Microcontroller Based Cryptosystem using RC4 Algorithm

Gaurav Pal
Department of Electronics and Telecommunication
Sinhgad College of Engineering, Pune, India
Email: palgaurav972@gmail.com

Prof. U R More
Department of Electronics and Telecommunication
Sinhgad College of Engineering, Pune, India
Email: urmore.scoe@sinhgad.edu

Abstract – The data security plays a very important role in wireless communication systems. Embedded based applications need sensitive data transfer between different nodes. In order to increase the Security and to reduce the hardware complexity, this proposed system focuses on the Efficient RC4 Algorithm which can be implemented in PIC microcontroller to adapt with many real time constraints such as encryption time, decryption time and secrecy of cipher. The additive feature of this proposed system is uses two input keys to make it optimal for sensitive data transfer between sender and receiver in real-time applications. The work extends with implementing the wireless transmission (RF) to transfer the data from encryption unit to decryption unit.

Keywords – Data Encryption, Data Security, Efficient RC4, RC4 Modifications, Secrecy Of Ciphers, Stream Cipher.

I. INTRODUCTION

Many of data security applications are realized as embedded systems which rely heavily on security mechanisms. The large shares of those embedded applications are wireless communication channel. Cryptosystem can provide security to valuable information. The idea of the work is to prohibit the hacking of confidential information and data in communication system which increases the reliability of communication system. In proposed system RC4 cipher is using two keys for data encryption and decryption. The work is intended to implement the system, which transmits the information without sending the original decryption keys. At the transmitter node input keys are combined as, one byte at a time with the plaintext stream using the bitwise exclusive OR operation. At the receiving end decryption unit use same input keys to generate original text from cipher text. Improvement in performance of algorithm is obtained by the Improved RC4 cipher, which is based on RC4A [1]. RC4A has eliminated most of the known attacks on RC4. So, it was selected to be combined with another simple modification of RC4 algorithm, which is named “A Modified RC4 cipher” [2], the particular combination, will output an efficient and secure modification of RC4[3].

II. DESCRIPTION OF RC4

RC4 is a stream cipher design in 1987 by Ron Rivest. While it is officially termed ’Rivest Cipher 4′, the RC4 algorithm is also known as ‘Ron’s Code’. RC4 algorithm generates a pseudorandom stream of bits (key stream). As with any stream cipher, these can be used for encryption by combining one bit at a time with the plaintext stream using the bit-wise exclusive-or(XOR); decryption is performed in same way (exclusive-or(XOR) with given data). For generation of key stream, cipher makes use of a secret internal state which consists of two parts:

i) A permutation of all 256 possible bytes (denoted “S”)

ii) Two 8-bit index-pointers (“i” and “j”).

The permutation is initialized with a variable length key, it may be between 40 to 256 bits, by the use of key-scheduling algorithm (KSA). Once this has been completed, the stream of bits is generated using the pseudo-random generation algorithm (PRGA).

Key scheduling algorithm (KSA):

The key-scheduling algorithm is use for initialization the permutation of “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 5–16, 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 [4].

Pseudo random algorithm (PRGA):

For as much iteration as are needed, the Pseudo random algorithm modifies the state and outputs byte of the key stream. In each iteration, the PRGA increments i, looks up the element of S, S[i], and adds that to j, exchanges the values of S[i] and S[j], and then uses the sum S[i] + S[j] (modulo 256) as an index to fetch a third element of S, (the key stream value K) which is XORed with the next byte of the message to produce the next byte of either cipher text or plaintext. Each element of S is swapped with another element at least once every 256 iterations [4].

III. ATTACKS ON RC4

Many cryptanalysis of RC4 emerged after the algorithm was made public in 1994. The cryptanalyses was divided into two parts, analysis of the initialization of RC4 which focuses on the initialization of KSA and analysis of the key stream generation which focuses on the internal state and the round operation of PRGA. The most serious weakness of RC4 that the probability of a zero output byte at the second round is twice as large as expected. The RC4 could be attacked completely if we can know portion of the secret key [5]. There is a Probabilistic correlation between the secret information and the public information which is which is found by Maitra Jenkins and Paul discovered the secret key from the initial state table using
biases in the first entries of the table [6]. They created some equations by the initial state table. They guess some of the bytes of the secret key and they obtain the rest of the key by using these equations. In 2007 introduces a statistical relation between output byte and the value of SOI at the time of the output generation [7]. Violeta Tomasevi and Slobodan Bojani introduced an abstraction in form of general conditions for cryptanalytic managing of the information about the current state of the RC4 stream cipher. The general strategy is used to favour more promising values that should be assigned to unknown entries in the RC4 table. Paul and Preneel have formally proved that only known elements of the S-box along with two index-pointers cannot predict more than a output bytes in the next N rounds [8]. They have also designed an efficient algorithm to deduce certain special RC4-states known as Non-fortuitous Predictive States.

IV. PROPOSED RC4 ALGORITHM

RC4 chooses a secret key k which is called the seed, and array S called S-box which contains N (N=2^n) elements (usually N=256, n=8). RC4 also contains two algorithms: KSA and PRGA. The KSA is Key Scheduling Algorithm. KSA, the S-box is filled from 0 to N-1. The PRGA is Pseudo Random Generation Algorithm. So, in this proposed work, the two algorithms improved and modified rc4 are combined for obtain a faster and secure RC4 stream cipher. The combination is done in the PRGA. So, the Key Scheduling Algorithm (KSA) in Improved RC4 remains the same in this cipher too. In PRGA generate use two random keys (k1 and k2) and use exclusive OR with cipher text or plain text.

DESIGN STEPS OF RC4 ALGORITHM:

STEP 1. INITIALIZATION OF S

To begin, the entries of S are set equal to the values from 0 through 255 in ascending order that is S[0] = 0, S[1] = 1, ..., S[255] = 255. A temporary vector T is also created. If the length of the key K is 256 bytes then K is transferred to T. Otherwise for a key of length, the first key length elements of T are copied from K and then K is repeated as many times as necessary to fill out T. These preliminary operations can be summarized as follows:

/* Initialization */
for i = 0 to 255 do
S[i] = i;
T[i] = K[i mod keylen];

STEP 2. INITIAL PERMUTATION

Temporary vector T is used to produce the initial permutation of S which involves starting with S[0] and going through to S[255], and, for each S[i], swapping S[i] with another byte in S according to a scheme dictated by T[i].

/* Initial Permutation of S */
j = 0;
for i = 0 to 255
j = (j + S[i] * k[i]) mod 256;
Swap (S[i], S[j]);

STEP 3. STREAM GENERATION

Stream generation involves starting with S[0] and going through to S[255] and for each S[i], swapping S[i] with another byte in S according to a scheme dictated by the current configuration of S. After S [255] is reached, the process continues starting over again at S [0].

/* Stream Generation */

Optimization

for x = 0 to L-1
i = (i+1) mod 256;
j = (j+S[i]) mod 256;
Swap S[i] and S[j];

Generated Key 1 = S ([S[i] + S[j]) mod 256];
Generated Key 2 = S ([S[i] + S[j]) mod 256];

PRGA (pseudorandom generation algorithm) , which is generate key stream k1and k2, key stream k1 is combined as one byte at a time with the plaintext stream using the bitwise exclusive OR operation. And the output (k1 XOR plaintext) of this operation will again exclusive OR with k2 which give the final output.

Output = M[x] XOR Generated Key 1;
Output = N[x] XOR Generated Key 2;

(Where ‘M[x]’ is the plain text message, ‘N[x]’ is the output of the plain text M[x] and key1 and ‘L’ is its length. At the receiving end decryption unit use same keys to generate original text from cipher text.)

V. BLOCK DESCRIPTION OF PROPOSED WORK

The main block diagram of “MICROCONTROLLER BASED CRYPTO SYSTEM USING RC4 ALGORITHMM” is depicted in Figure 1 and 2, which shows the complete operation of system. The principle feature of this system is usage RC4 algorithm. The security algorithm is chosen in such way that it occupies reduce area and time constraints with high performance. RC4 algorithm is implemented in PIC microcontroller which performs secure data transmission from sender to receiver with CC2500 RF wireless transceiver. Overall system contains two nodes.

i) Data transmitting node
ii) Data receiving node
Different blocks interconnect are:

i. KEYBOARD: The input data is given through PS2 keyboard to microcontroller.

ii. MICROCONTROLLER: RC4 algorithm is implemented on PIC18F458 platform to perform cryptography.

iii. TRANSCEIVER: CC2500 RF transceiver is used to transmit and receive the encrypted data through wireless communication.

iv. ANTENNA: Antenna is used to transmit and receive the data.

v. LCD DISPLAY: The 16X4 LCD is used to display the output plain text and cipher text.

This project relates to communications and more particularly to wireless cryptographic communication systems and methods. Its purpose is to integrate the area of wireless embedded communication systems and cryptography. The system can transfer any type of file using the wireless Communication (RF transmission) in proposed work, cryptography is implemented only to text files due to the limitation of memory and processing speed of an 8 bit PIC microcontroller. The radio operates CC2500 transceiver use to transmit and receive secure data between sender and receiver, at radius of 15-30m unlicensed Industrial Scientific and Medical band. The wireless communications channel is coupled with encoding and decoding device. The PIC microcontroller acts as the encoding and decoding device. A message to be converted is plain text to cipher text at the encoding terminal and cipher text to plain text at decoding terminal by means of efficient RC4 stream cipher algorithm.

VI. EXPERIMENTATION

The proposed system has two nodes transmitter and receiver, both sections consists of PIC microcontroller, transceiver, keyboard, and LCD display. At the transmitting node the input data (plain text and input keys) is provide through PS2 keyboard, PS2 keyboard has two signals includes both clock and data. The protocol has 11 bits, one start bit (0), eight data bits, one parity bit and one stop bit (1). The data is valid during the low period (after falling edge) of the clock pulse or we can say data is receiving at every falling edge of clock signal. The keyboard will count 10 clock pulses. After the tenth bit, the keyboard checks for a high level on the data line (the stop bit), and if it is high, it forces it low. When a key is pressed, this word is transmitted; keyboard also sends a break code when a key is released. The break code for most characters happens to be 0xF0 followed by the code for the key. Code is stored in an array. For example, the 'a' key has a scan code 0x1C (this is a way of saying 1C in hexadecimal, which is 28 in decimal or 00011100 in binary). After the getting the data from PS2 key board, Microcontroller perform RC4 encryption algorithm which is implement on it. RC4 algorithm generates key stream k1 and k2 with the help of input keys, key stream k1 is combined as one byte at a time with the plaintext stream using the bitwise exclusive OR operation. And output of this operation (k1 XOR plaintext) will again exclusive OR with k2 which gives the final output as cipher text. After the encryption, encrypted data is sent through the wireless transmitter. We are using CC2500 wireless transceiver for communication between transmitter and receiver. CC2500 supports fixed packet length protocols. Fixed packet length mode can be used for packets up to 255 bytes. In proposed system we are sending fixed data packet between 10 bytes to 30 Bytes of data. The radio operates CC2500 transceiver is able to transmit and receive secure data between sender and receiver, in radius of 15-30m unlicensed Industrial Scientific and Medical band. At the receiving end encrypted data (cipher text) is collect through RF receiver, at this node Microcontroller acts as a decryption unit and starts decryption process with the key generation followed by input keys and cipher text. Microcontroller decrypts this cipher text into original text when provides correct input keys through PS2 keyboard.

Example-

The encryption process at transmitting node is shown in Table I. Input text “Hello” word is converted into cipher text using the 4 digits two input key.

<table>
<thead>
<tr>
<th>Input text</th>
<th>Input key 1</th>
<th>Input key 2</th>
<th>Cipher Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hello</td>
<td>!@#$</td>
<td>a@12</td>
<td>xxxxx</td>
</tr>
</tbody>
</table>

The decryption process at receiving node is shown in Table II. Cipher text “xxxxx” is converted into original text when correct 4 digits two input keys were applied.

<table>
<thead>
<tr>
<th>Cipher Text</th>
<th>Input key 1</th>
<th>Input key 2</th>
<th>Original Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>xxxxx</td>
<td>!@#$</td>
<td>a@12</td>
<td>Hello</td>
</tr>
</tbody>
</table>

VII. RESULTS

The transmitter is design with RC4 algorithm and it is able to send the encrypted data to the receiver using CC2500 RF transceiver, receiver unit is also design with common RC4 algorithm and it is able to convert the cipher text into original plain text and display on 16x4 LCD.
**Performance of ciphers:**

Performance of cipher, encryption time, decryption time, secrecy and throughput calculated as follows:

1. **Encryption Time:** Encryption time (in ms) is the time taken to convert plain text (original message) into cipher text (encrypted message) in at encryption node. Encryption time was calculated by the help of timer2 module. This module is originated to work along with the PWM module of the PIC controller. Timer2 is an 8-bit timer with a prescaler, a postscaler, and a period register. First we set the Prescaler and Postscaler and set the period register PR2. A starting point of encryption operation, timer 2 module is on. This module will be turned off after operation of encryption. In proposed system we set Prescaler=1:16 and postscaler=1:16 and PR2=255. The output period of the module would be 13ms. It means after every 13ms Timer2 will reset and counter will increase by 1. For example if we are getting almost 4 counters in encryption so encryption time will be 13(ms)x 4=52ms.

2. **Decryption Time:** Decryption time (in ms) is the time taken to convert cipher text into plain text in at decryption node. Decryption time is calculated same as encryption time with the help of timer2 module at a starting point of decryption operation.

3. **Throughput:** Throughput is nothing but is a data transfer from one form to another in a particular time. Throughput was calculated by dividing the appropriate data size (Bytes) by encryption time in sec [3]. For example-From TABLE III 10 bytes of data takes 52.072ms time for encryption so throughput can calculates as,

   \[
   \text{Throughput} = \frac{10 \times 52.072 \times 1000}{192.047} \text{Bytes p/s} \tag{1}
   \]

4. **Secrecy:** Secrecy of cipher is defined as a set of transformations of one space (the set of possible messages) into a second space (the set of possible cryptograms) or in simple word we can say secrecy is the practice of hiding information from certain individuals or groups, perhaps while sharing it with other individuals. That which is kept hidden is known as the secret.

   The secrecy of ciphers is calculated by [3]

   \[
   H_c(K) = \sum(C)P(C) \sum[K]P_c(K) \log_2[P_c(K)] \tag{2}
   \]

First, we consider the Part 1 of secrecy; this is the entropy of the key K, given the relevant cipher. (Cipher text C, has been obtained using this particular key K)

1. Calculate how often each key byte is appeared in the key.
2. After that we calculate the probability of each byte appears (given the cipher) in the key and get the summation of Pc(K) * log2Pc(K).

Then consider the remaining half: Calculating P(C) and then summation.

1. Calculate how often each cipher byte has appeared in the cipher text.
2. And then calculate the probability of each byte appears in the key and get the summation (for all possibilities of the cipher bytes).

Then get the multiplication of part 1 and P(C) is calculated and finally the summation of all possibilities is calculated.

**TABLE III**

<table>
<thead>
<tr>
<th>Data Size (bytes)</th>
<th>Encryption Time (ms)</th>
<th>Decryption Time (ms)</th>
<th>SECRECY Digit per letter</th>
<th>Throughput (bytes p/s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>52.072</td>
<td>39.33</td>
<td>1.0413</td>
<td>192.04</td>
</tr>
<tr>
<td>15</td>
<td>52.675</td>
<td>39.74</td>
<td>1.568</td>
<td>284.76</td>
</tr>
<tr>
<td>20</td>
<td>53.063</td>
<td>39.75</td>
<td>1.728</td>
<td>376.91</td>
</tr>
<tr>
<td>25</td>
<td>53.342</td>
<td>39.97</td>
<td>1.8715</td>
<td>468.67</td>
</tr>
<tr>
<td>30</td>
<td>53.547</td>
<td>40.34</td>
<td>1.8982</td>
<td>560.255</td>
</tr>
</tbody>
</table>

**VIII. CONCLUSION**

The project “Microcontroller Based Cryptosystem using RC4 Algorithm” stream cipher cryptography is successfully developed and implemented with the least cost components. The project is successful to work up to the radius of 30m around the kit using ISM band. The experimental setup has two nodes, which can be emulated with different distance to evaluate the performance of the work. The correctness of the results has been checked and secure transmission has done. The specifications were all met according to the design and the cryptanalysis is made difficult for the hackers. Targeted performance metrics are complexity of key and accuracy of decoding logic at receiver end (Immunity against work).

**FUTURE WORK**

The project can also be modified into a wireless security system at military services where there is a risk of leakage of information. The projects can be made more compact using nanotechnology. The project cost is further reduced if produced in bulk quantity. This project can be further developed using audio and video inputs. The coverage area of this system can be increased beyond ISM band.

**ACKNOWLEDGMENT**

My gratitude goes to Prof. U R More, who guided me to do work in right way during my post graduate studies (Master Engineering) at the University of PUNE. This work is totally attributed to the guidance of above mentioned.

**REFERENCES**


**AUTHOR'S PROFILE**

**Mr. Gaurav Pal**
Obtained his Bachelor's Degree in Electronics & Communication Engineering from RGPV University in 2012. He is presently pursuing Masters Degree in VLSI & Embedded Systems from Pune University.