

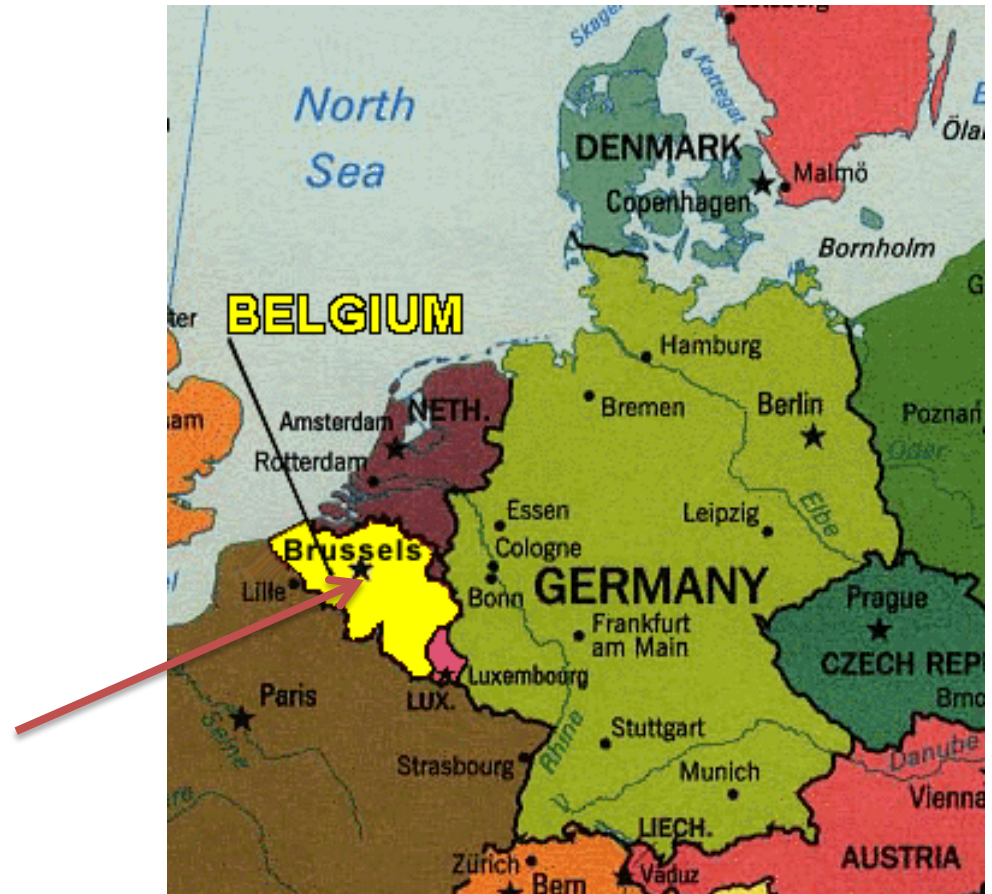
# RFID Security & Privacy Research

Dave Singelée

K.U.Leuven - SCD/COSIC

# K.U.Leuven - SCD/COSIC

COSIC: COmputer Security and Industrial Cryptography



# 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, HAMS1

Fundamental research in discrete mathematics

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

# RFID Security & Privacy Research

## RFID Security & Privacy Solutions

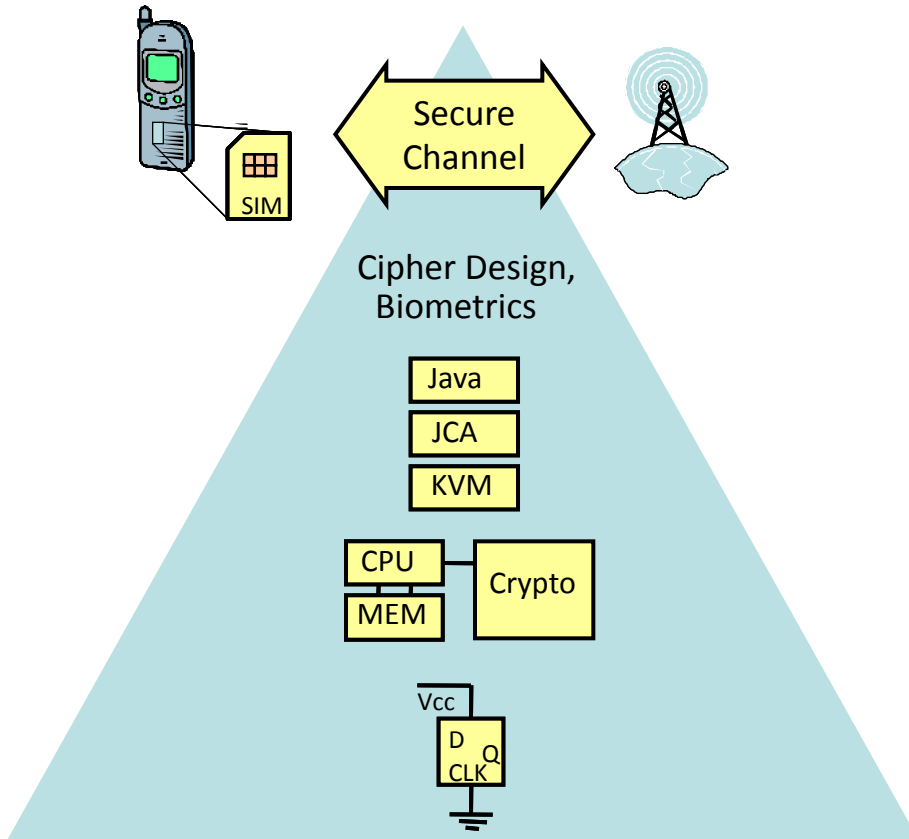


- Lightweight cryptographic primitives
- Compact, efficient and secure implementations

- Authentication protocols
  - Symmetric key
  - Public key
- Distance bounding protocols

- Privacy models
- Provable security

# Security = integrated solution



**Application:** supply chain, access control

**OS:** Operating system

**Crypto Algorithm/Protocol:** Embedded fingerprint matching, crypto, entity authentication

**Architecture:** Co-design, HW/SW, SOC

**Micro-Architecture:** co-processor design

**Circuit:** Circuit techniques to combat side channel analysis attacks

**Security is not a point solution**

# Holistic design approach

## Security requirements

- Authentication
- Impersonation attack
- Anti-counterfeiting
- Relay attacks

## Privacy requirements

- Tracking
- Location Privacy
- Unlinkability

## Implementation requirements

- Efficient algorithms
  - Compact
  - Low-cost
- Minimized energy consumption
- Side-channel resistant

## System requirements

- Scalability
- Back-end system
- Compatibility issues

RFID  
security  
solution

```
graph TD; S[Security requirements] --> C((RFID security solution)); P[Privacy requirements] --> C; I[Implementation requirements] --> C; Sys[System requirements] --> C;
```

# Contact information

## ESAT / SCD - COSIC

- Prof. Bart Preneel
- Prof. Ingrid Verbauwhede
- Prof. Vincent Rijmen
  
- <http://www.esat.kuleuven.be/cosic/>
- Tel: +32-16-321050  
Fax: +32-16-321969
  
- K.U.Leuven, ESAT / SCD - COSIC  
Kasteelpark Arenberg 10, bus 2446  
B-3001 Leuven-Heverlee
  
- RFID Security & Privacy  
Dave.Singelee@esat.kuleuven.be