SP 800-90C: Random Bit Generator Constructions

Elaine Barker

NIST

May 2, 2016

Purpose of 800-90C:

- To construct RBGs from **approved** entropy sources (see SP 800-90B) and DRBG mechanisms (see SP 800-90A)
  - DRBGs (a.k.a. pseudorandom number generators)
  - NRBGs (a.k.a. true random number generators)
- To specify health and validation testing requirements

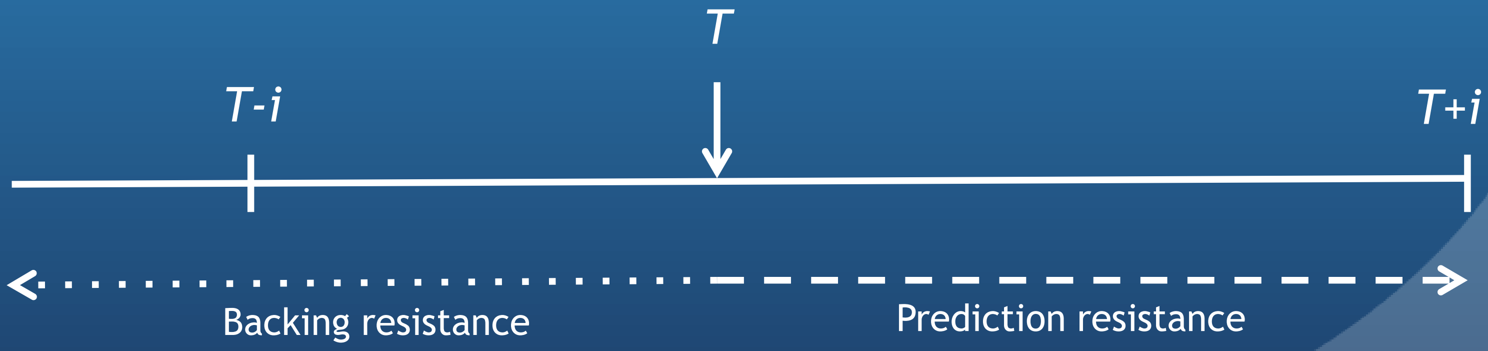
Assumptions (see Section 4.2):

- Each entropy source output has a fixed length and a fixed amount of entropy
- Entropy source outputs from the same source or multiple independent sources can be concatenated and the entropy added
- Entropy sources can provide indications of successes and failures
- Entropy source output can be conditioned to reduce bias or condense into a shorter bitstring
- Vetted conditioning functions can provide full-entropy output if *entopy_in* ≥ 2 × **min**(*narrowest_internal_width*, *output_length*);

  Note: for the vetted conditioning functions, *narrowest_internal_width* = *output_length*
- SP 800-90A DRBG mechanisms meet their security claims (e.g., claimed security strengths)

Definitions

- Backtracking Resistance: Knowledge of the state at time *T* cannot be used to determine states prior to time *T*
- Prediction Resistance: The insertion of fresh entropy at time *T* disallows determining the state at time *T* and *T+i* when any state prior to time T is known



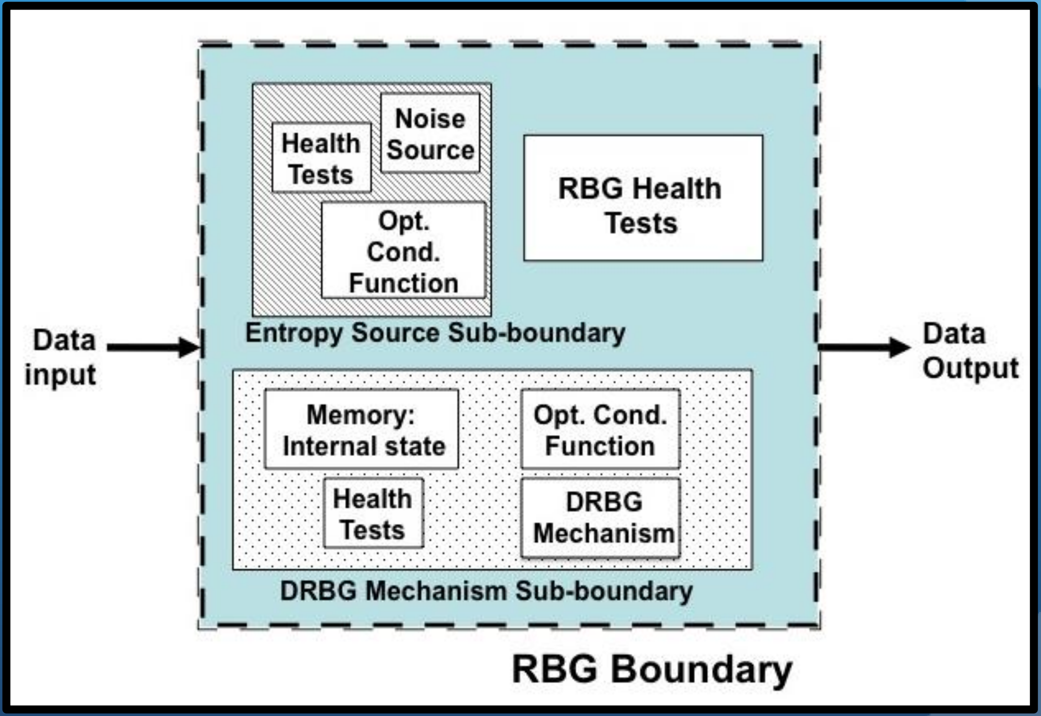
Definitions (contd.)

- Secure channel: A data path that ensures confidentiality, integrity, replay protection and mutual authentication
- Full entropy: Every bit of a bitstring has one bit of entropy; $\mathit{entropy\_in} \geq 2n$, where n is the size of the output

RBG Concepts:

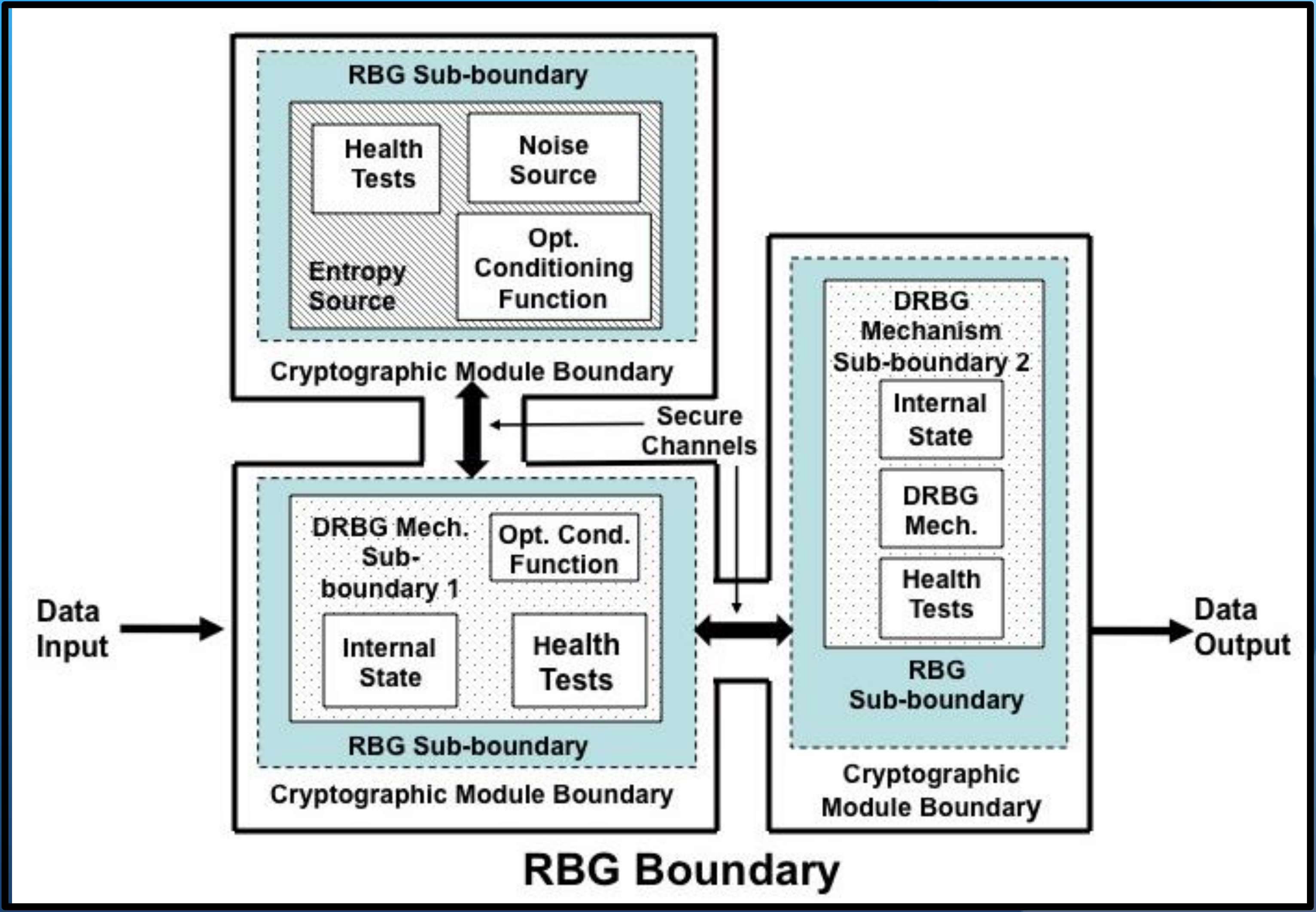
- Single and distributed boundaries (conceptual)

RBG within A Single Cryptomodule:



Cryptographic Module Boundary

Distributed RBG over Multiple Cryptomodules

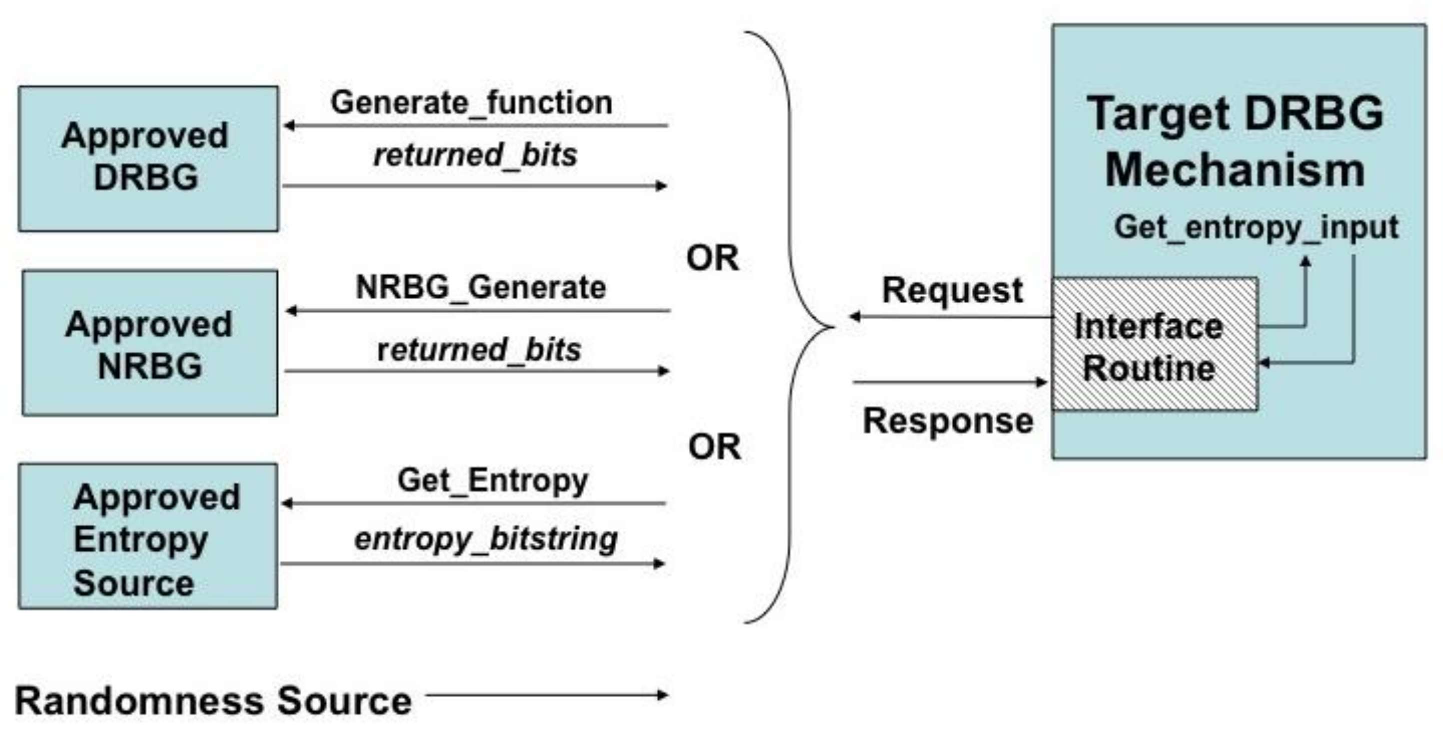


Concepts (contd.):

- Randomness source
  - Entropy source, RBG (DRBG or NRBG) or chain of RBGs
- Live Entropy Source: available when needed
- External conditioning on entropy-source output using vetted functions
- Prediction resistance: obtain fresh entropy from an entropy source (using a reseed capability)
- (Enhanced) NRBG (i.e., DRBG mechanism provided as a fallback)

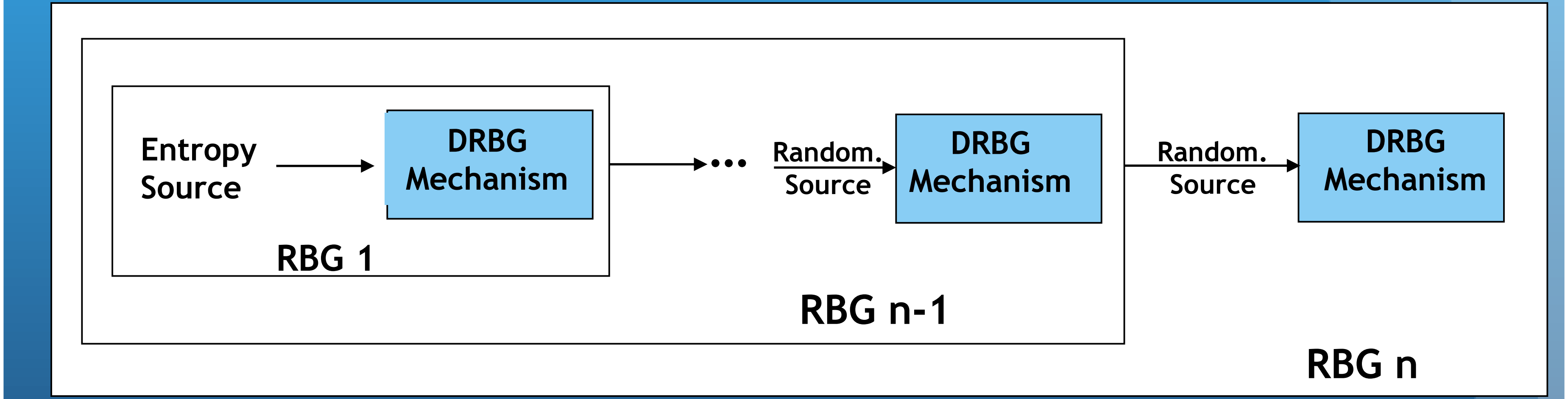
DRBG Randomness Sources:

- Randomness source only required for instantiation
- Live entropy source allows prediction resistance
- Reseed from any randomness source



DRBG Chain:

DRBG Chain



Which Randomness Sources?

Randomness Source	Purpose			
	Provide NRBG output	Instantiate Target DRBG	Reseed Target DRBG	Provide prediction resistance from Target DRBG
Entropy Source	Yes	Yes	Yes	Yes
NRBG*	---	Yes	Yes	Yes
DRBG (live entropy source available)	---	Yes	Yes	Yes
DRBG (NO live entropy source available)	---	Yes	Yes	No

* Includes an entropy source

DRBG Capabilities, Given the Availability of a Randomness Source:

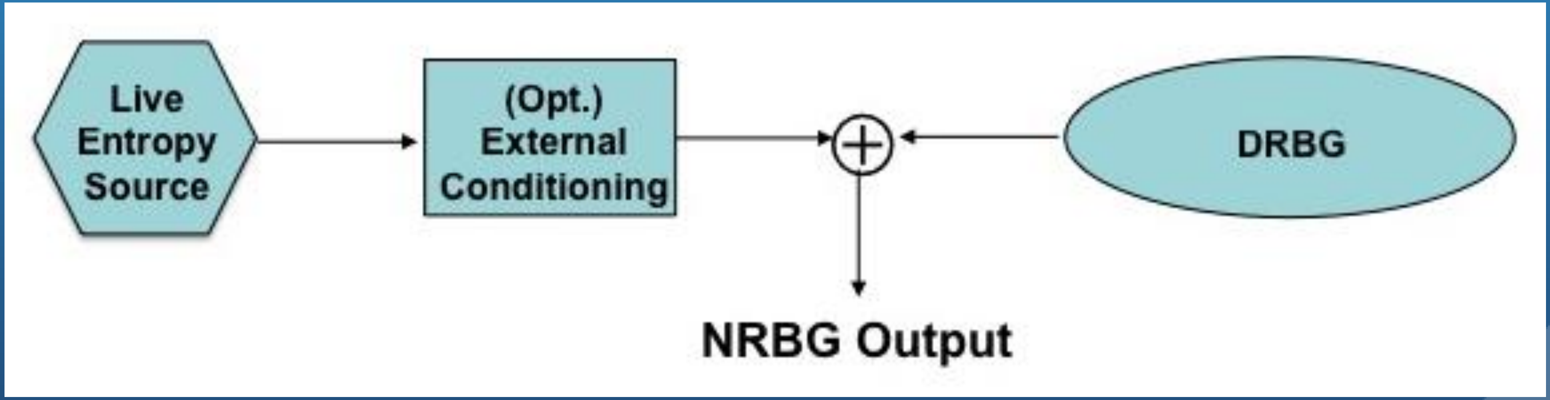
Randomness Source Availability	Live Entropy Source?	Comments
When required	Yes	The randomness source is an entropy source, an NRBG, or a source DRBG with access to a Live Entropy Source. A DRBG can be instantiated, generate bits, be reseeded, and provide prediction resistance.
When required	No	The randomness source is a source DRBG with no access to a Live Entropy Source. A DRBG can be instantiated, generate bits, and be reseeded, but cannot provide prediction resistance.
During instant. only	No	The randomness source is an entropy source, an NRBG, or a source DRBG with or without access to a Live Entropy Source. A DRBG can be instantiated and generate bits, but cannot be reseeded or provide prediction resistance.

NRBGs:

- Two constructions: XOR and Oversampling
- Live Entropy Source always required and used
- Approved DRBG mechanism required for the (enhanced) NRBG
  - Instantiated at the highest security strength possible
  - Fallback if an undetected entropy source failure
  - DRBG can be accessed directly (same or different instantiation)
- Provides full-entropy output
- Backtracking and prediction resistance always provided

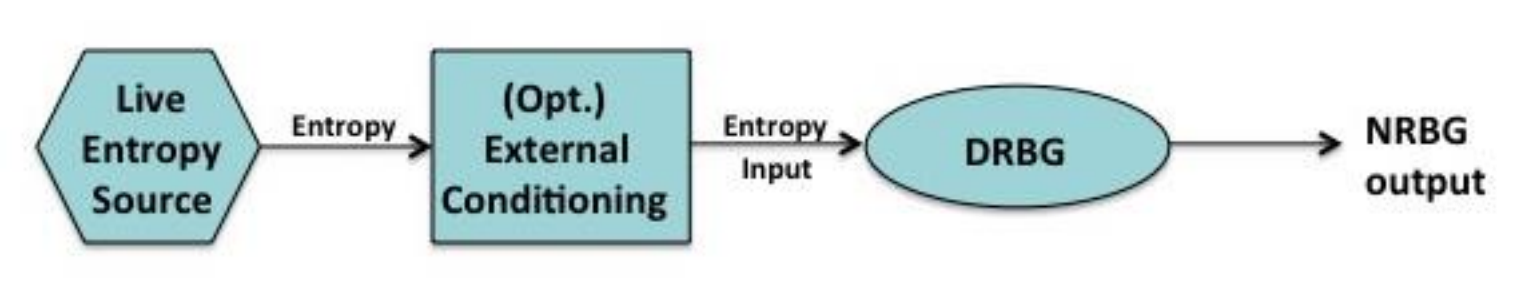
NRBGs: XOR Construction

- Requires full entropy (on the left side of the figure)
- External conditioning required if entropy source does not provide full entropy output (i.e., not optional in this case)



NRBGs: Oversampling Construction

- Entropy source need not provide full entropy output
- External conditioning can reduce entropy source bias, shorten entropy source output or provide full entropy, if desired



Additional Constructions:

- Get_entropy_input specifications to access randomness sources:
  - ○ Using a DRBG (with and without a prediction resistance capability)
  - ○ Using an NRBG
  - ○ Using an entropy source
    - ✓ The Get_Entropy call (i.e., interface with the entropy source capability); includes condensing constructions
    - ✓ With and without external conditioning
- Obtain full-entropy output from a DRBG with prediction resistance

Other Stuff:

- Combining RBGs: At least one must be approved
- Health testing
    - At startup and on-demand (entropy sources also have continuous tests)
    - Test whatever components are available
    - Enter an error state when an error is reported
        - ✓ Notify the consuming application
        - ✓ Consuming application then responsible for handling the error (e.g., request user guidance or prevent further RBG requests)

Other stuff (contd.):

- Implementation Validation
  - Validate 90A and 90B components
  - Validate 90C constructions (e.g., conditioning functions)
  - Documentation requirements (e.g., DRBG or NRBG, features supported, if the RBG is distributed)
- Examples:
  - XOR-NRBG
  - Oversampling NRBG
  - DRBG without a Randomness Source (after instantiation)
  - DRBG with a Live Entropy Source

SP 800-90C Availability

- SP 800-90C available for public comment at http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-90-C.
- Comments requested by June 13, 2016.
- Send comments to rbg_comments@nist.gov, with "Comments on Draft SP 800-90C" on the subject line.

Questions?

- Note that further RBG discussions will be held at the end of the workshop on Tuesday.