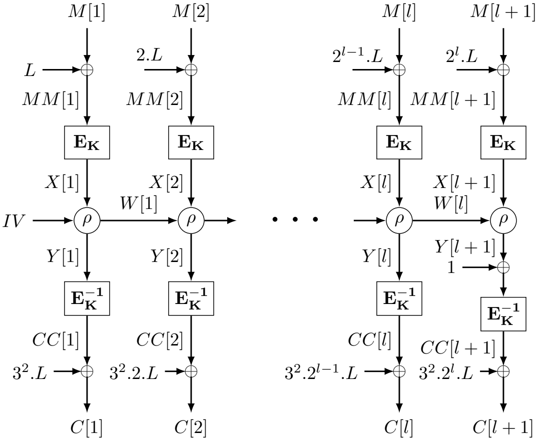
Hardware Performance of ELmD and ELmD(6,6)

Lilian Bossuet[1], Cuauhtemoc Mancillas-Lopez[1], Nilanjan Datta[2] and Mridul Nandi[2]

[1]Hubert Curien Laboratory, CNRS 5514. Jean Monnet University, Saint Etienne, France

[2]Indian Statistical Institute. Kolkata, India

ELmD Authenticated Encryption



$$L := E_K(0)$$

Main Features

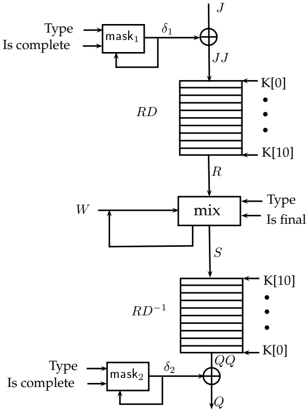
- Online.
- Efficient and Fast.
- Online Security in Nonce Repeating Scenario.
- Fully Pipeline Implementable.
- Can Incorporate Intermediate Tags.

Design Rationale

- EME like Structure -
  - To ensure Parallel structure and Fully Pipeline Implementation.
- Use of Online Linear Mix ρ -
  - Makes the construction online.
  - Incorporate Intermediate Tags.
- Use Decryption in Lower layer-
  - Minimize Enc-Dec combined implementation area.

Design of ELmD

Enc-Dec Combined hardware implementation area is minimized.



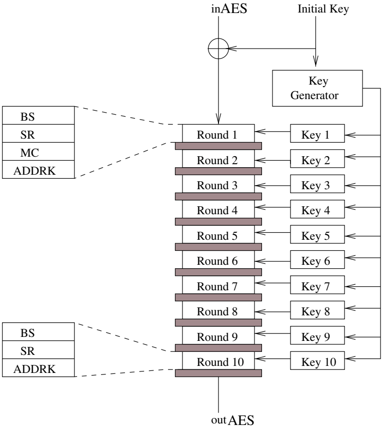
ELmD(6,6) Version

- Faster version of ELmD.
- 6 round AES encryption-decryption.
- $L := E_K(E_K(0))$ - To ensure randomness of L.
- Upper layer 6 round provides collision resistance property.
- Combined $12 = (6 + 6)$ round encryption provides desired randomness.

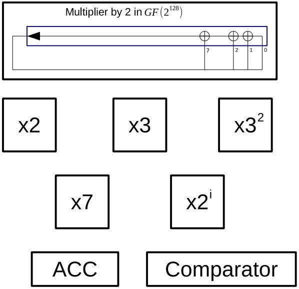
Design Decisions

- High performance FPGAs as underlying platform (Virtex 6).
- Pipeline designs.
- Single chip for encryption and decryption (for complete mode).
- Separated AES encryption and decryption cores.
- Shared key generator core for all AES cores.
- High speed oriented optimization.

Basic Blocks

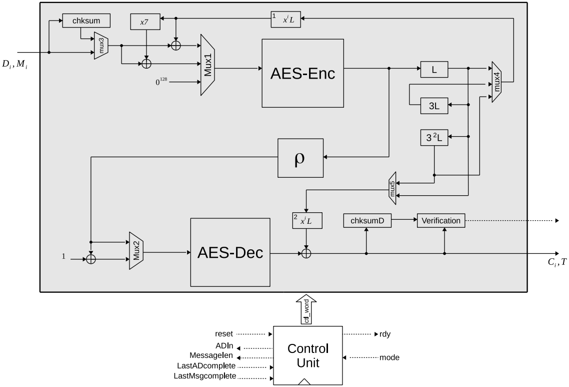


AES-core



Components

Architecture for ELmD



We developed architectures for COPA, OTR and OCB3 using the same design decisions.

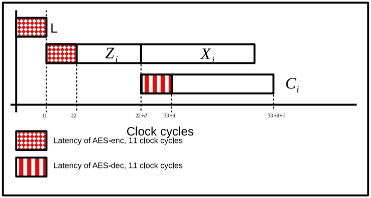
Operations in the time

ELmD(10,10)

$L = E_K(0)$

Total number of clock cycles to give tag:

$36 + d + l + 1$

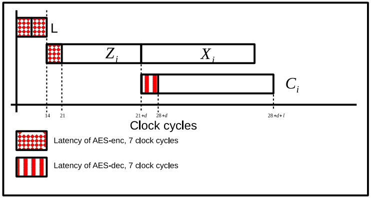


L
Z_i
X_i
C_i
11
22
22+d
33+d
33+d+l
Clock cycles
Latency of AES-enc, 11 clock cycles
Latency of AES-dec, 11 clock cycles

ELmD(6,6)

$L = E_K(E_K(0))$

$30 + d + l + 1$



L
Z_i
X_i
C_i
14
21
21+d
28+d
28+d+l
Clock cycles
Latency of AES-enc, 7 clock cycles
Latency of AES-dec, 7 clock cycles

Extra clock cycles are for reset, output synchronization and get the Tag.

Results for AES

Mode	Area			Frequency (MHz)	Throughput Gbps
	Slices	LUTs	Flip Flops		
AES-10 pipelined encryption	2023	7301	2824	315.16	38.47
AES-10 pipelined decryption	2360	9020	2693	239.34	30.63
AES-6 pipelined encryption	1635	4523	2329	315.16	38.47
AES-6 pipelined decryption	1639	5353	2400	239.34	30.63

Underlying platform xc6vlx240t-2ff1759. The results were taken from post-place and route reports.

Results for Modes

Mode	Area			Frequency	Lantency	Throughput
	Slices	LUTs	Flip Flops	(MHz)	clock cycles	Gbps
ELmD(10,10)	5225	16967	5578	234.64	$35 + d$	30.03
COPA	10391	32845	8336	230.87	$61 + d$	29.55
AES-GCM Virtex 5 Abdellatif et al, 2014	4770	-	-	311	-	36.92
OTR	4701	15333	5570	291.80	$25 + d$	37.35
ELmD(6,6)	3150	10783	4018	238.68	$30 + d$	30.55
OCB3	5180	16879	5846	234.87	$11 + d + Setup$ $+Stretch$	30.06
EME2 (Chakraborty et al, 2015)	10970	33350	9931	230.56	-	24.77

d is the number of 128−bit blocks of associated data.

The results were taken from post-place and route reports.

Latency is informative since the plaintext must be stored until verification process has been done.

Some Conclusions

- The design optimizations for area in ELmD(10,10) save physical resources in comparison with COPA and EME (combined implementation).
- ELmD(10,10) is competitive in area with GCM but slower. Remember that the security offers by ELmD(10,10) is stronger.
- OCB3 and ELmD(10,10) are comparable in terms of area, but OCB3 needs memory to store precomputed values for masking.
- ELmD(6,6) is smaller than OCB3, and their security is comparable.

Thanks for your attention

Questions?