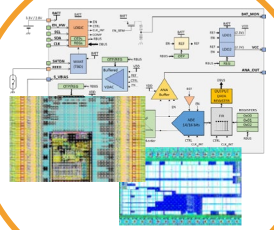
Some Pitfalls to Consider When Designing a TRNG

Grégoire Gimenez

2024/11/20

IC’Alps in a Nutshell

In-house Design Expertise



Analog & digital

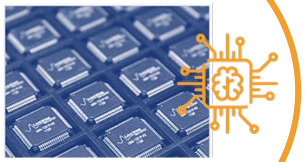
Embedded computing (ARM, RISC-V, …)

Sensor / transducers interfaces

Power management, energy harvesting

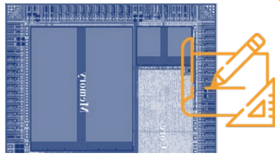
Hardware security

Turnkey Project



Prime contractor, taking full responsibility for milestone deliveries from idea/spec/RTL

Design & Back-end services for ASIC or IP level



A-la-carte – Start & stop to complement customers’ team

Certified QMS

First-time-right project execution

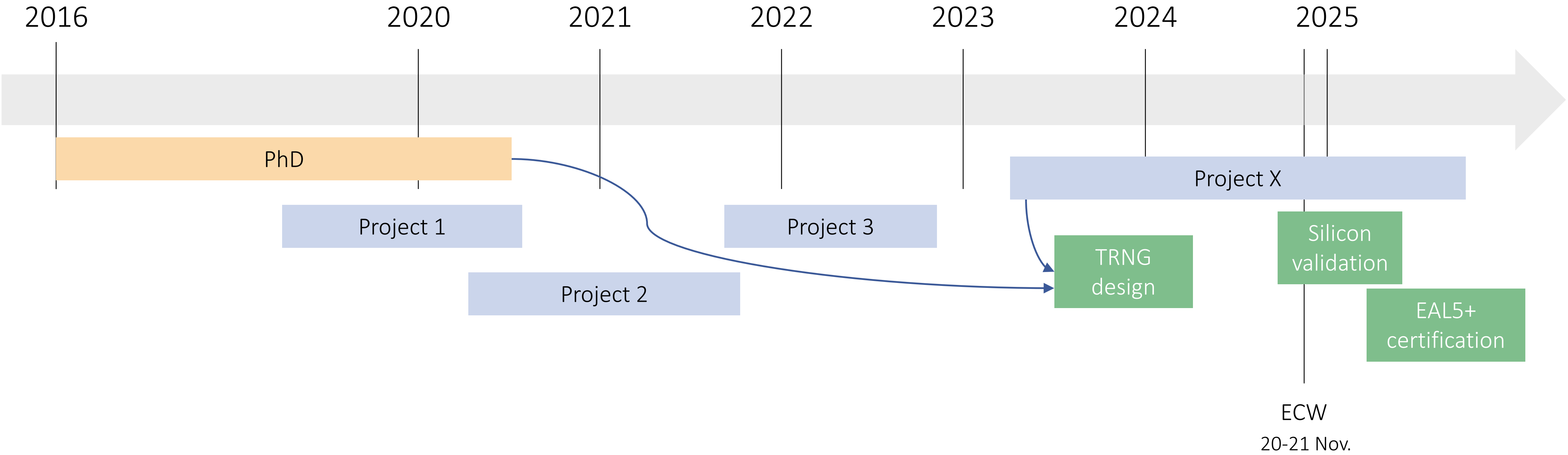
Full traceability

Markets

Medical (Implantable devices, ultrasounds, …)

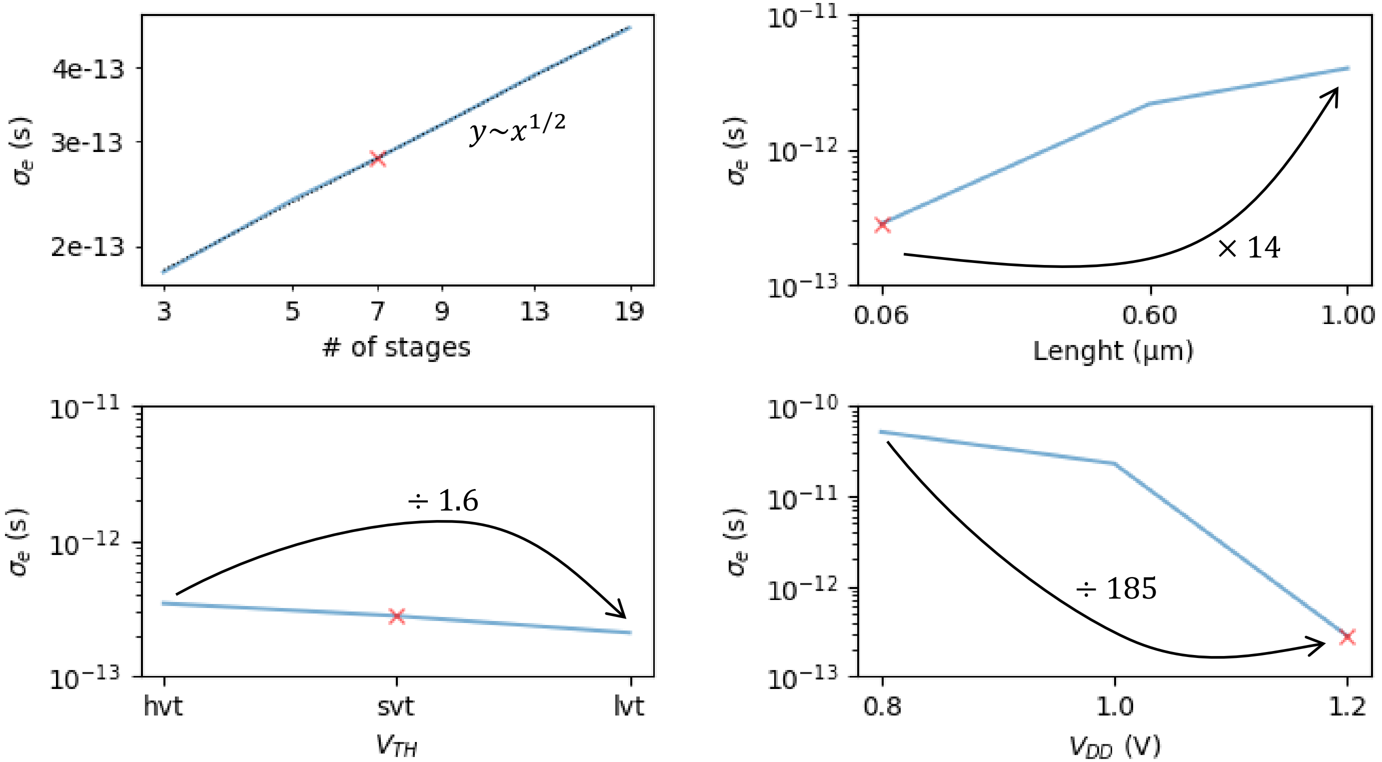
IoT/AI, Industrial, Automotive, Mil/Aero, Identity & Security

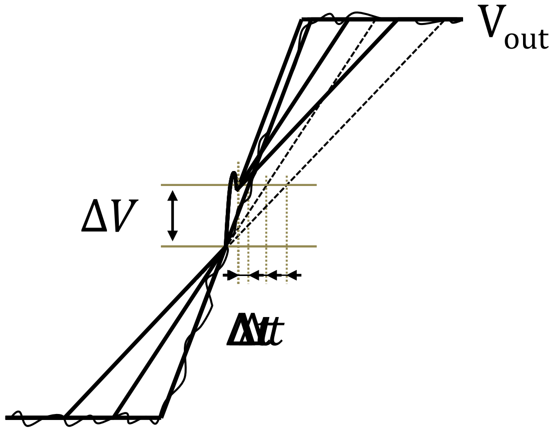
About this Presentation



Noise Amplification

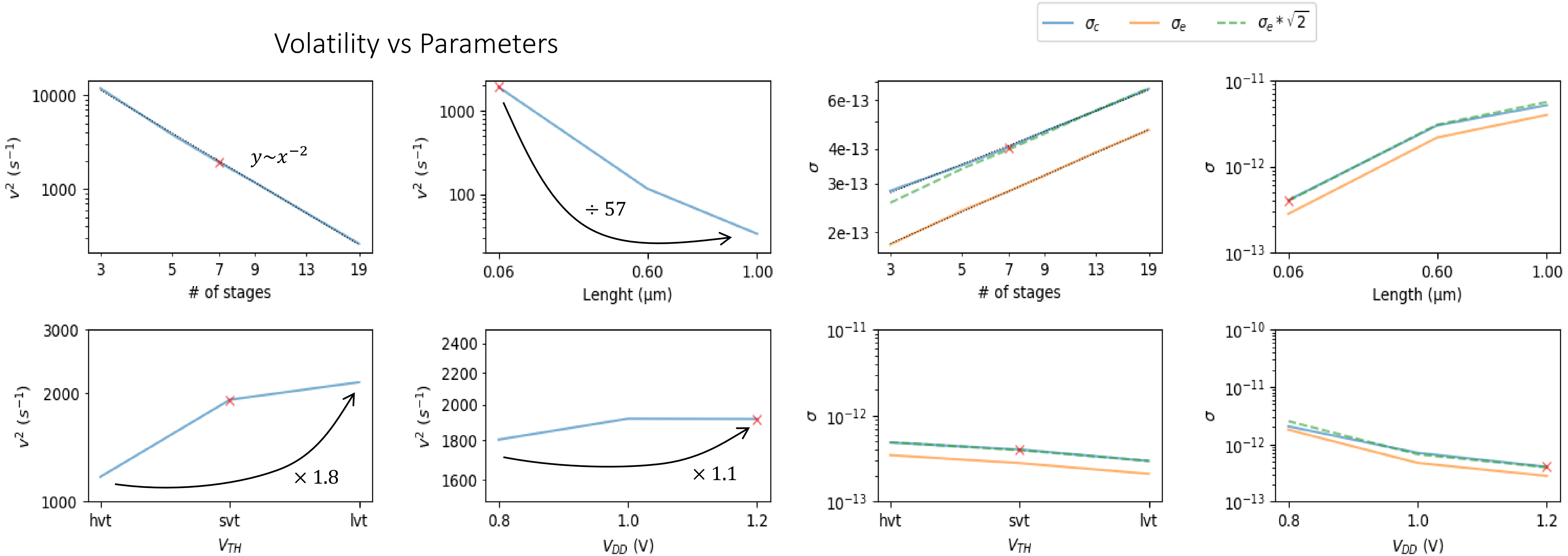
Edge Jitter vs Parameters





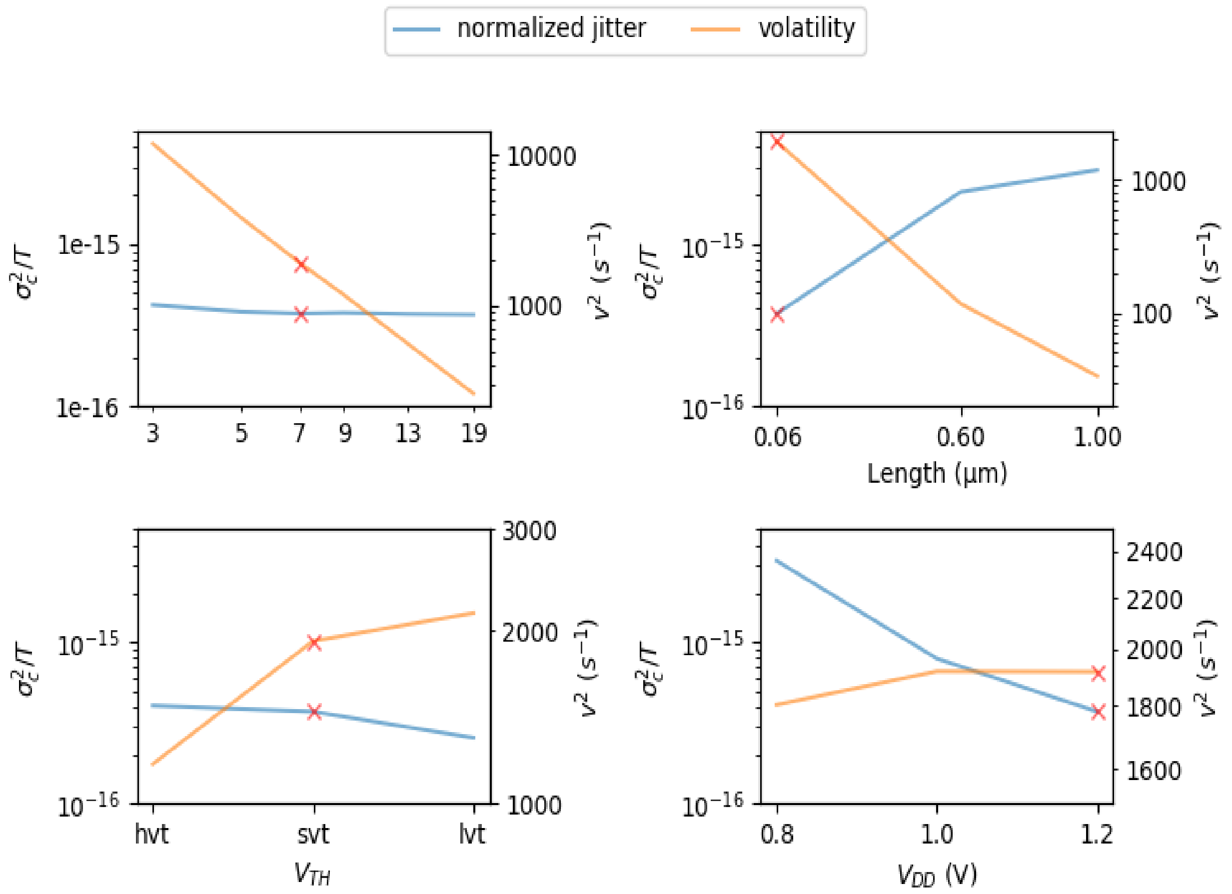
TIPS #1:
Do not hesitate to play with design parameters, there's room for optimization.

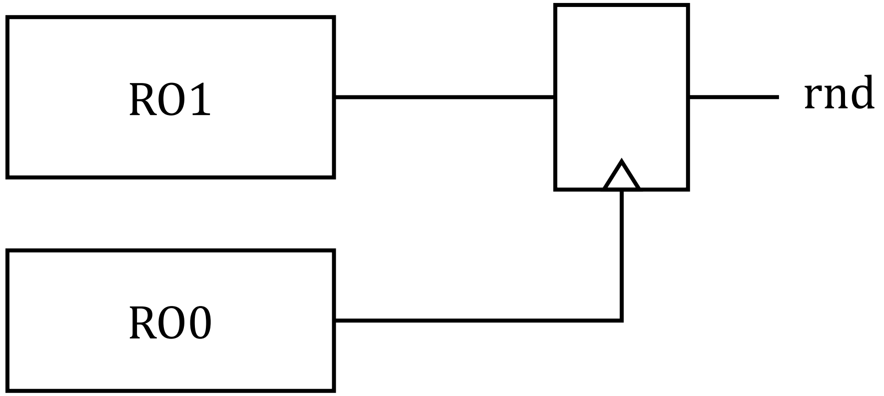
Did You Say Jitter ?



TIP #2:
Don't be fooled by the jitter, look at what matters for your design.

About Quality Factor



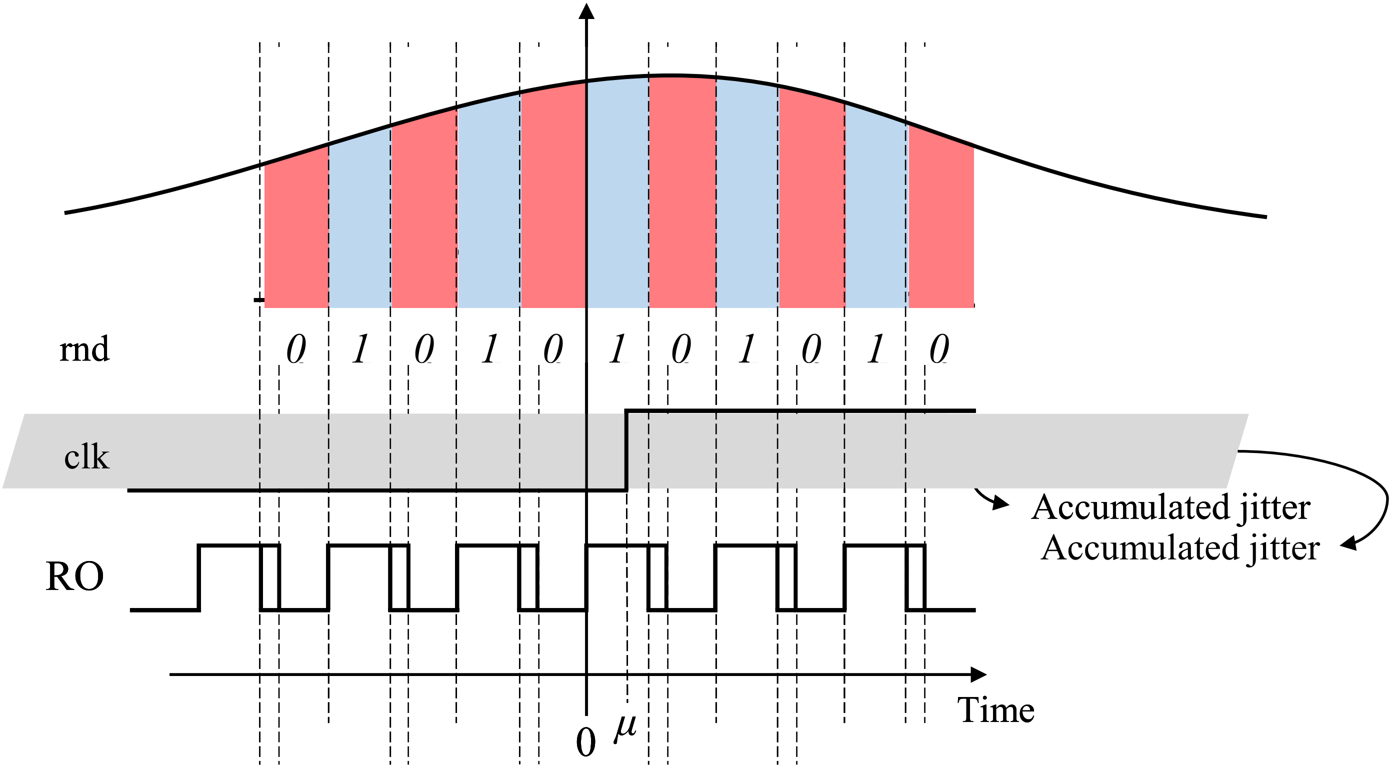


$$Q = T_0 \frac{\sigma_1^2}{T_1^3} + \frac{\sigma_0^2}{T_1^2} = T_0 \left(v_1^2 + \frac{1}{T_1^2} \frac{\sigma_0^2}{T_0} \right)$$

TIP #3:

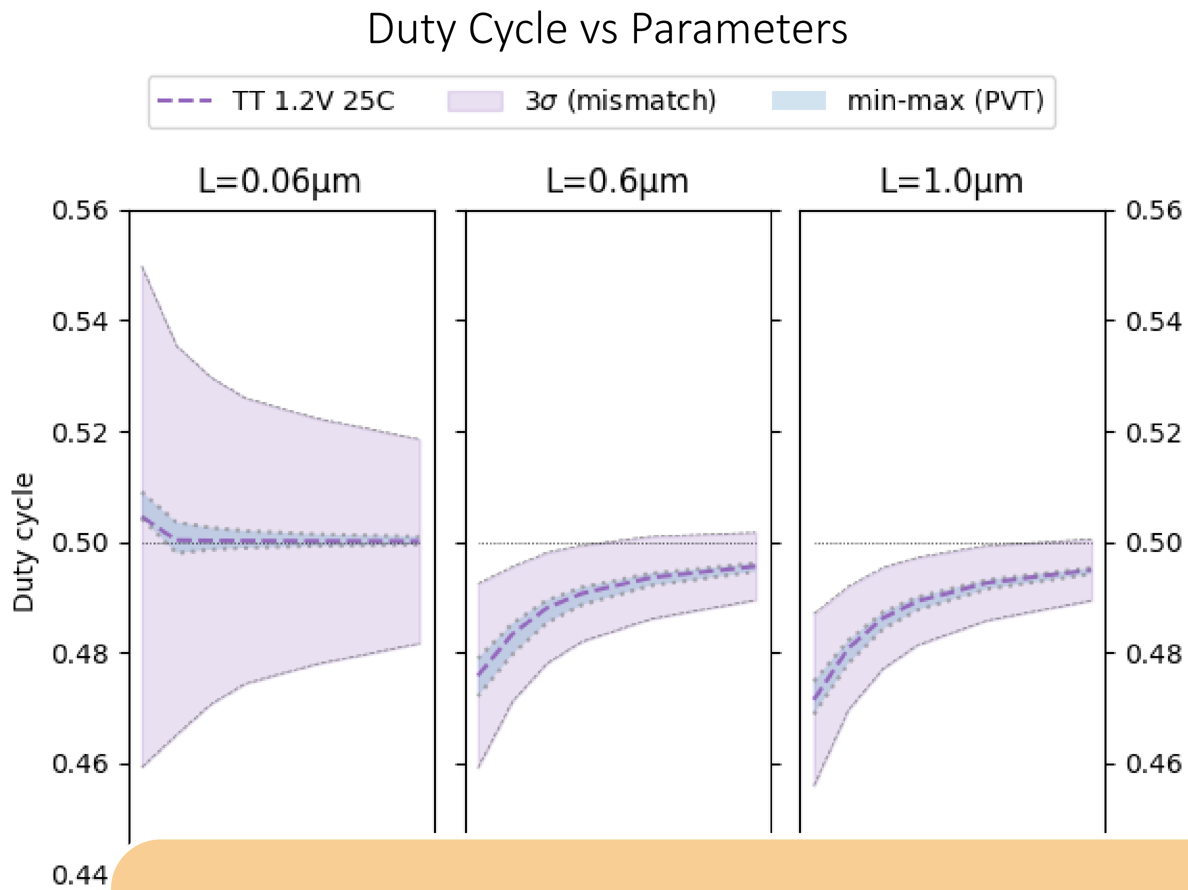
The quality factor is useful for comparing architectures and identifying optimal parameters, but…

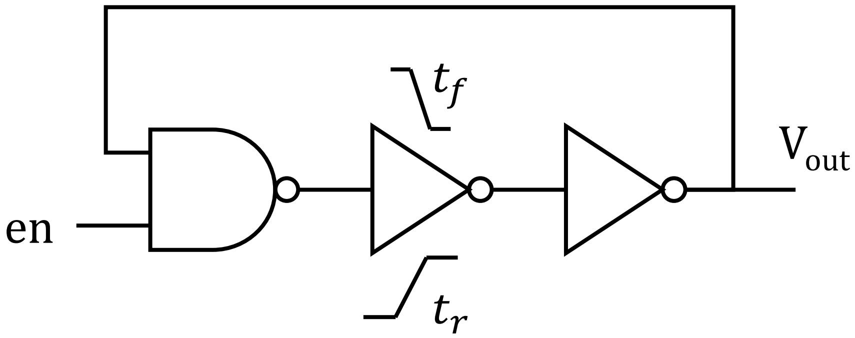
Some Intuitions about Randomness



TIP #4:
You must not forget the duty cycle.

Duty Cycle, the Troublemaker ?





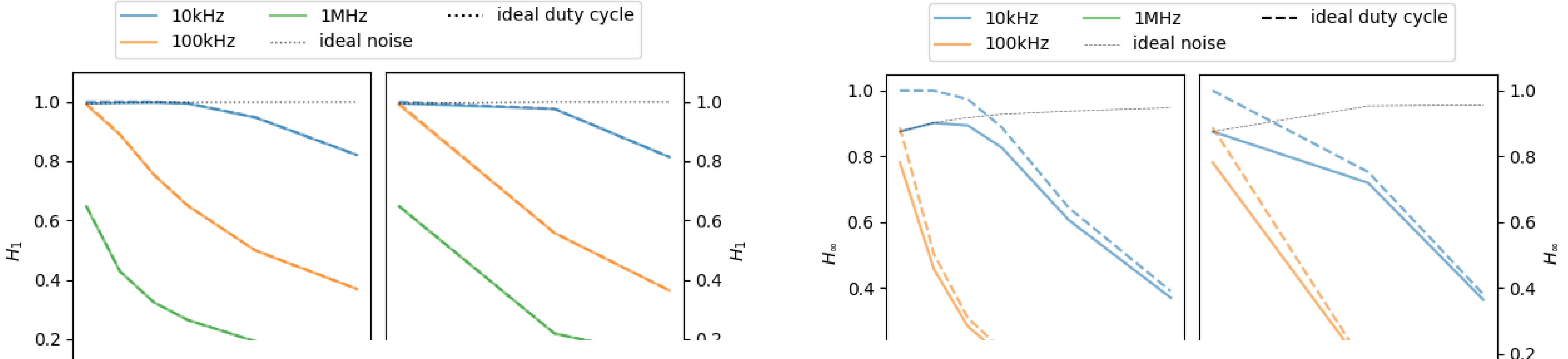
$$DC = \frac{1}{2} + \frac{t_r - t_f}{2N(t_r + t_f)}$$

$$DC = \frac{t_{rN} + \sum_1^{\frac{N-1}{2}} t_{f2i} + t_{r2i-1}}{\sum_1^N t_{fi} + t_{ri}}$$

TIP #5:
Worst-case estimates based on PVTs alone are not sufficient. Use mismatch simulation instead.

A Bit of Entropy

TIP #6:
It is (very) difficult for a single oscillator based architecture to meet such entropy rate targets.



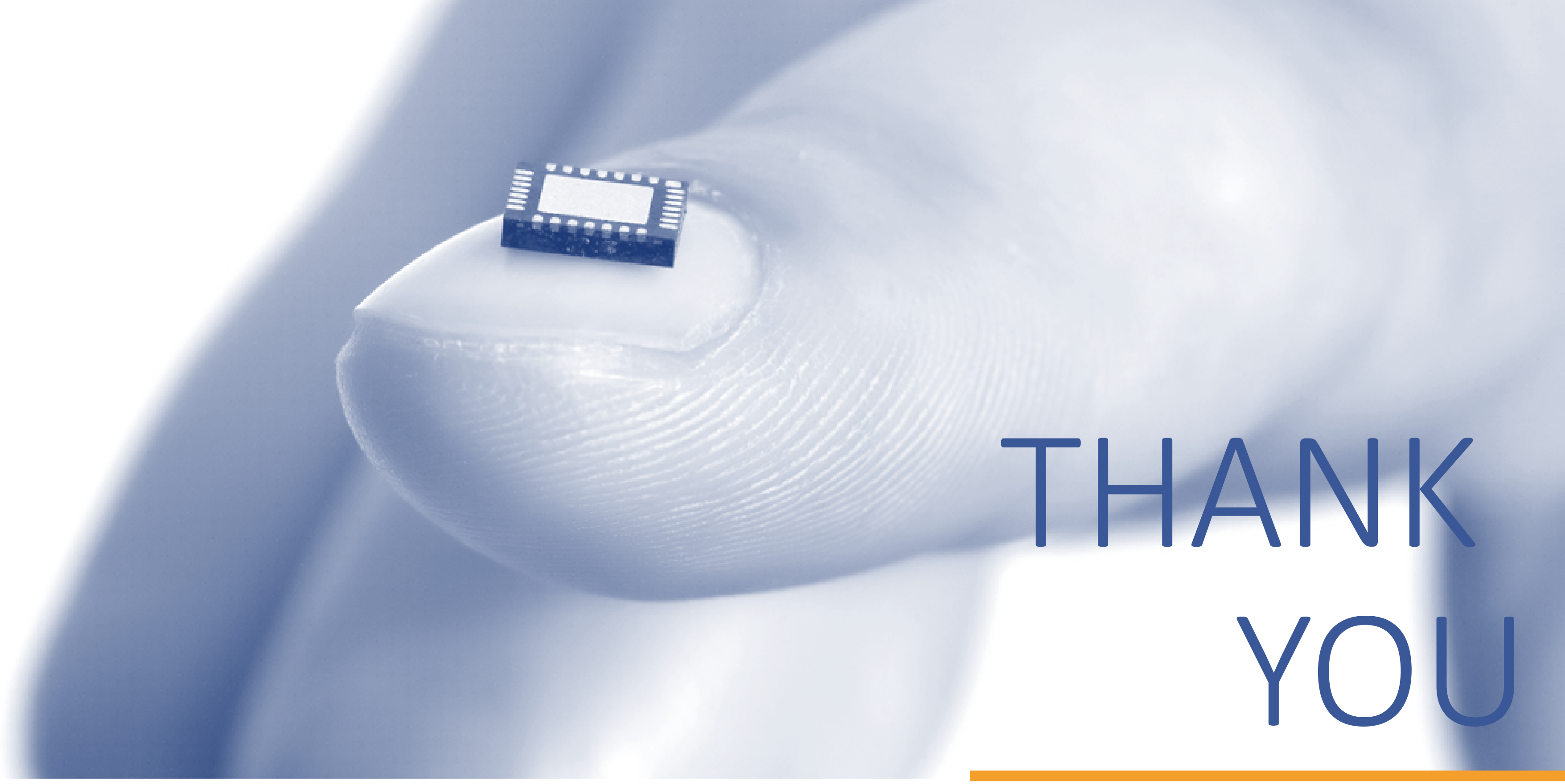
TIP #7:
Architecture using high-volatility RO are more sensitive to duty cycle, especially when considering min-entropy.

Conclusions

- Designing a TRNG is not trivial
  - Many design choices are possible and should be investigated when performance/power/area are targeted
  - Different parts of an entropy source require different optimizations
- Impact of duty cycle on the entropy should not be underestimated
  - Duty cycle should be correctly estimated with monte-carlo simulations
  - We should use stochastic models that takes duty cycle as input parameter
  - Architectures with few high volatility (XORed) ROs are very sensitive to duty cycle
  - They may require internal measurement (and monitoring ?) of the duty cycle
  - Architectures with many low volatility (XORed) ROs may be more efficient, but bring other concerns
- Volatility and duty cycle have opposite trends. It limits the design space.
- These conclusions drawn from a 55nm study, but mostly applicable in any technology node
- Some open questions :
  - Discrepancy between models
  - Are there any correlations between two successive periods for small/large L/starved rings ?
  - Defining a quality factor reunifying both jitter and duty cycle would help strike the right balance

Reference

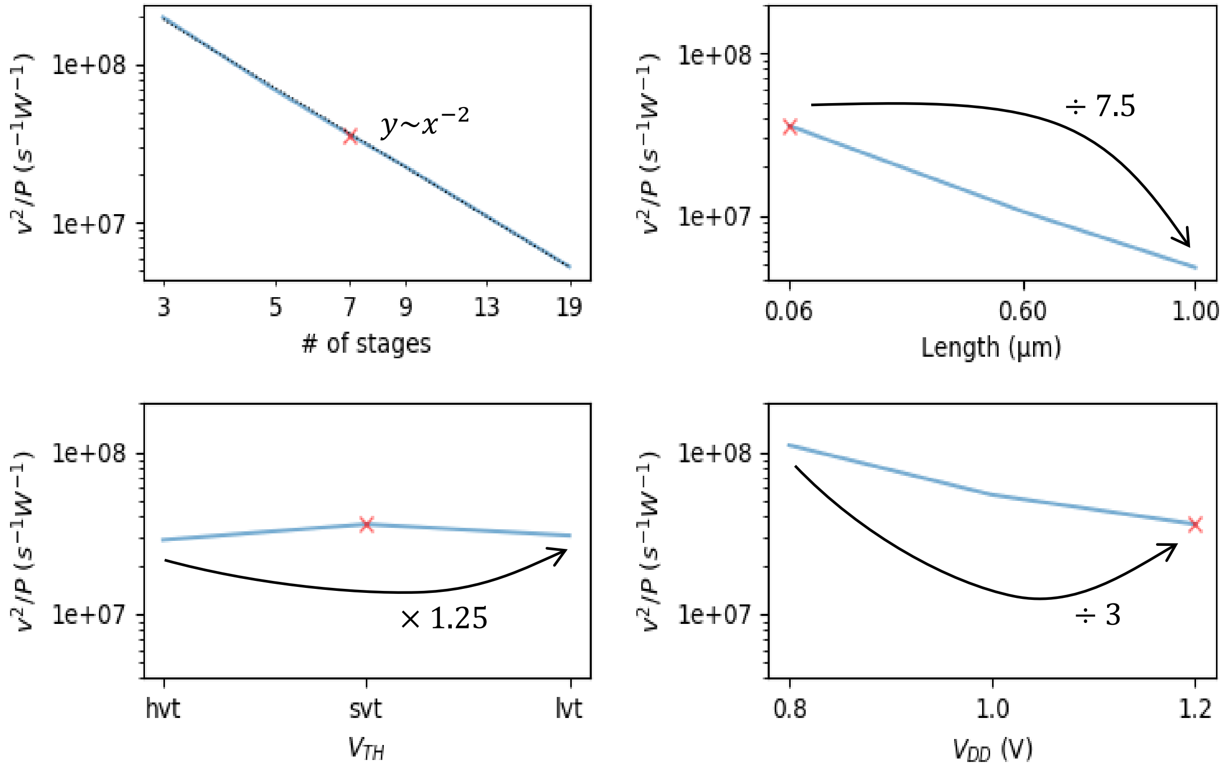
- [Saarinen21] M. J. O. Saarinen « On entropy and bit patterns of ring oscillator jitter ». In : *2021 Asian Hardware Oriented Security and Trust Symposium (AsianHOST)*. IEEE, 2021. p. 1-6.
- [Lubicz24] D. Lubicz and V. Fischer. « Entropy Computation for Oscillator-based Physical Random Number Generators ». *Journal of Cryptology* 37.2. 2024, p. 13.



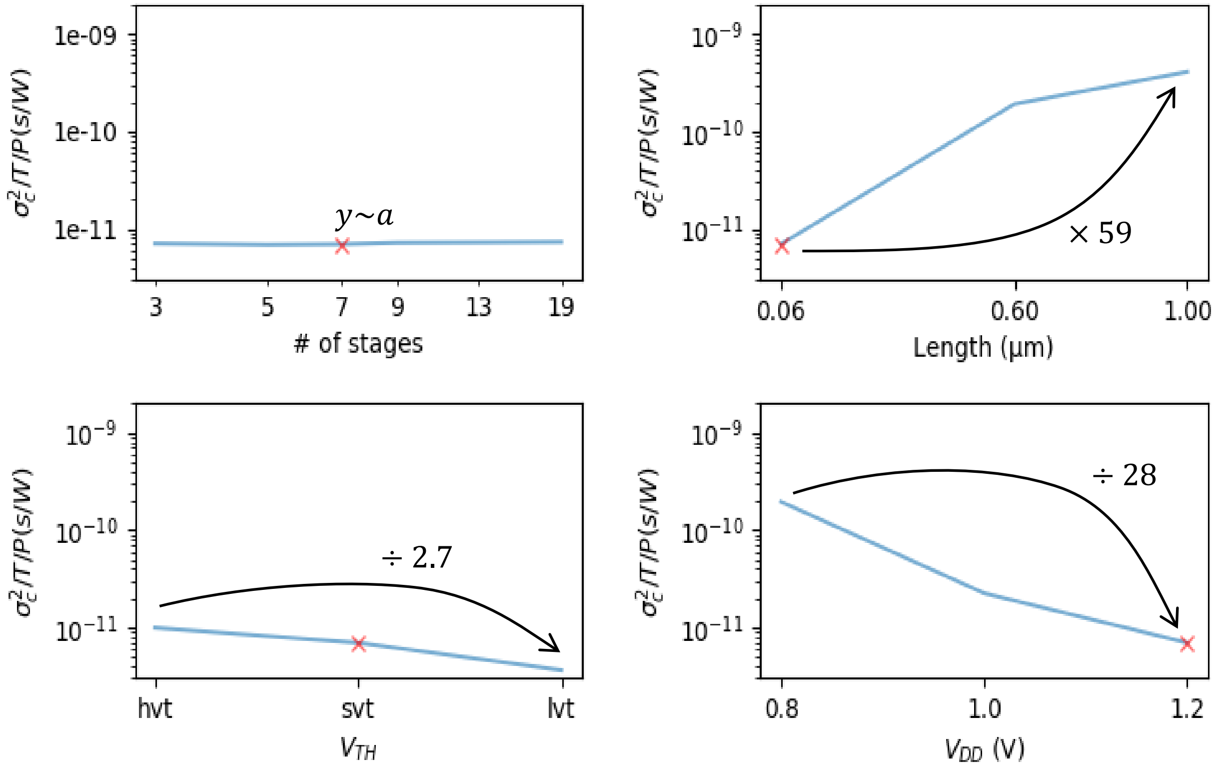
THANK YOU

Efficiency

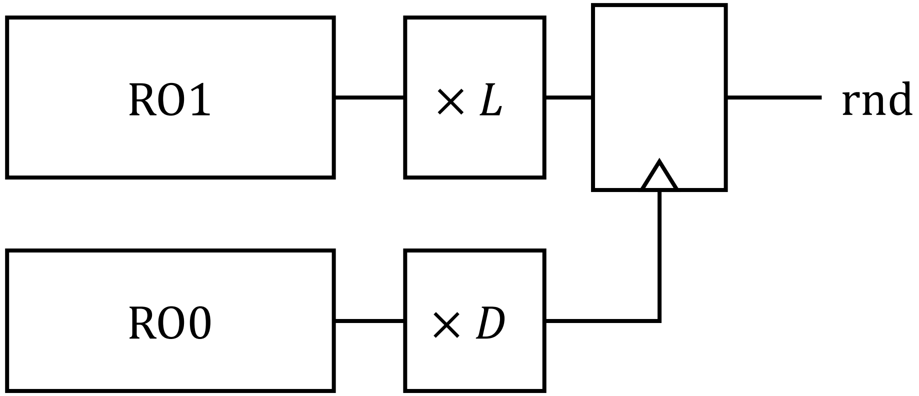
Volatility Efficiency



Normalized Jitter Efficiency



Generalized Architecture

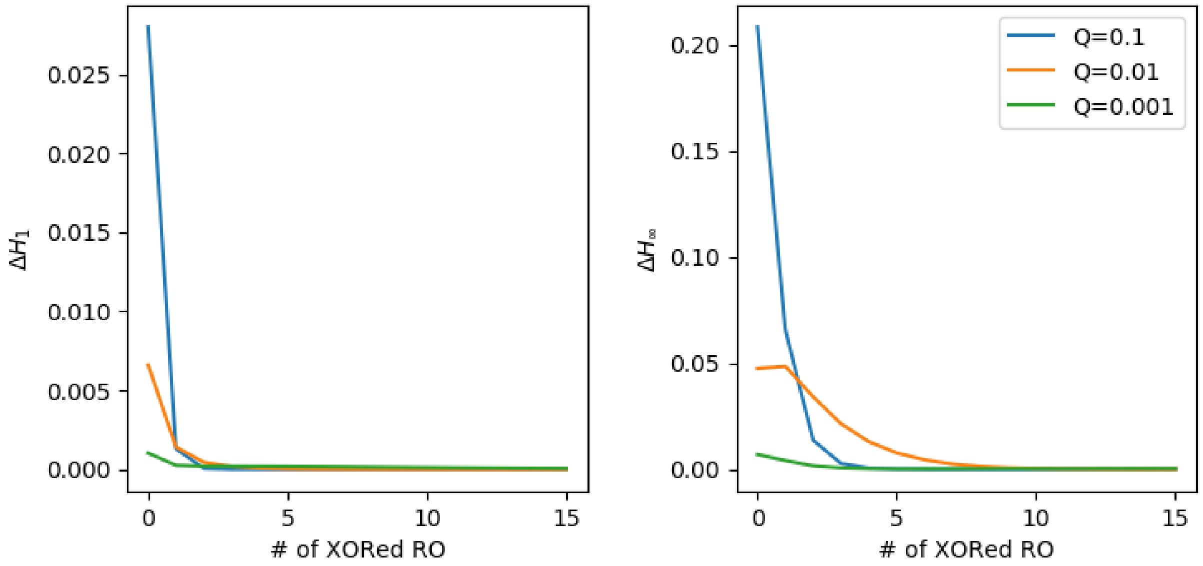


$$Q = v_{eq}^2 \Delta T = \frac{D}{L^2}\frac{T_0}{T_1} \times \left(\frac{\sigma_1}{T_1}\right)^2 + \frac{D}{L^2}\left(\frac{\sigma_0}{T_1}\right)^2$$

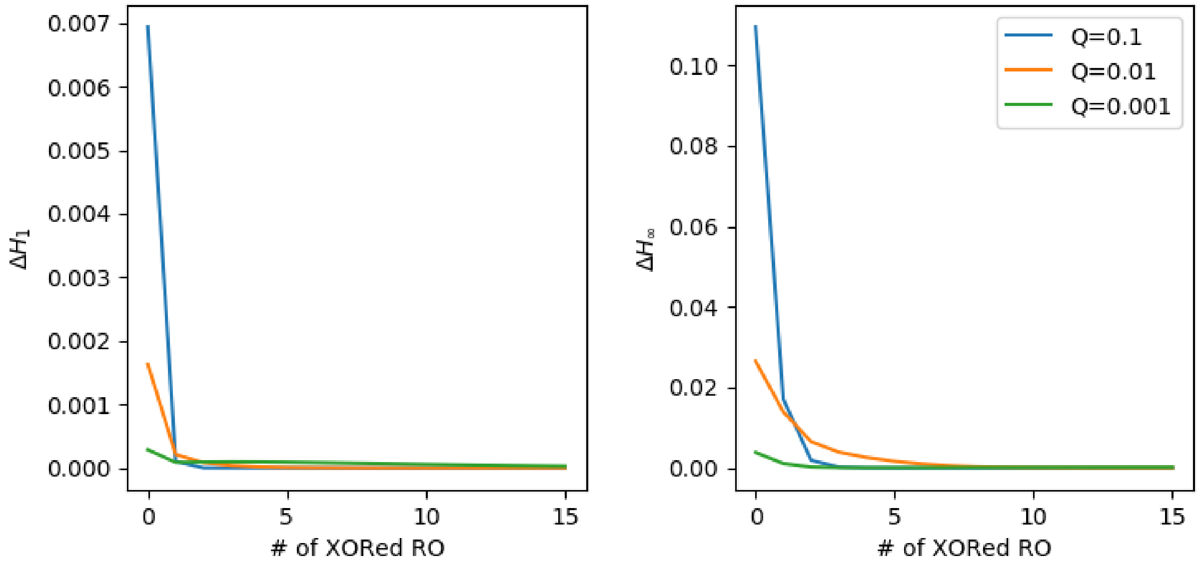
$$v_{eq}^2 = \frac{1}{L^2} \times \left(v_1^2 + \frac{1}{T_1^2}\frac{\sigma_0^2}{T_0}\right)$$

Entropy Loss due to Duty Cycle

Loss of Entropy Rate depending on the # of XORed RO*



DutyCycle=0.4



DutyCycle=0.45

*The loss is calculated against a TRNG with ideal RO (duty cycle=0.5)