2014 Fifth International Symposium on Electronic System Design

FPGA Implementation of Pipelined Blowfish Algorithm

Swagata Roy Chatterjee, Soham Majumder, Bodhisatta Pramanik
Department of ECE, Netaji Subhash Engineering College,
Kolkata, West Bengal 700152
rcswagata@gmail.com, sm.majumder91@gmail.com,
bodhipramanik@gmail.com

Mohuya Chakraborty
Department of IT, Institute of Engineering and Management
Kolkata, West Bengal 700091
mohuyacb@yahoo.com

***Abstract*— Objective of this paper is to enhance the throughput of Blowfish block cipher by designing a pipelined architecture of the same followed by implementation and evaluation of its performance in Field Programmable Gate Array. The proposed architecture was implemented by using Verilog HDL and was synthesized, placed and routed in Spartan3E chip XC3s500e-5fg320 using ISE Design Suite 12.1. Performance analysis of the proposed pipelined design shows a throughput of 6.3 Gbps as compared to 588.255 Mbps for non-pipelined design.**

Keywords- Encryption; Blowfish; Pipeline;Feistal Network

I. INTRODUCTION

Blowfish is a *FEISTEL NETWORK,* iterating an encryption function 16 times [1]. It is proven that Blowfish runs faster than DES or AES where frequent key changing is not required. So it is suitable for wireless network applications which exchanges small size packets like any type of emergency control signal. Here the main objective is to enhance the throughput of the algorithm utilizing pipelining technique. Previous work in the area of implementation of block ciphers like DES and AES on Field Programmable Gate Array (FPGA) was studied in [2], [3]. A pipelined architecture is designed by using Verilog HDL and the performance is evaluated on Spartan3E FPGA platform.

II. HARDWARE DESIGN OF PIPELINED BLOWFISH ALGORITHM

In a pipelined architecture, if a series of instructions are provided as input to a pipelined processor, then the second instruction will start executing before the first has been finished as shown in fig. 1[4].

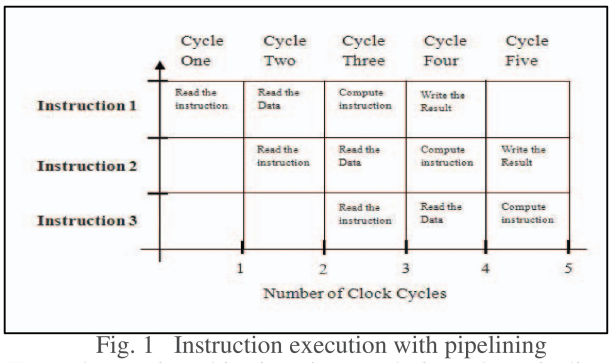

Fig. 1 Instruction execution with pipelining

Here the main objective is to design the pipelined architecture for encryption, so key expansion is not taken into consideration. The pipelined architecture of the blowfish algorithm is shown in fig. 2 where data path is controlled by designing a control unit and sixteen module blocks that are designed for each stage of iteration.

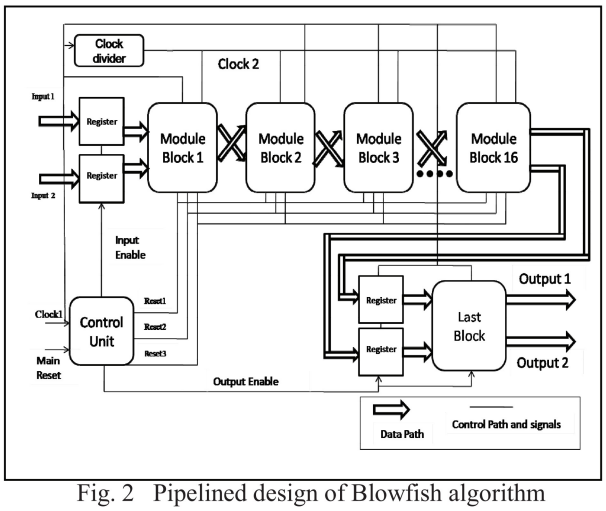

Fig. 2 Pipelined design of Blowfish algorithm

Only the first module block operates on the input raw data and rest module blocks operate on the computed output data from the previous module block. Each module needs three clock cycles to complete the computation. Here the first module block is made to operate on the second set of input raw data simultaneously with the second stage operating on the first set of data encrypted by the first module block. As a result, subsequent data words need extra 3 clock cycles each. The first input word is encrypted in 49 clock cycles, second word requires fifty two, the third requires fifty five clock cycles and so on.

The proposed Module Block as shown in fig. 3 is designed by inserting seven registers in order to allow for pipelining and is replicated sixteen times in the entire design, as in the original blowfish architecture. The proposed architecture differs from the original architecture in its working due to the addition of the last pair of register levels, and selective switching of the 3 register levels.

The first, second and third registers operate simultaneously in the first clock cycle and holds the input data during the entire clock cycle when the P box data is fetched and an exclusive-or operation is performed between the left 32 bits (LE-0) and 32 bits of the P-array that have already been initialized with the preset key. The right hand input data does

978-1-4799-6965-4/14 $31.00 © 2014 IEEE
DOI 10.1109/ISED.2014.51

not perform any computation during this cycle, and hence holds the original data.

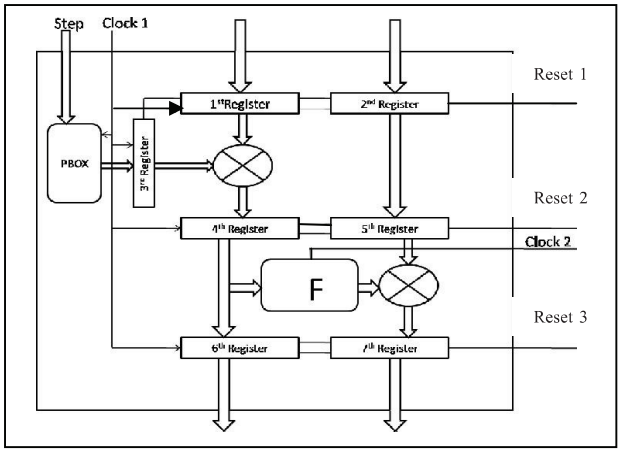

Fig. 3 Pipelined Module Block

The fourth and fifth registers operate in pair and hold the data needed for operation of the F block and second exclusive-or operation. The sixth and seventh registers store the computed final data of a module block from the subsequent blocks until the time of the next clock cycle when the next module block is ready to accept the data.

III. Performance Evaluation of Proposed Blowfish Architecture

The pipelined Blowfish Algorithm has been implemented using Verilog HDL on ISE 12.1. Simulation results shown in fig. 4 prove that encrypted data for the first word is obtained after the 49th clock cycle having duration of 2 ns at 100 ns..

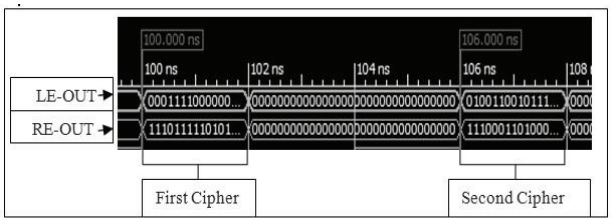

Fig. 4 Simulation results

The encrypted data for the second word appears after 3 clock cycles at 106 ns and so on. However, in case of normal blowfish architecture, there is no need for isolation of data between module blocks, as there is no parallel processing. Hence each module block of the normal blowfish architecture can be designed by using a minimum of 2 levels of registers. This leads to a maximum reduction in the number of registers needed in the normal blowfish architecture. Consequently, the number of clock cycles needed for one operation of a single data word decreases from 49 clock cycles to (16*2)+1 = 33 clock cycles for encryption, owing to 2 levels of registers in each block. Hence the mathematical expressions for required number of clock cycles (C) for the corresponding architectures for N data words are as follows.

C = N * 33 for normal architecture

C = (49 + ((N – 1)*3) for pipelined architecture

Fig. 5 shows that with each successive increase in number of input data words, the pipelined architecture provides the encrypted output in much less amount of clock cycles with respect to normal architecture. The comparative analysis of pipelined architecture with that of non pipelined one is highlighted in table I.

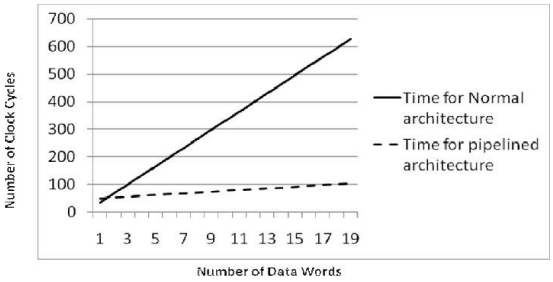

Fig. 5 Number of clock cycles vs number of data word plot

TABLE I. Comparative Analysis of Pipelined vs Non-pipelined Architectures of Blowfish Algorithm

Parameters	Non pipelined design	Proposed Pipelined design
Critical path delay(ns)	3.40	3.383
Frequency(MHz)	294.131	295.63
Throughput(bits/sec)	588.255Mbps	6.3Gbps
Latency(clock cycles)	33	49
Throughput per Slice	0.267Mbps	1.955Mbps

IV. Conclusion

The results of the proposed pipelined architecture for Blowfish algorithm in Verilog HDL show low critical path delay and high throughput at the expense of area as compared with the normal non-pipelined Blowfish algorithm.

References

[1] Bruce Schneier,"Description of new variable length key cipher,64 bit block cipher(blowfish)" ,fast software encryption,Spinger,pp 191-204.

[2] Tingyuan Nie,"A study of DES and Blowfish encryption Algorithm", Tencon 2009-2009,IEEE Region 10 Conference,Vol-2.

[3] S.M Yoo,D. Kotturi,D.W. Pan,J.Blizzard,"An AES crypto chip using ahigh speed parallel pipelined architecture",Elsevier,Microproccesors and Microsystems 29,2005,pp.317-326.

[4] E.J. Swankoski,V.Narayanan,M.Kandemir,M.J. Irwin,"A Parallel Architecture for Secure FPGA Symmetric Encryption", Proceeding of international conference on parallel and distributed processing symposium,April,2004