EFFICIENT AES IMPLEMENTATIONS ON ASICS & FPGAS

NORBERT PRAMSTALLER, STEFEN MANGARD, SANDRA DOMINIKUS AND JOHANNES WOLKERSTORFER

INTRODUCTION

- Why do we need dedicated hardware implementation for AES ?
  - High speed communication link
  - It’s easier to secure a small AES module than an entire processor
  - Reduce the power consumption

ASIC IMPLEMENTATION OF AES

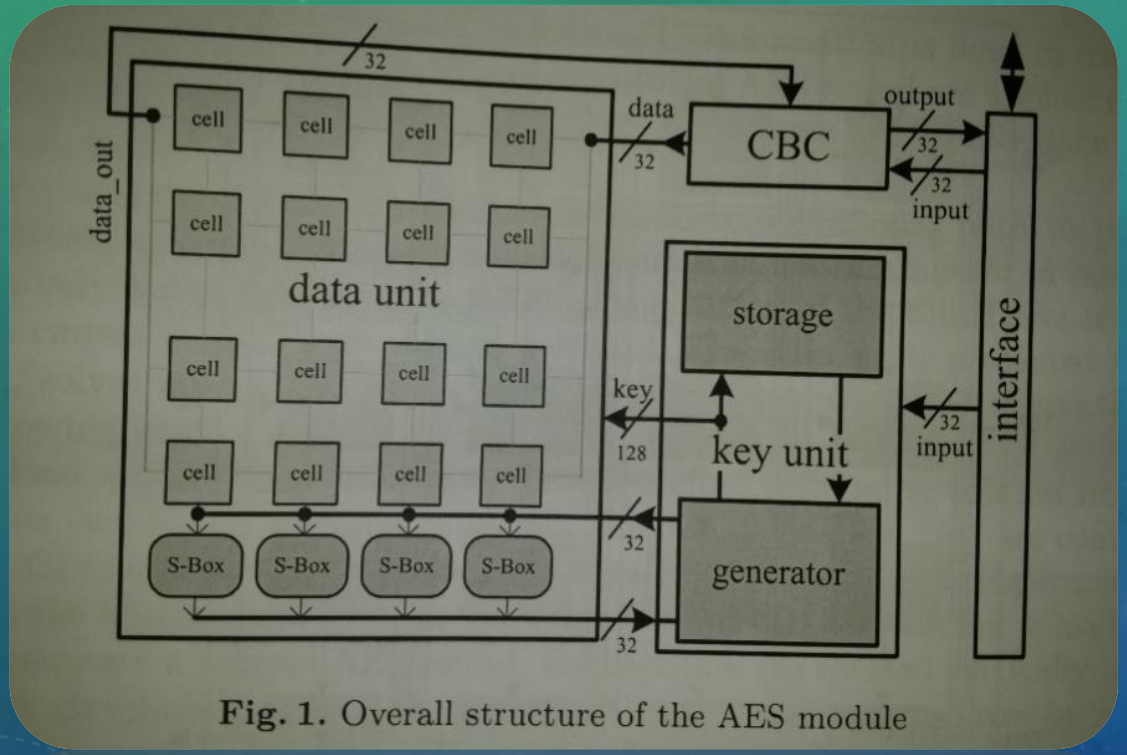

Fig. 1. Overall structure of the AES module

Table 2. Complexity of the AES-128 modules

Component	#	Minimum	#	Standard	#	High Perf.
S-Boxes	4	1,568	4	1,568	16	6,272
Multipliers	4	848	16	3,392	16	3,392
D. cells without mult.	16	1,392	16	1,392	16	1,392
Multiplexors	96	224	192	384	224	374
Data unit		**4,032**		**6,736**		**11,430**
Key generator	1	1,633	1	1,633	1	1,633
Key store	1	691	1	691	1	691
Key unit		**2,324**		**2,324**		**2,324**
AMBA + CBC	1	1,866	1	1,866	1	1,866
Control logic		319		279		230
Additional		**2,185**		**2,145**		**2,096**
Total		**8,541**		**11,205**		**15,850**

Table 3. Summary of the performance of the different AES-128 modules

Version	Clock Cycles	Throughput@50 MHz [*Mbps*]	Area [GE]
Minimum	92	70	8,541
Standard	65	98	11,205
High perf.	35	183	15,850

FPGA IMPLEMENTATION OF AES

Table 4. Hardware resources and throughput comparison

Work	Device	#CLB-slices	#BRAM	ECB mode Throughput [Mbps]
Gaj et al. [3]	Xilinx XCV1000	12,600	80	12,160
McLoone et al. [9] (I)	Xilinx XCV812E	2,222	100	6,956
McLoone et al. [9] (II)	Xilinx XCV3200E	2,577	112	5,800
McLoone et al. [9] (III)	Xilinx XCV3200E	2,995	138	5,000
McLoone et al. [9] (IV)	Xilinx XCV3200E	7,576	102	3,239
Dandalis et al. [5]	Xilinx XCV1000	5,673	?	353
Fischer et al. [6] (I)	FLEX 10KE200-1	2,530	24	451
Fischer et al. [6] (II)	ACEX 1K50-1	1,213	10	115
Chodowiec et al. [2]	Xilinx XC2S30-6	222	3	166
Our proposal	Xilinx XCV1000E	**1,125**	**0**	**215**

[9]: enc.: (I)AES-128, (II)AES-192, (III)AES-256, enc./dec.:(IV)AES-128
[6]: AES-128 enc./dec.: (I) fast configuration, (II) economic configuration