Security on Plastics: Fake or Real?

Nele Mentens
KU Leuven, imec-COSIC/ESAT

Joint work with Jan Genoe, Thomas Vandenabeele, Lynn Verschueren, Dirk Smets, Wim Dehaene, Kris Myny
KU Leuven & IMEC

CROSSING conference
September 9, 2019, Darmstadt, Germany

Outline

- Flexible electronics on plastics
- Challenge #1: crypto core on plastics
- Challenge #2: key hiding
- Remaining challenges
- Conclusion

Flexible electronics on plastics
Displays

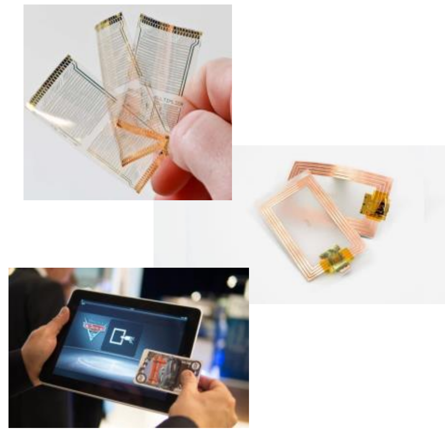
- Widespread commercial use in flexible displays
- Millions of thin-film transistors controlling the pixels

Flexible electronics on plastics
Digital circuits

- Large potential for flexible digital circuits in (passive) RFID/NFC chips, integrated in paper or plastics
- Examples:
  - Flexible labels
  - Intelligent packages
  - Smart blisters
  - Electronic medical patches

Flexible electronics on plastics
Digital circuits

- Circuits that have already been fabricated:
  - NFC transponder
  - 8-bit microprocessor with limited instruction set



Flexible electronics on plastics
Transistor technology

- Several thin-film transistor (TFT) technologies exist
  - Amorphous silicon TFTs
  - Low-temperature polycrystalline silicon TFTs
  - Organic TFTs
  - Amorphous metal-oxide TFTs
- Amorphous metal-oxide TFTs show the best combination of high performance and low processing cost
- a-IGZO (amorphous indium gallium zinc oxide) is used as a semiconductor

Flexible electronics on plastics
Comparison with silicon transistors

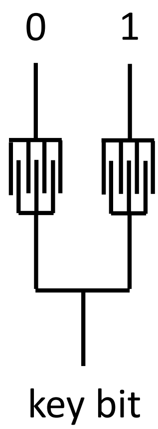
	silicon (10 nm)	a-IGZO (5 µm)		
Core supply voltage	0.7 V	5-10 V	→ ☹	Higher power consumption
Charge carrier mobility	500-1500 cm^2/Vs	2-20 cm^2/Vs	→ ☹	Lower performance
Transistor density	~ 45 mio per mm^2	10^3-10^4 per cm^2	→ ☹	Larger area
Semiconductor type	n-type and p-type	only n-type	→ ☹	Unipolar logic
Cost per 1000 transistors	> 0.3 USD	> 0.01 USD	→ ☺	Lower cost
Flexible?	no	yes	→ ☺	Bendable, stretchable

Flexible electronics on plastics
Non-volatile memory

- We need non-volatile memory to store values, such as cryptographic keys, after fabrication
- On plastic substrates, electrically readable/writable memory (e.g. flash) does not exist
- Two one-time programmable storage mechanisms are used:
  - Additive method: connect wires with conductive ink
  - Modificative method: cut wires with a laser

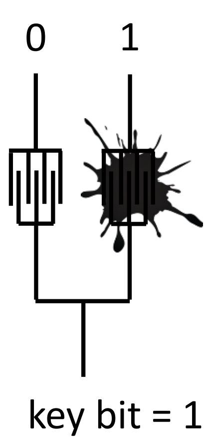
CROSSING, 2019, Darmstadt, Germany

Flexible electronics on plastics
Non-volatile memory



- Additive method:
  - Interdigitated finger structure
  - Connect wires with conductive ink

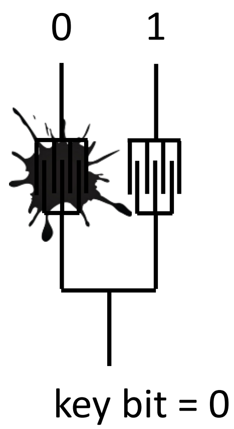
Flexible electronics on plastics
Non-volatile memory



- Additive method:
  - Interdigitated finger structure
  - Connect wires with conductive ink

Flexible electronics on plastics

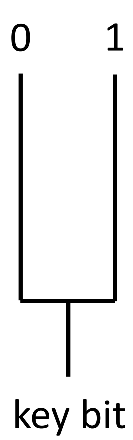
Non-volatile memory



- Additive method:
  - Interdigitated finger structure
  - Connect wires with conductive ink

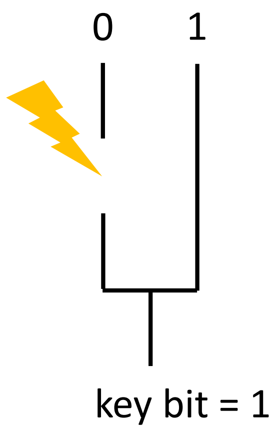
Flexible electronics on plastics

Non-volatile memory



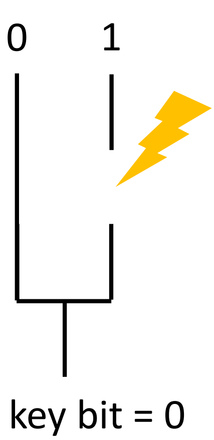
- Additive method:
  - Interdigitated finger structure
  - Connect wires with conductive ink
- Modificative method
  - Initial connection to 0 and 1
  - Cut wires with a laser

Flexible electronics on plastics
Non-volatile memory



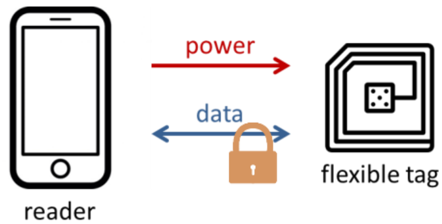
- Additive method:
  - Interdigitated finger structure
  - Connect wires with conductive ink
- Modificative method
  - Initial connection to 0 and 1
  - Cut wires with a laser

Flexible electronics on plastics
Non-volatile memory



- Additive method:
  - Interdigitated finger structure
  - Connect wires with conductive ink
- Modificative method
  - Initial connection to 0 and 1
  - Cut wires with a laser

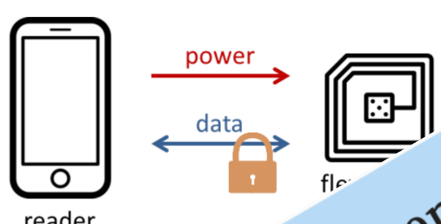
Flexible electronics on plastics
Security challenge



- To secure the communication between the flexible tag and the reader, many hurdles need to be overcome

- We concentrate on two challenges:
  - Challenge #1: integrate crypto cores in the flexible chip
    - The number of transistors in crypto cores exceed the number of transistors in flexible chips reported up to now
  - Challenge #2: prevent the key bits from being read out
    - The chips are not packaged and the features are relatively large
    - There is no electrically readable/writable memory

Flexible electronics on plastics
Security challenge



SEPTEMBER 9 - 10, 2019
CROSSING Conference on ~~Sustainable~~ Disposable Security & Privacy

CROSSING, 2019, Darmstadt, Germany

Challenge #1: crypto core on plastics
Design choices

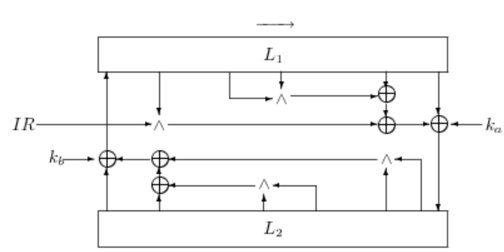
algorithm
architecture
gate
transistor

Challenge #1: crypto core on plastics
Design choices

algorithm
architecture
gate
transistor

KTANTAN32 [1]

- Block size: 32 bits
- Key size: 80 bits
- Fixed key, burnt into the device



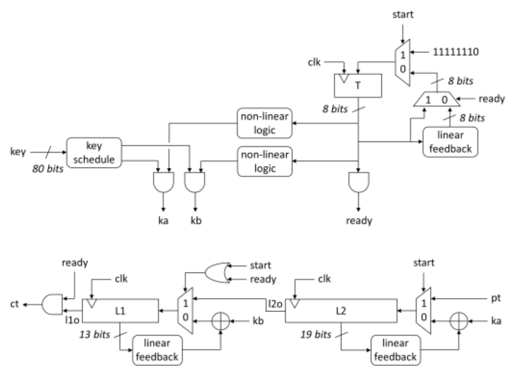
[1] C. De Cannière, O. Dunkelman, M. Knežević, *KATAN and KTANTAN—a family of small and efficient hardware-oriented block ciphers*, CHES 2009, p. 272-288.

Challenge #1: crypto core on plastics
Design choices

- algorithm
- **architecture**
- gate
- transistor

Serial architecture

- Inputs: start, clk, pt
- Outputs: ready, ct

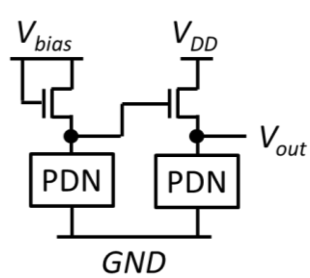


Challenge #1: crypto core on plastics
Design choices

- algorithm
- architecture
- **gate**
- transistor

pseudo-CMOS logic

- 6 TFTs in one NAND gate
- Pull-Down Network (PDN) repeated
- $V_{bias} > V_{DD} + 2V_T \rightarrow$ rail-to-rail output



Challenge #1: crypto core on plastics
Design choices

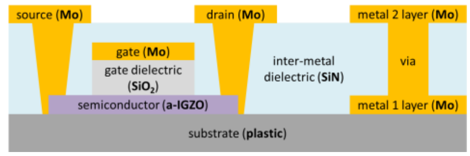
algorithm

architecture

gate

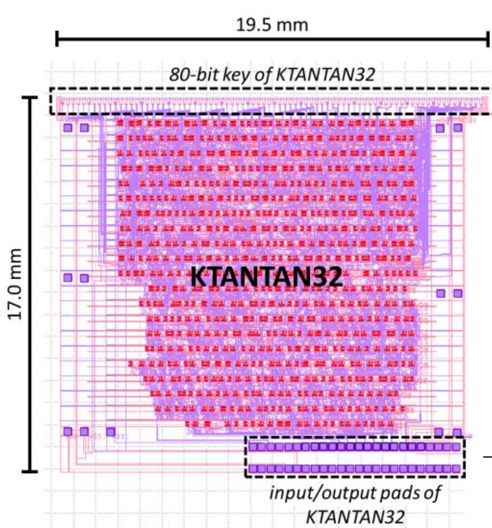
transistor

a-IGZO semiconductor



- Mo = molybdenum
- SiO_2 = silicon dioxide
- SiN = silicon nitride
- a-IGZO = amorphous indium gallium zinc oxide

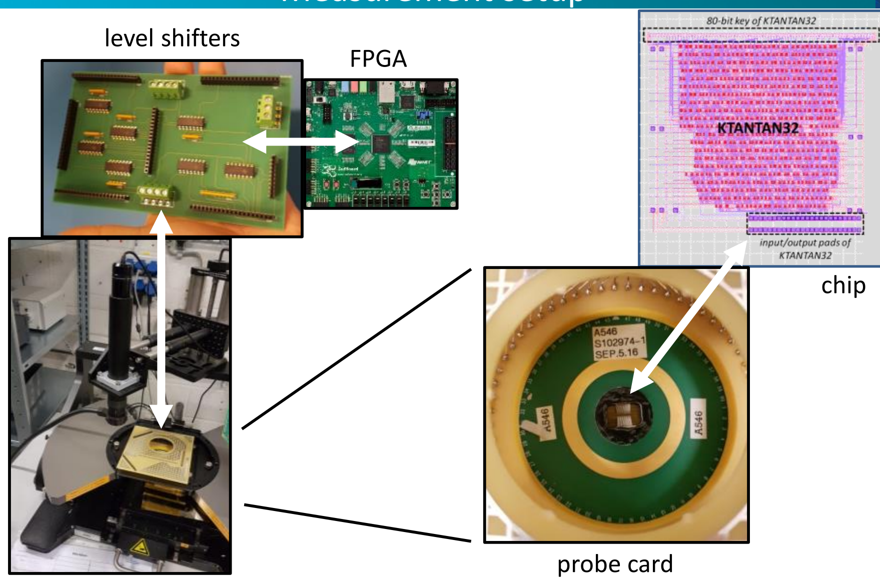
Challenge #1: crypto core on plastics
Layout



→ 48 pads for I/O, V_{DD}, V_{bias} and *GND*

- 4044 TFTs
- 331.5 mm²

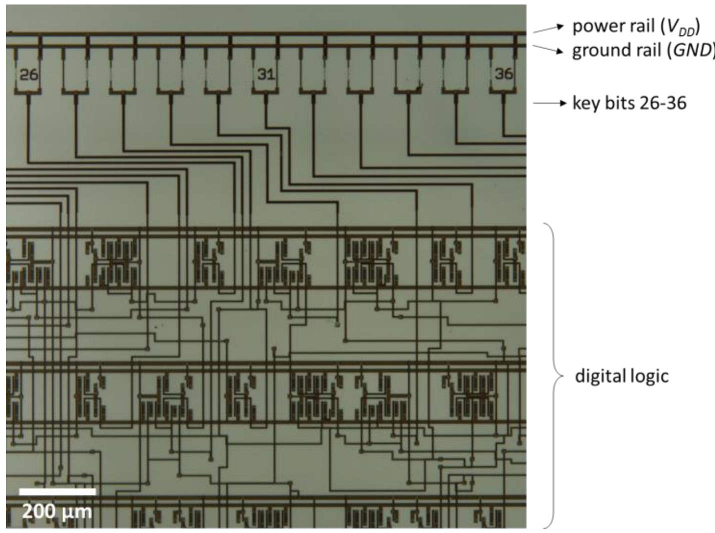
Challenge #1: crypto core on plastics
Measurement setup



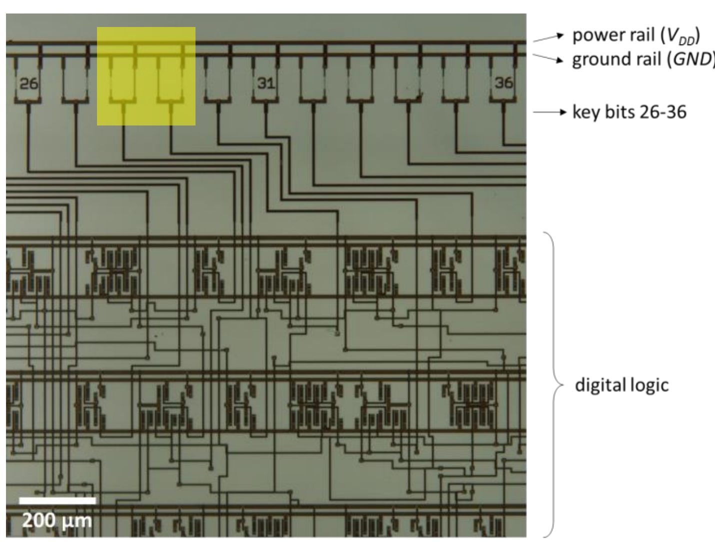
Challenge #1: crypto core on plastics
Measurement results

- Fixed 80-bit key: 07C1F07C1F07C1F07C1F (hex)
- 1000 plaintexts automatically applied
- 1000 correct ciphertexts for:
  - V_{DD} = 10 V and V_{bias} = 15 V
  - V_{DD} = 11 V and V_{bias} = 16.5 V
- Maximum clock frequency = 10 kHz
- Number of cycles:
  - 32 (for shifting in the plaintext)
  - 254 (for the actual encryption)
  - 32 (for shifting out the ciphertext)
- Total latency = 31.8 ms

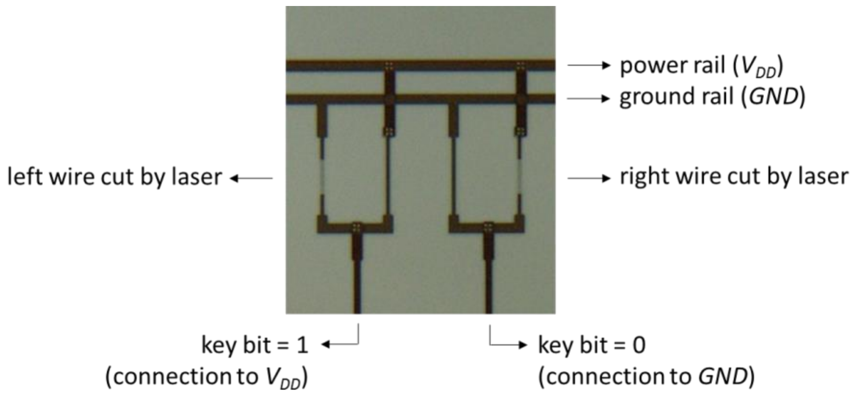
Challenge #1: crypto core on plastics
Key programming



Challenge #1: crypto core on plastics
Key programming

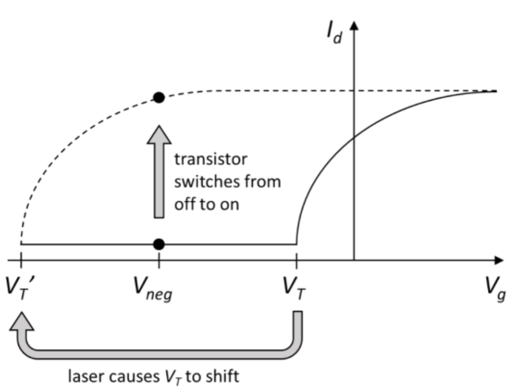


Challenge #1: crypto core on plastics
Key programming



PROBLEM: The key bits can easily be read out using a microscope

Challenge #2: key hiding
Proposed concept



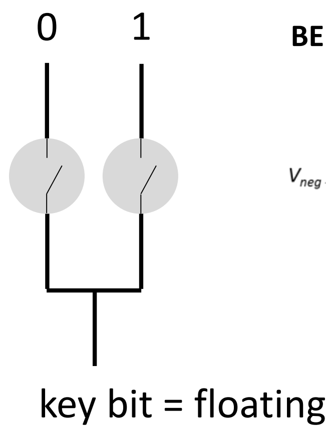
The temperature change caused by lasering, shifts the threshold voltage (V_T) and thus the I_d - V_g graph

↓

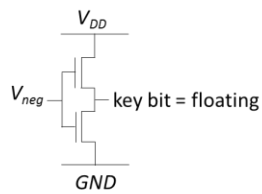
With a fixed input voltage (V_{neg}), the TFT switches from off to on

Challenge #2: key hiding
Proposed concept

FIRST OPTION



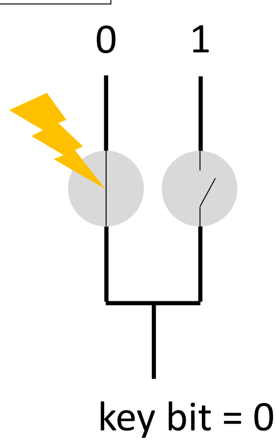
BEFORE LASERING



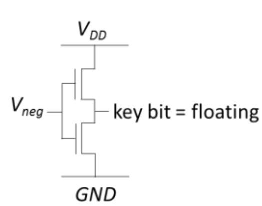
CROSSING, 2019, Darmstadt, Germany

Challenge #2: key hiding
Proposed concept

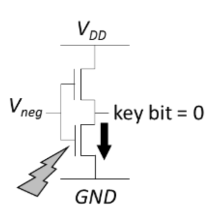
FIRST OPTION



BEFORE LASERING



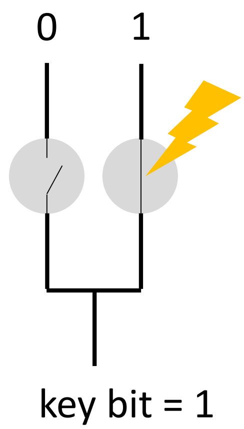
AFTER LASERING

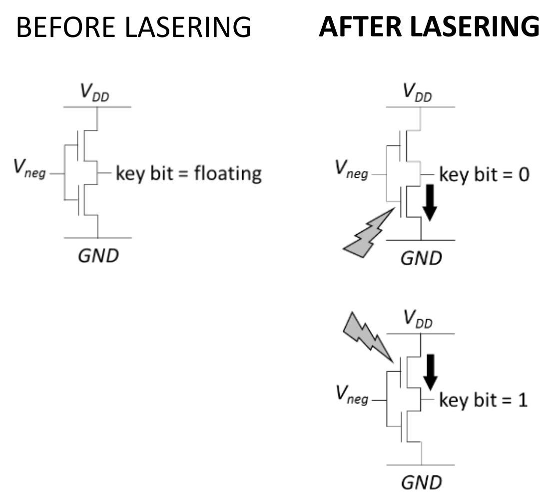


CROSSING, 2019, Darmstadt, Germany

Challenge #2: key hiding
Proposed concept

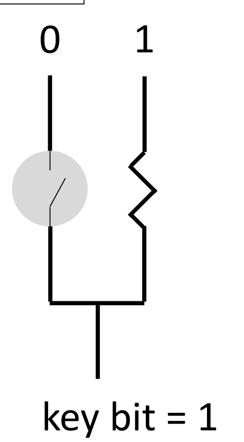
FIRST OPTION

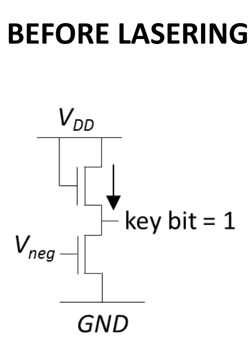




Challenge #2: key hiding
Proposed concept

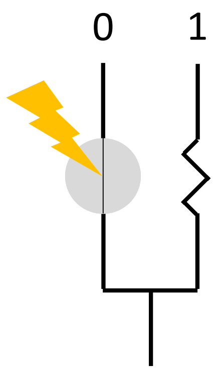
SECOND OPTION





Challenge #2: key hiding
Proposed concept

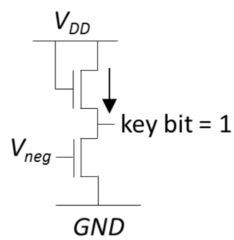
SECOND OPTION

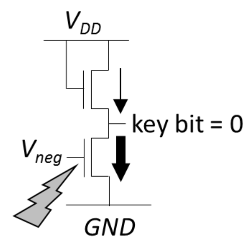


key bit = 0

BEFORE LASERING

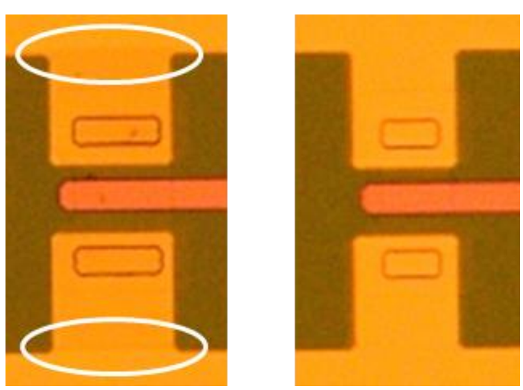
AFTER LASERING





Challenge #2: key hiding
Experimental validation

TFT microscope images



lasered not lasered

PROBLEM:

The difference is visible between a TFT that has been lasered and a TFT that has not been lasered

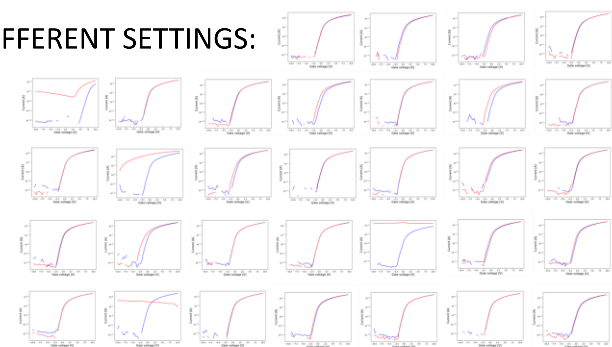
Challenge #2: key hiding
Experimental validation

SOLUTION:

Apply different settings of the laser to cause different V_T shifts that cannot be visually distinguished

EXPLORATION OF DIFFERENT SETTINGS:

- Blue:
  before lasering
- Red:
  after lasering



CROSSING, 2019, Darmstadt, Germany

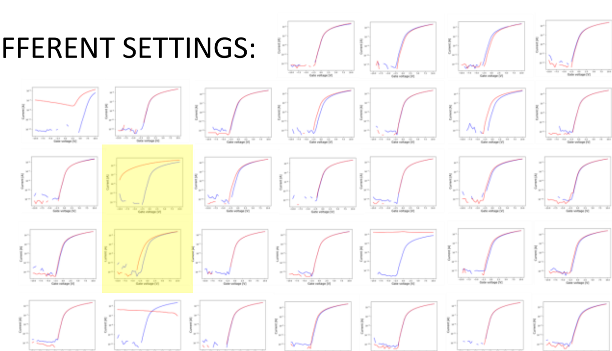
Challenge #2: key hiding
Experimental validation

SOLUTION:

Apply different settings of the laser to cause different V_T shifts that cannot be visually distinguished

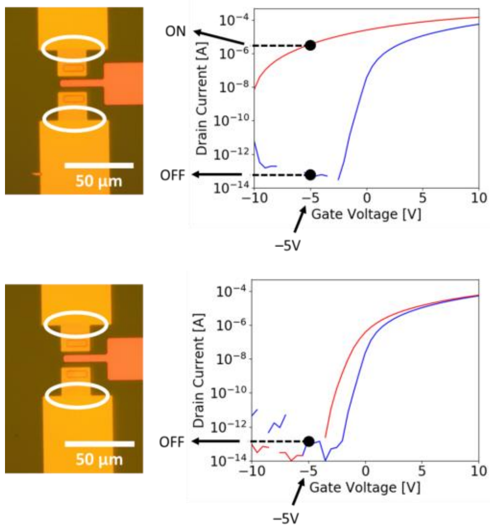
EXPLORATION OF DIFFERENT SETTINGS:

- Blue:
  before lasering
- Red:
  after lasering



CROSSING, 2019, Darmstadt, Germany

Challenge #2: key hiding
Experimental validation



SOLUTION:

Apply different settings of the laser to cause different V_T shifts that cannot be visually distinguished:

- Setting 1 (top image): attenuation of 45 dB in low energy mode; one pulse applied
- Setting 2 (bottom image): attenuation of 35 dB in low energy mode; two pulses applied

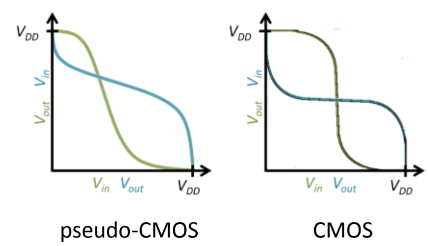
Challenge #2: key hiding
Possible alternative solution

- Additive method instead of modificative method:
  - Add ink at the top and the bottom of the chip
  - The ink should be:
    - Non-conductive
    - Non-transparent
    - Insoluble

CROSSING, 2019, Darmstadt, Germany

Remaining challenges

- Physically Unclonable Functions (PUFs) on plastics
  - Digital circuits continue to operate correctly when they are bended or stretched, but PUFs might not produce a reliable unique output
- True Random Number Generators (TRNGs) on plastics
  - The slope of the input-output characteristic of pseudo-CMOS gates is less steep compared to CMOS gates, so the design of TRNGs needs to be revisited



Conclusion

- We presented:
  - The first cryptographic core on flex foil
  - A solution for the “invisible” programming of the key bits
- There are many more security challenges to be tackled
- The technology is rapidly improving and soon ready for mainstream applications
- It is crucial to guarantee the security of these applications