



COSIC

FIDES: Lightweight Authentication Cipher with Side-Channel Resistance for Constrained Hardware

Begül Bilgin, Andrey Bogdanov, Miroslav Knežević,
Florian Mendel, and Qingju Wang



Side Channel Resistance

Side Channel Resistance

The Game...

Side Channel Resistance

The Game...

- ▶ **Mathematically secure crypto algorithms**

Side Channel Resistance

The Game...

- ▶ Mathematically secure crypto algorithms
 - ✓ AES, RSA, Keccak, OCB, ...



Side Channel Resistance

The Game...

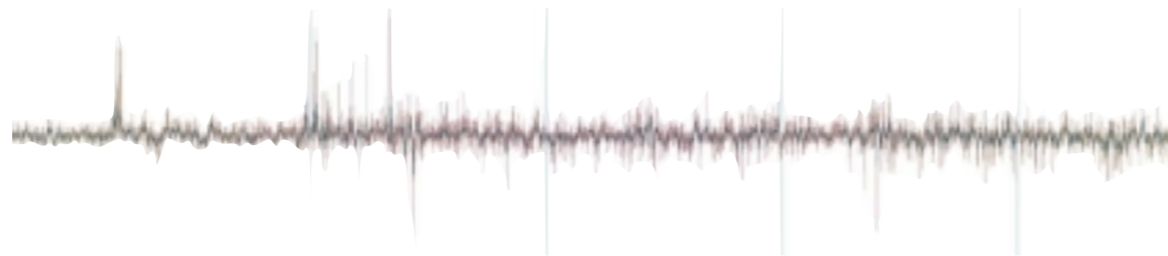
- ▶ Mathematically secure crypto algorithms
 - ✓ AES, RSA, Keccak, OCB, ...
- ▶ Weak implementation



Side Channel Resistance

The Game...

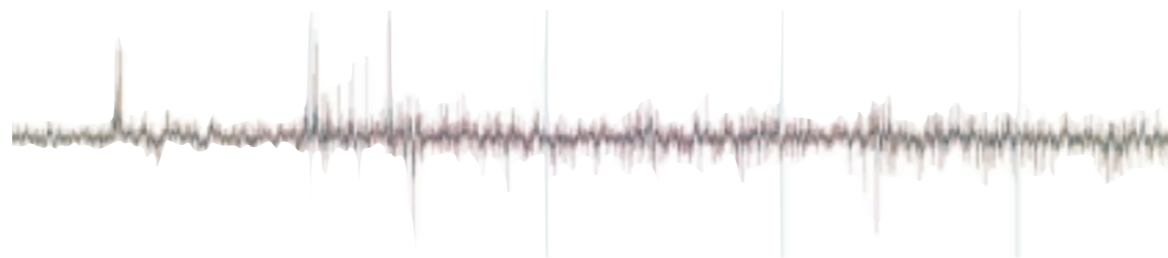
- ▶ Mathematically secure crypto algorithms
 - ✓ AES, RSA, Keccak, OCB, ...
- ▶ Weak implementation



Side Channel Resistance

The Game...

- ▶ Mathematically secure crypto algorithms
 - ✓ AES, RSA, Keccak, OCB, ...
- ▶ Weak implementation



Dependency between power consumption and intermediate value (depends on the key)

Side Channel Resistance

Side Channel Resistance

x Change the key frequently

Side Channel Resistance

- ✗ Change the key frequently
- ✗ Equalize power consumption

Side Channel Resistance

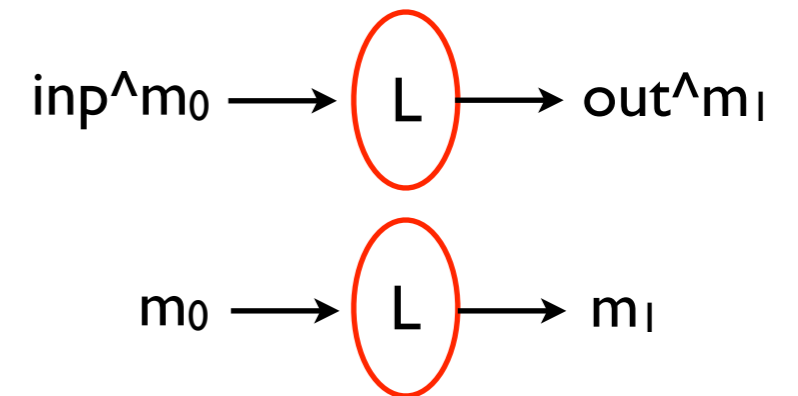
- ✗ Change the key frequently
- ✗ Equalize power consumption
- ✓ Randomize power consumption

Side Channel Resistance

- ✗ Change the key frequently
- ✗ Equalize power consumption
- ✓ Randomize power consumption
 - Boolean masking

Side Channel Resistance

- ✗ Change the key frequently
- ✗ Equalize power consumption
- ✓ Randomize power consumption
 - Boolean masking

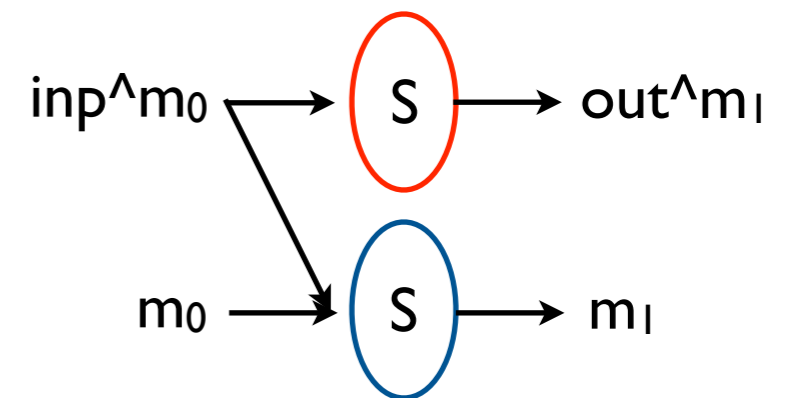


Side Channel Resistance

- ✗ Change the key frequently
- ✗ Equalize power consumption
- ✓ Randomize power consumption
 - Boolean masking

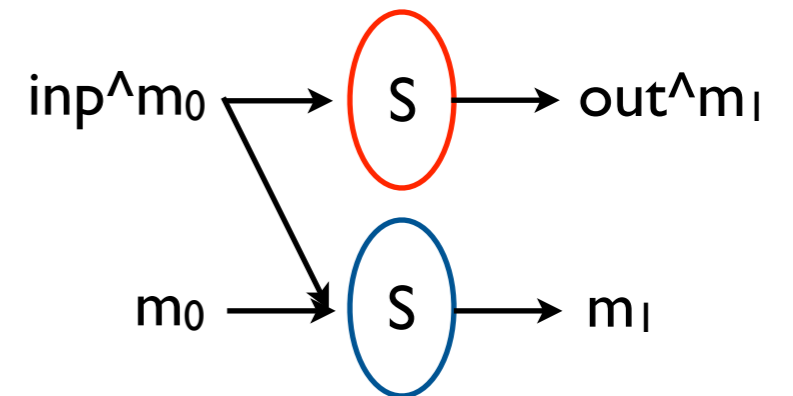
Side Channel Resistance

- ✗ Change the key frequently
- ✗ Equalize power consumption
- ✓ Randomize power consumption
 - Boolean masking



Side Channel Resistance

- ✗ Change the key frequently
- ✗ Equalize power consumption
- ✓ Randomize power consumption
 - Boolean masking
 - Multiplicative masking



Side Channel Resistance

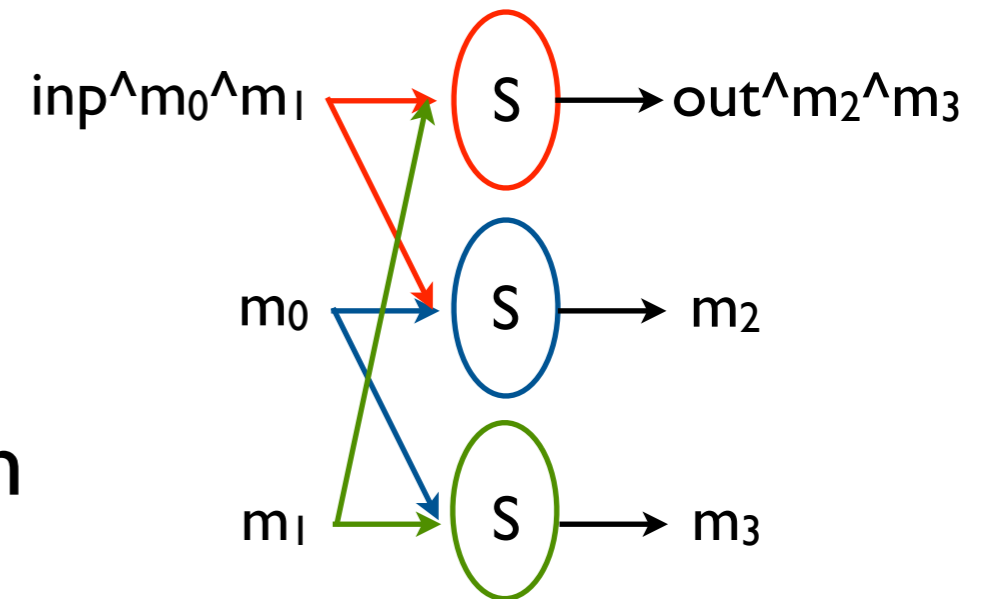
- ✗ Change the key frequently
- ✗ Equalize power consumption
- ✓ Randomize power consumption
 - Boolean masking
 - Multiplicative masking

Side Channel Resistance

- ✗ Change the key frequently
- ✗ Equalize power consumption
- ✓ Randomize power consumption
 - Boolean masking
 - Multiplicative masking
 - Secret sharing e.g. Threshold Implementations [Nikova'11]

Side Channel Resistance

- ✗ Change the key frequently
- ✗ Equalize power consumption
- ✓ Randomize power consumption
 - Boolean masking
 - Multiplicative masking
 - Secret sharing e.g. Threshold Implementations [Nikova'11]



Side Channel Resistance

Side Channel Resistance

Have the
design



Side Channel Resistance

Need
efficient impl.

Have the
design



Side Channel Resistance

Need
efficient impl.



Have the
design



Need
secure impl.



Side Channel Resistance

Need efficient impl.

Have the design

Need secure impl.

A cartoon boy with orange hair, wearing a green shirt and blue pants, sits on a large pile of red puzzle pieces. He has a confused expression, with wide eyes and a slightly open mouth. He is holding two puzzle pieces in his hands. The puzzle pieces are scattered around him, some forming a path.

1st Order

Multipl. Mask

Boolean Mask

TI

2nd Order

SW

HW

?? Still efficient ??

Side Channel Resistance

Need efficient impl.

Have the design

Need secure impl.

A cartoon boy with orange hair, wearing a green shirt and blue pants, sits on a large pile of red puzzle pieces. He has a worried expression, with wide eyes and a slightly open mouth. He is holding two puzzle pieces in his hands. The scene is surrounded by various labels: '1st Order' and 'Boolean Mask' to the left; 'Multipl. Mask' and 'TI' to the right; '2nd Order' to the left of the pile; 'SW' and 'HW' to the right of the pile; and 'Still efficient' at the bottom center.

1st Order

Boolean Mask

Multipl. Mask

TI

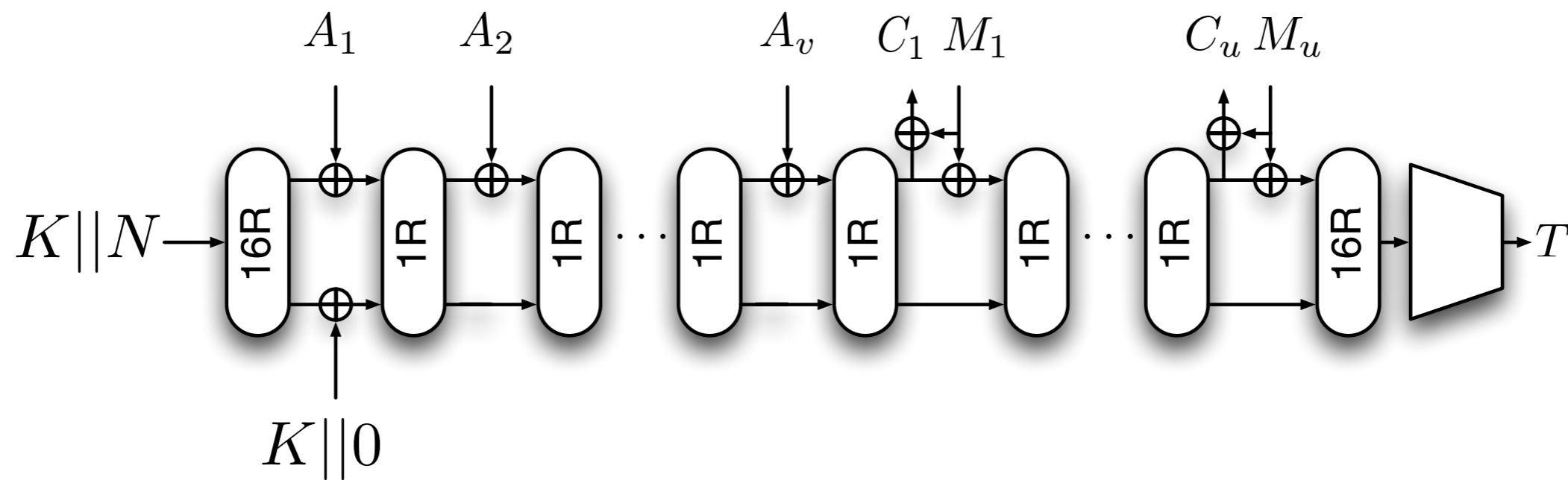
2nd Order

SW

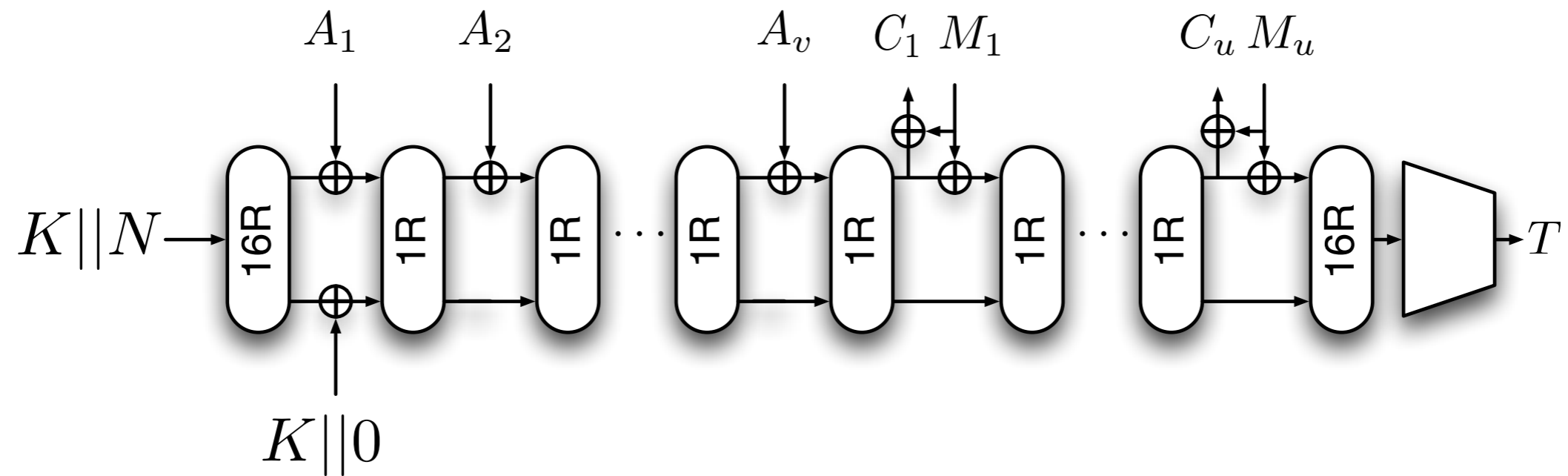
HW

Still efficient

Design - Structure

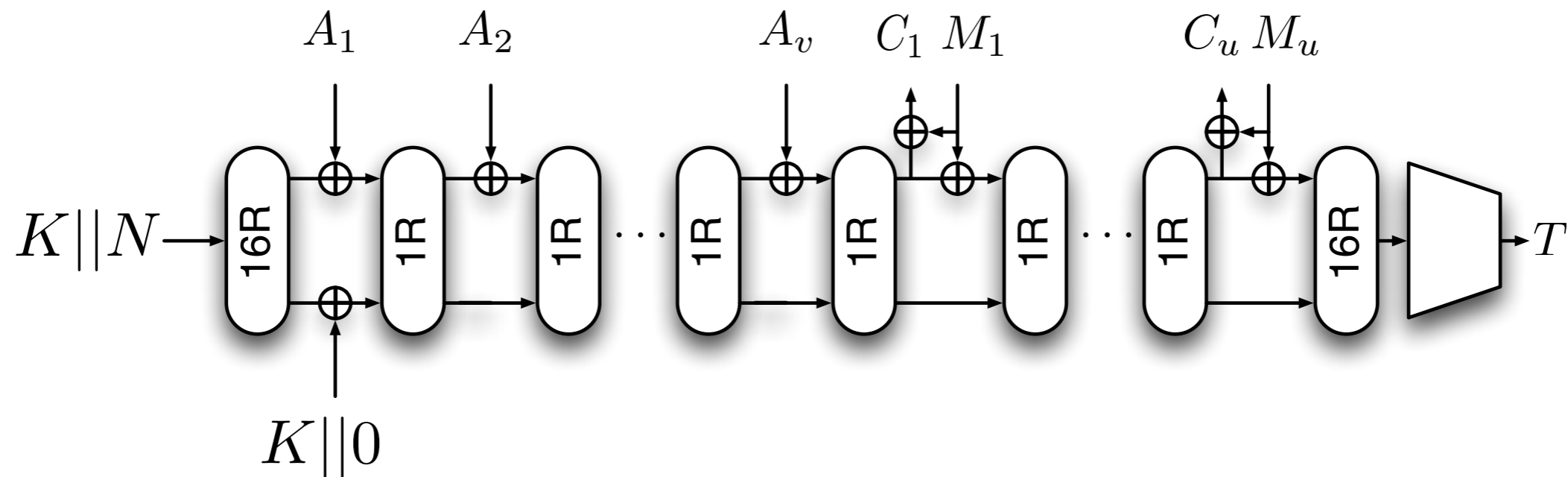


Design - Structure



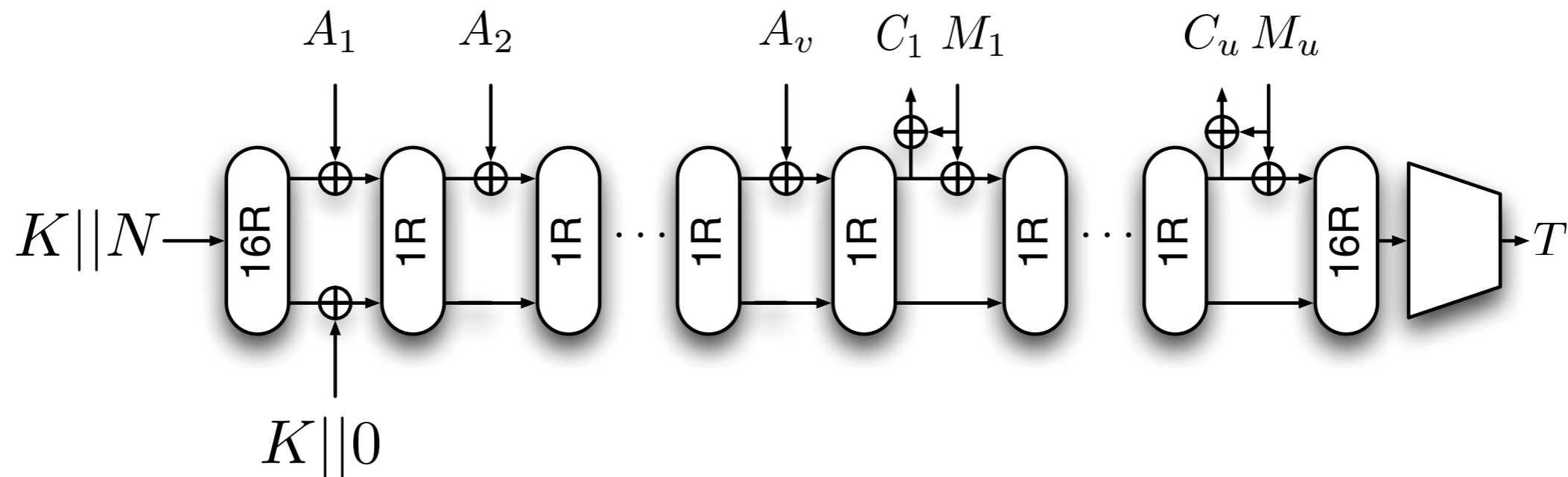
- Similar to duplex sponge

Design - Structure



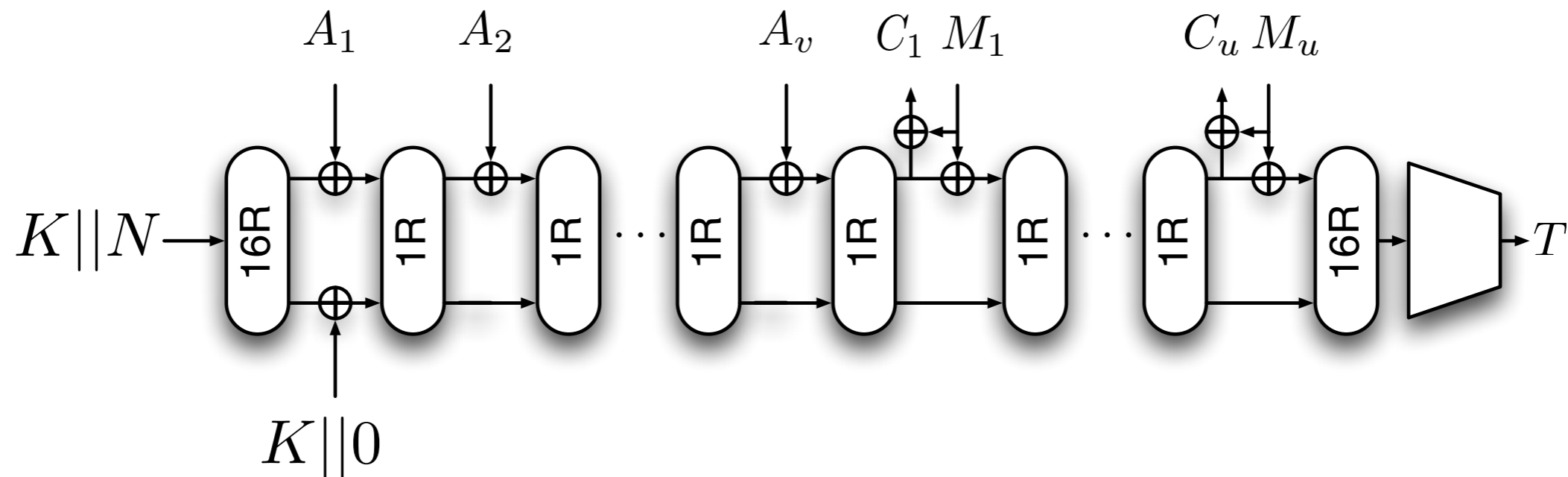
- Similar to duplex sponge
- Rounds are not keyed

Design - Structure



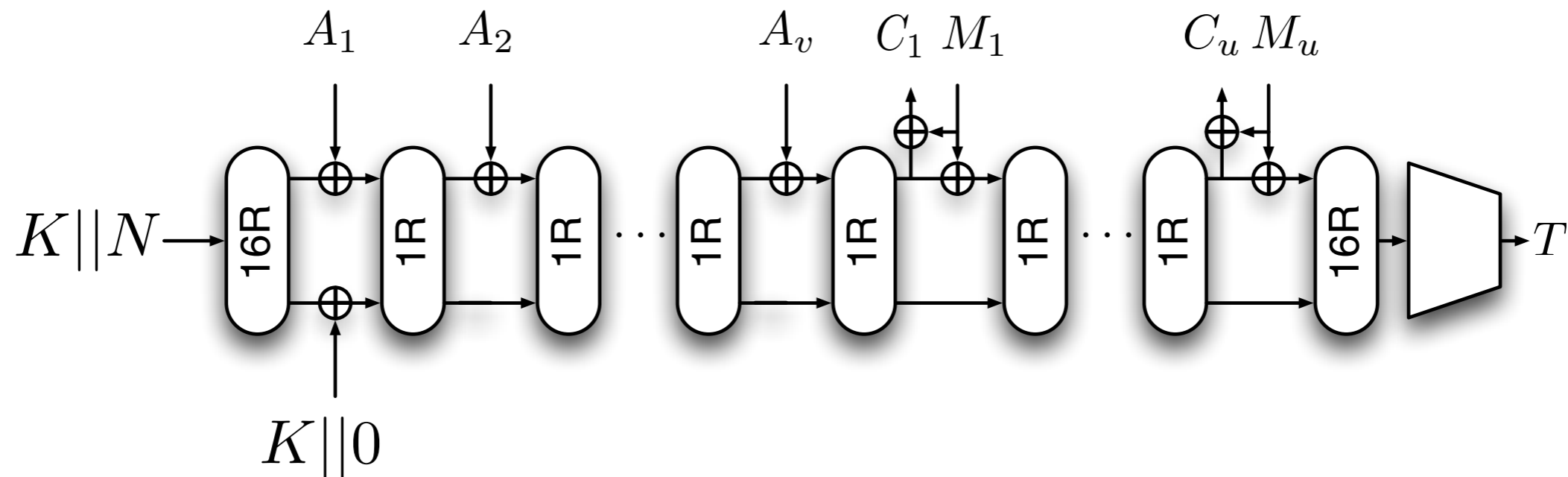
- Similar to duplex sponge
- Rounds are not keyed
- ✓ Online

Design - Structure



- Similar to duplex sponge
- Rounds are not keyed
- ✓ Online
- ✓ Single pass

Design - Structure

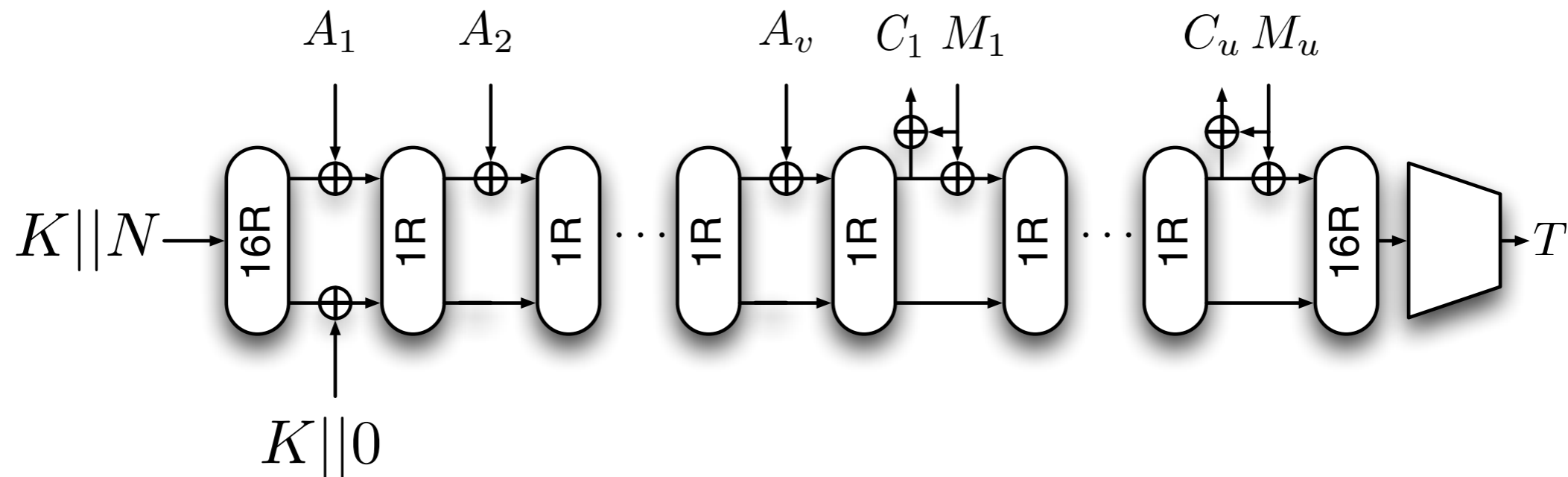


- Similar to duplex sponge
- Rounds are not keyed
- ✓ Online
- ✓ Single pass

FIDES-80

FIDES-96

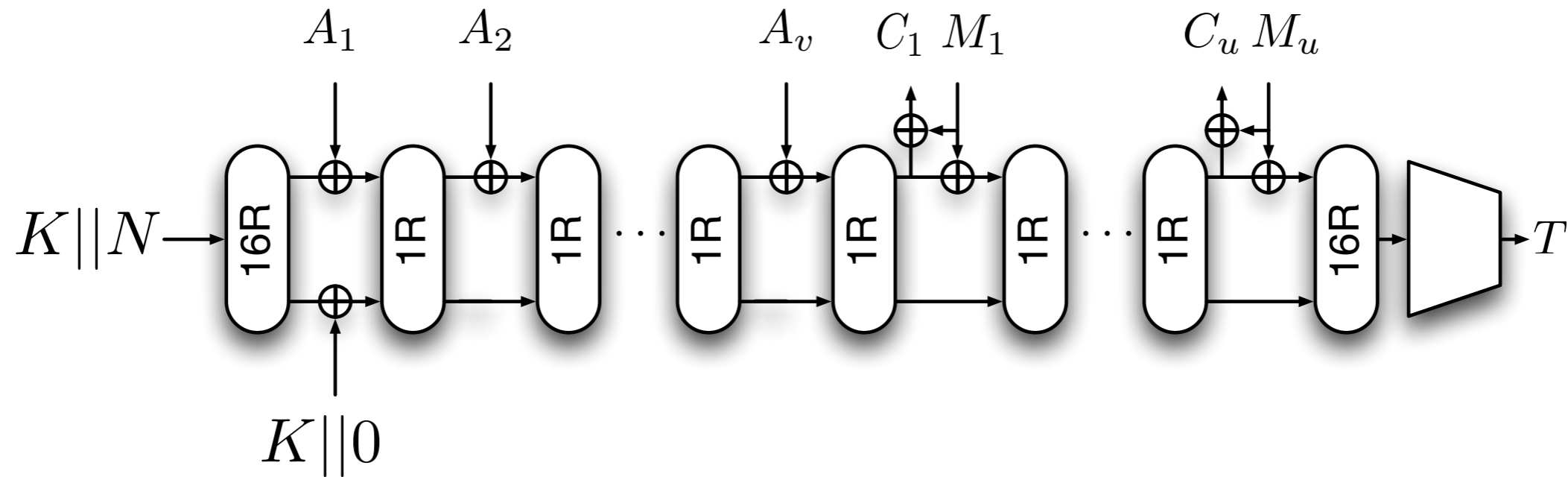
Design - Structure



- Similar to duplex sponge
- Rounds are not keyed
- ✓ Online
- ✓ Single pass

	b
FIDES-80	160
FIDES-96	192

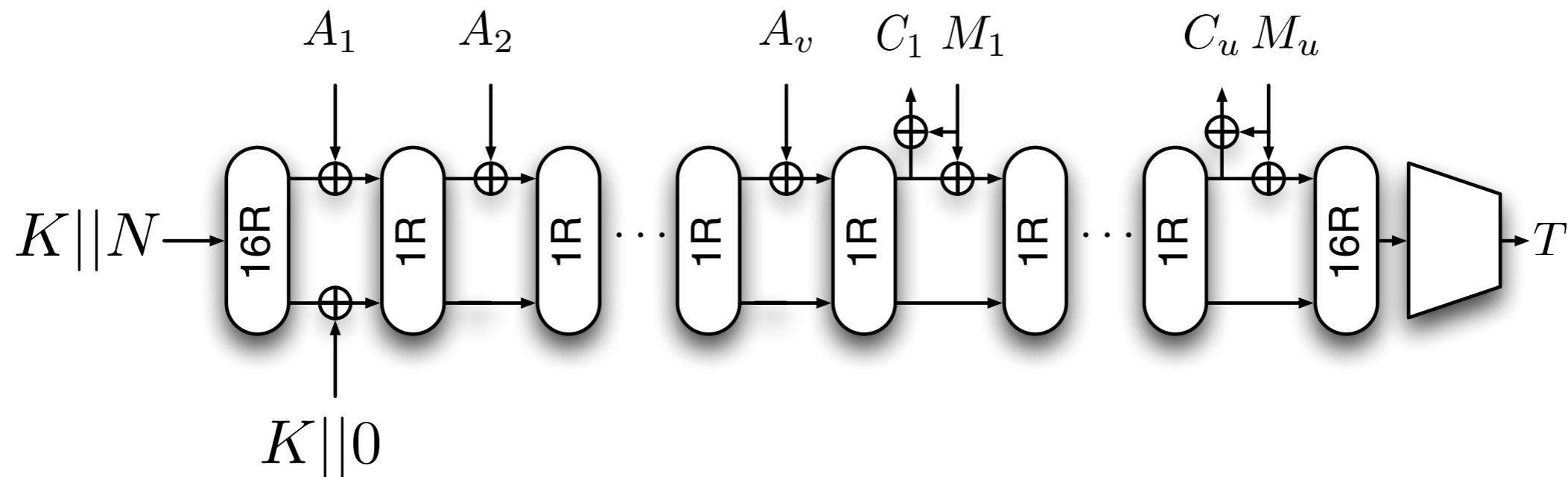
Design - Structure



- Similar to duplex sponge
- Rounds are not keyed
- ✓ Online
- ✓ Single pass

	b	$k/n/t$
FIDES-80	160	80
FIDES-96	192	96

Design - Structure



- Similar to duplex sponge
- Rounds are not keyed
- ✓ Online
- ✓ Single pass

	b	$k/n/t$	r
FIDES-80	160	80	10
FIDES-96	192	96	12

Design - Structure

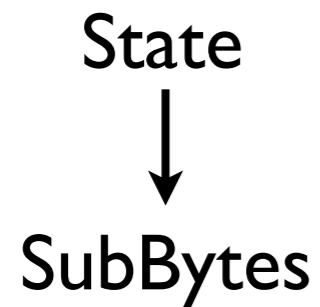
1R

State

$a_{0,0}$	$a_{0,1}$	$a_{0,2}$	$a_{0,3}$	$a_{0,4}$	$a_{0,5}$	$a_{0,6}$	$a_{0,7}$
$a_{1,0}$	$a_{1,1}$	$a_{1,2}$	$a_{1,3}$	$a_{1,4}$	$a_{1,5}$	$a_{1,6}$	$a_{1,7}$
$a_{2,0}$	$a_{2,1}$	$a_{2,2}$	$a_{2,3}$	$a_{2,4}$	$a_{2,5}$	$a_{2,6}$	$a_{2,7}$
$a_{3,0}$	$a_{3,1}$	$a_{3,2}$	$a_{3,3}$	$a_{3,4}$	$a_{3,5}$	$a_{3,6}$	$a_{3,7}$

Design - Structure

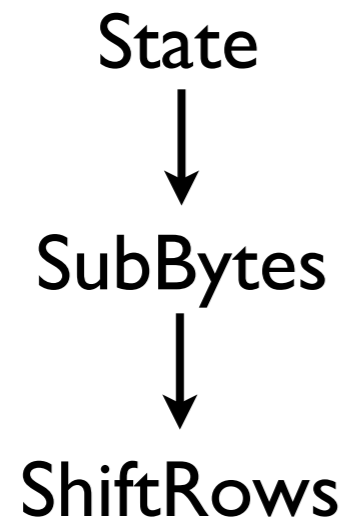
1R



$a_{0,0}$	$a_{0,1}$	$a_{0,2}$	$a_{0,3}$	$a_{0,4}$	$a_{0,5}$	$a_{0,6}$	$a_{0,7}$
$a_{1,0}$	$a_{1,1}$	$a_{i,j}$	$a_{1,3}$	$a_{1,4}$	$a_{1,5}$	$a_{1,6}$	$a_{1,7}$
$a_{2,0}$	$a_{2,1}$	$a_{2,2}$	$a_{2,3}$	$a_{2,4}$	$a_{2,5}$	$a_{2,6}$	$a_{2,7}$
$a_{3,0}$	$a_{3,1}$	$a_{3,2}$	$a_{3,3}$	$a_{3,4}$	$a_{3,5}$	$a_{3,6}$	$a_{3,7}$

Design - Structure

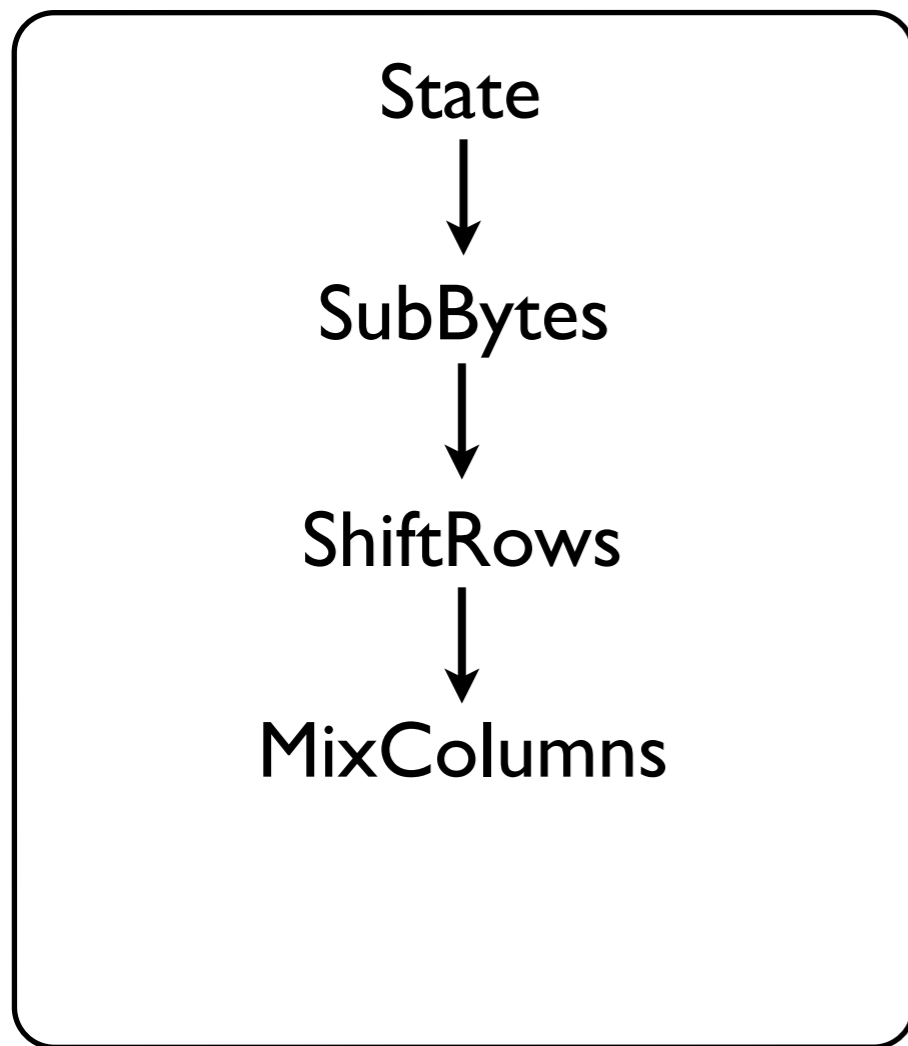
1R



$a_{0,0}$	$a_{0,1}$	$a_{0,2}$	$a_{0,3}$	$a_{0,4}$	$a_{0,5}$	$a_{0,6}$	$a_{0,7}$	0
$a_{i,0}$	$a_{i,1}$	$a_{i,2}$	$a_{i,3}$	$a_{i,4}$	$a_{i,5}$	$a_{i,6}$	$a_{i,7}$	1
$a_{2,0}$	$a_{2,1}$	$a_{2,2}$	$a_{2,3}$	$a_{2,4}$	$a_{2,5}$	$a_{2,6}$	$a_{2,7}$	2
$a_{3,0}$	$a_{3,1}$	$a_{3,2}$	$a_{3,3}$	$a_{3,4}$	$a_{3,5}$	$a_{3,6}$	$a_{3,7}$	7

Design - Structure

1R



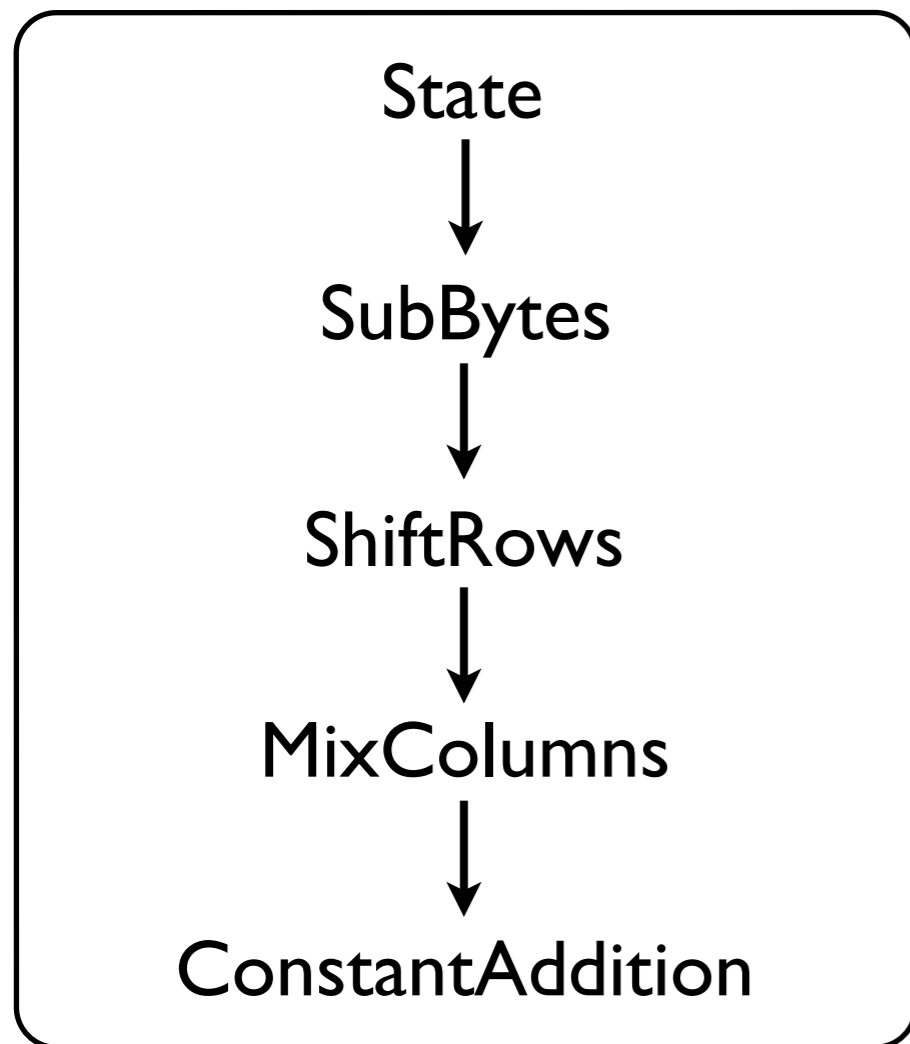
$a_{0,0}$	$a_{0,1}$	$a_{0,j}$	$a_{0,3}$	$a_{0,4}$	$a_{0,5}$	$a_{0,6}$	$a_{0,7}$
$a_{1,0}$	$a_{1,1}$	$a_{1,j}$	$a_{1,3}$	$a_{1,4}$	$a_{1,5}$	$a_{1,6}$	$a_{1,7}$
$a_{2,0}$	$a_{2,1}$	$a_{2,j}$	$a_{2,3}$	$a_{2,4}$	$a_{2,5}$	$a_{2,6}$	$a_{2,7}$
$a_{3,0}$	$a_{3,1}$	$a_{3,j}$	$a_{3,3}$	$a_{3,4}$	$a_{3,5}$	$a_{3,6}$	$a_{3,7}$

$$\otimes \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$$

Almost MDS
branch number is 4

Design - Structure

1R



Design - S-boxes

- FIDES-80: 5-bit Almost Bent (AB)
 - optimal resistance against differential & linear cryptanalysis
- FIDES-96: 6-bit Almost Perfect Nonlinear (APN)
 - optimal resistance against differential cryptanalysis

Design - S-boxes

- FIDES-80: 5-bit Almost Bent (AB)
 - optimal resistance against differential & linear cryptanalysis
- FIDES-96: 6-bit Almost Perfect Nonlinear (APN)
 - optimal resistance against differential cryptanalysis

++Low latency++

Design - S-boxes

- FIDES-80: 5-bit Almost Bent (AB)
 - optimal resistance against differential & linear cryptanalysis
 - degree 2 (two), 3(one), 4(one)
- FIDES-96: 6-bit Almost Perfect Nonlinear (APN)
 - optimal resistance against differential cryptanalysis
 - degree 4

++Low latency++

Design - S-boxes

- FIDES-80: 5-bit Almost Bent (AB)
 - optimal resistance against differential & linear cryptanalysis
 - **degree 2** (two), 3(one), 4(one)
- FIDES-96: 6-bit Almost Perfect Nonlinear (APN)
 - optimal resistance against differential cryptanalysis
 - **degree 4**

++Low latency++

Design - S-boxes

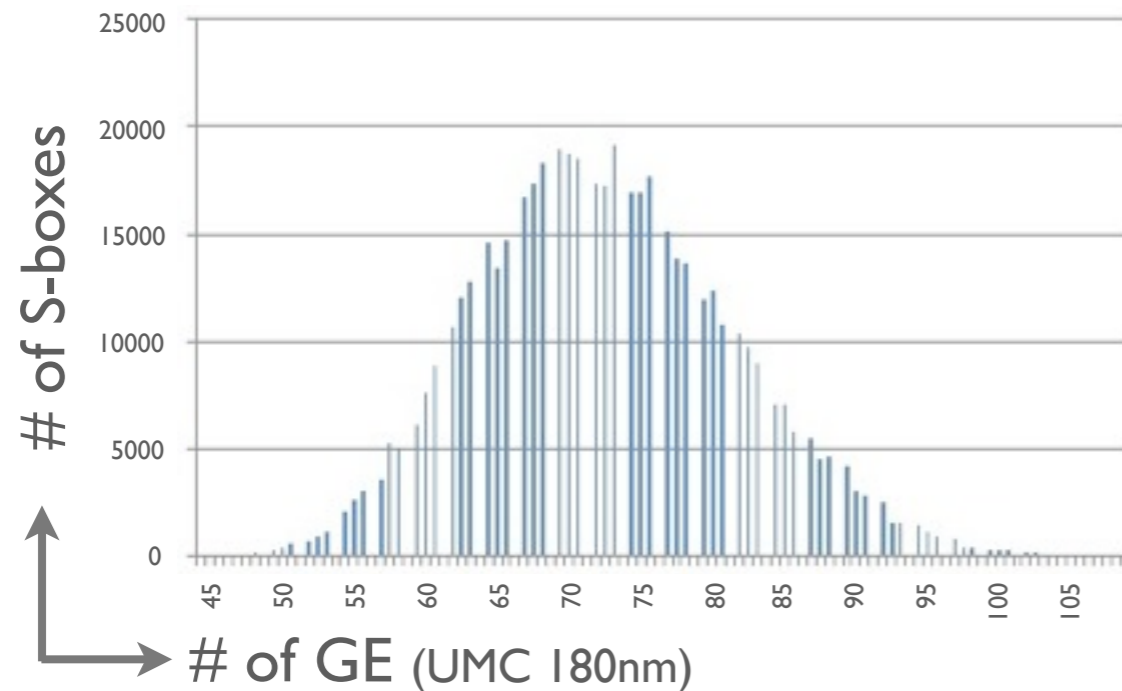
Design - S-boxes

Affine Equivalent to AB permutation with degree 2

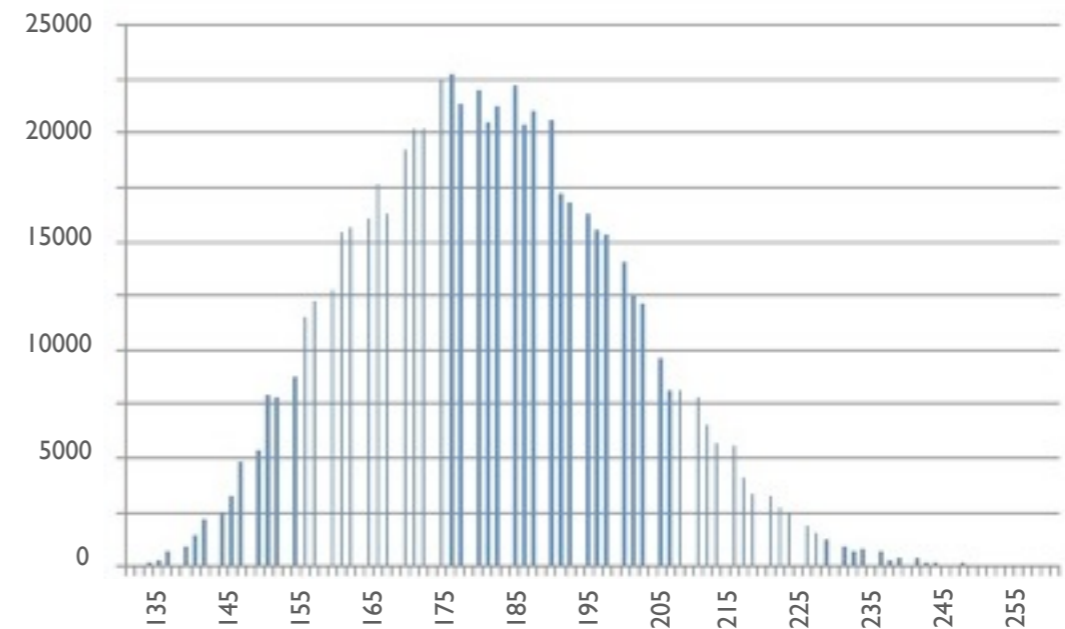
Design - S-boxes

Affine Equivalent to AB permutation with degree 2

Unshared S-box



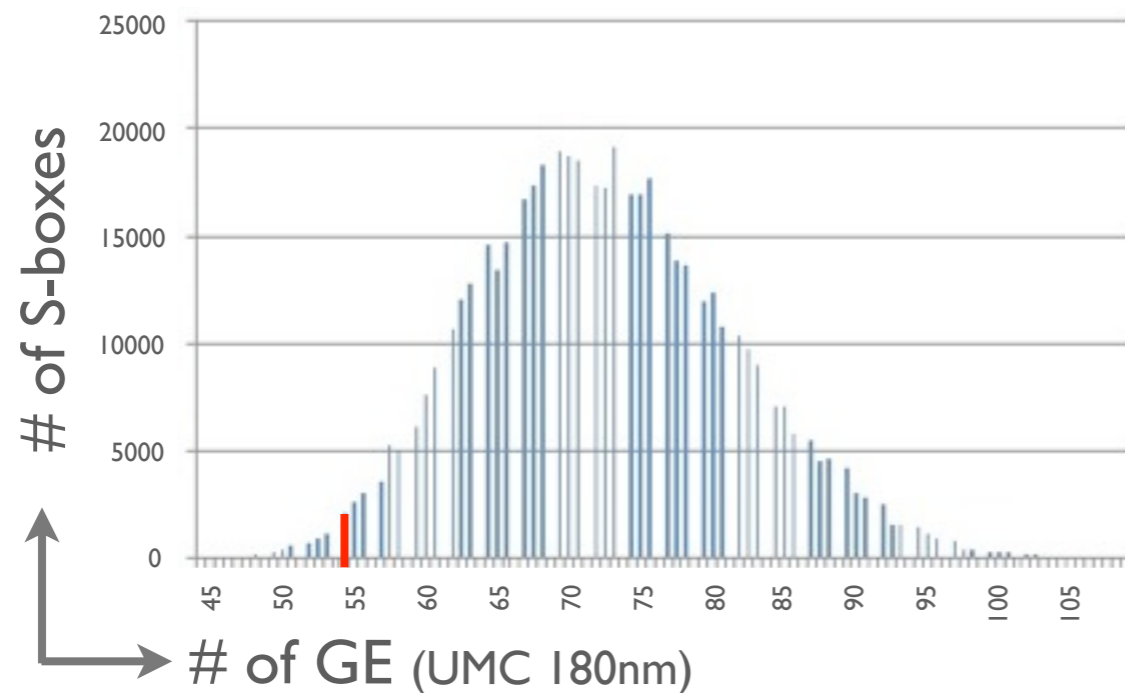
Shared S-box



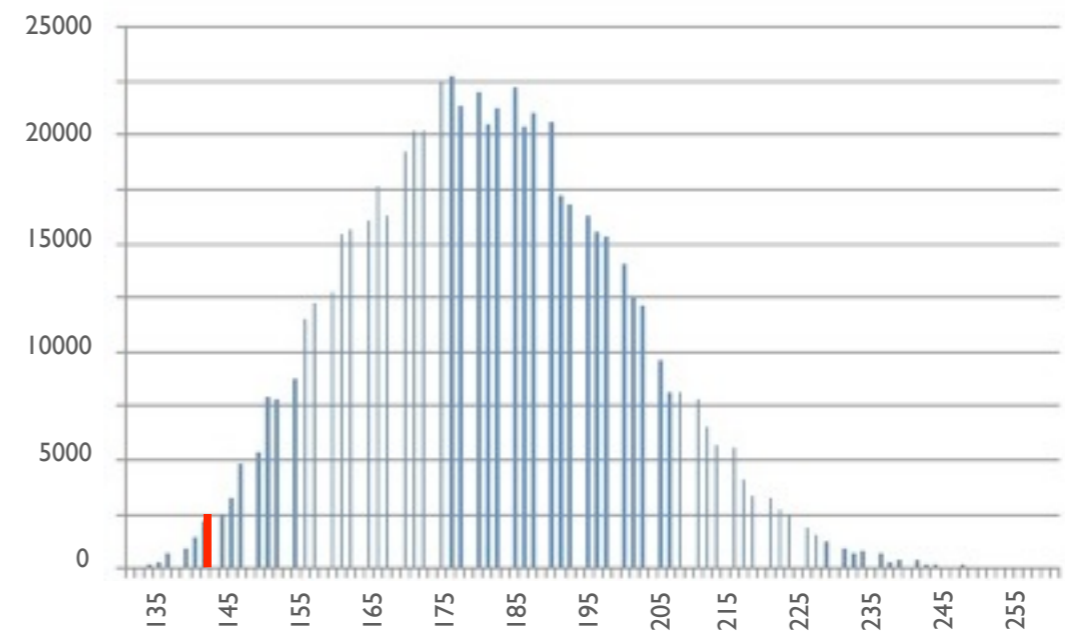
Design - S-boxes

Affine Equivalent to AB permutation with degree 2

Unshared S-box



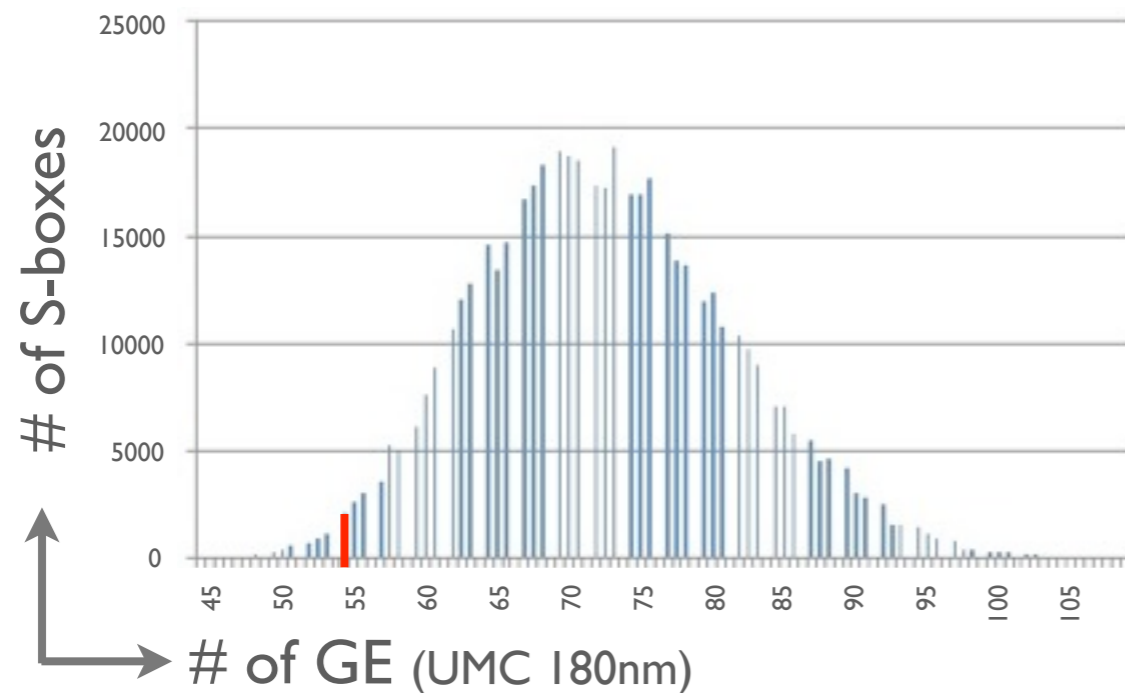
Shared S-box



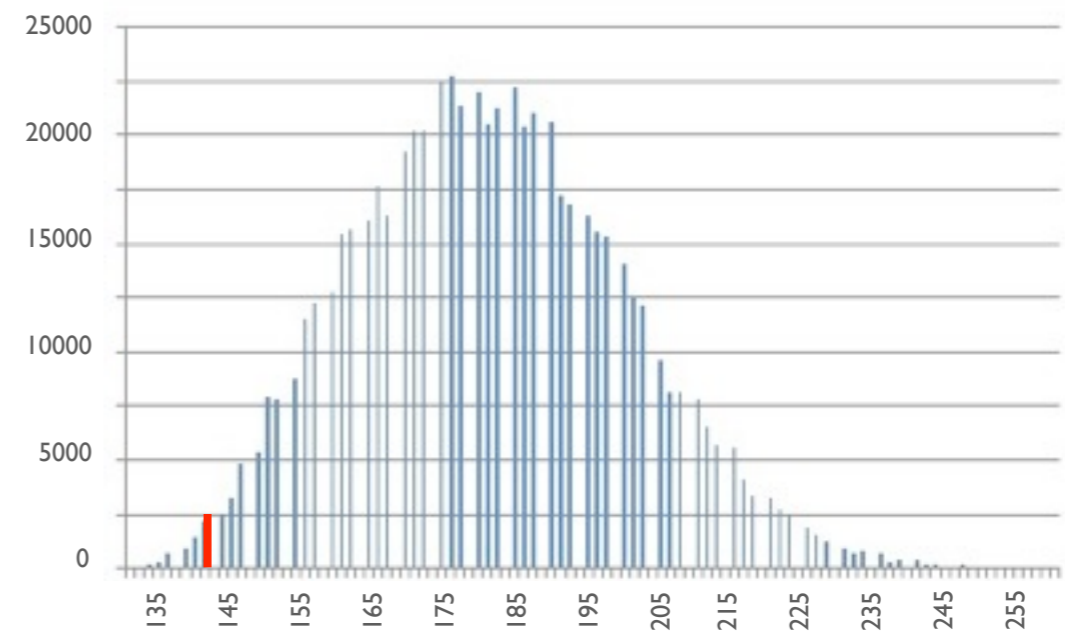
Design - S-boxes

Affine Equivalent to AB permutation with degree 2

Unshared S-box



Shared S-box



Similar for APN

Security Analysis

# rnd.	# Active S-box	
	any diff.	zero diff.
1	0	-
2	4	-
3	7	-
4	16	-
5	22	-
6	32	52
7	42	49
8	48	48

Security Analysis

# rnd.	# Active S-box	
	any diff.	zero diff.
1	0	-
2	4	-
3	7	-
4	16	-
5	22	-
6	32	52
7	42	49
8	48	48

- Differential & Linear Cryptanalysis

Security Analysis

# rnd.	# Active S-box	
	any diff.	zero diff.
1	0	-
2	4	-
3	7	-
4	16	-
5	22	-
6	32	52
7	42	49
8	48	48

- Differential & Linear Cryptanalysis
16 rounds: $2^{-4 \times 48 \times 2} = 2^{-384}$

Security Analysis

# rnd.	# Active S-box	
	any diff.	zero diff.
1	0	-
2	4	-
3	7	-
4	16	-
5	22	-
6	32	52
7	42	49
8	48	48

- Differential & Linear Cryptanalysis
16 rounds: $2^{-4 \times 48 \times 2} = 2^{-384}$
- Collision Trails

Security Analysis

# rnd.	# Active S-box	
	any diff.	zero diff.
1	0	-
2	4	-
3	7	-
4	16	-
5	22	-
6	32	52
7	42	49
8	48	48

- Differential & Linear Cryptanalysis
16 rounds: $2^{-4 \times 48 \times 2} = 2^{-384}$
- Collision Trails
16 rounds: $2^{-4 \times (48 + 48)} = 2^{-384}$

Security Analysis

# rnd.	# Active S-box	
	any diff.	zero diff.
1	0	-
2	4	-
3	7	-
4	16	-
5	22	-
6	32	52
7	42	49
8	48	48

- Differential & Linear Cryptanalysis
16 rounds: $2^{-4 \times 48 \times 2} = 2^{-384}$
- Collision Trails
16 rounds: $2^{-4 \times (48 + 48)} = 2^{-384}$
- Impossible Differential

Security Analysis

# rnd.	# Active S-box	
	any diff.	zero diff.
1	0	-
2	4	-
3	7	-
4	16	-
5	22	-
6	32	52
7	42	49
8	48	48

- Differential & Linear Cryptanalysis
16 rounds: $2^{-4 \times 48 \times 2} = 2^{-384}$
- Collision Trails
16 rounds: $2^{-4 \times (48 + 48)} = 2^{-384}$
- Impossible Differential
9 rounds

Implementation

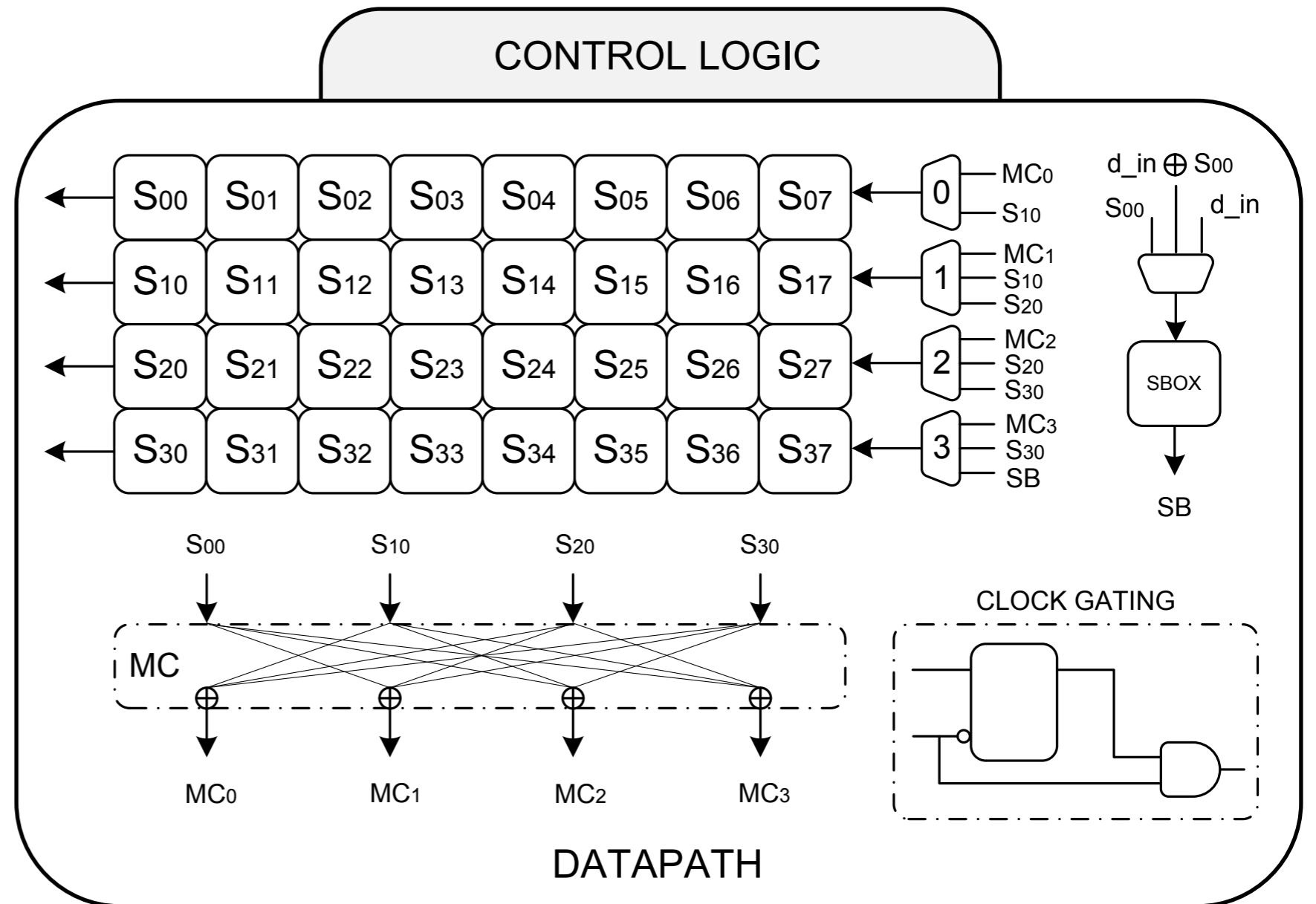
- FIDES-S
- FIDES-4S
- FIDES-R
- FIDES-T

Implementation

- FIDES-S
- FIDES-4S
- FIDES-R
- FIDES-T

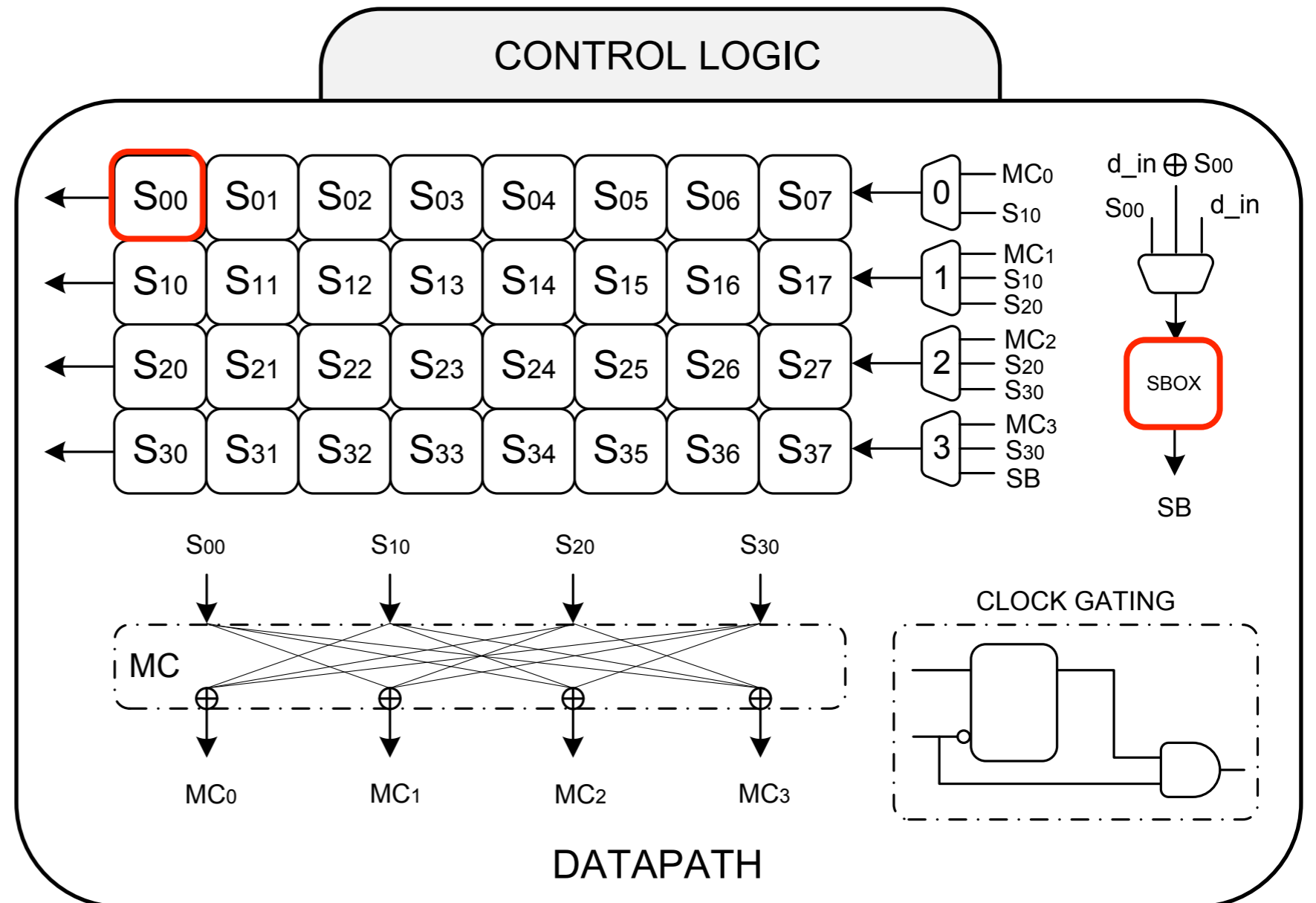
Implementation

- FIDES-S
- FIDES-4S
- FIDES-R
- FIDES-T



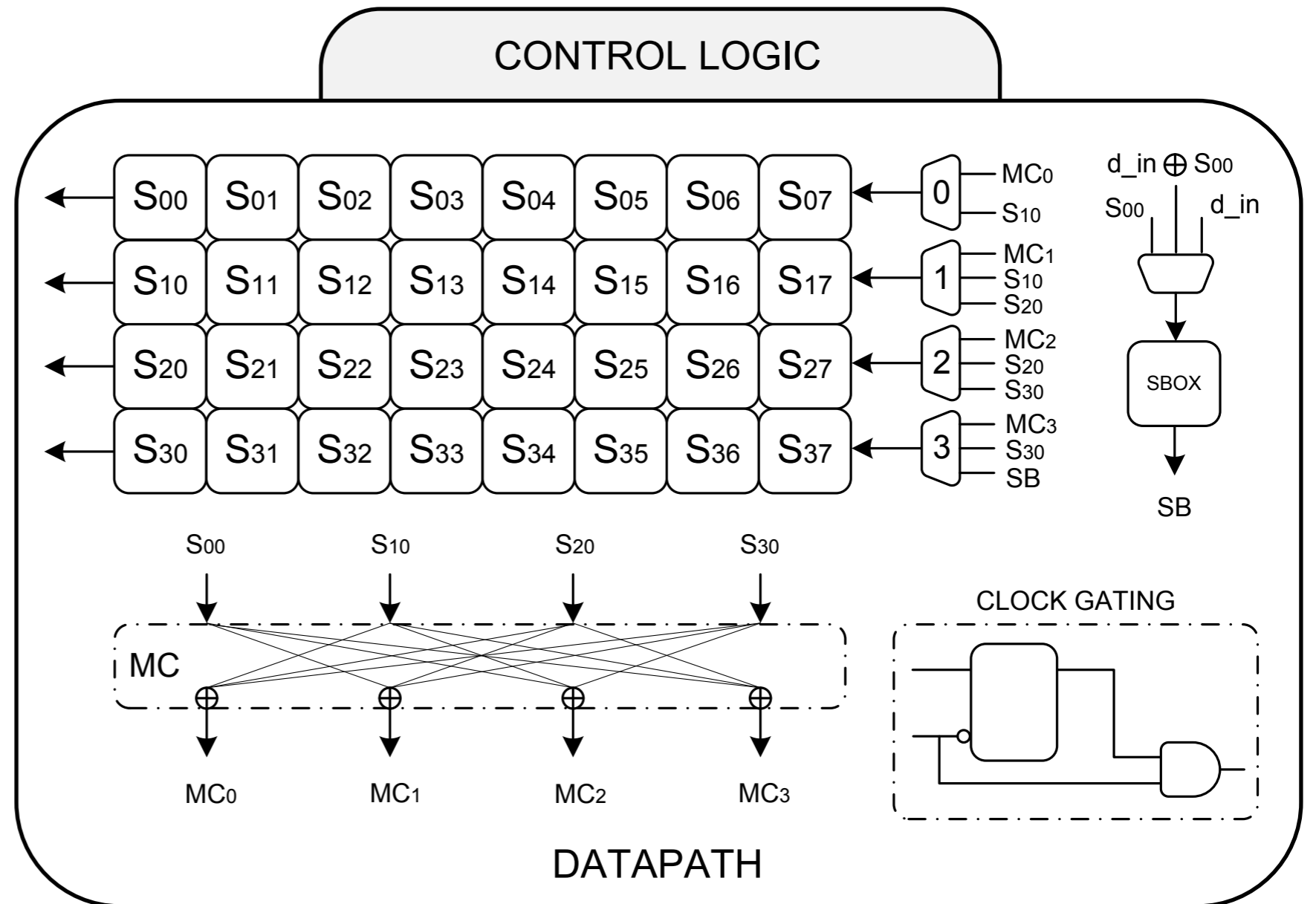
Implementation

- FIDES-S
- FIDES-4S
- FIDES-R
- FIDES-T



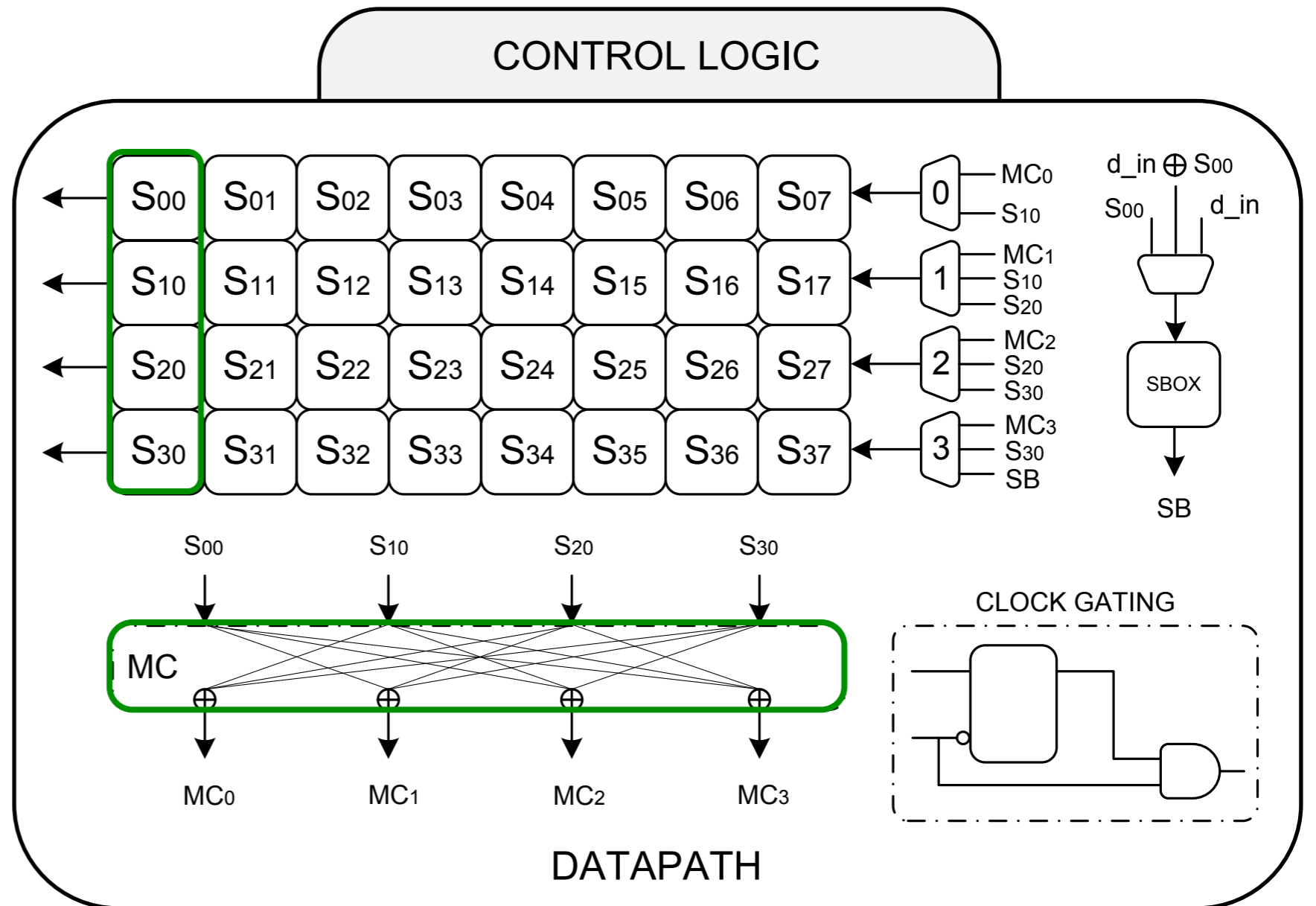
Implementation

- FIDES-S
- FIDES-4S
- FIDES-R
- FIDES-T



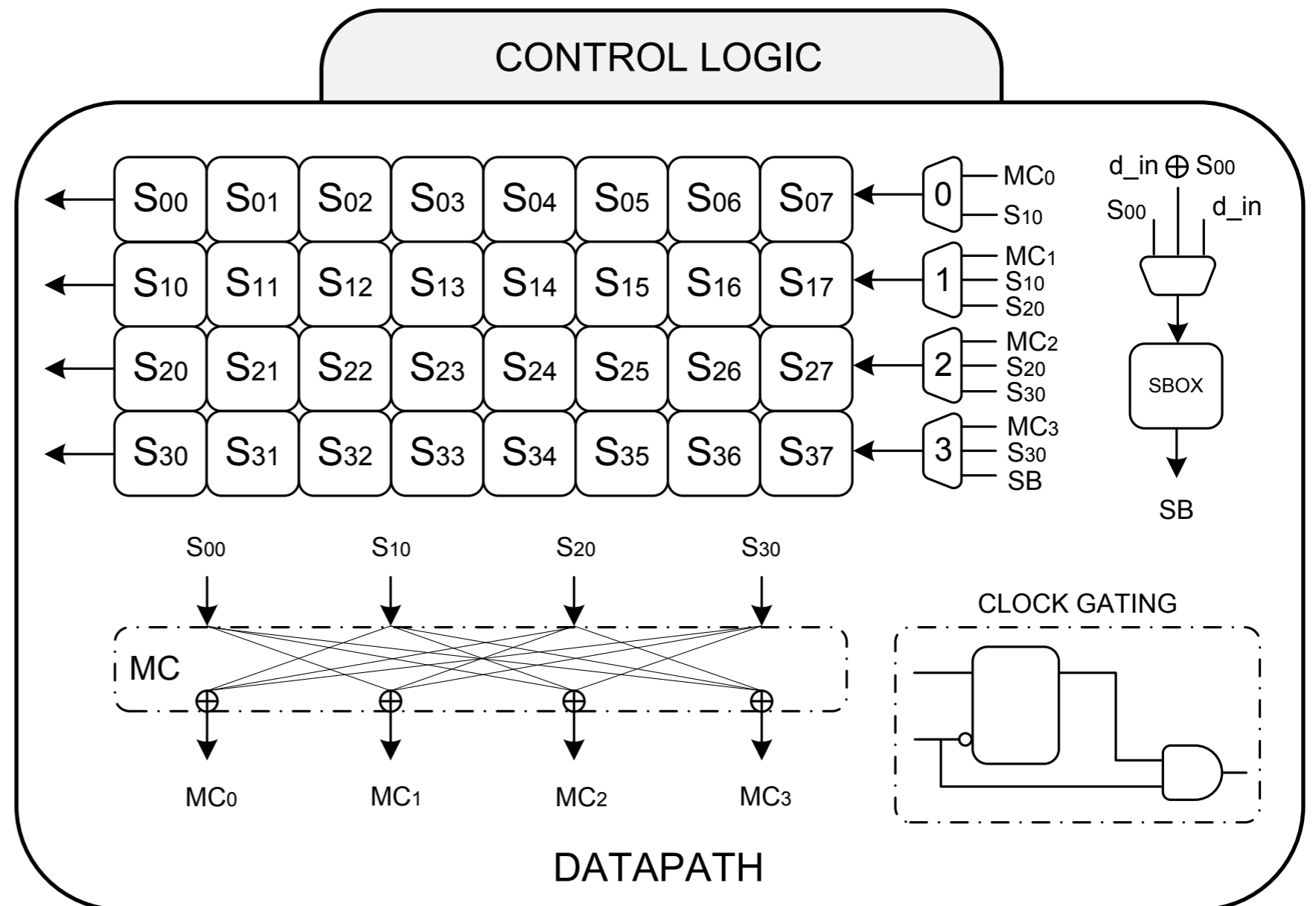
Implementation

- FIDES-S
- FIDES-4S
- FIDES-R
- FIDES-T



Implementation

- FIDES-S
- FIDES-4S
- FIDES-R
- FIDES-T

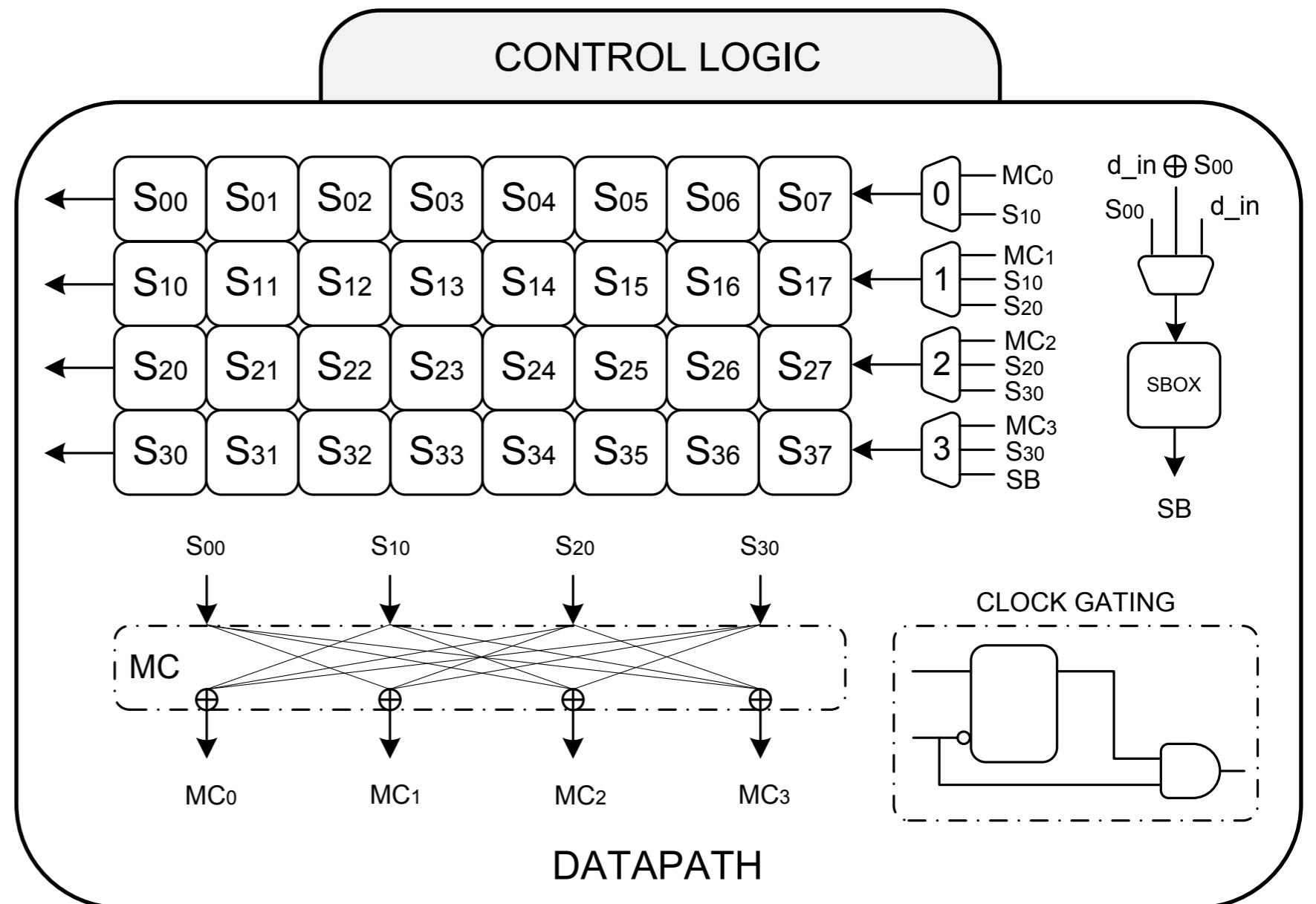


Implementation

- FIDES-S
- FIDES-4S
- FIDES-R
- FIDES-T

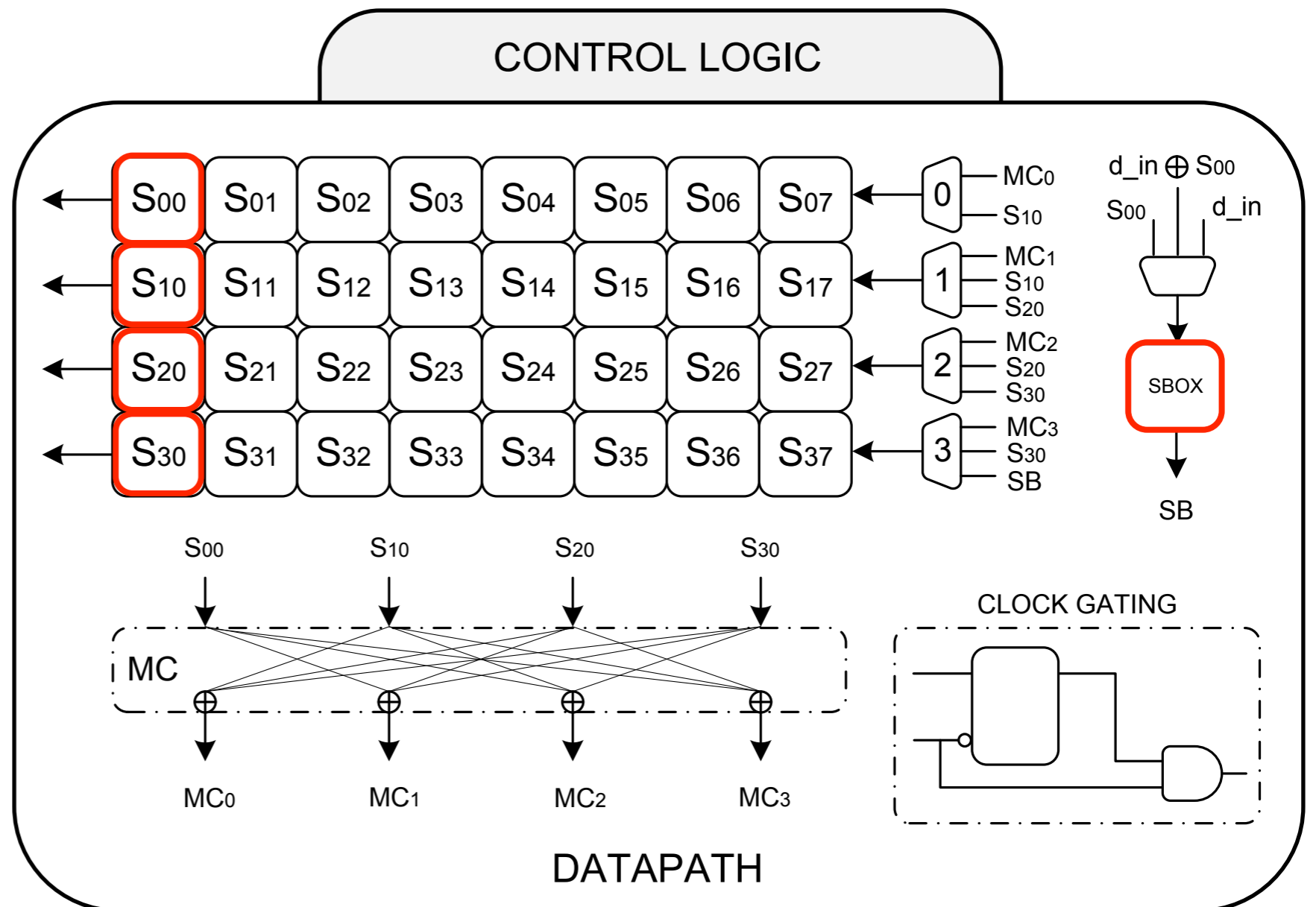
Implementation

- FIDES-S
- FIDES-4S
- FIDES-R
- FIDES-T



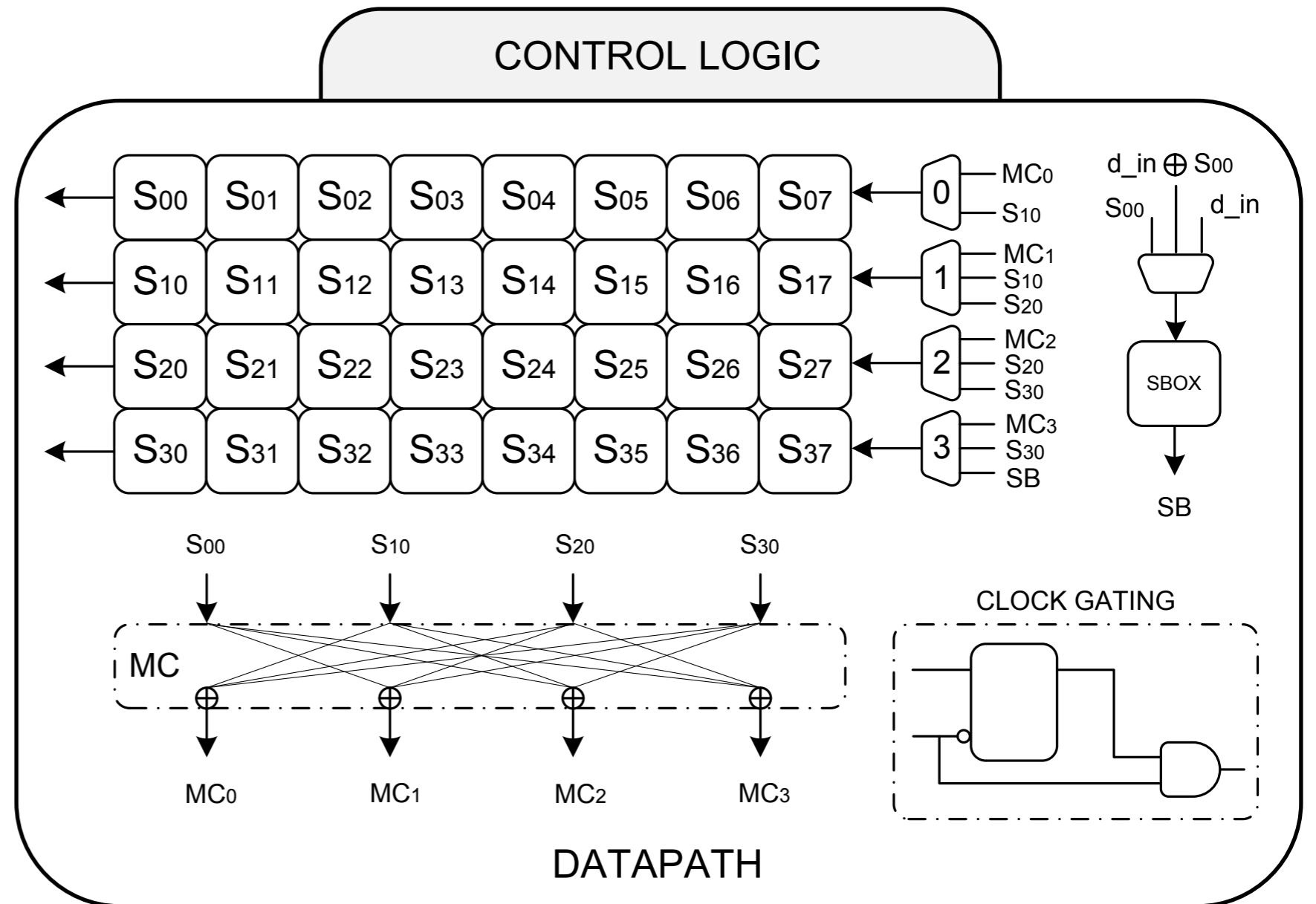
Implementation

- FIDES-S
- FIDES-4S
- FIDES-R
- FIDES-T



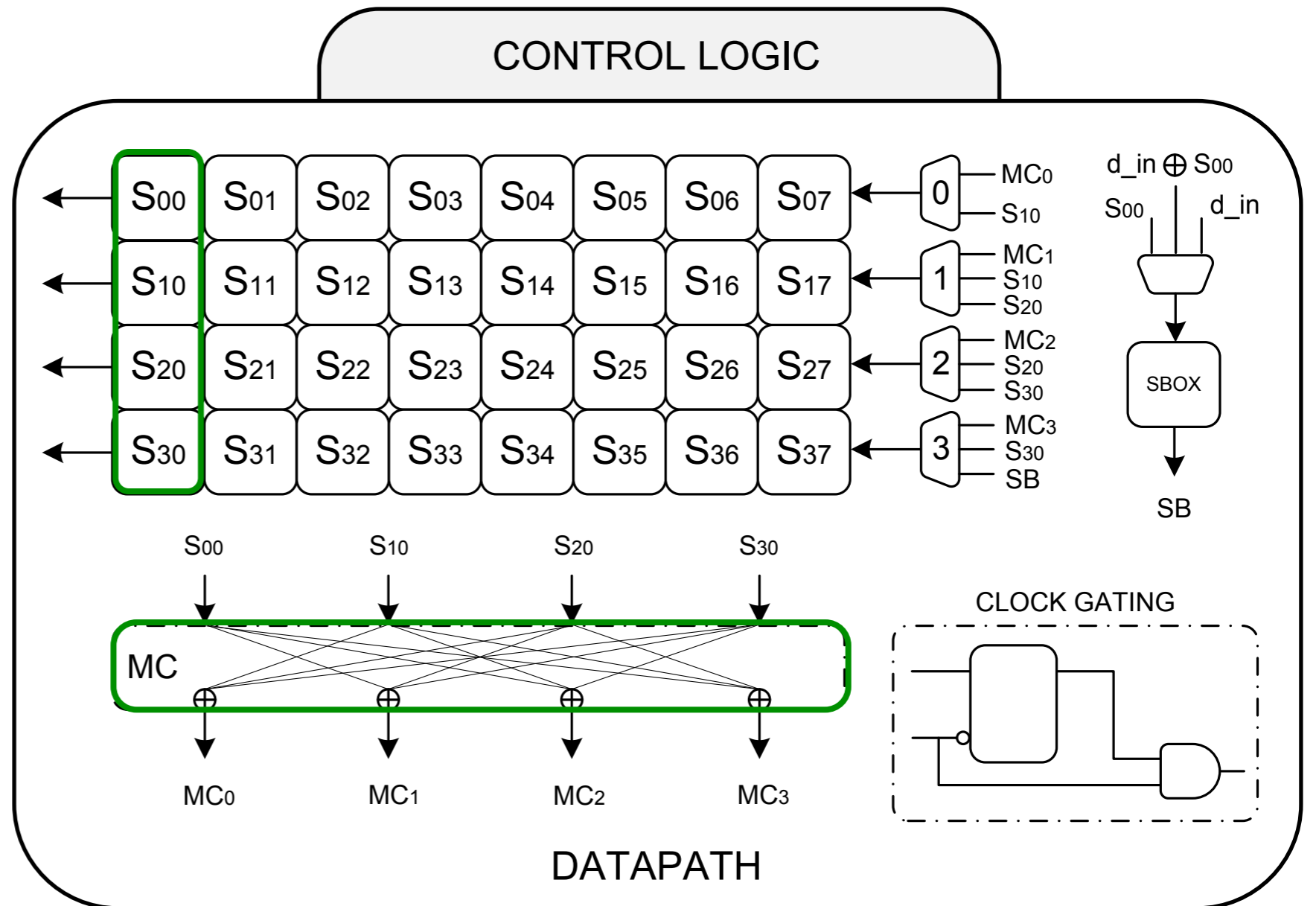
Implementation

- FIDES-S
- FIDES-4S
- FIDES-R
- FIDES-T



Implementation

- FIDES-S
- FIDES-4S
- FIDES-R
- FIDES-T

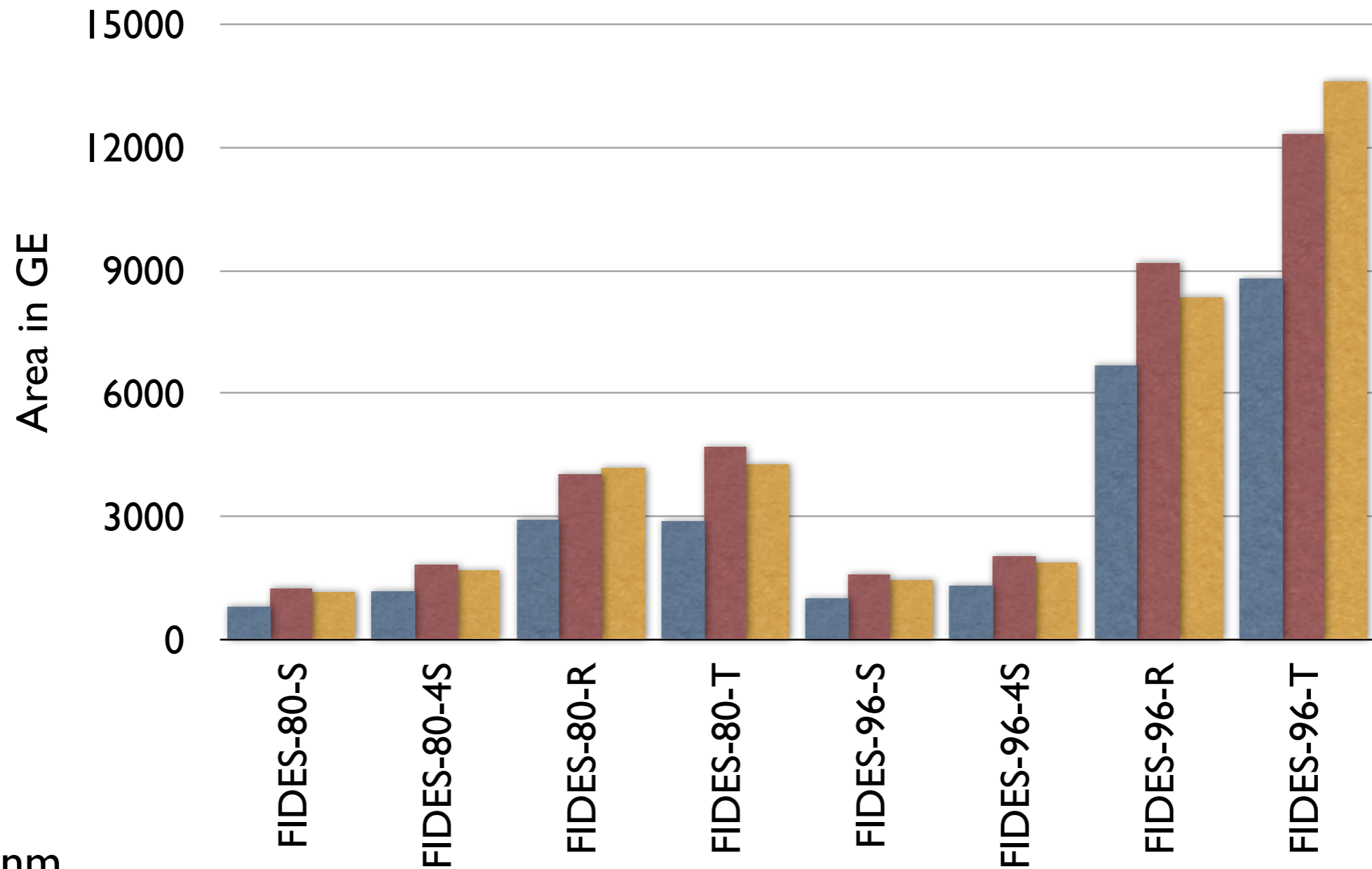


Implementation

- FIDES-S
- FIDES-4S
- FIDES-R
- FIDES-T

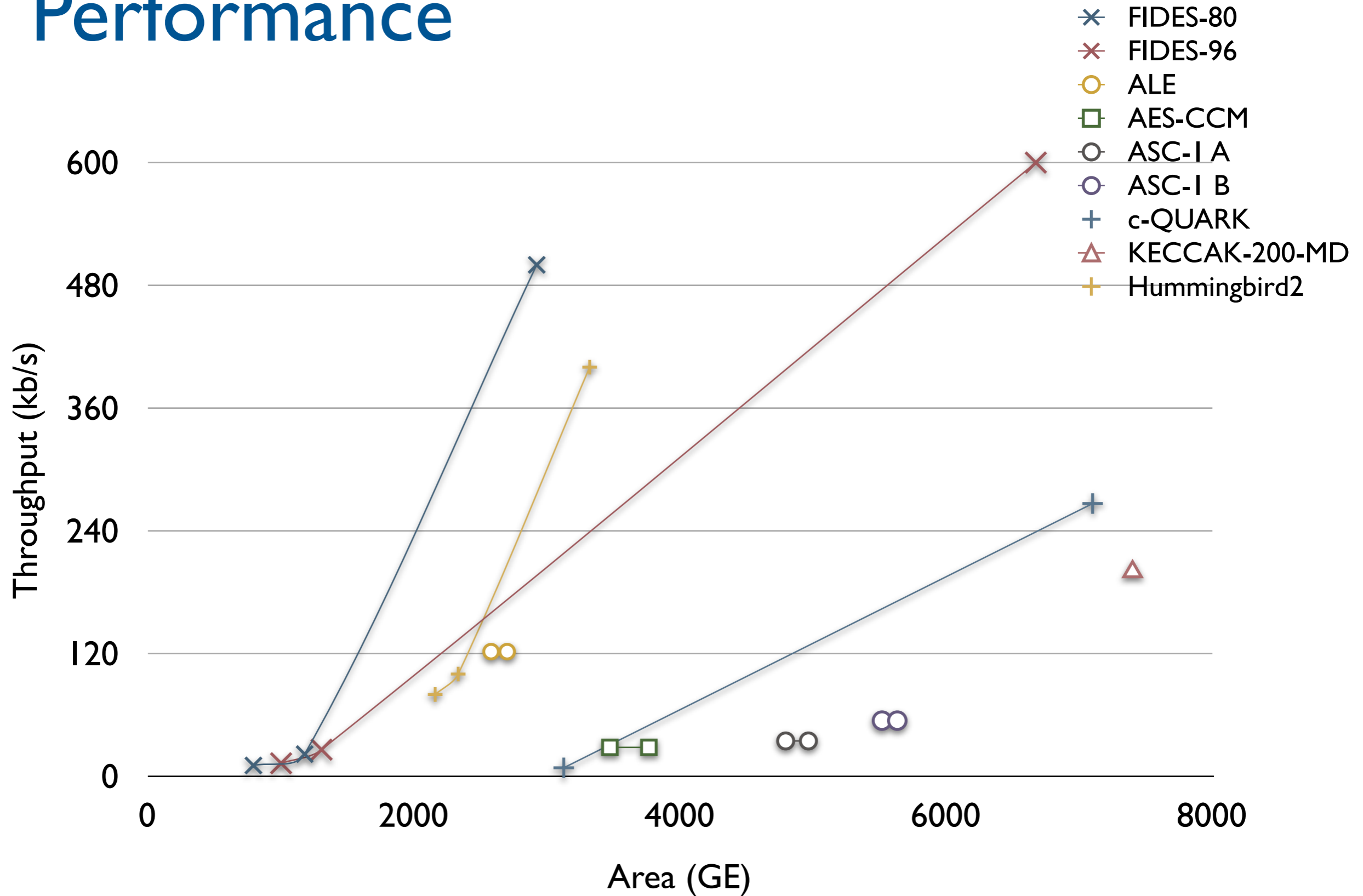
Performance

FIDES on Different Technologies



- NXP 90nm
- NANGATE 45nm
- UMC 130nm

Performance



Conclusion



FIDES

Conclusion



FIDES

- Lightweight AE
 - less than 1500GE
 - online, single-pass

Conclusion



FIDES

- Lightweight AE
 - less than 1500GE
 - online, single-pass
- with Side Channel Resistance
 - TI less than 5000 GE

Conclusion



FIDES

- Lightweight AE
 - less than 1500GE
 - online, single-pass
- with Side Channel Resistance
 - TI less than 5000 GE
- and 80-bit or 90-bit security
 - AB and APN permutations
 - almost MDS

THANK YOU!

