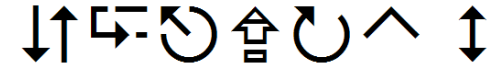




ECRYPT II



<http://www.ecrypt.eu.org>

Research challenges in cryptology

Bart Preneel

COSIC, K.U.Leuven, Belgium

Bart.Preneel@esat.kuleuven.be

<http://homes.esat.kuleuven.be/~preneel>

Information processing

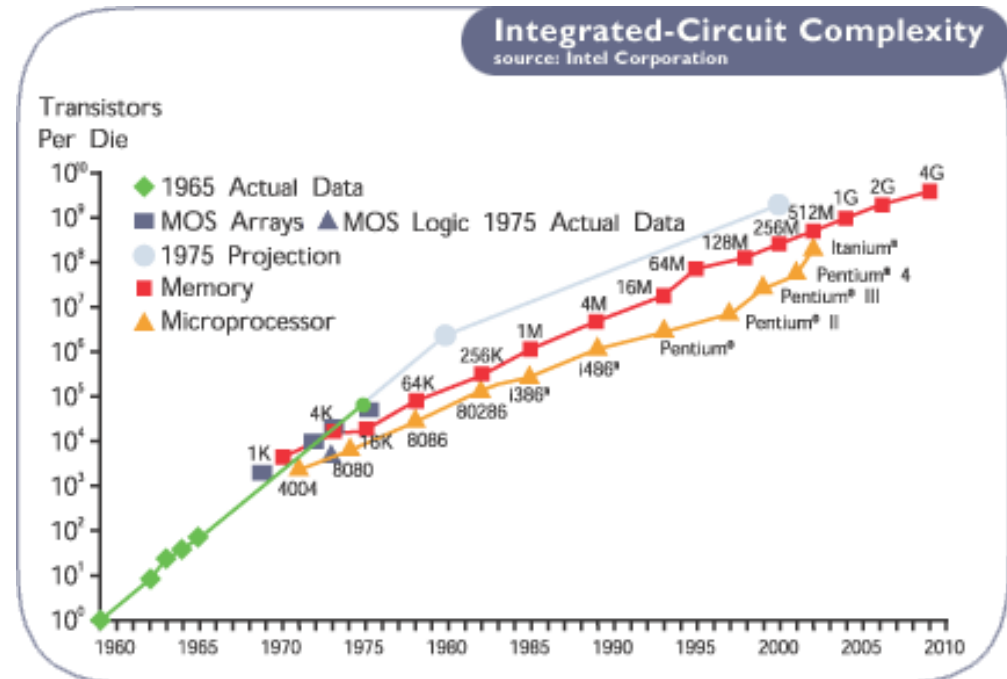
the Internet of things,
ubiquitous computing,
pervasive computing,
ambient intelligence (10^{12})

Internet and mobile (10^9)

PCs and LANs
(10^7)

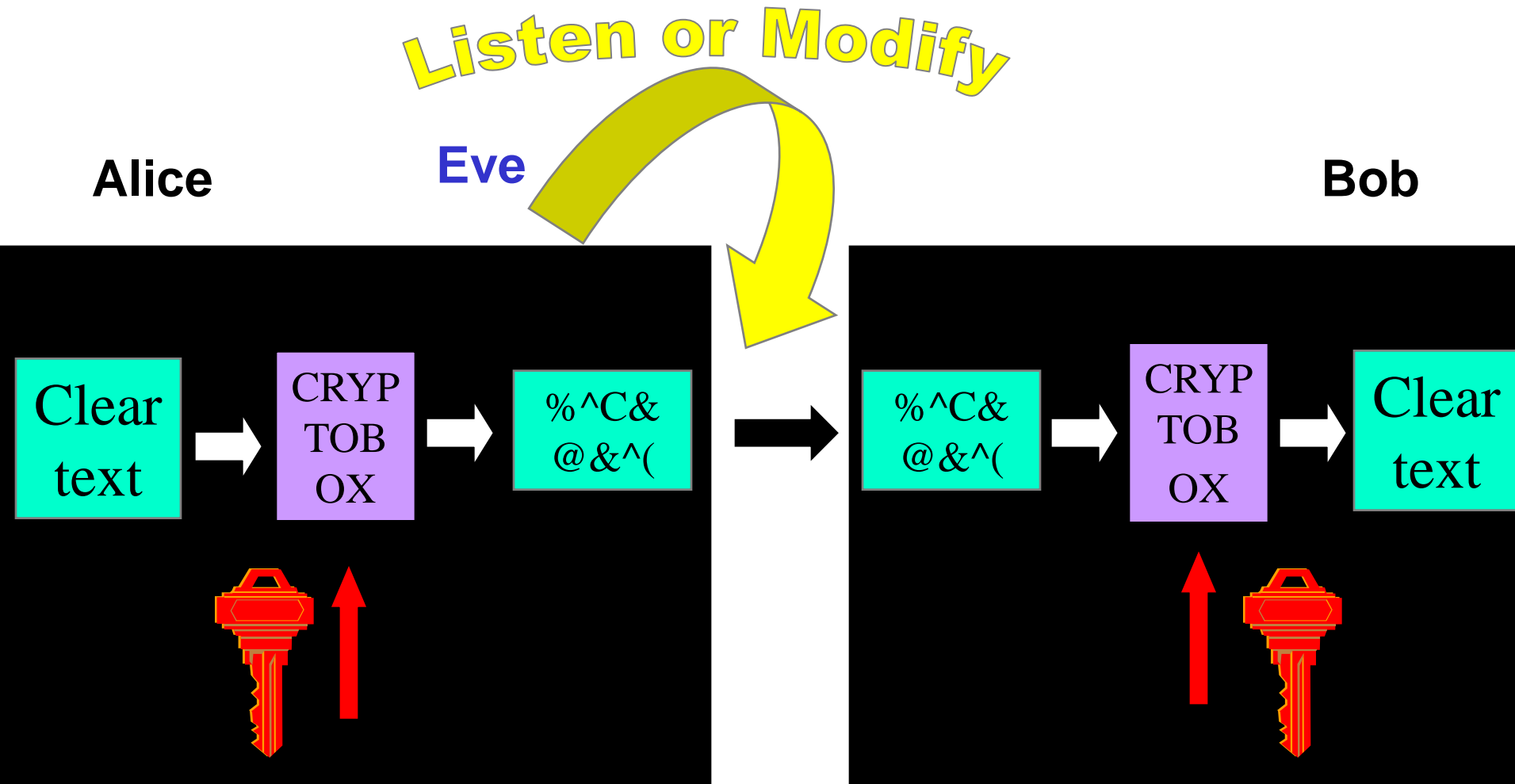
mainframe
(10^5)

mechanical
(10^4)

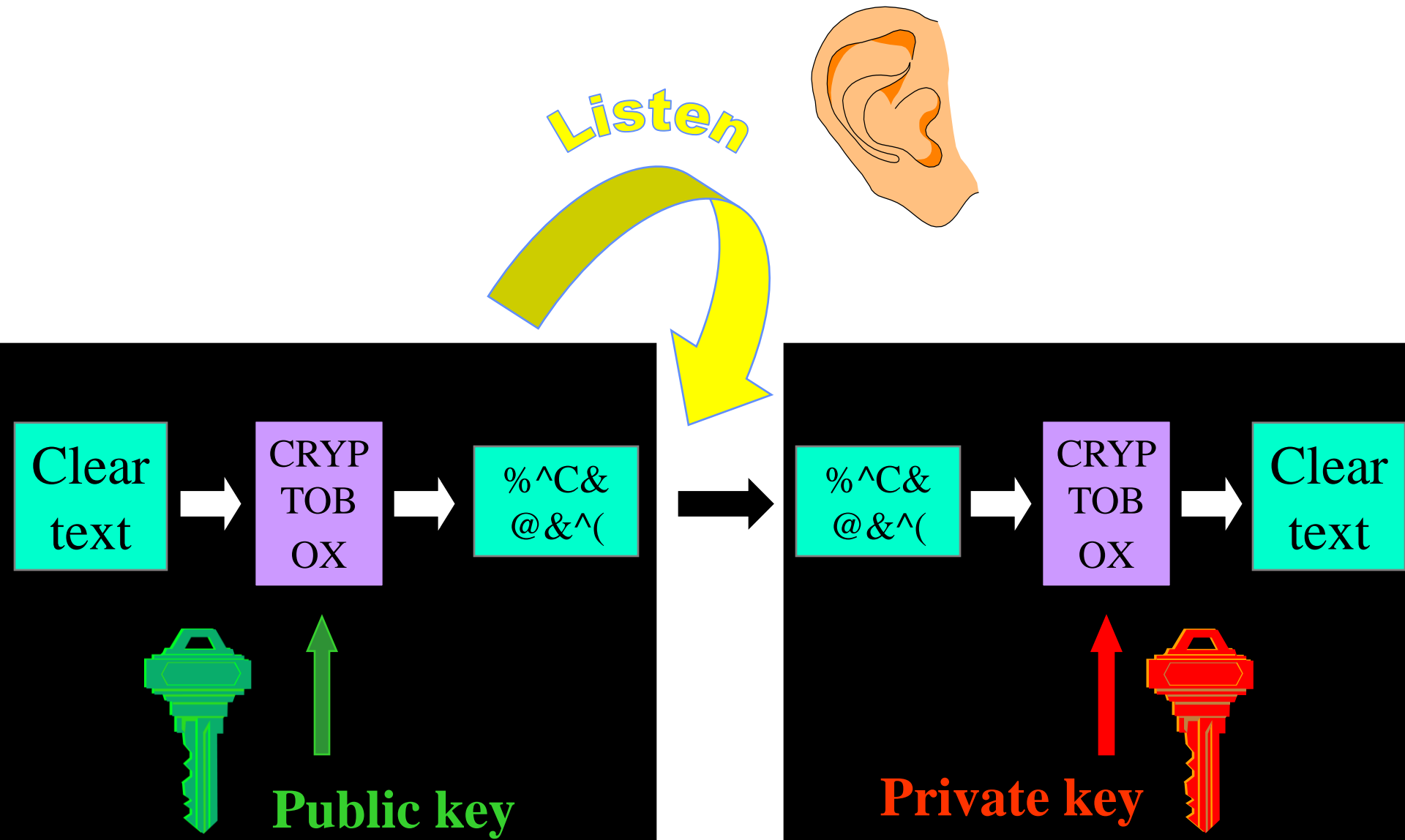


Cryptology principle

move protection of information to protection of keys



Public key cryptology: encryption



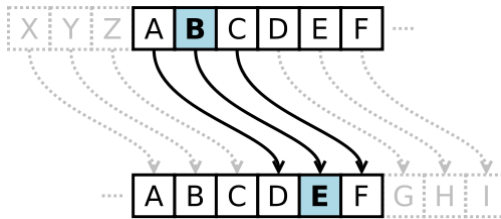
Crypto history



(electro-)mechanical devices
rotor machines
(1915-1975)



simple devices
(pre-1915)



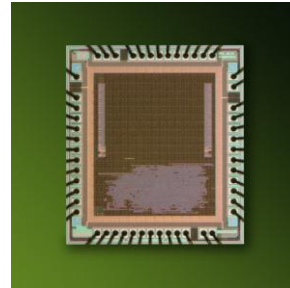
Caesar cipher
(1st century BC)



Syctale
(7th century BC)



Crypto hardware (1965-...)

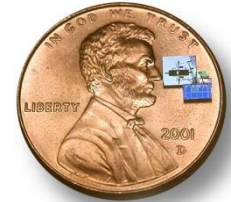
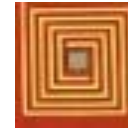
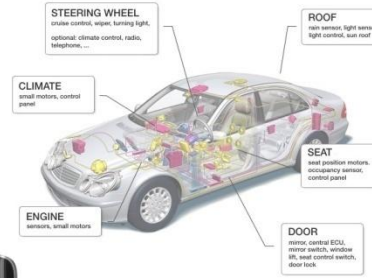


Crypto software (1990-...)



Crypto “everywhere”

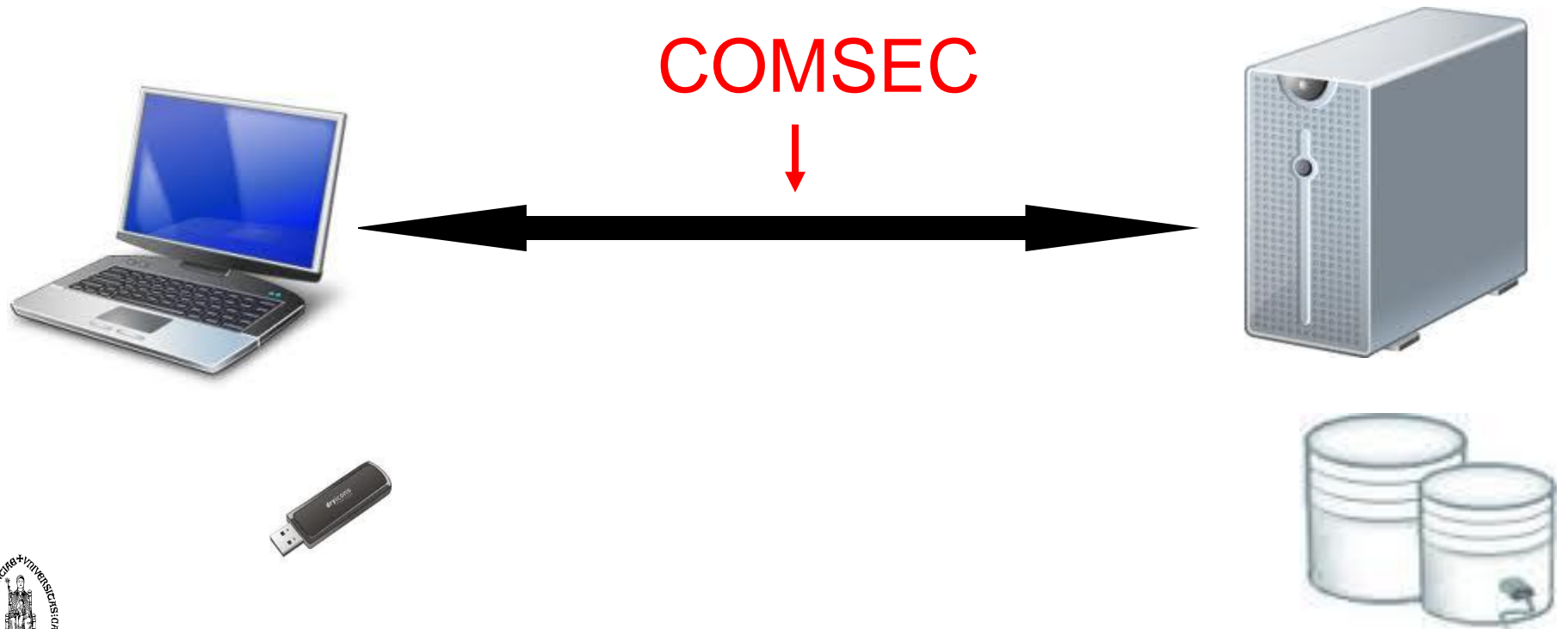
Everything is always connected everywhere



Continuum between software and hardware

ASIC (microcode) – FPGA – fully programmable processor – Intel NI instruction

Use of crypto



COMSEC

	Confidentiality	Data authentication	Entity authentication
1 G (analog)			
2 G (GSM)	weak		unilateral
3G			
WLAN			
TLS			unilateral
IPsec		optional ☹️	
Skype	not open	not open	not open

Not end to end



Use of crypto: COMPUSEC

- **Data at rest:**

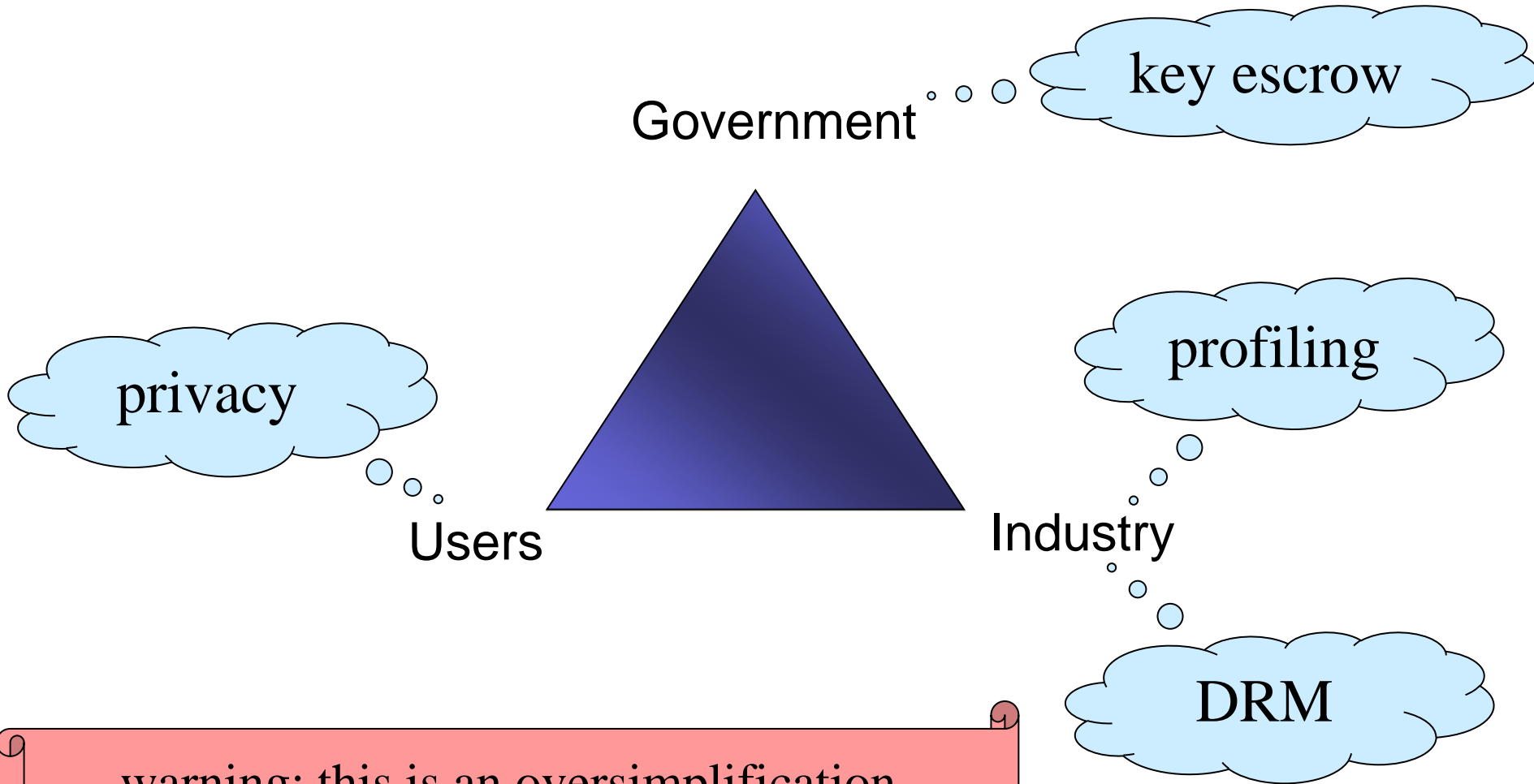
- Hard disk (Bitlocker)
- Database
- Floppy disk/CD/USB
- Mobile devices

- **Secure execution**

- TPM
- ARM TrustZone
- Apple DRM



Security for everyone?



warning: this is an oversimplification
– e.g. privacy is a security property

Secure cryptology but insecure systems

- Crypto is only a part of a complex security puzzle
 - how to deal with complexity?
 - how to manage evolving requirements?
 - how to avoid implementation errors?
- Economics: market failures
- Human factors
 - usability
 - social engineering

Missing or Insecure cryptology

- Crypto is missing because it is
 - too slow: Google
 - too big: RFID
 - too expensive
- Crypto can be insecure due to
 - continuous progress in cryptanalysis
 - long term security: progress in cryptanalysis
 - legacy problem: A5/1, Bluetooth, Keeloq
 - insecure implementations

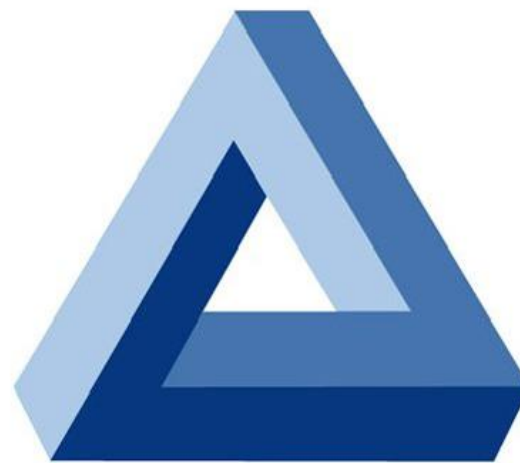
Challenges for cryptographic algorithms

- security for 50-100 years
- authenticated encryption of Terabit/s networks
- ultra-low power/footprint

secure software and
hardware
implementations

algorithm agility

performance



cost

security

AES (2001)



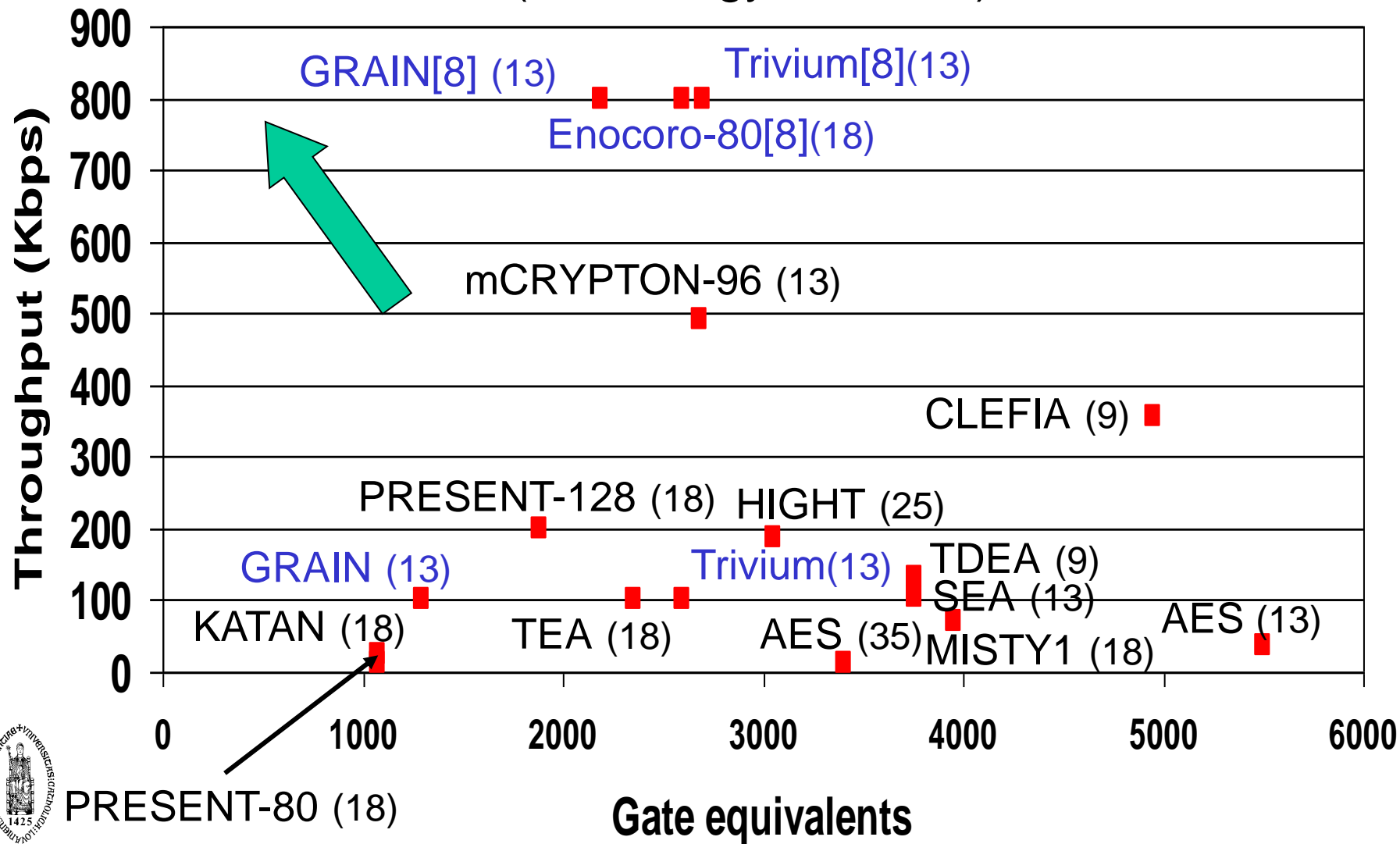
- FIPS 197 published after open competition
 - other standards: ISO, IETF, IEEE 802.11,...
- fast adoption in the market
 - except for financial sector
 - NIST validation list: 1501 implementations
 - <http://csrc.nist.gov/groups/STM/cavp/documents/aes/aesval.html>
- 2003: AES-128 also for **classified** information and AES-192/-256 for **secret** and **top secret** information!
- Excellent security/performance tradeoff

[Shamir '07] AES may well be the last block cipher

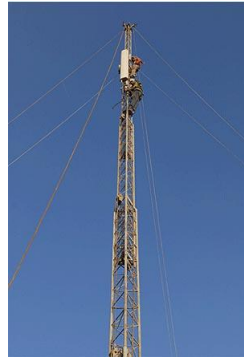
Low cost hw: throughput versus area

100 KHz clock

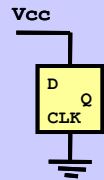
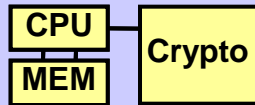
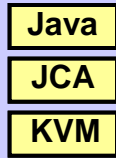
(technology in 10 nm)



Implementations in embedded systems



Cipher Design,
Biometrics



Protocol: low power authentication protocol design

Algorithm: public key, secret key, hash algorithms

Architecture: Co-design, HW/SW, SOC

Micro-Architecture: co-processor design

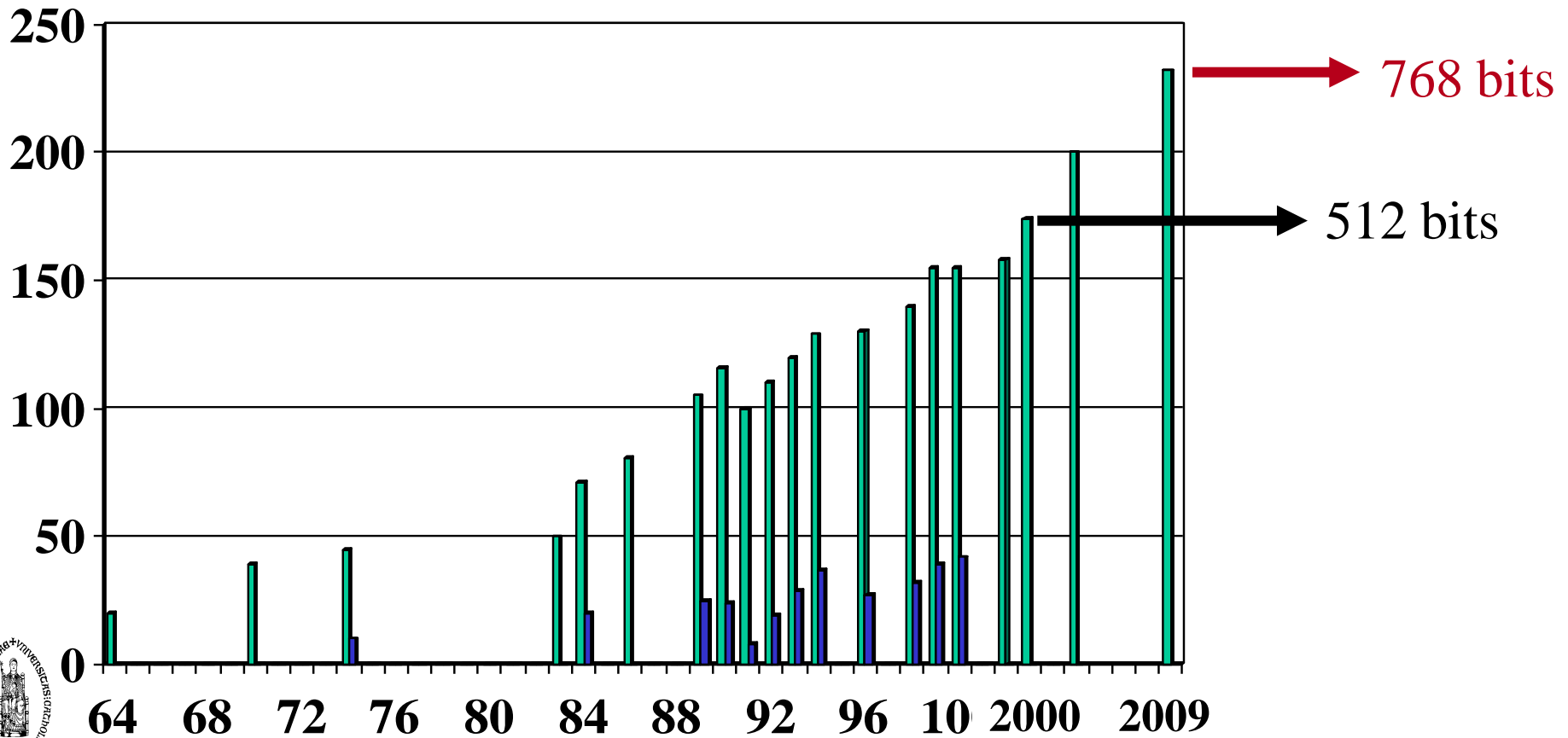
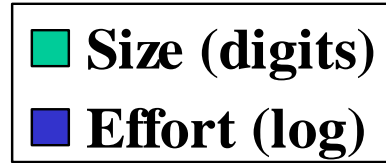
Circuit: Circuit techniques to combat side channel analysis

Public key cryptology (ECC)
15K gates - 13.8 μ W - 1.18 μ J

Factorisation records

2009: 768 bits or 232 digits

1 digit ~ 3.3 bits



New computational models: quantum computers?



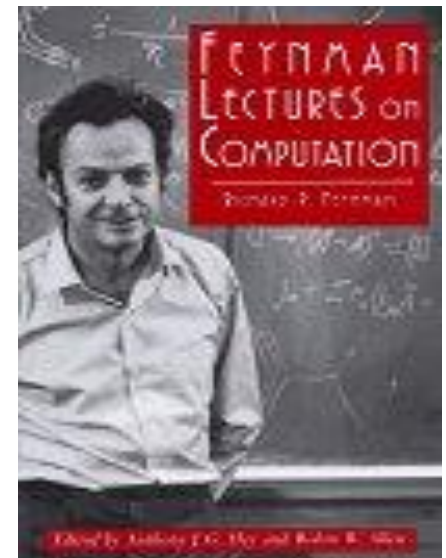
- exponential parallelism

n coupled quantum bits



2^n degrees of freedom !

- Shor 1994: perfect for factoring
- But: can a quantum computer be built?



4-channel Varian spectrometer

11.7 T Oxford magnet, room temperature bore

$15 = 5 \times 3$

grad students in sunny California...

2001

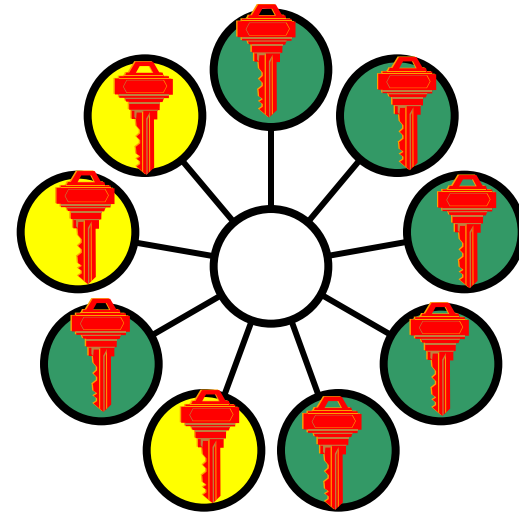
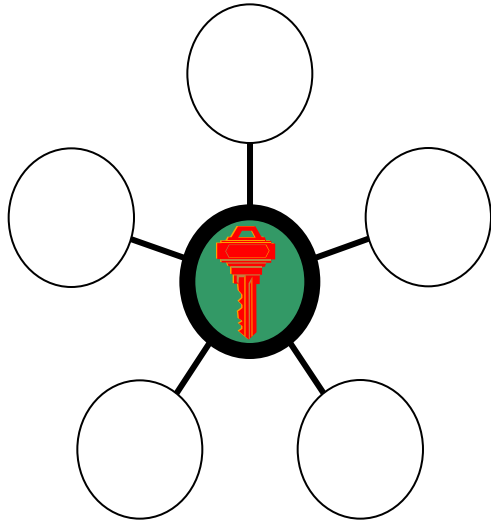
If a large quantum computer can be built...

- All schemes based on factoring (such as RSA) will be insecure
- Same for discrete log (ECC)
- Symmetric key sizes: x2
- Hash sizes: x2 for (2^{nd} preimages)



- This motivates the need for **Post Quantum Crypto**
- E.g., HFE, NTRU,...
- Matching current systems is hard

Secure computation: distributing trust



- PKI
- Banking
- Credit card
- Google
- ...

- Multi-party computation
 - e-voting
 - e-auction
 - smart devices

“you can trust it because you don’t have to”

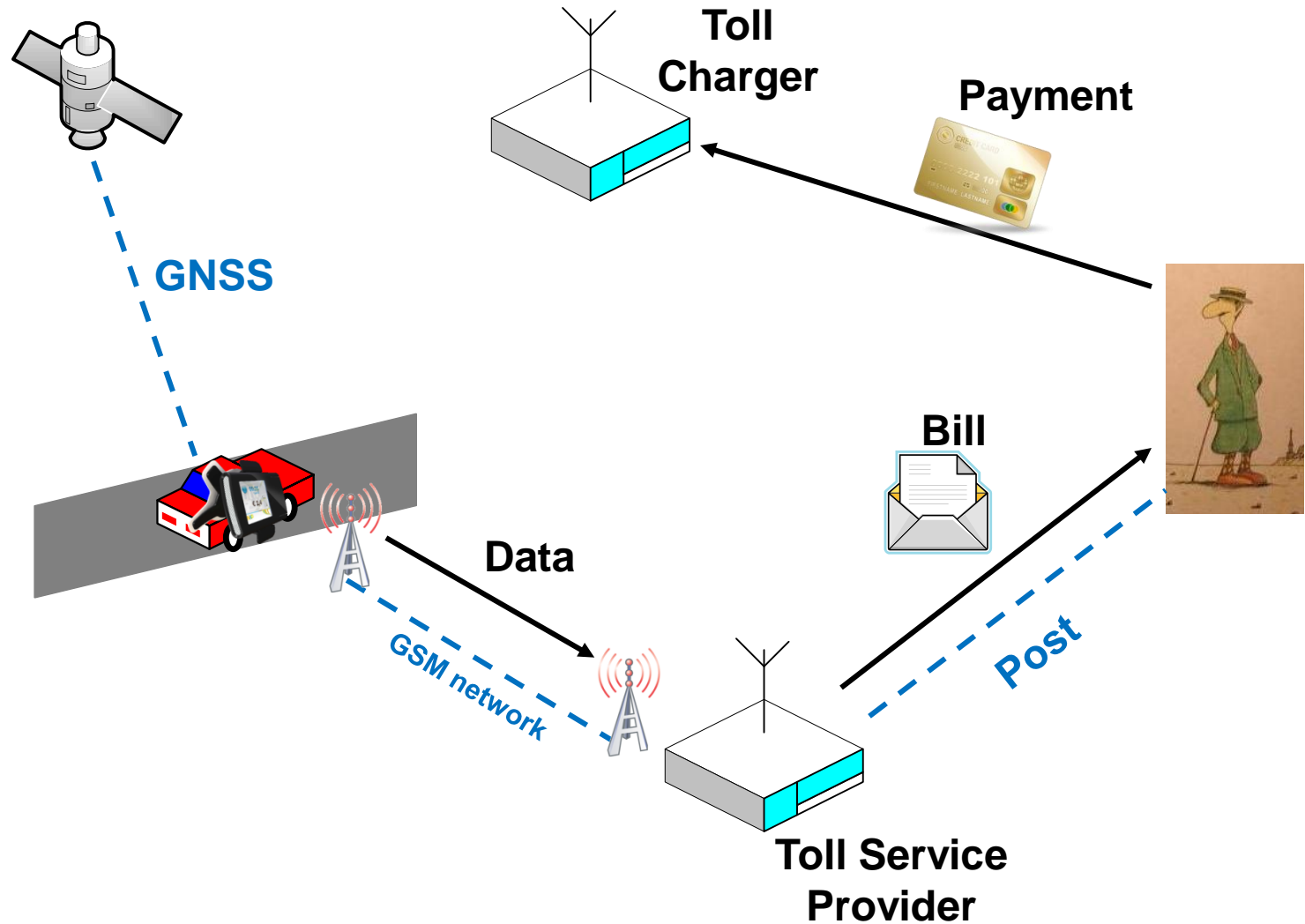
stop building databases with policies – go for privacy by design with true data minimization

Internet voting

- Helios [Adida'08] www.heliosvoting.org
 - sophisticated cryptographic protocols: open audit
 - open source
- Spring 2009: rector elections in UC, Belgium
- August 2010: adopted by IACR
- +
 - remote voting
 - as everything is encrypted, log files can be made public so disputes can be resolved easily
- --
 - coercion risk
 - Trojan or virus can easily undermine these elections (proof of concept [Desmedt'09])

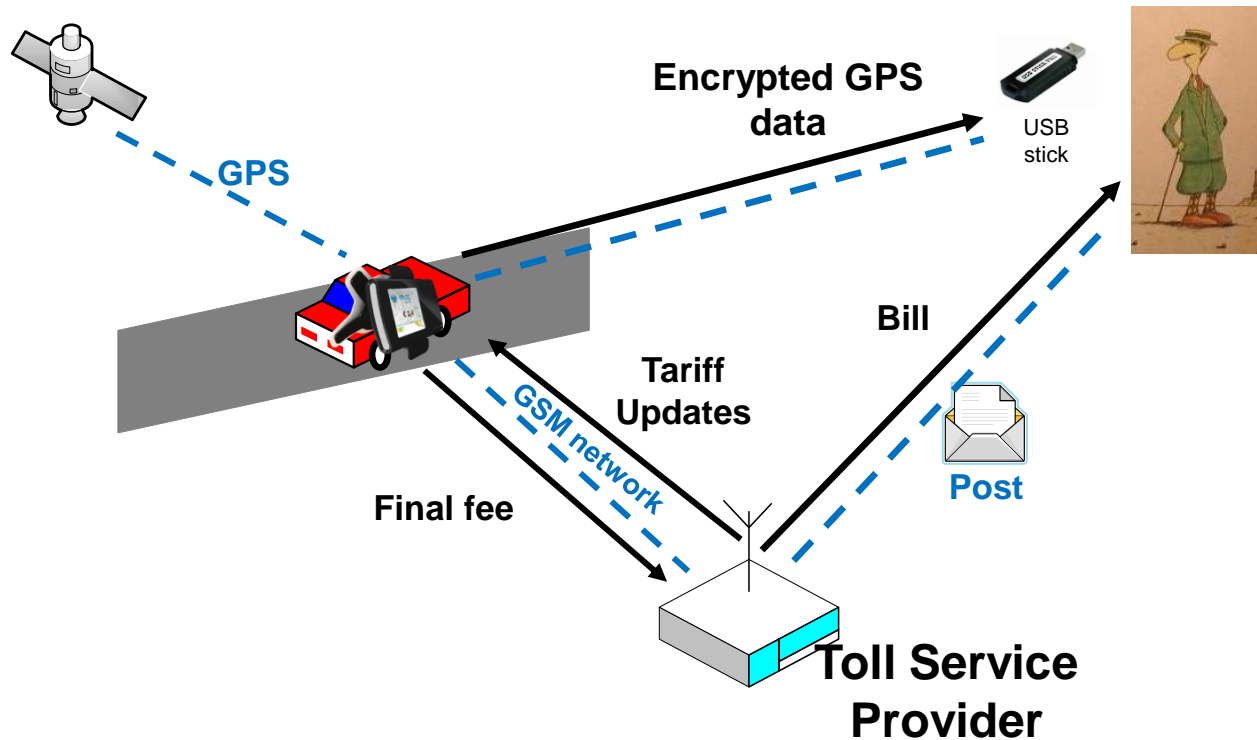
not suitable for public sector elections

Road pricing: current implementation

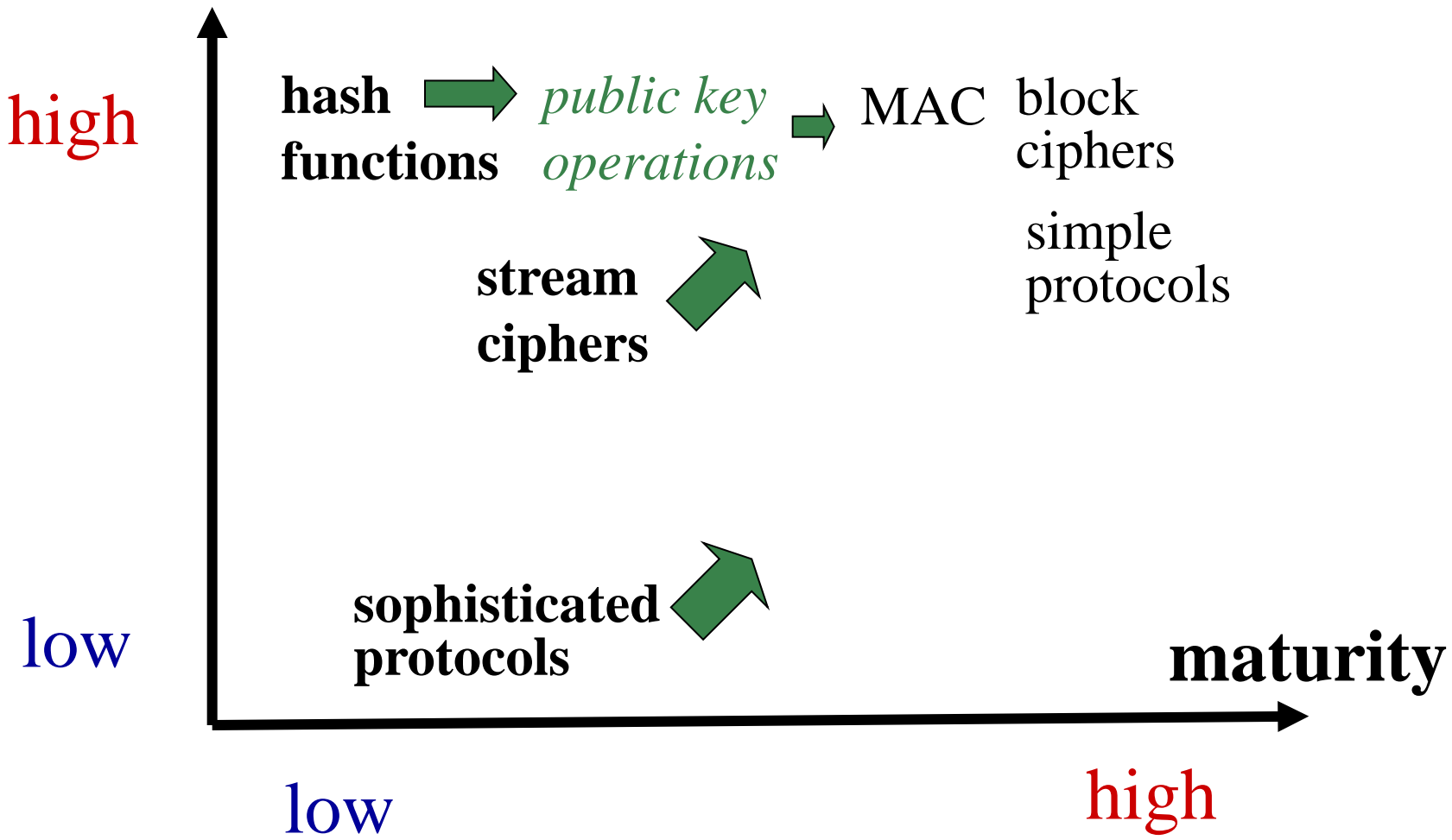


Privacy-Friendly Electronic Toll Pricing

No personal data leaves the domain of the user



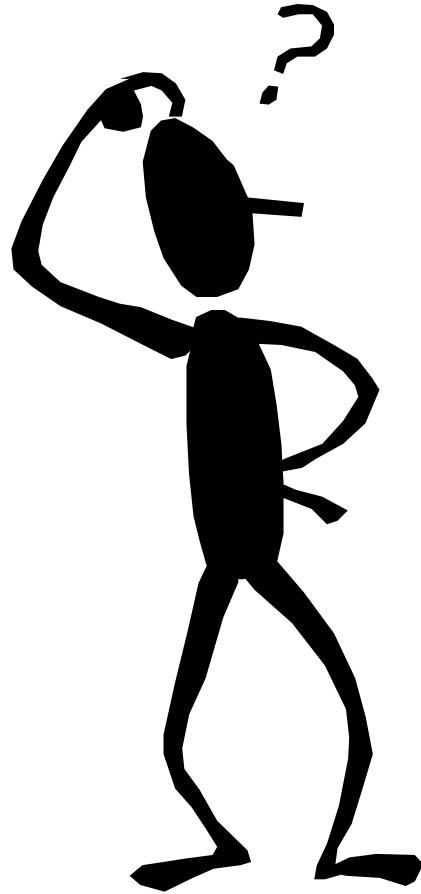
demand in applications



Conclusions

- success story but the crypto problem is **not** solved
- major challenges remain in cryptographic algorithm design and implementation
 - “green crypto”
 - secure implementations
- privacy enhancing technologies
 - privacy by design
 - anonymous networking
- linking crypto with physical world
 - biometrics, physical unclonable functions
- advanced crypto can do little miracles

The end

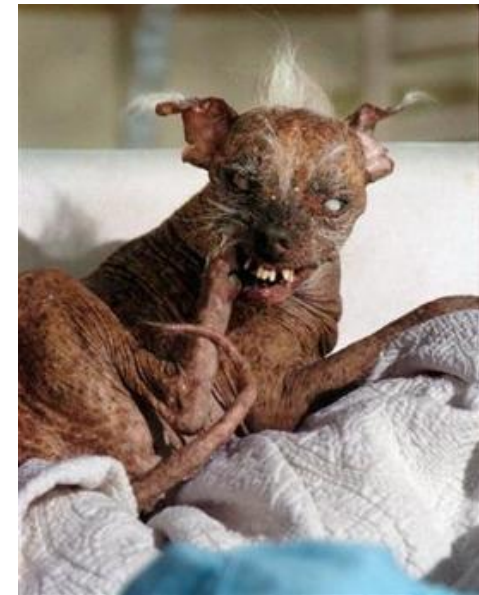


Thank you for
your attention

Extra slides

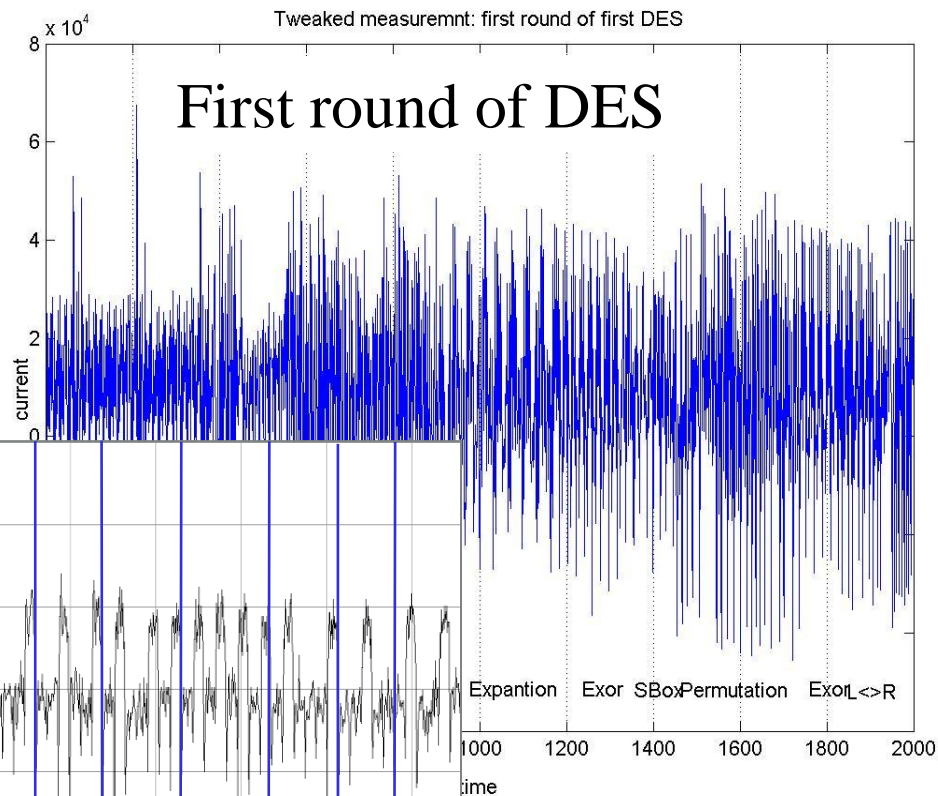
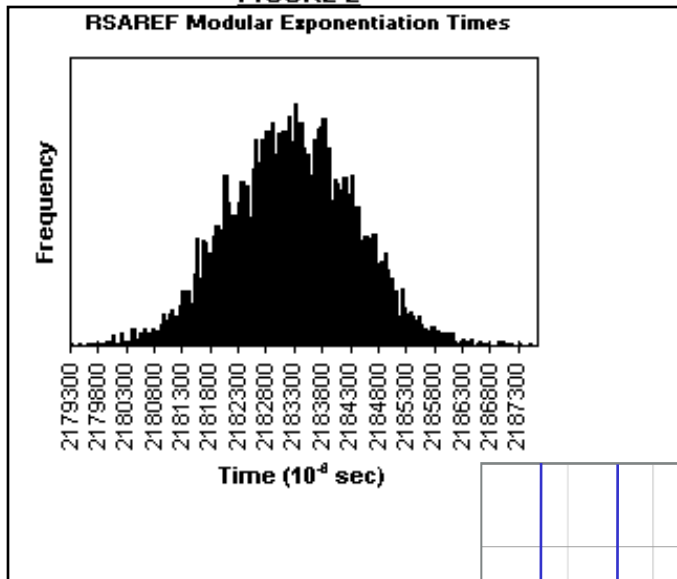


Models and reality



Implementations: side channel attacks

FIGURE 2



RSA

ion



Implementation attacks

Sun Tzu, The Art of War:

In war, avoid what is strong and attack what is weak

- measure: time, power, electromagnetic radiation, sound
- introduce faults (even in CPUs – bug attacks)
- combine with statistical analysis and cryptanalysis
- software: API attacks
- major impact on implementation cost

L.R. Knudsen: "It is not cryptanalysis, it is vandalism"



The power challenge:

AES-128 speed/power for various platforms (Joule/Gb)

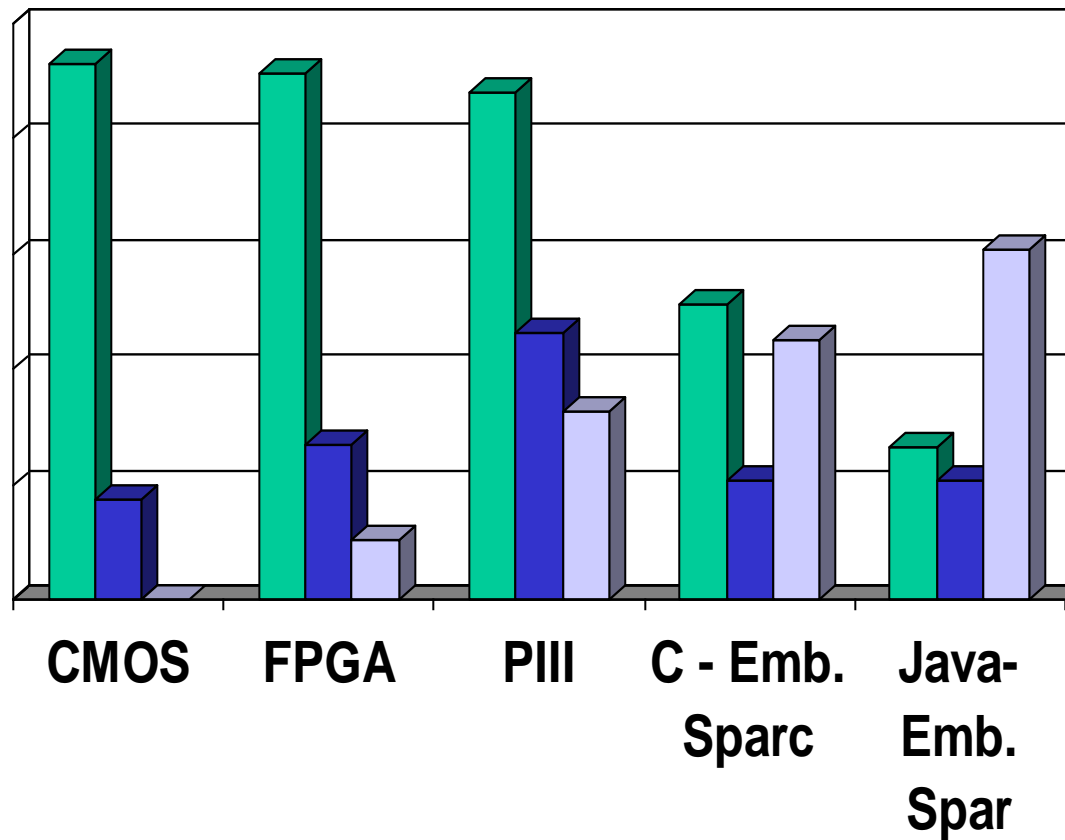
1 Gbit/s

1 Mbit/s

1 Kbit/s

Watt

mWatt



10⁶

10³

1

■ speed ■ power ■ power/speed

