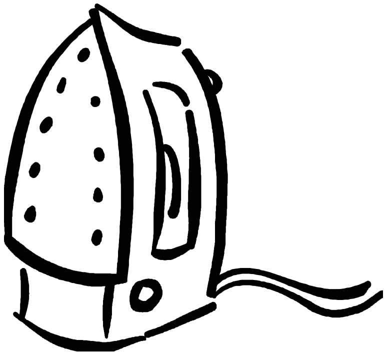
Engineering On-Chip Thermal ~~Attacks~~ Effects



Patrick Schaumont (ECE Dept, Virginia Tech)

Abhranil Maiti (ECE Dept, Virginia Tech)

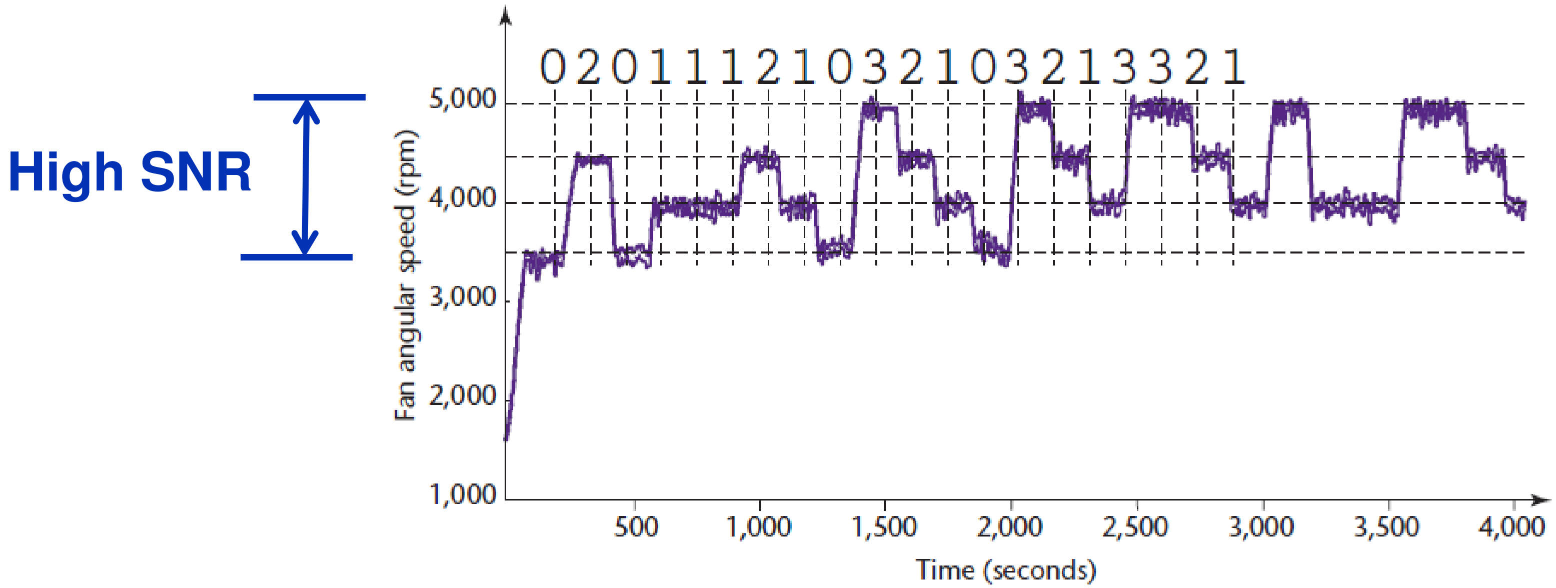
Zhimin Chen (ECE Dept, Virginia Tech)

Dagstuhl July 2009

Outline

- Thermal Covert Channel Filtering
  - On-chip heat generation and detection
  - Optimized detection using DSP
- Thermally indifferent PUF
  - Temperature Effects on PUF
  - Mitigating Temperature Effects
  - Area Optimized solution
- Measuring lots of (FPGA) chips ..

Covert Channel based on Heat



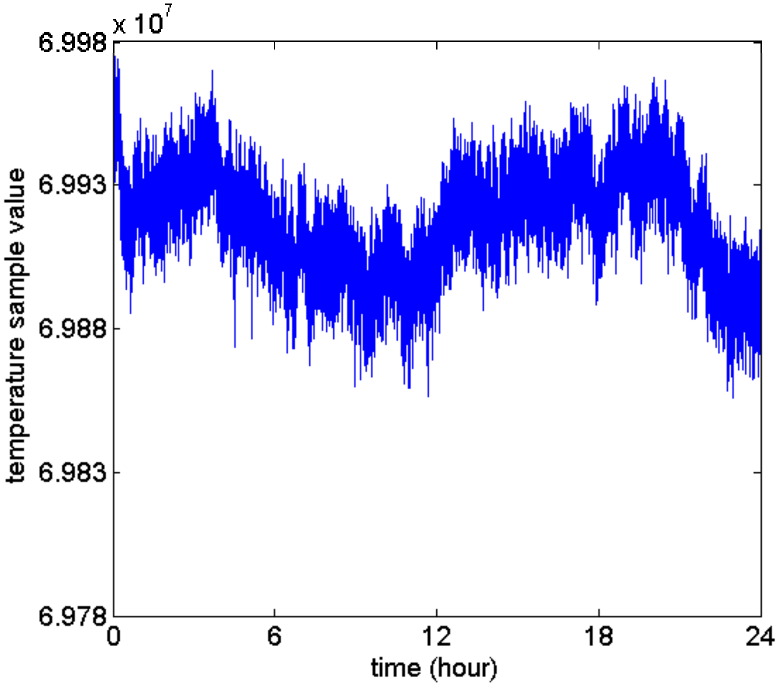
High SNR

Bandwidth ~ 0.0138 bps

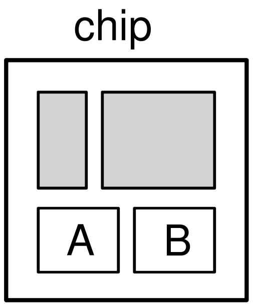
Brouchier, Kean, Marsh, Naccache, "Thermocommunication," ePrint IACR 2009/002

How *covert* can we make it?

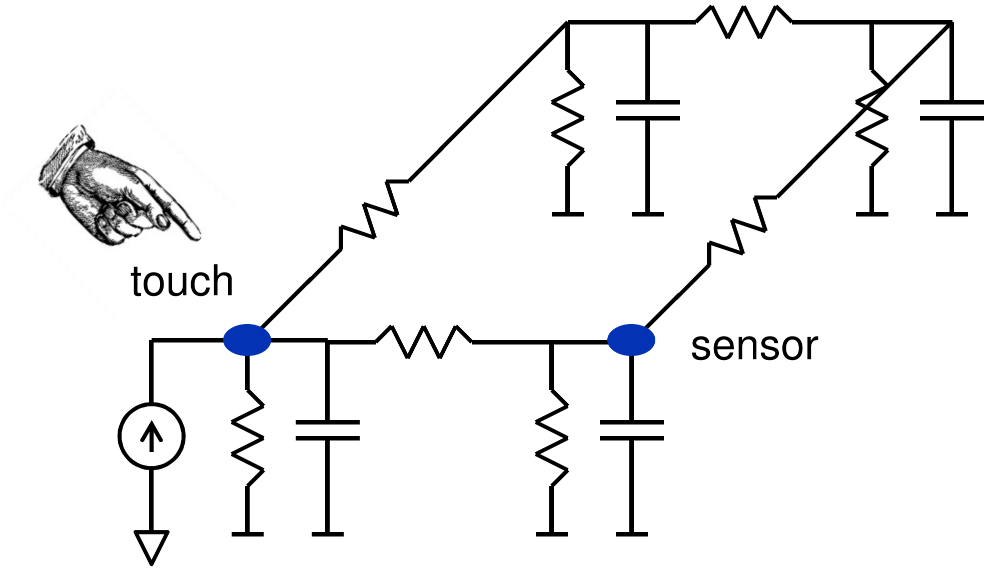
- **Temperature profile on an FPGA over 1 day**
  - **On-chip temperature measurement**
  - **We touched the FPGA package two times for a few seconds. Can you see when?**

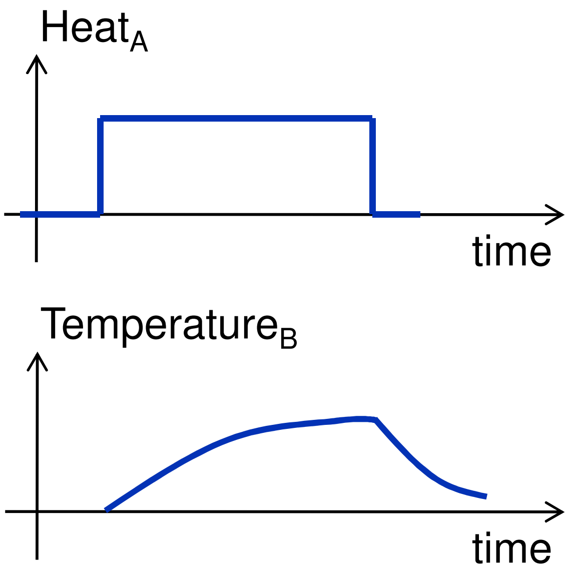


How touching a package affects T



Heat_A ⇨ Temperature_B

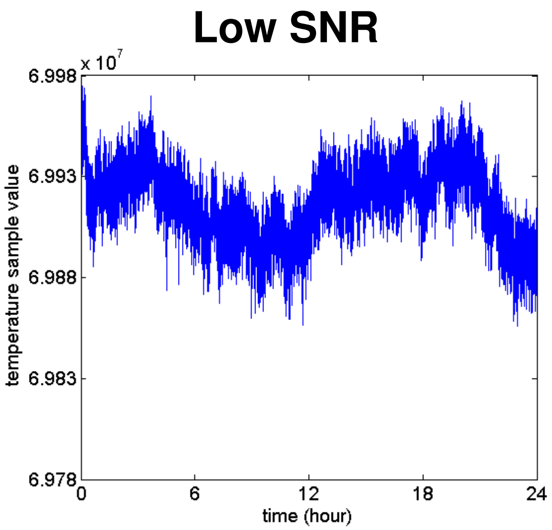


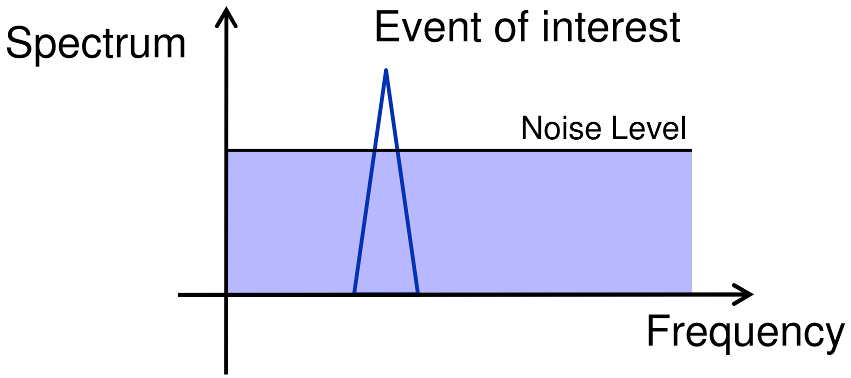


Pedram, Nazarian, "Thermal Modeling, Analysis, and Management in VLSI Circuits: Principles and Methods," Proc. IEEE, August 2006

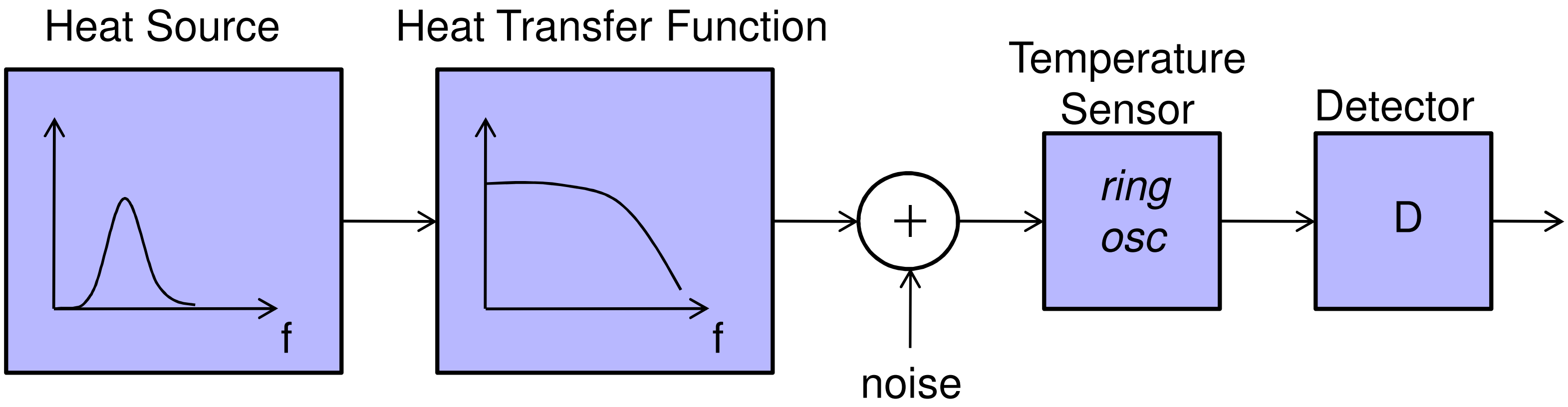
Can information be more covert?

- **Detecting Temperature *events* on an FPGA**
  - **SNR of 24-hour measurement is very poor**
  - **The energy in the event of interest if very small**
  - **But the event of interest may be band-limited !**



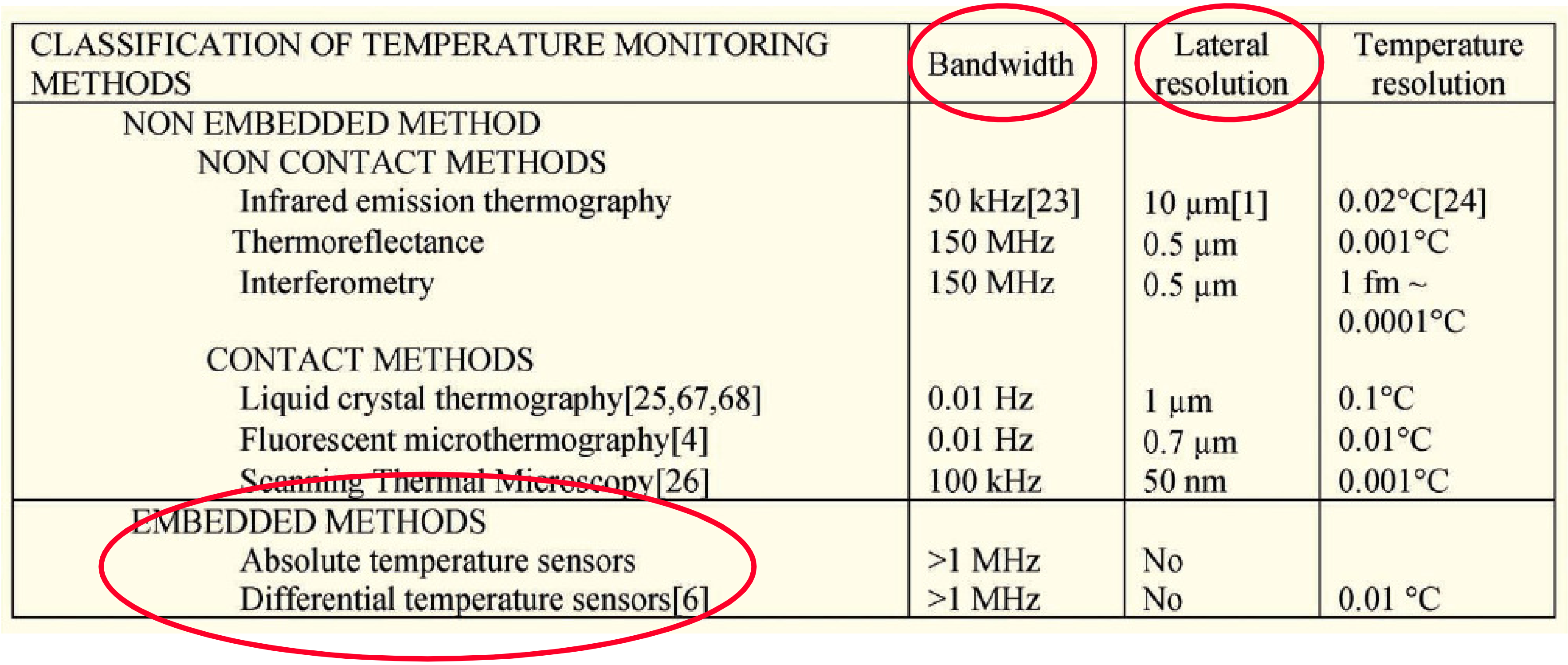


Our communications system



- **We need**
  - **A good sensor: sensitive, high bandwidth**
  - **A good detector**

Bandwidth and Resolution of Sensors

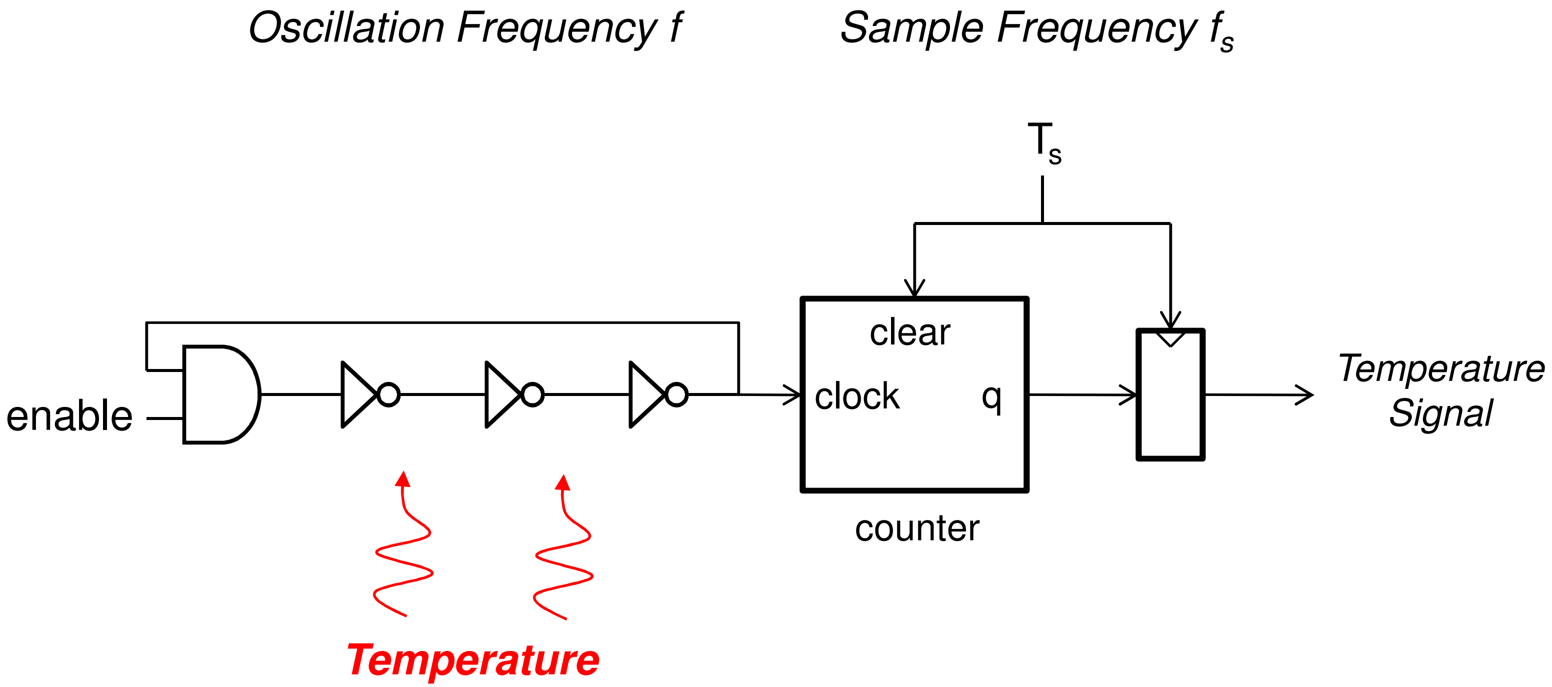


CLASSIFICATION OF TEMPERATURE MONITORING METHODS	Bandwidth	Lateral resolution	Temperature resolution
NON EMBEDDED METHOD			
NON CONTACT METHODS			
Infrared emission thermography	50 kHz[23]	10 µm[1]	0.02°C[24]
Thermoreflectance	150 MHz	0.5 µm	0.001°C
Interferometry	150 MHz	0.5 µm	1 fm ~ 0.0001°C
CONTACT METHODS			
Liquid crystal thermography[25,67,68]	0.01 Hz	1 µm	0.1°C
Fluorescent microthermography[4]	0.01 Hz	0.7 µm	0.01°C
Scanning Thermal Microscopy[26]	100 kHz	50 nm	0.001°C
EMBEDDED METHODS			
Absolute temperature sensors	>1 MHz	No	
Differential temperature sensors[6]	>1 MHz	No	0.01 °C

Altet, Claeys, Dilhaire, Rubio, "Dynamic Surface Temperature Measurements in ICs," Proc. IEEE, August 2006.

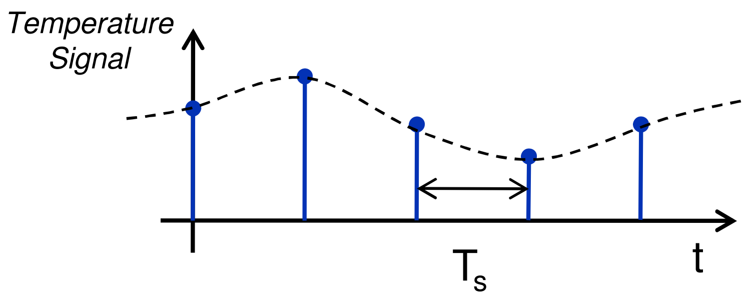
Ring-oscillator based Thermal Sensor

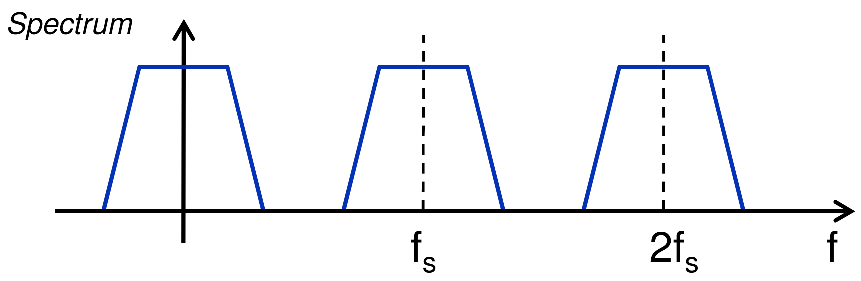
- **Sample a Free-running Ring Oscillator**



Ring-oscillator based Thermal Sensor

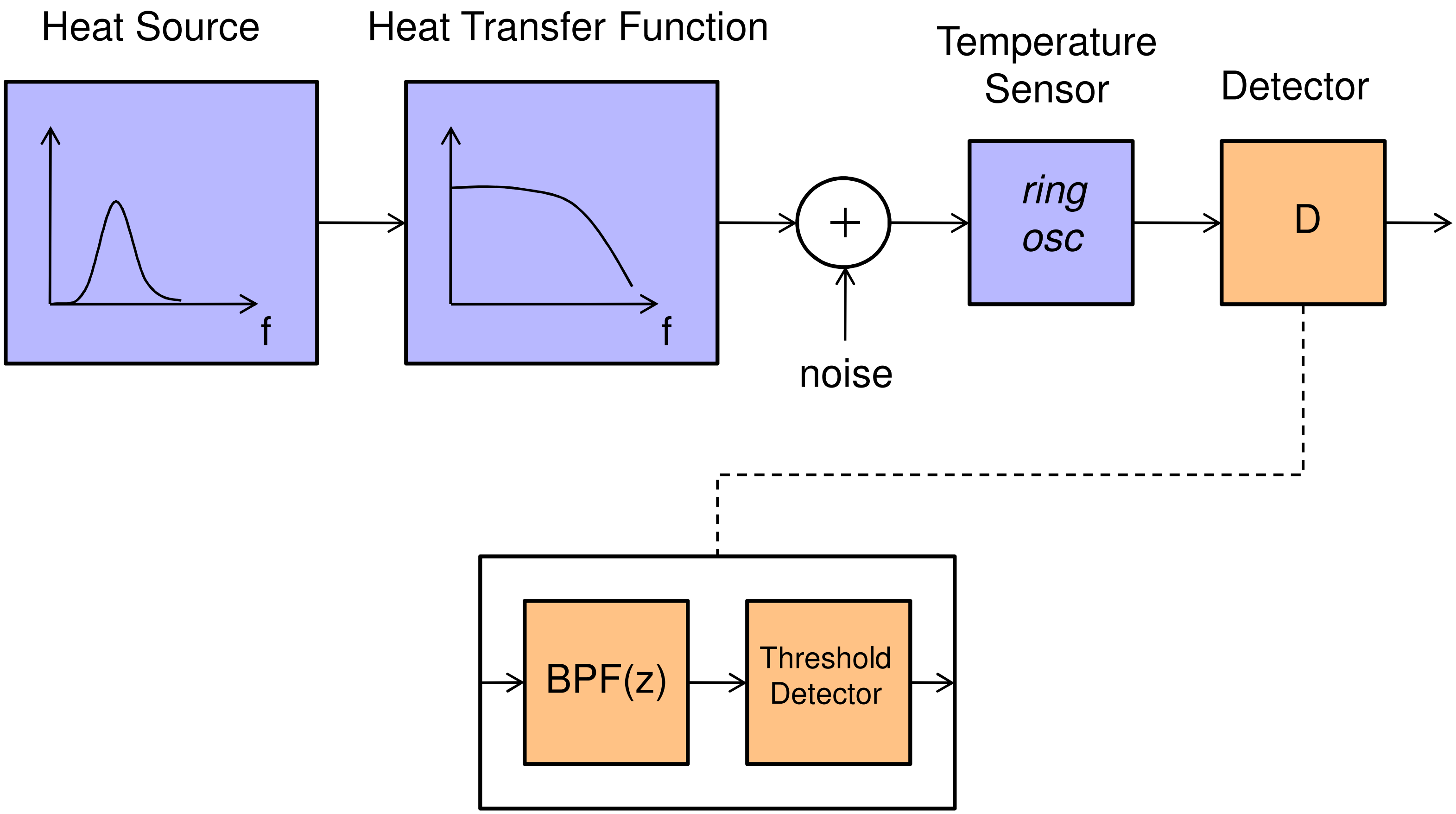
- **How good is this structure in detecting temperature *variations*?**



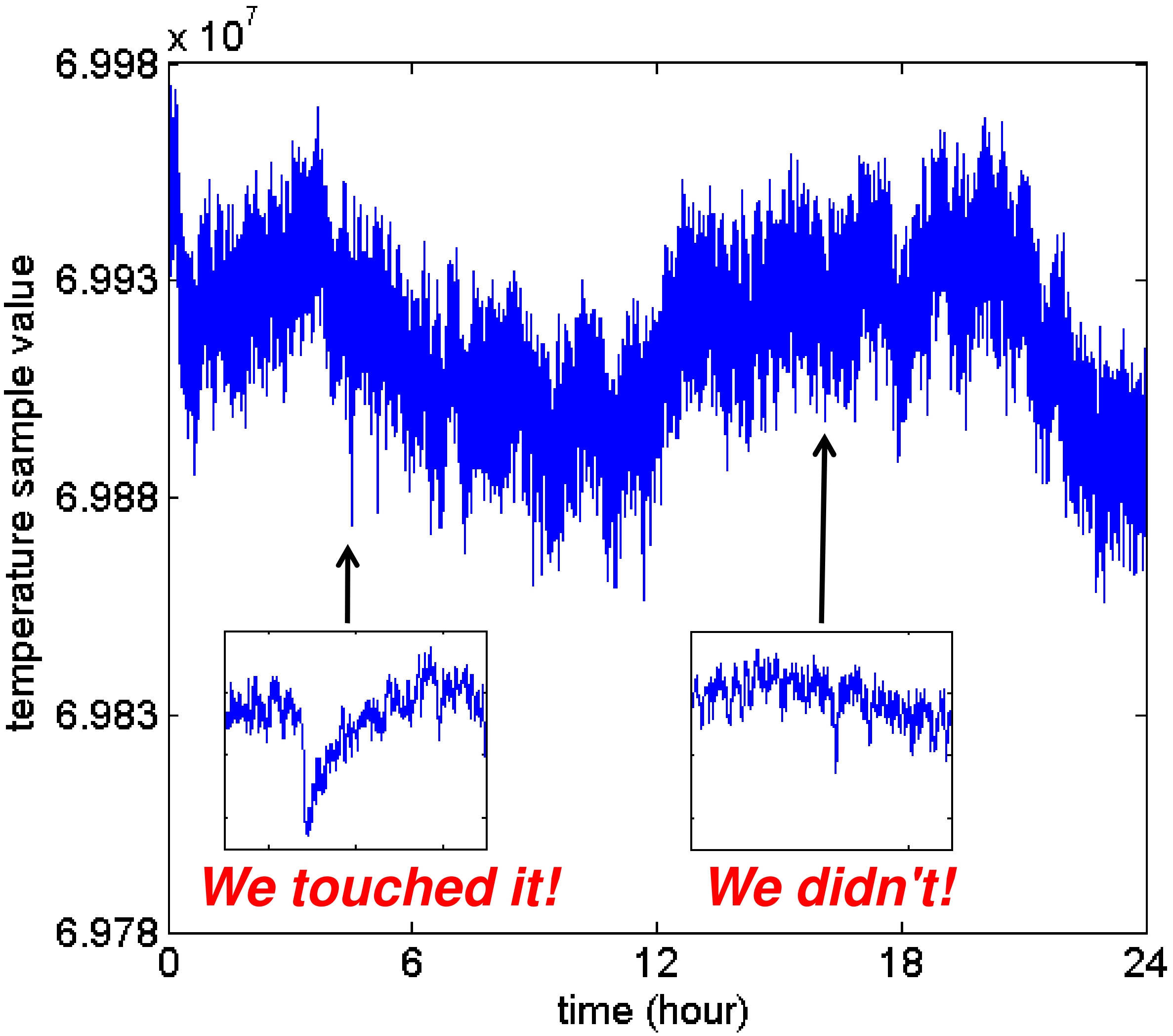


- **Detection bandwidth is limited by $f_s/2$**
- **However, a high f_s is not ideal either**
  - **Processing load**
- **Digital RO cannot be alias-free**

Our communications system

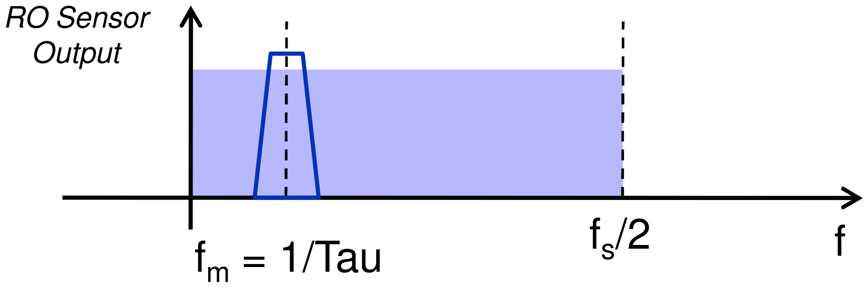


Select band based on expected signal



Tau ~ 20s

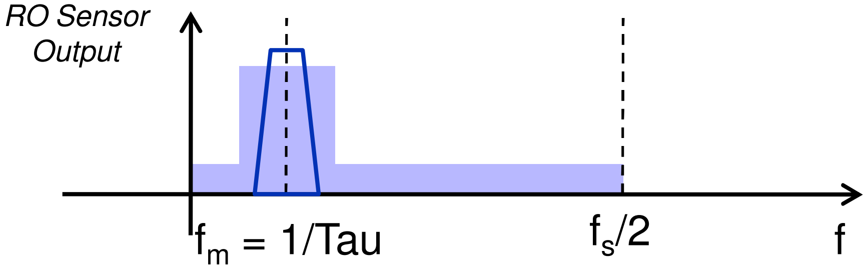
Select band based on expected signal



$$LPF(z) = 1 + z^{-1} + z^{-2} + .. + z^{-k}$$

$$HPF(z) = 1 - 2\,z^{-k} + z^{-2k}$$

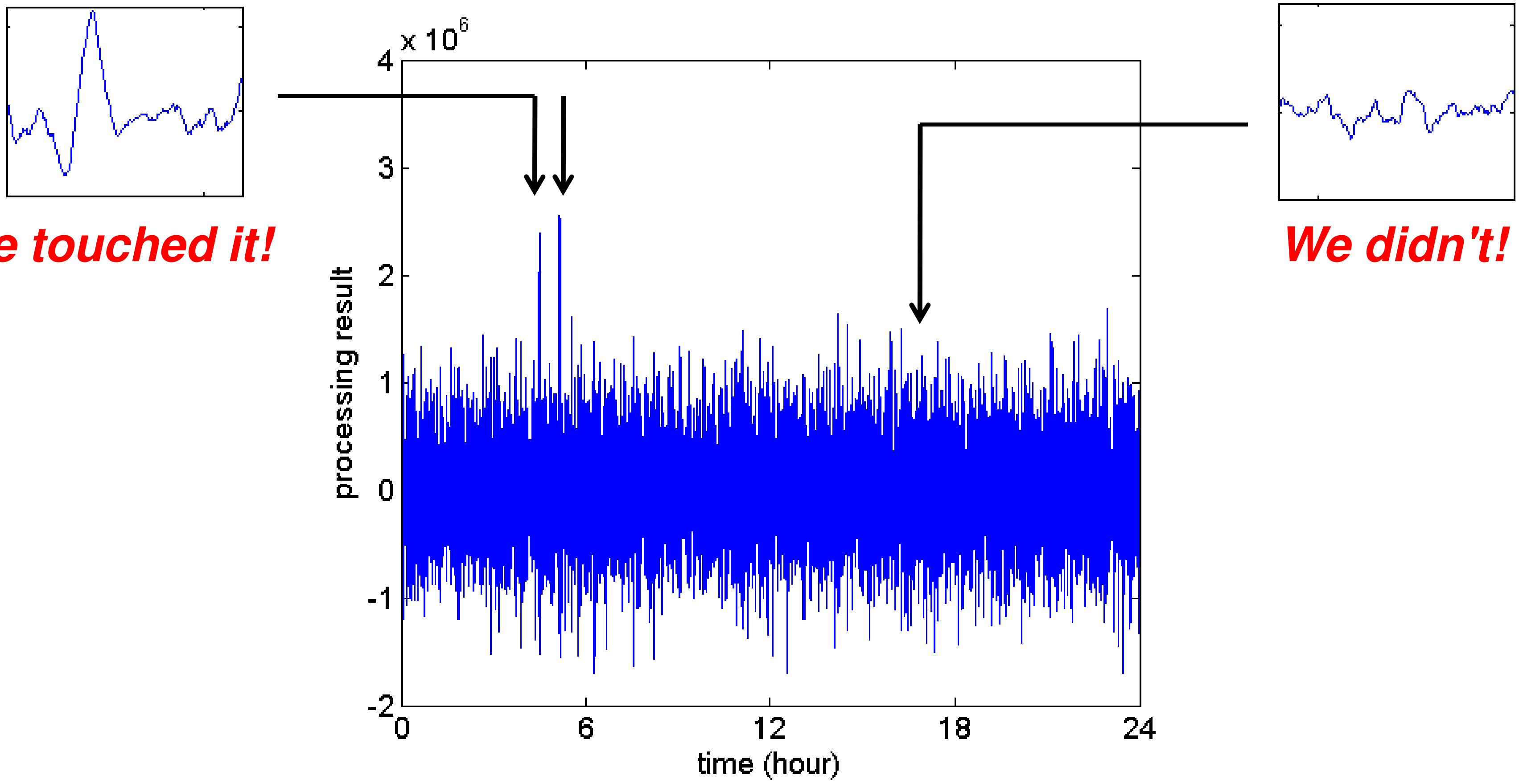
$$k = f_s \,/\, 2 \,/\, f_m$$



f_s = 3Hz
f_m = 0.05Hz
k = 30

Picoblaze
(8-bit uC)

After Filtering



We touched it!

We didn't!

Remember

1. **Suitable filtering based on DSP drastically increases sensitivity**

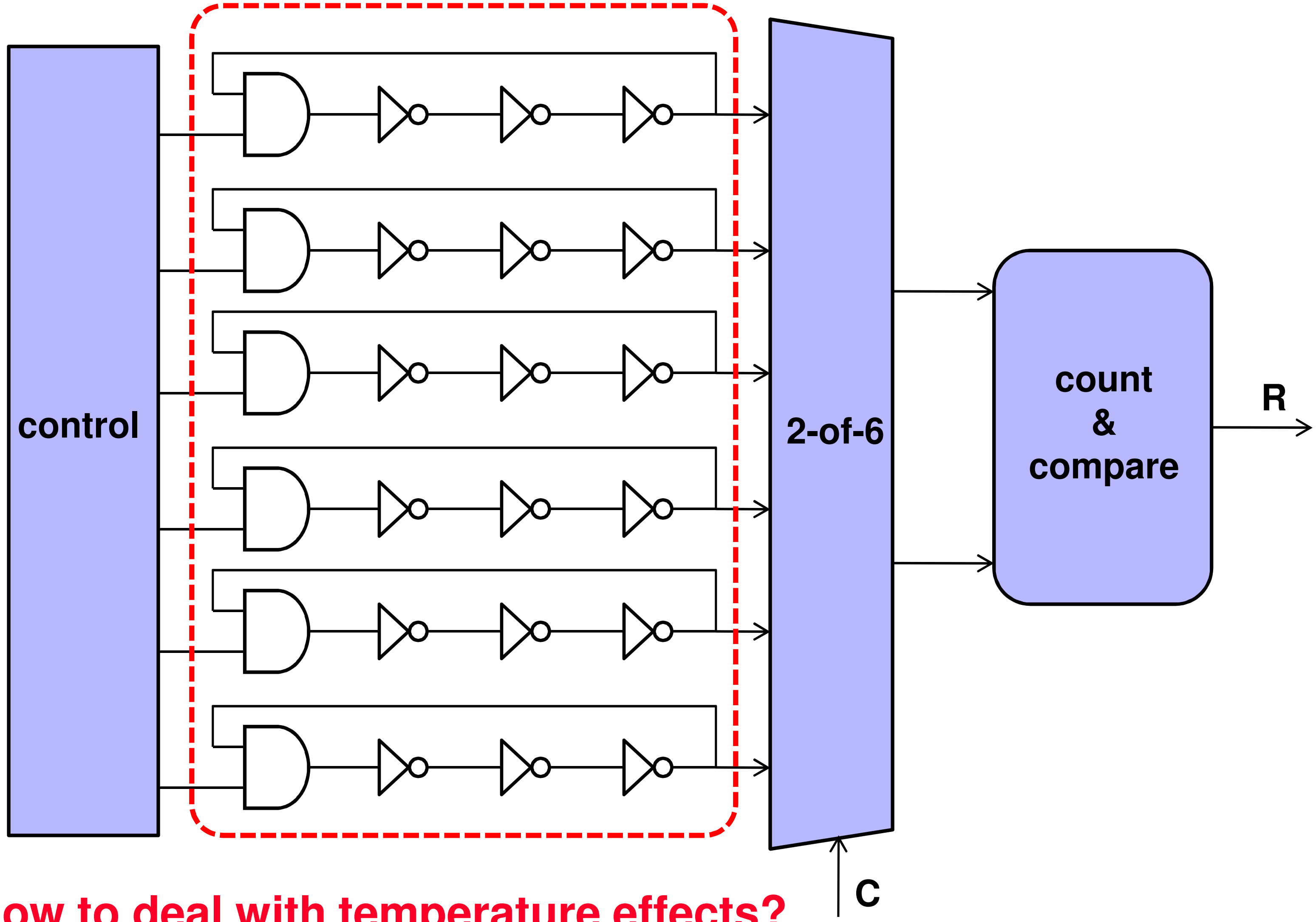
2. **Chip Temperature Sensors can have a high bandwidth (~MHz)**

   (Open issue: how well can this be exploited with simple on-chip sensors?)
   or:
   (Can thermal sensors be used for side-channel analysis as well?)

Outline

- Thermal Covert Channel Filtering
  - On-chip heat generation and detection
  - Optimized detection using DSP
- Thermally indifferent PUF
  - Temperature Effects on PUF
  - Mitigating Temperature Effects
  - Area Optimized solution
- Measuring lots of (FPGA) chips ..

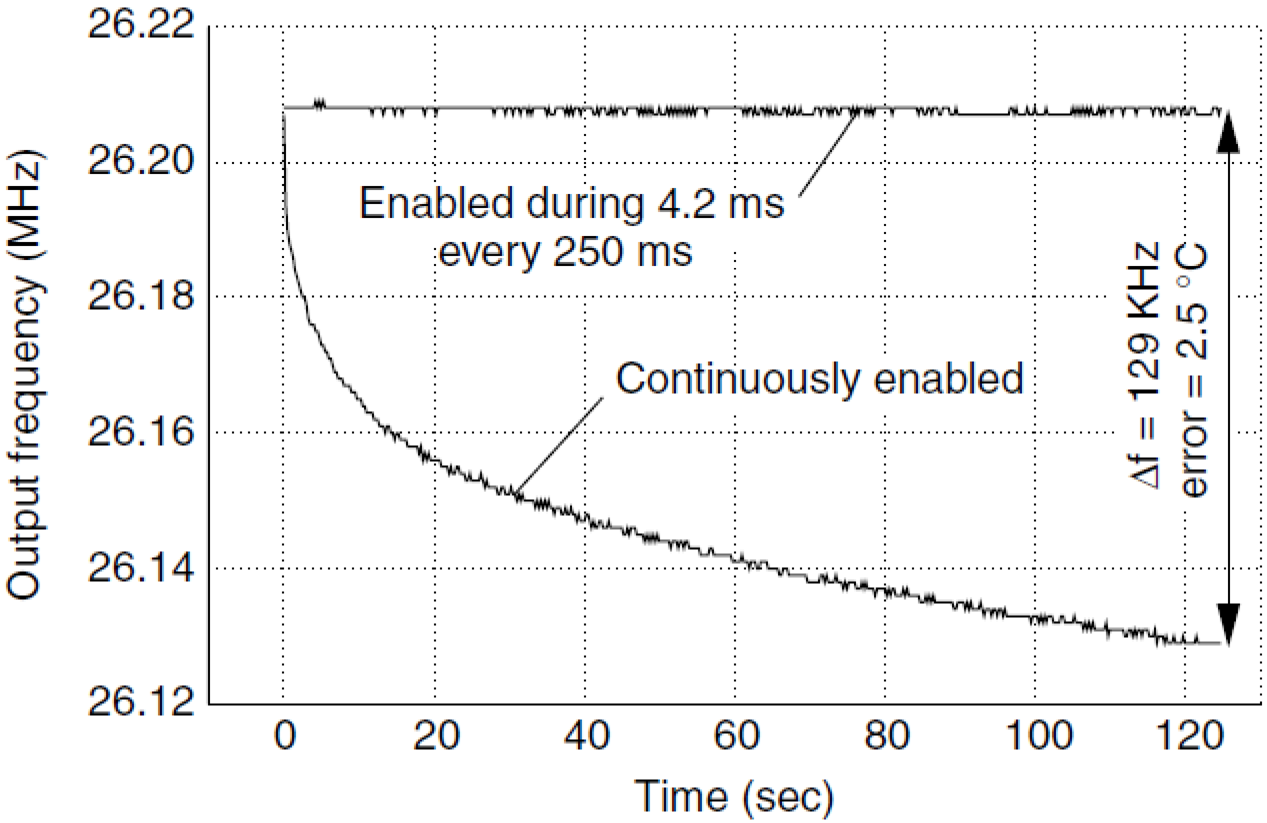
RO-based PUF



How to deal with temperature effects?

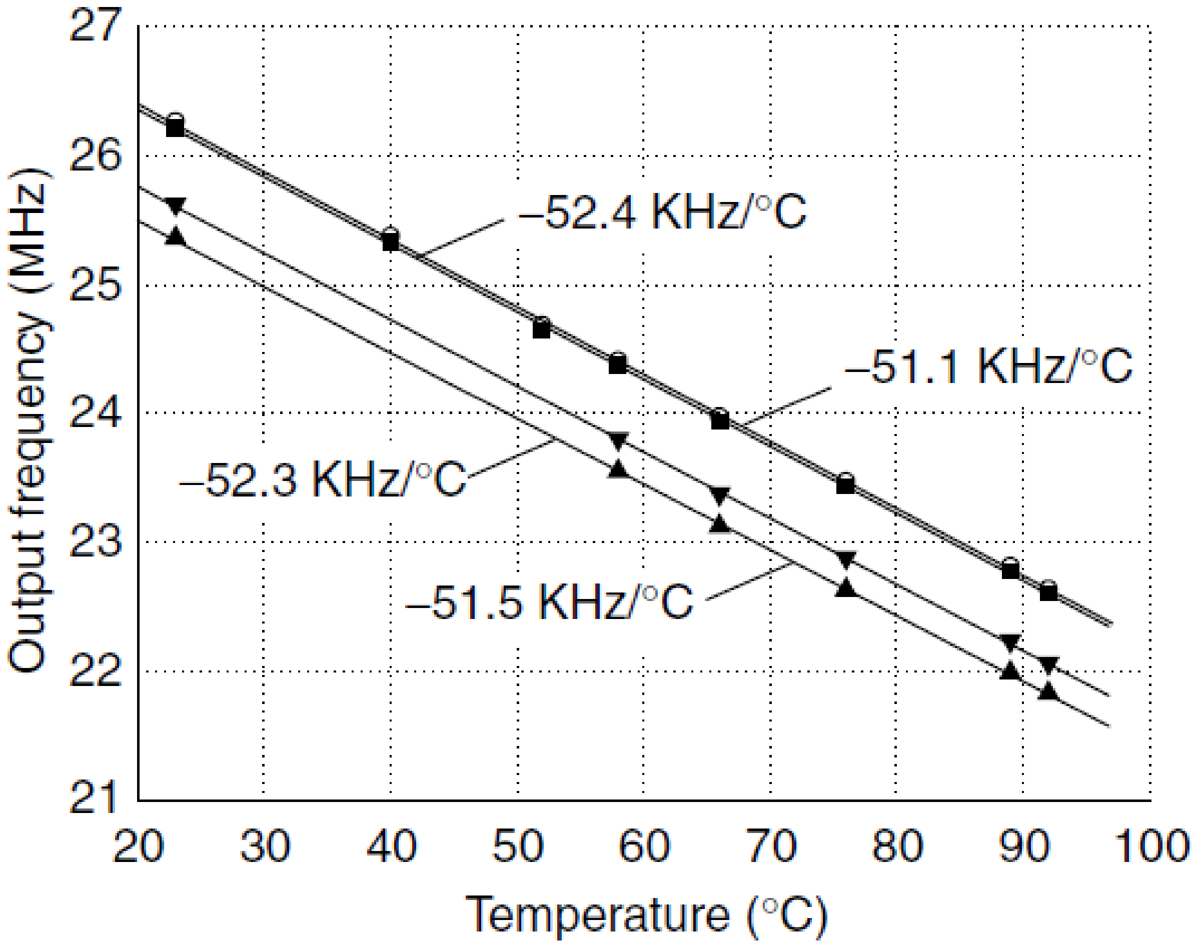
Self-Heating

- **Ensure RO's use low duty factor**



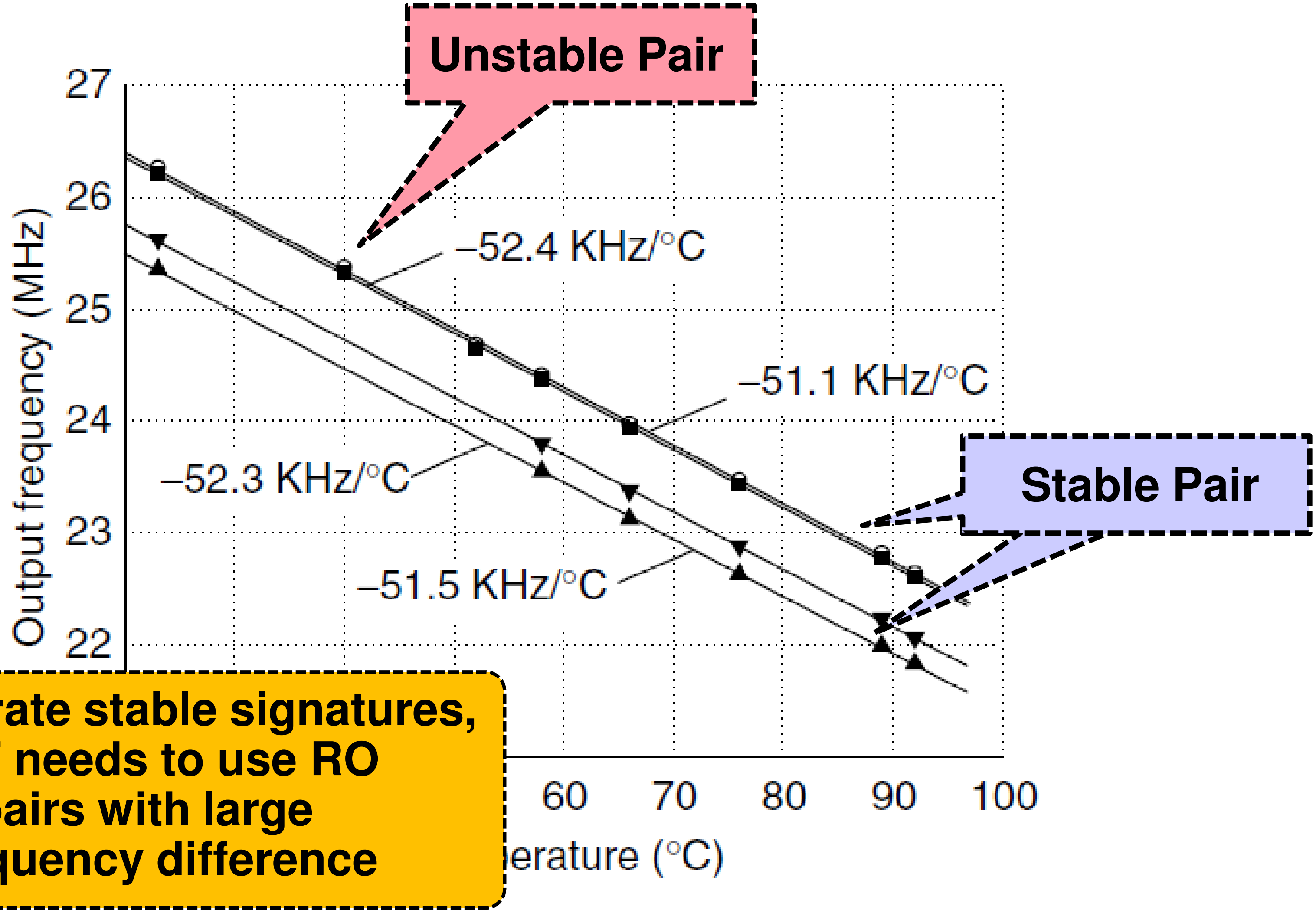
S. Lopez-Buedo et al, "Thermal Testing on Reconfigurable Computers," IEEE Design and Test, 4-11, Jan-Mar 2000.

Temperature Dependence



S. Lopez-Buedo et al, "Thermal Testing on Reconfigurable Computers," IEEE Design and Test, Jan-Mar 2000.

Temperature Dependence



Unstable Pair

Stable Pair

To generate stable signatures, PUF needs to use RO pairs with large frequency difference

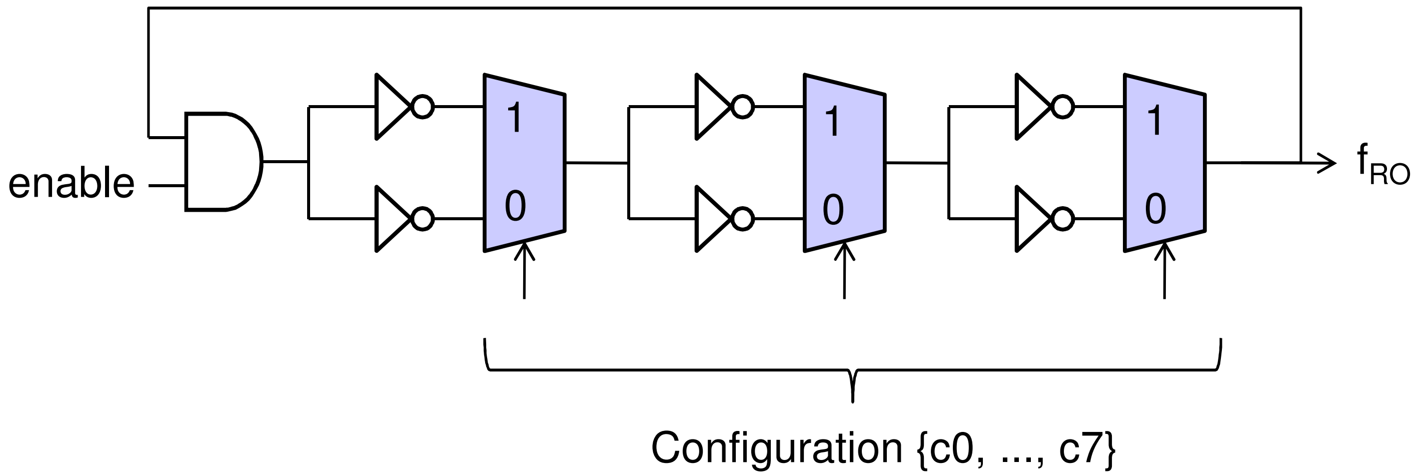
S. Lopez-Buedo et al, "Thermal Testing on Reconfigurable Computers," IEEE Design and Test, Jan-Mar 2000.

Brute-forcing stability

- Instead of comparing a pair of RO, consider a *group* of RO
  - Use only the maximum or minimum f [Suh 2007]
- This reduces the useful C/R space
- In turn, this leads to larger PUFs (more RO's), higher cost

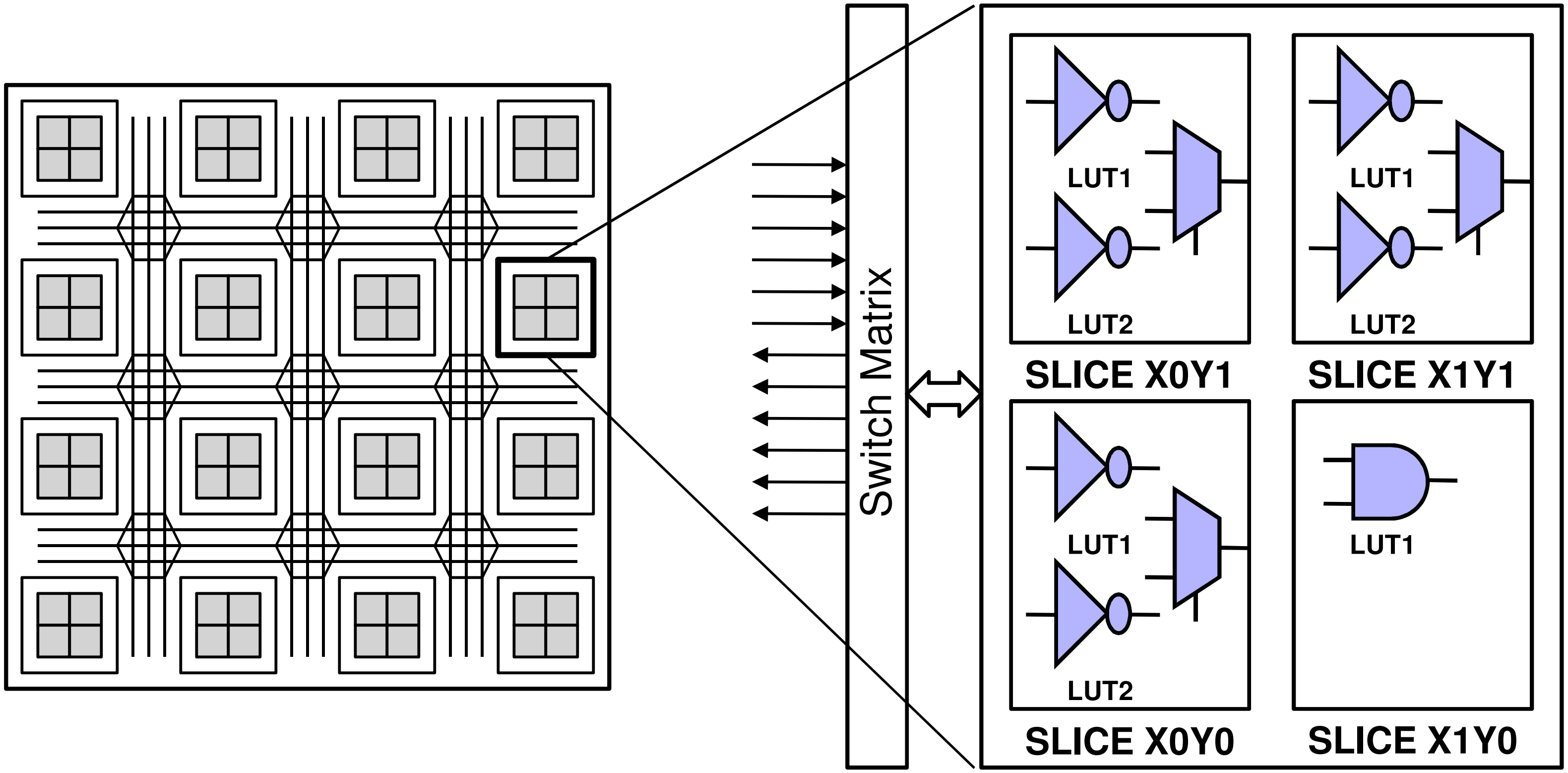
Compact, stable RO

- **Configurable Ring Oscillator**

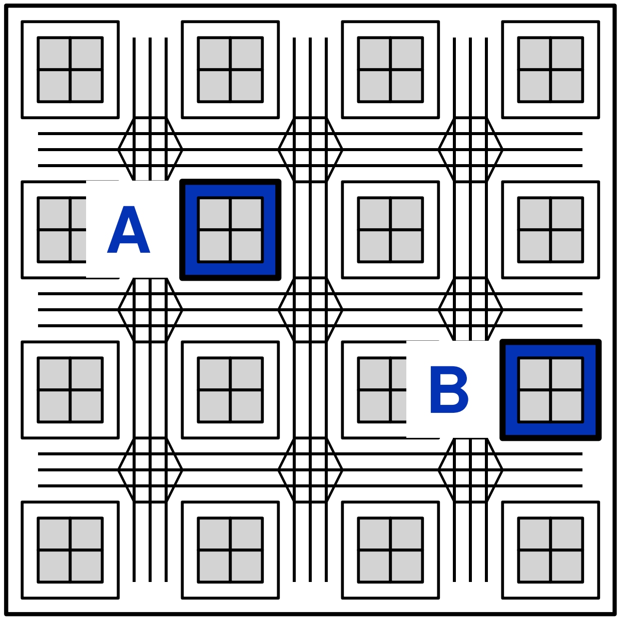


8 RO for the price of one

- **Configurable Ring Oscillator**
  - **Fits in a single CLB, uses only local routing**
  - **Reproducible macrocell**



Selecting the Configuration



- **Tuning**:

  a/ Apply each configuration {c0, .., c7} to A *and* B (this removes all dependencies on routing)

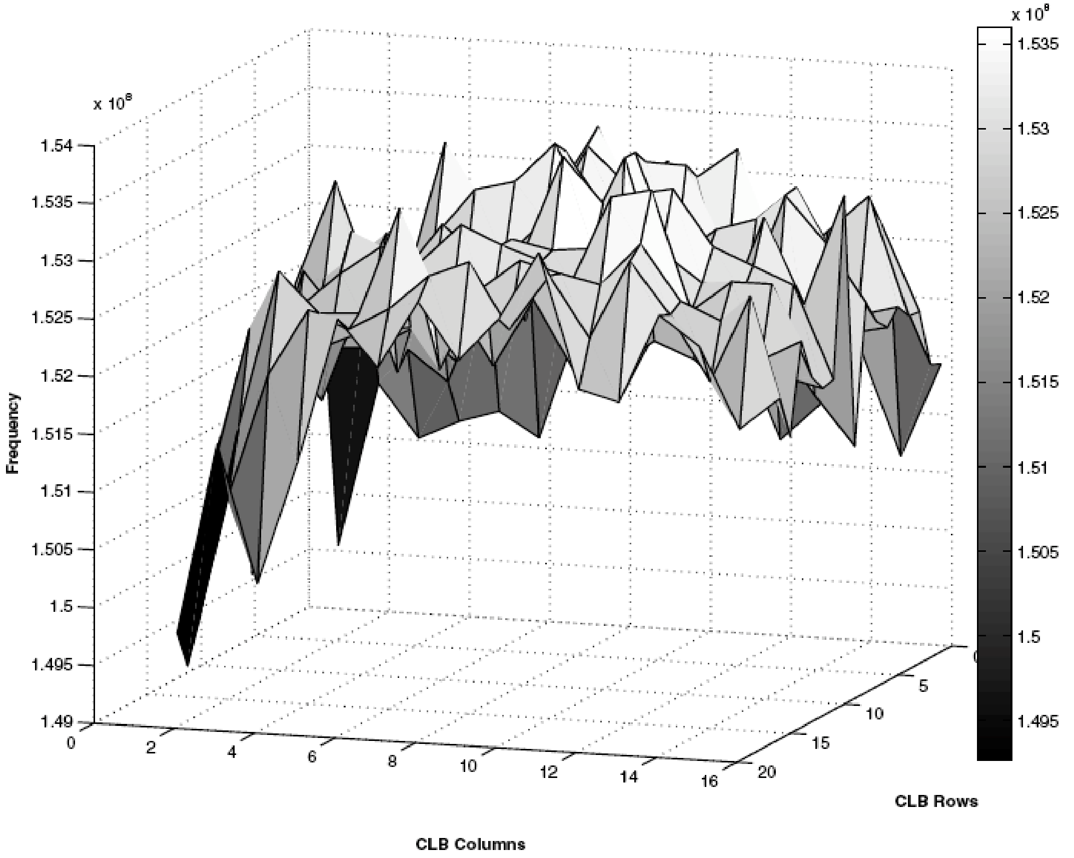
  b/ Determine and store the configuration g(A,B)=j for which maximum absolute frequency difference is obtained

- **Usage**:

  Each time pair A, B is compared, select configuration j

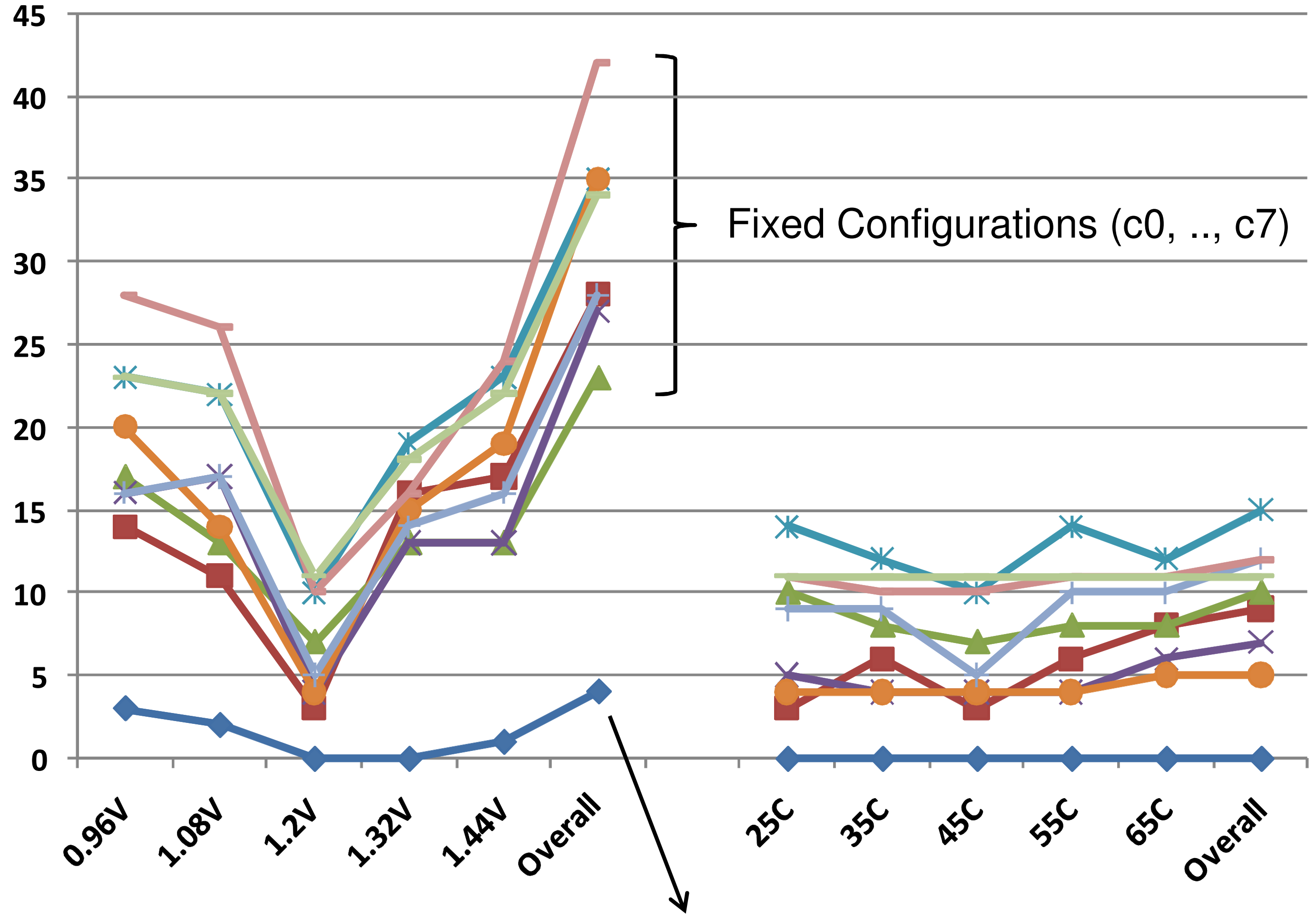
C/R Strategy for 128 RO

- **Fixed C:**
  - **Pairwise comparison of adjacent RO pairs**
  - **Compensate for correlated effects**



Measurements on 128-RO PUF

Unstable bits



Fixed Configurations (c0, .., c7)

Optimized Configuration

Remember

1. **Architecture Optimization can simultaneously address PUF stability and resource cost**

2. **Increasing PUF stability will simplify post-processing (*helper data processing*)**

Outline

- **Thermal Covert Channel Filtering**
  - **On-chip heat generation and detection**
  - **Optimized detection using DSP**
- **Thermally indifferent PUF**
  - **Temperature Effects on PUF**
  - **Mitigating Temperature Effects**
  - **Area Optimized solution**
- **Measuring lots of (FPGA) chips ..**

Recent PUF work

- **Hard to get PUF performance data for large populations (> 100 chips)**

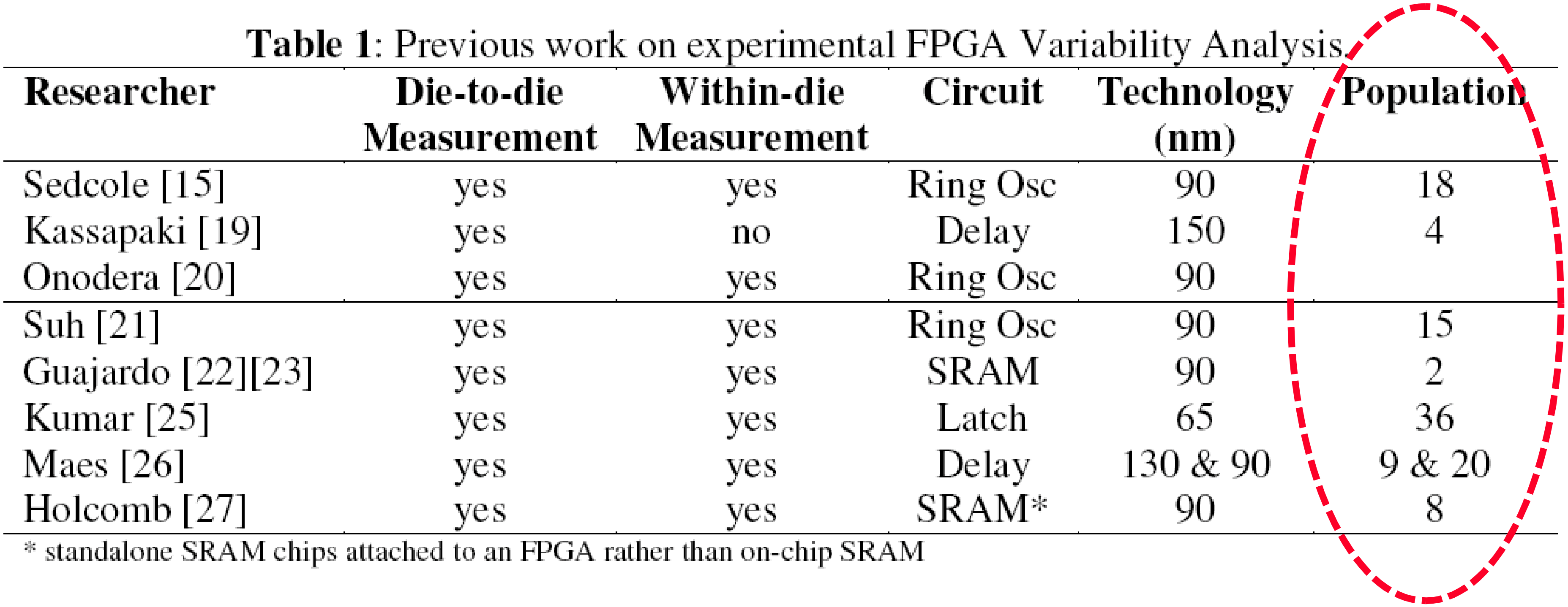


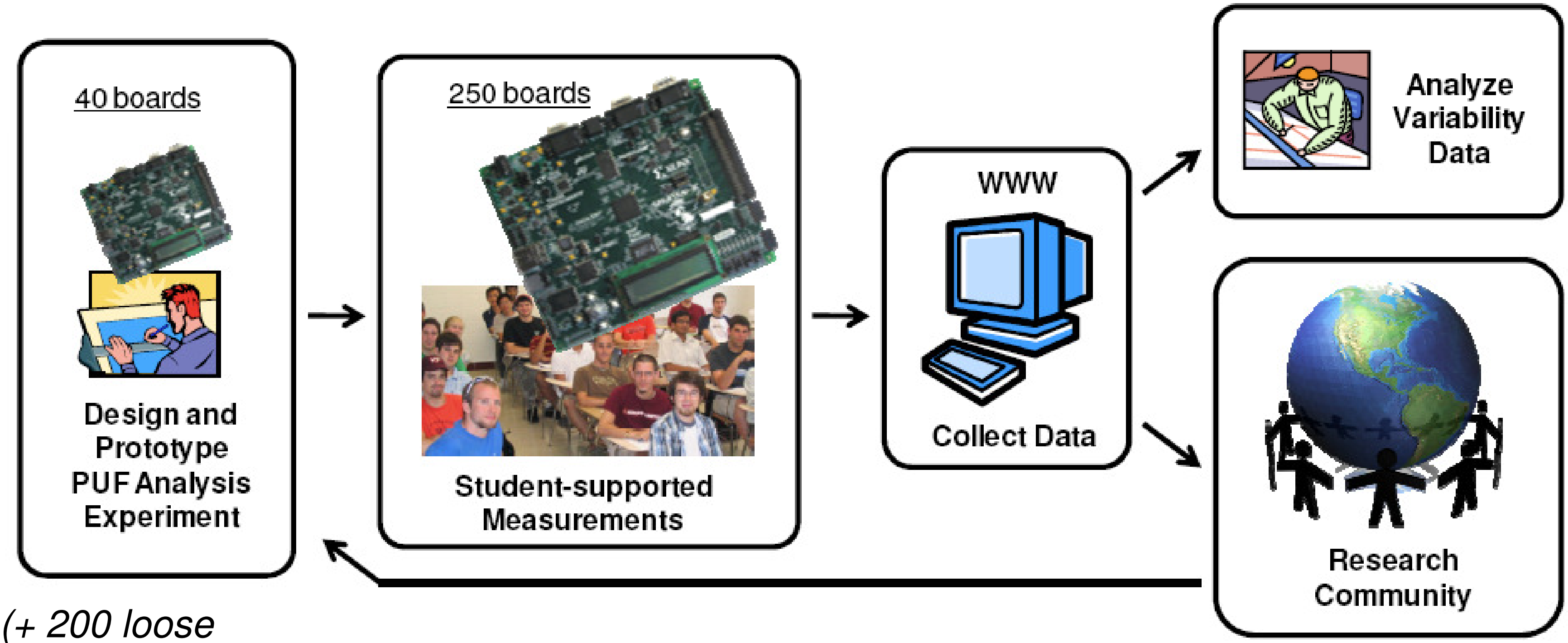
Table 1: Previous work on experimental FPGA Variability Analysis.

Researcher	Die-to-die Measurement	Within-die Measurement	Circuit	Technology (nm)	Population
Sedcole [15]	yes	yes	Ring Osc	90	18
Kassapaki [19]	yes	no	Delay	150	4
Onodera [20]	yes	yes	Ring Osc	90	
Suh [21]	yes	yes	Ring Osc	90	15
Guajardo [22][23]	yes	yes	SRAM	90	2
Kumar [25]	yes	yes	Latch	65	36
Maes [26]	yes	yes	Delay	130 & 90	9 & 20
Holcomb [27]	yes	yes	SRAM*	90	8

* standalone SRAM chips attached to an FPGA rather than on-chip SRAM

NSF Project

- ***Infrastructure to collect and analyze circuit variability in FPGAs***



40 boards

Design and Prototype PUF Analysis Experiment

250 boards

Student-supported Measurements

WWW

Collect Data

Analyze Variability Data

Research Community

(+ 200 loose XCV1000 FPGAs)