International Journal of advancement in electronics and computer engineering (IJAECE)
Volume 06, Issue 4, May 2017, pp.405-409, ISSN:2274-1412
Copyright © 2012:IJAECE(www.ijaece.com)

Comparative Analysis of RC4 Stream Cipher Using Verilog with Other Ciphers

Vaishali Singh [1], Shriddha Shrivastawa [2]

[1] Student, Department of Electronics & Telecommunication Engineering, Lakshmi Narain College of Technology Bhopal, vaishali.7sep91@gmail.com, India;

[2] Assistant Professor, Department of Electronics & Telecommunication Engineering, Lakshmi Narain College of Technology
Bhopal, shriddha_0606@rediffmail.com, India;

Abstract *– RC4 Stream Cipher, a kind of symmetric cryptography is one of the most famous stream ciphers in the field of Encryption Technologies. It was designed by Ron Rivets in the year 1987 is the most widely positioned commercial stream cipher. Its applications is mostly prominent in the area of network communication where widely used network protocols such as WPA, WEP, SSL and in Secure SQL, Microsoft Windows, Apple OCE, etc. are active. In this project, we have focused on the synthesis and simulation of RC4 algorithm using Verilog and the results can be further compared with the other ciphers. This project compacts with RC4 key stream generator, within the possibility of the model of an exchange shuffle, in order to attain improved safety. The main factors in RC4's realization over such a widespread range of solicitations are its speed and ease of implementation. The RC4 program is written in Verilog language and based on synthesis result it can be further downloaded on FPGA for its hardware realization (if needed).*

Keywords*: RC4, WPA, WEP, KSA, PRGA, FPGA, AES.*

I. Introduction

Cryptography is a world-known art and science of transforming plaintext (actual information or data) into cipher text (encrypted form of data) that stores information in storage or transit. The leading feature of cryptography is to solve the problems, which are related with verification, reliability and confidentiality of the information being transmitted over the electronic media. As the growing use of networks has made us concerned about the security. The mechanism which is needed to guarantee the protection & privacy of data sends between wired or wireless median developed the term cryptography. A protocol is an arrangement of actions, which is planned with two or more sides, through which an objective can be achieved. Cryptography also, is linked with the meaning of protocol. Thus, a cryptographic protocol is itself a protocol which uses cryptography. This procedure uses cryptographic algorithm and aims to cease the attempts of thefts and attacks of viruses. By the use of Theory of Statistics and Theory of Numbers now a day’s cryptography has been technologically advanced and strongly authenticated in science. Many kinds of cryptographic algorithms have been designed in order to solve the problems of leakage of information. The difficulty of these problems offers several categories of cryptographic algorithms. One of the known cryptographic algorithms is the RC4 stream cipher. Normally, security occurs as a result of having a huge number of different alterations.. Cryptography, which is actually a part of cryptology, is further classified as secret codes versus ciphers. Unlike Steganography, where data is concealed within other some unsecured text or data, cryptography pursues to deliver a message unintelligible even if the message is completely exposed. In 1987, Ron Rivest of RSA security designed rc4, consistently entitled as "Rivest Cipher 4", the RC acronym stands for "RON'S CODE". RC4 was initially a profession secret; still it was anonymously posted to the cipher punk’s mailing list in September 1994, due to this it was leaked out in 1994. The purpose of working of cryptography is to transmit the plaintext into a cipher text. Where the original message is called plaintext and coded data is called cipher text.

Plaintext + security key = cipher text.

After some researches on the web to catch a remarkable cryptographic primitive to implement, it has been decided to implement RC4 stream cipher. There are various reasons for choosing this stream cipher. As it is used by really important and prominent network protocols and standards such as WEP, WPA, TSL, SSL, etc. Another cause for this choice is that it is well known for its simplicity and efficiency.

The main objectives of this project are as follows:-

- To Implement RC4 algorithm in hardware description language that too by using Verilog language.
- After the generation of simulation and synthesis result for RC4 Stream Cipher Algorithm it will further compare with the other cipher technologies of encryption.

II. Theory

The basic use of cryptography is to solve complications like authentication, isolation & secrecy.Many types of algorithm were invented to enhance the sustainability of the cryptographic techniques. This project uses RC4 stream cipher due to its appealing features and widespread usage.

Cryptography is additionally categorized in two groups, which is given below

- Asymmetric key
- Symmetric key
    - Block Cipher
    - Stream Cipher

In an asymmetric cryptography, public key is used for the encryption process whereas at the decryption level of the information, private key is being used.

In a symmetric cryptography, for both the process of coding and decoding, a single key is used and that key should be known to both the ends.

Block cipher is another technique of symmetric cryptography which contains encryption of one block of text at a time. Where as in stream cipher, at a time, single bit encrypts.

II.1. Rivest Cipher Algorithms

This algorithm belongs to the family of symmetric key encryption algorithm which was initially invented by Ron Rivest. These algorithms are widely used in many different applications because of their favorable speed and variable capabilities of choosing key length. Though every algorithm has their own pros and cons. There are mainly six Rivest Cipher Algorithms that have been designed so far which are RC1, RC2, RC3, RC4, RC5 and RC6 but out of these only four are being commercially exists which are RC2, RC4, RC5, and RC6.

II.1.1. RC2 Cipher

It's a block encryption algorithm, developed in 1987. This algorithm is considered as a replacement of Data encryption Security which was a symmetric key algorithm. RC2 is a secret key block algorithm technique which uses variable key size from 1 to 128 bytes and the block size of 64 bits is used for both input and output of data. The whole algorithm was designed to take it easily implemented on 16 bit microprocessor.

II.1.2. RC4 Cipher

Bluetooth RC4 is the only Stream Cipher of a Symmetric Key Encryption Algorithm, where at both the ends, same algorithm is used. The whole key stream of data is XORed with the series of generated keys. The generated key stream doesn't depend on the used plain text. In this algorithm, the key length can be varies from 1 to 256 bytes i.e. 8 bits is used to initialize a 256 byte of state table.

Vernam Stream Cipher, a type of Stream Cipher was most widely used which was based on variable key length. It was popular due to its simplicity and mathematically was proven one of the strongest algorithms for the encryption of data.

- RC4 Is Used In Many Commercial Software Packages Such As Lotus Notes & Oracle Secure SQL.
- Now It Has Become The Part Of Some Commonly Used Encryption Protocols And Standards, Including WEP And WPA For Wireless Cards.

.

II.1.3 RC5 Cipher

RC5 is a symmetric block cipher which uses 32/64/128 bits for its encryption process. It was developed in 1994. RC5 cipher is having variable number of rounds, word size and a secret size. It heavily uses data dependent operations. Due to its feature of data dependent rotations, differential and linear cryptanalysis is not possible to perform. If the length of the key is long it will be more secure. However, if the key size is short, then algorithm will be weak.

II.1.4. RC6 Cipher

This algorithm is also based on block stream cipher algorithm and was developed in 1997, last in the series till now. It uses 128 bit block size and supports key sizes of 128, 192 and 256 bytes. It was designed to meet the requirement of the AES i.e. Advanced Encryption Algorithm. It makes use of 4 registers (each of 32 bits).

Being an advanced version of other Ciphers, it is more secure than RC5 but if we will consider all aspects of security, somewhere it is leading to RC4 Cipher someplace it is lacking. It uses fewer rounds and offers higher throughput.

III.Method

Steps of RC4 Algorithm

The steps for RC4 encryption algorithm are as follows:
1) Get the data to be encoded and the selected key.
2) Create two string arrays.
3) Initialize one array with numbers from 0 to 255.
4) Fill the other array with the selected key.
4) Randomize the first array based on the array of the key.

6) Randomize the first array in itself to generate the final key stream.
7) XOR the final (final) key stream with the information or data to be encoded via given cipher text.

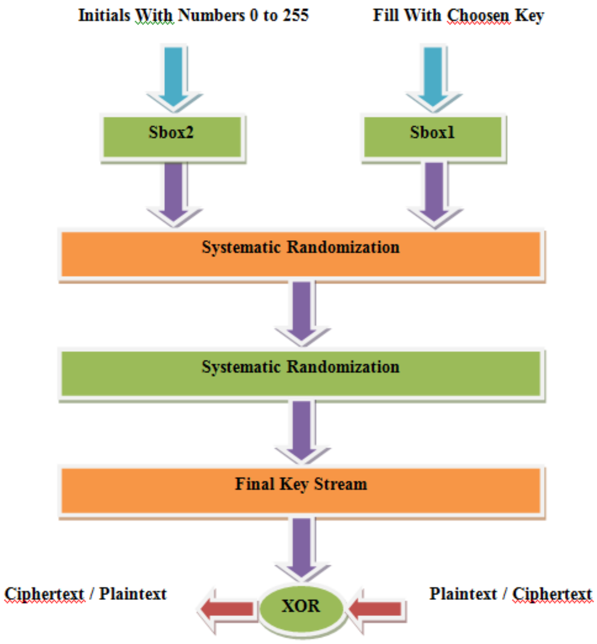


Fig. 1 Flow Diagram of Plaintext to Cipher text

III.1. RC4 STREAM CIPHER

RC4 uses key length which may varies from 1 byte to 256 bytes in order to initiate a 256-byte array. A 256-bytes array contains two types, S-Box and K-Box. The S-array is occupied linearly such as S0=0, S1=1, S2=2………..S255 = 255. The K-array contains the key, repeating as necessary times, so that the array should get complete. The RC4 key is usually restricted to 40 bits, for the reason of export restrictions but it is sometimes used as a 128 bits key. RC4 keys have the ability of using keys between 1 byte and 256 bytes. This algorithm works in two phases, the first phase is the key setup and the second phase is the pseudorandom key stream generation phase. The first and most tough phase is Key setup in this algorithm. The encryption key is used to attain an encrypting variable by utilizing twophases of arrays, first S-array & second is K-array and N-number of mixing operations, during N-bit key setup (N is the length of key). These operations of mixing consist of swapping (exchanging) bytes according to RC4 algorithm. Figure 1 shows the flow diagram of the RC4 two phases. RC4 uses two counters, counter i and the counter j, these are initialized to zero value. In the key setup phase the S-box is being modified according to pseudo-code:

KEY SETUP PHASE:

```
For i= 0 to 255
j = (j + Si + Ki) mod 256
Swap Si and Sj
```

Once the encrypting variables are made from the key setup phase, then it will processed to the pseudorandom key stream generation phase. The following codes provides the pseudorandom key stream generation phase:

KEY STREAM GENERATION PHASE:

```
i = (i+ 1) mod 256
j = (j + Si) mod 256
Swap Si, and Sj
t = (Si + Sj) mod 256
K = Si
```

Where this generated pseudo random code is XORed with the plain text/cipher text to generate cipher text/plain text. Once the receiver’s end gets the encrypted message, he decrypts the encrypted message by XORing with the same encrypting variable.

III.2. Key Scheduling Algorithm

Firstly S-table is initialized which is used to generate the permutation of integer from 0 to 255 bytes. It is initialized by KSA which shuffles *S* using the encryption key *K*.

KSA ALGORITHM

```
For i = 0 to N – l
S[i] = i;
j = 0;
For i = 0 to N-1
{
j = (j + S[i] + k[i]) mod N;
Swap(S[i], S[j]);
i = i + 1
}
```

III.3.Pseudo-Random Generation Algorithm

The algorithm consists of generating a key stream of the size of the message to encrypt. Firstly initialize the two indexes to 0 and then start the generation of the key stream one byte at a time until reached the size of the message to encrypt.

PR GENERATION ALGORITHM

```
i = j = 0;
Generation loop
{
i = (i + 1) mod N;
j = (j + S[i]) mod N;
Swap (S[i], S[j]);
```

Output = S[(S[i] + S[j]) mod N];

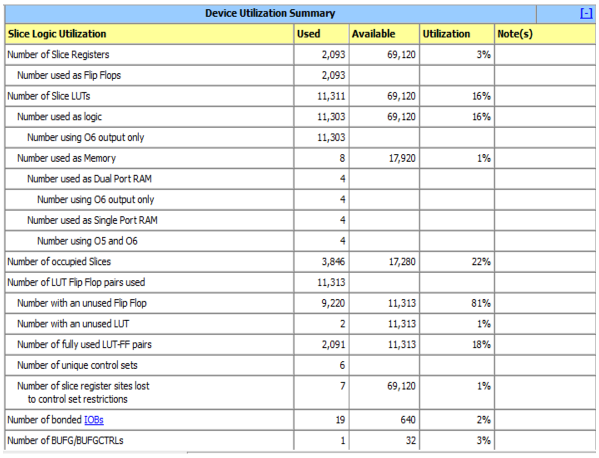
}

IV. Result

To ensure Equations Security Key Generation

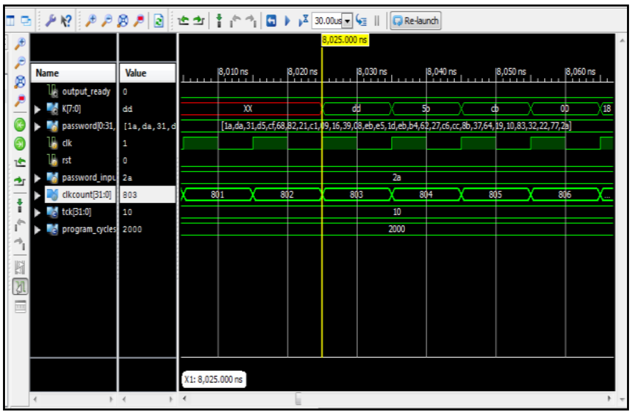
1. Synthesis Result.256 bit

2. Simulation Result. 256 bit.



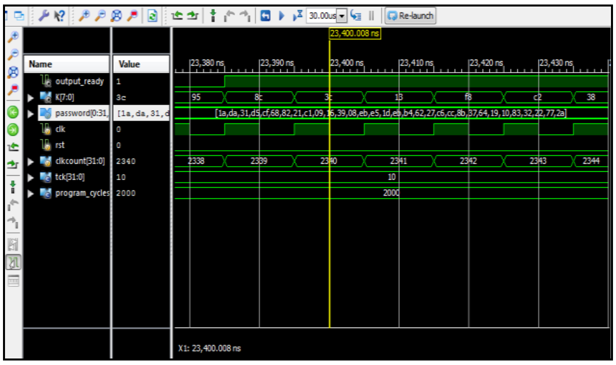
Device Utilization Summary				
Slice Logic Utilization	**Used**	**Available**	**Utilization**	**Note(s)**
Number of Slice Registers	2,093	69,120	3%	
Number used as Flip Flops	2,093			
Number of Slice LUTs	11,311	69,120	16%	
Number used as logic	11,303	69,120	16%	
Number using O6 output only	11,303			
Number used as Memory	8	17,920	1%	
Number used as Dual Port RAM	4			
Number using O6 output only	4			
Number used as Single Port RAM	4			
Number using O5 and O6	4			
Number of occupied Slices	3,846	17,280	22%	
Number of LUT Flip Flop pairs used	11,313			
Number with an unused Flip Flop	9,220	11,313	81%	
Number with an unused LUT	2	11,313	1%	
Number of fully used LUT-FF pairs	2,091	11,313	18%	
Number of unique control sets	6			
Number of slice register sites lost to control set restrictions	7	69,120	1%	
Number of bonded IOBs	19	640	2%	
Number of BUFG/BUFGCTRLs	1	32	3%	

Fig. 2 Synthesis Report For 256 Bit Key Size



Name	Value
output_ready	0
K[7:0]	dd
password[0:31,	[1a, da, 31, d
clk	1
rst	0
password_inpu	2a
clkcount[31:0]	803
tck[31:0]	10
program_cycles	2000

Fig. 3 Simulation Result of 256 Bit Key Generations output Ready Is One



Name	Value
output_ready	1
K[7:0]	3c
password[0:31,	[1a, da, 31, d
clk	0
rst	0
clkcount[31:0]	2340
tck[31:0]	10
program_cycles	2000

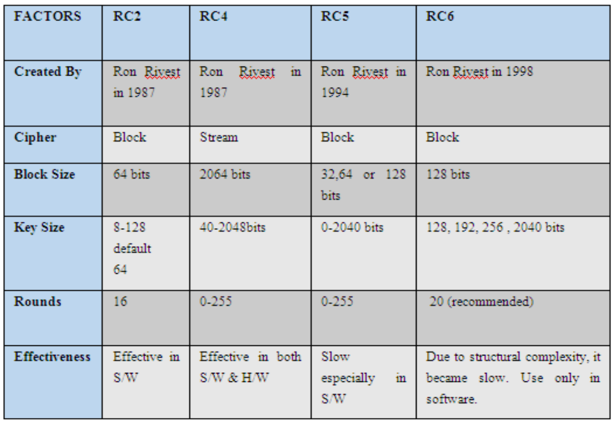
Fig. 4. Simulation Result of 256 Bit Key Generations When Output Ready Is One

IV.1. Advantages of FPGA

- The FPGA devices / element, enhances the security, reliability and performance.
- The encryption & decryption is performed stream wise, the data will remain secured in all respect.
- The FPGA are having the flexibility and high speed capability.
- They can be re-programmed to execute the more estimation intensive operations of a range of ciphers depending on security and application requirements.
- They also offer a better and cost effective solution than any ASIC or VLSI design of longer design cycle.
- Hardware implementation can be better than software in terms of high speed and level of security.

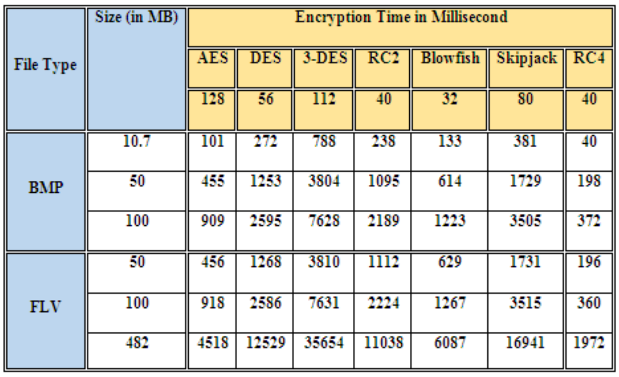
IV.2.Advantages of RC4 Stream Cipher

- This Cipher Is One Of The Most Extensively Used Stream Ciphers.
- It Takes Less Time To Generate The Cipher Text.
- Encryption Is Faster Than The Other Algorithms That Uses Block Cipher.
- RC4 Algorithm Can Easily Synchronize With The Transmission Even If The Data Is Lost.
- It Can Be Implemented In Hardware And Software Both.



FACTORS	RC2	RC4	RC5	RC6
Created By	Ron Rivest in 1987	Ron Rivest in 1987	Ron Rivest in 1994	Ron Rivest in 1998
Cipher	Block	Stream	Block	Block
Block Size	64 bits	2064 bits	32,64 or 128 bits	128 bits
Key Size	8-128 default 64	40-2048bits	0-2040 bits	128, 192, 256 , 2040 bits
Rounds	16	0-255	0-255	20 (recommended)
Effectiveness	Effective in S/W	Effective in both S/W & H/W	Slow especially in S/W	Due to structural complexity, it became slow. Use only in software.

Fig. 5 Comparison with Other Algorithm



File Type	Size (in MB)	Encryption Time in Millisecond						
		AES	DES	3-DES	RC2	Blowfish	Skipjack	RC4
		128	56	112	40	32	80	40
BMP	10.7	101	272	788	238	133	381	40
	50	455	1253	3804	1095	614	1729	198
	100	909	2595	7628	2189	1223	3505	372
FLV	50	456	1268	3810	1112	629	1731	196
	100	918	2586	7631	2224	1267	3515	360
	482	4518	12529	35654	11038	6087	16941	1972

Fig. 6 Encryption Time for Files of Different Sizes

V.Conclusion

By using the Verilog language for the implementation of RC4 Stream Cipher, the design achieves high data throughput using variable key length from 0 bit to 256 bits. This system alsooffers high flexibility as it can be used in many applications. The implementation of this project uses the FPGA platform, the other platforms with various control fundamentals can also be used like Embedded Systems, Digital signal processing technology. The comparative study of RC4 Stream Cipher with all the other Ciphers in different aspects led to the result that RC4 is the most flexible algorithm which can be securely implemented in both software and hardware and due to its simplicity and ease of approach will increases its speed of encryption flexibility in different platform of applications.

References

[1] Hardware Implementation of RC4 Stream Cipher for Wi-Fi Security by Vandana Malode , Nagnath Hulle, Of transaction 8654-34253-434-429 2014 IEEE

[2] P. kitsos, G. Kostopoulos, N. Sklavos and O.Koufopavlou.VLSI design laboratory IEEE Std 802.11. IEEE Standard: Hardware implementation of the RC4 stream cipher.

[3] Claude E. Shannon. Communication theory of secrecy systems. Bell Systems Technical Journal, 28(4):656–715, 1949.

[4] Yi Lu, Willi Meier, and Serge Vaudenay. The conditional correlation attack: Apractical attack on Bluetooth encryption. In Victor Shoup, editor, CRYPTO, volumeYi Lu and Serge Vaudenay. Cryptanalysis of an E0-like combiner with memory. J.

[5] Yi Lu and Serge Vaudenay. Cryptanalysis of an E0-like combiner with memory. J.Cryptology, 21(3):430–457, 2008.

[6] Rourab Paul, Amlan Chakrabarti and Ranjan Ghosh, “Hardware implementation of four byte per clock RC4 algorithm,” in Journal of latex class files Vol. 6 No. 1, Jan. 2007.

[7] Jaya Dofe and Manish Patil, “Hardware implementation of modified RC4 stream cipher using FPGA,” IOSRJEN, vol. 02, Issue 06, pp. 1447–1450, Jun. 2012.

[8] Poonam Jindal and Bramhajit Singh, “A survey on RC4 stream cipher,” IJCNIS, vol. 7, pp. 37–45, Jun. 2015.

[9] Rajendar Racherla and S. Nagakishor Bhavanam, “Design and simulation of enhancing RC4 stream cipher for Wi-Fi security using Verilog HDL,” IJERA, vol. 1, Issue 3, pp. 653–659.

[10] Sultan Weatherspoon, “Overview of IEEE 802.11b security,” Network Communication Group, Intel Technology Journal Q2, 2000.

[11] P. Hamalainen, M. Hannikainen, T. Hamalainen and J. Saarinen, “Hardware Implementation of the Improved WEP and RC4 Encryption Algorithms for Wireless Terminals”, The European Signal Processing Conference (EUSIPCO'2000), September 5-8, 2000, Tampere, Finland, pp. 2289-2292.

[12] P. D. Kundarewich, S. J.E. Wilton, A. J. Hu, “A CPLD- Based RC-4 Cracking System”, The 1999 Canadian Conference on Electrical and Computer Engineering, May 1999.

[13] K.H Tsoi, K.H Lee and P.H.W Leong, “A Massively Parallel RC4 Key Search Engine”, Proc. of the 10th Annual IEEE Symposium on Field-Programmable Custom Computing Machines (FCCM'02), September 22 - 24, 2002 Napa, California, pp. 13-21.