Hardware Implementation of Ciphers

Hari Priya Machiraju
Department of Electrical & Computer Engineering,
Oregon State University, Corvallis, Oregon 97331.
E-mail: machirha@engr.orst.edu

Abstract—
With the rapid growth in computer systems and electronic communications using virtual networks, the demand for a secure encryption has increased and with it the demand for high performance hardware implementations of the cryptographic algorithms. This paper studies the performances of different hardware implementations of cryptographic algorithms present in literature so far, placing emphasis mostly on DES and Rijndael. This aim of the paper is to gain an understanding of the different techniques used in the hardware implementation of the different cryptographic algorithms as well as the optimizations done in speed and throughput. It also discusses a new idea for implementing DES as well as Triple DES making use of afore mentioned designs.

I. Introduction

There are tremendous enhancements going on in the computer systems and electronic communication, which has rapidly changed the way of life of people. The introduction of high speed and bandwidth networking technologies like ATMs and Gigabit Ethernet and their secure encryption led to demand for the execution of the cryptographic algorithms that can handle these high data rates. Much work has been done in this area with the present available hardware implementations performing at speeds higher than 10 Gbps. This paper is going to look at some of these implementations and gain an understanding of the hardware design and architecture involved with an emphasis on DES.

The next section gives a brief description of the DES algorithm followed by the study of the different hardware implementation of DES and looking closely at their speed and throughput. Also a brief overview on the hardware architectures of other algorithms like RIJNDAEL, CRYPTON etc., followed by a conclusion are the different aspects dealt with in the paper.

II. DES Algorithm

DES is a hardware friendly algorithm which lends itself easily to pipelining and simple data manipulations that permit fast operations and thus very suited for the purposes we just talked about in the above section. There are several high speed DES hardware implementations present in the literature.

The DES algorithm is a block cipher which encrypts a 64 bit plain text block using a 56 bit key as its input and gives back 64 bit encrypted cipher text. The basic process of encryption and decryption are the same. Encryption involves an initial permutation then a function f involving XOR ing with a key that has undergone permutation then substitution as well as an inverse initial permutation again giving a final 64 bit cipher text. This is for a basic single round DES [1].

A 16 round DES starts with the initial permutation of the 64 bit plain text, followed by 16 rounds of the encryption and then an inverse initial permutation which gives a 64 bit cipher text. During encryption which is the same in each round, plain text is divided into left and right halves of 32 bits each and right half bits are transformed using the f function and the key which is also halved and permuted and then these are XORed with the left side 32 bits. The key is a subset of the original key in each round and after each round the plain text bits are swapped and the algorithm continues for the remaining rounds.In the f function the right 32 bits are expanded to 48 bits and XORed with the key bits and then go through the S-boxes and then after permutation, we get back the 32 bits of text that are again XORed with the left half and this process after 16 rounds gives the cipher text.

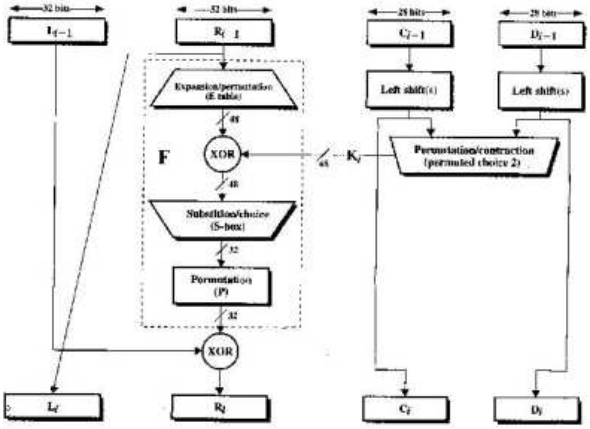

Figure 1: Block Diagram of DES [2]

III. Hardware Implementations and their performance

A. DES

DES has been a popular secret key encryption algorithm standard for AES till recently when it was replaced by Rijndael. It was and is still is used in many commercial and financial applications as it is resistant to all forms of crypto analysis. The algorithms can be software implemented as

Author is a graduate student at the Department of Electrical & Computer Engineering, Oregon State University, Corvallis, Oregon 97331. E-mail: machirha@engr.orst.edu

well as hardware implemented although hardware implementations give a significant improvements in speed by exploiting performance enhancement features like parallelism, by pipelining and other methods like loop unrolling etc,[3]. Application Specific Integrated Circuits (ASIC) are sometimes used for these special type of security applications mainly to reduce the power usage.

The first hardware implementation discussed in the paper is a SNL DES ASIC developed by the Sandia National Laboratories[4]. It was the fastest implementation with a speed that is 10 times faster than the then known currently available DES chips according to a survey by SNL. The speeds then which were less than 0.5Gbps were far below the encryption rates for the ATM encryptions which required speeds of over 10Gbps. The then existing implementations used to iterate data through the hardware of a single round for 16 times to get 16 rounds of DES and this resulted in low throughput and inability for key agility.

The SNL DES ASIC chip is a high speed fully pipelined implementation which provides encryption and decryption with a unique key input. It is an algorithm bypassing on each clock cycle where in for each clock cycle data may be encrypted or decrypted using a unique key or may be passed on without any change. When operated on 64 bit data at 105MHz the throughput was greater than 6.4 Gbps while the simulations showed it capable of speed of over 9.8Gbps.It was fabricated using 0.6 micron CMOS technology and its operational frequency was tested over voltage range of 4.5 to 5.5V with a temperature range of -55 to 125 degrees C and consumed a power of 6.5Watts.

As the design is a fully pipelined design , it took 18 cycles to completely process the data through the pipeline giving proper encrypted and decrypted data and all the key and control input signals also pass through the pipeline and exit the ASIC synchronized to the cipher texts.

The design enhancements identified for this design were to redesign the using Gallium Arsenide (GaAs) technology which will yield a throughput of 30 -40 Gbps with a 3 to 4 factor increase in speed.The authors also suggest many other ways in which these ASICS could be used to get speeds greater than 160 Gbps.

The above architecture also supports Triple DES which for higher speeds can be obtained by cascading multiple SNL DES ASICS to implement in encrypt-decrypt-encrypt mode.In cases where power is the constraint Triple DES can be implemented by iterating DES.

The next implementation of DES discussed in the one proposed by Steve Trimberger et al[1]. This paper describes the implementation and optimization of Encryption and decryption for FPGA core which has a data rate of 8.4 Gbps with 16 cycles of latency and 12 Gbps for 48 cycles of latency and the core takes a key which encrypts and decrypts data both of which may change on a cycle to cycle basis. The design was Verilog simulated and targeted for FPGA.

The implementation uses a multiplexer to select the key bits depending on the round and on whether the data is encrypted or decrypted. Look up tables of 64 x 4 are used for S-box calculations and a pipeline register has also been used to store the results of S-box calculations. The resulting circuit ran at 132Mhz encrypting at 8.4Gbps for a 16 cycles of latency. The speed of this design is approximately three times faster than the then fastest comparable FPGA implementations.

After DES it is Triple DES which was implemented and which is more secure than DES. This paper gives a brief overview of the Triple DES network encrypter by herbert et al [5]. This design is a single chip context agile encryption unit capable for using in high speed ATM networks. This Triple DES algorithm implemented in CBC mode of operation has data rates of above 155Mbps for various DES related algorithms. It is a full custom design methodology using 0.6 Micron CMOS technology and has been verified to have a correct functionality upto a clock rate of 275Mhz.

The network application of this design consists of two modules, a Down - Stream encryption module from where data is sent to the network and a second Up-Stream module which decrypts the receded data from the network and each can perform both DES encryption and decryption, because Triple DES algorithm whit two keys in EDE scheme demands both.It also has two FIFO buffers, FIFO IN and FIFO OUT for collecting data bytewise from an asynchronous interface and asynchronous output respectively. For this design a complete DES encryption -loading takes about 42 cycles, a Triple DES encryption 108 cycles and plaintext loading for 12 cycles. It gives the above mentioned data rate of 155Mbps for a supply voltage of 5.0 Volts at 250Mhz with a safety margin of 25Mhz and for 3.3 Volts at 160 Mhz was verified to give correct functionality.

B. RIJNDAEL

As the technology grew DES was not enough to give sufficient security, thus a new AES was selected by NIST from various algorithms. Thus Rijndael became the new AES in October 2000 replacing DES because of it's enhanced security levels.Henry Kuo et al [6] in their paper discuss different architectural optimizations for the VLSI implementation of the Rijndael algorithm. Rijndael algorithm implementation is more flexible compared to the Des implementations mentions in that this accepts varied block sizes of 128, 192 or 256 bits and can have variable key lengths of 128, 192 or 256 bits as well. A choice of doing encryptions in different rounds 10, 12 and 14 depending on the data and the key length is available. There are two modules to this implementation, one is the encryption module which generates the intermediate encryption data and a key scheduling module which generates the intermediate round keys using the initial key.

In the implementation of the algorithm only one hardware is used for encryption and it is reused to complete the whole encryption process to conserve most area and likewise keys are generated on the fly to reduce the amount of storage for the buffer. Thus this implementation hardware generates one set of subkey and reuses it for calculating all other subkeys and one clock cycle for one subkey generation. But this is the main drawback of the design as the

some of the modules need to be duplicated to get all the required operations done in one clock cycle for one round.

The hardware architecture for the design was described in Verilog XL and synthesized by Synopsis with a 0.18Micron stand cell Library. the results shows that the design has about 173,000 gates and the data encryption can be done at a rate of 1.82 Gbps.

M.McLoone et al in their paper[7] discussed high performance single -chip FPGA implementations of the Rijndael, These designs were implemented on the Virtex-E FPGA family of devices. Their encrypter core was capable of supporting different key sizes, 192 bit key designs which run at 5.8 Gbps and 256 key bit designs which run at 5.2 Gbps. Also the 128 bit key encrypter had a through put of 7Gbps which was then 3.5 times faster than the similar existing hardware designs and was 21 times faster than the then known software implementation and was claims as the fastest fully pipelined single chip FPGA Rijndael encrypter core.

The different specifications of 128-bit key Rijndael Encryption FPGA Implementations as mentioned in the [7].

	Type	Dev	Area	T	T/A
Gaj et al[8]	IL	XCV1000	2902	331.5	0.11
Dandalis et al[9]	IL	XCV1000	5673	353	0.06
Elbirt et al[10]	SP	XCV1000	9004	1940	0.22
McLoone et al	p	XCV812E	2222	6596	3.1

Table 1: Different specifications of 128-bit key Rijndael Encryption FPGA Implementation(T = Throughput ; T/A = Throughput/area)

C. The New DES Implementation

Research is going on in the Oregon State University for the hardware implementations of Ciphers. A new implementation for DES has been designed, which not only implements DES but also Triple DES with a choice for different modes like CBC and ECB. This encrypter core built using a 0.18 Micron technology runs at a speed of 800Mhz with a data rate of 150Gbps for a 16 rounds of DES and at a data rate of 50 Gbps for Triple DES in CBC mode and 40 Gbps for Triple DES in ECB mode at 500 Mhz with a supply voltage of 5.0 volts and a safety margin of 50Mhz for a 64 bit key.

The above Encrypter core mainly consists of the following blocks which are controlled by a control block present in the architecture. There is key agility i.e., different keys of different bit widths(bit widths can be sleeted using a multiplexer) can be used for different cycles using a random key generator and a multiplexer for selection of keys. The next block after key generator block and multiplexors is the encrypter and decryption blocks with a mode selection block and then a control block to control the whole process. Although the area in terms of gates is very large compared o the available implementations, in terms of throughput and speed this has tested to be the fastest so far. The design has been described using VHDL for FPGA implementations.

IV. Conclusion and Future Work

The paper thus discusses some of the important hardware implementations for DES and Rinjdael based on their performance in accordance with their speed and throughput and also a new implementation for DES which is still in it's primary stages has been discussed with future research still going on. Although the newly described design has only been tested for 64 bit keys, research is still going on, on the encrypter core for higher bit lengths. Also research has started on the hardware implementations for the new AES Rijndael as DES is slowly being replaced by Rijndael.

References

[1] Raymond Pang Steve Trimberger and Amit Singh, "A 12 gbps des encryptor/decryptor core in an fpga," in *Cryptographic Hardware and Embedded Systems — CHES'00*, Ç. K. Koç and C. Paar, Eds. 2000, Lecture Notes in Computer Science, No. 1717, pp. 156–163, Springer, Berlin, Germany.

[2] W. Stallings, *Cryptography and Network Security: Principles and Practice*.

[3] P.H.W. Leong O.Y.H. Cheung, K.H. Tsoi and M.P. Leong, "Tradeoffs in parallel and serial implementations of the international data encryption algorithm idea," in *Cryptographic Hardware and Embedded Systems — CHES'01*, Ç. K. Koç and C. Paar, Eds. 2001, Lecture Notes in Computer Science, No. 1717, pp. 333–348, Springer, Berlin, Germany.

[4] Perry J. Robertson Edward L. Witzke D. Craig Wilcox, Lyndon G. Pierson and Karl Gass, "A des asic suitable for network encryption at 10 gbps and beyond," in *Cryptographic Hardware and Embedded Systems —CHES'00*, Ç. K. Koç and C. Paar, Eds. 2000, Lecture Notes in Computer Science, No. 1717, pp. 37–48, Springer, Berlin, Germany.

[5] Udo Payer Karl Christian Posch Reinhard Posch Herbert Leitold, Wolfgang Mayerwieser and Johannes Wolkerstorfer, "A 155 mbps triple-des network encryptor," in *Cryptographic Hardware and Embedded Systems — CHES'00*, Ç. K. Koç and C. Paar, Eds. 2000, Lecture Notes in Computer Science, No. 1717, pp. 164–175, Springer, Berlin, Germany.

[6] H. Kuo and I. Verbauwhede, "Architectural optimization for a 1.82gbits/sec vlsi implementation of the aes rijndael algorithm," in *Cryptographic Hardware and Embedded Systems — CHES'00*, Ç. K. Koç and C. Paar, Eds. 2001, Lecture Notes in Computer Science, No. 1717, pp. 51–64, Springer, Berlin, Germany.

[7] M. McLoone and J.V. McCanny, "High performance single-chip fpga rijndael algorithm implementations," in *Cryptographic Hardware and Embedded Systems — CHES'00*, Ç. K. Koç and C. Paar, Eds. 2001, Lecture Notes in Computer Science, No. 1717, pp. 65–71, Springer, Berlin, Germany.

[8] P.Chodoweic K.Gaj, "Comparison of hardware performance of aes candidates using reconfigurable hardware," in *The Third Advanced Encryption Standards(AES3) Candidate Conference*, 2000.

[9] J.D.P. Rolin A.Dandalis, V.K.Prasanna, "A comparative study of performance of aes candidates using fpga's," in *The Third Advanced Encryption Standards(AES3) Candidate Conference*, 2000.

[10] B.Chetwynd A.J.Elbirt, W.Yip, "An fpga implementation and performance evaluation of the aes block cipher candidate algorithm," in *The Third Advanced Encryption Standards(AES3) Candidate Conference*, 2000.