ORIGINAL RESEARCH

LightWeight energy-efficient Block Cipher based on DNA cryptography to secure data in internet of medical things devices

Nabila Zitouni[1] · Maamar Sedrati[1] · Amel Behaz[1]

Received: 3 July 2023 / Accepted: 3 October 2023 / Published online: 19 October 2023

Abstract The purpose of this study is to secure data in internet of medical things (IoMT) environment while saving energy to improve objects lifetime. Therefore, a new LightWeight energy-efficient Block Cipher based on DNA cryptography named LWBC_DNA is proposed in this paper. This cipher combines both DNA and lightweight cryptography and uses a hybrid Substitution Permutation Network and Feistel Network structure. LWBC_DNA cipher encrypts blocks of 64 bits under a key of only 16 bits through 16 iterative rounds using simple operations such as concatenation, XOR, and XNOR in order to produce a 32-bit ciphertext. Performance and security evaluation proved that LWBC_DNA cipher provides excellent security performance and satisfies IoMT devices requirements in terms of simplicity, storage space, and energy consumption. Besides, security analysis confirms that the LWBC_DNA cipher is very powerful against various cryptographic attacks.

Keywords Internet of medical things (IoMT) · IoMT security · IoMT objects longevity · Lightweight cryptography · DNA cryptography

✉ Nabila Zitouni
n.zitouni@univ-batna2.dz

Maamar Sedrati
m.sedrati@univ-batna2.dz

Amel Behaz
a.behaz@univ-batna2.dz

[1] LaSTIC Laboratory, University of Mustapha Ben Boulaid Batna 2, Universite Batna 2, Batna, Algeria

1 Introduction

Internet of things (IoT) is a communication technology that represents a network of interconnected objects which have enhanced capabilities to interact with each other as well as with humans and the world around them to accomplish a variety of services [1]. The communication between objects and their surrounding is ensured through the use of sensors. Thus, IoT can be considered as a network of sensors that collect data. The use of sensors in IoT objects makes these objects able to sense any changes in their environment and make autonomous decisions [2]. Therefore, IoT applications based on embedded devices equipped with computational and internet connectivity capabilities direct the world to become smarter through several real-life applications in different daily life application areas such as learning, transportation, building, healthcare, agriculture, and manufacturing [3].

The healthcare domain is an essential part of life and has great societal importance, especially with the increase in chronic diseases such as heart disease, diabetes and cancer, and more particularly in recent years with the outbreak of the 2019 coronavirus (COVID-19) global pandemic [4]. The two main aspects that significantly help in controlling the spread of the COVID-19 virus are adherence to social distancing recommendations and effective patient tracking and tracing [5]. IoT technology has the ability to provide remote monitoring and data collection services, which makes this technology a critical aspect in combating virus pandemics propagation and particularly in improving the healthcare domain. The integration of IoT technology in medical systems is referred to as the internet of medical things (IoMT) [4]. While the internet of medical things offers many benefits, it also faces several challenges. Security and privacy are among the main IoMT challenges, especially since healthcare systems deal with delicate medical data that is often essential to life [6]. Thus, a new IoMT security method has been developed in this study.

The residual paper starts with an overview of the IoMT technology. The previous works related to the pertinent field are presented in Sect. 3. Section 4 describes in detail the working of the proposed cryptographic algorithm, while its implementation and performance evaluation are discussed in Sect. 5. Finally, the paper is concluded with a conclusion and future research.

2 Internet of medical things (IoMT)

The internet of medical things is a variant of IoT technology tailored for the healthcare field, so it can be defined as a set of medical devices and applications connected to each other and to the internet in order to carry out a number of functions, the most important of which is remote monitoring [5]. The healthcare sector can be considered the biggest beneficiary of IoT technology due to the large number of IoMT features in diverse areas including patient safety, exercise, health monitoring, diagnostics tools, drug delivery, and many other medical applications [7]. Although IoMT has many features, it also faces many challenges. Security is one of the biggest issues of this technology, especially as the healthcare field handles sensitive data. Further, in this field, it is not sufficient to simply sense and transmit data; it must also ensure that it is secured during transmission. Thus, IoMT data security and protection is crucial and strong cryptographic methods are paramount requirements for securing and protecting this information [6]. These cryptographic methods provide patient privacy and data security against many dangerous attacks. Conventional cryptographic methods consume an excessive amount of battery power, computational power, and physical space [8]. In IoMT world, these requirements make these methods inefficient or difficult to implement because IoMT things are constrained devices (i.e., limited in treatment and energy). Therefore, selecting the appropriate cipher that can provide maximum security while using minimum resources is a challenging task for IoMT devices.

LightWeight Cryptography (LWC) is a new cryptography field that seeks to offer solutions suitable for resource-constrained devices [9]. LWC algorithms are classified into symmetric and asymmetric algorithms. While addressing security issues for IoMT devices, lightweight symmetric algorithms are more beneficial as they use only one key to encrypt and decrypt data providing a simplified and faster operation. Unlike lightweight asymmetric algorithms that use a public and private key pair, one key is used in encryption and an alternate key is used in decryption, which makes them more complex, slower, and need more computational power [8]. Lightweight symmetric algorithms include lightweight stream ciphers, lightweight block ciphers, and lightweight hash functions. The lightweight block cipher type is more efficient and practically easier to implement when securing IoMT objects [10]. Substitution Permutation Network (SPN) and Feistel-based Network (FN) are the two main structures of lightweight block cipher algorithms. FN structure algorithm splits the block into two equal-sized blocks known as the left block and right block. In each round, a round function is applied to the key and the right block; the output is XOR-ed into the left block. Then, Blocks are swapped. On the other hand, the SPN structure algorithm is designed to work with the whole data block without needing to split it, where the data block is passed through several alternating rounds of substitution boxes (S-boxes) and permutation boxes (P-boxes) [9].

In contrast to block ciphers based on SPN structure, FN block ciphers take a long time and require a high number of rounds which results in consuming a large amount of energy. On the other hand, they have the same program for encryption and decryption processes as well as a small and simple round function, which leads to reduced hardware implementation costs [9]. In conclusion, FN structure is a good choice for applications where the implementation cost is more important than the security level, and SPN structure is preferred for applications where moderate security is needed. While the SPN-FN structure combination takes advantage of the features of both structures, achieving the objective of this research, which is securing IoMT objects while saving energy.

3 Related works

Lang Li et al. [11] proposed in 2016 an ultra-lightweight block cipher named QTL. This cipher uses a combination of both SPN and FN structure to cipher blocks of size 64 bits under keys of lengths 64 or 128 bits through 16 and 20 iterative rounds. QTL cipher uses four round sub-keys and two main operations, AddConstants and AddRoundKey, to encrypt data. The encryption and decryption algorithms are the same except for the round constants and round sub-keys which are used in reverse order to decrypt data. In order to mitigate the amount of area requirement and power consumption cost, this cipher avoided using a key schedule. The implementation of QTL required 1025.52 GE for QTL-64 and 1206.52 GE for QTL-128. According to the security evaluation of QTL block cipher performed by [12], QTL is not resistant to the standard statistical attacks on block ciphers and this is the principal drawback of this approach.

In 2017, a new lightweight encryption algorithm with a hybrid structure called Secure IoT (SIT) was developed [13]. SIT uses a 64-bit key to encrypt 64-bit blocks through five iterative rounds. Key expansion and Encryption are the two fundamental processes of SIT cipher. The Key expansion process is responsible to generate five unique keys used in the five rounds of the Encryption process. Both processes, Key expansion and Encryption, use very basic operations such as concatenation, XOR, and shifting. The research conducted in [14] employed the SIT lightweight block cipher to encrypt medical images. The results proved that this cipher provides sufficient security for medical images and has higher entropy[1], and better NPCR and UACI[2]. However, a detailed analysis of possible attacks has not been conducted.

SFN [15] is another lightweight block cipher that has a hybrid SPN and Feistel network structure. It was created in 2018 to be applied in constrained environments. SFN cipher uses 32 iterative rounds to cipher a 64-bit block under a key of 96 bits. This key is divided into two keys, the round key and the control key that are 64-bit and 32-bit respectively. This cipher is designed to be compact in both hardware environment and software platforms, where its hardware implementation requires 1876.04 GE. SFN cipher security analysis proves its immunity against several attacks, including related-key attacks, algebraic attacks, integral attacks, etc. Nevertheless, according to the comparative analysis of the most popular lightweight block ciphers performed by [16], the SFN cipher is not optimal in terms of size and speed.

In 2020, a new lightweight block cipher that is well suited for IoT communication called LRBC was introduced by Biswas and al. [17]. The cipher LRBC has a hybrid type structure (i.e., SPN and Feistel structure), a key size of only 16 bits, and a block size of 16 bits. There are 24 iterative rounds in this cipher; each round uses simple logical operations such as XOR operations, XNOR operations, concatenation, and transposition process. LRBC ensures high security with a balanced area and power consumption, where it takes for hardware implementation an area of 258.9 GE. Additionally, its smaller key size and key-consideration method allow it to consume less power and memory. The LRBC security evaluation demonstrated a security level of the cipher, where the avalanche effect is determined to be 55.75% and 58% concerning key and plaintext respectively, with robustness against linear, differential, and side channel attacks.

Hybrid Lightweight Cipher Algorithm (HLCA) was presented in 2021 by Al-Rahman and al. [18]. This cipher utilizes a mixture of SPN and FN structures and a 64-bit key to encrypt a 64-bit block in 10, 16, or 20 iterative rounds. At each round, one of the round function structures, Feistel round function or SPN round function, is chosen to cipher data. The determination of the round function structure is based on the binary bit-value of the secret key. The Feistel round function is selected if the binary bit-value is equal to zero; otherwise, the SPN round function is selected. Results of cipher implementation and evaluation with text and image data proved the strength and security level of the cipher using several important metrics including avalanche effect, execution time, correlation, entropy, NPCR and UACI. Nevertheless, a comprehensive analysis of potential attacks has not been performed.

Table 1 General characteristics of SPN-FN structure lightweight block ciphers

Cipher	Year	Block size (bits)	Key size (bits)	Rounds	Area (GE)
QTL	2016	64	64/128	16/20	1026
SIT	2017	64	64	05	–
SFN	2018	64	96	32	1876.04
LRBC	2020	16	16	24	258.9
HLCA	2021	64	64	10/16/20	–
LCB	2021	32	64	10	224

Another lightweight block cipher that uses a combination of SPN and Feistel structure to secure IoT devices was designed in 2021 [19]. This cipher, called LCB, operates with a block size of 32 bits and a key size of 64 bits. LCB cipher encrypts data in 10 rounds using simple operations such as XOR, bit scrambling, and concatenation. The decryption process of this cipher is the reverse manner of the encryption process. LCB needs a hardware area of 224 GE. This secure cipher satisfies the requirements of resource-constrained devices in terms of simplicity, power, and storage space. LCB cipher provides excellent security performance with an avalanche effect of 63.875% and 63.125% for plaintext and key respectively. Besides, it is immune to different types of cryptographic attacks.

Table 1 shows a comparison between the above discussed SPN-FN structure lightweight block ciphers; this comparison is based on the general characteristics of each cipher. All block ciphers convert a number of data bits into another form through a limited number of rounds using a number of bits as a key. These ciphers vary in their resource utilization (hardware implementation, energy consumption, etc.). Due to the applications variability and their requirements, it is difficult to define an algorithm that is suitable for all types of applications and devices. Since most IoMT objects are battery-powered devices where energy is limited and batteries are the only power source, securing IoMT devices needs a lightweight cipher with SPN-FN combined structure and consumes less energy. Among the SPN-FN ciphers compared above, the LRBC cipher is chosen as the focus of the study because it is the most suitable for IoMT devices in

[1] Entropy is an indicator of information randomness. It is used to measure the randomness of data after encryption.

[2] NPCR (Number of Changing Pixel Rate) and UACI (Unified Averaged Changed Intensity) are the two most common factors used to evaluate the strength of image encryption ciphers.

terms of security and energy consumption. The parameters that can reduce energy consumption and optimize IoMT devices' battery lifetime are key size, the number of rounds, and hardware implementation. LRBC cipher has a small key size, a moderate number of rounds, and a small hardware implementation which reduce energy consumption.

4 Overview of proposed algorithm

DNA cryptography [20] is a branch of biological science that combines cryptography with molecular biology for data hiding and more secure data transmission. In this cryptography field, data is encoded using four nucleotide bases, namely: A, T, C, and G for respectively Adenine, Thymine, Cytosine, and Guanine. These nucleotides are complementary in pairs, where the pairs (C, G) and (A, T) complement each other [21]. The main advantages of DNA cryptography are its minimal power and storage requirements.

The proposed cipher named LWBC_DNA, which combines both DNA and lightweight cryptography, provides a simple structure suitable for the IoMT environment. This cipher is a lightweight symmetric key block cipher with a hybrid SPN and Feistel network structure. It uses simple logical operations like concatenation, XOR, and XNOR operations. In the symmetric key algorithm, the data is encrypted by passing it through several rounds, where increasing the number of rounds ensures better security but leads to an increase in energy consumption. To maintain the strength of the encryption process, cryptographic algorithms are typically designed to take an average of 10 to 20 rounds [15]. Therefore, the proposed algorithm uses an average number of rounds (16 rounds) to cipher data, which ensures a security level and also minimizes energy consumption. LWBC_DNA works with a 64-bit data block, thus the lengthy plaintext is divided into several blocks of 64-bit length that are processed sequentially. The final ciphertext is obtained by merging the processing results of all data blocks. The block of 64 bits is encrypted using a secret key of size 16 bits and three main operation layers, DNA coding layer, Encryption layer, and DNA_ASCII layer.

4.1 Key generation

Building a lightweight cryptographic process requires strong and simple key generation. In the proposed method, four sub-keys K_i $(0 \le i \le 3)$ with 4 bits each are used in both encryption and decryption operations. These four sub-keys are derived from the main secret key which consists of 16 nucleotides N_j $(1 \le j \le 16)$, so each sub-key is composed of 4 nucleotides, where the nucleotides of K_i are nucleotides satisfying Eq. (1).

$$\mathrm{j \bmod 4 = i} \tag{1}$$

Table 2 DNA letters and their binary representation

DNA letter	Binary representation
A	00
T	11
C	01
G	10

4.2 DNA coding layer

LWBC_DNA utilizes a key of 16 nucleotide bits to cipher blocks of 64 binary bits. In the DNA coding layer, the binary plaintext bits are converted into a DNA sequence. The DNA sequence is composed of a series of letters (A, T, C, G), where each of these four letters represents a nucleotide and two binary bits. Therefore, the 64 bits binary plaintext (PT) is converted into a DNA sequence (DNA_PT) of 32 nucleotide bits. As in DNA coding where the pairs (C, G) and (A, T) complement each other, in binary coding the numbers 0 and 1 are complementary. Therefore, the pairs (00, 11) and (01, 10) also complement each other. Since each nucleotide letter represents two binary bits, there are 4! = 24 possible encoding methods. Nevertheless, only eight coding methods are convenient for the complementarity principle. Table 2 represents one of these eight coding methods.

4.3 Encryption layer

Plaintext protection is the main purpose of a cipher, where the encryption process is the procedure that transforms the clear plaintext into an unreadable form using confusion and diffusion techniques. Thus, making this procedure more resistant to cryptanalysis attacks is crucial.

In the LWBC_DNA encryption process, the DNA_PT sequence consists of 32 nucleotide bits N_j $(1 \le j \le 32)$ is divided into eight 4-bit sub-blocks DNA_PT_k $(0 \le k \le 7)$. Each DNA_PT_k is composed of nucleotides satisfying Eq. (2). These sub-blocks are passed for 16 consecutive rounds through three repeating steps, AddRoundKey, F-Function, and Round Transposition. The ciphertext generated after completing 16 consecutive rounds is converted to DNA_ASCII form. The encryption algorithm of the LWBC_DNA cipher is shown in Fig. 1 and is clearly represented in Algorithm 1. Notations used in the explanation algorithms are shown in Table 3.

$$jmod8 = k \tag{2}$$

4.3.1 AddRoundKey step

In the LWBC_DNA encryption process, four sub-keys are used through 16 rounds. At each round, only one sub-key is

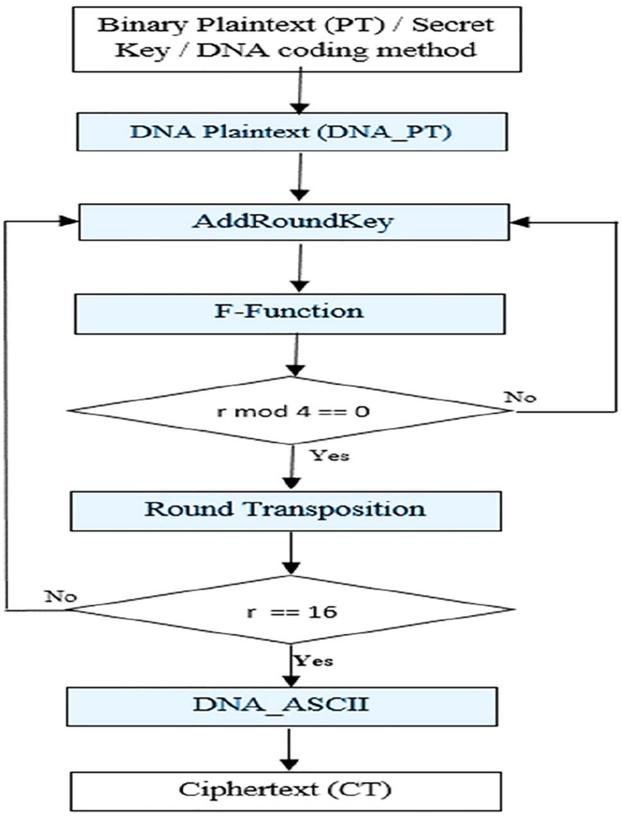

Fig. 1 Encryption procedure of LWBC_DNA cipher

Table 3 Notations

Notation	Function
⊕	XOR
⊙	XNOR
‖	Concatenation

used called the round key. The round key used in the round r is the sub-key K_i satisfying Eq. (3).

$$i = rmod4 \tag{3}$$

In an iterative round, the round key is XOR-ed with only half of the sub-blocks. These sub-blocks are DNA_PT_k satisfying Eq. (4). Therefore, the AddRoundKey consists of the DNA_XOR operation between the round key and each one of the four sub-blocks satisfying Eq. (4). The four 4-bit blocks resulting from the XOR operation act as input for the next step which is the F-Function operation. The DNA_XOR operation of the DNA coding method shown in Table2 is presented in Table 4, while the DNA_XNOR operation is the complementary of the DNA_XOR operation.

$$kmod2 = rmod2 \tag{4}$$

Table 4 DNA XOR operation

XOR	A	T	C	G
A	A	T	C	G
T	T	A	G	C
C	C	G	A	T
G	G	C	T	A

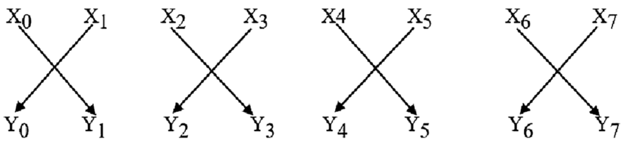

Fig. 2 Round transposition process of LWBC_DNA cipher

4.3.2 *F-Function step*

The F-Function design of the proposed LWBC_DNA algorithm is characterized by its great security and lightweight, where this function receives from the AddRoundKey step four 4-bit blocks. These blocks are passing through three different types of computing boxes: S-box, P-box, and L-box respectively. The S-box process takes the four F-Function input blocks as input, whereas the P-box process utilizes the calculated result of the S-box process as input. In the same way, the P-box output is applied as the input of the L-box process. The operations adopted inside each of these boxes are the computing boxes operations of the LRBC [17] cipher that have been modified to be suitable for DNA cryptography. The computations performed by boxes within the F-function of the proposed LWBC_DNA cipher are presented in Algorithm 2.

4.3.3 *Round transposition step*

The round transposition is a process that provides an additional level of security for the data. Therefore, in the proposed algorithm, after every four rounds, all sub-blocks are permuted as shown in Fig. 2. In this process, the sub-blocks of the pairs (DNA_PT_0, DNA_PT_1), (DNA_PT_2, DNA_PT_3), (DNA_PT_4, DNA_PT_5), and (DNA_PT_6, DNA_PT_7) are swapped.

4.4 DNA_ASCII layer

Securing the communication is not only encrypting the message, but it is also necessary to hide the encrypted message. The proposed LWBC_DNA cipher offers an extra layer of data security, where the ciphertext is hidden in a DNA-ASCII form. Therefore, the ciphertext DNA sequence (DNA_CT) is converted to DNA-ASCII form according to

Table 5 DNA-ASCII table

DNA sequence	DNA-ASCII code	DNA sequence	DNA-ASCII code
A A	0	G A	8
A C	1	G C	9
A G	2	G G	A
A T	3	G T	B
C A	4	T A	C
C C	5	T C	D
CG	6	T G	E
C T	7	T T	F

the DNA-ASCII table presented in Table 5. The result represents the final ciphertext (CT).

4.5 Decryption process

The transformation of encrypted data into its original form is called decryption, thus the decryption operation is the process of converting data that has been turned unreadable through the encryption process into its unencrypted form. Since the proposed LWBC_DNA cipher is a lightweight cipher with SPN-FN combined structure, the decryption algorithm is the reverse manner of the encryption process.

5 LWBC_DNA implementation and results

Although there is no simulator that is 100% efficient, employing certified and well-known network simulators is a useful technique to design and evaluate the performance of a new cipher. In order to carry out the proposed LWBC_DNA cipher performance, the network simulator named Cooja is used in Contiki-NG [22], which is a lightweight open source operating system developed for low-powered devices. The routing protocol used is the routing protocol for Low-Power and Lossy Networks called RPL [23]. The used simulation parameters are shown in Table 6, and the simulation results are discussed in the next sections.

5.1 Performance evaluation

5.1.1 Energy consumption

Reducing the energy consumption of IoMT devices is an important aspect to optimize device lifetime. Therefore, measuring the energy consumed by the device is crucial to evaluate the proposed cipher. The power trace tool provided by the network simulator Cooja is used to estimate power consumption. This tool tracks the device state, where

```
Input: 64-bit plaintext (PT), 16-bit Secret key (K),
       DNA coding method (C_DNA).
Output: 32-bit ciphertext.
Generate DNA_PT [1:32] using C_DNA method.
Divide DNA_PT into eight equal length sub-blocks
  $DNA\_PT_k[1:4] \mid_{0 \le k \le 7}$ as,
      $DNA\_PT_k = \big\|_{j=1}^{32} DNA\_PT[j],\ j \bmod 8 = k$
Generate the sub-keys $K_i[1:4] \mid_{0 \le i \le 3}$ divided from the secret key
  K [1:16] as,
      $K_i = \big\|_{j=1}^{16} K[j],\ j \bmod 4 = i$
For r = 1 to 16 by step 1 do
    Select the Round Key RK as, $RK = K_i,\ i = r \bmod 4$
    Add the Round Key RK to four sub-blocks $DNA\_PT_k$ as,
      $DNA\_PT_k = DNA\_PT_k \oplus RK,\ k \bmod 2 = r \bmod 2$
    Compute F-Function with the four sub-blocks $DNA\_PT_k$ added
      with the Round key RK.
    If (r mod 4 = = 0) then
        For k = 0 to 7 by step 2 do
            Permute ($DNA\_PT_k$, $DNA\_PT_{k+1}$)
End for ; End if ; End for
Generate DNA_Ciphertext as, $DNA\_CT = \big\|_{k=0}^{7} DNA\_PT_k$
Generate final Ciphertext as,
      CT = DNA_ASCII (DNA_CT)
```

Algorithm 1: LWBC_DNA Encryption Algorithm

```
Input: Four sub-blocks of DNA plaintext $PT_1, PT_2, PT_3, PT_4$
Output: Four DNA sequences
    V [4]= {A, T, C, G}
1.  S-box computation
        $IS_1 = PT_1 \oplus V$ ,  $IS_2 = PT_2 \oplus V$
        $IS_3 = PT_3 \oplus V$ ,  $IS_4 = PT_4 \oplus V$
2.  P-box computation
        $P_1 = IS_1[1] \| IS_2[4] \| IS_1[2] \| IS_2[3]$
        $P_2 = IS_1[3] \| IS_2[2] \| IS_1[4] \| IS_2[1]$
        $P_3 = IS_3[1] \| IS_4[4] \| IS_3[2] \| IS_4[3]$
        $P_4 = IS_3[3] \| IS_4[2] \| IS_3[4] \| IS_4[1]$
3.  L-box computation
    $T[1] = (P_1[1] \oplus P_2[4])$ ; $X[1] = (P_1[1] \odot A)$
    $T[2] = (P_1[2] \odot P_2[3])$ ; $X[2] = (P_1[2] \oplus T)$
    $T[3] = (P_1[3] \oplus P_2[2])$ ; $X[3] = (P_1[3] \odot C)$
    $T[4] = (P_1[4] \odot P_2[1])$ ; $X[4] = (P_1[4] \oplus G)$
    $T[5] = (P_3[1] \oplus P_4[4])$ ; $X[5] = (P_2[1] \odot A)$
    $T[6] = (P_3[2] \odot P_4[3])$ ; $X[6] = (P_2[2] \oplus T)$
    $T[7] = (P_3[3] \oplus P_4[2])$ ; $X[7] = (P_2[3] \odot C)$
    $T[8] = (P_3[4] \odot P_4[1])$ ; $X[8] = (P_2[4] \oplus G)$
  $L_1 = T[1] \| X[4] \| T[2] \| X[3] \| T[3] \| X[2] \| T[4] \| X[1]$
  $L_2 = T[5] \| X[8] \| T[6] \| X[7] \| T[7] \| X[6] \| T[8] \| X[5]$
$Z = L_1 \| L_2$
  $PT_1 = Z[1:4]$ , $PT_2 = Z[5:8]$ , $PT_3 = Z[9:12]$ , $PT_4 = Z[13:16]$
4.  End.
```

Algorithm 2: F-Function

Table 6 Simulation parameters

Parameters	Value
Mote device type	Z1 Zolertia
Voltage (vol)	3 V
TX current (TX_C)	17.4 mA
RX current (RX_C)	18.8 mA
CPU idle current (CPU_C)	0.426 mA
CPU power down current (LPM_C)	0.020 mA
RAM	8 KB
Flash memory	92 KB
ROM	96 KB
Transport protocol	UDP
Routing protocol	RPL (IPV6)
RTIMER_SECOND	32,768 ticks per second
Runtime	10 s
Microcontroller	MSP430F2617
Radio	CC2420

it keeps a record of power consumption and resource utilization of a device, and it produces energy consumption of the device or the sensor node in different states based on workload measurement interval (Runtime).

The energy consumption is categorized into four categories named TX, RX, CPU, and LPM. CPU Energy is the energy used for the computation process by the CPU, and LPM energy is the energy used when the CPU is in an idle state. TX energy refers to the energy consumed while the radio is in transmit mode, while RX energy refers to the energy consumed while the radio is in receive mode. The energy consumption is calculated using Eq. (5) [24].

$$\text{Energy(mW)} = \frac{\left(\text{CPU} * \text{CPU}_{\text{C}} + \text{LPM} * \text{LPM}_{\text{C}} + \text{TX} * \text{TX}_{\text{C}} + \text{RX} * \text{RX}_{\text{C}}\right) * \text{Vol}}{(\text{RTIMER} * \text{Runtime})} \tag{5}$$

The results of the energy consumption simulations showed that the energy consumed by the proposed LWBC_DNA cipher to manipulate data of size 64 bits is 0.8892 mW, while the energy consumed by the LRBC cipher to manipulate data of size 16 bits is 0.9819 mW. Therefore, as shown in Fig. 3, the LRBC cipher consumes more energy compared to the proposed LWBC_DNA cipher, and it increases when manipulating data with a long size.

5.1.2 Execution time

The cipher execution time is one of the most important factors in evaluating lightweight ciphers. Cipher execution time is the total time required to encrypt/decrypt specific data. The Rtimer library is one of the timer libraries provided by the Contiki-NG system. This library provides scheduling and execution of real-time tasks. According to execution time results, both LRBC and LWBC_DNA cipher require a few milliseconds as runtime. Manipulating 16-bit size data using LRBC cipher takes a time of 284 ms, while the proposed LWBC_DNA cipher requires a time of 705 ms to manipulate data of size 64-bit. Whereas, as shown in Fig. 4, the LRBC cipher requires a large amount of time compared to the LWBC_DNA cipher while implementing a long size data.

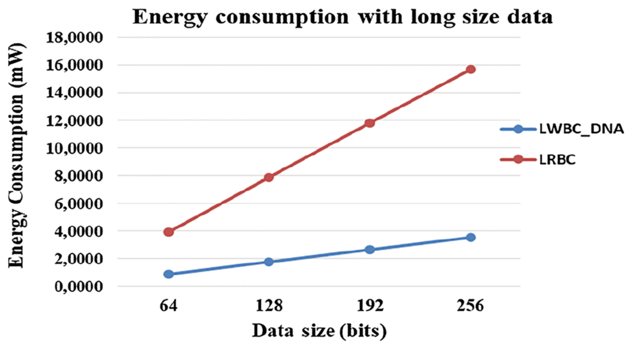

Fig. 3 Energy consumption with long size data

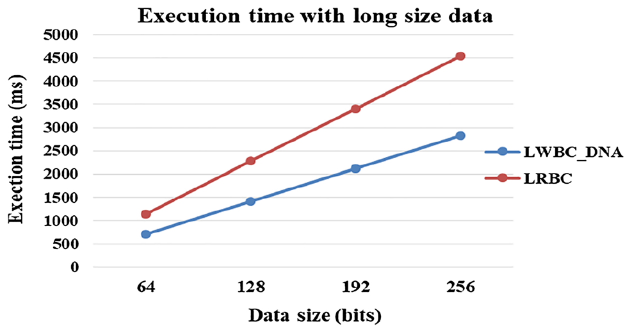

Fig. 4 Execution time with long size data

5.1.3 Hardware implementation

Energy consumption is one of the main challenges in constrained objects. Since the area required to implement a cipher directly affects energy utilization, hardware implementation is a critical issue when designing a lightweight encryption cipher to secure constrained objects. The proposed LWBC_DNA cipher implementation uses a 64-bit plaintext and a 16-bit key in order to generate the result after 16 rounds. The cipher consists of a 4×4 S-box, which takes less area and energy consumption compared to the

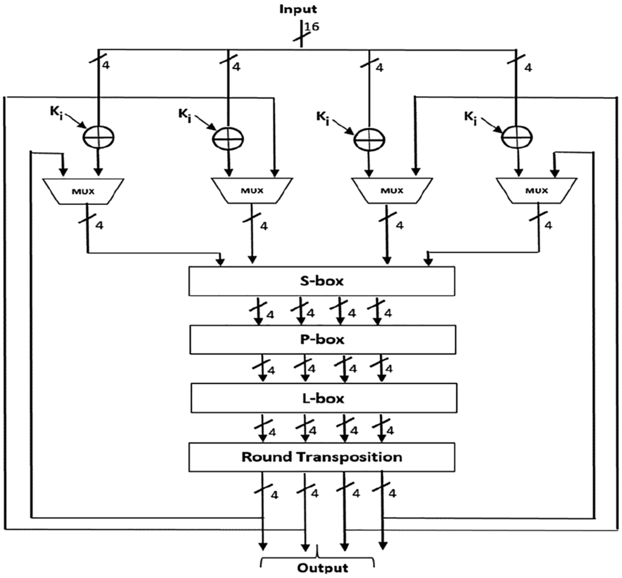

Fig. 5 Data path of LWBC_DNA cipher

8 × 8 S-box, in addition to concatenation, XOR, and XNOR lightweight operations.

Lightweight cipher hardware implementation is measured in gate equivalent (GE), which represents the physical area required to implement the cipher. Where one GE is equal to the area of a two-input NAND gate [25]. LWBC_DNA cipher data path represented in Fig. 5 shows the functional units that carry out data processing operations. The proposed cipher consists of four 4-bit 2-to-1 multiplexers (MUX), eight 4-bit XOR operations, and sixteen 1-bit XOR operations. Since each 1-bit XOR operation requires 1.76875 GE, a 4-bit XOR operation costs 7.075 GE area. While 4-bit 2-to-1 MUX takes an area of 0.5 GE [11]. Table 7 details the area required for different components used in the proposed cipher.

Table 7 Area requirement of LWBC_DNA

Module	Area (GE)
Data register	344
Sixteen 1-bit XOR	1.76875 × 16 = 28.3
Eight 4-bit XOR	7.075 × 8 = 56.6
Four 4-bit 2-to-1 MUX	0.5 × 4 = 2
Round transposition	0
Key register	86
Total	516.9

5.2 Security analysis

5.2.1 Avalanche effect

Avalanche effect (AE) is considered one of the most important security analyses when evaluating the security strength and goodness of a cryptographic cipher. This analysis checks the cipher sensitivity to any minor change in plaintext or key, where any random change in one of the input bits results in a significant change in ciphertext. When change influences at least half of the ciphertext bits (50%), the avalanche effect is considered as good [26]. Therefore, a higher avalanche effect implies greater security. The avalanche effect is calculated using Eq. (6).

$$AE = \frac{\text{Number of changed bit in ciphertext}}{\text{Number of bits in ciphertext}} * 100\% \tag{6}$$

The Hamming Distance (HD) between two equal length sequences is the number of different positions between the two sequences. This metric is used to measure the edit distance between two sequences. The avalanche effect estimation of the proposed LWBC_DNA cipher is performed by taking a fixed secret key and changing the hamming distance of the plaintext randomly up to 5 bits in five different test cases. The same procedure is employed for fixed plaintext and variable secret key. Graphical representations of the LWBC_DNA avalanche effect are presented in Figs. 6 and 7 for plaintext and key respectively. The proposed LWBC_DNA cipher avalanche effect is determined to be 60.625% and 69.5% concerning plaintext and key respectively. Thus, the proposed cipher achieves a considerable level of confusion and diffusion.

5.2.2 Attacks analysis

5.2.2.1 Linear attack The linear attack is one of the most critical attacks that can be used against symmetric key block ciphers. This attack type is referred to as a known plaintext attack, in which the attacker knows a random set of plaintexts and their corresponding ciphertexts. The linear attack is based on the study of probabilistic linear relationships between each plaintext and its corresponding ciphertext with the aim of approximating S-box operations using a linear expression in the form of Eq. 7 [17]. Where Xi = [Xi_1, Xi_2,…..] is the S-box input and Yi = [Yi_1, Yi_2,…….] is its corresponding output.

$$Xi1 \oplus Xi2 \oplus \ldots . \oplus Xin \oplus Yi1 \oplus Yi2 \oplus \ldots .. \oplus Yim = 0 \tag{7}$$

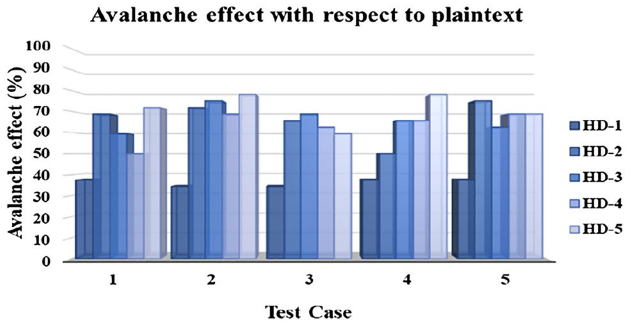

Fig. 6 Avalanche effect analysis with respect to plaintext

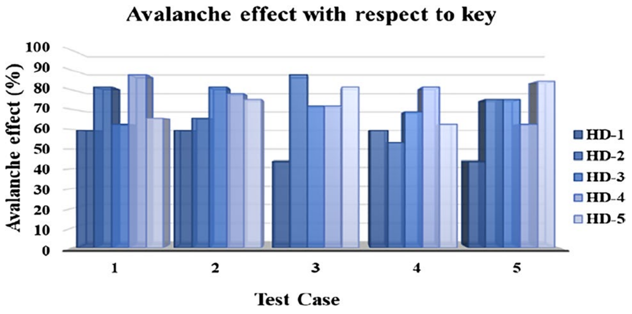

Fig. 7 Avalanche effect analysis with respect to key

As the S-box input bits of the proposed cipher are nucleotide bits, this S-box has $4^4 = 256$ possible inputs. Considering T the number of times a linear approximation holds, the associated probability of the linear approximation is calculated by $p = \frac{T}{4^4}$ while the corresponding bias is determined as $\varepsilon = P - \frac{1}{4}$. A bias value closer to $\frac{1}{4}$ indicates more protection against linear attack. Table 8 shows a sample of linear probability analysis of the proposed cipher S-Box taking five different random linear expressions. It has been noticed that most linear expressions have a linear probability value of exactly $\frac{1}{4}$ where the bias value is$\frac{1}{4} - \frac{1}{4} = 0$. Therefore, the LWBC_DNA cipher provides a higher level of protection against linear attacks.

Table 8 Linear probability analysis

Linear expression	Linear probability	Probability bias
$X1 \oplus X3 \oplus Y3 \oplus Y4$	1/4	0
$X2 \oplus X3 \oplus Y2$	1/4	0
$X1 \oplus X2 \oplus X4 \oplus Y_2 \oplus Y3$	1/4	0
$X4 \oplus Y3 \oplus Y4$	1/4	0
$X3 \oplus Y1 \oplus Y2 \oplus Y4$	1/4	0

5.2.2.2 Side channel attack Side channel attack is one of the powerful attacks against cryptographic techniques, especially lightweight ciphers. This attack is based on information involving the secret key generated by cryptographic cipher implementation, which makes it possible to discover the secret key from measured data [27]. Since the round keys used in the proposed cipher are independent of the plaintext, it is therefore impossible for an attacker to discover the secret key used. Thus, the LWBC_DNA cipher has high resistance against the side channel attack.

5.2.2.3 Related key attack In cryptography, a related key attack is a form of cryptanalysis in which the attacker observes cipher operation under several different keys in an attempt to determine the original key bits. In an encryption process, the related key attack can be possible only when the same key is used for all rounds [17]. In the proposed cipher, the secret key is divided into four independent sub-keys, and a different sub-key is used in each round. Therefore, it is more difficult for an attacker to determine the exact secret key sequence used. As a result, the LWBC_DNA cipher has great resistance to the related key attack.

5.3 Functionality analysis

LWBC_DNA cipher uses a hybrid SPN and FN structure to exploit the benefits of both structures, along with small block size and key size which facilitates the rapid diffusion of plaintext bits. The main purpose of combining lightweight and DNA cryptography is to improve data security and reduce power consumption. In the proposed cipher, the security depends on the secret key and DNA coding method, and the ciphertext is hidden in a DNA-ASCII form, which adds an extra layer of security.

Performance and security evaluation results demonstrated that LWBC_DNA ensures a high level of security and meets all requirements of resource-constrained devices. Energy consumption, execution time, and area requirements are the three analysis types used to evaluate the proposed cipher performance. Whilst the security strength has been estimated using avalanche effect and attack analysis. Experimental results show that the proposed LWBC_DNA cipher has an excellent performance in securing IoMT devices data with good avalanche effect and resistance against linear, side channel, and related key attacks. In addition to low requirements in terms of energy consumption, computational time, and area requirements.

6 Conclusion

In this research work, a new lightweight block cipher termed LWBC_DNA for resource-constrained IoMT devices is proposed. LWBC_DNA cipher enhances data security and objects longevity by combining both lightweight and DNA cryptography additionally to the benefits of both Feistel and SPN structure. Exploiting the random nature of DNA sequence allows the production of a robust secret key that is difficult for attackers to crack. Further, the main purpose of employing DNA sequences to encrypt data is to improve security and reduce power consumption. LWBC_DNA cipher achieves good confusion and diffusion effects with low computational time, area requirements, and energy consumption. In addition, it provides an extra layer of data security, where the ciphertext is hidden in a DNA-ASCII form. Unlike the security of modern cryptography ciphers that relies only on the key, the proposed cipher security relies on two factors, the key and the DNA coding method. As a result, the LWBC_DNA cipher ensures a high level of security, making it a promising technique to use in most IoMT devices.

7 Future research

The main objective of the proposed algorithm is to secure data in IoT devices while saving energy to improve objects lifetime, taking IoMT as an example. In our future work, we plan to analyze the powerful of our proposed security cipher against other cryptographic attacks. In addition, we intend to develop the proposed cipher in a real IoT platform to evaluate its performance.

Declarations

Conflict of interest Authors declare no conflict of interest.

References

1. Abi Sen AA, Eassa FA, Jambi K, Yamin M (2018) Preserving privacy in internet of things: a survey. Int J Inf Technol 10:189–200
2. Rishiwal V, Singh O (2021) Energy efficient emergency rescue scheme in wireless sensor networks. Int J Inf Technol 13:1951–1958
3. Sen AA, Yamin M (2021) Advantages of using fog in IoT applications. Int J Inf Technol 13:829–837
4. Asghari P (2021) A diagnostic prediction model for colorectal cancer in elderlies via internet of medical things. Int J Inf Technol 13(4):1423–1429
5. Udgata SK, Suryadevara NK (2021) COVID-19 sensors and internet of medical things (IoMT). Internet of things and sensor network for COVID-19. Springer Singapore, pp 39–53
6. Chaudhary RR, Chatterjee K (2022) A lightweight security framework for electronic healthcare system. Int J Inf Technol 14(6):3109–3121
7. Shakeel T, Habib S, Boulila W, Koubaa A, Javed AR, Rizwan M, Sufiyan M (2022) A survey on COVID-19 impact in the healthcare domain: worldwide market implementation, applications, security and privacy issues, challenges and future prospects. Complex Intell Syst. https://doi.org/10.1007/s40747-022-00767-w
8. Bhardwaj I, Kumar A, Bansal M (2017) A review on lightweight cryptography algorithms for data security and authentication in IoTs. 2017 4th International Conference on Signal Processing, Computing and Control (ISPCC). pp. 504–509
9. Dhanda SS, Singh B, Jindal P (2020) Lightweight cryptography: a solution to secure IoT. Wireless Pers Commun 112(3):1947–1980
10. Shamala LM, Zayaraz G, Vivekanandan K, Vijayalakshmi V (2021) Lightweight cryptography algorithms for internet of things enabled networks: an overview. J Phys Conf Ser 1717(1):012072
11. Li L, Liu B, Wang H (2016) QTL: a new ultra-lightweight block cipher. Microprocess Microsyst 45:45–55
12. Sadeghi S, Bagheri N, Abdelraheem MA (2017) Cryptanalysis of reduced QTL block cipher. Microprocess Microsyst 52:34–48
13. Usman M, Ahmed IA, Imran M, Khan S, Ali U (2017) SIT: a lightweight encryption algorithm for secure internet of things. Int J Adv Comput Sci Appl. https://doi.org/10.14569/IJACSA.2017.080151
14. Mishra Z, Mishra S, Acharya B (2021) High throughput novel architecture of SIT cipher for IoT application, nanoelectronics circuits and communication systems. Springer Singapore, pp 267–276
15. Li L, Liu B, Zhou Y, Zou Y (2018) SFN: a new lightweight block cipher. Microprocess Microsyst 60:138–150
16. Sehrawat D, Gill NS, Devi M (2019) Comparative analysis of lightweight block ciphers in IoT-enabled smart environment. 2019 6th International Conference on Signal Processing and Integrated Networks (SPIN), (pp. 915--920)
17. Biswas A, Majumdar A, Nath S, Dutta A, Baishnab K (2020) LRBC: a lightweight block cipher design for resource constrained IoT devices. J Ambient Intell Humaniz Comput. https://doi.org/10.1007/s12652-020-01694-9
18. Al-Rahman SQ, Sagheer A, Dawood O (2021) A hybrid lightweight cipher algorithm. Int J Comput Digital Syst. https://doi.org/10.12785/ijcds/110138
19. Roy S, Roy S, Biswas A, Baishnab KL (2021) LCB: light cipher block an ultrafast lightweight block cipher for resource constrained IOT security applications. KSII Trans Internet Inform Syst (TIIS) 15(11):4122–4144
20. Alhija MA, Turab N, Abuthawabeh A, Abuowida H, Al Nabulsi J (2022) DNA cryptographic approaches: state of art, opportunities, and cutting edge perspectives. J Theor Appl Inform Technol 100(18):5346–5358
21. Mohamed KS (2020) New trends in cryptography: quantum, blockchain, lightweight, chaotic, and DNA cryptography. New frontiers in cryptography. Springer International Publishing, pp 65–87
22. Contiki-NG, the OS for Next Generation IoT Devices. (n.d.). Retrieved from https://www.contiki-ng.org/

23. Kharrufa H, Al-Kashoash HA, Kemp AH (2019) RPL-based routing protocols in IoT applications: a review. IEEE Sens J 19(15):5952–5967
24. Lazarevska M, Farahbakhsh R, Shakya NM, Crespi N (2018) Mobility supported energy efficient routing protocol for IoT based healthcare applications, 2018 IEEE Conference on Standards for Communications and Networking (CSCN). pp. 1–5
25. Rana M, Mamun Q, Islam R (2020) Current lightweight cryptography protocols in smart city IoT networks: a survey. arXiv preprint arXiv:2010.00852
26. Taher HM, Al-Rahman SQ, Shawkat SA (2022) Best S-box amongst differently sized S-boxes based on the avalanche effect in the advance encryption standard algorithm. Int J Electr Comput Eng 12(6):2088–8708
27. Heuser A, Picek S, Guilley S, Mentens N (2017) Lightweight ciphers and their side-channel resilience. IEEE Trans Comput 69(10):1434–1448