Random Bit Generator Constructions

Elaine Barker

NIST

December 5, 2012

Background

- Started in 1998 in ASC X9F1 (Financial Services sub-committee)
- Being published in ANSI as ANS X9.82 (4 parts)
- Being published by NIST as SP 800-90 (3 parts)

Subject	NIST SP 800-90	ASC X9.82
Overview and Basic Principles		Part 1
Entropy Sources	90B	Part 2
Deterministic Random Bit Generators (DRBGs)	90A	Part 3
RBG Constructions (DRBGs and NRBGs)	90C	Part 4

SP 800-90C and X9.82, Part 4: RBG Constructions

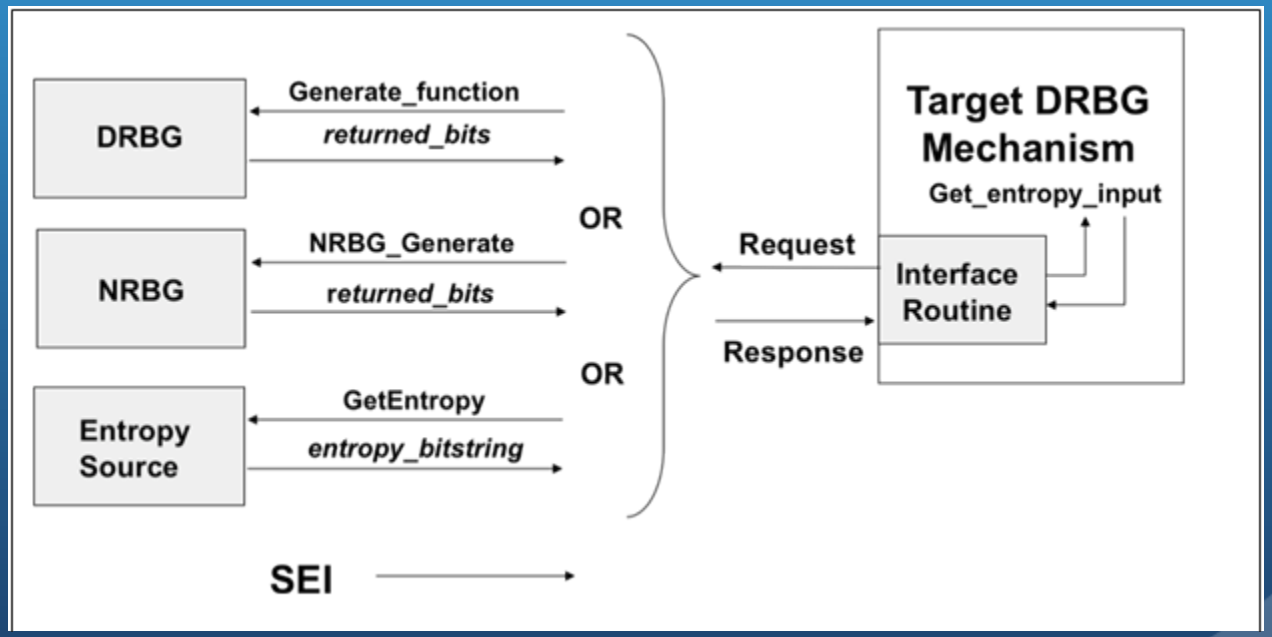
- Provided for public comment in September; comments due on December 5, 2012
- Purpose: To construct RBGs from **approved** entropy sources (see 800-9B) and DRBG mechanisms (see 800-90A)
  - DRBGs (a.k.a. pseudorandom number generators)
  - NRBGs (a.k.a. true random number generators)
- Extract of X9.82, Part 4; most constructions included

RBG Constructions (contd.)

- Concepts
  - (Conceptual) single and distributed boundaries
  - Live entropy sources: available when needed
  - Prediction resistance: obtain fresh entropy
  - Enhanced NRBG (i.e., DRBG mechanism provided as a fallback)
  - Sources of entropy input (SEI)
    - Entropy source
    - RBG (DRBG or NRBG)
    - Chain of RBGs

DRBGs

- With or without a live entropy source
- Live entropy source allows prediction resistance

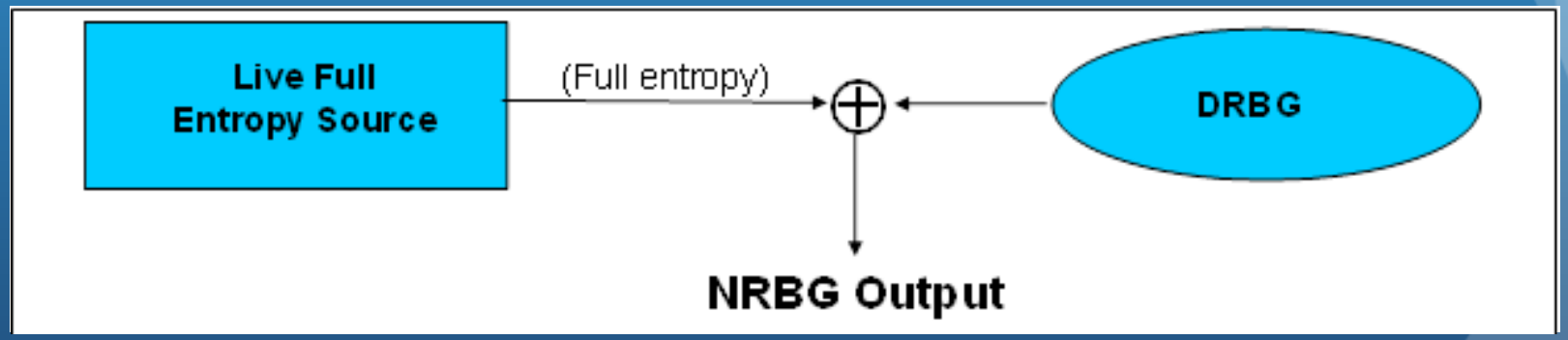


NRBGs

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

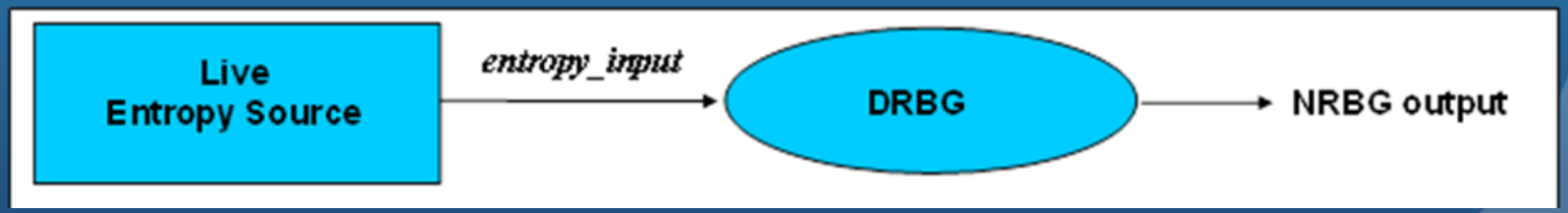
NRBGs: XOR Construction

- Requires full entropy source
- Entropy used to seed the DRBG not used for other purposes



NRBGs: Oversampling Construction

- Entropy source need not provide full entropy output
- Entropy_input = 2*n*; entropy output = *n*



RBG Constructions (contd.)

- Additional constructions
  - Using an RBG as an SEI
  - Using an entropy source as an SEI
- Testing
  - Health testing
  - Implementation validation
- RBG configurations
  - NRBGs: XOR and oversampling constructions
  - DRBGs: With and without a live entropy source
  - More complete examples in X9.82, Part 4

Issues

- How would we specify a “basic” NRBG (i.e., without a DRBG mechanism) and maintain assurance of good output?