Towards Low Energy Block Ciphers

Subhadeep Banik, Andrey Bogdanov, Francesco Regazzoni

Speaker: Francesco Regazzoni

Motivations

- IoT devices
- Implantable Devices
- Battery operated and (?) Energy harvesting devices
- **Energy is a very important parameter in several applications!**

Lightweight Block Ciphers

- A huge number of block ciphers since AES (Present, TWINE, Piccolo, KATAN/KTANTAN, Prince, Simon/Speck, Camelia ...)
- Low power design has been widely studied
- Low energy $\Rightarrow$ Not so much
- Kerckhof et al (CHES 2012), Batina et al (RFIDSec 2013).

Power vs Energy

- Both are important lightweight design metrics
- Power is the rate of energy consumption
- Energy is the time integral of power

$$E = \int_t P \, dt$$

- Energy $\Rightarrow$ total electric work done by the system

Power vs Energy

- Designing for low power/energy can be quite different
- Example: Serial architectures for block ciphers
- Less hardware area leads to low power consumption
- More cycles for one encryption $\Rightarrow$ energy optimality NOT guaranteed.

How do you measure energy?

- In this presentation we focus on ASIC
- Pretty accurate simulators...
- ... if you use them properly (and you state what you did...)

How to Reduce Energy?

- Exploit technology
- Modify the architecture and the design goals
- Design having low energy in mind since the beginning

Contents

Exploit Technology

- Change Technology
- Clock Gating
- Power Gating

Change Technology

- More advanced node?
- Low power library?
- Low leakage library?

- Does it fit your constraints?

Clock Gating

- Pruning of the clock tree
- Reduce switching activity

- Does it fit your constraints?
- Is it really convenient?

Power Gating

- Switching off part of the circuit
- Fine grain? Coarse grain?

- Does it fit your constraints?
- Is it really convenient?

Contents

Let's Explore the Design Space of AES

- Frequency?
- Unrolling?
- S-box architecture?

Effect of Frequency

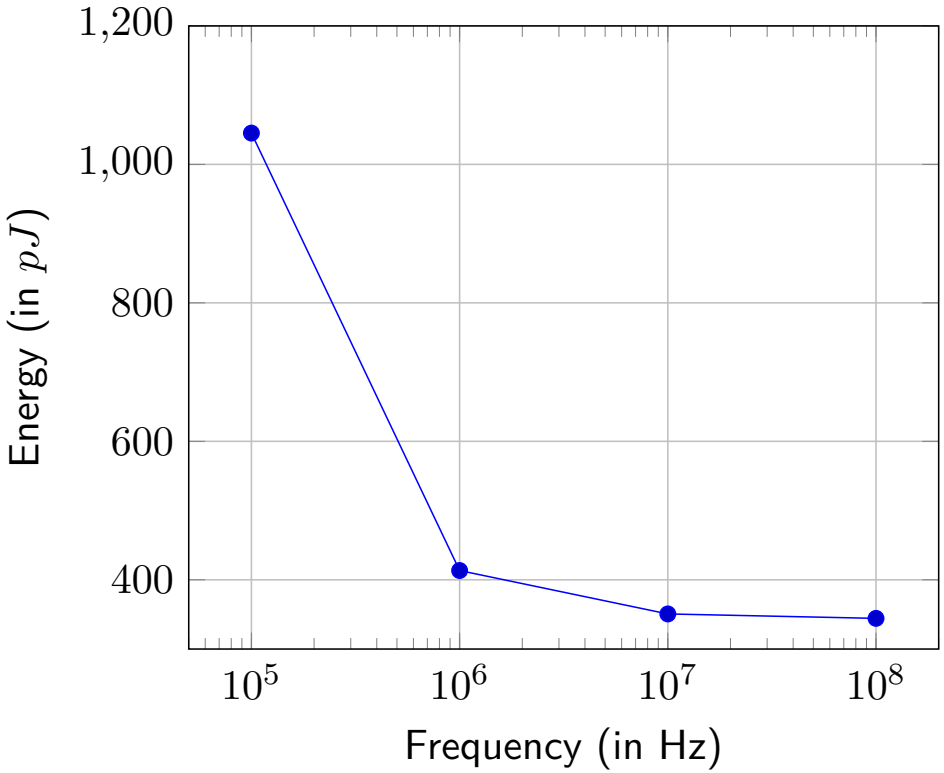


Figure: Energy consumption for round based `AES-128` vs clock frequency

Effect of Frequency

- Clock frequency: For low leakage process, not a factor at sufficiently high frequencies (upto $f_{max} = \frac{1}{\tau_{cr}}$).
- Role of design tool is minimal
- Same conclusion reached by Kerckchoff at al. (CHES 2012)

Energy Consumption: Case study AES-128

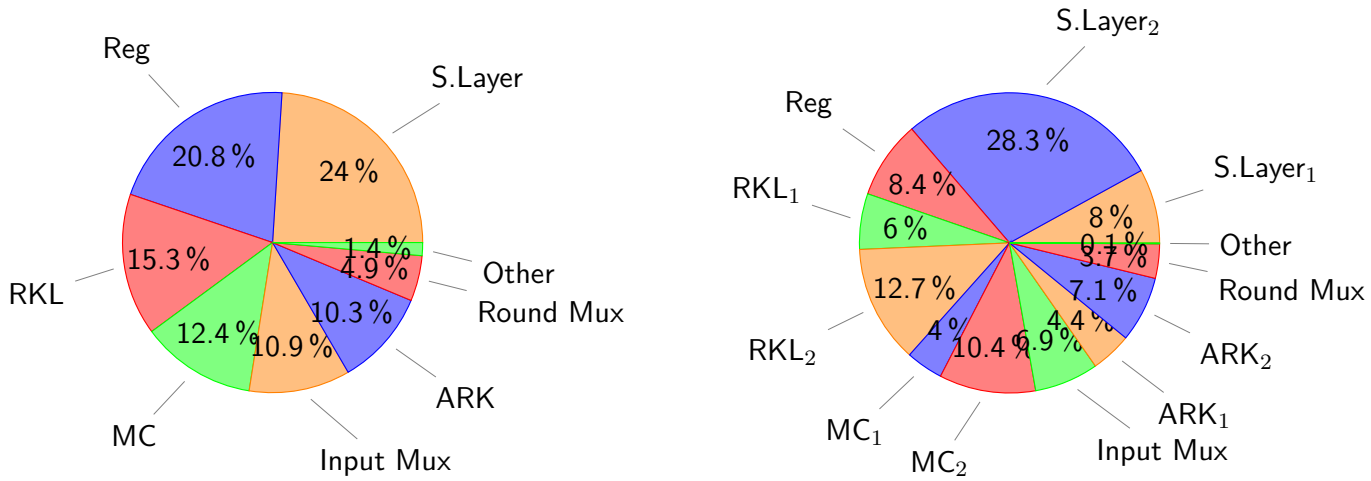
Serialization/Unrolling: Round Based clearly the best.

#	Design	Area(in GE)	#Cycles	Energy (pJ)	Energy/bit (pJ)
1	8-bit	2722.0	226	1913.1	14.94
2	32-bit (A_1)	4069.7	94	1123.3	8.77
	32-bit (A_2)	4061.8	54	819.2	6.40
	32-bit (A_3)	5528.4	44	801.7	6.26
3	64-bit (B_1)	6380.9	52	1018.7	7.96
	64-bit (B_2)	6362.6	32	869.8	6.79
	64-bit (B_3)	7747.5	22	616.2	4.81
4	Round based	12459.0	11	**350.7**	2.74
5	2-round	22842.3	6	593.6	4.64
6	3-round	32731.9	5	1043.0	8.15
7	4-round	43641.1	4	1416.5	11.07
8	5-round	53998.7	3	1634.4	12.77
9	10-round	101216.7	1	2129.5	16.64

Table: Area and Energy figures for different AES-128 architectures

Energy Consumption: Case study AES-128

Round Based vs 2-round unrolled.

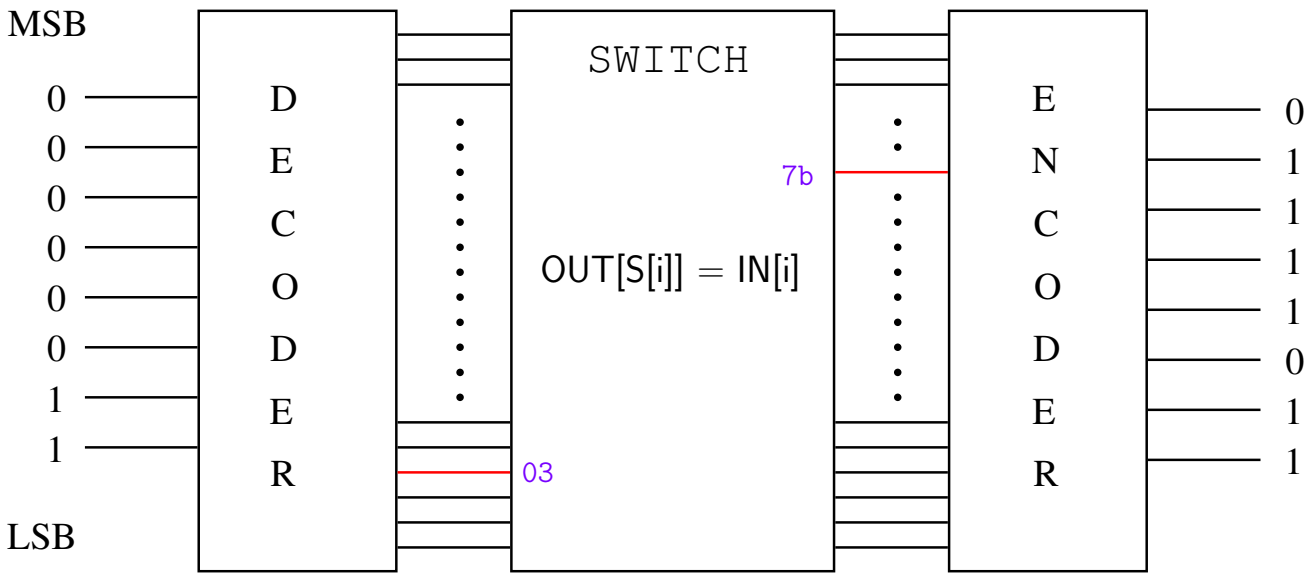


(a) Round based (b) 2-round unrolled

S.Layer: Substitution Layer	Reg: Registers	MC: MixColumn	ARK: Add Round Key	RKL: Round Key Logic

Figure: Energy shares for the Round based AES 128

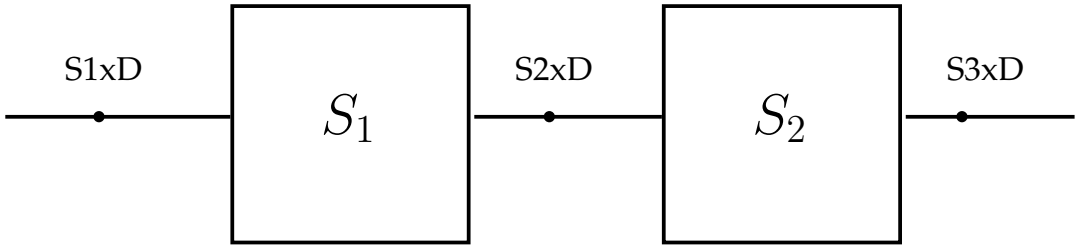
Exploring S-box Architectures



DSE S-box

- Decoder Switch Encoder
- Very little switching.
- One input bit flip $\Rightarrow$ 25% gates switch.
- Area $\approx$ 3.5 times Canright S-box.

Case Study: Two Rijndael S-Boxes



Total Time Range: 199742 - 204426 Page 1 of 1

#	Desig.	Signal	Value	Time: 199742 - 204426 X 1PS (C1: 2017812REF)
				200000 201000 202000 203000 204000
SG		Group 1		
001	Sim	S1xD [7:0]	8′hbb	70 bb
002	Sim	S2xD [7:0]	8′hea	51 e5 65 ea
003	Sim	S3xD [7:0]	8′h87	d1 6d ba 87

0 τ_d $2\tau_d$

S-Box Architectures Comparison

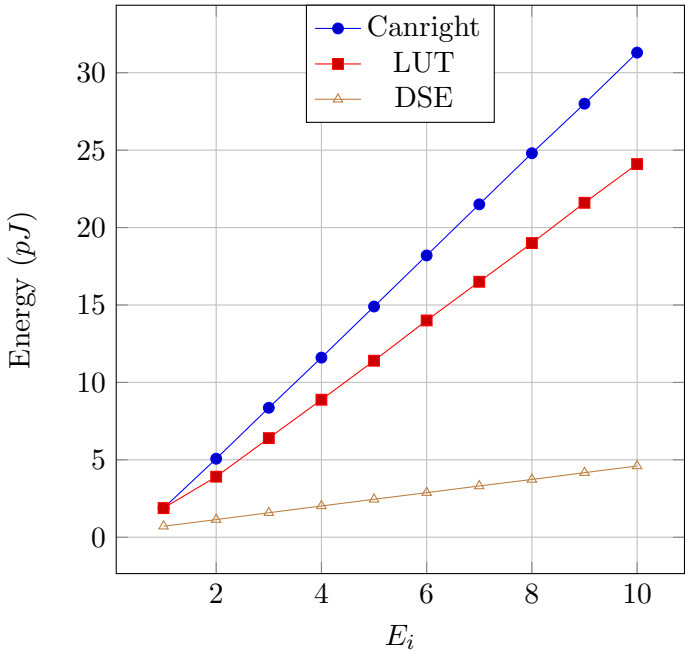


Figure: Energy per cycle E_i in i^{th} S-box S_i

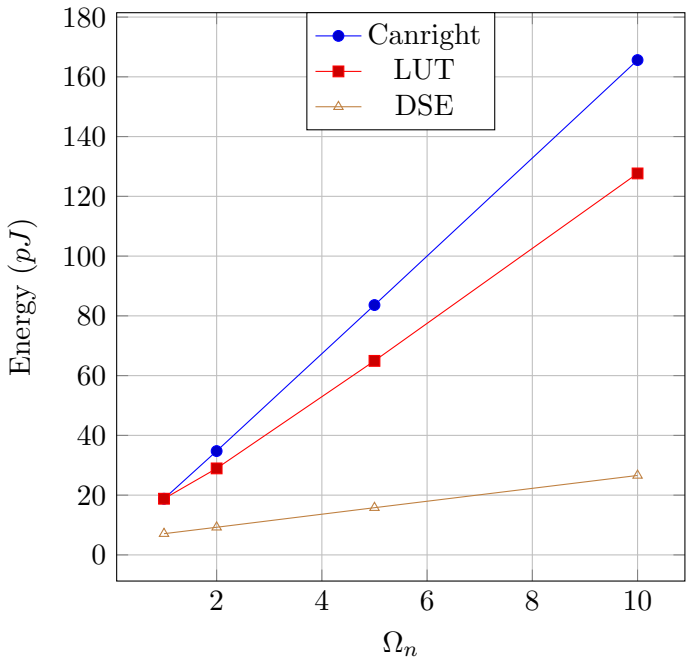
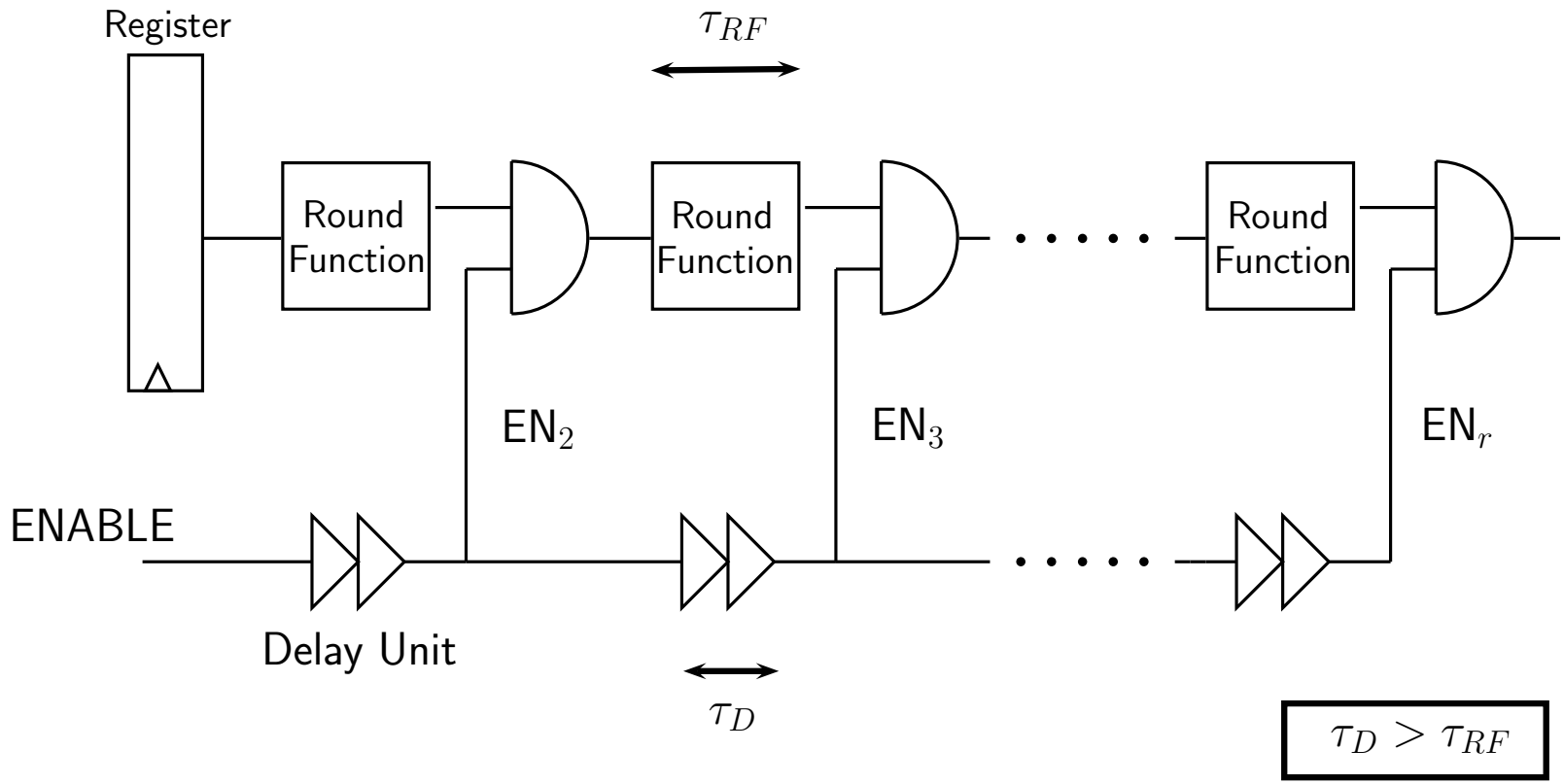


Figure: Energy Ω_n required to compute $S^{10}(x)$ using n S-boxes

Delays

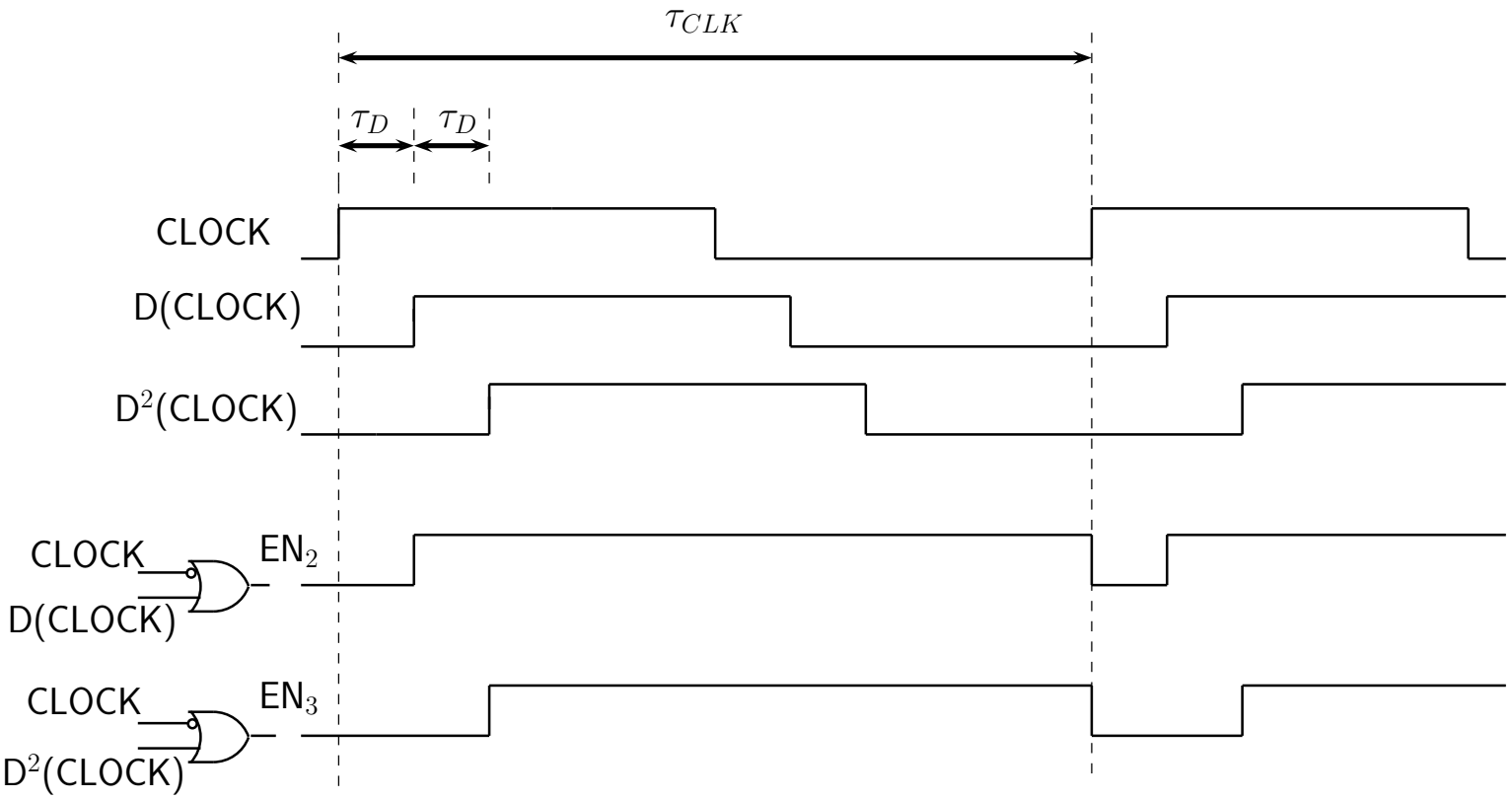
- Canright: 2.9 ns
- LUT : 2.1 ns
- DSE: 2.3 ns

The Idea of Round Gating



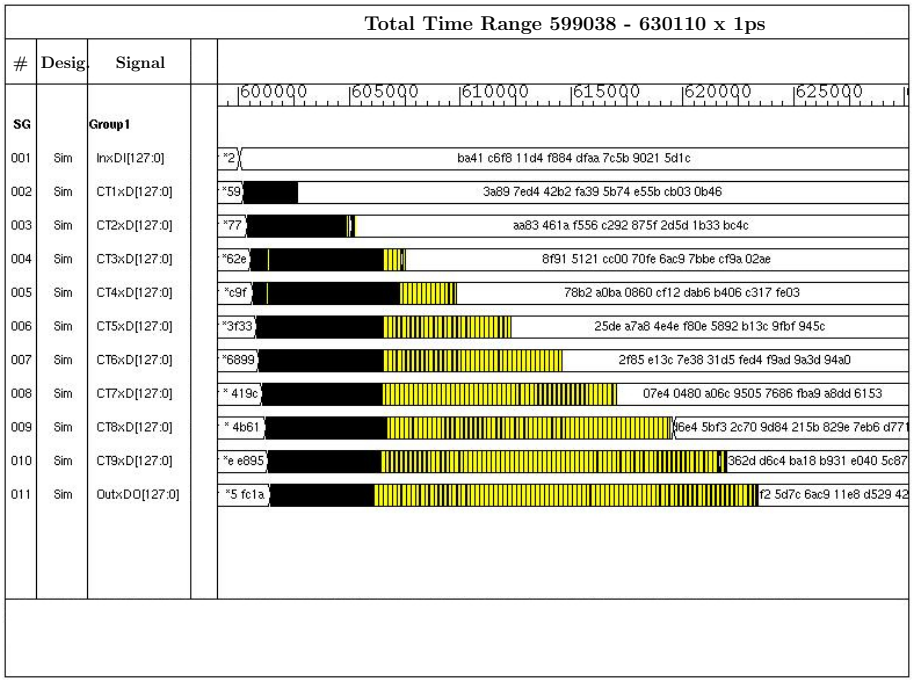
- Construct a delay unit with delay $\tau_D > \tau_{RF}$ i.e. the delay in round function.
- The ENABLE signal is transmitted through a chain of delay units.
- The AND gate is active only when ENABLE is High after τ_D seconds.
- RF$_{i+1}$ gets input only when output of RF$_i$ has become stable.

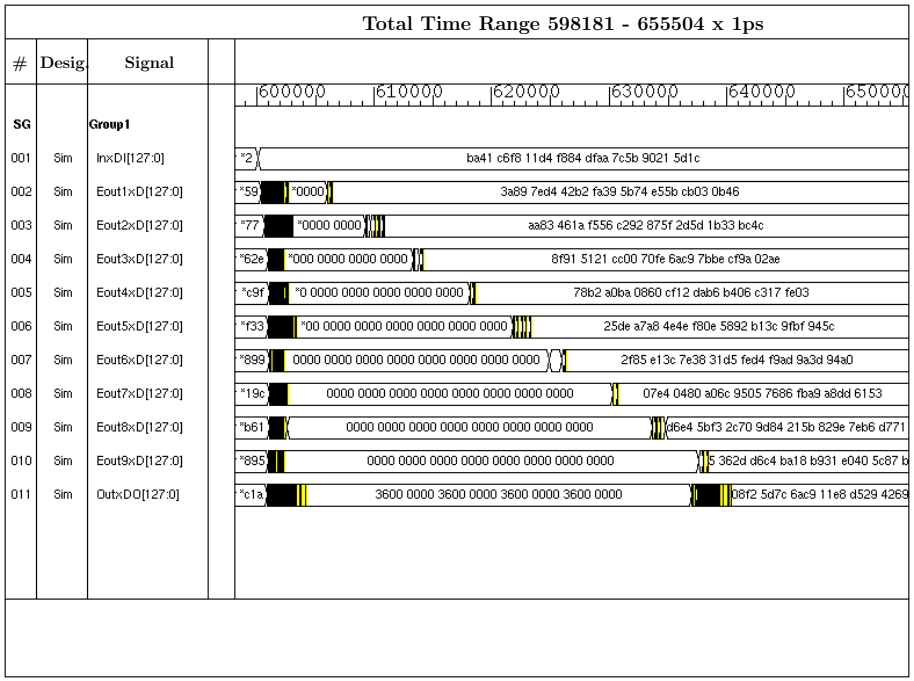
Implementation



- The EN_i signals are constructed by a network of OR gates.
- The delay units are made of buffers.

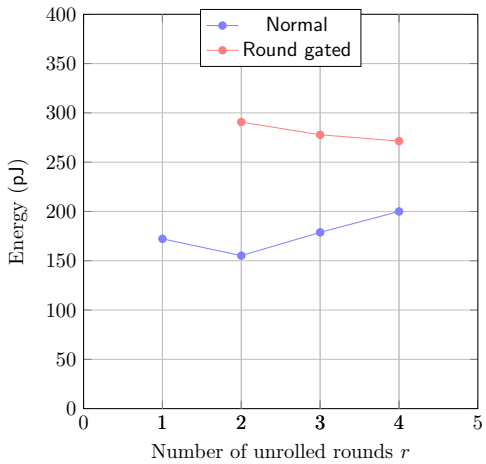
Snapshot for Unrolled AES Circuit (10 Rounds)



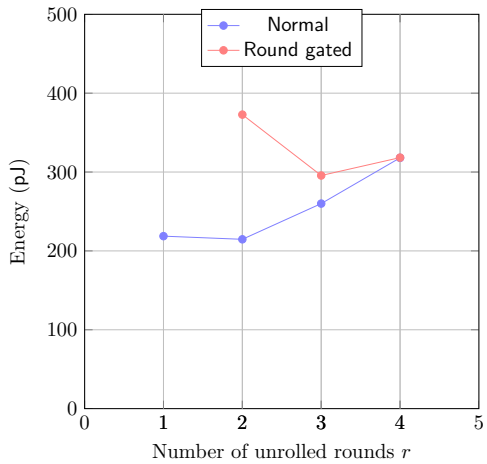


- Waveforms for the fully unrolled AES-128 circuit (normal and roundgated)
- The waveforms listed are the output signals of each successive round function
- With round gating, compounding of switching is prevented

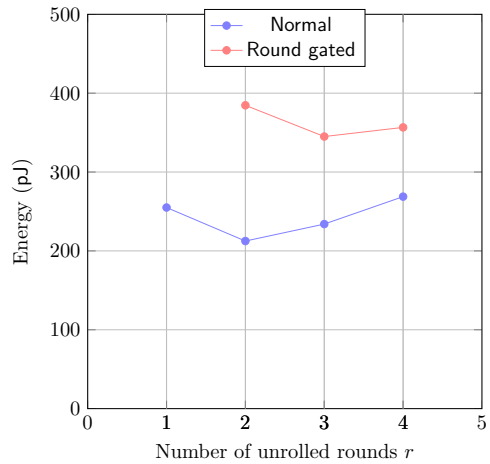
Experimental Results for $1 \leq r \leq 4$



(a) Present



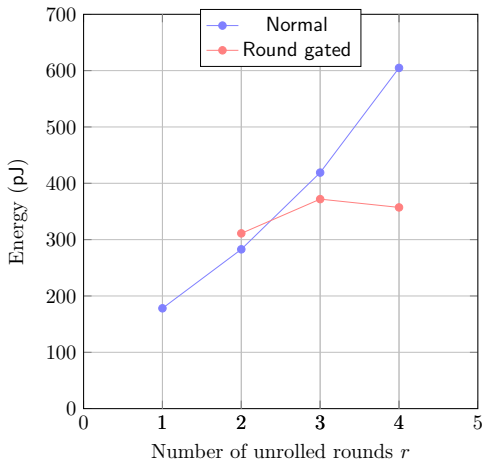
(b) TWINE



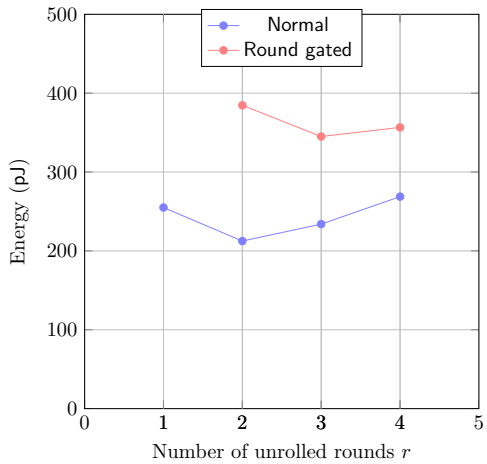
(c) Simon 64/96

Figure: Normal and Round Gated Energy consumptions

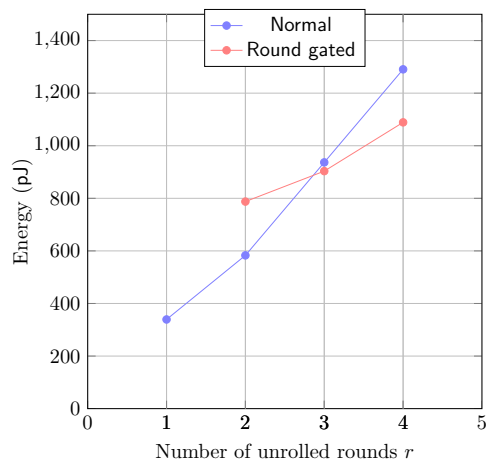
Experimental Results for $1 \leq r \leq 4$



(a) Piccolo



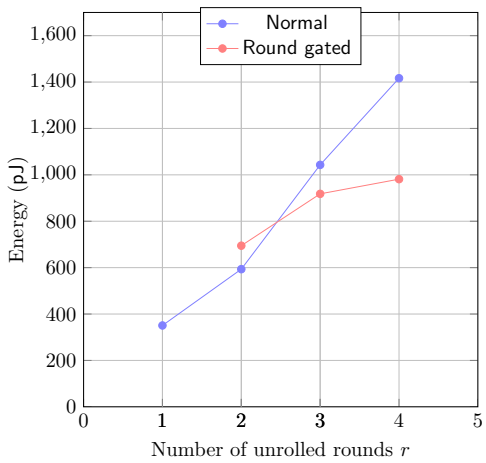
(b) LED 128



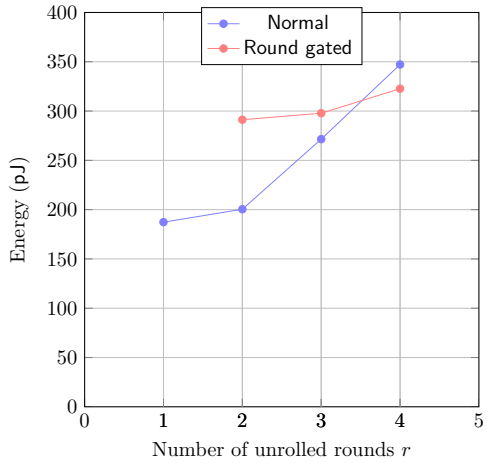
(c) Noekeon

Figure: Normal and Round Gated Energy consumptions

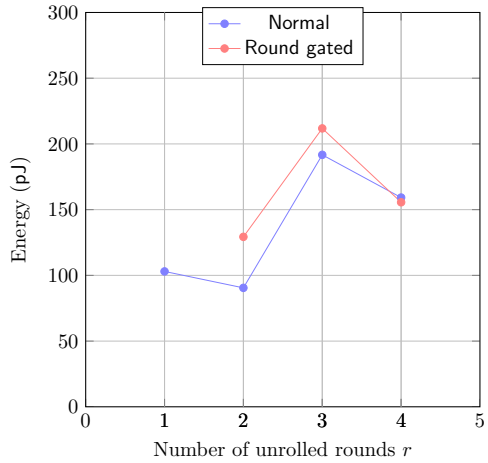
Experimental Results for $1 \leq r \leq 4$



(a) AES-128



(b) Midori 128



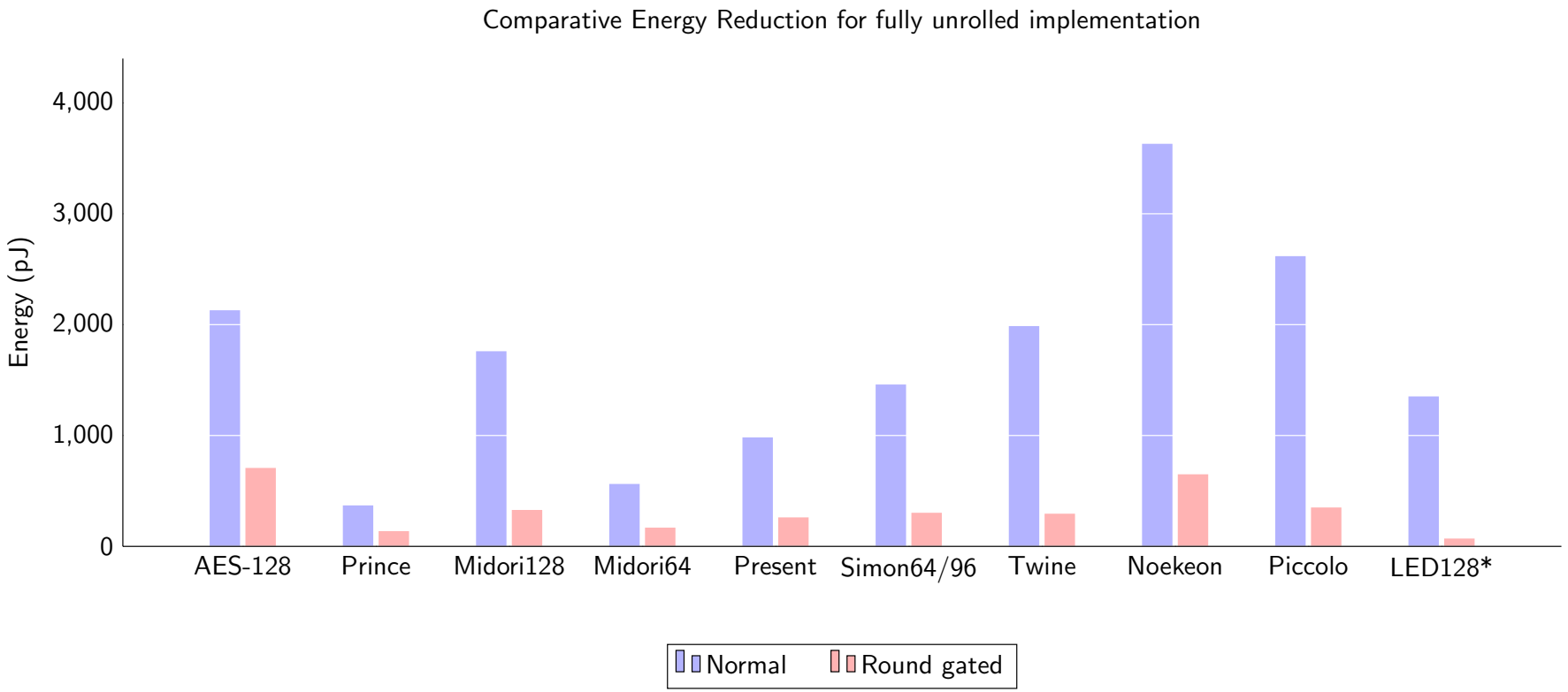
(c) Midori 64

Figure: Normal and Round Gated Energy consumptions

Comparison of fully unrolled circuits for various ciphers

#	Cipher	Blocksize/ Keysize	**Area(GE)**			**Total Energy (pJ)**			**Latency (ns)**	
			Normal	Round gated	% Change	Normal	Round gated	% Change	Normal	Round gated
1	AES-128	128/128	101217	105931	+4.7%	2129.5	707.7	-66.8%	28.5	54.3
2	Noekeon	128/128	24538	27113	+10.5%	3631.2	650.0	-82.1%	35.5	57.7
3	Midori128	128/128	21647	24109	+11.4%	1760.1	328.5	-81.3%	18.8	37.9
4	Midori64	64/128	8416	9612	+14.2%	563.1	168.9	-70.0%	14.4	30.9
5	LED 128	64/128	47257	52161	+10.4%	13526.5	705.8	-94.8%	121.3	229.3
6	Prince	64/128	7729	8567	+10.8%	369.5	137.3	-62.8%	11.5	22.0
7	Present	64/80	16036	20596	+28.4%	982.8	261.4	-73.4%	20.2	43.8
8	Piccolo	64/80	16132	18707	+16.0%	2617.7	350.7	-86.6%	45.1	88.0
9	Twine	64/80	15399	21260	+38.1%	1987.3	294.6	-85.2%	43.1	75.6
10	Simon 64/96	64/96	18403	25568	+38.9%	1459.9	282.0	-80.7%	15.6	37.8

Energy reduction for fully unrolled circuits



Take Home from Round Gating

Tradeoff on r

- For lower degrees of unrolling ($1 \leq r \leq 4$):
  - Round gating not always beneficial
  - The round gating circuit itself consumes some energy
  - For ciphers like PRESENT incremental switching is negligible
  - Hence round gating does more harm than good
- For higher degrees of unrolling/ fully unrolled designs
  - Round gating is always beneficial
  - Huge energy savings (over 60 %) with only minimal additional hardware
  - Latency approximately doubles

Contents

Take home from Exploration on AES

- Low delay $\Rightarrow$ Low switching activity
- Low delay of S. layer $\Rightarrow$ low energy of subsequent layers
- Multiple round unrolling $\Rightarrow$ unlikely to be energy-efficient
- Exceptions: `PRESENT`, `TWINE`
  $\rightarrow$ Low delay round functions: 2-round unrolled is best

Further exploration: 4-bit S-Box vs 8-bit S-Box

Table: A comparison of energy per cycle for round functions constructed with (A) 16 8-bit S-boxes, (B) 32 4-bit S-boxes.

	S-box	Delay in S (ns)	Energy per cycle (pJ)
A	DSE (8-bit)	2.25	14.00
	Rijndael(LUT)	2.10	38.88
	`mCrypton`	1.59	13.20
	`Whirlpool`	1.33	16.38
B	DSE (4-bit)	0.81	7.92
	`PRINCE`	0.36	4.87
	`PRESENT`	0.45	6.18

4-bit S-Box vs 8-bit S-Box

- 8-bit S-Box $\Rightarrow$ higher signal delay $\Rightarrow$ more energy
- DSE not optimal for a) 4-bit S-Box, b) simpler 8-bit S-Boxes
- Tradeoff $\Rightarrow$ 4-bit S-Box requires more rounds

Other Parameters

- SPN vs Feistel
  - → Feistel constructions apply round function to half the state
  - → Twice the # rounds for security margin → bad for energy
- Same argument for complex vs simple round function
- Key schedule: to or not to include
  - → Consumes 25% of energy in AES and 32% in PRESENT
  - → Undesirable for energy conservation

Main Decisions

- Round based architecture

  $\rightarrow$ Added motivation: ENC/DEC functionality easily available

  $\rightarrow$ `PRINCE` does not have an efficient round based circuit.

- Low delay, lightweight round function (involutive)

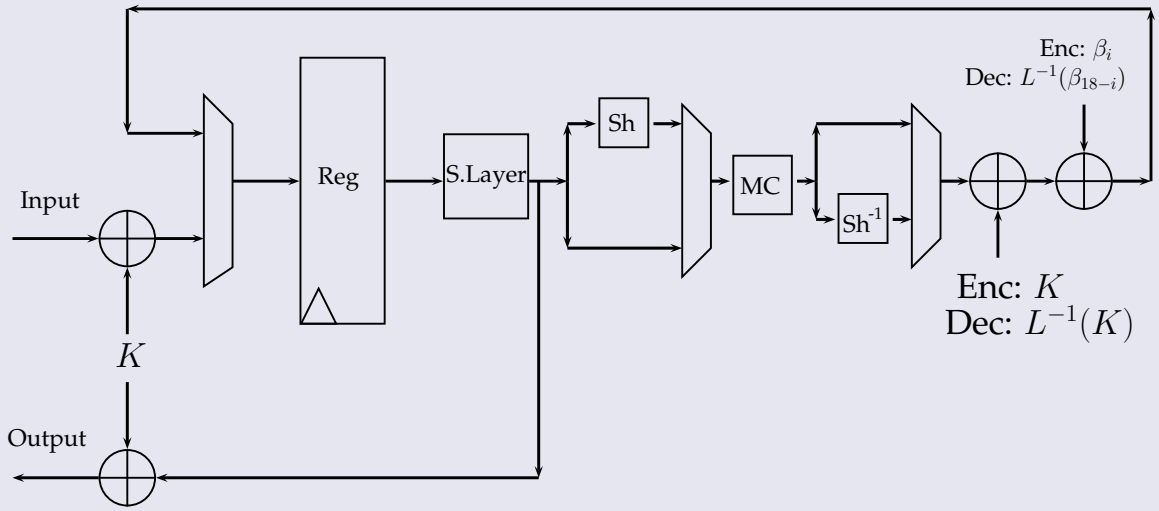
  $\rightarrow$ 4-bit S-box, optimal Linear Layer

- Smaller number of rounds

  $\rightarrow$ SPN architecture seems better

- No Key schedule

Midori Implementation



Simulation Results

Standard Cell library based on STM 90nm logic process

#	Cipher	Block Size	Architecture	Area (in GE)	Energy pJ	Energy/bit pJ	Average Power (μW)	Critical Path (ns)
1	AES	128	ED	21274	769.0	6.01	699.1	4.08
			E	12459	350.7	2.74	318.8	3.32
2	NOEKEON	128	ED	3439	331.5	2.59	184.2	3.79
			E	2284	338.0	2.64	187.8	3.38
3	SIMON 128/128	128	ED	3480	855.6	6.68	124.0	2.67
			E	2420	664.1	5.19	96.2	2.66
4	Midori128	128	ED	3661	228.3	1.78	108.7	2.44
			E	2522	187.3	1.46	89.2	2.25
5	PRESENT	64	ED	2186	250.2	3.91	75.8	2.32
			E	1440	172.3	2.69	52.2	2.09
6	PRINCE	64	ED	2650	146.3	2.29	112.5	4.09
			E	2286	144.7	2.26	111.3	4.06
7	Midori64	64	ED	2450	121.0	1.89	71.2	2.12
			E	1542	103.0	1.61	60.6	2.06

Energy vs Cumulative latency

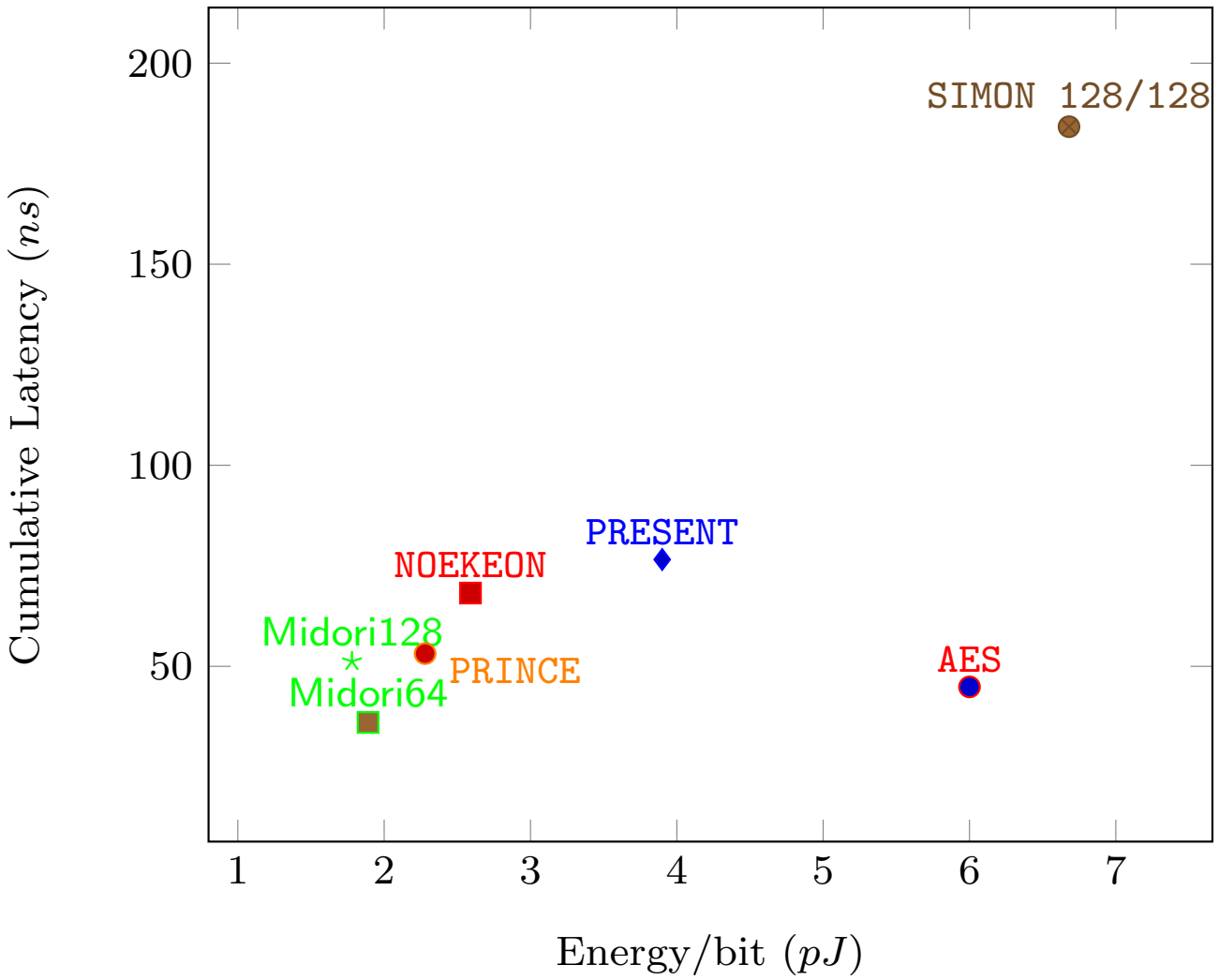


Figure: Cumulative Latency vs Energy/bit figures

Closing thoughts

- Is it meaningful in other platforms?
- Fairness of comparison!

Conclusions

- Energy is (going to be) a crucial design parameter for cryptography
- Low Energy can be achieved acting at several level of the design flow
- Know the needs of your target applications to identify the best approach

Questions?

Thank you for your attention!

Subhadeep Banik, Andrey Bogdanov, Francesco Regazzoni