Energy Evaluation of AES based Authenticated Encryption Algorithms (Online + NMR)

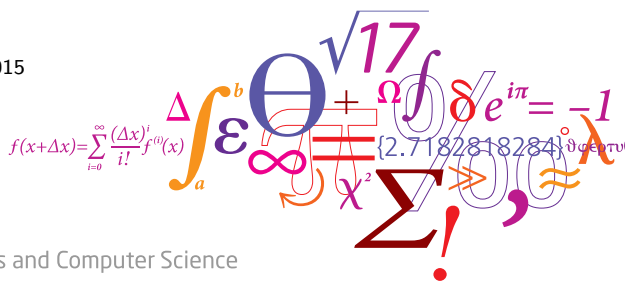
Subhadeep Banik[1], Andrey Bogdanov[1], Francesco Regazzoni[2]

[1] DTU Compute, Technical University of Denmark, Lyngby

[2] ALARI, USI

Directions in Authenticated Ciphers 2015

Singapore



DTU Compute

Department of Applied Mathematics and Computer Science

Outline

- Preliminaries
- AES - Some recent work (Banik et al SAC 2015)
- AES-COPA
- ELmD
- POET
- Conclusion

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 $\Rightarrow$ Total Electric work done by the Battery source.

Tradeoffs

- 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.

AES : Popular choice

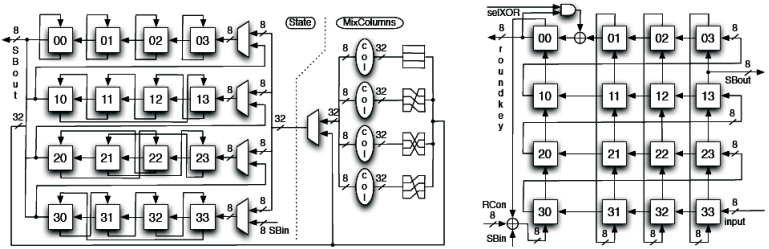


Figure : Lightweight AES

Caesar Candidates

- AES is a popular choice for the underlying block cipher.
- 15 out of 29 Candidates recommend AES.
- We analyze AES-COPA, ELmD and POET.
- All of the above are Nonce Misuse resistant and Online modes.

Energy Optimization I

Some factors affecting energy

- Clock Frequency — Power consumed directly varies with frequency.
- Architecture — Ex: S-Box architecture
  - Canright architecture (smallest)
  - LUT architecture (fastest)
  - DSE (Decoder Switch Encode) architecture

  MixColumns architecture
  - 152 gates
  - 108 gates (Satoh et al. Asiacrypt 2001)
- Serialization — Less power consumed but more cycles taken.
- Unrolling — More power consumed but less cycles taken.

Begin with AES 128

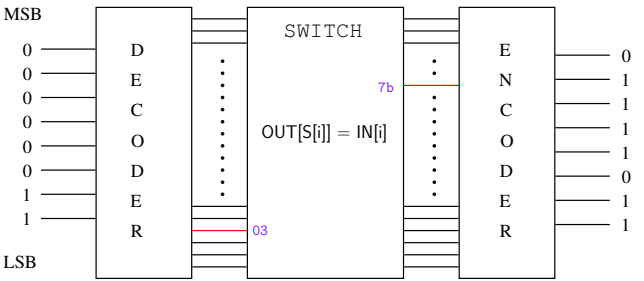
#	S-Box	MixColumn	Area(in GE)	Energy (in pJ)	Energy/bit (in pJ)
1	LUT	152 gates	13836.2	797.2	6.23
2	LUT	108 gates	13647.9	755.3	5.90
3	Canright	152 gates	8127.9	753.6	5.89
4	Canright	108 gates	7872.5	708.5	5.53
5	DSE	152 gates	12601.7	377.5	2.95
6	DSE	108 gates	12459.0	**350.7**	2.74

Table : Area, Energy figures for Round Based AES 128

Salient points

- Circuit implemented with Standard cell library of the 90 nm STM process.
- Operating Frequency : 10 MHz.
- DSE S-Box, 108 gate MixColumns best Energywise !!!

DSE S-box



DSE S-box

- Minimal energy consumption due to very little switching.
- One input bit flip $\Rightarrow$ 25% gates switch.
- Area $\approx$ 3.5 times Canright S-box.

Effect of Frequency

Frequency Dependence

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

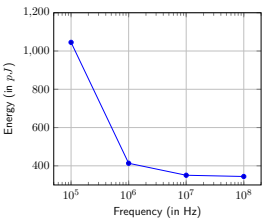


Figure : Energy consumption for Round Based AES-128 vs Clock frequency

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

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

Midori- A Block cipher for Low Energy [ASIACRYPT 15]

Midori 64/128

- Midori - Japanese word for green.
- Designed by Banik, Bogdanov, Isobe, Shibutani, Hiwatari, Akishita, Regazzoni.
- Optimized with respect to ENERGY.
- Encryption + Decryption with minimal overhead.
- SPN cipher : 4-bit Sbox, AMDS matrix, 64/128 bit blocksize.

Benchmarks

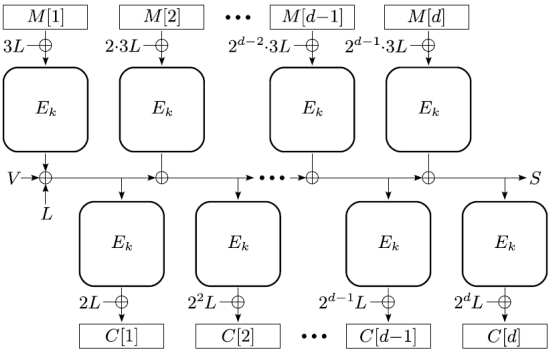
- Round based AES circuit is used in all constructions.
- We use Std cell library of STM 90nm process.
- Frequency fixed at 10 MHz, to minimize leakage.
- Energy is calulated for processing the empty AD and 16 Plaintext blocks.
- For the time being only Encryption+Tag generation is considered.

Overview of Results

#	Mode	Area (in GE)	#Cycles (16 PT Blocks)	Energy (nJ)	Energy/bit (pJ)
1	AES-COPA	18746	380	18.24	8.9
2	ELmD [1]	28294	379	39.01	19.05
	ELmD [2]	32355		24.44	11.93
3	POET	19918	400	27.88	13.62

Table : Energy consumptions for AES-COPA, ELmD, POET modes

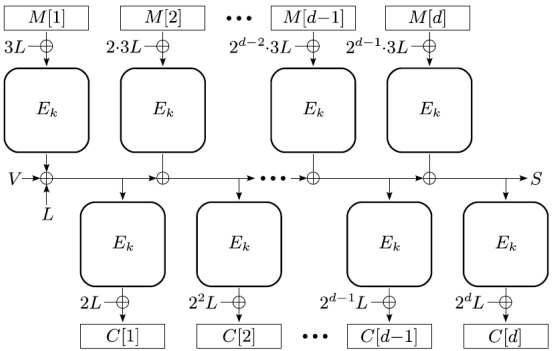
AES-COPA



AES-COPA

- Andreeva et al ASIACRYPT 2013.
- Two Block cipher calls per Plaintext block.
- Multiplication by $2, 3$ in $GF(2^{128})$.

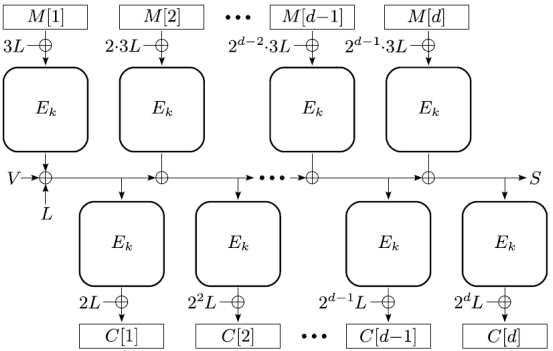
AES-COPA



Analysis

- Three extra registers required: L, ACC, V.
- Seems to be energy efficient.
- Other than AES core, Mult by 3, few Xors, not many power hungry modules.

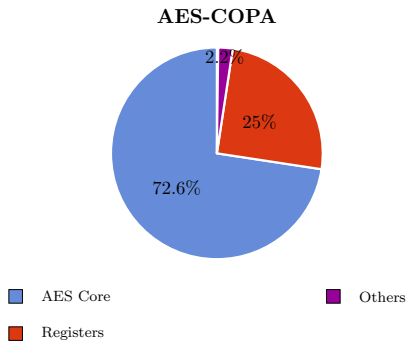
AES-COPA



Analysis

- Initial value generation : 23 cycles (2 ENC + 1 MULT).
- Thereafter every plaintext block takes 21 cycles (2 ENC calls).
- TAG takes another 21 cycles (2 ENC): Total 380 cycles for 16 Plaintext blocks.

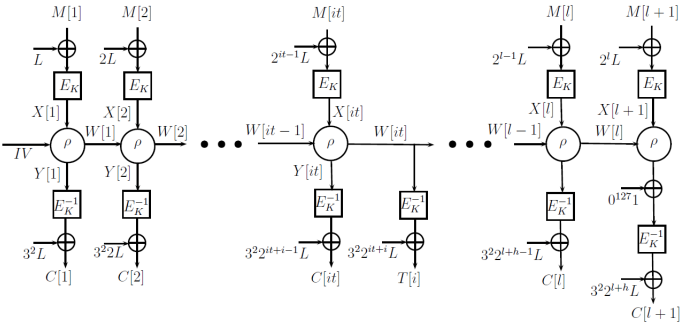
AES-COPA



Analysis

- Total Area of 18746 Gates.
- Total of 18.24 nJ for 16 Plaintext blocks (8.9 pJ/bit).
- AES core is the most power hungry module.

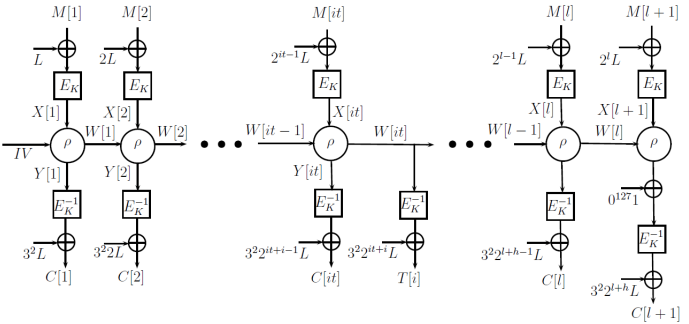
ELmD



ELmD

- Proposed by Datta/Nandi.
- Uses 1 Encryption+ 1 Decryption call per Plaintext block.
- Multiplication by $2, 3$ in $GF(2^{128})$.

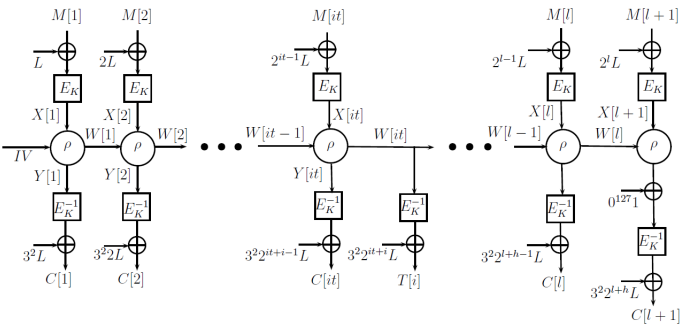
ELmD



Design similar to AES-COPA

- Three extra registers required: L, ACC, V.
- Additional Linear mix function uses (2 XOR+ 1 MULT3 + 1MULT2).
- Combined Encryption+Decryption core is more expensive for Power/Area.

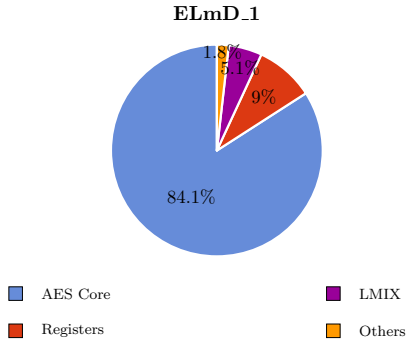
ELmD



Design similar to AES-COPA

- Initial value generation : 22 cycles (2 ENC).
- Thereafter every plaintext block takes 21 cycles (2 ENC calls).
- TAG takes another 21 cycles (2 ENC): Total 379 cycles for 16 Plaintext blocks.

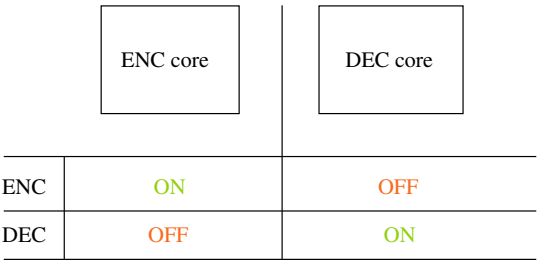
Implementation 1 : Combined ENC+DEC AES core



Evaluation

- Total Gate area : 28294 GE.
- Consumes 39.01 nJ for 16 Plaintext blocks (19.05 pJ/bit).
- Combined ENC+DEC AES core is not energy efficient.

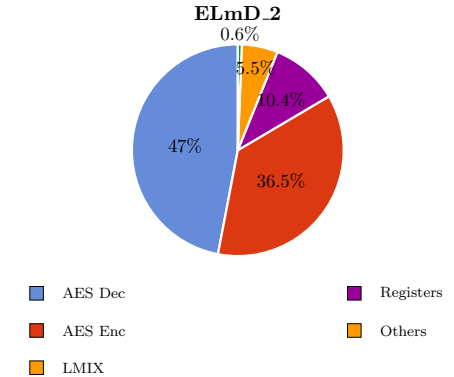
Implementation 2 : Separate ENC, DEC AES cores



Two Cores

- Two separate Cores for ENC and DEC.
- Each core can be turned OFF when inactive ⇒ Saves Power/Energy.
- Slightly larger area.

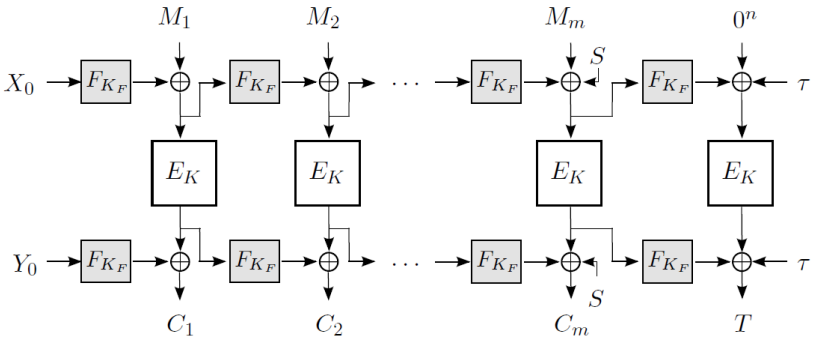
Implementation 2 : Separate ENC, DEC AES cores



Evaluation

- Total Gate area : 32355 GE.
- Consumes 24.44 nJ for 16 Plaintext blocks (11.93 pJ/bit).
- Slightly more energy than AES-COPA.

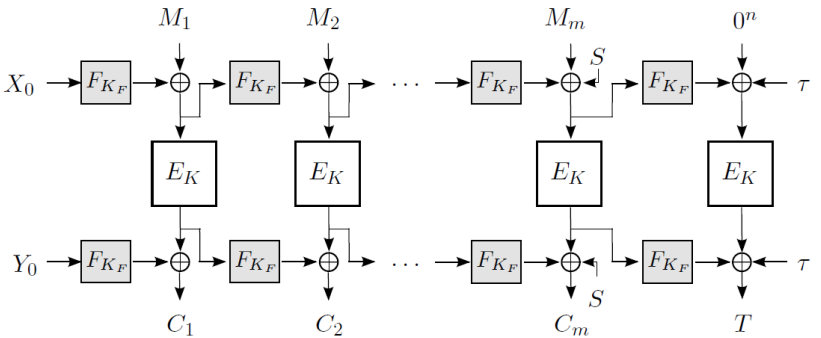
POET



POET

- Abed et al. FSE 2014.
- Uses 1 Encryption+ 2 Hash Function calls per Plaintext block.
- Multiplication by 2 in $GF(2^{128})$.

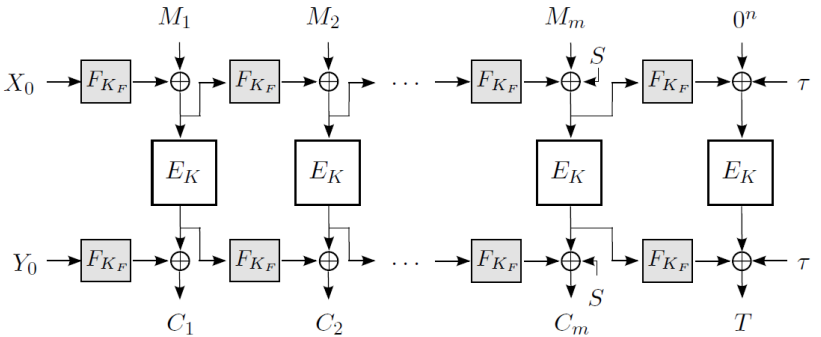
POET



Structure

- SIX extra registers required.
- 2 different Keys, Initial values used in the end.
- We analyze POET-AES10-AES4.

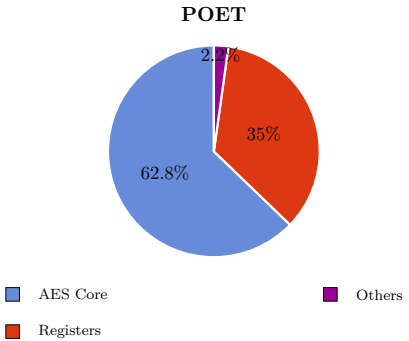
POET



Analysis

- Initial value generation : 77 cycles (7 ENC).
- Thereafter every plaintext block takes 19 cycles (1 ENC+2 UHF calls).
- TAG takes another 19 cycles: Total 400 cycles for 16 Plaintext blocks.

POET



Analysis

- Total Area of 19918 Gates.
- Total of 27.88 nJ for 16 Plaintext blocks (13.61 pJ/bit).
- AES core is the most power hungry module.

Overview of Results

#	Mode	Area (in GE)	#Cycles (16 PT Blocks)	Energy (nJ)	Energy/bit (pJ)
1	AES-COPA	18746	380	18.24	8.9
2	ELmD [1]	28294	379	39.01	19.05
	ELmD [2]	32355		24.44	11.93
3	POET	19918	400	27.88	13.62

Table : Energy consumptions for AES-COPA, ELmD, POET modes

Closing thoughts

- AES-COPA seems to be most energy efficient for Encryption+Tag Generation.
- Inverse free designs are better energywise..
- May see different trends for Decryption only/combined Encryption+Decryption implementation.


Technical University of Denmark
DTU
THANK YOU