Matthias Hiller, Georg Sigl and Michael Pehl

A New Model for Estimating Bit Error Probabilities of Ring-Oscillator PUFs

11/07/2013

8th International Workshop on Reconfigurable Communication-centric Systems-on-Chip

Outline

- Introduction to PUFs
- New Modeling Technique
- Empirical Results
- Conclusions

Introduction

Embedded security
Measurement, storage, processing, transmission of sensitive data

Secure key storage
Prerequisite for cryptography

Non-volatile memory
Secure, but expensive

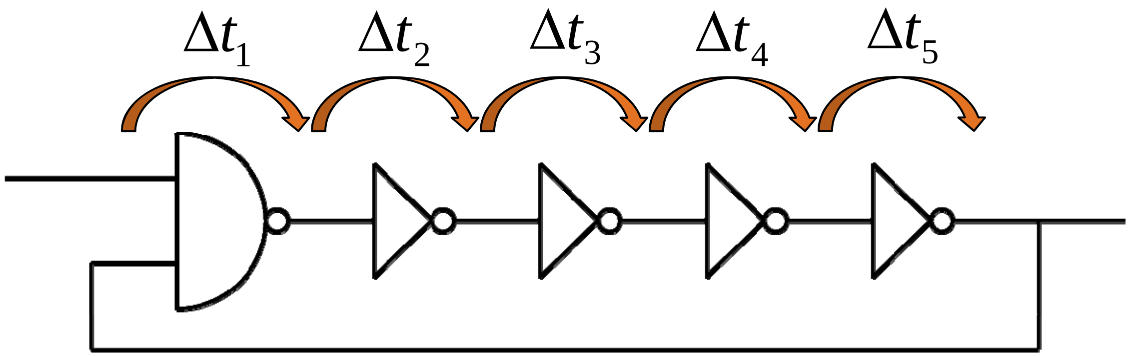
Technology and cost constraints

Solution: Physical Unclonable Functions

Physical Unclonable Functions

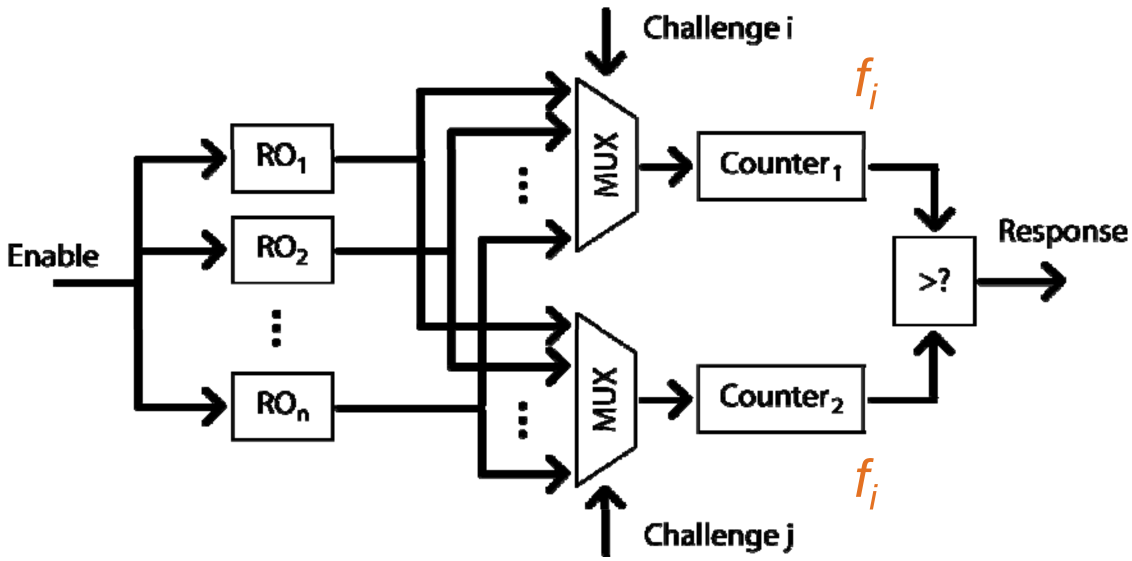
- Measurement of internal physical properties
- Randomness
- Precise PUF models necessary for error correction

Ring Oscillators from Logic Gates



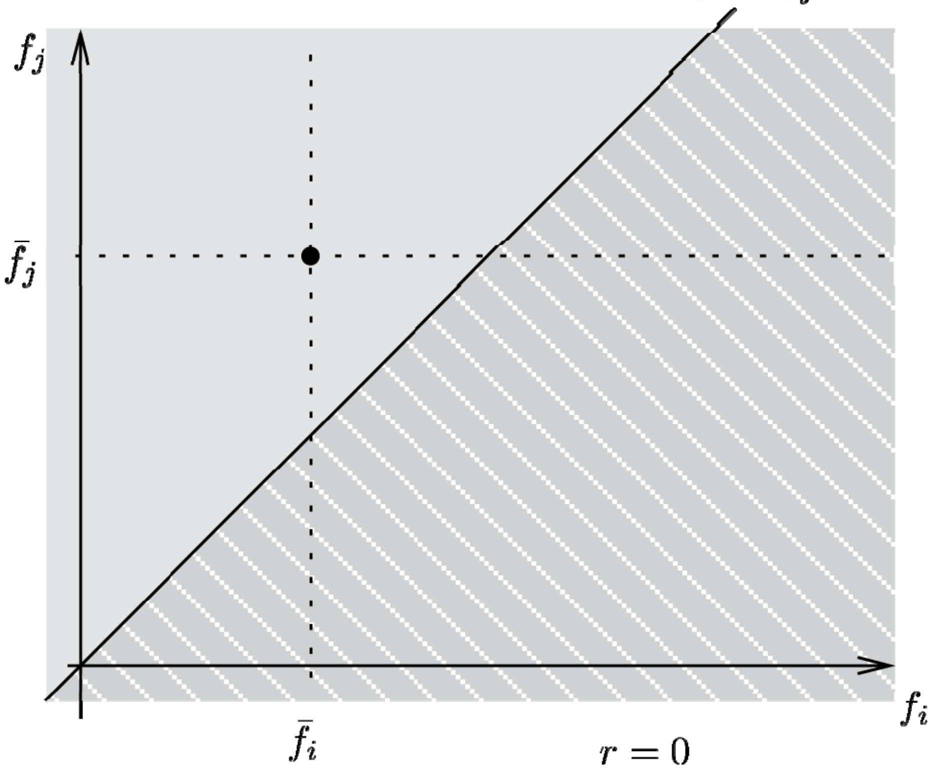
$$f = \frac{1}{\sum_{i=1}^{5} \Delta t_i}$$

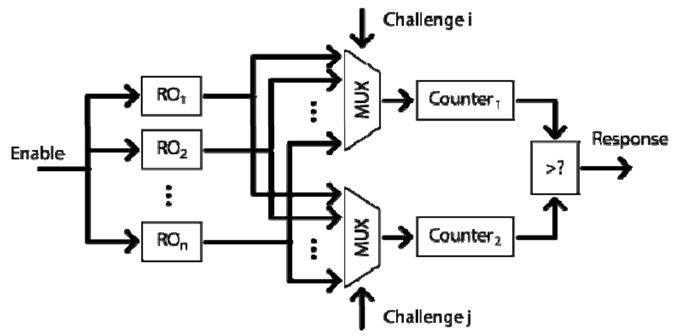
Ring Oscillator PUF



Suh et al., 2007

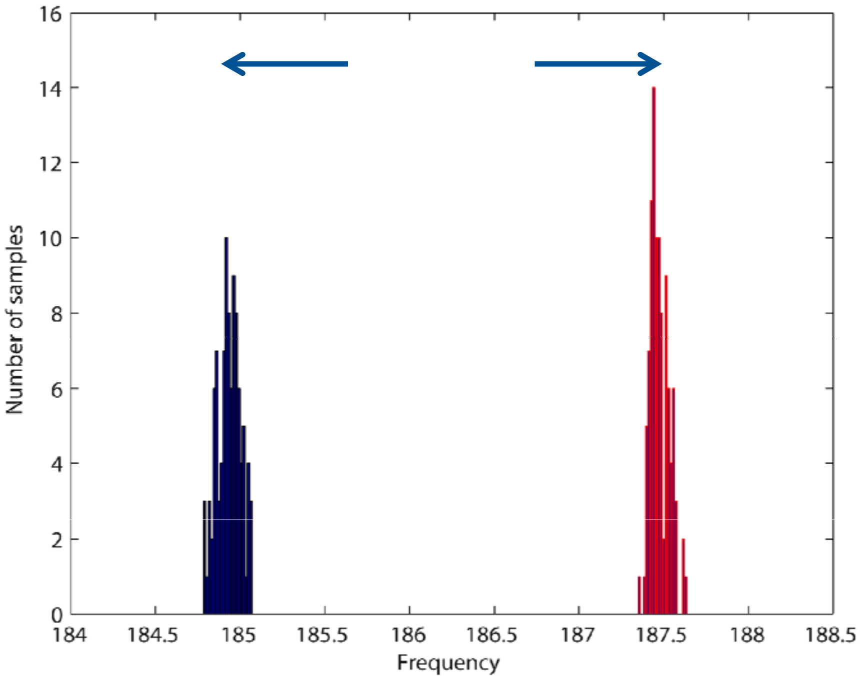
Bit derivation



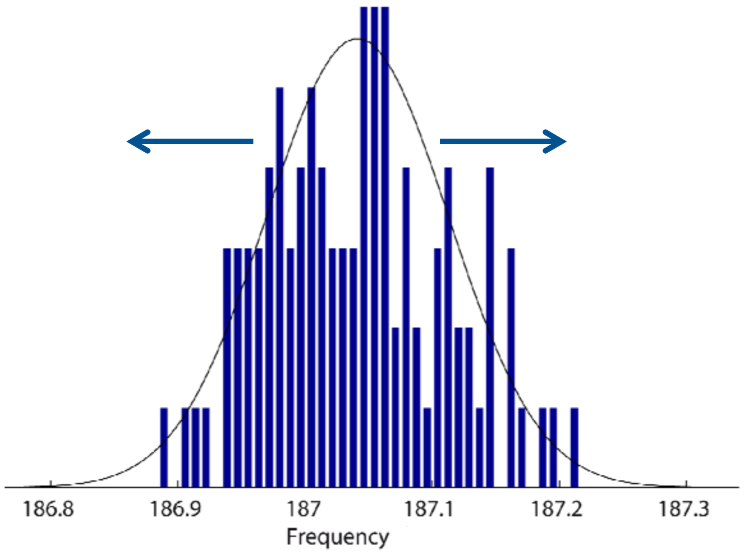


Randomness

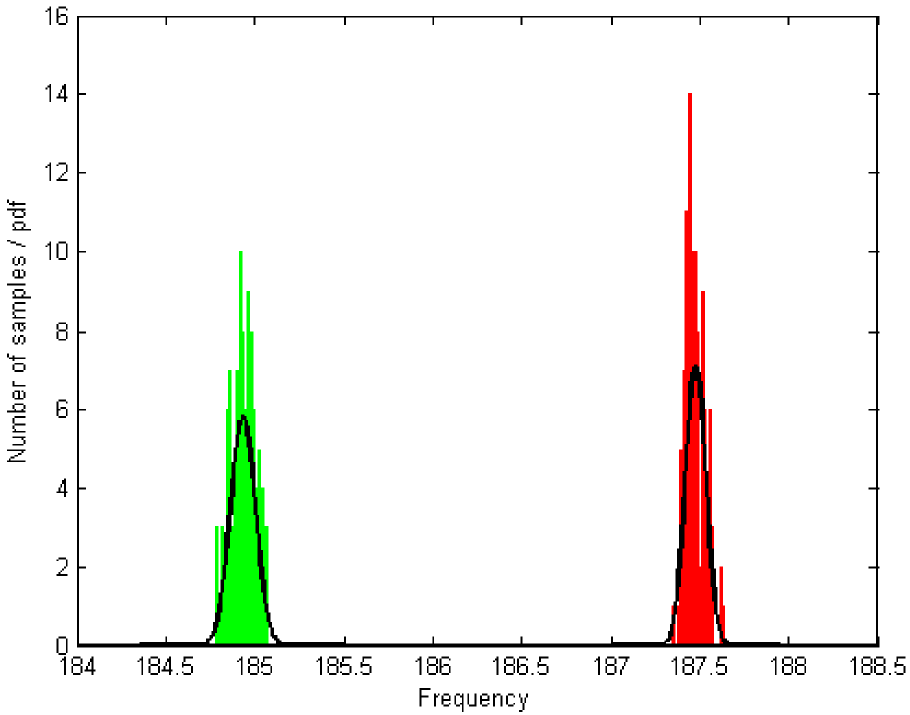
Uniqueness



Reliability



State of the art



- Direct comparison of frequencies
- Problem: Precision scales linearly with the effort

e.g. Maiti et al. (HOST 2010), Armknecht et al. (S&P 2011)

Outline

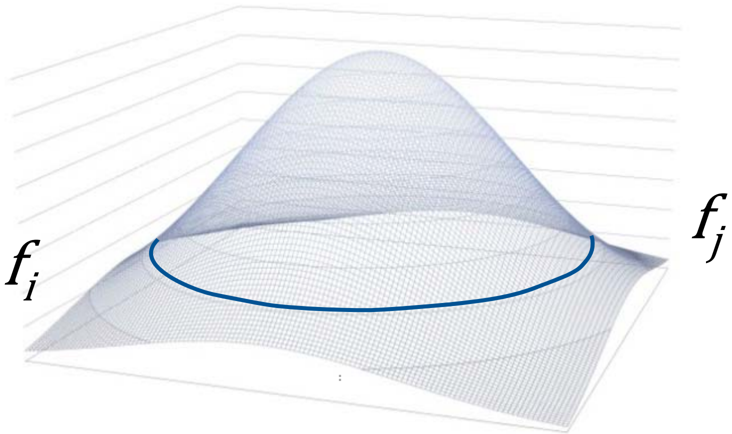
- Introduction to PUFs

- New Modeling Technique
- Empirical Results

- Conclusions

Multivariate Distribution

$$\bar{\mathbf{f}} = \left[\bar{f}_i; \bar{f}_j\right]^T$$



$$\mathbf{C} = \begin{bmatrix} \sigma_i^2 & \sigma_i \rho_{i,j} \sigma_j \\ \sigma_i \rho_{i,j} \sigma_j & \sigma_j^2 \end{bmatrix}$$

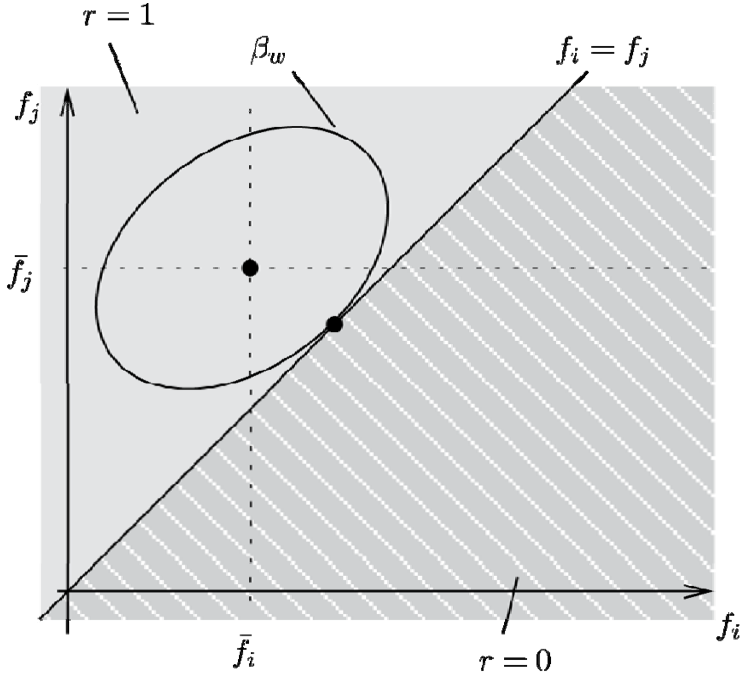
$$pdf(\mathbf{f}) = \frac{1}{2\pi\sqrt{\det(\mathbf{C})}} \exp\left(-\frac{(\mathbf{f}-\bar{\mathbf{f}})^T \mathbf{C}^{-1} (\mathbf{f}-\bar{\mathbf{f}})}{2}\right)$$

Reliability Analysis

$$x = [1, -1] \begin{bmatrix} f_i \\ f_j \end{bmatrix} = \mathbf{m}^T \mathbf{f}$$

$$\beta = \frac{(x - \bar{x})}{\sigma_x}$$

$$\beta_w^2 = \frac{(\bar{f}_i - \bar{f}_j)^2}{\mathbf{m}^T \mathbf{C} \mathbf{m}} = \frac{(\bar{f}_i - \bar{f}_j)^2}{\sigma_i^2 - 2\sigma_i \rho_{i,j} \sigma_j + \sigma_j^2}$$



$$P(r = 1) = P(\beta < \beta_w) = \int_{-\infty}^{\beta_w} \frac{1}{\sqrt{2\pi}} \exp\left(-\frac{\beta^2}{2}\right) d\beta$$

Outline

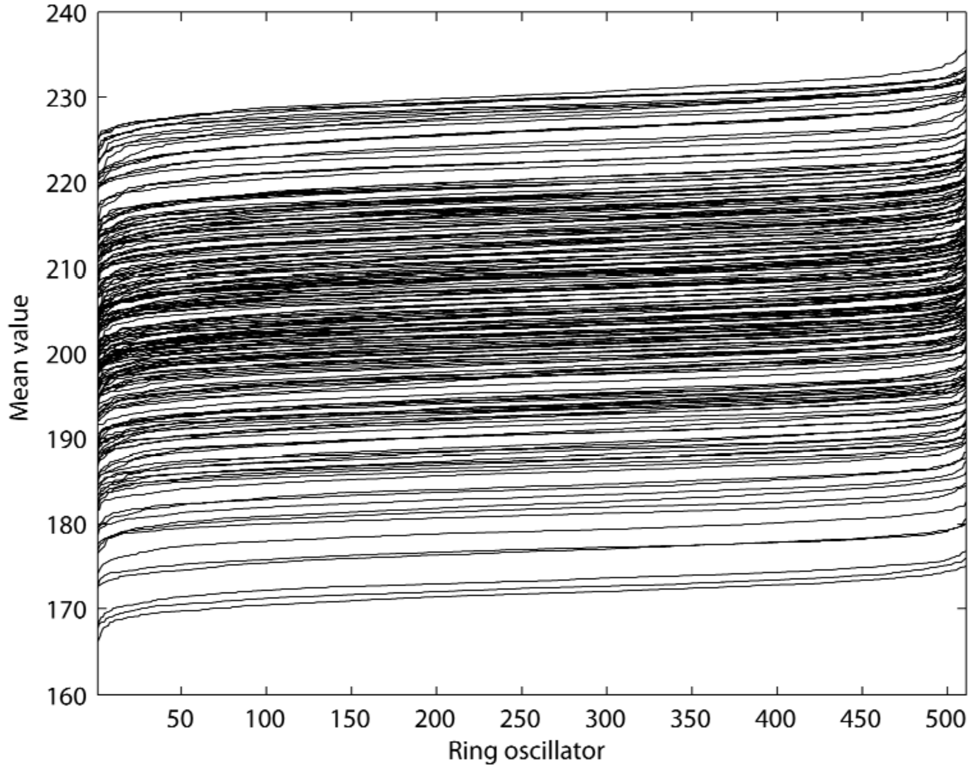
- Introduction to PUFs
- New Modeling Technique
- Empirical Results
- Conclusions

Empirical Data

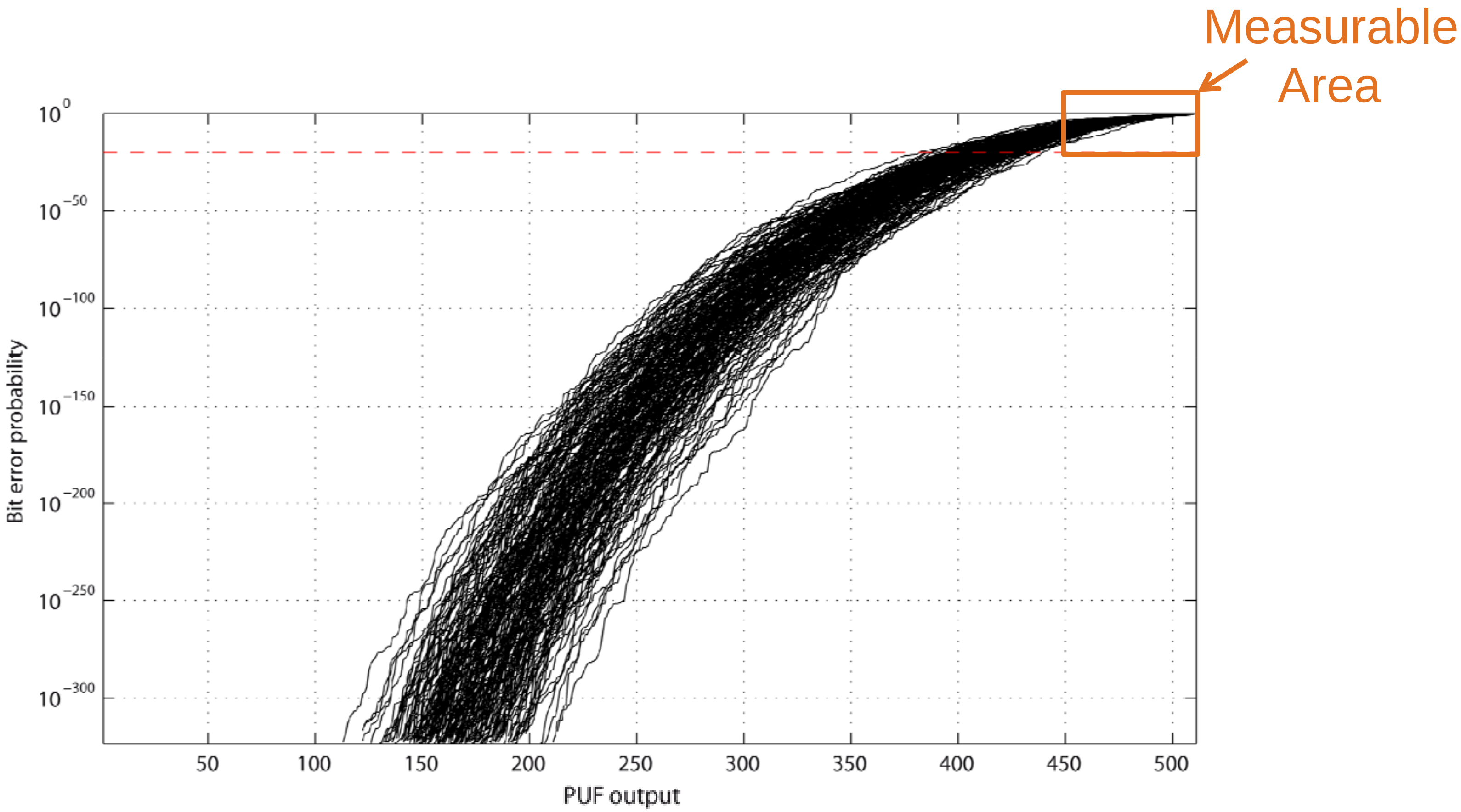
- Large scale case study at Virginia Tech in 2009
- Xilinx Spartan 3
- 193 FPGAs
- 512 ROs per FPGA
- 100 measurements per RO

http://rijndael.ece.vt.edu/puf

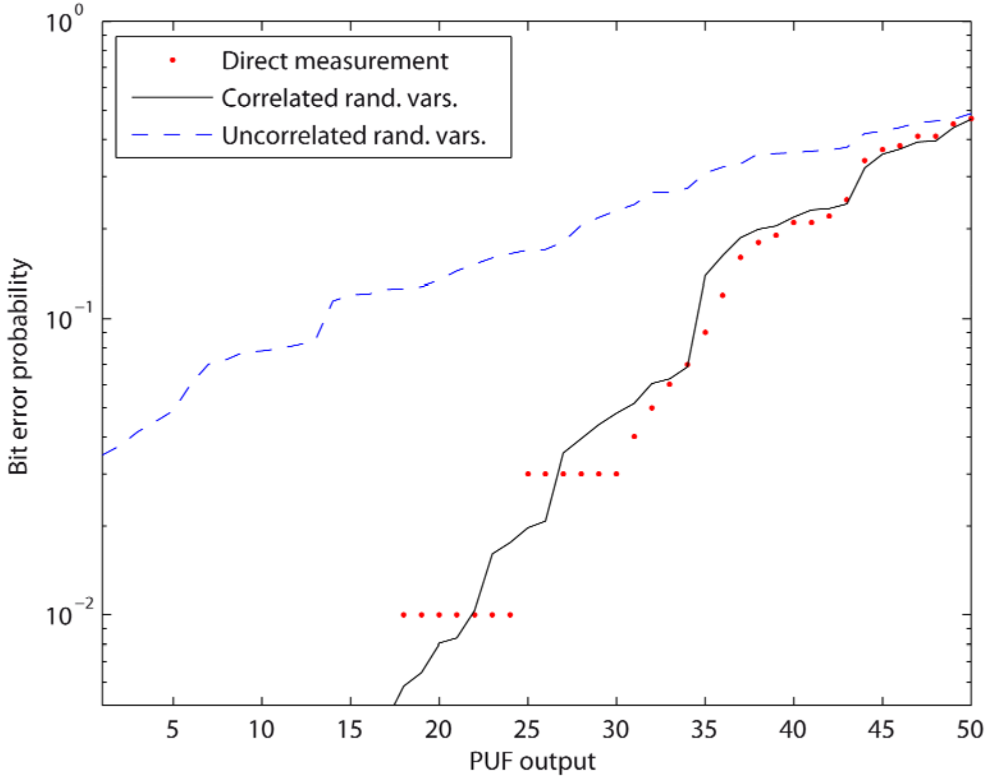
Frequency Distribution on FPGAs



Bit Error Probabilities with new Model



Validation of the Model



Conclusions

- Starting point:
  - Unknown bit error probability distribution
- New Model:
  - Correlated random variables
  - Estimation of entire bit error probability distribution
- Generalization:
  - Differential evaluation of physical measures for other PUF types (Voltage, Time, Resistance, Capacitance, …)

Lessons learned

- PUF measurements can be correlated, probably even under constant environmental conditions
- Theoretically founded demonstration that differential structures are useful
- RO PUF is a very reliable PUF
- New model as one step towards certification

Questions?