RUHR-UNIVERSITÄT BOCHUM

Security Arguments and Tool-based Design of Block Ciphers

PhD Defense

December 13th, 2019

Arbeitsgruppe Symmetrische Kryptographie, Horst-Görtz-Institut für IT Sicherheit, Ruhr-Universität Bochum
Friedrich Wiemer

2019-11-27

Security Arguments and Tool-based Design of Block Ciphers


RUHR-UNIVERSITÄT BOCHUM
Security Arguments and Tool-based Design of Block Ciphers
PhD Defense
December 13th, 2019
Arbeitsgruppe Symmetrische Kryptographie, Horst-Görtz-Institut für IT Sicherheit, Ruhr-Universität Bochum
Friedrich Wiemer

The setting

Block Ciphers and Security Notion

RUHR-UNIVERSITÄT BOCHUM
The setting
Block Ciphers and Security Notion

Block Ciphers

RUHR-UNIVERSITÄT BOCHUM
Block Ciphers

Security

RUB

RUHR-UNIVERSITÄT BOCHUM
Security
RUB

Substitution Permutation Networks

RUHR-UNIVERSITÄT BOCHUM
Substitution Permutation Networks

Overview

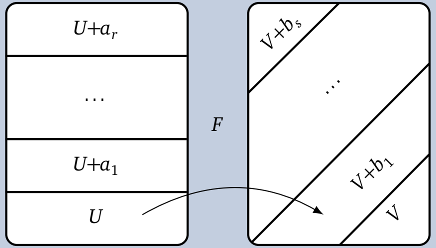
RUB

RUHR-UNIVERSITÄT BOCHUM
Overview
RUB
1 Introduction
2 Subspace Trail Attack
3 Security against Subspace Trail Attacks
4 Conclusion

Subspace Trail Cryptanalysis

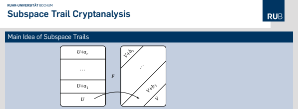
RUB

Main Idea of Subspace Trails



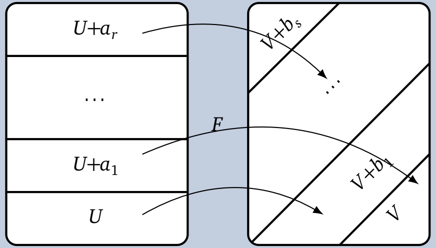
2019-11-27

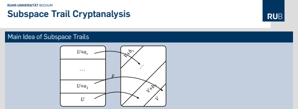
Security Arguments and Tool-based Design of Block Ciphers
└Subspace Trail Attack
└Subspace Trail Cryptanalysis



Subspace Trail Cryptanalysis

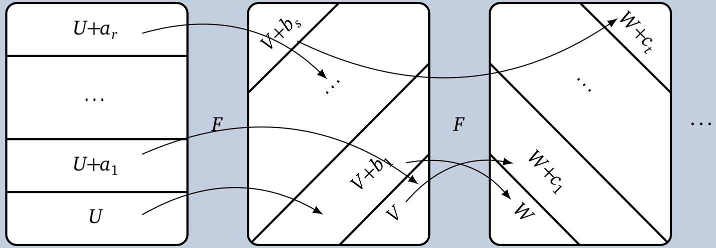
Main Idea of Subspace Trails





Subspace Trail Cryptanalysis

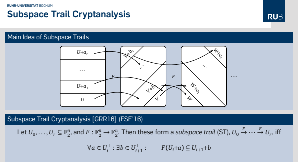
Main Idea of Subspace Trails



Subspace Trail Cryptanalysis [GRR16] (FSE'16)

Let $U_0, \dots, U_r \subseteq \mathbb{F}_2^n$, and $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$. Then these form a *subspace trail* (ST), $U_0 \xrightarrow{F} \cdots \xrightarrow{F} U_r$, iff

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



Our Goal

2019-11-27

Security Arguments and Tool-based Design of Block Ciphers
└─Subspace Trail Attack
└─Our Goal

RUHR-UNIVERSITÄT BOCHUM
Our Goal

Subspace Propagation

Given a starting subspace U, we can efficiently compute the corresponding longest subspace trail.

Lemma

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

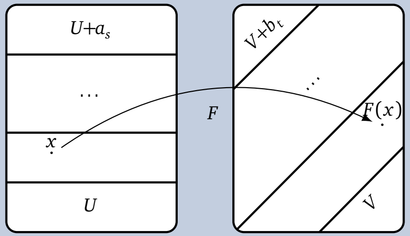
Subspace Propagation

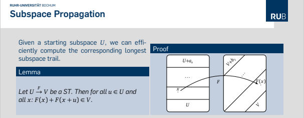
Given a starting subspace U, we can efficiently compute the corresponding longest subspace trail.

Lemma

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

Proof





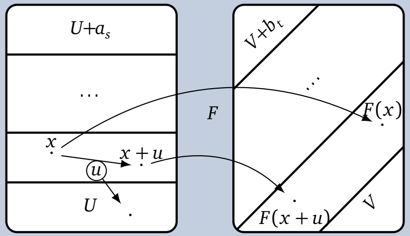
Subspace Propagation

Given a starting subspace U, we can efficiently compute the corresponding longest subspace trail.

Lemma

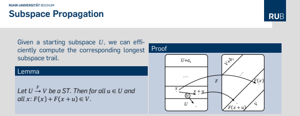
Let $U \xrightarrow{F} V$ be a ST. Then for all $u \in U$ and all x: $F(x) + F(x+u) \in V$.

Proof



2019-11-27

Security Arguments and Tool-based Design of Block Ciphers
└Subspace Trail Attack
└Subspace Propagation



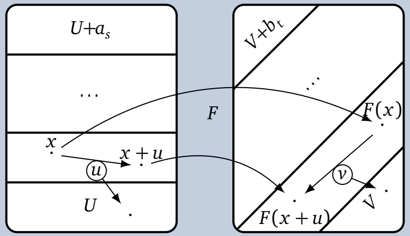
Subspace Propagation

Given a starting subspace U, we can efficiently compute the corresponding longest subspace trail.

Lemma

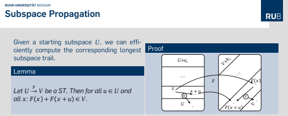
Let $U \xrightarrow{F} V$ be a ST. Then for all $u \in U$ and all x: $F(x) + F(x+u) \in V$.

Proof



2019-11-27

Security Arguments and Tool-based Design of Block Ciphers
└─Subspace Trail Attack
└─Subspace Propagation



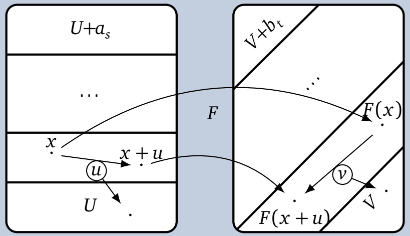
Subspace Propagation

Given a starting subspace U, we can efficiently compute the corresponding longest subspace trail.

Lemma

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

Proof

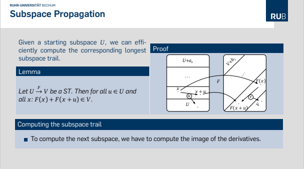


Computing the subspace trail

- To compute the next subspace, we have to compute the image of the derivatives.

2019-11-27

Security Arguments and Tool-based Design of Block Ciphers
└ Subspace Trail Attack
└ Subspace Propagation



Propagate a Basis

RUHR-UNIVERSITÄT BOCHUM
Propagate a Basis

`ComputeTrail` Algorithm

RUB

Computation of Subspace Trails

Input: A nonlinear function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, a subspace U.
Output: A subspace trail $U \rightrightarrows^F \cdots \rightrightarrows^F V$.

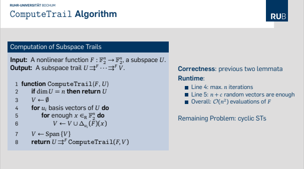
1 **function** $\texttt{ComputeTrail}(F, U)$
2 **if** $\dim U = n$ **then return** U
3 $V \leftarrow \emptyset$
4 **for** u_i basis vectors of U **do**
5   **for** enough $x \in_R \mathbb{F}_2^n$ **do**
6    $V \leftarrow V \cup \Delta_{u_i}(F)(x)$
7 $V \leftarrow \mathrm{Span}\{V\}$
8 **return** $U \rightrightarrows^F \texttt{ComputeTrail}(F, V)$

Correctness: previous two lemmata

Runtime:

- Line 4: max. n iterations
- Line 5: $n + c$ random vectors are enough
- Overall: $\mathcal{O}(n^2)$ evaluations of F

Remaining Problem: cyclic STs



How many random vectors are enough:
https://math.stackexchange.com/questions/564603/probability-that-a-random-binary-matrix-will-have-full-column-rank

How to Bound the Length of Subspace Trails

RUHR-UNIVERSITÄT BOCHUM
How to Bound the Length of Subspace Trails

Activating a single S-box only

RUHR-UNIVERSITÄT BOCHUM
Activating a single S-box only

The Connection to Linear Structures

RUHR-UNIVERSITÄT BOCHUM
The Connection to Linear Structures

S-boxes without Linear Structures

RUHR-UNIVERSITÄT BOCHUM
S-boxes without Linear Structures

S-boxes with Linear Structures

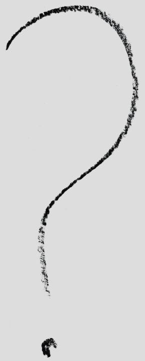
RUHR-UNIVERSITÄT BOCHUM
S-boxes with Linear Structures

Conclusion

Thanks for your attention!

Applications of ComputeTrail

- Bound longest probability-one subspace trail
- Link to Truncated Differentials
- Finding key-recovery strategies



Conclusion
Thanks for your attention!
Applications of ComputeTrail
Bound longest probability-one subspace trail
Link to Truncated Differentials
Finding key-recovery strategies

References I

References I