Modified SIMON approach towards lightweight cryptography scheme for multi data key pair combination

Aniket Kadukar[1,*], Urvashi Bansal[1]

[1]Department of Computer Science and Engineering, Dr. B.R. Ambedkar National Institute of Technology Jalandhar, India

Abstract

There are many IoT devices use by peoples to make their life easy, but there are some devices that are very important like healthcare devices which are very small in size and having very less memory and power backup. It is important to transfer data to the server with privacy, so we use encryption for that. To encrypt data in such small IoT devices we use lightweight cryptography. There are many healthcare IoT devices that uses SIMON algorithm and there is a need to optimise that algorithm to improve the execution time and memory consumption. In this paper we are introducing the new approach to optimise lightweight cryptography algorithm that is SIMON.

Keywords

Lightweight, Cryptography, Healthcare, SIMON, IoT

1. Introduction

Lightweight cryptography represents the encryption algorithms that uses very less computation power and less time for execution. Requirement of these types of algorithm is increase as the devices are increased. There are many devices that are very small in size so there is limitation of memory, processor and power usage. In this device we need to transfer data to the server or host system continuously. While transferring the data encryption is requires to ensure that the data will not accessed by unauthorised user. Lightweight cryptography is used in such devices which required very less computational power, less memory to store that program and uses less power. So we are going to optimise the SIMON cipher algorithm. This algorithm is used in various healthcare devices to encrypt the data while transferring the data.

1.1. SIMON Algorithm

SIMON can process data block of 32 to 128 bits and it requires key size from 64 to 256 bits to encrypt or decrypt that data.
SIMON(2n/mn) where, mn-bit is size of key
2n-bit size of data block

ACI'22: Workshop on Advances in Computation Intelligence, its Concepts Applications at ISIC 2022, May 17-19, Savannah, United States

*Corresponding author.
aniketak.cs.20@nitj.ac.in (A. Kadukar); urvashi@nitj.ac.in (U. Bansal)

Table 1
Parameters of SIMON cipher[1]

Block Size(2n)	Word Size(n)	Key Size(mn)	Key Word(m)	Rounds(r)
32	16	64	4	32
48	24	(72)(96)	(3)(4)	(36)(36)
64	32	(96)(128)	(3)(4)	(42)(44)
96	48	(96)(144)	(2)(3)	(52)(54)
128	64	(128)(192)(256)	(2)(3)(4)	(68)(69)(72)

m-word m must be 2, 3 or 4
n is equal to word size

National Security Agency (NSA) proposed the SIMON algorithm. It provides security to highly constrained devices. It is a Feistel block cipher. The existing cryptographic algorithm is designed keeping in mind hardware devices. This type of algorithm is designed to work under pervasive computing systems. Unlike all algorithms its main objective is to protect data. It uses round functions of left circular shift, bitwise OR and bitwise AND. It was developed to get best performance on hardware but fortunately it is giving best performance in hardware as well software.
Encryption: To encrypt 64bit plaintext P, it uses 44 round functions with 44 round keys generated using key schedule. The key expansion function and round are designed in such a way that they can be used in parallel if needed. Encryption and decryption are symmetric.
Decryption: To decrypt a 64 bit ciphertext c, first we swap 32 bit rightmost bits to 32 bits leftmost bits, then applying 44 round function and after completion of all 44 round function finally we swap 32 bit leftmost with rightmost and vice versa.

In Fig 1 Norah et al.[2] has introduced the new approach to SIMON algorithm that has reduced the time of execution of most of the data key combination of SIMON algorithm like SIMON(32/64), SIMON(48/72), SIMON(64/96), SIMON(96/96) and SIMON(128/128) but the ROM usage of SIMON(64/96), SIMON(96/96) and SIMON(128/128) has increased. SIMON(64/96) taking more time for execution. In this modification they have removed the left shift operation in the round function of the algorithm because of that some of the data key combination of SIMON algorithm has enhanced but some data key combination of this algorithm is not enhanced. While reducing the execution time of the algorithm ROM usage also increased.

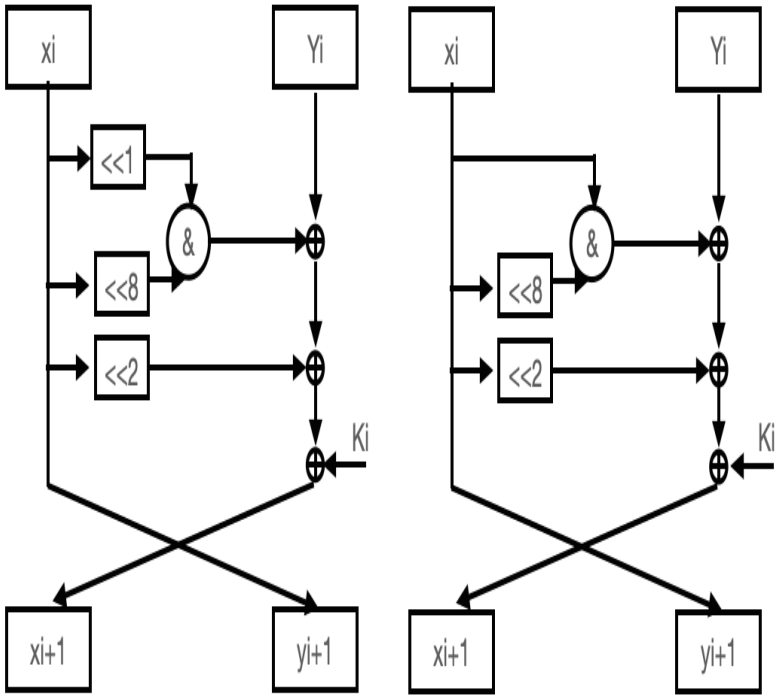

Figure 1: a) Original SIMON algorithm b) Norah et al.[1] Simon algorithm

1.2. Tools

Normal simulation tools, unlike Cooja, do not consider the necessity for an on-node processing technique. It's worth noting that Cooja has been used to imitate a number of cutting-edge medical monitoring systems. This simulation is built on the T-mote-sky platform, which is an board of MSP430-based with an IEEE802.15.4 wireless module. CC2420 a radio chip is used to save power and enable wake-up-fast from sleep. For all simulations, the platform provides a stable wireless fascinating communication that runs smoothly. The basic simulation parameters have been depicted. The MSP430 F1611 microcontroller on the implementation board has 48 KB of ROM, 10 KB of RAM. This hardware requires a battery that is similar to a real-life AA solid-state battery, with the added advantage of being able to connect to a computer and run through the USB connection.[1]

Author utilised the MSP-cycle-watcher, which was designed as a quality-control tool, this can calculate the clock cycle of encryption algorithm. The number of cycles in the encryption part's code is calculated by subtracting it from the total number of cycles in the entire code, which includes setup and post-processing overhead. To get result in a fair power consumption comparison research It is important to comparing exact encryption clock cycles. In addition,

this phase (counting encryption cycles) was done exactly by including a determination of check point for the conclusion and start of the counting process. They use a Bsize command in the MSP430 GCC compiler to estimate ROM usage in this study. The memory usage of this Bsize A measure is calculated automatically from the file which is of compiled code. The program's consumption of ROM is the total number of data and text bytes utilised and the consumption of ROM is determined for the specialised encryption portion only.RAM usage comprises both stack and data use. The consumption of data is calculated using the implementation information file and the command. To examine the stack usage, they used the MSP stack watcher during execution.[1]

2. Literature Review

In December 2015, a paper published by Dhruti Sharma[3] in that paper, she used functional Encryption technique in Healthcare related data transmission. The main idea is based upon presenting a framework so that centralised data can be utilized easily and effectively and also providing data privacy and data confidentiality to IoT healthcare system. In this she used concept of functional encryption and attribute-based cryptography technique such that data is processed with structured and systematic access control. So, lets talk about functional encryption. Actually, it is a generalised version of available public key encryption technique such as Homomorphic encryption, Identity based encryption etc. In functional encryption technique, firstly plaintext is encrypted then we run a predefined function on our encrypted data. Now, when this ciphertext goes to receiver end a predefined function is run by decryption phase and then convert output ciphertext to plaintext. In this encryption technique is using four algorithms for proper functioning. The first algo is setup algo, It is used to generate private key of master and public key of system. Now, 2nd algo i.e., encrypt is used for encrypting a message using public key and generates ciphertext. The 3rd algo GenTok is used for constructing token using private key. Then at last, execute algorithm used for conversion of ciphertext token to functional ciphertext.

Now let's see about Attribute based encryption technique, it is also a modified version of public key cryptography, in these various attributes are used to form a public key. This encryption technique help sender to define access policies for receiver and also provide fine access control to sender and that lead to control accessibility of data. In this methodology, we are just sending encrypted data over server which stores these data for further encrypted processing such as statistical computations, charts and report generation, forecasting etc. Using this technique, we are also providing data privacy as central system stored each data in encrypted form and can only be accessible by authorized person.

The authors of [4] experimented the attack on two lightweight cryptography algorithm i.e. SIMON and SIMECK by reducing their rounds. They reduced the round of SIMON(64/144) by 9 to 16 rounds and SIMECK64 by 2 rounds. After experiment on 45 round SIMON(64/144) and 42 rounds SIMECK64 they got very interesting results. SIMON algorithm is still more secure than SIMECK algorithm. Exponential time complexity is required to attack on these two algorithm and still got an success probability between 10% to 19%.

The authors of paper [5] suggest an encryption method based on simple mathematical

processes, as well as a simple authentication method based on a unique id. On ASCII values, the algorithm encrypts them. Each receiver has a distinct identifier, and the sender has a database of all receivers. There are three keys utilised in this game. The four random digits and receiver's alphanumeric id are used to create a palindrome number, which is used to create an encoding matrix. The encoding matrix and data ASCII values are used to encrypt data. The decryption procedure uses the decoding matrix, which is the inverse of the encoding matrix. However, security analysts have raised concerns about the entire procedure. The receiver receives the random number, keys and encrypted data seed from this point. Any intruder has the ability to launch a middle-man attack, leaving the entire process susceptible.

Authors of [6] present an approach based on a hybrid of the Genetic Algorithm (GA) and pseudorandom number sequence generating concepts. In this technique, only two GA operators are used. To choose the crossover operators among three. To produce pseudorandom sequences (uniform crossover, two points and single point) Blum Blum Shub is used. In addition, the encryption and decryption processes are carried out using five keys. The first key is an integer that specifies the block size used to partition plain text into blocks. The random sequences are generated using the second and third keys. The modulating factor is indicated by the fourth key, and the mutation oparation is indicated by the fifth key. The notion of GA and pseudorandom sequence generation is used in this technique to offer improved performance and security.

While studying above papers got some research gap that execution time is high of SIMON(64/96). While improving execution time of SIMON(64/96), SIMON(96/96), SIMON(128/128) ROM usage also increased. There are few works related to optimised SIMON(48/96), SIMON(64/128), SIMON(96/144), SIMON(128/192), SIMON(128/256).

3. Our Contribution

- To develop a modified approach to decrease the execution time. As the reduction of execution time helps in the faster communication between healthcare IoT device and main system or Doctor.
- To design modified approach to decrease the ROM usage.
- To deploy the approach on different multiple data key combination to verify check the performance. As some data key pair combination of SIMON algorithm using more RAM in optimized SIMON algorithm as compare to original algorithm as shown in fig 1, to overcome this problem we have introduced some solutions in Proposed Work. With all this changes lifetime of devices also will increased. This will very useful for devices which are implant in body of human with surgery like pacemaker.

4. Proposed Model

We are going to modify multiple parameters of algorithm in a such a way that the privacy will not compromise while doing this we will reduce the rounds of the algorithm so ROM usage will

Table 2
Literature Review

Year	Author	Objective	Limitations
2015[3]	Dhruti Sharma and Devesh Jinwala	Secure E-Health IOT system idea is given	Power Consumption of algorithms is not considered
2015[7]	Asmaa Sabet Anwar et al.	Security of image transmission	ROM usage is more
2017[8]	Athmika Aravind et al.	Working and implementation of IDEA and SIMON algorithms using Xilinx 14.2	SIMON's power consumption is less than IDEA but time delay is greater because of rounds.
2017[9]	Norah Alassaf et al.	Lightweight cryptography to secure medical data	ROM usage is not considered
2018[10]	Sohel Rana et al.	Comparison of light weight cryptographic algorithms	Response time Power Consumption of SIMON is greater then SPECK Cycle for key generation is greater than SPECK
2018[2]	Norah Alassaf et al.	Speedup algorithm	ROM usage is increases in SIMON(96/96) SIMON(128/128)
2018[11]	Mohamed Elhoseny et al.	Secure model for patient data transmission	Computation power is more
2019[1]	Bahram Rashidi	SIMON algorithm parameters	NA
2020[12]	Shrikant Taware et al.	Data Security	Power cunsumption is high
2021[4]	Gaëtan Leurent et al.	Attacks and security	Rounds of algorithm takes more time to execute
2021[13]	Anil Gopal Sawant et al.	Power Consumption	Execution speed is low
2021[14]	Bety Hayat Susanti et al.	Security	Power consumption is high

reduce and execution speed of algorithm will increase. Our main focus on the that data key combination for which there is very few work.

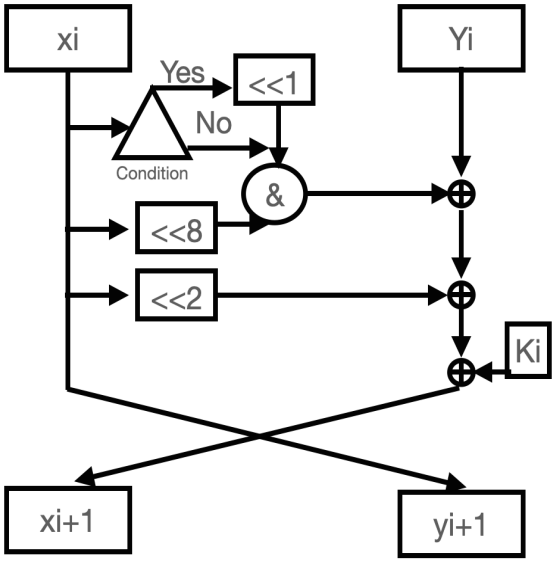

Figure 2: Proposed algorithm

In Fig 2 we have proposed the modified algorithm for SIMON algorithm. In this algorithm we are using left shift as the original SIMON algorithm for those data key pair combination where the ROM usage is increased by removing left shift by using simple if else condition in the program. Other data key pair combination will not use that left shift as they are performing well without that. Along with this we are going to reduce some rounds of some data key pair combinations of SIMON to increase the speed of algorithm and to decrease the ROM usage.

In Table 3 we have given the tentative reduction of the rounds for each data key combinations of SIMON algorithm. Security of algorithm is also considered while reducing the rounds of the SIMON algorithm. In existing SIMON algorithm there are 32 to 72 rounds. We are going to restrict that round by 0 to 9 cycles. By increasing the execution speed of the the algorithm power consumption will also going to decrease which will lead to increase the lifetime of healthcare devices.

5. Conclusion And Future Work

In this paper presented a modified version of SIMON lightweight cryptography algorithm for multi data key pair combinations to improve the execution speed and to decrease the ROM usage. Also focused on data key pair combinations having very few work related to that. This will help to increase the lifetime of the device as the time of execution and ROM usage of

Table 3
Rounds reduced for proposed algorithm

Block Size(2n)	Word Size(n)	Key Size(mn)	Key Word(m)	Rounds reduced by(r)
32	16	64	4	0-3
48	24	(72)(96)	(3)(4)	(0-4)(0-4)
64	32	(96)(128)	(3)(4)	(0-6)(0-6)
96	48	(96)(144)	(2)(3)	(0-7)(0-9)
128	64	(128)(192)(256)	(2)(3)(4)	(0-12)(0-14)(0-16)

algorithm is reduced. In future more modification in SIMON algorithms can done to increase the security without increasing the rounds of algorithm, So the execution speed and security both will not compromised.

References

[1] B. Rashidi, Flexible structures of lightweight block ciphers present, simon and led, IET Circuits, Devices & Systems 14 (2020) 369–380.

[2] N. Alassaf, A. Gutub, S. A. Parah, M. Al Ghamdi, Enhancing speed of simon: A light-weight-cryptographic algorithm for iot applications, Multimedia Tools and Applications 78 (2019) 32633–32657.

[3] D. Sharma, D. Jinwala, Functional encryption in iot e-health care system, in: International Conference on Information Systems Security, Springer, 2015, pp. 345–363.

[4] G. Leurent, C. Pernot, A. Schrottenloher, Clustering effect in simon and simeck, in: International Conference on the Theory and Application of Cryptology and Information Security, Springer, 2021, pp. 272–302.

[5] S. Dutta, T. Das, S. Jash, D. Patra, P. Paul, A cryptography algorithm using the operations of genetic algorithm & pseudo random sequence generating functions, International Journal 3 (2014).

[6] M. Alizadeh, M. Salleh, M. Zamani, J. Shayan, S. Karamizadeh, Security and performance evaluation of lightweight cryptographic algorithms in rfid, Kos Island, Greece (2012).

[7] A. S. Anwar, K. K. A. Ghany, H. E. Mahdy, Improving the security of images transmission, International Journal 3 (2015) 7–13.

[8] K. K. VG, A. Poojary, C. S. Rai, H. Nagesh, Implementation of lightweight cryptographic algorithms in fpga, in: 2017 International Conference on Circuits, Controls, and Communications (CCUBE), IEEE, 2017, pp. 232–235.

[9] N. Alassaf, B. Alkazemi, A. Gutub, Applicable light-weight cryptography to secure medical data in iot systems, Arabia (2003).
[10] S. Rana, S. Hossain, H. I. Shoun, M. A. Kashem, An effective lightweight cryptographic algorithm to secure resource-constrained devices, International Journal of Advanced Computer Science and Applications 9 (2018).
[11] M. Elhoseny, G. Ramírez-González, O. M. Abu-Elnasr, S. A. Shawkat, N. Arunkumar, A. Farouk, Secure medical data transmission model for iot-based healthcare systems, Ieee Access 6 (2018) 20596–20608.
[12] S. Taware, R. R. Chakravarthi, C. A. Palagan, K. Chandrasekaran, N. Vadivelan, Preserving mobile commerce iot data using light weight simon block cipher cryptographic paradigm, Journal of Ambient Intelligence and Humanized Computing 12 (2021) 6081–6089.
[13] P. Yalla, J.-P. Kaps, Lightweight cryptography for fpgas, in: 2009 international conference on reconfigurable computing and FPGAs, IEEE, 2009, pp. 225–230.
[14] B. Susanti, O. Permana, et al., Robustness test of simon-32, speck-32, and simeck-32 algorithms using fixed-point attacks, in: Journal of Physics: Conference Series, volume 1836, IOP Publishing, 2021, p. 012006.
[15] A. K. Mandal, C. Parakash, A. Tiwari, Performance evaluation of cryptographic algorithms: Des and aes, in: 2012 IEEE Students' Conference on Electrical, Electronics and Computer Science, IEEE, 2012, pp. 1–5.
[16] J. Gitanjali, N. Jeyanthi, C. Ranichandra, M. Pounambal, Ascii based cryptography using unique id, matrix multiplication and palindrome number, in: The 2014 International Symposium on Networks, Computers and Communications, IEEE, 2014, pp. 1–3.
[17] M. Hölbl, M. Kompara, A. Kamišalić, L. Nemec Zlatolas, A systematic review of the use of blockchain in healthcare, Symmetry 10 (2018) 470.
[18] A. Shehab, A. Ismail, L. Osman, M. Elhoseny, I. M. El-Henawy, Quantified self using iot wearable devices, in: International conference on advanced intelligent systems and informatics, Springer, 2017, pp. 820–831.