SCIENCE CHINA
Information Sciences

• **Supplementary File** •

Improved Nonlinear Invariant Attack

Haipeng Tong[1], Xuan Shen[2], Chao Li[1*] & Yunwen Liu[1]

[1]*College of Liberal and Sciences, National University of Defense Technology, Changsha 410073, China;*
[2]*College of Information and Communication, National University of Defense Technology, Wuhan 430010, China*

Appendix A

Table A1 Distribution of Q-equivalence classes, column 1 gives different affine equivalence classes, columns 2 to 5 give the number of Q-equivalence classes of different category

Representatives of affine equivalent class	$D_S = \{4\}$	$D_S = \{2,4\}$	$D_S = \{3,4\}$	$D_S = \{2,3,4\}$
0,1,2,13,4,7,15,6,8,11,12,9,3,14,10,5(G_0)	2688	4	13290	4178
0,1,2,13,4,7,15,6,8,11,14,3,5,9,10,12(G_1)	2688	2	13324	4146
0,1,2,13,4,7,15,6,8,11,14,3,10,12,5,9(G_2)	2688	5	13294	4173
0,1,2,13,4,7,15,6,8,12,5,3,10,14,11,9(G_3)	0	172	16048	3940
0,1,2,13,4,7,15,6,8,12,9,11,10,14,5,3(G_4)	2688	2	13372	4098
0,1,2,13,4,7,15,6,8,12,11,9,10,14,3,5(G_5)	2688	1	13350	4121
0,1,2,13,4,7,15,6,8,12,11,9,10,14,5,3(G_6)	0	224	15928	4008
0,1,2,13,4,7,15,6,8,12,14,11,10,9,3,5(G_7)	2688	2	13472	3998
0,1,2,13,4,7,15,6,8,14,9,5,10,11,3,12(G_8)	2688	5	13258	4209
0,1,2,13,4,7,15,6,8,14,11,3,5,9,10,12(G_9)	0	224	15842	4094
0,1,2,13,4,7,15,6,8,14,11,5,10,9,3,12(G_{10})	0	242	15822	4096
0,1,2,13,4,7,15,6,8,14,11,10,5,9,12,3(G_{11})	0	242	15924	3994
0,1,2,13,4,7,15,6,8,14,11,10,9,3,12,5(G_{12})	0	262	15808	4090
0,1,2,13,4,7,15,6,8,14,12,9,5,11,10,3(G_{13})	2688	0	13558	3914
0,1,2,13,4,7,15,6,8,14,12,11,3,9,5,10(G_{14})	0	216	15996	3948
0,1,2,13,4,7,15,6,8,14,12,11,9,3,10,5(G_{15})	0	234	15998	3928

Table A2 Representative and the total number of Q-equivalence classes

Category with D_S	Total number of Q-equivalence classes	Representative
$D_S = \{4\}$	21504	0,11,5,9,3,13,12,6,1,15,2,10,14,7,4,8
$D_S = \{2,4\}$	1837	0,3,9,5,7,13,12,14,1,11,6,2,10,15,8,4
$D_S = \{3,4\}$	234284	0,8,4,11,2,14,15,6,1,13,3,9,12,7,5,10
$D_S = \{2,3,4\}$	64935	0,10,4,9,2,12,13,6,1,15,3,11,14,7,5,8

Appendix B

Lemma 1 ([1]). There is an SPN cipher whose round function follows the construction used in LS-designs, and its linear layer can be represented as an orthogonal binary matrix. Assuming that there is a quadratic nonlinear invariant g_S for the

* Corresponding author (email: academic_lc@163.com)

Table A3 The basis of nonlinear invariants of $Q^{-1}S(Q(x)) \oplus c$, where S is the 5-bit S-box of FIDES-80

$g_0(x)$	$x[4] \oplus x[2] \oplus (x[1] \wedge x[4]) \oplus (x[0] \wedge x[3]) \oplus (x[0] \wedge x[1])$
$g_1(x)$	$x[4] \oplus (x[3] \wedge x[4]) \oplus x[2] \oplus (x[2] \wedge x[3]) \oplus (x[1] \wedge x[4]) \oplus (x[1] \wedge x[3] \wedge x[4]) \oplus (x[1] \wedge x[2]) \oplus (x[1] \wedge x[2] \wedge x[3]) \oplus x[0] \oplus (x[0] \wedge x[3] \wedge x[4]) \oplus (x[0] \wedge x[2]) \oplus (x[0] \wedge x[2] \wedge x[3]) \oplus (x[0] \wedge x[1]) \oplus (x[0] \wedge x[1]) \oplus (x[0] \wedge x[1] \wedge x[4])$
$g_2(x)$	$x[3] \oplus x[2] \oplus (x[2] \wedge x[3]) \oplus (x[1] \wedge x[2] \wedge x[4]) \oplus (x[1] \wedge x[2] \wedge x[3] \wedge x[4]) \oplus (x[0] \wedge x[3] \wedge x[4]) \oplus (x[0] \wedge x[2]) \oplus (x[0] \wedge x[2] \wedge x[3]) \oplus (x[0] \wedge x[1] \wedge x[4]) \oplus (x[0] \wedge x[1]) \oplus (x[3] \wedge x[4])$
$g_3(x)$	$x[4] \oplus x[3] \oplus (x[3] \wedge x[4]) \oplus x[2] \oplus (x[2] \wedge x[4]) \oplus (x[2] \wedge x[3]) \oplus (x[2] \wedge x[3] \wedge x[4]) \oplus (x[1] \wedge x[3] \wedge x[4]) \oplus x[0] \oplus (x[0] \wedge x[3] \wedge x[4]) \oplus (x[0] \wedge x[2]) \oplus (x[0] \wedge x[2] \wedge x[4]) \oplus (x[0] \wedge x[2] \wedge x[3] \wedge x[4]) \oplus (x[0] \wedge x[1]) \oplus (x[0] \wedge x[1] \wedge x[2])$
$g_4(x)$	$(x[0] \wedge x[3] \wedge x[4]) \oplus (x[0] \wedge x[2] \wedge x[3] \wedge x[4]) \oplus (x[0] \wedge x[1] \wedge x[4]) \oplus (x[0] \wedge x[1] \wedge x[2] \wedge x[4])$
$g_5(x)$	$(x[0] \wedge x[3]) \oplus (x[0] \wedge x[2] \wedge x[3]) \oplus (x[0] \wedge x[1] \wedge x[4]) \oplus (x[0] \wedge x[1] \wedge x[3]) \oplus (x[0] \wedge x[1] \wedge x[3] \wedge x[4]) \oplus (x[0] \wedge x[1] \wedge x[2] \wedge x[3])$
$g_6(x)$	$(x[3] \wedge x[4]) \oplus (x[2] \wedge x[4]) \oplus (x[2] \wedge x[3] \wedge x[4]) \oplus (x[1] \wedge x[3]) \oplus (x[0] \wedge x[3] \wedge x[4]) \oplus (x[0] \wedge x[2] \wedge x[4]) \oplus (x[0] \wedge x[2] \wedge x[3] \wedge x[4]) \oplus (x[0] \wedge x[1] \wedge x[3]) \oplus (x[0] \wedge x[1] \wedge x[3] \wedge x[4])$

S-box of the SPN cipher, then the function

$$g(x_1, \ldots, x_t) = \bigoplus_{i=1}^{t} g_S(x_i)$$

is a nonlinear invariant for the round function R.

Theorem 1. Let S denote an n-bit S-box. For any S-box S' that is Q-equivalent to S, one has $D_{S'} = D_S$.

Proof. Since S' is Q-equivalent to S, then there exists a $n \times n$ invertible matrix, such that $S' = Q^{-1}S(Q(x))$. Assuming that $g : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ is the nonlinear invariant of S, so that

$$g(x) \oplus g(S(x)) = c. \tag{B1}$$

Let $y = Q^{-1}(x)$ and $g'(x) = g(Q(x))$, we replace g and x in Equation B1 with g' and y respectively, then we have

$$g'(y) \oplus g'(Q^{-1}S(Q(y))) = c.$$

It implies that g' is a nonlinear invariant of S'. Since $g'(x) = g(Q(x)$, the algebraic degrees of $g(x))$ and $g'(x)$ are the same, which can be further concluded that every $g \in U(S)$ has a corresponding $g' \in U(S')$ with the same algebraic degree. In summary, $D_{S'} = D_S$ always holds.

Theorem 2. Without constant addition, suppose that two 4-bit optimal S-boxes S_1 and S_2 belong to the affine equivalence class whose representative is $G_i (0 \leqslant i \leqslant 15)$. Let

$$S_1(x) = B_1 G_i(A_1(x)), S_2(x) = B_2 G_i(A_2(x)),$$

where A_1, A_2, B_1, B_2 are 4×4 invertible matrices. S_1 and S_2 belong to the same Q-equivalence class if and only if

$$A_1 B_1 = A_2 B_2. \tag{B2}$$

In addition, this theorem holds for other affine equivalence classes.

Proof. Let

$$S_1'(x) = A_1 S_1(A_1^{-1}(x)) = A_1 B_1 G_i(x)$$
$$S_2'(x) = A_2 S_2(A_2^{-1}(x)) = A_2 B_2 G_i(x)$$

According to the definition of Q-equivalence, S_1 is Q-equivalent to S_1', S_2 is Q equivalent to S_2'. If $A_1 B_1 = A_2 B_2$, then $S_1' = S_2'$, so S_1 and S_2 belong to the same Q-equivalence class. On the other hand, if S_1 and S_2 belong to the same Q-equivalent class, then there exists an 4×4 invertible matrix Q such that

$$S_1(x) = Q^{-1}S_2(Q(x)) \Longrightarrow B_1 G_1(A_1(x)) = Q^{-1} B_2 G_i(A_2 Q(x)).$$

If the above equation holds, $B_1 = Q^{-1}B_2$ and $A_1 = A_2 Q$, which implies that $A_1 B_1 = A_2 B_2$. So that S_1 and S_2 belong to the same Q-equivalence class.

Corollary 1. Let $S = QG_i(x)$, where Q is 4×4 invertible matrix and G_i is one of the representative of 16 affine equivalence classes of optimal 4-bit S-boxes. By taking all possible values of Q, we can directly calculate the representative of each Q-equivalence class in S-boxes which are linear equivalent to G_i.

Proof. In Theorem 2, we set A_1 and A_2 as identity matrices and we get

$$S_1(x) = B_1 G_i(x), S_2(x) = B_2 G_i(x).$$

As long as any value in B_2, B_1 changes, Equation (B2) do not hold. That is, S_1 is not Q-equivalent to S_2. Therefore, when Q takes different values, the generated S-box S belongs to different Q-equivalent classes.

Proposition 1. Consider an R-round SPN block cipher E_K of the type mentioned in Preliminary. If its b-bit S-boxes $S(x)$ is replaced by

$$S' = Q^{-1}S(Q(x)) \oplus c,$$

where Q is an $b \times b$ binary invertible matrix and c is a constant over $\mathbb{F}_2^b$, then the changed round function

$$\mathsf{MC} \circ \mathsf{SR} \circ \mathsf{SB'} \circ \mathsf{AddKey}$$

($\mathsf{SB'}$ denotes that the S-box S is replaced by S')is equivalent to

$$\mathsf{Q}^{-1}\mathsf{M} \circ \mathsf{MC} \circ \mathsf{SR} \circ \mathsf{SB} \circ \mathsf{AddKey'} \circ \mathsf{QM}$$

where Q(or Q^{-1})M is to left-multiply each cell of the current internal state $s^{(r)}$ by Q(or Q^{-1}), and $\mathsf{AddKey'}$ is to bitwise XOR the internal state with the modified round keys $k_m^{(r)}$ whose specific form is

$$k_m^{(r)} = \begin{cases} \mathsf{QM}(k^{(0)}), r = 0 \\ \mathsf{QM}(k^{(r)} \oplus \mathsf{MC}(C)), 1 \leqslant r \leqslant R \end{cases} \tag{B3}$$

C is a $n \times m$ matrix over $\mathbb{F}_2^b$ whose cells are c.

Proof. We begin with the first round of encryption to prove the above proposition in detail. Firstly, $\mathsf{AddKey}(s^{(0)}) = s^{(0)} \oplus k^{(0)}$. It is trivial that $\mathsf{SB}(s^{(0)} \oplus k^{(0)})$ is transformed to

$$\mathsf{Q}^{-1}\mathsf{M} \circ \mathsf{SB}(\mathsf{QM}(s^{(0)} \oplus k^{(0)})) \oplus C = \mathsf{Q}^{-1}\mathsf{M} \circ \mathsf{SB}(\mathsf{QM}(s^{(0)}) \oplus k_m^{(0)}) \oplus C$$

after the substitution of S-box, which is equivalent to

$$\mathsf{Q}^{-1}\mathsf{M} \circ \mathsf{SB} \circ \mathsf{AddKey'} \circ \mathsf{QM}(s^{(0)}) \oplus C.$$

And it is easy to get that

$$\mathsf{SR}(\mathsf{Q}^{-1}\mathsf{M} \circ \mathsf{SB} \circ \mathsf{AddKey'} \circ \mathsf{QM}(s^{(0)}) \oplus C) = \mathsf{Q}^{-1}\mathsf{M} \circ \mathsf{SR} \circ \mathsf{SB} \circ \mathsf{AddKey'} \circ \mathsf{QM}(s^{(0)}) \oplus C.$$

Let $\mathsf{SR} \circ \mathsf{SB} \circ \mathsf{AddKey'} \circ \mathsf{QM}(s^{(0)}) = s_R^{(0)}$, then

$$\mathsf{MC}(\mathsf{Q}^{-1}\mathsf{M}(s_R^{(0)}) \oplus C) = \mathsf{MC} \circ \mathsf{Q}^{-1}\mathsf{M}(s_R^{(0)}) \oplus \mathsf{MC}(C).$$

Because M is a matrix over $\mathbb{F}_2$, i.e. each cell of a column of the state is replaced by the XOR sum of some elements in the same column, so that we can extract Q^{-1} and put it to the left of the state and the above equation is converted to $\mathsf{Q}^{-1}\mathsf{M} \circ \mathsf{MC}(s_R^{(0)}) \oplus \mathsf{MC}(C)$. Therefore the output of the 1-st round is

$$\mathsf{MC}(\mathsf{Q}^{-1}\mathsf{M} \circ \mathsf{SR} \circ \mathsf{SB} \circ \mathsf{AddKey'} \circ \mathsf{QM}(s^{(0)}) \oplus C) = \mathsf{Q}^{-1}\mathsf{M} \circ \mathsf{MC} \circ \mathsf{SR} \circ \mathsf{SB} \circ \mathsf{AddKey'} \circ \mathsf{QM}(s^{(0)}) \oplus \mathsf{MC}(C)$$

Let $\mathsf{Q}^{-1}\mathsf{M} \circ \mathsf{MC} \circ \mathsf{SR} \circ \mathsf{SB} \circ \mathsf{AddKey'} \circ \mathsf{QM}(s^{(0)}) = s_m^{(1)}$, then the input of the second round is $s_m^{(1)} \oplus \mathsf{MC}(C)$.

$$\begin{aligned} \mathsf{Q}^{-1}\mathsf{M} \circ \mathsf{SB} \circ \mathsf{QM} \circ \mathsf{AddKey}(s_m^{(1)} \oplus \mathsf{MC}(C)) &= \mathsf{Q}^{-1}\mathsf{M} \circ \mathsf{SB}(\mathsf{QM}(s_m^{(1)} \oplus k^{(1)} \oplus \mathsf{MC}(C))) \oplus C \\ &= \mathsf{Q}^{-1}\mathsf{M} \circ \mathsf{SB}(\mathsf{QM}(s_m^{(1)}) \oplus k_m^{(1)}) \oplus C \\ &= \mathsf{Q}^{-1}\mathsf{M} \circ \mathsf{SB} \circ \mathsf{AddKey'} \circ \mathsf{QM}(s_m^{(1)}) \oplus C. \end{aligned}$$

Similar to the first round, the output of the second round is

$$\mathsf{Q}^{-1}\mathsf{M} \circ \mathsf{MC} \circ \mathsf{SR} \circ \mathsf{SB} \circ \mathsf{AddKey'} \circ \mathsf{QM}(s_m^{(1)}) \oplus \mathsf{MC}(C).$$

It can be seen that after replacing the S-box, the technique for the first round can be analogously applied to other rounds. We can add $\mathsf{MC}(C)$ at the end of each round to the next round key, then the round function is transformed to $\mathsf{Q}^{-1}\mathsf{M} \circ \mathsf{MC} \circ \mathsf{SR} \circ \mathsf{SB} \circ \mathsf{AddKey'} \circ \mathsf{QM}$ as well as the input and round key states of the r-th round are transformed to $s_m^{(r)}$ and $k_m^{(r)}$. Particularly, $s_m^{(0)} = s^{(0)}$. We use *cipher* to denote ciphertext, so

$$\begin{aligned} cipher &= s_m^{(R)} \oplus \mathsf{MC}(C) \oplus k^{(R)} \\ &= \mathsf{Q}^{-1}\mathsf{M} \circ \mathsf{AddKey'} \circ \mathsf{MC} \circ \mathsf{SR} \circ \mathsf{SB} \circ \mathsf{AddKey'} \circ \mathsf{QM}(s_m^{(R-1)}) \end{aligned}$$

References

1 Todo Y, Leander G, Sasaki Y. Nonlinear invariant attack - practical attack on full SCREAM, iSCREAM, and Midori64. In: Proceedings of Advances in Cryptology - ASIACRYPT 2016, Hanoi, Vietnam, 2016, 3–33.