Research Article

Security Cryptanalysis of NUX for the Internet of Things

Yu Liu ¹, Xiaolei Liu ², and Yanmin Zhao³

¹School of Computer Engineering, Weifang University, Weifang 261061, China

²Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University, Jinan 250100, China

³Department of Computer Science, Faculty of Engineering, The University of Hong Kong, 999077, Hong Kong

Correspondence should be addressed to Yu Liu; yuliu@wfu.edu.cn and Xiaolei Liu; lxlmth@mail.sdu.edu.cn

Received 15 November 2018; Revised 13 May 2019; Accepted 23 May 2019; Published 12 June 2019

Guest Editor: Fagen Li

Copyright © 2019 Yu Liu et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

In order to adopt the restricted environment, such as radio frequency identification technology or sensor networking, which are the important components of the Internet of Things, lightweight block ciphers are designed. NUX is a 31-round iterative ultralightweight cipher proposed by Bansod *et al.* In this paper, we examine the resistance of NUX to differential and linear analysis and search for 1 ~ 31-round differential characteristics and linear approximations. In design specification, authors claimed that 25-round NUX is resistant to differential and linear attack. However, we can successfully perform 29-round differential attack on NUX with the 22-round differential characteristic found in this paper, which is 4 rounds more than the limitation given by authors. Furthermore, we present the key recovery attack on 22-round NUX using a 19-round linear approximation determined in this paper. Besides, distinguishing attack, whose distinguisher is built utilizing the property of differential propagation through NUX, is implemented on full NUX with data complexity 8.

1. Introduction

The Internet of Things is defined as a variety of devices and technologies such as sensors, radio frequency identification (RFID) technology, global positioning systems, infrared sensors, laser scanners, and gas sensors. Its essence is to use RFID technology to realize the automatic identification of items, the interconnection, and sharing of information through the computer Internet. In this kind of new cryptography environment, RFID technology and sensor networking have similar properties, such as weak computation abilities, small storage spaces, and strict power constraints. Therefore, traditional block ciphers are not suitable for this kind of extremely constrained environment. Hence, lightweight block ciphers are put forward for restricted environment and have shown importance in various applications. Recently, copious lightweight block ciphers are designed to maintain security under limited resource conditions, such as PRESENT [1], LBlock [2], and PRINCE [3]. And many cryptographers are concerned about the security of lightweight block ciphers.

Differential analysis, which is a chosen-plaintext attack, is proposed by Biham and Shamir to analyze DES [4]. Differential analysis studies probability propagation property in the encryption/decryption process. This method seeks for high probability differential characteristics to perform a distinguishing attack or a key-recovery attack. Later, linear analysis, which is the duality of differential analysis and is a known-plaintext attack, is presented by Matsui in EURO-CRYPT'93 [5]. Similarly, linear analysis studies the linear relationship between plaintexts and ciphertexts and finds linear approximations with high probability to build a distinguisher or carry out a key-recovery attack. In addition, these two methods are the most popular cryptanalysis methods nowadays. They have been used to analyze many ciphers and should be taken into consideration for designing a new cipher scheme [6–11].

NUX is a 31-round iterative lightweight block cipher proposed by Bansod *et al.* [12] which adopts generalized Feistel structure. And it supports 64-bit blocks and 80/128-bit keys. For the version with 128-bit key, the author pointed out that NUX needs 1022 GE, which is less than all existing ciphers.

TABLE 1: Comparison of tails on NUX.

Method	Rounds	Probability/bias	Reference
Differential	25	2^{-90}	[12]
	25	2^{-71}	Section 3.1
	31	2^{-88}	Section 3.1
Linear	25	2^{-66}	[12]
	25	2^{-41}	Section 4.1
	31	2^{-50}	Section 4.1

TABLE 2: Summary of attacks on NUX.

Attack type	Rounds	Time	Date	Memory (Bytes)	Reference
Differential	25	-	2^{90}	-	[12]
	29	$2^{121.73}$	2^{61}	2^{96}	Section 3.2
Linear	25	-	2^{132}	-	[12]
	25	2^{126}	$2^{63.7}$	2^{70}	Section 4.2
Distinguishing	31	8	8	0	Section 5

In terms of security, they expected that NUX could resist differential/linear analysis. They examined the resistance of NUX against differential/linear cryptanalysis. At last, they showed that NUX cipher with no less than 25 round is enough to resist linear or differential attack. Besides, a biclique attack on NUX is presented in [12].

Our Contribution

- (i) 1~31-round differential characteristics of NUX are searched for, and 10 25-round differential characteristics are found with probability 2^{-71} , which are better than the one with probability limitation 2^{-90} given in the design script, shown in Table 1.
- (ii) The resistance to the linear analysis for 1 ~ 31-round NUX is examined, and 48 25-round linear approximations are presented with absolute value of bias to be 2^{-41} better than the limitation on bias presented in the design script, which is 2^{-66} , depicted in Table 1.
- (iii) For full NUX, the probability of the best differential characteristic is 2^{-88} , and the absolute value of bias for the best linear approximation is 2^{-50} , which are described in Table 1.
- (iv) Using 22-round differential characteristic with probability 2^{-58} obtained in this paper, 29-round differential attack is performed with time, data, and memory complexity to be $2^{121.73}$ 29-round encryptions and 2^{61} and 2^{96} bytes, respectively. Furthermore, based on a 19-round linear approximation with bias to be 2^{-30} , 25-round linear attack is executed with time complexity 2^{126} 25-round encryptions, data complexity $2^{63.7}$, and memory complexity 2^{70} bytes. Till now, these two attacks are the best differential attack and best linear attack, respectively. A summary of our attacks is given in Table 2.

- (v) Utilizing the property of difference propagation through NUX, distinguishing attack can be implemented on full NUX with data complexity 8, which is depicted in Table 2.

The organization of the paper is as follows. The notations and description of NUX are given in Section 2. Section 3 shows the differential characteristics and differential attack on 29-round NUX. In Section 4, the linear approximations and linear attack on 25-round NUX are introduced. Section 5 describes distinguishing attacks between full NUX and random permutations. Finally, Section 6 concludes the paper.

2. Preliminaries

This section will list notations and operations used in this paper and describe NUX.

2.1. Notations and Operations

- (i) $\{0, 1\}^n$: The set of strings with n bits length.
- (ii) $x[i]$: The i -th bit of x , if $x \in \{0, 1\}^n$.
- (iii) $x[i : j]$: The j -th bit to i -th bit of x , if $x \in \{0, 1\}^n$.
- (iv) $x[i, j]$: The i -th and j -th bits of x , if $x \in \{0, 1\}^n$.
- (v) $x \parallel y$: Concatenation of x and y , if $x, y \in \{0, 1\}^n$.
- (vi) $\gg$: Right cyclic shift operation.
- (vii) $\ll$: Left cyclic shift operation.
- (viii) $\oplus$: XOR operation.

2.2. Description of NUX. NUX is a 31-round ultralightweight cipher based on generalized Feistel network. It supports a key length of 128/80 bits and a block length of 64 bits. The round function is illustrated in Figure 1.

There are two F-functions F_1 and F_2 , which are constructed by four 4×4 S-boxes and a circular shift operator.

TABLE 3: S-box used in NUX.

x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
S(x)	e	7	8	4	1	9	2	f	5	a	b	0	6	c	d	3

TABLE 4: Bit permutation table P in NUX.

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
P(i)	15	11	7	3	2	14	10	6	5	1	13	9	8	4	0	12

FIGURE 1: The round function of NUX.

The S-box is represented in Table 3. Then F_1 and F_2 can be depicted as follows:

$$\begin{aligned}
 F_1(x) &= S(x[7:4]) \parallel S(x[3:0]) \parallel S(x[15:12]) \parallel \\
 &\quad S(x[11:8]), \\
 F_2(x) &= S(x[2:0]) \parallel x[15] \parallel S(x[14:11]) \parallel \\
 &\quad S(x[10:7]) \parallel S(x[6:3]).
 \end{aligned} \tag{1}$$

The 64-bit input of the i -th round, X_i , is divided into 4 blocks of 16 bits, named X_i^4 , X_i^3 , X_i^2 , and X_i^1 , respectively.

$$X_i = X_i^4 \parallel X_i^3 \parallel X_i^2 \parallel X_i^1, \tag{2}$$

and then there are the following formulas:

$$\begin{aligned}
 X_{i+1}^4 &= P(X_i^2), \\
 X_{i+1}^3 &= P((X_i^1 \ggg 3) \oplus F_1(X_i^2) \oplus rk_i'), \\
 X_{i+1}^2 &= P((X_i^4 \lll 8) \oplus F_2(X_i^3) \oplus rk_i), \\
 X_{i+1}^1 &= P(X_i^3),
 \end{aligned} \tag{3}$$

where P is a 16-bit permutation, which is depicted in Table 4.

After 31 rounds, the ciphertext will be acquired as $X_{31}^4 \parallel X_{31}^3 \parallel X_{31}^2 \parallel X_{31}^1$. The key schedule is omitted and interested readers are referred to [12] for more details about NUX.

3. Differential Attack on 29-Round NUX

In this section, how to search for differential characteristics of NUX will be described. And then a key-recovery attack is conducted on 29-round NUX.

3.1. Differential Characteristics of NUX. To search for the differential characteristic of NUX, the different propagation between round functions should be considered. And how differences propagate through S-boxes should also be taken into account. When a difference passes through an S-box, the output difference and probability are determined by looking up the XOR difference distribution table (DDT) of the S-box.

Algorithm 1 is designed to search for differential characteristics of NUX, and notations used in this algorithm are depicted in Figure 2. From the structure of NUX, it is obvious that the probability of one round can be 1; that is, all the 8 S-boxes are passive. So a special $n - 1$ -round differential characteristic, $(\Delta_0^3 = \Delta_0^2 = 0)$, is chosen, and one-round differential characteristic with probability 1 is added to catch n -round differential characteristics. Meanwhile, Δ_i^4 and Δ_i^3 , which lie in the two branches on the left side, will not affect Δ_i^2 and Δ_i^1 , the two branches on the right side, during propagation in NUX. So differences of two branches on the left or right are set to 0, and the difference propagation in the other two branches will be focused on during the encryption process. In this way, the number of active S-boxes is always no

FIGURE 2: Differential representation of NUX.

Input: S-box S , Probability threshold $PrLim[30]$.
Output: A differential trail with the best probability.

- (1) Generate the DDT of S-box.
- (2) Store all 2, 4 and the corresponding input/output differences in DDT in the table DDT_p
- (3) **for** Each of 8 S-boxes in the first round **do**
- (4) **for** all non-zero entities in DDT **do**
- (5) **if** S-box is in F_2 **then**
- (6) $\Delta_1^3 = \Delta X_1^h \lll 3, \Delta_1^4 = \Delta_1^2 = \Delta_1^1 = 0$.
- (7) Store them in $R_{in}[1]$.
- (8) **else**
- (9) $\Delta_1^2 = \Delta X_1^l \ggg 8, \Delta_1^4 = \Delta_1^3 = \Delta_1^1 = 0$.
- (10) Store them in $R_{in}[1]$.
- (11) Calculate $\Delta_0^4, \Delta_0^3, \Delta_0^2, \Delta_0^1$, and store them in $R_{in}[0]$.
- (12) Calculate $\Delta_2^4, \Delta_2^3, \Delta_2^2, \Delta_2^1$, and store them in $R_{in}[2]$.
- (13) The probability is recorded as $Pr[1]$.
- (14) **for** $i \leftarrow 2$ to 30 **do**
- (15) **if** $\Delta_i^4 = \Delta_i^3 = 0$ **then**
- (16) $\Delta X_i^l = \Delta_i^2 \lll 8$
- (17) Travel DDT_p to get ΔY_i^l and its corresponding probability $PrRnd$
- (18) **else if** $\Delta_i^2 = \Delta_i^1 = 0$ **then**
- (19) $\Delta X_i^h = \Delta_i^3 \ggg 3$
- (20) Travel DDT_p to get ΔY_i^h and the corresponding probability $PrRnd$
- (21) Keep $Pr[i-1] \times PrRnd$, which greater than threshold $PrLim[i]$
- (22) Calculate $\Delta_{i+1}^4, \Delta_{i+1}^3, \Delta_{i+1}^2, \Delta_{i+1}^1$, and store them in $R_{in}[i+1]$.
- (23) $Pr[i] \leftarrow Pr[i-1] \times PrRnd$
- (24) **for** Each of 8 S-boxes in the first round **do**
- (25) **for** all non-zero entities in DDT **do**
- (26) Find the largest $Pr[i]$ and store it in $PrMax[i]$
- (27) Output different characteristics with probability $PrMax[i]$

ALGORITHM 1: Algorithm for differential characteristic on NUX.

more than 4 in one round, which can make the probability of the differential characteristic as large as possible. The results of our search algorithm are listed in Table 5.

Furthermore, the minimal numbers of active S-boxes of 1~5-round differential characteristics are shown in the design manuscript [12]. So the minimal number of active S-boxes is also studied, and the minimum active S-boxes of 4 5-round

differential characteristics are less than the ones given in [12], which are presented in Table 6.

3.2. Differential Attack on NUX. A 22-round differential characteristic is chosen with probability to be 2^{-58} , which is shown in Table 7, and 7 rounds are extended forward. The description is given in Figure 3. There are $\Delta_0^4 = 0x0400$,

TABLE 5: Differential characteristics of NUX.

Rounds	Probability	Number of tails
2	2^{-2}	192
3	2^{-4}	56
4	2^{-6}	4
5	2^{-7}	1
6	2^{-9}	2
7	2^{-11}	2
8	2^{-15}	8
9	2^{-15}	1
10	2^{-20}	16
11	2^{-24}	24
12	2^{-28}	4
13	2^{-31}	8
14	2^{-37}	4
15	2^{-41}	18
16	2^{-45}	2
17	2^{-46}	1
18	2^{-49}	4
19	2^{-52}	4
20	2^{-53}	2
21	2^{-58}	48
22	2^{-58}	2
23	2^{-63}	32
24	2^{-67}	49
25	2^{-71}	10
26	2^{-73}	4
27	2^{-75}	4
28	2^{-79}	16
29	2^{-79}	2
30	2^{-84}	32
31	2^{-88}	48

TABLE 6: Minimal number of active S-boxes from differential characteristic.

Reference	Number of active S-boxes				
	Rounds				
	1	2	3	4	5
[12]	0	1	2	5	9
Section 3.1	0	1	2	3	3

$\Delta_{22}^3 = 0x2080$, and $\Delta_0^3 = \Delta_0^2 = \Delta_0^1 = \Delta_{22}^4 = \Delta_{22}^2 = \Delta_{22}^1 = 0x0000$ according to the 22-round differential distinguisher. Then $\Delta_{23}^4 = \Delta_{23}^3 = 0x0000$, $\Delta_{23}^1 = 0x0050$, and Δ_{23}^2 satisfy the form as $(00 * * * 00 * * * 000 * * 0)$, where $*$ $\in \{0, 1\}$ can be deduced. And the output difference of the 28-th round is $\Delta_{29}^4 = \Delta_{29}^3 = 0x0000$. X_{23}^2 , $X_{23}^{2'}$, X_{23}^1 , and $X_{23}^{1'}$ can be gotten by 6-round decryption. So rk'_{23} , rk'_{24} , rk'_{25} , rk'_{26} , rk'_{27} , and rk'_{28} should be guessed and denoted by K_{guess} . The attack process is described as follows:

- (1) Collect N pairs of plaintext (P, P') satisfying $P \oplus P' = (\Delta_0^4, \Delta_0^3, \Delta_0^2, \Delta_0^1)$ and their corresponding ciphertext pairs (C, C') .
- (2) Initialize 2^{32} counters $\mathcal{V}[0], \mathcal{V}[1], \dots, \mathcal{V}[2^{32} - 1]$ and reset them.
- (3) For each plaintext pair (P, P') , check whether its ciphertext pair (C, C') satisfies $(C \oplus C')[63 : 32] = 0x00000000$. If the ciphertext pair meets the formula, $x = (C \oplus C')[31 : 0]$ and $\mathcal{V}[x]++$.
- (4) Initialize 2^{96} counters $\mathcal{V}_k[0], \mathcal{V}_k[1], \dots, \mathcal{V}_k[2^{96} - 1]$ and reset them.
- (5) Guess 96-bit key K_{guess} , and decrypt x to obtain X_{23}^2 , $X_{23}^{2'}$, X_{23}^1 , and $X_{23}^{1'}$. Check whether $X_{23}^2 \oplus X_{23}^{2'}$ and $X_{23}^1 \oplus X_{23}^{1'}$ are equal to Δ_{23}^2 and Δ_{23}^1 . If the conditions are met, then let $y = X_{23}^2 \parallel X_{23}^{2'} \parallel X_{23}^1 \parallel X_{23}^{1'}$.
- (6) Use y to calculate $X_{22}^4 \oplus X_{22}^{4'}$ and $X_{22}^3 \oplus X_{22}^{3'}$. If $X_{22}^4 \oplus X_{22}^{4'} = \Delta_{22}^4$ and $X_{22}^3 \oplus X_{22}^{3'} = \Delta_{22}^3$, $\mathcal{V}_k[K_{guess}]++$.
- (7) Set advantage a to be 51, which implies that the top 2^{45} absolute values in $\mathcal{V}_k$ are kept. For each remaining key, we guess the remaining 58-bit subkey and calculate the master key. Finally, we test the key by trail encryptions.

If set $N = 2^{60}$, then about 2^{28} pieces of data enter step (5), which means 2^{124} 6-round encryptions, that is, $2^{121.7}$ 29-round encryptions. The complexity of step (7) is 2^{103} 29-round encryptions. So the total time complexity of this attack is about $2^{121.73}$ 29-round encryptions.

The counters $\mathcal{V}_k$ require storing 2^{96} bytes, so the memory complexity for the attack is 2^{96} bytes. The data complexity is 2^{61} .

The success rate $P_s = \Phi((\sqrt{pNS_N} - \Phi^{-1}(1 - 2^{-a}))/\sqrt{S_N + 1}) = 98.71$ by [13].

4. Linear Attack on 25-Round NUX

Linear approximations of NUX are searched for in this section, and the 25-round key-recovery attack is performed on NUX using a 19-round linear approximation.

4.1. Linear Approximations of NUX. To search for linear approximations of NUX, how masks propagate through S-boxes should be taken into account. When a mask passes through an S-box, the linear approximation table (LAT) of the S-box is looked up to determine the output mask and bias. Algorithm 2 searches for linear approximations of NUX and notations used in this algorithm are depicted in Figure 4.

The bias of one round can be $1/2$, which can be obtained from the structure of NUX; that is, all the 8 S-boxes are passive. So special $(n - 1)$ -round linear approximations are chosen, which satisfy $(\Gamma_0^4 = \Gamma_0^1 = 0)$, and one-round linear approximation with bias 1 is added to catch n -round linear approximations. Similar to searching for differential characteristics, there is only one active S-box in the first

TABLE 7: 22-Round differential characteristic of NUX.

Rounds i	Δ_i^4	Δ_i^3	Δ_i^2	Δ_i^1	Probability
0	0400	0000	0000	0000	1
1	0000	0000	0080	0000	2^{-3}
2	0040	0001	0000	0000	2^{-2}
3	0000	0000	0010	8000	2^{-3}
4	0004	1000	0000	0000	2^{-2}
5	0000	0000	0002	0100	2^{-2}
6	0800	6002	0000	0000	2^{-5}
7	0000	0000	003b	0811	2^{-5}
8	c80c	2b30	0000	0000	2^{-7}
9	0000	0000	0480	4236	2^{-5}
10	2040	0600	0000	0000	2^{-3}
11	0000	0000	0005	2002	2^{-2}
12	8080	0003	0000	0000	2^{-2}
13	0000	0000	0040	8800	2^{-2}
14	0400	0030	0000	0000	2^{-2}
15	0000	0000	0008	4004	2^{-3}
16	0008	3000	0000	0000	2^{-2}
17	0000	0000	0000	0110	1
18	0000	4800	0000	0000	2^{-3}
19	0000	0000	0020	0201	2^{-2}
20	4000	0500	0000	0000	2^{-3}
21	0000	0000	0000	2020	1
22	0000	2080	0000	0000	*

round of $n - 1$ rounds. Meanwhile, Γ_i^4 and Γ_i^3 , which lie in the two branches on the left side, will not affect Γ_i^2 and Γ_i^1 , the two branches on the right side, during propagation in NUX. So the linear propagation on the left or right is taken into consideration, and differences of the other two branches are set to 0. In this way, the number of active S-boxes is always no more than 4 in one round, which can make the absolute value of the linear approximation bias as large as possible. The results of the search algorithm are listed in Table 8.

Moreover, the minimal numbers of active S-boxes of 1~5-round linear approximations are shown in the design manuscript [12]. And the minimal number of active S-boxes is also considered, and the minimum active S-boxes of 3~5-round linear approximations are less than the ones given in [12], which are presented in Table 9.

4.2. Linear Attack on NUX. Utilizing obtained linear approximations, a key-recovery attack can be applied to 25-round NUX using a 19-round linear approximation with bias 2^{-30} , which is described in Table 10. The 19-round linear approximation is put from the 4th to the 22th round of NUX, extending 3 rounds both backward and forward. The 25-round key-recovery attack is shown in Figure 5.

According to the linear approximation, there are $\Gamma_3^4 = \Gamma_3^2 = \Gamma_3^1 = \Gamma_{22}^3 = \Gamma_{22}^2 = 0x0000$, $\Gamma_3^3 = 0x1040$, $\Gamma_{22}^2 = 0x044c$,

and $\Gamma_{22}^1 = 0x24af$. Furthermore, the following formula can be gotten:

$$\begin{aligned}
& \Gamma_3^4 \cdot X_3^4 \oplus \Gamma_3^3 \cdot X_3^3 \oplus \Gamma_3^2 \cdot X_3^2 \oplus \Gamma_3^1 \cdot X_3^1 \oplus \Gamma_{22}^4 \cdot X_{22}^4 \oplus \Gamma_{22}^3 \\
& \cdot X_{22}^3 \oplus \Gamma_{22}^2 \cdot X_{22}^2 \oplus \Gamma_{22}^1 \cdot X_{22}^1 = \Gamma_3^3 \cdot X_3^3 \oplus \Gamma_{22}^2 \cdot X_{22}^2 \\
& \oplus \Gamma_{22}^1 \cdot X_{22}^1 = \kappa
\end{aligned} \quad (4)$$

where X_3^3 can be calculated through 3-round encryption by guessing 26-bit subkeys, which are denoted by K_{before} including rk'_0 , $rk_1[15, 13, 10, 8, 7, 5, 2, 0]$, and $rk'_2[15, 7]$. Besides, X_{22}^2 and X_{22}^1 are obtained by 3-round decryption, which involves 40-bit subkeys, namely, $rk'_{22}[15, 14, 13, 10, 7, 4, 2, 0]$, rk_{23} , and rk'_{24} . For the sake of simplicity, $rk'_{22}[15, 14, 13, 10, 7, 4, 2, 0]$ and rk_{23} are denoted by K_{mid} . In the following, the attack process is depicted.

- (1) Collect N plaintext/ciphertext pairs.
- (2) Initialize 2^{66} counters $\mathcal{V}_0[0], \mathcal{V}_0[1], \dots, \mathcal{V}_0[2^{66} - 1]$ and reset them.
- (3) Guess 26-bit key K_{before} .
- (4) For each plaintext/ciphertext pair, calculate $x = X_3^3[12, 6] \parallel C^4 \parallel C^3 \parallel C^2 \parallel C^1$. Then $\mathcal{V}_0[x] + 1$.
- (5) Initialize 2^{34} counters $\mathcal{V}_1[0], \mathcal{V}_1[1], \dots, \mathcal{V}_1[2^{34} - 1]$ and reset them.

FIGURE 3: Differential attack of 29-round NUX.

- (6) Guess 16-bit key rk'_{24} .
- (7) For every x , calculate $y = X_3^3[12, 6] \parallel X_{24}^2 \parallel X_{24}^1$. Then $\mathcal{V}_1[y] += \mathcal{V}_0[x]$.
- (8) Initialize 2^{66} counters $\mathcal{V}_k[0], \mathcal{V}_k[1], \dots, \mathcal{V}_k[2^{66} - 1]$ and reset them.
- (9) Guess 24-bit key K_{mid} .
- (10) For every y , calculate $X_{22}^2[10, 6, 3, 2]$ and $X_{22}^2[13, 10, 7, 5, 3, 2, 1, 0]$. Then compute $z = \Gamma_3^3 \cdot X_3^3 \oplus \Gamma_{22}^2 \cdot X_{22}^2 \oplus \Gamma_{22}^1 \cdot X_{22}^1$. If $z = 0$, then $\mathcal{V}_k[K_{before} \parallel rk'_{24} \parallel K_{mid}] += \mathcal{V}_1[y]$; otherwise, decrease the counter by $\mathcal{V}_1[y]$.

Input: S-box S , Bias threshold $\epsilon Lim[30]$.
Output: A linear approximation with the best bias.
Data: The number of active S-boxes in i rounds $S_{active}[i]$.
 The number of active S-boxes of the i -th round S_{active}^i .

- (1) Generate the LAT of S-box.
- (2) Store all 2, 4 and the corresponding input/output masks in LAT in the table LAT_p .
- (3) **for** Each of 8 S-boxes in the first round **do**
- (4) **for** all non-zero entities in LAT **do**
- (5) **if** S-box is in F_2 **then**
- (6) $\Gamma_1^4 = \Gamma Y_1^h \ggg 8$, $\Gamma_1^3 = \Gamma_1^2 = \Gamma_1^1 = 0$.
- (7) Store them in $R_{in}[1]$.
- (8) **else**
- (9) $\Gamma_1^1 = \Gamma Y_1^l \lll 3$, $\Gamma_1^4 = \Gamma_1^3 = \Gamma_1^2 = 0$.
- (10) Store them in $R_{in}[1]$.
- (11) Calculate $\Gamma_0^4, \Gamma_0^3, \Gamma_0^2, \Gamma_0^1$, and store them in $R_{in}[0]$.
- (12) Calculate $\Gamma_2^4, \Gamma_2^3, \Gamma_2^2, \Gamma_2^1$, and store them in $R_{in}[2]$.
- (13) Update $S_{active}[1]$ to be 1.
- (14) The bias is recorded as $\epsilon[1]$.
- (15) **for** $i \leftarrow 2$ to 30 **do**
- (16) **if** $\Gamma_i^4 = \Gamma_i^3 = 0$ **then**
- (17) $\Gamma Y_i^l = \Gamma_i^1 \ggg 3$
- (18) Travel LAT_p to get $\Gamma X_i^l, S_{active}^i$ and its corresponding bias ϵRnd
- (19) **else if** $\Gamma_i^2 = \Gamma_i^1 = 0$ **then**
- (20) $\Gamma Y_i^h = \Gamma_i^4 \lll 8$
- (21) Travel LAT_p to get $\Gamma X_i^h, S_{active}^i$ and the corresponding bias ϵRnd
- (22) Compute the total bias, and keep ones greater than threshold $\epsilon Lim[i]$
- (23) Calculate $\Gamma_{i+1}^4, \Gamma_{i+1}^3, \Gamma_{i+1}^2, \Gamma_{i+1}^1$, and store them in $R_{in}[i+1]$.
- (24) Update the number of active S-boxes $S_{active}[i]$ and bias $\epsilon[i]$
- (25) **for** Each of 8 S-boxes in the first round **do**
- (26) **for** all non-zero entities in DDT **do**
- (27) Find the largest $\epsilon[i]$ and store it in $\epsilon Max[i]$
- (28) Output linear approximations with bias $\epsilon Max[i]$

ALGORITHM 2: Algorithm for linear approximations on NUX.

FIGURE 4: Linear representation of NUX.

- (11) Set the advantage a to be 17, which means that the top 2^{49} absolute values in $\mathcal{V}_k$ are kept. For each remaining key, we guess 77-bit subkey to determine the master key. And then we test the key by trail encryptions.

If $N = 2^{63.7}$, then the time complexity of step (3), step (5), and step (7) is about $2^{89.7}$ 3-round encryption, 2^{108} 1-round decryption, and 2^{100} 2-round encryption, respectively. Besides, the complexity of step (11) is 2^{126} 25-round

FIGURE 5: Linear attack of 25-round NUX.

encryption. Hence, the total time complexity of this attack is about 2^{126} 25-round encryption.

Both the counters $\mathcal{V}_0$ and $\mathcal{V}_k$ need 2^{69} bytes to store, so the memory complexity for the attack is 2^{70} bytes. The data complexity is $2^{63.7}$.

The success rate $P_S = \Phi(2\sqrt{N} \cdot |\epsilon| - \sqrt{1 + N/2^n} \Phi^{-1}(1 - 2^{-a-1})) = 88.21$ by [14].

5. Distinguishing Attack on NUX

Generally speaking, the distinguishing attack is a kind of test algorithm, which tries to perform the nonrandom behavior

in cryptographic system. A distinguishing attack needs to find a distinguisher, which makes cryptographic algorithm different from random permutation. When analyzing NUX, we find a distinguisher with probability 1, that is, a deterministic distinguisher to distinguish NUX from a random permutation.

In Section 3, it has been pointed out that the two branches on the right side will not affect the two on the left side during difference propagation in NUX. Then, for the full-round NUX, when the input difference $(\Delta_0^4, \Delta_0^3, \Delta_0^2, \Delta_0^1)$ is $(0, 0, *, *)$, the output difference $(\Delta_{31}^4, \Delta_{31}^3, \Delta_{31}^2, \Delta_{31}^1)$ satisfies the form of $(*, *, 0, 0)$, shown in Figure 6, that is,

FIGURE 6: 31-Round differential distinguisher of NUX.

TABLE 8: Linear approximations of NUX.

Rounds	Bias	Number of tails
2	2^{-2}	288
3	2^{-3}	300
4	2^{-4}	13
5	2^{-5}	2
6	2^{-6}	4
7	2^{-10}	13
8	2^{-11}	62
9	2^{-12}	6
10	2^{-15}	70
11	2^{-16}	11
12	2^{-18}	70
13	2^{-19}	4
14	2^{-20}	2
15	2^{-22}	4
16	2^{-24}	16
17	2^{-26}	4
18	2^{-27}	4
19	2^{-30}	16
20	2^{-31}	4
21	2^{-33}	8
22	2^{-35}	60
23	2^{-37}	21
24	2^{-39}	25
25	2^{-41}	48
26	2^{-43}	103
27	2^{-44}	4
28	2^{-46}	7
29	2^{-48}	54
30	2^{-49}	4
31	2^{-50}	2

TABLE 9: Minimal number of active S-boxes from linear approximation.

Reference	Number of active S-boxes				
	Rounds				
	1	2	3	4	5
[12]	0	1	4	9	13
Section 4.1	0	1	2	3	3

$(0, 0, *, *) \xrightarrow[31\text{-round}]{Pr=1} (*, *, 0, 0)$. However, the probability of the output difference to be $(*, *, 0, 0)$ is $Pr_{random} =$

2^{-32} for random permutations, when the input difference is $(0, 0, *, *)$. So 4 pairs of plaintexts are chosen, which are (P_i, P'_i) , $(0 \leq i \leq 3)$, and $P_i \oplus P'_i = (0, 0, *, *)$, and the corresponding ciphertexts (C_i, C'_i) are checked to determine whether they satisfy $C_i \oplus C'_i = (*, *, 0, 0)$. The probability of obtaining such input/output differences is 1 for NUX, while it is 2^{-128} for a random permutation. Therefore, we can distinguish NUX from a random permutation. Besides, there is another distinguisher with probability 1, which is $(*, *, 0, 0) \xrightarrow[31\text{-round}]{Pr=1} (0, 0, *, *)$ and can be used to perform a distinguishing attack like the one described before. So we will not explore it here.

Since only 4 pairs of plaintexts are used in the distinguishing attack, the data complexity is 8. And the attack needs no storage. In other words, the complexity of memory is 0. The time complexity is 8 31-round encryptions.

6. Conclusions

NUX is a 31-round iterative ultralightweight cipher, which is suitable for extremely constrained environment and is applied to the Internet of Things. In this paper, differential and linear trails are searched for 1~31-round NUX, which are better than those proposed in design specification. Moreover, a key-recovery attack on 29-round NUX is given with the 22-round differential characteristic found in the paper, whose time, data, and memory complexities are $2^{121.73}$ 29-round encryptions and 2^{61} and 2^{96} bytes, respectively. Meanwhile, using 22-round differential characteristic obtained in the paper, 29-round differential attack is performed with time, data, and memory complexities to be 2^{126} 25-round encryptions and $2^{63.7}$ and 2^{70} bytes, respectively. Furthermore, a distinguishing attack can be implemented on full NUX with data complexity 8. Results in this paper are the best ones on NUX till now.

Data Availability

All the data are obtained by our programs and can be provided to interested readers by email.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work has been supported by National Cryptography Development Fund (no. MMJJ20170102), the National

TABLE 10: 19-Round linear approximation of NUX.

Rounds i	Γ_i^4	Γ_i^3	Γ_i^2	Γ_i^1	Bias
0	0000	1040	0000	0000	2^{-1}
1	0000	0000	0000	0500	2^{-2}
2	0001	4040	0000	0000	2^{-2}
3	0000	0000	0020	0600	2^{-2}
4	5100	0440	0000	0000	2^{-4}
5	0000	0000	8404	2028	2^{-3}
6	100a	a080	0000	0000	2^{-3}
7	0000	0000	0206	3000	2^{-3}
8	000a	2002	0000	0000	2^{-2}
9	0000	0000	0202	0800	2^{-2}
10	000a	0020	0000	0000	2^{-2}
11	0000	0000	0202	4010	2^{-3}
12	a000	0a00	0000	0000	2^{-2}
13	0000	0000	4040	0200	2^{-2}
14	1400	0400	0000	0000	2^{-3}
15	0000	0000	0084	0448	2^{-3}
16	01c3	8048	0000	0000	2^{-4}
17	0000	0000	9023	0180	2^{-2}
18	d800	4004	0000	0000	2^{-3}
19	0000	0000	044c	24af	*

Natural Science Foundation of China (nos. 61572293, 61502276, and 61692276), the National Natural Science Foundation of Shandong Province, China (ZR2016FM22), Major Scientific and Technological Innovation Projects of Shandong Province, China (2017CXGC0704), and Fundamental Research Fund of Shandong Academy of Sciences (no. 2018:12-16).

References

- [1] A. A. Bogdanov, L. R. Knudsen, G. Leander et al., "An ultra-lightweight block cipher," in *Proceedings of the Cryptographic Hardware and Embedded Systems (CHES 2007)*, P. Paillier and I. Verbauwhede, Eds., vol. 4727 of *Lecture Notes in Computer Science LNCS*, pp. 450–466, Springer, 2007.
- [2] W. Wu and L. Zhang, "LBlock: a lightweight block cipher," in *Proceedings of the 9th International Conference on Applied Cryptography and Network Security (ACNS 2011)*, J. Lopez and G. Tsudik, Eds., vol. 6715 of *Lecture Notes in Computer Science*, pp. 327–344, Springer, Heidelberg, Germany, 2011.
- [3] J. Borghoff, A. Canteaut, T. Güneysu et al., "PRINCE-A low latency block cipher for pervasive computing applications," in *Proceedings of the 25th Annual International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2012)*, X. Wang and K. Sako, Eds., vol. 7658 of *Lecture Notes in Computer Science*, pp. 208–225, Springer, Heidelberg, Germany, 2012.
- [4] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," *Journal of Cryptology*, vol. 4, no. 1, pp. 3–72, 1991.
- [5] M. Matsui, "Linear cryptanalysis method for DES cipher," in *Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques (EUROCRYPT 1993)*, T. Hellese, Ed., vol. 765 of *Lecture Notes in Computer Science*, pp. 386–397, Springer, 1993.
- [6] A. G. Bafghi, R. Safabakhsh, and B. Sadeghiyan, "Finding the differential characteristics of block ciphers with neural networks," *Information Sciences*, vol. 178, no. 15, pp. 3117–3131, 2008.
- [7] H. M. Heys and S. E. Tavares, "Substitution-permutation networks resistant to differential and linear cryptanalysis," *Journal of Cryptology. The Journal of the International Association for Cryptologic Research*, vol. 9, no. 1, pp. 1–19, 1996.
- [8] G. Jakimoski and L. Kocarev, "Differential and linear probabilities of a block-encryption cipher," *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 50, no. 1, pp. 121–123, 2003.
- [9] J. Kim and R. C.-W. Phan, "Advanced differential-style cryptanalysis of the NSA's Skipjack block Cipher," *Cryptologia*, vol. 33, no. 3, pp. 246–270, 2009.
- [10] F. Sano, K. Ohkuma, H. Shimizu, and S. Kawamura, "On the security of nested SPN cipher against the differential and linear cryptanalysis," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 86, no. 1, pp. 37–46, 2003.
- [11] B.-Z. Su, W.-L. Wu, and W.-T. Zhang, "Security of the SMS4 block cipher against differential cryptanalysis," *Journal of Computer Science and Technology*, vol. 26, no. 1, pp. 130–138, 2011.
- [12] G. Bansod, S. Sutar, A. Patil, and J. Patil, "NUX: a lightweight block cipher for security at wireless sensor node level. World academy of science, engineering and technology," *International Journal of Bioengineering and Life Sciences*, vol. 5, no. 1, 2018.
- [13] A. A. Selçuk, "On probability of success in linear and differential cryptanalysis," *Journal of Cryptology. The Journal of the International Association for Cryptologic Research*, vol. 21, no. 1, pp. 131–147, 2008.

- [14] A. Bogdanov and E. Tischhauser, “On the wrong key randomisation and key equivalence hypotheses in Matsui’s algorithm 2,” in *Proceedings of the International Workshop on Fast Software Encryption (FSE 2013)*, S. Moriai, Ed., vol. 8424 of *Lecture Notes in Computer Science*, pp. 19–38, Springer, 2014.