Copyright ⓒ 2022 KSII

Research on the Security Level of μ^2 against Impossible Differential cryptanalysis

Kai Zhang[1,2*], Xuejia Lai[1], Jie Guan[2], Bin Hu[2]
[1]Shanghai Jiao Tong University, Shanghai 200240, China
[2]PLA SSF Information Engineering University, Zhengzhou 450000, China
[e-mail: zhkai2010@139.com, lai-xj@cs.sjtu.edu.cn, guanjie007@163.com, hb2110@126.com]
*Corresponding author: Kai Zhang

Received February 25, 2021; revised January 6, 2022; accepted February 3, 2022; published March 31, 2022

Abstract

In the year 2020, a new lightweight block cipher μ^2 is proposed. It has both good software and hardware performance, and it is especially suitable for constrained resource environment. However, the security evaluation on μ^2 against impossible differential cryptanalysis seems missing from the specification. To fill this gap, an impossible differential cryptanalysis on μ^2 is proposed. In this paper, firstly, some cryptographic properties on μ^2 are proposed. Then several longest 7-round impossible differential distinguishers are constructed. Finally, an impossible differential cryptanalysis on μ^2 reduced to 10 rounds is proposed based on the constructed distinguishers. The time complexity for the attack is about $2^{69.63}$ 10-round μ^2 encryptions, the data complexity is $O(2^{48})$, and the memory complexity is $2^{63.57}$ Bytes. The reported result indicates that μ^2 reduced to 10 rounds can't resist against impossible differential cryptanalysis.

Keywords: Cryptanalysis, Lightweight Block Cipher, μ^2 Block Cipher, Impossible Differential cryptanalysis

This work was partially supported by the National Natural Science Foundation of China under Grant No. 61802437, 61902428, 62102448 and China Postdoctoral Science Foundation under Grant No. 2020M681314.

http://doi.org/10.3837/tiis.2022.03.012 **ISSN : 1976-7277**

1. Introduction

With the rapid development of micro devices in IoT(Internet of Things), RFID(Radio Frequency Identification), and smart card, there is a great demand for lightweight block ciphers in both scenarios of IoT[1,2] and RFID[3,4]. These lightweight block ciphers can protect the sensitive information in the devices with constrained computing capability. For lightweight block ciphers, there are many advantages such as simple structure, efficiency in both software and hardware platforms. And the design for this kind of block ciphers has been a focus for recent several years. Many good lightweight block ciphers are presented such as LBlock[5], PRESENT[6], GIFT[7], Midori[8], SIMON and SPECK[9] etc. In the year 2019, NIST proposed a standardization project LWC (LightWeight Cryptography) to enhance the development for lightweight ciphers. The lightweight block cipher $\mu 2$[10] is proposed in the year 2020. It has both good software and hardware performance, and it is especially suitable for constrained resource environment.

After the proposal of a new block cipher, various cryptanalytic methods should be considered to evaluate the security level thoroughly, such as differential cryptanalysis[11], linear cryptanalysis[12], integral cryptanalysis[13], impossible differential cryptanalysis[14,15], zero correlation linear cryptanalysis[16]. Due to the enormous workload, some cipher designers may miss some of the cryptanalytic methods, or estimate the security level roughly which needs cryptographers to fill the gap with more refined research.

Impossible differential cryptanalysis was independently put forward by Knudsen[14] and Biham[15]. So far, it is one of the most effective cryptanalytic techniques. The basic idea of impossible differential cryptanalysis is establishing an impossible differential distinguisher, then filter the wrong key candidates with this distinguisher until the correct key is recovered. The method of impossible differential cryptanalysis has been successfully applied to many block ciphers [17-21].

Contributions

In this paper, the main target is to evaluate the security level on μ^2 against impossible differential cryptanalysis.

- Firstly, according to the structure of μ^2, the diffusion property for the key schedule and some cryptographic properties for the round function are illustrated.
- Secondly, with "miss-in-the-middle" technique and an automatic approach, several longest impossible differential distinguishers are established.
- Finally, on the basis of "early-abort" technique and constructed impossible differential distinguishers, a concrete key recovery impossible differential cryptanalysis on μ^2 reduced to 10 rounds is proposed.

The organization for this paper is as follows. The notations used in this paper and a brief introduction on μ^2 are illustrated in section 2. Section 3 proposes some properties on μ^2 which will be used in later cryptanalysis. Some longest impossible differential distinguishers are explored in section 4. A key recovery attack on μ^2 is proposed in section 5 and section 6 concludes the paper.

2. Preliminary

2.1 Notations

- P : represents a 64-bit plaintext;
- C : represents a 64-bit ciphertext;
- X^i : intermediate value before the *i*-th round, which is consist of four 16-bit words $X^i = (X_3^i, X_2^i, X_1^i, X_0^i)$;
- K : master key;
- key^i : 80-bit key register at the *i*-th round;
- rk^i : round key for the *i*-th round, for each round key, rk^i can be seperated into four 16-bit parts, i.e. $(rk_3^i, rk_2^i, rk_1^i, rk_0^i)$;
- $x\|z$: represents the relationship of concatenation for vectors x and z.

2.2 Brief Description on μ^2

The block size for lightweight block cipher μ^2 is 64 bits, the key length is 80 bits and the cipher has 15 rounds.

Round Function

The structure of μ^2 is a Type-II GFS (GFS is short for generalized Feistel Structure, see **Fig. 1**, The F function in the GFS takes a 4-round SPN (SPN is short for substitution permutation network) structure which is illustrated in **Fig. 2**. Sbox is presented in **Table 1** and π bitwise permutation is defined as:

$$\pi[b_{15}b_{14}\cdots b_1b_0] = [b_3b_6b_9b_{12}b_7b_{10}\, b_{13}b_0b_{11}b_{14}b_1b_4b_{15}b_2b_5b_8].$$

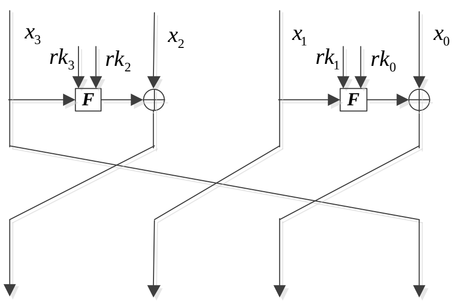

Fig. 1. Structure of μ^2

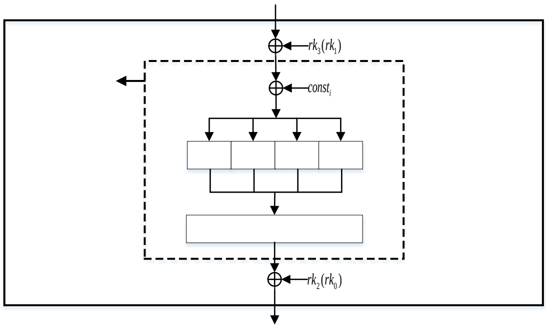

Fig. 2. Structure of F function

In **Fig. 2**, variable $const_i$ is a constant which is related to round of the SPN structure, round and position of the F function. Round keys in the bracket are for the right F function.

Table 1. Sbox for μ^2

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S(x)$	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2

Key Schedule

The key schedule of μ^2 is modified from a famous block cipher PRESENT, which can be summarized as below.

Firstly, the 80-bit register is initialized with the master key. Secondly, the key register is rotated by 61 bits on the left. Thirdly, substitute the 64th to 67th bits of the key register with the Sbox. Fourthly, XOR the 15th to the 18th bits with a four-bit round counter. Finally, the 64 most significant bits of the key register are extracted as the round key RK, which is segmented into 4 sub-round keys (rk_3, rk_2, rk_1, rk_0,

The mathematical form of this key register updating progress can be illustrated as below.

$$(1)\ [k_{79},k_{78},\cdots k_1,k_0] = [k_{18},k_{17},\cdots k_{20},k_{19}]$$
$$(2)\ [k_{79},k_{78},k_{77},k_{76}] = S[k_{79},k_{78},k_{77},k_{76}]$$
$$(3)\ [k_{67},k_{66},k_{65},k_{64}] = S[k_{67},k_{66},k_{65},k_{64}]$$
$$(4)\ [k_{18},k_{17},k_{16},k_{15}] = [k_{18},k_{17},k_{16},k_{15}] \oplus \text{round counter}$$

3. Cryptographic Properties for μ^2

Property 1: The key schedule of μ^2 has limited diffusion property. Specifically speaking, at the 12th round, there are still four bits of the key register key^{12} which are only affected by one bit of the master key (18,17,16,15 bits of key^{12} and 67,66,65,64 bits of master key K have one-to-one correspondence, At the 10th round, 12 bits of the key register key^{10} are only affected by one bit of the master key. Even for the last round, half of the key register (40 bits) are only affected by four bits of the master key.

The number of master key bits which affect 10th, 12th and last round's key register are illustrated in **Table 2** below. This property is critical for the phase of key recovery and it is the foundation to recover the master key bits rather than round key bits.

Table 2. Number of master key bits which affect the 15th, 12th and 10th round key register bits

<table>
<tr><td>Bit position of key¹⁵</td><td>7-10, 26-29, 45-52, 64-71</td><td colspan="2">11-14,30-33,53-56,72-75</td><td colspan="2">0-6,15-25,34-44, 57-63,76-79</td></tr>
<tr><td>Number of master key bits correlated</td><td>8</td><td colspan="2">7</td><td colspan="2">4</td></tr>
<tr><td>Bit position of key¹²</td><td>45-48, 64-67</td><td>7-10, 72-78, 49-52, 68-71</td><td colspan="2">0-6, 11-14, 19-25, 30-44,53-63,72-79</td><td>15-18</td></tr>
<tr><td>Number of master key bits correlated</td><td>8</td><td>7</td><td colspan="2">4</td><td>1</td></tr>
<tr><td>Bit position of key¹⁰</td><td>7-10, 26-29, 45-48, 64-67</td><td colspan="2">0-6, 11-14, 19-25, 30-33, 38-44, 49-52, 57-63, 68-79</td><td colspan="2">15-18, 34-37, 53-56</td></tr>
<tr><td>Number of master key bits correlated</td><td>7</td><td colspan="2">4</td><td colspan="2">1</td></tr>
</table>

Property 2: For any nonzero input difference of the Sbox, there exist 6.4 possible output differences on average.

Through analyzing the Sbox, it can be shown that the number of possible output differences for any nonzero input difference ranges from four to eight. And the mathematical expectation for this value is 6.4. If input difference zero is also taken into consideration, this mathematical expectation value is reduced to 6.

Property 3: For any nonzero input difference of one SPN round of the F function, there exist 1351 possible output differences on average.

For any nonzero input difference for one SPN round, they can be classified into four circumstances, i.e. one active Sbox to four active Sboxes. So in this circumstance, the number of output differences N can be calculated into the following formula:

$$N = \frac{C_4^1\cdot(2^4-1)\cdot 6.4 + C_4^2\cdot(2^4-1)^2\cdot 6.4^2 + C_4^3\cdot(2^4-1)^3\cdot 6.4^3 + C_4^4\cdot(2^4-1)^4\cdot 6.4^4}{2^{16}} = 88529280/65536 \approx 1351$$

To validate the correctness of Property 3, a simulation process is conducted. For each input difference, the number of output difference for one SPN round of the F function ranges from 4 to 4096, which is averaged to 1351. This result coincides with the theoretical analysis.

Property 4: For any nonzero input to output difference of the F function, the highest probability is 38/65536, and for each input difference, there exist 25779 possible output differences on average.

The difference distribution table (DDT) for the Sbox and F function is calculated. After analyzing the DDT of the F function, it is found that the highest differential probability is 38/65536. **Table 3** shows four highest probability differential characters in the DDT of the F function. After analyzing the difference distribution table of F function, it can be found that for each input difference, the number of output difference for the F function ranges from

23794 to 26023, which is averaged to 25779.

Table 3. Four highest probability differential character for the F function

Input Difference	Output Difference	Differential Probability
0x 0fd0	0x 2505	38/65536
0x dd00	0x 1850	34/65536
0x 007d	0x 5058	32/65536
0x 0f70	0x 0185	32/65536

4. Impossible Differential Distinguishers for μ^2

Using "miss-in-the-middle" technique, with an automatic approach, the possibility of constructing impossible differential distinguishers on μ^2 block cipher is investigated. All the possibilities for the modes of input and output differences are exhaustively searched, two 7-round and ten 6-round impossible differential distinguishers are found. **Table 4** illustrates these concrete distinguishers.

Here, the first 7-round impossible differential distinguisher $(0, a, 0, 0) \nrightarrow (0, 0, h, 0)$ is taken as an example to illustrate the constructing process for the distinguisher. The detail of the structure for the distinguisher can be explained in **Fig. 3** below.

Table 4. Some longest Impossible Differential Distinguishers for μ^2

Length	Impossible Differential Distinguishers
7-round	$(0, a, 0, 0) \nrightarrow (0, 0, h, 0)$
	$(0, 0, 0, a) \nrightarrow (h, 0, 0, 0)$
6-round	$(0, 0, 0, a) \nrightarrow (0, 0, h, 0)$
	$(0, 0, 0, a) \nrightarrow (0, h, 0, 0)$
	$(0, 0, 0, a) \nrightarrow (0, h, y, 0)$
	$(0, 0, a, 0) \nrightarrow (h, 0, 0, 0)$
	$(0, 0, a, b) \nrightarrow (h, 0, 0, 0)$
	$(0, a, 0, 0) \nrightarrow (0, 0, 0, h)$
	$(0, a, 0, 0) \nrightarrow (h, 0, 0, 0)$
	$(0, a, 0, 0) \nrightarrow (h, 0, 0, y)$
	$(a, 0, 0, 0) \nrightarrow (0, 0, h, 0)$
	$(a, b, 0, 0) \nrightarrow (0, 0, h, 0)$

In **Fig. 3**, "a, b, c, h, y, z" represent 16-bit nonzero differences and "?" represents the difference for the word is unknown, the word marked in red implies a contradiction.

5. Impossible Differential Cryptanalysis on μ^2

Based on the 7-round impossible differential constructed in section 4, a key recovery attack on μ^2 reduced to 10 rounds is proposed with adding two rounds before and one round after the distinguisher (See **Fig. 4**, The key recovery attack is mainly composed of two stages: data collection stage and key recovery stage.

Data Collection Stage:

On one hand, construct 2^m data sets. For each set, word X_1^0 of the plaintext P = $(X_3^0, X_2^0, X_1^0, X_0^0)$ are fixed to the same value and other words are arbitrary. So there are 48 bits (i.e. X_3^0, X_2^0, X_0^0) can be any distinctive values and 16 bits (i.e. X_1^0) are fixed to a constant for a data set. That is to say, for each data set, there can be about 2^{95} plaintext pairs ($C_{2^{48}}^2 \approx 2^{95}$, It is noted that when choosing a plaintext pair, ΔX_3^0, ΔX_2^0, ΔX_0^0 should be nonzero difference. So for each data set, there are about $[2^{16}*(2^{16}-1)/2]^3 \approx 2^{93}$ pairs satisfying the constraint of the input. On the other hand, suppose the difference of the output for the 10th round is ΔC = $(\Delta X_3^{10}, \Delta X_2^{10}, \Delta X_1^{10}, \Delta X_0^{10})$, ΔX_3^{10}, ΔX_0^{10} should be zero difference and ΔX_2^{10}, ΔX_1^{10} should be nonzero difference. So after sieving the difference of the ciphertexts, there are totally 2^{m+61} $(2^{m+93} \cdot 2^{-32})$ plaintext-cipher pairs left.

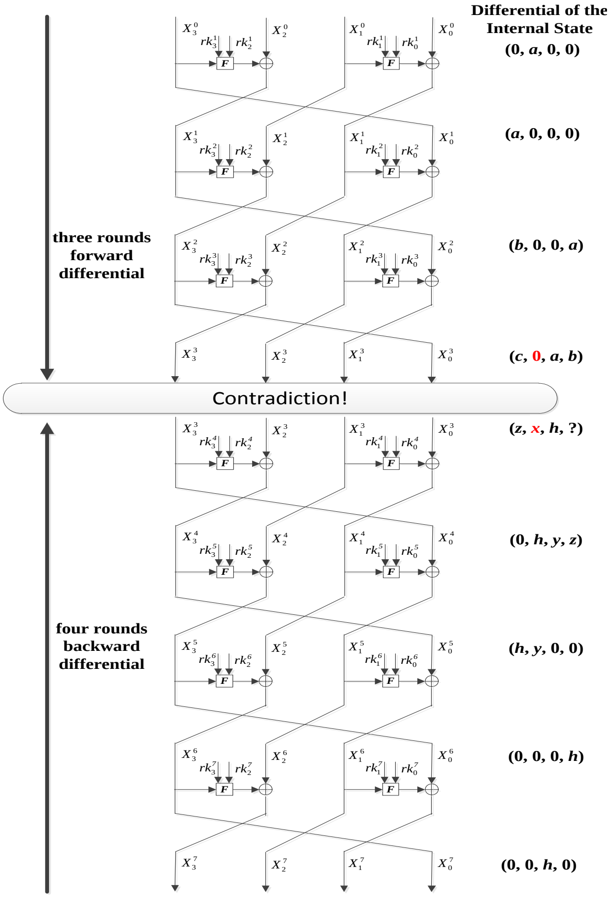

Fig. 3. Construction of the 7-round Impossible Differential for μ^2

During the research, it is found that if $\Delta X_0^0 \to \Delta X_3^0$, $\Delta X_3^0 \to \Delta X_2^0$ and $\Delta X_1^{10} \to \Delta X_0^{10}$ be three possible input difference to output differences for F function, the efficiency of sieving the wrong subkeys can be improved. This probability for the F function can be derived through Property 4, i.e. 25779/65536 ≈ 39.3% ≈ $2^{-1.35}$. Through this further sieving, there are $2^{m+56.95}$ ($2^{m+61} \cdot 2^{-1.35*3}$) plaintext-cipher pairs left.

Key Recovery Stage:

In the key recovery stage, "early-abort technique" is utilized to reduce the complexity, i.e. guessing the subkey bits in its smallest unit.

The details of the attack for the key recovery phase are illustrated as following three steps.

Step 1. For each plaintext-ciphertext pair after data collection stage, guess the 16 bits for the first round key rk_3^1. If $\Delta F(\Delta X_3^0, rk_3^1, rk_2^1) = \Delta X_2^0$, save the rk_3^1. The round key rk_2^1 needn't to be guessed because it doesn't affect the difference. According to the key schedule, these 16 bits have one-to-one correspondence with 79 to 64 bits of the master key which is illustrated in **Table 5** below. For the F function, each nonzero input difference can lead to 25779 output difference on average, so after this step, there are $2^{m+42.3}$ plaintext-ciphertext pairs left.

In this step, rk_3^1 is split into four segments at first. However, as the F function is a 4-round SPN structure which makes the confusion and diffusion of the input difference quite well, it is hard to split rk_3^1 and guess it step by step.

Table 5. Correspondence between rk_3^1 and master key bits

Number of rk_3^1 bit	15	14	13	12	11	10	9	8
Relevant master key bit	79	78	77	76	75	74	73	72
Number of rk_3^1 bit	7	6	5	4	3	2	1	0
Relevant master key bit	71	70	69	68	67	66	65	64

Step 2. After step 1, guess the 16 bits for the 10th round key rk_1^{10}. If $\Delta F(\Delta X_2^{10}, rk_1^{10}, rk_0^{10}) = \Delta X_1^{10}$, save the rk_1^{10}. Similarly, the round key rk_0^{10} needn't to be guessed. According to the key schedule, the 16 bits of rk_1^{10} corresponds with 41 to 59 bits of the master key bits, the detailed correspondence is illustrated in **Table 6** below. Accordingly, 19 master key bits: K[59-41] should be guessed to derive rk_1^{10}[15-0]. Also, for the F function, each nonzero input difference can lead to 25779 output difference on average, so after this step, there are $2^{m+27.65}$ plaintext-ciphertext pairs left.

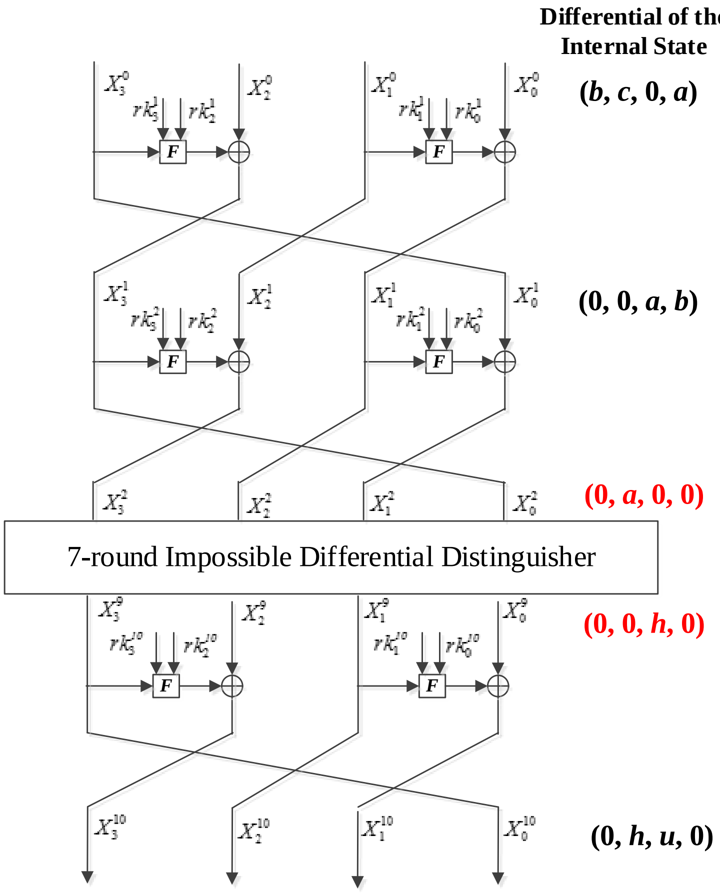

Fig. 4. Key Recovery Attack for μ^2

In **Fig. 4**, "*a*, *b*, *c*, *h*, *u*" represent 16-bit nonzero difference, the state marked in red represents an impossible differential distinguisher.

The concrete relationship between the round key bits of rk_1^{10} and master key bits are as follows:

(1) rk_1^{10}[9-6]= S (K [52-49] ⊕ 0111)

(2) rk_1^{10}[5-2]= K [48-45]

(3) rk_1^{10}[1,0]= S (K [44-41]) (two most significant bits)

(4) rk_1^{10}[12,11,10]= S (K [56-53] ⊕ 0011) (three least significant bits)

(5) rk_1^{10}[15,14,13]= S (S (K [56-53] ⊕ 0011) (most significant bit) || K [59-57]) (three least significant bits)

Table 6. Correspondence between rk_1^{10} and master key bits

Number of rk_1^{10} bit	15	14	13	12	11	10	9	8
Relevant master key bits	53 54 55 56 57 58 59	53 54 55 56 57 58 59	53 54 55 56 57 58 59	53 54 55 56	53 54 55 56	53 54 55 56	49 50 51 52	49 50 51 52
Number of rk_1^{10} bit	7	6	5	4	3	2	1	0
Relevant master key bits	49 50 51 52	49 50 51 52	48	47	46	45	41 42 43 44	41 42 43 44

Step 3. After step 2, at most 48 round key bits, i.e. rk_1^1, rk_0^1 and rk_1^2 need to be guessed to derive the difference at the boundary of the impossible differential distinguisher. For rk_1^1, extra 9 bits of the master key *K*[40-32] should be guessed. As $rk_0^1 \oplus rk_1^2$ can be regarded as a whole, so 16 bits (*K*[31-29], *K*[28]⊕*K*[63], *K*[27]⊕*K*[62], *K*[26]⊕*K*[61], *K*[25]⊕*K*[60], *K*[24-16]) should be guessed to derive $rk_0^1 \oplus rk_1^2$. If the output difference for the right *F* function of the second round equals to ΔX_0^1, i.e. $\Delta F(\Delta X_1^1, rk_1^2, rk_0^2) = \Delta X_0^1$, the output difference for the right branch of the second round equals to zero after Xoring ΔX_0^1, and the probability for this process is 1/25779. Iterate Step 1 to Step 3 until only one correct key is left.

After the steps above, through partial encryption (two rounds) and partial decryption (one round), if all the guessed key bits are correct, the 7-round impossible differential distinguisher in the middle will never occur. If the guessed key bits are incorrect, the impossible differential distinguisher will emerge with a fixed probability. This is the rule to judge the incorrect key from right one.

Following is the detailed relationship between the involved round key bits and master key bits in Step 3.

As $rk_1^1[15-0] = K[47-32]$, according to Step 2, seven bits (i.e. *K*[47-41]) have already been guessed, so only nine master key bits (i.e. *K*[40-32]) should be guessed here. Then as $rk_0^1[15-0] \oplus rk_1^2[15-0] = K[31-16] \oplus K[66-51]$, twelve involved master key bits (*K*[59-51] and *K*[66-64]) have already been guessed, so extra 16 bits information of the master key is needed.

Complexities of the Attack: There are altogether 60 bits information of the key which should be guessed during the attack.

Next, the number of data sets needed for the attack is illustrated. After sieving all the plaintext-ciphertext pairs for 2^m data sets, there are about $(2^{60}-1)\cdot(1-\frac{1}{25779})^{2^{m+27.65}}$ wrong key candidates left. If m=0, as $(2^{60}-1)\cdot\left(1-\frac{1}{25779}\right)^{2^{27.65}} \approx 0$, that is to say, almost all the wrong key candidates can be eliminated with only one data set for the attack.

- Time complexity: about $2^{69.63}$ 10-round encryption (the detail is illustrated in **Table 7** below,
- Data complexity: 2^{48} plaintext-ciphertext pairs.
- Memory complexity: about $2^{56.95}\cdot 4\cdot 8 + 2^{60}\cdot 8$ Bytes $\approx 2^{63.57}$ Bytes, which mainly depends on stored plaintext-ciphertext pairs and key candidates.

Table 7. Details of the time complexity for each step

Step	Number of master key bits guessed	Round key bits guessed	Corresponding master key bits guessed	Complexity (unit: 1-round encryption)
Step 1	16	rk_3^1	K[79-64]	$2^{m+56.95}\cdot 2^{16} \approx 2^{m+72.95}$
Step 2	19	rk_1^{10}	K[59-41]	$2^{m+42.3}\cdot 2^{19} \approx 2^{m+61.3}$
Step 3	25	$rk_1^1, rk_0^1 \oplus rk_1^2$	K[40-29], K[24-16], K[28]⊕K[63], K[27]⊕K[62], K[26]⊕K[61], K[25]⊕K[60]	$2^{m+27.65}\cdot 2^{25} \approx 2^{m+52.65}$
Total Complexity			$\approx 2^{m+69.63}$ 10-round encryption	

6. Conclusion

μ^2 is a newly proposed lightweight block cipher in 2020. However, the security evaluation for μ^2 against impossible differential cryptanalysis seems missing from the specification. To fill this gap, an impossible differential cryptanalysis on μ^2 is proposed. Firstly, some cryptographic properties on μ^2 are proposed. Secondly, with an automatic approach, several longest impossible differential distinguishers are proposed. Thirdly, based on one of the longest distinguishers, a concrete impossible differential cryptanalysis on μ^2 is proposed. The result of this paper shows that μ^2 reduced to 10 rounds can't resist against impossible differential cryptanalysis. To enhance the security level of μ^2 against the reported attack, more complex key schedule should be considered to shorten the length of the key recovery phase. The security level of μ^2 against other cryptanalytic methods should also be investigated which is left as a future work.

Acknowledgements

The authors would like to thank the anonymous reviewers for their helpful comments. This work was partially supported by the National Natural Science Foundation of China under Grant No. 61802437, 61902428, 62102448 and China Postdoctoral Science Foundation under Grant No. 2020M681314.

References

[1] Anand, R., Sinha, A., Bhardwaj, A., Sreeraj, A, "Flawed Security of Social Network of Things," in Handbook of Research on Network Forensics and Analysis Techniques, IGI Global, 2018, pp. 65-86. Article (CrossRef Link).

[2] Gupta, A., Srivastava, A., Anand, R., Tomažič, T, "Business Application Analytics and the Internet of Things: The Connecting Link," in New Age Analytics, Apple Academic Press, 2020, pp. 249-273. Article (CrossRef Link)

[3] Singh, P., Acharya, B., Chaurasiya, R. K, "Efficient VLSI Architectures of LILLIPUT Block Cipher for Resource-constrained RFID Devices," in *Proc. of 2019 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT)*, pp. 1-6, July, 2019. Article (CrossRef Link).

[4] Anusha, R., Shastrimath, V. V. D, "LCBC-XTEA: High throughput lightweight cryptographic block cipher model for low-cost RFID systems," in *Proc. of Computer Science On-line Conference*, Springer, Cham, pp. 185-196, April, 2019. Article (CrossRef Link).

[5] W. Wu and L. Zhang. L, "Block: A lightweight block cipher," in *Proc. of the 9th International Conference on Applied Cryptography and Network Security*, Nerja, Spain, pp. 327–344, 2011. Article (CrossRef Link).

[6] A. Bogdanov, L. R. Knudsen, G. Leander, et al., "PRESENT: An ultra-lightweight block cipher," in *Proc. of 9th International Workshop on Cryptographic Hardware and Embedded Systems*, Vienna, Austria, pp. 450–466, 2007. Article (CrossRef Link).

[7] S. Banik, S.K. Pandey, T. Peyrin, et al., "GIFT: A small present," in *Proc. of the 19th International Conference on Cryptographic Hardware and Embedded Systems*, Taipei, China, pp. 321–345, 2017. Article (CrossRef Link).

[8] S. Banik, A. Bogdanov, T. Isobe, et al., "Midori: A block cipher for low energy," in *Proc. of the 21st International Conference on the Theory and Application of Cryptology and Information Security*, Auckland, New Zealand, pp. 411–436, 2015. Article (CrossRef Link).

[9] R. Beaulieu, S. Treatman-Clark, D. Shors, et al., "The SIMON and SPECK lightweight block ciphers," in *Proc. of the 52nd ACM/EDAC/IEEE Design Automation Conference*, San Francisco, USA, pp. 1–6, 2015. Article (CrossRef Link).

[10] W. Z. Yeoh, J. S. Teh, and Mohd I. S. B. M. Sazali., "μ^2: A Lightweight Block Cipher," in *Proc. of Computational Science and Technology*, Springer, Singapore, pp. 281-290, 2020. Article (CrossRef Link).

[11] Biham, E., Shamir, A, "Differential cryptanalysis of DES-like cryptosystems," *Journal of CRYPTOLOGY*, 4(1), 3-72, 1991. Article (CrossRef Link).

[12] Matsui, M, "Linear cryptanalysis method for DES cipher," in *Proc. of Workshop on the Theory and Application of of Cryptographic Techniques*, Springer, Berlin, Heidelberg, pp. 386-397, 1993. Article (CrossRef Link).

[13] Knudsen, L., & Wagner, D, "Integral cryptanalysis," in *Proc. of International Workshop on Fast Software Encryption*, Springer, Berlin, Heidelberg, pp. 112-127, 2002. Article (CrossRef Link).

[14] L. R. Knudsen, "DEAL - a 128-bit block cipher," *Complexity*, 258(2), 216, 1998. Article (CrossRef Link)

[15] E. Biham, A. Biryukov, and A. Shamir, “Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials,” in *Proc. of International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, Berlin, Heidelberg, pp. 12-23, 1999. Article (CrossRef Link).
[16] Bogdanov, A., & Rijmen, V, “Linear hulls with correlation zero and linear cryptanalysis of block ciphers,” *Designs, codes and cryptography*, 70(3), 369-383, 2014. Article (CrossRef Link)
[17] W. Wu, W. Zhang, D. Feng, “Impossible differential cryptanalysis of reduced-round ARIA and Camellia,” *Journal of computer science and technology*, 22(3), 449-456, 2007. Article (CrossRef Link)
[18] W. Wu, L. Zhang, W. Zhang, “Improved Impossible Differential Cryptanalysis of Reduced-Round Camellia,” in *Proc. of Selected Areas in Cryptography (SAC 2008)*, Springer-Verlag, LNCS vol. 5381, pp. 442-456, 2008. Article (CrossRef Link)
[19] J. Chen, K. Jia, H. Yu, X. Wang, “New Impossible Differential Attacks of Reduced-Round Camellia-192 and Camellia-256,” in *Proc. of Information Security and Privacy (ACISP 2011)*, Springer- Verlag, LNCS vol. 6812, pp. 16-33, 2011. Article (CrossRef Link)
[20] C. Du, J. Chen, “Impossible Differential Cryptanalysis of ARIA Reduced to 7 Rounds,” in *Proc. of Cryptology and Network Security (CANS 2010)*, LNCS vol. 6467, pp. 20-30, 2010. Article (CrossRef Link)
[21] K. Zhang, J. Guan, B. Hu., “Impossible differential cryptanalysis on DVB-CSA,” *KSII Transactions on Internet and Information Systems (TIIS)*, 10(4), 1944-1956, 2016. Article (CrossRef Link)

Kai Zhang is a postdoctoral fellow at Shanghai Jiao Tong University. He received the M.S. and Ph.D. degree in cryptology from the PLA SSF Information Engineering University in 2013 and 2016. His main research interests lie in cryptanalysis. His works have been published in several refereed journals and he has been serving as a referee for several international journals in the area of information security and cryptology.

Xuejia Lai is a professor at Shanghai Jiao Tong University, IACR Fellow. He received Ph.D. of sc. techn in 1992 from the Swiss Federal Institute of Technology, Zurich. He is the co-designer of IDEA block cipher, proposed the concepts of Markov cipher, higher-order differentials, free-start attacks on hash functions; developed DNA algorithm for computing discrete logarithm and proposed public-key system using DNA-chip. He has served as general chair of Asiacrypt 2012, PC chair of Asiacrypt 2006, ISC 2011 and AsiaCCS 2012, and PC-member for about 100 conferences, and editor for 3 ISO standards. He is editor of journals JCST, JISE.

Jie Guan is a professor of the PLA SSF Information Engineering University, China. Her main subject interest is cryptography and her main teaching lies in the areas of information systems, the theory of cryptography and quantum computation. She received Ph.D. degree in cryptography from PLA SSF Information Engineering University in 2004.

Bin Hu is a professor of the PLA SSF Information Engineering University, China. His main subject interests and his main teaching are Boolean function, information security and cryptology. He received Ph.D degree in cryptography from PLA SSF Information Engineering University in 2008.