Development of Pipelined Blowfish Algorithm with Memory based S-Box

Namsangari Madhusudhan¹, P.Padma², Rtd. Prof..Rameshwar Rao³
¹Student of M.E ,ECE,UCE,OU.
² Assistant Professor, UCE,OU.
³UCE,OU.

madhusudhan895@gmail.com

Abstract: The main aim in the design of any encryption algorithm is to provide security against unauthorized attacks. With the fast progression of digital data exchange information security has become an important issue in data communication. Encryption algorithms play an important role in information security system. These algorithms consume a significant amount of computing resources such as CPU time, memory, and battery power. The data encryption algorithms should provide security and also should not be slow in performance because it is a common practice to embed encryption algorithms in other applications. Embedding of encryption algorithms in other applications also precludes a hardware implementation, and is thus a major cause of degraded overall performance of the system. Advanced encryption standard (AES) algorithm is used for protection against various classes of wireless attacks but it consumes more core area and power. Hence, we propose a development of pipelined Blowfish algorithm as an alternative security algorithm. In this paper the pipelined blow fish algorithm with memory based S box (with different memory sizes) has been developed and simulated using Xilinx Ise 14.2 using Verilog HDL using Zynq7000. The memory-based method is used to optimize the performance of Blowfish. The performance is analyzed in terms of its area, power and throughput.

Keyword: CPU, AES, Verilog HDL, Zynq7000

1. Introduction
In Cryptography, the message we are sending is referred as plain text and there will be a key which will be used for encrypting and decrypting the plain text. In cryptography there are Symmetric key cryptography and asymmetric key cryptography based on the keys we are using for encryption and decryption. In Symmetric key cryptography, the key used for both encryption and decryption is same. In Asymmetric key cryptography the keys used for encrypting and decrypting are different.

Blowfish is a symmetric key encryption algorithm which was designed in 1993 by Bruce Schner. It uses same key for encryption and decryption. It is based on the fiestal network in which 16 rounds are present. It has key expansion and encryption/decryption units. Blowfish has a block size of 64 bit and the key length will be from 32 bit to 448 bits. The input 64 bit is divided into 32 bit each. There is a P array with keys P1-P18 which will be generating sub key and there are 16 rounds each implementing F function. F function consists of 4 s boxes with 256 entries each. After 16 rounds the 32 bits generated are combined to get the cipher text. The decryption is reverse of the encryption process.
2. Pipelined Blowfish with Memory based S box

In pipelining, the instructions are fetched and executed parallelly. If there are a series of instructions present, the first instruction is fetched during the first clock cycle. In the second clock cycle, the first instruction will be reading the data and the fetching of second instruction will be done. In this way during a single clock cycle, fetching, decoding and execution of different instructions can be done using pipelining. We introduce registers in the blowfish algorithm before each module. The first module will take raw data as input and the other modules will be working on the data from previous modules. The pipelined architecture has been shown in the Figure 1 in which the registers introduced in between each module that is after each round. The F function present in this uses 4 S boxes with 256 entries each.

![Figure 1. Pipelined architecture](image)

In the proposed method the S boxes are replaced by a read only memory (ROM). In this project we have simulated the pipelined blowfish algorithm with (i) 1024 X 32 bit input ROM which is given in Figure 2 and (ii) 512 X 32 bit input ROM which is given in Fig.3 which are compared in terms of area, throughput and power. In the method with normal S boxes, registers are used and each register will have different clock ,input data. Each register will have its own timing delay which will degrade the speed. In the proposed memory method the 32 bit data is read from ROM at every positive edge of the clock and also requires less number of resources such as LUTs, multiplexers etc.

![Figure 2. 1024 ROM](image)
3. Results
The pipelined blowfish algorithm with 1024 ROM and 512 ROM based memory S boxes are developed and simulated using Xilinx ISE 14.2 using Verilog HDL.

The simulation results of pipelined blowfish algorithm with 1024 ROM based S box and 512 ROM based S box are given in the Figure 4 and Figure 5.

The results are analyzed in terms of area (in terms of number of LUTs utilized), power consumed and throughput. The design with 1024 ROM has consumed more number of LUTs i.e., more area compared to the design with 512 ROM based method. The power consumed by the excess LUTs in design with 1024 ROM has been saved in the design with 512 ROM.
4. Conclusion
Blowfish is a symmetric block cipher that can be effectively used for encryption and safeguarding of data. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for securing data. Blowfish was designed in 1993 by Bruce Schneier as a fast, free alternative to existing encryption algorithms. Blowfish is unpatented and license-free, and is available free for all uses. Blowfish Algorithm is a Feistel Network, iterating a simple encryption function 16 times. The block size is 64 bits, and the key can be any length up to 448 bits. The development of Blowfish algorithm (Pipelined architecture) with memory S box method (with 1024 and 512 ROM) has been done using Verilog HDL. These are compared in terms of area, power, and throughput. The objective of this project is to reduce the area in terms of slices of LUTs and also see that the throughput is increased. In this project Xilinx ISE 14.7 Design suite is used for simulation and synthesis. The block size can be increased to 256 bit by implementing the 128 bit blowfish algorithm by instantiating twice. The pipelined blowfish architecture can be blended with AES to get a hybrid cryptosystem for future works.

References
[1] R. S. Cordova, R. L. R. Maata and A. S. Halibas, “Blowfish Algorithm Implementation on Electronic Data in a Communication Network”, International Conference on Electrical and Computing Technologies and Applications (ICECTA), Ras Al Khaimah, United Arab Emirates, pp. 1-4, 2019.
[2] Nazeh Abdul Wahid MD, Ali A, Esparham B, Marwan MD, “A Comparison of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish for Guessing Attacks Prevention”, J Comp Sci Appl Inform Technol, vol. 3, no.2, pp. 1-7, 2018.
[3] I. A. Landge and B. K. Mishra, “VHDL based Blowfish implementation for secured Embedded System design”, Third International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB), Chennai, pp. 497-501, 2017.
[4] Shraddha Dadhich, “Performance Analysis of AES and DES Cryptographic Algorithms on Windows & Ubuntu using Java”, International Journal of Computer Trends and Technology (IJCTT), Vol.35, no.4, pp.179-183, 2016.
[5] S. S. Kondawar and D. H. Gawali, “Blowfish algorithm for patient health monitoring”, International Conference on Inventive Computation Technologies (ICICT), Coimbatore, pp. 1-6, 2016.
[6] R. Ahmad, A. A. Manaf and W. Ismail, “Development of an improved power-throughput Blowfish algorithm on FPGA,” 2016 IEEE 12th International Colloquium on Signal Processing & Its Applications (CSPA), Malacca City, pp. 237-241, 2016.
[7] Ritu T, Sanjay A. “Comparative Study of Symmetric and Asymmetric Cryptography Techniques”, International Journal of Advance Foundation and Research in Computer, vol.1, no.6, pp.68-76, 2014.