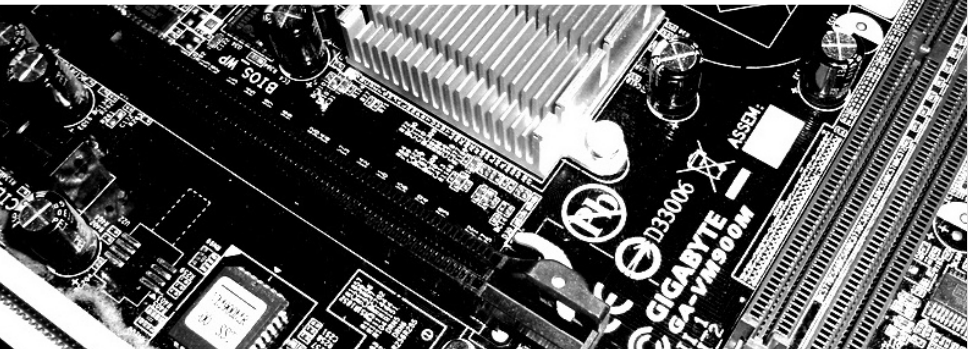


# Searching for Subspace Trails and Truncated Differentials

March 5th, 2018

Horst Görtz Institute for IT Security  
Ruhr-Universität Bochum

Gregor Leander, Cihangir Teczan, and *Friedrich Wiemer*

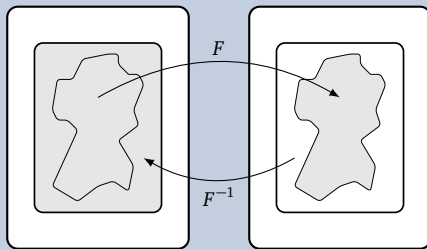


## Invariant Subspaces [Lea+11] (Crypto 2011)

Let  $U$  be a subspace of  $\mathbb{F}_2^n$ , and  $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ . We write  $U+a \xrightarrow{F} U+b$ , if

$$\exists a : \exists b : F(U+a) = U+b$$

## Main Idea



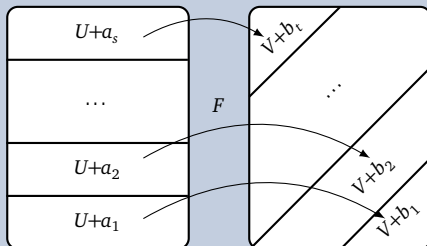
## Subspace Trail Cryptanalysis [GRR16] (Last Year's FSE)

Let  $U, V$  be subspaces of  $\mathbb{F}_2^n$ , and  $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ . We write  $U \xrightarrow{F} V$ , if

$$\forall a : \exists b : F(U+a) \subseteq V+b$$

We restrict ourselves to *essential* subspace trails.

## Main Idea



# The Problem

How to search efficiently for Subspace Trails?

## Security against Subspace Trails?

Given the round function  $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$  of an SPN cipher, prove the resistance against subspace trail attacks!

# The Problem

How to search efficiently for Subspace Trails?

## Security against Subspace Trails?

Given the round function  $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$  of an SPN cipher, prove the resistance against subspace trail attacks!

Main problem: Too many possible starting points.

Already for initially one-dimensional subspaces there are  $2^n$  possibilities.

Can't we just activate a single S-box and check to what this leads us?

# The Problem

How to search efficiently for Subspace Trails?

## Security against Subspace Trails?

Given the round function  $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$  of an SPN cipher, prove the resistance against subspace trail attacks!

Main problem: Too many possible starting points.

Already for initially one-dimensional subspaces there are  $2^n$  possibilities.

Can't we just activate a single S-box and check to what this leads us?

The short answer is:

No!<sup>1</sup>

---

<sup>1</sup>The long answer is this talk.

## Outline

- 1 Motivation
- 2 Intuition
- 3 Algorithm

# Preliminaries, Notations

## Subspace Complement

If  $U$  is a subspace of  $\mathbb{F}_2^n$ , we denote by  $U^\perp$  its *complement*:

$$U^\perp := \{u \in \mathbb{F}_2^n \mid \forall x \in U : \langle x, u \rangle = 0\}$$

## Derivative

Let  $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ . We denote the *derivative of  $F$  in direction  $u$*  by

$$\Delta_u(F)(x) := F(x) + F(x + u)$$

## Linear Structure

Let  $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ . Then  $(\alpha, u)$  is called a *linear structure*, if

$$\exists c \in \mathbb{F}_2 : \forall x \in \mathbb{F}_2^n : \langle \alpha, \Delta_u(F)(x) \rangle = c$$



# Intuition

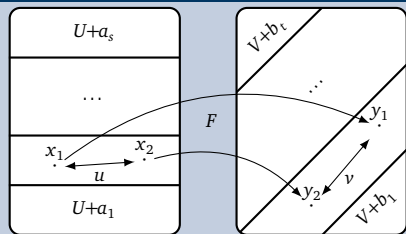
The Image of the Derivative is in the Subspace

## Lemma

Let  $U \xrightarrow{F} V$  be a subspace trail. Then

$$\forall u \in U : \text{Im}(\Delta_u(F)) \subseteq V.$$

## Remember:



## Proof

Let  $U \xrightarrow{F} V$ , then for every  $u \in U$

$$x \in U+x \xrightarrow{F} F(x) \in V+b,$$

$$x+u \in U+x \xrightarrow{F} F(x+u) \in V+b,$$

implying  $F(x) + F(x+u) \in V$ .  $\square$

# Link to Truncated Differentials

## Definition

Let  $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ . A *truncated differential* of probability one is a pair of affine subspaces  $U+t$  and  $V+t$ , s. t.

$$\forall u \in U : \forall x \in \mathbb{F}_2^n : \Delta_{u+s}(F)(x) \in V+t$$

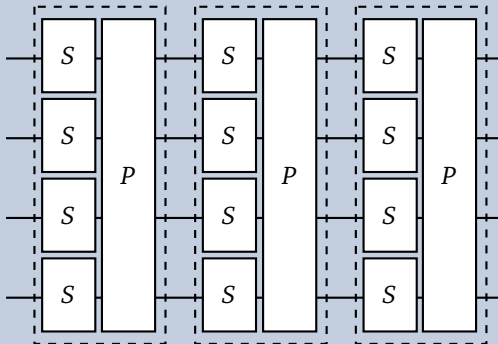
- Direct consequence from Lemma 1:

Link: Subspace Trails are Truncated Differentials with probability one

Let  $U \xrightarrow{F} V$  be a subspace trail. Then  $U+0$  and  $V+0$  are a truncated differential with probability one.

# Approach to the Algorithm

## SPN Structure



## Easy parts

- Given a starting subspace, computing the trail is easy.
- The effect of the linear layer  $P$  to a subspace  $U$  is clear:

$$U \xrightarrow{P} P(U)$$

## How to reduce the number of starting points?

Two possibilities, depending on the S-box  $S$ .

## Observation

For an S-box  $S$  and  $U \xrightarrow{S} V$ , because of the above lemma,

$$\begin{aligned} & \forall x, \forall u \in U : \Delta_u(S)(x) \in V \\ \Rightarrow & \forall \alpha \in V^\perp : \forall x, \forall u \in U : \langle \alpha, \Delta_u(S)(x) \rangle = 0. \end{aligned}$$

Thus,  $V^\perp$  consists of the linear structures of  $S$ .

## Theorem

*Let  $F : \mathbb{F}_2^{kn} \rightarrow \mathbb{F}_2^{kn}$  be an S-box layer that applies  $k$  S-boxes with no non-trivial linear structures in parallel. Then every essential subspace trail  $U \xrightarrow{F} V$  is of the form*

$$U = V = U_1 \times \cdots \times U_k,$$

*where  $U_i \in \{\{0\}, \mathbb{F}_2^n\}$ .*

# Possibility I

## Algorithm

- Simply activate single S-boxes
- Compute resulting subspace trail

## Complexity

Linear in the number of S-boxes.

In particular, in this case, bounds from activating single S-boxes are optimal.

This approach is independent of the S-box, i. e. any S-box without linear structures behaves the same with respect to subspace trails.

## Algorithm

- Simply activate single S-boxes
- Compute resulting subspace trail

## Complexity

Linear in the number of S-boxes.

In particular, in this case, bounds from activating single S-boxes are optimal.

This approach is independent of the S-box, i. e. any S-box without linear structures behaves the same with respect to subspace trails.

## The problem with S-boxes that have linear structures

Subspace trails through S-box layers with *one*-linear structures are not necessarily a direct product of subspaces (see e. g. Present).

# Possibility II

The long one, but only the idea

## Observation

If  $U_1 \xrightarrow{F} U_2$  is a subspace, then for any  $V_1 \subseteq U_1$  there exists a  $V_2 \subseteq U_2$ , s. t.  $V_1 \xrightarrow{F} V_2$ :

$$\begin{array}{ccc} U_1 & \xrightarrow{F} & U_2 \\ \cup & & \cup \end{array}$$

$$V_1 \xrightarrow{F} V_2$$

## Complexity (Size of $\mathbb{W}$ )

For an S-box layer  $F : \mathbb{F}_2^{kn} \rightarrow \mathbb{F}_2^{kn}$  with  $k$  S-boxes, each  $n$ -bit:  $|\mathbb{W}| = k \cdot 2^n$

## Algorithm Idea

- Find a good set  $\mathbb{W}$ , s. t. for any possible subspace trail over the S-box layer  $U \xrightarrow{F} V$ , there is an element  $W \in \mathbb{W}$  s. t.  $\{W\} \subseteq V$ .
- Compute the subspace trails for any starting point  $W \in \mathbb{W}$ .

## SPN ciphers with S-boxes without linear structures

| Cipher     | $r_e$ | $d$ | $r_d$ | $d$ |
|------------|-------|-----|-------|-----|
| AES        | 2     | 32  | 2     | 32  |
| Anubis     | 2     | 104 | —     | —   |
| Klein      | 3     | 60  | 2     | 32  |
| Kuznyechik | 1     | 8   | 1     | 8   |
| Prince     | 2     | 16  | 2     | 16  |
| Qarma      | 2     | 36  | 2     | 36  |



## SPN ciphers with S-boxes with linear structures

| Cipher    | LS    |     |       |     |
|-----------|-------|-----|-------|-----|
|           | $r_e$ | $d$ | $r_d$ | $d$ |
| Ascon     | 3     | 298 | 1     | 125 |
| Gift      | 3     | 60  | 3     | 60  |
| Keccak    | 2     | 546 | 1     | 169 |
| Present   | 3     | 43  | 3     | 63  |
| Pride     | 2     | 31  | 2     | 34  |
| Qarma     | 2     | 36  | 2     | 36  |
| Serpent   | 2     | 88  | 2     | 62  |
| Skinny64  | 5     | 48  | 5     | 48  |
| Skinny128 | 5     | 96  | 5     | 96  |

## SPN ciphers with S-boxes with linear structures

| Cipher    | LS    |     |       |     | No LS |      |       |     |
|-----------|-------|-----|-------|-----|-------|------|-------|-----|
|           | $r_e$ | $d$ | $r_d$ | $d$ | $r_e$ | $d$  | $r_d$ | $d$ |
| Ascon     | 3     | 298 | 1     | 125 | 3     | 310  | 1     | 155 |
| Gift      | 3     | 60  | 3     | 60  | 2     | 16   | 2     | 16  |
| Keccak    | 2     | 546 | 1     | 169 | 2     | 1290 | 1     | 270 |
| Present   | 3     | 43  | 3     | 63  | 2     | 16   | 2     | 16  |
| Pride     | 2     | 31  | 2     | 34  | 2     | 56   | 1     | 40  |
| Qarma     | 2     | 36  | 2     | 36  | 2     | 36   | 2     | 36  |
| Serpent   | 2     | 88  | 2     | 62  | 2     | 100  | 2     | 68  |
| Skinny64  | 5     | 48  | 5     | 48  | 4     | 48   | 4     | 48  |
| Skinny128 | 5     | 96  | 5     | 96  | 5     | 96   | 5     | 96  |

# Questions?

Thank you for your attention!



---

Mainboard & Questionmark Images: flickr

# References I

- [GRR16] L. Grassi, C. Rechberger, and S. Rønjom. "Subspace Trail Cryptanalysis and its Applications to AES". In: *IACR Trans. Symmetric Cryptol.* 2016.2 (2016), pp. 192–225. doi: 10.13154/tosc.v2016.i2.192-225.
- [Lea+11] G. Leander, M. A. Abdelraheem, H. AlKhzaimi, and E. Zenner. "A Cryptanalysis of PRINTcipher: The Invariant Subspace Attack". In: *CRYPTO*. Vol. 6841. LNCS. Springer, 2011, pp. 206–221. doi: 10.1007/978-3-642-22792-9\_12.