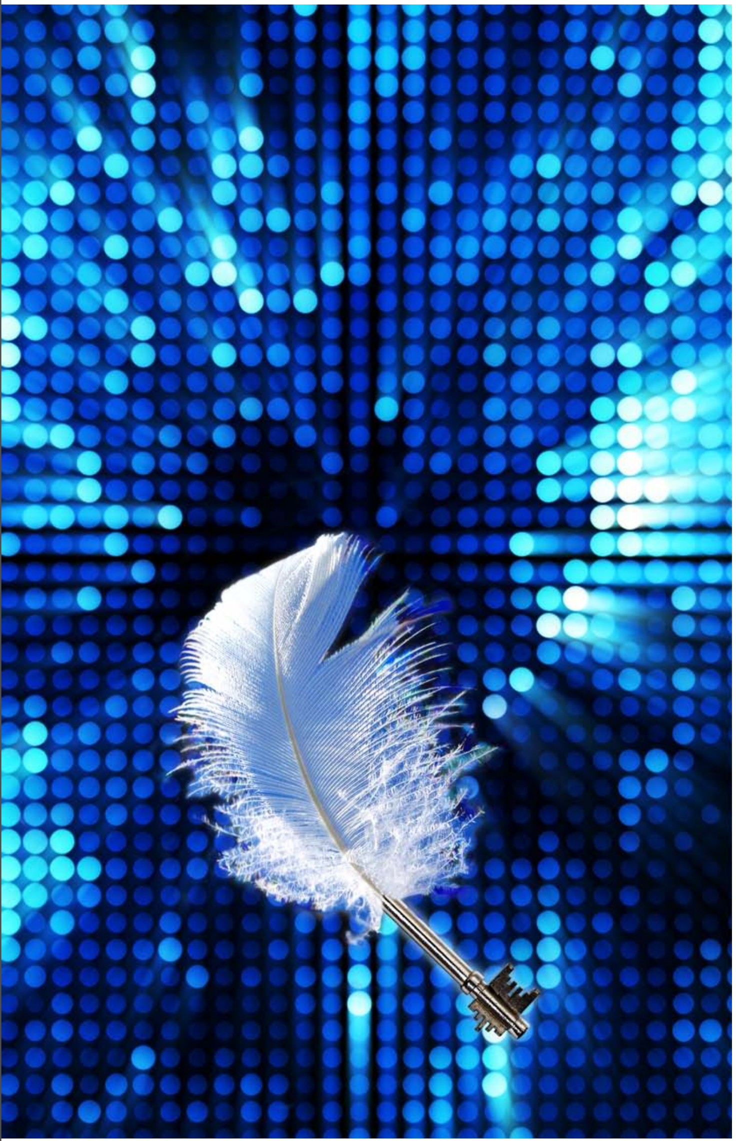
NANYANG TECHNOLOGICAL UNIVERSITY

Lightweight Crypto Design Principles - Approaches and Limitations

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

August 31, 2011



Agenda

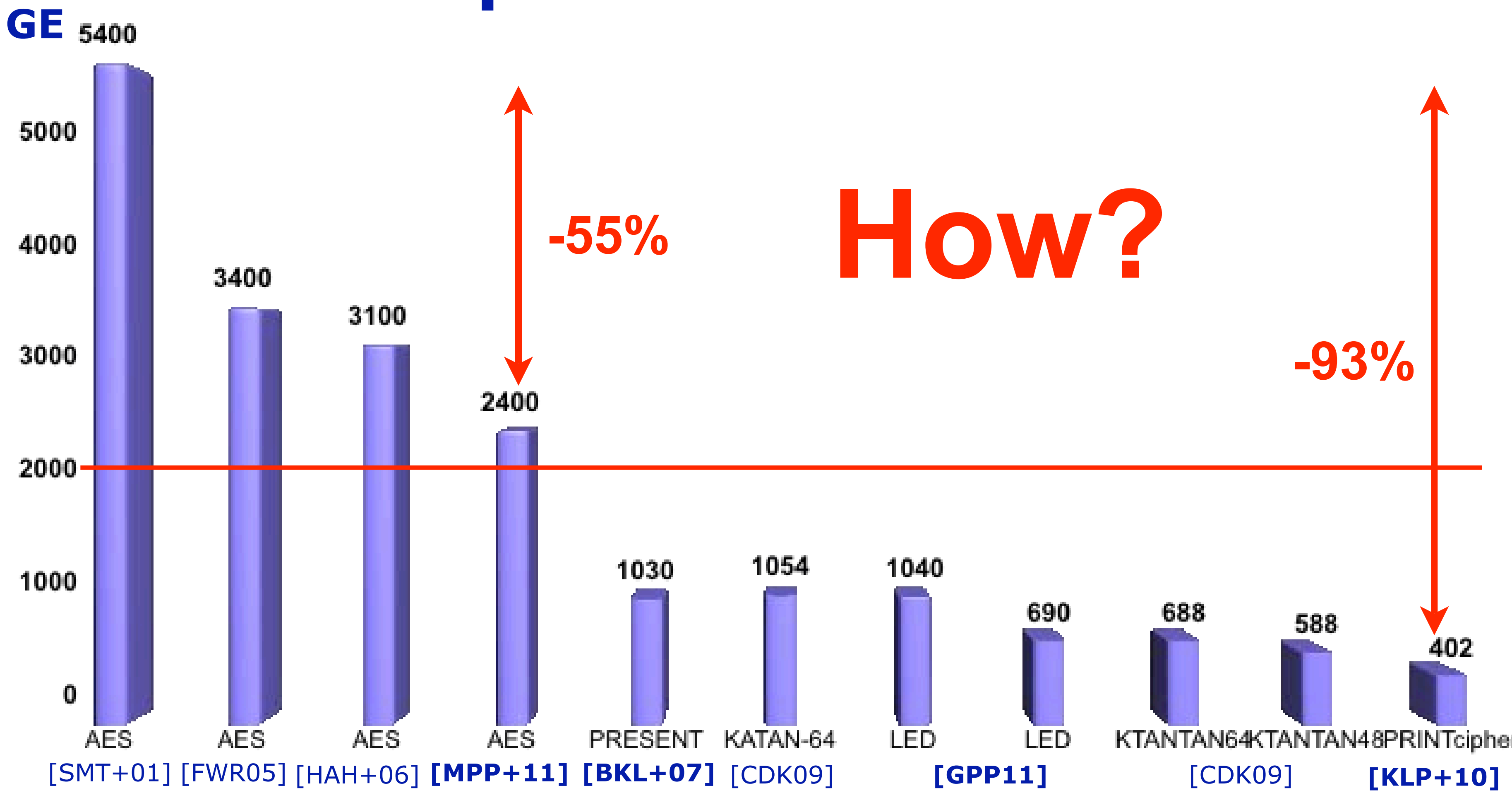
- **Motivation**
- Background
- AES
- PRESENT
- LED
- EPCBC
- Conclusions

Motivation

past	present	future
		
Mainframe	Personal	Pervasive

- Wireless communication
- Cost-driven deployment
- Devices are constrained
  - code size/area
  - CPU
  - power/energy

Evolution of Lightweight Block Ciphers



standardized BC, |k|=128

dedicated lightweight BC, |k|=80

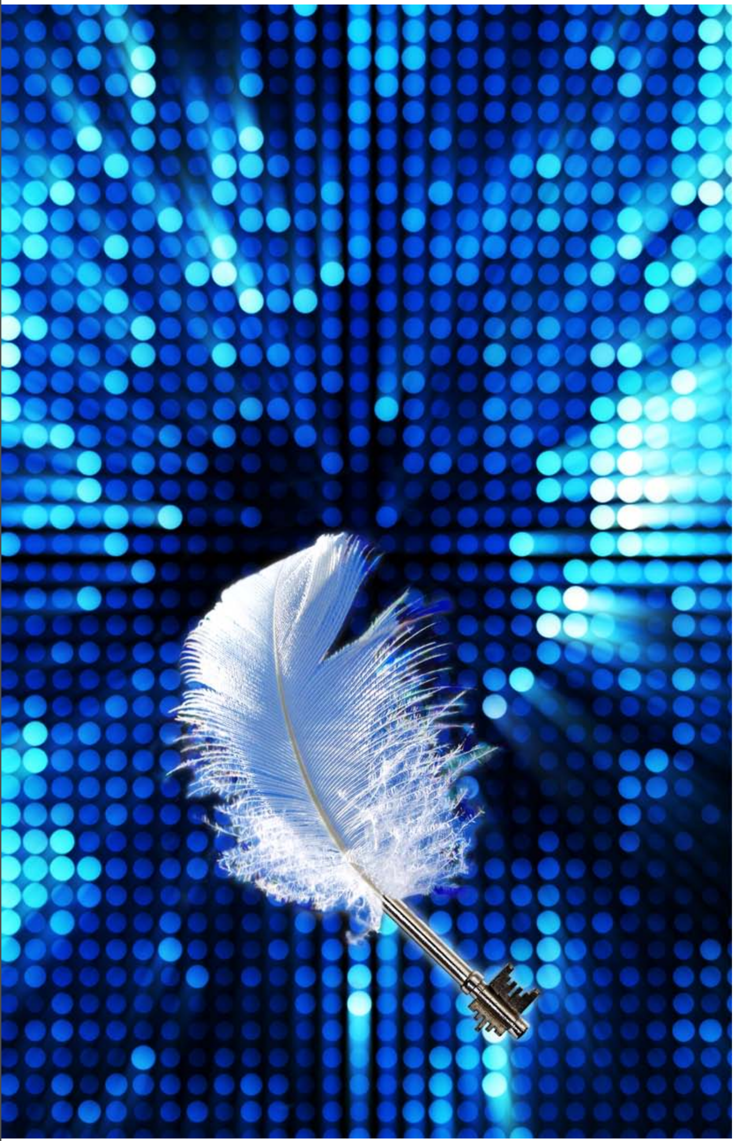
flexible key management

fixed key

Questions

How to Design Lightweight Crypto Primitives?

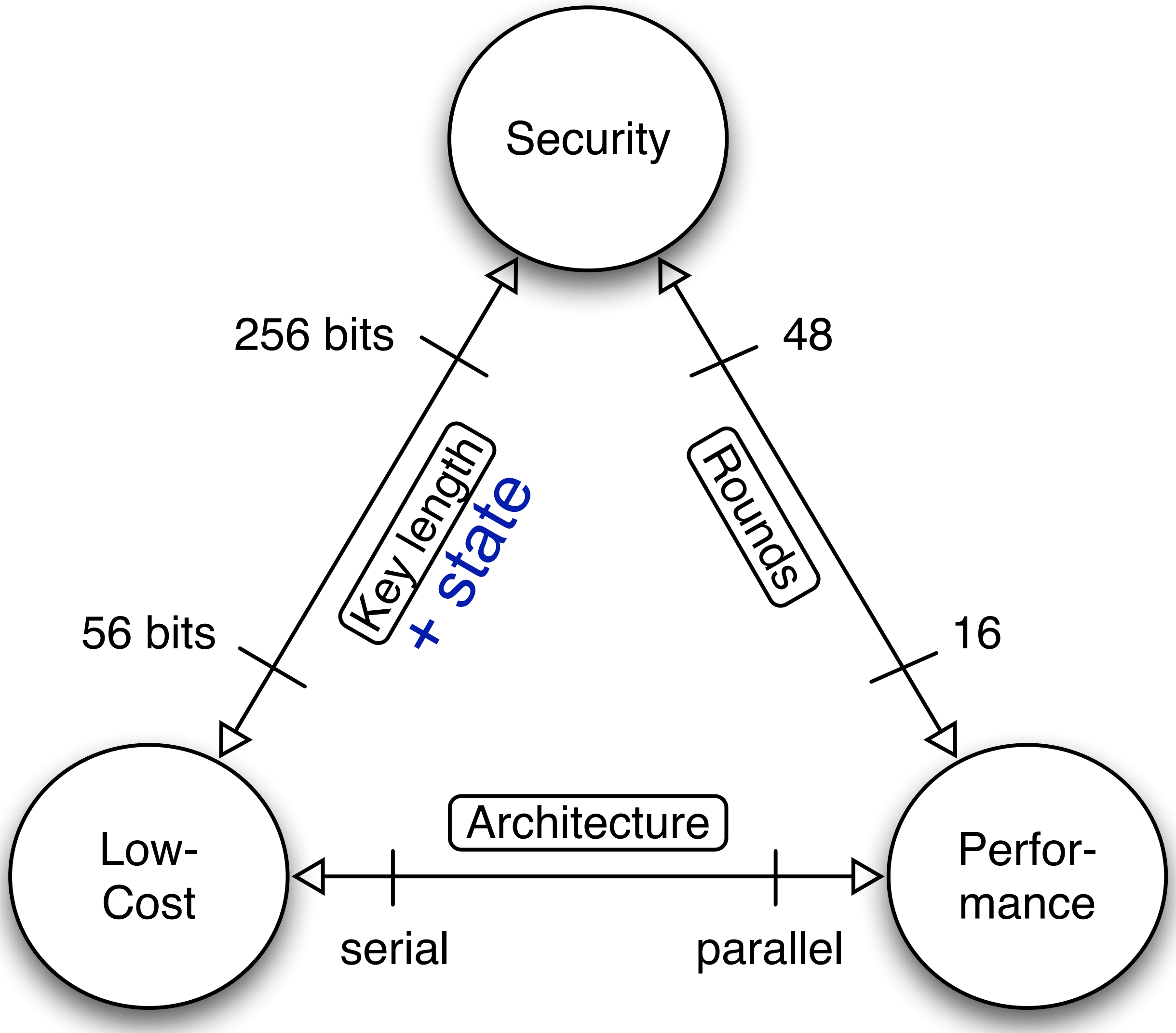
- How to make it small?
- How to make it secure?
- How to make it fast?
- How low can we go?



Agenda

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

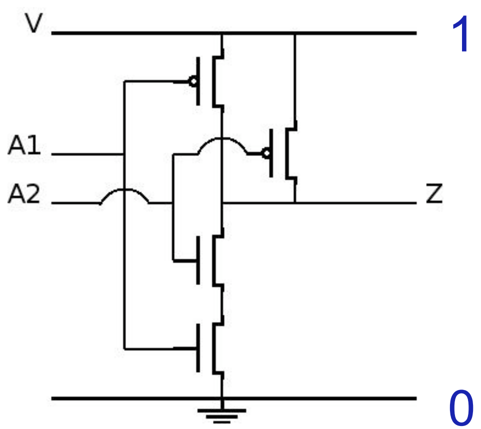
Trade-offs



Security
Low-Cost
Performance
Key length
+ state
256 bits
56 bits
Rounds
48
16
Architecture
serial
parallel

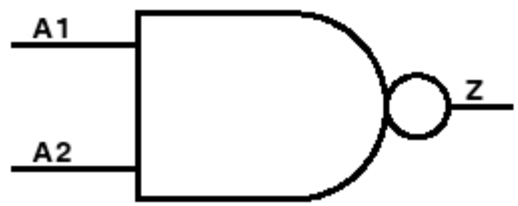
Gate Equivalent (GE)

NAND



A1	A2	Z
0	0	1
0	1	1
1	0	1
1	1	0

Standard Cells
UMCL18G212T3



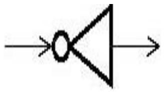
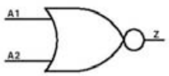
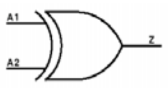
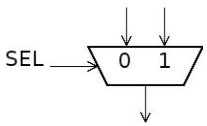
HDNAN2D1
9.677 µm²

1 GE

Athlon XP

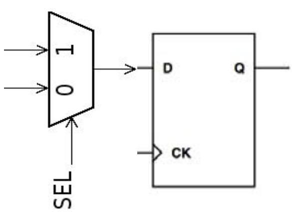
13.24 Mio GE

Hardware Complexities

	Gate	GE
	NOT	0.67
	NAND, NOR	1
	AND, OR	1.33
	XOR	2.67
	2-1-MUX	2.33

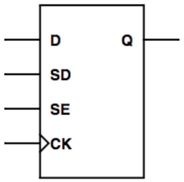
combinational logic

1-input FF



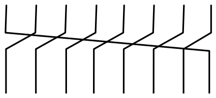
2.33 + 4.67 = 7

2-input FF



a.k.a. Scan-FF 6

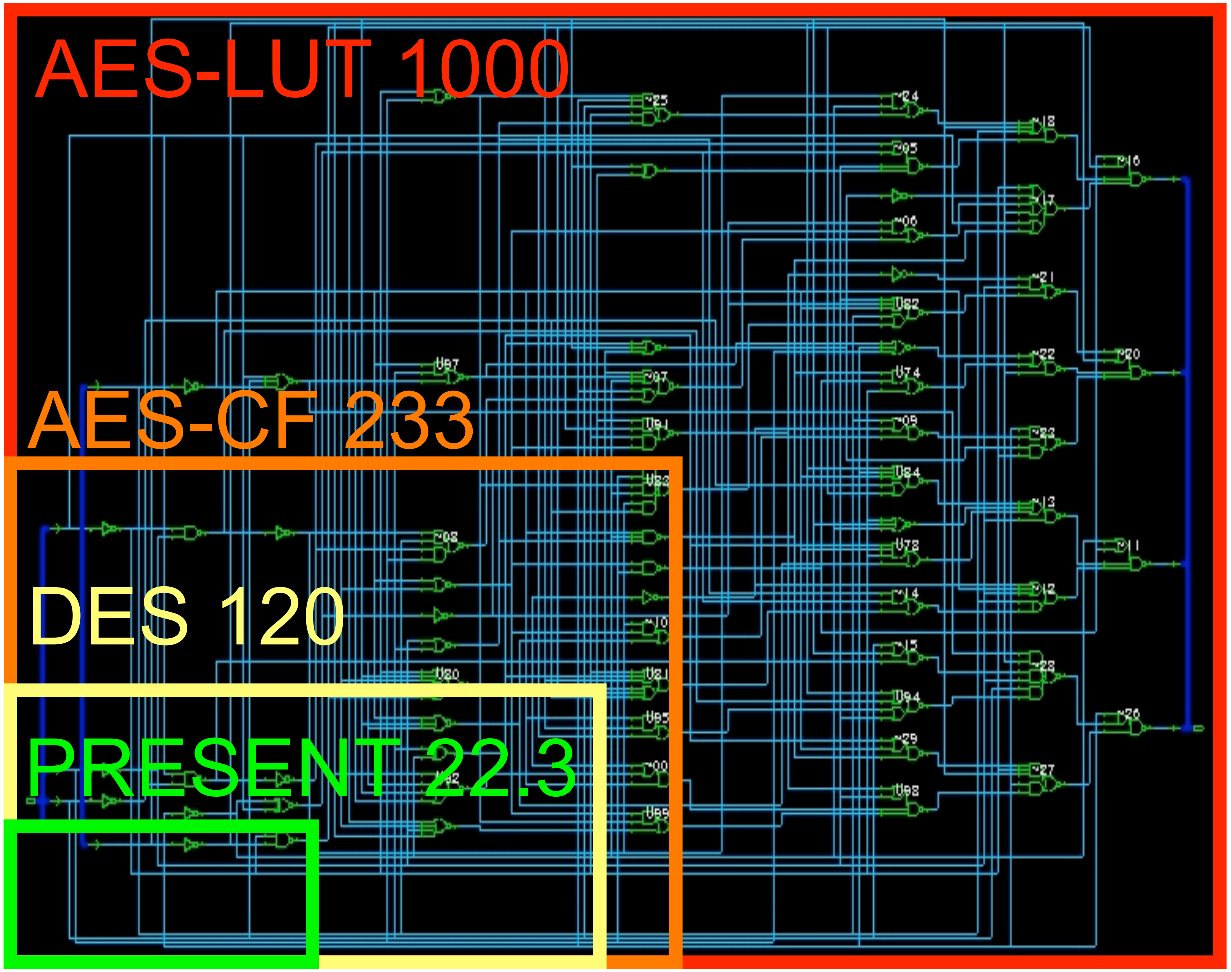
sequential logic



Bit permutations 0

wiring

Example: S-Boxes in Hardware

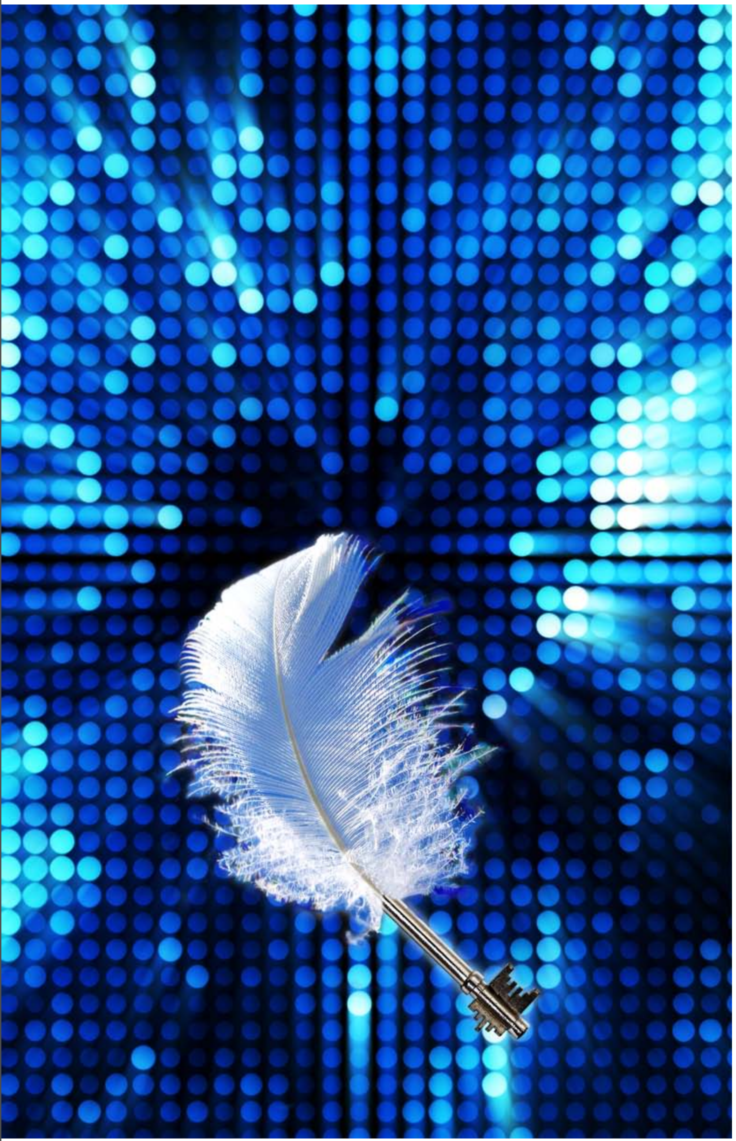


- LUT = Boolean functions
- highly non-linear
- High Boolean Complexity
- Large area

8 x 8

6 x 4

4 x 4



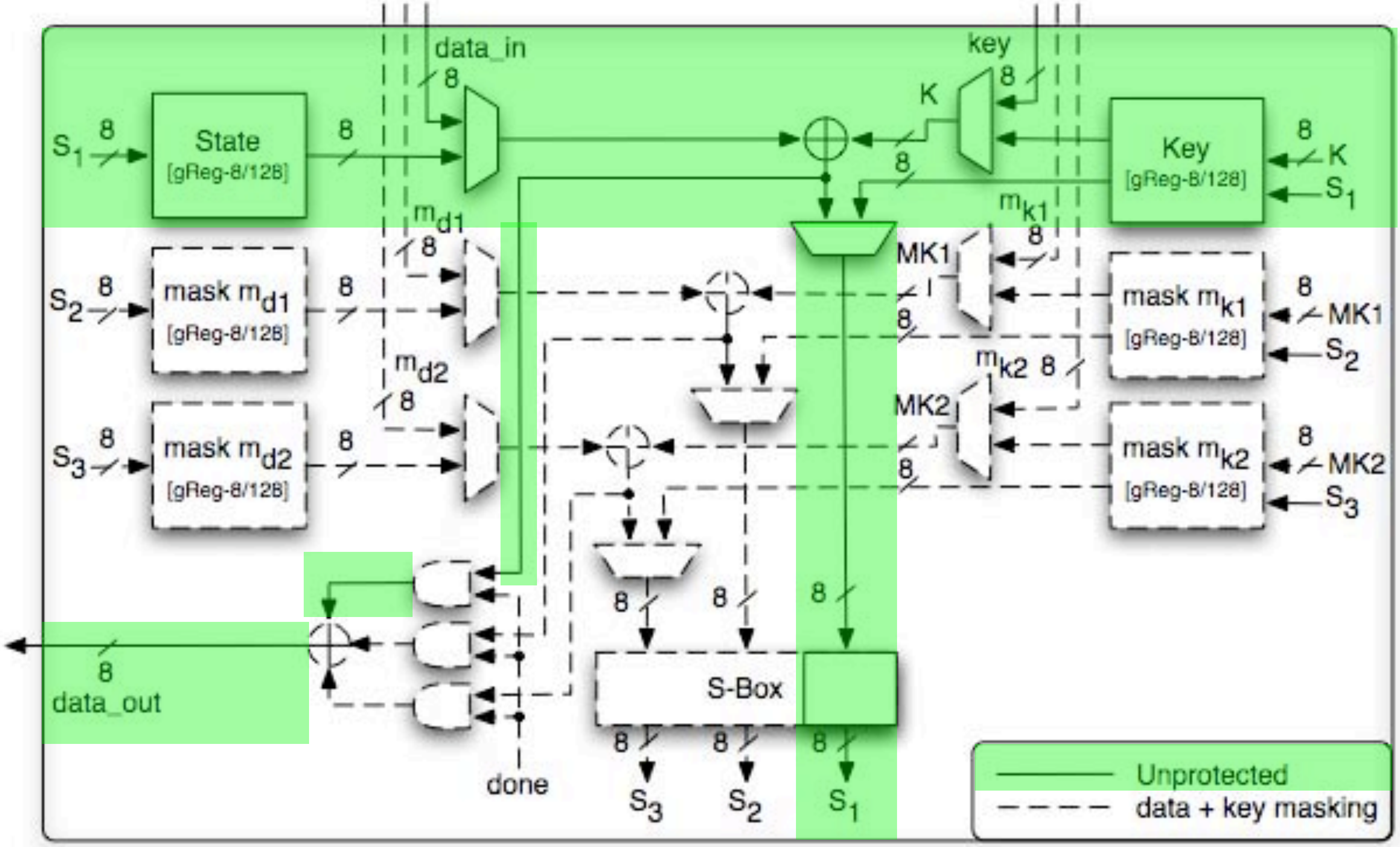
Agenda

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

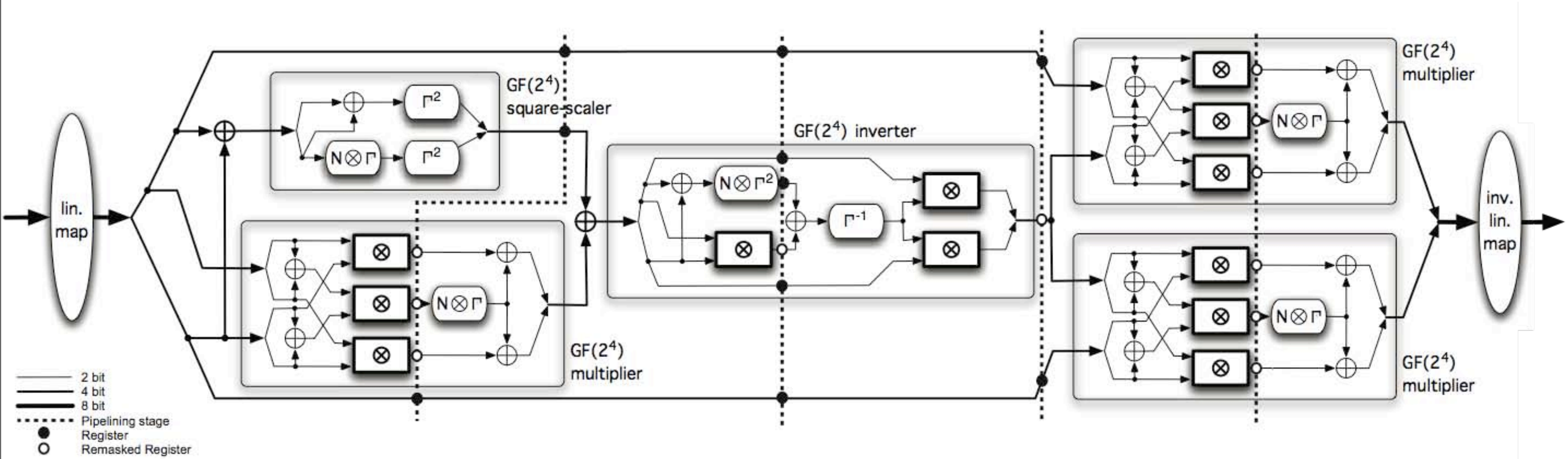
AES - Advanced Encryption Standard

- 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



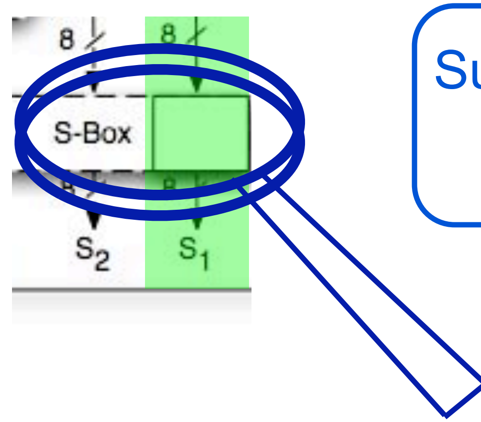
Hardware Architectures - S-Box



$S(x) = x^{-1}$, x in GF(2^8), S(0) = 0

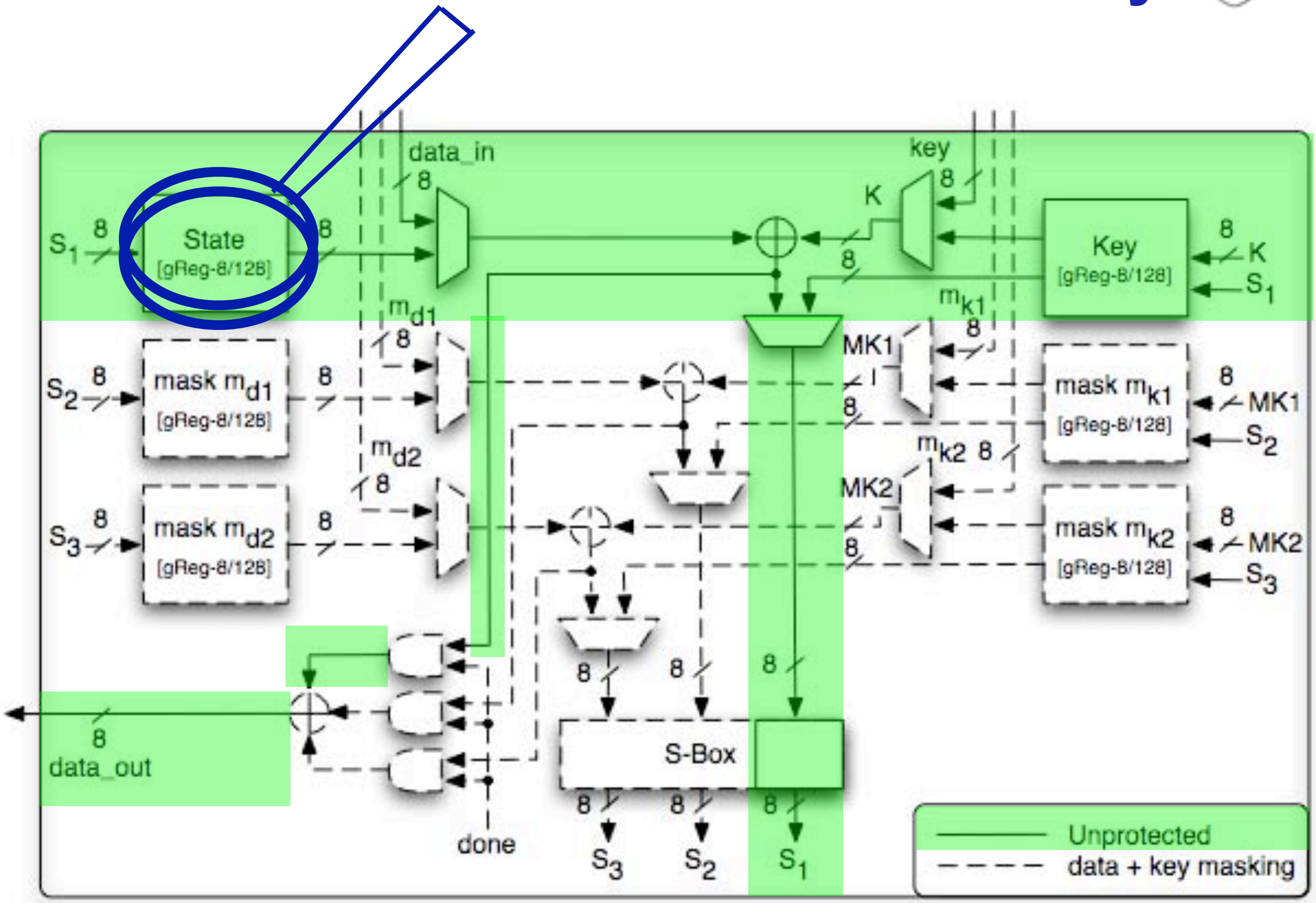
Composite Field

Based on Canright‘s Design

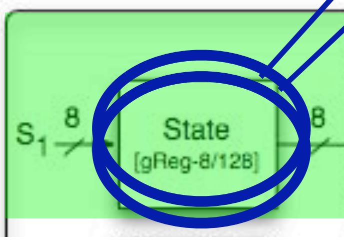


SubBytes	233 GE
	16 CLK

Hardware Architectures - State Array

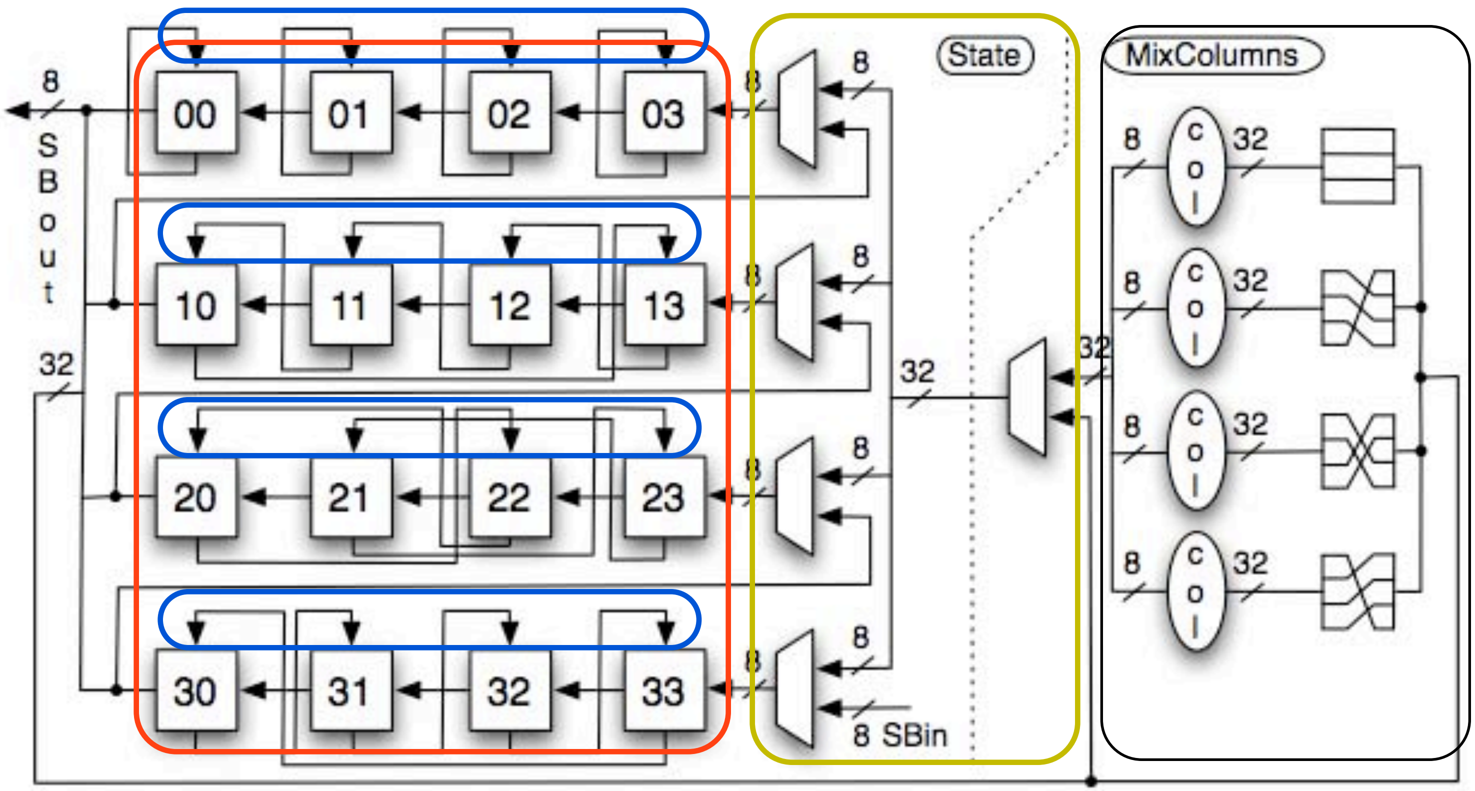


Hardware Architectures - State Array



ShiftRows	0 GE
	1 CLK

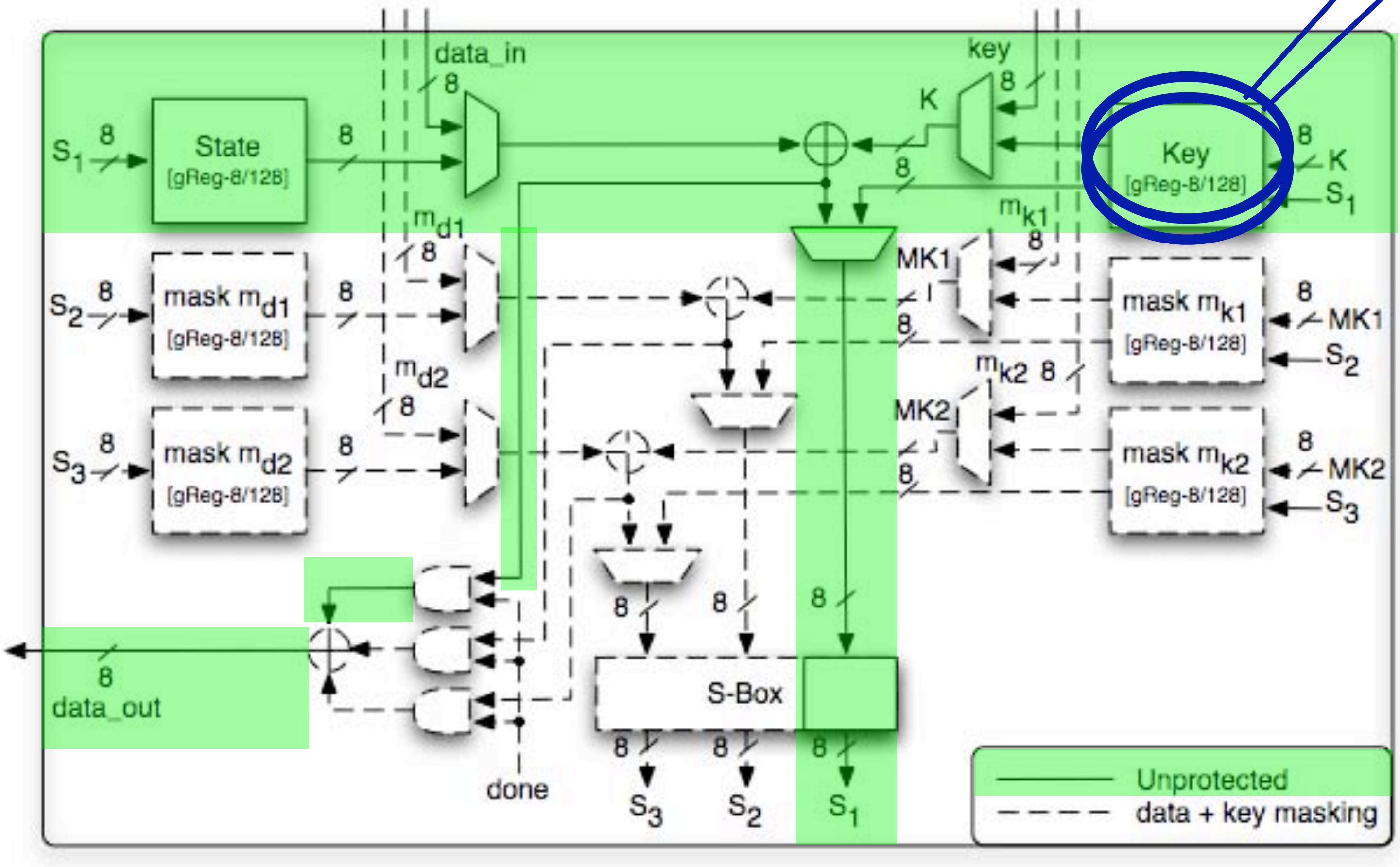
MixColumns	373 GE
	4 CLK



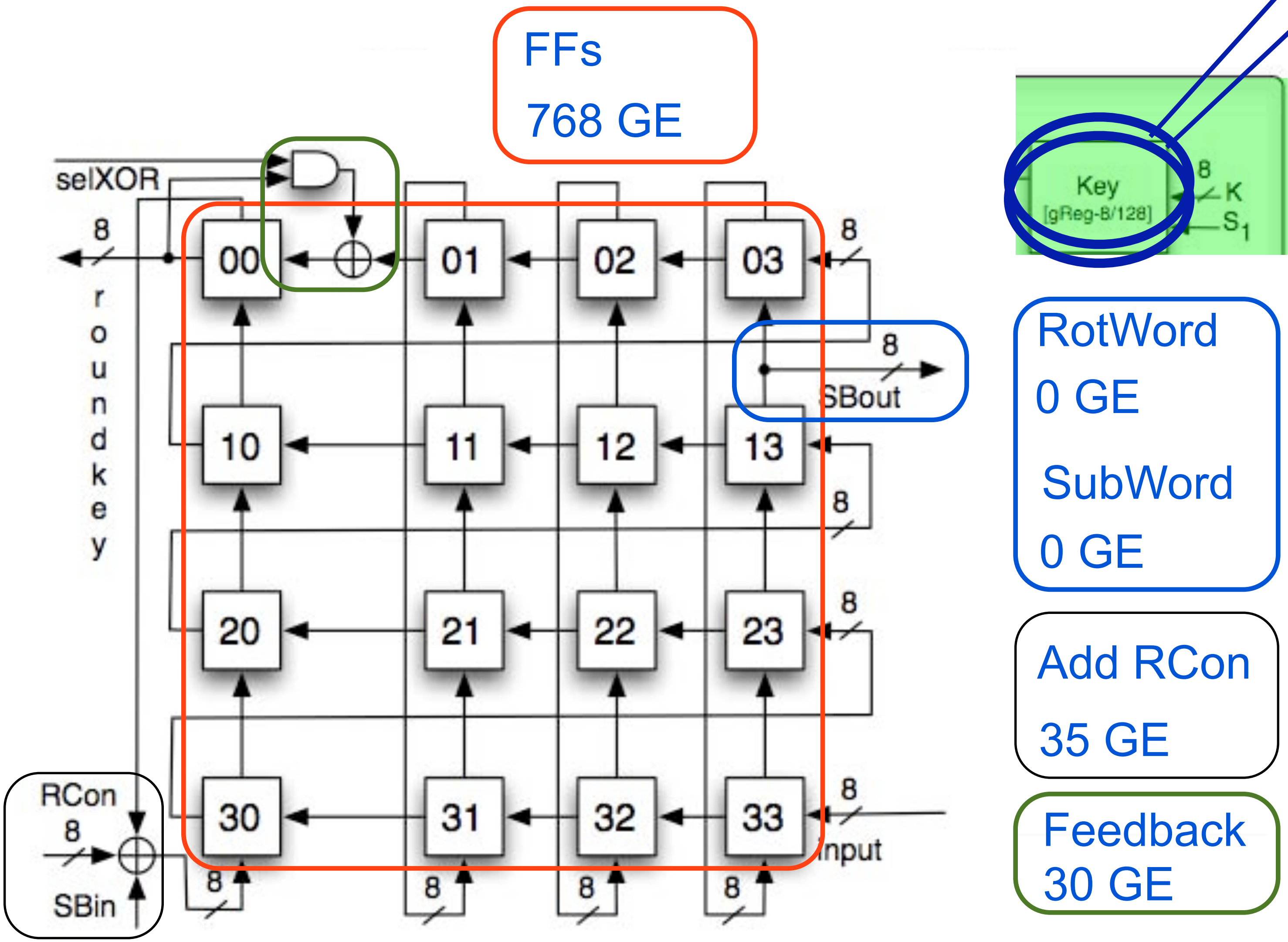
FFs
768 GE

MUXes
150 GE

Hardware Architectures - Key Array



Hardware Architectures - Key Array



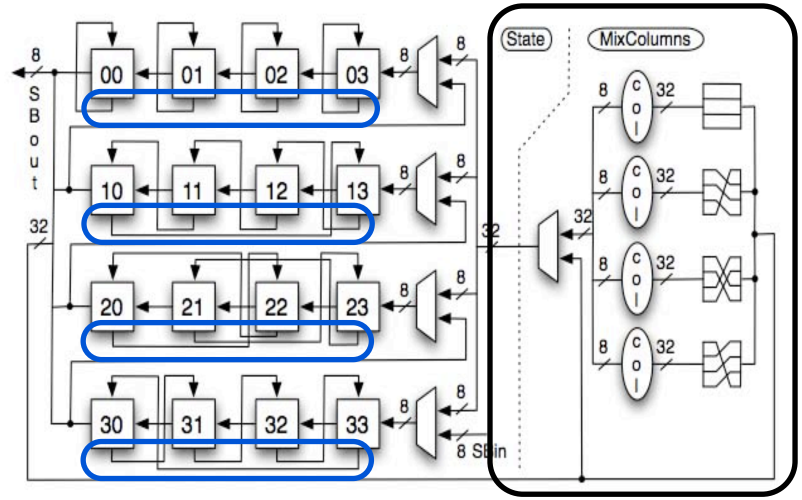
RotWord
0 GE
SubWord
0 GE

Add RCon
35 GE

Feedback
30 GE

AES Optimization Summary

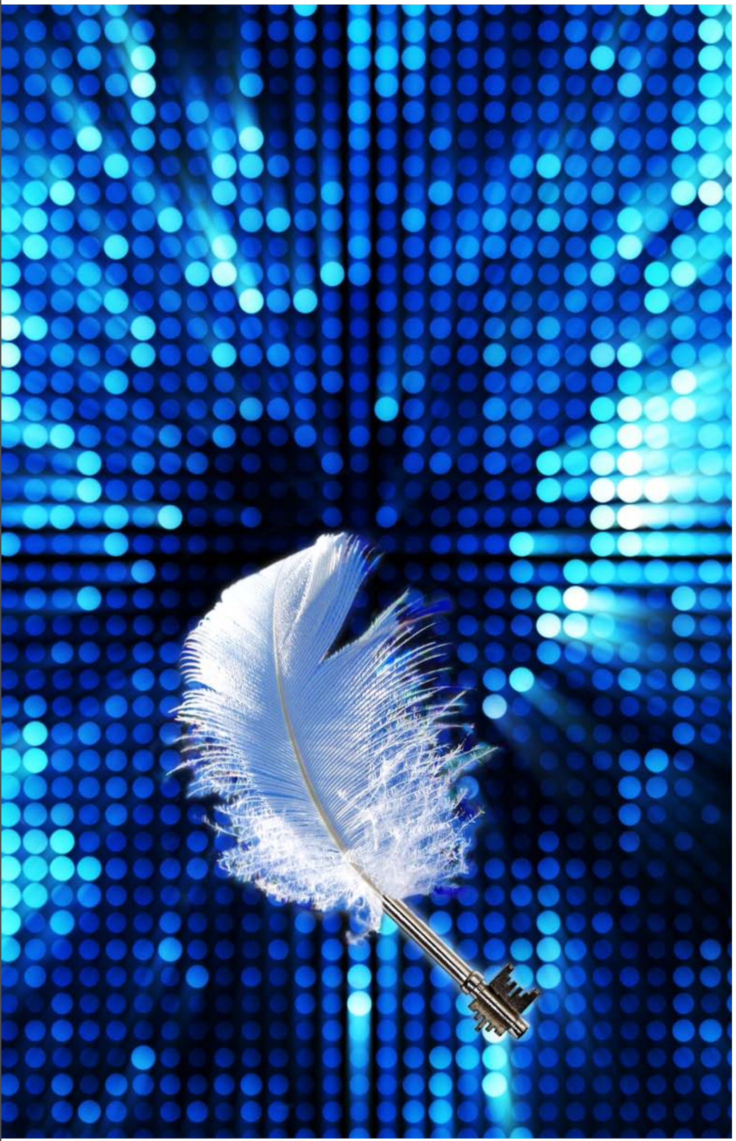
- Design goal:
  - low area
- Design Strategy:
  - Consequently exploiting Scan Flip-Flops
  - Optimizing for the global minimum
    - MixColumns not serialized
  - Minimizing the control logic
    - 16+4+1=21 cycle LFSR
  - Slight modification of the I/O byte order
    - Saves 373 GE



State: **59%**

crypto: **27%**

control: **14%**

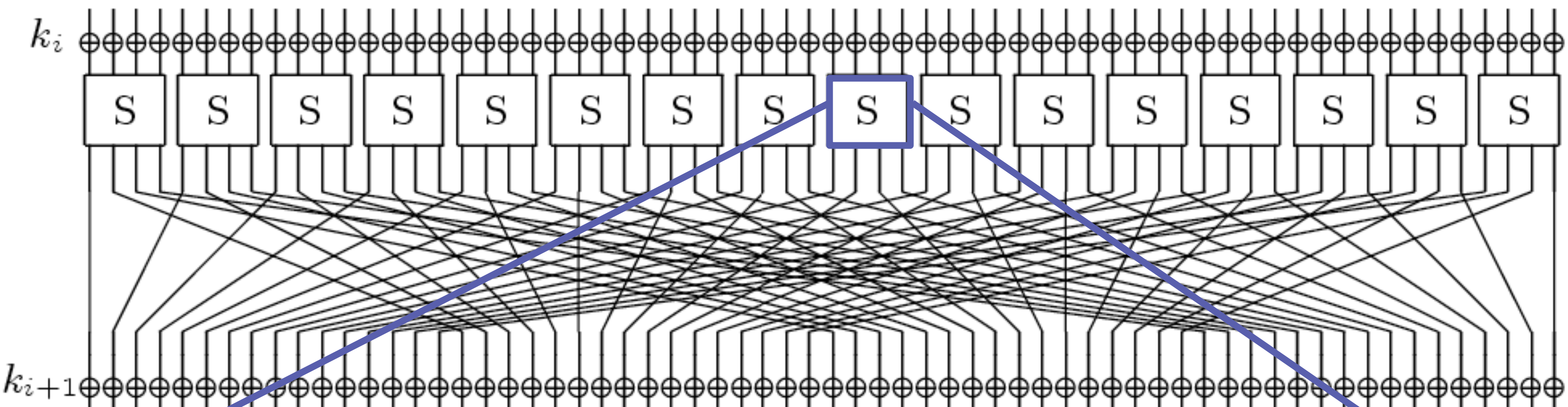


Agenda

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

PRESENT

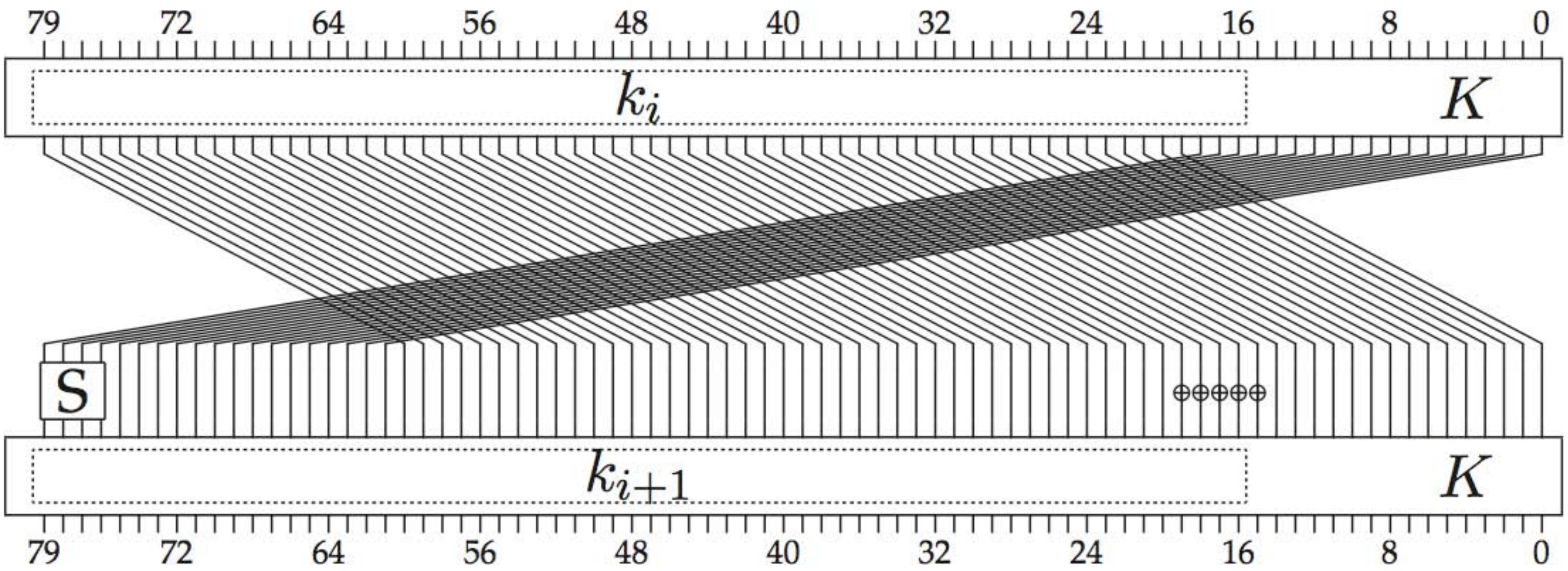
- Substitution-Permutation Network
- 64-bit block size, 80/128 bit key length, 31 rounds
- S-layer = 16 identical 4-bit S-boxes
- P-Layer is a bit permutation = no cost in hardware
- under standardization (ISO 29192-2)



x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S[x]$	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2

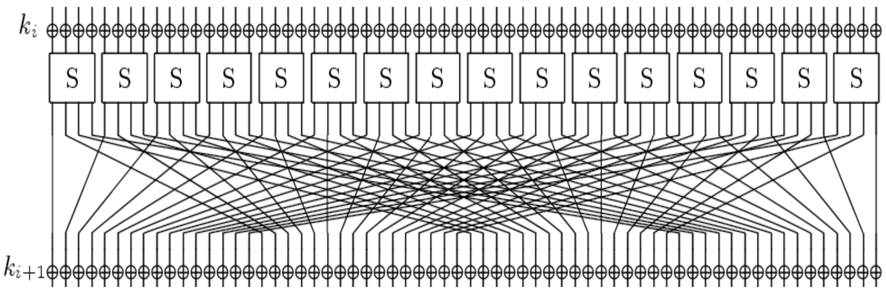
PRESENT-80 Key Schedule

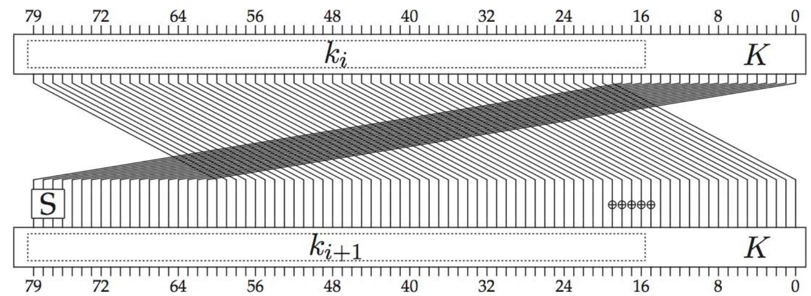
- simple design
- 61-bit left rotation = no cost in hardware
- same S-box as in datapath
- round counter used to thwart slide attacks

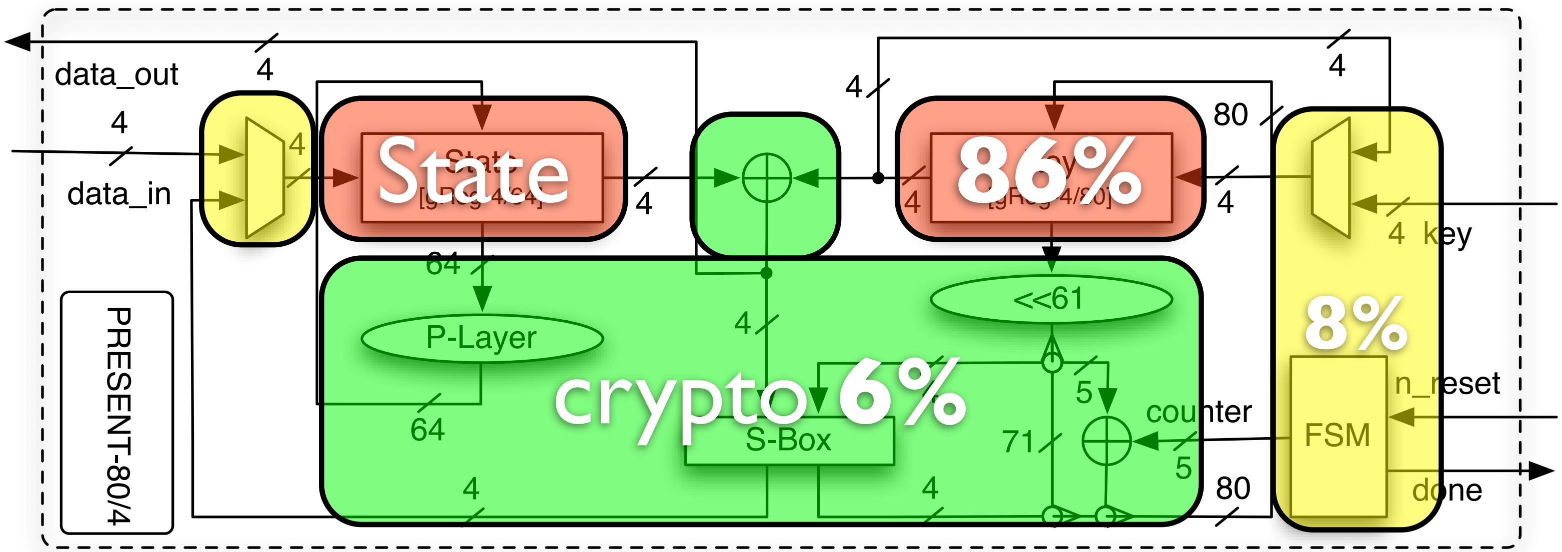


PRESENT HW Implementation

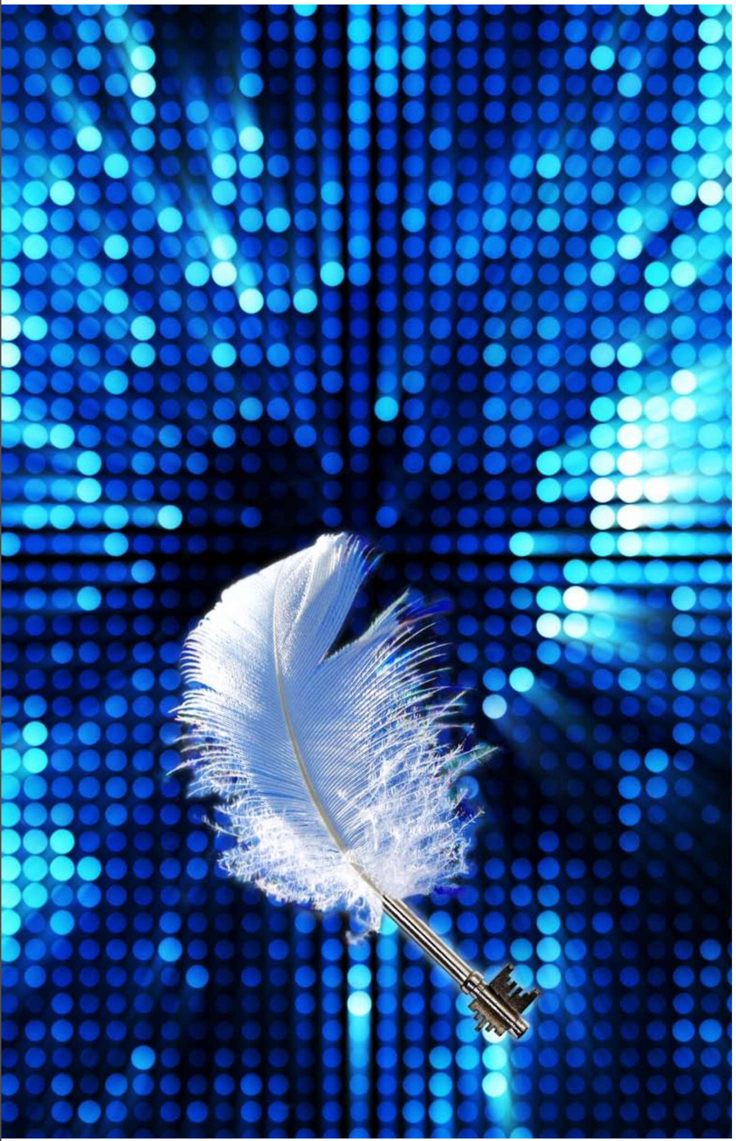
NANYANG TECHNOLOGICAL UNIVERSITY







1030 GE **516 CLK**



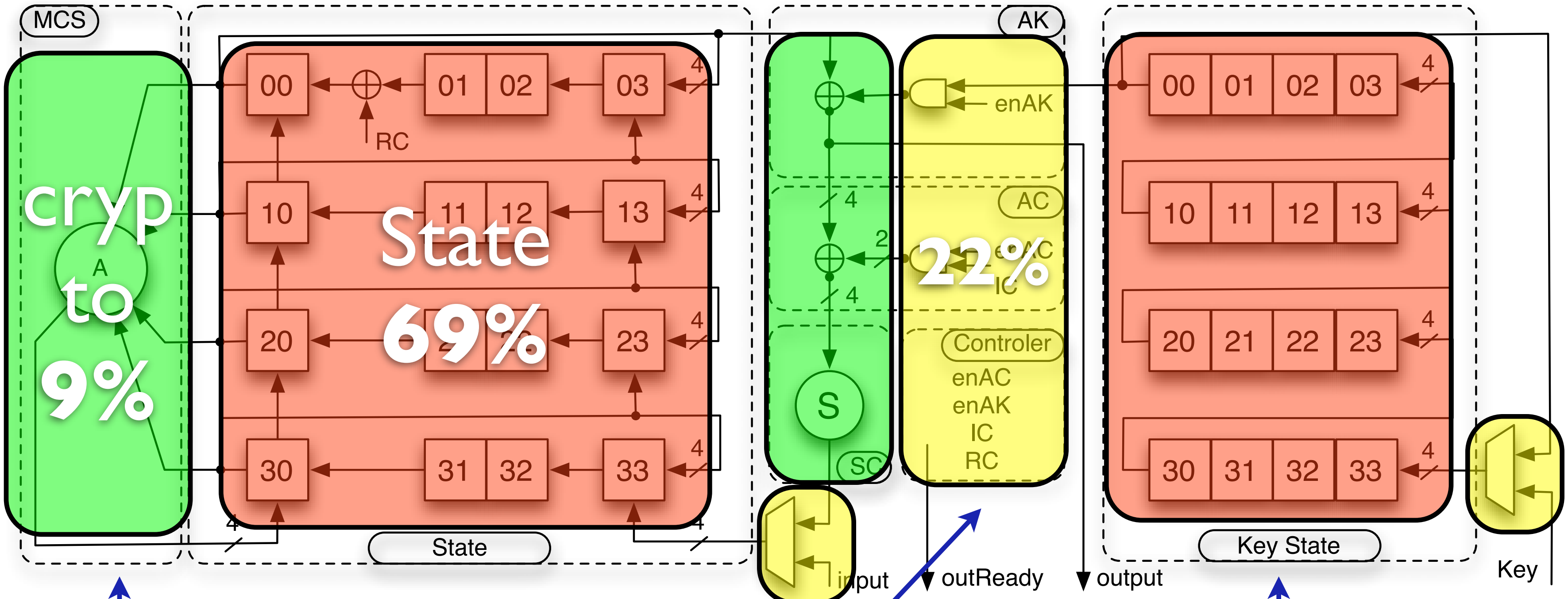
Agenda

- 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

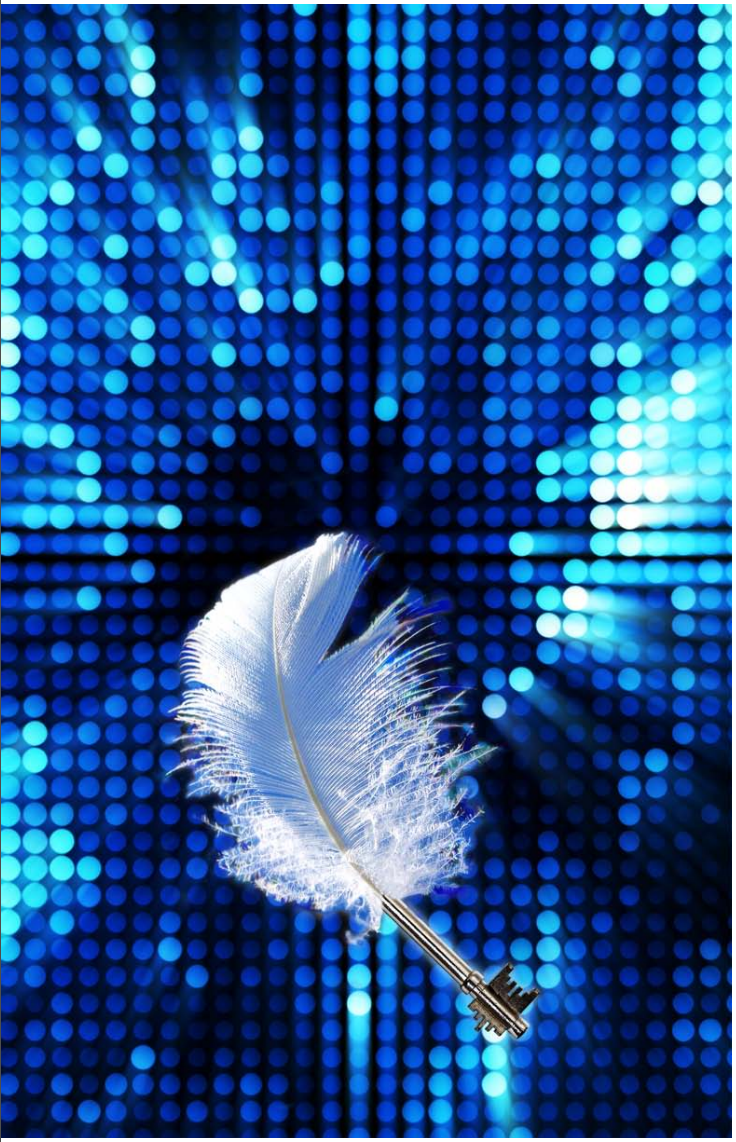


serialized MDS saves 120 GE

large control logic

no key schedule allows hard-wiring

1040 GE **1268 CLK**



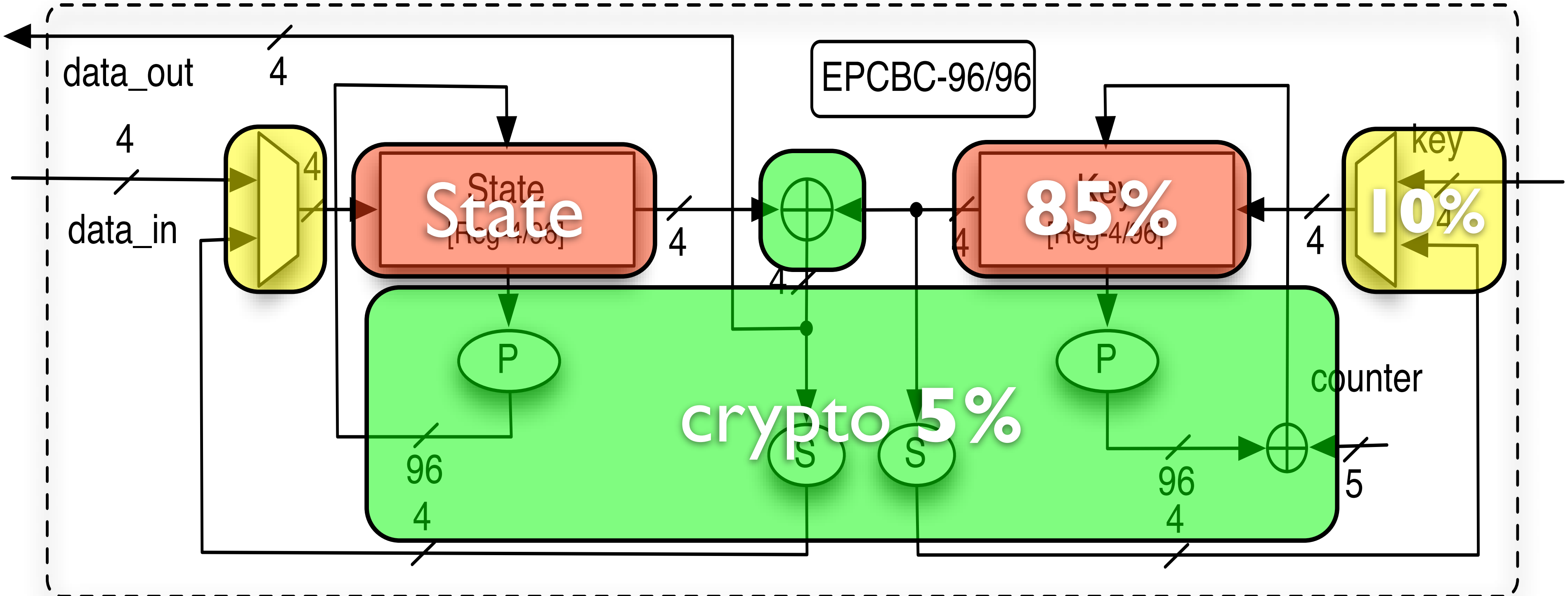
Agenda

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

EPCBC - Electronic Product Code Block Cipher

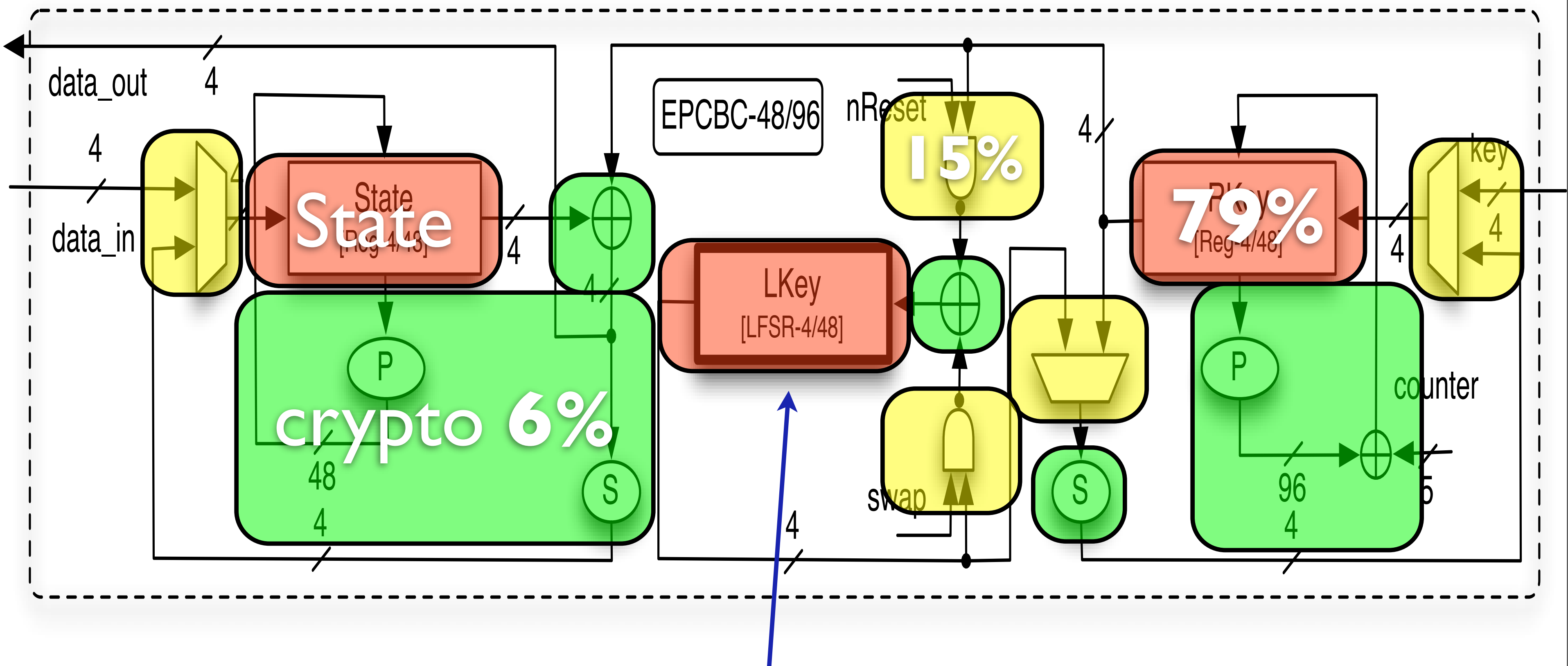
- Substitution-Permutation Network
- 96 bit key length, 32 rounds
- 48/96-bit block size
- Block size optimized for Electonic Product Code
- Based on PRESENT

EPC-96/96 HW Implementation



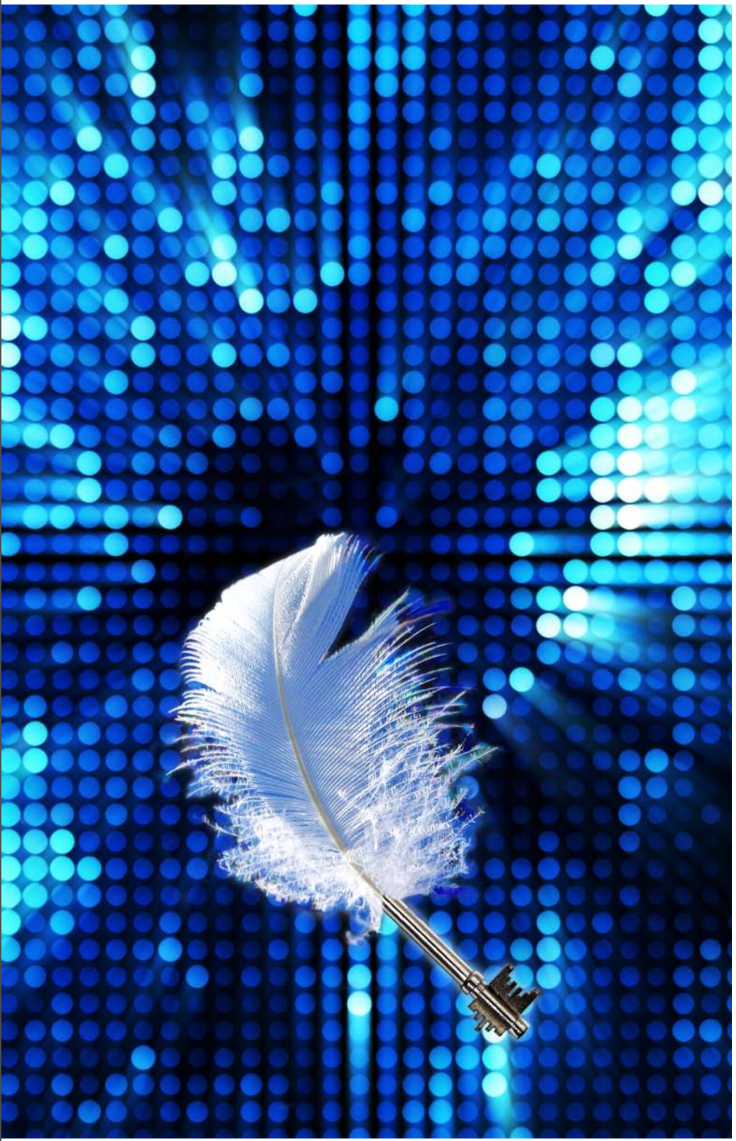
1333 GE **792 CLK**

EPC-48/96 HW Implementation



1-input FF

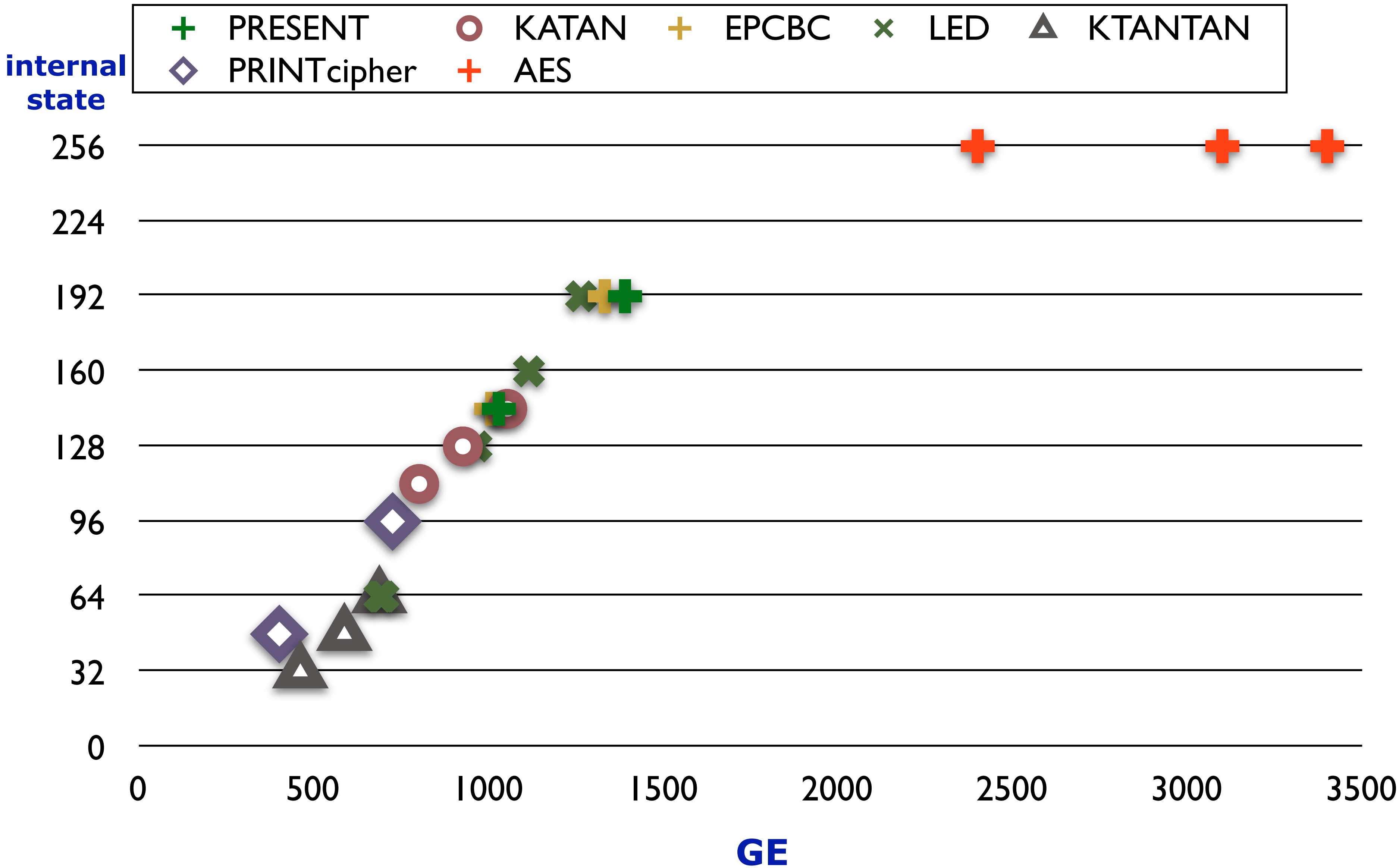
1008 GE **396 CLK**



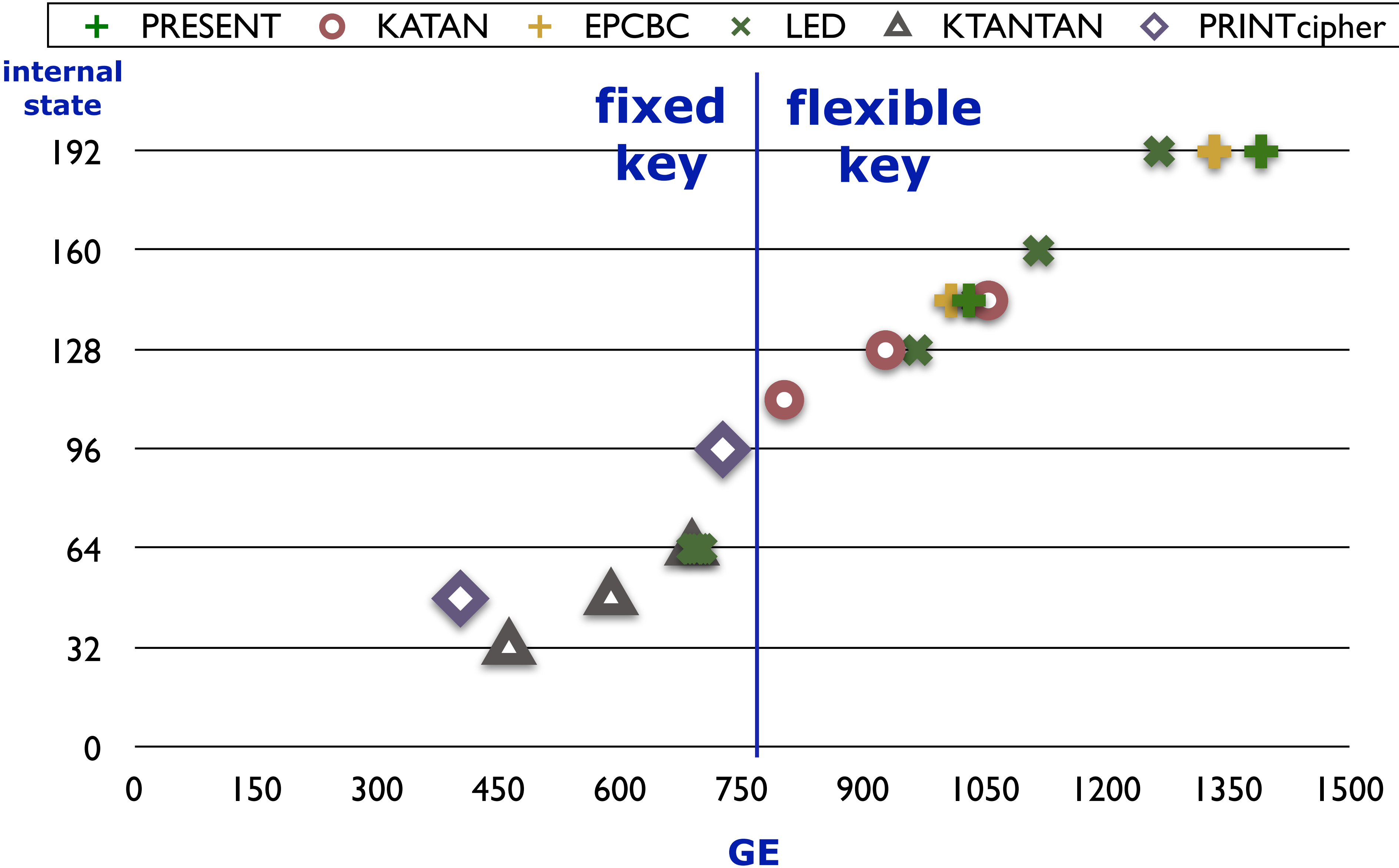
Agenda

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

Internal State vs. Area



Internal State vs. Area



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

[BKL+07] A. Bogdanov, L.R. Knudsen, G. Leander, C. Paar, A. Poschmann, M.J.B. Robshaw, Y. Seurin, and C. Vikkelsoe "PRESENT: An Ultra-Lightweight Block Cipher". Cryptographic Hardware and Embedded Systems - CHES 2007, 9. International Workshop, Vienna, Austria, Proceedings. LNCS, Springer-Verlag, September 10 - 13, 2007

[CDK09] de Cannière, C., Dunkelman, O., Knezević, M.: Katan and ktantan–a family of small and efficient hardware-oriented block ciphers. In: Clavier, C., Ga j, K. (eds.) CHES 2009. LNCS, vol. 5747, pp. 272–288. Springer, Heidelberg (2009)

[FWR05] M. Feldhofer, J. Wolkerstorfer, V. Rijmen, "AES Implementation on a Grain of Sand". Information Security, IEE Proceedings, 152(1):13-20, 2005.

[GPP11] J. Guo, T. Peyrin, A. Poschmann, "The LED Block Cipher", Cryptographic Hardware and Embedded Systems - CHES 2011, LNCS, Springer-Verlag, to appear 2011.

[HAH+06] Hämäläinen, P., Alho, T., Hännikäinen, M., Hämäläinen, T.D.: Design and Implementation of Low-Area and Low-Power AES Encryption Hardware Core. In: DSD, pp. 577–583 (2006)

[KLP+10] L. Knudsen, G. Leander, A. Poschmann, M.J.B. Robshaw, „PRINTcipher: A Block Cipher for IC-Printing“, In: Mangard, S., Standaert, F.-X. (eds.) CHES 2010. LNCS vol. 6225, pp. 16-32. Springer-Verlag.

[MPP+10] A. Moradi, A. Poschmann, C. Paar, S. Ling, H. Wang, "Pushing the Limits: A Very Compact and a Threshold Implementation of the AES". Advances in Cryptology - EUROCRYPT 2011, LNCS vol. 6632, 69 - 88, Springer-Verlag, May 2011.

[SMT+01] A. Satoh, S. Morioka, K. Takano, S. Munetoh, "A Compact Rijndael hardware architecture with S-Box optimization". Advances in Cryptology - ASIACRYPT 2001, LNCS vol. 2248, 239 - 254, Springer-Verlag, December 2001.

[YKP+11] H. Yap, K. Khoo, A. Poschmann, M. Henricksen, "EPCBC - A Block Cipher for Electronic Product Code Encryption". CANS 2011, LNCS, Springer-Verlag, to appear 2011.

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/