ISSN 2278-3091
Volume 9, No.1, January – February 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse96912020.pdf
https://doi.org/10.30534/ijatcse/2020/96912020

A Novel Key Scheduling Algorithm for Lightweight Cryptographic Applications

Asmita Poojari[1], Nagesh HR[2], Kiran Kumar V G[3] Shantharama Rai C[4]
[1]NMAM Institute of Technology, Nitte, Karkala, India, asmitapoojari@nitte.edu.in
[2]A J Institute of Engineering and Technology Mangaluru , India, kirankumar@ajiet.edu.in
[3]A J Institute of Engineering and Technology Mangaluru , India, nageshhrcs@rediffmail
[4]A J Institute of Engineering and Technology Mangaluru , India, csrai@ajiet.edu.in

ABSTRACT

Advancement in the area of wireless communication has increased the demands for lightweight security schemes as the sensor nodes and the devices used in these networks are resource constrained devices. One such area where the lightweight cryptographic system can be applied is the medical Internet of things. Since most of the devices in medical IOT is resource constrained it poses a challenge to traditional cryptographic algorithms which tend to lower the network performance as it requires high computational complexities, power consumption, and delays and hence the need for lightweight security in these devices. To prevent any unauthorized access or interruption it is crucial to ensure that data secrecy is maintained throughout the medical treatment. The most crucial thing in securing these resource constrained devices is the key used in encryption process since the entire security of the data is dependent on the key used. Even if the attacker has little knowledge of the key used in the encryption process, the entire security of the system can be lost. In this paper a lightweight key scheduling algorithm is proposed which can be used to generate the keys to be applied for encryption process in IOT devices used in medical care to improve the security of data transmitted in the healthcare environment.

Key words : Medical IOT, lightweight security, resource constrained, Internet of Things, key scheduling.

1. INTRODUCTION

Internet of Things (IoT) is the interconnection in which constrained devices are interconnected to perform some tasks. Healthcare industry is one of the fields where internet of things technology can be used to provide benefits to the patients having health issues wherein the patient's health can be monitored anytime and anywhere without the necessity of the patient to visit the doctor every time. At the same time health care industry using medical IoT is becoming one of the targeted industry for data security attackers. The medical sensors are one of the easy targets to exploit where its effect is very dangerous and life threatening leading to dangerous life and death problems. Medical fraud problem can lead to wrong treatment causing loss of lives and even illegal increase in financial cost. Some of the major security issues with respect to Medical IoT is allowing an unauthorized person to access patient's personal information, treatment details, and other details such as pharmaceutical details which makes patients life insecure and also mishandle the data against the patient. Conventional cryptographic techniques cannot be applied here as the Medical IOT devices are resource constrained devices which require low energy and power consumption, less memory space and secure. Hence the need for Lightweight cryptography. In this paper an optimized lightweight key scheduling algorithm is proposed which can be used in in the encryption of the sensitive data transmission between the medical IoT devices. The performance of the algorithm is tested using using the randomness test.

2. RELATED WORK

The research field of IoT and securing it with lightweight cryptography has gain light in the following years but Medical IoT has come to power recently. Very few researchers have implemented optimized lightweight cryptographic algorithms for resource constrained IoT devices.

Francois-Xavier et al. (2006) designed a software implementation of lightweight block cipher based on Fiestel structure, SEA which followed ARX based operations.[1].

Bogdanov et al. (2007) specified a hardware implementation of a block cipher PRESENT which followed Substitution and permutation structure. PRESENT has 64-bits block size and a key size of length 80/ 128 bits. It undergoes 31 rounds where each round applies same 4bit S-Box 16 times in parallel for non-linear substitution layer. But it has weak diffusion property [2].

Zheng Gong et al. (2011) specified block cipher named KLEIN based on SPN structure having 64-bit block size, key sizes of 64 or 80 or 96-bit and 12 or16 or 20 number

of rounds respectively. It combines the operations of AES [3] and PRESENT [2].

Lei Zhang et al. designed a lightweight block cipher called LBlock with block size of 64-bits and key size of 80-bits. Round function F follows substitution and permutation network. [4].

Julia Borghoff et al. (2012) designed lightweight block cipher called PRINCE which is based on FX construction It has a block size of 64-bits and a key size of 128-bits with 12 number of rounds [5].

Ray Beaulieu et al. (2013) designed lightweight block ciphers named SIMON and SPECK. The SIMON cipher has a block size of 2n-bits and a key size of mn-bits. Both use circular shift bit permutations. [6].

Several research works have been going on in the field of IoT security and especially one of its applications that is Medical IoT. M. A. Iqbal.(2016) [9] proposed a lightweight security protocol tailored for medical IoT devices with the main aim to reduce the energy consumption but it did not prove to be suitable for all the resource constrained medical devices.

M. Haghi. (2017). [10] identified how personal data can be leaked from the wearable devices in Medical IOT.

3. PROPOSED KEY SCHEDULING ALGORITHM

3.1 Initial Phase of key scheduling algorithm

The proposed key scheduling algorithm is used to generate the round keys which is used in the lightweight cryptographic system to be used in the medical IOT scenario The proposed algorithm takes as input the date of birth, aadhar number and the first name of the patient. This data is to be given by the patient and from this a unique input is created which becomes the input for the key scheduling algorithm. The steps work as follows:

1. A unique input is created by taking the first character of the first name of the patient, first digit of the date of birth followed by the 12 digit aadhar number followed by the last character of the first name followed by second digit date of birth.
2. This unique input is converted to 128 bits input key by performing necessary ASCII and hexadecimal conversion.
3. Next the 128 bits input key is divided into segments of 4 bits.
4. Then the 128 bits input key is converted into 4, 16-bits keys by performing the XOR function as shown in the figure.
5. Taking that 16-bit data as the input a pseudo random number is generated using linear feedback shift register. Then then the 16- bit data from the previous step and the output of the linear feedback shift register are XORed. This step will generate 4, 16- bit intermediate keys QI, Q2, Q3, Q4 which becomes the input for the Fibonacci scrambling algorithm.

3.2 Fibonacci scrambling algorithm

The Fibonacci scrambling algorithm generates 4 keys (K1, K2, K3, K4) which are XORed to generate the fifth key K5.These five keys are used as the round keys in the encryption process.

The scrambling algorithm works as follows:

1. Begin
2. Initialize the parameters: Q1, Q2,Q3, Q4 generated from step 3
3. Derive the first element of the key
   K (1) = mod (Q1*Q2 – Q1, Q3)
4. Derive the second element of the key
   K (2) = mod (Q1*Q2 – Q2, Q3)
5. Derive 3rd to nth key (where n is 4)
   for i=3 to n do
   K (i) = mod (K (i-1) + K (i-2) +3*i, Q4)
   end for
6. Generate the key sequences
7. End

The 4 unique keys generated are then xored to get the 5th key and these five keys become the input to the round function in the encryption process.

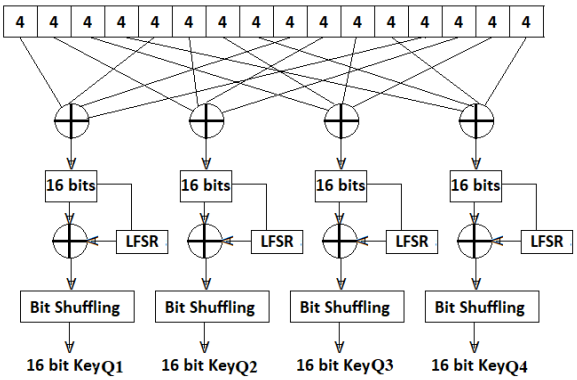

Figure 1: Key scheduling process

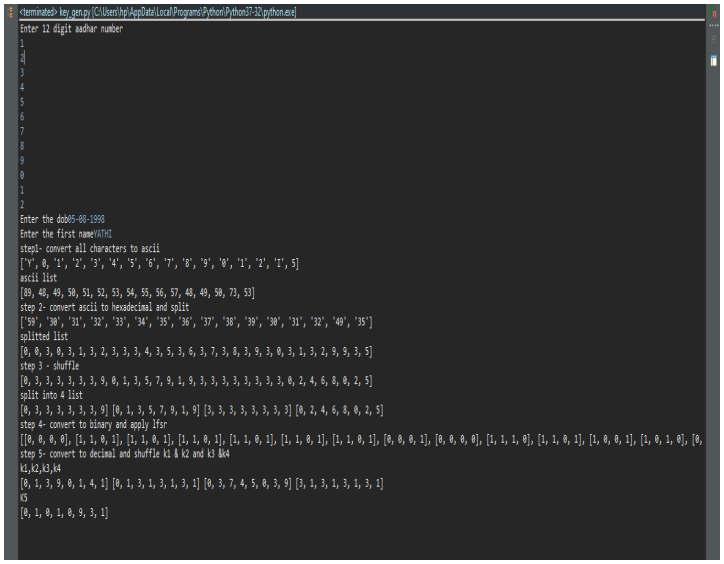

Figure 2: Implementation of the key scheduling algorithm.

4. SALIENT FEATURES OF THE KEY GENERATION ALGORITHM

The salient features of the proposed key scheduling algorithm is as follows:

- It is more secure in generating key for data encryption
- Efficient and high level of security against the intruders
- Requires domain knowledge to break the key.
- More randomness in the generated key.

5. PERFORMANCE ANALYSIS OF THE PROPOSED KEY GENERATION ALGORITHM.

The performance of the key generation algorithm is tested using the Pearson's correlation test which tests the correlation between two adjacent keys as shown in Table 1. The correlation test proves that the keys generated are completely random and hence provides more security if applied to the lightweight cryptographic algorithm.

Adjacent keys	Correlation value
K1,K2	0.085
K2,K3	0.088
K3,K4	0.018
K4,K5	0.078
K5,K1	0.057

Table 1 : Correlation analysis

5. CONCLUSION

In this paper a novel key generation algorithm is proposed which can be used to generate encryption keys that can be further used to encrypt the medical sensor data using lightweight cryptography. The keys generated by this process will be used as the input to the round function in the encryption process. The main aim of this proposal is to generate keys which are more random in nature in less time as this process will be applied to the resource constrained medical sensor devices.

REFERENCES

1. Standaert, F.X., Piret, G., Gershenfeld, N. and Quisquater, J.J.,April, 2006 . A scalable encryption algorithm for small embedded applications, International Conference on Smart Card Research and Advanced Applications, pp. 222-236, Springer, Berlin, Heidelberg. https://doi.org/10.1007/11733447_16
2. Bogdanov, A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M.J., Seurin, Y. and Vikkelsoe, C., September, 2007 . PRESENT - An ultralightweight block cipher, Vol. 4727, pp. 450466.
3. Daemen, J. and Rijmen, V., 1999. AES proposal: Rijndael.
4. Wu, W. and Zhang, L., 2011. LBlock: a lightweight block cipher, Applied Cryptography and Network Security, pp. 327-344, Springer Berlin/Heidelberg.
5. Borghoff, J., Canteaut, A., Güneysu, T., Kavun, E.B., Knezevic, M., Knudsen, L.R., Leander, G., Nikov, V., Paar, C., Rechberger, C. and Rombouts, P.,December, 2012, PRINCE–a low-latency block cipher for pervasive computing applications, International Conference on the Theory and Application of Cryptology and Information Security, pp. 208-225, Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-34961-4_14
6. Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B. and Wingers, L.,2013,The SIMON and SPECK Families of Lightweight Block Ciphers, Cryptology ePrint Archive.
7. Bansod, G., Raval, N. and Pisharoty, N., 2015. Implementation of a new lightweight encryption design for embedded security. IEEE Transactions on Information Forensics and Security, 10(1), pp.142-151.
8. Banik, S., Pandey, S.K., Peyrin, T., Sasaki, Y., Sim, S.M. and Todo, Y., 2017, September. GIFT: a small PRESENT. In International Conference on Cryptographic Hardware and Embedded Systems (pp. 321-345). Springer, Cham.
9. M. A. Iqbal. (2016, August). A novel authentication and key agreement protocol for internet of things-based resource-constrained body area sensors. In 2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW). [online]. pp. 315-320.Available:https://ieeexplore.ieee.org/document/7592744 https://doi.org/10.1109/W-FiCloud.2016.70
10. M. Haghi.,2017, Wearable devices in medical internet of things: scientific research and commercially available devices,Healthcare informatics research., pp. 4-15. https://doi.org/10.4258/hir.2017.23.1.4