ASPIRE
INVENT
ACHIEVE

imec

HUMAN++

Pioneering efficient healthcare

CHALLENGES IN APPLYING PUFS AS A BASIS FOR SECURITY IN BAN DEVICES

JOS HUISKEN

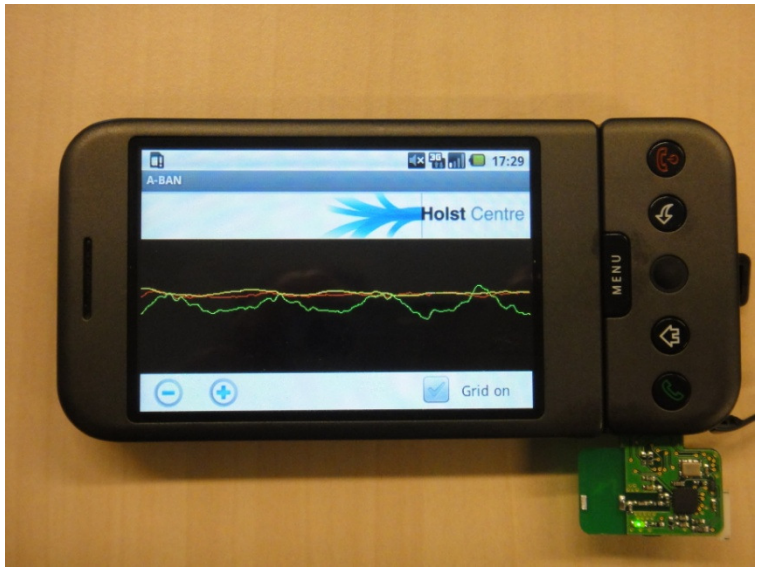
imec

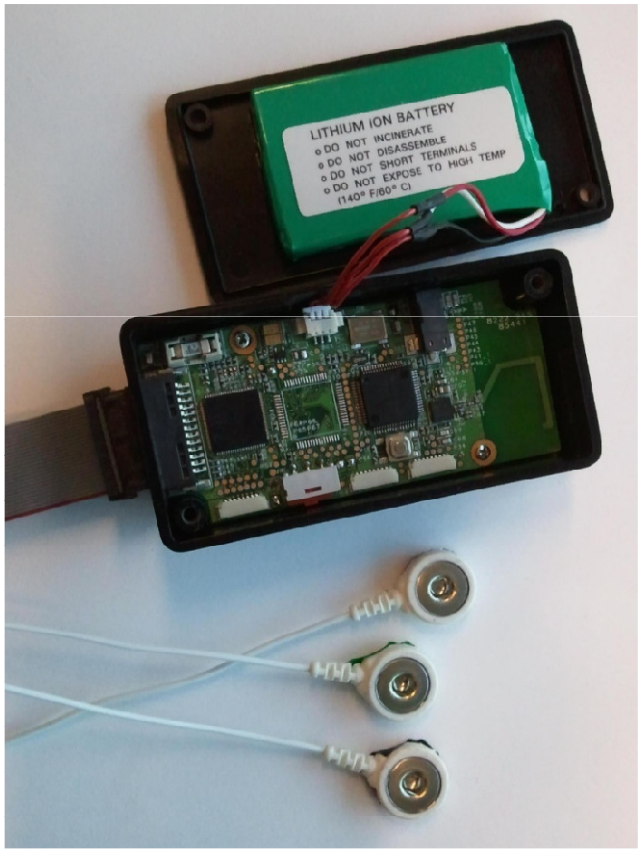
INTRODUCTION

Where do I come from?

"Digital Low Power" or

"Energy Constrained Digital"





Holst Centre
Open Innovation by IMEC and TNO

RECENT NEWS

Dutch government worried about privacy:

Patiëntendossier sneuvelt waarschijnlijk in Eerste Kamer

Door **Joost Schellevis**, dinsdag 29 maart 2011 17:04, views: 22.665

Waarschijnlijk gaat een meerderheid van de Nederlandse Eerste Kamer volgende week tegen de invoering van het landelijke Elektronisch Patiëntendossier stemmen. Enkel het CDA heeft aangegeven nog te twijfelen. De Senaat maakt zich zorgen om de privacy.

And we want to "auto-maintain" or "auto-fill" it...

Holst Centre
Open Innovation by IMEC and TNO

WBAN SECURITY DESIGN CHALLENGES

Security requirements in WBAN

- Secure proposal compatible with international standards and regulations
- Promoting and maintaining fundamental medical ethical principles and social expectations
- The attacker model has be well defined - Find the real security requirements of the system

Secure protocol design

- Proposing protocols for providing Secure Wireless Body Area Networks

Low power design

- Propose security protocols that are "Radio friendly" → Reduce the number of message exchanges
- Power efficient design for cryptographic functions → Optimize secure algorithms

Exploit technology variability to provide advanced security solutions

- Physical Unclonable Functions

Holst Centre
Open Innovation by IMEC and TNO

CONCEPT OF SILICON PUF

Due to *random process variations* NO two chips, even with the same layout, are identical!

- Variation is inherent in fabrication process
- Hard to remove or predict
- Relative variation increases with Moore's law

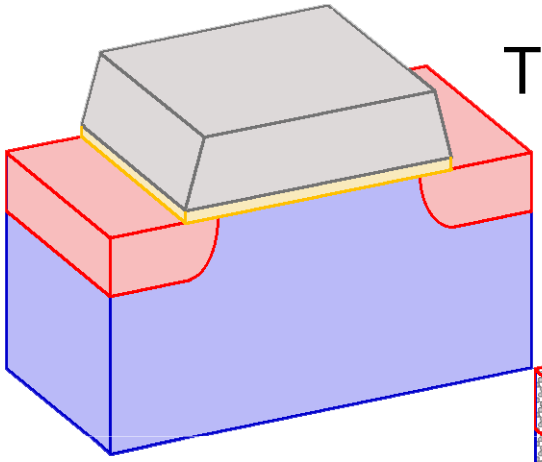
Examples:

- Combinatorial circuit path delay *MIT / Verayo*
- SRAM based *Philips / Intrinsic-Id*

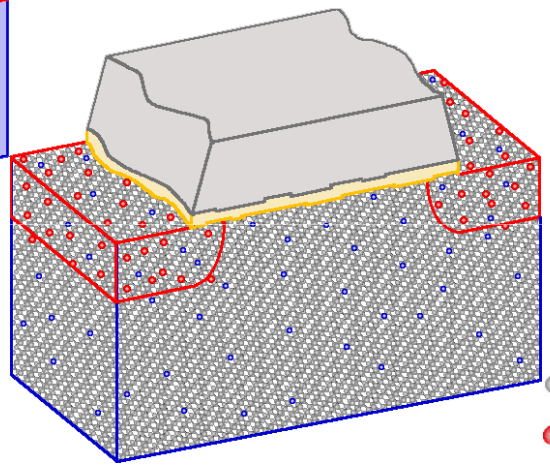
Holst Centre
Open Innovation by IMEC and TNO

VARIABILITY IN CMOS AND SRAM CELLS

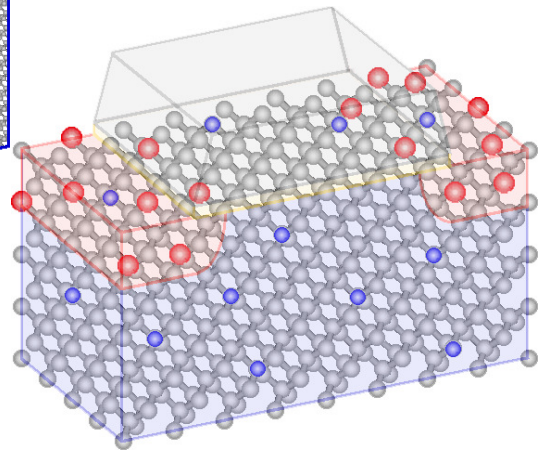
Threshold Voltage determined by doping



A 130 nm MOSFET



A 22 nm MOSFET

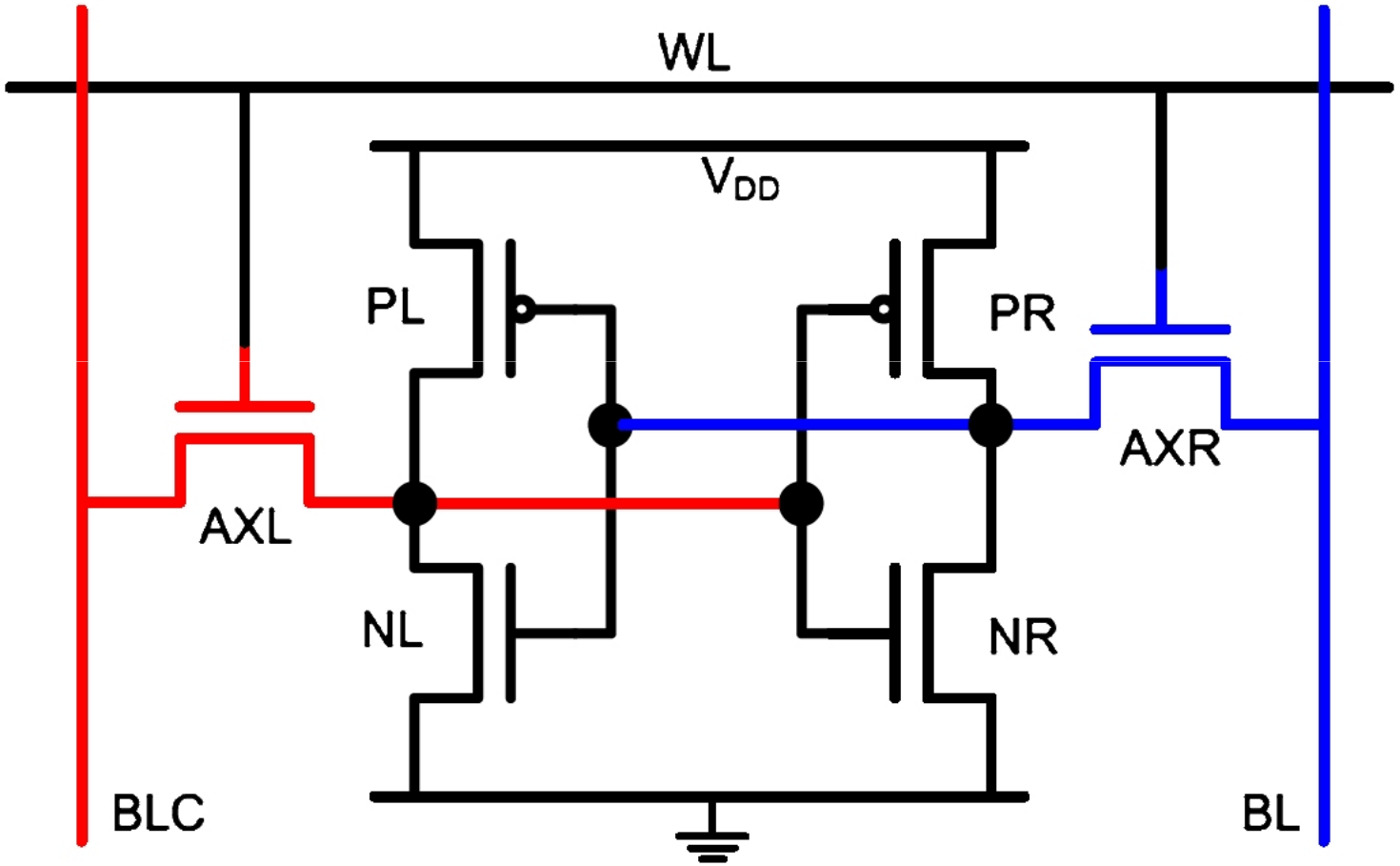


A 4.2 nm MOSFET

Holst Centre
Open Innovation by IMEC and TNO

imec

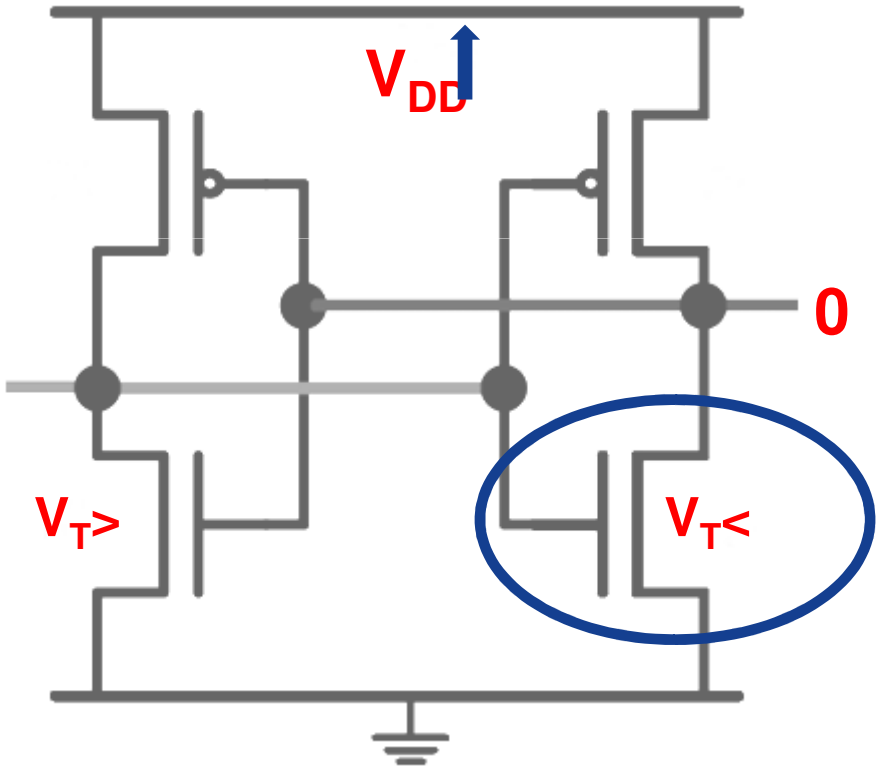
6T SRAM CELL



Holst Ce
Open Innovatio

imec

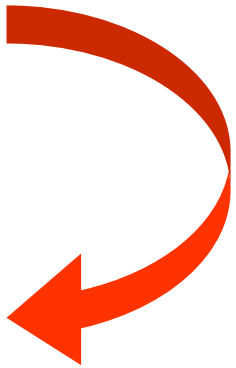
6T SRAM PUF



Holst Centre
Open Innovation by IMEC and TNO

INTRODUCTION SRAM PUF

Reliability:



~ 10% errors

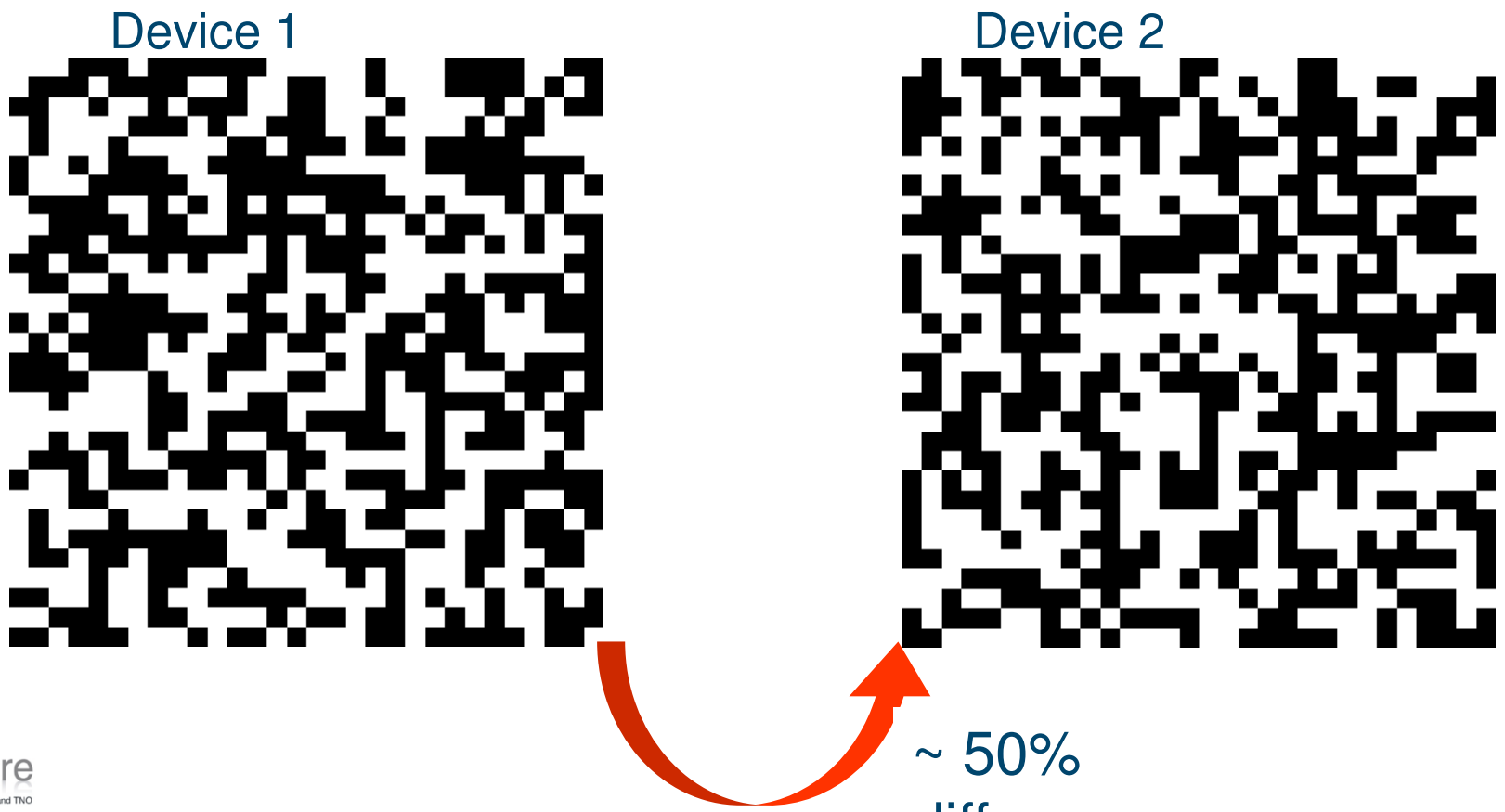
using:

BCH codes

Holst Centre
Open Innovation by IMEC and TNO

INTRODUCTION SRAM PUF

Uniqueness:

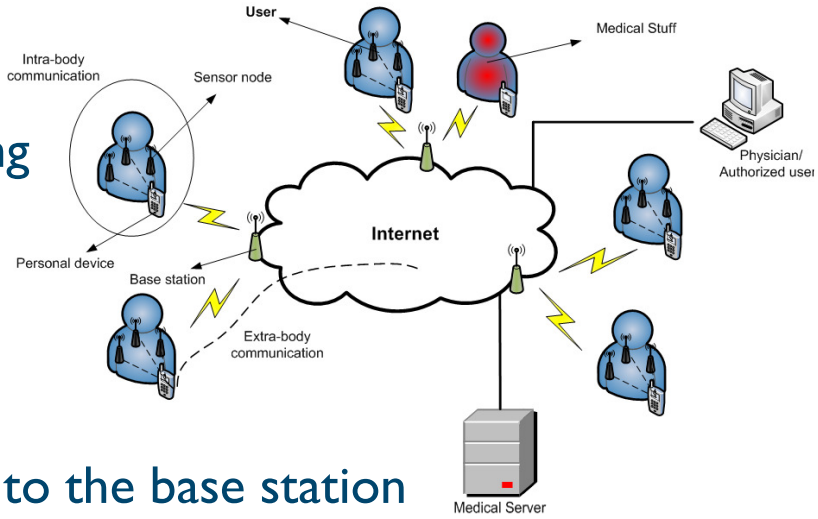


Holst Centre
Open Innovation by IMEC and TNO

imec

SENSOR: RESOURCE CONSTRAINED

WBAN - Wireless Body Area Network



Application domain biomedical data monitoring

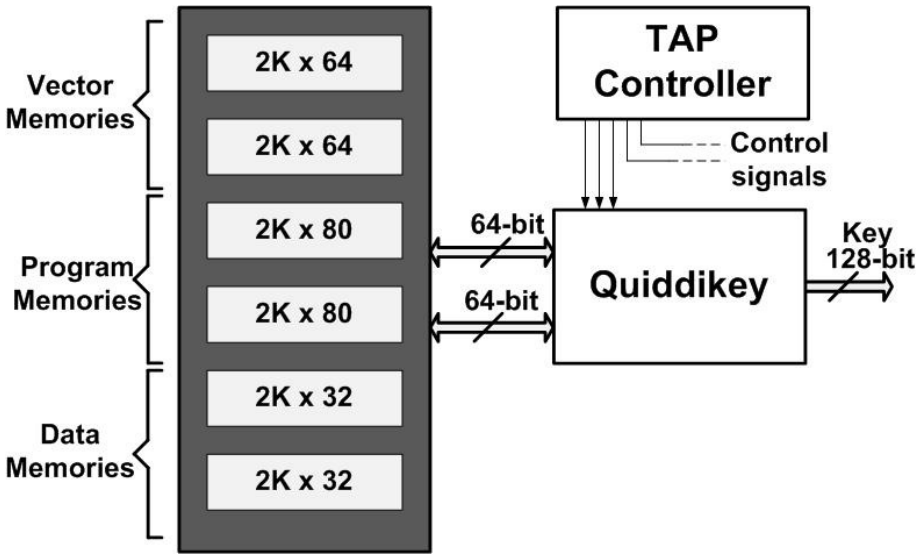
Focus on intra-body communication

Sensor nodes attached on human body

Transmit data to a personal device or directly to the base station

Physician has access to the data

SRAM PUF as fingerprint:



Holst Centre
Open Innovation by IMEC and TNO

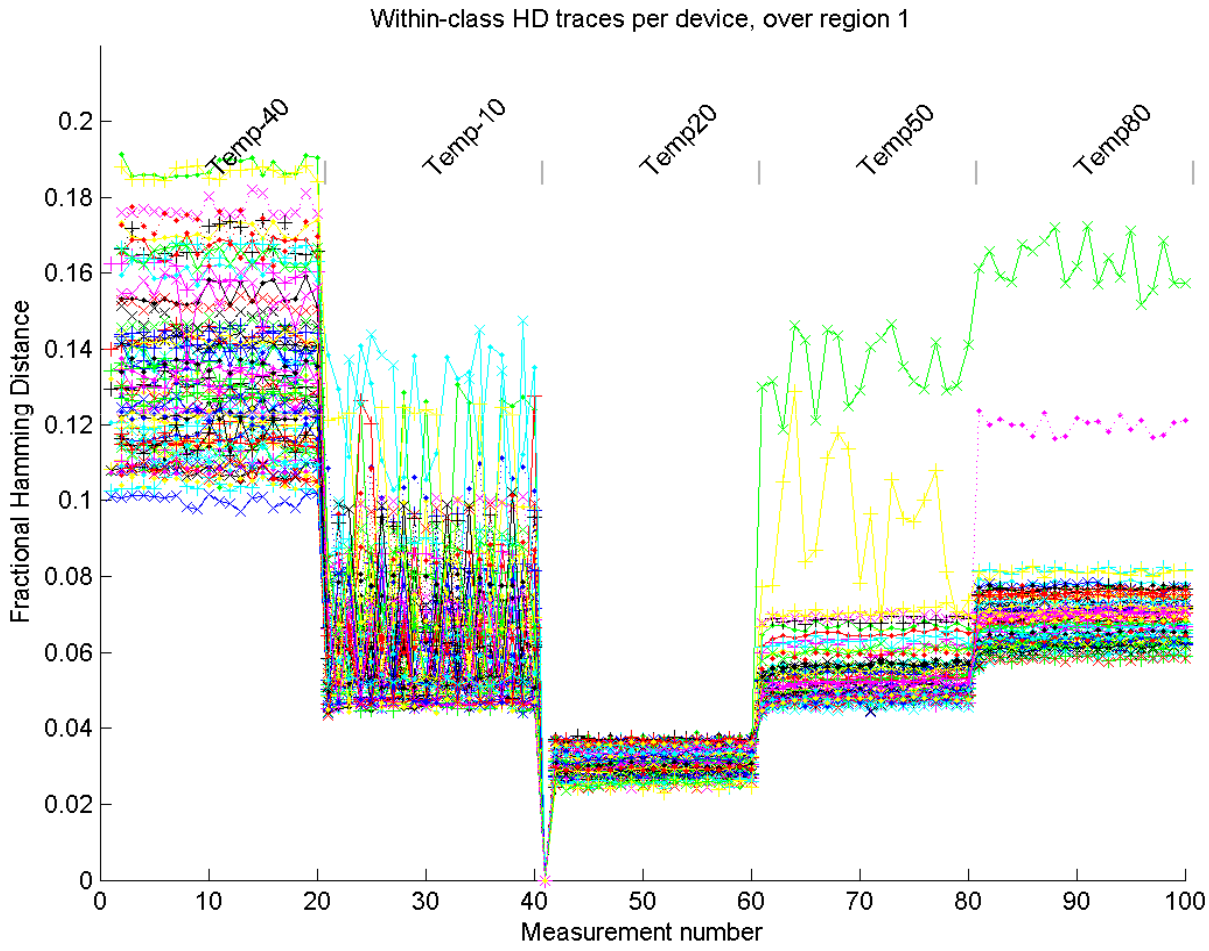
PUF RELIABILITY: TEMPERATURE

Study stability of start-up values at different temperatures

17 ICs measured under varying ambient temperature

Measurement at 20°C has been used as reference

Hamming Distance during test <19%



Holst Centre
Open Innovation by IMEC and TNO

imec

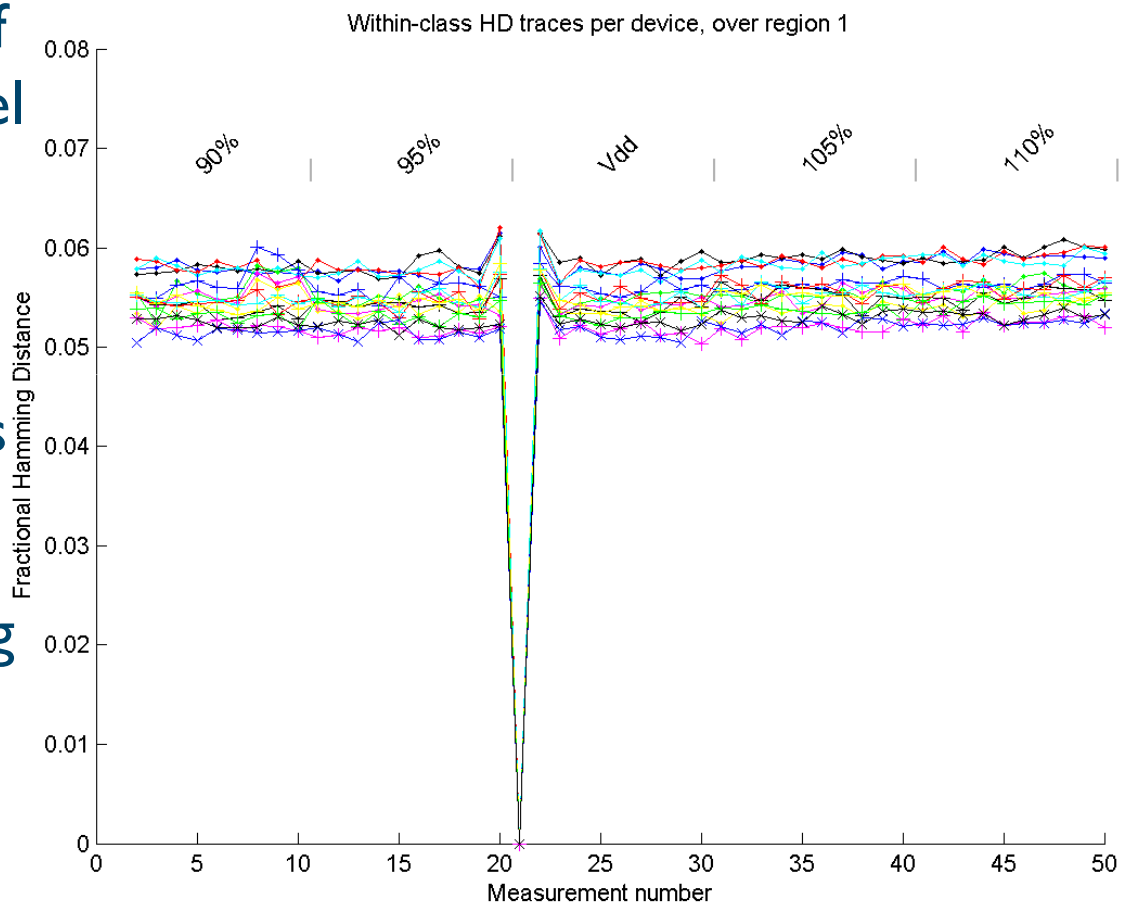
PUF RELIABILITY: VOLTAGE VARIATION

Study stability of start-up values under variations of power supply voltage level

4 ICs measured with different supply voltages

Measurement at VDD has been used as reference

Hamming Distance during test very low and constant



Holst Centre
Open Innovation by IMEC and TNO

PUF UNIQUENESS

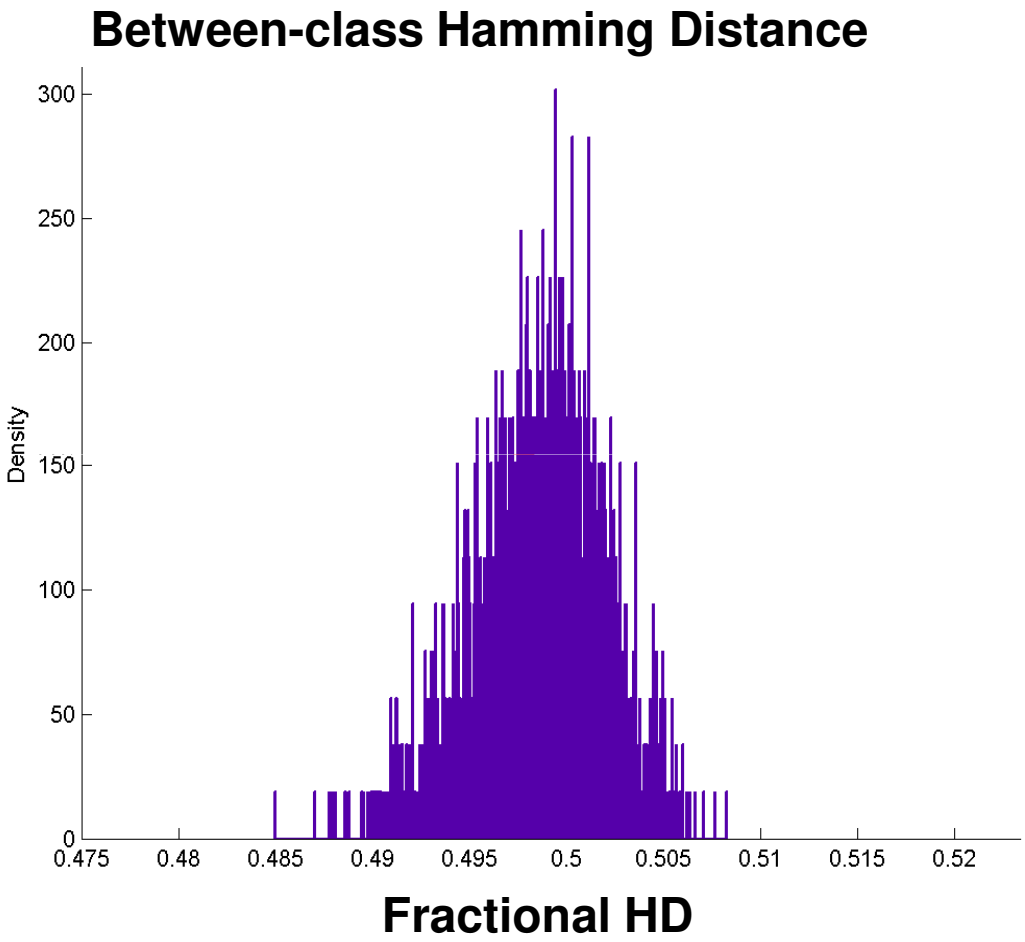
Study HD between different devices to determine uniqueness

Measurements from temp test used (17 ICs, 4 memories)

Measurements at +20˚C have been used for between-class HD

Between-class HDs distributed around 0.5 and are much larger than within-class HDs

No correlation between start-up patterns of different devices

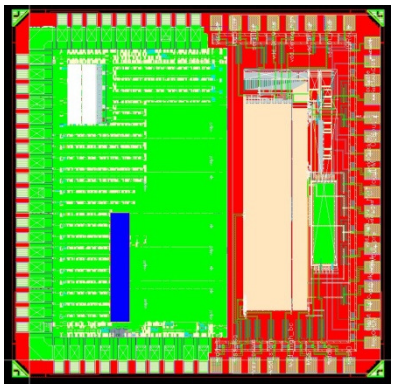


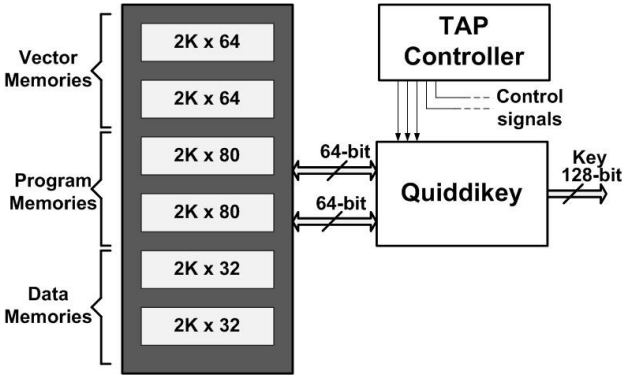
Holst Centre
Open Innovation by IMEC and TNO

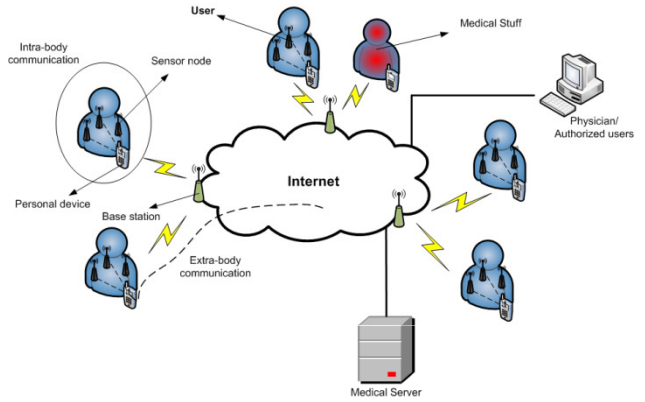
INGREDIENTS AND OUTLOOK

Components gradually become available:

6T-SRAM PUF in 65nm CMOS evaluation ongoing.



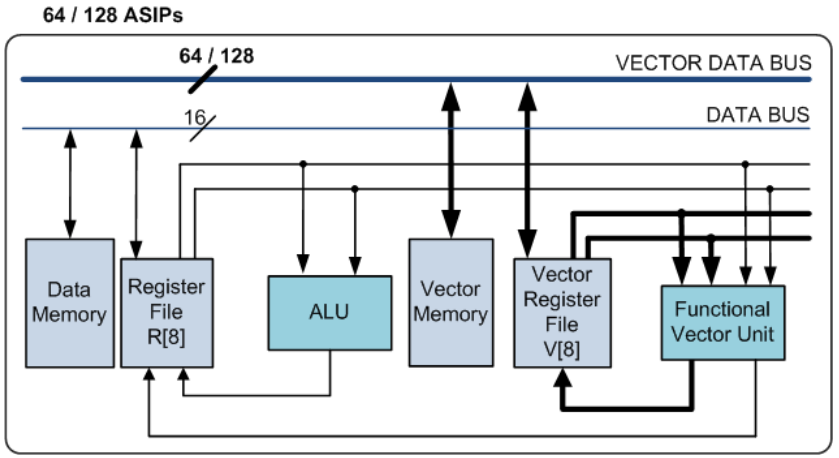




Processor for BAN (ASIP)

with AES extensions available.

Optimized for low energy



Holst Centre
Open Innovation by IMEC and TNO

CHALLENGES IN APPLYING SRAM-PUFS

CMOS Process Development: Good for PUFs, "bad" for IMD

- Reliability of processes is worsening due to increase in amount of applied materials.
- CMOS technologists already "promise" us: "Learn to design with unreliable components!" (Implantable today: >130nm...)

Security Community:

- What are the security (authentication/privacy) requirements?
  - Body Area Networks and ambulatory (remote and home) monitoring
  - Implants, such us pacemakers with built-in defibrillation
  - EEG headsets for brain-computer-interfacing
- Challenge in expanding the ECO-System
  - Semiconductor and Pharma Industry, Medical Device Manufacturers, Hospitals

Holst Centre
Open Innovation by IMEC and TNO

CONCLUSIONS

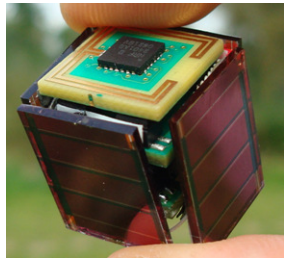
PUFs, using commercial 6T-SRAMs, have been evaluated successfully

- Different testing conditions have been applied, like varying ambient temperature and supply voltage level
- Experimental results prove that the initial state of the SRAMs are stable and tolerant for noise
- Derived start-up patterns from these memories are unique and unpredictable among other SRAM circuits

Conclusion: low power SRAMs are very useful for secure key storage without storing the key in non-volatile memory

Challenge: "PUF-based security is needed for ..."

- Biomedical remote healthcare
- Biomedical devices, implant or on-body
- Wireless sensor networks, such as smart buildings, or RFID in logistics



Holst Centre
Open Innovation by IMEC and TNO

imec

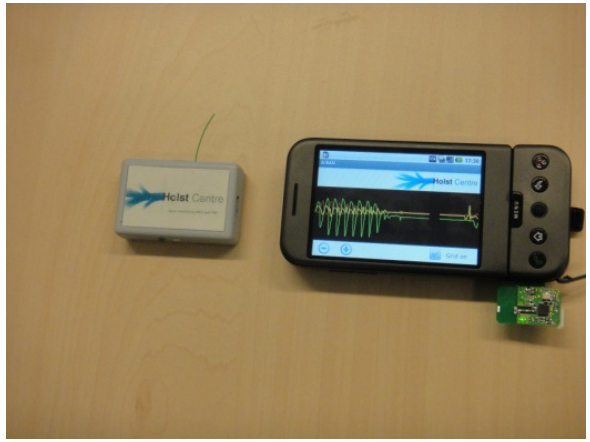
ASPIRE
INVENT
ACHIEVE

imec

FUTURE WORK

PUF evaluation

- Evaluate other SRAM types
- Evaluate other technologies than 90nm and 65nm



Continue work on application scenario

- WSN for biomedical data monitoring
- Combine SRAMs with Quiddikey and security blocks

Secure authentication and temporal key generation based on PUF

- Supporting PUF-based authentication without exposing the output of the PUF
- Protocol design for temporal key generation between sensor node and gateway (Master node)

Security of the communication link

- AES based: Encryption, decryption, data authentication, data integrity
- Side channel attacks protection

Holst Centre
Open Innovation by IMEC and TNO

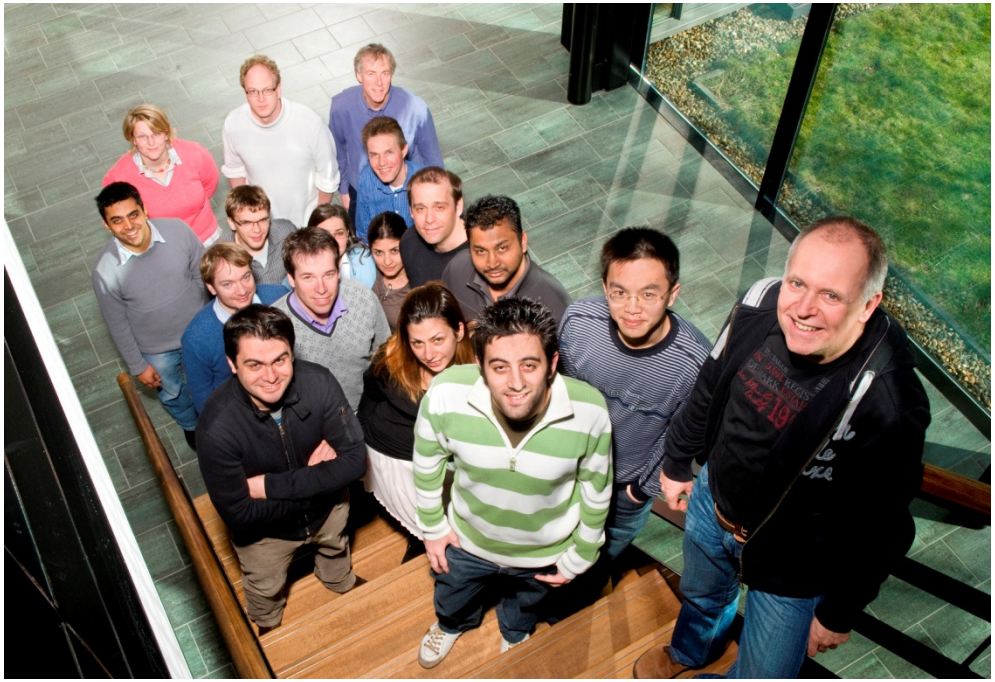
ACKNOWLEDGEMENTS

Intrinsic-Id:

Vincent van Leest, Geert-Jan Schrijen, Marten van Hulst, Pim Tuyls

Holst Centre / imec:

Georgios Selimis, Mario Konijnenburg, Mariam Ashouei



Holst Centre
Open Innovation by IMEC and TNO

imec