Smart (health) systems need smart security

Dave Singelée

ESAT COSIC

KU Leuven - iMinds

Smart Systems Industry Summit
October 14, 2014

Outline of the talk

- Who are we?
- Smart medical devices: security risks
- Cryptographic solutions
- Key generation
- Privacy
- Conclusion

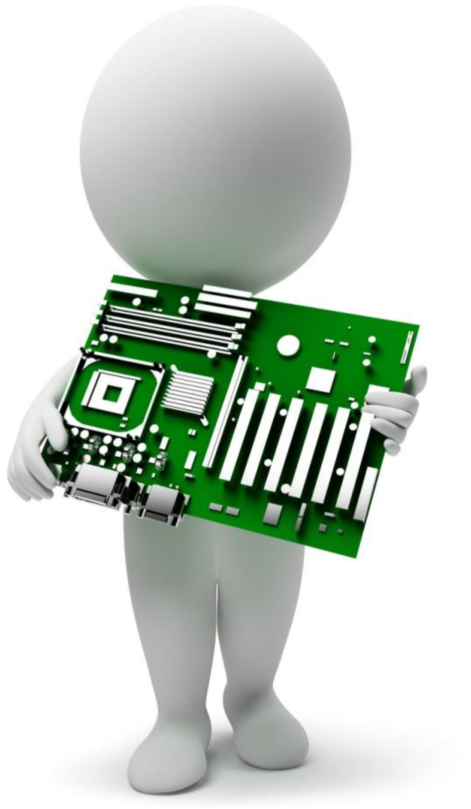
Outline of the talk

- Who are we?
- Smart medical devices: security risks
- Cryptographic solutions
- Key generation
- Privacy
- Conclusion

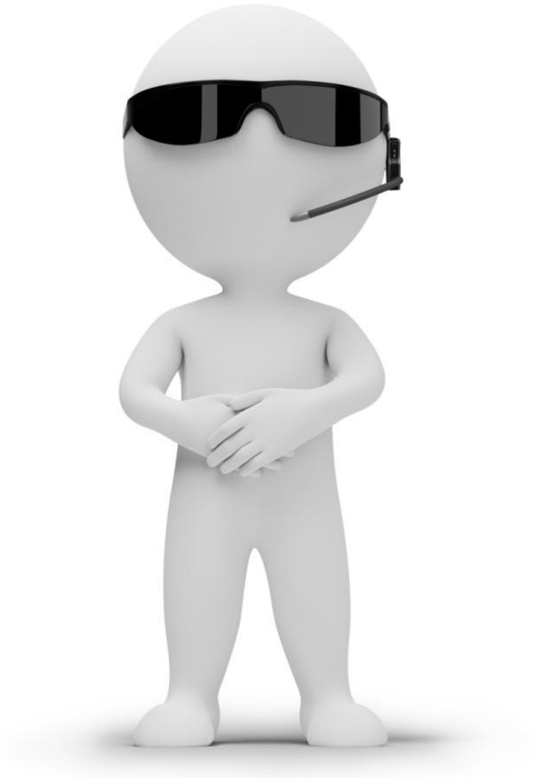
North Sea
BELGIUM
DENMARK
Kattegat
Copenhagen
Malmö
Bornholm
Hamburg
Bremen
Berlin
Poznań
Oder
Amsterdam
NETH.
Rotterdam
Essen
Cologne
Leipzig
Elbe
Brussels
Lille
Bonn
GERMANY
Prague
Frankfurt am Main
CZECH REP
Brno
Luxembourg
LUX.
Paris
Seine
Stuttgart
Strasbourg
Rhine
Munich
Danube
Vienna
LIECH.
AUSTRIA
Zürich
Bern
Vaduz

iMinds security department

ICRI
Legal
Engineering



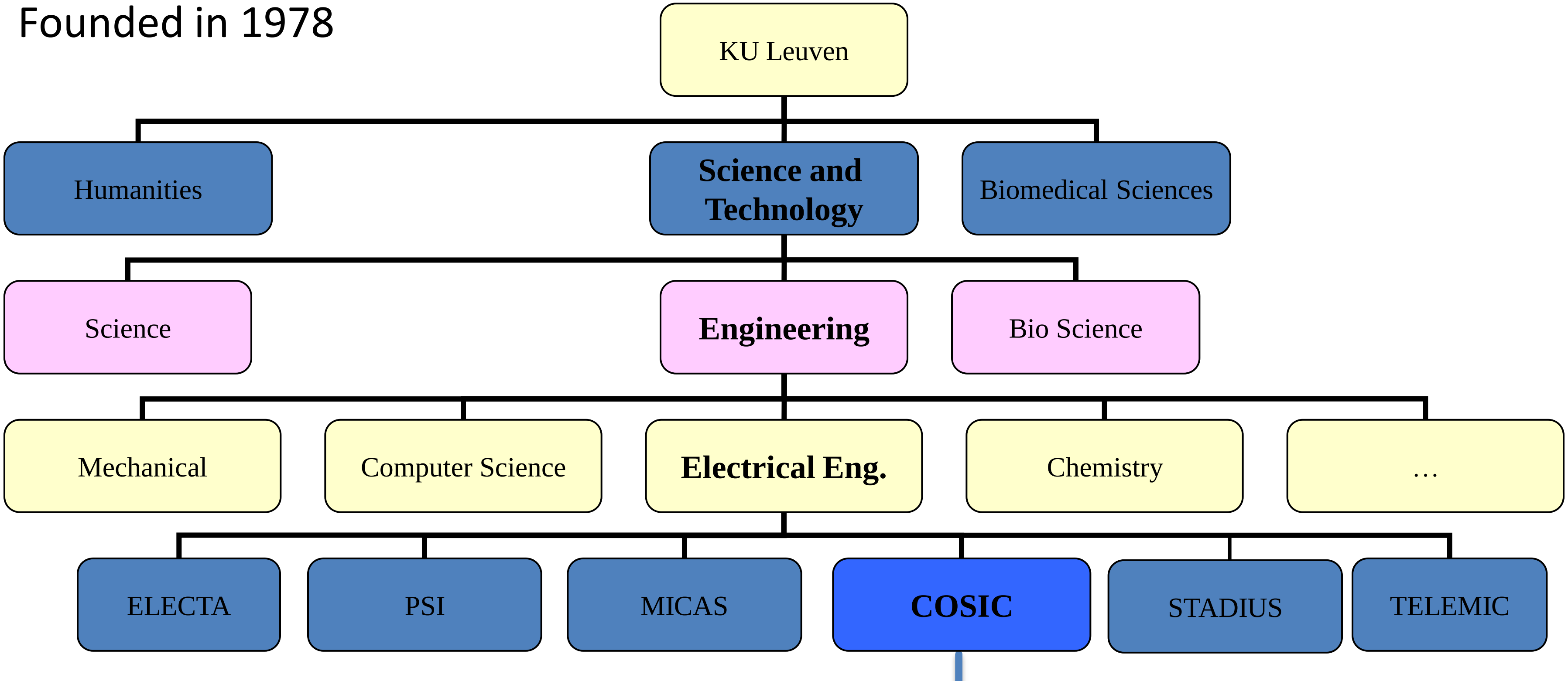
COSIC
Cryptographic
Engineering



DistriNet
Secure Software
Engineering

COSIC: COmputer Security and Industrial Cryptography

Founded in 1978



KU Leuven

Humanities

Science and Technology

Biomedical Sciences

Science

Engineering

Bio Science

Mechanical

Computer Science

Electrical Eng.

Chemistry

…

ELECTA

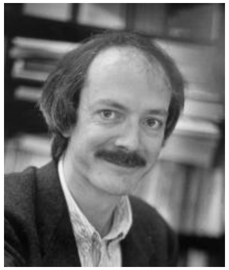
PSI

MICAS

COSIC

STADIUS

TELEMIC



Bart Preneel

Ingrid Verbauwhede

Vincent Rijmen

Claudia Diaz

COSIC - Research

Efficient and secure implementations

- software: block ciphers, point counting algorithms
- hardware: FPGA and ASIC
- side-channel attacks: power, timing, and electromagnetic analysis, fault attacks

Cryptographic protocols: design and cryptanalysis

entity authentication, credentials, oblivious transfer,

Cryptographic algorithms: design and cryptanalysis

block ciphers, stream ciphers, hash functions, MAC algorithms, (hyper)-elliptic curve cryptography
e.g.: AES, RIPEMD-160, HAMSI

Fundamental research in discrete mathematics

number theoretic algorithms, Boolean functions, secure multi-party computation, secret sharing

COSIC - Applications

Creating electronic equivalent of the real world:

confidentiality, digital signature, anonymity, payments, digital right managements, elections

- **Technologies:**
  - key management: ad hoc networks
  - anonymous communications and services
  - software tamper resistance and obfuscation
  - trusted platforms
  - multimedia security
- **Applications:**
  - electronic payments and commerce
  - e-government: electronic ID card, e-voting
  - car-to-car communications
  - **ehealth**

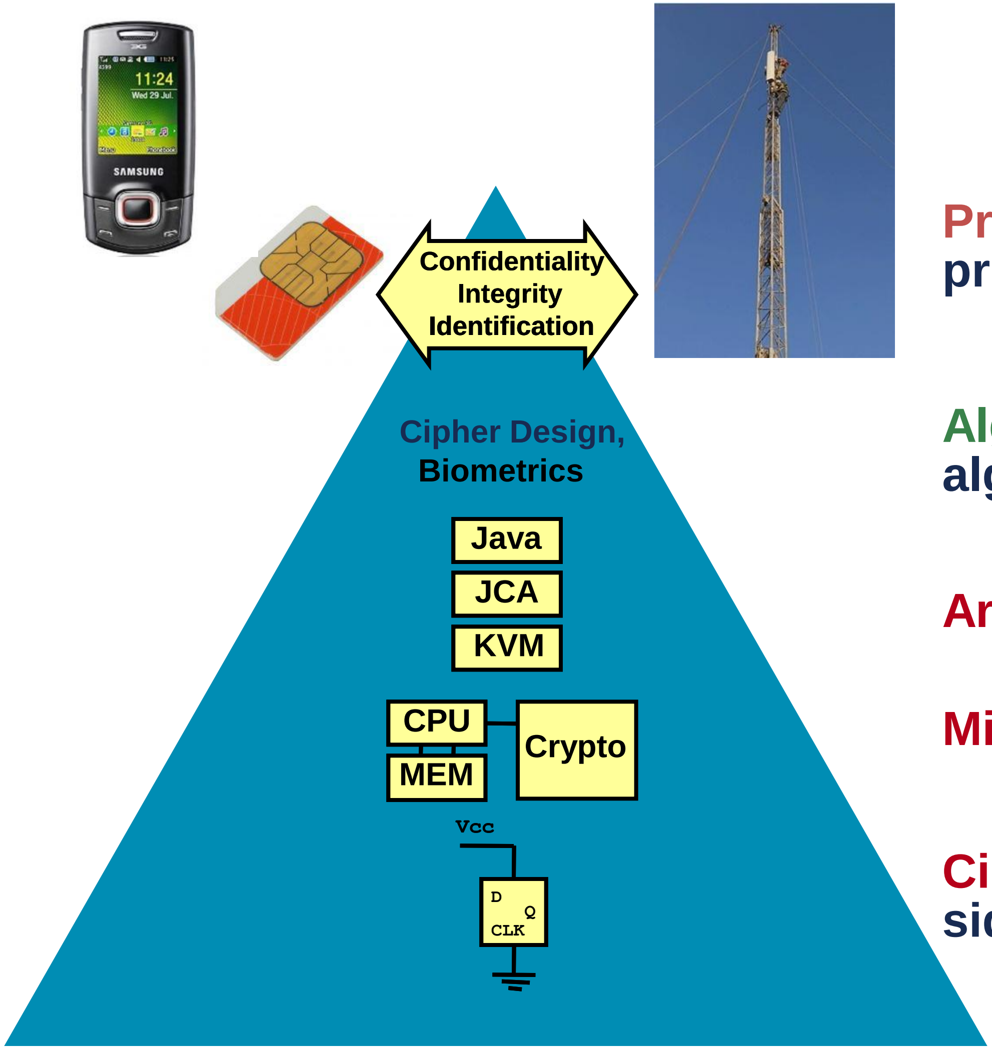
BELGIË IDENTITEITSKAART | BELGIQUE CARTE D'IDENTITE | BELGIEN PERSONALAUSWEIS | BELGIUM IDENTITY CARD

Naam / *Name* Dupont
Voornamen / *Given names* Sophie

Geboorteplaats en -datum / *Place and date of birth* Namen 01 MEI 1960
Geslacht / *Sex* V
Nationaliteit *Nationality* Belg
Kaartnr. / *Card No* 000-0001000-00

Geldig van - tot / *Valid from - until* 02.04.2003 - 02.04.2008
Handtekening van de houder / *Holder's signature*

Implementations in embedded systems



Protocol: low power authentication protocol design

Algorithm: public key, secret key, hash algorithms

Architecture: Co-design, HW/SW, SOC

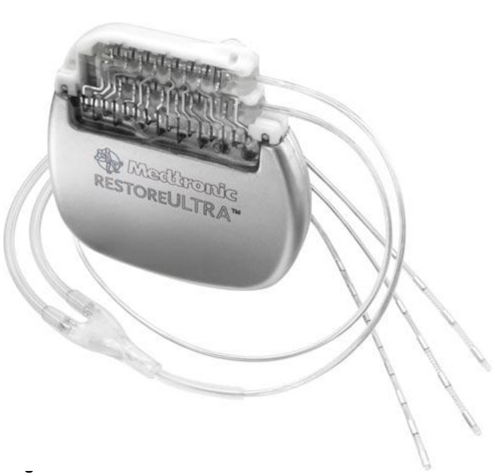
Micro-Architecture: co-processor design

Circuit: Circuit techniques to combat side channel analysis

Outline of the talk

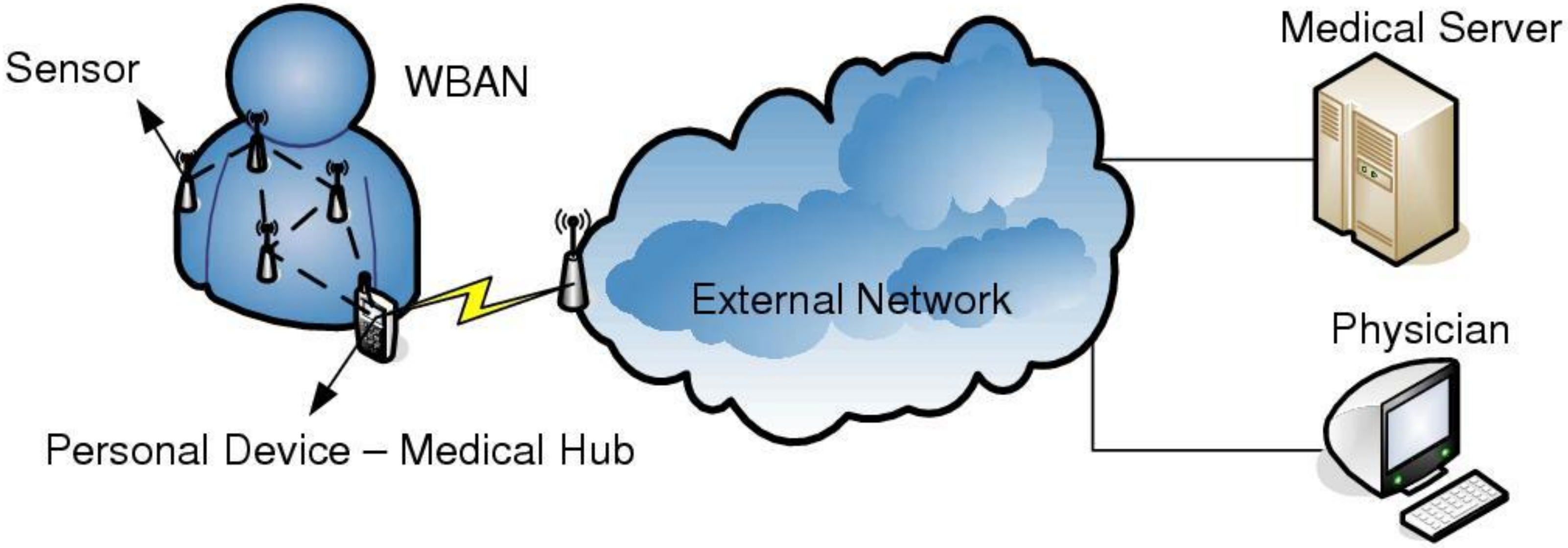
- Who are we?
- Smart medical devices: security risks
- Cryptographic solutions
- Key generation
- Privacy
- Conclusion

Implantable medical devices



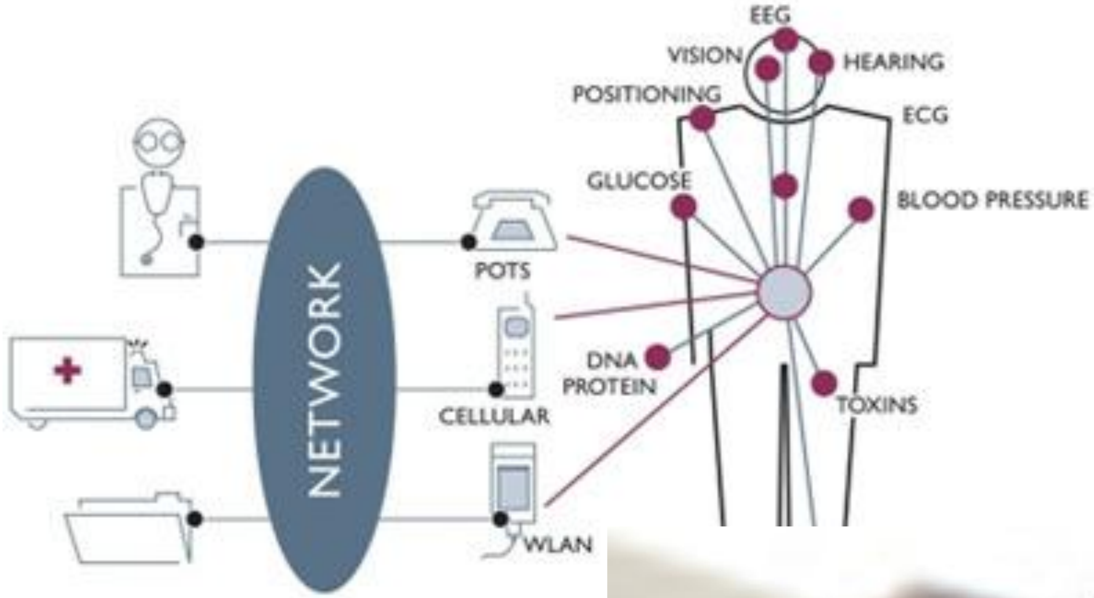
- Remote reprogramming / monitoring
- Software updates

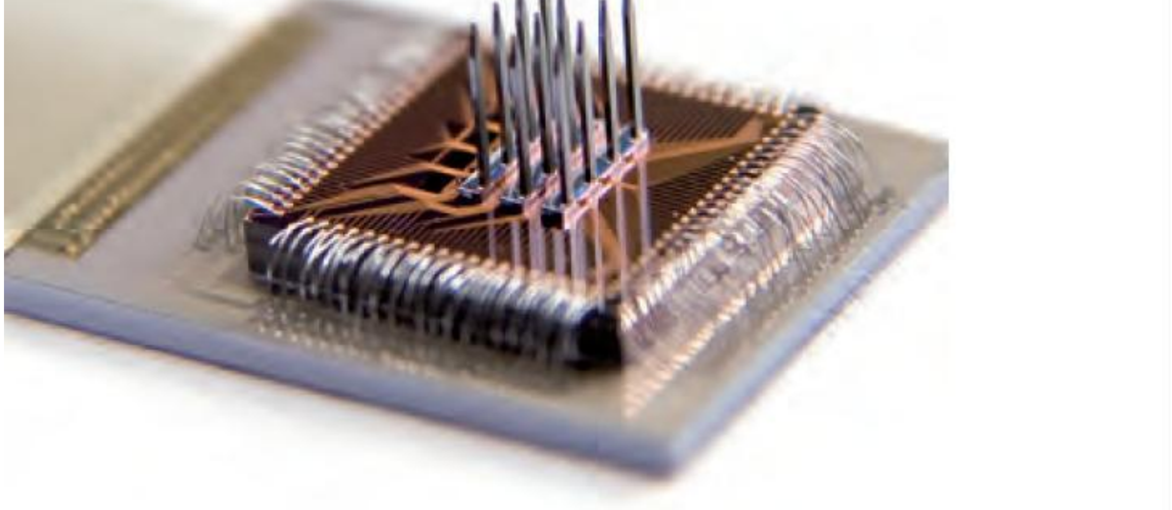
Wireless Body Area Networks



- WBAN: Sensor network on/in the patient
- Remote monitoring / reprogramming

(Ultra) low power medical devices



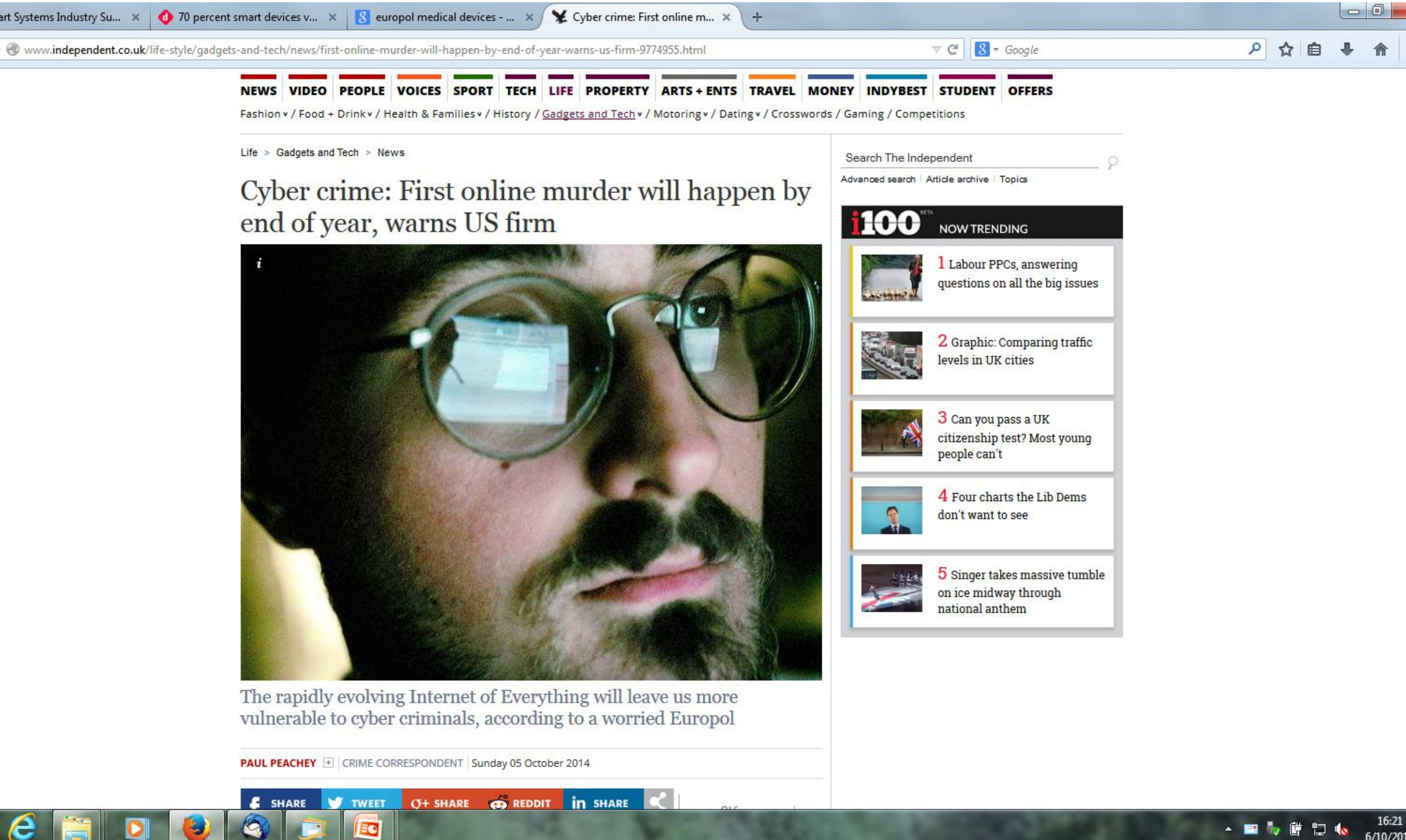


Wireless communication link

- **Wireless communication** omnipresent
  - MICS band / Bluetooth / ZigBee / …
  - More convenient
  - Extract medical telemetry
  - Remote commands
  - (Re)configuring device

- Wireless sensors
- Medical implants
- Internet of Things

Wireless communication link vulnerable to attacks



art Systems Industry Su...
70 percent smart devices v...
europol medical devices - ...
Cyber crime: First online m...
www.independent.co.uk/life-style/gadgets-and-tech/news/first-online-murder-will-happen-by-end-of-year-warns-us-firm-9774955.html
Google
NEWS VIDEO PEOPLE VOICES SPORT TECH LIFE PROPERTY ARTS + ENTS TRAVEL MONEY INDYBEST STUDENT OFFERS
Fashion / Food + Drink / Health & Families / History / Gadgets and Tech / Motoring / Dating / Crosswords / Gaming / Competitions
Life > Gadgets and Tech > News
Search The Independent
Advanced search | Article archive | Topics
i100 NOW TRENDING
SHARE TWEET SHARE REDDIT SHARE
16:21

Cyber crime: First online murder will happen by end of year, warns US firm

The rapidly evolving Internet of Everything will leave us more vulnerable to cyber criminals, according to a worried Europol

PAUL PEACHEY | CRIME CORRESPONDENT | Sunday 05 October 2014

1 Labour PPCs, answering questions on all the big issues

2 Graphic: Comparing traffic levels in UK cities

3 Can you pass a UK citizenship test? Most young people can't

4 Four charts the Lib Dems don't want to see

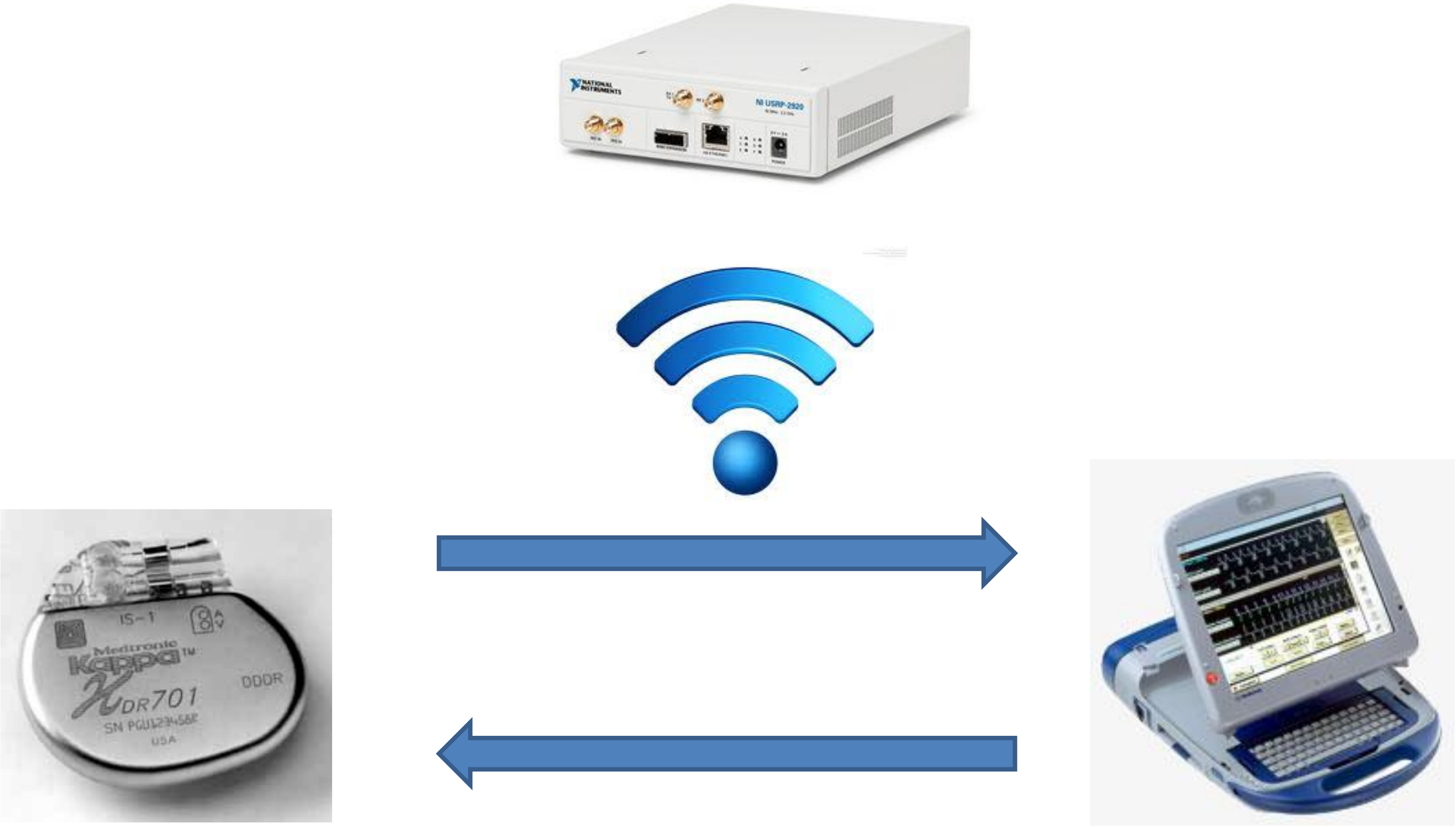
5 Singer takes massive tumble on ice midway through national anthem

Security and privacy risks

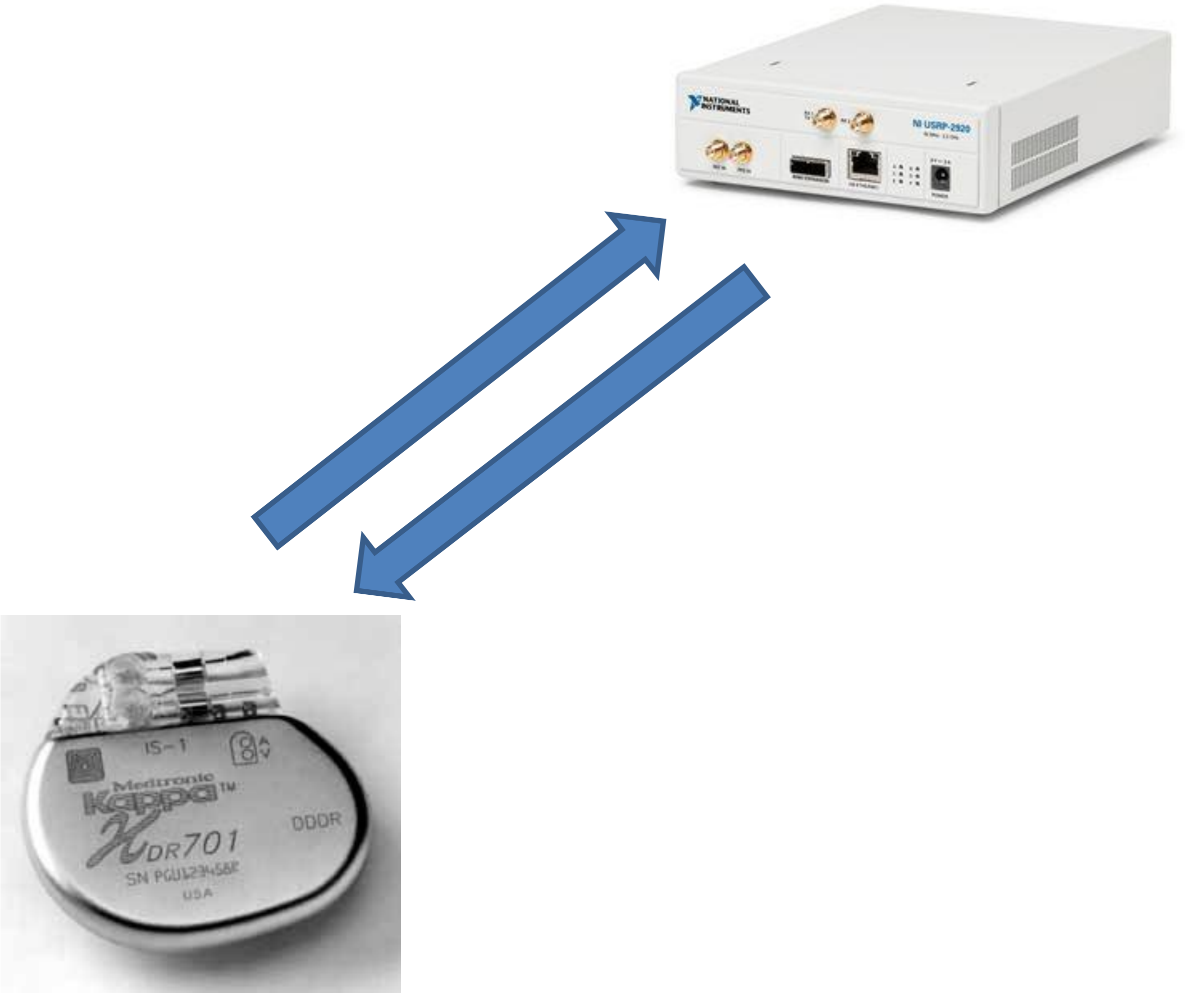
- Passive attacks
  - Eavesdropping
- Active attacks
  - Man-in-the-middle attacks
  - Replay attacks
  - Unauthorized commands
  - Denial-of-Service attacks
  - ….

Intercepting wireless communication

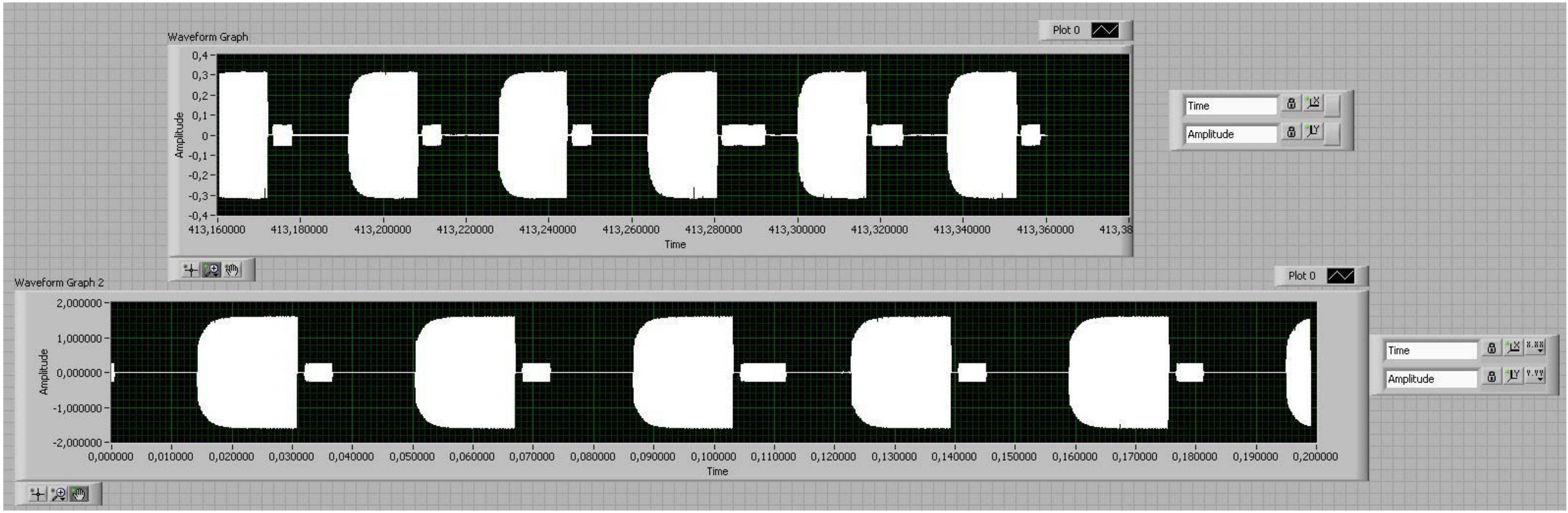
Software Defined Radio: setup



Software Defined Radio: setup



Software Defined Radio attacks



Software Defined Radio attacks

Outline of the talk

- Who are we?
- Smart medical devices: security risks
- Cryptographic solutions
- Key generation
- Privacy
- Conclusion

Secure wireless communication

- End-to-end security
- Cryptographic algorithms needed
- Technological challenges
  - Low-cost hardware resources
  - Ultra low-power budget
  - Limited memory
  - Long lifetime
  - …
- **Lightweight cryptography**

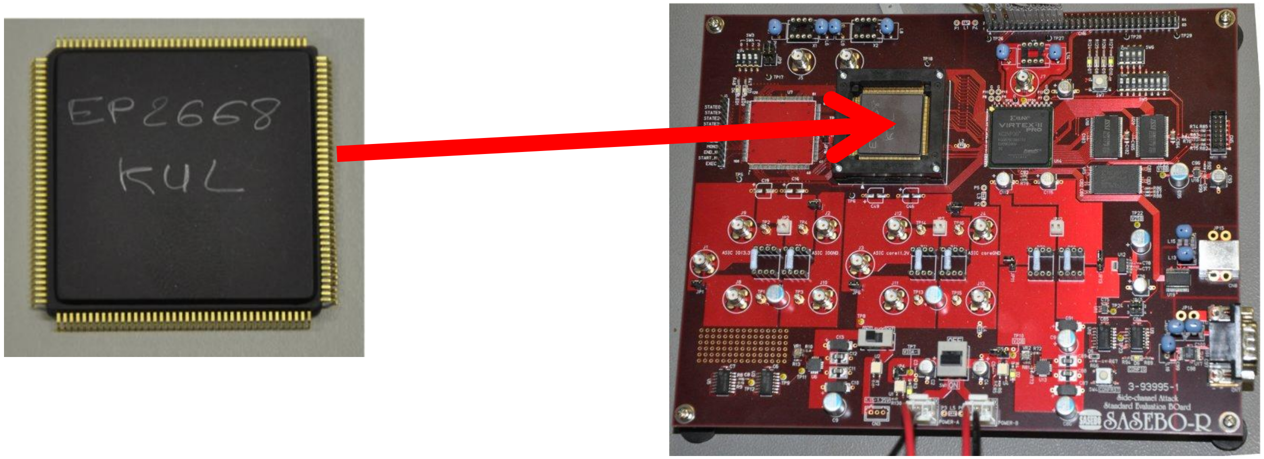
Lightweight cryptographic primitives

- Lightweight, compact cryptographic algorithms
  - KATAN (802 GE)
  - Present (1075 GE)
  - Trivium (2599 GE)

- Lightweight cryptographic protocols
  - Wireless authentication protocols
  - Broadcast authentication
  - Key agreement protocols

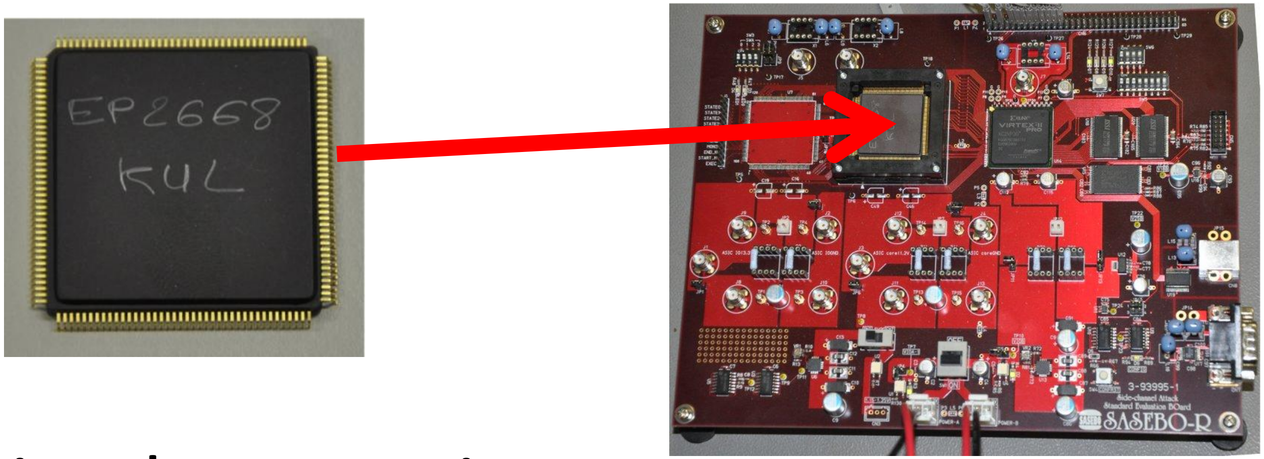
Embedded crypto implementations

- Efficient lightweight implementations
  - Within power, area, speed, … budgets
  - E.g., ECC processor (0.13μm - 14,566 GE - 7.3μW)



Embedded crypto implementations

- Efficient lightweight implementations
  - Within power, area, speed, … budgets
  - E.g., ECC processor (0.13µm - 14,566 GE - 7.3µW)



- Trustworthy implementations
  - Resistant to side-channel and fault injection attacks

=> BOTH are needed

Crypto: long lifetime

- Large key size
- Key updates -> cryptographic protocols needed
- Post-quantum cryptography
  - Multivariate Quadratic (MQ)
  - Lattice-based cryptography

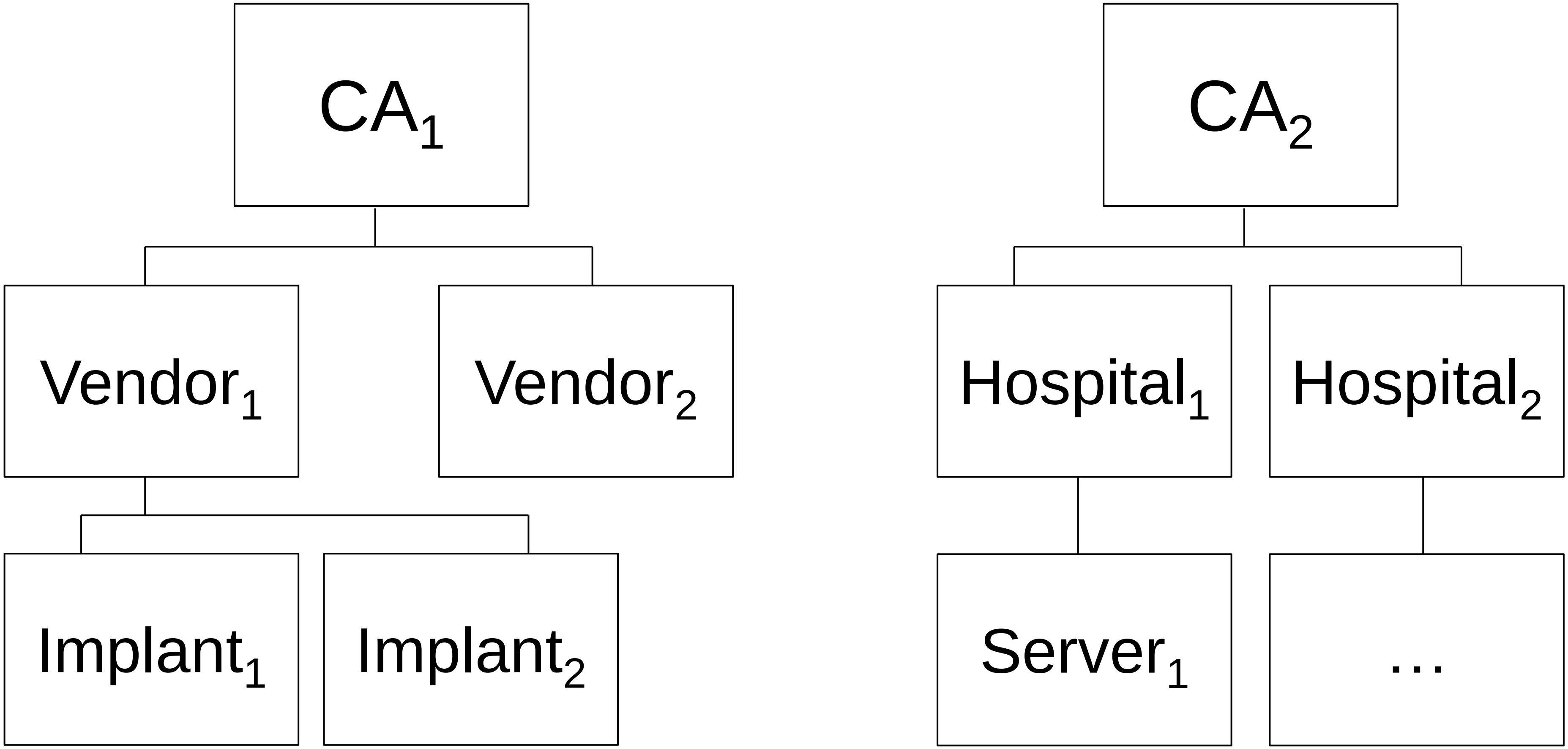
Outline of the talk

- Who are we?
- Smart medical devices: security risks
- Cryptographic solutions
- Key generation
- Privacy
- Conclusion

Key management

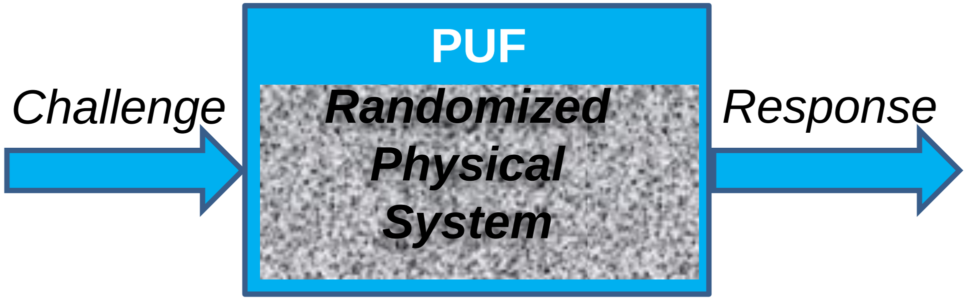
- Pre-installed
- Using out-of-band channel
  - Location-based
  - Physical contact
  - User input
  - Biometrics
  - …
- Physical Unclonable Functions (PUFs)
- Key distribution schemes
- PKI infrastructure

PKI Infrastructure



PUF: concept (I)

- **P**hysically
  Unclonable
  Functions



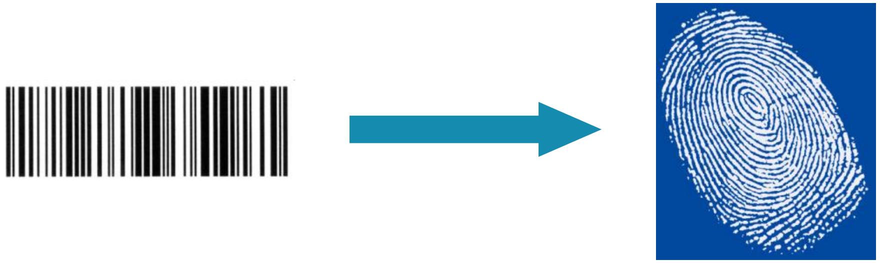
Challenge

PUF

Randomized Physical System

Response

- PUFs represent a paradigm shift in physical security:
  1. Explicitly programmed digital identity → Intrinsic physical identity

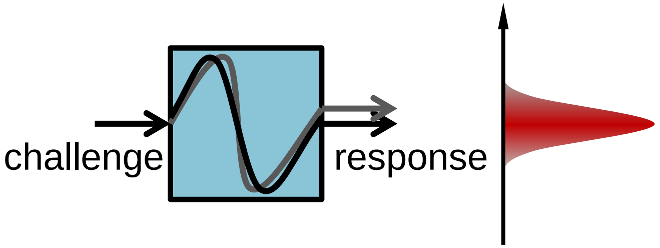


  2. Unclonable because of physical protection of digital data
     → Unclonable because of uncontrollable physics

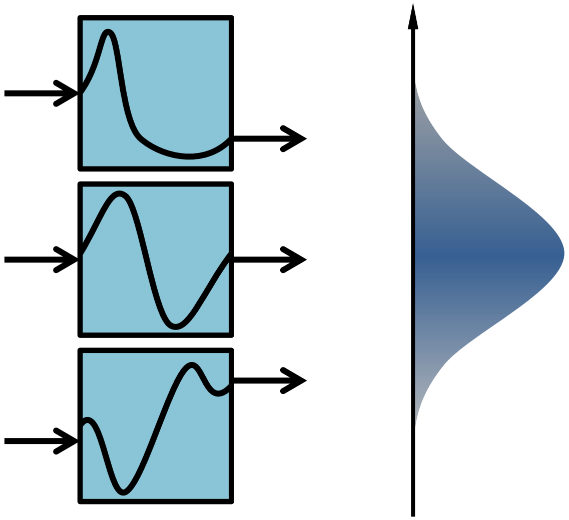
100110…00101

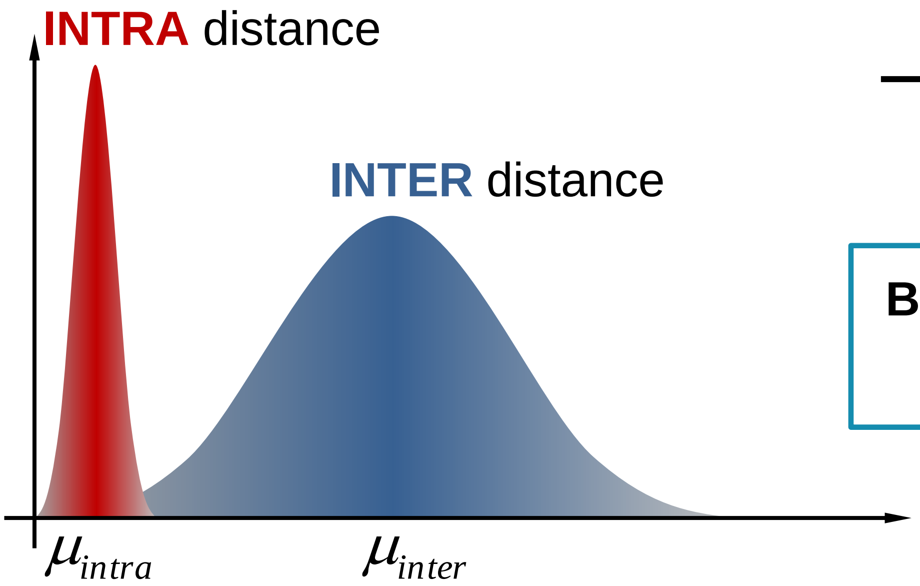
PUF: concept (II)

Single PUF instance



Multiple "identically manufactured" PUF instances



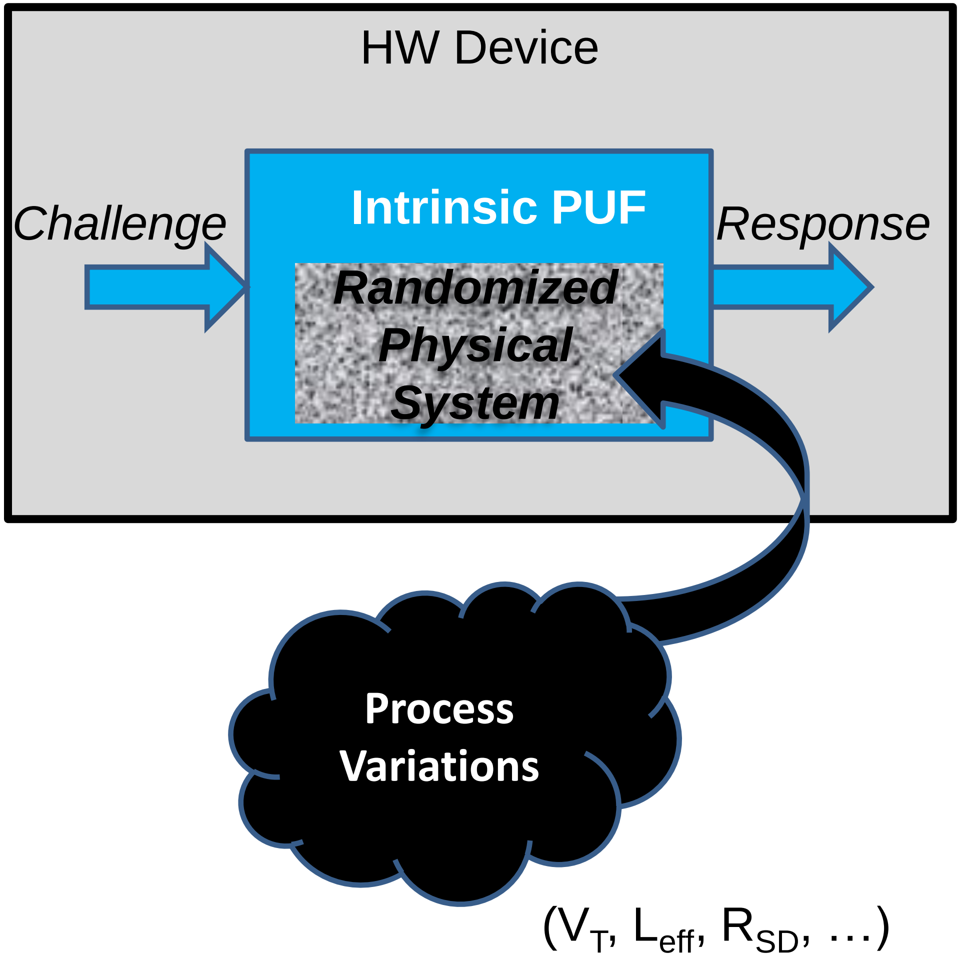


Basic PUF property:

$\mu_{inter} >> \mu_{intra}$

PUF: concept (III)

- Non-silicon
- Silicon
- Intrinsic
  1. Randomness = ***intrinsic*** manufacturing variability
     - no manufacturing overhead
     - i.c. CMOS process variations
  2. Integrated measurement
     - no external equipment
     - i.c. PUF response on-chip

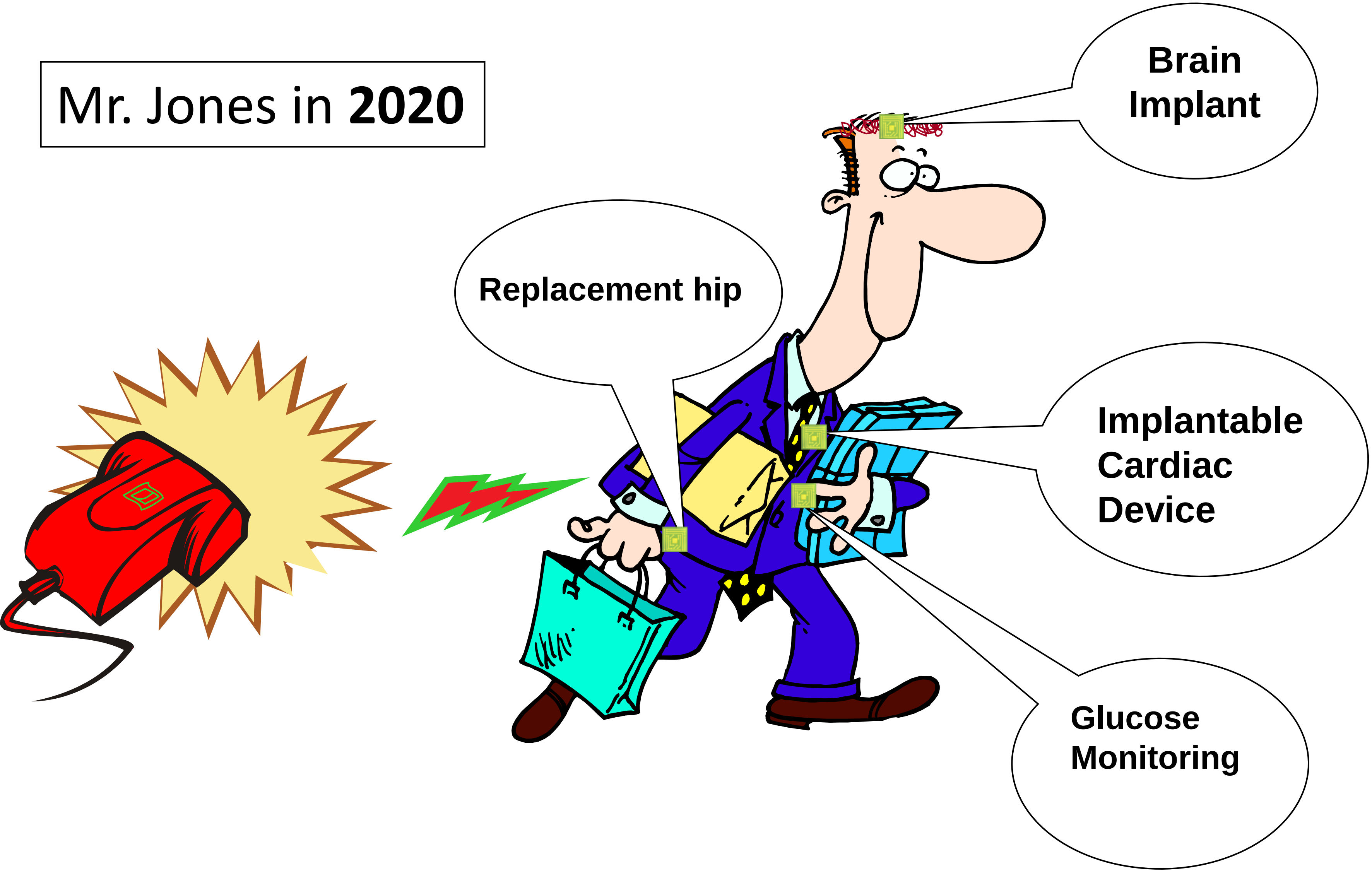


Outline of the talk

- Who are we?
- Smart medical devices: security risks
- Cryptographic solutions
- Key generation
- Privacy
- Conclusion

Privacy challenges

Mr. Jones in **2020**



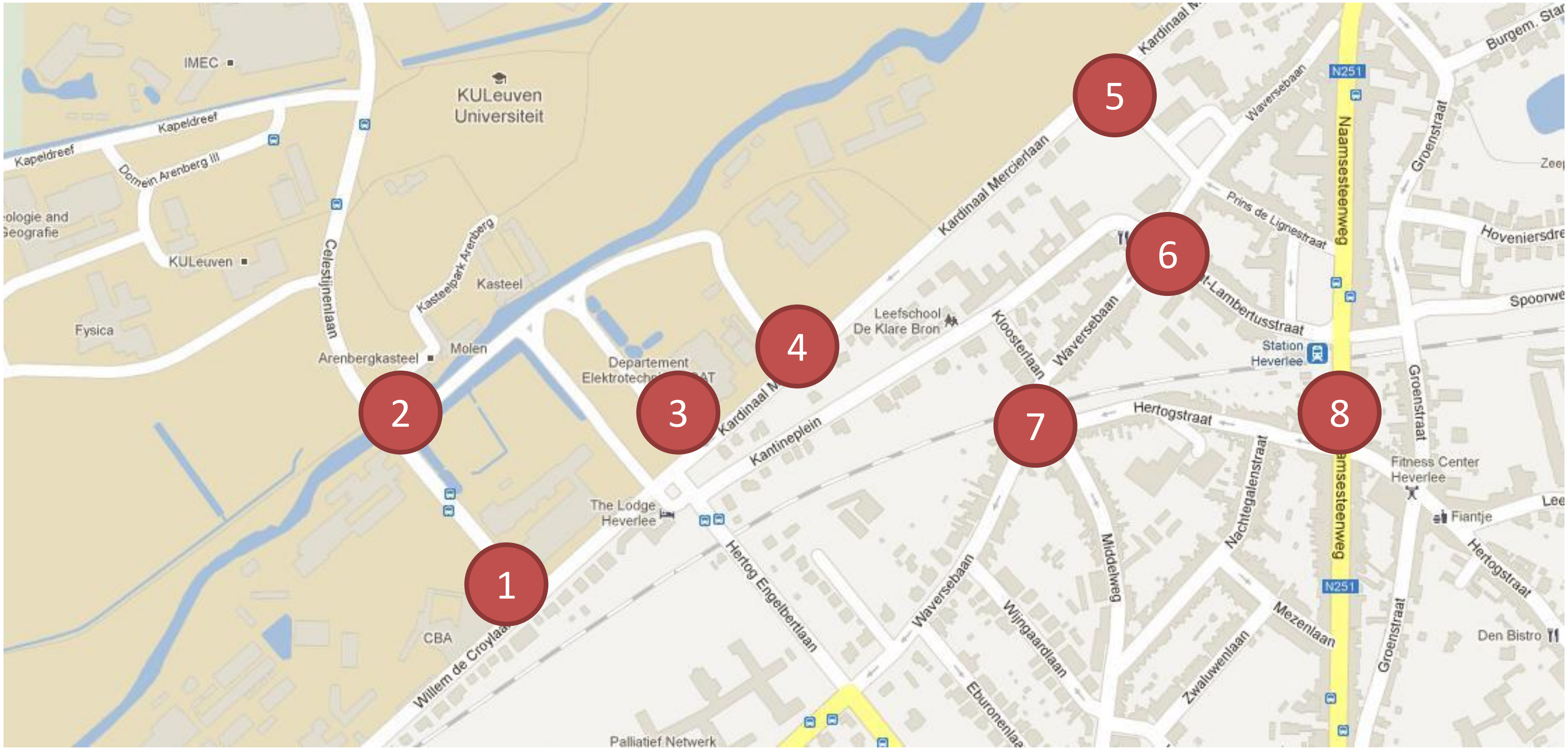
Brain Implant

Replacement hip

Implantable Cardiac Device

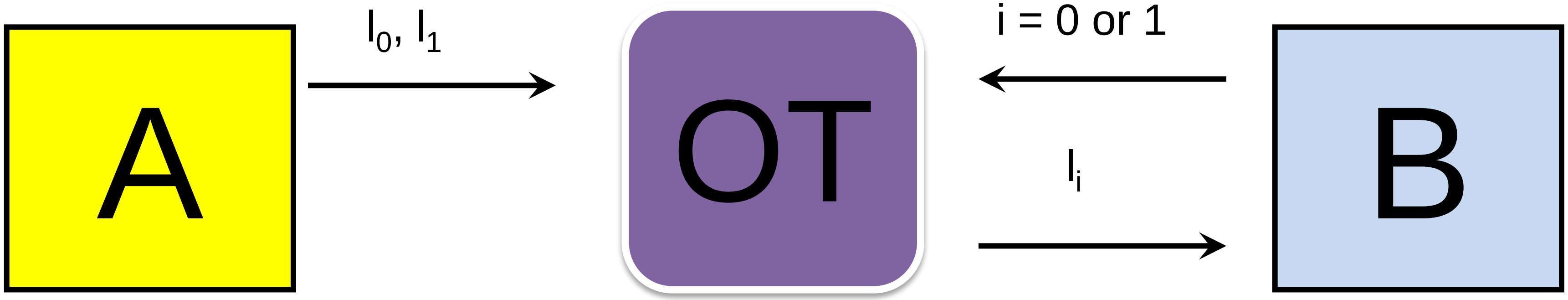
Glucose Monitoring

Location privacy



Data minimization

- **Homomorphic encryption**
- Oblivious transfer



- A does not learn which item B has chosen;
- B does not learn the value of the item that he did not choose

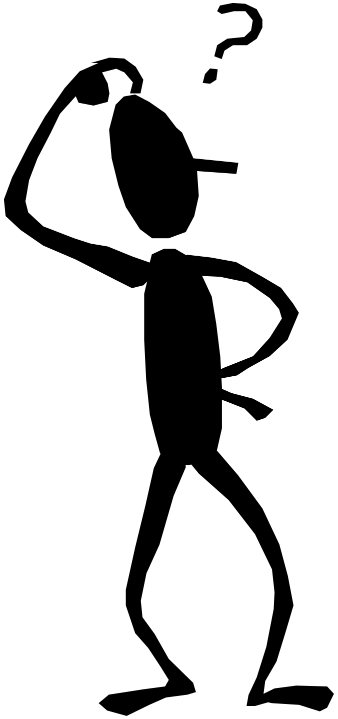
Outline of the talk

- Who are we?
- Smart medical devices: security risks
- Cryptographic solutions
- Key generation
- Privacy
- Conclusion

Conclusion

- **Smart security solutions are needed**
- Lightweight cryptography
- Security architecture
  - Key generation / agreement
  - Key update/revocation mechanisms
- Very long lifetime of cryptographic primitives (> 30 years)
- Privacy is also important
- Active area of research

Questions



Contact information

ESAT / COSIC

- **Dave.Singelee@esat.kuleuven.be**

- http://www.esat.kuleuven.be/cosic/

- K.U.Leuven, ESAT / COSIC
  Kasteelpark Arenberg 10, bus 2452
  B-3001 Leuven-Heverlee