COSIC

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

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

KU LEUVEN DTU NXP TU Graz

Outline

- Motivation
- Design
  - Structure
  - S-box
- Security Analysis
- Performance

Lightweight Design

Lightweight Design

Lightweight Design

Lightweight Design

- Block Ciphers e.g. PRESENT, KATAN, LED, …

Lightweight Design

- Block Ciphers e.g. PRESENT, KATAN, LED, …
- Stream Ciphers e.g. GRAIN, TRIVIUM, …

Lightweight Design

- Block Ciphers e.g. PRESENT, KATAN, LED, …
- Stream Ciphers e.g. GRAIN, TRIVIUM, …
- Hash Functions e.g. Spongent, Quark, ...

Lightweight Design

- Block Ciphers e.g. PRESENT, KATAN, LED, …
- Stream Ciphers e.g. GRAIN, TRIVIUM, …
- Hash Functions e.g. Spongent, Quark, ...

Confidentiality OR Authenticity

Lightweight Design

Confidentiality OR Authenticity

Lightweight AE

Confidentiality AND Authenticity

Lightweight AE

Confidentiality AND Authenticity

- OCB mode [Rogaway'01]
- Encrypt/MAC (EtM, MtE)

Lightweight AE

Confidentiality AND Authenticity

- OCB mode [Rogaway'01]
- Encrypt/MAC (EaM, MtE)

Additional operations and memory states

Lightweight AE

Confidentiality AND Authenticity

- OCB mode [Rogaway'01]
- Encrypt/MAC (EtM, MtE)

Additional operations and memory states

Dedicated lightweight designs

Lightweight AE

Confidentiality AND Authenticity

- OCB mode [Rogaway'01]
- Encrypt/MAC (EaM, MtE)

Additional operations and memory states

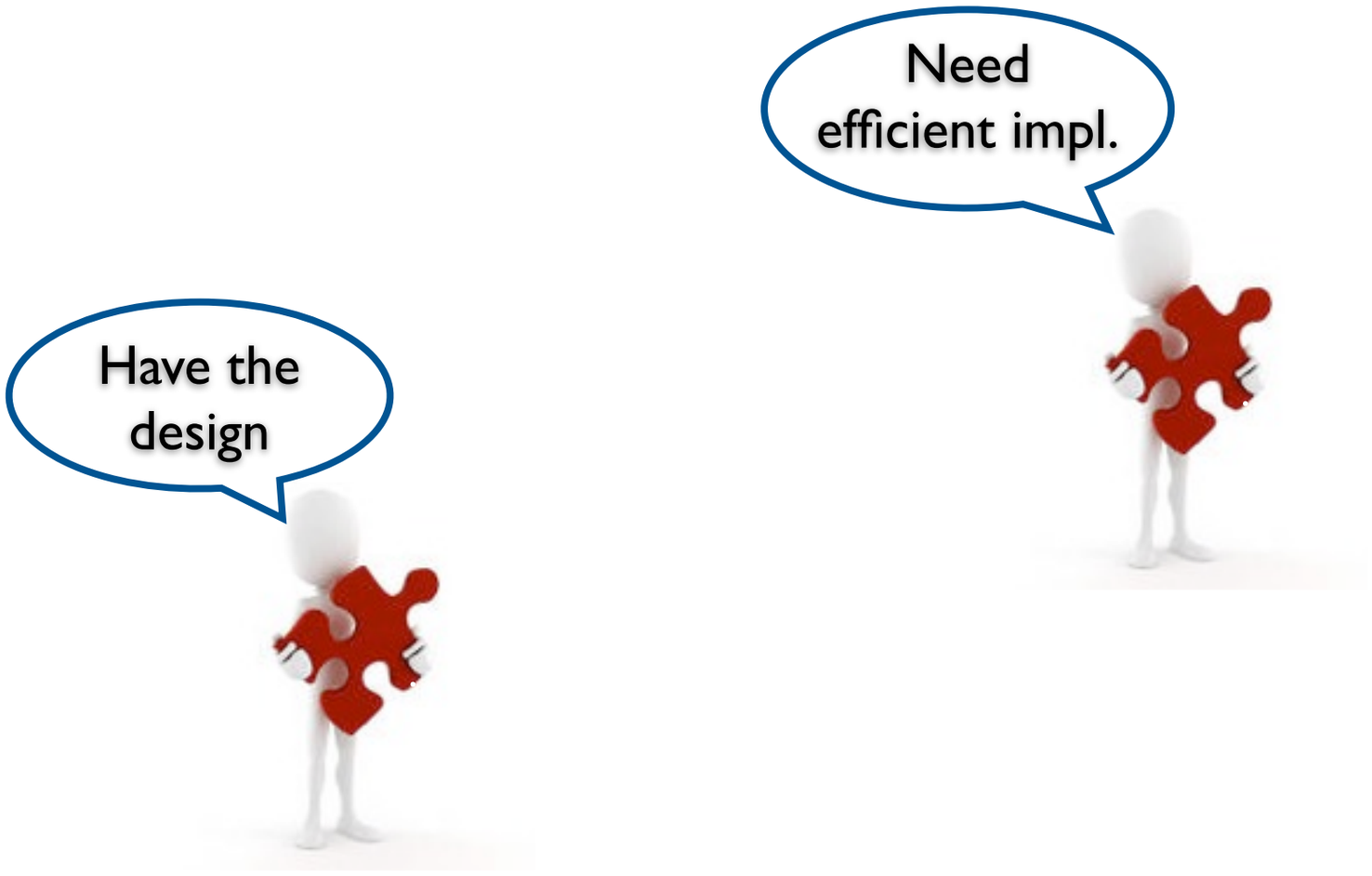
Dedicated lightweight designs

ALE[Bogdanov'13], Hummingbird-2[Engels'11], Grain-128a[Agren'11]

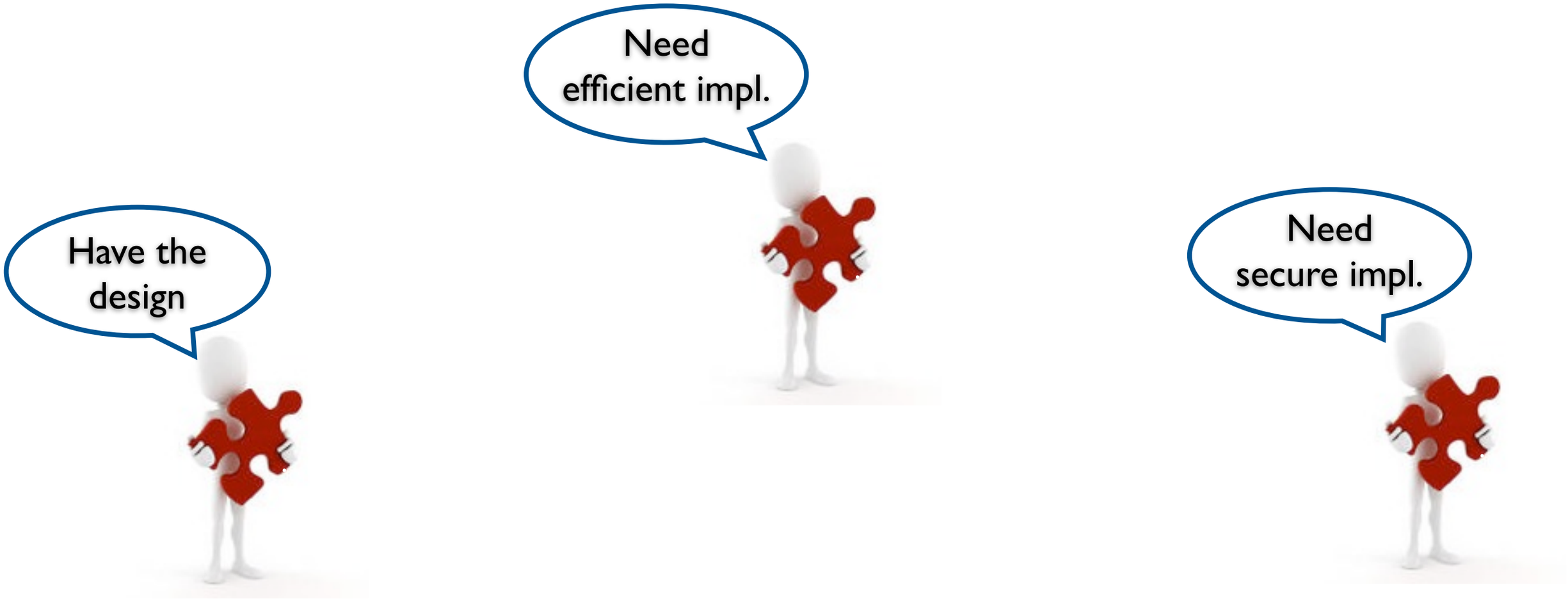
Side Channel Resistance

Side Channel Resistance

Side Channel Resistance



Side Channel Resistance



Side Channel Resistance

Need efficient impl.

Have the design

Need secure impl.

1st Order

Multipl. Mask

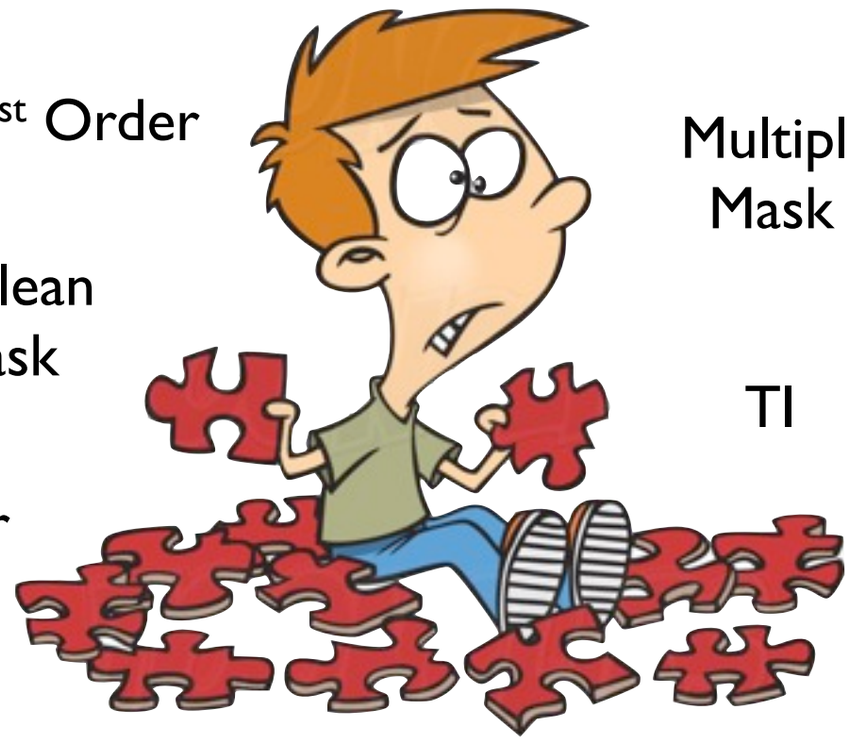
Boolean Mask

TI

2nd Order

SW

HW



?? Still efficient ??

Side Channel Resistance

Need efficient impl.

Have the design

Need secure impl.

1st Order

Multipl. Mask

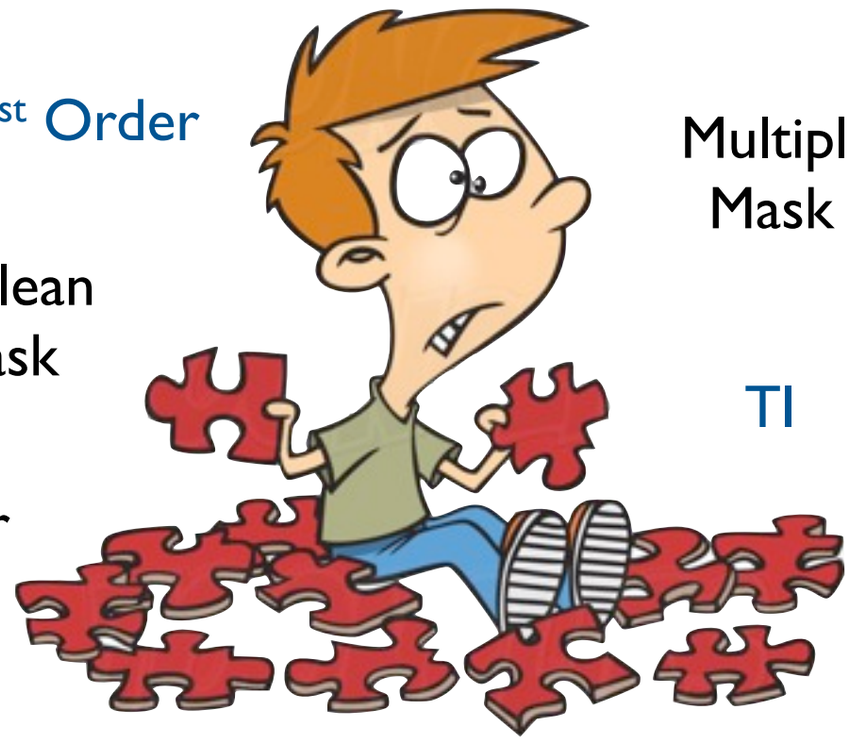
Boolean Mask

TI

2nd Order

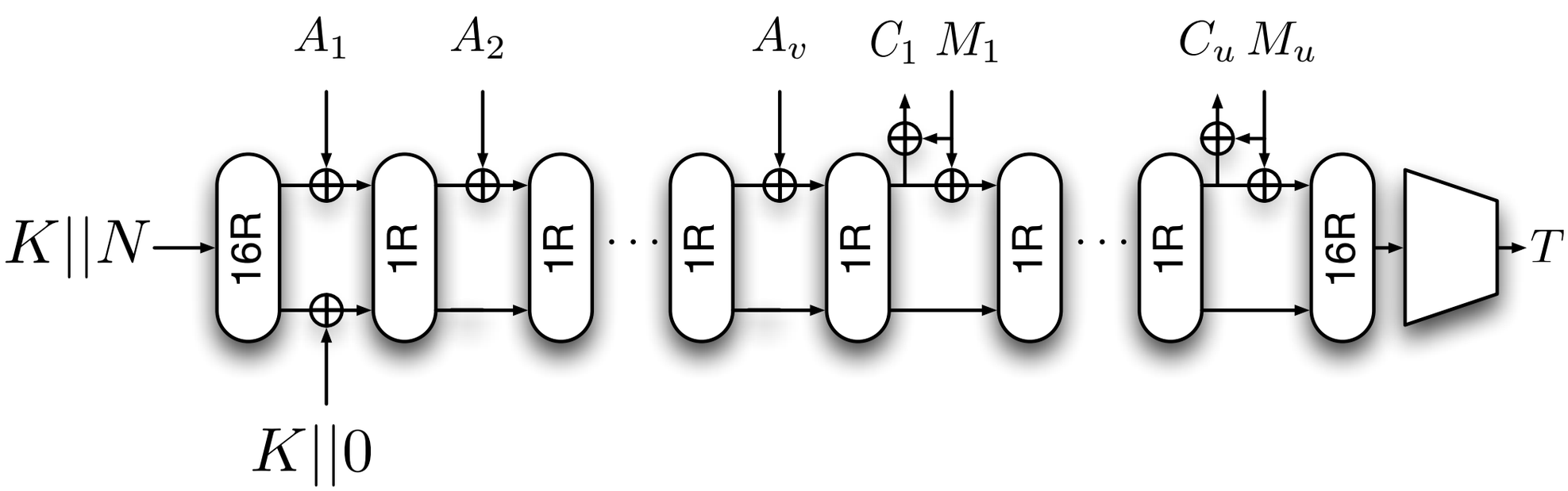
SW

HW

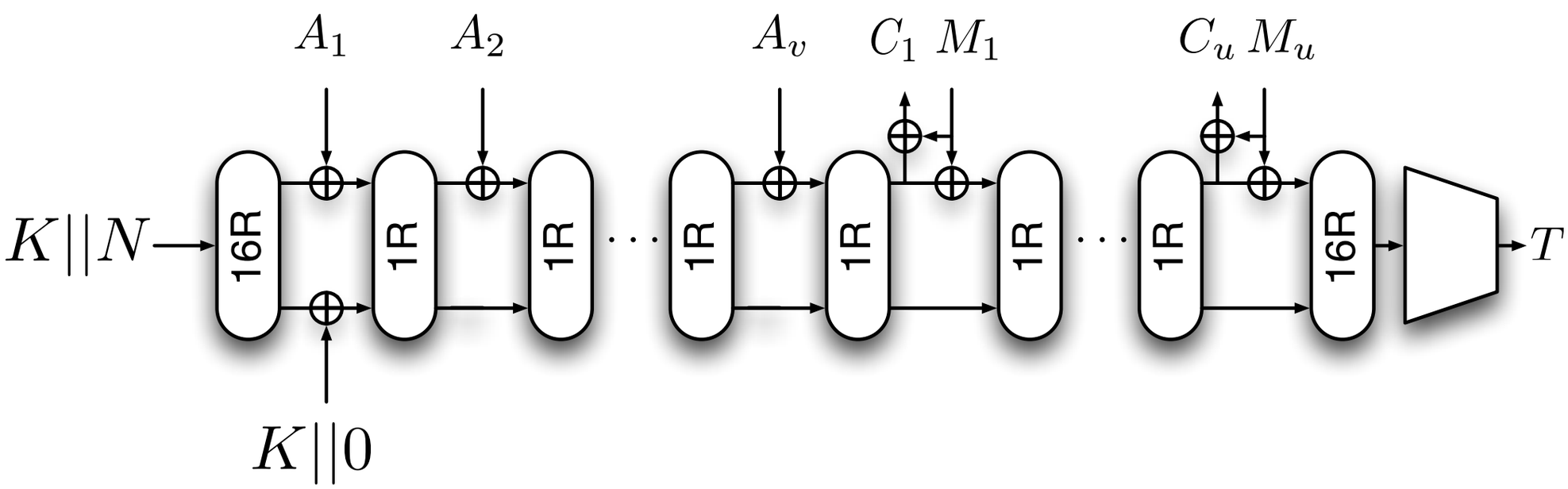


Still efficient

Design - Structure

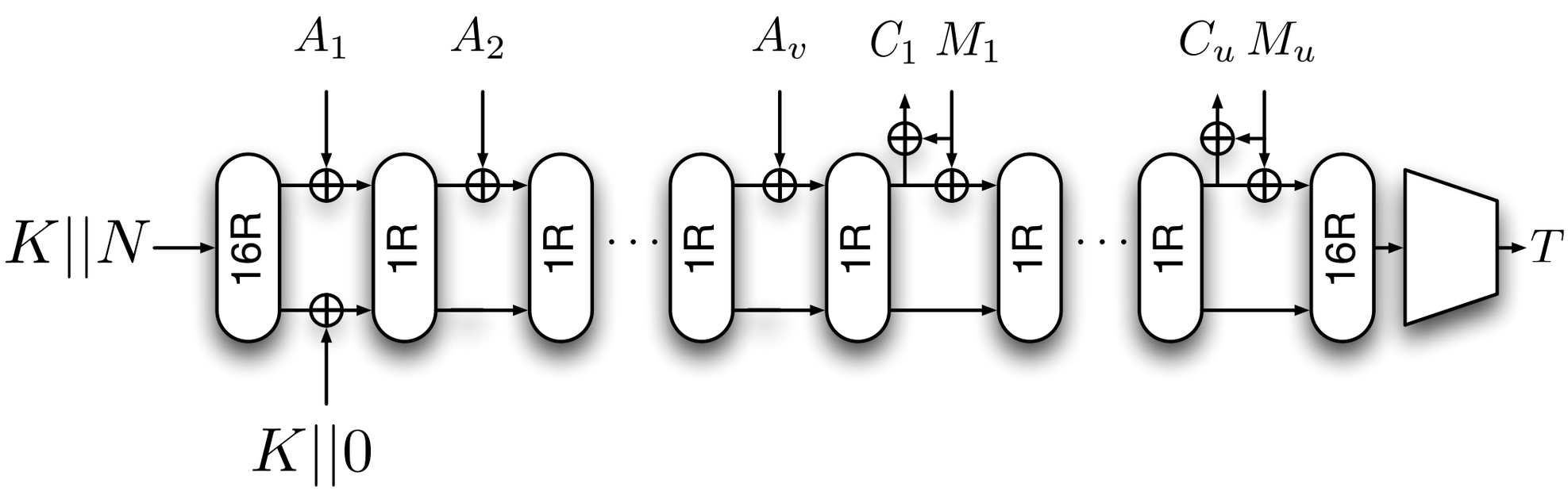


Design - Structure



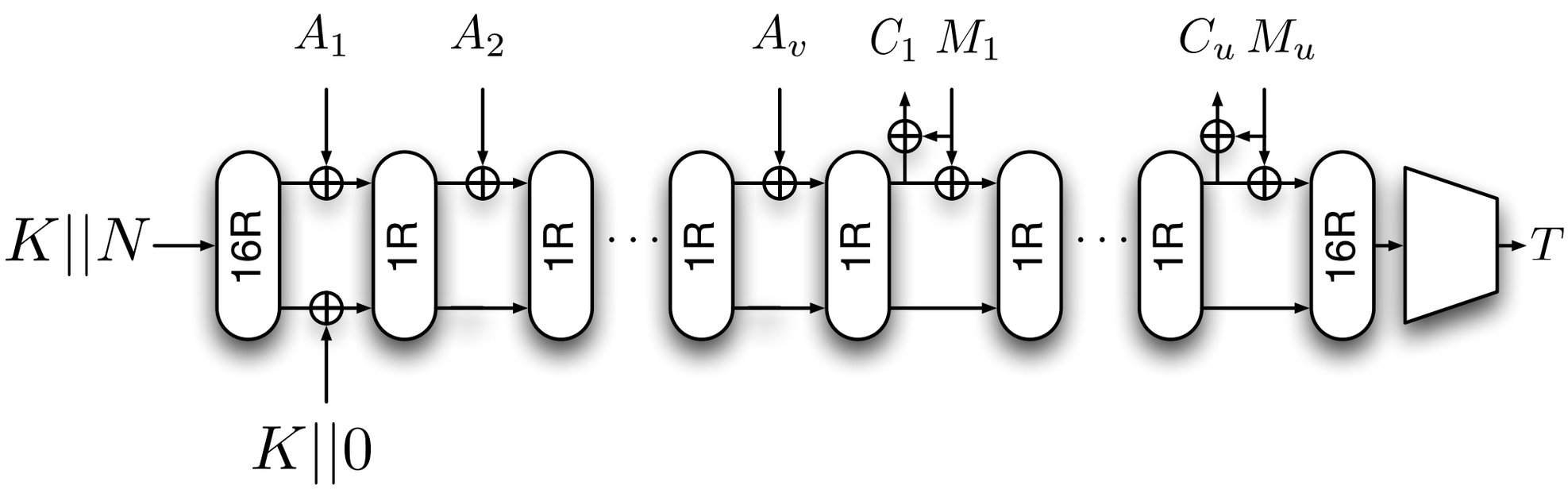
- Similar to duplex sponge

Design - Structure



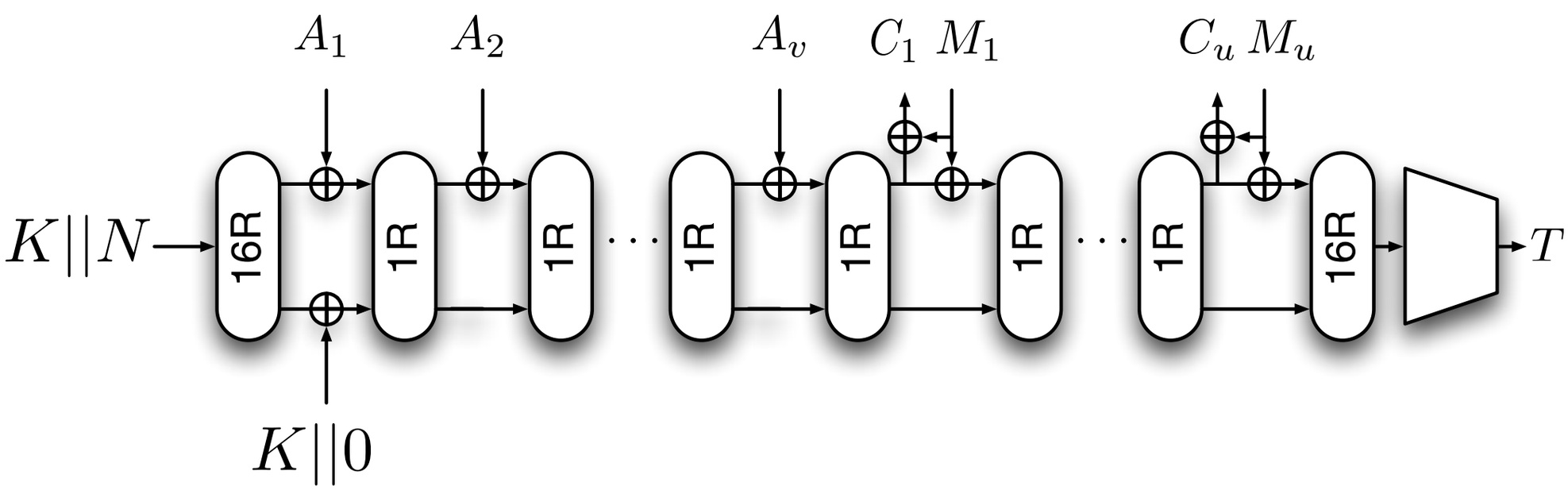
- Similar to duplex sponge
- Rounds are not keyed

Design - Structure



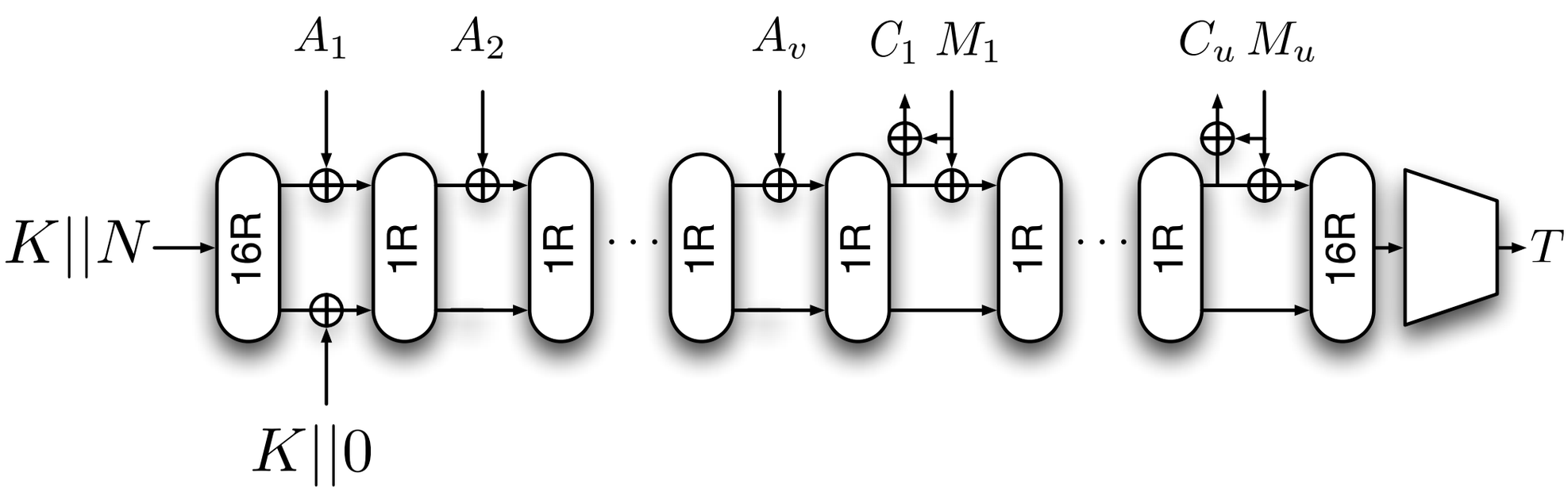
- Similar to duplex sponge
- Rounds are not keyed
- ✓ Online

Design - Structure



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

Design - Structure

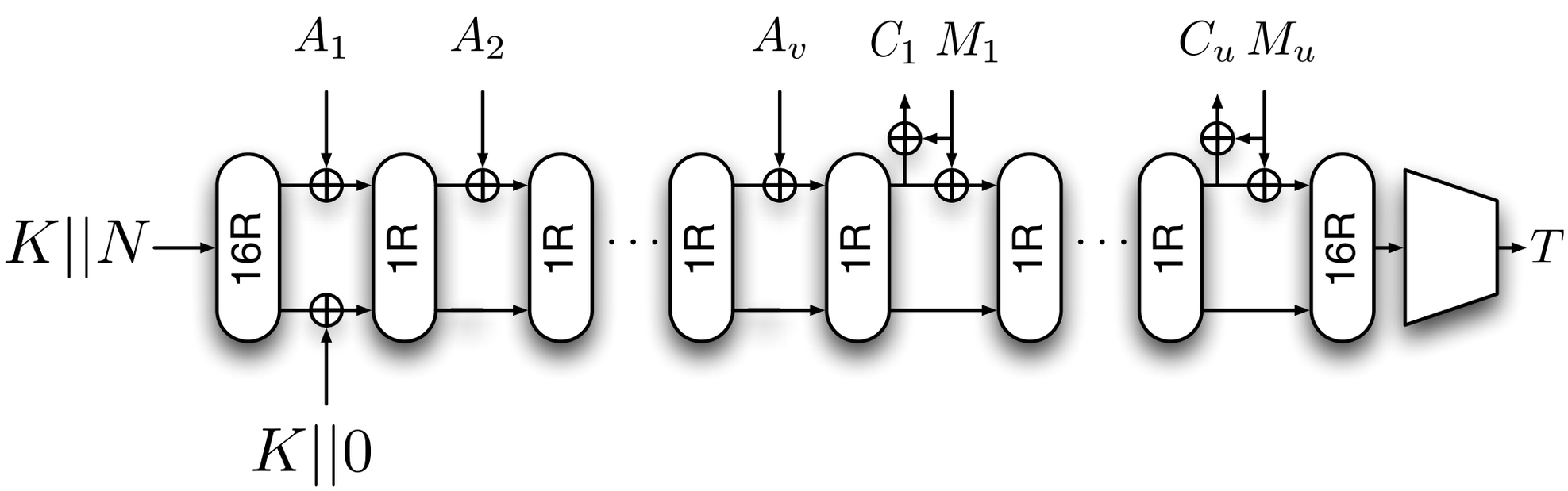


- Similar to duplex sponge
- Rounds are not keyed
- ✓ Online
- ✓ Single pass

FIDES-80

FIDES-96

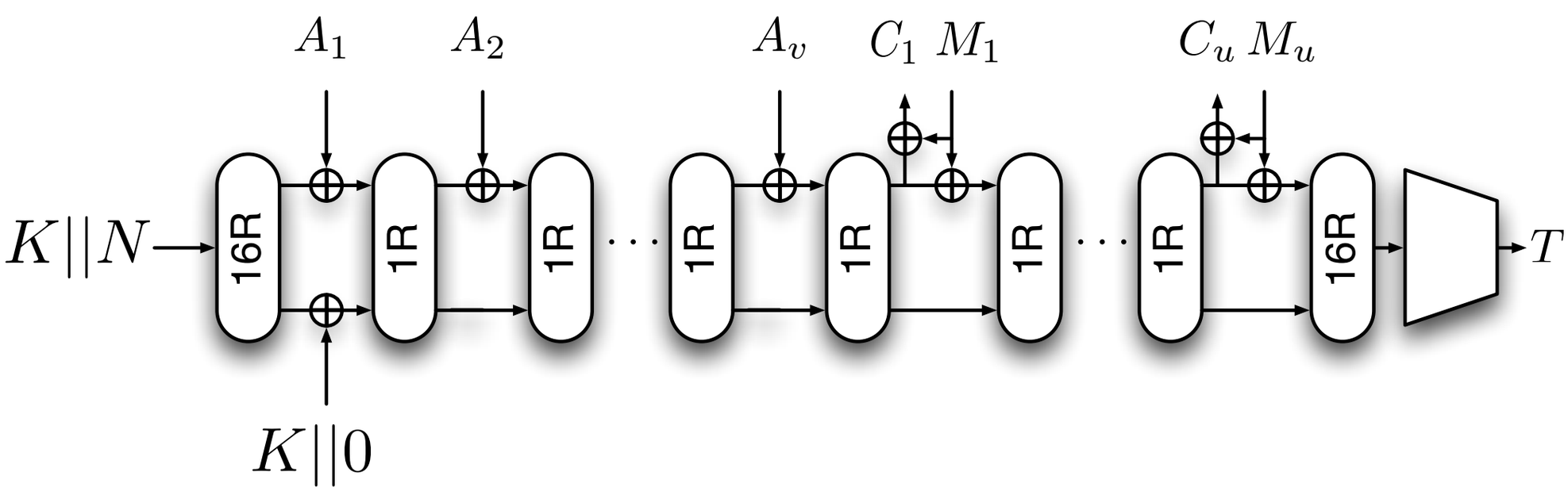
Design - Structure



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

	b
FIDES-80	160
FIDES-96	192

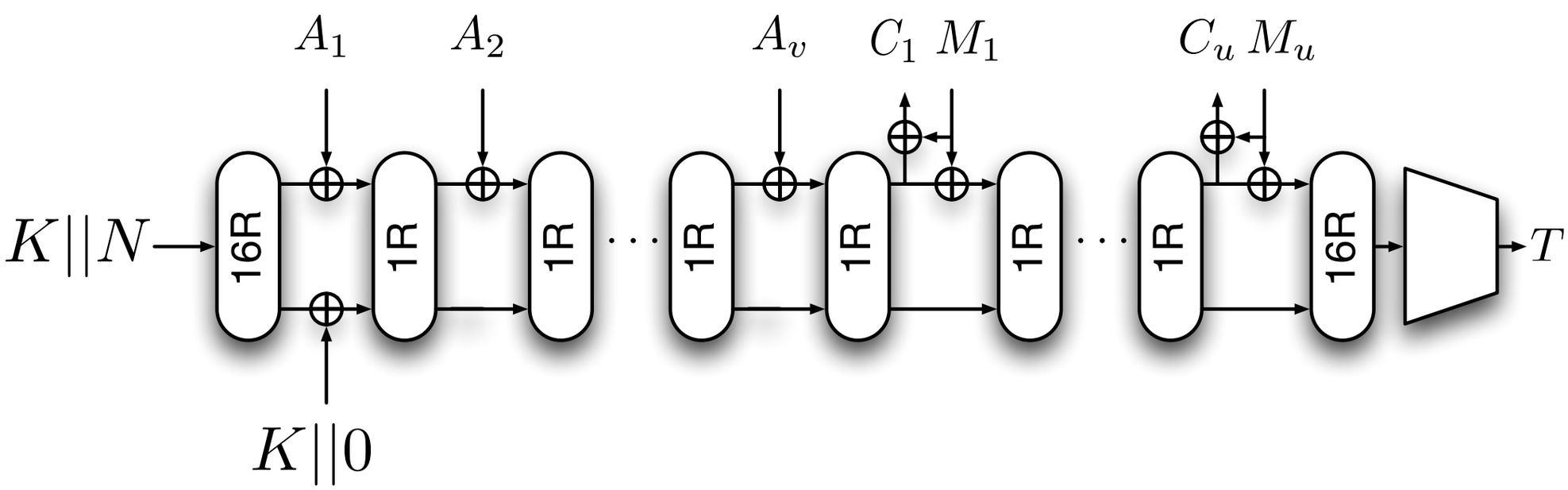
Design - Structure



- 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

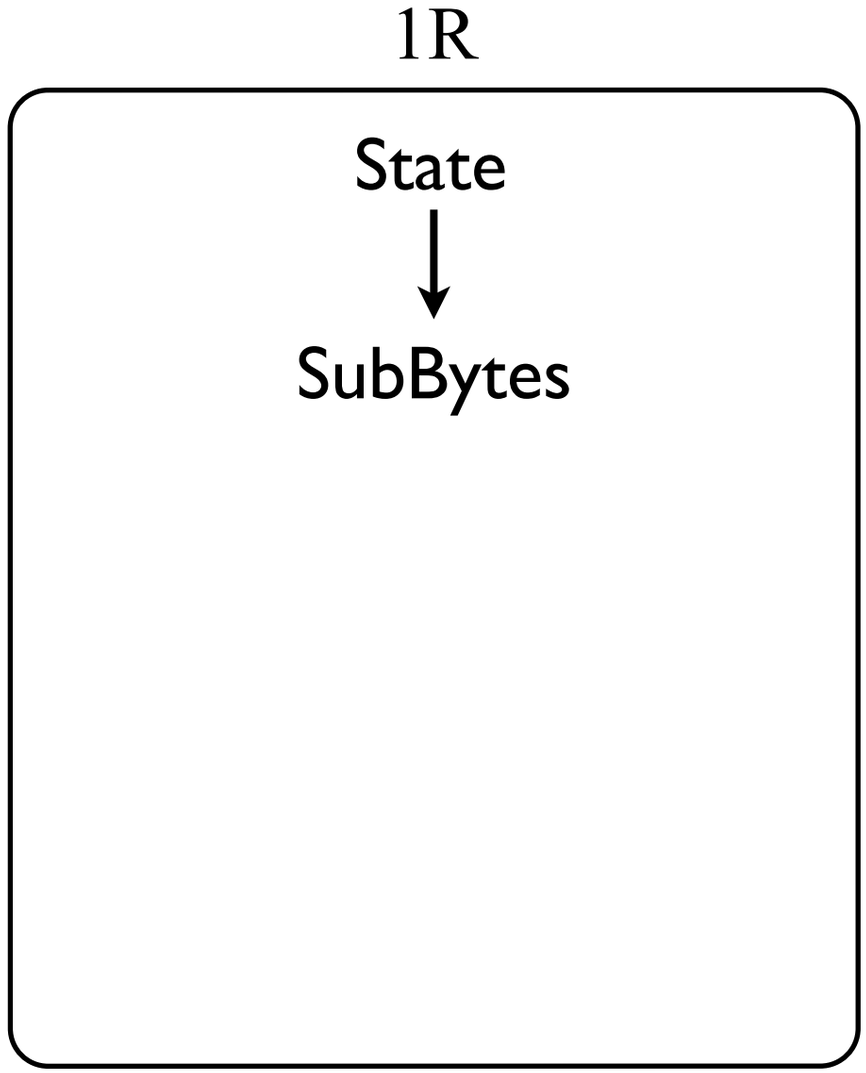
Design - Structure

1R

State

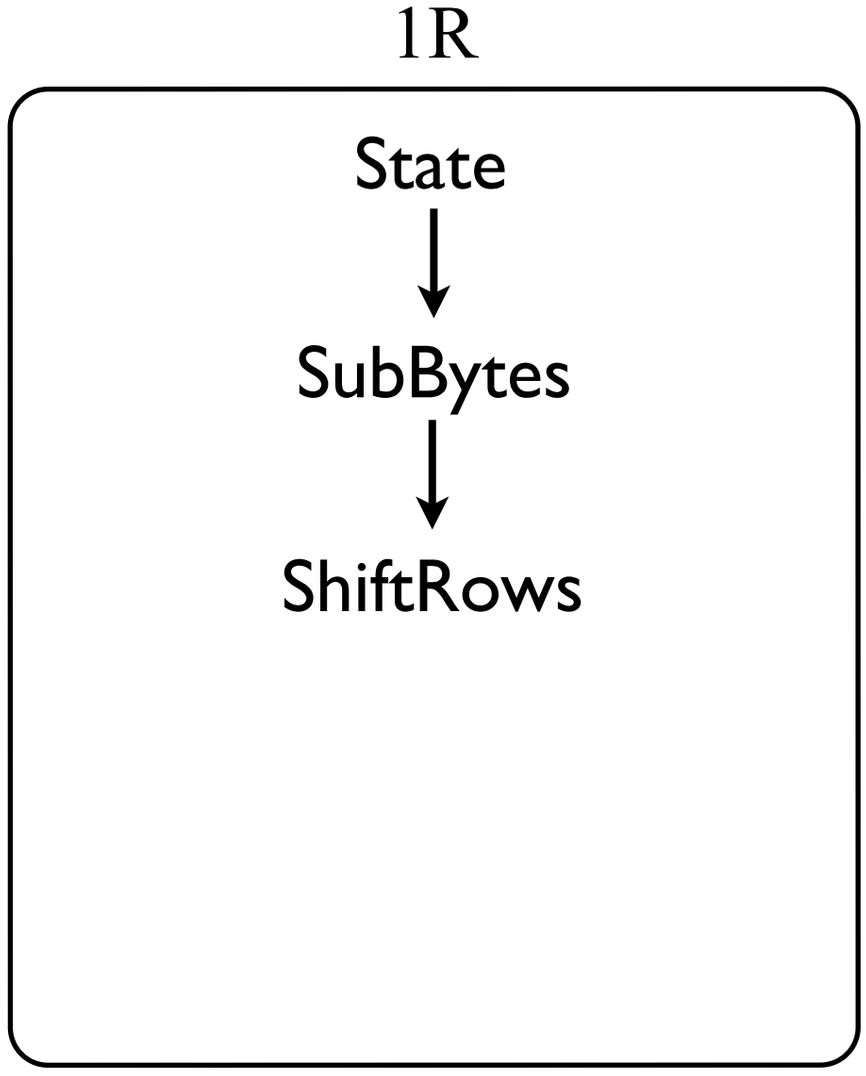
$a_{0,0}$	$a_{0,1}$	$a_{0,2}$	$a_{0,3}$	$a_{0,4}$	$a_{0,5}$	$a_{0,6}$	$a_{0,7}$
$a_{1,0}$	$a_{1,1}$	$a_{1,2}$	$a_{1,3}$	$a_{1,4}$	$a_{1,5}$	$a_{1,6}$	$a_{1,7}$
$a_{2,0}$	$a_{2,1}$	$a_{2,2}$	$a_{2,3}$	$a_{2,4}$	$a_{2,5}$	$a_{2,6}$	$a_{2,7}$
$a_{3,0}$	$a_{3,1}$	$a_{3,2}$	$a_{3,3}$	$a_{3,4}$	$a_{3,5}$	$a_{3,6}$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

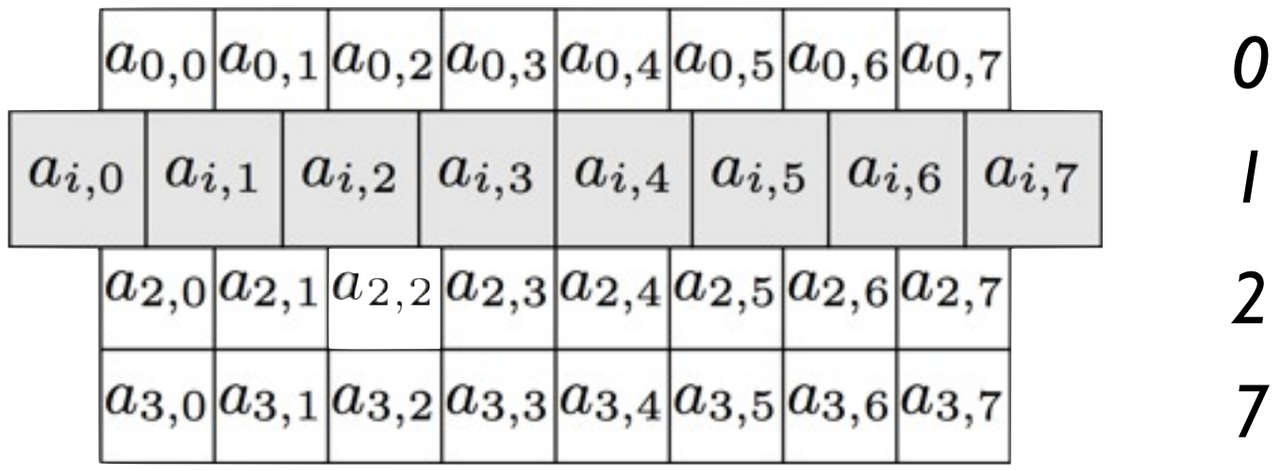
Design - Structure



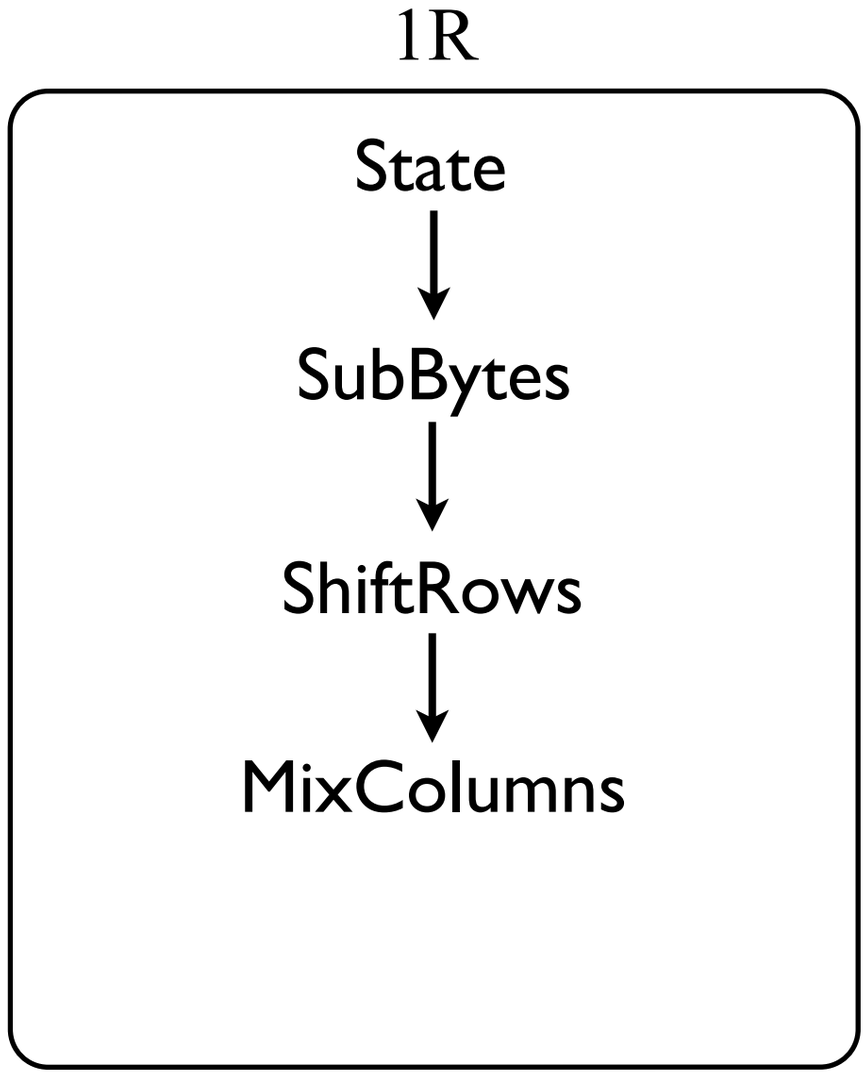
$a_{0,0}$	$a_{0,1}$	$a_{0,2}$	$a_{0,3}$	$a_{0,4}$	$a_{0,5}$	$a_{0,6}$	$a_{0,7}$
$a_{1,0}$	$a_{1,1}$	$a_{i,j}$	$a_{1,3}$	$a_{1,4}$	$a_{1,5}$	$a_{1,6}$	$a_{1,7}$
$a_{2,0}$	$a_{2,1}$	$a_{2,2}$	$a_{2,3}$	$a_{2,4}$	$a_{2,5}$	$a_{2,6}$	$a_{2,7}$
$a_{3,0}$	$a_{3,1}$	$a_{3,2}$	$a_{3,3}$	$a_{3,4}$	$a_{3,5}$	$a_{3,6}$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

Design - Structure





Design - Structure

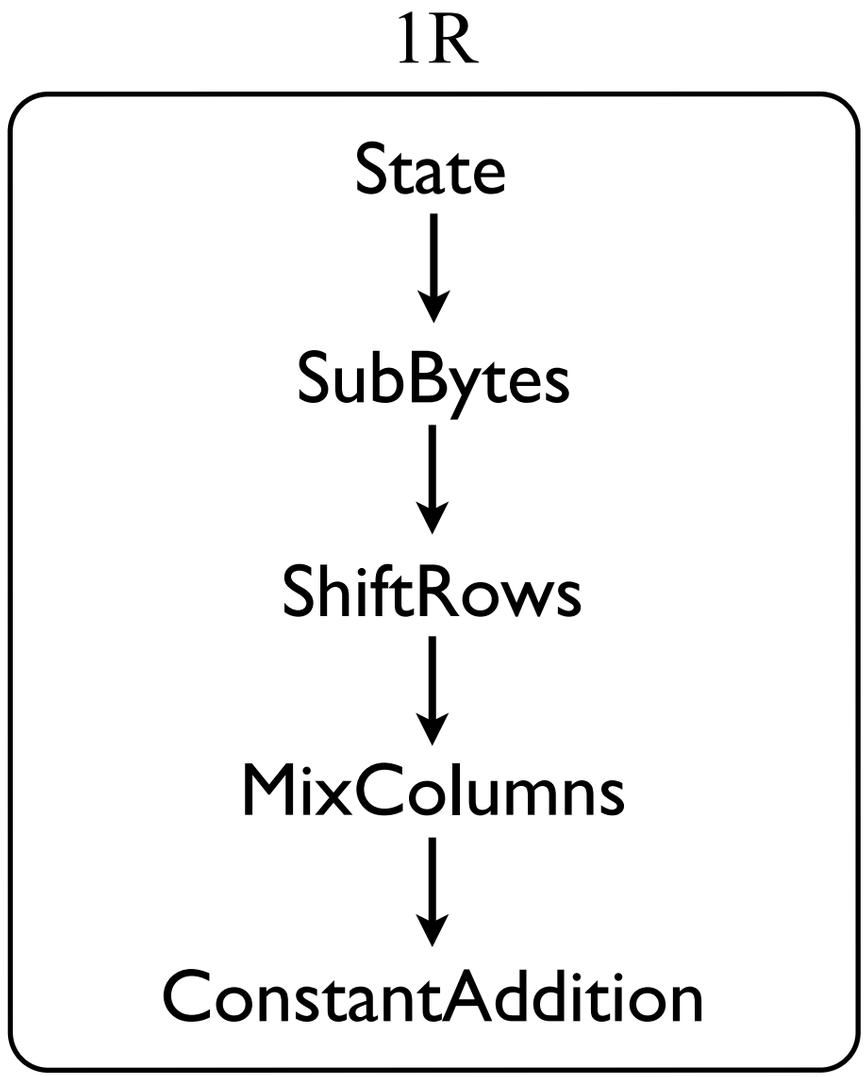


$$\begin{array}{|c|c|c|c|c|c|c|c|}
\hline
a_{0,0} & a_{0,1} & a_{0,j} & a_{0,3} & a_{0,4} & a_{0,5} & a_{0,6} & a_{0,7} \\
\hline
a_{1,0} & a_{1,1} & a_{1,j} & a_{1,3} & a_{1,4} & a_{1,5} & a_{1,6} & a_{1,7} \\
\hline
a_{2,0} & a_{2,1} & a_{2,j} & a_{2,3} & a_{2,4} & a_{2,5} & a_{2,6} & a_{2,7} \\
\hline
a_{3,0} & a_{3,1} & a_{3,j} & a_{3,3} & a_{3,4} & a_{3,5} & a_{3,6} & a_{3,7} \\
\hline
\end{array}$$

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

Almost MDS
branch number is 4

Design - Structure



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

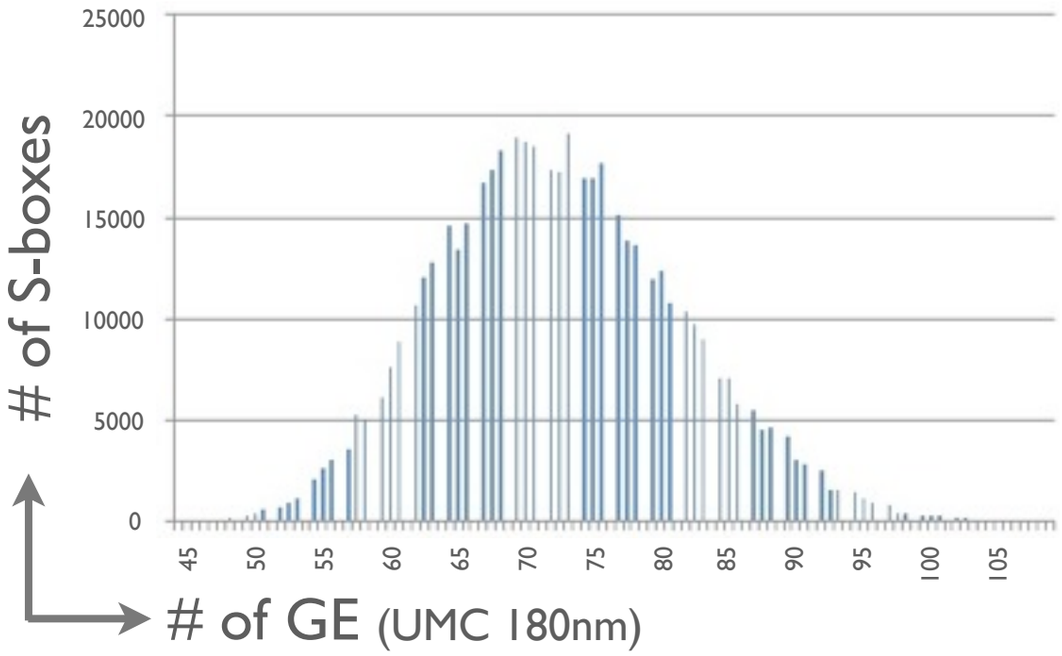
Design - S-boxes

Affine Equivalent to AB permutation

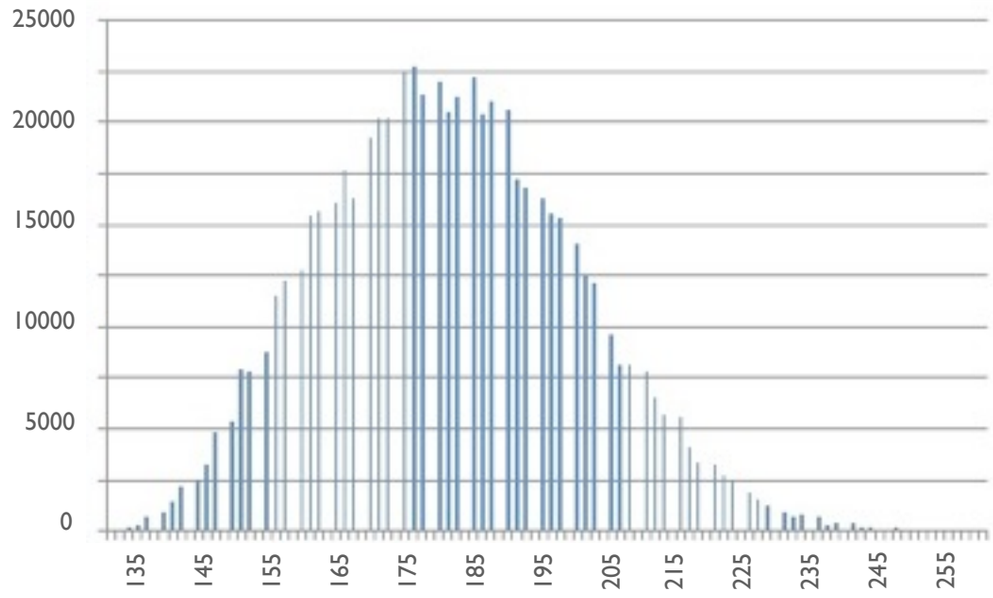
Design - S-boxes

Affine Equivalent to AB permutation

Unshared S-box



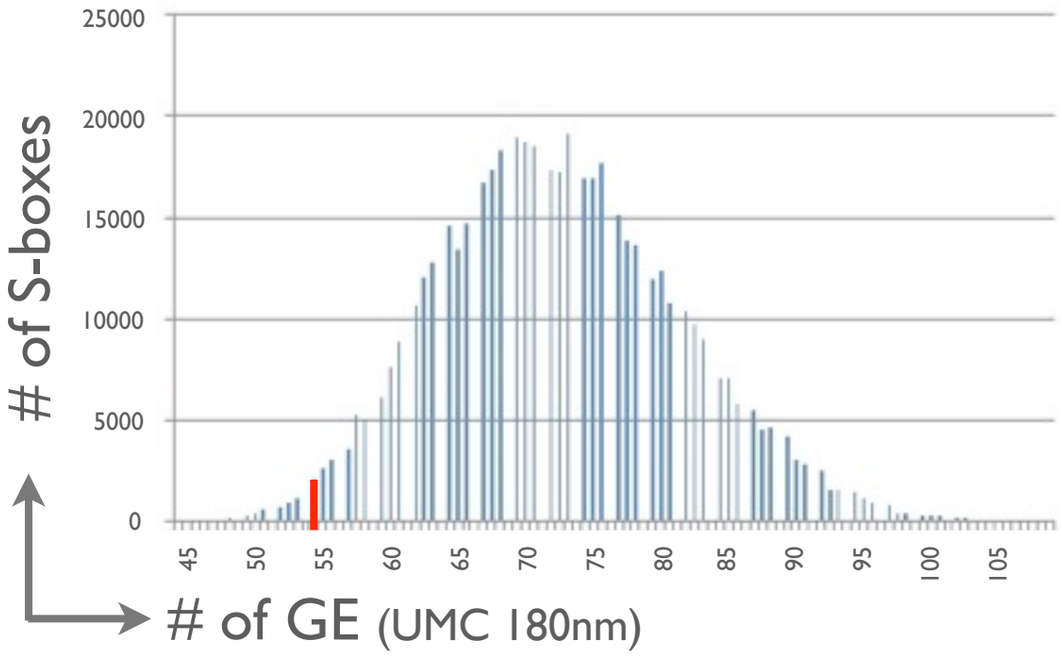
Shared S-box



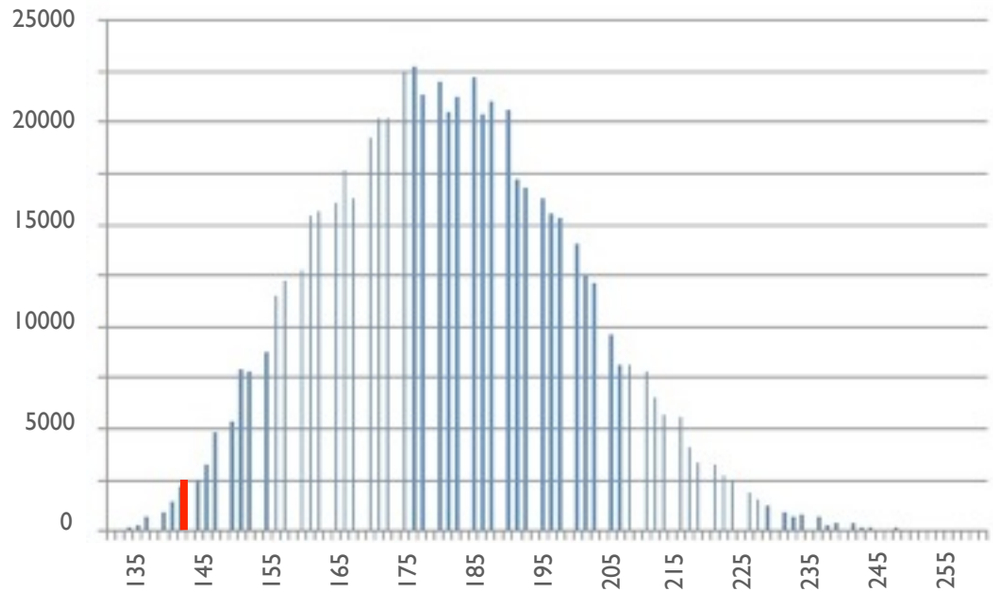
Design - S-boxes

Affine Equivalent to AB permutation

Unshared S-box



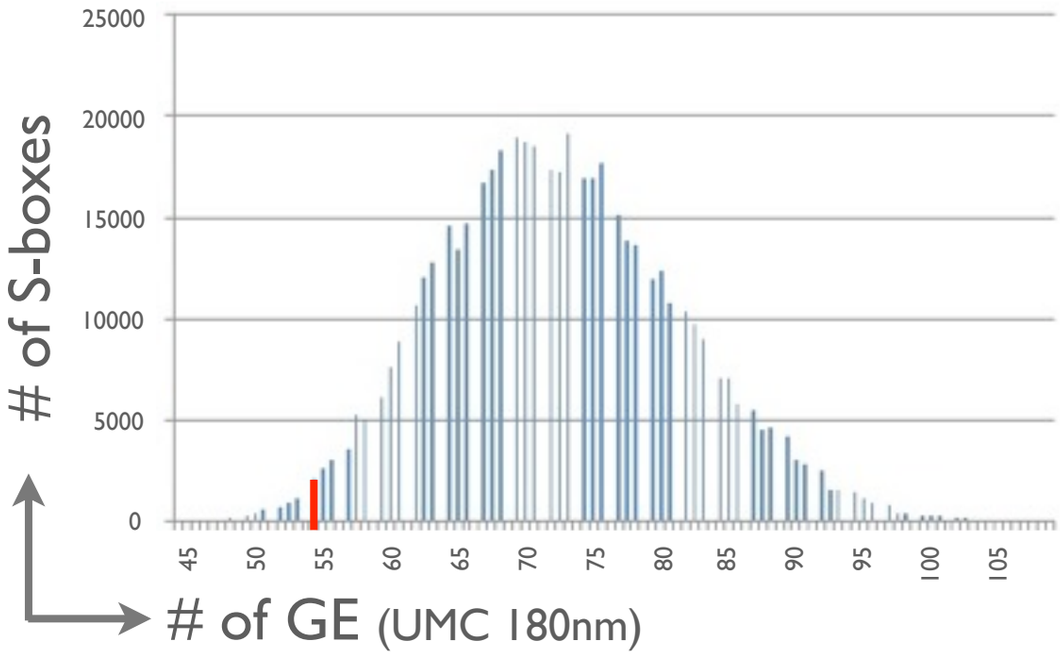
Shared S-box



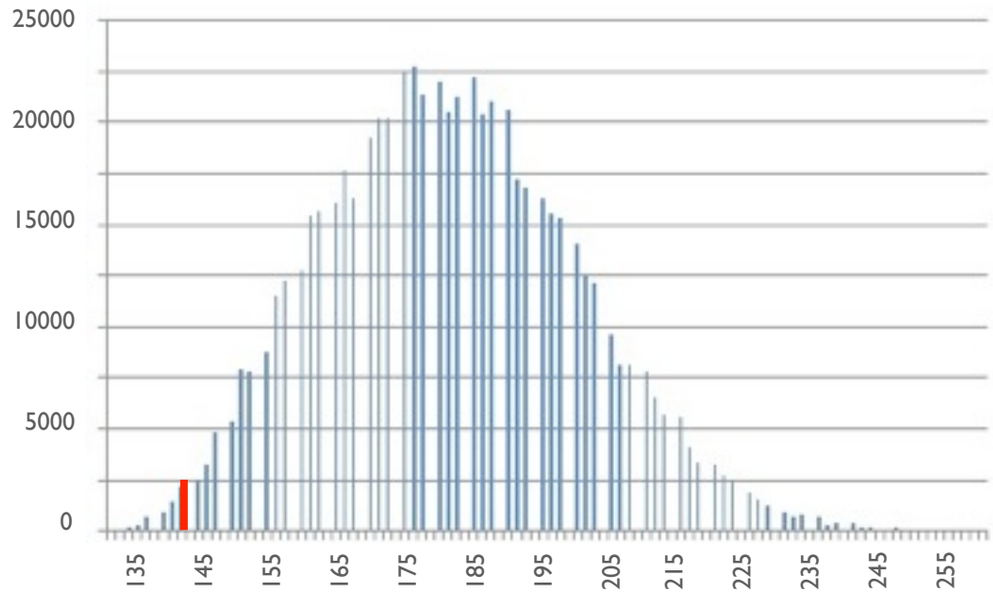
Design - S-boxes

Affine Equivalent to AB permutation

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: $2^{-4x48x2} = 2^{-384}$

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: $2^{-4x48x2} = 2^{-384}$
- 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: $2^{-4x48x2} = 2^{-384}$
- Collision Trails
  16 rounds: $2^{-4x(48+48)} = 2^{-384}$

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: $2^{-4x48x2} = 2^{-384}$
- Collision Trails
  16 rounds: $2^{-4x(48+48)} = 2^{-384}$
- 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: $2^{-4x48x2} = 2^{-384}$
- Collision Trails
  16 rounds: $2^{-4x(48+48)} = 2^{-384}$
- Impossible Differential
  9 rounds

Implementation

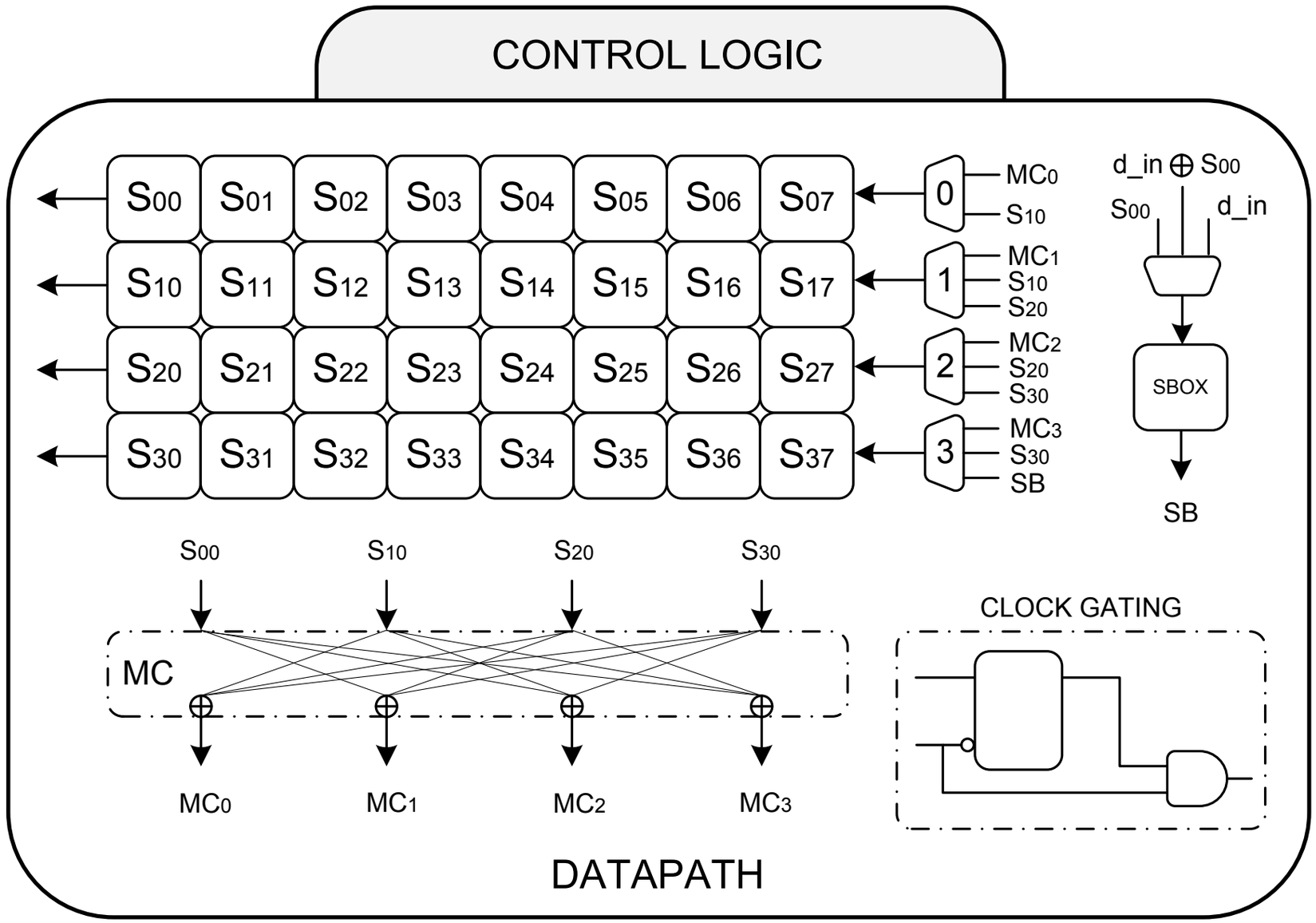
- FIDES-S
- FIDES-4S
- FIDES-R
- FIDES-T

Implementation

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

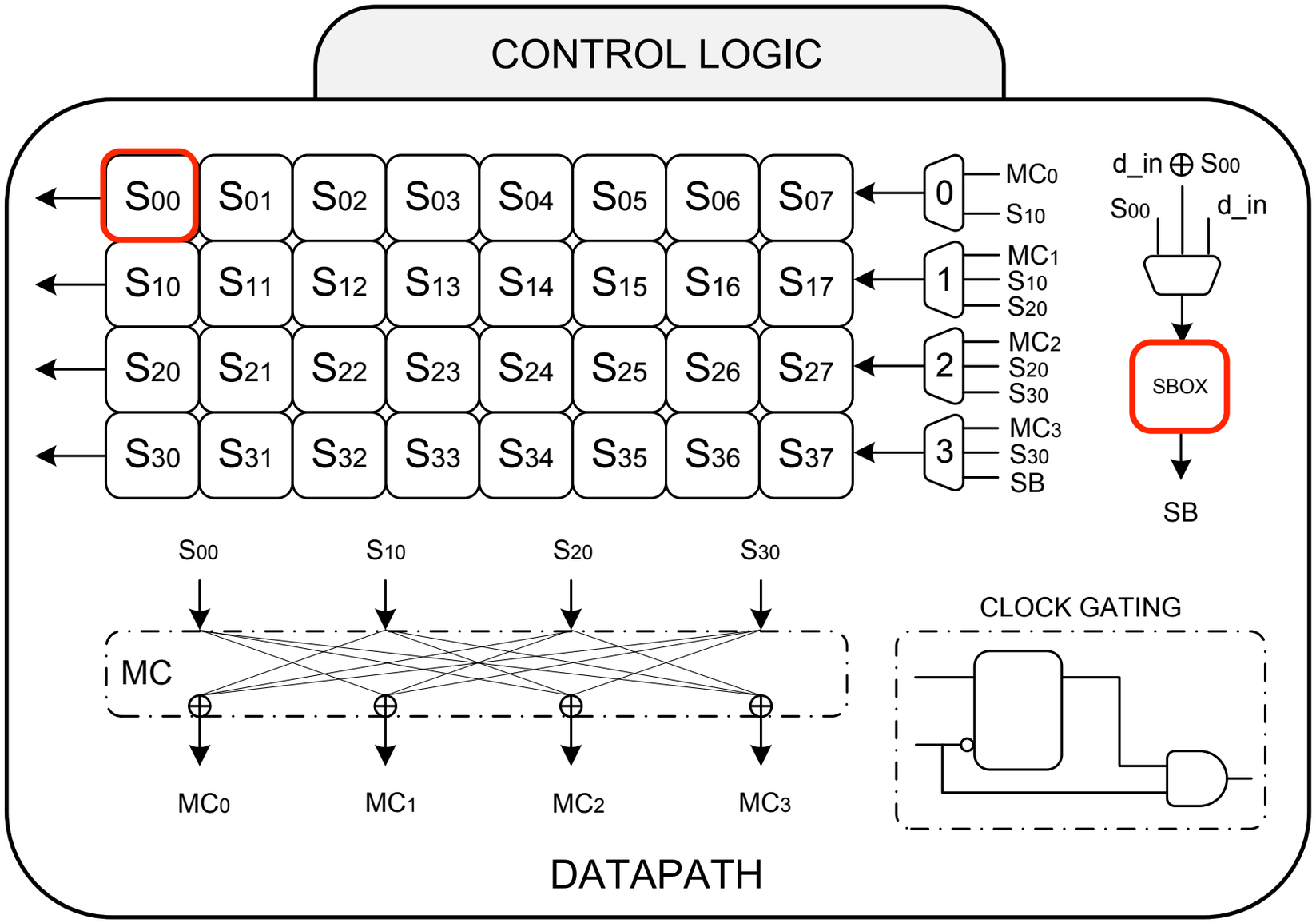
Implementation

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



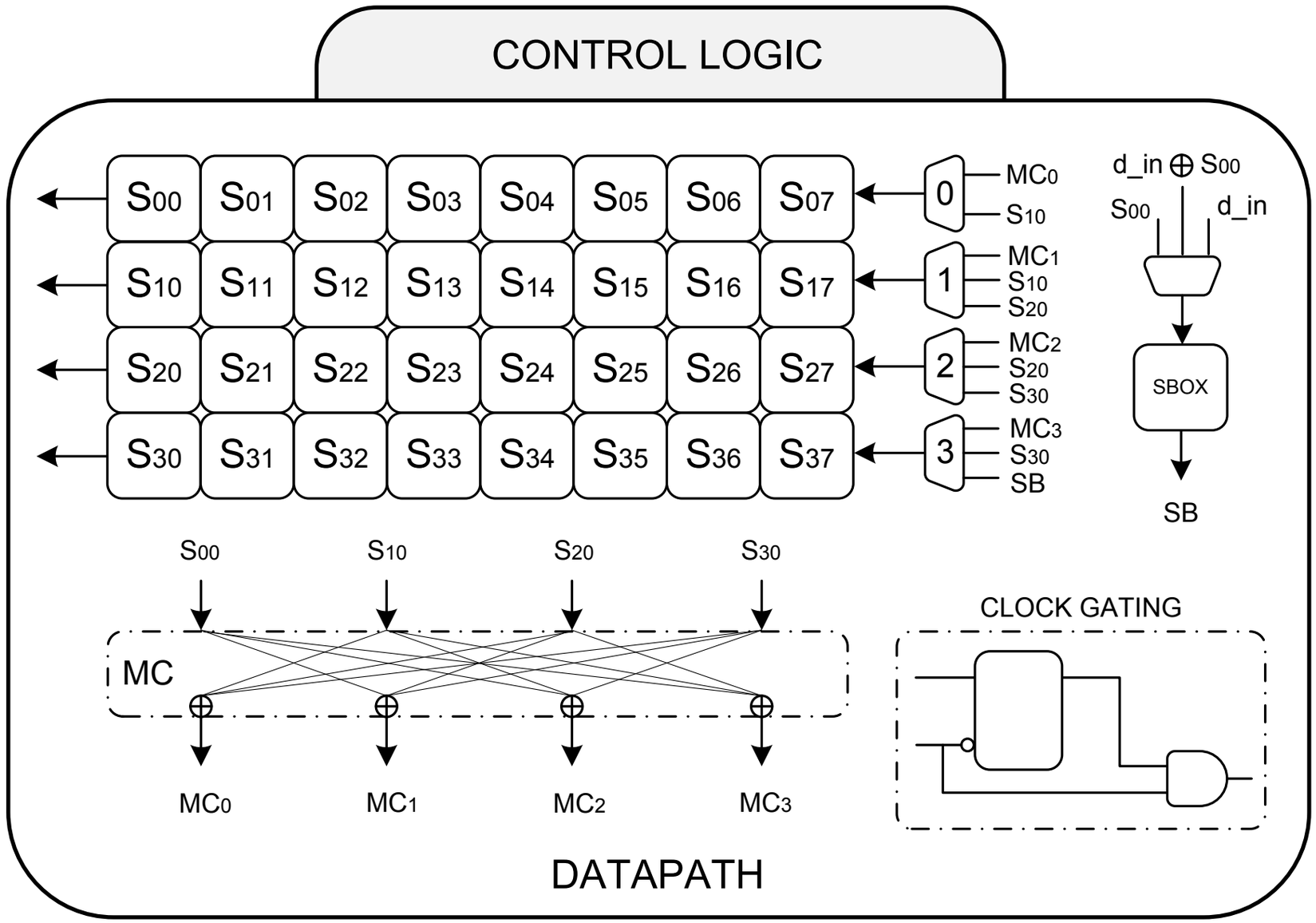
Implementation

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



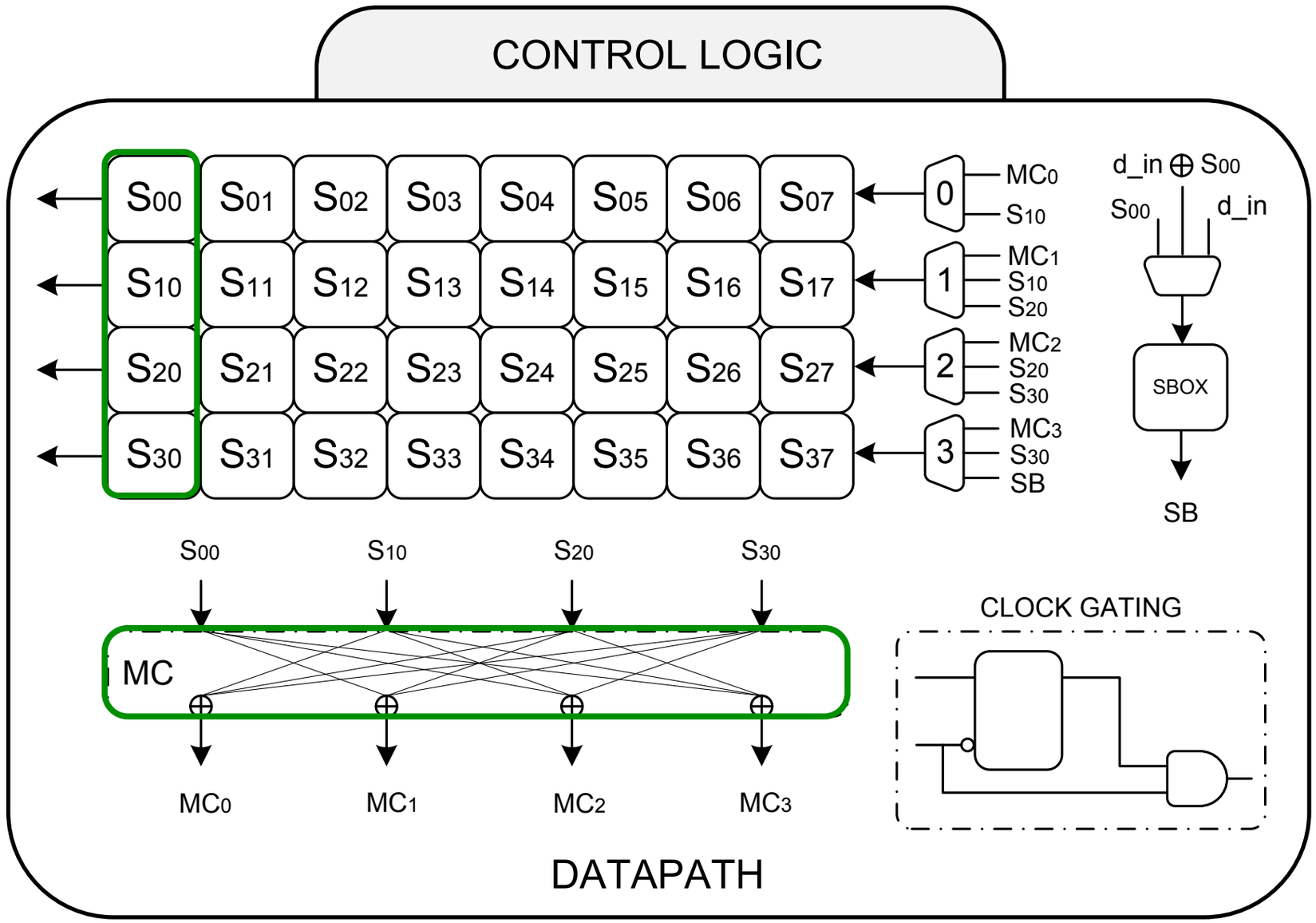
Implementation

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



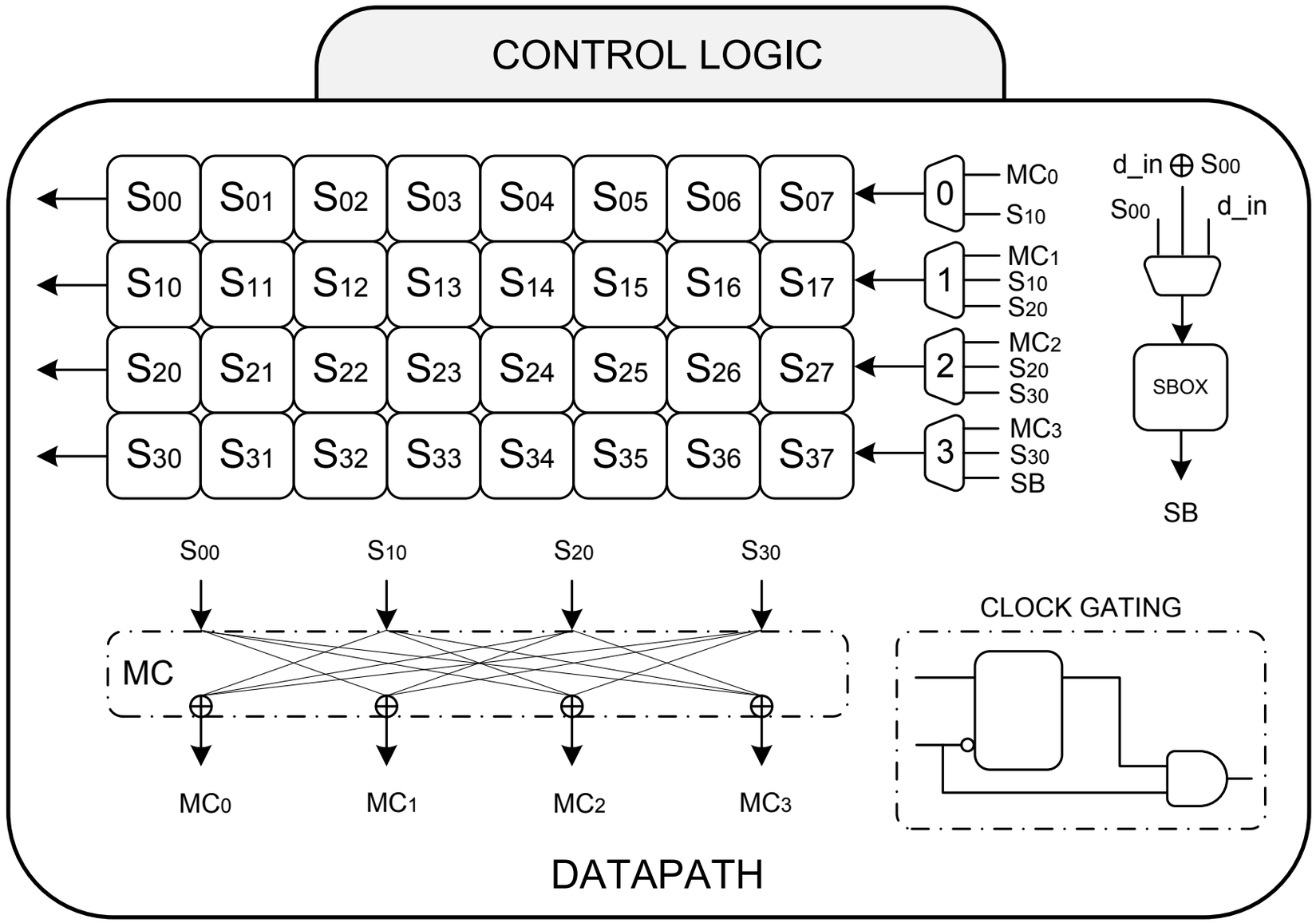
Implementation

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



Implementation

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

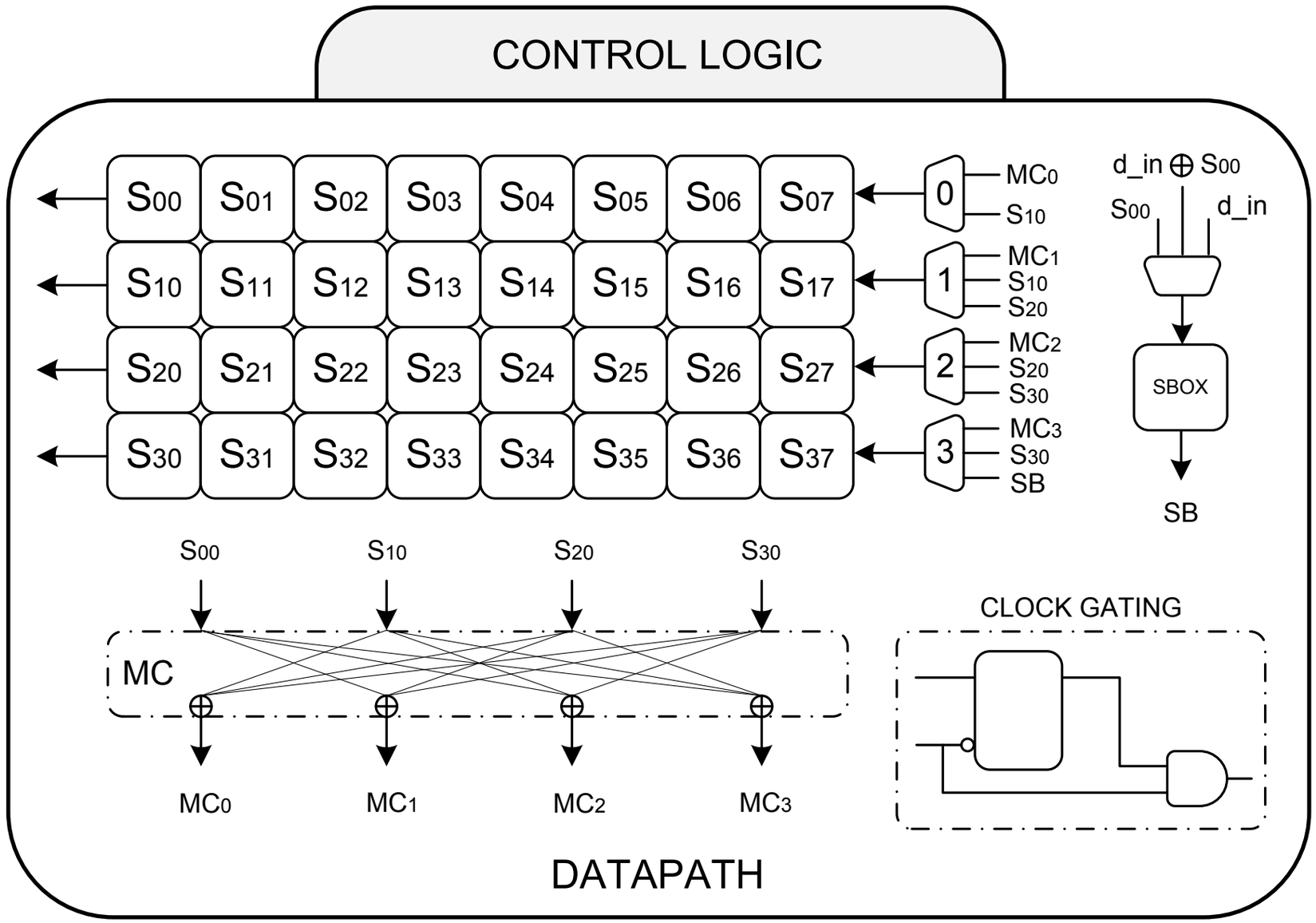


Implementation

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

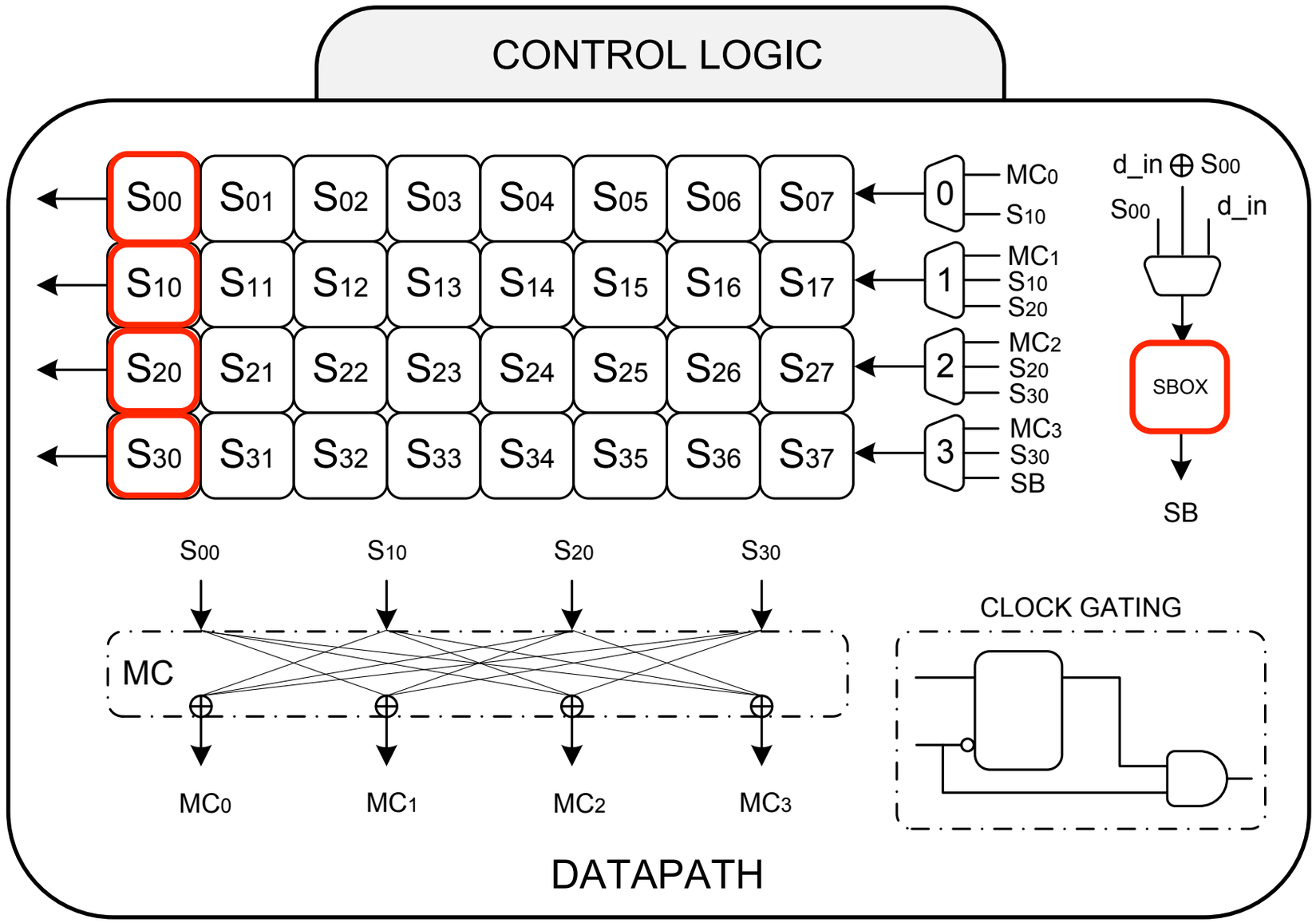
Implementation

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



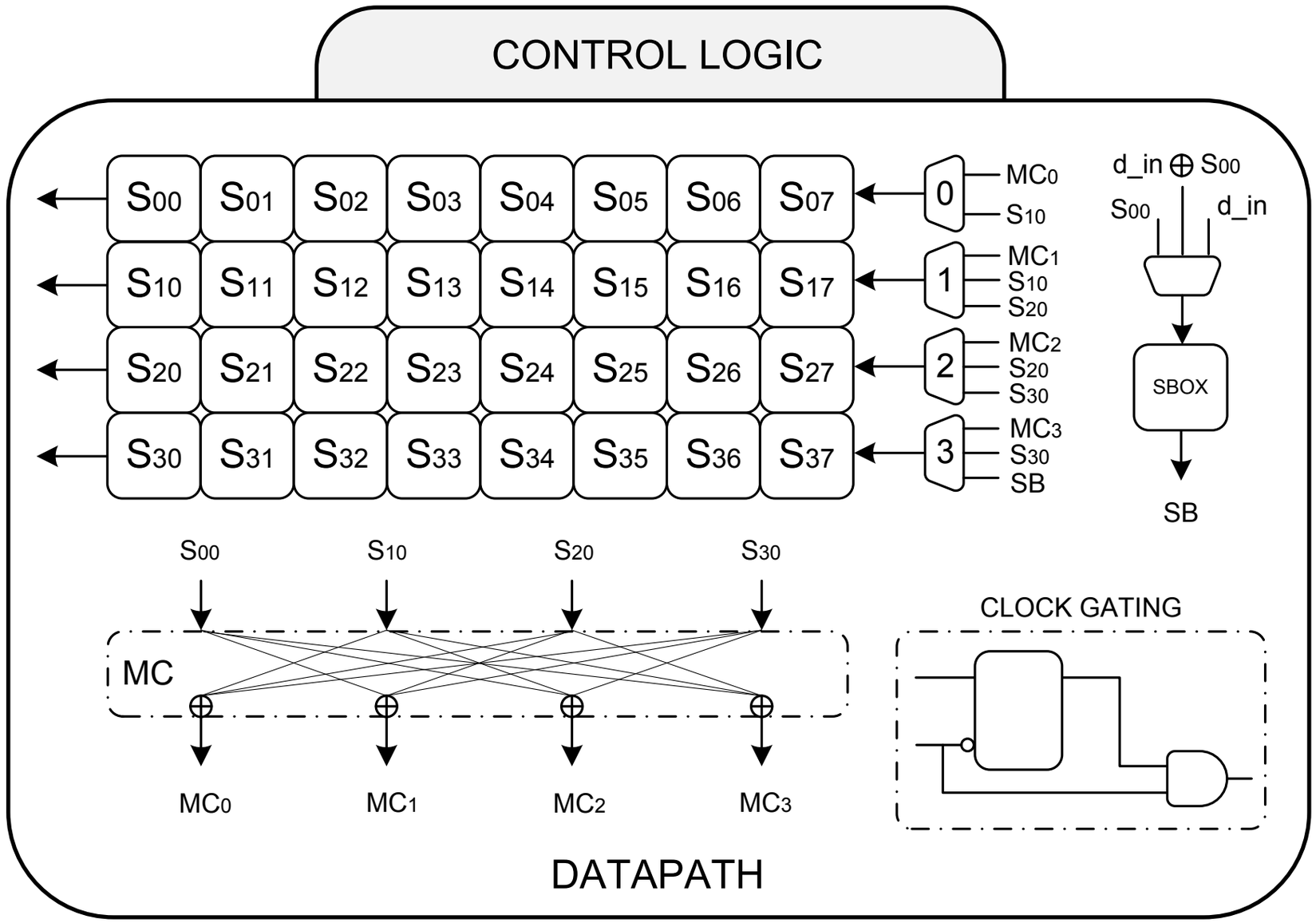
Implementation

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



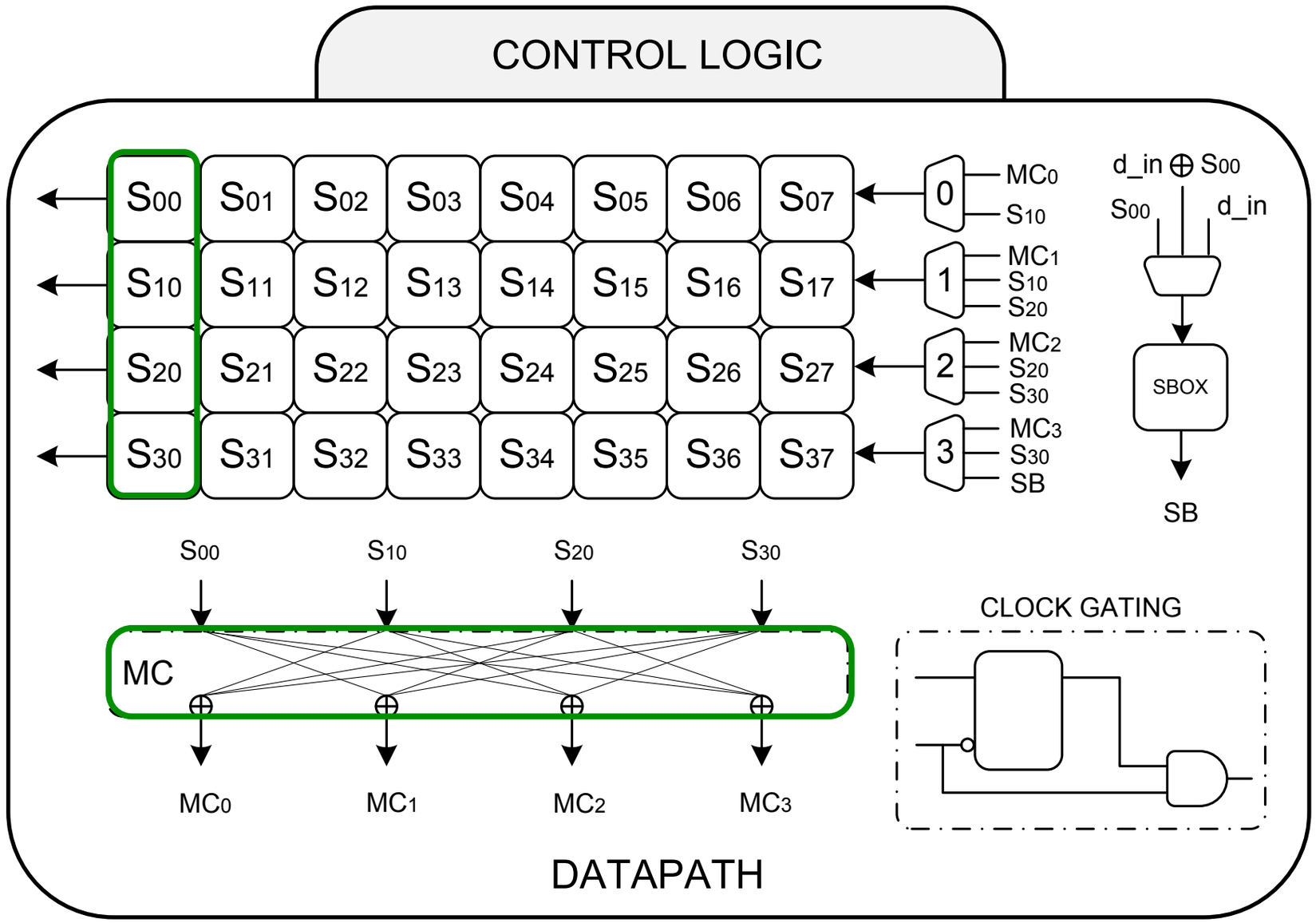
Implementation

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



Implementation

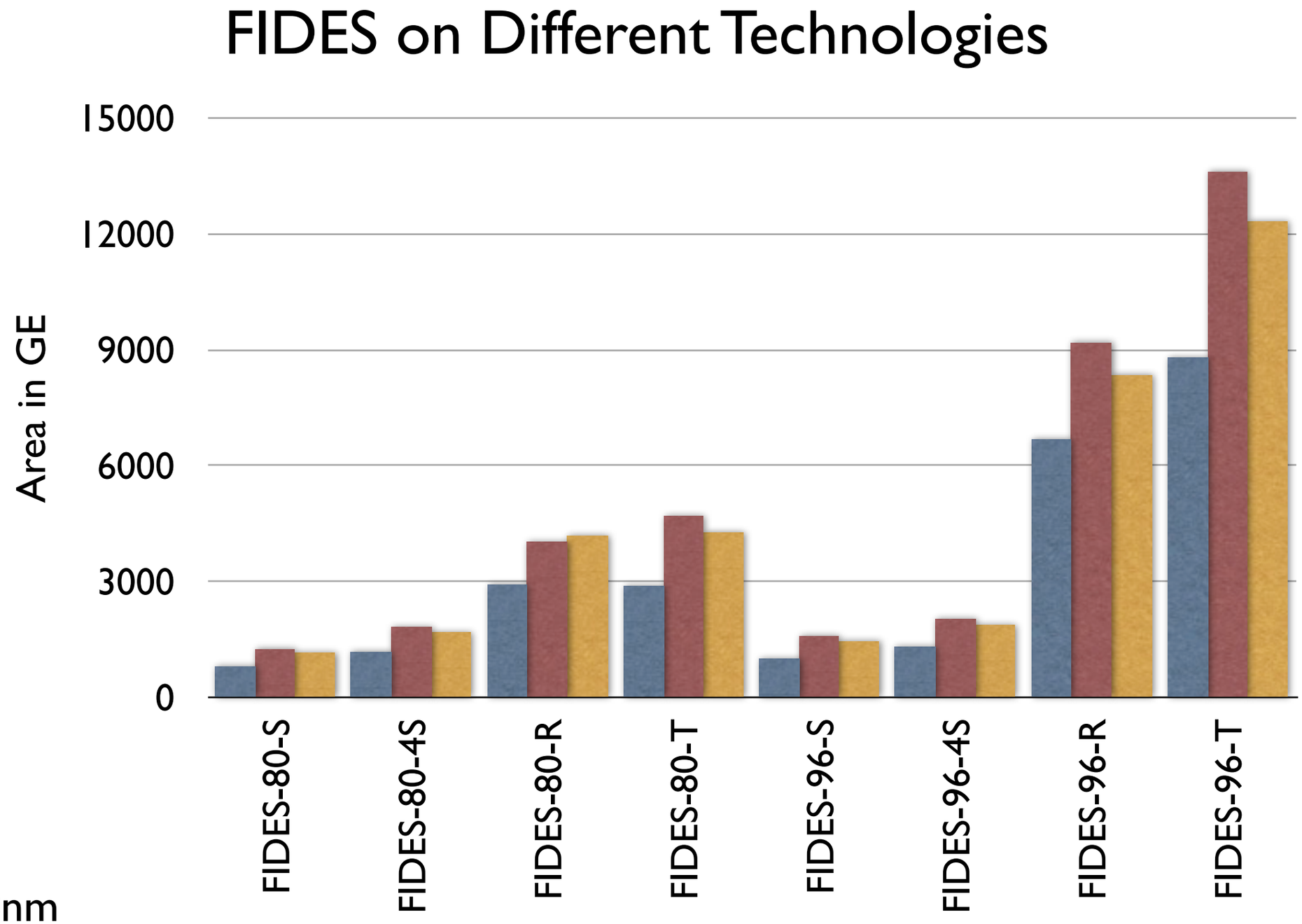
- FIDES-S
- FIDES-4S
- FIDES-R
- FIDES-T



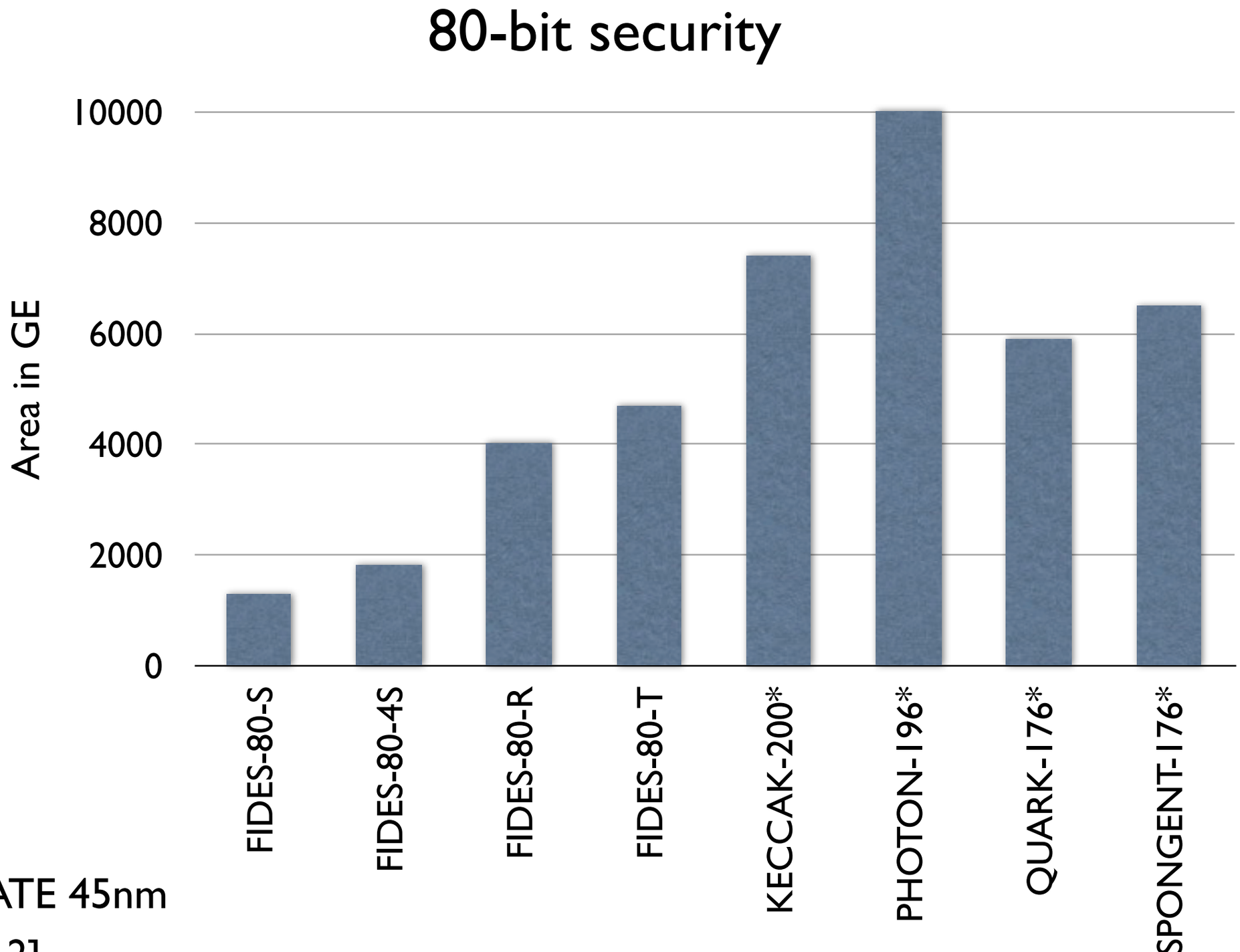
Implementation

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

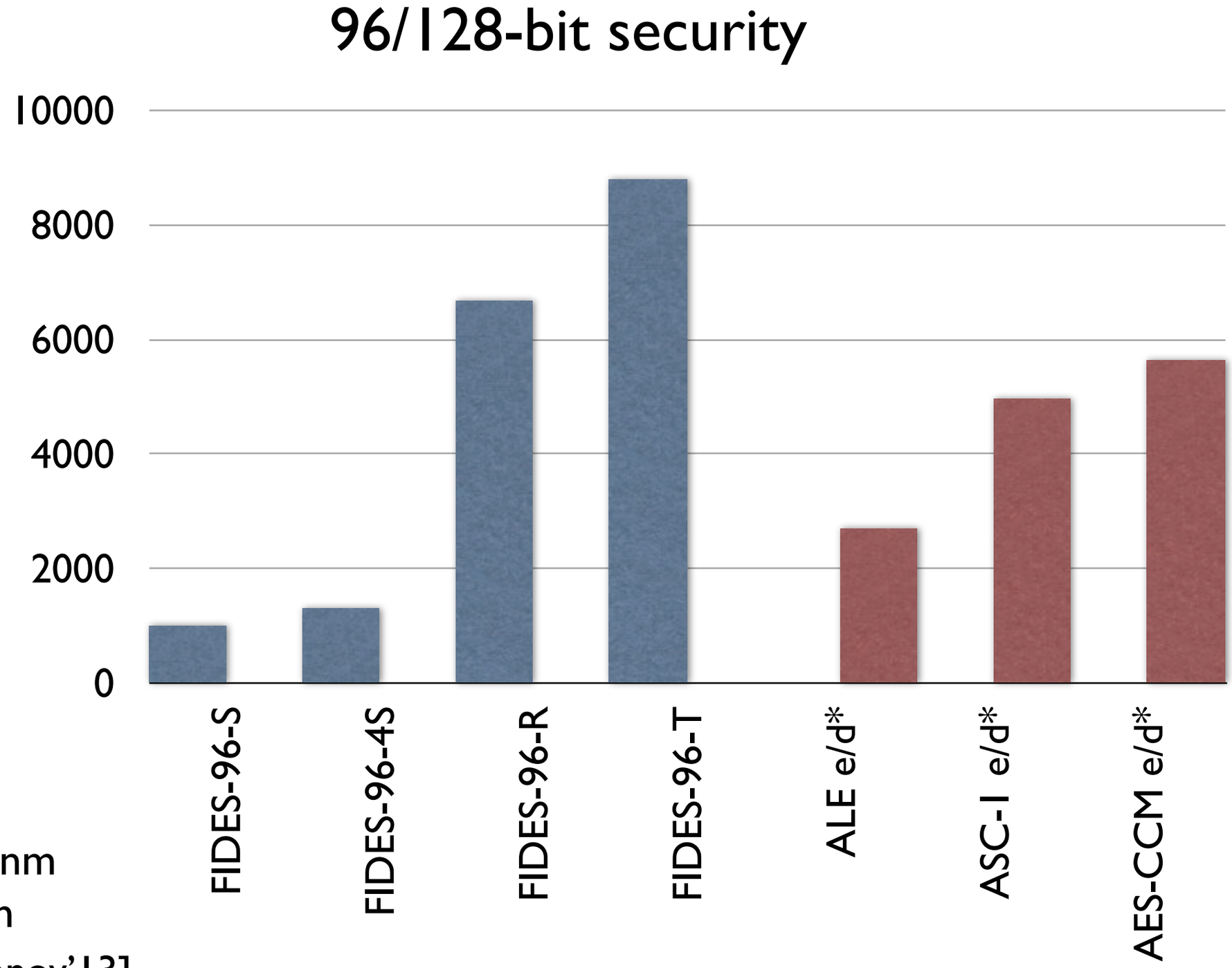
Performance



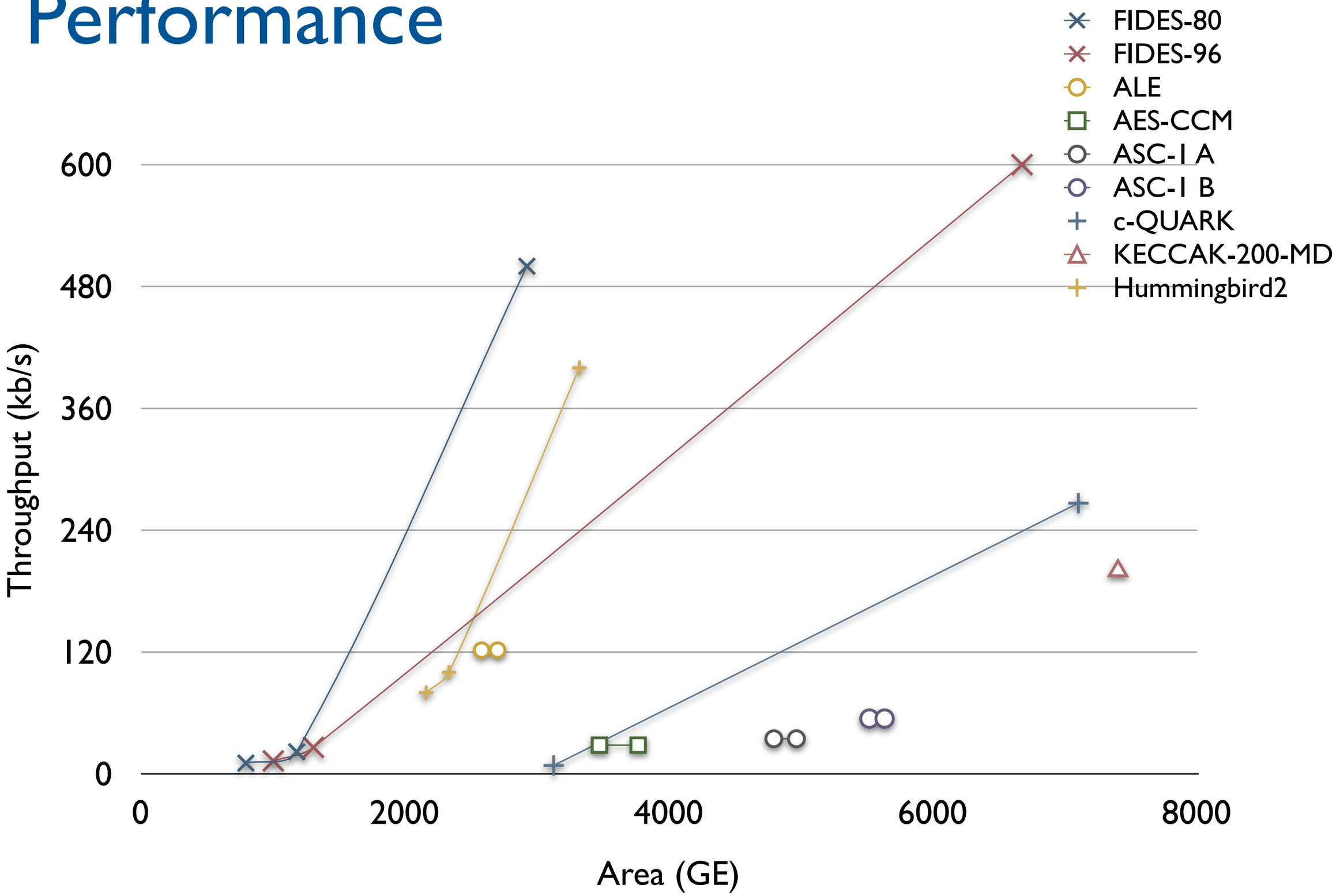
Performance



Performance



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!