SP 800-90C in Depth and Revision

Kerry McKay
RBG Workshop 2023
May 31, 2023
SP 800-90C describes random bit generator constructions made from elements described in SP 800-90A and SP 800-90B.
Different scenarios for which cryptographic module and RBG boundaries components reside in

Three RBG construction types specified

<table>
<thead>
<tr>
<th>Construction</th>
<th>Internal Entropy Source</th>
<th>Prediction Resistance</th>
<th>Full Entropy</th>
<th>Type of Randomness Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>RBG1</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Physical</td>
</tr>
<tr>
<td>RBG2</td>
<td>Yes</td>
<td>Yes*</td>
<td>No</td>
<td>Physical or non-physical</td>
</tr>
<tr>
<td>RBG3</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Physical</td>
</tr>
</tbody>
</table>

* If sufficient entropy is available
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
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.
• 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.
A bitstring is considered to have full entropy if the amount of entropy per bit is at least $1 - \varepsilon$, where $\varepsilon$ is at most $2^{-32}$.

- Discussed further in the next talk.
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 performed on the randomness source output to produce full-entropy bitstring

• Use hash-based and AES-based vetted conditioning functions from (SP 800-90B)
• 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)
• 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
• 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
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
In an RBG with single entropy source, RBG operation terminates when entropy source fails.

What happens when one of multiple entropy sources fail?
What happens when one of multiple entropy sources fail?
• What happens when one of multiple entropy sources fail?

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