Lightweight Security Solutions for IoT Implementations in Space

TECHNISCHE UNIVERSITÄT DARMSTADT

IEEE IoT Summit at RWW2019: "The Internet of Things Meets the Internet of Space"
20-21 January 2019 // Orlando, Florida, USA

Nikolaos Athanasios Anagnostopoulos, Yufan Fan, Tolga Arul,
Ravi Sarangdhar and Stefan Katzenbeisser

Security Engineering Group
Department of Computer Science
Technische Universität Darmstadt

IEEE IEEE Internet of Things MTT-S RWW SecEng Security Engineering

Outline

IoT in Space

TECHNISCHE UNIVERSITÄT DARMSTADT

- Commercial Off The Shelf (COTS) devices are cost-efficient due to economies of scale

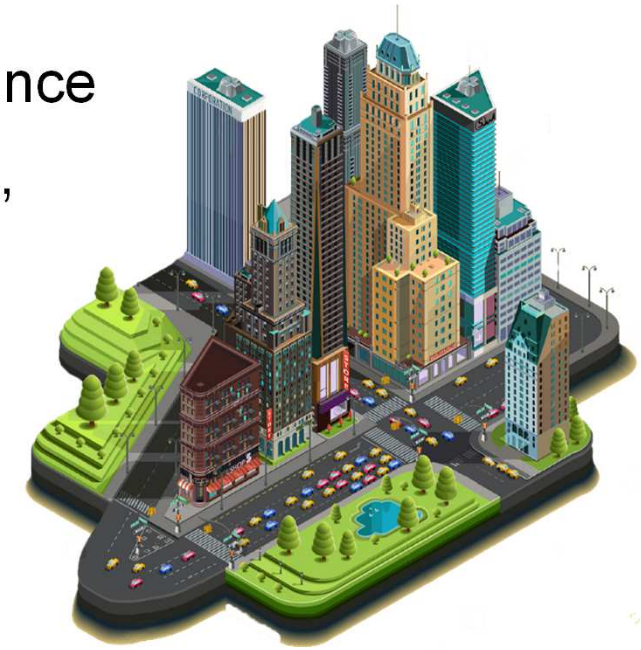
- COTS devices are resilient to:
  - Temperature variations (-110°C … 80°C)
  - Radiation 2000 gray (200 krad)

- These properties make COTS devices suitable for near-earth space applications

IOT IN SPACE

IoT on Earth

- Home-Automation, personal assistance, surveillance emergency notification, remote health monitoring, power metering, power generation control
- Wearables
- Traffic control, fleet management, toll collection, vehicle control, tracking, shipping, transport
- Asset management, predictive maintenence, m2m communication, process control, supply chain management
- Environmental monitoring
- Agriculture
- …



IOT IN SPACE

IoT in Space

TECHNISCHE UNIVERSITÄT DARMSTADT

- All services but in remote and underserved areas of the world
- Use of satellites, enabled by:
  - Continued scaling
  - Reduced cost
  - Advances in high-data-rate wireless communication
- Deployment in suborbit
  - Lower launching cost
  - Lower latency
  - Integration with terrestrial networks

IOT IN SPACE

Current Ventures

TECHNISCHE UNIVERSITÄT DARMSTADT

Organization(s)	Purpose
AWS, Iridium	...develop a satellite-based network called CloudConnect, designed specifically for IoT applications.
Orbcomm, APNTS	Construction of a China Gateway Earth Station (GES) to serve as a network link between the satellite system and worldwide infrastructure for M2M communication
SemTech, Alibaba Cloud	logistics tracking, air quality, food safety compliance, smoke detecting safety, smart meters, smart cities, smart manufacturing, smart agriculture
IOTEE	Coming first on a market set to have a total of 2 billion LPWA device units by 2022

IOT IN SPACE

Attacks on IoT

TECHNISCHE UNIVERSITÄT DARMSTADT

- Manipulation of sensor values
- Node subversion, capture, outage → Botnets, DDoS
- MITM
- …

→ PUFs to the rescue!

IOT IN SPACE

Introduction to PUFs

TECHNISCHE UNIVERSITÄT DARMSTADT

Physical Unclonable Functions (PUFs):

Physical: Based on physical variation during semiconductor manufacturing in integrated circuits, physical structure

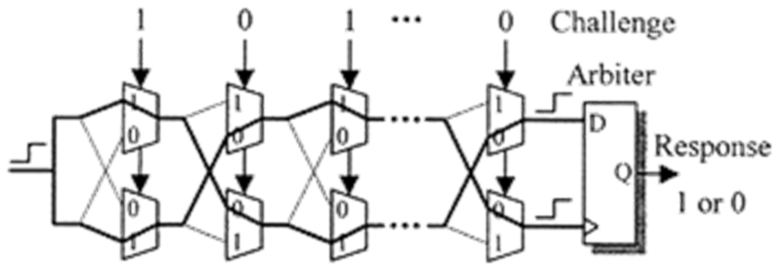
Unclonable: With high probability two physical structures of the same production process do not have exactly the same properties

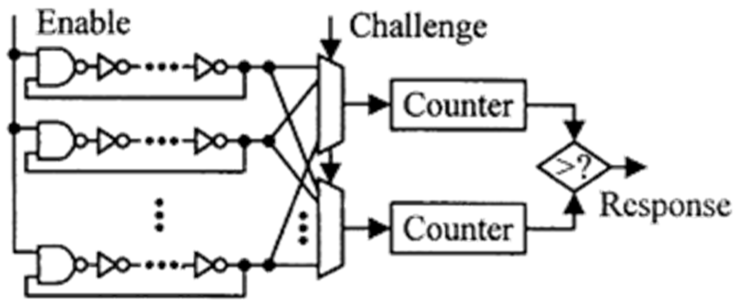
Function: Each device implements a different function;
for every input x there is a specific output y
(up to some noise handled by error correction)

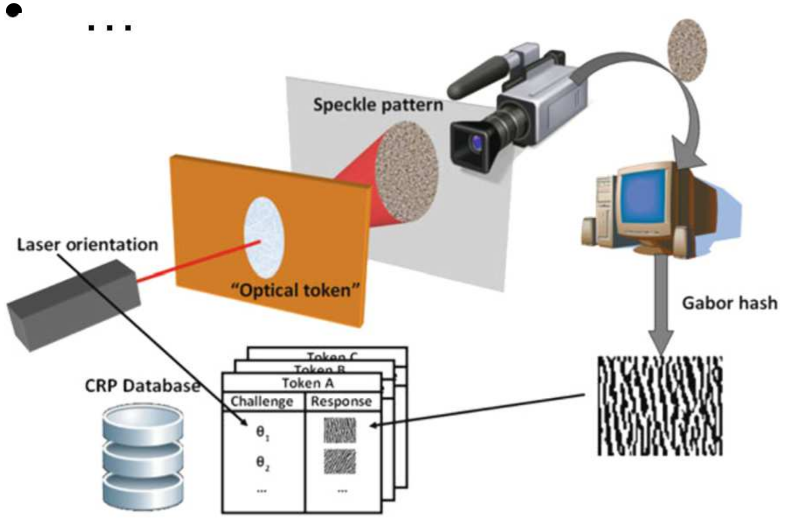
Introduction to PUFs:
PUF Types

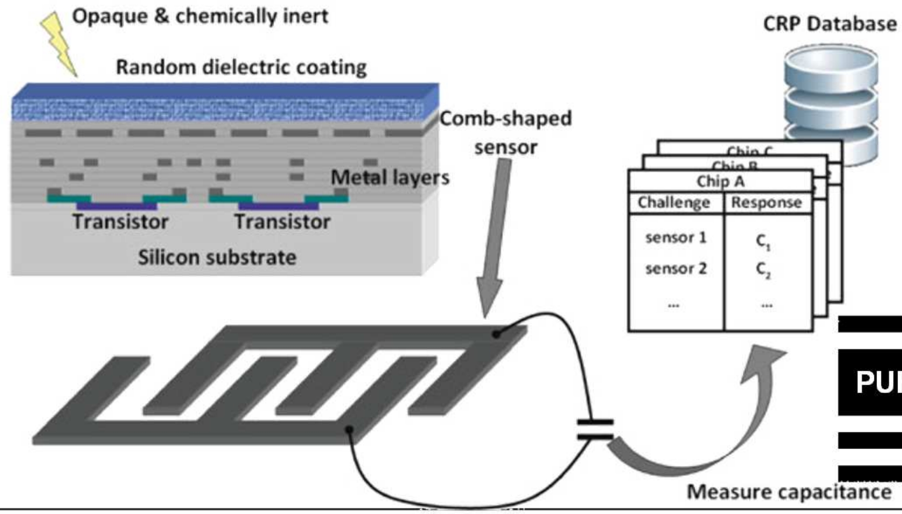
Different PUF structures:

- Memory-based: SRAM, DRAM, Flash
- Delay-based: Arbiter, Ring-oscillator
- Optical
- Coating
- …









PUF INTRO

Introduction to PUFs: Working principles

Utilization of different physical phenomena:

- SRAM:
  - Startup values
  - Retention and rowhammer
- DRAM:
  - Startup values
  - Retention
  - Retention and rowhammer
  - Remanence
  - Access latency
- Flash:
  - Erasure flaws

Introduction to PUFs: Working principles

TECHNISCHE UNIVERSITÄT DARMSTADT

Utilization of different physical phenomena:

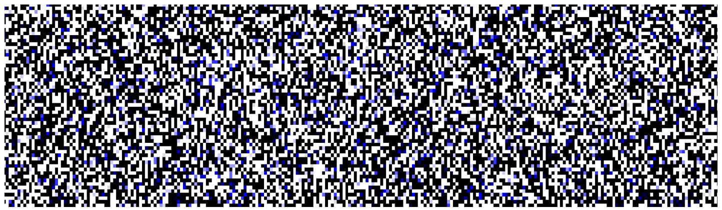
- SRAM:
  - **Startup values**
  - Retention and rowhammer
- DRAM:
  - **Startup values**
  - Retention
  - Retention and rowhammer
  - Remanence
  - Access latency
- Flash:
  - Erasure flaws

PUF INTRO

Introduction to PUFs: Working principles

Startup values

1	0	1	1	0	1	1	0
0	0	1	0	1	0	0	0
1	1	1	1	0	0	1	0
1	0	1	1	1	0	0	0



Introduction to PUFs: Working principles

TECHNISCHE UNIVERSITÄT DARMSTADT

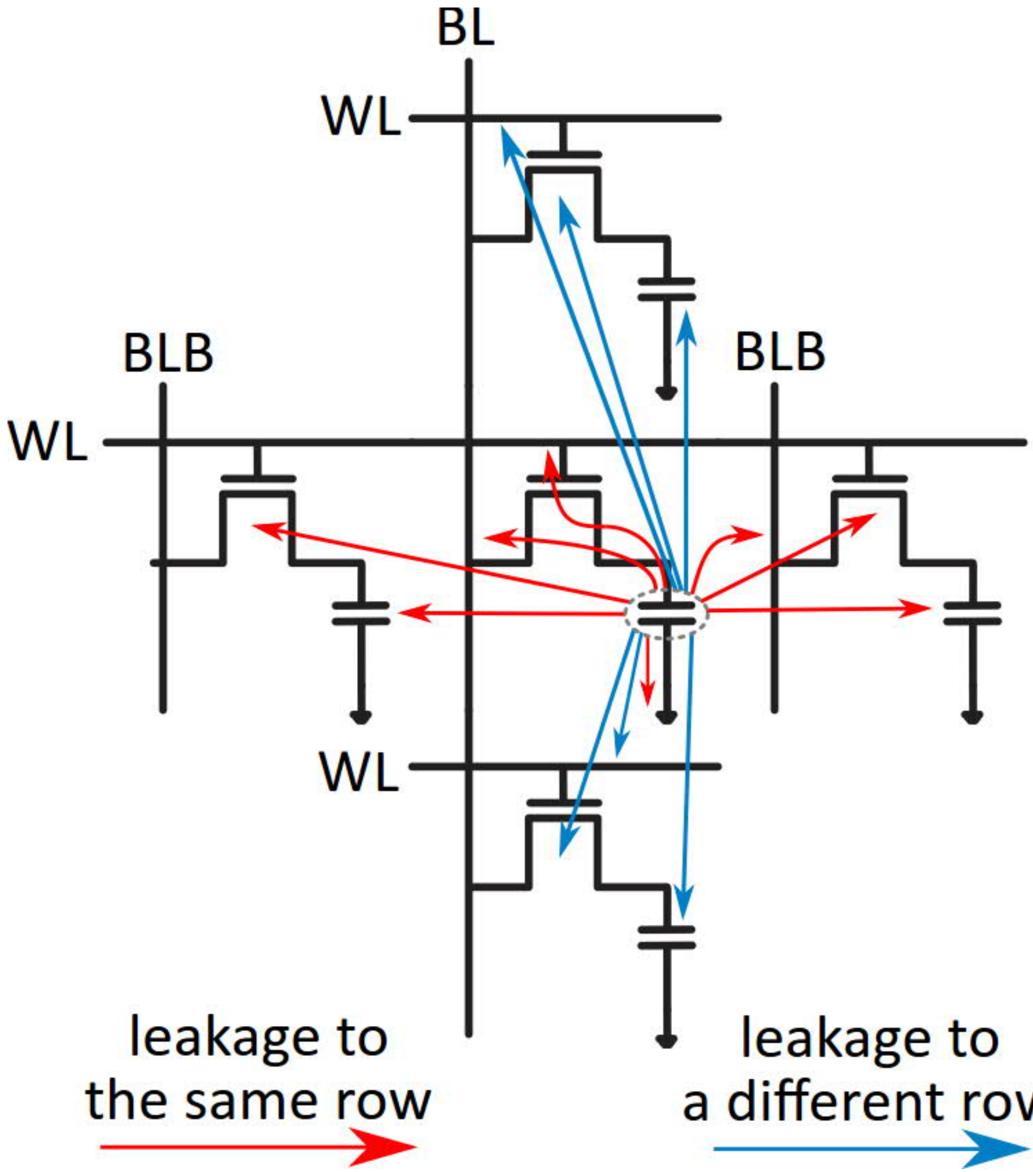
Utilization of different physical phenomena:

- SRAM:
  - Startup values
  - Retention and rowhammer
- DRAM:
  - Startup values
  - **Retention**
  - Retention and rowhammer
  - Remanence
  - Access latency
- Flash:
  - Erasure flaws

PUF INTRO

Introduction to PUFs: Working principles

Retention



PUF INTRO

Introduction to PUFs: Working principles

TECHNISCHE UNIVERSITÄT DARMSTADT

Utilization of different physical phenomena:

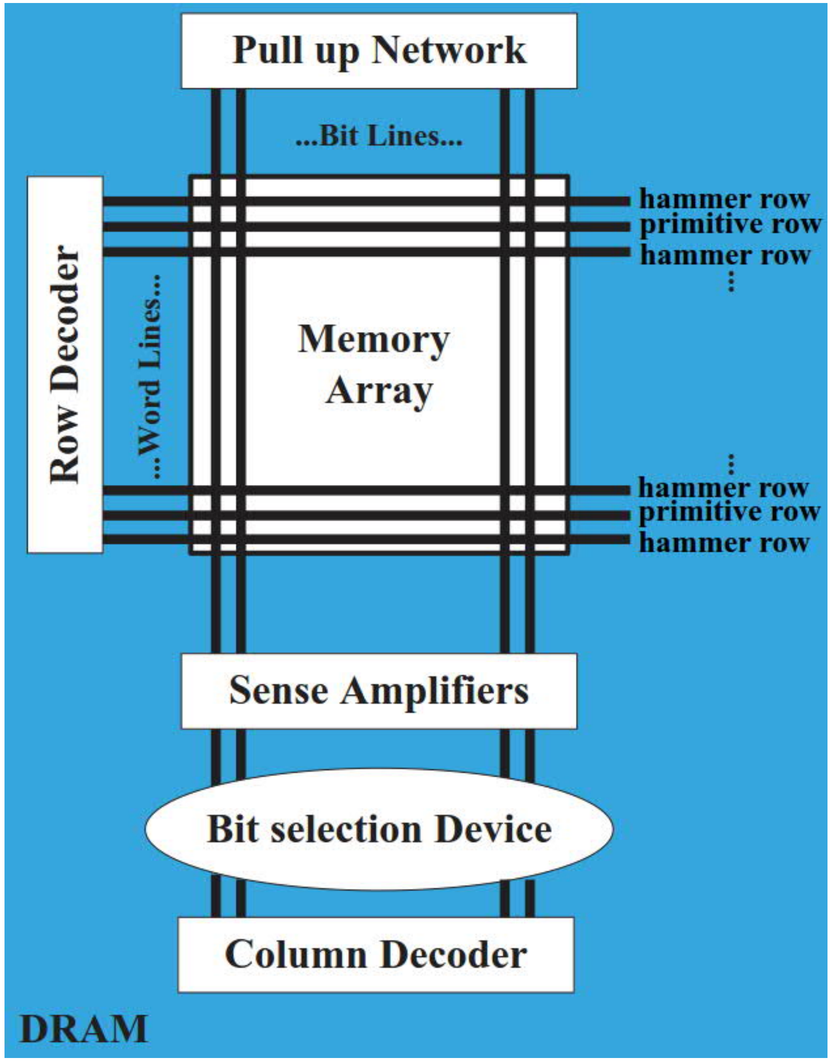
- SRAM:
  - Startup values
  - **Retention and rowhammer**
- DRAM:
  - Startup values
  - Retention
  - **Retention and rowhammer**
  - Remanence
  - Access latency
- Flash:
  - Erasure flaws

PUF INTRO

Introduction to PUFs: Working principles

TECHNISCHE UNIVERSITÄT DARMSTADT

Retention and Rowhammer



PUF INTRO

Introduction to PUFs: Working principles

TECHNISCHE UNIVERSITÄT DARMSTADT

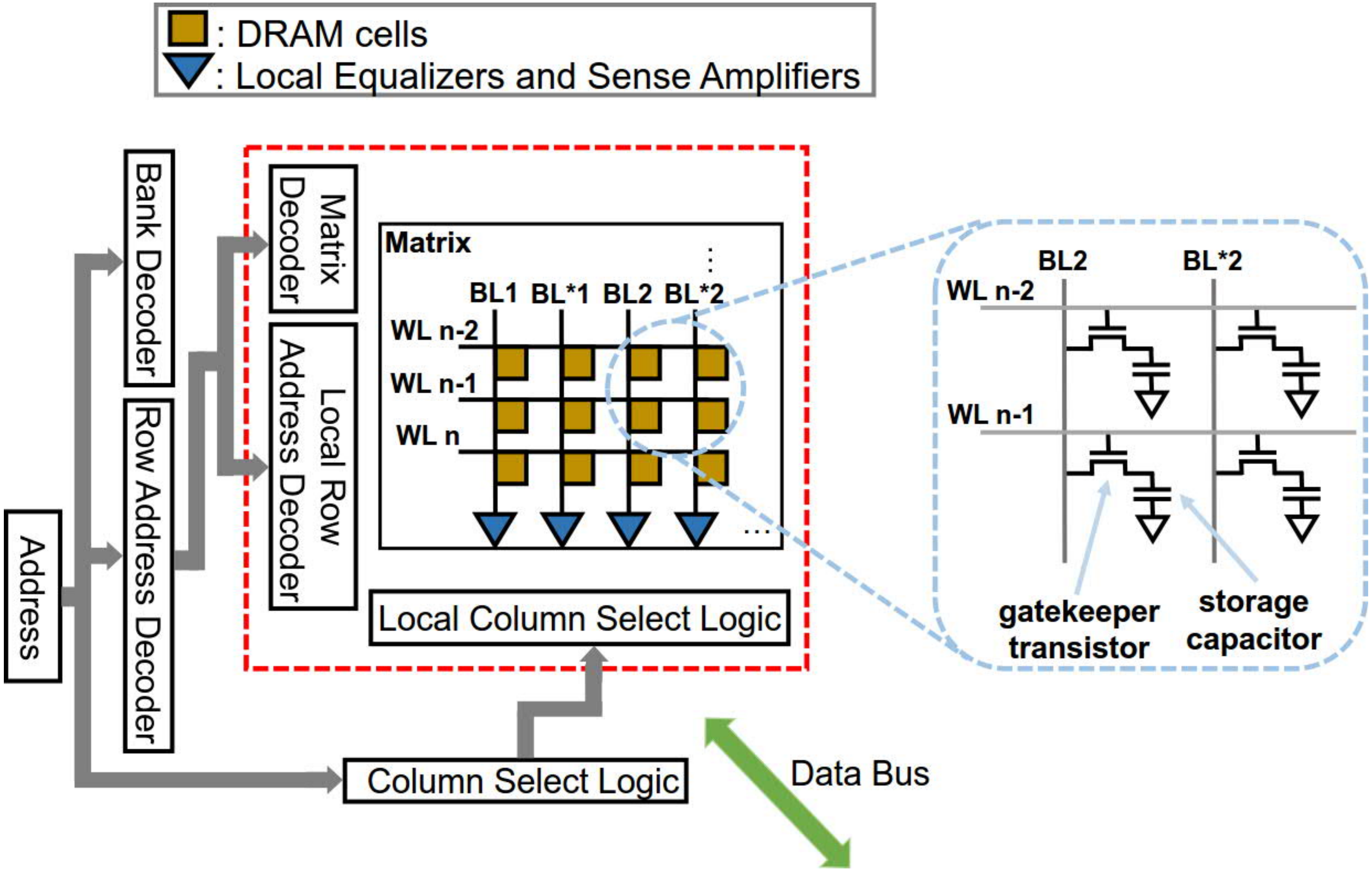
Utilization of different physical phenomena:

- SRAM:
  - Startup values
  - Retention and rowhammer
- DRAM:
  - Startup values
  - Retention
  - Retention and rowhammer
  - **Remanence**
  - Access latency
- Flash:
  - Erasure flaws

PUF INTRO

Introduction to PUFs: Working principles

Remanence



PUF INTRO

Introduction to PUFs: Working principles

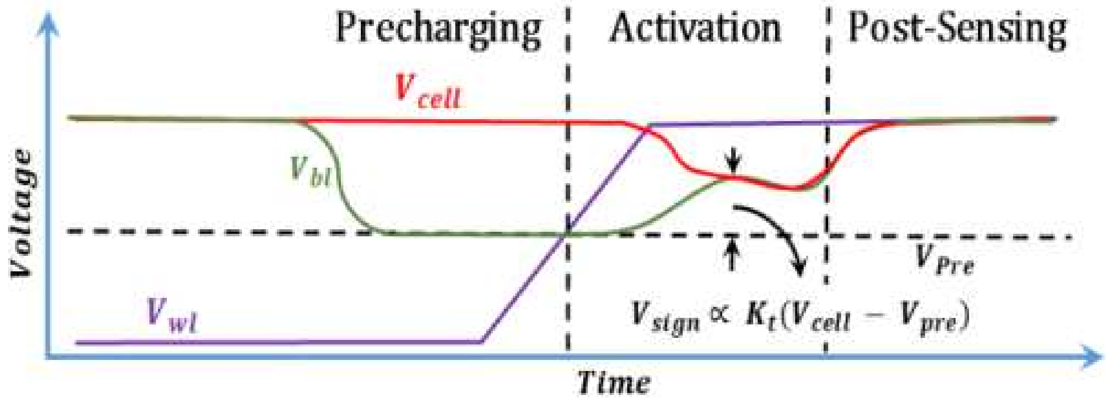
Utilization of different physical phenomena:

- SRAM:
  - Startup values
  - Retention and rowhammer
- DRAM:
  - Startup values
  - Retention
  - Retention and rowhammer
  - Remanence
  - **Access latency**
- Flash:
  - Erasure flaws

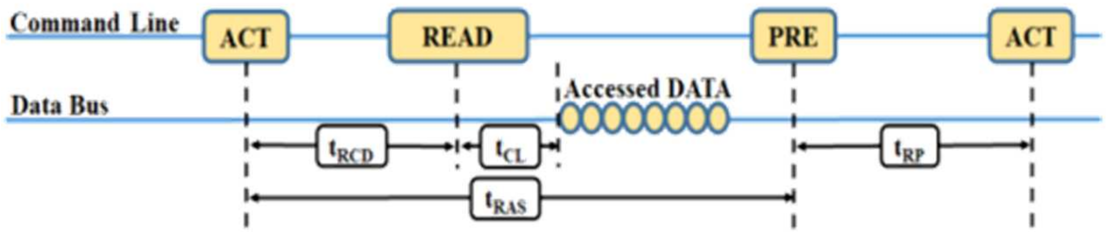
PUF INTRO

Introduction to PUFs: Working principles

Access Latency



(i) Signal waveform at reading cycle.



(ii) DRAM Timing at reading cycle.[20].

PUF INTRO

Introduction to PUFs: Working principles

TECHNISCHE UNIVERSITÄT DARMSTADT

Utilization of different physical phenomena:

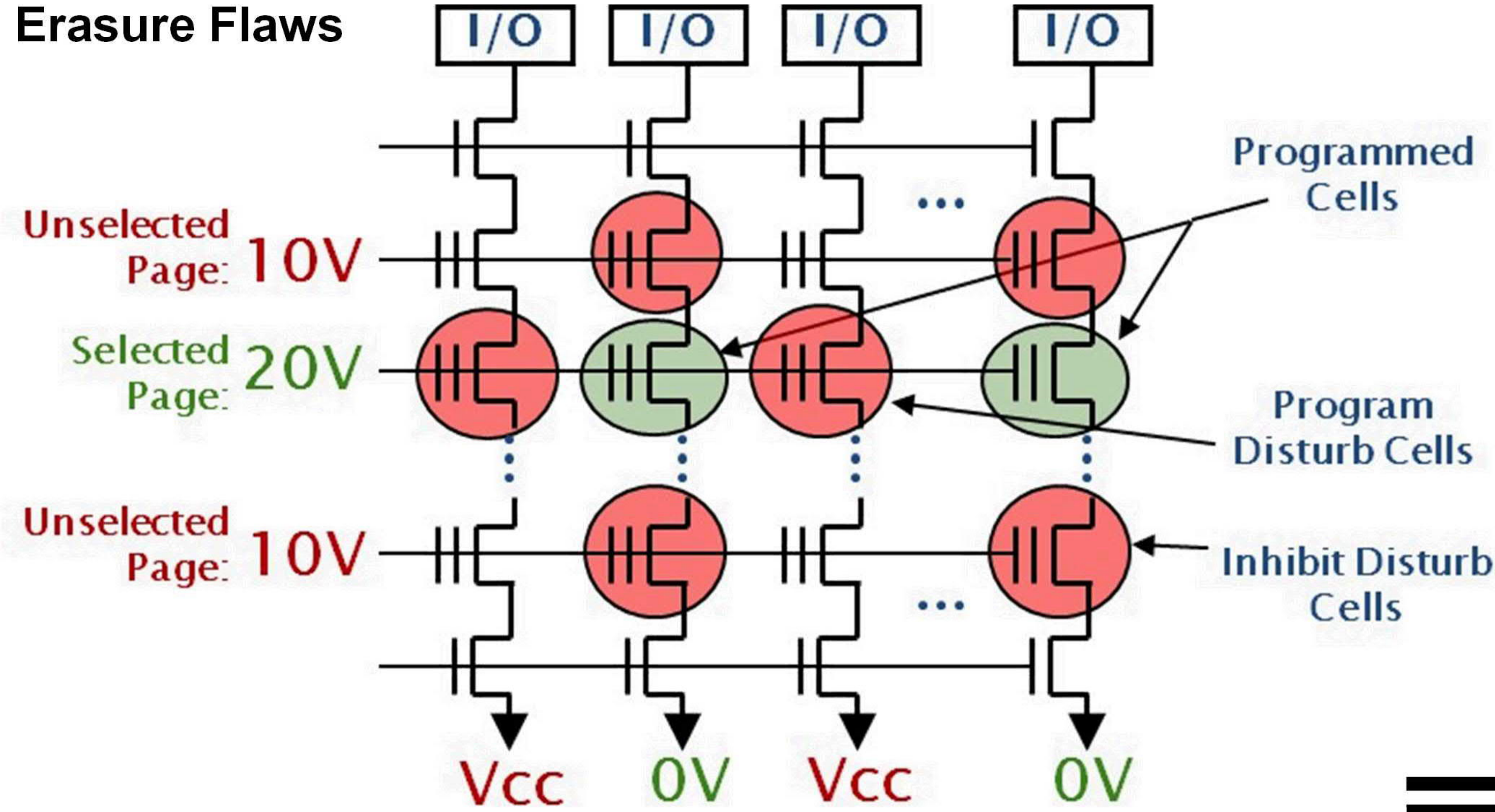
- SRAM:
  - Startup values
  - Retention and rowhammer
- DRAM:
  - Startup values
  - Retention
  - Retention and rowhammer
  - Remanence
  - Access latency
- Flash:
  - **Erasure flaws**

PUF INTRO

Introduction to PUFs: Working principles

TECHNISCHE UNIVERSITÄT DARMSTADT

Erasure Flaws



PUF INTRO

Introduction to PUFs:
IoT and PUFs so far

TECHNISCHE UNIVERSITÄT DARMSTADT

Security primitive used for:

- Identification
- Authentication
- Remote Attestation (Anti-counterfeiting, Tamper evidence)
- Key Agreement
- Random Number Generation

PUF INTRO

PUFs in Space:
IoT + PUFs + Space?

Advantages of PUFs

- Lightweight
- Cost-efficient
- Intrinsic (no additional HW, such as TPM, required)

However, the effect of environmental conditions on PUFs have to be investigated:

- Temperature variations
- Radiation

PUFS IN SPACE

PUFs in Space:
Definition of a good PUF: Quality metrics

TECHNISCHE UNIVERSITÄT DARMSTADT

Main objective:

How similar are two responses either

- from the same (intra-) or
- from a different (inter-) PUF instance

- Hamming Distance:

  Sum of bit differences in two measurements

- Jaccard Index:

$$\frac{\text{how many bit flip positions contain the same value in 2 measurements}}{\text{how many bit flip positions exist at all in 2 measurements}}$$

PUFS IN SPACE

PUFs in Space: What we knew

Memory Type	PUF Principle	Resilience against Temperature Variations
SRAM	Startup values	✓
DRAM	Startup values	✗
	Access latency	✓
	Retention	?
	Retention + Rowhammer	?
Flash	Erasure flaws	?

PUFs in Space:
Temparature Experiments: Setup I

- Used Hardware
  - DRAM retention PUF: Intel Galileo board
  - DRAM Rowhammer PUF: PandaBoard
  - Flash erasure flaw PUF: STM32F429

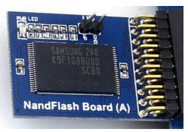
- Intel Galileo Gen. 2
  - 256MB DDR3 SDRAM

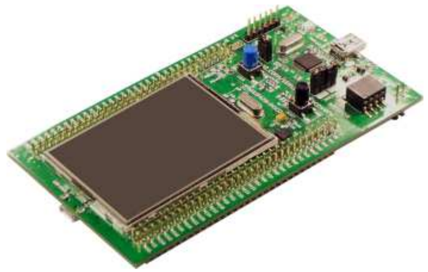
- PandaBoard ES
  - 1 GB LPDDR2 SDRAM

- STM32F429
  - 128MB NAND FLASH

Intel Galileo Board

PandaBoard





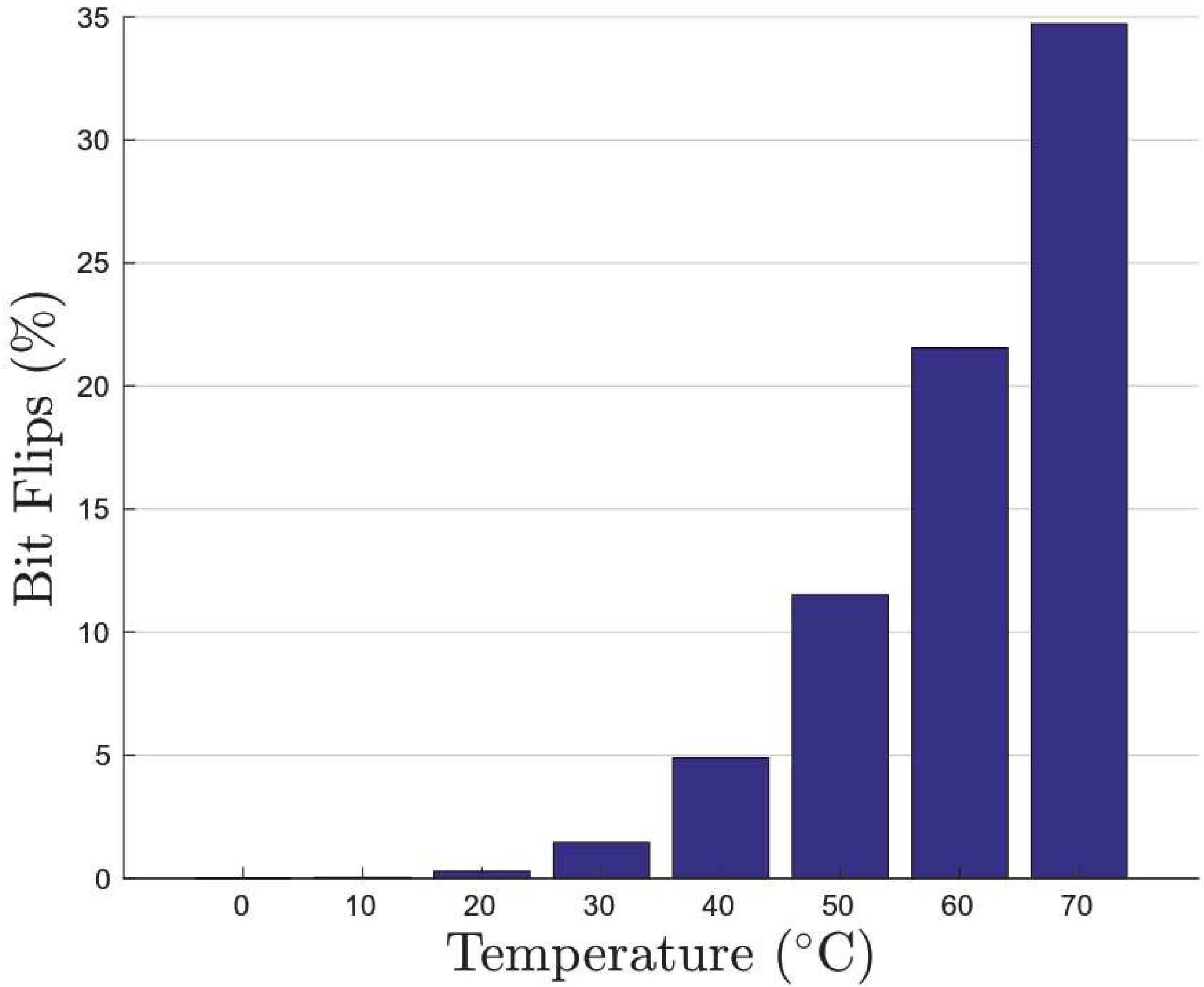
STM32F429

PUFS IN SPACE

PUFs in Space:
Temparature Experiments: Setup II

PUFS IN SPACE

PUFs in Space: Temparature Experiments: Results I



Number of bit flips

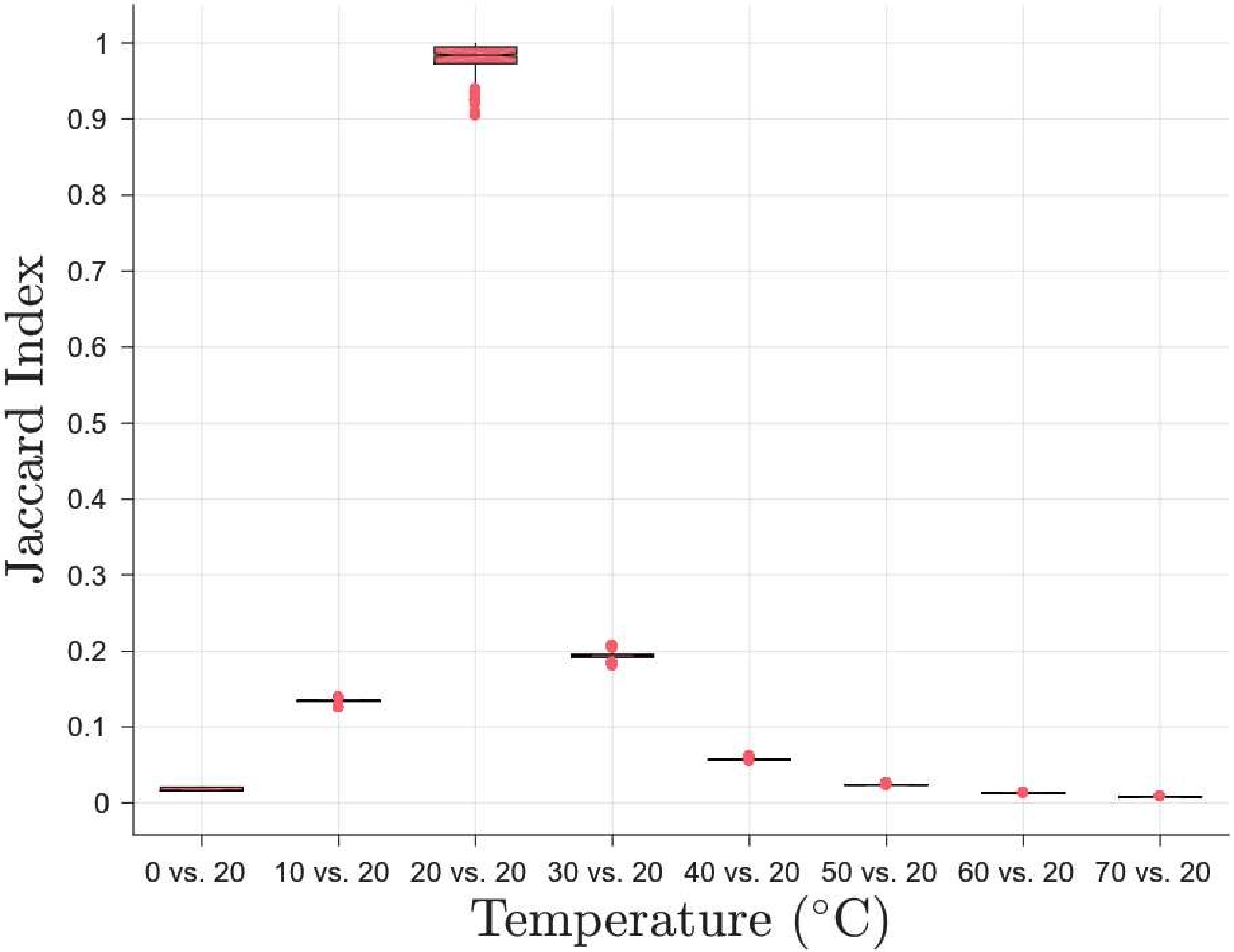
DRAM Retention PUF

Intel Galileo Board

Decay time: 300s

PUFS IN SPACE

PUFs in Space: Temparature Experiments: Results I



Intra-device Jaccard

Index 20°C vs 0-70°C

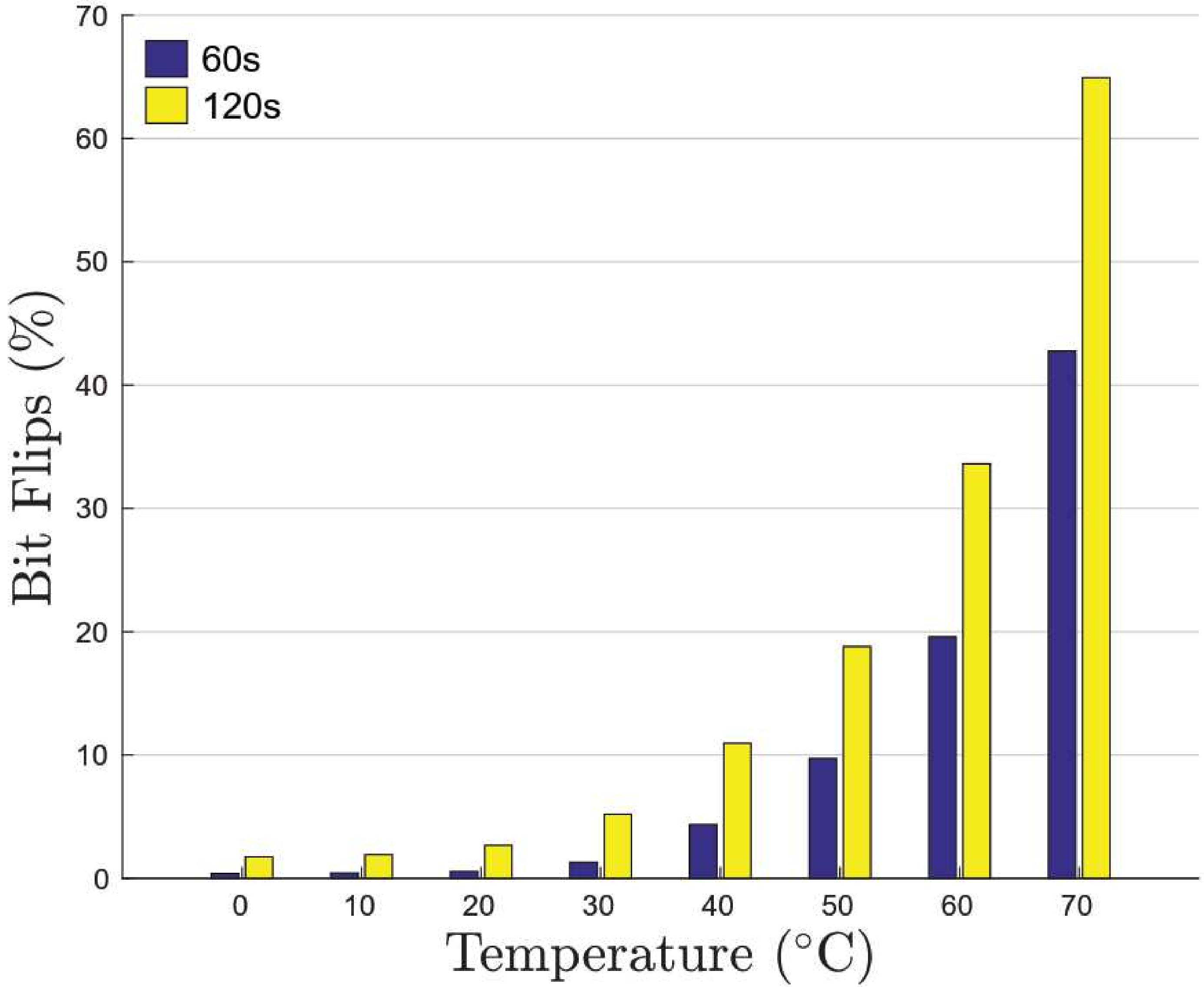
DRAM Retention PUF

Intel Galileo Board

Decay time: 300s

PUFS IN SPACE

PUFs in Space:
Temparature Experiments: Results II



Number of bit flips

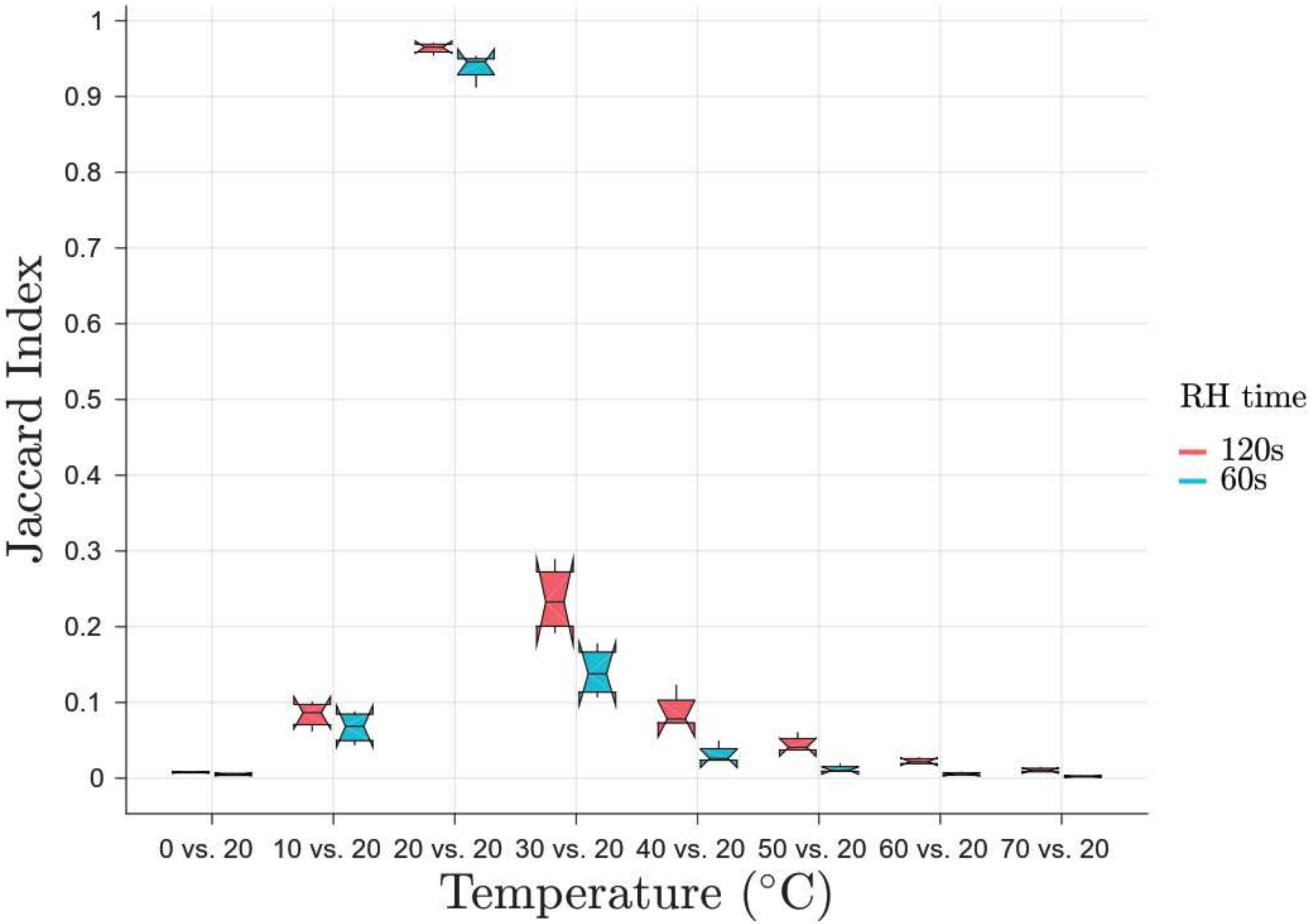
DRAM RH PUF

Pandaboard

RH times: 60s, 120s

PUFS IN SPACE

PUFs in Space:
Temparature Experiments: Results II



Intra-device Jaccard

Index 20°C vs 0-70°C

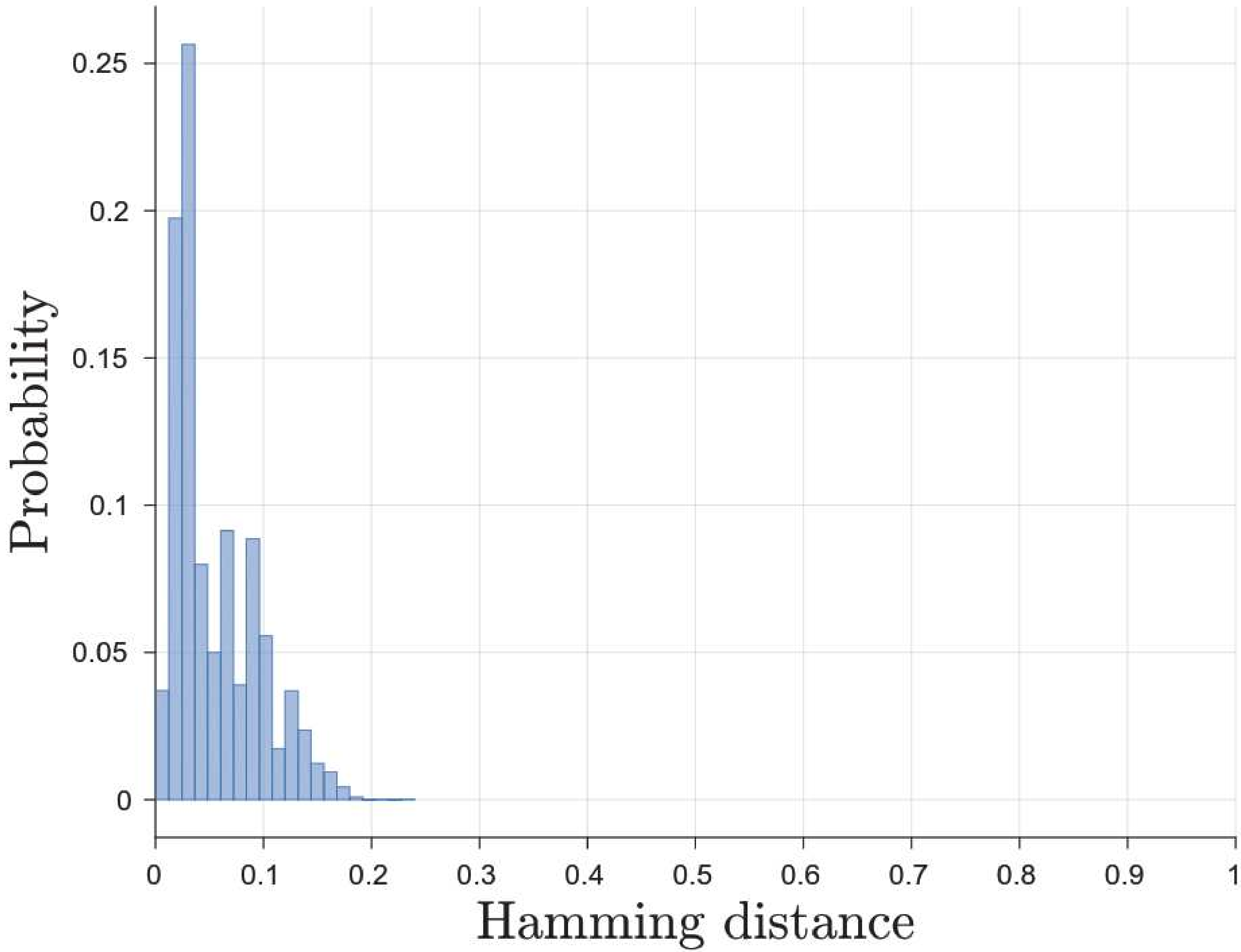
DRAM RH PUF

Pandaboard

RH times: 60s, 120s

PUFS IN SPACE

PUFs in Space:
Temparature Experiments: Results III



Hamming Distance

20°C vs 0-70°C

Flash PUF

1GBit NAND

PUFS IN SPACE

PUFs in Space:
What we knew

Memory Type	PUF Principle	Resilience against Radiation	
SRAM	Startup values	Relevant literature indicates resilience	?
DRAM	Startup values	If not refreshed for a number of seconds	✓
	Retention		
	Retention + Rowhammer		
Flash	Erasure flaws	Depends on type of radiation and scale of integration	?

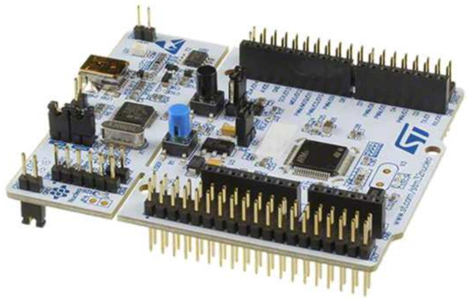
PUFS IN SPACE

PUFs in Space: Radiation Experiments: Setup I

TECHNISCHE UNIVERSITÄT DARMSTADT

- Used Hardware
  - SRAM PUF, Flash PUF on STM32F407, STM32 NUCLEO-64 L152RE
- STM32F407
  - 192 KB SRAM
  - 1 MB FLASH
- STM32 NUCLEO-64 L152RE
  - 80 KB SRAM
  - 512 KB FLASH

STM32F407



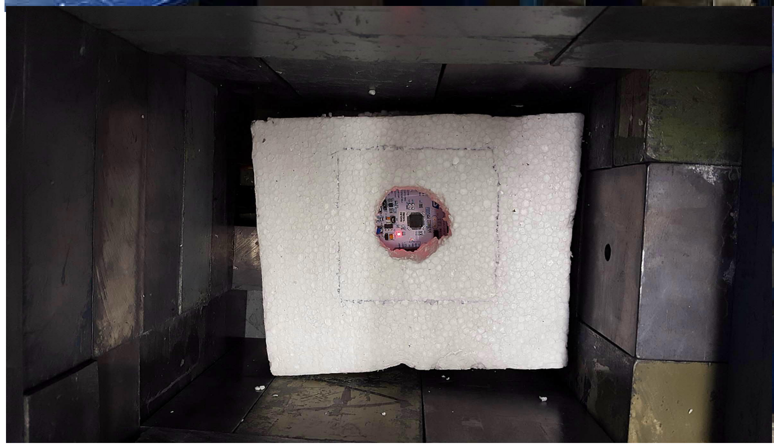
STM32 NUCLEO-64 L152RE

PUFS IN SPACE

PUFs in Space:
Radiation Experiments: Setup II

TECHNISCHE
UNIVERSITÄT
DARMSTADT

Strontium-90
β source



PUFS IN SPACE

PUFs in Space: Radiation Experiments: Setup III

TECHNISCHE UNIVERSITÄT DARMSTADT

Caesium-137
γ and β source

PUFS IN SPACE

PUFs in Space:
Radiation Experiments: Setup IV

X-rays

PUFS IN SPACE

PUFs in Space: Radiation Experiments: Results

TECHNISCHE UNIVERSITÄT DARMSTADT

Radioactive Source	Emissions	Time Tested	Total Dose Absorbed
${}^{137}_{55}Cs$	γ & β^-	10 days	0.024 Gy (2.4 rad)
${}^{90}_{38}Sr$	β^-	100 days	105.6 Gy (10.56 krad)[d] 432 Gy (43.2 krad)[n]
Hard X-ray source	10 MV X-rays	12 minutes	250 Gy (25 krad)

[d] For the STM32F407 Discovery board
[n] For the STM32 Nucleo-64 NUCLEO-L152RE board

PUFS IN SPACE

Conclusion

- Performed experiments on SRAM, DRAM and Flash PUFs considering the effect of temperature variations and radiation on PUF functionality
- Demostrated that PUFs can be used at least in conditions found in near-Earth orbits to provide lightweight, flexible and cost-efficient security solutions for IoT implementations in space
- Higher resilience to temperature variations can be achieved by robust cryptoprotocols and the use of internal temperature sensors
- Higher resilience to radiation can be achieved by aluminium alloy housing of satellite, rebooting, erasing and overwriting memory module, multiple challenges and employment of fuzzy extraction scheme

Department of Computer Science
Security Engineering Group

TECHNISCHE
UNIVERSITÄT
DARMSTADT

Dr. Tolga Arul
Postdoctoral Researcher

Mornewegstraße 32
64293 Darmstadt
arul@seceng.informatik.tu-darmstadt.de

Phone +49 6151 16-25649
Fax +49 6151 16-25627
www.seceng.de

Thank you for your attention