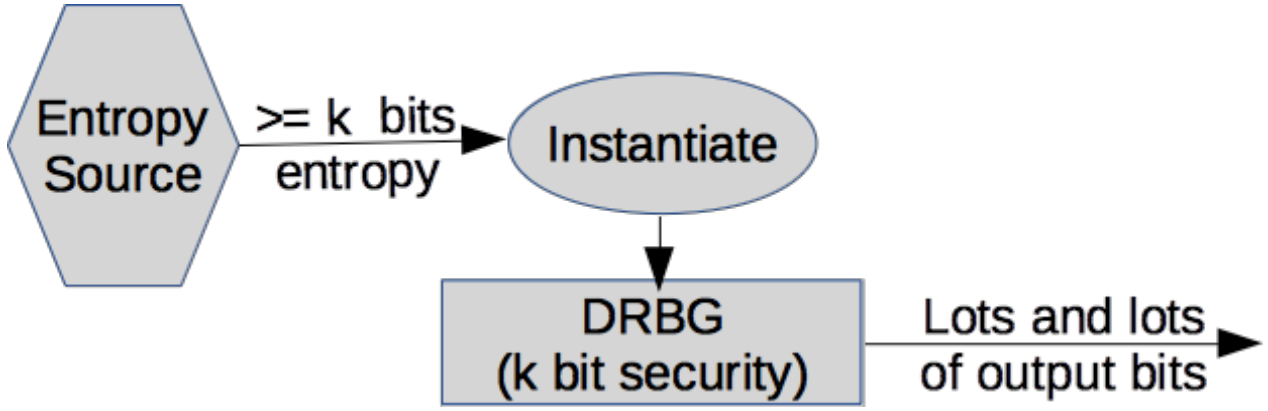
SP 800-90 Update

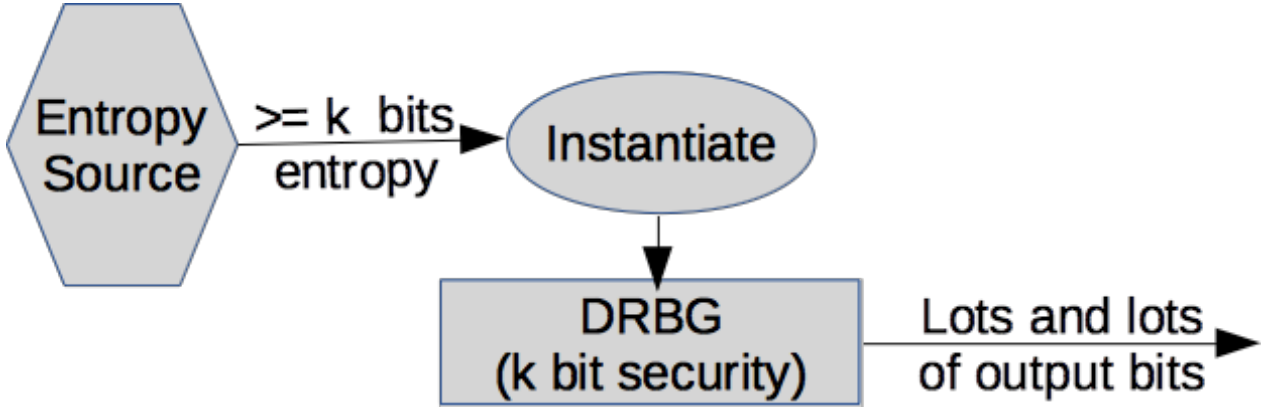
John Kelsey, NIST and COSIC/KU Leuven

Big Picture: SP 800-90



- SP 800-90A: DRBGs
- SP 800-90B: Entropy sources
- SP 800-90C: Putting them together

SP 800-90 Status



SP 800-90A: DRBGs

- Last revised > 10 years ago
- Beginning to revise now

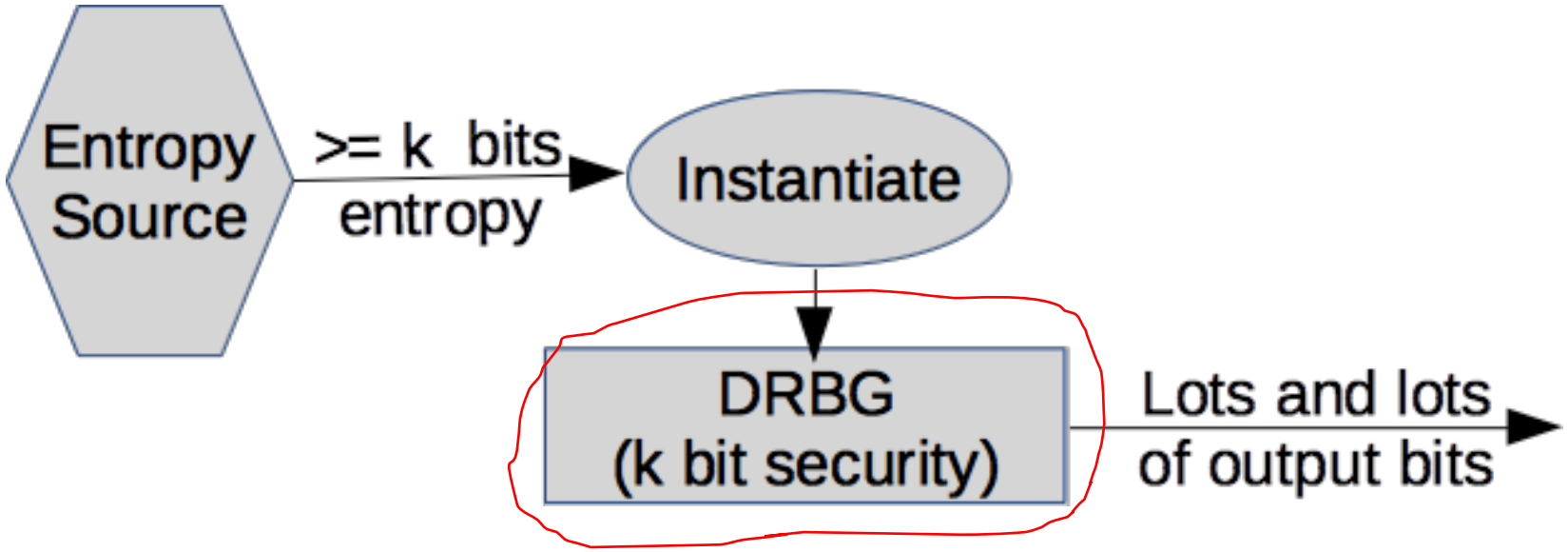
SP 800-90B: Entropy sources

- Plan to revise in future

SP 800-90C: Putting them together

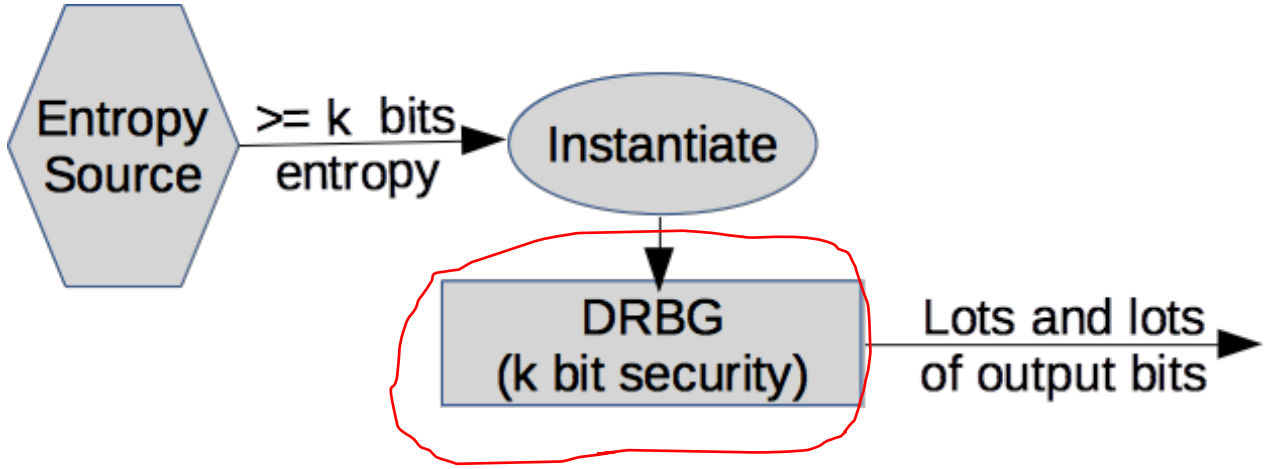
- Previous draft got lots of comments
- New draft out soon—hopefully final version

SP 800-90A: DRBGs



DRBG = Deterministic Random Bit Generator

SP 800-90A



- 90A defines approved DRBGs
  - AKA cryptographic PRNG
  - Deterministic
  - Give it an unguessable seed→ DRBG produces outputs indistinguishable from random

- Last revised: June 2015

90A Revisions

We recently started working on changes on SP 800-90A

- No more 112-bit security
- Removing SHA-1 and TDEA, adding SHA-3
- Updating requirements on CTR-DRBG and other DRBGs
- Changes in pseudocode and document conventions

Removing TDEA (3DES) and SHA1

- TDEA provides about 112 bits of security
  - Actual bound is complicated—depends on # of plaintexts seen
  - 112 bit security going away soon
  - Withdrawing support for TDEA across the board

- SHA-1 broken and deprecated for some years now
  - Trying to get it to go away
  - Next version of 90A will not allow SHA-1-based DRBGs

Entropy source → randomness source

DRBG can be seeded from:

- Entropy source
- Another RBG
  - *Source RBG* must provide at least security strength of DRBG being seeded!

- Needed for constructions in SP 800-90C
- Requires changes to language and requirements in 90A

CTR-DRBG and Derivation Functions

- Currently CTR-DRBG requires the use of bc-df unless seeded from a full-entropy source
  - Bc-df is clunky and inefficient
- Two new functions (CBC-MAC and CMAC)
- No derivation function needed when randomness source = RBG

More changes to DRBG requirements

- Old: entropy input + nonce to instantiate
- New: More entropy/randomness, no nonce

If we get seed material from:

- Entropy source: *3s/2* bits min-entropy
- RBG: *3s/2* bits

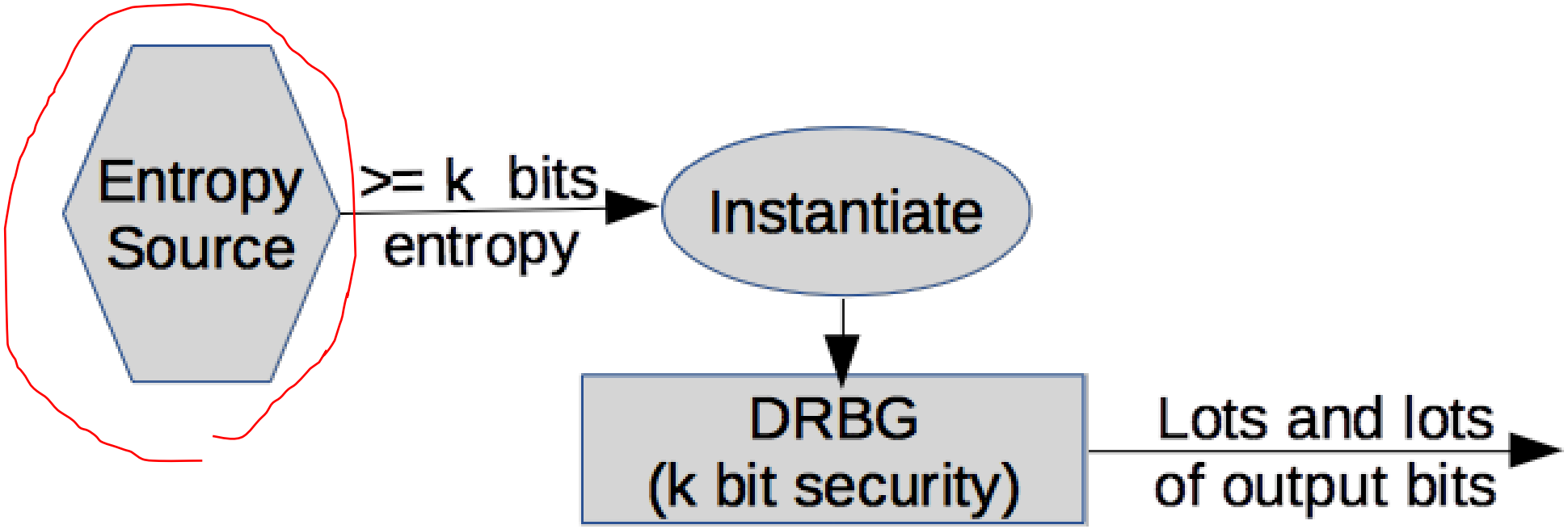
Note: *s* = security strength of DRBG being instantiated

Reseed interval and generate requests

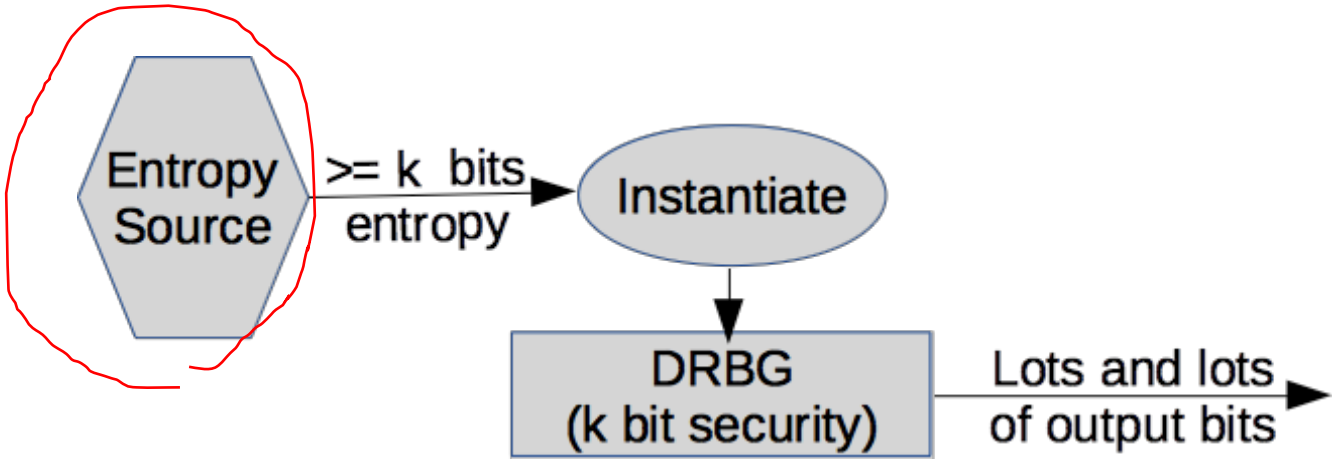
- Generate calls shall be atomic operation
  - No output from module until call is complete
  - Must complete in a short time

- Specified reseed interval is going away
  - Never much justification for limit of 2^{48} generate calls
  - Implementation can set own limit for how often to reseed

SP 800-90B: Entropy Sources



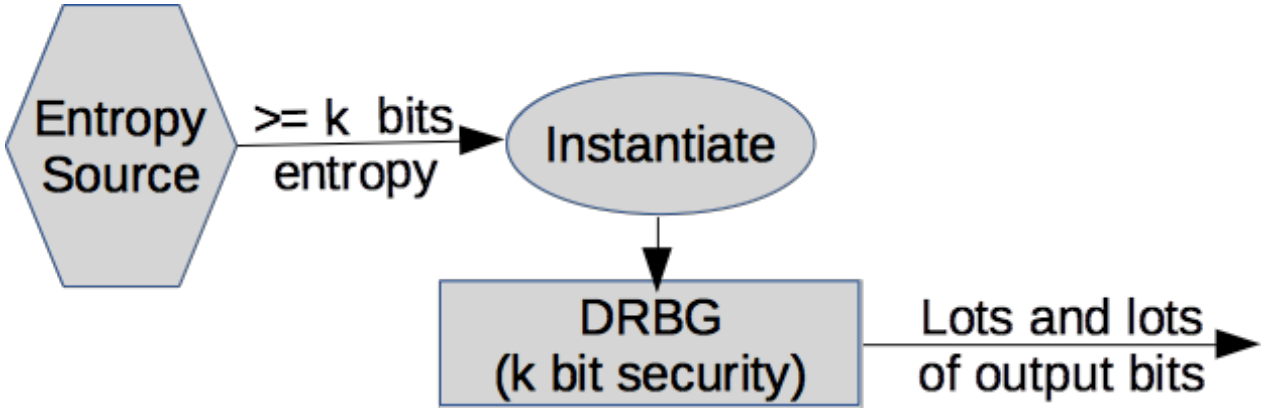
SP 800-90B



Building and testing an entropy source

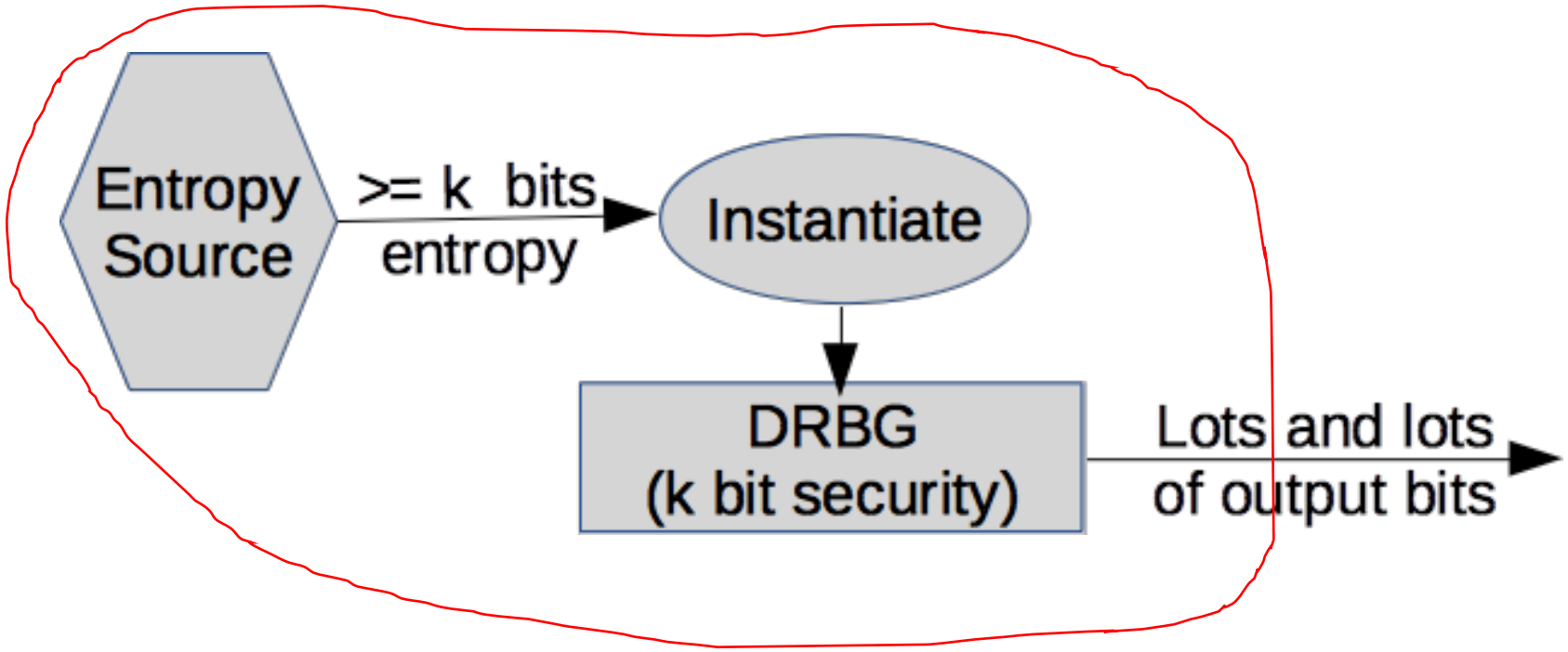
- Ultimate source of unpredictability
- Provide seed for DRBGs
- Can provide full-entropy output with conditioning
- Only nondeterministic part of RBG

SP 800-90B



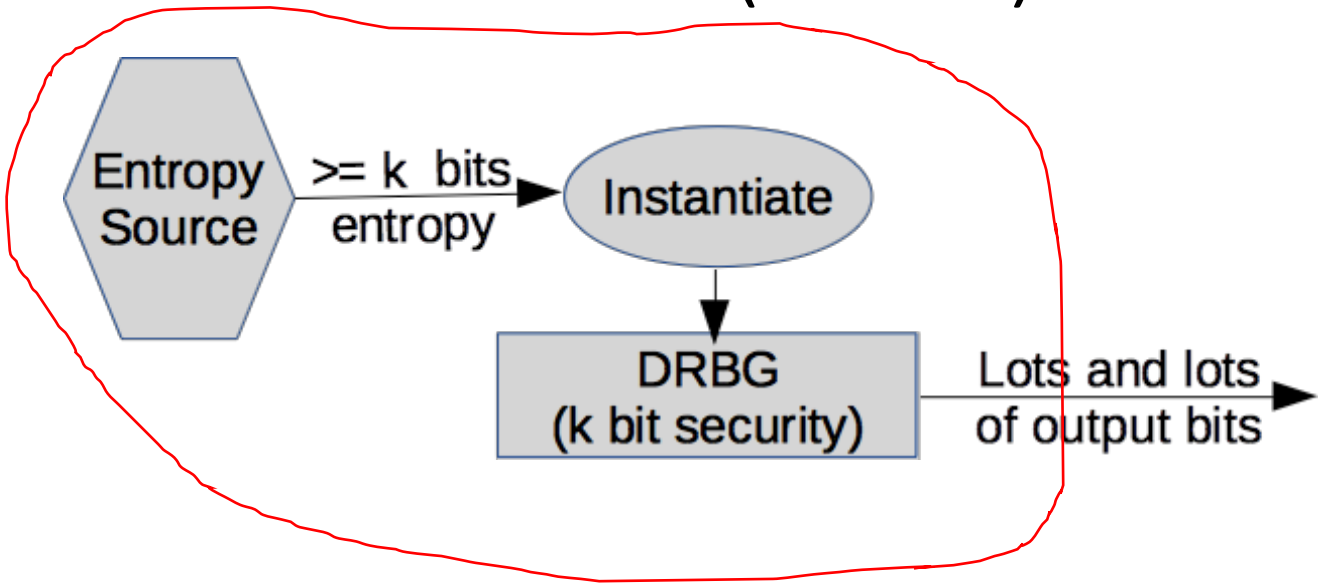
- Plan to revise in next couple years
- No hard timetable yet
- Planned revisions:
  - Stochastic models for physical entropy sources
  - Better requirements for evaluation
  - Better requirements for health tests
  - Moving requirements closer to AIS 20/31

SP 800-90C: Random Bit Generators (RBGs)



SP 800-90C: Random Bit Generators (RBGs)

- Four classes of RBG
  - RBG1: Externally seeded DRBG
  - RBG2: Internally seeded DRBG
  - RBG3: Full entropy RBG
  - RBGC: Trees of DRBGs



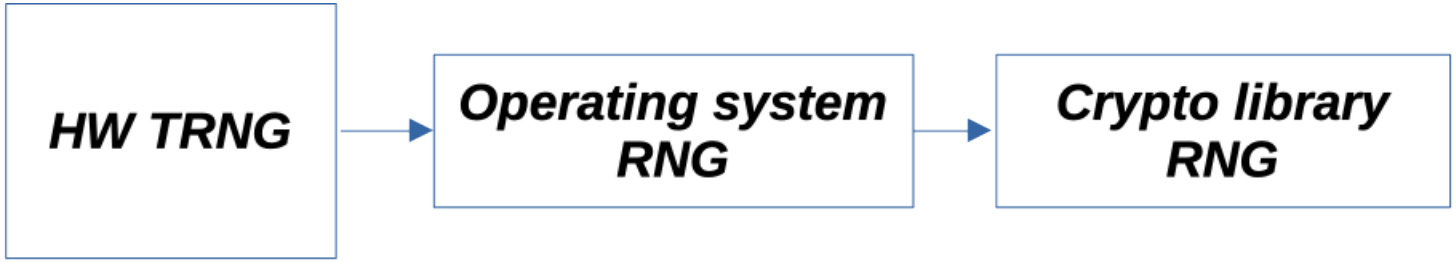
- Different performance/security tradeoffs

- Last draft out Sept 2022
- Public comments received Dec 2022

Next Draft Out Very Soon

- Big addition: RBGC construction ← Why we need new draft
  - Chains and trees of DRBGs
  - Initial seed source involves an entropy source
  - Commonly needed in software environments
- Many more minor changes
  - RBG3-RS revision
  - A bunch of minor fixes and changes to pseudocode or examples

Chains of RBGS are common in software

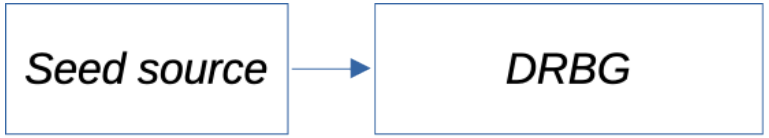


- Hard to see how else to do it
- 90C needs to allow this

  … without making the standard too complex to understand
- Previous draft did not include this

  …why we're going back out for public comment!

Solution: RBGC construction

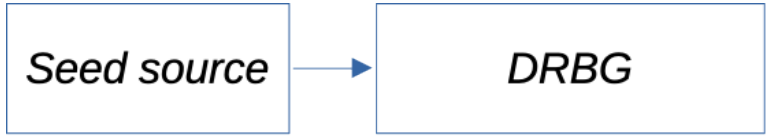


RBGC consists of:

- DRBG
- Seed source
  … which can be another RBGC

RBGC components

Seed source



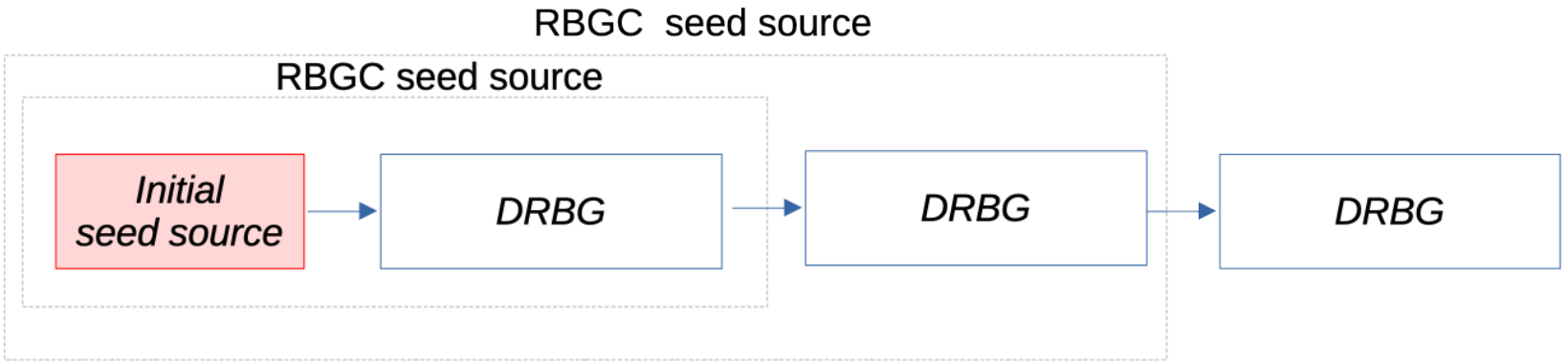
Any of

- RBG2
- RBG3
- Full entropy source
- Another RBGC ← *this allows chains and trees of RBGCs*

DRBG

Any approved DRBG

The initial source

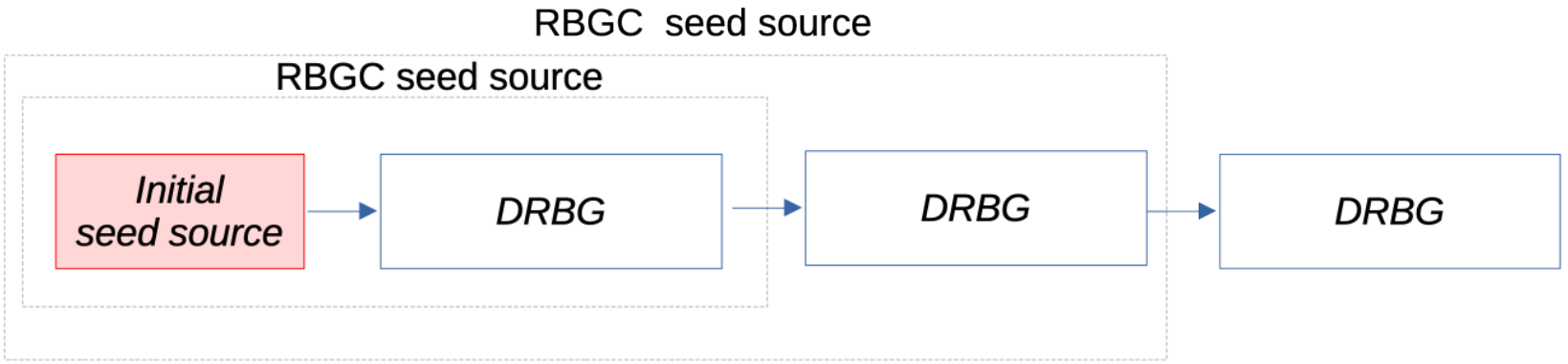


An RBGC can be a seed source…

… but the initial seed source has to provide some entropy

- RBG2
- RBG3
- Full entropy source

Everything depends on initial source



Requirements:

- Available entropy source
- Strong output bits

Initial seed source may be:

- RBG2(P)
- RBG2(NP)
- RBG3
- Full entropy source

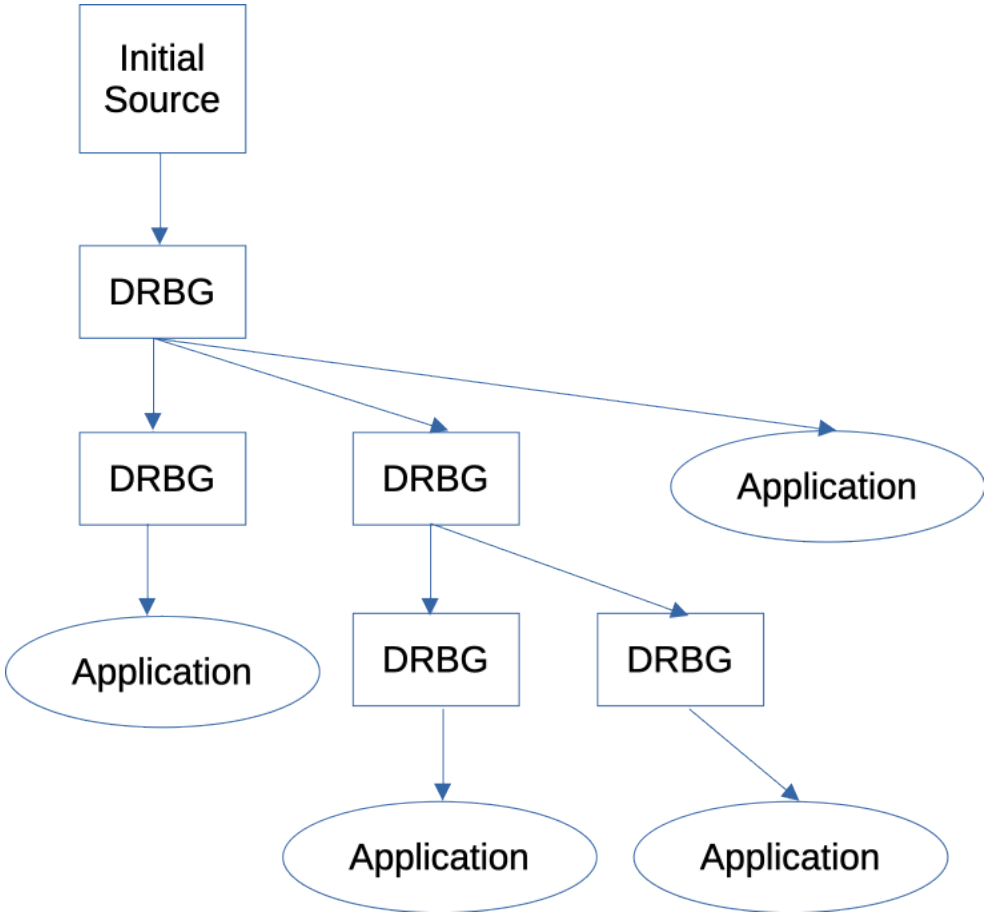
Chains of DRBGs: requirements

- Security strength can't increase
- Each DRBG has exactly **one** seed source
  - May also incorporate additional input
- A DRBG may provide seed material **AND** random bits
- **No loops allowed (See below)**

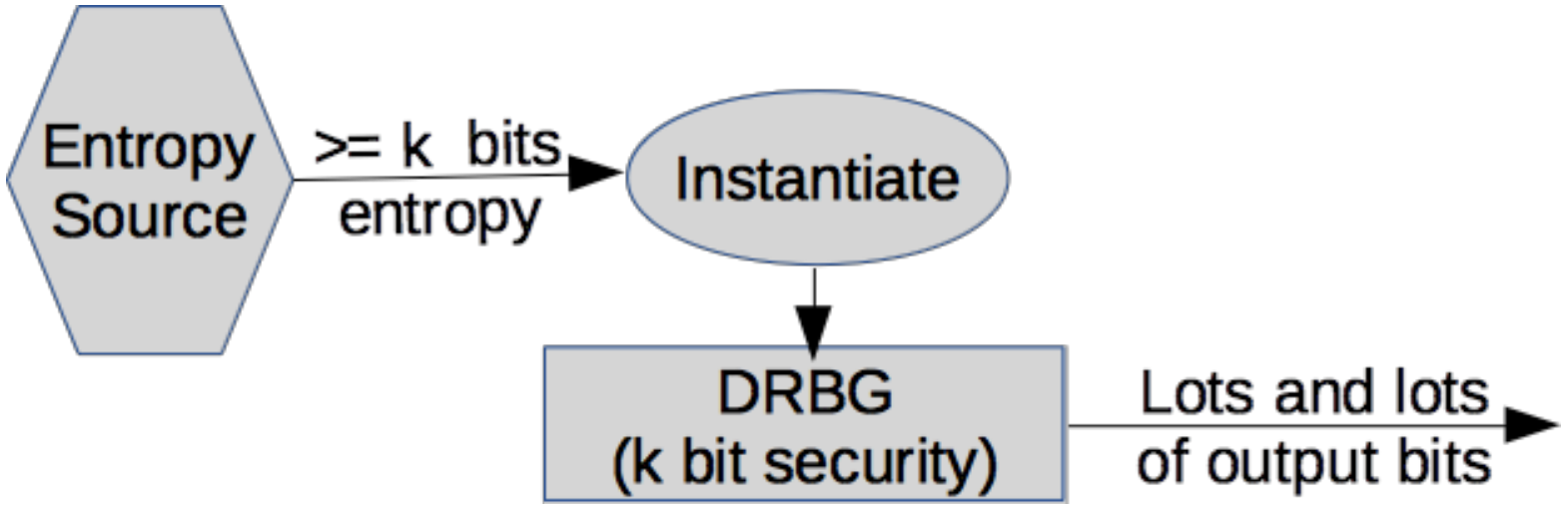
Trees of RBGs

- Each DRBG: one seed source
  - May also incorporate additional input
- Initial source: Ultimate root of trust
- One source → many DRBGs
- DRBGs can provide seed to other DRBGs

  …AND random bits to applications



Other SP 800-90 Related Work



Other 800-90 related work

- Collaboration with BSI
  - See Kerry and Werner's talk coming up
  - Goal: Make it practical to get same RBG/RNG through SP 800-90 and AIS 20/31

- ISO
  - Documents being developed for ISO
  - We've provided comments

- Ongoing research
  - Maybe a XOF based DRBG?

Shall vs Must

This is a change happening in many new/revised standards now.

- Many requirements in SP 800-90 not testable by labs
- Examples:
  - Environment
  - How module is used
- Previously: Written as SHALL requirements
  - Result: many SHALL requirements not testable
- Now: Written as MUST requirements
  - Specify requirements on how module is used
  - Product documentation
  - Restrictions on FIPS 140 certificate

Wrapup

- 90C: Going out for public comment very soon
  - Result should be final version of document
- 90A: Revisions have started
  - Lots of accumulated changes queued up
  - Just getting started
- 90B: Long-term plan to revise
  - Better evaluation of entropy sources
  - Stochastic models, better health tests, etc.