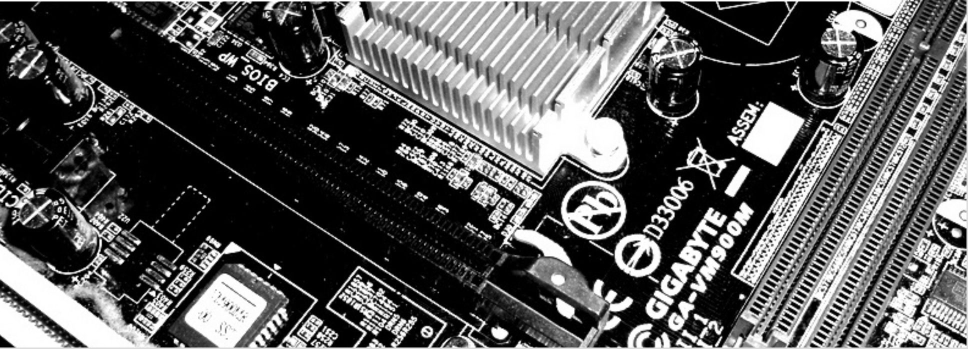
RUHR-UNIVERSITÄT BOCHUM

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*



Structural Attacks

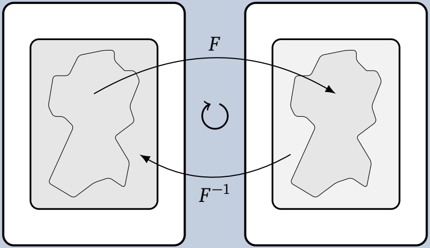
Invariant Subspaces

Invariant Subspaces [Lea+11] (Crypto 2011)

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

$$\exists a \in U^{\perp} : \exists b \in V^{\perp} : F(U{+}a) = U{+}b$$

Main Idea



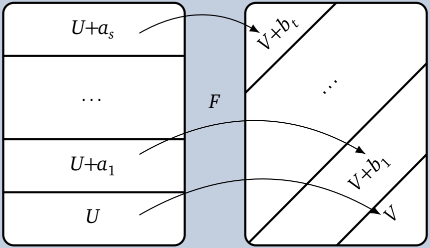
Subspace Trail Cryptanalysis [GRR16] (Last Year's FSE)

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

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

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

1

The Problem

How to search efficiently for Subspace Trails?

Security against Subspace Trails?

Given the round function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ 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?

1

The Problem

How to search efficiently for Subspace Trails?

Security against Subspace Trails?

Given the round function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ 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![1]

[1] The long answer is this talk.

Outline

RUB

Outline

Preliminaries, Notations

RUB

Subspace Complement

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

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

Derivative

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

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

Linear Structure

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$. Then (α, 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

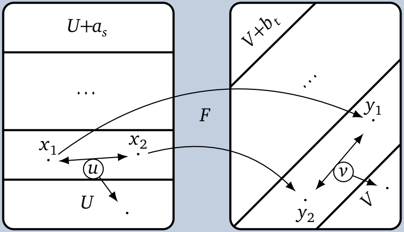
The Image of the Derivative is in the Subspace

Lemma

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

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

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 $F(x) + F(x+u) \in V$. □

Link to Truncated Differentials

RUB

Definition [Knu94; BLN14]

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

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

Link to Truncated Differentials

RUB

Definition [Knu94; BLN14]

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

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

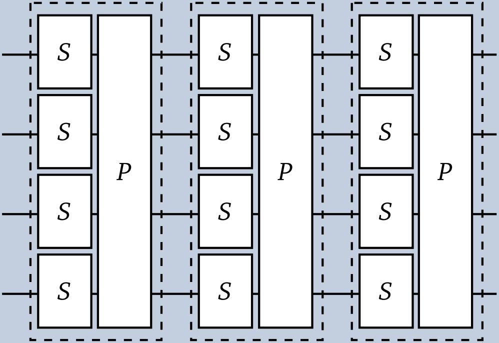
- Direct consequence from above Lemma:

Link: Subspaces 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 probabiliy 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.

Possibility I

The short one

Observation

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

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

Thus, $V^{\perp}$ consists of the (zero) linear structures of S.

Possibility I

The short one

RUB

Observation

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

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

Thus, $V^{\perp}$ consists of the (zero) linear structures of S.

Theorem

Let $F : \mathbb{F}_2^{kn} \to \mathbb{F}_2^{kn}$ 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 $U_i \in \left\{\{0\}, \mathbb{F}_2^n\right\}$.

Possibility I

Algorithm

RUB

Algorithm

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

Complexity (No. of starting Us)

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.

Possibility I
Algorithm

RUB

Algorithm

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

Complexity (No. of starting Us)

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. $V_1 \xrightarrow{F} V_2$:

$$\begin{array}{ccc} U_1 & \xrightarrow{F} & U_2 \\ \cup\!\mid & & \cup\!\mid \\ V_1 & \xrightarrow{F} & V_2 \end{array}$$

Possibility II

The long one, but only the idea

RUB

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. $V_1 \xrightarrow{F} V_2$:

$$\begin{array}{ccc} U_1 & \xrightarrow{F} & U_2 \\ \cup\!\mid & & \cup\!\mid \\ V_1 & \xrightarrow{F} & V_2 \end{array}$$

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

For an S-box layer $F : \mathbb{F}_2^{kn} \to \mathbb{F}_2^{kn}$ with k S-boxes, each n-bit: $|\mathbb{W}| = k \cdot (2^n - 1)$

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 $W \in \mathbb{W}$.

Questions?

Thank you for your attention!

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`.

[Lea+11] G. Leander, M. A. Abdelraheem, H. AlKhzaimi, and E. Zenner. “A Cryptanalysis of PRINTcipher: The Invariant Subspace Attack”. In: *CRYPTO’11*. Vol. 6841. LNCS. Springer, 2011, pp. 206–221. doi: `10.1007/978-3-642-22792-9_12`.

[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`.