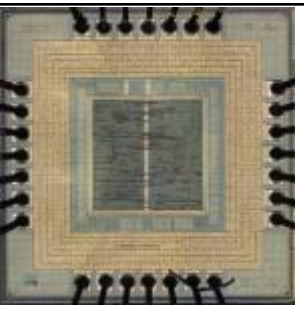
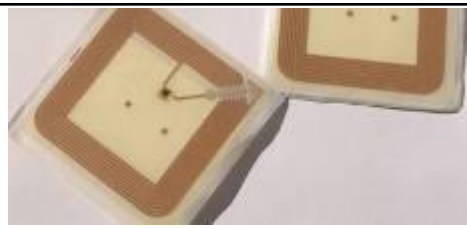


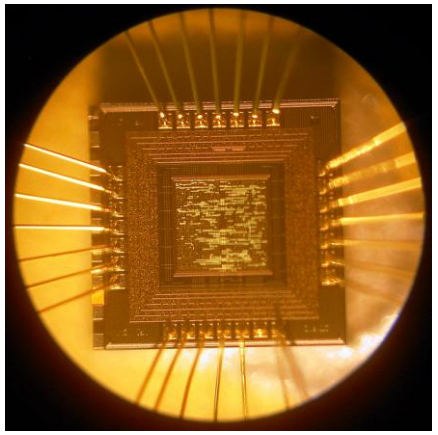


Strong Crypto for Tiny RFID Tags

Challenges and Design Issues

CONFERENCE ON RFID SECURITY 07

11-13 July 2007, Malaga, Spain



Martin Feldhofer

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

About us

IAIK TU Graz

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

Research groups

- Krypto 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

VLSI

RFID security research projects

"**Collaboration Rural**" – IP in FP6; IAIK performs research towards asymmetric crypto in RFID.

"**Building Radio frequency IDentification solutions for the Global Environment**" – IP in FP6; IAIK is task leader for secure RFID tags – deals symmetric security in UHF technology (SCA attacks for attacks on UHF technology)

Local initiative (sponsored by NXP) to support research and education @ TU Graz

FIT-IT: Secure NFC Applications (national cooperation with NXP)

Outline

Motivation

Requirements for RFID hardware

Low-power design strategies

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 not implement security mechanisms now?
- Are implementation attacks really a threat?
- Is this work theoretical research or has it practical relevance?

RFIDSec02 to RFIDSec07

Changing view on RFID security

- Sarma in 2002: first paper about RFID security at CHES 2002
- Sarma in 2003: "…standard crypto too costly on tags…", "…AES requires 20,000-30,000 gates…"
- Weis in 2003: "… strong crypto is not a realistic option …"
- Weis in 2003: "… only one-way hash function is required…"
- Juels in 2003: "…strong crypto on tags not possible…"
- Molnar in 2004: "… symmetric encryption, hash functions, or PRNGS are not possible on tags …"
- IAIK in 2004: "… AES possible on passive tags…"
- IAIK in 2006: "… AES much more suitable as hash functions …"
- RFIDSec06: proposals for ECC on tags
- Juels in 2007: "… integrate strong authentication into EPC standard …"
- RFIDSec07: many interesting proposals (GPS, …)

Why security for RFID systems?

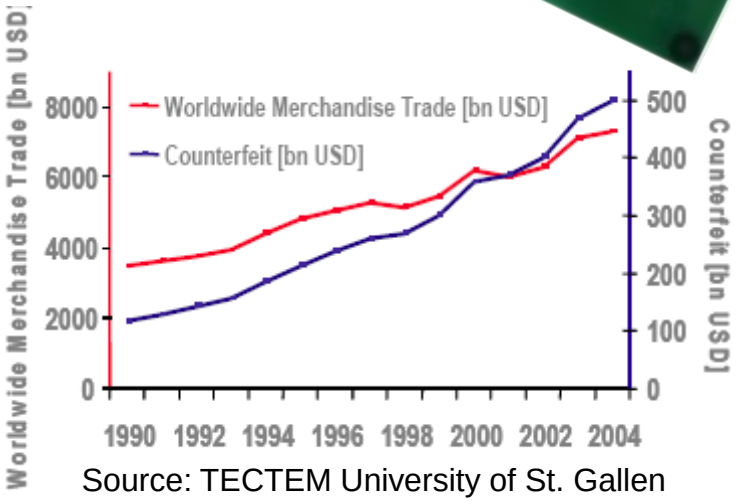
Counterfeiting

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



Source: TECTEM University of St. Gallen

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

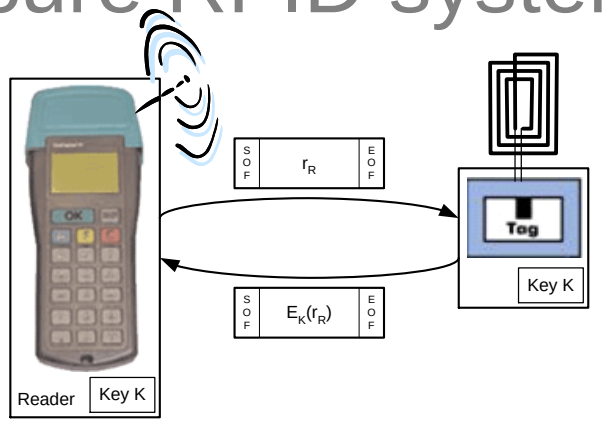
Activity tracking of persons via UID

Leakage of personal belongings data

Data protection is often referred to as showstopper ➔ user acceptance is important

➔ It is useful to integrate security into RFID systems

Requirements for a secure RFID system



Security protocol

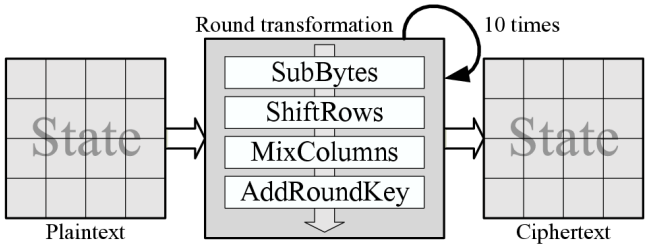
- Challenge-response authentication

Strong cryptography

- Appropriate key size (128 bits)

Cryptographic primitive

- Hash function, block cipher, universal hash function, public key algorithm
- "Lightweight" solution (HB, …)



Standardized algorithm

- Analyzed by many crypto experts (see DST)
- AES, SHA-1, SHA-256, MD5, Trivium, Grain

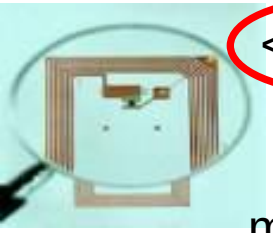
Goals: authentication and/or anonymity

What about the implementation costs of an RFID tag?

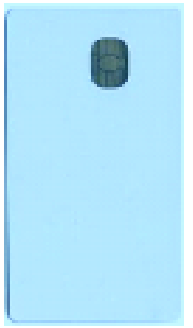
RFID tag vs. contact-less smart card

Common properties

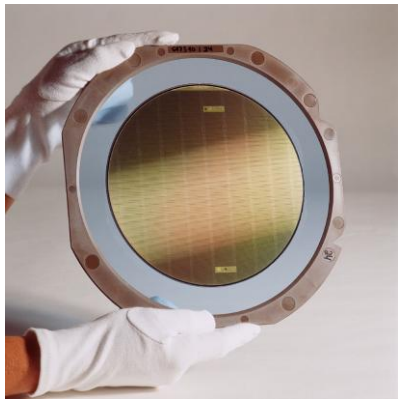
- Passively powered (no active power supply)
- Communication over air interface



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



Limitations of crypto hardware on passive tags



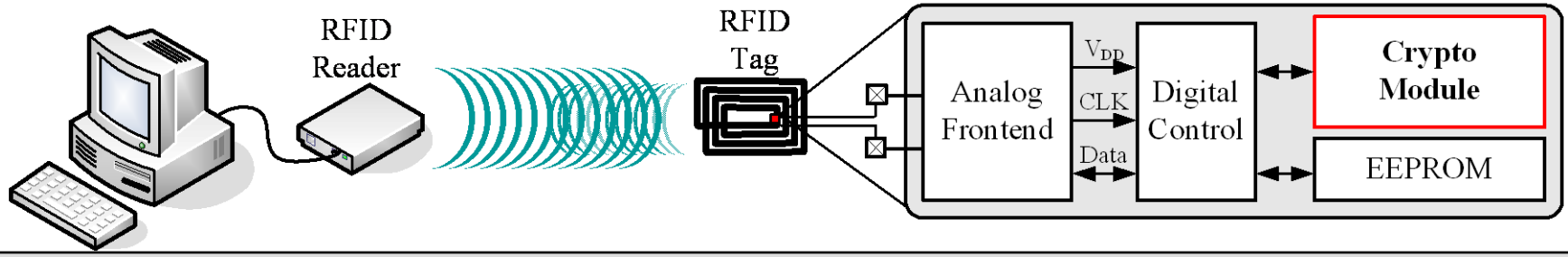
Chip area ~0.33 mm²

- 0.35 µm CMOS: 6,000 GE
- 0.18 µm CMOS: 25,000 GE
- Die size is proportional to silicon costs

Power consumption ~25 µW

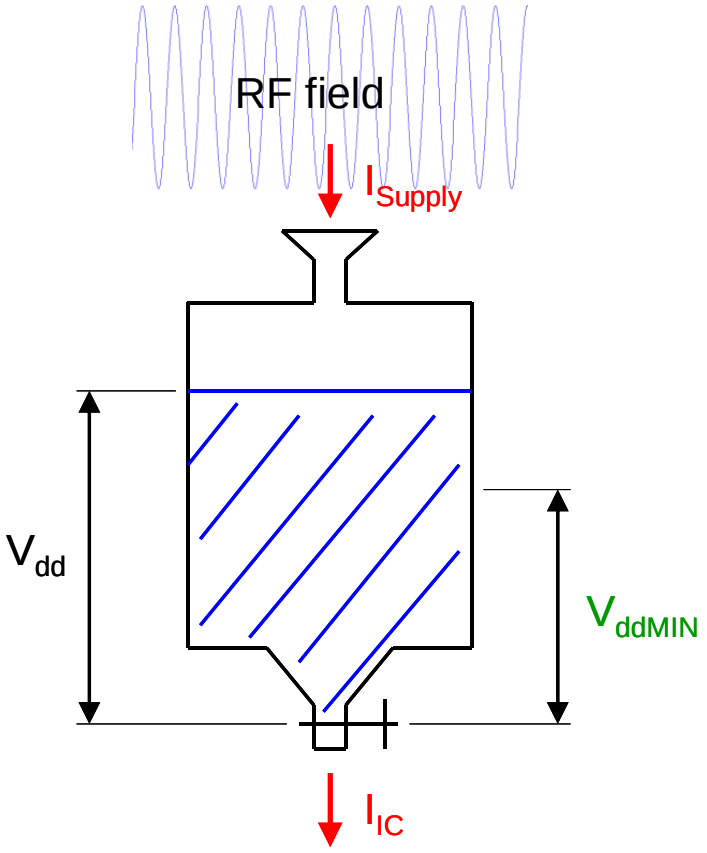
- Supply voltage ~ 1.5 V
- Mean current I_{avg} < 15 µA
- 0.35 µm CMOS: ~15 D-FF @ 1MHz
- Determines operating range

Conditions for a HF class-2 tag



Optimization goals

Low die-size optimization



Optimization metric

- (Area, Delay, Power)
  - Silicon area
  - Mean power
    - or mean current Iavg
  - Clock cycles
    - instead Tmin = #cycles / fmax

Low-power optimization

- Relevant for RFID tags
  - Energy consumption per cycle
  - Mean current consumption must not exceed available energy in capacitor
- Not relevant for RFID tags
  - Energy consumption per operation
  - Power consumption per operation (encryption)

Optimization techniques – Algorithmic level

Focus on standardized challenge-response protocols

Focus on standardized algorithms

Types of algorithms

- Symmetric encryption
- Hash algorithms
- Keyed hashes
- Asymmetric algorithms

Not analyzed

- Obviously too demanding algorithms
  - RSA
- Doubtable algorithms
  - NTRU, XTR
- Not yet: GPS, RSA variants

Selected algorithms

- Block cipher
  - AES-128
  - TEA, XTEA
- Stream cipher
  - Trivium
  - Grain
- Hash
  - MD5
  - SHA-1
  - SHA-256
- Asymmetric
  - ECC-192

Optimization techniques – Architecture level

Trade small size for speed

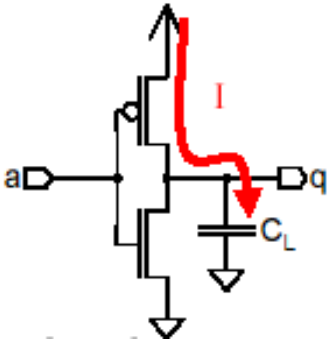
- Word width reduction
- Latency of reply
- Serialize operations (use clock cycles)

Example of LFSR

Optimization techniques – Circuit level

$P_{Total} = P_{Static} + P_{SC} + P_{Dynamic}$

- $P_{Dynamic} = C_L \cdot V_{DD}^2 \cdot f$



Lowering V_{DD}

- Limited by used technology (1.5V @ 0.35µm)

Use lowest possible clock frequency (<100 kHz)

- Limited by data rate (protocol)

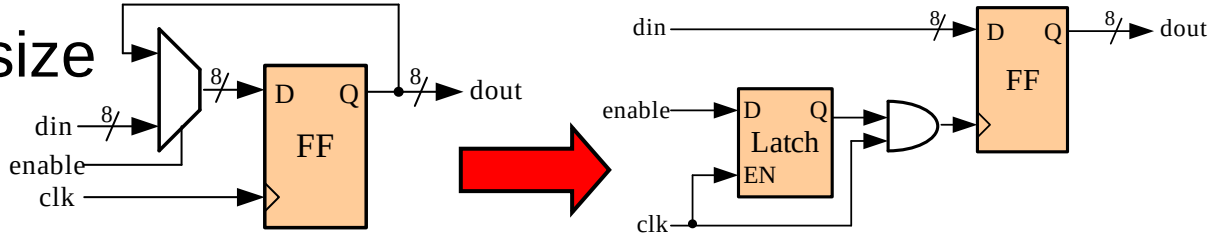
Avoiding glitching activity

- Clock gating
- Sleep-mode logic

Optimizations on circuit level

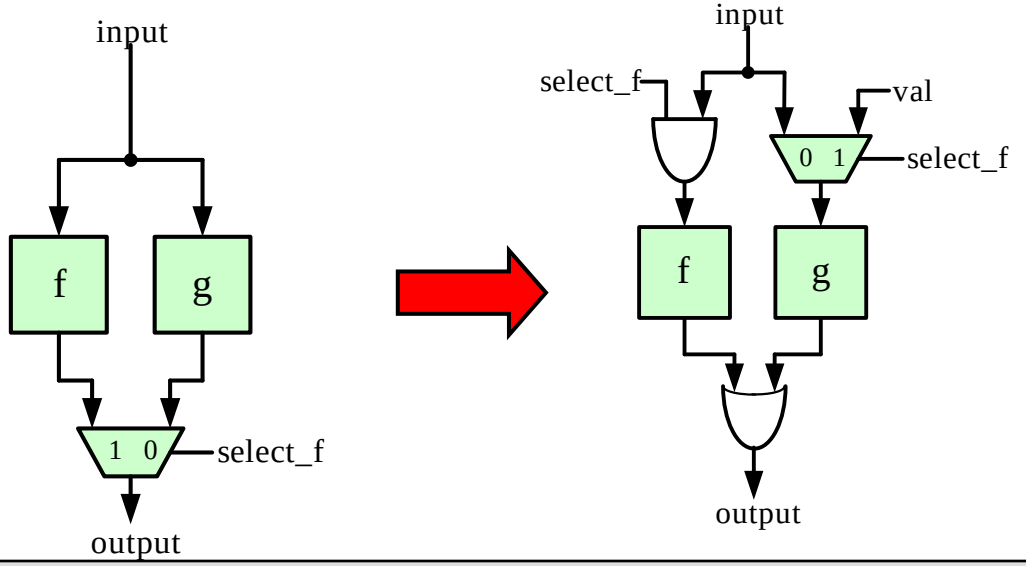
Clock gating

- Reduces activity
- Lowers circuit size



Sleep logic

- Not selected path consumes power
- Input gates block signal changes



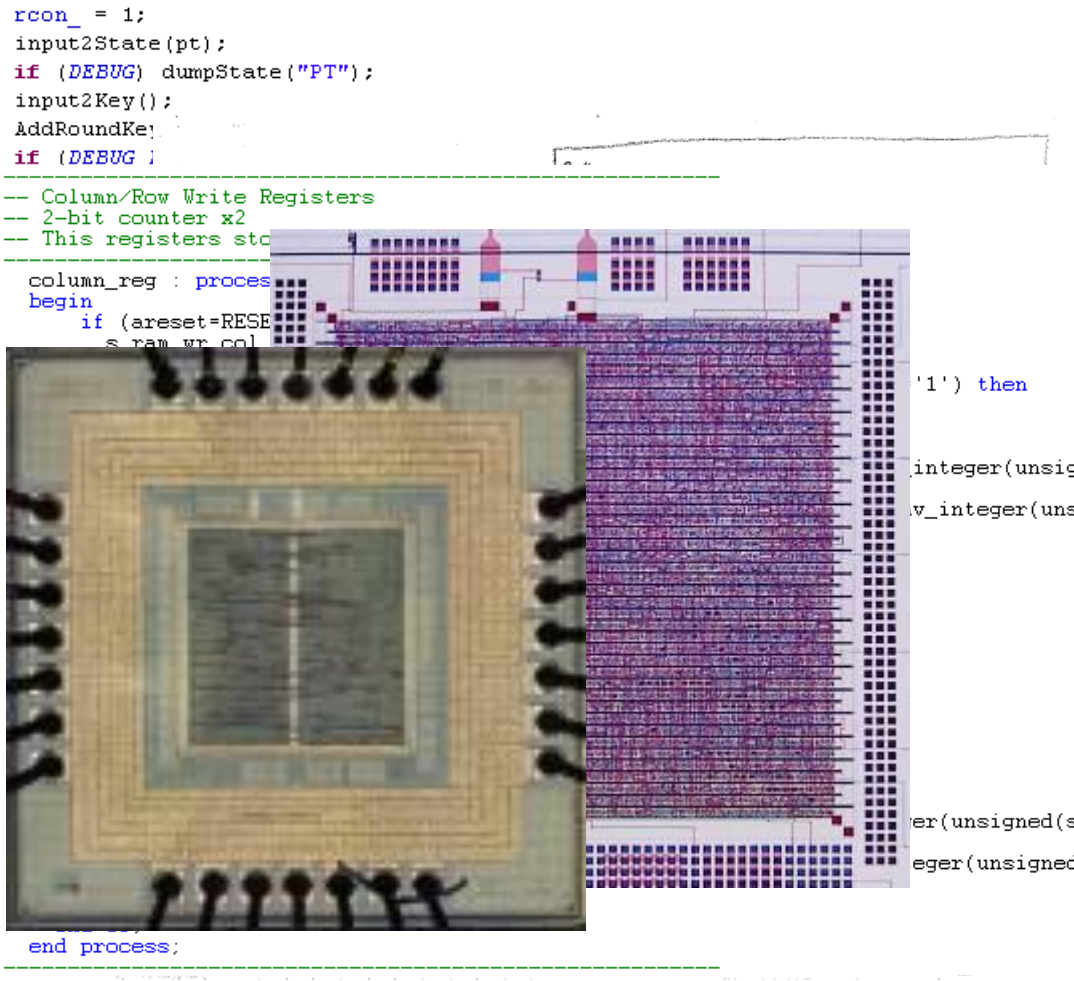
Optimum word width for clock gating

- Current consumption is at first glance proportional to number of clocked flip flops and latches
  - $I_{mean} \sim N/b + b$

    N…# flip flops in algorithm b…word width
- Minimization gives optimal data path word width
  - $b_{optimal} = \sqrt{N}$
    - $N_{AES} = 256$ ➔ $b_{opt} = 16$
    - $N_{SHA\text{-}1} = 832$ ➔ $b_{opt} = 28.8$
    - $N_{SHA\text{-}256} = 1024$ ➔ $b_{opt} = 32$
    - $N_{Trivium} = 288$ ➔ $b_{opt} = 17$
    - $N_{Grain} = 160$ ➔ $b_{opt} = 12.6$

Semi-custom design flow

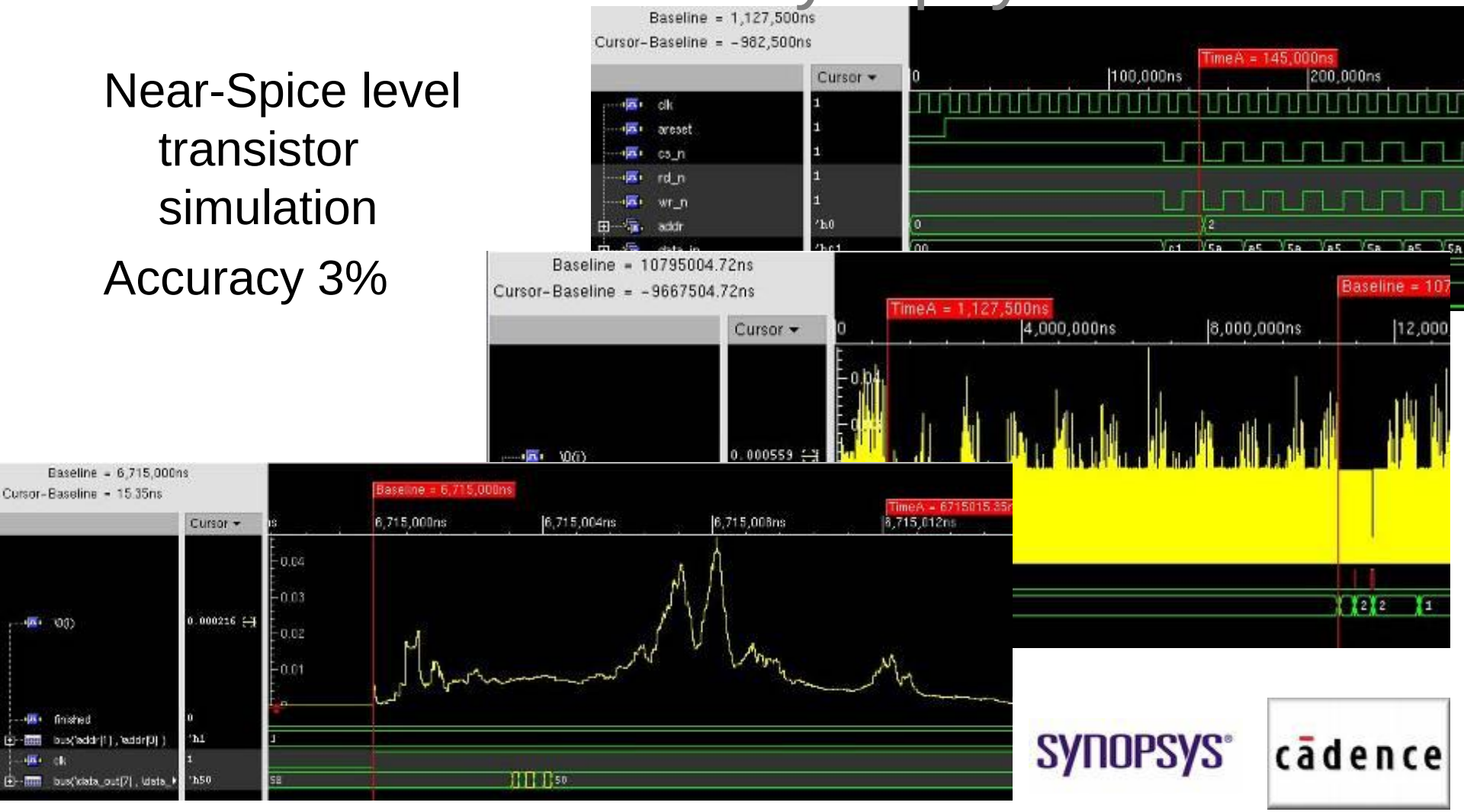
- Java Model
- HDL Code
- Synthesis
- Place & route
- Backend verification
- Fabrication



Power simulation – Synopsys Nanosim

Near-Spice level transistor simulation

Accuracy 3%



SYNOPSYS®

cadence

Survey of implemented algorithms

Block cipher

- AES-128
- TEA
- XTEA

Hash algorithm

- SHA-1
- SHA-256
- MD5

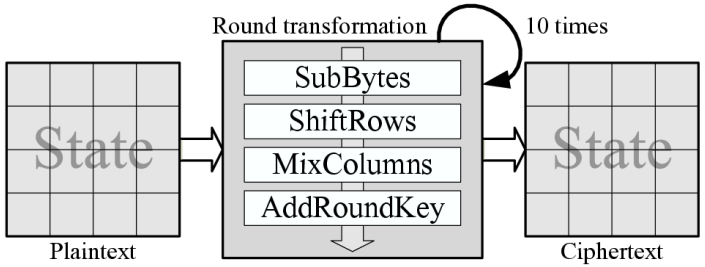
Stream cipher

- Trivium
- Grain

Public key algorithm

- ECC

AES-128



Features

- Encryption and decryption
- Round-key generation included

Architecture

- 8-bit datapath
  - 1 S-box
  - ¼ MixColumns
- 256 bit storage: RAM
  - 32 x 8-bit organization

Silicon implementation

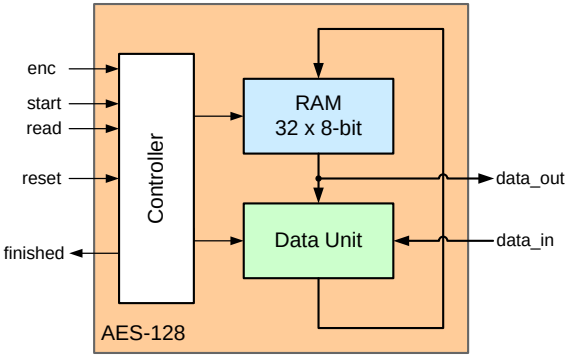
- On 0.35 µm CMOS
- Proven suitability for RFID
  - 0,25 mm²
  - 3 µA @ 1.5 V, 106 kHz

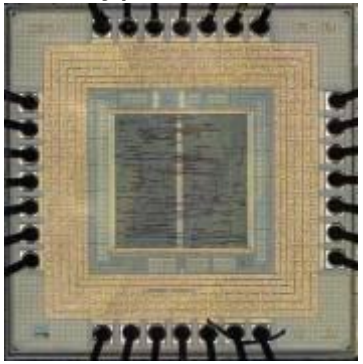
Balance

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

Difficulties

- Area*delay metric rather bad
  - ~1000 cycles per encryption





„Tina“: Tiny AES

Comparison of implementations

Algorithm	Chip area [GEs]	I_{mean} [µA @ 100kHz, 1.5V]	# Clock cycles
AES-128	3,400	3.0	1,032

Hash algorithms

Algorithms

- SHA-256, SHA-1, MD5

Architecture

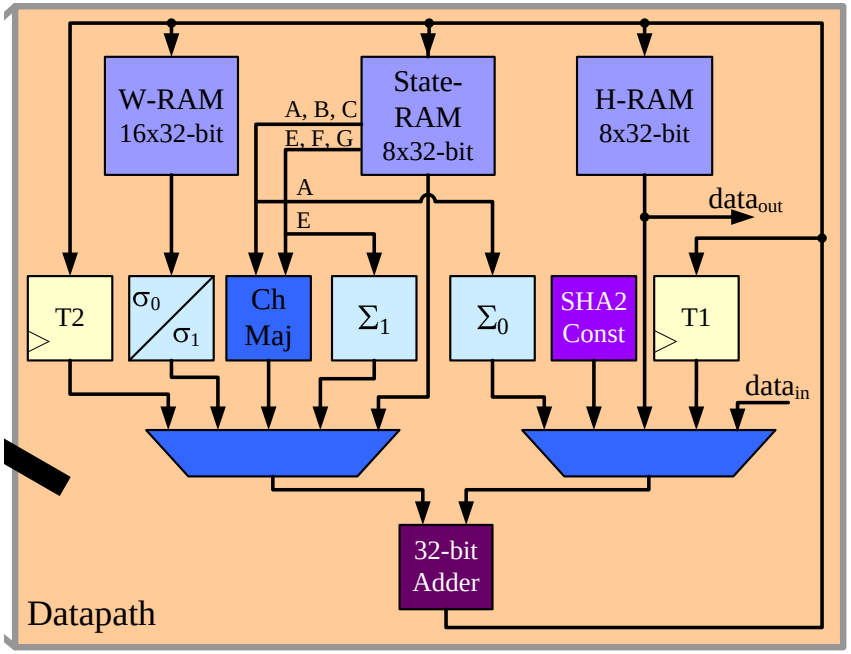
- 32-bit datapath
- Flip-flop based RAM
  - Msg expansion, state, chaining variables
- Tables as combinational logic

Goodies

- Clock gating of „RAM“
- No ROM for constants needed
- Sleep logic for datapath

Difficulties

- High HW complexity
  - Determined by storage effort
    - > 1024 bits

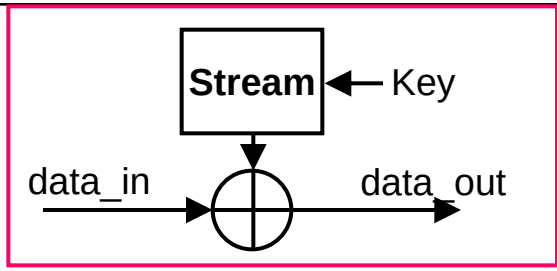


SHA-256 datapath

Comparison of implementations

Algorithm	Chip area [GEs]	I_{mean} [µA @ 100kHz, 1.5V]	# Clock cycles
AES-128	3,400	3.0	1,032
SHA-256	10,868	5.83	1,128
SHA-1	8,120	3.93	1,274
MD5	8,001	3.16	712

Stream ciphers



Algorithms

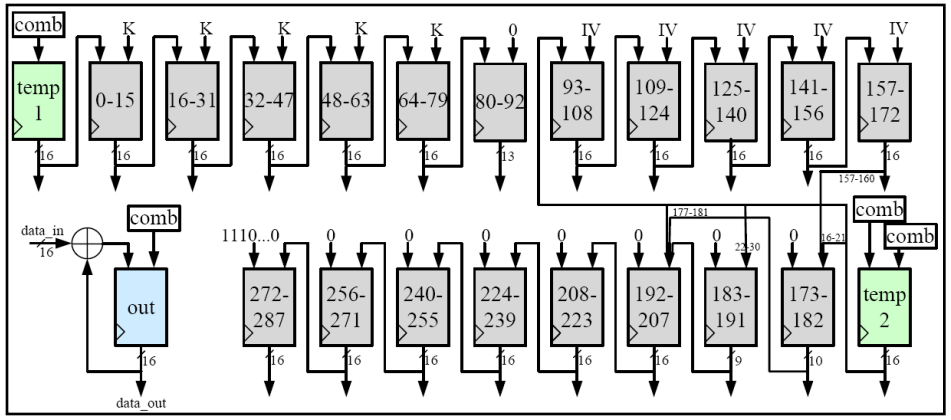
- Trivium, Grain

Architecture

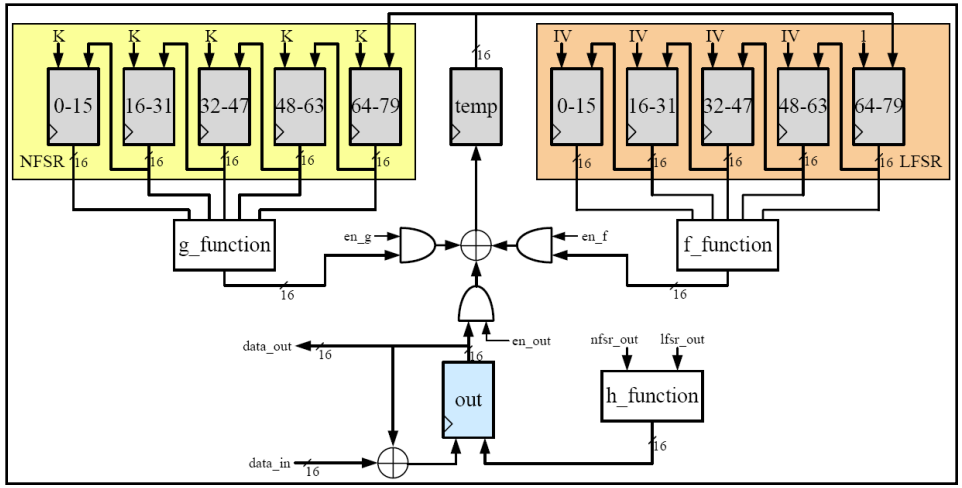
- 16-bit datapath
- Flip-flop based RAM

Goodies

- Distributed LFSR/NFSR
- Pipelined memory access to single 16-bit registers
- Sleep logic for datapath



Trivium datapath



Grain datapath

Comparison of implementations

Algorithm	Chip area [GEs]	I_{mean} [µA @ 100kHz, 1.5V]	# Clock cycles
AES-128	3,400	3.0	1,032
SHA-256	10,868	5.83	1,128
SHA-1	8,120	3.93	1,274
MD5	8,001	3.16	712
Trivium	3,090	0.68	(1,603) + 176
Grain	3,360	0.80	(130) + 104

Elliptic-Curve Cryptography

Algorithms

- ECC-192 (GF(p))

Architecture

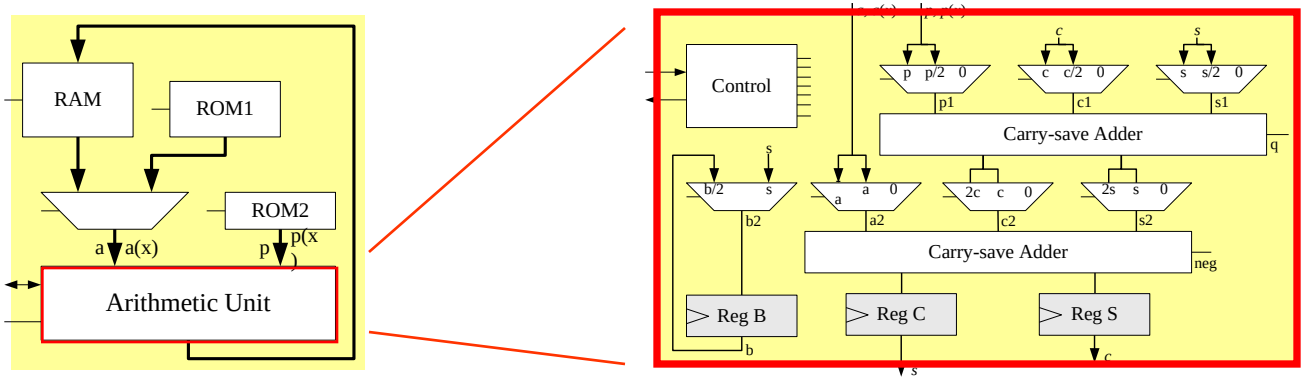
- Bit-serial multiplier
  - Redundant number representation
  - Dual-field capability
- RAM
  - Flip-flop based
  - 8 x 196-bit organization

Goodies

- Constants as combinational logic

Difficulties

- Control
  - Long: 500.000 clock cycles
  - Complicated
  - Requires hierarchical approach
    - State machine: field operations
    - Progr. control: point operations
- Circuit size: 23 kGE



Comparison of implementations

Algorithm	Chip area [GEs]	I_{mean} [µA @ 100kHz, 1.5V]	# Clock cycles
AES-128	3,400	3.0	1,032
SHA-256	10,868	5.83	1,128
SHA-1	8,120	3.93	1,274
MD5	8,001	3.16	712
Trivium	3,090	0.68	(1,603) + 176
Grain	3,360	0.80	(130) + 104
ECC-192	23,600	13.3	500,000
TEA	2,633	3.79	289

Comparison of algorithms

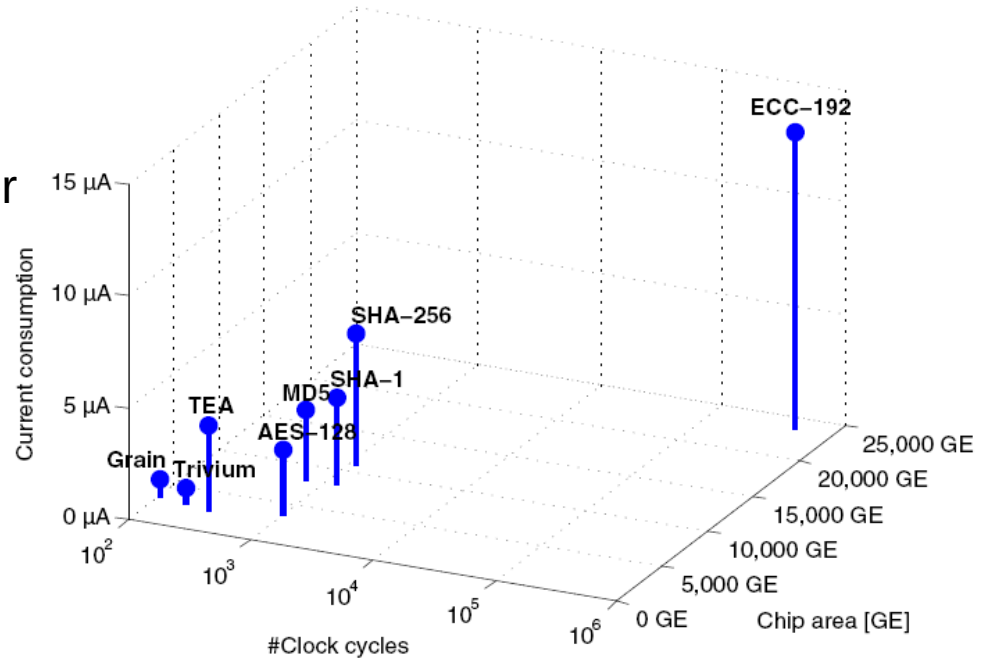
Comparison of hardware implementations

- Implemented on same platform
- Optimized using same methods

Result (128-bit crypto)

- AES-128 vs. SHA-256
  - A: AES 3-times smaller
  - A*t: AES 4-times better
  - A*t*P: AES 7-times better

Algorithm	Security [bits]	I_{mean} [μA@100kHz]	Chip area [GE]	Clock [cycles]
SHA-256	128	5.86	10,868	1,128
SHA-1	80	3.93	8,120	1,274
MD5	80	3.16	8,001	712
AES-128	128	3.0	3,400	1,032
ECC-192	96	18.85	23,600	502,000



Implementation security

Traditional attacks on security systems

- Cryptanalysis (mathematics) } Challenge-response protocol
- Strength of keys and algorithms } AES-128

But weakest link in system decides about security

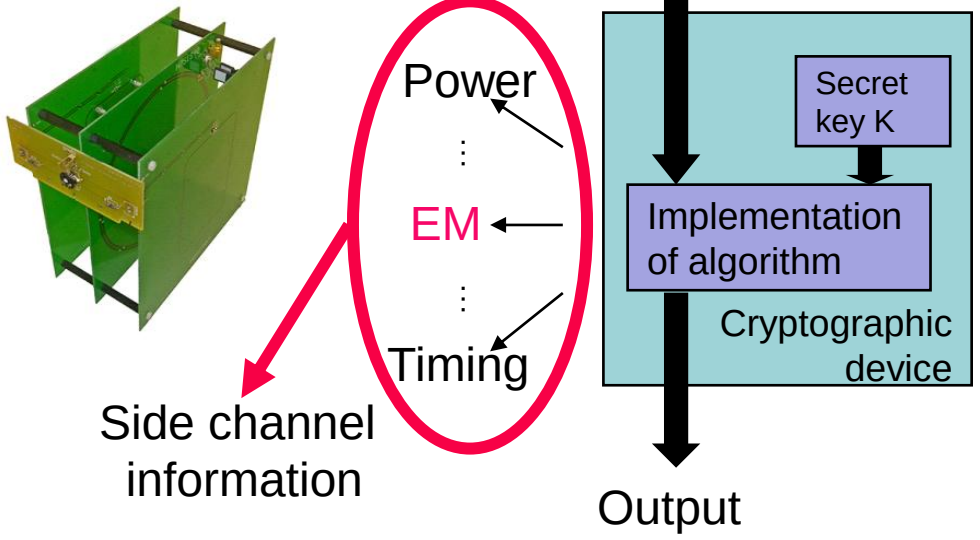
- Implementation security also very important

Active attacks

- Fault analysis
- Physical probing

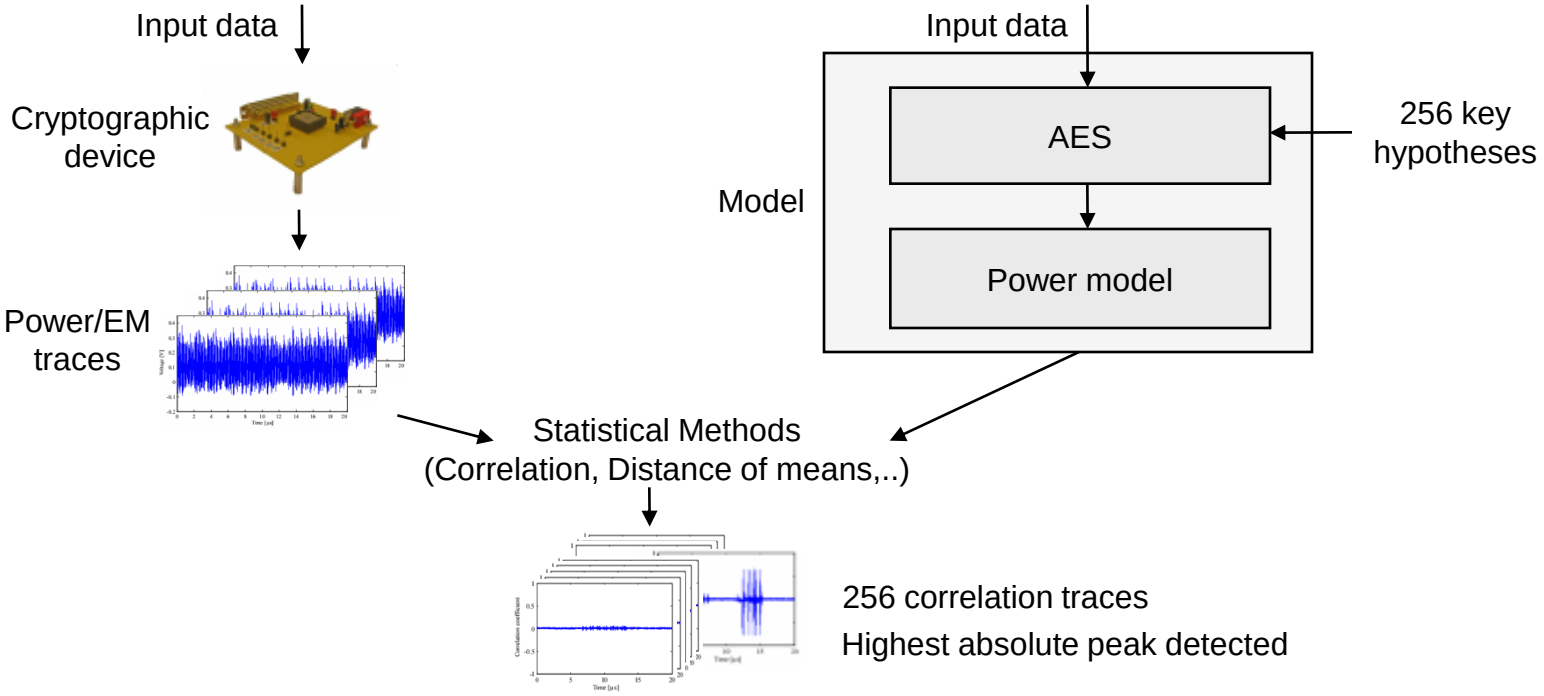
Passive attacks

- Side-channel analysis
  - Power consumption
  - Timing information
  - Electromagnetic radiation



Differential power/EM analysis

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



Challenges of SCA-secure AES implementation

Power consumption

- Determines operating range
- Below 15µA mean current consumption
- Target: max. 5 times higher

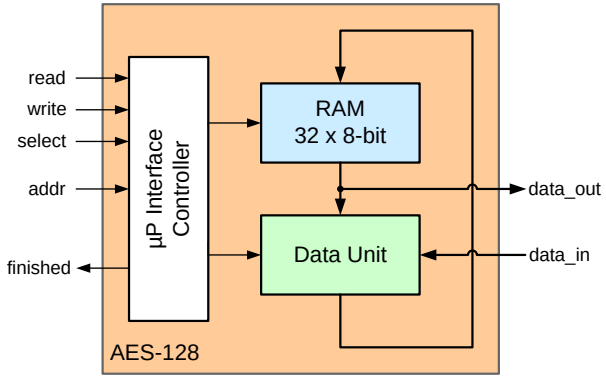
Chip area

- Die size equals silicon costs
- Less than 20,000 gate equivalents
- Target: max. 5 times larger

BUT

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

Implementation bases on existing AES architecture



Implementation of countermeasures

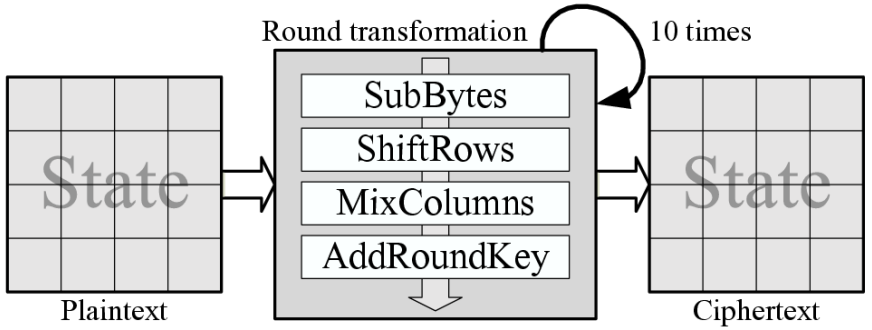
„The goal of countermeasures against SCA attacks is to make the power consumption of the device independent of the intermediate values of the executed algorithm.“ [Mangard, Oswald, Popp; Power Analysis Attacks – Revealing the Secrets of Smart Cards]

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

Randomizing the AES

AES algorithm



Shuffling of operations

a_{00}	a_{01}	a_{02}	a_{03}
a_{10}	a_{11}	a_{12}	a_{13}
a_{20}	a_{21}	a_{22}	a_{23}
a_{30}	a_{31}	a_{32}	a_{33}

Randomly choose a starting element (column & row)

New sequence:

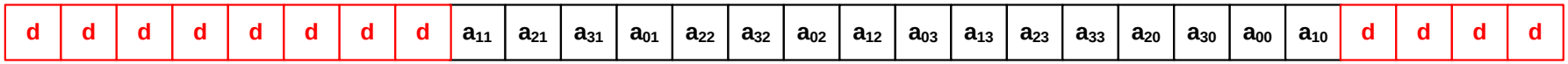
a_{11}	a_{21}	a_{31}	a_{01}	a_{22}	a_{32}	a_{02}	a_{12}	a_{03}	a_{13}	a_{23}	a_{33}	a_{20}	a_{30}	a_{00}	a_{10}

The probability that a certain element is processed at a certain point of time is now 1/16.

Increase randomization

Execution of dummy cycles

- Add a certain amount of dummy blocks randomly at the beginning and/or at the end



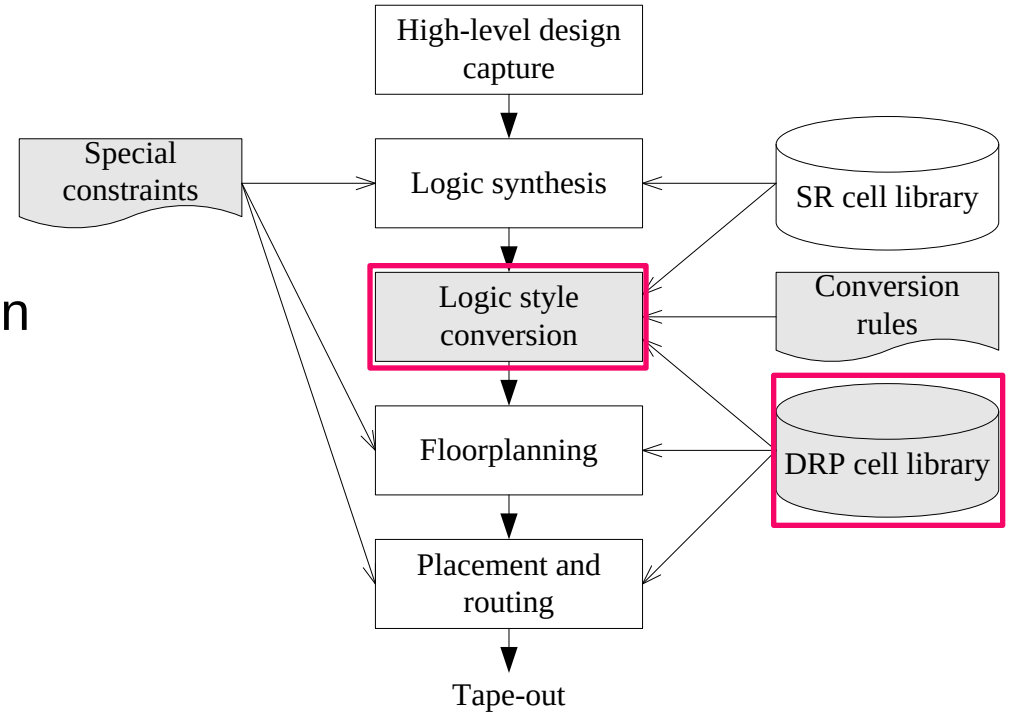
- Probability that a certain element occurs at a certain point of time is p = 1/(16 + n) (n … number of dummy cycles)
- e.g. n=12: probability that a certain element occurs at a certain point of time is 1/28

SCA-resistant logic style

Advantages of using logic styles

- Counteract leakage directly at the source
- Independent of circuit architecture
- Automatic implementation of secure circuits via a semi-custom design process is possible

Modified design flow



Answers

- Will every passive RFID tag has security features in a few years?
  - Hopefully, yes
- 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 not implement security mechanisms now?
  - 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
- SHA-1, SHA-256, MD5
- Trivium, Grain
- ECC
- TEA, XTEA

Implementation security is important aspect

➔ AES-128 is most suitable for passive RFID

Contact information

Martin Feldhofer
Institute for Applied Information Processing and Communications
TU Graz - Austria
Email: Martin.Feldhofer@iaik.tugraz.at

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






FIT-IT Project SNAP
sponsored by Austrian bm:vit
see www.fit-it.at