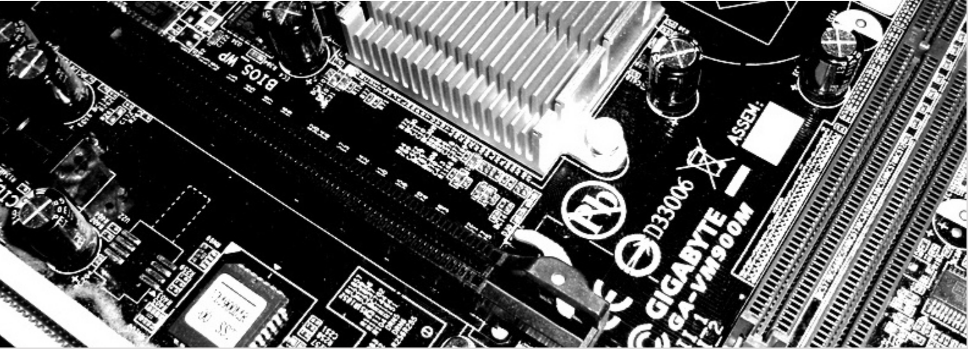
Searching for Subspace Trails and Truncated Differentials

March 5th, 2018

Horst Görtz Institute for IT Security
Ruhr-Universität Bochum
Gregor Leander, Cihangir Teczan, and *Friedrich Wiemer*



Structural Attacks

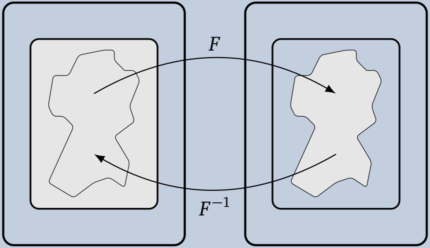
Invariant Subspaces

Invariant Subspaces [Lea+11] (Last Year's FSE)

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

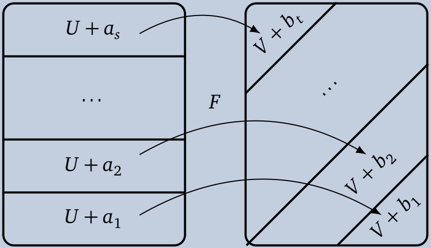


Subspace Trail Cryptanalysis [GRR16] (Last Year's FSE)

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

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

Main Idea



The Problem

How to search efficiently for subspace trails?

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

1 Motivation

2 Intuition

Preliminaries, Notations

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

Observation

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