Workshop on Cryptographic Hardware and Embedded Systems (CHES 2022)

Redshift: Manipulating Signal Propagation Delay via Continuous-Wave Lasers

Kohei Yamashita[1], Benjamin Cyr[2], Kevin Fu[2], Wayne Burleson[3], and Takeshi Sugawara[1]

[1]The University of Electro-Communications, Tokyo, Japan

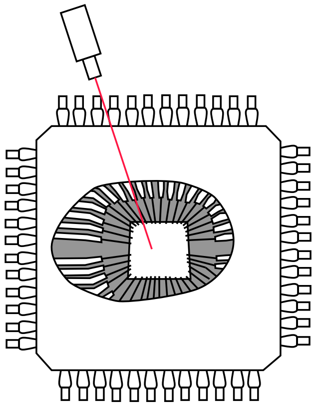
[2]University of Michigan, Ann Arbor, MI, USA

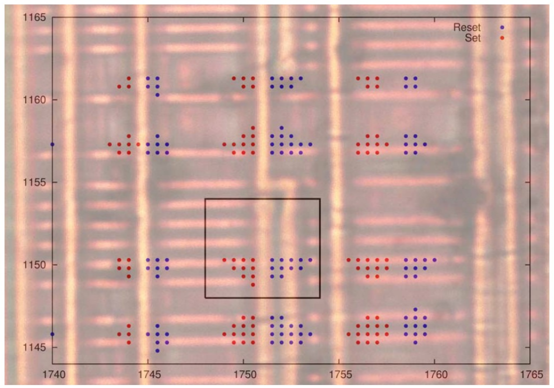
[3]University of Massachusetts, Amherst , MA, USA

This work is sponsored in part by the SECOM Science and Technology Foundation
and the Archimedes Center for Healthcare and Device Security

LFI: Laser Fault Injection

- Induces bit flips in digital circuits using a laser
- **Advantage**: Great spatial resolution for precise & stealthy attacks
  - Precise control over individual bits in memory
  - Impact is limited to a small region and detection-based countermeasure is challenging





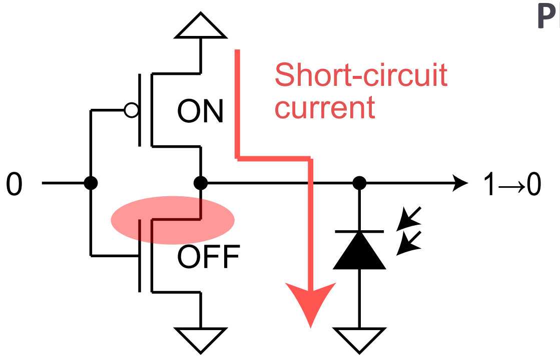
Selectively flipping bits in an SRAM (Roscian et al., FDTC 2013)

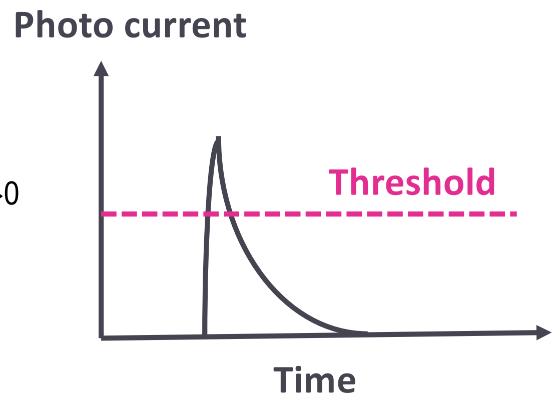
Red dots: bit-set faults

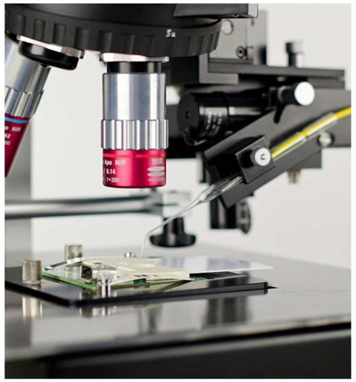
Blue dots: bit-reset faults

LFI: Laser Fault Injection cont.

- Successful bit flip needs a high peak power
  - A bit flip occurs only when a photocurrent exceeds a certain threshold
  - Commercial laser stations use high-power and short-pulse lasers, the state-of-the-art in optical engineering
- **Drawback**: expensive attack cost, typically >$100,000



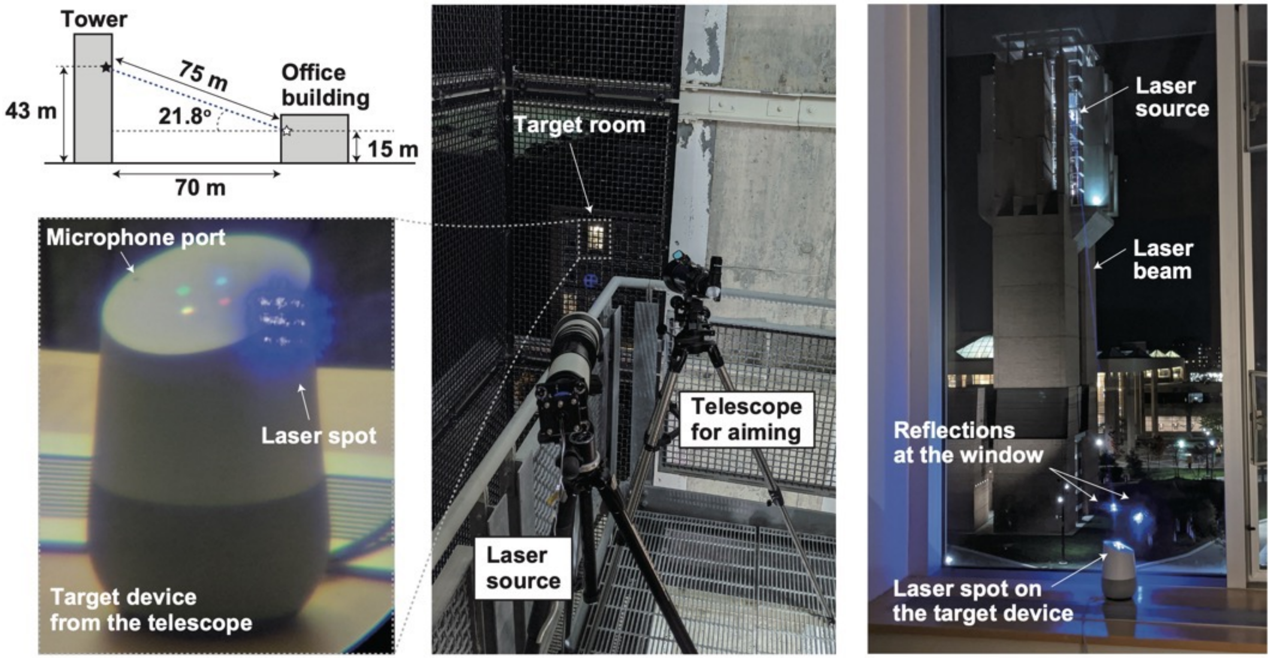




Riscure Laser Station
https://www.riscure.com

Light Commands: Extension of LFI to Microphones

- MEMS microphones receive fake audio when illuminated with amplitude-modulated laser
- Silent voice-command injection attack on smart speakers
- Extreme sensitivity
  - A laser pointer was sufficient

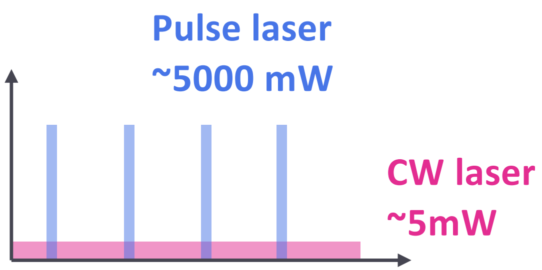


T. Sugawara, B. Cyr, S. Rampazzi, D. Genkin, and K. Fu, "Light Commands: Laser-Based Audio Injection on Voice-Controllable Systems," USENIX Security Symposium 2020.

Motivation and Contribution

- **The gap**
  - Conventional LFI needs an optimized high-power and short-pulse laser: ~5000 mW
  - A weak continuous-wave laser was sufficient for the microphone attack: ~5 mW

- **Conjecture**
  - Analog circuits can be more sensitive to light because they handle tiny voltage/current signals



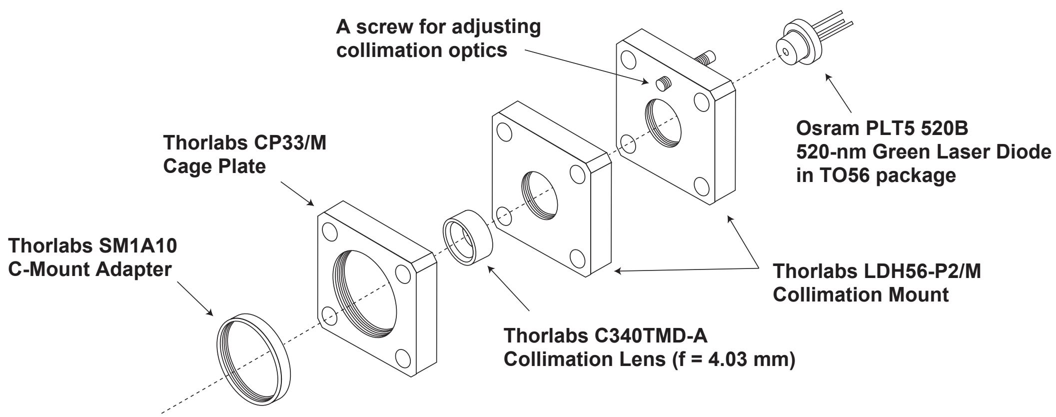
- **Contribution**
  - Redshift: Manipulating Signal Propagation Delay via Continuous-Wave Lasers

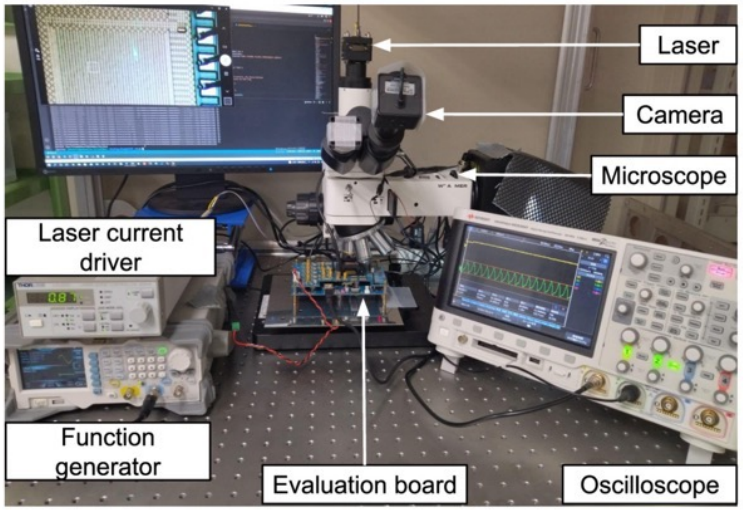
Outline

- **Intro**
- **Oscillator Frequency Shift**
  - Cheap laser setup
  - Frequency-manipulation experiments: ASICs and MCUs
  - Advantages
- **Application to PUFs**
  - Background: PUF-based key storage and its previous attack
  - State-biasing experiments: ring-oscillator and arbiter PUFs
  - State-recovery experiments
- **Discussion**
  - Causality
  - Countermeasures
- **Conclusion**

Cheap laser setup: a microscope with a laser diode

- A laser module with collimation optics compatible with a C-mount camera port
- Control the laser power through driving DC current, similarly to LED dimming
  - We use a laser-current deriver and an FG to programmatically control the laser

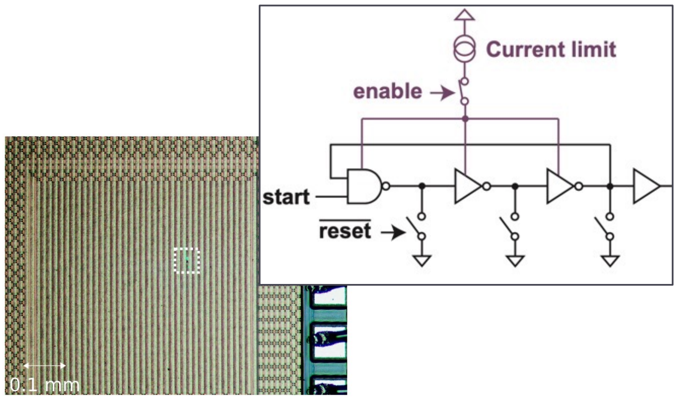




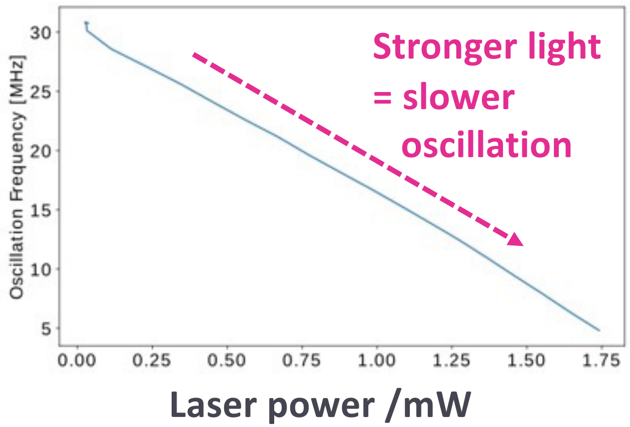
Experiment: Frequency shifts in ring oscillators in ASICs

- We put a depackaged ASIC chip under the microscope and aim the laser on an oscillator
- We gradually increase the laser power while measuring the oscillation frequency
- The frequency decreases almost linearly with injected laser power

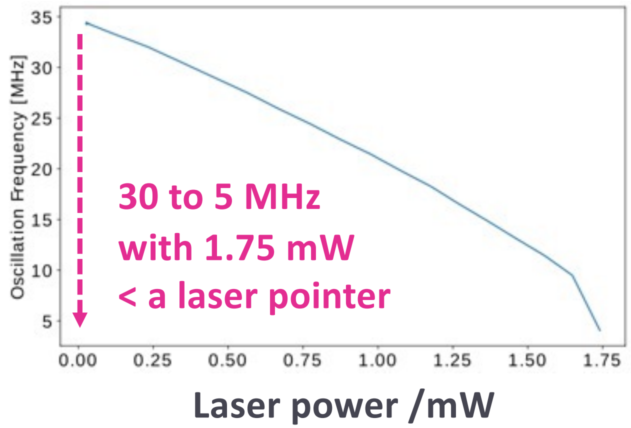
Target ring oscillator



180-nm ASIC

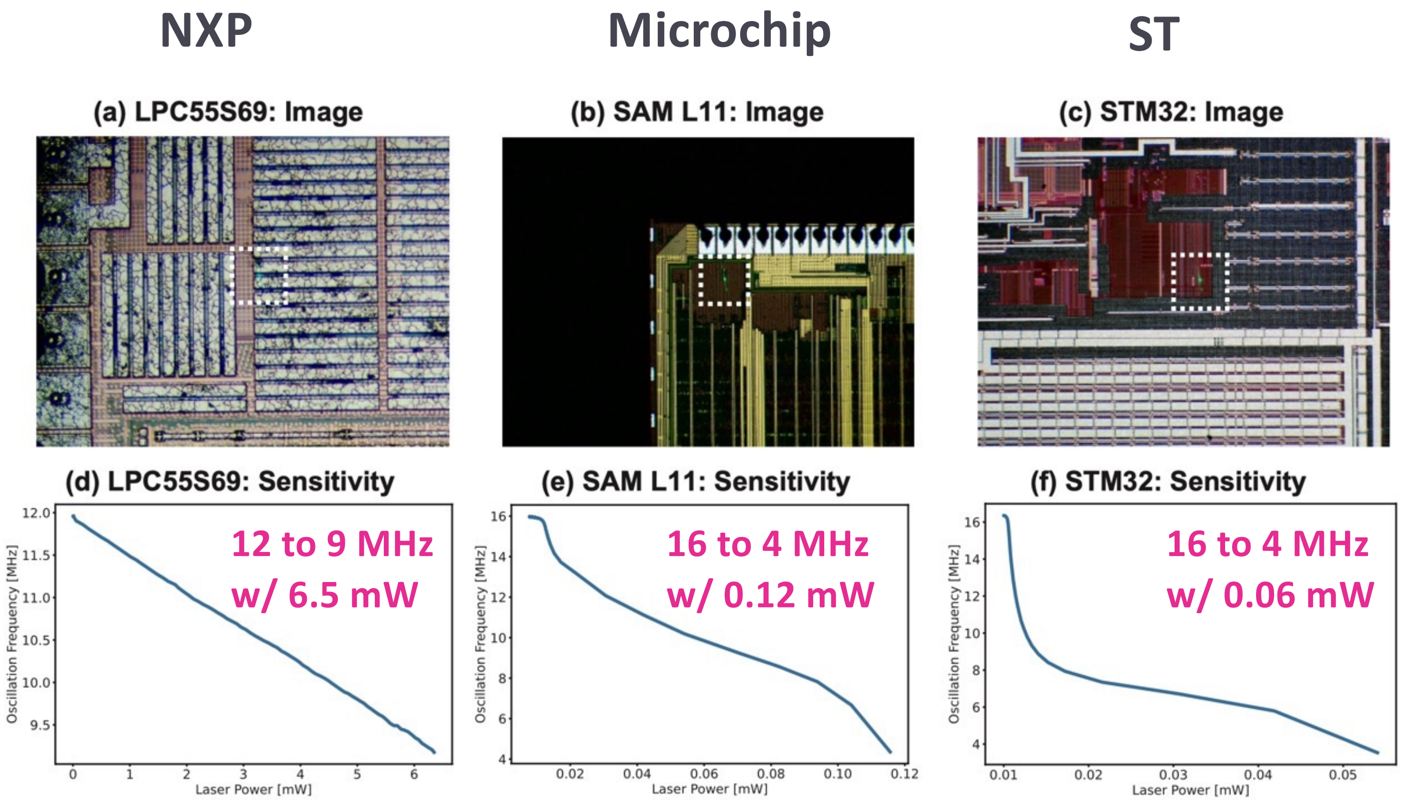


45-nm ASIC



Experiment: Frequency shifts in clock oscillators on MCUs

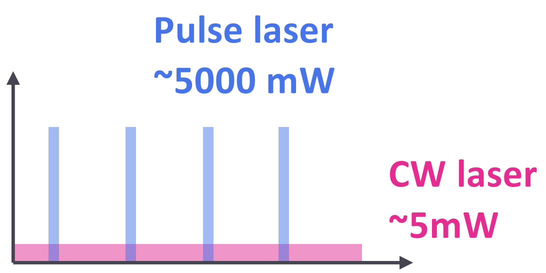
- Similar frequency shifts occur in clock oscillators on MCUs



Advantages

- **Laser Injection Attack on Delay-Sensitive Circuits**
  - Redshift extends the target of laser attacks from digital circuits to delay-sensitive analog circuits

- **Stealthiness**
  - The required laser power can be less than 1/1000
  - It can be below the threshold of laser detectors configured for pulse lasers



- **Cheaper Setup**
  - Our setup is around $5,000, which fits within the **Standard** equipment in CC
  - Cf. conventional laser station with >$100,000, categorized as **Specialized**

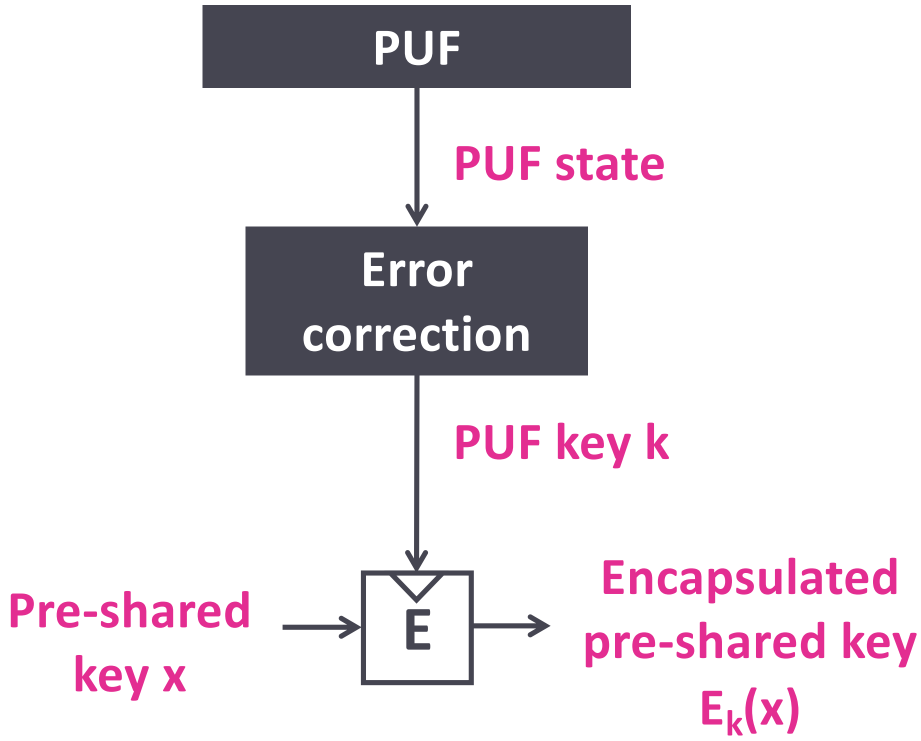
How can an attacker exploit Redshift?

- **PUFs**
  - The latter part of this talk

- **Other possible extensions**
  - RNG: disrupt entropy-source oscillators
  - Clock glitching: underclocking can cause synchronization errors
  - Evading sensor-based countermeasures
    - Laser illumination can cause false positives and/or negatives
    - On-chip sensors (e.g., an EM-probe detector) use oscillation frequency as a sensing principle

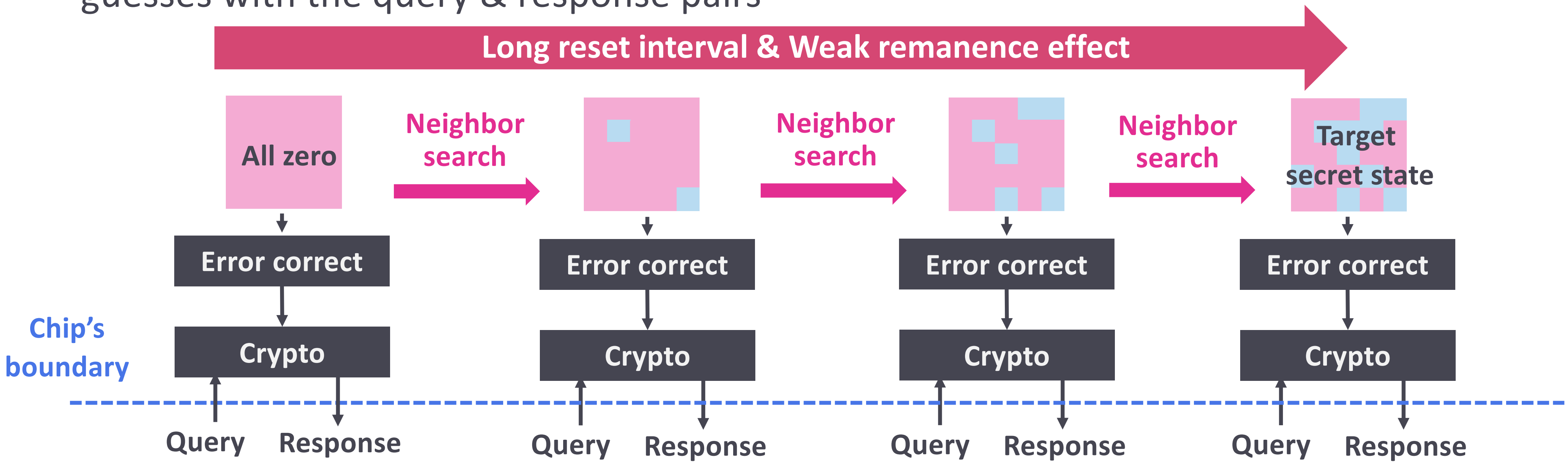
PUF and PUF-based key storage

- **PUF state**
  - A device-unique ID generated by a PUF from manufacturing variation
- **PUF key**
  - A cryptographic key from a PUF state with error correction
- **PUF-based key storage**
  - Encapsulation a pre-shared key with a PUF key
  - The keys appear only after the chip is turned on, providing the protection against reverse engineering



Zeitouni et al.'s SRAM-PUF attack exploiting remanence effect*

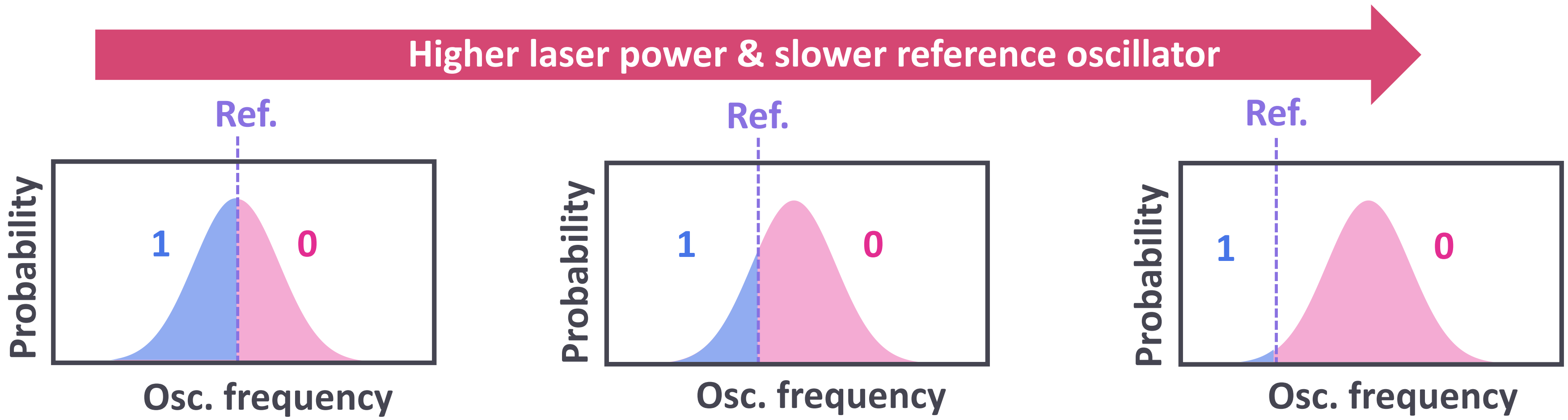
- Bias SRAM PUF states by gradually increasing the widths of reset pulses
- Recursively recover intermediate states with neighbor search while checking the guesses with the query & response pairs



*S. Zeitouni, Y. Oren, C. Wachsmann, P. Koeberl, and A.-R. Sadeghi, "Remanence decay side-channel: The PUF case," IEEE Trans. IFS 2016.

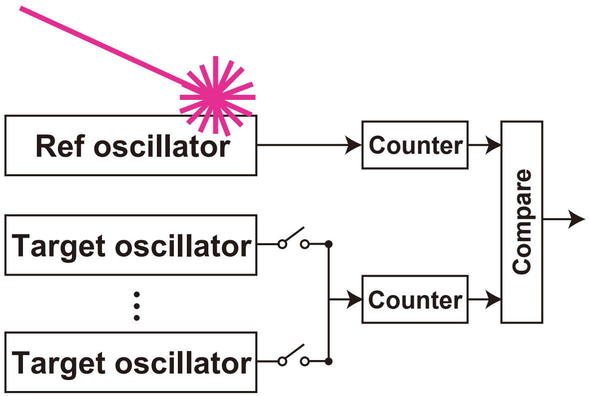
Extension with Redshift

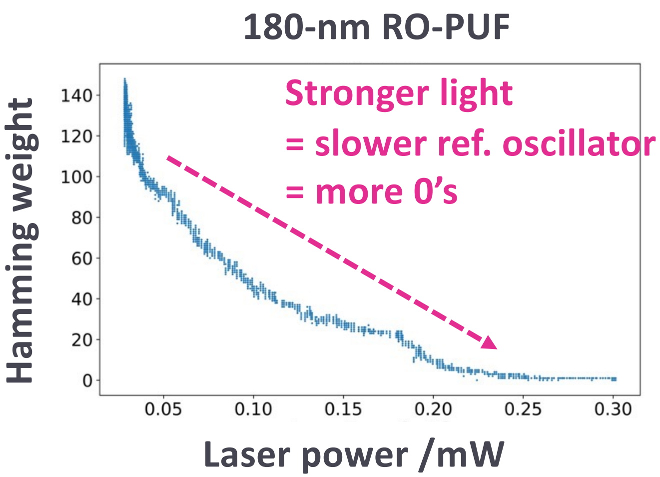
- **Idea: use Redshift to induce similar biases in delay PUFs**
- Simple target: RO-PUF with a fixed reference oscillator
  - Outputs 0 if a target oscillator is faster than the reference oscillator and 1 otherwise
- Slowing down the reference oscillator results in the bias in 0/1 population

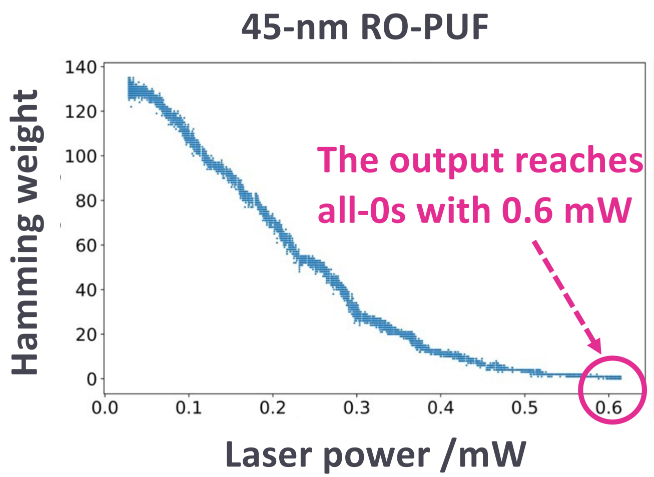


Experiment: biasing RO-PUF state

- Target: RO-PUFs in our ASIC chips that use the the previous ring oscillators
- Illuminate the reference oscillator while the PUFs generate 256-bit states
- HW decreases as we increase laser power

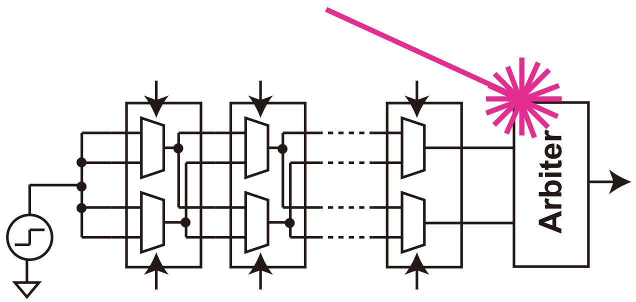


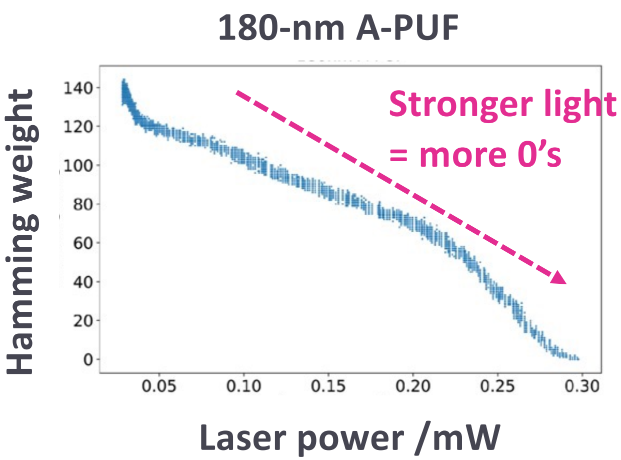


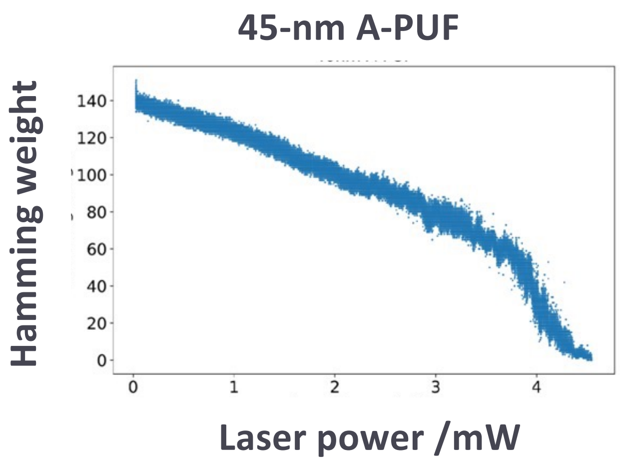


Experiment: biasing A-PUF state

- Redshift causes similar HW bias in A-PUF
  - Laser on an arbiter circuit makes one path slower than another
  - HW decreases as we increase laser power







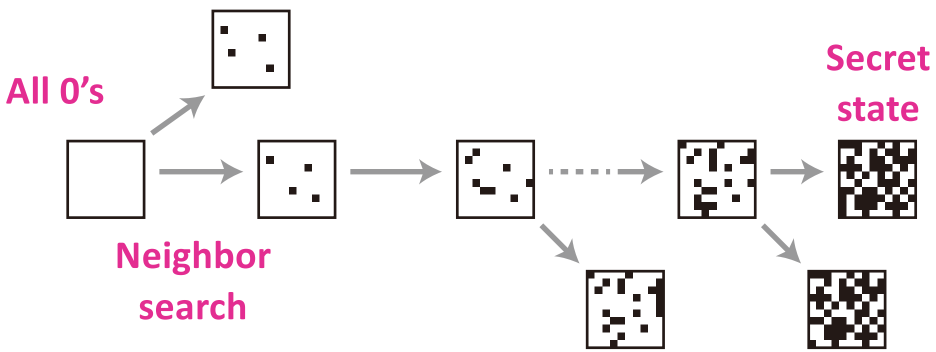
State-recovery experiments

- **Verifies state-recovery attack with error correction & crypto**
  - Simple error-correction scheme for generating a 128-bit key
    - Stable-bit selection & bitwise majority voting
  - Crypto service
    - AES-128 challenge & response

- **Measurement**
  - Illuminate the target PUF with a laser and query the crypto service 5 times for each laser power
  - Increment the laser power and repeat

State-recovery experiments cont.

- Search finishes within 1sec in all the cases
- The distance in neighbor search is the computational bottleneck: $\binom{128}{d_{max}}$
  - The next states is always found within 1- or 2-bit distances

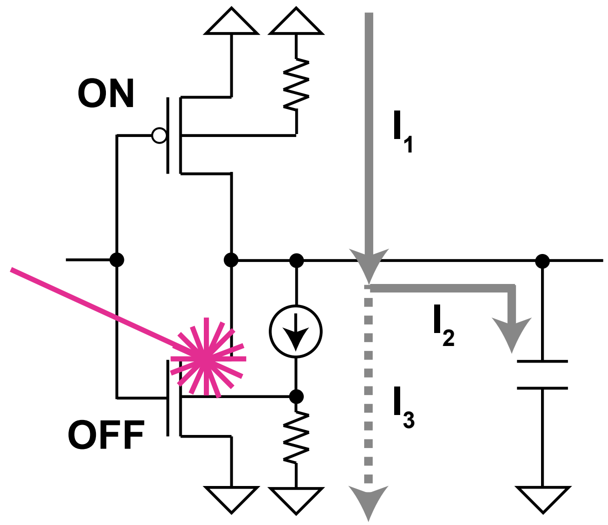


Target	Exec time [msec]	Max distance to next states d_{max} [bits]
180-nm RO-PUF	931	2
40-nm RO-PUF	22	1
180-nm A-PUF	39	1
40-nm A-PUF	233	1

Physical Causality

- **Conventional model with a current source**
  - A part of the driving current is wasted as photocurrent, increasing the time needed to charge the load capacitance
- **Laser-Assisted Device Alteration (LADA)**
  - Changes the transistor property with continuous-wave laser illumination for LSI failure analysis

Low-to-high transition



Countermeasures

- **On-Chip sensors for continuous-wave lasers**
  - Integration over time
- **Avoid a fixed reference oscillator in RO-PUF**
  - Pair-wise comparison, e.g., chaining*
- **Detecting a wrong PUF Keys**
  - Detect unsuccessful key generation and suspend crypto services
- **Hardware obfuscation**
  - Hide the PUF key-generations details needed for running the attack

*D. Merli, F. Stumpf, and C. Eckert, "Improving the quality of ring oscillator PUFs on FPGAs." *WESS 2010*

Conclusion

- **Summary**
  - A new laser attack that slows down delay-sensitive circuits using continuous-wave laser
  - Its application to PUF state-recovery attack
- **Future works**
  - Extending Redshift to other applications and analog circuits
  - Further verification of the causality through experiments and simulation

Thank you for listening!

Questions?