Securing Passive RFID Tags Using Strong Cryptographic Algorithms

4th European Workshop on RFID Systems and Technologies

10-11 June, 2008, Freiburg, Germany

Martin Feldhofer

IAIK – Graz University of Technology
Martin.Feldhofer@iaik.tugraz.at
www.iaik.tugraz.at

About us

Graz University of Technology →
Faculty of Computer Science →
Institute for Applied Information Processing and Communications (IAIK)

Research groups

- Crypto group (hash functions and block ciphers) – Vincent Rijmen
- EGIZ (e-government)
- Trusted computing/Java security
- Network security
- VLSI group
  - Implementation of crypto algorithms
  - SCA/fault attacks and countermeasures
  - RFID security and tag design

RFID Security Research Projects

- C@R: “**Collaboration Rural**”
  - IP in FP6; IAIK performs research towards asymmetric crypto in RFID
- BRIDGE: “**Building Radio frequency IDentification solutions for the Global Environment**”
  - IP in FP6; IAIK is task leader for secure RFID tags
- PROACT: Currently, local initiative (sponsored by NXP) to support RFID research and education @ TU Graz
  - Aims to get European Center of Excellence
- SNAP: Secure NFC Applications (national funded project, local cooperation with NXP)

Outline

- Motivation
- Requirements for RFID tag hardware
- Low-power design strategy
- Security algorithms in hardware
- Comparison of implementations
- Implementation security
- Conclusions

Questions

- Will every passive RFID tag has security features in a few years?
- What are the difficulties in designing hardware for passive RFID tags?
- Which cryptographic algorithm should be used?
- Why does the RFID industry does not have products with strong crypto?
- Are implementation attacks really a threat?
- Is this work theoretical research or has it practical relevance?

Why Security for RFID Systems?

Counterfeiting

Seven percent of world trade is counterfeited goods (ICC/2003)

- 500 billion USD in 2004 (TECTEM/2004)
- 5-10% of car parts (Commission EU/2004)
- 5-8% of pharmaceuticals (WHO/2002)
- 12% of toys in Europe (OECD/2000)

Problems

- High losses
- Decreases the value of brands
- Threat against public health and safety

Why Security for RFID Systems?

Privacy

Is “Big Brother” really watching you?

Monitoring of communication is easy

- Contact less, no clear line-of-sight, broadcast signal
- Even tag-to-reader load modulation observable in 4.5m distance

Activity tracking of persons via UID

Leakage of personal belongings data

→ It is useful to integrate security into RFID systems

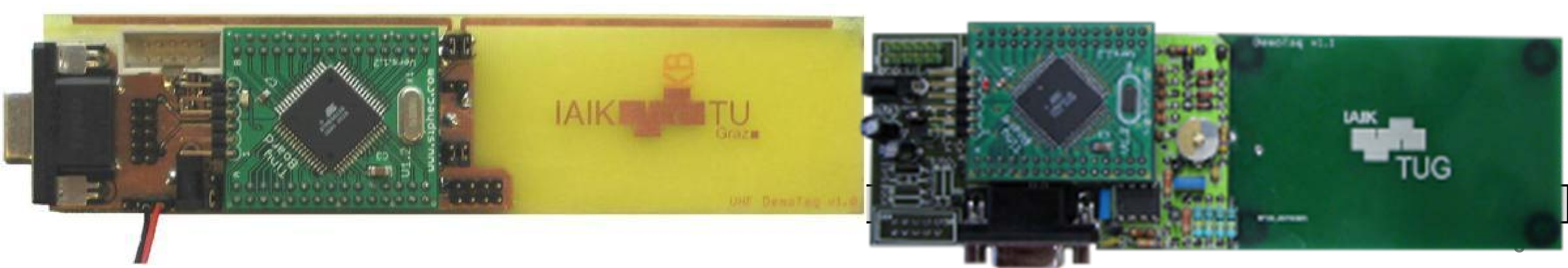
Tag Prototype Development

Can be used for …

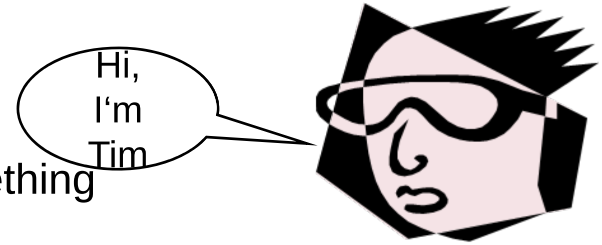
- … showing weaknesses in RFID systems
- … evaluate security protocols
- … testing of reader prototypes
- … demonstrate new applications

IAIK DemoTags

- HF (13.56MHz) and UHF (860MHz) frequency range
- Programmable via microcontroller



Identification vs. Authentication



Identification

- Claim to be somebody / something

Authentication

- Proof the claim (by special characteristic, shared knowledge, possession or trusted 3rd party)

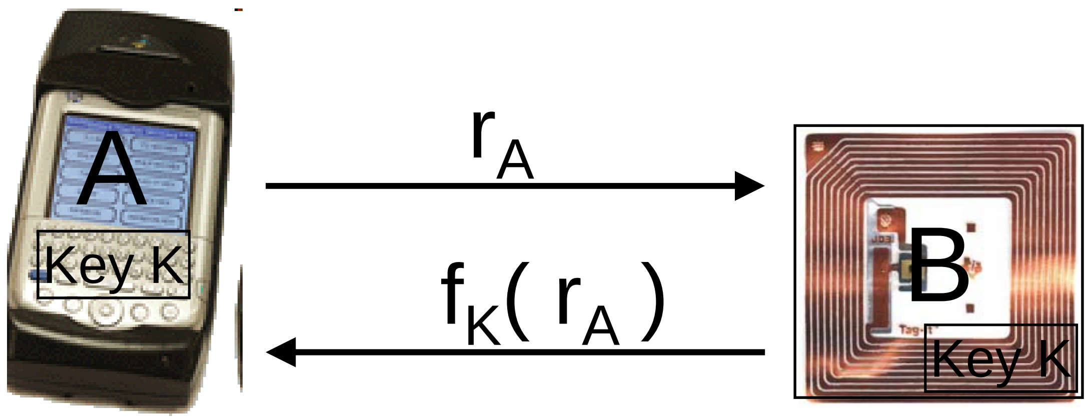
Pass word (weak authentication)

- user ID + password
- interactive
- be aware of replay attacks!

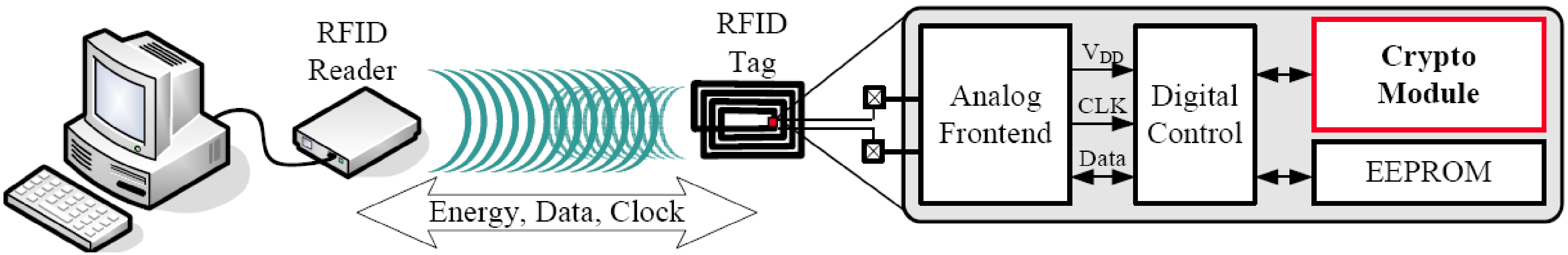
Tag Authentication Protocol

Challenge-response (strong authentication)

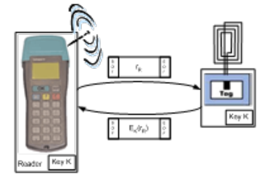
- Proofs knowledge of shared secret key
- Requires random “challenge”
- “Response” depends on challenge and secret key (encryption result)
- Compatibility to existing standards



Secure RFID System Architecture



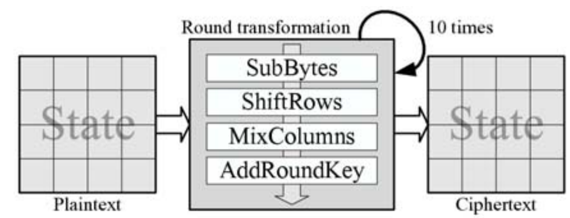
Requirements for a Secure RFID System



Security protocol
- Challenge-response authentication

Cryptographic primitive
- Hash function, block cipher, universal hash function, public key algorithm
- “Lightweight” solution (HB, …)

Standardized algorithm
- Analyzed by many crypto experts
- AES-128, SHA-1, SHA-256, MD5, Trivium, Grain



Strong cryptography
- Appropriate key size (128 bits)

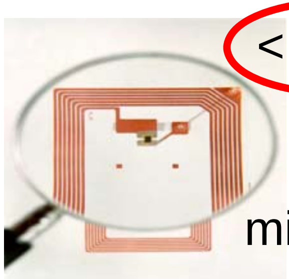
Authentication and/or anonymity

What about the implementation costs on an RFID tag?

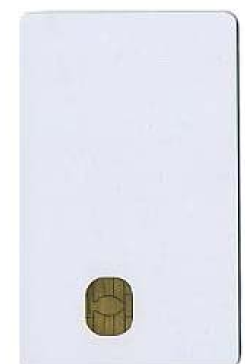
RFID Tag vs. Contact-Less Smart Card

Common properties

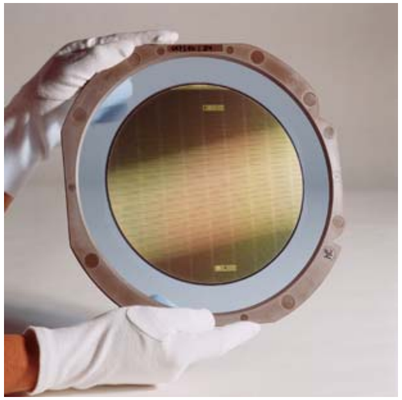
- Passively powered (no active power supply)
- Communication over air interface



RFID tag		CL smart card
< 1.2 - 5m	**Reading range**	< 10 cm
< 15µA (scarce)	**Power consumption**	~ 10mA (enough)
< 1 mm²	**Chip area**	15 -20mm²
minimal, 5-10 Cent	**Prize (€)**	some €
LF, HF, UHF	**Frequency**	HF
inventory (until now)	**Application**	authentication
dedicated circuit	**Hardware**	microcontroller
non/proprietary	**Security**	crypto coprocessor



Challenges of Hardware Implementations



Power consumption

- Maximum 25 µW
- Determines operating range (~1m required)
- Below 15µA (1.5 V) mean current consumption
- 0.35 µm CMOS: ~15 D-FF @ 1MHz

Chip area

- Die size equals silicon costs (5-20 Cent)
- Less than 5000 gate equivalents for security

Size of 0.5x0.5mm² pin

Security level

- Standardized key length
- 112, 128 bits

2^{55} odds of winning lottery AND being hit by lightning at the same day
2^{170} number of atoms in the planet

BUT

- Very low data rates (26 kbps) ➔ low clock frequency
- High number of available clock cycles

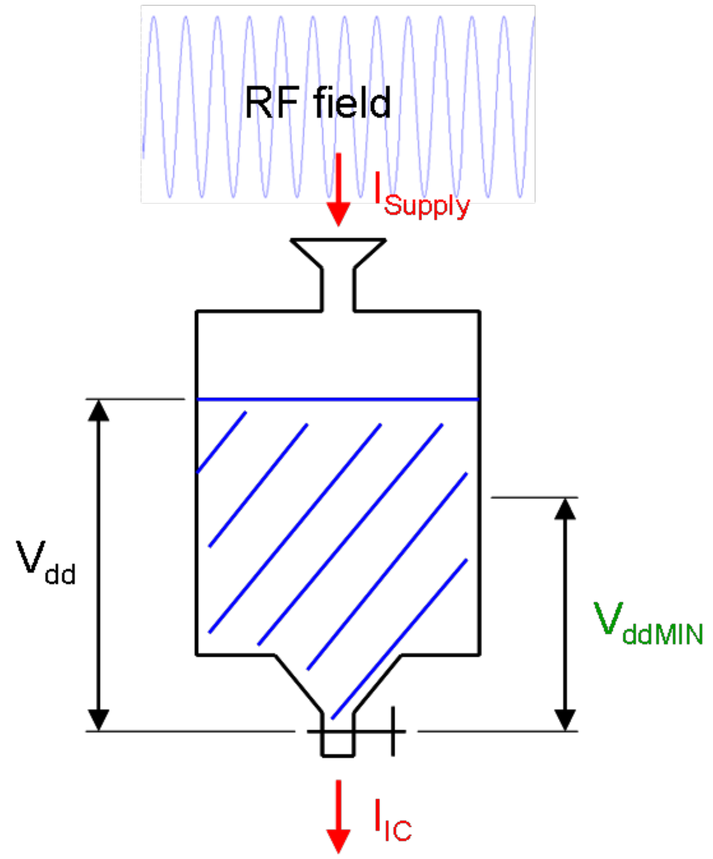
Low-Power Design for RFID Hardware

Not relevant for RFID tags

- Energy consumption per operation
- Power consumption per operation

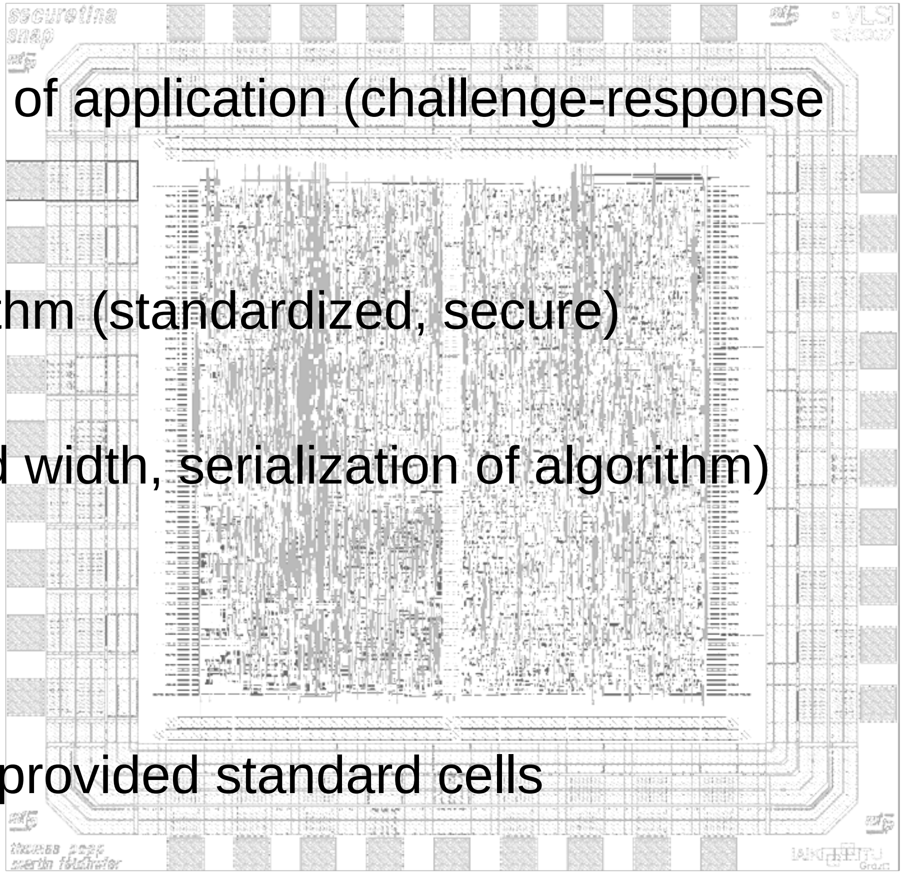
Relevant for RFID tags

- Power consumption per cycle
- Mean current consumption must not exceed available energy in capacitor



Design Strategies for Crypto on Passive RFID Tags

Design on different levels

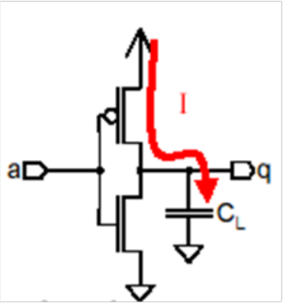


- System level
  - Protocol design, features of application (challenge-response authentication protocol)
- Algorithmic level
  - Select appropriate algorithm (standardized, secure)
- Architecture level
  - Data path structure (word width, serialization of algorithm)
- Circuit level
  - Avoid glitching activity
- Gate level (and below)
  - No influence because of provided standard cells

Low-Power Design

Power dissipation

- $P_{Total} = P_{Static} + P_{SC} + P_{Dynamic}$
- $P_{Dynamic} = C_L \cdot V_{DD}^2 \cdot f$



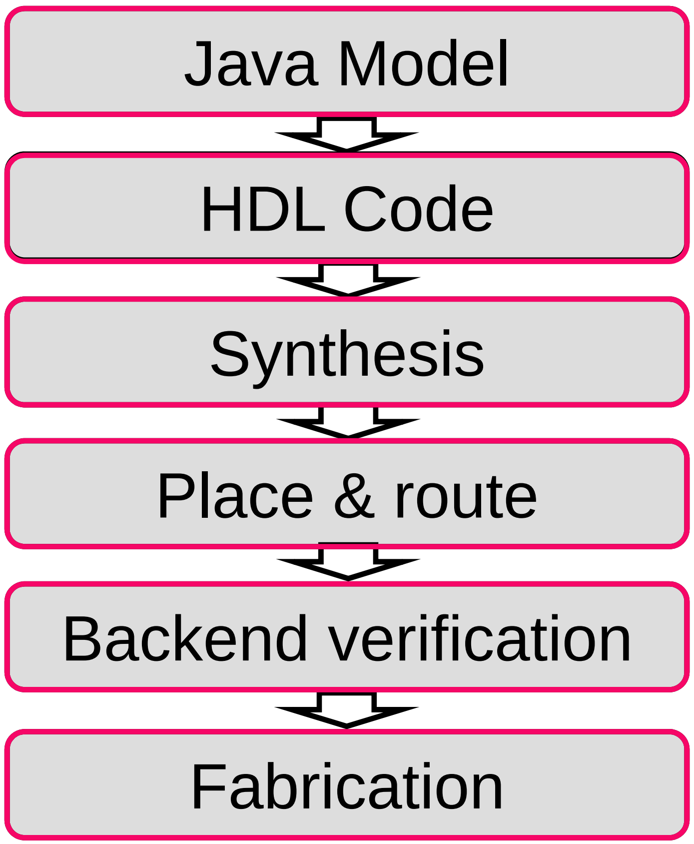
Design for power reduction

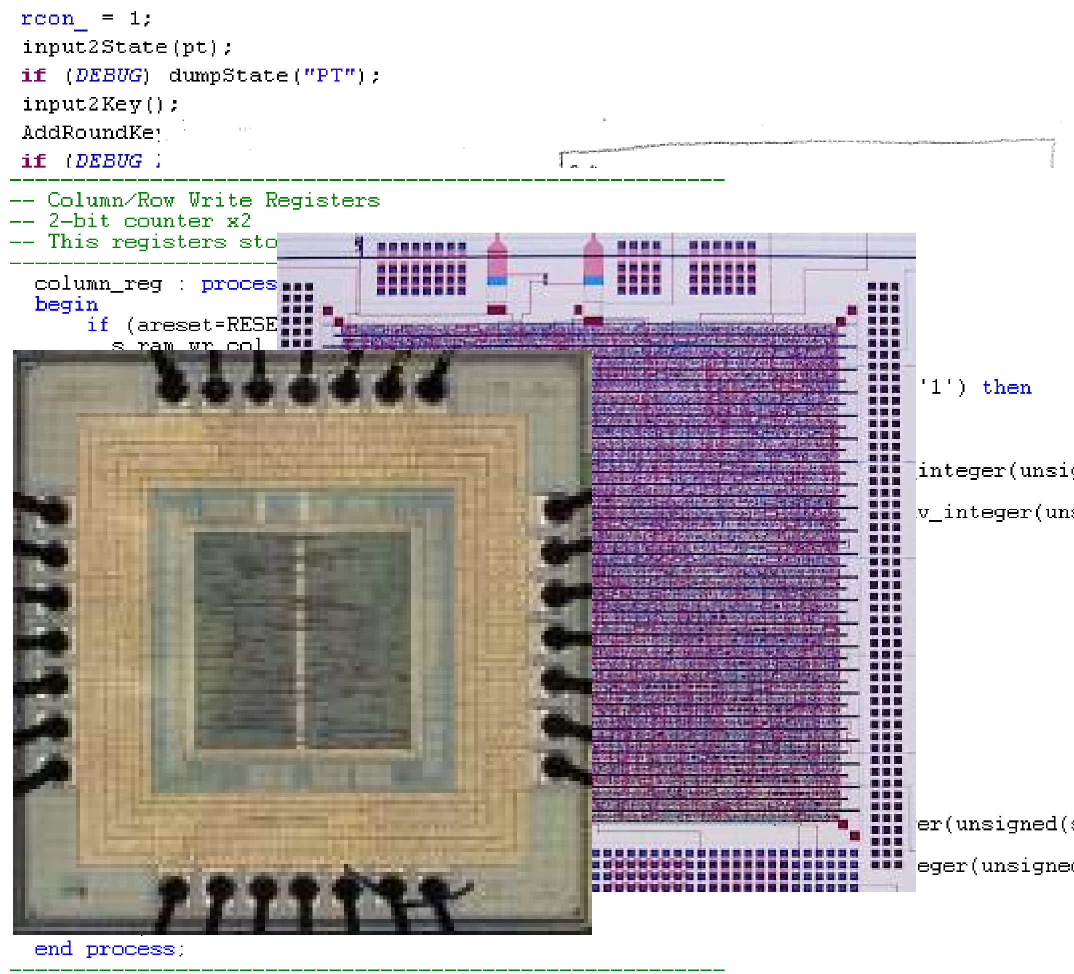
- Lowering V_{DD}
- Use lowest possible clock frequency (<100 kHz)
- Clock gating
- Avoiding glitching activity (sleep-mode logic)

Optimization goal

- Minimize triple (I_{mean} [µA], Chip area [GE], #Clock cycles)
- $P_{Dynamic} = C_L \cdot V_{DD}^2 \cdot f \cdot p_{sw}$

Semi-custom Design Flow





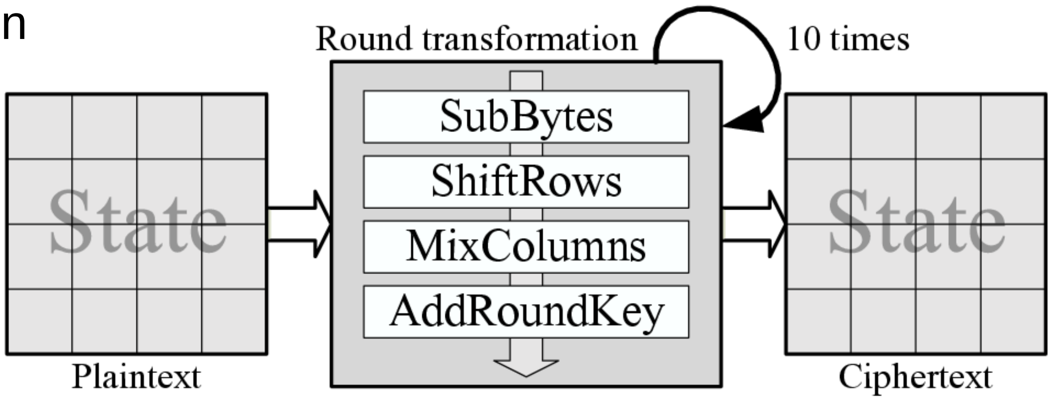
Why AES is Suitable for RFID Tags

Simplicity

- Symmetry
  - Round transformation
- Basic operations
  - Finite field GF(2^8)

Flexibility

- Architecture
  - 8-bit, 32-bit, 128-bit



Balance

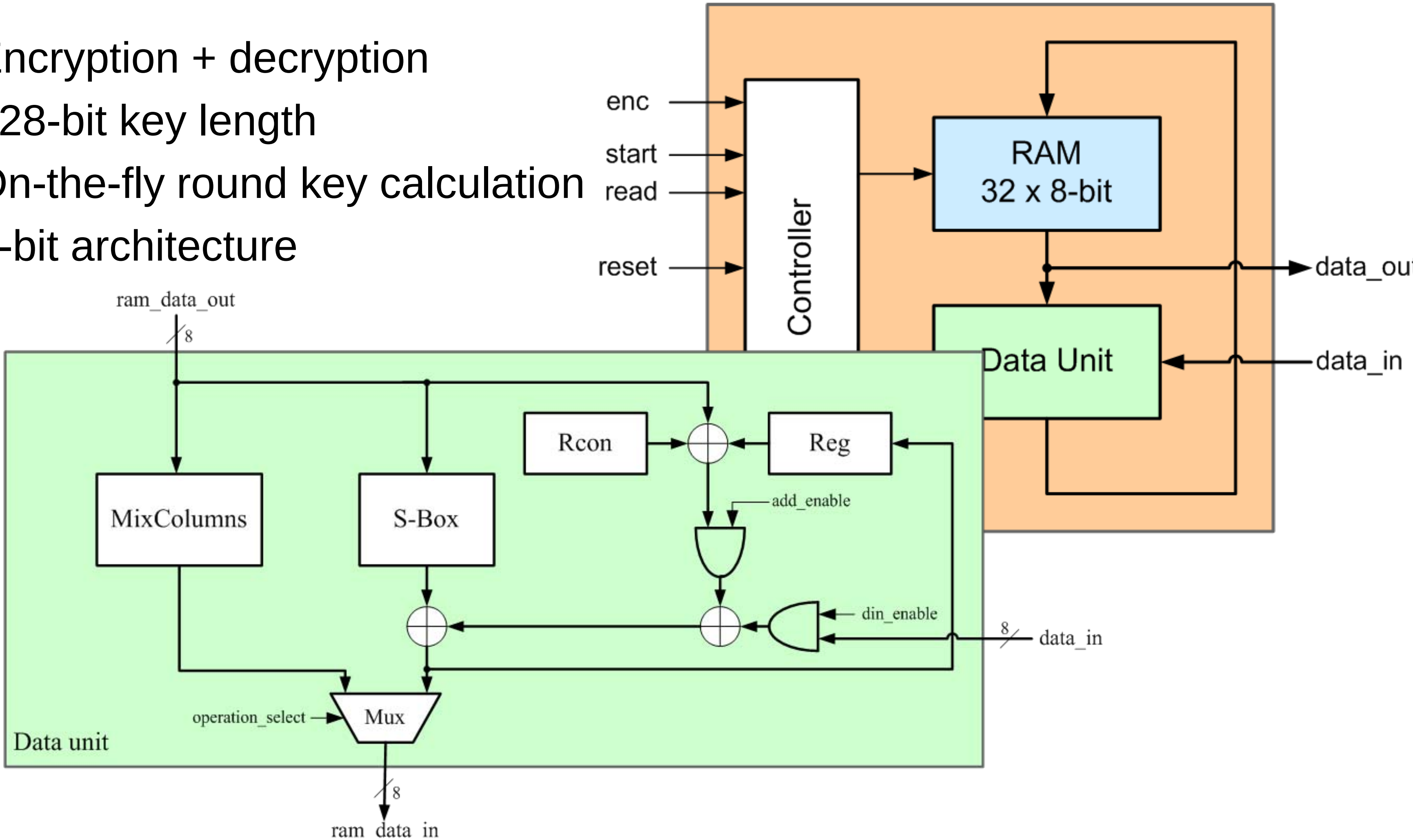
- Optimal relationship between flip flops and computational costs
- 256 bits memory and simple operations

Standardized

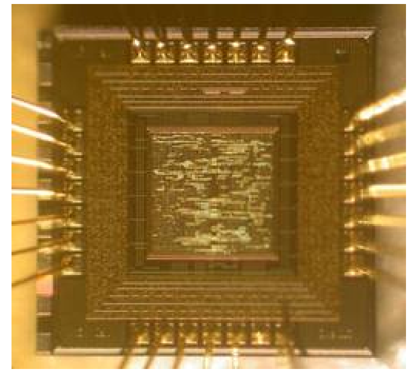
- FIPS standard since 2001

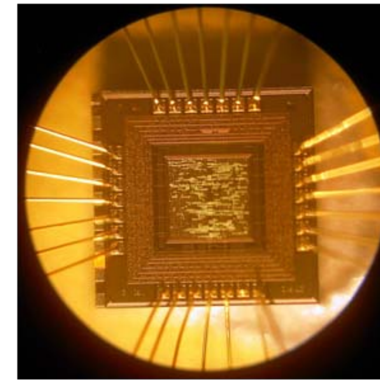
AES Architecture

- Encryption + decryption
- 128-bit key length
- On-the-fly round key calculation
- 8-bit architecture



Results of TINA





AES-128 hardware module

- Suitable for passive RFID tags

Chip area

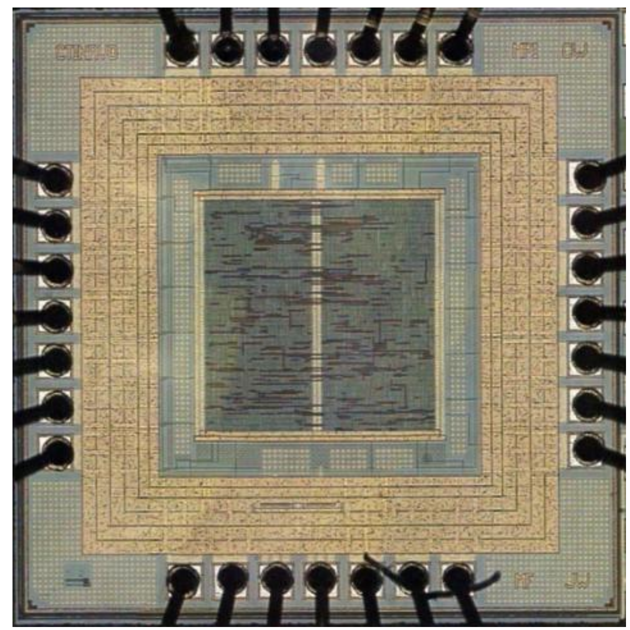
- 0.25 mm^2
- 3.400 GEs

Current consumption

- 3µA @ 100 kHz at 1.5 V
- Process: 0,35µm CMOS

Data throughput

- 1000 cycles / 128 bits



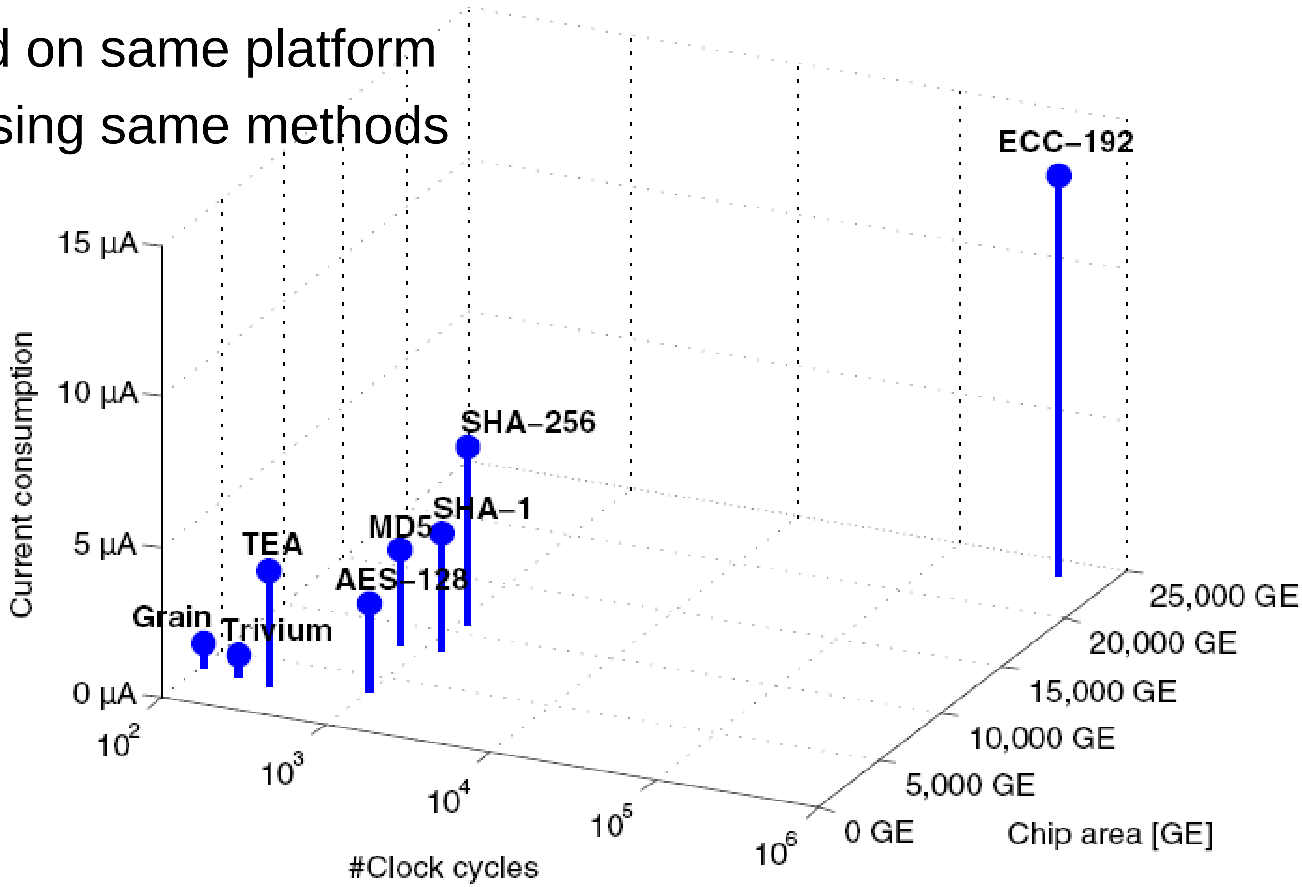
Comparison of Implementations

Algorithm	Chip area [GEs]	I_{mean} [µA @ 100kHz, 1.5V]	# Clock cycles
AES-128	3400	3.0	1032
SHA-256	10 868	5.83	1128
SHA-1	8120	3.93	1274
MD5	8001	3.16	712
Trivium	3090	0.68	(1,603) + 176
Grain	3360	0.80	(130) + 104
TEA	2633	3.79	289
ECC-192	23 600	13.3	500 000

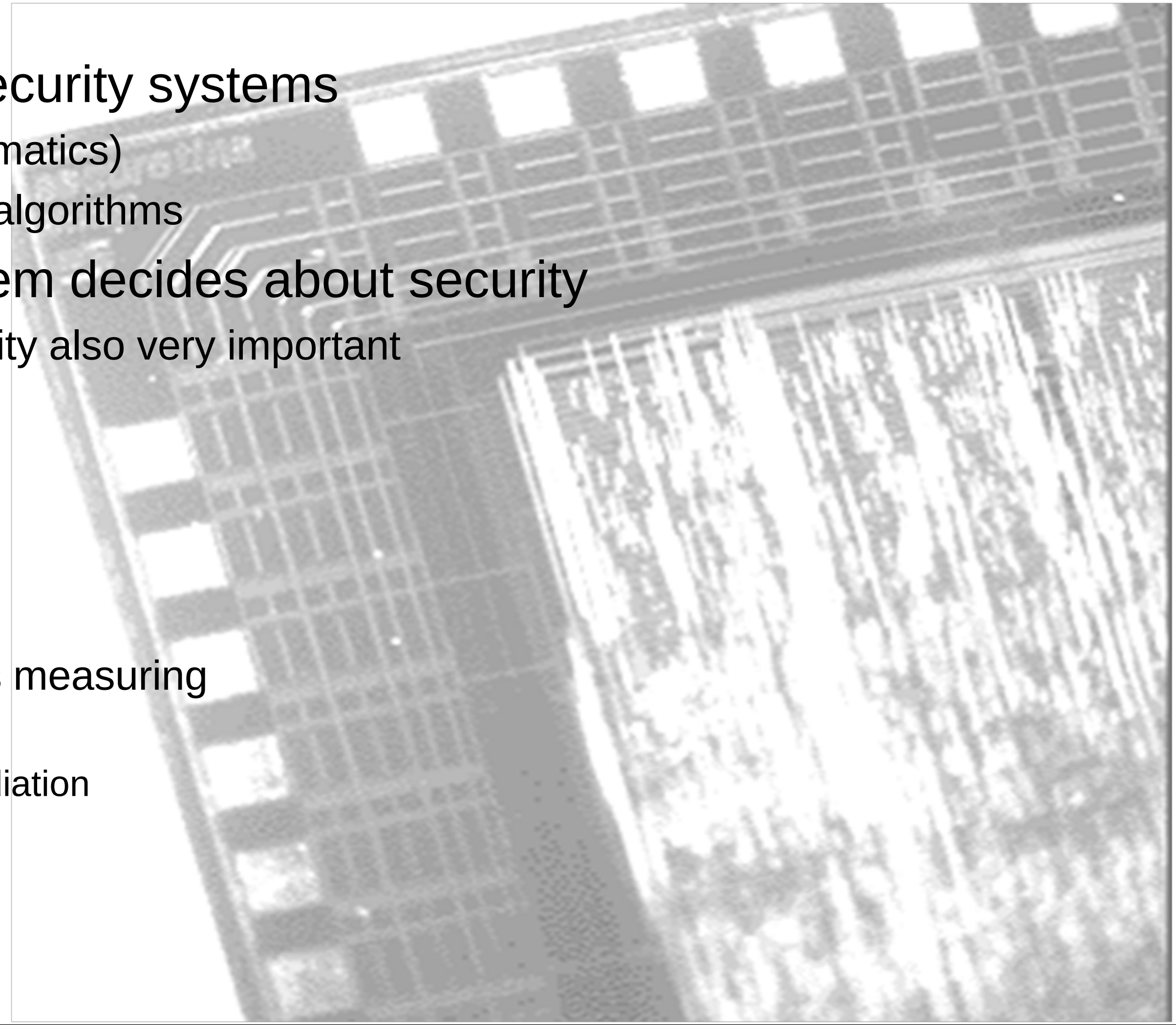
Comparison of Different Algorithms

Hardware implementations

- Implemented on same platform
- Optimized using same methods



Implementation Security



Traditional attacks on security systems

- Cryptanalysis (mathematics)
- Strength of keys and algorithms

But weakest link in system decides about security

- Implementation security also very important

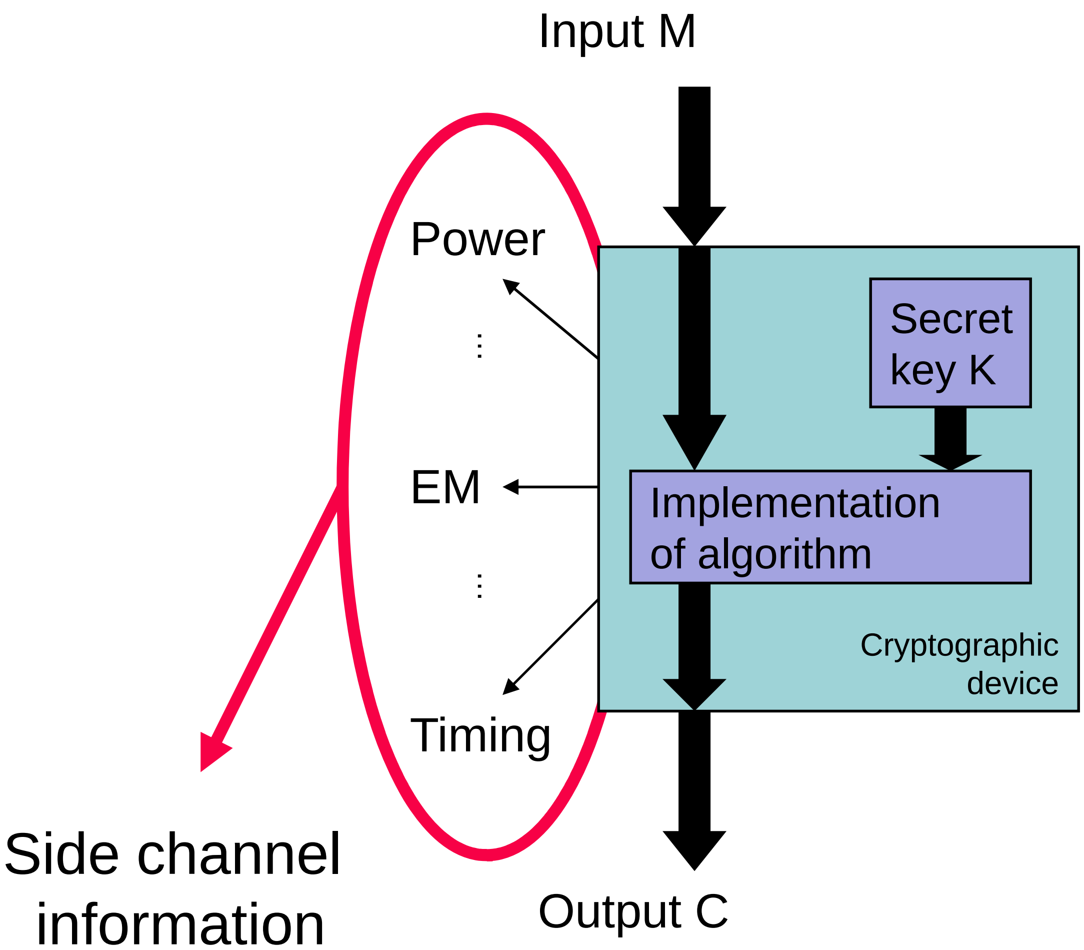
Active attacks

- Fault analysis
- Physical probing

Passive attacks

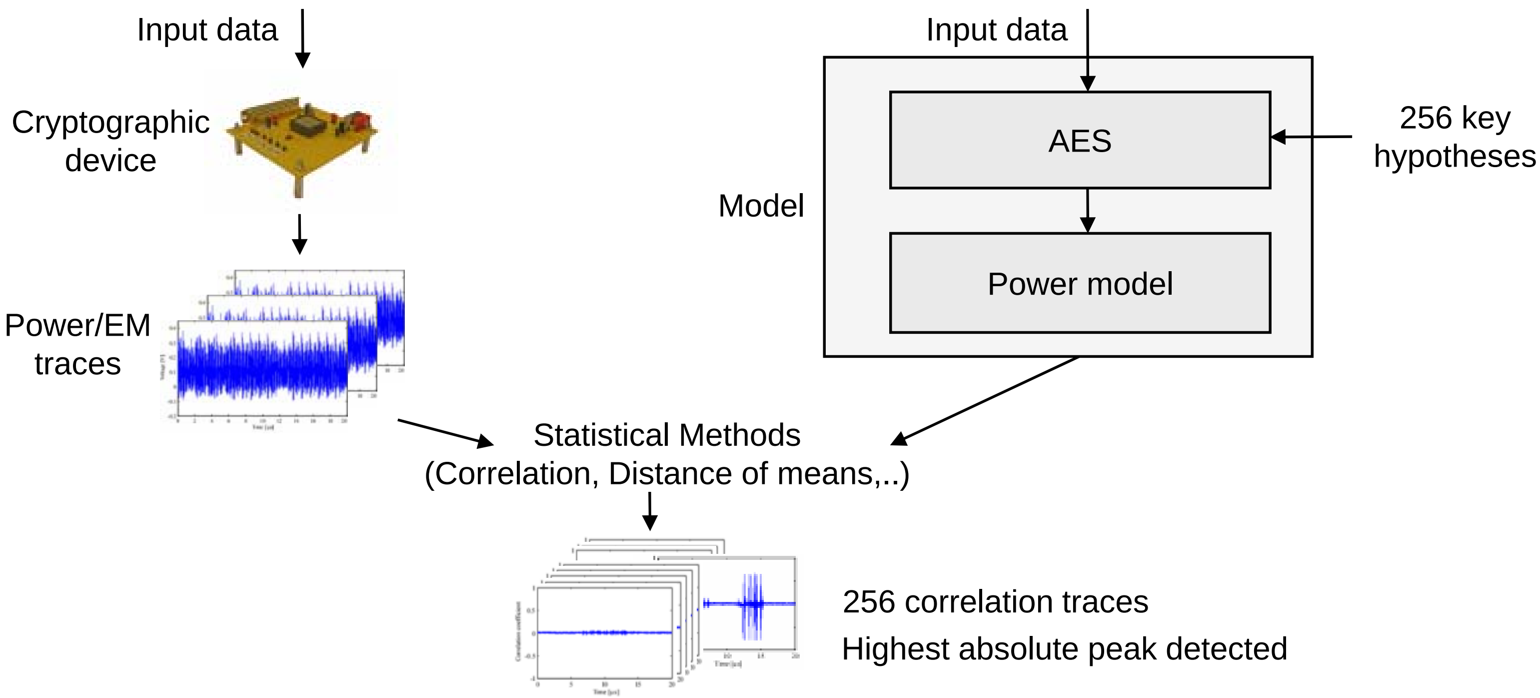
- Side-channel analysis measuring
  - Power consumption
  - Electromagnetic radiation
  - Timing information
  - Error messages

Side Channels of Cryptographic Devices



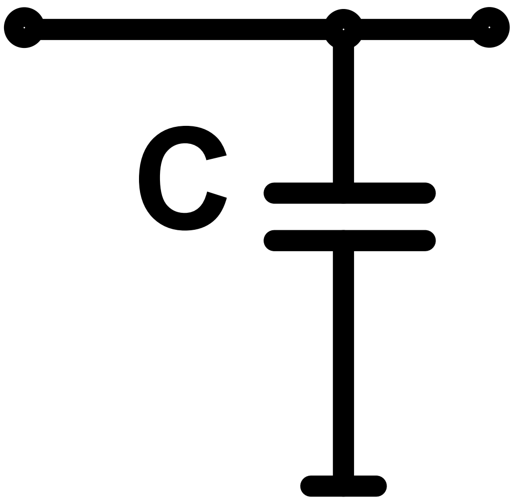
Differential Power/EM Analysis

- Target of the attacks is an intermediate value that depends on the secret key



Why Does SCA Work?

The problem is the data depending power dissipation of the internal nodes of (CMOS) circuits



Transition of node value	Power consumption
0 -> 0	P_{00}
0 -> 1	P_{01}
1 -> 0	P_{10}
1 -> 1	P_{11}

$P_{01} >> P_{10} > P_{00}, P_{11}$

$P_{00} + P_{10} \neq P_{01} + P_{11}$

Implementation of Countermeasures

„The goal of countermeasures against SCA attacks is to make the power consumption of the device independent of the intermediate values of the executed algorithm.“ [Mangard, Oswald, Popp; Power Analysis Attacks – Revealing the Secrets of Smart Cards]

Implemented countermeasures

- Hiding (Randomization)
  - Remove data dependency of power consumption
  - Shuffling of operations
  - Execution of dummy cycles
- Masking
  - Randomize intermediate values that are processed
  - Use an SCA-resistant logic style

Implementation Security Costs

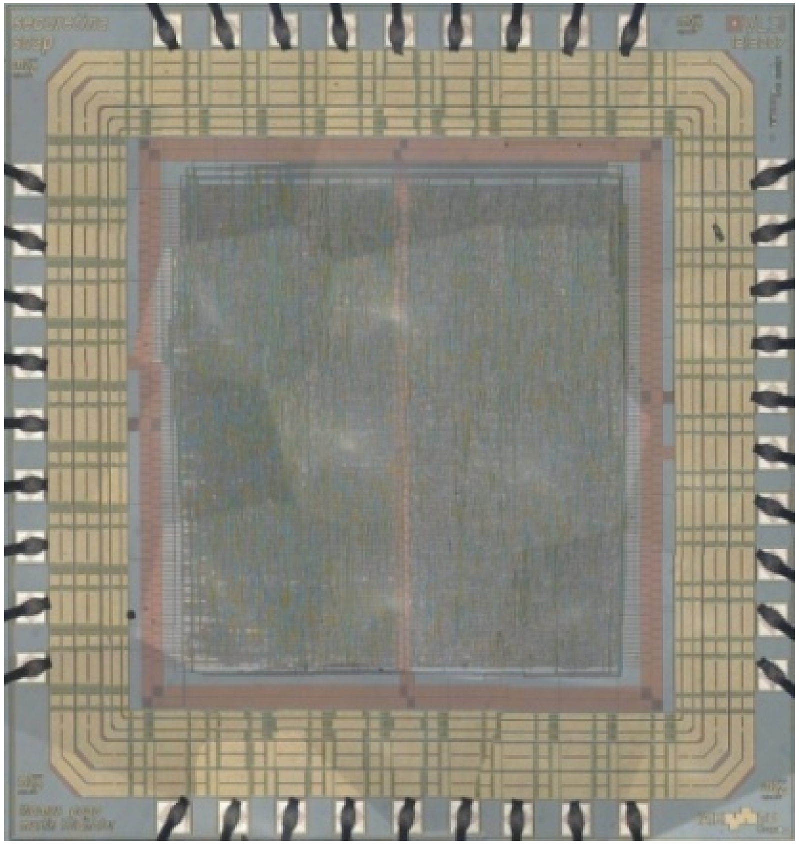
Requires higher power consumption

- 5 times higher

Requires more chip area

- 5 times larger

Die photo of secure AES chip



Answers

- Will every passive RFID tag has security features in a few years?
  - Probably not, but many tags will have
- What are the difficulties in designing hardware for passive RFID tags?
  - Power consumption and chip area
- Which cryptographic algorithm should be used?
  - Challenge-response protocols with AES-128 (public-key crypto perhaps possible in a few years)
- Why does the RFID industry does not have products with strong crypto?
  - Too busy at the moment
- Are implementation attacks really a threat?
  - If it is worth the effort, yes
- Is this work theoretical research or has it practical relevance?
  - Yes, prototypes in real silicon show feasibility of strong crypto on passive RFID tags

Conclusions

Strong cryptography required for RFID systems

Design for low power consumption

Implementation of algorithms

- AES-128

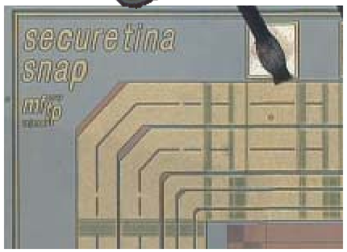
Implementation security

Contact information

- Martin Feldhofer
  IAIK – TU Graz
  Martin.Feldhofer@iaik.tugraz.at

Acknowledgements:

Johannes Wolkerstorfer
Thomas Popp
Michael Hutter
Stefan Tillich
Manfred Aigner
Christian Rechberger



4th Workshop on RFID Security

9th - 11th July 2008

Budapest, Hungary

Radio Frequency Identification

- Security
- Data Protection
- Applications
- Protocols
- Implementations
- Attacks

http://events.iaik.tugraz.at/RFIDSec08

Sponsored by:

Organized by: