Hardware Implementation of Some ECB-mix-ECB Based Algorithms

C. Mancillas López and L. Bossuet

Hubert Curien Laboratory UMR CNRS 5516, University of Lyon at Saint-Etienne, France.

cuauhtemoc.mancillas.lopez@univ-st-etienne.fr.

- PROJET FINANCÉ PAR L'ANR - PROJECT FUNDED BY THE ANR
ANR
SunamY

ECB-Mix-ECB

ECB-Mix-ECB is a general way to construct block cipher modes of operation proposed by Halevi and Rogaway in 2003. Its general structure is as follows:

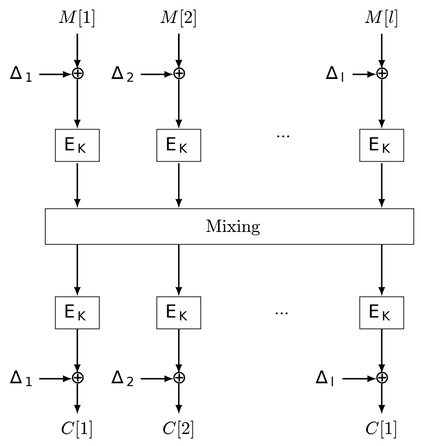
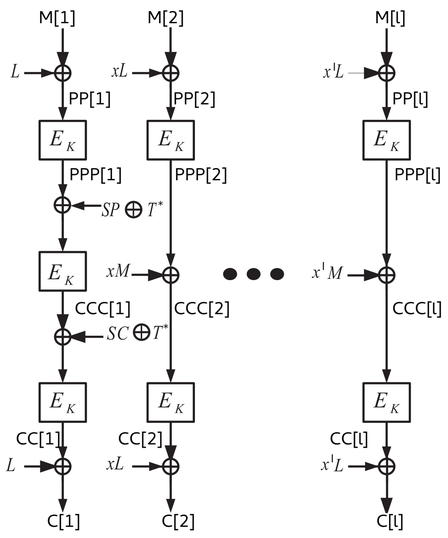


Figure: General structure.

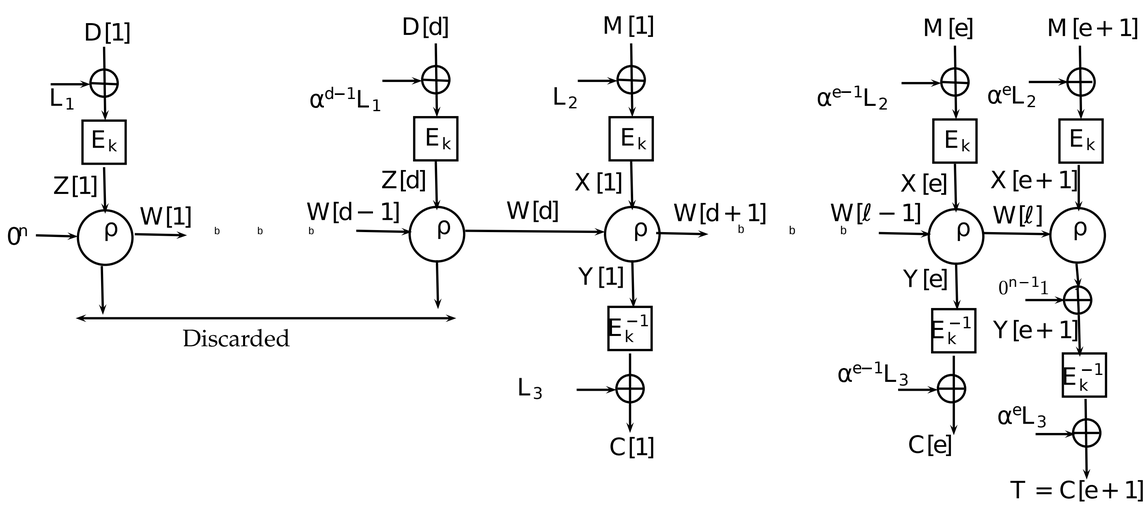
Any secure block cipher can be used, mixing function can be linear or non-linear and masking layers must warranty different values for each block, they can be generated by an LFSR.

EME2 (Halevi, 2004)



- Tweakable Enciphering Scheme
- Two passes
- $L \leftarrow E_K(0)$
- Non-linear Mixing
- $SP \leftarrow PPP[2] \oplus ... \oplus PPP[l]$
- $SC \leftarrow CCC[2] \oplus ... \oplus CCC[l]$
- $MP \leftarrow PPP[1] \oplus SP \oplus T^*$
- $MC \leftarrow E_K(MP)$
- $M \leftarrow MP \oplus MC$

ELmD (Datta and Nandi, 2014)



- Authenticated Encryption with Associated Data
- On-line
- Non-linear Mixing
- Second round candidate in CAESAR competition
- Fully pipelineable

Mixing function ρ is defined as:

$$y \leftarrow x \oplus 3 \cdot st,$$

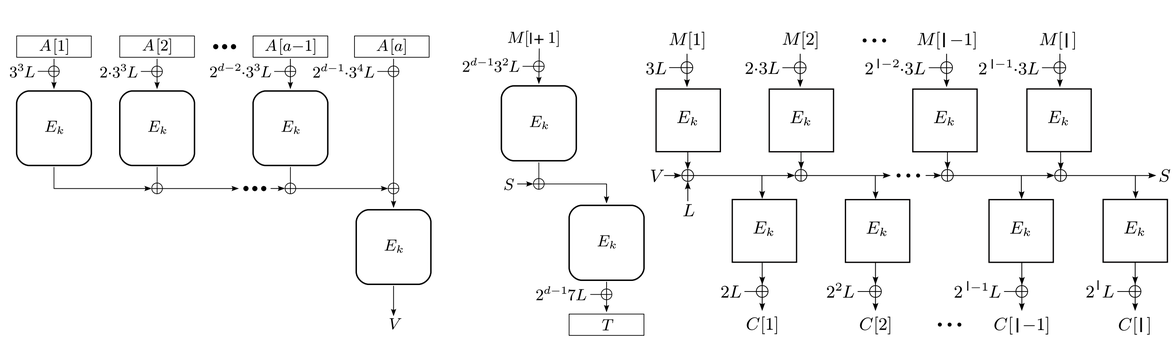
$$st' \leftarrow x \oplus 2 \cdot st,$$

and its inverse:

$$x \leftarrow y \oplus 3 \cdot st,$$

$$st' \leftarrow y \oplus st.$$

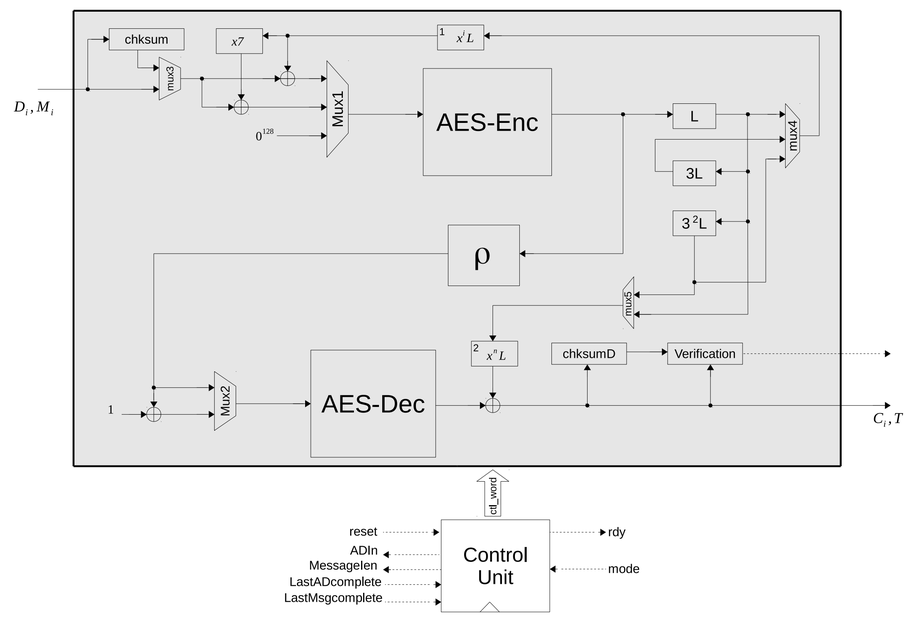
COPA(Andreeva et al, 2013)



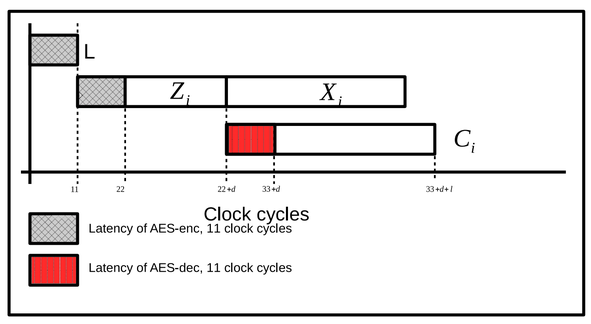
- Authenticated Encryption with Associated Data
- On-line
- Second round candidate in CAESAR competition
- Fully pipelineable
- It uses PMAC to process associated data

Architecture for ELmD

Our implementations were performed using pipeline, latency for AES cores is 11 clock cycles.



Operations in the time:



To get the real latency for C_i, two more clock cycles have to be added, one for the reset and other for final synchronization given a total time of $35 + d + l$ clock cycles. An additional clock cycle is used to give the tag T.

Results

In the following Table we show the results obtained after place and route using Xilinx ISE 13.4 and Virtex-6 (xc6vlx240t-2-ff1759) as a target device. Each Virtex-6 slice contains four 6-input-LUTs and eight flip flops, Virtex-5 slice contains only four flip flops).

Mode	Area			Frequency (MHz)	Lantency clock cycles	Throughput Gbps
	Slices	LUTs	Flip Flops			
ELmD	5225	16967	5578	234.64	$35 + d$	30.03
COPA	10391	32845	8336	230.87	$61 + d$	29.55
AES-GCM (Abdellatif et al. 2014) Virtex 5	4770	-	-	311	-	36.92
EME2 (chakraborty et al. 2015)	10970	33350	9931	230.56	-	24.77
AES-10 pipelined encryption	2023	7301	2824	315.16	1	38.47
AES-10 pipelined decryption	2360	9020	2693	239.34	1	30.63

CHES 2015, Saint-Malo, France. This work was realized in the frame of the TSUNAMY project number ANR-13-INSE-0002-02 supported by the French Agence Nationale de la Recherche.