Speed-Area Trade-off for 10 to 100 Gbits/s Throughput AES Processor

Alireza Hodjat
ahodjat @ee.ucla.edu
Electrical Engineering Department
University of California, Los Angeles

Ingrid Verbauwhede
ingrid @ee.ucla.edu
Electrical Engineering Department
University of California, Los Angeles

Abstract- **This paper explores the area-throughput trade-off for an ASIC implementation of the Advanced Encryption Standard (AES) algorithm in a 0.18 m CMOS technology. Three different pipelined implementations of the AES algorithm are presented which provide a throughput range between 15.7 to 77.6 Gbits/s with an area cost of 116 to 473 Kgates. Therefore, the AES algorithm in the counter mode of operation can be used to generate cryptographically secure pseudorandom numbers at a throughput rate of multi-ten Gbits/s. Thus it becomes available for encryption on an optical link.**

I. INTRODUCTION

In an optical network where users are connected together with an optical link, the data rate of the link is usually tens of Gbits/s. In one application, the optical switches require cryptographically secure random numbers at the rate of several 10 Gbits/s to generate the encrypted stream of data. For this purpose, the Advanced Encryption Standard algorithm [1] is used in the Counter mode of operation [2] to generate the sequences of random numbers from an initial 128-bit seed. References [3, 6, 9, 10] are some of the ASIC implementations and [7, 8, 11] present the fastest FPGA implementations of the AES algorithm. All of these architectures can achieve the throughput rate of several Gbits/s. The maximum throughput is 5.7 Gbits/s on ASIC and 12.2 Gbits/s on FPGA shown by [11].

This paper presents three different architectures for the AES algorithm that can accomplish the maximum throughput of 15.7 to 77.6 Gbits/s in a 0.18 m CMOS standard cell technology. For each design the area-speed trade-off is explored. The results are used to choose the most suitable case based on the throughput and area constraints depending on the number of users in the network.

II. DESIGN CONSIDERATIONS

Figure 1 shows the different steps of the AES algorithm. The AES algorithm is performed in N_r number of rounds. The architecture of one round contains two different datapaths, the encryption datapath and the key scheduling datapath. The details of each step are presented in the next section. The data block is 128 bits long and the key size can be 128, 192, or 256 bits. The size of the key defines the number of rounds that the algorithm is repeated. In order to achieve the highest possible throughput of the AES algorithm, the following optimization strategy is taken:

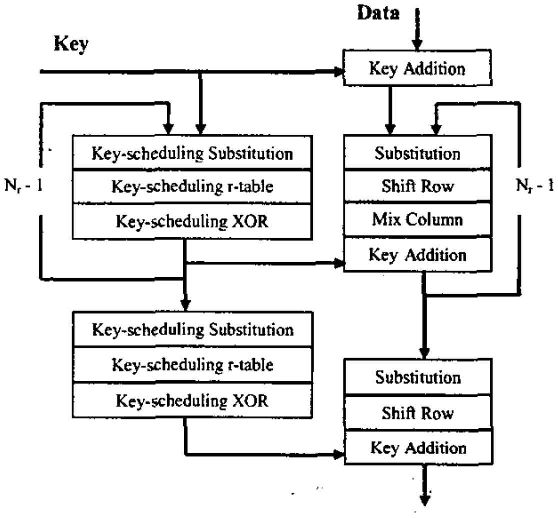

Fig 1. Advanced Encryption Standard Algorithm

1. The key length is limited to 128 bits. It helps to reduce the critical path of the key scheduling datapath. It also fixes the number of rounds, N_r , to be 10. This means that each input block is encrypted in 10 rounds.
2. The algorithm is loop-unrolled. Since the 128-bit key AES performs in 10 rounds, running the entire 10 rounds in one datapath sequentially reduces the achieved throughput. Therefore, the round-loop is unrolled.
3. Pipelining is used. Since the AES algorithm is used in the counter mode, which is a non-feedback mode of operation, the design can be pipelined. Figure 2 shows the details of the AES algorithm in the counter mode of operation. In the case of random number generation, the initial 128-bit seed is loaded into the seed register. This seed forms the initial value of the counter register. Every clock cycle the counter value is incremented. The counter value is loaded into the AES unit and it is encrypted. The encrypted value is the generated random number that is written out. Starting from a secure non-

0-7803-8104-1/03/$17.00 ©2003 IEEE

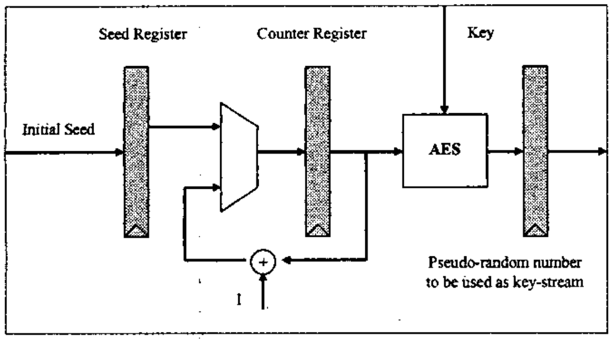

Fig 2. AES in counter mode of operation

repeating initial seed, 2^{128} sequences of 128-bit random numbers are generated. The details of the pipelined architecture of the AES unit are described in the next section. The three proposed designs have different pipelined architectures.

4. The choice of byte substitution phase. In this phase every byte of the data is substituted with another byte. The new byte is calculated using the GF(2^8) operations. There are two well-known implementations for the substitution phase of the AES algorithm. One approach is the direct implementation of the substitution boxes using lookup tables because all the 256 cases of the substitution bytes can be pre-computed and can be stored in a lookup table. The other approach is to use the GF(2^4) operations to calculate the substitution value on-line [6]. In our case, the direct implementation is chosen because it results in much faster critical path in a reasonable amount of gate counts. Reference [10] presents an experiment which shows the area-delay trade-off between direct implementation of the substitution phase versus the on-line calculation of substitution values.

III. PROPOSED PIPELINED ARCHITECTURES

In this section, three different pipelined architectures of the AES algorithm are presented. These architectures differ in various features such as the number of pipeline stages and the number of rounds that are implemented in hardware. The complete throughput and area performance of each of these architectures is provided in the next section.

A. Inner and outer round pipelining

Figure 3 shows the pipelined architecture of our first design. Every round is divided into four pipeline stages, substitution, shift-row, mix-column, and key-addition. Also all the 10 rounds are pipelined. The gray boxes in the figure show the pipeline registers. Including the first stage (key-addition) there are total of 41 pipeline stages. This is the ultra fast design that can achieve the maximum throughput of 77.6 Gbits/s. However the area cost is very high. Moreover, in this design the critical path is in the first pipe stage of each round which is the substitution phase of the AES algorithm.

B. Only outer round pipelining

Since the previous design implements the AES algorithm in 41 pipeline stages, there is a high area cost due to the number of registers used between pipeline stages. Figure 4 shows another design that only performs the outer round pipelining of the AES algorithm and the inner round pipeline registers are removed for the purpose of area optimization. Therefore, every round is performed in one clock cycle and there are a total of 11 pipeline stages. Here the critical path includes all the four phases of each round (substitution, shift row, mix column, and key addition). The complete synthesis result is provided in the next section.

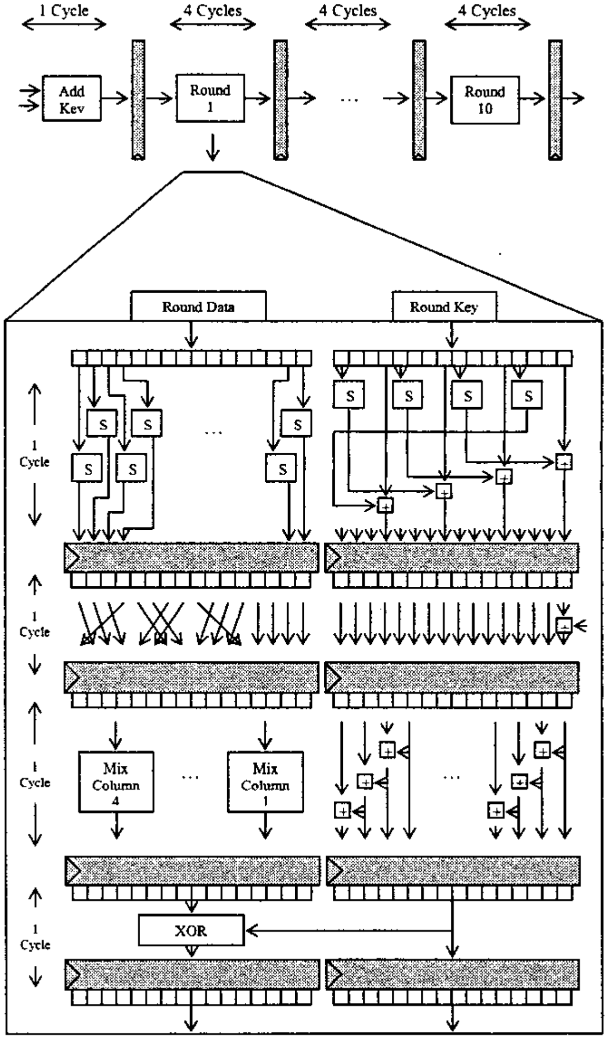

Fig 3. Inner-round and outer-round pipelined architecture

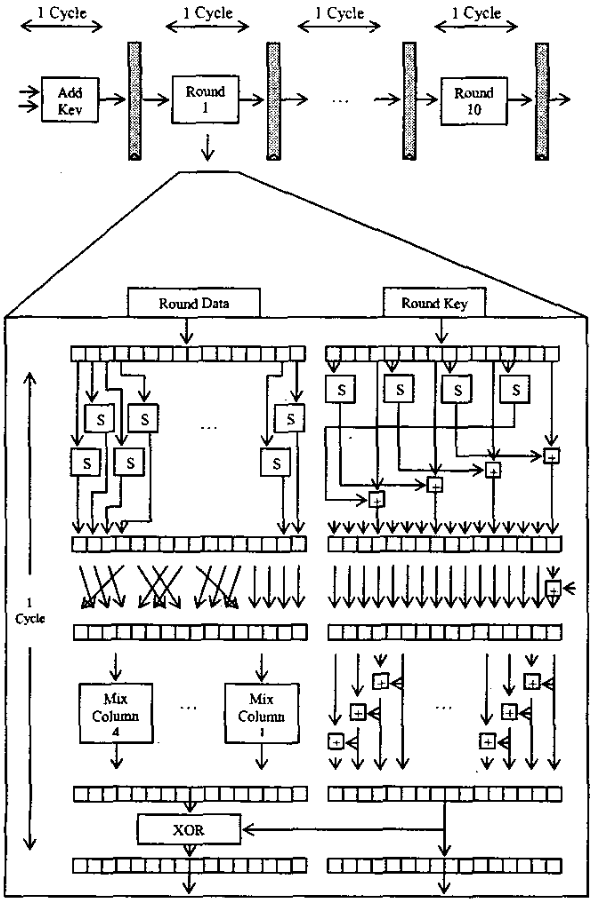

Fig 4. Outer-round only pipelined architecture

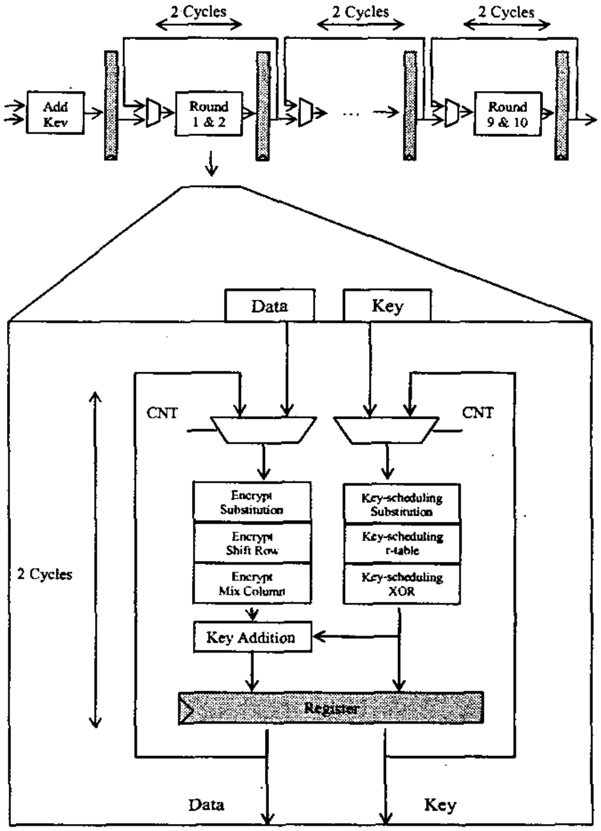

Fig 5. Multi-round pipelined architecture

C. *Multi-round pipelining*

For further area optimization, another pipelined architecture is designed which is shown in figure 5. Here, every two rounds are implemented on the same datapath and the pipelining is performed for every two rounds. There are a total of 5 pipeline stages and every pipe stage takes two cycles, which corresponds to two rounds of the algorithm. Therefore, one output is generated every two cycles. This way, a throughput of 15.7 to 23.1 Gbits/s is achieved with a reasonable area cost (between 116 to 225 Kgates).

IV. RESULTS

Table 1 shows the synthesis results of our three pipelined architectures of the AES algorithm using a 0.18 m CMOS standard cell technology. The inner and outer round pipelined architecture (subsection A above) has a critical path of between 1.65 to 2.14 nsec that results in the maximum throughput of between 59.7 to 77.6 Gbits/s. The area cost varies between 313 to 473 Kgates.

For the outer-round-only pipelined architecture (subsection B above), the critical path varies between 2.65 to 4.06 nsec which corresponds to a throughput of 31.5 to 48.2 Gbits/s and an area consumption of 211 to 372 Kgates. The multi-round pipelined architecture (subsection C above) has a critical path between 2.76 and 4.08 nsec and a throughput of 15.7 to 23.1 Gbits/s at the area cost of 116 to 225 Kgates. This design produces an output every two clock cycles. Figure 6 shows the area-throughput of our three different AES pipelined architectures. This figure is used to choose the most suitable design under the throughput and area constraints.

V. CONCLUSION

This paper presented the architecture, synthesis results and the area-speed trade-offs of three different pipelined architectures of the AES algorithm. The area-throughput trade-off result (figure 6) is used to design the most suitable random number generator based on the AES algorithm in the counter mode of operation under the area and throughput constraints. The final multi-ten Gbits/s AES based pseudo-random number generator is used to configure the optical switches.

TABLE 1
Synthesis results using 0.18 µm CMOS technology

Inner-round and Outer-round pipelining					
Clock per sample	1				
Latency (Cycles)	41				
Critical path (nsec)	1.65	1.69	1.79	1.90	2.14
Maximum frequency (MHz)	606	591	558	526	467
Area for one round (Kgates)	47.1	44.8	40.5	37.4	31.1
Throughput (Gbits/s)	77.6	75.6	71.4	67.3	59.7
Total area (Kgates)	473	450	407	376	313
Outer-round pipelining only					
Clock per sample	1				
Latency (Cycles)	11				
Critical path (nsec)	2.65	2.89	3.08	3.60	4.06
Maximum frequency (MHz)	377	346	325	277	246
Area for one round (Kgates)	37	29.5	26.3	22.5	20.8
Throughput (Gbits/s)	48.2	44.3	41.6	35.4	31.5
Total area (Kgates)	372	297	265	227	211
Multi-round pipelining					
Clock per sample	2				
Latency (Cycles)	11				
Critical path (nsec)	2.76	2.95	3.10	3.57	4.08
Maximum frequency (MHz)	362	339	322	280	245
Area for two rounds (Kgates)	44.4	40.8	32.3	24.8	22.5
Throughput (Gbits/s)	23.1	21.7	20.6	17.9	15.7
Total area (Kgates)	225	207	165	128	116

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. The authors would like to acknowledge the funding of this project.

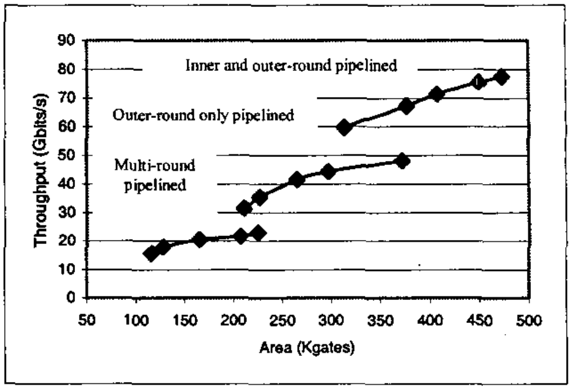

Fig 6. Area-throughput trade-off for the high speed pipelined AES implementations

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] M. Dworkin, SP 800-38A 2001, "Recommendation for Block Cipher Modes of Operations", December 01.

[3] A. Satoh, S. Morioka, K. Takano, S. Munetoh, "A Compact Rijndael Hardware Architecture with S-Box Optimization", ASIACRYPT 2001, LNCS 2248, pp. 239-254, 2001.

[4] http://www.nist.gov/aes/

[5] H. Kuo, P. Schaumont, and I. Verbauwhede, "A 2,29 Gbits.sec, 56 mW non-pipelined Rijndael AES Encryption IC in a 1.8 V, 0.18 um CMOS technology," Proc. 2002 CICC, pp. 147-50, May 2002.

[6] J. Wolkerstorfer, E. Oswald, M. Lamberger, "An ASIC Implementation of the AES Sboxes", Proc. RSA Conference 2002, San Jose, CA, February 2002.

[7] M. McLoone, J. McCanny, "High Performance Single Chip FPGA Rijndael Algorithm Implementations", Workshop on Cryptographic Hardware and Embedded Systems, Paris, 2001.

[8] A. Elbirt, W. Yip, B. Chetwynd, C. Paar, "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.

[9] T. Ichikawa et al, "Hardware Evaluation of the AES Finalists", in Proc. 3th AES Candidate Conference, New York, April 13-13, 2000.

[10] I. Verbauwhede, P. Schaumont, H. Kuo, "design and Performance testing of a 2.29 Gb/s Rijndael Processor", IEEE Journal of Solid-State Cuitcuits (JSSC), March 2003.

[11] K. Gaj and P. Chodowiec, "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, 2001.