Bridging the Gap Between the SP 800-90 Series and AIS 20/31

Kerry McKay
RBG Workshop 2023
May 31, 2023

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

ITL INFORMATION TECHNOLOGY LABORATORY

Overview

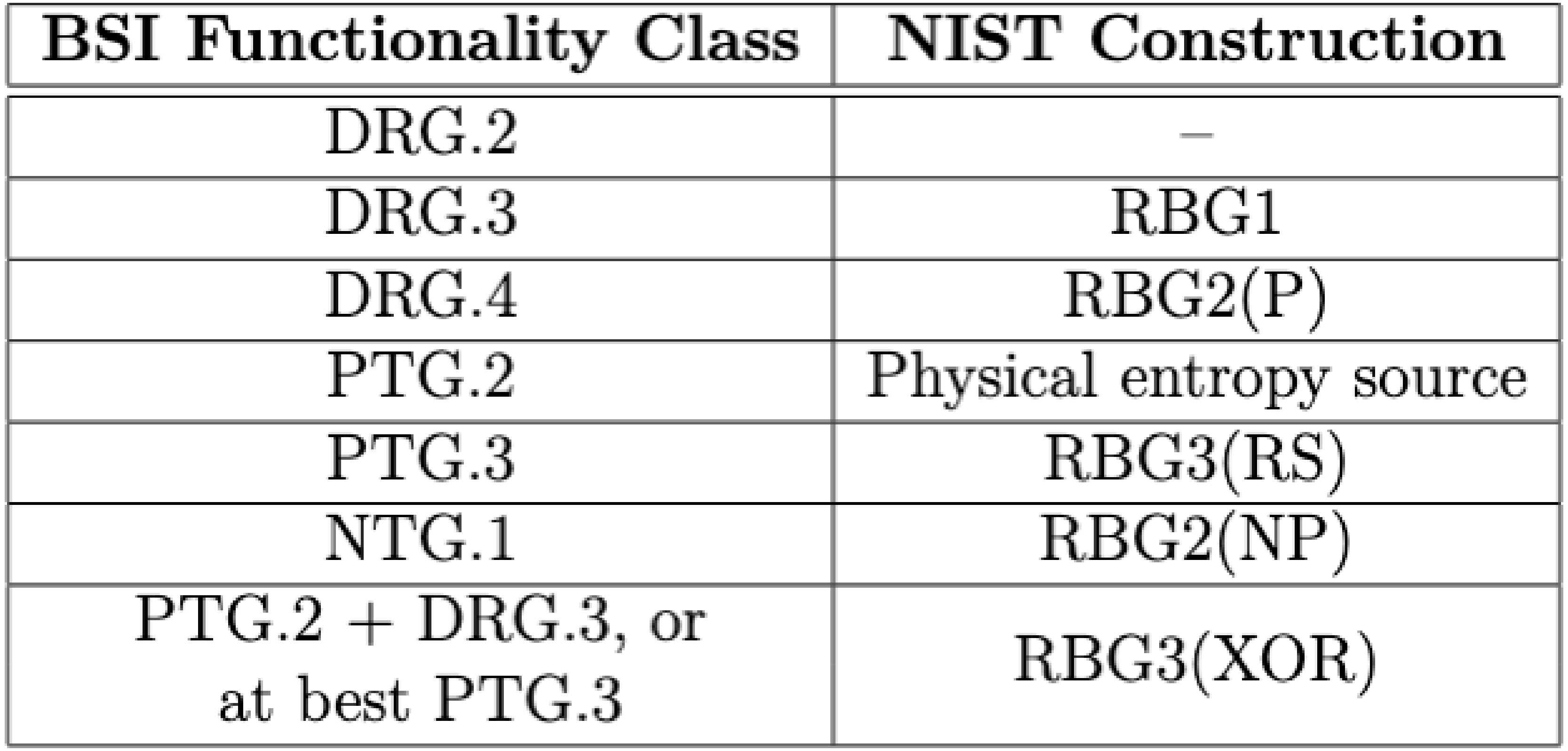
- Ongoing work between NIST and BSI to harmonize standards and guidelines on random number generation
- Main goal is to make it easier for a RBG/RNG design to pass validation testing according to both standards
- Writing a joint document
    - Similarities and different requirements for harmonization
    - Comparison of
        - Functionality Classes of AIS 20/31
        - Random Bit Constructions of SP 800-90 series

Randomness Standards

- SP 800-90A: Recommendation for Random Number Generation Using Deterministic Random Bit Generators
- SP 800-90B: Recommendation for the Entropy Sources used for Random Bit Generation
- SP 800-90C: Recommendation for Random Bit Generator Constructions
  - Draft September 2022

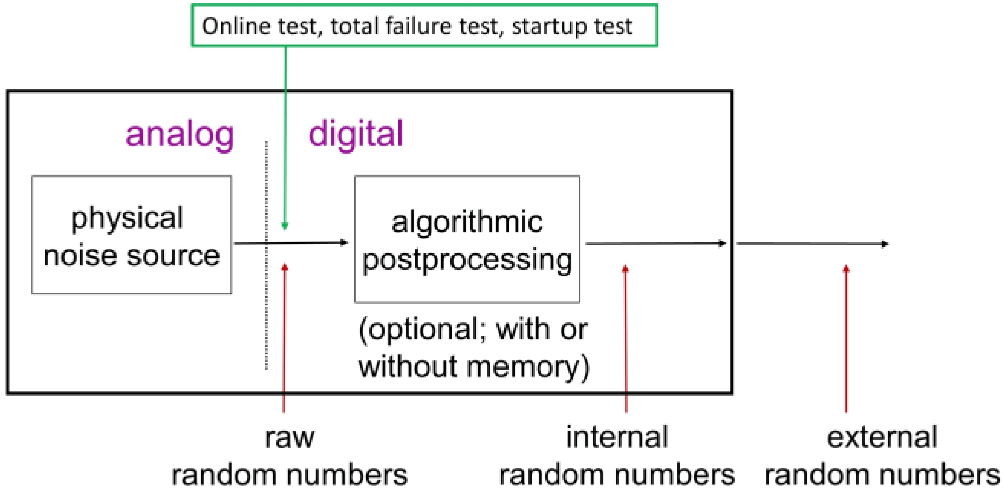
- AIS 20: Functionality Classes and Evaluation Methodology for Deterministic Random Number Generators
- AIS 31: Functionality Classes and Evaluation for Physical Random Number Generators
- Both point to a joint mathematical-technical reference, often simply called ‘AIS 20/31’
  - Draft September 2022

Functionality Classes vs. RBG Constructions

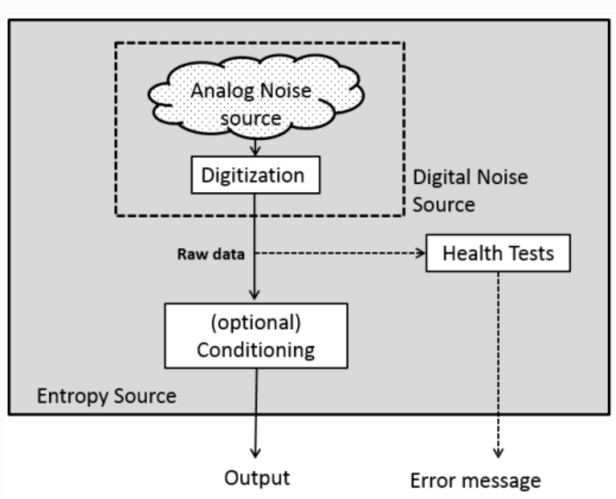


BSI Functionality Class	NIST Construction
DRG.2	–
DRG.3	RBG1
DRG.4	RBG2(P)
PTG.2	Physical entropy source
PTG.3	RBG3(RS)
NTG.1	RBG2(NP)
PTG.2 + DRG.3, or at best PTG.3	RBG3(XOR)

PTG.2 and Entropy Source



Online test, total failure test, startup test
analog
digital
physical noise source
algorithmic postprocessing
(optional; with or without memory)
raw random numbers
internal random numbers
external random numbers



PTG.2

- Physical noise source
- Postprocessing (optional)
- Online test, total failure test, start-up test
- Entropy per output bit ≥ PTG.2-specific bound
- *Not intended for 'direct' use*

Entropy Source

- Physical or non-physical noise source
- Conditioning (optional)
- Health tests
- No hard limit on entropy per bit value
- *Not intended for 'direct' use*

Additional Requirements

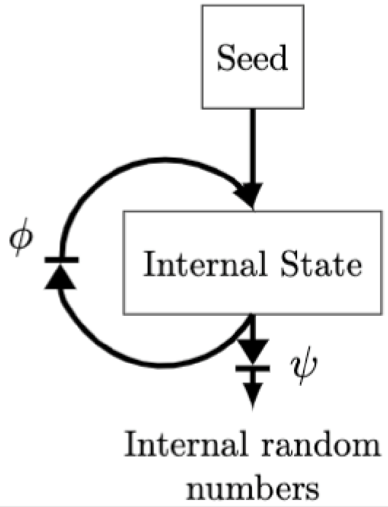
Validating PTG.2 as an entropy source

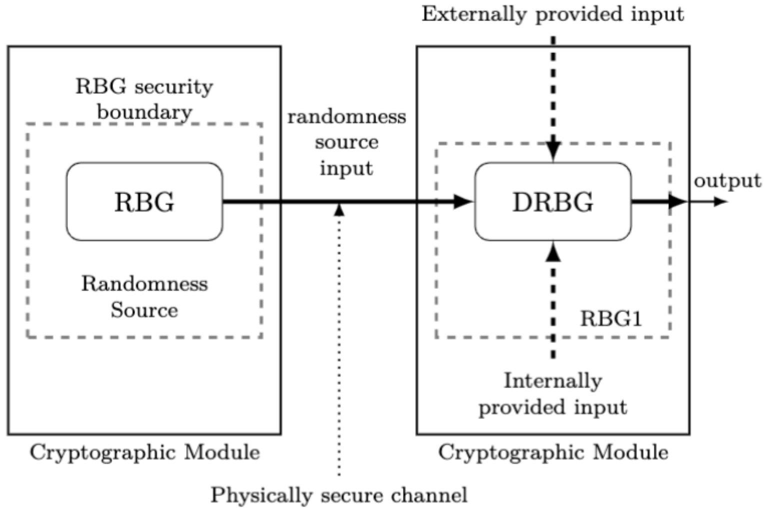
- On-demand tests, continuous tests
- Tests and predictors specified in SP 800-90B

Certifying an entropy source as PTG.2

- Noise from physical source
- Outputs follow [time-locally] stationarily distributed raw random numbers
- Entropy/bit ≥ PTG.2-specific bound (can be achieved by additional conditioning)
- Stochastic model
- Verification that the online test and the total failure test are effective
- Black box test suites

DRG.3 and RBG1





DRG.3

- Non-approved designs (security proofs required)
- Backward secrecy, forward secrecy and enhanced backward secrecy
- Appropriate seeding process
  - External true RNG (in particular: PTG.2, PTG.3, NTG.1)

RBG1

- Approved designs (SP 800-90A conformance)
- Backtracking resistance
- Appropriate seeding process
  - External randomness source:

    RBG2(P), RBG3

Additional Requirements

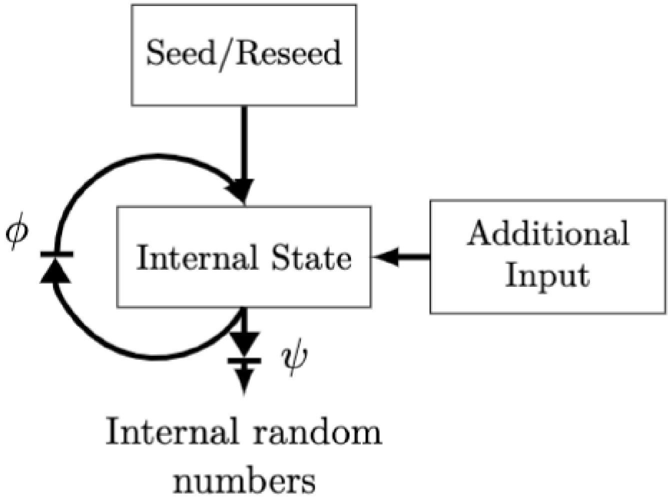
Validating DRG.3 as RBG1

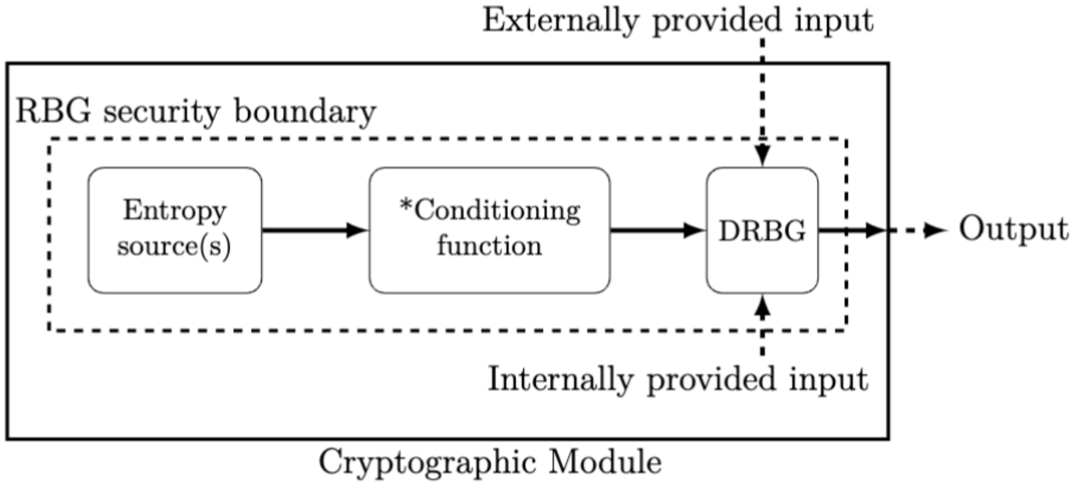
- SP 800-90A-approved design
- Seeding only with a physical RNG
  - PTG.2, PTG.3: min-entropy claim needed
  - Seed string contains enough entropy (DRG.3: ≥ 240 bit min-entropy after seeding)
- Known-answer test

Certifying RBG1 as DRG.3

- Verification of the algorithmic requirements of class DRG.3 (e.g., effective internal state: (i) size ≥ 252 bits, (ii) min-entropy after seeding ≥ 240 bits)
  - Waived for Hash_DRBG (Hash ≠ SHA-1)
- Seed with PTG.2, PTG.3, or NTG.1
- Possibly: more detailed proof of the seed entropy

DRG.4 and RBG2(P)





DRG.4

- Non-approved designs (security proofs required)
- Backward and forward secrecy
- Enhanced backward and forward secrecy
- Appropriate (re-)seeding process or additional high-entropy input
  - Physical RNG (in particular: PTG.2, PTG.3)

RBG2(P)

- Approved designs (SP 800-90A conformance)
- Backtracking and prediction resistance
- Appropriate (re-)seeding process
  - 90B-compliant internal physical entropy source

Additional Requirements

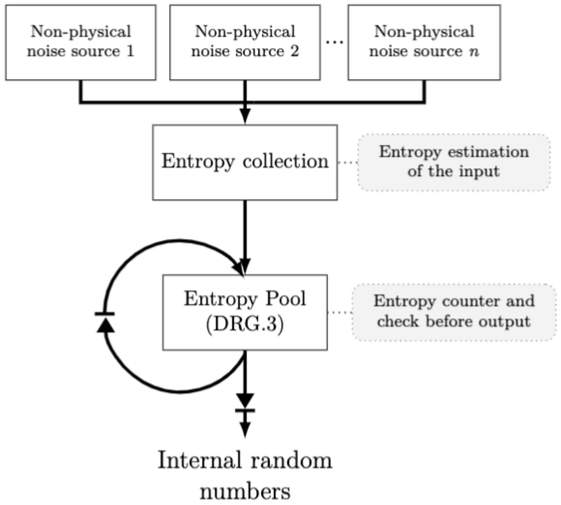
Validating DRG.4 as RBG2(P)

- SP 800-90A-approved design
- Prediction resistance only by reseeding from PTG.2, PTG.3
- Seed string contains enough entropy (DRG.3: ≥ 240 bit min-entropy after (re-)seeding)
- Known-answer test
- PTG.2, PTG.3: min-entropy claim needed

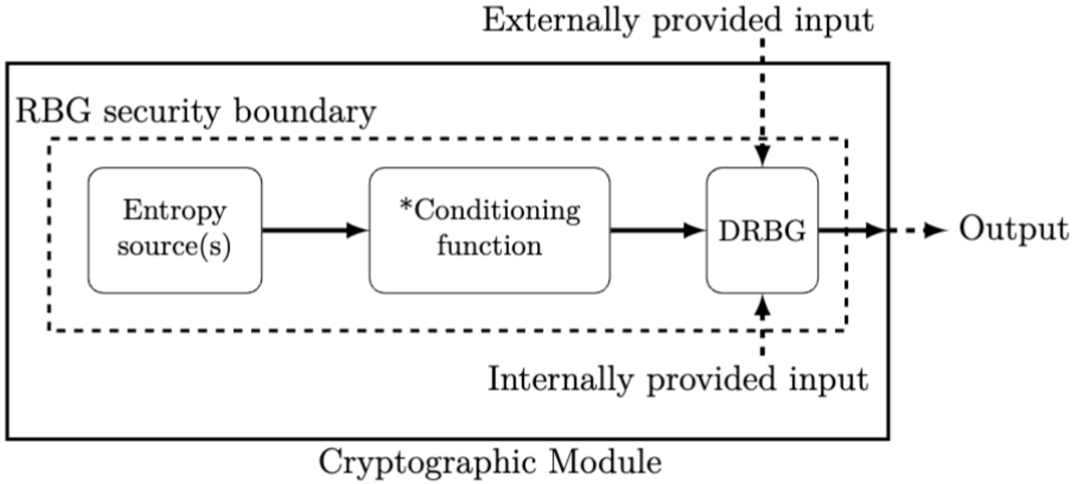
Certifying RBG2(P) as DRG.4

- Verification of the algorithmic requirements of class DRG.4
    - Waived for Hash_DRBG (Hash ≠ SHA-1)
- Stochastic model for randomness source
    - Satisfied if PTG.2, PTG.3 (RBG3(RS), RBG3(XOR) should also be appropriate)

NTG.1 and RBG2(NP)



Non-physical noise source 1
Non-physical noise source 2
...
Non-physical noise source n
Entropy collection
Entropy estimation of the input
Entropy Pool (DRG.3)
Entropy counter and check before output
Internal random numbers



NTG.1

- Non-physical noise source
- DRG.3-compliant postprocessing algorithm
- Min-entropy claim / output bit: at least 0.98

RBG2(NP)

- Non-physical noise source
- Approved designs (SP 800-90A conformance)
- Backtracking and prediction resistance
- Appropriate (re-)seeding process
  - 90B-compliant internal non-physical entropy source

Additional Requirements

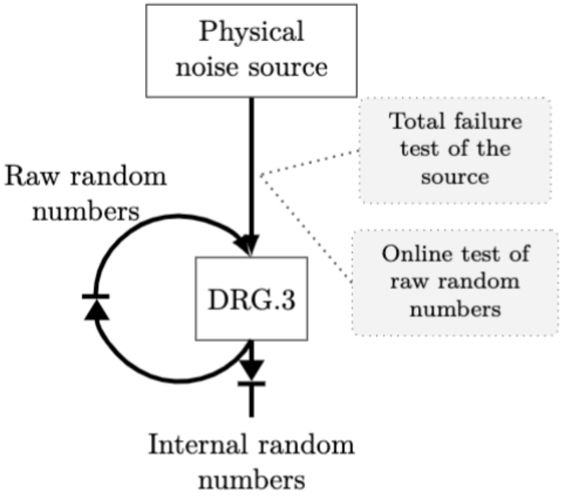
Validating NTG.1 as RBG2(NP)

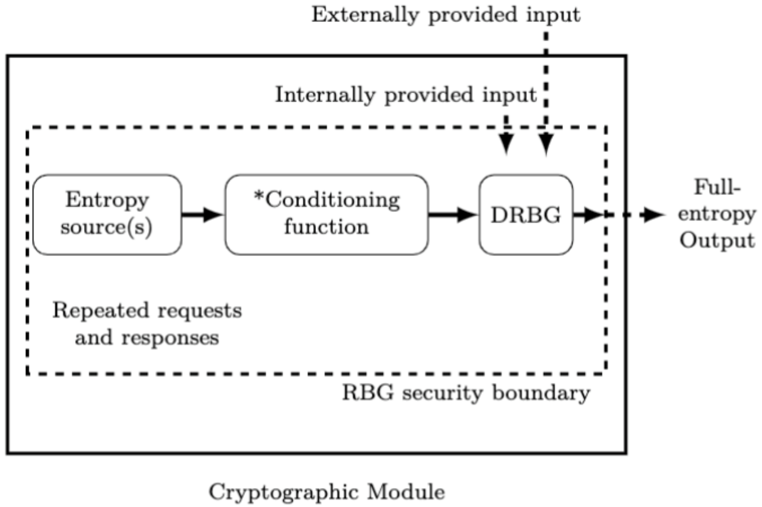
- SP 800-90A-approved postprocessing
- Fresh entropy only by reseeding
- Known-answer test
- Tests and predictors specified in SP 800-90B

Certifying RBG2(NP) as NTG.1

- Permanently fresh entropy
- Verification of the algorithmic requirements of class DRG.3
  - Waived for Hash_DRBG (Hash ≠ SHA-1)

PTG.3 and RBG3(RS)





PTG.3

- Physical noise source, usual case: PTG.2-compliant intermediate random numbers (input to postprocessing with memory, compliant to DRG.3)
- Postprocessing: data compression possible
- Maximum min-entropy claim / output bit: $1 - 2^{-32}$

RBG3(RS)

- SP 800-90B-compliant internal physical entropy source
- Deterministic part: 90A-approved design

Additional Requirements

Validating PTG.3 as RBG3(RS)

- SP 800-90A approved postprocessing
- Fresh entropy only by reseeding
- Min-entropy claim / output bit: $1 - 2^{-32}$ bit
- On-demand test, continuous test
- Known-answer test
- Tests and predictors specified in SP 800-90B

Certifying RBG3(RS) as PTG.3

- (Time-locally) stationarily distributed raw random numbers
- Stochastic model
- Verification that the online test and the total failure test are effective
- Postprocessing: verification of the algorithmic requirements of class DRG.3
  - Waived for hash_drbg (hash ≠ SHA-1)
- Black box test suites

Next Steps

- BSI and NIST in the process harmonizing RBG/RNG terminology of AIS 20/31 and SP 800-90
  - Some requirements harmonized as well
- A draft of a joint document (NIST & BSI) will be published soon
  - Contains comparisons of functionality classes and RBG constructions
  - Includes a joint glossary

Questions?

Thanks!