Lightweight Block Cipher Design

Gregor Leander

HGI, Ruhr University Bochum, Germany

Croatia 2014

Horst Görtz Institute for IT-Security

Outline

Outline

Upcoming IT-Landscape

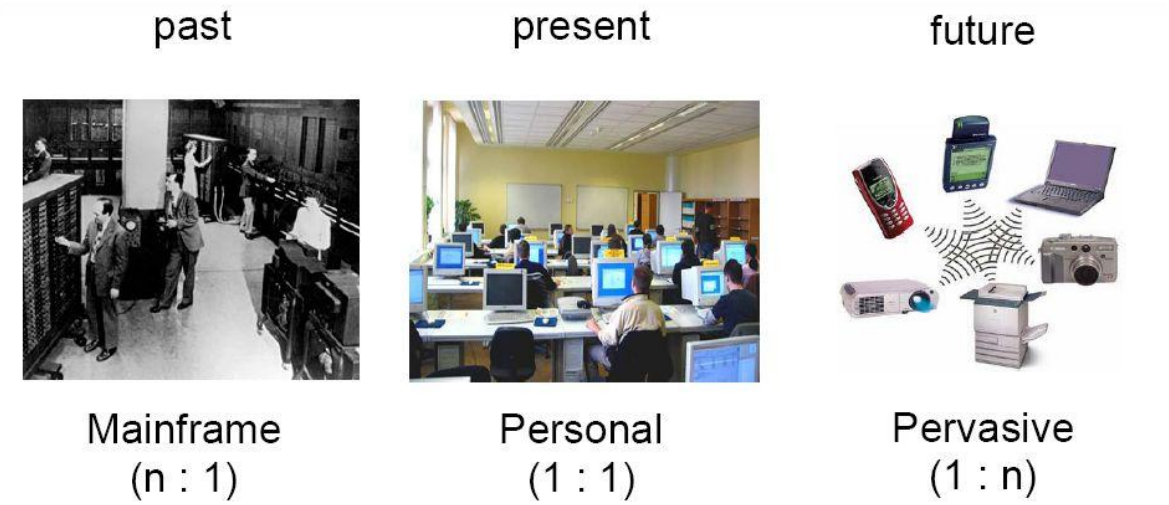


Figure: Upcoming IT-Landscape

More Precisely: RFID-Tags

RFID Tag

RFID=Radio-Frequency IDentification

Example I

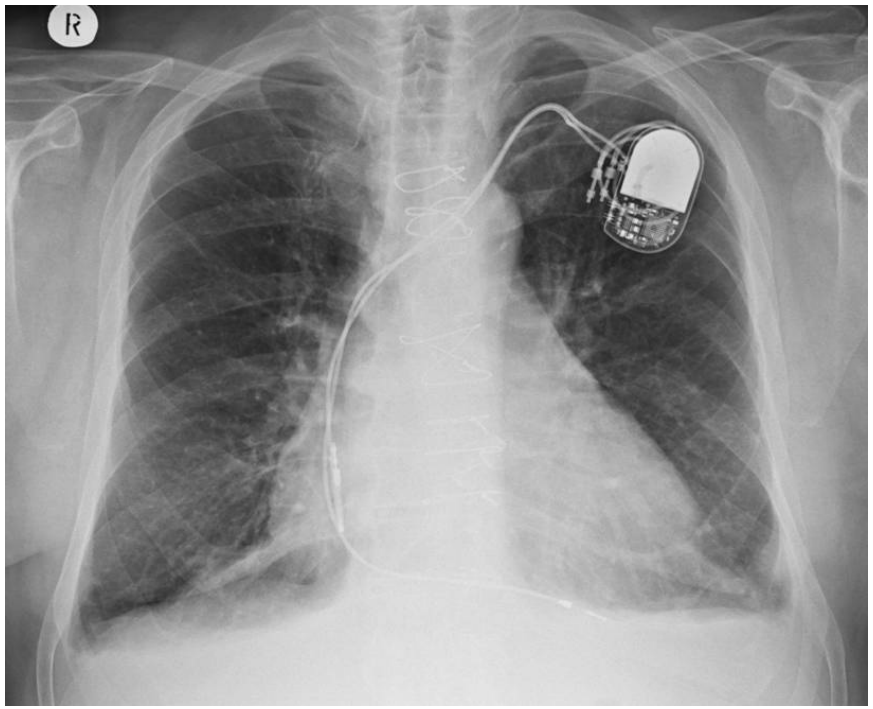
Quelle: Bundesministerium des Innern

Electronic Passports

Example II

Logistics

Example III



Pacemaker implants

Security

Question

Do we want this?

Security

Question

Do we want this?

If we want it, we want it secure!

Attacks I

Iron attacks in Russia

Attacks II

Fear: Terrorist attacks on pacemaker

Lightweight Cryptography

What is (not) Lightweight Cryptography

- Cryptography tailored to (extremely) constrained devices
- Not intended for everything
- Not intended for extremely strong adversaries
- Not weak cryptography

Lightweight Cryptography

Question

What about standard algorithms?

- AES is great for almost everywhere
- Mainly designed for software
- It is too expensive for very small devices
- It protects data stronger than needed

AES: The Swiss Army Knife

Domain Specific Cipher

On specific platforms/for specific criteria one can do better.

Lightweight Cryptography: Industry vs. Academia

Industry

Non-existence of lightweight block ciphers a real problem since the 90's.

- Many proprietary solutions
- Often: not very good.

Academia

Research on Lightweight block ciphers started only recently.

- Several good proposals available.
- Developed a bit away from industry demands.

Outline

Lightweight Ciphers in Real Life

Example (Algorithms Used In Real Products)

- Keeloq
- MIFARE
- DECT
- Kindle Cipher

What they have in common:

- efficient
- proprietary/not public
- non standard designs
- not good

A lot more out there...

Keeloq

Keeloq

A 32 bit block-cipher with a 64 bit key.

- Developed by Gideon Kuhn (around 1985).
- Sold for 10M$ to Microchip Technology Inc (1995).
- Algorithm for remote door openers: Cars, Garage, ...
- Used by: Chrysler, Daewoo, Fiat, GM, Honda, Toyota, Volvo, Volkswagen Group,...

KeeLoq

A Practical Attack on KeeLoq*,**

Sebastiaan Indesteege[1,***], Nathan Keller[2,†], Orr Dunkelman[1], Eli Biham[3], and Bart Preneel[1]

[1] Department of Electrical Engineering ESAT/SCD-COSIC, Katholieke Universiteit Leuven. Kasteelpark Arenberg 10, B-3001 Heverlee, Belgium.
{sebastiaan.indesteege,orr.dunkelman,bart.preneel}@esat.kuleuven.be
[2] Einstein Institute of Mathematics, Hebrew University. Jerusalem 91904, Israel.
nkeller@math.huji.ac.il
[3] Computer Science Department, Technion. Haifa 32000, Israel.
biham@cs.technion.ac.il

Abstract. KeeLoq is a lightweight block cipher with a 32-bit block size and a 64-bit key. Despite its short key size, it is widely used in remote keyless entry systems and other wireless authentication applications. For example, authentication protocols based on KeeLoq are supposedly used by various car manufacturers in anti-theft mechanisms. This paper presents a practical key recovery attack against KeeLoq that requires 2^{16} known

EUROCRYPT 2008

MIFARE

MIFARE Cipher

A stream cipher with an 48 bit key.

- widely used in contactless smart cards
- billions of smart card chips
- electronic bus and train tickets

MIFARE Cipher

A Practical Attack on the MIFARE Classic

Gerhard de Koning Gans, Jaap-Henk Hoepman, and Flavio D. Garcia

Institute for Computing and Information Sciences
Radboud University Nijmegen
P.O. Box 9010, 6500 GL Nijmegen, The Netherlands
gkoningg@sci.ru.nl,
jhh@cs.ru.nl,
flaviog@cs.ru.nl

Abstract. The MIFARE Classic is the most widely used contactless smart card in the market. Its design and implementation details are kept secret by its manufacturer. This paper studies the architecture of the card and the communication protocol between card and reader. Then it gives a practical, low-cost, attack that recovers secret information from the memory of the card.

CARDIS 2008

DECT

DECT Cipher

A stream cipher with an 64 bit key.

- cordless home telephones
- 30.000.000 base station in Germany
- also baby phones, traffic lights, etc

DECT Cipher

Cryptanalysis of the DECT Standard Cipher

Karsten Nohl[1] and Erik Tews[2] and Ralf-Philipp Weinmann[3]

[1] University of Virginia,
[2] Technische Universität Darmstadt,
[3] University of Luxembourg
nohl@cs.virginia.edu,
e_tews@cdc.informatik.tu-darmstadt.de,
ralf-philipp.weinmann@uni.lu

Abstract. The DECT Standard Cipher (DSC) is a proprietary 64-bit stream cipher based on irregularly clocked LFSRs and a non-linear output combiner. The cipher is meant to provide confidentiality for cordless telephony. This paper illustrates how the DSC was reverse-engineered from a hardware implementation using custom firmware and information on the structure of the cipher gathered from a patent. Beyond disclosing the DSC, the paper proposes a practical attack against DSC that recovers the secret key from 2^{15} keystreams on a standard PC with a success rate of

FSE 2010

Kindle

Kindle Cipher (PC1)

A stream cipher with an 128 bit key.

- Amazons Kindle ebook
- DRM system

Kindle Cipher

Cryptanalysis of the "Kindle" Cipher

Alex Biryukov, Gaëtan Leurent, Arnab Roy

University of Luxembourg
alex.biryukov@uni.lu, gaetan.leurent@uni.lu, arnab.roy@uni.lu

Abstract. In this paper we study a 128-bit-key cipher called PC1 which is used for the DRM system of the Amazon Kindle e-book reader. This is the first academic cryptanalysis of this cipher and it shows that PC1 is a very weak stream cipher, and can be practically broken in a known-plaintext and even in a ciphertext-only scenario.

SAC 2012

Outline

Why?

Question

Why do they do that?

We need

- secure
- well analyzed
- public

ciphers for highly resource constrained devices.

General Design Philosophy

Guidelines/Goals

- Efficiency: Here mainly area
- Simplicity
- Security

Design Considerations: Hardware

Hardware

What do things cost in hardware?

Suggestion

Make it an interdisciplinary project!

Cost Overview

Question

What should/should not be used?

Rule of Thumb:

- NOT: 0.5 GE
- NOR: 1 GE
- AND: 1.33 GE
- OR: 1.33
- XOR: 2.67

Registers/Flipflops: $6 - 12$ GE per bit!

Design Decisions I

Question

Block size/ Key size?

Storage (FF) is expensive in hardware.

- Block size of 128 is too much.
- We do not have to keep things secret forever.

Decision

Relative Small Block Size: 32,48 or 64
Key size: 80 bit often enough

Block Cipher Parts

SP-Network

We have to design

- Non-linear-Layer
- Linear-Layer
- Key-scheduling

Here we focus on the Non-linear-Layer and the Linear-Layer.

Design Issues

Design Issues

The S-Layer has to maximize nonlinearity.
It has to be cheap.

The S-Layer consist of a number of Sboxes executed in parallel

$$S_i : \mathbb{F}_2^b \rightarrow \mathbb{F}_2^b$$

In hardware realized as Boolean functions.

Design Issues

Question

Different Sboxes vs. all Sboxes the same?

A serialized implementation becomes smaller if all Sboxes are the same.

Decision

Only one Sbox.

Design Issues

Question

What size of Sbox?

In general: The bigger the Sbox the more expensive it is in hardware.

Sbox Costs

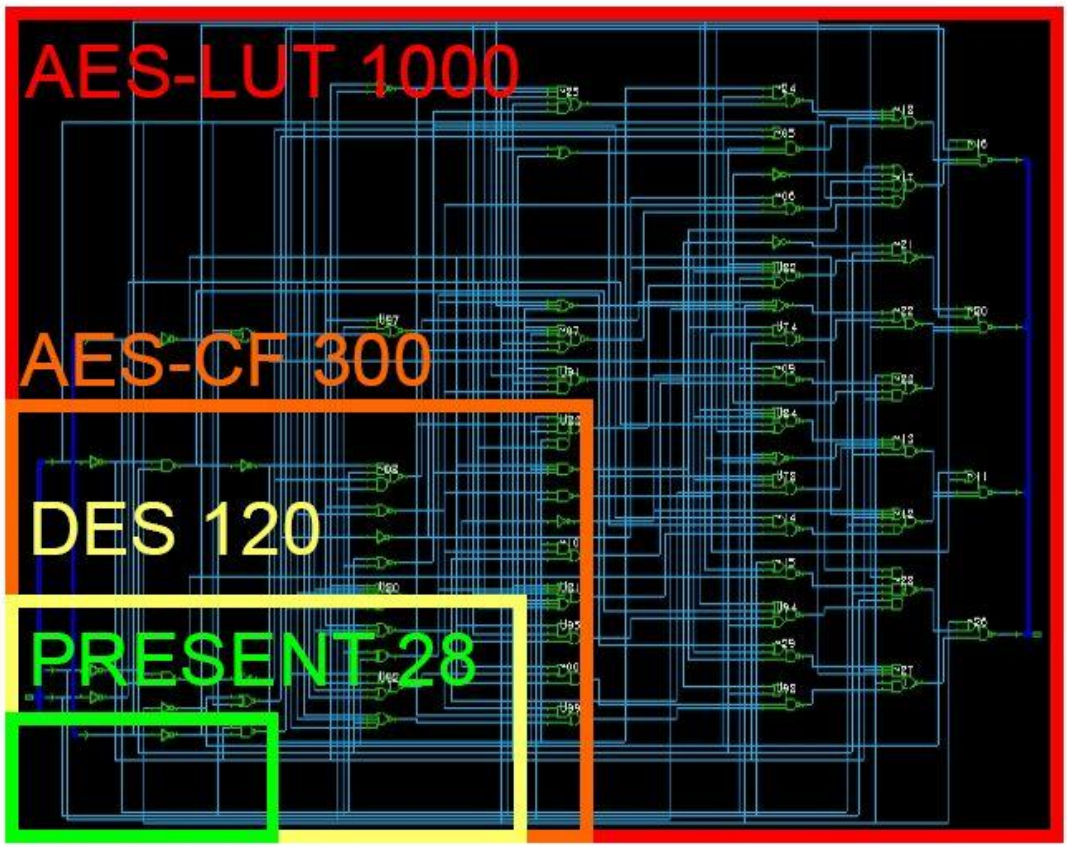


Figure: Comparison of Sboxes

P-Layer

Design Issues

The P-Layer has to maximize diffusion.
It has to be cheap.

- Many modern ciphers: MDS codes (great diffusion!)
- DES: Bit permutation (no cost!)

Design Decision

- Use less diffusion per round
- Use more rounds

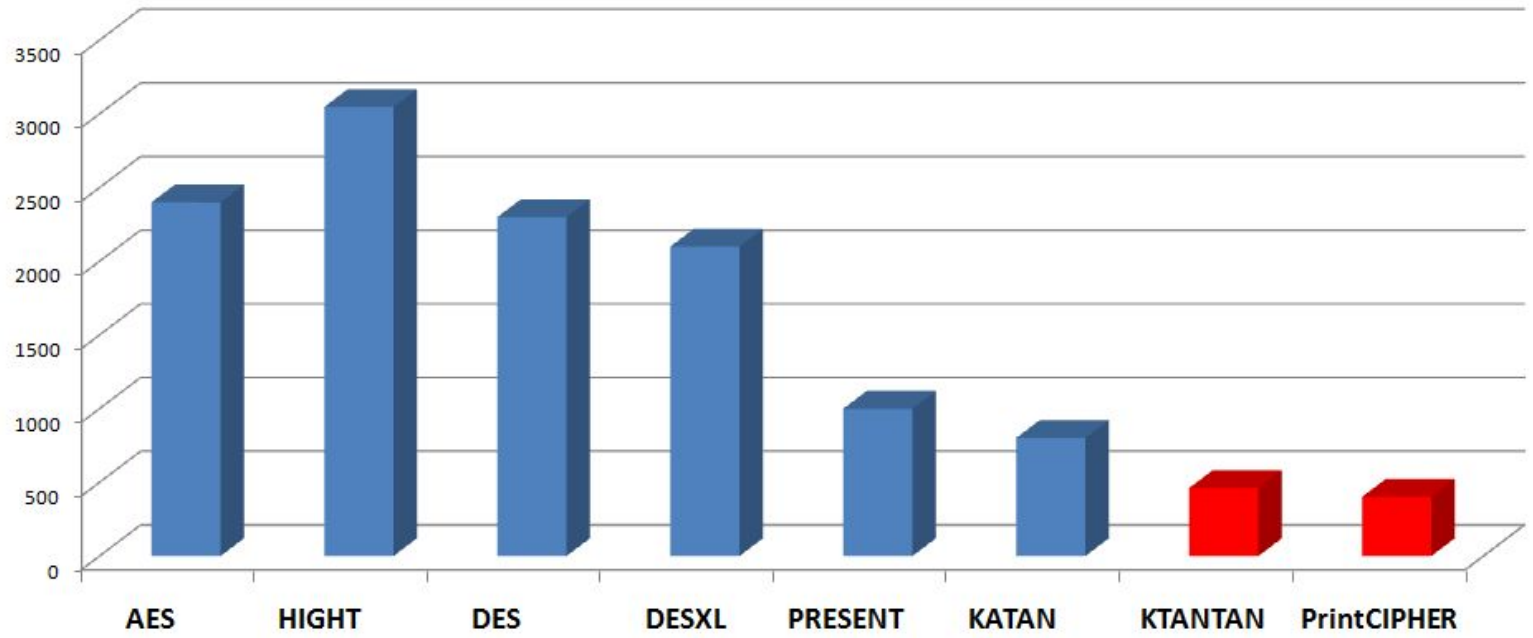
Examples

Modern Lightweight block ciphers

- SEA
- DESL
- PRESENT
- KATAN/ KTANTAN
- HIGHT
- PrintCIPHER

A lot more out there...

A comparison: (To be taken with care)



A fair comparison is difficult

- Many dimensions
- Depends on the technology

First Example: PRESENT

PRESENT (CHES 2007)

A 64 bit block cipher with 80/128 bit key and 31 rounds.

Developed by RUB/DTU/ORANGE

- SP-network
- 4 bit Sbox
- Bit permutation as P-layer

PRESENT: Overview

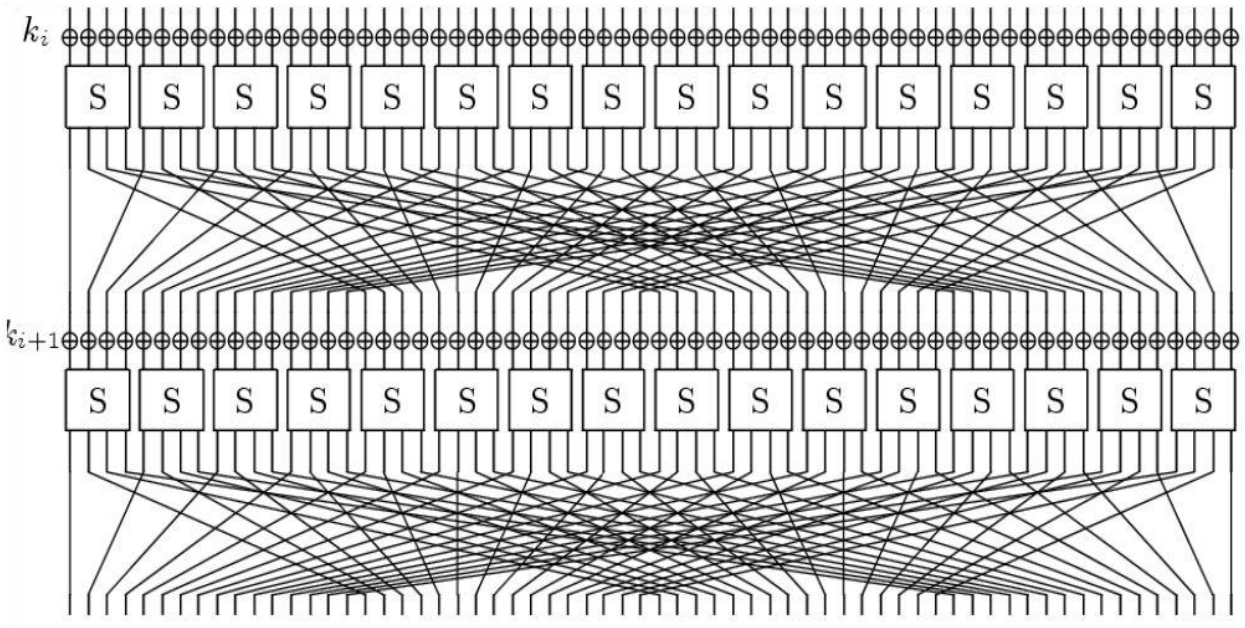


Figure: Overview of PRESENT

Second Example: KATAN

KATAN (CHES 2009)

A 32/48/64 bit block cipher with 80 bit key and 254 rounds.

Developed by KUL

- A (kind of) Feistel-cipher
- Highly unbalanced
- Inspired by Trivium
- Very simple non-linear function

KATAN: Overview

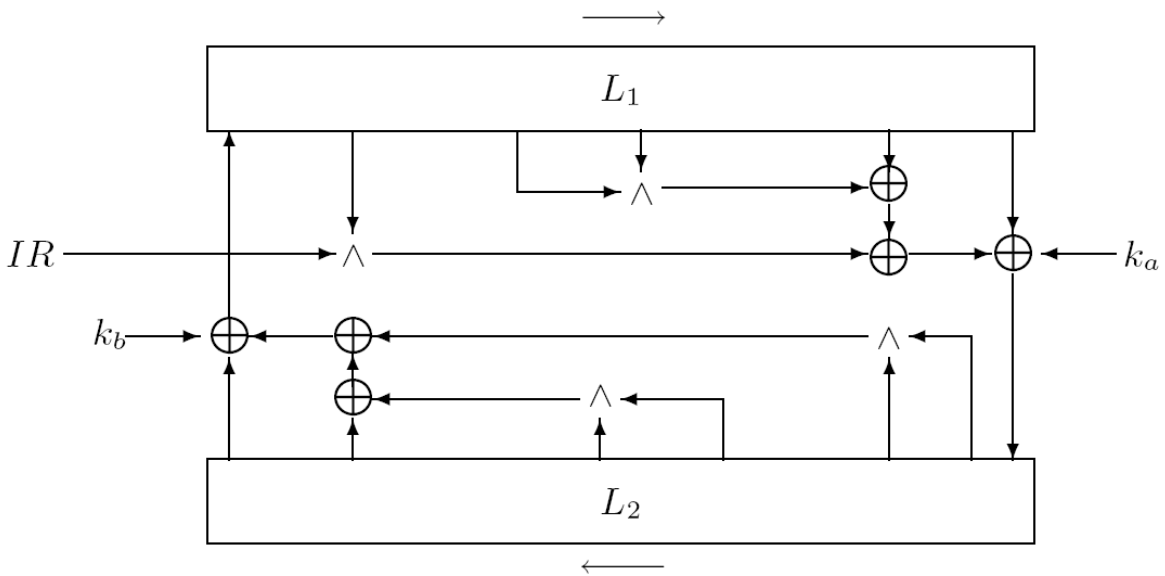


Figure: Overview of KATAN

Third Example: LED

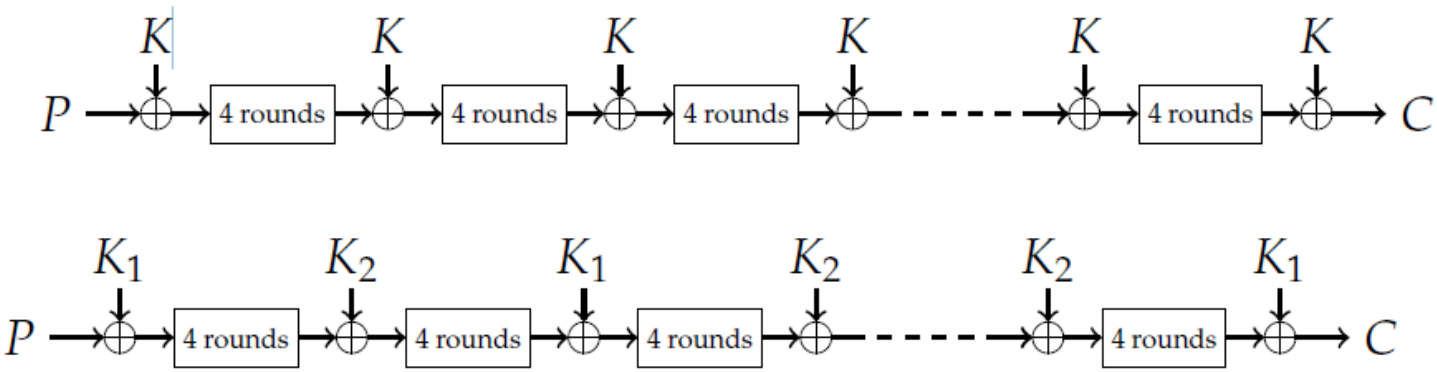
LED (CHES 2011)

A 64 bit block cipher with $64 - 128$ bit key and 32/48 rounds.

Developed by NTU and Orange Labs

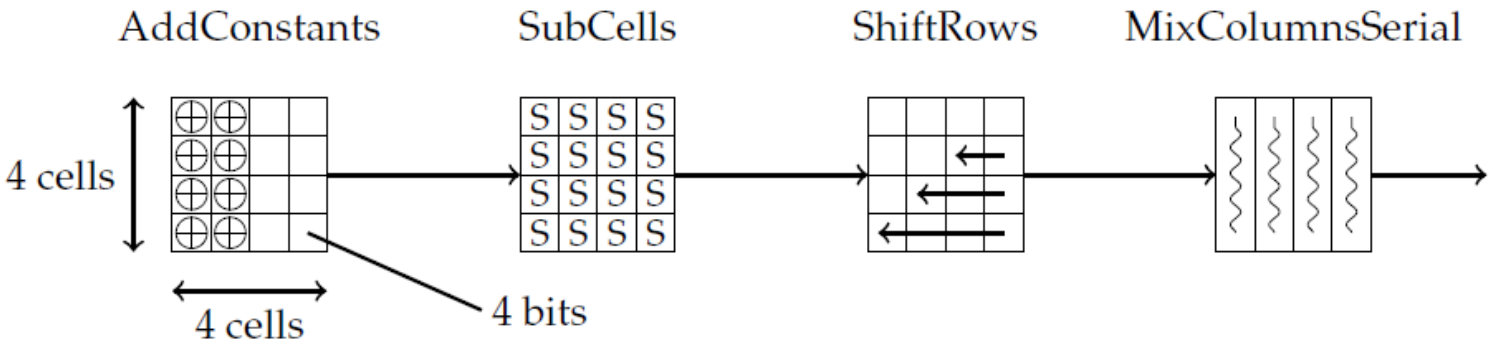
- A SP-network
- Inspired by AES
- Nice tweak to Mix Columns

LED: Overview



LED: Round Function

Very AES inspired:

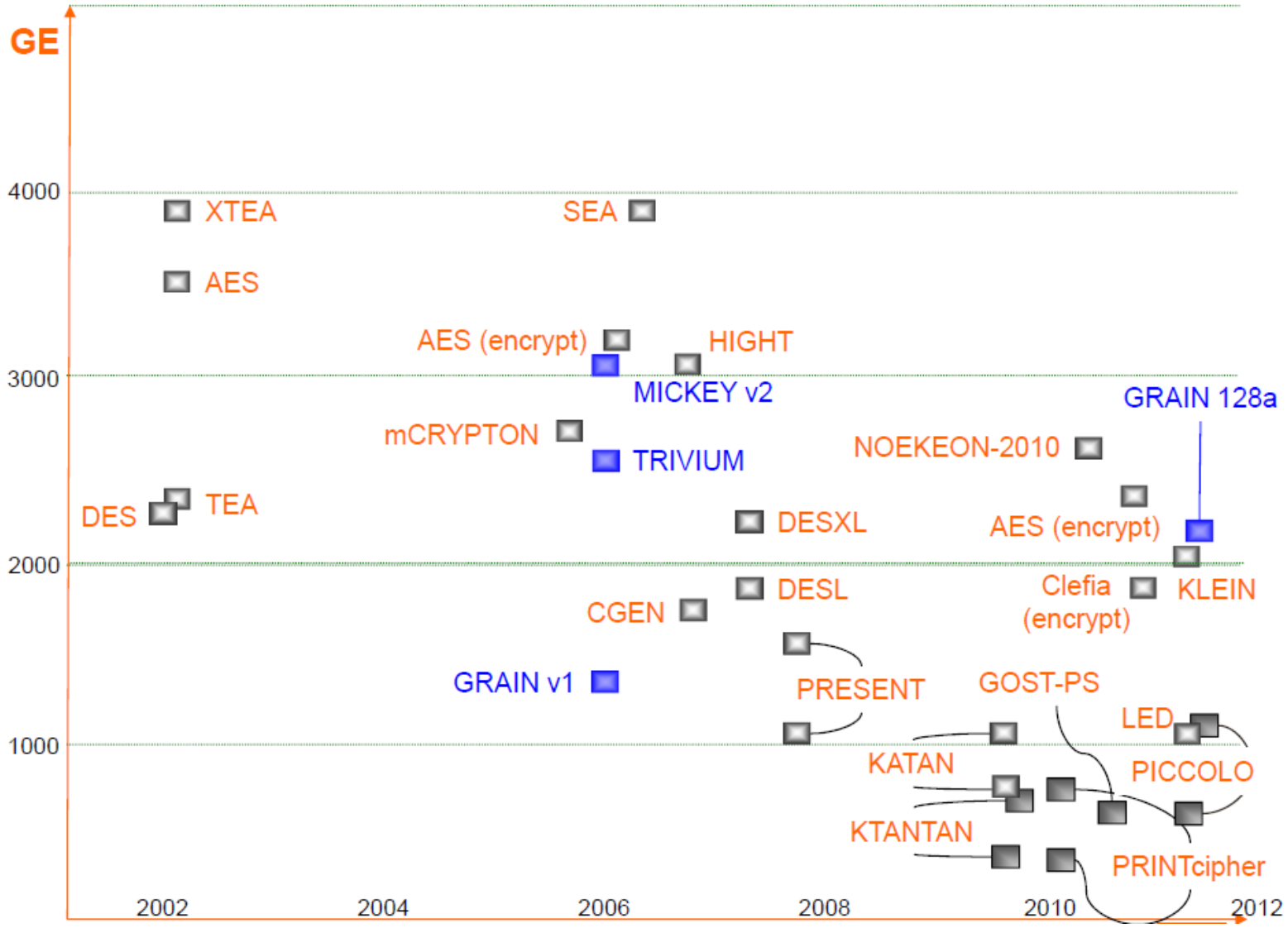


Nice Trick – Hardware friendly MDS Matrix:

$$(B)^4 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 4 & 1 & 2 & 2 \end{pmatrix}^4 = \begin{pmatrix} 4 & 1 & 2 & 2 \\ 8 & 6 & 5 & 6 \\ B & E & A & 9 \\ 2 & 2 & F & B \end{pmatrix}$$

Very hardware friendly (but slower).

Overview: As Time Goes By



Outline

How Far Can You Go?

Memory

Given a block-size and a key-size the (minimal) memory requirements are fixed.

Focus on Area

Minimize the overhead to this.

- PRESENT: 80 percent memory
- KATAN: $\approx$ 90 percent memory

Even doing nothing is not a lot cheaper!

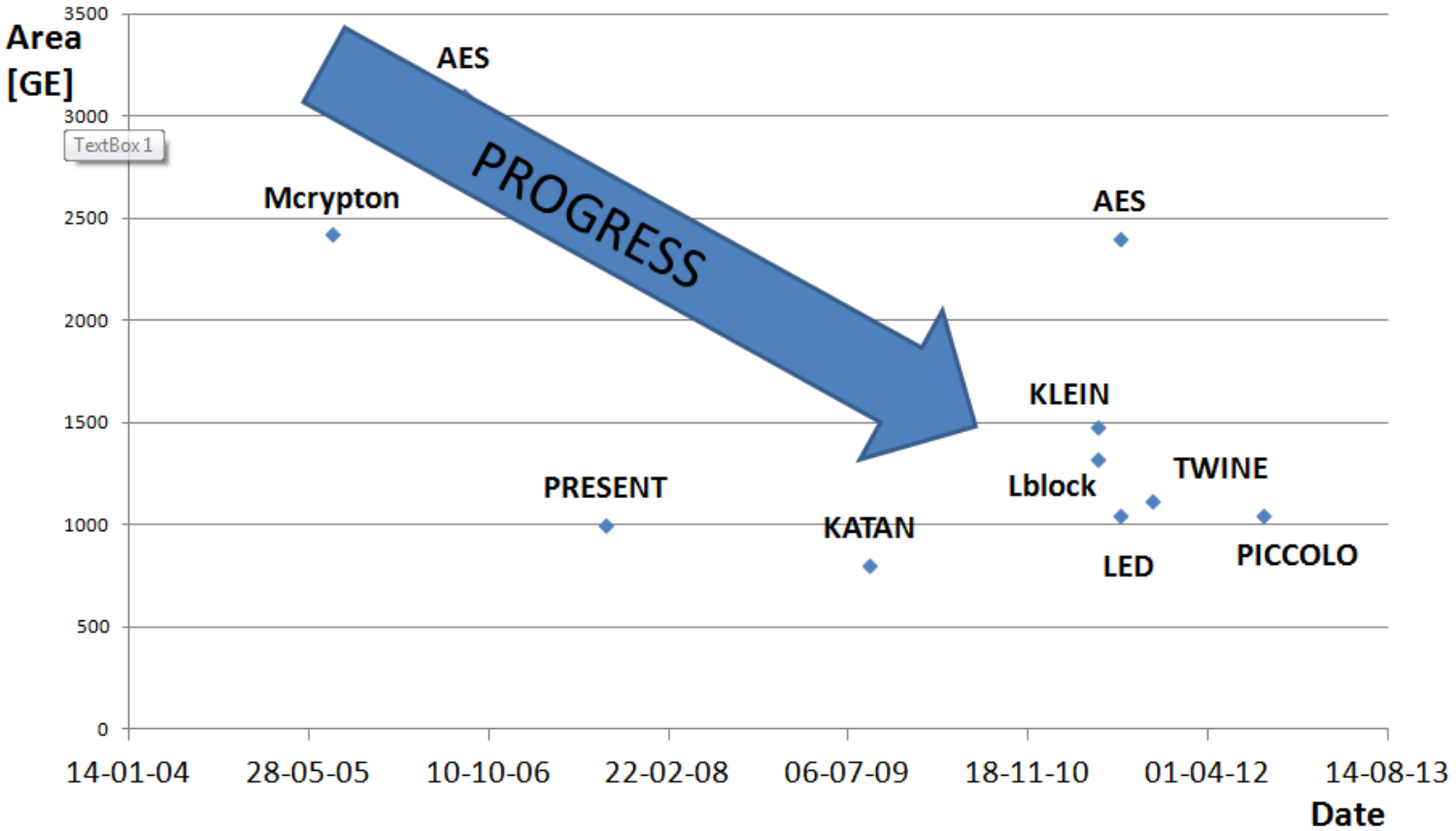
A Critical View (I)

Even doing nothing is not a lot cheaper!

Good or Bad?

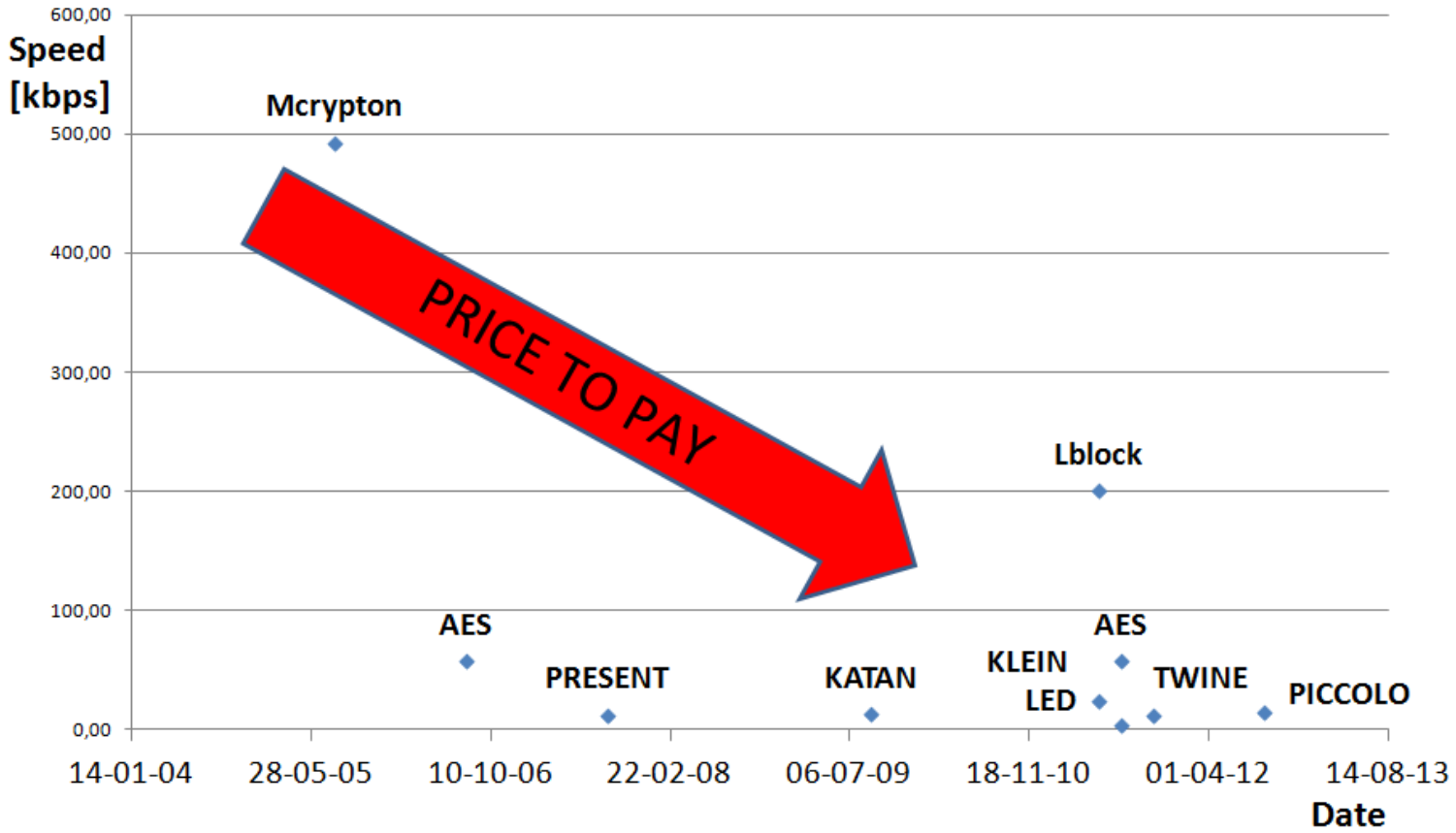
- In terms of area: Good
- In terms of energy: Bad

Progress



Design Date vs. Area

A Critical View (II)



Design Date vs. Speed

A Critical View (III)

Area Only

There seem only a few scenarios where the only criteria is area

For those good examples are available.

Time To Move On

Focus on other criteria!

Outline

Time To Move On

Focus on other criteria!

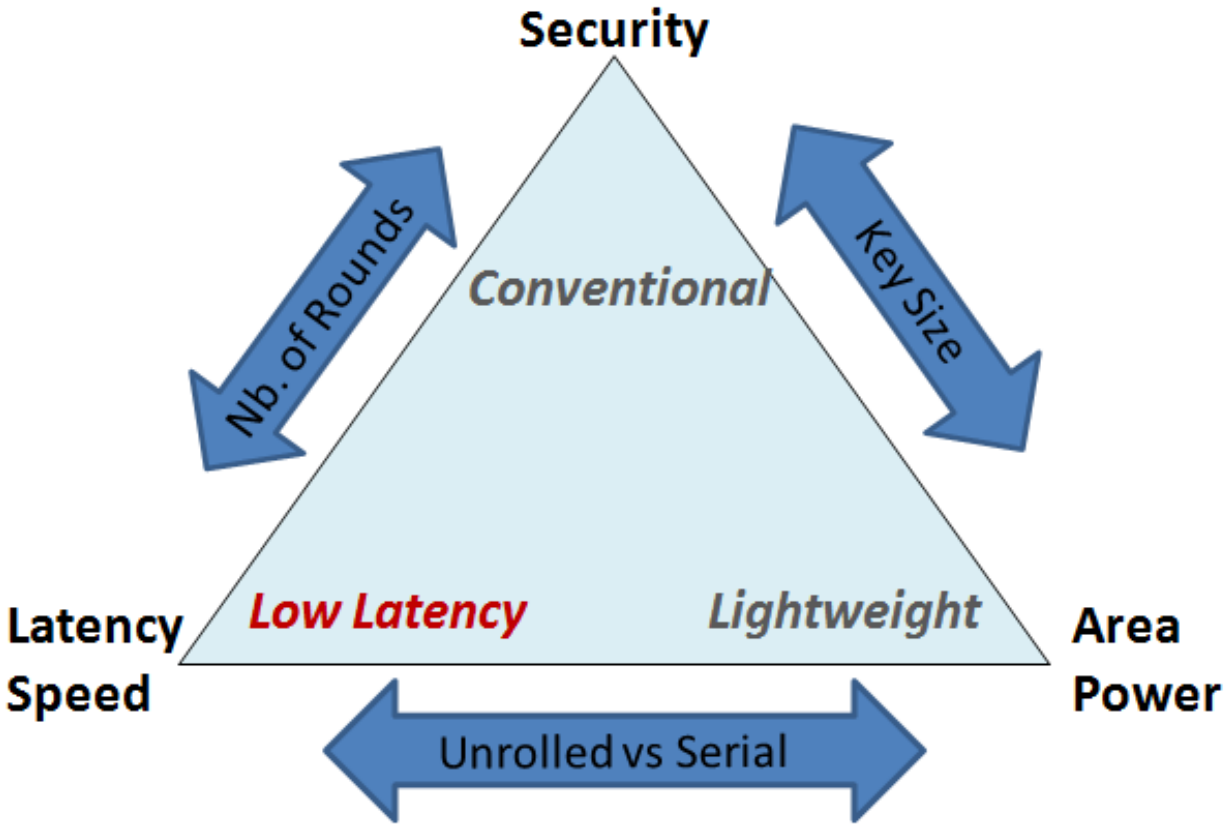
Examples:

- Latency
- Side-channel

Latency

Latency

Time to encrypt one block



Latency

Low-Latency Encryption – Is "Lightweight = Light + Wait"?*

Miroslav Knežević, Ventzislav Nikov, and Peter Rombouts

NXP Semiconductors, Leuven, Belgium

Abstract. The processing time required by a cryptographic primitive implemented in hardware is an important metric for its performance but it has not received much attention in recent publications on lightweight cryptography. Nevertheless, there are important applications for cost effective low-latency encryption. As the first step in the field, this paper

CHES 2012

PRINCE

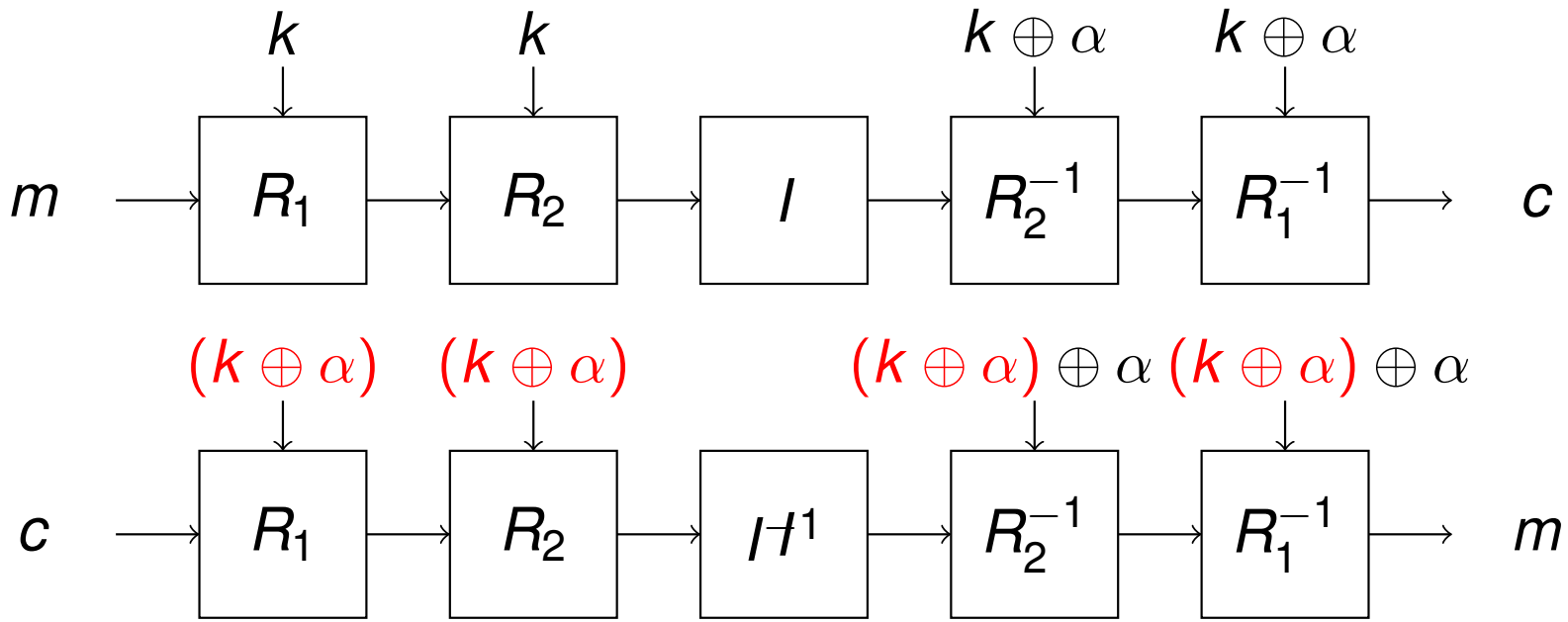
PRINCE (ASIACRYPT'12)

A block cipher optimized for low-latency (Designed by DTU, RUB, and NXP)

More precisely:

- one single clock cycle
- low latency $\Rightarrow$ high clock rates
- moderate hardware costs
- encryption and decryption with low overhead.

PRINCE - Overview



Enc vs. Dec

Decryption is Encryption with a different key!

$$E_k^{-1}(m) = E_{k \oplus \alpha}(m)$$

$\alpha =$ `0xc0ac29b7c97c50dd`

Side-Channel Resistance

Side-Channel Resistance

Without protection having a strong cipher is useless

Therefore: Masking necessary

Usual Approach

1. Design a cipher
2. Try to mask it efficiently

Side-Channel Resistance by Design

Usual Approach

1. Design a cipher
2. Try to mask it efficiently

Better

Design ciphers that are easy to mask

First approach already in 2000: NOEKEON

FSE 2014: LS-Designs

A familiy of easy to mask block ciphers

Designed by UC-Louvain and INRIA

Main idea

Opposite approach of what is done usually:

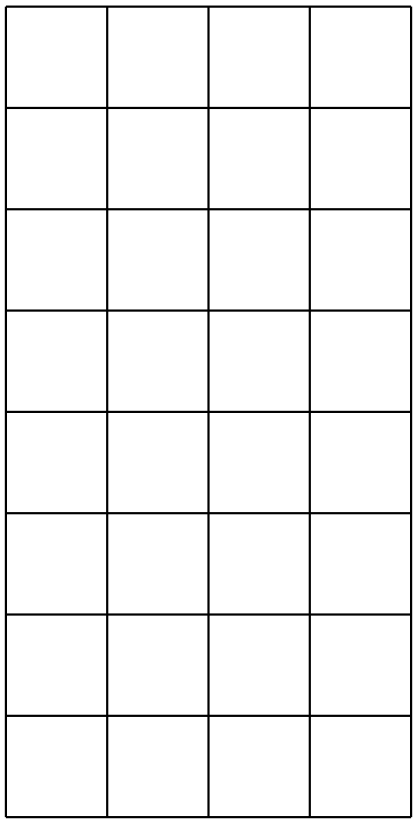
- Use tables for the linear-layer
- Use (few) logical operations for S-boxes

Two instances:

- Robin
- Fantomas

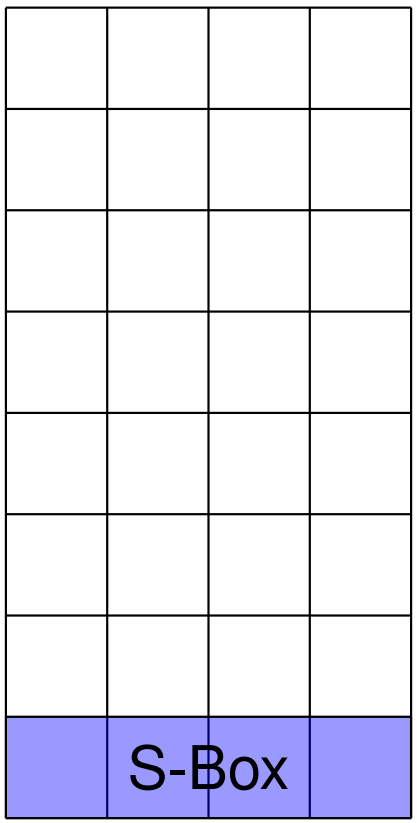
LS-Designs: Structure

- One box is a bit
- Registers correspond to columns



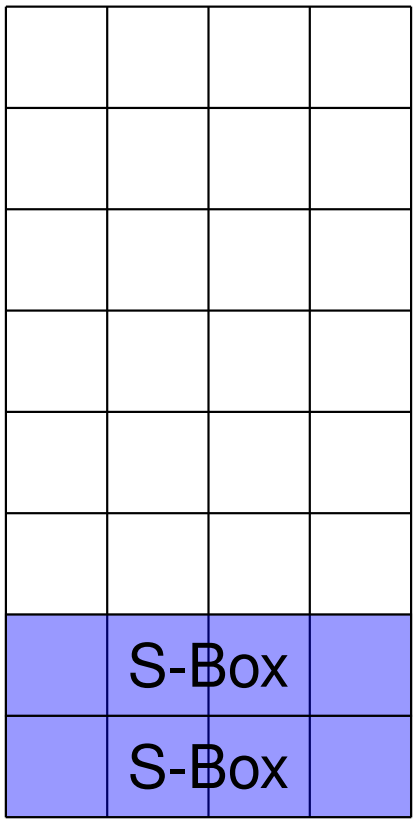
LS-Designs: Structure

- One box is a bit
- Registers correspond to columns



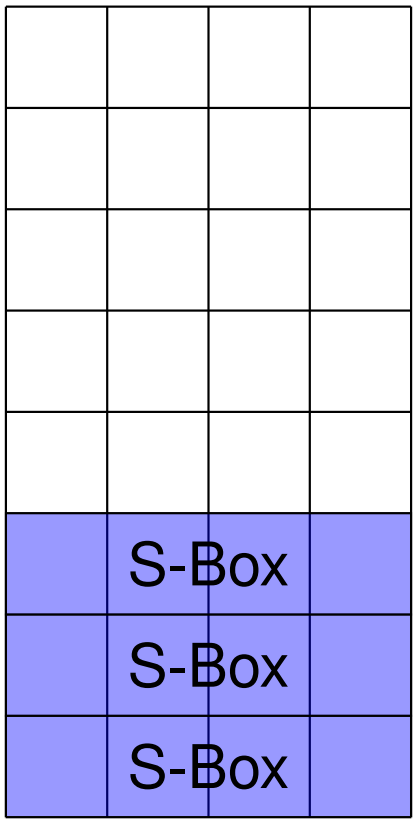
LS-Designs: Structure

- One box is a bit
- Registers correspond to columns



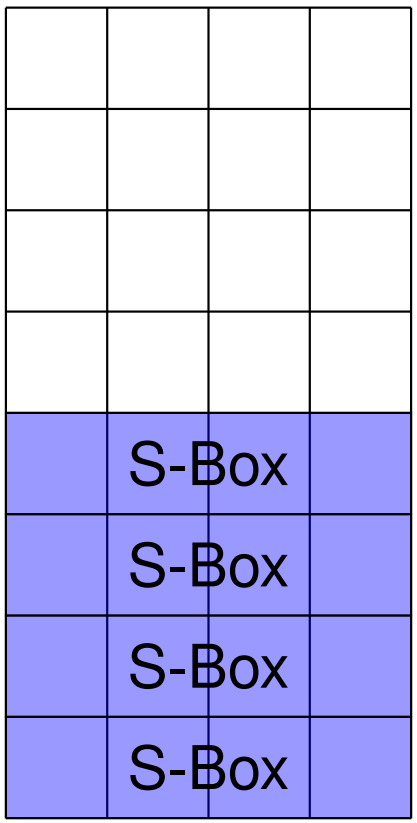
LS-Designs: Structure

- One box is a bit
- Registers correspond to columns



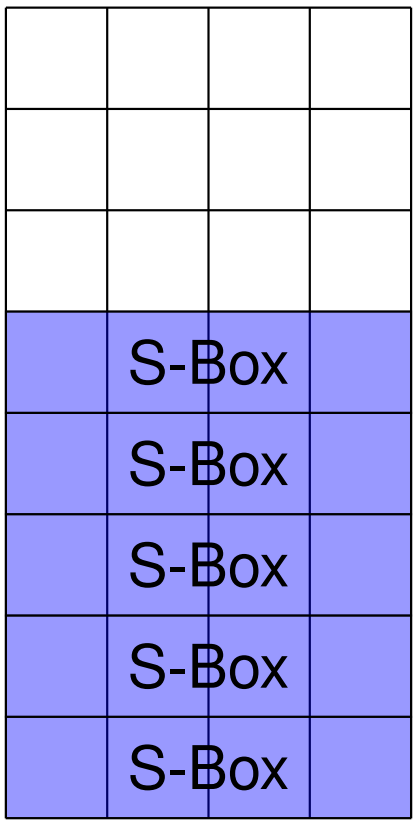
LS-Designs: Structure

- One box is a bit
- Registers correspond to columns



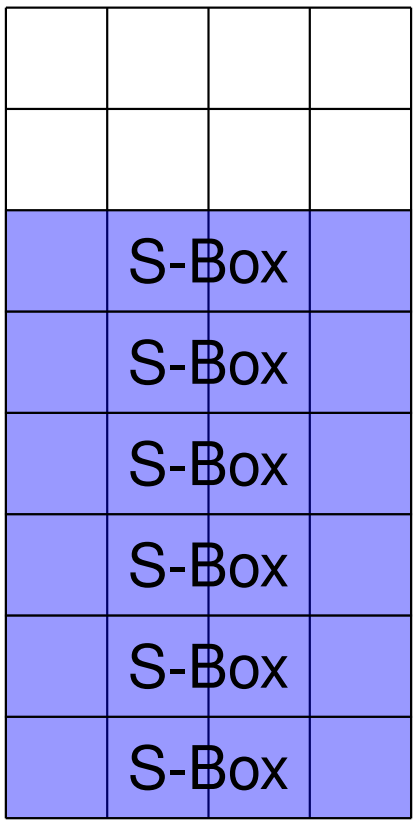
LS-Designs: Structure

- One box is a bit
- Registers correspond to columns



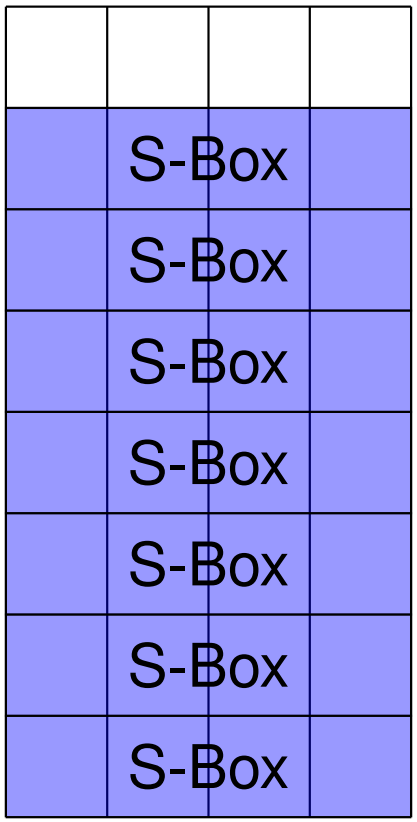
LS-Designs: Structure

- One box is a bit
- Registers correspond to columns



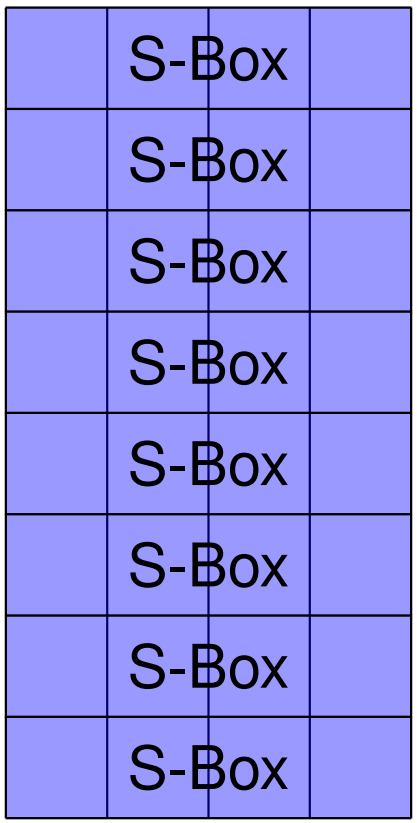
LS-Designs: Structure

- One box is a bit
- Registers correspond to columns



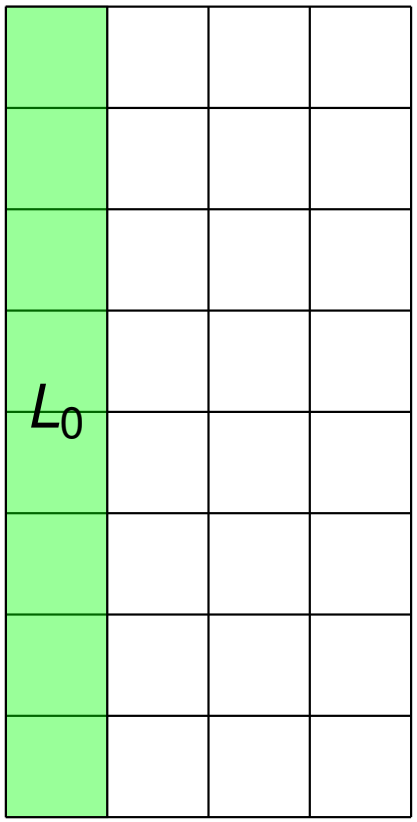
LS-Designs: Structure

- One box is a bit
- Registers correspond to columns



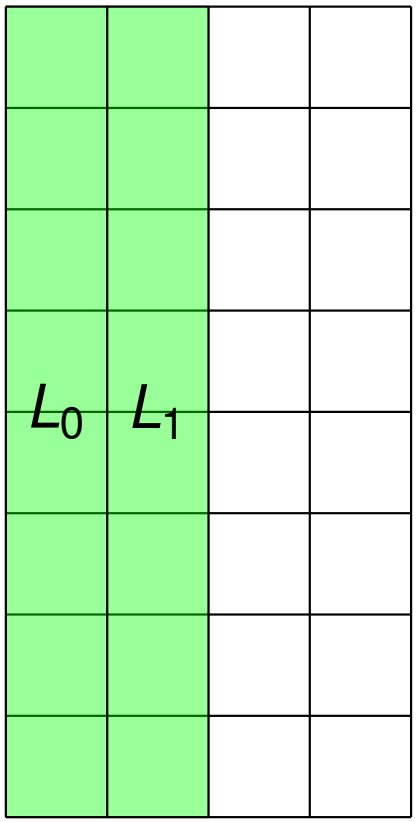
LS-Designs: Structure

- One box is a bit
- Registers correspond to columns



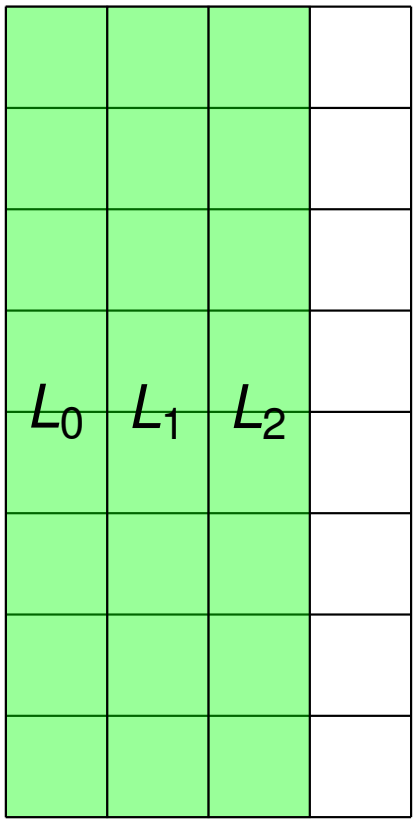
LS-Designs: Structure

- One box is a bit
- Registers correspond to columns



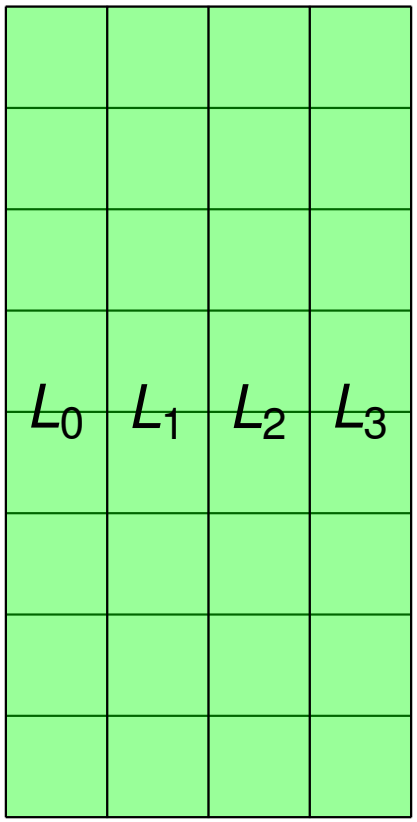
LS-Designs: Structure

- One box is a bit
- Registers correspond to columns



LS-Designs: Structure

- One box is a bit
- Registers correspond to columns



Outline

Conclusion

Lightweight Block Ciphers

An interesting research area

- Interesting problems
- Innovative designs
- New insights

Besides Practical Relevance

Better understanding of block ciphers in general.

The End

Thank you