CASSIDIAN
CYBERSECURITY

# A New Proposal for Lightweight Cryptography: LILLIPUT

Julien FRANCQ

July 1st 2014

# A New Proposal for Lightweight Cryptography: LILLIPUT

Julien FRANCQ

July 1st 2014

# RFID for Authentication

- Identification: only provides an identity (UID)
  - Logistic for non-safety critical products
  - Cheap
- Authentication: provides an identity and a proof
  - Access control, payment, ePassports, *etc.*
  - Cryptography (Challenge-Response Protocol (CRP))
  - More expensive

# Simple CRP Examples

- Unilateral authentication

$$\begin{aligned} &\text{Reader} \rightarrow \text{Tag} \quad C \\ &\text{Reader} \leftarrow \text{Tag} \quad R = E_K(C) \\ &\text{Reader} \rightarrow \text{Tag} \quad C' = D_K(R), \text{ if } C' = C \text{ then accept Tag} \end{aligned}$$

- Bilateral authentication

$$\begin{aligned} &\text{Reader} \rightarrow \text{Tag} \quad C_r \\ &\text{Reader} \leftarrow \text{Tag} \quad R_t = E_K(C_t, C_r) \\ &\text{Reader} \rightarrow \text{Tag} \quad R_r = E_K(C_r, C_t) \end{aligned}$$

- ISO 9798 : "*Entity Authentication – Mechanisms using...*"
  - -2 : "*...symmetric encipherment algorithms*",
  - -3 : "*...digital signatures*",
  - -4 : "*...cryptographic check function*"

# Metrics for Comparison

## Metrics

- Power consumption
- Area
- Computation time

# (Dynamic) Power Consumption

$$P_{\text{dyn}} = C_L.V_{dd}^2.f.N$$

- Low supply voltage $V_{dd} < 1V$
- Low clock frequency $f = k \times 100\ kHz$
- Low $C_L \Rightarrow$ Low gate count
- Low switching activity ($N$)

[1] P. Kitsos and Y. Zhang. "*RFID Security – Techniques, Protocols and System-on-Chip Design*". Springer, ISBN : 978-0-387-76480-1, p. 387.

# Available Power Budget for Crypto

- 2 kinds of RFID tags:
  - Actively powered (battery)
  - Passively powered (reader)
- Harsh contraints on the power consumption (power, energy)

| RFID System | Range | $P_{avg}$ | $I_{avg}$ |
|---|---|---|---|
| HF (13.56 MHz) | 1 m | 22.5 $\mu$W | 15 $\mu$A ($V_{dd} = 1.5$ V) |
| UHF (900 MHz) | 5 m | 4 $\mu$W | 4 $\mu$A ($V_{dd} = 1$ V) |

- Crypto. on UHF systems is much harder to realize than on HF systems

[2] P. Kitsos and Y. Zhang. "*RFID Security – Techniques, Protocols and System-on-Chip Design*". Springer, ISBN : 978-0-387-76480-1, Table 2 p. 384.

# Gate Equivalents

- Area in $\mu m^2$, dependent of the process technology
- $\Rightarrow$ *Gate Equivalents*, GE
- 1 GE = Area of a NAND2 gate
- Nb. of GEs = Area ($\mu m^2$)/Area of a NAND2
- Nb. of GE nearly independant of the technology $\Rightarrow$ Ease comparisons
- Ex. : UMCL18G212T3

| Gate | NOT | NAND | NOR | AND | OR | XOR | MUX | FF |
|---|---|---|---|---|---|---|---|---|
| GE | 0.67 | 1 | 1 | 1.33 | 1.33 | 2.67 | 2.33 | 5.33-12.33 |

# How much GEs for 5 Cents?


- 1-2 cents/5 for an overall circuit in CMOS 0.35 $\mu$m
- 4 cents/mm$^2$
- If half of the *layout* is related to the crypto $\Rightarrow$ 0.125-0.25 mm$^2$
- $\Rightarrow$ 2000-4000 GEs for the crypto
- Old estimation, but still considered today as a valid upper bound

[3] S. E. Sarma. "*Towards the 5 Cents Tag*". Technical Report MIT-AUTOID-WH-006. MIT, Auto-ID Center, 2001.

# Computation Time

- Time for anti-collision standardized
  - ISO/IEC 14443-3,4, 15693, 18000: $\sim$ 10-100 $\mu$s (anti-collision)
- Acceptable response time for ISO/IEC 14443-4: 100 ms max.
- Generally accepted: 1000 clock cycles at 100 kHz

# Security Level Adapted to RFID

- Applications require moderate level of security
- $\Rightarrow$ 80 bits
  - Adapted to short-term security
- 5 cents RFID tags will have difficulties to fight in a long-term against very powerful attackers

# Security Level Adapted to RFID

- Applications require moderate level of security
- $\Rightarrow$ 80 bits
  - Adapted to short-term security
- 5 cents RFID tags will have difficulties to fight in a long-term against very powerful attackers

# Generic Methods

- *Clock Gating*
  - Parts of circuit are virtually switched off when they are not in use
- Sleep Logic
  - Maintain constant inputs of useless outputs of combinatory parts
- Serial architectures
  - One part of a round is computed per clock cycle
  - Datapath width: $n$ bits $\rightarrow$ $w = n/k$ bits
  - Optimal: $w = \sqrt{n}$

# Standard Approach

- Implement standard algorithms whatever the cost

# Standard Approach

- Implement standard algorithms whatever the cost

# Dedicated Approach

- Implement modified standard algorithms

# Dedicated Approach

- Implement modified standard algorithms

# Exotic Approach

- Implement *ad hoc* algorithms

# Exotic Approach

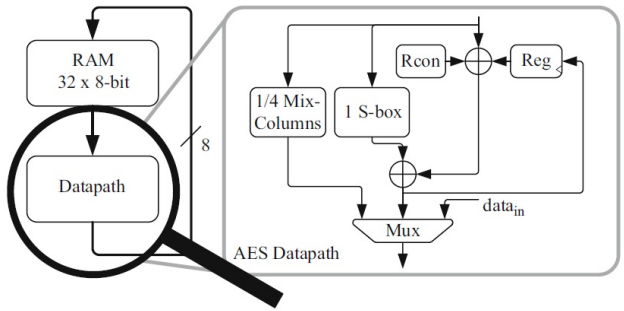
- Implement *ad hoc* algorithms

# Exotic Approach

- Implement *ad hoc* algorithms


# AES Module Architecture of [4]

- 8 bits architecture
- 3 components:
  - Controller (FSM): round execution, RAM addresses, control signals for the datapath
  - RAM (single port, flip-flops): 32 8-bit registers, *clock-gating* (only one byte clocked per clock cycle)
  - Datapath




[4] M. Feldhofer, S. Dominikus and J. Wolkerstorfer. "*Strong Authentication for RFID Systems Using the AES Algorithm*". CHES 2004, pp. 357-370.

# Implementation Results

- 3503 GEs, 3.0 $\mu$A, 100 kHz, 1.5V
- 1044 clock cycles
- RAM: main area and power consumption cost
- $\Rightarrow$ Can fit in RFID tags

| Module/component | $I_{mean}$ | | Chip area | |
|---|---|---|---|---|
| | (µA at 100 kHz) | (%) | (GE) | (%) |
| RAM | 1.55 | 51.7 | 2,065 | 58.9 |
| S-box | 0.4 | 13.3 | 345 | 9.8 |
| MixColumns | 0.25 | 8.3 | 350 | 10.0 |
| Register | 0.1 | 3.3 | 58 | 1.7 |
| Adder | 0.05 | 1.7 | 80 | 2.3 |
| Controller (FSM) | 0.55 | 18.3 | 490 | 14.0 |
| Others | 0.1 | 3.3 | 115 | 3.3 |
| *Total* | *3.0* | *100* | *3,503* | *100* |

# Benefits of *Low-Power* (LP) CMOS

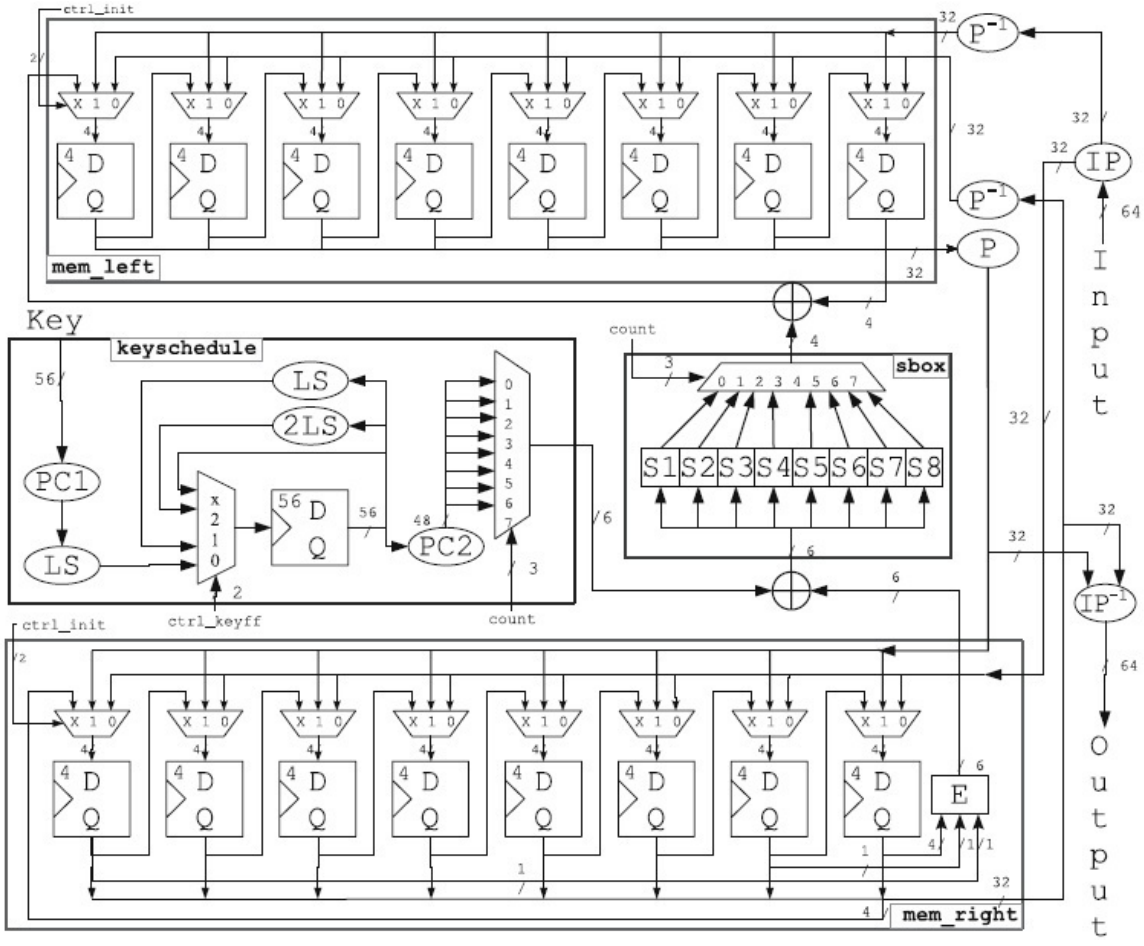
| AES | GEs | Techno. CMOS | Area ($mm^2$) | *Clock Cycles* | $V_{dd}$ (36 kbps) | Freq. (kHz) (36 kbps) | *Pow.* ($\mu$W) (36 kbps) |
|---|---|---|---|---|---|---|---|
| [5] | 3400 | 0.35 $\mu$m | 0.25 | 1032 | 0.65 | 290 | 2.45 |
| [6] | 5500 | 0.13 $\mu$m | 0.021 | 356 | 0.75 | 100 | 0.69 |
| [7] | 3500 | 65 nm LP | 0.018 | 1142 | 0.36 | 322 | 0.25 |


[5] M. Feldhofer, J. Wolkerstorfer and V. Rijmen. "*AES Implementation on a Grain of Sand*". IEEE Proc. Inf. Secur. 152(1), 13−20, 2005.
[6] T. Good and M. Benaissa. "*692 nW Advanced Encryption Standard (AES) on a 0,13 $\mu$m*". IEEE Transactions on VLSI Systems (99), 1 (2009).
[7] C. Hocquet, D. Kamel, F. Regazzoni, J.-D. Legat, D. Flandre, D. Bol and F.-X. Standaert. "*Harvesting the potential of nano-CMOS for Lightweight Cryptography: an Ultra-Low-Voltage 65 nm AES Coprocessor for Passive RFID Tags*". J. Cryptogr. Eng. (2011), 1, 79−86.

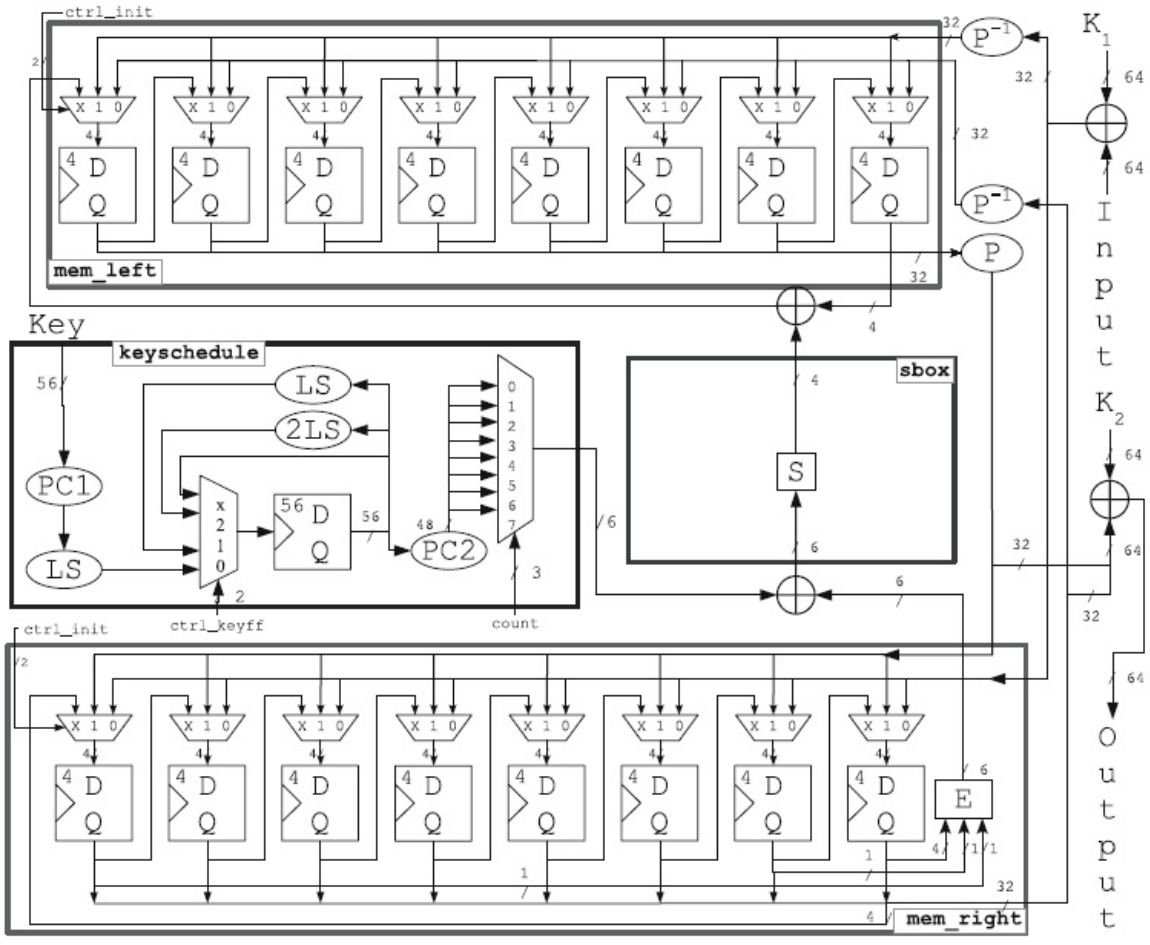
# DES, DESX, DESL, DESXL

- DES designed with hardware efficiency in mind
- Block size: 64 bits, key size: 56 bits.
- Key length of DES limits its usefulness in many applications
- DESX proposed by Rivest : $\mathrm{DESX}_{k\|k_1\|k_2}(M) = k_2 \oplus \mathrm{DES}_k(k_1 \oplus M)$, 184 bits key, overhead: 14%
- DESXL (resp. DESL) derived from DESX (resp. DES) but has 2 modifications:
  - IP et $\mathrm{IP}^{-1}$ are omitted
  - 8 SBoxes are replaced by only one, more lightweight, used 8 times
  - Greater resistance to differential/linear cryptanalysis than the original 8 SBoxes of DES

# Datapath of a Serial DES



# Datapath of a Serial DESXL



# Confusion/Diffusion

- Block cipher: confusion + diffusion
- Confusion
  - Non-linear layer
  - *S-Boxes*
  - Similar SBoxes executed in parallel
  - In hardware realized as Boolean functions
  - Generally 4-bit SBoxes
- Diffusion
  - Linear layer
  - Bit permutation (not so good diffusion, but very cheap)
  - MDS codes (good diffusion, but costly)

# *Key Schedule*

- On-the-fly round keys computation
- A fixed (hardwired) key allows:
  - to save a lot of GE,
  - avoid related-key attacks.
- Examples of lightweight *Key Schedules*:
  - KTANTAN: round-key-bits selected from the master-key
  - PRINTcipher: all round keys are the same
- Please don't design too lightweight Key Schedules!
  - Meet-in-the-Middle Attacks
- Diversify the keys

# Some Examples of Lightweight Block Ciphers

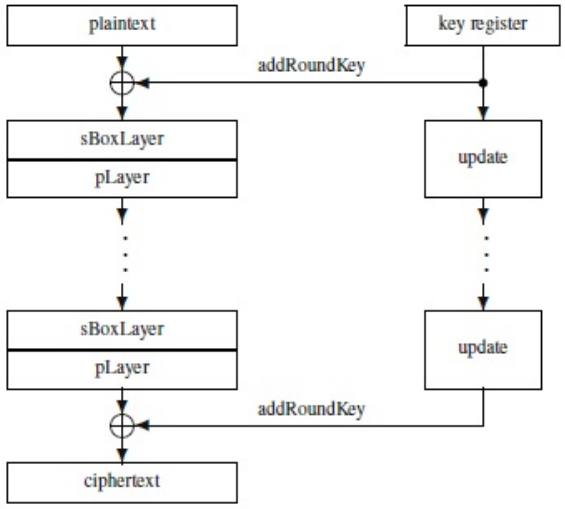
| | Key Size | Block Size | S-Box | Permutation | *Key Schedule* |
|---|---|---|---|---|---|
| AES | 128 | 128 | 8 | MDS | LIGHT |
| NEOKEON | 128 | 128 | 4 | BINARY | NO |
| MINI-AES | 64 | 64 | 4 | MDS | LIGHT |
| MCRYPTON | 64, 92, 128 | 64 | 4 | BINARY | LIGHT |
| PRESENT | 80, 128 | 64 | 4 | BIT PERM. | LIGHT |
| KLEIN | 64, 80, 96 | 64 | 4 | MDS | LIGHT |
| LED | 64, 128 | 64 | 4 | MDS | NO |

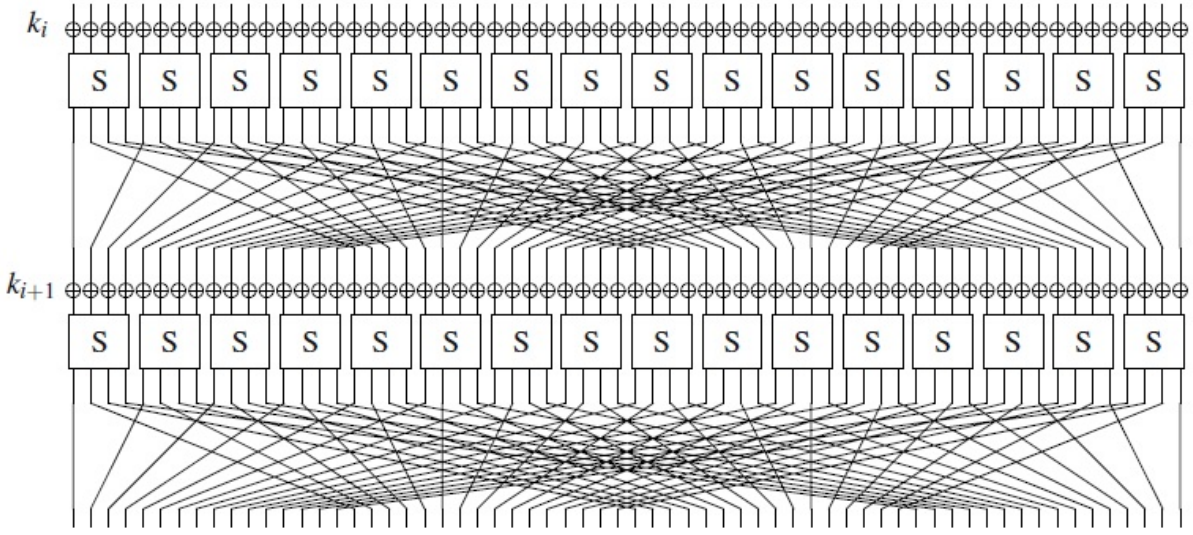
# SPN or Feistel?

- Feistel : $L_{i+1} = R_i$, $R_{i+1} = L_i \oplus f(R_i, k_{i+1})$
- SPN (*Substitution-Permutation Network*) : $L_{i+1} \| R_{i+1} = g(L_i \| R_i, k_{i+1})$
- 2 major advantages of Feistel ciphers compared to SPN ciphers:
  - $f$ identical for encryption and decryption
  - Only hardware for one half of the cipher state
- But :
  - Some simple CRPs don't need decryption
  - Feistels require more rounds than a SPN ($\Rightarrow$ time and power consumption penalty)
  - Feistels require XORs to mix the untransformed state with the transformed one (overhead: 2.5 - 3 GEs par bit)
- $\Rightarrow$ At first sight, SPNs win (*e.g.*, PRESENT)
- Counter-example: LILLIPUT

# PRESENT

generateRoundKeys()
**for** $i = 1$ to $31$ **do**
  addRoundKey(STATE,$K_i$)
  sBoxLayer(STATE)
  pLayer(STATE)
**end for**
addRoundKey(STATE,$K_{32}$)



# How Far Can We Go?

- Lower bound on area for a given block cipher fixed by the storage of the state and the round keys
  - *e.g.*, 64-bit block cipher with a 80-bit key: 864 GEs (without key-schedule)
- To get small logic, minimize algorithm description
- Impressive results:
  - PRESENT: 80% memory
  - KATAN: 90% memory

# Chronology

- 1st generation:
  - Only area optimisations in mind,
  - SPNs (*e.g.*, PRESENT).
- When we want to optimise area in priority, we take "weak" SBoxes and permutations but the number of clock cycles has to increase
- Non-optimal from latency and energy point of view
- 2nd generation:
  - Choose more secure SBoxes and permutation
  - Consider side-channel resistance by design

[8] J. Borghoff, A. Canteaut, T. Güneysu, E. B. Kavun, M. Knezevic, L. R. Knudsen, G. Leander, V. Nikov, C. Paar, C. Rechberger, P. Rombouts, S. S. Thomsen, T. Yalçin. "*PRINCE - A Low-Latency Block Cipher for Pervasive Computing Applications - Extended Abstract*". ASIACRYPT 2012: pp. 208-225.
[9] M. Knezevic, V. Nikov and P. Rombouts. "*Low-Latency Encryption – Is Lightweight = Light + Wait?*". CHES 2012, LNCS 7428, pp. 426 – 446.

[10] V. Grosso, G. Leurent, F.-X. Standaert, K. Varici. "*LS-Designs: Bitslice Encryption for Efficient Masked Software Implementations*". FSE 2014.

# Introduction

- Designed by Gaël Thomas, Thierry Berger (Limoges University, France) and Marine Minier (INSA Lyon, France)
- New lightweight 64-bit block cipher with 80-bit key
- Extended Generalized Feistel Network (EGFN) [Berger *et al.*, SAC 2013]
- Compact SBox (23 GEs) with desirable security properties
- Improved diffusion
- Involutive structure
- Compares well to other lightweight ciphers in encryption/decryption mode

# LILLIPUT Encryption

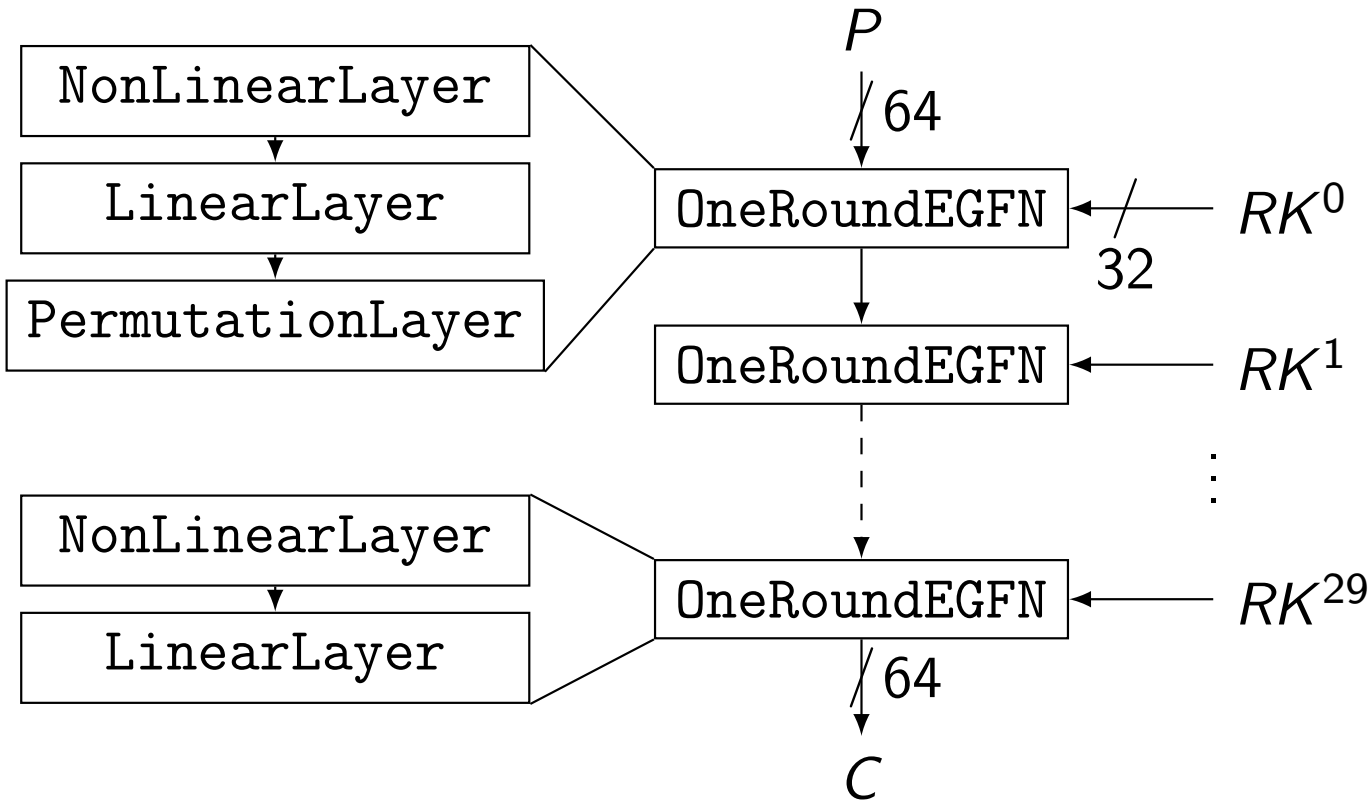



Figure : Lilliput Encryption

# LILLIPUT Decryption

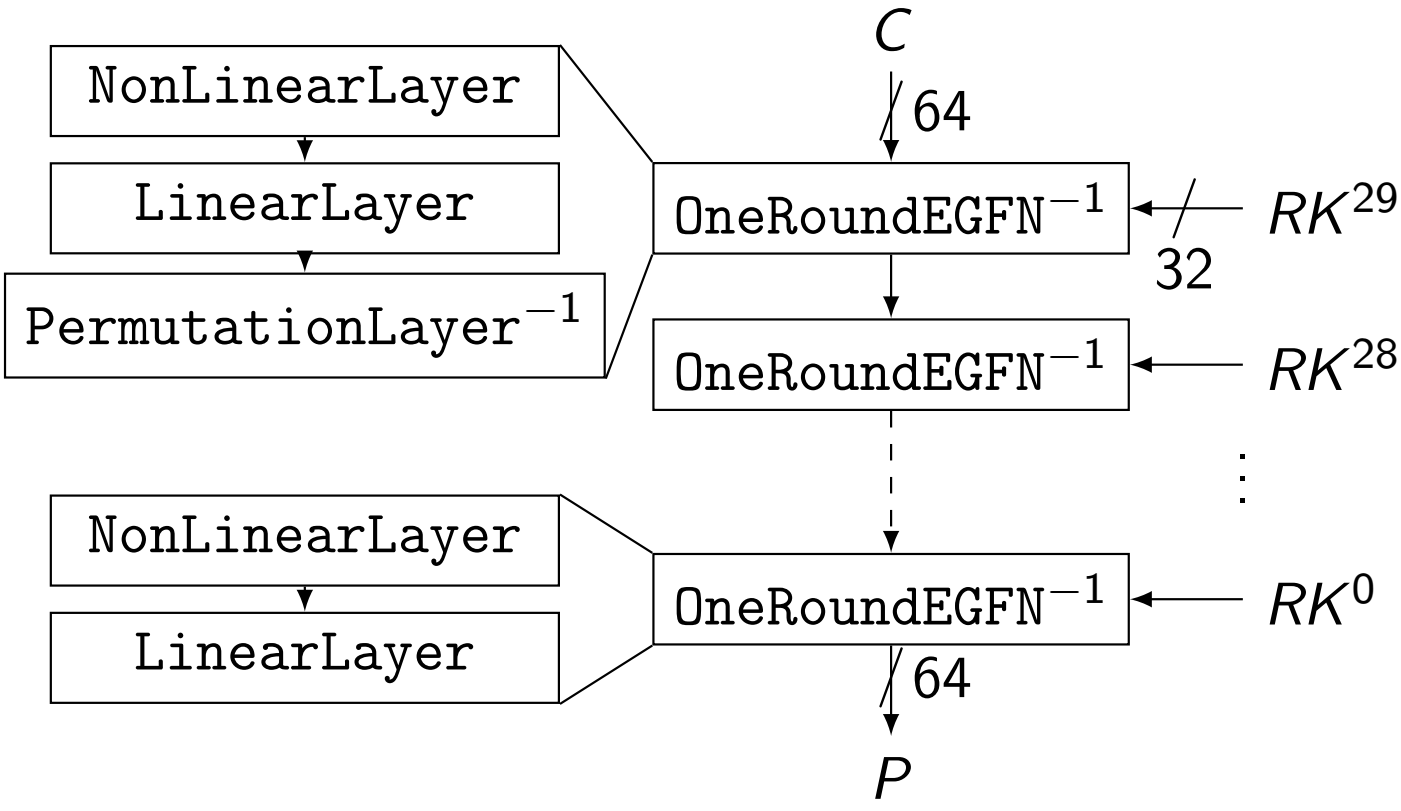
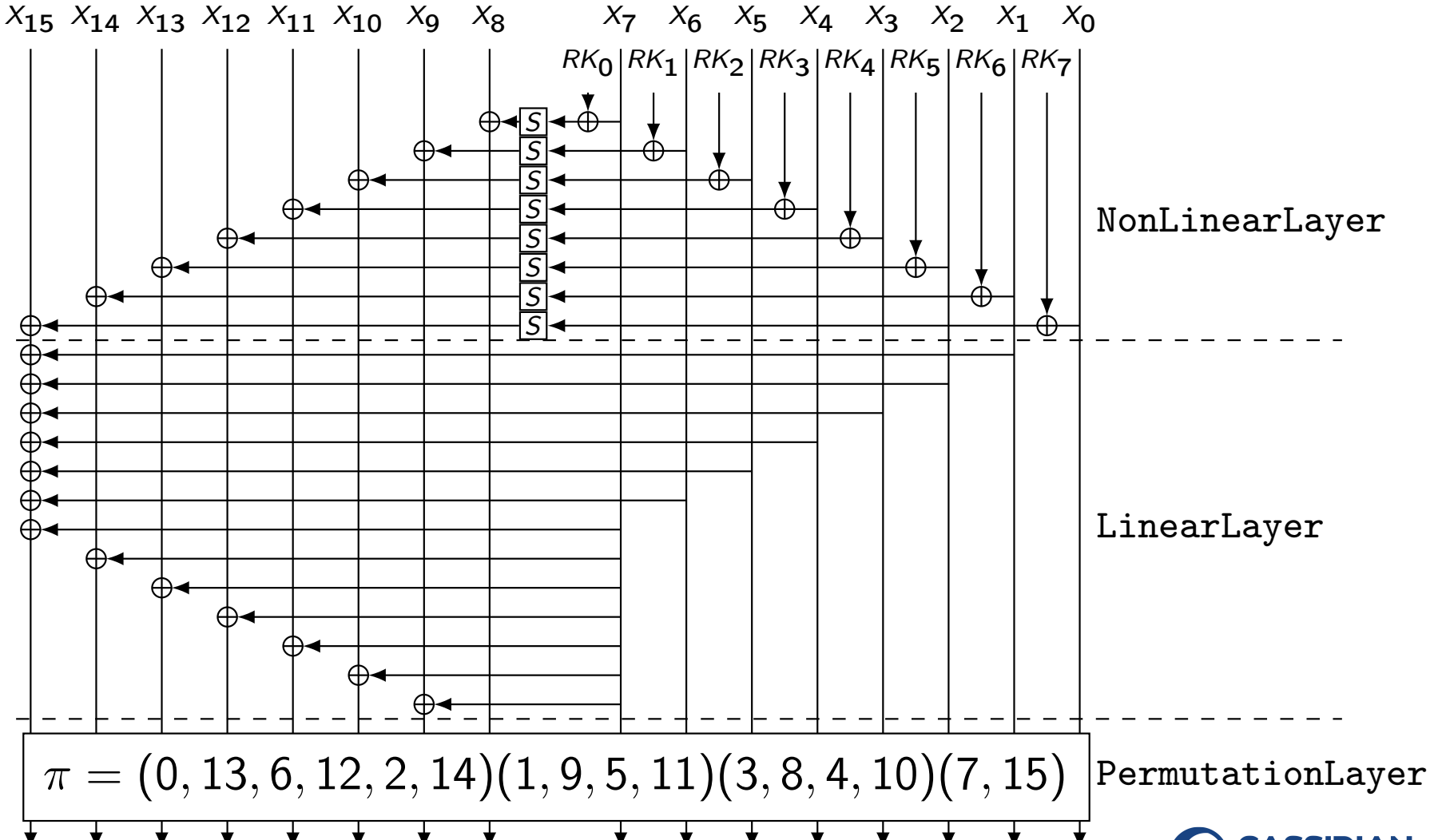
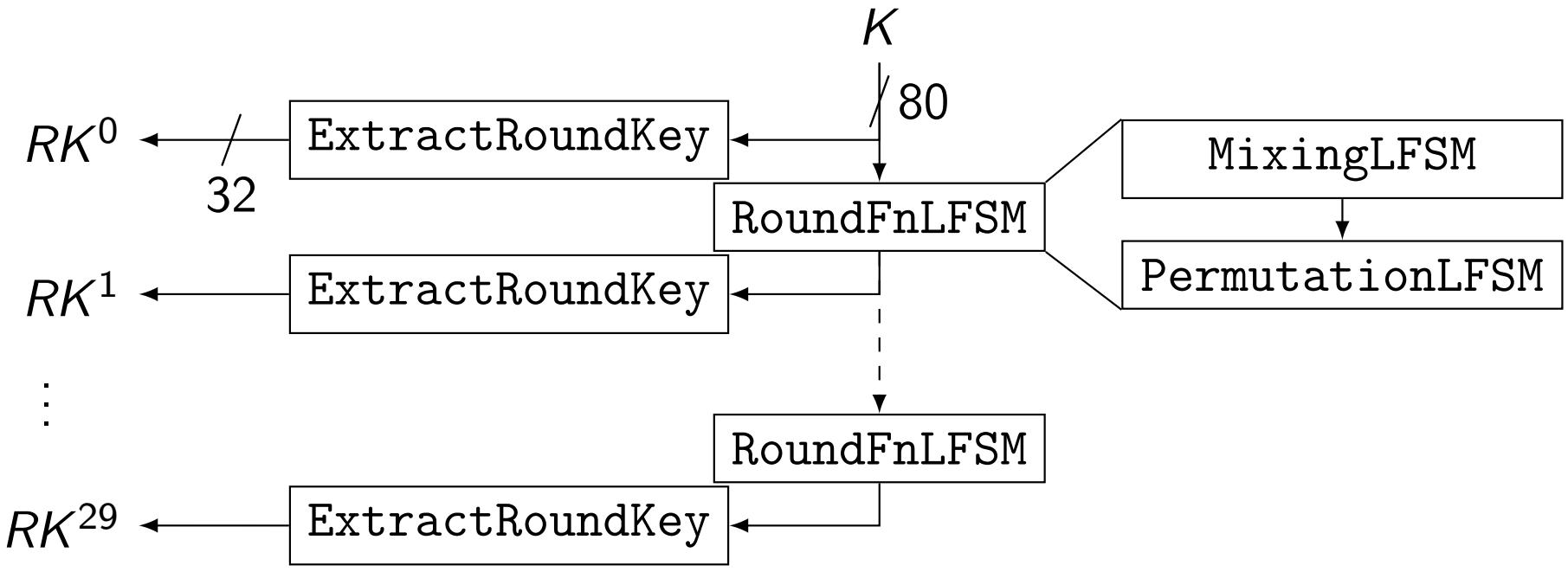



Figure : Lilliput Decryption

# OneRoundEGFN

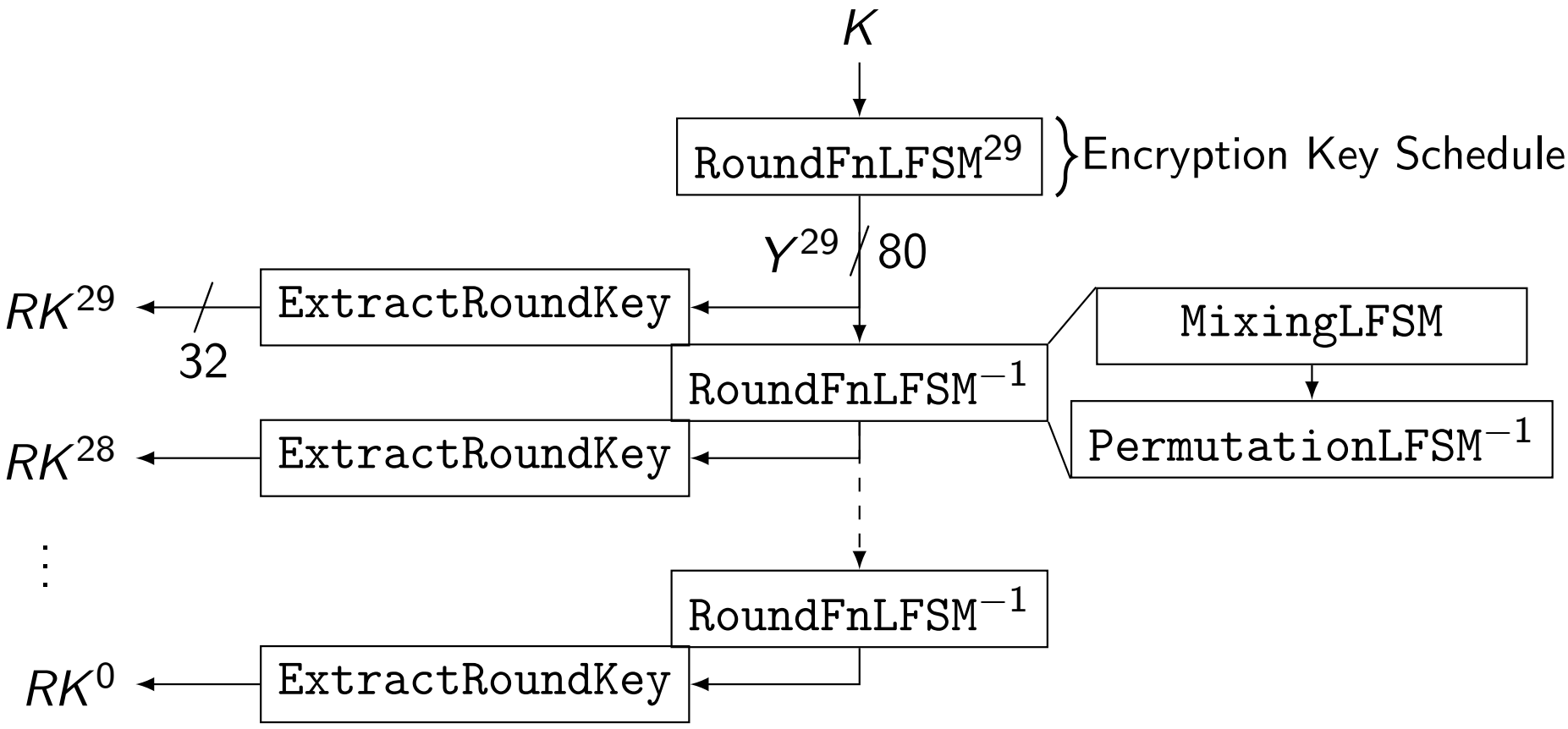


# Key Schedule in Encryption Mode




- ExtractRoundKey: 8 SBoxes
- Current round number xored to the last 5 bits of the subkey

# Key Schedule in Decryption Mode



# Security Analysis

- Resistance against:
  - Differential/Linear Cryptanalysis
  - Impossible Differential Attack
  - Integral Attack
  - Related Key and Chosen Key Attacks
- No attack against:
  - 22 rounds of LILLIPUT in the single key settings
  - 25 rounds of LILLIPUT in the relative, known and chosen key settings
- $\Rightarrow$ Security Margin (30 rounds)

# SPN or Feistel? (continued)

- "Some simple CRPs don't need decryption"
  - CRPs only for unilateral authentication, but quid for mutual authentication?
- Feistels require more rounds than a SPN ($\Rightarrow$ time and power consumption penalty)
  - Fast diffusion fills the gap
- Feistels require XORs to mix the untransformed state with the transformed one
  - $21 \times 4$ XORs $= 189$ GEs

# Theoretical vs. Practical Implem. Results

| Component | Cost (GEs) |
|---|---|
| Storage | 828 |
| SBoxes | 368 |
| XORs | 317.25 |
| 2-to-1 MUXes | 288 |
| Total (theo.) | 1801.25 |
| Total (prac.) | 1832 |

- VHDL, low-power High Vt 65 nm standard-cell library, Synopsis Design Vision D-2010.03-SP5-2 for synthesis and power simulation, typical foundry values (1.2 V, 25°), no scan flip-flops, low-area

# Comparison

| | Lat. (cycles) | Thr. (kbit/s) | Area (GEs) | Power ($\mu$W) | Logic Process |
|---|---|---|---|---|---|
| PRESENT-80 | 32 | 200 | 1570 | 5 | 0.18 $\mu$m |
| TWINE | 36 | 178 | 1799 | NA | 90 nm |
| LBlock | 32 | 200 | 1320 | NA | 0.18 $\mu$m (theo.) |
| *Piccolo*-80 | 27 | 237 | 1274 | NA | 0.13 $\mu$m (theo.) |
| Lilliput | 30 | 213 | 1832 | 0.9 | LP 65nm |

- At first sight, Lilliput appears not competitive, but:
  - Only encryption is implemented,
  - Use of scan flip-flops,
  - Optimisations,
  - Theoretical vs. practical implementation results
- At the end, LILLIPUT enc./dec. has lower (resp. bigger) gate count than the block ciphers which have a (un)secure Key Schedule, *e.g.* PRESENT and TWINE (LBlock and Piccolo)
- The price to pay to have a secure Key Schedule is reasonable ($\approx$ 200 GEs)

# Summary

- RFID tags face harsh contraints
  - Low area
  - Low power
  - Short messages
- Lightweight block ciphers must...
  - have a small internal state
  - allow a serial implementation
  - have a low latency
  - provide a short output
- Implement cryptography in UHF tags is a challenge
- Lightweight cryptography crucial for RFID security
- LILLIPUT is an interesting candidate where mutual authentication is required

# Open Questions

- Sharing tag resources (memory, arithmetic) between cryptographic modules
  - Ideal case: "one-for-all" (encryption, MAC, PRNG, *etc.*)
- Think about side-channel protection from the design phase
- Authenticated Encryption
- Public-Key Cryptography
- Find a lightweight block cipher which is efficient both in hard and soft

## Lightweight Cryptography is an Exciting Topic!

- Many new candidates to analyze regularly
- Interdisciplinary domain
- Hunt hidden overheads

# Thanks. Questions?