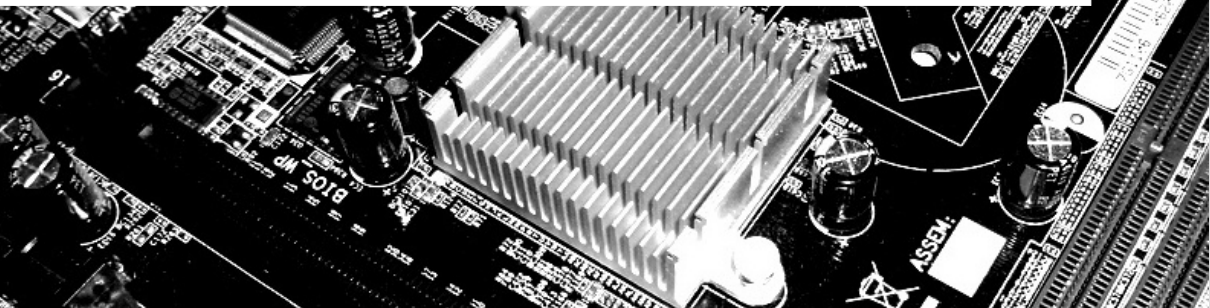


# Searching for Subspace Trails and Truncated Differentials

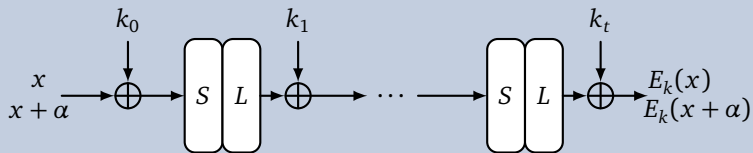
March 5th, 2018

Horst Görtz Institute for IT Security  
Ruhr-Universität Bochum

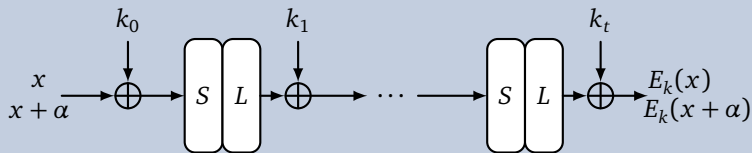
Gregor Leander, Cihangir Teczan, and *Friedrich Wiemer*



## SPN Cipher



## SPN Cipher



## Definition [Knu94; BLN14]

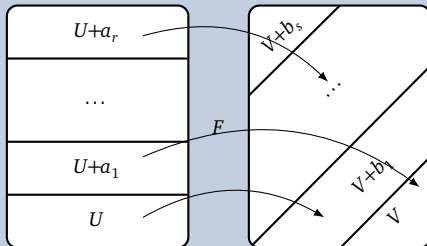
Let  $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ . A *truncated differential* of probability one is a pair of affine subspaces  $U+s$  and  $V+t$  of  $\mathbb{F}_2^n$ , s. t.

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

# Structural Attacks

## Subspace Trail Cryptanalysis

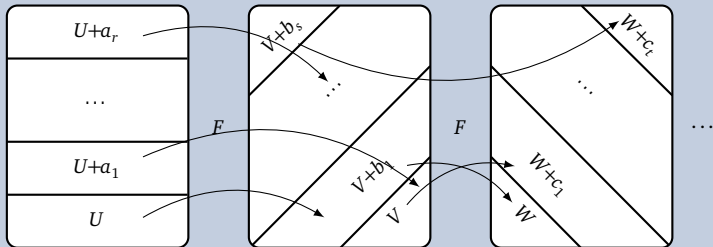
### Main Idea



# Structural Attacks

## Subspace Trail Cryptanalysis

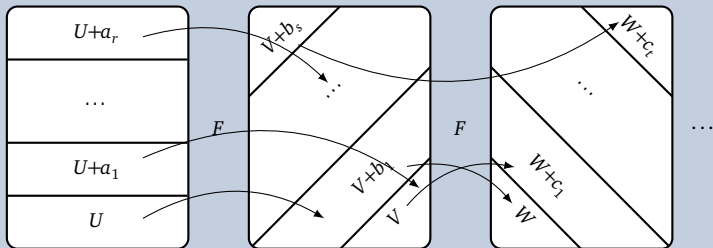
### Main Idea



# Structural Attacks

## Subspace Trail Cryptanalysis

### Main Idea



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

Let  $U_0, \dots, U_r \subseteq \mathbb{F}_2^n$ , and  $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ . We write  $U_0 \xrightarrow{F} \dots \xrightarrow{F} U_r$ , iff

$$\forall a \in U_i^\perp : \exists b \in U_{i+1}^\perp : F(U_i + a) \subseteq U_{i+1} + b$$

## Outline

- 1 Motivation
- 2 Link to Truncated Differentials
- 3 Security against Subspace Trail Attacks

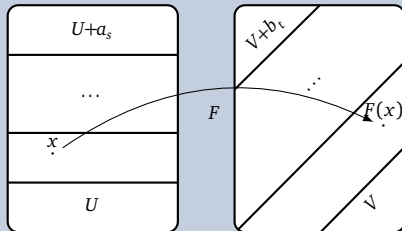
# Intuition

The Image of the Derivative is in the Subspace

## Lemma

Let  $U \xrightarrow{F} V$  be a subspace trail. Then for all  $u \in U$  and all  $x: F(x) + F(x + u) \in V$ .

## Proof





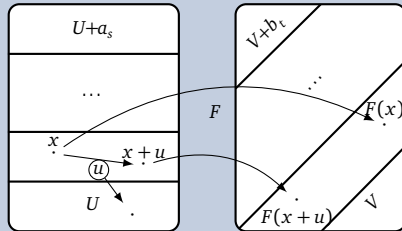
# Intuition

The Image of the Derivative is in the Subspace

## Lemma

Let  $U \xrightarrow{F} V$  be a subspace trail. Then for all  $u \in U$  and all  $x: F(x) + F(x + u) \in V$ .

## Proof



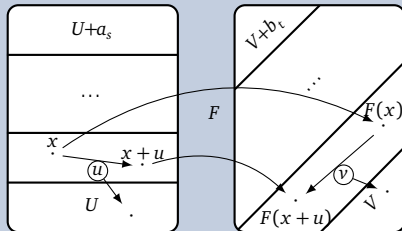
# Intuition

The Image of the Derivative is in the Subspace

## Lemma

Let  $U \xrightarrow{F} V$  be a subspace trail. Then for all  $u \in U$  and all  $x: F(x) + F(x + u) \in V$ .

## Proof



# Link to Truncated Differentials

Direct consequence from above Lemma

## Theorem (Subspace Trails are Truncated Differentials with probability one)

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

Then  $U+0$  and  $V+0$  form a truncated differential with probability one.

Subspace Trails are thus a special case of truncated differentials.

# Provable Resistant against Subspace Trails

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!

# Provable Resistant against Subspace Trails

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  $2^n - 1$  possibilities.

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

# Provable Resistant against Subspace Trails

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  $2^n - 1$  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>

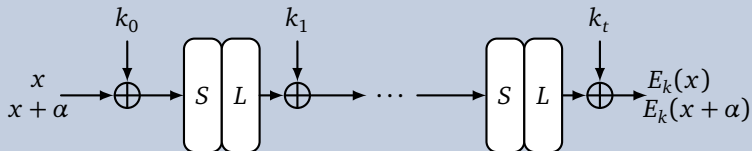
---

<sup>1</sup>The long answer is: Read our paper 😊

# Approach to the Algorithm

How to reduce the number of starting points?

## SPN Cipher



## Easy parts

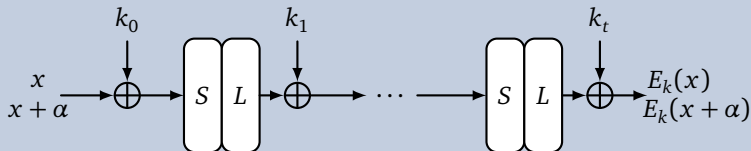
- Given a starting subspace, computing the trail is easy.
- The effect of the linear layer  $L$  to a subspace  $U$  is clear:

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

# Approach to the Algorithm

How to reduce the number of starting points?

## SPN Cipher



### Easy parts

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

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

### S-box: First Observation

For an S-box  $S$  and  $U \xrightarrow{S} V$ , because of the above lemma,  $\forall x \in \mathbb{F}_2^n$  and  $\forall u \in U$ :

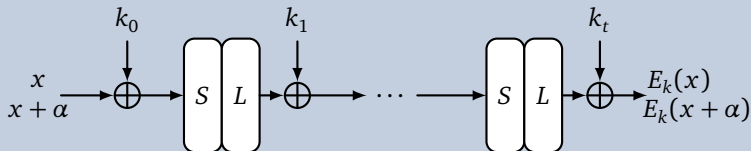
$$\begin{aligned} S(x) + S(x + u) &\in V \\ \Leftrightarrow \langle \alpha, S(x) + S(x + u) \rangle &= 0 \quad \forall \alpha \in V^\perp. \end{aligned}$$



# Approach to the Algorithm

How to reduce the number of starting points?

## SPN Cipher



### Easy parts

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

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

### S-box: First Observation

For an S-box  $S$  and  $U \xrightarrow{S} V$ , because of the above lemma,  $\forall x \in \mathbb{F}_2^n$  and  $\forall u \in U$ :

$$\begin{aligned} S(x) + S(x + u) &\in V \\ \Leftrightarrow \langle \alpha, S(x) + S(x + u) \rangle &= 0 \quad \forall \alpha \in V^\perp. \end{aligned}$$

By definition,  $V^\perp$  is the set of zero-linear structures of  $S$ .

# Possibility I

The short one

## 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.

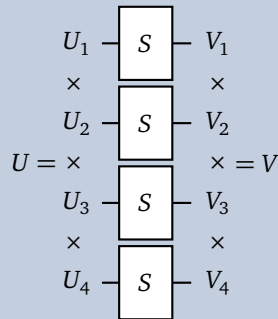
Then every essential subspace trail  $U \xrightarrow{F} V$  is of the form

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

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

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

## SPN Round: S-box layer



## Algorithm

- Simply (de-)activate S-boxes
- Compute resulting subspace trail

## Complexity (No. of starting $Us$ )

For  $k$  S-boxes:  $2^k$  (can be further decreased to  $k$ ).

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 (de-)activate S-boxes
- Compute resulting subspace trail

## Complexity (No. of starting $Us$ )

For  $k$  S-boxes:  $2^k$  (can be further decreased to  $k$ ).

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

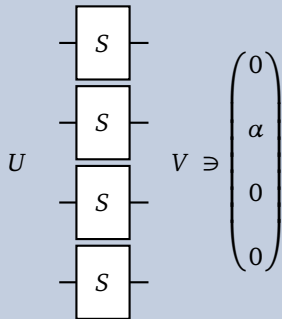
## The problem with S-boxes that have linear structures

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

# Possibility II

S-boxes with linear structures

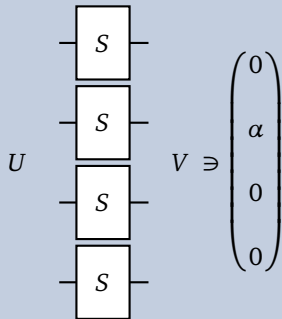
## Observation



# Possibility II

S-boxes with linear structures

## Observation



## Algorithm Idea

Compute the subspace trails for any starting point  $W_{i,\alpha} \in \mathbb{W}$ , with

$$W_{i,\alpha} := (0, \dots, 0, \underbrace{\alpha}_{i-1}, 0, \dots, 0)$$

## 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:  
 $|\mathbb{W}| = k \cdot (2^n - 1)$

# Conclusion/Questions

Thank you for your attention!

## Main Result

- Provable bound length of *every possible* subspace trail in SPN cipher

## Open Problems

- Other structures then SPNs?
- Truncated Differentials?



---

Mainboard & Questionmark Images: flickr

# References I

- [Knu94] L. R. Knudsen. "Truncated and Higher Order Differentials". In: *FSE'94*. Vol. 1008. LNCS. Springer, 1994, pp. 196–211. doi: 10.1007/3-540-60590-8\_16.
- [BLN14] C. Blondeau, G. Leander, and K. Nyberg. "Differential-Linear Cryptanalysis Revisited". In: *FSE'14*. Vol. 8540. LNCS. Springer, 2014, pp. 411–430. doi: 10.1007/978-3-662-46706-0\_21.
- [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.