Implementation of RC4 Algorithm For Secured Wireless Communication

Jadhav Rajashri.k[1], Navale Damayanti.D[2], Phatangare Madhuri.S[3], Rakibe Rakibe.S[4]
[1, 2, 3, 4] Department Of Electronics & Telecommunication Engineering
[1, 2, 3, 4] JSPM's Bhivarabai Sawant Institute Of Technology & Research, Wagholi,

Abstract- *RC4 is a popular stream cipher, which is widely used in many security protocols and standards due to its speed and flexibility. An efficient and high throughput hardware implementation of the RC4 algorithm. The main idea of the proposed architecture is the utilization of a tri-port RAM to reduce the memory resource and to increase throughput. The proposed design requires two clock cycles for generating one byte of ciphering key and uses only a block of 256 bytes RAM. These result in 50% increment of system throughput and three times reduction of RAM resource compared to the recent architectures. The proposed implementation supports variable key length from 8 to 128 bits and achieves 80 MB/s throughput at 160 MHz operating frequency. It aims to support the WEP security in the MAC layer of 600 Mbps 4×4 MIMO wireless LAN system based on IEEE 802.11n standard. The RC4 stream cipher is used in the security protocol WEP in IEEE 802.11b wireless network. The proposed design is also more efficient in terms of power consumption.*

Keywords- RC4 algorithm, RC4's hardware implement, WEP, WLANs security, tri-port RAM, etc.

I. INTRODUCTION

The Rivest cipher algorithm has been proposed by Ron Rivest of RSA security in 1987. It was kept as a trade secret until 1994. The Rc4 algorithm defines a method to generate pseudo random stream of bits, which is called as a ciphering key,from a provided a master key. In today's world of Internet connected computers, every application should consider security the top priority even for stand-alone applications. RC4 is the algorithm of choice because of its ease of implementation and its speed. The data security plays a central role in the design of future IT systems by prohibiting the hacking of confidential information and data in IT system. Cryptosystem can still provide security to protect valuable information.The transmitter and receiver unit is designed by using RC4 algorithm with stream cipher in which the key is secured from hacker. The work with implementation of the system to transmit the information without sending the key for decryption, the key automatically generate at the receiver by the use of pseudo random sequence generator.

A key is input to pseudorandom bit generator that produces a stream of 8 bit numbers that are apparently random. A 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 operation.

RC4 stream cipher [1, 2, 4, 5] is one of the symmetric encryption methods. The symmetric encryption indicates that the transmitter and the receiver share a same key. By using the same key, we can encrypt or decrypt data to achieve confidentiality. In theory, if nobody can discover the key, we can communicate and transmit data securely. Although RC4 is a symmetric cipher, the key which is used in RC4 is not like DES (Data Encryption Standard) or AES (Advanced Encryption Standard) [5], which encrypts or decrypts data with keys directly. The key used in RC4 simply permutes a 256-byte array. Once the permutation procedure is finished, the key is never used again. After that, a byte stream is selected from the 256-byte array in a systematic fashion, and it is used to encrypt or decrypt data. RC4 uses a variable-length key K, where the key length is from 1 to 256 bytes, and a 256-byte array S is used in RC4. In initialization process, let S[i] be i, where i is from 0 to 255, and then we put the variable-length key in a 256-byte array T. If the length of the key K is 256 bytes, then T stores this key. Otherwise, if the length of a key K is L bytes (L < 256), the first L elements of T are copied from K and then K is repeated as many times as possible to fill out T. We use C-language to describe the initialization process as follows.

```
// initial memory
for (i = 0; i <= 255; i++) {
S[i] = i;
T[i] = K[i % L]; }
```

Next, we use T to do initial permutation of S. Thus, the elements in S are still the values from 0 to 255. We use C-language codes to describe this process as follows.

```
// key shuffling
j = 0;
for (i = 0; i <= 255; i++) {
R1 = S[i];
j = (j + R1 + T[i]) % 256;
R2 = S[j];
S[j] = R1;
S[i] = R2; }
```

Finally, we choose 1-byte value from the permuted S, and at the same time swap some two bytes in the S. For the sake of clarity, the corresponding C-language codes are described as follows.

```
// stream generation
i = 0, j = 0;
while (true) {
i = (i + 1) mod 256;
R1 = S[i];
j = (j + R1) % 256;
R2 = S[j];
S[j] = R1;
S[i] = R2;
t = (R1 + R2) % 256;
stream = S[t];
}
```

II. OBJECTIVE OF PROJECT

The objective of secured statistics cryptosystem using stream cipher cryptography for mobile adhoc networks is secure transmission of information between sender and receiver without any involvement of hackers. To secure the data and information in proposed system transmission of key is avoiding in order decrypting the data at the receiver node. The system uses microcontroller and performance of the cryptosystem is analyze by implementing the stream cipher based RC4 cryptographic algorithm

III. LITERATURE REVIEW

P. Israsena, Thailand IC Design Incubator, National Electronics and Computer Technology Center, Thailand Science Park, Thailand. “Design and Implementation of Low Power Hardware Encryption for Low Cost Secure RFID Using TEA” explains about the design and implementation of hardware encryption core for low cost RFID using TEA algorithm. Low cost RFIDs have requirements in terms of cost related to area and power consumption making conventional encryption unsuitable. This paper proposes the use of TEA algorithm for medium security systems. Three new implementations based on multiple single and digit serial adders are designed and evaluated for their suitability. It is found that the multiple adder design meets the requirements with the lowest power consumption. Recently low cost radio frequency identification has been the topic of interest within both academic and industry domains.

Thomas Eisenbarth, Sandeep Kumar and Axel Poschmann, Department of Information Technology,Ruhr University Bochum. “A Survey of Lightweight Cryptography Implementations” explains aboutlight weight cryptography implementations and compares them to state of the art results in their field. This survey covers recent hardware and software implementations of symmetric as well as asymmetric ciphers. Software and hardware implementations are given separately because they have different and sometimes contrary characteristics. For example bit permutations are virtually free in hardware whereas in software they can significantly slow down implementations. Also large substitution tables are often software friendly but hardware realizations can be Recently low cost radio frequency identification has been the topic of interest sensor nodes the energy and storage relatively costly. Finally the evaluation metric is different. For software implementations we compare both RAM and ROM requirements and the required number of clock cycles. For hardware implementations it focused on the required chip size and the number of clock cycles.

Eka Stuwarad, Candra Gunawan, Ary Setijadi, Carmadi Machbub, Laboratory for Control and Computer Systems, Department Of Electrical Engineering, Bandung Institute Of Technology, “First Step toward Internet Based Embedded Control System”explains aboutNetwork has been evolving significantly in last decade. Many computers and devices have been attached to the IP network and many applications were taken place over it .One of interesting applications is building embedded control system which has connectivity to Internet. This paper explains an implementation of embedded web server with security support which becomes an example of control application over IP network. A security algorithm TEA Tiny Encryption Algorithm has been implemented in a microprocessor system together with TCP IP stack. The microprocessor system is based on 8051 family microcontroller which serves as web server. consumptionwithin both academic and industry domains.

Devesh C. Jinwalaldhiren, R. Patelkankar, S. Dasgupta, Department of Computer Engineering, National Institute of Technology, surat“Investigating and Analyzing the Light weight ciphers for Wireless Sensor Networks”explains about the Wireless Sensor Networks are characterized by the severe constraints in the computational storage and energy resources. Though there has been significant improvement in the available computational resources due to the proliferation of the next generation resources of sensor nodes are still limited. As the sensor nodes are often deployed in ubiquitous and pervasive environments. It is necessary to ensure communications security in a WSN. However the use of the security protocols adds to the associated overhead therefore ensuring communications security in a WSN is a challenge. Since the core component of any security protocol is the cipher used the overhead due to a security protocol can be largely reduced by employing lightweight cipher. But at the same time the cipher so employed must ensure appropriate levels of security with standard key sizes.

Dalel BouslimiMember of IEEE Gouenoun CoatrieuxMichel and Christian rouse, Nigeria. “A Joint Encryption/Watermarking System for Verifying the Reliability of Medical Images” explains about the proposes of joint encryption/watermarking system for the purpose of protecting medical images. This system is based on an approach which combines a substitutive water marking algorithm the quantization index modulation with an encryption algorithm a stream cipher algorithm or a block cipher algorithm. Watermarking and encryption are conducted jointly at the protection stage watermark extraction and decryption can be applied independently. The security analysis of our scheme and experimental results achieved on 8 bit depth ultrasound images as well as on 16 bit encoded positron emission tomography images demonstrate the capability of our system to securely make available security attributes in both spatial and encrypted domains.

Nico Dottling Rafael Dowsley Jorn Muller Quade and Anderson C. A. Nascimento, “A CCA2 Secure Variant of the McEliece Cryptosystem” explains about the McEliece public key encryption scheme has become an interesting alternative to cryptosystems based on number theoretical problems. Different from RSA and ElGamal McEliece PKC is not known to be broken by a quantum computer. Moreover even though McEliece PKC has a relatively big key size encryption and decryption operations are rather efficient. In spite of all the recent results in coding theory based cryptosystems to the date there are no constructions secure against chosen cipher text attacks in the standard model the de facto security notion for public key cryptosystems. In this paper we show the first construction of a McEliece based public key cryptosystem secure against chosen cipher text attacks in the standard model.

A. G. Chefranov Eastern Mediterranean University, Famagusta, North Cyprus and Taganrog State University of Radio Engineering, Taganrog “Pseudo-Random Number Generator RC4 Period Improvement” explains about the A new pseudo-random number generator algorithm RC4E, having period significantly greater than RC4 has, is proposed. It is an extension of RC4. It uses RC4 as a main engine and Heap’s algorithm as a second engine, providing enumeration of all possible permutations. Second engine is invoked periodically and it resets the current state of the main engine. Experiments, conducted on the both algorithms, showed their good statistical properties and practically same performance.
Jun-Dian Lee and Chih-Peng Fan,Department of Electrical Engineering, National Chung Hsing University“Efficient Low Latency RC4 Architecture Designs for IEEE 802.11i WEP/TKIP” explains about the novel low-latency RC4 implementations with cell-based VLSI design flow are proposed for IEEE 802.11i WEP/TKIP. The RC4 stream cipher is used in the security protocol WEP in IEEE 802.11b wireless network, and is also used in the TKIP of wireless network IEEE 802.11i cryptography. The major process of RC4 algorithm is to shuffle the memory continuously. For quick memory shuffling, we investigate two different memory shuffling architectures to design the RC4. By using single-port 128x16 memory design, this architecture reduces 25% shuffling latency, compared with the conventional single-port 256x8 architecture. By using dual-port 256x8 memory design, this architecture achieves less latency and less power consumption at the same time. Both of the proposed architectures can reduce much latency in comparison with the conventional single-port 256x8 memory design.

IV. METHODOLOGY

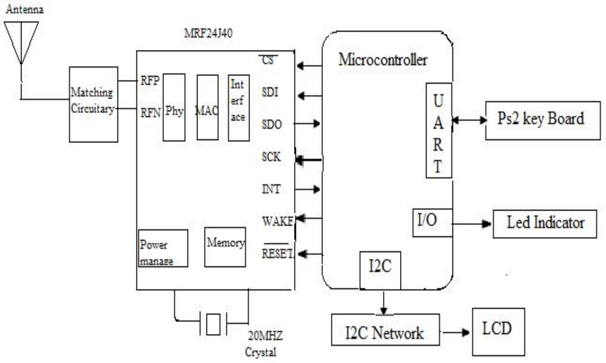


Figure 1. Block dia.of RC4 Algorithm (Transmitter section)

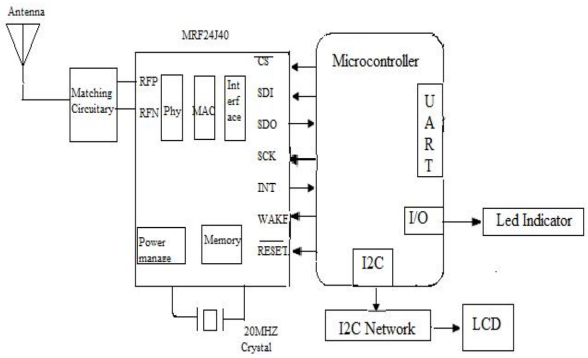


Figure 2. Block dia.of RC4 Algorithm (Receiver section)

PIC Microcontroller

PIC Microcontroller is a low power and high performance 8 bit MCU with peripheral flexibility in a small package for cost sensitive applications in the PIC18J series. It is designed with RISC architecture. The PIC18F45J11 is ideal for applications requiring cost effective low power solutions with a robust peripheral set in a small package. The security algorithm for secure data transmission is written and loaded in the microcontroller. It performs encryption and decryption of data and information at sender and receiver node. The microcontroller unit is connected with UART, I2C, PS2 keyboard and transceiver unit.

LCD

The 14 pin LCD display with 20 rows and 4 columns are used to display the data characters such as string, integer and characters. The encrypted data and respective string of pseudorandom keys are displayed on it.

RF Transreceiver

The MRF24J40MA is a 2.4 GHz IEEE Std. 802.15.4 compliant surface mount module with integrated crystal internal voltage regulator matching circuitry and PCB antenna. The protocol provides reliable direct wireless communication via an easy to use programming interface. The encrypted data and information from sender node is transmitted and received at the receiver through this transceiver in wireless communication medium. The microcontroller unit is interfaced with transceiver for sending the encrypted data and information through transport layer. The crystal oscillator connected with it generates the pulses for performing the operation. The transceiver contains temporary memory unit for fetching the data as well as hold it during busy period of transmission. It also holds the internally generated Pseudo random key. The matching circuitry matches the impedance of transceiver and antenna and transform the data depends upon the transmission medium. In wireless communication the encrypted data stream is changed into radio frequency waves for transmission.

software reuired

MPLAB IDE

The microcontroller has a number of peripheral device circuits on the same chip. Some peripheral devices are called input/output ports. I/O ports are pins on the microcontroller that can be used as outputs and driven high or low to send signals blink lights drive speakers just about anything that can be sent through a wire. Often these pins are bidirectional and can also be configured as inputs allowing the program to respond to an external switch sensor or to communicate with some external device. In order to design such a system it must be decided which peripherals are needed for an application. Analog to Digital Converters allow microcontrollers to connect to sensors and receive changing voltage levels. Serial communication peripherals allow to stream communications over a few wires to another microcontroller to a local network or to the internet. Peripherals on the PIC MCU called timers accurately measure signal events and generate and capture communications signals produce precise waveforms even automatically reset the microcontroller if it gets hung or lost due to a power glitch or hardware malfunction. Other peripherals detect if the external power is dipping below dangerous levels so the microcontroller can store critical information and safely shut down before power is completely lost. The peripherals and the amount of memory an application needs to run a program largely determines which PIC MCU to use.

PICkit 2:

Connecting to the device the PICkit2 is capable of programming a variety of flash-based microchip PIC microcontroller listed in the PIC kit2 readme file on the CD ROM which can also be viewed by selecting help > readme.When the PIC kit2 programmer application a first opened it will attempt to identify the connected device by the device ID and display it in the configuration window.

Figure 3. PICKIT2

Advantages

1. The main advantage of new proposed system is absence of key generation unit and hence it builds up the speed of data transfer.
2. This system is based on symmetric key cryptography which is based on stream cipher bit by bit encryption and decryption of data at sender and receiver node.
3. If the key stream is treated as a stream of bytes then all of the 256 possible byte values should appear approximately equally often
4. The encryption sequence has a large period

Applications

Application Rc4 based cryptosystem

Cryptography system is widely being used to solve problems belonging to data confidentiality, data integrity, data secrecy and authentication and various domains.

Military Application

Cryptographic system for military use depends on degree of security of confidential information. While protecting information from unfriendly eyes, a system must still allow communications to take place rapidly, and to be usable by need to conduct communications. It must be usable under all conditions that the communications must take place. Cryptography provides means to guarantee the following critical issues of information and communication in military services such as confidentiality and integrity.

Monitoring communication

Cryptography provides tremendously robust encryption which can impede the government's efforts to legitimately perform electronic reconnaissance. In order to meet this need, key is escrowed via entrusted third party. This technology allows the use of strong encryption, but also allows the government when legally authorized to obtain decryption keys held by escrow agents.

Authentication Application

Cryptography is closely linked to the theory and practice of using passwords and modern systems often use strong cryptographic transforms conjunction with physical properties.

V. RESULT

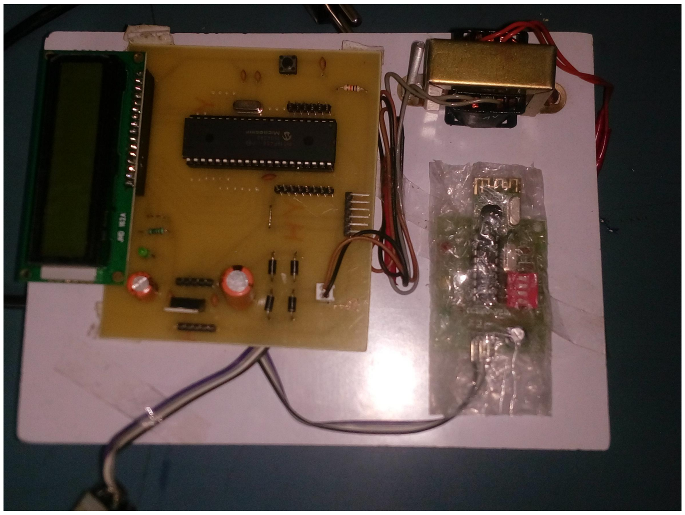


Figure 4.

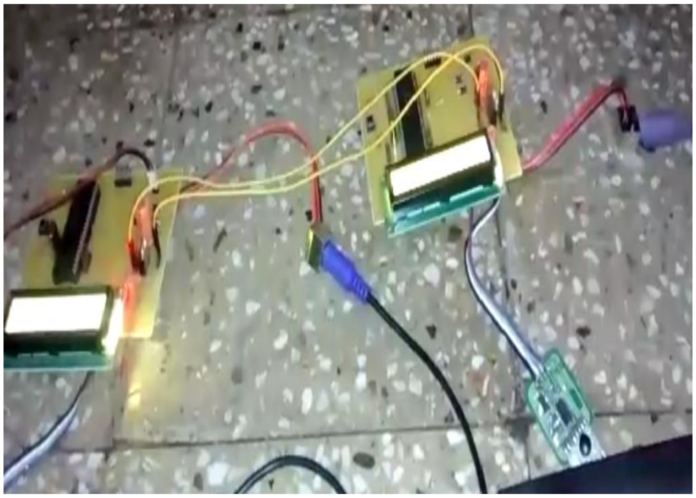
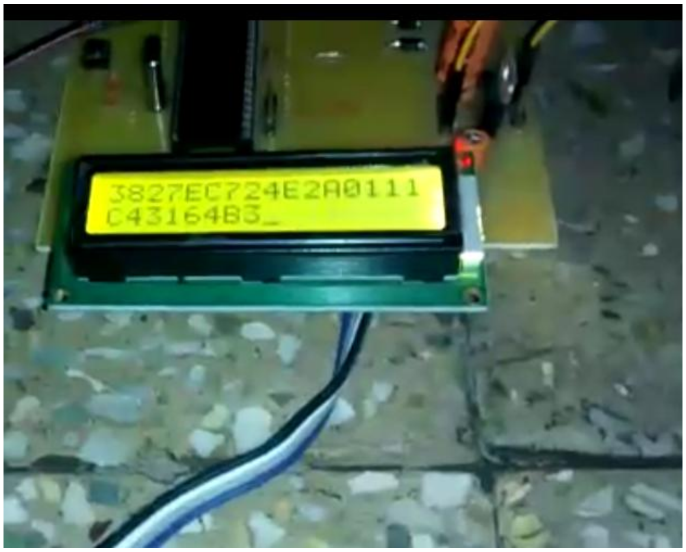


Figure 5.



```
3827EC724E2A0111
C43164B3_
```

Figure 6.

VI. CONCLUSION

Firstly, this paper introduced RC4 stream ciper and several attacks on it. Based on the weakness of the relations between the state of S-box in RC4, we present an improved RC4 in this paper. The new algorithm has destroyed the relations. The new algorithm enchanced the security of RC4, and it is faster than RC4. However, whether the improved RC4 has other loopholes remains to be tested.

REFERENCES

[1] An Improved RC4 Stream Cipher Jian Xie, Xiaozhong Pan Department of E lectronic Technology E ngineering College of Armed Police Force Xi' an, China

[2] Efficient Low-Latency RC4 Architecture Designs for IEEE 802.11i WEP/TKIP Jun-Dian Lee and Chih-Peng Fan* Department of Electrical Engineering, National Chung Hsing University, 250 Kuo-Kuang Road, Taichung 402, Taiwan, R.O.C.

[3] Hardware Implementation of High Throughput RC4 Algorithm Thi Hong Tran, Leonardo Lanante, Yuhei Nagao, Masayuki Kurosaki, Hiroshi Ochi Dept. of Computer Science and Electronics, Kyushu Institute of Technology, 680-4 Iizuka Fukuoka JAPAN

[4] Mantin, A. Shamir, "A Practical Attackon Broadcast RC4," FastSoftware Encryption 2001 (M.Matsui,ed.), vol.2355 of LNCS, pp.152-164, Springer-Verlag, 2001