Silicon Physical Random Functions

Blaise Gassend, Dwaine Clarke, Marten van Dijk and Srinivas Devadas
Massachusetts Institute of Technology
Laboratory for Computer Science
Cambridge, MA 02139, USA

CCS 2002

presented by Fabian Schläfli

Identification vs Authentication

- Identification
  - the process of providing a system with your identity
- Authentication
  - the process of verifying that the claimed identity is correct

Identification:

Authentication:

Overview

- Executive Summary
- Problem, Goal & Background
- Key Approach and Ideas
- Novelty
- Mechanisms
- Key Results
- Summary
- Strengths and Weaknesses
- Takeaways
- Research history
- Discussion

Executive Summary

- **Problem:** providing authentication for an Integrated Circuit (IC) is difficult, expensive and insecure
- **Goal:** provide a method that provides authentication for ICs that is inexpensive, reliable and secure
- **Method:** implement a circuit that gives characteristic responses for each IC and that is hard to predict
- **Result:** secure authentication that is reliable even under varying environmental conditions

Overview

- Executive Summary
- Problem, Goal & Background
- Key Approach and Ideas
- Novelty
- Mechanisms
- Key Results
- Summary
- Strengths and Weaknesses
- Takeaways
- Research history
- Discussion

Problem

- There are different applications which require identifying and authenticating an IC
  - e.g. smartcard

image source: https://www.vtg.admin.ch/de/service/info_trp/smartcard.html

Problem

- There are different applications which require identifying and authenticating an IC
  - e.g. smartcard

- Available methods involved embedding a unique secret key on the IC
  - to provide authentication these ICs have to be made resistant to attacks that attempt to discover the key
    - manufacturing such ICs is expensive and difficult
  - numerous attacks against such ICs are known
    - e.g. opening the IC and removing layers to analyze it

image source (SIM card): https://technology.inquirer.net/75833/house-oks-bill-sim-card-registration-final-reading
image source (credit card): https://www.viseca.ch/de/kreditkarten

Goal

- Provide a method to identify and authenticate an IC such that:
  - the method is **inexpensive**
  - the method is **fast** and **easy** to evaluate
  - the authentication **works reliably** even under varying environmental conditions
  - the authentication is **secure** against both invasive and non-invasive attacks

Background

- Manufacturing process variations
  - mask variations
  - temperature variations
  - pressure variations

- The magnitude of delay variation due to random variations can be 5% or more

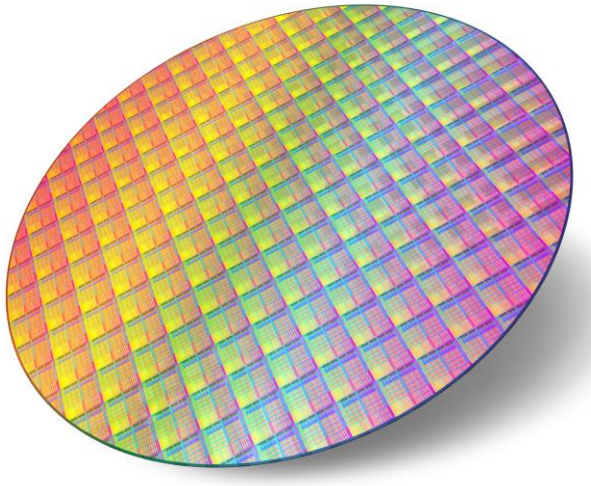


image source: https://www.waferworld.com/silicon-wafer-processing-process/

Overview

- Executive Summary
- Problem, Goal & Background
- Key Approach and Ideas
- Novelty
- Mechanisms
- Key Results
- Summary
- Strengths and Weaknesses
- Takeaways
- Research history
- Discussion

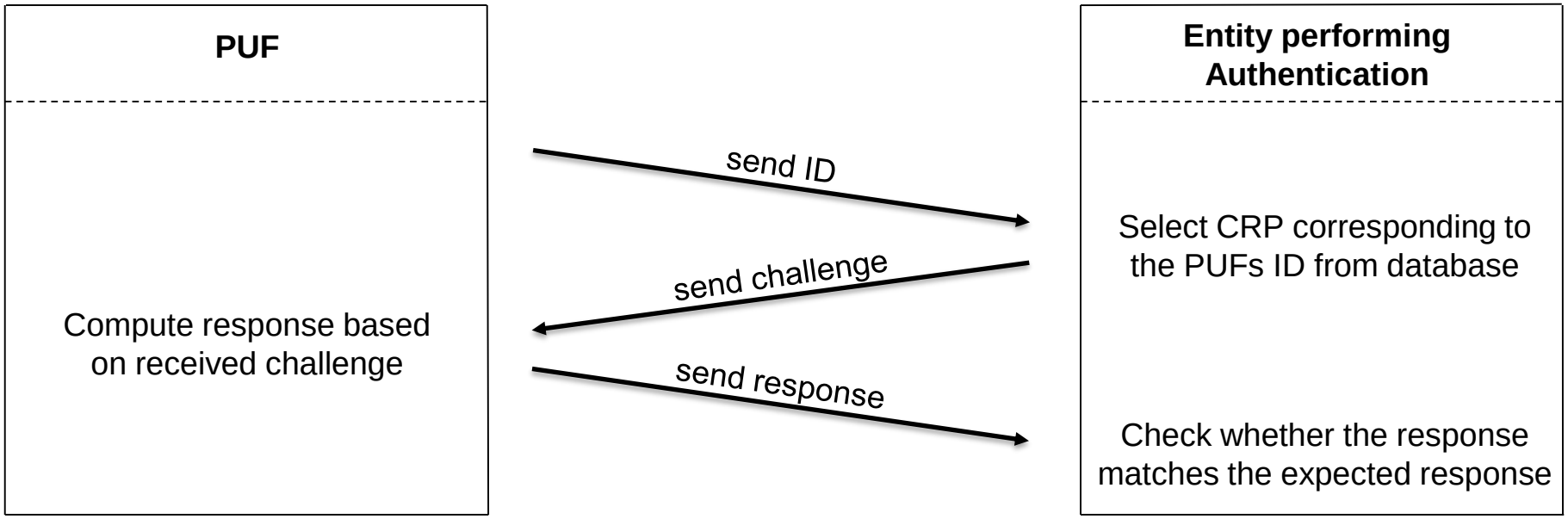
Key Approach and Ideas

- Authenticate an IC by implementing a function that returns unpredictably different output on different ICs

- Physical Unclonable Function (PUF)
  - also called: Physical Random Function
  - function that maps challenges to responses
    - challenge response pair (CRP)
  - physical function which returns different responses to the same challenge on different devices
  - "digital fingerprint" of the device
  - easy to evaluate
  - hard to characterize

Key Approach and Ideas: Authentication

- The entity performing the authentication has to:
  - analyze each PUF after production
  - store characteristic CRPs in a database for each PUF



Key Approach and Ideas: Building a PUF

- Use the delay variations that result from the manufacturing process variations to build a PUF
  - **fast** to evaluate
  - provides a **high level of security**
  - **inexpensive** to produce
  - requires **no secure packaging**
- Build a circuit that has a variable delay from device to device
- Measure the delay when applying a given input and return a value depending on the delay as response
- Return delay ratio rather than just the delay to provide reliability against environmental variations

Overview

- Executive Summary
- Problem, Goal & Background
- Key Approach and Ideas
- Novelty
- Mechanisms
- Key Results
- Summary
- Strengths and Weaknesses
- Takeaways
- Research history
- Discussion

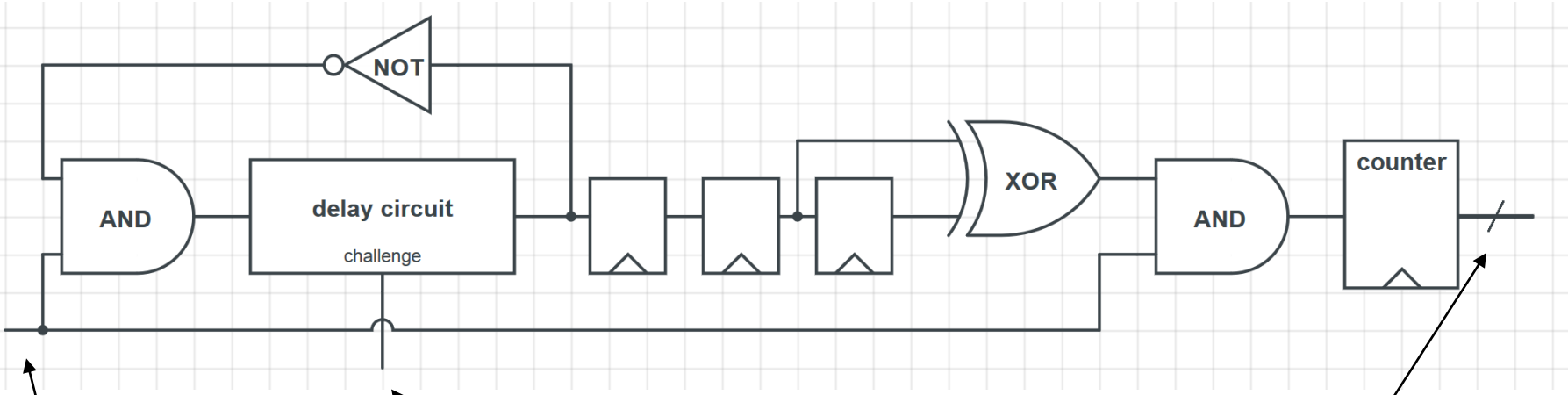
Novelty

- Eliminate the need to embed a secret key for authentication
  - provides more security
  - cheaper to manufacture
  - previous work was only able to identify ICs based on manufacturing variations, but not authenticate them
- First to work reliably even under varying environmental conditions
- Introduced the term PUF which is still being used today

Overview

- Executive Summary
- Problem, Goal & Background
- Key Approach and Ideas
- Novelty
- Mechanisms
- Key Results
- Summary
- Strengths and Weaknesses
- Takeaways
- Research history
- Discussion

Mechanism: Measurement Circuit



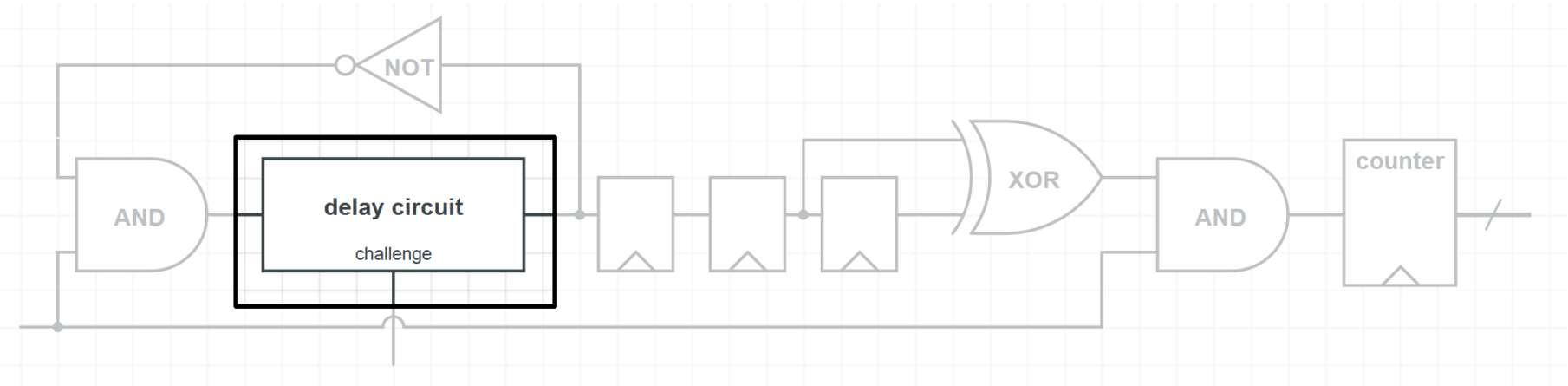
challenge

counting bit: set to "1" for a predefined amount of clock cycles to enable the measurement

"response": gets further processed to ensure reliability against environmental variations

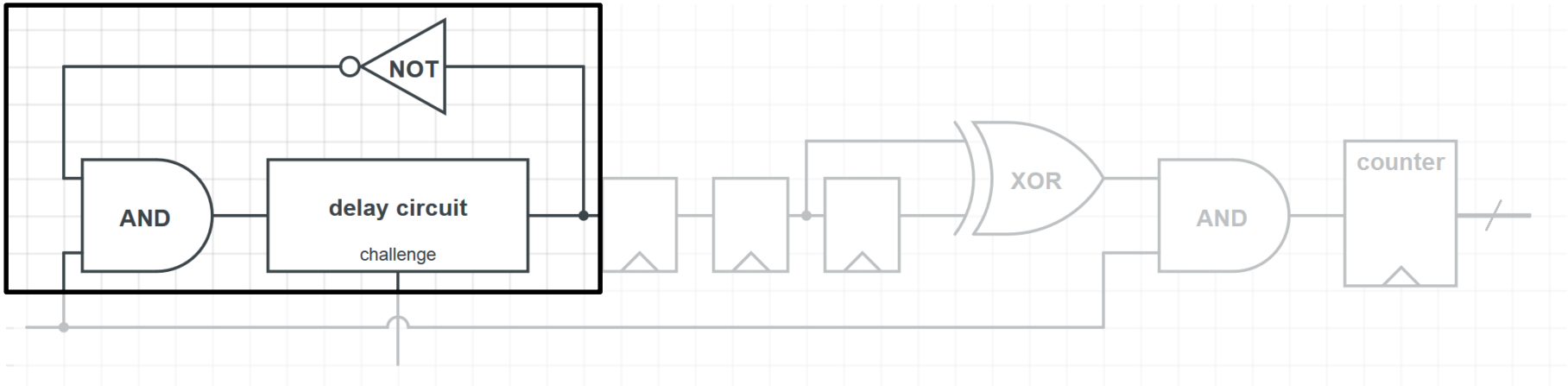
Mechanism: Measurement Circuit

- delay circuit: variable delay from device to device
  - more in a few moments



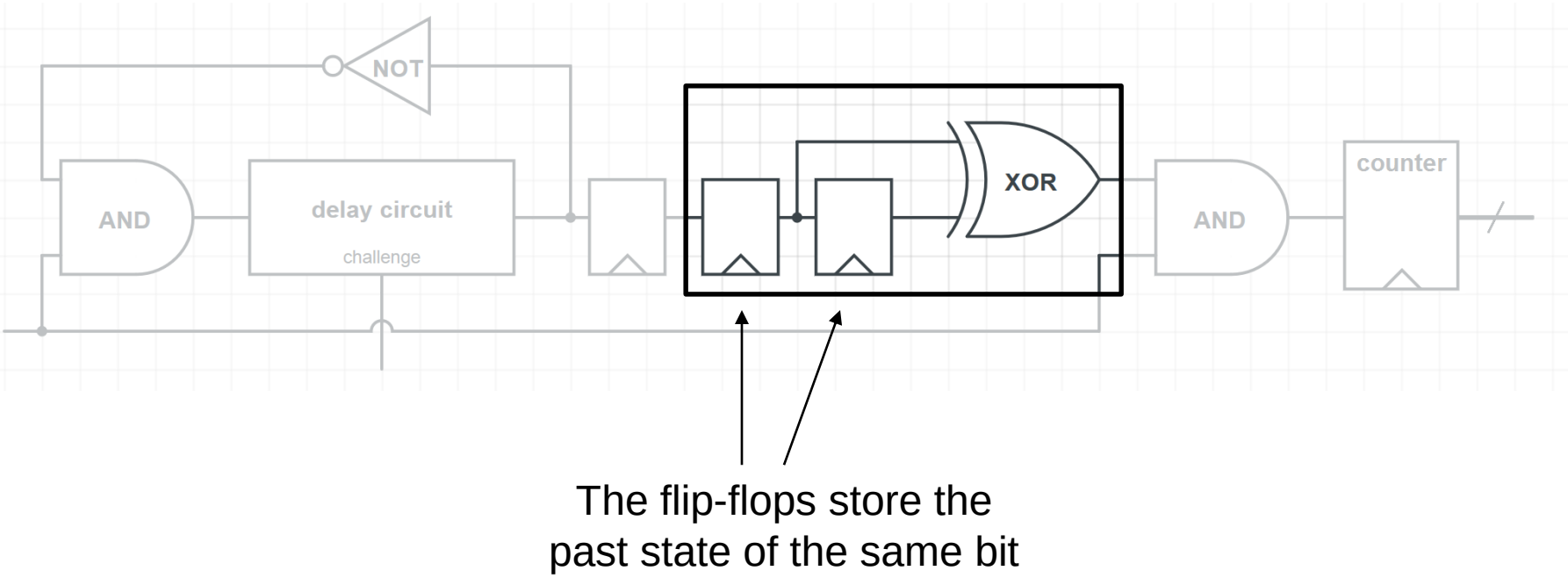
Mechanism: Measurement Circuit

- oscillator block: self-oscillating circuit
  - frequency is determined by the delay of the delay circuit



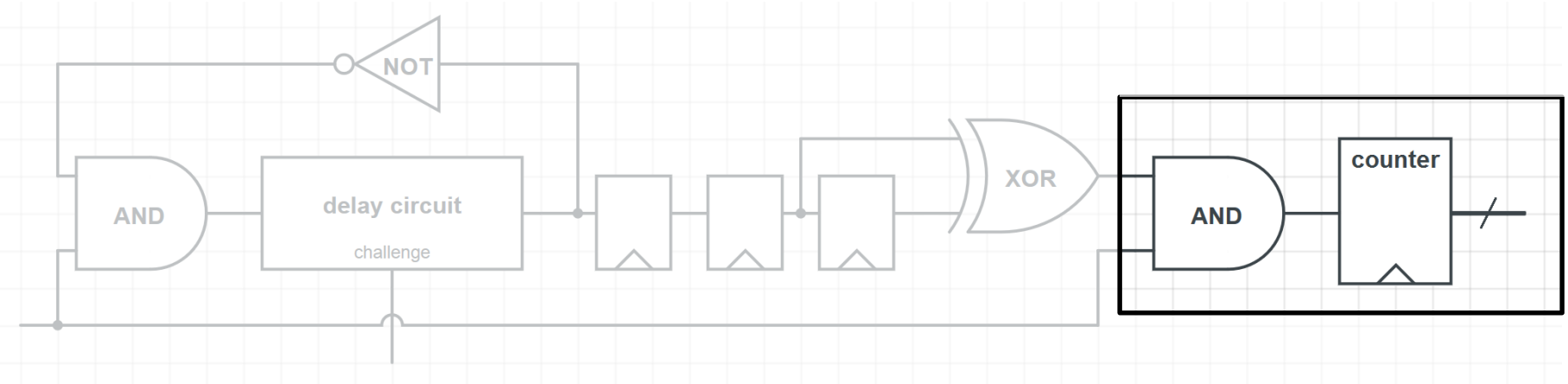
Mechanism: Measurement Circuit

- edge-detector
  - XOR outputs "1" exactly when the two FFs store different values



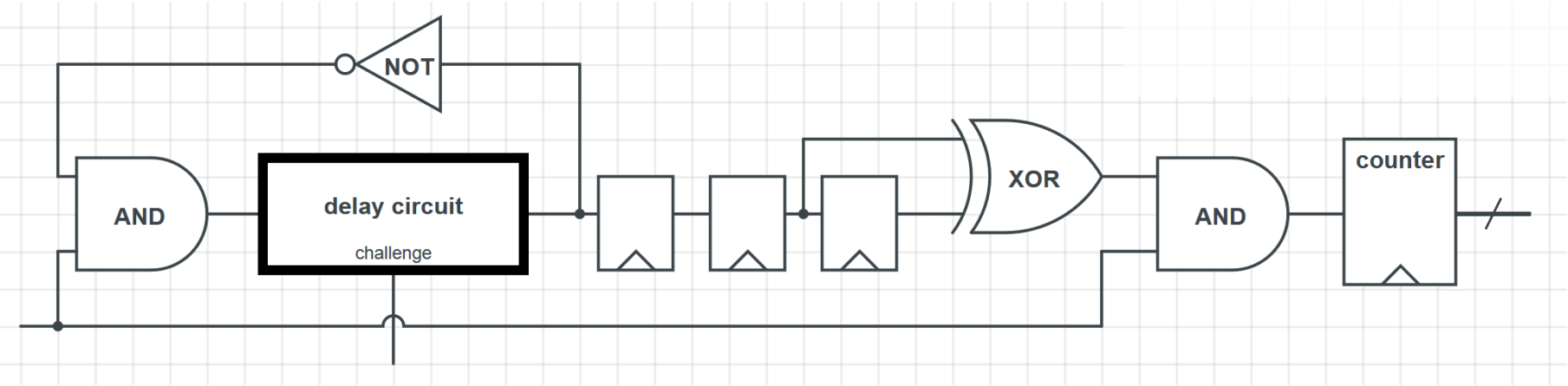
Mechanism: Measurement Circuit

- counting mechanism
  - increases its value if and only if an edge got detected and the frequency is still being measured



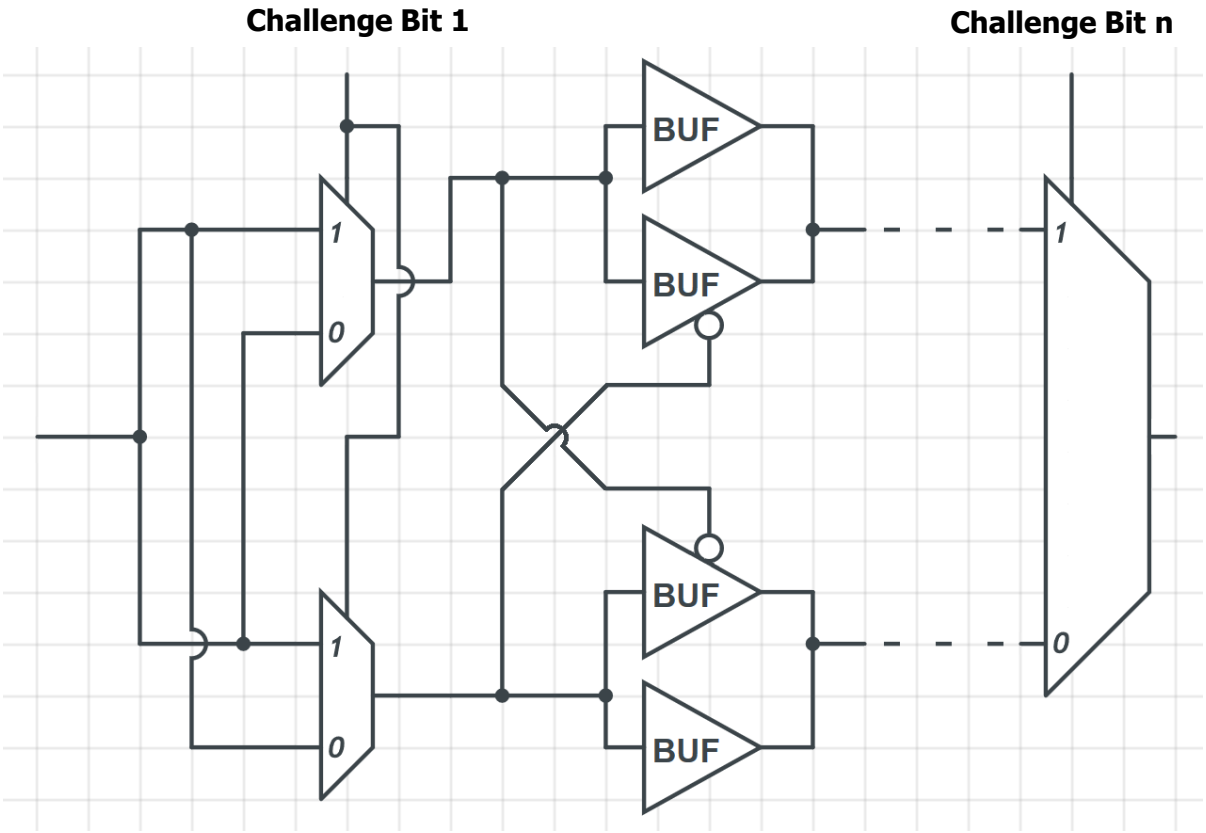
Mechanism: Measurement Circuit

- Detailed delay circuit



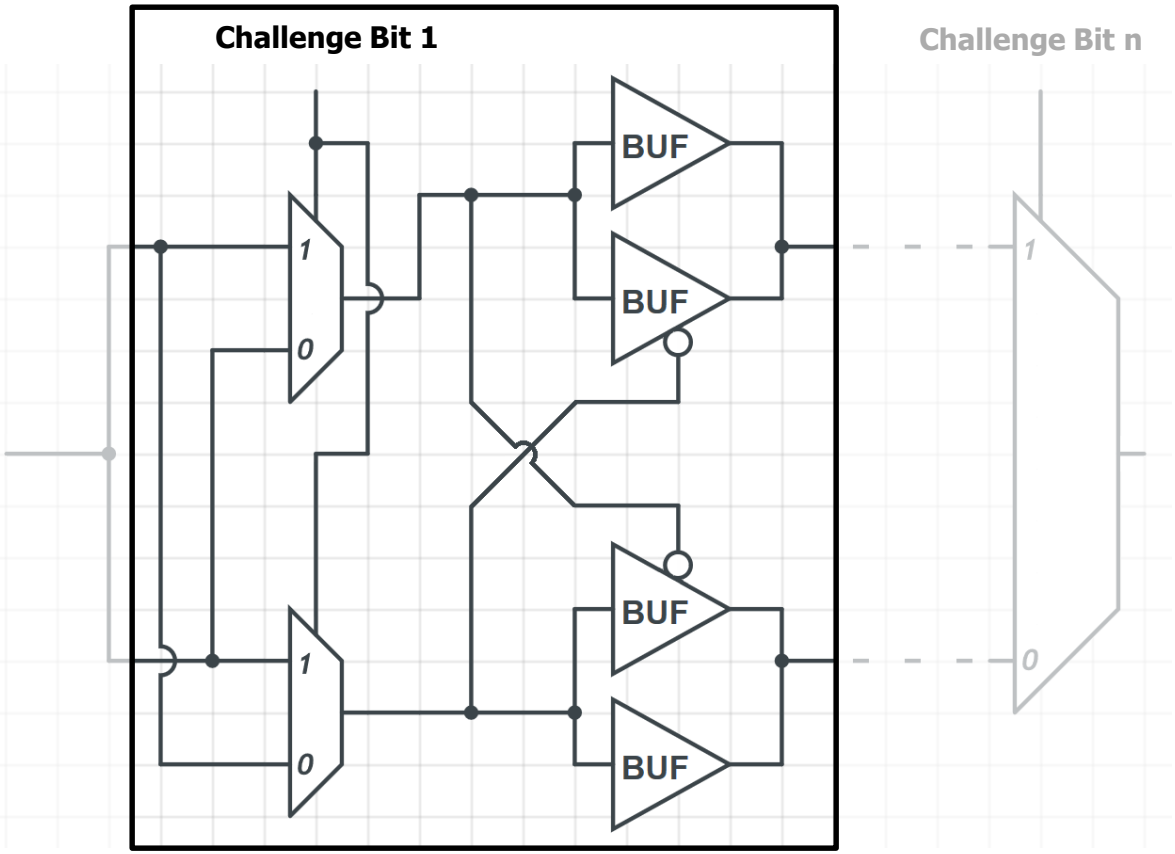
Mechanism: Delay Circuit

- Delay circuit
  - Challenge consists of n Bits



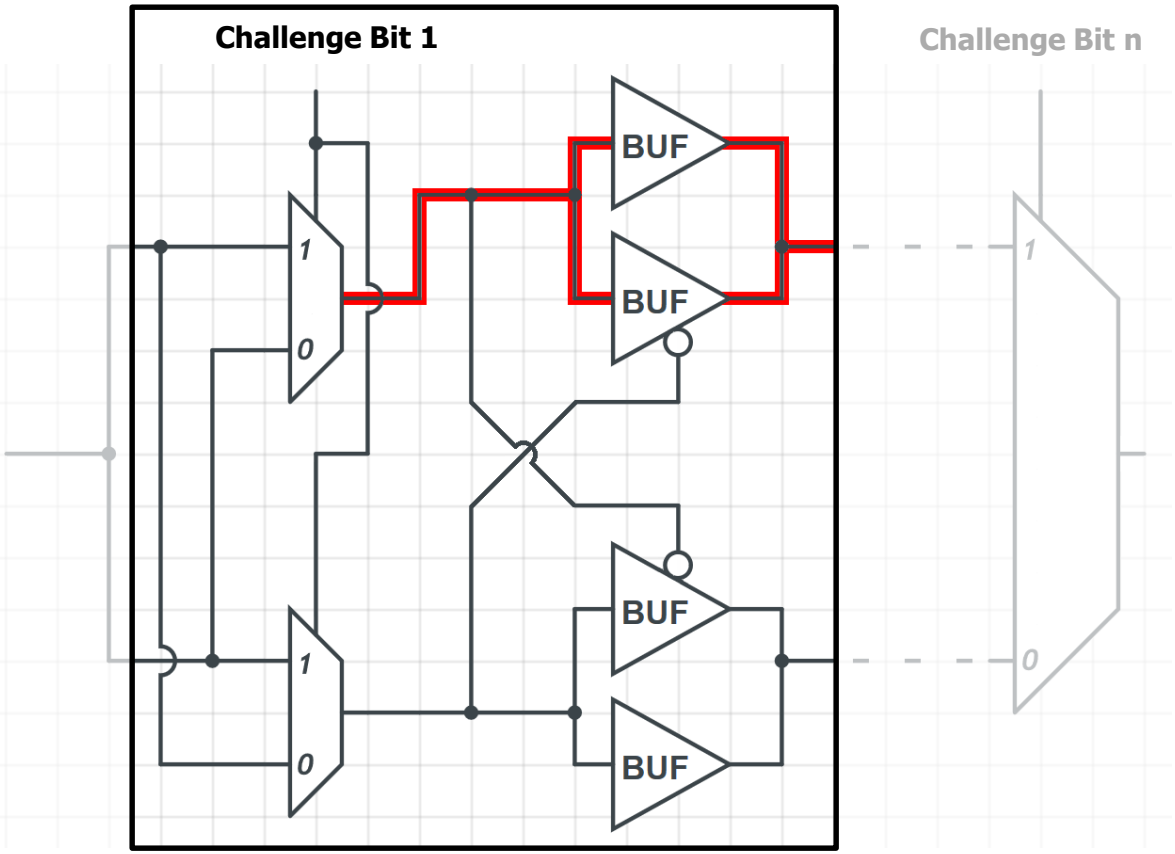
Mechanism: Delay Circuit

- Consists of n-1 stages
  - Each stage has two paths



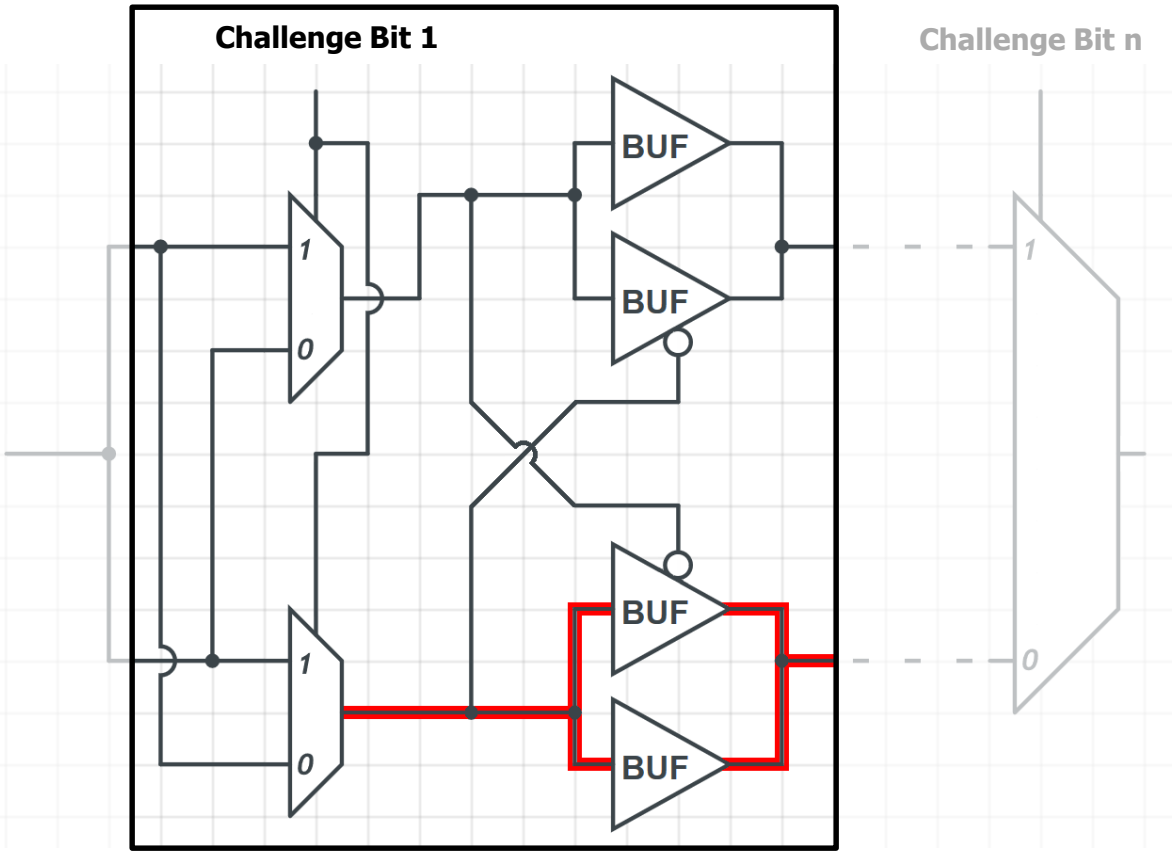
Mechanism: Delay Circuit

- Consists of n-1 stages
  - Each stage has two paths: upper path



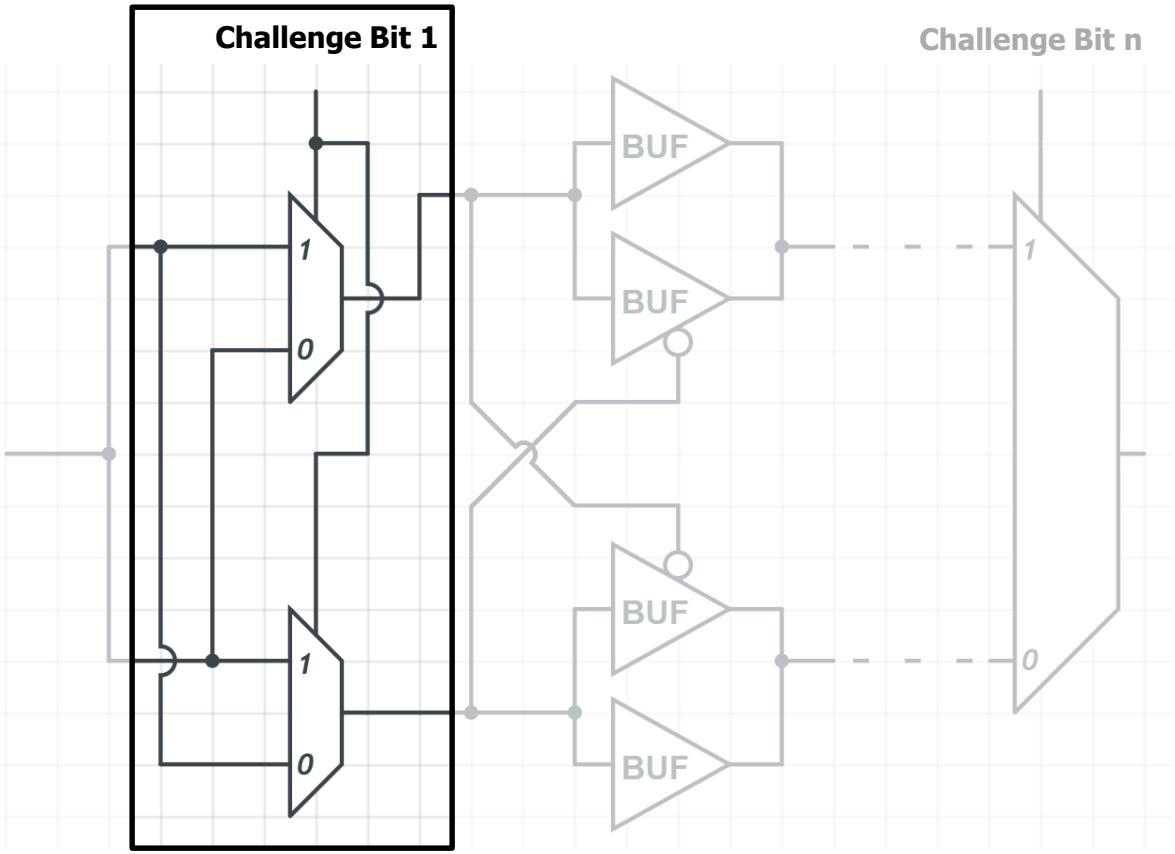
Mechanism: Delay Circuit

- Consists of n-1 stages
  - Each stage has two paths: lower path



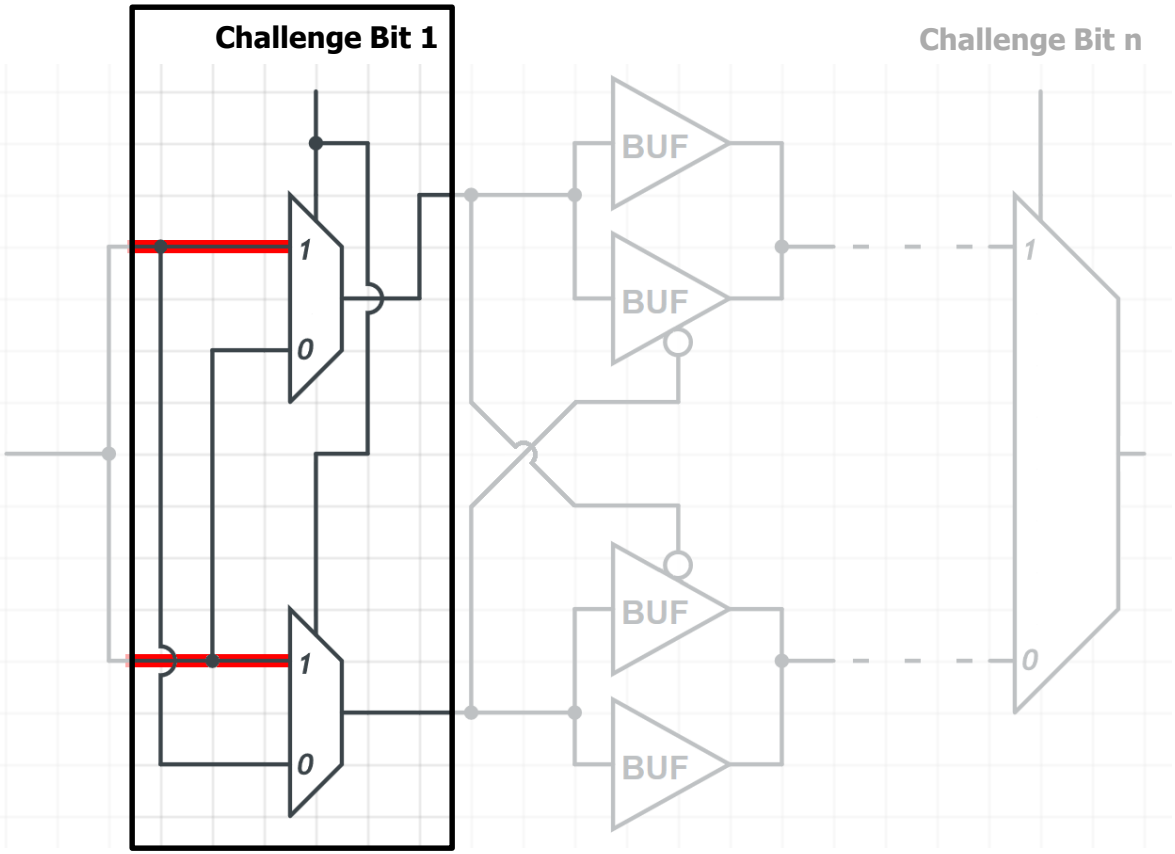
Mechanism: Delay Circuit

- A stage is made up of 2 blocks
  - First block: switch block



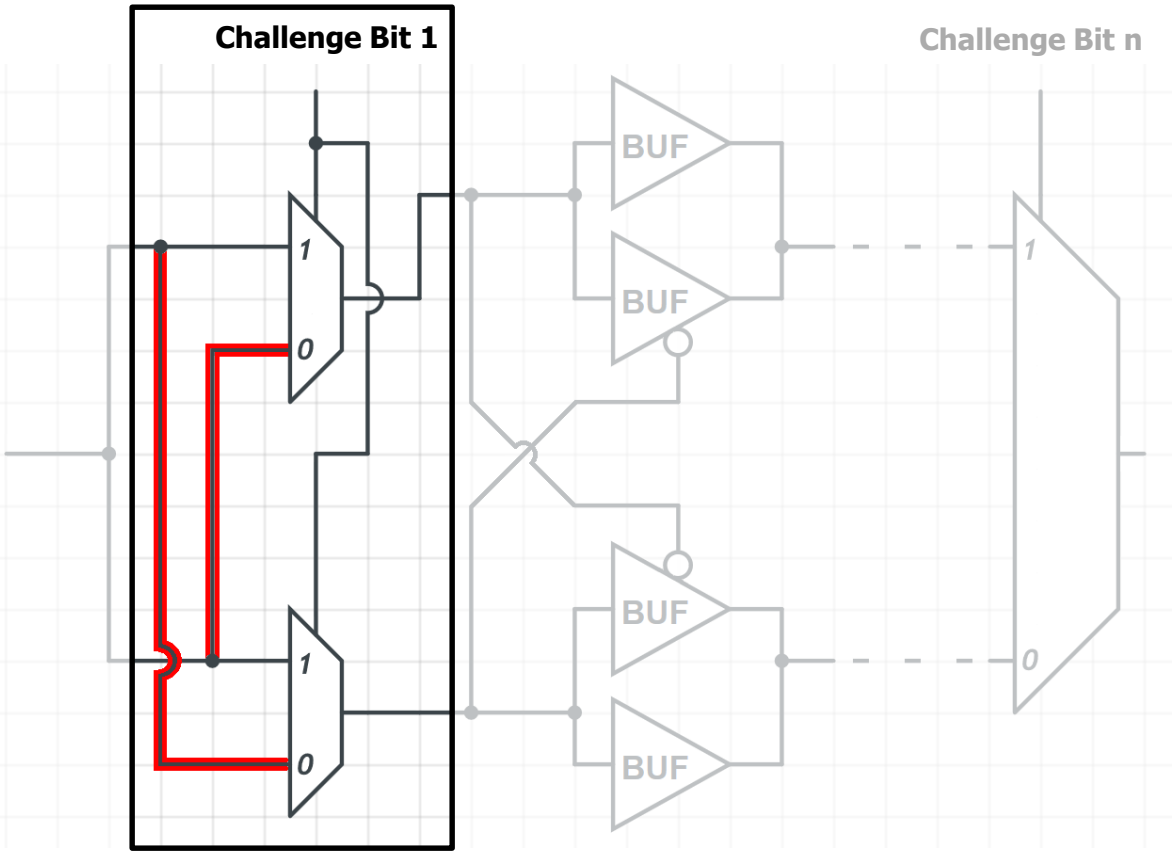
Mechanism: Delay Circuit

- A stage is made up of 2 blocks
  - First block: switch block



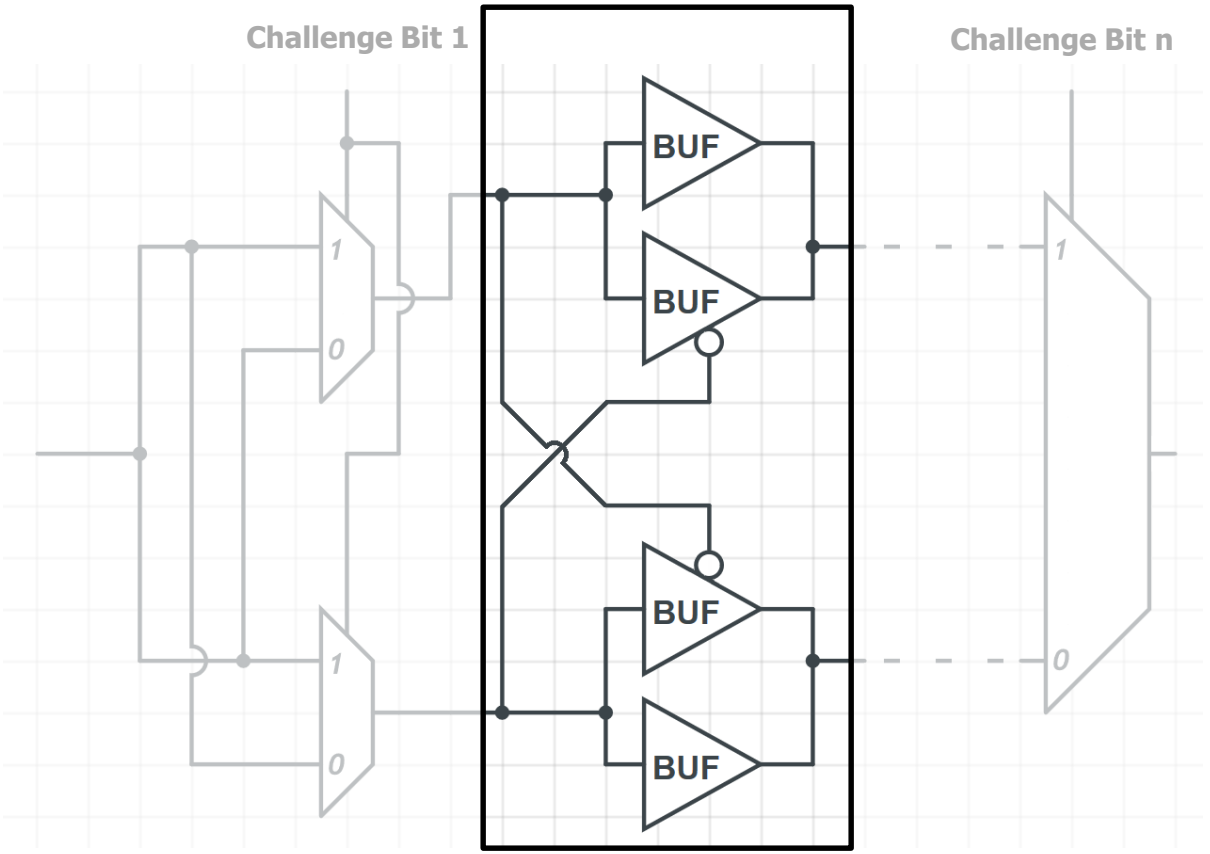
Mechanism: Delay Circuit

- A stage is made up of 2 blocks
  - First block: switch block



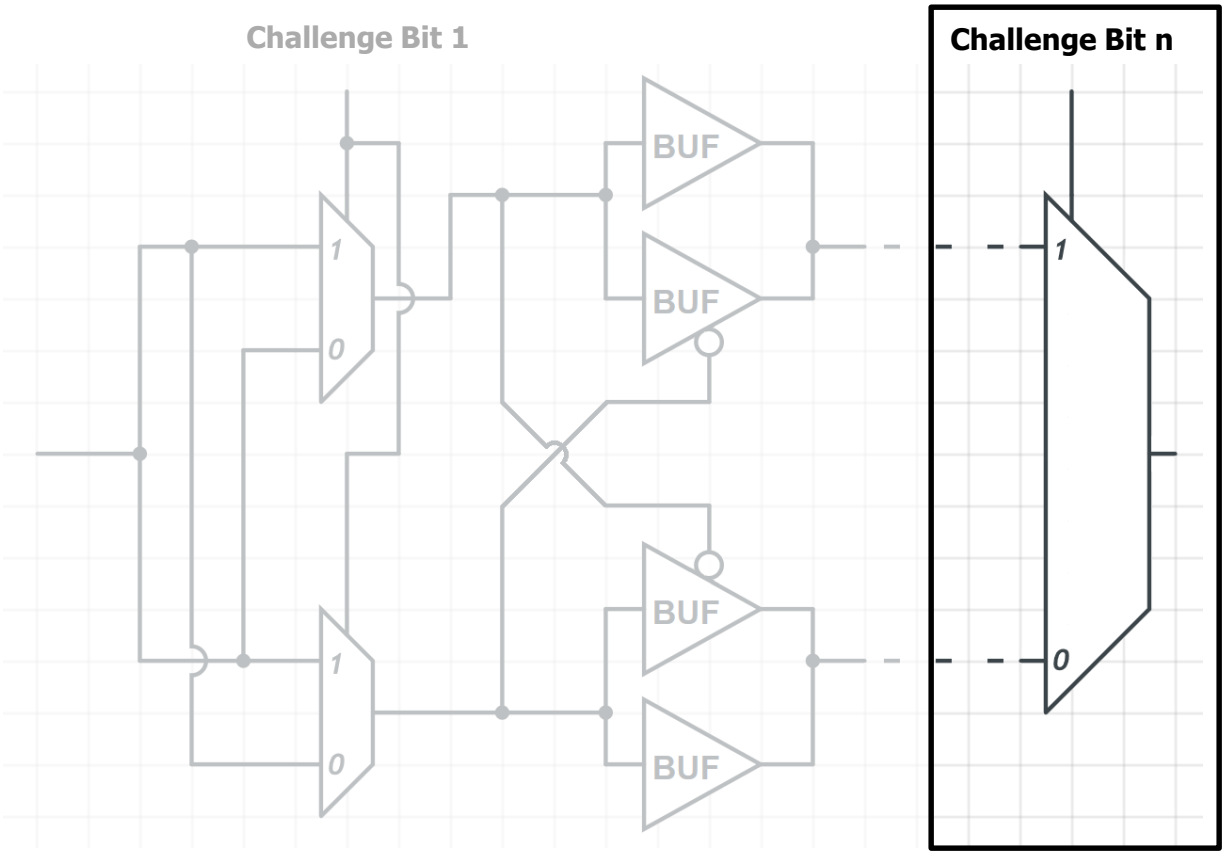
Mechanism: Delay Circuit

- A stage is made up of 2 blocks
  - Second block: variable delay block



Mechanism: Delay Circuit

- Remaining bit of the challenge is used to select whether the upper or the lower path gets propagated forward

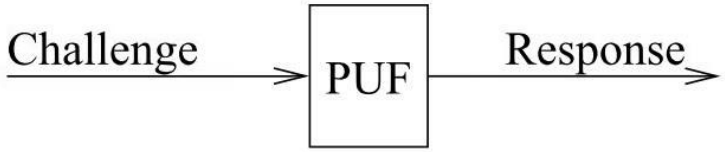


Mechanism: Providing Reliability

- Problem of environmental variations
  - Varying ambient temperatures can influence the junction temperatures, which in turn directly influence the delays of the circuit
- Solution: Build multiple circuits and take the delay ratio
  - You can evaluate all the circuits in parallel
  - More stable result (can compensate at least 25 degrees Celsius in ambient temperature variation)

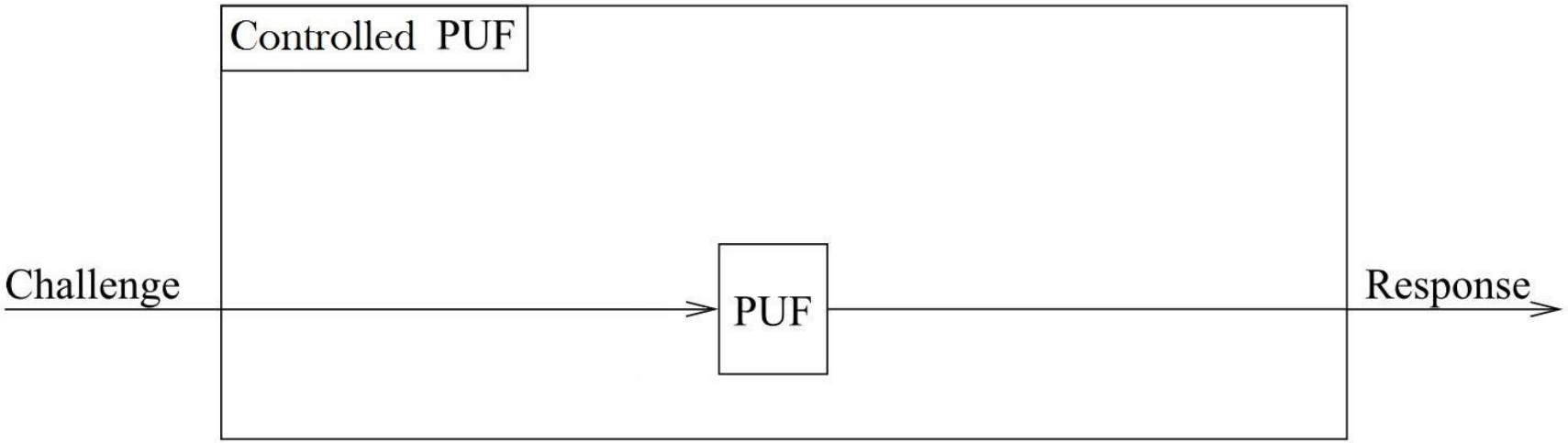
Mechanism: Controlled PUF

- The PUF as we know it:



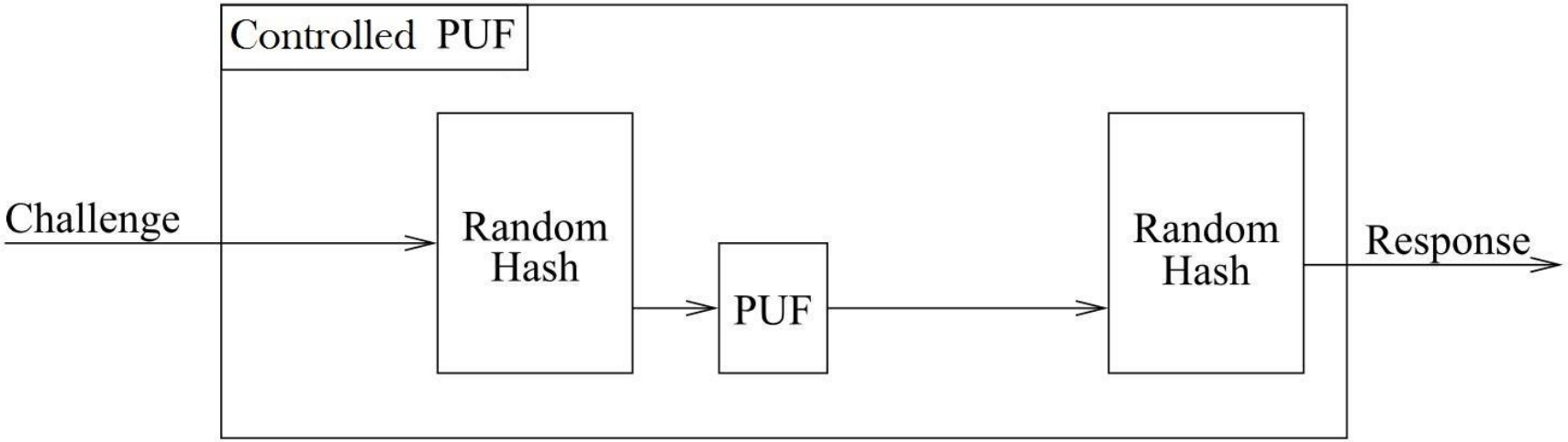
Mechanism: Controlled PUF

- Some additional features:



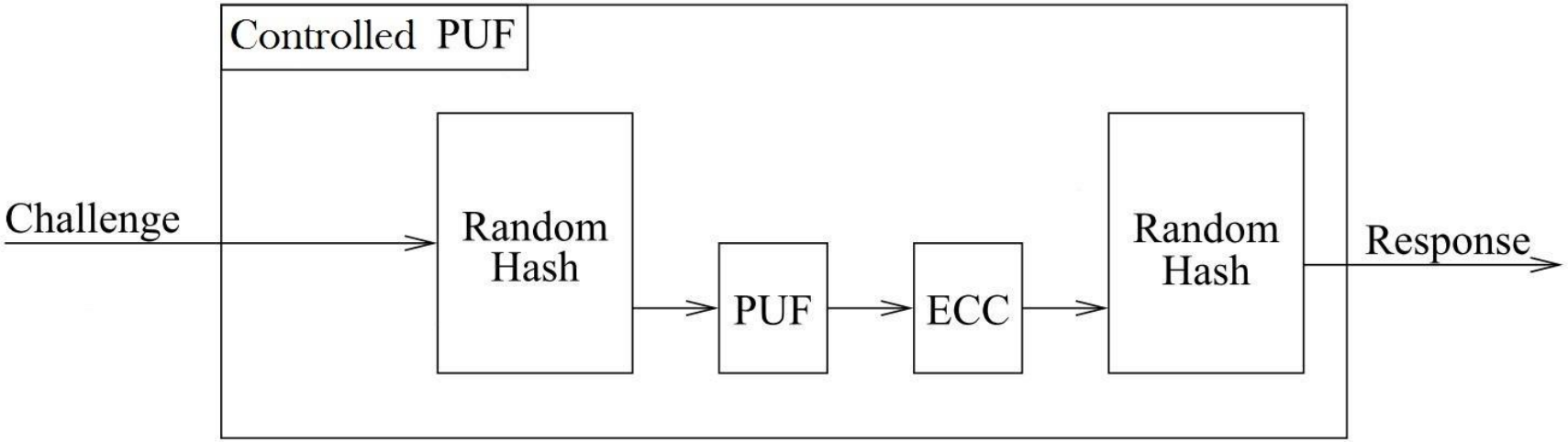
Mechanism: Controlled PUF

- Some additional features:
  - **Hash functions:** to disguise the internal challenge and response



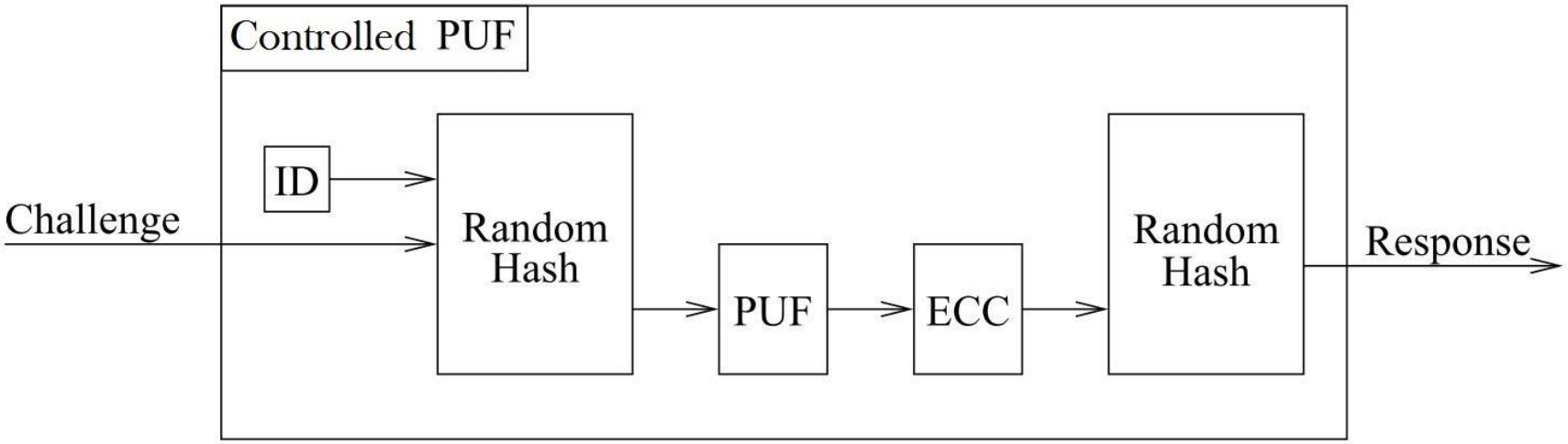
Mechanism: Controlled PUF

- Some additional features:
  - **Hash functions:** to disguise the internal challenge and response
  - **Error correction:** to provide more reliability



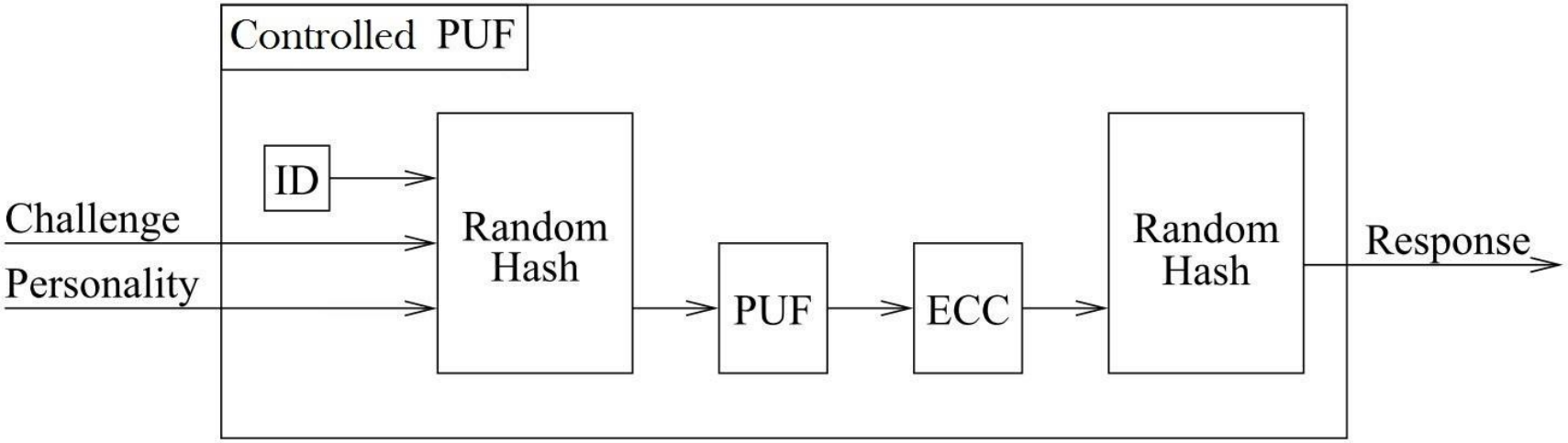
Mechanism: Controlled PUF

- Some additional features:
  - **Hash functions:** to disguise the internal challenge and response
  - **Error correction:** to provide more reliability
  - **Unique identifier:** to provide unambiguity



Mechanism: Controlled PUF

- Some additional features:
  - **Hash functions:** to disguise the internal challenge and response
  - **Error correction:** to provide more reliability
  - **Unique identifier:** to provide unambiguity
  - **Application specific personality:** to provide privacy



Overview

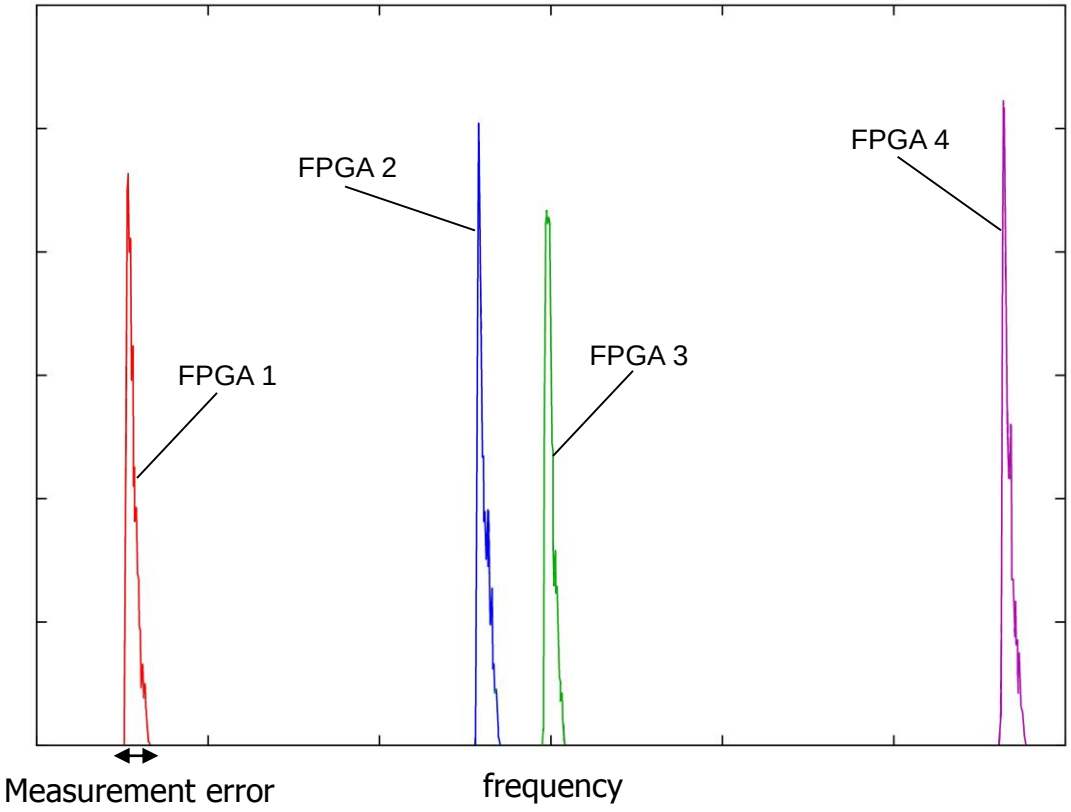
- Executive Summary
- Problem, Goal & Background
- Key Approach and Ideas
- Novelty
- Mechanisms
- Key Results
- Summary
- Strengths and Weaknesses
- Takeaways
- Research history
- Discussion

Key Results: Methodology

- Implementation of ICs on FPGAs
- All FPGAs have exactly the same circuits programmed onto them
  - Delay circuit consists of 32 Buffers
  - Clock speed of 50 MHz
  - Loop delay of approximately 60 ns

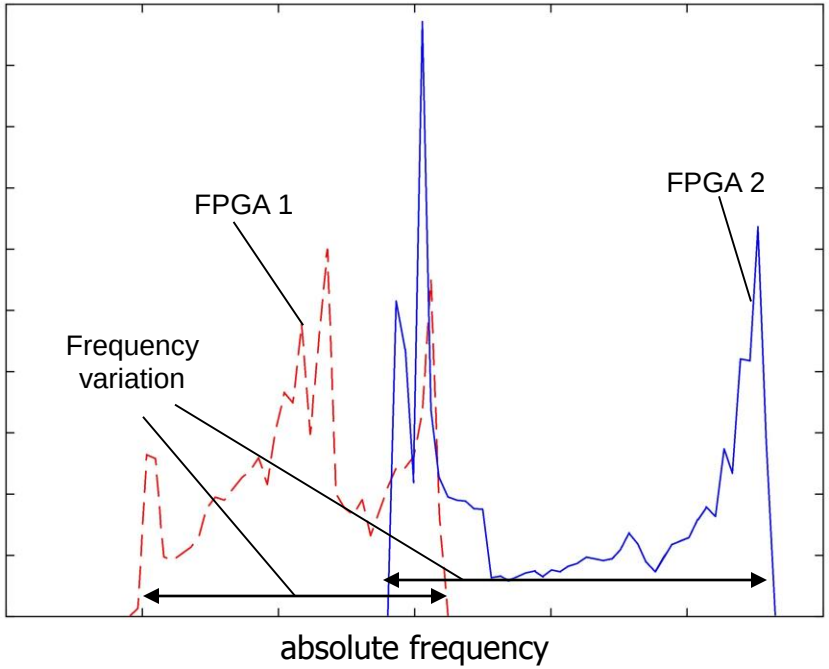
Key Results

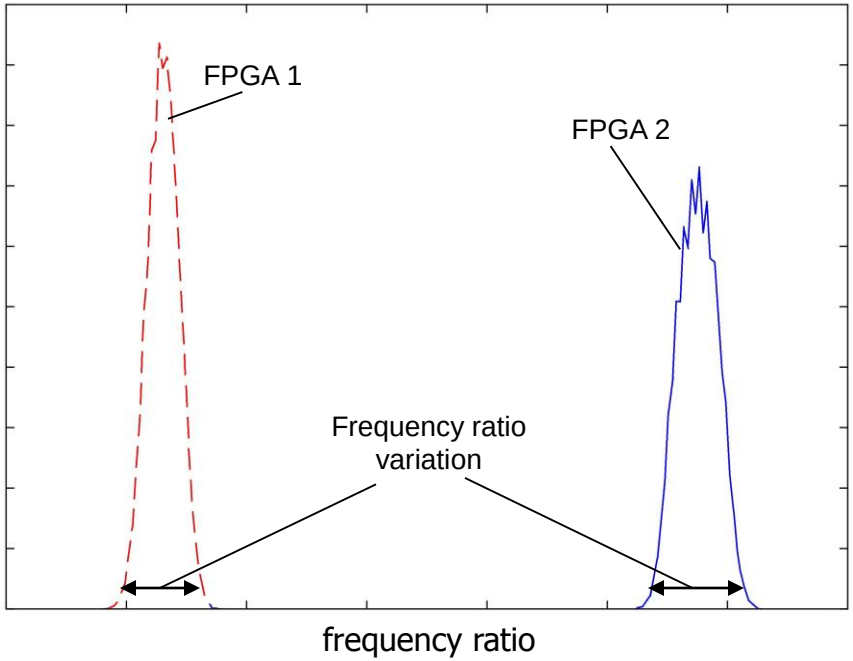
- Measurement error vs Inter-FPGA variation
  - Inter-FPGA variation is significantly larger than measurement error
  - Information about identity can be extracted



Key Results

- Absolute frequency vs frequency ratio (variable temperature between 25 and 50 degrees Celsius)
  - Absolute frequency: variation is too big to extract identity information
  - Frequency ratio: extraction of identity information is possible





Overview

- Executive Summary
- Problem, Goal & Background
- Key Approach and Ideas
- Novelty
- Mechanisms
- Key Results
- Summary
- Strengths and Weaknesses
- Takeaways
- Research history
- Discussion

Summary

- **Problem:** providing authentication for an Integrated Circuit (IC) is difficult, expensive and insecure
- **Goal:** provide a method that provides authentication for ICs that is inexpensive, reliable and secure
- **Method:** implement a circuit that gives characteristic responses for each IC and that is hard to predict
- **Result:** secure authentication that is reliable even under varying environmental conditions

Overview

- Executive Summary
- Problem, Goal & Background
- Key Approach and Ideas
- Novelty
- Mechanisms
- Key Results
- Summary
- Strengths and Weaknesses
- Takeaways
- Research history
- Discussion

Strengths

- Provides a reliable way to identify and authenticate ICs
- Method is inexpensive
- Method is fast to evaluate
- Method is reliable even under varying ambient temperatures
- Overall well structured and written paper

Weaknesses

- Local environmental variations might cause false negatives
  - Delay ratios would fail to compensate temperature changes if they only occur locally
- The results of the experiments are not explained very well
  - The plots are missing axes labeling
  - Sometimes peculiar units get used without explanation
- The entity performing the authentication needs to maintain a database containing all necessary CRPs for each user
  - Since each CRP can be used only once, this can add up to quite a big amount of data
- If you run out of CRPs you need to "reload" the database
- Dependent on the production procedure being inaccurate
  - PUFs will not work anymore if environmental variations and measurement errors dominate manufacturing process variations

Overview

- Executive Summary
- Problem, Goal & Background
- Key Approach and Ideas
- Novelty
- Mechanisms
- Key Results
- Summary
- Strengths and Weaknesses
- Takeaways
- Research history
- Discussion

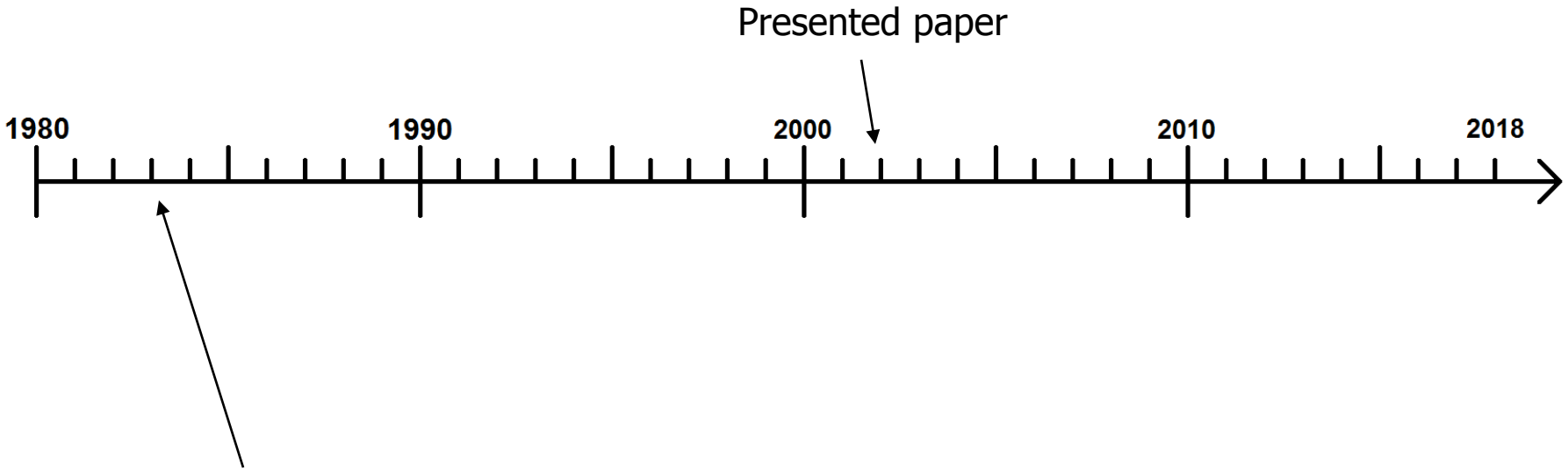
Takeaways

- PUFs are a reliable and secure way to provide identification and authentication for ICs
- Authentication is possible without the need of a secret key
- PUFs are gaining interest in the industry today
- Drawbacks of a method can prove to be helpful when trying to solve another problem

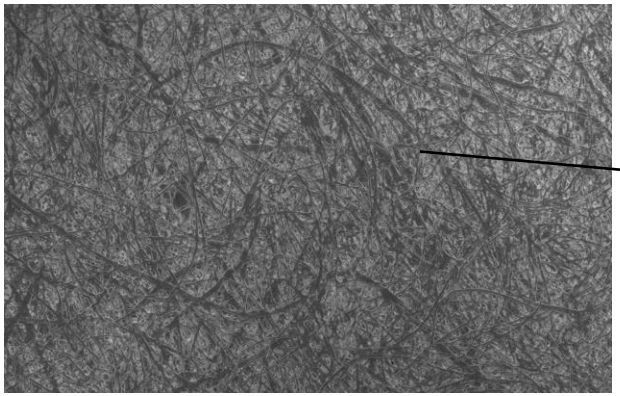
Overview

- Executive Summary
- Problem, Goal & Background
- Key Approach and Ideas
- Novelty
- Mechanisms
- Key Results
- Summary
- Strengths and Weaknesses
- Takeaways
- Research history
- Discussion

Research History



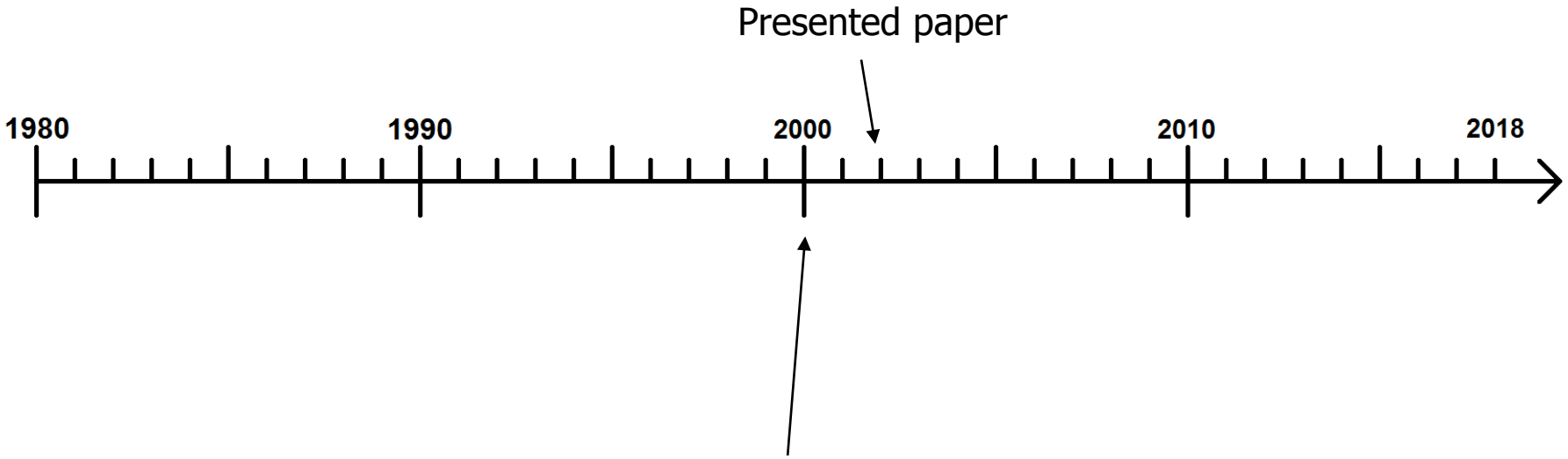
D. Bauder, An Anti-counterfeiting Concept for Currency Systems. Technical Report PTK-11990, Sandia National Labs, Albuquerque, NM, 1983



Use structure of paper to identify counterfeit banknotes

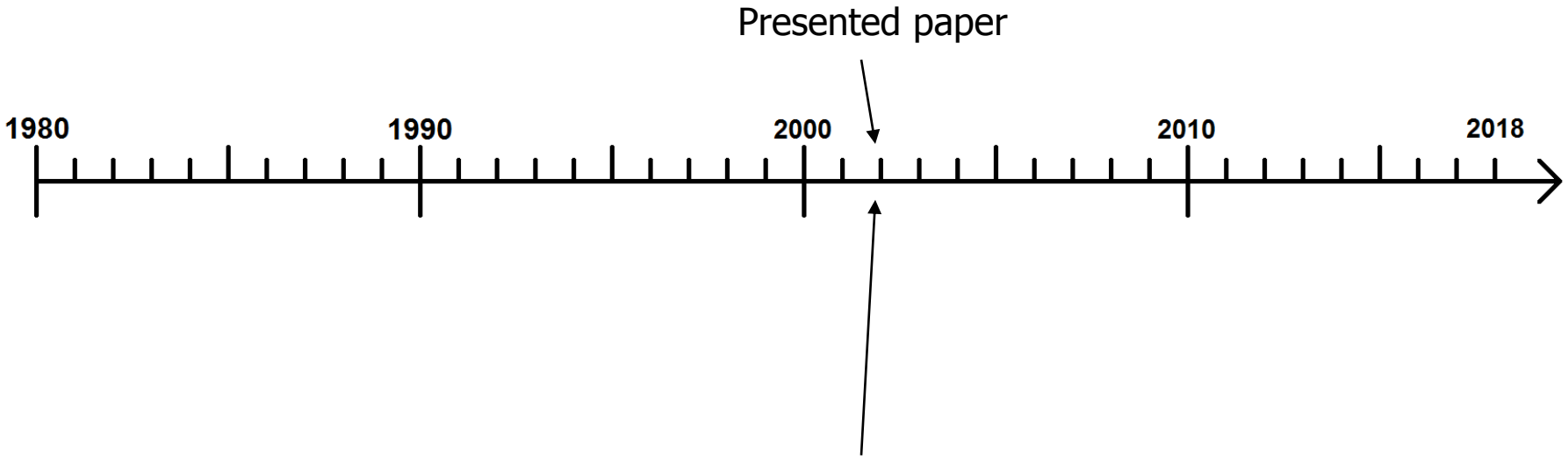
image source: https://de.wikipedia.org/wiki/Papier#/media/File:Paper_sheet_100x_-_SEM_MUSE.tif

Research History

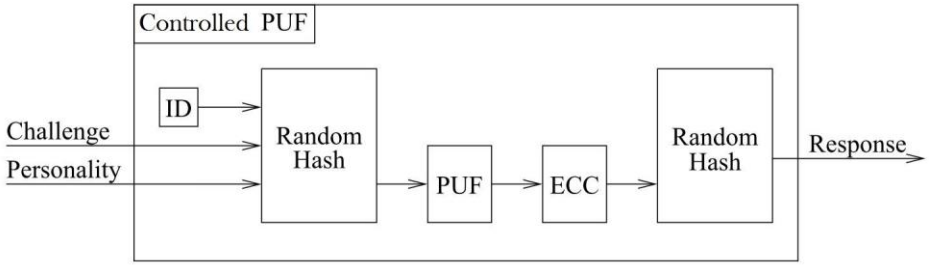


K. Lofstrom, W. R. Daasch, and D. Taylor. “IC Identification Circuit Using Device Mismatch”. In Proceedings of ISSCC 2000, pages 372–373, February 2000

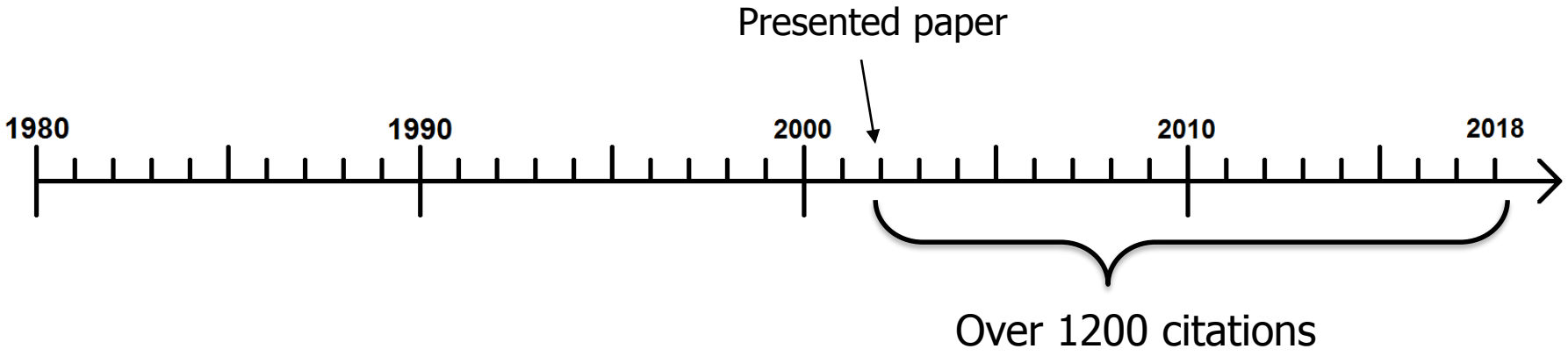
Research History



B. Gassend, D. Clarke, M. van Dijk, and S. Devadas. Controlled Physical Random Functions. In Proceedings of the 18th Annual Computer Security Conference, December 2002



Research History



Silicon physical random functions

B Gassend, D Clarke, M Van Dijk… - Proceedings of the 9th …, 2002 - dl.acm.org

We introduce the notion of a Physical Random Function (PUF). We argue that a complex integrated circuit can be viewed as a silicon PUF and describe a technique to identify and authenticate individual integrated circuits (ICs). We describe several possible circuit …

☆ Cited by 1283 Related articles All 20 versions

Research History

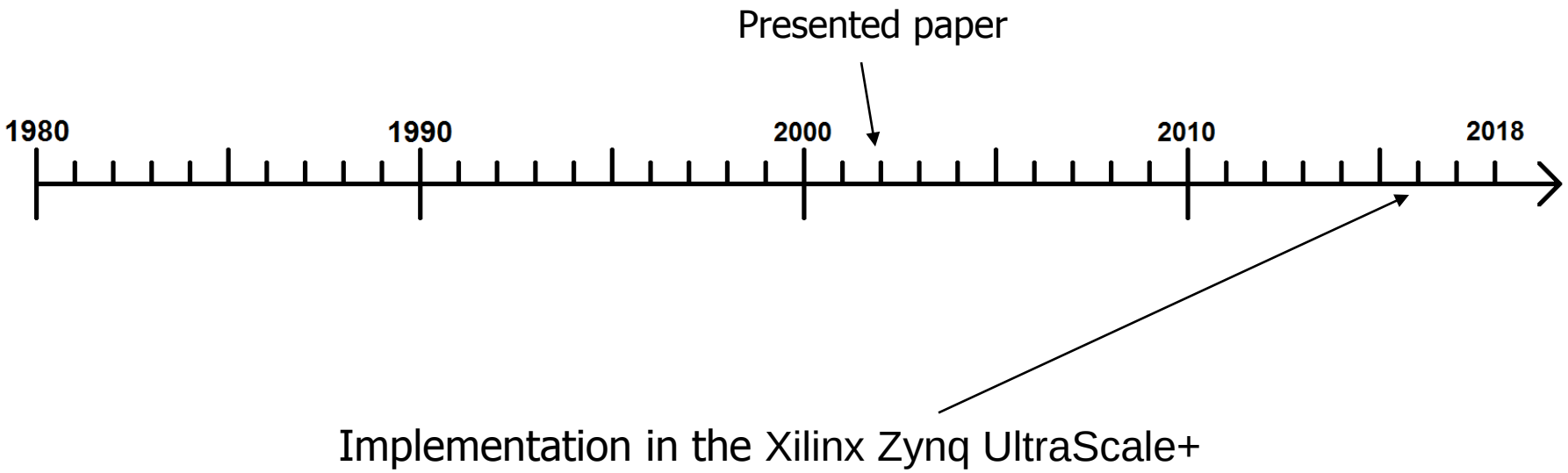
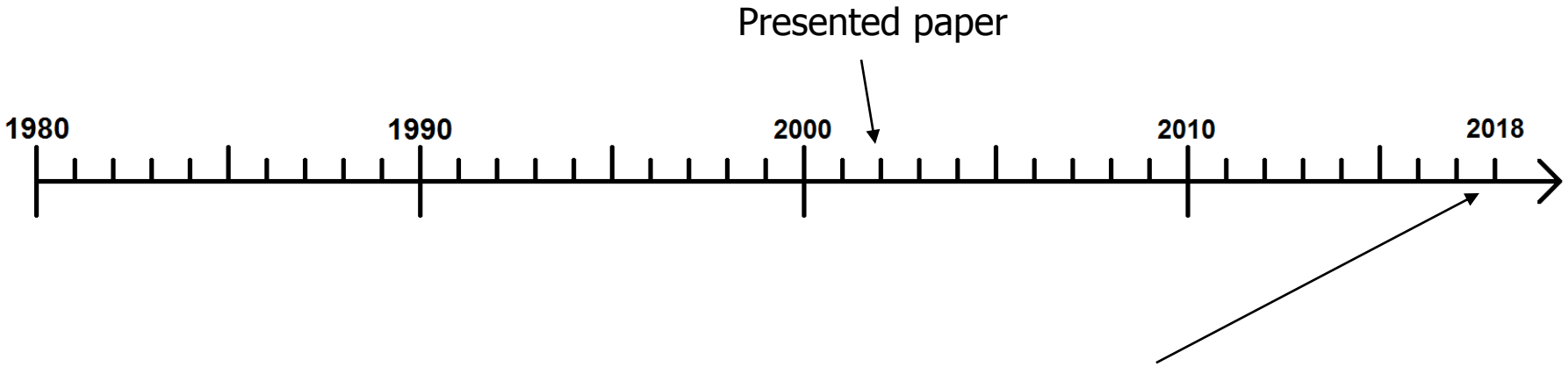
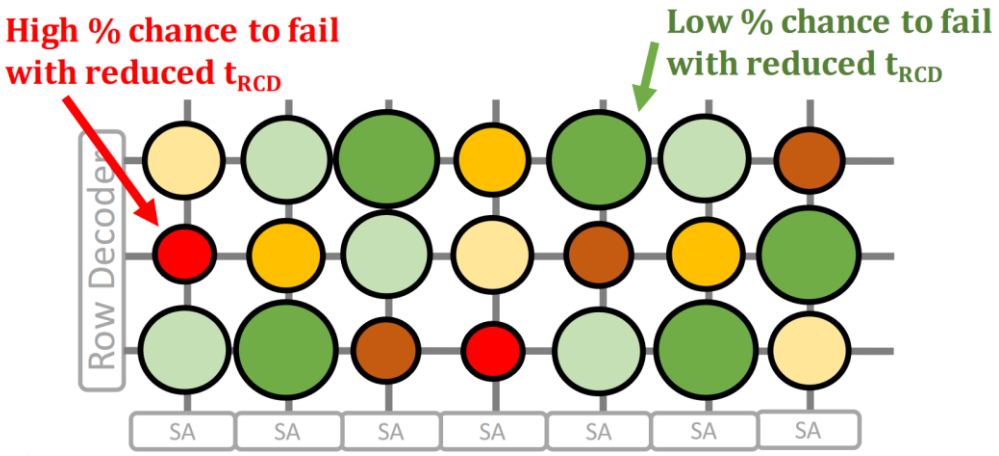


image source: http://linuxgizmos.com/com-duo-expands-upon-quad-a53fpga-zynq-ultrascale/

Research History



J. S. Kim, M. Patel, H. Hassan, and O. Mutlu, "The DRAM Latency PUF: Quickly Evaluating Physical Unclonable Functions by Exploiting the Latency–Reliability Tradeoff in Modern DRAM Devices," in HPCA, 2018.



Overview

- Executive Summary
- Problem, Goal & Background
- Key Approach and Ideas
- Novelty
- Mechanisms
- Key Results
- Summary
- Strengths and Weaknesses
- Takeaways
- Research history
- Discussion

Discussion

- Can you think of any attacks against the described PUFs?

Discussion

- 1st approach:
  - Produce a copy of the PUF
  - Would require production and characterization of a huge amount of ICs

Discussion

- 2nd approach:
  - Measure the delay of each device and wire in the IC precisely to build a model of the PUF
  - **Invasive attack**
    - Likely to change the behavior of the PUF due to electromagnetic coupling which renders the measurements worthless
  - **Non-invasive attack**
    - E.g. Differential Power Analysis is not very useful either because the power consumption does not really depend on the delays of the individual internal devices

Discussion

- 3rd approach:
  - Exhaustively enumerating all challenges and afterwards replay them from a database
  - Possible but basically unfeasible

Discussion

- 4th approach:
  - Measuring the responses to a limited amount of challenges and building a model based on these measurements
  - Probably the most promising attack
  - However properties of the PUF such as the non-monotony of the delays make it quite hard to determine a model

Discussion

- Can you think of other types of PUFs?
  - Delay PUF
  - DRAM PUF
  - Paper PUF
  - Optical PUF
  - Fingerprint

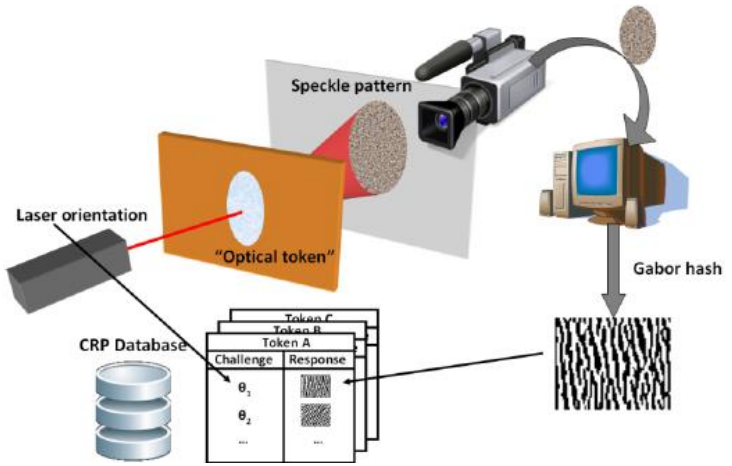
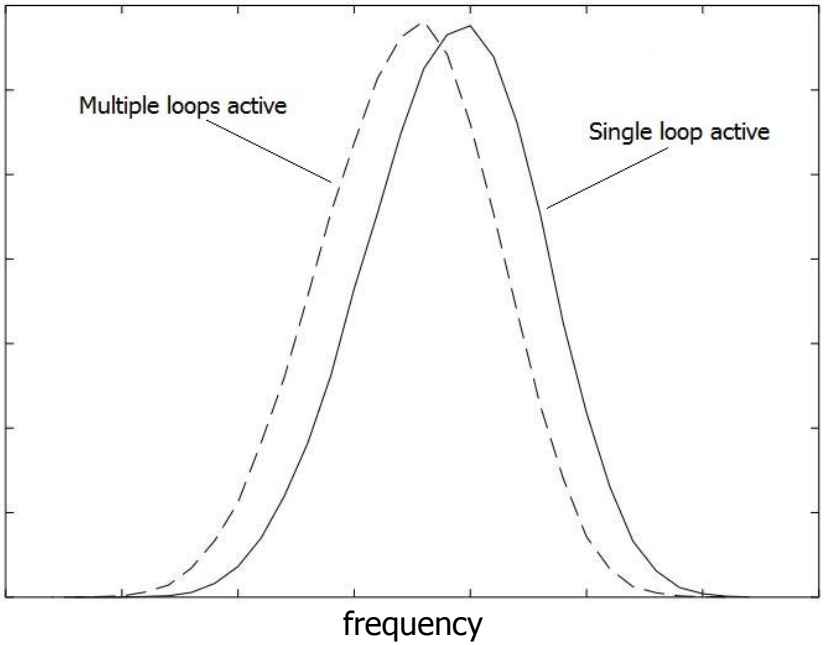


image source (Optical PUF): https://www.researchgate.net/figure/Basic-operation-of-an-optical-PUF_fig1_226371108
image source (Fingerprint): https://www.nytimes.com/2012/06/10/magazine/who-made-those-fingerprints.html

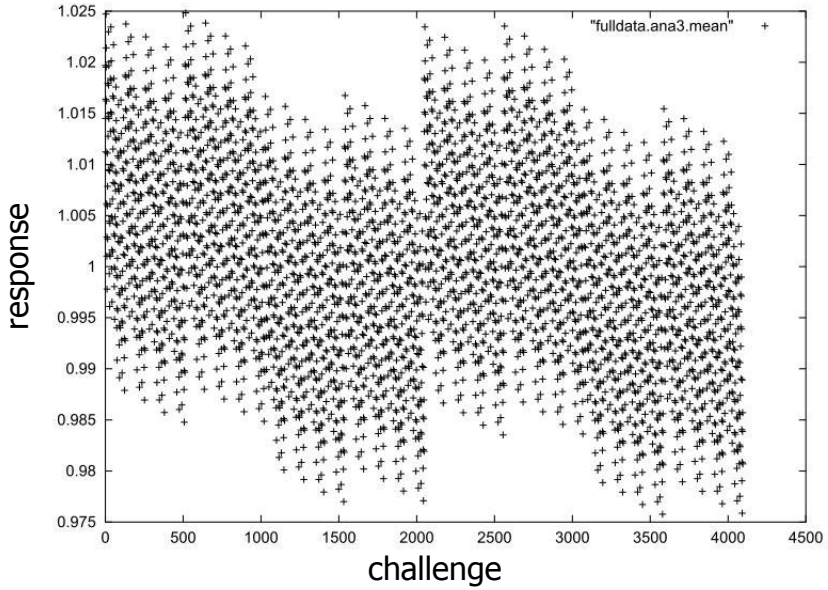
Backup

- Frequency shift resulting from electromagnetic coupling compared to measurement error

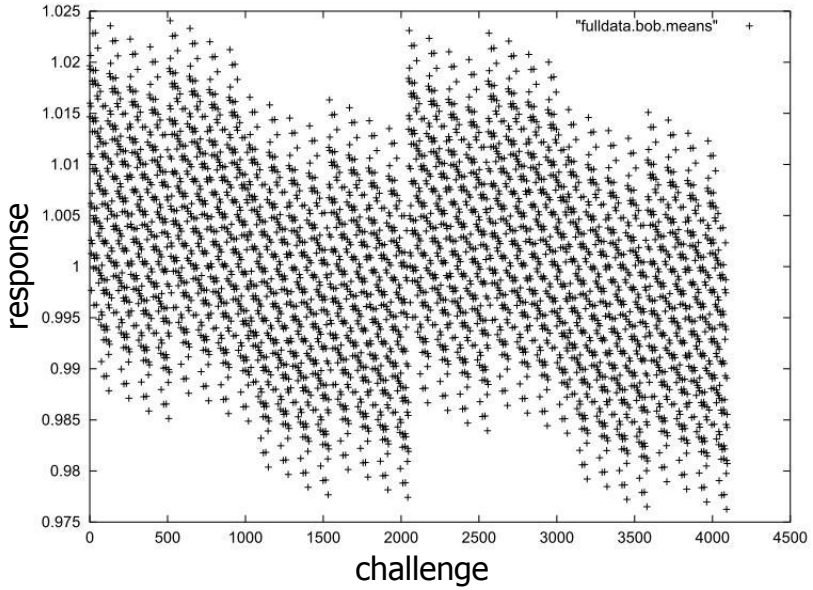


Backup

- The differences between FPGA can only be detected through differences in texture, not in the overall structure



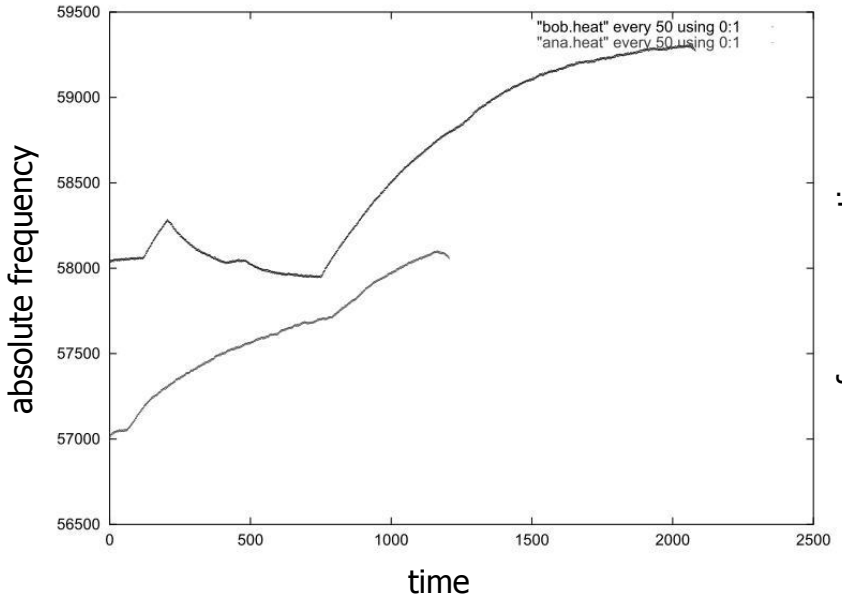
(a) FPGA 1



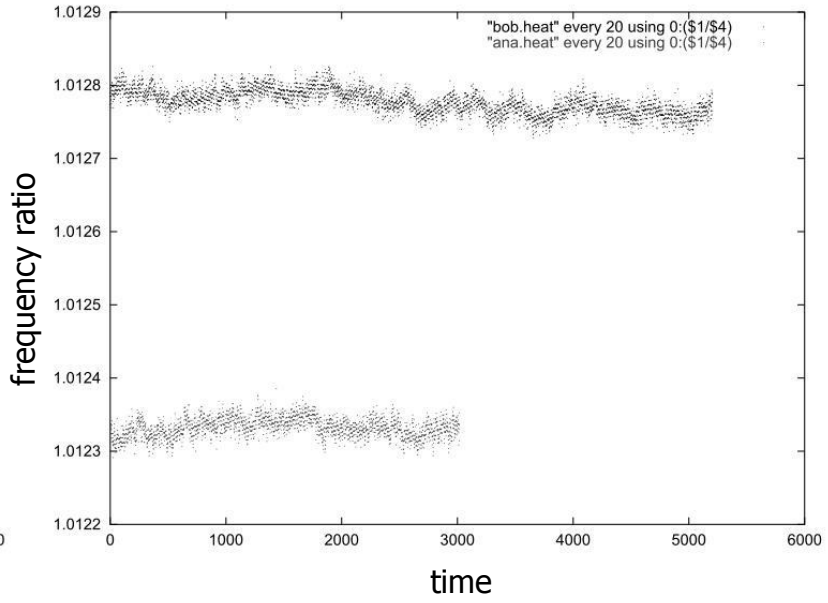
(b) FPGA 2

Backup

- Measure responses in time when undergoing changes in ambient temperature with and without compensation



(c) Uncompensated



(d) Compensated