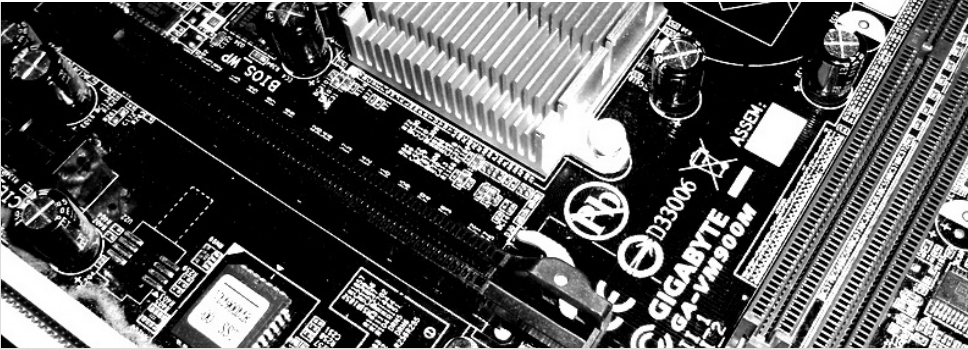
RUHR-UNIVERSITÄT BOCHUM

# The Invariant Set Attack

## 26th January 2017

**Workgroup Symmetric Cryptography**
**Ruhr University Bochum**

Friedrich Wiemer



# Nonlinear Invariant Attack

Practical Attack on Full SCREAM, iSCREAM, and Midori64

## Paper

- Todo, Leander, and Sasaki [TLS16] at AsiaCrypt'16
- Structural attack, brakes SCREAM, iSCREAM and Midori64 (surprise, surprise)[1] in the *weak key setting*

## Organisation

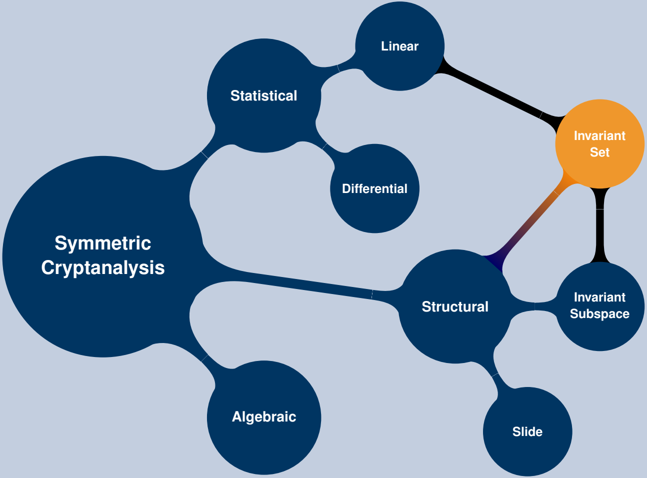


[1] Useless LaTeX Fact: Did you know that `\time` is an anagram of `\item`?

# Context

or: similar attacks?

## Attacks in Symmetric Cryptanalysis



# Linear Cryptanalysis

Taking the fun out of it

- invented by Matsui [Mat93]
- broke DES
- together with Differential Cryptanalysis best studied attack on block ciphers

Image: `http://www.isce2009.ryukoku.ac.jp/eng/keynote_address.html`

# Linear Cryptanalysis

Taking the fun out of it

## Core Idea

Given a block cipher $E_k : \mathbb{F}_2^n \to \mathbb{F}_2^n$, find an *input mask* $\alpha \in \mathbb{F}_2^n$ and an *output mask* $\beta \in \mathbb{F}_2^n$, s. t.

$$\langle \alpha, x \rangle \oplus \langle \beta, E_k(x) \rangle = c$$

holds with high probability for a constant $c$.

- $\alpha \xrightarrow{E_k} \beta$ is called a *linear approximation* of $E_k$
- much more to deal with: we have to keep the distribution over $k$ in mind and so on and so forth

# Invariant Subspace Attack
## Almost there

- invented by Leander *et al.* [Lea+11]
- broke PRINTCIPHER

Image: http://www.lightsec.org/2013/images/gregor_leander.jpg

# Invariant Subspace Attack

Almost there

## Core Idea

- ...

# Invariant Set Attack

## or: Nonlinear Invariant Attack

### Core Idea

Given a block cipher $E_k : \mathbb{F}_2^n \to \mathbb{F}_2^n$, s. t. $E_k(x) = E(x \oplus k)$, find an efficiently computable nonlinear Boolean function $g : \mathbb{F}_2^n \to \mathbb{F}_2$, s. t.

$$g(E(x \oplus k)) = g(x \oplus k) \oplus c = g(x) \oplus g(k) \oplus c \qquad (1)$$

for a constant $c$ and many $k$.

- $g$ is called *nonlinear invariant*
- keys for which Eq (1) holds are called *weak keys*

# Invariant Set Attack

## Step-by-Step

### Typical block cipher construction: key-alternating function

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ and $E_{k_1,k_2,\dots,k_r} : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be of the form

$$E_k(x) = F(\cdots F(x \oplus k_1) \cdots \oplus k_r).$$

# Invariant Set Attack

## Step-by-Step

Notation: we write $y_0 = x$, $y_i = F(y_{i-1} \oplus k_i)$, and thus $y_r = E_k(x)$.

### Nonlinear invariant for the round function

Assume there exists a nonlinear invariant $g$ for $F$, s. t. all keys $k_i$ are weak. Then:

# Invariant Set Attack

## Step-by-Step

Notation: we write $y_0 = x$, $y_i = F(y_{i-1} \oplus k_i)$, and thus $y_r = E_k(x)$.

### Nonlinear invariant for the round function

Assume there exists a nonlinear invariant $g$ for $F$, s. t. all keys $k_i$ are weak. Then:

$$g(E_k(x)) = g(y_r)$$

# Invariant Set Attack

## Step-by-Step

Notation: we write $y_0 = x$, $y_i = F(y_{i-1} \oplus k_i)$, and thus $y_r = E_k(x)$.

### Nonlinear invariant for the round function

Assume there exists a nonlinear invariant $g$ for $F$, s. t. all keys $k_i$ are weak. Then:

$$\begin{aligned} g(E_k(x)) &= g(y_r) \\ &= g(F(y_{r-1} \oplus k_r)) \end{aligned}$$

# Invariant Set Attack

## Step-by-Step

Notation: we write $y_0 = x$, $y_i = F(y_{i-1} \oplus k_i)$, and thus $y_r = E_k(x)$.

### Nonlinear invariant for the round function

Assume there exists a nonlinear invariant $g$ for $F$, s. t. all keys $k_i$ are weak. Then:

$$\begin{aligned} g(E_k(x)) &= g(y_r) \\ &= g(F(y_{r-1} \oplus k_r)) \\ &= g(y_{r-1}) \oplus g(k_r) \oplus c_r \end{aligned}$$

# Invariant Set Attack

## Step-by-Step

RUB

Notation: we write $y_0 = x$, $y_i = F(y_{i-1} \oplus k_i)$, and thus $y_r = E_k(x)$.

### Nonlinear invariant for the round function

Assume there exists a nonlinear invariant $g$ for $F$, s. t. all keys $k_i$ are weak. Then:

$$
\begin{aligned}
g(E_k(x)) &= g(y_r) \\
&= g(F(y_{r-1} \oplus k_r)) \\
&= g(y_{r-1}) \oplus g(k_r) \oplus c_r \\
&\vdots \\
&= g(x) \oplus \bigoplus_{i=1}^{r} g(k_i) \oplus c_1
\end{aligned}
$$

# Invariant Set Attack

## Weak Keys

It seems quite unlikely that Eq (1) holds for many $k$.

### Example nonlinear invariant

$$g : \mathbb{F}_2^4 \to \mathbb{F}_2$$
$$(x_4, x_3, x_2, x_1) \mapsto x_4 x_3 \oplus x_3 \oplus x_2 \oplus x_1$$

# Invariant Set Attack

## Weak Keys

It seems quite unlikely that Eq (1) holds for many $k$.

### Example nonlinear invariant

$$g : \mathbb{F}_2^4 \to \mathbb{F}_2$$
$$(x_4, x_3, x_2, x_1) \mapsto x_4x_3 \oplus x_3 \oplus x_2 \oplus x_1$$

### $g$ is nonlinear invariant for key xor and has 4 weak keys:

Split $g$ in a nonlinear part $f$ and a linear part $\ell$:

$$g(x_4, x_3, x_2, x_1) = f(x_4, x_3) \oplus \ell(x_2, x_1)$$

All $k$ of the form $k = (0, 0, k_2, k_1)$ are weak – and these are exactly four possible keys.

# Results

RUB

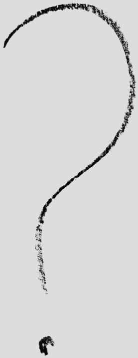
## Attack Complexities

| | # Weak $\mathtt{k}$ | max. # Recovered Bits |
|---|---|---|
| SCREAM | $2^{96}$ | 32 bits |
| iSCREAM | $2^{96}$ | 32 bits |
| Midori64 | $2^{64}$ | $32\mathtt{h}$ bits |

| | Data Complexity | Time Complexity |
|---|---|---|
| SCREAM | 33 ciphertexts | $32^3$ |
| iSCREAM | 33 ciphertexts | $32^3$ |
| Midori64 | $33\mathtt{h}$ ciphertexts | $32^3 \cdot \mathtt{h}$ |

# Questions?

## Thank you for your attention!



Mainboard & Questionmark Images: flickr

# References I

[Lea+11] G. Leander, M. A. Abdelraheem, H. AlKhzaimi, and E. Zenner. “A Cryptanalysis of PRINTcipher: The Invariant Subspace Attack”. In: *CRYPTO*. Vol. 6841. LNCS. Springer, 2011, pp. 206–221.

[Mat93] M. Matsui. “Linear Cryptanalysis Method for DES Cipher”. In: *EUROCRYPT*. Vol. 765. LNCS. Springer, 1993, pp. 386–397.

[TLS16] Y. Todo, G. Leander, and Y. Sasaki. “Nonlinear Invariant Attack - Practical Attack on Full SCREAM, iSCREAM, and Midori64”. In: *ASIACRYPT (2)*. Vol. 10032. LNCS. 2016, pp. 3–33.