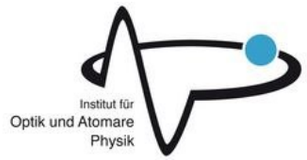
Physical Characterization of Arbiter PUFs

Shahin Tajik, Enrico Dietz, Sven Frohmann, Dmitry Nedospasov,
Clemens Helfmeier, Helmar Dittrich, Jean-Pierre Seifert, Christian Boit

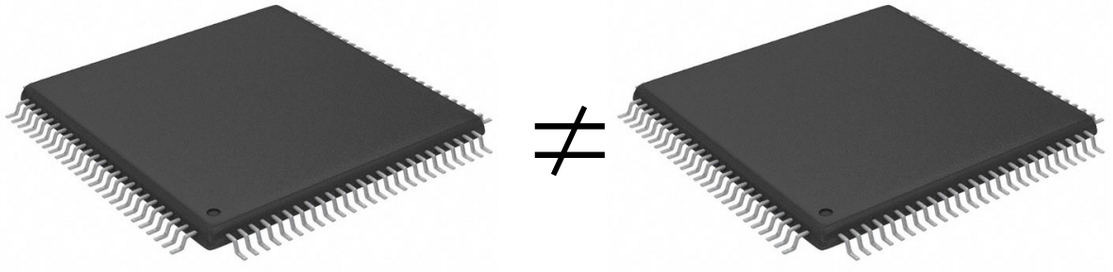


Physically Unclonable Functions (PUFs)

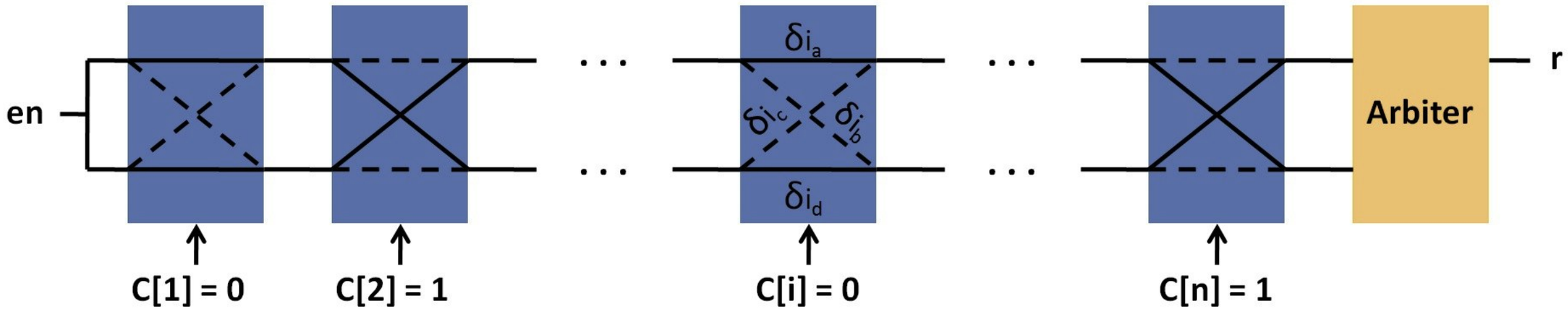
- Secure Integrated Circuits (ICs) for: **Authentication**, **Identification**, **Transaction**, **Communication**

- Utilizing manufacturing processing variations on different chips to make them unique

- **Fingerprint** of the IC



Arbiter PUF



- Utilizing intrinsic timing differences of 2 symmetrically designed electrical paths
- Direct or crossed paths in each stage based on challenge bit
- Response by the Arbiter based on arrival of first signal
- **Assumption: Attacker cannot measure individual delays**

Are Arbiter PUFs Secure?

1. Modeling Attacks

   - Building model on a large subset of challenge-response pairs (CRPs) to predict the response for new challenges with a high probability

   - Disadvantages: based on **trial** and **error** estimates and **required large number of CRPs**

2. Side-channel Attacks

   - Semi-invasive attacks using side channel information such as EM radiation to break Ring Oscillator PUFs

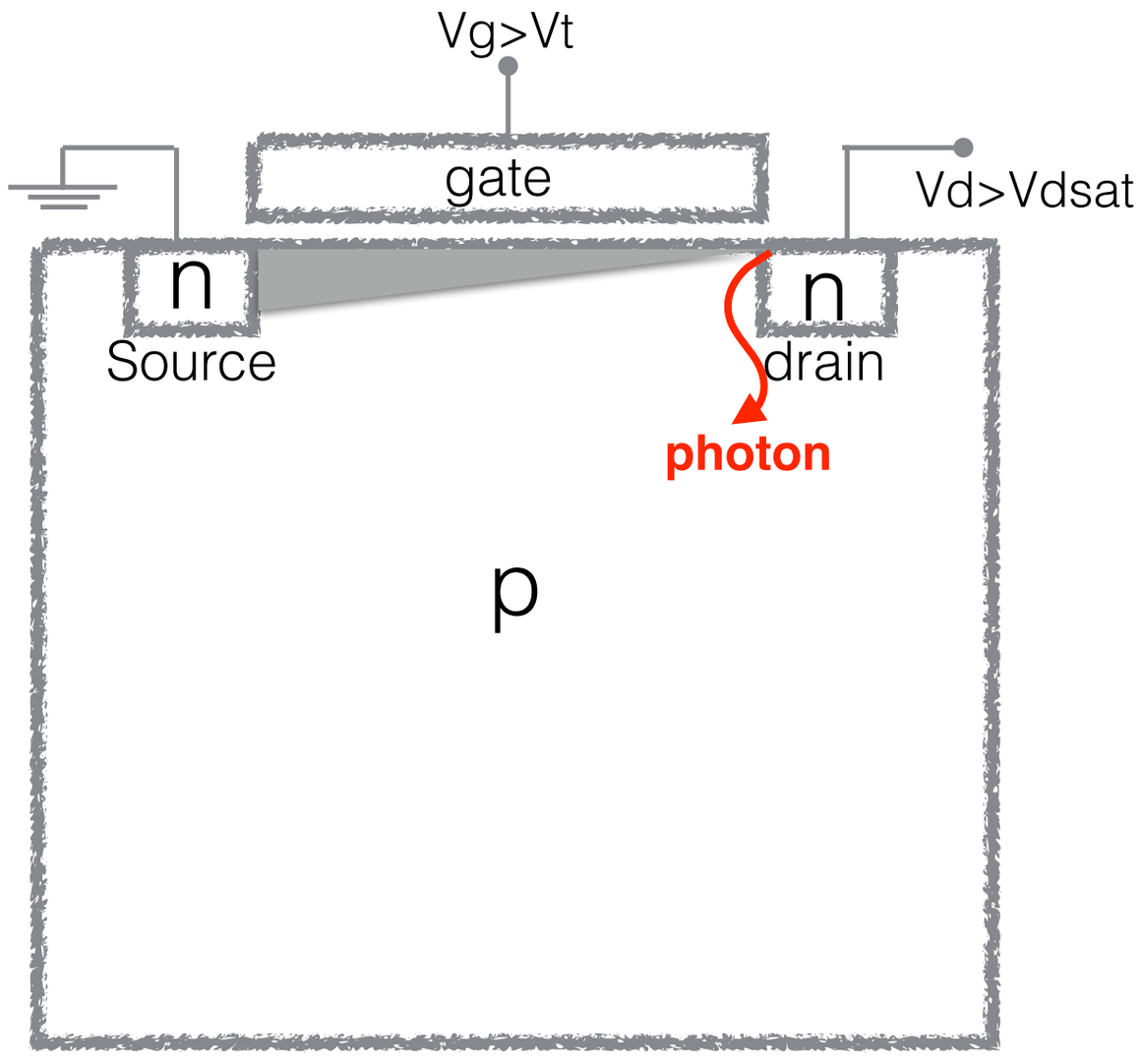
   - Disadvantage: **Applicable only to one type of the arbiter PUFs**

New Attack by Photonic Emission Analysis

- Photonic emission by CMOS transistors during a switching event

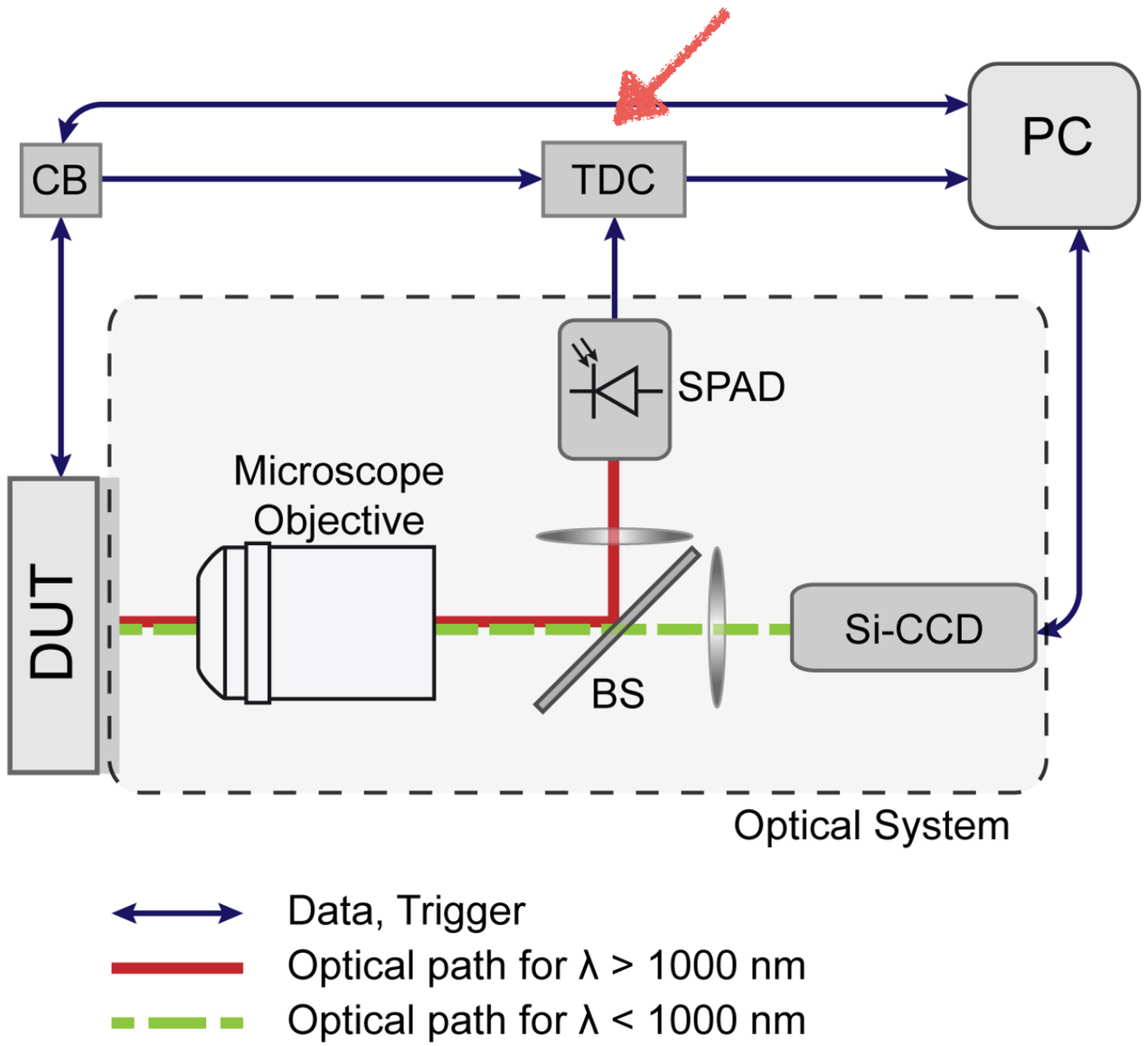
- Obstruction of optical path on the IC frontside by mesh layers

- Observing near-infrared (NIR) emissions from IC backside



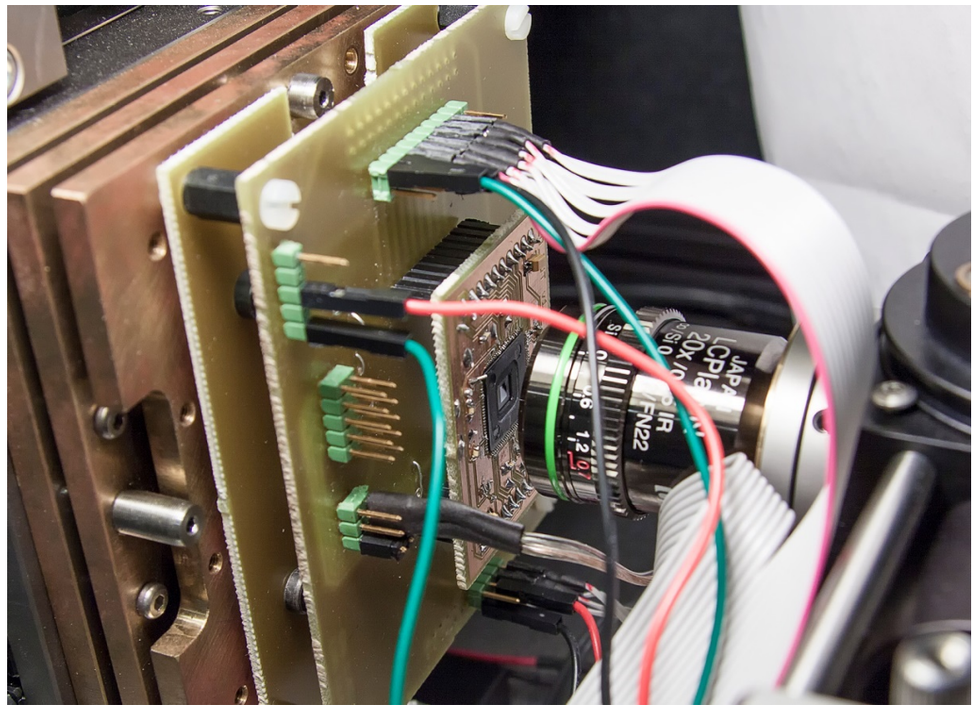
Measurement Setup

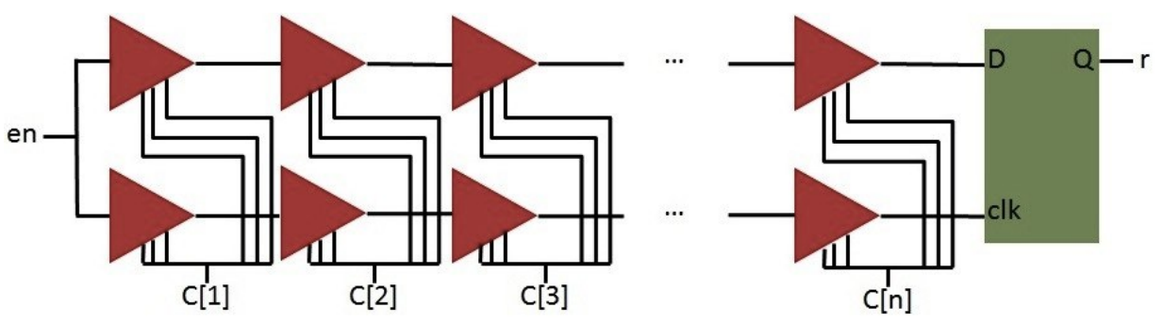
- Spatial analysis by Si-CCD camera
- Detection of single photons by InGaAs avalanche diode
- Measurement of the delay between enabling the PUF and the time of emitted photon by Time-to-digital (TDC)
- Measurement resolution: **6 ps**



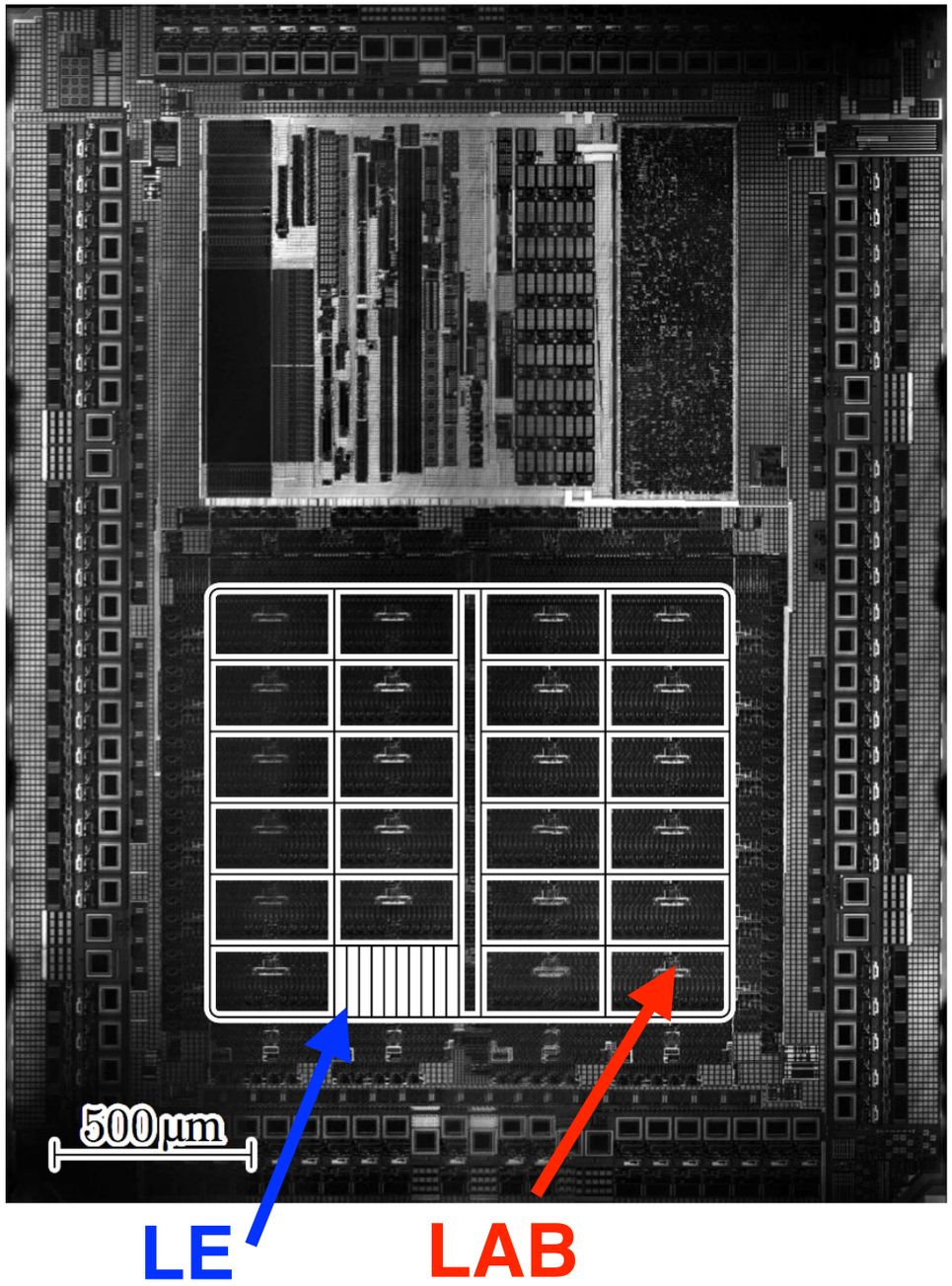
Device under Test

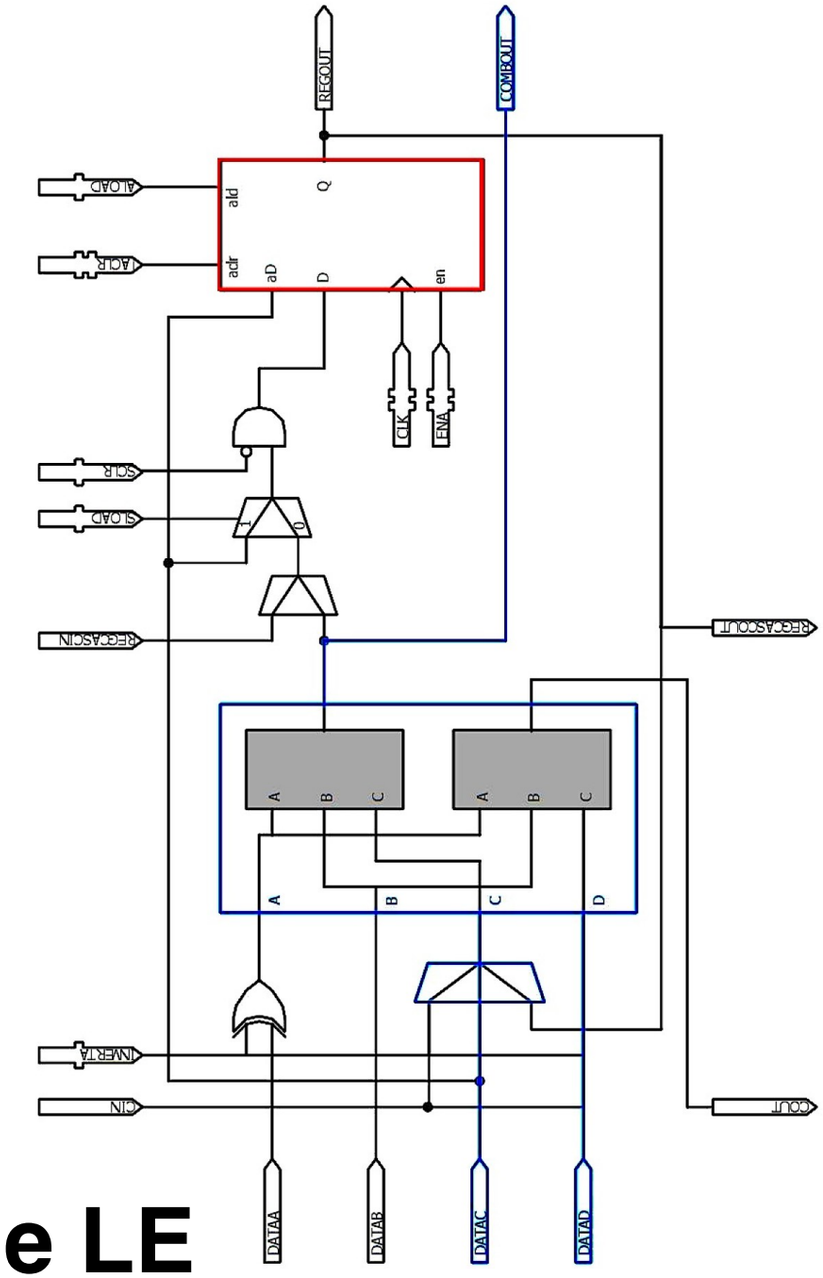
- Altera MAX V Complex Programmable Logic Device (CPLD) as platform
- Implementation of an 8-bit arbiter PUF
- Implementation of PUF by 2 independent buffers chains due to routing constraints in LUT





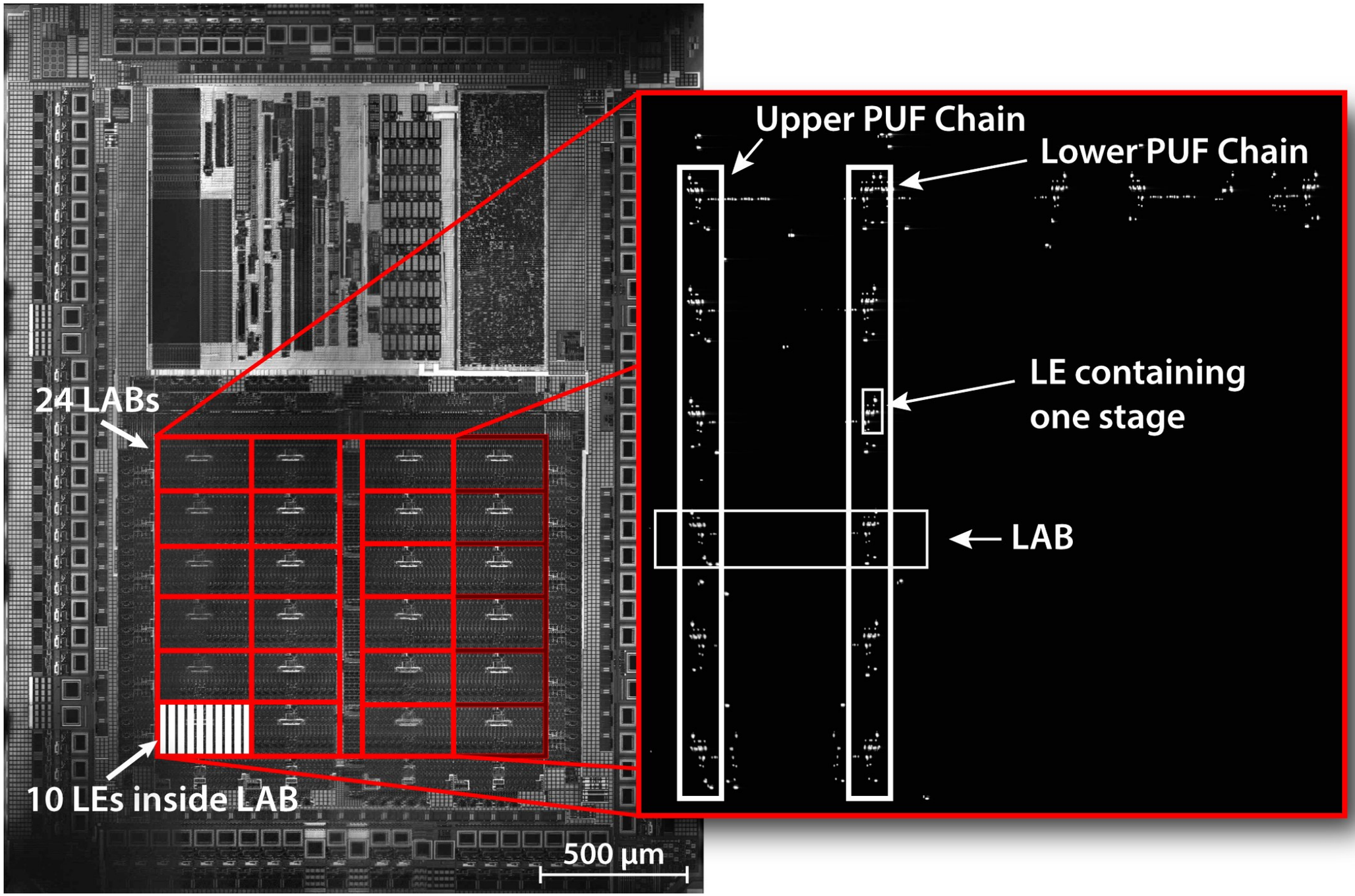
Overlay of Chip from Backside



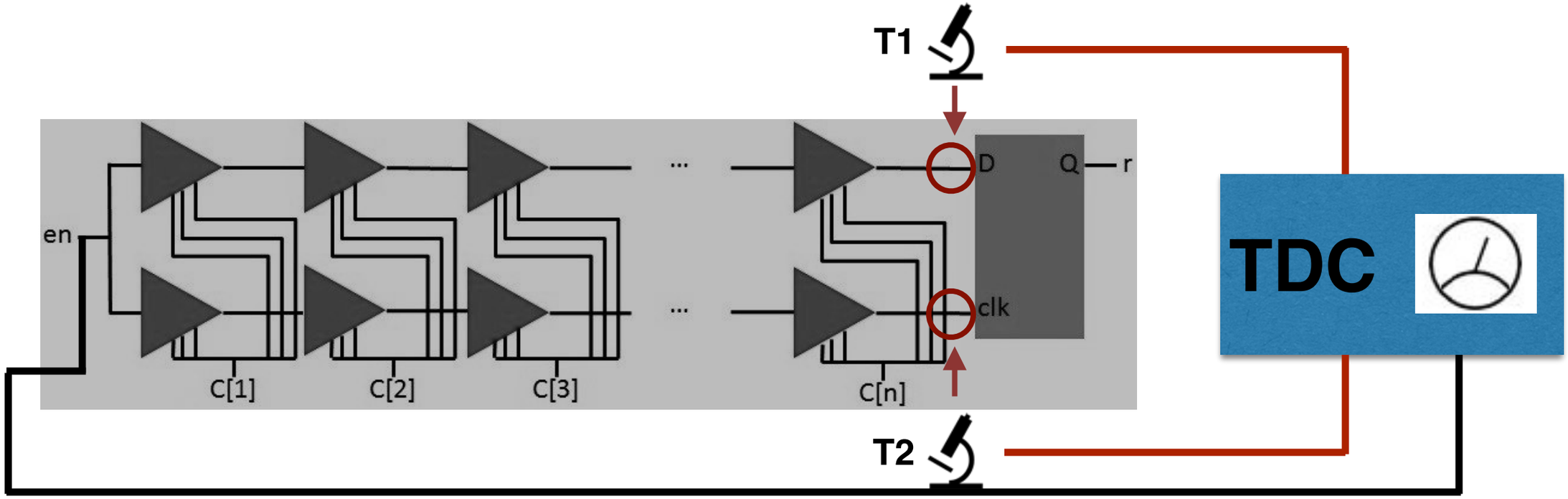


Single LE

Optical Emission of Arbiter PUF from IC Backside



Measurement of Delays (1)



- Measuring timing differences at the end of the chain on both paths

✳ **No response is needed!**

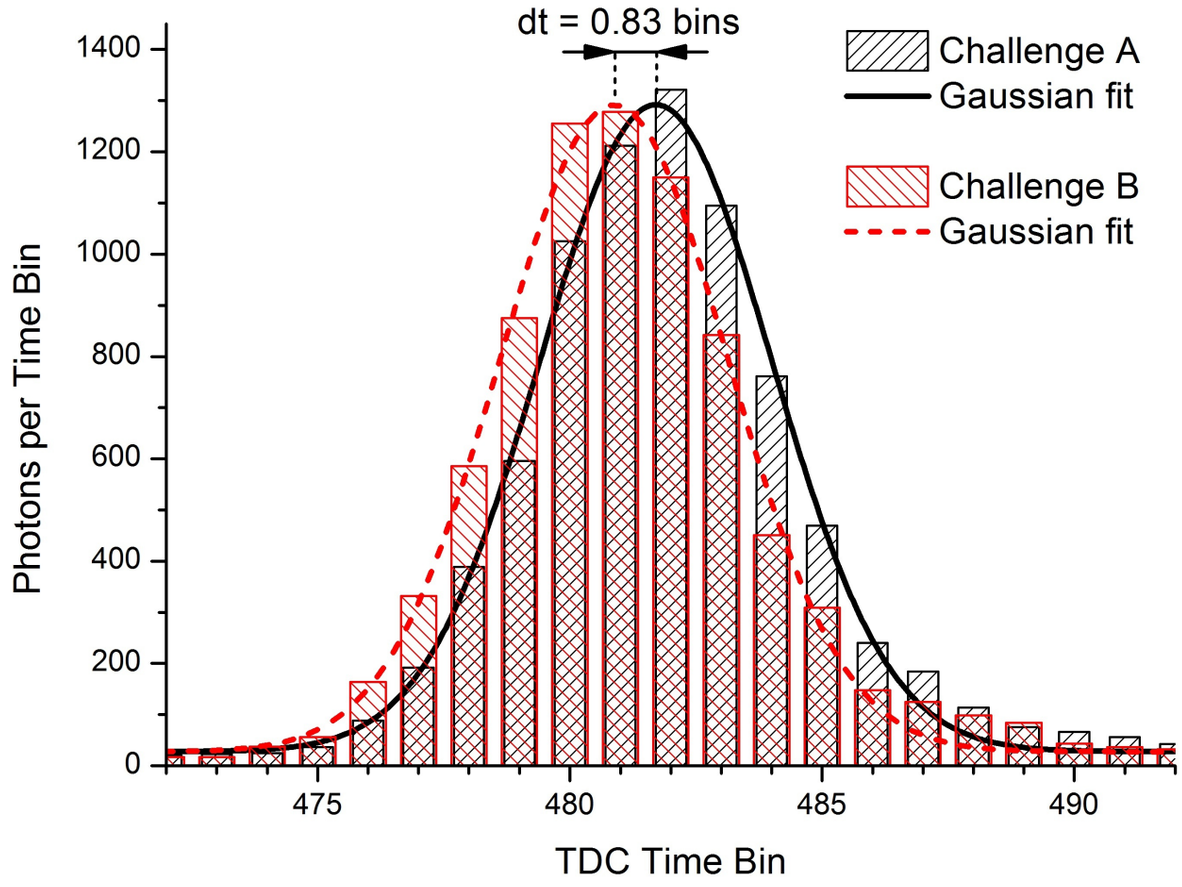
Measurement of Delays (2)

Characterization of the PUF with n+1 challenge: 1 reference challenge and **n** challenge with hamming distance one

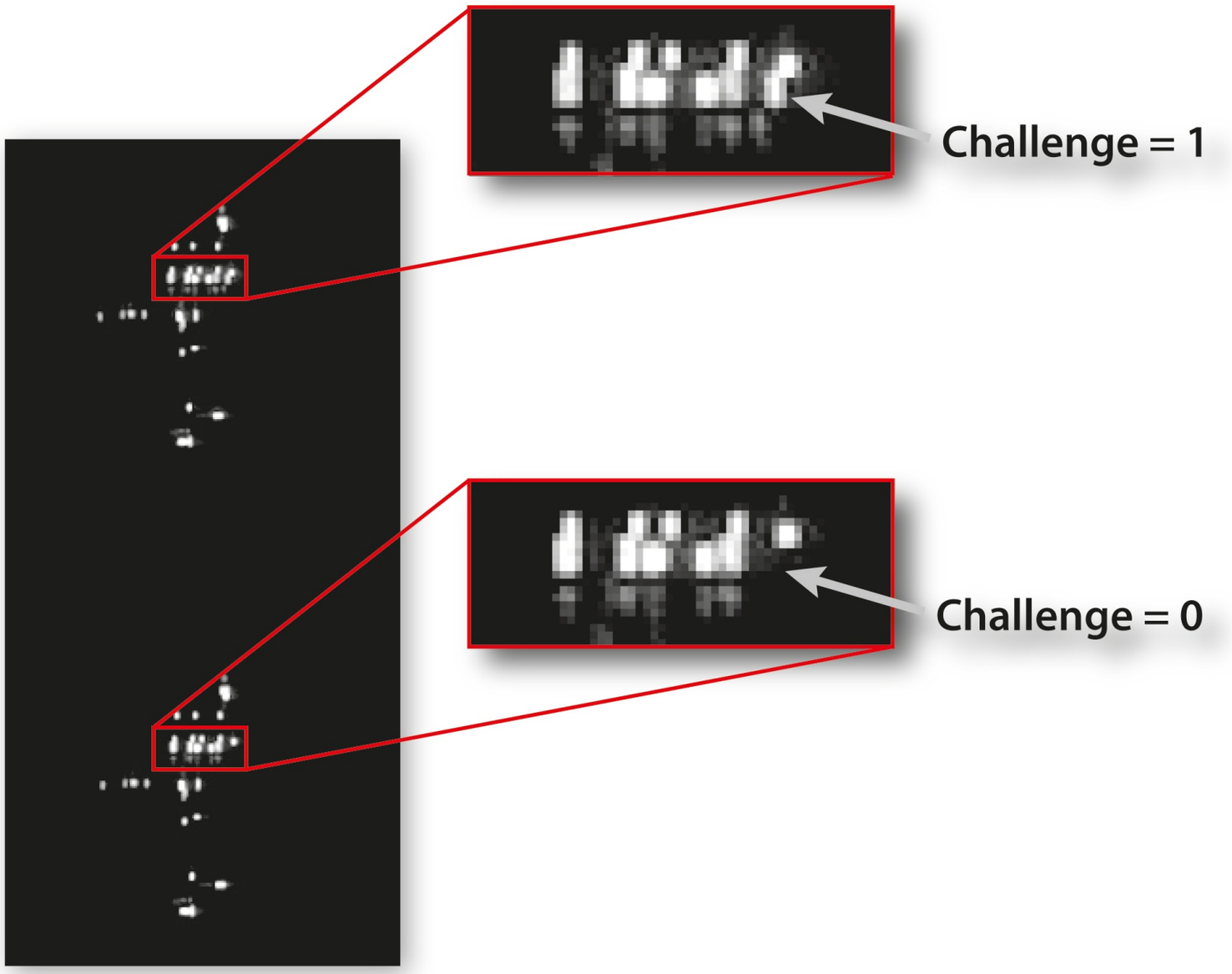
E.g.

C(0) = 0000…00 >> **Reference**
C(1) = 1000…00 >> **δ1 = +10 ps**
C(2) = 0100…00 >> **δ2 = +185 ps**
C(3) = 0010…00 >> **δ3 = -16 ps**

C(x) = 1110…00 >> +179 ps
measured value = +175 ps



Reading Challenge bits from emissions



Picosecond Imaging Circuit Analysis (PICA)

Conclusion

- Photonic emission analysis can break the security of arbiter PUF
- Far less challenges are required to characterize the PUF
- Linear increase of required challenges with number of PUF stages