IACR Transactions on Symmetric Cryptology
ISSN 2519-173X, Vol. 2018, No. 4, pp. 62–79. DOI:10.13154/tosc.v2018.i4.62-79

Generalized Nonlinear Invariant Attack and a New Design Criterion for Round Constants

Yongzhuang Wei[1], Tao Ye[1], Wenling Wu[2], Enes Pasalic[1,3]

[1] Guilin University of Electronic Technology,
Guilin, Guangxi Province 541004, China
walker_wyz@guet.edu.cn,fendouyetao@163.com
[2] TCA Laboratory, State Key Laboratory of Computer Science (SKLCS), Institute of Software,
Chinese Academy of Sciences, Beijing 100190, China
wwl@tca.iscas.ac.cn
[3] University of Primorska, FAMNIT, Koper 6000, Slovenia
enes.pasalic6@gmail.com

Abstract. The nonlinear invariant attack was introduced at ASIACRYPT 2016 by Todo *et al.*. The attack has received extensive attention of cryptographic community due to its practical application on the full-round block ciphers SCREAM, iSCREAM, and Midori64. However, the attack heavily relies on the choice of round constants and it becomes inefficient in the case these constants nonlinearly affect the so-called nonlinear invariants. In this article, to eliminate the impact from the round constants, a generalized nonlinear invariant attack which uses a pair of constants in the input of nonlinear invariants is proposed. The efficiency of this extended framework is practically confirmed by mounting a distinguishing attack on a variant of full-round iSCREAM cipher under a class of 2^{80} weak keys. The considered variant of iSCREAM is however resistant against nonlinear invariant attack of Todo *et al.*. Furthermore, we investigate the resistance of block ciphers against generalized nonlinear invariant attacks with respect to the choice of round constants in an extended framework. We introduce a useful concept of *closed-loop invariants* of the substitution box (S-box) and show that the choice of robust round constants is closely related to the existence of linear structure of the closed-loop invariants of the substitution layer. In particular, we demonstrate that the design criteria for the round constants in Beierle *et al.*'s work at CRYPTO 2017 is not an optimal strategy. The round constants selected using this method may induce certain weaknesses that can be exploited in our generalized nonlinear invariant attack model. This scenario is efficiently demonstrated in the case of a slightly modified variant of the Midori64 block cipher.

Keywords: Block cipher · Nonlinear invariant attack · Boolean function · iSCREAM · Round constants.

1 Introduction

The design of block ciphers, used as symmetric key encryption algorithms, is well understood and their security has been traditionally evaluated using some standard cryptanalytic techniques such as differential attacks [BS90], linear attacks [Mat93], and their diverse variations [LH94] [HTW15]. During the last few years some other cryptanalytic methods applicable to certain families of block ciphers have emerged. Nevertheless, whereas most of the well established designs are quite robust to these new methods it appears that primarily lightweight block ciphers are susceptible to these attacks. This feature is mainly due to a rather simplified design strategy of certain lightweight block ciphers and in particular their simple key schedule.

Received: 2018-09-01, Accepted: 2018-11-01, Published: 2018-12-13

Recently, the nonlinear invariant attack was introduced at ASIACRYPT 2016 by Todo *et al.* [TLS16] and it gained a lot of attention due to its efficient application in breaking full-round block ciphers such as SCREAM [GLSV15], iSCREAM [GLSV14b] and Midori64 [BBI+15]. However, the attack is only successful in the case that the secret key is chosen from a subset of weak keys. The nonlinear invariant attack can be seen as a further extension of the invariant subspace attack introduced in [LAAZ11] [LMR15], which identifies the property of having inputs and outputs that belong to the same affine subspace through (many) encryption rounds (again assuming that the secret key is chosen from a class of weak keys). The core idea of the nonlinear invariant attack is to look for a nonlinear Boolean function $g : GF(2)^n \longrightarrow GF(2)$ for which the evaluation of $g(x) \oplus g(E(x, k))$ is constant for any x, where $E(x, k)$ is the encryption function of a considered n-bit block cipher. The function g is then called a nonlinear invariant for $E(x, k)$ and those keys $k \in \mathcal{K}$ for which g is nonlinear invariant are called *weak keys*. In general, for a random permutation this property holds with a probability of about 2^{1-N} if N plaintext/ciphertext pairs are considered (assuming g is a balanced Boolean function). Consequently, any block cipher admitting nonlinear invariants can be easily distinguished from a random permutation.

In general, nonlinear invariants for a full-round block cipher are derived by finding nonlinear invariants for each separate round (if these exist). These are then merged together in a similar way as one obtains differential/linear characteristics of a block cipher. Nevertheless, in order to extend a nonlinear invariant of a single round to the whole cipher, it is necessary that all round keys belong to the family of weak keys. Even though this assumption appears to be quite unrealistic, it was demonstrated in [TLS16] that certain recently proposed lightweight block ciphers have serious weaknesses in this context. Another important point is the fact that, apart from the assumption on weak keys, the success of this attack heavily relies on the choice of the round constants so that their proper selection can protect cipher against these attacks [BCLR17].

1.1 Our contribution

In this work, we introduce a generalized nonlinear invariant attack (GNIA) which, in difference to the classical one, uses a pair of constants in the input of a nonlinear invariant g. More specifically, for a block cipher $E(x, k)$ one tries to identify a nonlinear Boolean function $g : GF(2)^n \longrightarrow GF(2)$ and a *pair* of n-bit constants (a_1, a_2) so that $g(x \oplus a_1) \oplus g(E(x, k) \oplus a_2)$ is constant for any x, where the key k belongs to a class of weak keys. The main benefit of this approach is that the pair of constants (a_1, a_2) can be useful for eliminating the nonlinear effect of the round constants. The framework of our generalized nonlinear invariant attack on substitution-permutation network (SPN) block ciphers is then investigated and its efficiency is firstly justified by specifying a distinguishing attack on a slightly modified variant of full-round block cipher iSCREAM. The attack is valid for the identified class of weak keys of cardinality 2^{80}. However, it should be noticed that this variant of iSCREAM cipher is resistant against nonlinear invariant attack of Todo *et al.* [TLS16] [TLS18].

Moreover, the resistance of block ciphers against generalized nonlinear invariant attacks with respect to the choice of round constants is discussed in an extended framework. Instead of using a single nonlinear invariant g, for a given block cipher $E(k, x)$ the adversary may attempt to identify two different nonlinear Boolean functions $g_1, g_2 : GF(2)^n \longrightarrow GF(2)$ such that $g_1(x) \oplus g_2(E(x, k))$ is constant for any x, for some class of weak keys. This extended framework relates to the work of Beierle *et al.* [BCLR17], where the resistance of certain block ciphers against the original nonlinear invariant attack of Todo *et al.* [TLS16] [TLS18] with respect to the choice of round constants was considered. The main conclusion in [BCLR17] is that the round constants can be chosen independently of the substitution layer in most of the cases. However, we show that the choice of round constants can be closely related to the properties of the substitution layer of a given block cipher in our extended framework (using two invariants g_1 and g_2). More precisely, it is demonstrated, by considering a variant of Midori block cipher, that the choice of robust round constants largely depends on the existence of linear structures of invariants of the substitution layer. The application of our extended generalized nonlinear invariant attack, by means of specifying a distinguishing attack on this cipher, therefore indicates that the suggested design criteria for the choice of round constants considered in Beierle *et al.* [BCLR17] is not necessarily optimal. To circumvent these kind of attacks, we introduce an additional criterion for the choice of round constants that takes into account *closed-loop invariants* of the S-boxes. These closed-loop invariants essentially relate the input and output of a given S-box in a special manner. Then, based on their existence, it is demonstrated that a distinguishing attack on a slightly modified version of Midori64 cipher can be efficiently mounted. Nevertheless, it has been confirmed by computer simulations that some prominent block ciphers, such as PRESENT [BKL+07], PRINCE [BCG+12], and Lblock [WZ11], do not admit closed-loop invariants and are therefore resistant to generalized nonlinear invariant attacks.

1.2 Related works

The nonlinear cryptanalysis of block ciphers was first studied by Harpes *et al.* [HKM95] and later by Knudsen *et al.* [KR96], where both methods can be seen as certain extension of linear cryptanalysis. Nevertheless, only recently the first successful application of the nonlinear cryptanalysis on full-round block ciphers was presented in [TLS16] which uses full-round nonlinear invariants. In the context of the choice of round constants, whose suitable choice may render these attacks against lightweight block ciphers inefficient, some strategies were discussed in [BCLR17] but the proposed criteria appear not to be sufficient.

1.3 Organization

The rest of the paper is organized as follows. The basic ideas behind generalized nonlinear invariant attacks are described in Section 2. An extended framework of this approach applied to SPN block ciphers is discussed in Section 3. In Section 4, an efficient application of our approach is illustrated by mounting a distinguishing attack on a variant of full-round block cipher iSCREAM. The resistance against the generalized nonlinear invariant attack with respect to the choice of robust round constants and the concept of closed-loop invariants is discussed in Section 5. Some concluding remarks are given in Section 6.

2 Generalized nonlinear invariant attack

2.1 Notation

We present our notation in Table 1.
Without loss of generality, we assume that the nonlinear terms of invariant $g(x)$ only involve the first s input variables (where s can be equal to n), whereas the remaining t variables are related in a linear manner.

2.2 Basic idea of GNIA

In this section, the basic ideas behind generalized nonlinear invariant attacks are discussed. For a considered r-round iterative block cipher, the ciphertext C is derived by encrypting a plaintext P using the round subkeys K_i, where $i = 0, \dots, r-1$. More precisely,

$$x_0 = P, \quad x_{i+1} = F_{K_i}(x_i) = F(x_i) \oplus K_i, \quad x_r = C, \tag{1}$$

Table 1: The notation used throughout the paper

$\|\|$	Concatenation
g'	A generalized nonlinear invariant of a single S-box.
$U(S, a_1, a_2)$	The set of generalized nonlinear invariants of an S-box.
g_S	A generalized nonlinear invariant of the S-box layer.
g	A generalized nonlinear invariant of the round function, $g(x) = f(x^{(1)}) \oplus \ell(x^{(2)})$.
f	The nonlinear part of the nonlinear invariant function, $GF(2)^s \longrightarrow GF(2)$.
ℓ	The linear part of the nonlinear invariant function, $GF(2)^t \longrightarrow GF(2)$, and $s + t = n$.
a_i	$a_i = (a_i^{(1)} \parallel a_i^{(2)}) \in GF(2)^n, a_i^{(1)} \in GF(2)^s, a_i^{(2)} \in GF(2)^t, (i = 1, 2)$.
K_j	$K_j = (K_j^{(1)} \parallel K_j^{(2)}) \in GF(2)^n, K_j^{(1)} \in GF(2)^s, K_j^{(2)} \in GF(2)^t, (j = 0, \ldots, r-1), s + t = n$.
x	For $x = (x^{(1)} \parallel x^{(2)}) \in GF(2)^n, x^{(1)} \in GF(2)^s$, $x^{(2)} \in GF(2)^t, s + t = n$.
$M_\star[j]$	For a binary $n \times m$ matrix M, $M_\star[j] \in GF(2)^n$ is the *jth* column of M.
$M_i[\star]$	For a binary $n \times m$ matrix M, $M_i[\star] \in GF(2)^m$ is the *ith* row of M.

where $F : GF(2)^n \to GF(2)^n$ is the round function of an n-bit block cipher, and $F_{K_i}(x_i) = F(x_i) \oplus K_i$ indicates that the output of the round function is XORed with the round subkey K_i. For simplicity, the effect of adding a pre-whitening key is ignored.

The basic idea of our generalized nonlinear invariant attack is to look for a nonlinear Boolean function $g : GF(2)^n \longrightarrow GF(2)$ and a pair of n-bit constants $(a_1, a_2) \in GF(2)^n \times GF(2)^n$ such that $g(x \oplus a_1) \oplus g(F_{K_i}(x) \oplus a_2) = c$ (where c is a binary constant) holds for any x. To specify a generalized nonlinear invariant of the whole ciphers one needs to identify weak subkeys K_j in each round $(j = 0, \ldots, r-1)$ and the constants (a_1, a_2) which are contained in some nonlinear terms of the nonlinear invariant $g(x)$. A subset of keys $\{K\}$ which, along with a suitable pair of constants (a_1, a_2), gives rise to a generalized nonlinear invariant g is called a class of weak keys. Nevertheless, identifying nonlinear invariants for a given block cipher is generally hard and computationally infeasible unless S-boxes are quite small or alternatively there are some structural properties that may be employed. Using the notation given in Table 1, we have the following observation.

Proposition 1. *If the round subkeys K_j, for $j = 0, \ldots, r-1$, and the constants a_1, a_2 satisfy the condition: $a_1^{(1)} \oplus a_2^{(1)} \oplus K_j^{(1)} = \mathbf{0}$, then the generalized nonlinear invariant attack can be applied to a full-round block cipher.*

Proof. Let $c_j \in GF(2)$ be a binary constant, for any $j = 0, 1, \ldots, r-1$. Assume that g is a generalized nonlinear invariant of the round function, i.e. $g(x) = f(x^{(1)}) \oplus \ell(x^{(2)})$, where $f(x^{(1)})$ is the nonlinear part of $g(x^{(1)} \parallel x^{(2)})$ and $\ell(x^{(2)})$ is the linear part of $g(x^{(1)} \parallel x^{(2)})$ (see Table 1). In order to eliminate the impact from the round constants in the nonlinear part of g, we consider the two cases below.

Case 1: In the case $a_1^{(1)} = \mathbf{0}, a_2^{(1)} \oplus K_j^{(1)} = \mathbf{0}$, using (1), we have

$$\begin{aligned}
g(C) &= g(x_r \oplus a_2 \oplus a_2) \\
&= g(F(x_{r-1}) \oplus K_{r-1} \oplus a_2 \oplus a_2) \\
&= g(F(x_{r-1}) \oplus a_2) \oplus \ell(K_{r-1}^{(2)} \oplus a_2^{(2)}) \\
&= g(x_{r-1} \oplus a_1) \oplus \ell(K_{r-1}^{(2)} \oplus a_2^{(2)}) \oplus c_{r-1} \\
&= g(x_{r-1} \oplus a_2 \oplus a_2) \oplus \ell(K_{r-1}^{(2)} \oplus a_2^{(2)} \oplus a_1^{(2)}) \oplus c_{r-1}
\end{aligned}$$

$$\begin{array}{rl} \dots & \\ = & g(P) \oplus \sum_{i=0}^{r-1} \ell(K_i^{(2)} \oplus a_2^{(2)} \oplus a_1^{(2)}) \oplus \sum_{j=0}^{r-1} c_j. \end{array}$$

Moreover, we have

$$g(P) \oplus g(C) = Const.'.$$

Case 2: In the case $a_1^{(1)} \neq \mathbf{0}, a_1^{(1)} \oplus a_2^{(1)} \oplus K_j^{(1)} = \mathbf{0}$, we have

$$\begin{array}{rcl} g(C \oplus a_1) & = & g(x_r \oplus a_1 \oplus a_2 \oplus a_2) \\ & = & g(F(x_{r-1}) \oplus K_{r-1} \oplus a_1 \oplus a_2 \oplus a_2) \\ & = & g(F(x_{r-1}) \oplus a_2) \oplus \ell(K_{r-1}^{(2)} \oplus a_2^{(2)} \oplus a_1^{(2)}) \\ & = & g(x_{r-1} \oplus a_1) \oplus \ell(K_{r-1}^{(2)} \oplus a_2^{(2)} \oplus a_1^{(2)}) \oplus c_{r-1} \\ & \dots & \\ & = & g(P \oplus a_1) \oplus \sum_{i=0}^{r-1} \ell(K_i^{(2)} \oplus a_2^{(2)} \oplus a_1^{(2)}) \oplus \sum_{j=0}^{r-1} c_j. \end{array}$$

Moreover, we have

$$g(P \oplus a_1) \oplus g(C \oplus a_1) = Const.'.$$

□

Similarly to the nonlinear invariant attack in [TLS16], by using Proposition 1, the invariant property is preserved through the whole cipher and it immediately leads to a distinguishing attack. Namely, assume that (P_i, C_i) (for $i = 1, \ldots, N$) are N pairs of plaintexts and the corresponding ciphtexts. In the known-plaintext attack scenario, the adversary can easily determine whether $g(P) \oplus g(C)$ (or $g(P \oplus a_1) \oplus g(C \oplus a_1)$) is constant or not for all pairs. Because any random permutation has this property with a probability of 2^{1-N} if g is balanced, the adversary can easily distinguish the block cipher from a random permutation by using Proposition 1.

Remark 1. *To resist slide attacks [BW99, BW00] or invariant subspace attacks [LAAZ11], the round constants $c_i^*, i = 0, \ldots, r-1$, are usually XORed with the round subkeys. For a classical nonlinear invariant attack of Todo* et al. *[TLS16], if some nonlinear term of g involves a nonzero bit of round constant c^*, then the attack becomes rather inefficient [TLS16]. On the other hand, our generalized version uses a pair of constants (a_1, a_2), which can be helpful for eliminating the impact from the round constants c_i^*.*

3 GNIA framework for SPN block ciphers

We consider the following round function $F : GF(2)^{n\times m} \longrightarrow GF(2)^{n\times m}$ of an SPN cipher that consists of an S-box layer $\mathcal{S} : GF(2)^{n\times m} \longrightarrow GF(2)^{n\times m}$ and a linear layer $\mathcal{L} : GF(2)^{n\times m} \longrightarrow GF(2)^{n\times m}$:

$$F(x) = \mathcal{L} \circ \mathcal{S}(x),$$

where $\mathcal{S}(x_\star[1], \ldots, x_\star[m]) = (S(x_\star[1]), \ldots, S(x_\star[m]))$, $x = (x_\star[1], \ldots, x_\star[m]) \in GF(2)^{n\times m}$, and $x_\star[j] = (x_1[j], \ldots, x_n[j]) \in GF(2)^n, j \in \{1, \ldots, m\}$. That is, m S-boxes with n-bit input are used in each round. For simplicity, we only consider the case that the SPN cipher uses identical S-boxes even though a similar analysis can be performed when different S-boxes are used.

3.1 Generalized nonlinear invariants of S-box layer

In order to find generalized nonlinear invariants of a round function $F(x)$, we first analyze the S-box layer. For any S-box $S : GF(2)^n \longrightarrow GF(2)^n$, whose output is $y_j = S(x_\star[j])$ where $x_\star[j] \in GF(2)^n$ and $j \in \{1, \ldots, m\}$, we denote by

$$U(S, a_1, a_2) = \{g' \mid g'(x_\star[j] \oplus a_1) = g'(S(x_\star[j]) \oplus a_2) \oplus c, c \in GF(2), x_\star[j] \in GF(2)^n\},$$

a set of generalized nonlinear invariants $g' : GF(2)^n \to GF(2)$.

To identify $g' \in U(S, a_1, a_2)$, we represent g' in the algebraic normal form (ANF) as

$$g'(x_\star[j]) = \sum_{u \in GF(2)^n} \lambda_u^{(j)} (x_\star[j])^{(u)}, \;\; x_\star[j] \in GF(2)^n, \tag{2}$$

where $(x_\star[j])^{(u)}$ means $\prod_{i=1}^n (x_i[j])^{u_i}$, and $x_i[j]$ and u_i are the ith bits of $x_\star[j]$ and u, respectively. Here, $\lambda_u^{(j)} \in GF(2)$ are 2^n binary coefficients that need to be calculated later (provided that g' exists). The main idea is that, for any given triple (a_1, a_2, c) and all $x_\star[j] \in GF(2)^n$, we transform the equation

$$\sum_{u \in GF(2)^n} \lambda_u^{(j)} ((S(x_\star[j]) \oplus a_1)^{(u)} \oplus (x_\star[j] \oplus a_2)^{(u)}) = c \tag{3}$$

into 2^n linear (or affine) relations that include the coefficients $\lambda_u^{(j)}$. More precisely, for each fixed a_1, a_2, c and $x_\star[j]$, using equation (3), we can obtain a linear (or affine) equation that involves 2^n binary coefficients $\lambda_u^{(j)}$ as variables. Thus, when $x_\star[j]$ ranges over $GF(2)^n$ one obtains an affine equation system with 2^n equations. In particular, if the system has a full rank then using the Gaussian elimination method we can obtain all $\lambda_u^{(j)}$, for different $u \in GF(2)^n$. Otherwise, the process is repeated for other a_1, a_2, and c.

Notice that for the practical sizes of S-boxes, which are usually at most 8 bits, this process of specifying the coefficients $\lambda_u^{(j)}$ can be efficiently conducted on a standard PC. Moreover, to obtain a generalized nonlinear invariant of the substitution layer, consisting of m identical S-boxes, we observe the following easy fact.

Property 1. Assume that $g'_j \in U(S, a_1, a_2)$, $j = 1, \ldots, m$, are arbitrary generalized nonlinear invariants of each round for a given S-box. If $g_{\mathcal{S}}(x_\star[1], \ldots, x_\star[m]) = \sum_{j=1}^m c_j g'_j(x_\star[j])$, $(c_j \in GF(2))$, then $g_{\mathcal{S}}$ is a generalized nonlinear invariant of the S-box layer, i.e.

$$\sum_{j=1}^m c_j \times \{g'_j(x_\star[j] \oplus a_1) \oplus g'_j(S(x_\star[j]) \oplus a_2)\} = Const.. \tag{4}$$

3.2 Generalized nonlinear invariants of linear layer

We now consider an SPN cipher where a MixColumn-like operation is used as a linear layer. Actually, such a linear layer is commonly used in AES-like ciphers [DR02] and LS-like designs [GLSV14a]. In particular, the LS design can be viewed as a composition of a linear layer $\mathcal{L}$ and a substitution layer $\mathcal{S}$, thus its round operation can be compactly described as $\mathcal{L} \circ \mathcal{S}$. More specifically, we consider the linear layer being implemented as a parallel computation performed using an $m \times m$ binary diffusion matrix M. The diffusion process then corresponds to taking each i-th output bit of the m S-boxes to form a row vector of length m which is then multiplied by M to obtain a new binary vector of length m. Before we present the result that shows the existence of generalized nonlinear invariants of the round function (provided the existence of quadratic nonlinear invariants of a given S-box), for convenience of the reader we give an example of using an orthogonal binary matrix M for achieving diffusion.

Example 1. Assume that the round function consists of four identical 4-bit S-boxes S and a binary diffusion orthogonal matrix M of size 4×4. The matrix M, the input state X and the output Y of any of the four S-boxes are respectively written as,

$$M = \begin{bmatrix} m_0[0] & m_0[1] & m_0[2] & m_0[3] \\ m_1[0] & m_1[1] & m_1[2] & m_1[3] \\ m_2[0] & m_2[1] & m_2[2] & m_2[3] \\ m_3[0] & m_3[1] & m_3[2] & m_3[3] \end{bmatrix},$$

$$X = \begin{bmatrix} x_0[0] & \cdots & x_0[3] \\ x_1[0] & \cdots & x_1[3] \\ x_2[0] & \cdots & x_2[3] \\ x_3[0] & \cdots & x_3[3] \end{bmatrix}, \ Y = \begin{bmatrix} y_0[0] & \cdots & y_0[3] \\ y_1[0] & \cdots & y_1[3] \\ y_2[0] & \cdots & y_2[3] \\ y_3[0] & \cdots & y_3[3] \end{bmatrix}.$$

Let $x_i[j]$ denote the entry in the i-th row and j-th column of X, for $i, j \in \{0, \ldots, 3\}$. Let a generalized nonlinear invariant function of the S-box $((y_0[j], y_1[j], y_2[j], y_3[j]) = S((x_0[j], x_1[j], x_2[j], x_3[j])))$ be given as

$$g'_j(x_\star[j]) = (x_0[j] \oplus 1) \times (x_1[j] \oplus 1) \in US(S, a_1 = (1,1,0,0), a_2 = (1,1,0,0)).$$

That is, we have

$$(x_0[j] \oplus 1) \times (x_1[j] \oplus 1) \oplus (y_0[j] \oplus 1) \times (y_1[j] \oplus 1) = 0, j \in \{0,1,2,3\}.$$

The matrix M is applied to the i-th row of Y, which is denoted as $Y_i[\star] \in GF(2)^4$, $i \in \{0, \ldots, 3\}$. After the operation $Y_i[\star] \times M$, $i \in \{0,1,2,3\}$, the state is changed to Y'.

$$Y' = \begin{bmatrix} y'_0[0] & y'_0[1] & y'_0[2] & y'_0[3] \\ y'_1[0] & y'_1[1] & y'_1[2] & y'_1[3] \\ y'_2[0] & y'_2[1] & y'_2[2] & y'_2[3] \\ y'_3[0] & y'_3[1] & y'_3[2] & y'_3[3] \end{bmatrix},$$

$$Y' = \begin{bmatrix} Y_0[\star] \times M_\star[0] & Y_0[\star] \times M_\star[1] & Y_0[\star] \times M_\star[2] & Y_0[\star] \times M_\star[3] \\ Y_1[\star] \times M_\star[0] & Y_1[\star] \times M_\star[1] & Y_1[\star] \times M_\star[2] & Y_1[\star] \times M_\star[3] \\ Y_2[\star] \times M_\star[0] & Y_2[\star] \times M_\star[1] & Y_2[\star] \times M_\star[2] & Y_2[\star] \times M_\star[3] \\ Y_3[\star] \times M_\star[0] & Y_3[\star] \times M_\star[1] & Y_3[\star] \times M_\star[2] & Y_3[\star] \times M_\star[3] \end{bmatrix},$$

where $M_\star[j]$ is the jth column of matrix M, and $M_i[\star]$ is the ith row of matrix M. Since M is an orthogonal matrix, i.e., $M \times M^T$ is the identity matrix, we have the following equation

$$\begin{cases} M_{i_1}[\star] \times (M_{i_2}[\star])^T = 1 & i_1 = i_2 \\ M_{i_1}[\star] \times (M_{i_2}[\star])^T = 0 & i_1 \neq i_2, \end{cases} \tag{5}$$

where $i_1, i_2 \in \{0, \ldots, 3\}$. Using Property 1, we can easily find a generalized nonlinear invariant function of the S-box layer which is given as

$$\sum_{j=0}^{3} (x_0[j] \oplus 1) \times (x_1[j] \oplus 1) \oplus (y_0[j] \oplus 1) \times (y_1[j] \oplus 1) = 0. \tag{6}$$

Using equation (5), we have

$$\sum_{j=0}^{3} (y'_0[j] \oplus 1) \times (y'_1[j] \oplus 1) = \sum_{j=0}^{3} (y_0[j] \oplus 1) \times (y_1[j] \oplus 1),$$

which directly implies that

$$\sum_{j=0}^{3}(x_0[j]\oplus 1)\times(x_1[j]\oplus 1)\oplus(y_0'[j]\oplus 1)\times(y_1'[j]\oplus 1)=0$$

is also the generalized nonlinear invariant function of both substitution and linear layer.

Theorem 1. *Assume that the round function of an SPN-based block cipher uses LS design rationale and that the binary representation of its linear layer $\mathcal{L}$ is an orthogonal matrix $M\in GF(2)^{m\times m}$. If there is a quadratic generalized nonlinear invariant $g'\in U(S,a_1,a_2)$, then the function*

$$g(x)=\sum_{j=1}^{m} g'(x_\star[j])$$

is also a generalized nonlinear invariant for the round function $\mathcal{L}\circ\mathcal{S}$.

Proof. By Property 1, g is a generalized nonlinear invariant of the S-box layer $\mathcal{S}$. Let the input and output of the linear layer be $x=(x_\star[1],\dots,x_\star[m])\in GF(2)^{n\times m}$ and $y=(y_\star[1],\dots,y_\star[m])\in GF(2)^{n\times m}$, respectively. Let $x_i[j]$ and $y_i[j]$ denote the jth bit of $x_i,y_i\in GF(2)^n$, respectively. Denote the transpose of x,y by $x^T,y^T\in GF(2)^{m\times n}$, where $(x_i[\star])^T=(x_i[1],\dots,x_i[m])^T,(y_i[\star])^T=(y_i[1],\dots,y_i[m])^T$. Let a_1, $a_2\in GF(2)^n$, $a_1^*=(a_1,a_1,\dots,a_1)\in GF(2)^{n\times m}$, $a_2^*=(a_2,a_2,\dots,a_2)\in GF(2)^{n\times m}$. Then, we have $(y_i[\star])^T=M\times(x_i[\star])^T$ for all $i=1,\dots,n$. Since g' is a quadratic function we have

$$g'(S(x_\star[j])\oplus a_2) \quad = \quad \sum_{i_1=1}^{n}\sum_{i_2=1}^{n} r_{i_1i_2}((S_{x_\star[j]}[i_1]\oplus a_2[i_1])\cdot(S_{x_\star[j]}[i_2]\oplus a_2[i_2])),$$

where $r_{i_1i_2}$ are the coefficients of g and $S_{x_\star[j]}[i]$ denotes the i-th output bit of $S(x_\star[j])$. Moreover, we have

$$\sum_{j=1}^{m} g'(S(x_\star[j])\oplus a_2)=\sum_{j=1}^{m}\sum_{i_1=1}^{n}\sum_{i_2=1}^{n} r_{i_1i_2}((S_{x_\star[j]}[i_1]\oplus a_2[i_1])\cdot(S_{x_\star[j]}[i_2]\oplus a_2[i_2])). \tag{7}$$

From the definition of inner product $\langle x_{i_1}[\star],x_{i_2}[\star]\rangle=\sum_{j=1}^{m}x_{i_1}[j]\cdot x_{i_2}[j]$, we have

$$\sum_{j=1}^{m} g'(S(x_\star[j])\oplus a_2)=\sum_{i_1=1}^{n}\sum_{i_2=1}^{n} r_{i_1i_2}\langle(\mathcal{S}(x)\oplus a_2^*)_{i_1}[\star],(\mathcal{S}(x)\oplus a_2^*)_{i_2}[\star]\rangle.$$

On the other hand, using the orthogonality of M, we have

$$\begin{aligned}\sum_{j=1}^{m} g'(y_\star[j])\oplus a_2) &= \sum_{i_1=1}^{n}\sum_{i_2=1}^{n} r_{i_1i_2}\langle(\mathcal{S}(x)\oplus a_2^*)_{i_1}[\star]\cdot M,(\mathcal{S}(x)\oplus a_2^*)_{i_2}[\star]\cdot M\rangle\\ &= \sum_{i_1=1}^{n}\sum_{i_2=1}^{n} r_{i_1i_2}\langle(\mathcal{S}(x)\oplus a_2^*)_{i_1}[\star],(\mathcal{S}(x)\oplus a_2^*)_{i_2}[\star]\rangle\\ &= \sum_{j=1}^{m} g'(S(x_\star[j])\oplus a_2).\end{aligned}$$

Therefore, $g(x)$ is a generalized nonlinear invariant for the round function $\mathcal{L}\circ\mathcal{S}$. □

Remark 2. Let $g'\in U(S,a_1,a_2)$ and M be an orthogonal matrix. Then, Theorem 1 states that there exists a generalized nonlinear invariant $g(x)=\sum\limits_{j=1}^{m}g'(x_\star[j])$ for the round function $\mathcal{L}\circ\mathcal{S}$ if the algebraic degree of g' is $deg(g')=2$. Proposition 1 and Theorem 1 then induce a generalized nonlinear invariant attack that can be mounted on SPN block ciphers that admit quadratic nonlinear invariants.

4 Practical attack on a variant of iSCREAM

In this section, we describe a practical generalized nonlinear invariant attack against a variant of authenticated encryption algorithm iSCREAM by exploiting the identified class of 2^{80} weak keys. However, this variant of iSCREAM cipher is resistant against standard nonlinear invariant attacks.

4.1 Brief description of iSCREAM

The authentication encryption algorithm iSCREAM was proposed by Grosso *et al.* [GLSV14b] and it uses a similar structure as SCREAM, the latter being a candidate of the CAESAR competition [CAE13]. More precisely, iSCREAM uses a tweakable variant of LS-design with an 8×16 binary state matrix, i.e. the block state of iSCREAM is 128 bits. Representing the state of iSCREAM as $x \in GF(2)^{8\times 16}$ (formally an 8×16 binary matrix) this authenticated encryption process is described in Algorithm 1, where S and L denote the 8-bit S-box and 16-bit linear layer of the cipher, respectively. In particular, let $x_i[\star] \in GF(2)^{16}$ denote the i-th row of x, for $i \in \{1, \ldots, 8\}$, and $x_\star[j] \in GF(2)^8$ denote the j-th column of x, where $j \in \{1, \ldots, 16\}$. Moreover, let $x_i[j]$ denote the entry in the i-th row and j-th column of x.

iSCREAM takes a 128-bit key K and a 128-bit tweak T as input. The key schedule of iSCREAM is defined as follows:

$$\begin{aligned} TK(\delta = 2i) &= T \oplus K, \\ TK(\delta = 2i+1) &= (T <<<_{16} 1), \end{aligned} \tag{8}$$

where $<<<_{16}$ means that all the rows (16-bit) of the state matrix of size 8×16 are cyclically rotated to the left by one position. The parameter T is given as $T = (N||c||00000000)$, where c is a four bytes block counter and N is an eleven bytes nonce. In order to reduce the implementation cost, iSCREAM uses quite simple round constants $RC(\rho)$ which are defined as follows:

(1) Let $C(\rho) = 27 \cdot \rho \bmod 256$, where the binary representation of $C(\rho)$ is the first byte of $RC(\rho)$ after being XORed with the first byte of the first row of state x.

(2) The remaining bits of $RC(\rho)$, except for those of $C(\rho)$, are all set to zero, thus $RC(\rho)$ only interacts with the first byte of the first row of state x.

The pseudocode of this algorithm is as follows [GLSV14b]:

Algorithm 1

```
$x \Leftarrow P \oplus TK(0)$;            //$x$ is a $8 \times 16$ bits matrix state.
while $0 < \delta \leq N_s$ do
    while $0 < r \leq N_r$ do
        $\rho = 2 \times (\delta - 1) + r$;     //$N_r$ is the number of rounds per step.
        while $0 \leq j < 16$ do
            $x_\star[j] = S(x_\star[j])$;        //S-box Layer Operation.
        end while
        $x \Leftarrow x \oplus RC(\rho)$;
        while $0 \leq i < 8$ do
            $x_i[\star] = L(x_i[\star])$;        //L-box Layer Operation.
        end while
    end while
    $x \Leftarrow x \oplus TK(\delta)$;          //Tweakey addition Operation.
end while
*return* $x$
```

4.2 A slightly modified variant of iSCREAM

To demonstrate a practical application of our attack, we consider a minor modification of iSCREAM block cipher which shares the same round function and key schedule algorithm as original iSCREAM. However, the only difference is that the new round constants $RC(\rho, \alpha)$ are selected according to the following rules:
(1) Let $C(\rho) = 27 \cdot \rho \bmod 256$, where the binary representation of $C(\rho)$ is the first byte of $RC(\rho, \alpha)$ after being XORed with the first byte of the first row of state x.
(2)The fifth row and seventh row of $RC(\rho, \alpha)$ are all-one vectors in even rounds only, otherwise these are all-zero vectors. Denoting $\alpha = (1, 1, \ldots, 1) \in GF(2)^{16}$, the addition $x \oplus RC(\rho, \alpha)$ implies that $\alpha \oplus x_5[\star]$ and $\alpha \oplus x_7[\star]$ is performed in each even round, where $x_5[\star]$ and $x_7[\star]$ are the fifth and seventh row of the state x, respectively. The state x is unaffected in odd rounds since formally α is then the all-zero vector.

This slightly more complex procedure of deriving round constants may appear to be more secure but we demonstrate that one can efficiently mount generalized nonlinear invariant attacks, whereas the second rule above implies that the nonlinear invariants proposed by Todo *et al.* in [TLS16] [TLS18] are nonlinearly affected by round constants (this can be easily verified) so that their attack cannot be applied in this case.

4.3 An application of GNIA to the considered variant of iSCREAM

The linear layer of iSCREAM actually achieves diffusion by means of an orthogonal matrix, as described in the previous section. Therefore, by Theorem 1, to identify generalized nonlinear invariants for the round function of the considered variant of iSCREAM we need to search for quadratic Boolean functions $g' \in U(S, a_1, a_2)$ of the S-box S. By computer simulations (using the Gaussian elimination method), we have the following observation.

Let $x_\star[j], y_\star[j] = S(x_\star[j]) \in GF(2)^8$, for $j = 1, \ldots, 16$. Let again $x_i[j], y_i[j] \in GF(2)$, for $j \in \{1, \ldots, 16\}$ and $i \in \{1, \ldots, 8\}$ denote the i-th bit of $x_\star[j]$ and $y_\star[j]$, respectively. The least significant bit is on the right so that $(y_8[j], \ldots, y_1[j]) = S(x_8[j], \ldots, x_1[j])$. Then, the S-boxes of iSCREAM admit a quadratic nonlinear invariant given by

$g'(x_\star[j]) = x_1[j] \oplus x_3[j] \oplus x_6[j] \oplus x_8[j] \oplus x_5[j] \cdot x_6[j] \oplus x_6[j] \cdot x_7[j] \in U(S, a_1 = (1, 1, 0, 1, 1, 0, 1, 1),\ a_2 = (0, 0, 0, 0, 0, 1, 1, 1))$.

Using Theorem 1, one can easily verify that the Boolean function

$$g(x \oplus a_1^*) = \textstyle\sum_{j=1}^{16} g'(x_\star[j] \oplus a_1),$$

is a generalized nonlinear invariant for the round function of iSCREAM, where $x \in GF(2)^{8\times 16}$ and $a_1^* = (a_1, \ldots, a_1) \in GF(2)^{8\times 16}$. More precisely, since $\sum_{j=1}^{16} g'(x_\star[j] \oplus a_1) = \sum_{j=1}^{16} g'(y_\star[j] \oplus a_2)$, after some manipulation it can be further deduced that

$$g(x \oplus a_1^*) = g(\mathcal{S}(x) \oplus a_2^*) = g(y \oplus a_2^*),$$

where $\mathcal{S}(x)$ represents the S-box layer and $a_2^* = (a_2, \ldots, a_2) \in GF(2)^{8\times 16}, y = \mathcal{S}(x) \in GF(2)^{8\times 16}$.

Let $\gamma = (0, \ldots, 0) \in GF(2)^{16}$ or $\gamma = (1, \ldots, 1) \in GF(2)^{16}$, then $L^{-1}(\gamma) = \gamma$, where $L^{-1}(x)$ is the inverse permutation of the 16-bit linear layer of iSCREAM. The Observation 2 is easily verified since the linear layer of iSCREAM uses a particular orthogonal matrix always having odd Hamming weight in each column (or row).

Next, we need to show that these functions are also generalized nonlinear invariants taking into account both the addition of round constant and tweakey addition. Notice that for the tweakey addition operation defined by (8), one can impose certain constraints on the selection of the key and tweak so that

$K_5[\star] = (1, \ldots, 1) \in GF(2)^{16}, K_6[\star] = (0, \ldots, 0) \in GF(2)^{16}, K_7[\star] = (1, \ldots, 1) \in GF(2)^{16},$

$T_5[\star] = (1, \ldots, 1) \in GF(2)^{16}, T_6[\star] = (0, \ldots, 0) \in GF(2)^{16}, T_7[\star] = (1, \ldots, 1) \in GF(2)^{16}$.

On the other hand, the round constant $C(\rho)$ of iSCREAM (of size one byte) is XORed only with the first byte of the first row of x, thus only affecting $x_1[j]$ which is not contained (as a monomial) in the nonlinear terms of g. Moreover, since in even rounds of our modified version of iSCREAM the values $RC_5[\star] = RC_7[\star] = (1, \ldots, 1) \in GF(2)^{16}$ are used (in the S-box layer) then their impact on the nonlinear terms of g can be completely eliminated by performing the operation

$$a_1^* \oplus a_2^* \oplus RC(\rho, \alpha) \oplus L^{-1}(TK(\delta)) = a_1^* \oplus a_2^* \oplus RC(\rho, \alpha) \oplus TK(\delta), \tag{9}$$

where (see Observation 2) $(TK(\delta))_u[\star] = T_u[\star] \oplus K_u[\star] = (0, \ldots, 0) \in GF(2)^{16}$, for $u \in \{5, 6, 7\}$. Similarly, using $RC_5[\star] = RC_7[\star] = (0, \ldots, 0) \in GF(2)^{16}$ in odd rounds, their impact on the nonlinear terms of g can also be completely eliminated by performing (9) using now $(TK(\delta))_5[\star] = T_5[\star] = (1, \ldots, 1) \in GF(2)^{16}$, $(TK(\delta))_6[\star] = T_6[\star] = (0, \ldots, 0) \in GF(2)^{16}$, $(TK(\delta))_7[\star] = T_7[\star] = (1, \ldots, 1) \in GF(2)^{16}$.

Therefore, in the S-box layer, $a_1^* \oplus a_2^* \oplus RC(\rho, \alpha) \oplus L^{-1}(TK(\delta))$ only linearly affects g. i.e.

$$g(x \oplus a_1^* \oplus a_2^* \oplus RC(\rho, \alpha) \oplus L^{-1}(TK(\delta))) = g(x) \oplus g(a_1^* \oplus a_2^* \oplus RC(\rho, \alpha) \oplus L^{-1}(TK(\delta))),$$

where there are in total 2^{80} weak keys.

Let P^* and C^* respectively denote the plaintext and ciphertext of the considered variant of iSCREAM. In the so-called N_s-step mode of iSCREAM (see also Algorithm 1 and the case 2 in Proposition 1), it can be verified that (using $N_r = 1$) P^* and C^* are related as below:

$$g(P^* \oplus a_1^*) \oplus g(C^* \oplus a_1^*) = \sum_{\rho=1}^{N_s} g(a_1^* \oplus a_2^* \oplus RC(\rho, \alpha) \oplus L^{-1}(TK(\rho))). \tag{10}$$

If the user key belongs to the class of weak keys, then (10) is constant for all plaintexts, their corresponding ciphertexts and the given key. However, if the user key does not belong to the class of weak keys, then (10) is constant with a probability 2^{1-N} when N plaintext/ciphertext pairs are available. This observation immediately leads to an efficient distinguishing attack on this variant of iSCREAM.

Remark 3. *Assume instead that $N_r = 2$ and that the rule (2) in Section 4.2 is changed so that $RC_5[\star] = RC_7[\star] = \alpha = (1, \ldots, 1) \in GF(2)^{16}$ is used in each round. Then, even selecting $RC_2[\star], RC_3[\star], RC_4[\star]$, and $RC_8[\star]$ at random, our generalized nonlinear invariant attack can be still mounted on this variant of full-round iSCREAM cipher. Similarly to the attack above, we can impose certain constraints on the key and tweak so that $K_u[\star], T_u[\star] = (0, \ldots, 0) \in GF(2)^{16}$, for $u \in \{5, 6, 7\}$. In this case, one can verify that P^* and C^* are related as below:*

$$g(P^* \oplus a_1^*) \oplus g(C^* \oplus a_1^*) = \sum_{\rho=1}^{2N_s} g(RC(\rho, \alpha) \oplus a_1^* \oplus a_2^*) \oplus \sum_{\delta=1}^{N_s} g(TK(\delta)). \tag{11}$$

Remark 4. *Most interestingly, when $N_r = 1$, our generalized nonlinear invariant attack can be applied to the original full-round iSCREAM cipher.* More precisely, we impose the constraints so that $K_u[\star] = (0, \ldots, 0) \in GF(2)^{16}$, for $u \in \{5, 6, 7\}$, whereas $T_5[\star] = T_7[\star](1, \ldots, 1) \in GF(2)^{16}$, and $T_6[\star] = (0, \ldots, 0) \in GF(2)^{16}$. Then, it can be verified that P^* and C^* are related as below:

$$g(P^* \oplus a_1^*) \oplus g(C^* \oplus a_1^*) = \sum_{\rho=1}^{N_s} g(RC(\rho)) \oplus \sum_{\delta=1}^{N_s} g(L^{-1}(TK(\delta)) \oplus a_1^* \oplus a_2^*).$$

The attack is valid for the identified class of weak keys of size 2^{80}. It should be noticed that this class is completely different from the class of 2^{96} weak keys of iSCREAM used in the invariant subspace attack of Leander *et al.* [LMR15] and the class of 2^{97} weak keys in a nonlinear invariant attack due to Todo *et al.* [TLS18]. This demonstrates both the efficiency and authenticity of our approach compared to the previous methods.

5 Resistance against GNIA

In this section, we discuss the resistance of certain families of block ciphers against GNIA (using its extended framework given in Section 5.2) with regard to the choice of robust round constants. As an illustrative example, the resistance of a certain variant of the Midori block cipher (with different round constants) against the generalized nonlinear invariant attack is analyzed. Furthermore, we introduce a useful concept of so-called closed loop invariants and propose a new design criterion regarding the choice of round constants.

5.1 A brief description of a variant of Midori64

Recently, Beierle *et al.* [BCLR17] have investigated the resistance of block ciphers against the standard nonlinear invariant attacks from the security perspective related to a suitable choice of round constants. More precisely, assume that $k_i = k \oplus RC_i$ and $k_j = k \oplus RC_j$ are the subkeys of the i-th and j-th round, where RC_i and RC_j, respectively, are the corresponding round constants. Let D denote a set of the (XOR) difference between two round constants that are involved in rounds, where the same round key k (derived from the master key) is used, that is

$$D = \{(RC_i \oplus RC_j) = (k_i \oplus k_j) : k_i = k \oplus RC_i, k_j = k \oplus RC_j, 1 \leq i \neq j \leq m < N_s\},$$

where N_s is the number of iterative rounds of a given block cipher. If L stands for the linear layer operation of the block cipher, then the smallest L-invariant subspace of $GF(2)^n$ that contains D is denoted by $W_L(D)$. Note that $W_L(D)$ has two basic properties, namely it is a linear subspace of $GF(2)^n$ and secondly $W_L(D)$ is invariant under the operation L.

In order to resist standard nonlinear invariant attacks, it was suggested that the dimension of $W_L(D)$ (i.e., $\dim(W_L(D))$) should be sufficiently large. Optimally, $W_L(D)$ should cover the whole input space $GF(2)^n$. In particular, it was pointed out in [BCLR17] that the choice of round constants can be done independently of the substitution layer in many cases. However, in the framework of generalized nonlinear invariant attacks, we find that the choice of round constants may also depend on the substitution layer. In other words, a large dimension of $W_L(D)$ is not a sufficient condition to protect block ciphers against generalized nonlinear invariant attacks.

To justify the above statement, we analyze the robustness of a variant of Midori block cipher with respect to the choice of round constants. Midori is a lightweight block cipher proposed by Banik *et al.* in [BBI$^+$15] which is particularly suitable for resource-constrained environments. Midori has two versions, namely 64-bit block size (Midori64) and 128-bit block size (Midori128), both using a 128-bit secret key. Since we only consider the resistance of Midori64 against generalized nonlinear invariant attacks, we only briefly describe Midori64.

Midori64 uses an SPN structure and a very simple key schedule. The initial state of Midori64 can be seen as a 4×4-nibble array, which is updated by the round function. Initially, a 64-bit plaintext block of input data is entered to the initial state matrix and after that the key pre-whitening is performed. The state is then iteratively processed 16 times by applying the round function to it. Finally, the state is XORed with the post-whitening key, and the corresponding ciphertext is obtained (see the pseudocode of this algorithm below).

Algorithm 2 Midori-Core(X , WK, K_0, K_1 ,R)

```
$S \Leftarrow KeyAdd(X, WK)$;
while $0 \leq i \leq R-2$ do
    $S \Leftarrow SubCell(S)$;
    $S \Leftarrow ShuffleCell(S)$;
    $S \Leftarrow MixColumn(S)$;
    $S \Leftarrow KeyAdd(S, RK_i)$
end while
$S \Leftarrow SubCell(S)$
$Y \Leftarrow KeyAdd(S, WK)$
```

The round function of Midori64 consists of four operations, i.e., SubCell, ShuffleCell, Mixcolumn, and KeyAdd. These operations act as follows.

(1) **SubCell**: Each nibble of the state matrix is substituted by using the 4-bit S-box S specified in Table 2.

Table 2: S-box of Midori64

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S(x)$	C	A	D	3	E	B	F	7	8	9	1	5	0	2	4	6

(2) **ShuffleCell**: Let $s_0, s_1, \ldots, s_{15}$ be 16 nibbles of the state. The cell permutation is defined as

$$(s_0, s_1, \ldots, s_{15}) = (s_0, s_{10}, s_5, s_{15}, s_{14}, s_4, s_{11}, s_1, s_9, s_3, s_{12}, s_6, s_7, s_{13}, s_2, s_8).$$

This operation is similar to shiftRows in AES.

(3) **Mixcolumn**: Each column of the state is multiplied by a 4 × 4 orthogonal binary matrix M.

(4) **KeyAdd**: The state is XORed with the round key RK_i in round i.

In the key schedule algorithm of Midori64, the 128-bit master key is represented as $K = (K_0, K_1)$, where K_0 and K_1 are 64-bit keys. Then the round subkeys are generated as follows:

$$RK_i = K_{i\ mod\ 2} \oplus \alpha_i, \text{ for } i = 0, 1, \ldots, 14; \qquad WK = K_0 \oplus K_1,$$

where WK is the whitening key (only used in the first and last round) and each α_i is a fixed 64-bit constant for round i. In particular, each nibble of α_i is either 0001 or 0000, which is very helpful for keeping the energy consumption in hardware implementation low.

We now introduce a Midori64 variant, to demonstrate the efficiency of attacks based on the concept of closed-loop invariants, which shares the same round function and key schedule algorithm as the original Midori64. However, denoting $\alpha_i^* = (\alpha_i^{*1} || \cdots || \alpha_i^{*16})$, $\alpha{*}_i^j \in GF(2)^4$, for $i = 0, 1, \ldots, 14$ and $j = 1, \ldots, 16$, the only difference is that the round constants are now selected according to the following rules:
(1) If i mod $2 = 1$, the 1st and 3rd entry of $\alpha{*}_i^j$ are always 0.
(2) If i mod $2 = 0$, α_i^* can be chosen at random.

We notice that using the two rules above, one can easily select α_i^* so that $W_L(D) = \{(0000), (0001), \ldots, (1111)\}^{16}$ (viewed as sixteen times Cartesian product). In other words, a large dimension of $W_L(D)$ can be obtained, thus satisfying the criterion in [BCLR17].

5.2 Closed-loop invariants for the variant of Midori64

To discuss the generalized nonlinear invariant attack in a more general framework, we introduce a new concept of closed-loop invariants of an S-box. For any given S-box $S : GF(2)^n \longrightarrow GF(2)^n$, we define a closed-loop invariant as

$$CLI(S, g_1', g_2') = \{(g_1', g_2') \mid g_1'(x) \oplus g_2'(y) = c_1, g_2'(x) \oplus g_1'(y) = c_2, c_i \in GF(2), \forall x \in GF(2)^n\},$$

where $y = S(x)$ denotes the output of a given S-box.

Now for any generalized nonlinear invariant $g' \in U(S, a_1, a_2)$, let $g_1'(x) = g'(x \oplus a_1)$ and $g_2'(y) = g'(y \oplus a_2) = g'(S(x) \oplus a_2)$. It can be easily verified that g' satisfies

$$g_1'(x) \oplus g_2'(y) = g'(x \oplus a_1) \oplus g'(S(x) \oplus a_2) = c,$$

which is just a special case of the closed-loop invariant obtained when $g' = g_1' = g_2'$.

Moreover, the standard nonlinear invariant can be seen a special case of the closed-loop invariant of S-box when $g' = g_1' = g_2'$.

For the single S-box of Midori64 written as $S(x_4, \dots, x_1) = (y_4, \dots, y_1), x_i, y_i \in GF(2)$, where x_1 is the least significant bit, the functions

$$g_1'(x) = x_1 \oplus x_2 \oplus x_4 \oplus x_1x_3, \text{ and } \quad g_2'(y) = y_1 \oplus y_3$$

are such that $(g_1', g_2') \in CLI(S, g_1', g_2')$. By computer simulation (a standard search by varying the possible coefficients of the algebraic normal form of quadratic functions), the following equations are then valid

$$g_1'(x_4, \dots, x_1) \oplus g_2'(y_4, \dots, y_1) = 1, \quad g_2'(x_4, \dots, x_1) \oplus g_1'(y_4, \dots, y_1) = 1.$$

Notice that for odd i, the 1st and 3rd bit of α^{*j}_i are always 0 and these positions of constants α^{*j}_i are not contained in the nonlinear terms of the closed-loop invariant $CLI(S, g_1', g_2')$. Also, the ShuffleCell operation does not affect the closed-loop invariant. Moreover, the binary matrix M used in Mixcolumn operation is orthogonal. Therefore, the following Boolean functions:

$$g_1(X) = \sum_{j=1}^{16} g_1'(X_j), \quad g_2(X) = \sum_{t=1}^{16} g_2'(X_t), \quad X_j, X_t \in GF(2)^4,$$

constitute the closed-loop invariant of the round function $Y = F(X)$, where $X = (X_1, \dots, X_{16}) \in GF(2)^{64}, Y = (Y_1, \dots, Y_{16}) \in GF(2)^{64}$. More precisely, we have the following relationship:

$$g_1(X) \oplus g_2(Y) = 0, \quad g_1(Y) \oplus g_2(X) = 0.$$

5.3 A distinguishing attack on the variant of Midori64

Similarly to the discussion in Section 4.2, a distinguishing attack on the variant of Midori64 can be mounted under the weak key assumption. Let $\ell(X)$ be the linear part of g_1. We have $g_1(P) \oplus g_1(C) = Const.$, and this $Const.$ is actually a linear combination of certain parameters involved in the round function in the full encryption process. This fact can be justified as follows. Assume X^i is the output of i-th round after the **KeyAdd** operation, i.e. $X^i = F(X^{i-1}) \oplus RK_i$. We again denote by $\mathcal{S}(X)$ the output of the S-box layer and by $F(X)$ the output of the round function. Then,

$$\begin{aligned}
g_1(C) &= g_1(\mathcal{S}(X^{14}) \oplus WK) \\
&= g_1(\mathcal{S}(X^{14})) \oplus \ell(WK) \\
&= g_2(X^{14}) \oplus \ell(WK) \\
&= g_2(F(X^{13}) \oplus RK_{14}) \oplus \ell(WK) \\
&= g_2(F(X^{13})) \oplus g_2(RK_{14}) \oplus \ell(WK) \\
&\vdots \\
&= g_1(P) \oplus \ell(WK) \oplus g_2(RK_0) \oplus \ell(RK_1) \cdots \oplus g_2(RK_{14}) \oplus \ell(WK).
\end{aligned}$$

Therefore,

$$Const. = g_1(C) \oplus g_1(P) = \ell(WK) \oplus g_2(RK_0) \oplus l(RK_1) \oplus \cdots \oplus g_2(RK_{14}) \oplus \ell(WK),$$

where $WK = (WK^1 || \cdots || WK^{16})$ and $RK_i = (RK_i^1 || \cdots || RK_i^{16})$, for $i = 0, 1, \ldots, 14$.

Moreover, since $RK_i = K_{i \ mod \ 2} \oplus \alpha^*{}_i$, we have

$$Const. = \ell(K_1) \oplus g_2(\alpha_0^*) \oplus \ell(\alpha_1^*) \oplus \cdots \oplus \ell(\alpha_{13}^*) \oplus g_2(\alpha_{14}^*),$$

where $K_1 = (K_1^1 || \cdots || K_1^{16})$, $\alpha_i^* = (\alpha^{*1}_i || \cdots || \alpha^{*16}_i)$. Finally, the adversary can get the equation $g_1(P) \oplus g_1(C) = Const.$ (for the Midori64 variant) which is always satisfied (for a weak key), whereas this happens with a probability 1/2 for a random permutation.

Considering our variant of Midori64, we observe that the round keys repeat each second round. We therefore define

$$D := \{\alpha_0^* \oplus \alpha_2^*, \alpha_0^* \oplus \alpha_4^*, \ldots, \alpha_0^* \oplus \alpha_{14}^*, \alpha_1^* \oplus \alpha_3^*, \alpha_1^* \oplus \alpha_5^*, \ldots, \alpha_1^* \oplus \alpha_{13}^*\}.$$

Using previously described rules to specify the round constants α^{*j}_i, one can easily obtain a large dimension of $W_L(D)$ by selecting some appropriate round constants, (note that some α_i^* can be chosen at random if the rules of Section 5.1 are used). Nevertheless, as demonstrated above, a large dimension of $W_L(D)$ is only a necessary condition to protect the block ciphers against generalized nonlinear invariant attacks (using the CLI framework), since there may exist linear closed-loop invariants for a given S-box. For instance, the linear invariant $g_2'(y) = y_1 \oplus y_3$ cannot be affected by any round constant.

In fact, both the attack on a variant of iSCREAM given in Section 4.3 (see Remark 3) and the attack in Section 5.3 on a variant of Midori64 indicate that a large dimension of $W_L(D)$ is only a necessary design criterion. Thus, having the round constants satisfying the subspace dimension criterion of Beierle *et al.* [BCLR17] does not necessarily protect block ciphers against GNIA (assuming the existence of closed-loop invariants).

5.4 A new design criterion for round constants

To obtain robust round constants, we recall the definition of linear structures of Boolean functions.

Definition 1. Let $f : GF(2)^n \rightarrow GF(2)$ be a Boolean function. Then, $\alpha \in GF(2)^n$ is called a linear structure of f if $f(x) \oplus f(x \oplus \alpha)$ is a constant function.

It is well-known that set of all linear structures builds a linear subspace of $GF(2)^n$ which we denote by $I(f)$, thus

$$I(f) = \{\alpha \mid f(x) \oplus f(x \oplus \alpha) = Const., \alpha \in GF(2)^n, x \in GF(2)^n\}.$$

Using the notion of linear structures, a new design criterion related to the choice of round constants can be formulated as follows.

Design criterion: *Assume that all closed-loop invariants of a given S-box have been identified. Then, one must ensure that for each closed-loop invariant (thus $CLI(S, g'_1, g'_2)$ where g'_1 and g'_2 are known) if g'_i is nonlinear, $i \in \{1, 2\}$, then the corresponding robust round constants should not be contained in $I(g'_i)$, $i \in \{1, 2\}$.*

As an example, the standard Midori64 uses the round constants such that only the least significant bit in each nibble possibly changes. For the nonlinear invariant $g' = x_1 \oplus x_2 \oplus x_3 \oplus x_3x_4$ in [TLS16], it is easily verified that the constant nibble (0001) of α_i belongs to $I(g)$. Then, the attack described in [TLS16] can be efficiently applied. However, for $g'_1 = x_1 \oplus x_2 \oplus x_4 \oplus x_1x_3$ specified in Observation 2, the same constant nibble (0001) of α_i is not in $I(g'_1)$. Therefore, the attack described in Section 5.3 cannot be applied to the standard Midori64.

Remark 5. *By computer simulations, it has been confirmed that the full versions of lightweight block ciphers PRESENT [BKL$^+$07], PRINCE [BCG$^+$12], and Lblock [WZ11] all have robust round constants which are resistant against generalized nonlinear invariant attacks.*

Remark 6. *Essentially closed-loop invariants can be easily generalized, for instance using three Boolean functions and similarly defining $CLI(S, g_1, g_2, g_3)$. In this case, the design criterion is accordingly adjusted ensuring that for each generalized closed-loop invariant $CLI(S, g_1, g_2, g_3)$, for known g'_1, g'_2, and g'_3, in the case g'_i is nonlinear the corresponding robust round constants should not be contained in $I(g'_i)$, for $i \in \{1, 2, 3\}$. However, finding closed-loop invariants in this case is probably much harder.*

6 Conclusions

To eliminate the impact from the round constants in standard nonlinear invariant attacks, we have introduced a generalized nonlinear invariant attack. A new framework for the generalized nonlinear invariant attack on SPN block ciphers has also been proposed. As an application example, a new distinguishing attack on a slightly modified variant of full-round iSCREAM cipher has been proposed. Moreover, the resistance of block ciphers against our generalized nonlinear invariant attack, taking into account the selection of round constants, has been investigated. Finally, a new design criterion regarding the choice of robust round constants (that render GNIA inefficient) has been presented.

Acknowledgements

The authors would like to thank Jiqiang Lu and Gregor Leander for their helpful comments on earlier versions of the paper. The authors would also like to thank Elmar Tischhauser and the anonymous reviewers for their valuable suggestions and comments.
Yongzhuang Wei and Tao Ye are supported in part by the National Key R&D Program of China (No. 2017YFB0802000) and in part by the Natural Science Foundation of China (Nos. 61572148, 61872103). Enes Pasalic is partly supported by the Slovenian Research Agency (research program P3-0384 and research project J1-9108).

References

[BBI$^+$15] Subhadeep Banik, Andrey Bogdanov, Takanori Isobe, Kyoji Shibutani, Harunaga Hiwatari, Toru Akishita, and Francesco Regazzoni. Midori: A Block Cipher for Low Energy. In *Advances in Cryptology - ASIACRYPT 2015 - 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, November 29 - December 3, 2015, Proceedings, Part II*, pages 411–436, 2015.

[BCG$^+$12] Julia Borghoff, Anne Canteaut, Tim Güneysu, Elif Bilge Kavun, Miroslav Knezevic, Lars R. Knudsen, Gregor Leander, Ventzislav Nikov, Christof Paar, Christian Rechberger, Peter Rombouts, Søren S. Thomsen, and Tolga Yalçin. PRINCE - A Low-latency Block Cipher for Pervasive Computing Applications - Extended Abstract. In *Advances in Cryptology - ASIACRYPT 2012 - 18th International Conference on the Theory and Application of Cryptology and Information Security, Beijing, China, December 2-6, 2012. Proceedings*, pages 208–225, 2012.

[BCLR17] Christof Beierle, Anne Canteaut, Gregor Leander, and Yann Rotella. Proving Resistance Against Invariant Attacks: How to Choose the Round Constants. In *Advances in Cryptology - CRYPTO 2017 - 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2017, Proceedings, Part II*, pages 647–678, 2017.

[BKL$^+$07] Andrey Bogdanov, Lars R. Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew J. B. Robshaw, Yannick Seurin, and C. Vikkelsoe. PRESENT: An Ultra-lightweight Block Cipher. In *Cryptographic Hardware and Embedded Systems - CHES 2007, 9th International Workshop, Vienna, Austria, September 10-13, 2007, Proceedings*, pages 450–466, 2007.

[BS90] Eli Biham and Adi Shamir. Differential Cryptanalysis of DES-like Cryptosystems. In *Advances in Cryptology - CRYPTO '90, 10th Annual International Cryptology Conference, Santa Barbara, California, USA, August 11-15, 1990, Proceedings*, pages 2–21, 1990.

[BW99] Alex Biryukov and David A. Wagner. Slide Attacks. In *Fast Software Encryption, 6th International Workshop, FSE '99, Rome, Italy, March 24-26, 1999, Proceedings*, pages 245–259, 1999.

[BW00] Alex Biryukov and David A. Wagner. Advanced Slide Attacks. In *Advances in Cryptology - EUROCRYPT 2000, International Conference on the Theory and Application of Cryptographic Techniques, Bruges, Belgium, May 14-18, 2000, Proceeding*, pages 589–606, 2000.

[CAE13] CAESAR - Competition for Authenticated Encryption: Security, Applicability, and Robustness. information available at http://competitions.cr.yp.to/caesar.html. 2013.

[DR02] Joan Daemen and Vincent Rijmen. *The Design of Rijndael: AES - The Advanced Encryption Standard*. Information Security and Cryptography. Springer, 2002.

[GLSV14a] Vincent Grosso, Gaëtan Leurent, François-Xavier Standaert, and Kerem Varici. LS-Designs: Bitslice Encryption for Efficient Masked Software Implementations. In *Fast Software Encryption - 21st International Workshop, FSE 2014, London, UK, March 3-5, 2014. Revised Selected Papers*, pages 18–37, 2014.

[GLSV14b] Vincent Grosso, Gaëtan Leurent, François-Xavier Standaert, and Kerem Varici. SCREAM v1. Submission to CAESAR competition. 2014.

[GLSV15] Vincent Grosso, Gaëtan Leurent, François-Xavier Standaert, and Kerem Varici. SCREAM v3. Submission to CAESAR competition. 2015.

[HKM95] Carlo Harpes, Gerhard G. Kramer, and James L. Massey. A Generalization of Linear Cryptanalysis and the Applicability of Matsui's Piling-Up Lemma. In *Advances in Cryptology - EUROCRYPT '95, International Conference on* *the Theory and Application of Cryptographic Techniques, Saint-Malo, France, May 21-25, 1995, Proceeding*, pages 24–38, 1995.

[HTW15] Tao Huang, Ivan Tjuawinata, and Hongjun Wu. Differential-Linear Cryptanalysis of ICEPOLE. In *Fast Software Encryption - 22nd International Workshop, FSE 2015, Istanbul, Turkey, March 8-11, 2015, Revised Selected Papers*, pages 243–263, 2015.

[KR96] Lars R. Knudsen and Matthew J. B. Robshaw. Non-Linear Approximations in Linear Cryptanalysis. In *Advances in Cryptology - EUROCRYPT '96, International Conference on the Theory and Application of Cryptographic Techniques, Saragossa, Spain, May 12-16, 1996, Proceeding*, pages 224–236, 1996.

[LAAZ11] Gregor Leander, Mohamed Ahmed Abdelraheem, Hoda AlKhzaimi, and Erik Zenner. A Cryptanalysis of PRINTcipher: The Invariant Subspace Attack. In *Advances in Cryptology - CRYPTO 2011 - 31st Annual Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2011. Proceedings*, pages 206–221, 2011.

[LH94] Susan K. Langford and Martin E. Hellman. Differential-Linear Cryptanalysis. In *Advances in Cryptology - CRYPTO '94, 14th Annual International Cryptology Conference, Santa Barbara, California, USA, August 21-25, 1994, Proceedings*, pages 17–25, 1994.

[LMR15] Gregor Leander, Brice Minaud, and Sondre Rønjom. A Generic Approach to Invariant Subspace Attacks: Cryptanalysis of Robin, iSCREAM and Zorro. In *Advances in Cryptology - EUROCRYPT 2015 - 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part I*, pages 254–283, 2015.

[Mat93] Mitsuru Matsui. Linear Cryptanalysis Method for DES Cipher. In *Advances in Cryptology - EUROCRYPT '93, Workshop on the Theory and Application of of Cryptographic Techniques, Lofthus, Norway, May 23-27, 1993, Proceedings*, pages 386–397, 1993.

[TLS16] Yosuke Todo, Gregor Leander, and Yu Sasaki. Nonlinear Invariant Attack - Practical Attack on Full SCREAM, iSCREAM, and Midori64. In *Advances in Cryptology - ASIACRYPT 2016 - 22nd International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, December 4-8, 2016, Proceedings, Part II*, pages 3–33, 2016.

[TLS18] Yosuke Todo, Gregor Leander, and Yu Sasaki. Nonlinear Invariant Attack: Practical Attack on Full SCREAM, iSCREAM, and Midori64. *Journal of Cryptology*, pages 1432–1378, Apr 2018.

[WZ11] Wenling Wu and Lei Zhang. Lblock: A Lightweight Block Cipher. In *Applied Cryptography and Network Security - 9th International Conference, ACNS 2011, Nerja, Spain, June 7-10, 2011. Proceedings*, pages 327–344, 2011.