - Consider the most powerful possible attacker trying to predict this string
  - P_{MAX} is prob of most likely output *given all possible attacker knowledge*

$$h_{min} = -lg(P_{MAX})$$

- In 90B, we get entropy from an *entropy source*

Big Picture: Entropy and SP 800-90

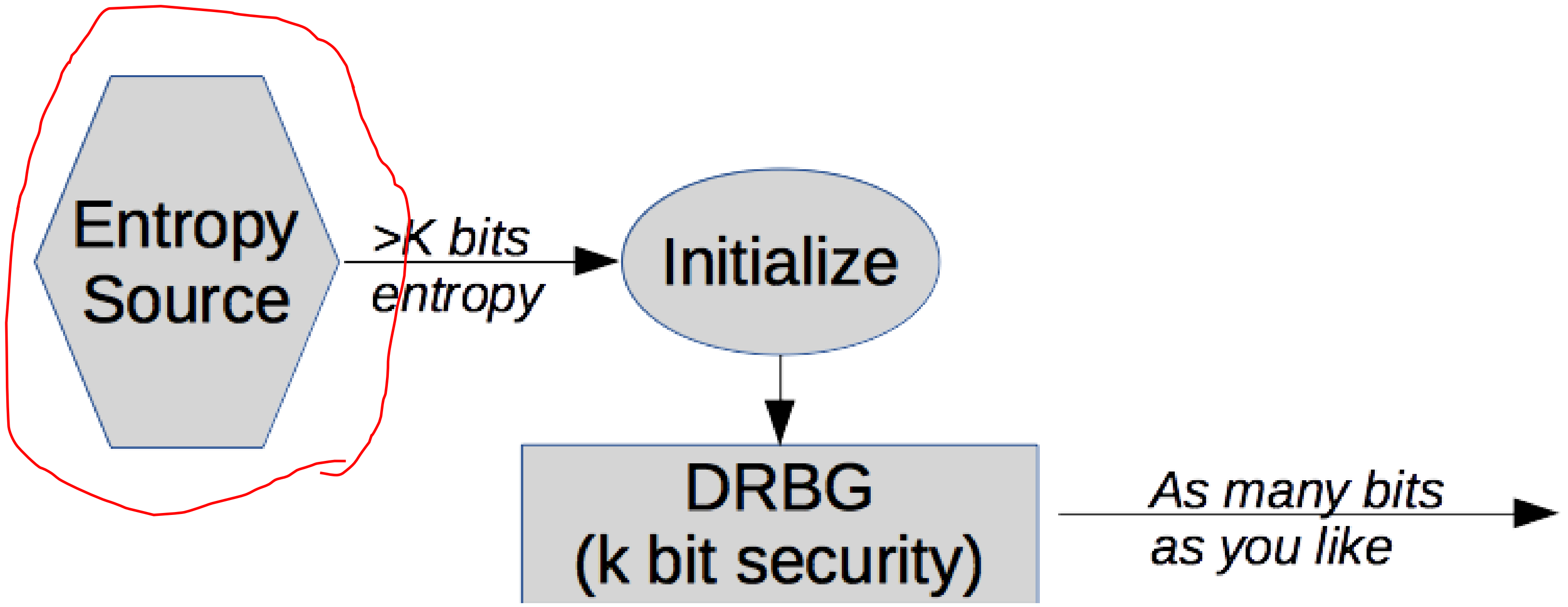


- We know how to build DRBGs
  - Deterministic algorithm
  - Published—attacker knows everything
  - Based on a cryptographic primitive

- The magic of a DRBG:
  - Takes an *unguessable* string.
  - Produces a string of *indistinguishible-from-random* output bits.

- What we need from Entropy Source:
  - String of bits
  - Known amount of entropy
  - Internal tests to make sure it's working

How Do We Build an Entropy Source?



- EVERYTHING in this picture is deterministic…

  …EXCEPT the Entropy Source
- Entropy Source:
  - Provides bitstrings with known amount of **entropy**
  - …so we can initialize DRBG securely

SP 800-90B is all about building entropy sources.

How to Build an Entropy Source
The SP 800-90B View

Noise Source

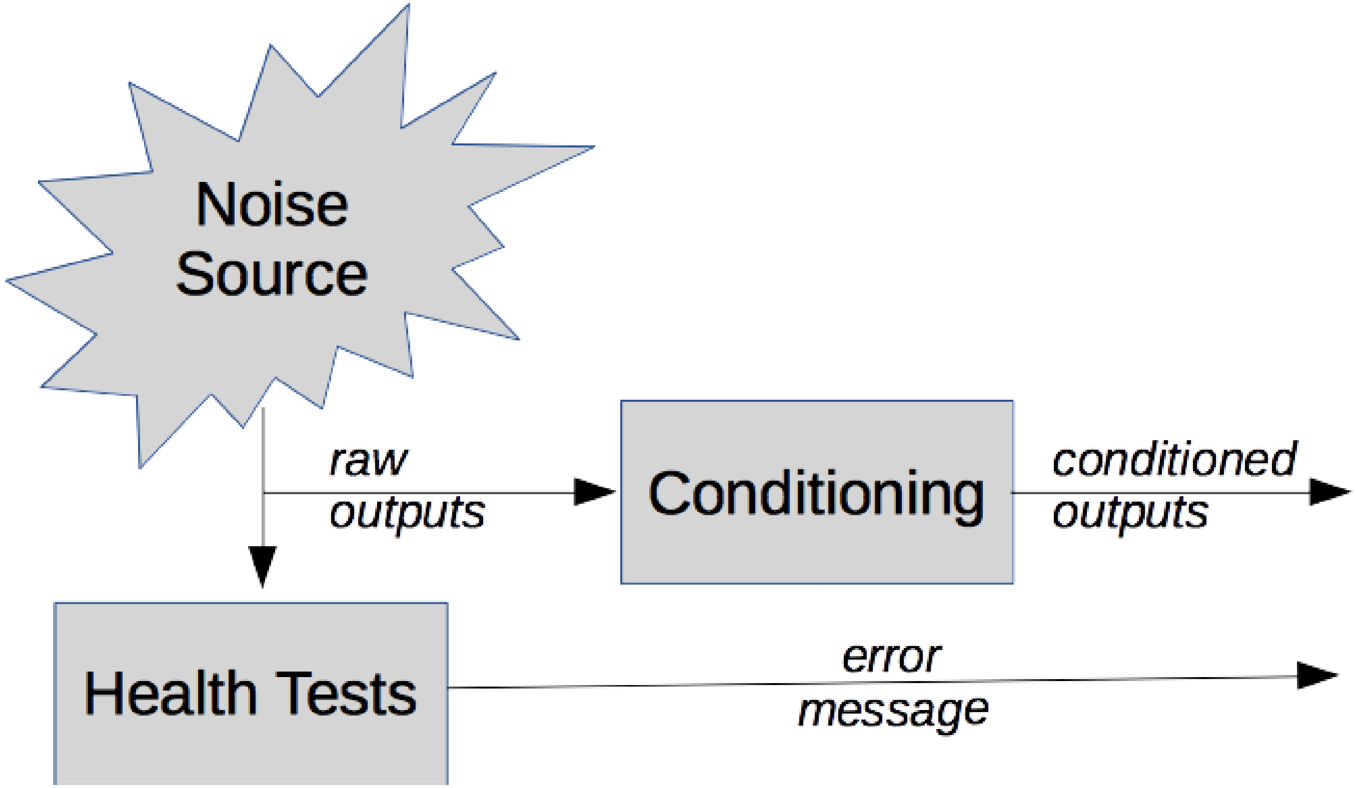
Where entropy comes from.

Health tests

Verify noise source still working correctly.

Conditioning

Optional processing of noise source outputs to improve statistics.



*Reminder: An entropy source provides bitstrings with **known** entropy/sample*

Two types of noise source

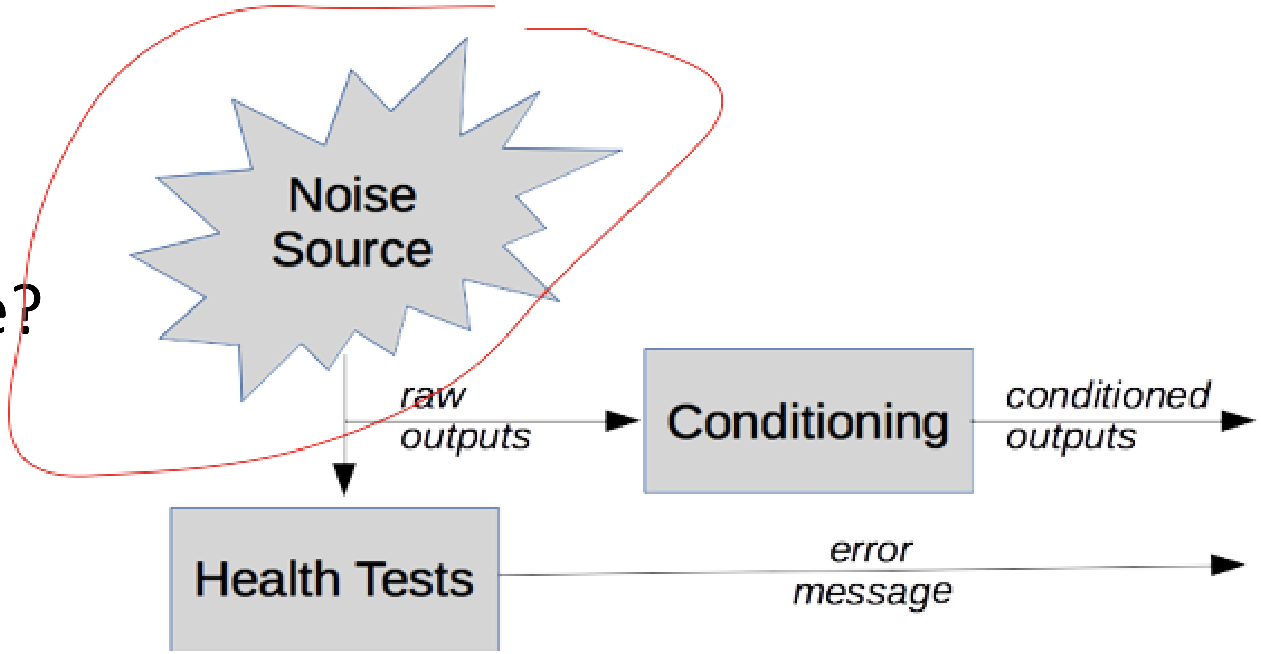
- Physical source
  - Purpose-built source of entropy
  - Unpredictibility based on some physical phenomenon
  - Should be simple enough to be modeled well
  - Examples:

  Ring oscillators, metastable latches, noisy diodes, single-photon sources

- Nonphysical source
  - "Found" source of entropy
  - Typically measured on a computer in software
  - Examples:

  Interrupt timings, memory access timings, hard-drive access timing*

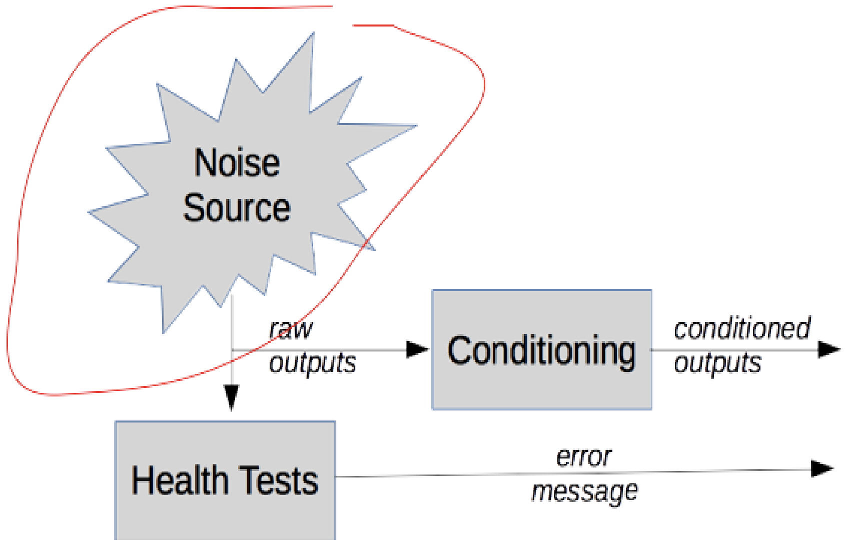
Estimating Entropy



- How unpredictable is noise source?
  - We need a lower bound on: entropy per raw output
- Two ways to estimate this:
  - Modeling
  - Statistical testing / black box estimators
- We require both
- ...currently lean more on black-box estimators
- ...trying to move to more modeling of source

Statistical Testing/Black Box Estimation

- Requirement: RAW BITS from noise source
  - Need access to unprocessed bits from noise source
  - Not always easy to define exactly what “raw” is
  - Collect lots of data



- Tests and entropy estimate depends on whether source claims to provide iid data or non-iid data.

This works better as a sanity check than as a direct entropy estimate.

IID sources

- If the source is really well behaved....
  - Every output independent of all other outputs
  - Not varying over time
- ...then entropy estimation is very easy
  - We just count the most common output
  - Apply a binomial bound and we're done

- Most sources are not iid

IID evaluation

- Source is only considered as iid if designer claims it
- Complicated set of tests to try to falsify claim of iid
- IID claim must also be justified in report (reviewer must verify that this is a reasonable claim for this source)
- If accepted as an IID source, entropy estimation is simple

Non-IID sources

- Most sources are not IID
- Even if source passes IID tests, it may not be reasonable to assume independence of nearby outputs.

Non-IID track: throwing spaghetti at the wall

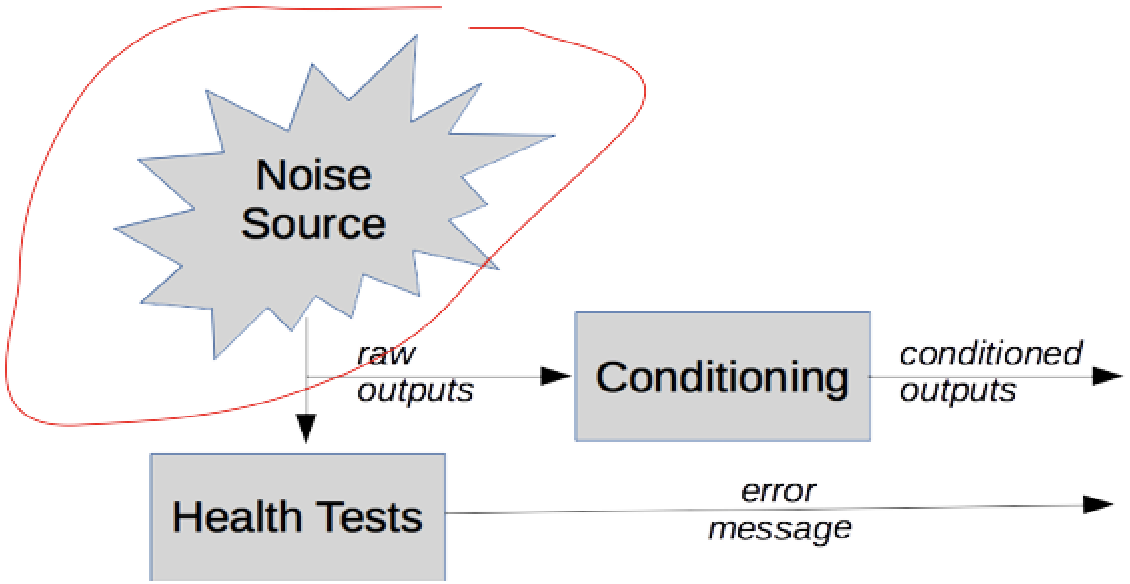
- Apply a large set of black-box entropy estimators to dataset
  - Each one makes different assumptions about source distribution
- Take the lowest estimate as the entropy estimate

Black box testing, cont'd

- We collect sequential and restart data
- Derive entropy estimates from each
- The result is generally pretty conservative...
- ...but it's also extremely ad-hoc.

- Black box testing without knowing internals of entropy source is not very powerful.
- Works best as a sanity check on estimate that comes from modeling source.

Modeling



- Start with complete understanding and description of source
- Stochastic model
  - Build a model to describe source behavior
  - Estimate parameters of model
  - Derive upper bound on P_{MAX} from model

    --> lower bound on h_{min}

  NOTE: this is only practical for physical sources
- Less rigorous justification for nonphysical sources
  - Describe measured behavior and experiments
  - Justify existence of entropy

Questions about the noise source

- **How does the noise source work? (What's unpredictable about it?)**

  "The operation of the noise source shall be documented…"

- **Where does the unpredictability come from?**

  "…where the unpredictability comes from"

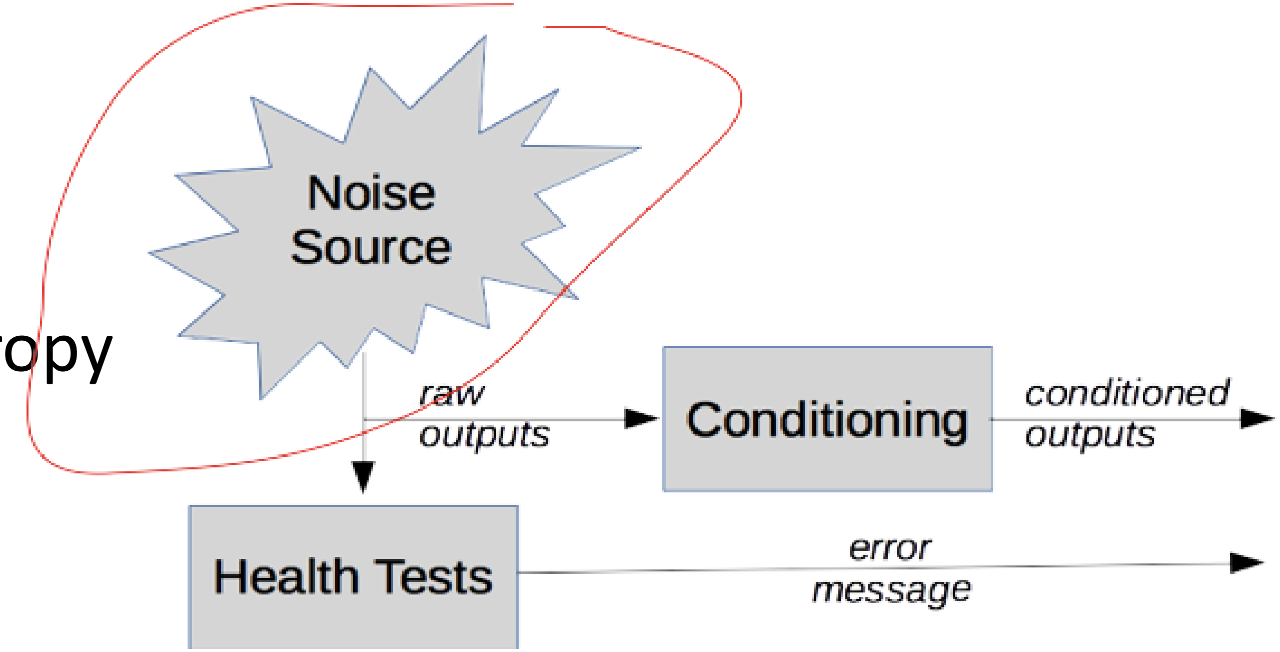
- **How much entropy / output is produced?**

  "Documentation shall provide an explicit statement of the expected entropy provided…"

- **How do you know? (Justify the entropy estimate.)**

  "…provide a technical argument for why the noise source can support that entropy rate."

Estimating Entropy: Summary

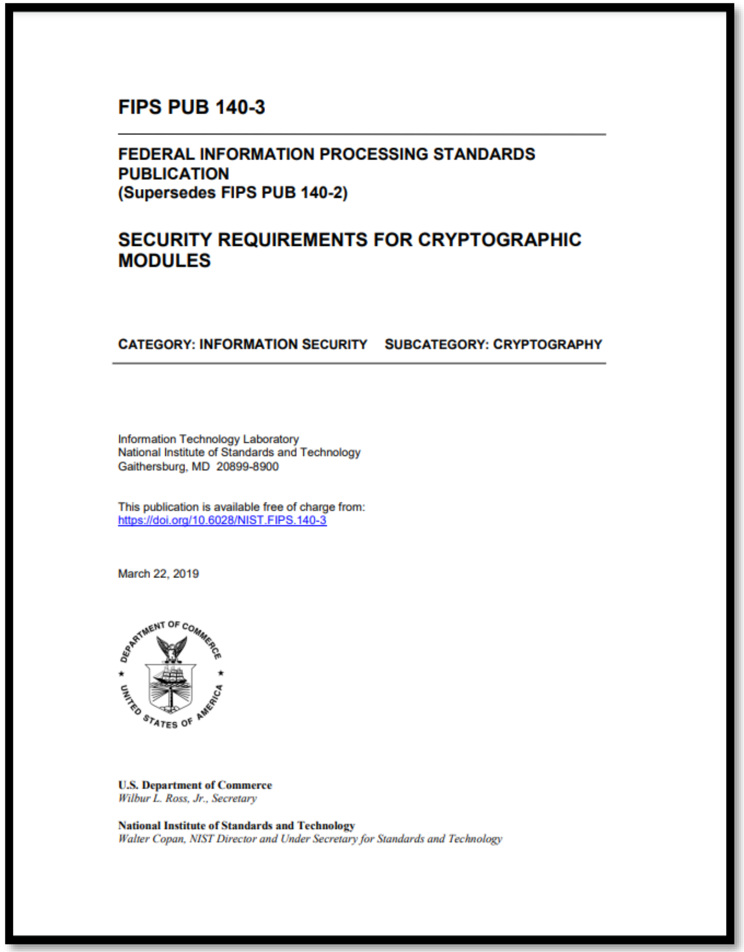


- We need to know how much entropy we're getting from noise source
- Two ways to do this:
  - Modeling
  - Statistical testing/black box estimation
- Questions to start with:
  - Where is the actual unpredictability coming from?
  - Can I quantify it?
  - …at least a lower-bound?
- Black box estimators are a "sanity check," but can be badly wrong.
- Model estimate is better, *assuming your model describes source well*.

Part III : Validation

Validation Process

- In order to comply with Federal Information Processing Standards 140-3, all SP 800-90A DRBGs and SP 800-90B Entropy Sources must be validated.
- DRBGs are validated through the Cryptographic Algorithm Validation Program (CAVP)
- Entropy sources and RBG constructions* are validated through the Cryptographic Module Validation Program (CMVP)



FIPS PUB 140-3

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION
(Supersedes FIPS PUB 140-2)

SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES

CATEGORY: INFORMATION SECURITY SUBCATEGORY: CRYPTOGRAPHY

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

This publication is available free of charge from:
https://doi.org/10.6028/NIST.FIPS.140-3

March 22, 2019

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary for Standards and Technology

DRBG Validation

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

NIST COMPUTER SECURITY RESOURCE CENTER CSRC

PROJECTS | CRYPTOGRAPHIC ALGORITHM VALIDATION PROGRAM

Cryptographic Algorithm Validation Program CAVP

Implementation Name	Crypto HAL-Core
Description	The ADRF88xx/89xx is an RF System-on-Chip designed for use in energy storage applications.
Version	2.2.5
Type	FIRMWARE

Vendor: Analog Devices
Corporate Headquarters
One Analog Way
Wilmington, MA 01887
USA
(781) 935-5565
1-800-262-5643

Contacts: Lei Poo
1-617-583-2384
Jonathan Simon
1-510-400-2936

A2728 First Validated: 7/26/2022

Collapsed | Expanded | Aggregated

Operating Environment	Algorithm Capabilities
ARM Cortex M4F with ADRF8800/8900 Series	AES-CCM
ARM Cortex M4F with ADRF8800/8900 Series	Counter DRBG Prediction Resistance: No Supports Reseed Capabilities: Mode: AES-128 Derivation Function Enabled: Yes Additional Input: 256 Entropy Input: 312 Nonce: 72 Personalization String Length: 256

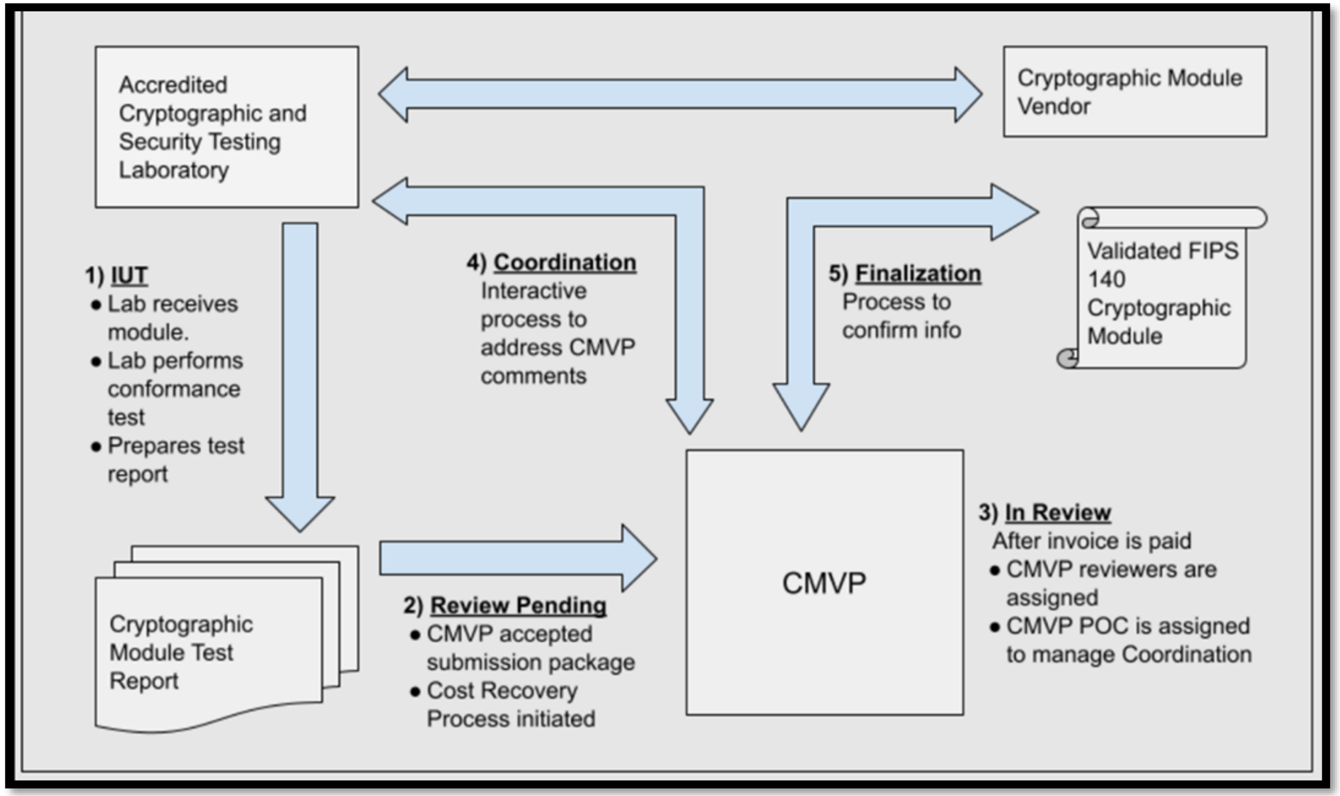
Entropy Source Validation

- Beginning 07 November 2020, entropy sources in FIPS 140-2 and FIPS 140-3 module submissions are required to be compliant to NIST SP 800-90B*
    - Previous submissions denoted "NDRNG" on validation certificate, met requirements in Implementation Guidance

- Until mid 2022, all entropy reports were submitted along with the module validation report

- Beginning mid 2022, Entropy Source Validation Test System (ESVTS) available for separate entropy source report submission

Entropy Source Review Process – With Module (until 01 Jan 2023)



1. Module includes entropy source (new reports tested to 90B). Same lab for both module and entropy report.

2. Separate cost for entropy will apply in the future.

3. Previously, module reviewers were also entropy reviewers. Now, dedicated entropy reviewers are assigned.

4. Entropy POC address entropy comments, while module POC address module comments. Both module and entropy comments are sent to the lab at the same time for each round.

5. Once finalized, module, inclusive of the entropy source (ENT) is validated and assigned a certificate number.

ESV Review Process (mandatory 01 Jan 2023)

- Decouple entropy source validation from module validation
- Lab submits raw noise, restart samples and any conditioned output sample data through ESVTS
  - SP 800-90B estimators run on ESV servers
- Reference ESV Cert in a similar manner to CAVP Certs
- Reuse validated entropy sources in multiple modules

ESV Web Client

‹ NIST

Welcome to the Entropy Source Validation (ESV) website

This website is a NIST Cryptographic Module Validation Program (CMVP) Tool allowing accredited labs to complete and upload submissions justifying conformance to SP 800-90B

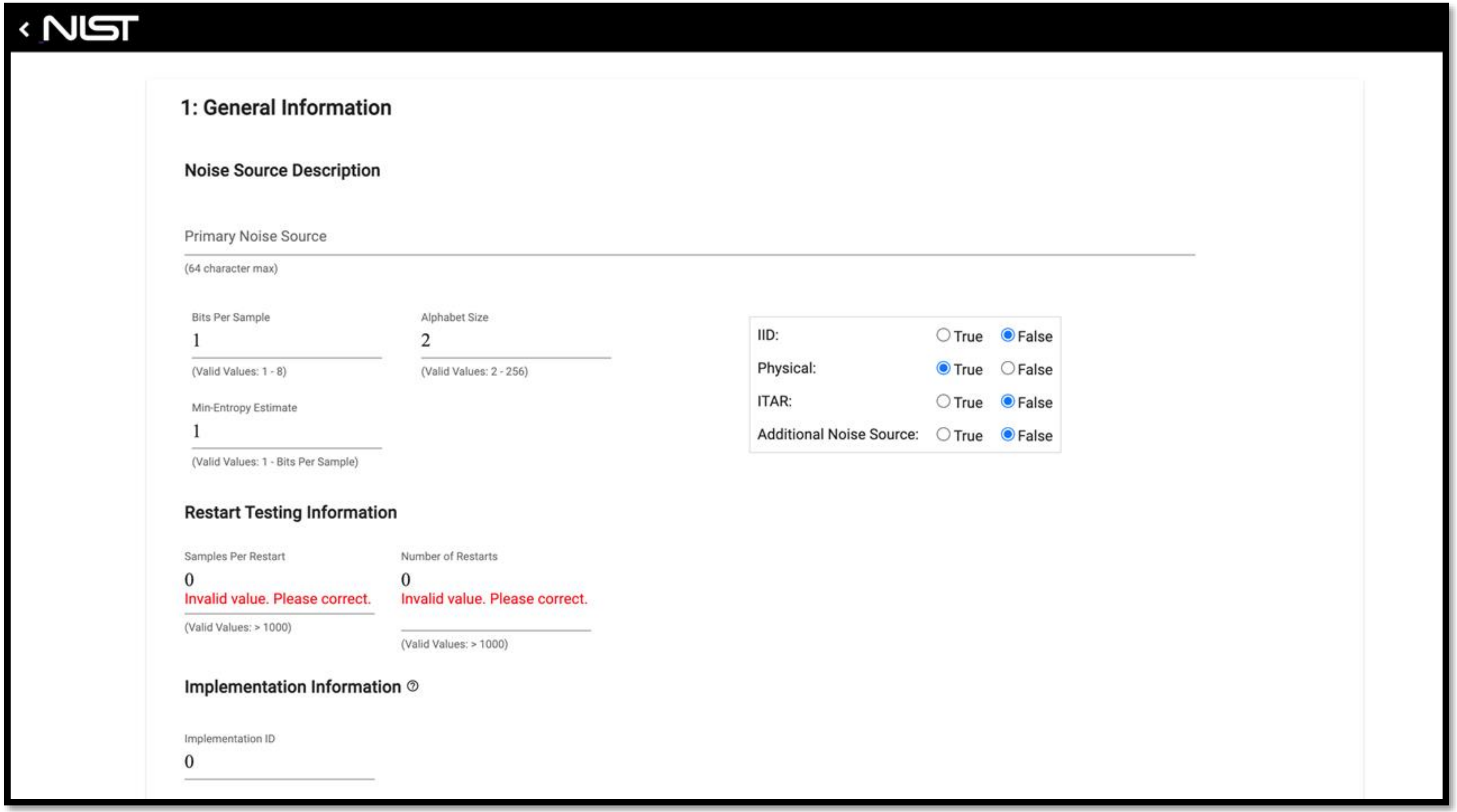
Submissions include 5 parts:

1. Information about the entropy source
2. Information about any conditioning components
3. Files containing samples collected from the entropy source
4. Supporting documentation justifying conformance to all relevant SHALL statements in SP 800-90B
5. Supporting documentation outlining how a cryptographic module may utilize the entropy source

Begin Submission ▶

To learn more about SP800_90B Entropy click here

ESV Web Client



First ESV Certificate Issued

NIST

Entropy Certificate E1

Details

Source Name	NetApp CryptoMod
Standard	SP 800-90B
Category	Non-Physical
Description	CPU Jitter RNG v3.4.0
Version	3.0
Reuse status	Bound to Module

	Operating Environments	**Vetted Conditioning Component CAVP Certificates**
Entropy Per Sample: Full entropy Sample Size: 256 bits	• ONTAP 9.11.1 running on an AFF A250 running on Intel® Xeon® D-2164IT (Skylake) without PAA	• A2640 (SHA3-256)
Entropy Per Sample: Full entropy Sample Size: 256 bits	• ONTAP 9.11.1 running on an AFF A400 running on Intel® Xeon® Silver 4210 (Cascade Lake) with PAA	• A2640 (SHA3-256)
Entropy Per Sample: Full entropy Sample Size: 256 bits	• ONTAP 9.11.1 running on an AFF A900 running on Intel® Xeon® Platinum 8352Y (Ice Lake) with PAA	• A2640 (SHA3-256)

Vendor

NetApp, Inc.
3060 Olsen Drive
San Jose, California 95128
USA

NetApp Security Assurance Team
+1 (919) 476-5600
ng-psg-sa@netapp.com

Files

Public Use Document

Validation History

08/29/2022	EID-32-E003	Lightship Security, Inc.

Observations

- Entropy source validation is a review-intensive process
  - SP 800-90B estimators produce min-entropy estimate on collected data
  - 82 requirements (**shall** statements) in SP 800-90B
- Entropy report reviewers – and lab staff – need specialized technical background
  - Digital and analog circuits, semiconductor physics, information theory, stochastic processes
- 44 entropy sources validated to SP 800-90B up to September
  - 31 – CPU Jitter (incl. Linux RNG)
  - 9 – Oscillator(s)
  - 3 – Other hardware
  - 1 – Quantum source

Conclusion

NIST

- Generating random unpredictable numbers is hard.
- Many things can go wrong (unintentionally and intentionally)
- Standards/guidelines are useful, but they have limitations.
- A good understanding of the design is necessary to estimate entropy.

Development of guidelines on random number generation is an ongoing process.

Contact: rbg_comments@nist.gov