Adjusting laser injections for fully controlled faults

Franck Courbon[1,2], Philippe Loubet-Moundi[1],
Jacques Fournier[3], Assia Tria[3]

[1] **GEMALTO**, Security Labs, @ La Ciotat, France

[2] **Ecole des Mines de Saint-Etienne**, CMP-GC/LSAS, @ Gardanne, France

[3] **CEA**, CEA Tech Region, DPACA/LSAS, @ Gardanne, France,

COSADE 2014
Tuesday 15th April 2014

COSADE 2013 *Fault Analysis Attack session*

10:50 11:15	***coffee break***
	session 2: Fault Analysis Attack ***Session chair: Alexandre Berzatti*** **Defeating with Fault Injection a Combined Attack Resistant Exponentiation** Benoît Feix (XLIM, Limoges University / Inside Secure, France), Alexandre Venelli (Inside Secure, France).
11:15 12:30	**Fault Attacks on Projective-to-Affine Coordinates Conversion** Diana Maimut (École Normale Supérieure), Cédric Murdica (Secure-IC, Télécom ParisTech), David Naccache (Ecole Normale Supérieure), Mehdi Tibouchi (NTT Secure Platform Laboratories). **Improved Algebraic Fault Analysis: A Case Study on Piccolo and Applications to Other Lightweight Block Ciphers** Fan Zhang (University of Connecticut, USA), Xinjie Zhao (Ordnance Engineering College, China, and The Institute of North Electronic Equipment), Shize Guo (The Institute of North Electronic Equipment, China), Tao Wang (Ordnance Engineering College, China), Zhijie Shi (University of Connecticut, USA)

COSADE 2013 *Fault Analysis Attack session*

10:50 11:15	***coffee break***
	session 2: Fault Analysis Attack ***Session chair: Alexandre Berzatti*** **Defeating with Fault Injection a Combined Attack Resistant Exponentiation** Benoît Feix (XLIM, Limoges University / Inside Secure, France), Alexandre Venelli (Inside Secure, France).
11:15 12:30	**Fault Attacks on Projective-to-Affine Coordinates Conversion** Diana Maimut (École Normale Supérieure), Cédric Murdica (Secure-IC, Télécom ParisTech), David Naccache (Ecole Normale Supérieure), Mehdi Tibouchi (NTT Secure Platform Laboratories). **Improved Algebraic Fault Analysis: A Case Study on Piccolo and Applications to Other Lightweight Block Ciphers** Fan Zhang (University of Connecticut, USA), Xinjie Zhao (Ordnance Engineering College, China, and The Institute of North Electronic Equipment), Shize Guo (The Institute of North Electronic Equipment, China), Tao Wang (Ordnance Engineering College, China), Zhijie Shi (University of Connecticut, USA)

Ecole Nationale Supérieure des Mines SAINT-ETIENNE cea gemalto

COSADE 2013 P

		Fault Model		
		Large Faults Section 4	Two Faults Section 5	Known Fault Section 6
ECSM	Double-and-Add	×	×	×
	Double-and-Add always	×	×	×
	Signed Digit method	×	×	×
	Sliding Window	×	×	×
	Signed Sliding Window	×	×	×
	Montgomery Ladder	✓	✓	✓
	co-Z Montgomery Ladder	×	×	×
Countermeasures	Random Projective Coordinates *before* the ECSM	✓	✓	×
	Random Projective Coordinates *after* the ECSM	✓	✓	✓
	Random Curve Isomorphism	✓	✓	×
	Scalar Randomization	✓	✓	×
	Point Blinding	✓	✓	✓
	Point Verification *before* the conversion	×	×	×
	Point Verification *after* the conversion	✓	✓	✓

Table 2. Synthesis of the attacks

10:50 11:15 *coffee break*

session 2: Fault Analysis Attack

Session chair: Alexandre Berzatti

Defeating with Fault Injection a Combined A
Benoît Feix (XLIM, Limoges University / Insi
(Inside Secure, France).

11:15 12:30 **Fault Attacks on Projective-to-Affine Coordinates Conversion**
Diana Maimut (École Normale Supérieure), Cédric Murdica (Secure-IC, Télécom ParisTech), David Naccache (Ecole Normale Supérieure), Mehdi Tibouchi (NTT Secure Platform Laboratories).

Improved Algebraic Fault Analysis: A Case Study on Piccolo and Applications to Other Lightweight Block Ciphers
Fan Zhang (University of Connecticut, USA), Xinjie Zhao (Ordnance Engineering College, China, and The Institute of North Electronic Equipment), Shize Guo (The Institute of North Electronic Equipment, China), Tao Wang (Ordnance Engineering College, China), Zhijie Shi (University of Connecticut, USA)

Ecole Nationale Supérieure des Mines SAINT-ETIENNE cea gemalto

COSADE 2013 P

		Fault Model		
		Large Faults Section 4	Two Faults Section 5	Known Fault Section 6
ECSM	Double-and-Add	×	×	×
	Double-and-Add always	×	×	×
	Signed Digit method	×	×	×
	Sliding Window	×	×	×
	Signed Sliding Window	×	×	×
	Montgomery Ladder	✓	✓	✓
	co-Z Montgomery Ladder	×	×	×
Countermeasures	Random Projective Coordinates *before* the ECSM	✓	✓	×
	Random Projective Coordinates *after* the ECSM	✓	✓	✓
	Random Curve Isomorphism	✓	✓	×
	Scalar Randomization	✓	✓	×
	Point Blinding	✓	✓	✓
	Point Verification *before* the conversion	×	×	×
	Point Verification *after* the conversion	✓	✓	✓

Table 2. Synthesis of the attacks

10:50 11:15 ***coffee break***

session 2: Fault Analysis Attack

Session chair: Alexandre Berzatti

Defeating with Fault Injection a Combined A
Benoît Feix (XLIM, Limoges University / Insi
(Inside Secure, France).

11:15 12:30 **Fault Attacks on Projective-to-Affine Coordinates Conversion**
Diana Maimut (École Normale Supérieure), Cédric Murdica (Secure-IC, Télécom ParisTech), David Naccache (Ecole Normale Supérieure), Mehdi Tibouchi (NTT Secure Platform Laboratories).

Improved Algebraic Fault Analysis: A Case Study on Piccolo and Applications to Other Lightweight Block Ciphers
Fan Zhang (University of Connecticut, USA), Xinjie Zhao (Ordnance Engineering College, China, and The Institute of North Electronic Equipment), Shize Guo (The Institute of North Electronic Equipment, China), Tao Wang (Ordnance Engineering College, China), Zhijie Shi (University of Connecticut, USA)

Ecole Nationale Supérieure des Mines SAINT-ETIENNE cea gemalto

COSADE 2013 P

		Fault Model		
		Large Faults Section 4	Two Faults Section 5	Known Fault Section 6
ECSM	Double-and-Add	×	×	×
	Double-and-Add always	×	×	×
	Signed Digit method	×	×	×
	Sliding Window	×	×	×
	Signed Sliding Window	×	×	×
	Montgomery Ladder	✓	✓	✓
	co-Z Montgomery Ladder	×	×	×
Countermeasures	Random Projective Coordinates *before* the ECSM	✓	✓	×
	Random Projective Coordinates *after* the ECSM	✓	✓	✓
	Random Curve Isomorphism	✓	✓	×
	Scalar Randomization	✓	✓	×
	Point Blinding	✓	✓	✓
	Point Verification *before* the conversion	×	×	×
	Point Verification *after* the conversion	✓	✓	✓

Table 2. Synthesis of the attacks

10:50 11:15 ***coffee break***

session 2: Fault Analysis Attack

Session chair: Alexandre Berzatti

Defeating with Fault Injection a Combined A
Benoît Feix (XLIM, Limoges University / Insi
(Inside Secure, France).

11:15 12:30 **Fault Attacks on Projective-to-Affine Coordinates Conversion**
Diana Maimut (École Normale Supérieure), Cédric Murdica (Secure-IC, Télécom ParisTech), David Naccache (Ecole Normale Supérieure), Mehdi Tibouchi (NTT Secure Platform Laboratories).

Improved Algebraic Fault Analysis: A Case Study on Piccolo and Applications to Other Lightweight Block Ciphers
Fan Zhang (University of Connecticut, USA), Xinjie Zhao (Ordnance Engineering College, China, and The Institute of North Electronic Equipment), Shize Guo (The Institute of North Electronic Equipment, China), Tao Wang (Ordnance Engineering College, China), Zhijie Shi (University of Connecticut, USA)

Ecole Nationale Supérieure des Mines SAINT-ETIENNE cea gemalto

COSADE 2013 F

		Fault Model		
		Large Faults Section 4	Two Faults Section 5	Known Fault Section 6
ECSM	Double-and-Add	×	×	×
	Double-and-Add always	×	×	×
	Signed Digit method	×	×	×
	Sliding Window	×	×	×
	Signed Sliding Window	×	×	×
	Montgomery Ladder	✓	✓	✓
	co-Z Montgomery Ladder	×	×	×
Countermeasures	Random Projective Coordinates *before* the ECSM	✓	✓	×
	Random Projective Coordinates *after* the ECSM	✓	✓	✓
	Random Curve Isomorphism	✓	✓	×
	Scalar Randomization	✓	✓	×
	Point Blinding	✓	✓	✓
	Point Verification *before* the conversion	×	×	×
	Point Verification *after* the conversion	✓	✓	✓

Table 2. Synthesis of the attacks

10:50 11:15 *coffee break*

session 2: Fault Analysis Attack

Session chair: Alexandre Berzatti

Defeating with Fault Injection a Combined A
Benoît Feix (XLIM, Limoges University / Insi
(Inside Secure, France).

11:15 12:30 **Fault Attacks on Projective-to-Affine**
Diana Maimut (École Normale Supéri
ParisTech), David Naccache (Ecole N
Secure Platform Laboratories).

Improved Algebraic Fault Analysis: A
Other Lightweight Block Ciphers
Fan Zhang (University of Connecticut
College, China, and The Institute of N
Institute of North Electronic Equipme
College, China), Zhijie Shi (University o

3 Fault Model

The fault model assumed for AFA on Piccolo in this paper is described as follows.

- The adversary can choose the plaintext to be encrypted and obtain the corresponding correct and faulty ciphertext.
- The adversary can inject a fault. So one of the nibbles at the input of F functions in the 23rd round is wrong, as shown in Fig. 3. In Section 6, this assumption can be further weaken when extending our AFA to more rounds.
- The adversary knows the fault position but does not know the exact location nor the value of faults. In other words, he can specify which round to inject the faults, but has no control either on which byte or nibble to be altered, nor on the values.

Ecole Nationale Supérieure des Mines SAINT-ETIENNE cea gemalto

COSADE 2013 F

		Fault Model		
		Large Faults Section 4	Two Faults Section 5	Known Fault Section 6
ECSM	Double-and-Add	×	×	×
	Double-and-Add always	×	×	×
	Signed Digit method	×	×	×
	Sliding Window	×	×	×
	Signed Sliding Window	×	×	×
	Montgomery Ladder	✓	✓	✓
	co-Z Montgomery Ladder	×	×	×
Countermeasures	Random Projective Coordinates *before* the ECSM	✓	✓	×
	Random Projective Coordinates *after* the ECSM	✓	✓	✓
	Random Curve Isomorphism	✓	✓	×
	Scalar Randomization	✓	✓	×
	Point Blinding	✓	✓	✓
	Point Verification *before* the conversion	×	×	×
	Point Verification *after* the conversion	✓	✓	✓

Table 2. Synthesis of the attacks

10:50 11:15 *coffee break*

session 2: Fault Analysis Attack

Session chair: Alexandre Berzatti

Defeating with Fault Injection a Combined A
Benoît Feix (XLIM, Limoges University / Insi
(Inside Secure, France).

11:15 12:30 **Fault Attacks on Projective-to-Affine**
Diana Maimut (École Normale Supéri
ParisTech), David Naccache (Ecole N
Secure Platform Laboratories).

Improved Algebraic Fault Analysis: A
Other Lightweight Block Ciphers
Fan Zhang (University of Connecticut
College, China, and The Institute of N
Institute of North Electronic Equipme
College, China), Zhijie Shi (University o

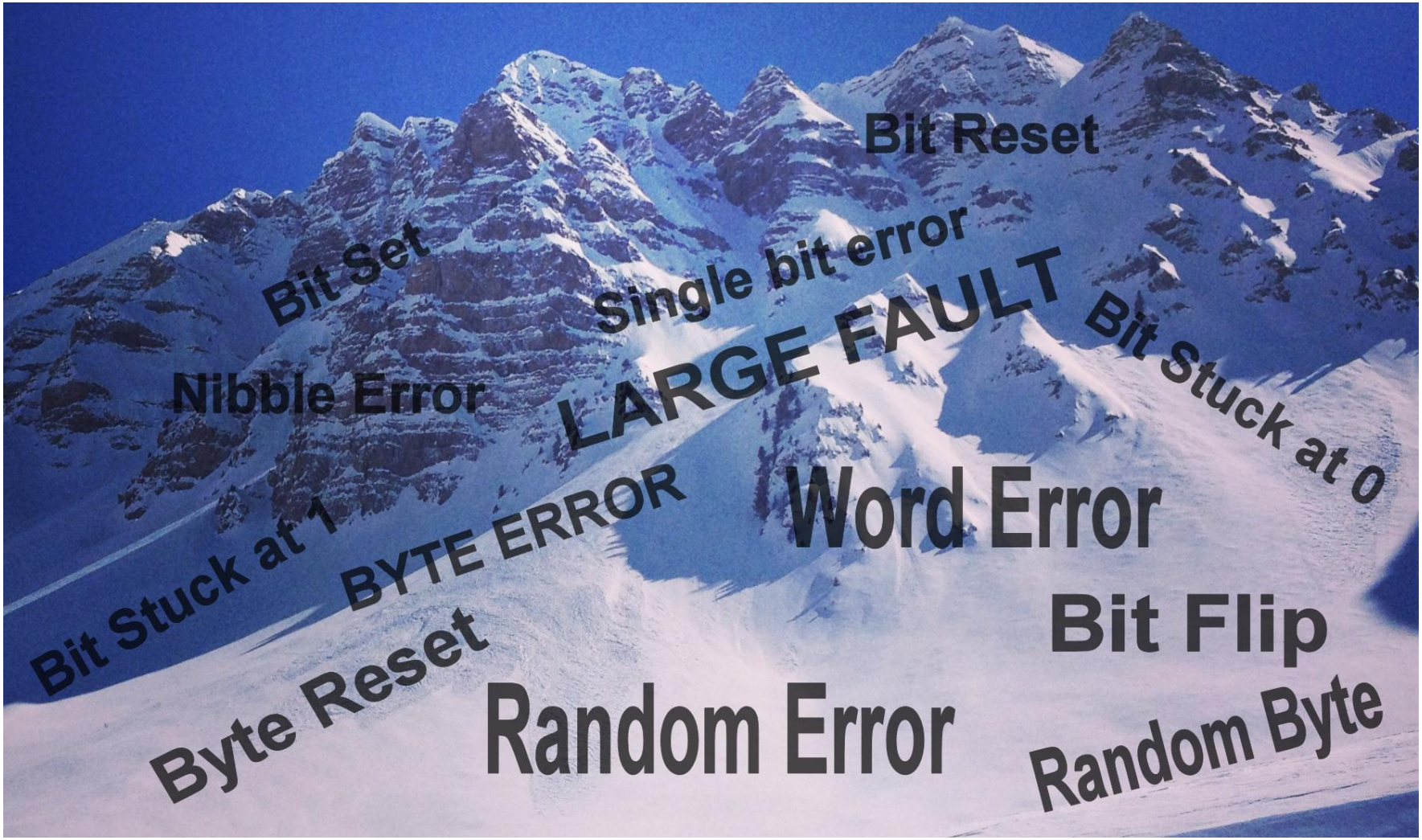
3 Fault Model

The fault model assumed for AFA on Piccolo in this paper is described as follows.

- The adversary can choose the plaintext to be encrypted and obtain the corresponding correct and faulty ciphertext.
- The adversary can inject a fault. So one of the nibbles at the input of F functions in the 23rd round is wrong, as shown in Fig. 3. In Section 6, this assumption can be further weaken when extending our AFA to more rounds.
- The adversary knows the fault position but does not know the exact location nor the value of faults. In other words, he can specify which round to inject the faults, but has no control either on which byte or nibble to be altered, nor on the values.

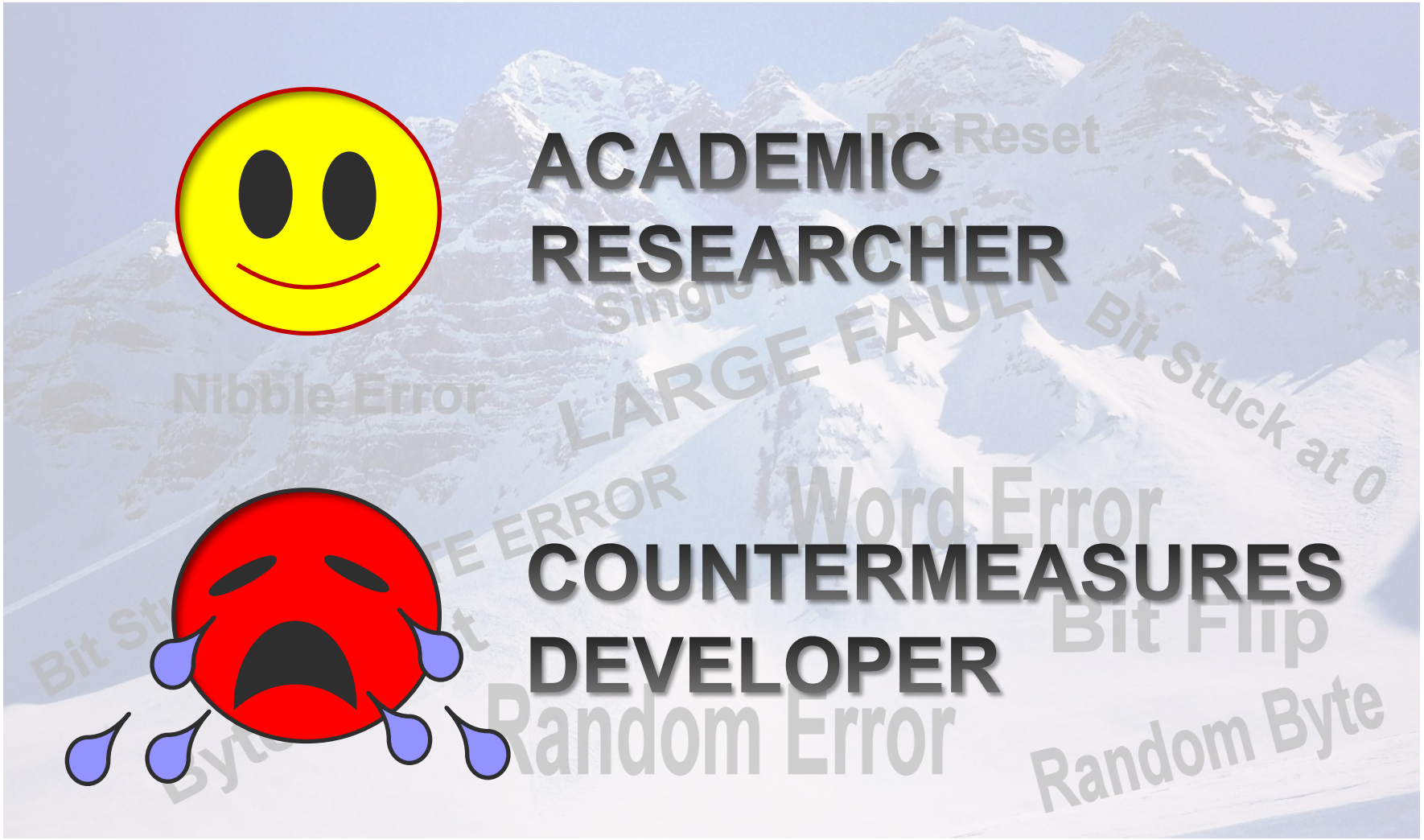
Ecole Nationale Supérieure des Mines SAINT-ETIENNE cea gemalto

Fault Models in real life



Ecole Nationale Supérieure des Mines SAINT-ETIENNE cea gemalto

Fault Models in real life



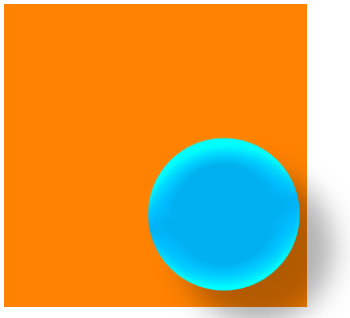
AGENDA

- Trends and Motivations
- Equipment & Technology
- Results
- Laser fault correlation with physical transistors implementation
- Results summary and conclusion

Trends and Motivations

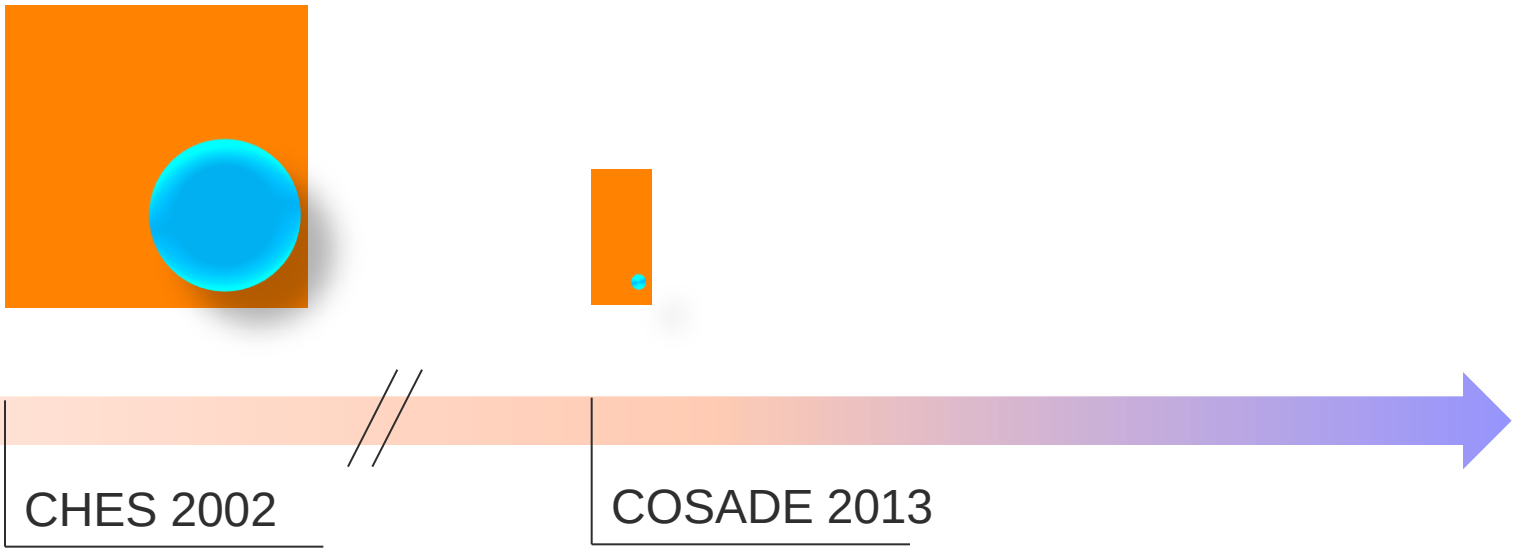
Optical Fault Injection trends

	Skorobogatov
Techno node	*1200nm*
SRAM cell size	*~20µmx20µm (6T)*
Spot size	*~10µm*



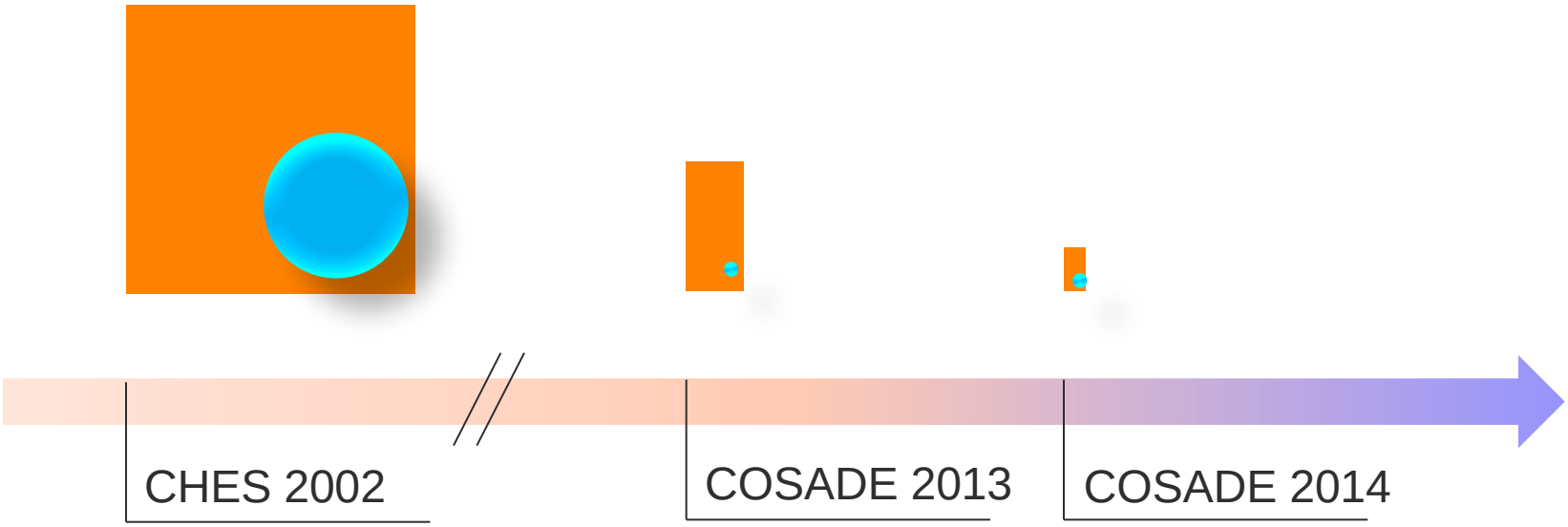
Optical Fault Injection trends

	Skorobogatov	Roscian & Al.
Techno node	*1200nm*	*250nm*
SRAM cell size	*~20µmx20µm (6T)*	*9µmx4µm (5T)*
Spot size	*~10µm*	*~1µm*



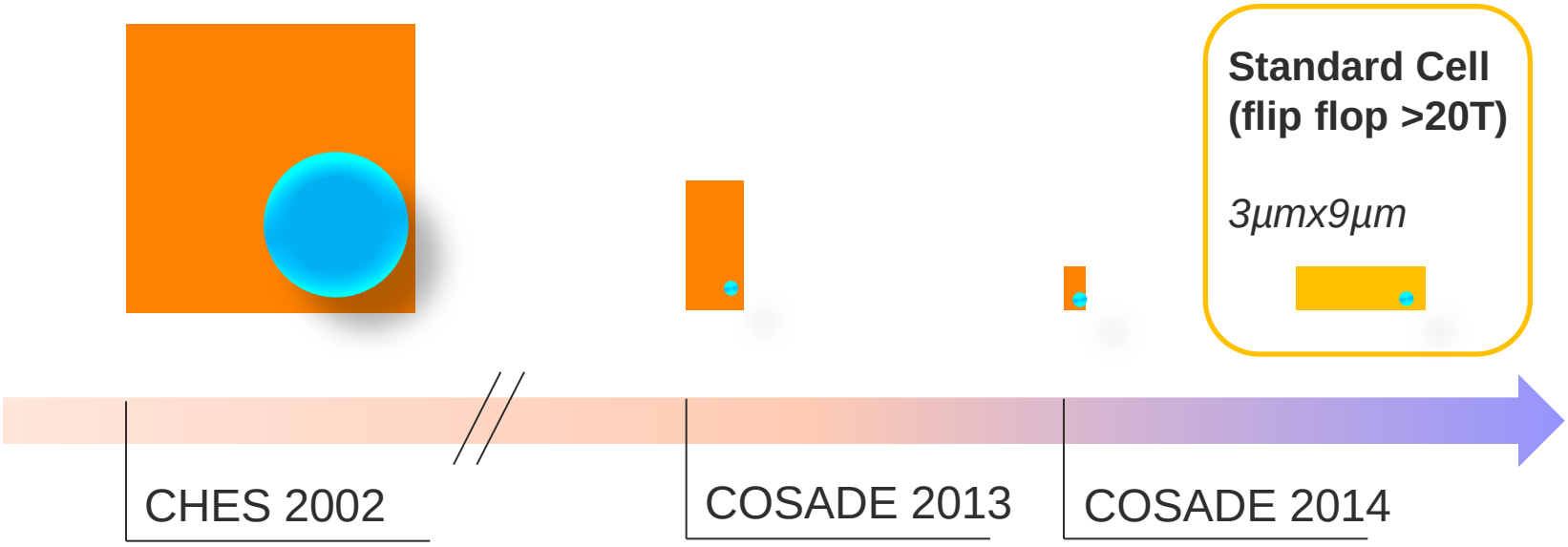
Optical Fault Injection trends

	Skorobogatov	Roscian & Al.	
Techno node	*1200nm*	*250nm*	*90nm*
SRAM cell size	*~20µmx20µm (6T)*	*9µmx4µm (5T)*	*3µmx1.5µm (6T)*
Spot size	*~10µm*	*~1µm*	*~1µm*

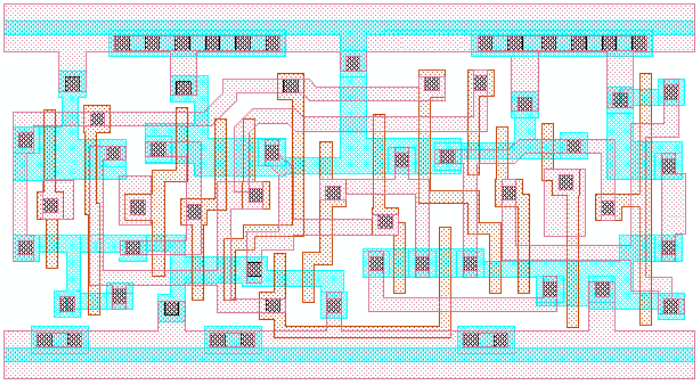


Optical Fault Injection trends

	Skorobogatov	Roscian & Al.	
Techno node	*1200nm*	*250nm*	*90nm*
SRAM cell size	*~20µmx20µm (6T)*	*9µmx4µm (5T)*	*3µmx1.5µm (6T)*
Spot size	*~10µm*	*~1µm*	*~1µm*

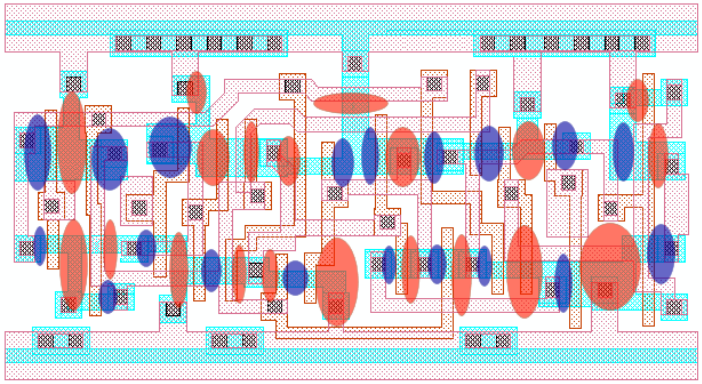


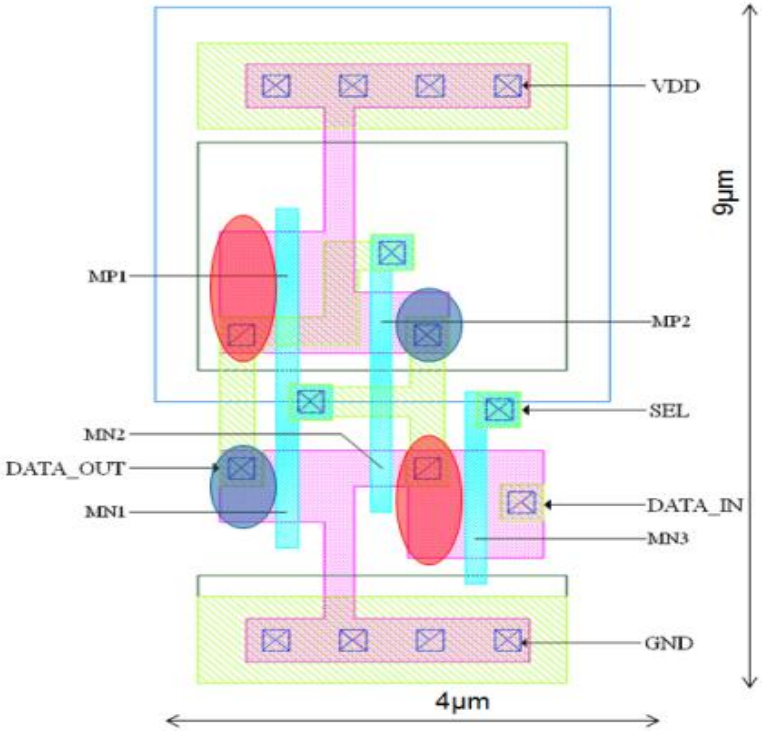
Motivations



- We target:
  - The synthesized logic of a recent technology chip (*90nm*)
  - A gate with a large number of transistors (>20T)
  - A standard cell critical for security, flip flop gate
    - Key & data registers, internal coprocessor states

Motivations





Courtesy of Roscian & Al.

- We target:
  - The synthesized logic of a recent technology chip (*90nm*)
  - A gate with a large number of transistors (>20T)
  - A standard cell critical for security, flip flop gate
    - Key & data registers, internal coprocessor states
- Extented numbers of theoretical sensitivity zones, complex simulation

Fault model?

Ecole Nationale Supérieure des Mines SAINT-ETIENNE cea gemalto

Equipment and technology

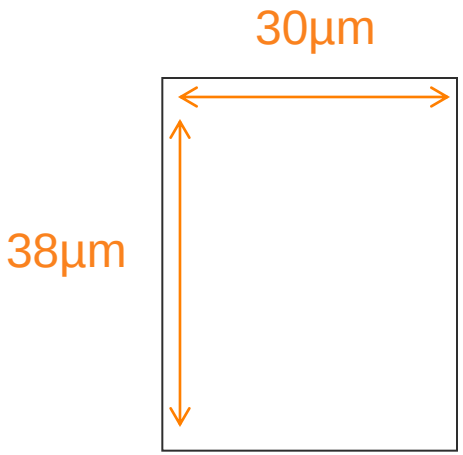
Flexible laser platform

- **Wavelength:** 1064nm
- **Spot size:** About 1µm
- **Energy :** Dozens of nJ
- **Backside approach**
- **50x objective**
- **3-Axis stage** with submicrometer resolution

Device under test and scenario

- Techno node: 90nm
- Open sample
  - Write/read register
  - 8 bits
- “Static” perturbation of registers
  - No timing considerations
- After a global chip scanning with a large spot size and scan step, the register area is found
- Laser parameters are adapted to get a maximum of generated photo-current and a single gate effect
- Experiments performed on a restricted area
  - 1µm step

1. Load data register
2. Perform laser shot
3. Read back register value



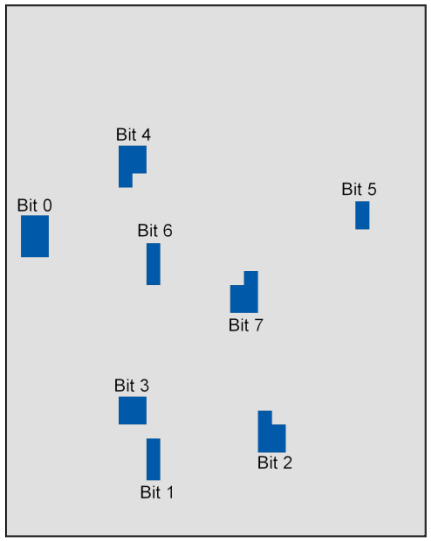
Results

Forcing bits vs. laser spot location

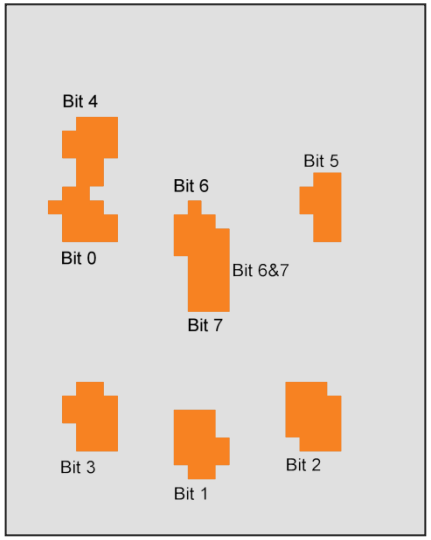
- Blue: ‘0’ to ‘1’ sensitive position, bit-set area
- Orange: ‘1’ to ‘0’ sensitive position, bit-reset area
- Gray: No effect

30µm

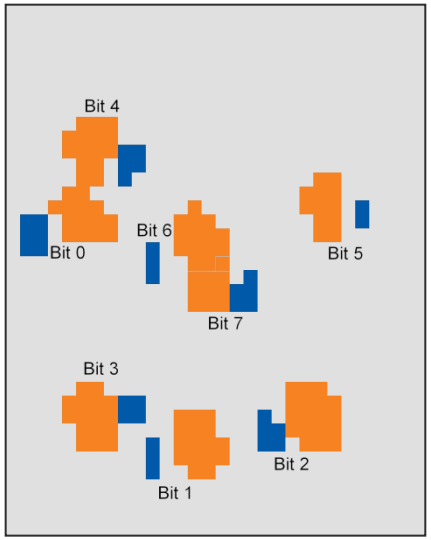
Init at **“0000 0000”**



Init at **“1111 1111”**



Both mapping



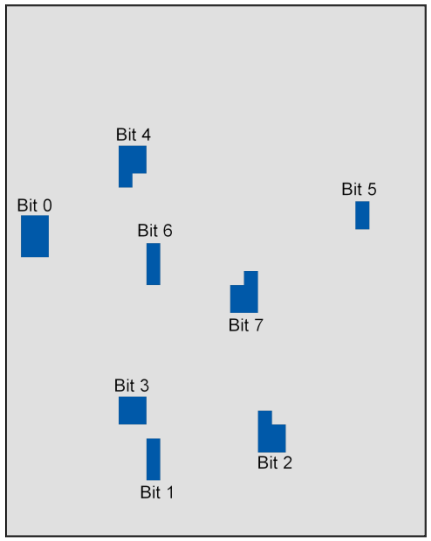
38µm

Forcing bits vs. laser spot location

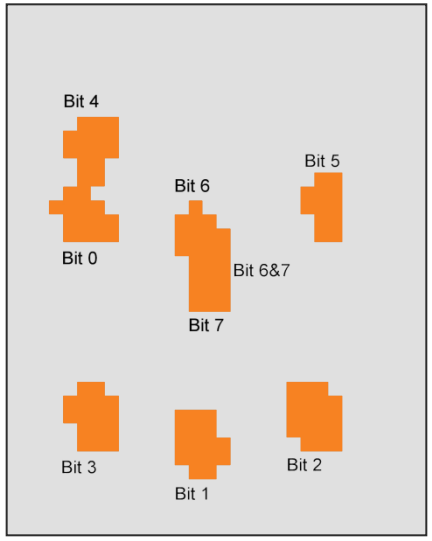
- Blue: ‘0’ to ‘1’ sensitive position, bit-set
- Orange: ‘1’ to ‘0’ sensitive position, bit-reset
- Gray: No effect

30µm

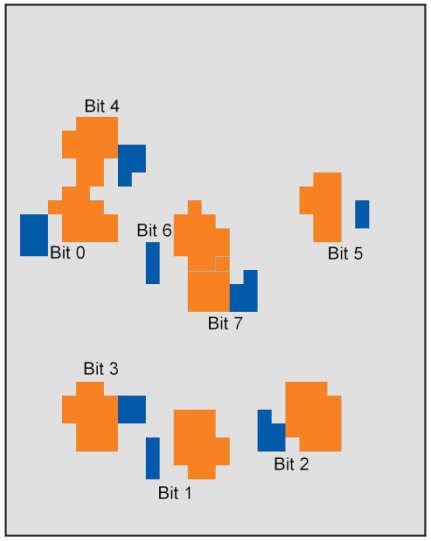
Init at **“0000 0000”**



Init at **“1111 1111”**



Both mapping



38µm

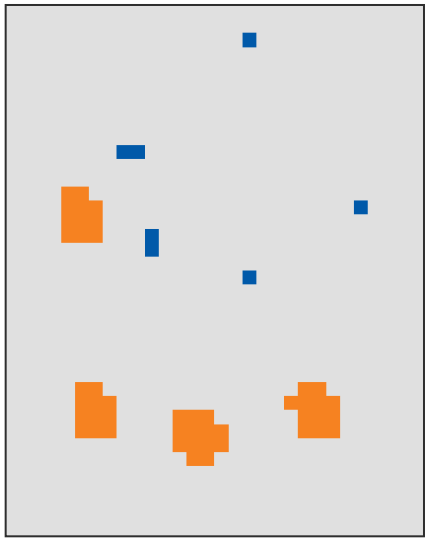
- One shot over one position forces a bit to one distinct value

Ecole Nationale Supérieure des Mines SAINT-ETIENNE cea gemalto

Forcing bits by laser energy level

- Blue: ‘0’ to ‘1’ sensitive position
- Orange: ‘1’ to ‘0’ sensitive position
- Gray: No effect
- Register initialized at ‘**00001111**’

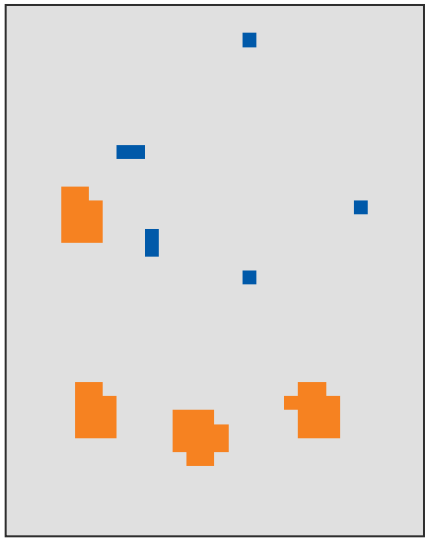
32nJ



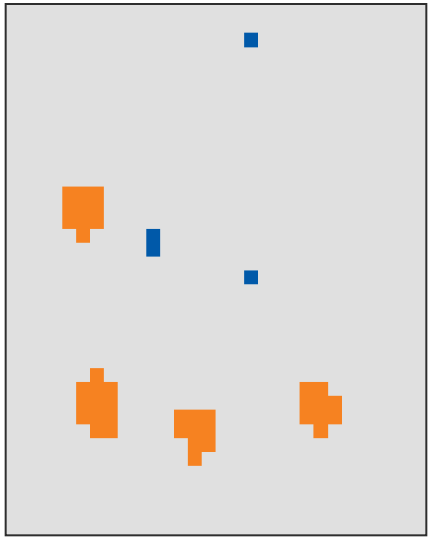
Forcing bits by laser energy level

- Blue: ‘0’ to ‘1’ sensitive position
- Orange: ‘1’ to ‘0’ sensitive position
- Gray: No effect
- Register initialized at ‘**00001111**’

32nJ



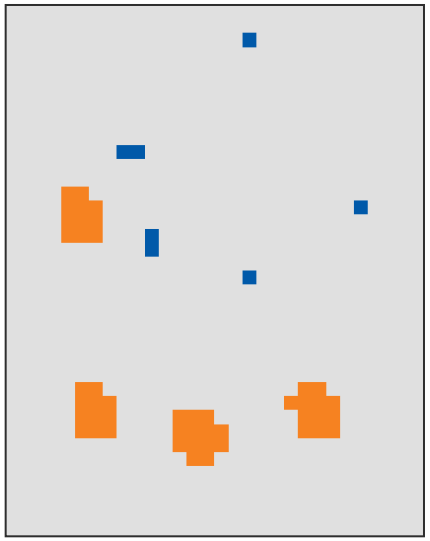
13nJ



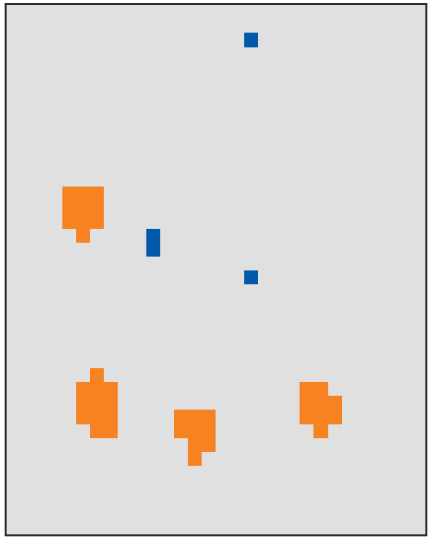
Forcing bits by laser energy level

- Blue: ‘0’ to ‘1’ sensitive position
- Orange: ‘1’ to ‘0’ sensitive position
- Gray: No effect
- Register initialized at ‘**00001111**’

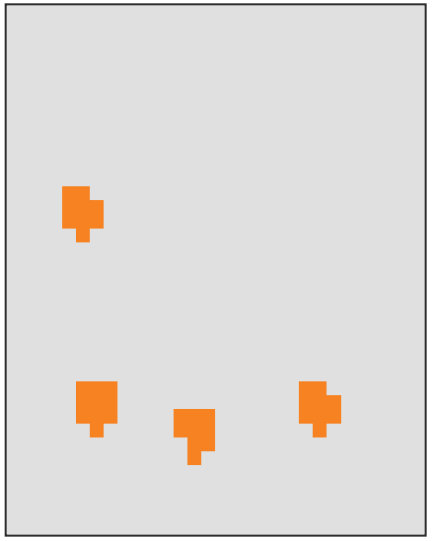
32nJ



13nJ



10nJ

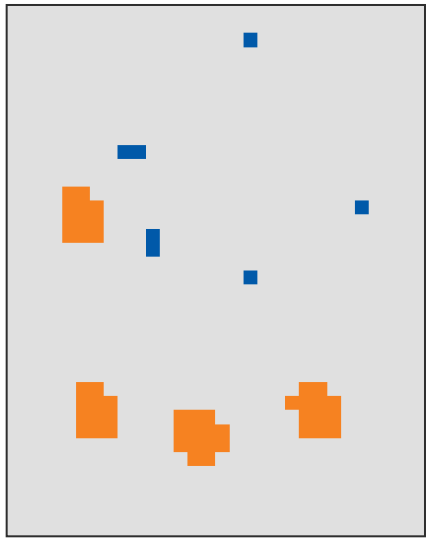


Ecole Nationale Supérieure des Mines SAINT-ETIENNE cea gemalto

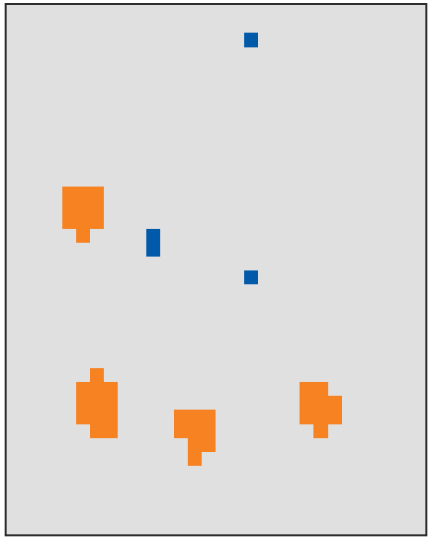
Forcing bits by laser energy level

- Blue: ‘0’ to ‘1’ sensitive position
- Orange: ‘1’ to ‘0’ sensitive position
- Gray: No effect
- Register initialized at ‘**00001111**’

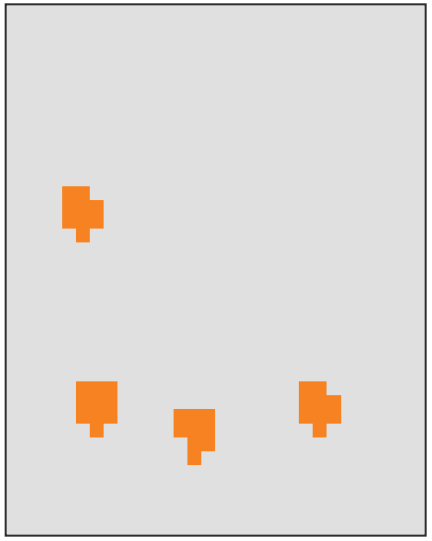
32nJ



13nJ



10nJ



- With a fine tuned energy, only ‘1’ to ‘0’ transitions are possible
- Targeting the zone with this energy leads to clear the register

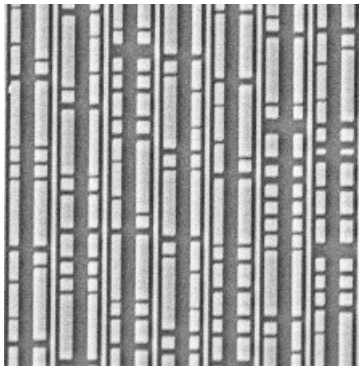
Laser fault correlation with physical transistors implementation

Getting physical transistors implementation

- As the laser effects are linked to the underlying hardware implementation

- Invasive approach to retrieve transistors/gate location

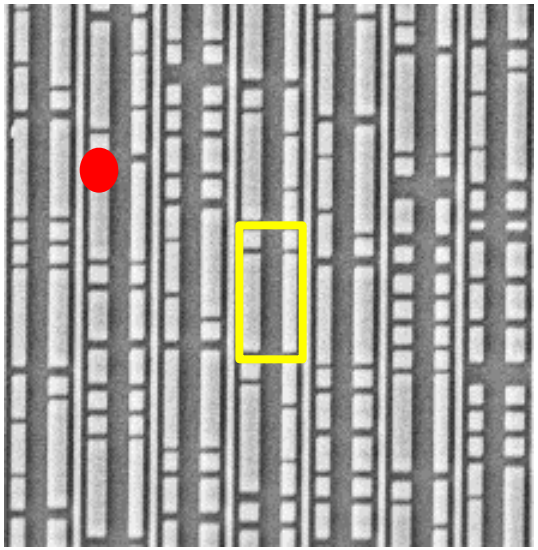
- We get the transistors' wells location



Highlighting laser and physical parameters

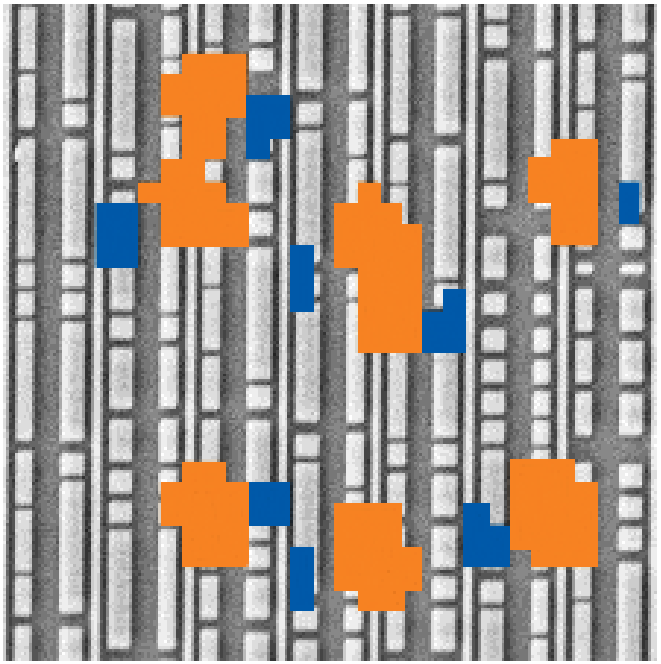
- PMOS and NMOS columns are highlighted
  - p-wells are larger than n-wells

- Gate and spot area are also given



Fault correlation with transistors implementation

- We overlay the fault mapping and the SEM image

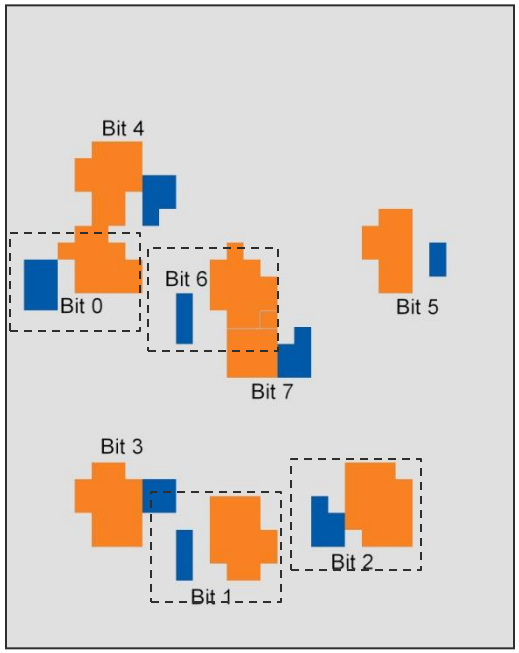


- ‘1 to 0’ transitions are present over NMOS transistors
- ‘0 to 1’ transitions are present over PMOS transistors

More information can be obtained…

- PMOS/NMOS laser sensitivity difference

- Gates orientation
  - Half of the bits have their bit-set sensitive part on the left of the bit-reset sensitive part



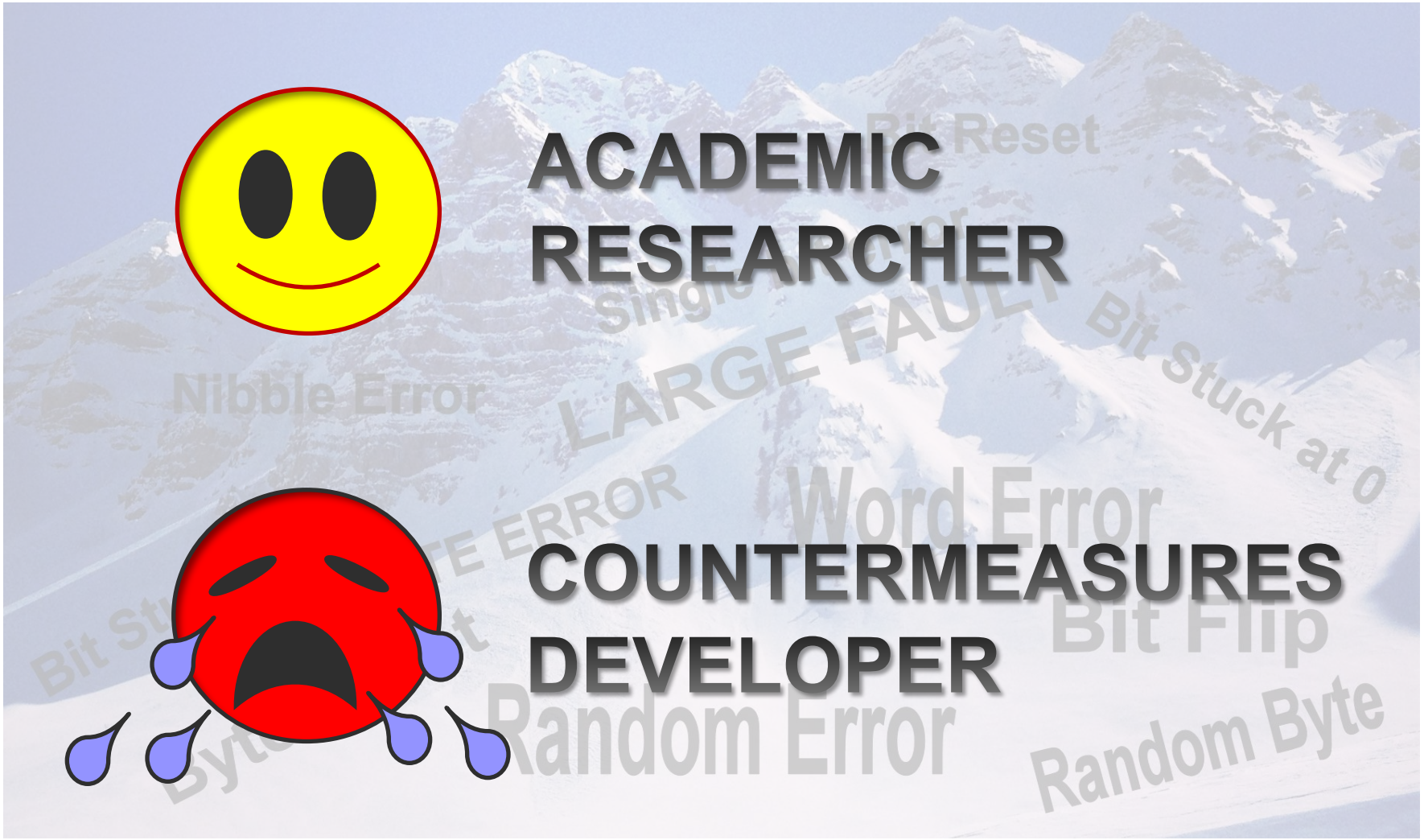
It can help for reverse engineering

Conclusion & Future work

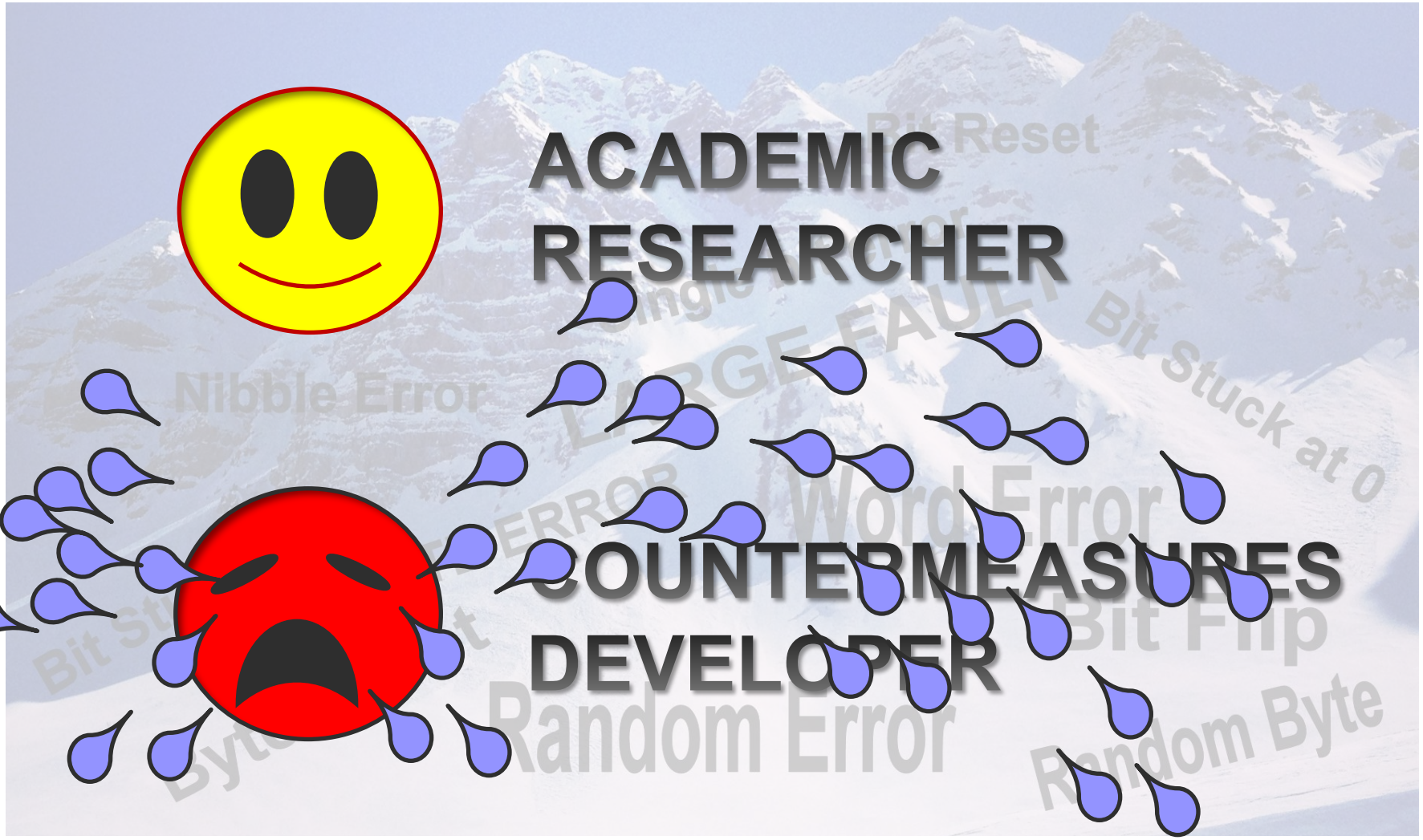
Conclusion

- By adjusting laser location or energy level we can control with a 100% success rate bit values in a - 90nm - register
- Our results shown a direct dependancy between fault model injection and gate implementation
- Single bit set and single bit reset must be considered for any attack

Fault Models in real life



Fault Models in real life

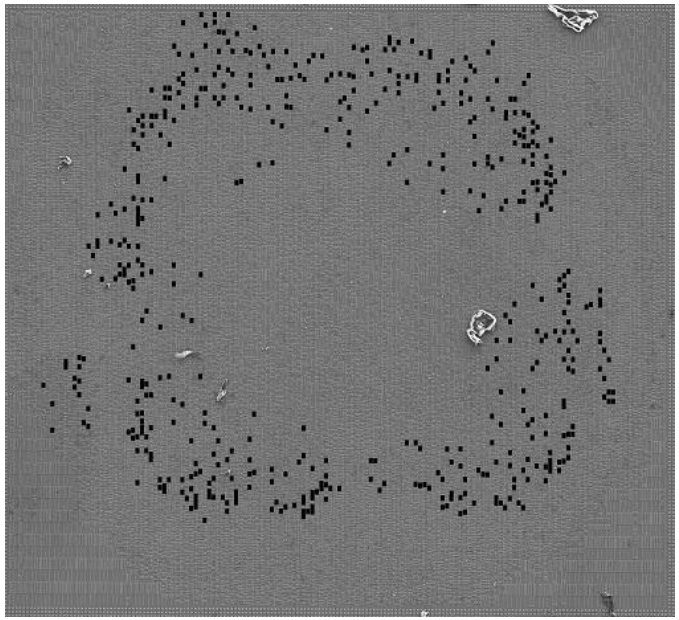


Next step

- How to find registers over the chip?
  - Poster paper to appear in the proceedings of HOST 2014:

"Increasing the efficiency of laser fault injections using fast gate level reverse engineering"

by Franck Courbon, Philippe Loubet-Moundi, Jacques Fournier and Assia Tria



Thank you for your attention