ISSN 2278-3091
Volume 8, No.4, July – August 2019
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse69842019.pdf
https://doi.org/10.30534/ijatcse/2019/69842019

Performance Metrics and Energy Evaluation of a Lightweight Block Cipher in Human Sensor Networks

Radhika Rani Chintala[1], Narasinga Rao M R[2], Somu Venkateswarlu[3]

[1]Research Scholar, Department of CSE, KLEF, Guntur, Andhra Pradesh, India
[2]Professor, Department of CSE, KLEF, Guntur, Andhra Pradesh, India
[3]Professor, Department of CSE, KLEF, Guntur, Andhra Pradesh, India

ABSTRACT

The vast increase in the development of Human Sensor Networks (HSN) and nodes has led to the increase in the exchange of the data among the sensor devices. Usually, the sensor devices will be having limited resources such as low battery power, less memory, etc. and should be capable to handle sensitive and private data. Normal encryption methods will not be suited for these sensor devices as they require large resources. For this reason, lightweight block ciphers are used for encrypting data on sensor devices. These algorithms should balance the security requirements along with energy consumption. In this paper, different design parameters and performance metrics for computing the energy being consumed by an encryption algorithm have been discussed. Lightweight block ciphers may work on different block sizes. To have a fair assessment among the ciphers, energy cost has been considered in order to encode one bit of plaintext. Energy per bit is considered as an important performance metric in measuring the energy efficiency of a cipher algorithm in low resource constraint devices.

Key words : Human Sensor Networks, Lightweight block ciphers, Energy consumption, Sensor devices.

1. INTRODUCTION

The smart electronic devices used by Human Sensor Networks are designed and developed with less processing capability, low back up power supply and low memory capacity. Their physical dimensions are very less. The applications running on these devices may drain the power very fast, resulting in switching off the device. But the battery can’t be charged continuously and always. The applications running on the device demands more energy than is generally stored in the battery. Hence energy conservation methodologies are becoming very critical while designing the HSN devices. Even the data security need to be considered while designing them [1].

The autonomous HSN devices works in two fundamental modes: Sleep and Active modes. The mode of operation is dependent on amount of energy being consumed and on performance of the device. Apart from these two fundamental modes there may be other secondary modes as well, depending upon the working conditions. Device’s duty cycle has to be maximized and energy consumption has to be minimized for proper energy management of the device. Thus the device’s battery life can be extended.

Researchers have suggested various symmetric and asymmetric encryption algorithms for HSN nodes [2]. Asymmetric encryption is used when the HSN device is having enough computing power, free memory and battery energy [3].

2. UNITS

The organization of lightweight encryption algorithm is shown in Figure.1. There are two main blocks in the design namely Key scheduling block and round function block with T rounds [4]. Each round takes n-bit data that is generated by previous round, performs the encryption using the sub-key and generates an n-bit cipher text, which in turn is given as an input to next round. The key schedule function will take master key as an input and expands it into sub-keys, where each sub-key is given to one round. Lightweight ciphers (Ktantan [5]) which use fixed key do not contain key scheduling function.

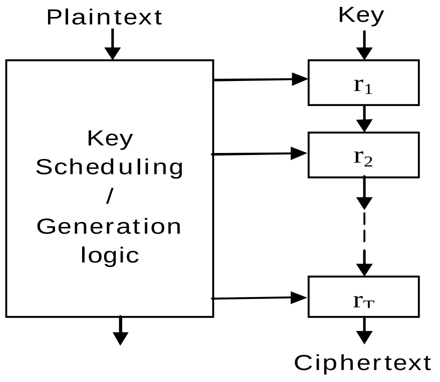

Figure 1: Encryption Algorithm

Depending upon the type of the encryption algorithm, the number of the rounds, the round functionality and the key scheduling function will be varied [6], [7]. Lightweight block ciphers [8] usually have larger number of rounds with simple operations and simple key schedule functionality [9]. Table 1 describes the different parameters and constants of the design as shown below.

Table 1: Design Parameters and Constants

Symbol	Description
n	No. of bits in a block
r_T	Total no. of rounds
r_i	No. of implemented rounds
F_q	Frequency
A_D	Design Area
CT	Cycle Time or Clock time period
T_B	Time consumed to encrypt data of single block
C_B	No. of cycles required to encrypt data of single block
E_B	Energy consumed to encrypt data of single block
E_1	Energy consumed to encrypt one bit
C_0	Idle cycles between blocks
D_R	Register time delay
D_C	Combinational logic time delay
T_{r1}	Time delay for one round
t_0	t_0 is equal to T_{r1} when $n = 0$
t_n	Time increase in T_{r1} w.r.t n
A_1	Area covered by one round
A_0	Area covered by overhead logic(control and key scheduling)
A_n	Increase in area w.r.t n
A_r	Area covered by r_i rounds
g	Growth in A_r w.r.t r_i
g_0	Growth in A_r w.r.t r_i when $n = 0$
g_n	Growth in A_r w.r.t r_i when n increases
g_b	Growth in A_n per bit
P_u	Power consumed for unit area
P_d	Power consumed for unit area based on r_i
P_i	Power consumed for unit area irrespective of r_i

The implementation of lightweight block cipher algorithm is shown in Figure 2. It contains the blocks namely registers, Overhead logic and the round's function. Registers are used to save the initial data, intermediate data and the final data. Overhead logic is used to generate the sub-keys. Round's function is used to implement r_i rounds.

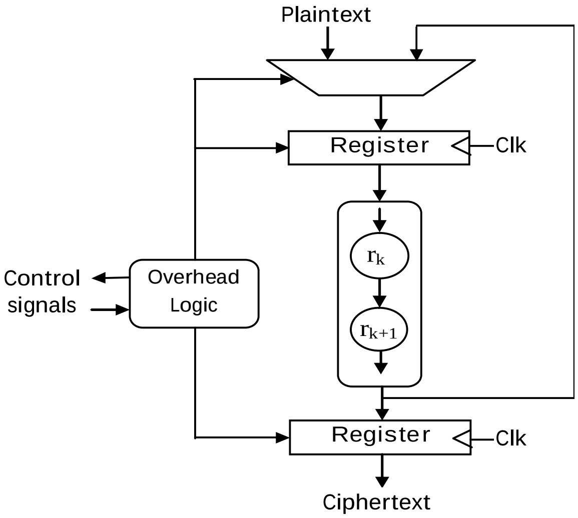

Figure 2: Encryption Algorithm Implementation

3. ENERGY EVALUATION

E_B of energy is consumed by a device with and area A_D for encrypting single block of data. Energy needed for encrypting one bit E_1 can be expressed as:

$$E_1 = E_B / n \tag{1}$$

No of cycles required for encrypting one block data, C_B, depends on r_T and r_i. (r_T denotes number of encryption rounds as per algorithm and r_i denotes no. of encrypting rounds used in realization). The time required for encrypting one block of data is $C_B \times CT$.

The timing delays of registers and the combinational logic circuits used gives the lower limit on cycle time. The minimum cycle time will be sum of registers delay and the delay of combinational logic circuit.

If there are r_i encryption rounds, delay produced by combinational logic circuit, D_C can be:

$$D_C = r \times T_{r1} \tag{2}$$

Where T_{r1} i.e., delay consumed by one round.

T_{r1} has two components namely constant t_0, and n-rate t_n, and can be represented as:

$$T_{r1} = t_0 + t_n \times n \tag{3}$$

Substituting (3) in (2) we get:

$$D_C = r_i \times (t_0 + t_n \times n) \tag{4}$$

$$CT = D_R + r_i \times (t_0 + t_n \times n) \tag{5}$$

$$T_B = C_B \times (D_R + r_i \times (t_0 + t_n \times n)) \tag{6}$$

Also, throughput is defined as [2] [7]:

$$\text{Throughput} = (n_b \times F_q) / C_B \tag{7}$$

If the hardware part implementation is fit for r_i rounds of execution per cycle, one block of data is encrypted by r_T/r_i cycles. Moreover, there may be idle cycles (C_0) between data blocks to load the plain text and yield encrypted text. Usually, C_0=2 cycles. Consequently, number of cycles to encode one unit of data is:

$$C_B = (r_T/r_i) + C_0 \tag{8}$$

3.1 Area

The area of the implementation will depend on no. of rounds used in hardware realization (r_i), no. of bits in a block (n) and the overhead logic. Area can be:

$$A_D = A_r + A_n + A_0 \tag{9}$$

A_r is relative to r^g, where $g < 1$. The growth of A_r relative to r_i is below the linear as the optimization methods combine few of the common logic among the rounds. It is seen that g relies upon n and can be communicated as:

$$g = g_n \times n + g_0 \tag{10}$$

$$A_r = r^g \times A_1 = r^{(gn \times n + g0)} \times A_1 \tag{11}$$

A_n is directly proportional to n.

$$A_n = g_b \times n \tag{12}$$

Using the equations (9) to (12),

$$A_D = r^{(gn \times n + g0)} \times A_1 + g_b \times n + A_0 \tag{13}$$

3.2 Power

Power consumption of a design can be represented as:

$$P = P_s + P_d \tag{14}$$

Where P_s denotes the static power and leakage and is ignored in this work, as it is denotes a negligible amount of overall power [10]. P_d is the dynamic power. Therefore, design power can be represented as:

$$P = P_u \times F_q \times A_D \tag{15}$$

Where P_u gives the switching activity factor, which denotes how dynamically the design nodes are being switched. r_i is linearly proportional to the activity factor, which means that, by increasing the r_i, the logic levels in cycle will be increased, which leads to the increase in activity factor [11 - 14].

Based on the implementations of cipher designs, the rough linear equation of a P_u can be given as:

$$P_u = P_d \times r_i + P_i \tag{16}$$

Rewrite (15) as:

$$P = (P_d \times r_i + P_i) \times F_q \times A_D$$

Where $F_q = 1/CT$

$$\Rightarrow P = ((P_d \times r_i + P_i) \times A_D) / CT \tag{17}$$

3.3 Energy

Energy for encrypting one block of data can be represented as:

$$E_B = T_B \times P \tag{18}$$

Lightweight block ciphers may work on different block sizes, n. To have a fair assessment among the ciphers, we consider energy cost in order to encode one bit of plaintext. Therefore, Energy per bit E_1 can be represented as:

$$E_1 = E_B / n \tag{19}$$

E_1 is considered as an important performance metric in measuring the energy efficiency of a cipher in low resource constraint devices [9], [15].

4. CONCLUSION

In low resource constraint devices, one of the important and challenging parameter is energy. To increase the device’s performance, the energy stored in the battery has to be consumed very intelligently. For this to be done, the present paper discussed about the energy being consumed by low resource sensor devices (generally used in HSN nodes). The energy being consumed has been calculated qualitatively, during the encrypting and working process. Thus the throughput of the device can be increased, while reducing the energy cost and extending the life of the battery.

REFERENCES

1. Radhika Rani Chintala, Narasinga Rao M R, Somu Venkateswarlu, "**Review on the security issues in Human Sensor Networks for Healthcare Applications**", International Journal of Engineering and Technology, vol. 7, no. 2.32, pp. 269-274, 2018. https://doi.org/10.14419/ijet.v7i2.32.15582
2. S. Singh, P. K. Sharma, S. Y. Moon, and J. H. Park, "**Advanced lightweight encryption algorithms for iot devices: survey, challenges and solutions**," Journal of Ambient Intelligence and Humanized Computing, pp. 1–18, 2017. https://doi.org/10.1007/s12652-017-0494-4
3. Daojing SC & Shaohua, "**A Novel and a Lightweight System to secure Wireless Health Sensor Networks**", IEEE Journal of Biomedical and Health Informatics, vol. 18, no. 1, pp. 23-32, Jan. 2014. https://doi.org/10.1109/JBHI.2013.2268897
4. J. Bassam J. Mohd, Thaier Hayajneh, "**Lightweight Block Ciphers for IoT: Energy Optimization and Survivability Techniques**", DOI 10.1109/ ACCESS.2018.2848586, IEEE Access, 2016.
5. C. De Canniere, O. Dunkelman, and M. Knezevic, "**Katan and ktantan–a family of small and efficient hardware-oriented block ciphers**," in Cryptographic Hardware and Embedded Systems-CHES 2009. Springer, pp. 272–288, 2009. https://doi.org/10.1007/978-3-642-04138-9_20
6. Ch.Radhika Rani, L.Sai Jagan, Ch.Harika Lakshmi, A.V.V.D. Ravali,"**Lightweight Encryption Algorithms for Wireless Body Area Networks**", International Journal of Engineering and Technology, vol. 7, no. 2.20, pp. 64 – 66, 2018. https://doi.org/10.14419/ijet.v7i2.20.11754
7. Radhika Rani Chintala, S. Srujana, N. Ajith Kumar, "**An Analysis of Lightweight Block Ciphers in Wireless Body Area Networks**", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 7C2, pp. 413-418, 2019. https://doi.org/10.14419/ijet.v7i2.20.11754
8. G. Hatzivasilis, K. Fysarakis, I.Papaefstathiou, and C. Manifavas, "**A Review of Lightweight Block Ciphers**", Journal of Cryptographic Engineering, vol. 8, no. 2, pp. 1–44, 2017. https://doi.org/10.1007/s13389-017-0160-y
9. B. J. Mohd, T. Hayajneh, and A. V. Vasilakos, "**A survey on lightweight block ciphers for low-resource devices: Comparative study and open issues**," Journal of Network and Computer Applications, vol. 58, pp. 73–93, 2015. https://doi.org/10.1016/j.jnca.2015.09.001
10. N. H. Weste and D. Harris, "**CMOS VLSI design: a circuits and systems perspective**", Pearson Education India, 2015.
11. B. J. Mohd, T. Hayajneh, M. Z. Shakir, K. A. Qaraqe, and A. V. Vasilakos, "**Energy model for light-weight block ciphers for WBAN applications**," in Wireless Mobile Communication and Healthcare (Mobihealth), 2014 EAI 4th International Conference on. IEEE, pp. 1–4, 2014.
12. E. Boemo, J. P. Oliver, and G. Caffarena, "**Tracking the pipelining-power rule along the fpga technical literature**", in Proceedings of the 10th FPGA world Conference ACM, pp.9, 2013. https://doi.org/10.1145/2513683.2513692
13. S. J. Wilton, S.-S. Ang, and W. Luk, "**The impact of pipelining on energy per operation in field-programmable gate arrays**", in FPL. Springer, pp. 719–728, 2004. https://doi.org/10.1007/978-3-540-30117-2_73
14. N. Rollins and M. J. Wirthlin, "**Reducing energy in fpga multipliers through glitch reduction**", All Theses and Dissertations, https://scholarsarchive.byu.edu/etd/1105, 2007.
15. S. Kerckhof, F. Durvaux, C. Hocquet, D. Bol, and F.-X. Standaert, "**Towards Green Cryptography: A Comparison of Lightweight ciphers from the Energy viewpoint**," in Cryptographic Hardware and Embedded Systems–CHES 2012, pp. 390–407, Springer, 2012. https://doi.org/10.1007/978-3-642-33027-8_23