On the Way to Monitor Random Number Generation

Characterisation of noise sources

Haddad Patrick
Phd-1 Student
patrick.haddad@univ-st-etienne.fr
patrick.haddad@st.com

10th CryptArchi Workshop
Chateau de Goutelas
06/21/2012

Motivation

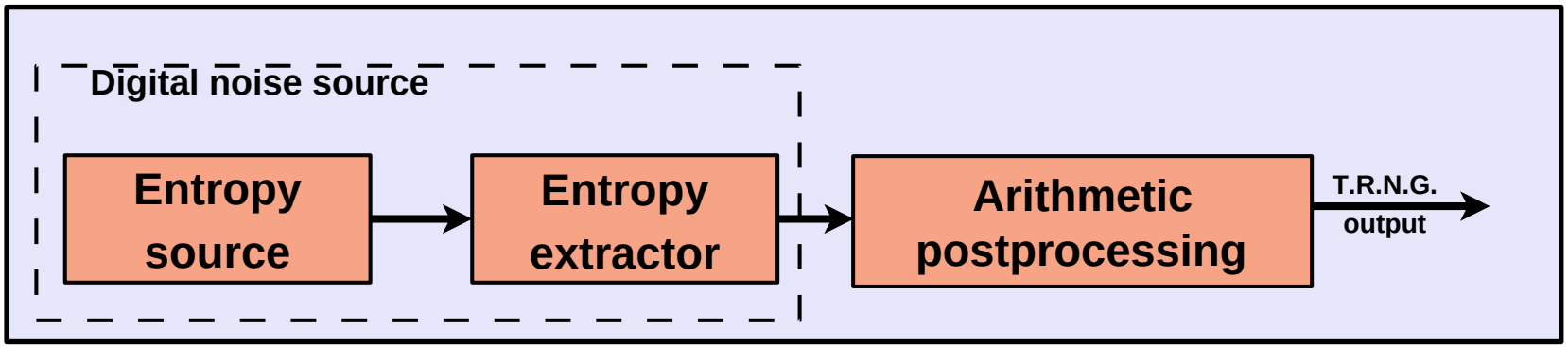
- Recent works[1] show the possibility to bias a T.R.N.G. output sequence.
  => Significant vulnerabilities in many cryptographic systems

- A T.R.N.G. has to conserve its statistical properties, and the unpredictability of the generated sequence, even during intentional or unintentional variations of the environment.

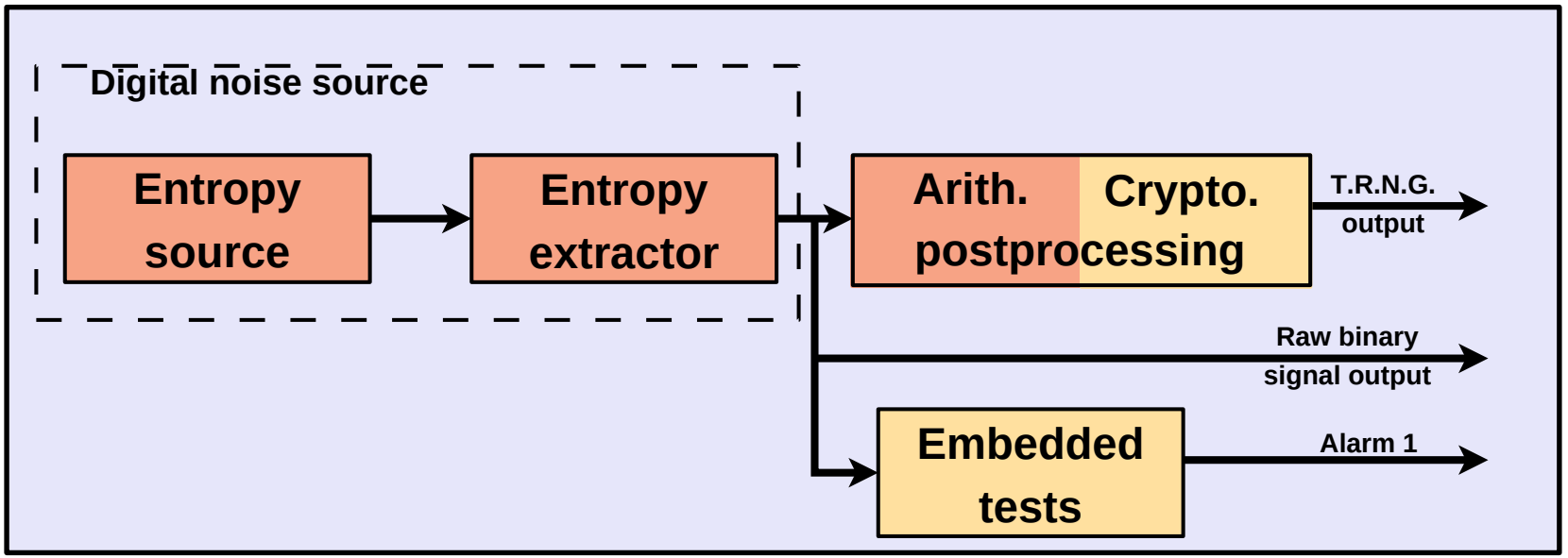
How to ensure the randomness of the sequence?

[1] Bayon et al.:Contactless Electromagnetic Active Attack on Ring Oscillator Based True Random Number Generator, COSADE 2012

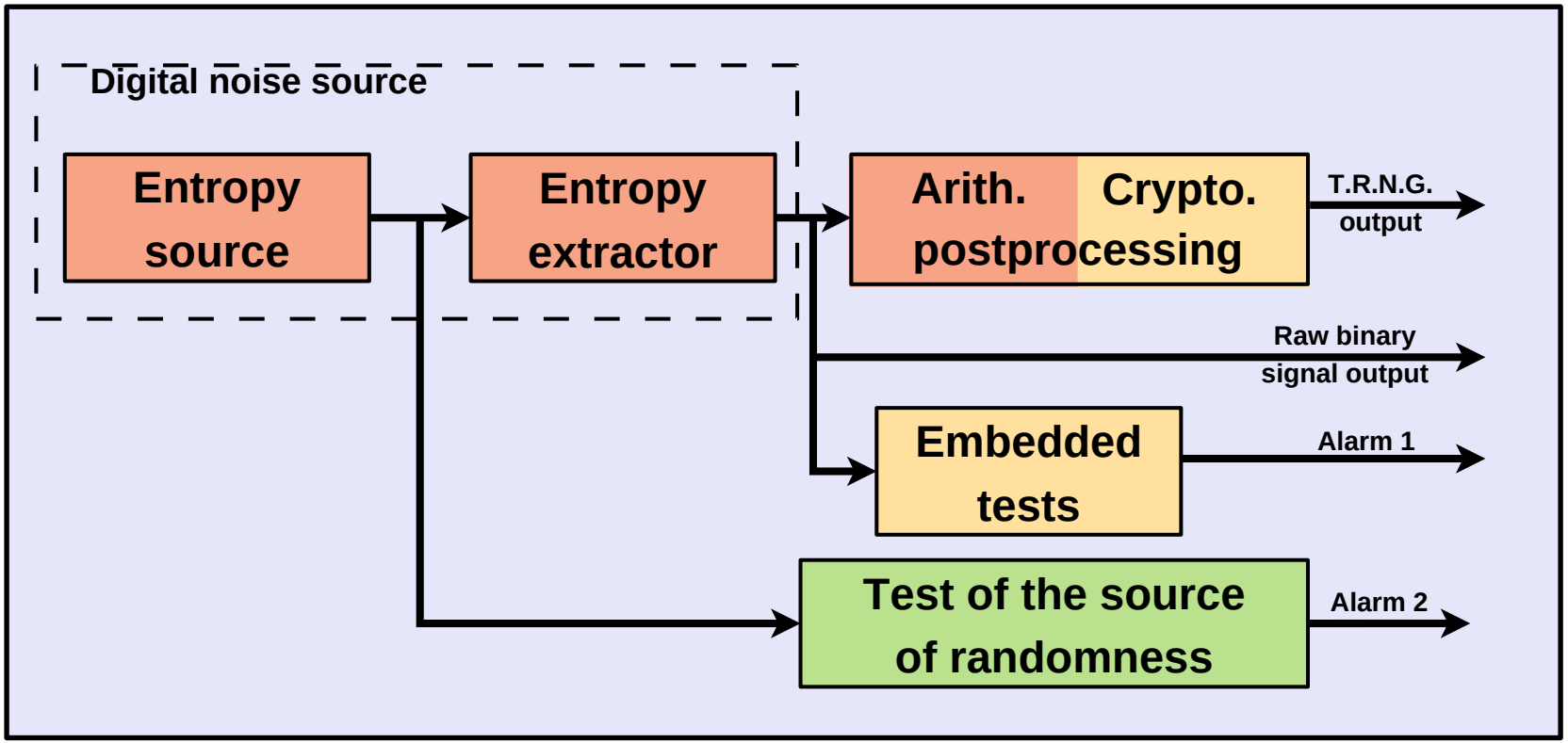
A classical design



The design recommended by BSI

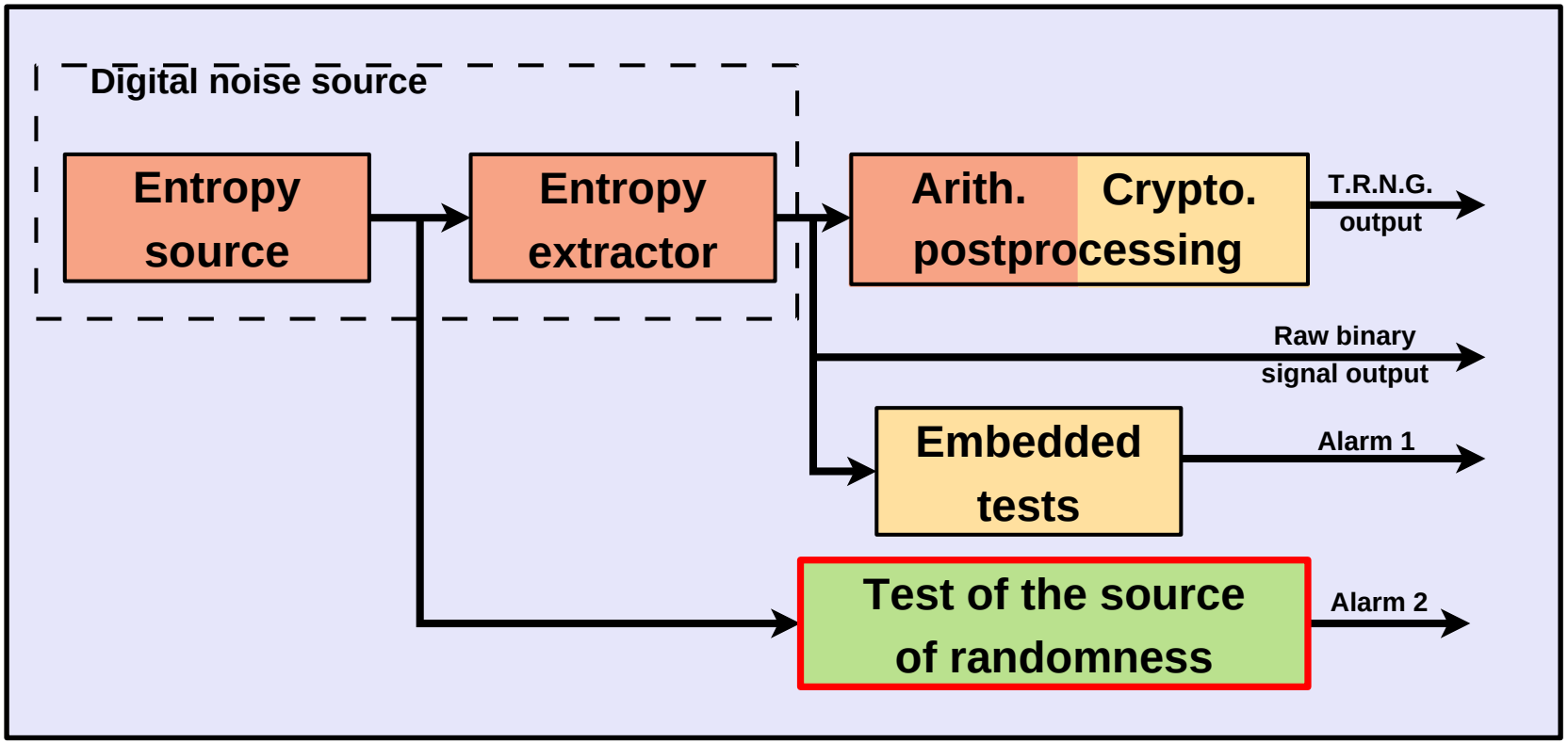


An extended security design



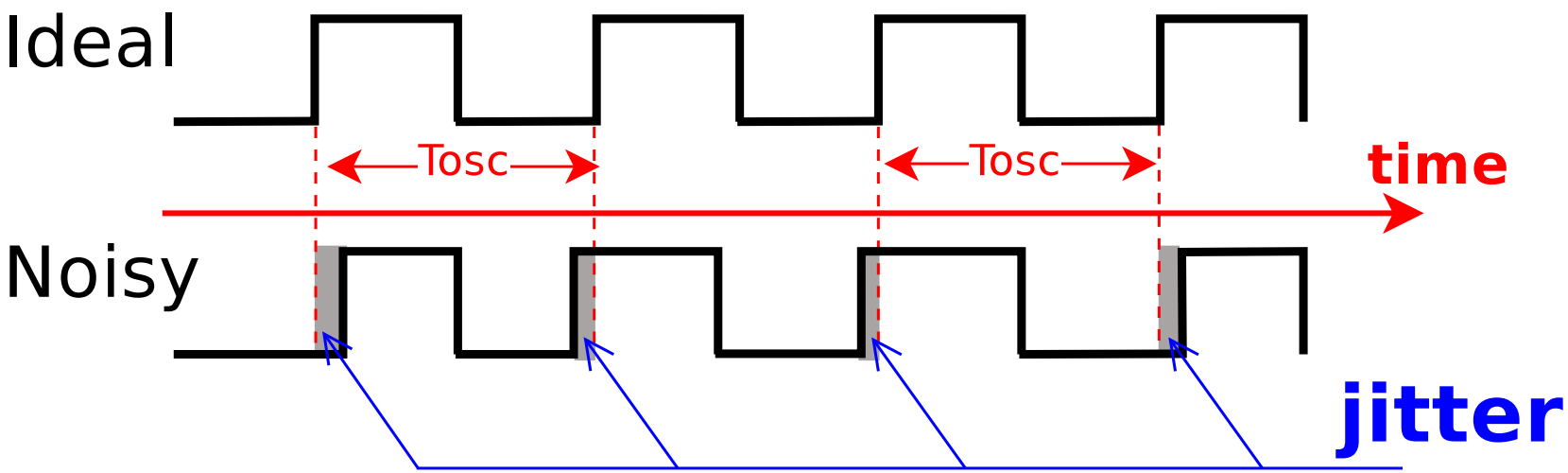
V. Fischer: A Closer Look at Security in Random Number Generators Design, COSADE 2012

An extended security design



V. Fischer: A Closer Look at Security in Random Number Generators Design, COSADE 2012

Noisy oscillators are often used as entropy source.



What is the expected behaviour of the jitter?

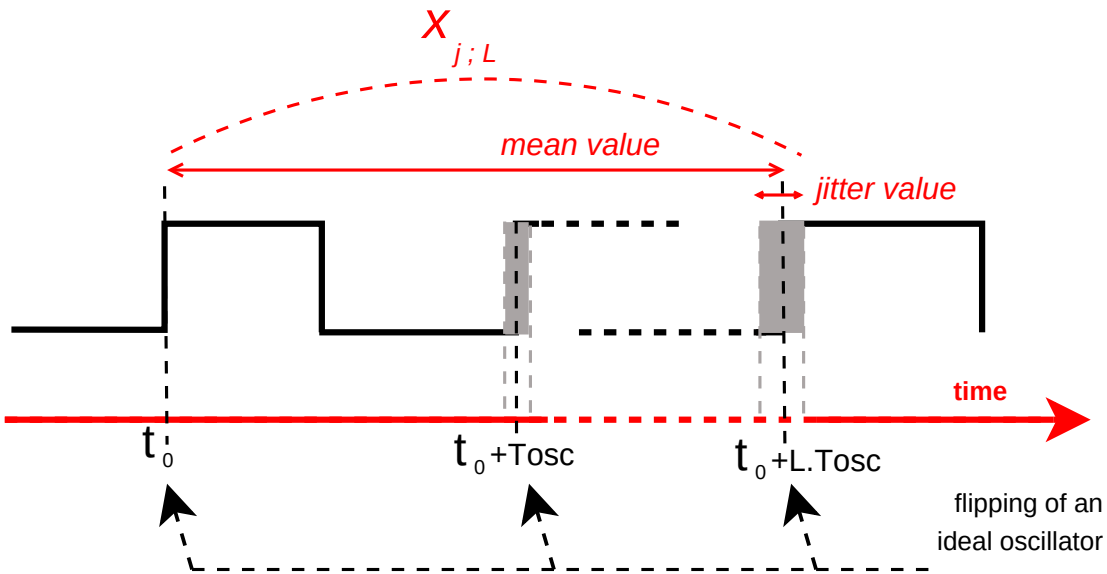
How to measure it?

1. Assuming that jitter is caused by thermal noises
   - Model of noisy oscillators
   - Measurement protocol
   - Results

2. Assuming that jitter is caused by a composition of differents noise types
   - Model of noisy oscillators
   - Measurement protocol
   - Results

The expected behaviour

Hypothesis:
Assuming the presence of only thermal noise in the circuit, Baudet et al.[4] modeled the evolution of the phase jitter by a Wiener stochastic process.



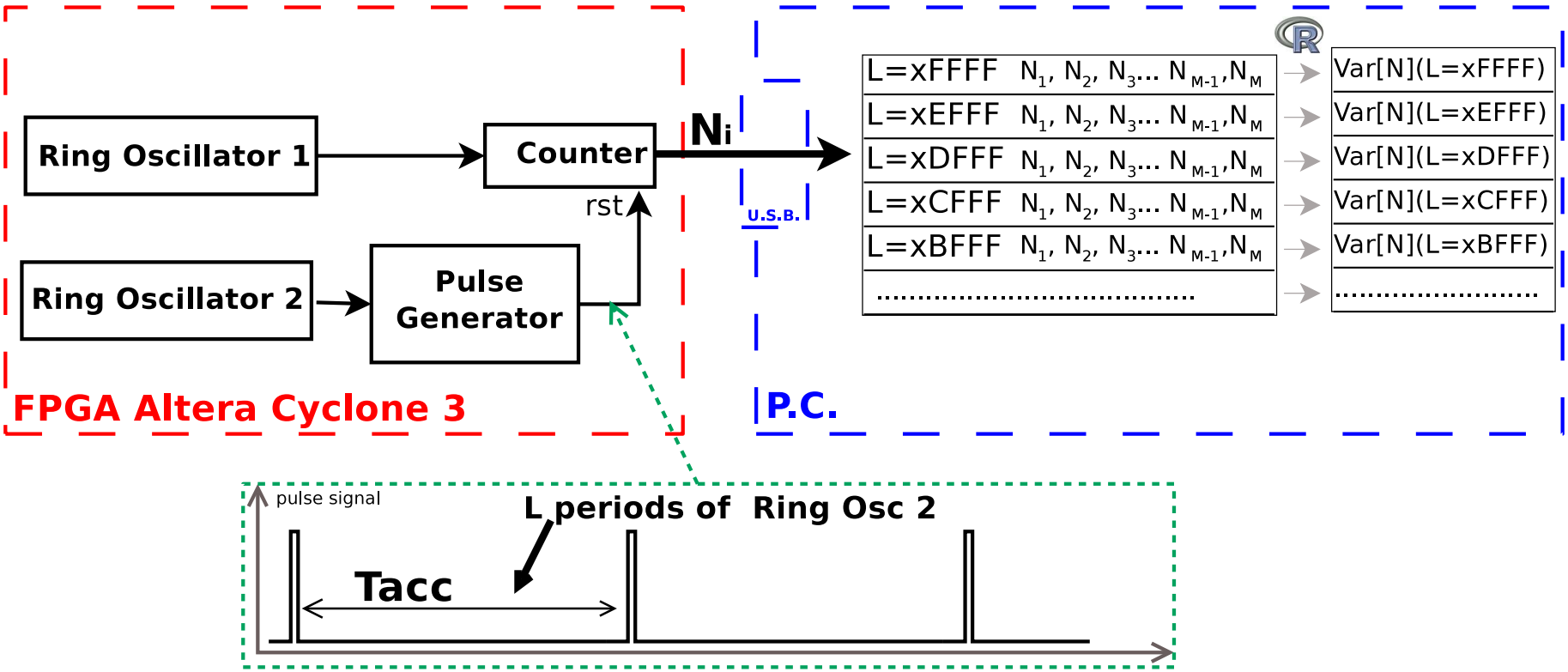
$x_{j;L}$ is the duration between L flipping of the oscillators

Consequence: The variance of X_L is expected to be proportional to L .

[4] Baudet et al.: On the Security of Oscillator-Based Random Number Generators, Journal of Cryptology 24, 2 (2011)

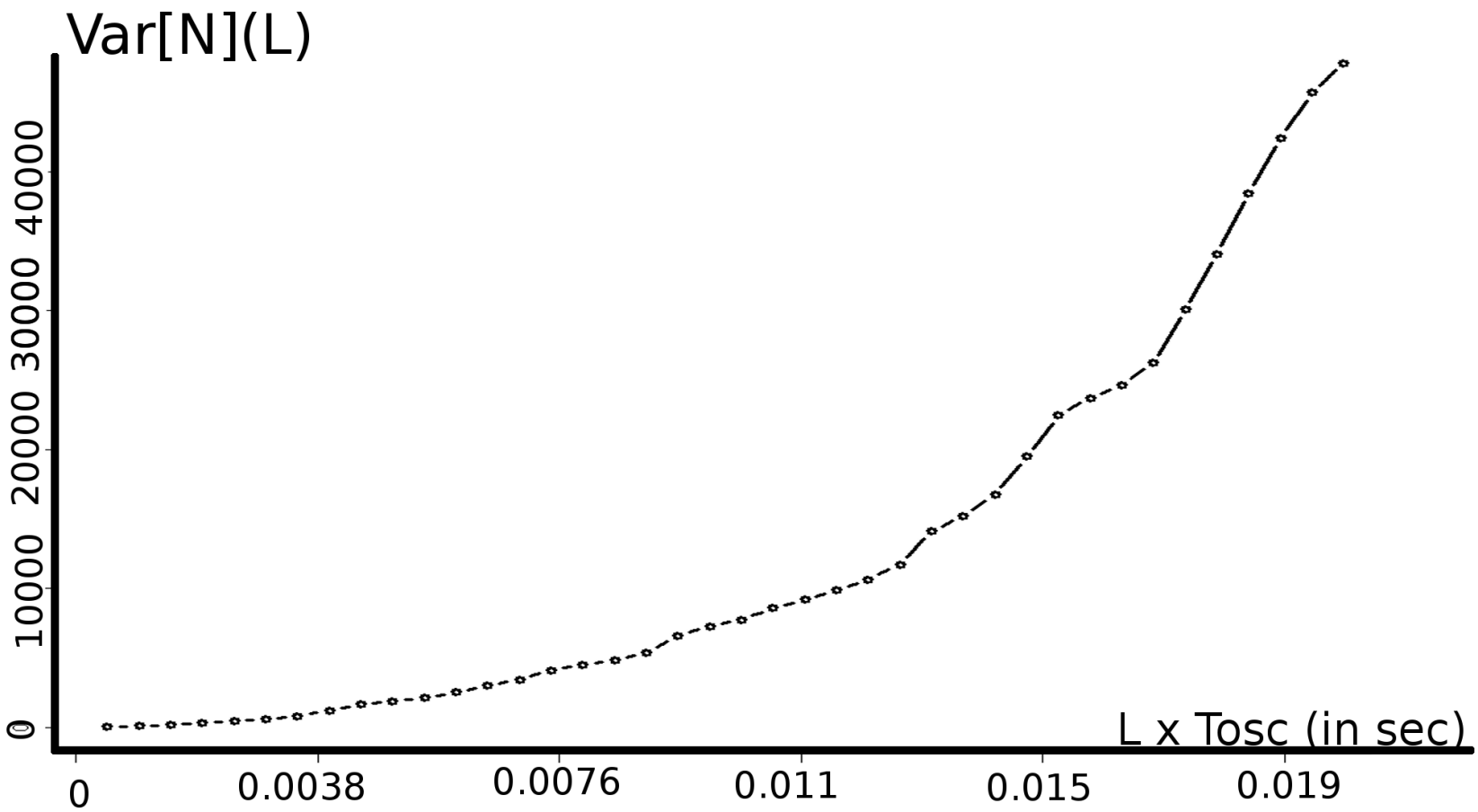
Measurement protocol

10 delay element ring oscillators implemented in Altera Cyclone 3



Then the variance of $[N]_{j=1..n}$ is expected to be proportional to L

Results



The variance of $[N]_{j=1..M}$ is not proportional to L

Summary

- **We assumed the presence of only thermal noise in the circuit**
  => The variance of X_L is expected to be proportional to L
- **In the Altera Cyclone 3 : is it not the case**
- **Thermal noise is not the only noise type present**

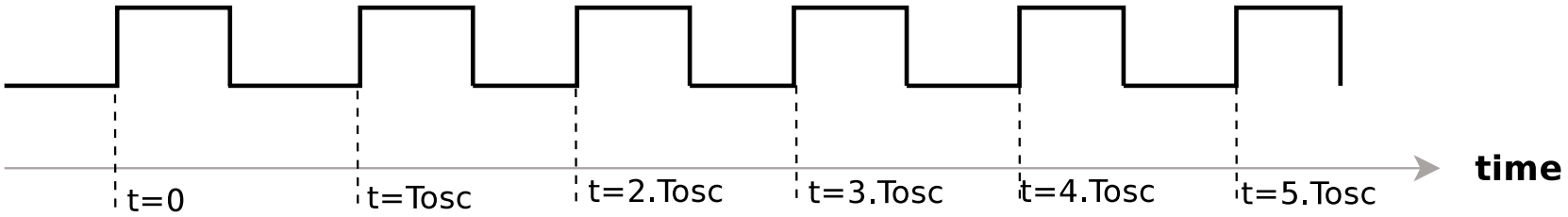
1. Assuming that jitter is caused by thermal noises
   - Model of noisy oscillators
   - Measurement protocol
   - Results

2. Assuming that jitter is caused by a composition of differents noise types
   - Model of noisy oscillators
   - Measurement protocol
   - Results

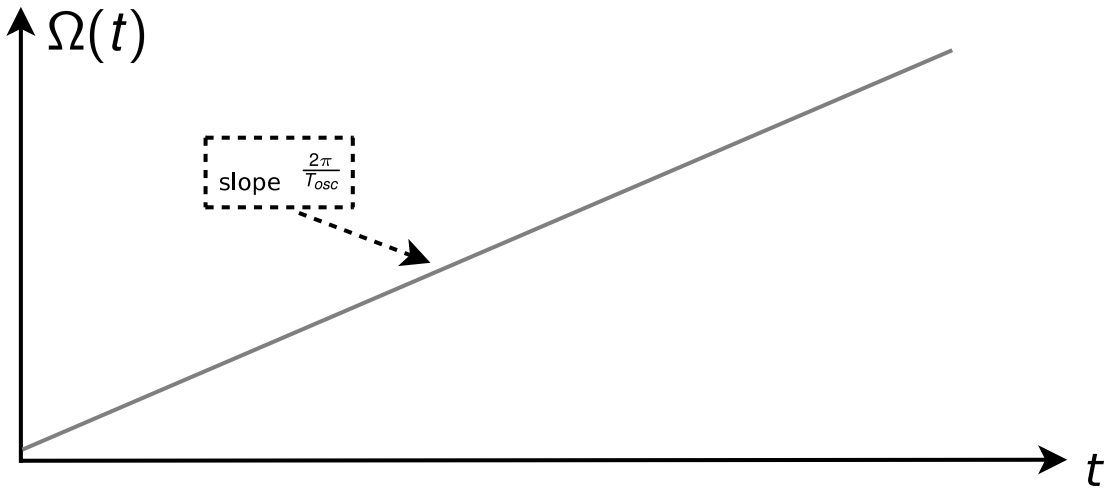
An ideal oscillator

$$V_{ideal}(t) = G\left(\frac{2\pi}{T_{osc}} \cdot t\right)$$

where G is a 2π periodic function

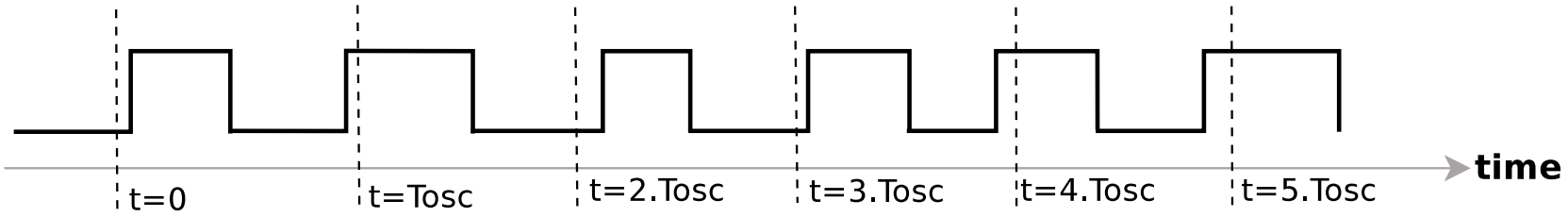


The total phase : $\Omega(t) = \frac{2\pi}{T_{osc}} \cdot t$

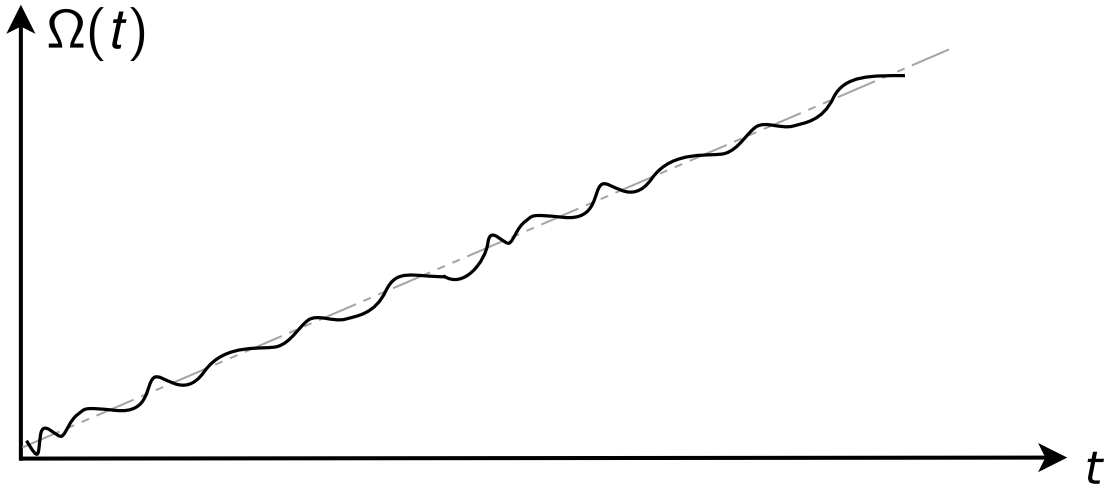


A noisy oscillator

$$V_{noisy}(t) = G\left(\frac{2\pi}{T_{osc}} \cdot t + \phi(t)\right)$$

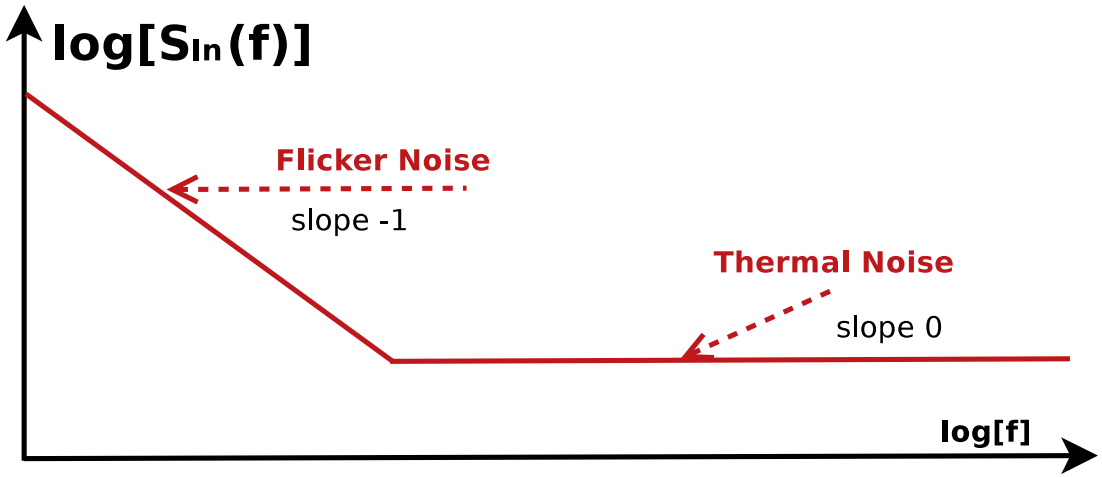


The total phase : $\Omega(t) = \frac{2\pi}{T_{osc}} \cdot t + \phi(t)$



Noise currents are described in the frequency domain using the P.S.D.[5]

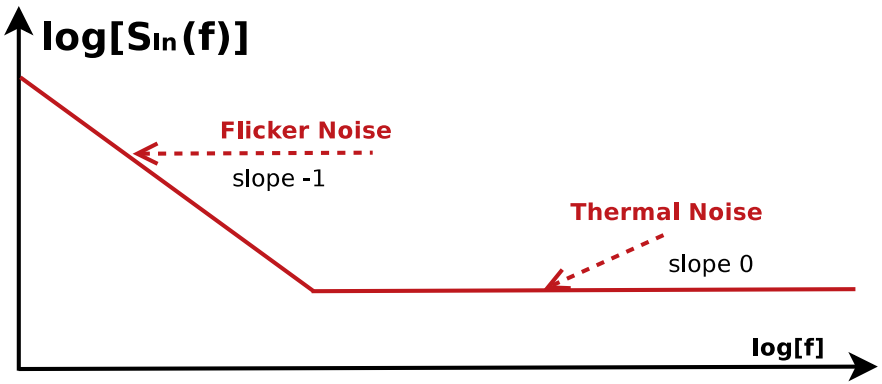
2 noise types are dominant in CMOS transistors



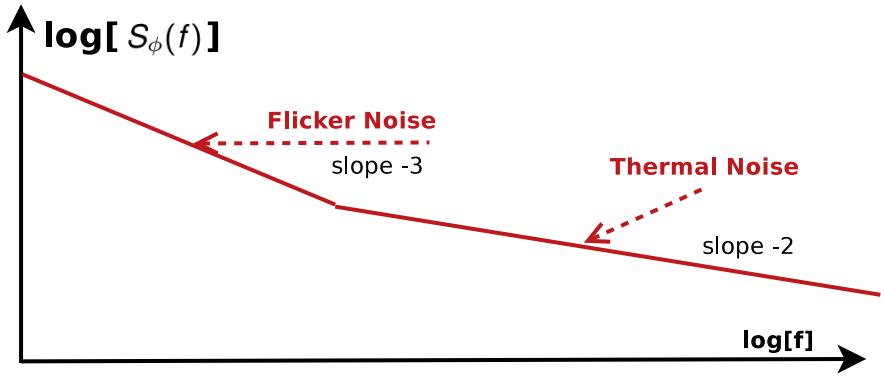
Noise currents P.S.D.

[5] Power Spectral Density

According to several analysis such as [6], noise currents P.S.D. are transformed in terms of $\phi(t)$ P.S.D. such as:



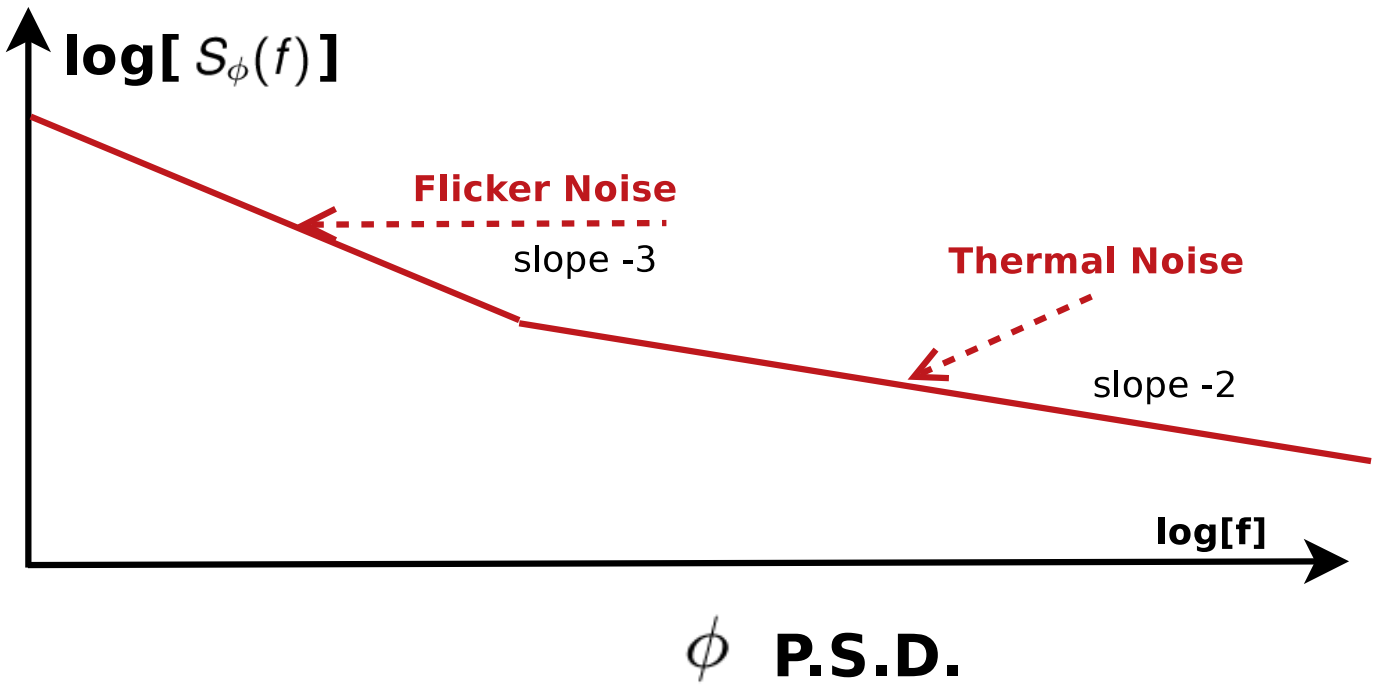
Noise currents P.S.D.



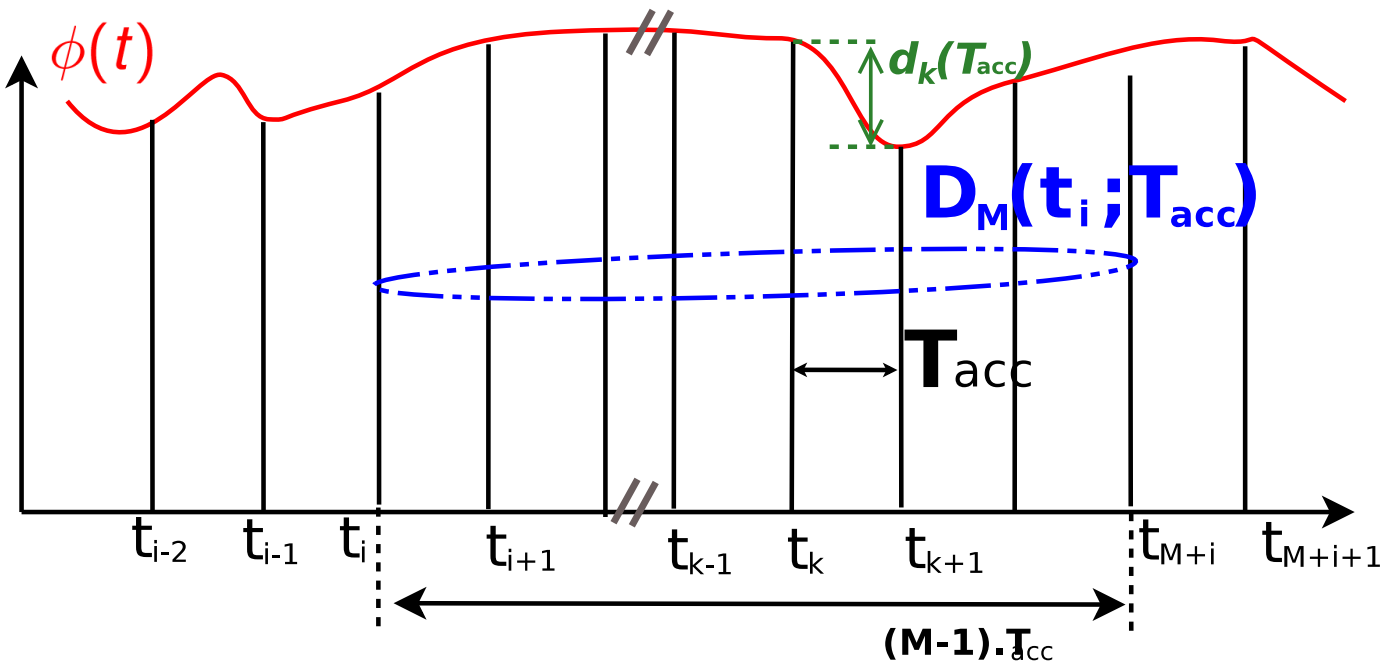
ϕ P.S.D.

[6] Hajimiri et al.: A general theory of phase noise in electrical oscillators, IEEE Journal of Solid State Circuits (1998).

The expected behaviour



Measurement protocol

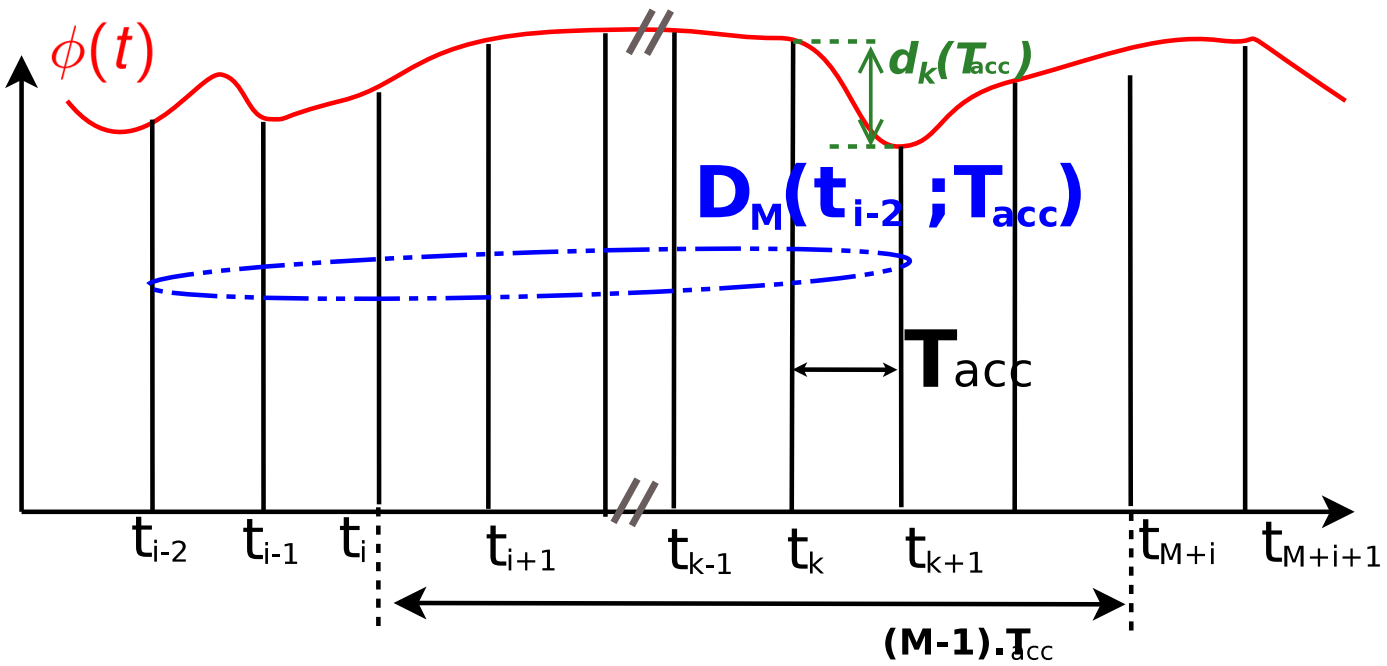


1. Let us define $d_k(T_{acc})$ as : $d_k(T_{acc}) = \phi(t_{k+1}) - \phi(t_k)$
2. Let $D_M(t_i; T_{acc})$ be the variance estimator of samples $\{d_i(T_{acc}), \ldots, d_{i+M-1}(T_{acc})\}$
3. Let $\langle D_M(t_i; T_{acc})\rangle$ be the infinite time average of $D_M(t_i; T_{acc})$. According to [7]:

$$\langle D_M(t_i; T_{acc})\rangle = \frac{4}{M-1} \int_0^{\infty} \frac{M^2 sin^2(\pi f T_{acc}) - sin^2(\pi f M T_{acc})}{M} \cdot S_\phi(f) \cdot df$$

[7] Barnes et al.: Characterization of Frequency Stability, IEEE Transactions on Instrumentation and Measurement (May 1971)

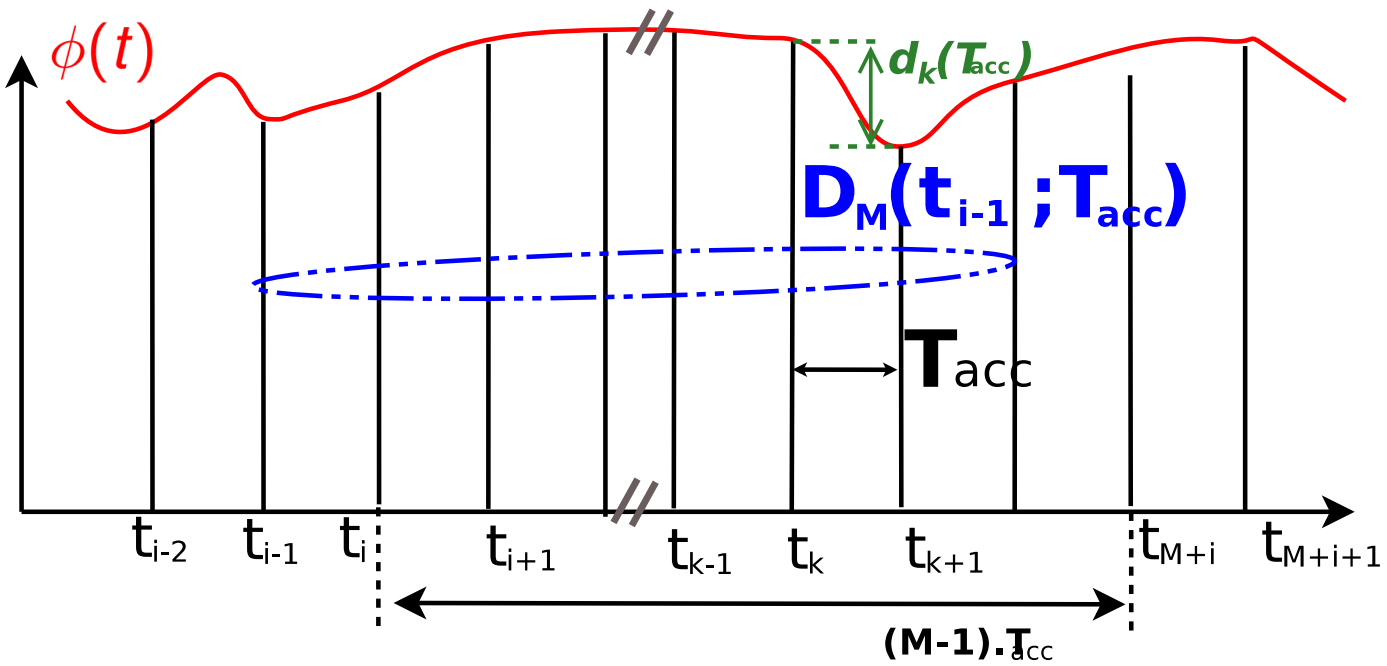
Measurement protocol



1. Let us define $d_k(T_{acc})$ as : $d_k(T_{acc}) = \phi(t_{k+1}) - \phi(t_k)$
2. Let $D_M(t_i; T_{acc})$ be the variance estimator of samples $\{d_i(T_{acc}), \ldots, d_{i+M-1}(T_{acc})\}$
3. Let $\langle D_M(t_i; T_{acc})\rangle$ be the infinite time average of $D_M(t_i; T_{acc})$.

$$\langle D_M(t_i; T_{acc})\rangle = \frac{4}{M-1}\int_0^{\infty} \frac{M^2 sin^2(\pi f T_{acc}) - sin^2(\pi f M T_{acc})}{M} \cdot S_\phi(f) \cdot df$$

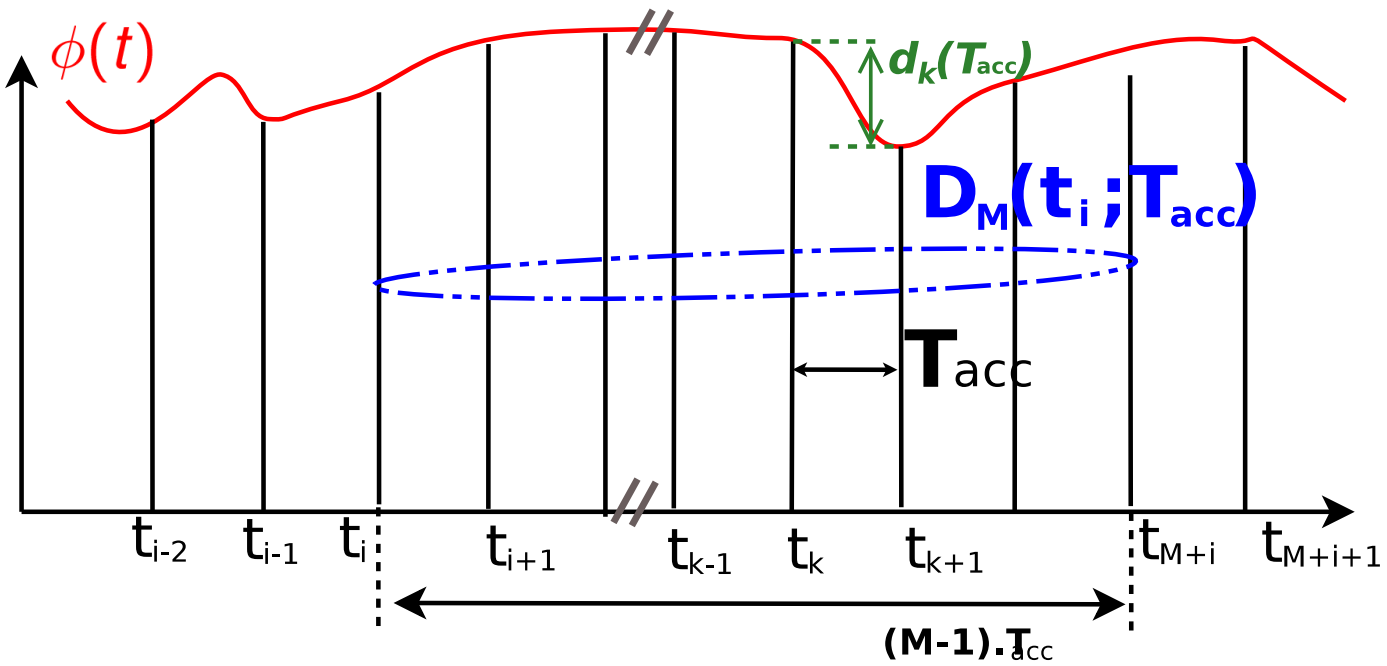
Measurement protocol



1. Let us define $d_k(T_{acc})$ as : $d_k(T_{acc}) = \phi(t_{k+1}) - \phi(t_k)$
2. Let $D_M(t_i; T_{acc})$ be the variance estimator of samples $\{d_i(T_{acc}), \ldots, d_{i+M-1}(T_{acc})\}$
3. Let $\langle D_M(t_i; T_{acc})\rangle$ be the infinite time average of $D_M(t_i; T_{acc})$.

$$\langle D_M(t_i; T_{acc})\rangle = \frac{4}{M-1}\int_0^{\infty} \frac{M^2 sin^2(\pi f T_{acc}) - sin^2(\pi f M T_{acc})}{M} \cdot S_\phi(f) \cdot df$$

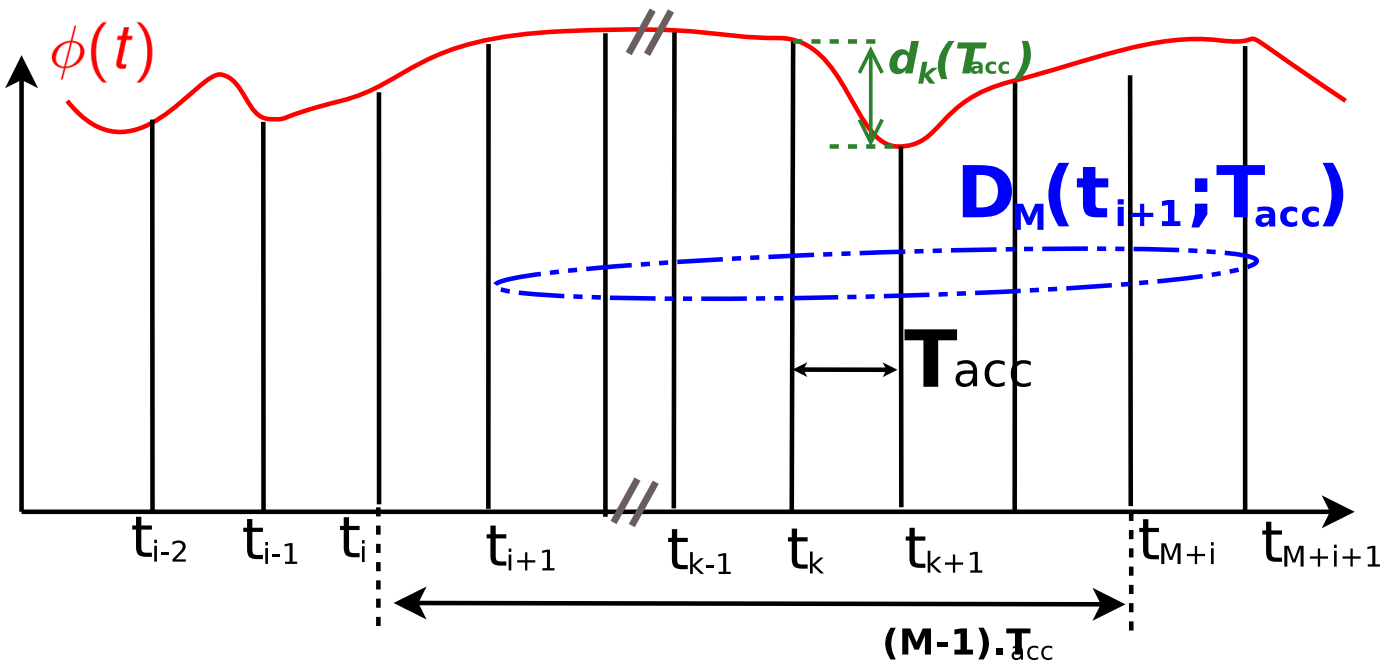
Measurement protocol



1. Let us define $d_k(T_{acc})$ as : $d_k(T_{acc}) = \phi(t_{k+1}) - \phi(t_k)$
2. Let $D_M(t_i; T_{acc})$ be the variance estimator of samples $\{d_i(T_{acc}), \ldots, d_{i+M-1}(T_{acc})\}$
3. Let $\langle D_M(t_i; T_{acc})\rangle$ be the infinite time average of $D_M(t_i; T_{acc})$.

$$\langle D_M(t_i; T_{acc})\rangle = \frac{4}{M-1}\int_0^{\infty} \frac{M^2 sin^2(\pi f T_{acc}) - sin^2(\pi f M T_{acc})}{M} \cdot S_\phi(f) \cdot df$$

Measurement protocol



1. Let us define $d_k(T_{acc})$ as : $d_k(T_{acc}) = \phi(t_{k+1}) - \phi(t_k)$
2. Let $D_M(t_i; T_{acc})$ be the variance estimator of samples $\{d_i(T_{acc}), \ldots, d_{i+M-1}(T_{acc})\}$
3. Let $\langle D_M(t_i; T_{acc})\rangle$ be the infinite time average of $D_M(t_i; T_{acc})$.

$$\langle D_M(t_i; T_{acc})\rangle = \frac{4}{M-1}\int_0^{\infty} \frac{M^2 sin^2(\pi f T_{acc}) - sin^2(\pi f M T_{acc})}{M} \cdot S_\phi(f) \cdot df$$

Measurement protocol

1. Thermal noise only : $S_\phi(f) = a_{-2} \cdot f^{-2}$,

$$\langle D_M(t_i; T_{acc}) \rangle = 2 \cdot a_{-2} \cdot \pi^2 \cdot T_{acc}$$

2. Flicker noise only : $S_\phi(f) = a_{-3} \cdot f^{-3}$,

$$\langle D_M(t_i; T_{acc}) \rangle = 4 \cdot a_{-3} \cdot \pi^2 \cdot \frac{M \cdot ln(M)}{M-1} \cdot T_{acc}^2$$

3. Assuming that S_ϕ can be written as: $S_\phi(f) = a_{-3} \cdot f^{-3} + a_{-2} \cdot f^{-2}$,

$$\langle D_M(t_i; T_{acc}) \rangle = 2 \cdot a_{-2} \cdot \pi^2 \cdot T_{acc} + 4 \cdot a_{-3} \cdot \pi^2 \cdot \frac{M \cdot ln(M)}{M-1} \cdot T_{acc}^2$$

Measurement protocol

The total phase difference beetween t_k and $t_k + T_{acc}$ is:

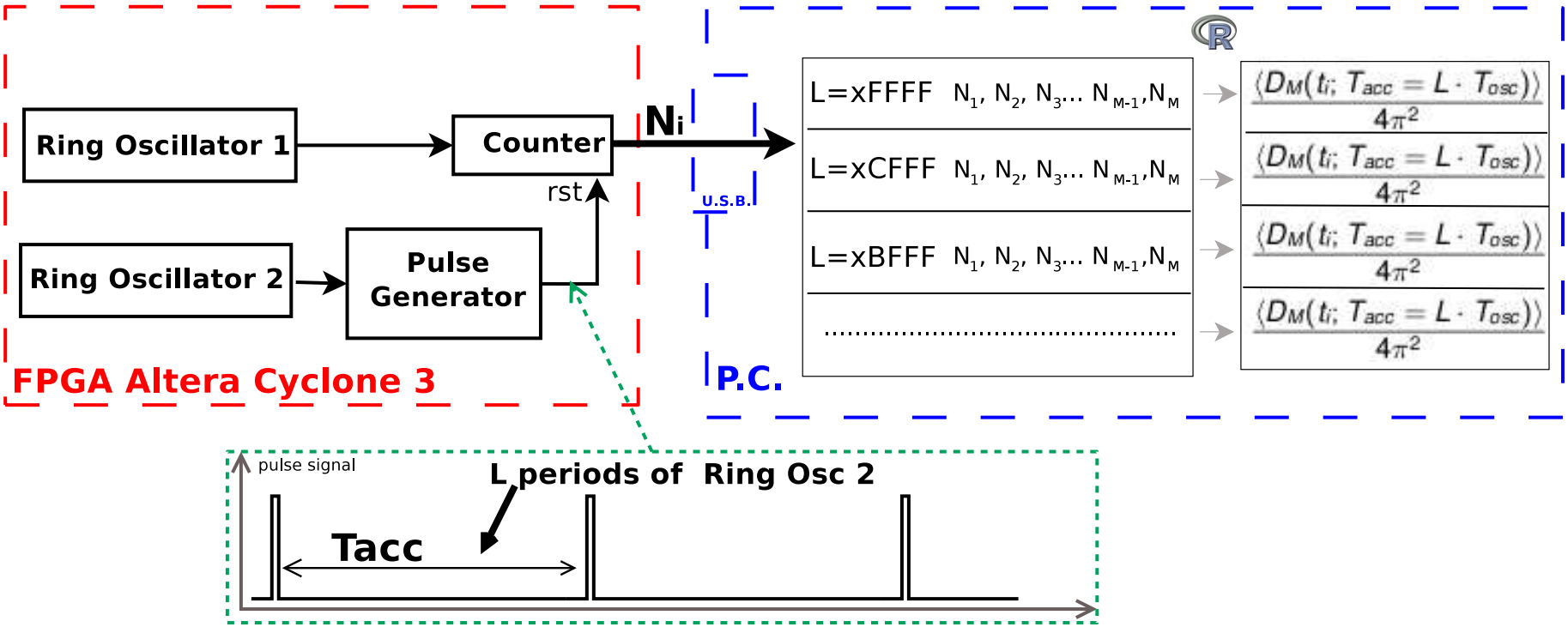
$$\Omega(t_k + T_{acc}) - \Omega(t_k) = \frac{2\pi}{T_{osc}} \cdot T_{acc} + \phi(t_k + T_{acc}) - \phi(t_k)$$

Let N_k be the number of rising edges beetween t_k and $t_k + T_{acc}$ then:

$$2\pi \cdot N_k \leq \frac{2\pi}{T_{osc}} \cdot T_{acc} + d_k(T_{acc}) \leq 2\pi \cdot (N_k + 1)$$

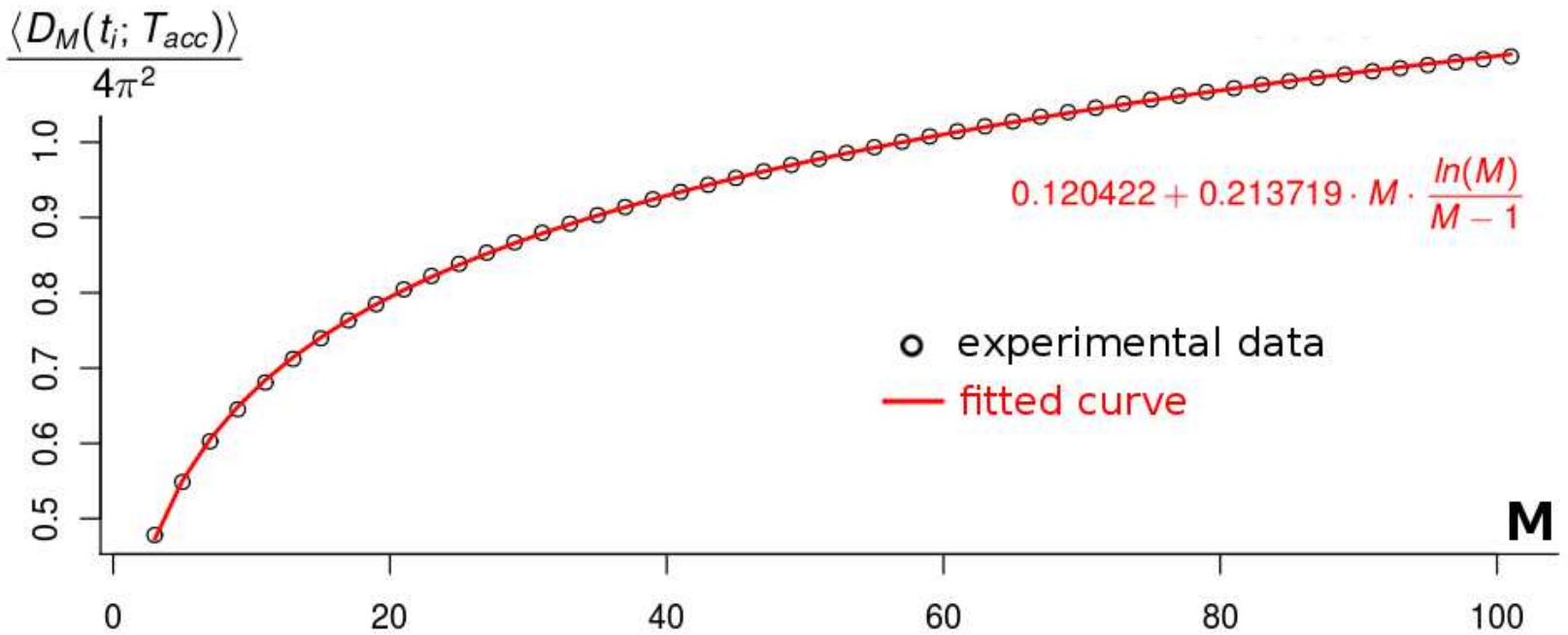
The resolution is 2π

Measurement protocol

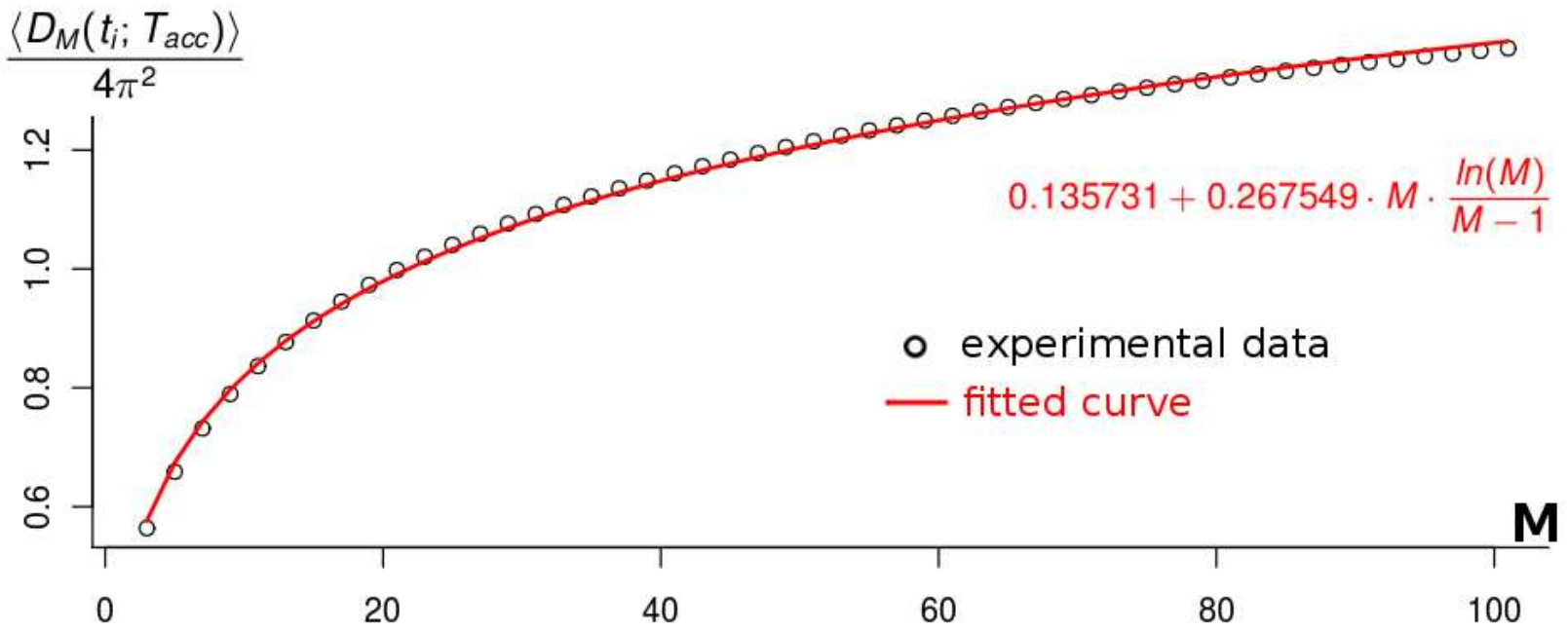


Same measurement protocol as presented before. . .
. . . but the computation in the P.C. is different

$$T_{acc} = 155\mu s$$


$\frac{\langle D_M(t_i; T_{acc})\rangle}{4\pi^2}$
0.5
0.6
0.7
0.8
0.9
1.0
0
20
40
60
80
100
M
$0.120422 + 0.213719 \cdot M \cdot \frac{ln(M)}{M-1}$
experimental data
fitted curve

$$T_{acc} = 186\mu s$$


$\frac{\langle D_M(t_i; T_{acc})\rangle}{4\pi^2}$
0.6
0.8
1.0
1.2
0
20
40
60
80
100
M
$0.135731 + 0.267549 \cdot M \cdot \frac{ln(M)}{M-1}$
experimental data
fitted curve

Conclusion and future work

- **2 noises are dominant in CMOS (flicker and thermal)**
- **Previous results highlights the presence of theses 2 noises in Altera Cyclone 3**

- **We proposed a promising way to measure the contribution of different types of noise**
  We need further implementations in other FPGA families and dedicated ASIC

Open questions

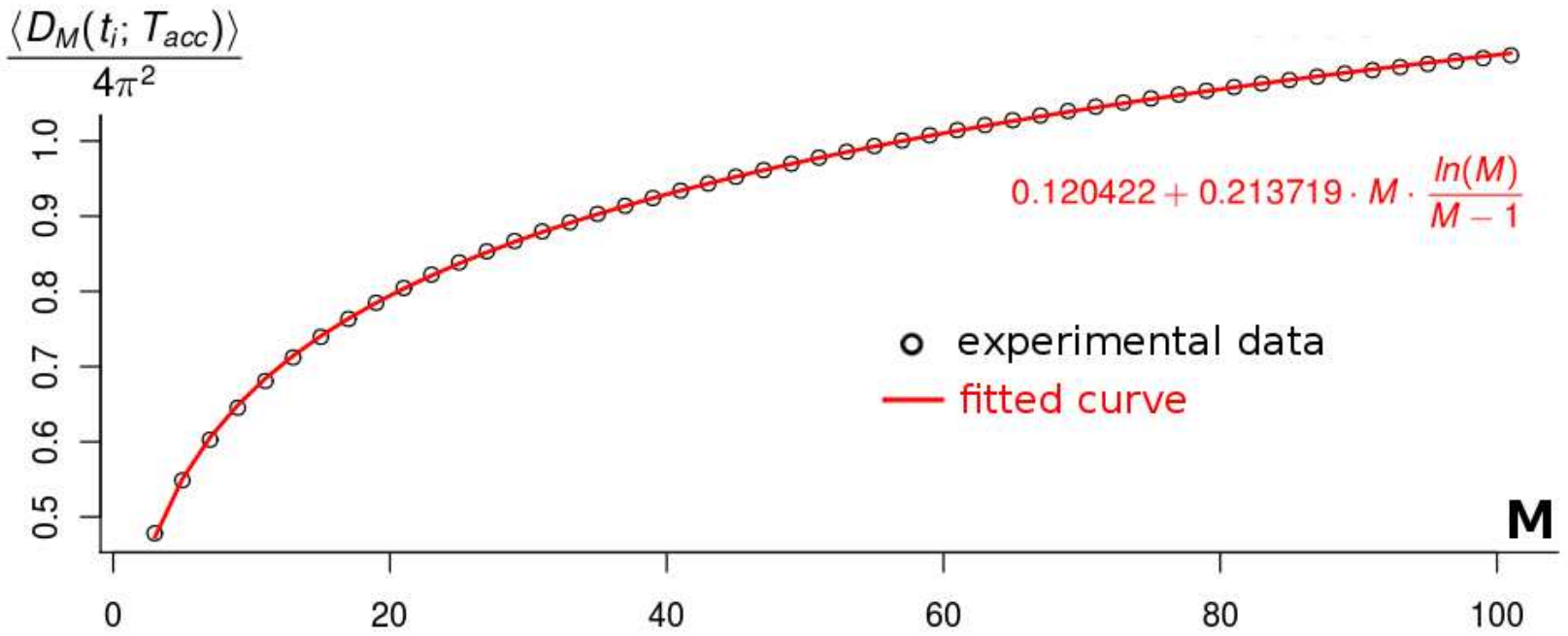
- **Flicker noise is more significant in recent technology nodes**

- **Does flicker noise have enough randomness?**
  What is its impact on the raw random number sequence?
  Does the flicker noise is usable?

Thank you for your attention

Merci dankie faleminderit amesegenallo
danke thank you شكراً eskerrik asko
благодаря 謝謝 고맙습니다 hvala
tak gracias tøkk vinaka kiitos tank
ευχαριστώ aguyjé mahalo הדות
köszönöm terima kasih grazie
ありがとう akun khob chai weebale
баярлалаа фала misoatra dank dzękuję
obrigado mulţumesc спасибо хвала
vďaka tangi tack asante salámat khob
khun teşekkür ederim дякую cám
jëre-jëf ngiyabonga…

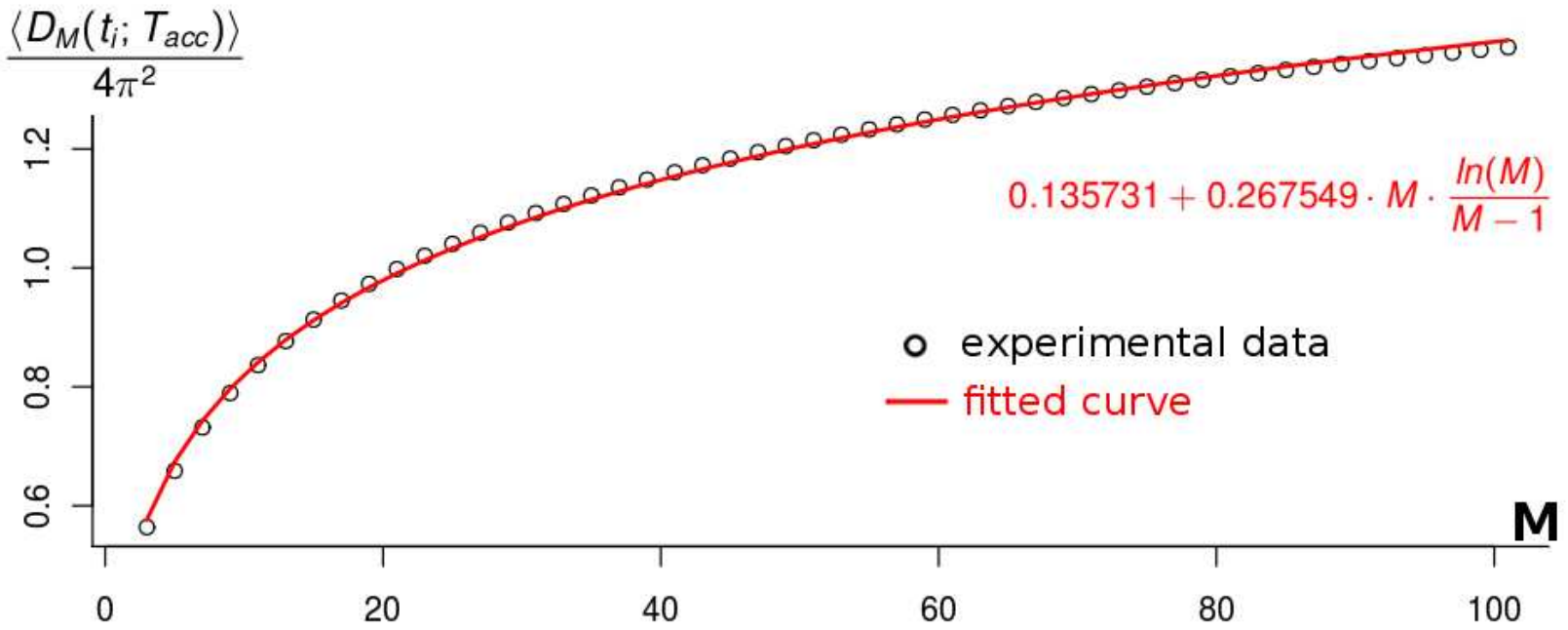
$$T_{acc} = 155\mu s$$



$$\frac{a_{-2}}{2} = \frac{0.120422}{155 \cdot 10^{-6}} = 776.9 rad^2 \cdot s^{-1}$$

$$a_{-3} = \frac{0.213719}{(155 \cdot 10^{-6})^2} = 8.895 \cdot 10^6 rad^2 \cdot s^{-2}$$

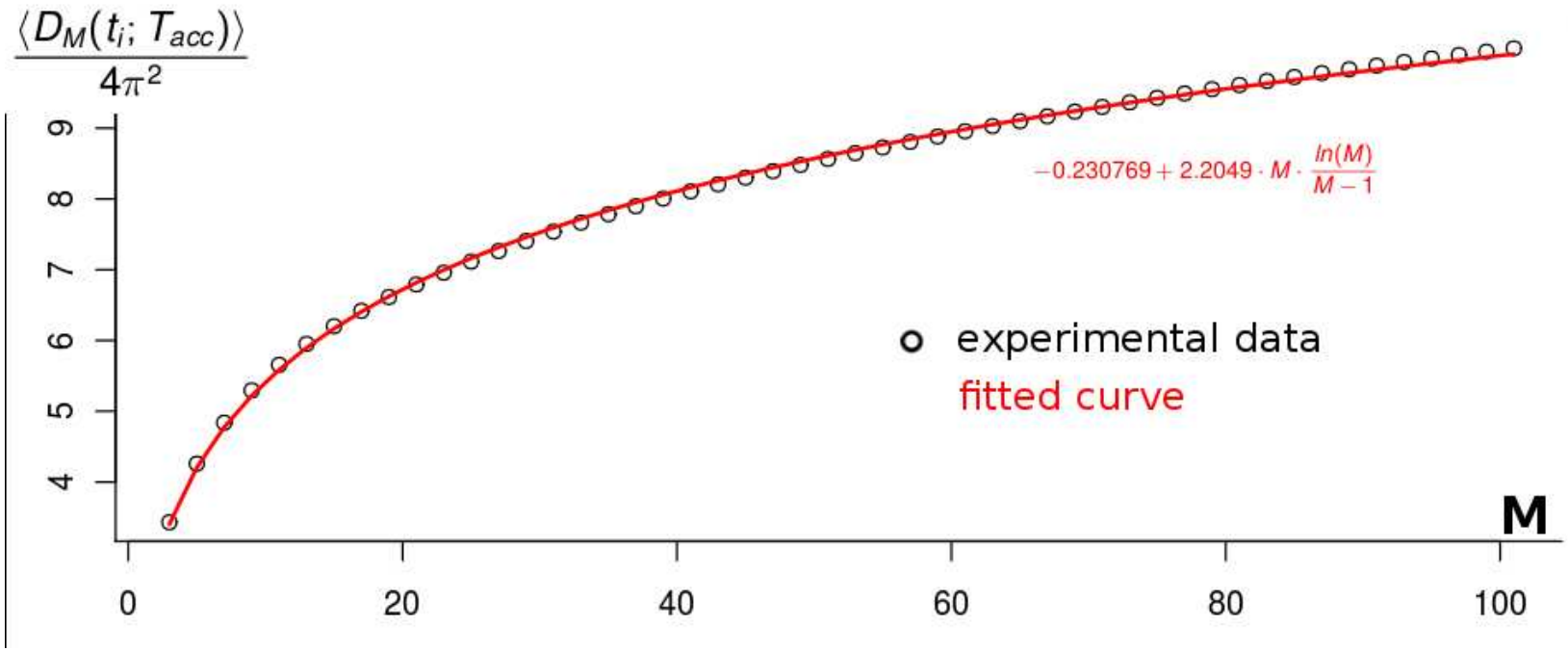
$$T_{acc} = 186\mu s$$



$$\frac{a_{-2}}{2} = \frac{0.135731}{186 \cdot 10^{-6}} = 729.7 rad^2 \cdot s^{-1}$$

$$a_{-3} = \frac{2.2049}{(186 \cdot 10^{-6})^2} = 7.733 \cdot 10^6 rad^2 \cdot s^{-2}$$

$$T_{acc} = 496\mu s$$



$$\frac{a_{-2}}{2} = \frac{-0.230769}{496 \cdot 10^{-6}} = -465.3 rad^2 \cdot s^{-1}$$

$$a_{-3} = \frac{2.2049}{(496 \cdot 10^{-6})^2} = 8.962 \cdot 10^6 rad^2 \cdot s^{-2}$$

Proposal : extract the same entropy as the measured one (by online tests).