Lightweight Crypto Design Principles
- Approaches and Limitations

Axel Poschmann
Division of Mathematical Sciences
School of Physical and Mathematical Sciences

August 31, 2011
Agenda

- Motivation
- Background
- AES
- PRESENT
- LED
- EPCBC
- Conclusions
Motivation

past
Mainframe

present
Personal

future
Pervasive

• Wireless communication
• Cost-driven deployment
• Devices are constrained
  • code size/area
  • CPU
  • power/energy
Evolution of Lightweight Block Ciphers

How?

-55%

-93%

standardized BC, $|k| = 128$

dedicated lightweight BC, $|k| = 80$

flexible key management

fixed key

Axel Poschmann

Lightweight Crypto Design Principles

31.08.2011
Questions

How to Design Lightweight Crypto Primitives?

• How to make it small?
• How to make it secure?
• How to make it fast?
• How low can we go?
Agenda

- Motivation
- Background
- AES
- PRESENT
- LED
- EPCBC
- Conclusions
Trade-offs

- Security
- Key length + state
- Rounds
- 256 bits
- 48
- 56 bits
- 16

Low-Cost
- serial
- Architecture

Performance
- parallel
Gate Equivalent (GE)

**NAND**

<table>
<thead>
<tr>
<th>A1</th>
<th>A2</th>
<th>Z</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

**Standard Cells**
UMCL18G212T3

**HDNAN2D1**
9.677 µm²

**Athlon XP**
13.24 Mio GE

1 GE
### Hardware Complexities

<table>
<thead>
<tr>
<th>Gate</th>
<th>GE</th>
</tr>
</thead>
<tbody>
<tr>
<td>NOT</td>
<td>0.67</td>
</tr>
<tr>
<td>NAND, NOR</td>
<td>1</td>
</tr>
<tr>
<td>AND, OR</td>
<td>1.33</td>
</tr>
<tr>
<td>XOR</td>
<td>2.67</td>
</tr>
<tr>
<td>2-1-MUX</td>
<td>2.33</td>
</tr>
</tbody>
</table>

- **1-input FF**: $2.33 + 4.67 = 7$
- **2-input FF**: a.k.a. Scan-FF 6
- **Bit permutations**: 0
- **wiring**
Example: S-Boxes in Hardware

- LUT = Boolean functions
- highly non-linear
- High Boolean Complexity
- Large area

8 x 8
6 x 4
4 x 4
Agenda

- Motivation
- Background
- AES
- PRESENT
- LED
- EPCBC
- Conclusions
AES - Advanced Encryption Standard

- THE general purpose symmetric encryption standard
- Successor of DES
- NIST standard since 2001
- Substitution-Permutation Network
- 128-bit block size
- 128/192/256 bit key length, 10/12/14 rounds
- SubBytes = 16 identical 8-bit S-boxes
- ShiftRows is a simple byte-wise rotation
- MixColumns uses an MDS matrix
Hardware Architectures - S-Box
Hardware Architectures - S-Box

S(x) = x⁻¹, x in GF(2⁸), S(0) = 0

Composite Field

Based on Canright’s Design

SubBytes  233 GE
           16 CLK
Hardware Architectures - State Array
Hardware Architectures - State Array

ShiftRows 0 GE
1 CLK

MixColumns 373 GE
4 CLK

FFs 768 GE
MUXes 150 GE
Hardware Architectures - Key Array
Hardware Architectures - Key Array

- FFs: 768 GE
- RotWord: 0 GE
- SubWord: 0 GE
- Add RCon: 35 GE
- Feedback: 30 GE
AES Optimization Summary

✦ Design goal:
  • low area

✦ Design Strategy:
  • Consequently exploiting Scan Flip-Flops
  • Optimizing for the global minimum
    - MixColumns not serialized
  • Minimizing the control logic
    - 16+4+1=21 cycle LFSR
  • Slight modification of the I/O byte order
    - Saves 373 GE
Agenda

• Motivation
• Background
• AES
• PRESENT
• LED
• EPCBC
• Conclusions
PRESENT

- Substitution-Permutation Network
- 64-bit block size, 80/128 bit key length, 31 rounds
- S-layer = 16 identical 4-bit S-boxes
- P-Layer is a bit permutation = no cost in hardware
- under standardization (ISO 29192-2)
PRESENT-80 Key Schedule

- simple design
- 61-bit left rotation = no cost in hardware
- same S-box as in datapath
- round counter used to thwart slide attacks
PRESENT HW Implementation

data_in

key

State

P-Layer

S-Box

FSM

data_out

PRESENT-80/4

crypto

1030 GE

516 CLK

PRESENT-4/64

PRESENT-4/80

k_{i+1}

k_i

86%

8%

counter

n_reset

done

1030 GE

516 CLK

Axel Poschmann

Lightweight Crypto Design Principles
Agenda

- Motivation
- Background
- AES
- PRESENT
- LED
- EPCBC
- Conclusions
LED - Light Encryption Device

- Substitution-Permutation Network
- 64-bit block size
- 64-128 bit key length, 32/48 rounds
- No Keyschedule allows hard wiring of the key
- SubBytes = 16 identical 4-bit S-boxes
- ShiftRows is a simple nibble-wise rotation
- MixColumnsSerial uses a serialized MDS matrix
LED-80 HW Implementation

- serialized MDS saves 120 GE
- large control logic
- no key schedule allows hard-wiring

1040 GE

1268 CLK

Axel Poschmann

Lightweight Crypto Design Principles
Agenda

• Motivation
• Background
• AES
• PRESENT
• LED
• EPCBC
• Conclusions
EPCBC - Electronic Product Code Block Cipher

- Substitution-Permutation Network
- 96 bit key length, 32 rounds
- 48/96-bit block size
- Block size optimized for Electronic Product Code
- Based on PRESENT
EPC-96/96 HW Implementation

1333 GE

792 CLK
EPC-48/96 HW Implementation

1008 GE
396 CLK

Axel Poschmann
Lightweight Crypto Design Principles
31.08.2011
Agenda

• Motivation
• Background
• AES
• PRESENT
• LED
• EPCBC
• Conclusions
Internal State vs. Area

- **PRESENT**
- **KATAN**
- **EPCBC**
- **LED**
- **KTANTAN**
- **PRINTcipher**
- **AES**

Graph showing the relationship between internal state and area for different cryptographic algorithms.
Internal State vs. Area

fixed key | flexible key

<table>
<thead>
<tr>
<th>Internal State</th>
<th>Area</th>
</tr>
</thead>
<tbody>
<tr>
<td>192</td>
<td></td>
</tr>
<tr>
<td>160</td>
<td></td>
</tr>
<tr>
<td>128</td>
<td></td>
</tr>
<tr>
<td>96</td>
<td></td>
</tr>
<tr>
<td>64</td>
<td></td>
</tr>
<tr>
<td>32</td>
<td></td>
</tr>
</tbody>
</table>

PRESENT | KATAN | EPCBC | LED | KTANTAN | PRINTcipher

Axel Poschmann  Lightweight Crypto Design Principles  31.08.2011
Conclusions

Lessons learned

• Minimize internal state (key length + block size)
• Use as small S-boxes as possible
• Use 1- and 2-input FFs whenever possible
• Minimize control logic (keep it as regular as possible)
• Choose I/O accordingly
Conclusions

Outlook

• Can we go further?
  – Probably not much wrt area

• What next?
  – Increase throughput
  – HW **AND** SW efficiency
  – Hash functions (PHOTON, SPONGENT)
  – Asymmetric Crypto
  – Lightweight Side Channel Countermeasures
    • Temasek Lab on SCA @ NTU
References


Thank You!

Questions?

Axel Poschmann
Division of Mathematical Sciences
Nanyang Technological University
SPMS-MAS-05-01, 50 Nanyang Avenue
Singapore 639798
T (65) 6514-8399 GMT+8h
E axel.poschmann@gmail.com
W www.ntu.edu.sg/home/aposchmann/