Proving Resistance Against Invariant Attacks

How to Choose the Round Constants

Christof Beierle, Anne Canteaut, Gregor Leander and Yann Rotella

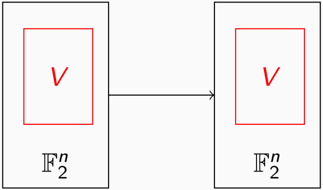
24 avril 2017

JC2 - La Bresse - France

Ruhr-Universität Bochum, Germany
Inria de Paris

The invariant supspace attack [Leander et al. 11]

Linear subspace $\boldsymbol{V}$ invariant under $\boldsymbol{E_k}$.

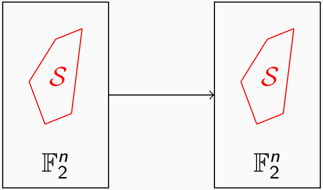


$$\boldsymbol{E_k}(\boldsymbol{V}) = \boldsymbol{V}$$

Table of contents

The nonlinear invariant attack [Todo, Leander, Sasaki 16]

Partition of $\mathbb{F}_2^n$ invariant under $\boldsymbol{E_k}$.



$$\boldsymbol{E_k(\mathcal{S}) = \mathcal{S}} \text{ or } \boldsymbol{E_k(\mathcal{S}) = \mathbb{F}_2^n \setminus \mathcal{S}}$$

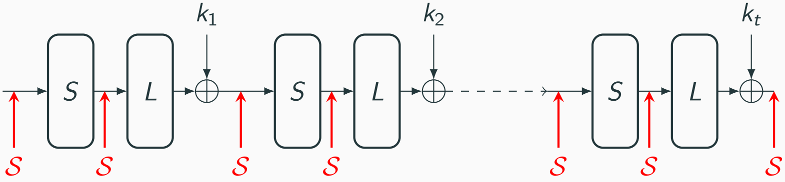
Definition (Invariant)

Let $\boldsymbol{g}$ a Boolean function such that $\boldsymbol{g(x) = 1}$ iff $\boldsymbol{x \in \mathcal{S}}$, then

$$\forall \boldsymbol{x} \in \mathbb{F}_2^n,\ \boldsymbol{g \circ E_k(x) + g(x) = c} \text{ with } \boldsymbol{c = 0} \text{ or } \boldsymbol{c = 1}$$

$\boldsymbol{g}$ is called an **invariant for $\boldsymbol{E_k}$.**

The case of SPN ciphers



Definition (linear structure)

$\mathbf{LS}(\boldsymbol{g}) = \{\alpha \in \mathbb{F}_2^{\boldsymbol{n}} : \boldsymbol{x} \mapsto \boldsymbol{g}(\boldsymbol{x} + \alpha) + \boldsymbol{g}(\boldsymbol{x}) \text{ is constant}\}$

Two conditions on $\boldsymbol{g}$

- $(\boldsymbol{k_i} + \boldsymbol{k_j})$ has to be a linear structure of $\boldsymbol{g}$.
- $\mathbf{LS}(\boldsymbol{g})$ is invariant under $\boldsymbol{L}$.

Simple key schedule

If $\boldsymbol{k_i} = \boldsymbol{k} + \boldsymbol{c_i}$,

$$\text{Let } \boldsymbol{D} = \{(\boldsymbol{c_i} + \boldsymbol{c_j})\} \text{ and}$$

$$\boldsymbol{W_L(D)} = \text{smallest subspace invariant under } \boldsymbol{L} \text{ which contains } \boldsymbol{D}.$$

Question

Is there a non-trivial invariant $\boldsymbol{g}$ for the Sbox-layer such that

$$\boldsymbol{W_L(D)} \subseteq \mathbf{LS}(\boldsymbol{g}) \text{ ?}$$

Proving resistance against the attack

The simple case

If $\dim W_L(D) \geq n - 1$,

Then the invariant attack does not apply.

- Skinny-64. $\mathbf{\dim W_L(D) = 64}$ ✓
- Prince. $\mathbf{\dim W_L(D) = 56}$ ✓+ other techniques
- Mantis-7. $\mathbf{\dim W_L(D) = 42}$ ✓+ other techniques
- Midori-64. $\mathbf{\dim W_L(D) = 16}$ ✗

Maximizing the dimension of $W_L(c)$

$$W_L(c) = \langle L^t(c), t \in \mathbb{N} \rangle$$

dim $W_L(c) =$ smallest d such that there exist $\lambda_0, \ldots, \lambda_d \in \mathbb{F}_2$:

$$\sum_{t=0}^{d} \lambda_t L^t(c) = 0$$

dim $W_L(c)$ is the degree of the minimal polynomial of c

Theorem

There exists c *such that* **dim** $W_L(c) = d$ *if and only if* d *is the degree of a divisor of the minimal polynomial of* L.

$$\max_{c \in \mathbb{F}_2^n} \dim W_L(c) = \deg \mathrm{Min}_L$$

How to choose better constants?

Example

- **LED.**
  $\mathrm{Min}_L = (X^8 + X^7 + X^5 + X^3 + 1)^4 (X^8 + X^7 + X^6 + X^5 + X^2 + 1)^4$
  then there exist some c such that $\dim W_L(c) = 64$
- **Skinny-64.** $\mathrm{Min}_L = X^{16} + 1 = (X + 1)^{16}$ then there exist some c such that $\dim W_L(c) = d$ for any $1 \leq d \leq 16$
- **Prince.**
  $\mathrm{Min}_L = (X^4 + X^3 + X^2 + X + 1)^2 (X^2 + X + 1)^4 (X + 1)^4$
  $\max_c \dim W_L(c) = 20$
- **Mantis and Midori.** $\mathrm{Min}_L = (X + 1)^6$
  $\max_c \dim W_L(c) = 6$

Rational canonical form

Definition

When $\mathbf{deg(Min}_L\mathbf{)} = \boldsymbol{n}$, $\boldsymbol{L}$ is equivalent to the companion matrix:

$$C(\mathrm{Min}_L) = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & & & & \\ 0 & 0 & 0 & \dots & 1 \\ p_0 & p_1 & p_2 & \dots & p_{n-1} \end{pmatrix}$$

More generally

$$\begin{pmatrix} C(Q_1) & & & \\ & C(Q_2) & & \\ & & \ddots & \\ & & & C(Q_r) \end{pmatrix}$$

$Q_1 = \mathrm{Min}_L$, Q_1, ... , Q_r are the invariant factors of $\boldsymbol{L}$,with $Q_r|..|Q_1$.

Example

For Prince.

$$\begin{aligned} \mathrm{Min}_L(X) &= X^{20}+X^{18}+X^{16}+X^{14}+X^{12}+X^{8}+X^{6}+X^{4}+X^{2}+1 \\ &= (X^4+X^3+X^2+X+1)^2(X^2+X+1)^4(X+1)^4 \end{aligned}$$

8 invariant factors:

$$\begin{aligned} Q_1(X) &= Q_2(X) \\ &= X^{20}+X^{18}+X^{16}+X^{14}+X^{12}+X^{8}+X^{6}+X^{4}+X^{2}+1 \\ Q_3(X) &= Q_4(X) = X^8+X^6+X^2+1 = (X+1)^4(X^2+X+1)^2 \\ Q_5(X) &= Q_6(X) = Q_7(X) = Q_8(X) = (X+1)^2 \end{aligned}$$

Maximizing the dimension of $W_L(c_1, \ldots, c_t)$

Theorem

Let $Q_1, Q_2, \ldots, Q_r$ be the r invariant factors of L. For any $t \leq r$,

$$\max_{c_1,\ldots,c_t} \dim W_L(c_1, \ldots, c_t) = \sum_{i=1}^{t} \deg Q_i.$$

We need r elements to get $W_L(D) = \mathbb{F}_2^n$.

For Prince.

For $t = 5$, $\max \dim W_L(c_1, \ldots, c_5) = 20 + 20 + 8 + 8 + 2 = 58$

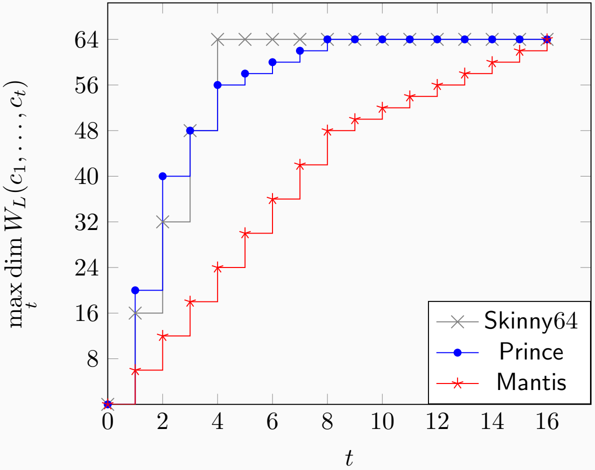
We need **8** elements to get the full space.

Mantis and Midori. $r = 16$ invariant factors

$Q_1(X) = \ldots, Q_8(X) = (X + 1)^6$ and $Q_9(X) = \ldots, Q_{16}(X) = (X + 1)^2$

We need **16** elements to get the full space.

Maximum dimension for $\#D$ constants



For random constants

For $t \geq r$,

$$\Pr_{c_1,\ldots,c_t \xleftarrow{\$} \mathbb{F}_2^n}[W_L(c_1,\cdots,c_t) = \mathbb{F}_2^n]$$

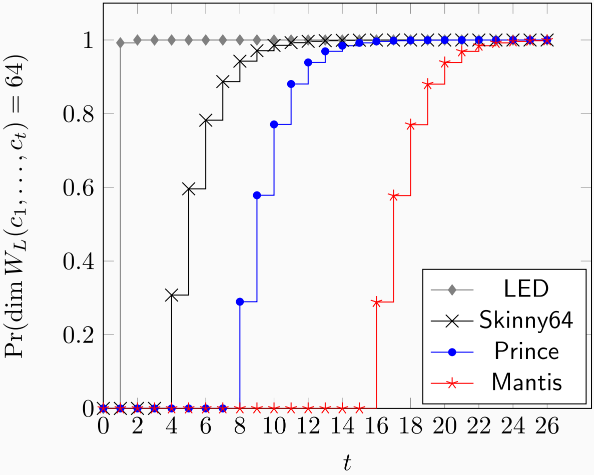
can be computed from the degrees of the irreducible factors of $\mathbf{Min}_L$ and from the invariant factors of L.

LED.

$$\mathrm{Min}_L(X) = (X^8 + X^7 + X^5 + X^3 + 1)^4(X^8 + X^7 + X^6 + X^5 + X^2 + 1)^4$$

$$\Pr_{c \xleftarrow{\$} \mathbb{F}_2^{64}}[W_L(c) = \mathbb{F}_2^{64}] = (1 - 2^{-8})^2 \simeq 0.9922$$

Probability to achieve the full dimension



Conclusion

Easy to prevent the attack:

- by choosing a linear layer which has a few invariant factors
- by choosing appropriate round constants

Open question: Can we use different invariants for the Sbox-layer and the linear layer?

Conclusion

Easy to prevent the attack:

- by choosing a linear layer which has a few invariant factors
- by choosing appropriate round constants

Open question: Can we use different invariants for the Sbox-layer and the linear layer?