KATHOLIEKE UNIVERSITEIT
LEUVEN



Joos, Secure hardware and spin-offs…

Prof. Dr. Ir. Ingrid Verbauwhede
http://www.esat.kuleuven.be/cosic

Outline

- Why secure crypto hardware?
- At first: design for efficiency
- Currently: design for efficiency and physical security
- Future: Crypto entangled with environment



Why crypto hardware?

- Joos emphasized that research was *not* for the military
- Focus on civilian applications



[Source: Veto, jr. 10, nr. 1, oct. 1983]

When Hardware design?

- Fast
- Small
- Low power
- Secure
- (Analog, RF)











HW

SW

HW

Crypto algorithms in hardware?

1. Design for efficiency



1. Design for efficiency

- Goal:
  - Area: count number of transistors, memory size
  - Speed or throughput: Gbits/sec
  - Power/Energy: cooling problems or battery consumption

- Challenge for crypto algorithms:
  - Strange arithmetic: Sboxes, Galois fields
  - Large word lengths (RSA of 512 bits in 1990!)
  - Unfit for software programming
  - Apply crypto know how (Yvo Desmedt) to HW design

Power and energy minimization!

- Energy: Joules
- Battery content



- Pacemakers: non-rechargeable batteries!

- Power: Cooling - Watts

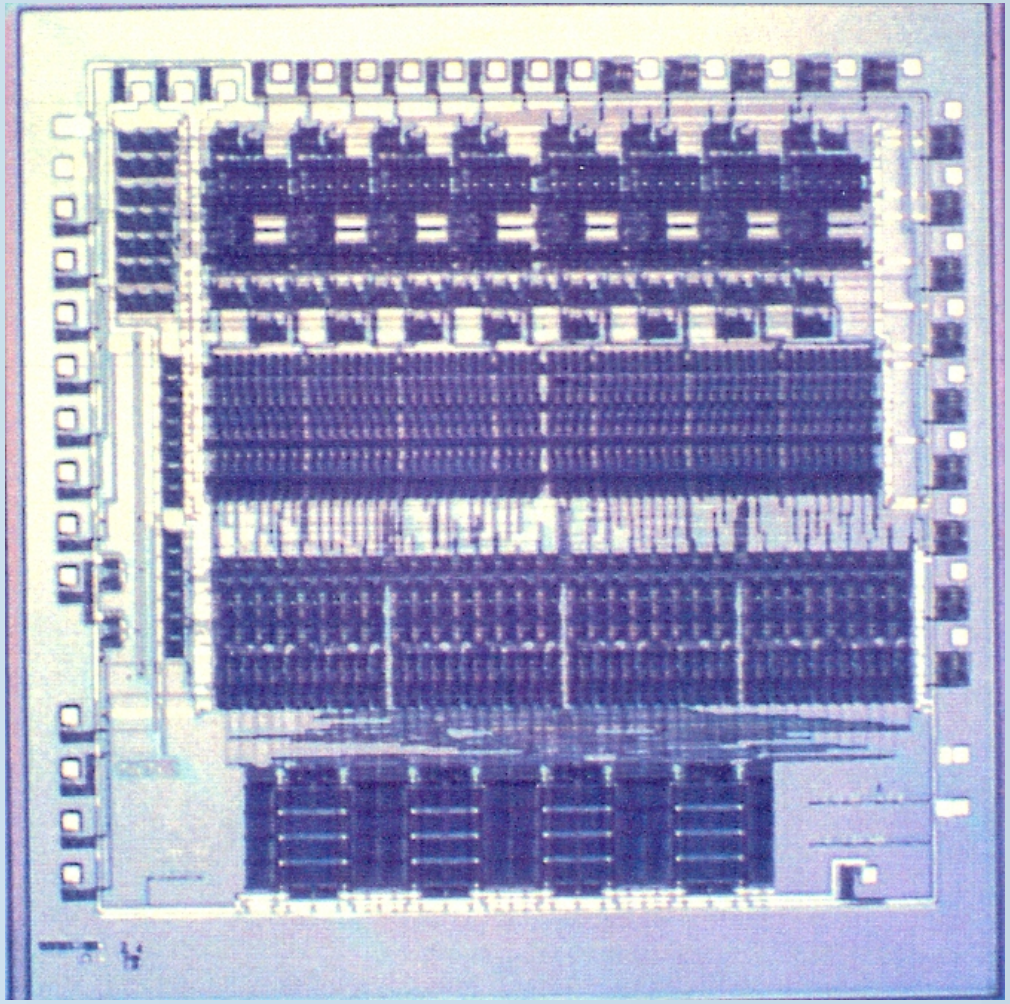


[Source: SFO Chronicle, Google cooling infrastructure]

DES prototype chip

- 3 µm CMOS
- 2 levels of metal
- 25 mm^2
- 12000 Transistors
- 32 Mbits/sec

(for all modes of operation)



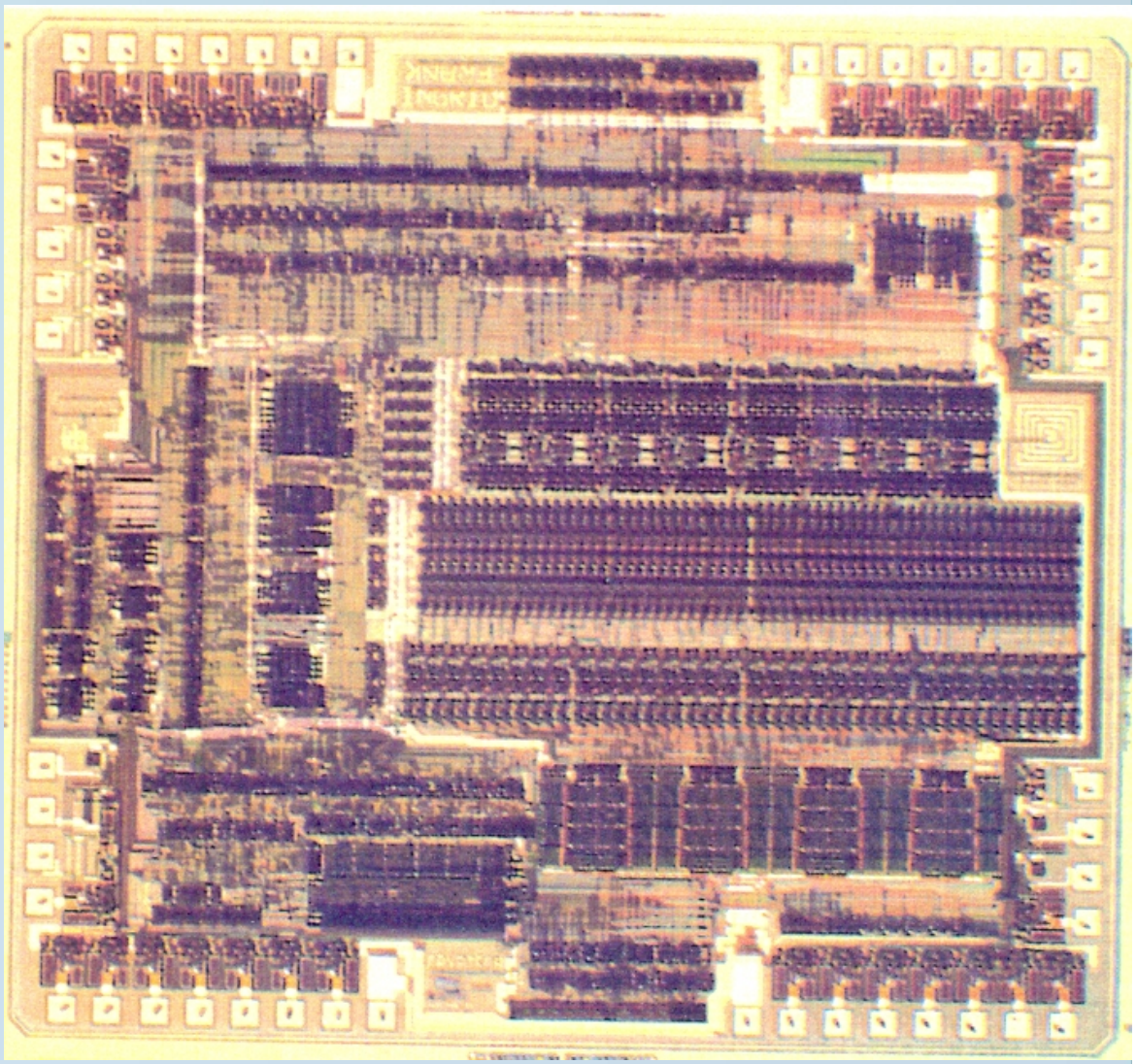
I. Verbauwhede, F. Hoornaert, J. Vandewalle, and H. De Man, "Security and performance optimization of a new DES Data Encryption Chip," IEEE Journal of Solid-State Circuits 23(3), pp. 647-656, 1988.

Visit of the king



2nd generation

- Commercial version
- 2.4 µm CMOS
- 25 mm^2
- 18000 transistors
- Standard cells
  - For controllers and I/O
  - Make your own cells
  - Use tool from
  - Davio group (UCL)
- 30Mbits/sec commercial
- Fastest available

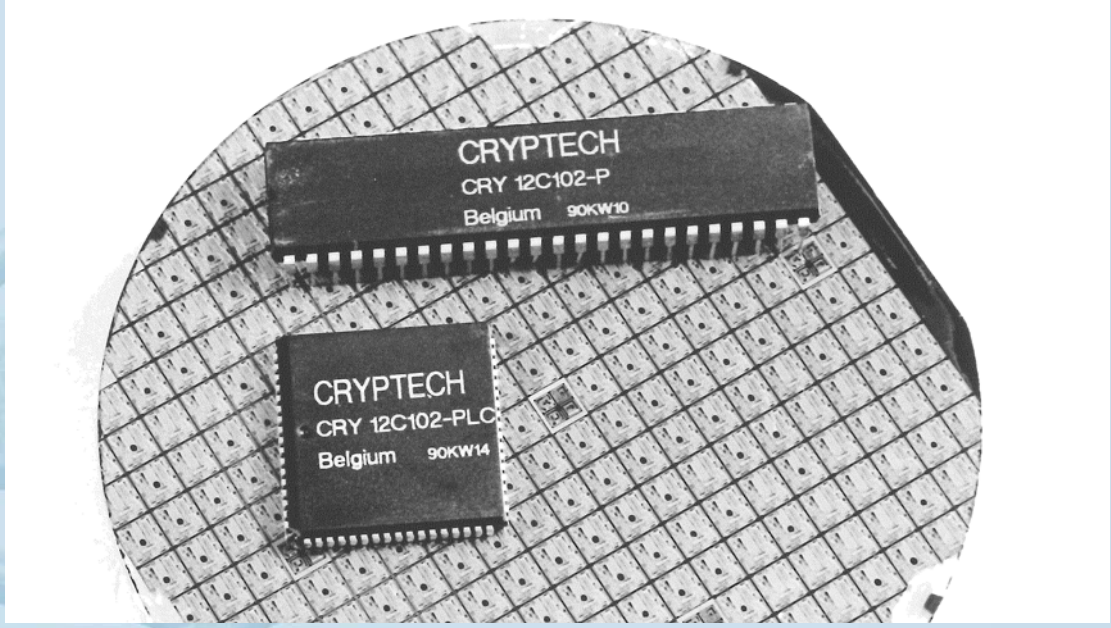


CRYPTECH

KATHOLIEKE UNIVERSITEIT LEUVEN

Cryptech and ESAT

The co-operation between Cryptech and the Electronics, Systems, Automation & Technology (ESAT) research laboratory of Belgium's renowned Catholic University of Leuven (Louvain) is both long-standing and rewarding. At the time when the need for a European encryption technology source became obvious, the ideas and know-how of ESAT became a vital asset in the creation of Cryptech.



2. Design for efficiency *and* security



Side channel analysis: main idea



"Breaking into a Safe is hard, because one has to solve a single, very hard problem..."



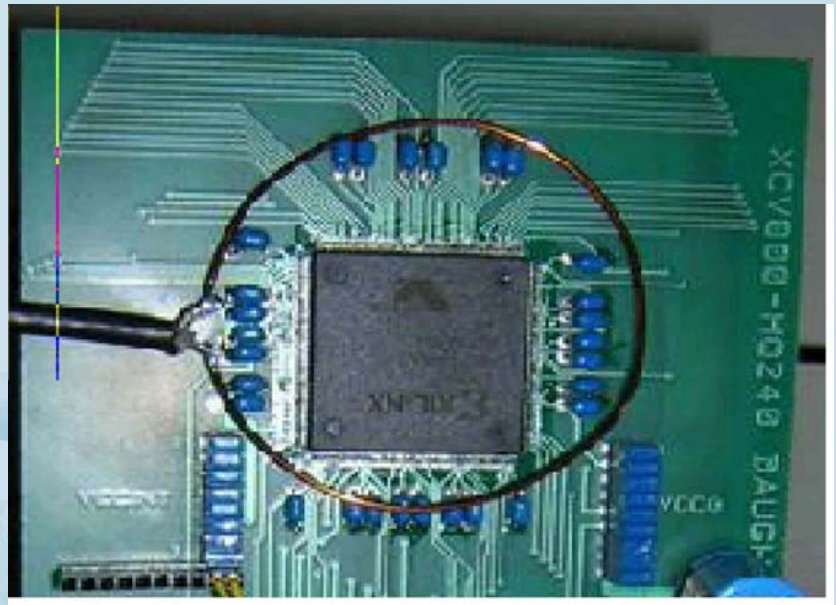
"Things are different if it is possible to solve many small problems instead..."

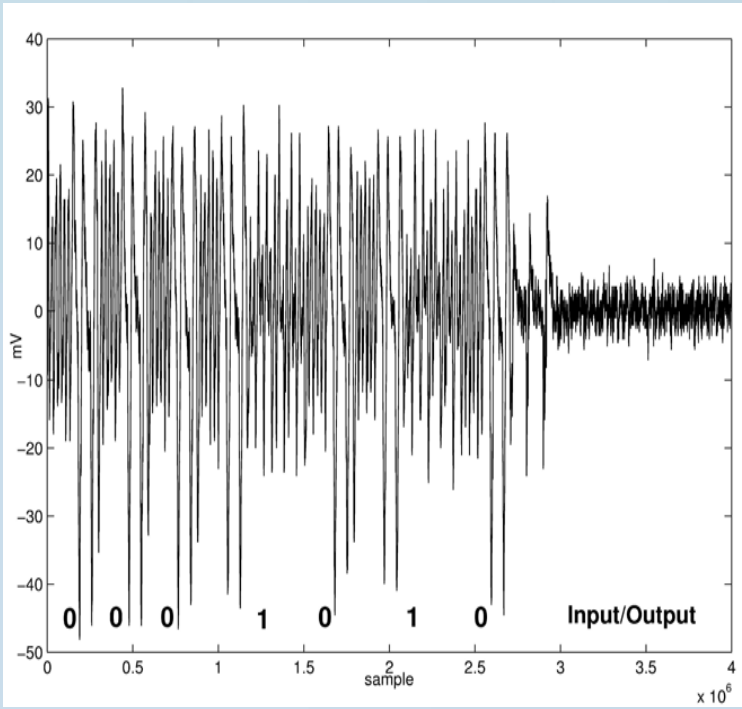
"Divide et impera!"



2. Design for efficiency AND security

SEMA attack: Simple Electromagnetic Attack on Elliptic Curve Public Key implementation.





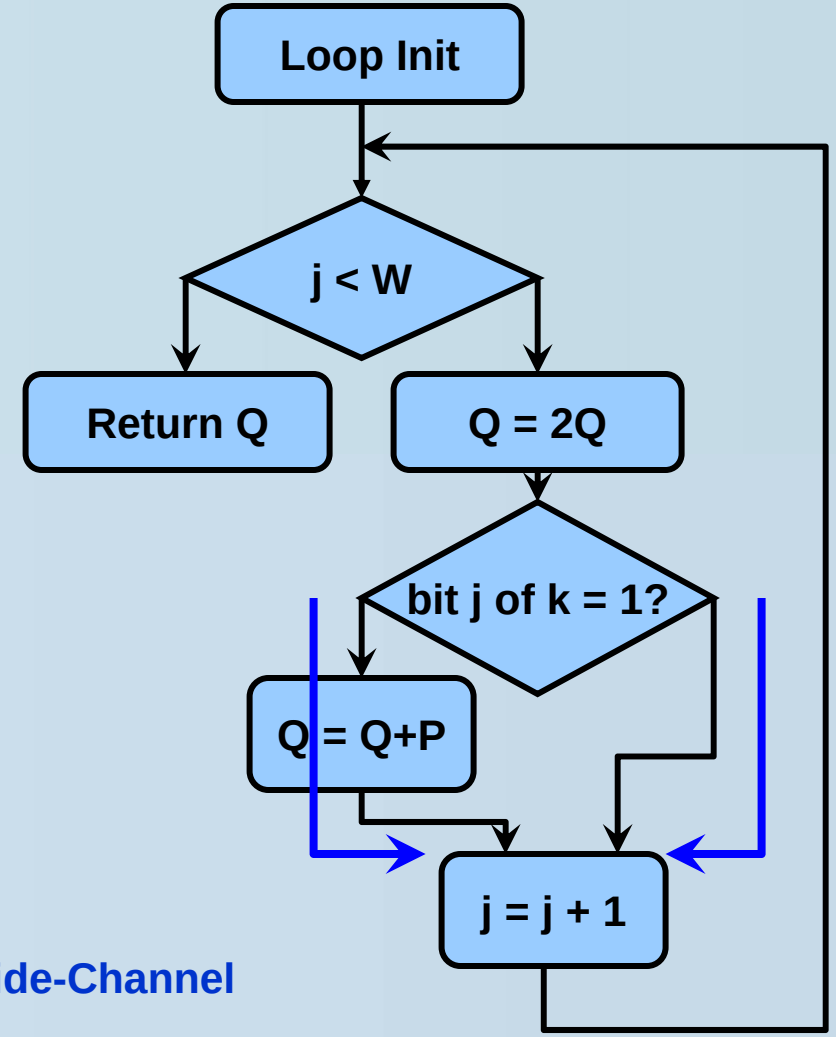
[E. Demulder EUROCON 2005]

Insecure implementation

Elliptic Curve Public Key
"Point Multiplication" algorithm
Top level description

```
In: point P, key k (W bits)
Output: Q = k.P

for j = 0 to W – 1
    Q = 2.Q /* double */
    if (bit j of k) is 1 then
        Q = Q + P /* add */
Return Q
```



Timing Side-Channel

New algorithm design: Rijndael

- HW and SW ‘friendly’
- Rijndael evaluation
  before it became standard
- Enc + Dec
- 0.18 µm CMOS
- Standard cells
- 2.3 Gbits/sec
- 56 mW

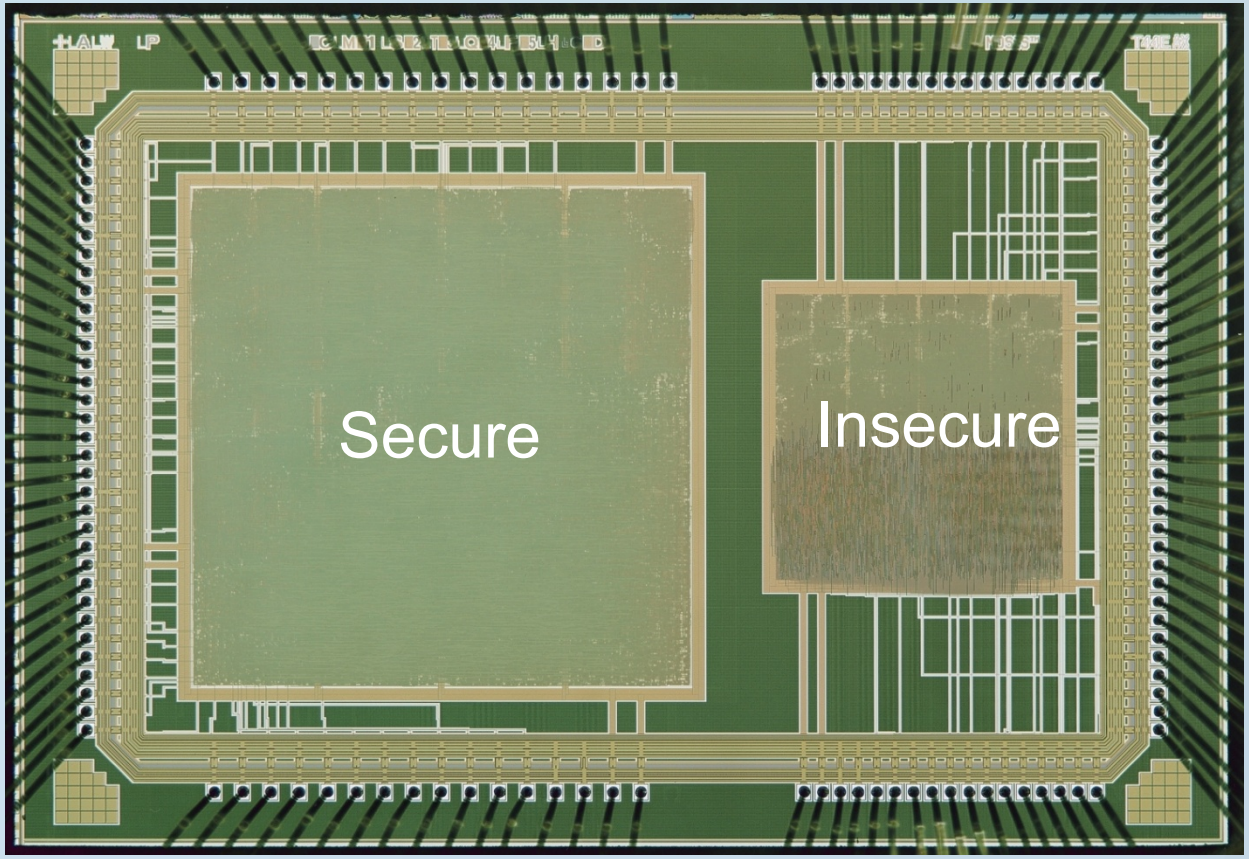


[JSSC 2003]

AES *with* countermeasures

- AES, 2nd generation
- Regular & WDDL based implementation
- Standard cells

- 1 Gbit/sec to 3.8 Gbits/sec
- 50 to 200mW



[CHES2005]

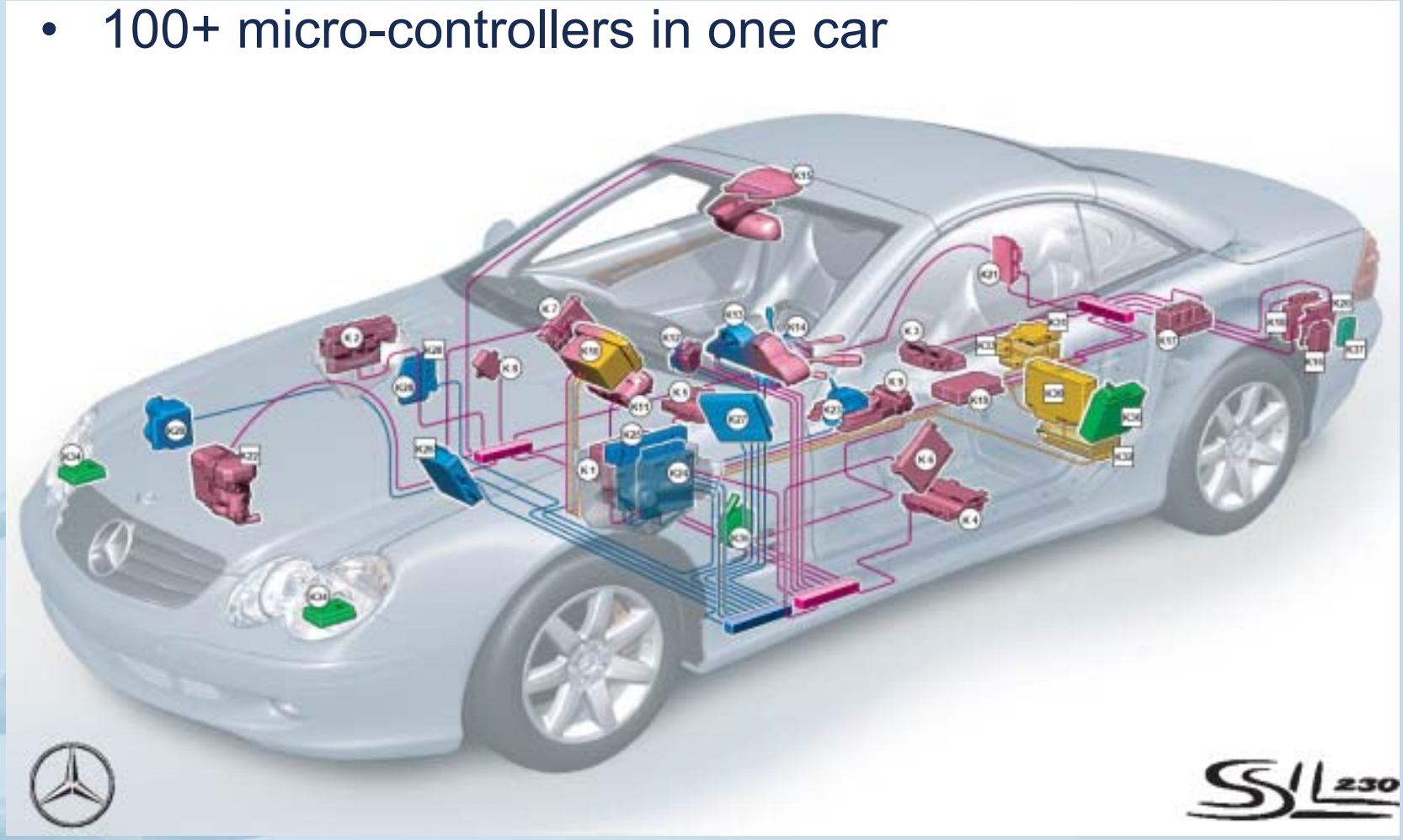
Crypto algorithms in hardware?

3. Efficiency, security *and* immersed

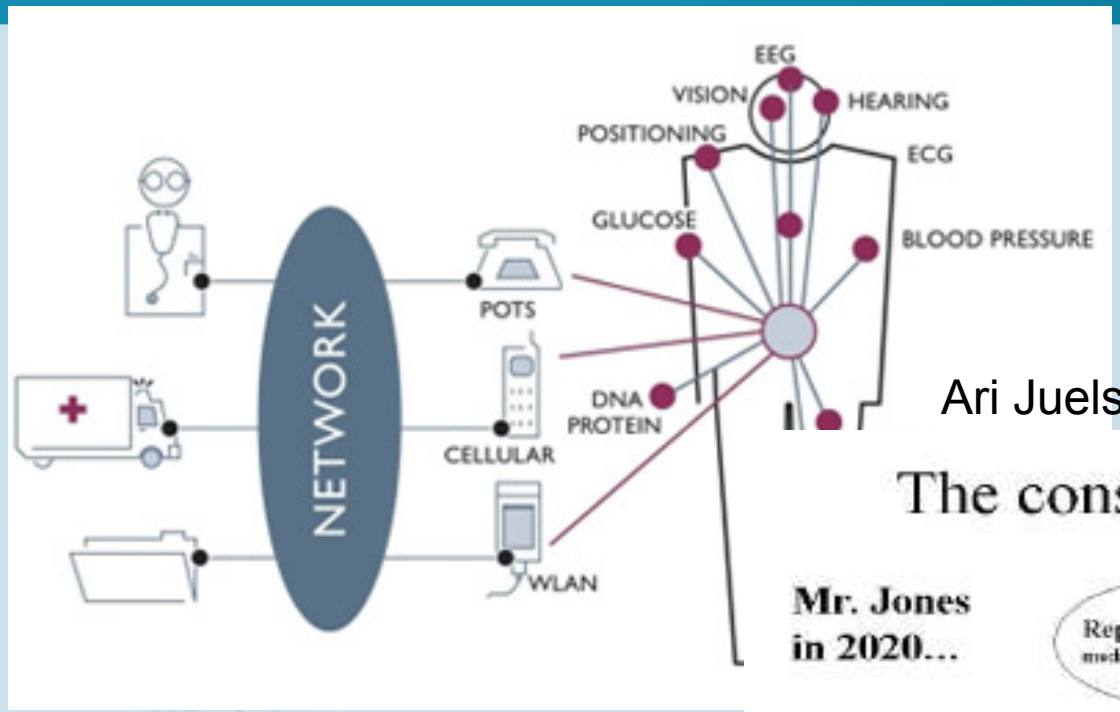


3. Efficiency, security AND immersed

- New generation of applications
- 100+ micro-controllers in one car

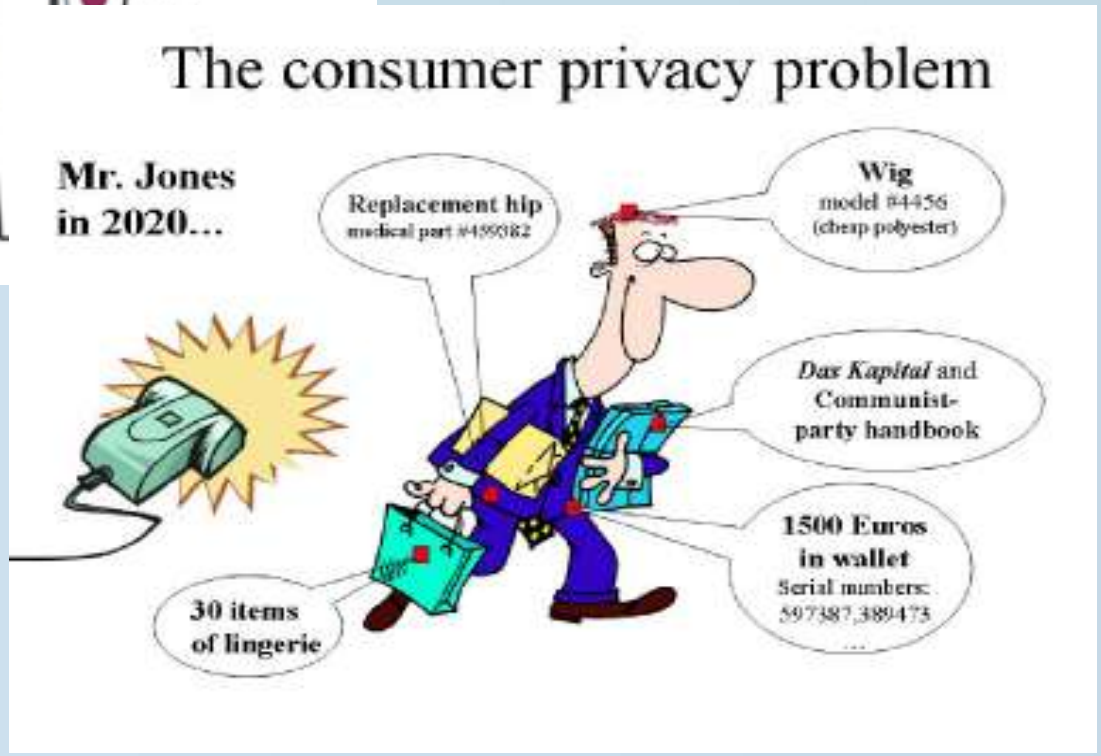


Embedded crypto everywhere

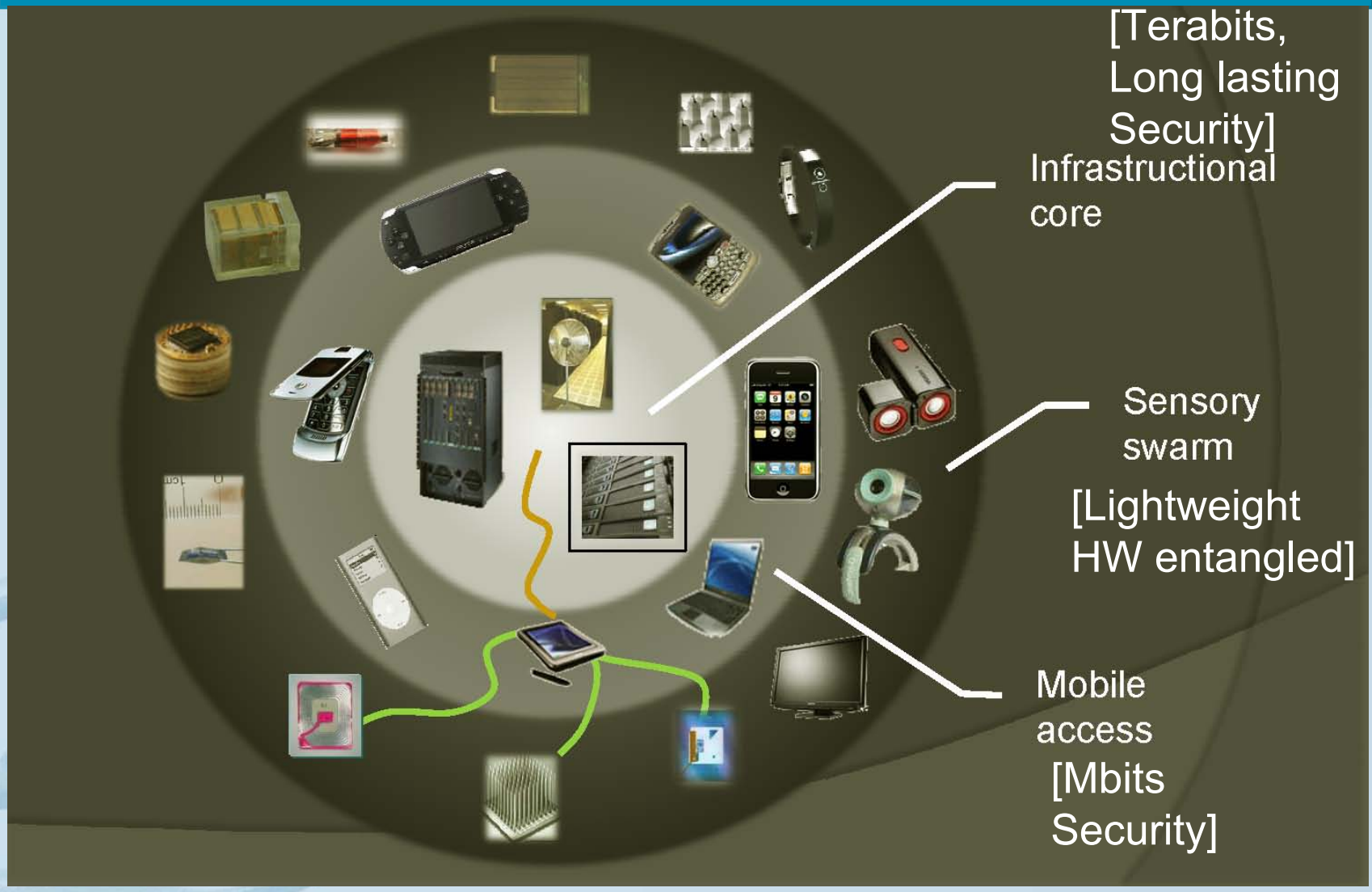


IMEC: Human++ project

Ari Juels: RFID tracking problem



UC Berkeley SWARM LAB

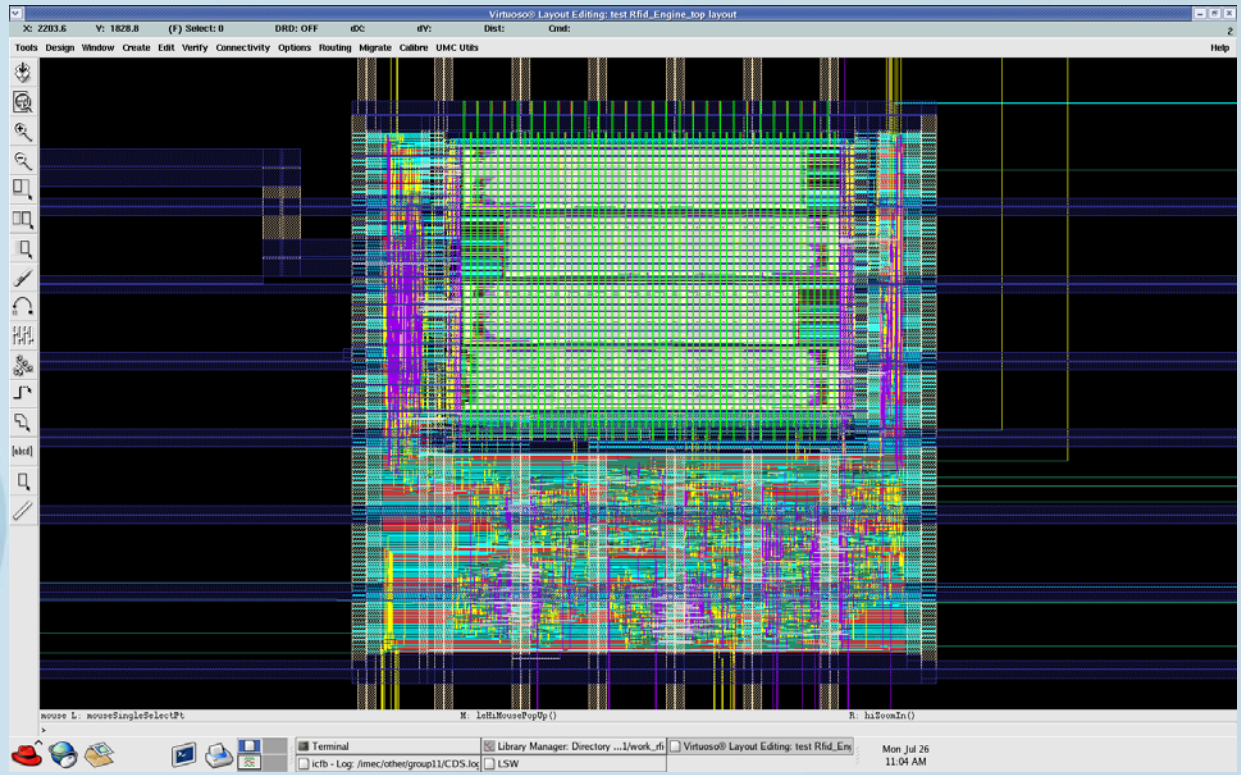


[Source: J. Rabaey: A Brand New Wireless Day]

Light weight crypto

Public key crypto (elliptic curve)for a passive RFID tag

- 50 µW, 100 msec per PM, = 5.1 µJ per PM
- 0.13 µm (8 layers of metal!), 0.54 mm^2
- Attack resistance built-in



Conclusions

Ever increasing need for secure crypto hardware
(so far all civilian applications)

- Past: efficiency
- Present: efficiency and security
- Future: efficiency, security and immersed

Thanks Joos!

