A 21.54 Gbits/s Fully Pipelined AES Processor on FPGA

Alireza Hodjat and Ingrid Verbauwhede
Electrical Engineering Department
University of California, Los Angeles
{ahodjat, ingrid} @ ee.ucla.edu

Abstract

This paper presents the architecture of a fully pipelined AES encryption processor on a single chip FPGA. By using loop unrolling and inner-round and outer-round pipelining techniques, a maximum throughput of 21.54 Gbits/s is achieved. A fast and area efficient composite field implementation of the byte substitution phase is designed using an optimum number of pipeline stages for FPGA implementation. A 21.54 Gbits/s throughput is achieved using 84 Block RAMs and 5177 Slices of a VirtexII-Pro FPGA with a latency of 31 cycles and throughput per area rate of 4.2 Mbps/Slice.

1. Introduction

The Advanced Encryption Standard was accepted as a FIPS standard in November 2001 [1]. Since then, there have been many different hardware implementations for ASIC and FPGA. References [2, 3, 4, and 5] present architectures and results for ASIC implementation. On the other hand, references [6, 7, 8, 9, 10, and 11] present implementations of the AES algorithm on FPGA that can achieve a throughput rate from 1 to 20 Gbits/s. This paper presents our proposed fully pipelined architecture with an optimum number of pipeline stages for the byte substitution phase of the AES algorithm. It can provide a throughput of 21.54 Gbits/s with a throughput per area rate of 4.2 Mbps/Slice.

2. Fully pipelined AES implementation

The Advanced Encryption Standard [1] is composed of four different steps that are repeated in N_r number of rounds. These are byte substitution, shift row, mix column, and key addition. When a key size of 128 bits is used, the number of rounds the algorithm is repeated (N_r) is equal to ten. Figure 1 shows the unrolled and fully pipelined implementation of the AES algorithm. The shift row step is just interconnection and the key addition is XORing of the round data and the round key. The mix column step consists of a chain of XORs to permute the elements of data in each column. The arithmetic of these three stages can be combined in one pipeline stage for each round. On the other hand the most expensive step is the byte substitution phase, which is explained next.

3. Byte substitution phase

In the byte substitution phase (Sbox), the input is considered as an element of GF(2^8). First the multiplicative inverse in GF(2^8) is calculated. Then, an affine transformation over GF(2) is applied [1]. Either, all the substitute values have to be pre-calculated and stored in the Block RAMs or on the fly calculation of the values must be implemented in logic. Rijmen [12] suggests an algorithm that calculates the byte substitution phase using the GF(2^4) operations.

Figure 2 shows the architecture of byte substitution phase when the input is mapped into the GF(2^4) elements and the GF(2^4) operations are used. This is the most area efficient implementation of Sboxes. Due to the long delay of this architecture, pipelining must be used. Figure 3 shows the LUT usage and the critical path delay of the pipelined implementation of one Sbox using this architecture synthesized for VirtexII-Pro FPGA (pre-place and route). The bar graph shows the delay and the plotted line shows the LUT usage. The best delay-LUT combination is the design with three pipeline stages. Also figure 4 shows the throughput per area metric for different pipelined implementations. The most efficient designs are those with three and six pipeline stages for the byte substitution phase as shown in figure 2. The dotted lines are the pipeline registers for the three-stage byte substitution and the solid lines are the registers for six-stage Sbox. In addtion the last pipeline stage of each round of the AES algorithm includes the shift row, mix-column and key addition phase (figure 1). Therefore the optimum pipelined implementations have a total of four or seven pipeline stages for each round of AES.

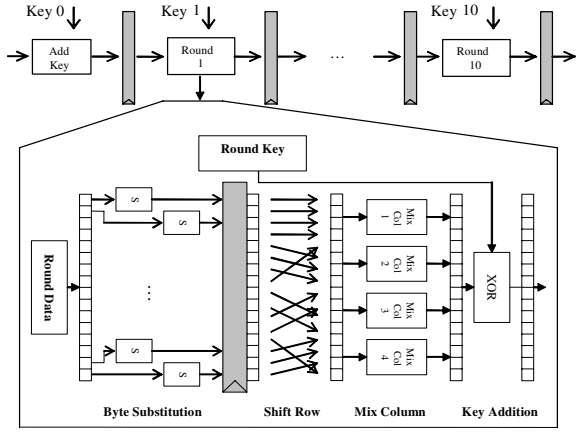

Figure 1. Fully pipelined Advanced Encryption Standard

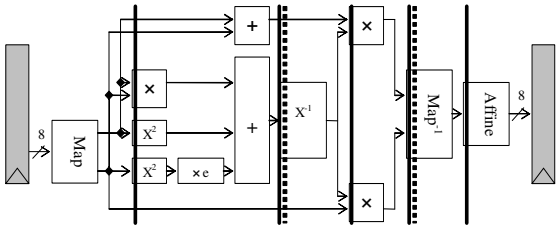

Figure 2. The pipelined composite field implementation of the byte substitution phase

Proceedings of the 12th Annual IEEE Symposium on Field-Programmable Custom Computing Machines (FCCM'04)
0-7695-2230-0/04 $ 20.00 IEEE

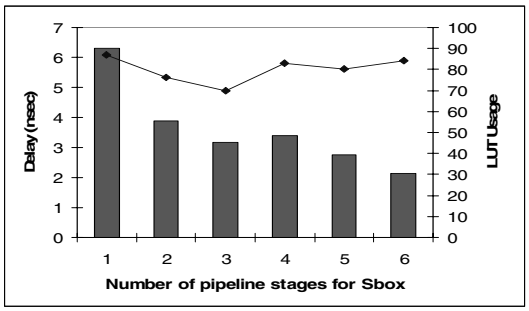

Figure 3. The delay and LUT usage for a pipelined Sbox

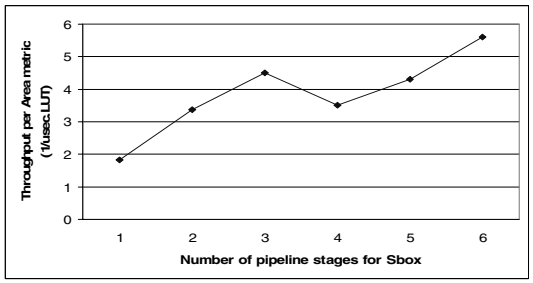

Figure 4. Optimum number of pipeline stages for one Sbox

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 Mbps/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
Through put	21.54 Gbits/s	21.54 Gbits/s	21.64 Gbits/s	20.11 Gbits/s

Table2. Comparison with other FPGA implementations

Design	Device	Slices	B RAM	Through put	Mbps / Slice
FPGA Implementation comparison when Block RAM is not used					
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 Implemenation 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.