

Investigation of Sensitivity of Different Logic and Memory Cells to Laser Fault Injections

Dmytro Petryk



MOTIVATION

Data security is realized using **cryptographic algorithms**:

- based on secrecy of cryptographic keys
- the goal of attackers is to reveal the secret/private keys

Time to reveal cryptographic key is much longer than the relevance of protected data

"Hello" + = "KZOKVey81c="

+ = "KZOK0ey81c="

Physical attacks **reduce** the time to reveal the key

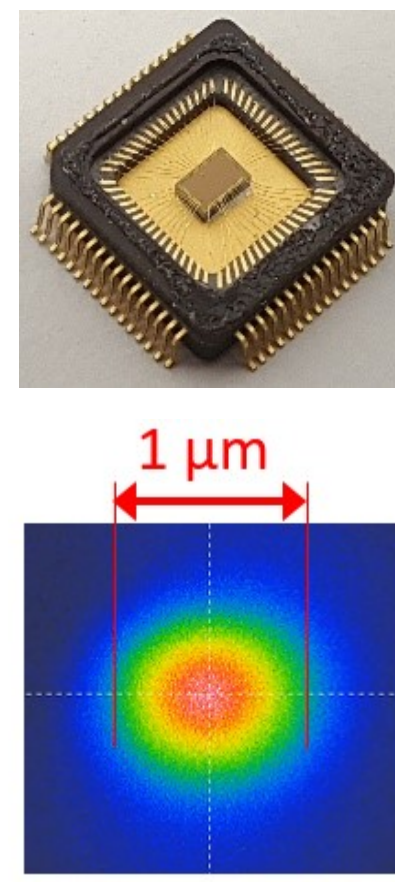
Fault Injection attacks:

- Injection
- Analysis
- Revealing the key

OPTICAL FI ATTACKS & SETUP

Optical FI attacks:

- Semi-invasive
 - decapsulation of the chip
- Spatial precision
 - down to 1 μm
- Accurate timing
 - tens of fs



Volatile

Cryptographic implementations (e.g. AES, RSA): microcontroller or FPGA

Results:

- Key retrieval
- Bypass PIN check
- Instruction skipping

Non-volatile

Non-cryptographic implementations:

- different logic and memory cells

Results:

- Transient and permanent faults

RRAMs (HfO₂-based):

- different architecture

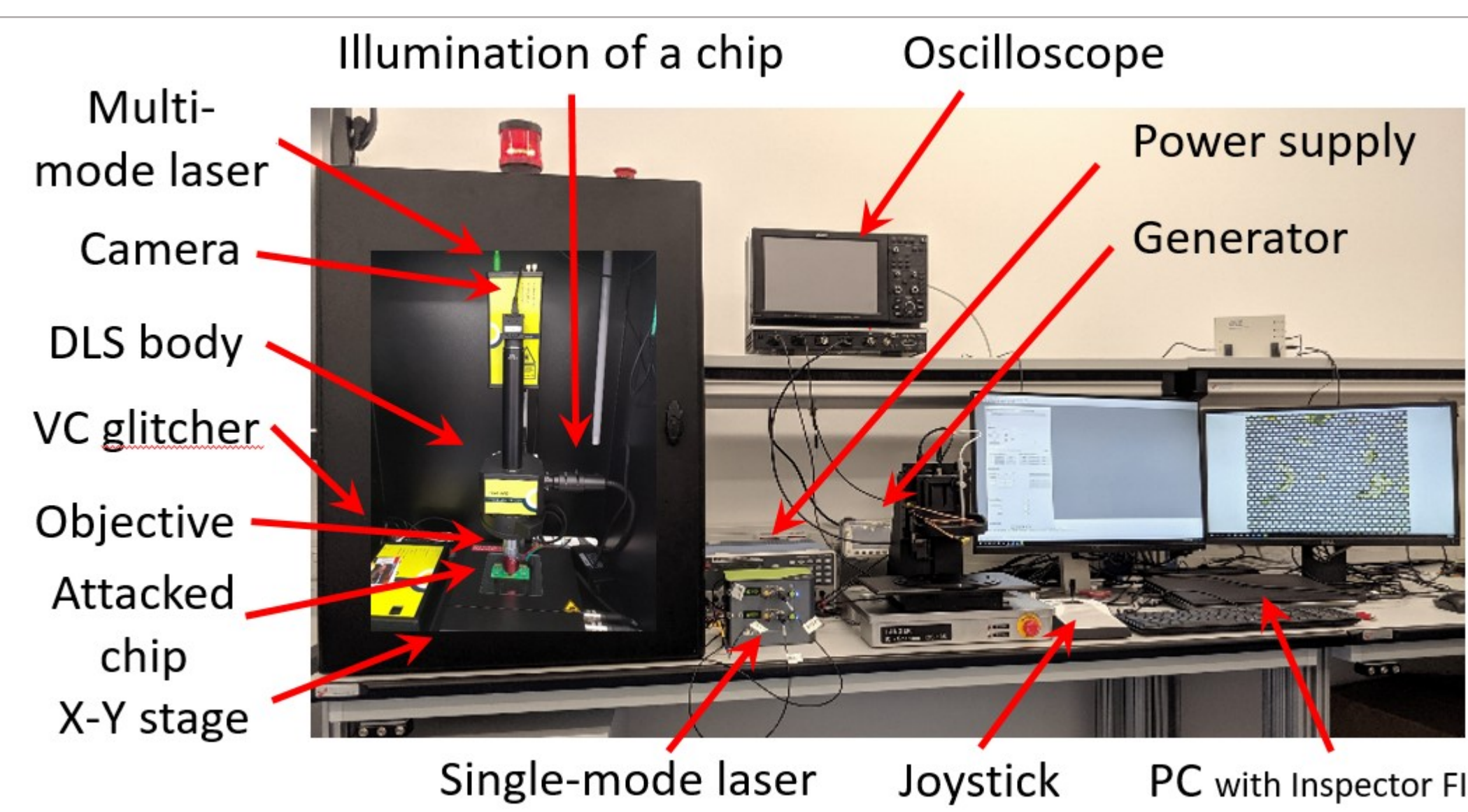
Results:

- Transitions of states

Most of the attacks in the overviewed literature were done through a **back-side** of a chip and focused on feasibility of **FI**

Verification of setup parameters:

- Power: 0.00 V (0.26 V) – 3.30 V (3.44 V), linear control
- Pulse duration: 20 ns – 100 μs (1 μs)
- Spot size:
- Single-mode laser: 15 (45.0), 4 (11.0), 1.5 (3.2) or 1 (1.5) [μm]
- Multi-mode laser: 60x14 (150.0x74.0), 15x3.5 (29.5x17.5), 6x1.5 (8.6x5.2) or not given (5.9x3.3)
- Chip position: 3 μm accuracy, 0.25 μm step



RESULTS

Volatile

- Libval chips based on standard library cells:
 - 250 nm (SG25H3)
 - 130 nm (SG13G2)
- Radiation-hard shift registers:
 - JICG, 250 nm
 - TMR, 130 nm

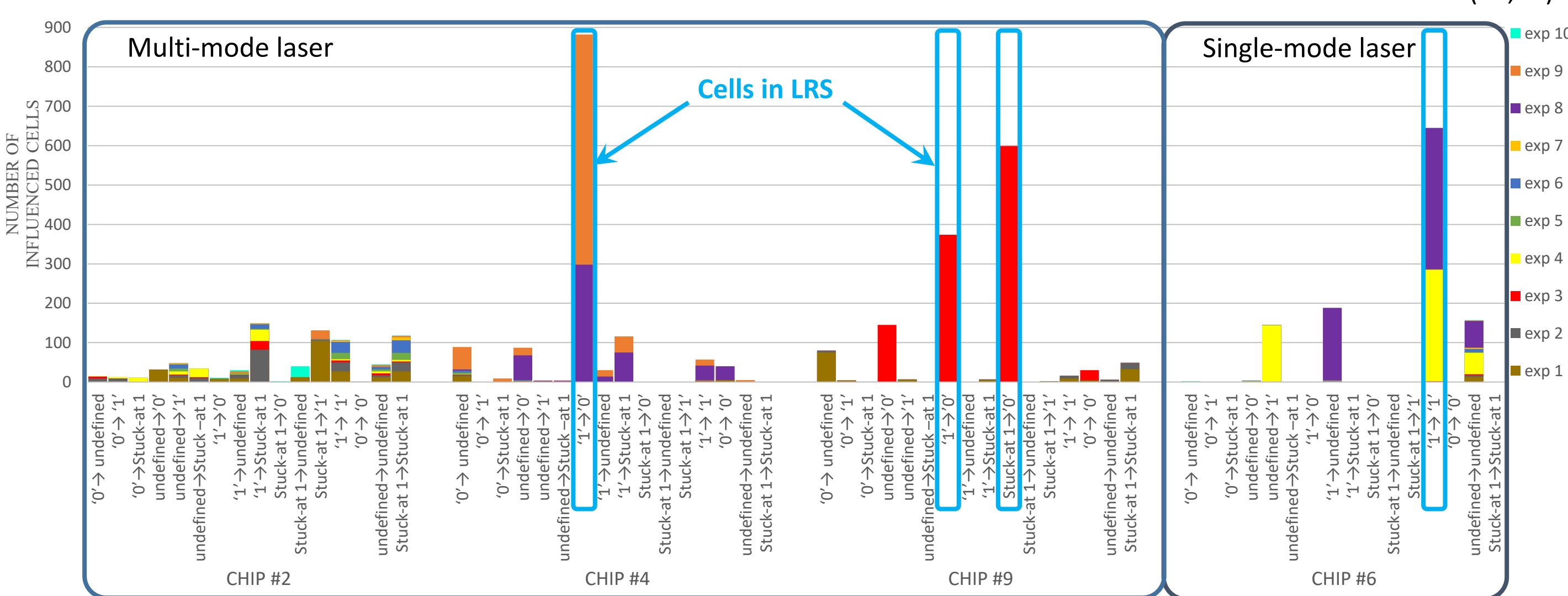
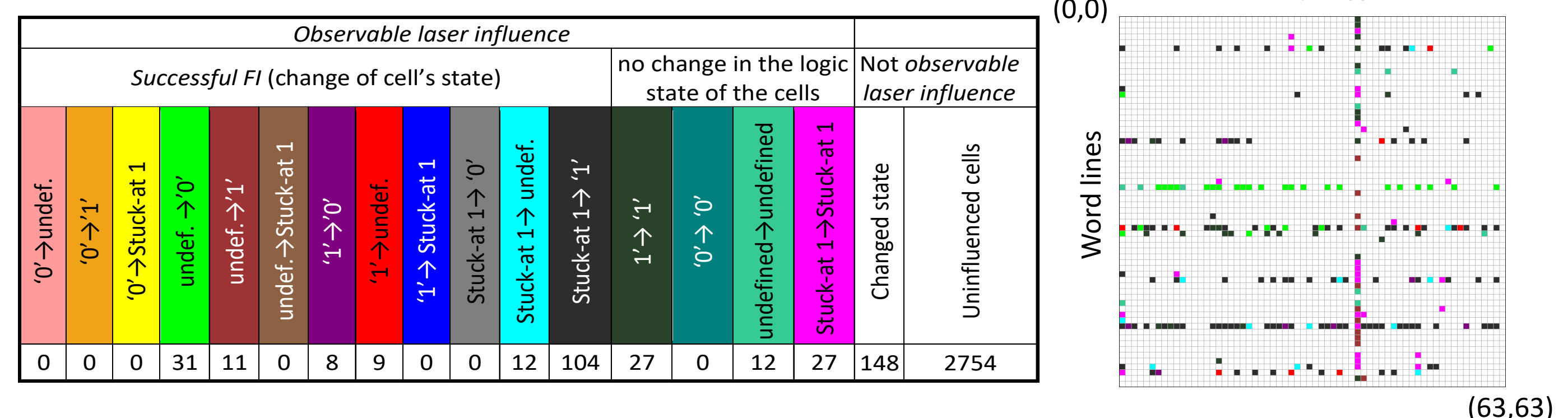
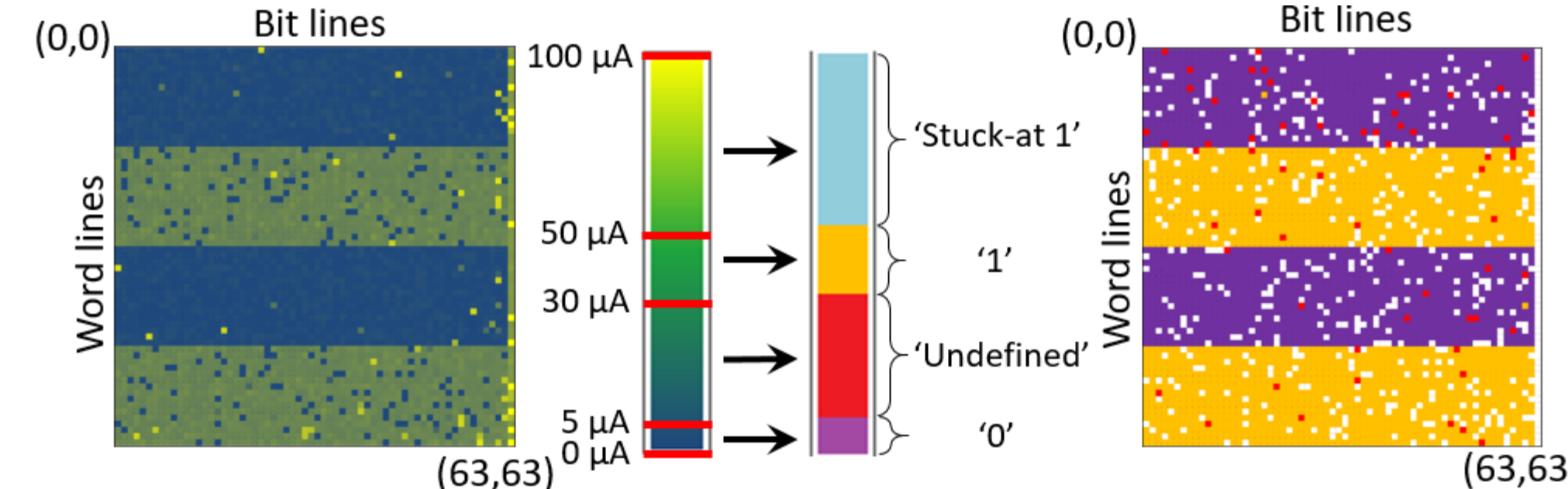
Chip	Libval, 250 nm				Libval, 130 nm			
	Single-mode		Multi-mode		Single-mode		Multi-mode	
Gate	FF	INV	NAND	NOR	FF	INV	NAND	NOR
Bit-set	✓	x	x	x	✓	x	x	x
Bit-reset	x	✓	✓	✓	x	✓	✓	✓
Bit-flip	x	x	x	x	x	x	x	x
Stuck-at	x	x	x	x	✓	✓	✓	x

Shift register	JICG		TMR	
	Single-mode	Multi-mode	Single-mode	Multi-mode
Bit-set	✓	✓	x	✓
Bit-reset	✓	✓	x	✓
Bit-flip	x	✓	x	x
Stuck-at	x	x	x	x

Not all attacked cells were manipulated due to metal fillers

Non-volatile

- IHP chips with RRAM cells:
 - 250 nm
 - 4k bit
 - 1T-1R architecture



Optical FI attacks against JICG shift-registers

Bit-set:

Bit-reset:

Single-mode laser:

Multi-mode laser:

PMOS

Overlap of two areas

FUTURE WORK

RRAM: further investigation is required

- Precise manipulation of RRAM cells
- Investigation of cross-bar structures
 - Important for AI-accelerators

Laser illumination attacks

- Improving SCA attacks by increasing power consumption of a circuit (without FI)
- Concentrating on analysis of static power consumption (data dependent)

Metal fillers

- placed over sensitive areas of cells are expected to prevent the front-side attacks
- the placement of the metal fillers can be automated

Basis for countermeasures

Can be a new SCA leakage source

Low-cost countermeasure

The research was carried out within a framework of Inter-dependent Challenges of Reliability, Security and Quality in Nanoelectronic Systems Design (RESCUE) project (funded by the European Union's Horizon 2020 research and innovation program under the Marie Skłodowska-Curie grant agreement No 722325) and internal IHP project Total Resilience.

