
Horst-Görtz Institut
für IT Sicherheit

# Performance Analysis of Contemporary Lightweight Block Ciphers on 8-bit Microcontrollers

Sören Rinne, Thomas Eisenbarth, and Christof Paar

Horst Görtz Institute for IT Security

Ruhr-Universität Bochum, Germany

# Overview



1. Motivation
   - Embedded Systems
   - Our Platform
2. Implemented Ciphers
   - Overview of Ciphers
   - Implementation Criteria
3. Results and Comparison
   - Code Size
   - Throughput

# What are Embedded Systems?


+

=

=
**Embedded System**

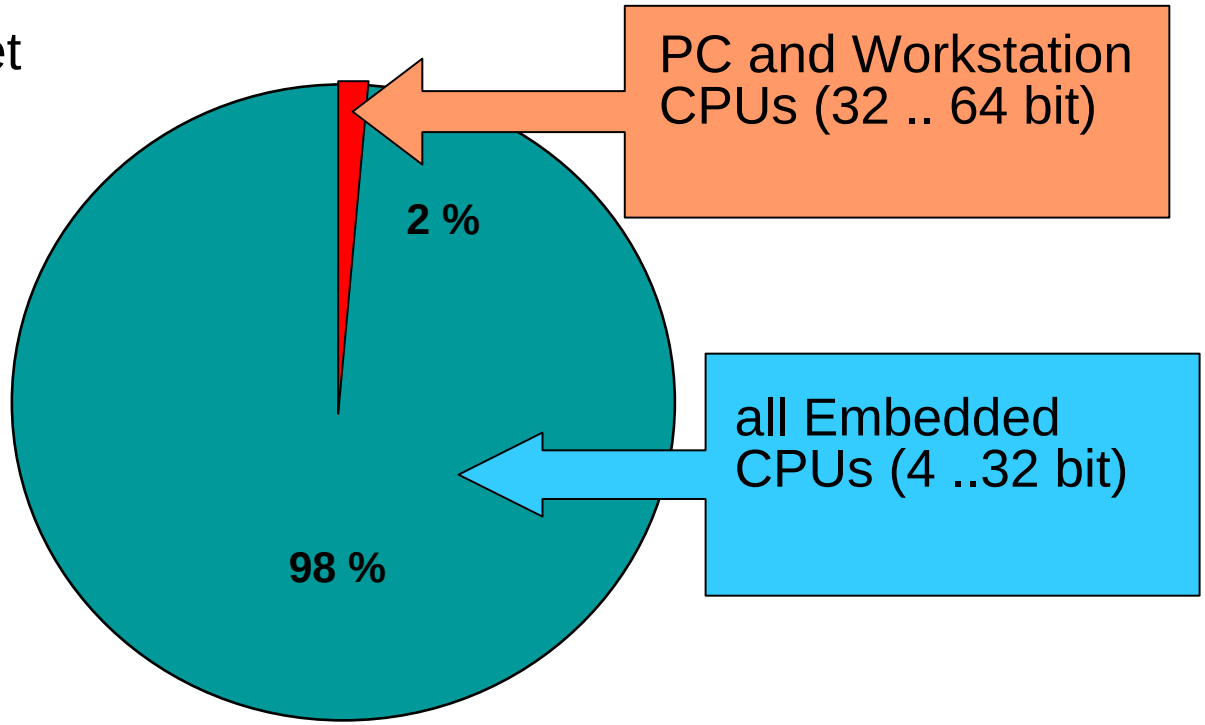
- „Processor hidden in a product“, or
- „A computer that doesn‘t look like a computer“
- Single purpose device
- Interacts with the world



# Is this really important?

Horst-Görtz Institut für IT Sicherheit

Current CPU market by the numbers



# Lightweight Ciphers



Motivation:

- Ubiquitous computing evolves

- New lightweight ciphers are being proposed

Main Question:

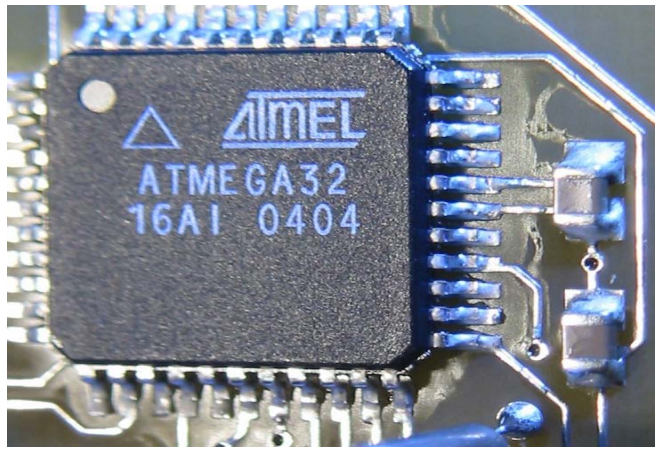
Are lightweight ciphers able to outperform the AES on constrained devices?

# Chosen Platform
# 8-bit Microcontroller



8-bit Atmel AVR processor:

- e.g. ATmega family:
- ~130 instructions, most of them single cycle (RISC architecture)
- 32 general purpose registers of 8 bit size
- 8 - 128 kBytes of program memory (FLASH)
- 1 - 4 kBytes of volatile memory (SRAM)
- several Power Savings modes



# Overview



1. Motivation
   - Embedded Systems
   - Our Platform
2. **Implemented Ciphers**
   - Overview of Ciphers
   - Implementation Criteria
3. Results and Comparison
   - Code Size
   - Throughput

# Discussed Ciphers

Horst-Görtz Institut für IT Sicherheit

| Cipher | Cipher remark | Presented at |
|---|---|---|
| DES(X) | DESX: key whitening | FIPS 46 1976 |
| (X)TEA | Arithmetic operations only | FSE 1994 |
| AES | DES successor | FIPS 197 1997 |
| SEA | Parametric in text, key and processor size | ECRYPT Workshop 2005 |
| HIGHT | 8-bit oriented, high throughput | CHES 2006 |
| DES-L | Single S-Box design | FSE 2007 |
| PRESENT | Small outline SPN | CHES 2007 |

| Cipher | DES | DESX | TEA | XTEA | AES | SEA | HIGHT | DES-L | PRESENT |
|---|---|---|---|---|---|---|---|---|---|
| Block length | 64 | 64 | 64 | 64 | 128 | 96 | 64 | 64 | 64 |
| Key length | 56 | 184 | 128 | 128 | 128 | 96 | 128 | 56 | 80 |
| Rounds | 16 | 16 | 32 | 32 | 10 | 141 | 32 | 16 | 32 |

# PRESENT

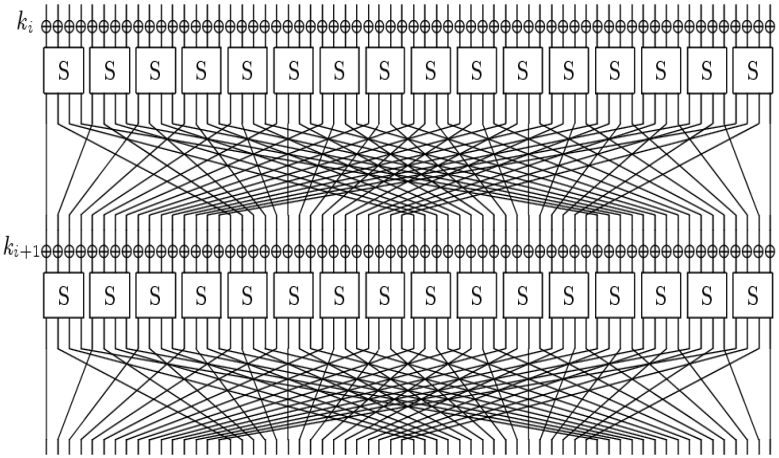



Fig. 1. . The S/P network for PRESENT.

Hard facts:

- 64 Bit block length
- 80 Bit key length
- 32 rounds

Performed operations:

- XOR with key
- 4x4 bit S-Box
- Bit permutation

Designed for hardware implementation

# Design Criteria

Major design goal of embedded devices : Low Costs

Security:

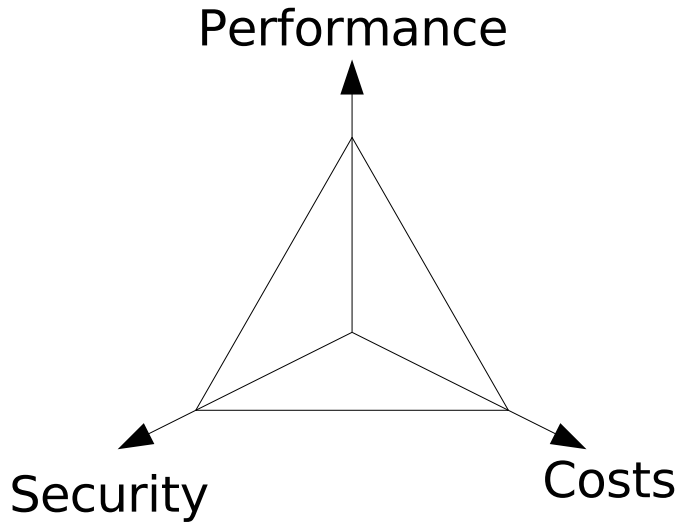
- Lightweight Crypto

Performance:

- Small Payloads
- Response Time

Cost:

- Device Cost
- Overall System Cost



# Implementation Step



Performance:

Response time and availability

Device cost:

small code size → cheaper device

System cost:

wireless devices → power consumption

Execution time is cost in energy storage!!!

We focus on cost: **code size-performance trade off**

# Overview



1. Motivation
   - Embedded Systems
   - Our Platform
2. Implemented Ciphers
   - Overview of Ciphers
   - Implementation Criteria
3. **Results and Comparison**
   - Code Size
   - Throughput

# Results - Our Implementations

Horst-Görtz Institut für IT Sicherheit

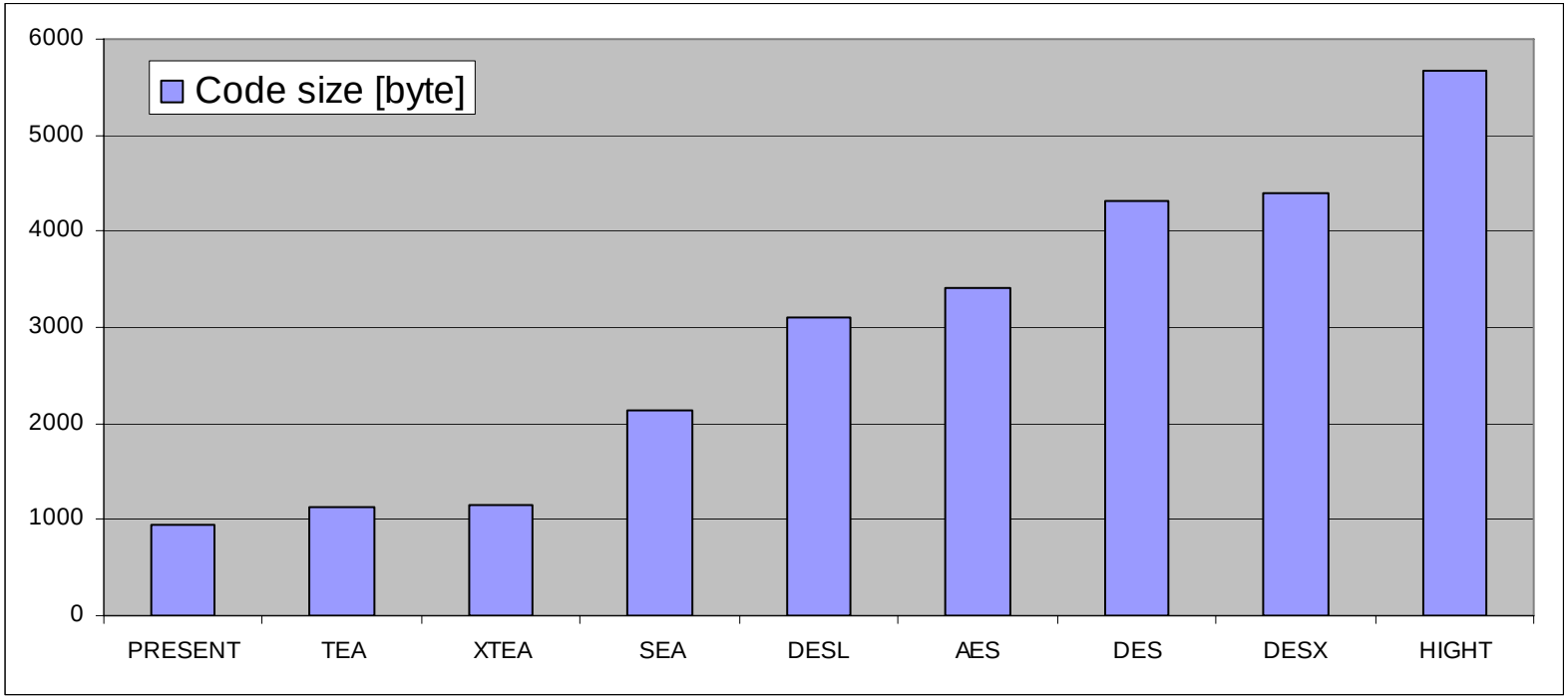
Ciphers implemented in Assembly language

- reduces code size
- yields higher performance

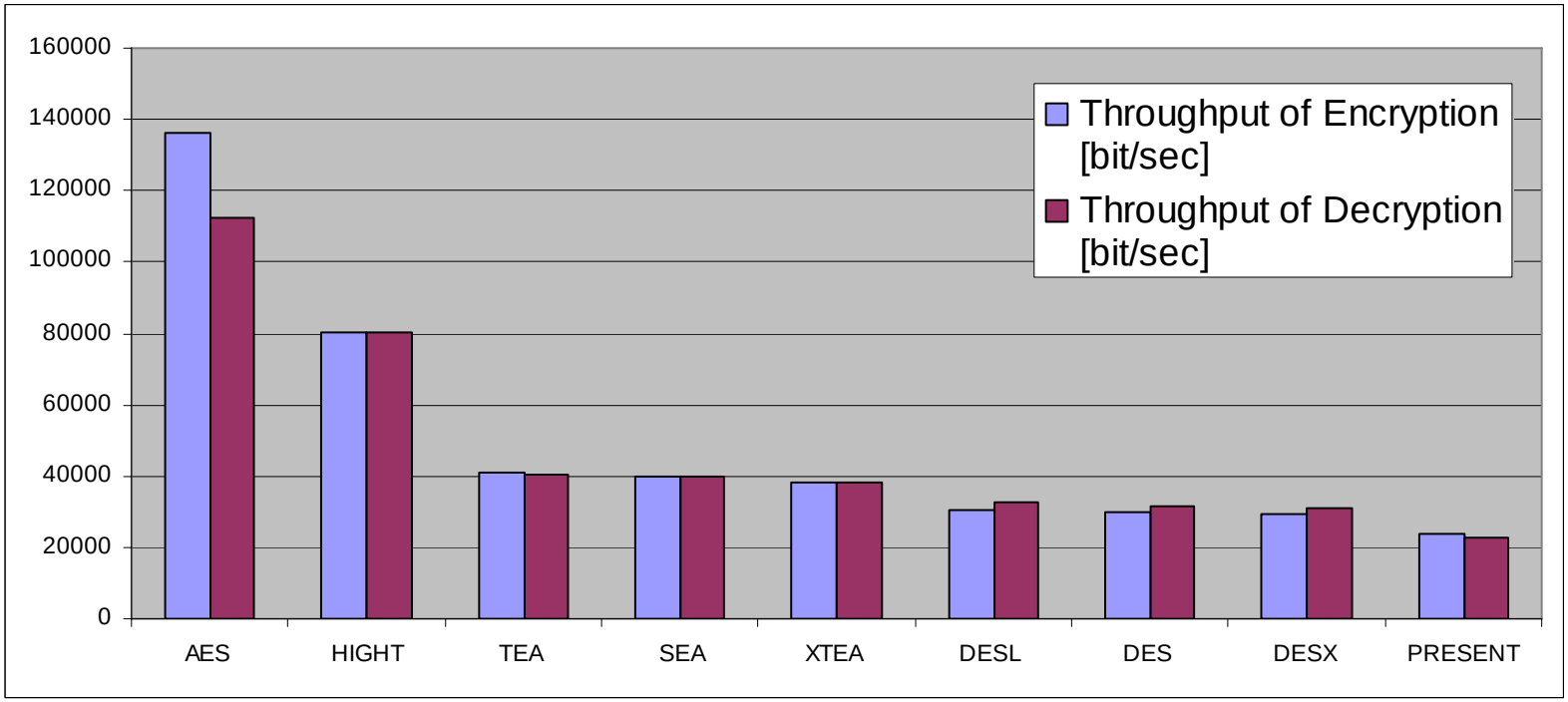
Keep code size small wherever performance is not reduced too much.

- Keep all states in registers
- on the fly key scheduling (no SRAM usage)
- only small LUTs (8-bit S-boxes) that give a good performance – code-size tradeoff
- no macros (no loop unrolling)

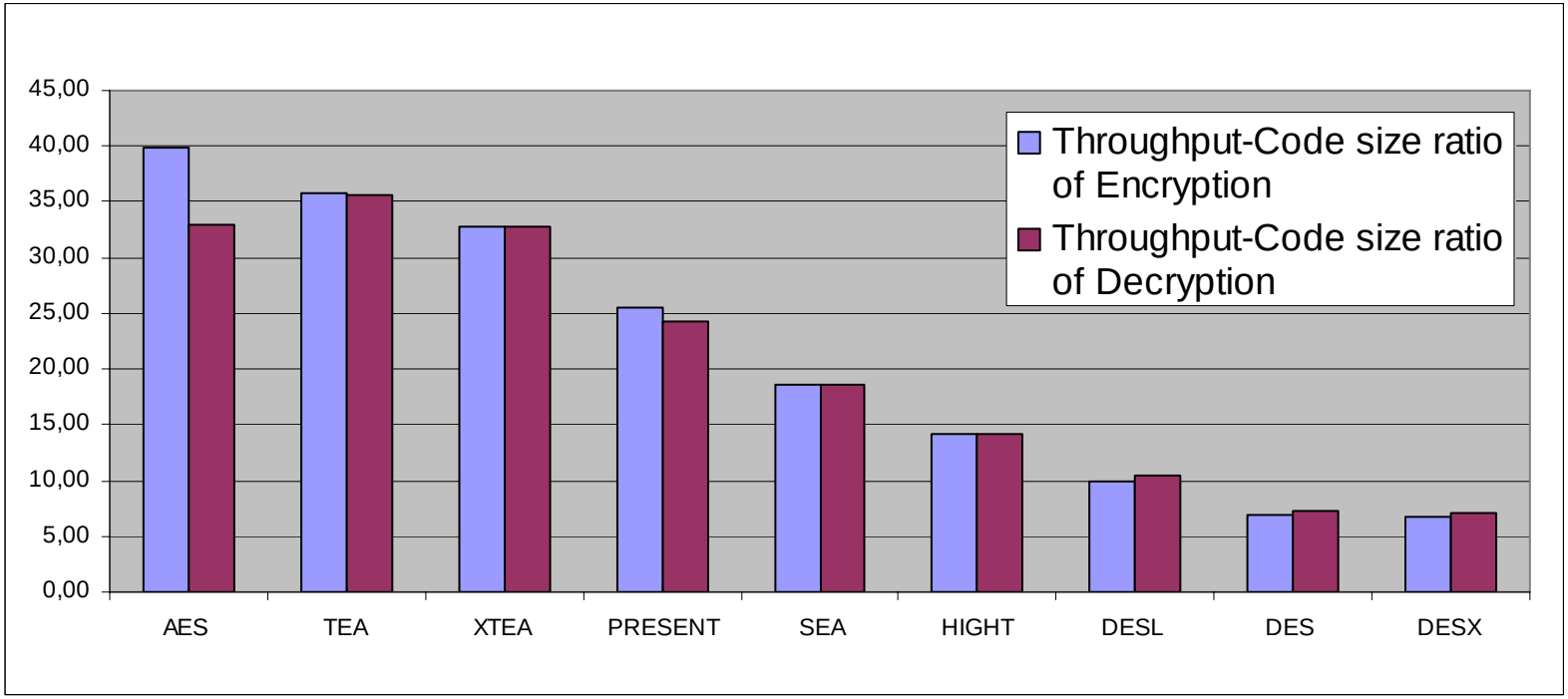
# Results – Code Size



# Results – Throughput



# Results – Throughput- Code Size Ratio



# Concluding Remarks

Horst-Görtz Institut für IT Sicherheit

Generally AES seems to be the best allround choice.

For small code size (X)TEA and even PRESENT seem to be a decent choice

Results will be put on the web, together with other implementations for the focused platform:

www.lightweightcrypto.org



# Thanks for your attention!

eisenbarth@crypto.rub.de