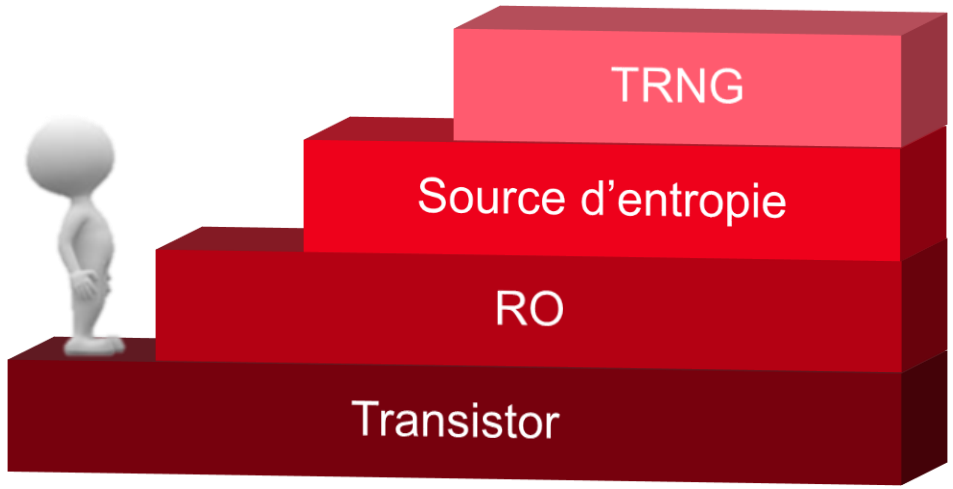
Effets des différents bruits sur la variance d'Allan du jitter dans des RO: Expérimentation et émulation

Licinius Benea, Florian Pebay-Peyroula, Romain Wacquez, Mikael Carmona

Sommaire

Introduction

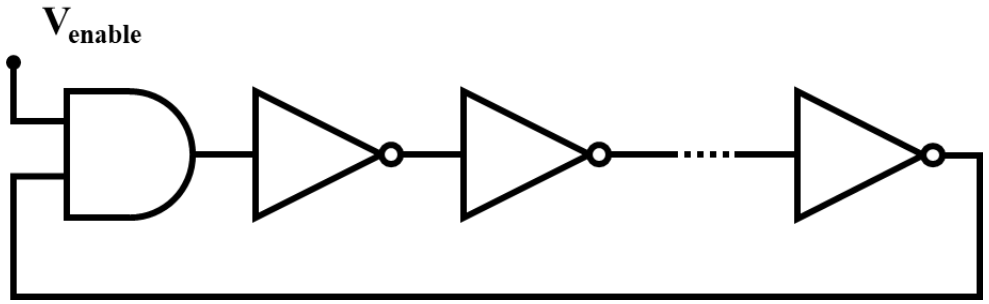
- Générateurs d'aléa (TRNG – True Random Number Generators):
  - Cryptographie
  - Simulations
  - Jeux
- Notre choix : oscillateurs en anneau (Ring Oscillator - RO)
  - Maîtrise des modèles
  - Petite surface
- Modèle stochastique basé sur les phénomènes physiques est requis pour les normes actuelles (AIS-31)
- Notre approche:
  - Top down – intégration des tous les niveaux: depuis transistor jusqu'au TRNG complet

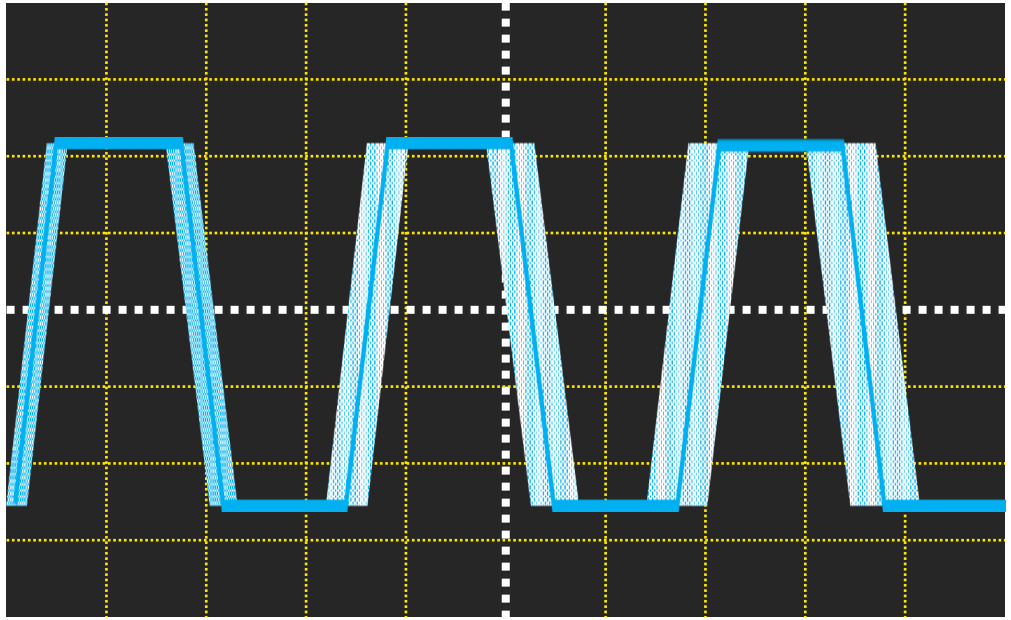


2. Sources de bruit dans les ROs

Oscillateur en anneau

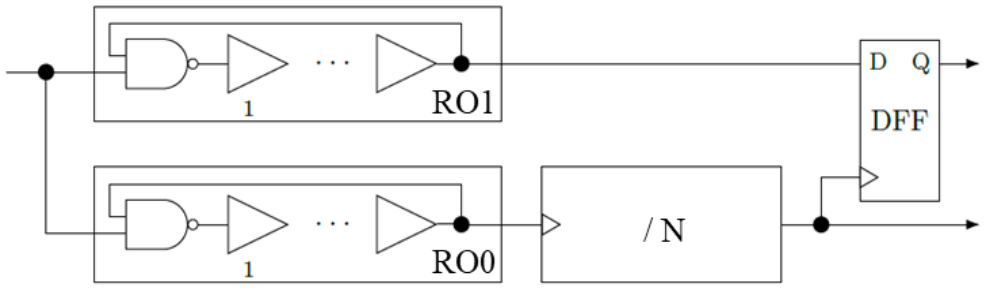
- RO – suite d'un nombre impairs des portes inverseurs
- Le signal périodique est imparfait :
  - Gigue (jitter) :
    - Aléatoires:
      - Phénomènes physiques:
        - Bruit thermique
        - Bruit flicker
      - Mesure/échantillonnage :
        - Bruit de quantification
    - Déterministe
    - Parasite (ex. cross-talk)
- Le jitter augmente avec le temps d'accumulation





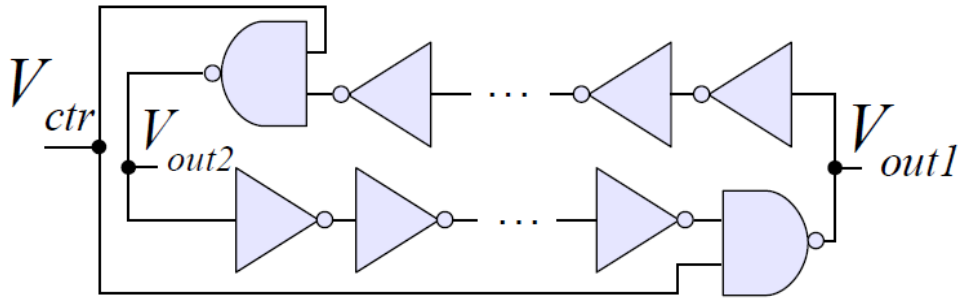
Types de RO-TRNG

1. Elementary RO-TRNG



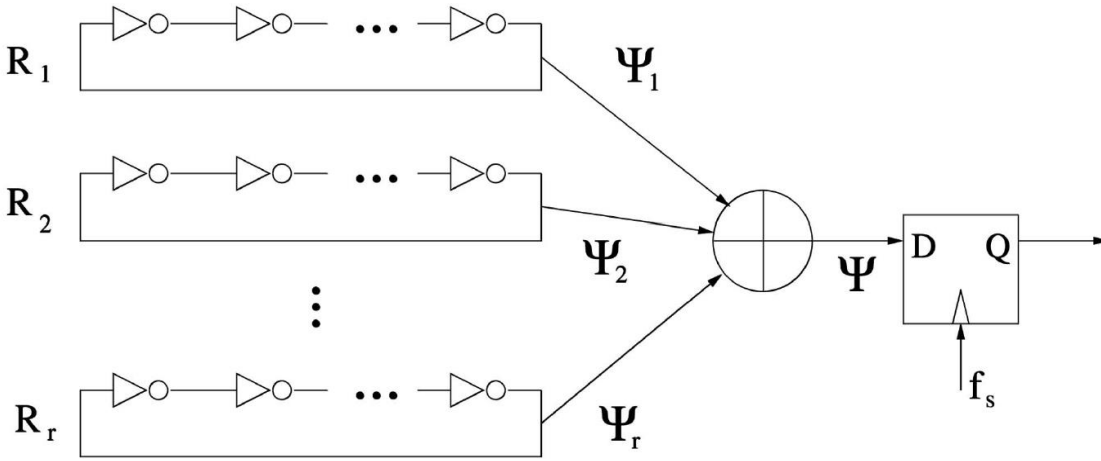
[Baudet 2011]

2. Transient Effect RO-TRNG

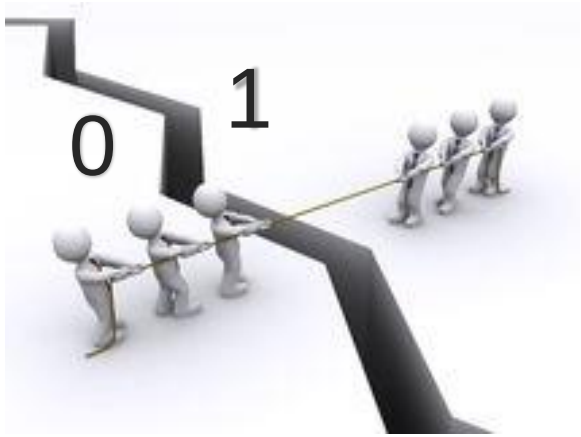


[Haddad 2015]

3. Multi-RO-TRNG



[Sunar 2007]

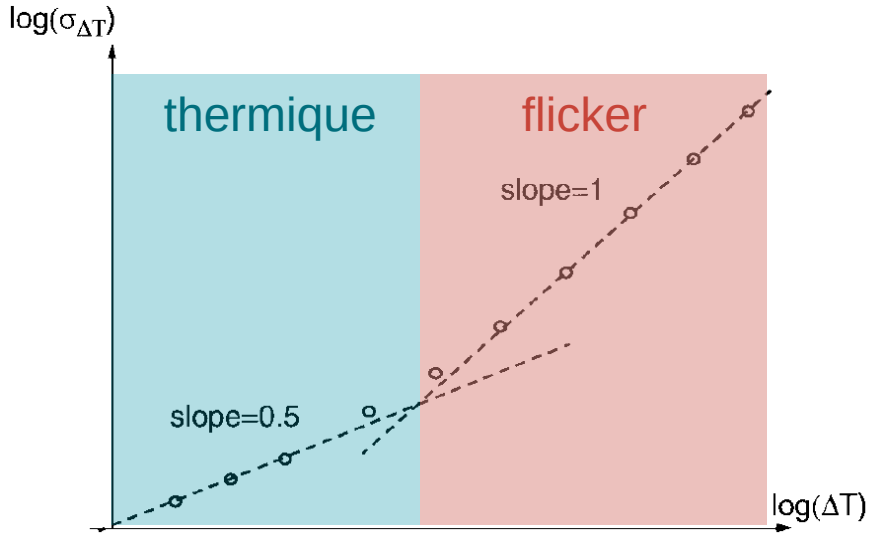


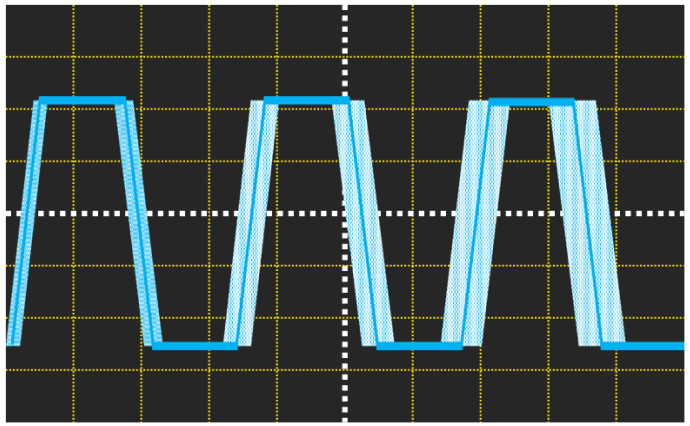
Sources physiques de jitter

- Plusieurs modèles de bruit de phase des ROs existant dans la littérature : tous originaires du modèle de [Hajimiri 1999]

- On quantifie le jitter par la variance (pour les résultats présentés)

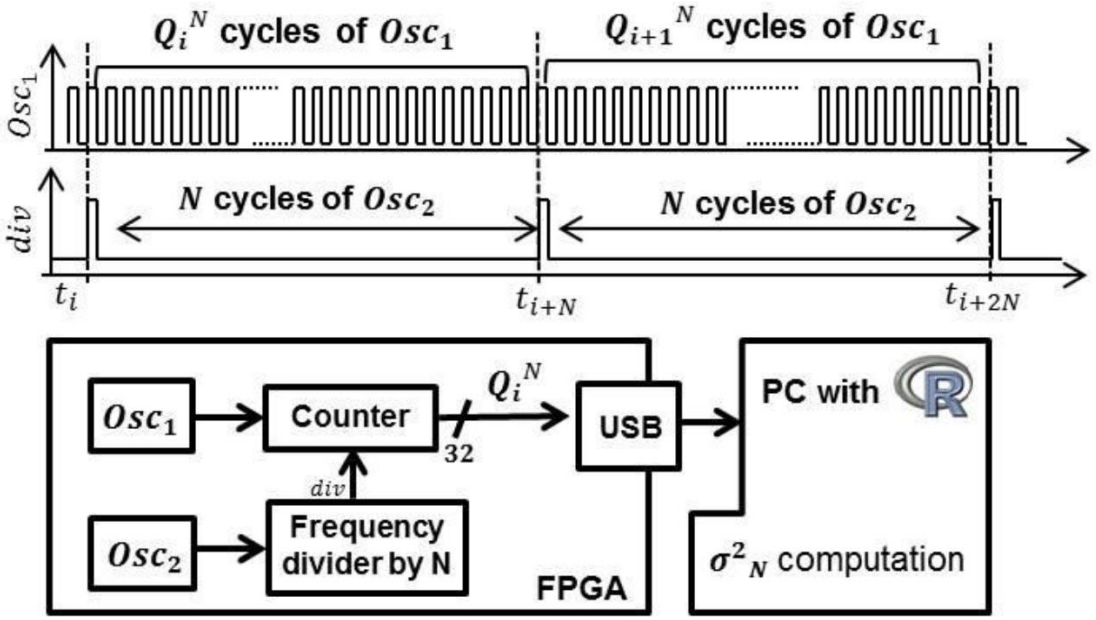
- Les deux sources physiques sont:
  - Bruit thermique (aléatoire)
    - la variance accumulée est la somme des variances des transitions précédentes
  - Bruit flicker (corrélé)
    - l'écart-type accumulée est la somme des écarts-types précédents

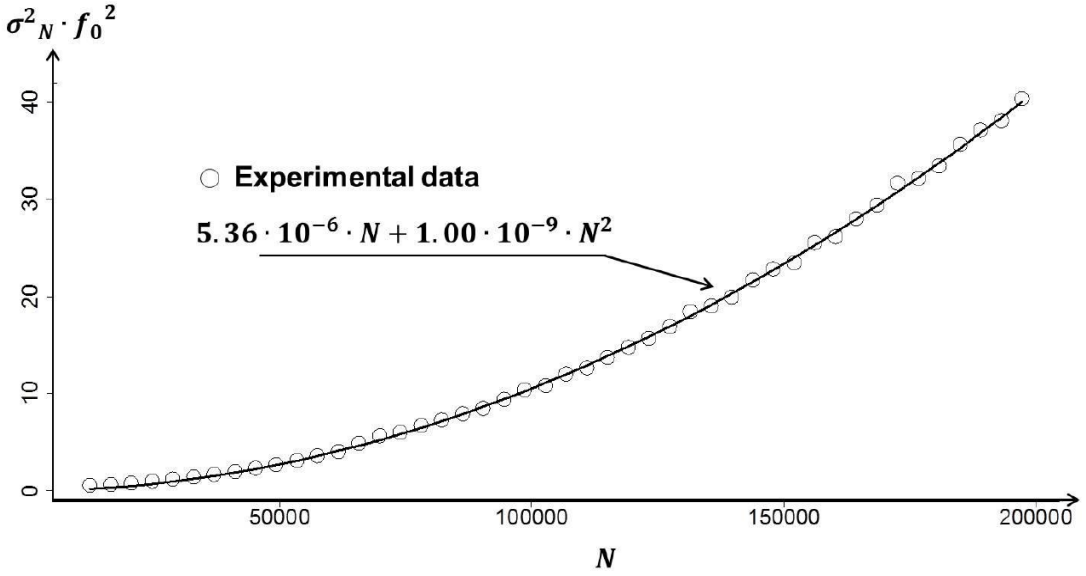




Mesure de jitter pour RO-TRNG

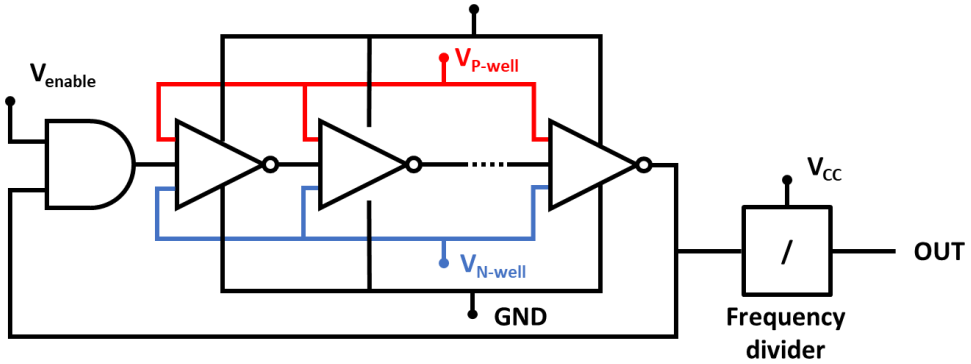
- On utilise la variance d'Allan [Haddad 2014]
- On compte le nombre d'oscillations du RO1 pendant l'accumulation de N cycles du RO2
- Un comportement parabolique : une composante linéaire (thermique) et une composante parabolique (flicker)

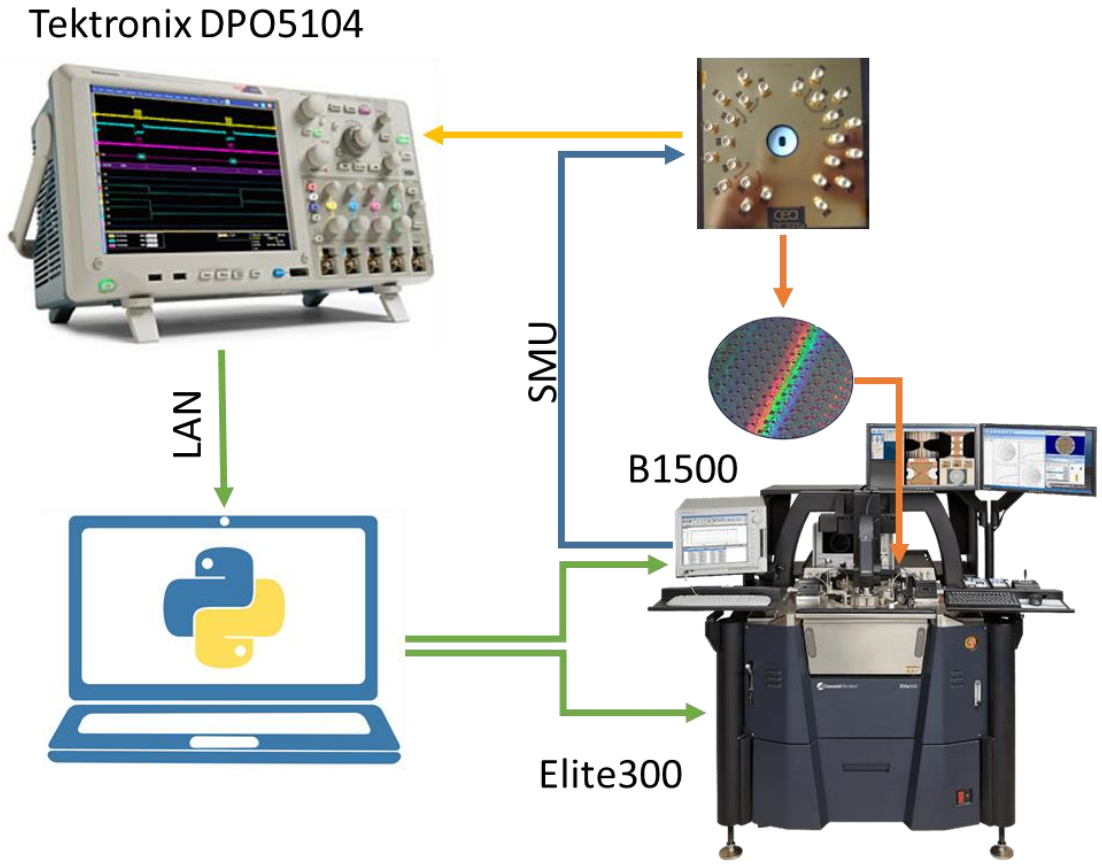




Montage expérimental pour la mesure de jitter

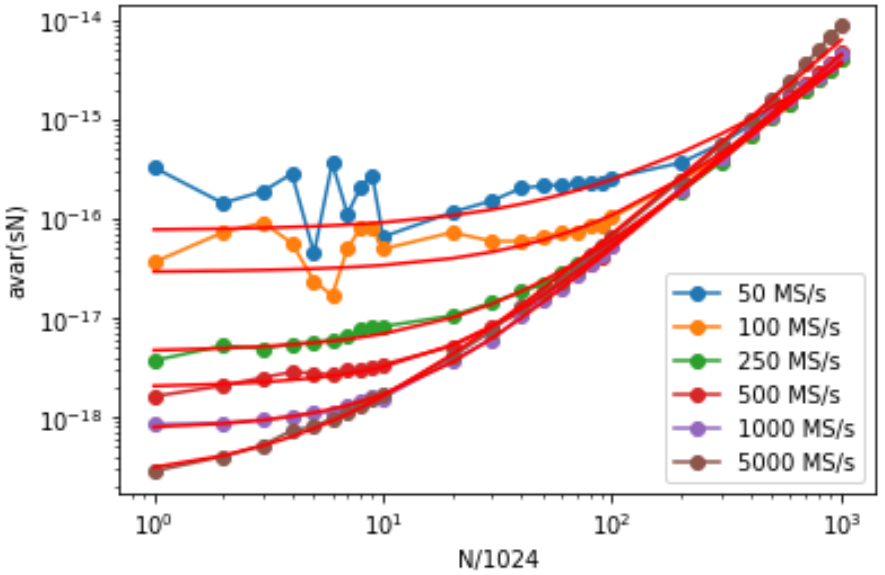
- Chaîne de mesure:
  - Banc Cascade Microtech Elite 300
  - Analyseur HP B1500
  - OscilloscopeTektronix DPO5104
- RO technologie 28nm (300mm) ~500 MHz
  - étages inverseurs : 101
  - Diviseur de fréquence : 1024
    - Jitter ~ 2ps, éch. oscillo. : 12,5 ps max

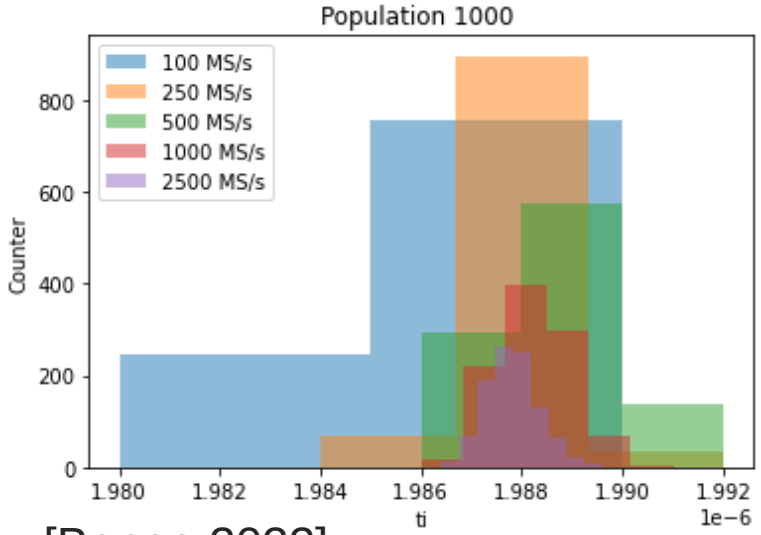




Echantillonnage

- L'échantillonnage joue un rôle important dans la caractérisation du jitter
- Les courbes commencent par un plateau qui provient du bruit de quantification
- Le plateau varie en fonction de la fréquence d'échantillonnage
- Le jitter est surestimé si l'échantillonnage est mauvais : conséquences sur la caractérisation des sources de bruit





[Benea 2022]

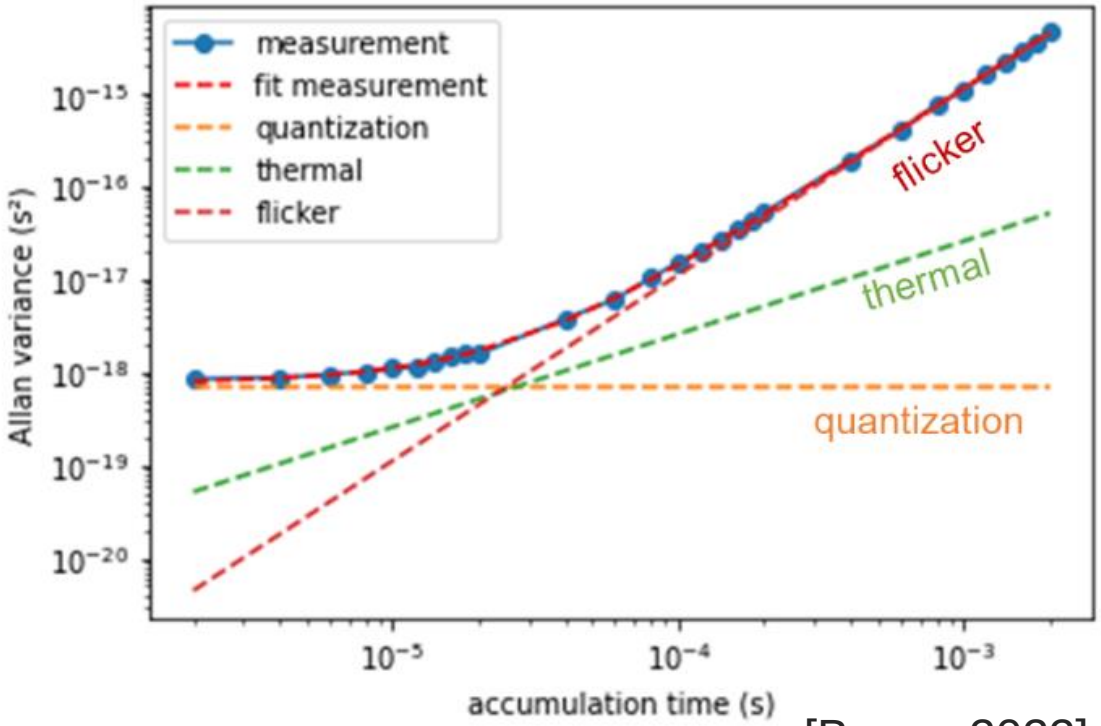
Conséquence 1 : bruit de quantification

- Sources de bruit:
  - Quantification (échantillonnage)
  - Thermique (parfaitement aléatoire)
  - Flicker (autocorrélé - prédictibilité)

- Introduction d'un terme correspondant au bruit de quantification (plateau observé aussi dans [Allini2018]):

$$\sigma_N^2 = a_0 + a_1 \cdot N + a_2 \cdot N^2$$

- Utilisation d'une méthode de régression normalisée (Least-Squares Normalized Error Regression Algorithm) [Grantham 2006]

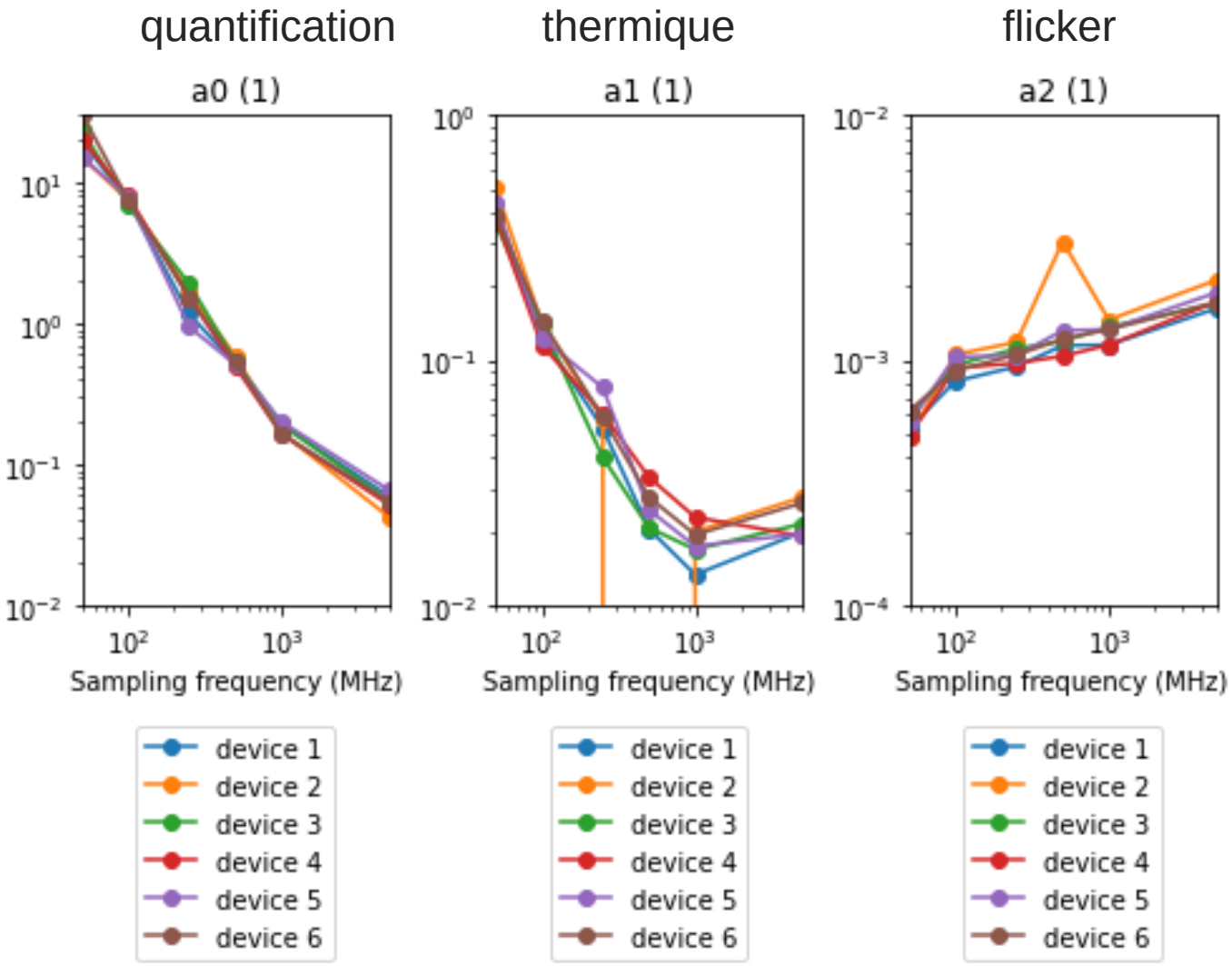


[Benea 2022]

Conséquence 2 : surestimation du bruit thermique

$$\sigma_N^2 = a_0 + a_1 \cdot N + a_2 \cdot N^2$$

- a_0 diminue avec la fréquence d'échantillonnage
- a_1 diminue avec la fréquence d'échantillonnage jusqu'à ce que $F_{ech}=1000*F_0$
  - Surestimation du bruit thermique
- a_2 reste constant



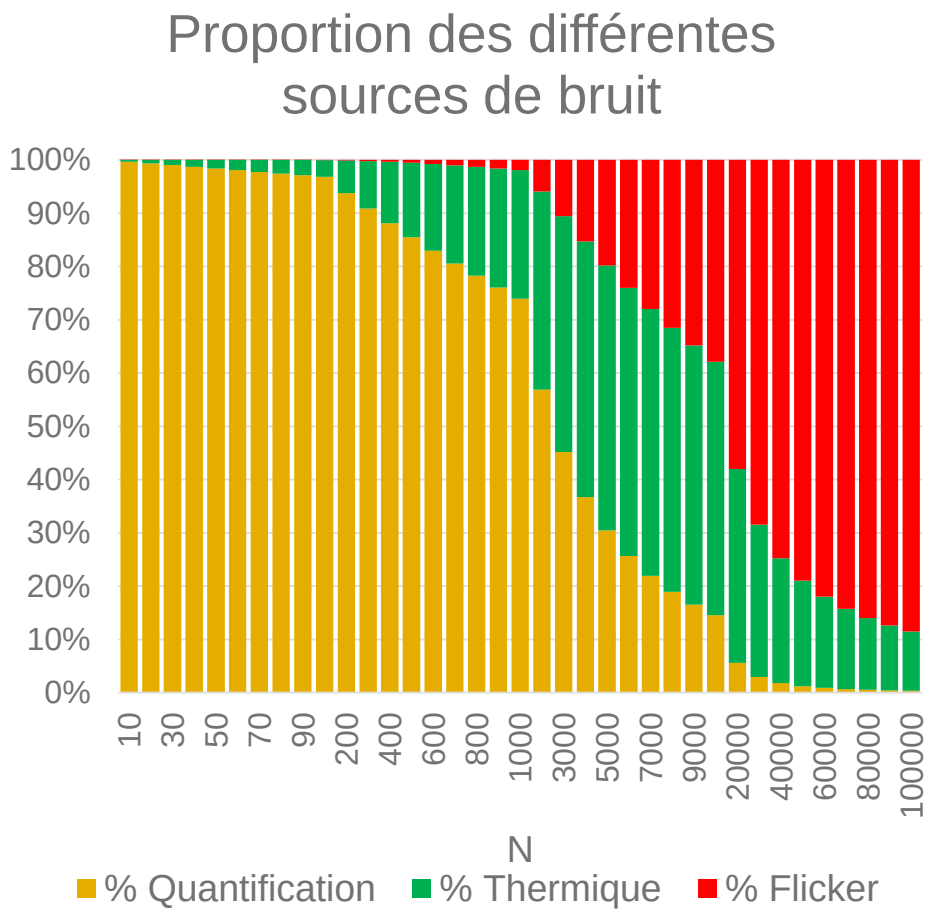
[Benea 2022]

Conséquence 3 : mix des sources de bruit

- Proportion des différentes sources de bruit à partir des coefficients des régressions paraboliques extraits à $F_{ech}/F_0 = 10000$

- Problématique:
  - Entropie calculée selon les modèles existant seulement à partir du bruit thermique (max. 50%)
  - Le point de fonctionnement du TRNG se trouve souvent dans un endroit qui est dominé par le bruit flicker

- Prochaine étape:
  - Emulateur (python) : ajuster les sources de bruit



3. Emulateur

Conclusion

Mesure:

- Caractérisation du jitter est une mesure complexe
  - utilisation des plusieurs outils (histogrammes/variance/spectres) pour identifier les sources physiques/effets indésirables
- Le jitter est toujours un mix de sources de bruit (dont le thermique ~ 50% maximum)
- Dans les dispositifs réels il y a d'autres sources de bruit (externes et internes)

Bibliographie

[Baudet 2011] M. Baudet, D. Lubicz, J. Micolod, and A. Tassiaux, ‘On the Security of Oscillator-Based Random Number Generators’, J Cryptol, vol. 24, no. 2, pp. 398–425, Apr. 2011, doi: 10.1007/s00145-010-9089-3.

[Benea 2022] L. Benea, M. Carmona, F. Pebay-Peyroula, and R. Wacquez, ‘On the Characterization of Jitter in Ring Oscillators using Allan variance for True Random Number Generator Applications’, in 2022 25th Euromicro Conference on Digital System Design (DSD), Maspalomas, Spain: IEEE, Aug. 2022, pp. 534–538. doi: 10.1109/DSD57027.2022.00077.

[Haddad 2014] P. Haddad, Y. Teglia, F. Bernard, and V. Fischer, ‘On the assumption of mutual independence of jitter realizations in P-TRNG stochastic models’, in Design, Automation & Test in Europe Conference & Exhibition (DATE), 2014, Dresden, Germany: IEEE Conference Publications, 2014, pp. 1–6. doi: 10.7873/DATE.2014.052.

[Haddad 2015] P. Haddad, V. Fischer, F. Bernard, and J. Nicolai, ‘A Physical Approach for Stochastic Modeling of TERO-Based TRNG’, in Cryptographic Hardware and Embedded Systems -- CHES 2015, T. Güneysu and H. Handschuh, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2015, pp. 357–372. doi: 10.1007/978-3-662-48324-4_18.

[Keshner 1982] M. S. Keshner, ‘1/f noise’, Proceedings of the IEEE, vol. 70, no. 3, pp. 212–218, 1982.

[Sunar 2007] B. Sunar, W. Martin, and D. Stinson, ‘A Provably Secure True Random Number Generator with Built-In Tolerance to Active Attacks’, IEEE Trans. Comput., vol. 56, no. 1, pp. 109–119, Jan. 2007, doi: 10.1109/TC.2007.250627.

[Timmer 1995] J. Timmer and M. Koenig, ‘On generating power law noise.’, Astronomy and Astrophysics, vol. 300, p. 707, 1995.

colorednoise F. Patzelt, Colorednoise. 2022. [Online]. Available: https://github.com/felixpatzelt/colorednoise