

Figure 3. The delay and LUT usage for a pipelined Sbox

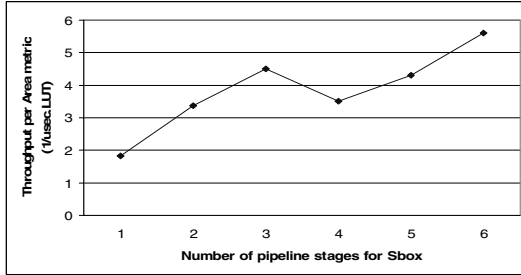


Figure 4. Optimum number of pipeline stages for one Sbox

4. Performance results

The performance results of our proposed architectures are shown in table 1 and are compared with related work in table 2. The Synplicity tool for synthesis and the Xilinx's ISE tool for place and route are used. Moreover, when the Block RAMs are used, the Sboxes of the key scheduling and the first five rounds of the encryption datapath are mapped onto Block RAMs and the rest of them are designed using the pipelined implementation of section 3. This way, the first five rounds take 10 clock cycles because byte substitution takes one clock cycle on a BRAM.

5. Conclusion

The architecture of a fully pipelined AES processor is presented. It can achieve a maximum throughput of 21.54 Gbits/s using 84 Block RAMs and 5177 Slices of VirtexII-Pro FPGA with an optimum number of pipeline stages for the byte substitution phase and a throughput/area rate of 4.2 Mbits/Slice.

6. Acknowledgment

This material is based upon work supported by the Space and Naval Warfare Systems Center - San Diego under contract No.N66001-02-1-8938. This funding is acknowledged.

Table1. Performance result (After place and route)

Design	4 stages per round, no BRAM	4 stages per round with BRAM	7 stages per round, no BRAM	7 stages per round with BRAM
Slices	12450	5177	9446	6400
LUTs	22358	8285	16650	9432
BRAM	-	84	-	84
Critical path	5.94 nsec	5.94 nsec	5.91 nsec	6.36 nsec
Freq.	168.3 MHz	168.3 MHz	169.1 MHz	157.1 MHz
latency	41 cycles	31 cycles	71 cycles	46 cycles
Throughput	21.54 Gbits/s	21.54 Gbits/s	21.64 Gbits/s	20.11 Gbits/s

Table2. Comparison with other FPGA implementations

FPGA Implementation comparison when Block RAM is not used					
Design	Device	Slices	B RAM	Through put	Mbps / Slice
Elbirt et al [6]	XCV1000 - 4	10992	-	1.94 Gbits/s	0.17
Standaert et al [10]	XCV3200E-8	15112	-	18.56 Gbits/s	1.2
Jarvinen et al [13]	XC2V2000-5	10750	-	17.8 Gbits/s	1.66
Design with 4 stages in round	XC2VP30 - 7	12450	-	21.54 Gbits/s	1.7
Design with 7 stages in round	XC2VP20 - 7	9446	-	21.64 Gbits/s	2.3
FPGA implementation comparison when Block RAM is used					
Gaj et al [7]	XCV1000 - 6	12600	80	12.1 Gbits/s	0.96
McLoone et al [8]	XCV812E - 8	2222	100	6.95 Gbits/s	3.1
Standaert et al [10]	XCV3200E-8	2784	100	11.77 Gbits/s	4.2
Saggese et al [11]	XVE2000 - 8	5810	100	20.3 Gbits/s	3.4
Design with 4 stages in round	XC2VP20 - 7	5177	84	21.54 Gbits/s	4.2

6. References

- [1] National Institute of Standards and Technology (U.S.), Advanced Encryption Standard. Available at: <http://csrc.nist.gov/publication/drafts/dfips-AES.pdf>
- [2] Satoh et al, "A Compact Rijndael Hardware Architecture with S-Box Optimization", ASIACRYPT 2001, LNCS 2248, pp.239-254.
- [3] J. Wolkerstorfer, E. Oswald, M. Lamberger, "An ASIC Implementation of the AES Sboxes", Proc. RSA Conference 2002, San Jose, CA, February 2002.
- [4] T. Ichikawa et al, "Hardware Evaluation of the AES Finalists", in Proc. 3th AES Candidate Conference, New York, April 2000.
- [5] I. Verbauwhede, P. Schaumont, H. Kuo, "Design and Performance testing of a 2.29 Gb/s Rijndael Processor", IEEE Journal of Solid-State Circuits (JSSC), March 2003.
- [6] A. Elbirt et al, "An FPGA-based performance evaluation of the AES block cipher candidate algorithm finalists", IEEE Trans. of VLSI Systems, 9.4, pp.545-557, August 2001.
- [7] Gaj et al, "Fast Implementation and Fair Comparison of the Final Candidates for Advanced Encryption Standard Using Field Programmable Gate Arrays", CT-RSA 2001, LNCS 2020, pp.84-99.
- [8] McLoone et al, "High Performance Single-Chip FPGA Rijndael Algorithm Implementations", CHES 2001, Paris, France, 2001.
- [9] Marie McLoone, John V. McCanny, "Single-Chip FPGA Implementation of the Advanced Encryption Standard Algorithm", FPL 2001, LNCS 2147, pp. 152-161, 2001.
- [10] Standaert et al, "Efficient Implementation of Rijndael Encryption in Reconfigurable Hardware: Improvements and Design Tradeoffs", CHES 2003, LNCS 2779, pp. 334-350, 2003.
- [11] Saggese et al, "An FPGA-Based Performance Analysis of the Unrolling, Tiling, and Pipelining of the AES Algorithm", FPL 2003, LNCS 2778, pp. 292-302, 2003.
- [12] V. Rijmen, "Efficient Implementation of the Rijndael S-box", available at: <http://esat.kuleuven.ac.be/~rijmen/rijndael/sbox.pdf>
- [13] Jarvinen et al, "A fully pipelined memoryless 17.8 Gbps AES-128 encryptor", International Symposium on Field Programmable Gate Arrays, pp. 207-215. 2003.