Crypto implementations for RFID tags

Learning from the smart card industry

Manfred Aigner

IAIK – Graz University of Technology

Topics

- About us @IAIK
- Motivation for standardized security on a tag
- Security requirements for RFID tags
- Limitations due to technology
- Hash vs. symmetric encryption
- Results so far (developed at IAIK)
- Future research topics
- Conclusions

About IAIK and PROACT

Graz University of Technology (Austria)
Faculty of Computer Science

- **Institute for Applied Information Processing … (IAIK)**
  - IT-Security from design of crypto algorithms via secure implementation and networks to eGovernment applications
- VLSI Group: 12 researchers dealing with crypto implementations in HW and related topics like ISE, SCA, HW/SW co-design, SOC design
  - Major activities at the moment: Crypto implementations for resource restricted environments (smart cards, RFIDs, emb. systems), ISE for crypto, side-channel analysis, SOC design, quantum cryptography
  - Strong interaction with other groups at IAIK (crypto, networks, e-government)
  - Current Projects: SCARD, SENSE, eCrypt, QCC, ISDPA, PROACT

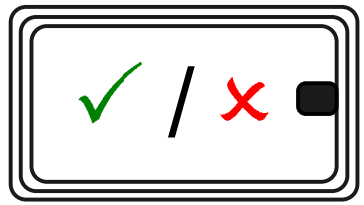
PROACT Programme for Advanced Contactless Technology

VLSI

Benefits from security on tags

Tag authentication:

- "Proof of origin":
  anti-cloning / anti-forgery
  of tags / products



Reader authentication:

- Privacy amplification for customer
- Integrity of data on tag (re-writeable tags)
- Authorized kill / selective kill
- Extended supply chain to the customer

Mutual authentication

- Anti eavesdropping of
  reader-tag communication by encrypted
  communication

Standardized crypto for RFID

Global applications call for standardized crypto algorithms
-> RFID is a global technology

Standardized algorithms are intensively approved by crypto community – probability of flaws is lower than for proprietary algorithms

Standardized protocols: Most systems are broken because of flaws in the protocol -> use established protocols instead of re-inventing the wheel

Some arguments against and for standardized algorithms

Known attacks can be applied easily by everyone if algorithms are public

- This does not take into account that developers of systems might also be attackers (later)

Especially side-channel analysis is/will be a problem for standard crypto on RFID. Knowledge for SCA on standard algorithms is public

- RFID tags are in the hand of attackers. SC attacks are also an issue on proprietary algorithms, as soon as some details about the algorithm / implementation are public

Custom built algorithms/protocols use less resources

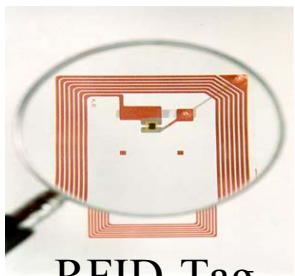
- … but they are potentially also less secure (be aware that you do not know future application of your tags, e.g. see broken ExxonMobile SpeedPass)
- Proper implementation of standardized algorithms allow integration into passive devices

Security requirements for "secure tags" @ IAIK

- No "lightweight" or "XOR-crypto". Security makes sense if state-of-the-art measures are applied
- Use standardized algorithms to allow exploitation on global market
- The high number of tags/objects, where each tag protects a small value, calls for high security level
- High number of tags needs clever key management
- No reduction of reading distance nor significant rises of costs/tag is acceptable
- Compatibility with installed infrastructure is necessary

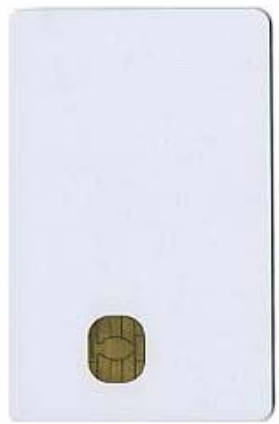
Limitations due to technology

- Limited power consumption (vs. energy consumption of battery powered devices) ~ 10µA average
- Area consumption limited (less problem with evolving SC technologies) < 1mm²
- Execution time (given by reader-tag protocol)
- Protocols: Communication is initiated by reader
- Very limited memory access (few kBytes and slow)
- No physical protection possible



RFID-Tag

~ 1m	**Reading range**	~ 10 cm
no	**Security**	high
minimal	**Price/tag**	some €
< 20µA	**Power cons.**	< 10mA
ISO 18000	**Standard**	ISO 14443



The fairy tale of inexpensive hash primitives

Publications about hash lock schemes argue that hash is cheaper to implement than encryption

- This is true for SW on 32-bit µC platforms, but not for optimized HW-implementations

Reason:

- SHA-1 input block = 512 bit (64 byte) input (before msg-schedule and 2560 (320byte) after)
- AES = 128 bit(data block) + 128 bit key + min. 1 S-Box

Comparison:

Algorithm	Implementation	CLB-Slices (XILINX Spartan)	Cycles
AES (enc & dec)	Tiny AES (IAIK-FPGA)	444	~ 1000
SHA-1	IAIK SHA-1 (IAIK-FPGA)	791 (*)	~ 250

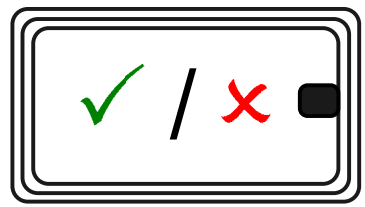
(*) 360 Slices only for msg schedule

Necessary enhancements for secure tags

System:

- Extended personalization / key upload to tag
- Key generation / management / distribution

Tag authentication



- Authentication command(s)
- Crypto primitive (e.g. AES enc) on tag
- Secure key storage on tag
- Crypto capability or online-access of reader (to access verification server)

Necessary enhancements for secure tags

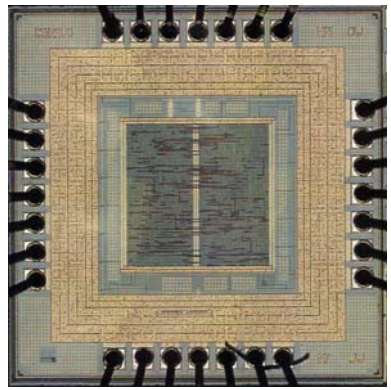
System:

- Extended personalization / key upload to tag
- Key generation / management / distribution

Reader Authentication

- Authentication commands
- Crypto primitive (e.g. AES enc) on tag
- Crypto capability of reader
- Secure key storage on tag and reader
- Nounce generation (RNG) on tag
  (fake ID generation)

Results so far @ IAIK



TinyAES (worldwide smallest AES):

- AES module enc/dec; 1000 cycles
- 4,5 µW (Philips 0.35µm, 100kHz)
- Available as IP module, tested/verified

Security Layer for ISO-18000 (using AES)

- Anti-Cloning
- Privacy enhancement
- Tested with reader/tag prototypes

ECCU – An ECC module for passive wireless devices

- Available as IP module

ECCU
Elliptic Curve Crypto Unit

Future research

- Key management / personalization
- Testability of crypto tags
- SCA secure AES module
- Nounce generation
- Application/middleware development
- Asymmetric crypto for RFID (ecc)

Conclusions

- Standardized crypto (algorithm and protocol) is necessary for open applications to avoid security flaws
- Protection against implementation attacks (like SCA) will be necessary also for many applications with inexpensive RFID tags
- Implementation of standardized crypto (AES, ecc) is possible on passive tags without reduction of operation range
- More research is necessary to allow easy and secure integration into applications

Bibliography

•Martin Feldhofer, Johannes Wolkerstorfer, Vincent Rijmen; **"AES Implementation on a Grain of Sand"**, IEE Proceedings on Information Security, Volume 152, Issue 1, pp. 13–20, October 2005.

•J. Wolkerstorfer, **"Is Elliptic-Curve Cryptography Suitable to Secure RFID Tags?"**, Workshop on RFID and Light-weight Cryptography, Graz- August 2005

•Martin Feldhofer, Johannes Wolkerstorfer:**"Low-power Design Methodologies for an AES Implementation in RFID Systems"**, ECRYPT Workshop on Cryptographic Advances in Secure Hardware CRASH 2005, Leuven, Belgium, September 6-7, 2005.

•Martin Feldhofer, Manfred Aigner, Sandra Dominikus; **"An Application of RFID Tags using Secure Symmetric Authentication"**, in Proceedings of 1st International Workshop on Privacy and Trust in Pervasive and Ubiquitous Computing - SecPerU 2005, in conjunction with IEEE ICPS'2005, pp. 43–49, ISBN 960-531-179-8, Santorini Island, Greece, July 14, 2005.

•Sandra Dominikus, Elisabeth Oswald, Martin Feldhofer: **"Symmetric Authentication for RFID Systems in Practice"**, ECRYPT Workshop on RFID and Lightweight Crypto, Graz, Austria, July 14-15, 2005.

•Manfred Aigner, Martin Feldhofer: **"Secure Symmetric Authentication for RFID Tags"**, Telecommunication and Mobile Computing TCMC2005 Workshop, Graz, Austria, March 8-9, 2005.

•M. Feldhofer, S. Dominikus, J. Wolkerstorfer: **"Strong Authentication for RFID Systems using the AES Algorithm"**, will be presented on the CHES conference held on August 11-13 2004 in Boston

•M. Feldhofer: **"A Proposal for an Authentication Protocol in a Security Layer for RFID Smart Tags"**, MELECON conference held on May 1 - 5 2004 in DubrovnikPROACT Webpage

PROACT Programme for Advanced Contactless Technology

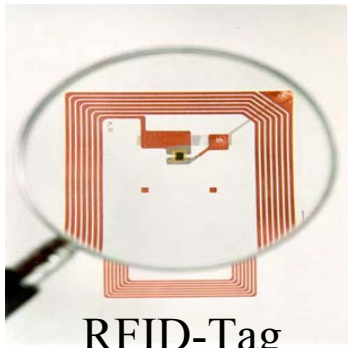
An initiative of Philips together with Graz University of Technology

VLSI

About IAIK and PROACT

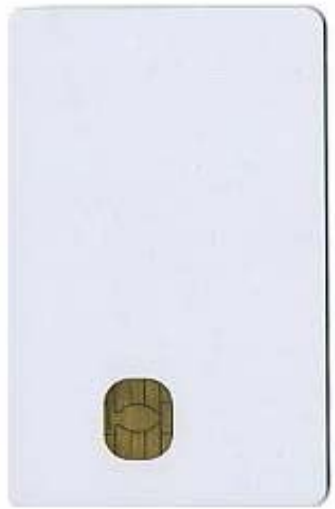
- Philips (Graz / Gratkorn is the RFID competence center of Philips) and Graz University of Technology
- Intensify teaching and research of RFID related topics
- At the moment six institutes of two faculties involved – lead for first term at IAIK
- Core topics of first term
  - RFID and security (security layers for RFID protocols, secure implementation)
  - Compliance testing

RFID Tags vs. smart card (contact-less)



RFID-Tag

~ 1m	**Reading range**	~ 10 cm
no	**Security**	high
minimal	**Price/tag**	some €
< 20µA	**Power cons.**	< 10mA
ISO 18000	**Standard**	ISO 14443



Reasons for vulnerabilities

Working principles of RFID Technology

- Contact-less
- No clear line-of-sight
- Broadcast of signal

Perfect working conditions for attacker!

Security threats

Violation of privacy

- Consumer tracking
- Data protection
- Tracking of personal data

Unauthorized access to the tag's memory

Forgery of tags

Existing “countermeasures”

- Shielding using metal foils
- Protection of privacy
  - Destruction at point-of-sale
  - “Blocker tags”
- Memory protection
  - Write once, read many
  - Access through pass phrase
- XOR-“cryptography”

Cryptographic approach

Identification

- Claim to be have a certain identity (username)

Authentication

- Proof of identity
- Showing knowledge, possession, inherent feature

Authentication mechanisms (1)

Passwords (weak authentication)

- Userid + password
- Interactive
- Replay attack

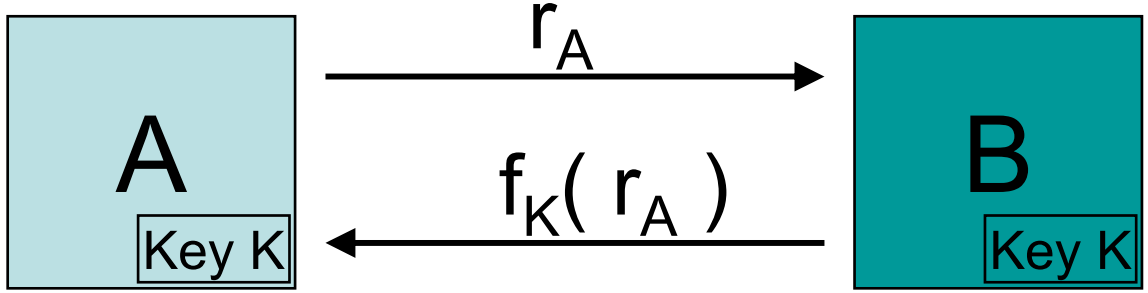
Zero-knowledge protocols

- Demonstrate knowledge of secret without revealing information about it
- Iterative

Authentication mechanisms (2)

Challenge response (strong authentication)

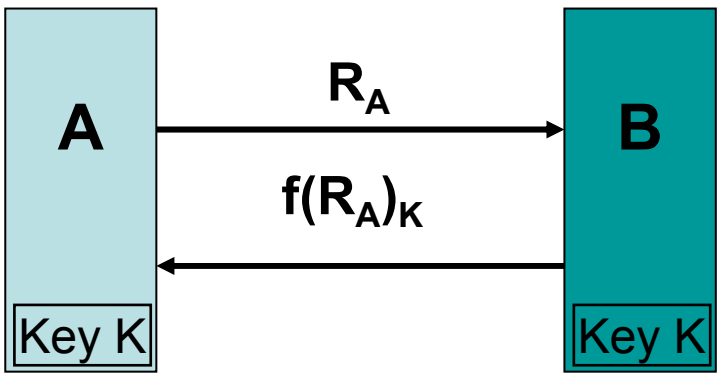
- Knowledge of a secret
- Time-variant challenge
- Response depends on challenge and secret



Challenge-response authentication (1)

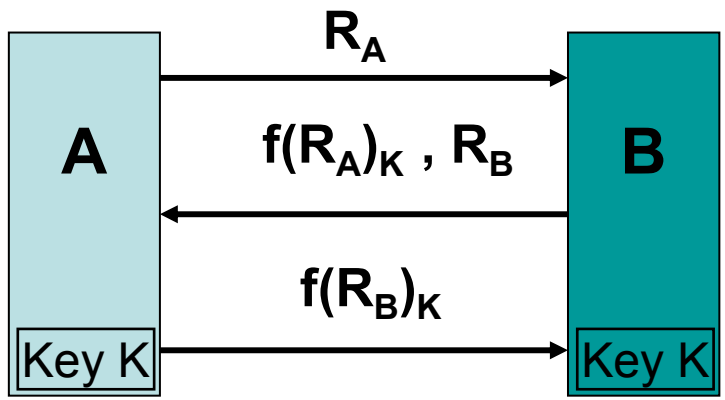
Unilateral

- Authentication of tag
  - Forgery
- Authentication of reader
  - Privacy
- Two pass



Mutual

- Forgery and privacy
- Three pass



Challenge-response authentication (2)

Symmetric

- Same key at both entities $K_A=K_B$
- Key distribution problem
- Key management difficulties
- Fast and efficient
- Closed systems (offline)

Asymmetric

- Public key and private key $K_A \neq K_B$
- Certificate management
- Slow and complex
- Open systems (online certificates)
- Tag-only authentication

Requirements for security-enhanced tag (ART Project)

Security level

- No “pseudo securitiy” → strong cryptographic primitives
- Standardized symmetric algorithm (AES)
- Standardized crypto protocol

Protocol

- Prevent forgery
- Supply of privacy
- Useable with existing infrastructure → compatibility to existing standards
  - ISO/IEC 18000

Encryption algorithm

Advanced Encryption Standard (AES)

- Symmetric block cipher algorithm
- 128-bit data blocks

128-bit key length

10 rounds

Encryption-only is needed for authentication purpose

Hardware requirements (tag)

Minimal power consumption

- < 20 μA average

Low die-size

- < 1 mm^2

Low cost

- ~5 Cent vs. ~50 Cent

Maximum number of clock cycles for AES

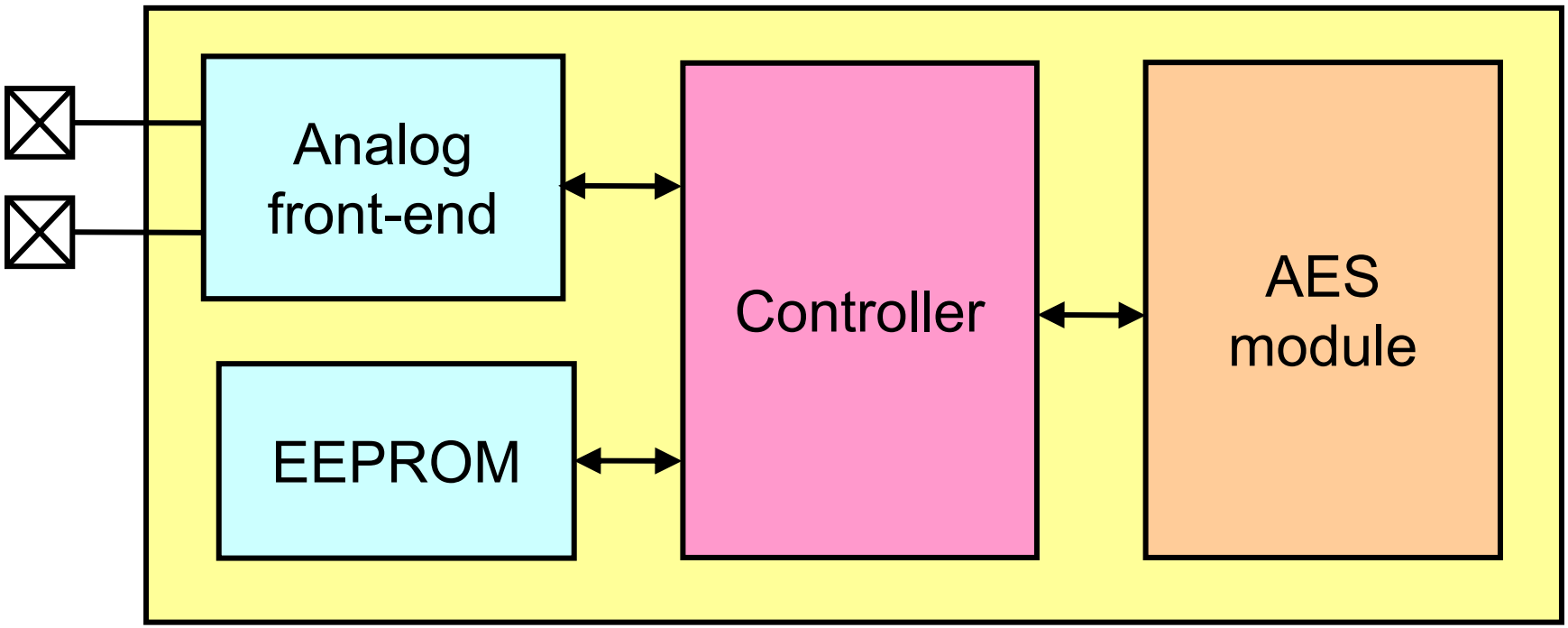
- ~1000 cycles @ 100 kHz

TINA- Tiny AES: The smallest AES implementation known

TINA results:

- Stand alone AES module with µP-interface
- AES-128 encryption and decryption
- On-the-fly Roundkey computation
- Consumption: < 4.5 µW (Philips 0.35µm, 100kHz)
- Area: < 0,25 mm²

Architecture of an RFID tag - “Secure embedded system”



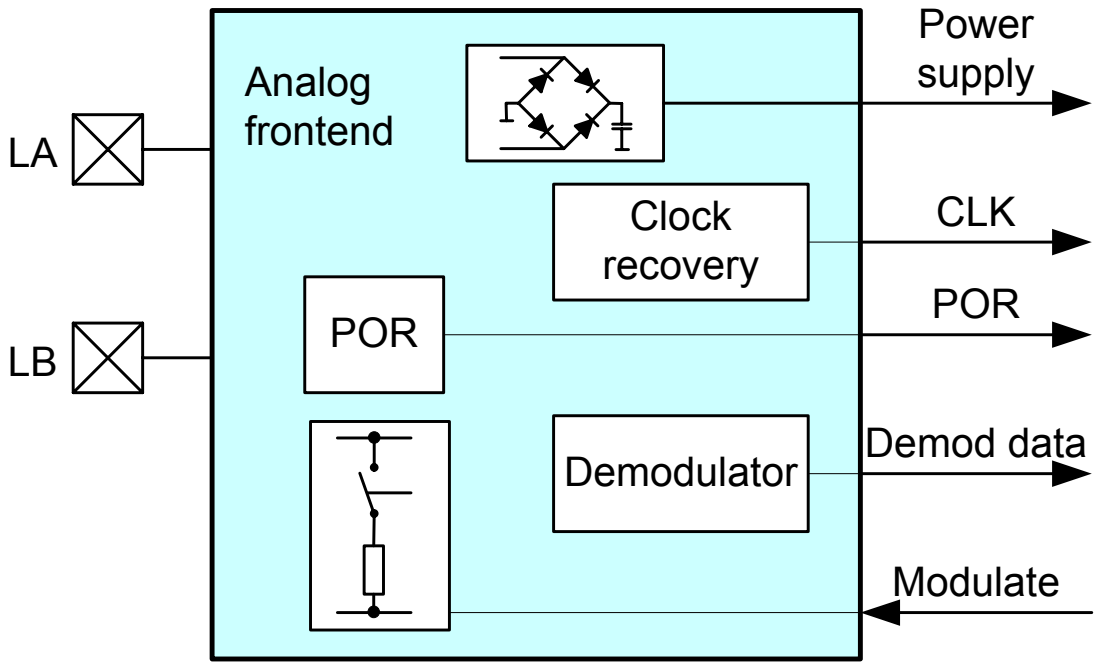
Analog frontend (Philips)

Power supply of tag

Frequency recovery for digital part of the tag

Power-on reset

Modulation/
demodulation
of data

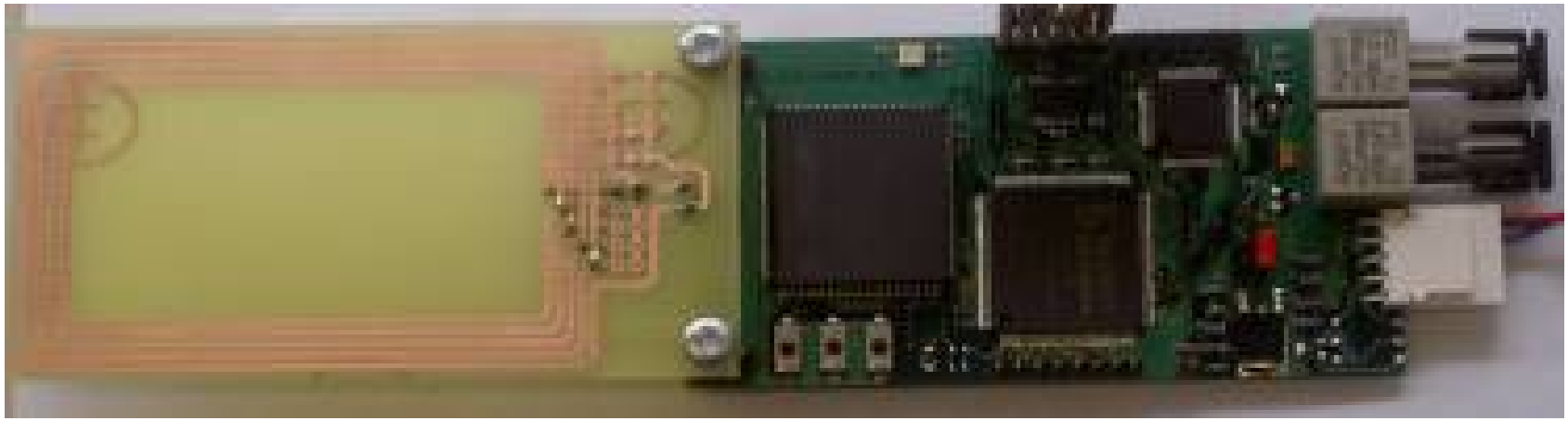


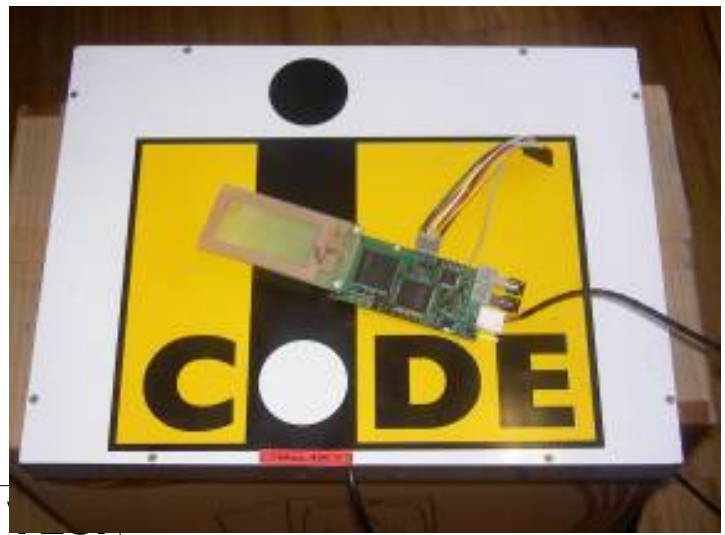
EEPROM

- Stores non-volatile data
  - UID
  - Secret key
- Programmed during personalization phase
- Protection
  - Unauthorized read
  - Tampering

Addr.	Data
0	UID[0]
1	UID[1]
…	…
128	KEY[15]

Crypto tag prototype using FPGA





- External power supply
- Interfaces for real-time observation during operation in the field
- Configurable digital parts
- Operates with standard reader

PETRA: Protocol emulation

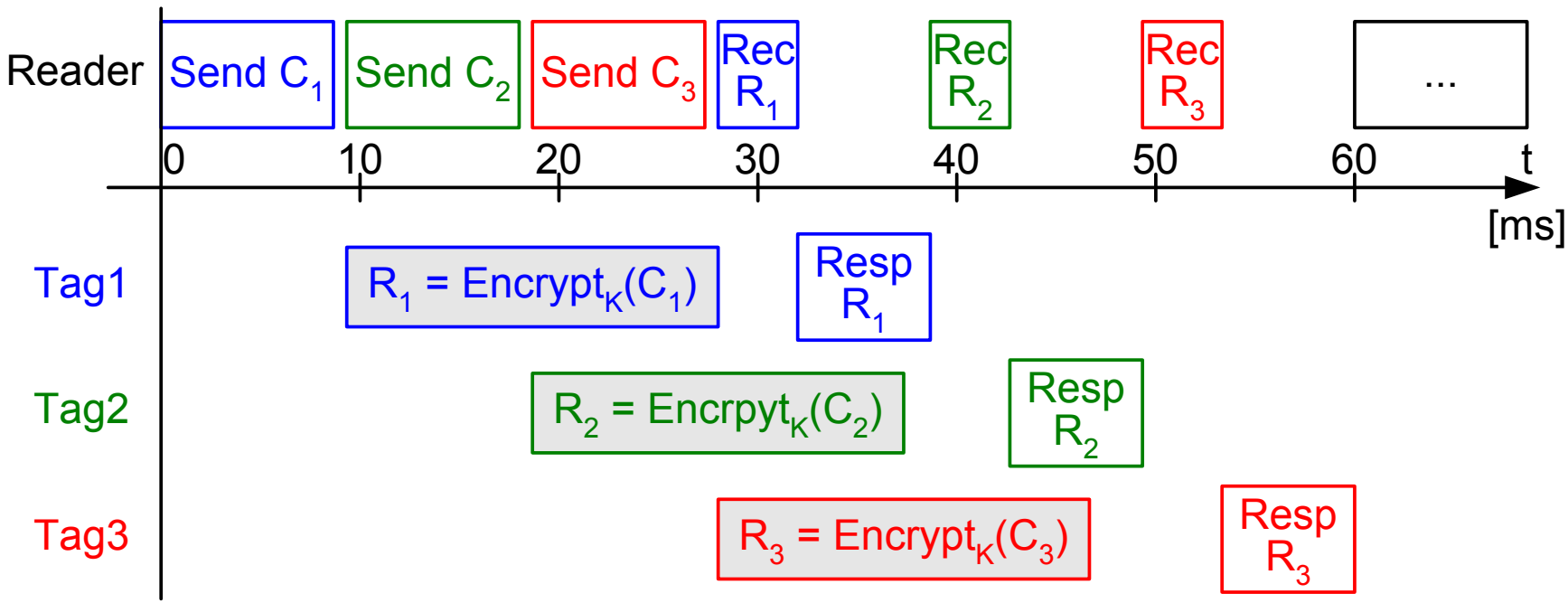
Protocol Evaluation Tool for RFID Application

Emulates arbitrary nr of tags in a cycle accurate manner

Allows to simulate e.g. protocol extensions and get “typical values”

Perfect tool for e.g. tests of different parameters for anti-collision in different applications

Interleaved protocol



Authentication of approx. 50 tags per second possible

Application: Secure Supply Chain for Pharmaceuticals

Benefits:

- Secure proof of origin during whole distribution chain
- Facilitated customs declaration
- Possible proof of origin by end-consumer possible without infringing user's privacy
- Secure return for disposal of drugs