RUHR-UNIVERSITÄT BOCHUM

Bit-Sliding: A Generic Technique for Bit-Serial Implementations of SPN-based Primitives

28. Sep. 2017

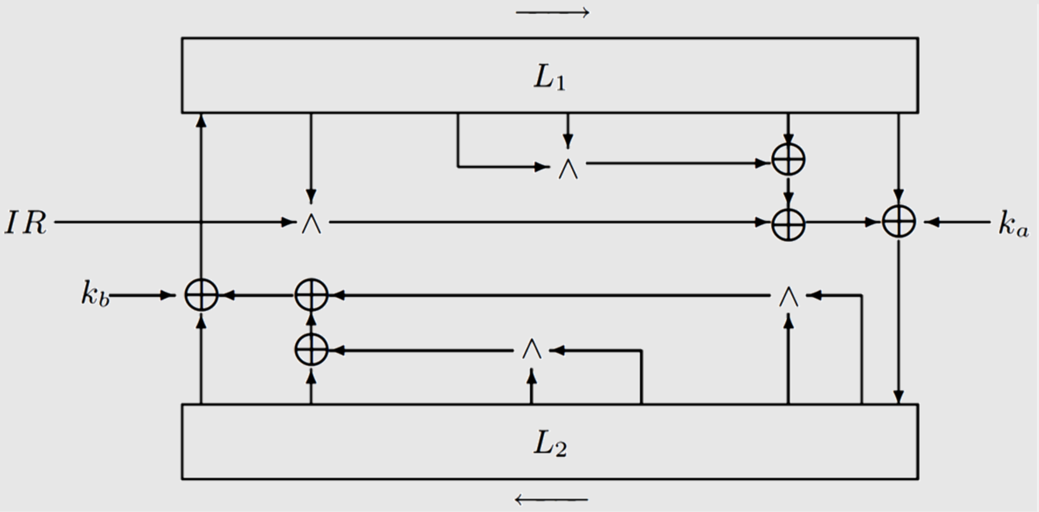
Jérémy Jean, Amir Moradi, Thomas Peyrin, Pascal Sasdrich

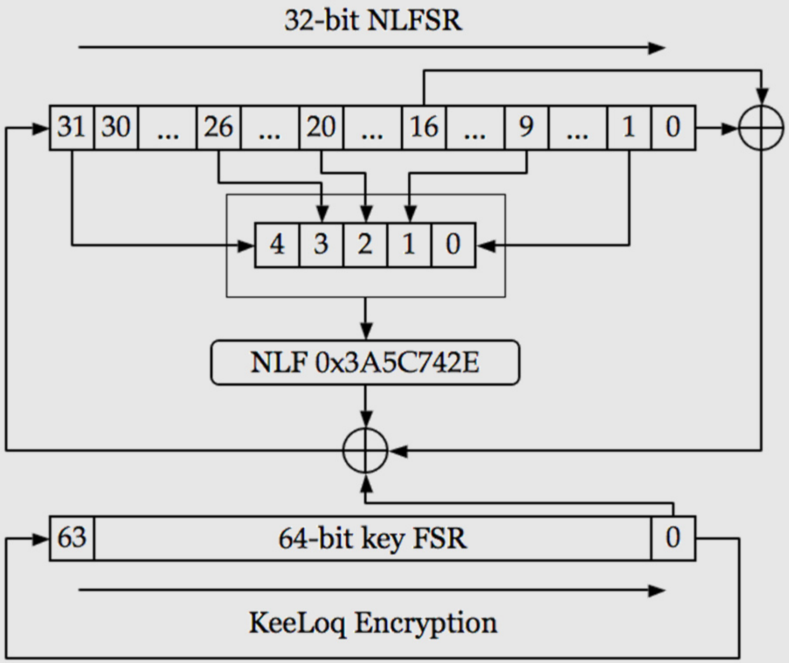
ANSSI Crypto Lab, Paris, France
Ruhr University Bochum, Germany
Temasek Laboratories, Nanyang Technological University, Singapore

Horst Görtz Institute
for IT-Security

Story?

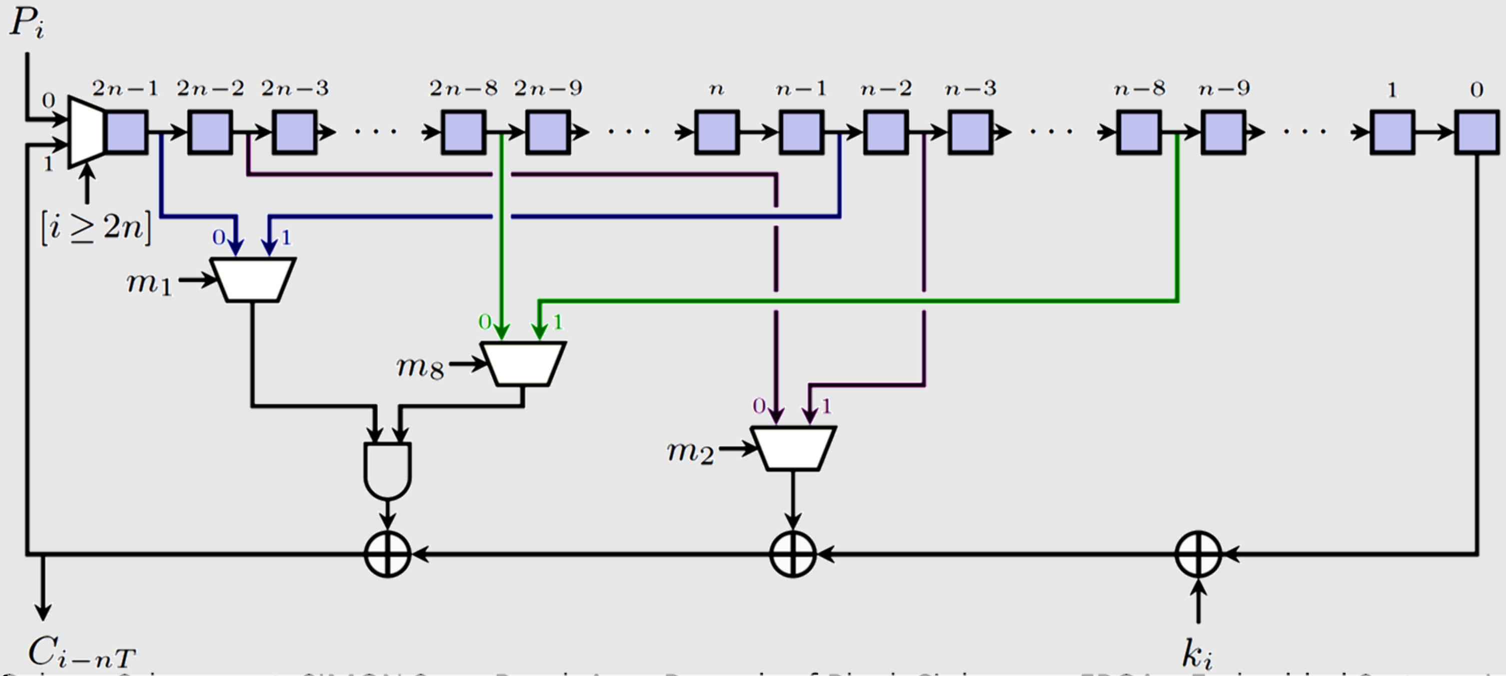
- motivated by KATAN & Simon bit-serial implementations
  - KATAN: NLFSR/steam-cipher construction (borrowed from KeeLoq)





Story?

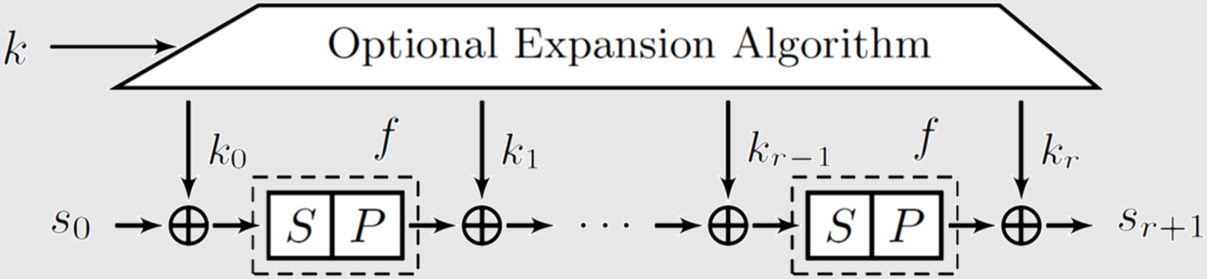
- motivated by KATAN & Simon bit-serial implementations
  - KATAN: NLFSR/steam-cipher construction (borrowed from KeeLoq)
  - Simon: Feistel
    - allows even a scalable architecture*



* Aysu, Gulcan, Schaumont: SIMON Says: Break Area Records of Block Ciphers on FPGAs. Embedded Systems Letters 2014

Story?

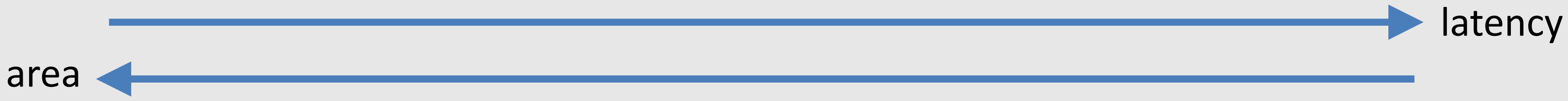
- motivated by KATAN & Simon bit-serial implementations
  - KATAN: NLFSR/steam-cipher construction (borrowed from KeeLoq)
  - Simon: Feistel
    - allows even a scalable architecture*
- How about SPN constructions?



* Aysu, Gulcan, Schaumont: SIMON Says: Break Area Records of Block Ciphers on FPGAs. Embedded Systems Letters 2014

SPN & Implementation Trade-offs

- fully unrolled … pipeline … round-based … serial



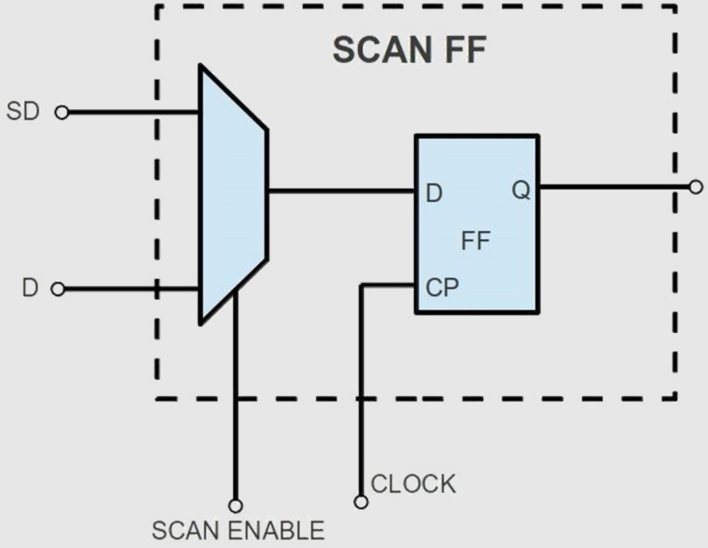
latency

area

- lightweight cryptography (smallest footprint): **serial** arch.
  - s-bit Sbox and l-bit linear function
    - s-bit data path, l a multiple of s (s-bit serial implementation)
  - PRESENT, LED, Klein, …: 4-bit serial
  - AES: 8-bit serial
  - enables to employ scan flip-flops

Scan Flip-flop

- developed & used in scan chain for testing purposes
- operates as (but smaller than) a MUX + D-FF

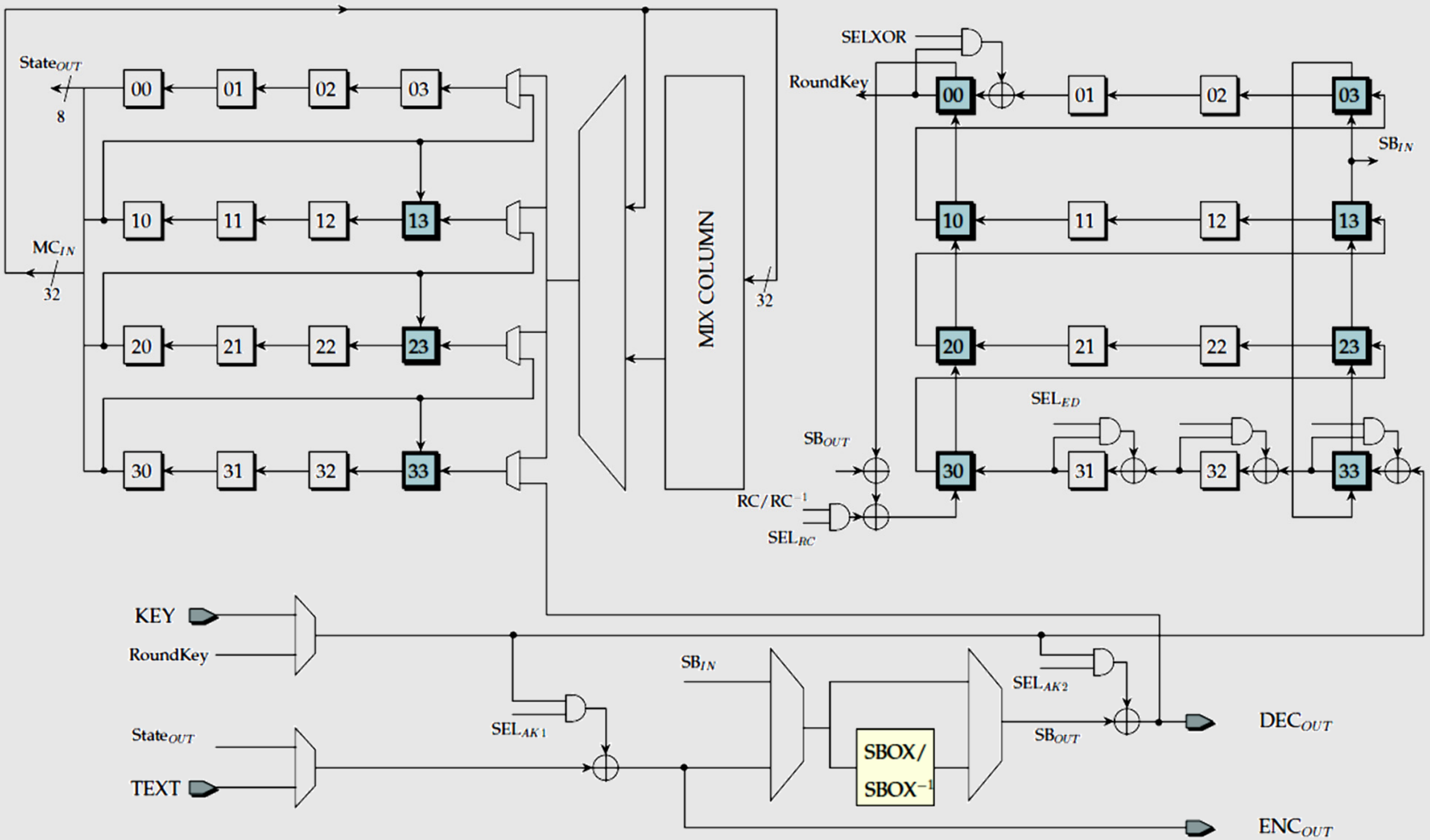


	UMC180	UMC130	UMC90	Ngate45	IBM130
	GE	GE	GE	GE	GE
1-bit D FF	4.67	5.00	4.25	5.67	4.25
1-bit Scan FF	6.00	6.25	5.75	7.67	5.50

MUX ≈ 2.33 GE

GE: Gate Equivalence: area of a NAND gate

Smallest Known Serial AES, Atomic AES v2.0



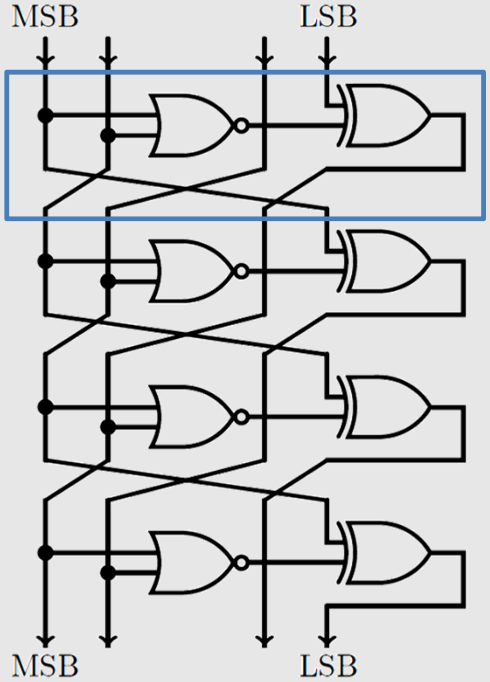
Banik, Bogdanov, Regazzoni, ePrint Archive: Report 2016/1005

Atomic AES v2.0

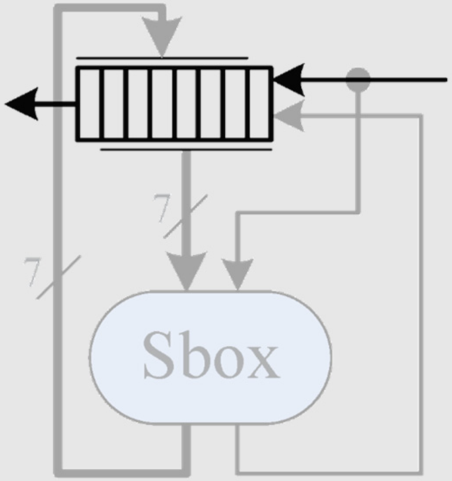
- supports both ENC & DEC
- clock gating for each row (due to ShiftRows & ShiftRows^{-1})
- 3 × 8-bit scan FF(state) + 8 × 8-bit scan FF(key): 88 scan FF
- $MC^{-1}(x) = MC(MC(MC(x)))$
- Canright Sbox (supporting Sbox^{-1})
- 2060 GE (STM 90nm)
  - 246 clock cycles ENC
  - 326 clock cycles DEC

Bit-Sliding

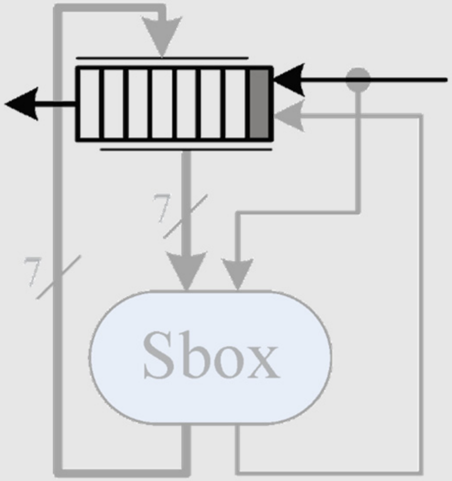
- use as many as possible regular FF, use less scan FF
- almost all register cells always shift (regular FF)
  - a few have multiple inputs (scan FF)
- challenge 1: s-bit Sbox
  - easy for PICCOLO & SKINNY Sboxes
  - how about AES, PRESENT, …?
    - no way (yet) than using the Sbox in parallel
- challenge 2: permutation
  - ad hoc, easy for AES, hard for PRESENT



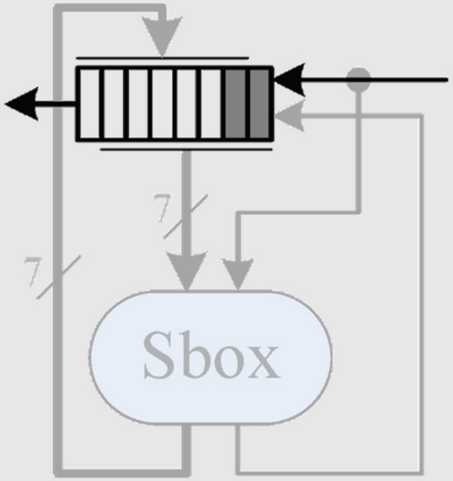
How Sbox works



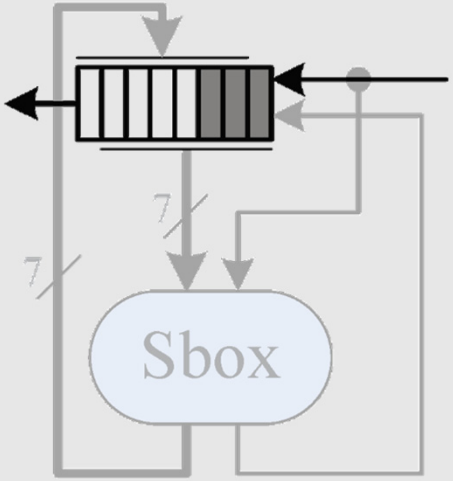
How Sbox works



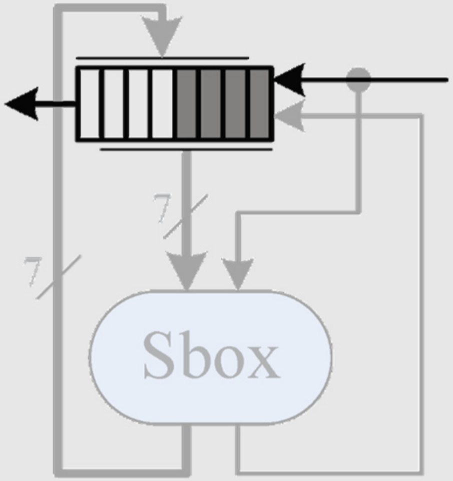
How Sbox works



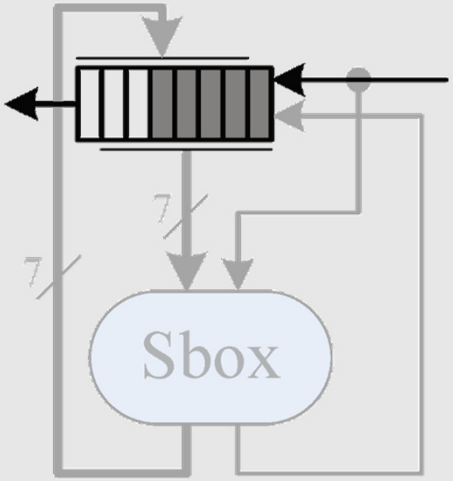
How Sbox works



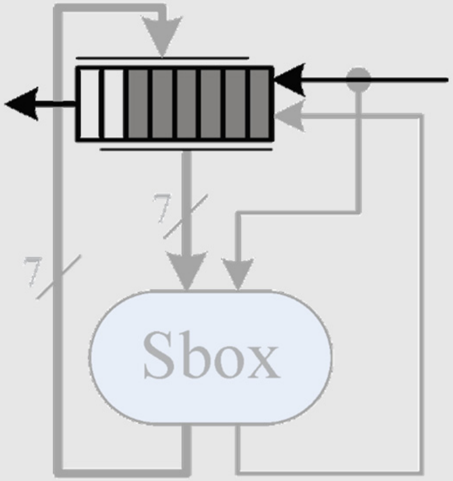
How Sbox works



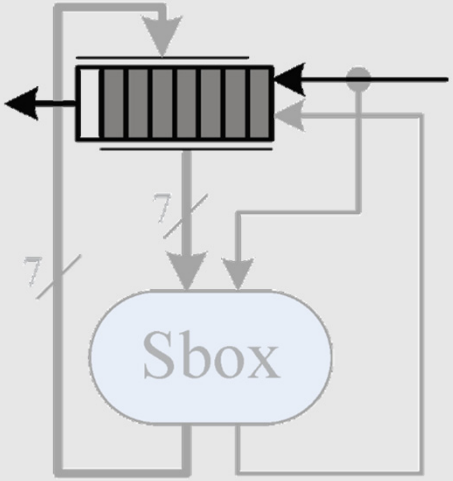
How Sbox works



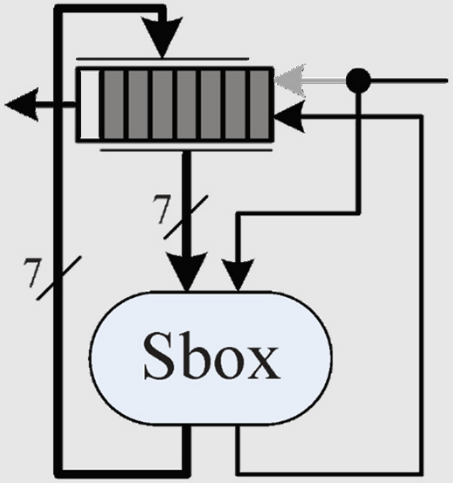
How Sbox works



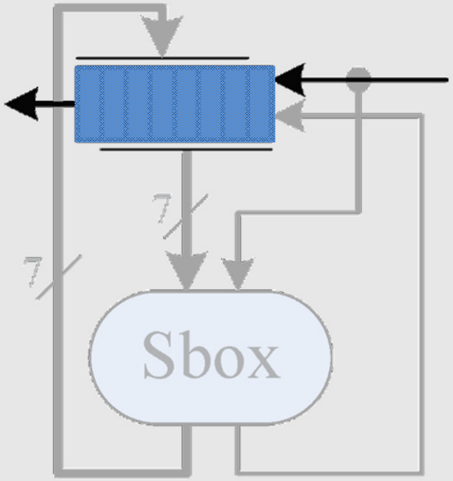
How Sbox works



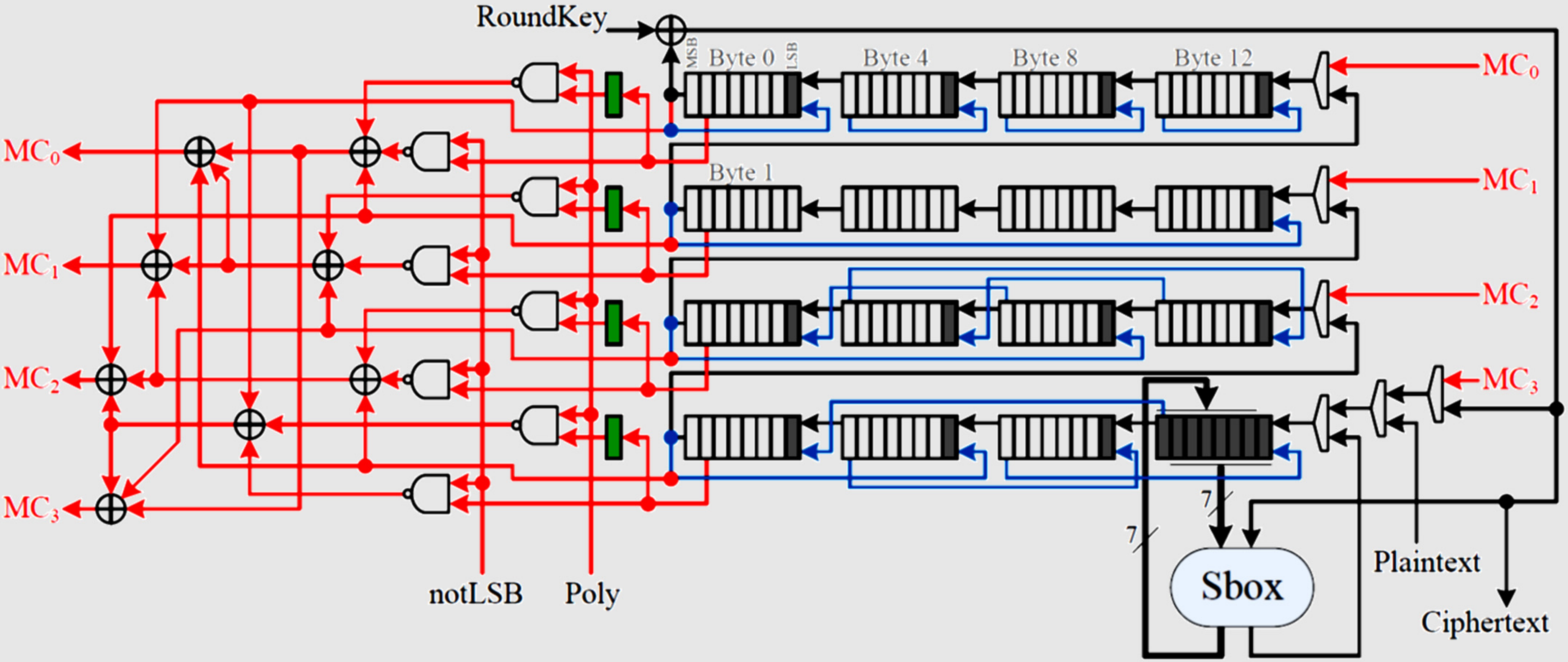
How Sbox works



How Sbox works

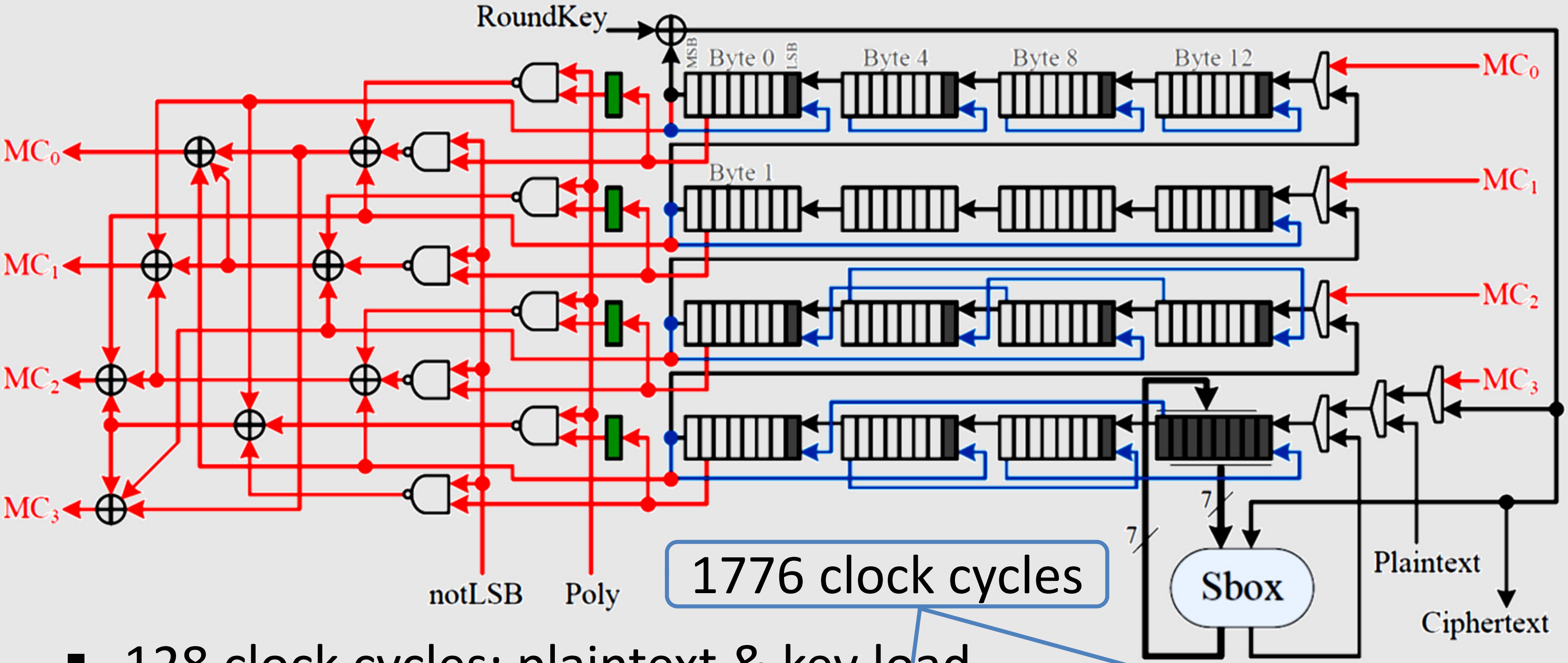


Bit-Serial AES-128, ENC only (state)



- 20 scan FF (state)
- no clock gating, no enable signal

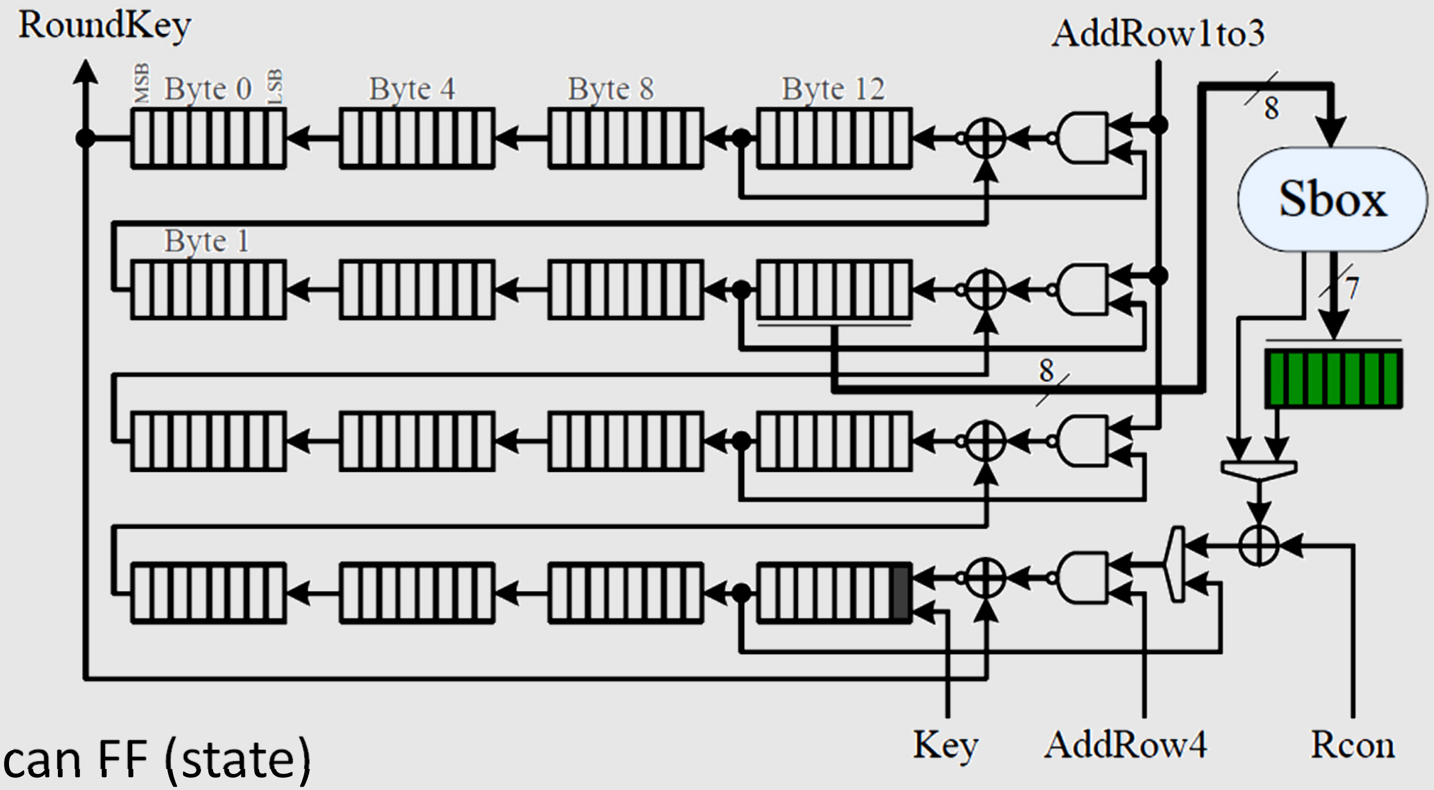
Bit-Serial AES-128, ENC only (state)



1776 clock cycles

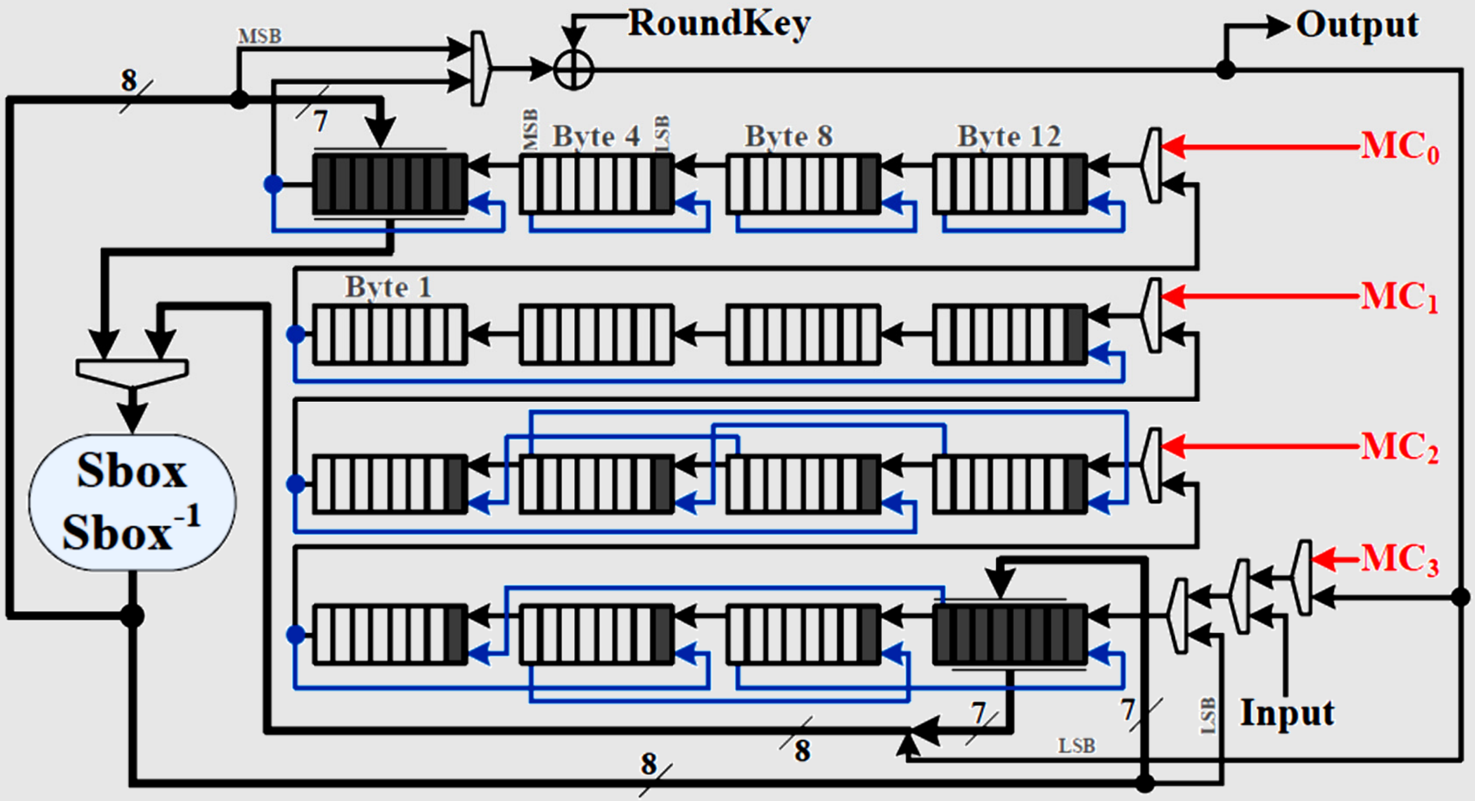
- 128 clock cycles: plaintext & key load
- 128 clock cycles: AddKey & SubBytes
- 8 clock cycles: ShiftRows 32 clock cycles: MixColumns

Bit-Serial AES-128, ENC only (key)



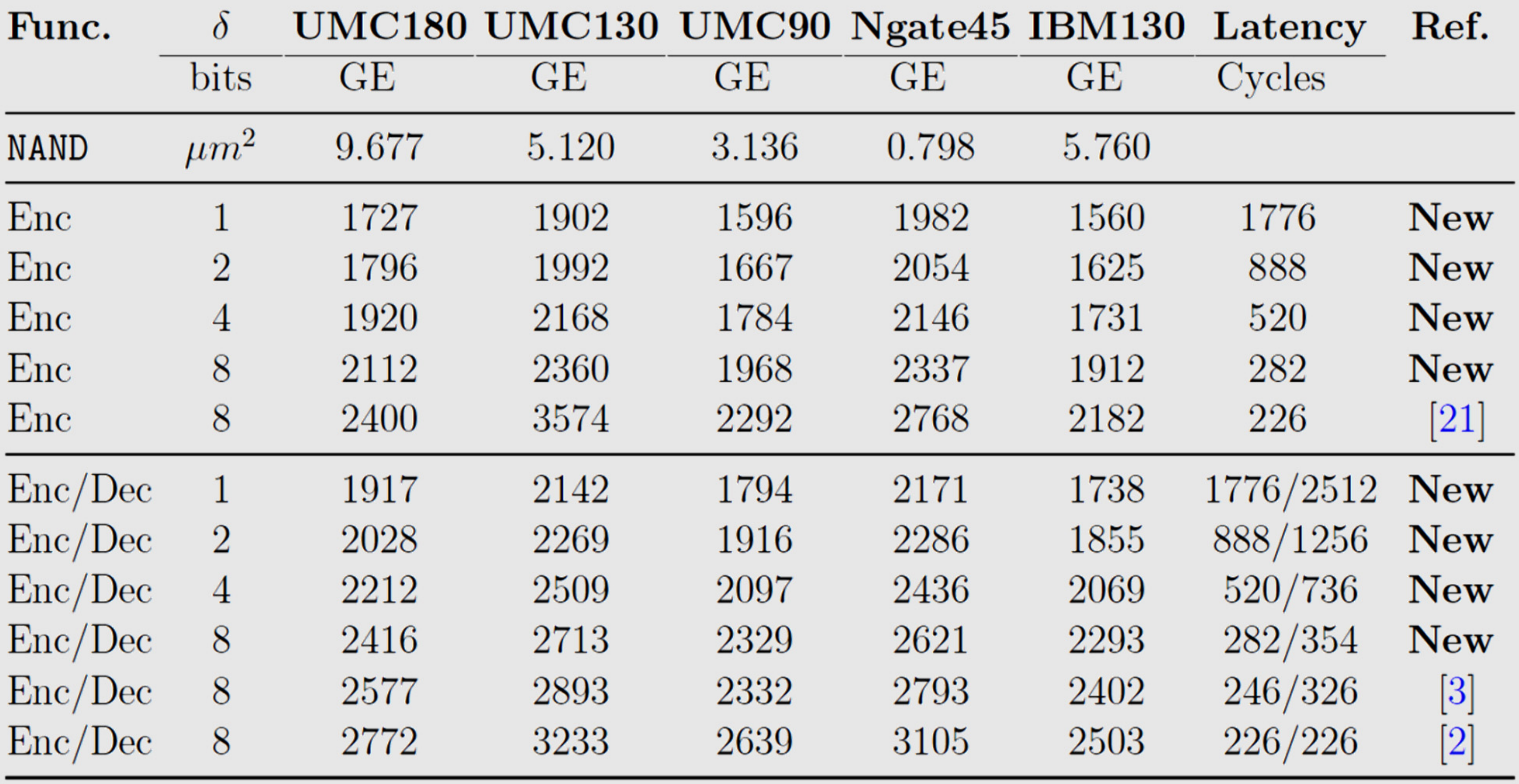
- 1 scan FF (state)
- 1 clock gating
- 7 extra FF (shared with MC)
- the largest difference compared to state of the art

Bit-Serial AES-128, ENC & DEC (state)



- 27 scan FF (state) + 1 scan FF (key)
- no clock gating, no enable signal
- $MC^{-1}=MC^3$, $SR^{-1}=SR^3$ (no extra logic)

Results (AES-128)



Func.	δ	UMC180	UMC130	UMC90	Ngate45	IBM130	Latency	Ref.
	bits	GE	GE	GE	GE	GE	Cycles	
NAND	μm^2	9.677	5.120	3.136	0.798	5.760		
Enc	1	1727	1902	1596	1982	1560	1776	New
Enc	2	1796	1992	1667	2054	1625	888	New
Enc	4	1920	2168	1784	2146	1731	520	New
Enc	8	2112	2360	1968	2337	1912	282	New
Enc	8	2400	3574	2292	2768	2182	226	[21]
Enc/Dec	1	1917	2142	1794	2171	1738	1776/2512	New
Enc/Dec	2	2028	2269	1916	2286	1855	888/1256	New
Enc/Dec	4	2212	2509	2097	2436	2069	520/736	New
Enc/Dec	8	2416	2713	2329	2621	2293	282/354	New
Enc/Dec	8	2577	2893	2332	2793	2402	246/326	[3]
Enc/Dec	8	2772	3233	2639	3105	2503	226/226	[2]

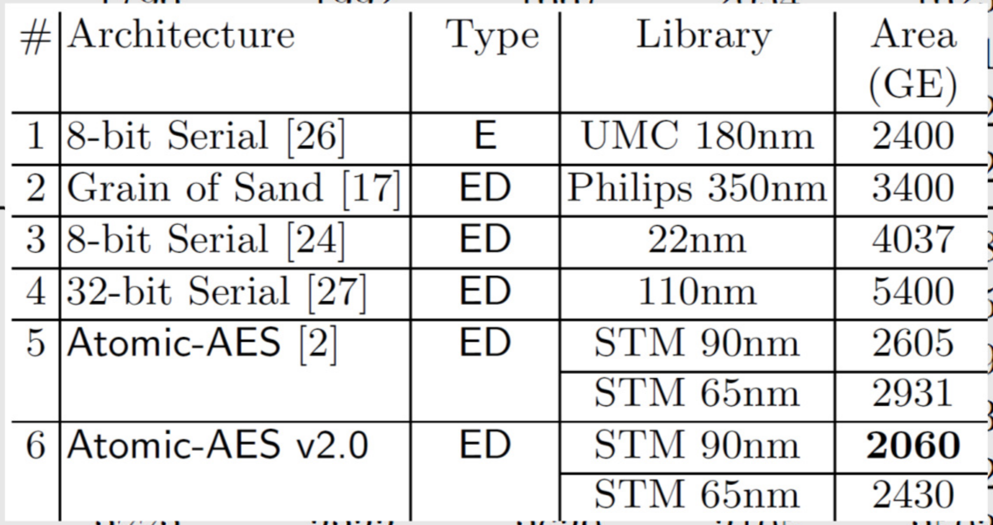
[2] Banik, Bogdanov, Regazzoni: Atomic-AES: A compact implementation of the AES enc/dec core. INDOCRYPT 2016

[3] Banik, Bogdanov, Regazzoni: Atomic-AES v2.0. ePrint Archive: Report 2016/1005

[21] Moradi, Poschmann, Ling, Paar, Wang: Pushing the limits: A very compact and a TI of AES. EUROCRYPT 2011

Results (AES-128)

Func.	δ	UMC180	UMC130	UMC90	Ngate45	IBM130	Latency	Ref.
	bits	GE	GE	GE	GE	GE	Cycles	
NAND	μm^2	9.677	5.120	3.136	0.798	5.760		
Enc	1	1727	1902	1596	1982	1560	1776	**New**
Enc	2	1796	1992	1667	2054	1625	888	**New**
Enc	4	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	520	**New**
Enc	8	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	282	**New**
Enc	8	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	226	[21]
Enc/Dec	1	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	1776/2512	**New**
Enc/Dec	2	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	888/1256	**New**
Enc/Dec	4	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	520/736	**New**
Enc/Dec	8	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	282/354	**New**
Enc/Dec	8	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	246/326	[3]
Enc/Dec	8	2772	3233	2639	3105	2503	226/226	[2]



#	Architecture	Type	Library	Area (GE)
1	8-bit Serial [26]	E	UMC 180nm	2400
2	Grain of Sand [17]	ED	Philips 350nm	3400
3	8-bit Serial [24]	ED	22nm	4037
4	32-bit Serial [27]	ED	110nm	5400
5	Atomic-AES [2]	ED	STM 90nm	2605
			STM 65nm	2931
6	Atomic-AES v2.0	ED	STM 90nm	**2060**
			STM 65nm	2430

[2] Banik, Bogdanov, Regazzoni: Atomic-AES: A compact implementation of the AES enc/dec core. INDOCRYPT 2016

[3] Banik, Bogdanov, Regazzoni: Atomic-AES v2.0. ePrint Archive: Report 2016/1005

[21] Moradi, Poschmann, Ling, Paar, Wang: Pushing the limits: A very compact and a TI of AES. EUROCRYPT 2011

Results (AES-128)

Func.	δ	UMC180	UMC130	UMC90	Ngate45	IBM130	Latency	Ref.
NAND								
Enc	1	1727	1902	1596	1982	1560	1776	New
Enc	2	1796	1992	1667	2054	1625	888	New
Enc	4	1920	2168	1784	2146	1731	520	New
Enc	8	2112	2360	1968	2337	1912	282	New
Enc	8	2400	3574	2292	2768	2182	226	[21]
Enc/Dec	1	1917	2142	1794	2171	1738	1776/2512	New
Enc/Dec	2	2028	2269	1916	2286	1855	888/1256	New
Enc/Dec	4	2212	2509	2097	2436	2069	520/736	New
Enc/Dec	8	2416	2713	2329	2621	2293	282/354	New
Enc/Dec	8	2577	2893	2332	2793	2402	246/326	[3]
Enc/Dec	8	2772	3233	2639	3105	2503	226/226	[2]

Visconti, Schiavo, Peralta: Improved upper bounds for the expected circuit complexity of dense systems of linear equations over GF(2). ePrint 2017/194

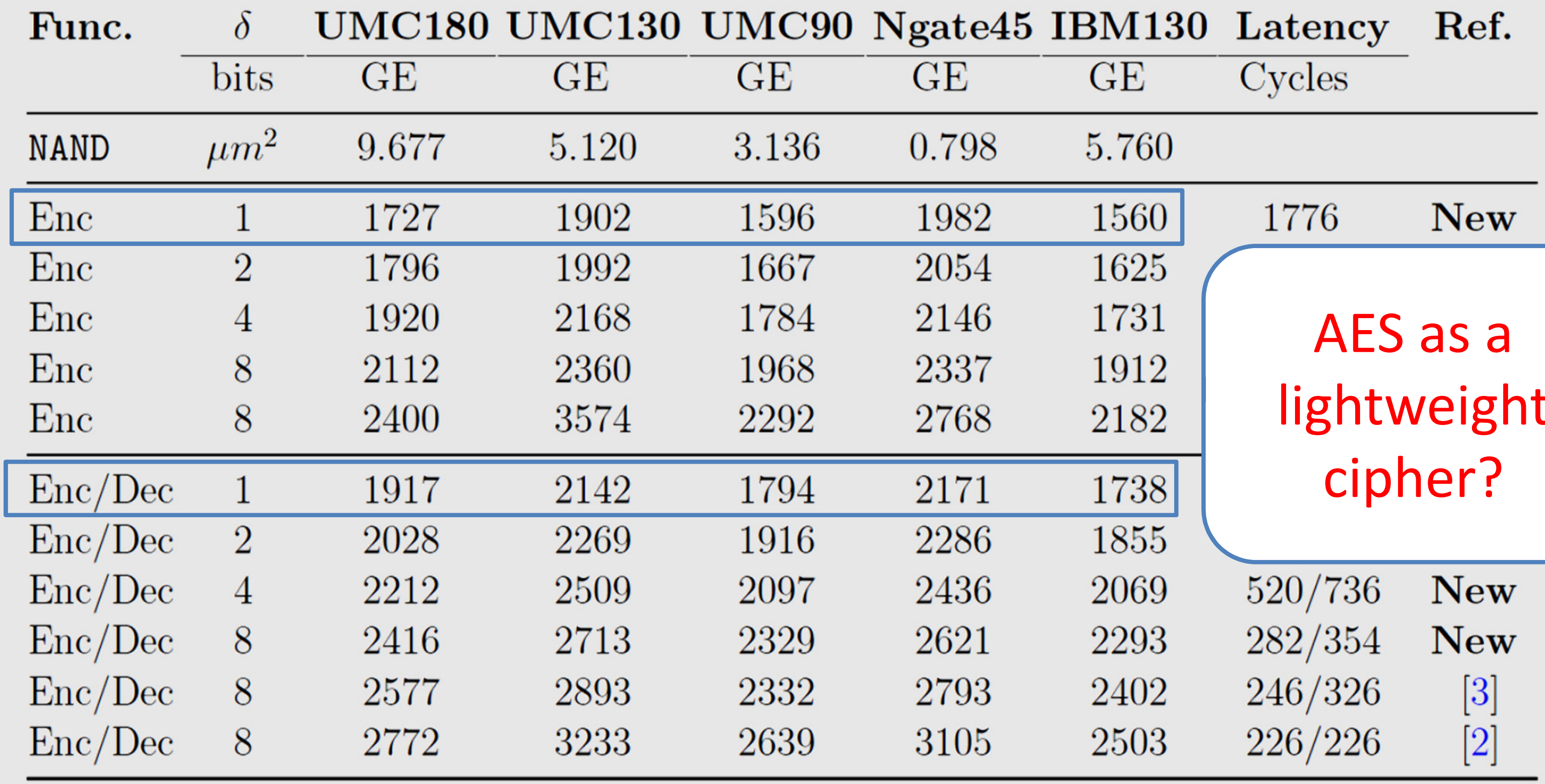
David Canright: A Very Compact S-Box for AES. CHES 2005

[2] Banik, Bogdano ore. INDOCRYPT 2016

[3] Banik, Bogdanov

[21] Moradi, Poschmann, Ling, Paar, Wang: Pushing the limits: A very compact and a TI of AES. EUROCRYPT 2011

Results (AES-128)



Func.	δ	UMC180	UMC130	UMC90	Ngate45	IBM130	Latency	Ref.
	bits	GE	GE	GE	GE	GE	Cycles	
NAND	μm^2	9.677	5.120	3.136	0.798	5.760		
Enc	1	1727	1902	1596	1982	1560	1776	New
Enc	2	1796	1992	1667	2054	1625		
Enc	4	1920	2168	1784	2146	1731		
Enc	8	2112	2360	1968	2337	1912		
Enc	8	2400	3574	2292	2768	2182		
Enc/Dec	1	1917	2142	1794	2171	1738		
Enc/Dec	2	2028	2269	1916	2286	1855		
Enc/Dec	4	2212	2509	2097	2436	2069	520/736	New
Enc/Dec	8	2416	2713	2329	2621	2293	282/354	New
Enc/Dec	8	2577	2893	2332	2793	2402	246/326	[3]
Enc/Dec	8	2772	3233	2639	3105	2503	226/226	[2]

AES as a lightweight cipher?

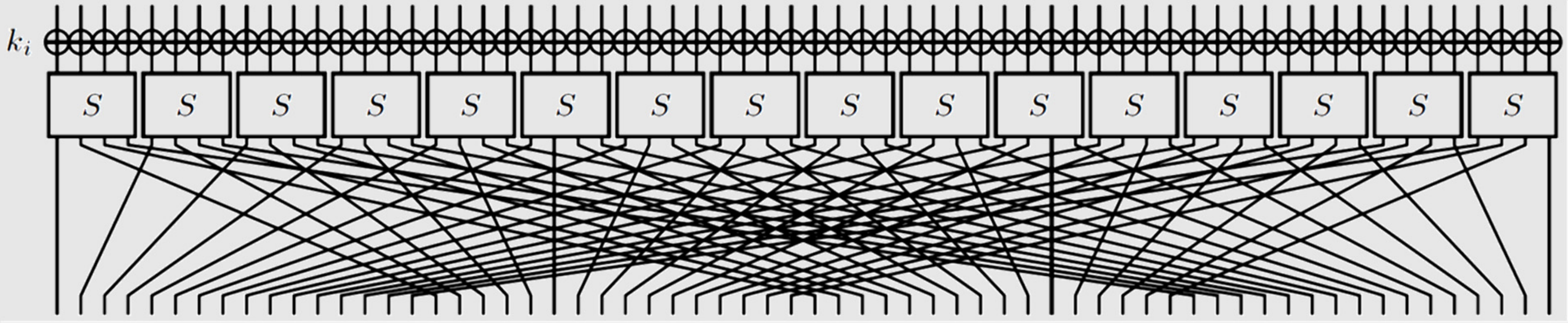
[2] Banik, Bogdanov, Regazzoni: Atomic-AES: A compact implementation of the AES enc/dec core. INDOCRYPT 2016

[3] Banik, Bogdanov, Regazzoni: Atomic-AES v2.0. ePrint Archive: Report 2016/1005

[21] Moradi, Poschmann, Ling, Paar, Wang: Pushing the limits: A very compact and a TI of AES. EUROCRYPT 2011

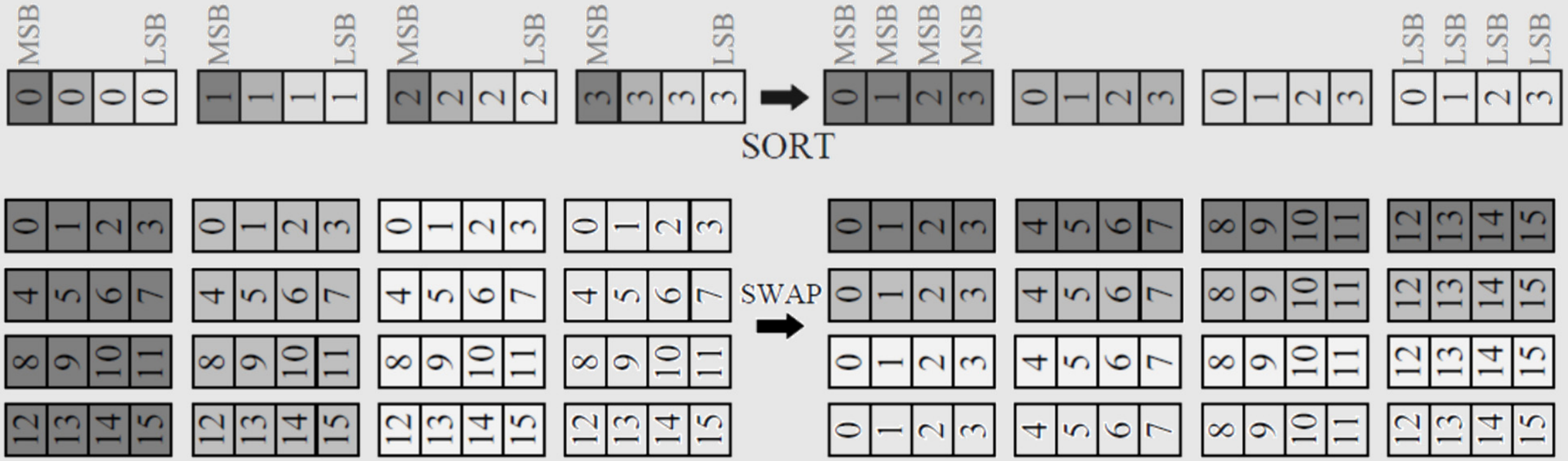
Bit-Serial PRESENT

- the same principle for Sbox
- the diffusion layer: bit-permutation network



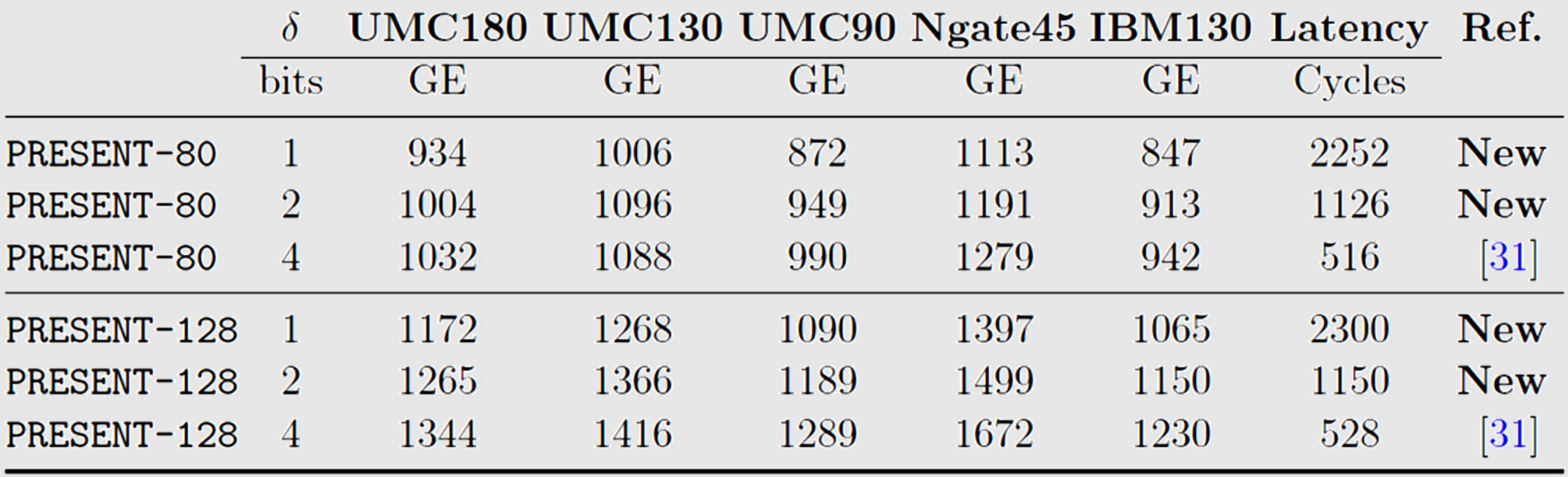
Bit-Serial PRESENT

- the same principle for Sbox
- the diffusion layer: bit-permutation network
  - our approach: two-level permutation



the same independently found by
Reis, Aranha, López: PRESENT Runs Fast - Efficient and Secure Implementation in Software. CHES 2017

Results (PRESENT)

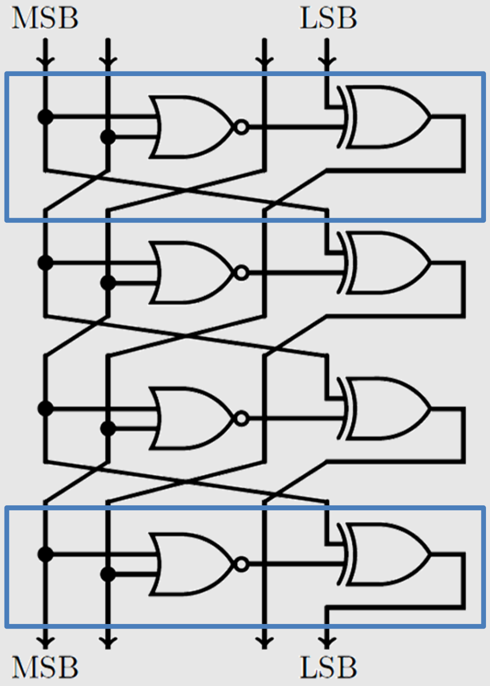


	δ	UMC180	UMC130	UMC90	Ngate45	IBM130	Latency	Ref.
	bits	GE	GE	GE	GE	GE	Cycles	
PRESENT-80	1	934	1006	872	1113	847	2252	New
PRESENT-80	2	1004	1096	949	1191	913	1126	New
PRESENT-80	4	1032	1088	990	1279	942	516	[31]
PRESENT-128	1	1172	1268	1090	1397	1065	2300	New
PRESENT-128	2	1265	1366	1189	1499	1150	1150	New
PRESENT-128	4	1344	1416	1289	1672	1230	528	[31]

[31] Ya, Khoo, Poschmann, Henricksen: EPCBC - A Block Cipher Suitable for Electronic Product Code Encryption. CANS 2011

Skinny

- first glance: iterative Sbox construction helps
- reality: the parallel technique still better
  - not fully iterative (last round different)
  - Sbox itself small
  - Bit-serial already slow
    - becomes almost 4 times slower
- the same for 8-bit variant

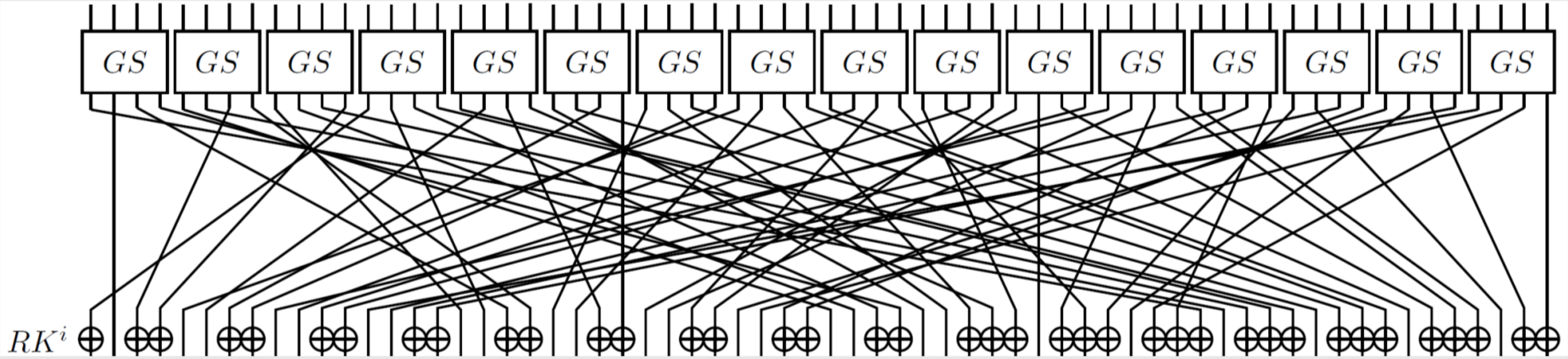


Conclusions

- not anymore monopoly on bit-serial and scalable architecture by Simon & Speck
- iterative Sbox not necessarily helps
- small Sboxes in lightweight crypto anyways
  - see GIFT: A Small PRESENT. CHES 2017
- diffusion layer more important to enable bit-serialization

Conclusions

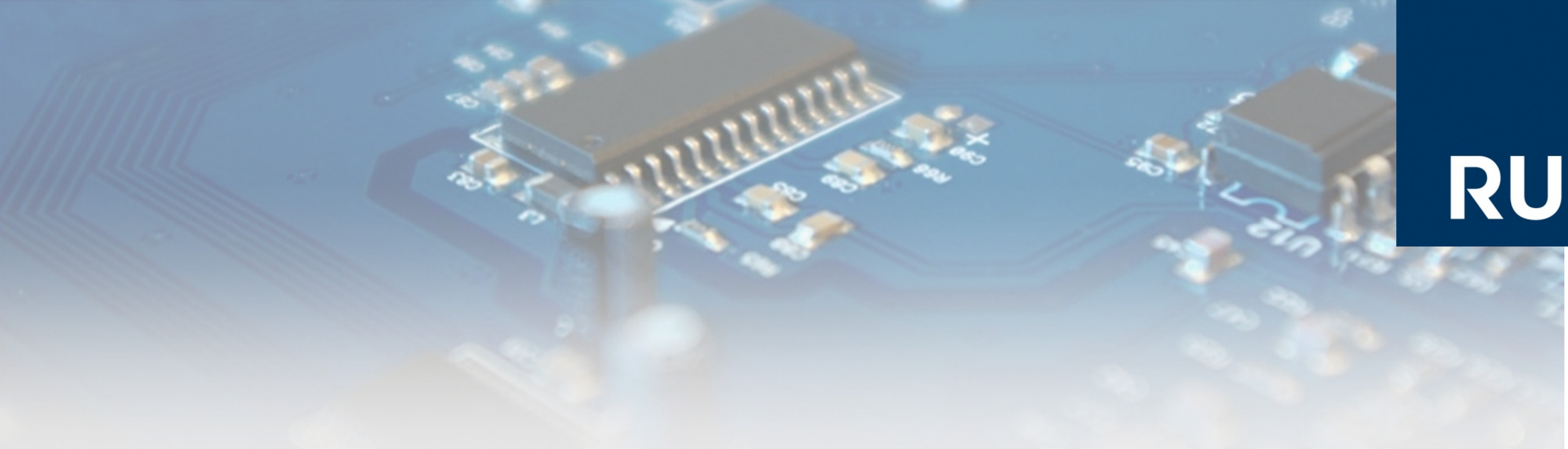
- not anymore monopoly on bit-serial and scalable



- diffusion layer more important to enable bit-serialization
  - Skinny < PRESENT < GIFT
    - (for 64-bit state & 128-bit key)

Conclusions

- not anymore monopoly on bit-serial and scalable architecture by Simon & Speck
- iterative Sbox not necessarily helps
- small Sboxes in lightweight crypto anyways
  - see GIFT: A Small PRESENT. CHES 2017
- diffusion layer more important to enable bit-serialization
  - Skinny < PRESENT < GIFT
    - (for 64-bit state & 128-bit key)
- latency high anyway
  - high energy consumption, but expected low power consumption



Thanks!

any questions?

amir.moradi@rub.de

Embedded Security Group, Ruhr University Bochum, Germany