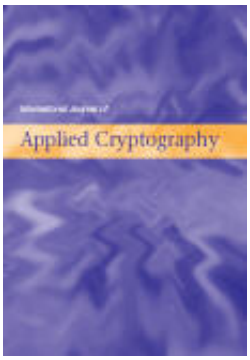
INDERSCIENCE PUBLISHERS
Linking academia, business and industry through research



International Journal of Applied Cryptography

ISSN online: 1753-0571 - ISSN print: 1753-0563
https://www.inderscience.com/ijact

Yoyo cryptanalysis on Future

Sandip Kumar Mondal, Mostafizar Rahman, Santanu Sarkar, Avishek Adhikari

DOI: 10.1504/IJACT.2024.10063224

Article History:

Received:	21 January 2023
Last revised:	26 August 2023
Accepted:	06 September 2023
Published online:	03 May 2024

Yoyo cryptanalysis on Future

Sandip Kumar Mondal

Department of Pure Mathematics,
University of Calcutta,
Kolkata, India
Email: sandipkumarmondal80@gmail.com

Mostafizar Rahman

RC Bose Centre for Cryptology and Security,
Indian Statistical Institute,
Kolkata, India
Email: mrahman454@gmail.com

Santanu Sarkar*

Department of Mathematics,
Indian Institute of Technology Madras,
Chennai, India
Email: sarkar.santanu.bir1@gmail.com
*Corresponding author

Avishek Adhikari

Department of Mathematics,
Presidency University,
Kolkata, India
Email: avishek.adh@gmail.com

Abstract: In ASIACRYPT 2017, Rønjom et al. reported Yoyo tricks on generic rounds of SPNs. Then they applied it to AES and found the most effective way to distinguish AES in several rounds. In FSE 2018, Saha et al. distinguished AES in a known key setting up to 8 rounds. In AFRICACRYPT 2022, Gupta et al. published a block cipher Future, whose design is like AES with some tweaks. In this paper, we analysed Future by Yoyo trick in both secret key settings and known key settings. We show that in the secret key setting, one can distinguish Future upto five and six rounds with data complexity $2^{9.83}$ and $2^{58.83}$ respectively. We also demonstrate that with known key settings, one can distinguish Future with data complexity 2^{15} for both six and eight rounds. Our attack is based on an adaptively chosen plaintext/ciphertext attack.

Keywords: distinguisher; Future; Yoyo.

Reference to this paper should be made as follows: Mondal, S.K., Rahman, M., Sarkar, S. and Adhikari, A. (2023) 'Yoyo cryptanalysis on Future', *Int. J. Applied Cryptography*, Vol. 4, Nos. 3/4, pp.238–249.

Biographical notes: Sandip Kumar Mondal received his BSc in Mathematics(H) from the University of Calcutta, Calcutta, India, in 2014, and an MSc in Pure Mathematics from the University of Calcutta, Calcutta, India, in 2016. Presently he is working as a junior research fellow in the Department of Pure Mathematics, University of Calcutta. His research interests include cryptology and security.

Mostafizar Rahman is currently working as a post-doctoral researcher at University of Hyogo. He completed his BTech and MTech from the Aligarh Muslim University in 2013 and 2016, respectively. He received his PhD from the Indian Statistical Institute, Kolkata in 2022. His current research interests include design and analysis of symmetric-key primitives.

Santanu Sarkar received his PhD in Mathematics from the Indian Statistical Institute, India, in 2011. He is currently a Professor at the Indian Institute of Technology Madras, India. Before that, he was a guest researcher at the National Institute of Standards and Technology (NIST), US. His main research interests include cryptology and number theory.

Avishek Adhikari received his Master's in Pure Mathematics from the University of Calcutta in 2001 and a PhD from the Indian Statistical Institute, India, in 2004. He is currently a Professor at the Department of Mathematics, Presidency University, India. His main research interests include cryptology, algebra, and graph theory.

1 Introduction

With the advent of advanced technologies, the usage of network-connected *resource-constraint* devices has increased drastically. These, in turn, have motivated the cryptographic community to search for block ciphers optimised for such use cases. Katan (De Cannière et al., 2009), Present (Bogdanov et al., 2007), Skinny (Beierle et al., 2016), LED (Guo et al., 2011), etc. are proposed with these design constraints in mind.

Many times, the design principle of such block ciphers is based on substitution and permutation layers. The main goal of a block cipher structure is to maintain security, privacy, and randomness. So one should not be able to distinguish the output of a cipher from a same-length random string. Most of the time, a distinguisher is a statistical or structural feature that is not expected to be present in a similar random function. At the SHA3 competition (National Institute of Standards and Technology, 2007), there were numerous attacks against the Keccak-f public permutation of SHA3 winner Keccak, such as the zero-sum distinguisher [introduced by Aumasson and Meier (2009)]. However, many distinguishing attacks have been reported both on secret-key and known-key settings [introduced by Knudsen and Rijmen (2007)] on AES (Daemen and Rijmen, 2002). Huang et al. (2009) analysed the internal structure of ALPHA-MAC using a five-round algebraic property of AES. Ghosh et al. (2017) propose a new infective countermeasure for preventing fault attacks on the AES block cipher. It is fascinating to study ciphers as public permutations under the known-key paradigm. Knudsen and Rijmen also contend that the non-existence of known-key distinguishers implies the non-existence of secret-key distinguishers, which makes studying the former crucial. In this work, we explore the block cipher Future under distinguishing attacks on both secret-key and known-key settings.

Here we investigate a particular cryptanalysis technique called the Yoyo game, which was first introduced by Biham et al. (1998) and implemented on 16 rounds of SKIPJACK. The Yoyo game is built on adaptively creating new pairings of plaintexts and ciphertexts that retain a certain property inherited from the original pair, similar to Boomerang attacks (Wagner, 1999). Zero difference between the pairs is a commonly used property. Imagine that plaintext/ciphertext has a zero difference property after some rounds of the cipher. A Yoyo game verifies whether new pairs of plaintexts/ciphertexts that are formed by swapping bytes/words of the original pairs have the same zero difference after the same number of rounds. Applying the Yoyo game on the Feistel network, Biryukov et al. (2016) have found a seven-round distinguisher for Feistel networks. In ASIACRYPT 2017, (Rønjom et al., 2017) analysed the Yoyo game on substitution-permutation (SP) networks. They proposed a deterministic distinguisher on two generic SP rounds. Saha et al. (2018) distinguished AESQ up to 16 rounds and distinguished AES up to 8 rounds in the known key setting scenario.

The block cipher Future was proposed by Gupta et al. (2022), which adopts the general structure of the AES round function and tweaks its components for the use of lightweight cryptographic primitives. MDS matrices provide maximum diffusion in block ciphers. However, most lightweight block ciphers do not use MDS matrices in their round function because of their high implementation cost. Future overcomes this challenge by constructing its MDS matrix from four sparse matrices, which cost significantly less to implement in hardware. İlter and Selçuk (2023) construct the MILP model for differential cryptanalysis and linear cryptanalysis on Future. They find a differential characteristic for five-round Future with probability 2^{-62} and a linear characteristic for five-round Future with linear bias 2^{-31}. In Gupta et al. (2022), the designers of Future find an integral distinguisher for six-round Future. Also, the designers predict that the meet-in-the-middle attack may work up to seven rounds. The Yoyo attack is more efficient than linear and differential cryptanalysis on the reduced round Future. This is evident from Table 1, which shows that the Yoyo attack requires less data complexity to distinguish the reduced round Future.

1.1 Our contribution

In this paper, the block cipher Future is analysed with respect to the Yoyo attacks. Both the models – secret-key setting and known-key setting are considered while performing the analysis. First of all, we adapt the notion of Yoyo attacks on nibble-based block cipher Future. In doing so, a distinguishing attack is mounted on five-round and six-round Future in the secret-key setting with a data complexity of $2^{9.83}$ and $2^{58.83}$ respectively. Then we show that for a five-round Future one can find the 128-bit secret key with 2^{64} time complexity. In the known-key setting the notion of impossible Yoyo distinguisher and bi-directional Yoyo distinguisher is applied to mount distinguishing attacks on six-round and eight-round Future with a data complexity of 2^{15}. All the attacks presented in this paper require negligible memory. Our results are tabulated in Table 1.

1.2 Organisation of the paper

Rest of the paper is organised as follows. In Section 2, we tabulate some notations which are used throughout the paper. In addition to that, a brief description of Future and Yoyo attacks is provided in this section. Details regarding Yoyo attacks on five-round and six-round Future in the secret-key setting are discussed in Section 3 with a key recovery attack on five-round Future. Section 4 illustrates Yoyo attacks upon the six-round and eight-round Future in the known-key setting. Finally, the concluding remarks are furnished in Section 5.

Table 1 Comparison of attacks on Future

Key setting	*Round*	*Time complexity**	*Data complexity***	*Memory complexity*	*Attack types*	*Reference*
Secret key	5	$2^{8.83}$ XOR	$2^{9.83}$	Negligible	Yoyo	Section 3
	6	$2^{58.83}$ XOR	$2^{58.83}$	Negligible		
	5	2^{31} XOR	2^{32}	Negligible	Linear	İlter and Selçuk (2023)
	6	2^{62} XOR + 2^{63} MAs***	2^{63}	Negligible	Differential	
Known key	6	$2^{14.415}$	2^{15}	Negligible	Yoyo	Section 4
	8	2^{15}	2^{15}	Negligible		

Notes: *time complexity refers to the time taken to run a single instance of the cipher (unless explicitly specified); **data complexity refers to the number of oracle accesses required; ***MAs refer to the number of memory accesses.

2 Preliminaries

In this section, first of all, we discuss the notations used in the paper. Then, we briefly describe the block cipher Future. Finally, we discuss the Yoyo attack technique.

2.1 Notations

We use the term 'nibble' for 4-bit string and use the term 'word' for four nibbles. The additional notations used in this paper are listed in Table 2.

Table 2 Notations

Notation	*Description*
$K \lll n$	n bits left cyclic shift of binary string K
$w(v)$	Total number of 1 present in the binary string v
$Enc_k(A)$	k round encryption of Future with input state A
$Dec_k(A)$	k round decryption of Future with input state A
$\bar{v}$	Complement of the binary string v
$F \circ G$	Composition of two function F and G, that is $F \circ G(x) = F(G(x))$

2.2 Future

Future is a block cipher published in AFRICACRYPT 2022. It has a 128-bit key length. It receives a 64-bit plaintext as its state and outputs a 64-bit ciphertext. The state can be expressed as 16 4-bit nibbles as follows:

$$State = \begin{bmatrix} s_0 & s_4 & s_8 & s_{12} \\ s_1 & s_5 & s_9 & s_{13} \\ s_2 & s_6 & s_{10} & s_{14} \\ s_3 & s_7 & s_{11} & s_{15} \end{bmatrix},$$

where each s_i is a 4-bit nibble.

In Future, the authors used the four functions namely, SubCell, MixColumn, ShiftRows, and AddRoundKey. The Encryption of the cipher is given in Algorithm 1. The details of the four functions are given below:

- *SubCell (SC):* This is the nonlinear transformation of Future. In which a 4-bit SBox is applied to each nibble of the state, i.e.,

$$s_i \leftarrow SBox(s_i).$$

Table 3 SBox of Future

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

- *MixColumn (MC):* This is the linear transformation of Future. In which the state is multiplied by an MDS matrix M, i.e., $State = M * State$, where

$$M = \begin{bmatrix} 8 & 9 & 1 & 8 \\ 3 & 2 & 9 & 9 \\ 2 & 3 & 8 & 9 \\ 9 & 9 & 8 & 1 \end{bmatrix}.$$

- *ShiftRow (SR):* ShiftRow rotates each row of the state. It rotates every nibble of i^{th} row by i step to the right for i = 0, 1, 2, 3, i.e.,

$$\begin{bmatrix} s_0 & s_4 & s_8 & s_{12} \\ s_1 & s_5 & s_9 & s_{13} \\ s_2 & s_6 & s_{10} & s_{14} \\ s_3 & s_7 & s_{11} & s_{15} \end{bmatrix} \leftarrow \begin{bmatrix} s_0 & s_4 & s_8 & s_{12} \\ s_{13} & s_1 & s_5 & s_9 \\ s_{10} & s_{14} & s_2 & s_6 \\ s_7 & s_{11} & s_{15} & s_3 \end{bmatrix}.$$

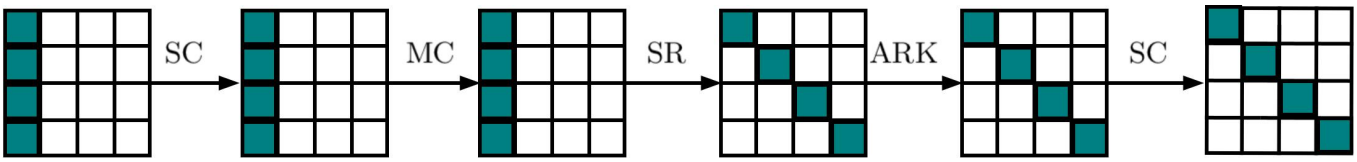
- *AddRoundKey (ARK):* A 64-bit round key (round key generation is discussed later) is xor with the 64-bit state.
- *Round key generation of future:* Let $K = k_0 k_1 \cdots k_{127}$ be the 128-bit key of the cipher Future. Let $K_0 = k_0 k_1 \cdots k_{63}$ and $K_1 = k_{64} k_{65} \cdots k_{127}$. Then the round keys are

$$RK[i] = \begin{cases} K_0 \leftarrow K_0 \lll (5 \cdot \frac{i}{2}) & \text{if } 2|i \\ K_1 \leftarrow K_1 \lll (5 \cdot \lfloor \frac{i}{2} \rfloor) & \text{if } 2 \nmid i, \end{cases} \quad (1)$$

for $0 \le i \le 10$. Now a single bit '1' is xored with each 4-bit nibble (in different positions) of every round except the 0th, 5th, and 10th rounds.

A detailed analysis can be found in the original paper (Gupta et al., 2022) of Future.

Figure 1 SuperSBox of Future (see online version for colours)



Algorithm 1 Future encryption

Input: Plaintext P and Subkeys $RK[0], RK[1], ..., RK[10]$
Output: Cipher text C

$State$ = AddRoundKey($P, RK[0]$)
for $i = 1$ *to* 9 **do**
  $State$ = SubCell($State$)
  $State$ = MixColumn($State$)
  $State$ = ShiftRows($State$)
  $State$ = AddRoundKey($State, RK[i]$)
$State$ = SubCell($State$)
$State$ = ShiftRows($State$)
C = AddRoundKey($State, RK[10]$)
return C

2.2.1 *SuperSBox of Future*

Let $S = SC \circ SR \circ MC \circ SC$. The input of S consists of four parallel column vectors, each of which has four nibbles. Now after the SC operation, each column maps into that column. Also, MC is a function that takes a column as input and gives a column as output. Now after the SR operation, each column vector goes to the diagonal vectors. After that, SC operation takes the diagonal to the same diagonal. So if we see the input of S as a four column vector each of which contains four nibbles, then the output of S is the diagonal vector. Here each column maps into a specific diagonal. We can see S as a four parallel SBoxes which acts on the columns of the input state. We call these 32-bit SBox as SuperSBox. The SuperSBox is visualised in Figure 1.

2.3 *Yoyo attacks*

Here, we provide some notions related to the Yoyo game in the context of substitution-permutation network-based block ciphers.

2.3.1 *Zero difference pattern*

Definition 2.1 (Rønjom et al., 2017): Let $\alpha = (\alpha_0, \alpha_1, ..., \alpha_{n-1}) \in \mathbb{F}_q^n$. Let $\nu(\alpha) = (z_0, z_1, ..., z_{n-1}) \in \mathbb{F}_2^n$ where $z_i = 1$ if $\alpha_i = 0$ and $z_i = 0$ otherwise. Then $\nu(\alpha)$ is the zero difference pattern for α.

In the case of Future, we write a state $\alpha = (\alpha_0, \alpha_1, \alpha_2, \alpha_3) \in \mathbb{F}_{2^{16}}^4$ where sometimes we use α_i as a column of the state α and sometimes we use α_i as a diagonal of the state. So here we define $\nu_{col}(\alpha) = \nu(\alpha)$ when α_i's are considered as columns of the state and $\nu_{diag}(\alpha) = \nu(\alpha)$ when α_i's are considered as diagonals of the state.

For example, let

$$\alpha = \begin{bmatrix} 0\,0\,3\,4 \\ 0\,6\,0\,8 \\ 0\,a\,b\,0 \\ 0\,d\,e\,f \end{bmatrix}.$$

Now if we consider α_i as columns of the state α then α = (0, 06ad, 30be, 480f) and then $\nu_{col}(\alpha)$ = (1, 0, 0, 0). On the other hand if we consider α_i as diagonals of the state α then α = (06bf, 0, 380d, 40ae) and then $\nu_{diag}(\alpha)$ = (0, 1, 0, 0).

Now if we write $\nu(\alpha_i)$ then we take α_i as four nibbles, i.e., $\alpha_i \in \mathbb{F}_{2^{16}}^1 = \mathbb{F}_{2^4}^4$. In the above example α_1 = (0, 6, a, d) so $\nu(\alpha_1)$ = (1, 0, 0, 0).

2.3.2 *Deterministic Yoyo distinguisher for two generic SP-rounds*

In a symmetric key cryptosystem, many ciphers are created by applying substitution and permutation operations repeatedly. One generic SP-round means one substitution S and one permutation L operation. So n generic SP-rounds means n times one generic SP-round has repeated.

Definition 2.2 (Rønjom et al., 2017): Let $v \in \mathbb{F}_2^n$ be a boolean vector. Let $\alpha, \beta \in \mathbb{F}_q^n$ be a pair of states. Then $\rho^v(\alpha, \beta)$ is a new state created from α and β. The i^{th} component of $\rho^v(\alpha, \beta)$ is defined as follows:

$$\rho_i^v(\alpha, \beta) = \begin{cases} \alpha_i, & \text{if } v_i = 1 \\ \beta_i, & \text{if } v_i = 0. \end{cases} \tag{2}$$

Two generic SP rounds can be written as $G_2 = L \circ S \circ L \circ S$. Rønjom et al. (2017) find a deterministic distinguisher for two generic SP rounds G_2. For finding the distinguisher authors ignore the last permutation layer L as this does not violate any security of the cipher. So we can write two generic SP rounds as $G_2 = S \circ L \circ S$, where L is a permutation layer. The deterministic Yoyo distinguisher for G_2 is described in the following proposition.

Proposition 1 (Rønjom et al., 2017): Let $P_0, P_1 \in \mathbb{F}_q^n$ and $C_0 = G_2(P_0)$, $C_1 = G_2(P_1)$. Let $v \in \mathbb{F}_2^n$. Suppose $C_0' = \rho^v(C_0, C_1)$ and $C_0' = \rho^v(C_1, C_0)$. Then

$$\nu(G_2^{-1}(C_0') \oplus G_2^{-1}(C_1')) = \nu(P_0 \oplus P_1).$$

Now in the cipher Future if we take $S = SC \circ MC \circ SR \circ SC$ and $L = SR \circ MC$, then the two-round Future can

be written as $R^2 = L \circ S$. In our analysis, we remove the operation ARK as ARK have no effect when we take the XOR difference of two states. So four-round Future can be written as $R^4 = S \circ L \circ S$. Here we remove the last linear layer L for simplicity of our attack. When we use Yoyo distinguisher for a four-round, we call it a four-round Yoyo game in the forward direction. Now we see that $S^{-1} \circ L^{-1} \circ S^{-1}$ is also a two SP-rounds. So here also Yoyo distinguisher works. Here we call it a four-round Yoyo game in the backward direction.

Let (P_0, P_1) be a pair of states. Then one can generate a new pair (C_0, C_1) by using the function ρ^v twice, where $C_0 = \rho^v(P_0, P_1)$ and $C_1 = \rho^v(P_1, P_0)$. The new pair depends on the value of v. As $|v| = n$, there are 2^n choices of v. So one can generate 2^n pairs from P_0, P_1. Note that if ρ^v generate the pair (C_0, C_1) then $\rho^{\bar{v}}$ generate the pair (C_1, C_0). The pair (C_0, C_1) and the pair (C_1, C_0) generate same set $\{C_0, C_1\}$. We can generate $2^{n-1} - 1$ many new sets from a given pair. In case of Future $n = 4$. So we can generate 7 distinct new pairs. For generating new pair we use the method used in Rønjom et al. (2017). Algorithm 2 is used for generating these pairs.

Algorithm 2 $SWAP_{col}(\alpha, \beta)$

Input: $\alpha = (\alpha_0, \alpha_1, \alpha_2, \alpha_3)$, $\beta = (\beta_0, \beta_1, \beta_2, \beta_3)$ be two state where α_i, β_i are columns of the state α and β respectively.
Output: α'

```
α' = α
for i = 0 to 3 do
    if α_i ≠ β_i then
        α'_i = β_i
        Break
return α'
```

In Algorithm 2, if we take $\alpha = (\alpha_0, \alpha_1, \alpha_2, \alpha_3)$ and $\beta = (\beta_0, \beta_1, \beta_2, \beta_3)$ where α_i, β_i are diagonals of the state α and β respectively, then we call the above function as $SWAP_{diag}(\alpha, \beta)$.

3 Yoyo attack on Future in the secret-key setting

This section discusses the Yoyo attack on Future in a secret key setting in which the secret key is unknown to the attacker.

3.1 Distinguishing attack on five-round Future

In this subsection, we devise a distinguisher for five-round Future. The distinguisher is based on exploring a well-known property (refer to Lemma 2) of the minimum distance separable (MDS) matrix.

Let M be an MDS matrix of order $n \times n$ with branch number $(n+1)$. Then for a vector $A \in \mathbb{F}_q^n$, the active nibbles in A and MA are at least $(n+1)$. This result is also true for M^{-1}. Thus we have the following result.

Lemma 2 (Daemen and Rijmen, 2002): Assume that $A \in \mathbb{F}_q^n$ is a non-zero vector. Let M be an MDS matrix of order $(n \times n)$ with branch number $(n+1)$. Then $w(\nu(A)) + w(\nu(MA)) \leq (n-1)$.

Proof: This is a well-known property of the MDS matrix.

□

Rønjom et al. (2017) distinguished five-round AES by Yoyo distinguisher. Here, we take a similar approach. Now five rounds Future can be written as

$$\begin{aligned} R^5 &= S \circ L \circ S \circ SR \circ MC \circ SC \\ &= S \circ L \circ S \circ X, \text{ where } X = SR \circ MC \circ SC. \end{aligned}$$

We have already discussed that for the $S \circ L \circ S$ construction, there exists a deterministic Yoyo distinguisher. Now for the five-round Future, there is an extra operation X, which is dependent on the cipher Future. So we need to analyse the operation X. Let $(Q_0 \oplus Q_1)$ be a state difference such that $w(\nu_{col}(Q_0 \oplus Q_1)) = t$. Now if we take X^{-1} of these two states, SWAP them, and then take the operation X on these states, we get the state difference $(Q_0' \oplus Q_1')$. Then also $w(\nu_{col}(Q_0' \oplus Q_1')) = t$. This result is given below as a proposition:

Proposition 3: Let Q_0 and Q_1 be two states such that $w(\nu_{col}(Q_0 \oplus Q_1)) = t$. Let $P_0 = \rho^v(X^{-1}(Q_0), X^{-1}(Q_1))$ and $P_1 = \rho^v(X^{-1}(Q_1), X^{-1}(Q_0))$. Then $w(\nu_{col}(X(P_0) \oplus X(P_1))) = t$.

Proof: We know that $X = SR \circ MC \circ SC$.

It is clear that for any two states A_0, A_1, the relations

$$\rho^v(SC(A_0), SC(A_1)) = SC(\rho^v(A_0, A_1)) \tag{3}$$

and

$$\rho^v(MC(A_0), MC(A_1)) = MC(\rho^v(A_0, A_1)) \tag{4}$$

hold. It is noted that here we consider the state A_0, A_1 column wise while computing ρ^v. Using equations (3) and (4) we can say that

$$\begin{aligned} &\rho^v(MC \circ SC(A_0), MC \circ SC(A_1)) \\ &= MC \circ SC(\rho^v(A_0, A_1)) \end{aligned} \tag{5}$$

From equation 5, we can say that when we take the operation X^{-1} over Q_0 and Q_1 then applying the function ρ^v for changing the pair is the same as changing the pair after the operation SR using the function ρ^v.

We now show that if $w(\nu_{col}(A_0 \oplus A_1)) = t$, $B_0 = \rho^v(SR^{-1}(A_0), SR^{-1}(A_1))$, $B_1 = \rho^v(SR^{-1}(A_1), SR^{-1}(A_0))$, then $w(\nu_{col}(SR(B_0) \oplus SR(B_1))) = t$.

Now $SR^{-1}(A_0) \oplus SR^{-1}(A_1) = \rho^v(SR^{-1}(A_0), SR^{-1}(A_1)) \oplus \rho^v(SR^{-1}(A_1), SR^{-1}(A_0)) = B_0 \oplus B_1$. Since SR is a linear operation, we have $(A_0 \oplus A_1) = (SR(B_0) \oplus SR(B_1))$. Thus we have

$$w(\nu_{col}(A_0 \oplus A_1)) = w(\nu_{col}(SR(B_0) \oplus SR(B_1))). \tag{6}$$

Therefore if $w(\nu_{col}(Q_0 \oplus Q_1)) = t$ and $P_0 = \rho^v(X^{-1}(Q_0), X^{-1}(Q_1))$ and $P_1 = \rho^v(X^{-1}(Q_1), X^{-1}(Q_0))$, then using the equations (5) and (6) we say that $w(\nu_{col}(X(P_0) \oplus X(P_1))) = t$. □

Now in the above Proposition 3 we assume that $w(\nu_{col}(X(P_0) \oplus X(P_1))) = t$. So now we try to find out the probability of $w(\nu_{col}(X(P_0) \oplus X(P_1)) = t$ for some special choice of the input plaintext P_0 and P_1. The next proposition is as follows:

Proposition 4: Let P_0 and P_1 be two inputs of X with $w(\nu_{col}(P_0 \oplus P_1)) = 3$. Then probability of $w(\nu_{col}(X(P_0) \oplus X(P_1))) = t$ is approximately $\binom{4}{t}(2^{-4})^t$.

Proof: Let $w(\nu_{col}(P_0 \oplus P_1)) = 3$, i.e., there is only one active column in $P_0 \oplus P_1$. As the SC operation takes a non-zero difference to a non-zero difference and zero difference to a zero difference, so after the SC operation there is one active column in xor difference states. Now after MC, we get only one active column in xor difference. In this active column, t nibbles are zero with a probability approximately $\binom{4}{t}(2^{-4})^t$. So after SR operation, there are $(4-t)$ active columns with probability approximately $\binom{4}{t}(2^{-4})^t$, i.e., $w(\nu_{col}(X(P_0) \oplus X(P_1))) = t$ with probability $\binom{4}{t}(2^{-4})^t$. □

Now, we mount a distinguishing attack on Future, i.e., we obtain some property for Future which will distinguish it from a random permutation. For this purpose, we investigate the function X and find a property that is always true for Future but not always true for a random permutation. The next proposition is about the property which will help us to distinguish Future.

Proposition 5: Let P_0 and P_1 be two inputs of X. Suppose $w(\nu_{col}(X(P_0) \oplus X(P_1))) = t$. Then every column of $P_0 \oplus P_1$ contains atmost $(3-t)$ zero nibbles.

Proof: Given that $w(\nu_{col}(X(P_0) \oplus X(P_1))) = t$. Therefore there are $(4-t)$ active columns in $X(P_0) \oplus X(P_1)$. After applying SR^{-1} there are atmost $(4-t)$ active nibbles in every column. Suppose a column has atmost $(4-t)$ active nibbles. Then there are at least t nibbles that are inactive. Then using Lemma 2 we say that after MC^{-1} that column contains atmost $(3-t)$ inactive nibbles, i.e. zero nibbles. Therefore every column of $P_0 \oplus P_1$ contains atmost $(3-t)$ zero nibbles. □

We are now ready to distinguish cipher Future for reduced rounds. Next, we describe the distinguishing attack for five-round Future.

We see that the five-round Future can be written as $R^5 = S \circ L \circ S \circ X$, where $X = SR \circ MC \circ SC$. Let P_0, P_1 be two states such that $w(\nu_{col}(X(P_0) \oplus X(P_1))) = t$. Take $Q_0 = X(P_0)$ and $Q_1 = X(P_1)$. Then $w(\nu_{col}(Q_0 \oplus Q_1)) = t$. Now let $C_0 = S \circ L \circ S(Q_0)$ and $C_1 = S \circ L \circ S(Q_1)$ be the ciphertext corresponding to the plaintext P_0, P_1. Applying the ρ^v function we changed the pair (C_0, C_1) to the pair (C_0', C_1'), i.e., $C_0' = \rho^v(C_0, C_1)$, $C_1' = \rho^v(C_1, C_0)$. Suppose $Q_0' = S^{-1} \circ L^{-1} \circ S^{-1}(C_0')$, $Q_1' = S^{-1} \circ L^{-1} \circ S^{-1}(C_1')$. Then, $w(\nu_{col}(Q_0' \oplus Q_1')) = t$ as this is the four-round Yoyo game in the forward direction from the pair (Q_0, Q_1). Let $P_0' = X^{-1}(Q_0')$ and $P_1' = X^{-1}(Q_1')$. Then by Proposition 5 we can say that $P_0' \oplus P_1'$ contains atmost $(3-t)$ inactive nibbles in each column. So if we get a column with $(4-t)$ inactive nibbles, then we get a contradiction. Let $P_0'' = \rho^v(P_0', P_1')$ and $P_1'' = \rho^v(P_1', P_0')$. Using Proposition 3 we can say that $w(\nu_{col}(X(P_0'') \oplus X(P_1''))) = t$. So we can continue this and check whether any contradiction occurs or not.

Algorithm 3 Five-round distinguish attack

Input: $2^{5.415}$ pairs (P_0, P_1) such that $w(\nu_{col}(P_0 \oplus P_1)) = 3$.
Output: 1 for Future and –1 for not Future.

```
for x = 0 to 2^5.415 do
    choose P0, P1 randomly such that w(ν_col(P0 ⊕ P1)) = 3
    flag = 0
    for y = 0 to 2^3.415 do
        C0 = Enc5(P0), C1 = Enc5(P1)
        C0' = SWAP_diag(C0, C1), C1' = SWAP_diag(C1, C0)
        P0' = Dec5(C0), P1' = Dec5(C1)
        for i = 0 to 3 do
            if 2 ≤ (w(ν((P0' ⊕ P1')_i))) < 4 then
                flag = 1
                break
        P0 = SWAP_col(P0', P1'), P1 = SWAP_col(P1', P0')
    if flag == 0 then
        return 1
return –1
```

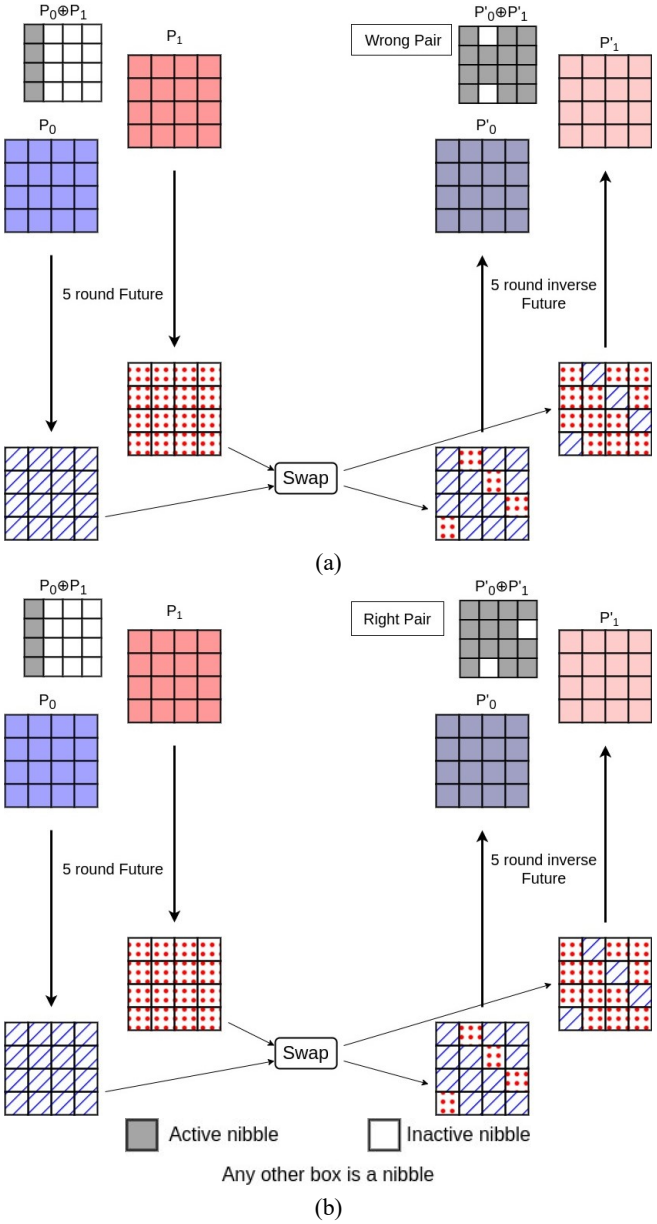
Now there is a probability that we get $w(\nu_{col}(X(P_0) \oplus X(P_1))) = t$ for some random input P_0, P_1. When we get a pair (P_0, P_1) such that $w(\nu_{col}(X(P_0) \oplus X(P_1))) = t$, we can continue the above process without any contradiction for the cipher Future. But in the case of the random permutation, we get a contradiction after a certain time. So for a pair, if we get a contradiction then we call that pair a wrong pair, and if we do not get any contradiction, then we call that pair a right pair. In Algorithm 3 we describe the attack for $w(\nu_{col}(X(P_0) \oplus X(P_1))) = 2$. In Figure 2 we give examples of wrong pair and right pair for $w(\nu_{col}(X(P_0) \oplus X(P_1))) = 2$. In the next subsection, the complexity of this attack is given.

3.1.1 *Complexity analysis*

To find the complexity of the above algorithm, we first try to find out the probability of at least one column with at least $(4-t)$ inactive nibbles. So our next lemma is as follows.

Lemma 6: The probability of at least one column with at least $(4-t)$ inactive nibbles in a random state is approximately $p_1(t) = 4\binom{4}{t}(2^{-4})^{4-t}$.

Figure 2 Five-round distinguishing attack, (a) as in $P'_0 \oplus P'_1$ there are two inactive nibbles in a single column, (P_0, P_1) is a wrong pair (b) as in $P'_0 \oplus P'_1$ every column has at most one inactive nibble, (P_0, P_1) is a right pair (see online version for colours)



Proof: The probability of getting $(4-t)$ inactive nibbles in a column is $\binom{4}{t}(2^{-4})^{4-t}$. There are four columns in a state. So the probability of getting at least one column with at least $(4-t)$ inactive nibbles is approximately $p_1(t) = 4\binom{4}{t}(2^{-4})^{4-t}$. □

Now we take P_0, P_1 with $w(\nu_{col}(P_0 \oplus P_1)) = 3$. From Proposition 4 the probability of $w(\nu_{col}(X(P_0) \oplus X(P_1))) = t$ is $p_2(t) = \binom{4}{t}(2^{-4})^t$. Therefore to get a pair such that $w(\nu_{col}(X(P_0) \oplus X(P_1))) = t$, we have to generate $p_2(t)^{-1}$ pairs and for every pair we create $p_1(t)^{-1}$ pairs by Yoyo game to distinguished five-round Future. Hence, the total data complexity for this distinguishing attack is $2 \cdot p_1(t)^{-1} \, p_2(t)^{-1}$.

Hence, the data complexities for $t = 1, 2, 3$ are 2^{11}, $2^{9.83}$ and 2^{11} respectively. In Algorithm 3 we describe our distinguishing attack for $t = 2$. In this case $p_1(2)^{-1} = 2^{3.415}$ and $p_2(2)^{-1} = 2^{5.415}$. In Algorithm 3 we see that after getting the pair (P'_0, P'_1) we need to xor that pair for further analysis. So the time complexity of Algorithm 3 is $2^{5.415} \cdot 2^{3.415} = 2^{8.83}$ xor operation of states.

3.2 Distinguishing attack on six-round Future

The six-round Future can be written as $R^6 = S \circ L \circ S \circ L \circ S$. Similar to the five-round attack, here also we try to find out some condition which is true for the cipher Future but not true for a random permutation. Rønjom et al. (2017) used the relation [for proof see Daemen and Rijmen (2007)] between the input difference and the output difference of the function $S \circ L \circ S$ for distinguished six-round AES. Here we also try to find out a relation between the input difference and output difference of the function $S \circ L \circ S$ for distinguished six-round Future. Our next theorem is about that relation.

Theorem 7: Let P_0, P_1 be two state and $Q_0 = S \circ L \circ S(P_0)$, $Q_1 = S \circ L \circ S(P_1)$. Then $w(\nu_{col}(P_0 \oplus P_1)) + w(\nu_{diag}(Q_0 \oplus Q_1)) \leq 3$ if $w(\nu_{col}(P_0 \oplus P_1)) \leq 3$.

Proof: Let $w(\nu_{col}(P_0 \oplus P_1)) = t$. Then after the operation S there are $(4-t)$ active diagonals. So every column contains atmost $(4-t)$ active nibbles, i.e., every column contains at least t inactive nibbles. Now $L = SR \circ MC$. So after MC operations by Lemma 2 (for $n = 4$), we can say that every column contains atmost $(3-t)$ inactive nibbles, i.e., every column contains at least $4-(3-t) = (1+t)$ active nibbles. So after the SR operation, there are at least $(1+t)$ active columns. So after operation S there are at least $(1+t)$ active diagonals, i.e., there are atmost $(3-t)$ inactive diagonals. So $w(\nu_{diag}(Q_0 \oplus Q_1)) \leq (3-t)$. Therefore $w(\nu_{col}(P_0 \oplus P_1)) + w(\nu_{diag}(Q_0 \oplus Q_1)) \leq t + (3-t) = 3$. □

Let us take a pair of plaintext (P_0, P_1) such that $w(\nu_{col}((L \circ S(P_0)) \oplus (L \circ S(P_1)))) = t$ where $1 \leq t \leq 3$. Suppose $Q_0 = L \circ S(P_0)$ and $Q_1 = L \circ S(P_1)$. Now let $C_0 = Enc_6(P_0)$ and $C_1 = Enc_6(P_1)$ i.e., $C_0 = S \circ L \circ S(Q_0)$ and $C_1 = S \circ L \circ S(Q_1)$. Then we can say that $w(\nu_{col}(Q_0 \oplus Q_1)) + w(\nu_{diag}(C_0 \oplus C_1)) \leq 3$ by Theorem 7.

$$\text{i.e., } w(\nu_{diag}(C_0 \oplus C_1)) \leq 3 - t. \tag{7}$$

Now $w(\nu_{col}(Q_0 \oplus Q_1)) = t$. From here we play a four-round Yoyo game in the forward direction and get Q'_0, Q'_1, i.e., $Q'_0 = S^{-1} \circ L^{-1} \circ S^{-1}(C_0)$ and $Q'_1 = S^{-1} \circ L^{-1} \circ S^{-1}(C_1)$. From Proposition 1 we say that $w(\nu_{col}(Q'_0 \oplus Q'_1)) = t$. Now $w(\nu_{col}(Q'_0 \oplus Q'_1)) = t \implies w(\nu_{diag}(S(Q'_0) \oplus S(Q'_1))) = t$. Let $P'_0 = S^{-1} \circ L^{-1}(Q'_0)$,

$P'_1 = S^{-1} \circ L^{-1}(Q'_1)$, i.e., $P'_0 = S^{-1} \circ L^{-1} \circ S^{-1}(S(Q'_0))$, $P'_1 = S^{-1} \circ L^{-1} \circ S^{-1}(S(Q'_1))$. Therefore by Theorem 7 we write $w(\nu_{diag}(S(Q'_0) \oplus S(Q'_1))) + w(\nu_{col}((P'_0 \oplus P'_1))) \leq 3$. Thus we have

$$w(\nu_{col}((P'_0 \oplus P'_1))) \leq 3 - t. \quad (8)$$

Now let $R_0 = S(Q'_0)$, $R_1 = S(Q'_1)$. Therefore $w(\nu_{diag}(R_0 \oplus R_1)) = t$. If we play a four-round Yoyo game in the backward direction from the pair (R_0, R_1) and we get (R'_0, R'_1), i.e., $R'_0 = S \circ L \circ S(P'_0)$ and $R'_1 = S \circ L \circ S(P'_1)$. Then from Proposition 1 we can say that $w(\nu_{diag}(R'_0 \oplus R'_1)) = t$ and so $w(\nu_{col}(S^{-1}(R'_0) \oplus S^{-1}(R'_1))) = t$, i.e., $w(\nu_{col}((L \circ S(P'_0)) \oplus (L \circ S(P'_1)))) = t$. Now we are at the stage where we start. Continue this process up to a certain time (which is discussed in the next subsection), if we get a contradiction of the equations (7) or (8) then we can say that the cipher is not Future, and if the conditions are satisfied up to a certain time, we conclude that the cipher is Future. So for a pair, if we get a contradiction, then we call that pair a wrong pair, and if we do not get any contradiction, then we call that pair a right pair. In Algorithm 4 we describe the attack for $w(\nu_{col}((L \circ S(P_0)) \oplus (L \circ S(P_1)))) = 2$. In Figure 3 we give examples of wrong pair and right pair for $w(\nu_{col}((L \circ S(P_0)) \oplus (L \circ S(P_1)))) = 2$.

Algorithm 4 Six-round distinguish attack

Input: $2^{28.415}$ pairs (P_0, P_1)
Output: 1 for Future and -1 for not Future

for x = *0 to* $2^{28.415}$ **do**
  choose P_0, P_1 randomly
  flag = 0
  for y = *0 to* $2^{29.415}$ **do**
    if $(w(\nu_{col}(P_0 \oplus P_1))) \geq 2$ **then**
      flag = 1
    $C_0 = Enc_6(P_0)$
    $C_1 = Enc_6(P_1)$
    if $(w(\nu_{diag}(C_0 \oplus C_1))) \geq 2$ **then**
      flag = 1
    $C'_0 = SWAP_{diag}(C_0, C_1)$, $C'_1 = SWAP_{diag}(C_1, C_0)$
    $P'_0 = Dec_6(C_0)$, $P'_1 = Dec_6(C_1)$
    $P_0 = SWAP_{col}(P'_0, P'_1)$, $P_1 = SWAP_{col}(P'_1, P'_0)$
  if *(flag == 0)* **then**
    return 1
return–1

Complexity analysis

Now for a random permutation the probability of getting a xor differential state with at least $(4 - t)$ inactive word is $q_1(t) = \binom{4}{4-t}(2^{-16})^{(4-t)}$. At first we assume that $w(\nu((L \circ S(P_0) \oplus L \circ S(P_1)))) = t$. Now the probability of getting such state is $q_2(t) = \binom{4}{t}(2^{-16})^t(1 - 2^{-16})^{(4-t)}$.

Therefore for getting a pair such that $w(\nu(L \circ S(P_0) \oplus L \circ S(P_1))) = t$, we have to generate $q_2(t)^{-1}$ pairs. In this case, we are trying to get a contradiction by two equations (7) and (8), one is a relation between ciphertext pair and one is a relation between plaintext pair. So for every pair we create $\frac{q_1(t)^{-1}}{2}$ pairs by Yoyo game to distinguished six-round Future. The total data complexity for this distinguishing attack is $2 \cdot q_2(t)^{-1} \frac{q_1(t)^{-1}}{2} = q_2(t)^{-1} q_1(t)^{-1}$. The data complexities for $t = 1, 2, 3$ are 2^{60}, $2^{58.83}$ and 2^{60}, respectively. Now in Algorithm 4 we describe our distinguishing attack for $t = 2$. In this case $q_1(2)^{-1} = 2^{29.415}$ and $q_2(2)^{-1} = 2^{29.415}$. In Algorithm 4 we see that when we get the pairs (P_0, P_1) and (C_0, C_1) then we have to xor the pairs for further analysis. So the time complexity for Algorithm 4 is $2^{28.415} \cdot 2^{29.415} \cdot 2 = 2^{58.83}$ xor operation of states.

3.3 Key recovery attack on five-round Future

From Section 3, we see that five-round Future can be written as $R^5 = S \circ L \circ S \circ X$, where $X = SR \circ MC \circ SC$. In this section, we will find the subkey $RK[0]$ which is xor in the beginning of R^5. The MixColumn matrix M in Future is defined by the matrix

$$M = \begin{bmatrix} \alpha^3 & \alpha^3 \oplus 1 & 1 & \alpha^3 \\ \alpha \oplus 1 & \alpha & \alpha^3 \oplus 1 & \alpha^3 \oplus 1 \\ \alpha & \alpha \oplus 1 & \alpha^3 & \alpha^3 \oplus 1 \\ \alpha^3 \oplus 1 & \alpha^3 \oplus 1 & \alpha^3 & 1 \end{bmatrix}.$$

Let P_x be the plaintext, and let $(P_x)_i$ denote the i'th column of the plaintext P_x for $0 \leq i \leq 3$. Now we take two plaintexts P_0 and P_1 such that $(P_0)_0 = (0, i, 0, 0)$ and $(P_1)_0 = (z, z \oplus i, 0, 0)$ where z is a random non-zero element in $\{0, 1\}^4$ and the other columns are equal for the two plaintexts. Let $RK[0] = (RK[0][0], RK[0][1], RK[0][2], RK[0][3])$ where each $RK[0][i]$ is the column of the the subkey $RK[0]$. Now the difference between the first column of the two partial encrypted plaintexts through $MC \circ SC \circ ARK$ becomes

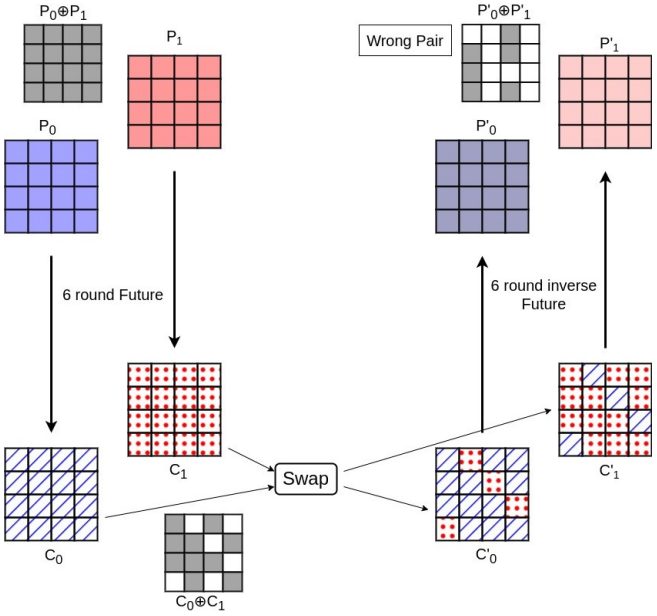
$$\begin{aligned} &\alpha^3 d_0 \oplus (\alpha^3 \oplus 1) d_1 = m_0 \\ &(\alpha \oplus 1) d_0 \oplus \alpha d_1 = m_1 \\ &\alpha d_0 \oplus (\alpha \oplus 1) d_1 = m_2 \\ &(\alpha^3 \oplus 1) d_0 \oplus (\alpha^3 \oplus 1) d_1 = m_3 \end{aligned}$$

where $d_0 = SBox[RK[0][0]] \oplus SBox[z \oplus RK[0][0]]$ and $d_1 = SBox[i \oplus RK[0][1]] \oplus SBox[z \oplus i \oplus RK[0][1]]$. Now, the equation pertaining to m_3 can be written as follows

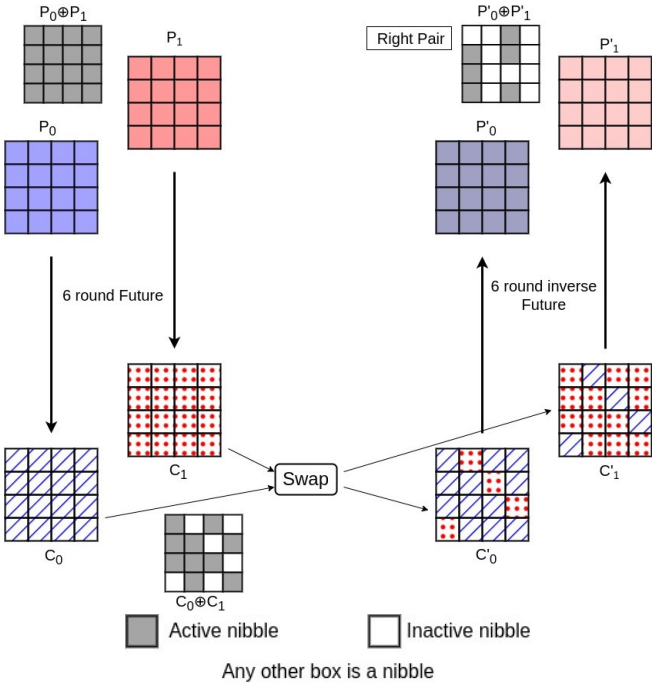
$$\begin{aligned} m_3 = &(\alpha^3 \oplus 1)(SBox[RK[0][0]] \\ &\oplus SBox[z \oplus RK[0][0]]) \\ &\oplus (\alpha^3 \oplus 1)(SBox[RK[0][1] \oplus z \oplus i] \\ &\oplus SBox[z \oplus RK[0][1] \oplus i]). \end{aligned}$$

The value of m_3 becomes zero for $i \in \{RK[0][0] \oplus RK[0][1], z \oplus RK[0][0] \oplus RK[0][1]\}$. So if we run through all values of $i \in \{0, 1\}^4$, we can find at least two values of i for which the term m_3 in fourth equation is zero.

Figure 3 Six-round distinguishing attack, (a) as in $P'_0 \oplus P'_1$ there are two inactive columns, (P_0, P_1) is a wrong pair (b) as in $C_0 \oplus C_1$ there is one inactive diagonal, and $P'_0 \oplus P'_1$ has one inactive column, (P_0, P_1) is a right pair (see online version for colours)



(a)



(b)

Now we form a set of plaintext as follows. For each i generate a pair of plaintexts P_0 and P_1 such that the first column of P_0 and P_1 are (0, i, 0, 0) and (z, $z \oplus i$, 0, 0) respectively. Other columns for P_0 and P_1 are the same. Now we generate four new pair of plaintexts by five-round Yoyo game (one can see Algorithm 5 for more clarity). This four pairs with the pair (P_0, P_1) forms a set of pairs of plaintext with five elements. So if a pair is of the correct form then it satisfies the fourth equation with $m_3 = 0$.

Algorithm 5 Key recovery attack on five-round Future

Input: 2^4 plaintext pairs (P_0, P_1) such that $(P_0)_0$ = (0, i, 0, 0) and $(P_1)_0$ = (1, 1 $\oplus$ i, 0, 0) for i = 0, 1, ..., 2^{4-1} and $(P_0)_j = (P_1)_j$ for j = 1, 2, 3.
Output: Subkey $SK[0][0]$

for i = *0 to* 2^{4-1} **do**
  P_0 = 0, P_1 = 0
  $(P_0)_0$ = (0, i, 0, 0), $(P_1)_0 = (1, 1 \oplus i, 0, 0)$
  $S = \{(P_0, P_1)\}$
  for y = *1 to 4* **do**
    $C_0 = Enc_5(P_0)$, $C_1 = Enc_5(P_1)$
    $C'_0 = SWAP_{diag}(C_0, C_1)$, $C'_1 = SWAP_{diag}(C_1, C_0)$
    $P'_0 = Dec_5(C_0)$, $P'_1 = Dec_5(C_1)$
    $P_0 = SWAP_{col}(P'_0, P'_1)$, $C_1 = SWAP_{col}(P'_1, P'_0)$
    $S = S \cup \{(P_0, P_1)\}$
  for $SK[0][1] = 0$ *to* 2^{4-1} **do**
    for $SK[0][2] = 0$ *to* 2^{4-1} **do**
      for $SK[0][3] = 0$ *to* 2^{4-1} **do**
        $SK[0][0] = SK[0][1] \oplus i$
        for *every* $\{P_0, P_1\} \in S$ **do**
          if $m_3 \neq 0$ **then**
            jump to the next possible $SK[0]$
        return $SK[0]$

Now the adversary can test for remaining 2^{12} candidate keys and check the fourth equation for all five pairs, where we know that $RK[0][0] \oplus RK[0][1] \in \{i, i \oplus z\}$ for known values of i and z. The equation holds for a random key for all five pairs with probability $2^{-4 \cdot 5} = 2^{-20}$. So when testing for total 2^{12} keys there may be a false positive occurs with probability $2^{-20} \cdot 2^{12} = 2^{-8}$. Now when a key satisfies the condition for five pairs then one can generate more plaintext pairs to remove the false positive. As this happens rarely this does not affect the total data complexity. The total $2^4 \cdot 5$ number of adaptively chosen plaintext pairs is needed for finding the correct key. Thus the data complexity for this attack is $2 \cdot 2^4 \cdot 5 \approx 2^{7.32}$.

Now to find the correct key, we test only for the fact that $RK[0][0] = RK[0][1] \oplus i$ and do not use the fact $RK[0][0] = RK[0][1] \oplus i \oplus z$ as i runs over all 2^4 possible values. Now for each i we need to check 2^{12} keys candidate. and for each check, we need to calculate four s-boxes. So we need to calculate $2^{12} \cdot 2 \cdot 4 \cdot 5 \cdot 2^4 = 2^{21.32}$ s-boxes. Now we assume that one round costs 16 s-box calculation. So the time complexity is equivalent to $\frac{2^{21.32}}{16 \cdot 5}$ = 2^{15} five-rounds of Future.

Through a similar process, we can find out the values of $RK[0][1]$, $RK[0][2]$, and $RK[0][3]$. After that we find $RK[1]$ by exhaustive search and hence the key is recovered.

Complexity analysis

The data complexity of recovering $RK[0][0]$ is $2^{7.32}$. Therefore the total data complexity of recovering the whole $RK[0]$ is $4 \cdot 2^{7.32} = 2^{9.32}$. The time complexity of recovering $RK[0][0]$ is 2^{15}. Therefore the total time

complexity of recovering the whole $RK[0]$ is $4 \cdot 2^{15} = 2^{17}$. The time complexity of recovering the subkey $RK[1]$ is 2^{64}. The overall time complexity of recovering the subkeys $RK[0]$ and $RK[1]$ is dominated by the time complexity of recovering $RK[1]$. Therefore, the overall time complexity of recovering the secret key is dominated by 2^{64}.

4 Yoyo attacks on Future in the known-key setting

This section discusses the Yoyo attack on Future in a known key setting. That is, the attacker knows the secret key. Here we try to show that reduced round of Future (up to eight-round) can not be used as an internal permutation of another cipher.

4.1 Attack on six-round Future

The six-round Future can be written as $R^6 = S_3 \circ L_2 \circ S_2 \circ L_1 \circ S_1$, where $S_1 = S_2 = S_3 = S$ and $L_1 = L_2 = L$. Here we give an impossible differential Yoyo distinguisher for six-round Future and show that using that distinguisher we can distinguish six-round Future from a random permutation.

Let (Q_0, Q_1) be a pair such that $w(\nu_{diag}(Q_0 \oplus Q_1)) = 3$. Take $P_0 = S_1^{-1} \circ L_1^{-1} \circ S_2^{-1}(Q_0)$ and $P_1 = S_1^{-1} \circ L_1^{-1} \circ S_2^{-1}(Q_1)$. Suppose $P_0' = \rho^v(P_0, P_1)$, $P_1' = \rho^v(P_1, P_0)$. Let $Q_0' = S_2 \circ L_1 \circ S_1(P_0')$ and $Q_1' = S_2 \circ L_1 \circ S_1(P_1')$. So we claim that $w(\nu_{diag}(Q_0' \oplus Q_1')) = 3$, since this is four-round Yoyo game in the backward direction. So there exists a diagonal in $Q_0' \oplus Q_1'$ such that at least one nibble is active in that diagonal and other diagonals are inactive. Hence there exists a column in $Q_0' \oplus Q_1'$ such that the exact one nibble is active in that column. So after MC operation, all four nibble of that column is active. Hence after SR all the columns are active. So after L_2 operation, all columns are active. As a result, after S_3 operation, all the diagonals are active. Let $C_0 = S_3 \circ L_2(Q_0')$ and $C_1 = S_3 \circ L_2(Q_1')$. Then $w(\nu_{diag}(C_0 \oplus C_1)) = 0$. Therefore for some pair (Q_0, Q_1) satisfying $w(\nu_{diag}(Q_0 \oplus Q_1)) = 3$ if we get $w(\nu_{diag}(C_0 \oplus C_1)) > 0$ which is impossible for Future, we can conclude that the cipher is not Future. For a random permutation with probability $4.2^{-16} = 2^{-14}$, there exists an inactive diagonal in $C_0 \oplus C_1$. Therefore we first randomly choose 2^{14} pairs Q_0, Q_1 such that $w(\nu_{diag}(Q_0 \oplus Q_1)) = 3$ and get the corresponding 2^{14} pairs C_0, C_1 using the above described method. If the cipher is Future, we get $w(\nu_{diag}(C_0 \oplus C_1)) = 0$ for every pair. Otherwise, we can get a pair with a high probability such that $w(\nu_{diag}(C_0 \oplus C_1)) > 0$. Algorithm 6 describes the six-round distinguish attack in the known key setting.

Complexity analysis

In Algorithm 6 the loop in line 1 iterates 2^{14} times. For each iteration, the encryption function in line 5 is called twice. This means that the encryption function will be called a total of $2 \times 2^{14} = 2^{15}$ times. The data complexity of the attack is the number of times the encryption function is called. In this case, the data complexity is 2^{15}. For each iteration, in line 3 the function $S^{-1} \circ L^{-1} \circ S^{-1}$ called twice. The function $S^{-1} \circ L^{-1} \circ S^{-1}$ is equivalent to four-round Future. Here the encryption function is six-round Future. The time complexity of an attack is the number of operations required to break the cipher. Therefore the time complexity of this attack with respect to six-round Future is $2 \times 2^{14} \times \frac{4}{6} = 2^{14.415}$.

Algorithm 6 Six-round distinguish attack in known key setting

Input: 2^{14} pairs (Q_0, Q_1) such that $w(\nu_{diag}(Q_0 \oplus Q_1)) = 3$

Output: 1 for Future and –1 for not Future

1 **for** x = *0 to* 2^{14} **do**
2 choose Q_0, Q_1 randomly such that $w(\nu_{diag}(Q_0 \oplus Q_1)) = 3$
3 $P_0 = S^{-1} \circ L^{-1} \circ S^{-1}(Q_0)$, $P_1 = S^{-1} \circ L^{-1} \circ S^{-1}(Q_1)$
4 $P_0' = SWAP_{col}(P_0, P_1)$, $P_1' = SWAP_{col}(P_1, P_0)$
5 $C_0 = Enc_6(P_0')$, $C_1 = Enc_6(P_1')$
6 **if** $(w(\nu_{diag}(C_0 \oplus C_1))) \geq 1$ **then**
7 **return**–1
8 **return** 1

4.2 Attack on eight-round Future

The eight-round Future can be written as $R^8 = S_4 \circ L_3 \circ S_3 \circ L_2 \circ S_2 \circ L_1 \circ S_1$, where $S_1 = S_2 = S_3 = S_4 = S$ and $L_1 = L_2 = L_3 = L$. Saha et al. (2018) present an impossible differential bi-directional Yoyo trick to distinguish eight-round AES in the known key setting. This technique is used to distinguish eight-round Future in the known key settings.

Let (Q_0, Q_1) be a pair such that $w(\nu_{diag}(Q_0 \oplus Q_1)) = 3$. Take $P_0 = S_1^{-1} \circ L_1^{-1} \circ S_2^{-1}(Q_0)$ and $P_1 = S_1^{-1} \circ L_1^{-1} \circ S_2^{-1}(Q_1)$. Suppose $P_0' = \rho^v(P_0, P_1)$ $P_1' = \rho^v(P_1, P_0)$. Let $Q_0' = S_2 \circ L_1 \circ S_1(P_0')$ and $Q_1' = S_2 \circ L_1 \circ S_1(P_1')$. So we claim that $w(\nu_{diag}((Q_0' \oplus Q_1'))) = 3$, since this is four-round Yoyo game in the backward direction. So there exists a diagonal in $Q_0' \oplus Q_1'$ such that at least one nibble is active in that diagonal and other diagonals are inactive. So there exists a column in $Q_0' \oplus Q_1'$ such that the exact one nibble is active in that column. So, after the MC operation, all four nibbles in that column are active, and after the SR operation, all columns are active. Hence, after the L_2 operation, all columns are active. Let $R_0 = L_2(Q_0')$ and $R_1 = L_2(Q_1')$. Therefore $w(\nu_{col}(R_0 \oplus R_1)) = 0$. Let $C_0 = S_4 \circ L_3 \circ S_3(R_0)$ and $C_1 = S_4 \circ L_3 \circ S_3(R_1)$.

Let $C_0' = \rho^v(C_0, C_1)$, $C_1' = \rho^v(C_1, C_0)$. Let $R_0' = S_3^{-1} \circ L_3^{-1} \circ S_4^{-1}(C_0')$ and $R_1' = S_3^{-1} \circ L_3^{-1} \circ S_4^{-1}(C_1')$. So we claim that $w(\nu_{col}((R_0' \oplus R_1'))) = 0$ since this is four-round Yoyo game in the forward direction. Therefore there are no inactive columns in $R_0' \oplus R_1'$.

Therefore for some pair (Q_0, Q_1) satisfying $w(\nu_{diag}(Q_0 \oplus Q_1)) = 3$ if we get $w(\nu_{col}((R_0' \oplus R_1'))) > 0$ which is impossible for the cipher Future, we can conclude that the cipher is not Future. Now for a random permutation

with probability $4.2^{-16} = 2^{-14}$, there exists an inactive column in $(R'_0 \oplus R'_1)$. Therefore we first randomly choose 2^{14} pairs (Q_0, Q_1) such that $w(\nu_{diag}(Q_0 \oplus Q_1)) = 3$ and get the corresponding 2^{14} pairs R'_0, R'_1 using the above described method. Now if the cipher is Future, we get $w(\nu_{col}((R'_0 \oplus R'_1))) = 0$ for every pair. If the cipher is not Future, we can get a pair with a high probability such that $w(\nu_{col}((R'_0 \oplus R'_1))) > 0$. Algorithm 7 describes the eight-round distinguish attack in the known key setting.

Algorithm 7 Eight-round distinguish attack in known key setting

Input: 2^{14} pairs (Q_0, Q_1) such that $w(\nu_{diag}(Q_0 \oplus Q_1)) = 3$
Output: 1 for Future and –1 for not Future

1 **for** x = *0 to* 2^{14} **do**
2 choose Q_0, Q_1 randomly such that $w(\nu_{diag}(Q_0 \oplus Q_1)) = 3$
3 $P_0 = S^{-1} \circ L^{-1} \circ S^{-1}(Q_0)$, $P_1 = S^{-1} \circ L^{-1} \circ S^{-1}(Q_1)$
4 $P'_0 = SWAP_{col}(P_0, P_1)$, $P'_1 = SWAP_{col}(P_1, P_0)$
5 $C_0 = Enc_8(P'_0)$, $C_1 = Enc_8(P'_1)$
6 $C'_0 = SWAP_{diag}(C_0, C_1)$, $C'_1 = SWAP_{diag}(C_1, C_0)$
7 $R'_0 = S^{-1} \circ L^{-1} \circ S^{-1}(C'_0)$, $R'_1 = S^{-1} \circ L^{-1} \circ S^{-1}(C'_1)$
8 **if** $(w(\nu_{col}(R'_0 \oplus R'_1)) \geq 1$ **then**
9 **return**–1
10 **return** 1

Complexity analysis

In Algorithm 7 the loop in line 1 iterates 2^{14} times. For each iteration, the encryption function in line 5 is called twice. This means that the encryption function will be called a total of $2 \times 2^{14} = 2^{15}$ times. In this case, the data complexity is 2^{15}. For each iteration, in lines 3 and 7 the function $S^{-1} \circ L^{-1} \circ S^{-1}$ is called four times. The function $S^{-1} \circ L^{-1} \circ S^{-1}$ is equivalent to four-round Future. Here the encryption function is eight round Future. Therefore the time complexity of this attack with respect to eight round Future is $4 \times 2^{14} \times \frac{4}{8} = 2^{15}$.

5 Conclusions

In the security analysis of Future (Gupta et al., 2022), the authors did not mention the Yoyo attack. In this paper, we analysed Future with respect to Yoyo trick in secret key setting and known key setting. We see that in the secret key setting, Future can be distinguished up to five- and six-round with data complexity $2^{9.83}$ and $2^{58.83}$, respectively. We show that the 128-bit secret key of five-round Future can be recovered with time complexity 2^{64}. We further show that for both six and eight rounds, Future can be distinguished in the known key settings with data complexity 2^{15}. Future work in this area could explore the application of the Yoyo attack to other block ciphers. One possible direction for Future work is to develop new methods for defending against the Yoyo attack. This could involve designing new block ciphers that are less susceptible to the Yoyo attack.

Acknowledgements

We thank the anonymous reviewers for the insightful comments, which help to improve the technical as well as the editorial quality of our manuscript. Sandip Kumar Mondal is thankful to the University Grants Commission (UGC). Research of Dr. Avishek Adhikari is partially supported by DST-FIST Project, Government of India, vide sanction order: SR/FST/MS-I/2019/41.

References

Aumasson, J-P. and Meier, W. (2009) *Zero-sum Distinguishers for Reduced Keccak-f and for the Core Functions of Luffa and Hamsi*, NIST Mailing List [online] https://www.aumasson.jp/data/papers/AM09.pdf (accessed 23 January 2023).

Beierle, C., Jean, J., Kölbl, S., Leander, G., Moradi, A., Peyrin, T., Sasaki, Y., Sasdrich, P. and Sim, S.M. (2016) 'The SKINNY family of block ciphers and its low-latency variant MANTIS', in Robshaw, M. and Katz, J. (Eds.): *Advances in Cryptology – CRYPTO 2016 – 36th Annual International Cryptology Conference, Lecture Notes in Computer Science, Proceedings, Part II*, Springer, Santa Barbara, CA, USA, 14–18 August, Vol. 9815, pp.123–153, DOI: 10.1007/978-3-662-53008-5_5.

Biham, E., Biryukov, A., Dunkelman, O., Richardson, E. and Shamir, A. (1998) 'Initial observations on Skipjack: cryptanalysis of Skipjack-3XOR', in Tavares, S.E. and Meijer, H. (Eds.): *Selected Areas in Cryptography '98, SAC'98, Proceedings, Lecture Notes in Computer Science*, Springer, Kingston, Ontario, Canada, 17–18 August, Vol. 1556, pp.362–376, DOI: 10.1007/3-540-48892-8_27.

Biryukov, A., Leurent, G. and Perrin, L. (2016) 'Cryptanalysis of Feistel networks with secret round functions', in Dunkelman, O. and Keliher, L. (Eds.): *Selected Areas in Cryptography – SAC 2015*, Springer International Publishing, Cham, pp.102–121, ISBN: 978-3-319-31301-6.

Bogdanov, A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M.J.B., Seurin, Y. and Vikkelsoe, C. (2007) 'PRESENT: an ultra-lightweight block cipher', in Paillier, P. and Verbauwhede, I. (Eds.): *Cryptographic Hardware and Embedded Systems – CHES 2007, 9th International Workshop, Lecture Notes in Computer Science, Proceedings*, Springer, Vienna, Austria, 10–13 September, Vol. 4727, pp.450–466, DOI: 10.1007/978-3-540-74735-2_31.

Daemen, J. and Rijmen, V. (2002) *The Design of Rijndael: AES – The Advanced Encryption Standard*, Information Security and Cryptography, Springer, ISBN: 3-540-42580-2, DOI: 10.1007/978-3-662-04722-4.

Daemen, J. and Rijmen, V. (2007) 'Plateau characteristics', *IET Inf. Secur.*, Vol. 1, No. 1, pp.11–17, DOI: 10.1049/iet-ifs:20060099.

De Cannière, C., Dunkelman, O. and Knezevic, M. (2009) 'KATAN and KTANTAN – a family of small and efficient hardware-oriented block ciphers', in Clavier, C. and Gaj, K. (Eds.): *Cryptographic Hardware and Embedded Systems – CHES 2009, 11th International Workshop, Lecture Notes in Computer Science, Proceedings*, Springer, Lausanne, Switzerland, 6–9 September, Vol. 5747, pp.272–288, DOI: 10.1007/978-3-642-04138-9_20.

Ghosh, S., Saha, D., Sengupta, A. and Chowdhury, D.R. (2017) 'Preventing fault attacks using fault randomisation with a case study on AES', *International Journal of Applied Cryptography*, Vol. 3, No. 3, pp.225–235, DOI: 10.1504/IJACT.2017.086231.

Guo, J., Peyrin, T., Poschmann, A. and Robshaw, M.J.B. (2011) 'The LED block cipher', in Preneel, B. and Takagi, T. (Eds.): *Cryptographic Hardware and Embedded Systems – CHES 2011 – 13th International Workshop, Lecture Notes in Computer Science, Proceedings*, Springer, Nara, Japan, 28 September–1 October, Vol. 6917, pp.326–341, DOI: 10.1007/978-3-642-23951-9_22.

Gupta, K.C., Pandey, S.K. and Samanta, S. (2022) 'Future: a lightweight block cipher using an optimal diffusion matrix', in Batina, L. and Daemen, J. (Eds.): *Progress in Cryptology – AFRICACRYPT 2022*, Springer Nature, Cham, Switzerland, pp.28–52, ISBN: 978-3-031-17433-9.

Huang, J., Seberry, J. and Susilo, W. (2009) 'A five-round algebraic property of AES and its application to the alpha-MAC', *International Journal of Applied Cryptography*, Vol. 1, No. 4, pp.264–289, DOI: 10.1504/IJACT.2009.028027.

İlter, M.B. and Selçuk, A.A. (2023) 'MILP-aided cryptanalysis of the Future block cipher', in Bella, G., Doinea, M. and Janicke, H. (Eds.): *Innovative Security Solutions for Information Technology and Communications*, Springer Nature, Cham, Switzerland, pp.153–167, ISBN: 978-3-031-32636-3.

Knudsen, L.R. and Rijmen, V. (2007) 'Known-key distinguishers for some block ciphers', in Kurosawa, K. (Ed.): *Advances in Cryptology – ASIACRYPT 2007, 13th International Conference on the Theory and Application of Cryptology and Information Security, Lecture Notes in Computer Science, Proceedings*, Springer, Kuching, Malaysia, 2–6 December, Vol. 4833, pp.315–324, DOI: 10.1007/978-3-540-76900-2_19.

National Institute of Standards and Technology (2007) *SHA-3: Cryptographic Hash Algorithm Competition* [online] https://csrc.nist.gov/projects/hash-functions/sha-3-project (accessed 23 January 2023).

Rønjom, S., Bardeh, N.G. and Helleseth, T. (2017) 'Yoyo tricks with AES', in Takagi, T. and Peyrin, T. (Eds.): *Advances in Cryptology – ASIACRYPT 2017 – 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Lecture Notes in Computer Science, Proceedings, Part I*, Springer, Hong Kong, China, 3–7 December, Vol. 10624, pp.217–243, DOI: 10.1007/978-3-319-70694-8_8.

Saha, D., Rahman, M. and Paul, G. (2018) 'New Yoyo tricks with AES-based permutations', *IACR Trans. Symmetric Cryptol.*, No. 4, pp.102–127, DOI: 10.13154/tosc.v2018.i4.102-127.

Wagner, D. (1999) 'The Boomerang attack', in *Fast Software Encryption, 6th International Workshop, FSE '99, Lecture Notes in Computer Science, Proceedings*, Springer, Rome, Italy, 24–26 March, Vol. 1636, pp.156–170, DOI: 10.1007/3-540-48519-8_12.