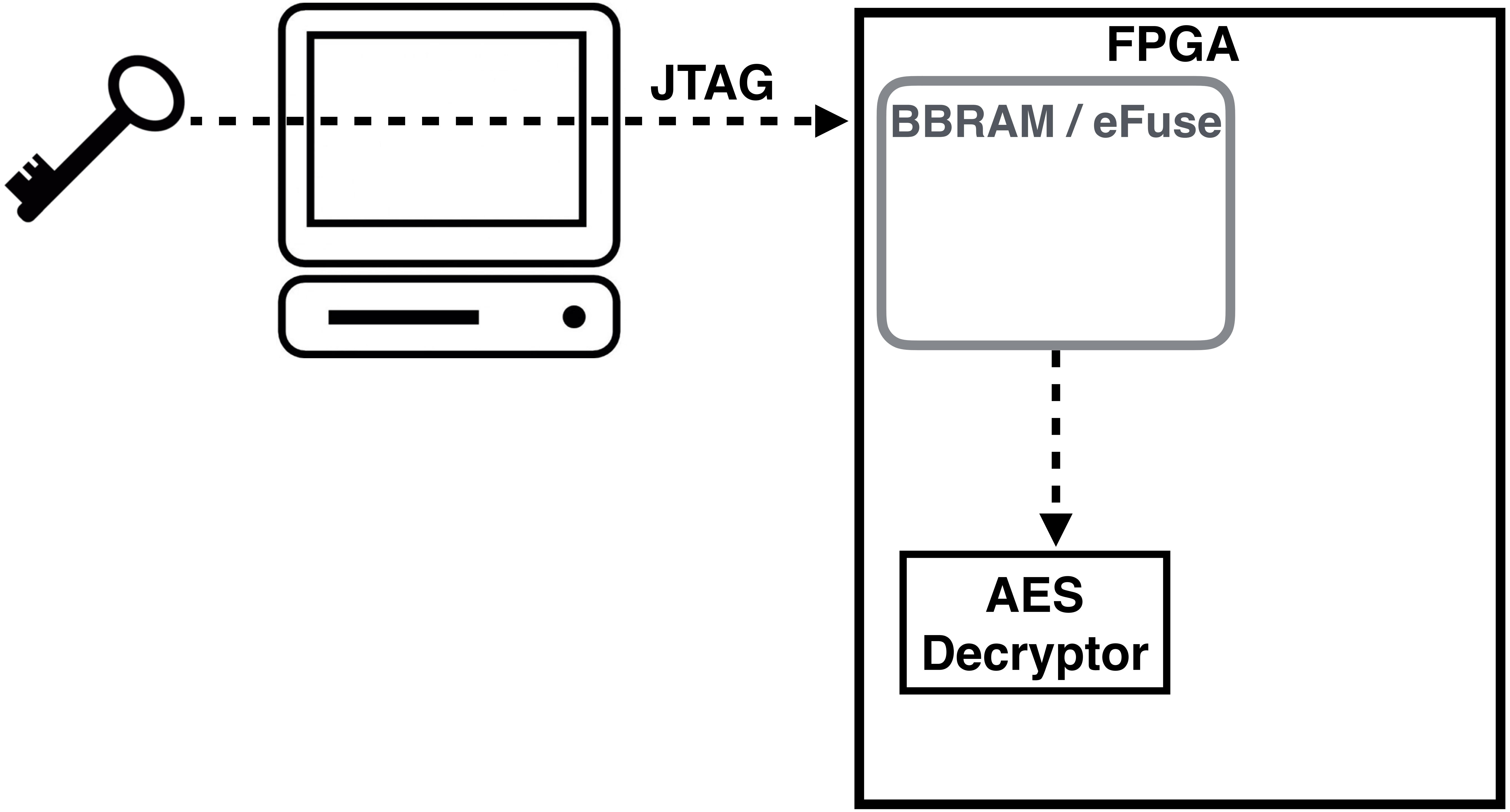
Key Extraction Using Thermal Laser Stimulation: A Case Study on Xilinx Ultrascale FPGAs

Heiko Lohrke[1], Shahin Tajik[1,2], Thilo Krachenfels[1], Christian Boit[1], and Jean-Pierre Seifert[1]
[1]Technische Universität Berlin, [2]University of Florida

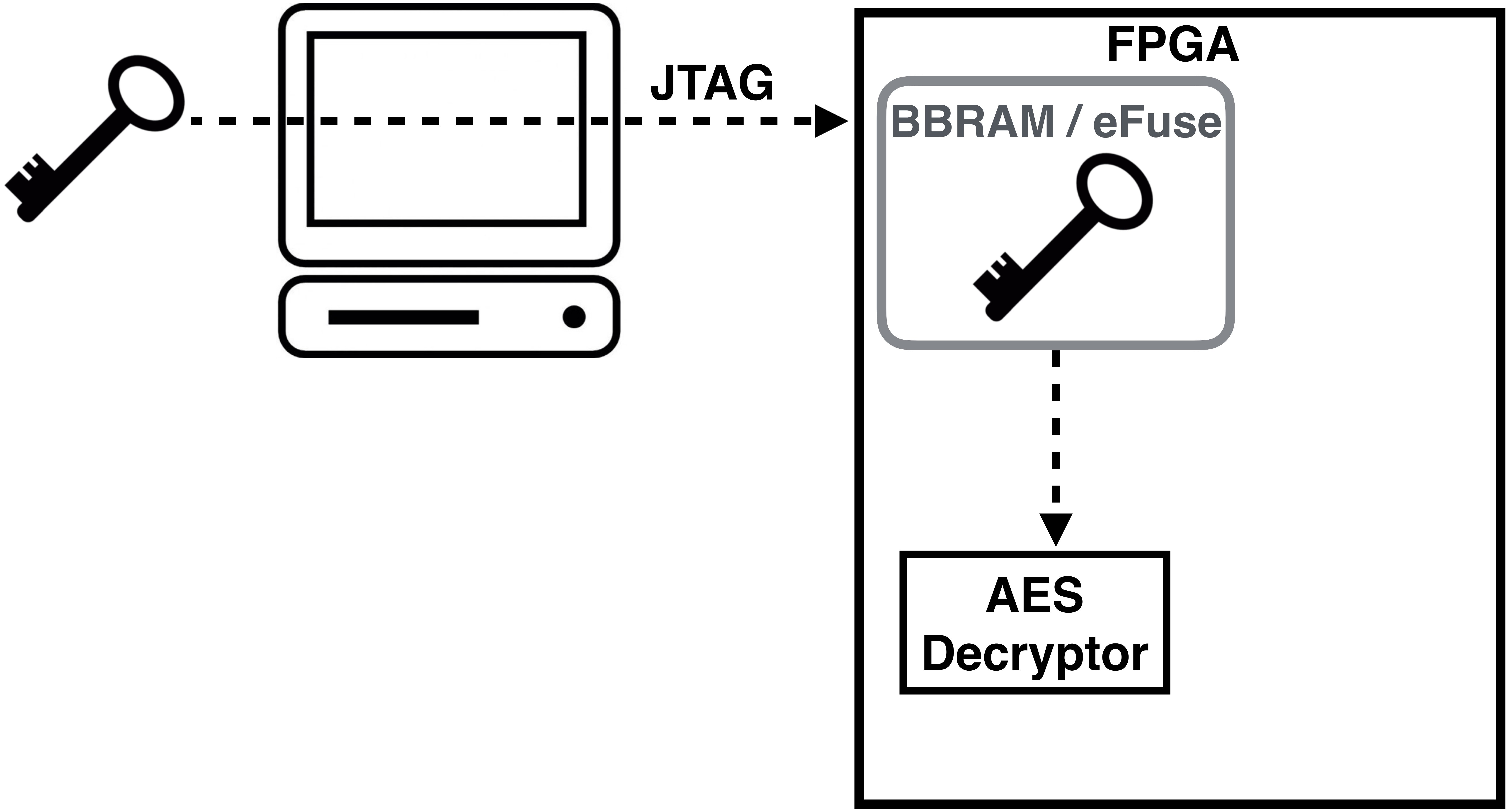
September 10th, 2018
CHES 2018

Background

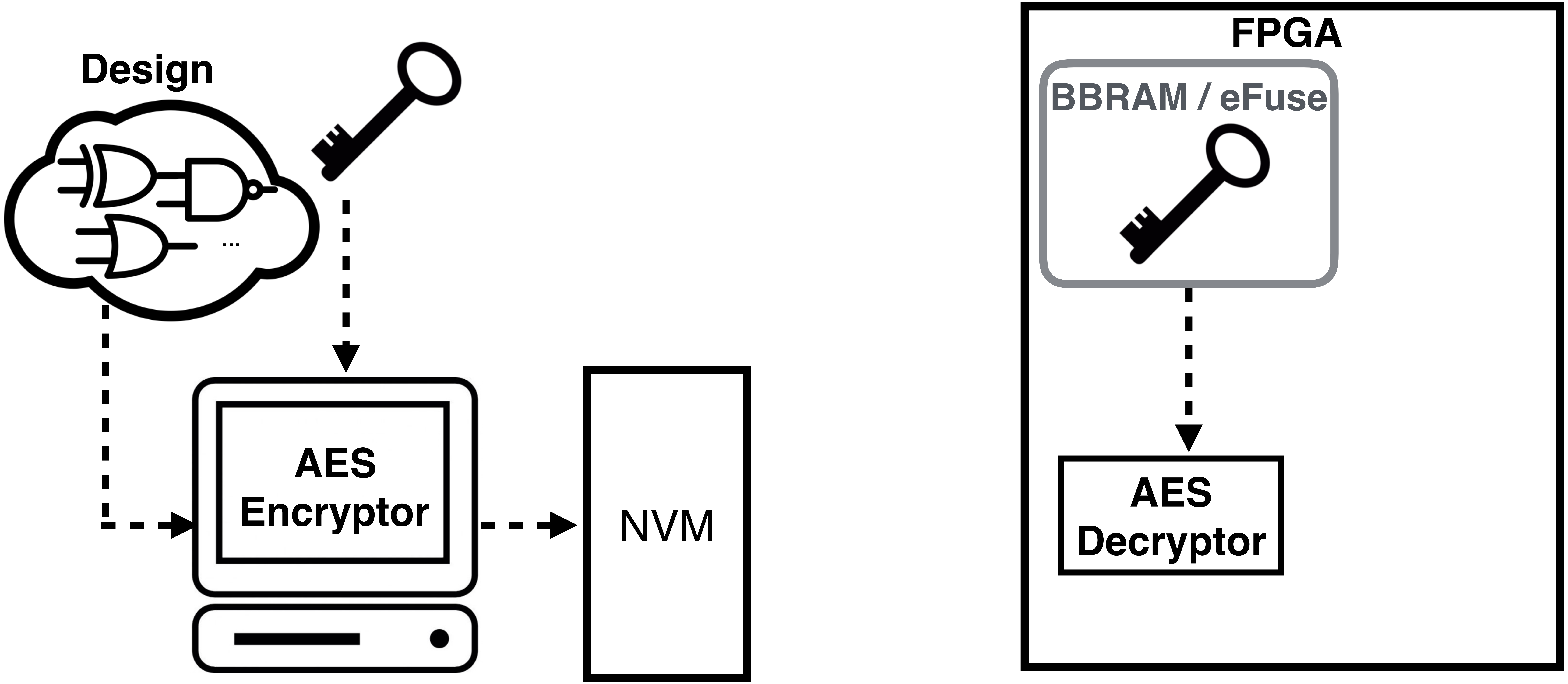
Bitstream Encryption



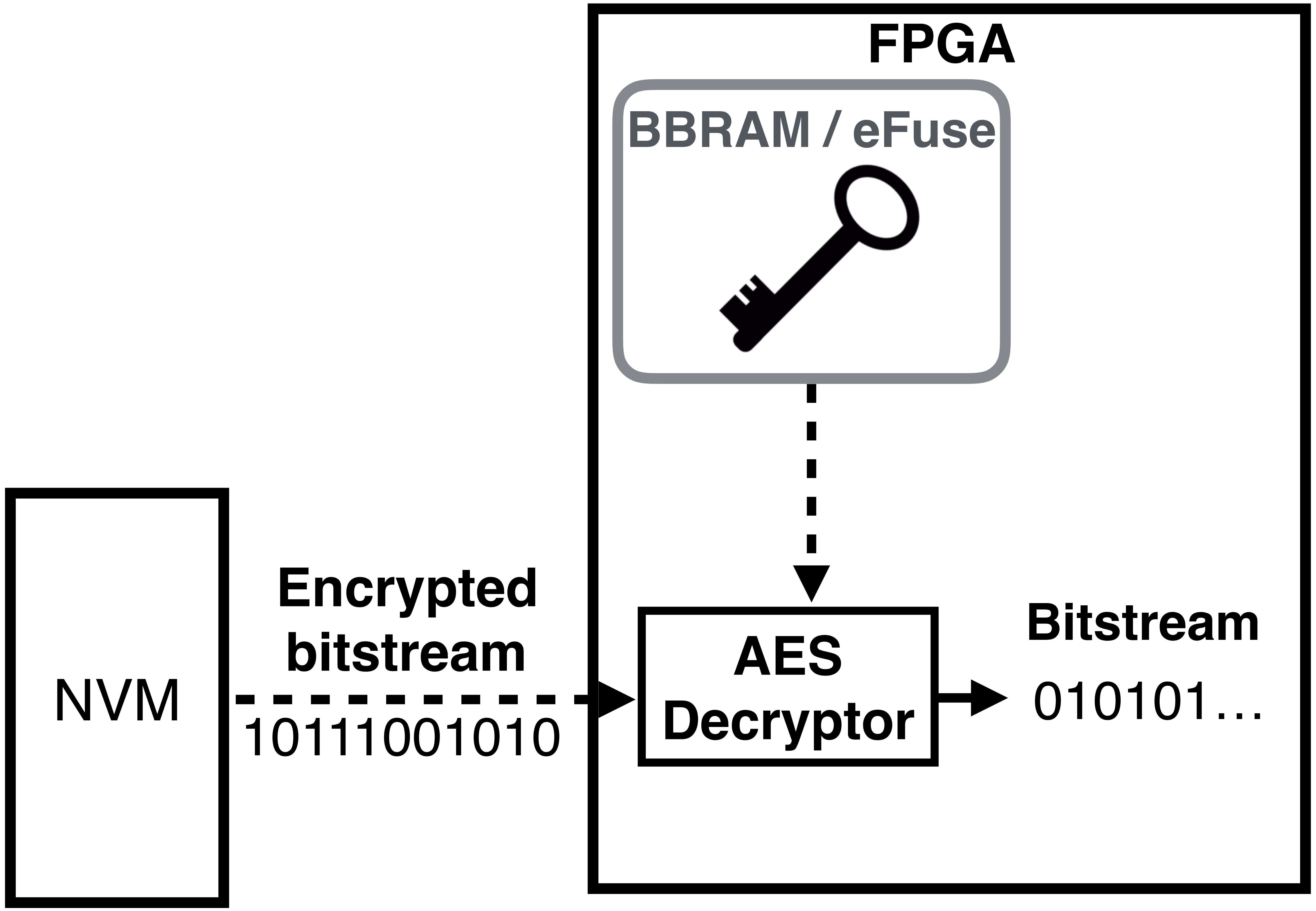
Bitstream Encryption



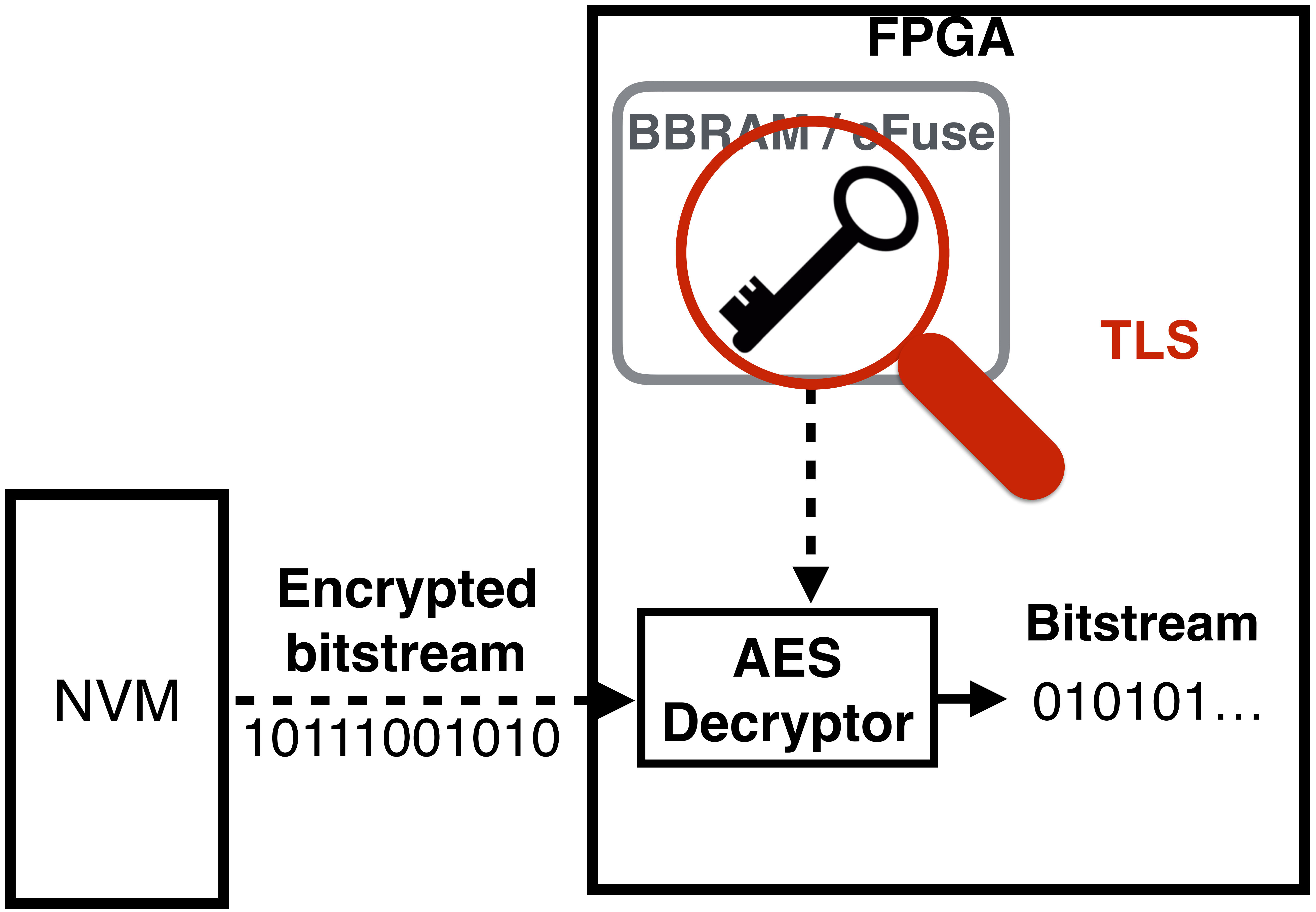
Bitstream Encryption



Bitstream Encryption

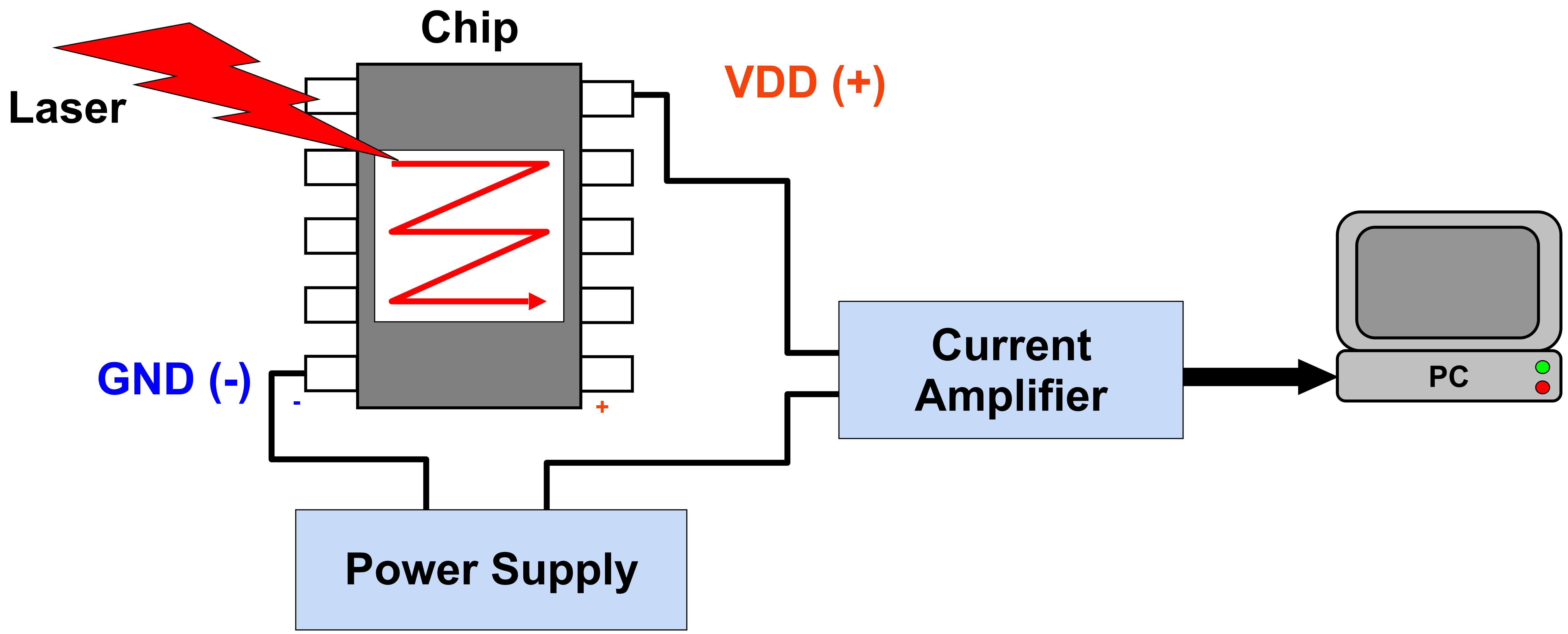


Case Study: Key Extraction from BBRAM



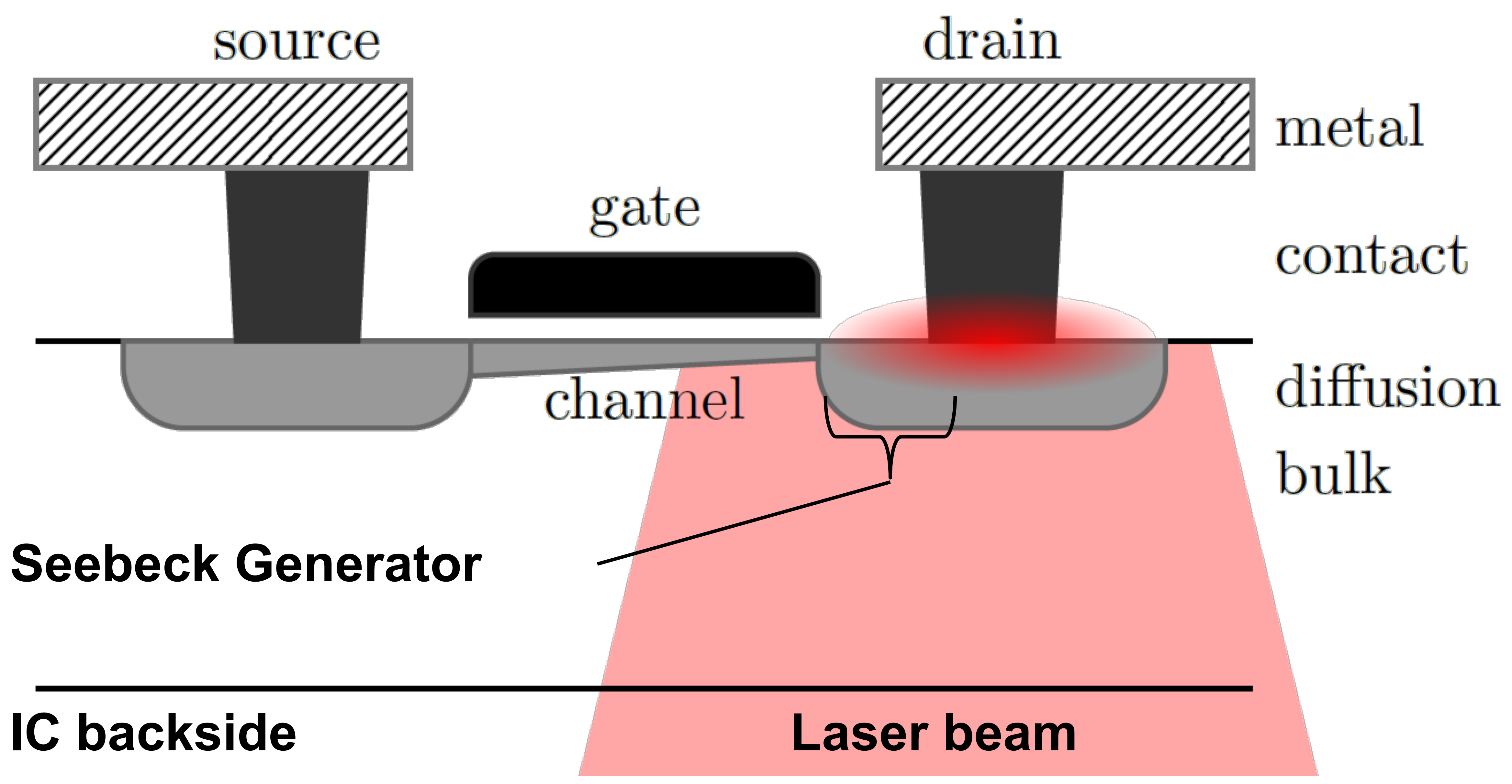
Thermal Laser Stimulation (TLS)

- 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



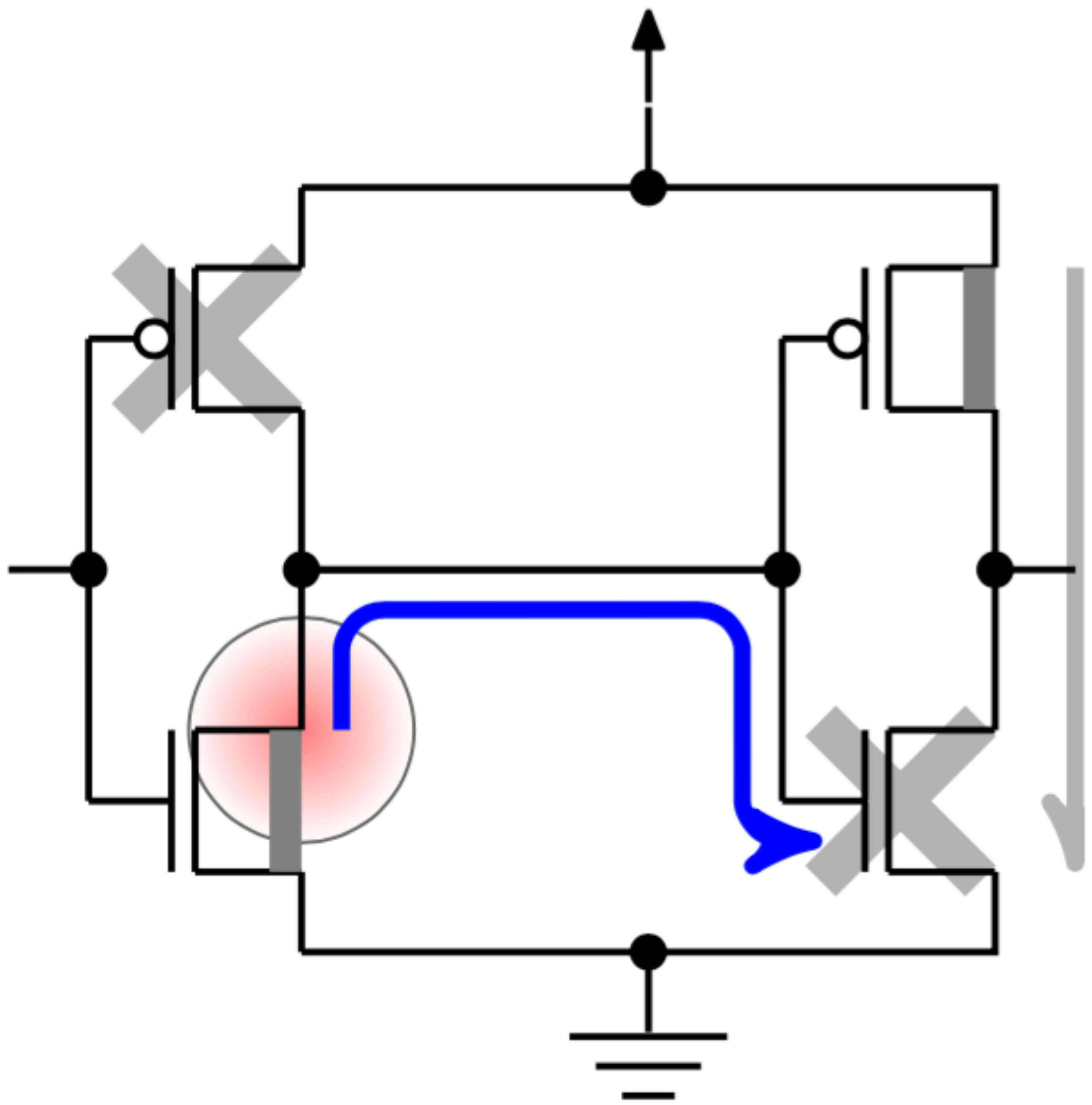
SRAM readout using TLS

- Thermal stimulation leads to thermal gradient at the source/drain of the transistors
- Different materials lead to Seebeck voltage generation
- Seebeck voltage alters gate voltage of non-conducting transistor -> increased leakage current
- Which parts of the cell are sensitive depends on cell logical state



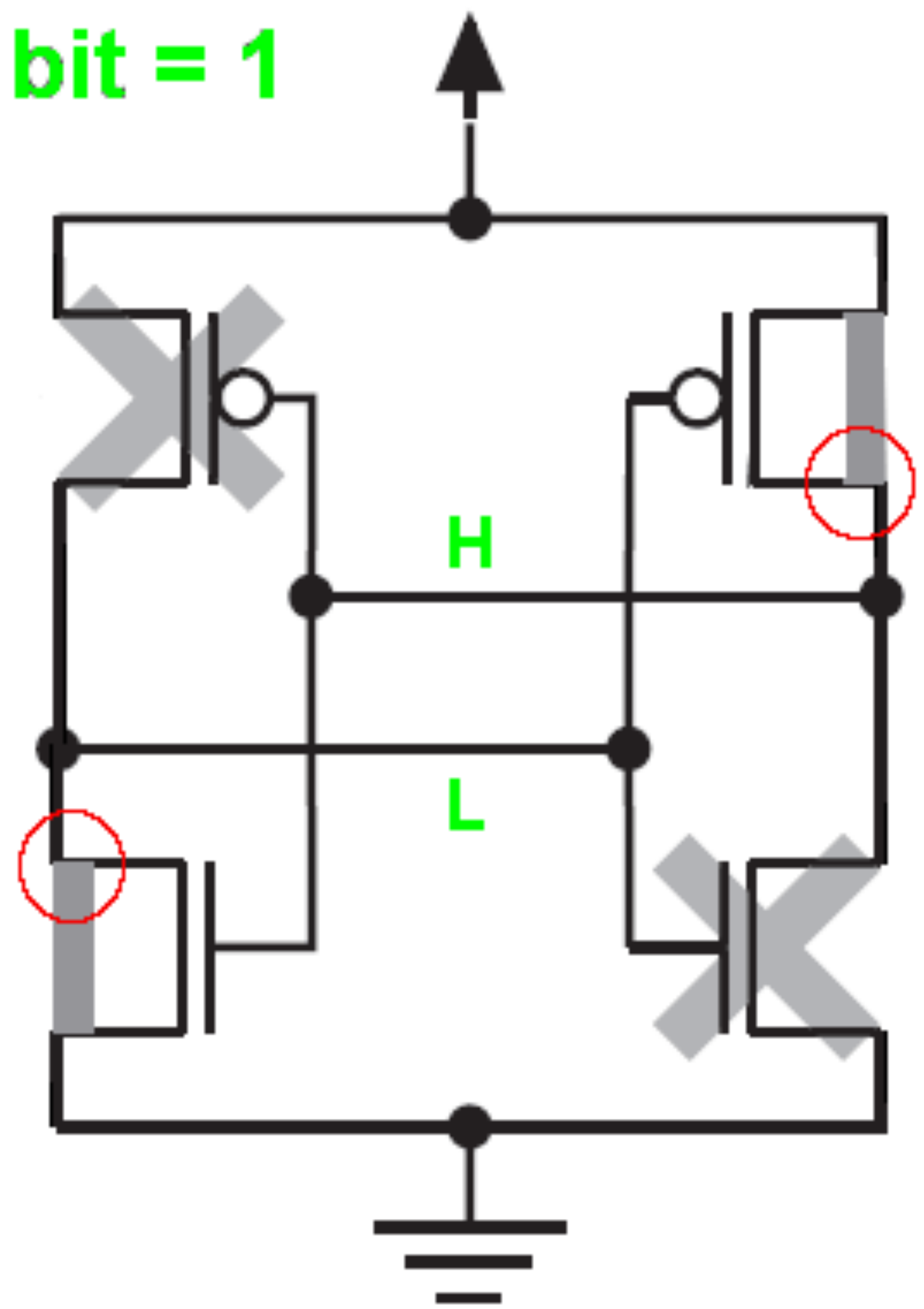
SRAM readout using TLS

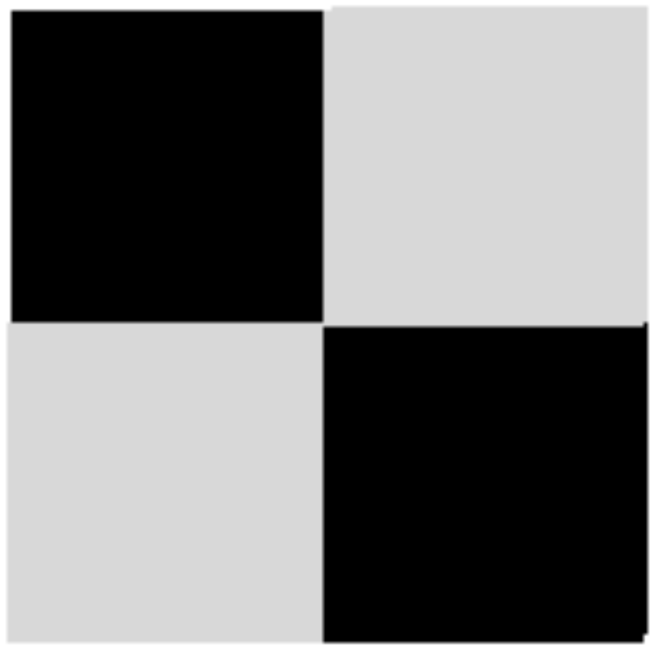
- Thermal stimulation leads to thermal gradient at the source/drain of the transistors
- Different materials lead to Seebeck voltage generation
- Seebeck voltage alters gate voltage of non-conducting transistor -> increased leakage current
- Which parts of the cell are sensitive depends on cell logical state



SRAM readout using TLS

- Thermal stimulation leads to thermal gradient at the source/drain of the transistors
- Different materials lead to Seebeck voltage generation
- Seebeck voltage alters gate voltage of non-conducting transistor -> increased leakage current
- Which parts of the cell are sensitive depends on cell logical state



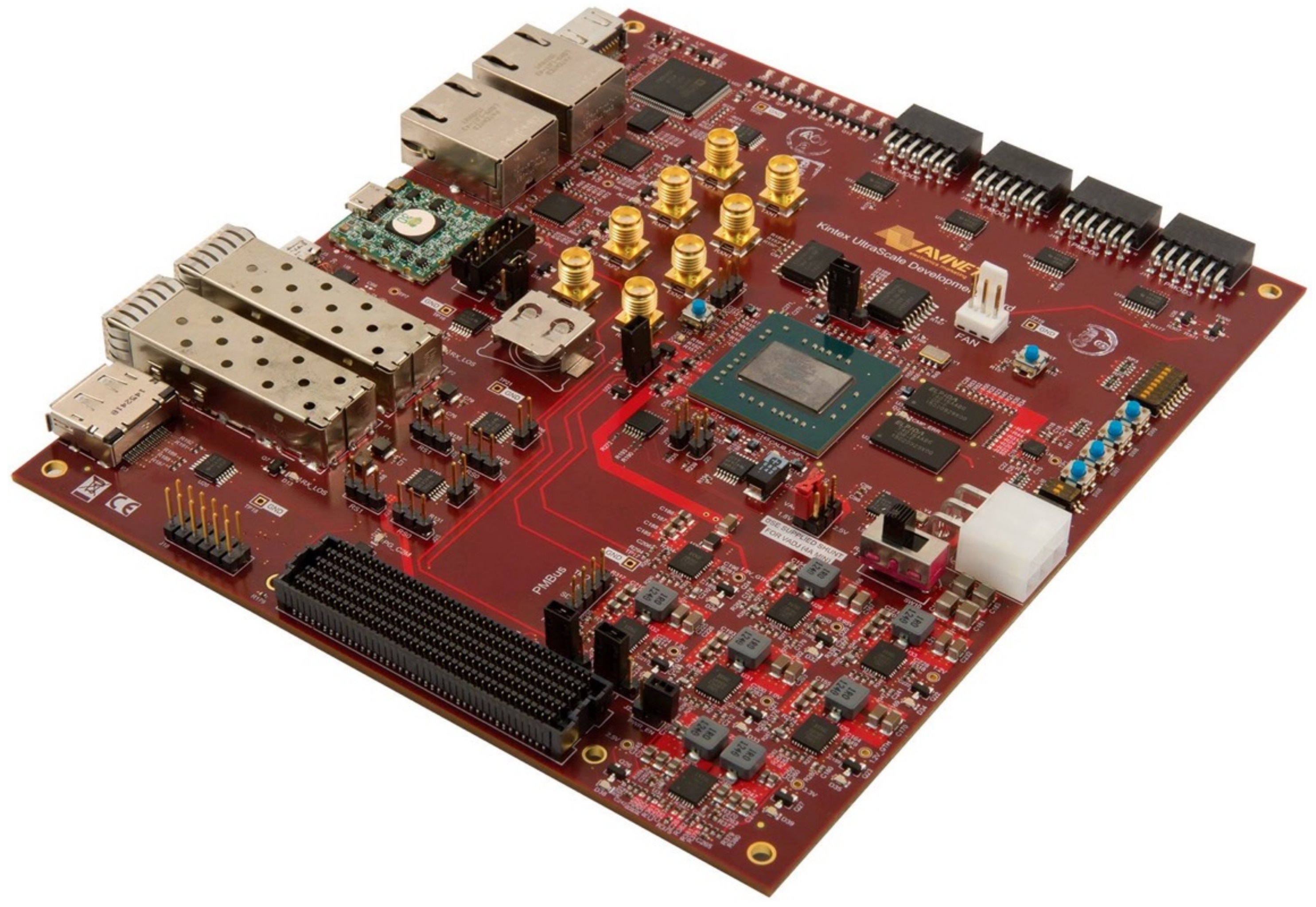


Experimental Setup

Experimental Setup

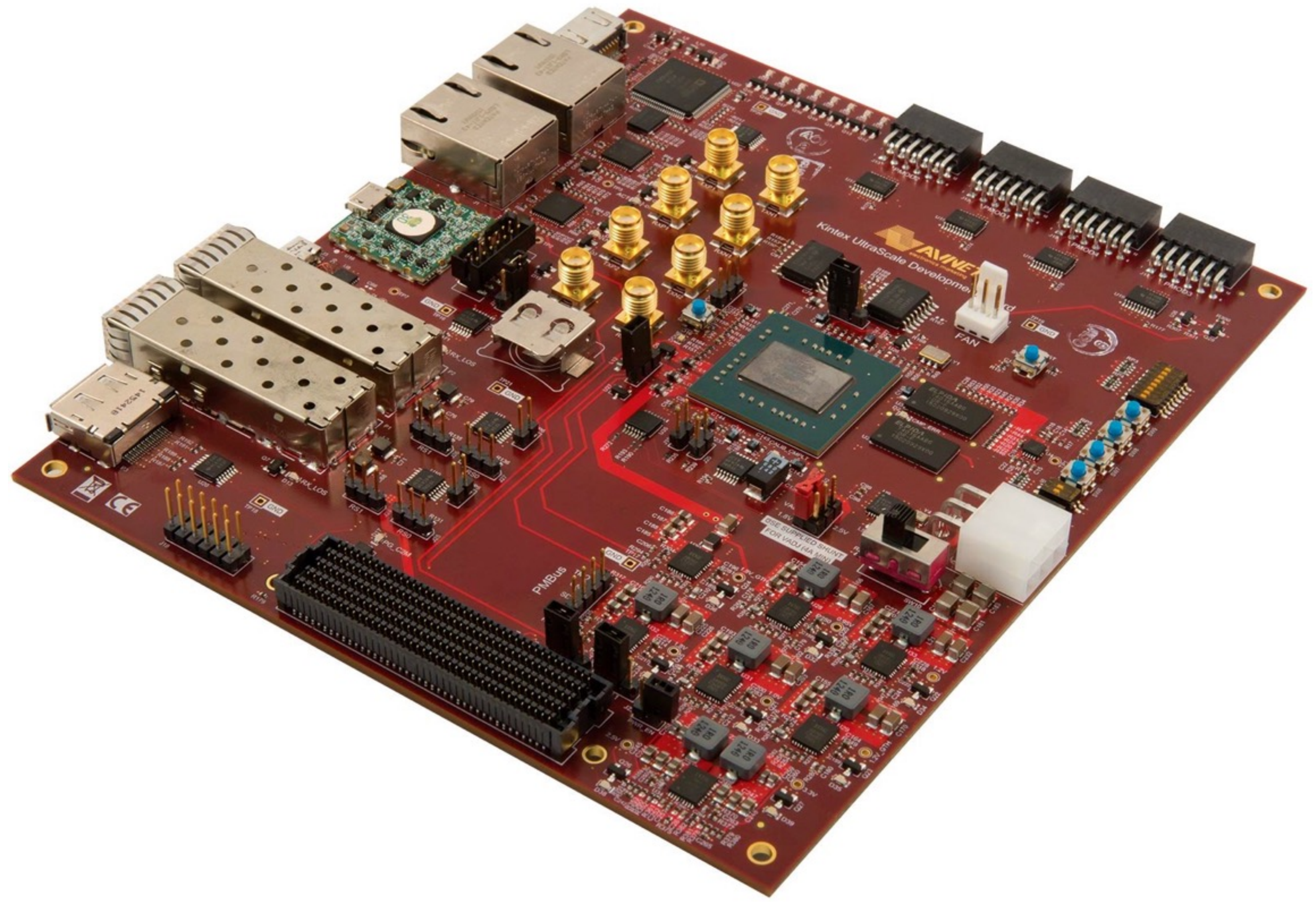
Experimental Setup

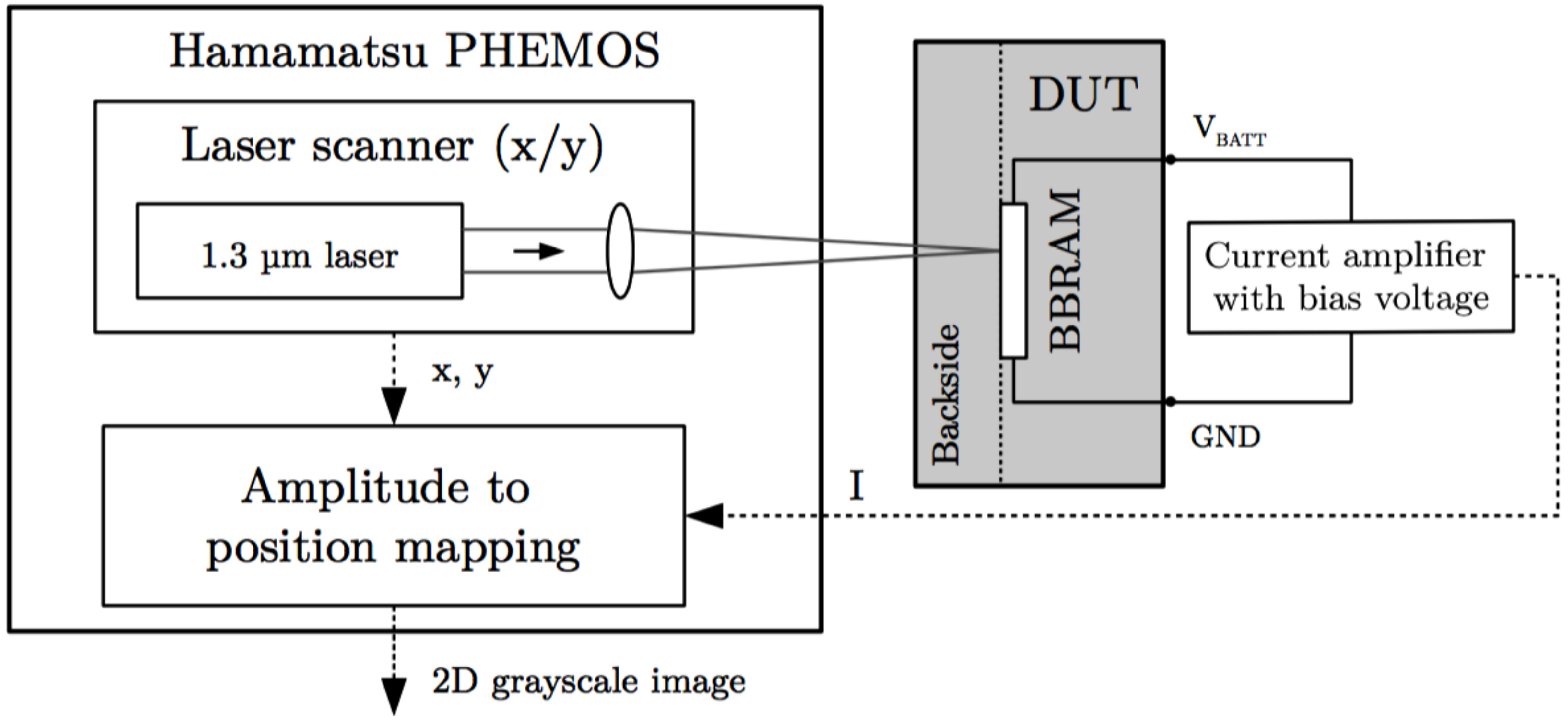
- **Device under Test (DUT):** Avnet Kintex UltraScale Development Board
  - Chip's technology: 20 nm
  - No chip preparation (e.g., depackaging, silicon polishing, etc.) required



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 wavelength: 1.3 μm
  - Laser spot size: approximately 1 μm





Results

Localizing the Configuration Logic

Xilinx Kintex UltraScale in flip chip package

Localizing the Configuration Logic

Xilinx Kintex UltraScale
in flip chip package

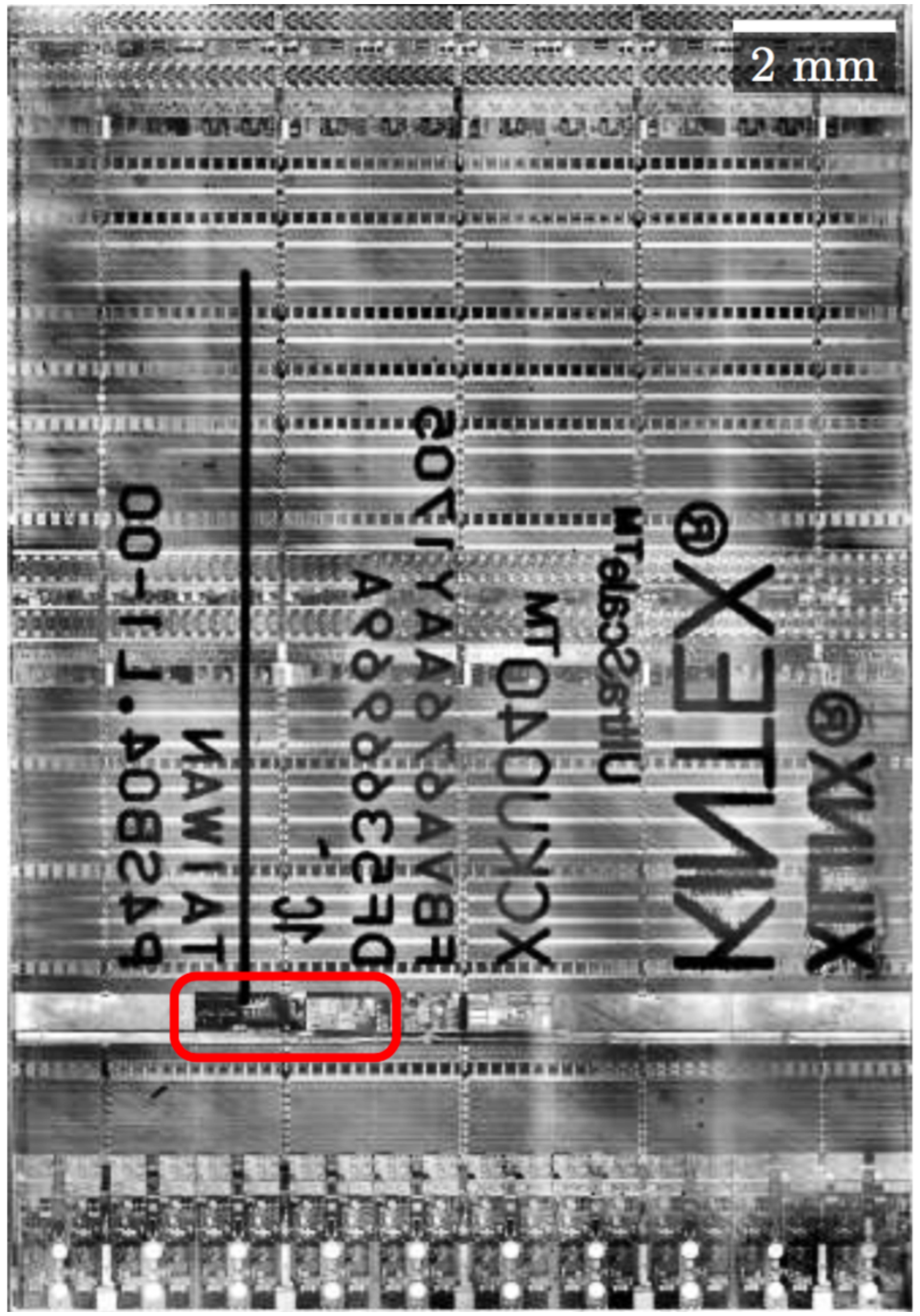
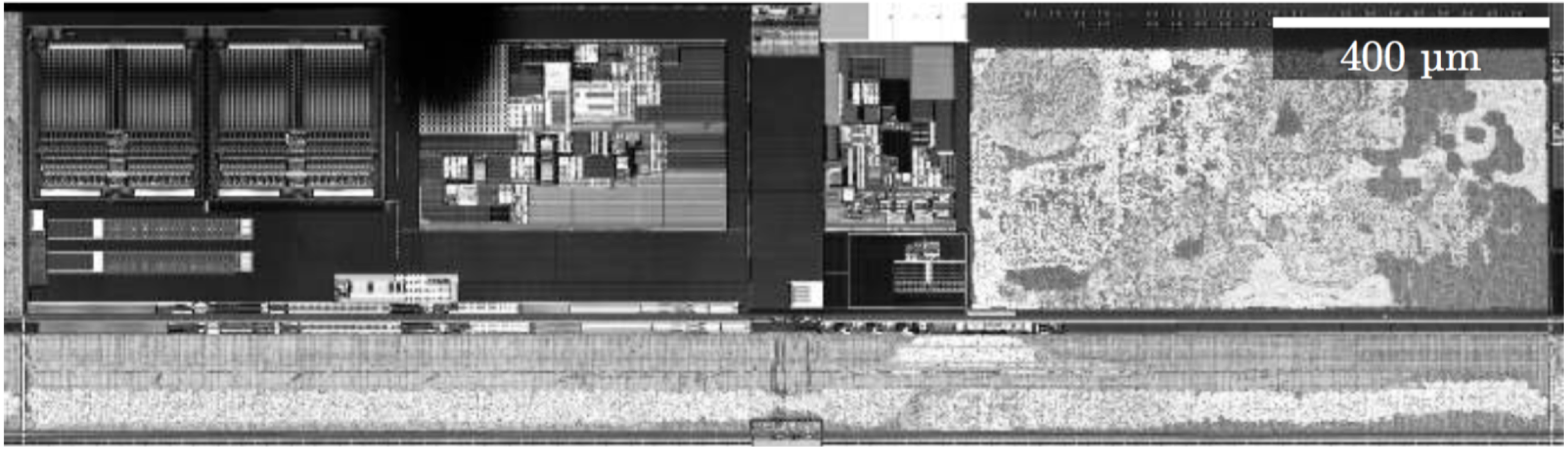


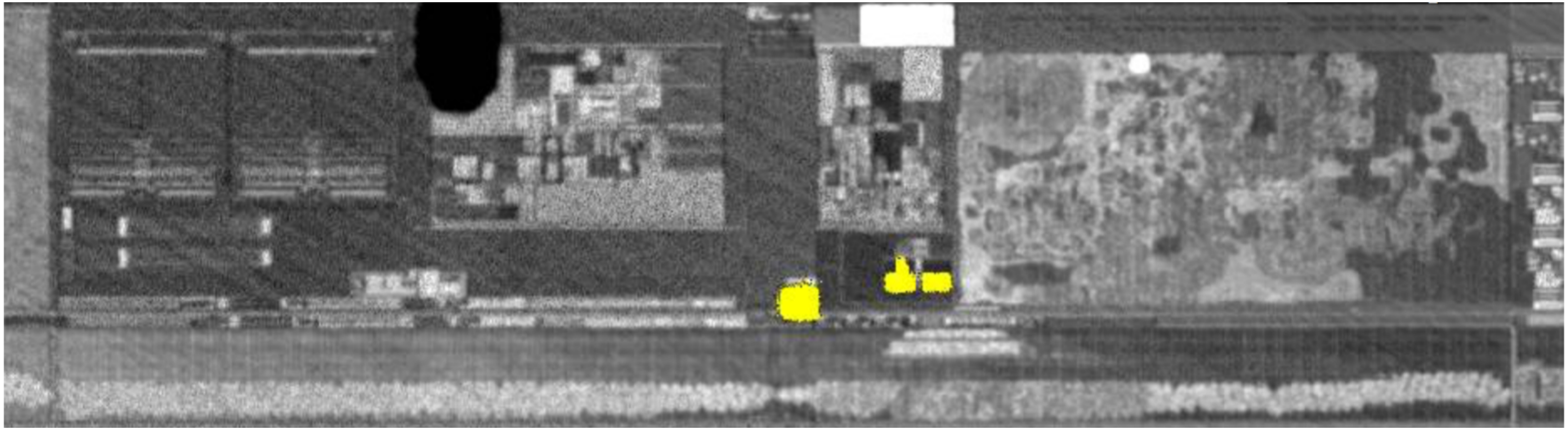
Image acquisition with a laser
scanning microscope

Localizing the Configuration Logic



Configuration Logic

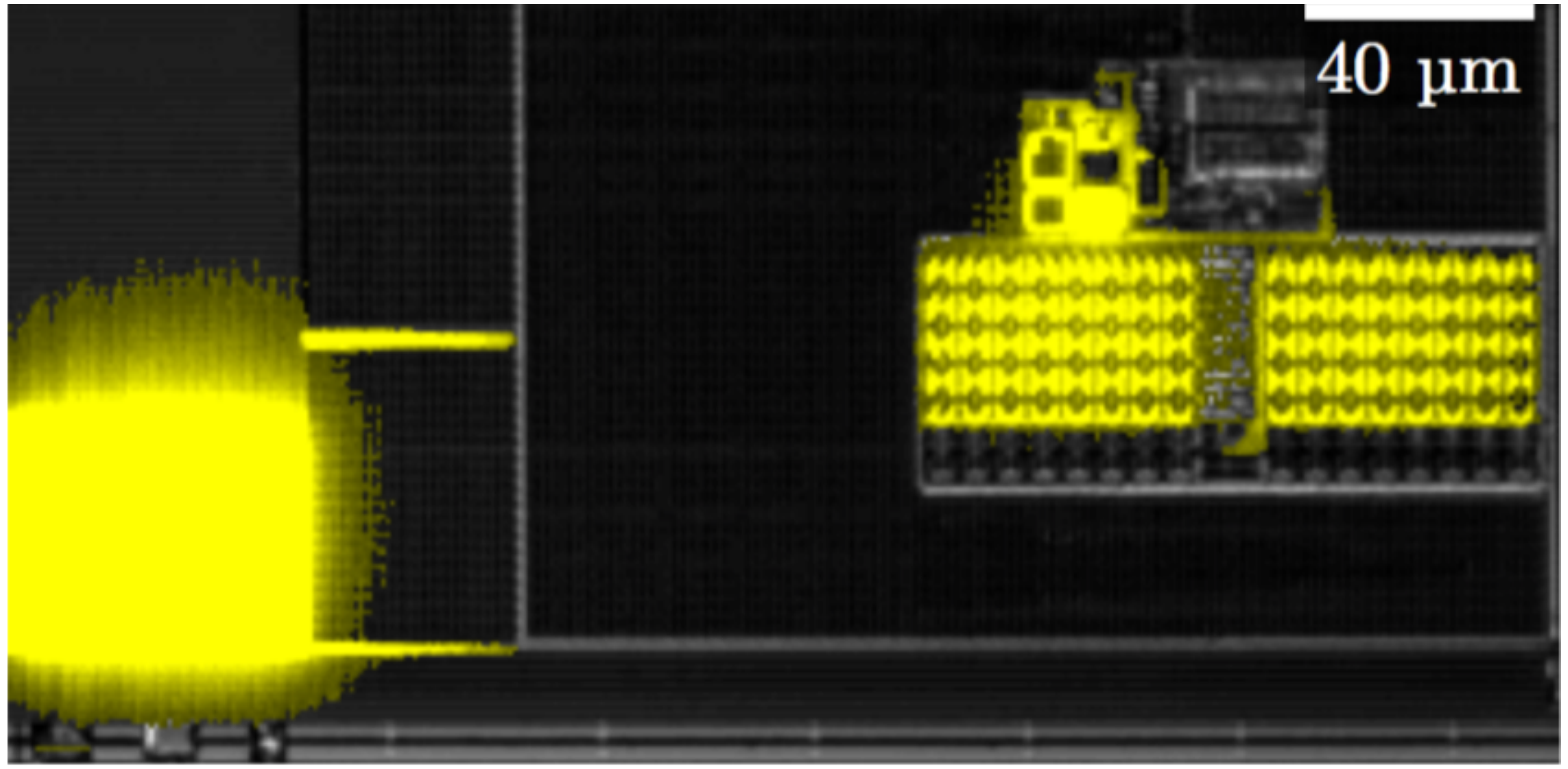
Localizing BBRAM using Laser Stimulation



Localizing BBRAM using Laser Stimulation

Laser Stimulation of configuration area and measuring the current on VBATT when BBRAM key is set

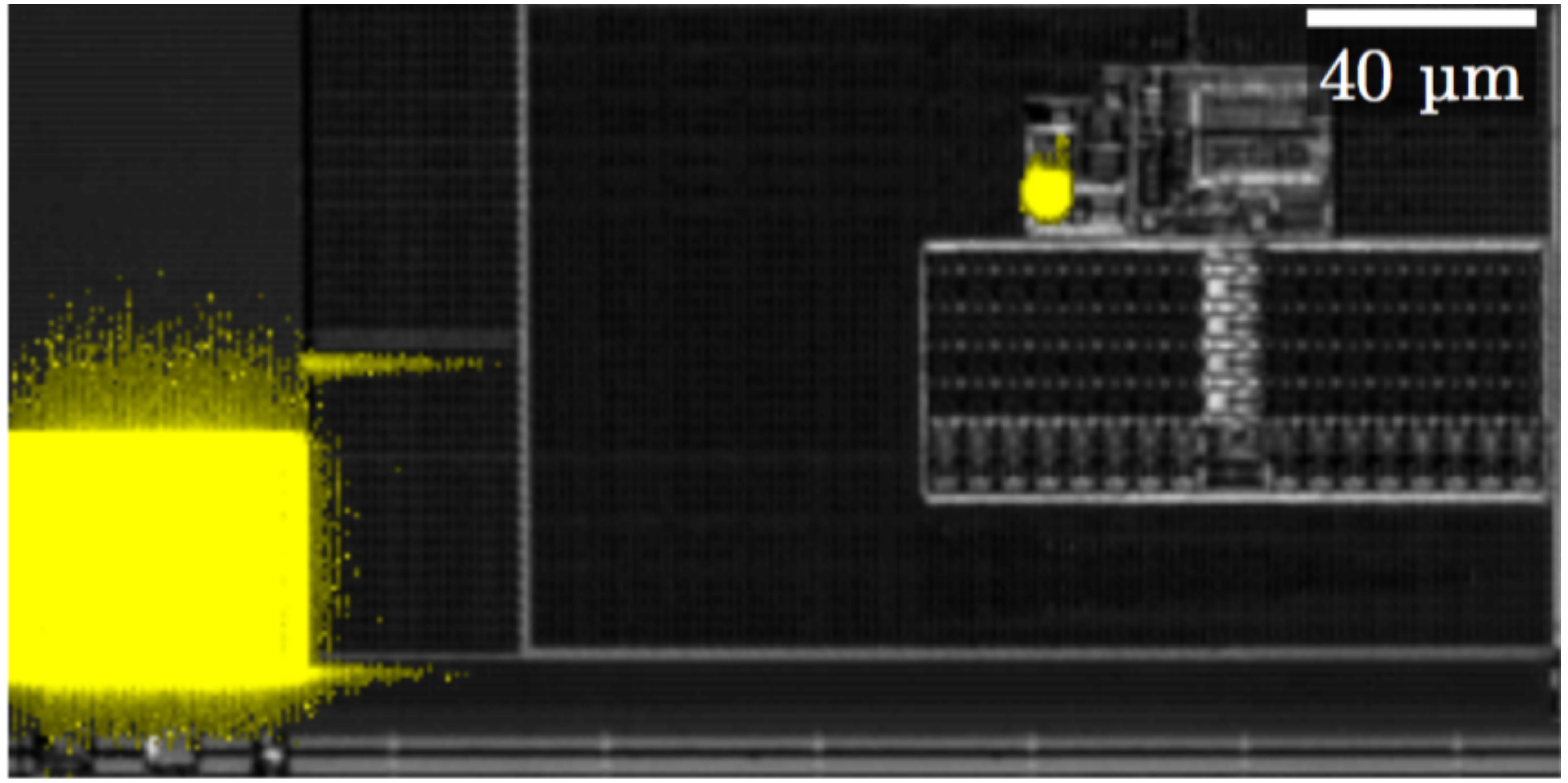
FPGA is powered off in all experiments!



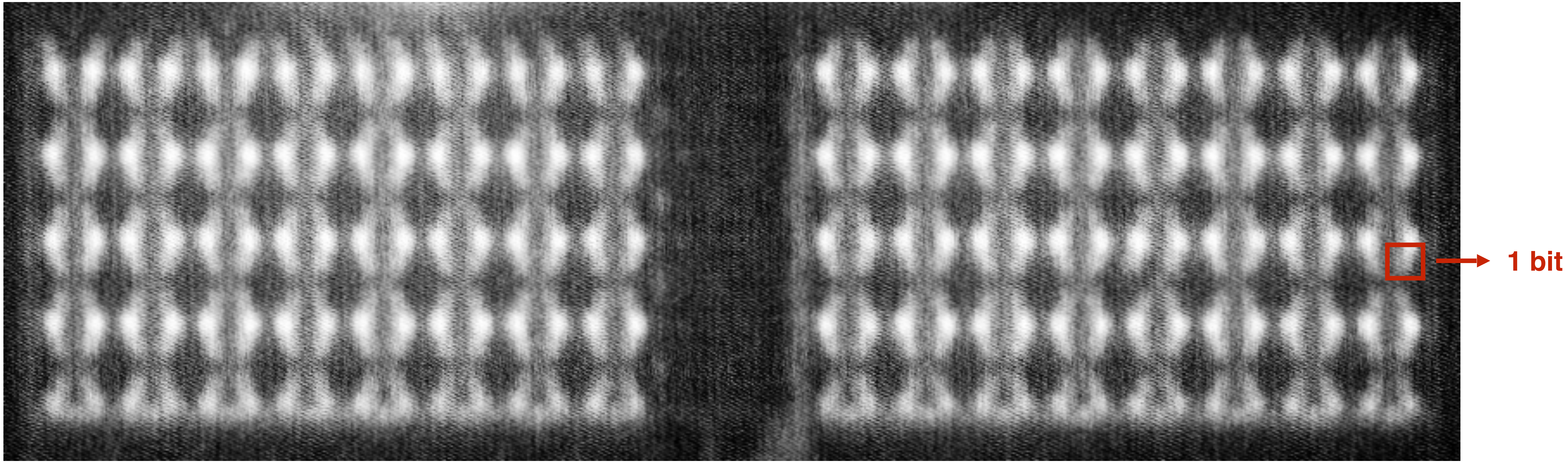
Localizing BBRAM using Laser Stimulation

Laser Stimulation of configuration area and measuring the current on VBATT when BBRAM key is not set

FPGA is powered off in all experiments!

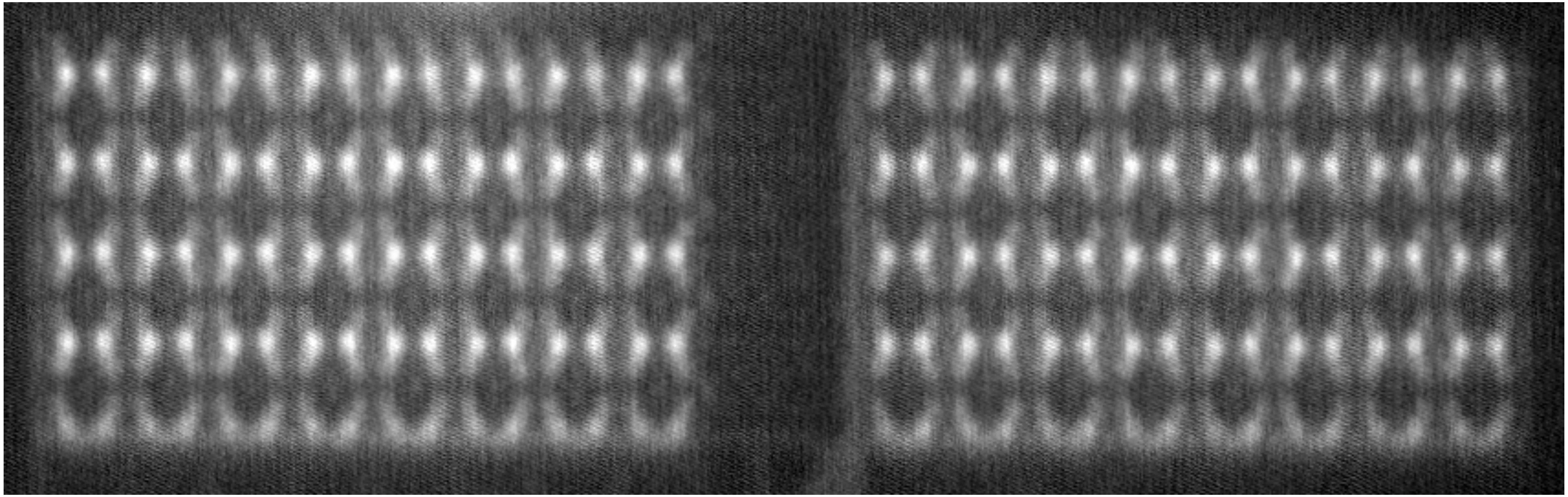


Localizing the key bits in BBRAM by TLS (1)



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

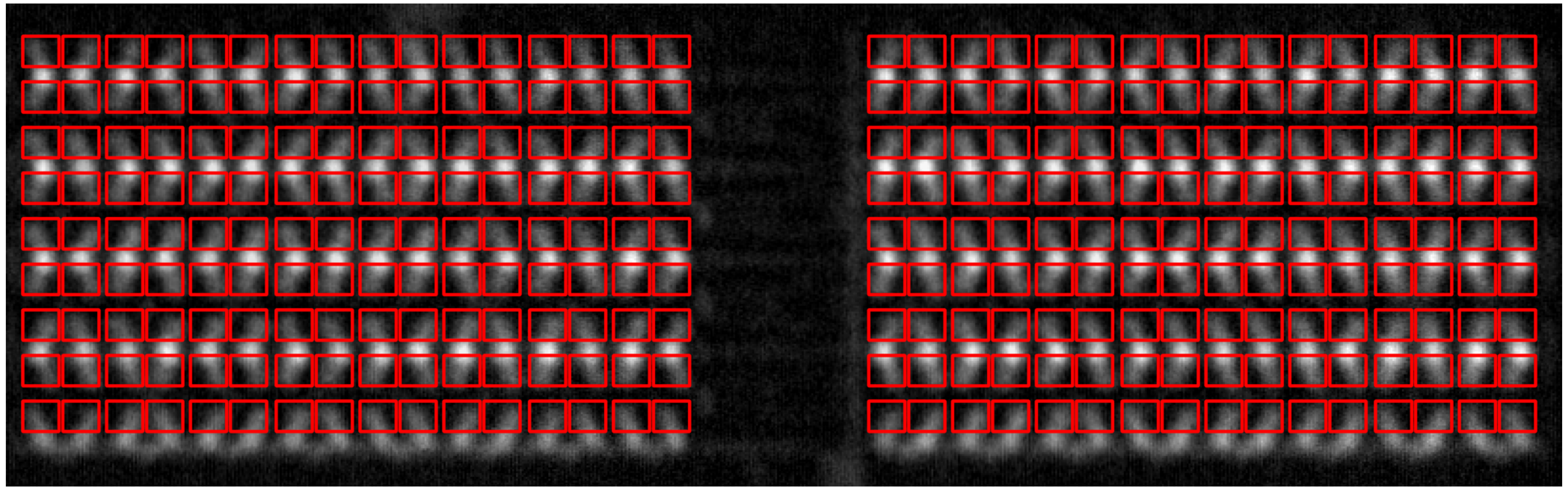
Localizing the key bits in BBRAM by TLS (2)



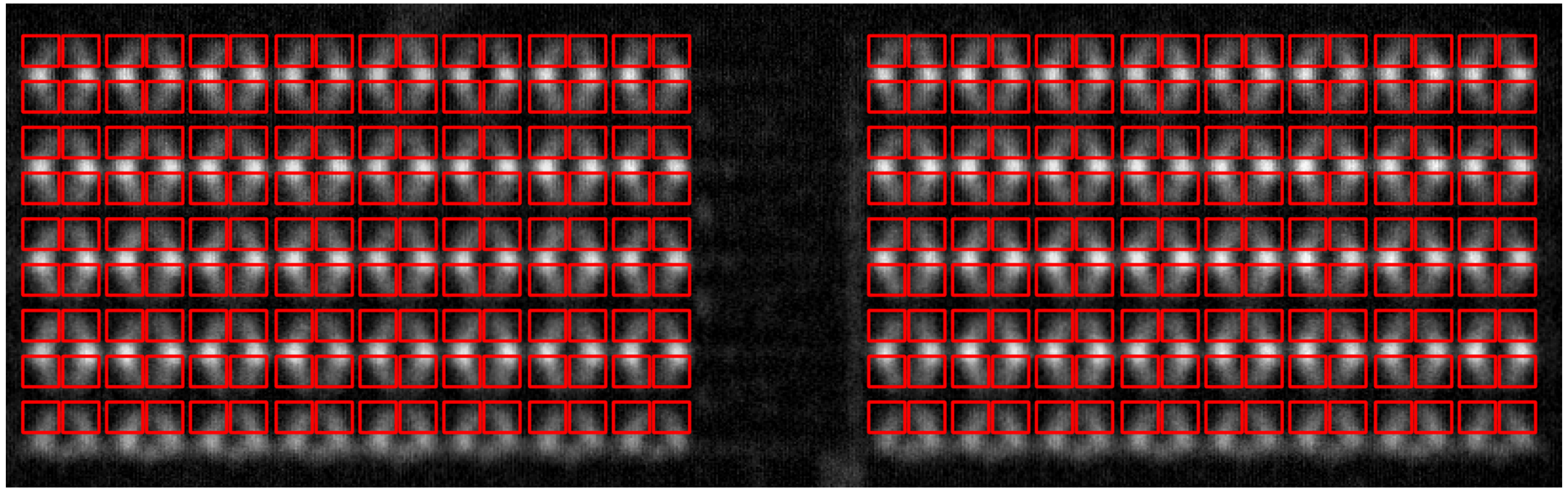
Set all 256 bits to “1” and reset all bits to “0” again.

Automatic Key Recovery

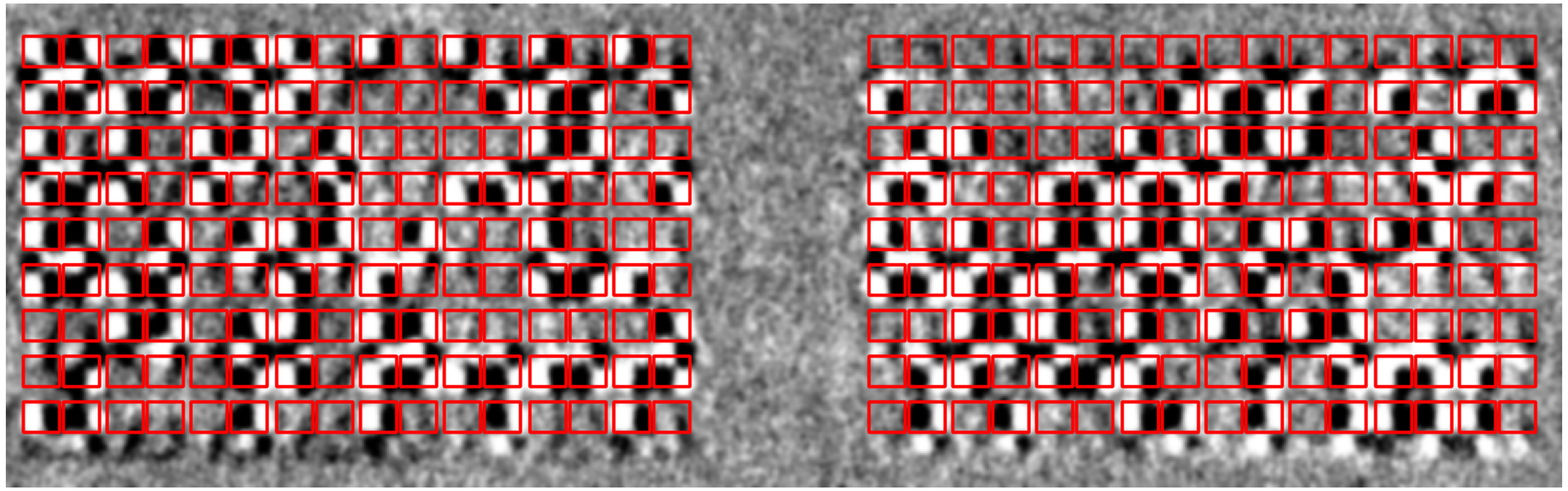
Target image containing the key



Reference image of the cleared BBRAM



Automatic Key Recovery



0xd781b86f274630b561f39c9736f512eb0adf714f0d5c836c7a76ff627aca4923

Conclusion

- The required effort to develop the attack is shown to be less than **7 hours**.
- The lower cost and higher availability of TLS in comparison to other optical attacks makes this technique even more threatening.
- The stored key in the BBRAM of the FPGA can be extracted when the FPGA is disconnected from power >> conventional side-channel countermeasures are incapable of preventing such an attack.

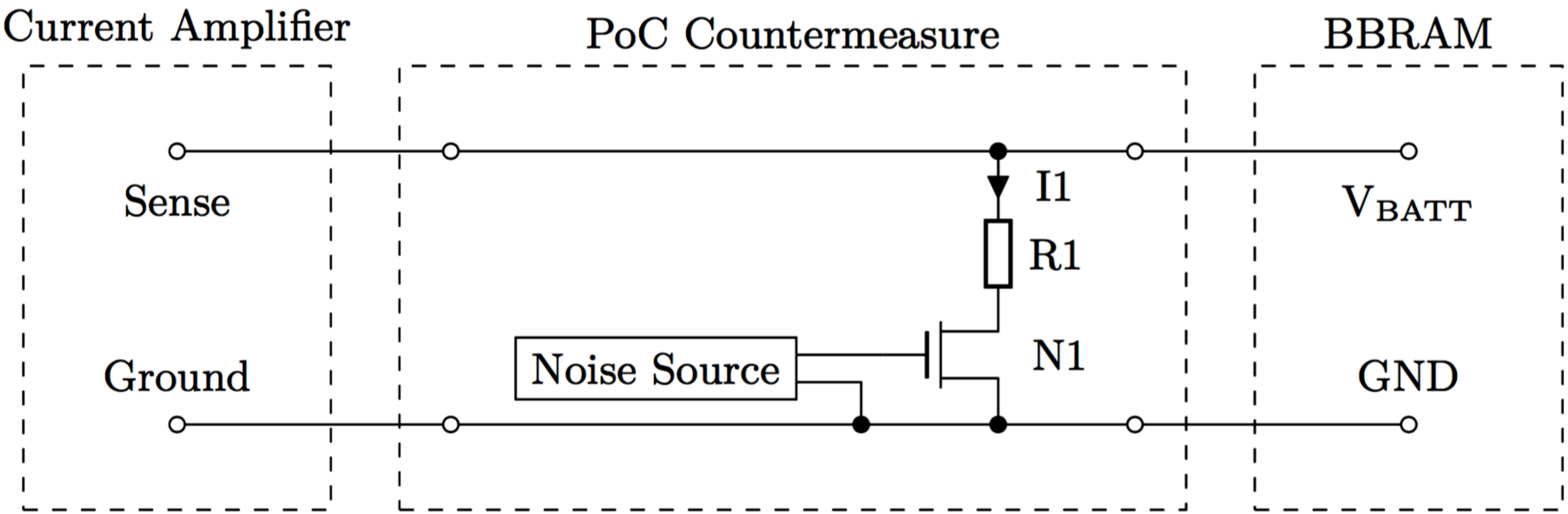
Thank you

Countermeasure: Adding Noise

- **Countermeasure Requirements:**
  - Preventing the attack, even when the FPGA is turned off
  - Not draining the backup battery excessively, so that the device can be in its powered-off state for a long time.
  - Realizable by standard processes

Countermeasure: Adding Noise

- **Countermeasure Requirements:**
  - Preventing the attack, even when the FPGA is turned off
  - Not draining the backup battery excessively, so that the device can be in its powered-off state for a long time.
  - Realizable by standard processes



Countermeasure Results