Some Approaches to Generate $H_{submitter}$ for Periodically Sampled Ring Oscillators

… or

Lies My Stochastic Model Told Me

Joshua E. Hill, PhD

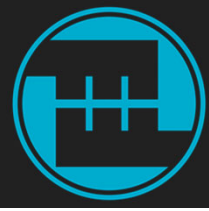
ICMC 2021
20210903
(Presentation Version *20210904*-1)

Producing $H_{submitter}$ For Ring Oscillator Designs

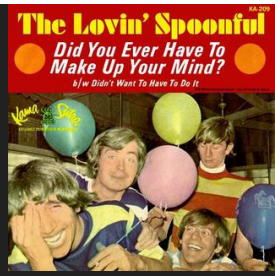
In today's talk, I'll discuss:

- Selecting reasonable assumptions and a compatible stochastic model.
- Establishing conservative model parameters.
- Accounting for external influences.
- Output independence.

Stochastic Models

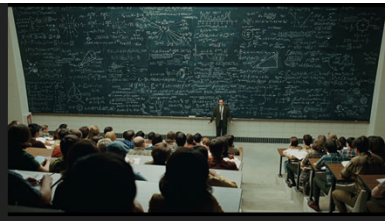


Selecting a Stochastic Model



- There are a variety of stochastic models that can be used to produce min entropy estimates.
- We'll cover a few options and reference a few others.

Stochastic Models



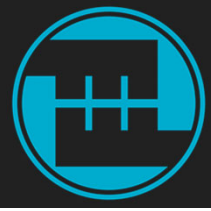
- Killmann, Schindler. *A Design for a Physical RNG with Robust Entropy Estimators*. 2008. Models a pair of noisy diodes and produces an average case Shannon entropy estimate under a weak set of assumptions.
  - [SM.KS] is an adaptation of this model to a periodically sampled ring oscillator under stronger assumptions (as in [MLCXLJ]) which produces a min entropy estimate.
  - [SM.KS-MIN] The [SM.KS] model, adapted into a “worst case” model with a weaker assumption regarding the initial phase distribution.
- Baudet, Lubicz, Micolod, Tassiaux. *On the Security of Oscillator-Based Random Number Generators.* 2010. Produces an average-case per-bit Shannon entropy.
  - [SM.BLMT] is an adaption of this model that produces a min entropy estimate.
  - [SM.BLMT-W] denotes a wide-output variant of the [SM.BLMT] model.
- [SM.J] Ben Jackson’s “serial XOR” model presented at the CMUF Entropy WG meeting on 20190618.
- Markku-Juhani O. Saarinen’s model from *On Entropy and Bit Patterns of Ring Oscillator Jitter*. 2021.
  - [SM.S] denotes the average case per-bit model.
  - [SM.S-W] denotes the wide-output model.

All of these models are conceptually related, but vary in how they perform the calculation.

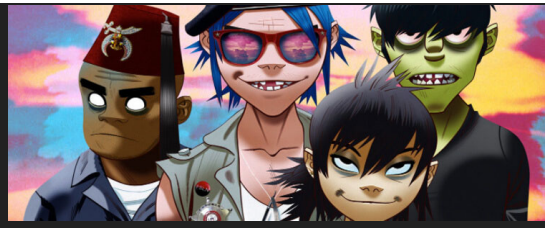
Common Ground

Some assumptions apply to all the models examined here:

- [A.JDist] The credited period (time) variation (jitter) is normally distributed and IID.
  - This isn't too wild, as the local Gaussian noise is mainly due to junction thermal noise, which induces this distribution.
  - This is not the same as saying that the output is IID.
  - Note the original Killmann-Schindler assumption set is somewhat weaker than this.
- Miscellaneous Numerical Analytic Assumptions [A.NumA]
  - $\sigma_o \ll T_o$



Assumptions, Inc.



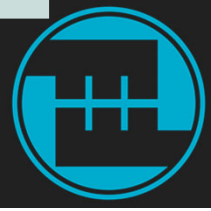
The selection of appropriate assumptions is fundamentally important in this process.

- Predictability of variation:
  - [A.AV] All variation is unpredictable vs
  - [A.SV] Only some subset of variation is unpredictable.
- Attacker Assumptions:
  - [A.KSP] Attacker knows starting phase vs
  - [A.ISP] Attacker can influence the starting phase.
- Accumulated Jitter Assumptions:
  - [A.AJL] Credited accumulated jitter is large vs
  - [A.AAJ] Any credited accumulated jitter is meaningful.
- XOR Processing:
  - [A.XOR] Consecutively sampled bits are serially XORed vs
  - [A.NXOR] Sampled bits are not serially XORed.

When you Assume…

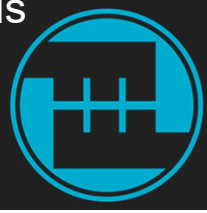
The assumptions establish which stochastic model is meaningful.

Model	A.AV	A.SV	A.KSP	A.ISP	A.AJL	A.AAJ	A.XOR	A.NXOR
SM.KS	X	X	X		X	X		X
SM.KS-MIN	X	X	X	X	X	X		X
SM.BLMT	X	X	X		X			X
SM.BLMT-W	X		X		X			X
SM.J	X	X	X		X	X	X	X
SM.S	X	X	X		X	X		X
SM.S-W	X		X		X	X		X

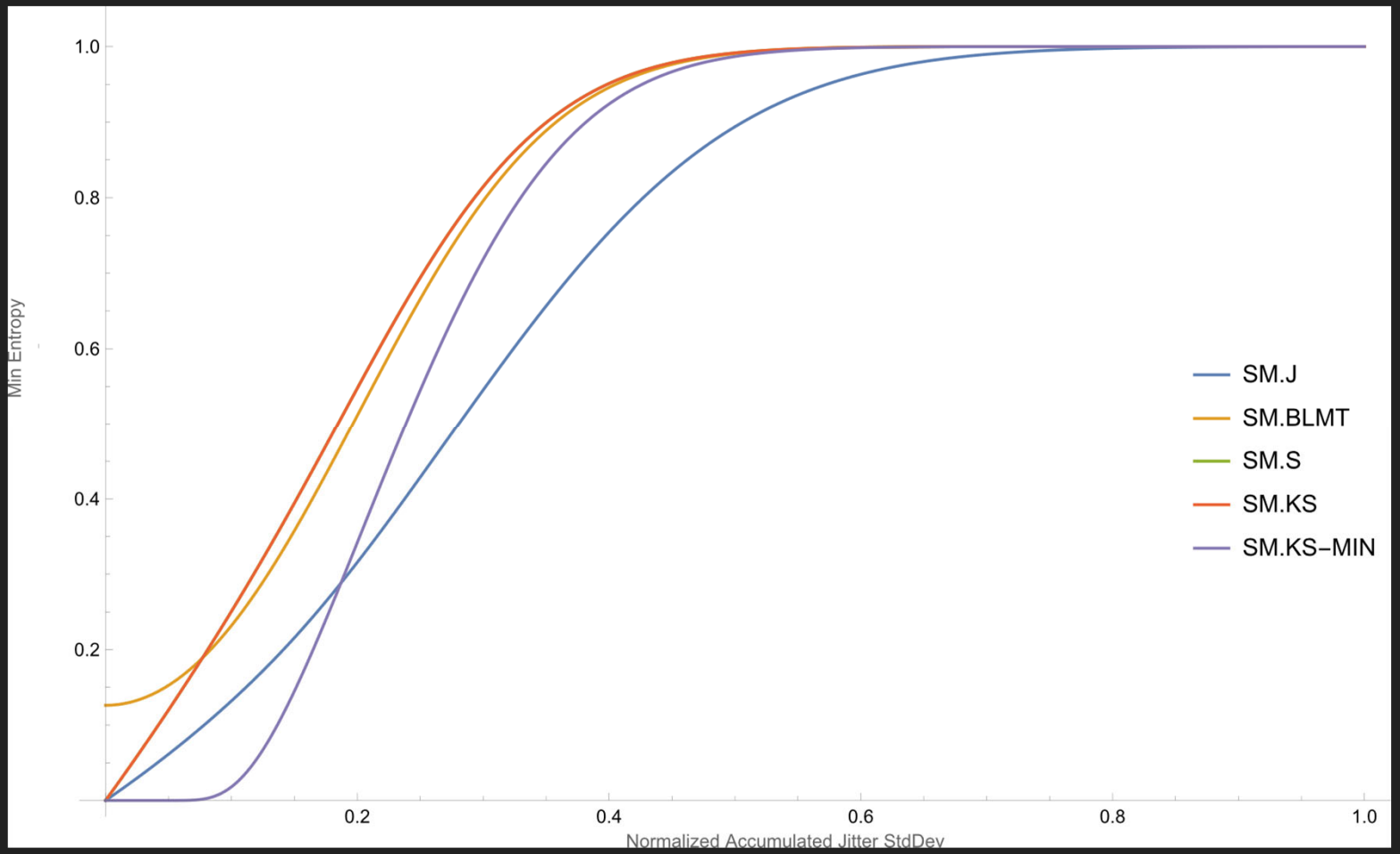


In Summary…

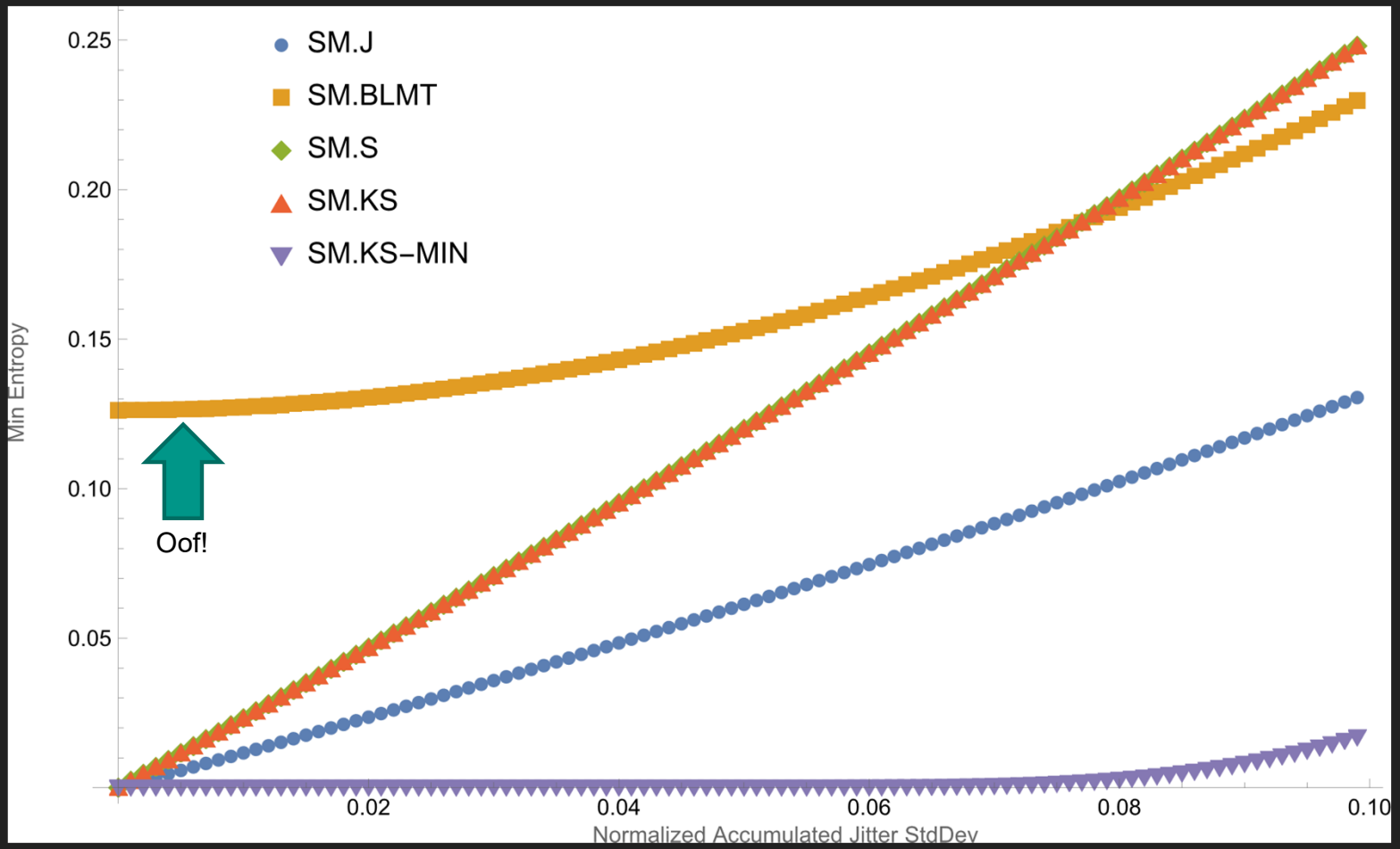
- The “Wide” models (SM.BLMT-W and SM.S-W) require much stronger assumptions; all variation must be IID Normal and unpredictable (A.AV).
  - This assumption isn’t generally valid in the long term.
  - As the size of the tuple increases:
    - The difficulty of calculating these models increases exponentially.
    - The accuracy of these models decreases due to accumulation of correlated variation.
  - This presentation doesn’t further discuss the “wide” models.
- SM.KS-MIN accounts for the most powerful attackers that can set the initial phase (A.ISP). This assumption results in a worst-case min entropy.
- SM.BLMT and its variants require a substantial accumulated jitter (A.AJL); the model only produces reasonable results when the normalized accumulated jitter is at least 10%.
  - This makes the SM.BLMT variants a bad choice for many common designs.
- Serial XOR of outputs can (in the worst case) reduce in min entropy. SM-J accounts for this possible reduction.



What Have You Done For Me Lately?



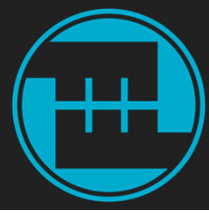
Enhance!


SM.J
SM.BLMT
SM.S
SM.KS
SM.KS−MIN
Min Entropy
0.25
0.20
0.15
0.10
0.05
Oof!
0.02
0.04
0.06
0.08
0.10
Normalized Accumulated Jitter StdDev

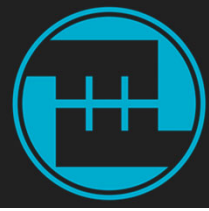
And...?

Some high level observations:

- SM.S and SM.KS produce essentially equivalent results.
- SM.KS-MIN produces the lowest entropy estimate in most common parameters ranges.
  - This isn't surprising, as the attacker is more powerful in this model.



Model Parameters



What Parameters?

- All of these models can be phrased in terms of a single normalized accumulated jitter proportion (called “quality” in various of these papers).
- σ_o denotes the (credited) jitter standard deviation, T_o $(= 1/f_o)$ is the ring oscillator’s period, and T_s $(= 1/f_s)$ is the sample period.

Jitter Proportion

$$\tilde{\sigma}_o = \frac{\sigma_o}{T_o}\sqrt{\lfloor T_s/T_o \rfloor}$$

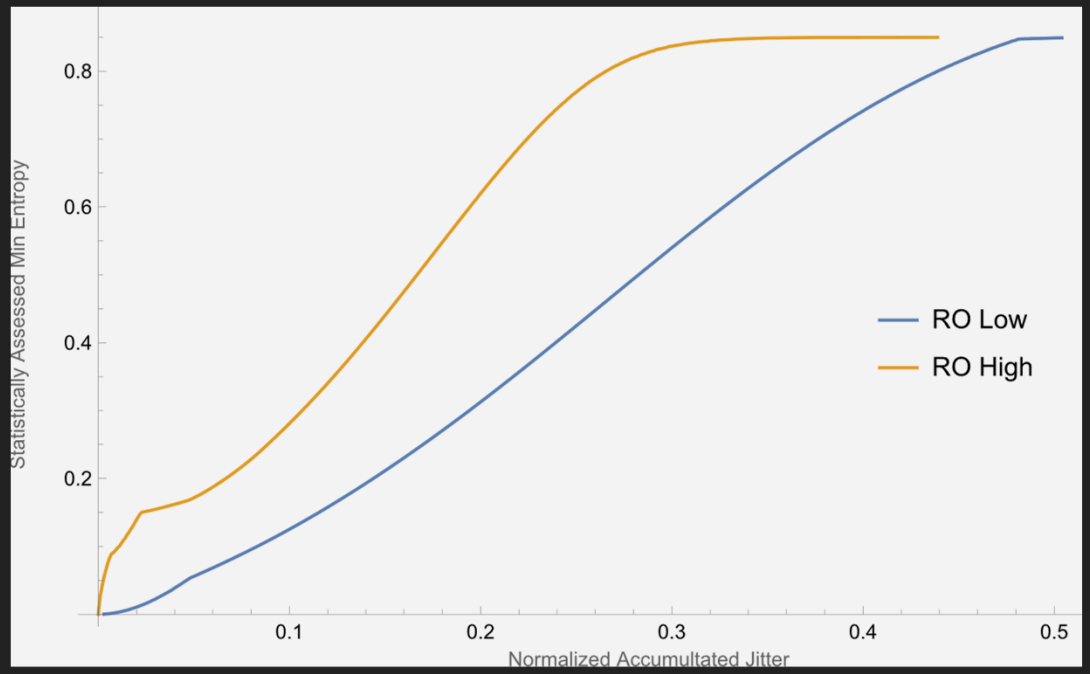
Number of RO cycles per sample

$$= f_o \sigma_o \sqrt{\lfloor f_o/f_s \rfloor}$$

Whence, Parameters?

We can arrive at this parameter in a number of ways:

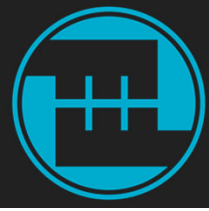
- Measure the value directly.
- Simulate the circuit / process.
- Infer the parameter from statistical test results.



Parameters, What?

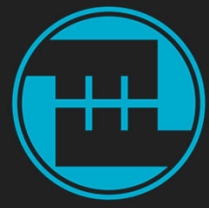
There are… complications.

- Direct measurement can pose problems:
  - Measurement is best accomplished on-chip.
  - External measurement is likely to overestimate jitter due to the capacitive effects of probes, pins, traces, etc.
- These parameters generally vary significantly (often by a factor of 2-10) across the PVT range.
  - The “worst case” values (those producing the smallest modeled entropy) should be used.



Parameters, Ugh!

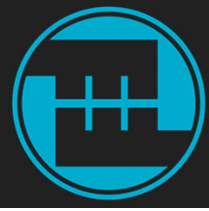
- The obtained parameters generally account for all variation.
- We can only credit entropy from the unpredictable portion of the variation, generally that due to local Gaussian jitter (A.SV).
  - Such variation is normally distributed and independent (as required by our models!)
  - Other variation (e.g. 1/f noise) is generally highly correlated and can accumulate more quickly than variation due to independent sources.
  - Correlated variation is likely to eventually dominate the uncorrelated variation (but the uncorrelated variation is still present!)



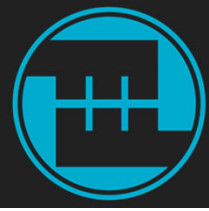
Ewww… Parameters!?!

How to establish the proportion of variation due to local Gaussian jitter?

1. Use a differential design where non-local variation is “canceled”, e.g. [BLMT].
   - Note, the local correlated variation still impacts the measurement, but may be small in many systems.
2. Simulation of variation due to local Gaussian jitter.
3. Gathering many data sets at different sampling rates, and then using curve fitting, e.g. [HTBF] and [ZCFCXF].
4. Estimating this value using publicly available information (e.g., about 30.5% in [BLMT])



External Influences

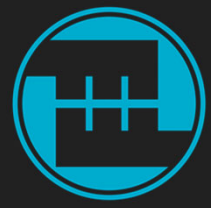


Curse you Christiaan Huygens!

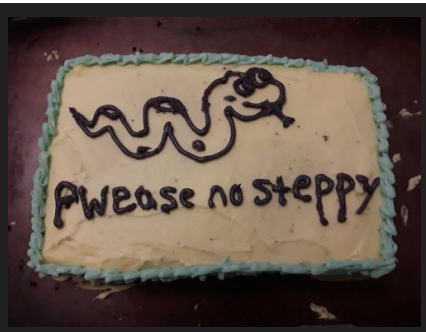
Oscillators can be influenced by each other and by external signals (e.g., other elements in the same package or through frequency injection).

- Entrainment tends to be more of an issue for ring oscillators with similar designs (e.g., using the same delay elements) that are not electrically well isolated.
- There are a few relevant studies into this entrainment in noise sources:
  - In [BBFV], the authors note that up to 25% of the rings in their design appeared to readily entrain.
  - In [MBBF], the authors noted that full ring entrainment tended to only occur when the nominal frequencies of the rings were close (<3% difference) to the entrained frequency.
  - These studies don't investigate entrainment at the delay element level.
- In the absence of effective design protections against entrainment, it is conservative to presume that some of the included ring oscillators are entrained, and do not contribute entropy.

Independence and Conditional Entropy



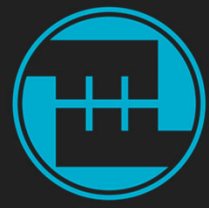
“Give Me Liberty, or Give Me Cake!”



Output symbols are not expected to be independent. Absent an output independence claim, how do we know how entropy accumulates?

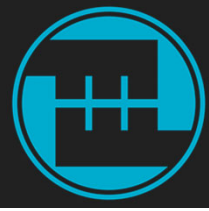
- So long as we only credit variation due to independent variation, the estimate serves as a lower bound for the conditional entropy (min entropy conditioned on prior outputs, i.e., the non-mutual portion of the information).
- Crediting only the conditional entropy allows for straight-forward entropy accounting.
- This approach depends on correctly bounding the portion of observed variation due to local Gaussian noise.

In Conclusion



On Why Hard Problems are Hard

- Stochastic models are not magical things that smell pleasant and produce truth.
- In order to get meaningful results from a ring oscillator stochastic model, one must:
  - Understand which assumptions are reasonable for the design and implementation under analysis,
  - Select a stochastic model that is compatible with those assumptions,
  - Estimate the relevant parameters in a conservative way, and
  - Discard entropy from ring oscillators that may be entrained.

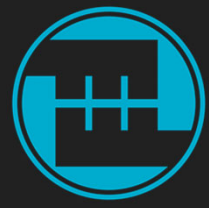


Reasonable Results Require Care

“Garbage In, Garbage Out!” Applies Here

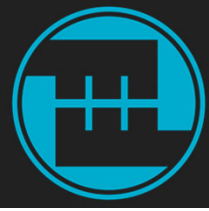
Implementations

- The models that are covered in detail here are all implemented in Theseus's "ro-model" tool.
  - These all take normalized accumulated jitter standard deviation and report min entropy estimates.
- Parameter inference can be accomplished using the NIST statistical test suite and Theseus's "linear-interpolate" tool.



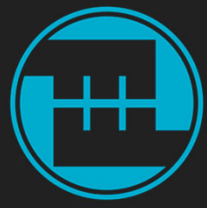
References (Stochastic Models)

- [SM.KS] Killmann / Schindler. *A Design for a Physical RNG with Robust Entropy Estimators*. 2008.
- [MLCXLJ] Ma, Lin, Chen, Xu, Lie, Jing. *Entropy Evaluation for Oscillator-based True Random Number Generators*. 2014.
- [SM.BLMT] Baudet / Lubicz / Micolod / Tassiaux. *On the Security of Oscillator-Based Random Number Generators.* 2010.
- [SM.J] Ben Jackson's "serial XOR" model presented at the CMUF Entropy WG meeting on 20190618.
- [SM.S-*] Markku-Juhani O. Saarinen's model from *On Entropy and Bit Patterns of Ring Oscillator Jitter*. 2021.



References (Parameters)

- [HTVF] Haddad, Teglia, Bernard, Fischer. *On the assumption of mutual independence of jitter realizations in P-TRNG stochastic models*. 2014.
- [ZCFCXF] Zhu, Chen, Fan, Chen, Xi, Feng. *Jitter Estimation with High Accuracy for Oscillator-Based TNRGs*. 2019.
- [BBFV] Bochard, Bernard, Fischer, and Valtchanov. *True-Randomness and Pseudo-Randomness in Ring Oscillator-Based True Random Number Generators*.
- [MBBF] Mureddu, Bochard, Bossuet, and Fischer. *Experimental Study of Locking Phenomena on Oscillating Rings Implemented in Logic Devices.* 2019.



References (Software)

- [GitHub] https://github.com/KeyPair-Consulting/Theseus