Security challenges and opportunities in emerging device technologies

A case study on flexible electronics

Nele Mentens

n.mentens@liacs.leidenuniv.nl / nele.mentens@kuleuven.be

Universiteit Leiden The Netherlands
liacs Leiden Institute of Advanced Computer Science
KU LEUVEN
COSIC
ESAT
imec

International Winter School on Microarchitectural Security, December 5-9, 2022

Security challenges and opportunities in **emerging device technologies**

A case study on flexible electronics

Universiteit Leiden
KU LEUVEN

Emerging Technologies

- International Roadmap for Devices and Systems (IRDS) [1]
  - Is the successor of the International Technology Roadmap for Semiconductors (ITRS) since 2016
  - Predicts the evolution of electronic devices and systems
  - Describes the evolution towards deep-submicron technologies
  - Also mentions **devices and systems that do not rely on bulk silicon technology**
  - Publishes annual reports by several International Focus Teams (IFT)

[1] "International roadmap for devices and systems - executive summary," https://irds.ieee.org/images/files/pdf/2020/2020IRDS ES.pdf, 2020.

Emerging Technologies

- International Roadmap for Devices and Systems (IRDS) [1]
  - Is the successor of the International Technology Roadmap for Semiconductors (ITRS) since 2016
  - Predicts the evolution of electronic devices and systems
  - Describes the evolution towards deep-submicron technologies
  - Also mentions **devices and systems that do not rely on bulk silicon technology**
  - Publishes annual reports by several International Focus Teams (IFT)
- Examples of emerging technologies
  - Electronics on flexible foil (IFT “More than Moore”) -> low cost, flexibility
  - Memristors (IFT “Beyond CMOS”) -> high performance, high density
  - Ultra low leakage technologies, like fully depleted silicon on insulator (IFT “More Moore”) -> low power consumption

[1] “International roadmap for devices and systems - executive summary,” https://irds.ieee.org/images/files/pdf/2020/2020IRDS ES.pdf, 2020.

Emerging Technologies

- International Roadmap for Devices and Systems (IRDS) [1]
  - Is the successor of the International Technology Roadmap for Semiconductors (ITRS) since 2016
  - Predicts the evolution of electronic devices and systems
  - Describes the evolution towards deep-submicron technologies
  - Also mentions **devices and systems that do not rely on bulk silicon technology**
  - Publishes annual reports by several International Focus Teams (IFT)
- Examples of emerging technologies
  - Electronics on flexible foil (IFT "More than Moore") -> low cost, flexibility
  - Memristors (IFT "Beyond CMOS") -> high performance, high density
  - Ultra low leakage technologies, like fully depleted silicon on insulator (IFT "More Moore") -> low power consumption
- The IRDS also emphasizes that **security** is an important requirement

[1] "International roadmap for devices and systems - executive summary," https://irds.ieee.org/images/files/pdf/2020/2020IRDS ES.pdf, 2020.

Universiteit Leiden

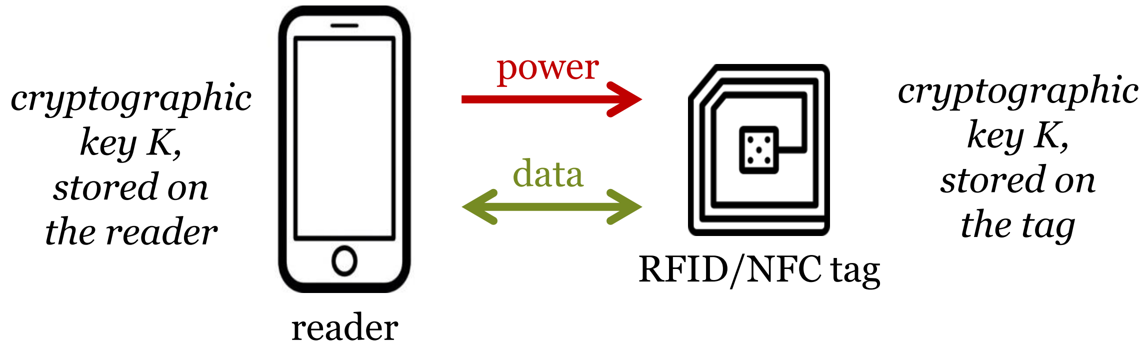
KU LEUVEN

Security challenges and opportunities in emerging device technologies

A case study on flexible electronics

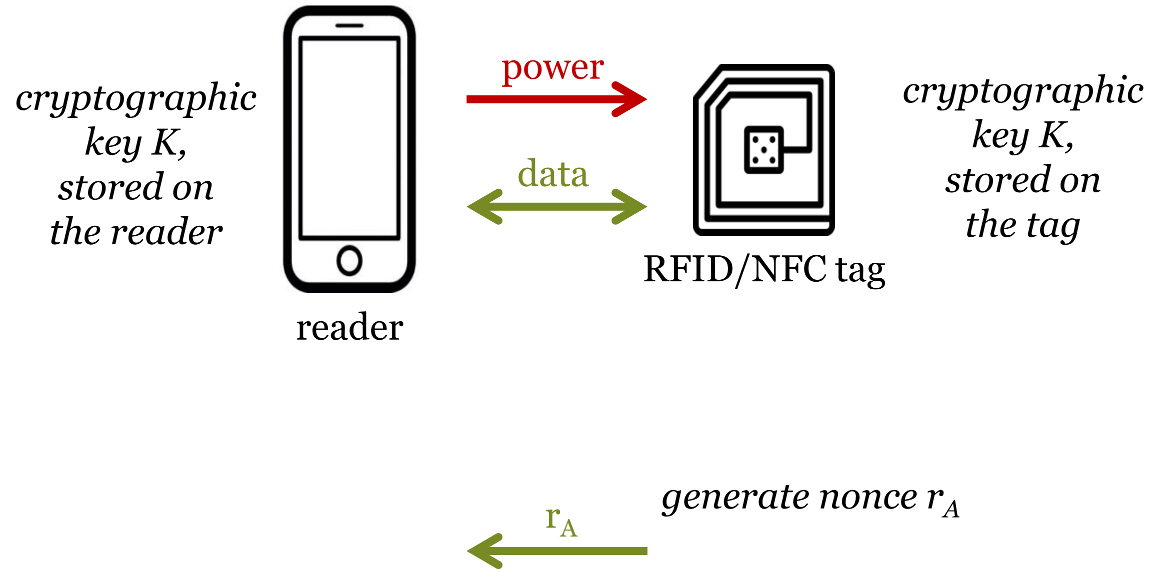
Hardware security requirements

- Illustrative example to explain the hardware requirements of a lightweight device (e.g. a passive RFID or NFC tag) → reader authentication protocol



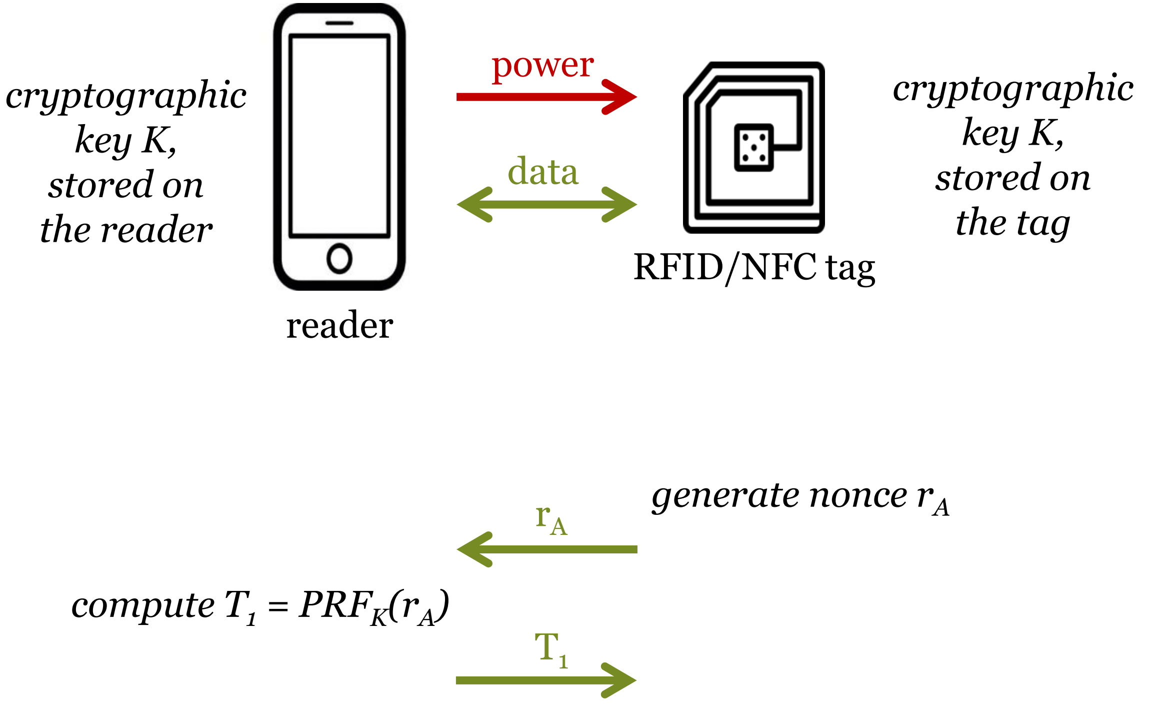
Hardware security requirements

- Illustrative example to explain the hardware requirements of a lightweight device (e.g. a passive RFID or NFC tag) → reader authentication protocol



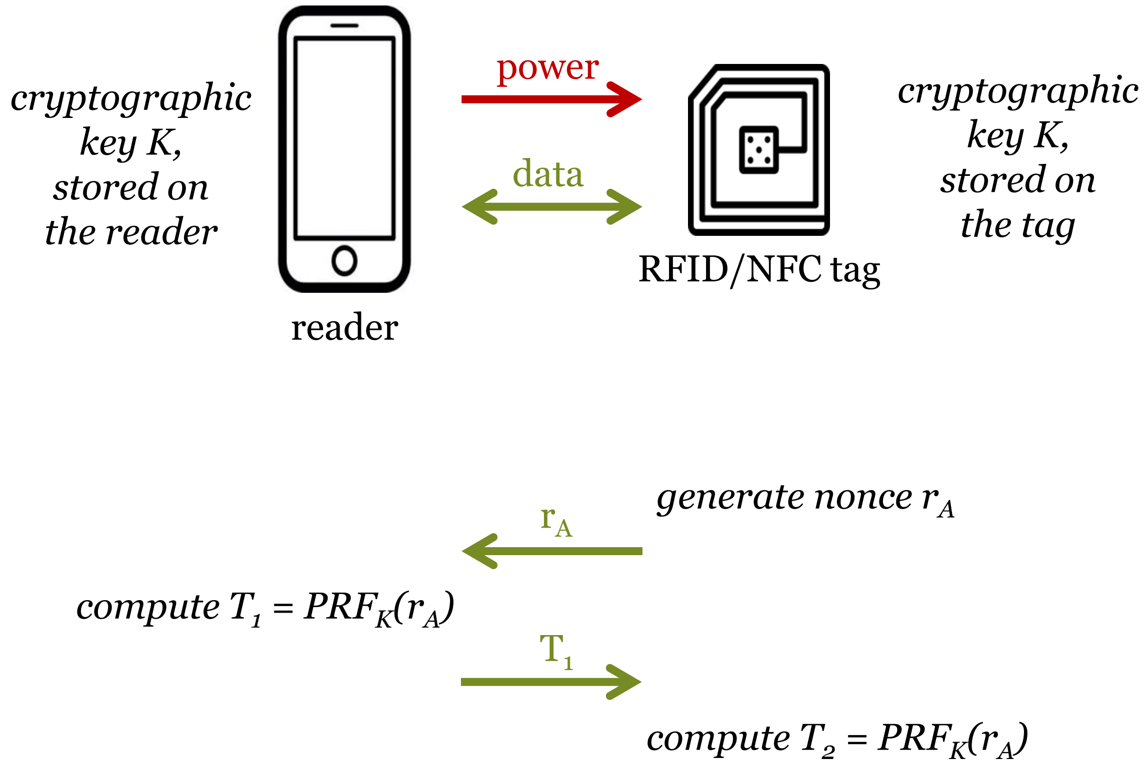
Hardware security requirements

- Illustrative example to explain the hardware requirements of a lightweight device (e.g. a passive RFID or NFC tag) → reader authentication protocol



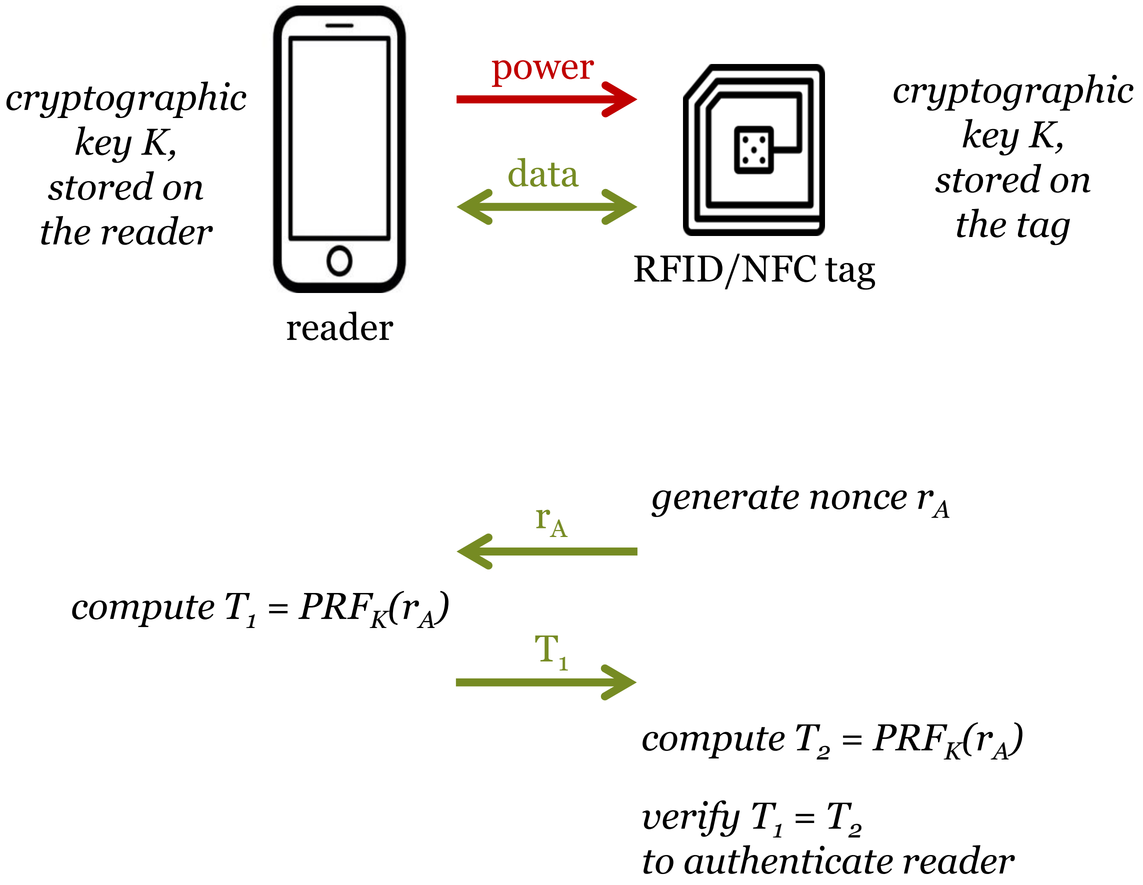
Hardware security requirements

- Illustrative example to explain the hardware requirements of a lightweight device (e.g. a passive RFID or NFC tag) → reader authentication protocol



Hardware security requirements

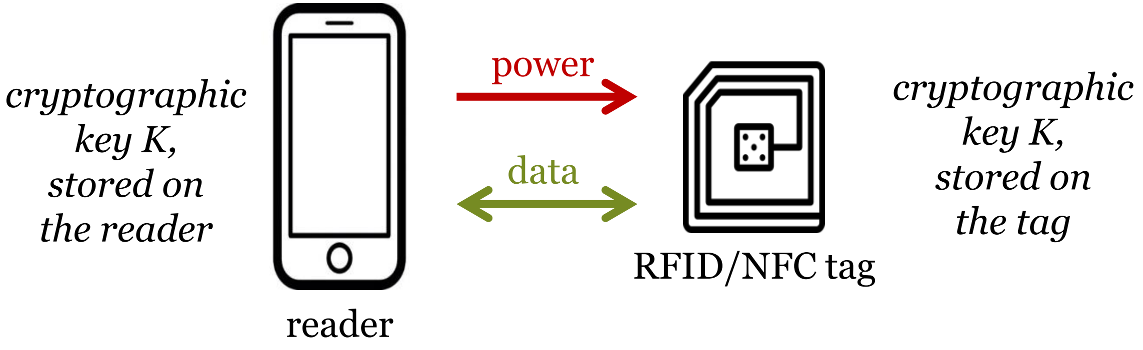
- Illustrative example to explain the hardware requirements of a lightweight device (e.g. a passive RFID or NFC tag) → reader authentication protocol



Hardware security requirements

- Illustrative example to explain the hardware requirements of a lightweight device (e.g. a passive RFID or NFC tag) → reader authentication protocol

Hardware security requirements to protect against a remote adversary?



Tag: *generate nonce r_A*

Tag → reader: r_A

Reader: *compute $T_1 = PRF_K(r_A)$*

Reader → tag: T_1

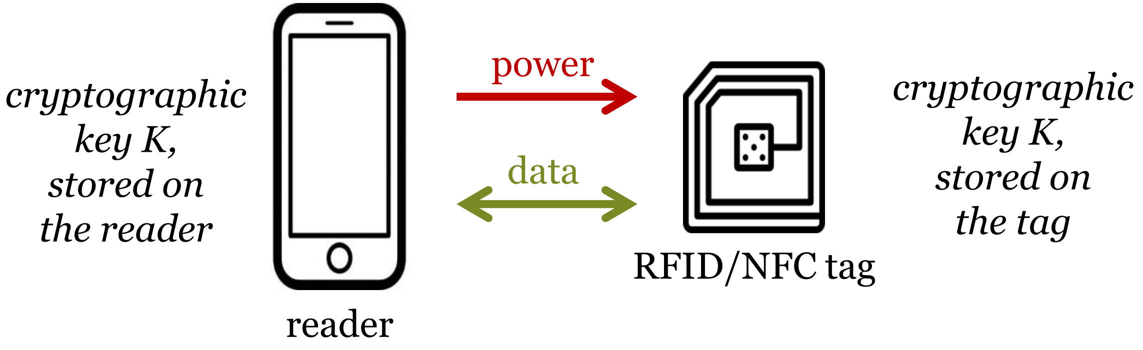
Tag: *compute $T_2 = PRF_K(r_A)$*

Tag: *verify $T_1 = T_2$ to authenticate reader*

Hardware security requirements

- Illustrative example to explain the hardware requirements of a lightweight device (e.g. a passive RFID or NFC tag) → reader authentication protocol

Hardware security requirements to protect against a remote adversary?



generate nonce r_A

Nonce generator

r_A ←

compute $T_1 = PRF_K(r_A)$

T_1 →

compute $T_2 = PRF_K(r_A)$

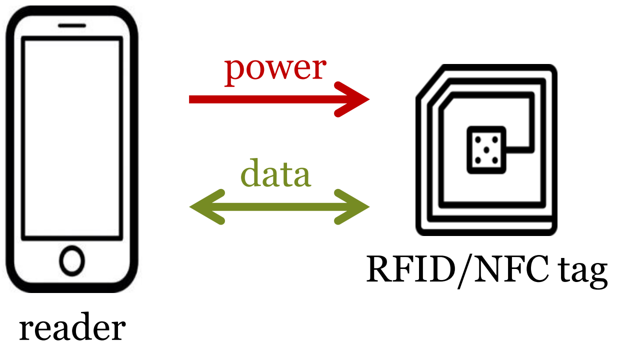
verify $T_1 = T_2$
to authenticate reader

Hardware security requirements

- Illustrative example to explain the hardware requirements of a lightweight device (e.g. a passive RFID or NFC tag) → reader authentication protocol

Hardware security requirements to protect against a remote adversary?

cryptographic key K, stored on the reader



cryptographic key K, stored on the tag

generate nonce r_A

Nonce generator

r_A ←

compute $T_1 = PRF_K(r_A)$

T_1 →

compute $T_2 = PRF_K(r_A)$

Digital crypto circuit

verify $T_1 = T_2$
to authenticate reader

Hardware security requirements

Universiteit Leiden

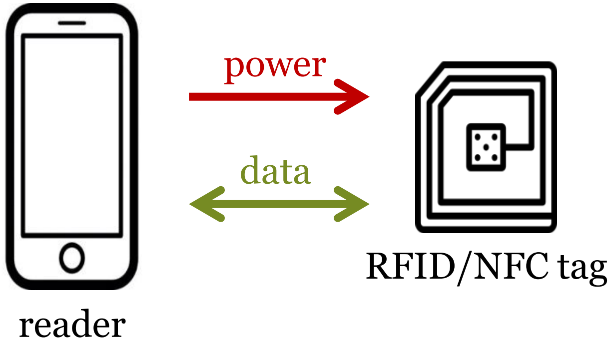
KU LEUVEN

- Illustrative example to explain the hardware requirements of a lightweight device (e.g. a passive RFID or NFC tag) → reader authentication protocol

Hardware security requirements to protect against a remote adversary?

Hardware security requirements to protect against a physical adversary?

cryptographic key K, stored on the reader



cryptographic key K, stored on the tag

generate nonce r_A

Nonce generator

r_A

compute $T_1 = PRF_K(r_A)$

T_1

compute $T_2 = PRF_K(r_A)$

verify $T_1 = T_2$ *to authenticate reader*

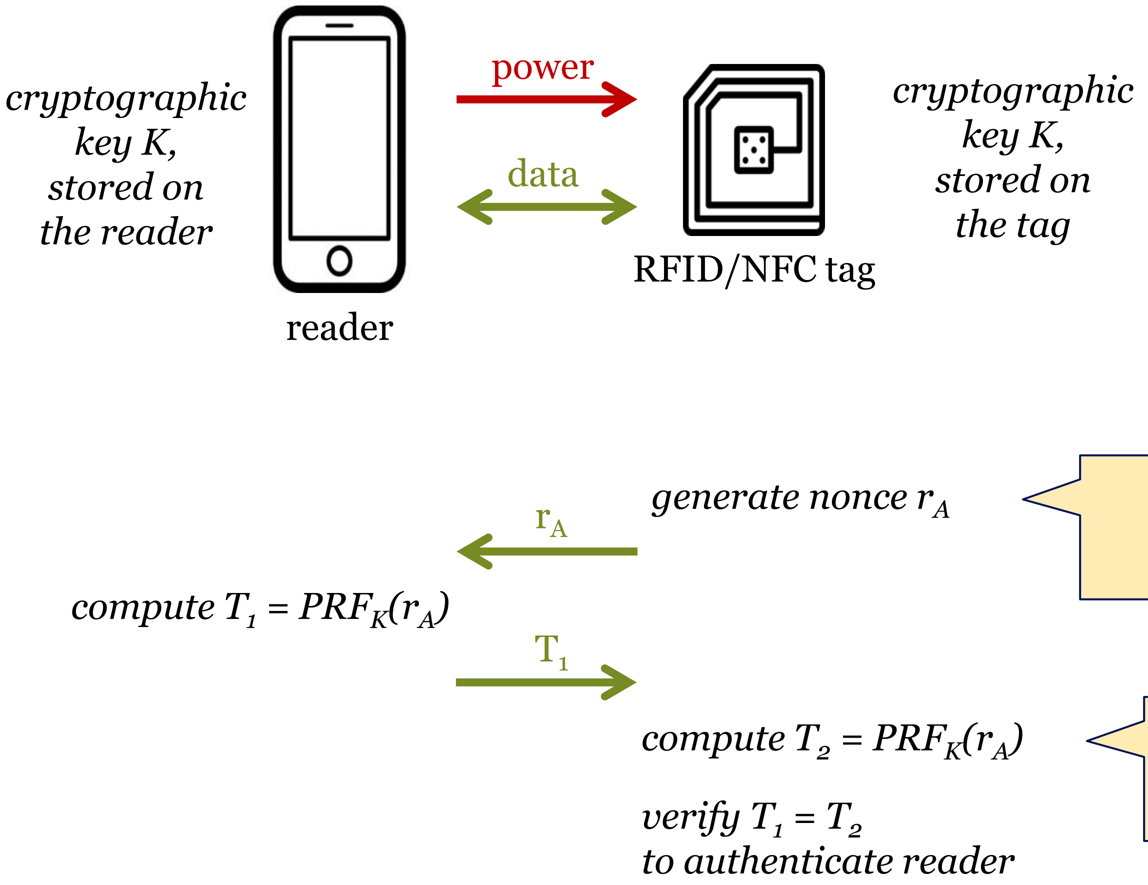
Digital crypto circuit

Hardware security requirements

- Illustrative example to explain the hardware requirements of a lightweight device (e.g. a passive RFID or NFC tag) → reader authentication protocol

Hardware security requirements to protect against a remote adversary?

Hardware security requirements to protect against a physical adversary?



Secure key storage

Nonce generator

Digital crypto circuit

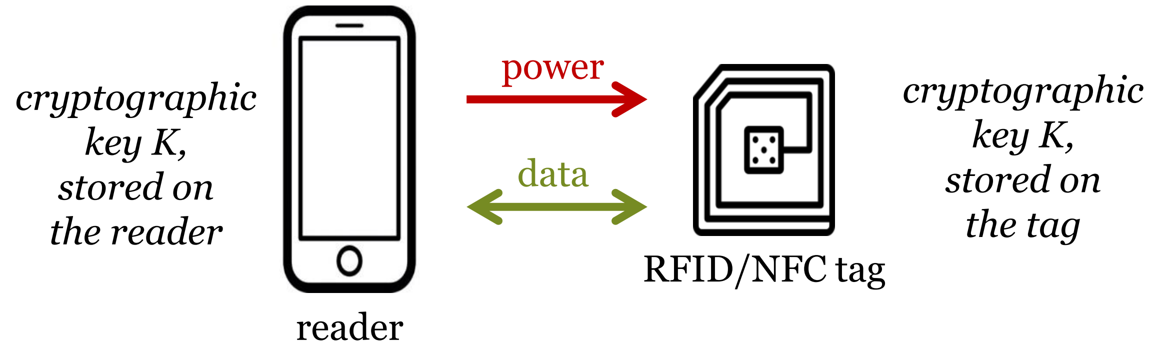
Hardware security requirements

Universiteit Leiden
KU LEUVEN

- Illustrative example to explain the hardware requirements of a lightweight device (e.g. a passive RFID or NFC tag) → reader authentication protocol

Hardware security requirements to protect against a remote adversary?

Hardware security requirements to protect against a physical adversary?



Secure key storage

Protection against IP theft

generate nonce r_A

Nonce generator

r_A ←

compute $T_1 = PRF_K(r_A)$

T_1 →

compute $T_2 = PRF_K(r_A)$

verify $T_1 = T_2$ to authenticate reader

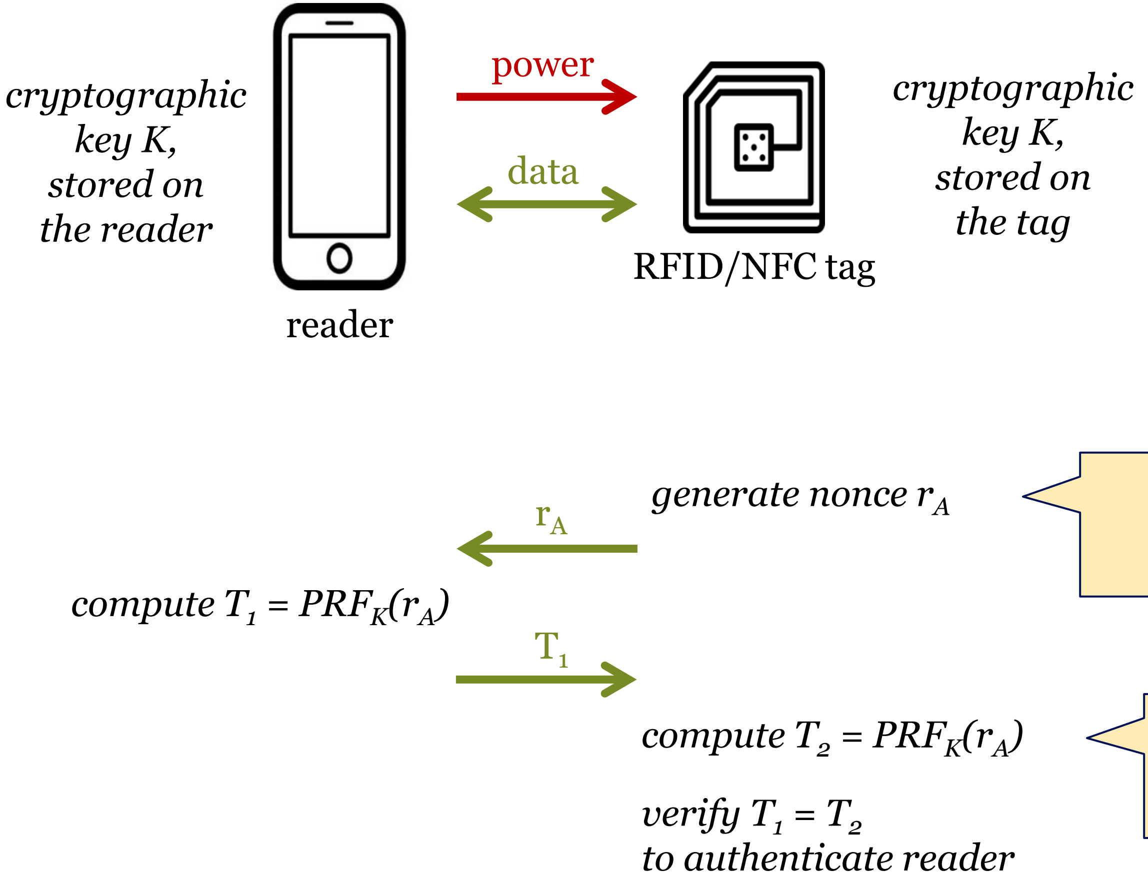
Digital crypto circuit

Hardware security requirements

- Illustrative example to explain the hardware requirements of a lightweight device (e.g. a passive RFID or NFC tag) → reader authentication protocol

Hardware security requirements to protect against a remote adversary?

Hardware security requirements to protect against a physical adversary?



Secure key storage

Protection against IP theft

Protection against physical attacks

Nonce generator

Digital crypto circuit

Universiteit Leiden

KU LEUVEN

Security challenges and opportunities in emerging device technologies

A case study on flexible electronics

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

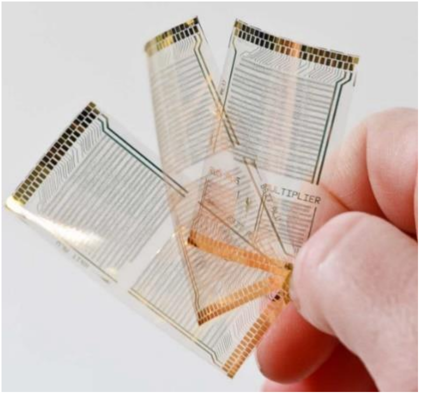
Universiteit Leiden

KU LEUVEN

- 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

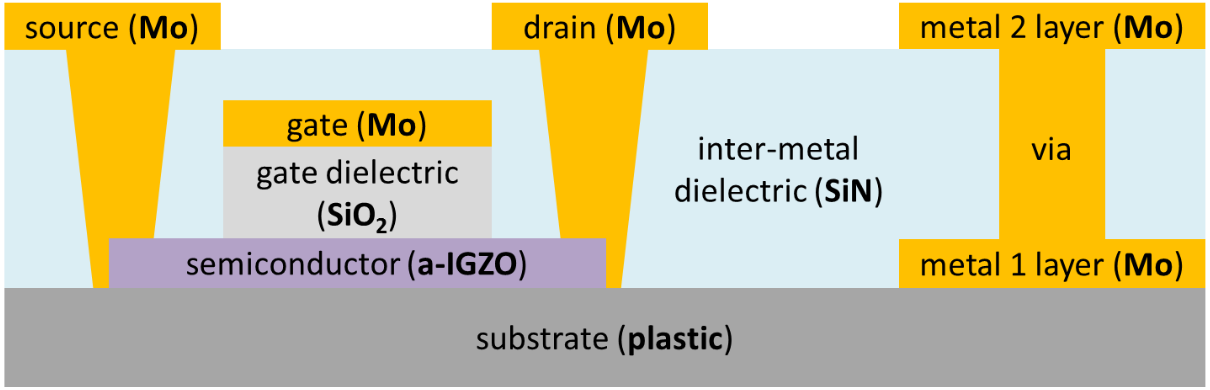
Flexible electronics on plastics
Digital circuits

- Circuits that have already been fabricated:
  - NFC transponder
  - Small microprocessors with limited instruction sets



Flexible electronics on plastics
Transistor technology

- 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 chips

Universiteit Leiden

KU LEUVEN

	silicon (10 nm)	a-IGZO (5 µm)	a-IGZO newer generation (0.8 µm)
Core supply voltage	0.7 V	5-10 V	3-10 V
Charge carrier mobility	500-1500 cm^2/Vs	~ 10 cm^2/Vs	~ 10 cm^2/Vs
Transistor density	~ 45 mio per mm^2	10^3-10^4 per cm^2	10^4-10^5 per cm^2
Semiconductor type	n-type and p-type	only n-type	only n-type
Cost per 1000 transistors	> 0.3 USD		> 0.01 USD
Flexible?	no	yes	yes

- ⇨ ☹ Higher power consumption
- ⇨ ☹ Lower performance
- ⇨ ☹ Larger area
- ⇨ ☹ Unipolar logic
- ⇨ ☺ Lower cost
- ⇨ ☺ Bendable, stretchable

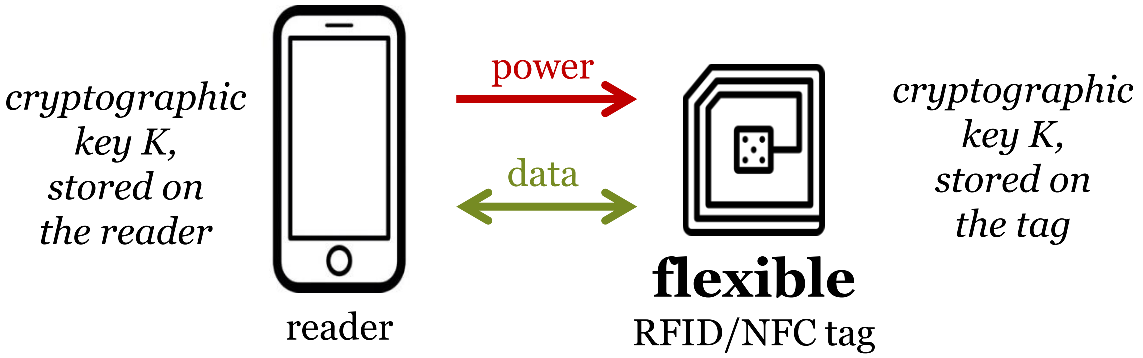
Hardware security requirements

Universiteit Leiden
KU LEUVEN

- Illustrative example to explain the hardware requirements of a lightweight device (e.g. a passive RFID or NFC tag) → reader authentication protocol

Hardware security requirements to protect against a remote adversary?

Hardware security requirements to protect against a physical adversary?



Secure key storage

Protection against IP theft

Protection against physical attacks

generate nonce r_A

Nonce generator

r_A ←

compute $T_1 = PRF_K(r_A)$

T_1 →

compute $T_2 = PRF_K(r_A)$

verify $T_1 = T_2$
to authenticate reader

Digital crypto circuit

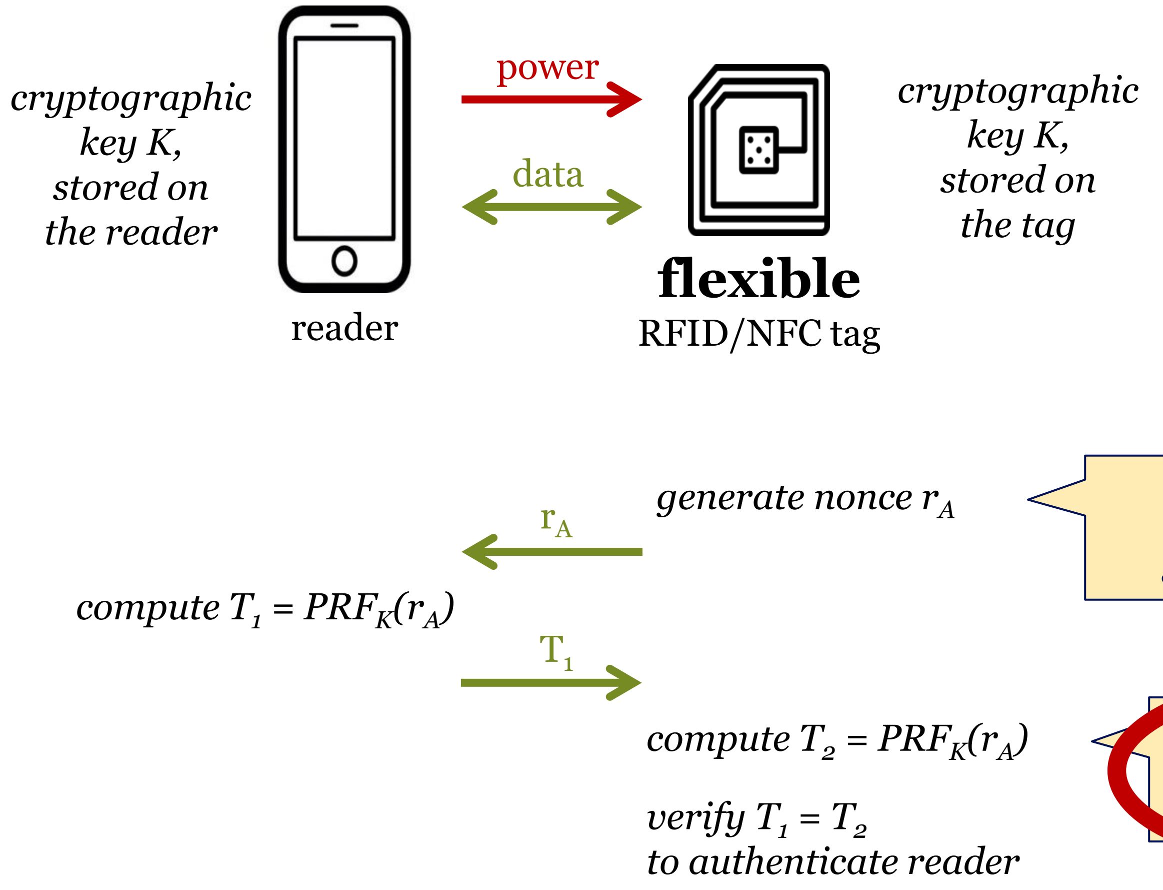
Hardware security requirements

Universiteit Leiden
KU LEUVEN

- Illustrative example to explain the hardware requirements of a lightweight device (e.g. a passive RFID or NFC tag) → reader authentication protocol

Hardware security requirements to protect against a remote adversary?

Hardware security requirements to protect against a physical adversary?



Secure key storage

Protection against IP theft

Protection against physical attacks

Nonce generator

Digital crypto circuit

Digital crypto circuit

- Cryptographic algorithms can be executed on
  - A general-purpose processor
  - Dedicated digital hardware

Digital crypto circuit

Universiteit Leiden
KU LEUVEN

- Cryptographic algorithms can be executed on
  - A general-purpose processor
  - Dedicated digital hardware
- On flexible foil, dedicated digital hardware is the best (or only) option
  - Existing general-purpose processors are not (yet) able to do crypto
  - Besides crypto, only limited functionality is needed on the flexible tag

Digital crypto circuit

Design choices

algorithm
architecture
gate
transistor

Digital crypto circuit
Design choices

algorithm

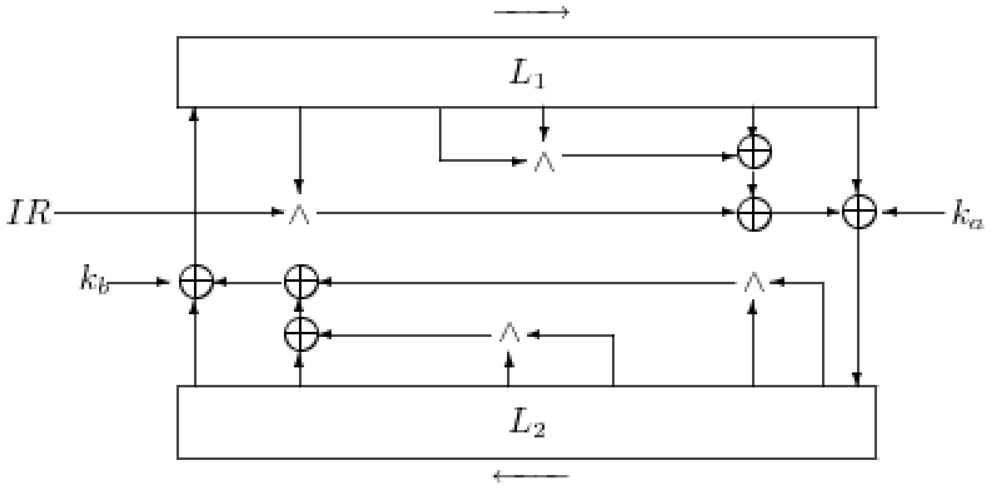
architecture

gate

transistor

KTANTAN32 [2]

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



[2] De Cannière et al., “KATAN and KTANTAN—a family of small and efficient hardware-oriented block ciphers,” CHES 2009, p. 272-288.

Digital crypto circuit

Design choices

algorithm

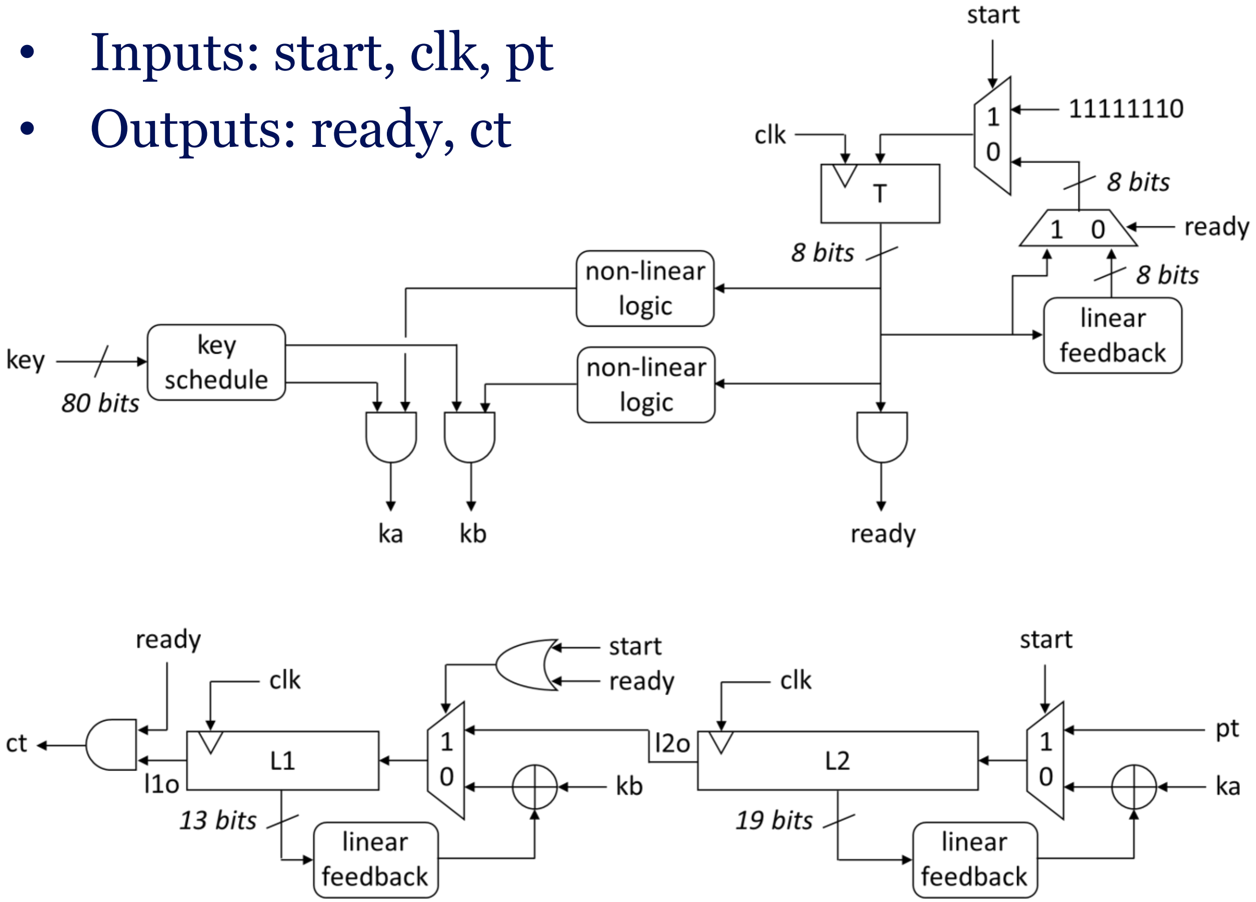
architecture

gate

transistor

Serial architecture

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



Digital crypto circuit
Design choices

algorithm

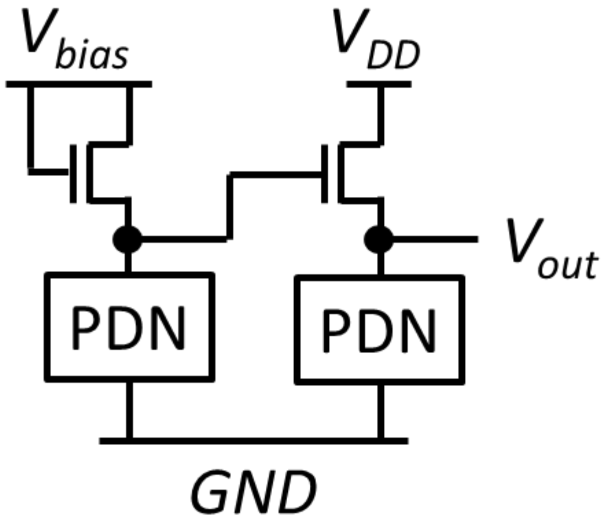
architecture

gate

transistor

Pseudo-CMOS logic

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



Digital crypto circuit
Design choices

algorithm

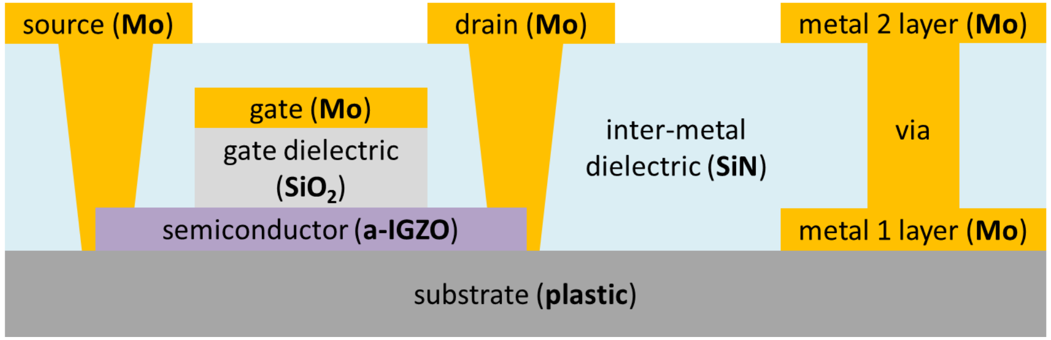
architecture

gate

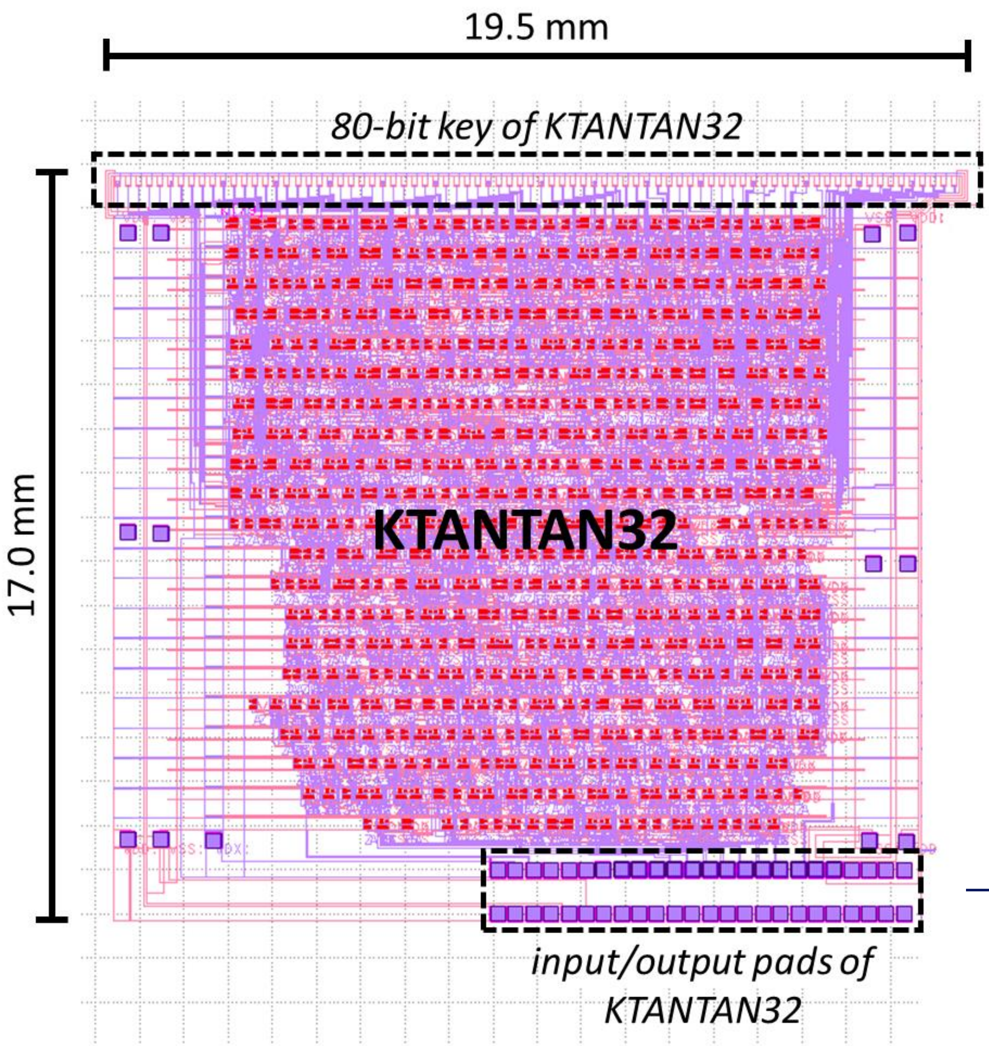
transistor

a-IGZO semiconductor

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



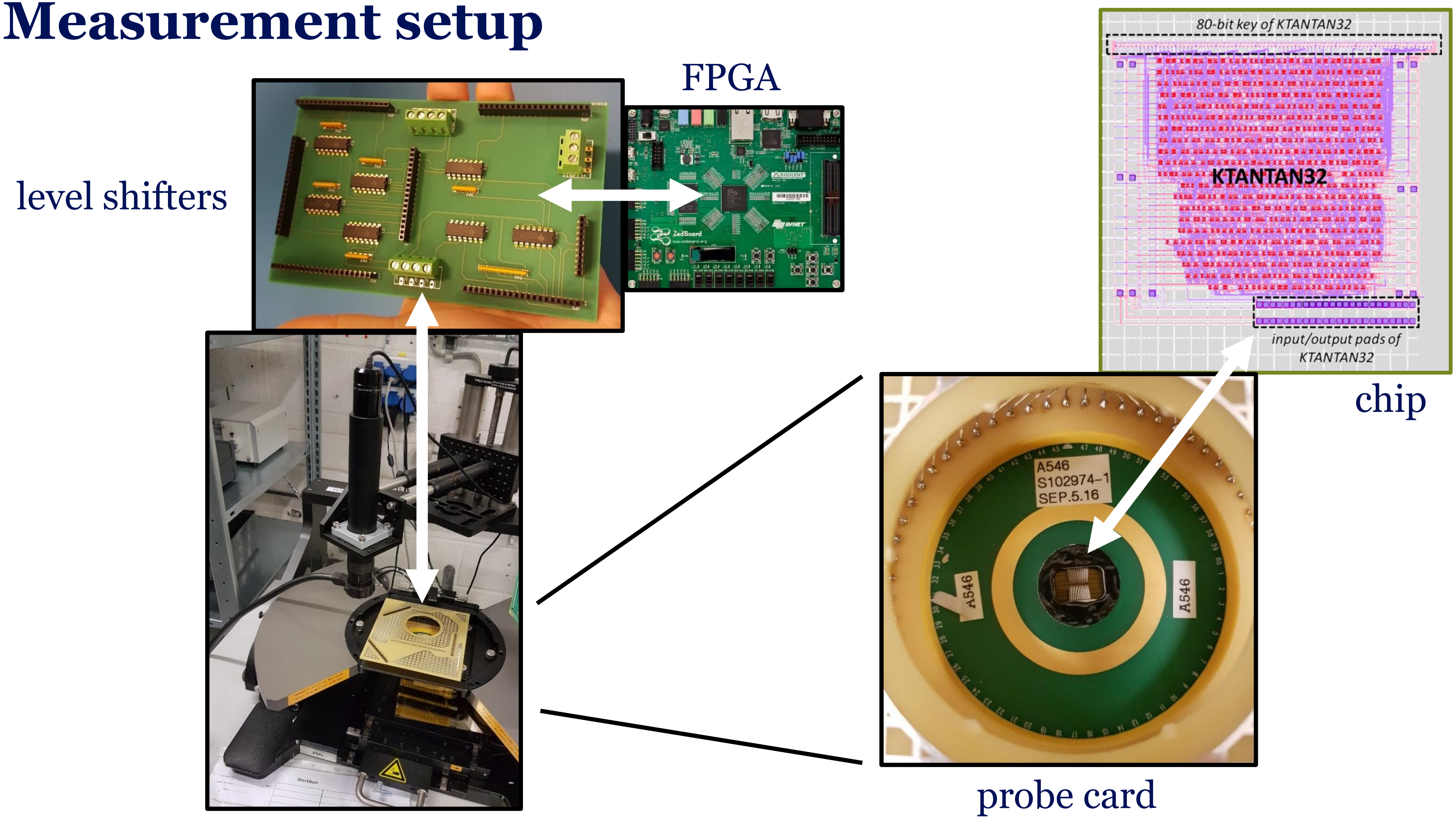
Digital crypto circuit
Lay-out



- 4044 TFTs
- 331.5 mm²

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

Digital crypto circuit
Measurement setup



Digital crypto circuit
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

Hardware security requirements

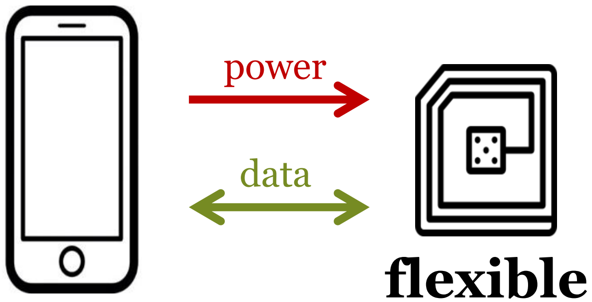
Universiteit Leiden
KU LEUVEN

- Illustrative example to explain the hardware requirements of a lightweight device (e.g. a passive RFID or NFC tag) → reader authentication protocol

Hardware security requirements to protect against a remote adversary?

Hardware security requirements to protect against a physical adversary?

cryptographic key K, stored on the reader



reader

flexible
RFID/NFC tag

cryptographic key K, stored on the tag

Secure key storage

Protection against IP theft

Protection against physical attacks

generate nonce r_A

Nonce generator

r_A

compute $T_1 = PRF_K(r_A)$

T_1

compute $T_2 = PRF_K(r_A)$

Digital crypto circuit ✓

verify $T_1 = T_2$
to authenticate reader

Secure key storage

- Key storage mechanisms:
  - One-time programmable (OTP) memory with fuses
  - Non-volatile memory (e.g. flash)
  - Battery-backed volatile memory (e.g. SRAM)

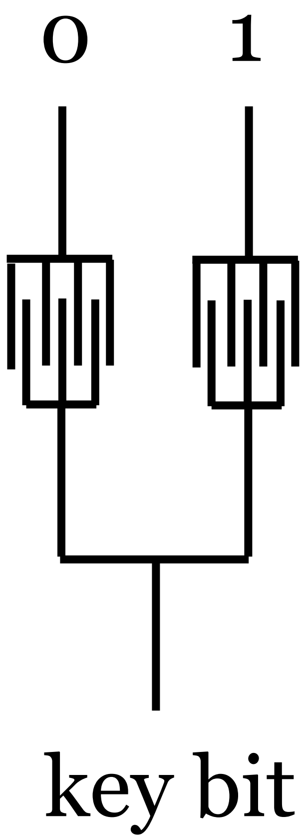
Secure key storage

- Key storage mechanisms:
  - One-time programmable (OTP) memory with fuses
  - ~~Non-volatile memory (e.g. flash)~~
  - ~~Battery-backed volatile memory (e.g. SRAM)~~
- On flexible foil
  - Electrically readable/writable non-volatile memory does not (yet) exist
  - OTP storage mechanisms are the only option (so far)

Secure key storage

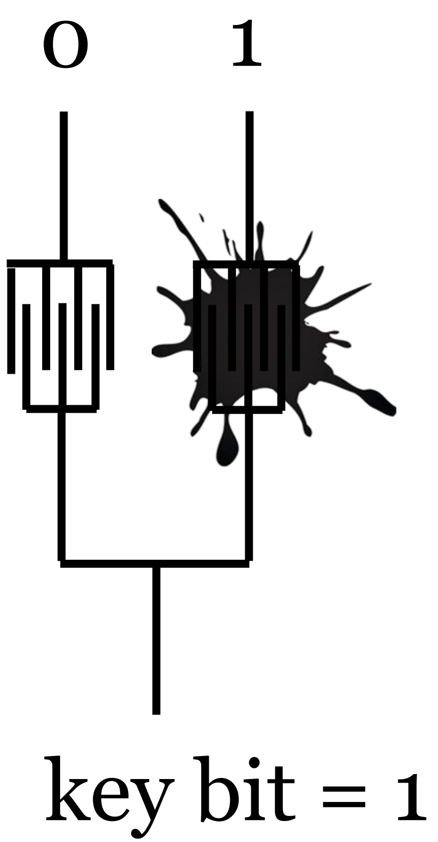
- Key storage mechanisms:
  - One-time programmable (OTP) memory with fuses
  - ~~Non-volatile memory (e.g. flash)~~
  - ~~Battery-backed volatile memory (e.g. SRAM)~~
- On flexible foil
  - Electrically readable/writable non-volatile memory does not (yet) exist
  - OTP storage mechanisms are the only option (so far)
    - Additive method: connect wires with conductive ink
    - Modificative method: cut wires with a laser

Secure key storage
One-time programmable key storage



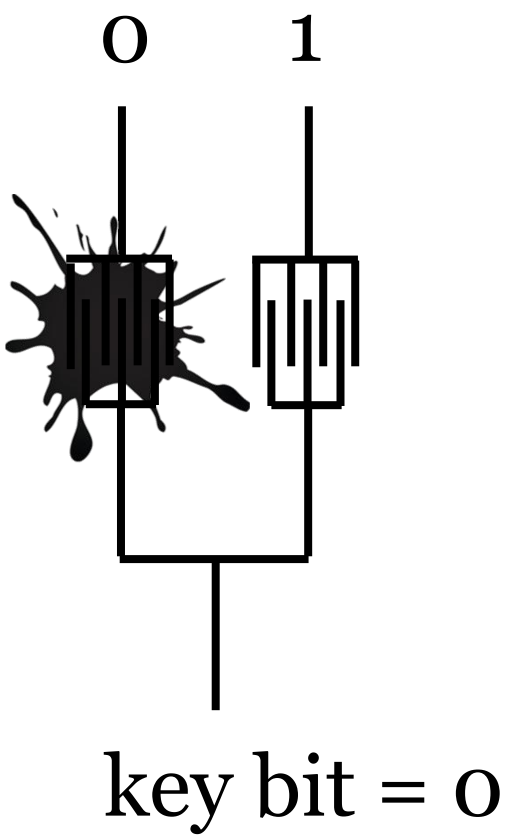
- Additive method:
  - Interdigitated finger structure
  - Connect wires with conductive ink

Secure key storage
One-time programmable key storage



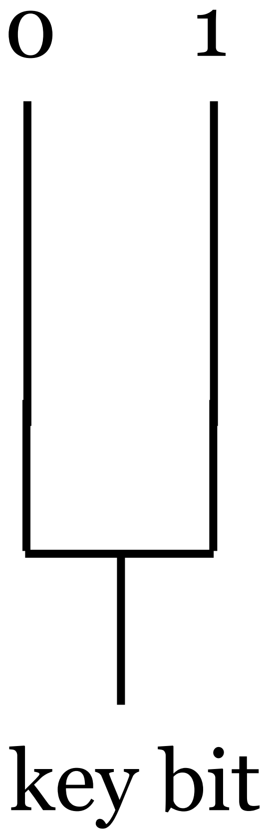
- Additive method:
  - Interdigitated finger structure
  - Connect wires with conductive ink

Secure key storage
One-time programmable key storage



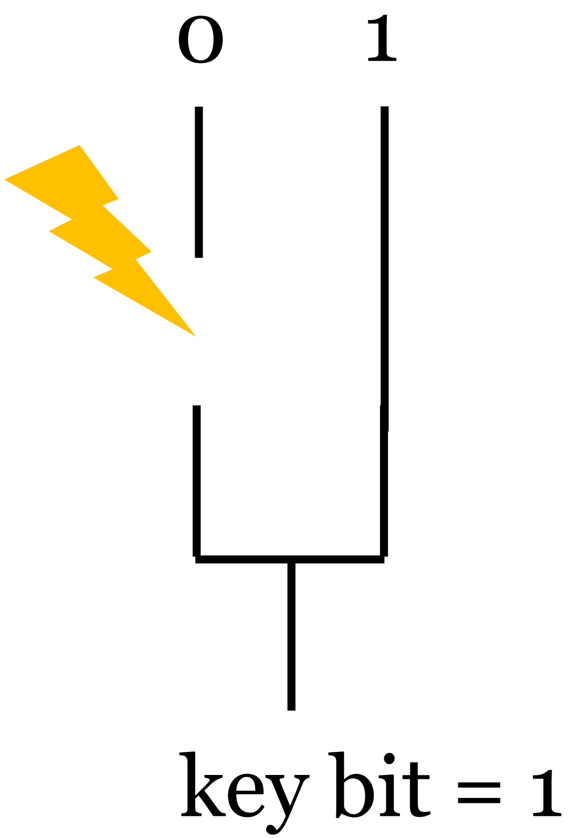
- Additive method:
  - Interdigitated finger structure
  - Connect wires with conductive ink

Secure key storage
One-time programmable key storage



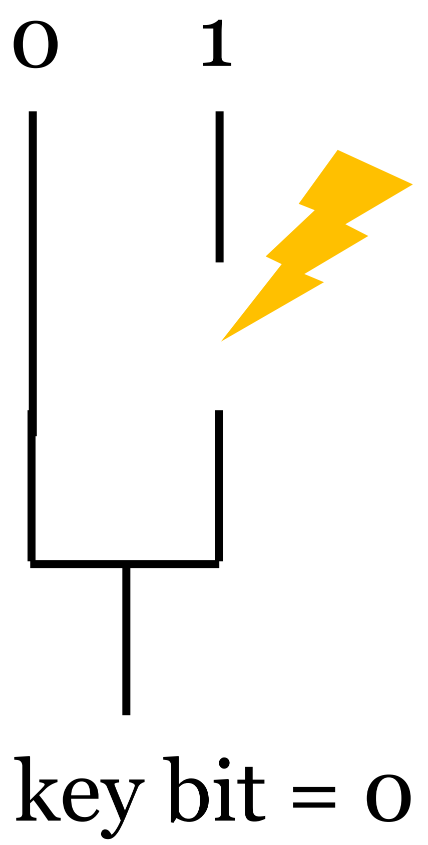
- Additive method:
  - Interdigitated finger structure
  - Connect wires with conductive ink
- Modificative method:
  - Initial connection to 0 and 1
  - Cut wires with a laser

Secure key storage
One-time programmable key storage



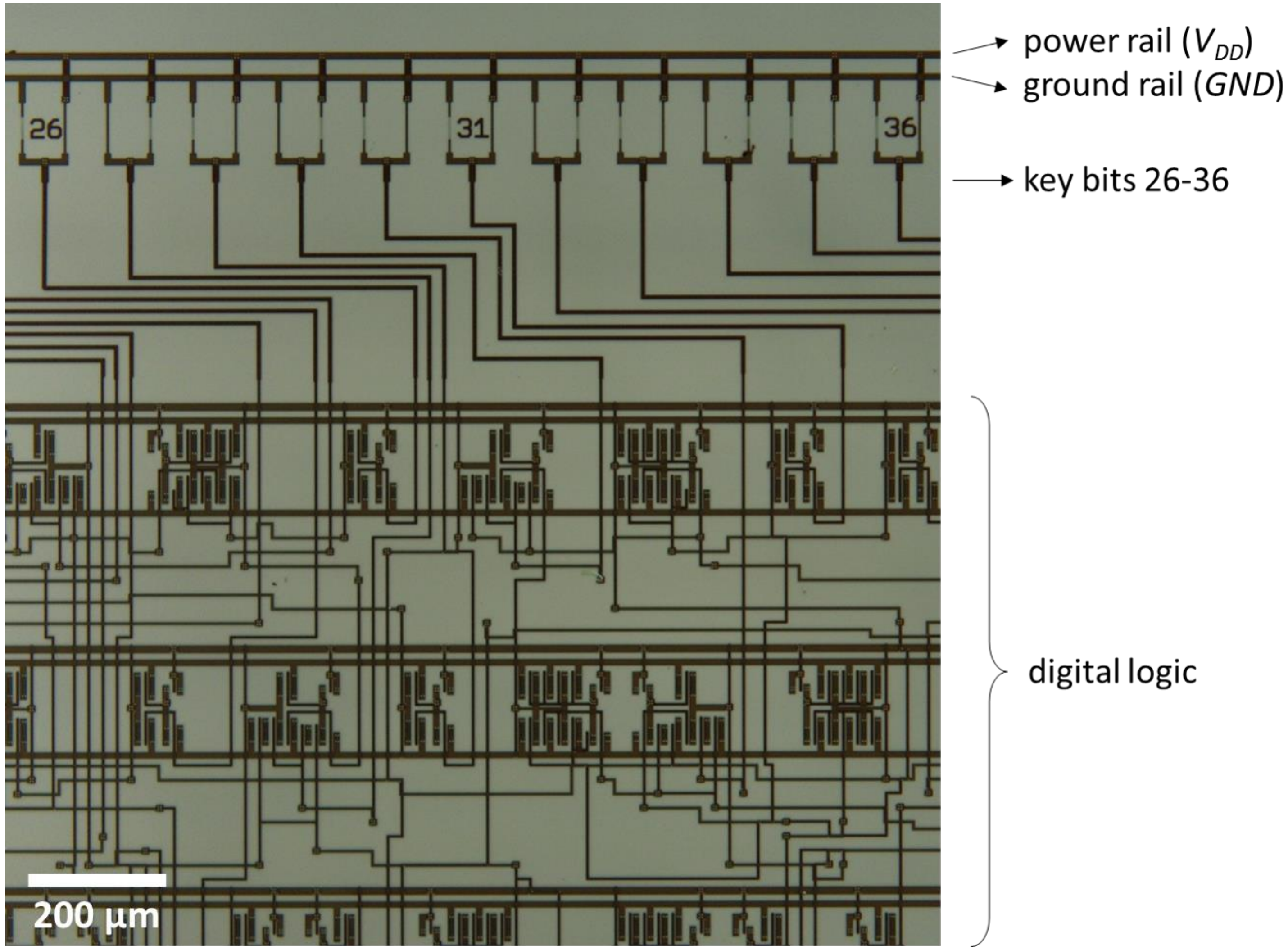
- Additive method:
  - Interdigitated finger structure
  - Connect wires with conductive ink
- Modificative method:
  - Initial connection to 0 and 1
  - Cut wires with a laser

Secure key storage
One-time programmable key storage

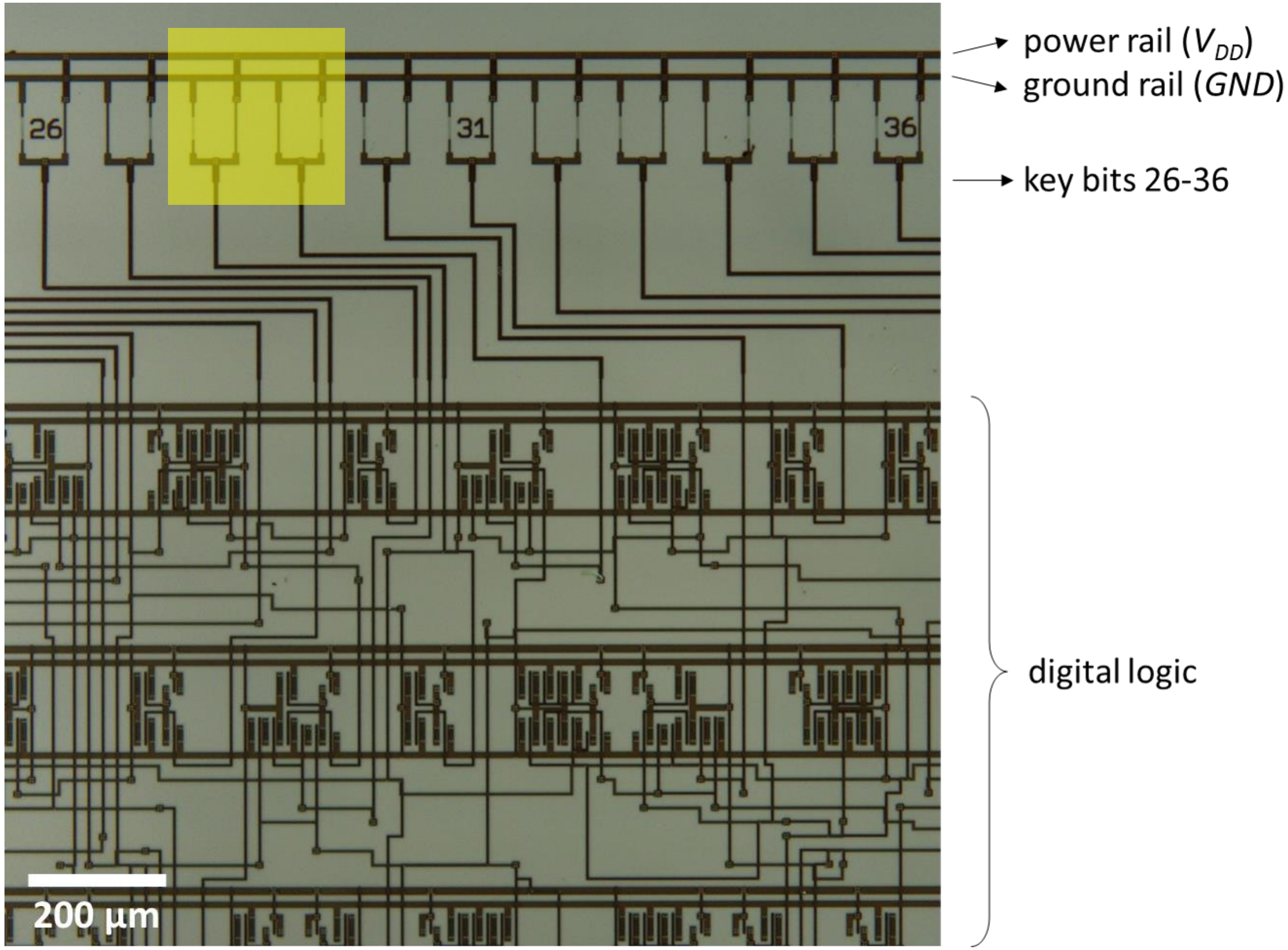


- Additive method:
  - Interdigitated finger structure
  - Connect wires with conductive ink
- Modificative method:
  - Initial connection to 0 and 1
  - Cut wires with a laser

Secure key storage
Modificative method based on lasering

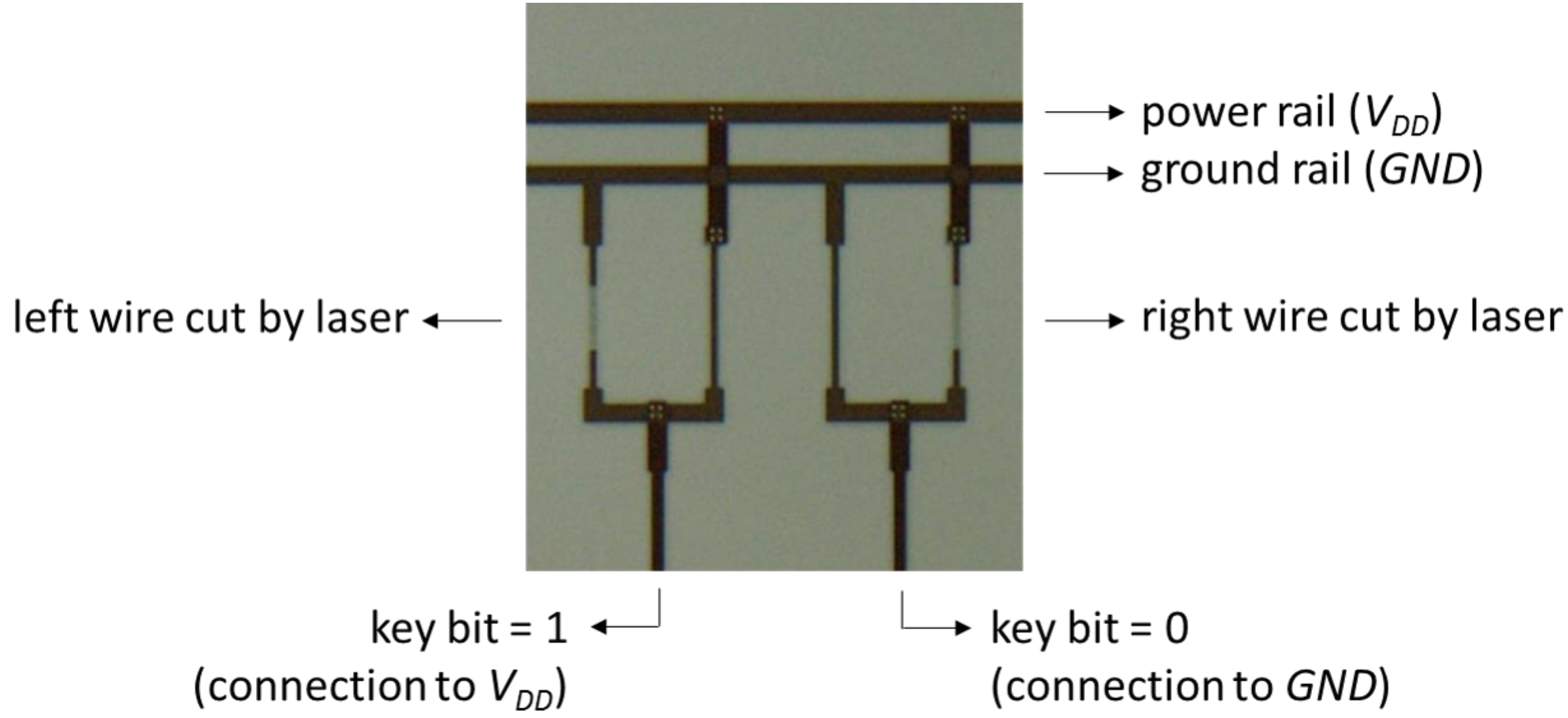


Secure key storage
Modificative method based on lasering



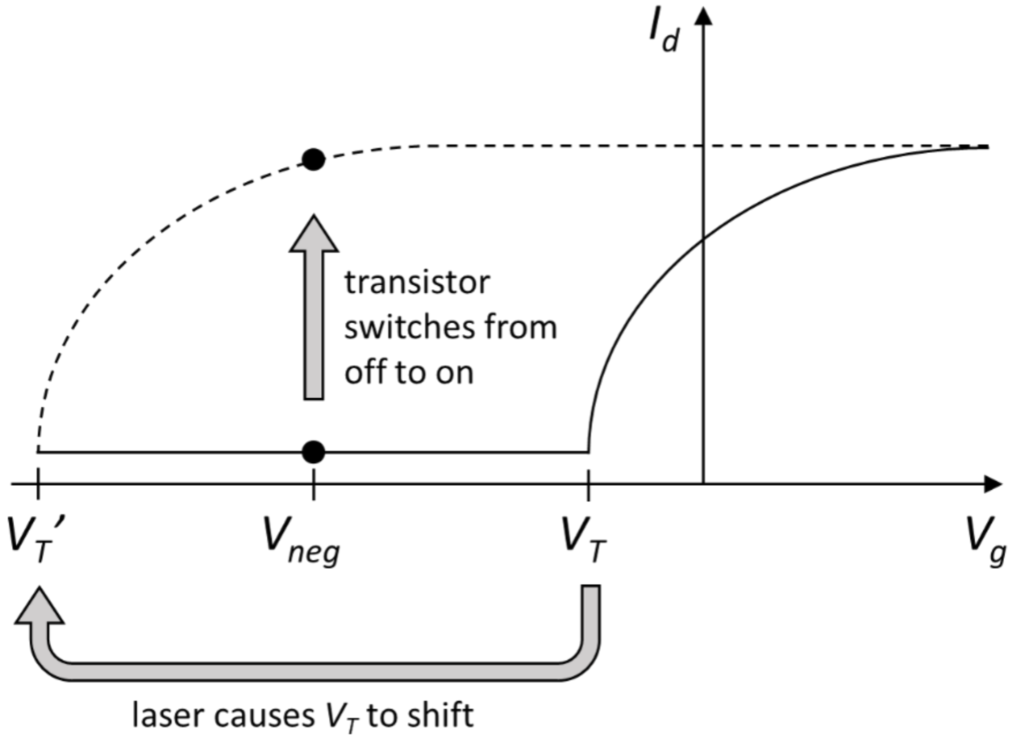
Secure key storage

Modificative method based on lasering



PROBLEM: The key bits can easily be read out using a microscope
(chips are not packaged, features are large)

Secure key storage
Read-out prevention with lasering

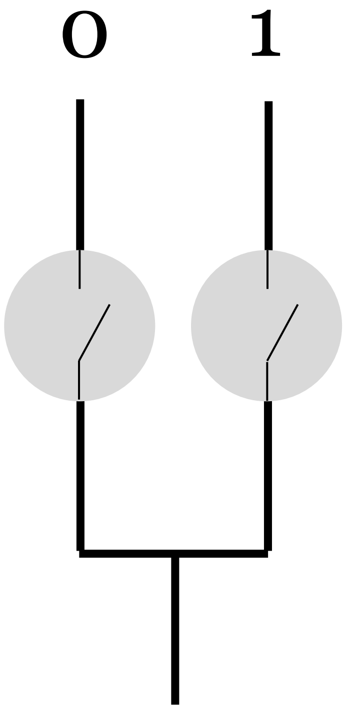


The temperature change caused by lasering, shifts the threshold voltage (V_T) and thus the I_d - V_g graph

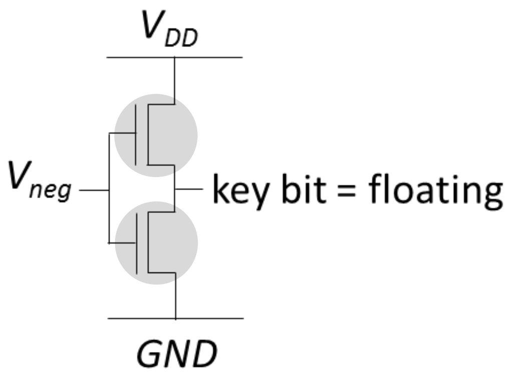
↓

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

Secure key storage
Read-out prevention with lasering

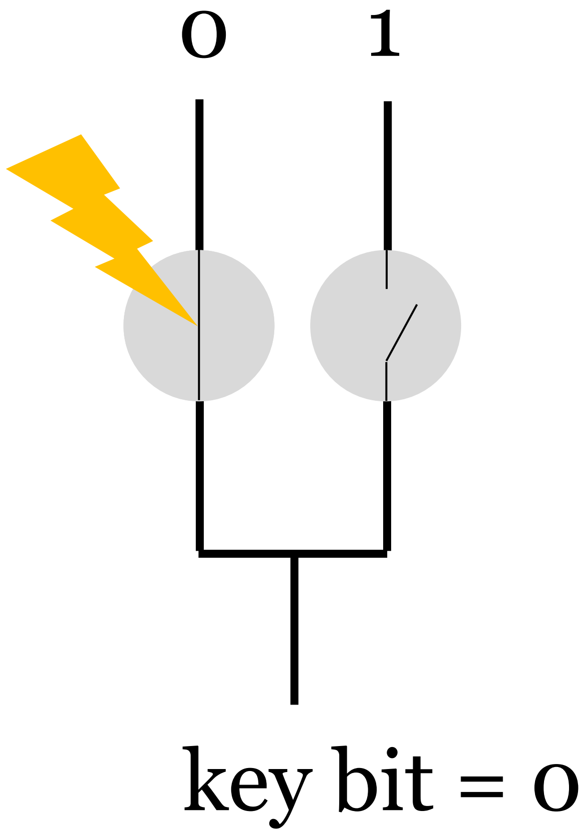


BEFORE LASERING

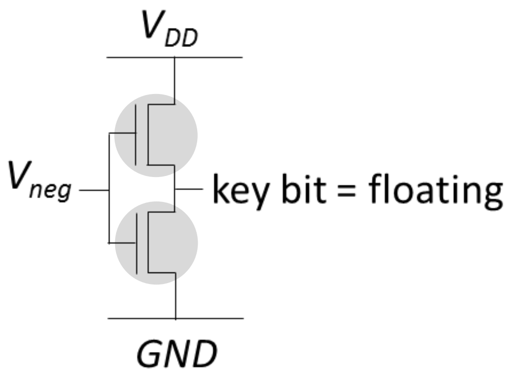


key bit = floating

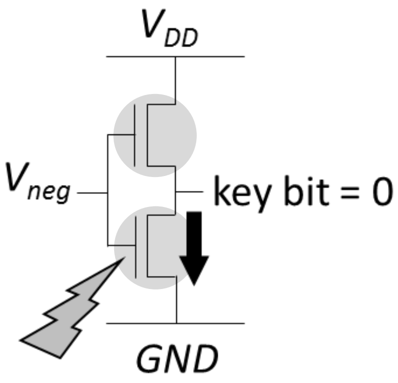
Secure key storage
Read-out prevention with lasering



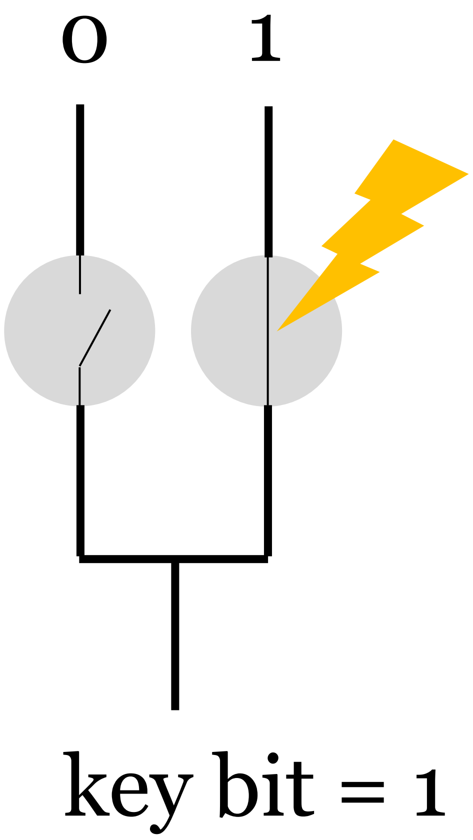
BEFORE LASERING



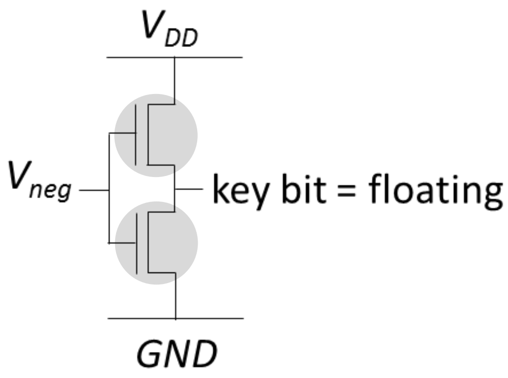
AFTER LASERING



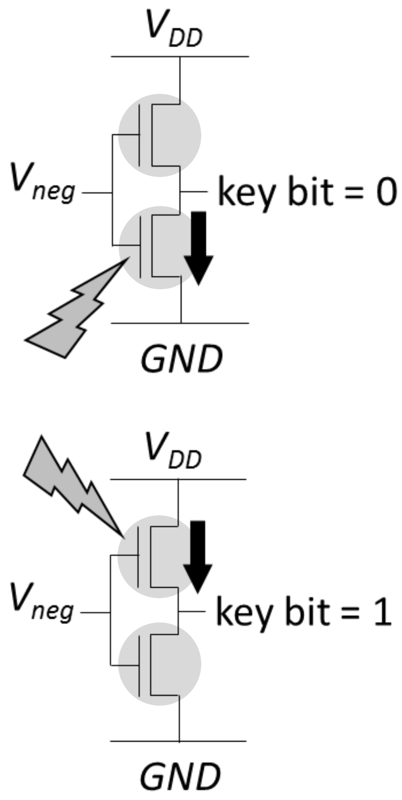
Secure key storage
Read-out prevention with lasering



BEFORE LASERING

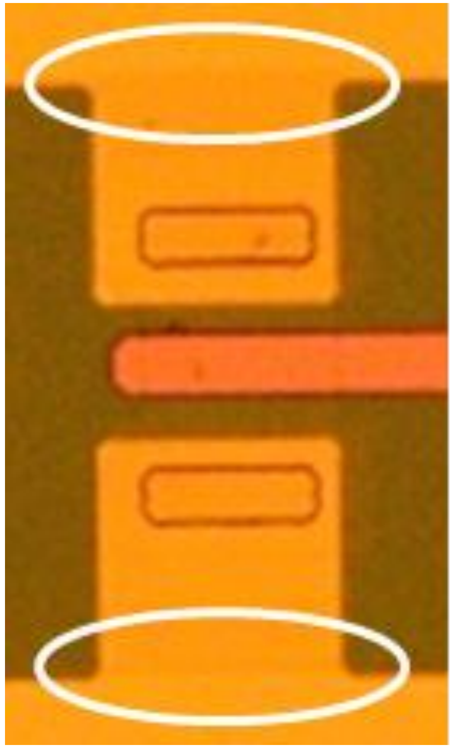


AFTER LASERING

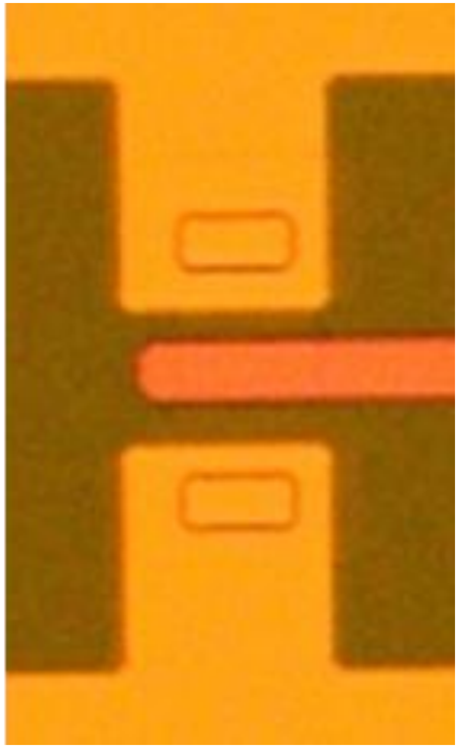


Secure key storage
Read-out prevention with lasering

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

Universiteit Leiden

KU LEUVEN

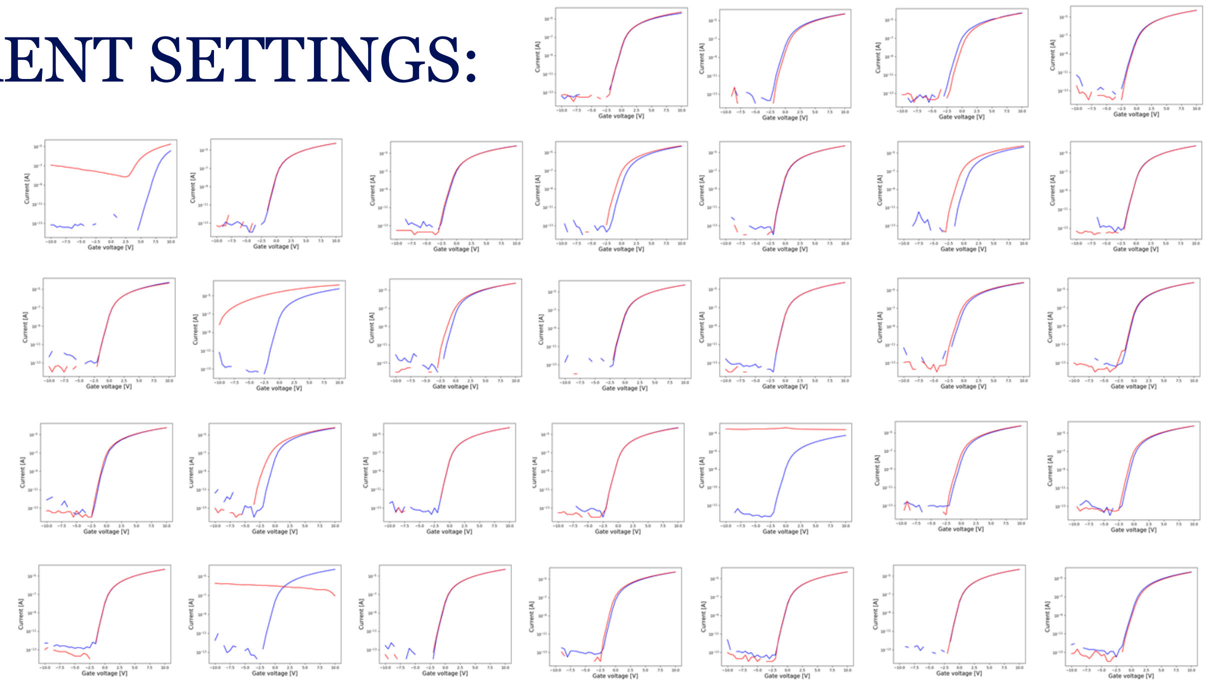
Secure key storage
Read-out prevention with lasering

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



Secure key storage

Read-out prevention with lasering

Universiteit Leiden

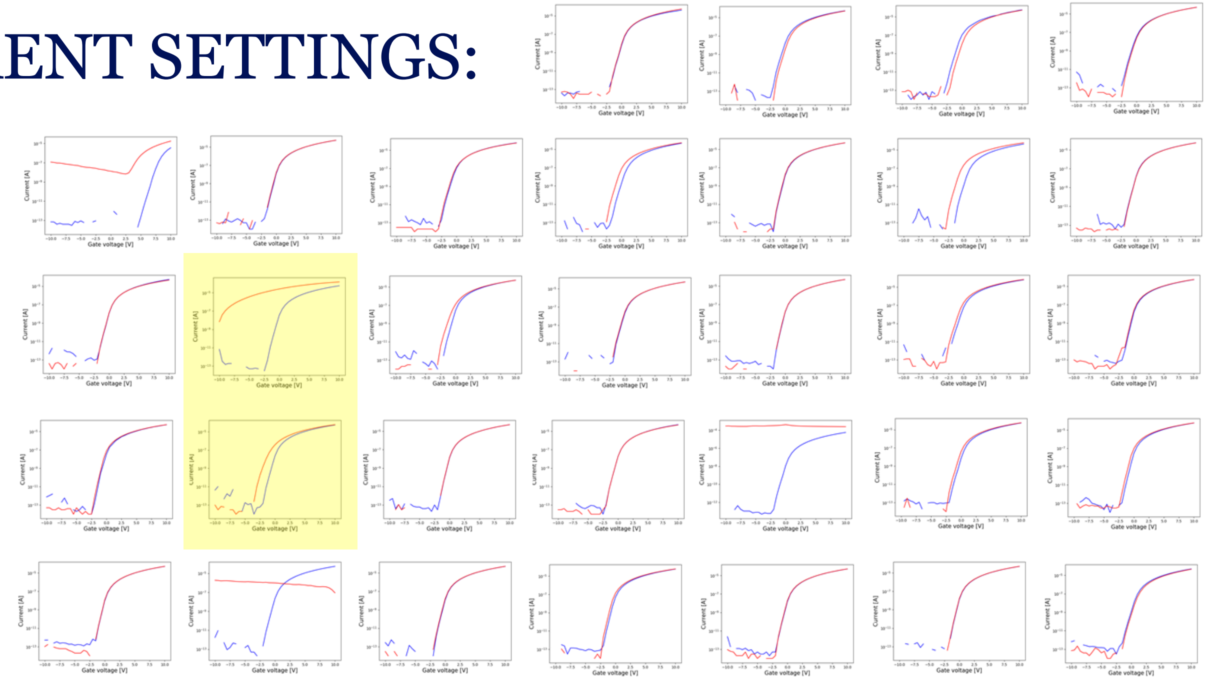
KU LEUVEN

SOLUTION:

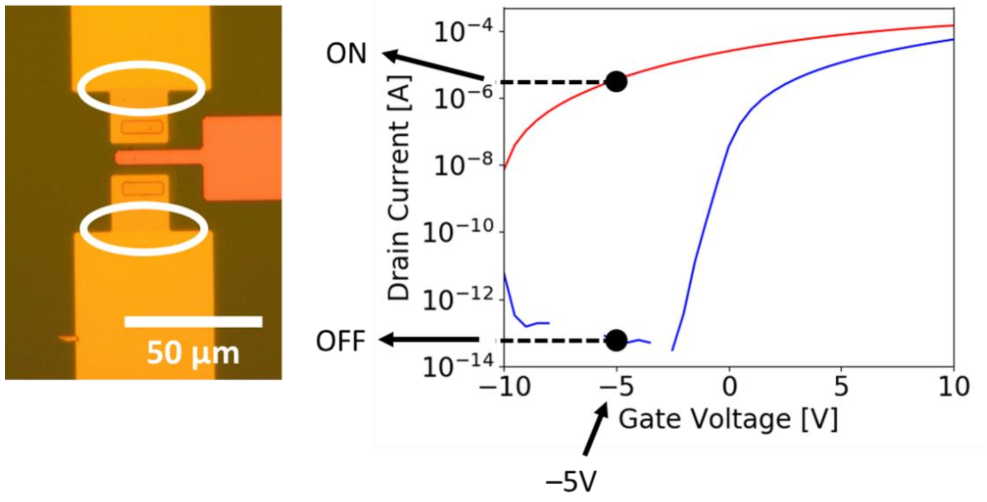
Apply different settings of the laser to cause different V_T shifts that cannot be visually distinguished

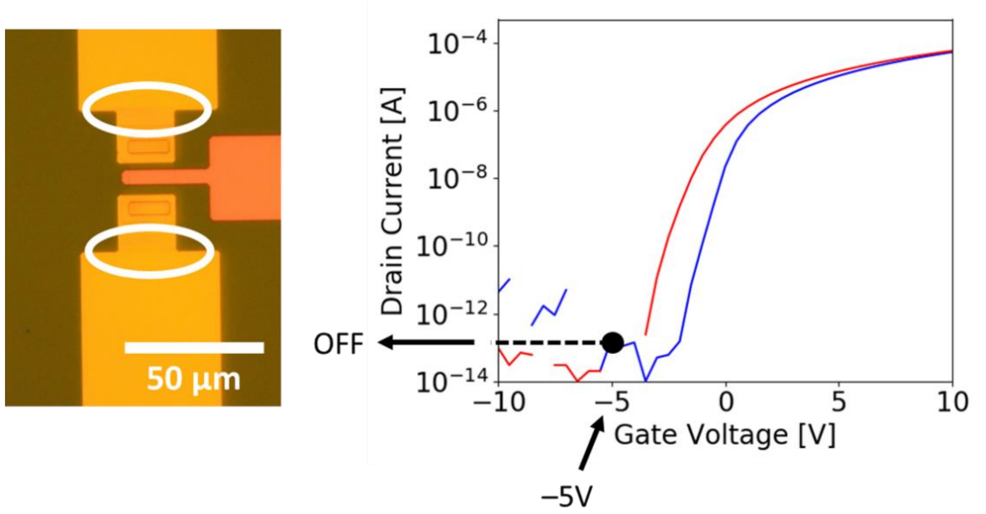
EXPLORATION OF DIFFERENT SETTINGS:

- Blue:
  before lasering
- Red:
  after lasering



Secure key storage
Read-out prevention with lasering





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

Secure key storage

Alternative: Read-out prevention with ink

- 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

Secure key storage

Alternative: Physical(ly) Unclonable Function (PUF)

Universiteit Leiden

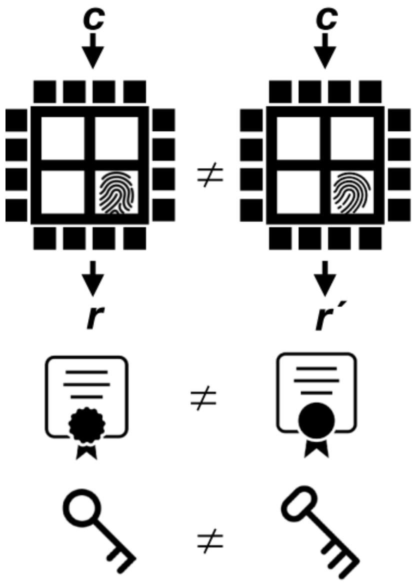
KU LEUVEN

- Physical(ly) Unclonable Functions (PUFs):
  - A PUF generates a unique value based on physical variation
  - The difference with traditional key storage mechanisms is that PUFs do not store a key but generate a key when the power is turned on

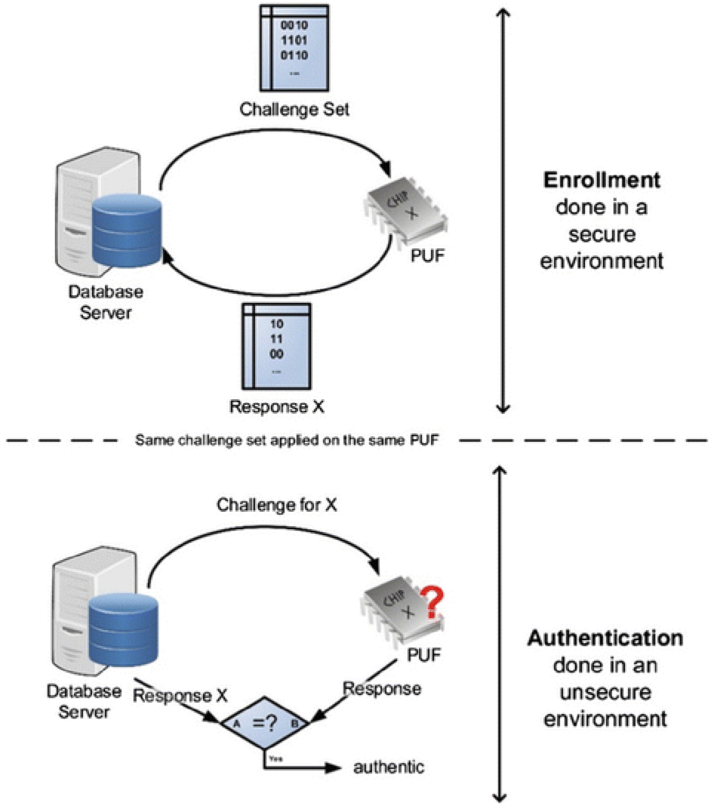
Secure key storage

Alternative: Physical(ly) Unclonable Function (PUF)

- Physical(ly) Unclonable Functions (PUFs) use process variation for:
  - Device-unique key generation
  - Device authentication



Source: Ganji et al., CHES 2019 tutorial



Source: Alioto, M., "Enabling the Internet of Things", 2017

Secure key storage
Alternative: Physical(ly) Unclonable Function (PUF)

Universiteit Leiden

KU LEUVEN

- PUF properties
  - Easy evaluation
  - Uniqueness
  - Reproducibility/reliability
    - Different operating conditions such as temperature and supply voltage
  - Unclonability
  - Unpredictability
  - One-way function
  - Tamper evidence

Secure key storage
Alternative: Physical(ly) Unclonable Function (PUF)

- PUF properties → challenges
  - Easy evaluation
  - Uniqueness
  - Reproducibility/reliability
    - Different operating conditions such as temperature and supply voltage
    - Digital circuits continue to operate correctly when they are bended or stretched, but PUFs might not produce a reliable unique output when bended or stretched
  - Unclonability
  - Unpredictability
  - One-way function
  - Tamper evidence

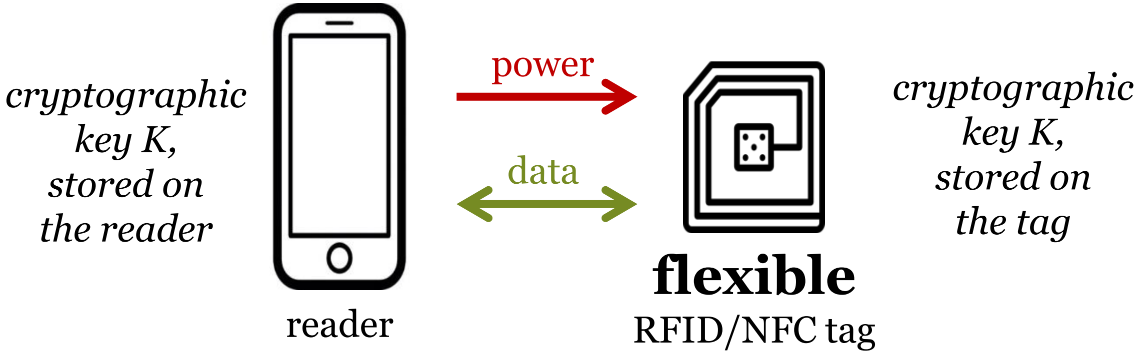
Hardware security requirements

Universiteit Leiden
KU LEUVEN

- Illustrative example to explain the hardware requirements of a lightweight device (e.g. a passive RFID or NFC tag) → reader authentication protocol

Hardware security requirements to protect against a remote adversary?

Hardware security requirements to protect against a physical adversary?



Secure key storage ✓

Protection against IP theft

Protection against physical attacks

generate nonce r_A

r_A ←

Nonce generator

compute $T_1 = PRF_K(r_A)$

T_1 →

compute $T_2 = PRF_K(r_A)$

verify $T_1 = T_2$
to authenticate reader

Digital crypto circuit ✓

Hardware security requirements

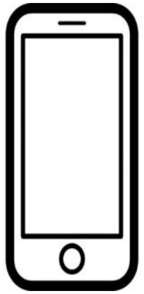
Universiteit Leiden
KU LEUVEN

- Illustrative example to explain the hardware requirements of a lightweight device (e.g. a passive RFID or NFC tag) → reader authentication protocol

Hardware security requirements to protect against a remote adversary?

Hardware security requirements to protect against a physical adversary?

cryptographic key K, stored on the reader



reader

power →

data ↔

flexible
RFID/NFC tag

cryptographic key K, stored on the tag

Secure key storage ✓

Protection against IP theft

Protection against physical attacks

generate nonce r_A

← r_A

Nonce generator

compute $T_1 = PRF_K(r_A)$

T_1 →

compute $T_2 = PRF_K(r_A)$

verify $T_1 = T_2$
to authenticate reader

Digital crypto circuit ✓

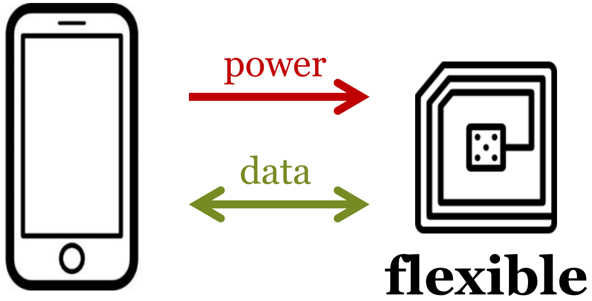
Hardware security requirements

- Illustrative example to explain the hardware requirements of a lightweight device (e.g. a passive RFID or NFC tag) → reader authentication protocol

Hardware security requirements to protect against a remote adversary?

Hardware security requirements to protect against a physical adversary?

cryptographic key K, stored on the reader



reader

RFID/NFC tag

cryptographic key K, stored on the tag

Secure key storage ✓

Protection against IP theft ✓

Protection against physical attacks

generate nonce r_A — Nonce generator

r_A ←

compute $T_1 = PRF_K(r_A)$

T_1 →

compute $T_2 = PRF_K(r_A)$ — Digital crypto circuit ✓

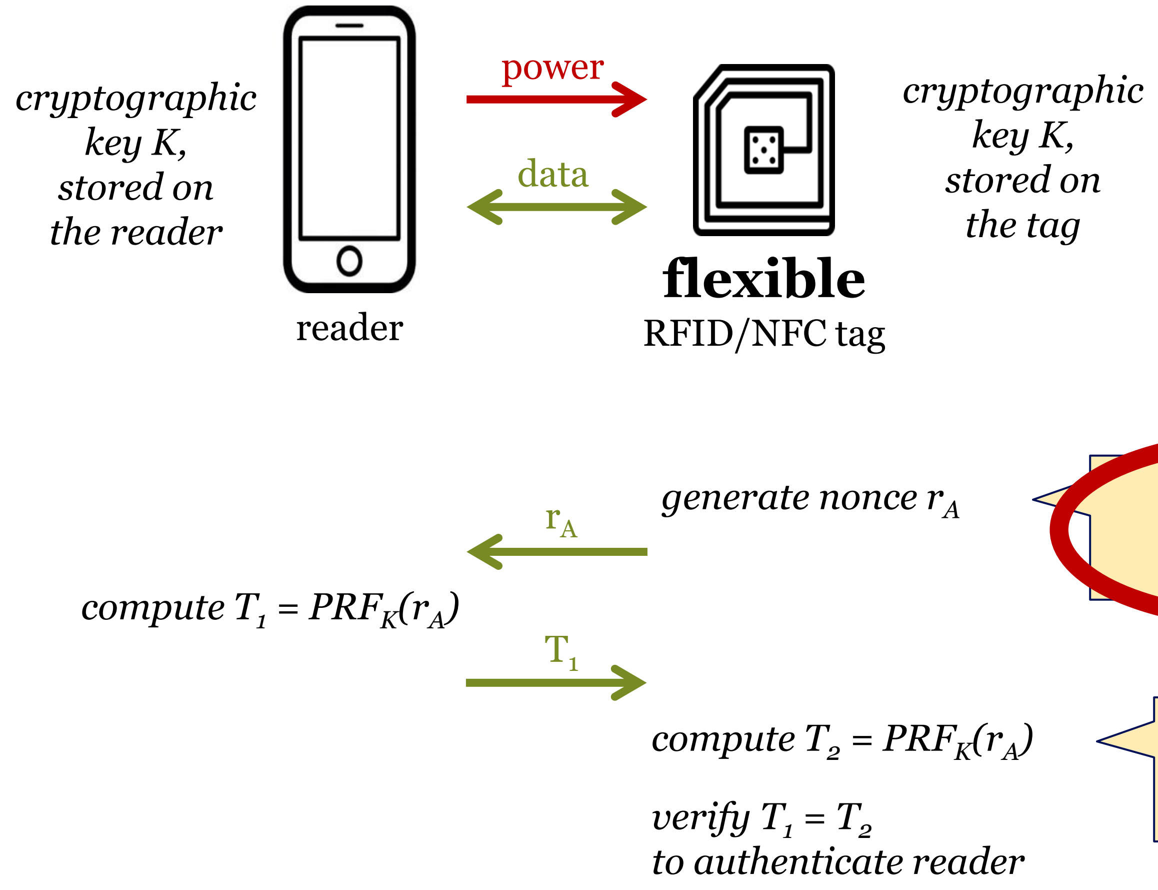
verify $T_1 = T_2$ *to authenticate reader*

Hardware security requirements

- Illustrative example to explain the hardware requirements of a lightweight device (e.g. a passive RFID or NFC tag) → reader authentication protocol

Hardware security requirements to protect against a remote adversary?

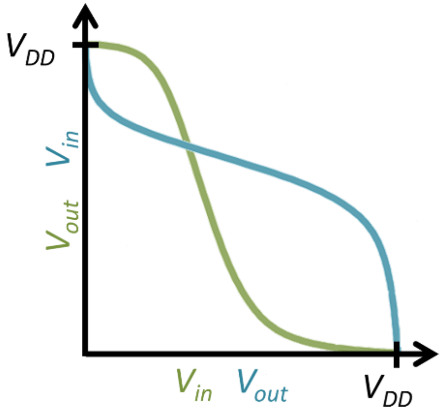
Hardware security requirements to protect against a physical adversary?



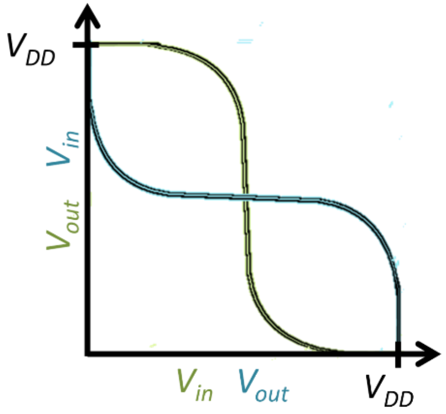
- Secure key storage ✓
- Protection against IP theft ✓
- Protection against physical attacks
- Nonce generator
- Digital crypto circuit ✓

Nonce generator

- To generate a nonce, we either need a True Random Number Generator (TRNG) or non-volatile storage
  - Electrically readable/writable non-volatile memory does not exist (yet) in the considered technology
  - 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 explored



pseudo-CMOS



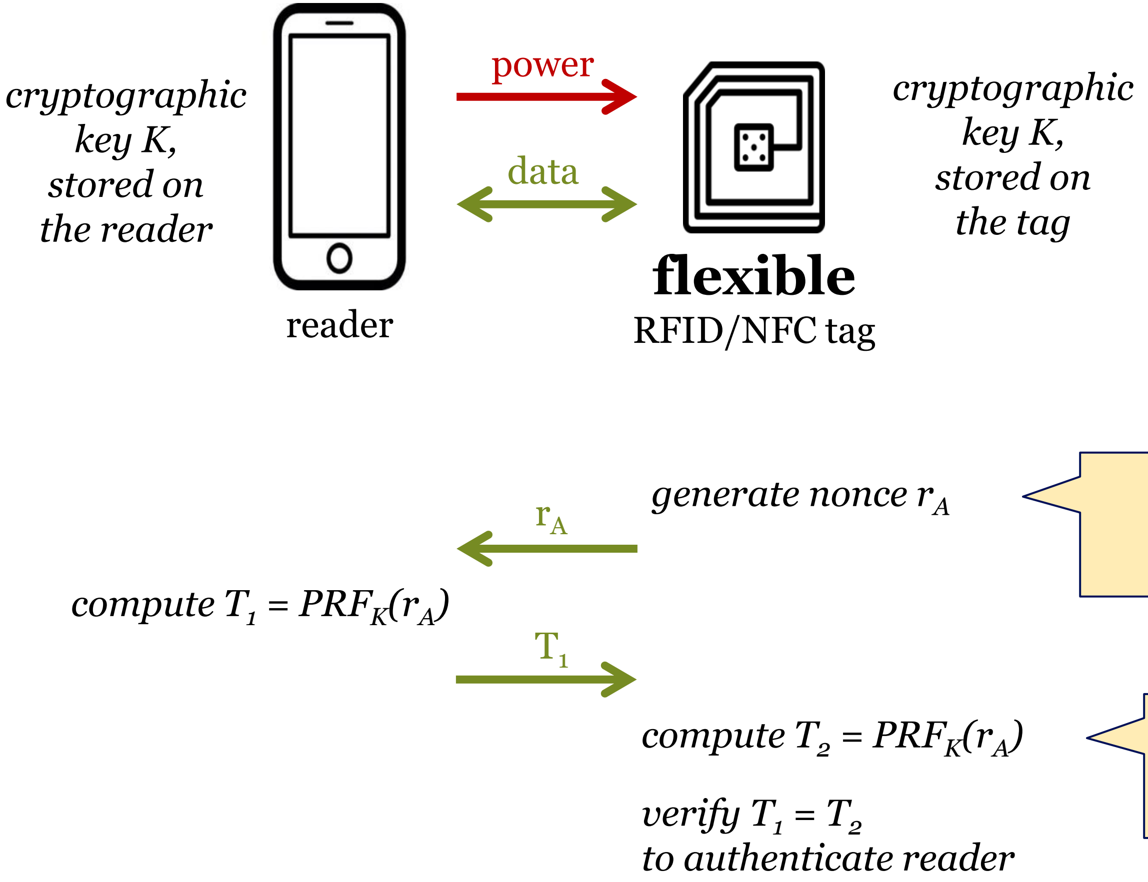
CMOS

Hardware security requirements

- Illustrative example to explain the hardware requirements of a lightweight device (e.g. a passive RFID or NFC tag) → reader authentication protocol

Hardware security requirements to protect against a remote adversary?

Hardware security requirements to protect against a physical adversary?



Secure key storage ✓

Protection against IP theft ✓

Protection against physical attacks

Nonce generator ?

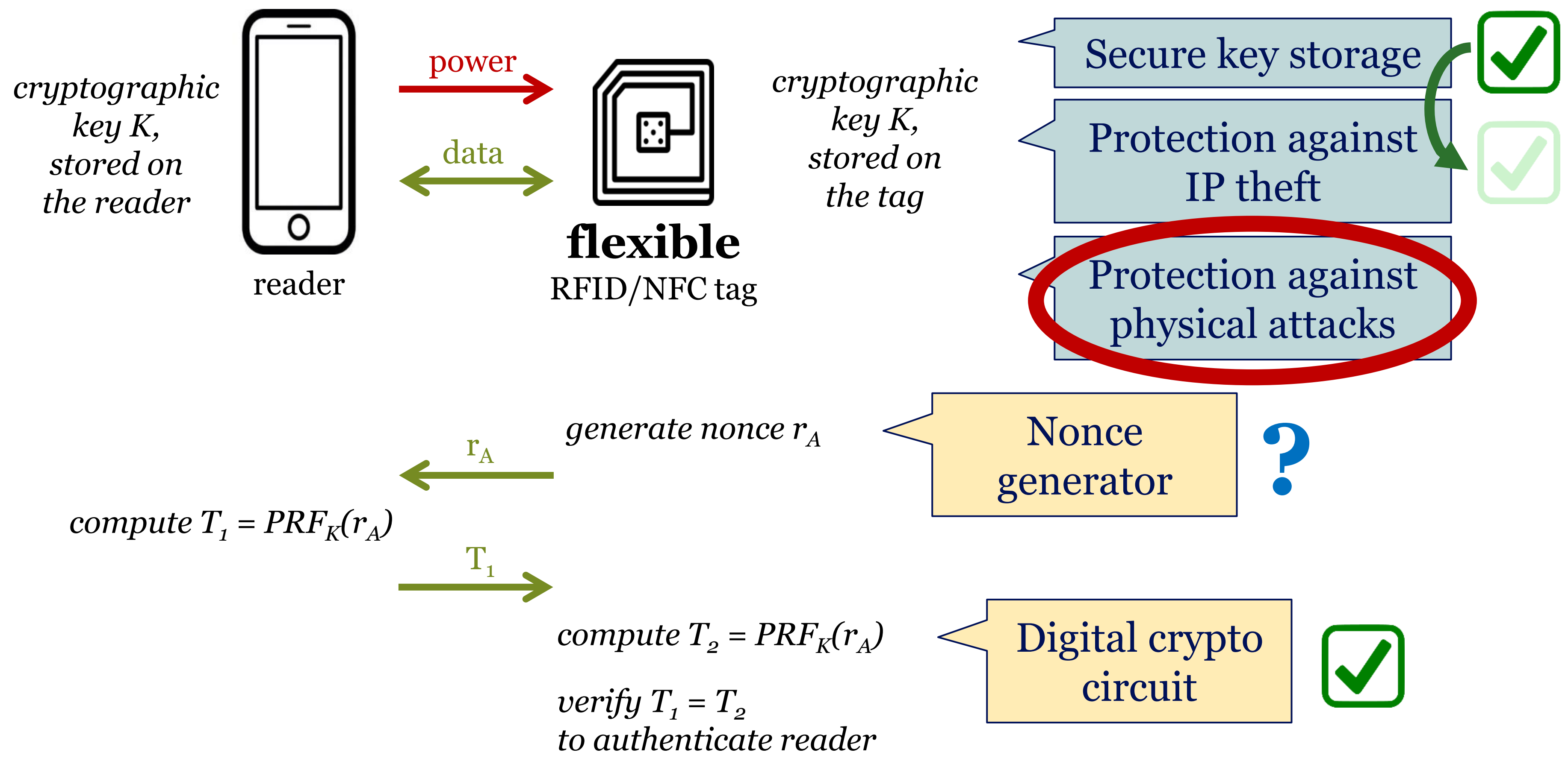
Digital crypto circuit ✓

Hardware security requirements

- Illustrative example to explain the hardware requirements of a lightweight device (e.g. a passive RFID or NFC tag) → reader authentication protocol

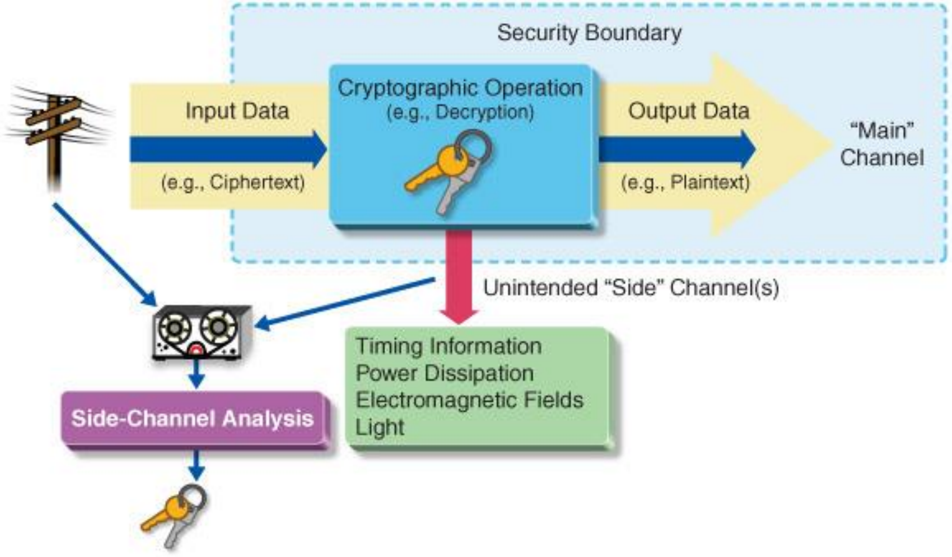
Hardware security requirements to protect against a remote adversary?

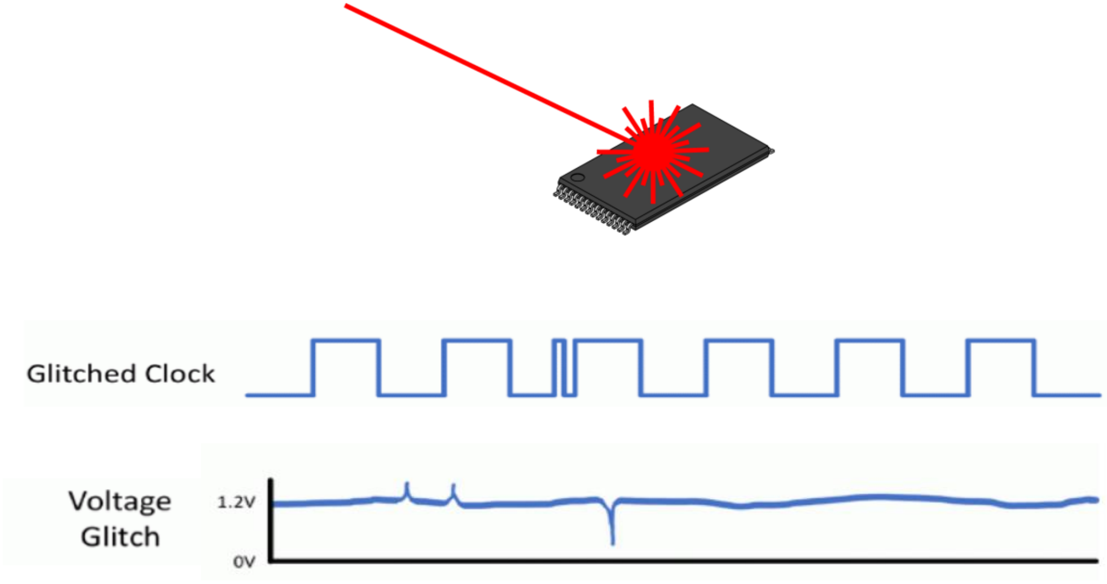
Hardware security requirements to protect against a physical adversary?



Physical attacks

- Side-channel analysis attacks extract secret information from side channels
- Fault analysis attacks introduce computational errors to expose secret information



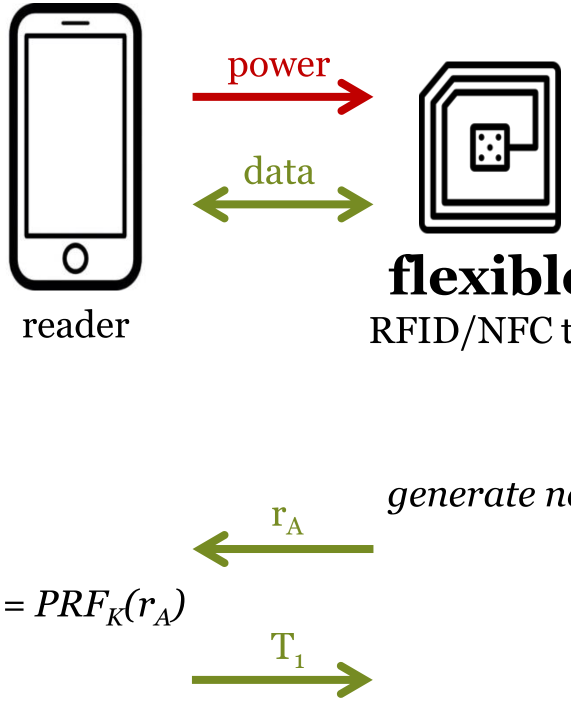


Hardware security requirements

- Illustrative example to explain the hardware requirements of a lightweight device (e.g. a passive RFID or NFC tag) → reader authentication protocol

Hardware security requirements to protect against a remote adversary?

Hardware security requirements to protect against a physical adversary?



Remaining challenges

- The delay of the authentication protocol needs to be compliant to NFC standards
- Mutual authentication causes an even longer delay
- Public-key cryptography requires even more transistors

Security challenges and opportunities in emerging device technologies

A case study on flexible electronics

State of the art

Emerging device	PUF	TRNG	Crypto	SCA	FA	Obfus.
Memristor	✓	✓	✓			
FD-SOI	✓	✓	✓	✓	✓	
Flex electronics						
- EGFET	✓	✓				
- Organic TFT	✓					
- Metal-oxide TFT			✓			✓

State of the art

Emerging device	PUF	TRNG	Crypto	SCA	FA	Obfus.
Memristor	✓	✓	✓			
FD-SOI	✓	✓	✓	✓	✓	
Flex electronics						
- EGFET	✓	✓				
- Organic TFT	✓					
- Metal-oxide TFT			✓			✓

[3] Yang et al., “Memristor-based chaotic circuit for text/image encryption and decryption,” ISCID, 2015.

[4] Mishra et al., “Memristor based cryptographic information processing for secured communication systems,” ICCSD, 2020.

State of the art

Emerging device	PUF	TRNG	Crypto	SCA	FA	Obfus.
Memristor	✓	✓	✓			
FD-SOI	✓	✓	✓	✓	✓	
Flex electronics						
- EGFET	✓	✓				
- Organic TFT	✓					
- Metal-oxide TFT			✓			✓

[5] Wang et al., "A novel true random number generator design leveraging emerging memristor technology," GLSVLSI, 2015.

[6] Uddin et al., "On the theoretical analysis of memristor based true random number generator," GLSVLSI, 2019.

State of the art

Emerging device	PUF	TRNG	Crypto	SCA	FA	Obfus.
Memristor	✓	✓	✓			
FD-SOI	✓	✓	✓	✓	✓	
Flex electronics						
- EGFET	✓	✓				
- Organic TFT	✓					
- Metal-oxide TFT			✓			✓

[7] Liu et al., “A highly reliable and tamper-resistant RRAM PUF: Design and experimental validation,” HOST, 2016.

[8] Uddin et al., “Techniques for improved reliability in memristive crossbar PUF circuits,” ISVLSI, 2016.

[9] Pang et al., “A novel PUF against machine learning attack: Implementation on a 16 Mb RRAM chip,” IEDM, 2017.

[10] Koeberl et al., “Memristor PUFs: a new generation of memory-based physically unclonable functions,” DATE, 2013.

[11] Rose et al., “Foundations of memristor based PUF architectures,” NANOARCH, 2013.

State of the art

Universiteit Leiden

KU LEUVEN

Emerging device	PUF	TRNG	Crypto	SCA	FA	Obfus.
Memristor	✓	✓	✓			
FD-SOI	✓	✓	✓	✓	✓	
Flex electronics						
- EGFET	✓	✓				
- Organic TFT	✓					
- Metal-oxide TFT			✓			✓

[12] Chatterjee et al., "Memristor based arbiter PUF: Cryptanalysis threat and its mitigation," VLSID, 2016.

[13] Govindaraj and Ghosh, "A strong arbiter PUF using resistive RAM within 1T-1R memory architecture," ICCD, 2016.

[14] Uddin et al., "Robustness analysis of a memristive crossbar PUF against modeling attacks," IEEE TNANO, 2017.

[15] Zeitouni et al., "On the security of strong memristor-based physically unclonable functions," DAC, 2020.

State of the art

Universiteit Leiden

KU LEUVEN

Emerging device	PUF	TRNG	Crypto	SCA	FA	Obfus.
Memristor	✓	✓	✓			
FD-SOI	✓	✓	✓	✓	✓	
Flex electronics						
- EGFET	✓	✓				
- Organic TFT	✓					
- Metal-oxide TFT			✓			✓

[16] Danger et al., “Analysis of mixed PUF-TRNG circuit based on SR-latches in FD-SOI technology,” DSD, 2018.

State of the art

Universiteit Leiden

KU LEUVEN

Emerging device	PUF	TRNG	Crypto	SCA	FA	Obfus.
Memristor	✓	✓	✓			
FD-SOI	✓	✓	✓	✓	✓	
Flex electronics						
- EGFET	✓	✓				
- Organic TFT	✓					
- Metal-oxide TFT			✓			✓

[17] Dutertre et al., "Sensitivity to laser fault injection: CMOS FD-SOI vs. CMOS bulk," IEEE TDMR, 2018.

State of the art

Emerging device	PUF	TRNG	Crypto	SCA	FA	Obfus.
Memristor	✓	✓	✓			
FD-SOI	✓	✓	✓	✓	✓	
Flex electronics						
- EGFET	✓	✓				
- Organic TFT	✓					
- Metal-oxide TFT			✓			✓

[18] Kamel et al., “Side-channel analysis of a learning parity with physical noise processor,” JCEN, 2020.

State of the art

Emerging device	PUF	TRNG	Crypto	SCA	FA	Obfus.
Memristor	✓	✓	✓			
FD-SOI	✓	✓	✓	✓	✓	
Flex electronics						
- EGFET	✓	✓				
- Organic TFT	✓					
- Metal-oxide TFT			✓			✓

[19] Beckers et al., "Energy and side-channel security evaluation of near-threshold cryptographic circuits in 28nm FD-SOI technology," ACM CF, 2022.

State of the art

Emerging device	PUF	TRNG	Crypto	SCA	FA	Obfus.
Memristor	✓	✓	✓			
FD-SOI	✓	✓	✓	✓	✓	
Flex electronics						
- EGFET	✓	✓				
- Organic TFT	✓					
- Metal-oxide TFT			✓			✓

[20] Erozan et al., "Design and evaluation of physical unclonable function for inorganic printed electronics," ISQED, 2018.

[21] Erozan et al., "Inkjet-printed EGFET-based physical unclonable function—design, evaluation, and fabrication," IEEE TVLSI, 2018.

State of the art

Emerging device	PUF	TRNG	Crypto	SCA	FA	Obfus.
Memristor	✓	✓	✓			
FD-SOI	✓	✓	✓	✓	✓	
Flex electronics						
- EGFET	✓	✓				
- Organic TFT	✓					
- Metal-oxide TFT			✓			✓

[22] Erozan et al., “A compact low-voltage true random number generator based on inkjet printing technology,” IEEE TVLSI, 2020.

State of the art

Emerging device	PUF	TRNG	Crypto	SCA	FA	Obfus.
Memristor	✓	✓	✓			
FD-SOI	✓	✓	✓	✓	✓	
Flex electronics						
- EGFET	✓	✓				
- Organic TFT	✓					
- Metal-oxide TFT			✓			✓

[23] Kuribara et al., "Organic physically unclonable function on flexible substrate operable at 2 V for IoT/IoE security applications," Organic Electronics, 2017.

State of the art

Emerging device	PUF	TRNG	Crypto	SCA	FA	Obfus.
Memristor	✓	✓	✓			
FD-SOI	✓	✓	✓	✓	✓	
Flex electronics						
- EGFET	✓	✓				
- Organic TFT	✓					
- Metal-oxide TFT			✓			✓

[24] Mentens et al., "Security on plastics: Fake or real?" TCHES, 2019.

State of the art

Emerging device	PUF	TRNG	Crypto	SCA	FA	Obfus.
Memristor	✓	✓	✓			
FD-SOI	✓	✓	✓	✓	✓	
Flex electronics						
- EGFET	✓	✓				
- Organic TFT	✓					
- Metal-oxide TFT			✓			✓

Overview in:

[25] Batina et al., “Invited: Security Beyond Bulk Silicon: Opportunities and Challenges of Emerging Devices”, DAC, 2021.

Thanks! Questions?

Nele Mentens

n.mentens@liacs.leidenuniv.nl / nele.mentens@kuleuven.be