Security on Plastics: Fake or Real?

Nele Mentens, Jan Genoe, Thomas Vandenabeele,
Lynn Verschueren, Dirk Smets, Wim Dehaene, Kris Myny

Cryptographic Hardware and Embedded Systems (CHES)
August 26-28, 2019, Atlanta, US

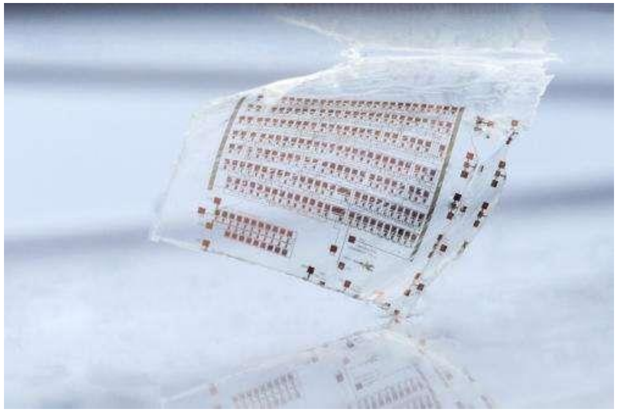
KATHOLIEKE UNIVERSITEIT LEUVEN

Outline

- Flexible electronics on plastics
- Our implementation
- Our key hiding solution
- Conclusion

Flexible electronics on plastics
Applications

- Commercially used in flexible displays
- Large potential for flexible digital circuits in (passive) RFID/NFC chips, integrated in paper or plastics
- Examples: smart packages, intelligent labels, electronic paper

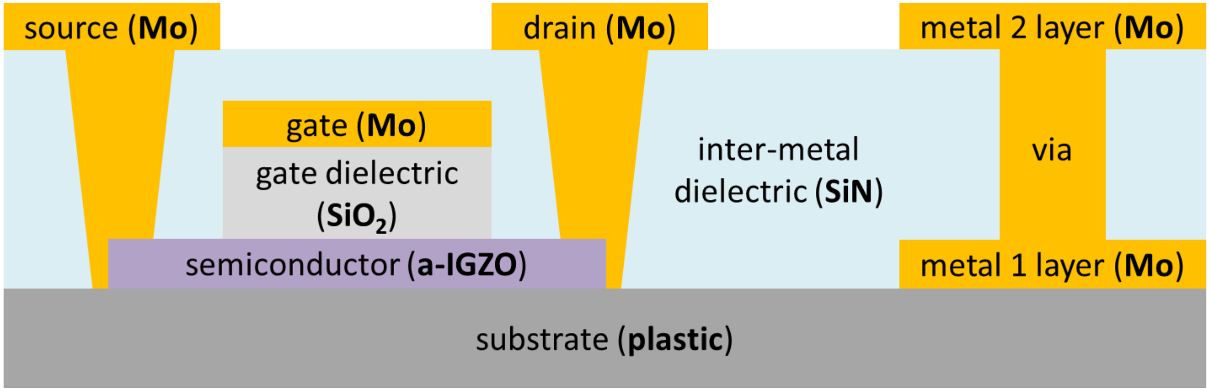


[source figures: imec]

Flexible electronics on plastics
Technology

KATHOLIEKE UNIVERSITEIT LEUVEN

- Several thin-film transistor (TFT) technologies exist
- Amorphous metal-oxide TFTs show the best combination of high performance and low processing cost



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

Flexible electronics on plastics

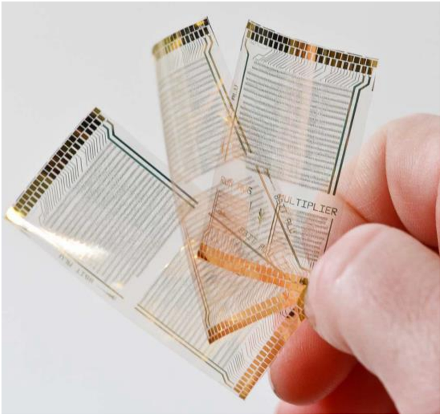
Comparison with silicon transistors

	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
Security challenge

KATHOLIEKE UNIVERSITEIT LEUVEN

- To secure the communication between the flexible tag and the reader, many hurdles need to be overcome
- In this work, we concentrate on two challenges:
  - Integrate crypto cores in the flexible chip
    - The maximum number of TFTs in one chip, reported up to now, is only 3504
  - 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

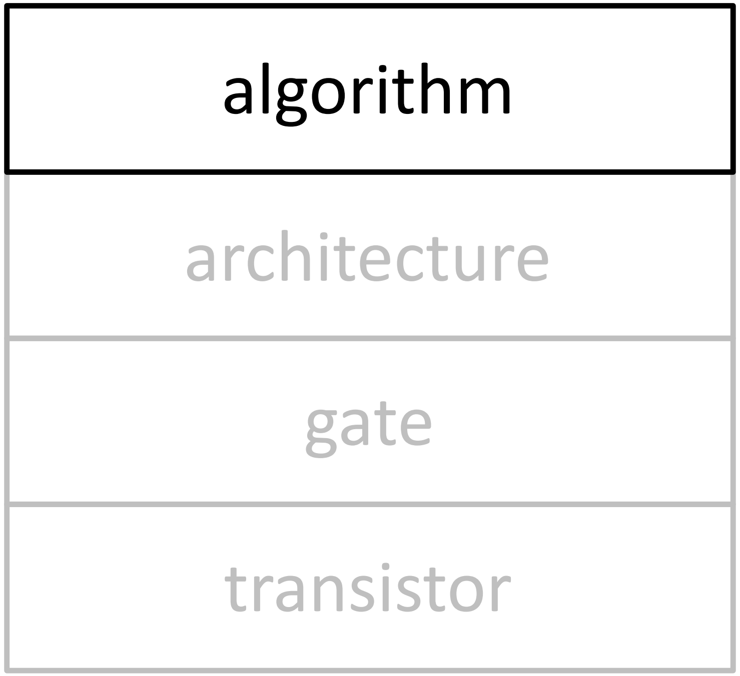


[source figures: imec]

Our implementation
Design choices

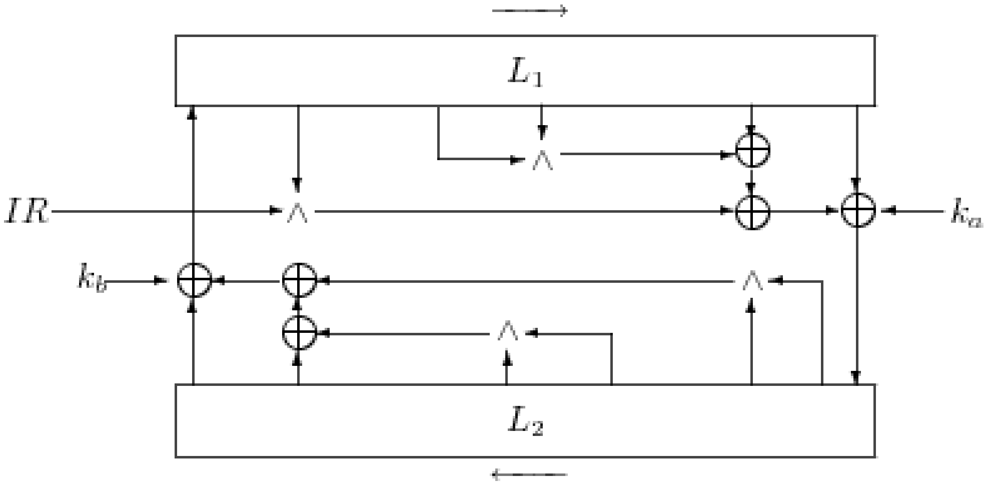
algorithm
architecture
gate
transistor

Our implementation
Design choices



KTANTAN32*

- Block size: 32 bits
- Key size: 80 bits
- Fixed key



*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.

Our implementation
Design choices

algorithm

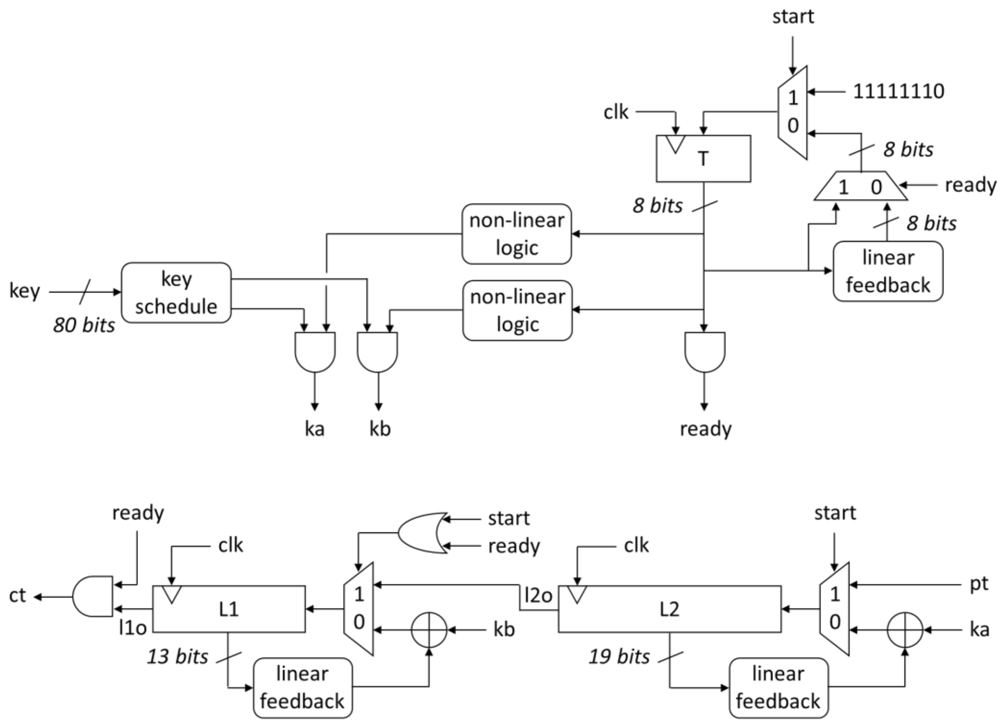
architecture

gate

transistor

Serial architecture

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



Our implementation

Design choices

algorithm

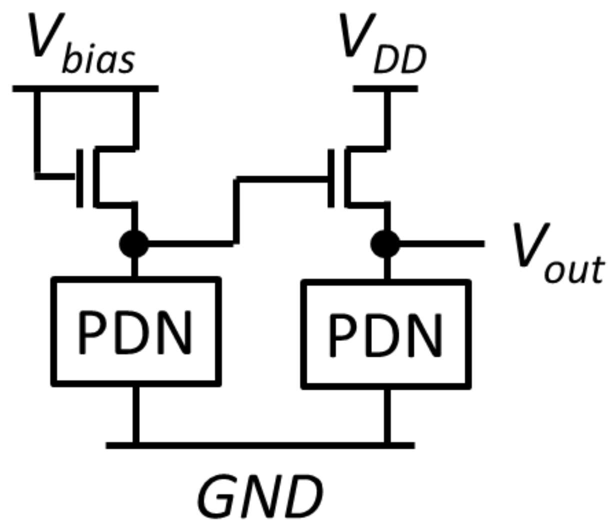
architecture

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



Our implementation
Design choices

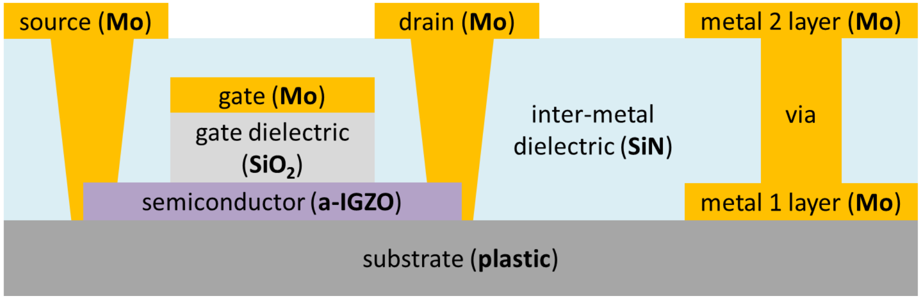
algorithm

architecture

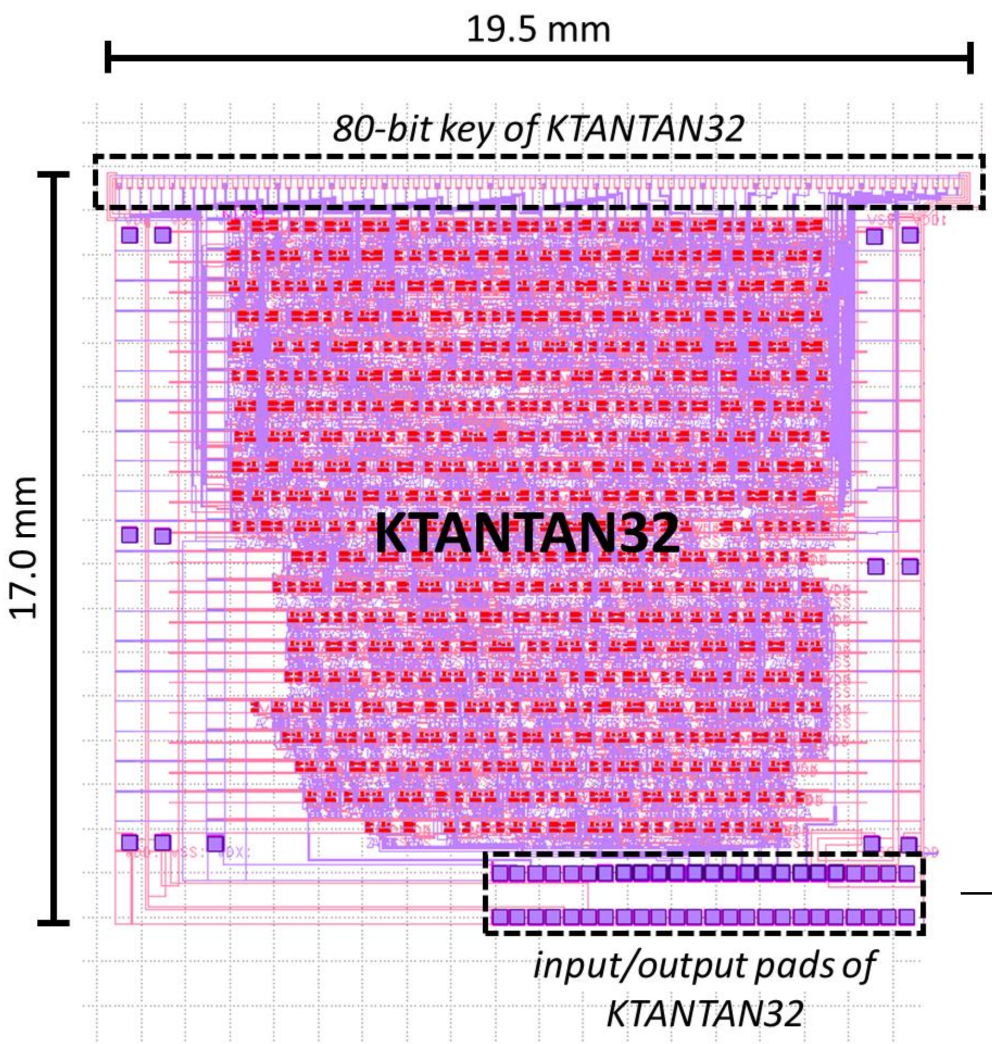
gate

transistor

a-IGZO semiconductor



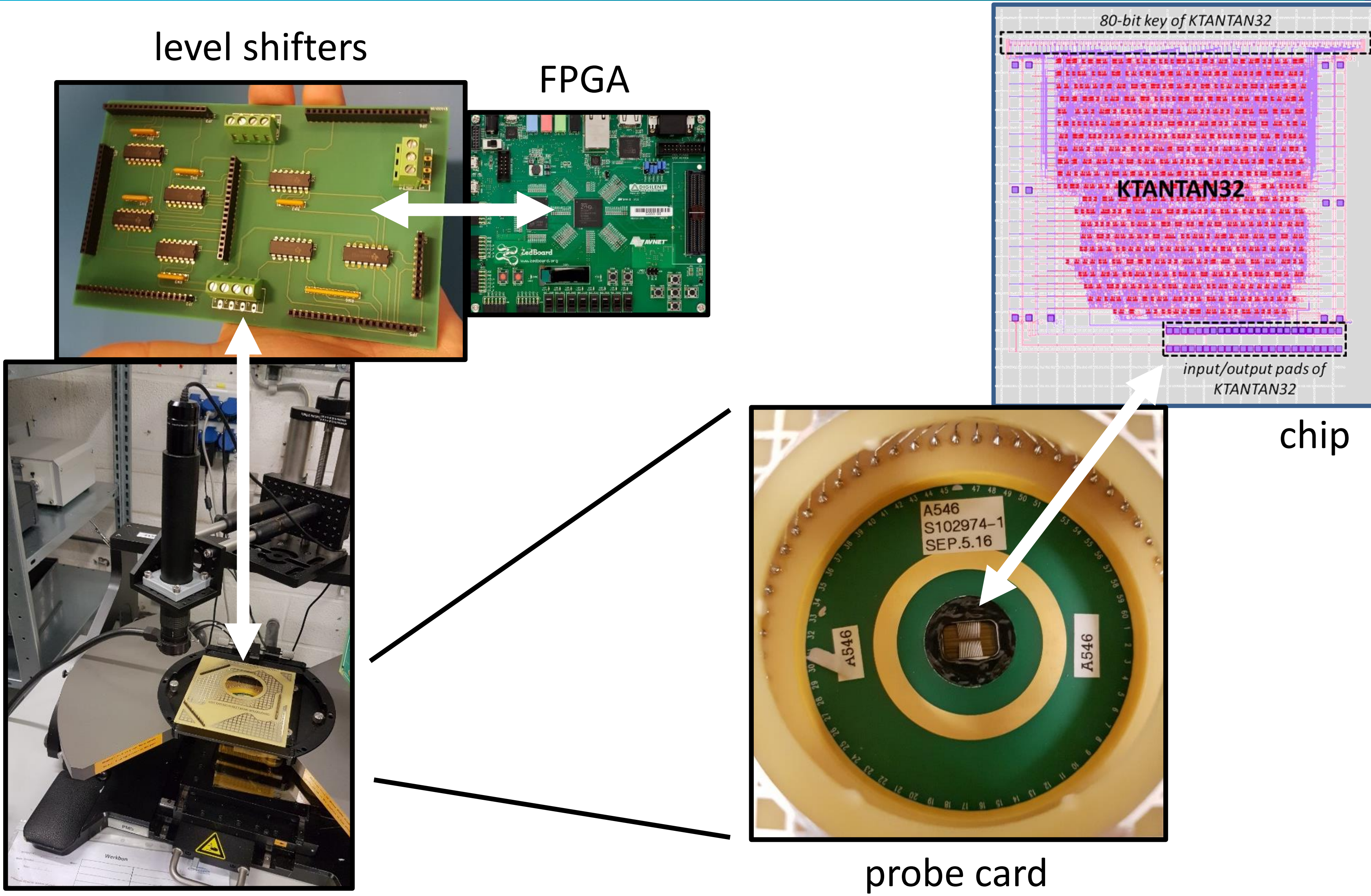
Our implementation
Layout



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

- 4044 TFTs
- 331.5 mm^2

Our implementation
Measurement setup

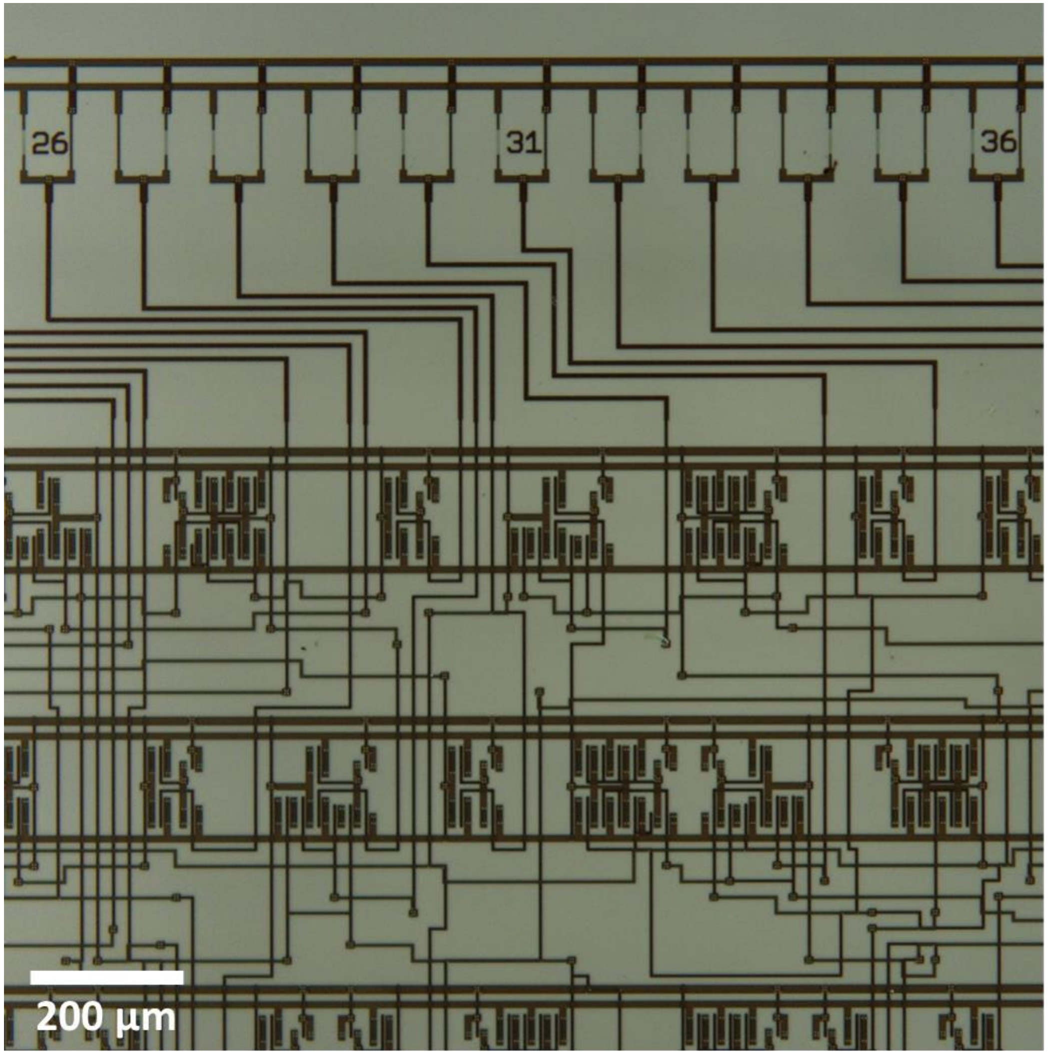


Our implementation
Measurement results

- 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

Our implementation

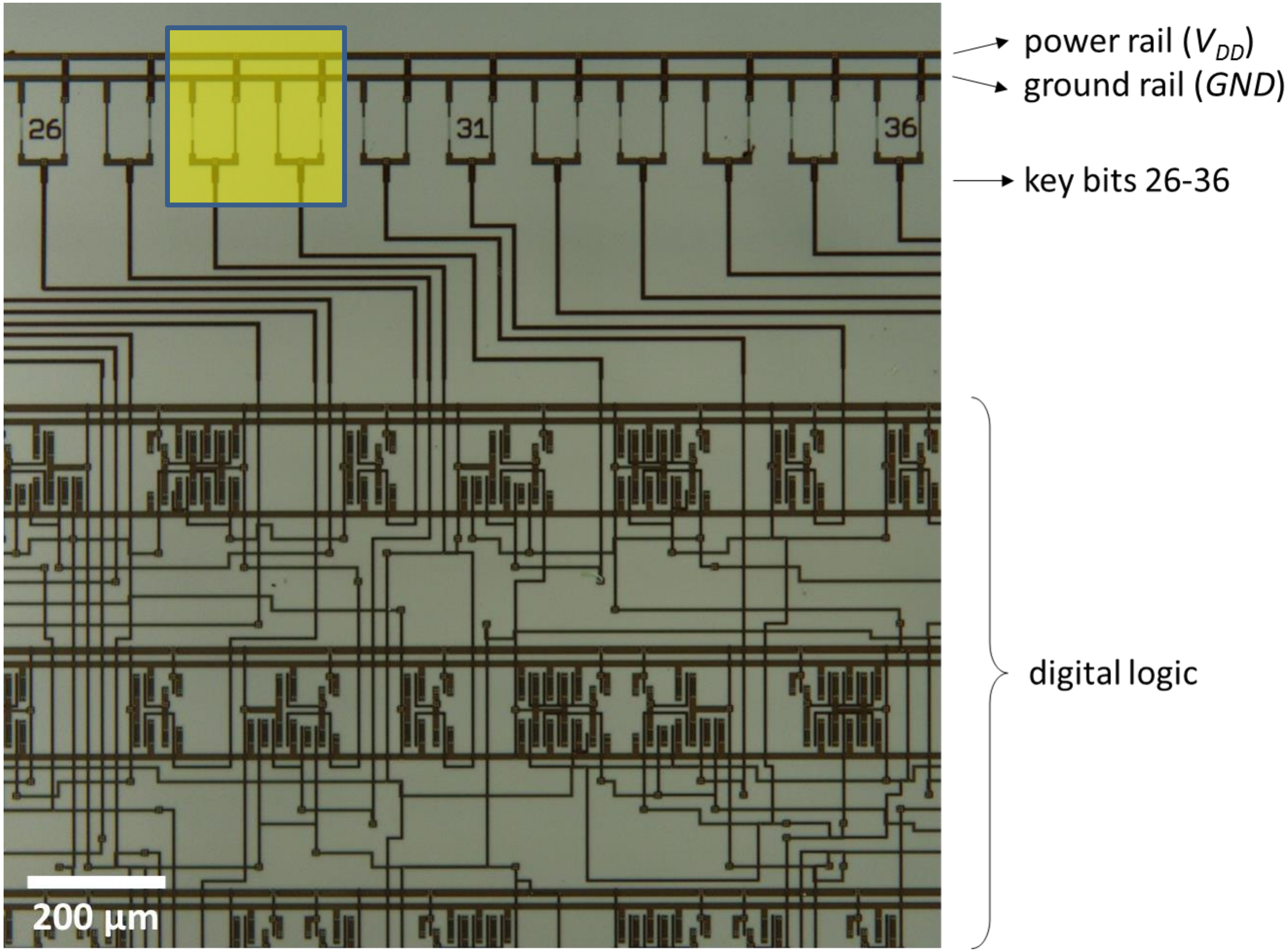
Key programming



power rail (V_{DD})
ground rail (*GND*)
key bits 26-36
digital logic

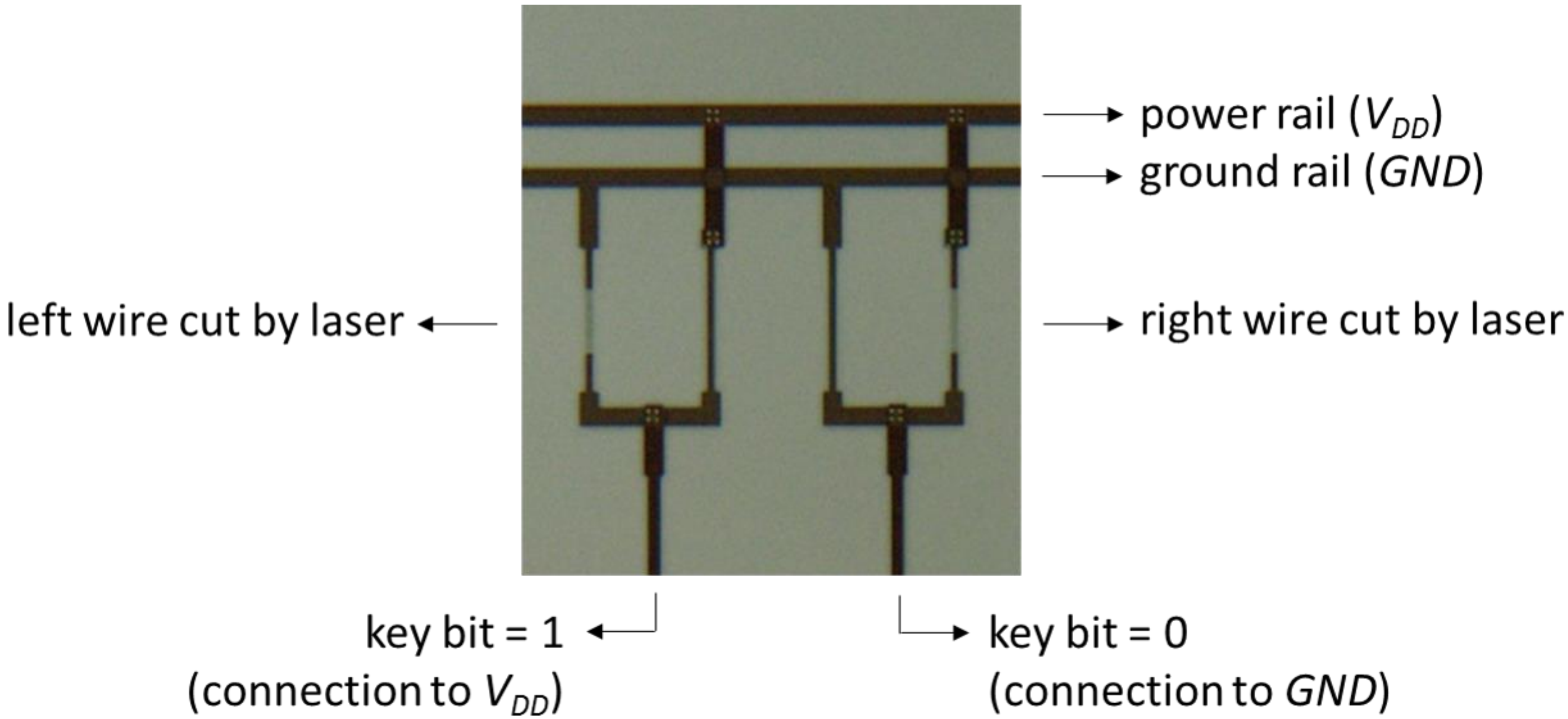
Our implementation

Key programming



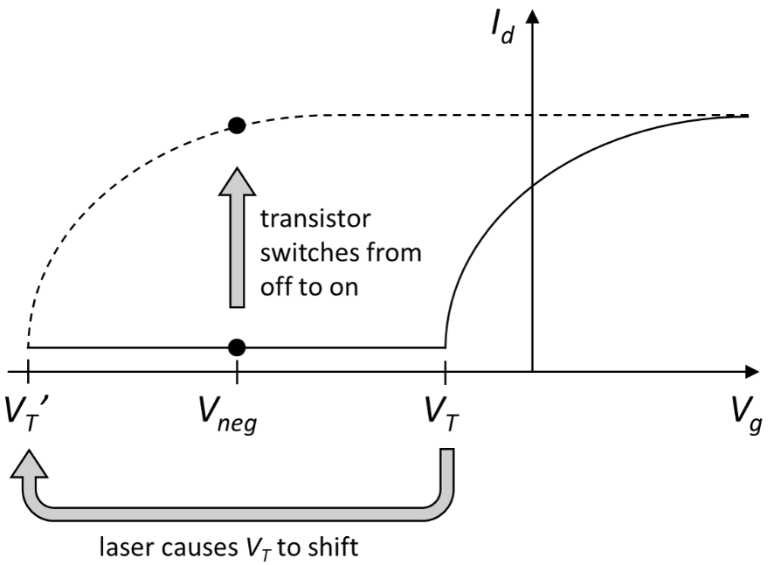
Our implementation

Key programming



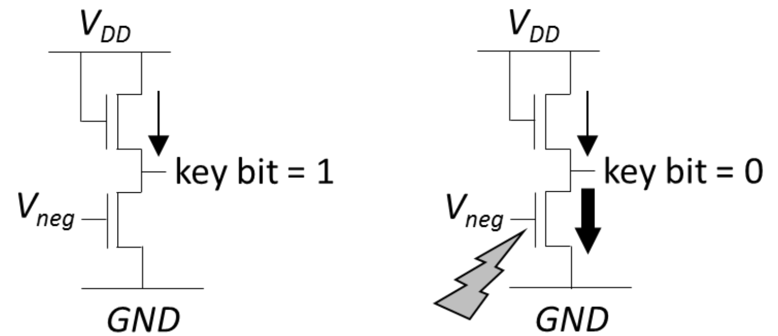
PROBLEM: The key bits can easily be read out using a microscope

Our key hiding solution
Proposed concept

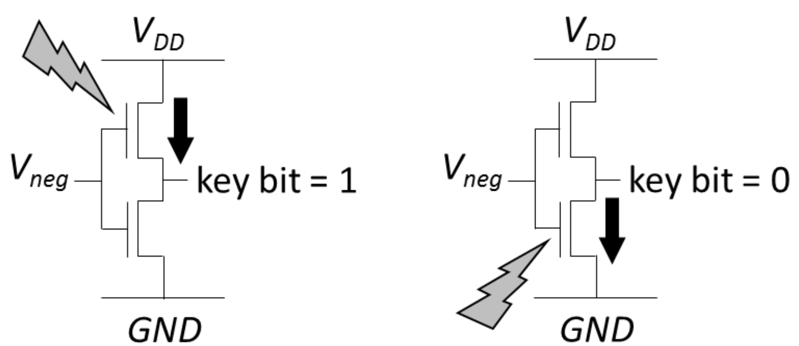


The temperature change caused by lasering, shifts the threshold voltage (V_T) and thus the I_d - V_g graph

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



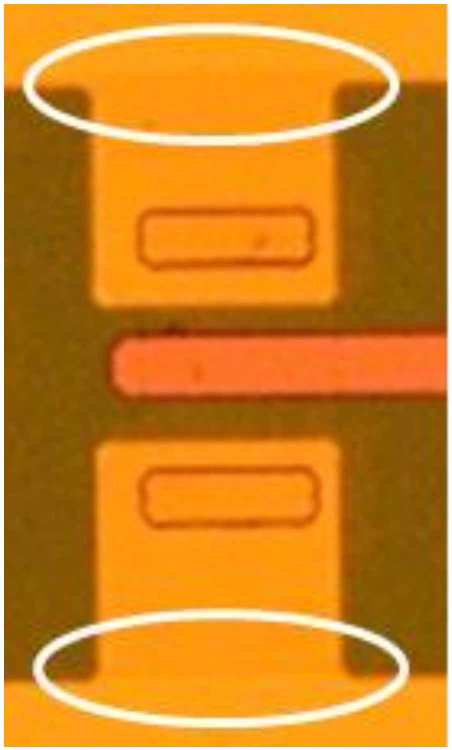
First option for key programming



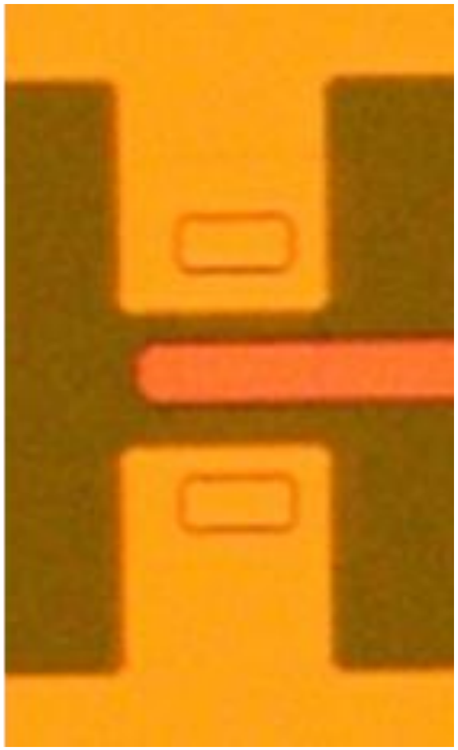
Second option for key programming

Our key hiding solution
Experimental validation

TFT microscope images



lasered

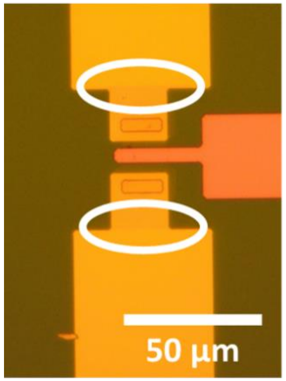


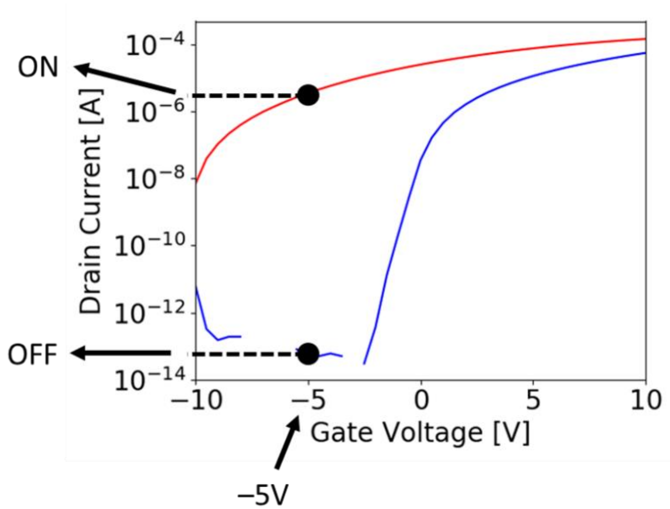
not lasered

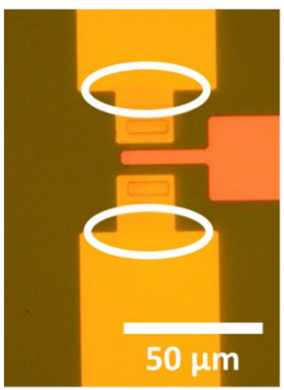
PROBLEM:

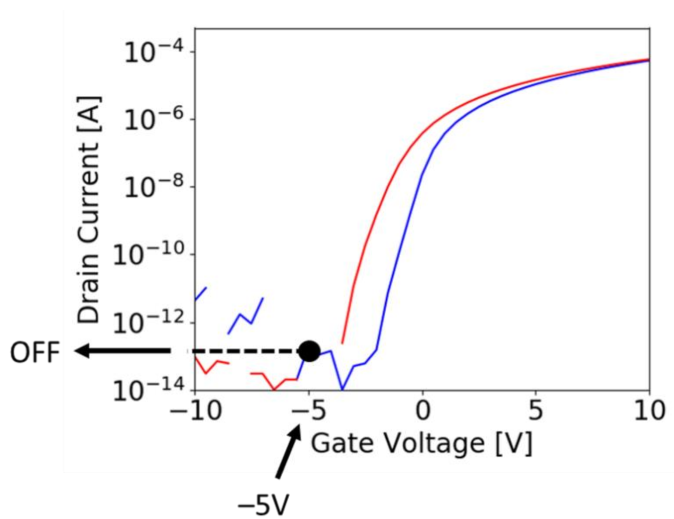
The difference is visible between a TFT that has been lasered and a TFT that has not been lasered

Our key hiding solution
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

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