Indonesian Journal of Electrical Engineering and Computer Science
Vol. 4, No. 1, October 2016, pp. 116 ~ 124
DOI: 10.11591/ijeecs.v4.i1.pp116-124

Quantitative Analysis and Comparison of Symmetric Cryptographic Security Algorithms

Mahaba Saad*[1], Khalid Youssef [2], Hala Abdel-Kader[3]
[1,3]Dept. of Electrical Engineering, Shoubra Faculty of Engineering, Benha University, Cairo, Egypt
[2]Dept. of Communications, Institute of Aviation Engineering &Technology, Aviation Academy, Giza, Egypt
*Corresponding author, email: eng_mahaba@yahoo.com

Abstract

Nowadays, the rapid evolution of communication systems offers, to a very large percentage of population, access to a huge amount of information and a variety of means to use in order to exchange personal data. Hence the search for the best solution to offer the necessary protection against the data intruders' attacks along with providing these services in time is one of the most interesting subjects in the security related communities. Cryptography is usually referred to as "the study of secret". Encryption is the process of converting normal text to unreadable form. There are a variety of encryption algorithms have been developed. This paper provides quantitative analysis and comparison of some symmetric key cryptographic ciphers (DES, 3DES, AES, Blowfish, RC5, and RC6). The quantitative analysis approach is a step towards optimizing the security operations for an efficient next generation family of network processors with enhanced speed and power performance. A framework will be proposed as a reference model for quantitative analysis of security algorithm mathematical and logical operations.

Keywords*: Cryptographic, quantitative analysis, reference model*

1. Introduction

Cryptography is one of the most critical and necessary element of every network infrastructure and communication. It is an important research topic due to the explosive growth in data communications and Internet services. There are five goals of cryptography; confidentiality, authentication, data integrity, non-repudiation, and service reliability and availability. It can be divided into two families: Asymmetric key cryptography; the data is encrypted with the public key and decrypted with private key. Symmetric key cryptography; encrypt and decrypt data by using a single key. These are based on a mathematical function to encrypt a plain-text message and to produce cipher message. In this Paper a quantitative analysis will be conducted on the selected Symmetric key algorithms to abstract the algorithm operations in terms of basic operations that could be directly implemented on arithmetic and logic operator according to current network processor architectures.

The quantitative analysis approach is a step towards optimizing the security operations for an efficient next generation family of network processors with enhanced speed and power performance. In section 3, a framework will be proposed as a reference model for quantitative analysis of security algorithm mathematical and logical operations.

XOR ($\oplus$) operator and rotate shift left are the most importantly used for all cryptographic algorithms, which there are basic operation. Addition modulo 2^{32} (mod 2^{32}) and multiplication Modulo 2^{32} operations are also used for some cryptographic algorithms.

2. Cryptographic Algorithms for Symmetric Block Ciphers

Original data that to be transmitted or stored is called plaintext, which can be readable and understandable either by a person or by a computer. Whereas the disguised data so-called ciphertext, which is unreadable, neither human nor machine can properly process it until it is decrypted. A system or product that provides encryption and decryption is called cryptosystem. Cryptosystem uses an encryption algorithms which determines how simple or complex the

Received April 3, 2016; Revised July 26, 2016; Accepted August 11, 2016

encryption process will be. The security of an encryption system should rely on the secrecy of the encryption/decryption key instead of the encryption algorithm itself, the encryption system will not be able to protect the ciphertext once the algorithm is broken. The security level of an encryption algorithm is measured by the size of its key space. The larger size of the key space is, the more time the attacker needs to do the exhaustive search of the key space, and thus the higher the security level is. Data Encryption Standard (DES), 3DES, Advanced Encryption Standard (AES), Blowfish, RC5, and RC6 are the selected algorithm used for quantitative analysis. Description and function of these algorithms is briefly discussed.

DES [1-2] is the oldest data encryption standard. It operates on blocks of 64-bits in size for plaintext and key. The key actually looks like a 64 bit quantity, but one bit in each of the 8 octets is used for odd parity on each octet. There are 2^{56} possible keys that must be tried to encrypt or decrypt the data block. 56-bit key is used in DES and 16 round of each 48-bit sub keys are formed by permuting 56-bit key. Plainedtext block size of 64-bit is made from L and R blocks of 32-bit. The advantages of DES: any a change of one input or key bit results in changing more than half output bits. Also, each bit of cipher text depends upon multiple bits of plaintext and key. DES is now considered to be insecure for many applications. This is chiefly due to the 56-bit key size being too small; DES keys have been broken in less than 24 hours by Brute force attack in which it consists of systematically checking all possible keys until the correct key is found. There are also some analytical results which demonstrate theoretical weaknesses in the cipher.

3DES [2] is designed to increase the encryption level. 3DES runs three times slower than DES, It also has low performance, 1/3 throughput of DES, or in other words it needs 3 times than DES to process the same amount of data. It is quite slow for hardware and software implementations. But it is easy to implement, secure and very efficient in hardware. It takes three 64-bit keys, for an overall key length of 192 bits (3*64 bit) that eliminates many of the attacks that can be used to reduce the amount of time it takes to break DES. The procedure and operations are exactly the same as regular DES, but it is repeated three times.

AES [2-3] was designed after DES and 3DES, so AES is more secure than them due to the larger-size key. AES operates on a 4×4 matrix of bytes termed as a state. So the strength of AES showed by the combination of security, performance, efficiency, implementation ability, and flexibility. It allows the data length of 128, 192 and 256 bits, and supporting three different key lengths, 128, 192, and 256 bits. AES works with byte quantities so it must be converted into bytes. AES is an iterated block cipher. This means that the same operations are performed many times on a fixed number of bytes. These operations are: ADD ROUND KEY, BYTE SUB, SHIFT ROW, and MIX COLUMN.

Blowfish [5-7] is a symmetric block cipher that encrypts data in 64-bit blocks. The algorithm has two parts, key expansion and data encryption. Eighteen 32-bit sub-keys, and four arrays (the S-boxes), each of size 256 by 32 bits, from a key of at most 448 bits (56 bytes). The data encryption uses a 16-round Feistel Network. The main operations used in Blowfish are XOR and Addition modulo 2^{32}.

RC5 [8-9] is a parameterized algorithm, designated as RC5-w/r/b, where w: word size (in bits), r: number of rounds, b: length of key (in bytes). The allowable value of w is 16, 32 and 64; the allowable values of r and b range from 0 to 255. RC5 is a highly efficient and flexible cryptographic algorithm, for which many parameters (key size, block size, number of rounds) can be adjusted to tradeoff security strength with power consumption and computational overhead. The parameter of RC5-32/12/16 is commonly chosen. There are three operations: words addition, XOR, and data-dependent left rotation of x by y denoted by x <<< y.

RC6 [10] appears to be a useful cryptographic solution that has taken the advantage of RC5 and the AES evaluations. RC6 remains an ideal choice for many high-security and high-performance applications. RC6 encryption, like RC5 parameterized algorithm RC6-w/r/b, (w= 32; (lg(w) = 5), r= 20, and b= 16, 24, or 32). RC6 is based on seven operations like addition modulo 2^w, subtraction modulo 2^w, XOR of w-bit words, multiplication modulo 2^w, Rotate the w-bit word to the left or to the right, and Parallel assignment of values on the right to registers on the left. The addition, subtraction, and multiplication operations use two's complement representations.

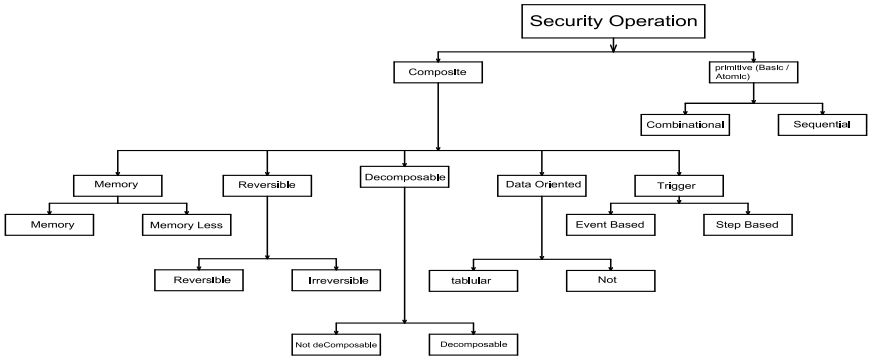

Figure 1. Reference Model of Proposed Security Operation

3. Security Operation Reference Model (SORM) As a Framework for Quantitative Analysis of Algorithms

Any security operation can be described by the reference model, it may classify as a composite or primitive (basic /atomic). The primitive is a simple operation which can be implemented by logic gates, and there are two kinds of atomic operations; combinational logic and sequential logic. Composite operation is computations performed by an algorithm. It can be mapped into one or more basic operation. This operation can be memory or memory less, reversible or irreversible, data oriented tabular or not, event based or step based and decomposable or not decomposable as shown in Figure1. Projection of reference model on cryptographic selected security algorithm operations is listed below.

Reference Model of DES Operations, XOR operation can be classified as primitive, memory less, reversible, and combinational. Rotation Shift Left operation can be classified as atomic, memory (registers of 32bit), clock based, reversible, and sequential. Rotation shift left by two bite is composite operation, memory (registers of 32bit), clock based, reversible, and decomposable. It can be decomposed into more atomic operation like two register for input and output, rotate shift left for shifting one bit and after another clock cycle make second shift. Permutation operation is composite, data oriented table base, memory less, and decomposable. It can be decomposed into more primitive operation like one table, two register for input and output, and one combination. S-Box operation is composite, data oriented table base, memory less, and decomposable. It can be mapped into more atomic operation like 8 s-box table (s1 to s8 table), three register 48bit for input, 4bit for output from s-box table, and 32bit for final output, and 4 combinations, one for grouping of data 6* 8bit, two for selecting row and column, and one for generate final output from this operation. The all reference model of DES algorithm decomposed operations can be summarized in Table 1. The number of each operation used in this algorithm will be found in the following table.

Table 1. Reference Model of All DES Algorithm Operations

Operation	No. of operation in DES	Primitive/Basic/ Atomic	Composite
XOR (⊕)	64	atomic, memory less, reversible, and combinational	
Rotate left shift	4 left shift by one bit	atomic, memory(registers of 32bit) , clock based, reversible, and sequential	
Rotate left shift	12 left shift by two bit		Composite, memory (registers of 32bit), clock based, reversible, and decomposable.
Permutation	16for 32bit input & output , 1 for 64bit input x56bit output, 1 for 64bit input & output, 16 for 56bit input x48bit output, 16 for 32bit input x48bit output, 16 for 64bit input & output		Composite, data oriented table base, memory less, and decomposable.
Des S-Box	16		Composite, data oriented table base, memory less, and decomposable.

Reference Model of 3DES Operations, there are 3 different modes in 3DES; in DES-EEE3 mode (encyrpte plainedtext with k1 followed by another encyrpte with K2 followed by another encyrpte with k3), these are exactly the same as regular DES, but it is repeated three times. The all reference model of 3DES algorithm decomposed operations is the same as DES but number of operations in 3DES is multiply by 3 of DES operations.

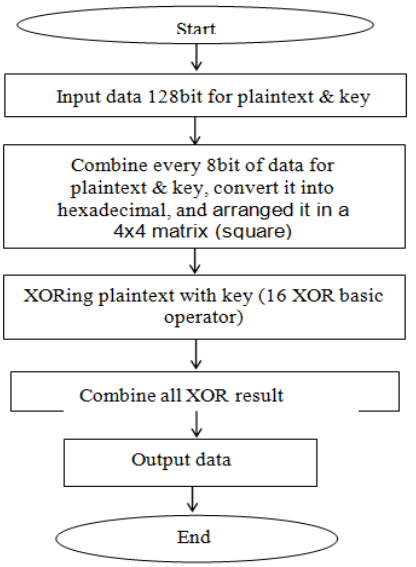

Figure 2. Add Round Key Operation Flowchart

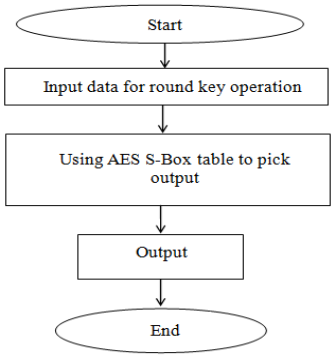

Figure 3. Sub Byte Operation Flowchart

Table 2. Reference Model of All AES Algorithm Operations

Operation	No. of operation in AES (10 round)	Basic	Composite
XOR (⊕)	16 per one round for Add key operation, 48 per one round for Mix Column operation, and 20 per one round for Key Expansion operation	Primitive, memory less, reversible, and combinational	
Rotate left shift (Byte shifter)	1 left shift by 1byte, 1 left shift by 2byte, 1 left shift by 3byte		Composite, not data oriented, memory, and decomposable.
Add Round Key Operation	11		Composite, not data oriented table base, memory less, and decomposable
Sub Byte Operation	10		Composite, data oriented table base, memory less, and decomposable
Shift Row Operation	10		Composite, not data oriented, memory, and decomposable.
Mix Column Operation	9		Composite, data oriented table base, memory less, and decomposable.
Key Expansion Operation	10		Composite, data oriented table base, memory, and decomposable.

Reference Model of AES Operations, add Round Key operation as shown in Figure 2 can be decomposed into more atomic operation like two register for input and output, XOR operator, and 2 combinations, one for grouping of data 16* 8bit to be converted to hexadecimal, and one for generate final output from this operation. Sub Byte operation is composite, it can be decomposed into more atomic operation like AES S-Box table, two register for input and output as shown in Figure 3. Shift Row operation is composite, it can be decomposed into more

atomic operation like 4 register for input and one for output, 5 combination for data byte, and 3 rotate left shift operation (byte shifter not bit shifter) are be listed as one 1byte shifter, 2byte shifter, and 3byte shifter. Mix Column operation is so complex operation. It is composite, It can be decomposed into more atomic operation like two tables L and E, registers for input and output, 5combination, for multiplication operation (16 total multiplications) there are 48 XOR, 64 mathematical addition, and subtraction for hexadecimal value. Key Expansion operation is composite, It can be decomposed into more atomic operation like circular shift, AES S-Box, registers for input and output, 2combination, 20 XOR operator as shown in Figure 4. The all reference model of AES algorithm decomposed operations can be summarized in Table 2.

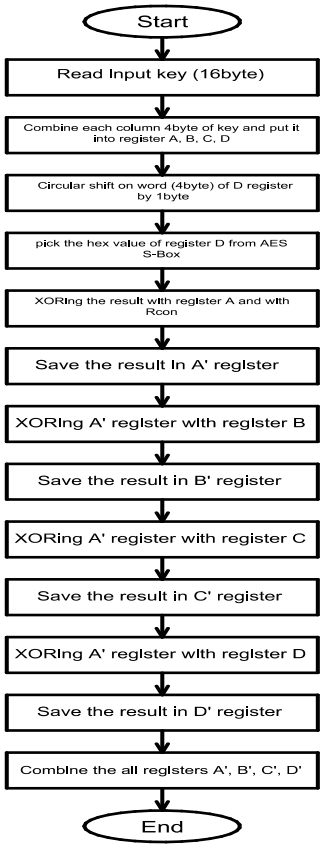

Figure 4. Key Expansion Operation Flowchart

Reference Model of Blowfish Operations, data encryption operation is composite, data oriented table base, memory, and decomposable. As shown in Figure 5, it can be mapped into more simple operations like 4 S-array (4 byte), registers 32bit for input and output, 1 combination for output cipher text, addition mod 2^{32}, subtraction and 50 XOR operation for generate final output from this operation. Key expansion operation is composite, data oriented table base, memory, and decomposable. It looks like data encryption operation, it can be mapped into more simple operations like registers 32 bit for input and output, 4 S-array (4 byte), addition mod 2^{32}, subtraction and 68 XOR operation (18 XORing key with P-array + 50 XOR for data encryption operation) for generate final output from this operation as shown in Figure 6. The reference model of Blowfish algorithm decomposed operations can be summarized in Table 3.

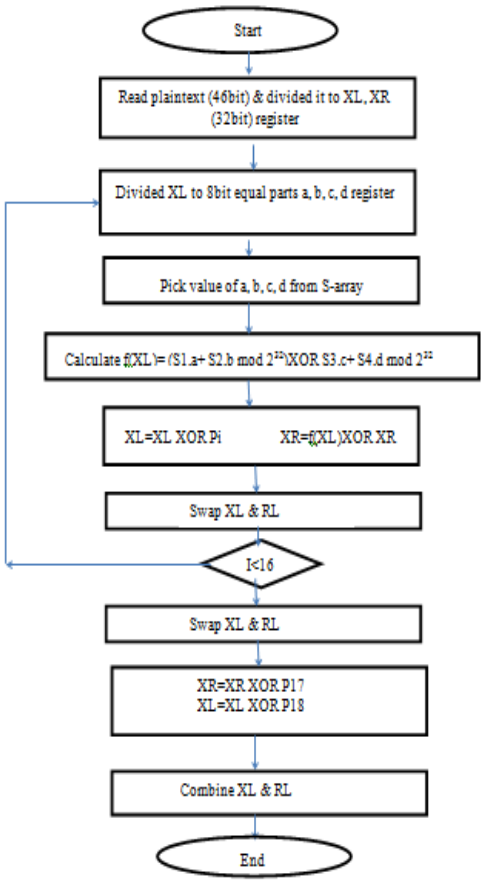

Figure 5. Data Encryption Operation Flowchart of Blowfish Algorithm

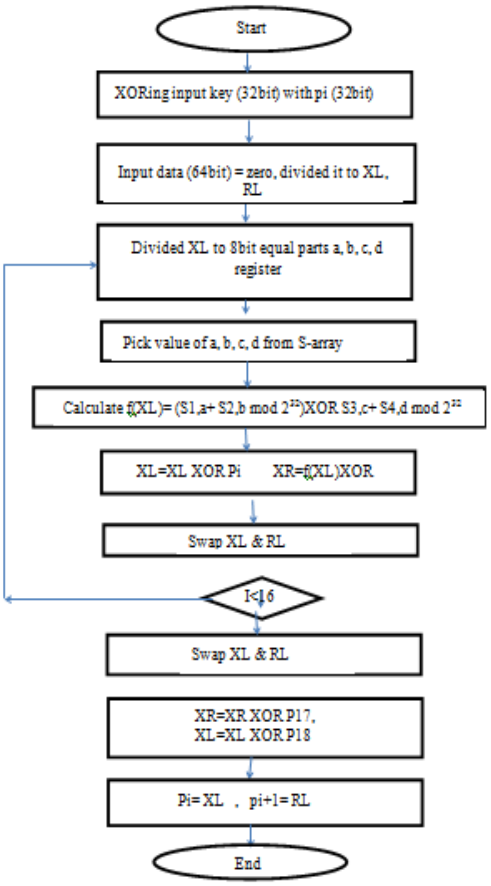

Figure 6. Key Expansion Operation Flowchart of Blowfish Algorithm

Reference Model of RC5 Operations, Data encryption operation is composite, not data oriented table base, memory, and decomposable. It can be mapped into more simple operations like 32bit registers for input and output, 1 combination for output cipher text, addition and subtraction mod 2^{32}, 24 XOR operations, and 24 rotate shift left by different value of LE and RE as shown in Figure 7. Key expansion operation is composite, not data oriented table base, memory, and decomposable. It can be mapped into more simple operations like addition and subtraction mod 2^{32}, registers for input and output, 78(3t=78) rotate shift left by 3 and 78 rotate shift left by unknown variable of X and Y as shown in Figure 8. The reference model of RC5 algorithm decomposed operations can be summarized in Table 4.

Table 3. Reference Model of All Blowfish Algorithm Operations

Operation	No. of operation in Blowfish	Basic	Composite
XOR (⊕)	50 for data encryption operation, 68 for key expansion operation	atomic, memory less, reversible, and combinational	
data encryption	1		Composite, memory (registers of 32bit), data oriented table base, and decomposable.
key expansion	1		Composite, memory (registers of 32bit), data oriented table base, and decomposable.

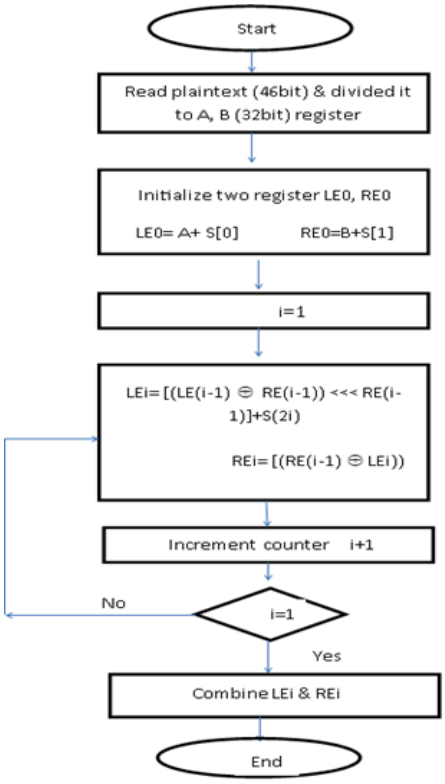

Figure 7. Data Encryption Operation Flowchart with RC5-32/12/16

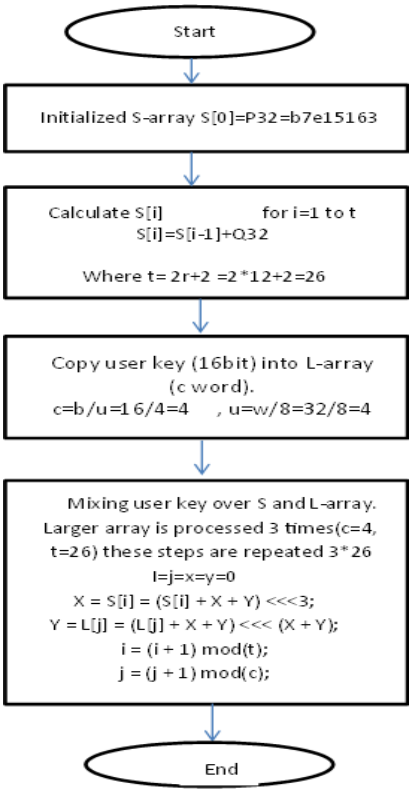

Figure 8. Key Expansion Operation Flowchart of RC5 Algorithm

Table 4. Reference Model of All RC5 Algorithm Operations

Operation	No. of operation in RC5	Basic	Composite
XOR (⊕)	24for data encryption operation	atomic, memory less, reversible, and combinational	
Rotate left shift by unknown variable	24 left shift by unknown variable of RE,LE for data encryption operation, 78 shift by 3 and 78 shift by unknown variable for key expansion operation		Composite, memory, clock based, reversible, and decomposable.
data encryption	1		Composite, memory (registers of 32bit), not data oriented table base, and decomposable.
key expansion	1		Composite, memory, not data oriented table base, and decomposable.

Reference Model of RC6 Operations, Data encryption operation is composite. It can be mapped into more simple operations like 32bit registers for input and output, 1combination for output cipher text, addition, subtraction, and multiplication mod 2^{32}, 40 XOR operation, and 40 rotate shift left by 5 and 40 shifter by different calculated value of u and t. Key expansion operation is composite. It can be mapped into more simple operations like addition, subtraction, and multiplication mod 2^{32}, registers for input and output, 132 rotate shift left by 5 and 132 rotate shift left by unknown variable of A+B. The reference model of RC6 algorithm decomposed operations can be summarized in Table 5.

Table 5. Reference Model of All RC6 Algorithm Operations

Operation	No. of operation in RC6	Basic	Composite
XOR (⊕)	40for data encryption operation	atomic, memory less, reversible, and combinational	
Rotate left shift by unknown variable	40 left shift by unknown variable z, and 40 left shift by 5 for data encryption operation, 132shift by 3 and 132shift by unknown variable p= A+B for key expansion operation		Composite, memory, clock based, reversible, and decomposable.
data encryption	1		Composite, memory (registers of 32bit), not data oriented table base, and decomposable.
key expansion	1		Composite, memory, not data oriented table base, and decomposable.

4. Comparison between Common Operations used in Security Algorithms

A new comparative study between selected algorithms according to reference model of common operations used in these algorithms is listed in Table 6. The structure of DES, 3DES uses fewer types of atomic and composite operations rotate shift left, XOR, and eight 6bit-to-4bit S-boxes. Compared to AES uses byte shifting, XOR, one 8bit-to-8bit S-box, and field multiplication. Also, for RC5 and RC6 uses byte shifting by different value, XOR, addition mod 2^{32}, subtraction mod 2^{32}, multiplication mod 2^{32}.

Table 6. Comparison between DES, 3DES, AES, Blowfish, RC5, RC6

	DES		3DES		AES			Blowfish	RC5		RC6		
No. of round	16		16*3		10			16	12		20		
XOR	64		192		84			118	24		40		
S-Box	16		48		10			-	-		-		
Rotate shift left	1bit	2bit	1bit	2bit	1byte	2byte	3byte	-	3	unknown variable	5	3	unknown variable
	4	12	12	36	1	1	1		78	102	40	132	132
Addition mod 2^{32}	-		-		-			64	26+6+3*78= 286		84+43+3*132= 523		
Subtract from 2^{32}	-		-		-			≤ 16	≤ 12		≤ 20		
Multiply mod 2^{32}	-		-		-			-	-		40		

5. Conclusion

This paper proposes new comparative study between selected algorithms based on a completely defined reference model and framework for security algorithms operations that explained and defined mathematically a framework for common operations used in security algorithms that is better to be interpreted in a new instruction set architecture for next generation network processors. The study held included the following algorithms: DES, 3DES, AES, Blowfish, RC5 and RC6 according to reference model of quantitative analysis for composite and primitive operations. The quantitative analysis approach is a step towards optimizing the security operations; increase overall performance and speed with low area and low power consumption for an efficient next generation family of network processors used for network application like machine to machine (M2M) communication.

References

[1] JO Grabbe. The DES Algorithm Illustrated. http://page.math.tu-berlin.de/~kant/teaching/hess/krypto-ws2006/des.htm.

[2] William Stallings. Cryptography and Network Security: Principles and Practice. Sixth Edition. United States of America: Pearson. 2014.

[3] Douglas Selent. Advanced Encryption Standard. *Rivier Academic Journal.* 2010; 6(2): 1-14.

[4] PGSM Ankita Verma. Comparative Study of Different Cryptographic Algorithms. *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)*. 2016; 5(2): 58-63.

[5] KV Saikumar Manku. Blowfish Encryption Algorithm for Information Security. *ARPN Journal of Engineering and Applied Sciences, 2006-2015 Asian Research Publishing Network (ARPN)*. 2015; 10(10): 4717-4719.

[6] TS Atia. Development of a New Algorithm For Key And S-Box Generation In Blowfish Algorithm. *Journal of Engineering Science and Technology School of Engineering, Taylor's University*. 2014; 9(4): 432-442.

[7] PA Tanjyot Aurora. Blowfish Algorithm. *International Journal of Computer Science and Communication Engineering IJCSCE Special issue on "Recent Advances in Engineering & Technology" NCRAET.* 2013; 3(4): 238-243.

[8] SP Vishnu N. Implementation of RC5 Symmetric Key Encryption Algorithm for Secure Communication. *IJRIT International Journal of Research in Information Technology*. 2013; 1(3): 14-17.

[9] HAS Mowafak Hasan. Modified Cryptanalysis of RC5. *The International Arab Journal of Information Technology*. 2006; 3(4): 299-302.

[10] SS Vikas Tyagi. Enhancement of Rc6 (Rc6_En) Block Cipher Algorithm and Comparison with Rc5 & Rc6. *Journal of Global Research in Computer Science*. 2012; 3(4).

[11] M Sumathi, D Nirmala, R Immanuel Rajkumar. Study of Data Security Algorithms using Verilog HDL. *International Journal of Electrical and Computer Engineering (IJECE).* 2015; 5(5): 1092-1101.