Technische Universität Berlin

Laser-Based Attacks Against FPGA Bitstream Encryption

Heiko Lohrke | Seminar on Security of Embedded Electronic Systems | 07.06.2019

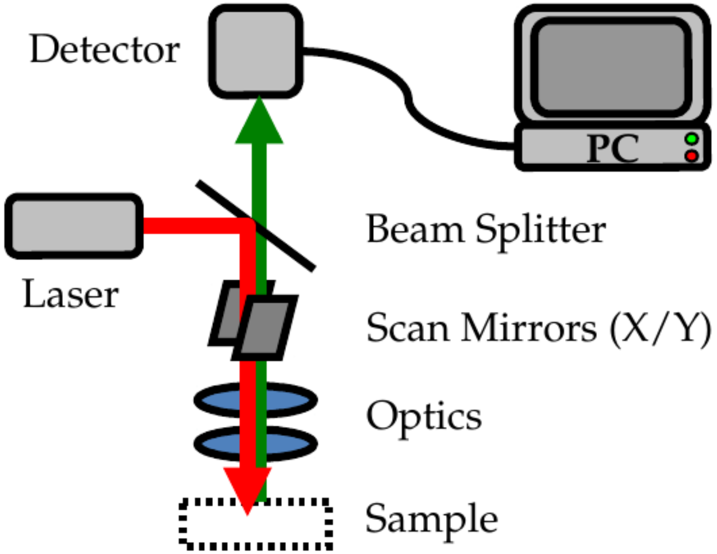
Outline

- Background
  - Laser Scanning Microscopes
  - Field Programmable Gate Array Bitstream Encryption
- Decryption Key Extraction Using Thermal Laser Stimulation
- Plaintext Data Extraction Using Optical Contactless Probing
- Conclusion

Outline

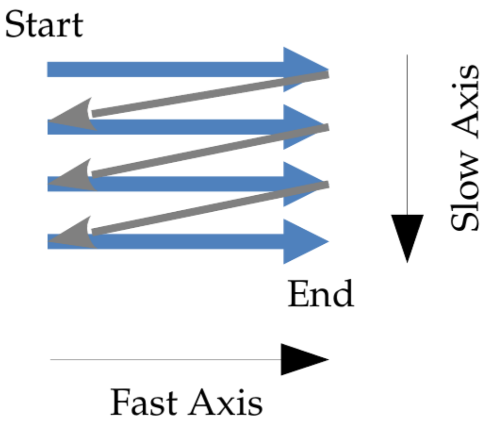
- Background
  - Laser Scanning Microscopes
  - Field Programmable Gate Array Bitstream Encryption
- Decryption Key Extraction Using Thermal Laser Stimulation
- Plaintext Data Extraction Using Optical Contactless Probing
- Conclusion

Background: Laser Scanning Microscope (LSM)



Features:

- Acquire optical images:

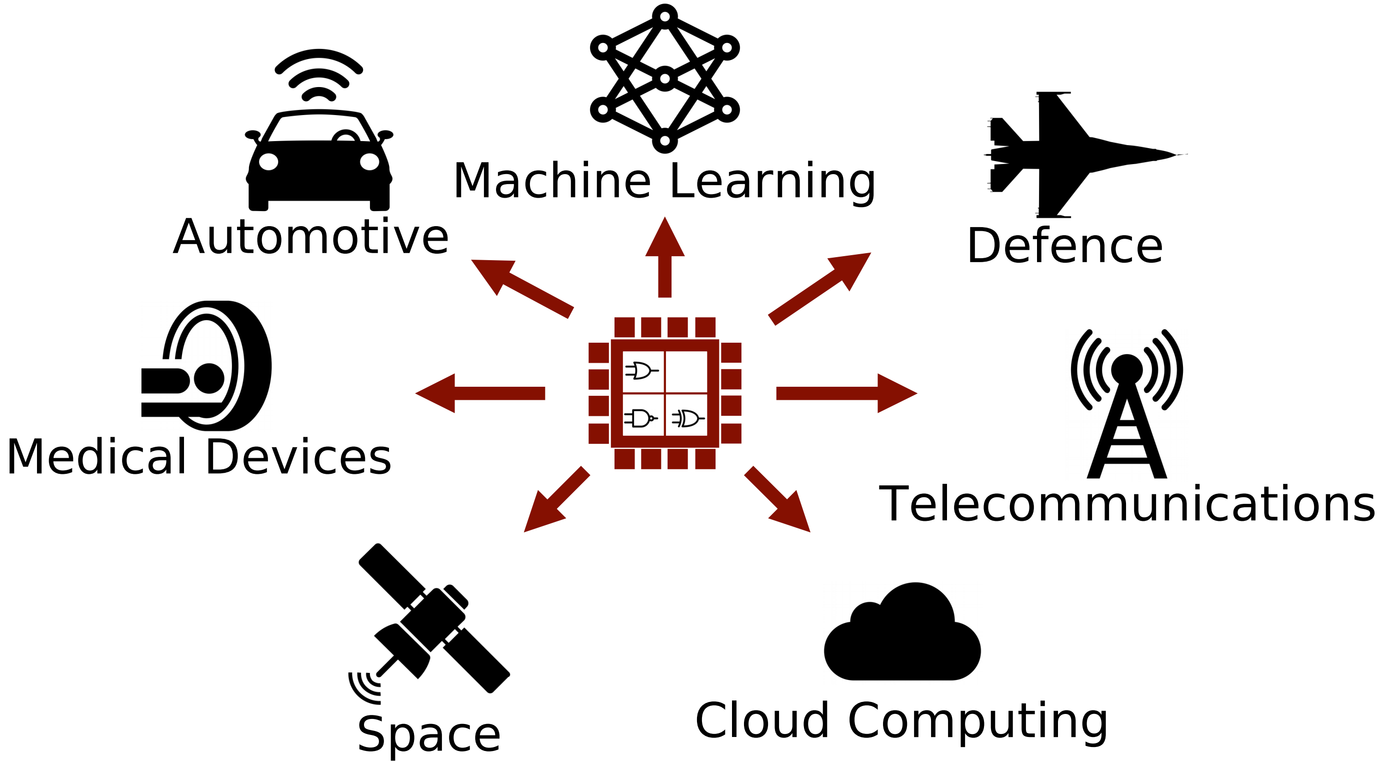


- Apply laser radiation to sample
- Analyze reflected light

Commercial LSMs

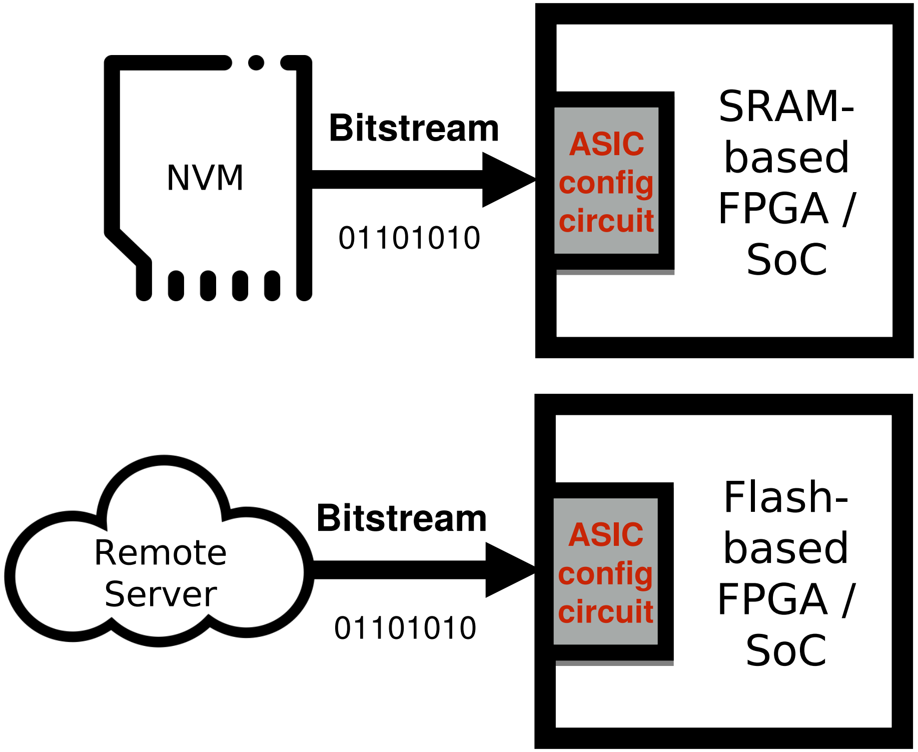
Hamamatsu Phemos 1000

FPGAs

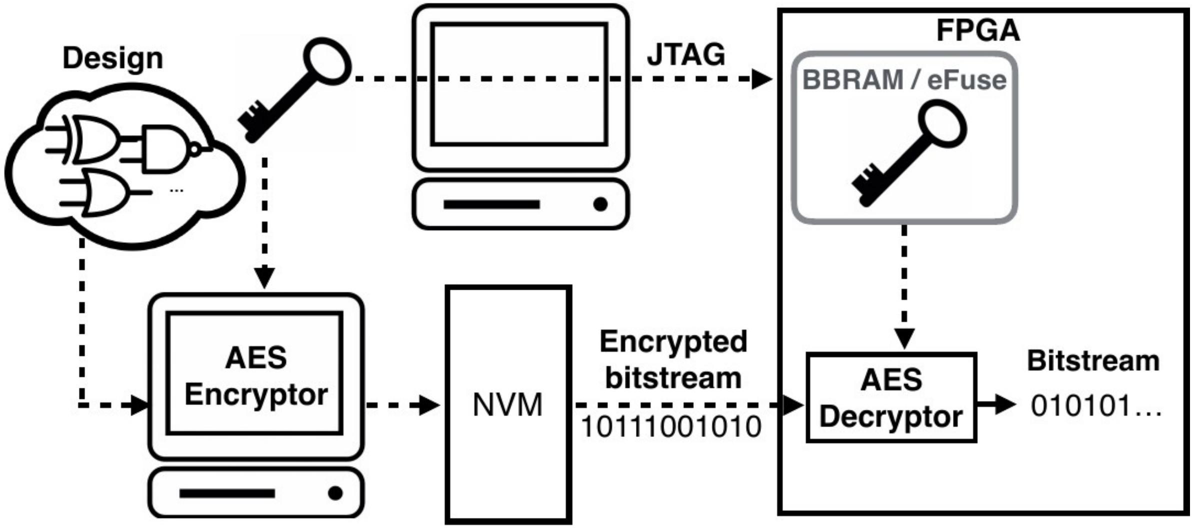

Machine Learning
Automotive
Defence
Medical Devices
Telecommunications
Space
Cloud Computing

Security of FPGAs

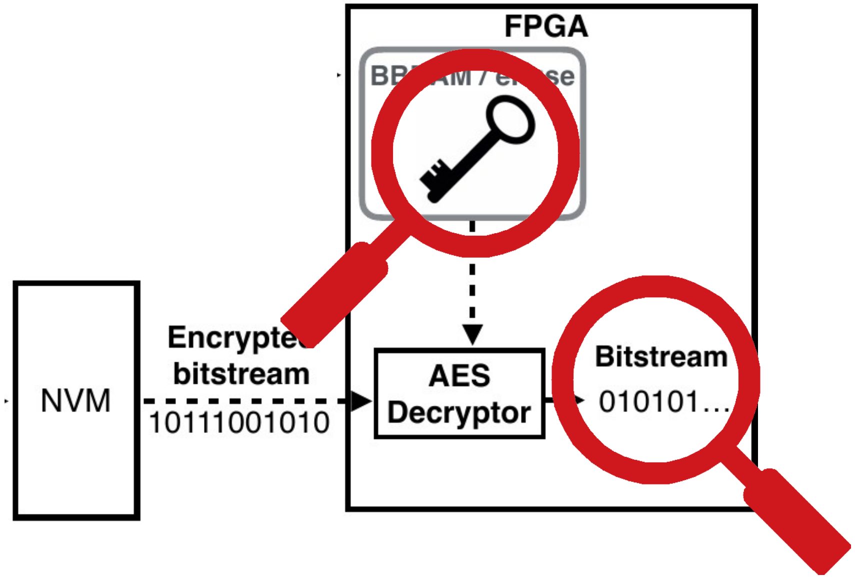
- Bitstream: configuration data containing **Intellectual Property (IP)** and **secrets** for reconfigurable hardware
- The bitstream can be loaded in the field (**adversarial environment**)
- Threats: cloning, reverse-engineering, tampering or spoofing



FPGA Bitstream Encryption



Attack Locations in the Field



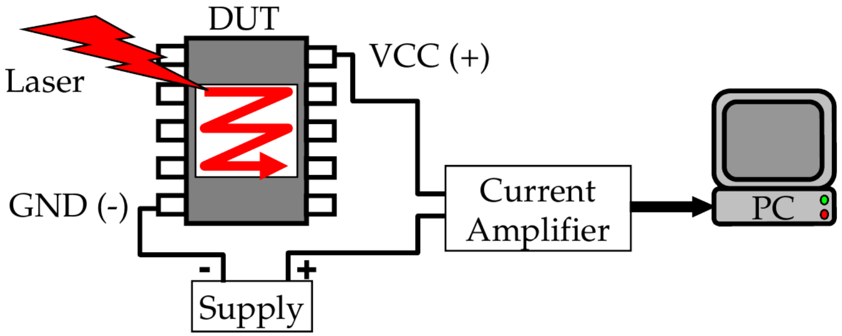
Outline

- Background
  - Laser Scanning Microscopes
  - Field Programmable Gate Array Bitstream Encryption
- Decryption Key Extraction Using Thermal Laser Stimulation
- Plaintext Data Extraction Using Optical Contactless Probing
- Conclusion

Thermal Laser Stimulation (TLS)

- Used in failure analysis to find failure cause locations
- Analyzes device’s reaction to thermal (1.3 µm) laser radiation
- Has potential to extract sensitive information from device, esp. SRAM

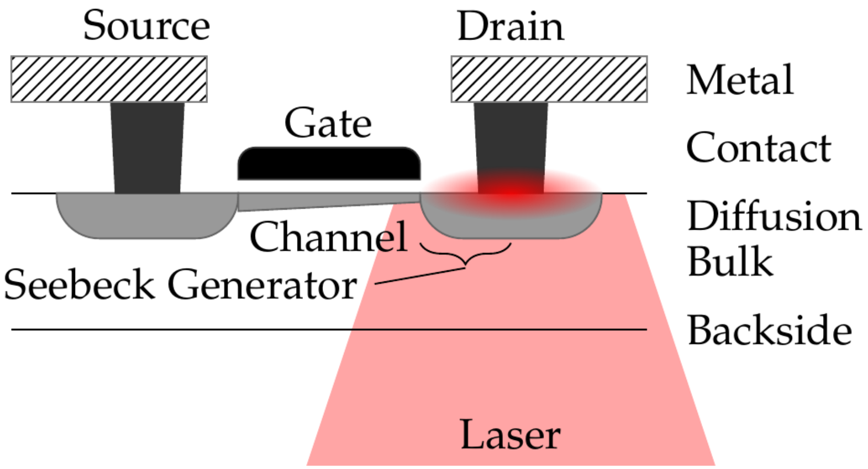
Thermal Laser Stimulation Setup



- Laser scans across the opened device
- Temperature increases locally
- Changes in current consumption occur
- Current consumption is plotted over the X/Y laser location

→ Resulting "Stimulation Response Map" allows to identify areas which increase current consumption when stimulated

Seebeck Voltage Generation in MOSFETs



1.3 µm laser stimulation

→ thermal gradient

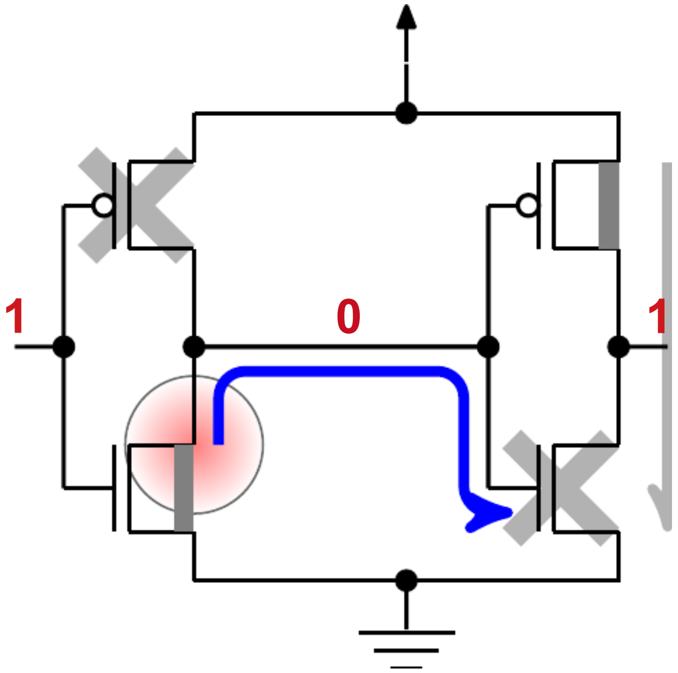
Different materials

→ Seebeck voltage

Result:

laser-induced voltage source between S-D if transistor is on

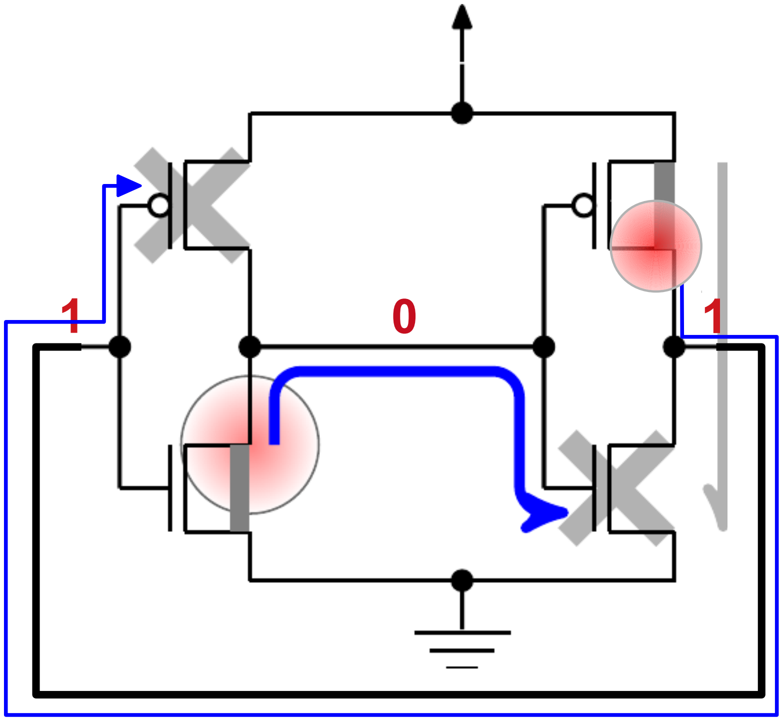
Thermal Laser Stimulation of an SRAM Cell



Simple case: two inverters

- NMOS transistor of first inverter is stimulated
- Seebeck voltage influences second NMOS transistor
- Supply-Ground leakage is increased

Thermal Laser Stimulation of an SRAM Cell

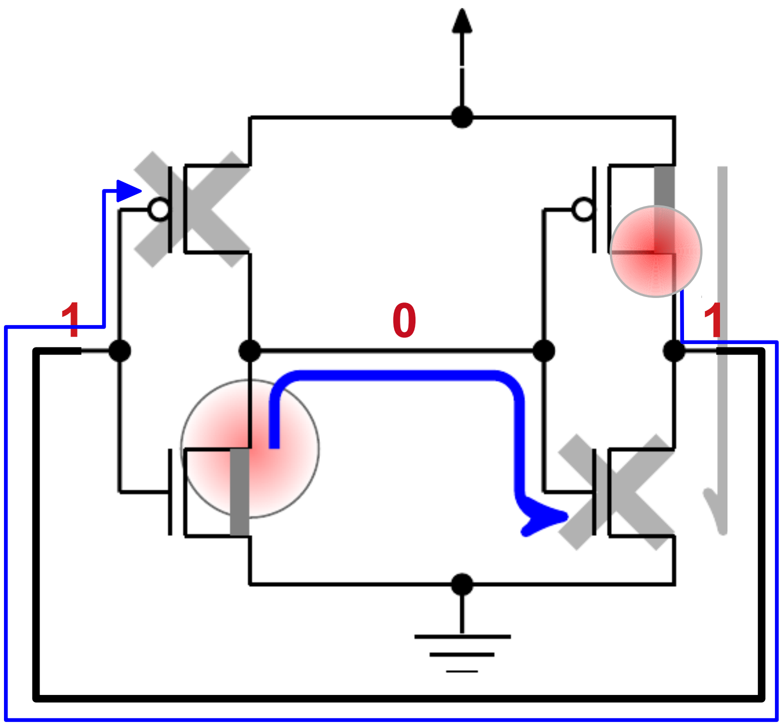


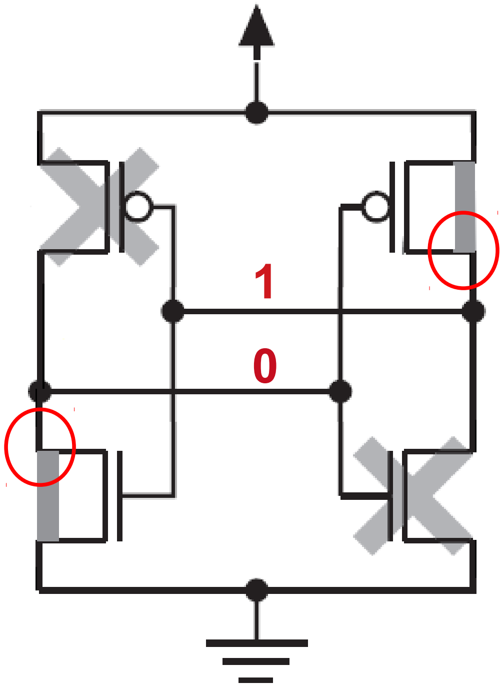
Simple case: two inverters

- NMOS transistor of first inverter is stimulated
- Seebeck voltage influences second NMOS transistor
- Supply-Ground leakage is increased

SRAM cell: cross-coupled inverters (1 bit)

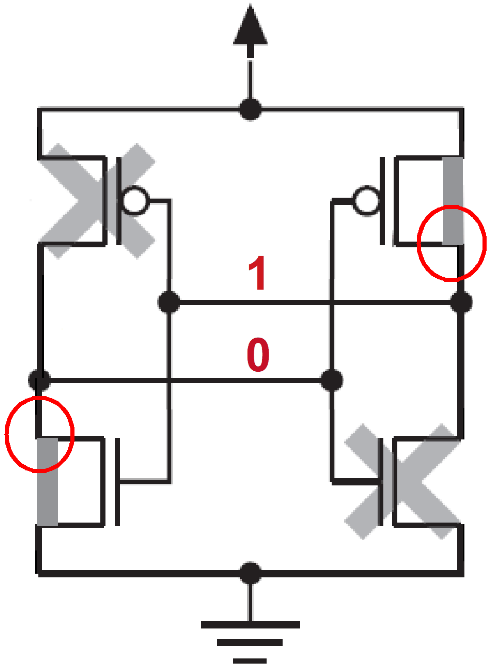
Thermal Laser Stimulation of an SRAM Cell



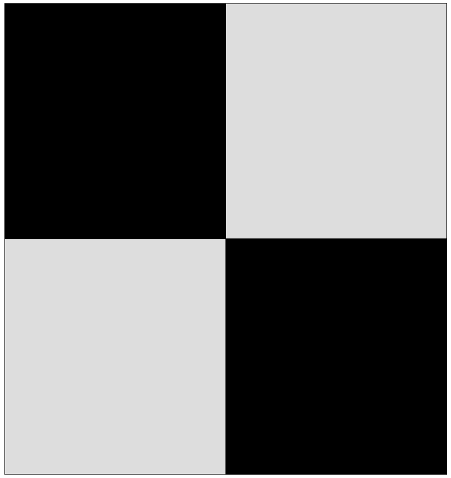


Thermal Laser Stimulation of an SRAM Cell

Bit = 1



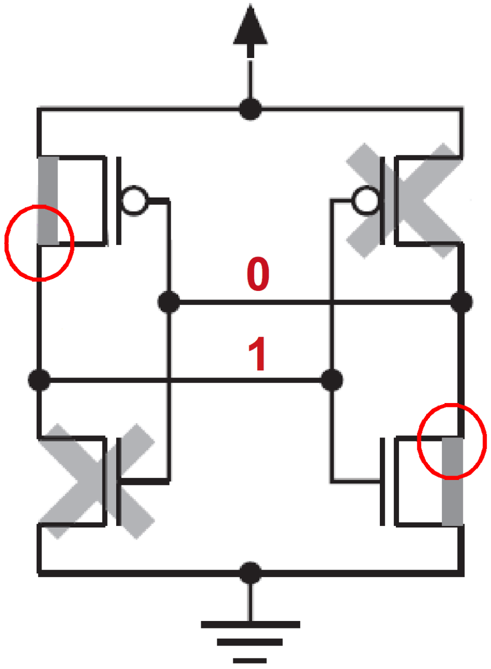
SRAM Cell



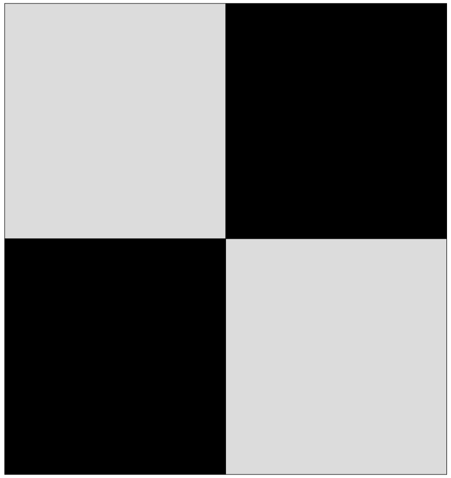
Stimulation Response

Thermal Laser Stimulation of an SRAM Cell

Bit = 0



SRAM Cell

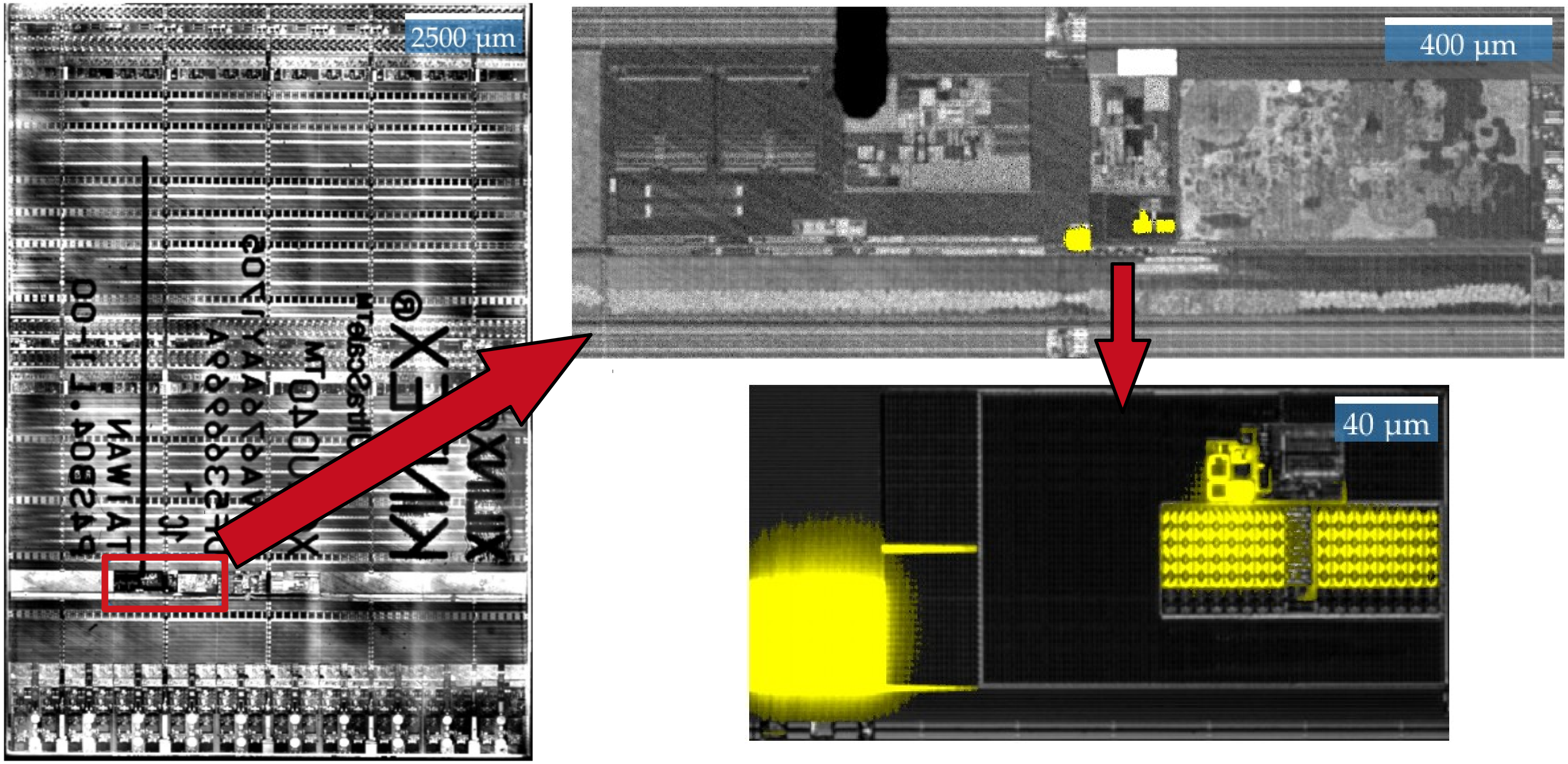


Stimulation Response

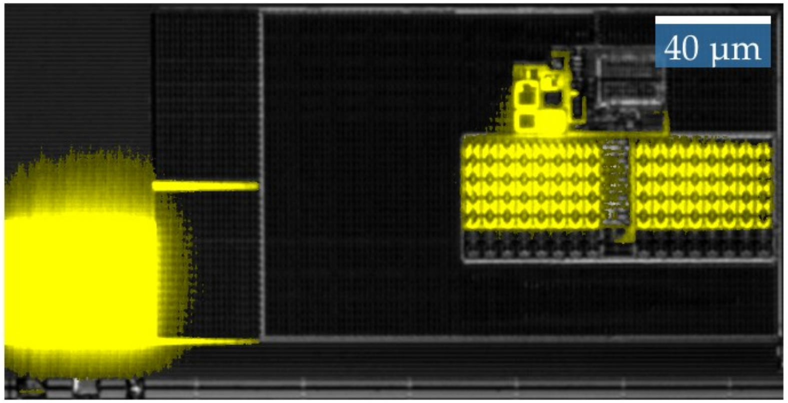
Decryption Key Extraction Using Thermal Laser Stimulation

- Device: Xilinx Kintex Ultrascale FPGA (20 nm)
- Flip-Chip: no preparation or thinning
- 256-bit AES key is used for bitstream decryption
- Key can be stored in battery-backed SRAM (BBRAM)
- Attack: Locate and extract decryption key

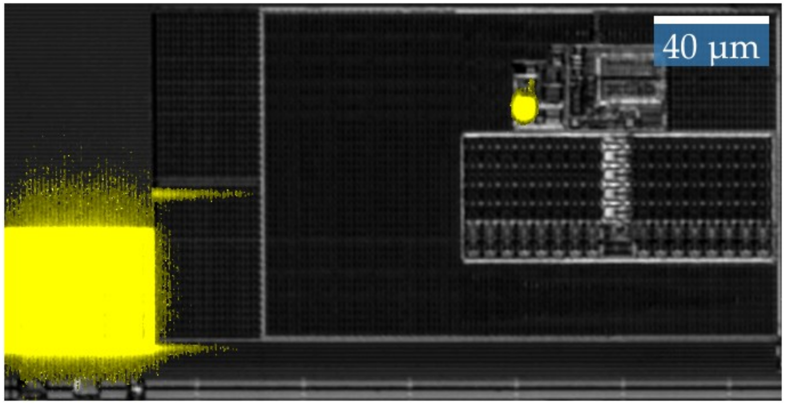
Key Memory Localization



Key Memory Localization

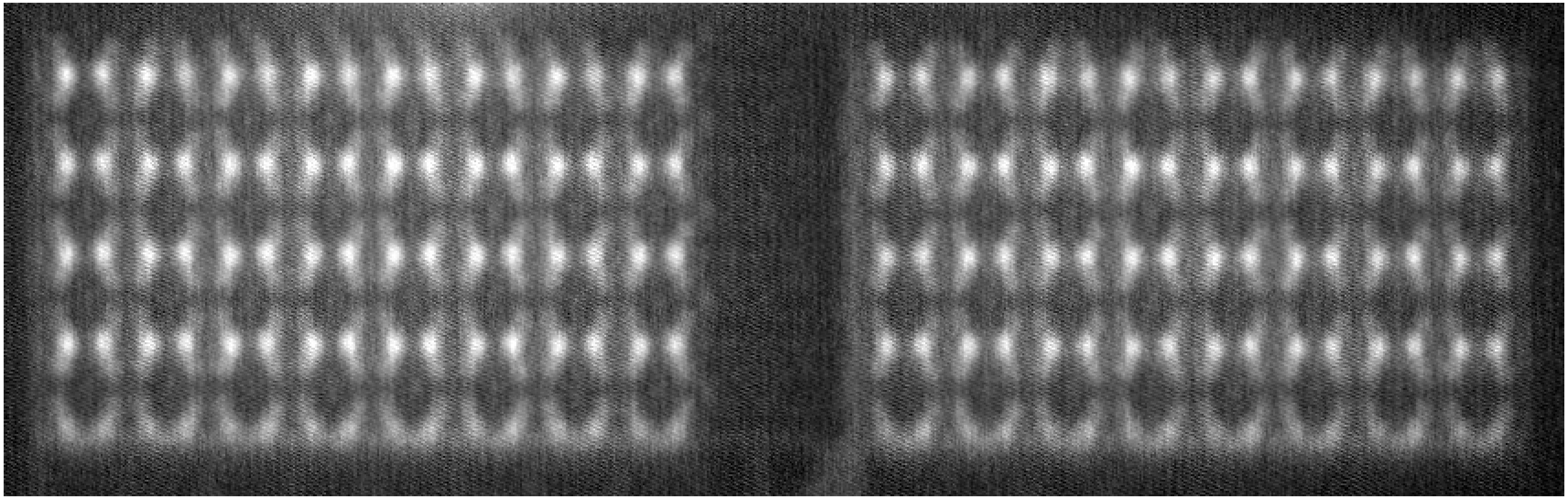


BBRAM Key Storage On



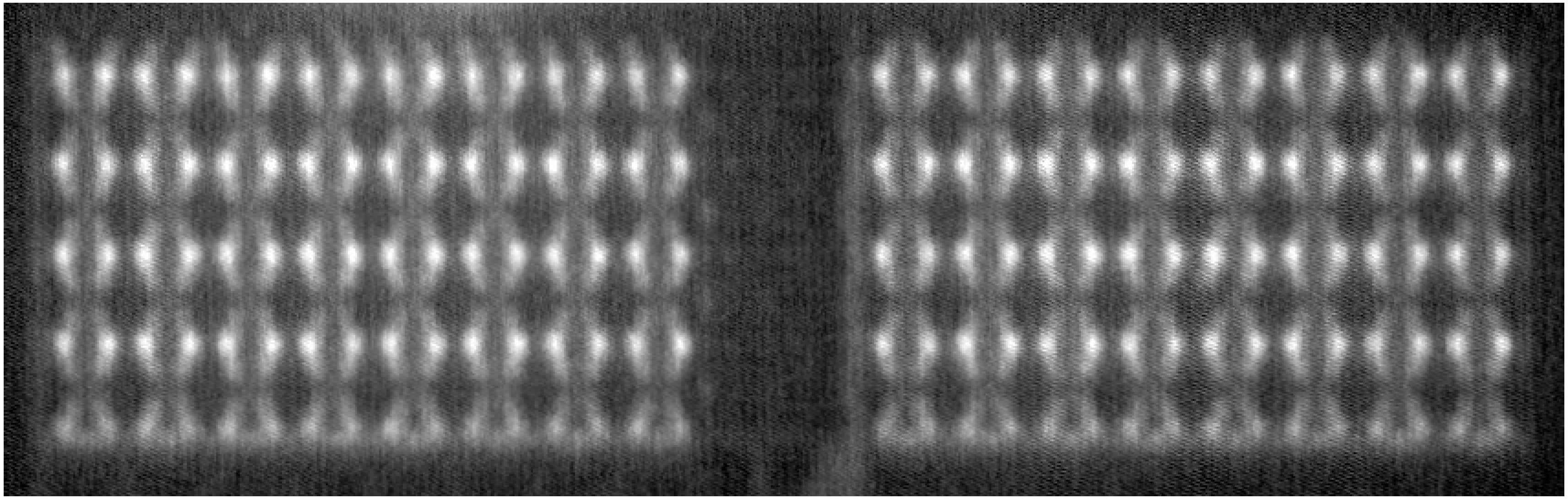
BBRAM Key Storage Off

Key Data Extraction: Bits Flipped



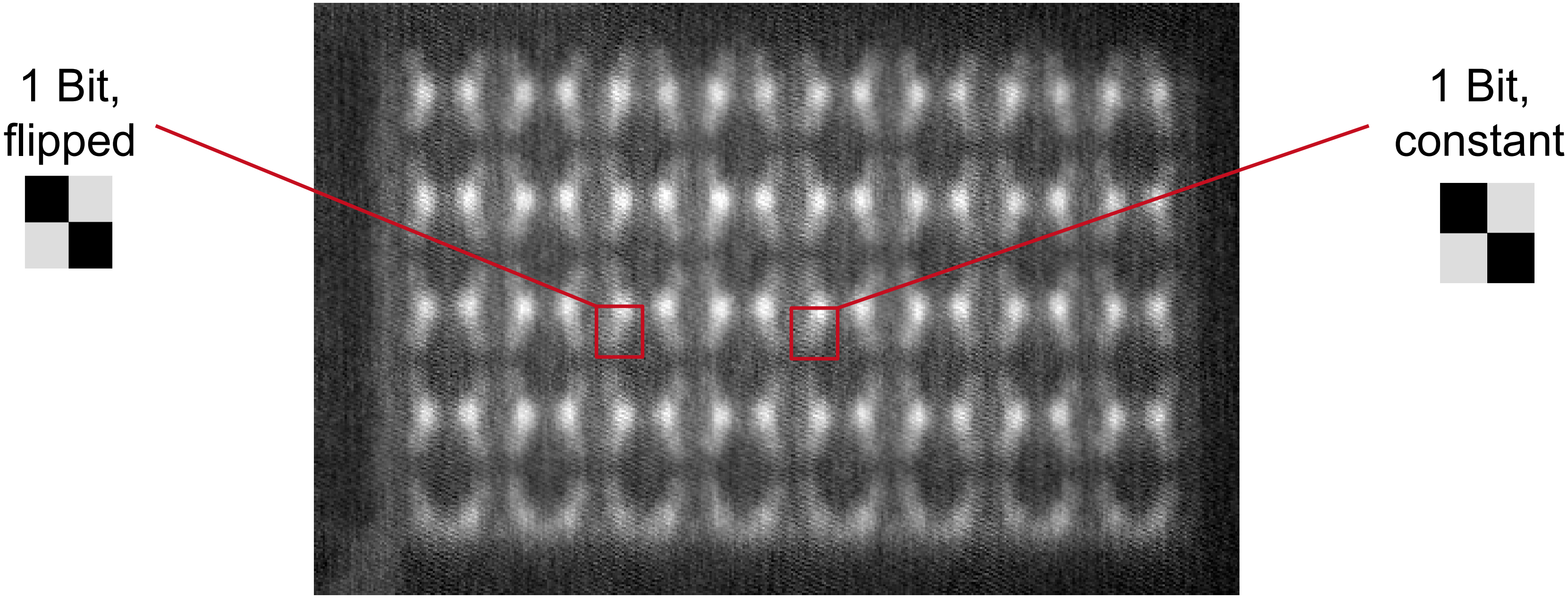
- TLS response map is data-dependent
- Bit can likely be extracted from TLS pattern
  → Detailed look at single cells needed

Key Data Extraction: Bits Flipped



- TLS response map is data-dependent
- Bit can likely be extracted from TLS pattern
  → Detailed look at single cells needed

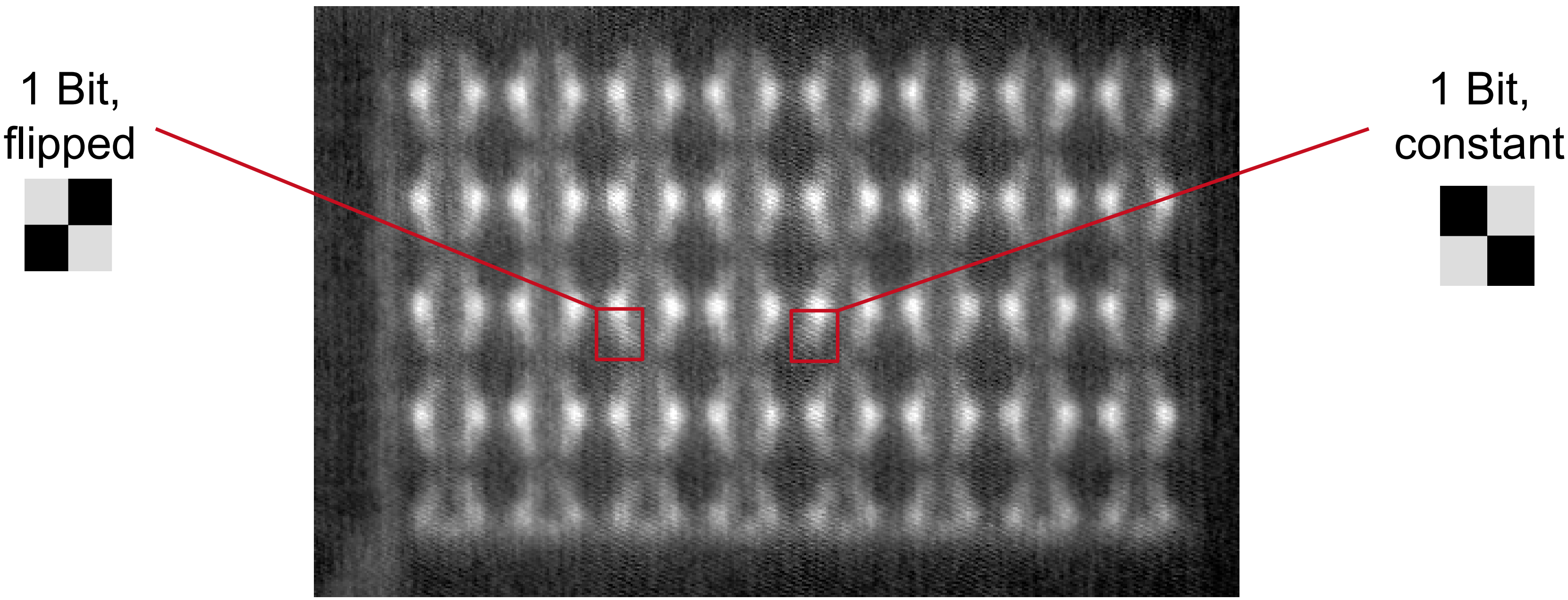
Key Data Extraction: Bits Flipped



- 0/1 state can be extracted for every cell

→ Which cell corresponds to which key bit?

Key Data Extraction: Bits Flipped



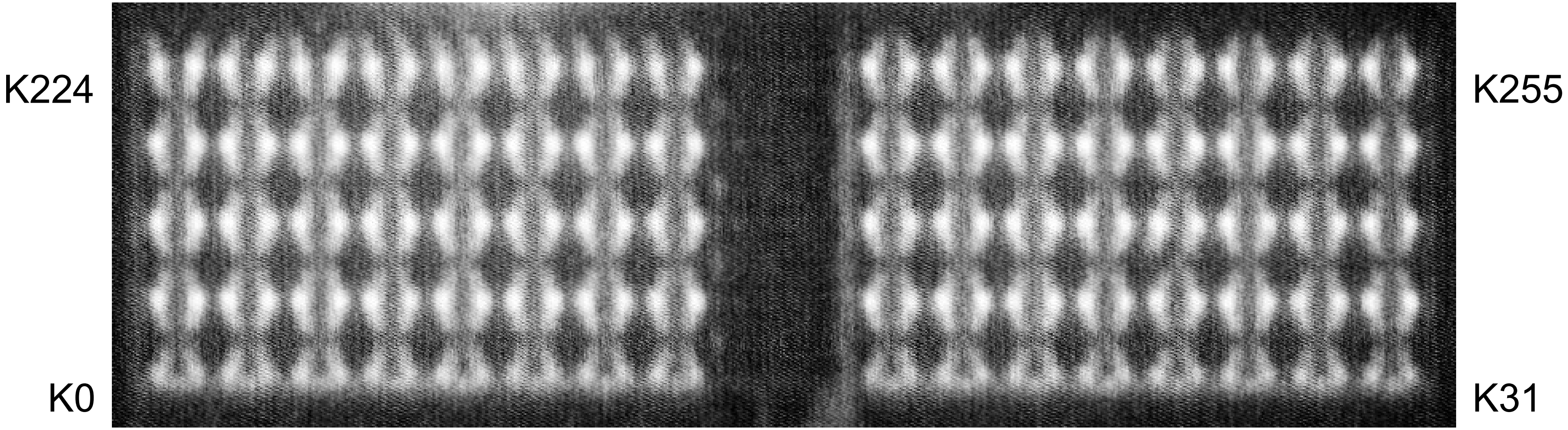
1 Bit, flipped

1 Bit, constant

- 0/1 state can be extracted for every cell

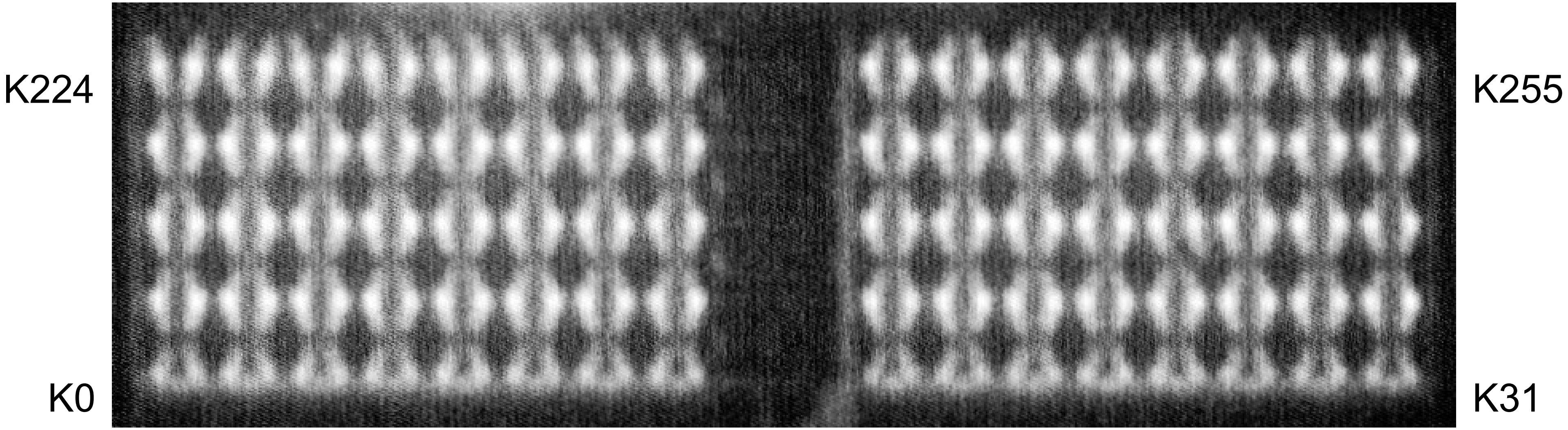
→ Which cell corresponds to which key bit?

Key Data Extraction: Bit Shifted



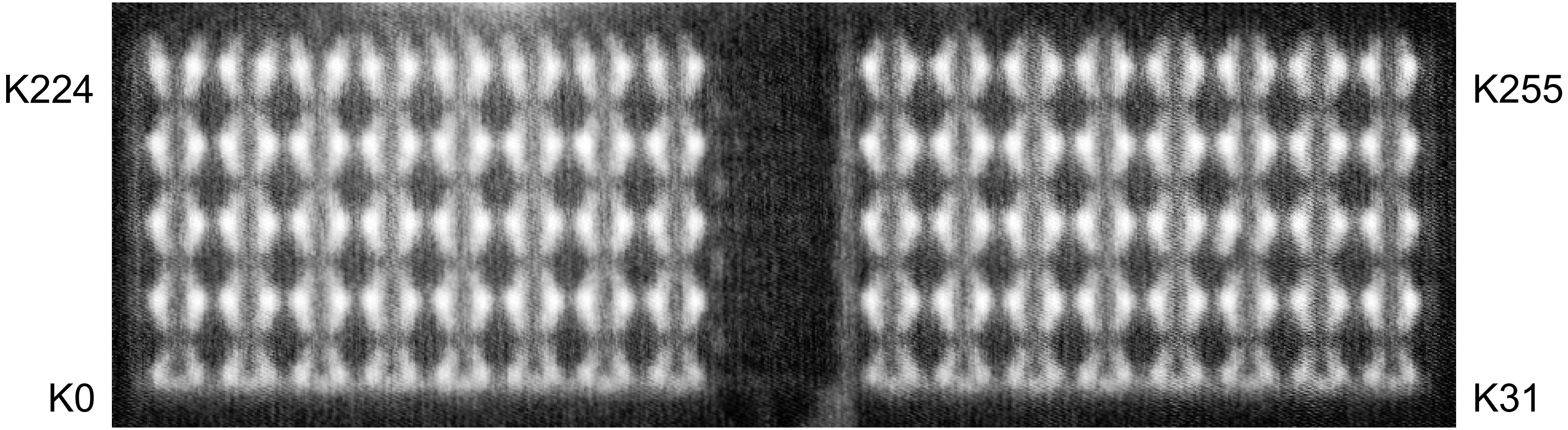
- Key with single bit set shows bit locations
- Mapping is straightforward
- Stimulation pattern + mapping:
  → Full recovery of key data

Key Data Extraction: Bit Shifted



- Key with single bit set shows bit locations
- Mapping is straightforward
- Stimulation pattern + mapping:
  → Full recovery of key data

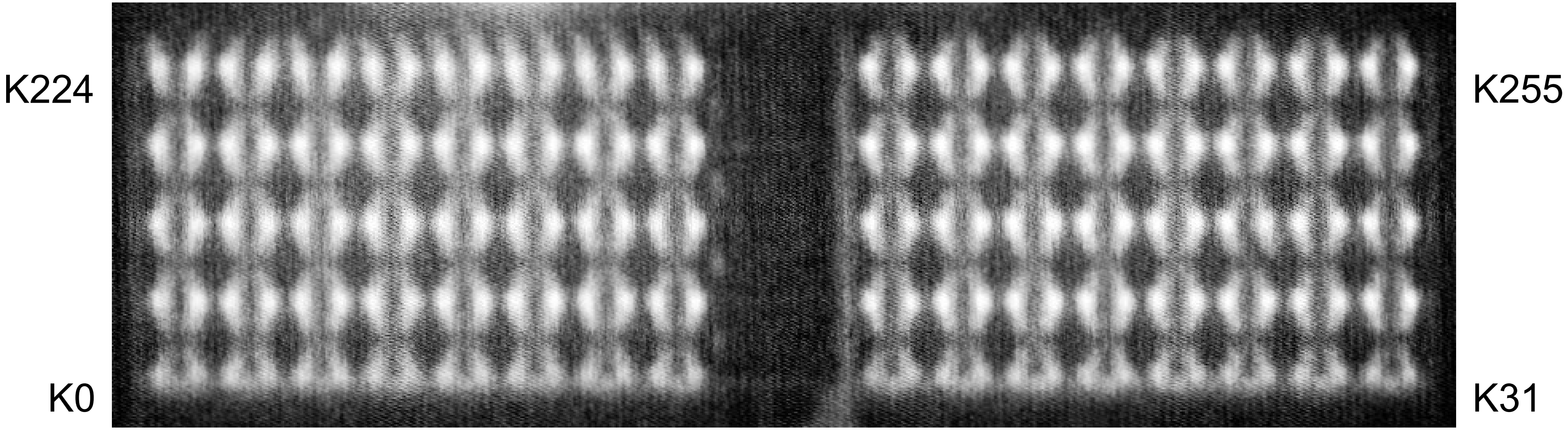
Key Data Extraction: Bit Shifted



- Key with single bit set shows bit locations
- Mapping is straightforward
- Stimulation pattern + mapping:

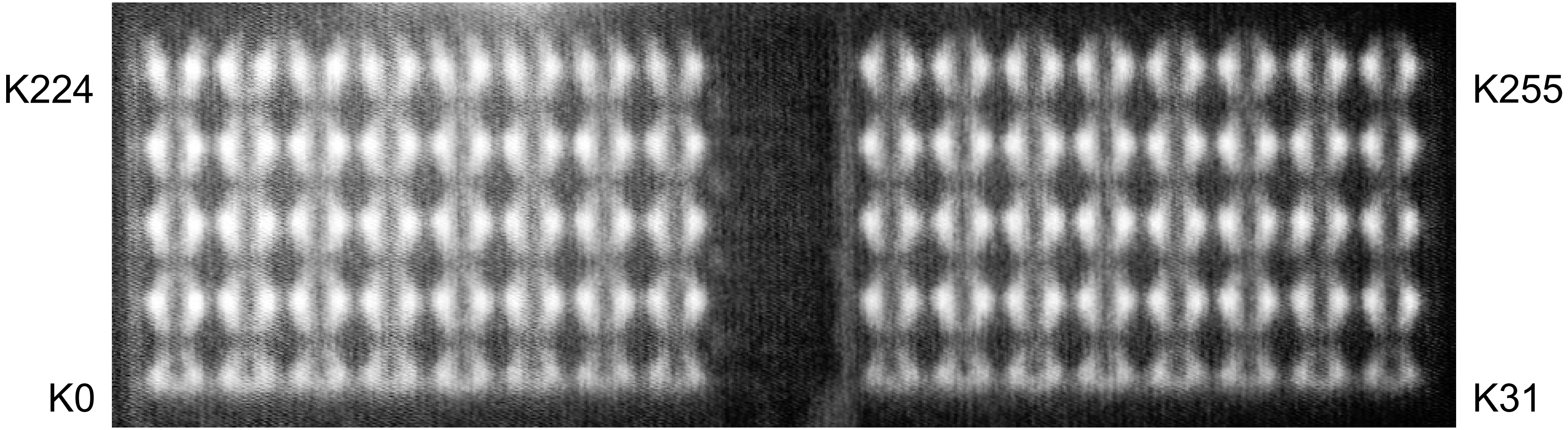
  → Full recovery of key data

Key Data Extraction: Bit Shifted



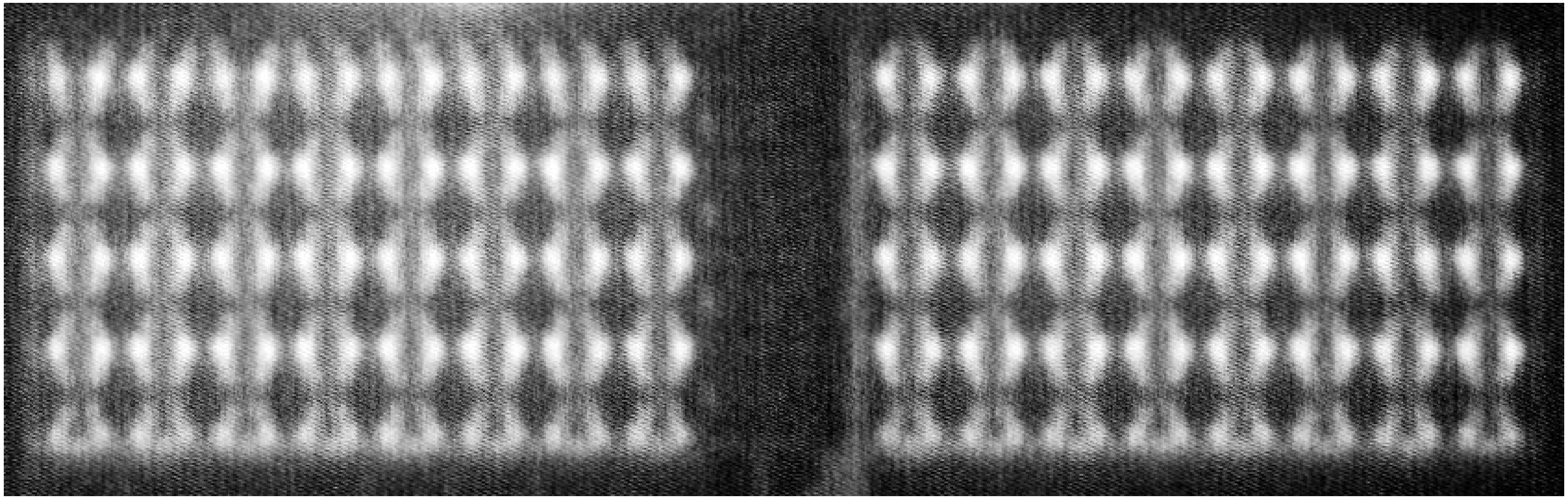
- Key with single bit set shows bit locations
- Mapping is straightforward
- Stimulation pattern + mapping:
  → Full recovery of key data

Key Data Extraction: Bit Shifted



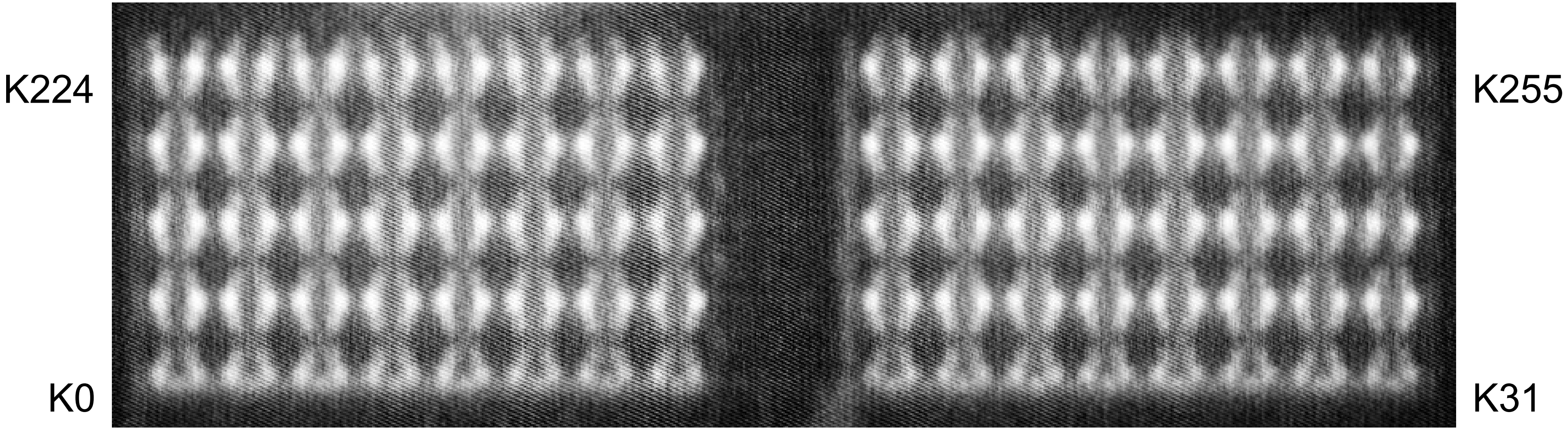
- Key with single bit set shows bit locations
- Mapping is straightforward
- Stimulation pattern + mapping:
  → Full recovery of key data

Key Data Extraction: Bit Shifted



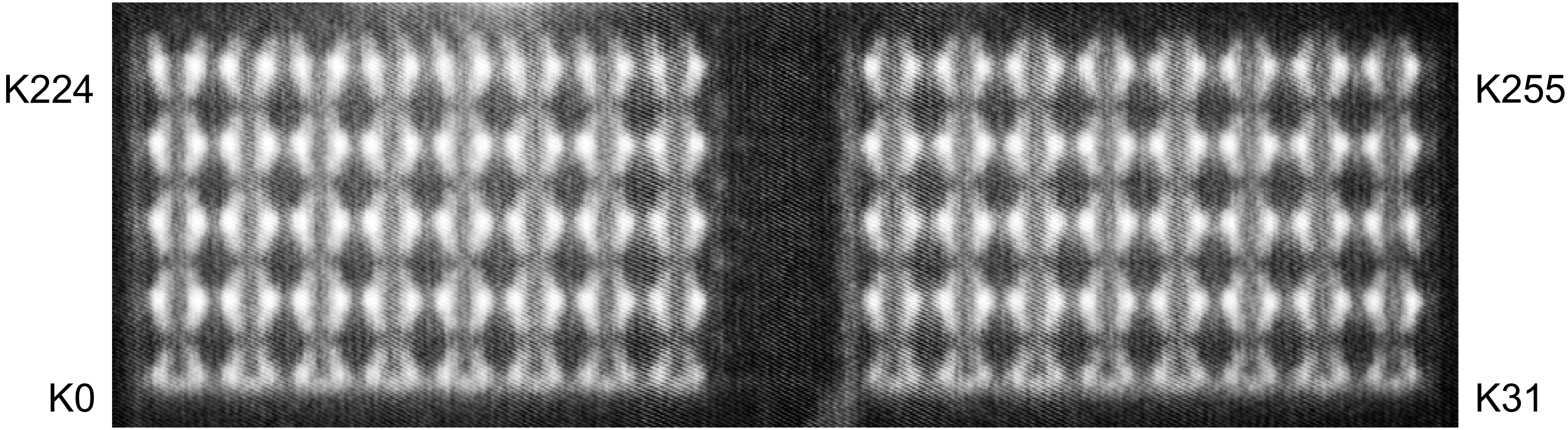
- Key with single bit set shows bit locations
- Mapping is straightforward
- Stimulation pattern + mapping:
  → Full recovery of key data

Key Data Extraction: Bit Shifted



- Key with single bit set shows bit locations
- Mapping is straightforward
- Stimulation pattern + mapping:
  → Full recovery of key data

Key Data Extraction: Bit Shifted



- Key with single bit set shows bit locations
- Mapping is straightforward
- Stimulation pattern + mapping:
  → Full recovery of key data

Conclusion Thermal Laser Stimulation

Kintex Ultrascale (20 nm):

- Lab time for reverse engineering: 7 h
- Automated key extraction: 7 keys, no errors, 15 min/key
- Cell size larger than expected, ca. (3 μm)^2 vs. (0.3 μm)^2

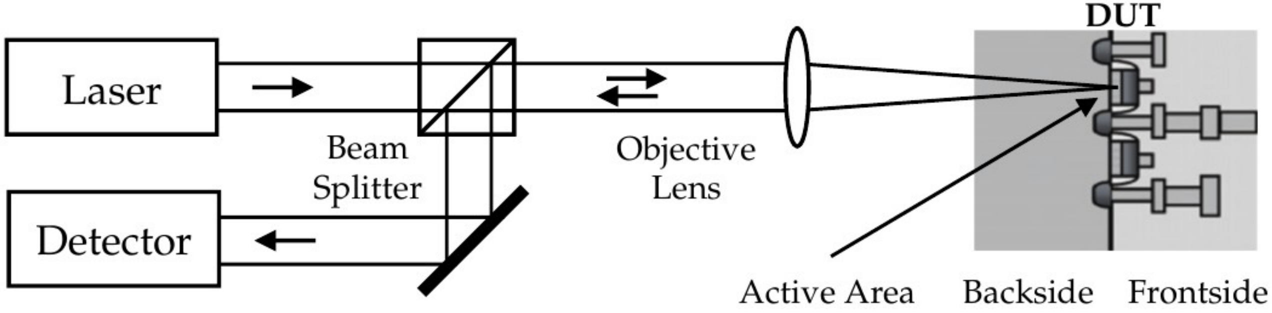
Expected SRAM cell size limit:

- (2 μm)^2 current setup
- (0.5-0.6 μm)^2 with resolution-enhancing lens (SIL)

Outline

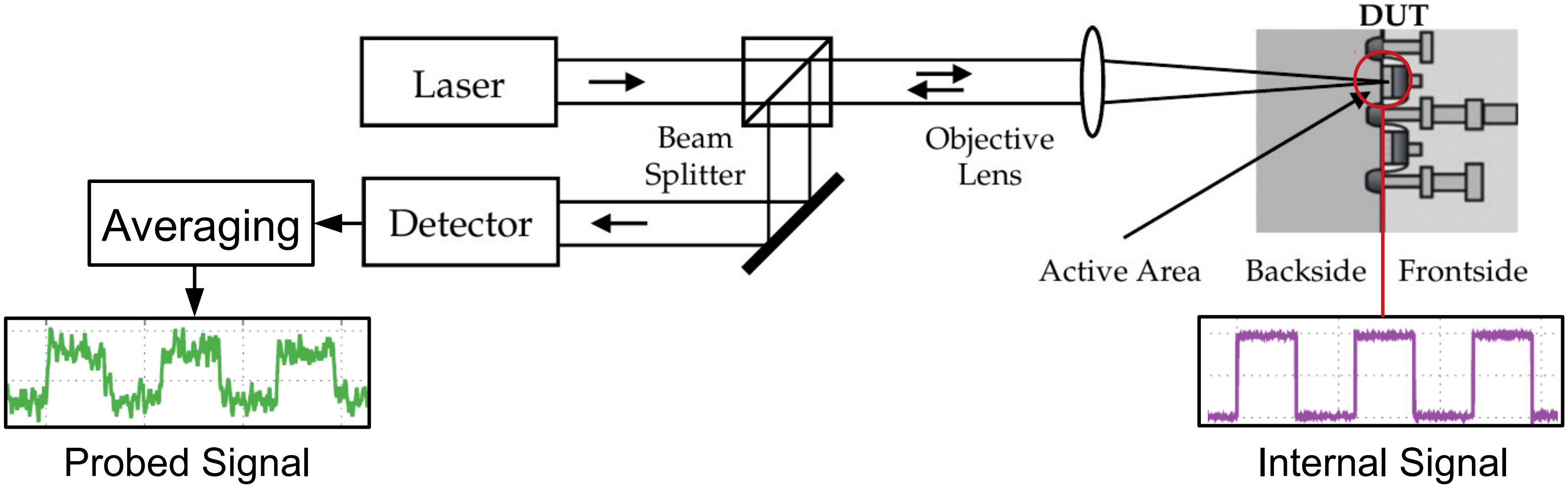
- Background
  - Laser Scanning Microscopes
  - Field Programmable Gate Array Bitstream Encryption
- Decryption Key Extraction Using Thermal Laser Stimulation
- Plaintext Data Extraction Using Optical Contactless Probing
- Conclusion

Optical Contactless Probing



- Changes of absorption coefficient and refractive index in active area by electrical field and current → small light modulation (ppm)
- Detector signal is modulated by signal at transistor
- Can be analyzed to extract information from silicon

Optical Contactless Probing

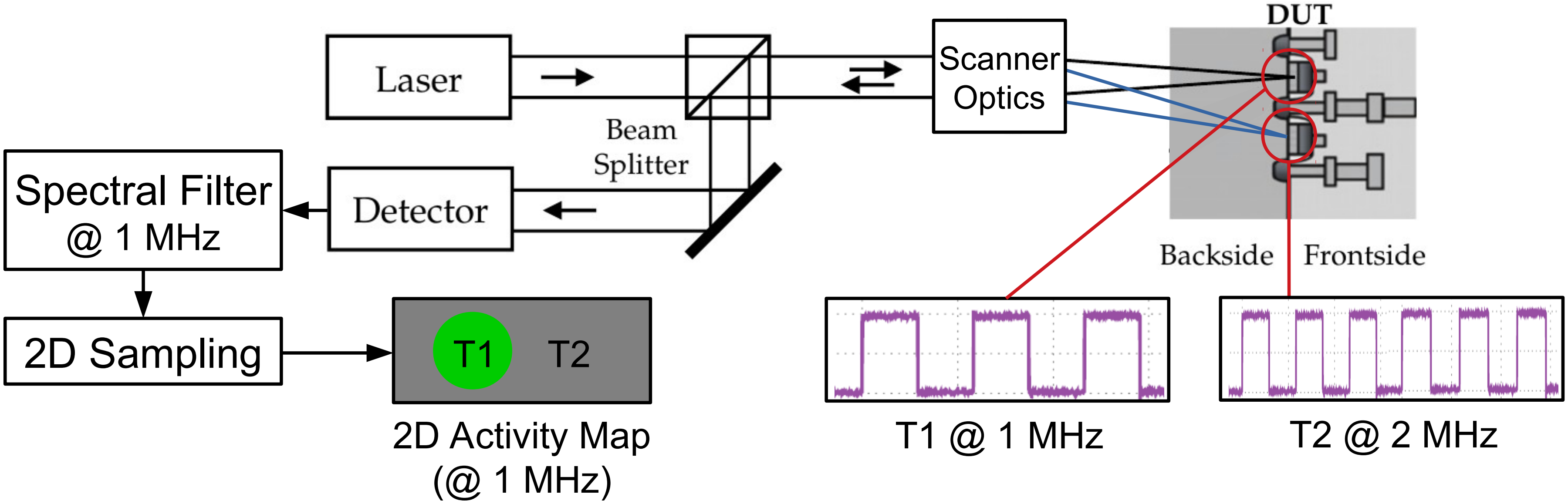


Laser Voltage Probing (LVP):

Beam is stationary, transistor modulates reflected light

→ probing of electrical signal via averaged detector signal

Optical Contactless Probing



Laser Voltage Imaging (LVI):

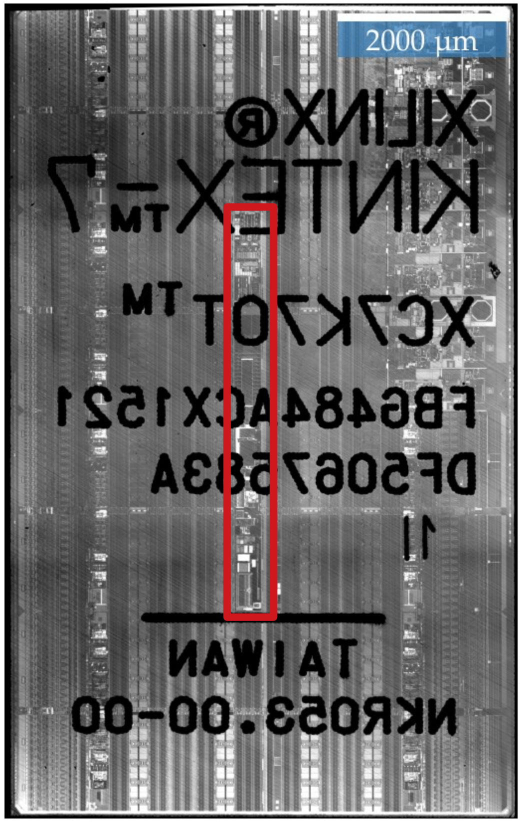
Beam is *scanned*, for every pixel modulation is frequency-filtered

→ *2D map* of transistors active at the filtered frequency

Plaintext Data Extraction using LVP/LVI

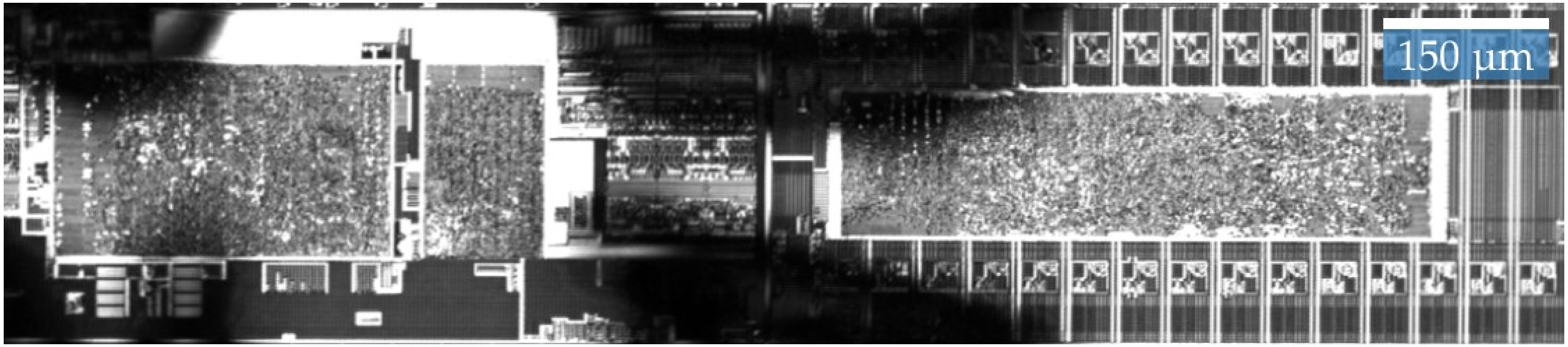
- Device: Xilinx Kintex 7 FPGA (28 nm)
- Flip-Chip: no preparation
- 256-bit AES decryption core
- Approach:
  - Locate output of decryption core
  - Extract plaintext data optically

Optical Overview



- Candidates for configuration logic can be identified optically
- Additional information from datasheets
- LVI tests with externally available configuration clock for confirmation
- LVP allowed to observe data entering the configuration logic

Configuration Area



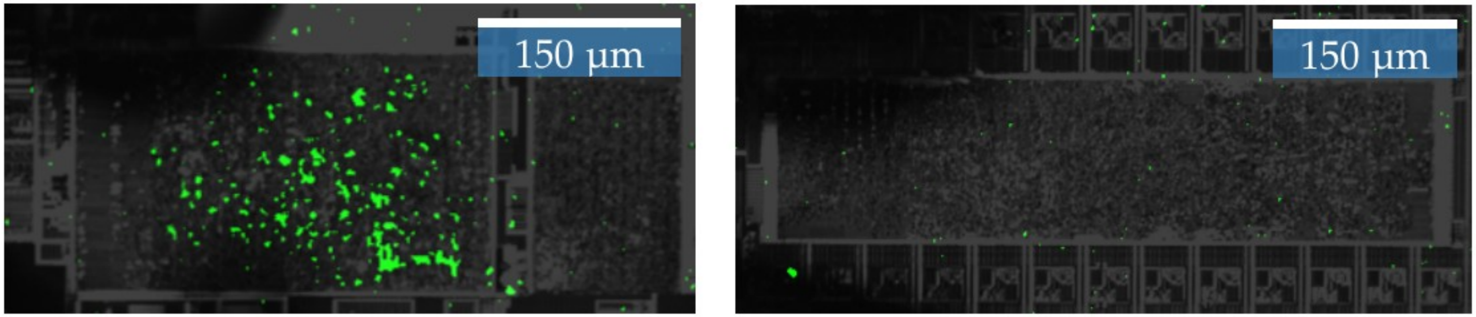
Central configuration area:

- Two candidates for synthesized cores found visually

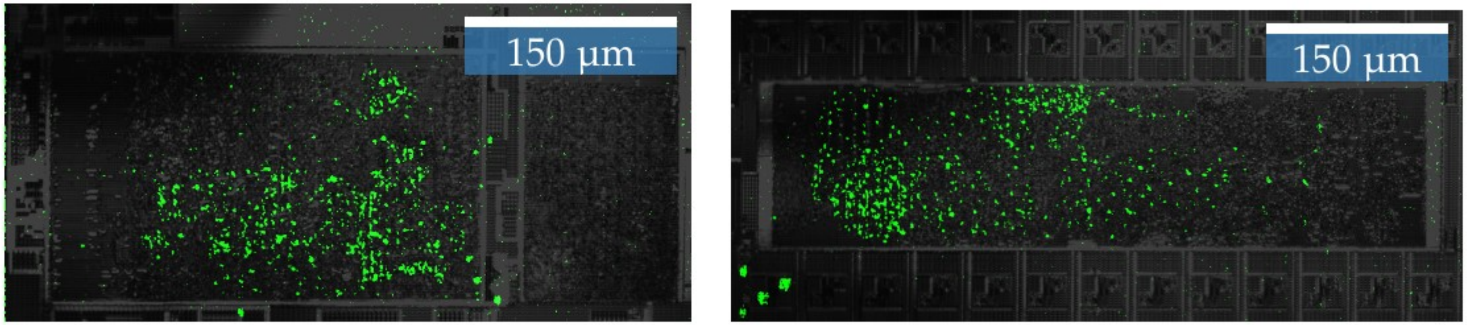
→ Which one is the decryption core?

LVI @ Configuration Clock: Encrypted vs. Unencrypted

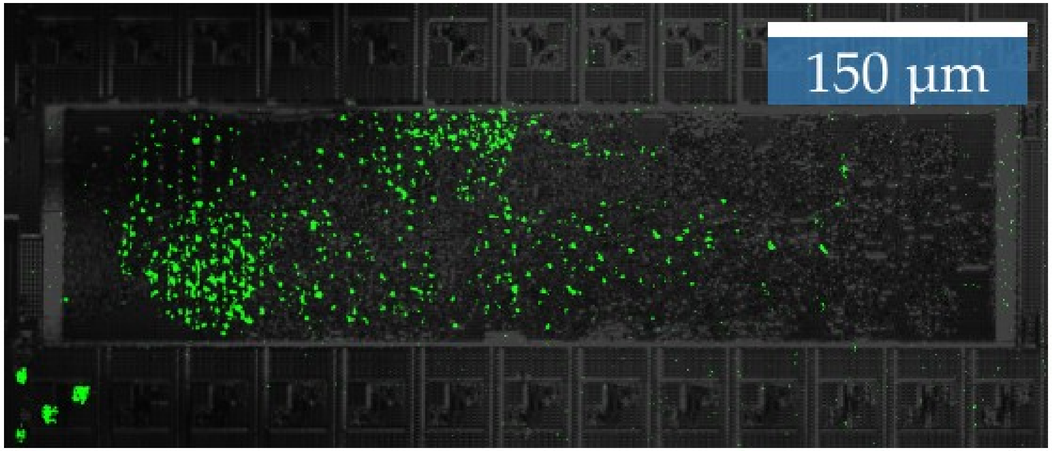
Encryption Off:



Encryption On:



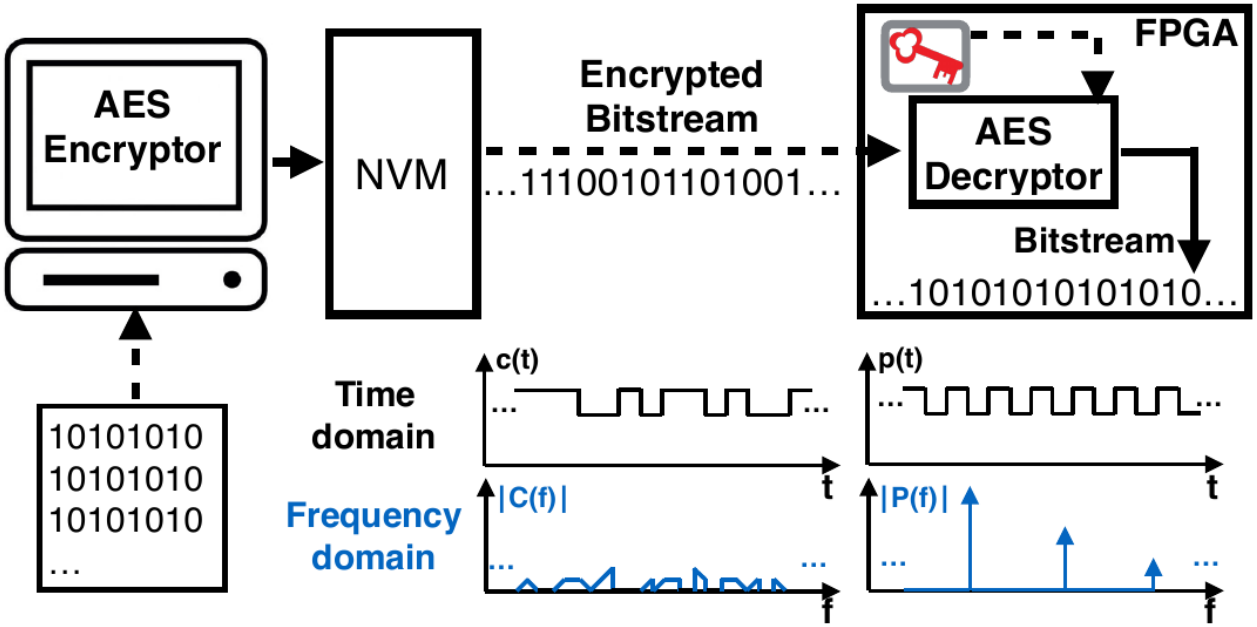
Localization of Plaintext Transistors



Decryption core found, but only clock activity visible
→ How to locate plaintext transistors?

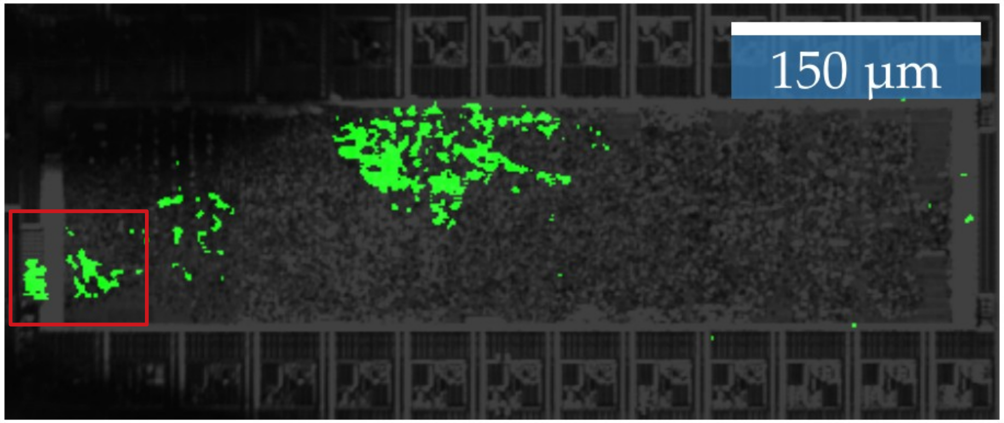
Idea: Make **only** plaintext transistors detectable in LVI map

Plaintext Frequency Induction



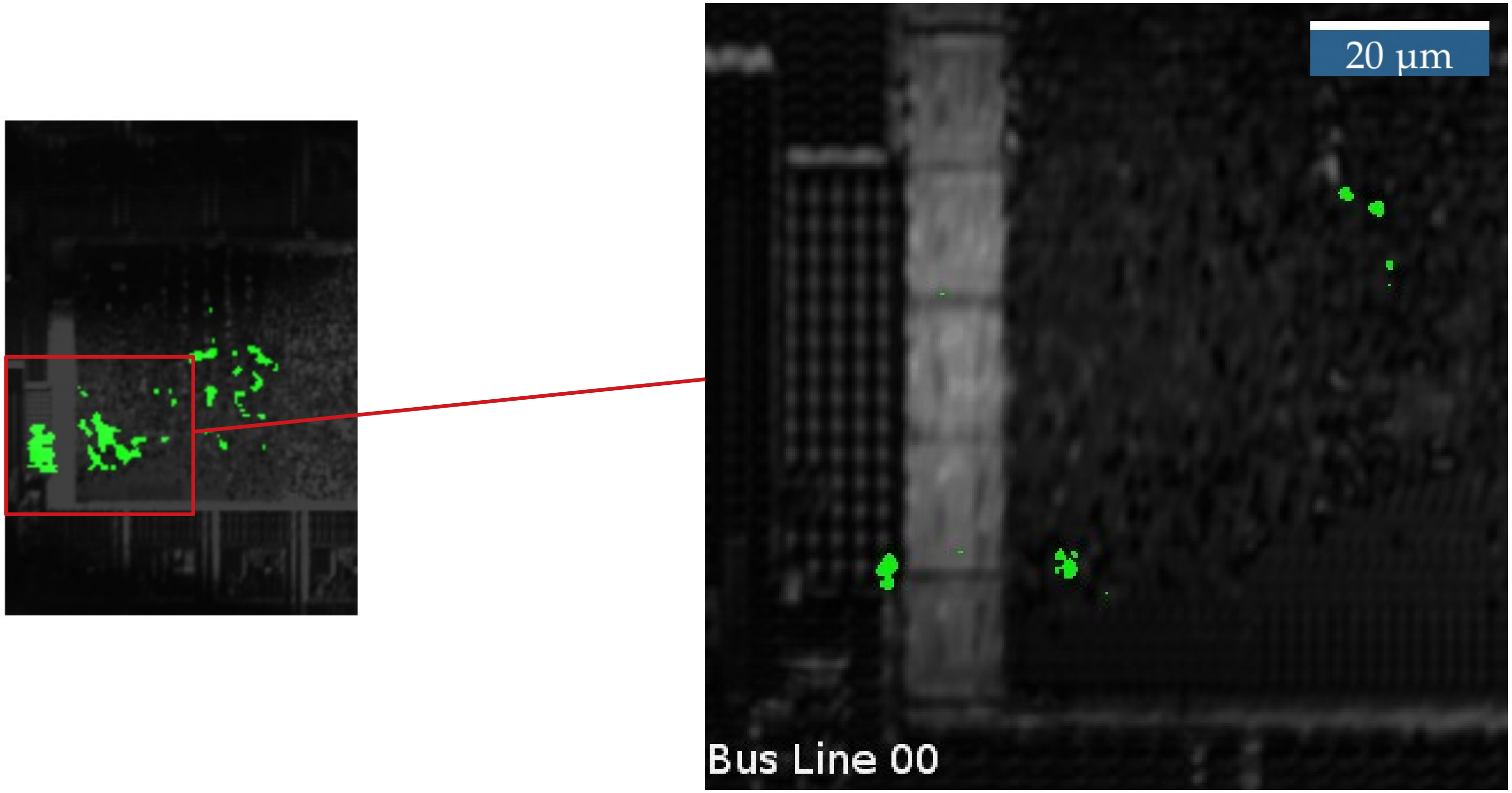
- Modified bitstream creates periodicity in plaintext
- Ciphertext has no periodicity due to encryption
- Only plaintext gates will switch with induced frequency → discoverable via LVI

LVI with Plaintext Frequency Induction

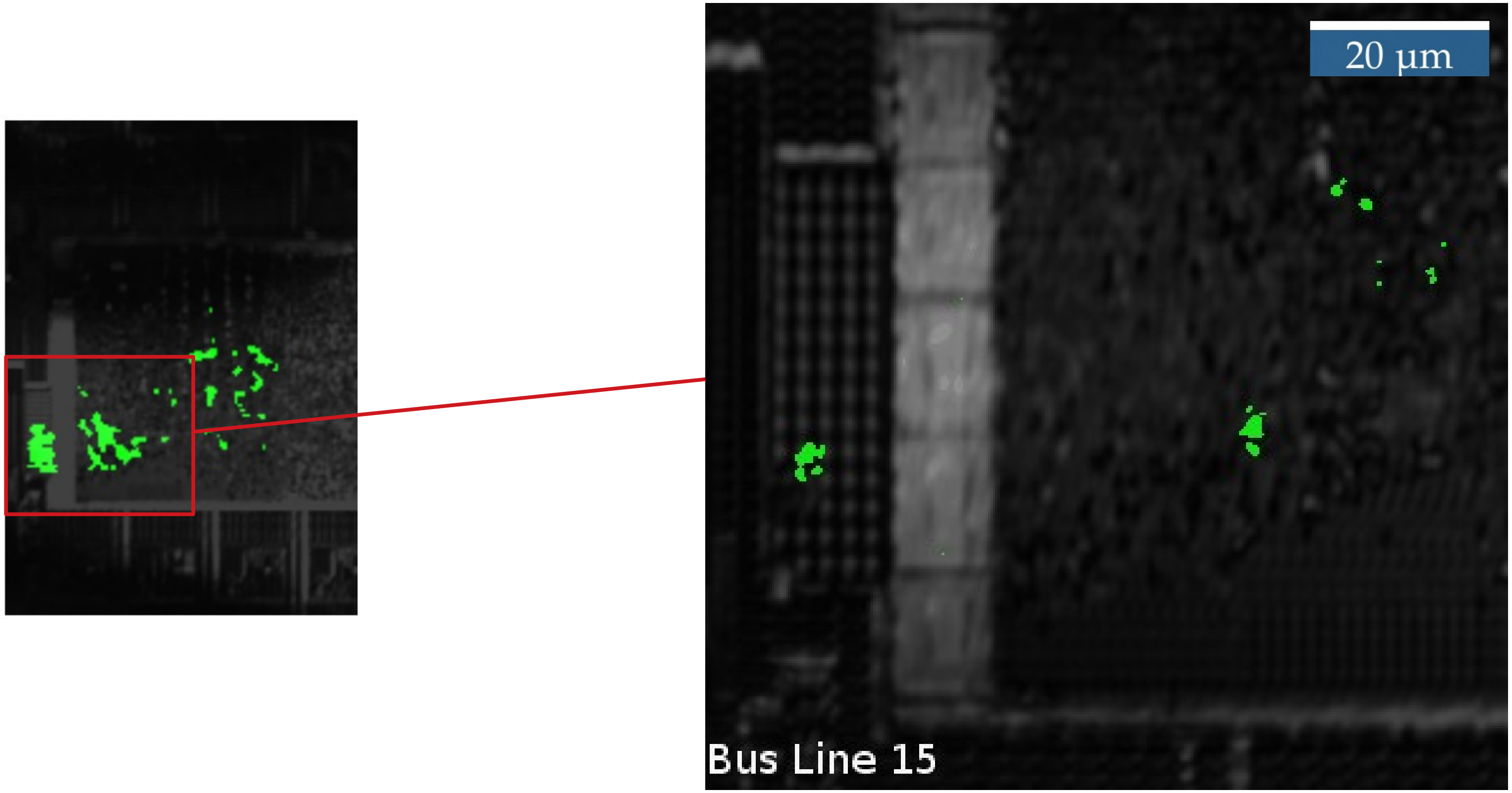


- 32-bit bus: correction of frequency generation
  → Output candidate found in bottom left area
- Bus line mapping needed
- Approach:
  - Induce frequency only on single bus line
  - Repeat for all bus lines

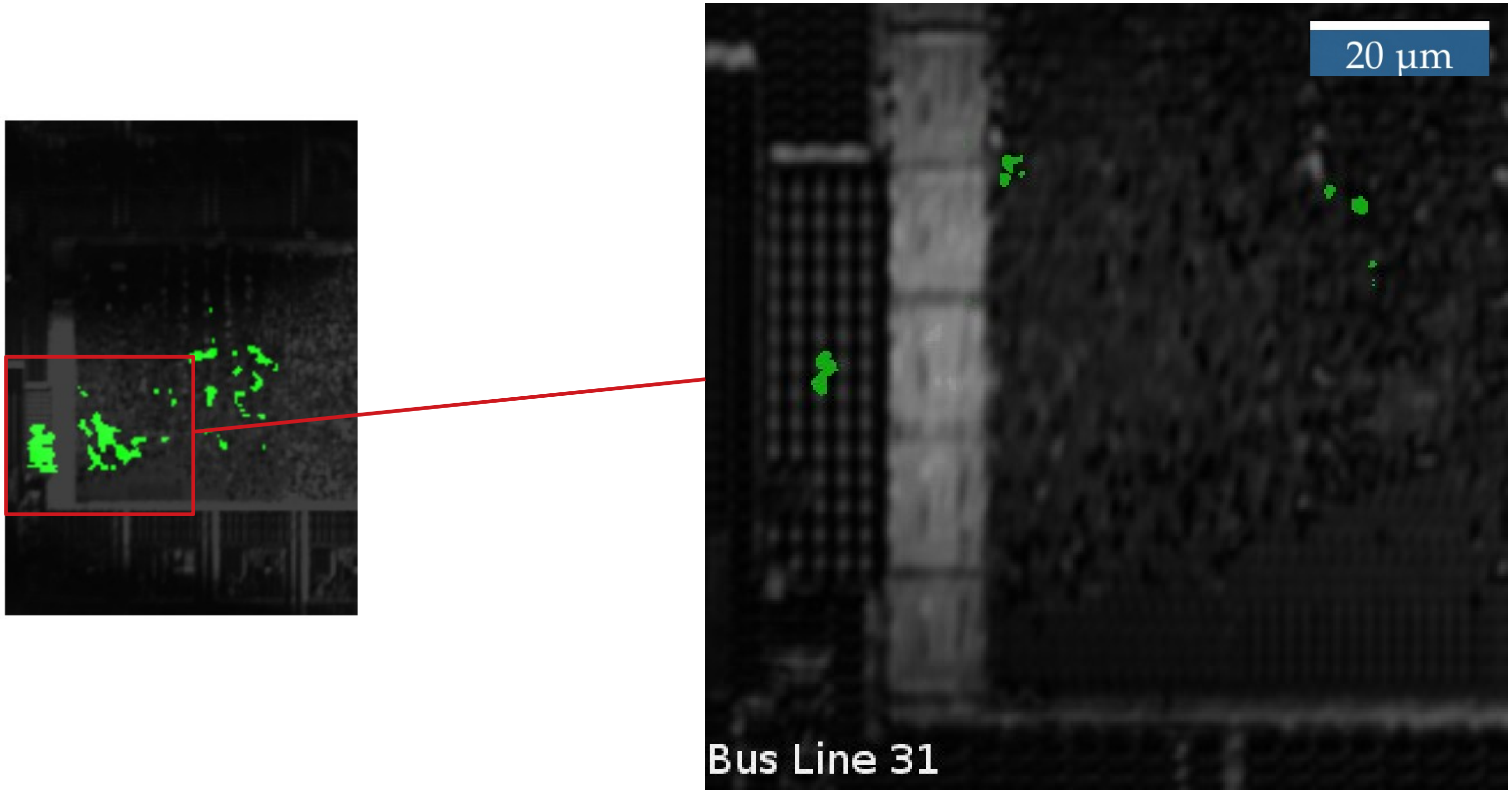
Bus Line Mapping



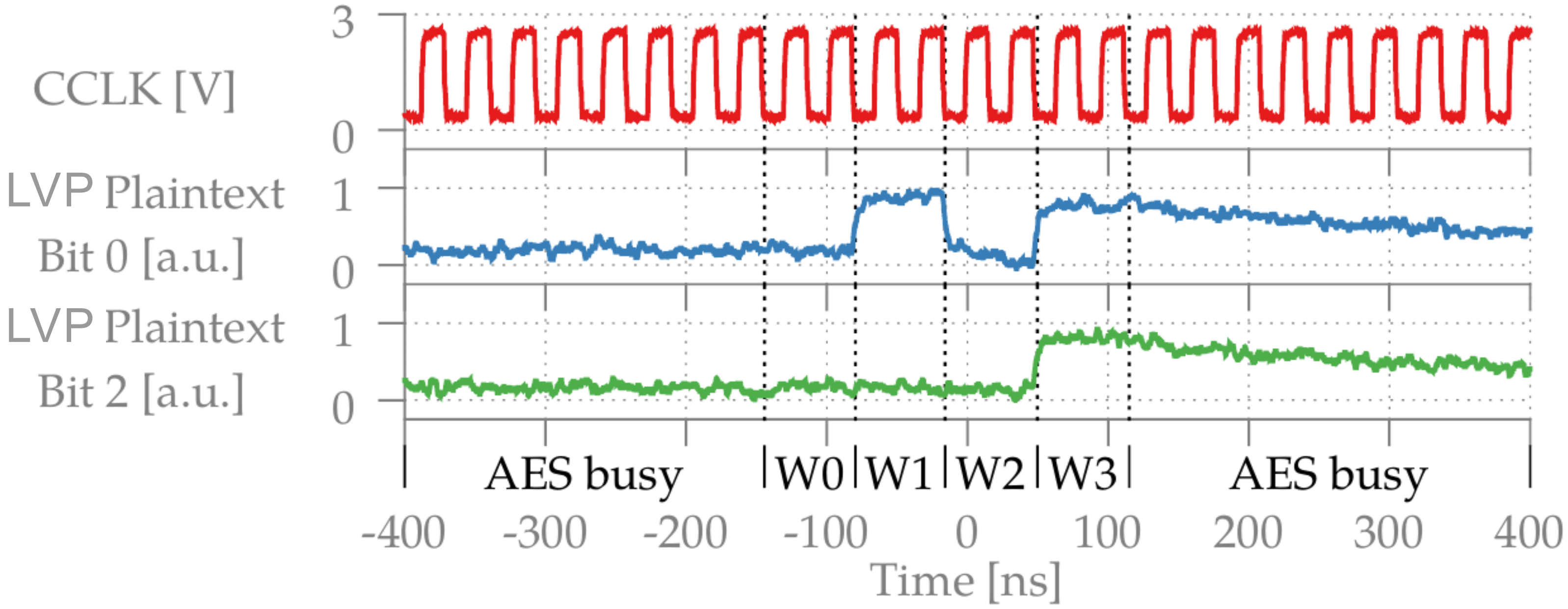
Bus Line Mapping



Bus Line Mapping



Data Extraction via Laser Voltage Probing



→ Full plaintext can be extracted by probing all 32 bus lines this way

Conclusion Optical Probing

Kintex 7 (28 nm):

- Attack conducted non-invasively
- Lab time for reverse engineering: 75 h
- Full bitstream extraction: 43 minutes (acquisition time, estimated)

Attack Limitations:

- Configuration clock is key for averaging synchronization
- Expected transistor *separation* limit:
  - 1 µm current setup
  - 0.25 µm with resolution-enhancing lens (SIL)

Outline

- Background
  - Laser Scanning Microscopes
  - Field Programmable Gate Array Bitstream Encryption
- Decryption Key Extraction Using Thermal Laser Stimulation
- Plaintext Data Extraction Using Optical Contactless Probing
- Conclusion

Conclusion

- Small technology sizes are susceptible to optical attacks

  → 1 µm optical resolution vs. 28/20 nm technology size
- Attack can be mounted in a non-invasive manner and without any device preparation
- Fast reverse engineering possible (10 days / 7 hours)
- Lower cost and higher availability of TLS in comparison to other optical attacks makes this technique especially threatening.

→ If no proper IC backside protection is realized, future generations of FPGAs will still be vulnerable to such attacks

References

LVI/LVP Attacks:

“No Place to Hide: Contactless Probing of Secret Data on FPGAs”, H. Lohrke, S. Tajik, C. Boit, J.-P. Seifert, CHES 2016: Cryptographic Hardware and Embedded Systems

“On the power of optical contactless probing: Attacking bitstream encryption of FPGAs”, S. Tajik, H. Lohrke, J.-P. Seifert, C. Boit, CCS '17 Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security

TLS Attacks:

“Key Extraction Using Thermal Laser Stimulation”, H. Lohrke, S. Tajik, T. Krachenfels, C. Boit, J.-P. Seifert, IACR Transactions on Cryptographic Hardware and Embedded Systems (2018)

“Evaluation of Low-Cost Thermal Laser Stimulation for Data Extraction and Key Readout”, T. Krachenfels, H. Lohrke, J.-P. Seifert, E. Dietz, S. Frohmann. H.-W. Hübers, to be published in Journal of Hardware and Systems Security

Thank you!