Architecture and Method to design common PUF/TRNG functions

Cryptachi Workshop
Monday 29 June 2015

Jean-Luc DANGER
Prof. **Télécom ParisTech**
Scientific Advisor **Secure-IC**

Joint work with **Yves Mathieu,** Prof. **Télécom ParisTech**
Thibault Portebeuf, project Leader **Secure-IC**

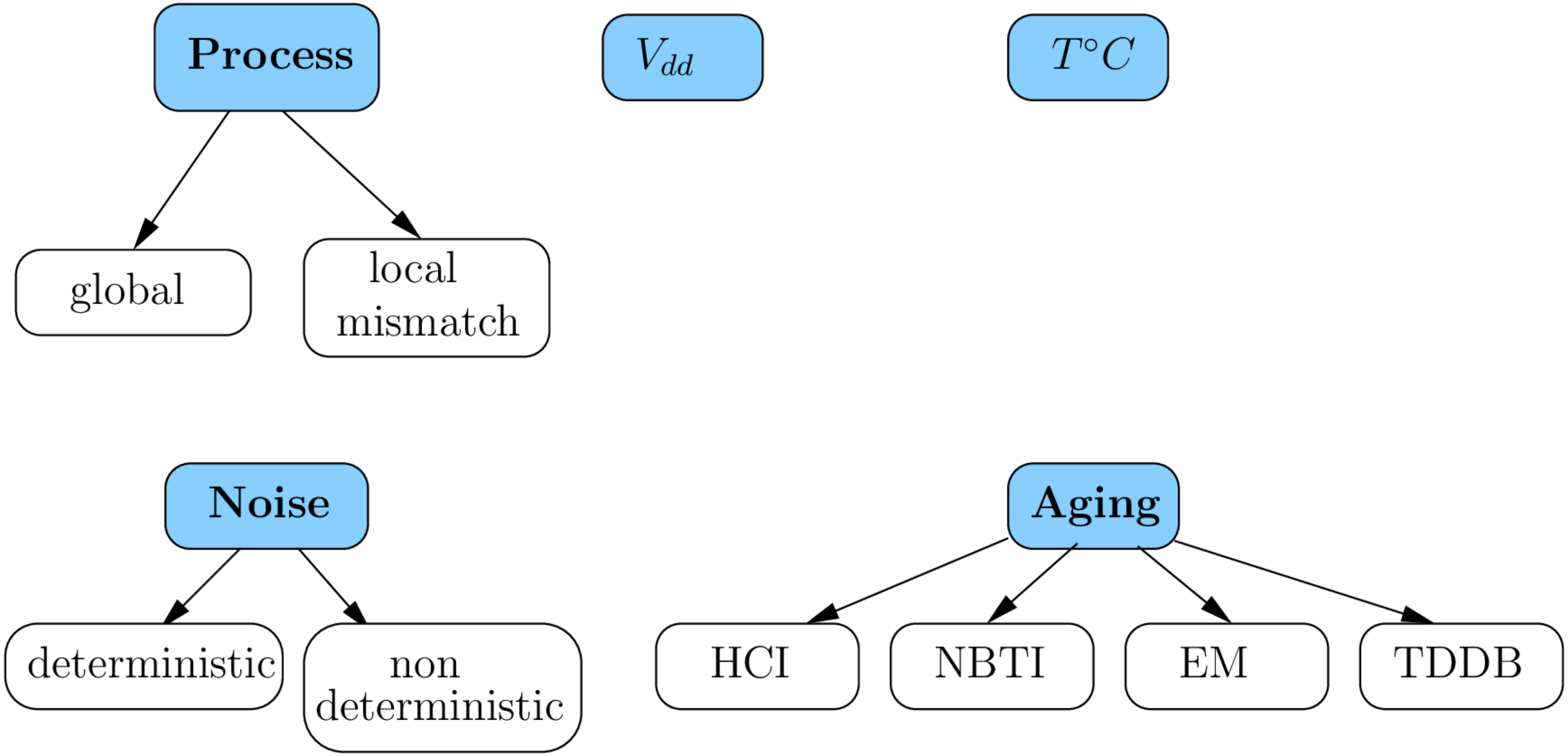
Agenda

- IC Variability for PUF/TRNG
- Mixed PUF/TRNG concept
- Results
- Conclusions

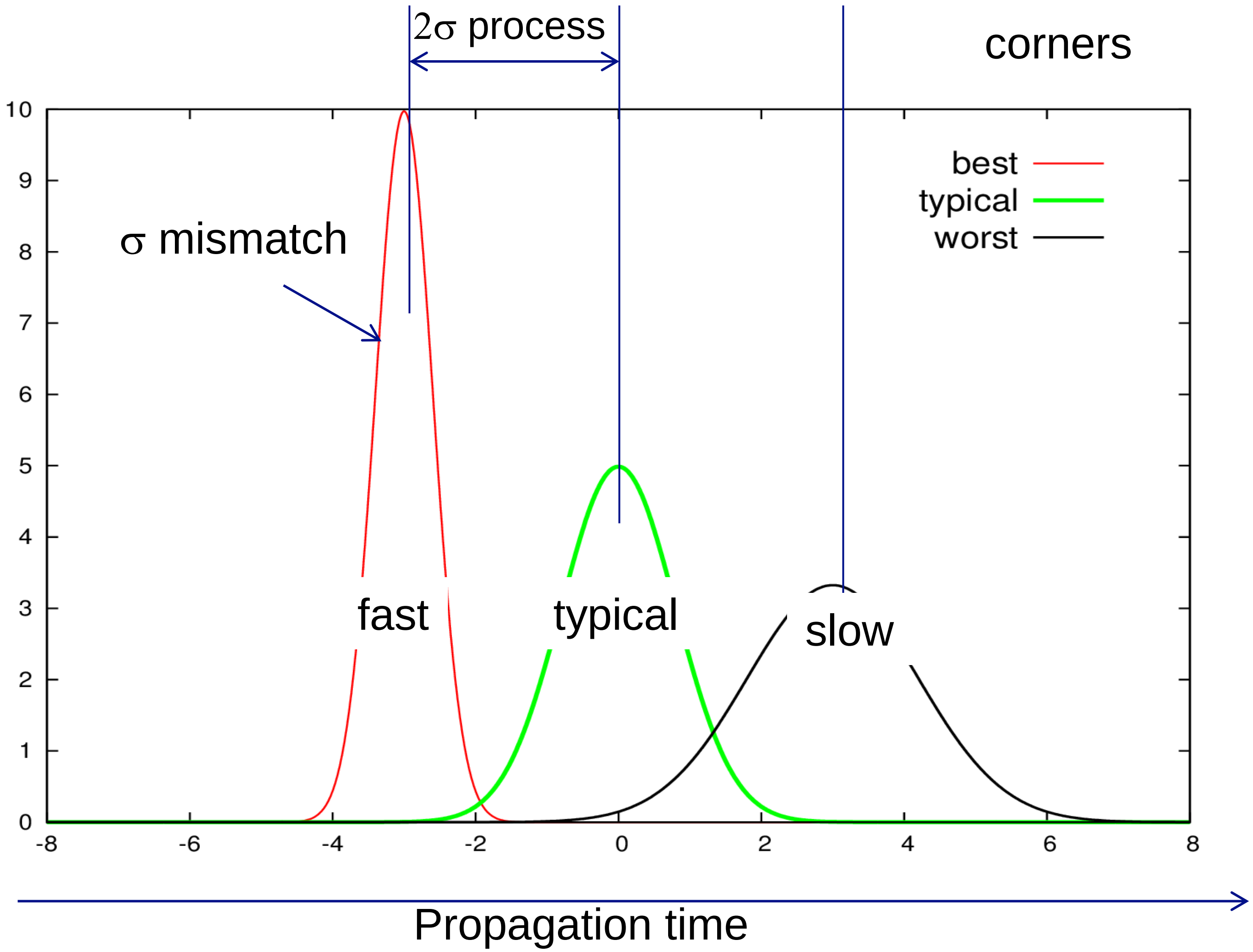
Agenda

- **IC Variability for PUF/TRNG**
- Mixed PUF/TRNG concept
- Results
- Conclusions

Causes of IC Variability



Process dispersion



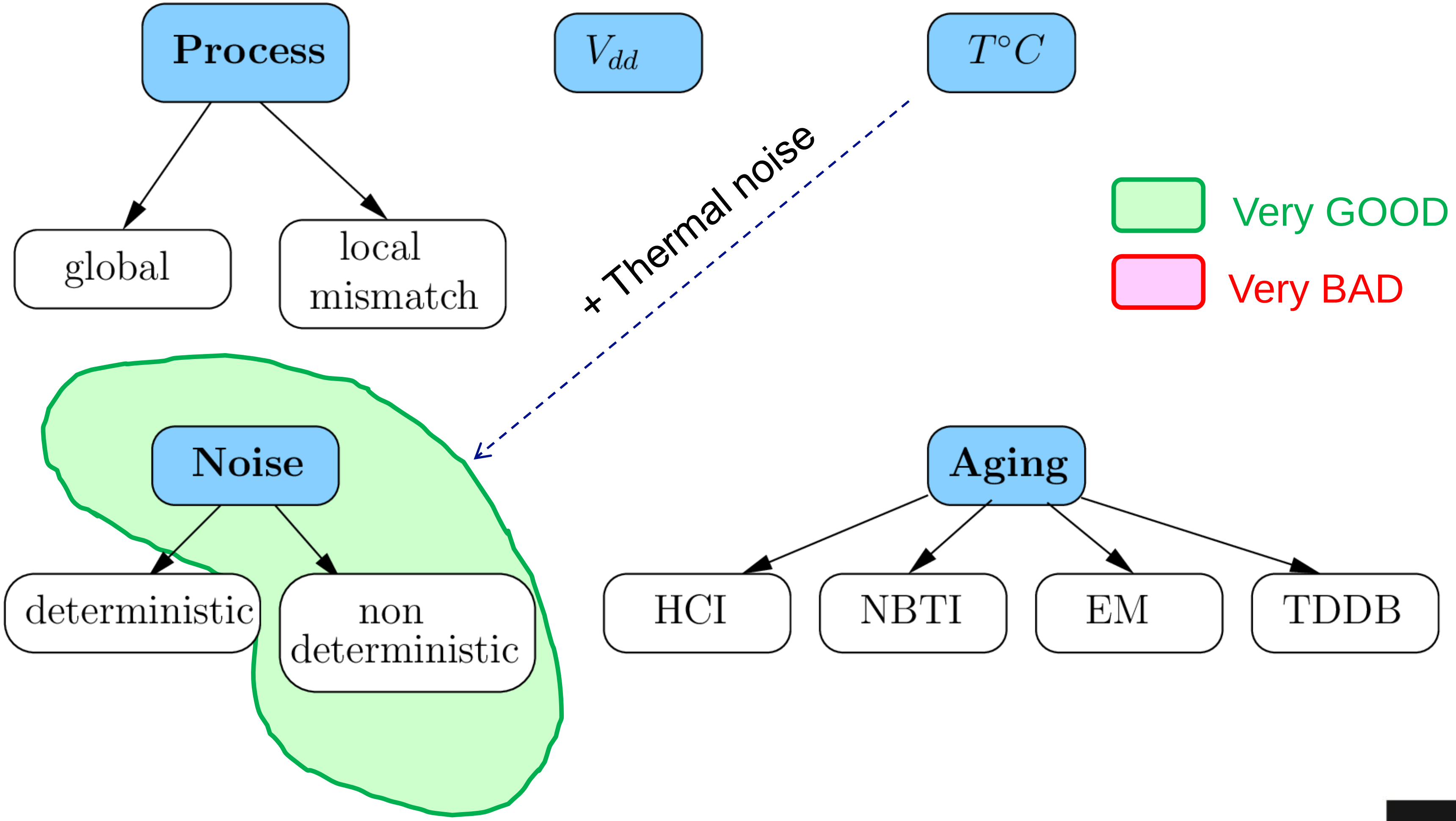
Noise

- **Sum of different phenomenon:**
  - Thermal noise
  - 1/F noise
  - Shot noise
  - Popcorn noise
  - Crosstalk
  - Interference → Source of attacks

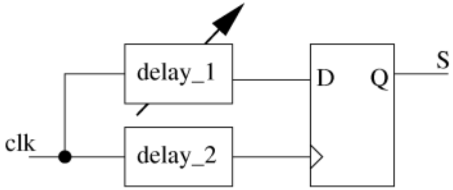
Ideally TRNG should be:

- undetermisitic (temporal dependance)
- uncorrelated (spatial dependance)

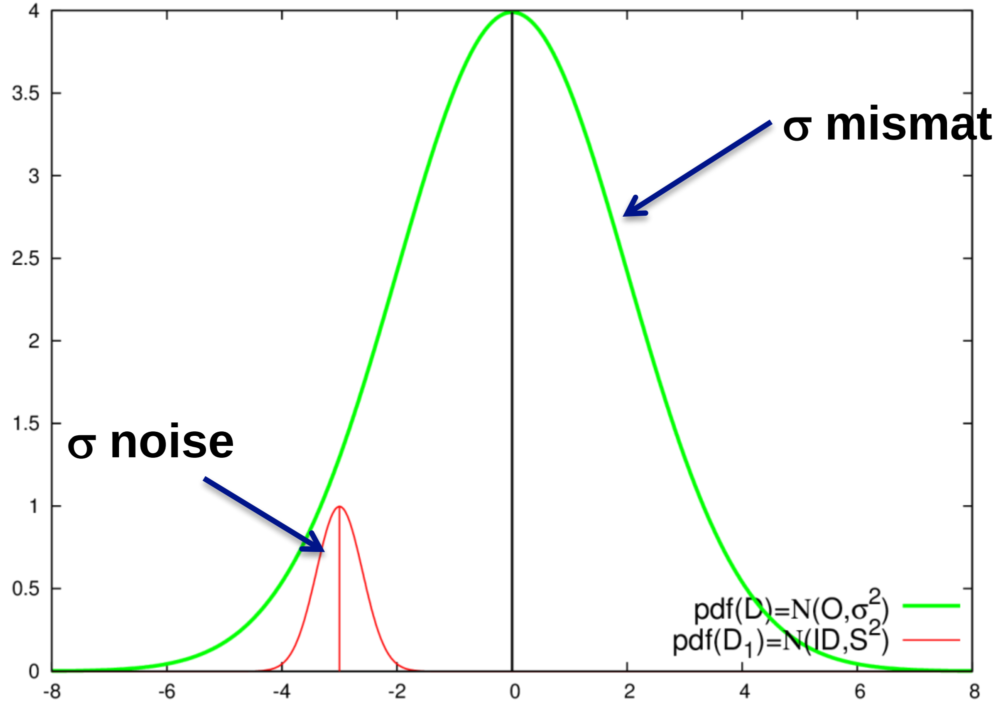
Variability impact for TRNG



Example: TRNG based on metastability



TRNG area

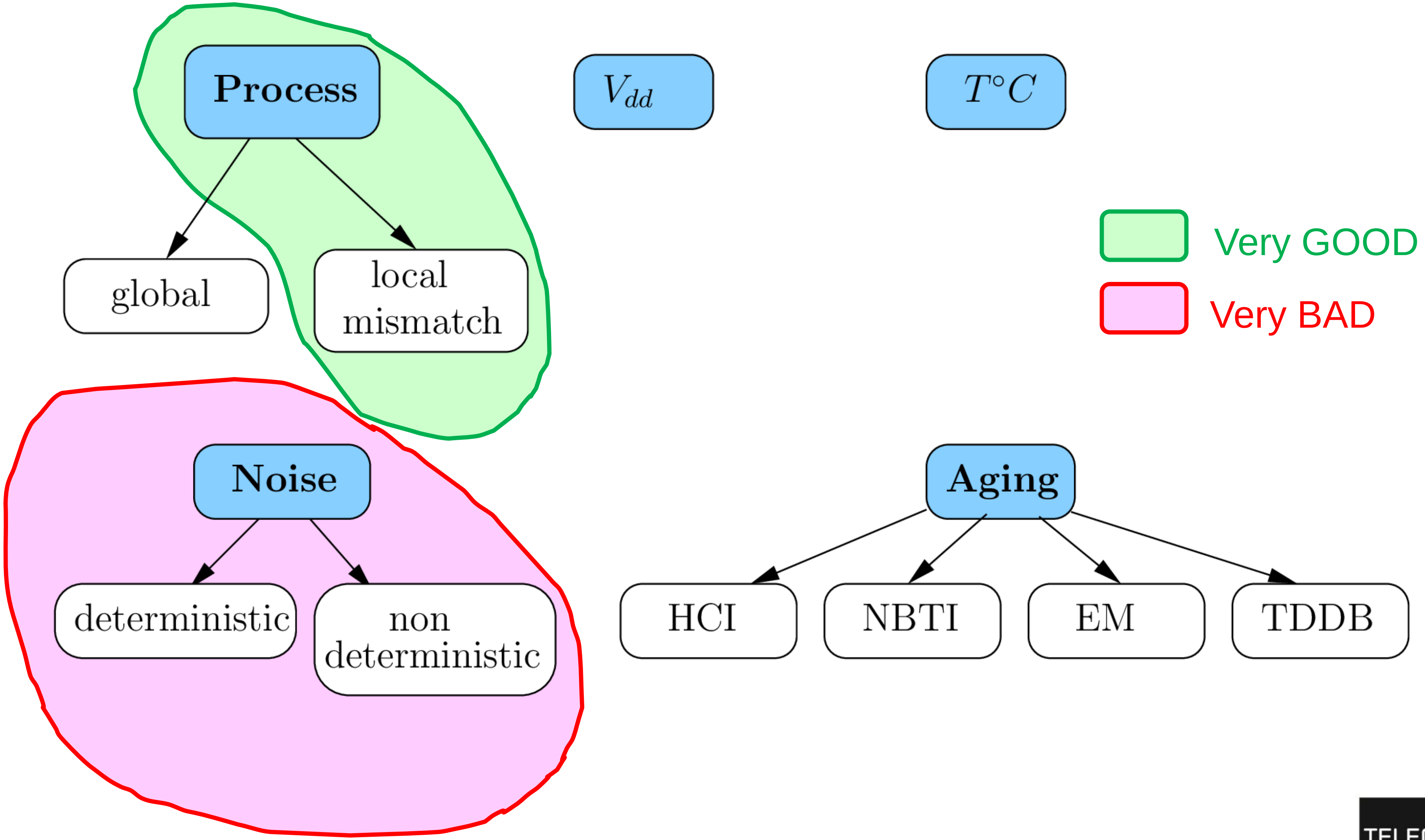


σ mismatch

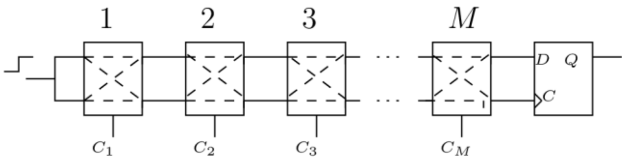
σ noise

T_su distribution

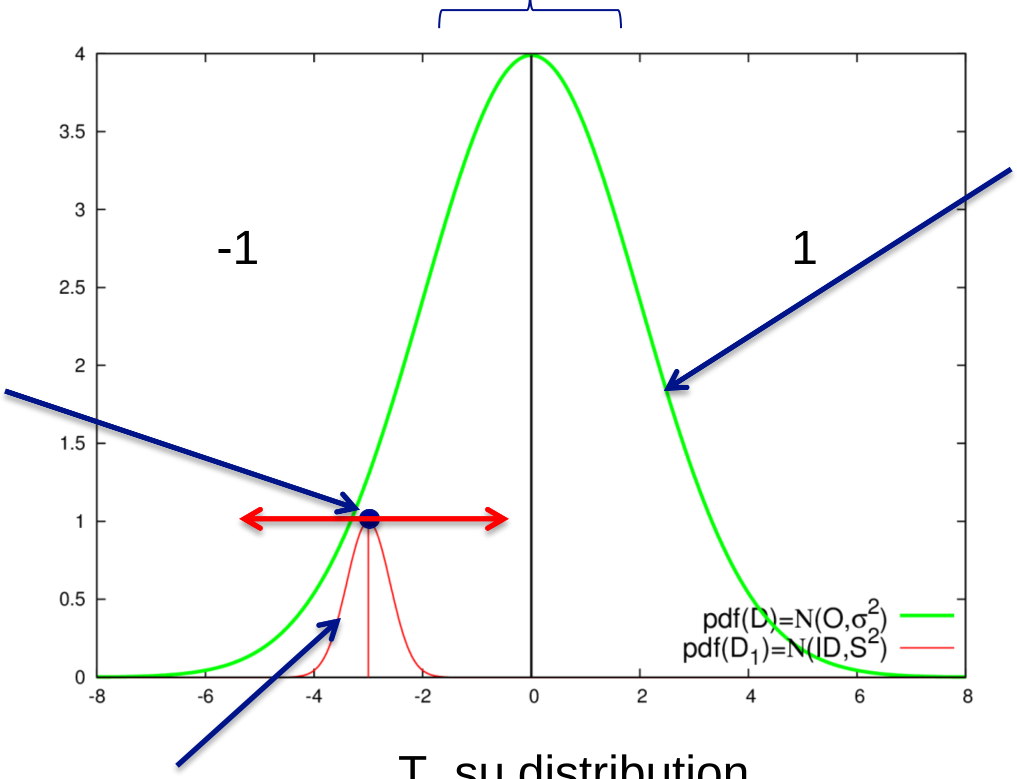
Variability impact for PUF



Example: Delay PUF



Unreliability area



-1

1

σ mismatch

Impact of T°C, Vdd, aging

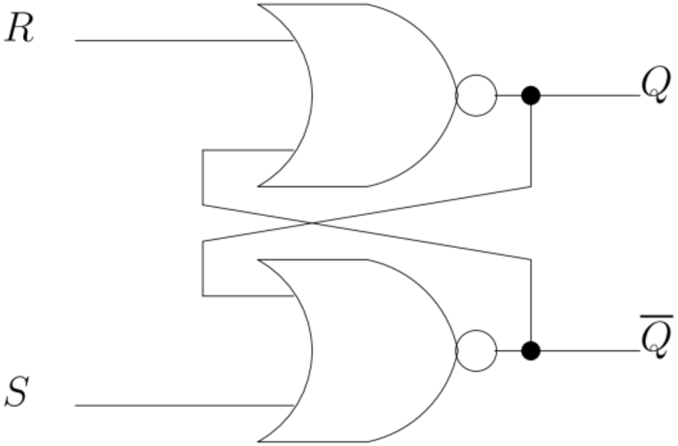
σ noise

T_su distribution

Agenda

- IC Variability for PUF/TRNG
- **Mixed PUF/TRNG concept**
- Results
- Conclusions

Basic element: RS latch



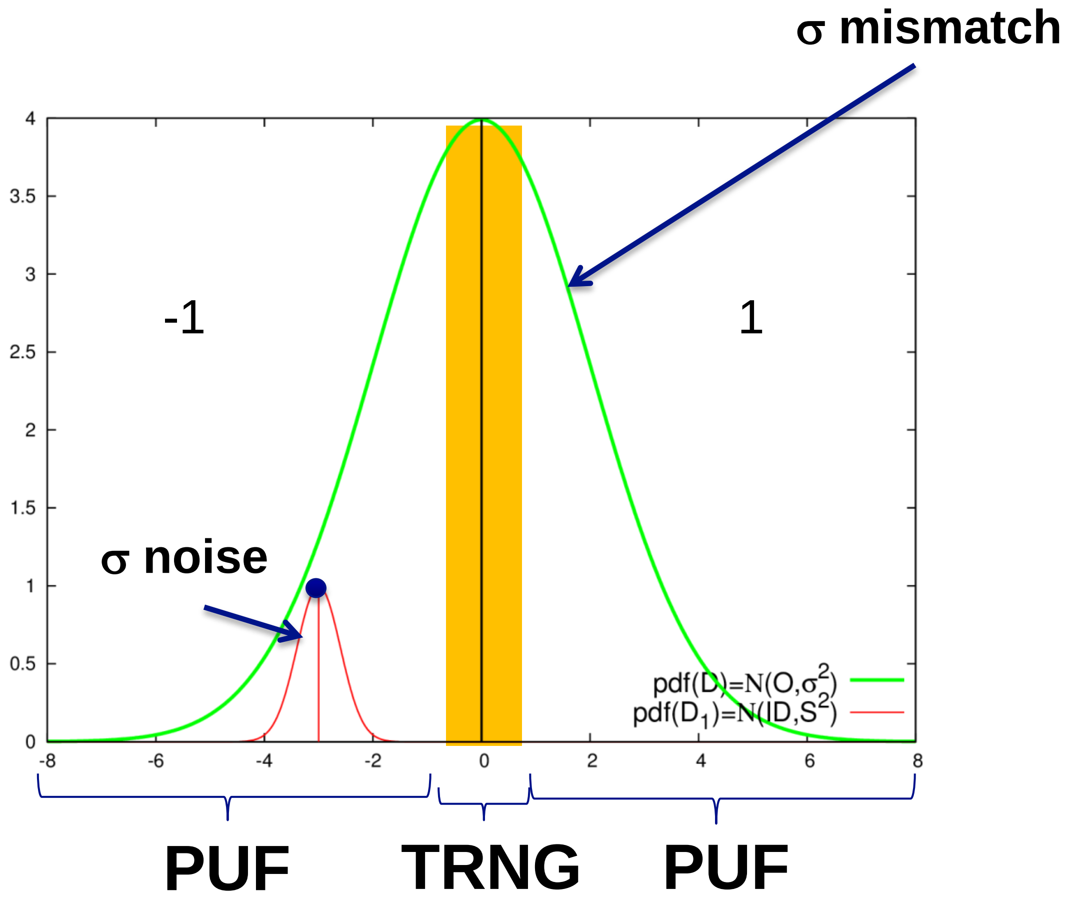
When R and S goes '1' to '0':

❑ **Metastable** state which converges toward a stable state.

❑ The stable state depends on:

- noise => **TRNG**(Open Loop TRNG,…)
- mismatch => **PUF** (latch PUF, TERO PUF,…)

RS latch: either TRNG or PUF



σ mismatch

-1

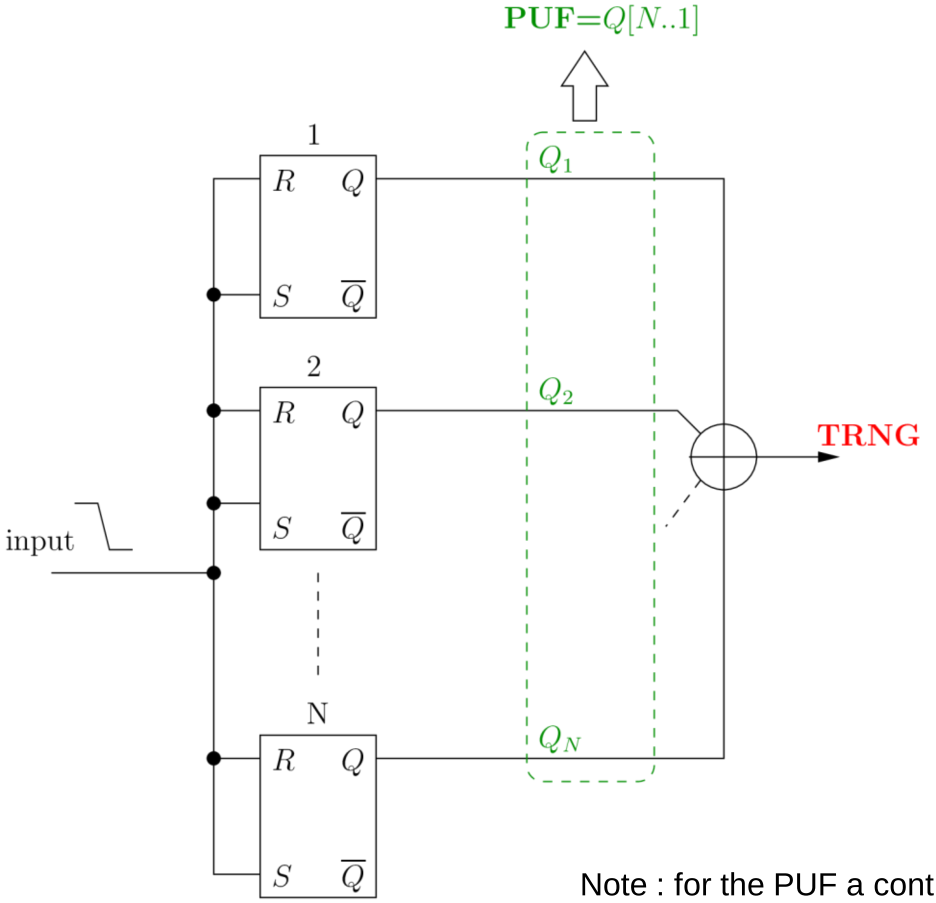
1

σ noise

PUF **TRNG** **PUF**

T_su distribution

PUF/TRNG architecture



Note : for the PUF a controlled delay line is necessary to detect unreliable RS latches

TRNG Statistical model

- **First define the required entropy H => P_H**
- **Then compute the probability to get a good circuit with 1 RS latch**

  P_ref= erf(erf^{-1}(2.P_H – 1) σ noise/ σ mismatch)

- **Then deduce the probability to get a good circuit with N elements**
  - Pr (required entropy with N RS)

    =1-(1-P_ref)^{N}

  - Pr (required entropy with N RS and correlated noise)

    =(1-(1-P_ref)^{N}) $^{\alpha}$

    Ratio uncorrelated/correlated noise

Note: The correlated noise corresponds to a shift of all the t_su distribution

PUF Statistical model

- **First, define the unreliable area (or noise margin = W σ noise) , in the center of the t-su distribution**
- **Then, compute the probability to get a reliable PUF**

$$P\_rel = 1 - erf\left(\frac{W}{\sqrt{2}}\frac{\sigma\_noise}{\sigma\_mismatch}\right)$$

- **Then, compute the probability to get at least L reliable bits among N**

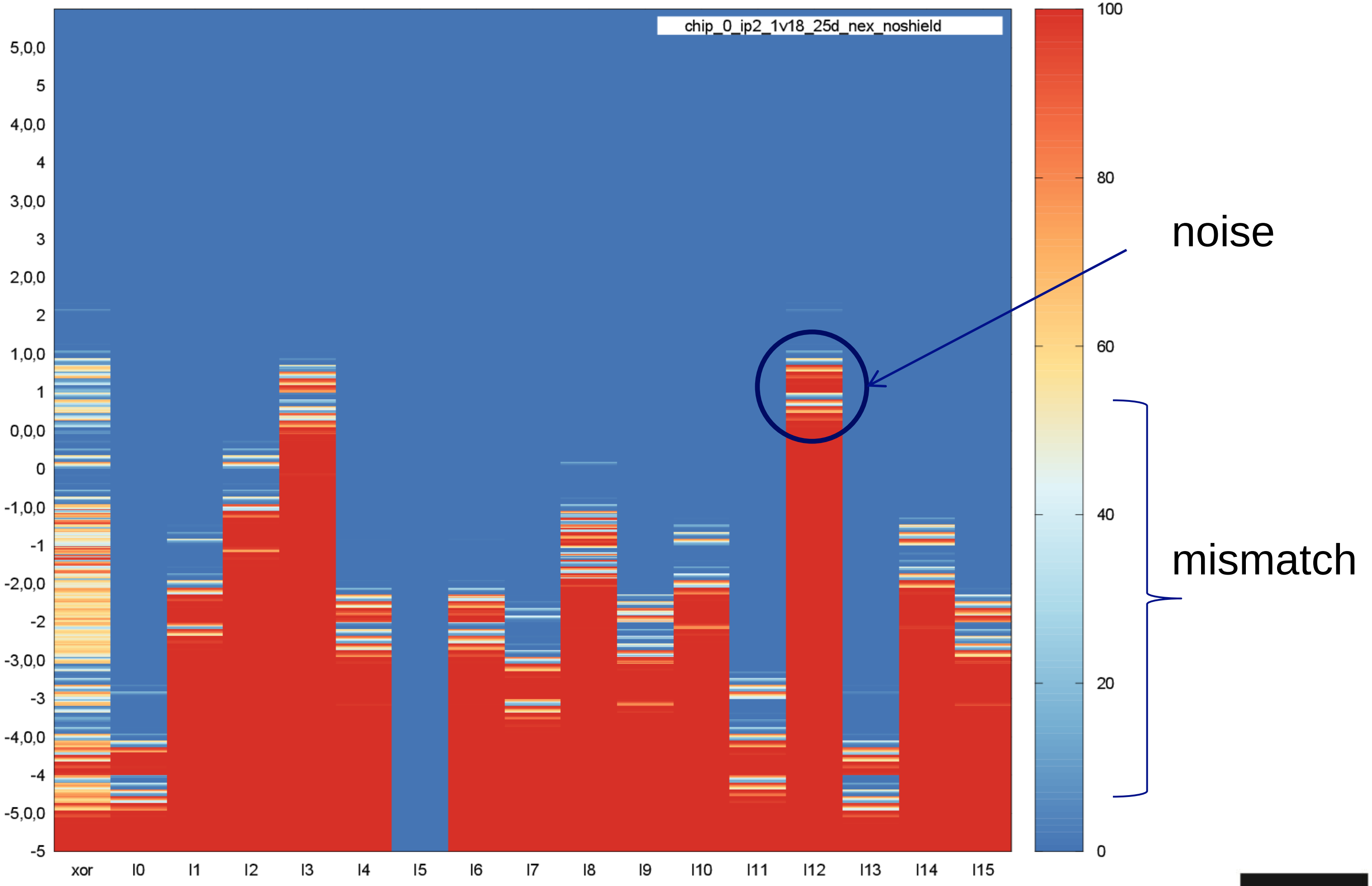
$$\mathrm{Pr}\_L_{reliable\_bits} = \beta(\mathrm{Pr}\_rel;L,N-L+1)$$

Uncomplete Beta function
= cumulative distribution of a binomial law

Agenda

- IC Variability for PUF/TRNG
- Mixed PUF/TRNG concept
- **Results**
- Conclusions

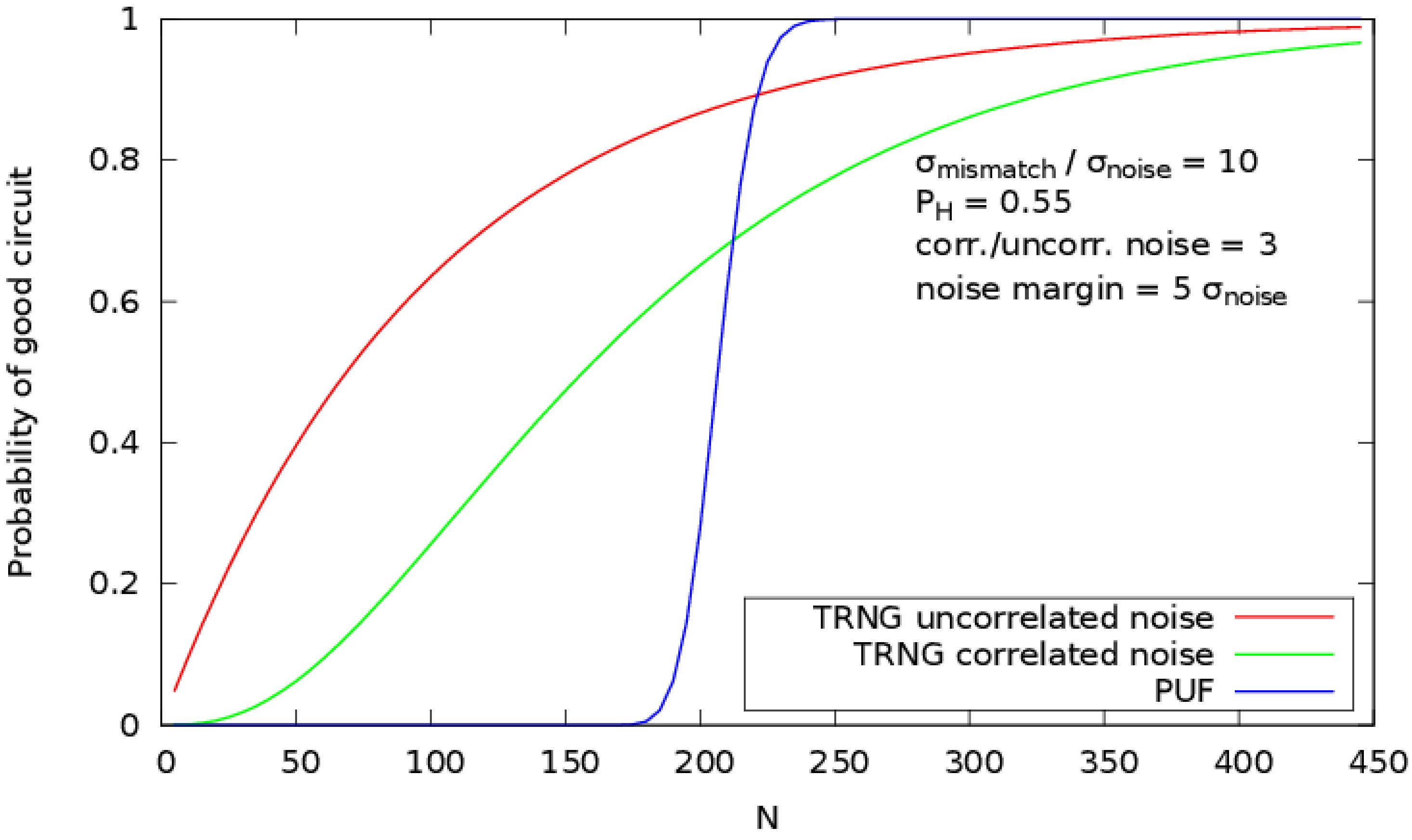
Results with 16 latches in 65nm technology



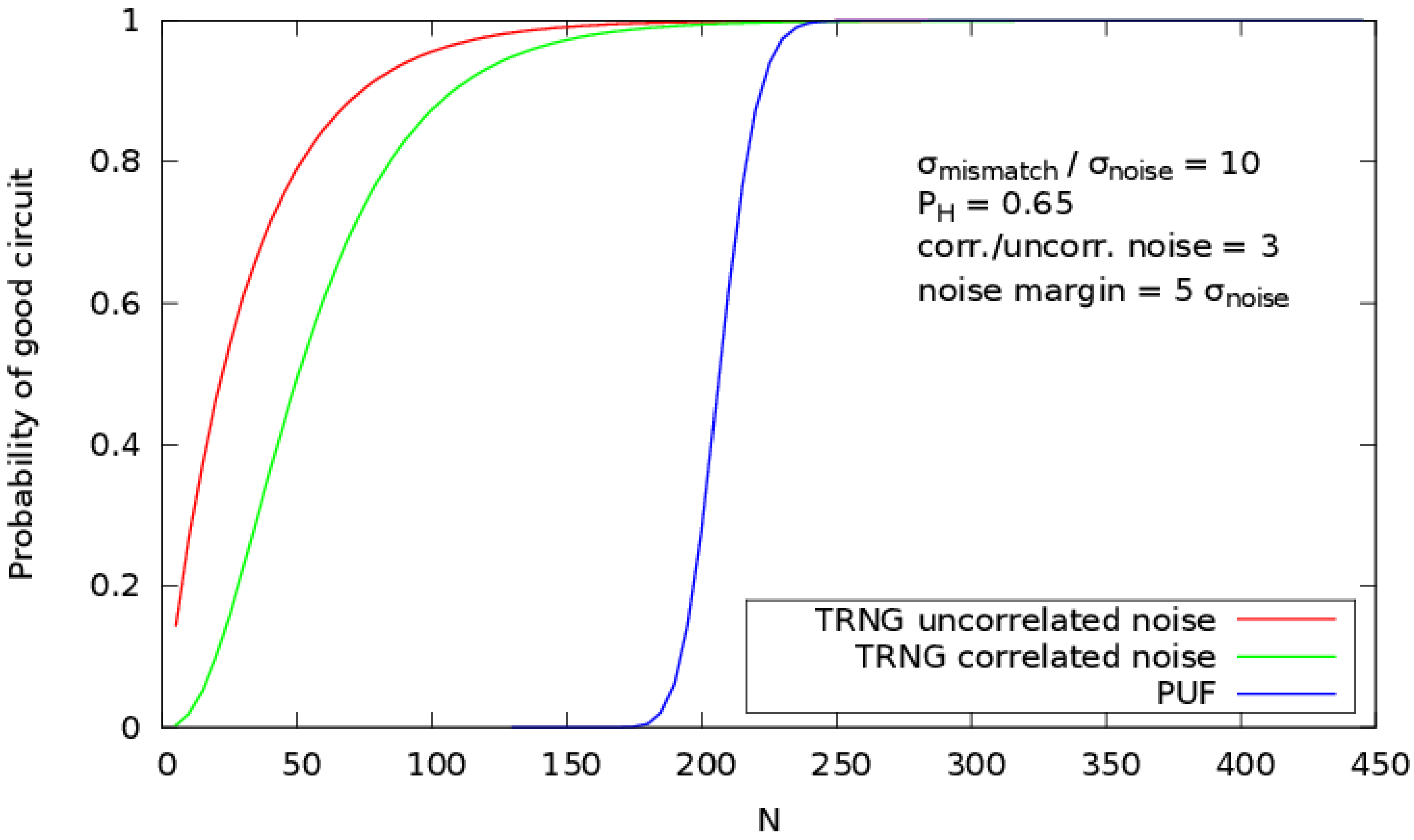
noise

mismatch

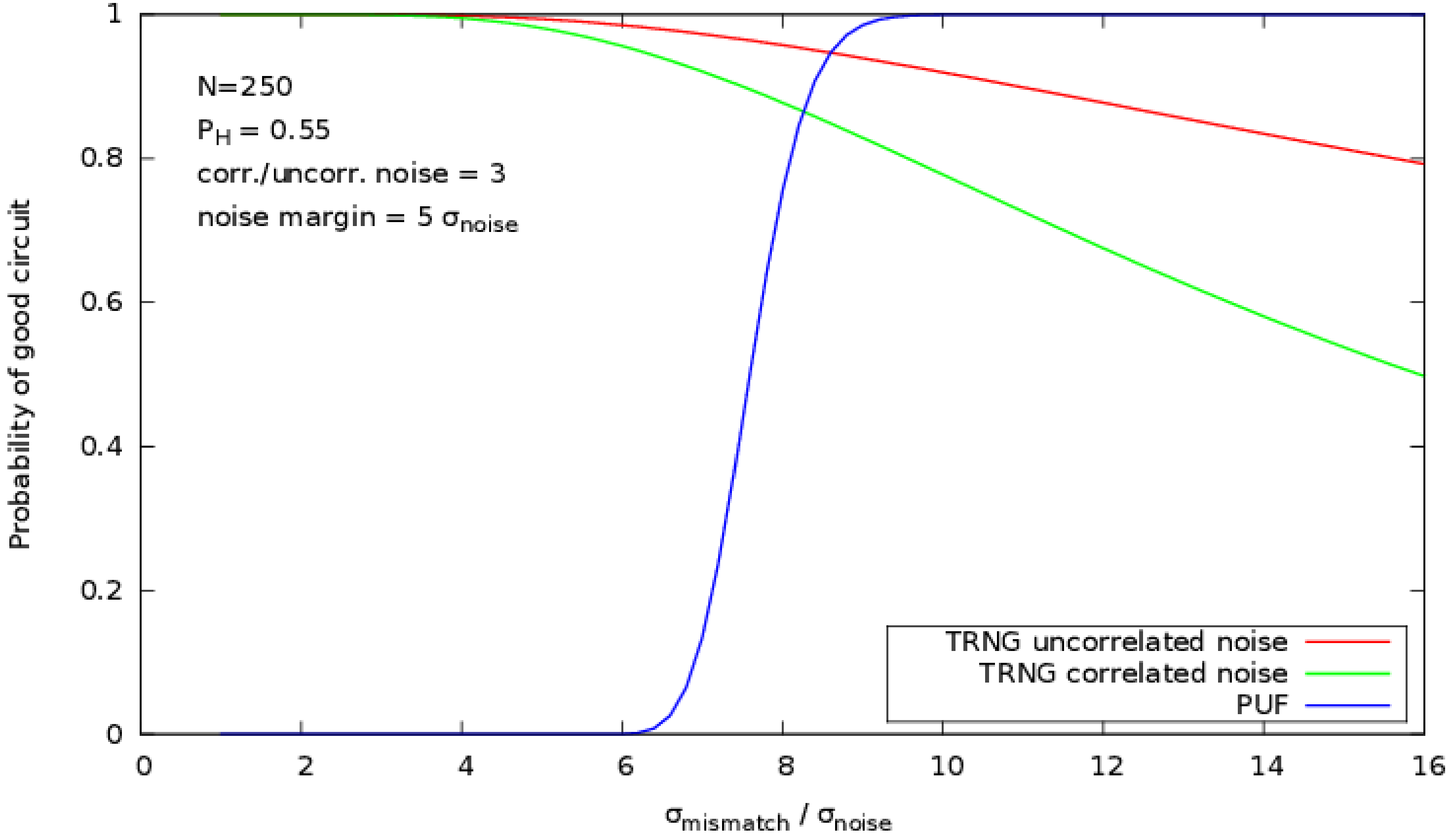
Impact of N with high entropy required



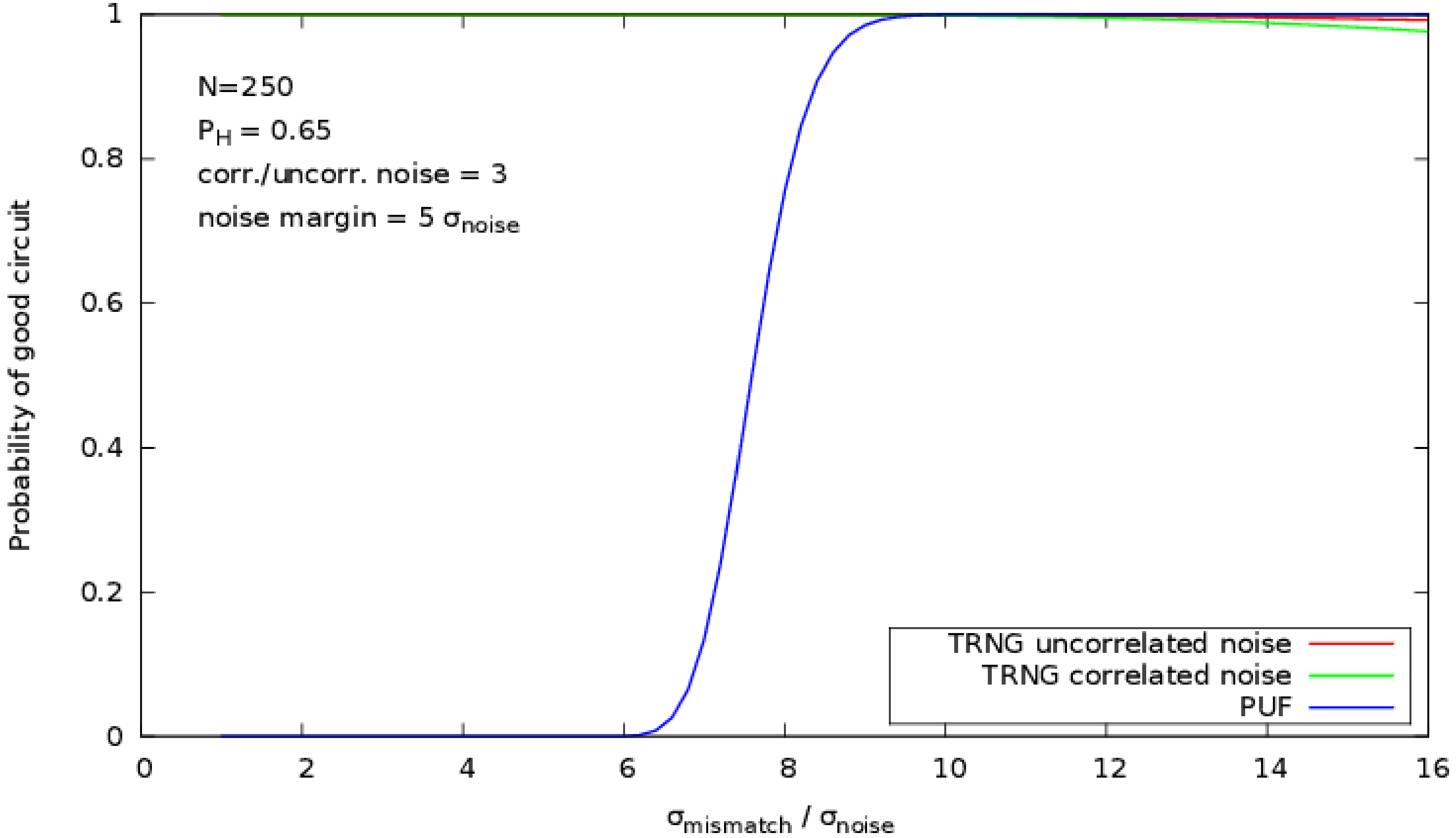
Impact of N with medium entropy required



Impact of σ_mismatch / σ_noise, high entropy required



Impact of σ_mismatch / σ_noise medium entropy required



Agenda

- IC Variability for PUF/TRNG
- Mixed PUF/TRNG concept
- Results
- **Conclusions**

Conclusions

- **A TRNG/PUF can be obtained from a set of many RS latches**
  - Exploits noise when T_su near 0
  - Exploits mismatch when T_su great
- **Statistical models depend on:**
  - σ mismatch/ σ noise
  - N
  - Required entropy for TRNG
  - Correlated noise for TRNG
  - Noise margin for PUF
- **N can be low**
  - by further post processing to enhance the entropy:
    - XORs, von neumann, compression,…