On Jitter Transfer in Ring Oscillators and Comprehensive Modelling of 1/f Noises

Maciej Skorski[1]

University of Cantabria

European Cyber Week 2024

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
UC Universidad de Cantabria

[1]The work done during research stay at Hubert Curien Laboratory

Outline

Outline

About Differential Measurement

- Measures the effect by *comparing sensing and referencing signals*
- Widely used, from explosives detection to random number generation

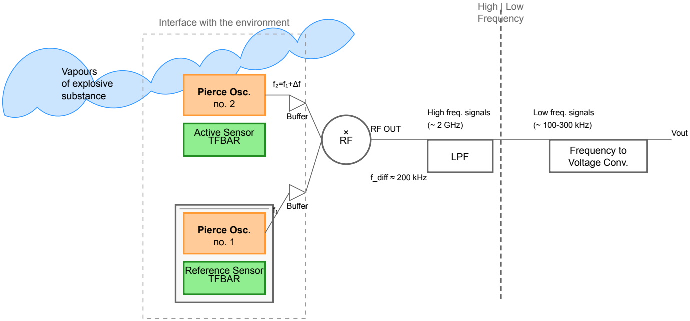


Figure: The mechanism of explosives detection [Vasile et al., 2021]. The sensor's resonating frequency is changed by the mass of attached molecules of explosives. The change can be detected by comparison with a not exposed reference sensor.

Differential Measurement in Oscillatory TRNGs

- Bits are generated by sampling one signal with another, both noisy (!)
- Two noisy signals approximated by a noisy-free + double-noise setup
- *Approximation enables analyses* of TRNGs [Baudet et al., 2011]

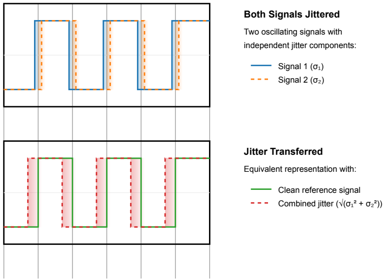


Figure: Jitter Transfer in Ring Oscillators. Two noisy signals are approximated by a noisy-free and double-noisy one, enabling security analysis.

The Challenge

- Key question: is this correct?
- Why it matters: critical for quantitative security evaluation
- Mathematical formulation: two noisy oscillatory signals

$$
\begin{aligned}
s_0(t) &= w(\phi_0 + f_0 t + \xi_t^0) \\
s_1(t) &= w(\phi_1 + f_1 t + \xi_t^1),
\end{aligned}
$$

  s_1 sampled at the edges of s_0. Here f_i are frequencies, ϕ_i are initial locations, and ξ_t^i are Brownian motions with volatility σ_i modelling phase modulation.
- How do they combine in sampling ?

Key Result: Model of Jitter Transfer

Under the assumption $\sigma_0^2 \ll f_0$:

- Sampling bits from two noisy oscillators equivalent to sampling from:
  - Clock s_0 being jitter-free
  - Signal s_1 having volatility:

$$\sigma = \sqrt{\frac{f_1^2}{f_0^2}\sigma_0^2 + \sigma_1^2}$$

- Error bounds available through normal approximation quality
- Critical for analysing multi-oscillator TRNGs

Difficulty

Analysing arrival times of the rising edges is hard (hitting times).

Exact Statistical Properties

Key Distributions:

- Phase distribution at sampling time T_k:

$$\Phi_1(T_k) \sim \mathrm{N}(\phi_1 + f_1 T_k, \sigma_1^2 T_k)$$

- Clock edge timing for the k-th rising edge:

$$T_k \sim \mathrm{IG}\left(\frac{k-\phi_0}{f_0}, \frac{(k-\phi_0)^2}{\sigma_0^2}\right)$$

- Period distribution between edges:

$$T_{k+1} - T_k \sim \mathrm{IG}\left(\frac{1}{f_0}, \frac{1}{\sigma_0^2}\right)$$

Important Note

These exact formulas enable precise security analysis

Normal Approximation

- When $\frac{\sigma_0^2}{f_0} \to 0$, we have:

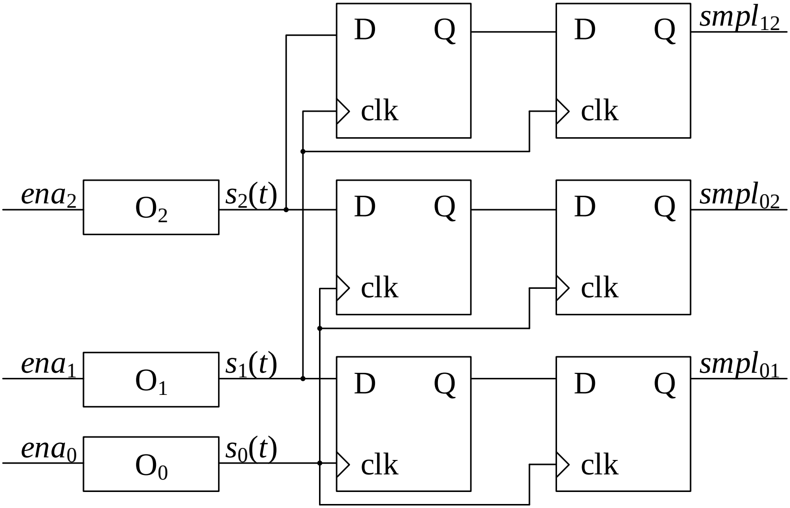
$$\frac{\phi_1(T_{k+1}) - \phi_1(T_k) - \mu}{v} \xrightarrow{d} \mathrm{N}(0,1),$$

  where:
  - $\mu = \frac{f_1}{f_0}$
  - $v = \sqrt{\frac{\sigma_1^2}{f_0} + \frac{f_1^2\sigma_0^2}{f_0^3}}$
- Convergence is uniform in σ_1, f_1
- Quality improves as jitter-to-period ratio decreases

Applications

- Novel tool for analysing multi-ring oscillator TRNGs
- Enables:
  - Quantitative differential jitter measurements
  - Individual oscillator volatility recovery
  - More accurate entropy rate computation
- Two practical methods:
  - Method 1: Assumes linear jitter variance with period
  - Method 2: No assumptions, requires extra hardware

Implementation Details



Implementation Results

Key Findings:

- Hardware tests on Intel Cyclone V FPGA
- Method 1 assumptions not always valid:
  - Significant discrepancies observed
  - $\sigma_0(T_0)$ can vary by factor of 2
- Method 2 more reliable:
  - Consistent results across experiments
  - Proven numerically stable
  - Small hardware overhead (one extra flip-flop)

Details and Future Work

- For technical details, please refer to [Lubicz and Skorski, 2024]
- The techniques use Laplace Transform and results on hitting times
- Extensions to generic Gaussian Processes via [Decreusefond and Nualart, 2008]...?

Outline

Challenge

- Randomness used in games, simulations, cryptography...
- Entropy models needed for security (NIST-90B, AIS20/31)
- Tests confirm pseudorandomness, many fast proposals lack guarantees!
- What is a good stochastic model for voltage/quantum RNGs?

Oscillatory TRNG Basics

- Periodic signal with phase noise:

$$y(t) = \sin(2\pi f t + \xi(t))$$

- Bit extraction by subsampling and checking low/high state:

$$b_n = \begin{cases} 1 & y(nT) > 0 \\ 0 & y(nT) \leq 0 \end{cases}$$

- Security depends on phase noise $\xi(t)$ modelling
- Similar modelling possible for electric field (quantum effects)

Five-Power Noise Law

Per empirical evidence [Howe et al., 1981], for hardware-dependent constants h_α:

- Instantaneous frequency spectrum:

$$S_{\dot{\xi}}(\omega) \approx \sum_{\alpha=-2}^{2} h_\alpha \omega^\alpha$$

- Phase spectrum:

$$S_{\xi}(\omega) \approx \sum_{\alpha=-2}^{2} h_\alpha \omega^{\alpha-2}$$

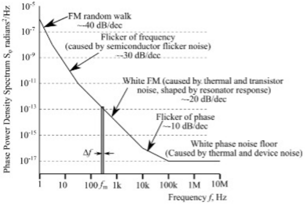


Figure: Five-Power Spectral Law (www.harmanluxuryaudionews.com)

Novel Gaussian Process Phase Model

Assumption: Phase follows Fractional Brownian Motion [Lévy, 1953]

$$\xi(t) = \frac{1}{\Gamma(H+1/2)} \int_0^t (t-u)^{H-1/2} \mathrm{d}B_u$$

where B_u is Brownian motion and H is the Hurst–Hölder exponent.

Key Properties:

- Extends Barnes and Allan's proposal [Barnes and Allan, 1966]
- Non-stationary Gaussian Process
- Flexible to match expected spectral law
- Posterior is Gaussian with uncertainty estimates

Covariance Properties

- The covariance equals

$$\mathbf{Cov}[L_H(t), L_H(t+\tau)] = \frac{2t^{H+\frac{1}{2}}(t+\tau)^{H-\frac{1}{2}}\,{}_2F_1\left(1, \frac{1}{2}-H; H+\frac{3}{2}; \frac{t}{t+\tau}\right)}{\Gamma(H+1/2)^2(2H+1)}.$$

- Important special cases
  - For $H=1$ (flicker noise)

$$\mathbf{Cov}[L_0(t), L_0(t+\tau)] = \frac{1}{\pi}\left(\sqrt{t}\sqrt{t+\tau}(2t+\tau) - \tau^2 \tanh^{-1}\left(\frac{\sqrt{t}}{\sqrt{t+\tau}}\right)\right),$$

  - For $H=1/2$ (white noise)

$$\mathbf{Cov}[L_1(t), L_1(t+\tau)] = t.$$

- Sampling can be easily implemented, also on GPU!

Path Samples

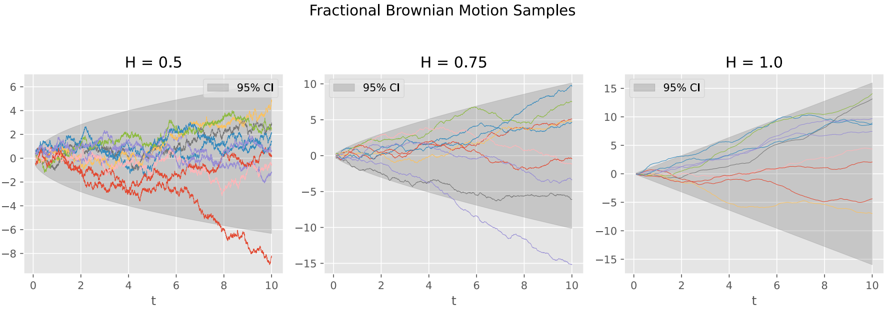


Figure: Path Samples using Cholesky's Decomposition.

Spectral Properties

Flexibility of Gaussian Process matches empirical law:

- Wigner-Ville spectral density (time-averaged):

$$S_{\xi}^{WV}(\omega) \approx \omega^{-2H-1}$$

- $H = 1$: flicker frequency modulation ($\alpha = -1$)
- $H = 1/2$: white noise frequency modulation ($\alpha = 0$)

Power Spectral Density

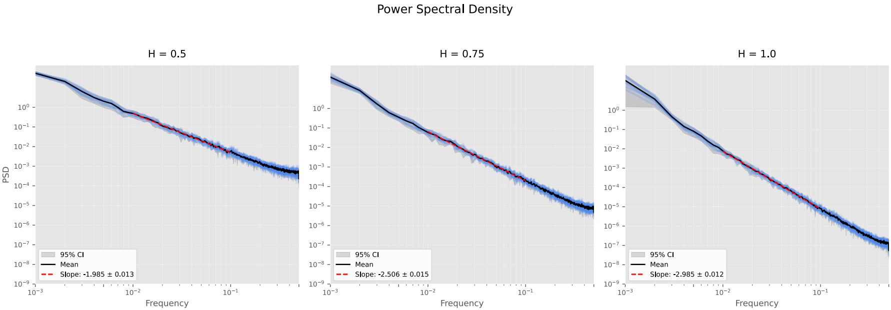


Figure: Spectral Density using Welch's Estimator.

Security Analysis

Approach:

- Focus on flicker and white noise components
- Evaluate unpredictability of next phase $X = X_n$
- Consider attacker knowing past locations $Y = X_1, \ldots, X_{n-1}$
- Use Schur-complement leakage rule:

$$\mathbf{Cov}[X] = \mathbf{Cov}[X] - \mathbf{Cov}[Y, X]^{\top}\mathbf{Cov}[Y]^{-1}\mathbf{Cov}[Y, X]$$

Key Findings:

- Leftover variance stabilizes away from zero
- Implies unpredictability and non-trivial security
- Strengthens the Monte-Carlo approach [Peetermans and Verbauwhede, 2024]

Leakage Resiliency

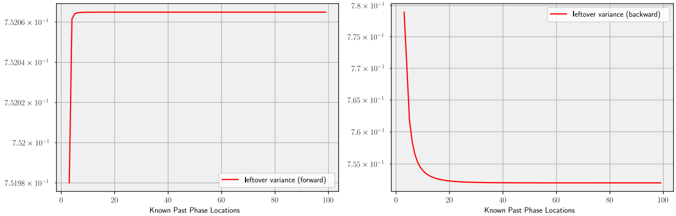


Figure: Leftover variance (conditioned on past locations).

Summary

- Precise model for jitter transfer, application to multi-ring TRNG
- Comprehensive noise modelling using fBm, security through leftover variance

Details and Future Work

- For technical results, see [Skorski, 2024]
- Implementation PoC with GPU acceleration
  https://www.kaggle.com/code/mskorski/fractional-brownian-motion?scriptVersionId=207845405
- TBD: Accurate determination of hardware constants
- TBD: Formal proof of bounded leakage conjecture for leftover variance
- TBD: Optimization of sampling efficiency

Acknowledgements

- Special thanks to Viktor Fischer and Nathalie Bochard!

Outline

References

Barnes, J. and Allan, D. (1966).
A statistical model of flicker noise.
Proceedings of the IEEE, 54(2):176–178.

Baudet, M., Lubicz, D., Micolod, J., and Tassiaux, A. (2011).
On the Security of Oscillator-Based Random Number Generators.
Journal of Cryptology, 24(2):398–425.

Decreusefond, L. and Nualart, D. (2008).
Hitting times for Gaussian processes.
The Annals of Probability, 36(1).

Howe, D., Allan, D., and Barnes, J. (1981).
Properties of Signal Sources and Measurement Methods.
In *Thirty Fifth Annual Frequency Control Symposium*, pages 669–716. IEEE.

III

References

Lévy, P. (1953).
Random Functions: General Theory with Special Reference to Laplacian Random Functions.
University of California Publications in Statistics. University of California Press.

Lubicz, D. and Skorski, M. (2024).
Quantifying Jitter Transfer for Differential Measurement: Enhancing Security of Oscillator-Based TRNGs.

Peetermans, A. and Verbauwhede, I. (2024).
TRNG Entropy Model in the Presence of Flicker FM Noise.
IACR Transactions on Cryptographic Hardware and Embedded Systems, 2024(4):285–306.

Skorski, M. (2024).
Modelling 1/f Noise in TRNGs via Fractional Brownian Motion.

III
References

Vasile, F., Craciun, A., Vladescu, M., Schiopu, P., Feies, V., Busu, I., Codreanu, N., Moise, M., Ionita, S., and Raducu, M. (2021).
Electronic Circuit for Differential Measurement using Resonant Sensors: Designing Approach.
In *2021 13th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, pages 1–6, Pitesti, Romania. IEEE.

Thank you!

Questions?