IMPLEMENTATION OF WLAN WEP PROTOCOL BY RC4 ALGORITHM IN VHDL

B. Subhakara Rao[1], M. Prashanthi[2], G. Phani Kumar[3]

[1]*Assistant professor, ECE Department, MIET, Jaggiahpet, A.P, India,* ***subhakararao408@gmail.com***
[2]*P.G Student, ECE Department, S.I.T.S, Khamamm, A.P, India,* ***prashanthi.manukonda@gmail.com***
[3]*Assitant Professor, ECE Department, S.V.E.C, Bobbili, A.P,India,****svpprincipal180@gmail.com***

Abstract

The WLAN is a network that utilizes radio frequency technology. The security of wireless data stream becomes particularly prominent. The WLAN uses RC4 stream encryption algorithm of the WEP protocol to enhance its Security.WEP itself also has fatal Security flaws, tampering with the data for a variety of active attacks. In essence, the problem is not in RC4 itself but in the way to generate the key and how to use the key for RC4 encryption. Many hacker and computer security experts have discovered the WEP design flaws, which indicate that IEEE 802.11 standard can only provide limited support to confidentiality, WEP provides a 40-bit key which may be sufficient to keep away a common hacker but in capable to ward of professional hacker. WLAN has become a hot spot of application in the field of telecommunication. To secure WLAN for data transmission, RC4 algorithm is able to provide the advantages of fast performance resource constrained environment. This paper analyzes the security of RC4 algorithm, presents a way to enhance the security of RC4 algorithm and analysis the affection of the enhanced algorithm. RC4 is probably the most widely used stream cipher now a day due to its simplicity and high efficiency. This paper also focuses on the research to enhance RC4 algorithm that includes analyzes the security of RC4 algorithm, presents a way to enhance the security of RC4 algorithm. The data is encrypted by XOR ing data with the key stream which is generated by RC4 algorithm.

Index Terms: *Cryptography, Field Programmable Gate Array (FPGA), RC4 Algorithm, Message Digest (DM).*

--- *** --

1. INTRODUCTION

Cryptographic algorithms can be divided into three several classes: public key algorithms, symmetric key algorithms, and hash functions. While the first two are used to encrypt and decrypt data, the hash functions are one-way functions that do not allow the processed data to be retrieved. This project focuses on generating secured keys. Currently, the most commonly used hash functions are the MD5 and the RC4. Algorithm with 128-bit output Digest Messages (DMs), respectively. Enhancing Rc4 algorithm for WLAN WEP Protocol is used to send the data in a secured way. In earlier version of this project RC4 algorithm and Hash function were not a part of it and hence it consisted of many drawbacks and it was very easy to hack. This was the main reason to implement the enhanced version of this paper. RC4 is probably the most widely used stream cipher now a day due to its simplicity and high efficiency. This project focuses on the research to enhance RC4 algorithm that includes analyzes the security of RC4 algorithm. RC4 has become part of some commonly used encryption protocols and standards, including WEP for wireless cards the principle of RC4 algorithm consists of two components key scheduling algorithm (KSA) and PRGA. The data is encrypted by XOR ing data with the key stream which is generated by RC4 algorithm Rc4 is standardized to provide security services in WLAN using the WEP protocol. The main objective of this paper is to design and implement Enhanced WLAN by using RC4. Here the data is transmitted in a secured manner from sender to the receiver. The main application of the WLAN is to use the RC4 which is used to enhance its performance. Mainly this application helps us to improve the security level of the data which is being transmitted. As RC4 is probably the most widely used stream cipher. Now days due to its simplicity and high efficiency, the attack on RC4 is also research topic. Depending on the faults in earlier structure, the RC4 and Hash functions have been implemented. The RC4 and Hash helps us to send the data in a secured way. The results are analyzed by simulating the code using Xilinx ISE 9.2i Project Navigator tool.

2. DESCRIPTION OF RC4 ALGORITHM

In cryptography, RC4 (also known as ARC4 or ARCFOUR meaning Alleged RC4,) is the most widely-used stream cipher and is used in popular protocols such as Secure Sockets Layer (SSL) (to protect Internet traffic) and WEP (to secure wireless networks). While remarkable for its simplicity and speed in software, RC4 has weaknesses that argue against its use in new systems. It is especially vulnerable when the beginning of the output key stream is not discarded, non-random or related keys are used, or a single key stream is used twice; some ways of using RC4 can lead to very insecure cryptosystems such as WEP.

Cipher: In cryptography, a cipher (or cypher) is an algorithm for performing encryption or decryption a series of well-defined steps that can be followed as a procedure. An alternative, less common term is encipherment. In non-technical usage, a "cipher" is the same thing as a "code"; however, the concepts are distinct in cryptography

2.1 TYPES OF CIPHERS

2.1.1 BLOCK CIPHERS

In cryptography, a block cipher is a symmetric key cipher operating on fixed-length groups of bits, called blocks, with an unvarying transformation. A block cipher encryption algorithm might take a 128-bit block of plaintext as input, and output a corresponding 128-bit block of cipher text. The exact transformation is controlled using a second input the secret key. Decryption is similar: the decryption algorithm takes, in this example, a 128-bit block of cipher text together with the secret key and yields the128-bit block plaintext.

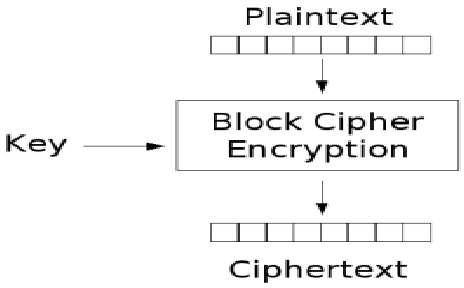


Fig 1 Block Ciphers

To encrypt messages longer than the block size (128 bits in the above example), a mode of operation is used.

2.1.2 STREAM CIPHER

A typical stream cipher encrypts plaintext one byte at a time, although a stream cipher may be designed to operate on one bit at a time or on units larger than a byte at a time. Figure is a representative diagram of stream cipher structure. In this structure a key is input to a pseudorandom bit generator that produces a stream of 8-bit numbers that are apparently random pseudorandom stream is one that is generated by an algorithm but is unpredictable without knowledge of the input key. The output of the generator, called a key stream, is combined one byte at a time with the plaintext stream using the bitwise exclusive-OR (XOR) operation.

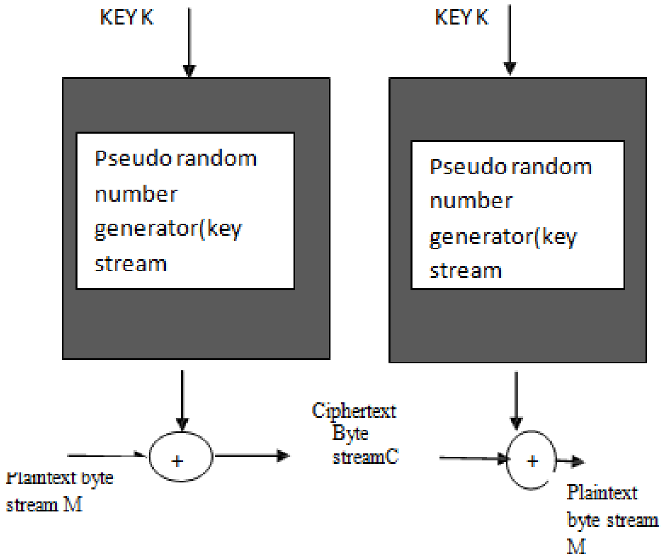

KEY K
KEY K
Pseudo random number generator(key stream
Pseudo random number generator(key stream
+
+
Ciphertext Byte streamC
Plaintext byte stream M
Plaintext byte stream M

Fig 2 Stream Cipher

The encryption sequence should have a large period. A pseudorandom number generator uses a function that produces a deterministic stream of bits that eventually repeats. The longer the period of repeat the more difficult it will be to do cryptanalysis. The key stream should approximate the properties of a true random number stream as close as possible. For example, there should be an approximately equal number of 1s and 0s. If the key stream is treated as a stream of bytes, then all of the 256 possible byte values should appear approximately equally often. The more random-appearing the key stream is, the more randomized the cipher text is, making cryptanalysis more difficult. With a properly designed pseudorandom number generator, a stream cipher can be as secure as block cipher of comparable key length. The primary advantage of a stream cipher is that stream ciphers are almost always faster and use far less code than do block ciphers. RC4 can be implemented in just a few lines of code. The advantage of a block cipher is that you can reuse keys. However, if two plaintexts are encrypted with the same key using a stream cipher, then cryptanalysis is often quite simple. If the two ciphertext streams are XORed together, the result is the XOR of the original plaintexts. If the plaintexts are text strings, credit card numbers, or other byte streams with known properties, then cryptanalysis may be successful. Wireless Local Area Network (WLAN) is the network that utilizes radio frequency technology instead of traditional coaxial.

WLAN is widely used in many conditions, especially when it's difficult to install traditional network. As the openness and sharing of wireless channel nature, the security of wireless data stream becomes particularly prominent .IEEE802.11 standard for WLAN defines two types of authentication open system authentication and shared key authentication, and uses RC4 stream encryption algorithm of the Wired Equivalent Protection (WEP) protocol to enhance its security. However, the facts show that the WEP protocol has not met the desired level of safety.

2.2 RC4 ALGORITHM IMPLEMENTATION

The principle of RC4 algorithm consists of two components: key-scheduling algorithm (KSA) and pseudo-random number generation algorithm (PRGA). The key function of KSA is to complete initialization of RC4Key, while the key function of PRGA is to produce pseudo-random number. The pseudo code for RC4algorithm (KSA and PRGA) is shown below.

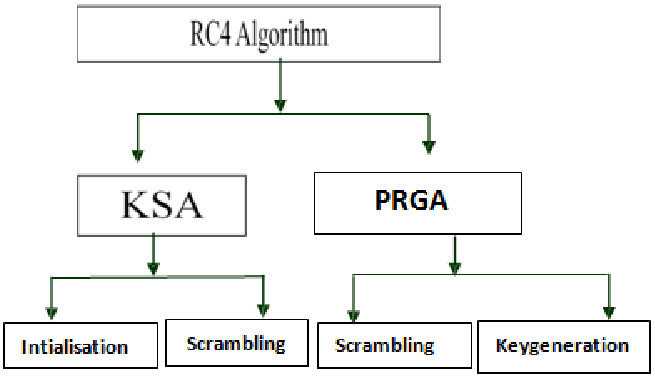


Fig 3 pseudo code for RC4 Algorithm

RC4 is a table based binary additive stream cipher which uses the output word of the key stream generator for its key stream. For most applications the word length is n = 8. RC4 is a unique design for a key stream generator. The large internal memory of RC4 and the dynamic updating of tables imply that RC4 is secure from conventional attacks on key stream generators.

2.2.1 THE KEY-SCHEDULING ALGORITHM (KSA)

The key-scheduling algorithm is used to initialize the permutation in the array "S". "key length" is defined as the number of bytes in the key and can be in the range 1 ≤ key length ≤ 256, typically between 5 and 16, corresponding to a key length of 40 – 128 bits. First, the array "S" is initialized to the identity permutation. S is then processed for 256 iterations in a similar way to the main PRGA, but also mixes in bytes of the key at the same time.

```
for i from 0 to 255
S[i] := i end for

j := 0

for i from 0 to 255

j := (j + S[i] + key[i mod key length]) mod 256
swap(&S[i],&S[j])
end for.
```

3. THE PSEUDO RANDOM GENERATION ALGORITHM (PRGA)

Pseudo random number generator (PRNG), also known as a deterministic random bit generator (DRBG), is an algorithm for generating a sequence of numbers that approximates the properties of random numbers. The sequence is not truly random in that it is completely determined by a relatively small set of initial values, called the PRNG's state. Although sequences that are closer to truly random can be generated using hardware random number generators, pseudorandom numbers are important in practice for simulations (e.g., of physical systems with the Monte Carlo method), and are central in the practice of cryptography and procedural generation.

A PRNG can be started from an arbitrary starting state using a seed state. It will always produce the same sequence thereafter when initialized with that state. The maximum length of the sequence before it begins to repeat is determined by the size of the state, measured in bits. However, since the length of the maximum period potentially doubles with each bit of 'state' added, it is easy to build PRNGs with periods long enough for many practical applications.

If a PRNG's internal state contains n bits, its period can be no longer than 2n results. For some PRNGs the period length can be calculated without walking through the whole period. Linear Feedback Shift Registers (LFSRs) are usually chosen to have periods of exactly 2n−1. Linear congruential generators have periods that can be calculated by factoring. Mixes (no restrictions) have periods of about 2n/2 on average, usually after walking through a non repeating starting sequence. Mixes that are reversible have periods of about 2n−1 on average, and the period will always include the original internal state. Although PRNGs will repeat their results after they reach the end of their period, a repeated result does not imply that the end of the period has been reached, since its internal state may be larger than its output; this is particularly obvious with PRNGs with a 1-bit output.

Most pseudorandom generator algorithms produce sequences which are uniformly distributed by any of several tests. It is an open question, and one central to the theory and practice of cryptography, whether there is any way to distinguish the output of a high-quality PRNG from a truly random sequence without knowing the algorithm(s) used and the state with which it was initialized. The security of most cryptographic algorithms and protocols using PRNGs is based on the assumption that it is infeasible to distinguish use of a suitable PRNG from use of a truly random sequence. The simplest examples of this dependency are stream ciphers, which (most often) work by exclusive or-ing the plaintext of a message with the output of a PRNG, producing cipher text. The design of cryptographically adequate PRNGs is extremely difficult; because they must meet additional criteria (see below). The size of its period is an important factor in the cryptographic suitability of a PRNG, but not the only one.

4. EXPERIMENTAL SET UP

Modern cryptographic technique is divided into two types, symmetric encryption system and public key encryption system. Symmetric encryption system communicating parts need a safe way to ensure key sharing; public key encryption system communicating parts have their own pair of keys.

In general, data processing efficiency of public key encryption system is not as high as symmetric encryption system, but the key is easier to manage. Therefore, we use public key encryption system for both parts to consult and then consult the key, use symmetric cryptography for data encryption and decryption. This maximizes the advantage of two types of cryptography.

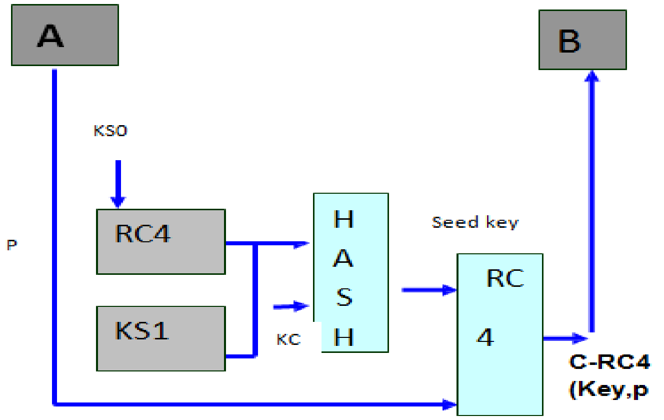


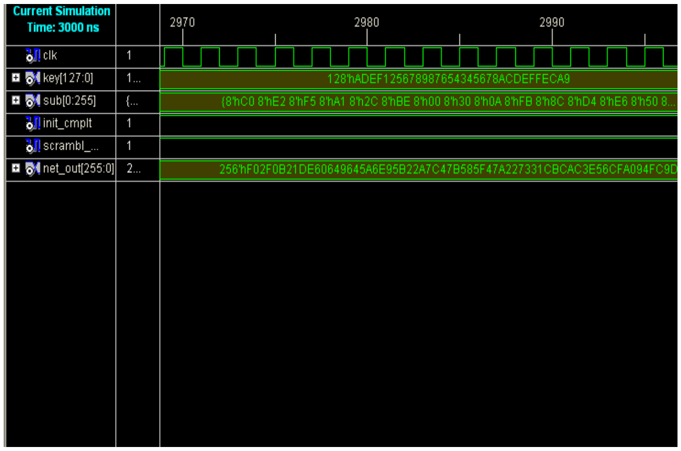
Fig 4. Experimental set up for the RC4 algorithm for WLAN.

The RC4 encryption process is divided into three stages:

1. Session key negotiation stage,
2. Seed key generation stage
3. Data processing stage.

5. RESULTS

The simulation results are from XILINX ISE 9.2i with Model-sim simulator. The results are described as follows.



```
Current Simulation
Time: 3000 ns              2970                    2980                    2990
clk            1
key[127:0]     1...   128'hADEF12567898765434567 8ACDEFFECA9
sub[0:255]     {...   {8'hC0 8'hE2 8'hF5 8'hA1 8'h2C 8'hBE 8'h00 8'h30 8'h0A 8'hFB 8'h8C 8'hD4 8'hE6 8'h50 8...
init_cmplt     1
scrambl_...    1
net_out[255:0] 2...   256'hF02F0B21DE60649645A6E95B22A7C47B585F47A227331CBCAC3E56CFA094FC9D
```

Fig 5. RC4 Algorithm.

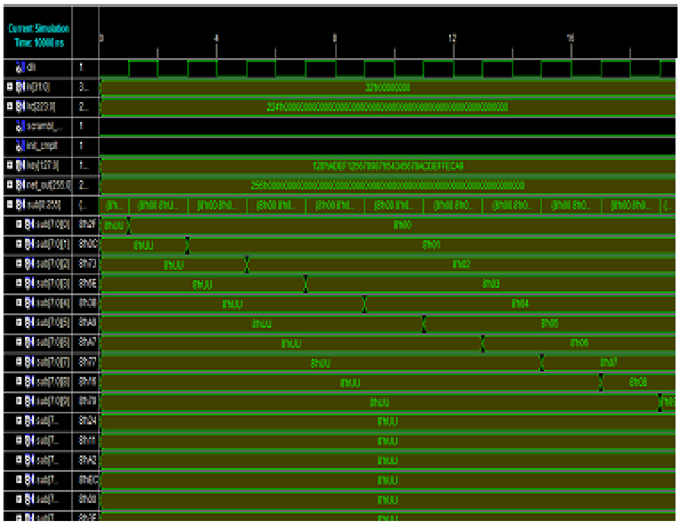


Fig6. Output of S box.

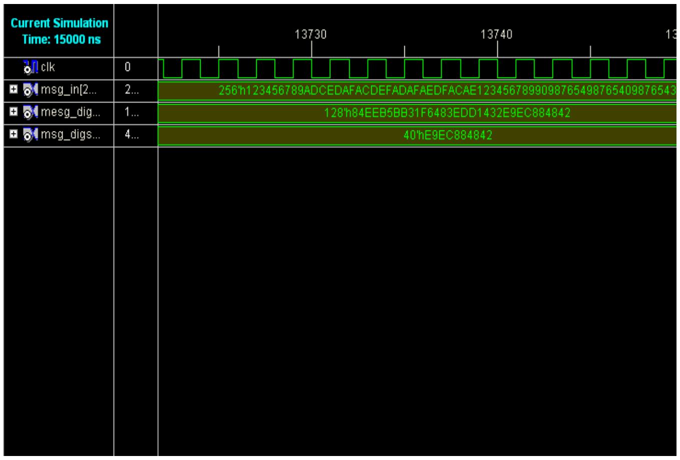


Fig 7. Output of MD5

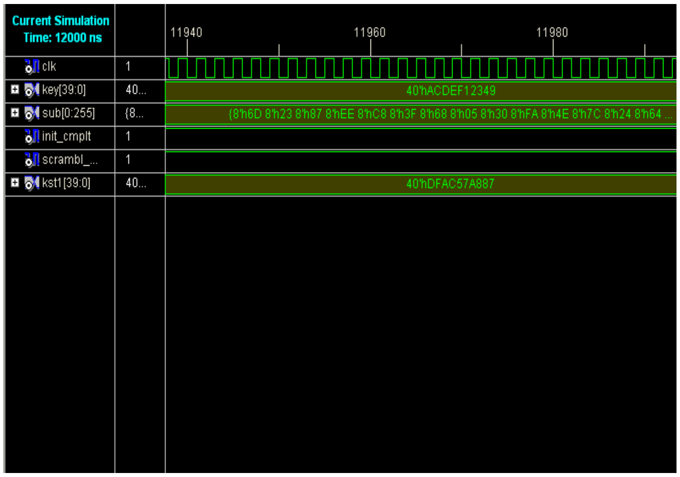


Fig 8 Output of second of RC4.

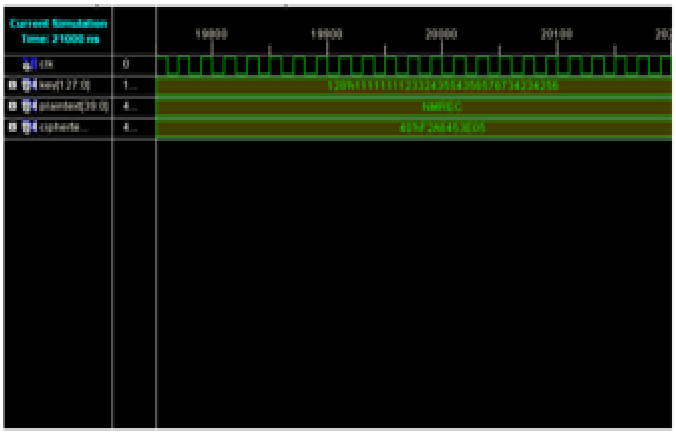


Fig 9. Encrypted Algorithm

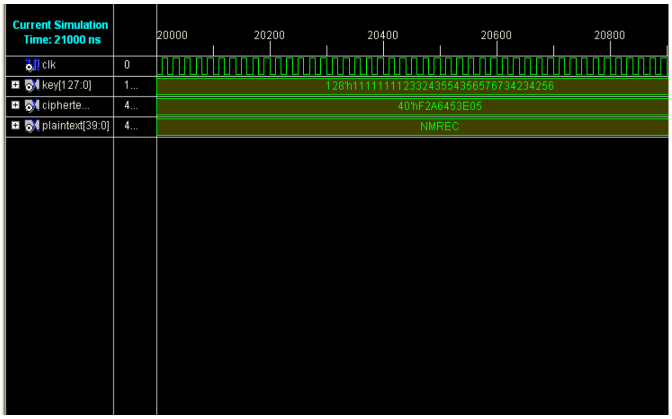


Fig 10. Decrypted Algorithm

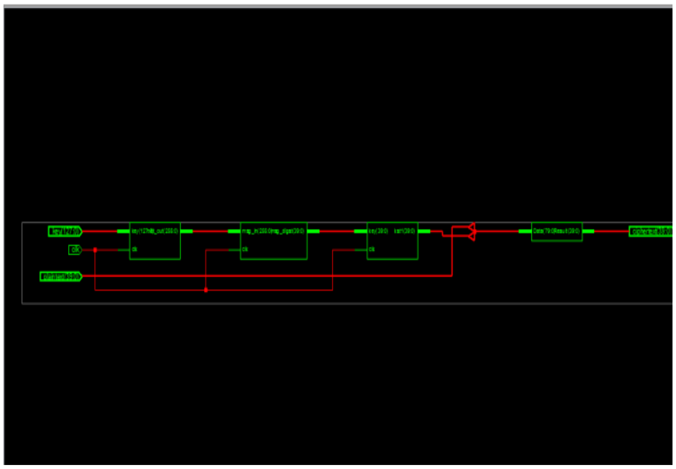


Fig 11. RTL schematic

6. CONCLUSION

The second RC4 algorithm generates key. This key is encrypted with plaintext then Cipher text can be produced .Hence the data can be transmitted in a secured manner from one destination to the other without having any fear of data getting easily hacked. Whenever continuous data transmission is needed one can use this project process to send the data in a secured manner. It has the several applications in the field of the SSL Communication, Rekeying, and Efficient Implementation and in many applications of RC4 requires efficient speed in either software or hardware. It also has the future work in the development of the improved RC4 can raise the security level of WLAN, it can be easy method. The new block encryption algorithm such as RC5 will be used as the security solution for its high encryption level in future. With the implementation of elgamal software, transmission of data will become more secure, it will be very difficult for the hackers to hack the transmitted information.

REFERENCES

[1]. Cryptography and Network security by William Stallings 3rd Edition.

[2]. Martin, Analysis of the stream cipher RC4, Master's thesis (IEEE2010).

[3]. Wireless Local Area networks by S.K. Basandra,S. Jaiswal.

[4]. Rivest, R., "The MD4 Message Digest Algorithm", MIT and RSA Data Security.

[5]. Maocai Wang, Guangming Dai, Hanping Hu, Security Analysis for IEEE802.11.Wireless Communications, Networking and Mobile Computing, 2008.

[6] Enhancing RC4 algorithm for WLAN WEP Protocol By Yao Ya,Jiang Chong, Wang Xingwei in IEEE 2010.

[7] Design of SHA-1 Algorithm based on FPGA by Cheng Xiao-hui, Deng Jian-zhi in 2010.