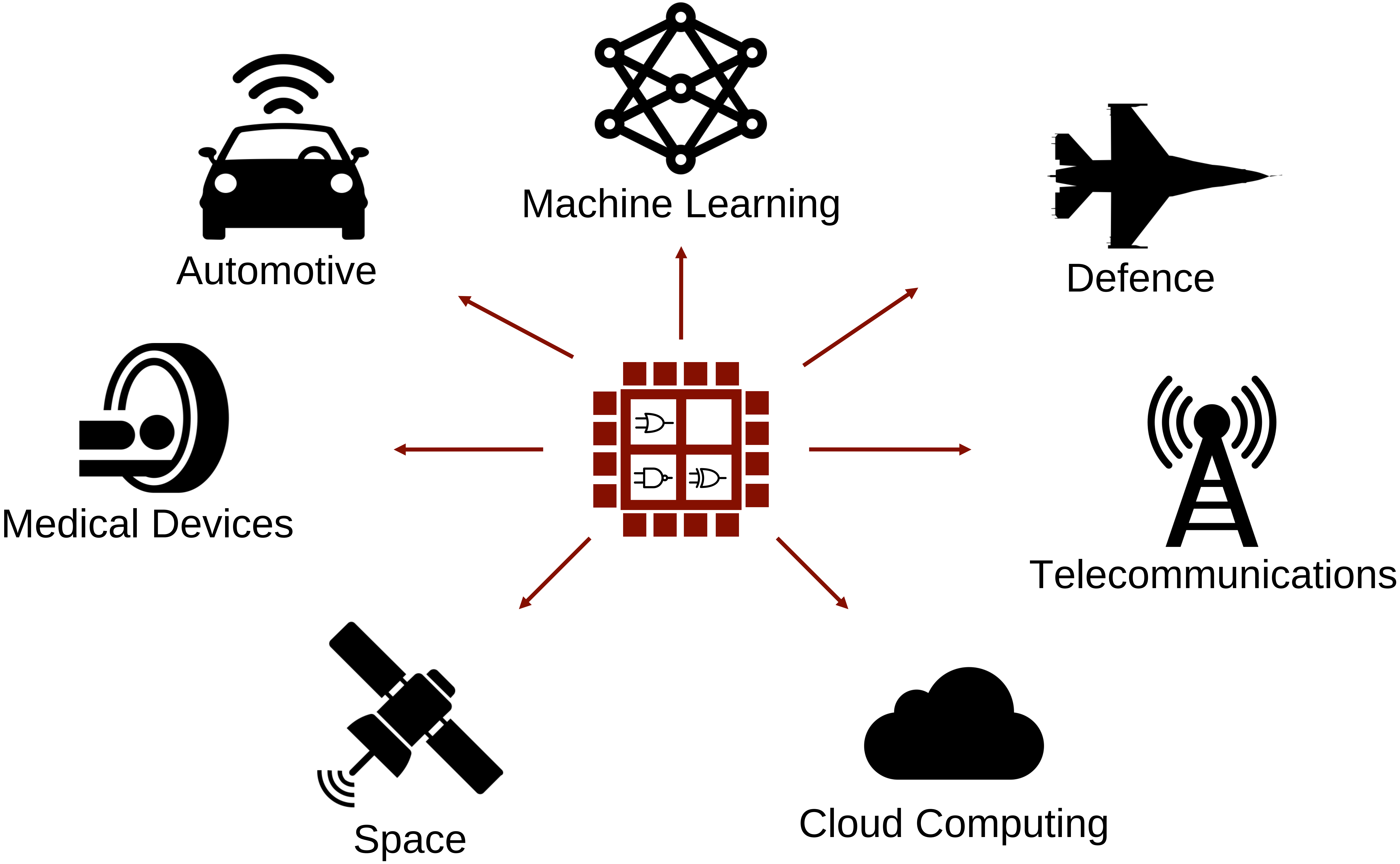
Applications of optical analysis in Reverse-Engineering

Presented by: Mir Tanjidur Rahman
Dr. Navid Asadi

Physical Inspection and AttacKs on ElectronicS (PHIKS)

Evaluating the security of Field Programmable Gate Arrays (FPGAs) as case studies

Field Programmable Gate Array (FPGA)



Machine Learning

Automotive

Defence

Medical Devices

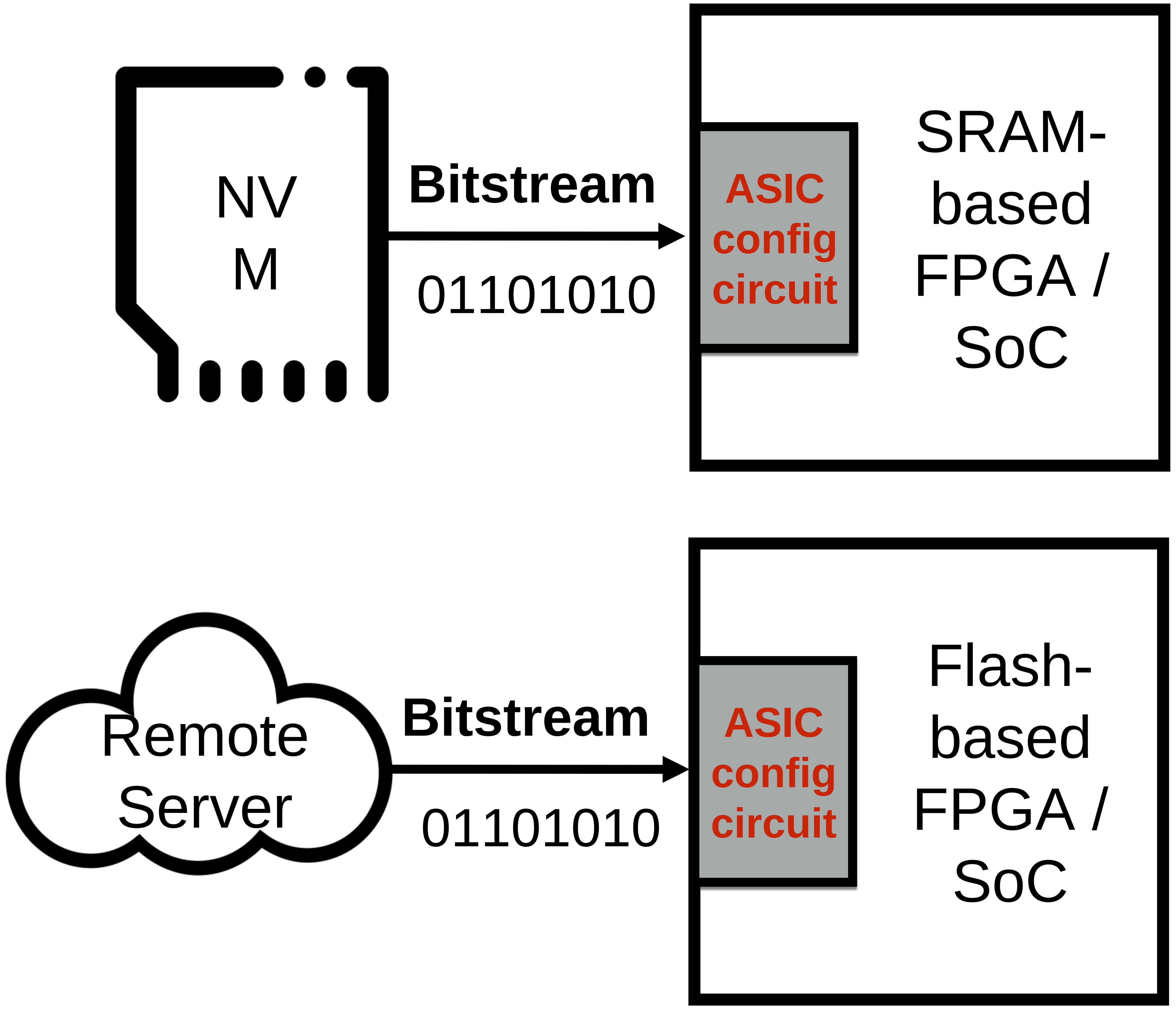
Telecommunications

Space

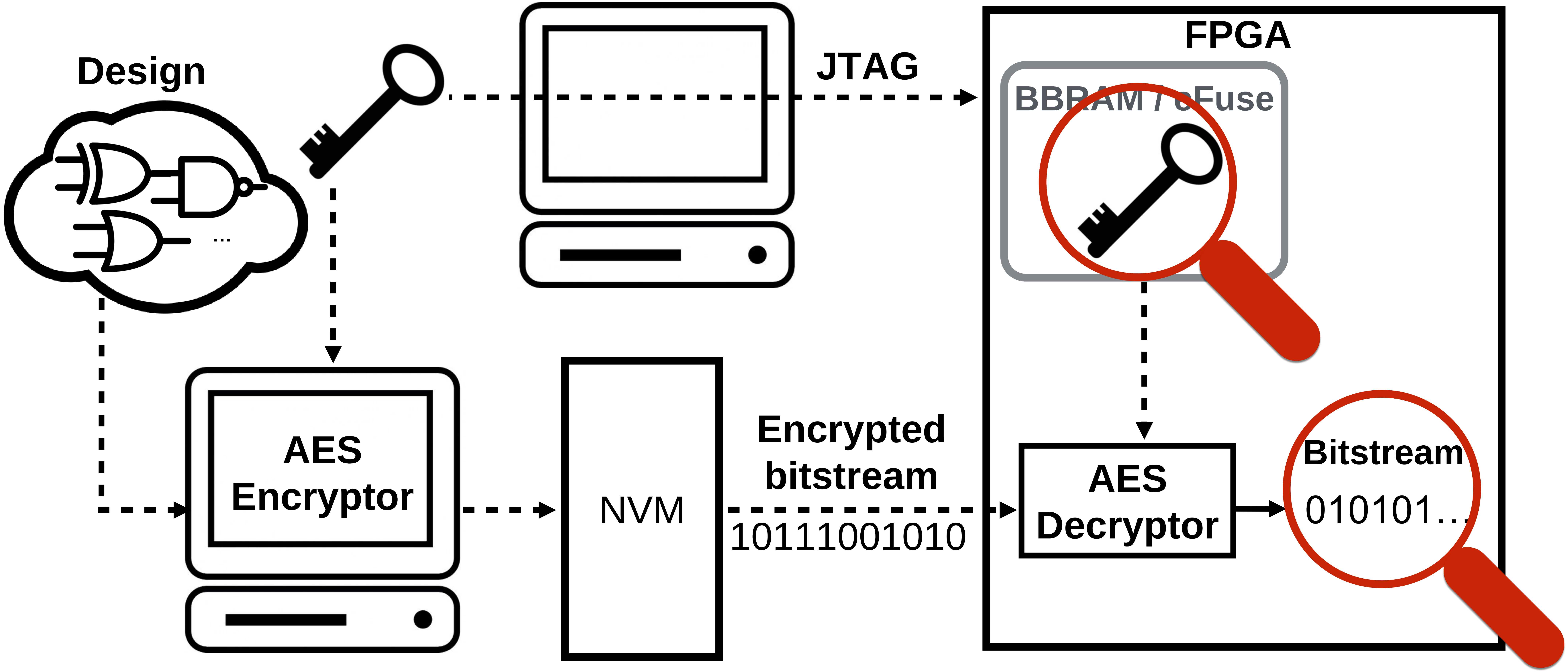
Cloud Computing

Security of FPGAs

- **Bitstream:** configuration data containing Intellectual Property (IP) and secrets for reconfigurable hardware
- The bitstream can be loaded in the field (**adversarial environment**)
- **Threats:** cloning, reverse-engineering, tampering or spoofing



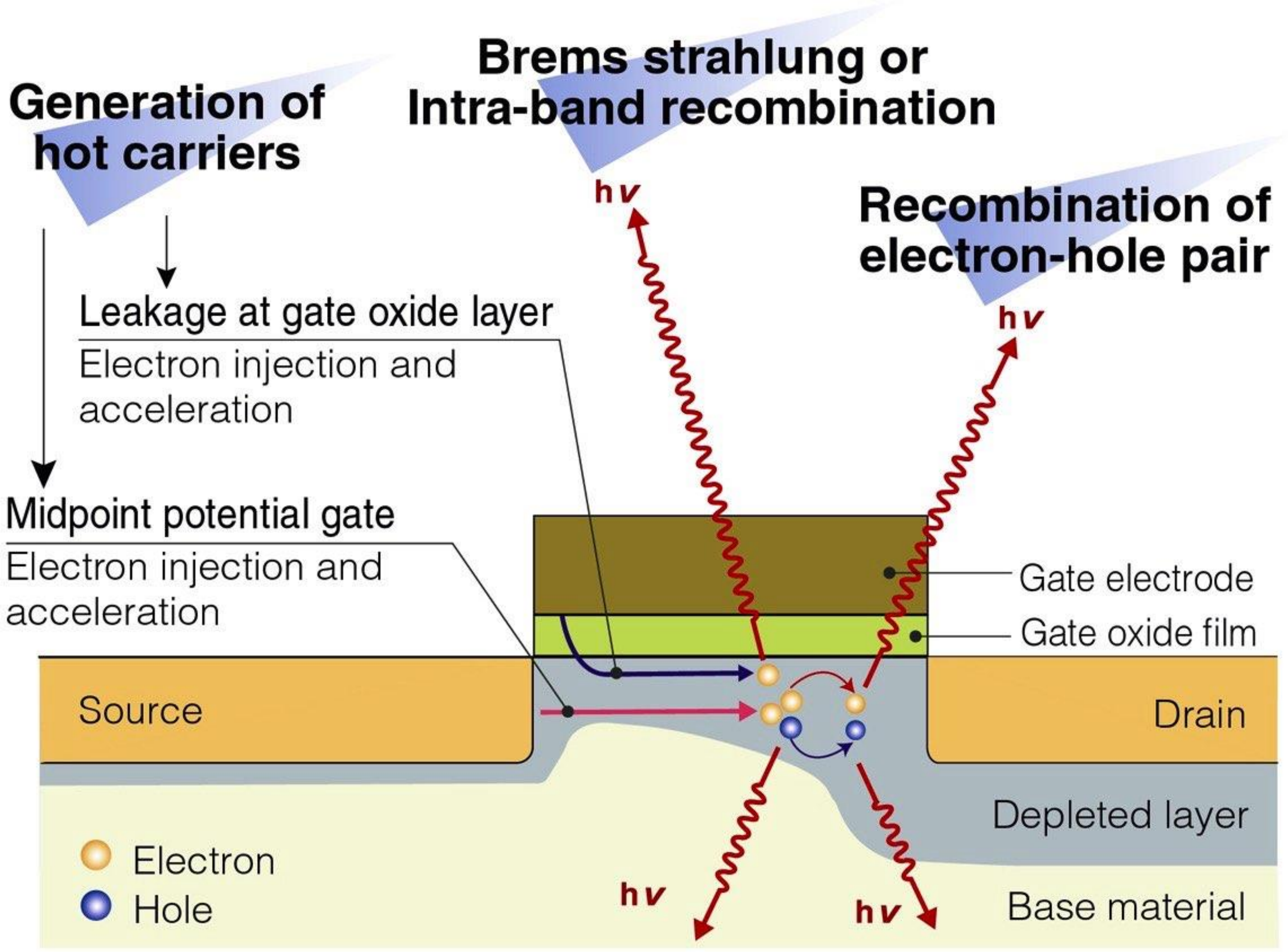
Case Study: Attacking Bitstream Encryption of FPGAs



Photon Emission Analysis

Mechanism of Photon Emission

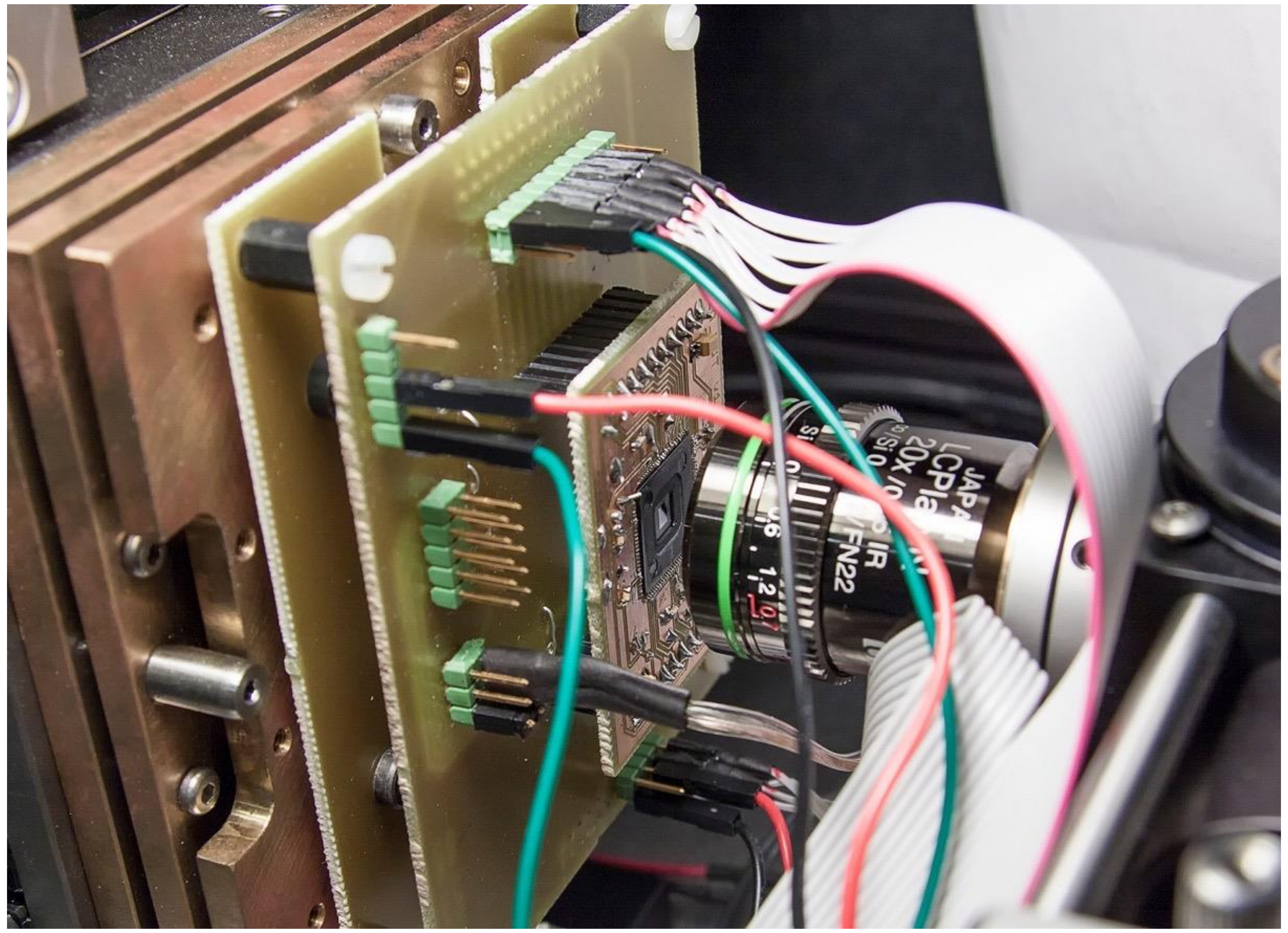
- As carriers are accelerated by electric fields they gain kinetic energy, which is then released via generating photons.
- In CMOS transistors this hot-carrier luminescence takes place at the drain edge where the source-drain electric field is most intense and predominantly in n-type transistors as electrons are more easily accelerated than holes.
- In the case of CMOS-inverter, the vast majority of photons are generated when the input switches from 0 to 1 >> data dependent
- The photon generation rate is governed primarily by the supply voltage and the switching frequency of the transistor under observation.



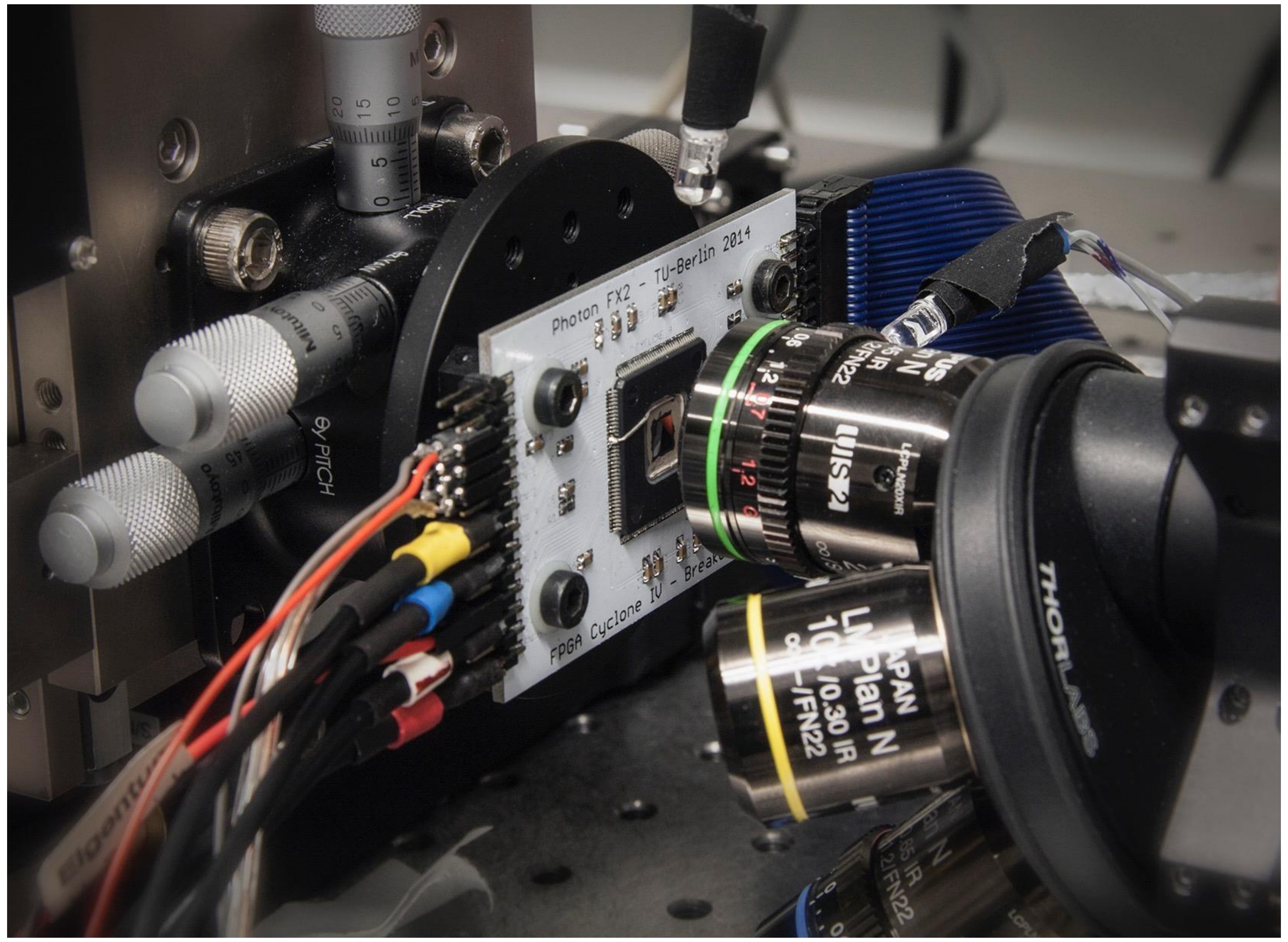
Generation of hot carriers
Brems strahlung or Intra-band recombination
Recombination of electron-hole pair
hν
hν
Leakage at gate oxide layer
Electron injection and acceleration
Midpoint potential gate
Electron injection and acceleration
Gate electrode
Gate oxide film
Source
Drain
Depleted layer
Electron
Hole
hν
hν
Base material

Backside Access

- **Older package technologies like QFPs should be decapsulated and soldered upside down on a custom PCB**



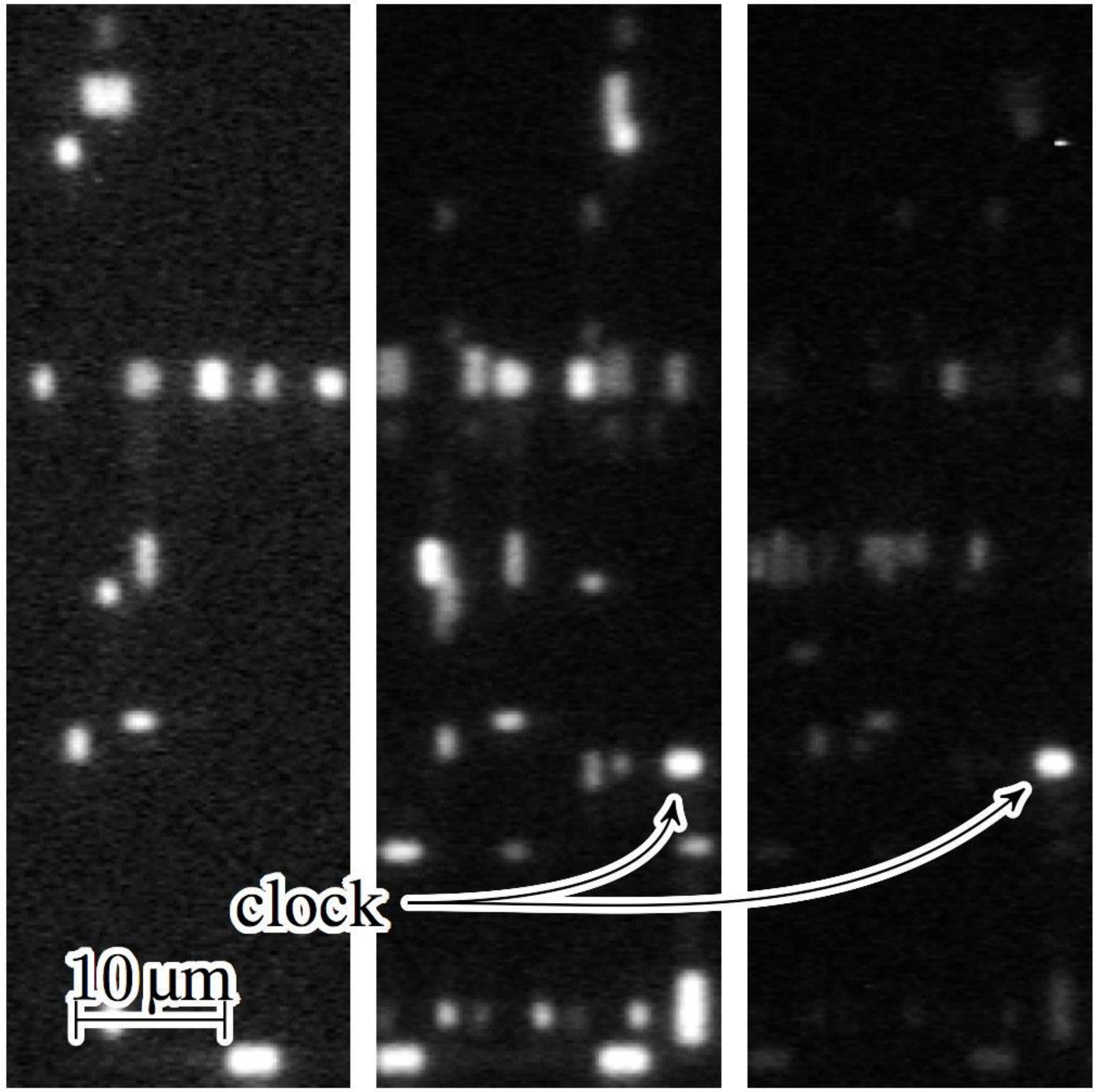
Altera MAX V CPLD (180 nm)



Altera Cyclone IV FPGA (60 nm)

Emission of Combinatorial vs. Sequential Logic

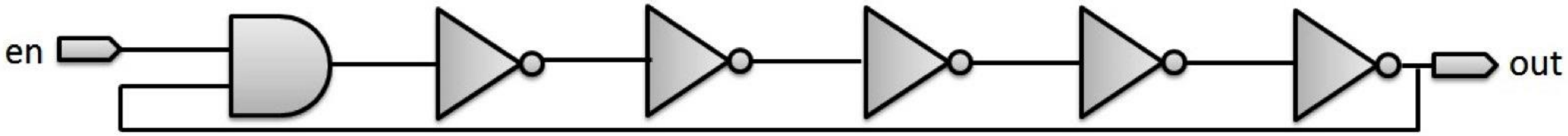
- A Combinatorial Logic: **AND**, **OR**, **NOT**, **XOR**, etc.
- Sequential Logic: Counter, Shift Register, State Machines, etc.
- **Presence of Clock buffers in Sequential Logic**

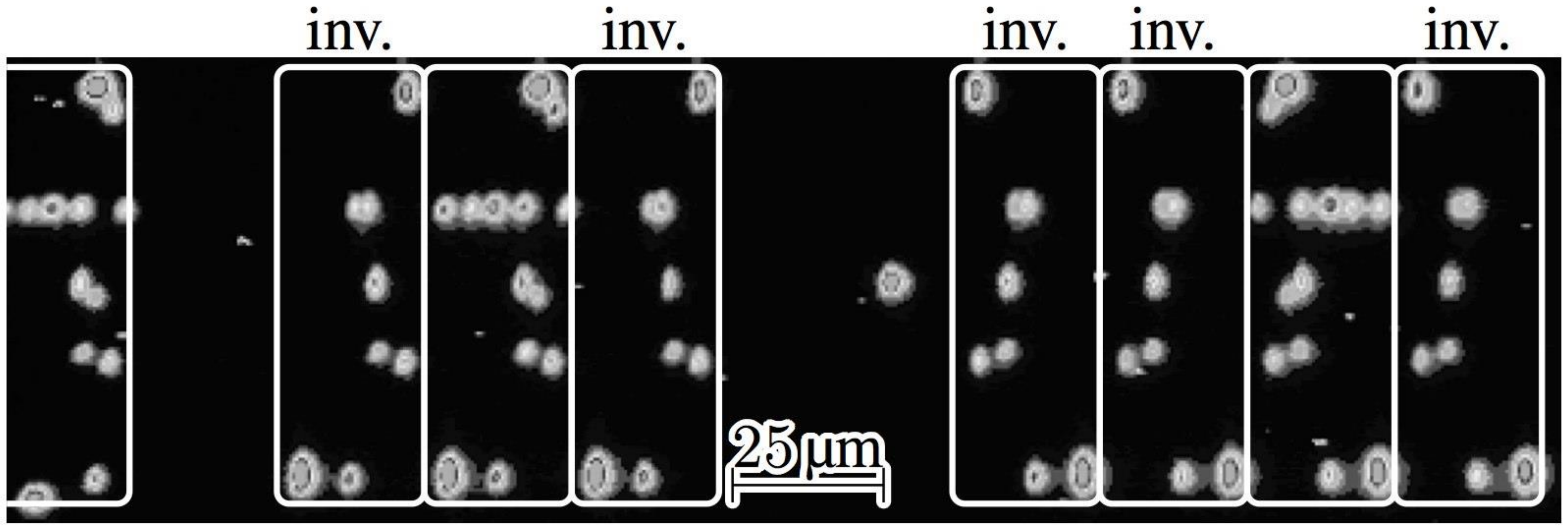


Altera MAX V (180 nm)

Example (1): Emission of a Ring-Oscillator

- Identical Switching Frequency by all LEs
- Switching frequency independent and generally higher than clock frequency
- **Applications**: TRNG and Internal Clocks

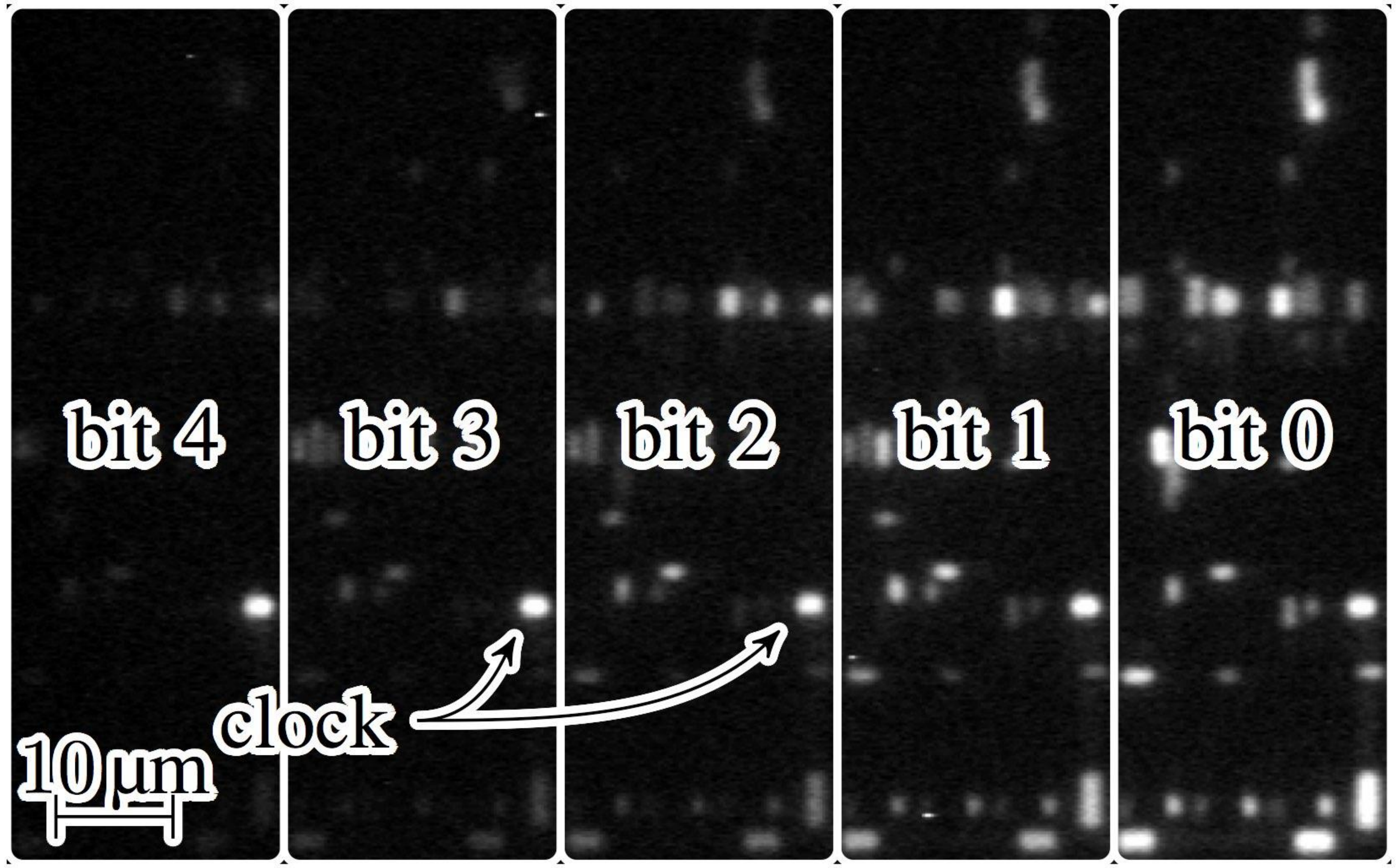




Altera MAX V (180 nm)

Example (2): Emission of a Binary Counter

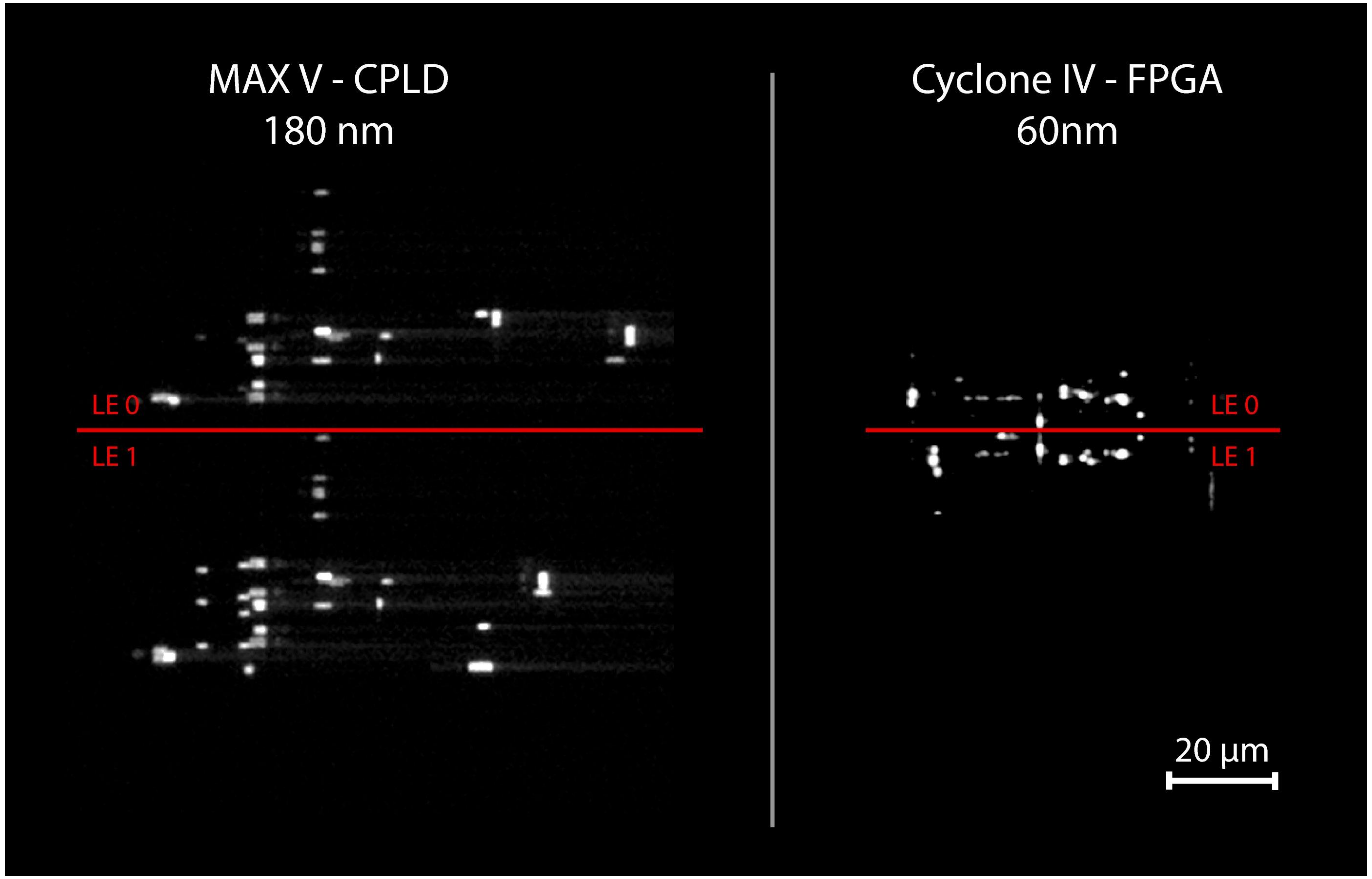
- n-bit counter = n clocked registers + some combinatorial logic
- Identical switching frequency of the clock for all registers
- **Applications**: Delay and Timing circuits such as asynchronous protocols



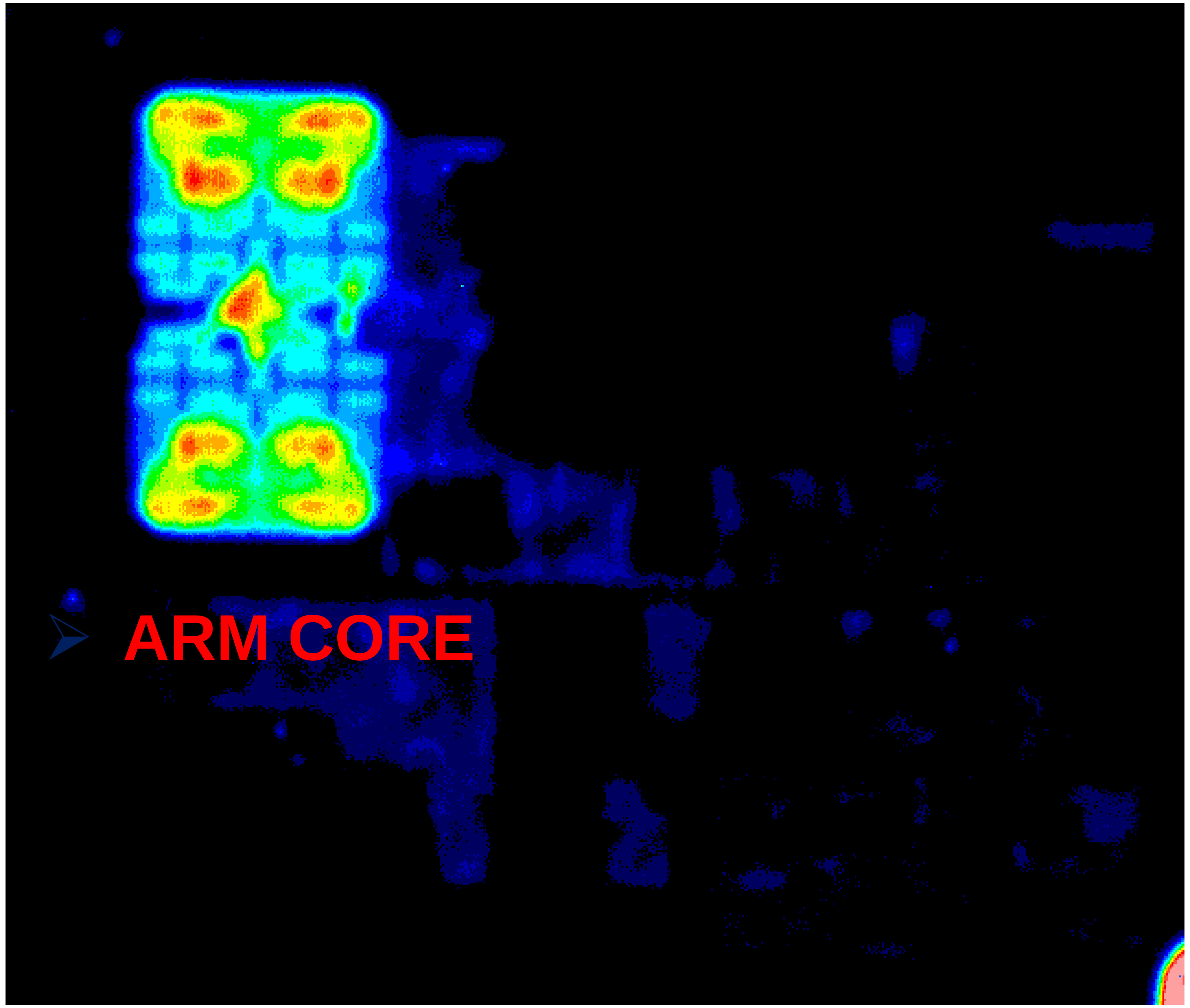
Altera MAX V (180 nm)

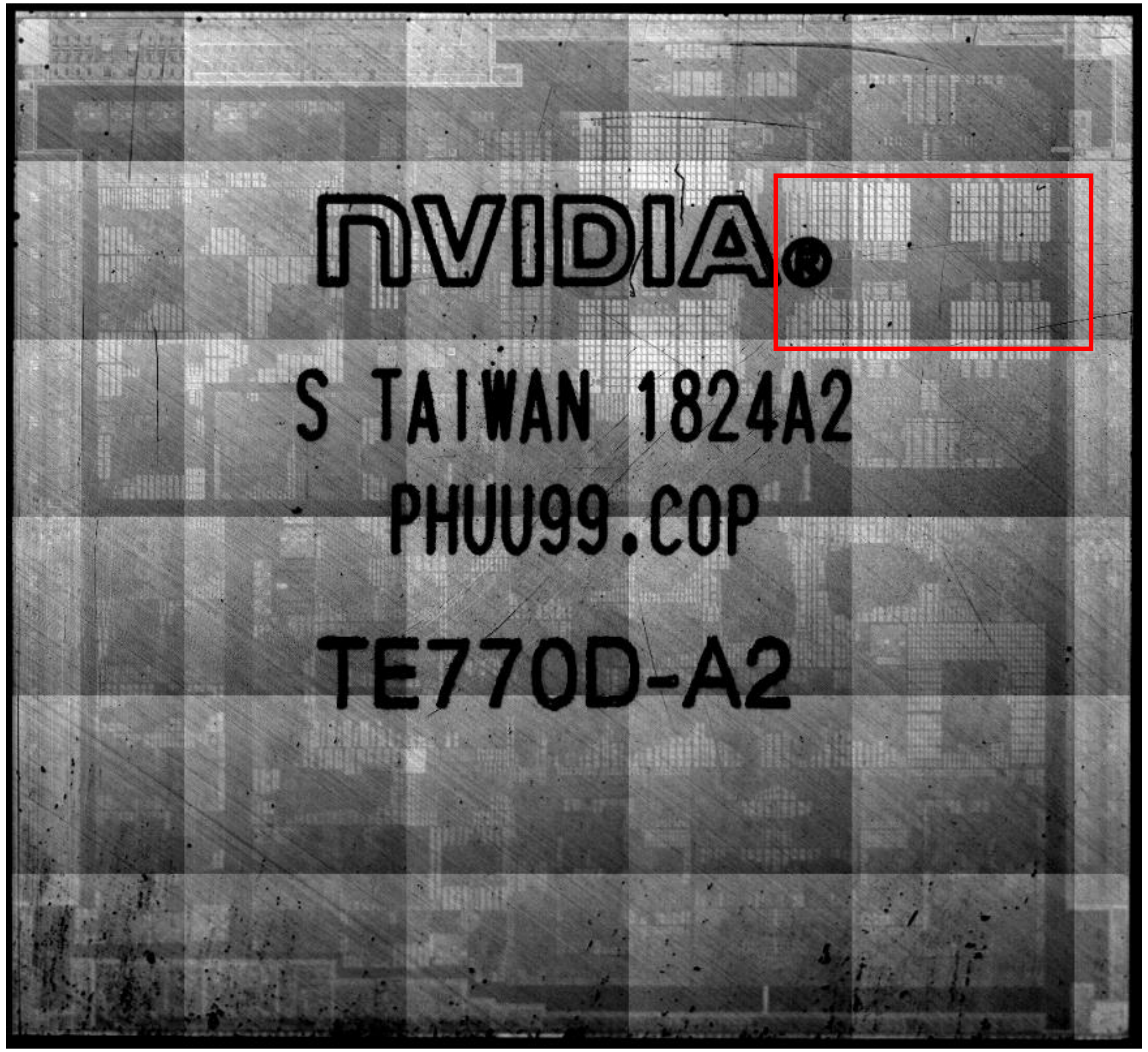
Impact of Technology size on Photon Emission

- Lower supply voltage for smaller technologies >> less photon emission rate
- Smaller technology >> harder to resolve a transistor
- Large space between transistors in LUTs >> resolving of transistors still possible for the attacker

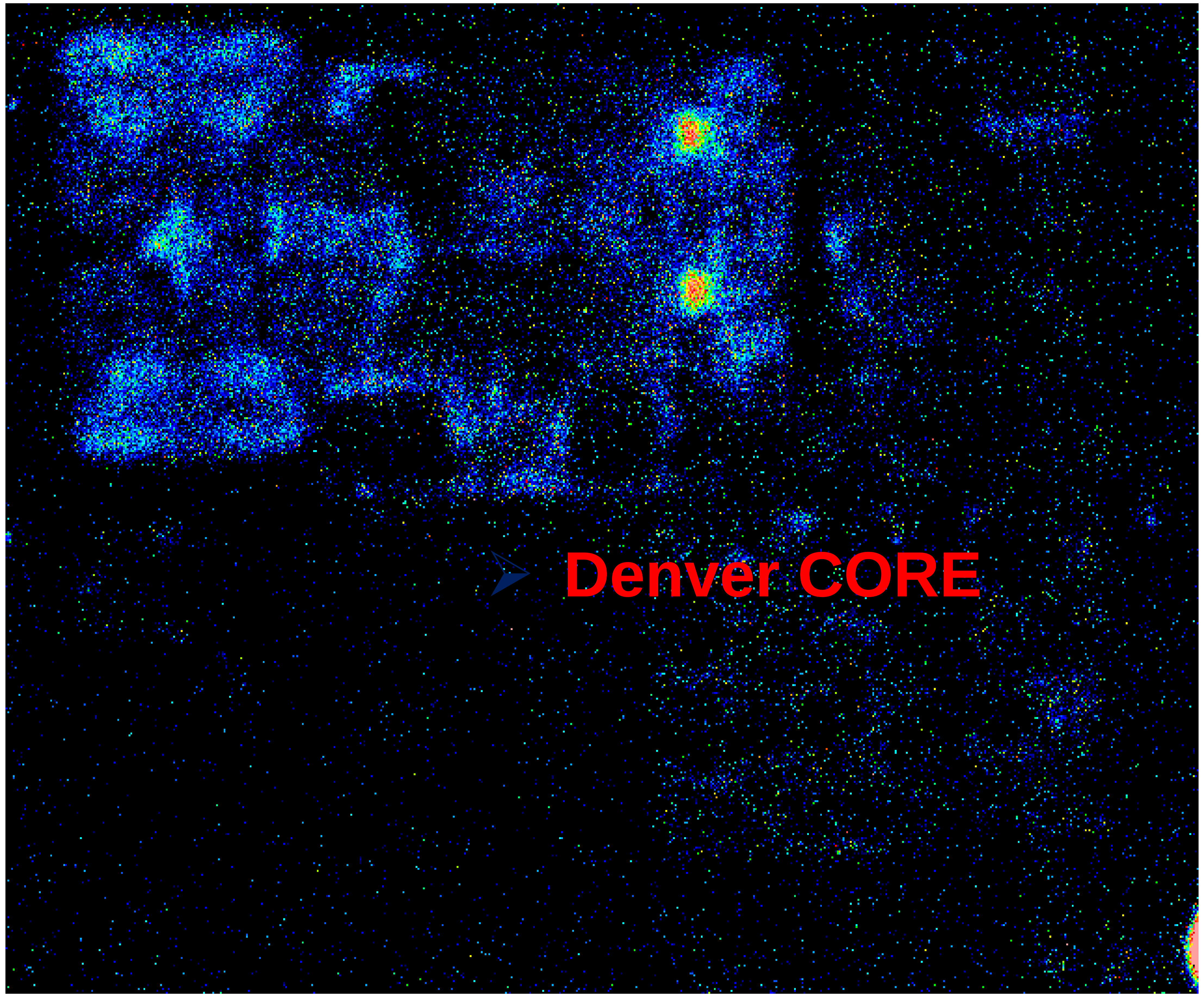


Core Localizaiton in NVIDIA AI CHIP

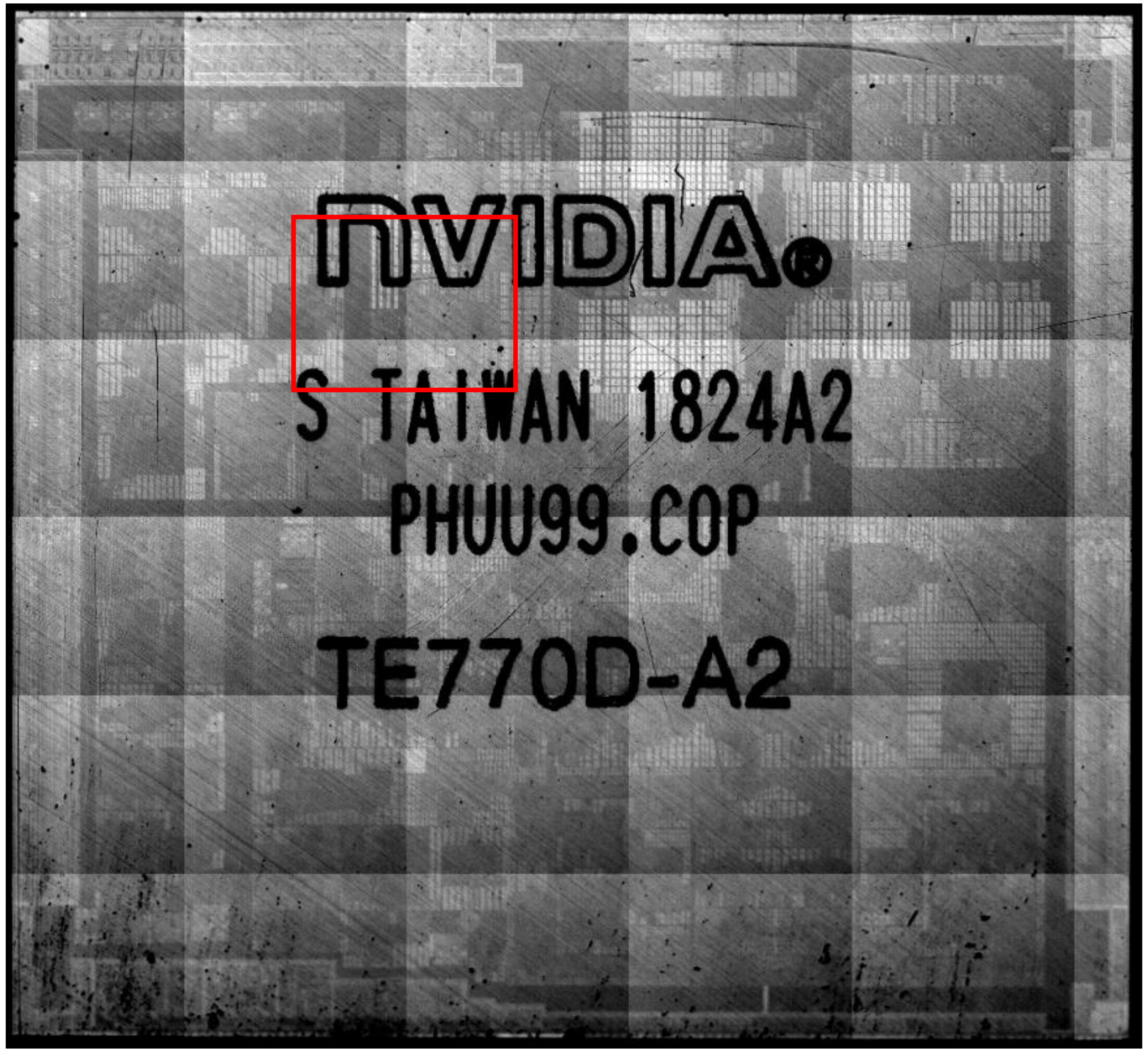




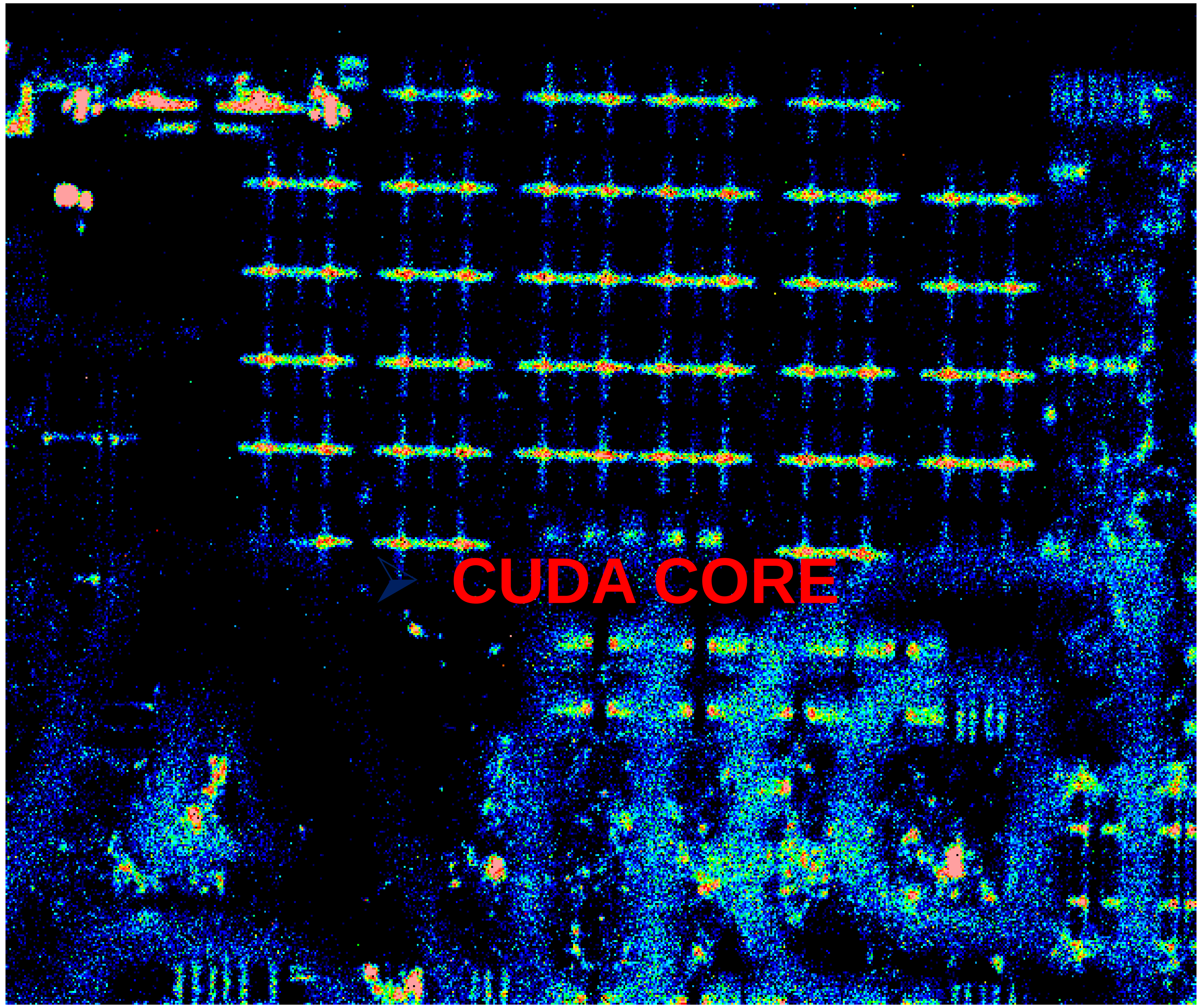
Core Localizaiton in NVIDIA AI CHIP

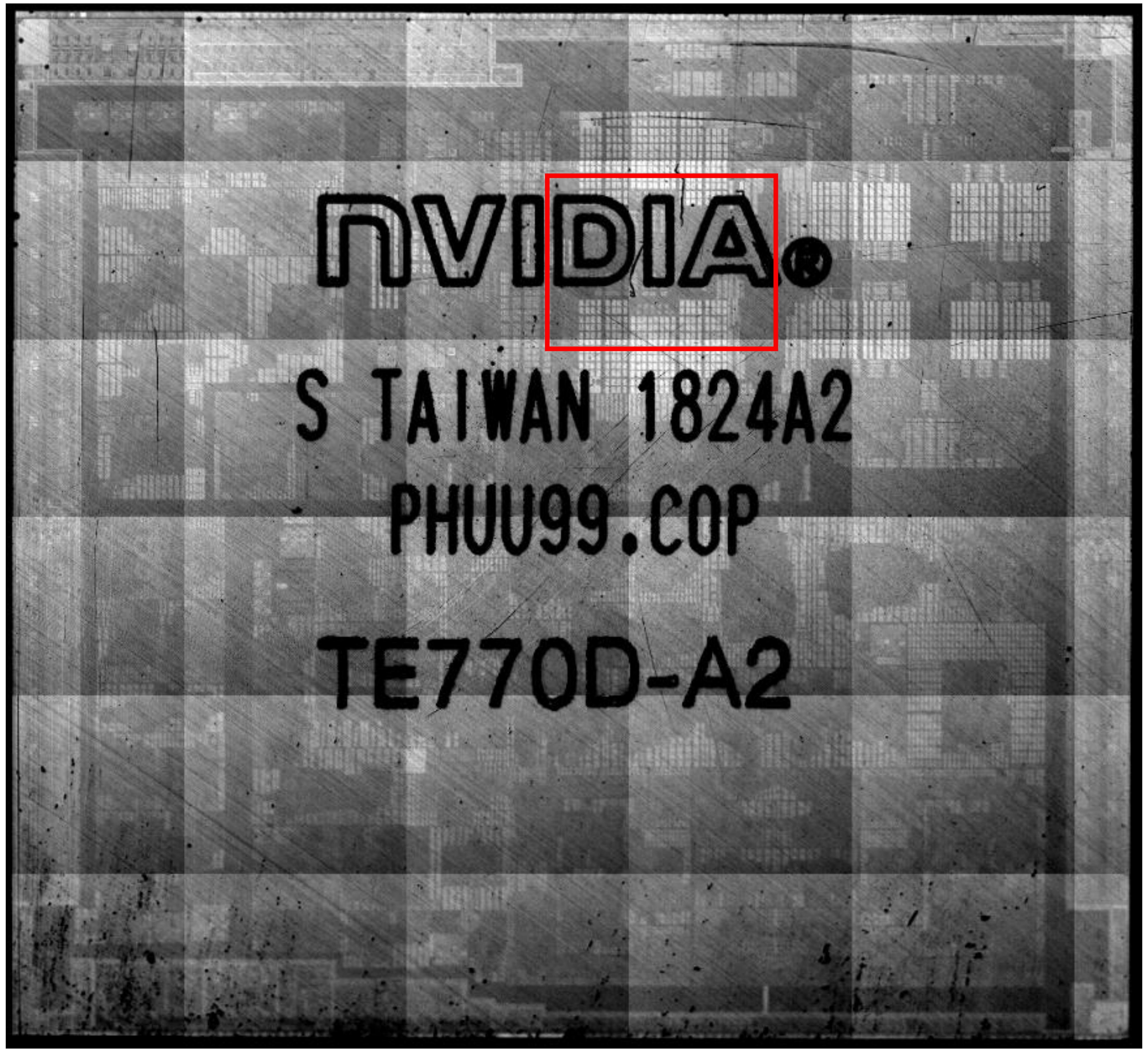


➢ Denver CORE



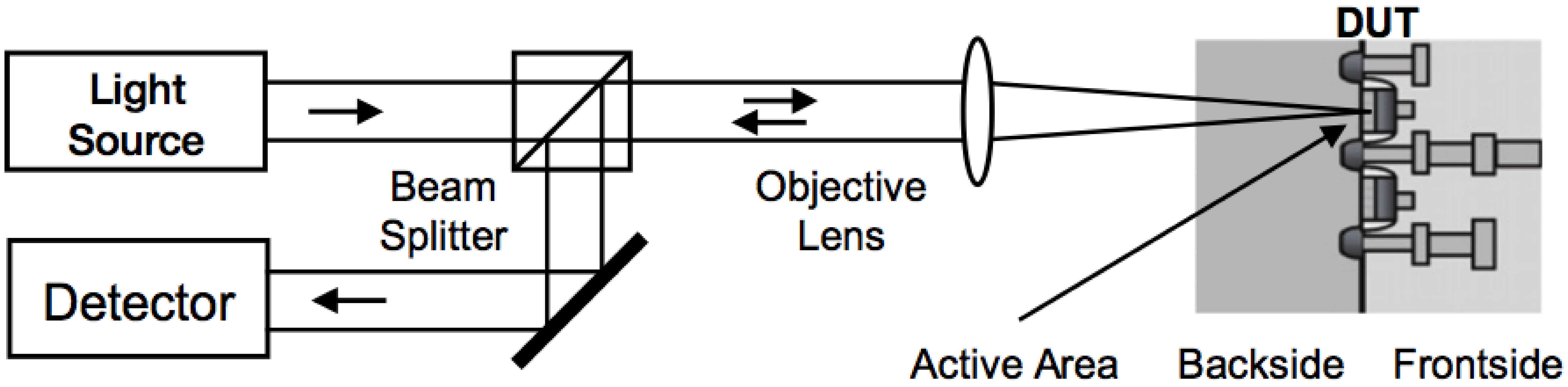
Core Localizaiton in NVIDIA AI CHIP





Optical Contactless Probing

Optical Contactless Probing

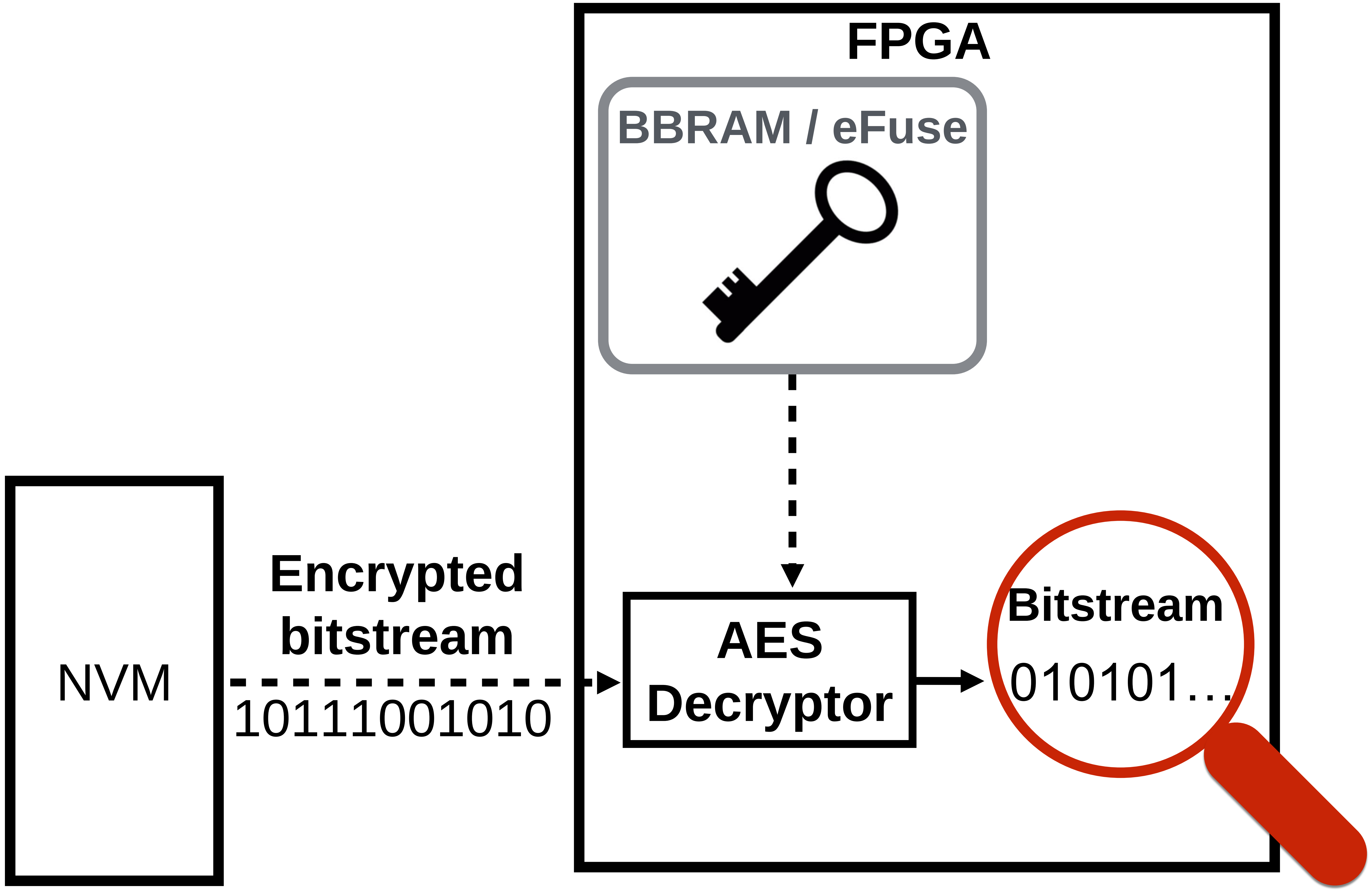


- **Changes in the absorption coefficient and the refractive index of device in active area by electrical field and current.**

- **Electro-Optical Probing (EOP)** or **Laser Voltage Probing (LVP):** Optical beam intensity altered by voltage/current —> probing of electrical signals on the node

- **Electro-Optical Frequency Mapping (EOFM)** or **Laser Voltage Imaging (LVI):** Feeding the reflected signal to a detector with a narrow band frequency filter while scanning the laser—> detecting node switching with this frequency

Plaintext Extraction

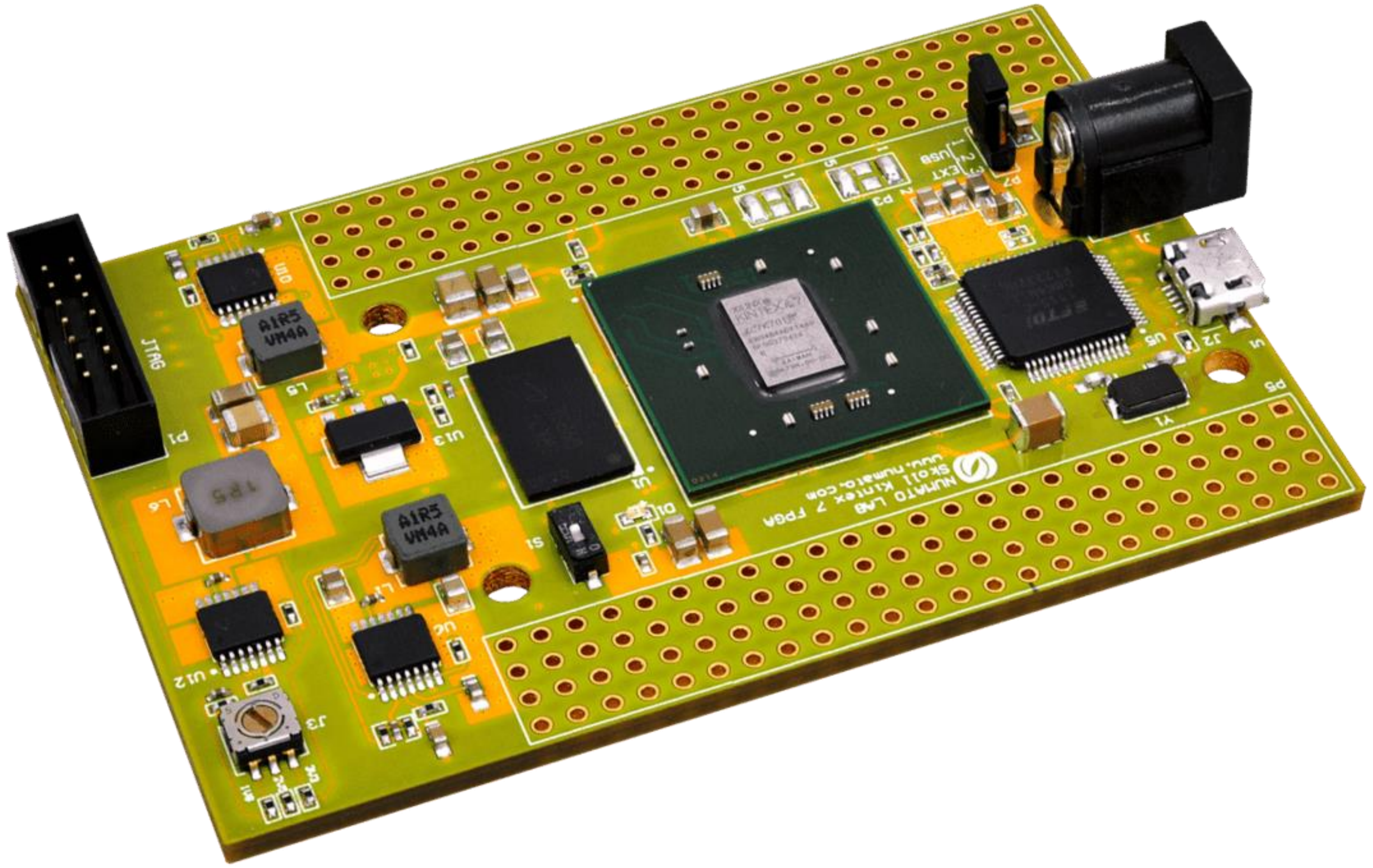


Optical Contactless Probing

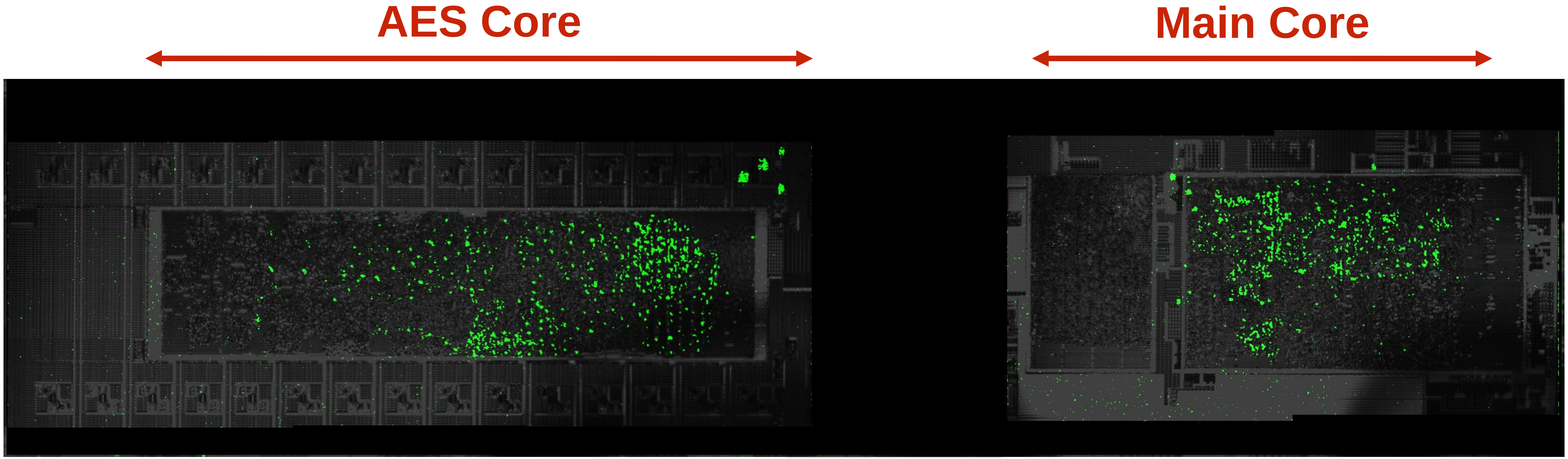
Tajik, S., Lohrke, H., Seifert, J. P., & Boit, C. "**On the Power of Optical Contactless Probing: Attacking Bitstream Encryption of FPGAs**," In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security.

Experimental Setup

- **Device under Test (DUT):** Skoll - Xilinx Kintex 7 development board
  - Chip's technology: 28 nm
  - No chip preparation (e.g., depackaging, silicon polishing, etc.)
- **Optical Setup:** Hamamatsu PHEMOS-1000
  - Laser wavelength: 1.3 μm
  - Laser spot size: >1 μm



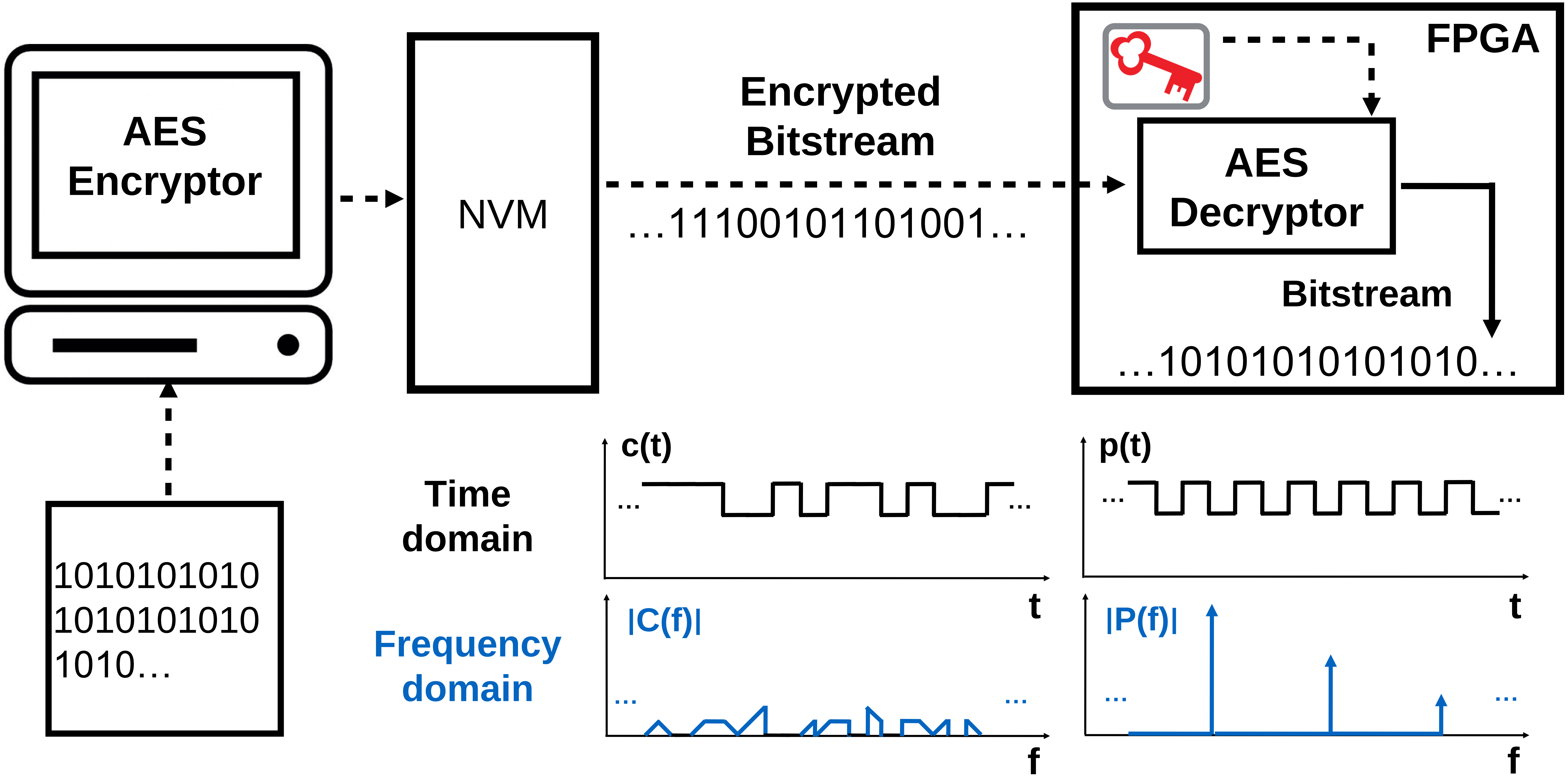
Localizing Decryption Core using EOFM



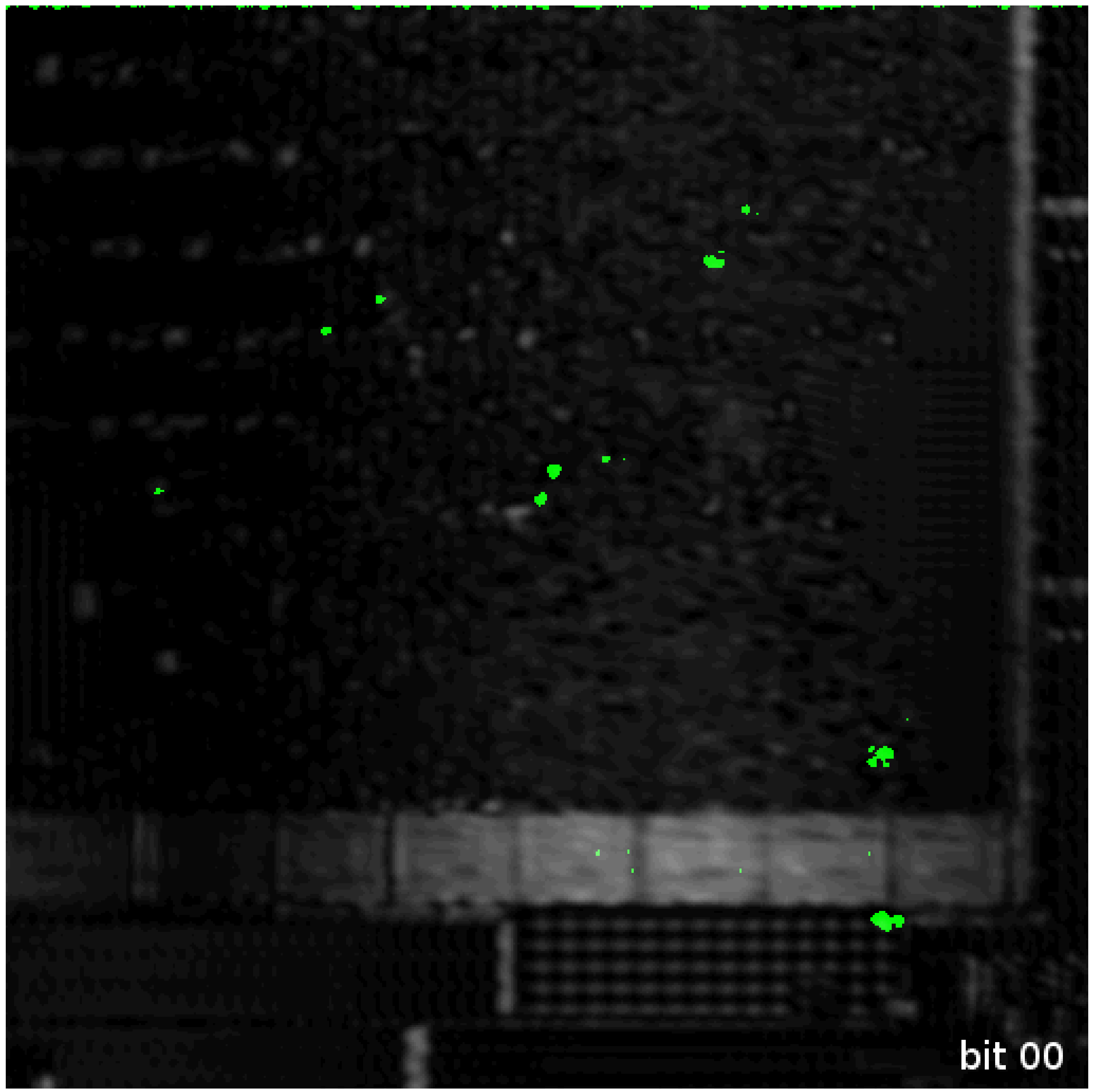
Clock activity for unencrypted bitstream

Clock activity for encrypted bitstream

Frequency Analysis of Regular Bitstream

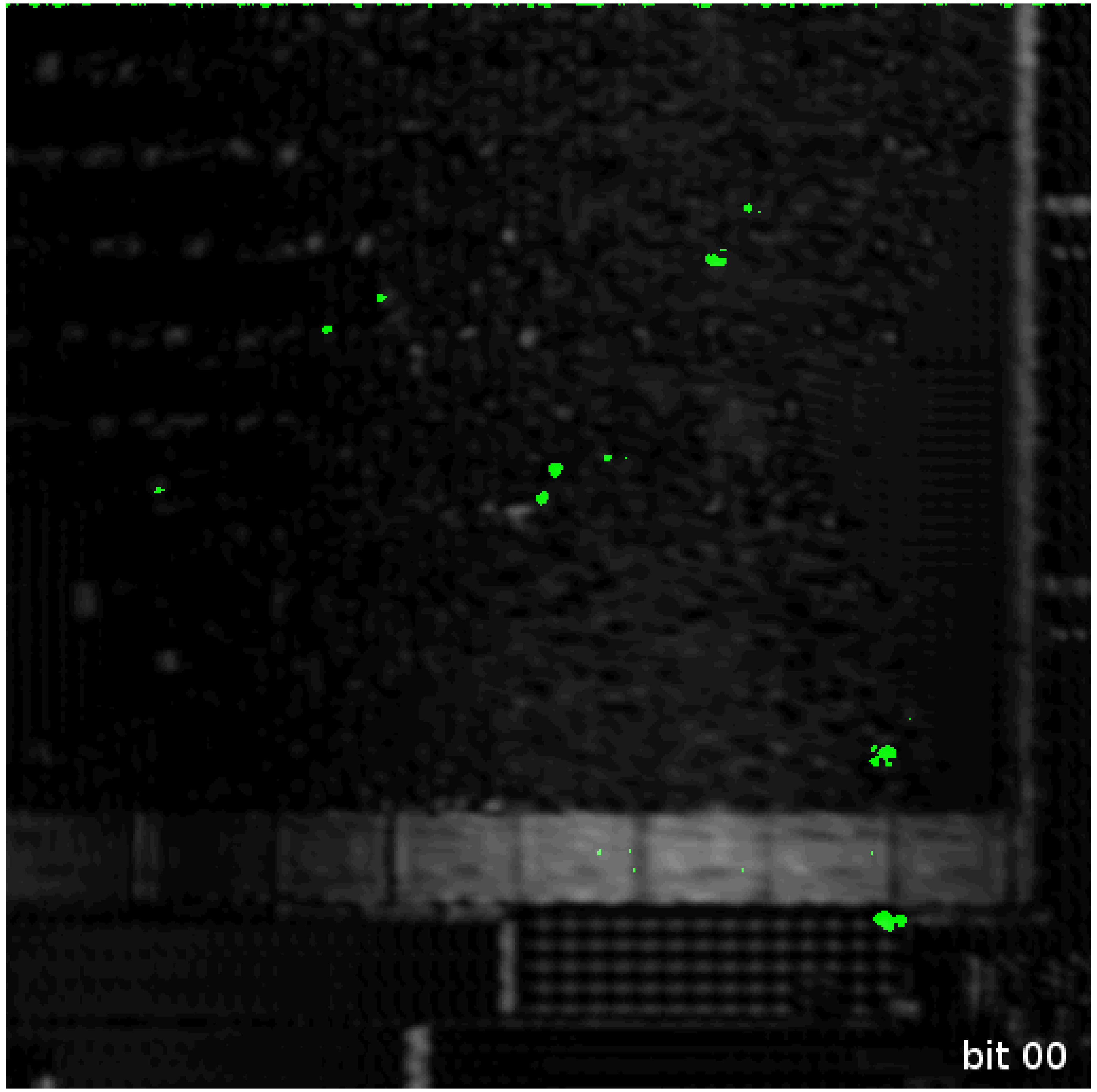


Locating the plaintext data

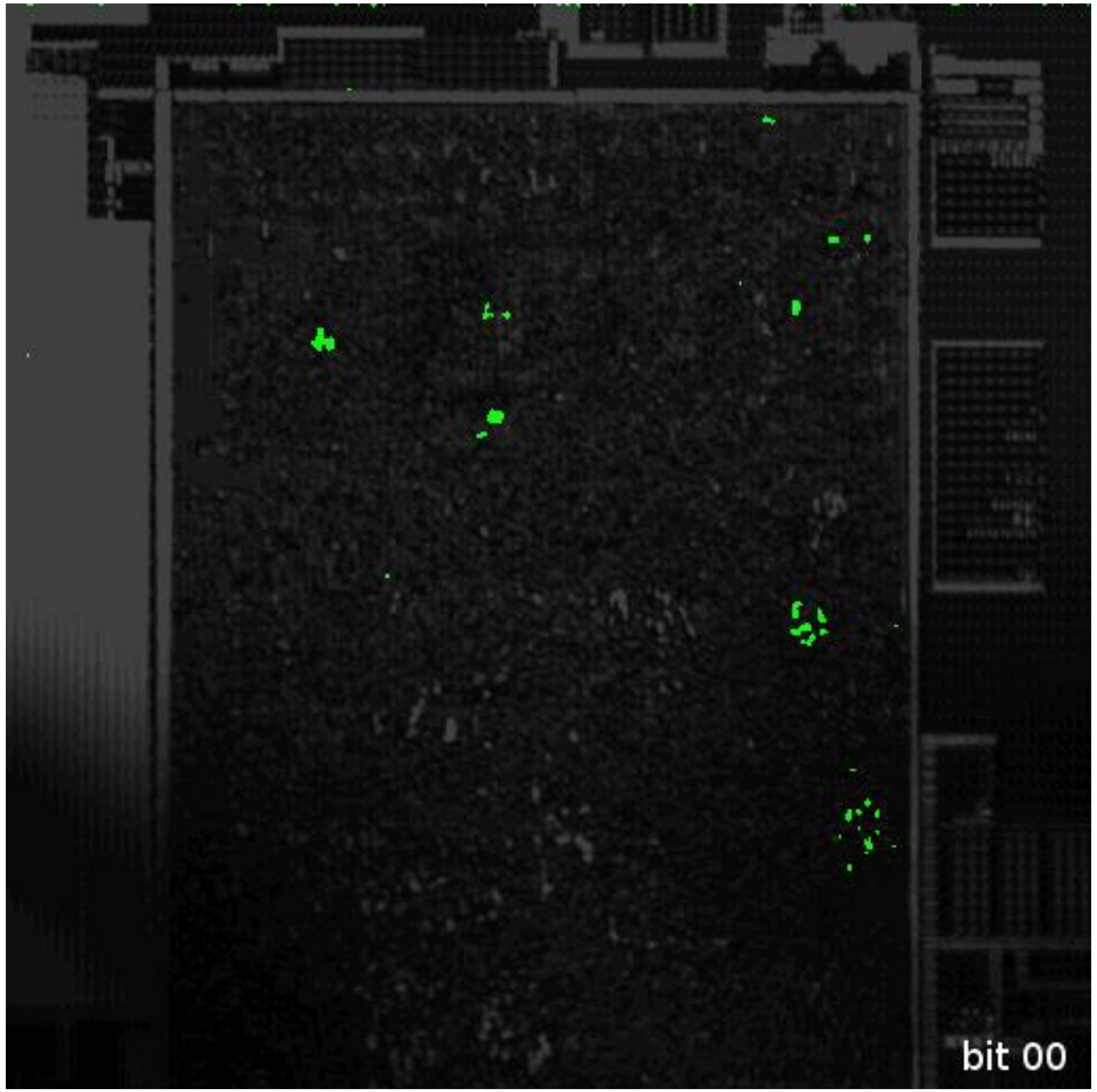


Locations in AES output port

Locating the plaintext data

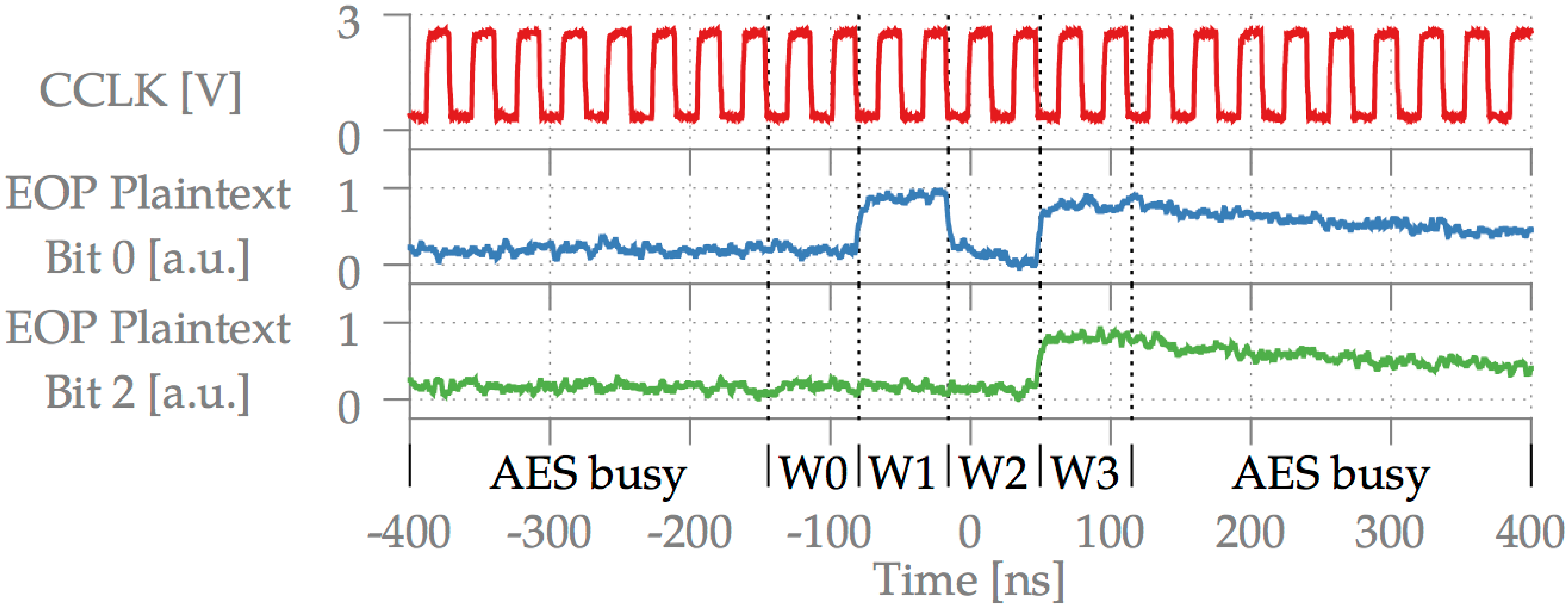


Locations in AES output port



Locations inside main core logic mesh

Extracting Plaintext Data using EOP



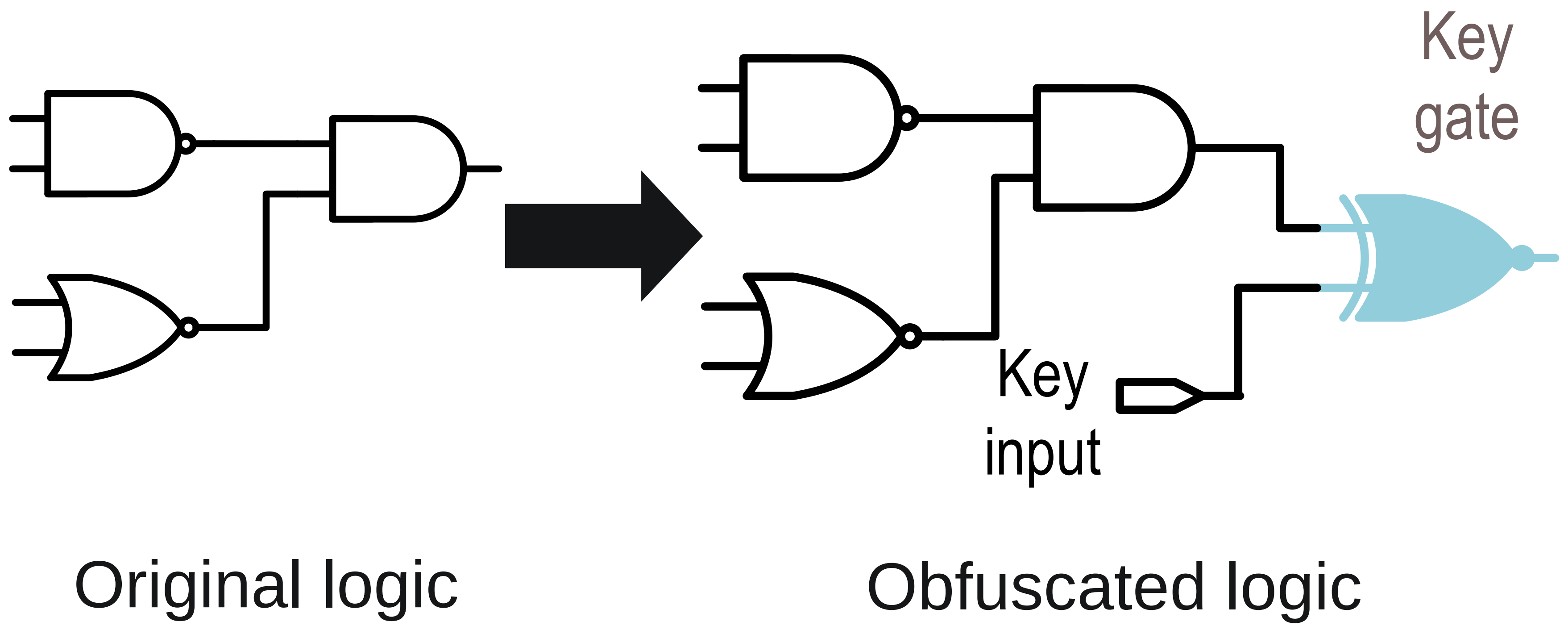
Logic Locking: Active IP Protection Mechanism

Goal

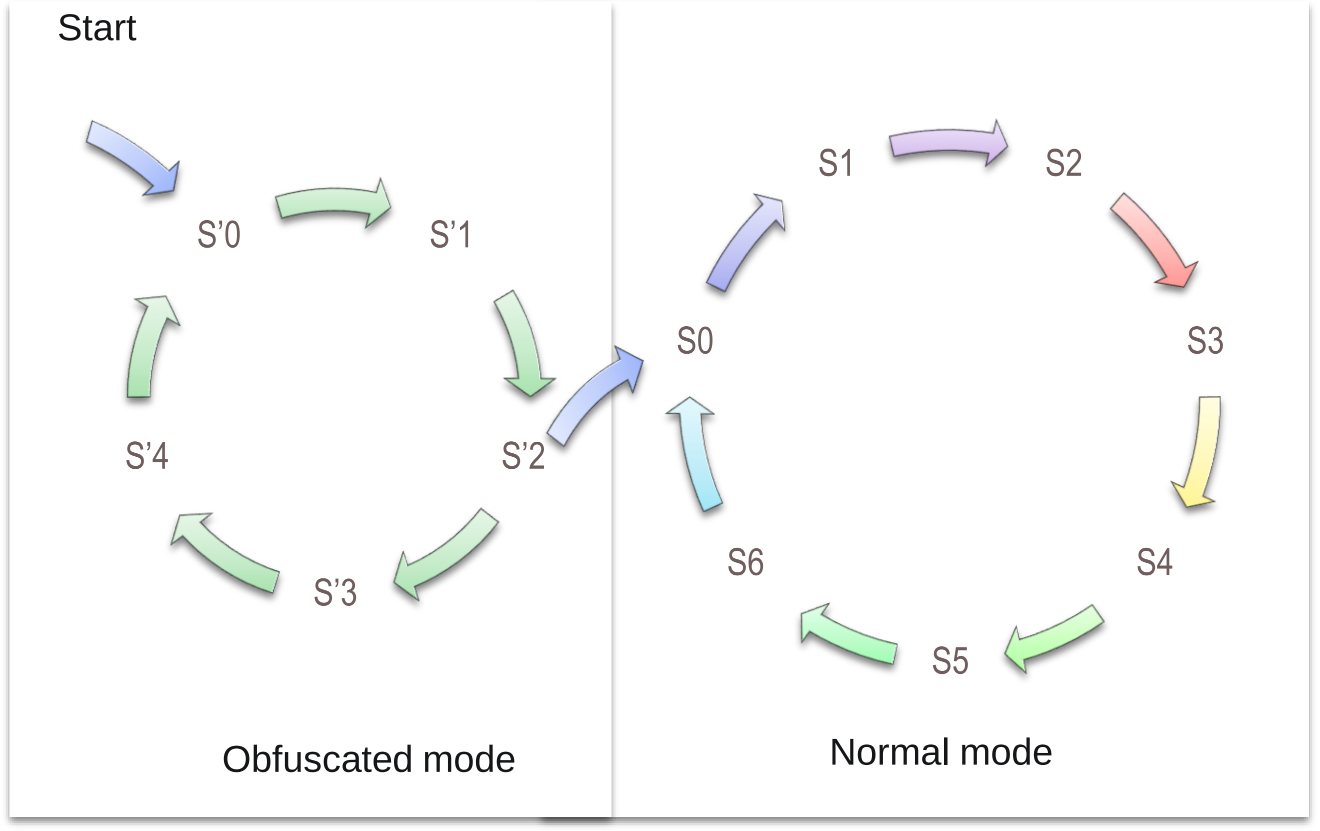
- Locking functionality of IP by inserting additional logic
- key programmed in trusted facility after fabrication

Classification

- Combinational Logic Locking: Locking design w ith logic gates
- Finite State Machine (FSM) Locking: Locking w ith state transition graph modification



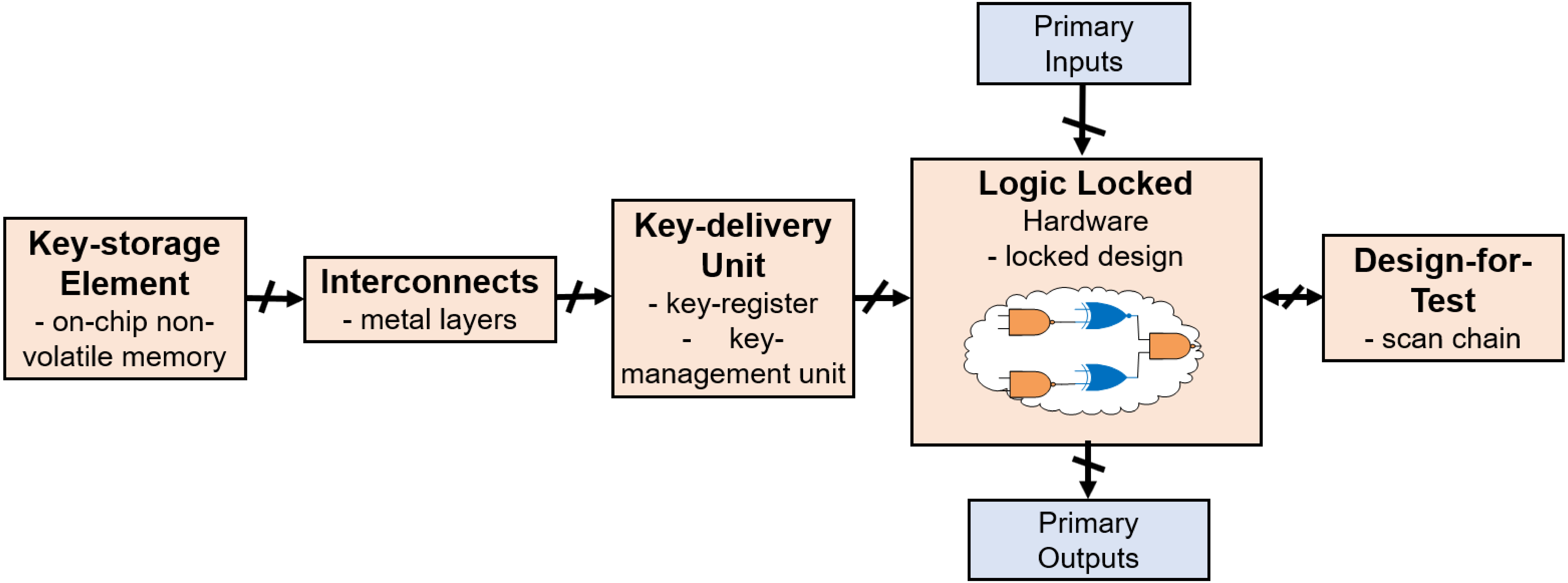
Combinational logic obfuscation



Finite State Machine Locking

Core-Components of Logic Locking

- Components mandatory for functionality of a logic locked chip



Key-storage Element
- on-chip non-volatile memory

Interconnects
- metal layers

Key-delivery Unit
- key-register
- key-management unit

Logic Locked Hardware
- locked design

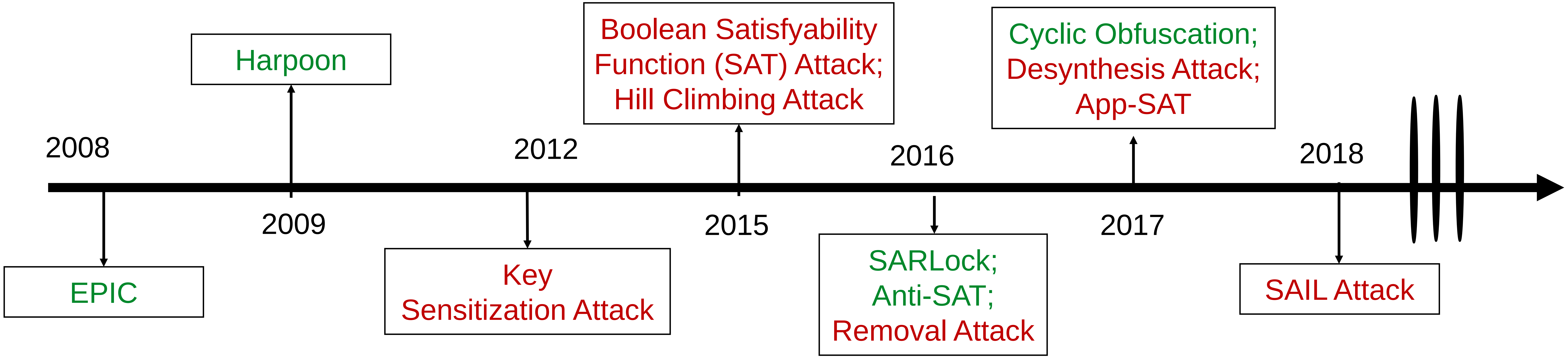
Design-for-Test
- scan chain

Primary Inputs

Primary Outputs

All Rights Reserved

Time-line for Logic Locking so Far



2008

EPIC

2009

Harpoon

2012

Key Sensitization Attack

2015

Boolean Satisfyability Function (SAT) Attack; Hill Climbing Attack

2016

SARLock; Anti-SAT; Removal Attack

2017

Cyclic Obfuscation; Desynthesis Attack; App-SAT

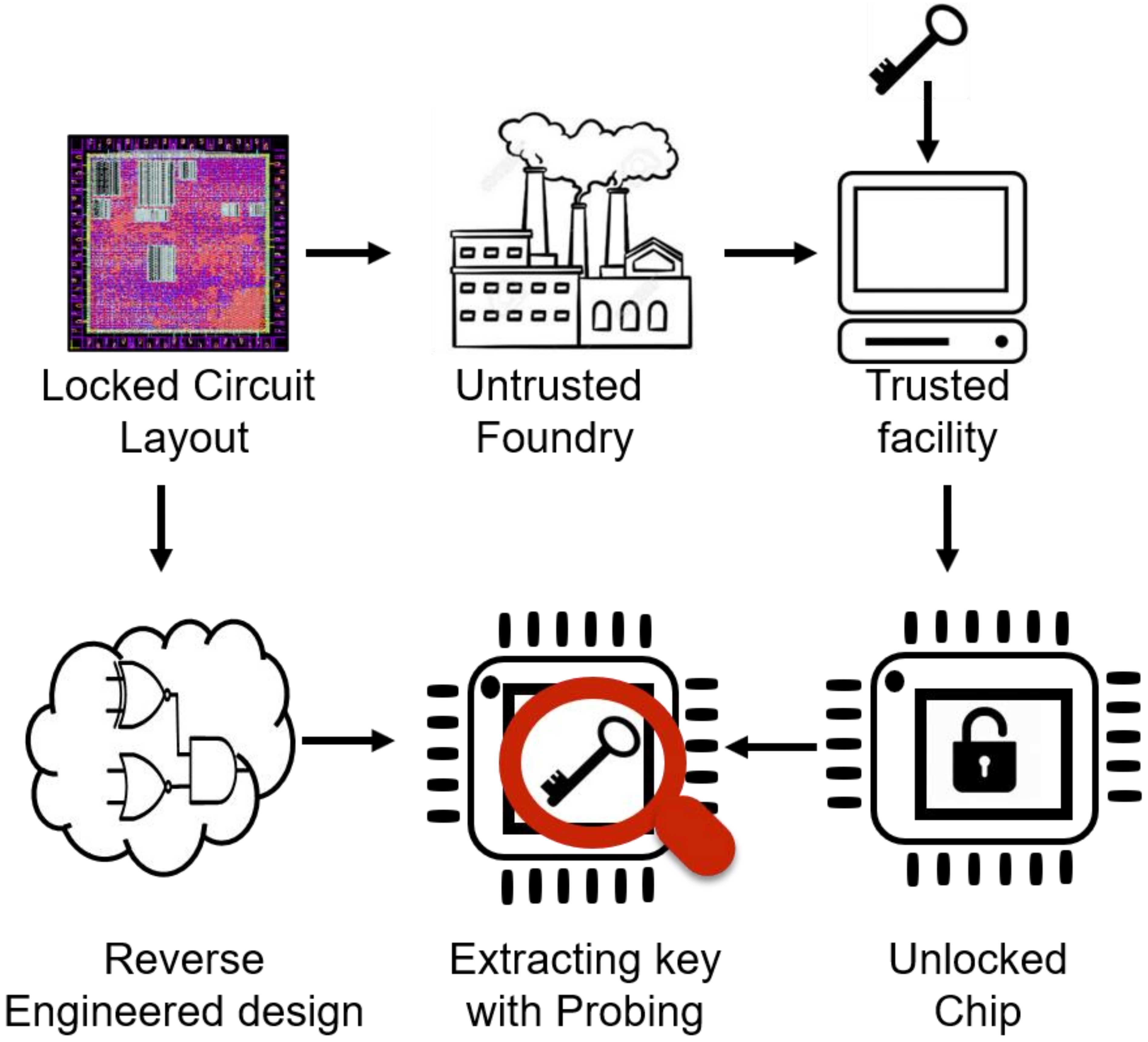
2018

SAIL Attack

- ➢ Adversary → Only untrusted foundry?
- ➢ Vulnerable only to algorithm approach?
- ➢ What about other capabilities of adversary? → Failure analysis tools

Threat Model & Potential Adversary

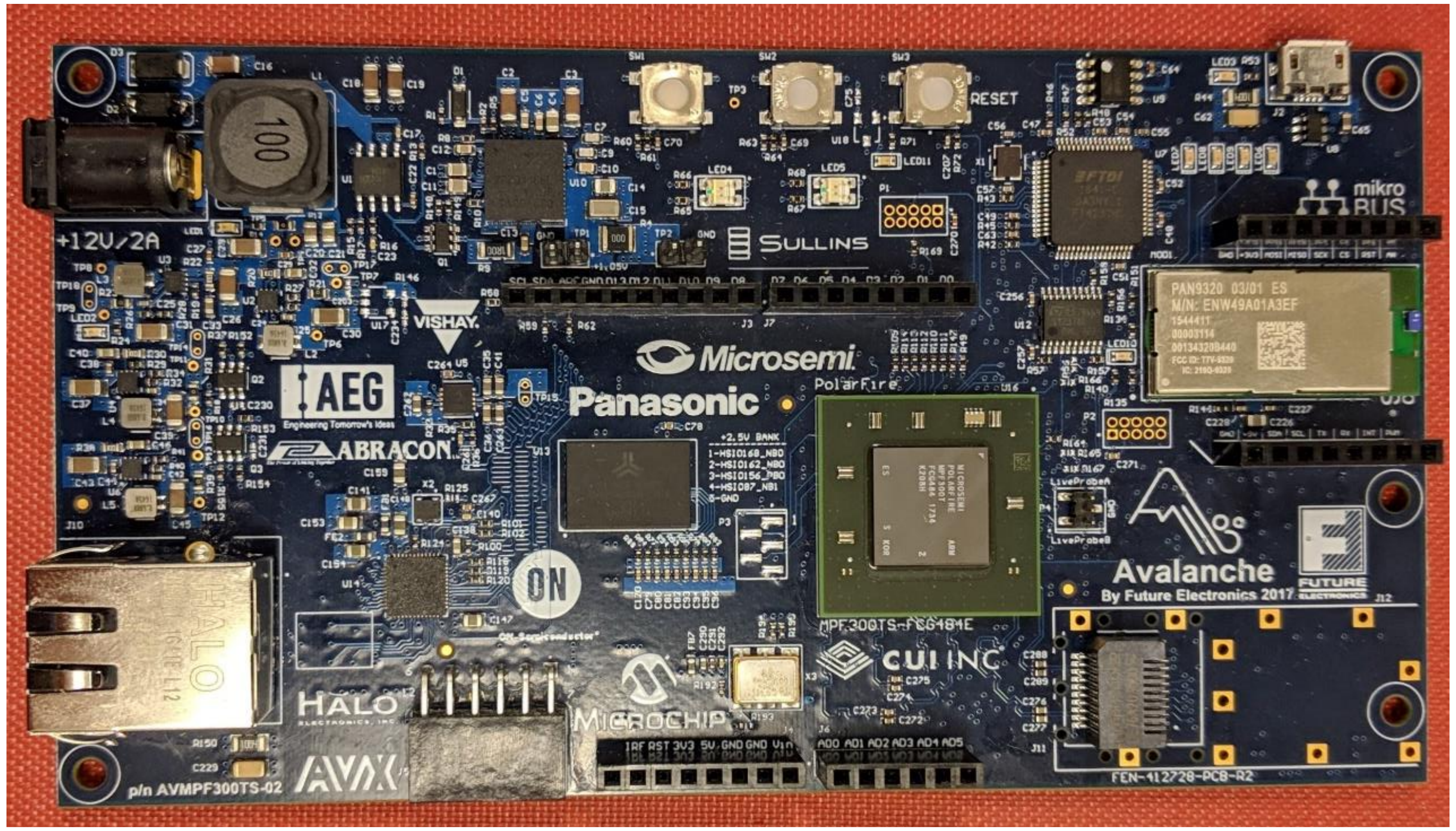
- Threat model is approach exploited by an adversary to access the protected assets, i.e, locking key

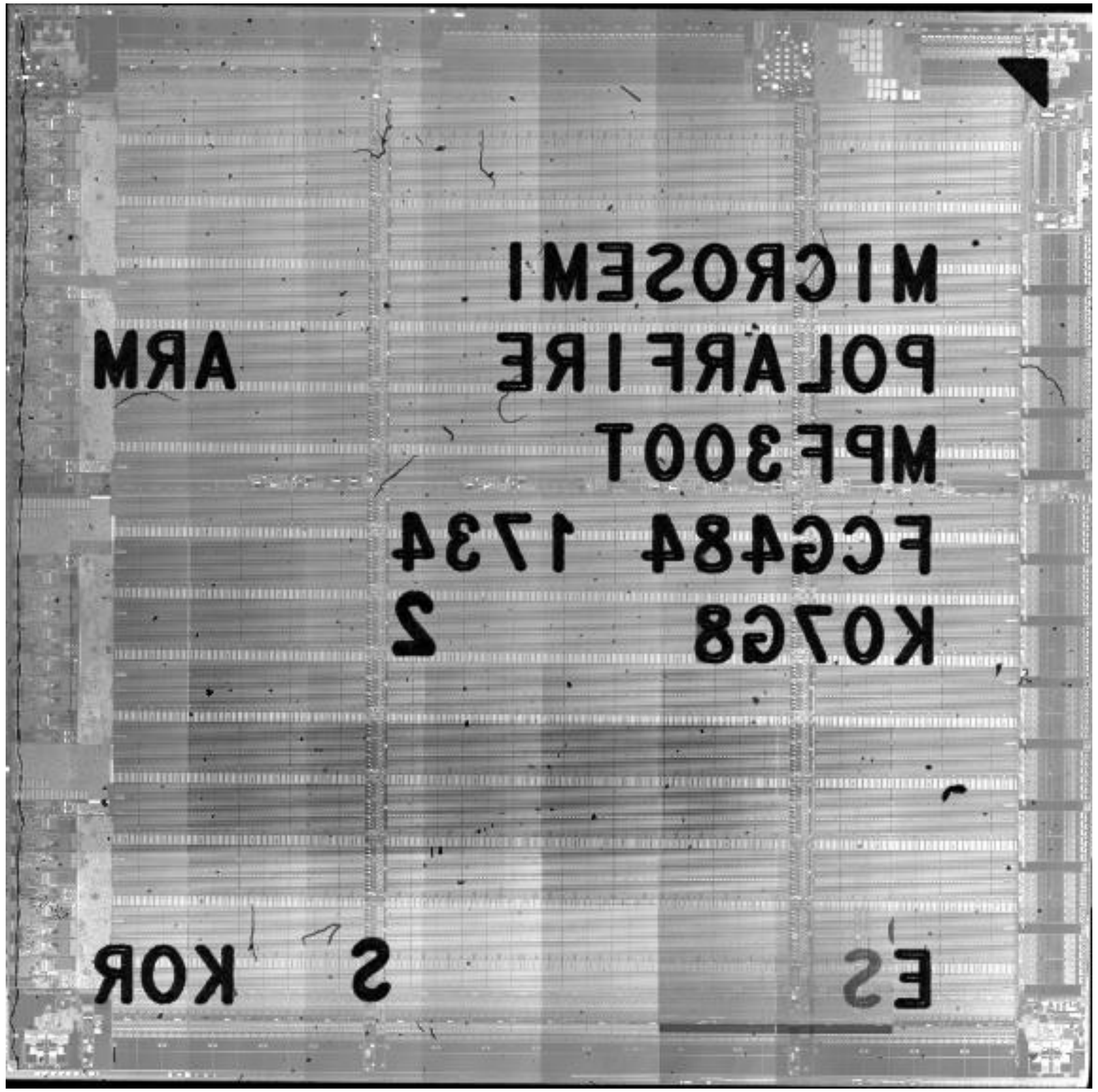


Adversary	Asset Holding
SoC Integrator	1.Soft/Hard IP 2.GDS II file
3rd Design Service Provider	1.IP Design 2.GDS II file
Foundry	1. GDS II file
Assembly and Distributor	1. Unlocked chip
End User	1.Unlocked chip 2.Documentation of chip

Partial reverse engineering and suitable failure analysis tool is sufficient for attack

Case Study –II: Flip-flop Probing

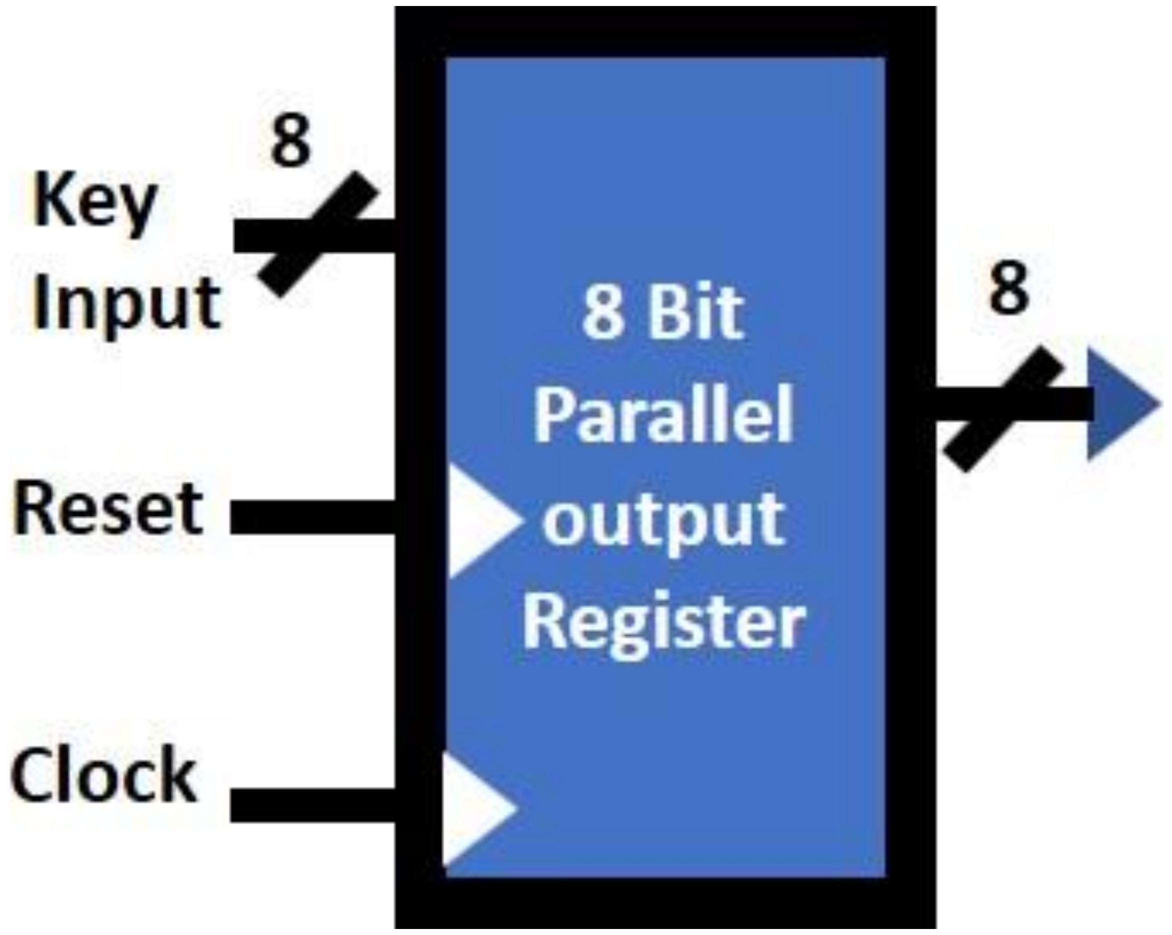


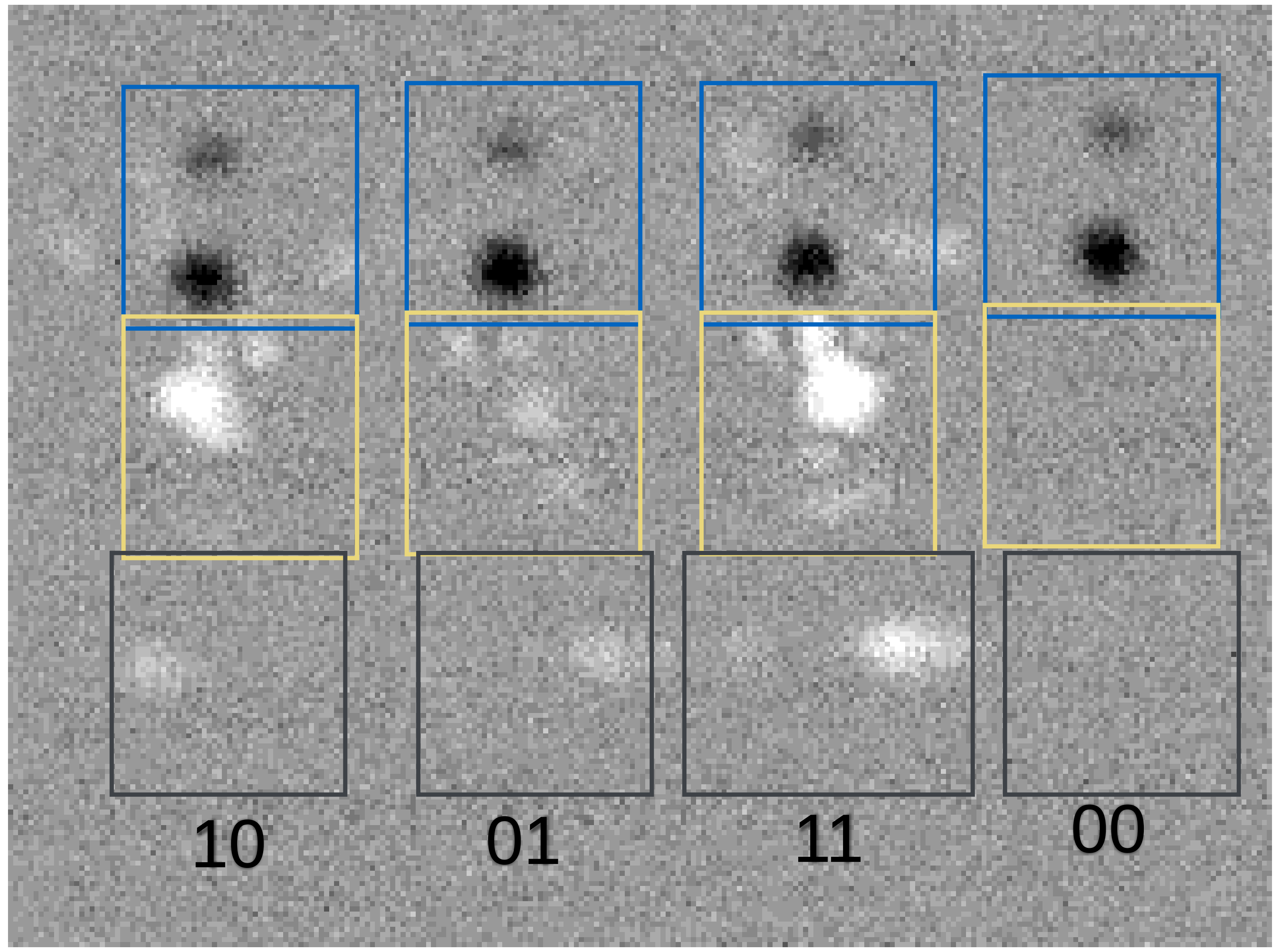


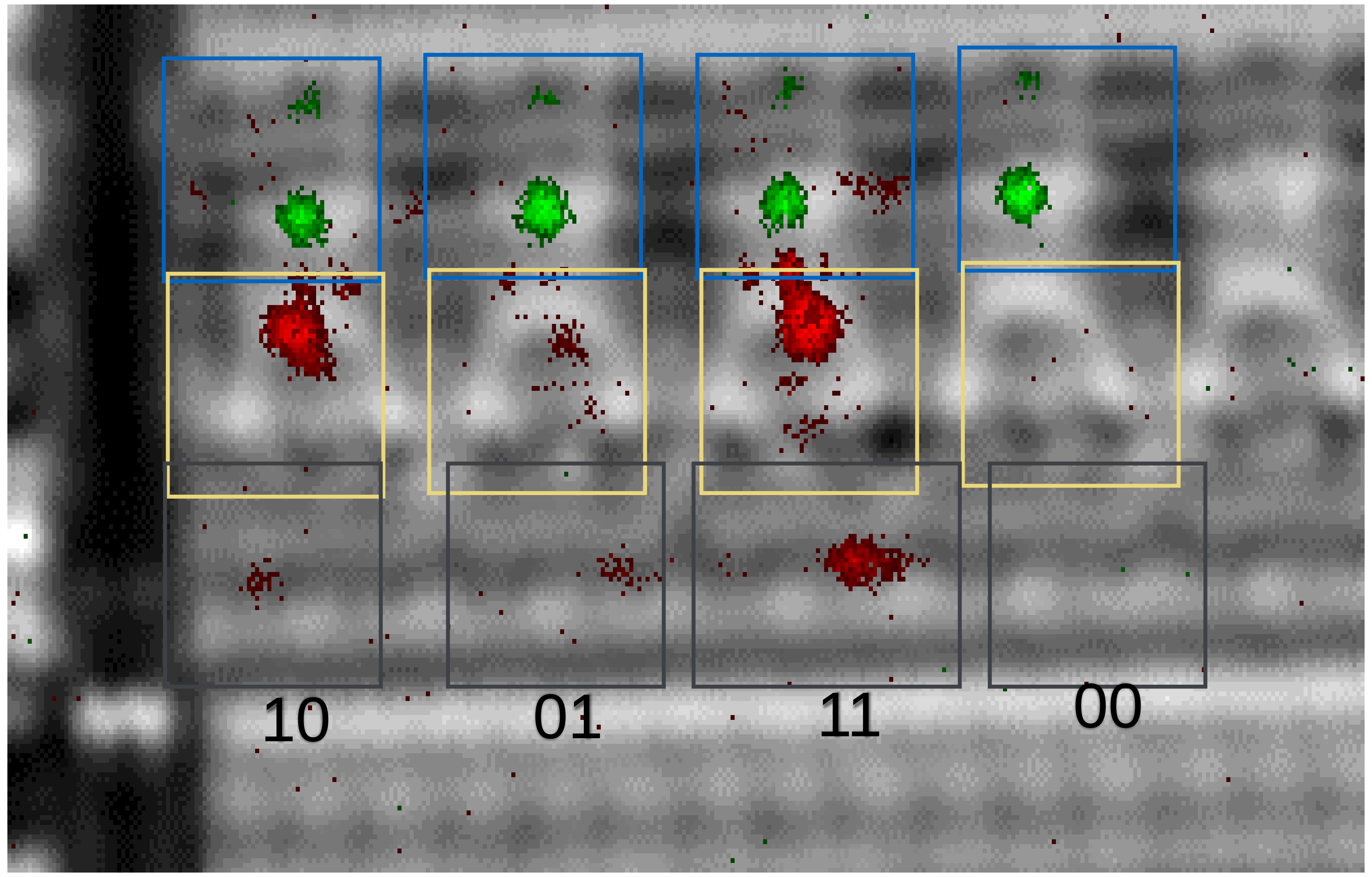
Microsemi die image collected with 1300nm laser

- ➢ Avalanche FPGA development board
- ➢ 28 nm technology Microsemi MPF300 Polarfire chip

Reverse Engineering DUT

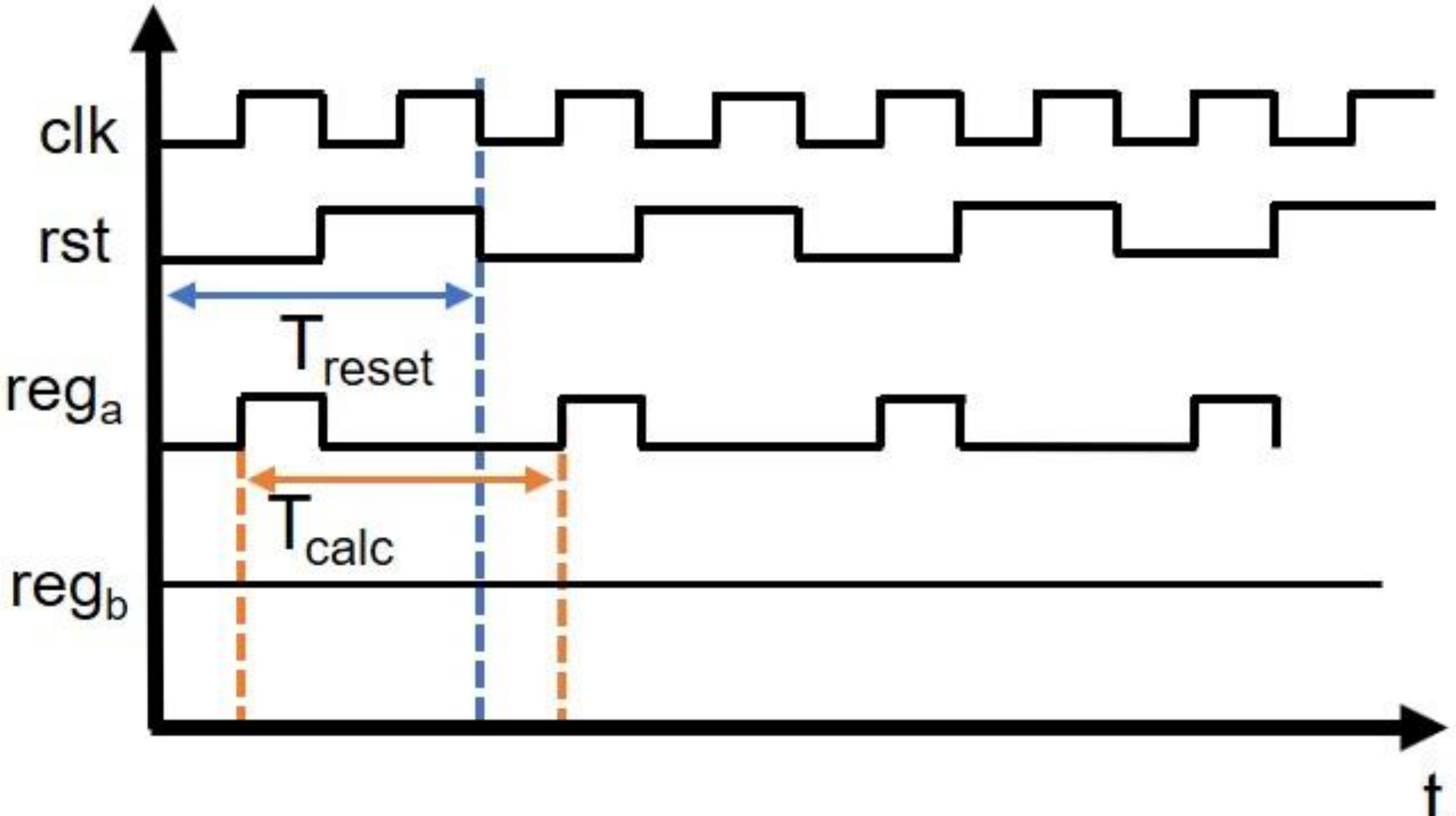




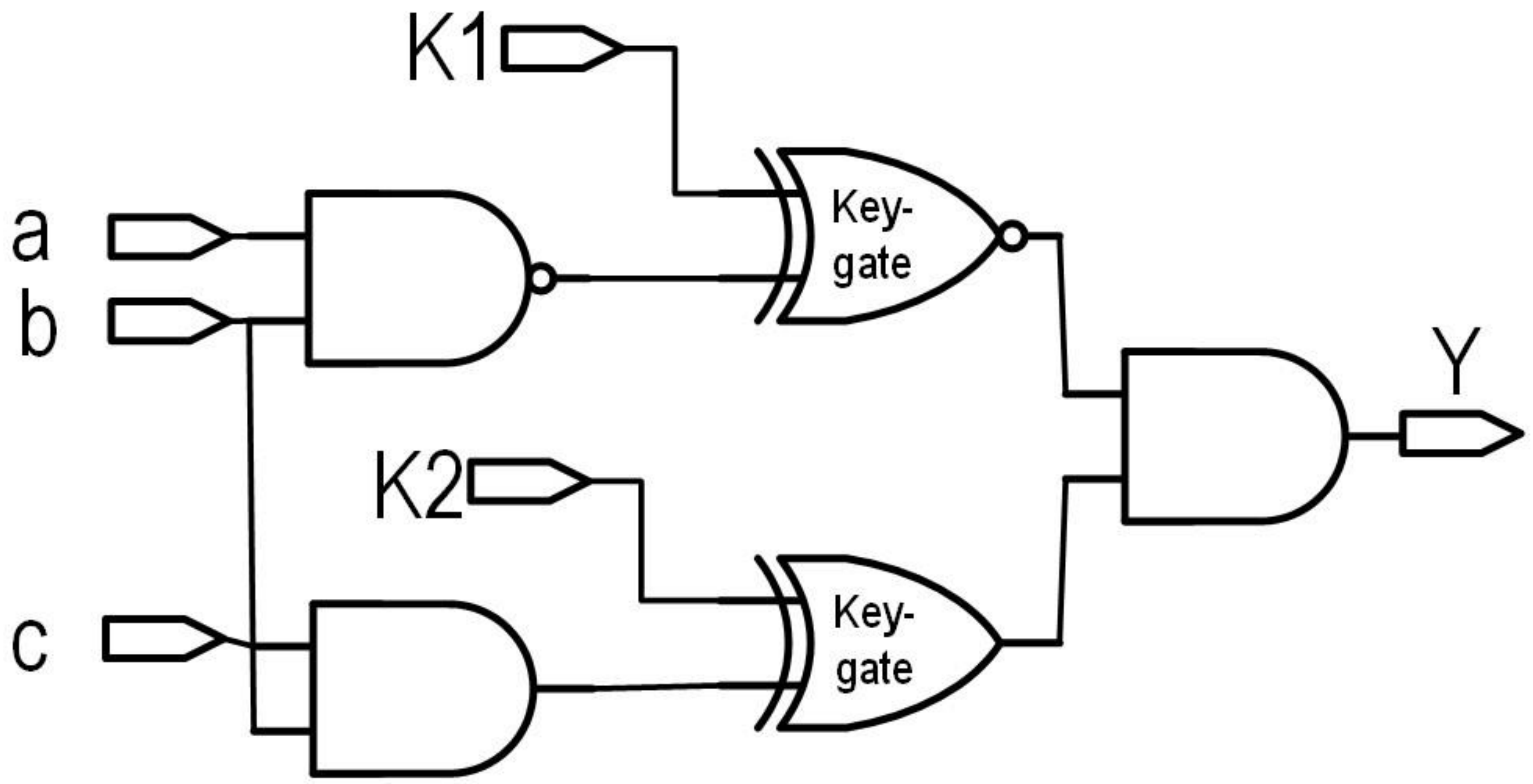


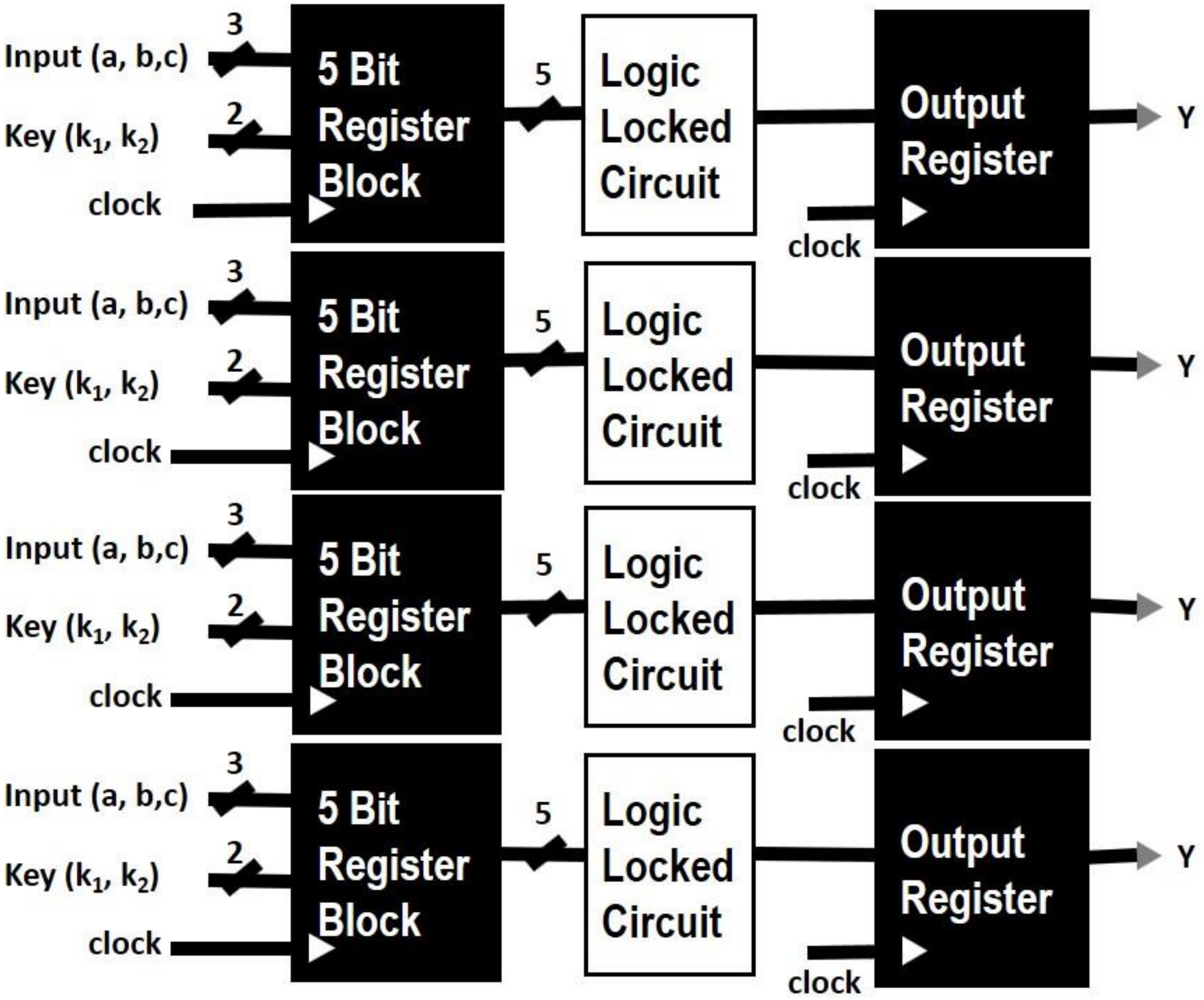
Probing Registers in DUT

- Activity shows for two different frequency
- White dot corresponds to registers



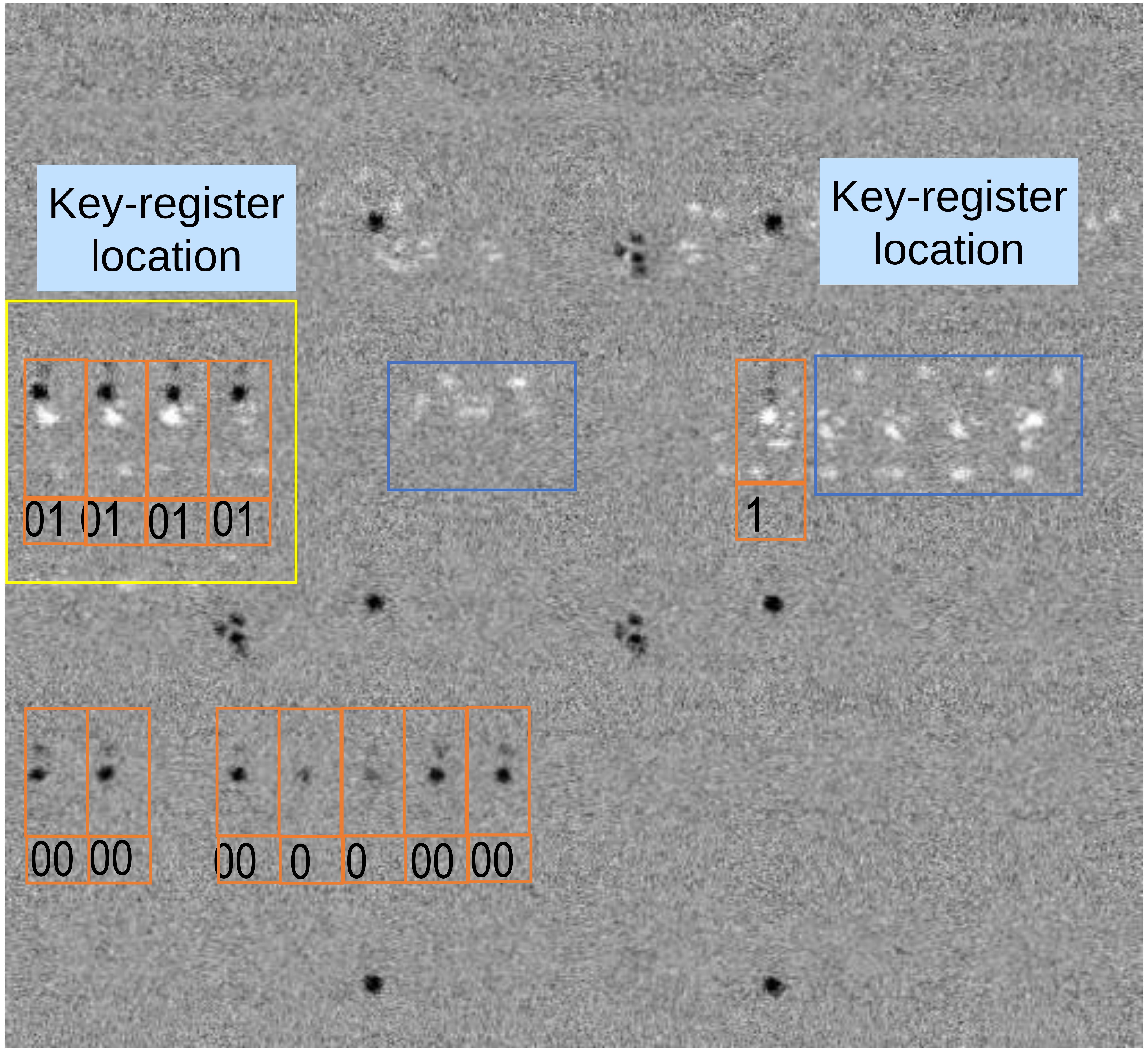
Proof-of-Concept Implementation



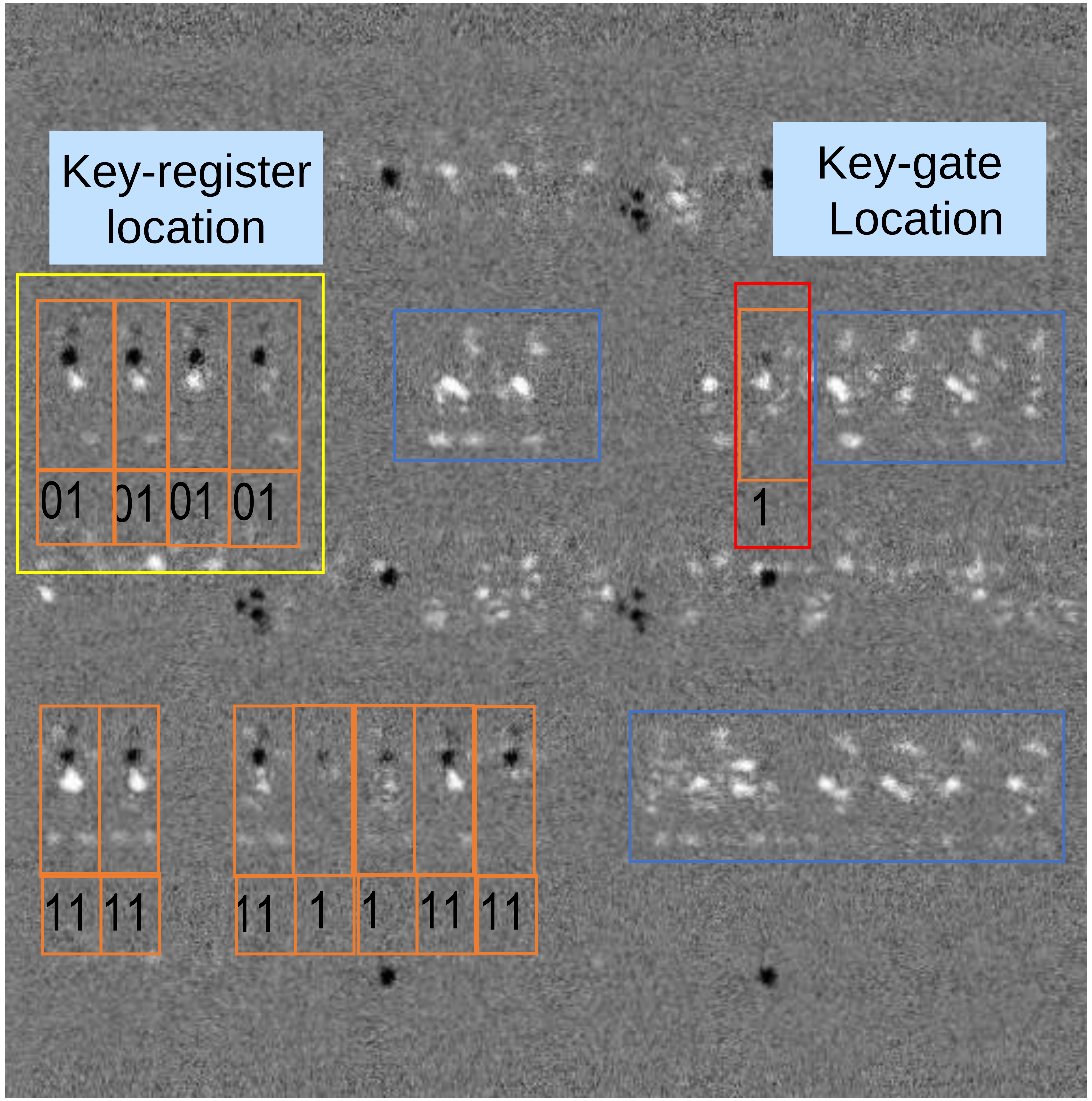


- **K1, k2 → key-input (key-register) → constant v alue stored**
- **a, b, c → user input (general purpose register) → variable stored value**

Exposing Key-register and Key Value



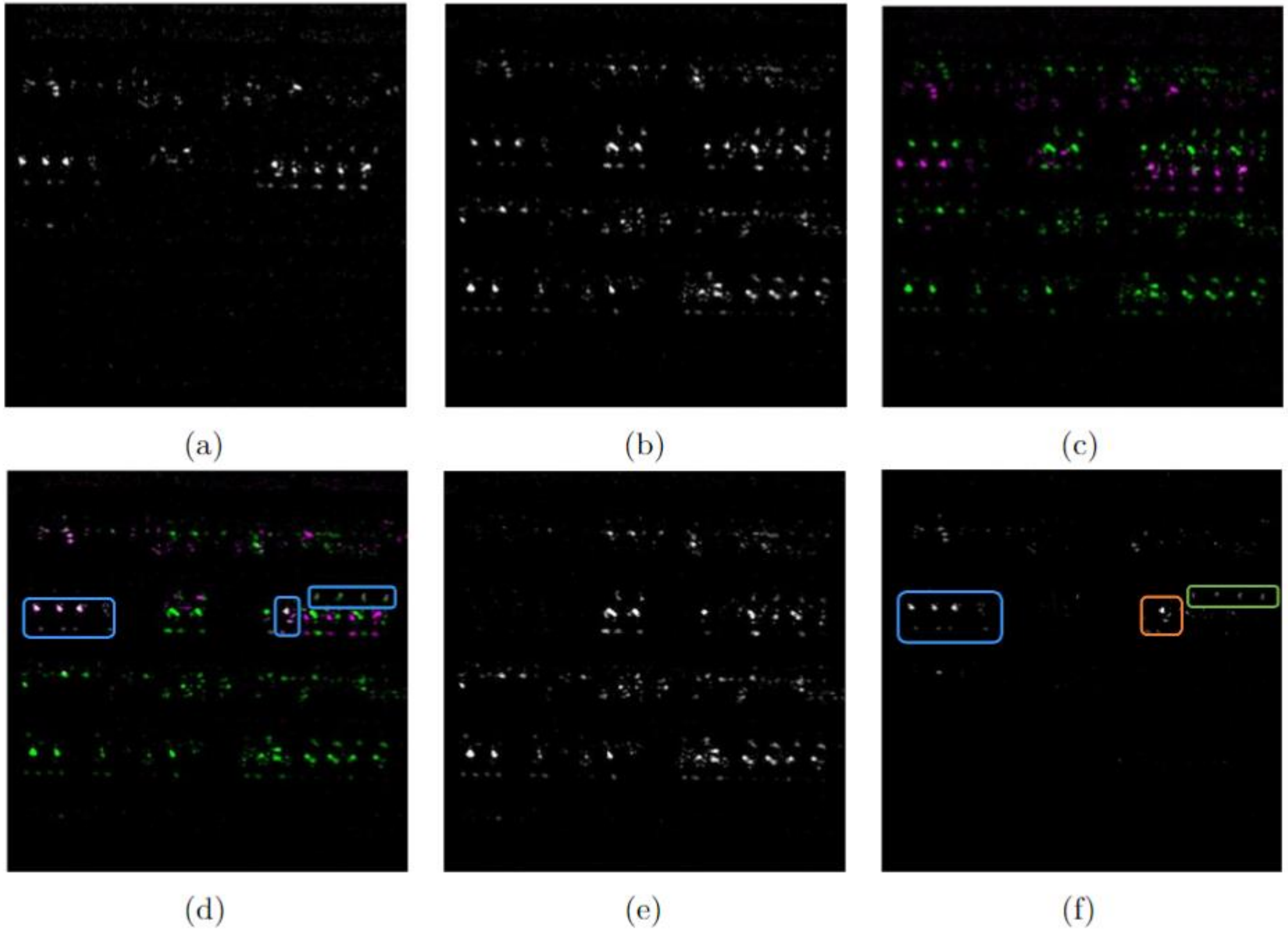
Register and clock activity when input connected to ground



Register and clock activity when input connected to active

Exposing Key-register and Key Value

Simple image registration, subtraction, or image co-relation can automate the whole process

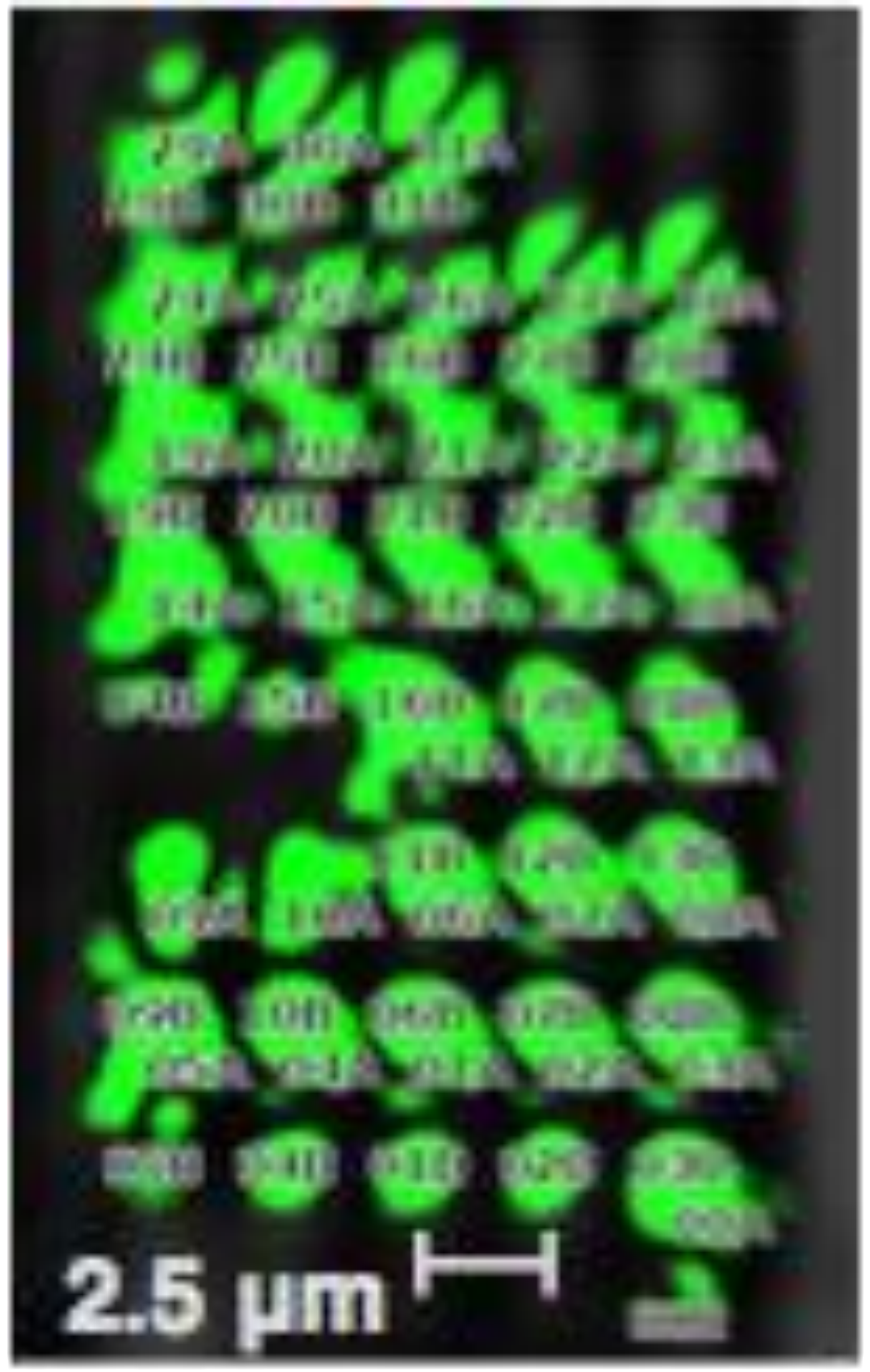


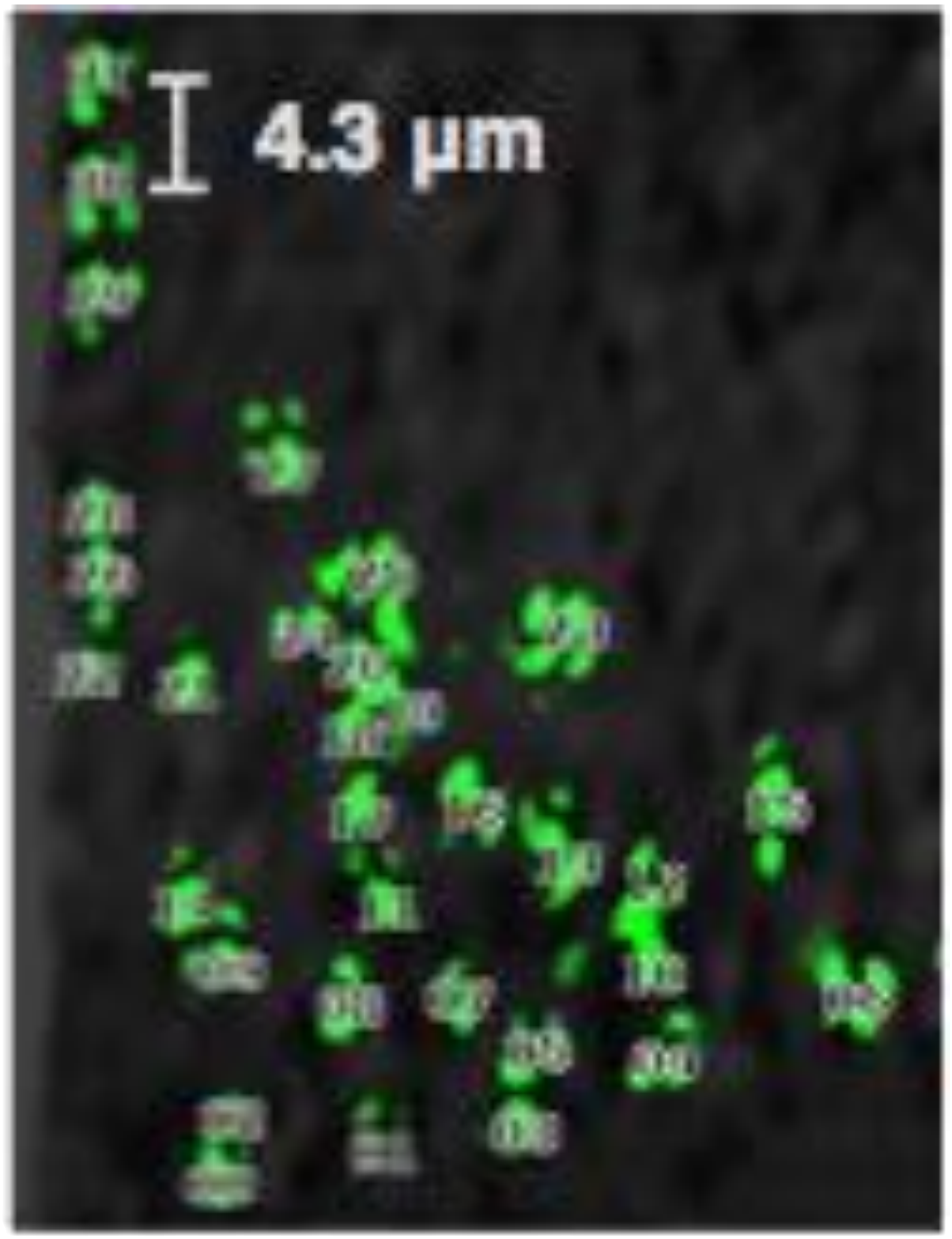
(a) (b) (c)

(d) (e) (f)

Technology Size vs. Optical Resolution

- The real limiting factor for an attacker is not the technology size, but the distance of a probing location of interest to the next location, (Optical Resolution and spot size)
- the separation between locations carrying different streams of data can actually be much larger than the technology size.

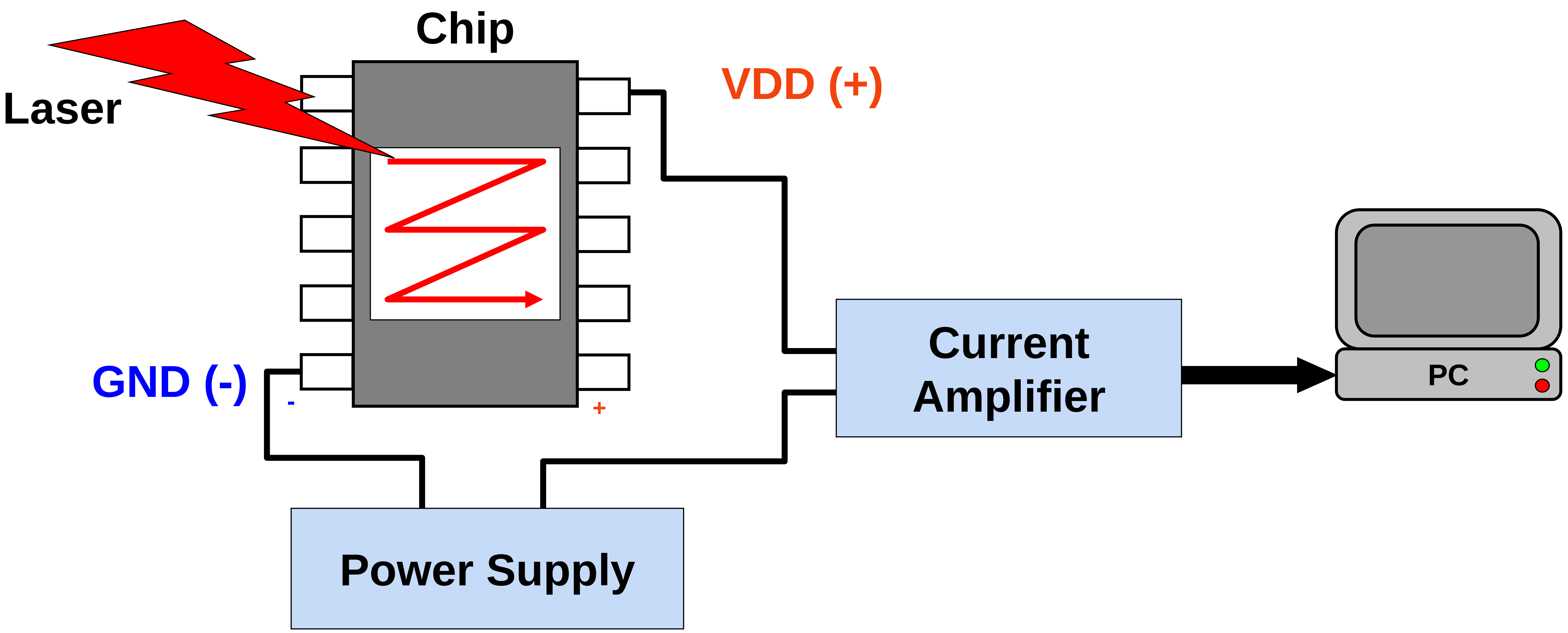




Laser Stimulation

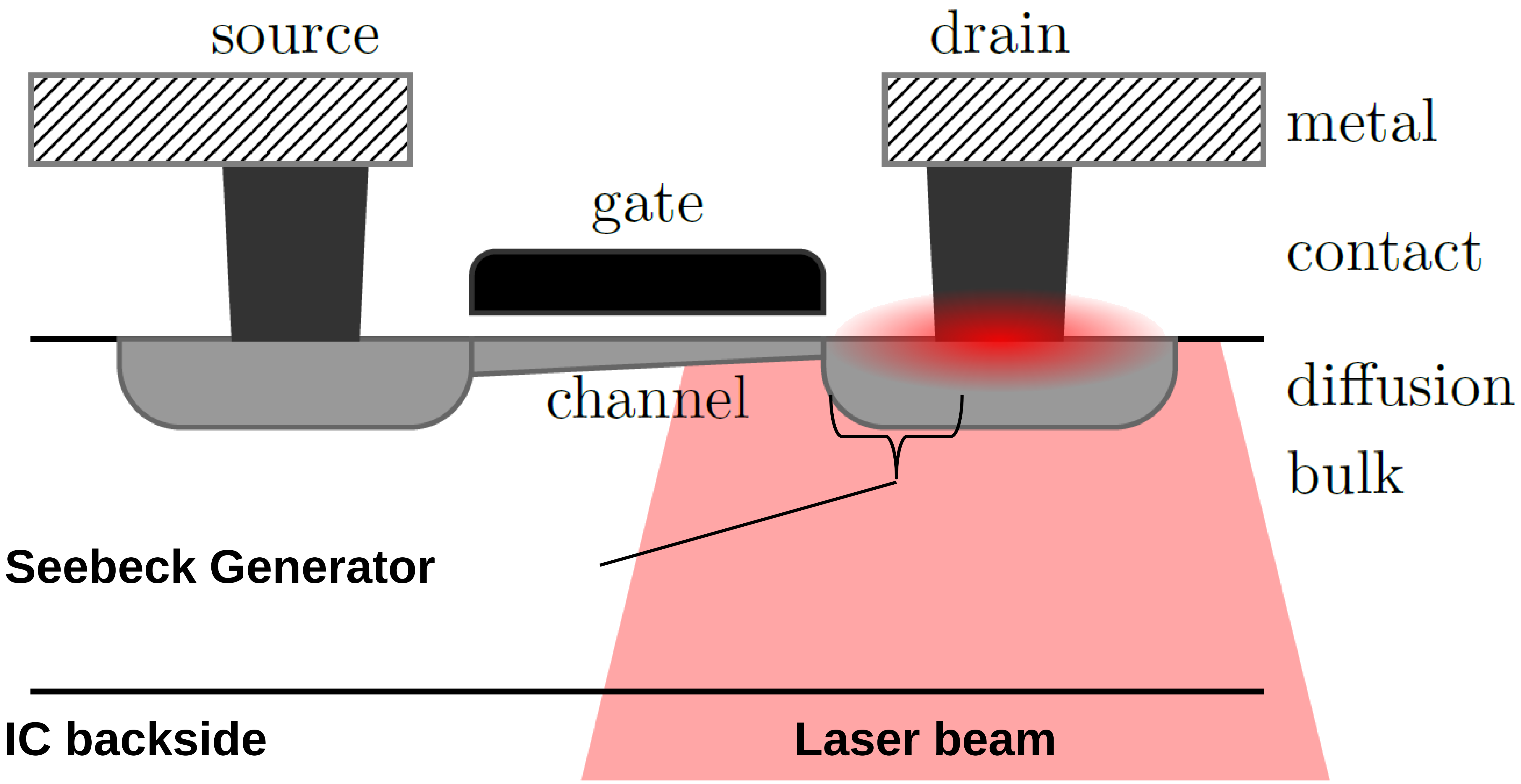
Thermal Laser Stimulation (OBIRCH)

- The chip is scanned with a 1.3 μm laser beam from the backside
- The current changes in response to the local thermal stimulations
- Measured current is monitored by a current amplifier >> a proportional analog voltage is generated
- Analog voltage is fed into image acquisition hardware while scanning the laser

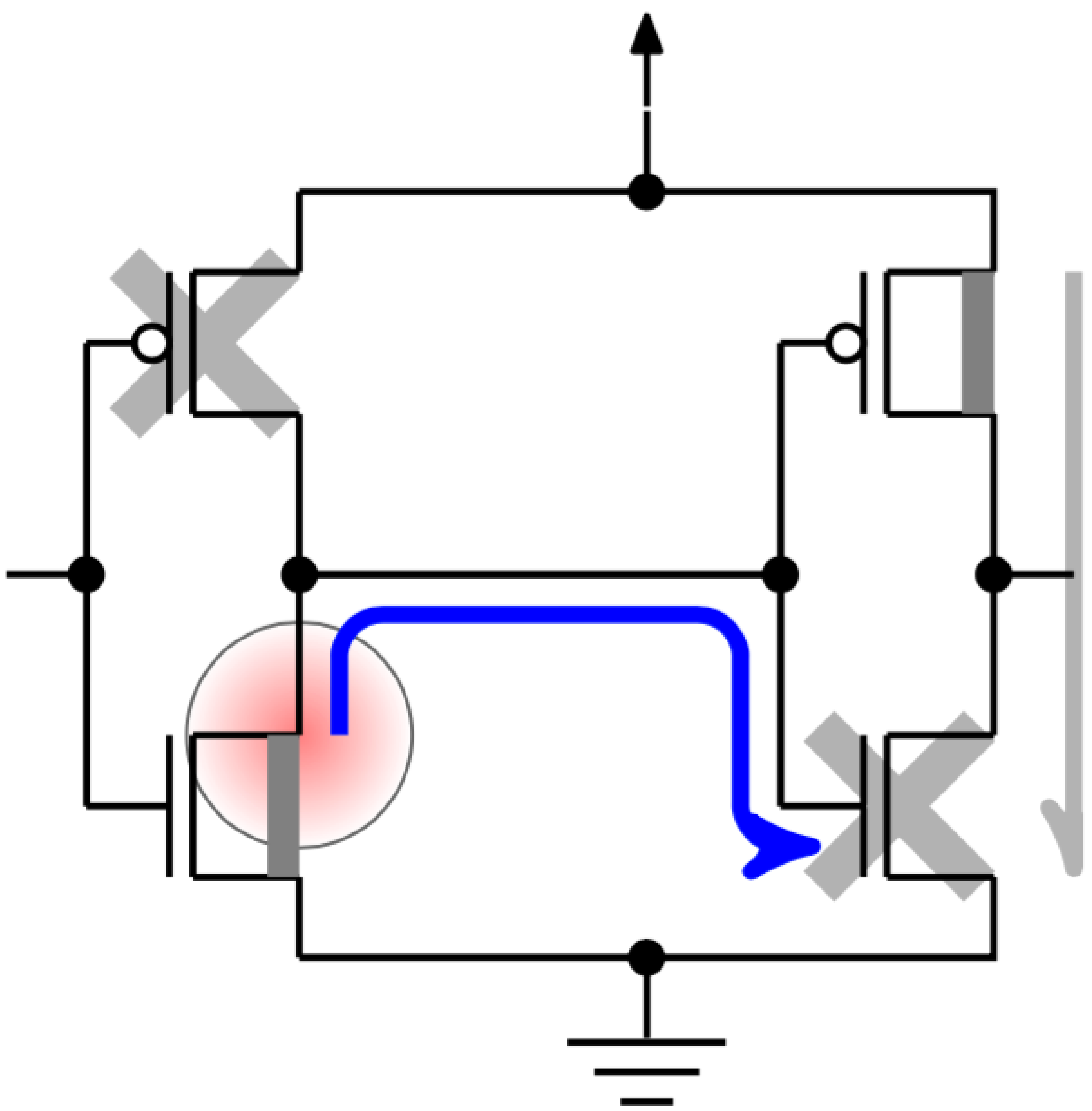


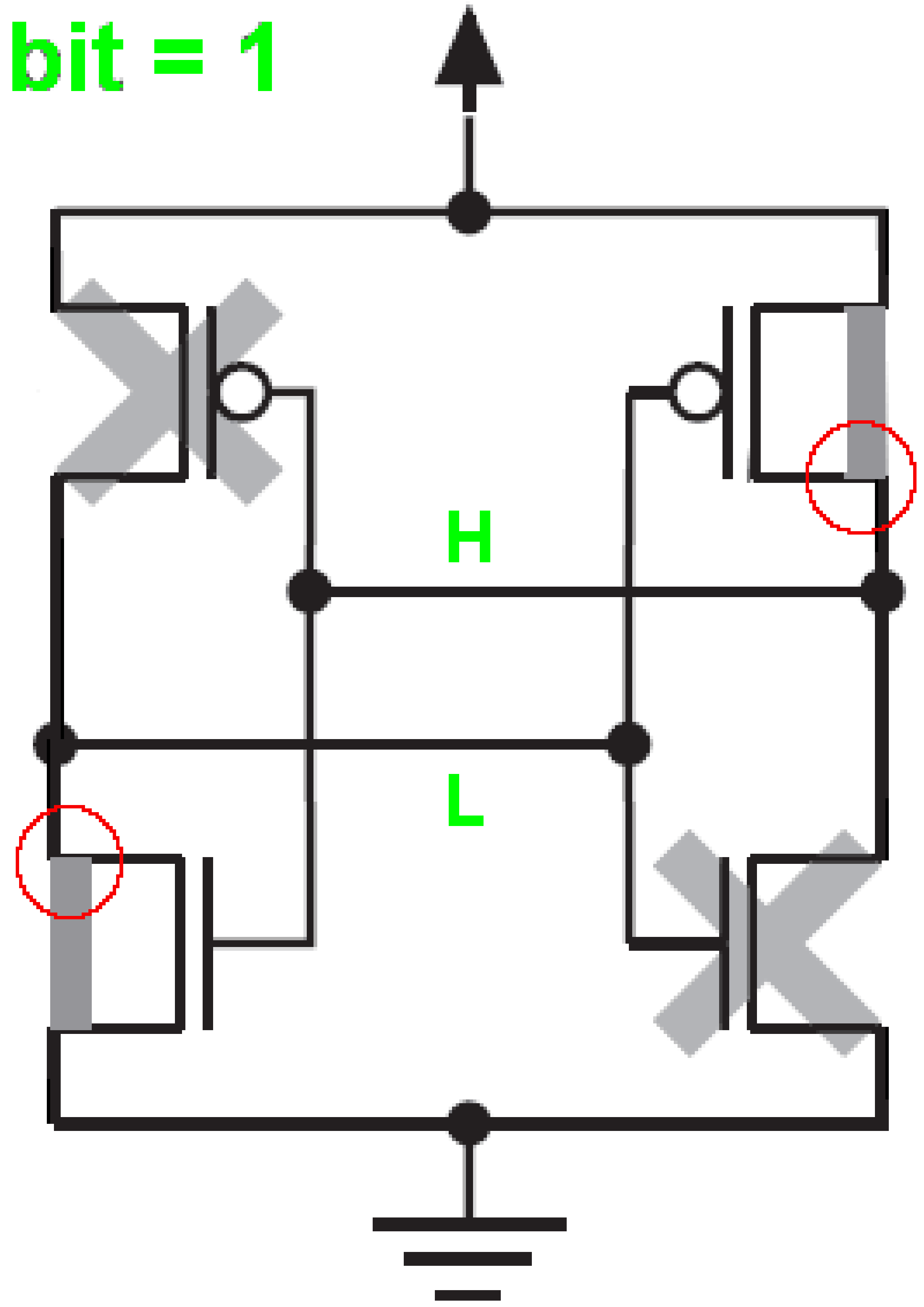
SRAM readout using TLS (1)

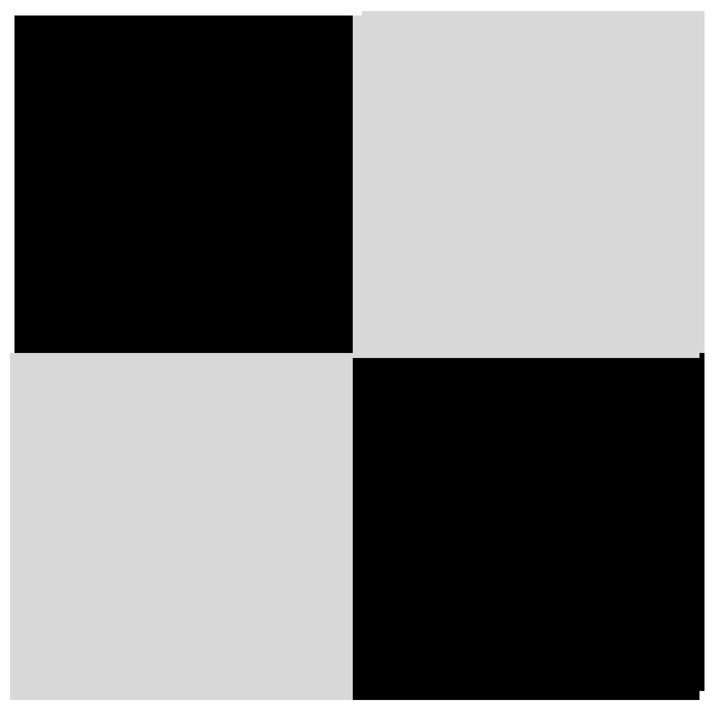
- Thermal stimulation leads to thermal gradient at the source/drain of the transistors
- Different materials lead to Seebeck voltage generation



SRAM readout using TLS (2)

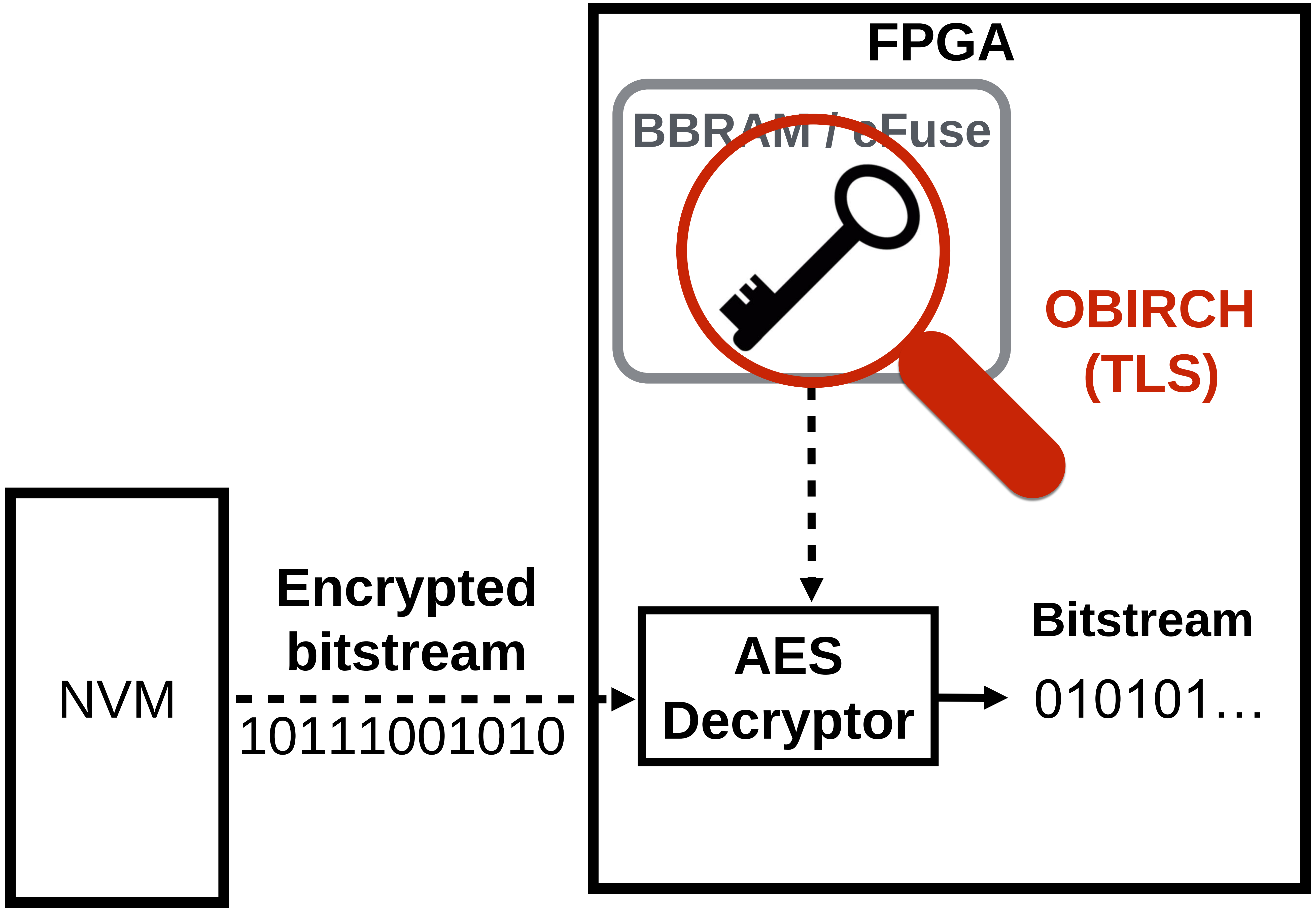






- The Seebeck voltage changes current flow through the "off" transistors >> leakage current increases
- Reaction of different areas of SRAM cells to TLS, depending on the stored value

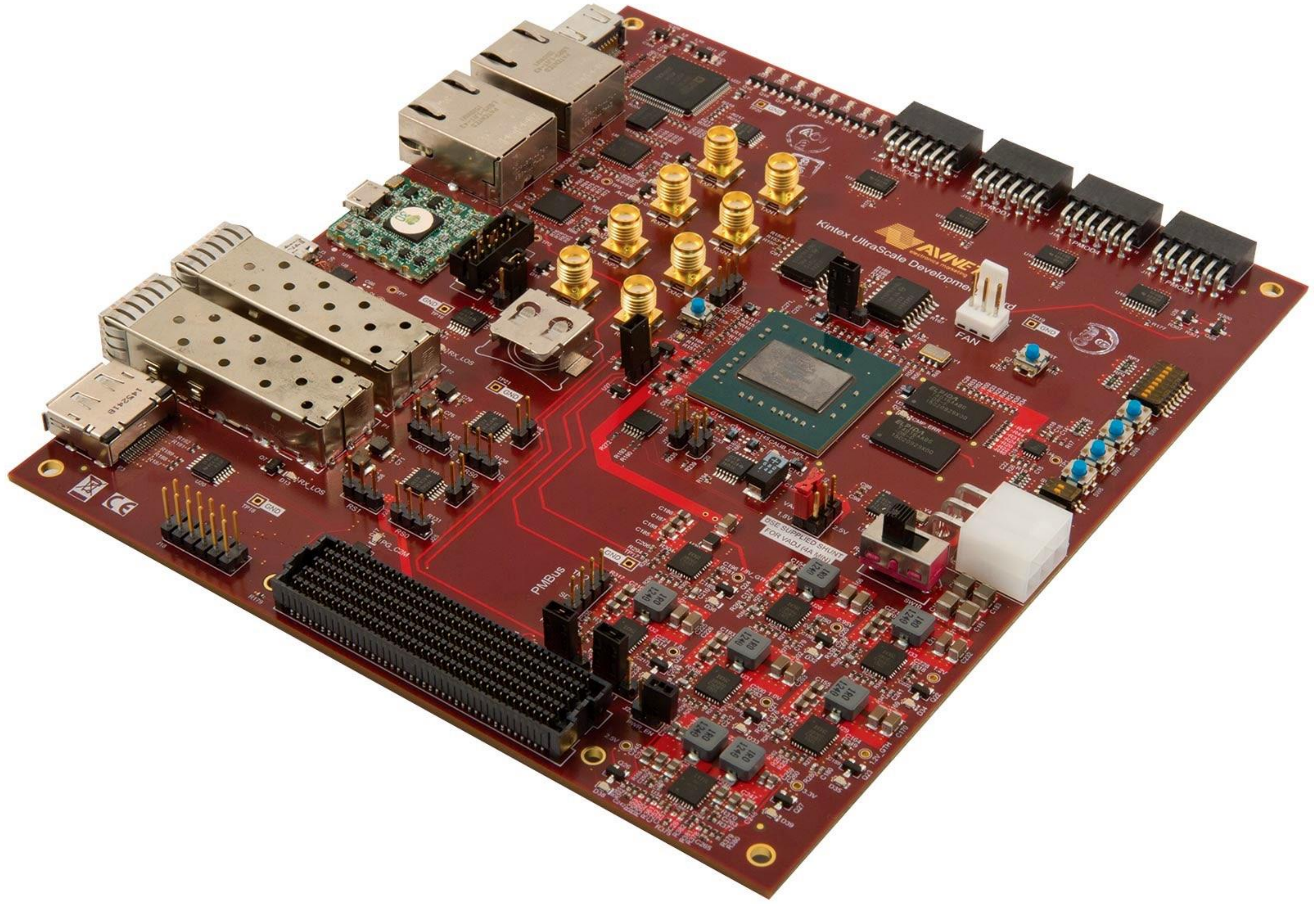
Key Extraction

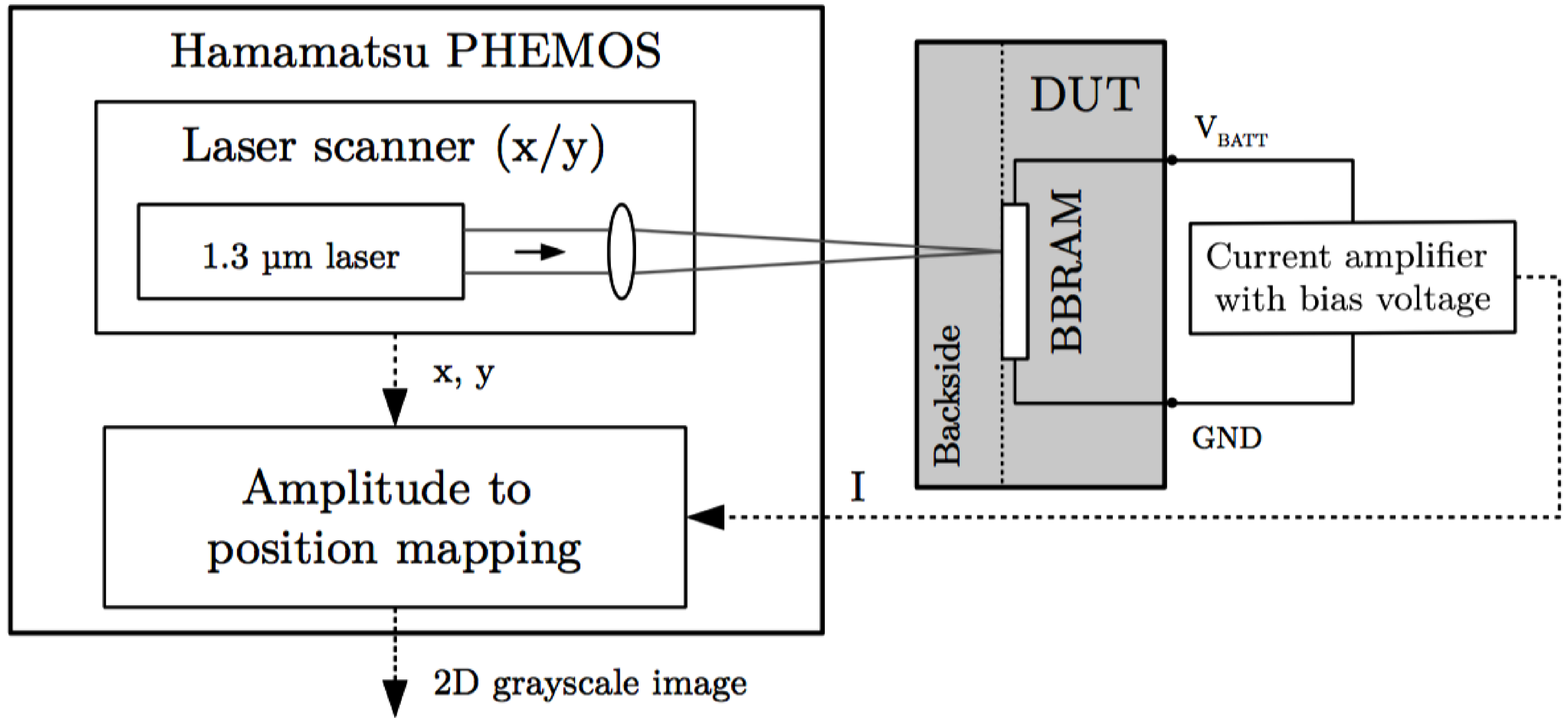


Lohrke, H., Tajik, S., Boit, C., & Seifert, J. P. “**Key Extraction Using Thermal Laser Stimulation: A Case Study on Xilinx Ultrascale FPGAs**,” *accepted for CHES 2018*

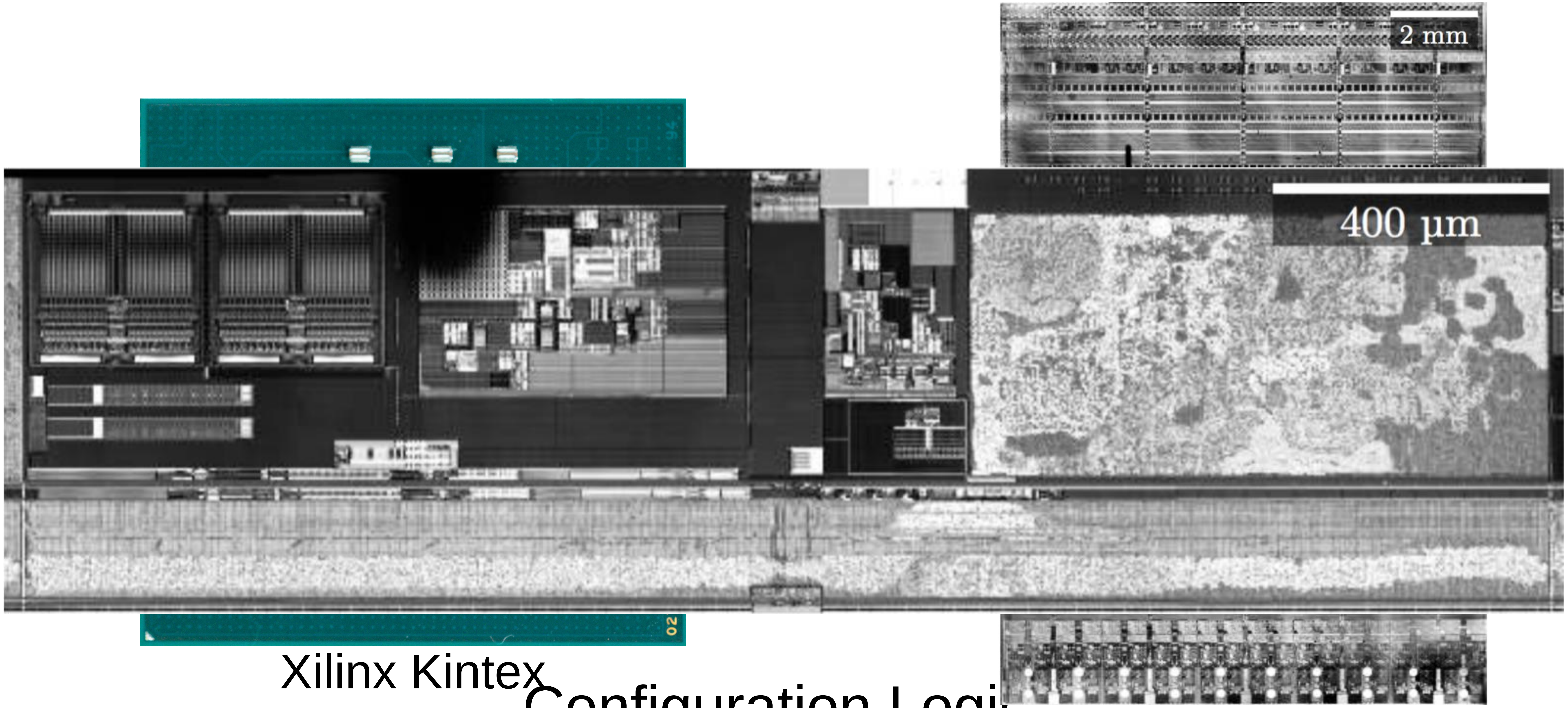
Experimental Setup

- **Device under Test (DUT):** Avnet Kintex UltraScale Development Board
  - Chip's technology: 20 nm
  - No chip preparation (e.g., depackaging, silicon polishing, etc.) required
- **Optical Setup:** Hamamatsu PHEMOS-1000
  - Laser wavelengths: 1.1 and 1.3 μm
  - Laser spot size: approximately 1 μm





Localizing the Configuration Logic



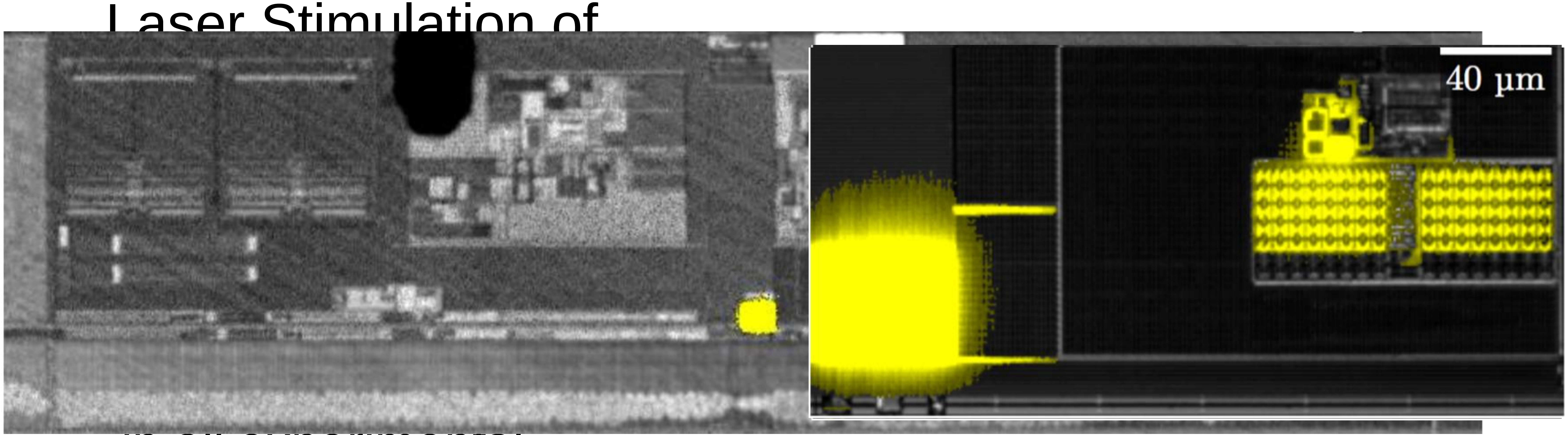
Xilinx Kintex UltraScale in flip chip package

Configuration Logic

Image acquisition with a laser scanning microscope

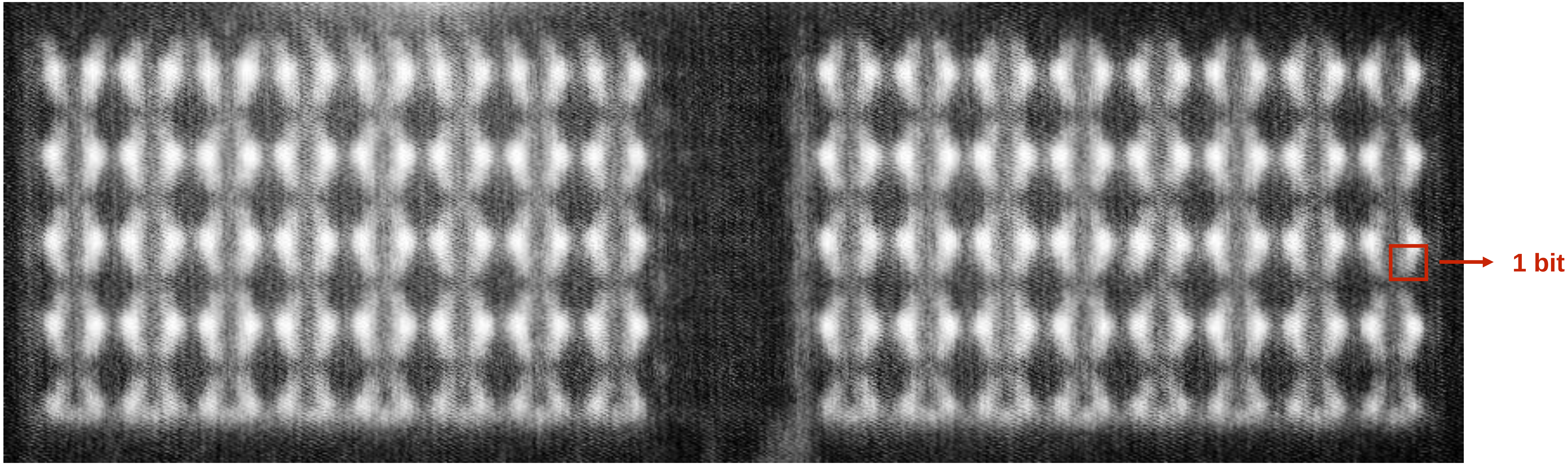
Localizing BBRAM using Laser Stimulation

Laser Stimulation of



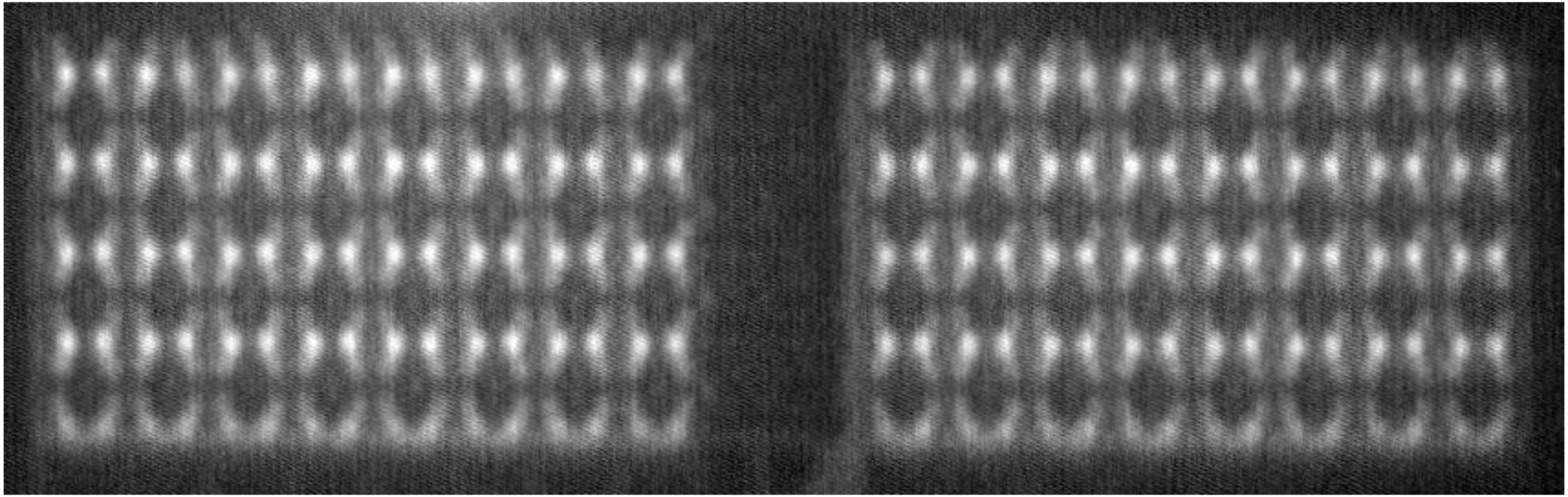
in all experiments!

Localizing the key bits in BBRAM by TLS



Set 255 bits to “0” and one bit to “1”.
Shifting the bit “1” eight times by one bit

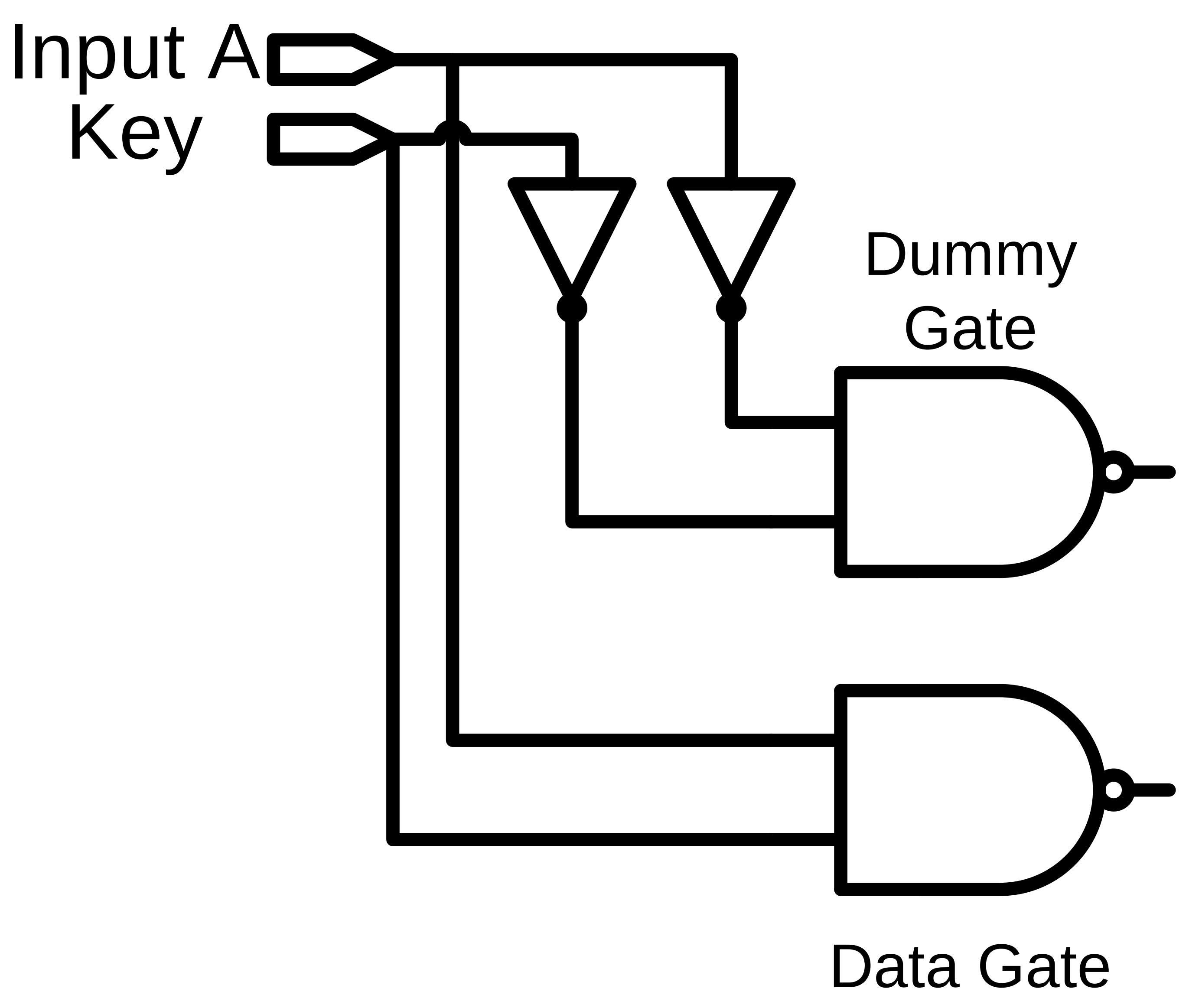
Localizing the key bits in BBRAM

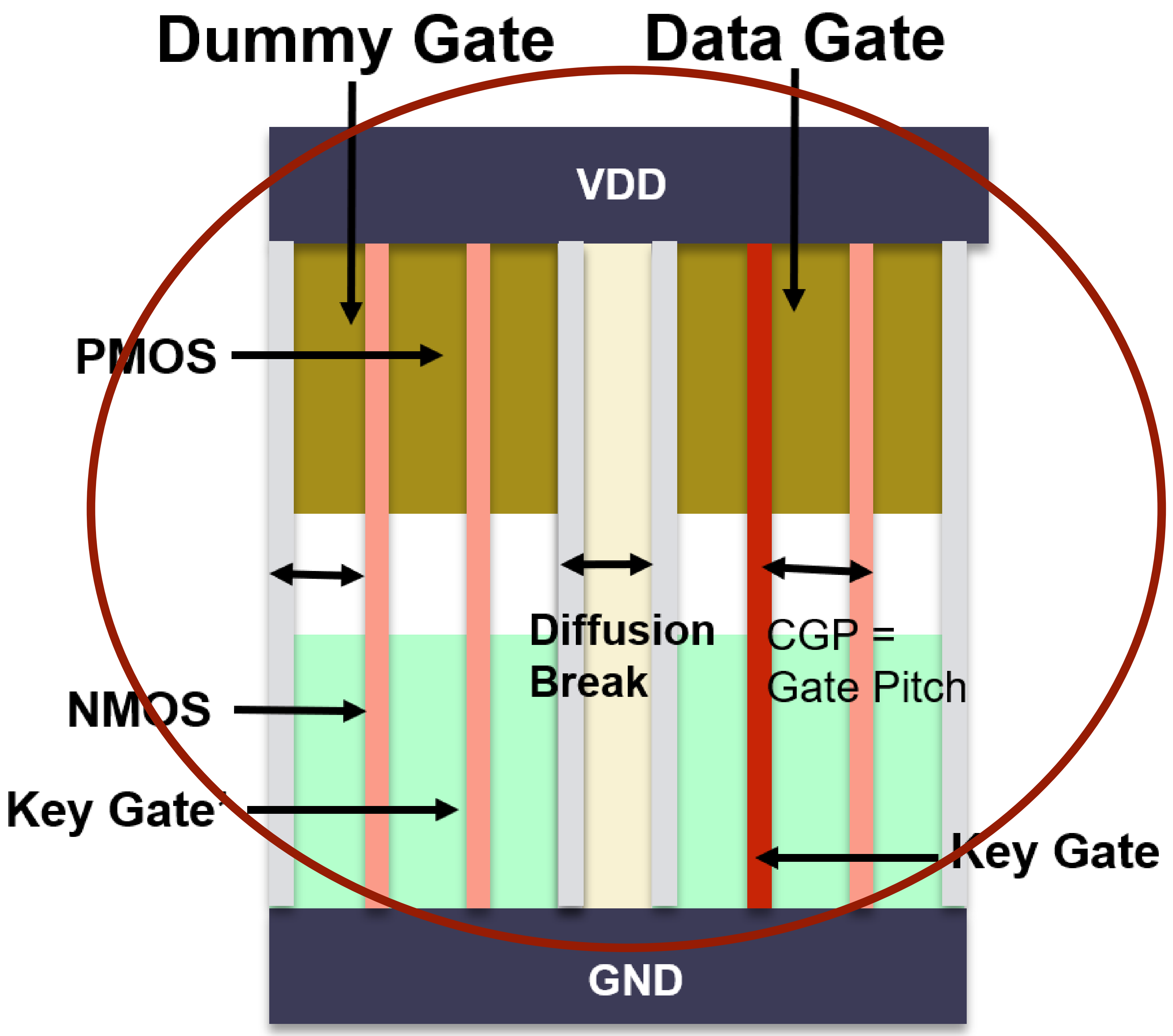


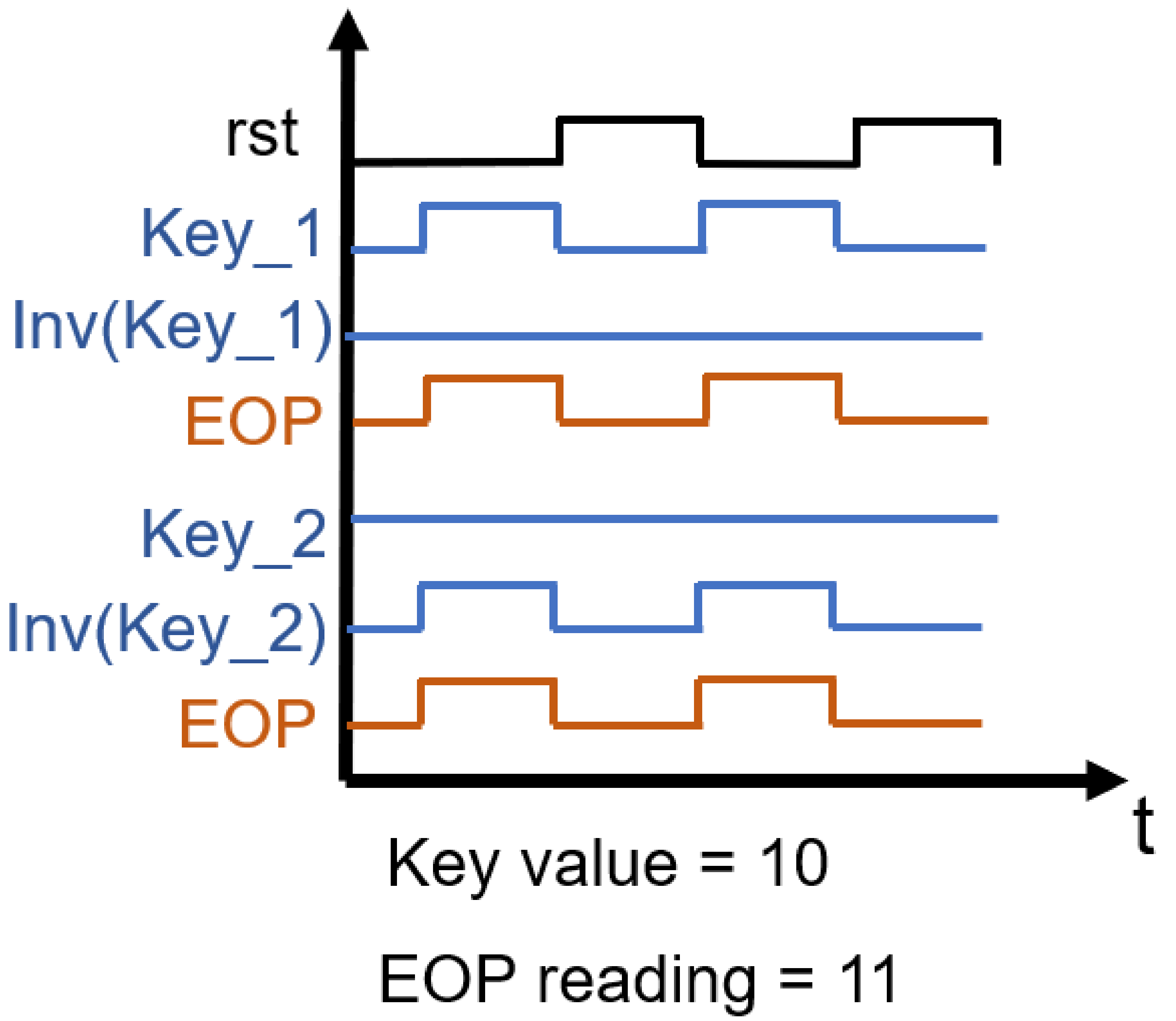
Set all 256 bits to “1” and reset all bits to “0” again.

Countermeasures against Optical Attacks

Circuit Based Solution: Dummy Gate

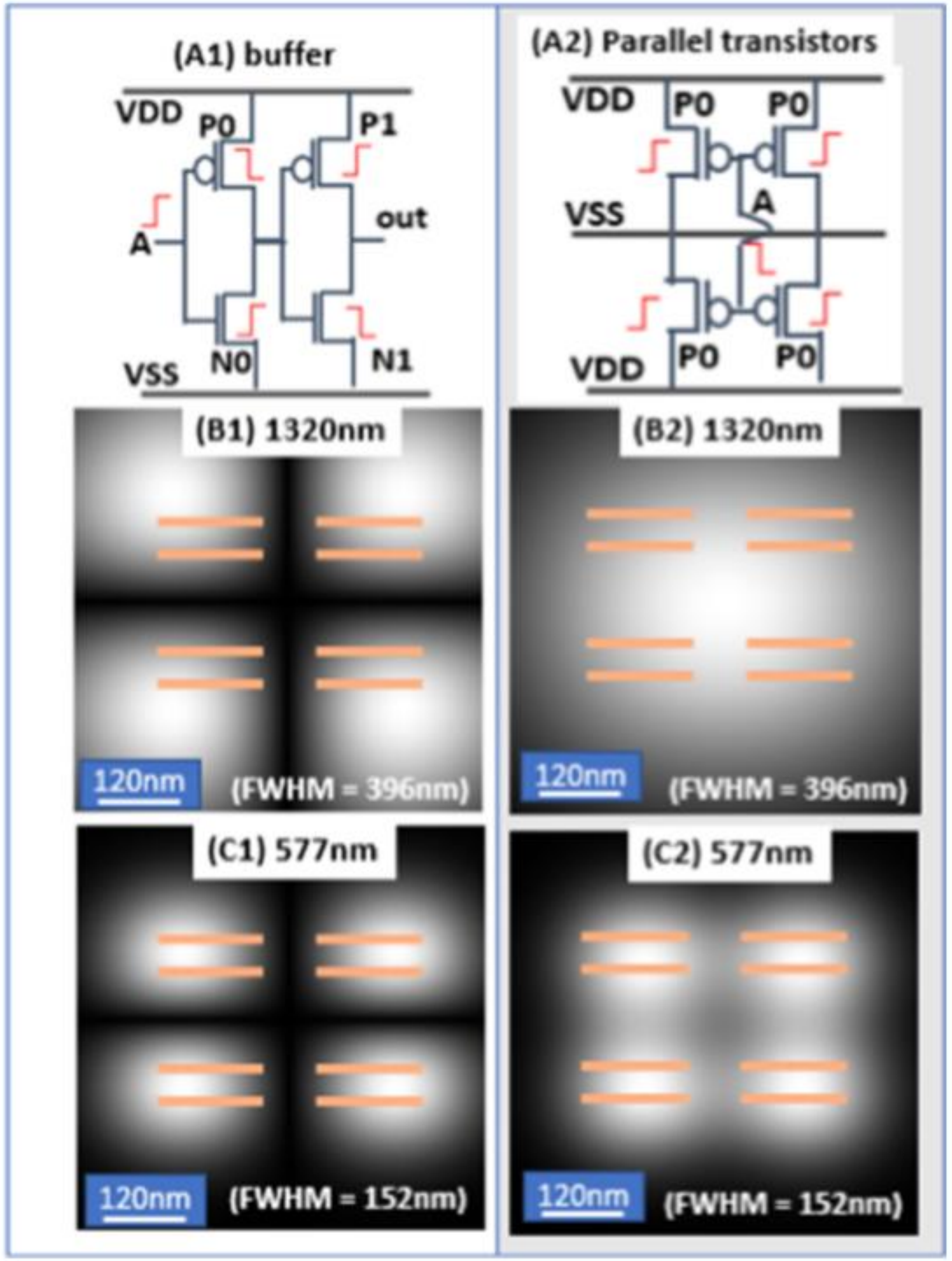






- In physical layout, dummy gate and data gate will be placed at lower distance than optical resolution
- Necessary to localize exact transistor connected to key → security by maximizing time-cost

Concealing Gate: EOFM Protection



- Two transistors operating at same frequency and switching at same direction, i.e., either 1→0 or vice versa, is difficult to differentiate. (see A2 implementation)
- Two transistors operating at same frequency but with opposite switching direction will be easy to distinguish, though the transistors may be placed lower than optical resolution distance. (see A1 implementation)

Concealing Gate: EOFM Protection

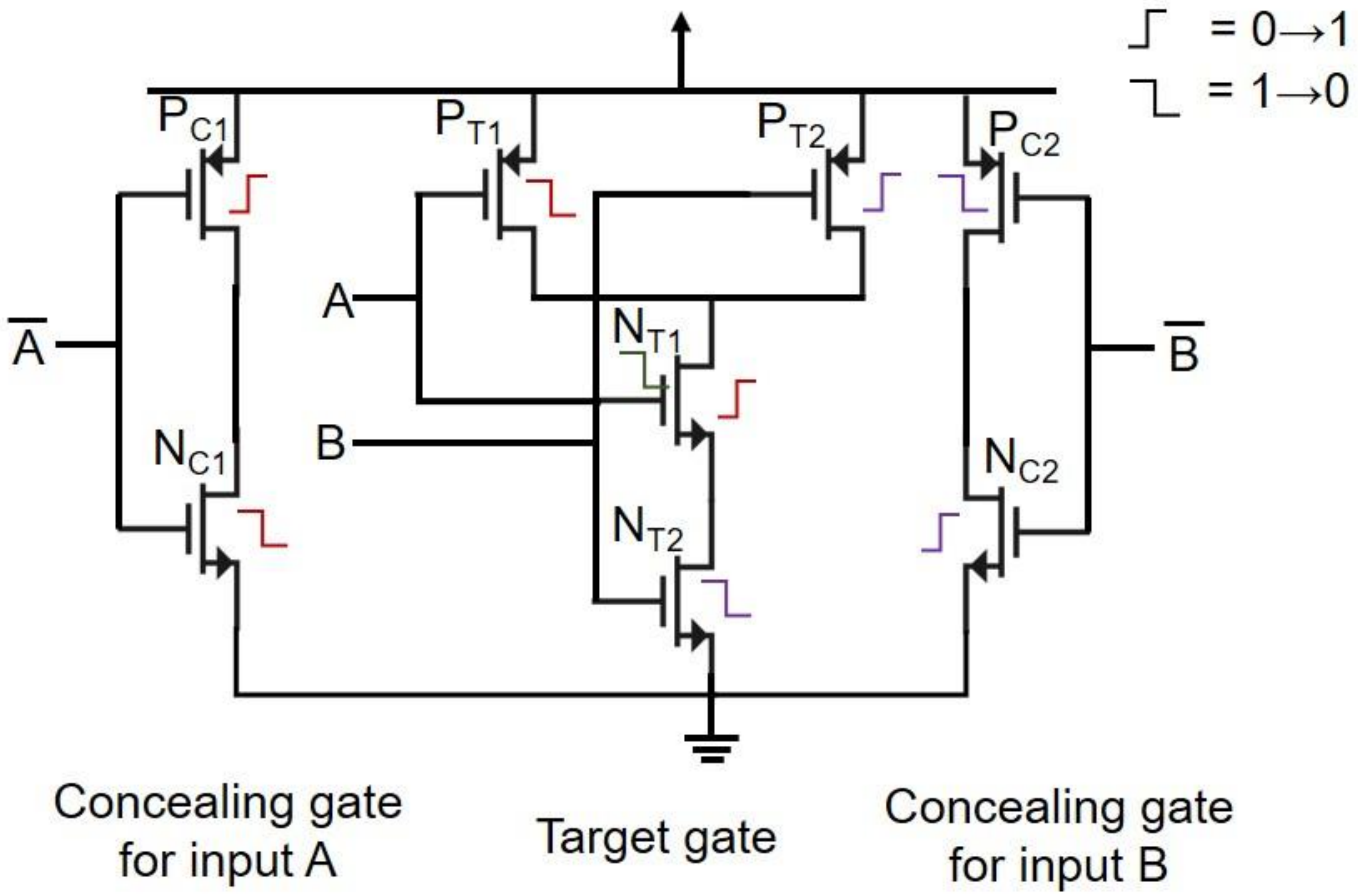


Fig. A

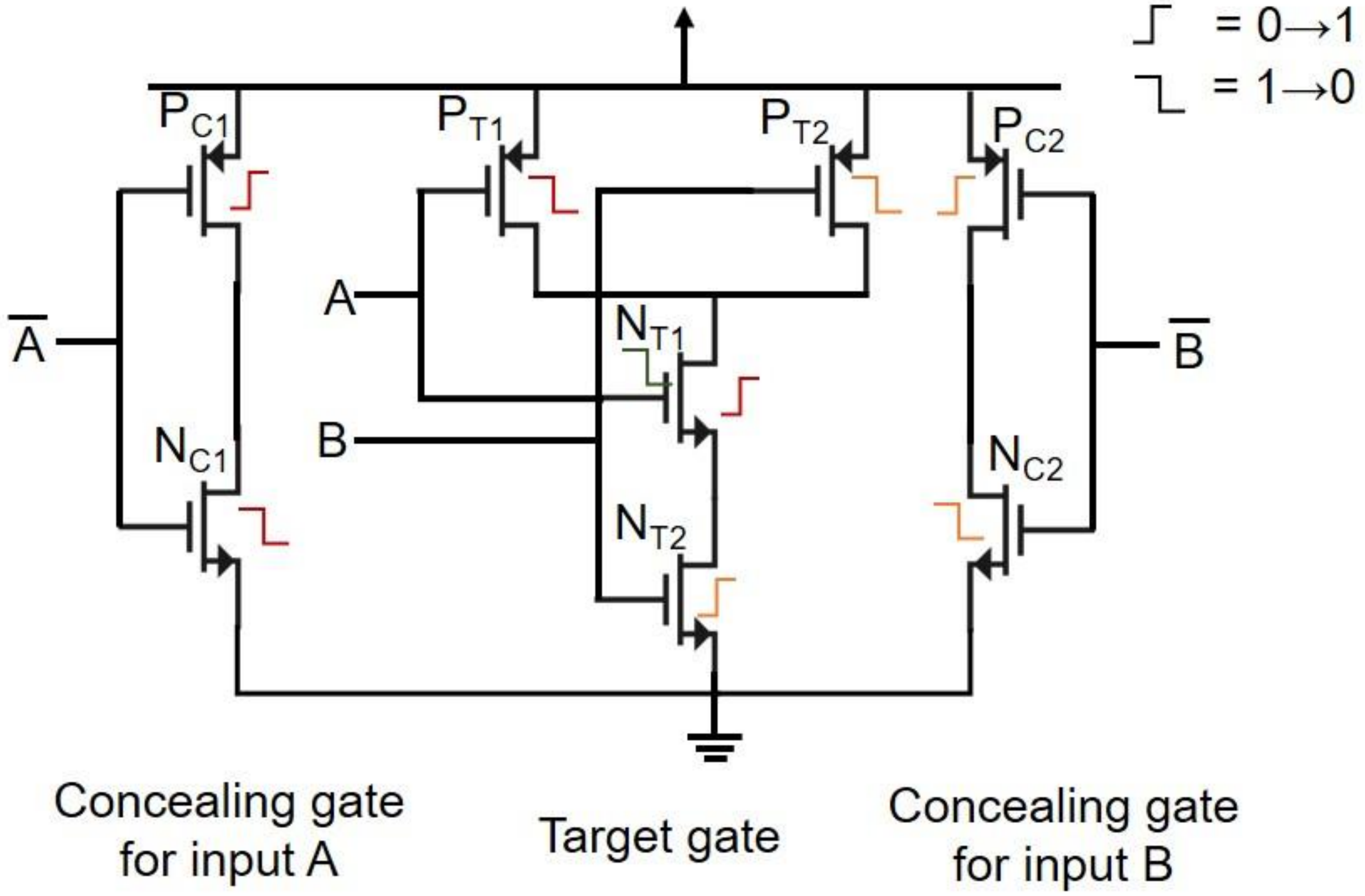
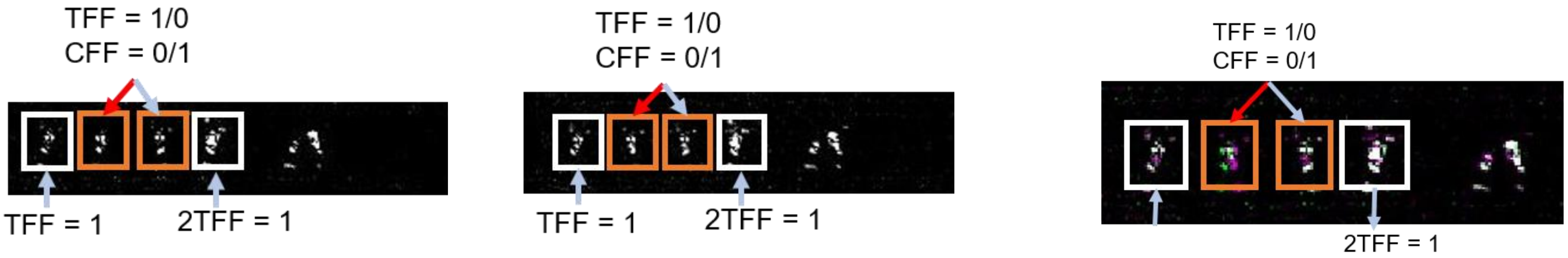


Fig. B

- P_{C1} mask P_{T1} activity by merging the edges of P_{T2} (Fig A) or P_{C2}(Fig. B). If distance between P_{C1} and P_{C2} is less than optical resolution, the PT1 transistor can be assumed to be protected.

Concealing Gate: EOFM/EOP Protection

EOFM Data with Concealing Gate



TFF = 1/0
CFF = 0/1

TFF = 1

2TFF = 1

TFF = 1/0
CFF = 0/1

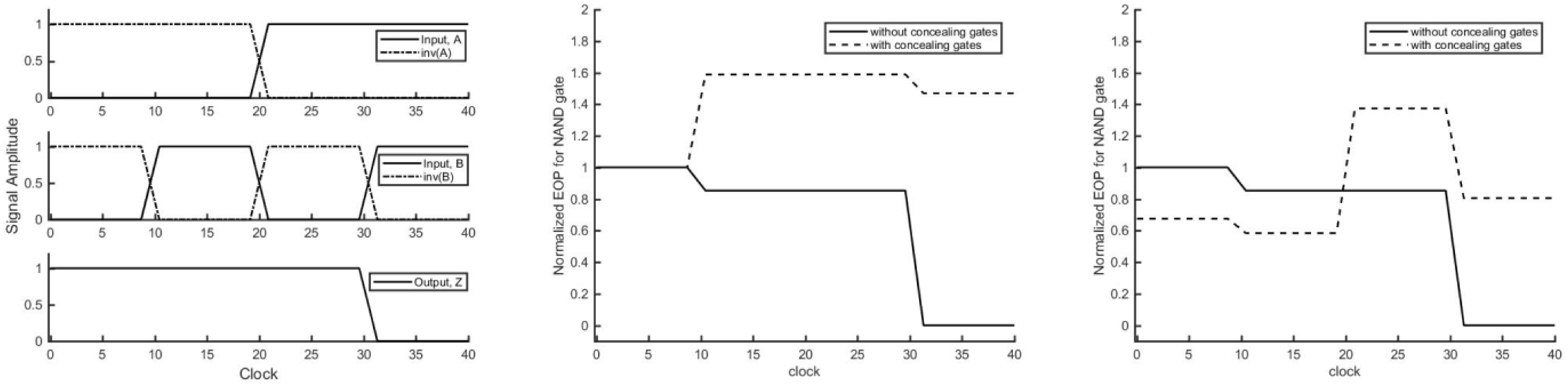
TFF = 1

2TFF = 1

TFF = 1/0
CFF = 0/1

2TFF = 1

EOP Data with Concealing Gate

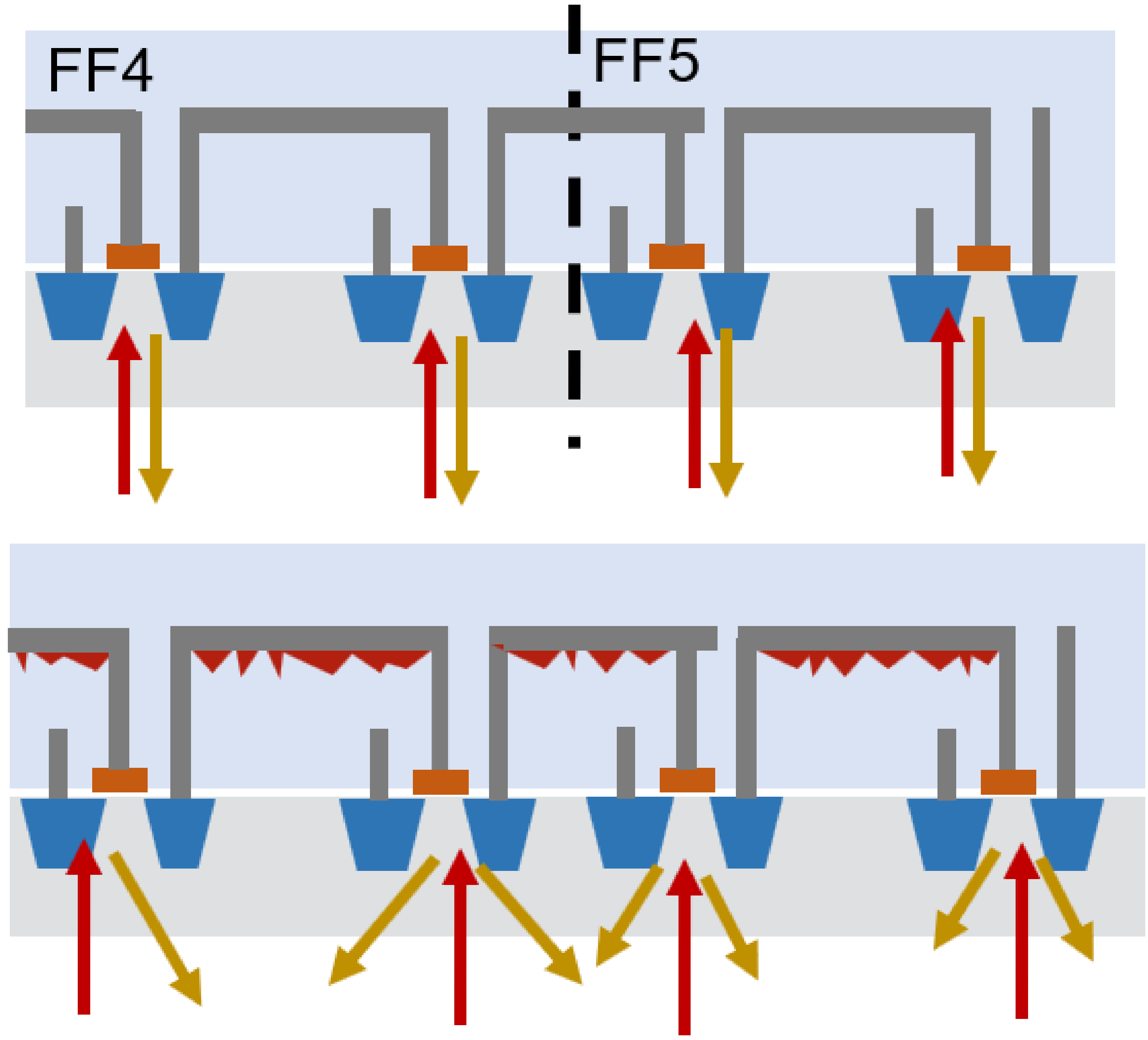


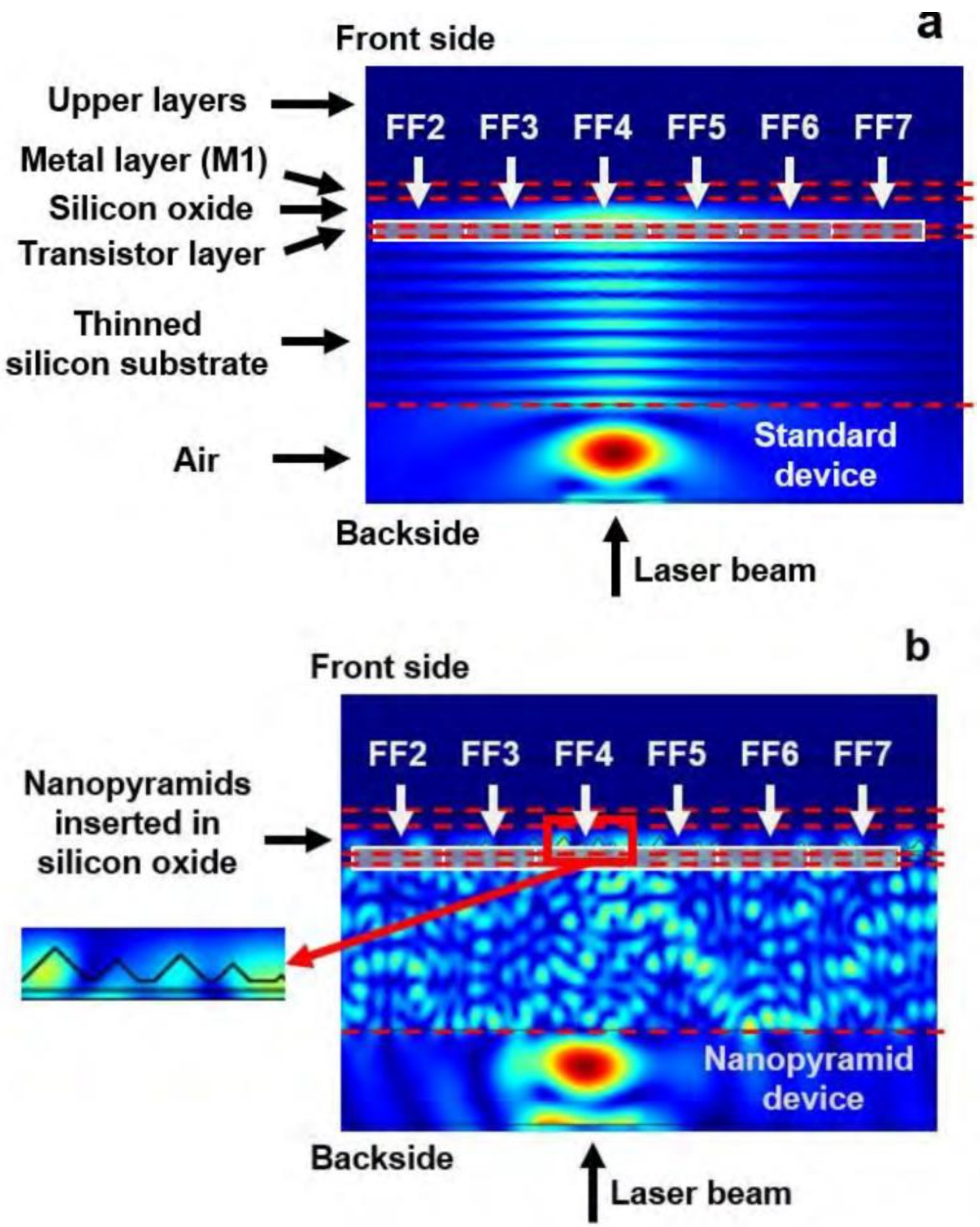
(a)

(b)

(c)

Nanopyramid to Camouflage Circuit Activity



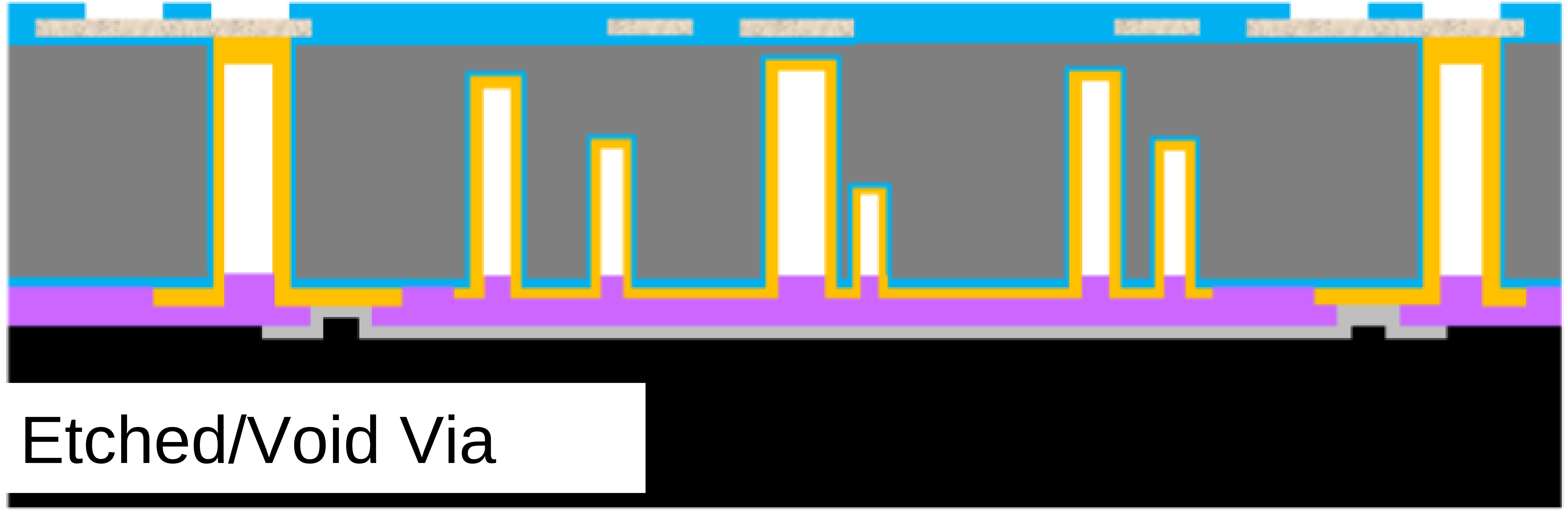


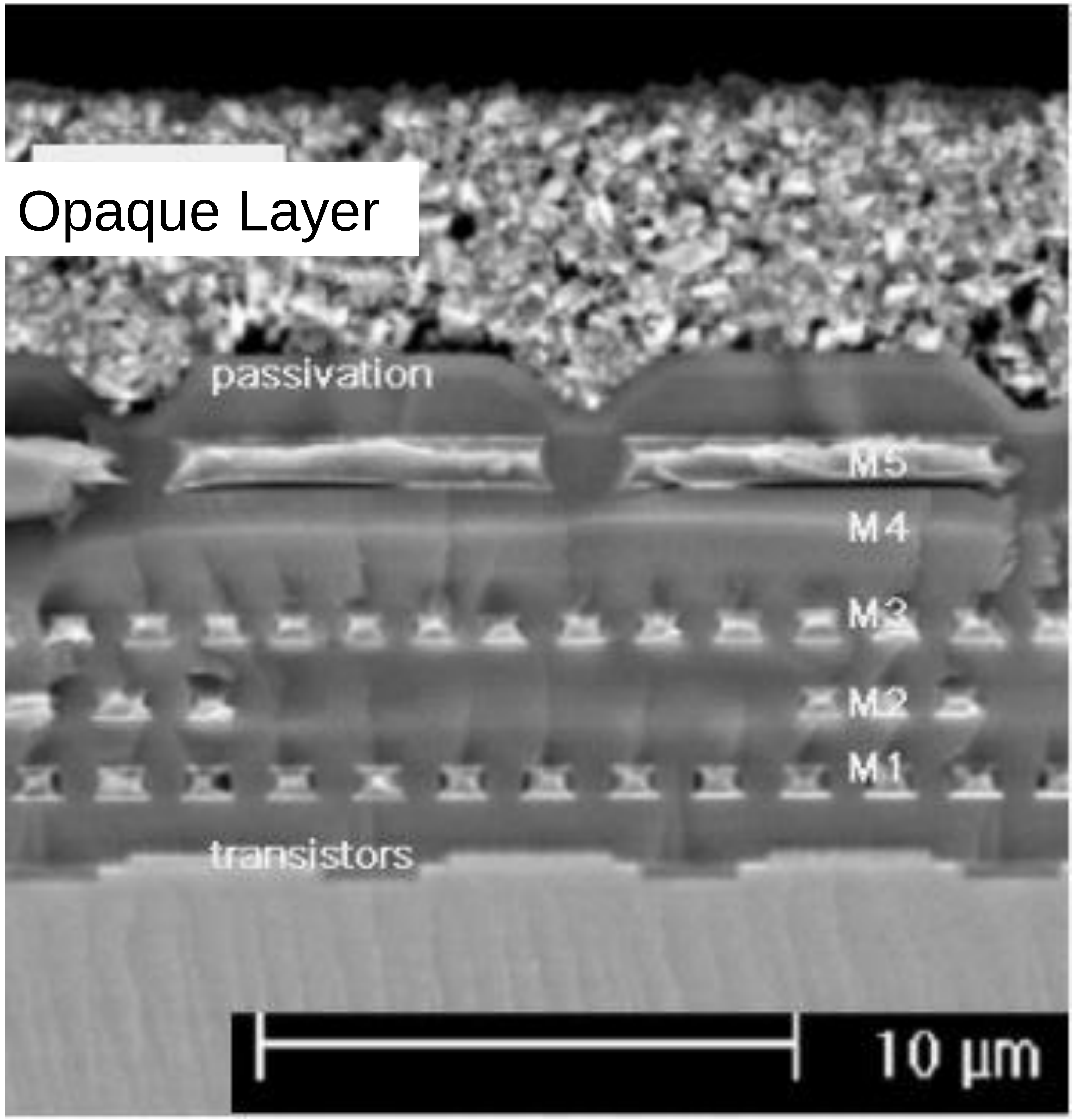
- ➢ Laser scattering is applicable for any l

  aser based attack approach
- ➢ No additional power or area

All Rights Reserved

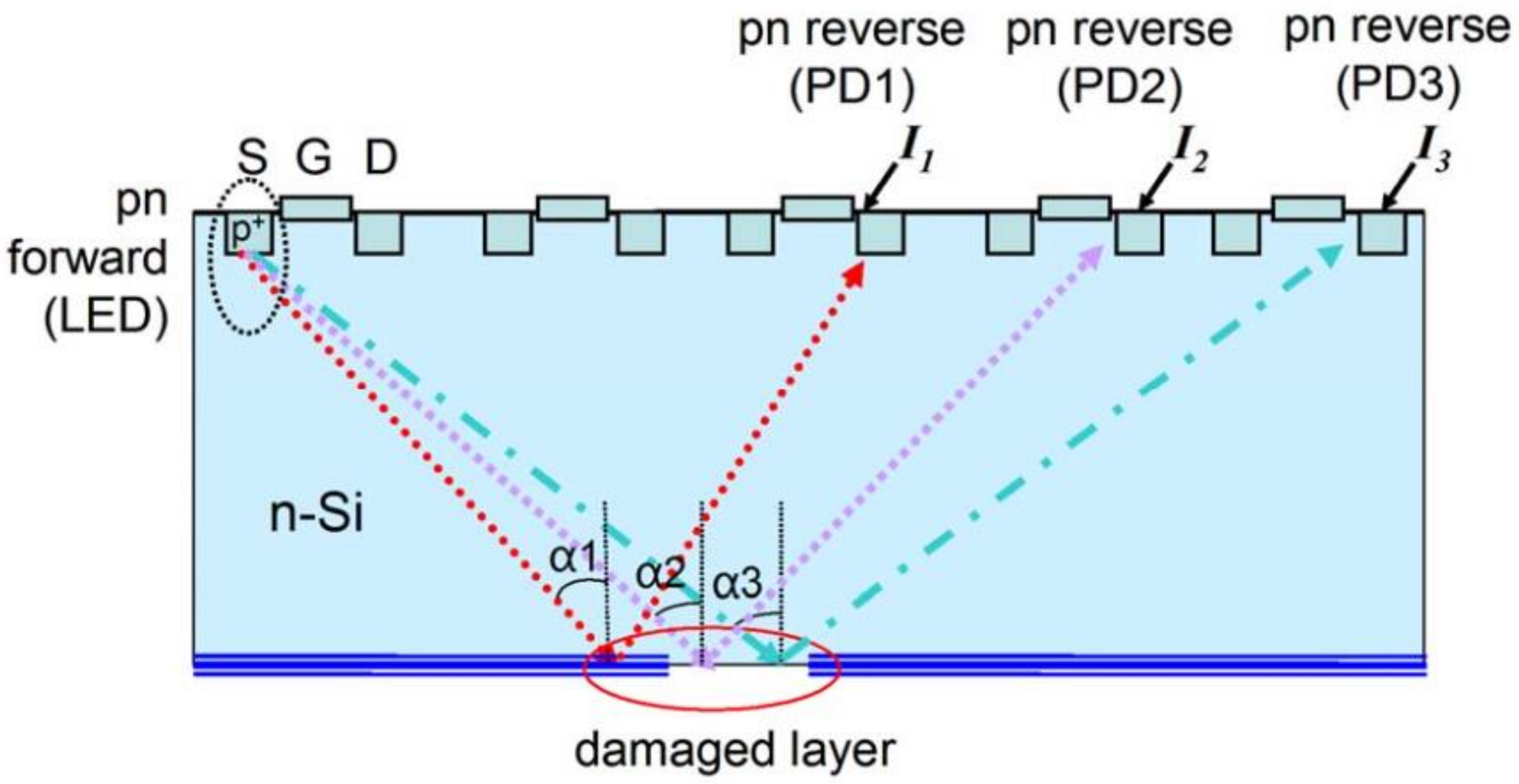
Material Based Solution: Literature Review

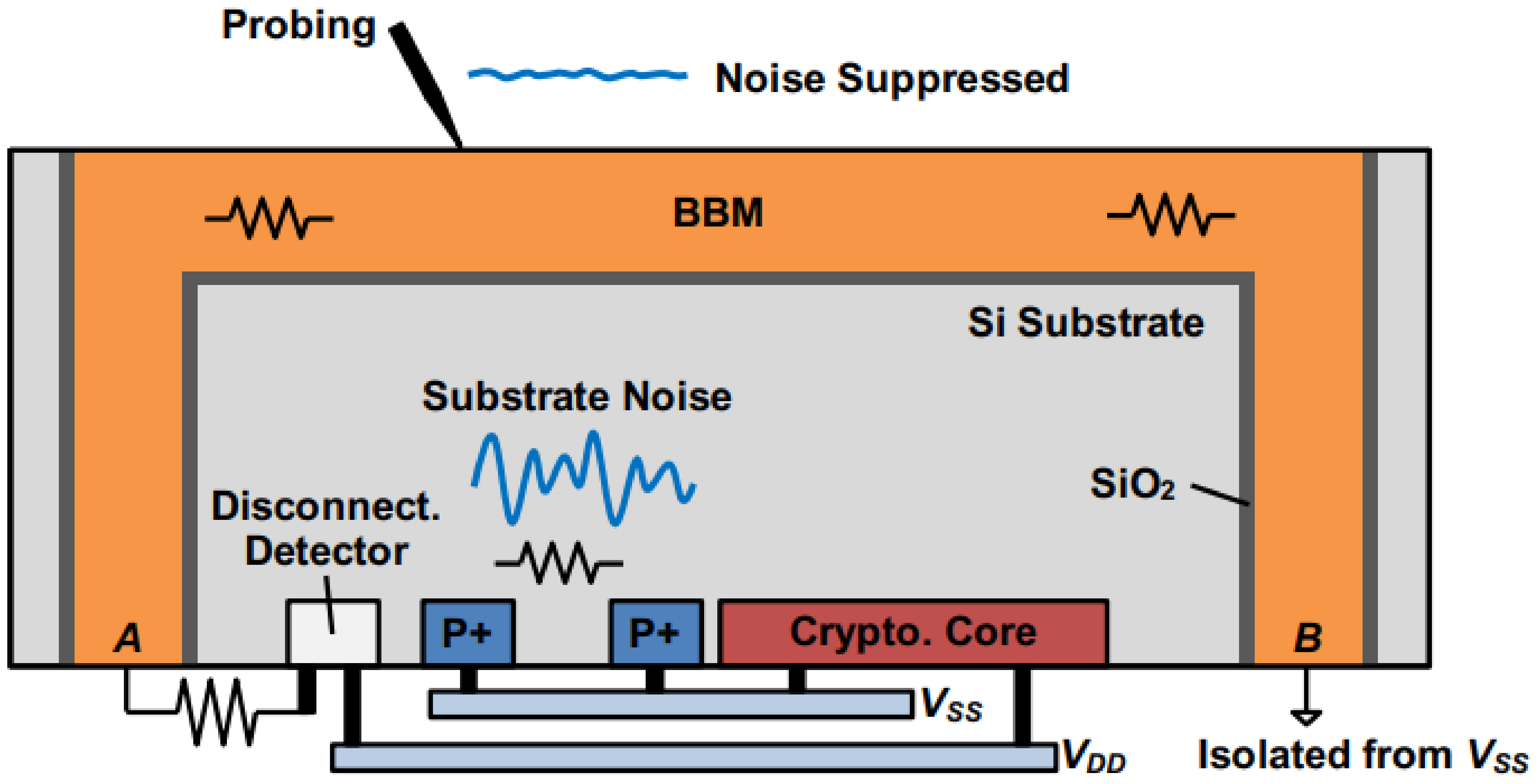


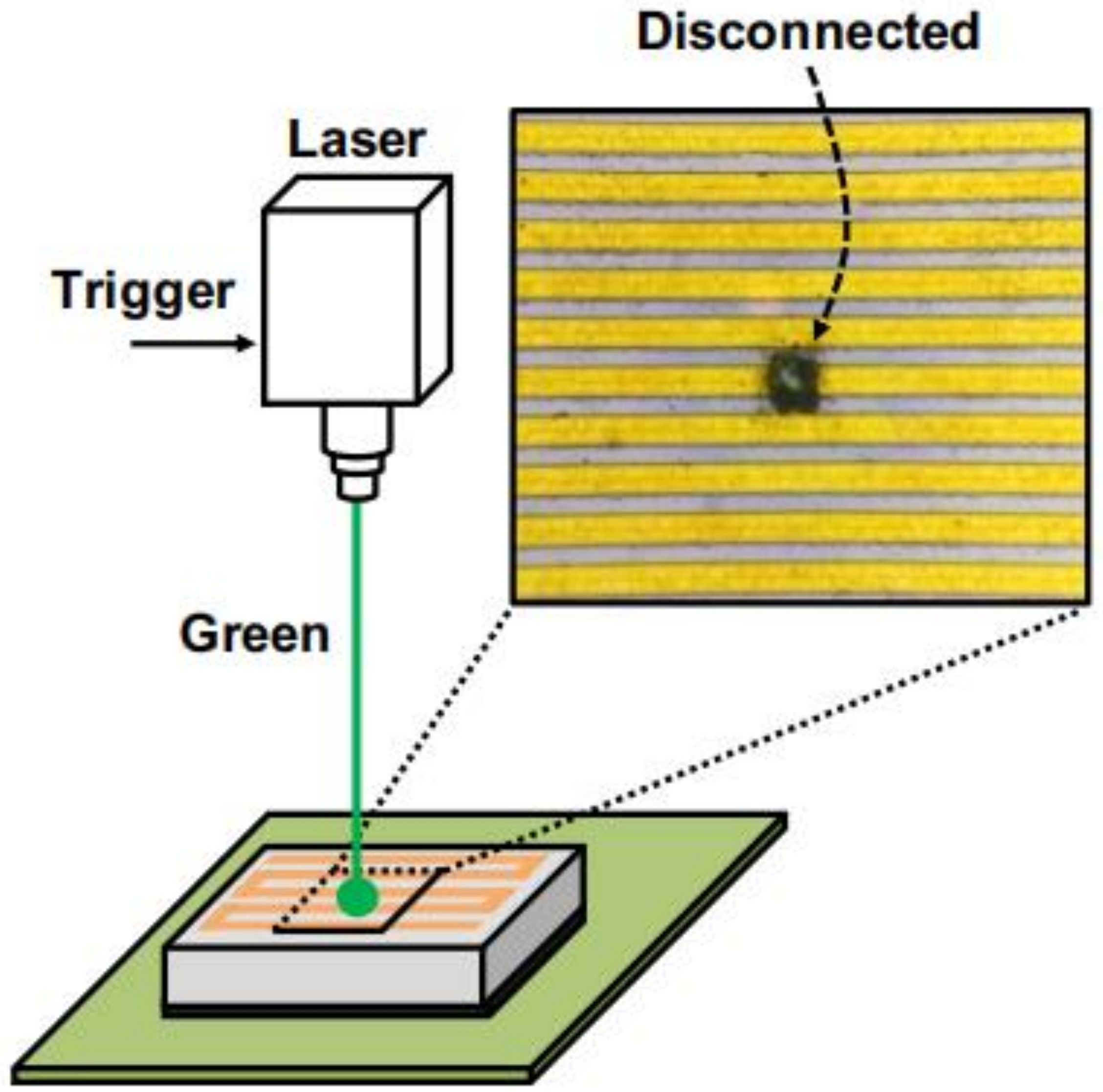


- **Etched/Void Via**
  - aging
  - reliability
- **Opaque layer**
  - Removable by polishing

Device Based Solution: Literature Review

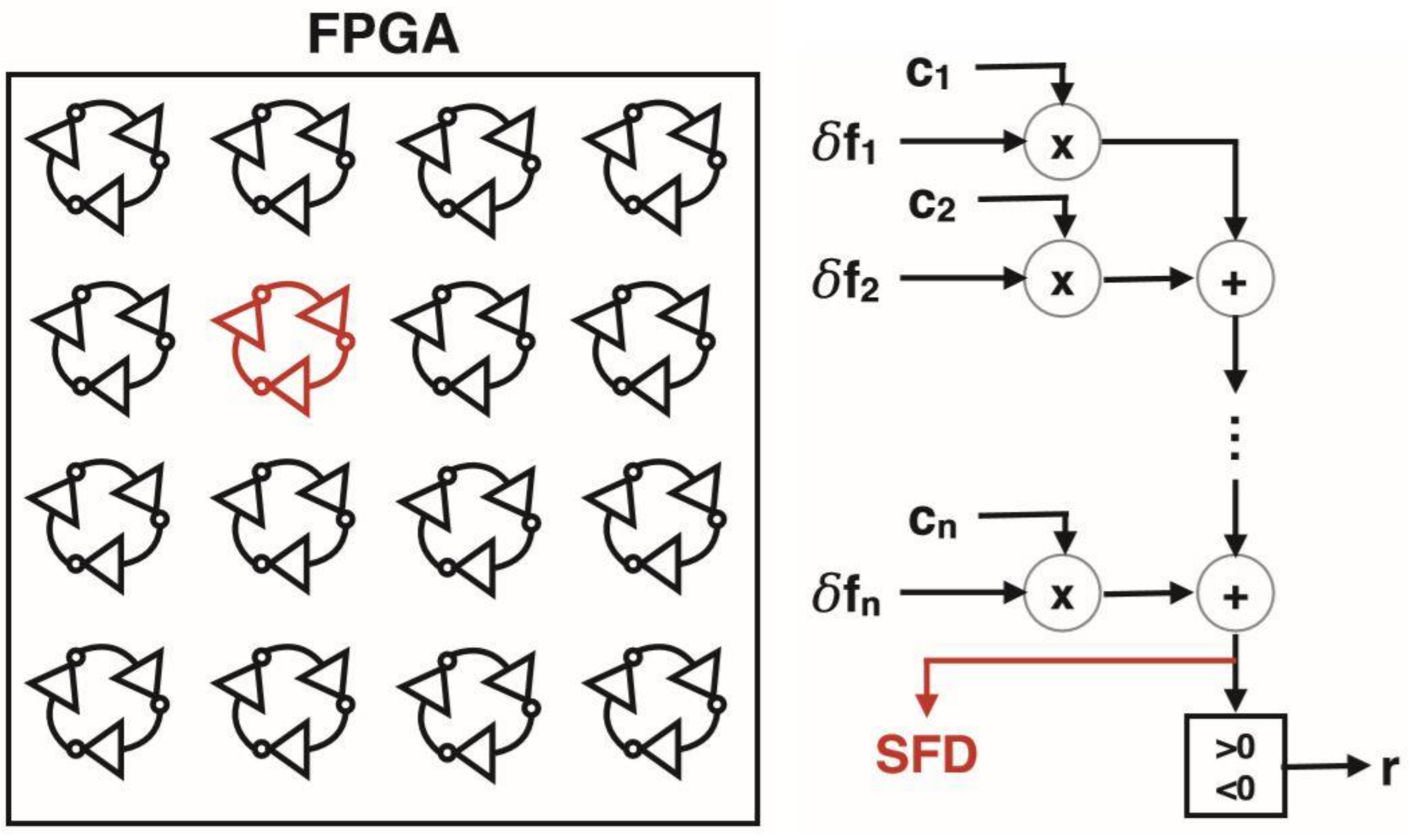




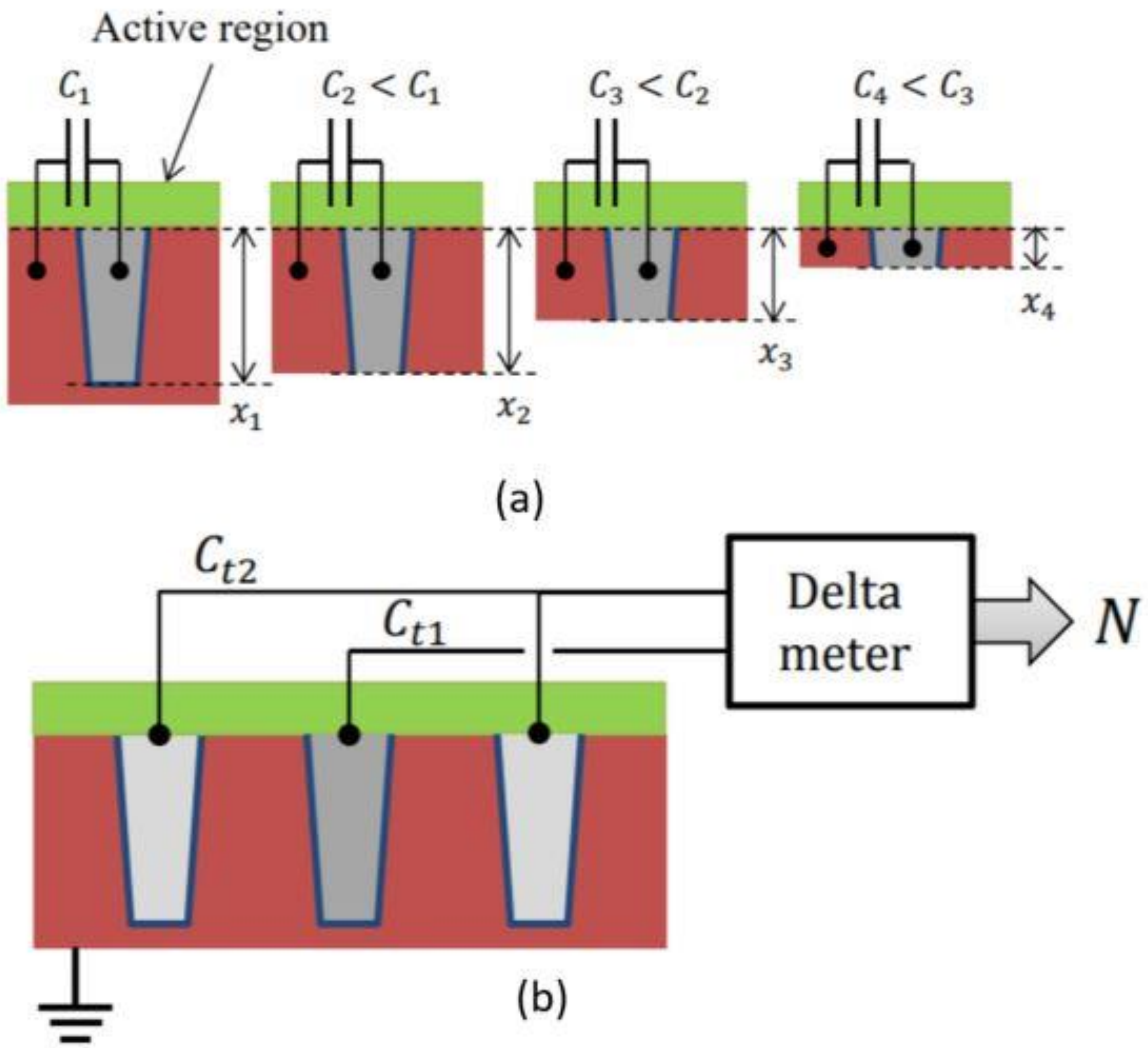


- **P-N photo diode:**
    - Applicable for LFI
- **Backside Mesh:**
    - Bypassed with circuit edit

Circuit Based Solution: Literature Review



(a) (b)



- Additional area and optimization required
- Mostly ineffective against thermal laser → focused on laser fault detection