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

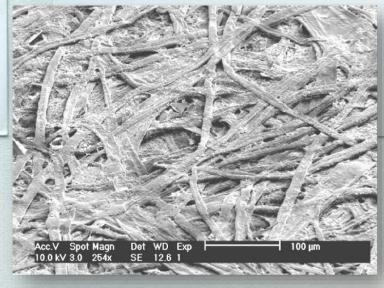
Kapeldreef 75 3001 Leuven Belgium M +32 477 96 13 63

www.imec-int.com

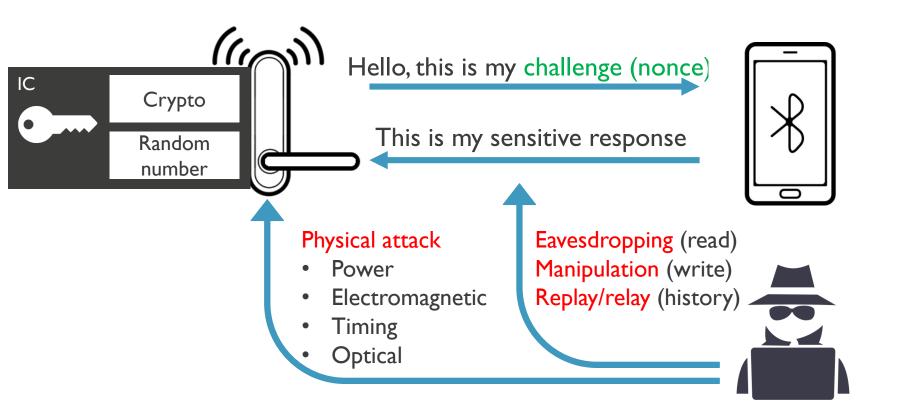
mec

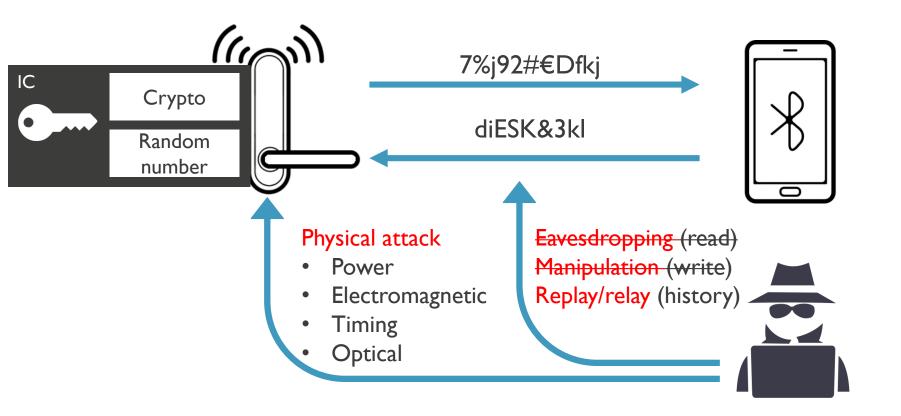
THOMAS KALLSTENIUS, PhD

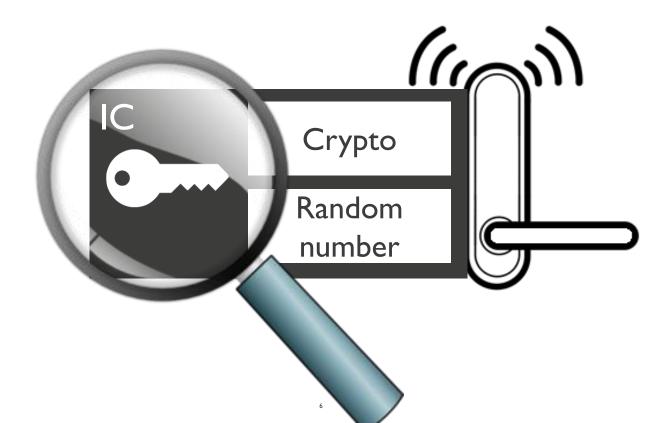
program director distributed trust thomas.kallstenius@imec.be



PHYSICAL UNCLONABLE FUNCTIONS





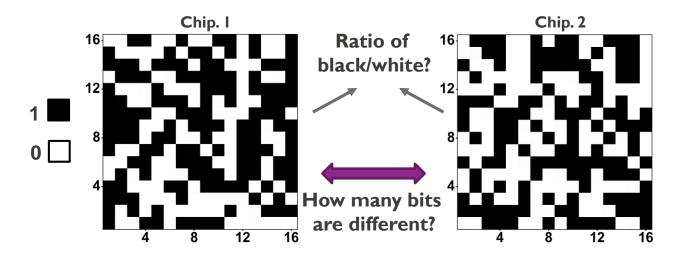


IMEC'S PHYSICAL UNCLONABLE FUNCTION (PUF) BASED ON INTRINSIC RANDOMNESS OF OXIDE BREAKDOWN POSITIONS IN CMOS



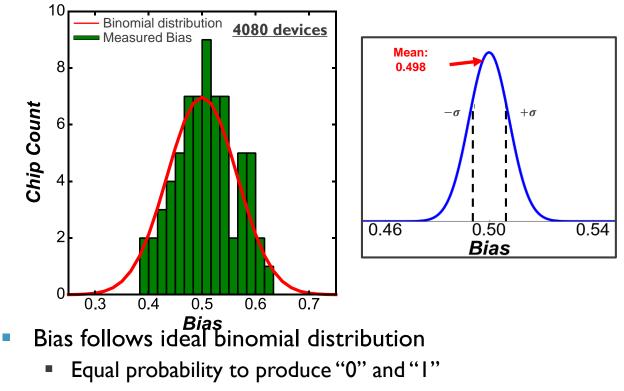
3 unique features Low cost, low power for IoT, reliable, small footprint
No trusted third party: key generation by service provider
Both random key generation & programmable keys

HOW GOOD IS THE PUF? RANDOMNESS AND UNIQUENESS



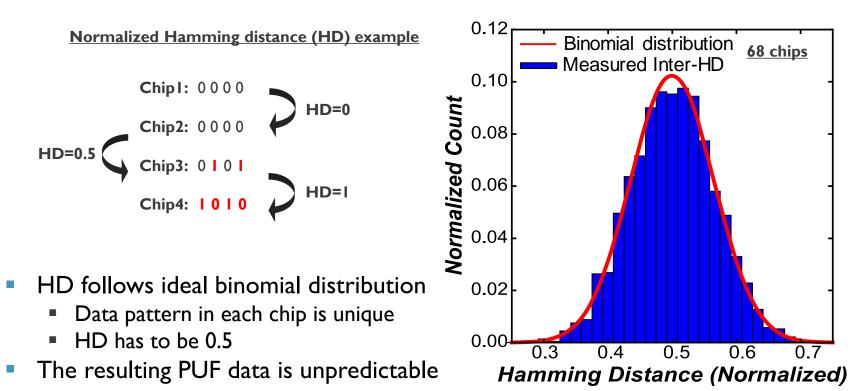
- Randomness
 - Probability of having "I" and "0"
- Uniqueness
 - Difference between chips

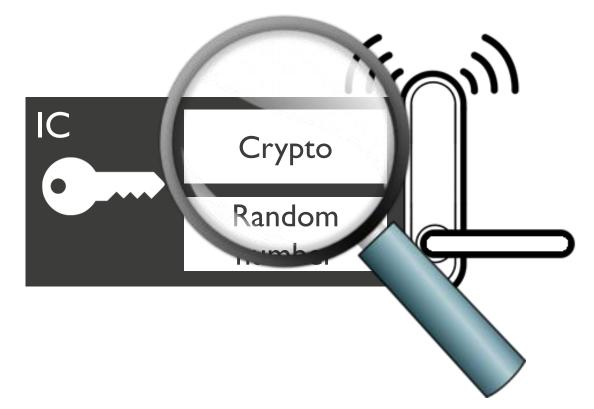
(I) RANDOMNESS: FOLLOWS BINOMINAL DISTRIBUTION



Overall bias 0.498 is within ±σ bound

(II) UNIQUENESS: INTERCHIP HAMMING DISTANCE





AES – INVENTED BY IMEC RESEARCH GROUP COSIC AT KU LEUVEN

0 1 0 40 Mar 10.52 AM Q # Finder File Edit View Go Window Help ●●● 🗉 💷 < > 🏠 🛒 ⊕ ●●● □ == < > ☆ == 0 0 0 0 0 0 i en.wikipedia.org iii wsj.com Stoxx 600 🔺 374.73 0.34% U.S. 10 Yr A 4/32 Yield 2.589% Euro ± 1.0628 0.22% . Buttenslides Talk Sandbox Preferences Beta Watchlist Contributions Log out = THE WALL STREET JOURNAL. Read Edit View history 🏠 Search Wikipedia Article Talk Subscribe Sign In CLOSE X WIKIPEDIA Wikimania, our Wikimedia community conference. - U.S. Officials Plan -- Big Tech Deadline to propose posters, discussions, and trainings is March 30th! to Unveil Charges The Free Encyclopedia Reshapes Auto Drivin with translational Tied to Yahoo Hack Supply Chain With atest Deals Main page Advanced Encryption Standard Contents Featured content (★) (*) (A) 622 From Wikipedia, the free encyclopedia Current events Random article The Advanced Encryption Standard (AES), also Donate to Wikipedia Advanced Encryption Standard known by its original name Rijndael.[5][6] is a In Belgium, an Encryption (Rijndael) Wikipedia store specification for the encryption of electronic data Interaction a, a, a, a, a, b., b., b., b., established by the U.S. National Institute of Powerhouse Rises Help Sublivies Di Di Di Di Di Di Standards and Technology (NIST) in 2001.[7] a, a, a, a, a, About Wikipedia a. a. a. Community portal AES is a subset of the Rijndael cipher^[8] developed University of Leuven has become a battleground in the fight Recent changes by two Belgian cryptographers, Joan Daemen and a, a, a, between privacy and surveillance Contact page Vincent Rijmen, who submitted a proposal to NIST during the AES selection process.[8] Rijndael is a What links here The SubBytes step, one of four stages in a round By AMIR MIZROCH family of ciphers with different key and block sizes. Related changes of AFS Updated Dec. 10, 2015 8:51 p.m. ET For AES, NIST selected three members of the Unload file Genera Special pages Rijndael family, each with a block size of 128 bits, Designers Vincent Rijmen, Joan Daemen Permanent link

but three different key lengths: 128, 192 and 256

is now used worldwide. It supersedes the Data

in 1977. The algorithm described by AES is a

AES has been adopted by the U.S. government and

Encryption Standard (DES),[9] which was published

symmetric-key algorithm, meaning the same key is

used for both encrypting and decrypting the data.

Page information

Wikidata item Cite this name

Create a book

In other projects

Download as PDF

Printable version

Print/export

bits.

First

nublished

Successors

Key sizes

Derived from Square

1998

NSA

100 644

Anubis, Grand Cru

Certification AES winner, CRYPTREC, NESSIE,

Cipher detail

128, 192 or 256 bits^[1]

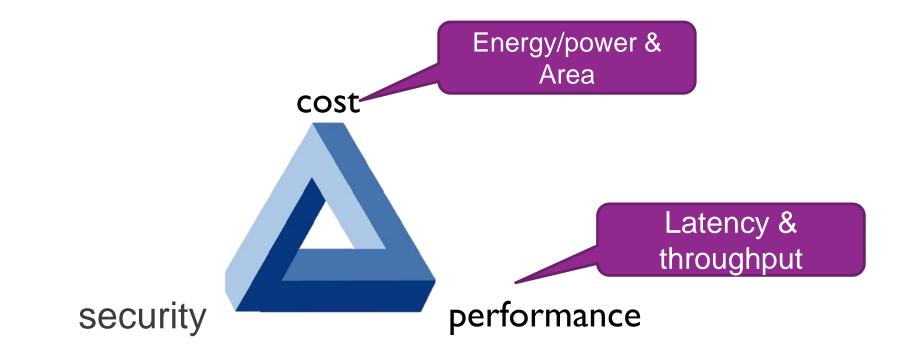
LEUVEN, Belgium-A 600-year-old Catholic university here has become an unexpected battleground in the fight between privacy advocates and those who think governments and law enforcement need more powerful online surveillance.

a

>

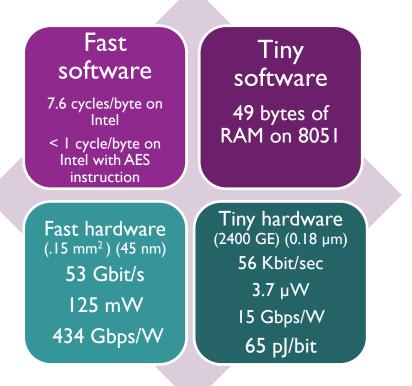
Tucked in the woods outside this medieval town in Dutch-speaking Flanders, the electrical-engineering department of Katholieke Universiteit Leuven is

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



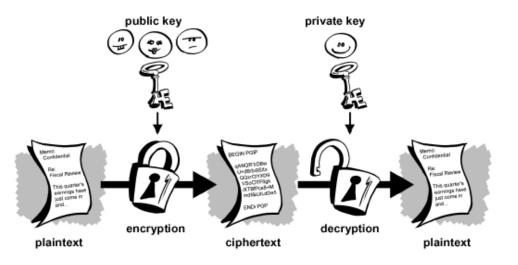
LIGHTWEIGHT CRYPTO: ENERGY PER BIT VERSUS AREA

(10 MHz clock, 90 nm)



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

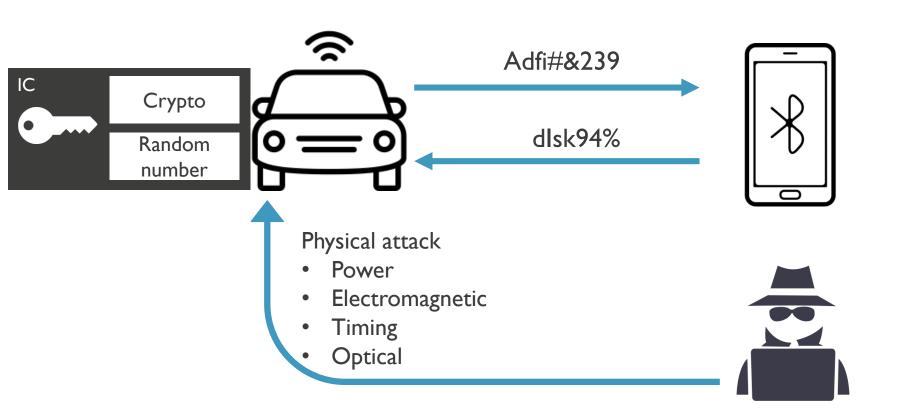
	AES-128 – symmetric-key (128-bit security)	ECC-163 – public-key (80-bit security)
Latency (# cycles)	226	86,200
Power (µW)	3.7	7.3
Energy per bit (pJ/bit)	65	38,600
Technology (µm)	0.18	0.13

LOW POWER PUBLIC KEY CRYPTOGRAPHY FOR IoT DEVICES

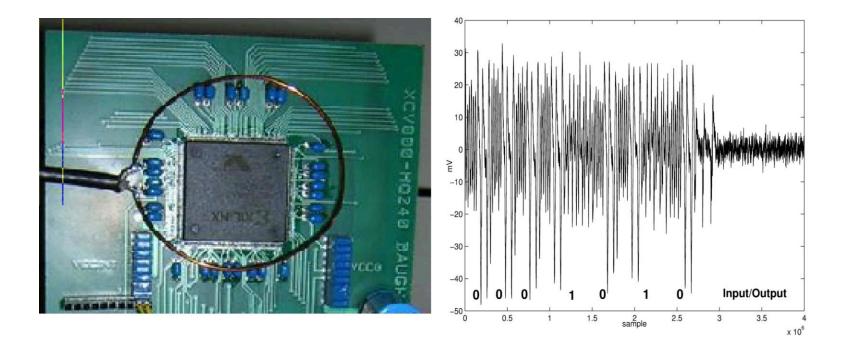
- Public key crypto necessary for 50B+ IoT devices
- Efficient elliptic curve cryptography: one point multiplication <5µJ
- Based on optimized HW and SW codesign

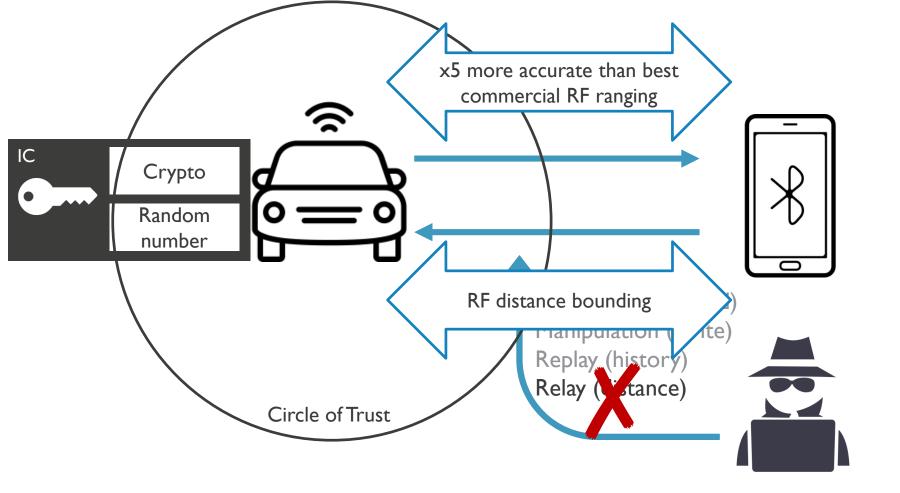
Reference: Ingrid Verbauwhede et al, imec COSIC research group at KU Leuven

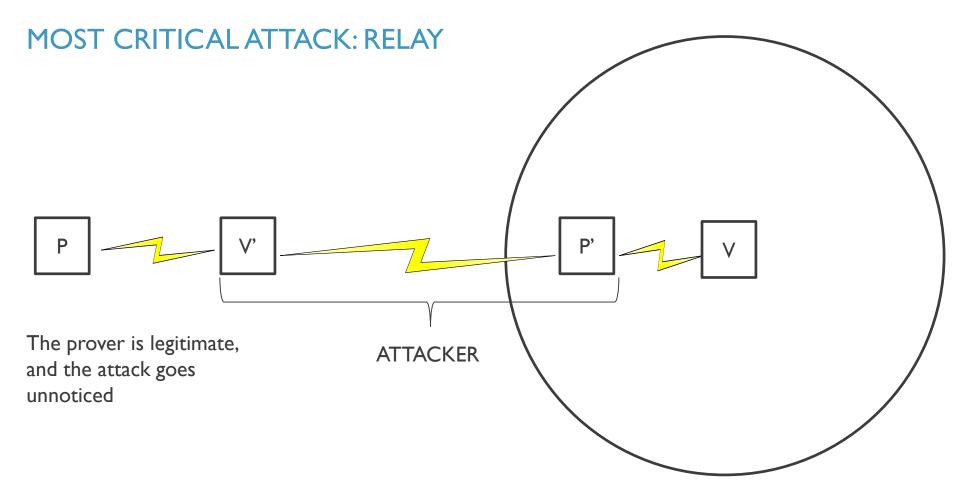


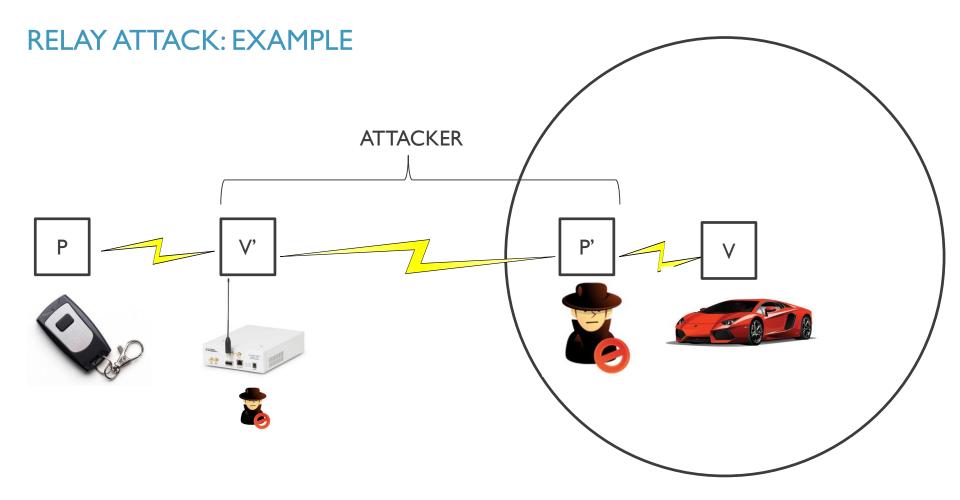


PHYSICAL ATTACKS: COUNTERMEASURES CHANGE THE IMPLEMENTATION TRADEOFFS









-

.

MID,

OLV

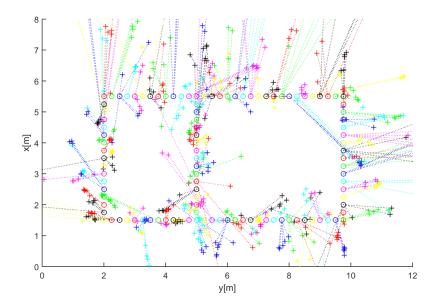
SQ

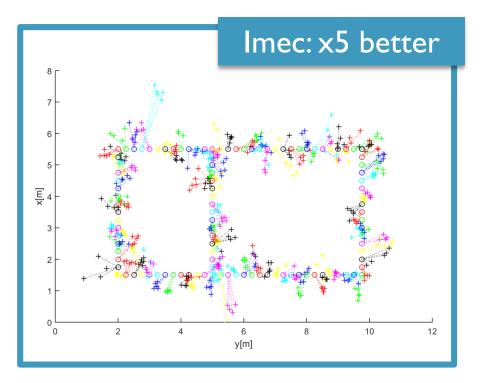
WEST

Camera 01

RANGING: APPLES-TO-APPLES COMPARISON IN 2.4GHZ ISM BAND, ON STANDARDIZED RADIO

Phase Difference - Atmel approach









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

mec