Round Gating for Low Energy Block Ciphers

Subhadeep Banik, **Andrey Bogdanov**

DTU Compute, Technical University of Denmark, Lyngby, Denmark

Francesco Regazzoni

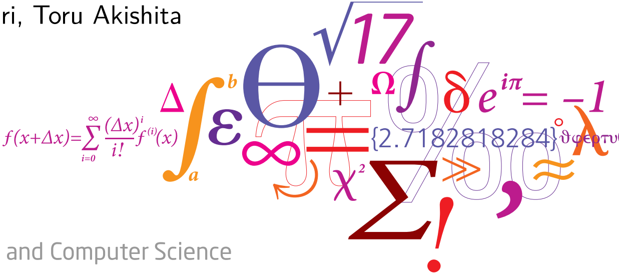
ALARI, University of Lugano, Switzerland

Takanori Isobe, Harunaga Hiwatari, Toru Akishita

Sony Corporation, Japan

IEEE HOST 2016

McLean, VA



DTU Compute

Department of Applied Mathematics and Computer Science

Outline

- Preliminaries
- AES-128: A Case Study
- CMOS Energy Consumption Model
- Round Gating
- Conclusion

Lightweight Block Ciphers

State of the Art

- Numerous block ciphers since AES
- E.g.: Present, TWINE, Piccolo, KATAN, Prince. Simon/Speck, ...
- Low area and low power designs widely studied
- Low energy ⇒ largely unexplored
- Kerckhof et al (CHES 2012), Batina et al (RFIDSec 2013)

Power vs Energy

Power and 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 ⇒ total electric work done by the system

Tradeoffs

- Designing for low power/energy can be quite different
- Example: serial architectures for block ciphers
- In general, lower hardware area implies lower power consumption
- More cycles per encryption ⇒ energy optimality NOT guaranteed

AES-128: A Case Study

Effect of Frequency

Frequency Dependence

- $P_{dyn} \propto Freq \Rightarrow P_{dyn} = \frac{CONST}{T} \Rightarrow E_{dyn} = P_{dyn}T = CONST$
- $E_{stat} = \int_T P_{stat}\, dt$

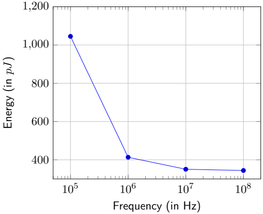


Figure: Energy consumption for round-based AES-128 vs Clock frequency

Not Surprising

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

Energy Consumption: Case Study AES-128

Observation

- Serialization/Unrolling: Round-based designs are clearly 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

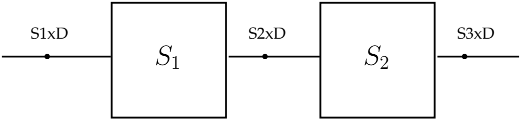
Energy in CMOS gates

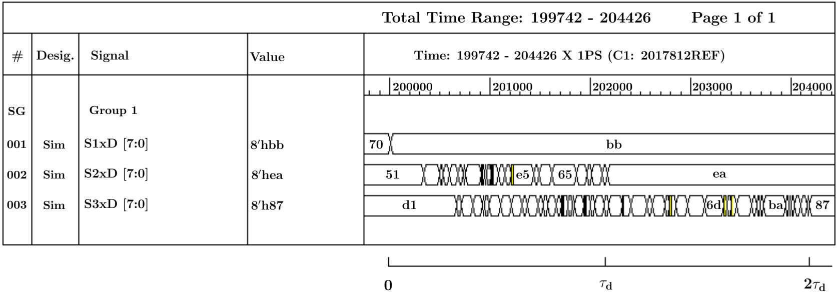
- Two major sources of power in CMOS circuits:
  - **Dynamic dissipation due to the charging and discharging of load capacitances.**
  - Static dissipation due to leakage current and other current drawn continuously from the power supply.
- In a given time interval, if the cell makes n transitions, then

Observation

$$E_{dyn} = E \cdot n = \left(\frac{1}{2} C_L V_{DD}^2 + E_{int} \right) \cdot n$$

Case Study: Two `Rijndael` S-Boxes





Total Time Range: 199742 - 204426 Page 1 of 1

#	Desig.	Signal	Value
SG		Group 1	
001	Sim	S1xD [7:0]	8′hbb
002	Sim	S2xD [7:0]	8′hea
003	Sim	S3xD [7:0]	8′h87

Time: 199742 - 204426 X 1PS (C1: 2017812REF)

Case Study: n Rijndael S-Boxes

- If we place n Rijndael S-Boxes sequentially: $E_1, E_2, E_3, \ldots$ is an arithmetic sequence.

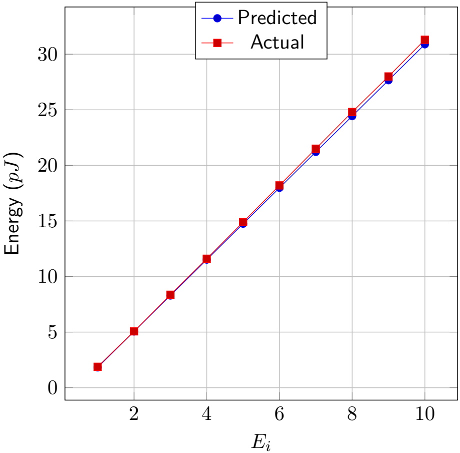


Figure: Actual and Predicted Energy consumptions per cycle E_i

Energy Model: Iterated Block Ciphers

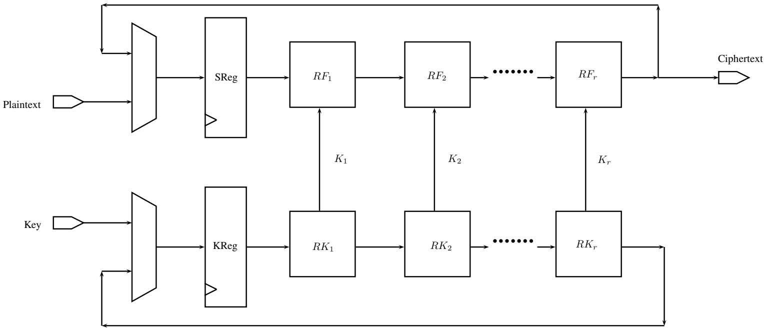


Figure: Block Cipher Architecture

Energy consumptions

- Energy consumed in each of the RF_i and RK_i blocks is in arithmetic progression.
- If there are R rounds in the algorithm, encryption in $1 + \lceil \frac{R}{r} \rceil$ rounds.

Energy Model: Iterated Block Ciphers

Total Energy per encryption

- Energy consumption per encryption: shown in Banik et al. (SAC 2015)

$$\mathbf{E}_r = E_r \cdot \left(1 + \left\lceil \frac{R}{r} \right\rceil\right) = (Ar^2 + Br + C) \cdot \left(1 + \left\lceil \frac{R}{r} \right\rceil\right)$$

- For ”light" round functions like PRESENT, TWINE, SIMON, MIDORI $r = 2$ is the optimal configuration
- For “heavy" round functions like AES, LED, PICCOLO, NOEKEON $r = 1$ is optimal

Block Ciphers: Best Energy Configuration

Tradeoff on r

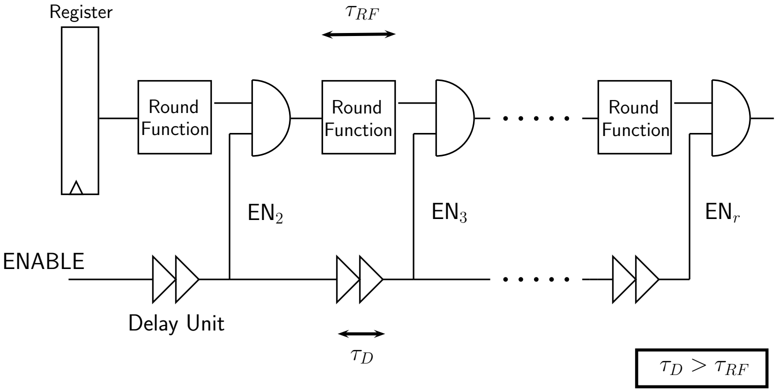
- Suitable value of r ?
- High r
  - Low latency: Critical in e.g. memory encryption
  - Lower energy required to update registers
  - More energy in later rounds due to compounding switching activity
- Low r
  - Lower energy consumed per cycle
  - Avoids compounding switching activity in later rounds
  - High latency!

The Idea of Round Gating

Round Gating

- For high r (unrolled designs): compounding switching of transient signals across round functions
- Primarily responsible for high energy consumption.
- What if transients are limited to one round?
- The idea is to present the output of RF_i to the input of RF_{i+1} only when the signal has stabilized
- Can lead to substantial energy savings for unrolled low-latency designs!

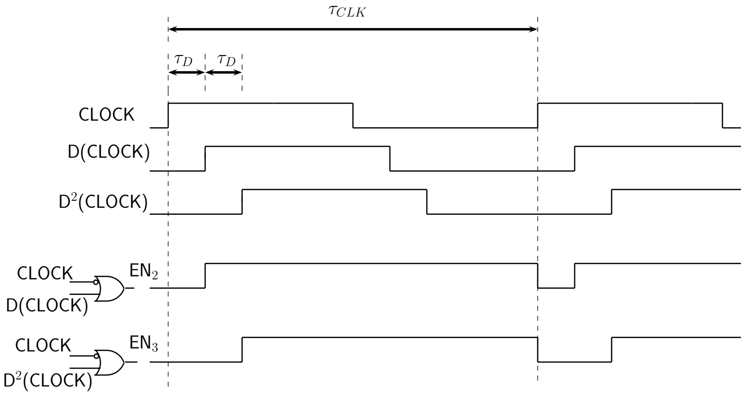
The Idea of Round Gating



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.

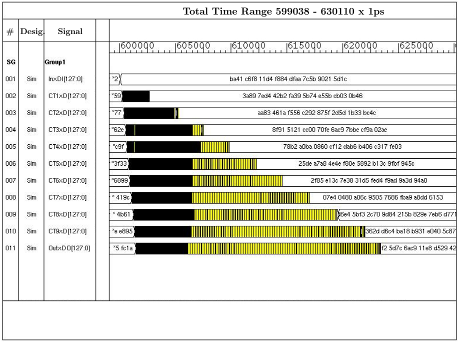
Implementation



Round Gating

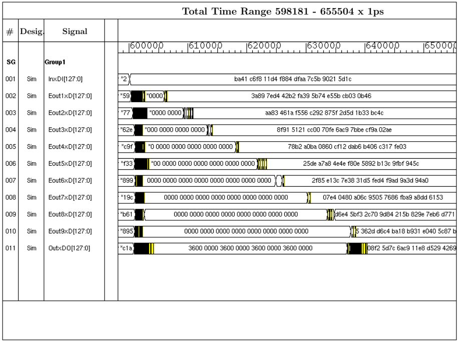
- The EN_i signals are constructed by a network of OR gates.
- The delay units made of buffers.

Snapshot for Unrolled AES Circuit (10 Rounds)



Total Time Range 599038 - 630110 x 1ps

#	Desig.	Signal	
SG		Group1	
001	Sim	InxDI[127:0]	*2 ba41 c6f8 11d4 f884 dfaa 7c5b 9021 5d1c
002	Sim	CT1xD[127:0]	*59 3a89 7ed4 42b2 fa39 5b74 e55b cb03 0b46
003	Sim	CT2xD[127:0]	*77 aa83 461a f556 c292 875f 2d5d 1b33 bc4c
004	Sim	CT3xD[127:0]	*62e 8f91 5121 cc00 70fe 6ac9 7bbe cf9a 02ae
005	Sim	CT4xD[127:0]	*c9f 78b2 a0ba 0860 cf12 dab6 b406 c317 fe03
006	Sim	CT5xD[127:0]	*3f33 25de a7a8 4e4e f80e 5892 b13c 9fbf 945c
007	Sim	CT6xD[127:0]	*6899 2f85 e13c 7e38 31d5 fed4 f9ad 9a3d 94a0
008	Sim	CT7xD[127:0]	* 419c 07e4 0480 a06c 9505 7686 fba9 a8dd 6153
009	Sim	CT8xD[127:0]	* 4b61 d6e4 5bf3 2c70 9d84 215b 829e 7eb6 d771
010	Sim	CT9xD[127:0]	*e e895 362d d6c4 ba18 b931 e040 5c87
011	Sim	OutxDO[127:0]	*5 fc1a f2 5d7c 6ac9 11e8 d529 42



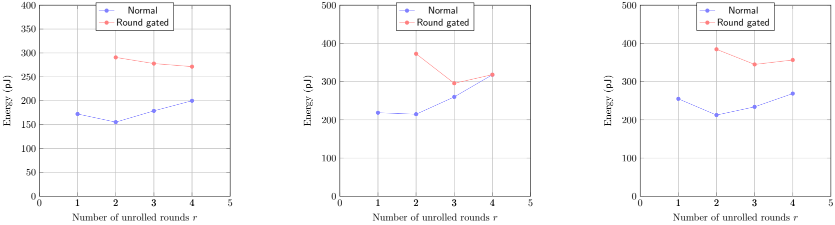
Total Time Range 598181 - 655504 x 1ps

#	Desig.	Signal	
SG		Group1	
001	Sim	InxDI[127:0]	*2 ba41 c6f8 11d4 f884 dfaa 7c5b 9021 5d1c
002	Sim	Eout1xD[127:0]	*59 *0000 3a89 7ed4 42b2 fa39 5b74 e55b cb03 0b46
003	Sim	Eout2xD[127:0]	*77 *0000 0000 aa83 461a f556 c292 875f 2d5d 1b33 bc4c
004	Sim	Eout3xD[127:0]	*62e *000 0000 0000 0000 8f91 5121 cc00 70fe 6ac9 7bbe cf9a 02ae
005	Sim	Eout4xD[127:0]	*c9f *0 0000 0000 0000 0000 0000 78b2 a0ba 0860 cf12 dab6 b406 c317 fe03
006	Sim	Eout5xD[127:0]	*f33 *00 0000 0000 0000 0000 0000 0000 25de a7a8 4e4e f80e 5892 b13c 9fbf 945c
007	Sim	Eout6xD[127:0]	*899 0000 0000 0000 0000 0000 0000 0000 0000 2f85 e13c 7e38 31d5 fed4 f9ad 9a3d 94a0
008	Sim	Eout7xD[127:0]	*19c 0000 0000 0000 0000 0000 0000 0000 0000 07e4 0480 a06c 9505 7686 fba9 a8dd 6153
009	Sim	Eout8xD[127:0]	*b61 0000 0000 0000 0000 0000 0000 0000 0000 d6e4 5bf3 2c70 9d84 215b 829e 7eb6 d771
010	Sim	Eout9xD[127:0]	*895 0000 0000 0000 0000 0000 0000 0000 0000 5 362d d6c4 ba18 b931 e040 5c87 b
011	Sim	OutxDO[127:0]	*c1a 3600 0000 3600 0000 3600 0000 3600 0000 08f2 5d7c 6ac9 11e8 d529 4269

Round Gating

- 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 $1 \leq r \leq 4$



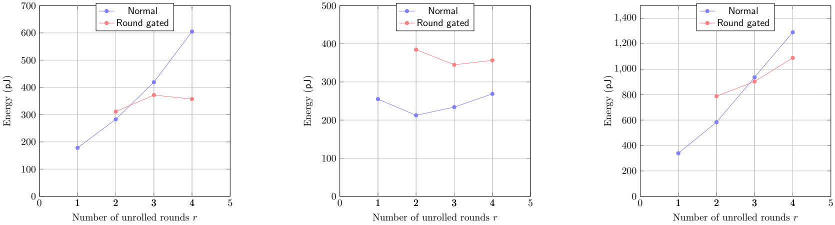
(a) Present

(b) TWINE

(c) Simon 64/96

Figure: Normal and Round Gated Energy consumptions

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



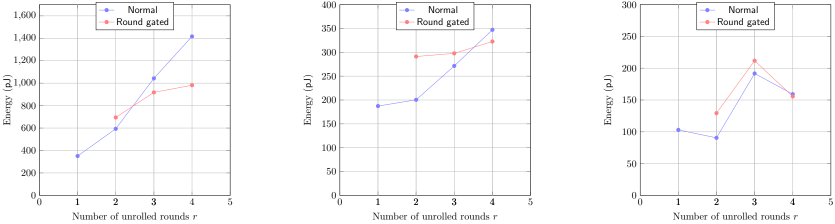
(a) Piccolo

(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

Conclusions

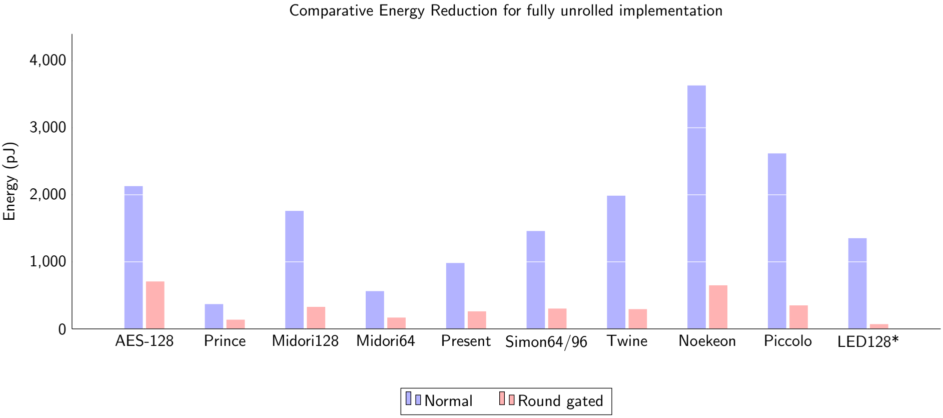
Tradeoff on r

- 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

Comparison of fully unrolled circuits for various ciphers

#	Cipher	Blocksize/	**Area(GE)**			**Total Energy** (pJ)			**Latency** (ns)	
		Keysize	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



Some Inferences

Energy optimality

- Signal delay across round ⇒ more switching activity in later rounds
  - So, $r = 1, 2$ usually the optimal energy configuration
- However higher r may be required in specific applications (eg. low delay memory encryption)
- Simpler round functions tend to have smaller signal delay
- Eg: Present, TWINE, Simon 64/96
- For low r, round gating does not improve energy performance

For fully unrolled ciphers

- Round gating is highly effective
- Substantial energy savings with minimal hardware overhead

THANK YOU