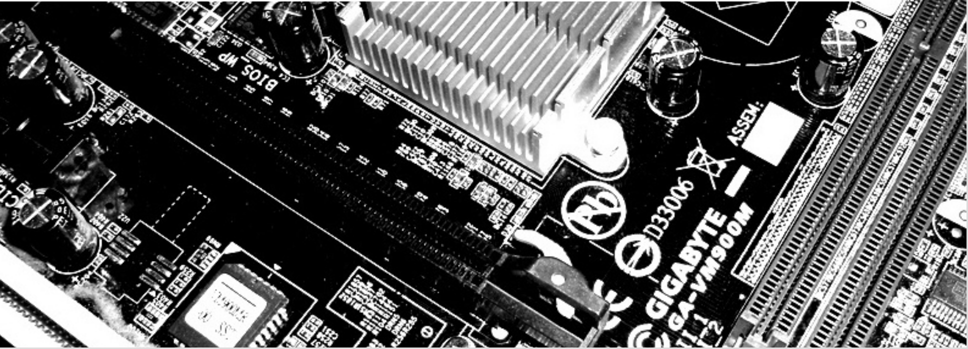
RUB

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*

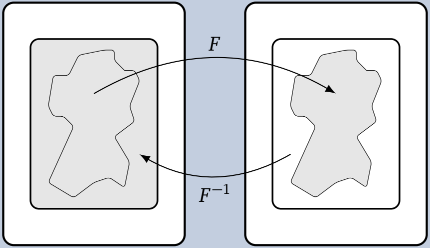


Invariant Subspaces [Lea+11] (Crypto 2011)

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

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

Main Idea



Structural Attacks

Subspace Trail Cryptanalysis

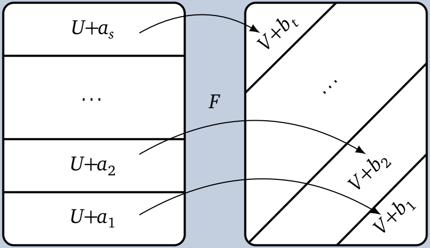
Subspace Trail Cryptanalysis [GRR16] (Last Year's FSE)

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

RUB

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 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?

RUB

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![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

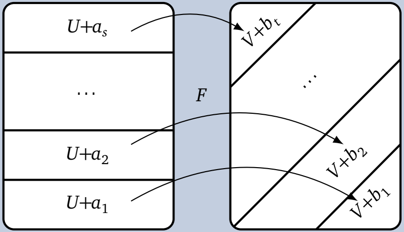
The Image of the Derivative is in the Subspace

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 $u \in U$

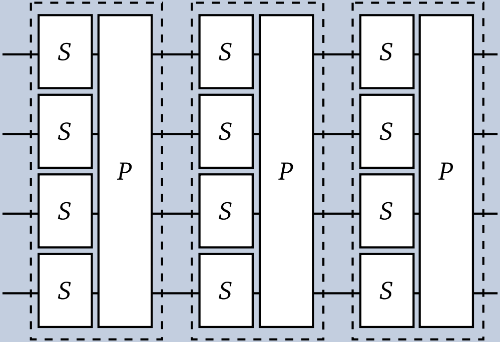
$$x \in U{+}x \xrightarrow{F} F(x) \in V{+}b,$$

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

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

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

RUB

Observation

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

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

Thus, $V^\perp$ consists of the 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

Algorithm

Simply activate single S-boxes.

The problem with S-boxes that have linear structures

Possibility II

The long one

RUB

Observation

If $U_1 \xrightarrow{F} U_2$ is a subspace, so is $V_1 \xrightarrow{F} V_2$:

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