ICMC 2020

Summary of Entropy-Relevant Content

Joshua E. Hill, PhD
(Version 20201103 D9)

Introduction

- This is a summary of the new entropy/RBG information presented at/about ICMC 2020.
  - This includes some updates in later meta-discussions and e-mail.
  - You should try to review the original presentations for any topics you are interested in.
  - There is a lot of introductory / place setting / reviewed information that I skipped.
  - This is mostly **not** my content.
    - I can answer questions based on my understanding of the material, but my responses shouldn't be viewed as authoritative.
- NIST titles are presently in flux.
  - I tried to list the titles folks were transitioning into.
  - I may have misunderstood.
  - No slight is intended. ☺

On Comments and Their Provenance

- I have integrated context and comments from various sources.
  - Such comments are clearly marked. [Josh: Like this.]
  - Diagrams are pulled directly from the source presentations and cited by author.
- *Comment Dramatis Personæ*:
  - Chris: Christopher T. Celi (ESVTS Developer, Program Manager of CAVP)
  - Mike: Michael J. Cooper (previous STVM Group Manager)
  - Tim: Timothy A. Hall (acting STVM Group Manager)
  - Josh: Joshua E. Hill (*The Deliverator* [of this presentation], KeyPair)
  - John: John M. Kelsey (NIST 90A/B/C Author)
  - Marcos: Marcos Portnoi (atsec)
  - Allen: Allen L. Roginsky (NIST/CMVP, main NIST entropy reviewer)
  - Meltem: Meltem Sönmez Turan (NIST 90B/C Author)

Meltem Sönmez Turan
on
SP 800-90B rev1

SP 800-90B rev1
Meltem Sönmez Turan (NIST 90B/C Author)

- Full entropy definition
  - Amount of entropy per bit is at least $1 - \varepsilon$ where $\varepsilon \leq 2^{-32}$.
  - [Josh: This is less strict than the definition in the 2012 draft of SP 800-90B, where $\varepsilon \leq 2^{-64}$.]
- Truncated vetted conditioning components can be used as vetted components.
  - Just use the truncated size as n_{out}.

SP 800-90B rev1
Meltem Sönmez Turan (NIST 90B/C Author)

- Aligning with BSI AIS-20 / AIS-31 standards
  - Trying to remove contradicting requirements.
  - Use stochastic models (especially for physical sources).
  - Moving from a black box to a white box approach.
    - [Josh: It isn't clear to me what this means; quite a lot of design information is required for a current 90B validation. Werner seems to use “white box” to mean “producing entropy estimates based on a stochastic model”.]
  - Health tests tailored to the characteristics of the design.
    - [Josh: The arguments used to support the APT and RCT presume that the noise source is IID. I asked what was happening with the existing APT and RCT. Meltem stated that they don't currently expect to remove these tests.]

SP 800-90B rev1
Meltem Sönmez Turan (NIST 90B/C Author)

- Work is proceeding to improve the quality of predictors.
  - Some academic findings suggest some refinements.
    - [Meltem: e.g., Zhu, Ma, Chen, Lin, Jing. *Analysis and Improvement of Entropy Estimators in NIST SP 800-90B for Non-IID Entropy Sources*]
    - [Josh: See Section 4.4 of this paper.]
- "Special thanks to the CMUF Entropy WG for comments and suggestions."
- [Meltem: Currently mainly working on the lightweight cryptography project. Intend to make significant progress with SP 800-90B rev1 after SP 800-90C is published.]
  - [Josh: It isn't clear if this is after the 90C draft is published, or the final 90C document.]

John Kelsey
on
SP 800-90C

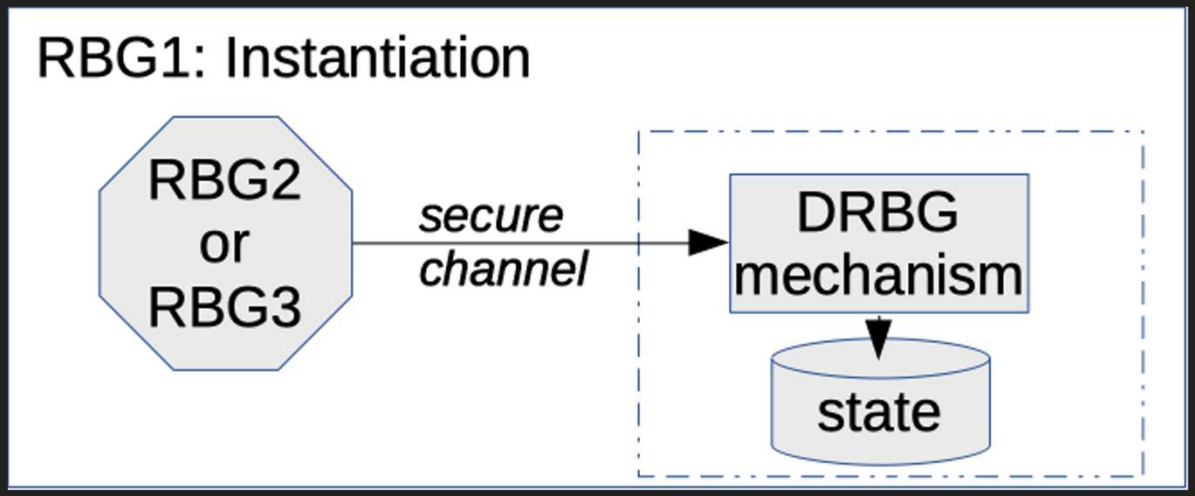
SP 800-90C: Summary
John Kelsey (NIST 90A/B Author)

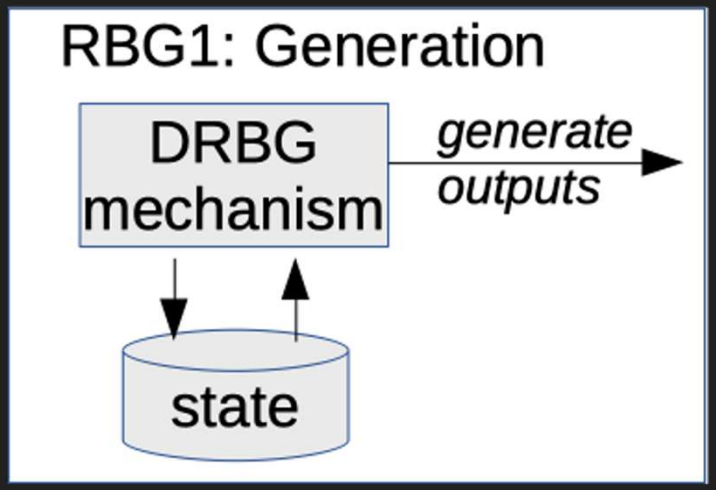
- RBGs combine an entropy source (ES) and a DRBG.
- There are three classes: RBG1, RBG2, and RBG3.
- 90C specifies a definition of a Full Entropy Source (FES).
- 90C specifies how to use vetted conditioning functions as external conditioning.
- 90C updates 90A requirements:
  - Harmonizing with AIS-20 / AIS-31.
    - Goal: Trying to make it as easy as possible to satisfy both in the same product.
  - Apply lessons from the last 14 years.

SP 800-90C: Full Entropy Sources and Strings
John Kelsey (NIST 90A/B Author)

- 90C specifies a definition of a Full Entropy Source (FES).
  - Ideally these have the goal of information-theoretic security.
- 90C provides a way of generating full entropy strings using any entropy source with external conditioning:
  - n+64 bits of entropy are input into a vetted conditioning function [Josh: with $nw \geq n$?], yielding n bits of entropy out.
  - [Meltem: A distinguishing game connects this with the new 90B definition. This will be detailed in a 90C appendix.]

SP 800-90C: RBG1
John Kelsey (NIST 90A/B Author)





[John]

SP 800-90C: RBG1: Externally Seeded DRBG
John Kelsey (NIST 90A/B Author)

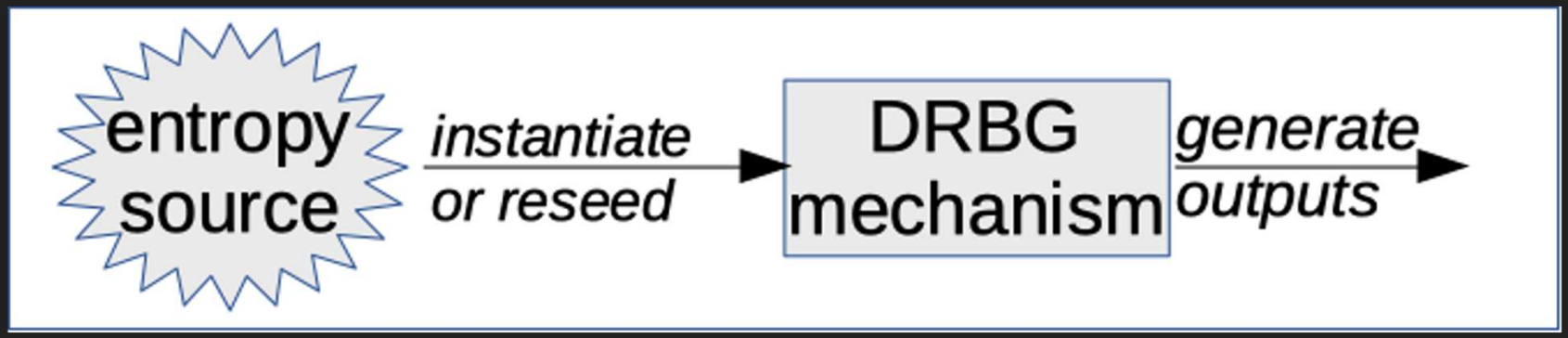
- RBG2 or RBG3 seeds the RBG1 (security strength >= the RBG1 claimed security strength) via a physically secure channel.
  - Here there are no shared secrets and no randomness so we can't establish a cryptographically secure channel.
  - [Josh: It is not clear to me why there can't be pre-loaded shared secrets. One side clearly can't be relied upon to produce random values for instantiation, which does limit the available secure channel protocols here. What about reseeding?]
- Many RBG1 requirements may be untestable at the module level, as the RBG2 or RBG3 may be outside the cryptomodule boundary.

SP 800-90C: RBG1: Externally Seeded DRBG
John Kelsey (NIST 90A/B Author)

- Need secure persistent storage of state.
  - Compromise of memory should not reveal prior RBG states.
    - [Josh: For some designs, this clearly precludes storing intra-generate state.]
- No ability to recover from a compromise after instantiation.
  - [Josh: Why can't these be reseeded via a secure channel? Are we assuming that any compromise includes any stored shared secrets?]
- **NIST is unsure if they should include this RBG class.**
  - NIST wants feedback on this.

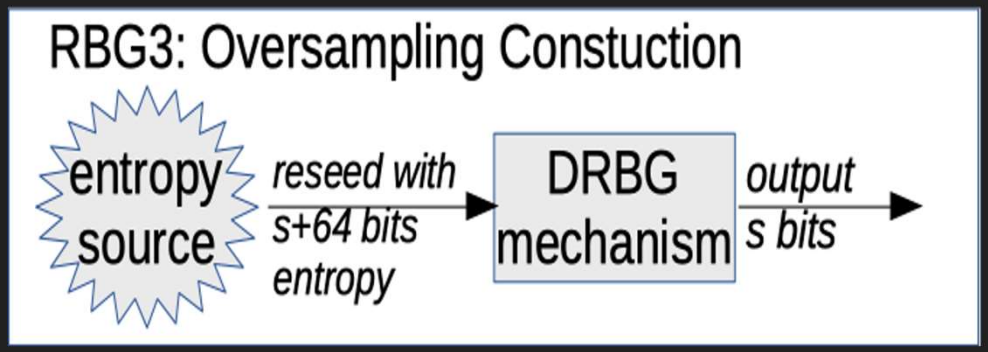
SP 800-90C: RBG2
John Kelsey (NIST 90A/B Author)

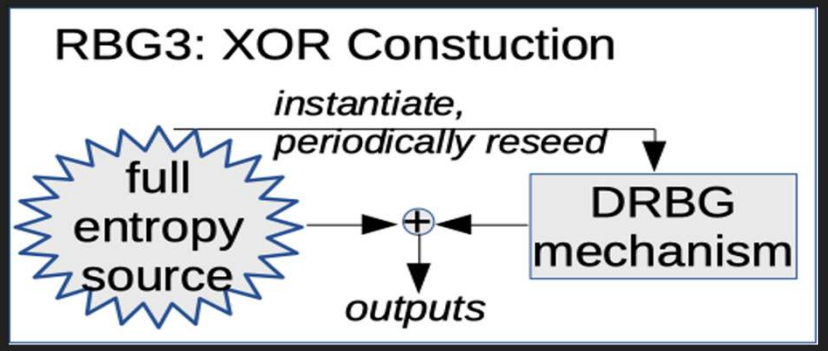
- RBG2: internally seeded
  - Expected to be the dominant design in practice.



[John]

SP 800-90C: RBG3
John Kelsey (NIST 90A/B Author)





[John]

SP 800-90C: RBG3
John Kelsey (NIST 90A/B Author)

- RBG3: full entropy RBG (née NRBG)
  - Intended to be information-theoretic secure.
  - Should also offer some side channel benefits.
- DRBG component required to have 256-bit security strength.
- [Josh: seems to be basically the same constructions as in the 2016 draft of 90C.]
- Oversampling construction now requires s+64 bits of entropy in (s is the security strength; s = 256 by the above) for every s bits out.
  - [Josh: Note, this is a relaxation of the 2016 draft, where s bits of entropy input per round would support s/2 bits of entropy output.]
- XOR construction requires a FES.
  - Seed DRBG.
  - Outputs DRBG output XOR FES output.

SP 800-90C: Changes to 90A
John Kelsey (NIST 90A/B Author)

- No more TDEA / SHA-1 / 112-bit security strength.
- Remove nonce from all DRBGs.
  - [Josh: In the sense of the CTR_DRBG with no derivation function, which morally had a randomly generated nonce. In the current 90B terminology, all RBGs will be required to have a random nonce that is provided as a part of the *entropy_input* string.]
  - For security strength s, always require $1.5 \times s$ bits of entropy.
- 90A DRBG no longer allowed to be instantiated at lower than maximal strength.
  - [Josh: Both Allen and I have raised concerns regarding this change.]

SP 800-90C: Changes to 90A
John Kelsey (NIST 90A/B Author)

- 90A allows up to 2^{16} bytes of output, and it isn't clear that this needs to be done all at once.
- This has led to attacks, both in distinguishability and using side channels.
- Current plan:
  - Generate requests shall be complete before any output bits are used.
  - Generate requests should be kept as short as possible.
- Should NIST forbid very long requests?
  - NIST wants feedback on this.
  - [Josh: I think that the maximal length should probably be reduced, particularly for the CTR_DRBG.]

SP 800-90C: Changes to 90A
John Kelsey (NIST 90A/B Author)

- CTR_DRBG bc_df is expensive and ugly.
  - For RBG1, we can avoid use of the bc_df.
    - [Josh: currently phrased as “CTR_DRBG with no derivation function”.]
  - Currently working on a lighter-weight option for instantiation.

SP 800-90C: Administrivia
John Kelsey (NIST 90A/B Author)

- SP 800-90C public comments "soon".
- Eventually, the only way to get an approved RBG will be 90C.
  - Transition is TBD.
- [Josh: None of these RBGs allow for arbitrary chaining of DRBGs. The RBG1 is the only RBG that is seeded using a non-local entropy source, and that is seeded by another RBG2/RBG3, so DRBGs can never be chained more than 2 deep.]

Werner Schindler
on
AIS-20 and AIS-31 Updates

AIS-20 / AIS-31
Werner Schindler (AIS-20 / AIS-31 Author)

- AIS-20 / AIS-31 being updated.
  - Draft should appear in Q1 2021.
- BSI and NIST want to further align.
  - e.g., 90A seems to be compliant to DRG.3 and DRG.4.
    - Proofs will be present in the mathematical-technical reference of AIS-20 / AIS-31.
    - These proofs can simply be referred to within an AIS-20 / AIS-31 validation.
    - Need a joint definition of "request" in AIS-20 and SP 800-90A.

Chris Celi
on the
Entropy Source Validation Scope

SP 800-90B Validation Scope
Chris Celi (Program Manager, CAVP)

- A separate scope is being established for entropy sources in 2021.
  - Entropy source certificates will be issued in this scope.
  - [Mike: a separate NVLAP scope of accreditation is required.]
  - You can validate an entropy source without validating the module.
  - [Allen: Many issues need to be resolved, especially when reusing non-physical entropy sources.]
- Validations of entropy sources using Entropy Source Validation Test System (ESVTS).
  - ESVTS is expected to be available online by the end of 2020.
  - ESVTS interface will be similar to ACVTS.

SP 800-90B Validation Scope
Chris Celi (Program Manager, CAVP)

- "Our program [Chris: STVM] will support automated validations of":
  - Algorithms
  - Modules
  - Entropy sources

SP 800-90B Validation Scope: Notes From the Chorus

- [Josh: I doubt that many of the existing FIPS 140-2/3 or SP 800-90* requirements can be tested using automated testing. I'm concerned that there is some risk that this effort will lead to ignoring important requirements that are essentially subtle technical arguments.]
- [Chris and Tim: The current plan is to have the CMVP reviewers who are presently tasked with entropy source review conduct the technical evaluation of the submitted entropy assessment reports. Currently, this is Allen (NIST) and Jonathan (CCCS).]
- [Allen: NIST management has a goal of automated testing for 90B, and they will need to find out for themselves that this isn't broadly possible for many of the 90B requirements.]

SP 800-90B Scope
Chris Celi (Program Manager, CAVP)

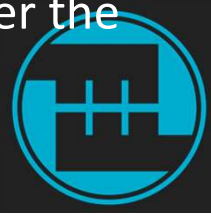
- Workshop expected centered on the validation of SP 800-90B requirements.
  - Want to establish consistent, uniform expectations of test evidence.
  - Soliciting a case study for open review.
    - Cited example was Linux /dev/random.
    - [Josh: It is unclear how this would work given the extensive non-compliance of the Linux /dev/random source to SP 800-90B. See Stephan Müller's excellent ICMC presentation, or my less focused CMUF Entropy WG presentations on this topic.]
  - Workshop is anticipated to occur in late 2020 or 2021.
    - [Josh: The schedule is still TBD as of November 3, 2020.]

SP 800-90B Scope
Chris Celi (Program Manager, CAVP)

- Pre-review of entropy sources is offered
  - [Allen: these should be submitted through a FIPS lab; the lab should send the reports to Carolyn French and Beverly Trapnell so that they have insight into the CMVP workload. CMVP will distribute the reports as necessary.]
  - [Tim: This is a one shot pre-review, and the review can be targeted to compliance in a limited area, or a complete entropy report.]
  - [Josh: It is not clear to what degree the results of the review will be binding.]
    - [Chris: The pre-review is not a path to a certificate, it is a means of offering insight on how to write an entropy report that would lead to a certificate.]
  - [Chris and Tim: Only 20 pre-reviews will be conducted, this pre-review option is only available until Jan 1, 2021. One review pass per vendor only.]
- It is not yet clear how SP 800-90C is going to be validated.

2020-Oct-20 Entropy CMUF WG Meeting
Chris Celi (Program Manager, CAVP)

- Entropy Scope name is 17ESV.
- Labs need to apply to expand their scope to include this.
  - Only 17ACVT (ACVP) 3rd party labs can seek accreditation under this new scope.
- Requirements for a public facing document analogous to the security policy in FIPS 140 validations are TBD.
- Entropy Sources with different “operating environments” are likely to require separate assessment.
  - This is likely to be structured similarly to how algorithm certificate applicability works.
- CMVP reviewers will continue to perform the reviews of the documents even after the scope is set up.



Mike Cooper and Mary Baish
on the
CMVP and NIAP Integration with the Entropy Source Validation Scope

SP 800-90B NIAP Integration

Mike Cooper (previous STVM Group Manager) and Mary Baish (Director of NIAP, NIAP 90B Author)

- Separate SP 800-90B scope expected to be helpful for both programs
  - The NIAP SP 800-90B transition schedule is TBD.
  - NIAP will eventually require that evaluated TOEs [Josh: those with entropy sources?] use an entropy source listed on NIST's Entropy Source validation list.

SP 800-90B NIAP Integration

Mike Cooper (previous STVM Group Manager) and Mary Baish (Director of NIAP, NIAP 90B Author)

- It isn't clear how this entropy source validation is going to be integrated into both programs.
  - CMVP will continue to require an Entropy Assessment Report (EAR).
  - NIAP will continue to require an EAR.
    - This EAR may be much shorter than the current EARs.
    - [Josh: The implication seems to be that the NSA is still going to conduct a review of these reports.]
    - No final decision has been made as to what must be in the NIAP EAR.
  - [Josh: If EARs are provided during the CMVP and NIAP reviews beyond the entropy certificate, then the 90B certificate may not mean much, as an entropy source with a 90B certificate could later be rejected by CMVP and/or NIAP during their additional reviews.]
    - [Tim: In the CMVP case, this should not occur as the same people would be conducting both reviews.]

Stephan Müller
on the
(non)-SP 800-90B Compliance of
Linux /dev/random

Linux /dev/[u]random and SP 800-90B

Stephan Müller (atsec)

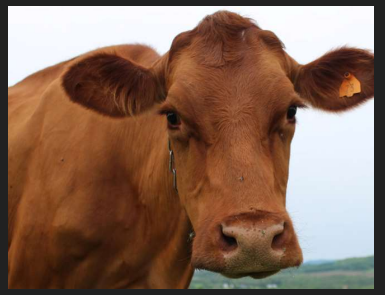
- Summary: Linux /dev/random is not 90B compliant.
  - [Josh: This was an excellent presentation, but I'm not going to summarize it here because most of the identified issues were previously discussed in a series of CMUF Entropy WG presentations on 2020-01-14 [Marcos], 2020-02-25 [Josh], and 2020-03-10 [Josh].]

Joshua E. Hill
on
Further SP 800-90B Technical and Process Comments

90B Technical and Process Comments
Joshua Hill (KeyPair)

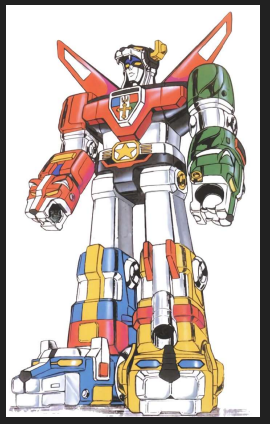
- The creation of the recent IG 7.19, which helps to clarify CMVP's interpretation of SP 800-90B.
  - [Josh: Extensively covered in most of the CMUF Entropy WG meetings between August 2019 and August 2020. Not summarized here.]
- Some problems in the statistical construction of some of the SP 800-90B estimators and a proposed fix (and why this isn't generally a big deal).
  - [Josh: Discussed in a prior CMUF Entropy WG meeting on 2019-11-19. Not summarized here.]
- A proposed statistical (meta-)assessment strategy that helps to reduce the variation in statistical assessment.

How Now?



- For a fixed noise source with fixed entropy-relevant parameters, a min entropy estimator's assessment conforms to some fixed distribution.
- It's hard to comment on this distribution given only a single result.
- Sometimes this distribution is unhelpfully wide, which risks intermittent "downstream" validation failures.
- How do we get a more meaningful and stable assessment?

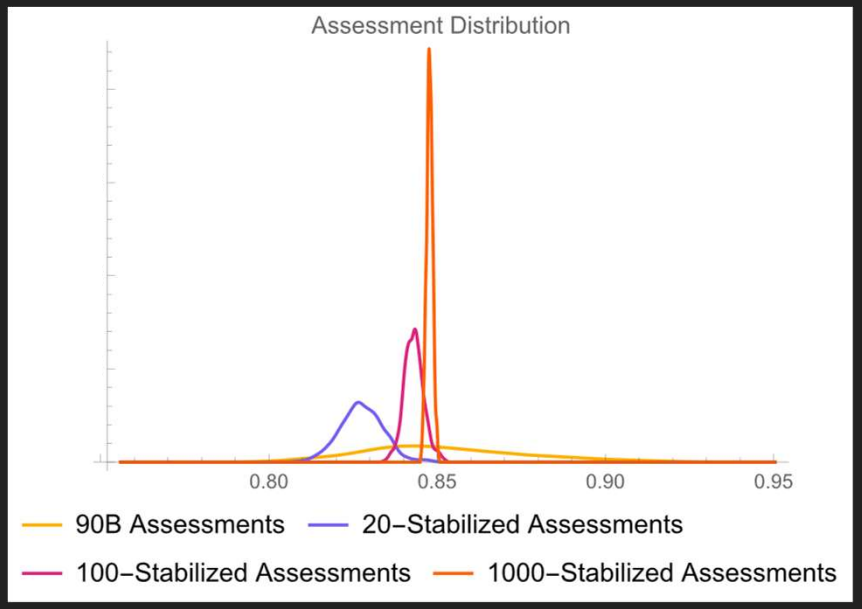
“And I’ll Form the Head!”

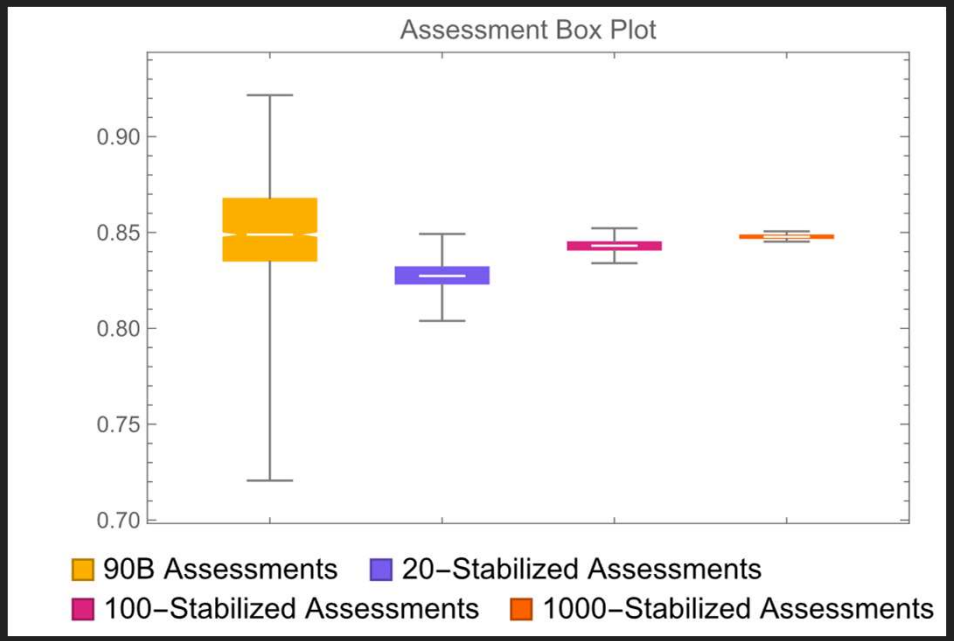


Summary:

- Perform r rounds of testing.
- Summarize the results of the r rounds of testing for each estimator.
  - For all estimators other than the Markov Estimator, bootstrap the median.
  - For the Markov Estimator, bootstrap the 0.5^{th} percentile.
- Take the minimum of the per-estimator overall results.
- This is the r-stabilized assessment.

Example Results

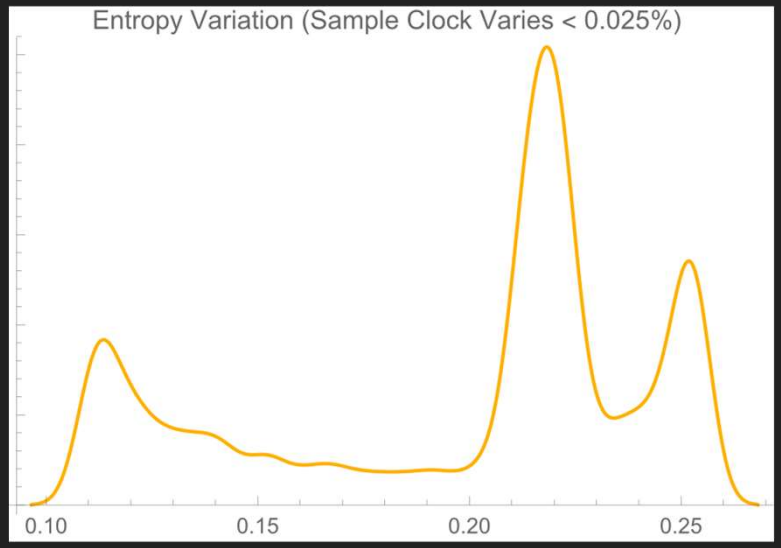




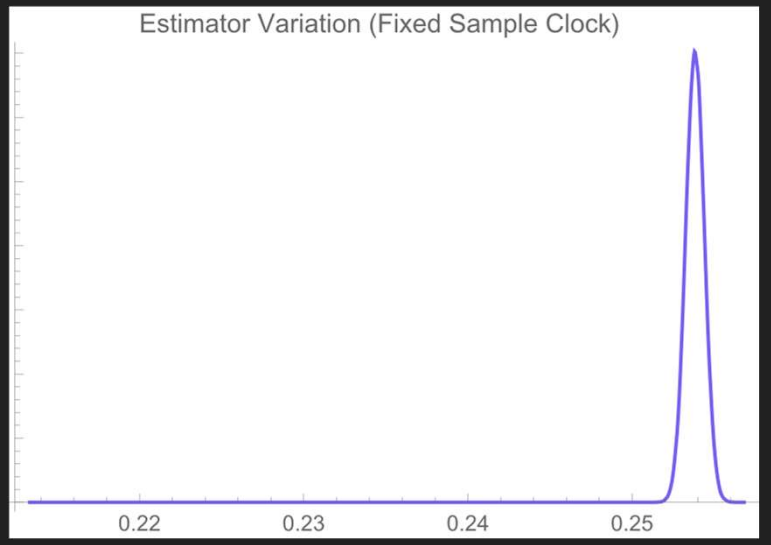
Simulated 1GHz Ideal RO Sampled at Approximately 1MHz with a Per-Cycle Period Jitter of $\sigma \approx 11.8$ps (n=1,000)

Right, That's Bad. Okay, Important Safety Tip... Thanks Egon!

- Not all assessment variation is due to estimator variation.
- Many (most?) noise sources have entropy-relevant parameters that can affect the actual min entropy produced.



$\neq$



Simulated 1GHz Ideal RO Sampled at Approximately 1MHz with a Per-Cycle Period Jitter of $\sigma \approx 2.8$ps (n=250,000)

He's No Fun, He Fell Right Over

- How can this be compliantly integrated into the SP 800-90B assessment process?
- Calculate the r-stabilized assessment.
- Perform a single "Large Block Assessment" on the full data set.
- Take the minimum of the r-stabilized assessment and the "Large Block Assessment".
- This is mappable to the SP 800-90B process (the Large Block Assessment **is** the SP 800-90B assessment process, but with more data than required by SP 800-90B).
- If the r-stabilized assessment is lower than the Large Block Assessment, this can be thought of as reducing $H_{submitter}$.

Cue The Drumroll!
All Right, Open Your Boxes!

- OK, that isn't really practical. Try GitHub.
  - https://www.github.com/KeyPair-Consulting/Theseus
- This is the SP 800-90B assessment tool that I wrote while working at UL.
- This tool is now owned by KeyPair.
- KeyPair generously agreed to release this tool as open source.
- The code here is mostly licensed under the 3-Clause BSD license, with some small parts more liberally licensed.
- You can use this tool to perform all the testing approaches that I presented today.

Questions?