KU LEUVEN

RUB

RUHR-UNIVERSITÄT BOCHUM

Spin Me Right Round: Rotational Symmetry for FPGA-Specific AES

CHES 2018, Amsterdam

SPONSORED BY THE

fwo

Federal Ministry of Education and Research

Grant. Nr. 16KIS0666 SYSKIT_HW

Lauren De Meyer[1], Amir Moradi[2], Felix Wegener[2]

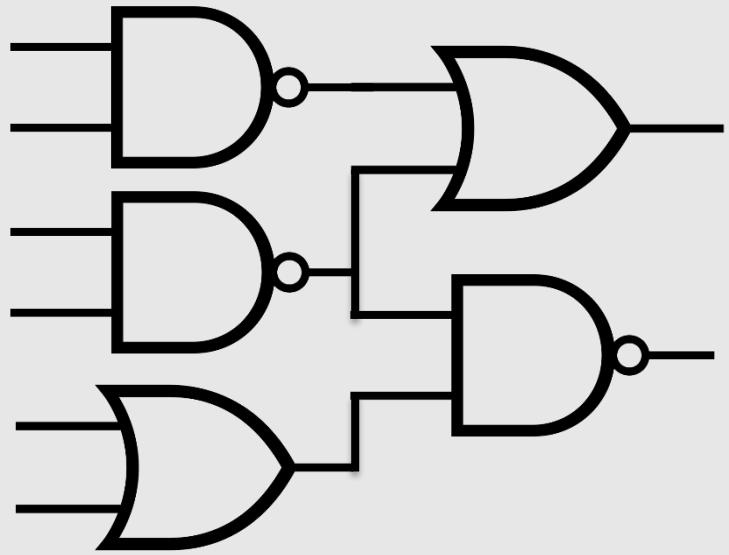
[1] imec - COSIC, KU Leuven, Belgium
[2] Horst Görtz Institute for IT-Security, Ruhr-Universität Bochum, Germany

COSIC

hgi Horst Görtz Institute for IT-Security

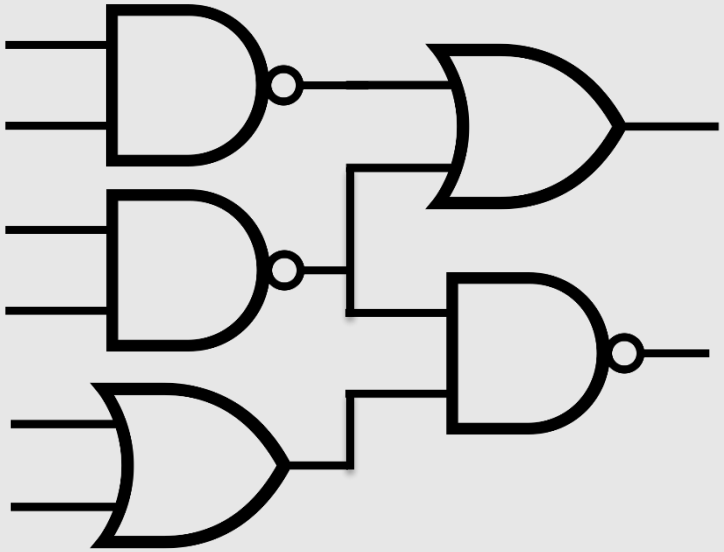
Area Optimization: ASICs vs FPGAs

ASIC

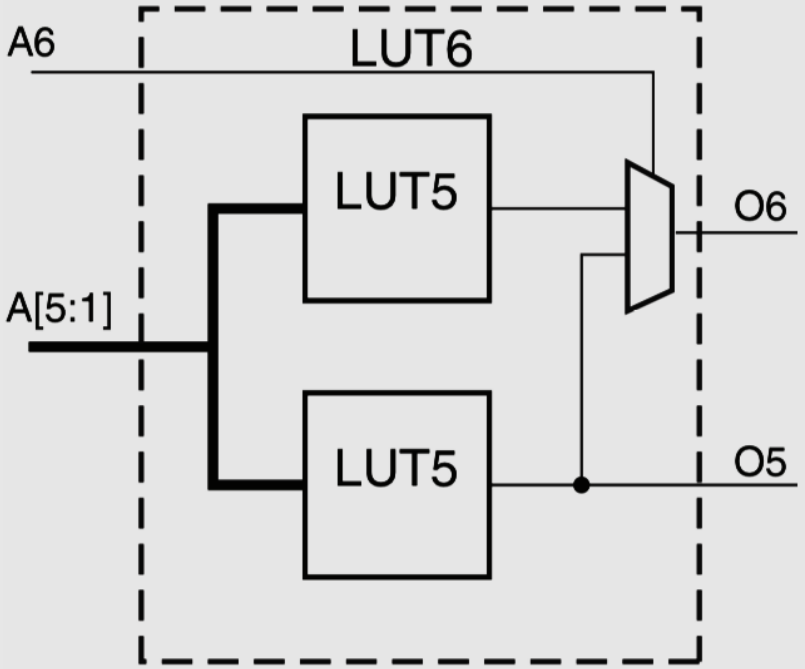


Area Optimization: ASICs vs FPGAs

ASIC



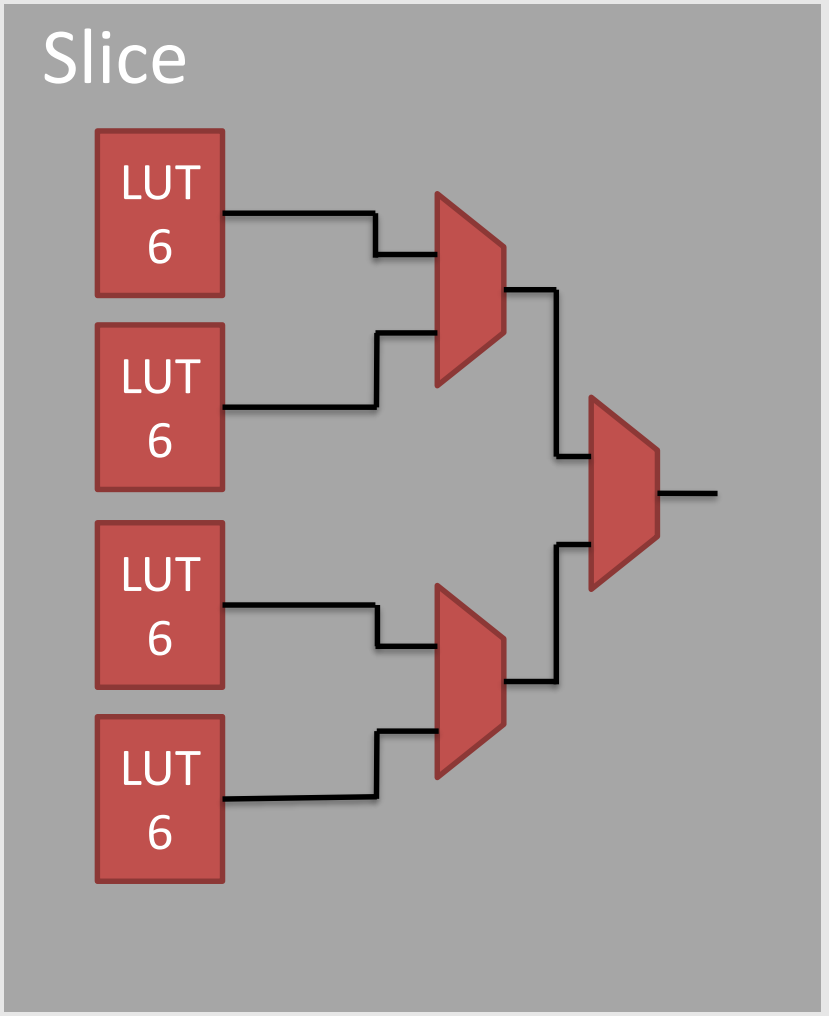
FPGA (Xilinx 6/7 series)



Spartan-6 FPGA Configurable Logic Block User Guide

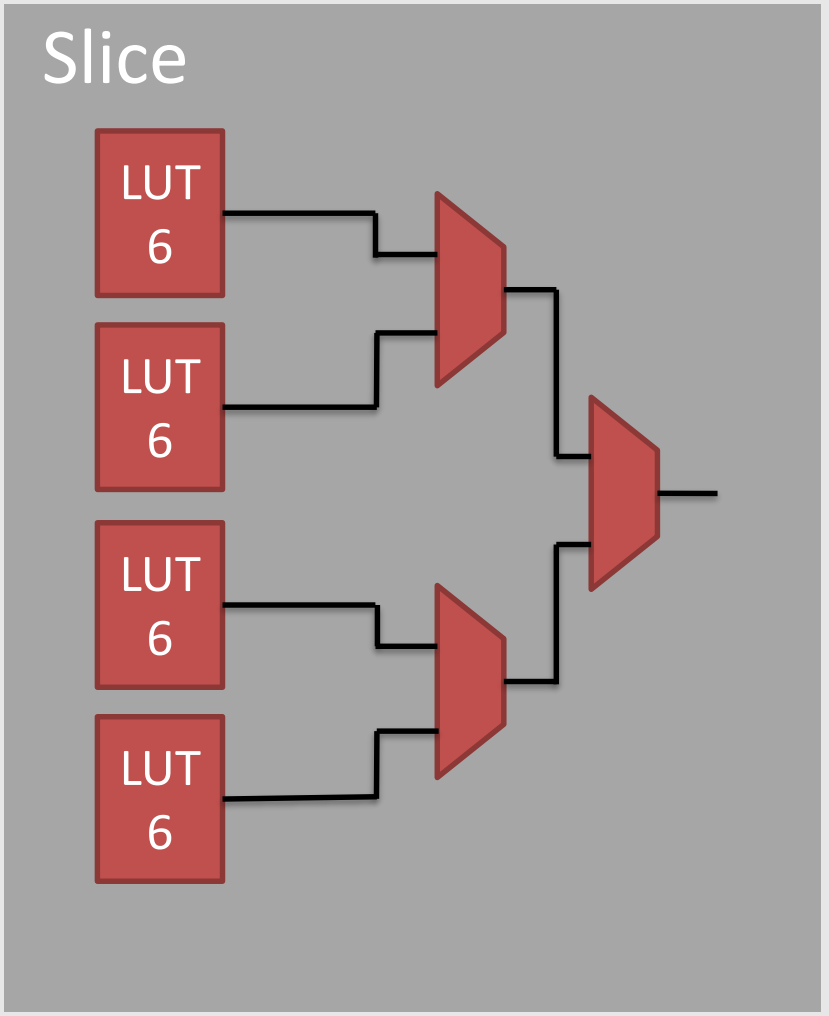
FPGA Building Blocks (Xilinx)

- Slice contents:
  - 4 LUT6 elements
  - Auxiliar MUX
  - (8 registers)



FPGA Building Blocks (Xilinx)

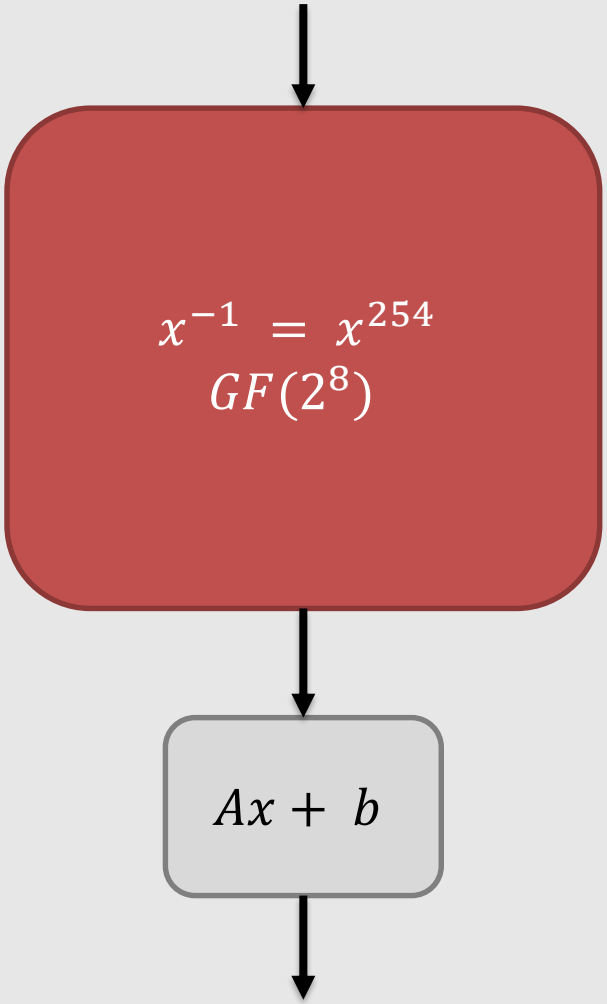
- Slice contents:
  - 4 LUT6 elements
  - Auxiliar MUX
  - (8 registers)



One slice can implement any $\mathbb{F}_2^8 \rightarrow \mathbb{F}_2$ function

AES S-box Structure

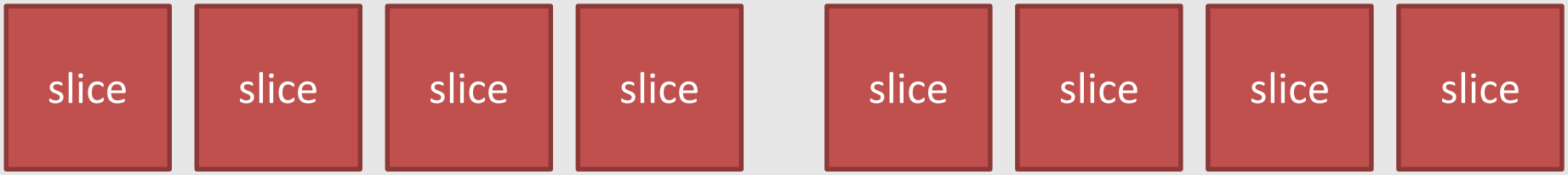
Power Map



Affine Map

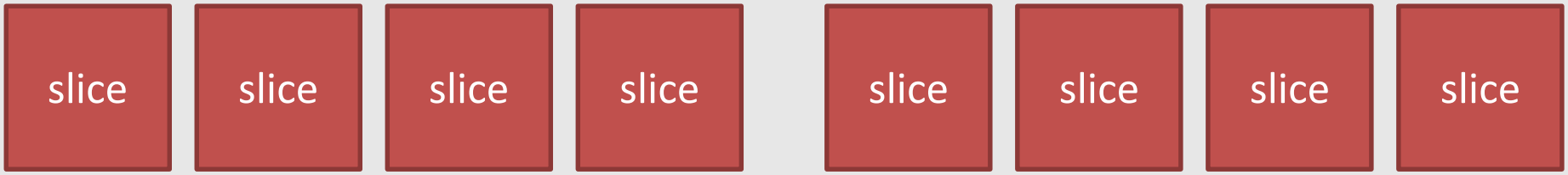
AES S-box in FPGAs

- Naive Approach: one slice per coordinate: **8 slices**



AES S-box in FPGAs

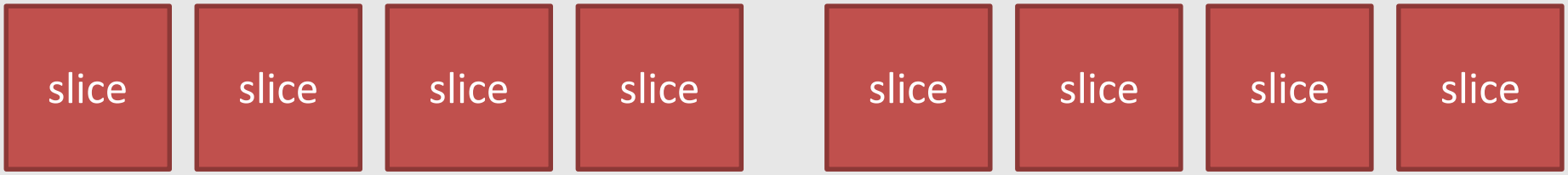
- Naive Approach: one slice per coordinate: **8 slices**



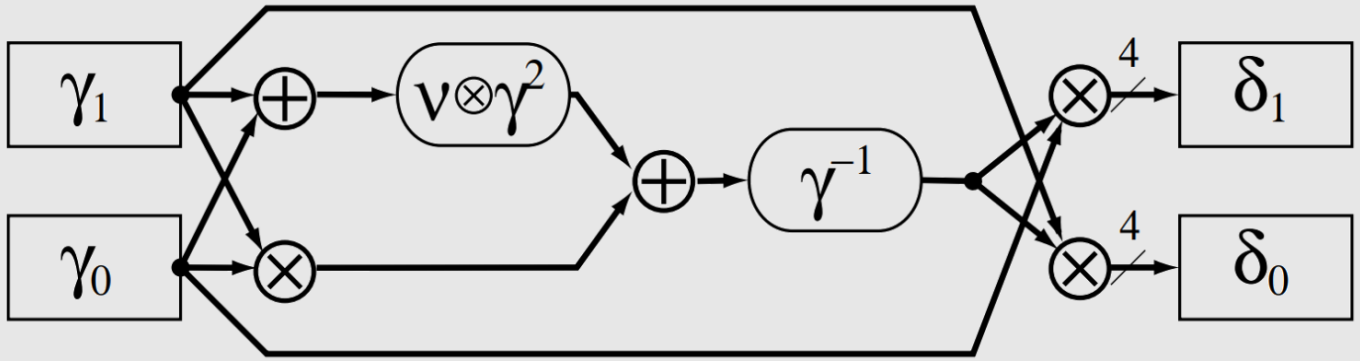
- Algebraic degree 7 → no obvious improvements

AES S-box in FPGAs

- Naive Approach: one slice per coordinate: **8 slices**



- Algebraic degree 7 → no obvious improvements
- Tower field doesn‘t suit LUTs



Canright. *A Very Compact S-box for AES*. CHES 2005

AES S-box in FPGAs

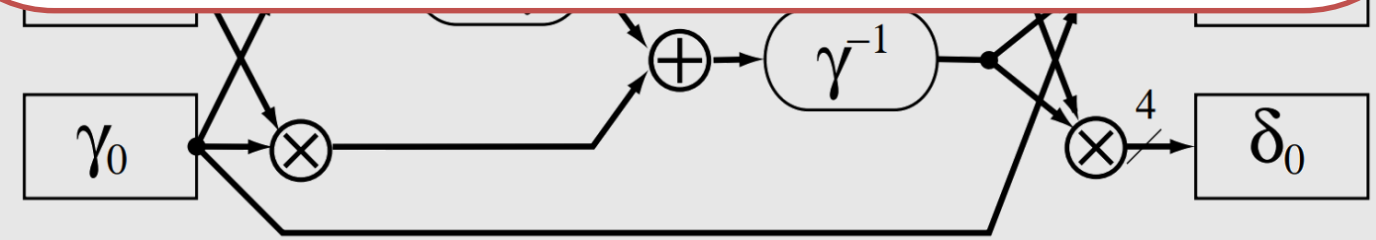
- Naive Approach: one slice per coordinate: **8 slices**

slice

slice

Our Contribution:
Reduction to **4 slices**

- Alg
- Tov



Canright: *A Very Compact S-box for AES*. CHES 2005

Rotational Symmetry of Power Maps

Inversion in $GF(2^8)$: $x \mapsto x^{254}$

Conversion to normal base: $x \mapsto \phi(x)$

Rotation: $rot(\,(a_0, \ldots, a_{n-1})\,) = (a_{n-1}, a_0, \ldots, a_{n-2})$

Rotational Symmetry of Power Maps

Inversion in $GF(2^8)$: $x \mapsto x^{254}$

Conversion to normal base: $x \mapsto \phi(x)$

Rotation: $rot(\,(a_0, \ldots, a_{n-1})\,) = (a_{n-1}, a_0, \ldots, a_{n-2})$

Theorem[1]:

Power Map: $F(x) = x^m$ in $GF(2^8)$

Normal base: $S(x) = \phi(F(\phi^{-1}(x)))$

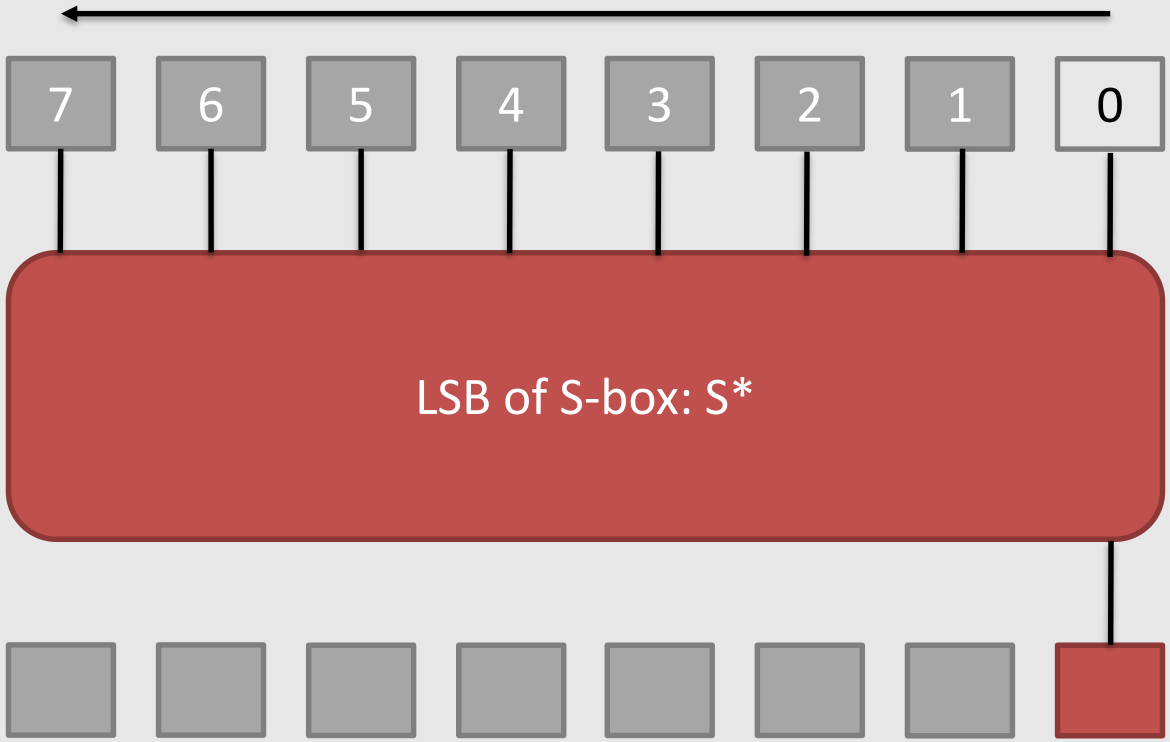
$\Rightarrow$

$$rot(S(x)) = S(rot(x))$$

[1] Rijmen, Barreto, Gazzoni Filho. *Rotation Symmetry in Algebraically Generated Cryptographic Substitution Tables*. Information Processing Letters 2008

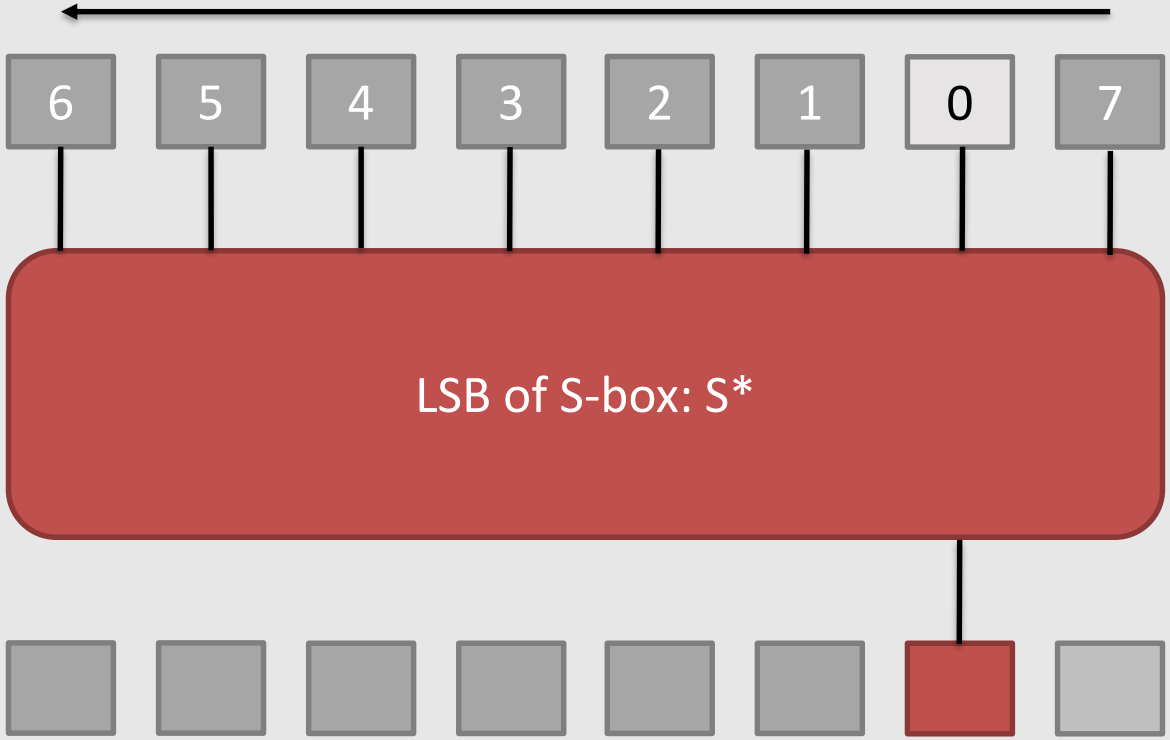
Rotational Symmetry: Area Reduction

Idea: Create circuit for **only one** coordinate function (LSB)



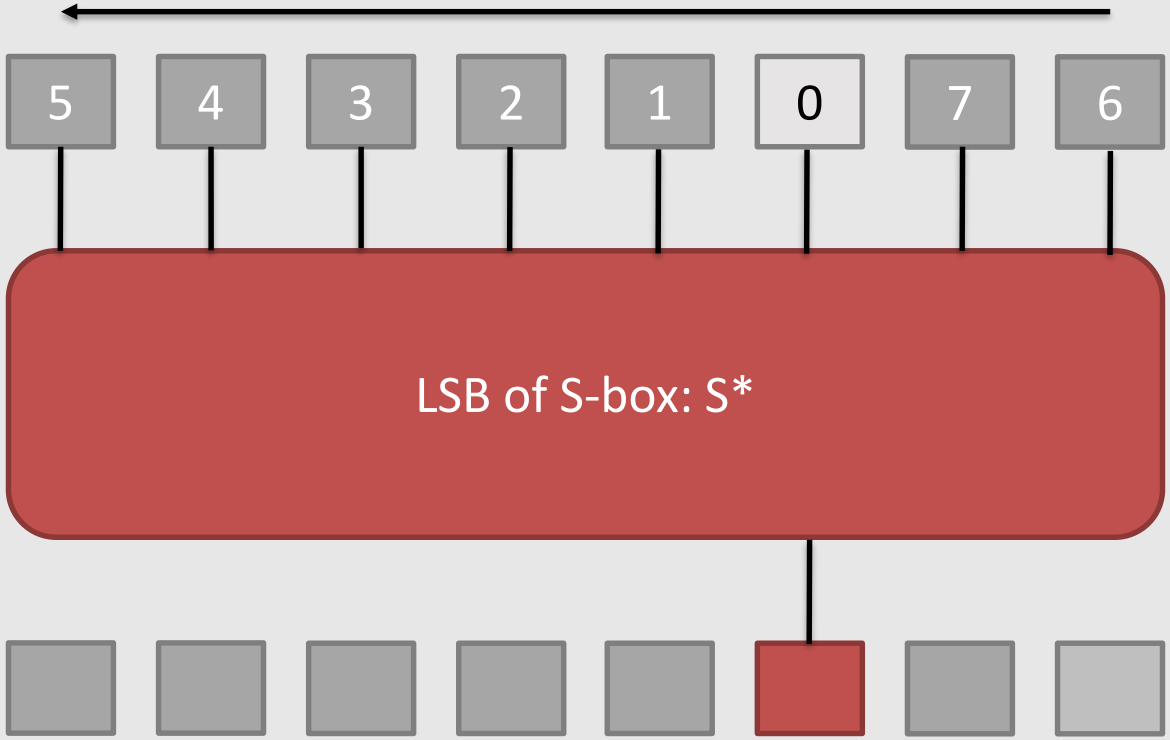
Rotational Symmetry: Area Reduction

Idea: Create circuit for **only one** coordinate function (LSB)



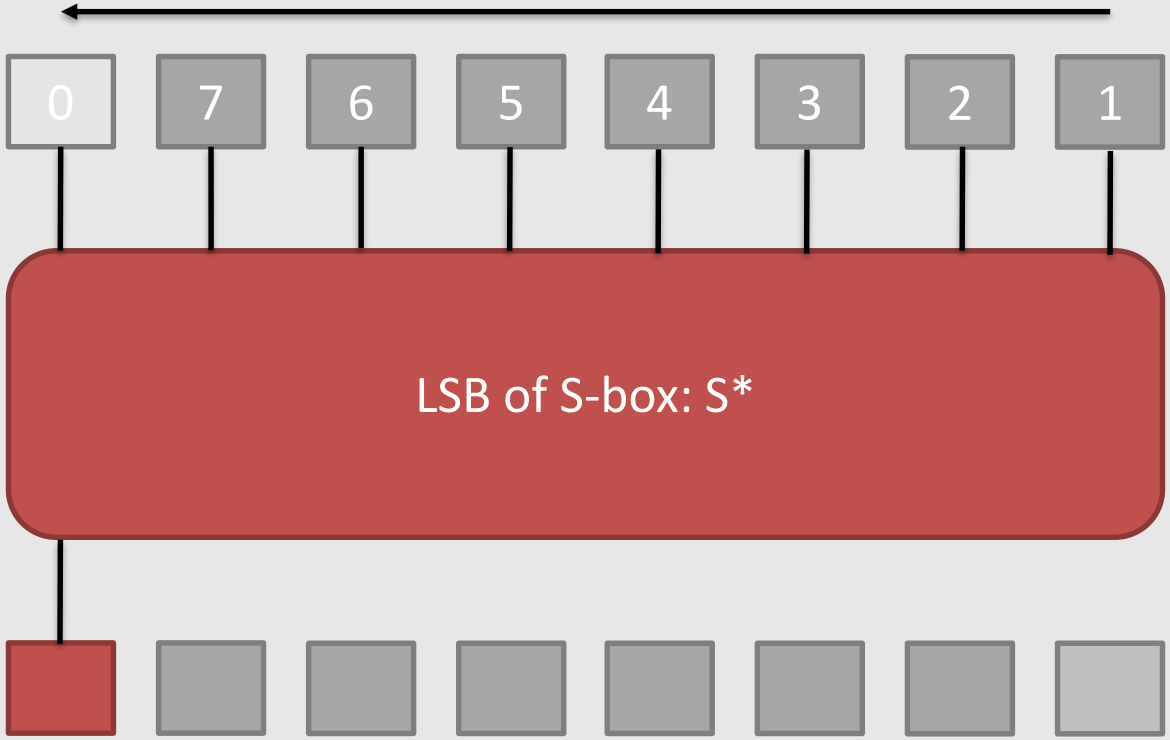
Rotational Symmetry: Area Reduction

Idea: Create circuit for **only one** coordinate function (LSB)

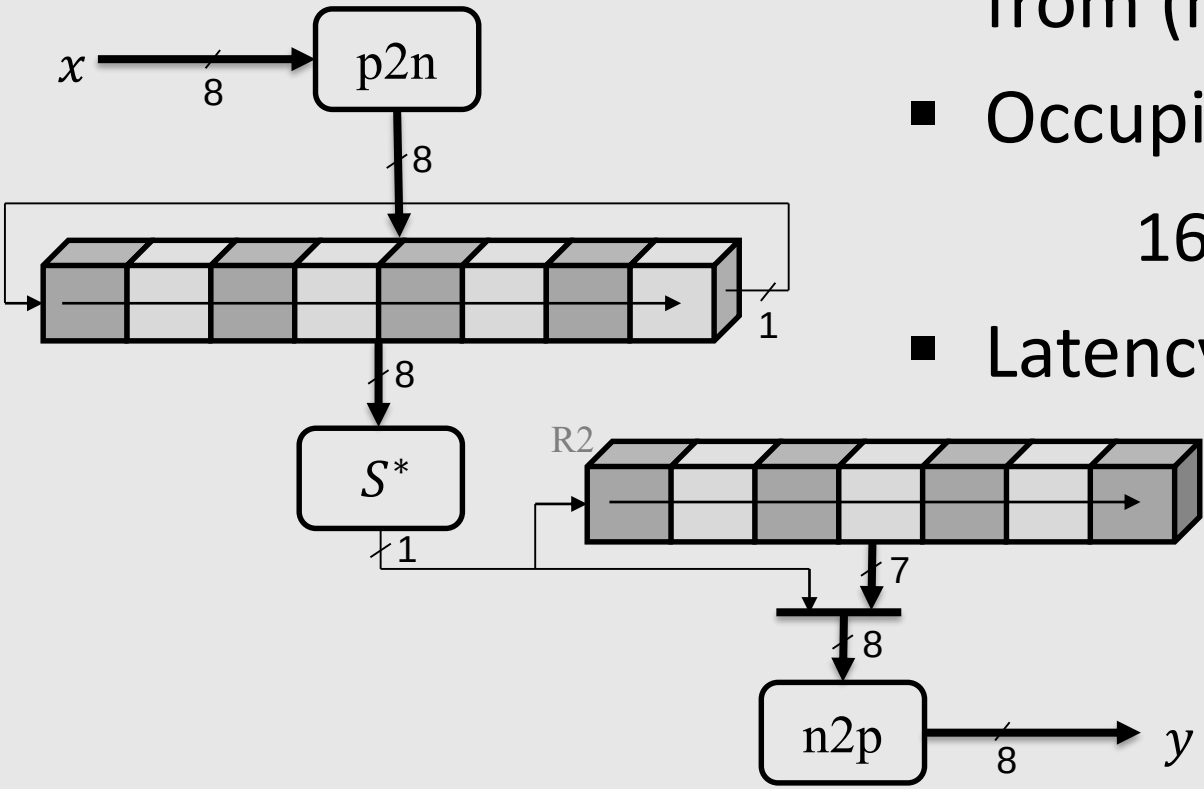


Rotational Symmetry: Area Reduction

Idea: Create circuit for **only one** coordinate function (LSB)



AES S-box: Byte-serial Circuit



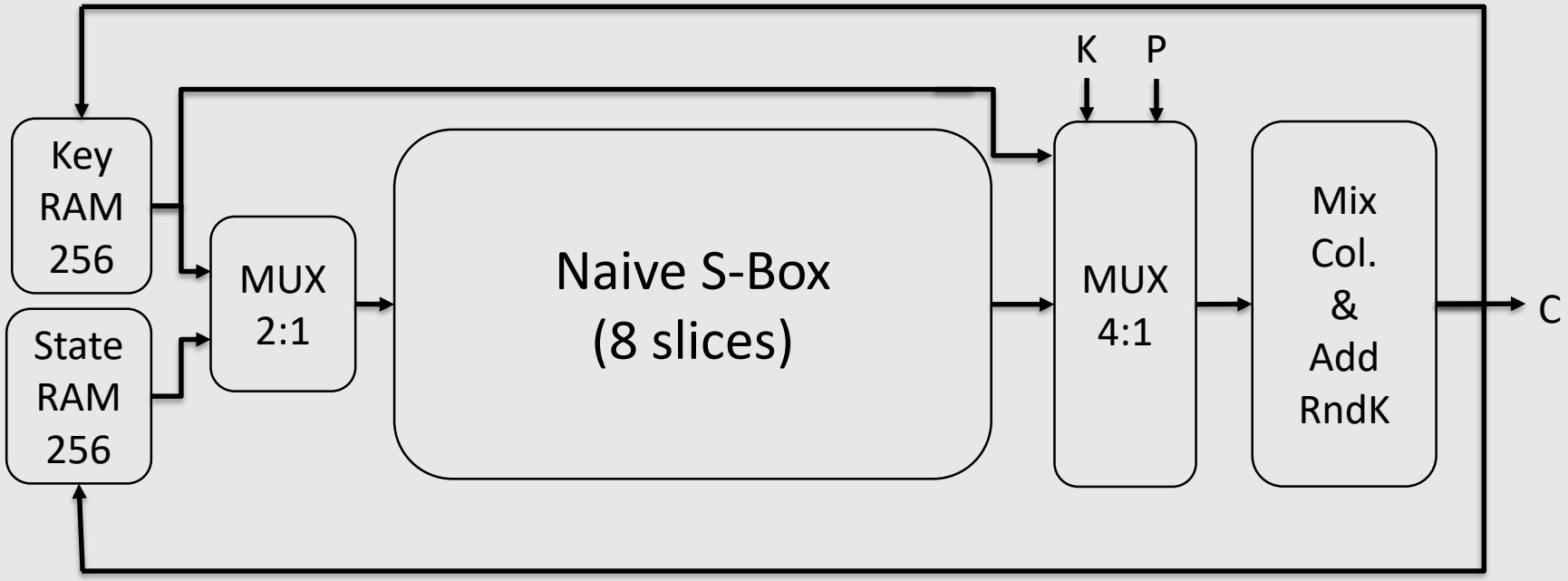
- Transformation to (p2n) and from (n2p) normal basis
- Occupies 4 slices:

  16LUTs / 15Regs
- Latency: 8 cycles

First Design:
Improve smallest FPGA-specific AES

Former record by Sasdrich *et al.*[1]

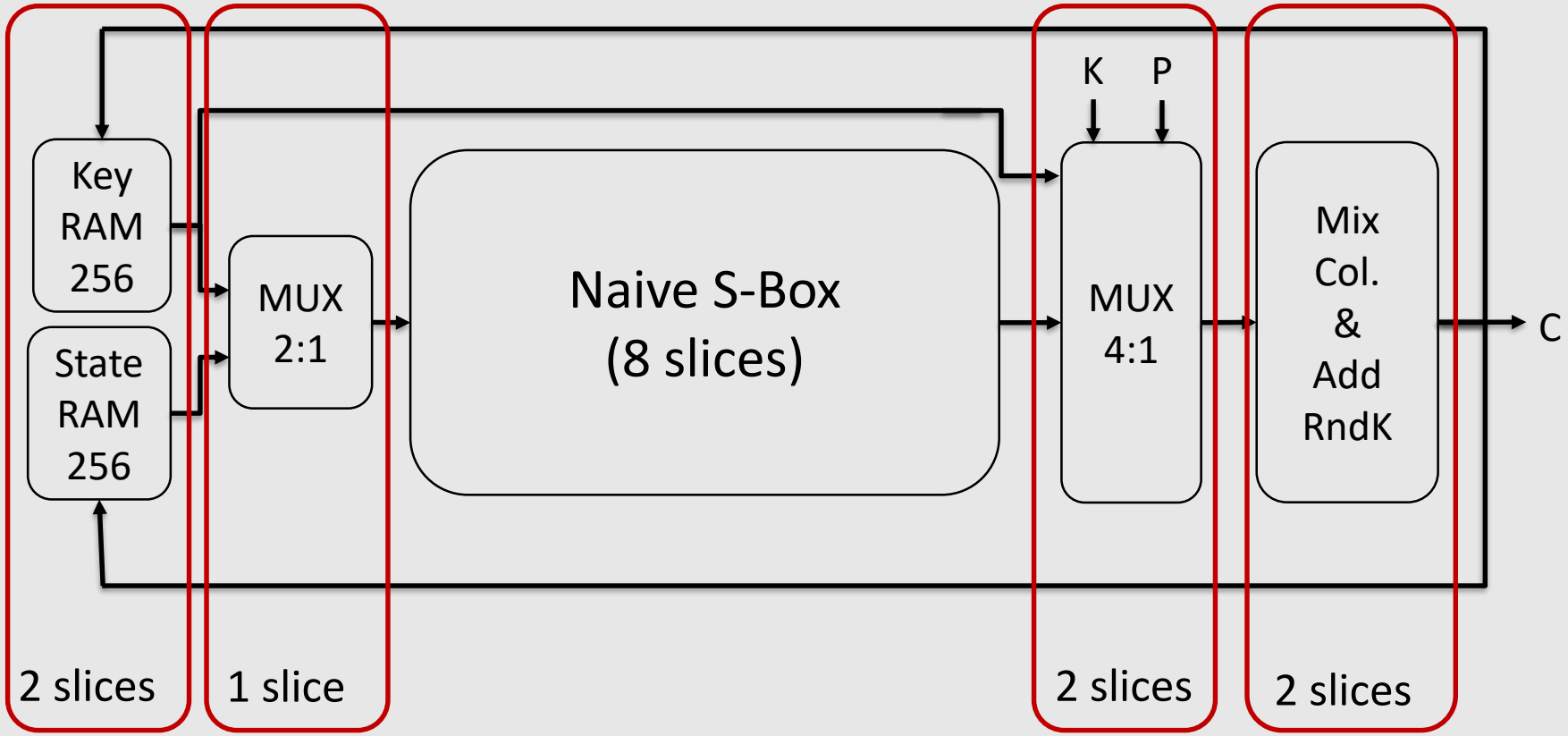
- **21 slices** on Xilinx Spartan-6
- 15 slices shown + 6 for control unit



[1] Sasdrich, Güneysu. *A grain in the silicon: SCA-protected AES in less than 30 slices*. ASAP 2016

Former record by Sasdrich *et al.*[1]

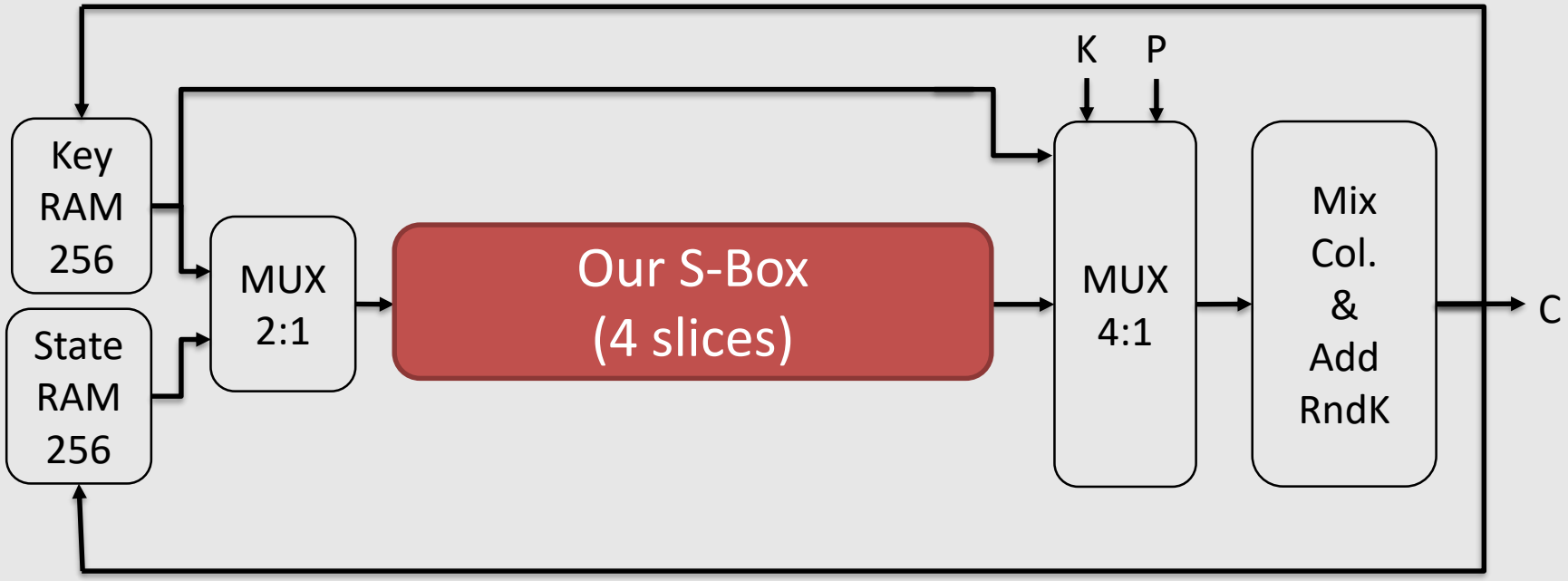
- **21 slices** on Xilinx Spartan-6
- 15 slices shown + 6 for control unit



[1] Sasdrich, Güneysu. *A grain in the silicon: SCA-protected AES in less than 30 slices*. ASAP 2016

Former record by Sasdrich *et al.*[1]

- **21 slices** on Xilinx Spartan-6
- 15 slices shown + 6 for control unit



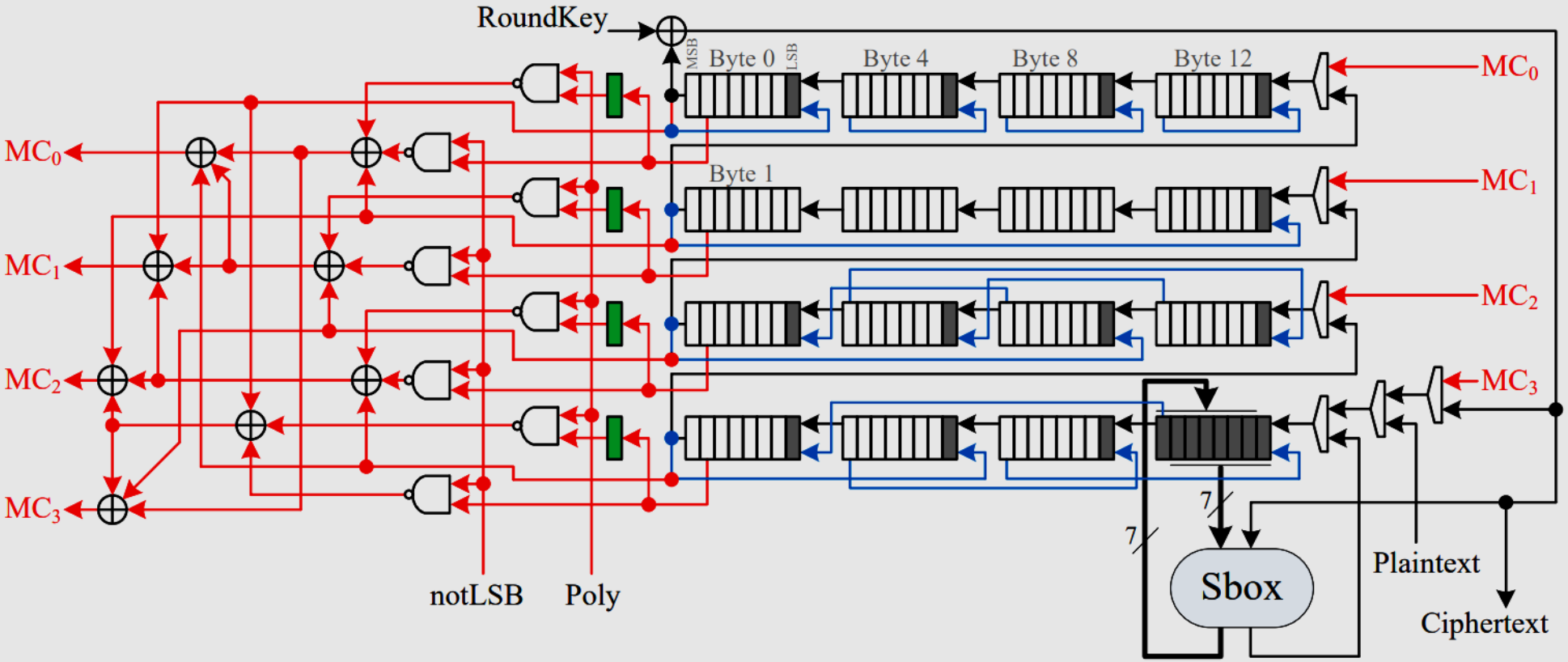
Total design: 17 slices

[1] Sasdrich, Güneysu. *A grain in the silicon: SCA-protected AES in less than 30 slices*. ASAP 2016

Second Design:
Port smallest AES on ASICs to FPGAs

Bitsliding Design: Jean *et al*, CHES 2017[1]

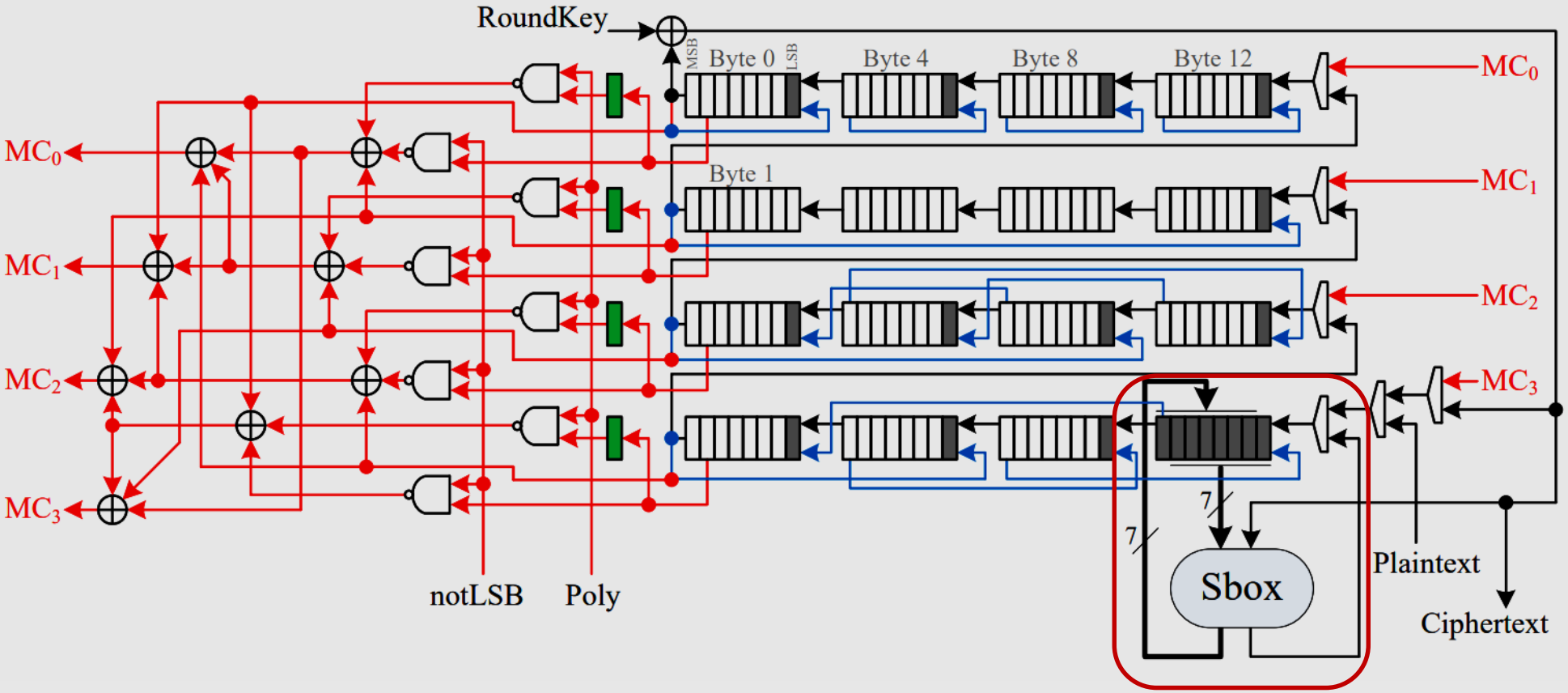
Adapt smallest ASIC-based AES to FPGAs



[1] Jean, Moradi, Peyrin, Sasdrich. *Bit-sliding: A generic technique for bit-serial implementations of SPN-based primitives - applications to AES, PRESENT and SKINNY*. CHES 2017

Bitsliding Design: Jean *et al*, CHES 2017[1]

Adapt smallest ASIC-based AES to FPGAs

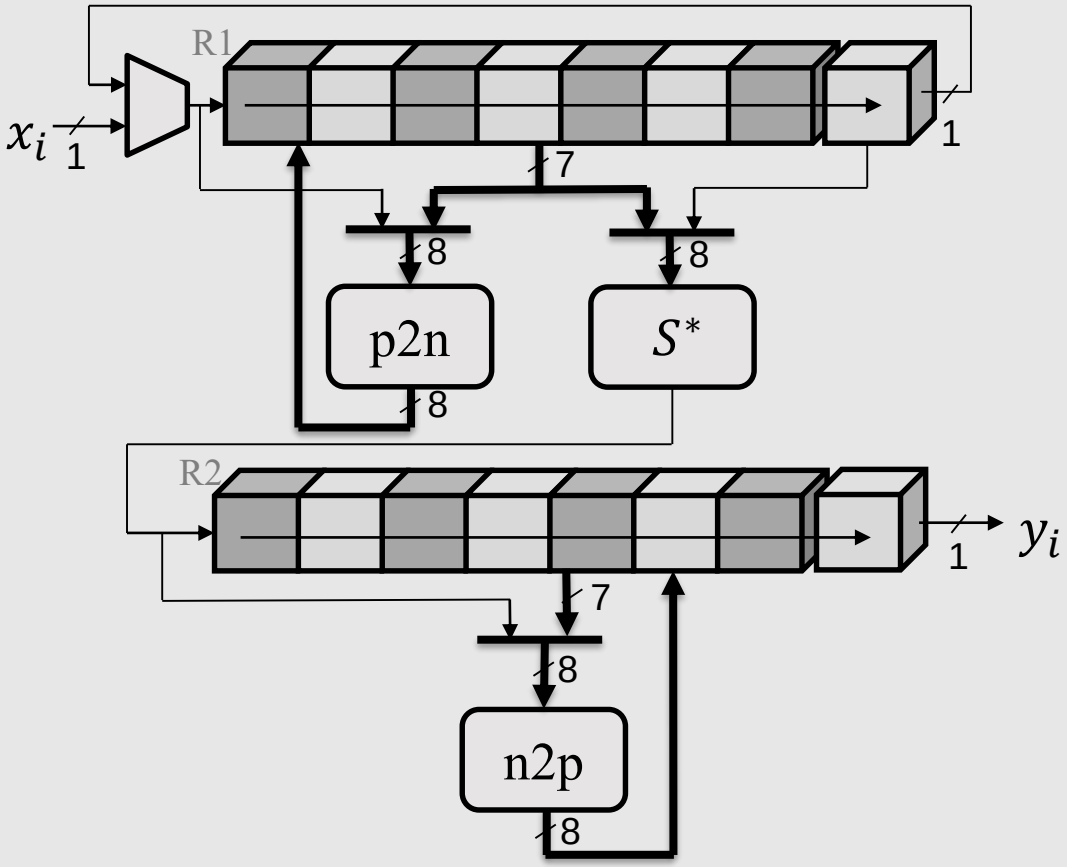


[1] Jean, Moradi, Peyrin, Sasdrich. *Bit-sliding: A generic technique for bit-serial implementations of SPN-based primitives - applications to AES, PRESENT and SKINNY*. CHES 2017

Fully-bitserial S-box

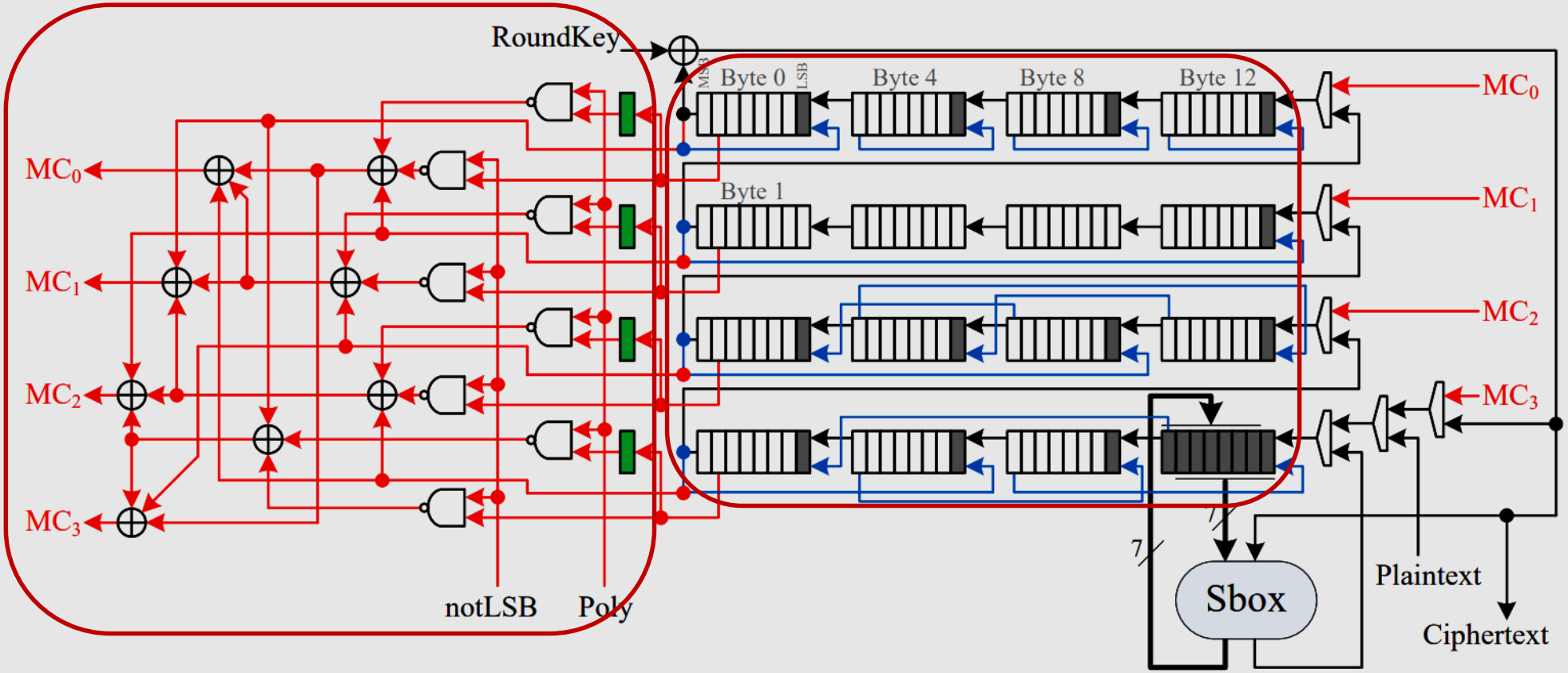
- Bitserial in-/output
- Area: 4 slices:

  16 LUTs, 16 Regs
- Latency: 16 Cycles



Bitsliding Design: Jean *et al*, CHES 2017[1]

Adapt smallest ASIC-based AES to FPGAs



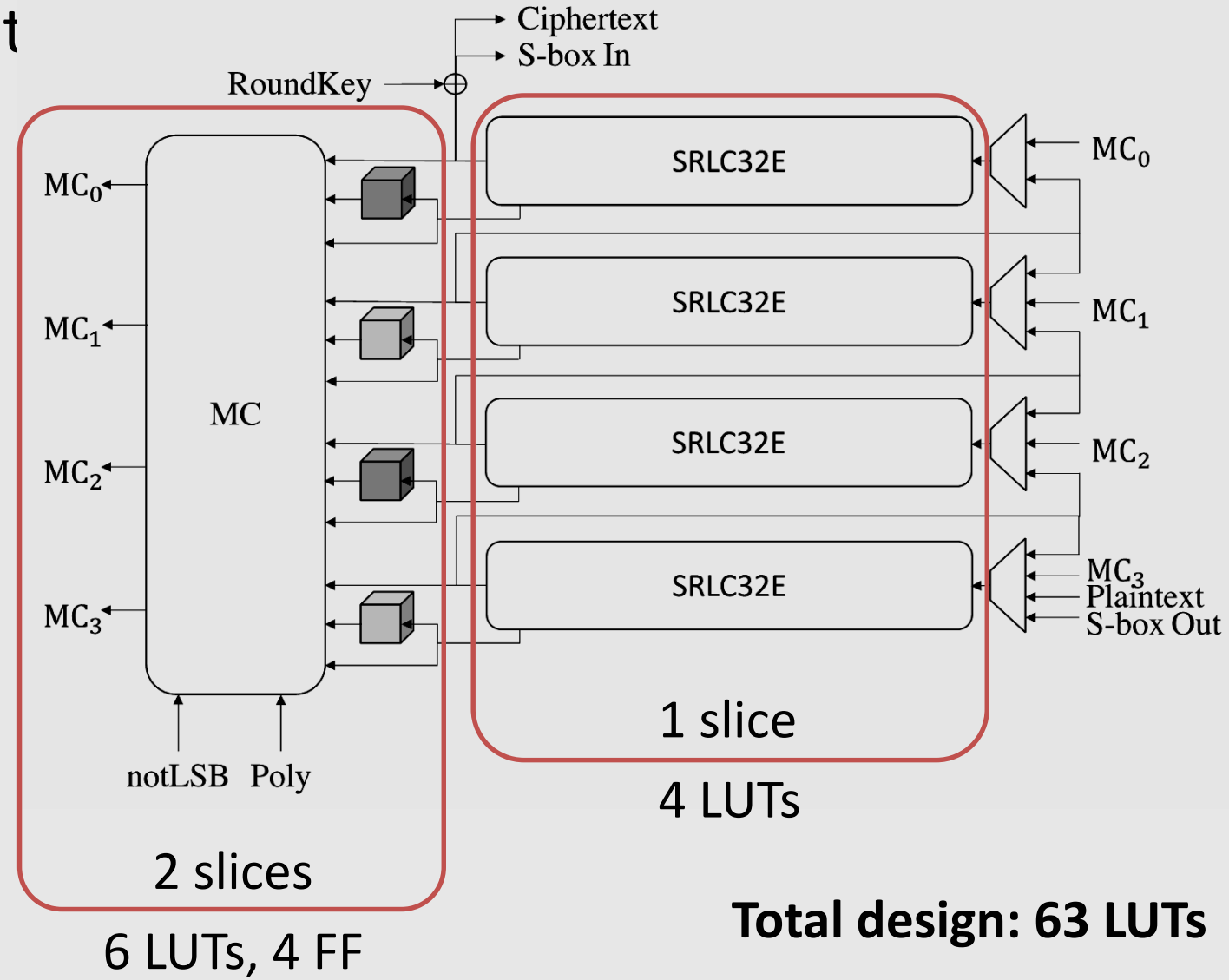
[1] Jean, Moradi, Peyrin, Sasdrich. *Bit-sliding: A generic technique for bit-serial implementations of SPN-based primitives - applications to AES, PRESENT and SKINNY*. CHES 2017

Bitsliding on an FPGA

- 4 LUTs as 32-bit shift registers
- Shiftrows:

  32 cycles
- Mixcolumns:

  32 cycles



Total design: 63 LUTs

Comparison

Design	# LUTs	# Flipflops	# Slices	#Clockcyc.	Max. Freq.
Sasdrich *et al.* [SG16]	84	**24**	21	**1471**	108 Mhz
Our AES based on [SG16]	68	39	**17**	5538	109 Mhz
Our AES based on [JMPS17]	**63**	38	19	4852	155 Mhz

[SG16] Sasdrich, Güneysu. *A grain in the silicon: SCA-protected AES in less than 30 slices*. ASAP 2016
[JMPS17] Jean, Moradi, Peyrin, Sasdrich. *Bit-sliding: A generic technique for bit-serial implementations of SPN-based primitives - applications to AES, PRESENT and SKINNY*. CHES 2017

Third Design:
Smallest First-order secure AES on FPGAs

Masking

- Decomposition into cubic function[1]:

$$x^{-1} = x^{254} = (x^{26})^{49}$$

- Implement **one** coordinate of each cubic function:

$$G^*(\phi(x)) = \phi(x^{26}), \qquad F^*(\phi(x)) = \phi(x^{49})$$

[1] Moradi. *Advances in Side-channel Security.* 2016

Masking

- Decomposition into cubic function[1]:

$$x^{-1} = x^{254} = (x^{26})^{49}$$

- Implement **one** coordinate of each cubic function:

$$G^*(\phi(x)) = \phi(x^{26}), \qquad F^*(\phi(x)) = \phi(x^{49})$$

- Find first-order masking (CMS[2]):

  any-order: $d + 1$ input sh. / $(d + 1)^t$ output sh.

  first-order: 2 input shares / 8 output shares

[1] Moradi. *Advances in Side-channel Security.* 2016

[2] Reparaz, Bilgin, Nikova, Gierlichs, Verbauwhede. *Consolidating masking schemes*. CRYPTO 2015

Masking

- Decomposition into cubic function[1]:

$$x^{-1} = x^{254} = (x^{26})^{49}$$

- Implement **one** coordinate of each cubic function:

$$G^*(\phi(x)) = \phi(x^{26}), \qquad F^*(\phi(x)) = \phi(x^{49})$$

- Find first-order masking (CMS[2]):

  any-order: $d + 1$ input sh. / $(d + 1)^t$ output sh.

  first-order: 2 input shares / 8 output shares

Problem: How to find CMS sharing of cubic function?

[1] Moradi. *Advances in Side-channel Security.* 2016

[2] Reparaz, Bilgin, Nikova, Gierlichs, Verbauwhede. *Consolidating masking schemes*. CRYPTO 2015

Masking

- Decomposition into cubic function[1]:
-
-

Solution: Our Heuristic

Split function G into parts: G^A, G^B, G^C

2 input shares / 8 output shares each

(Details in the paper)

es

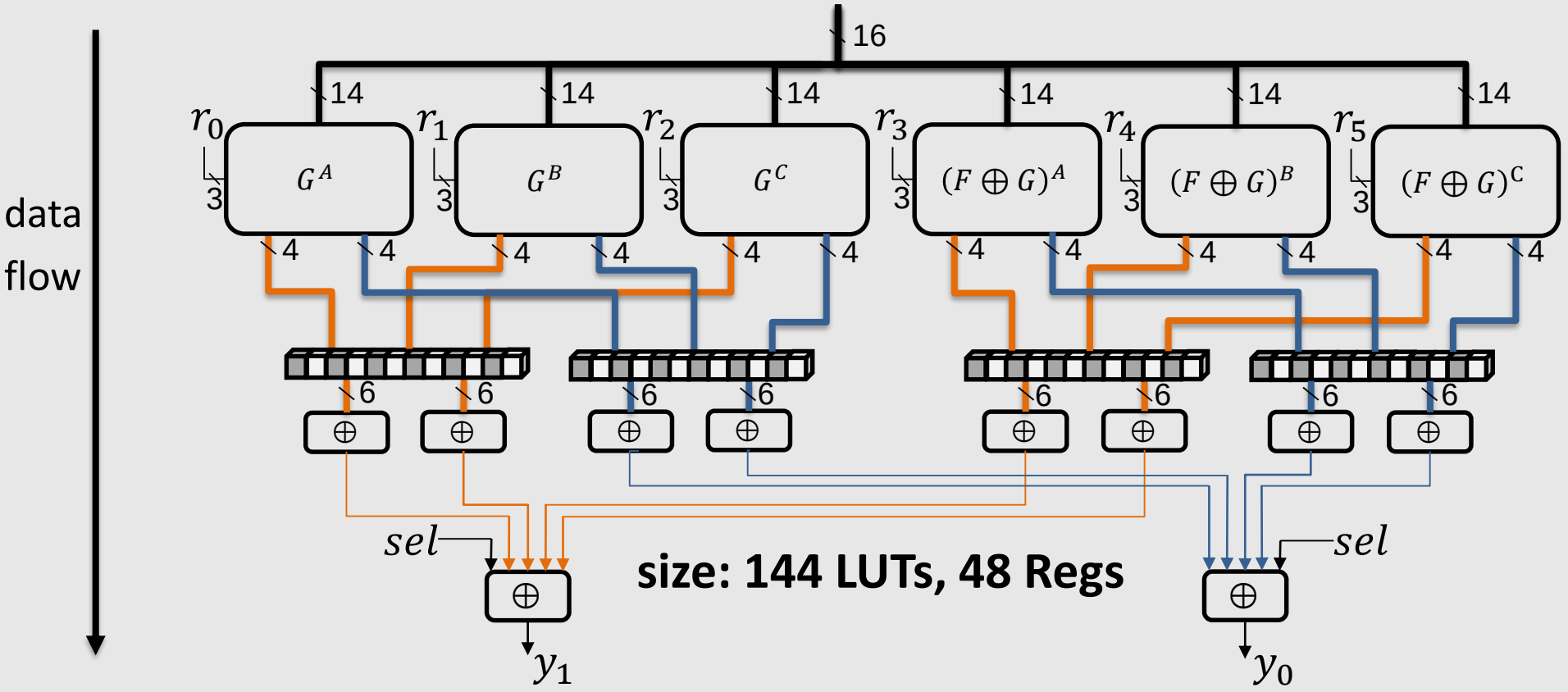
Pro on?

[1] Moradi. *Advances in Side-channel Security.* 2016

[2] Reparaz, Bilgin, Nikova, Gierlichs, Verbauwhede. *Consolidating masking schemes*. CRYPTO 2015

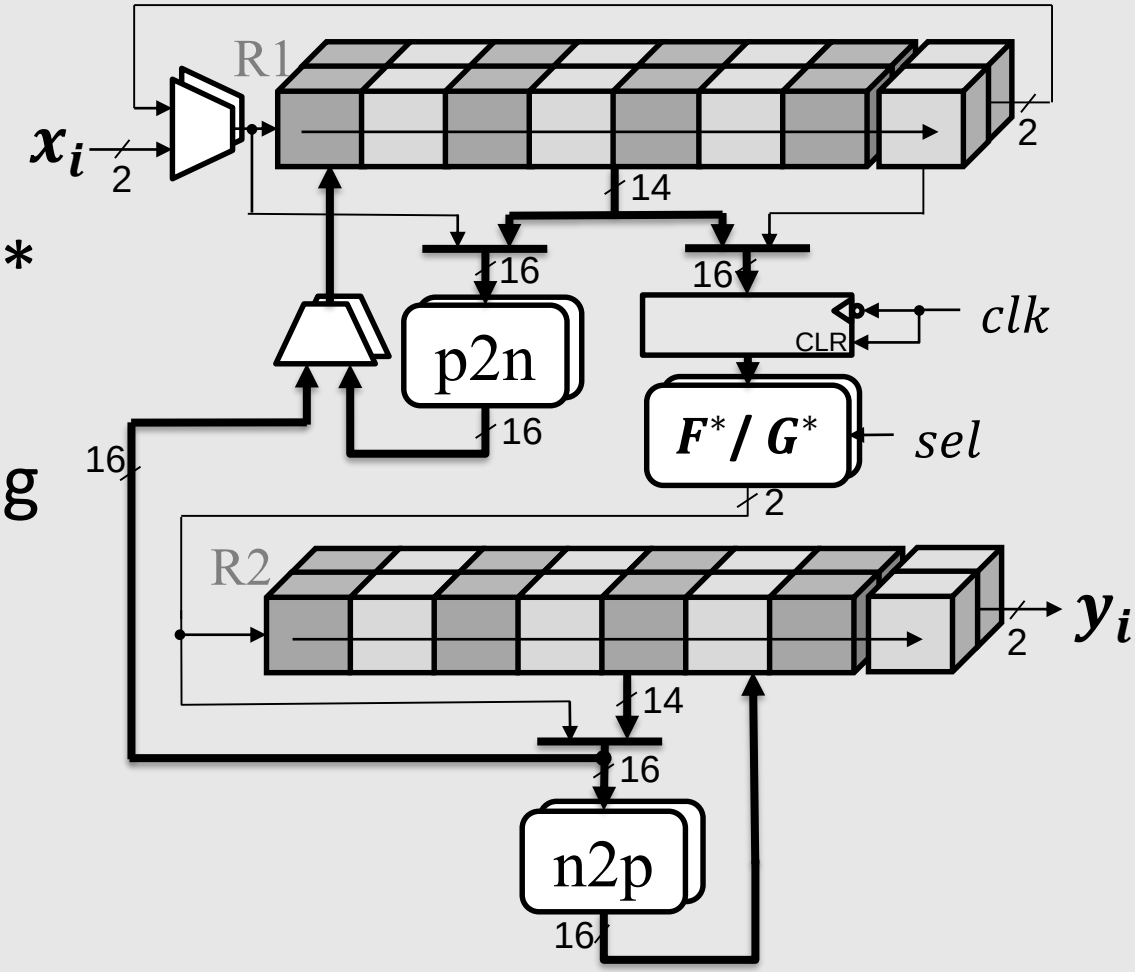
Non-complete realization of F*/G*

- 18 bits of randomness / cycle
- Dependence on only 14 bits each reduces area



Two-share S-box

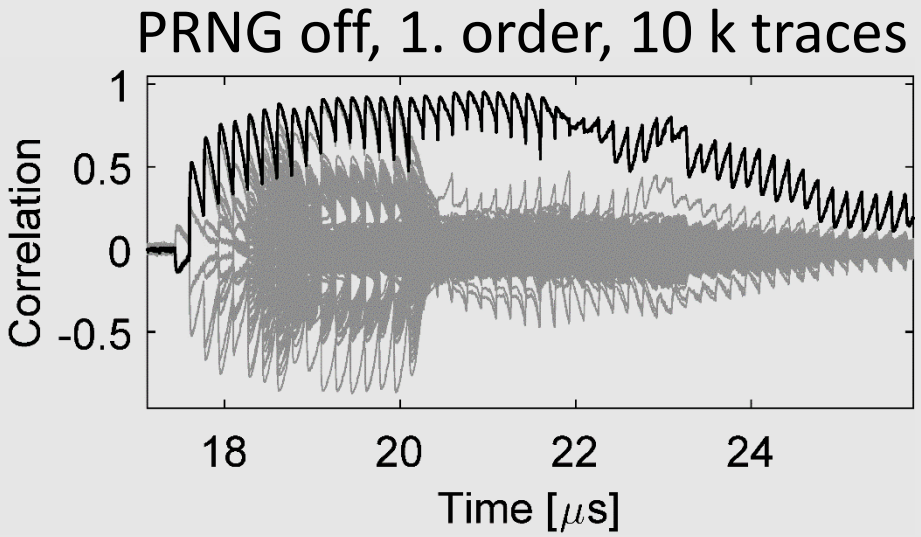
- First-order secure design
- Clear register to F*/G* on negative edge
- Area: 182 LUTs, 96 Reg
- Latency: 26 cycles



SCA Evaluation: Moments-Correlating DPA

Measurement Setup:

- Sakura-G platform
- Oscilloscope: 625 MS/s
- Target: 6 MHz
- Additional AC amplifier

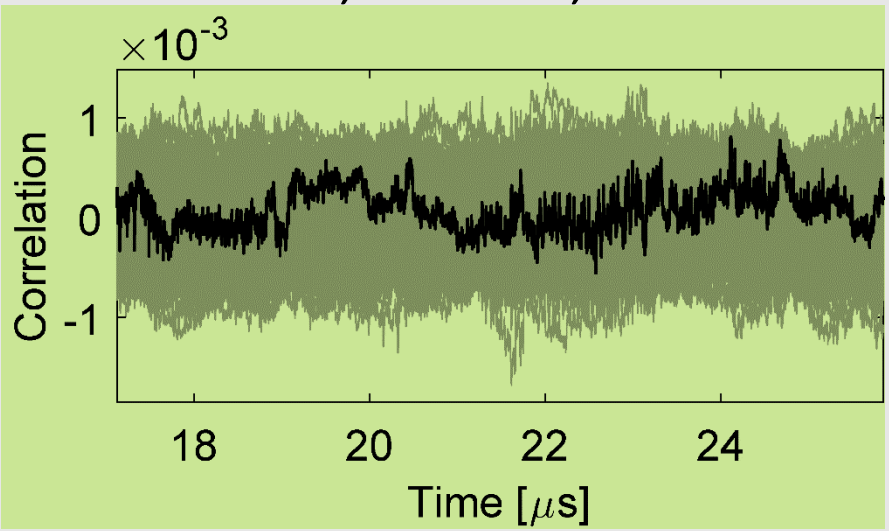


SCA Evaluation: Moments-Correlating DPA

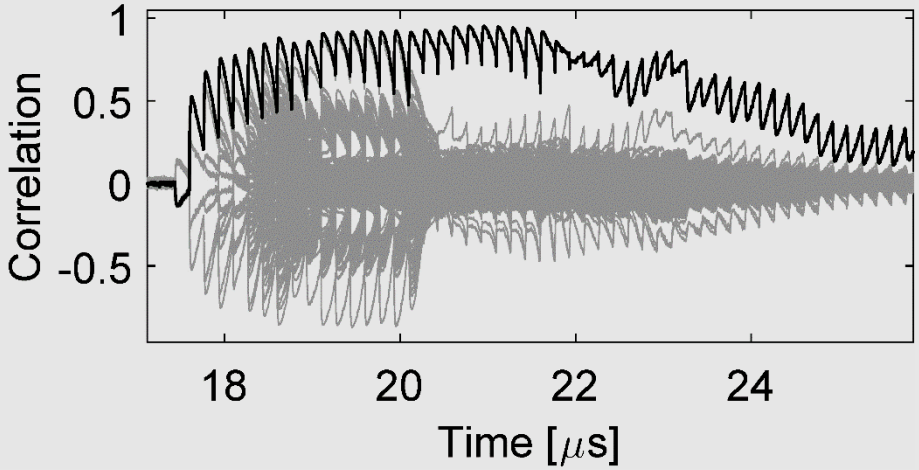
Measurement Setup:

- Sakura-G platform
- Oscilloscope: 625 MS/s
- Target: 6 MHz
- Additional AC amplifier

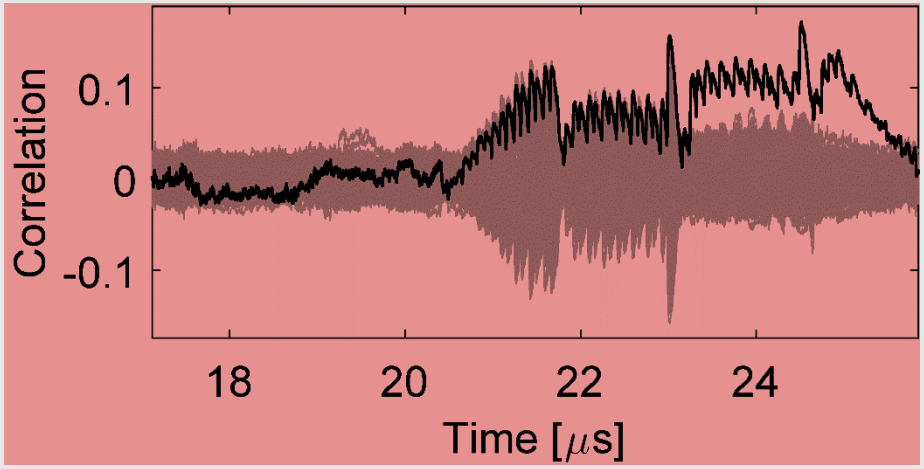
PRNG on, 1. order, 10 M traces



PRNG off, 1. order, 10 k traces



PRNG on, 2. order, 10 k traces



Comparison: First-order secure Designs

Design	# LUTs	# FF	# Slices	#Cycles	#Rand. Bits	Max. Freq.
Bilgin et al. [BGN+15]	1198	611	475	**246**	32	127 MHz
Gross et al [GMK17]	595	734	366	**246**	**18**	103 MHz
Cnudde et al [CRB+16]	1191	642	553	275	54	181 MHz
This work	**293**	**124**	**162**	6852	**18**	103 MHz

[BGN+15] Bilgin, Gierlichs, Nikova, Nikov, Rijmen. *Trade-offs for threshold implementations illustrated on AES*. IEEE TCAD 2015.
[GMK17] Groß, Mangard, Korak. *An efficient side-channel protected AES implementation with arbitrary protection order*. CT-RSA 2017
[CRB+16] De Cnudde, Reparaz, Bilgin, Nikova, Nikov, Rijmen. *Masking AES with d+1 shares in hardware*. CHES 2016

Summary

This presentation:

- New size-record for FPGA-specific AES
- Smallest first-order secure AES on FPGA devices

Further contributions in the paper:

- Latency optimizations for the Sasdrich *et al.* design
- New heuristic to mask Boolean functions with d + 1 Shares

KU LEUVEN

RUB

Thanks!

any questions?

felix.wegener@rub.de

Lauren De Meyer[1], Amir Moradi[2], Felix Wegener[2]

[1] imec - COSIC, KU Leuven, Belgium
[2] Horst Görtz Institute for IT-Security, Ruhr-Universität Bochum, Germany

COSIC

hgi Horst Görtz Institute for IT-Security