Update on NIST SP 800 90C
Recommendation for Random Bit Generator (RBG) Constructions

Meltem Sönmez Turan, NIST
April 28, 2021

National Institute of Standards and Technology
U.S. Department of Commerce

INFORMATION TECHNOLOGY LABORATORY

SP 800-90C Drafts

First draft Elaine Barker and John Kelsey, August 2012

https://csrc.nist.gov/csrc/media/publications/sp/800-90c/draft/documents/draft-sp800-90c.pdf

Second draft Elaine Barker and John Kelsey, April 2016

https://csrc.nist.gov/CSRC/media/Publications/sp/800-90c/draft/documents/sp800_90c_second_draft.pdf

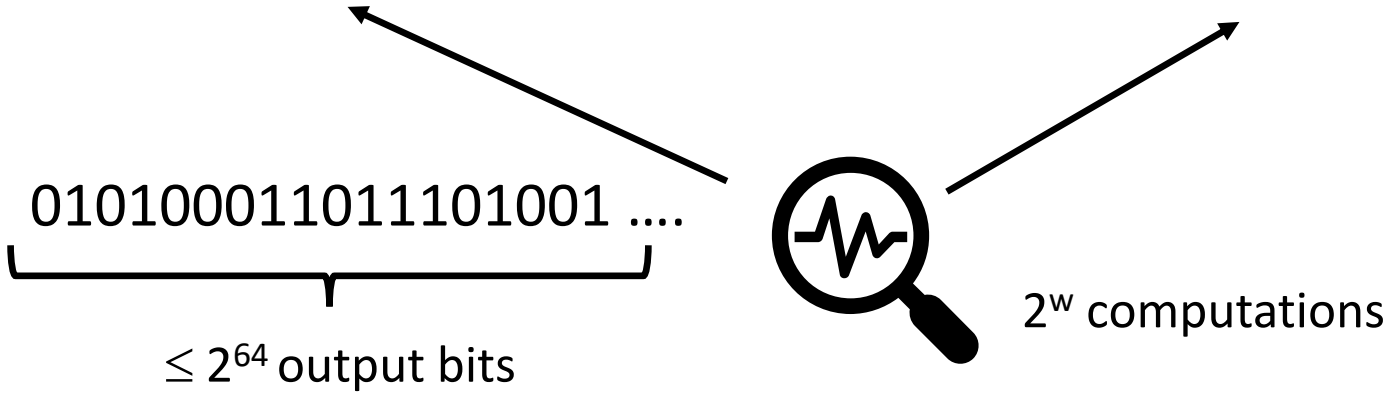
Third draft Elaine Barker, John Kelsey, Allen Roginsky, Meltem Sonmez Turan, Darryl Buller, Aaron Kaufer (TBD 2021)

DISCLAIMER : Some of the details presented may be subject to chance.

RBG Security

Ideal random sources generate full-entropy outputs.

RBGs are designed with a security goal of *indistinguishability* from an ideal random source.



Probability of success is $\leq \frac{1}{2} + 2^{w-s-1} + \varepsilon$, $\varepsilon \leq 2^{-32}$

An RBG with a security strength of *s* bits is suitable for any application with a targeted security strength that does not exceed *s* (e.g. 128, 192 or 256).

RBG Constructions

Method of designing an RBG or some component of an RBG to accomplish a specific goal.

Each RBG includes

- a DRBG from SP 800-90A and
- a validated entropy source from SP 800-90B.

90C defines three RBG constructions : RBG1, RBG2 and RBG3.

Entropy Sources

Physical entropy source (PES) if the primary noise source of the entropy source is physical i.e., using dedicated hardware (e.g., ring oscillators, thermal noise, shot noise, jitter, or metastability).

Non-physical entropy source (NPES) if the primary noise source of the entropy source is non-physical, i.e., entropy is provided by system data (e.g., the entropy present in the output of API functions, RAM data, or system time).

Entropy assessment – Method 1

RBG includes at least one physical entropy sources (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.

Entropy assessment – Method 2

RBG includes at least one non-physical entropy sources (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.

Example

RBG consists of one PES and one NPES.

pes_i : i^{th} output of a PES, and $npes_i$: i^{th} output of an NPES.

Request for 128 bits of entropy, the concatenated bitstring might be something like:

- $pes_1 || pes_2 || npes_1 || pes_3 || \ldots || npes_m || pes_n$,

Method 1 only considers the entropy in pes_1, pes_2, ..., pes_n

Method 2 considers all the entropy in pes_1, pes_2, ... pes_n and in $npes_1$, $npes_2$, ..., $npes_m$ is counted.

Assumptions (1 of 2)

- An entropy source is independent of another entropy source if their security boundaries do not overlap (e.g., they reside in separate cryptographic modules), and there are no common noise sources.

- The entropy-source and RBG output is at most 2^{64} bits.

- Entropy-source outputs has a fixed length, and each entropy-source output contains fixed amount of entropy, that was assessed during entropy-source implementation validation. This is assumed to be at least 0.1 bits per bit of output.

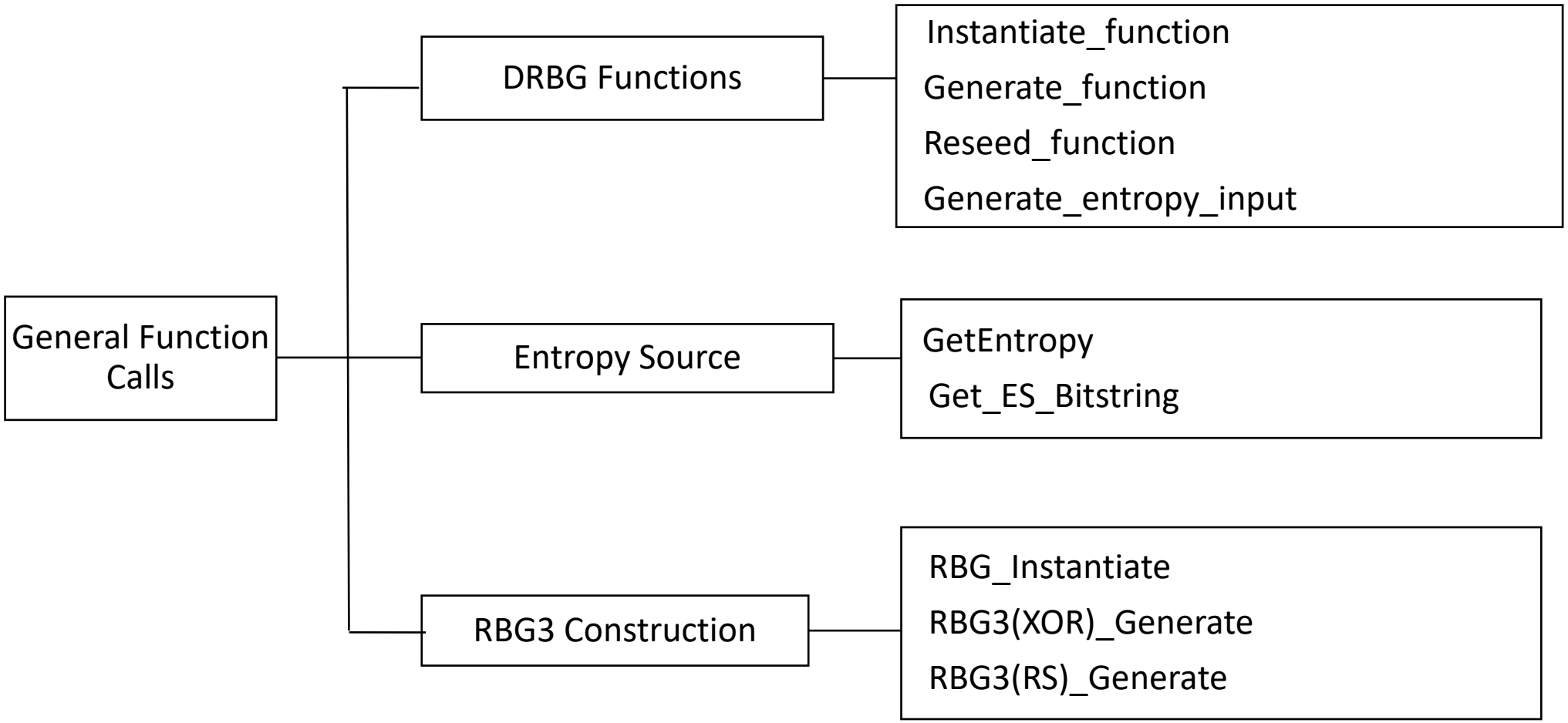
- Each entropy source has been characterized as either a *physical entropy source* or a *non-physical entropy source* upon successful validation.

Assumptions (2 of 2)

- To obtain n full-entropy bits in the output block of a cryptographic primitive, at least $n + 64$ bits of entropy are required as input to the primitive.
  - Example to obtain 256 full-entropy bits from a SHA-256 operation, a bitstring with at least 320 bits of entropy is required as input to the operation.

- To instantiate a DRBG at a security strength of s bits,
  - a bitstring at least $3s/2$ bits long is needed from a randomness source for an RBG1 construction,
  - a bitstring with at least $3s/2$ bits of entropy is needed from an entropy source for an RBG2 or RBG3 construction.

Function Calls

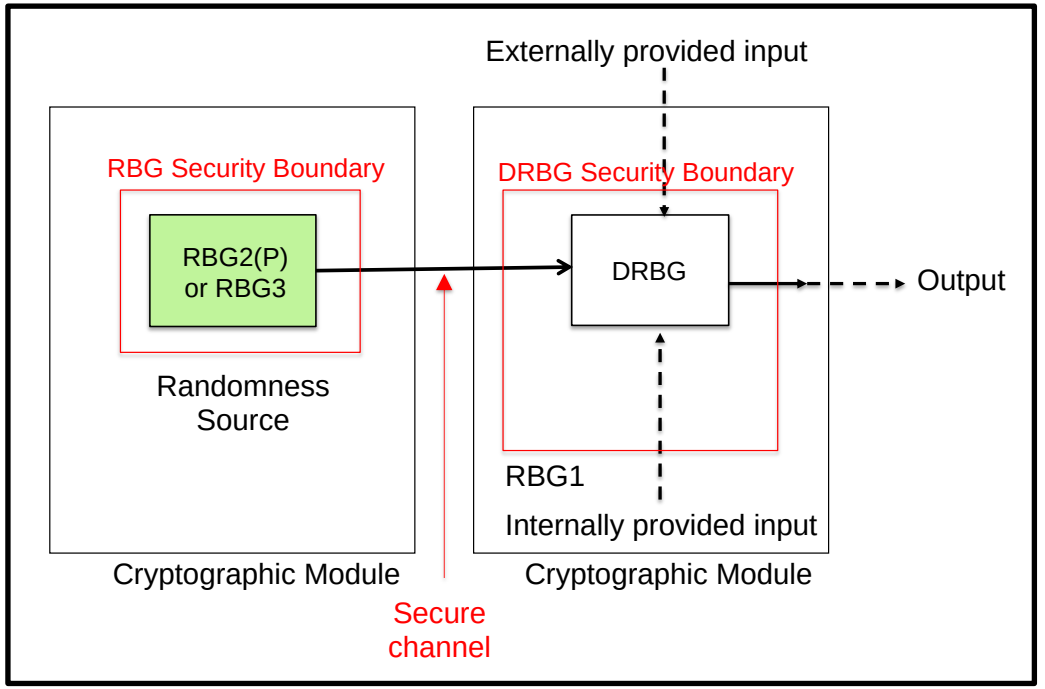


RBG1

An RBG1 construction does not have access to a randomness source after instantiation.

It is instantiated once in its lifetime over a secure channel from an external RBG with appropriate security properties.

- does not support reseeding
- does not provide *prediction resistance*



RBG1 Requirements (not exhaustive)

- Uses an approved DRBG from 90A.
- Shall not produce any output until it is instantiated.
- Shall not permit itself to be instantiated more than once.
- Shall not provide output for generate requests specifying a security strength greater than the instantiated security strength of the DRBG.
- When s bits of security strength is targeted,
  - 3s/2 bits of entropy is used for Hash_DRBG, HMAC_DRBG, CTR_DRBG (with a derivation function)
  - S+128 bits of entropy is used for CTR_DRBG (without a derivation function)
- RBG2(P) or RBG3 construction is used as a randomness source.

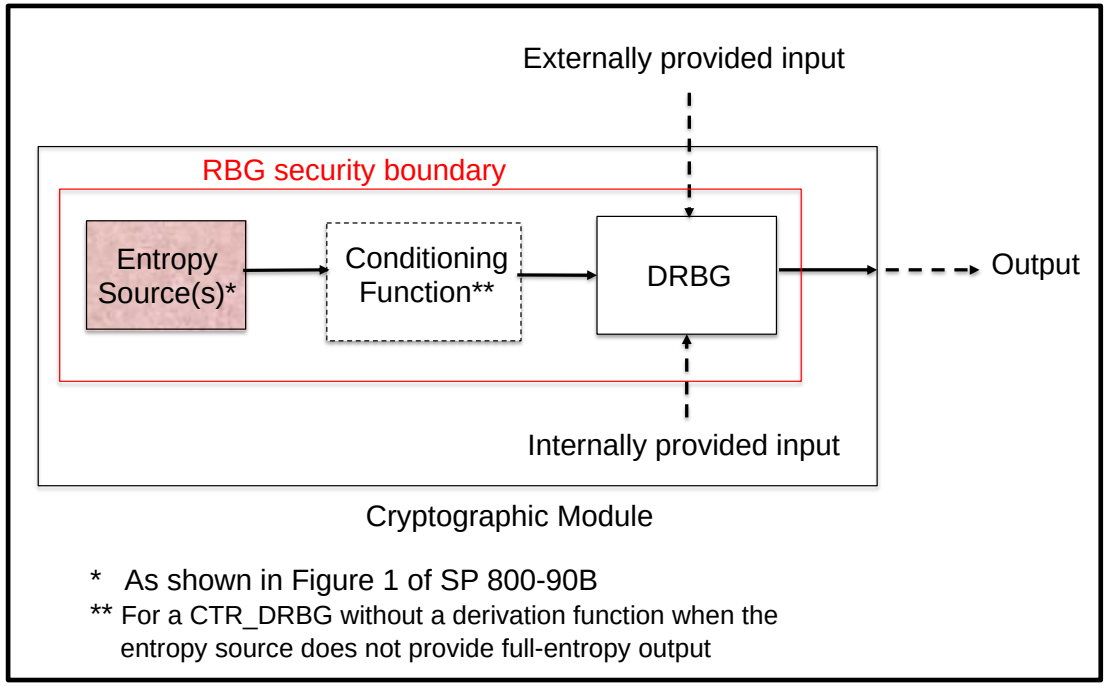
RBG2

RBG2 construction has continuous access to one (or more) validated entropy sources within its RBG security boundary.

- Provides prediction resistance

Two types

- RBG2(P) uses at least one physical source , uses Method 1
- RBG2(NP) uses at least one non-physical source, uses Method 2



RBG2 Requirements (not exhaustive)

- Uses approved DRBG from 90A and validated entropy source from 90B.
- Includes reseeding capability to support prediction resistance.
- Validated entropy source(s) shall be used to instantiate and reseed the DRBG. A non-validated entropy source(s) shall not be used for this purpose
- To instantiate the DRBG at a security strength of s bits.
  - $(s + 128)$ bits with full entropy is used for CTR_DRBG without a derivation function
  - at least $3s/2$ bits of entropy is used for Hash_DRBG, HMAC_DRBG or CTR_DRBG (with a derivation function)

RBG3

RBG3 construction is designed to provide a full entropy.

Two types:

- RBG3(XOR) construction is based on combining the output of one or more validated entropy sources with the output of an instantiated, **approved** DRBG using an XOR operation.
- RBG3(RS) construction is based on using one or more validated entropy sources to provide entropy input for the DRBG by continuously reseeding.

RBG3 Requirements (not exhaustive)

- Only entropy obtained from physical entropy sources are counted towards fulfilling entropy request.
- Only validated entropy sources are used to provide the entropy.

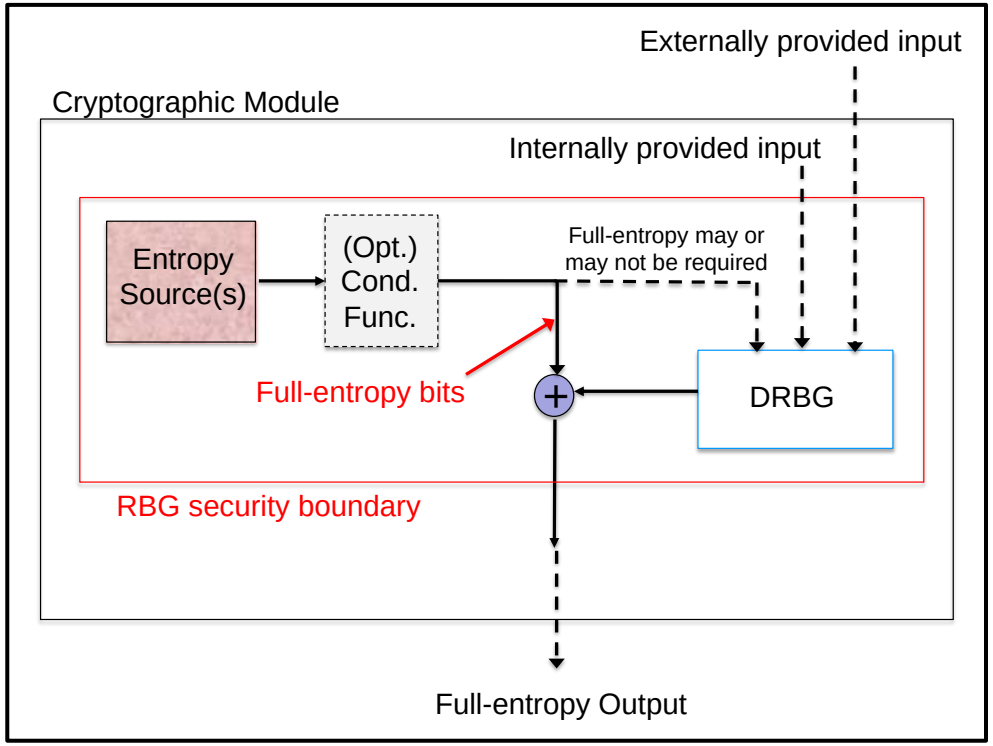
- DRBG supports 256 bits of security.
- Includes a reseed function

RBG3(XOR) Construction

RBG3(XOR) construction contains one or more validated entropy sources and a DRBG whose outputs are XORed to produce full-entropy output.

DRBG support 256-bit security strength and should be reseeded periodically

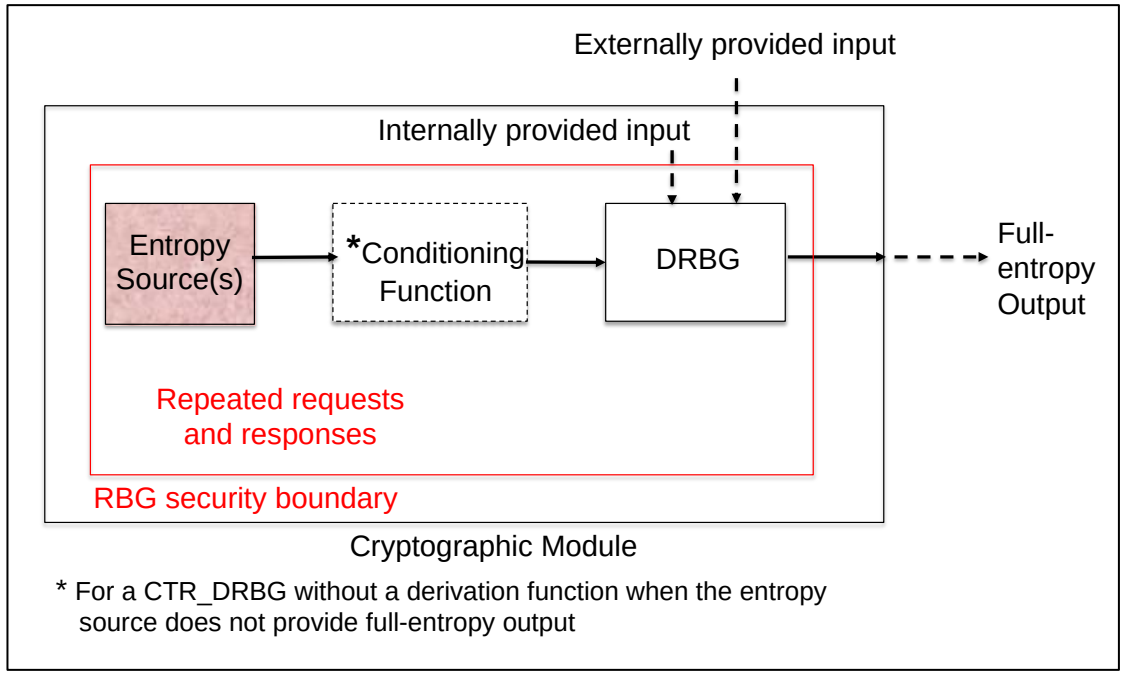
Full-entropy bitstrings shall be provided to XOR either directly from the concatenated output of validated physical entropy source(s) or by an external conditioning function using validated entropy source(s) using Method 1.



RBG3(RS) Construction

RBG3(RS) construction contains one or more validated entropy sources and a DRBG whose outputs are XORed to produce full-entropy output.

DRBG is supports 256-bit security strength.



Comparison

CONSTRUCTION	INTERNAL ENTROPY SOURCE	PREDICTION RESISTANCE	FULL ENTROPY
RBG1	No	No	No
RBG2	Yes	Yes	No
RBG3	Yes	Yes	Yes

Call for Feedback

New draft uses fewer construction options.

In a future revision of SP 800-90C, should other constructions be included?

Specifically, the RBGs specified herein always include a DRBG mechanism from SP 800-90A. Should RBG constructions that consist of entropy sources with internal conditioning but with no DRBG be included?

Note that there are security implications if the entropy source fails in an undetected manner and the RBG continues to produce output.

Call for Feedback and Notes

Does anyone foresee a compelling need to externally condition entropy-source output when full entropy is not required (e.g., to compress the entropy in a very long bitstring into a bitstring of an acceptable length)?

Note that an external conditioning function based on a hash function could be used to compress the entropy in very long bitstrings, if necessary.

Notes

The RBG constructions use NIST-**approved** cryptographic primitives.

- Three-key TDEA is currently allowed.
  - SP 800-131A indicates that its use is deprecated through 2023 and will be disallowed thereafter. 90C **does not approve** the use of three-key TDEA in an RBG.
- For some applications, the use of SHA-1 has been discouraged or disallowed. This document **does not approve** the use of SHA-1 in an RBG.
- The use of the SHA-3 hash functions are allowed in SP 800-90C for the Hash_DRBG and HMAC_DRBG but are not currently included in SP 800-90A.
- SP 800-90A will be revised to exclude the use of TDEA and SHA-1 and include the use of the SHA-3 family of hash functions.

Notes

Since 2030 is the projected date for requiring a minimum security strength of 128 bits for U.S. government applications, RBGs are specified to provide 128, 192, and 256 bits of security strength.

112-bit security strength has been removed.

Thanks

Comments and suggestions on the SP 800-90C plans are welcome

Contact: rbg_comments@nist.gov