SP 800-90C in Depth and Revision

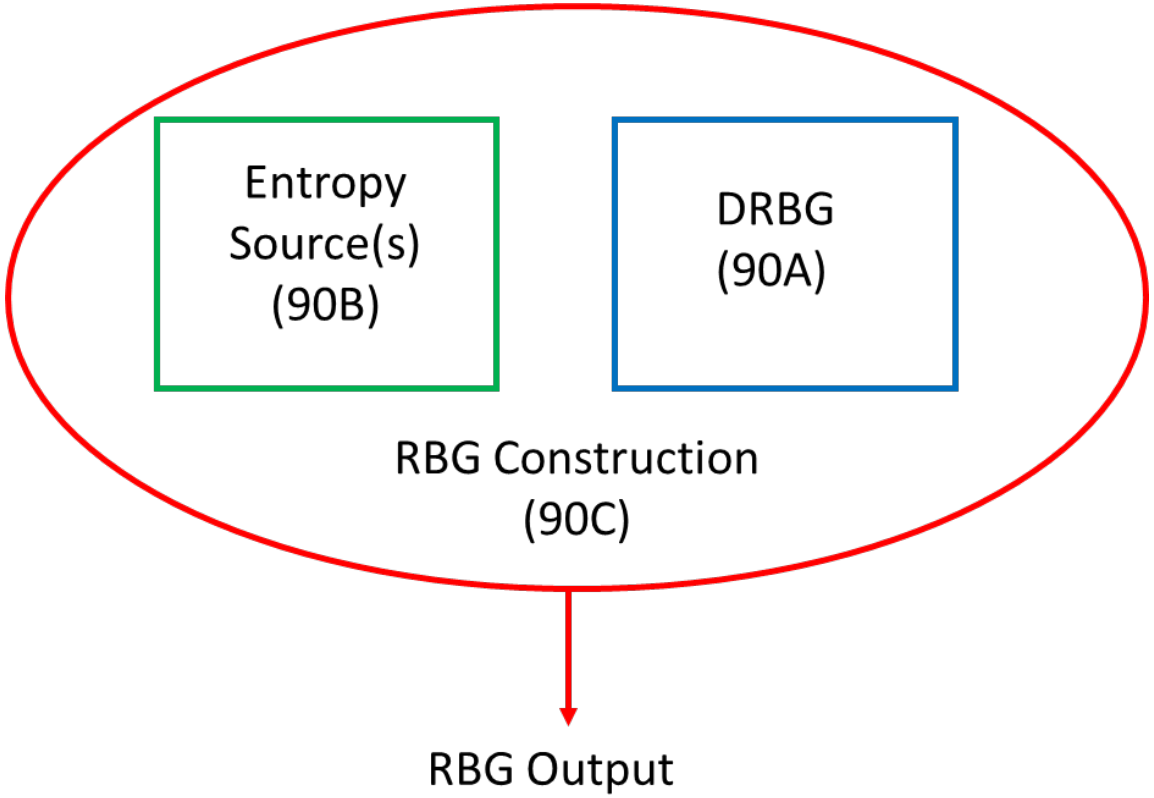
Kerry McKay
RBG Workshop 2023
May 31, 2023

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

ITL INFORMATION TECHNOLOGY LABORATORY

90C Purpose

- SP 800-90C describes random bit generator constructions made from elements described in SP 800-90A and SP 800-90B



RBG Constructions

- Different scenarios for which cryptographic module and RBG boundaries components reside in

- Three RBG construction types specified

Construction	Internal Entropy Source	Prediction Resistance	Full Entropy	Type of Randomness Source
RBG1	No	No	No	Physical
RBG2	Yes	Yes*	No	Physical or non-physical
RBG3	Yes	Yes	Yes	Physical

* If sufficient entropy is available

Sources of Randomness

- 90C expands the sources where credited random bits may be obtained
  - Entropy source(s) may be physical or non-physical
  - Another RBG

- Two methods of crediting entropy
  - Only from physical sources
  - From both non-physical and physical sources

Counting Entropy: Method 1

- RBG includes at least one physical entropy source (might also include more non-physical entropy sources).
- Only the entropy from the physical entropy source(s) is counted.
- Entropy provided by a non-physical entropy source(s) is not counted even if the non-physical entropy source outputs are used.

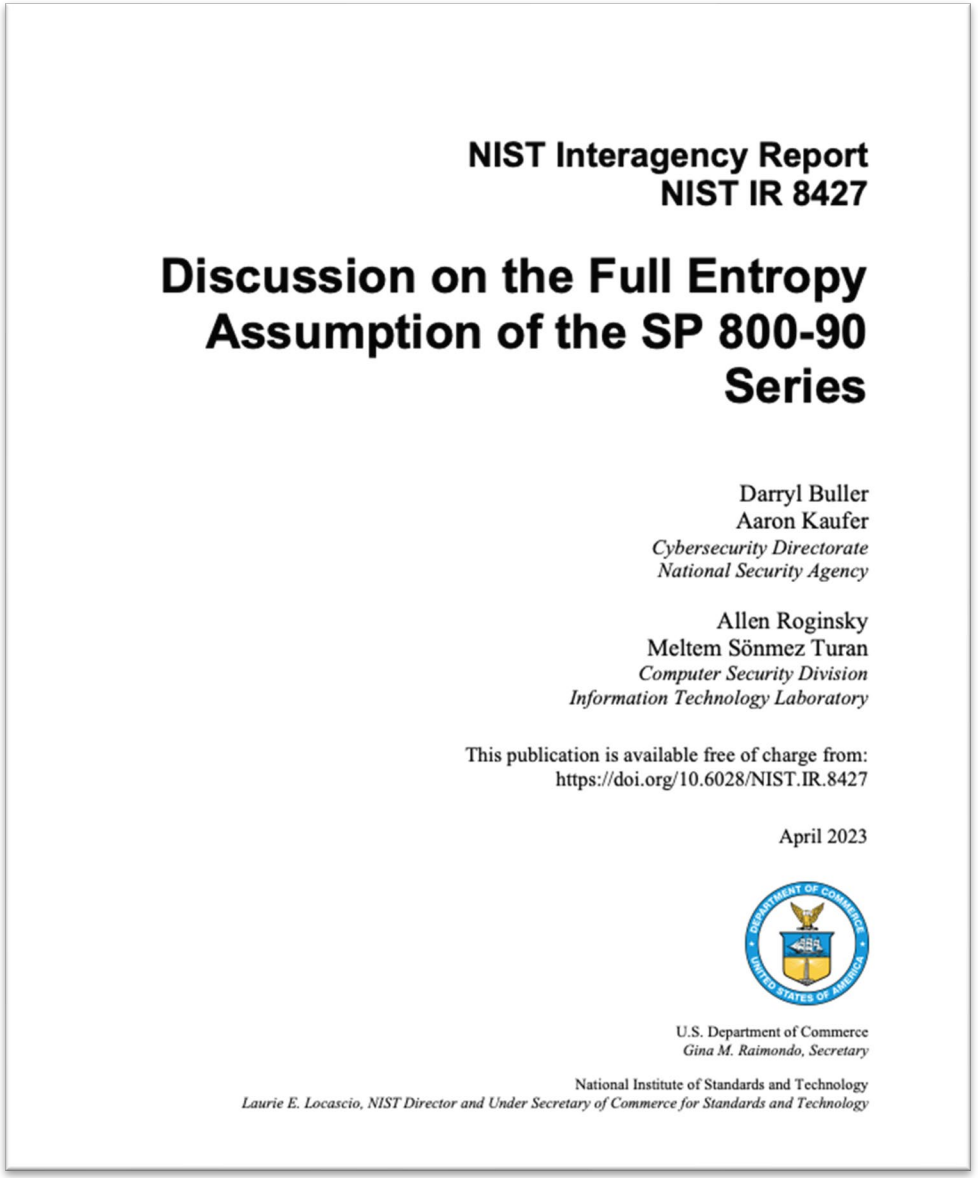
Counting Entropy: Method 2

- RBG includes at least one non-physical entropy source (might also include one or more physical entropy sources).

- The entropy from both non-physical entropy sources and (if present) physical entropy sources is counted when fulfilling an entropy request.

Full Entropy

- A bitstring is considered to have full entropy if the amount of entropy per bit is at least 1 - ϵ, where ϵ is at most 2^{-32}
  - Discussed further in the next talk



NIST Interagency Report
NIST IR 8427

Discussion on the Full Entropy Assumption of the SP 800-90 Series

Darryl Buller
Aaron Kaufer
Cybersecurity Directorate
National Security Agency

Allen Roginsky
Meltem Sönmez Turan
Computer Security Division
Information Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8427

April 2023

U.S. Department of Commerce
Gina M. Raimondo, Secretary

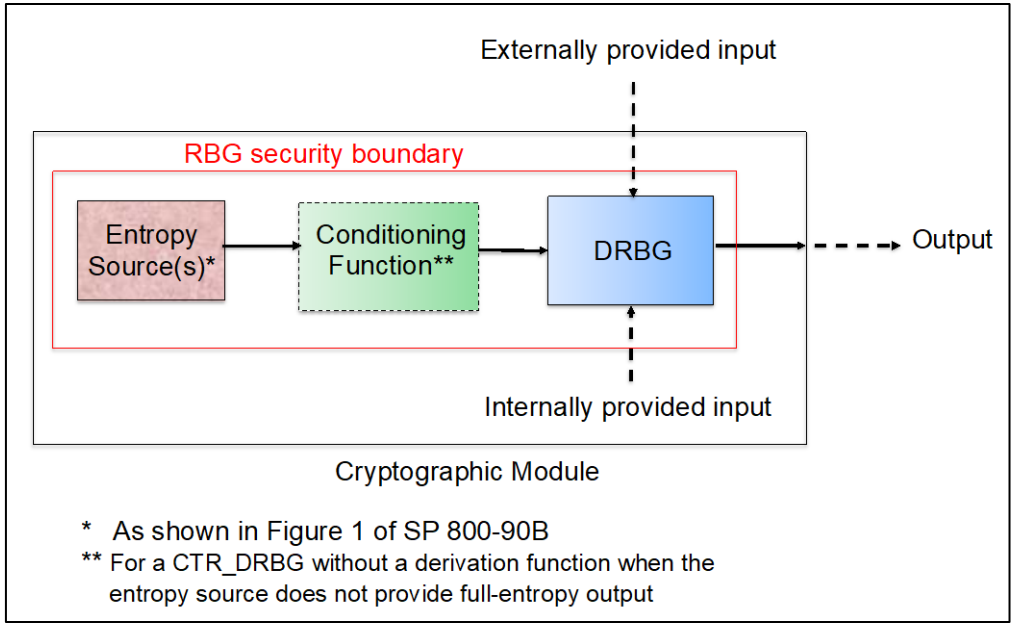
National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

Boundaries and Assumptions

- Security boundaries
  - Cryptographic module boundary contains RBG and other cryptographic functions
  - RBG security boundary inside the cryptographic module boundary

- Assumptions and assertions
  - Entropy sources are independent
  - Randomness input comes only from approved sources of randomness
  - Entropy-source output properties
    - Has a fixed length
    - Has a fixed amount of entropy
    - Can be concatenated, and entropy = sum of the concatenated outputs

RBG2 Construction



- Includes one or more entropy sources
- RBG2(P) uses entropy from one or more physical entropy sources
- RBG2(NP) uses entropy from any validated non-physical or physical entropy sources

- Reseeding support
  - Can provide prediction resistance if sufficient entropy is present
  - The application may not have the ability to request a reseed
- Full-entropy output not provided

External Conditioning

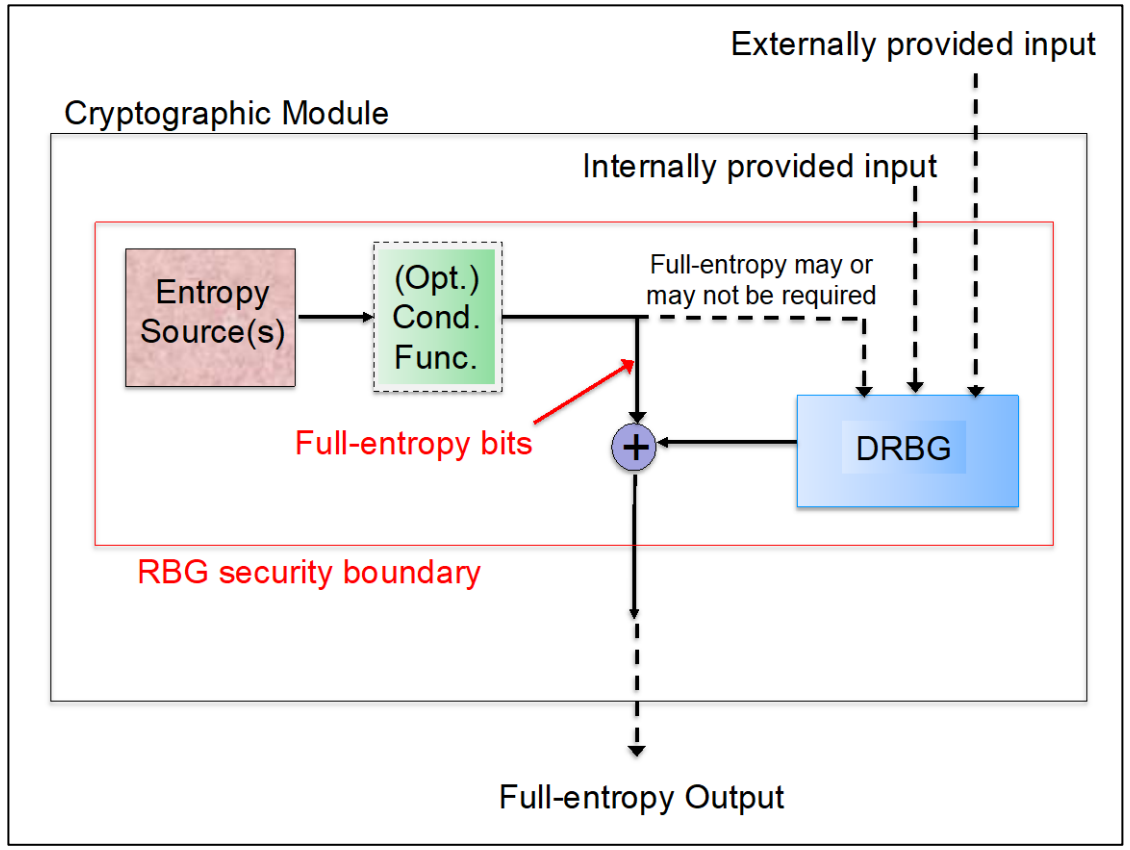
- External conditioning performed on the randomness source output to produce full-entropy bitstring
- Use hash-based and AES-based vetted conditioning functions from (SP 800-90B)

RBG3 Construction

- Constructions with highest security assurances
- Features
  - Includes one or more entropy sources and a DRBG mechanism
    - Entropy only credited from physical sources
  - Designed to continue operation using the DRBG if an entropy-source failure is undetected
  - Direct access to DRBG mechanism
  - Prediction resistance

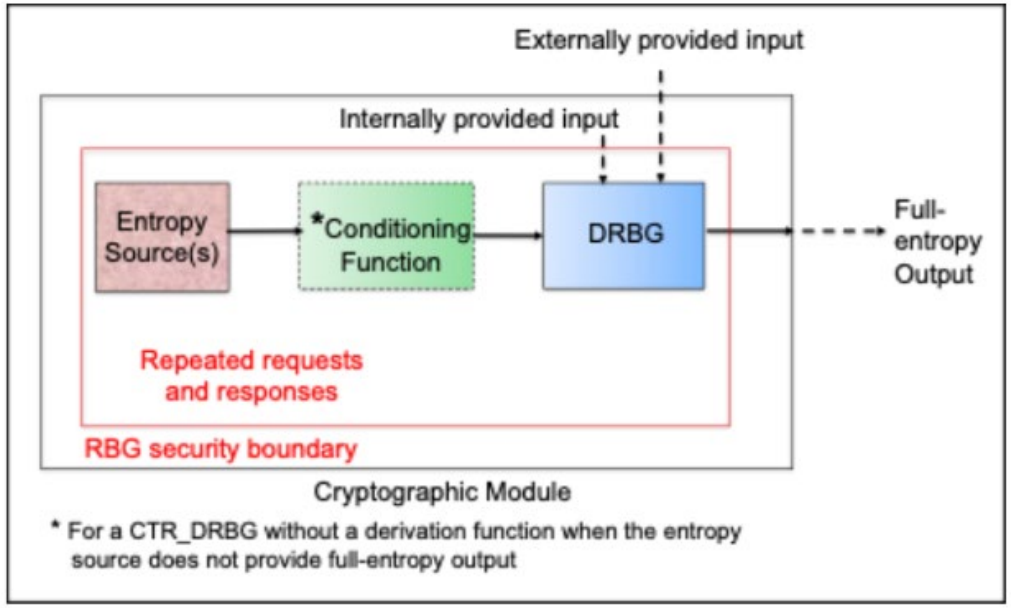
- Two RBG3 constructions:
  - RBG3(XOR)
  - RBG3(RS)

RBG3(XOR) Construction



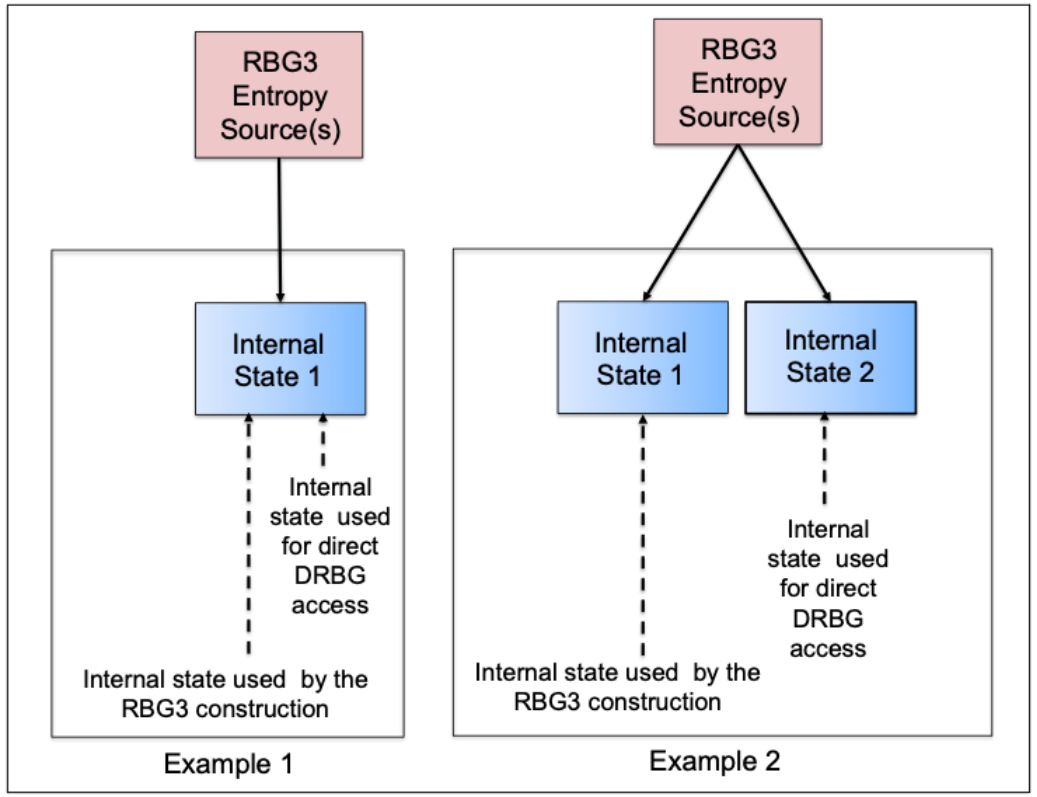
- One or more validated entropy-sources and a DRBG whose outputs are XORed to produce full-entropy output
- DRBG shall be reseeded occasionally
- If entropy sources cannot provide full-entropy output, external conditioning required

RBG3(RS) Construction



- *s* bits with full entropy can be extracted from the DRBG if at least *s* + 64 bits of fresh entropy are inserted into the DRBG before generating the output.
- Entropy can be inserted by reseeding and as additional input obtained directly from the entropy source(s)

Direct DRBG Access

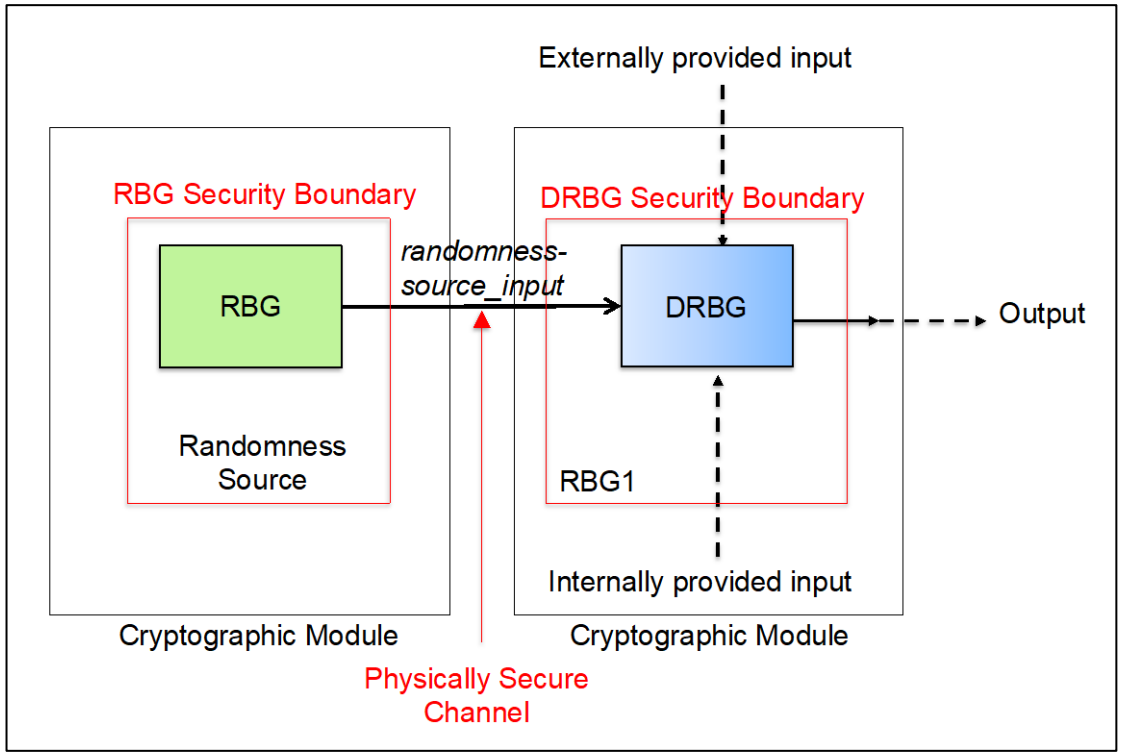


- RBG3 may allow direct access to DRBG implementation(s)
- Direct-access DRBG meets RBG2(P) requirements with reseed function

- RBG3(RS):
  - If prior use of DRBG is from RBG3(RS), the DRBG has to be reseeded before producing output

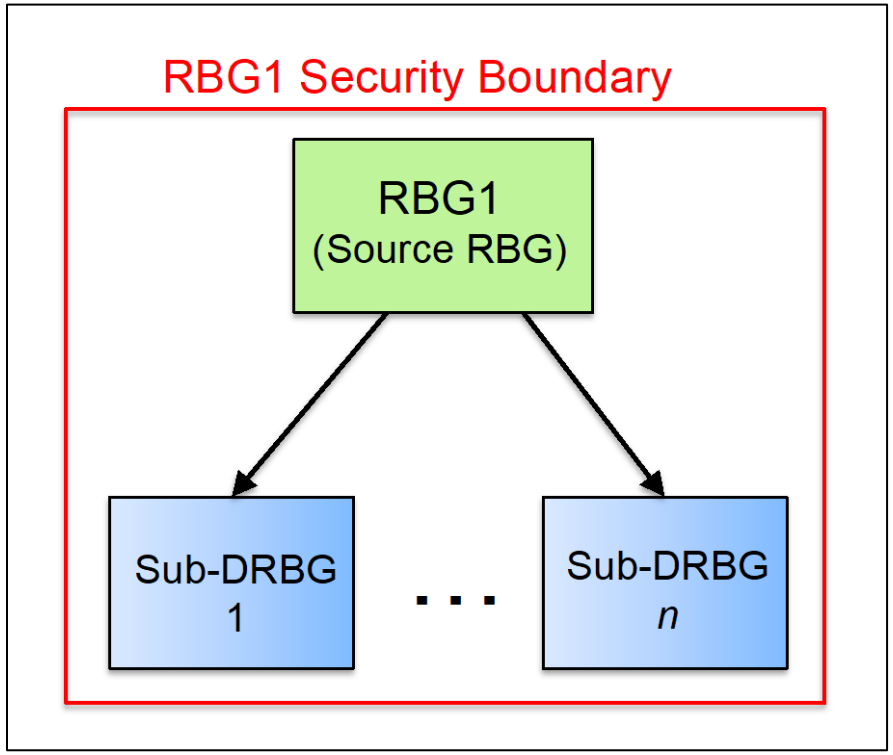
- RBG3(XOR) and RBG3(RS):
  - Reseed DRBG periodically (e.g., a predetermined period of time or number of generation requests)

RBG1 Construction



- No internal randomness source
- Seeded by external RBGs with physical entropy sources (RBG2(P) or RBG3) via a physical secure channel
- Can only be instantiated once, never reseeded

RBG1 Sub-DRBGs



- RBG1 construction can instantiate one layer of subordinate DRBGs (Sub-DRBG)
- Sub-DRBGs reside in the same security boundary as the RBG1 source
- Sub-DRBG output shall not provide input for the RBG1 source

Additional topics

- Testing: Health and implementation validation
- Appendices:
  - Entropy vs. security strength
  - Examples
  - Addendum for SP 800-90A: Instantiating and reseeding a CTR_DRBG

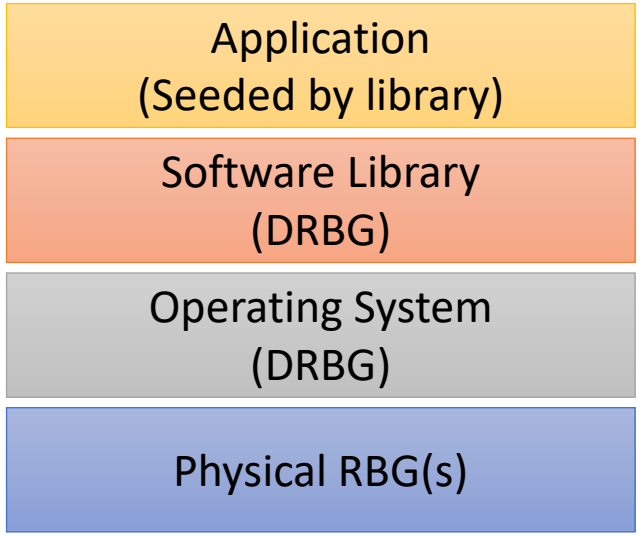
Public Comments

Public Comment Highlights

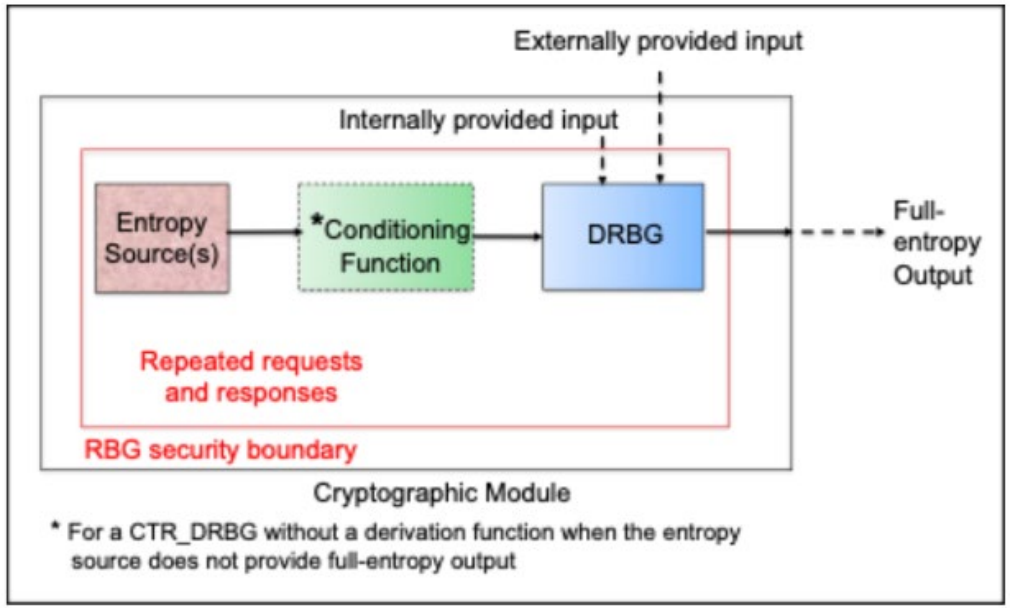
- 90c in public comment period from September 7, 2022 to December 7, 2022
- Received about 75 public comments from eight sources
- Covered many topics, including:
  - Requests for additional constructions (e.g., chained DRBGs, no DRBG)
  - Requests for additional information (e.g., rationale, justifications)
  - RBG termination upon entropy source failure
  - Entropy calculations
  - Editorial

Chained DRBGs

- Critical need for chained DRBGs
  - Current draft does not include DRBG seeded by other DRBGs
- Will be discussed further in presentation tomorrow



Entropy Input for RBG3(RS)

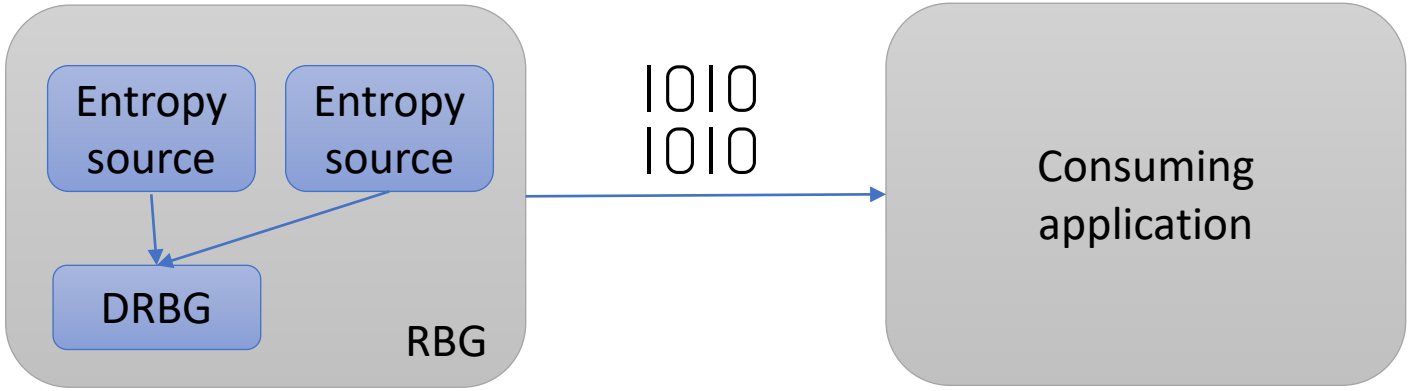


- Reseed DRBG with *s*+64 bits of min-entropy
  - Reseed normally gets only *s* bits on min-entropy
- Multiple requests for entropy required
- Could use additional input to obtain required entropy in fewer calls

More on this tomorrow

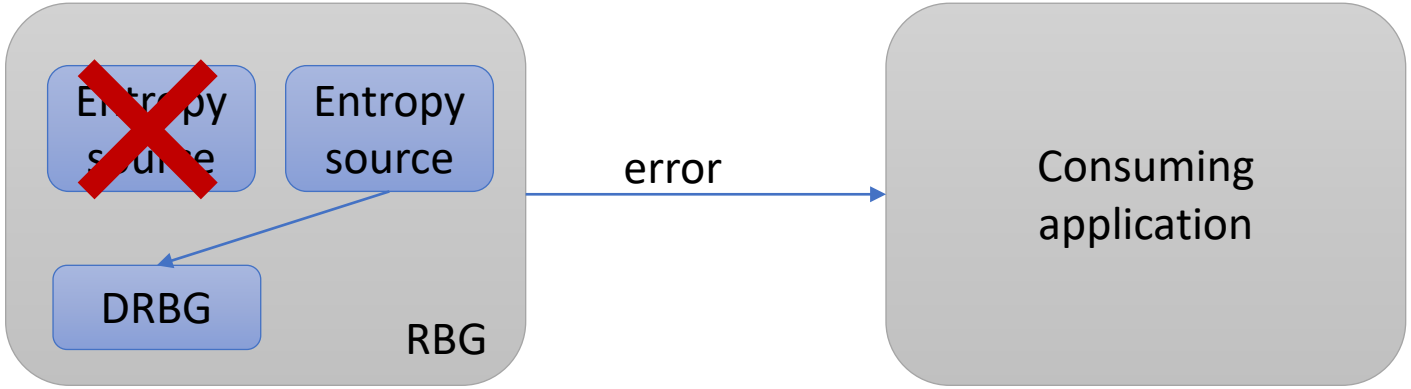
Entropy Source Failure

- In an RBG with single entropy source, RBG operation terminates when entropy source fails
- What happens when one of multiple entropy sources fail?



Entropy Source Failure

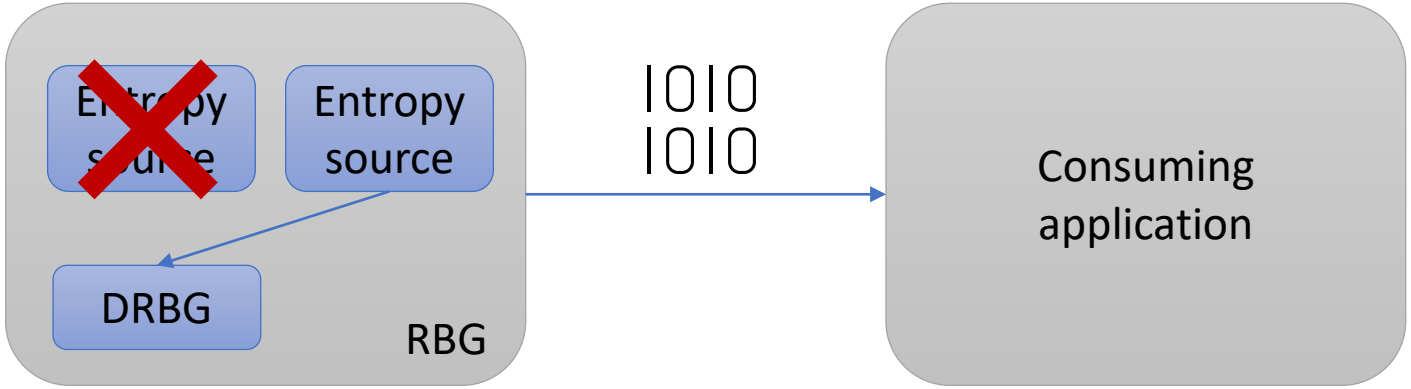
- What happens when one of multiple entropy sources fail?



Entropy Source Failure

- What happens when one of multiple entropy sources fail?

Terminate use of failed sources, but continue to use others (if present)

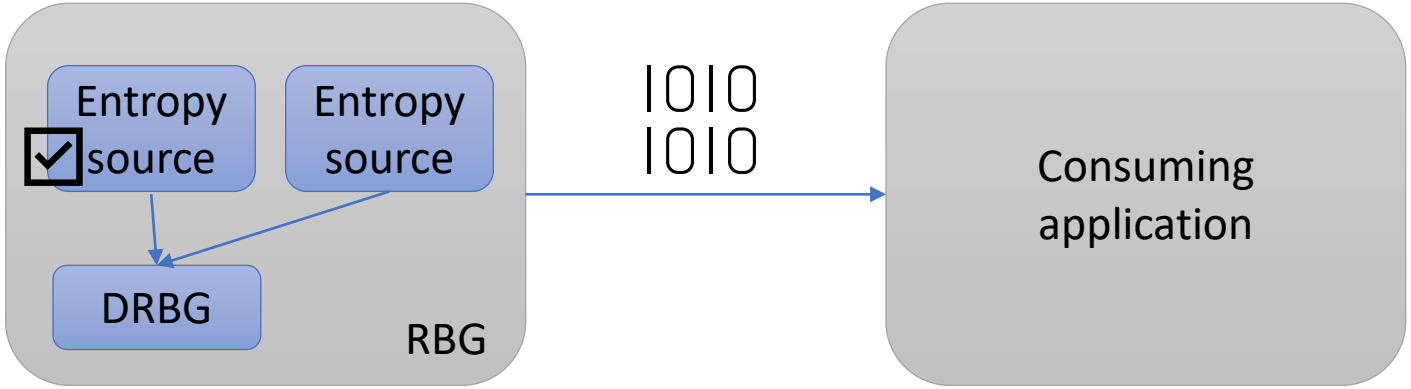


Entropy Source Failure

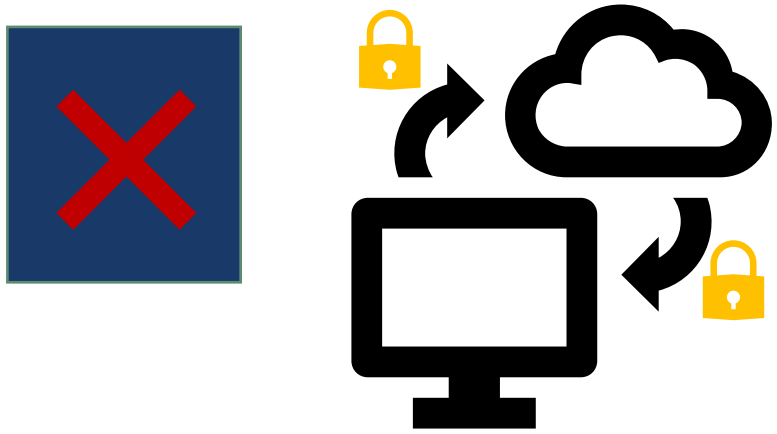
- What happens when one of multiple entropy sources fail?

Resume use of entropy source when:

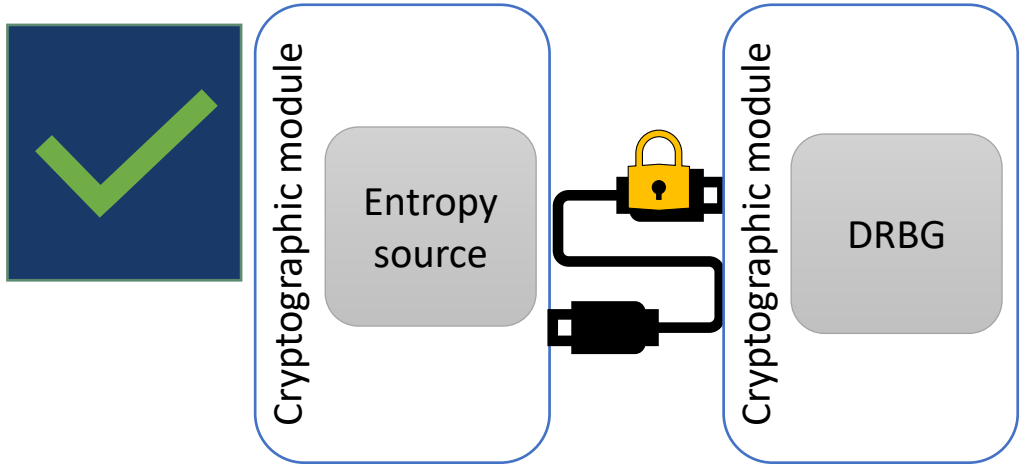
- Conditions that caused the failure corrected; and
- Tested for successful operation



Secure Channel



- **Not** a channel whose security relies entirely on cryptography



- A physically protected secure path for transferring data between two cryptographic modules
- Ensures confidentiality, integrity, and replay protection
- Mutual authentication between the modules

Next Steps

- Update document to address public comments
- At this point, undecided whether next version will be:
  - Draft that includes DRBG chains; or
  - Final with a placeholder for DRBG chains
    - Add later through revision or addendum
- Please join open discussion tomorrow to share your thoughts on this and other issues

Questions?

Thanks!