Information Processing Letters 138 (2018) 27–30

Contents lists available at ScienceDirect

Information Processing Letters

www.elsevier.com/locate/ipl

New observations on invariant subspace attack

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

[a] imec-COSIC KU Leuven, Leuven, Belgium
[b] College of Liberal Arts and Sciences, National University of Defense Technology, Changsha, China

ARTICLE INFO

Article history:
Received 29 January 2017
Accepted 29 January 2018
Available online 30 May 2018
Communicated by S. Faust

Keywords:
Cryptography
Invariant subspace attack
AES-like
Lightweight block ciphers

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.

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 [1–4]. 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 [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 $W = (W_1,$

E-mail addresses: yunwen.liu@esat.kuleuven.be (Y. Liu), vincent.rijmen@esat.kuleuven.be (V. Rijmen).

https://doi.org/10.1016/j.ipl.2018.01.015
0020-0190/

$W_2, \ldots, W_s$) 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 $(F_l \circ F_s) \times (v + A) = u + A$. 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 [13] 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 [13]. 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 $(v + A, \mathbb{F}_{2^s})$.*

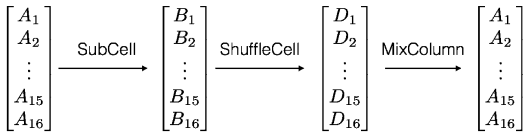

Fig. 1. The propagation of affine subspaces in the AES-like* cipher.

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, $0 \le i \le b - 1$.*

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 [14], Midori [3] and KLEIN [15]. 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. 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 Fig. 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.