ISSN: 0975-8585

Research Journal of Pharmaceutical, Biological and Chemical Sciences

Enhancing RFID Security by incorporating Lightweight Block Cipher Using Arduino.

Winnie Beulah Rosario*, and D Manivannan.

School of Computing, SASTRA University, Thanjavur, India- 613 401.

ABSTRACT

The data in embedded devices are prone to various security related issues and also the hardware limitations have to be examined. The conventional algorithms like AES, DES, and other such ciphers are incompatible with the modern embedded devices. Lightweight block cipher PRESENT, is the most suited algorithm is highly optimized to suit applications ranging from low embedded devices to high data critical functions. Owing to the fact that RFID security related issues poses a major threat to these intense critical applications, PRESENT is sought to be the feasible solution. The paper proposes the methodology of providing a highly secure solution to RFID with PRESENT. The ultra-lightweight algorithm is used to enhance the RFID security issues and in long term meeting out to the constraints. The addressable constraints such as power, memory and resource constraints are taken care of by this proposal. The scope can be further extended to data critical application in various streams, as PRESENT is proven highly efficient with the application intended. The paper anticipates the trends of providing the security for RFID based applications, by an encryption and decryption modules in two different locations. The cipher text is transmitted wirelessly through Zigbee units extending it to multiple RFID data to be encrypted and decrypted through the PRESENT algorithm.

Keywords: PRESENT, ARDUINO UNO, RFID, and Zigbee.

Corresponding author

INTRODUCTION

Cryptography plays a vital role in enhancing the security of embedded systems. The modern cryptographic algorithm varies from the traditional ones in terms of code size, its efficiency to the intended application, the timing and the memory complexity and finally the cryptanalysis to prove its vulnerability to the various attacks. These algorithms play an exceptional role in various streams such as data communications varying from low embedded applications to highly sensitive and critical areas of application [10]. Secondly, they provide a high degree of data protection, authentication in terms of user validation, reliability and confidentiality. To provide a highly secure embedded system it is essential that a suitable cryptographic algorithm must be chosen to meet out the requirements [8].

The Radio Frequency Identification technology (RFID) finds increasingly use in various streams naming a few like *impatient medication*, authentication, chain automation in supply chains and products identification. The security concerns of RFID are the main area of concern of disabling vulnerabilities in the embedded system [5].The lightweight block cipher is the key concept in this paper as it is effectively suited in applications where there are constraints in terms of resources and power. Certain conditions have to be leveraged in choosing a cryptographic algorithms which includes the device performance metrics like battery-life, and as stated above the memory requirements, latency in computation and bandwidth for communication [4]. There are numerous ciphers which suit the application in specific of the platform and the hardware provisions namely the block ciphers, stream ciphers, involution ciphers which are in existence [4]. The lightweight symmetric block ciphers falls under the “Lightweight Cryptography” based on certain criteria namely the power consumption and memory requirements [8].

In this paper, a proposal is made for providing high security for RFID by implementing the light weight block cipher PRESENT. PRESENT is an ultra-lightweight block especially for RFID based applications and resource constrained environments [1]. It is Substitution- Permutation network (SPN) with size of keys varying in 80 and 128 bits [7]. On the security and the constraints point of view the 80-bit key size is suited with the application intended. The encryption and the decryption module are implemented in ARDUINO UNO, which is a high performance AVR and typically a low power microcontroller which inherits the RISC architecture with lesser number of bits. The proposed methodology and the algorithm description will be dealt elaborately in the section 3 and section 4 respectively.

Related Work

The major concern of embedded devices and applications is enhancing the security aspects so that data is protected. Ensuring the data integrity, authentication varying from small systems to critical applications, cryptography is taken as the reliable measure. Lightweight cryptography is highly secure with minimal resource requirements. One such effective lightweight block cipher namely PRESENT is used in resource constrained environments. The variations in the PRESENT algorithm in terms of making its more complicated for the attacker to breakthrough are dealt exclusively in the paper. RFID finds use in many streams namely product identification, impatient medication, and many such day to day applications [5]. In such a scenario the threats to RFID considering the security levels can be categorized into Sniffing, Cloning, Relay, Replay and Service denial based attacks [6]. All these attacks take the data in the RFID tag into consideration. Highly vital applications such as impatient medication which has become most sorted in the medical field can imposed to such threats [3]. Taking all these as the key concept, the PRESENT algorithm suited for providing the security countermeasures for RFID[6]. The data in RFID is made secure with the PRESENT algorithm where it is encrypted and the key-dependent S-box makes it highly secure [3]. The information is made secure owing to the fact it may be sensitive application or confidential and have expedites its use for critical applications.

Algorithm Description

PRESENT, an lightweight block cipher of low resource requirements referred to as ultra-lightweight typically suited for hardware based approaches and passive devices like RFID. It is an example of Substitution and Permutation network (SPN) wherein it has two key length supports of 80 bits and 128 bits. Taken the application into consideration the 80 bit key size is recommended which is highly adequate for applications inquiring low security especially deployments involving tag based [7]. Secondly, as mentioned it competes with the design objectives of stream ciphers in hardware oriented approaches.

The 31 rounds consists of exclusive OR operation precisely XOR operation for introducing a round key k_j for 1≤ j ≤32, where a key is specially allocated for post-whitening which is k_{32} which is to provide high degree of security in repeated iterations of block cipher, one bit- permutation and substitution layer accounting for non-linearity using 4*4 bit S-box applied parallel for about 16 times [1]. The pseudo code along with top-level algorithm description is given below:

```
MakeRoundKeys()
for j=1 to 31
do
RoundKeyaddition(STATE[],$K_J$)
  S-BoxLayer(STATE[])
  P-Layer(STATE[])
end for
RoundKeyaddition(STATE[],$K_{32}$)
```

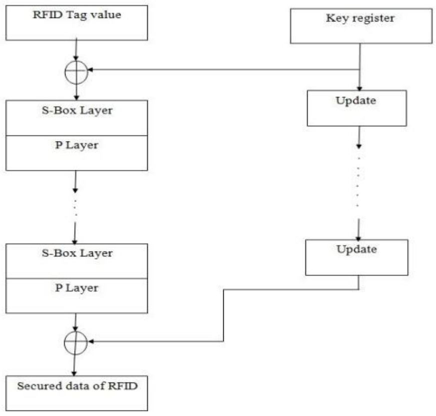


Figure 1: Schematic top-level Flow of PRESENT algorithm.

Add Round key: the round key is given by the notations $k_j = k_{63}^j....k_0^j$for 1≤ j ≤32 and the current state is denoted by STATE $b_{63}....b_0$, the operation consists for 0 ≤ i ≤ 63,

$$b_i \to b_i \quad k_i^j . \oplus$$

S-Box Layer: The algorithm makes use of 4-bit*4-bit S-box typically represented by the function S: $\mathrm{F}_2^4 \to \mathrm{F}_2^4$. The S-box is modified to enhance the security and performance for the intended application. The modifications made are stated below:

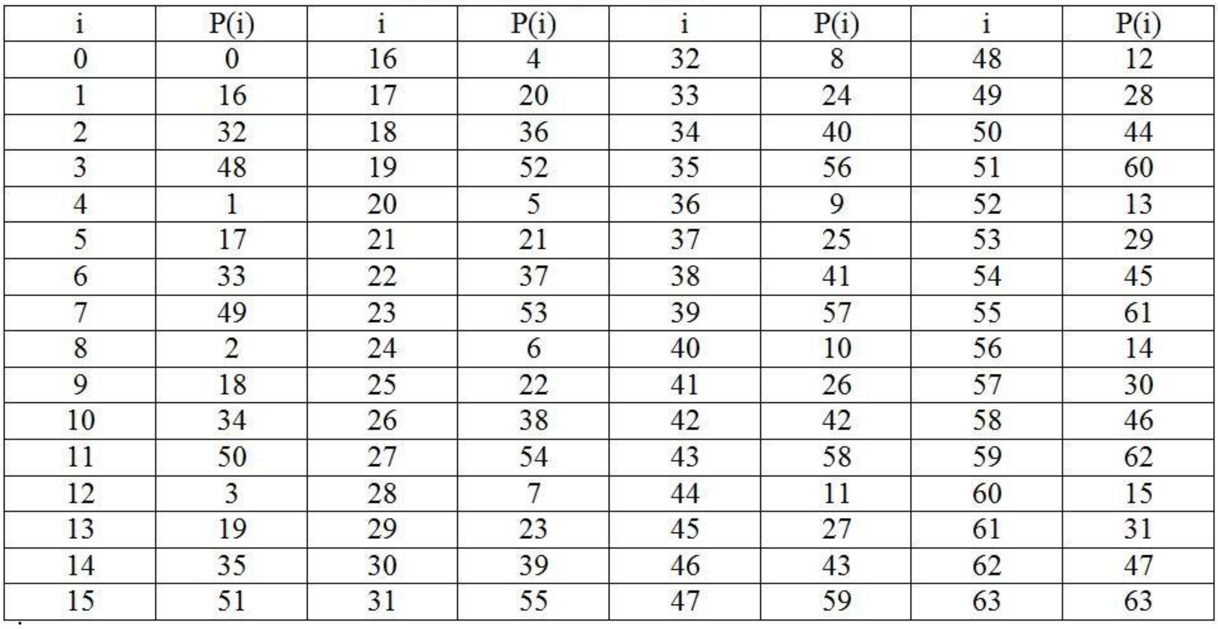
- The key dependent S-box is preferred instead of the fixed S-box which is done through two steps.
- The major concern of this modification is that it is highly secure in terms its efficiency proved against linear and differential cryptanalysis.
- The first step in this modified algorithm is choosing the best S-box which has the equivalent characteristics of PRESENT.
- The linear and differential cryptanalysis are the best tools for checking the security standards of the algorithm where in the linear analysis is done with the Walsh Transform which describes the closeness of the Boolean function f to whether it is affine or linear function.
- The Differential Cryptanalysis explores the strength of the algorithm by checking its non-random behavior by giving certain differences in the input and output to check it is highly probable that is a highly secure block cipher.

- The above criteria were examined and the good S-boxes were found to be Serpent S-boxes. The hexadecimal notation of the S-box is given below:

X	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
S(x)	3	8	F	1	A	6	5	B	E	D	4	2	7	0	9	C
$S^{-1}(x)$	D	3	B	0	A	6	5	C	1	E	4	7	F	9	8	2

Table 1: S-box representation in hexadecimal notation

P-Layer: The permutation uses the diffusion concept and is typically one-bit permutation which is represented in the figure 2:



i	P(i)	i	P(i)	i	P(i)	i	P(i)
0	0	16	4	32	8	48	12
1	16	17	20	33	24	49	28
2	32	18	36	34	40	50	44
3	48	19	52	35	56	51	60
4	1	20	5	36	9	52	13
5	17	21	21	37	25	53	29
6	33	22	37	38	41	54	45
7	49	23	53	39	57	55	61
8	2	24	6	40	10	56	14
9	18	25	22	41	26	57	30
10	34	26	38	42	42	58	46
11	50	27	54	43	58	59	62
12	3	28	7	44	11	60	15
13	19	29	23	45	27	61	31
14	35	30	39	46	43	62	47
15	51	31	55	47	59	63	63

Figure 2: Bit permutation in PRESENT.

Key Schedule: The key register, primarily left shifted by 61 positions, the 4 bits in the left-most is proceeded through the S-box and the key values from k_{19}…k_{15} is XORed with round counter which is the typical key scheduling in PRESENT algorithm.

The proposal also inhibits the property of choosing one S-box i.e. Serpent S-box which is given by the pseudo code:

```
aKey size = 80bit
Plain text = 64 bit
Cipher text = 64 bit
Key = LSB 64-bit from akey
        S-boxes []=$S_0$ ,$S_1$,$S_2$,…….$S_{15}$
        STATE= Plain text
        For
          i= 1 to 31
do
Key_calculate= Key[0….3] XOR Key[60…63].
S-box_new= S-boxes_Array[key_calculate].
STATE = STATE XOR Key.
S-box_new(STATE).
P-box (STATE)
Key update.
End
Cipher text = STATE XOR Key.
```

The new S-box is chosen by performing XOR operation between the elements of the key which is found more secure than the fixed S-box. It relies on the fact that the attackers require more time to retrieve the key and to check the elements of the S-box used.

Hardware Description

Most of the lightweight Cryptographic algorithms are hardly implemented in high-end processor. PRESENT is a hardware profile oriented cipher and highly optimized for space considerations precisely constraints regarding space, memory and power consumption likely resource constrained environments. The block diagram of the proposed prototype is described in figure 3.

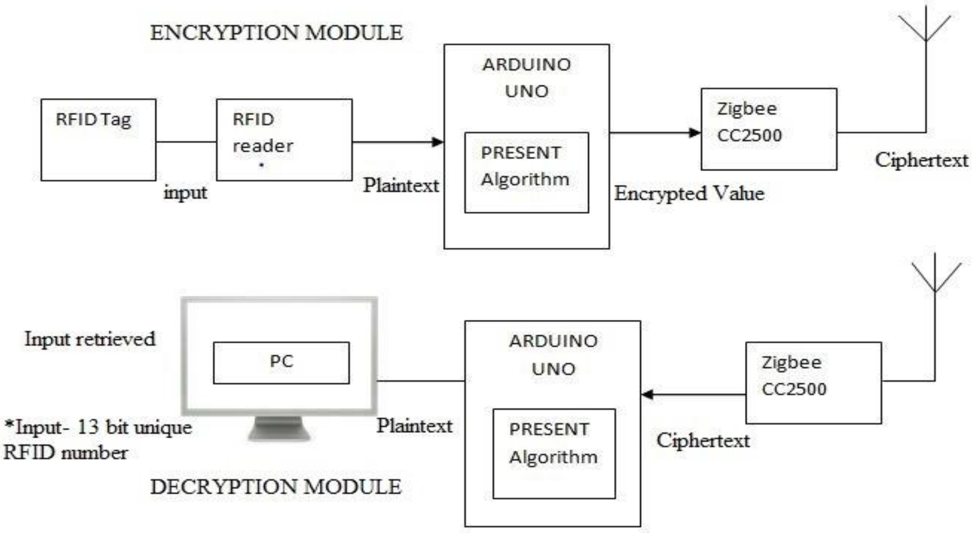


Figure 3: Hardware module of the proposed prototype

The proposed method has two modules for encryption and decryption performed separately through wireless medium. The Read-only passive RFID Tag is used containing a 13-digit code of alphanumeric characters. This unique code is read by RFID reader module (MCRF200) operated at 125-Khz frequency. The reader emits the radio frequency waves through the antenna and these waves travel through the medium. They typically energize the passive tag and collect the data signal from the tag followed by processing of the signal. The reader delivers the information processed to the ARDUINO UNO where the encryption part of the PRESENT algorithm is done. The ARDUINO UNO is a low power AVR Microcontroller with less number of bits and capable of executing the instructions at 1MIPS with its advanced RISC architecture. The PRESENT algorithm encryption module obtains the 13-bit code as in processed information from the reader as the input. This input is sent through series of steps as mentioned in the algorithm description, section 4. The plain text is encrypted and obtained as the cipher text. This cipher text is sent wirelessly to the decryption module through the zigbee CC2500 which is a low-cost 2.5 GHZ transceiver modeled for low power applications exclusively for the RF enabled remote controls.

The decryption module has the zigbee CC2500 at its receiving end to obtain the cipher text and sends this cipher text as the input to the PRESENT Decryption algorithm in the ARDUINO UNO. The cipher text is decrypted to the plain text and the original data is retrieved back. This is typically shown in the HyperTerminal or via the Serial monitor in the ARDUINO 1.0.5 IDE. The system provides the higher level of security to the RFID data through the lightweight Cryptographic algorithm PRESENT. To increase the levels of complexity in breaking through the data, the encryption and the decryption is done in two different ARDUINO enabling the computation are done faster, providing integrity, security levels to the RFID. The system can be classically integrated to any RFID applications and exclusively for impatient medication wherein low-level of security is provided through short length of Pseudo Random Number Generator PRNG [3] used. The PRESENT algorithm is highly secure and is of low-memory requirements which make it the feasible solutions to enhance the levels of security in RFID based applications.

EXPERIMENTAL

The overall hardware prototype of the proposed system for providing security to the RFID through the lightweight bock cipher PRESENT is given in the figure 4.The encryption module and decryption modules of the hardware prototype is given in figure 4 and the input read from the RFID tag and the cipher text obtained from processing through the PRESENT lightweight cryptographic algorithm is transmitted to the decryption module. The input 13 bit unique code is processed and converted to initial value which is encrypted. The encryption module is kept in location 1.

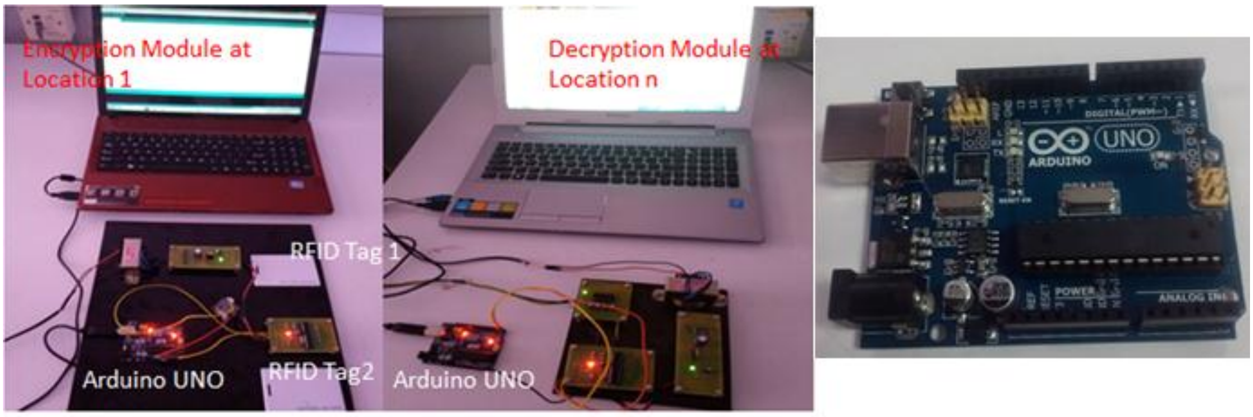
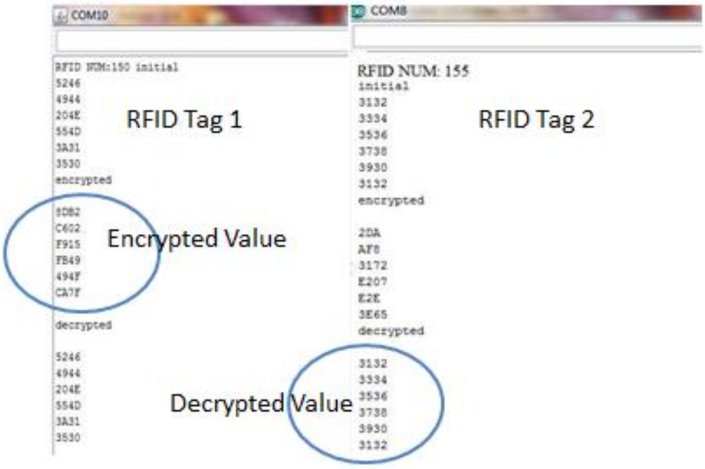


Figure 4: Experimental Setup of the Encryption, Decryption module.

The decryption module of the prototype and the HyperTerminal output of the cipher text to Plaintext where in the initial value is retrieved is shown in figure4 and figure 5.This module is kept in location n to provide coverage and other such scalability factors. The Arduino Uno which is key component in algorithm processing is also shown in figure 4.The main area of concern in any embedded system is enhancing the security where in the system can be employed in highly critical areas. The proposed methodology achieves the high degree of security by incorporating the lightweight block cipher PRESENT for low level embedded applications RFID and the scope can be extended to suit smart card applications, passive low power embedded devices. Furthermore in comparison with the existing system, the lightweight block cipher PRESENT, occupies less memory space specified by few bytes in comparison with the Pseudo Random Number Generator and especially in resource constrained environments.



```
RFID NUM:150 initial
5246
4944
204E
554D
3A31
3530
encrypted

8DB2
C602
F915
FB49
494F
CA7F

decrypted

5246
4944
204E
554D
3A31
3530
```

```
RFID NUM: 155
initial
3132
3334
3536
3738
3930
3132
encrypted

2DA
AF8
3172
E207
E2E
3E65
decrypted

3132
3334
3536
3738
3930
3132
```

Figure 5: Sample output at the HyperTerminal.

CONCLUSION

The embedded devices urges the security as the main concern considering the fact it is highly probable that the device can be attacked in various methods such as data, memory, and the other functionalities. All the system working nature can be highly disruptive if the data is not secure. In this paper, the method to provide security to data for an embedded application concerning RFID is discussed with the PRESENT algorithm as the key factor. In future, the block cipher can be used as an involutive cipher with a block ciphers such as PRINCE, providing the enhanced security solution for resource constrained environment. This can provide an highly secure, feasible and low power requirement and memory requirements solution make an compact secure embedded structure.

ACKNOWLEDGEMENT

We thank SASTRA University for providing financial support for this research work under the Research and Modernization fund– R&M/0008/SOC – 001/2009-10.

REFERENCES

[1] Bogdanov, L.R. Knudsen, G. Leander, C. Paar, A. Poschmann, M.J.B. Robshaw, Y. Seurin, and C. Vikkelsoe, "PRESENT: An Ultra-Lightweight Block Cipher", Springer, Chapter 10, 2007, pp. 450-466.

[2] Muhammad Reza Z'aba1, Norziana Jamil, MohdEzanee Rusli, Md. Zaini Jamaludin, Ahmad AzlanMohdYasir, "I-PRESENT: An Involutive Lightweight Block Cipher", Journal of Information Security 5, 2014, 114-122.

[3] MasoumehSafkhania, NasourBagherib, MajidNaderi, "A note on the security of IS-RFID, an inpatient medication safety", International journal of medical informatics 83, 2014, 82–85.

[4] JiaHao Kong, Li-MinnAng, KahPhooiSeng, "A comprehensive survey of modern symmetric cryptographic solutions for resource constrained environments", Journal of Network and Computer Applications 49, 2015, 15–50.

[5] Avery Williamson Sr., Li-Shiang Tsay, Ibraheem A. Kateeb, Larry Burton, "Solutions for RFID Smart Tagged Card Security Vulnerabilities", AASRI Procedia 4,2013, 282 – 287.

[6] Wei Xie , Lei Xie , Chen Zhang , Qiang Wang , JianXu, Quan Zhang a, Chaojing Tang, "RFID seeking: Finding a lost tag rather than only detecting its missing", Journal, ofNetwork and Computer Applications 42, 2014, 135–142.

[7] Julio Cesar Hernandez-Castro, Pedro Peris-Lopez,"On the Key Schedule Strength of PRESENT", SPRINGER,2012, 253-263.

[8] SagarKhurana, SouvikKolay, Chester Rebeiro and DebdeepMukhopadhyay, "Lightweight Cipher Implementations on Embedded Processors", IEEE, 2013, 83-87.

[9] HristinaMihajloska, DaniloGligoroski, "A New approach into Constructing S-boxes for Lightweight Block ciphers", 8th Conference on Informatics and Information Technology with International Participation (CIIT),2013, 14-18.

[10] Sergey Panasenko and Sergey Smagin, "Lightweight Cryptography: Underlying Principles and Approaches", International Journal of Computer Theory and Engineering, Vol. 3, No. 4, 2011, pp. 516-520.