SCIENCE CHINA
Information Sciences

• LETTER •

March 2022, Vol. 65 139103:1–139103:3
https://doi.org/10.1007/s11432-019-2632-1

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*

Received 15 April 2019/Revised 15 August 2019/Accepted 30 August 2019/Published online 24 May 2021

Citation Tong H P, Shen X, Li C, et al. Improved nonlinear invariant attack. Sci China Inf Sci, 2022, 65(3): 139103, https://doi.org/10.1007/s11432-019-2632-1

Dear editor,

In Asiacrypt 2016, Todo et al. [1] proposed a nonlinear invariant attack, a new type of distinguisher that covers any number of rounds for a substitution-permutation network (SPN) cipher under weak keys. The main idea of the nonlinear invariant attack is to find a Boolean function $g : \mathbb{F}_2^n \to \mathbb{F}_2$ such that the evaluation of $g(x) \oplus g(E_k(x))$ is constant for any x, where $E_k(x)$ is a block cipher. The function g is called the nonlinear invariant of E_k and the keys k that satisfy the condition are called weak keys. In addition, Todo et al. [1] proved that the nonlinear invariants of an SPN cipher can be found exactly as long as the cipher satisfies three conditions: the cipher is LS-design, the transformation matrix of the linear layer is orthogonal, and the S-box has quadratic nonlinear invariants.

Previous studies have focused mostly on the influence of round constants on nonlinear invariant attacks. Beierle et al. [3] showed that the success of a nonlinear invariant attack depends mainly on the selection of round constants, and presented some strategies to find round constants as a countermeasure against the nonlinear invariant attack. In order to eliminate the influence of round constants, Wei et al. [4] proposed a generalized nonlinear invariant attack to use a pair of constants in the input of nonlinear invariants. By introducing the useful concept of closed-loop invariants of the S-box, Wei et al. also proposed a new method for selecting round constants that improves upon the strategy proposed by Beierle et al.

In this study, we study the equivalence of nonlinear invariants in S-boxes and propose an improved nonlinear invariant attack with an application to attack full FIDES-80 under 2^{32} weak keys.

Equivalence of nonlinear invariants in S-boxes.

Proposition 1 ([5]). Let S and S' be two 4-bit S-boxes. If S is bijective, and the differential uniformity and nonlinearity are both 4, then the S is called a optimal S-box. S and S' are called affine equivalent if there exist two invertible 4×4 matrices A, B over $\mathbb{F}_2$, and constants $a, b \in \mathbb{F}_2^4$ such that $S'(x) = B(S(A(x) \oplus a)) \oplus b$. If S is an optimal S-box, S' is also an optimal S-box.

On the basis of Proposition 1, several results on the classification of 4-bit optimal S-boxes have been presented [5,6]. Affine equivalence preserves differential uniformity and nonlinearity, and an interesting point of research is whether it also preserves nonlinear invariants. However, our results show that by introducing a new definition of equivalence, the algebraic degree of nonlinear invariants can be preserved.

Definition 1 (Q-equivalence). Two n-bit S-boxes, S and S', are called Q-equivalent if there exists an $n \times n$ invertible matrix Q over $\mathbb{F}_2$ such that $S'(x) = Q^{-1}S(Q(x))$.

Definition 2 (Category). We use D_S to denote a set of algebraic degrees of invariants contained in the space of nonlinear invariants, with the exception of trivial invariants, of an n-bit S-box S, i.e., $D_S = \{\deg(g) | g \in U(S)\}$, where $U(S)$ is a nonlinear invariant space of S. A set that contains all the n-bit S-boxes with the same elements in D_S is called a category.

Here we demonstrate that the invariants of the S-boxes belonging to the same Q-equivalence class have the same algebraic degree.

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

According to the above theorem, one can classify 4-bit S-boxes into different Q-equivalent classes according to the elements in D_S. Additionally, we propose the following theorems to efficiently retrieve the representative of each Q-equivalent class in negligible time.

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

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

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 $A_1 B_1 = A_2 B_2$. In addition, this theorem holds for other affine equivalence classes.

Corollary 1. Let $S = QG_i(x)$, where Q is a 4×4 invertible matrix and G_i is one of the representatives of the 16 affine equivalence classes of optimal 4-bit S-boxes. By taking all

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

possible values of Q, we can directly calculate the representative of each Q-equivalence class in the S-boxes that is linearly equivalent to G_i.

We classify $2^{32.6}$ 4-bit S-boxes in different affine equivalence classes separately and give the distribution of Q-equivalence classes (Tables A1 and A2 in Appendix A). Obviously, the S-boxes of the Q-equivalence classes in categories with $D_S = \{4\}, \{3, 4\}$ have no quadratic nonlinear invariants; so it is impossible to determine the nonlinear invariants of ciphers according to Lemma 1 (in Appendix B).

Improved nonlinear invariant attack. Here we recall a certain type of AES-like SPN cipher. Assume that the internal state can be expressed as an $n \times m$ matrix over $\mathbb{F}_2^b$. The internal state is updated iteratively by R round functions, and the input and round key states of the r-th round are denoted by $s^{(r)}$ and $k^{(r)}$, respectively. Particularly, a cell of $s^{(r)}$(or $k^{(r)}$) is denoted by $s_{i,j}^{(r)}$ (or $k_{i,j}^{(r)}$). The round function can be expressed as $\mathsf{MC} \circ \mathsf{SR} \circ \mathsf{SB} \circ \mathsf{AddKey}$.

AddKey: The state $s^{(r)}$ is bitwise XORed with the $n \times m \times b$-bit roundkey $k^{(r)}$ generated by the key schedule. SB: The SubBytes (SB) step is the S-box layer. A b-bit S-box S is applied to every b-bit cell of the state $s^{(r)}$ in parallel. SR: This transformation is a cell shift, which can be defined as a permutation $\pi_{\mathsf{SR}} = (l_0, l_1, \ldots, l_{n-1})$ acting on $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ that moves cell $s_{i,j}^{(r)}$ by l_i positions to the left in its original row. MC: The MixColumns (MC) transformation is applied to m columns of $s^{(r)}$ in parallel. More precisely, the state $s^{(r)}$ is left-multiplied by an $n \times n$ orthogonal binary matrix M. After the last round of encryption, the final ciphertext is obtained as $s^{(R)} \oplus k^{(R)}$.

We introduce an improved nonlinear invariant attack. The main idea is to replace the n-bit S-box S by $Q^{-1} \circ S \circ Q \oplus c$ where Q is an $n \times n$ invertible matrix in $\mathbb{F}_2$ and $c \in \mathbb{F}_2^n$, so that the replaced S-box has quadratic nonlinear invariants. In addition, we can prove that the original block cipher E_K is changed to $Q^{-1} \circ E_{K'} \circ Q$ after replacing the S-box.

Proposition 2. Consider an R-round SPN block cipher E_k of the type mentioned before. If its b-bit S-box $S(x)$ is replaced by $S' = Q^{-1}S(Q(x)) \oplus c$, where Q is a $b \times b$ binary invertible matrix and c is a constant over $\mathbb{F}_2^b$, then the changed round function $\mathsf{MC} \circ \mathsf{SR} \circ \mathsf{SB'} \circ \mathsf{AddKey}$[1)] 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 acts to left-multiply each cell of the current internal state $s^{(r)}$ by Q (or Q^{-1}), and AddKey' is to bitwise XOR the internal state with the modified round keys $k_m^{(r)}$ whose specific forms are

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

where C is an $n \times m$ matrix over $\mathbb{F}_2^b$ with c cells.

Because $\mathsf{Q}^{-1}\mathsf{M} \circ \mathsf{QM}$ is equal to an identical transformation, only QM at the input and $\mathsf{Q}^{-1}\mathsf{M}$ at the output of the cipher are preserved in the iterative process of the round function, assuming that the block cipher E_k is transformed to $\widehat{E_k}$ after the S-box substitution. From the above analysis, we can conclude that $\widehat{E_k}$ is equivalent to $\mathsf{Q}^{-1}\mathsf{M} \circ E_{k'} \circ \mathsf{QM}$, where k' indicates that the round key $k^{(r)}$ is replaced by $k_m^{(r)}$. Note that $E_{k'}$ is equivalent to changing the key schedule of the original block cipher E_k. The relationship between E_k, $\mathsf{Q}^{-1}\mathsf{M} \circ E_{k'} \circ \mathsf{QM}$, $E_{k'}$, and $\widehat{E_k}$ is depicted in Figure 1.

1) SB'indicates that the S-box S is replaced by S'.

In conclusion, if an appropriate matrix Q and a constant c are selected such that $Q^{-1}S(Q(x)) \oplus c$ has quadratic nonlinear invariants that are linear (or constant) in some of the inputs, then by Lemma 1 we can obtain the nonlinear invariants of $\mathsf{Q}^{-1}\mathsf{M} \circ E_{k'} \circ \mathsf{QM}$. From the quadratic nonlinear invariants, we can directly obtain the weak key form of $k^{(r)}$. Finally, we can calculate the set (denoted by $\mathcal{K}$) of weak keys of $k_m^{(r)}$ using the relationship between $k_m^{(r)}$ and $k^{(r)}$. Thus, if the round keys $k^{(r)} \in \mathcal{K}$, we can execute a distinguishing attack on the block cipher E_k.

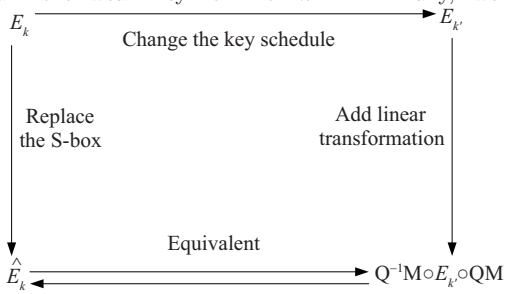

Figure 1 Relationship between E_k, $\mathsf{Q}^{-1}\mathsf{M} \circ E_{k'} \circ \mathsf{QM}$, $E_{k'}$ and $\widehat{E_k}$.

Application to full FIDES-80. Bilgin et al. [7] presented a lightweight authentication cipher FIDES at CHES 2013. The round function of FIDES-80 can be described as $\mathsf{CA} \circ \mathsf{MC} \circ \mathsf{SR} \circ \mathsf{SB}$. Let

$$Q = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}, \quad c = 1.$$

We can calculate the bases of nonlinear invariants of $Q^{-1}S(Q(x)) \oplus c$ (Table A3 in Appendix A). By observing the combinations of these bases, we find that $g_0(x) = x[4] \oplus x[2] \oplus (x[1] \wedge x[4]) \oplus (x[0] \wedge x[3]) \oplus (x[0] \wedge x[1])$ is a quadratic invariant where the third bit is not included in the nonlinear component. The 5-bit nibble of the round constant $\mathrm{RC}^{(r)}$ in row i and column j is denoted by $\mathrm{rc}_{i,j}^{(r)}$. The weak constant form of $\mathrm{RC}^{(r)}$ can be obtained immediately according to the specific form of the function $g_0(x)$, which is $\mathrm{rc}_{i,j}^{(r)} = (0, 0, 0, 0, 0)$ or $(0, 0, 1, 0, 0)$. Thus, from (1), we can discern whether each 5-bit cell of $\mathrm{RC}_m^{(r)}$ is $(1, 1, 1, 0, 0)$ or $(1, 1, 0, 1, 0)$, $\mathrm{RC}_m^{(r)}$ is a weak constant. Therefore, the density of weak constants corresponding to the nonlinear invariant g of a round transformation of FIDES-80 is 2^{-128}, i.e., there are 2^{32} weak constants.

Our method can be used to mount a distinguishing attack under a weak constant, assuming that the plaintext and ciphertext of the R-round FIDES-80 transformation are $s^{(0)}$ and $s^{(R)}$, respectively, and that all the round constants $\mathrm{RC}_m^{(r)}$ are weak. The relation between $s^{(0)}$ and $s^{(R)}$ is given as

$$g(\mathsf{Q}^{-1}\mathsf{M}(s^{(0)})) = g(\mathsf{Q}^{-1}\mathsf{M}(s^{(R)})) = \text{const},$$

which always holds for arbitrary $s^{(0)}$ when the weak constants $\mathrm{RC}_m^{(r)}$ are fixed.

Conclusion. We have proved that the introduction of Q-equivalence preserves the algebraic degree of the nonlinear invariants. Using this property, we partially classify 4-bit affine equivalent optimal S-boxes into four different categories according to their Q-equivalence. Furthermore, we propose an improved nonlinear invariant attack based on a new technique to substitute the S-box, and apply it to attack full FIDES-80 through nonlinear invariants with 2^{32} weak constants.

Detailed proofs of all the above theorems, corollary, and proposition can be found in Appendix B.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. 61672530, 61702537, 61772545).

Supporting information Appendixes A and B. The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

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, 2016. 3–33

2 Grosso V, Leurent G, Standaert F X, et al. LS-Designs: bitslice encryption for efficient masked software implementations. In: Fast Software Encryption. Berlin: Springer, 2014. 18–37

3 Beierle C, Canteaut A, Leander G, et al. Proving resistance against invariant attacks: how to choose the round constants. In: Proceedings of the 37th Annual International Cryptology Conference, Santa Barbara, 2017. 647–678

4 Wei Y Z, Ye T, Wu W L, et al. Generalized nonlinear invariant attack and a new design criterion for round constants. IACR Trans Symmetric Cryptol, 2018, 4: 62–79

5 Leander G, Poschmann A. On the classification of 4 bit S-boxes. In: Arithmetic of Finite Fields. Berlin: Springer, 2007. 159–176

6 Zhang W T, Bao Z Z, Rijmen V, et al. A new classification of 4-bit optimal S-boxes and its application to PRESENT, RECTANGLE and SPONGENT. In: Proceedings of International Workshop on Fast Software Encryption, Istanbul, 2015. 494–515

7 Bilgin B, Bogdanov A, Knezevic M, et al. Fides: lightweight authenticated cipher with side-channel resistance for constrained hardware. In: Proceedings of Cryptographic Hardware and Embedded Systems—CHES 2013. Berlin: Springer, 2013. 142–158