NIST Standards on Random Bit Generation

Overview

Meltem Sönmez Turan

NIST Random Bit Generation Workshop 2023

May 31, 2023

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

ITL INFORMATION TECHNOLOGY LABORATORY

This talk

aims to provide an overview of the **NIST standards** on cryptographic random number generation.

Cryptographic random number generation

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

Many real-world failures:

- Heninger et al. (2012) performed a network survey of TLS and SSH servers, and collected certificates and recovered RSA and DSA keys, due to low entropy during key generation.
- Bernstein et al. (2013) studied the Taiwan's national "Citizen Digital Certificate" database and efficiently factored 184 distinct RSA keys due to low-quality hardware RNG.

- Heninger et al., *Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices*, 21st USENIX Security Symposium, 2012.
- Bernstein et al., *Factoring RSA Keys from Certified Smart Cards: Coppersmith in the Wild*. ASIACRYPT 2013

Challenges in random number generation

Designing random bit generators (RBGs)

- Finding a robust randomness source and correctly extracting randomness
- Difficult to know how unpredictable the outputs are (i.e., estimating entropy)

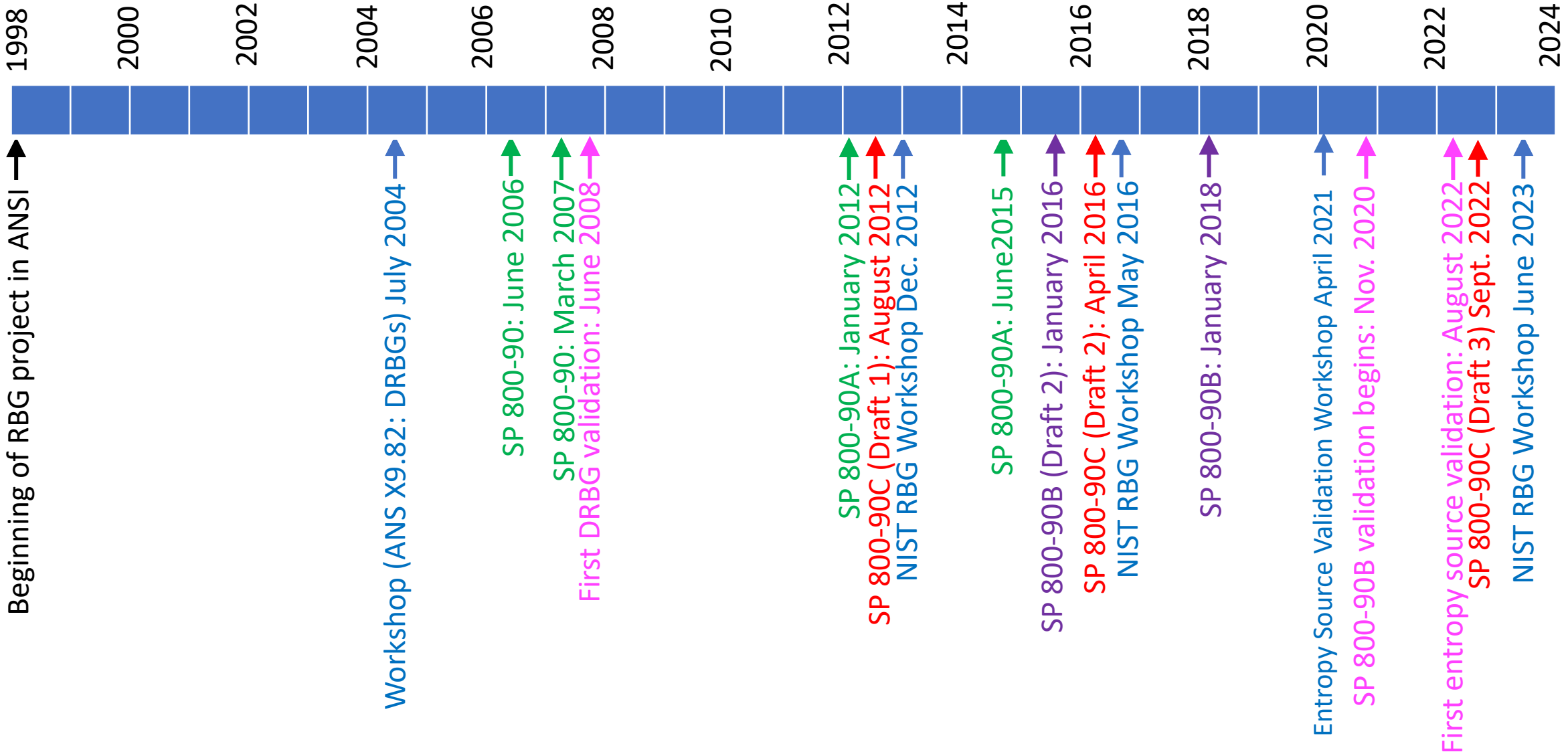
Developing standards for RBGs and validating RBGs

- Difficult to develop guidelines and recommendations that are easy to validate
- Expert knowledge on the randomness sources
- Difficult to verify some of the claims
- Practical constraints (e.g., budget, evaluation time)

NIST standards on Random Bit Generation

SP 800-90A	SP 800-90B	SP 800-90C	SP 800-22
• Deterministic Random Bit Generators (DRBGs)	• Noise, entropy sources • Entropy estimation techniques • Health tests • Validation	• Various RBG constructions • Guidelines on how to merge DRBGs and entropy sources	• Statistical randomness test suite

Timeline


1998
2000
2002
2004
2006
2008
2010
2012
2014
2016
2018
2020
2022
2024
Beginning of RBG project in ANSI
Workshop (ANS X9.82: DRBGs) July 2004
SP 800-90: June 2006
SP 800-90: March 2007
First DRBG validation: June 2008
SP 800-90A: January 2012
SP 800-90C (Draft 1): August 2012
NIST RBG Workshop Dec. 2012
SP 800-90A: June2015
SP 800-90B (Draft 2): January 2016
SP 800-90C (Draft 2): April 2016
NIST RBG Workshop May 2016
SP 800-90B: January 2018
Entropy Source Validation Workshop April 2021
SP 800-90B validation begins: Nov. 2020
First entropy source validation: August 2022
SP 800-90C (Draft 3) Sept. 2022
NIST RBG Workshop June 2023

SP 800-90A (2015)

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

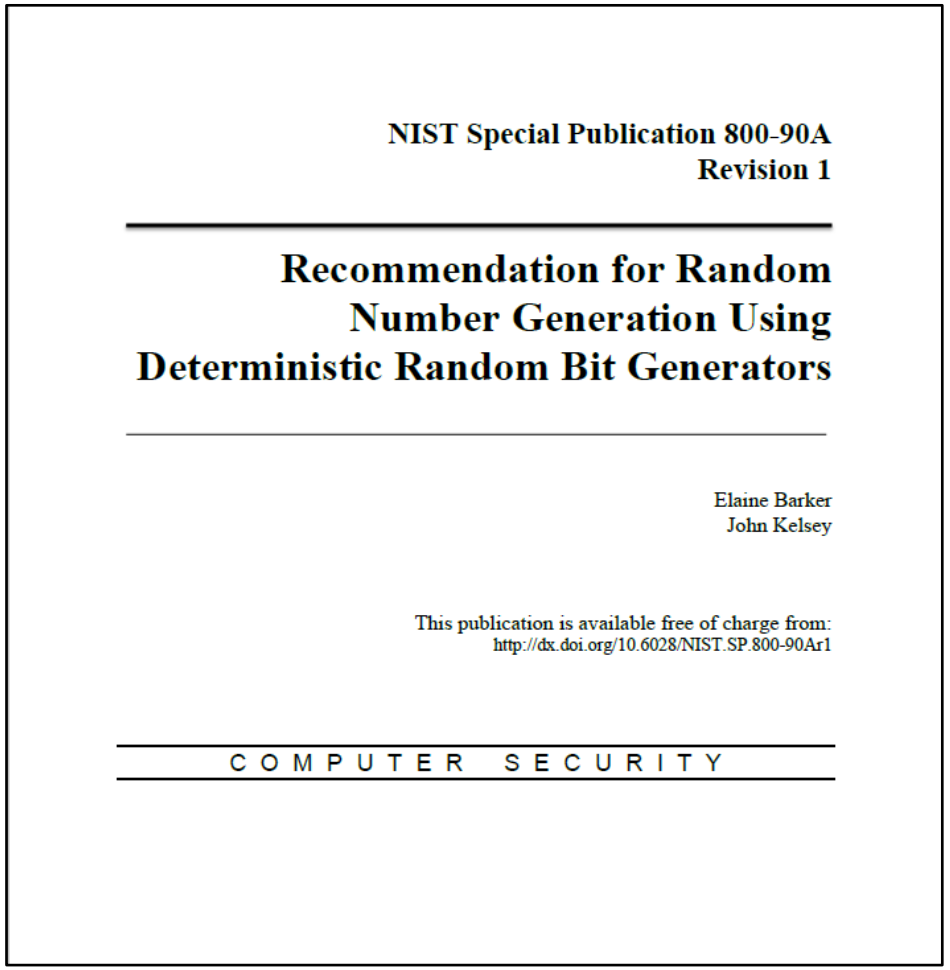
- Approves three DRBGs:
  CTR_DRBG, Hash_DRBG, HMAC_DRBG

Earlier versions:

As SP 800-90: June 2006 and March 2007

As SP 800-90A: January 2012

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

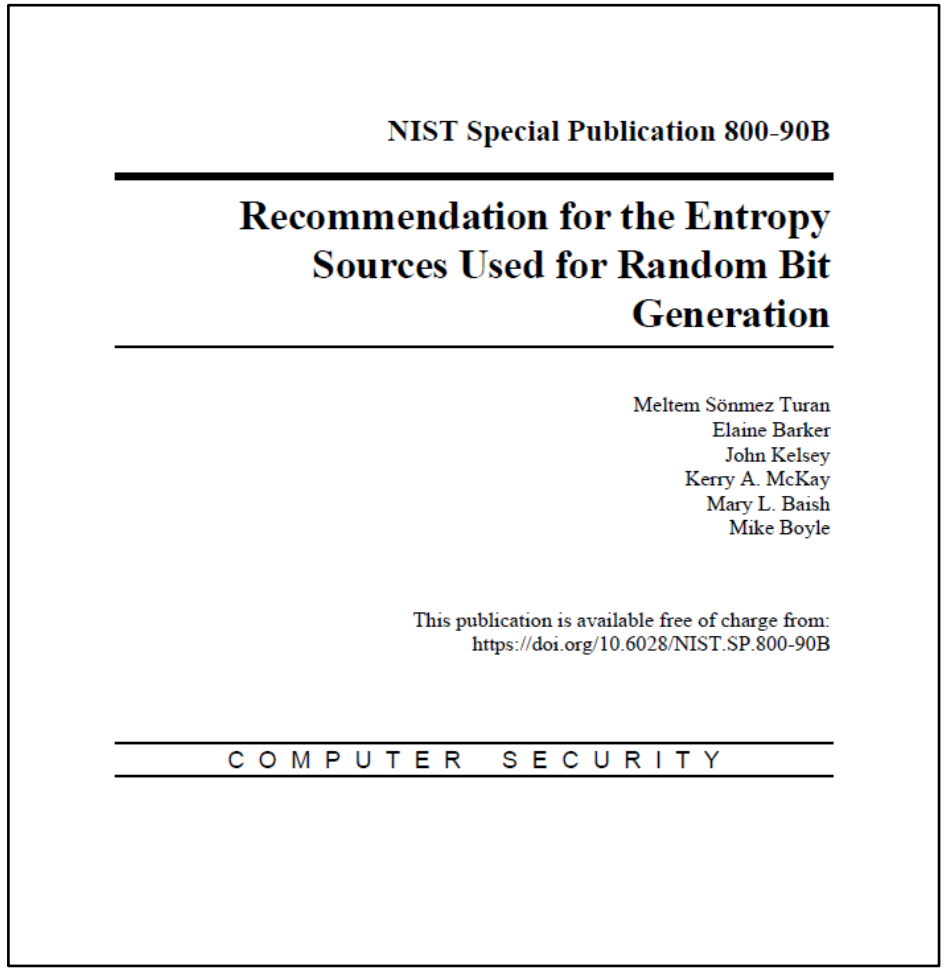
COMPUTER SECURITY

SP 800-90B (2018)

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

Earlier versions (drafts): August 2012 and January 2016

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

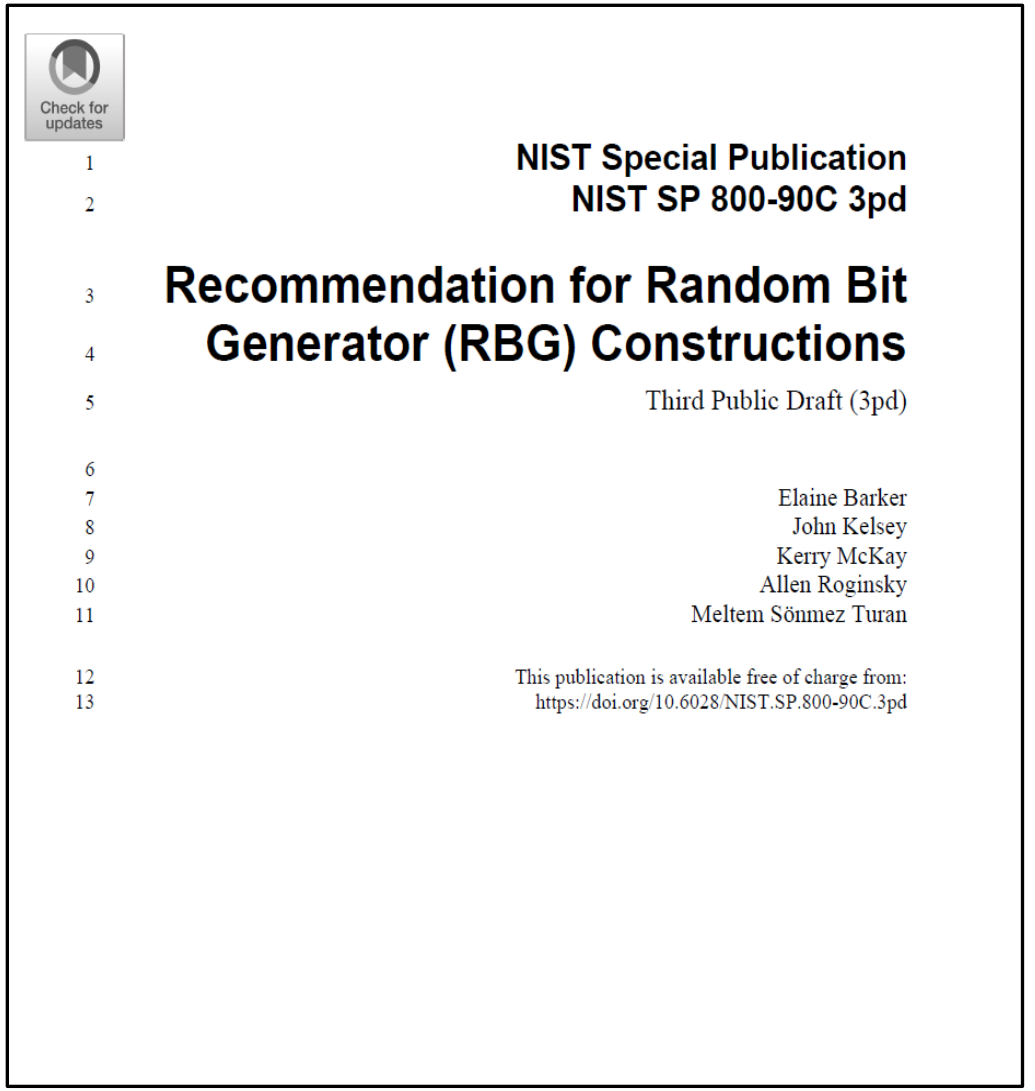
Draft SP 800-90C (2022)

Describes three RBGs constructions (using 90A and 90B):

- 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 (drafts): August 2012 and April 2016.

Next steps: Include DRBG chains (RBGC)



Check for updates

NIST Special Publication
NIST SP 800-90C 3pd

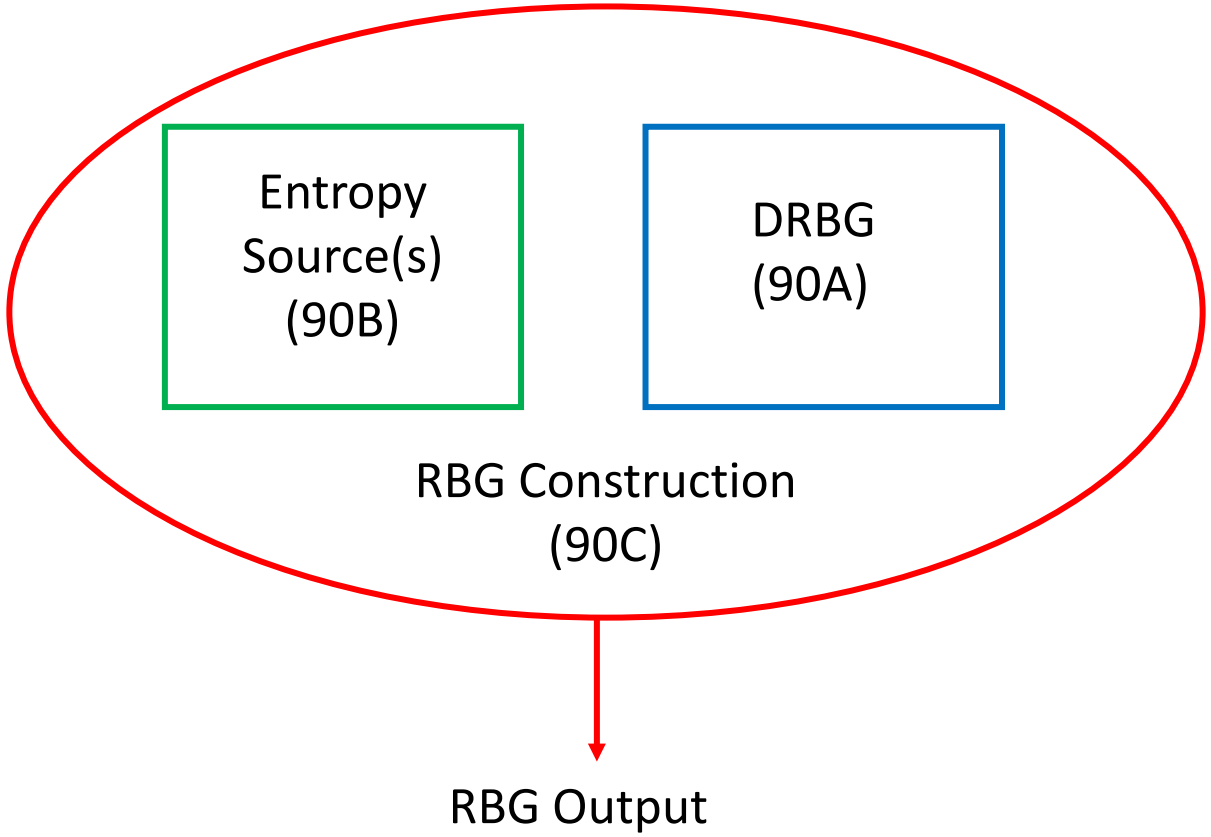
Recommendation for Random Bit Generator (RBG) Constructions

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

Parts of SP 800 90 Series



SP 800-22 (2010)

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

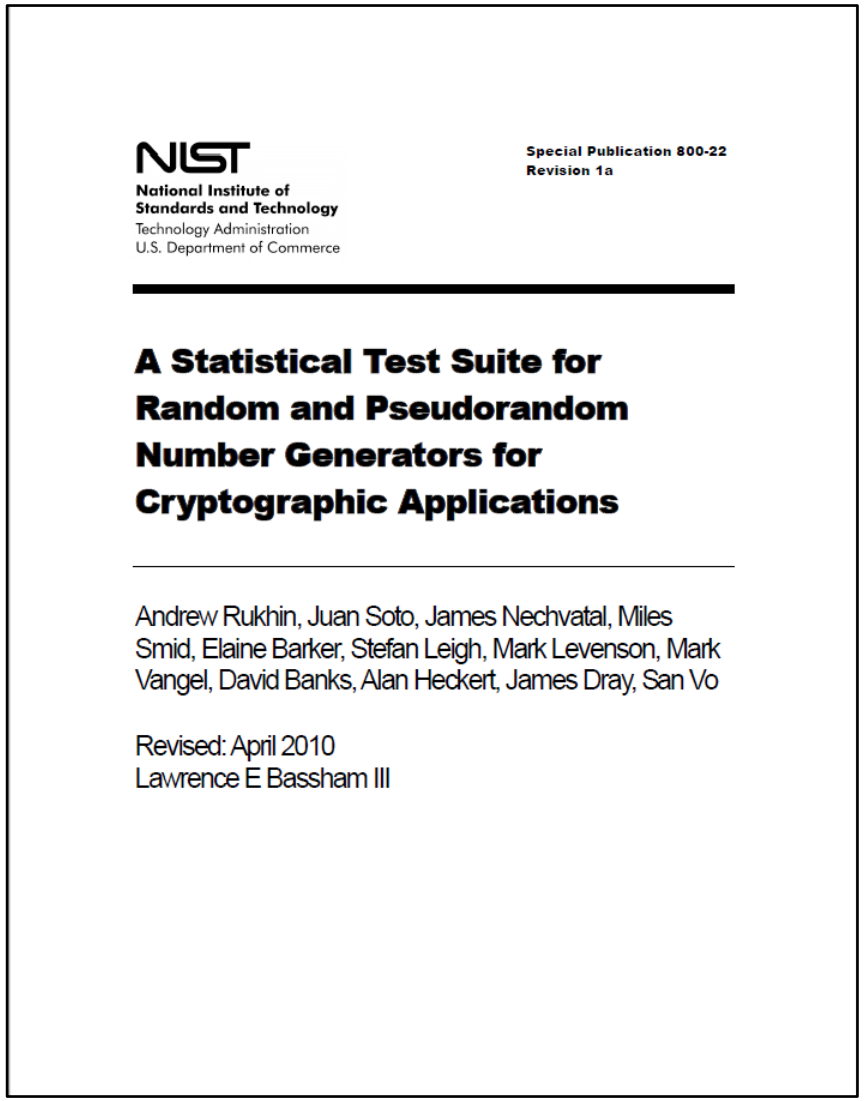
Earlier version: May 2001 and August 2008.

Next steps:

In 2022, *Crypto publication review board* completed the review of SP 800-22 and proposed **revising** 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

Standards Alignment

RBG standards by BSI (Germany) :

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

NIST and BSI are jointly working to align the RBG standards; will publish a joint NIST-BSI report to compare the processes.

Other RBG standards :

- ANSI X9.82: Part 4-2011 (RNGs for the financial services industry)
- ISO/IEC 18031:2011 (Random Bit Generation)
- ISO/IEC 20543:2019 (Test and analysis methods for RBGs within ISO/IEC 19790 and ISO/IEC 15408)

This workshop

- Get feedback on NIST random number generation standards
  - Dedicated talks for SP 800 90A/B/C and revision plans (chaining DRBGs, health tests etc.)
  - Open discussions

Thanks!

Contact NIST team

rbg_comments@nist.gov

Public forum

rbg-forum@list.nist.gov

Website

https://csrc.nist.gov/Projects/random-bit-generation