Proving resistance against invariant attacks: How to choose the round constants

Christof Beierle, Anne Canteaut, Gregor Leander, Yann Rotella

Ruhr-Universität Bochum, Germany
Inria Paris, France

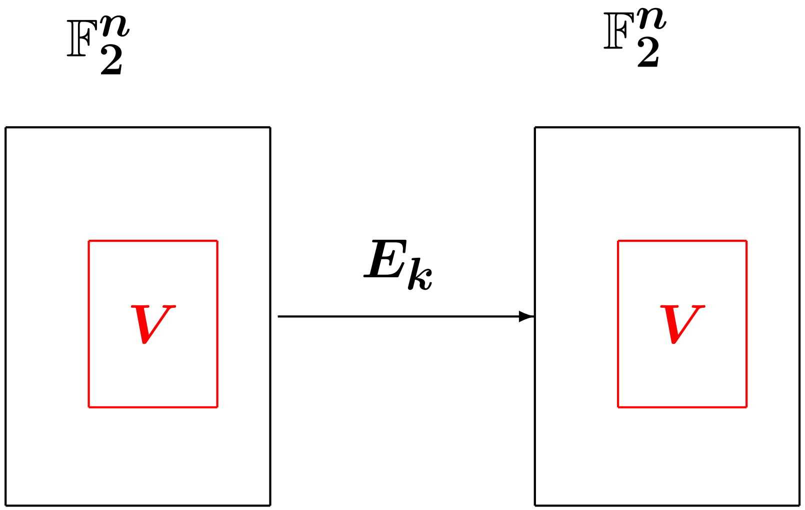
BFA 2017, July 2017

Outline

- A new condition on the existence of nonlinear invariants
- How to check that the attack does not apply for a given cipher
- Impact of the round constants and of the linear layer

The invariant subspace attack [Leander et al. 11]

Linear subspace invariant under E_k.

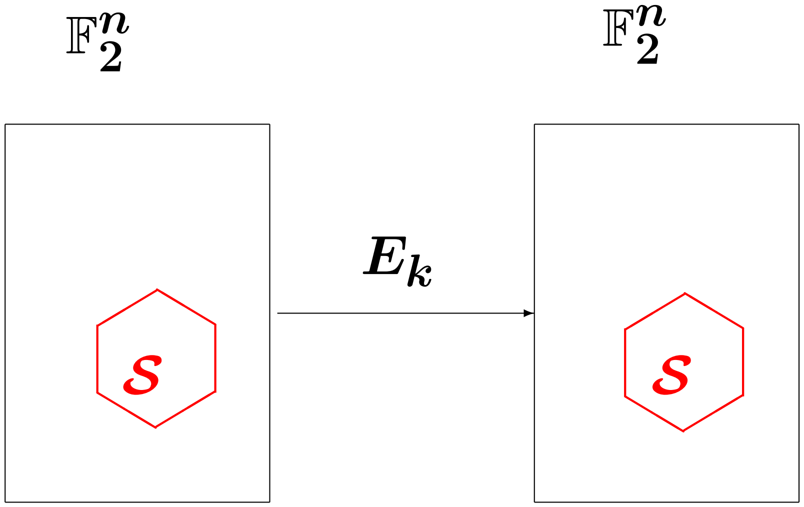


V: a linear subspace of $\mathbb{F}_2^n$

$$E_k(V) = V$$

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

Non-trivial partition of $\mathbb{F}_2^n$ invariant under E_k:



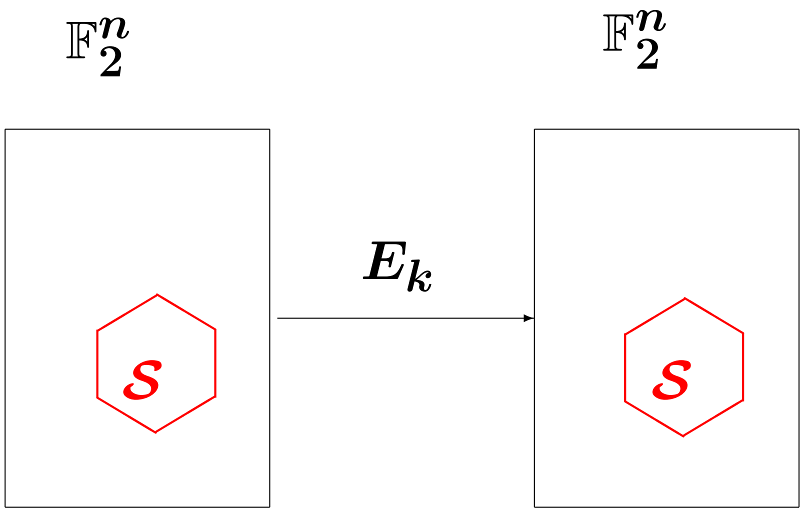
$\mathcal{S}$: any subset of $\mathbb{F}_2^n$

$$E_k(\mathcal{S}) = \mathcal{S}$$

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

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

Non-trivial partition of $\mathbb{F}_2^n$ invariant under E_k:



$\mathcal{S}$: any subset of $\mathbb{F}_2^n$

$E_k(\mathcal{S}) = \mathcal{S}$

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

Equivalently:

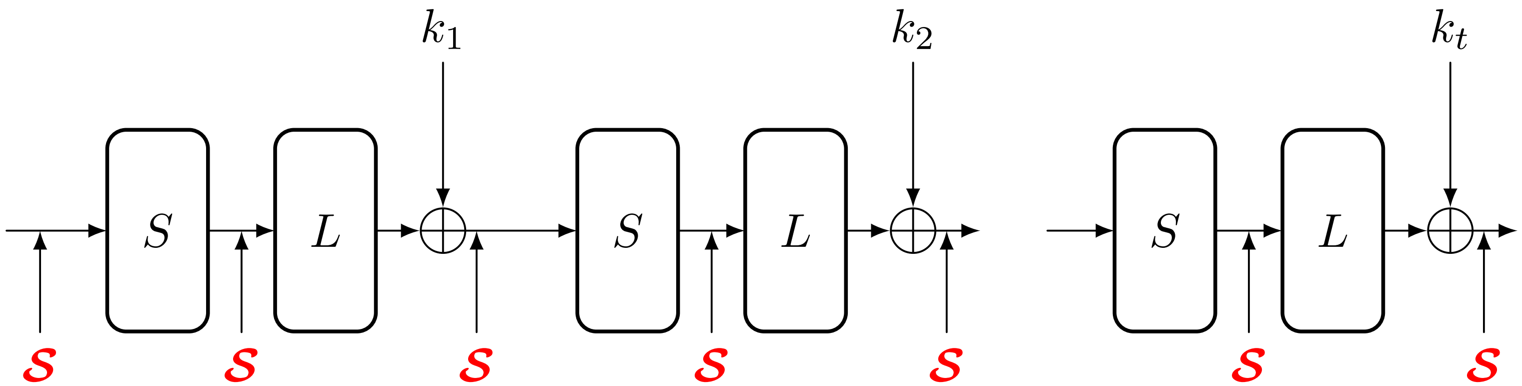
Let g be the Boolean function defined by $g(x) := 1$ iff $x \in \mathcal{S}$

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

Such a g is called an invariant for E_k.

Using the same invariant for all layers in a key-alternating cipher

Find an invariant $\boldsymbol{g}$ for the Sbox-layer and for all $\mathbf{Add}_{\mathbf{k_i}} \circ \boldsymbol{L}$.



Finding an invariant g for all $\mathsf{Add}_{\mathsf{k_i}} \circ L$

$$g(L(x) + k_i) = g(x) + \varepsilon_i \qquad g(L(x) + k_j) = g(x) + \varepsilon_j$$

$$\Rightarrow g(L(x) + k_i) = g(L(x) + k_j) + (\varepsilon_i + \varepsilon_j)$$

$$\iff g(y + k_i + k_j) = g(y) + (\varepsilon_i + \varepsilon_j)$$

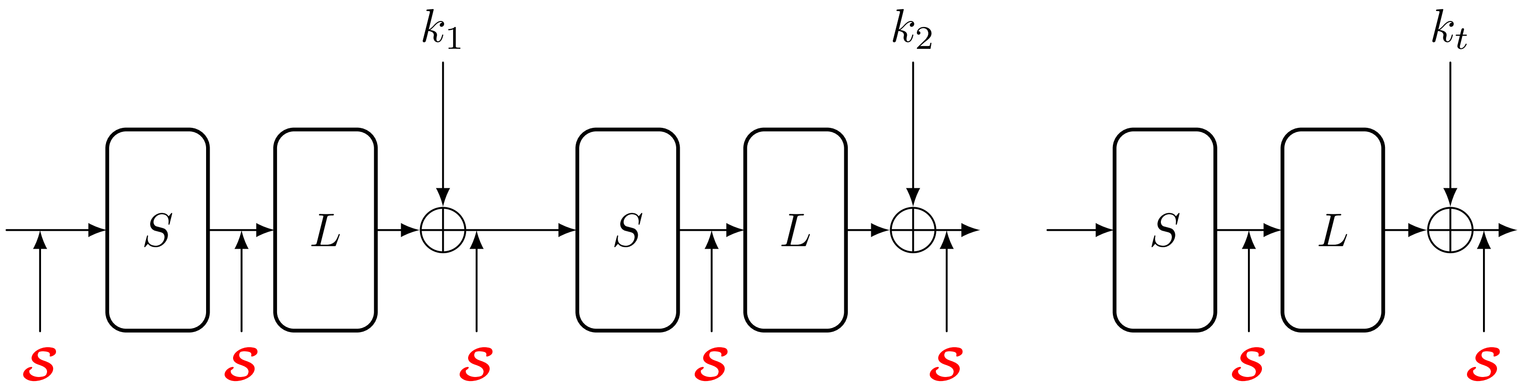
$(k_i + k_j)$ is a linear structure of g.

Linear space of a Boolean function g:

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

Using the same invariant for all layers in a key-alternating cipher

Find an invariant $\boldsymbol{g}$ for the Sbox-layer and for all $\mathbf{Add_{k_i}} \circ \boldsymbol{L}$.

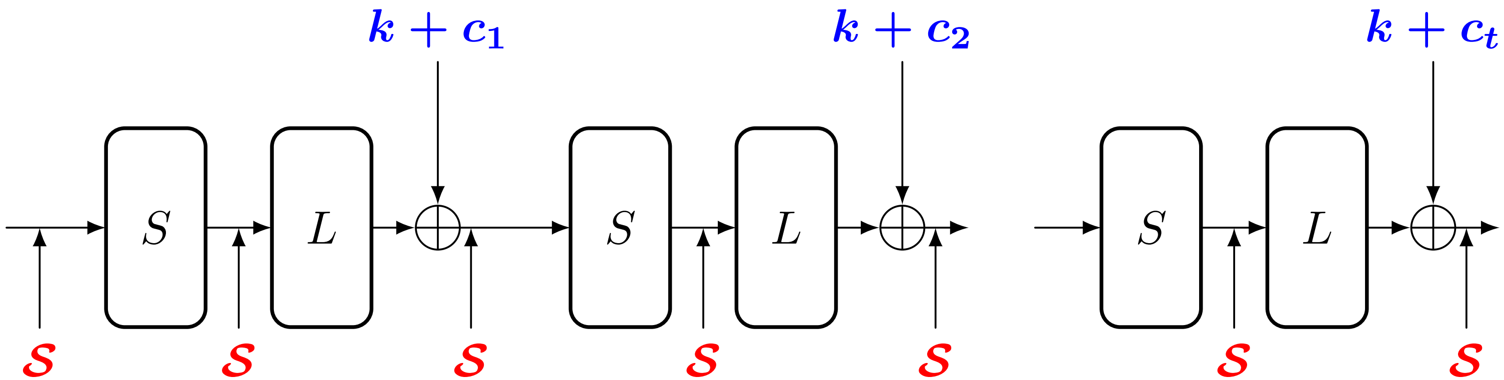


$\boldsymbol{g}$ is an invariant for the Sbox layer and satisfies:

- $\mathbf{LS}(\boldsymbol{g})$ contains $(\boldsymbol{k_i} + \boldsymbol{k_j})$
- $\mathbf{LS}(\boldsymbol{g})$ is invariant under $\boldsymbol{L}$

Very simple key schedules

All round-keys are defined by $k_i = k + c_i$



The main condition for very simple key schedules

$$D := \{(c_i + c_j) \text{ such that } k_i = k + c_i \text{ and } k_j = k + c_j\}$$

$W_L(D) :=$ smallest subspace invariant under L which contains D .

Is there a non-trivial invariant g for the Sbox-layer such that

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

Checking that such invariants do not exist

A simple case

Question:

Is there an invariant g for the Sbox-layer such that $W_L(D) \subseteq \mathsf{LS}(g)$?

If $\dim W_L(D) \geq n - 1$, then $\deg g \leq 1$, which is impossible unless the Sbox layer has a component of degree 1.

If $\dim W_L(D) \geq n - 1$, the attack does not apply.
This holds for any choice of the Sbox-layer.

Some lightweight ciphers

Skinny-64-64.

$$D = \{\mathbf{RC}_1 + \mathbf{RC}_{17},\ \mathbf{RC}_2 + \mathbf{RC}_{18},\ \mathbf{RC}_3 + \mathbf{RC}_{19},\ \mathbf{RC}_4 + \mathbf{RC}_{20},\ \mathbf{RC}_5 + \mathbf{RC}_{21}\}$$

$$\dim W_L(D) = 64$$

The round-constants and L guarantee that the attack does not apply.

Prince.

$$D = \{\mathbf{RC}_1 + \mathbf{RC}_2,\ \mathbf{RC}_1 + \mathbf{RC}_3,\ \mathbf{RC}_1 + \mathbf{RC}_4,\ \mathbf{RC}_1 + \mathbf{RC}_5,\ \alpha\}.$$

$$\dim W_L(D) = 56$$

Mantis-7.

$$D = \{\mathbf{RC}_1 + \mathbf{RC}_2, \mathbf{RC}_1 + \mathbf{RC}_3, \mathbf{RC}_1 + \mathbf{RC}_4, \mathbf{RC}_1 + \mathbf{RC}_5, \mathbf{RC}_1 + \mathbf{RC}_6, \mathbf{RC}_1 + \mathbf{RC}_7, \alpha\}.$$

$$\dim W_L(D) = 42$$

Midori-64.

$$W_L(D) = \{0000, 0001\}^{16}, \quad \dim W_L(D) = 16$$

When $\dim W_L(D) < n$

$\alpha \in$ **LS**(g) iff $g(x+\alpha) + g(x) = \varepsilon$ for all x.

0-linear structures.
$\alpha \in$ **LS**$^0(g)$ iff $g(x+\alpha) + g(x) = 0$ for all x.

If a subspace Z of LS$^0(g)$ is known

- g is constant on each $a + Z$ since $g(a+z) = g(a)$ for any $z \in Z$
- $g(S(x)) = g(x) + \varepsilon$ for all x, then g is constant on $S(Z)$.

If $Z \subseteq \mathsf{LS}^0(g)$ is known

$L = \{\}$
repeat
  $z \xleftarrow{\$} Z$
  Compute $S(z)$
  Add to L a representative of the coset of $S(z)$
until $|L| = 2^{n - \dim Z}$

But $W_L(D) \subseteq \mathsf{LS}(g)$, while we need $Z \subseteq \mathsf{LS}^0(g)$...

Finding a subspace of $\mathsf{LS}^0(g)$

Prince.

For any $x \in \mathsf{LS}(g)$, $(x + L(x)) \in \mathsf{LS}^0(g)$.

$$D' := \{x + L(x),\ x \in D\}.$$

we have $\dim W_L(D') = 51$.

$\Rightarrow$We can check that the Sbox-layer of Prince has no non-trivial invariant g with $W_L(D') \subseteq \mathsf{LS}^0(g)$.

Mantis-7.

$$D = \{\mathsf{RC}_1 + \mathsf{RC}_2, \mathsf{RC}_1 + \mathsf{RC}_3, \mathsf{RC}_1 + \mathsf{RC}_4, \mathsf{RC}_1 + \mathsf{RC}_5, \mathsf{RC}_1 + \mathsf{RC}_6, \mathsf{RC}_1 + \mathsf{RC}_7, \alpha\}.$$

$$\Rightarrow W_L(D) \subseteq \mathsf{LS}^0(g)$$

We can check that the Sbox-layer of Mantis has no non-trivial invariant g with $W_L(D) \subseteq \mathsf{LS}^0(g)$.

Very different behaviours

Skinny-64-64.

$$D = \{\mathsf{RC}_1 + \mathsf{RC}_{17},\ \mathsf{RC}_2 + \mathsf{RC}_{18},\ \mathsf{RC}_3 + \mathsf{RC}_{19},\ \mathsf{RC}_4 + \mathsf{RC}_{20},\ \mathsf{RC}_5 + \mathsf{RC}_{21}\}$$

$$\dim W_L(D) = 64$$

Prince.

$$D = \{\mathsf{RC}_1 + \mathsf{RC}_2,\ \mathsf{RC}_1 + \mathsf{RC}_3,\ \mathsf{RC}_1 + \mathsf{RC}_4,\ \mathsf{RC}_1 + \mathsf{RC}_5,\ \alpha\}.$$

$$\dim W_L(D) = 56$$

Mantis-7.

$$D = \{\mathsf{RC}_1 + \mathsf{RC}_2, \mathsf{RC}_1 + \mathsf{RC}_3, \mathsf{RC}_1 + \mathsf{RC}_4, \mathsf{RC}_1 + \mathsf{RC}_5, \mathsf{RC}_1 + \mathsf{RC}_6, \mathsf{RC}_1 + \mathsf{RC}_7, \alpha\}.$$

$$\dim W_L(D) = 42$$

Can we find better round-constants?

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 relative 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.

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

For some lightweight ciphers

LED.

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

There exist some c such that $\dim W_L(c) = 64$

Skinny-64.

$$\textbf{Min}_L(X) = X^{16} + 1 = (X + 1)^{16}$$

There exist some c such that $\dim W_L(c) = d$ for any $1 \leq d \leq 16$.

Prince.

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

$$\max_c \dim W_L(c) = 20$$

Mantis and Midori.

$$\textbf{Min}_L(X) = (X + 1)^6 \Rightarrow \max_c \dim W_L(c) = 6$$

Rational canonical form

When $\deg(\mathbf{Min}_L) = n$, there is a basis for which the matrix of L is the companion matrix

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

More generally, there is a basis for which the matrix of L is

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

for r polynomials $Q_r \mid Q_{r-1} \mid \cdots \mid Q_1 = \mathbf{Min}_L$

Q_1, Q_2, ... , Q_r are called the invariant factors of L.

Example

For Prince.

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

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 $W_L(c_1, \dots, c_t)$

Theorem. Let $Q_1, Q_2, \dots, Q_r$ be the r invariant factors of L.

For any $t \leq r$,

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

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

For Prince.

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

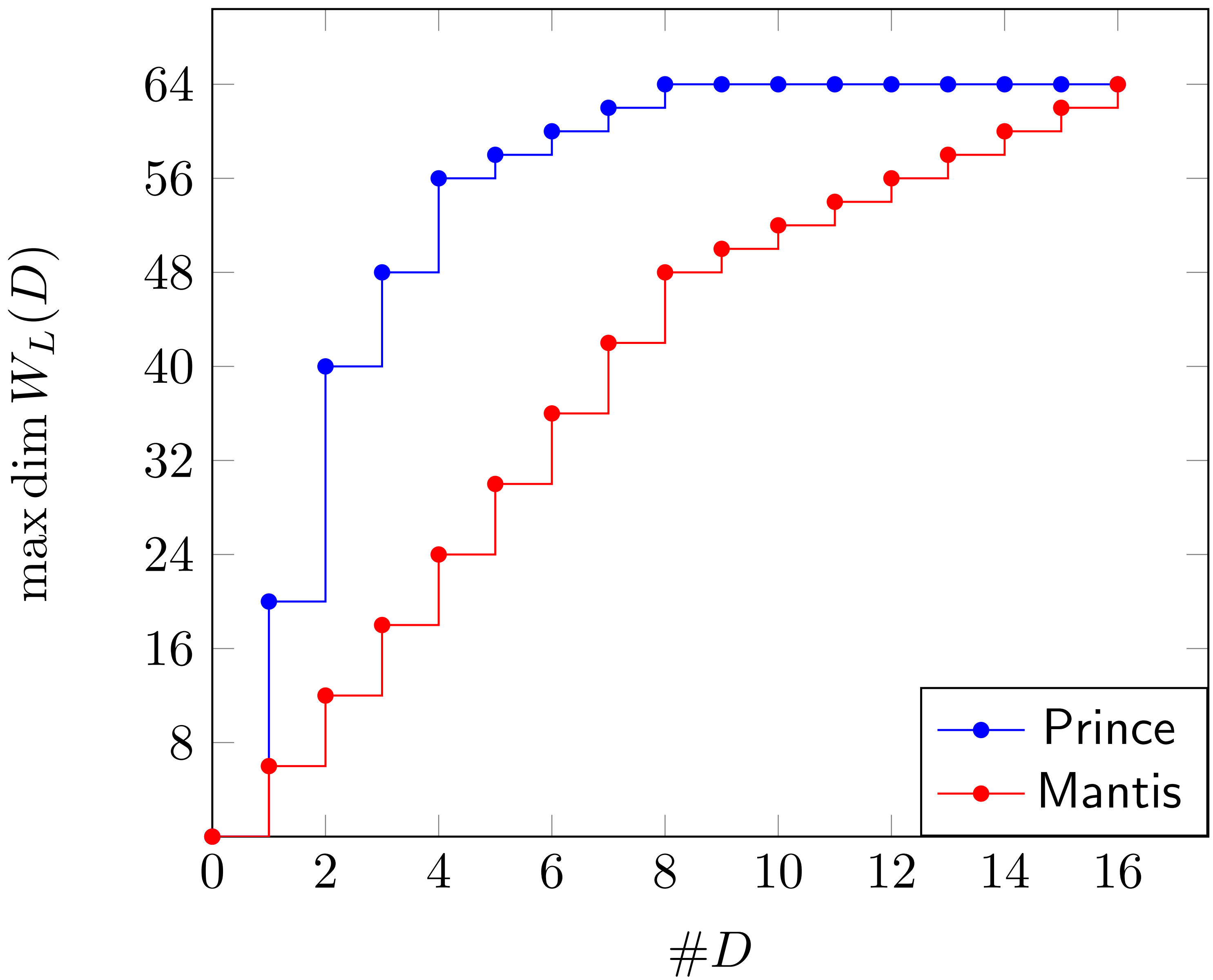
We need 8 elements to get the full space.

Mantis and Midori. $r = 16$ invariant factors

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

For $t = 7,\ \max \dim W_L(c_1, \dots, c_7) = 42,$
For $t = 8,\ \max \dim W_L(c_1, \dots, c_8) = 48.$
We need 16 elements to get the full space.

Maximum dimension for $\#D$ constants



For random constants

For $t \geq r$,

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

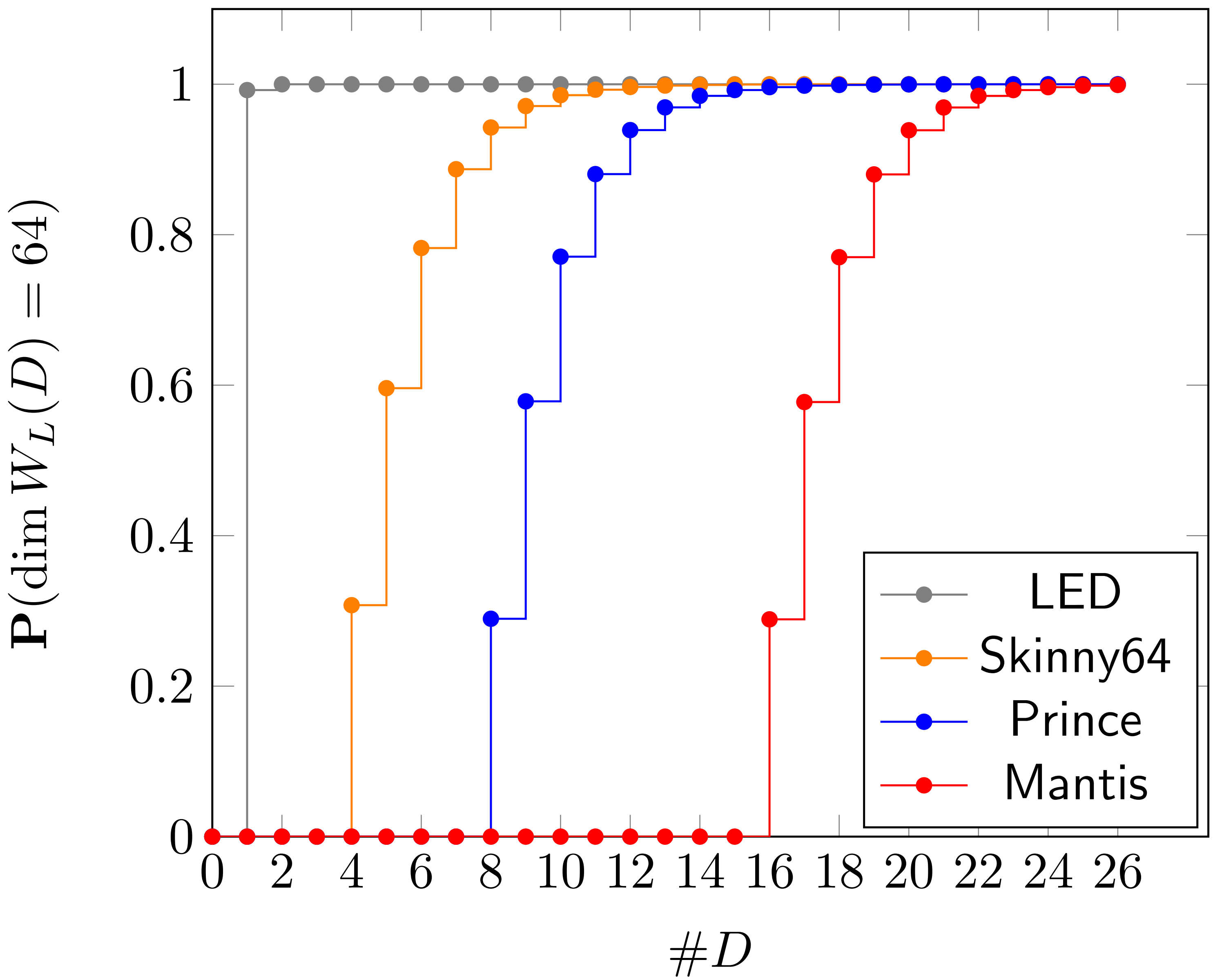
can be computed from the degrees of the irreducible factors of $\textbf{Min}_L$ and from the invariant factors of L.

LED.

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

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

Probability to achieve the full dimension



Conclusions

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?