Chinese Journal of Electronics
Vol.32, No.2, Mar. 2023

Cryptanalysis of Full-Round Magpie Block Cipher

YANG Yunxiao[1], SUN Bing[1,2,4], and LIU Guoqiang[1,3]

(1. *College of Liberal Arts and Sciences, National University of Defense Technology, Changsha 410073, China*)

(2. *State Key Laboratory of Cryptology, P.O. Box 5159, Beijing 100878, China*)

(3. *State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Science, Beijing 100093, China*)

(4. *Hunan Engineering Research Center of Commercial Cryptography Theory and Technology Innovation, Changsha 410073, China*)

Abstract — Magpie is a lightweight block cipher proposed by Li *et al.* in *Acta Electronica Sinica* volumn 45, issue 10. It adopts an substitution-permutation network (SPN) structure with a block size of 64 bits and the key size of 96 bits, respectively. To achieve the consistency of the encryption and decryption, which is both hardware and software friendly, 16 bits of the key are used as control signals to select S-boxes and another 16 bits of the key are used to determine the order of the operations. As the designers claimed, the security might be improved as different keys generate different ciphers. This paper analyzes the security of Magpie, studies the difference propagation of Magpie, and finally finds that the cipher has a set of 2^{80} weak keys which makes the full-round encryption weak, and corrects the lower bound of the number of active S-boxes to 10 instead of 25 proposed by the designers. In the weak key model, the security of the cipher is reduced by the claimed 2^{80} to only 4×2^{16}.

Key words — Block cipher, Differential cryptanalysis, Weak key, Active S-boxes, Magpie.

I. Introduction

In recent years, the development of automotive systems, smart healthcare, distributed computation, the Internet of things (IoT), etc. have greatly changed our daily life. Those areas mentioned above usually utilize highly constrained devices to interconnect and communicate. While bringing convenience to the public, those devices also bring challenges to data security and personal privacy. Although the conventional cryptographic standards such as AES [1] are secure, they might be no longer suitable to implement in resource-constrained devices owing to the tradeoff made for desktop or server environment.

In 2013, the National Institute of Standards and Technology (NIST) initiated a lightweight cryptography project to evaluate the performance of cryptographic standards on constrained devices and to understand the necessity of dedicated lightweight cryptographic standards. After the necessity is confirmed, NIST published a call for algorithms to be considered for lightweight cryptographic standards. After three rounds of evaluation and public cryptanalysis, NIST published the final list containing 10 lightweight cryptography ciphers on March 19, 2021. During the project, NIST also published two formal reports [2], [3] on the lightweight cryptography, in which the design requirements and the tradeoff between security and resource consumption are clarified. These reports act as significant guidelines for the development of lightweight cryptography and standardized applications.

The design of lightweight block ciphers is an important part of the lightweight cryptography. In many applications, a lightweight block cipher is used not only to encrypt and decrypt data but also to construct other cryptography primitives, such as hash functions, authenticated encryptions, pseudorandom functions and so on.

Usually, there are two ways to design a lightweight block cipher. The first one is to simplify the con-

Manuscript Received June 15, 2021; Accepted Dec. 1, 2021. This work was supported by the National Natural Science Foundation of China (61772545, 61702537, 62002370) and State Key Laboratory of Information Security (2020-MS-02).

© 2023 Chinese Institute of Electronics. DOI:10.23919/cje.2021.00.209

ventional and well-analyzed block ciphers to improve their efficiency. For instance, DESL [4] is a simplified version of DES [5], as the number of S-boxes in a single round is reduced to one in DESL. The second way is to design from scratch. For example, PRESENT [6] is one of the block ciphers optimized for constrained hardware environments. The S-box layer of PRESENT uses gate circuits and the P-layer uses bit-permutation. There are many other block ciphers that utilize the same strategy such as GIFT [7], PRIDE [8], Robin [9], Mysterion [10] and etc. To increase the security, some designers use round functions which are controlled by specific bits of the key. For instance, the S-box layer of PRINTCIPHER [11] is controlled by specific bits of the master key.

Differential cryptanalysis is one of the important methods of evaluating the security of a block cipher. At CRYPTO 1990, Biham and Shamir formally proposed the differential cryptanalysis [12] and achieved breakthrough results against DES and DES-like block ciphers. The idea of differential cryptanalysis was also called the T-method [13] within IBM, but due to technical protection, it was only made public after 1990. Differential cryptanalysis is a kind of chosen plaintext attack that utilizes the plaintext pairs with specific differences to study the statistical properties of differences of the corresponding ciphertext pairs, based on which the keys could be recovered. With the development of the differential cryptanalysis, there are many variants evolved from differential cryptanalysis, such as impossible differential cryptanalysis [14], high-order differential cryptanalysis [15], truncated differential cryptanalysis [16], boomerang attack [17], etc. The essence of these methods is still to study the features of difference propagation during encryption and decryption.

Magpie is an substitution-permutation network (SPN) lightweight block cipher proposed by Li *et al.* in *Acta Electronica Sinica* in 2017 [18]. It uses specific bits of the master key to control the selection and the sequence of the components, which makes the decryption process identical to encryption, provided only the round keys are adjusted. Therefore, the designers claimed that the cipher could be implemented with a smaller area and a high throughput compared with PRESENT. The security against differential cryptanalysis and linear cryptanalysis is guaranteed by wide trail strategy [19] as the designers claim that the number of the active S-boxes of 4-round Magpie is lower bounded by 25, which provides sufficient security margin. However, as will shown in this paper, the designers neglected the impact of different round functions on the characteristics of difference propagation.

In this paper, we analyze the security of Magpie against the differential cryptanalysis in the weak key setting. Depending on the feature that the round functions are different, we find that for certain control signals which are called weak keys in this paper, the linear operations of two consecutive rounds might be canceled. Furthermore, there are 2^{80} weak keys in Magpie. In this case, any input difference cannot achieve full diffusion for full-round Magpie, thus the security is reduced from 2^{80} to 4×2^{16}, which can be conquered easily by a PC in minutes. We also prove that the minimum number of active S-boxes of 4-round Magpie is 10 instead of 25.

The arrangement of this paper is as follows: Section II briefly introduces the Magpie cipher. Section III analyzes the difference propagation of Magpie. Section IV proves the property of Magpie in the weak key model and the minimum number of the active S-boxes of 4-round Magpie is lower bounded by 10. Section V summarizes the main work of this paper.

II. Preliminaries

1. Notation

$\mathbb{F}_2$ — Finite field with two elements;
$\mathbb{F}_{2^n}$ — Finite field with 2^n elements;
$\oplus$ — Exclusive-or;
$P/P[i]$ — Plaintext / the i-th bit of plaintext;
$C/C[i]$ — Ciphertext / the i-th bit of ciphertext;
$K/K[i]$ — The key / the i-th bit of key;
E_0 — Round function controlled by 0;
E_1 — Round function controlled by 1;
$E_{K[i]}$ — Round encryption controlled by $K[i]$;
$\overline{K[i]}$ — The negation of $K[i]$;
$f^n(x)$ — $\underbrace{f \circ f \circ \cdots \circ f}_{n}(x)$.

2. Basic definitions

For a block cipher E whose block size is n bits, denote a pair of plaintext by $(P, P^*) \in \mathbb{F}_2^{n\times 2}$, the input difference is defined as $P \oplus P^* = \alpha \in \mathbb{F}_2^n$. Similarly, denote by (C_i, C_i^*) the outputs of the i-round corresponding to (P, P^*), then $C \oplus C^* = \beta \in \mathbb{F}_2^n$ is defined as the output difference. (α, β) is called an r-round differential of the block cipher E. When $r = 1$, differential (α, β) reveals the characteristics of the round function.

The differential characteristic of an r-round block cipher is denoted as $\Omega = (\beta_0, \beta_1, \ldots, \beta_r)$, which means the input difference is β_0, and the corresponding j-th round difference is $\beta_j (1 \le j \le r)$.

Note that for a given pair (P, P^*), XORing a round key or constant does not change the value of difference since $P \oplus P^* = (P \oplus K) \oplus (P^* \oplus K)$.

3. Round function components of Magpie

The round functions of Magpie are similar to those

of the AES. However, in order to optimize the hardware implementation, Magpie operates on 4-bit nibbles rather than 8-bit bytes in AES. Thus, the state can be represented as a 4×4 matrix over $\mathbb{F}_{2^4}$. Some unnecessary details are omitted in the description of the cipher, and we refer to [18] for details.

SubCells applies 16 4×4 S-boxes to 16 corresponding nibbles. Each of the 16 S-boxes can be either the S-box of PRESENT or its inverse, depending on some specific bits of the key. Since the S-box is bijective, a non-zero input difference of the S-box always produces a non-zero output difference. This operation will simply be denoted as S in the following.

ShiftRows rotates the first row to the left by 3 nibbles, the second row by 2 nibbles, the third row is by 1 nibble, and keeps the fourth row (see Fig.1). In the following, this operation will be denoted by RS and the inverse will be denoted by RS^{-1}. When the control bit is 1, RS is used. Otherwise, we use RS^{-1}.

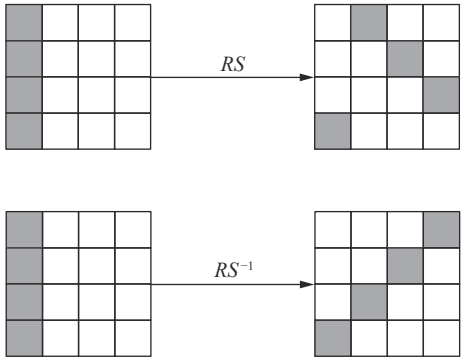

Fig. 1. ShiftRows

MixColumns mixes the state column by column. It multiplies each column by either a 4×4 matrix M over $\mathbb{F}_{2^4}$ or its inverse M^{-1}. we simply use MC to denote this operation and MC^{-1} the inverse (see Fig.2). When the control signal is 1/0, MC/MC^{-1} is performed, respectively.

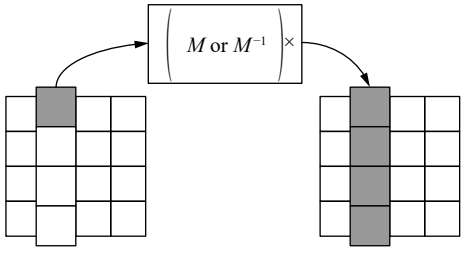

Fig. 2. MixColumns

AddConstants adds a round constant $RC[i]$ to the most significant nibble and the least significant nibble of the state. In the following, this operation will be denoted as RC.

AddRoundKeys adds the round keys to the state, which is denoted by AK in the following.

4. Description of Magpie

Magpie has 32 rounds with a block size of 64 bits and a key size of 96 bits. The 96-bit key of Magpie is divided into 3 different parts. $K[0\ldots63]$ are updated and XORed with the state in each round; $K[64\ldots79]$ are the control bits selecting the S-boxes in SubCells; $K[80\ldots95]$ determine the round functions. Specifically, there are 2 different round functions E_0 and E_1 in Magpie defined as following:

$$E_1(x) \triangleq AK \circ MC \circ RS \circ S \circ AC(x)$$
$$E_0(x) \triangleq AC \circ S \circ RS^{-1} \circ MC^{-1} \circ AK(x)$$

When $K[i+80]=0$, both the $2i$-th and $(2i+1)$-th rounds are E_0. When $K[i+80]=1$, both the $2i$-th and $(2i+1)$-th rounds are E_1.

Accordingly, the encryption of Magpie can be denoted as

$$E_{K[95]} \circ E_{K[95]} \circ \cdots \circ E_{K[81]} \circ E_{K[81]} \circ E_{K[80]} \circ E_{K[80]}(x)$$

Obviously, for a same round key and constant, we always have

$$E_1 \circ E_0(x) = E_0 \circ E_1(x) = x$$

Therefore, the decryption can be computed as

$$E_{\overline{K[80]}} \circ E_{\overline{K[80]}} \circ \cdots \circ E_{\overline{K[94]}} \circ E_{\overline{K[94]}} \circ E_{\overline{K[95]}} \circ E_{\overline{K[95]}}(x)$$

The encryption of Magpie can be described as in Algorithm 1.

Algorithm 1 Encryption of Magpie

Input: P (plaintext), K (key).
Output: C (ciphertext).
$State = P$;
$AK(State, K[0\ldots63])$;
for $i = 0$ to 31 do
if $K[80 + i/2] == 1$ then
$E_1(State, K)$;
$S(K[0\ldots63])$;
end if
if $K[80 + i/2] == 0$ then
$S(K[0\ldots63])$;
$E_0(State, K)$;
end if
end for
$AK(State, K[0\ldots63])$;
$C = State$.

It should be noticed that only 64 bits of the secret key will be updated by SubCells during encryption or decryption, so the 32-bit control signal does not change in the process of encryption, which means the selection

and the sequence of components do not change after the secret key is determined.

III. Difference Propagation in Magpie

In this section, we are going to show some properties of the round function of Magpie.

Property 1 SubCells and ShiftRows are commutative, e.g., for any $x \in \mathbb{F}_{2^4}^{4\times 4}$, we always have:

$$RS \circ S(x) = S \circ RS(x)$$

This property is easy to check as the SubCells and ShiftRows only operate over nibbles and there is no interplay between different nibbles.

Property 2 Let $T = \left\{ \begin{pmatrix} \delta_0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \middle| \delta_0 \in \mathbb{F}_{2^4} \right\}$. For any $x \in \mathbb{F}_{2^4}^{4\times 4}$, let $f_2(x) = E_0 \circ E_1(x)$. Then, for any $x \in \mathbb{F}_{2^4}^{4\times 4}$ and $\delta \in T$, we have

$$f_2(x) \oplus f_2(x \oplus \delta) \in T$$

Proof We prove this property by tracing the difference propagation through $E_0 \circ E_1$.

Firstly, for any non-zero difference δ_0, the difference propagation through E_1 is as follows:

$$\begin{pmatrix} \delta_0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \xrightarrow{AC} \begin{pmatrix} \delta_0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \xrightarrow{S}$$

$$\begin{pmatrix} \delta_1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \xrightarrow{RS} \begin{pmatrix} 0 & \delta_1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \xrightarrow{MC}$$

$$\begin{pmatrix} 0 & \delta_2 & 0 & 0 \\ 0 & \delta_3 & 0 & 0 \\ 0 & \delta_4 & 0 & 0 \\ 0 & \delta_5 & 0 & 0 \end{pmatrix} \xrightarrow{AK} \begin{pmatrix} 0 & \delta_2 & 0 & 0 \\ 0 & \delta_3 & 0 & 0 \\ 0 & \delta_4 & 0 & 0 \\ 0 & \delta_5 & 0 & 0 \end{pmatrix}$$

where δ_1 is a non-zero value corresponding to the input difference δ_0, and

$$M \begin{pmatrix} \delta_1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} \delta_2 \\ \delta_3 \\ \delta_4 \\ \delta_5 \end{pmatrix}, \quad M^{-1} \begin{pmatrix} \delta_2 \\ \delta_3 \\ \delta_4 \\ \delta_4 \end{pmatrix} = \begin{pmatrix} \delta_1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

Therefore, we have the following difference propagation through E_0:

$$\begin{pmatrix} 0 & \delta_2 & 0 & 0 \\ 0 & \delta_3 & 0 & 0 \\ 0 & \delta_4 & 0 & 0 \\ 0 & \delta_5 & 0 & 0 \end{pmatrix} \xrightarrow{AK} \begin{pmatrix} 0 & \delta_2 & 0 & 0 \\ 0 & \delta_3 & 0 & 0 \\ 0 & \delta_4 & 0 & 0 \\ 0 & \delta_5 & 0 & 0 \end{pmatrix} \xrightarrow{MC^{-1}}$$

$$\begin{pmatrix} 0 & \delta_1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \xrightarrow{RS^{-1}} \begin{pmatrix} \delta_1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \xrightarrow{S^{-1}}$$

$$\begin{pmatrix} \delta_6 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \xrightarrow{AK} \begin{pmatrix} \delta_6 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

where δ_6 is a non-zero value corresponding to the input difference δ_1.

Thus, the output difference $f_2(x) \oplus f_2(x \oplus \delta)$ is also an element in T, which ends the proof.

Similarly, we can construct some other T's such that Property 2 holds. In other words, $E_0 \circ E_1(x)$ is equivalent to another substitution $S^*(x)$ nibble by nibble. Notice that although the value $S^*(x)$ might be key-dependent, it keeps the nibbles with non-zero input difference.

Property 3 Let

$$T_0 = \left\{ \begin{pmatrix} \delta_0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \delta_1 \\ 0 & 0 & \delta_2 & 0 \\ 0 & \delta_3 & 0 & 0 \end{pmatrix} \middle| \delta_0, \delta_1, \delta_2, \delta_3 \in \mathbb{F}_{2^4} \right\}$$

and $f_4(x) = E_0 \circ E_0 \circ E_1 \circ E_1(x)$, where $x \in \mathbb{F}_{2^4}^{4\times 4}$. Then, for any $x \in \mathbb{F}_{2^4}^{4\times 4}$, $\delta \in T_0$, we have

$$f_4(x) \oplus f_4(x \oplus \delta) \in T_0$$

Proof We prove this property by tracing the difference propagation through $E_0 \circ (E_0 \circ E_1) \circ E_1$:

Firstly, according to the definition of E_1, the difference propagation through E_1 is as following:

$$\begin{pmatrix} \delta_0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \delta_1 \\ 0 & 0 & \delta_2 & 0 \\ 0 & \delta_3 & 0 & 0 \end{pmatrix} \xrightarrow{AC} \begin{pmatrix} \delta_0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \delta_1 \\ 0 & 0 & \delta_2 & 0 \\ 0 & \delta_3 & 0 & 0 \end{pmatrix} \xrightarrow{S}$$

$$\begin{pmatrix} \delta'_0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \delta'_1 \\ 0 & 0 & \delta'_2 & 0 \\ 0 & \delta'_3 & 0 & 0 \end{pmatrix} \xrightarrow{RS} \begin{pmatrix} 0 & \delta'_0 & 0 & 0 \\ 0 & \delta'_1 & 0 & 0 \\ 0 & \delta'_2 & 0 & 0 \\ 0 & \delta'_3 & 0 & 0 \end{pmatrix} \xrightarrow{MC}$$

$$\begin{pmatrix} 0 & \delta_4 & 0 & 0 \\ 0 & \delta_5 & 0 & 0 \\ 0 & \delta_6 & 0 & 0 \\ 0 & \delta_7 & 0 & 0 \end{pmatrix} \xrightarrow{AK} \begin{pmatrix} 0 & \delta_4 & 0 & 0 \\ 0 & \delta_5 & 0 & 0 \\ 0 & \delta_6 & 0 & 0 \\ 0 & \delta_7 & 0 & 0 \end{pmatrix}$$

where δ'_i is the corresponding output difference of the S-box whose input difference is δ_i.

Then, following Property 2, since it keeps the nibbles with non-zero input difference, the difference propagation through $E_0 \circ E_1$ is

$$\begin{pmatrix} 0 & \delta_4 & 0 & 0 \\ 0 & \delta_5 & 0 & 0 \\ 0 & \delta_6 & 0 & 0 \\ 0 & \delta_7 & 0 & 0 \end{pmatrix} \xrightarrow{E_0 \circ E_1} \begin{pmatrix} 0 & \delta_8 & 0 & 0 \\ 0 & \delta_9 & 0 & 0 \\ 0 & \delta_{10} & 0 & 0 \\ 0 & \delta_{11} & 0 & 0 \end{pmatrix}$$

where $\delta_8, \delta_9, \delta_{10}, \delta_{11} \in \mathbb{F}_{2^4}$.

Finally, according to the definition of E_0, the differential propagation through E_0 is

$$\begin{pmatrix} 0 & \delta_8 & 0 & 0 \\ 0 & \delta_9 & 0 & 0 \\ 0 & \delta_{10} & 0 & 0 \\ 0 & \delta_{11} & 0 & 0 \end{pmatrix} \xrightarrow{AK} \begin{pmatrix} 0 & \delta_8 & 0 & 0 \\ 0 & \delta_9 & 0 & 0 \\ 0 & \delta_{10} & 0 & 0 \\ 0 & \delta_{11} & 0 & 0 \end{pmatrix} \xrightarrow{MC^{-1}}$$

$$\begin{pmatrix} 0 & \delta'_8 & 0 & 0 \\ 0 & \delta'_9 & 0 & 0 \\ 0 & \delta'_{10} & 0 & 0 \\ 0 & \delta'_{11} & 0 & 0 \end{pmatrix} \xrightarrow{RS^{-1}} \begin{pmatrix} \delta'_8 & 0 & 0 & 0 \\ 0 & 0 & 0 & \delta'_9 \\ 0 & 0 & \delta'_{10} & 0 \\ 0 & \delta'_{11} & 0 & 0 \end{pmatrix} \xrightarrow{S^{-1}}$$

$$\begin{pmatrix} \delta_{12} & 0 & 0 & 0 \\ 0 & 0 & 0 & \delta_{13} \\ 0 & 0 & \delta_{14} & 0 \\ 0 & \delta_{15} & 0 & 0 \end{pmatrix} \xrightarrow{AK} \begin{pmatrix} \delta_{12} & 0 & 0 & 0 \\ 0 & 0 & 0 & \delta_{13} \\ 0 & 0 & \delta_{14} & 0 \\ 0 & \delta_{15} & 0 & 0 \end{pmatrix}$$

where $\delta_{12}, \delta_{13}, \delta_{14}, \delta_{15} \in \mathbb{F}_{2^4}$ and this ends the proof.

Moreover, in a similar manner with the proof of Property 3, there are 3 more different sets that have the same property with set T_0. Specifically, they are

$$T_1 = \left\{ \begin{pmatrix} 0 & \delta_0 & 0 & 0 \\ \delta_1 & 0 & 0 & 0 \\ 0 & 0 & 0 & \delta_2 \\ 0 & 0 & \delta_3 & 0 \end{pmatrix} \middle| \, \delta_0, \delta_1, \delta_2, \delta_3 \in \mathbb{F}_{2^4} \right\}$$

$$T_2 = \left\{ \begin{pmatrix} 0 & 0 & \delta_0 & 0 \\ 0 & \delta_1 & 0 & 0 \\ \delta_2 & 0 & 0 & 0 \\ 0 & 0 & 0 & \delta_3 \end{pmatrix} \middle| \, \delta_0, \delta_1, \delta_2, \delta_3 \in \mathbb{F}_{2^4} \right\}$$

$$T_3 = \left\{ \begin{pmatrix} 0 & 0 & 0 & \delta_0 \\ 0 & 0 & \delta_1 & 0 \\ 0 & \delta_2 & 0 & 0 \\ \delta_3 & 0 & 0 & 0 \end{pmatrix} \middle| \, \delta_0, \delta_1, \delta_2, \delta_3 \in \mathbb{F}_{2^4} \right\}$$

IV. Security Analysis of Magpie

In this section, according to the properties given in Section III, we find a set of weak keys which enables the attacker to retrieve the plaintext from the corresponding ciphertext by the dictionary attack. We also re-evaluate the minimum number of active S-boxes and correct the lower bound from 25 to 10.

1. The weak keys of Magpie

Since the encryption and decryption process of Magpie and the selection of primitives are related to the control signals in specific bits of the key, the security analysis must be the key-dependent model.

Theorem 1 Let the 16-bit control signal be (1010101010101010) and the corresponding 32-round Magpie be $f_{32}(x)$. Then for any $x \in \mathbb{F}_{2^4}^{4\times 4}$ and $\delta \in T_i$ $(i = 0, 1, 2, 3)$, we have

$$f_{32}(x) \oplus f_{32}(x \oplus \delta) \in T_i$$

Proof While the control signal is (1010101010101010), $f_{32}(x) = E_0 \circ E_0 \circ E_1 \circ E_1 \cdots E_0 \circ E_0 \circ E_1 \circ E_1(x) \triangleq (E_0 \circ E_0 \circ E_1 \circ E_1)^8(x)$.

Without generality, let $i = 0$ for set T_i. According to Property 3, for any input difference belongs to T_0, we have

$$\begin{pmatrix} \delta_0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \delta_1 \\ 0 & 0 & \delta_2 & 0 \\ 0 & \delta_3 & 0 & 0 \end{pmatrix} \xrightarrow{E_0 \circ E_0 \circ E_1 \circ E_1} \begin{pmatrix} \delta_4 & 0 & 0 & 0 \\ 0 & 0 & 0 & \delta_5 \\ 0 & 0 & \delta_6 & 0 \\ 0 & \delta_7 & 0 & 0 \end{pmatrix}$$

where $\delta_k \in \mathbb{F}_{2^4}$ for $0 \le k \le 7$.

For the same reason, we have

$$\begin{pmatrix} \delta_4 & 0 & 0 & 0 \\ 0 & 0 & 0 & \delta_5 \\ 0 & 0 & \delta_6 & 0 \\ 0 & \delta_7 & 0 & 0 \end{pmatrix} \xrightarrow{E_0 \circ E_0 \circ E_1 \circ E_1} \begin{pmatrix} \delta_8 & 0 & 0 & 0 \\ 0 & 0 & 0 & \delta_9 \\ 0 & 0 & \delta_{10} & 0 \\ 0 & \delta_{11} & 0 & 0 \end{pmatrix}$$

where $\delta_k \in \mathbb{F}_{2^4}$ for $0 \le k \le 11$, that is

$$(E_0 \circ E_0 \circ E_1 \circ E_1)^2(x) \oplus (E_0 \circ E_0 \circ E_1 \circ E_1)^2(x \oplus \delta) \in T_0$$

Therefore, for any positive integer t, we can deduce

$$(E_0 \circ E_0 \circ E_1 \circ E_1)^t(x) \oplus (E_0 \circ E_0 \circ E_1 \circ E_1)^t(x \oplus \delta) \in T_0$$

Since t can be any positive integer, the characteristic of difference propagation can be not only preserved for 32-round Magpie, but for any $4t$-round Magpie with specific control signals.

If the control signal part of a 96-bit key is (1010101010101010), the key is called weak key and there are 2^{80} weak keys in total. By Theorem 1, if a weak key is chosen, 4 nibbles of input difference can only be diffused to the same 4 nibbles after 32-round encryption of Magpie, which is vulnerable to brute force attacks. The attackers should only construct 4 tables with a size of 2^{16} to store all pairs of plaintext and the corresponding ciphertext, and there is no need to recover the master key as the dictionary attack can completely crack Magpie. The rationale of this weak key attack is presented in Theorem 2.

Theorem 2 If a weak key K is chosen, the corresponding 32-round Magpie can be denoted as $f_{32}(x) \triangleq (E_0 \circ E_0 \circ E_1 \circ E_1)^8(x)$. Then for any plaintext P, the corresponding ciphertext can be divided into 4 parts, i.e. $f_{32}(P) = \bigoplus_{i=0}^{3} f_{32}(P_i)$ and $f_{32}(P_i) \in T_i$

for $0 \le i \le 3$, where P and P_i are denoted as follows:

$$P = \begin{pmatrix} p_{0,0} & p_{0,1} & p_{0,2} & p_{0,3} \\ p_{1,0} & p_{1,1} & p_{1,2} & p_{1,3} \\ p_{2,0} & p_{2,1} & p_{2,2} & p_{2,3} \\ p_{3,0} & p_{3,1} & p_{3,2} & p_{3,3} \end{pmatrix}$$

$$P_0 = \begin{pmatrix} p_{0,0} & 0 & 0 & 0 \\ 0 & 0 & 0 & p_{1,3} \\ 0 & 0 & p_{2,2} & 0 \\ 0 & p_{3,1} & 0 & 0 \end{pmatrix}$$

$$P_1 = \begin{pmatrix} 0 & p_{0,1} & 0 & 0 \\ p_{1,0} & 0 & 0 & 0 \\ 0 & 0 & 0 & p_{2,3} \\ 0 & 0 & p_{3,2} & 0 \end{pmatrix}$$

$$P_2 = \begin{pmatrix} 0 & 0 & p_{0,2} & 0 \\ 0 & p_{1,1} & 0 & 0 \\ p_{2,0} & 0 & 0 & 0 \\ 0 & 0 & 0 & p_{3,3} \end{pmatrix}$$

$$P_3 = \begin{pmatrix} 0 & 0 & 0 & p_{0,3} \\ 0 & 0 & p_{1,2} & 0 \\ 0 & p_{2,1} & 0 & 0 \\ p_{3,0} & 0 & 0 & 0 \end{pmatrix}$$

Proof Let the corresponding ciphertext of P be

$$C = \begin{pmatrix} c_{0,0} & c_{0,1} & c_{0,2} & c_{0,3} \\ c_{1,0} & c_{1,1} & c_{1,2} & c_{1,3} \\ c_{2,0} & c_{2,1} & c_{2,2} & c_{2,3} \\ c_{3,0} & c_{3,1} & c_{3,2} & c_{3,3} \end{pmatrix}$$

and the corresponding $C_i \in T_i$. For all $i_0, i_1, i_2, i_3 \in \mathbb{F}_2^4$, we can pre-compute a table $\mathcal{T}$ containing all possible plaintext P and corresponding ciphertext C.

According to Theorem 1, C_i is uniquely determined by P_i and is independent of P_j where $j \neq i$. Thus, the table $\mathcal{T}$ can be divided into 4 sub-tables $\mathcal{T}_0, \mathcal{T}_1, \mathcal{T}_2, \mathcal{T}_3$, where $\mathcal{T}_i$ contains the pairs (P_i, C_i).

Then, for any plaintext $P = P_0 \oplus P_1 \oplus P_2 \oplus P_3$, we find the corresponding ciphertext C_0, C_1, C_2 and C_3 in $\mathcal{T}_0, \mathcal{T}_1, \mathcal{T}_2$ and $\mathcal{T}_3$, respectively. Then, the ciphertext of P is $C = C_0 \oplus C_1 \oplus C_2 \oplus C_3$, i.e. $f_{32}(P) = \bigoplus_{i=0}^{3} f_{32}(P_i)$.

The attack needs 2^{16} pre-computations and 4 tables, each of which is with the size 2^{16}.

2. The minimum number of active S-boxes in 4-round Magpie

The designers shown in [18] that any 4-round Magpie has at least 25 active S-boxes. However, the proof only concerns about properties of one round function and neglects the interplay between different round functions under different control signals. Since AddRoundKey and AddConstants don't change the difference, they are omitted in the expression of round functions for simplicity. Due to the fact M and M^{-1} are MDS matrices, for any non-zero vector $(\alpha_0, \alpha_1, \alpha_2, \alpha_3)^{\mathrm{T}}$, let $M \cdot (\alpha_0, \alpha_1, \alpha_2, \alpha_3)^{\mathrm{T}} = (\alpha_4, \alpha_5, \alpha_6, \alpha_7)^{\mathrm{T}}$, we have

$$\min\left(\#\left\{i \middle| \alpha_i \neq 0\right\}\right) = 5$$

According to the properties in Section III, we can deduce:

Theorem 3 For any non-zero input difference, the number of active S-boxes in 4-round Magpie is lower bounded by 10.

Proof According to the description of Magpie, one signal control two consecutive rounds, so there must be two identical consecutive rounds, i.e. $E_0 \circ E_0(x)$ or $E_1 \circ E_1(x)$ in 4-round Magpie. Besides, there must be no three consecutive rounds where E_0 and E_1 are alternated, i.e. there is no $E_0 \circ E_1 \circ E_0(x)$ or $E_1 \circ E_0 \circ E_1(x)$. Therefore, the expression of 4-round Magpie has 10 different cases in total. Specifically, they are:

$$E_0 \circ E_0 \circ E_0 \circ E_0(x) \quad (1)$$

$$E_1 \circ E_1 \circ E_1 \circ E_1(x) \quad (2)$$

$$E_1 \circ E_0 \circ E_0 \circ E_0(x) \quad (3)$$

$$E_1 \circ E_1 \circ E_0 \circ E_0(x) \quad (4)$$

$$E_1 \circ E_1 \circ E_1 \circ E_0(x) \quad (5)$$

$$E_0 \circ E_1 \circ E_1 \circ E_1(x) \quad (6)$$

$$E_0 \circ E_0 \circ E_1 \circ E_1(x) \quad (7)$$

$$E_0 \circ E_0 \circ E_0 \circ E_1(x) \quad (8)$$

$$E_0 \circ E_1 \circ E_1 \circ E_0(x) \quad (9)$$

$$E_1 \circ E_0 \circ E_0 \circ E_1(x) \quad (10)$$

Case (1) and (2) are the same as the case proved in [18], so there are at least 25 active S-boxes in case (1) and (2). Before studying the other 8 cases, we first evaluate 2-round Magpie.

$E_0 \circ E_1(x)$, according to Property 2, when there is only 1 nibble of input difference is non-zero, the output difference must have only 1 non-zero nibble as linear operations cancel each other. So there are at least 2 active S-boxes.

$E_1 \circ E_0(x)$ can be expanded to $MC \circ RS \circ S \circ S \circ RS^{-1} \circ MC^{-1}(x)$. When there are 4 non-zero nibbles in the input difference and they are placed in the same column, according to the property of MC, there are at least 4 non-zero nibbles in output difference and the pattern is as same as the input difference. Under this

circumstance, the propagation of difference is depicted in Fig.3, there are at least 2 active S-boxes.

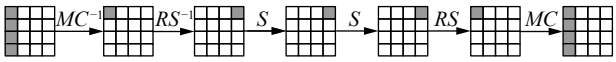

Fig. 3. Difference propagation of $E_1 \circ E_0(x)$.

$E_0 \circ E_0(x)$ can be expanded to $S \circ RS^{-1} \circ MC^{-1} \circ S \circ RS^{-1} \circ MC^{-1}(x)$. When there are 4 non-zero nibbles in the input difference and they are placed in the same column, according to the property of MC, there are at least 4 non-zero nibbles in output difference and they are placed in different columns and different rows. Under this circumstance, the propagation of difference is depicted in Fig.4 , there are at least 5 active S-boxes.

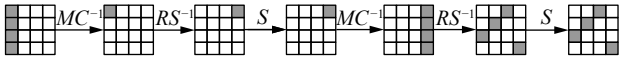

Fig. 4. Difference propagation of $E_0 \circ E_0(x)$.

$E_1 \circ E_1(x)$ can be expanded to $MC \circ RS \circ S \circ MC \circ RS \circ S(x)$. When there are 4 non-zero nibbles in the input difference and they are placed in the same column after RS, according to the property of MC, there are at least 4 non-zero nibbles in output difference and they are placed in the same column. Under this circumstance, the propagation of difference is depicted in Fig.5, there are at least 5 active S-boxes. And it can be verified easily that if there is only 1 nibble of input difference is non-zero, the number of active S-boxes is also 4, but there are 16 non-zero nibbles in output difference.

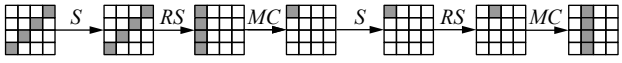

Fig. 5. Difference propagation of $E_1 \circ E_1(x)$.

According to the above analysis about 2-round Magpie, the input difference should meet specific conditions to make the number of active S-boxes minimized.

In cases (3) and (5), the first 2 rounds and the last 2 rounds can not satisfy the conditions make the number of 2-round active S-boxes minimized at the same time. It can be verified easily that the minimum number of active S-boxes for cases (3) and (5) is 25.

In cases (4) and (7), the first 2 rounds and the last 2 rounds can exactly make the number of 2-round active S-boxes minimized at the same time. So the minimum number of active S-boxes is $5 + 5 = 10$.

In cases (6), (8), (9), and (10), the situations are simplified as the $E_0 \circ E_1(x)$ keeps the nibbles with non-zero difference. It can be verified easily that when there is 1 nibble of input difference is non-zero, the minimum number of active S-boxes in cases (6), (8) and (10) is 10. In case (9), when there are 4 non-zero nibbles in the input difference and non-zero nibbles are placed in the same column, the number of active S-boxes is at least 10.

In summary, the number of the active S-boxes in 4-round Magpie is lower bounded by 10. Moreover, case (7) can be expanded to the weak keys in Theorem 1, and the minimum number of active S-boxes for $4t$ rounds is $10t$. For example, let the input difference be

$$\begin{pmatrix} \delta_0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

In case (4), when the number of the active S-boxes reaches the minimum number, the corresponding output difference of $E_0 \circ E_0 \circ E_1 \circ E_1(x)$ must be

$$\begin{pmatrix} \delta_0' & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

And every 4-round encryption is controlled by the same signals according to the weak keys in Theorem 1, so the minimal number of active S-boxes is $10t$ for $4t$-round encryption under the weak keys.

V. Conclusions

In this paper, we analyzed the security of the full-round Magpie block cipher. Firstly, we find the MC and RS in $E_0 \circ E_1(x)$ can be canceled, which makes the 2-round encryption $E_0 \circ E_1(x)$ is actually equivalent to a SubCells. Therefore, it can be deduced that under specific control signals, the 4-round encryption $E_0 \circ E_0 \circ E_1 \circ E_1(x)$ is not sufficiently diffused and the pattern of input difference can be iterated for every 4 rounds.

Then, due to the insufficient diffusion of $E_0 \circ E_0 \circ E_1 \circ E_1(x)$, we find a special 16-bit control signal which makes the full-round Magpie weak. Thus, the number of corresponding weak keys is 2^{80} and the density in the whole key space is only 2^{-16}. Once the weak keys are selected, the cipher can be divided into 4 independent sub-ciphers, which is quite vulnerable to brute force attacks. The security is reduced to 4×2^{16} from the claimed 2^{80} as the attackers. Moreover, according to the difference propagation, we re-evaluate the lower bound of the number of active S-boxes in 4-round encryption and prove that there are at least 10 active S-boxes in 4-round Magpie which is much less than 25 as provided by the designers.

In summary, when designing a block cipher, using part of the secret key as control signals to change the round functions might bring a greater challenge to the cryptanalyst, and the security analysis requires more detailed confirmation by the designer.

References

[1] FIPS-197:2001, The Advanced Encryption Standard (AES), NIST, USA.

[2] K. John, K. Jinkeon, A. Kerry, *et al.*, "Report on lightweight cryptography," *National Institute of Standards and Technology Internal Report*, NISTIR 8114, 2017.

[3] B. Larry, C. Donghoon, K. John, *et al.*, "Status report on the first round of the NIST lightweight cryptography standardization process," *National Institute of Standards and Technology Internal Report*, NISTIR 8268, 2019.

[4] G. Leander, C. Paar, A. Poschmann, *et al.*, "New lightweight DES variants," in *Proceedings of the 14th International Conference on Fast Software Encryption*, Luxembourg, Luxembourg, pp.196–210, 2007.

[5] FIPS-46:1977, Data Encryption Standard, NIST, USA.

[6] A. Bogdanov, L. R. Knudsen, G. Leander, *et al.*, "PRESENT: An ultra-lightweight block cipher," in *Cryptographic Hardware and Embedded Systems – CHES 2007, Lecture Notes in Computer Science (vol.4727)*, Springer, Berlin, Heidelberg, pp.450–466, 2007.

[7] S. Banik, S. K. Pandey, T. Peyrin, *et al.*, "GIFT: A small present," in *Cryptographic Hardware and Embedded Systems – CHES 2017, Lecture Notes in Computer Science (10529)*, Springer, Cham, pp.321–345, 2017.

[8] M. R. Albrecht, B. Driessen, E. B. Kavun, *et al.*, "Block ciphers - Focus on the linear layer (feat. PRIDE)," in *Proceedings of Advances in Cryptology – CRYPTO* 2014, Santa Barbara, California, USA, pp. 57–76, 2014.

[9] A. Journault, F. X. Standaert and K. Varici, "Improving the security and efficiency of block ciphers based on LS-designs," in *Proceedings of Cryptographic Hardware and Embedded Systems – CHES 2017, Lecture Notes in Computer Science (vol.10529)*, Springer, Cham, pp.495–509, 2017.

[10] V. Grosso, G. Leurent, F. X. Standaert, *et al.*, "LS-designs: Bitslice encryption for efficient masked software implementations," in *Fast Software Encryption – FSE 2014, Lecture Notes in Computer Science (vol.8540)*, Springer, Berlin, Heidelberg, pp.18–37,2014.

[11] L. Knudsen, G. Leander, A. Poschmann, *et al.*, "PRINTcipher: A block cipher for IC-printing," in *Cryptographic Hardware and Embedded Systems – CHES 2010, Lecture Notes in Computer Science, (vol.6225)*, Springer, Berlin, Heidelberg, pp.16–32, 2010.

[12] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," *J. Cryptology* , no.4, pp.3–72, 1991.

[13] D. Coppersmith, "The data encryption standard (DES) and its strength against attacks," *IBM Journal of Research and Development*, vol.38, no.3, pp.243–250, 1994.

[14] E. Biham, A. Biryukov, and A. Shamir, "Cryptanalysis of skipjack reduced to 31 rounds using impossible differentials," *Journal of Cryptology* , vol.18, no.4, pp.291–311, 2005.

[15] X. Lai, "Higher order derivatives and differential cryptanalysis," in *Communications and Cryptography, The Springer International Series in Engineering and Computer Science (vol.276)*, Springer, Boston, , pp.227–233, 1994.

[16] L. R. Knudsen, "Truncated and higher order differentials," in *Fast Software Encryption — FSE 1994, Lecture Notes in Computer Science (vol.1008)*, Springer, Berlin, Heidelberg, pp.196–211, 1994.

[17] D. Wagner, "The boomerang attack," in *Fast Software Encryption — FSE 1999, Lecture Notes in Computer Science (vol.1636)*, Springer, Berlin, Heidelberg, pp.156–170, 1999.

[18] L. Li, K. Li, W. He, *et al.*, "Magpie: A high-security lightweight block cipher," *Acta Electronica Sinica*, vol.45, no.10, pp.2521–2527, 2017. (in Chinese)

[19] J. Daemen, V. Rijmen, "The wide trail design strategy," in *Cryptography and Coding – Cryptography and Coding 2001, Lecture Notes in Computer Science (vol.2260)*, Springer, Berlin, Heidelberg, pp.222–238, 2001.

YANG Yunxiao was born in 1996. He is an M.S. candidate of College of Liberal Arts and Sciences, National University of Defense Technology. His research interest is cryptanalysis.
(Email: yyx23@live.com)

SUN Bing (corresponding author) is an Associate Professor in National University of Defense Technology. He received the Ph.D. degree from National University of Defense Technology in 2009. His research interests include the cryptography, especially cryptanalysis of symmetric primitives.
(Email: happy_come@163.com)

LIU Guoqiang is an Associate Professor in National University of Defense Technology. He received the Ph.D. degree from Information Science and Technology Institute in 2015. His current interests include the cryptography, especially cryptanalysis of symmetric primitives.
(Email: liuguoqiang87@hotmail.com)