New Observations on Invariant Subspace Attack

Yunwen Liu[a,b], Vincent Rijmen[a]

[a] *Dept. Electrical Engineering (ESAT), KU Leuven and imec, Leuven, Belgium*
[b] *College of Science, National University of Defense Technology, Changsha, China*

Abstract

Invariant subspace attack is a novel cryptanalytic technique which breaks several recently proposed lightweight block ciphers. In this paper, we propose a new method to bound the dimension of some invariant subspaces in a class of lightweight block ciphers which have a similar structure as the AES but with 4-bit Sboxes. With assumptions on the diffusion layer, the dimension of any invariant subspaces is at most 32 when the inputs into each Sboxes are linearly independent. The observation brings new insights about the invariant subspace attack, as well as lightweight countermeasures to enhance the resistance against it.

Keywords: Invariant subspace attack, AES-like, lightweight block ciphers

1. Introduction

Over the last few years, lightweight block ciphers have become the new trend of symmetric primitives which are suitable for various constrained environments [1, 2, 3, 4]. Performance always comes with a price. For the lightweight block ciphers, some of them trade in a tolerable amount of security margin under certain attack models to achieve improved performance in hardware implementation. Without an explicit guideline, it is an interesting question whether a slight change towards higher efficiency may have devastating consequences.

A new type of attack named invariant subspace attack [5] is of special interest. It was invented in the analysis of a lightweight block cipher PRINTcipher

Email address: yunwen.liu@esat.kuleuven.be (Yunwen Liu)

[6]. The discovery of invariant subspace attack often seems like ad-hoc, until a generic algorithm to detect the existence of the invariant subspaces was proposed in 2015 [7]. Another victim of the attack is a recently-proposed block cipher Midori[3, 8]. Unlike differential cryptanalysis [9] and linear cryptanalysis [10] which are extensively studied and comprehensively understood, a guideline of avoiding the invariant subspace attack needs to be drawn by a "provably secure" framework.

A short solution to resist invariant subspace attack is to use heavier key schedules or randomised constants. However, in lightweight designs, an ultra-light key schedule reduces the hardware cost greatly. In the meantime, there are designs without key schedule yet having shown no vulnerability to the invariant subspace attack so far, such as Fantomas [11].

In this paper, we focus on the lightweight AES-like ciphers with 4-bit Sboxes. It can be shown that the dimension of an invariant subspace is upper bounded by 32. Due to the fact that the majority of lightweight block ciphers follow a similar structure with the AES, it may cast light on the provable security framework against invariant subspace attack for lightweight designs.

The rest of this paper is organised as follows. In Section 2, we show the propagation of affine subspaces through a round function. Section 3 studies the invariant subspace in the AES-like lightweight block ciphers and new countermeasures. Finally, we conclude in Section 4.

2. Characterisation of Invariant Subspace Attack

We denote an n-bit vector in $\mathbb{F}_{2^n}$ by $x = (x_{n-1}, x_{n-2}, \ldots, x_0)$. An affine subspace of $\mathbb{F}_{2^t}^s$ is denoted by $W = (W_1, W_2, \ldots, W_s)$ where W_i is an affine subspace on $\mathbb{F}_{2^t}$. The cardinality of a set S is denoted by $|S|$. Denote by "$\cdot$" the inner product. For a vectorial boolean function f over $\mathbb{F}_n$, the component function f_λ is the boolean function $\lambda \cdot f$, where $\lambda \in \mathbb{F}_n$ is nonzero.

Suppose that the round function F is composed with an Sbox layer F_s, a linear layer F_l and a key addition F_k, where $F = F_k \circ F_l \circ F_s$. If there exists an

affine subspace $v + A$ such that it is stable under F, $F(v + A) = v + A$, then when the round key $k \in v + u + A$, we have $(F_l \circ F_s)(v + A) = u + A$. It means that the invariant subspace property in the round function of a key-alternating block cipher is equivalent to the propagation of special affine subspaces [5]. It is interesting to notice that the propagation of affine spaces is also discussed in other studies, such as plateau characteristics [12]. Since the inverse of a linear layer is also linear, one has $F_s(v + A) = F_l^{-1}(u) + F_l^{-1}(A)$. Therefore, next we will focus on the propagation of affine subspaces through a layer of Sboxes.

Definition 1. *Let f be a (nonlinear) function from $\mathbb{F}_{2^n}$ into $\mathbb{F}_{2^m}$. If an affine subspace $(v + A) \subseteq \mathbb{F}_{2^n}$ is mapped to $(u + B) \subseteq \mathbb{F}_{2^m}$ which is also an affine subspace, then $(v + A \to u + B)$ is called an affine subspace propagation.*

The linear relation $(v, w)-$linear in the Sboxes has been studied by Boura *et al.* in [14] where the component function of an Sbox $S_\lambda, \lambda \in W$ with $|W| = w$ is of degree at most 1 over all cosets of V with $|V| = v$. However, in most applications, the property only holds for certain cosets. Therefore, we introduce the following notion.

Definition 2. *Let f be a function from $\mathbb{F}_{2^n}$ into $\mathbb{F}_{2^m}$. Then, f is called linear with respect to (V, W) if there exist two affine subspaces $V \subseteq \mathbb{F}_{2^n}$ and $W \subseteq \mathbb{F}_{2^m}$ with $\dim V = v$ and $\dim W = w$, such that, for all $\lambda \in W$, f_λ has degree at most 1 on V.*

The propagation of affine subspaces through 4-bit Sboxes has been discussed with the difference distribution table by Guo *et al.* in [8], while in this paper, we aim to fit it into the framework of the criterion on linear relations in Sboxes [14]. For the sake of completeness, we present the following proposition.

Proposition 1. *Let S be an s-bit Sbox. Then the image of a 2-dimensional affine subspace $v+A$ under the Sbox is also an affine subspace $u+B$ of dimension 2 if and only if the Sbox is linear with respect to $(v + A, \mathbb{F}_{2^s})$.*

In most lightweight block cipher designs, optimal 3-bit and 4-bit Sboxes are usually adopted to obtain optimised performance in hardware. It is easy to show

that no optimal 4-bit Sbox admits 3-dimensional affine subspace propagations, while many transitions of 2-dimensional and 1-dimensional affine subspaces can be found. Hence, we focus on the 3-bit and 4-bit Sboxes in the sequel.

Theorem 1. *Let S be an optimal s-bit Sbox with $s = 3, 4$. Then the image of an affine subspace $v + A$ with dimension no larger than $s-1$ under the Sbox is also an affine subspace $u + B$ if and only if S is linear with respect to $(v + A, \mathbb{F}_{2^s})$.*

Proof. The proof follows from the transition of spaces in 3- and 4-bit Sboxes. □

Theorem 2. *Let $F = (S_0, S_1, \ldots, S_{b-1})$ be a layer of optimal s-bit ($s = 3, 4$) Sboxes. Then there exists an affine subspace $v+A = (v_0+A_0, v_1+A_1, \ldots, v_{b-1}+A_{b-1})$ whose image through the Sbox layer is also an affine subspace $u + B = (u_0 + B_0, u_1 + B_1, \ldots, u_{b-1} + B_{b-1})$ if and only if $v_i + A_i = \mathbb{F}_2^s$ or F restricted on $v_i + A_i$ is a linear transformation, $0 \leq i \leq b - 1$.*

3. Bounding the Invariant Subspaces in the AES-like* Ciphers

3.1. AES-like Ciphers*

The success of the AES invokes many designs taking a similar structure, to name but a few, LED [15], Midori [3] and KLEIN [16]. The states $(s_0, s_1, \ldots, s_{15})$ can be arranged by a 4×4 matrix, with each state being of 4-bit or 8-bit. The round function of an AES-like cipher includes SubByte (or SubCell), ShiftRow (or ShuffleCell), MixColumn, KeyAdd and ConstAdd. The first three operations are on 4-bit or 8-bit words, which means there are no bit-level operations. Here we focus on the lightweight AES-like ciphers with 4-bit Sboxes, and denote them by AES-like*.

*3.2. Bounds on Invariant Subspace Attacks in AES-like**

The invariant subspace attacks up-to-date are found in two ways, ad-hoc or heuristic search. Rather than checking possible attacks after every adjustment of parameters and components, it is preferable for designers to have a guideline of avoiding the existence of large invariant subspaces during the design process.

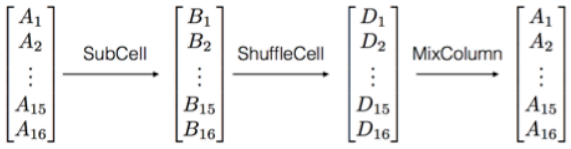

Figure 1: The propagation of affine subspaces in the AES-like* cipher.

Based on the characterisations in the previous section, we will show that the dimension of some invariant subspaces in AES-like* ciphers can be bounded.

Assume that there exists an invariant subspace $A = (A_1, A_2, \ldots, A_{16})$ in the round function of an AES-like* block cipher. We ignore the KeyAdd and ConstAdd for a moment, since they have no influence on the dimension of the affine subspaces. According to Theorem 2, the output sets after SubCell, ShuffleCell are also affine subspaces. Hence we denote the output sets B, D after SubCell and ShuffleCell by $B = (B_1, B_2, \ldots, B_{16})$ and $D = (D_1, D_2, \ldots, D_{16})$, as illustrated in Figure 1.

We limit the input space $A = (A_1, A_2, \ldots, A_{16})$ to be such that the restrictions A_i over each Sbox are linearly independent with each other. Then, we have the following bound on the dimension of the invariant subspaces.

Theorem 3. *Let f be the round function without key and constant addition of an AES-like* cipher with an MDS MixColumn layer. When the input space $A = (A_1, A_2, \ldots, A_{16})$ is such that the restrictions A_i over each Sbox are linearly independent with each other, the dimension of any invariant subspace is at most 32.*

Proof. We show that the restriction of the invariant subspace A over every Sbox is of dimension at most 2. Firstly, the subspaces propagating through 4-bit Sboxes are of dimension 1, 2, or 4, and the dimensions of the intermediate outputs through the Sbox layer remain the same, hence $\sum \dim(A_i) = \sum \dim(B_i)$. Note here that the sum of the dimensions of the restricted spaces only equals the dimension of the input space when the restrictions are linearly independent with each other. While the ShuffleCell operation simply permutes the cells, the only

operation that has an influence on the dimensions of the restricted subspaces is the MixColumn layer. For the four cells involved in a MixColumn operation, w.l.o.g (A_1, A_2, A_3, A_4), we consider the following cases.

Case 1. Suppose that there is one cell taking values of $\mathbb{F}_2^4$. Since all the entries in an MDS matrix are nonzero (the inverse of an MDS matrix is also MDS), the dimensions of $D_i, i = 1, 2, 3, 4$ are also 4.

Case 2. Suppose that there are two or three cells taking all values of $\mathbb{F}_2^4$. Since all the entries of the MDS matrix are nonzero, and the values in each cell are independent from other cells, the dimensions of $D_i, i = 1, 2, 3, 4$ are also 4.

So for **Case 1** and **2**, $\sum \dim(D_i) > \sum \dim(A_i)$. However, we know from the SubCell layer that $\sum \dim(A_i) = \sum \dim(B_i)$, thus $\sum \dim(D_i) > \sum \dim(B_i)$, which contradicts the fact that the ShuffleCell operation only permute the cells without changing their dimensions.

Case 3. Suppose that all four cells take values in $\mathbb{F}_2^4$, then the dimensions of $D_i, i = 1, 2, 3, 4$ are also 4. Recall that in the construction of the ShuffleCell, in order to achieve good diffusion, it is preferably to spread the cells from the same column into different columns. That is to say the cells of dimension 4 are distributed into 4 different columns. As a result, Case 3 is either a contradiction by Case 1 or a trivial case where all 16 cells receive inputs in $\mathbb{F}_2^4$.

To conclude, if there exists an invariant subspace in an AES-like* cipher with MDS MixColumn layer, every cell can only take a value from 2-dimensional subspaces, which means the total dimension is at most 32. □

There are also AES-like* lightweight proposals with non-MDS MixColumn layer such as Midori64 and Skinny64 [4]. Those diffusion layers have less structural properties to fit into a general conclusion. Here we take the round function of Midori64 without key and constant addition as an example. Assume that the input cells are linearly independent. Since the linear layer of Midori64 is NMDS, we consider the following cases inside a MixColumn operation as in the proof of Theorem 3.

Case 1. Suppose there is one cell taking values of $\mathbb{F}_2^4$, then three of the four

D_i's are of dimension 4.

Case 2. Suppose that there are two or three cells taking values of $\mathbb{F}_2^4$, and they are independent, then the dimensions of $D_i, i = 1, 2, 3, 4$ are also 4.

A similar contradiction can be deduced as in the proof of Theorem 3. Therefore, for the round function of Midori64 without the addition of keys and constants, if there are any invariant subspaces with independent input cells, each cell is of dimension at most 2. Recall that the round constants of Midori on each cell are 0 or 1, they are more likely to fall into some aforementioned invariant subspaces. It can also be seen as a general explanation of the "unfortunate combination of constants" as described in the discovery of the distinguisher [8].

3.3. Countermeasures and Discussions

Countermeasures to resist the invariant subspace attack can be deduced based on Theorem 3. Firstly we study the properties of the invariant subspaces in the keyless and constant-less round function of a given cipher, based on which a guideline for the choice of the constants can be deduced. For the round function of AES-like* ciphers with MDS MixColumn layer and Midori64, when considering the invariant subspaces with independent inputs on each cells, each cell should be of dimension at most 2.

As a consequence, we deduce a countermeasure as follows. Denote the set of the constants on a single cell over all rounds by C_{const}. The designer choose C_{const} such that there is no 2-dimensional subspace V of $\mathbb{F}_2^4$ satisfying

$$C_{const} \subseteq V.$$

To be specific, if the constants on the first cell s_0 are $\{1, 2, 3, 4, 5\}$ over the first five rounds, and clearly $\{1, 2, 3, 4, 5\}$ could not fall into any 2-dimensional subspaces, then the propagation of any nontrivial invariant subspaces with independent inputs on each cells will be blocked after five rounds. Hence, invariant subspace attack cannot be found for arbitrary number of rounds. It is obvious that this is much more lightweight compared with a heavier key schedule or complex constants.

Remark 1. *The bound and countermeasures are tailored for AES-like* primitives, which are suitable for the majority of current lightweight designs. While the bounding technique does not directly apply to bit-level operations, we leave the generalisation to bit-based designs as an open problem.*

4. Conclusion

In this paper, we study the property of the invariant subspace attacks for a type of SPN ciphers. We show that the existence of invariant subspaces is closely related to the previous framework of linear relations in the Sboxes. Furthermore, we prove that the dimension of possible invariant subspaces in the AES-like* ciphers can be bounded; hence a lightweight countermeasure is proposed.

Acknowledgements.

This work was supported in part by the Research Fund KU Leuven OT/13/071, the Flemish Government through FWO Thresholds G0842.13 and grant agreement No H2020-MSCA-ITN-2014-643161 ECRYPT-NET. Yunwen Liu is partially supported by China Scholarship Council (CSC 201403170380) and National Natural Science Foundation (No. 61672530).

References

[1] A. Bogdanov, L. R. Knudsen, G. Leander, *et al.*, PRESENT: An Ultra-Lightweight Block Cipher, in: CHES 2007, Springer, 2007, pp. 450–466.

[2] J. Borghoff, A. Canteaut, T. Güneysu, *et al.*, PRINCE– A Low-Latency Block Cipher for Pervasive Computing Applications, in: ASIACRYPT 2012, Springer, 2012, pp. 208–225.

[3] S. Banik, A. Bogdanov, T. Isobe, *et al.*, Midori: A Block Cipher for Low Energy, in: ASIACRYPT 2015, Springer, 2015, pp. 411–436.

[4] C. Beierle, J. Jean, S. Kölbl, *et al.*, The SKINNY Family of Block Ciphers and Its Low-Latency Variant MANTIS, in: CRYPTO 2016, Springer, 2016, pp. 123–153.

[5] G. Leander, M. A. Abdelraheem, H. AlKhzaimi, *et al.*, A Cryptanalysis of PRINTcipher: the Invariant Subspace Attack, in: CRYPTO 2011, Springer, 2011, pp. 206–221.

[6] L. Knudsen, G. Leander, A. Poschmann, *et al.*, PRINTcipher: A Block Cipher for IC-printing, in: CHES 2010, Springer, 2010, pp. 16–32.

[7] G. Leander, B. Minaud, S. Rønjom, A Generic Approach to Invariant Subspace Attacks: Cryptanalysis of Robin, iSCREAM and Zorro, in: EUROCRYPT 2015, Springer, 2015, pp. 254–283.

[8] J. Guo, J. Jean, I. Nikolić, *et al.*, Invariant Subspace Attack Against Midori64 and The Resistance Criteria for Sbox Designs, Cryptology ePrint Archive, Report 2016/973, 2016. `http://eprint.iacr.org/2016/973`.

[9] E. Biham, A. Shamir, Differential Cryptanalysis of DES-Like Cryptosystems, Journal of CRYPTOLOGY 4 (1991) 3–72.

[10] M. Matsui, Linear Cryptanalysis Method for DES Cipher, in: EUROCRYPT 1993, Springer, 1993, pp. 386–397.

[11] V. Grosso, G. Leurent, F.-X. Standaert, *et al.*, LS-designs: Bitslice Encryption for Efficient Masked Software Implementations, in: FSE 2014, Springer, 2014, pp. 18–37.

[12] J. Daemen, V. Rijmen, Plateau Characteristics, IET Information Security 1 (2007) 11–17.

[13] L. Grassi, C. Rechberger, S. Rnjom, Subspace Trail Cryptanalysis and its Applications to AES, Cryptology ePrint Archive, Report 2016/592, 2016. `http://eprint.iacr.org/2016/592`.

[14] C. Boura, A. Canteaut, A New Criterion for Avoiding the Propagation of Linear Relations Through an Sbox, in: FSE 2013, Springer, 2013, pp. 585–604.

[15] J. Guo, T. Peyrin, A. Poschmann, *et al.*, The LED block cipher, in: CHES 2011, 2011, pp. 326–341.

[16] Z. Gong, S. Nikova, Y. W. Law, KLEIN: A new family of lightweight block ciphers, in: RFIDSec 2011, 2011, pp. 1–18.