Modelling Power Noise via Gaussian Processes with Applications to True Random Number Generators

Maciej Skorski

Hubert Curien Laboratory, France
Czech Technical University, Prague

CREACH LABS Cryptography Seminar, June 27, 2025

Outline

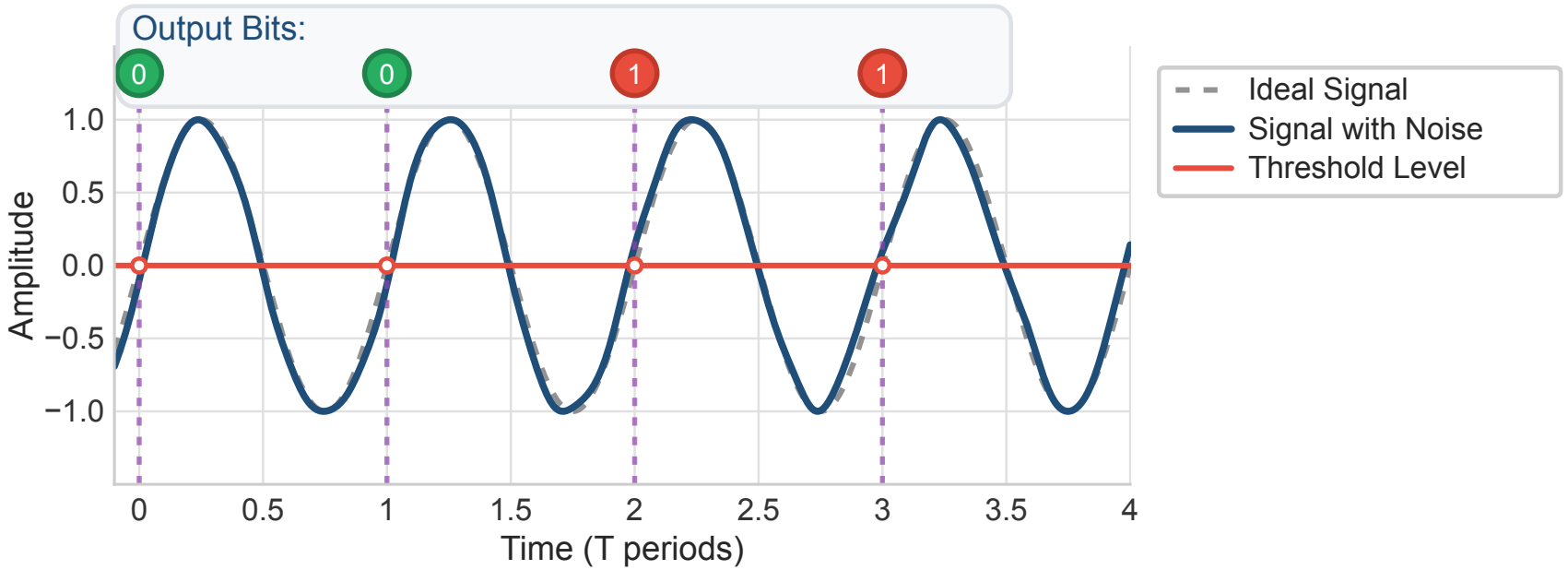
Oscillatory Random Number Generators

- Leverage physical noise in electronic circuits for cryptography
- Generate bits by thresholding instantaneous phase:

$$b_t = w(2\pi f_0 t + \phi_0 + \phi_t)$$

where w is a square wave with duty cycle α and ϕ_t is phase noise.

- Randomness due to signal crossings earlier or later than expected



Modelling Challenge

- Electronic principles and experiments provide understanding of spectrum...

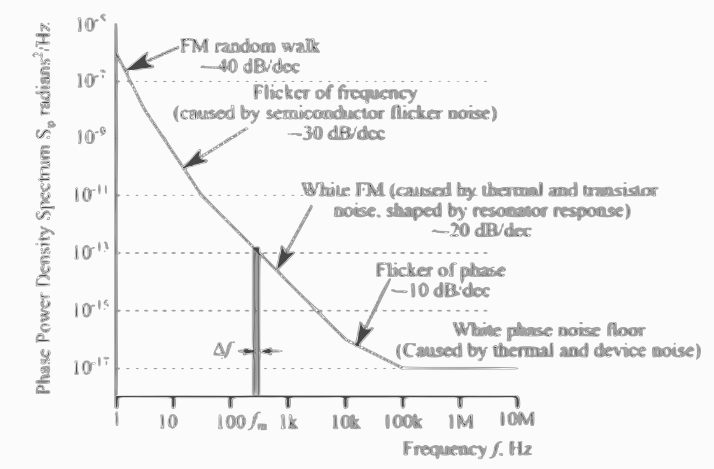


Figure: Power Law for phase spectrum.

Leeson's model of noise in oscillators [Lee66]

$$S_\phi(\omega) = \frac{2FkT}{P_s}\left(1+\left(\frac{\omega_0}{2Q_L\omega}\right)^2\right)\left(1+\frac{\omega_c}{\omega}\right)$$

where $S_\phi(\omega)$ is phase noise PSD, F is amplifier noise factor, k is Boltzmann's constant, T is temperature, P_s is signal power, ω_0 is carrier frequency, Q_L is loaded quality factor, ω_m is offset frequency, and ω_c is flicker corner frequency,...

- **Cryptographic security** requires *time-domain* properties, particularly conditional dependencies / predictability under partial observation (leakage)
- **Gap:** Spectral models $\neq$ temporal correlation models

Related Work

- Basic properties of 1/f noise correlations studied [Kes82]
- Gaussian process model for 1/f noise proposed [BJTA82], but without accurate temporal and spectral analysis
- Hardware implementations shown randomness quality gains from 1/f noise [BCF+24]
- Short-memory numerical approximations proposed for TRNG simulation [PV24]
- **Gap:** No tractable analytical model capturing long-range dependencies in coloured noise for security analysis

Novel Contributions

1. **Realistic Noise Model**: Fractional Brownian Motion for phase noise

$$\phi_t^H = \frac{1}{\Gamma(H+1/2)} \int_0^t (t-u)^{H-1/2} dB_u$$

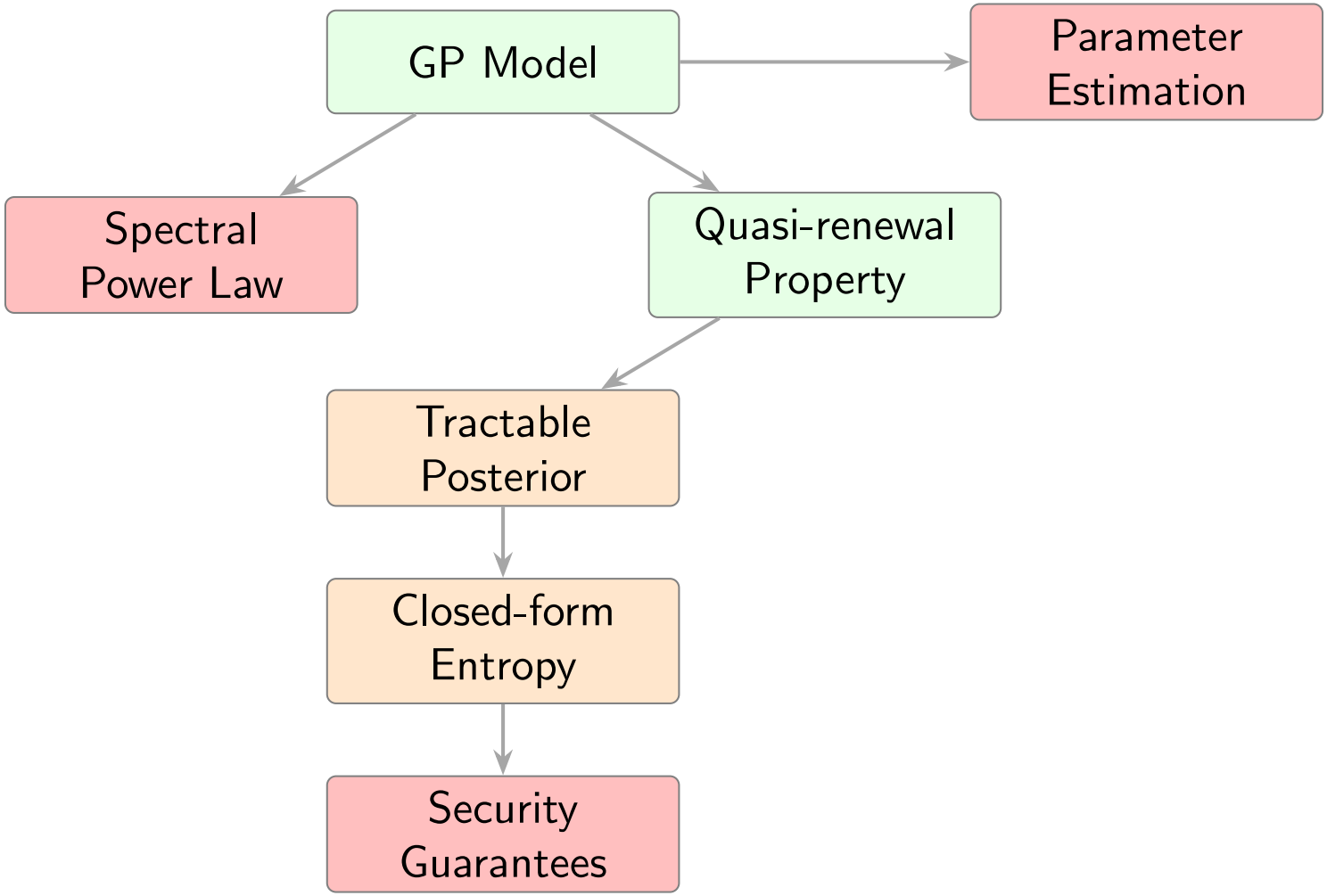
   with spectrum $\propto \omega^{-2H-1}$
2. **Quantified Leakage Resilience**: Conditional variance scales as τ^{2H}
3. **Closed-Form Entropy Analysis**: Exact entropy of Gaussian posteriors
4. **Parameter Estimation**: Allan variance-based coefficient recovery

Key Achievement

First tractable analytical model bridging power-law spectra ω^{-2H-1} (white to flicker noise) with cryptographic security requirements

Preprint available: [Sko24]

Theoretical Framework



Fractional Brownian Motion Properties

Using basics of Ito calcuus one obtains:

Covariance (Closed Form)

$$\mathrm{Cov}(\phi_s^H, \phi_t^H) = \frac{t^{H-\frac{1}{2}} s^{H+\frac{1}{2}}\, {}_2F_1\left(1, \frac{1}{2} - H; H + \frac{3}{2}; \frac{s}{t}\right)}{\Gamma(H + \frac{1}{2})\Gamma(H + \frac{3}{2})}, \quad 0 < s < t$$

Variance

$$\mathrm{Var}[\phi_t^H] = \frac{t^{2H}}{2H\Gamma(H + \frac{1}{2})^2}, \quad 0 < t$$

Correlation (Time Ratio Dependent)

$$\mathrm{Cor}(\phi_t^H, \phi_s^H) = \frac{4H\, {}_2F_1\left(1, \frac{1}{2} - H; H + \frac{3}{2}; \frac{1}{r}\right)}{(2H+1)\sqrt{r}}$$

where $r = \max\{t, s\}/\min\{t, s\}$.

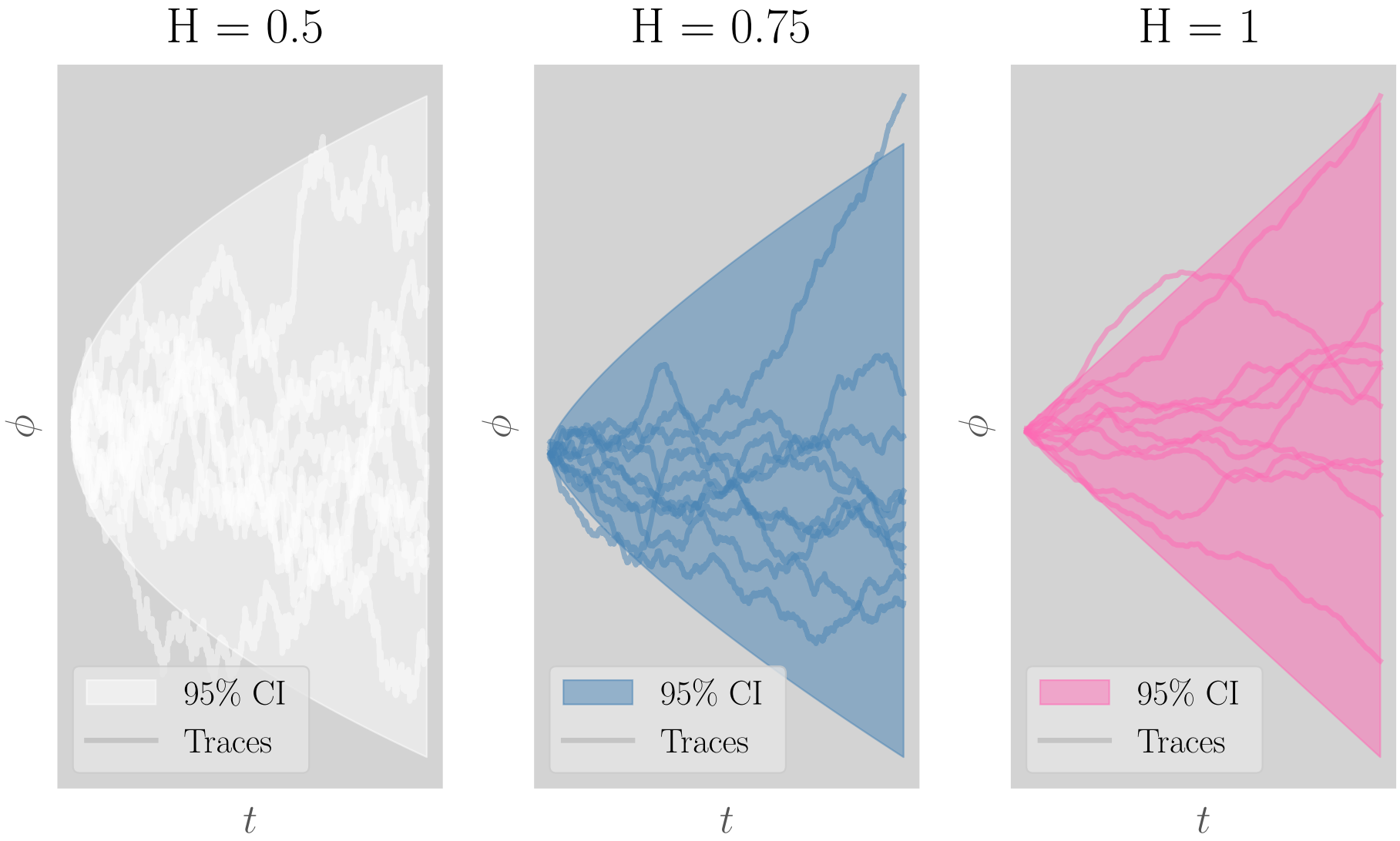


Figure: Sample paths for different Hurst parameters.

Spectral Analysis: Theory

Wigner-Ville Spectrum

Time-averaged spectrum exhibits power law:

$$\bar{S}_{\phi_H}(T,\omega) = \omega^{-2H-1}\left(1 + O_H((T\omega)^{H-3/2})\right)$$

White Noise ($H = 0.5$):

$$S_\phi(\omega) \propto \omega^{-2}, \quad S_{\dot{\phi}}(\omega) \propto \omega^0$$

Flicker Noise ($H = 1$):

$$S_\phi(\omega) \propto \omega^{-3}, \quad S_{\dot{\phi}}(\omega) \propto \omega^{-1}$$

where $\dot{\phi} = \frac{\Delta\phi}{\Delta t}$ is instantaneous frequency

Validation

FBM captures dominant TRNG noise sources with exact power laws

Spectral Analysis: Proof

For closed form:

- Express covariance in time-lag coordinates: $K(t_1, t_2) = K(t - \tau, t + \tau)$
- Observe that derivatives are rational functions
- Evaluate Fourier transform of derivatives, then integrate back

For asymptotics:

- Use properties of hypergeometric functions

Spectral Analysis: Empirical Validation

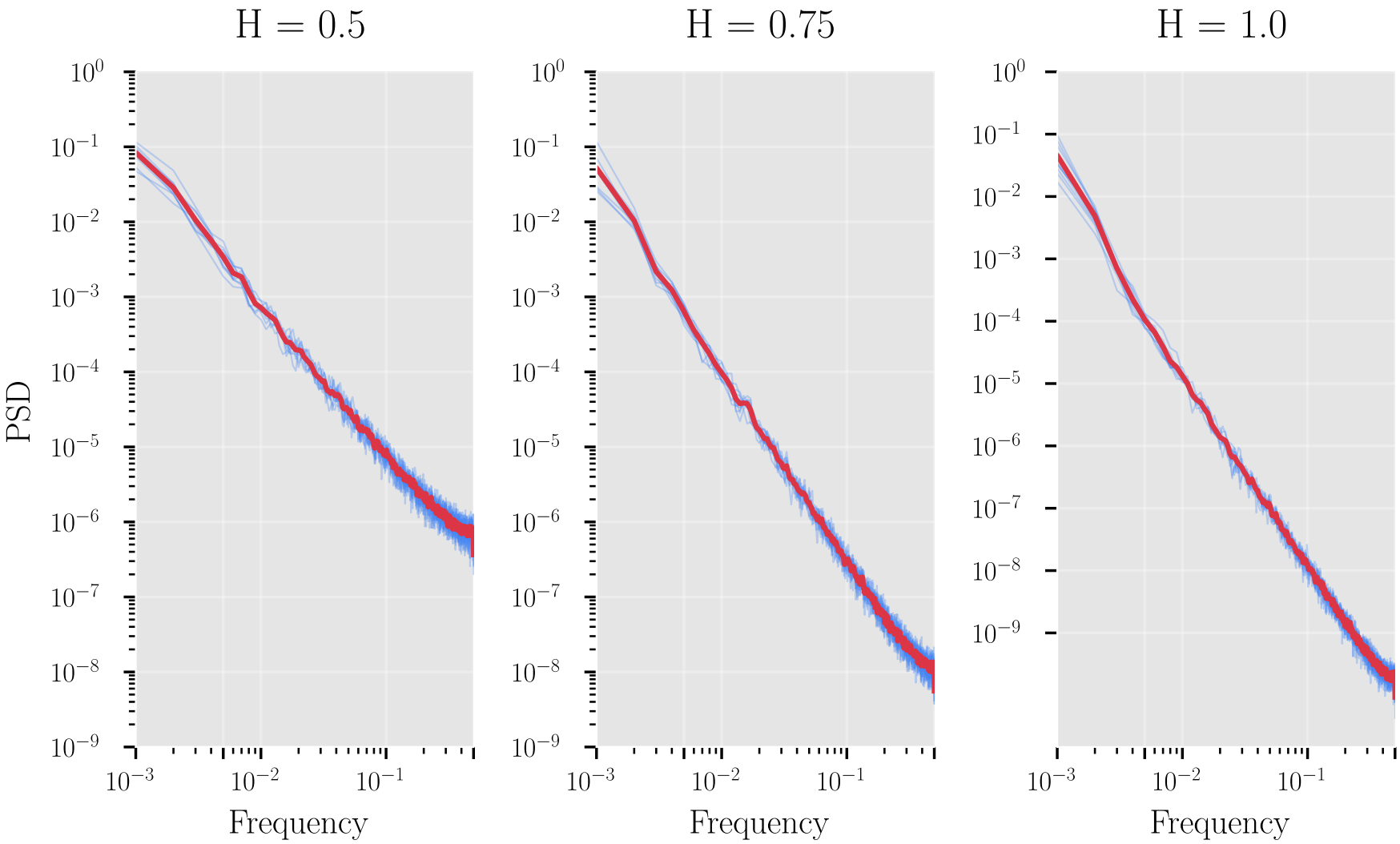


Figure: Power spectral density for various Hurst exponents.

Leakage Resilience

Quasi-Renewal Property

For $s < t$:

$$\mathrm{Var}(\phi_t^H \mid \phi_{\leq s}^H) = \mathrm{Var}(\phi_{t-s}^H) = \frac{(t-s)^{2H}}{2H\Gamma(H+\frac{1}{2})^2}$$

Security implications:

- Conditional variance depends only on time gap $\tau = t - s$
- Uncertainty grows as τ^{2H} (power-law recovery)
- Enables tractable analysis of information leakage
- Process "restarts" after conditioning on past observations

Key Insight

Complete observation history provides significantly more predictive power than pairwise correlations suggest—crucial for TRNG security analysis

Entropy Analysis

Folded / Wrapped Gaussian Distribution

For $Y = X \bmod r$ where $X \sim \mathcal{N}(\mu, \sigma^2)$:

$$p_Y(y) = r^{-1}\vartheta_3\left(\pi(\mu - y)/r, e^{-2\pi^2\sigma^2/r^2}\right)$$

Min-Entropy under Gaussian Posterior

$$\max_{\phi_0} \text{bias}(b_t \mid \Phi_{\leq s}, \phi_0) = \epsilon(\sigma(t|s), \alpha)$$

where

$$\epsilon(\sigma, \alpha) = \left| \frac{1}{\pi} \int_0^{\alpha\pi} \vartheta_3\left(y/2, e^{-\sigma^2/2}\right) dy - \frac{1}{2} \right|$$

Higher noise variance $\rightarrow$ Lower bias $\rightarrow$ Higher entropy

Parameter Estimation

Allan Variance Method

For twice-differenced FBM:

$$\mathrm{Var}(\Delta^2_{t,h}\phi^H_t) = h^{2H}\left(\frac{(4-4^H)\csc(H\pi)}{\Gamma(2H+1)} + O_H((h/t)^{4-2H})\right)$$

Special Cases

$$H = 1/2: \quad \mathrm{Var}(\Delta^2_{t,h}\phi^{1/2}_t) = 2h(1+O((h/t)^3))$$

$$H = 1: \quad \mathrm{Var}(\Delta^2_{t,h}\phi^1_t) = \frac{4\log 2}{\pi}h^2(1+O((h/t)^2))$$

- Nearly unbiased estimation
- Connects theoretical constants to hardware measurements
- Validated with FPGA data (1M samples on CycloneV and SmartFusion)

Sampling Bandwidth

Mixed Noise Model

For phase noise $\phi = \sum_{H \in \{1/2,1\}} c_H \phi_t^H$:

$$\sigma^2 = \sum_{H \in \{1/2,1\}} c_H^2 \frac{(\Delta t)^{2H}}{2H\Gamma(H + \frac{1}{2})^2}$$

Min-Entropy Rate

$$\mathbf{H}_\infty(b_n \mid b_{\leq n-1}, \phi_0) = \epsilon(\sigma, \alpha)$$

Design Implication

Sampling interval Δt directly determines security through noise variance trade-off

Summary & Impact

Achieved

- **Tractable framework** with closed-form expressions
- **Physical realism** via power-law spectral densities
- **Security guarantees** through leakage resilience analysis
- **Calibration** via parameter estimation

Significance

- Bridges physical modelling with cryptographic requirements
- Eliminates simulation-based approach limitations
- Enables rigorous TRNG security evaluation

Future Work

GPU-accelerated sampling for analysing post-processing.

Acknowledgements

I am grateful to:

- **Viktor Fischer** for inspiring the research
- **Nathalie Bochard** for support with hardware experiments
- **Florent Bernard** for valuable discussions on modelling
- **Licinius Benea** for valuable insights on flicker noise

Thank You

Questions?

References I

- Licinius Benea, Mikael Carmona, Viktor Fischer, Florian Pebay-Peyroula, and Romain Wacquez, *Impact of the Flicker Noise on the Ring Oscillator-based TRNGs*, IACR Transactions on Cryptographic Hardware and Embedded Systems **2024** (2024), no. 2, 870–889.
- JA Barnes, RH Jones, PV Tryon, and DW Allan, *Stochastic models for atomic clocks*, Annual Precise Time and Time Interval Systems and Applications Meeting, 1982, pp. 295–306.
- M.S. Keshner, *1/f noise*, Proceedings of the IEEE **70** (1982), no. 3, 212–218.
- D.B. Leeson, *A simple model of feedback oscillator noise spectrum*, Proceedings of the IEEE **54** (1966), no. 2, 329–330.
- Adriaan Peetermans and Ingrid Verbauwhede, *Trng entropy model in the presence of flicker fm noise*, IACR Transactions on Cryptographic Hardware and Embedded Systems **2024** (2024), no. 4, 285–306.

References II

Maciej Skorski, *Modelling 1/f Noise in TRNGs via Fractional Brownian Motion*, October 2024.