Improbable Differential Attacks on Reduced FOX64

Chong Zhang[1, a], Zhiyi Qu[2, b], Zhendong Yu[3, c]

[1]School of Information Science & Engineering, Lanzhou University, Lanzhou 730000, China;

[2] School of Information Science & Engineering, Lanzhou University, Lanzhou 730000, China;

[3] School of Information Science & Engineering, Lanzhou University, Lanzhou 730000, China;

[a]116543311@qq.com, [b]quzy@lzu.edu.cn, [c]yuzhd13@lzu.edu.cn

Keywords: FOX cipher, improbable differential attack, Impossible differential attack.

Abstract. FOX is a family of block ciphers designed by Junod and Vaudenay in 2004, which is the result of a joint project with the company MediaCrypt AG in Switzerland. Several attacks on reduced FOX have been proposed. In this paper we present an improbable differential cryptanalysis on the reduced-round FOX. By using this method, we present the attacks on 6, 7, and 8-round FOX64 with the time complexity of 276.92, 2141.27, and 2205.85 respectively.

Introduction

FOX [1], also known as IDEA-NXT, is a family of block ciphers designed by Junod and Vaudenay in 2004. The high level of FOX adopts a modified structure of Lai-Massey Scheme [2], which can be proven to have good pseudorandom properties in the Luby-Rackoff paradigm and decorrelation in hesitance properties. FOX has two version, both have the variable number of rounds which depends on the key size. The first FOX64/k/r has a 64-bit block-size with a variable key length which is a multiple of 8 and up to 256 bits. The second FOX128/k/r uses a 128-bit block-size with the same possible key lengths. The original design suggests these two ciphers should be iterated for 16 rounds. The round function of FOX uses SPS (Substitution-Permutation-Substitution) structure with sub-key addition of those three layers. The key schedule of FOX is very complex, which uses the round function as a compress function to generate sub-keys from the master key.

The designers of FOX have analyzed the security of FOX against differential attacks, linear attacks, integral attacks, statistical attacks, slide attacks, interpolation attacks and algebraic attacks [3]. In 2006, Wu et al. made some improvement of integral attack [4]. For FOX64, the time complexity of their improved integral attack on 4, 5, 6, 7 rounds is $2^{45.4}$, $2^{109.4}$, $2^{173.4}$ and $2^{237.4}$, respectively. Then, Wu et al. proposed the impossible differential attack on reduced FOX [5]. They presented impossible differential attack could break 5, 6, 7 rounds FOX64 with 2^{39} chosen plaintexts and 2^{71}, 2^{135}, 2^{199} one-round encryptions respectively.

As we known, impossible differential cryptanalysis [6] uses the impossible differential shows that a particular difference can't occur for the correct key. Therefore, if these differences are satisfied under a trial key, then it cannot be the correct one. Thus, the correct key can be obtained by eliminating all or most of the wrong keys. Recently, Tezcan [7] proved that it is possible to obtain differentials such that the predicted differences occur less frequently for the correct key. This new cryptanalytic technique is called the improbable differential attack and the impossible differential attack is just a special case of it. The power of this method was shown in [7] by constructing the 15-round improbable differential cryptanalysis of CLEFIA. This was the best known attack on CLEFIA. Moreover, in [8], they presented an improbable differential attacks on PRESNET. In this paper, we find 5-round improbable differentials of FOX and use them to attack 6, 7, and 8-round FOX64.

Description of FOX64

In FOX64/k/r, the number of round r must satisfy $12 \le r \le 255$. The key length is k bits, which is a multiple of 8 and no more than 256 bits. Here we give brief descriptions of FOX64, for more details refer to [1].

Round Function f_{32}. The round function f_{32} consists of three main parts: sigma4 denotes a substitution part; mu4 denotes a diffusion part; and a round key addition part. Let $f_{32} : \{0,1\}^{32} \times \{0,1\}^{64} \to \{0,1\}^{32}$, for a 32-bit input $x \in \{0,1\}^{32}$ and a 64-bit round key $k = k_0 \| k_1$, $f_{32}(x,k) = sigma4(mu4(sigma(x \oplus k_0)) \oplus k_1) \oplus k_0$.

The substitution transformation sigma4: $\{0,1\}^{32} \to \{0,1\}^{32}$ consists of 4 parallel applications of a non-linear bijective s-box. The linear bijection mu4: $[GF(256)]^4 \to [GF(256)]^4$ considers an input (x_0, x_1, x_2, x_3) as a vector $(x_0, x_1, x_2, x_3)^T$ over $[GF(256)]^4$ and multiple it with a MDS matrix to output vector with the same size. The branch number of the MDS matrix is 5. The MDS matrix is defined as follows:

$$\begin{pmatrix} 1 & 1 & \beta & \alpha \\ 1 & \beta & \alpha & 1 \\ \beta & \alpha & 1 & 1 \\ \alpha & 1 & \beta & 1 \end{pmatrix}$$

Where $\beta = \alpha^{-1} \oplus 1$, α is a root of the irreducible polynomial $m(x) = x^8 \oplus x^7 \oplus x^6 \oplus x^5 \oplus x^4 \oplus x^3 \oplus 1$.

Encryption and Decryption of FOX64. FOX64 is 15-times iteration of round transformation Imor64, followed by the applications of last round transformation called Imid64.

The round transformation Imor64 is defined as

$$(y_L \| y_R) = or(x_L \oplus f_{32}(x_L \oplus x_R, k)) \| (y_R \oplus f_{32}(x_L \oplus x_R, k)),$$

where $x_L \| x_R$ and $y_L \| y_R$ represent the input and output of Imor64, respectively, k is the round key, $or(a,b) = (b, a \oplus b)$ is a linear orthomorphism. The Imid64 function is a slightly modified version of Imor64, namely the orthomorphism or is replaced by the identity transformation. Moreover, for the *Imid64* transformation, bit-wise exclusive OR the two parts of an input is obviously equal to bit-wise exclusive OR the two parts of output.

The encrypted result by FOX64 for a 64-bit plaintext P is defined as

$$C = Imid64(Imor64(\ldots(Imor64(P, k_1), \cdots, k_2), k_r),$$

where $k_1, k_2, \cdots k_r$, are round sub-keys.

Improbable Differential Attack

The improbable differential cryptanalysis was proposed by Tezcan [7]. The attack aims to find a differential with an α input difference and an β output difference so that these differences are observed with probability $p_{c,k}$ for the correct key and with probability $p_{w,k}$ for a wrong key, where $p_{c,k} < p_{w,k}$. One way of obtaining such differences is to find nontrivial differentials that have α input difference and an output difference other than β, or vice versa.

Since $p_{c,k}$ is less than $p_{w,k}$, improbable differential aims to use N plaintext pairs and count the hits that every guessed sub-key gets and expect that the counter for the correct sub-key to be less than a threshold T. Number of hits a wrong sub-key gets can be seen as a random variable of a binomial distribution with parameters N, $p_{c,k}$ (and a random variable of a binomial distribution with parameters N, $p_{w,k}$ for the correct sub-key). The non-detection error probability p_{nd} denotes the probability of the counter for the correct sub-key to be higher than T. And the false alarm error

probability p_{fa} denotes the probability of the counter for a random wrong sub-key to be no more than T. Therefore, the success probability of an improbable differential attack is $1-p_{nd}$. Here, we first present the following lemma 1 which will be used to estimate $S_{N,P_{c,k}}$ and $S_{N,P_{w,k}}$, respectively.

Lemma 1 [7] let $p_{c,k}$ and $p_{w,k}$ be two real numbers such that $0<p_{c,k}<p_{w,k}<1$ and let τ such that $p_{c,k}<\tau<p_{w,k}$. Let $S_{N,P_{c,k}}$, $S_{N,P_{w,k}}$ follow a binomial law of respective parameters $(N,p_{c,k})$, $(N,p_{w,k})$. Then as $N\to\infty$

$$P(S_{N,P_{c,k}}<\tau N)\approx\frac{(1-p_{c,k})\sqrt{\tau}}{(\tau-p_{c,k})\sqrt{2\pi N(1-\tau)}}e^{-ND(\tau\|p_{c,k})};\quad P(S_{N,P_{w,k}}\geq\tau N)\approx\frac{p_{w,k}\sqrt{1-\tau}}{(p_{w,k}-\tau)\sqrt{2\pi N\tau}}e^{-ND(\tau\|p_{w,k})},$$

where $D(\tau\|p)=\tau\ln(\tau/p)+(1-\tau)\ln[(1-\tau)/(1-p)]$.

Then, the number of required samples N can be obtained from the Algorithm 1.

Algorithm 1: the number of required samples N [7].

Input. $p_{c,k}$, $p_{w,k}$, p_{nd}, p_{fa}. Output: N, τ;

Let $\tau_{\min}=p_{c,k}$, $\tau_{\max}=p_{w,k}$;

Repeat

$\tau=\frac{\tau_{\min}+\tau_{\max}}{2}$;

Compute N_{nd} such that $\forall N>N_{nd}$, $P(S_{N,P_{c,k}}<\tau N)\leq p_{nd}$;

Compute N_{fa} such that $\forall N>N_{fa}$, $P(S_{N,P_{w,k}}\geq\tau N)\leq p_{fa}$;

If $N_{nd}>N_{fa}$, then $\tau_{\min}=\tau$; Else $\tau_{\max}=\tau$;

Until $N_{nd}=N_{fa}$;

Let $N=N_{nd}$; Return N, τ;

Since $p_{nd}=1-p_S$, where p_S is the successful probability of improbable differential attack. Thus, if $p_{nd}=0.5$, the successful probability is $p_S=50\%$; $p_{nd}=0.01$ means the successful probability is $p_S=99\%$. And the N_{nd} and N_{fa} can be calculated by a dichotomic search, which means that the time complexity of Algorithm 1 is $\log(2N)$.

Improbable Differentials of 5-round FOX

In this section, by using the properties of s-box and permutation P in FOX64, we will present 5-round improbable differentials.

Lemma 2 [1] The orthomorphism $or(x,y)=(y,x\oplus y)$ and its inverse mapping $io(x,y)=(x\oplus y,x)$ has the following properties: $or^2(x,y)=io(x,y)$, $io^2(x,y)=or(x,y)$;

Lemma 3 For the s-box of FOX, the average value of the same input difference corresponding to the same output difference is $p=\sum_{\alpha}\{\sum_{\beta}\Pr^2(s(x)\oplus s(x\oplus\alpha)=\beta)\}/2^8\approx 2^{-6.08}$.

Proof. Given the input difference α, the probability of the same input difference corresponding to the same output difference is

$$\begin{aligned}\Pr[s(x)\oplus s(x\oplus\alpha)=s(y)\oplus s(y\oplus\alpha)]&=\sum_{\beta}\Pr[s(x)\oplus s(x\oplus\alpha)=\beta,s(y)\oplus s(y\oplus\alpha)=\beta]\\&=\sum_{\beta}\Pr^2[s(x)\oplus s(x\oplus\alpha)=\beta]\end{aligned}$$

Hence, the average value of the same input difference corresponding to the same output difference is $p=\sum_{\alpha}\{\sum_{\beta}\Pr^2(s(x)\oplus s(x\oplus\alpha)=\beta)\}/2^8$, observing the difference distribution table of s-box, we get $p\approx 2^{-6.08}$.

Lemma 4 For the F-function of FOX, the probability of the following types of differential characteristic is

$p\approx 2^{-6.08}:(b00b)\to(*0**);(0bb0)\to(0***);(00bb)\to(**0*);(0b0b)\to(***0)$. Where $*$ denotes any possible value of $\{0,1\}^8$.

Proof. The F-function of FOX is SPS structure. If the input difference of F-function is $(b00b)$, by lemma 3, the probability for the output difference $(c00c)$ of the first layer S-box is $p\approx 2^{-6.08}$. Go through the P transform, we get the output difference

$$\begin{pmatrix} c\oplus\alpha c \\ 0 \\ c\oplus zc \\ c\oplus\alpha c \end{pmatrix}=\begin{pmatrix} 1 & 1 & 1 & \alpha \\ 1 & z & \alpha & 1 \\ z & \alpha & 1 & 1 \\ \alpha & 1 & z & 1 \end{pmatrix}\begin{pmatrix} c \\ 0 \\ 0 \\ c \end{pmatrix}$$

Hence the output difference of the second layer S-box is $(\gamma_1 0\gamma_2\gamma_3)$, where γ_1, γ_2 and γ_3 are any value of $\{0,1\}^8$. Hence, $pr[(b00b)\to(*0**)]\approx 2^{-6.08}$. In the same way, we can prove the remaining 3 kinds of differential characteristic.

Using the Lemma 4, we can obtain the following types of 5-round improbable differential of FOX64.

Theorem 1 For 5-round FOX64 (the last round without or transform), all the following types of improbable differential are with probability $p\approx 2^{-6.08}$, where $a\neq 0$, $b\neq 0$:

$$(00a0,00a0)/(000a,000a)/(a0a0,a0a0)\to(bbb0,bbb0);$$
$$(00a0,00a0)/(000a,000a)/(0a0a,0a0a)\to(bb0b,bb0b);$$
$$(00a0,00a0)/(0a00,0a00)/(a0a0,a0a0)\to(b0bb,b0bb);$$
$$(00a0,00a0)/(0a00,0a00)/(0a0a,0a0a)\to(0bbb,0bbb);$$

Where / denotes different input differences with the same output difference takes on the same improbable differential probability.

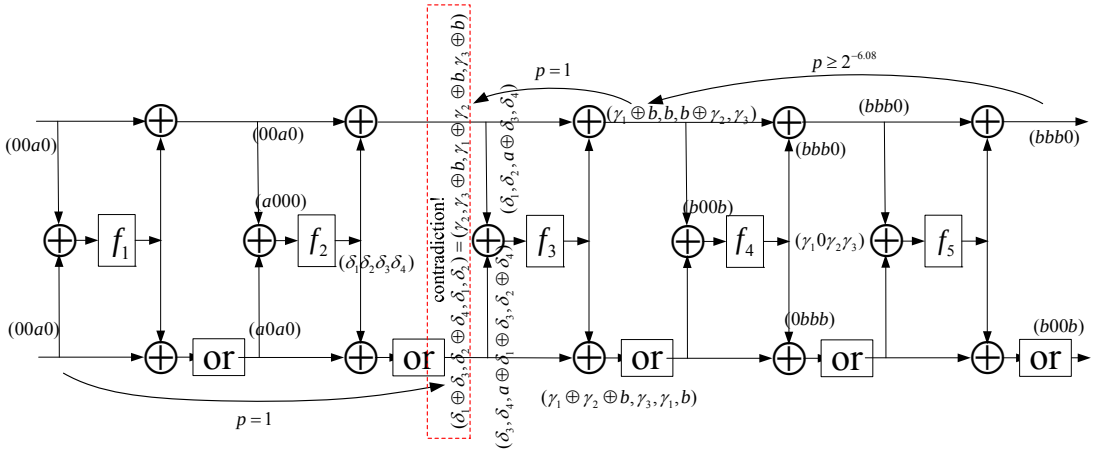

Fig. 1 The 5-round improbable differential of FOX64

Proof. (See as Fig. 1) If the input difference is $(00a0,00a0)$, then the input difference for the second round transform is $(\Delta L_1,\Delta R_1)=(a0a0,00a0)$. By lemma 2, $(a000)$ is the input difference of f_2. Suppose the output of f_2 is $\beta=(\delta_1,\delta_2,\delta_3,\delta_4)$, since the branch number of mu4 is 5, namely $\delta_i\neq 0\quad(1\le i\le 4)$. Hence the input of the third round transform is $(\Delta L_2,\Delta R_2)=((\delta_3,\delta_4,a\oplus\delta_1\oplus\delta_3,\delta_2\oplus\delta_4),(\delta_1,\delta_2,a\oplus\delta_3,\delta_4))$, so $\Delta L_2\oplus\Delta R_2=(\delta_1\oplus\delta_3,\delta_2\oplus\delta_4,\delta_1,\delta_2)$

(Eq.1). From the decryption direction, if the output difference of the 5-round transform is $(\Delta L_5, \Delta R_5) = (bbb0, bbb0)$, denote the output difference of f_5 as Δa , then $(\Delta L_4, \Delta R_4) = (bbb0 \oplus \Delta a, bbb0 \oplus \Delta a)$, namely $\Delta a = 0$. The input difference of f_4 is $(b00b)$. By lemma 4, the probability satisfying the output difference $(\gamma_1 0 \gamma_2 \gamma_3)$ of f_4 is $p \approx 2^{-6.08}$. Then $\Delta L_3 = (\gamma_1, b, b \oplus \gamma_2, b \oplus \gamma_3)$, $\Delta R_3 = (b \oplus \gamma_1, b, b \oplus \gamma_2, \gamma_3)$.

Therefore $\Delta L_2 \oplus \Delta R_2 = io(\Delta L_3) \oplus \Delta R_3 = (\gamma_2, \gamma_3 \oplus b, \gamma_1 \oplus \gamma_2 \oplus b, \gamma_3 \oplus b)$ (Eq.2). The second and fourth element of vector $(\gamma_2, \gamma_3 \oplus b, \gamma_1 \oplus \gamma_2 \oplus b, \gamma_3 \oplus b)$ both are $\gamma_3 \oplus b$. However, in Eq.1, the second and fourth element of vector $(\delta_1 \oplus \delta_3, \delta_2 \oplus \delta_4, \delta_1, \delta_2)$ are $\delta_2 \oplus \delta_4$ and δ_2 respectively. Since $\delta_4 \neq 0$, $\delta_2 \oplus \delta_4 \neq \delta_2$. $(\delta_1 \oplus \delta_3, \delta_2 \oplus \delta_4, \delta_1, \delta_2) \neq (\gamma_2, \gamma_3 \oplus b, \gamma_1 \oplus \gamma_2 \oplus b, \gamma_3 \oplus b)$, this is a contradiction.

Thus $(00a0, 00a0) \rightarrow (bbb0, bbb0)$ is the probable impossible differential of 5-round FOX64 with probability $p \approx 2^{-6.08}$ .Also, we can prove the remaining results with the same method.

By Theorem 1, if the input is $(00a0, 00a0)$, four kinds of output $(bbb0, bbb0)$, $(bb0b, bb0b)$, $(b0bb, b0bb)$, $(0bbb, 0bbb)$ are all improbable differential of 5-round FOX64 with probability $p \approx 2^{-6.08}$.

Improbable Differential Attacks on FOX64

Improbable Differential Attacks on 6-round FOX64. We put one additional round on the plaintext side of the 5-round improbable differentials to attack 6 rounds of FOX64 and recover first round sub-key $RK^1_{(64)}$ (see Fig. 2).

Data collection phase. Choose 2^n structure of $2^{40} - 2^{32}$ plaintexts each $(x_1, x_2, x_3, x_4, x_5, x_2 \oplus c_1, x_1 \oplus x_3 \oplus x_5 \oplus c_2, x_4 \oplus c_3)$, where x_1, x_2, x_3, x_4, x_5 take all possible value but $x_1 \oplus x_5 \neq 0$ and c_1, c_2, c_3 are constant. Such a structure of plaintexts can propose $(2^{40} - 2^{32})^2 / 2 \approx 2^{79}$ plaintext pairs. And each pair has the form $(x_1, x_2, x_3, x_4, x_5, x_2, x_1 \oplus x_3 \oplus x_5, x_4)$. Choosing only the ciphertexts pairs which have the following forms: $(bbb0, bbb0)$, $(bb0b, bb0b)$, $(b0bb, b0bb)$, $(0bbb, 0bbb)$. Therefore there are $2^N \times 2^{79} \times 4 \times (2^8 \times 2^{-64}) = 2^{N+25}$ pairs left after this phase.

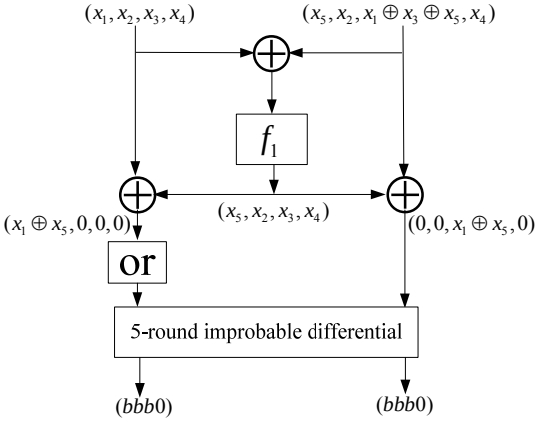

Fig. 2. Improbable differential attack on 6-round FOX64

Key recovery phase. For each remaining pair, when the output difference of f_1 in the first round is (x_5, x_2, x_3, x_4) , the input difference of the second round must be $(0, 0, x_1 \oplus x_5, 0, 0, 0, x_1 \oplus x_5, 0)$, which satisfies the input form of 5-round improbable differential in the Theorem 1.

Step 1: For the subkey $RK^1_{(64)} = RK^1_{0(32)} \| RK^1_{1(32)}$ of the first round, we guess each $RK^1_{0(32)}$ and let $i = 1$, proceed the following steps:

Step 1.1: For the i-th pair plaintext, we can calculate $mu4(sigma4(x \oplus RK^1_{0(32)}))$ for each plaintext. According to the condition on $f_1(x, RK^1_{(64)}) = sigma4(mu4(sigma4(x \oplus RK^1_{0(32)})) \oplus RK^1_{1(32)}) \oplus RK^1_{0(32)}$, we can obtain the differential characteristic $b \to \beta = (x_5, x_2, x_3, x_4)$ of the second $sigma4$.

Step 1.2 According to the differential characteristic $b \to \beta = (x_5, x_2, x_3, x_4)$ of the second $sigma4$, looking up inout-ouput difference table of each S-box to find the inputs. Moreover we have calculated $mu4(sigma4(x \oplus RK^1_{0(32)}))$ for each plaintext, thus we can get $RK^1_{1(32)}$. Then, we keep counters to $RK^1_{1(32)}$ for every guess of $RK^1_{0(32)}$ and increase the corresponding counter when the improbable differential is obtained with a guessed key. According to the Algorithm 1, we can obtain the number of required samples N and the threshold T. Thus, if the counter is less than T, it maybe the correct key. Otherwise, if the counter is more than or equal to T, we remove the wrong key $RK^1_{1(32)}$.

Steps 1.3 If all of the possible $RK^1_{1(32)}$ are removing, it means that $RK^1_{0(32)}$ is a wrong key. Then return to Step1 and check the next $RK^1_{0(32)}$. Otherwise, if all of the remaining plaintext pairs have been passed the checking, go to step 2, else increase i and go to Step1.1.

Step 2 Output the candidate round key $RK^1_{(64)} = RK^1_{0(32)} \,||\, RK^1_{1(32)}$.

The probability of satisfying the improbable differential for a wrong key is $p_{w,k} = 2^{-32}$. Therefore the probability of obtaining the improbable differential for a correct key is $p_{c,k} = 2^{-32} \times (1 - 2^{-6.08}) \approx 2^{-32.02}$. During the attack we try to obtain the 64-bit round key $RK^1_{(64)} = RK^1_{0(32)} \,||\, RK^1_{1(32)}$ and for the correct key to get the least number of hits, false alarm probability must be less than 2^{-64}. Feeding the Algorithm 1 with $p_{w,k}$, $p_{c,k}$, $p_{fa} = 2^{-65}$ and $p_{nd} = 0.01$ shows that when the threshold T is $46988 < 2^{16}$, $N_\infty \approx 2^{47.52}$ pairs are needed for the correct key to remain below the threshold and all of the wrong ones to remain above it with a success probability of 99%.

Attack complexity. For $N_\infty \approx 2^{47.52}$, we need $2^{22.52}$ structures such that $2^{N+25} = 2^{47.52}$, hence the data complexity is $2^{40} \times 2^{22.52} = 2^{62.52}$. Moreover for every guess of $RK^1_{0(32)}$, we perform $2^{47.52}$ F-function computations which are $2^{32} \times 2^{47.52} \times 1/6 \approx 2^{76.92}$ encryptions. So the time complexity is $2^{76.92}$.

Improbable Differential Attacks on 7, 8-round FOX64

We expand our 6-round attack by one round on the ciphertext side to break 7-round FOX64. During the attack, we guess the 64-bit sub-key $RK^7_{(64)}$.

Data collection phase. Choose the same form plaintexts as the 6-round attack and obtain all the ciphertexts. Then guess the 64-bit sub-key $RK^7_{(64)}$ to recover the output of the sixth round transformation. Choose only the output difference $(bbb0, bbb0)$, $(bb0b, bb0b)$, $(b0bb, b0bb)$, $(0bbb, 0bbb)$ of the sixth round transformation. Therefore there are $2^N \times 2^{79} \times 4 \times (2^8 \times 2^{-64}) = 2^{N+25}$ pairs remaining.

Key recovery phase. During the attack we need guess the left 32-bit of $RK^1_{(64)}$ and 64-bit of $RK^7_{(64)}$. Thus the probability of satisfying the improbable differential for a wrong key is also $p_{w,k} = 2^{-32}$. Therefore, the probability of obtaining the improbable differential for a correct key is $p_{c,k} = 2^{-32} \times (1 - 2^{-6.08}) \approx 2^{-32.02}$. Hence, feeding the Algorithm 1 with $p_{w,k}$, $p_{c,k}$ $p_{fa} = 2^{-129}$ and $p_{nd} = 0.01$ shows that when the threshold T is $84696 < 2^{17}$, $N_\infty \approx 2^{48.37}$

pairs are required for the correct key to remain below the threshold and all of the wrong ones to remain above it with a success probability of 99%.

Attack complexity. For $N_\infty \approx 2^{48.37}$, we need $2^{23.37}$ structures such that $2^{N+25} = 2^{48.37}$, thus the data complexity is $2^{40} \times 2^{23.37} = 2^{63.37}$. Moreover, for every guess of $RK^1_{0(32)}$ and $RK^7_{(64)}$, we perform $2^{48.37}$ F-function computations which is $2^{48.37} \times 2^{64} \times 2^{32} \times 1/7 \approx 2^{141.27}$ encryptions. So the time complexity is $2^{141.27}$.

We expand our 7-round attack by one round on the ciphertext side to break 8-round FOX64. We need guess the left 32-bit of $RK^1_{(64)}$ and 128-bit of $RK^7_{(64)}$ and $RK^8_{(64)}$. For the input $p_{w,k} = 2^{-32}$, $p_{c,k} = 2^{-32.02}$, $p_{fa} = 2^{-193}$, and $p_{nd} = 0.01$, Algorithm 1 produces the outputs $T = 118129 < 2^{17}$, $N_\infty \approx 2^{48.85}$. Hence the data complexity and time complexity are $2^{40} \times 2^{23.85} = 2^{63.85}$ and $2^{48.85} \times 2^{128} \times 2^{32} \times 1/8 \approx 2^{205.85}$ respectively.

Conclusion

In this paper, we find 5-round improbable differentials and use them to attack 6, 7 and 8-round FOX64. To the best of our knowledge, these are the best cryptanalytic results on FOX up to this date. For 6-round FOX64, the data complexity increases from 2^{56} to $2^{62.52}$, but the time complexity decreases from 2^{133} to $2^{76.92}$. For 7-round FOX64, the data complexity increases from 2^{39} to $2^{63.37}$, but the time complexity decreases from 2^{197} to $2^{141.27}$. Moreover, this is the first paper pointing out 8-round FOX64 is vulnerable against the statistical attack. Hence in order to provide security against improbable attacks, block designers should ensure that their designs contain no good improbable differentials. Although, we have broken the 8-round FOX64, the full-round is still safe now, the original design suggests FOX64 cipher should be iterated for 16 rounds.

Reference

[1] P.Junod and S. Vaudenay, "FOX: a new Family of Block Ciphers," Selected Areas in Cryptography-SAC 2004, LNCS 2595, pp.131-146, Springer-Verlag.

[2] S.Vaudenay, "On the Lai-Massey scheme," Advances in Cryptology-ASIACRYPT'99, LNCS 1716, pp.8-19,Springer-Verlag.

[3] Nakahara. An analysis of FOX. Information and Computer System Security, 2008.

[4]Wenling Wu, Wentao Zhang and Dengguo Feng. Integral Cryptanalysis of Reduced FOX Block Cipher. Information Security and Cryptology - ICISC 2005, LNCS 3935, pp. 229-241, Springer-Verlag, 2006.

[5] Zhongming Wu et.al. Impossible Differential Cryptanalysis of FOX. Proceedings of the first International Conference: December 17-19, 2009, Beijing China. Springer-Verglag, LNCS. 2010, 6163: 236-249.

[6]Biham, E., Shamir, A. Miss in the middle attacks on IDEA and Khufu[C]. FSE 1999, LNCS, vol. 1636, pp. 124-138. Springer-Verlag (1999).

[7]Cihangir Tezcan. The improbable Differential attack: Cryptanalysis of reduced round CLEFIA. INDOCRYPT 2010. LNCS, vol. 6498, pp. 197-209.

[8]Celine Blondeau and Benoit Gerard. On the data complexity of statistical attacks against block ciphers. Workshop on Coding and Cryptography – WCC 2009, pp.469-488.