**THOMAS KALLSTENIUS, PhD**
program director distributed trust
thomas.kallstenius@imec.be

Kapeldreef 75
3001 Leuven
Belgium

M +32 477 96 13 63

www.imec-int.com

imec

**THOMAS KALLSTENIUS, PhD**
program director distributed trust
thomas.kallstenius@imec.be

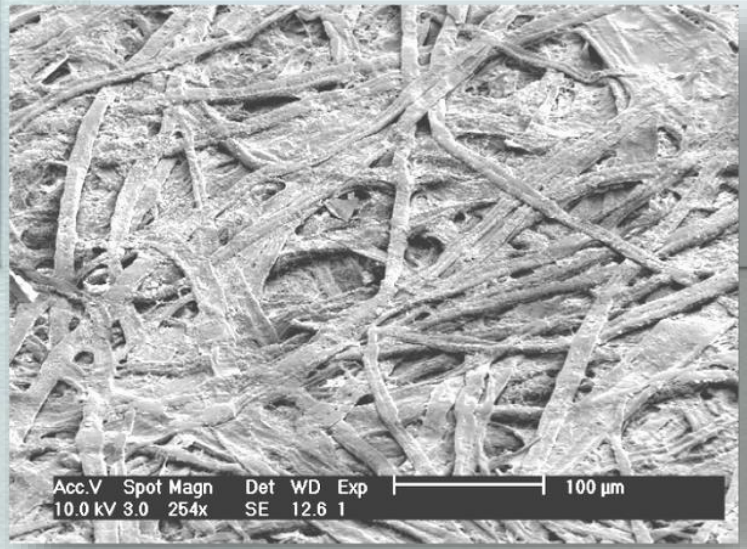
Kapeldreef 75
3001 Leuven
Belgium

M +32 477 96 13 63

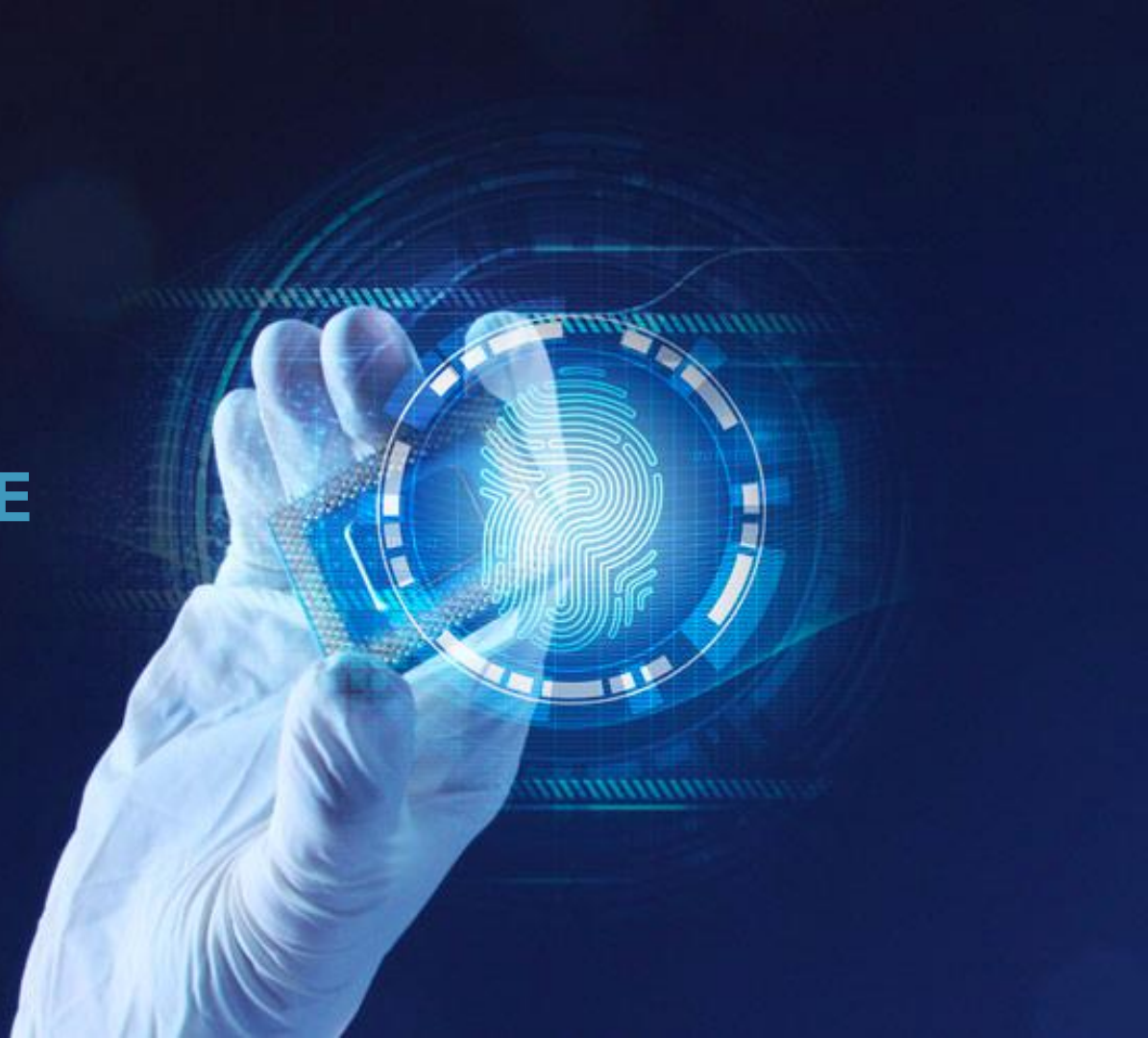
www.imec-int.com

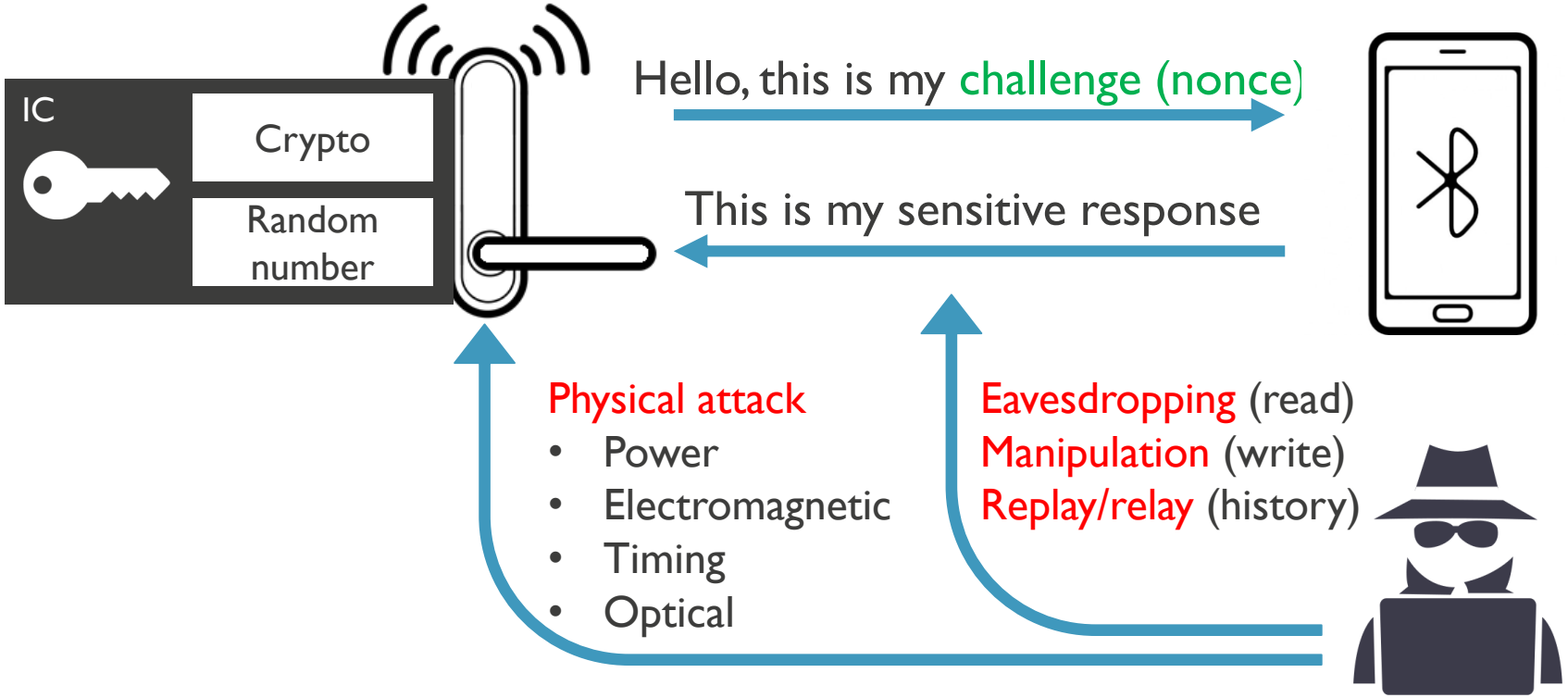
imec

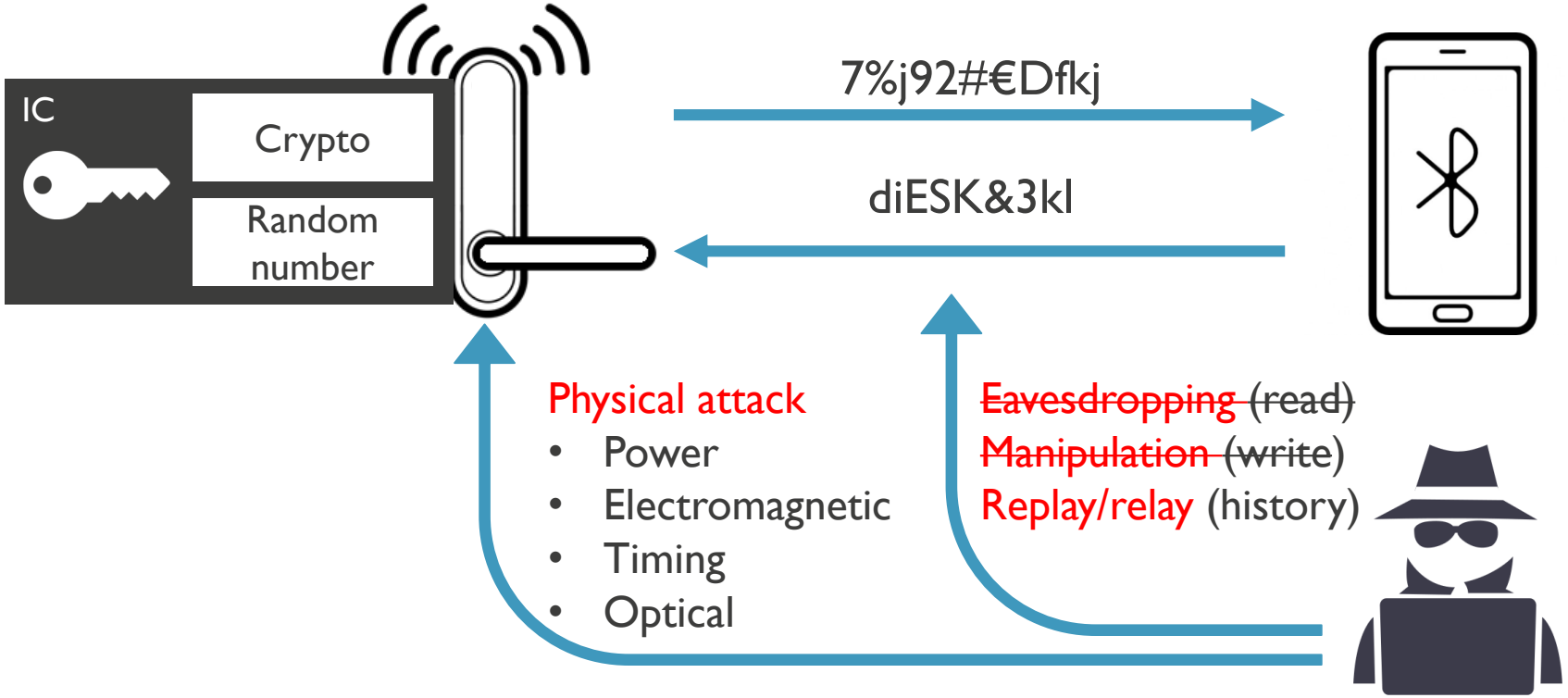
**THOMAS KALLSTENIUS, PhD**
program director distributed trust
thomas.kallstenius@imec.be

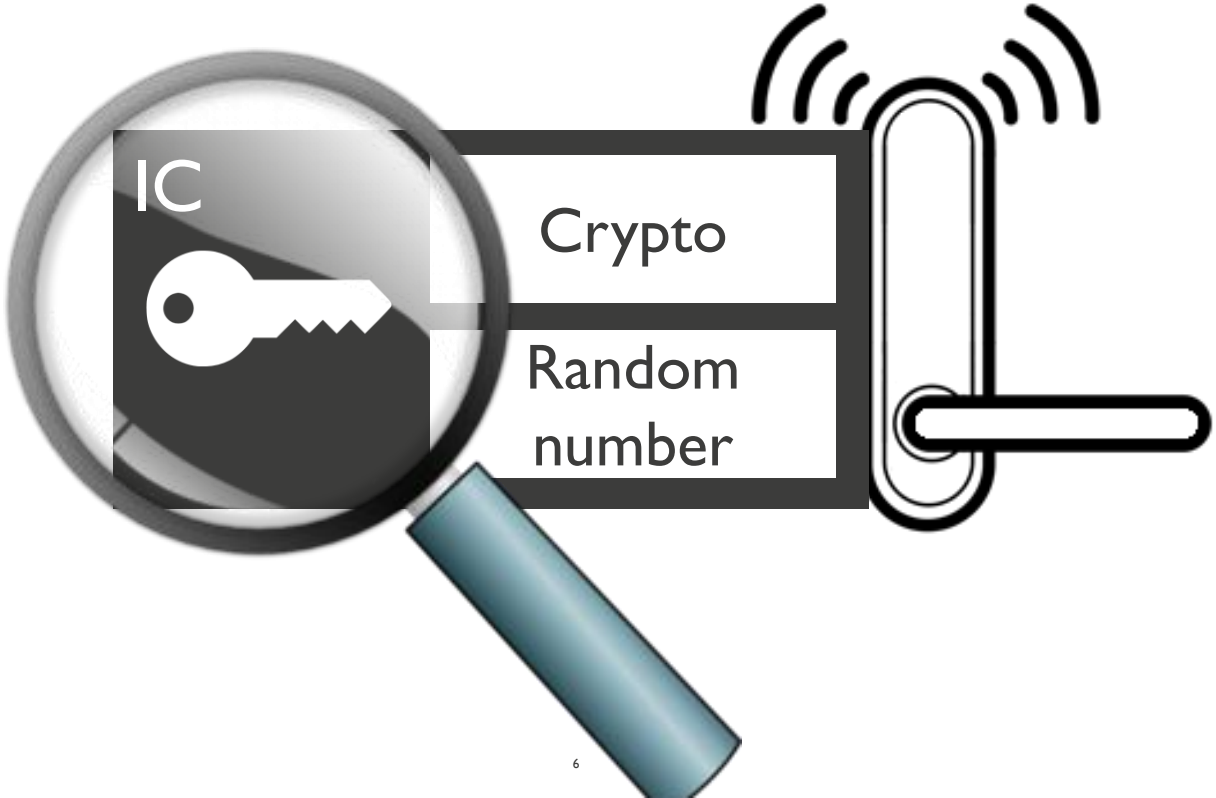


# PHYSICAL UNCLONABLE FUNCTIONS



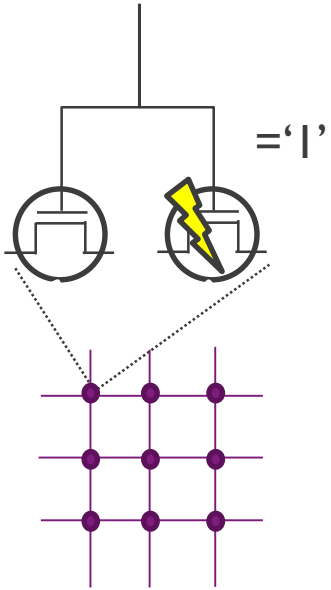

IC
Crypto
Random number
Hello, this is my challenge (nonce)
This is my sensitive response
Physical attack
• Power
• Electromagnetic
• Timing
• Optical
Eavesdropping (read)
Manipulation (write)
Replay/relay (history)

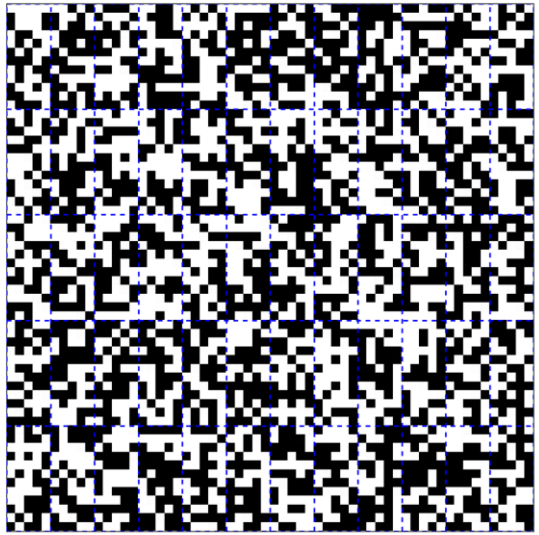

IC
Crypto
Random number
7%j92#€Dfkj
diESK&3kl
Physical attack
• Power
• Electromagnetic
• Timing
• Optical
~~Eavesdropping~~ (~~read~~)
~~Manipulation~~ (~~write~~)
Replay/relay (history)

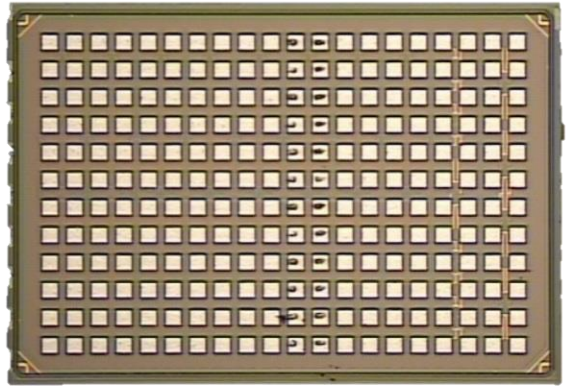

IC
Crypto
Random
number

# IMEC'S PHYSICAL UNCLONABLE FUNCTION (PUF)

## BASED ON INTRINSIC RANDOMNESS OF OXIDE BREAKDOWN POSITIONS IN CMOS



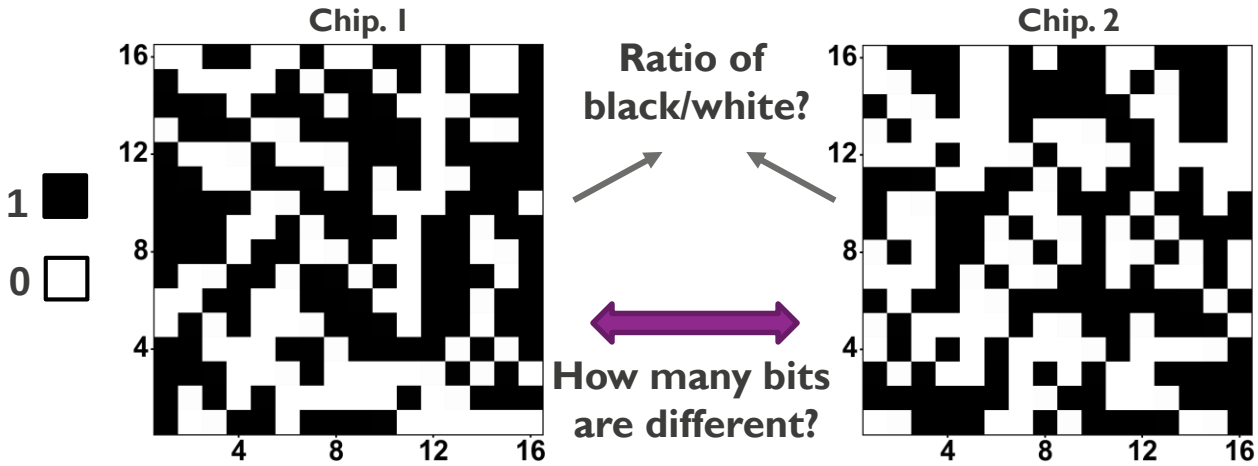





3 unique features

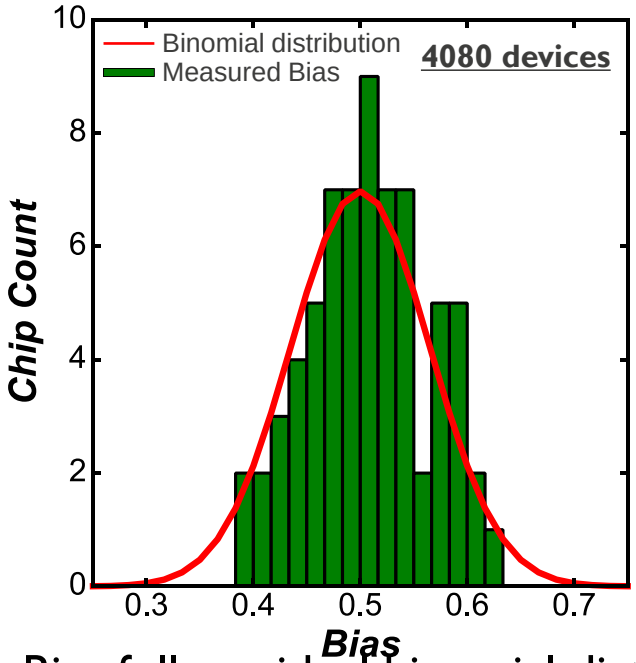
- ✓ Low cost, low power for IoT, reliable, small footprint
- ✓ No trusted third party: key generation by service provider
- ✓ Both random key generation & programmable keys

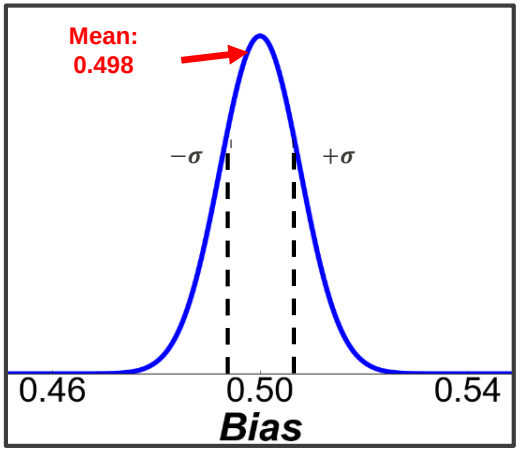
# HOW GOOD IS THE PUF? RANDOMNESS AND UNIQUENESS




- Randomness
  - Probability of having "1" and "0"
- Uniqueness
  - Difference between chips

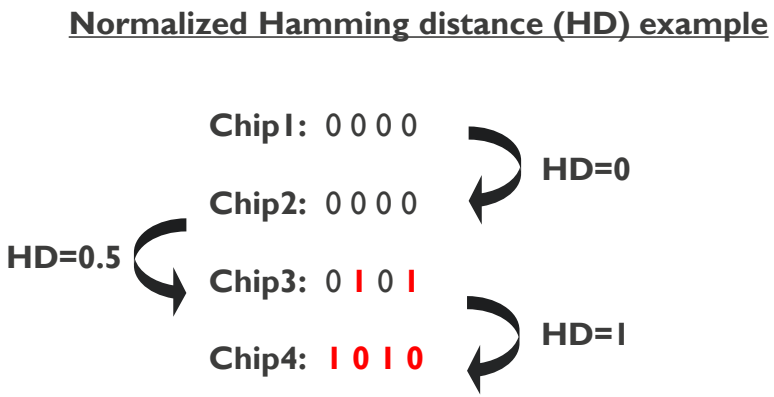
# (I) RANDOMNESS: FOLLOWS BINOMINAL DISTRIBUTION

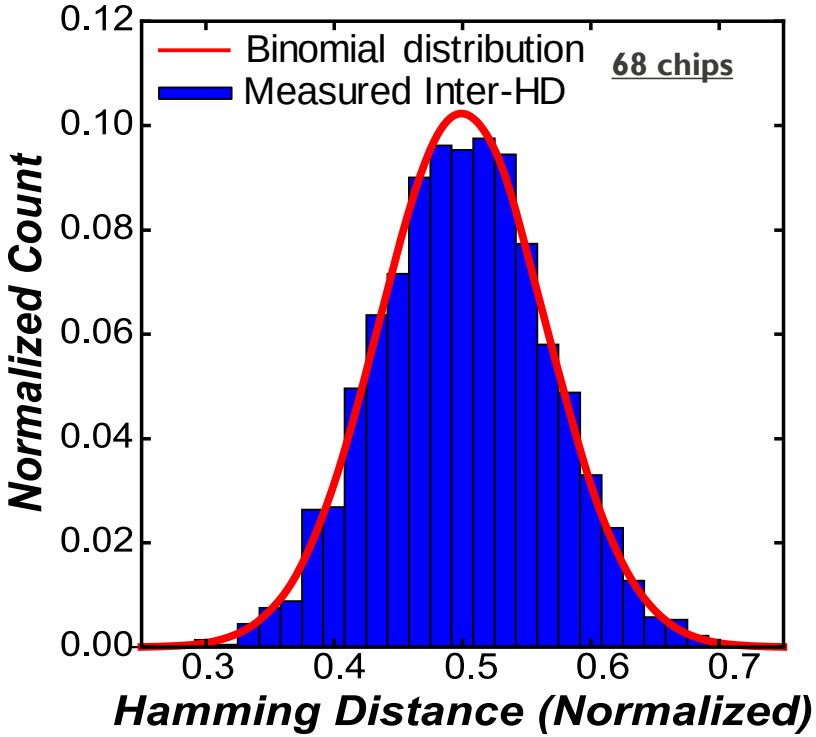


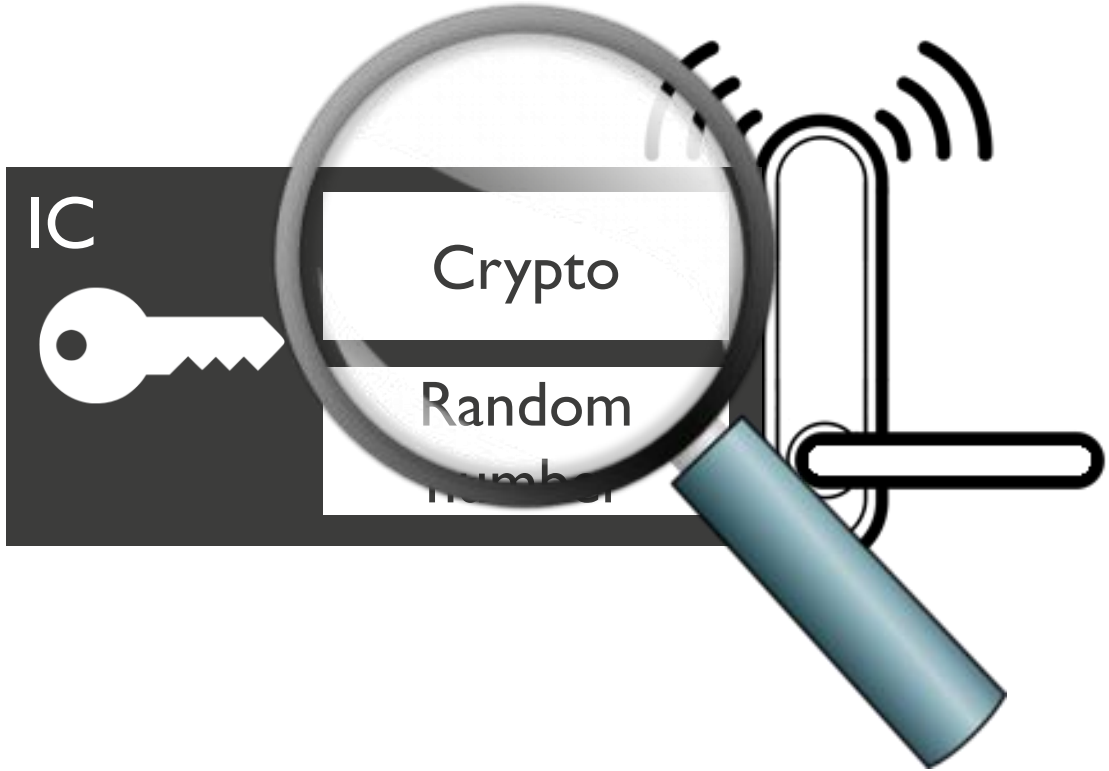

- Bias follows ideal binomial distribution
  - Equal probability to produce "0" and "1"
- Overall bias 0.498 is within ±σ bound

# (II) UNIQUENESS: INTERCHIP HAMMING DISTANCE



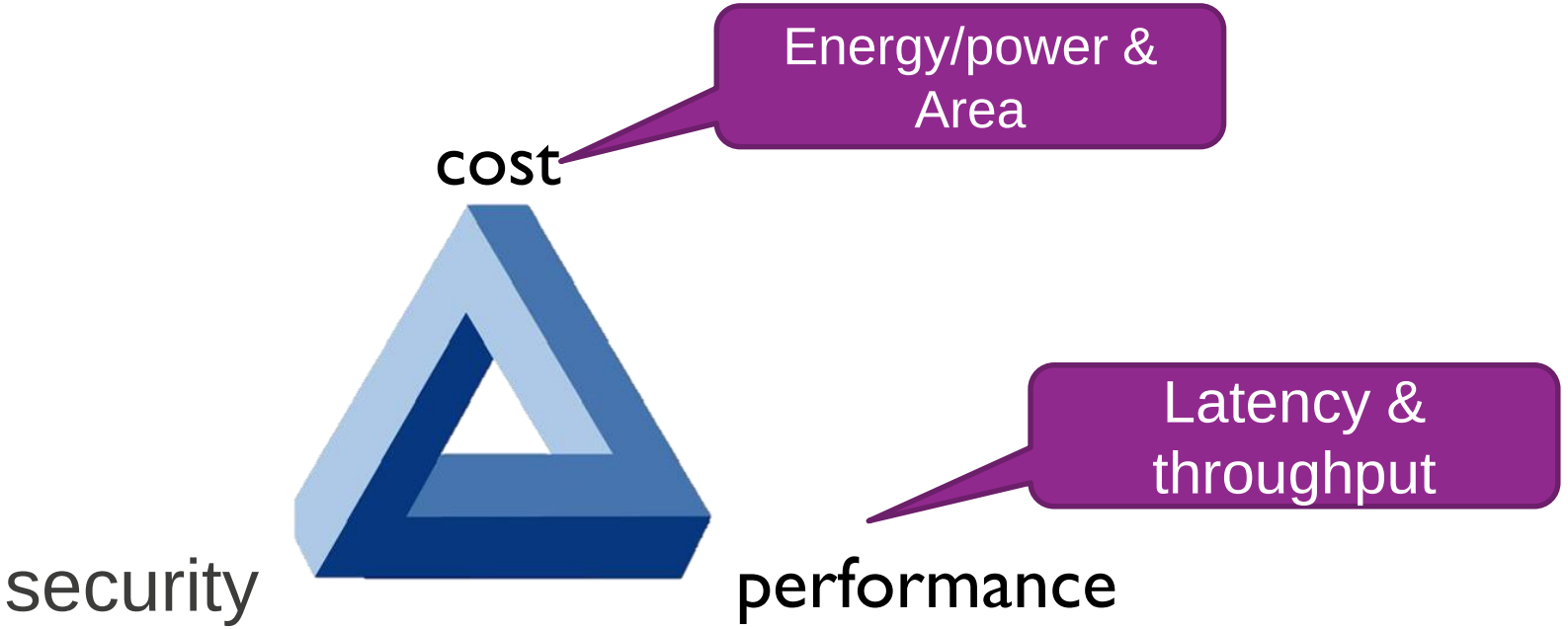




- HD follows ideal binomial distribution
  - Data pattern in each chip is unique
  - HD has to be 0.5
- The resulting PUF data is unpredictable


IC
Crypto
Random

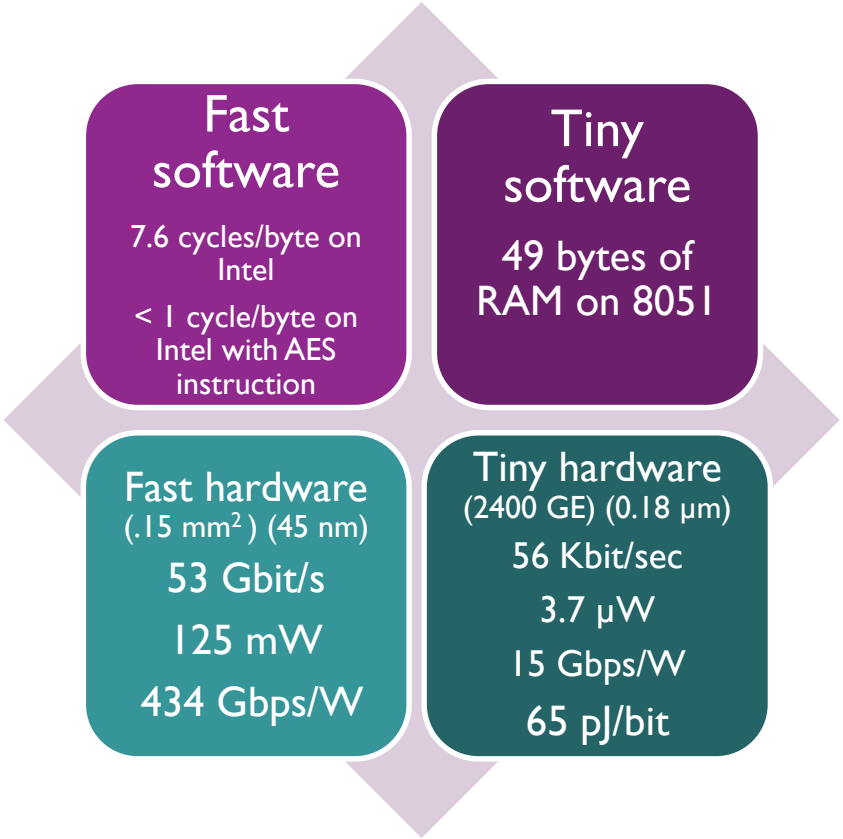
# AES – INVENTED BY IMEC RESEARCH GROUP COSIC AT KU LEUVEN

# LIGHTWEIGHT CRYPTO: CAN WE IMPROVE OVER AES?

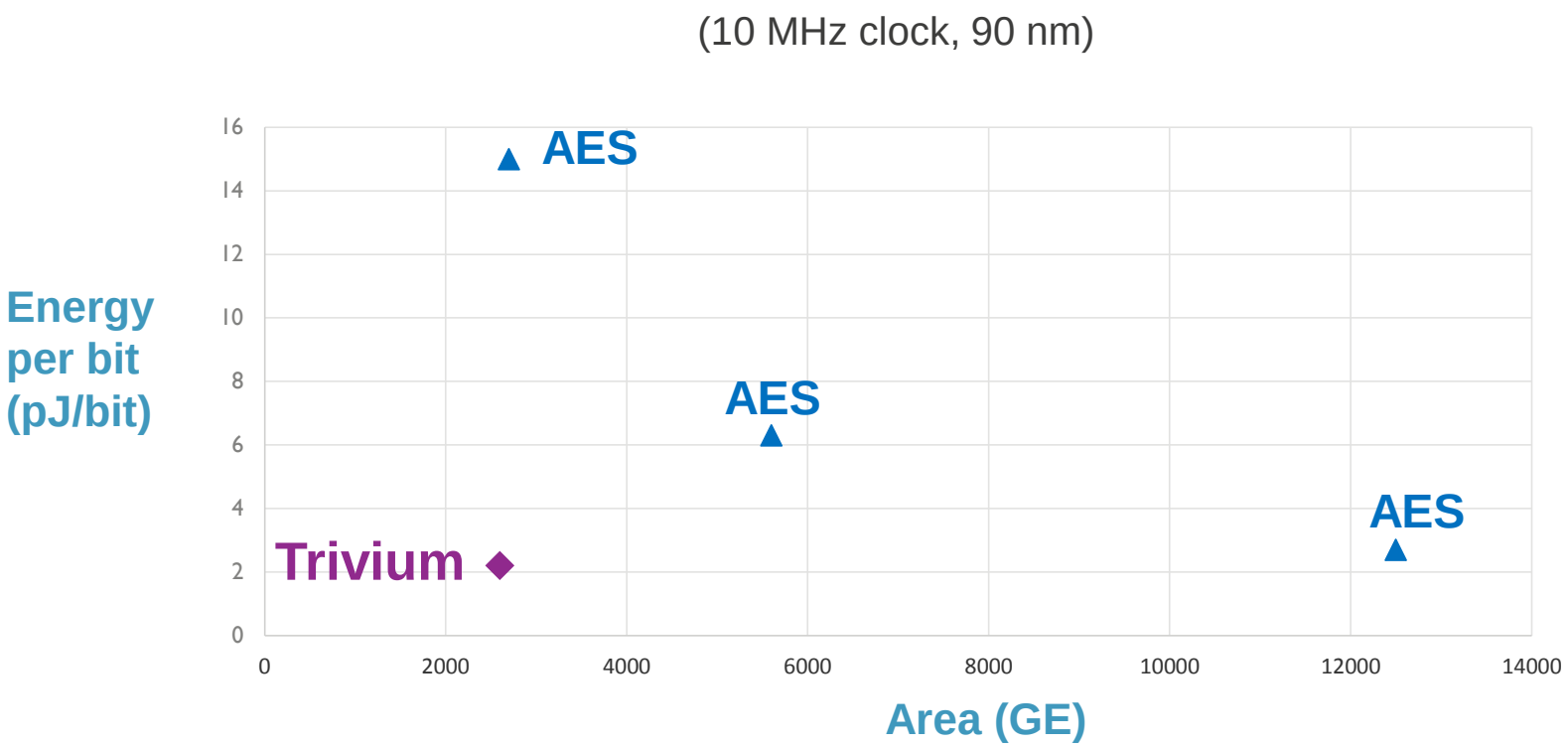


# AES IMPLEMENTATIONS – DESIGNED@COSIC

- Global de facto standard: ISO, IETF, IEEE 802.15.4, Lora, WPA2
- > 4000 certified products
- Billions of deployments

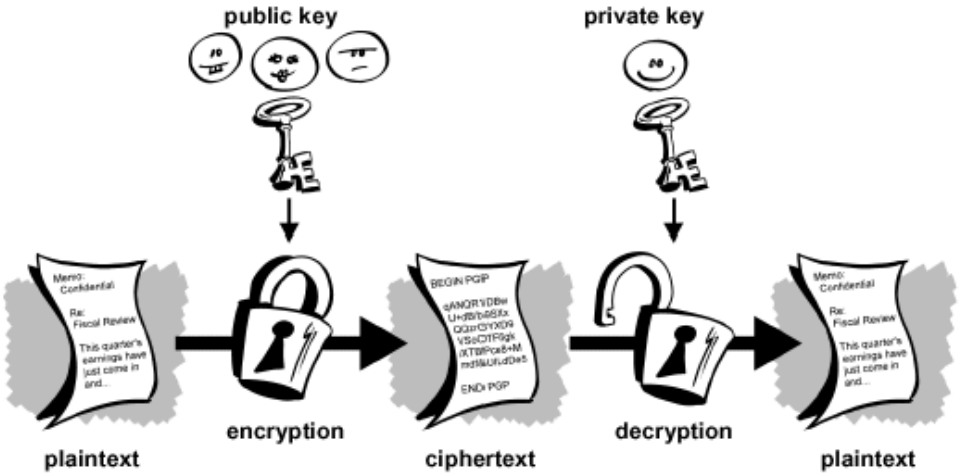


# LIGHTWEIGHT CRYPTO: ENERGY PER BIT VERSUS AREA



# PUBLIC-KEY CRYPTOGRAPHY

- No global secrets
- Key management easier
- Energy cost several hundred times larger
- In practice: RSA and ECC



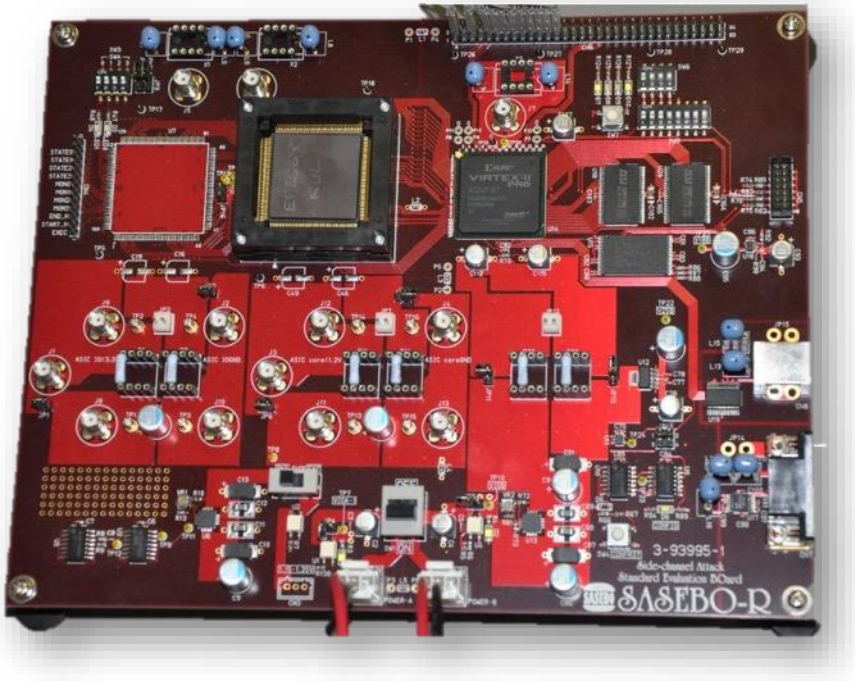
# SYMMETRIC KEY VERSUS PUBLIC-KEY CRYPTOGRAPHY

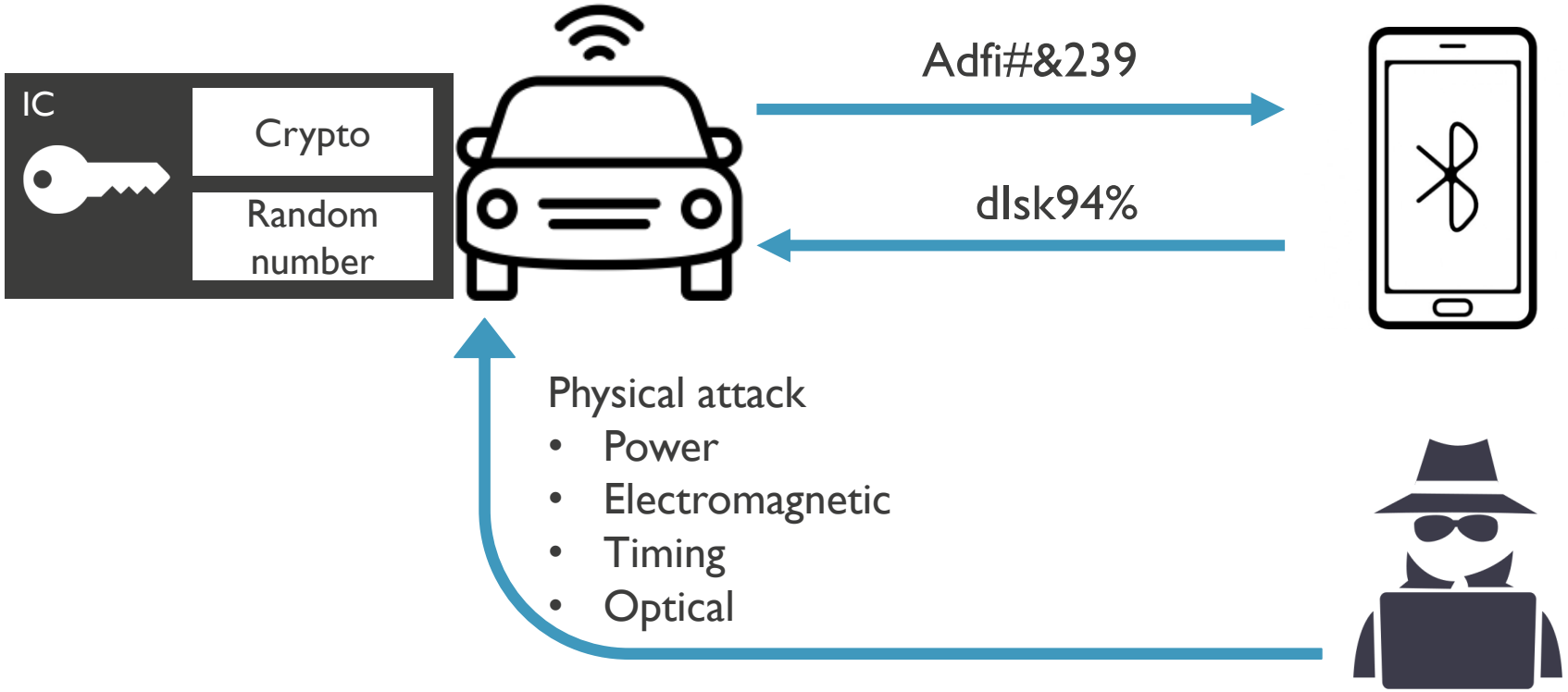
| | AES-128 – symmetric-key (128-bit security) | ECC-163 – public-key (80-bit security) |
|---|---|---|
| Latency (# cycles) | 226 | 86,200 |
| Power (µW) | 3.7 | 7.3 |
| Energy per bit (pJ/bit) | 65 | 38,600 |
| Technology (µm) | 0.18 | 0.13 |

# LOW POWER PUBLIC KEY CRYPTOGRAPHY FOR IoT DEVICES

- Public key crypto necessary for 50B+ IoT devices
- Efficient elliptic curve cryptography: one point multiplication <5µJ
- Based on optimized HW and SW co-design

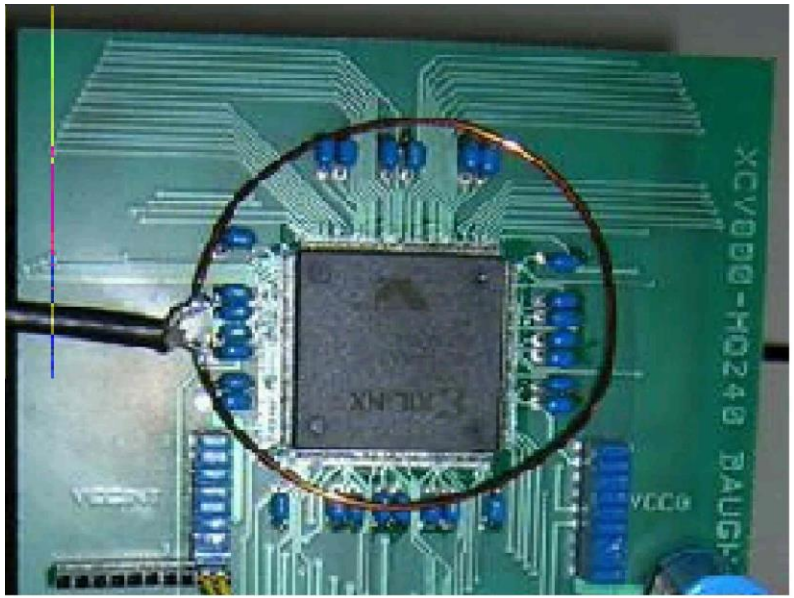
*Reference: Ingrid Verbauwhede et al, imec COSIC research group at KU Leuven*

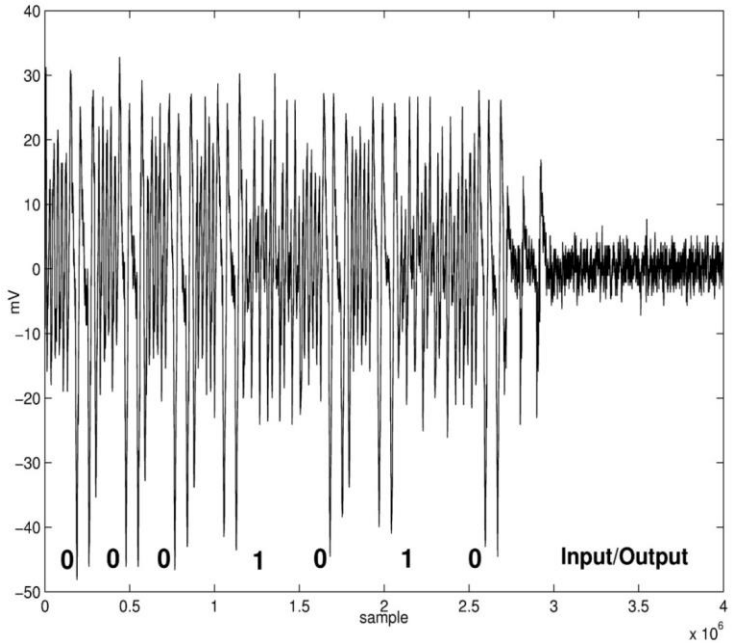


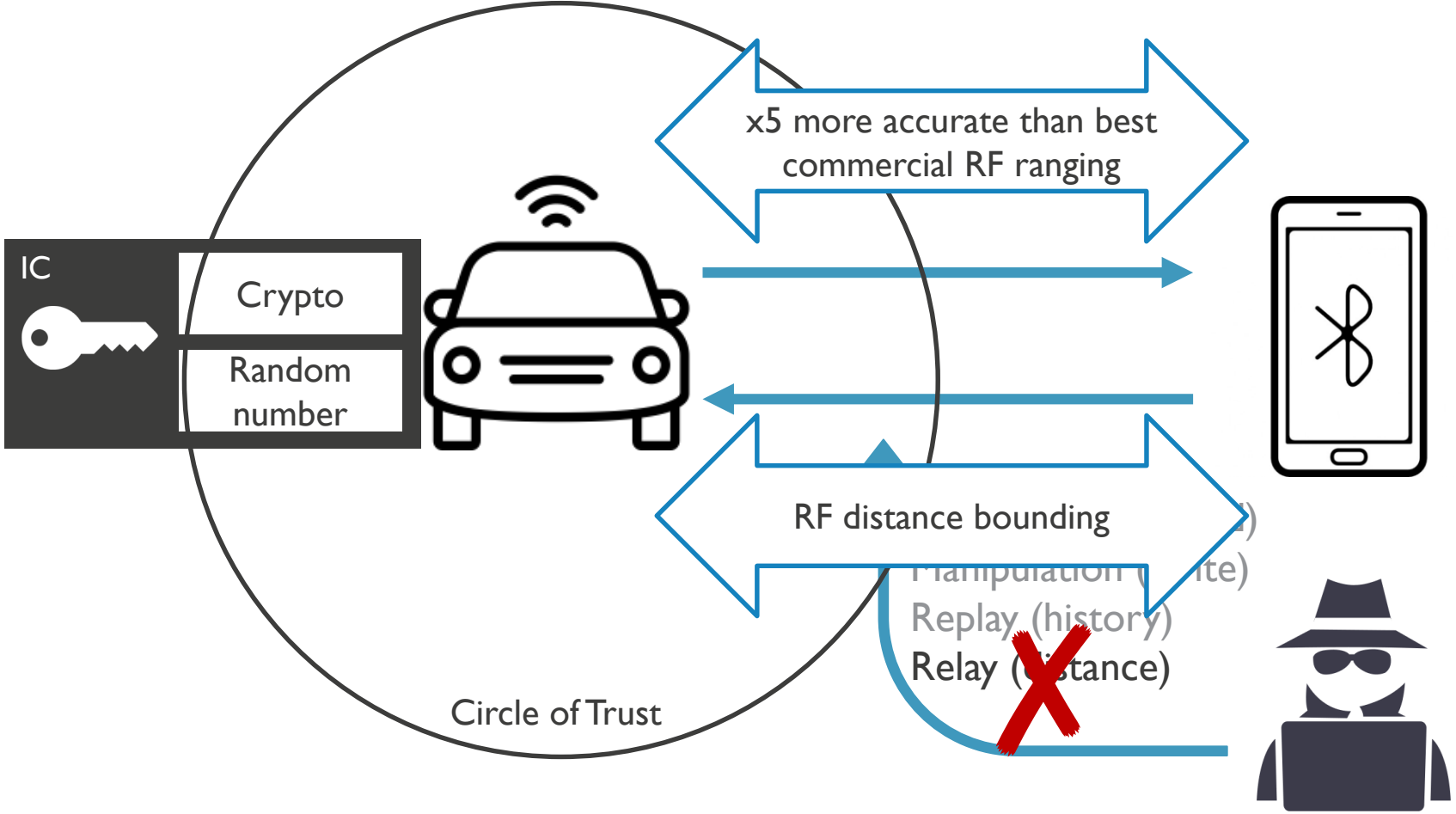

IC
Crypto
Random number
Adfi#&239
dIsk94%
Physical attack
• Power
• Electromagnetic
• Timing
• Optical

# PHYSICAL ATTACKS:

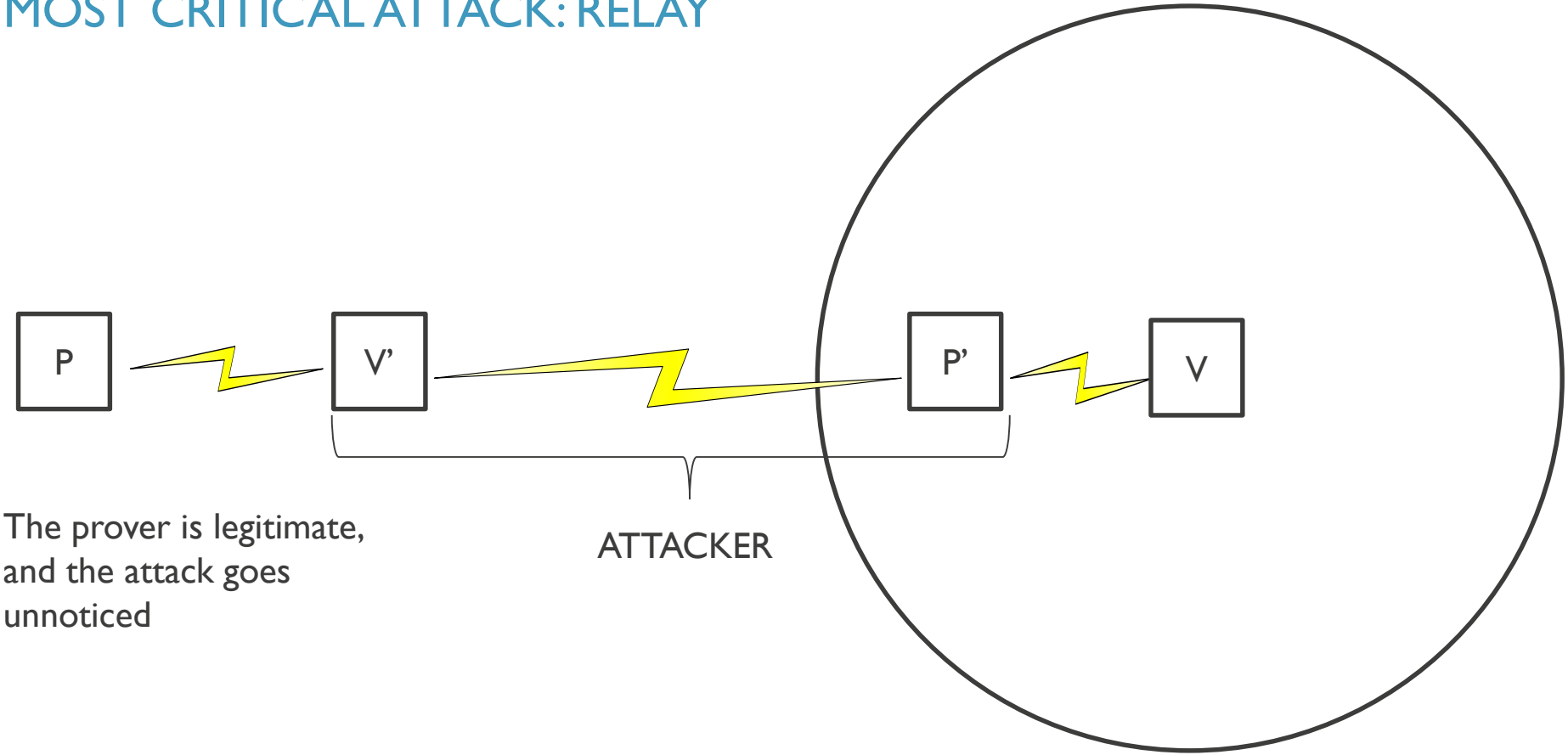
## COUNTERMEASURES CHANGE THE IMPLEMENTATION TRADEOFFS





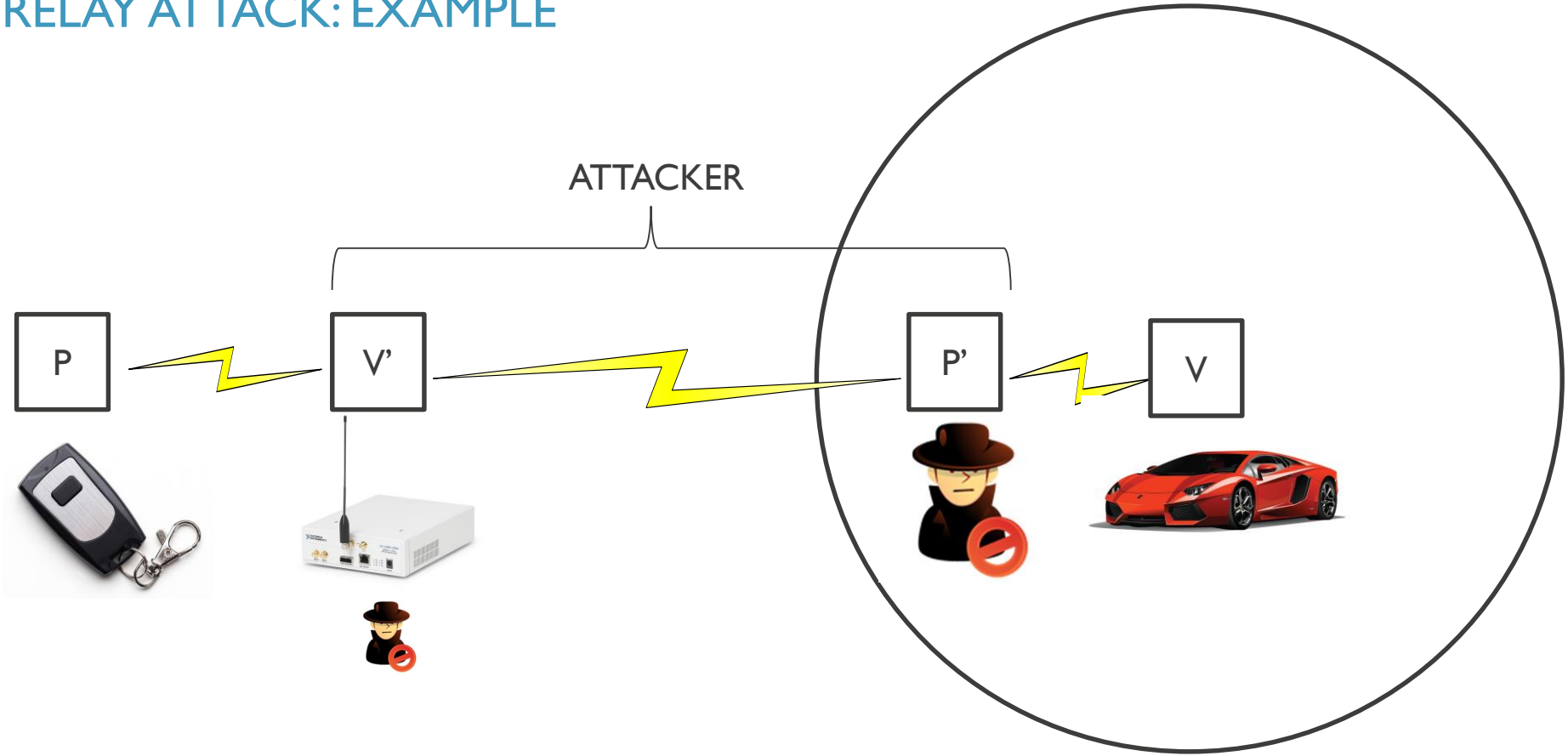

x5 more accurate than best commercial RF ranging
IC
Crypto
Random number
RF distance bounding
Replay (history)
Relay (distance)
Circle of Trust

# MOST CRITICAL ATTACK: RELAY




The prover is legitimate, and the attack goes unnoticed

# RELAY ATTACK: EXAMPLE

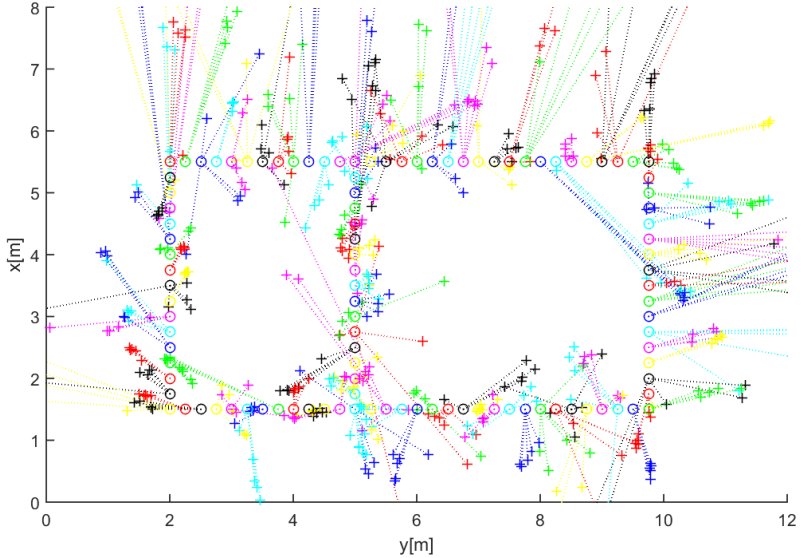



09-25-2017 Mon 01:01:25
WEST MIDLANDS POLICE
Camera 01

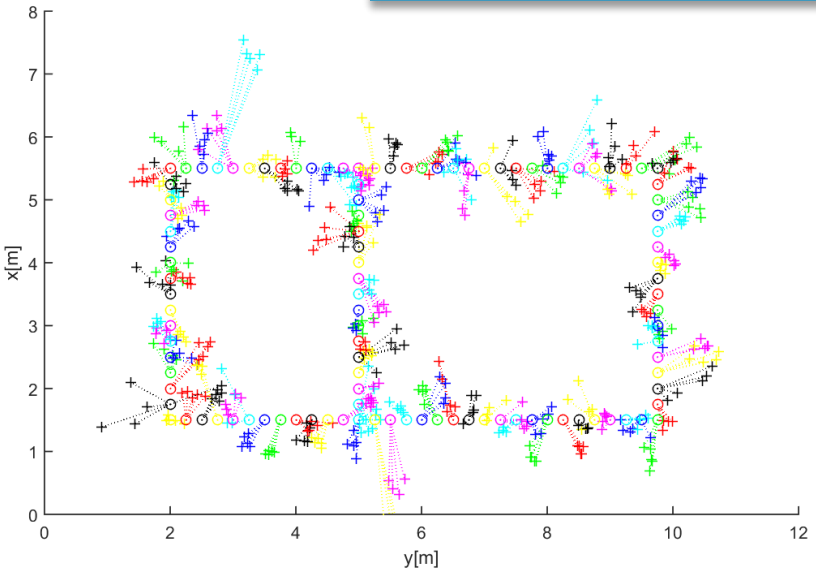
# RANGING: APPLES-TO-APPLES COMPARISON

## IN 2.4GHZ ISM BAND, ON STANDARDIZED RADIO

### Phase Difference - Atmel approach




Imec: x5 better



# SECURE PROXIMITY USE CASES


Smart locks

Secure data access

Secure Commissioning

Next generation BLE beacons

# R&D TEAM


Trust4Cloud

Security4IoT

Data Protection & Privacy

# IN SUMMARY: A WINNING HAND TO DEAL WITH THE COMPLEXITY

**THOMAS KALLSTENIUS, PhD**
program director distributed trust
thomas.kallstenius@imec.be

Kapeldreef 75
3001 Leuven
Belgium

M +32 477 96 13 63

www.imec-int.com

imec

**THOMAS KALLSTENIUS, PhD**
program director distributed trust
thomas.kallstenius@imec.be

Kapeldreef 75
3001 Leuven
Belgium

M +32 477 96 13 63

www.imec-int.com

imec

**THOMAS KALLSTENIUS, PhD**
program director distributed trust
thomas.kallstenius@imec.be

Kapeldreef 75
3001 Leuven
Belgium

M +32 477 96 13 63

www.imec-int.com

imec