Choosing Round Constants in Lightweight Block Ciphers and Cryptographic Permutations

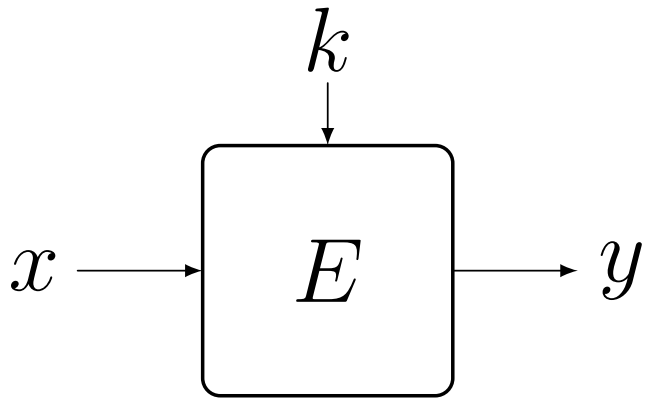
Christof Beierle

SnT, University of Luxembourg, Luxembourg

(joint work with Anne Canteaut, Gregor Leander, and Yann Rotella)

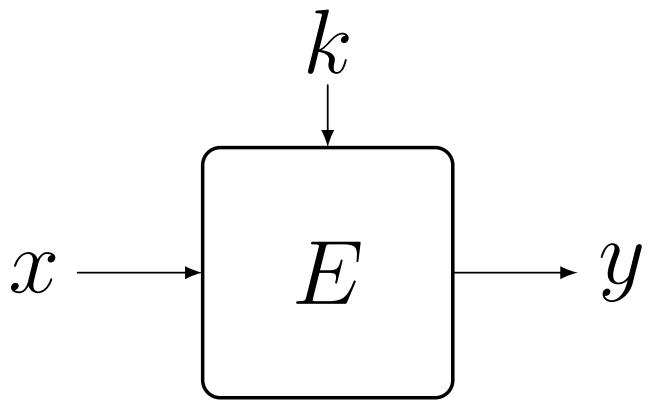
October, 10, 2018

Block Cipher vs. Cryptographic Permutation

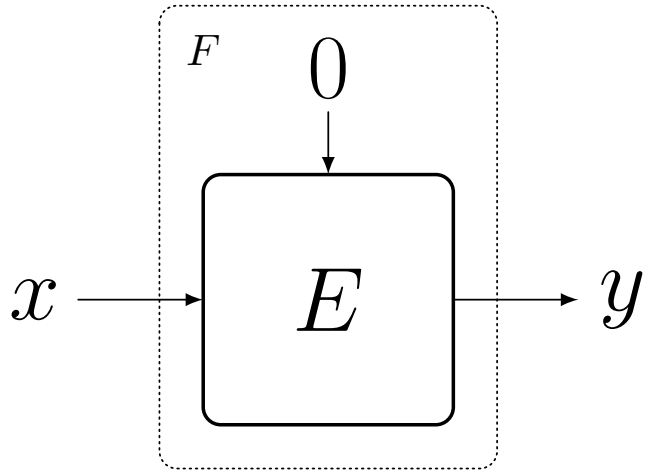


$E: \mathbb{F}_2^n \times \mathbb{F}_2^\kappa \to \mathbb{F}_2^n,\ (x, k) \mapsto E_k(x) = y$

Block Cipher vs. Cryptographic Permutation



$E\colon \mathbb{F}_2^n \times \mathbb{F}_2^\kappa \to \mathbb{F}_2^n,\ (x,k) \mapsto E_k(x) = y$



$F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n,\ x \mapsto E_0(x) = y$

Special Case

A cryptographic permutation can be seen as a block cipher with a fixed key!

Why Round Constants are Needed

- Avoiding to use always the same round ($\rightarrow$ slide attacks)
- Avoiding symmetries

Why Round Constants are Needed

- Avoiding to use always the same round ($\rightarrow$ slide attacks)
- Avoiding symmetries

Example: NORX [Aumasson, Jovanovic, Neves 2014]

If the input to the NORX permutation is in the set

$$\mathcal{S} = \left\{ \begin{pmatrix} a & a & a & a \\ b & b & b & b \\ c & c & c & c \\ d & d & d & d \end{pmatrix} \mid a, b, c, d \in \mathbb{F}_2^w \right\},$$

the output also is in $\mathcal{S}$.

Basic Definitions

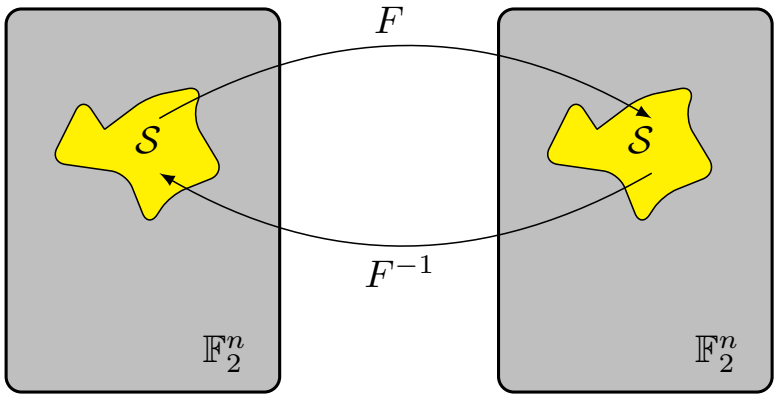
Definition: Invariant Set

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a permutation. We say that $\mathcal{S} \subseteq \mathbb{F}_2^n$ is an invariant set under F if $F(\mathcal{S}) = \mathcal{S}$ or $F(\mathcal{S}) = \mathbb{F}_2^n \setminus \mathcal{S}$.

Basic Definitions

Definition: Invariant Set

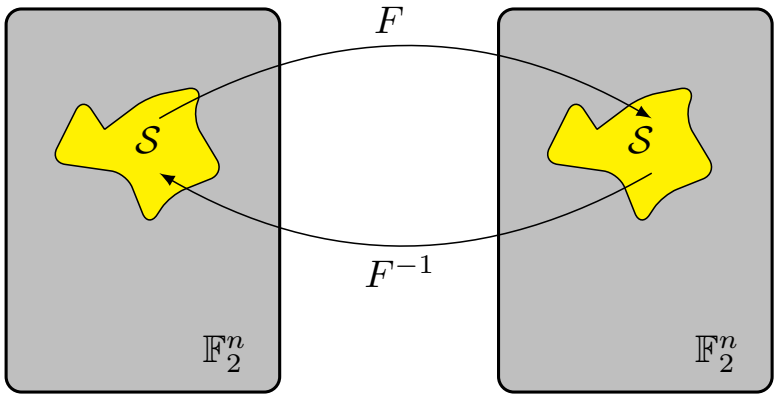
Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a permutation. We say that $\mathcal{S} \subseteq \mathbb{F}_2^n$ is an invariant set under F if $F(\mathcal{S}) = \mathcal{S}$ or $F(\mathcal{S}) = \mathbb{F}_2^n \setminus \mathcal{S}$.

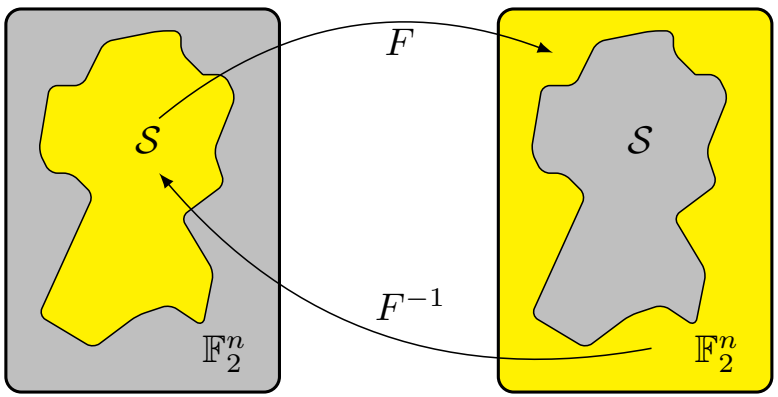


Basic Definitions

Definition: Invariant Set

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a permutation. We say that $\mathcal{S} \subseteq \mathbb{F}_2^n$ is an invariant set under F if $F(\mathcal{S}) = \mathcal{S}$ or $F(\mathcal{S}) = \mathbb{F}_2^n \setminus \mathcal{S}$.

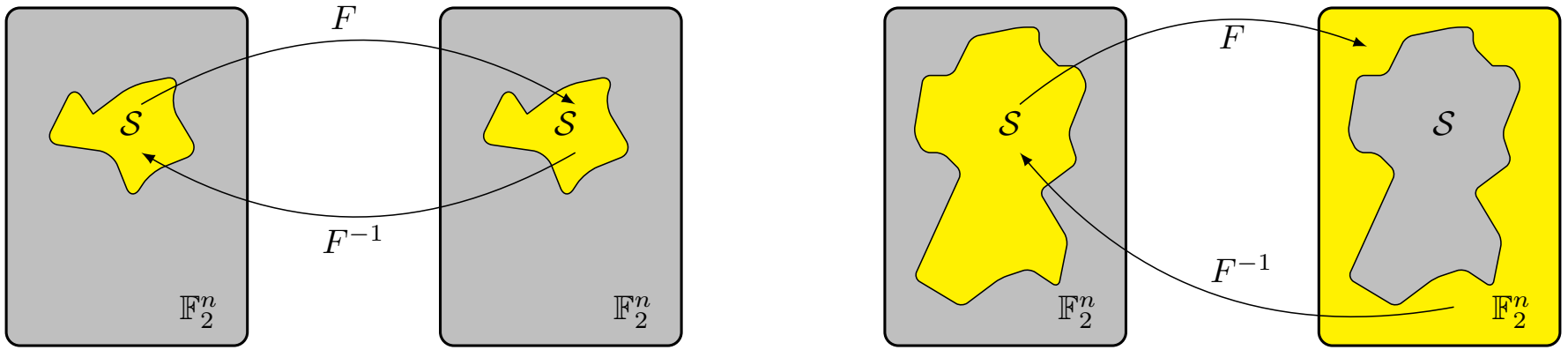




Basic Definitions

Definition: Invariant Set

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a permutation. We say that $\mathcal{S} \subseteq \mathbb{F}_2^n$ is an invariant set under F if $F(\mathcal{S}) = \mathcal{S}$ or $F(\mathcal{S}) = \mathbb{F}_2^n \setminus \mathcal{S}$.



Equivalently:

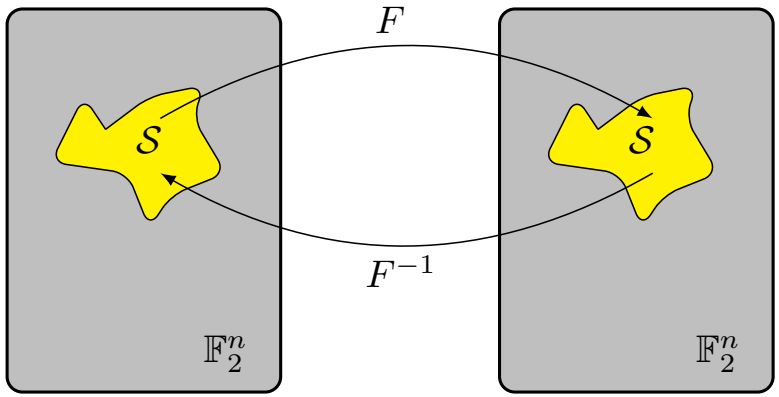
Let g be the Boolean function defined by $g(x) := 1$ iff $x \in \mathcal{S}$. Then,

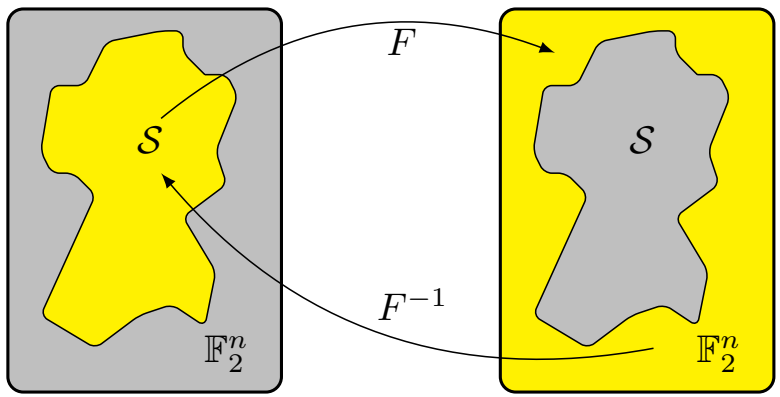
$$\forall x \in \mathbb{F}_2^n : g(F(x)) = g(x) \text{ or } \forall x \in \mathbb{F}_2^n : g(F(x)) = g(x) + 1.$$

Basic Definitions

Definition: Invariant Set

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a permutation. We say that $\mathcal{S} \subseteq \mathbb{F}_2^n$ is an invariant set under F if $F(\mathcal{S}) = \mathcal{S}$ or $F(\mathcal{S}) = \mathbb{F}_2^n \setminus \mathcal{S}$.





Equivalently:

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

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

Definition: Invariant Function

Any Boolean function $g : \mathbb{F}_2^n \to \mathbb{F}_2$ for which $g \circ F + g$ is constant is called an invariant for F.

Invariant Attacks

Examples of invariants g for F: $(g \circ F + g$ is constant)

- $g = \mathbf{0}$. Equivalent to having $\mathcal{S} = \{\}$
- $g = \mathbf{1}$. Equivalent to having $\mathcal{S} = \mathbb{F}_2^n$

} trivial invariants

Invariant Attacks

Examples of invariants g for F: ($g \circ F + g$ is constant)

- $g = \mathbf{0}$. Equivalent to having $\mathcal{S} = \{\}$
- $g = \mathbf{1}$. Equivalent to having $\mathcal{S} = \mathbb{F}_2^n$

} trivial invariants

- $g(x) = 1$ iff $x \in \mathcal{U}$ for an affine subspace $\mathcal{U} \subseteq \mathbb{F}_2^n$.
  $\rightarrow$ Invariant Subspace Attack [Leander et al. 2011]

Invariant Attacks

Examples of invariants g for F: ($g \circ F + g$ is constant)

- $g = \mathbf{0}$. Equivalent to having $\mathcal{S} = \{\}$
- $g = \mathbf{1}$. Equivalent to having $\mathcal{S} = \mathbb{F}_2^n$

} trivial invariants

- $g(x) = 1$ iff $x \in \mathcal{U}$ for an affine subspace $\mathcal{U} \subseteq \mathbb{F}_2^n$.
  $\rightarrow$ Invariant Subspace Attack [Leander et al. 2011]

Consider a block cipher $E : \mathbb{F}_2^n \times \mathbb{F}_2^\kappa \rightarrow \mathbb{F}_2^n,\ (x, k) \mapsto E_k(x)$.

Nonlinear Invariant Attack [Todo, Leander, Sasaki 2016]

If for some keys k, one can find (non-trivial) invariants for E_k, the cipher is vulnerable to the Nonlinear Invariant Attack. Keys which allow for the attack are called weak keys of E.

This Leads to a Distinguisher

The knowledge of a (non-trivial) invariant g for E_k allows to distinguish the instance from a random permutation $\mathcal{P}_{\text{rand}}$.

This Leads to a Distinguisher

The knowledge of a (non-trivial) invariant g for E_k allows to distinguish the instance from a random permutation $\mathcal{P}_{\text{rand}}$.

- given oracle access to $\mathcal{O} \in \{E_k, \mathcal{P}_{\text{rand}}\}$

This Leads to a Distinguisher

The knowledge of a (non-trivial) invariant g for E_k allows to distinguish the instance from a random permutation $\mathcal{P}_{\text{rand}}$.

- given oracle access to $\mathcal{O} \in \{E_k, \mathcal{P}_{\text{rand}}\}$
- choose $m_1, \ldots, m_d \in \mathbb{F}_2^n$

This Leads to a Distinguisher

The knowledge of a (non-trivial) invariant g for E_k allows to distinguish the instance from a random permutation $\mathcal{P}_{\text{rand}}$.

- given oracle access to $\mathcal{O} \in \{E_k, \mathcal{P}_{\text{rand}}\}$
- choose $m_1, \ldots, m_d \in \mathbb{F}_2^n$
- check if $\forall i \in \{1, \ldots, d\} : g(\mathcal{O}(m_i)) + g(m_i)$ is constant

Many Lightweight Ciphers Vulnerable to Invariant Attacks

For instance:

- PRINT-cipher [Leander et al. 2011]
- Midori-64 [Guo et al. 2016] [Todo, Leander, Sasaki 2016]
- iSCREAM [Leander, Minaud, Rønjom 2015]
- SCREAM [Todo, Leander, Sasaki 2016]
- NORX v2.0 [Chaigneau et al. 2017]
- Simpira v1 [Rønjom 2016]
- Haraka v.0 [Jean 2016]

Main Goal: Prevent against Invariant Attacks

Our Main Goal (Block Ciphers)

Given a block cipher $E : \mathbb{F}_2^n \times \mathbb{F}_2^\kappa \to \mathbb{F}_2^n,\ (x, k) \mapsto E_k(x)$. Show that there are no weak keys, i.e., for any k, one can find only trivial invariants for E_k.

Main Goal: Prevent against Invariant Attacks

Our Main Goal (Block Ciphers)

Given a block cipher $E : \mathbb{F}_2^n \times \mathbb{F}_2^\kappa \to \mathbb{F}_2^n,\ (x, k) \mapsto E_k(x)$. Show that there are no weak keys, i.e., for any k, one can find only trivial invariants for E_k.

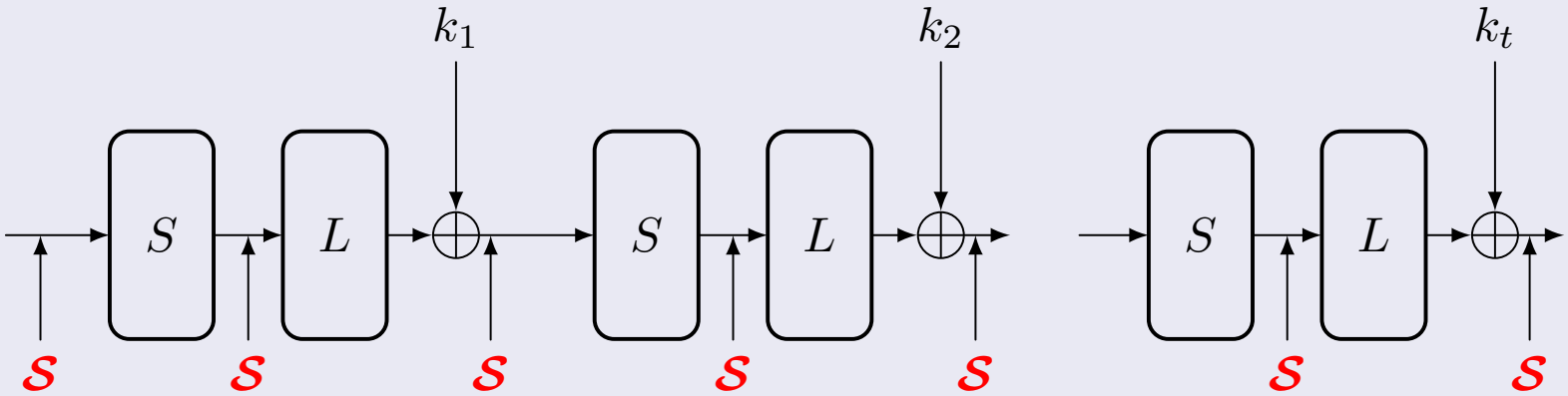
Our Main Goal (Cryptographic Permutation)

Given a permutation $F : \mathbb{F}_2^n \to \mathbb{F}_2^n,\ x \mapsto F(x)$. Show that one can find only trivial invariants for F.

Our Model

Simplification (SPN): Assume the Same Invariant for all Layers

We consider only those invariants g, that are simultaneously invariants for the S-box layer and for all $\mathsf{Add}_{\mathsf{k_i}} \circ L$.



Almost all real attacks we know exploit such an iterative structure!
One exception: [Beyne 2018]

1. Lightweight SPNs: Proving Resistance against Invariant Attacks

2. Design Criteria on the Linear Layer and the Round Constants

Structure of the Invariants for all $\mathrm{Add}_{k_i} \circ L$

Let g be an invariant for both $\mathrm{Add}_{k_i} \circ L$ and $\mathrm{Add}_{k_j} \circ L$. We then have:

$$g(L(x) + k_i) = g(x) + \text{const.} \qquad g(L(x) + k_j) = g(x) + \text{const.}$$

Structure of the Invariants for all $\mathrm{Add}_{k_i} \circ L$

Let g be an invariant for both $\mathrm{Add}_{k_i} \circ L$ and $\mathrm{Add}_{k_j} \circ L$. We then have:

$$g(L(x) + k_i) = g(x) + \text{const.} \qquad g(L(x) + k_j) = g(x) + \text{const.}$$

$$\begin{aligned} \implies \quad & g(L(x) + k_i) = g(L(x) + k_j) + \text{const.} \\ \iff \quad & g(y + k_i + k_j) = g(y) + \text{const.} \end{aligned}$$

Structure of the Invariants for all $\mathrm{Add}_{k_i} \circ L$

Let g be an invariant for both $\mathrm{Add}_{k_i} \circ L$ and $\mathrm{Add}_{k_j} \circ L$. We then have:

$$g(L(x) + k_i) = g(x) + \text{const.} \qquad g(L(x) + k_j) = g(x) + \text{const.}$$

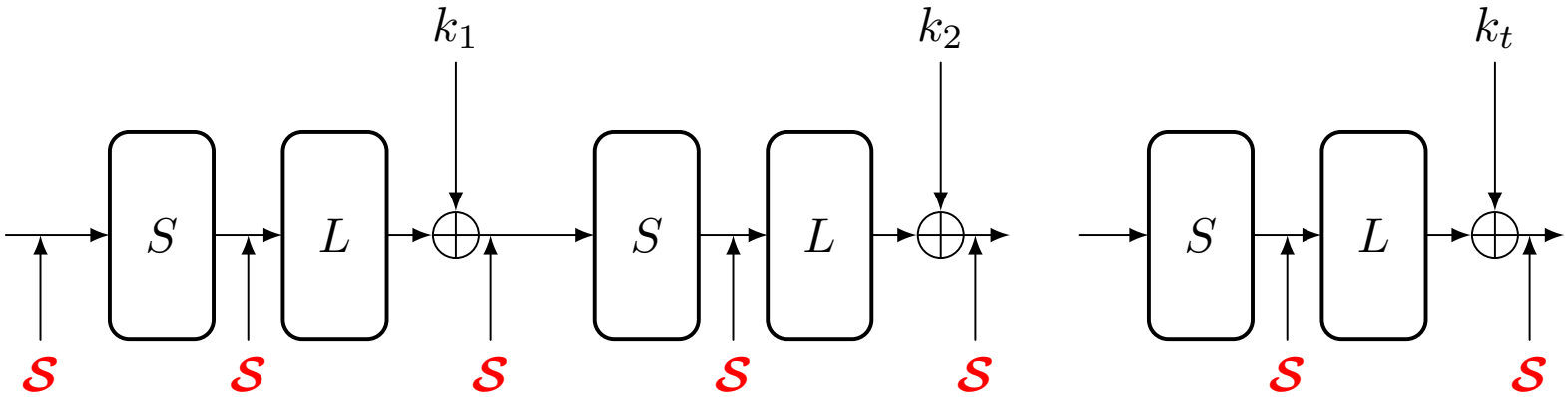
$$\begin{aligned} \implies \quad & g(L(x) + k_i) = g(L(x) + k_j) + \text{const.} \\ \iff \quad & g(y + k_i + k_j) = g(y) + \text{const.} \end{aligned}$$

$(\mathbf{k_i} + \mathbf{k_j})$ is a linear structure of g.

Definition: Linear Structures of a Boolean Function g

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

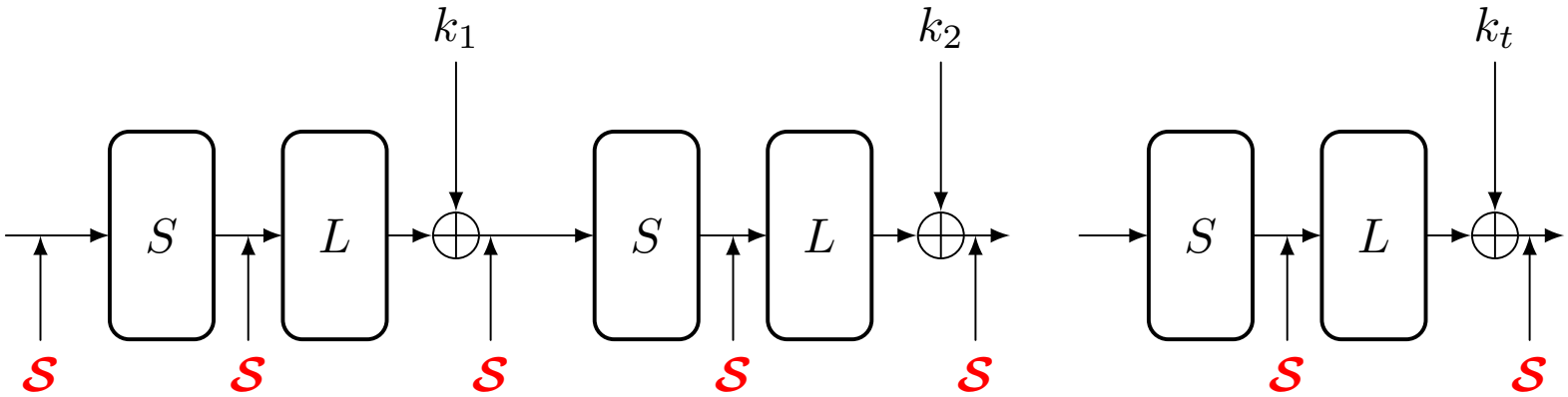
Requirements on an Invariant g



g has to be an invariant for the S-box layer and has to satisfy:

- LS(g) contains all round key differences ($k_i + k_j$).
- LS(g) is invariant under L, i.e., $L(\text{LS}(g)) = \text{LS}(g)$.

Requirements on an Invariant g



g has to be an invariant for the S-box layer and has to satisfy:

- LS(g) contains all round key differences ($k_i + k_j$).
- LS(g) is invariant under L, i.e., $L(\text{LS}(g)) = \text{LS}(g)$.

How does the key schedule look like?

SPNs with very Simple Key Schedules

In many lightweight block ciphers, the round keys only differ by addition of a publicly-known round constant, i.e.,

$$\forall i : k_i := k + c_i.$$

Thus, $k_i + k_j = c_i + c_j \in \mathsf{LS}(g)$.

SPNs with very Simple Key Schedules

In many lightweight block ciphers, the round keys only differ by addition of a publicly-known round constant, i.e.,

$$\forall i : k_i := k + c_i.$$

Thus, $k_i + k_j = c_i + c_j \in \mathrm{LS}(g)$.

In a cryptographic permutation, we only have publicly-known round constants, i.e.,

$$\forall i : k_i := 0 + c_i.$$

Thus, $k_i + k_j = c_i + c_j \in \mathrm{LS}(g)$.

Proving the Non-Existence of Invariants

Main Condition on an Invariant g

1. g has to be an invariant for the S-box layer and
2. The smallest L-invariant subspace of $\mathbb{F}_2^n$ that contains all $c_i + c_j$ must be a subset of $\mathrm{LS}(g)$. We denote this subspace by $W_L(\{c_i + c_j \mid i, j\})$.

Proving the Non-Existence of Invariants

Main Condition on an Invariant g

1. g has to be an invariant for the S-box layer and
2. The smallest L-invariant subspace of $\mathbb{F}_2^n$ that contains all $c_i + c_j$ must be a subset of $\mathrm{LS}(g)$. We denote this subspace by $W_L(\{c_i + c_j \mid i, j\})$.

Important Observation

Assume that the S-box layer has no component of algebraic degree 1.
If $\dim W_L(\{c_i + c_j \mid i, j\}) \geq n - 1$, there are only the trivial invariants that fulfill the above main condition!

Proving the Non-Existence of Invariants

Main Condition on an Invariant g

1. g has to be an invariant for the S-box layer and
2. The smallest L-invariant subspace of $\mathbb{F}_2^n$ that contains all $c_i + c_j$ must be a subset of $\mathrm{LS}(g)$. We denote this subspace by $W_L(\{c_i + c_j \mid i, j\})$.

Important Observation

Assume that the S-box layer has no component of algebraic degree 1.
If $\dim W_L(\{c_i + c_j \mid i, j\}) \geq n - 1$, there are only the trivial invariants that fulfill the above main condition!

Why?

- If $\dim W_L(\{c_i + c_j \mid i, j\}) \geq n - 1$, then $\dim \mathrm{LS}(g) \geq n - 1$.

Proving the Non-Existence of Invariants

Main Condition on an Invariant g

1. g has to be an invariant for the S-box layer and
2. The smallest L-invariant subspace of $\mathbb{F}_2^n$ that contains all $c_i + c_j$ must be a subset of $\mathrm{LS}(g)$. We denote this subspace by $W_L(\{c_i + c_j \mid i, j\})$.

Important Observation

Assume that the S-box layer has no component of algebraic degree 1.
If $\dim W_L(\{c_i + c_j \mid i, j\}) \geq n - 1$, there are only the trivial invariants that fulfill the above main condition!

Why?

- If $\dim W_L(\{c_i + c_j \mid i, j\}) \geq n - 1$, then $\dim \mathrm{LS}(g) \geq n - 1$.
- But then, g is linear (or affine).

Proving the Non-Existence of Invariants

Main Condition on an Invariant g

1. g has to be an invariant for the S-box layer and
2. The smallest L-invariant subspace of $\mathbb{F}_2^n$ that contains all $c_i + c_j$ must be a subset of $\mathrm{LS}(g)$. We denote this subspace by $W_L(\{c_i + c_j \mid i, j\})$.

Important Observation

Assume that the S-box layer has no component of algebraic degree 1.
If $\dim W_L(\{c_i + c_j \mid i, j\}) \geq n - 1$, there are only the trivial invariants that fulfill the above main condition!

Why?

- If $\dim W_L(\{c_i + c_j \mid i, j\}) \geq n - 1$, then $\dim \mathrm{LS}(g) \geq n - 1$.
- But then, g is linear (or affine).
- Since the S-box layer does not have a linear (or affine) component, g must be trivial.

Applying the Argument to some Examples

Important Observation

If $\dim W_L(\{c_i + c_j \mid i, j\}) \geq n - 1$, the invariant attack does not apply!

This holds for any (reasonable) choice of the S-box layer.

Applying the Argument to some Examples

Important Observation

If $\dim W_L(\{c_i + c_j \mid i, j\}) \geq n - 1$, the invariant attack does not apply!

This holds for any (reasonable) choice of the S-box layer.

Skinny-64-64. $\dim W_L(\{c_i + c_j \mid i, j\}) = 64 \qquad (n = 64)$

✓ the attack does not apply

Applying the Argument to some Examples

Important Observation

If $\dim W_L(\{c_i + c_j \mid i, j\}) \geq n - 1$, the invariant attack does not apply!

This holds for any (reasonable) choice of the S-box layer.

Skinny-64-64. $\dim W_L(\{c_i + c_j \mid i, j\}) = 64 \qquad (n = 64)$

✓ the attack does not apply

Prince. $\dim W_L(\{c_i + c_j \mid i, j\}) = 56 \qquad (n = 64)$

dimension too low

Applying the Argument to some Examples

Important Observation

If $\dim W_L(\{c_i + c_j \mid i, j\}) \geq n - 1$, the invariant attack does not apply!

This holds for any (reasonable) choice of the S-box layer.

Skinny-64-64. $\dim W_L(\{c_i + c_j \mid i, j\}) = 64 \qquad (n = 64)$

✓ the attack does not apply

Prince. $\dim W_L(\{c_i + c_j \mid i, j\}) = 56 \qquad (n = 64)$

dimension too low

Mantis-7. $\dim W_L(\{c_i + c_j \mid i, j\}) = 42 \qquad (n = 64)$

dimension too low

Applying the Argument to some Examples

Important Observation

If $\dim W_L(\{c_i + c_j \mid i, j\}) \geq n - 1$, the invariant attack does not apply!

This holds for any (reasonable) choice of the S-box layer.

Skinny-64-64. $\dim W_L(\{c_i + c_j \mid i, j\}) = 64 \qquad (n = 64)$

✓ the attack does not apply

Prince. $\dim W_L(\{c_i + c_j \mid i, j\}) = 56 \qquad (n = 64)$

dimension too low

Mantis-7. $\dim W_L(\{c_i + c_j \mid i, j\}) = 42 \qquad (n = 64)$

dimension too low

Midori-64. $\dim W_L(\{c_i + c_j \mid i, j\}) = 16 \qquad (n = 64)$

dimension too low

Applying the Argument to some Examples

Important Observation

If $\dim W_L(\{c_i + c_j \mid i, j\}) \geq n - 1$, the invariant attack does not apply!

This holds for any (reasonable) choice of the S-box layer.

Skinny-64-64. $\dim W_L(\{c_i + c_j \mid i, j\}) = 64 \qquad (n = 64)$

✓ the attack does not apply

Prince. $\dim W_L(\{c_i + c_j \mid i, j\}) = 56 \qquad (n = 64)$

✓ the attack does not apply (using properties of the S-box layer)

Mantis-7. $\dim W_L(\{c_i + c_j \mid i, j\}) = 42 \qquad (n = 64)$

✓ the attack does not apply (using properties of the S-box layer)

Midori-64. $\dim W_L(\{c_i + c_j \mid i, j\}) = 16 \qquad (n = 64)$

✗ dimension too low

How to Use Properties of the S-box

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

$$\mathsf{LS}_0(g) := \{\alpha \in \mathbb{F}_2^n : x \mapsto g(x+\alpha) + g(x) = 0\} \subseteq \mathsf{LS}(g)$$

We know $\dim \mathsf{LS}_0(g) \in \{\dim \mathsf{LS}(g), \dim \mathsf{LS}(g) - 1\}$. How to find $\mathsf{LS}_0(g)$?

How to Use Properties of the S-box

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

$$\mathsf{LS}_0(g) := \{\alpha \in \mathbb{F}_2^n : x \mapsto g(x+\alpha) + g(x) = 0\} \subseteq \mathsf{LS}(g)$$

We know $\dim \mathsf{LS}_0(g) \in \{\dim \mathsf{LS}(g), \dim \mathsf{LS}(g) - 1\}$. How to find $\mathsf{LS}_0(g)$?

First Lemma

Let g be an invariant for $\mathsf{Add}_{\mathsf{k_i}} \circ L$ for some k_i and let V be an L-invariant subspace of $\mathsf{LS}(g)$. Then, for any $s \in V$, it is $s + L(s) \in \mathsf{LS}_0(g)$.

How to Use Properties of the S-box

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

$$\mathsf{LS}_0(g) := \{\alpha \in \mathbb{F}_2^n : x \mapsto g(x+\alpha) + g(x) = 0\} \subseteq \mathsf{LS}(g)$$

We know $\dim \mathsf{LS}_0(g) \in \{\dim \mathsf{LS}(g), \dim \mathsf{LS}(g) - 1\}$. How to find $\mathsf{LS}_0(g)$?

First Lemma

Let g be an invariant for $\mathsf{Add}_{\mathsf{k_i}} \circ L$ for some k_i and let V be an L-invariant subspace of $\mathsf{LS}(g)$. Then, for any $s \in V$, it is $s + L(s) \in \mathsf{LS}_0(g)$.

Second Lemma

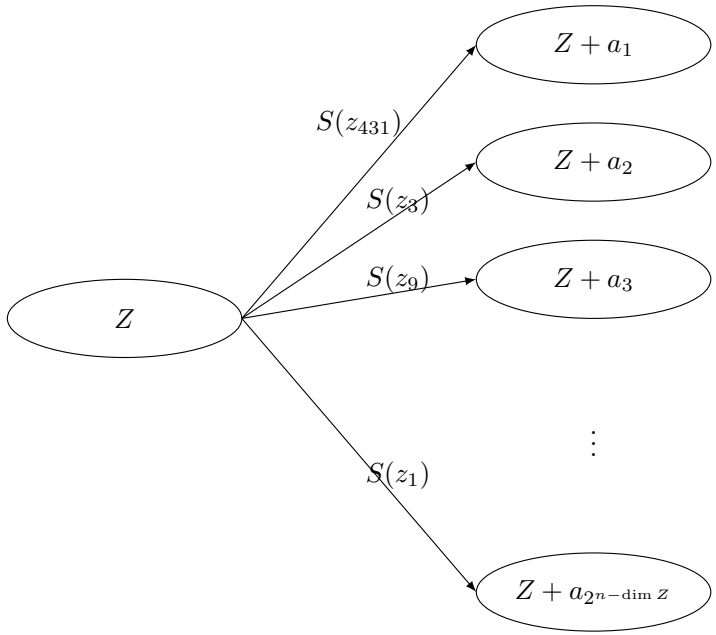
Let g be an invariant for S, where $S \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ is a permutation with an odd cycle. Then, $s \in \mathsf{LS}(g) \cap \{S(x) + x \mid x \in \mathbb{F}_2^n\}$ implies $s \in \mathsf{LS}_0(g)$.

How to Use Properties of the S-box

Lemma

Let $g\colon \mathbb{F}_2^n \to \mathbb{F}_2$ be an invariant for S and let Z be a subspace of $\mathbb{F}_2^n$ with $Z \subset \mathsf{LS}_0(g)$. Then

- g is constant on each coset $Z + a$
- g is constant on $S(Z)$



How to Use Properties of the S-box

Lemma

Let $g\colon \mathbb{F}_2^n \to \mathbb{F}_2$ be an invariant for S and let Z be a subspace of $\mathbb{F}_2^n$ with $Z \subset \mathrm{LS}_0(g)$. Then

- g is constant on each coset $Z + a$
- g is constant on $S(Z)$

Algorithm

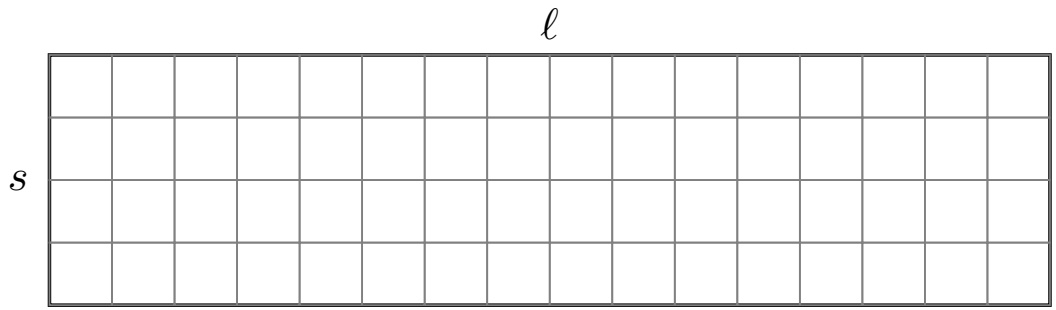
1: $R = \{\}$
2: **repeat**
3: $\quad z \xleftarrow{\$} Z$
4: $\quad$ Compute $S(z)$
5: $\quad$ Add to R a representative of the coset defined by $S(z)$
6: **until** $|R| = 2^{n-\dim Z}$

Example: LS Designs (e.g., Ascon)

Important Observation

If $\dim W_L(\{c_i + c_j \mid i, j\}) \geq n - 1$, the invariant attack does not apply!

This holds for any (reasonable) choice of the S-box layer.



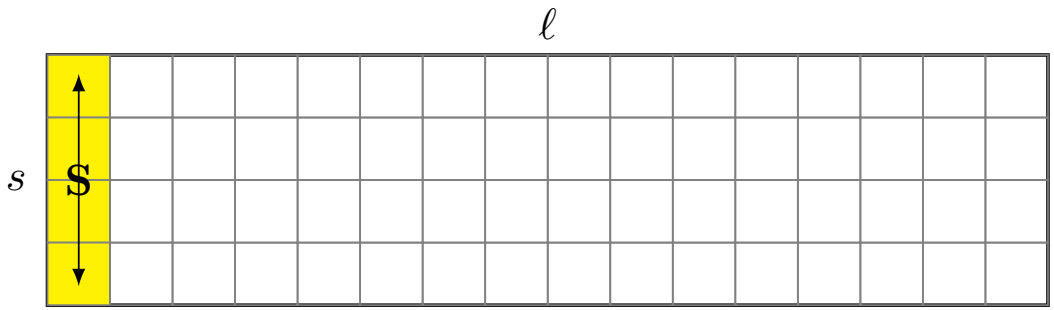
$$n = s \cdot \ell$$

Example: LS Designs (e.g., Ascon)

Important Observation

If $\dim W_L(\{c_i + c_j \mid i, j\}) \geq n - 1$, the invariant attack does not apply!

This holds for any (reasonable) choice of the S-box layer.



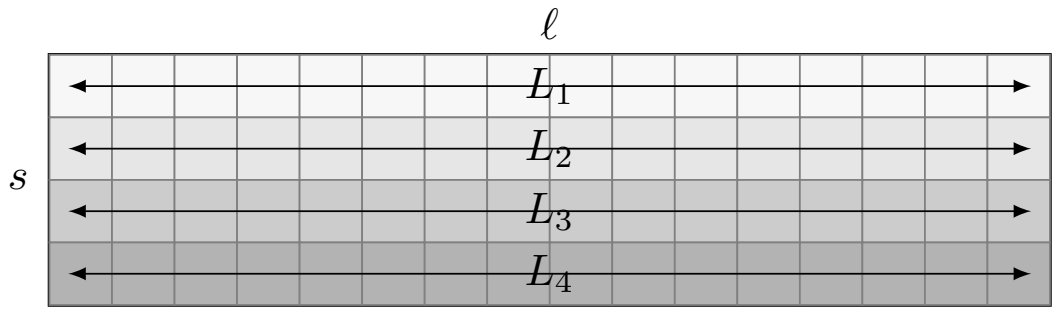
$$n = s \cdot \ell$$

Example: LS Designs (e.g., Ascon)

Important Observation

If $\dim W_L(\{c_i + c_j \mid i, j\}) \geq n - 1$, the invariant attack does not apply!

This holds for any (reasonable) choice of the S-box layer.

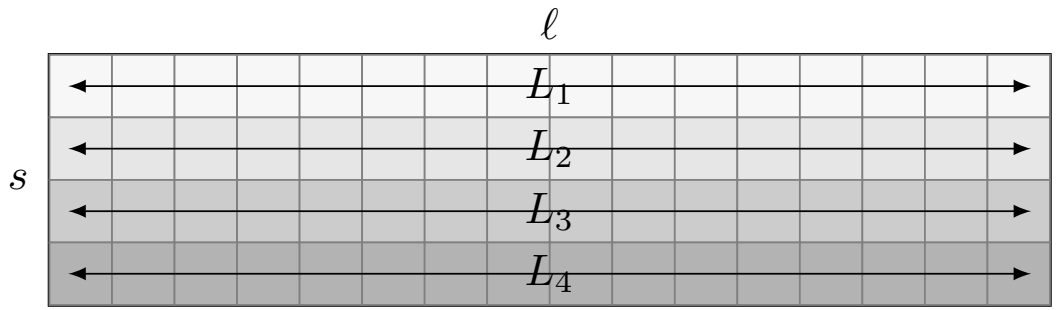


Example: LS Designs (e.g., Ascon)

Important Observation

If $\dim W_L(\{c_i + c_j \mid i, j\}) \geq n - 1$, the invariant attack does not apply!

This holds for any (reasonable) choice of the S-box layer.



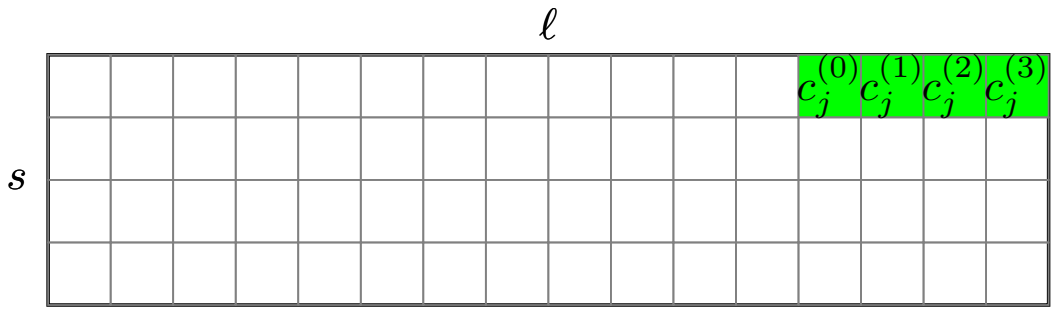
$$L = \begin{pmatrix} L_1 & & & \\ & L_2 & & \\ & & L_3 & \\ & & & L_4 \end{pmatrix}$$

Where to Put the Constants?

Important Observation

If $\dim W_L(\{c_i + c_j \mid i, j\}) \geq n - 1$, the invariant attack does not apply!

This holds for any (reasonable) choice of the S-box layer.



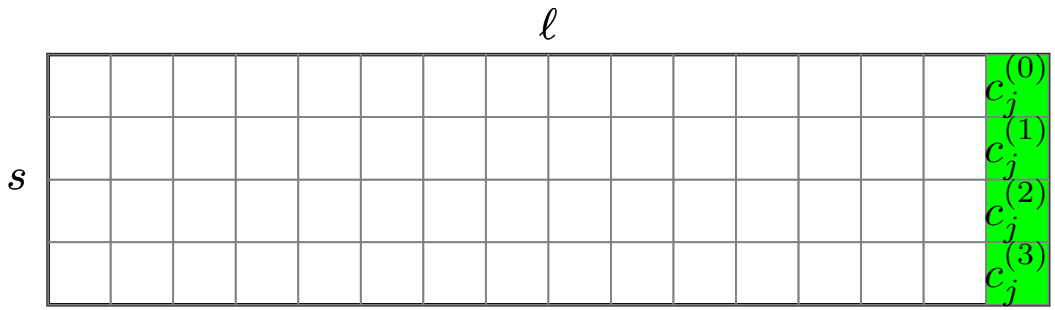
$$L = \begin{pmatrix} L_1 & & & \\ & L_2 & & \\ & & L_3 & \\ & & & L_4 \end{pmatrix}, \quad \dim W_L(\{c_i + c_j \mid i, j\}) \leq \ell$$

Where to Put the Constants?

Important Observation

If $\dim W_L(\{c_i + c_j \mid i, j\}) \geq n - 1$, the invariant attack does not apply!

This holds for any (reasonable) choice of the S-box layer.



For the argument, it would be better to put the constants in the columns.

Remark

A low dimension doesn't imply insecurity of the permutation!

1 Lightweight SPNs: Proving Resistance against Invariant Attacks

2 Design Criteria on the Linear Layer and the Round Constants

Very Different Behavior for each Cipher

Skinny-64-64. $\dim W_L(\{c_i + c_j \mid i, j\}) = 64$

The constants are sparse. In particular, $c_i + c_j = \texttt{0xab0000000000000}$.

Very Different Behavior for each Cipher

Skinny-64-64. $\dim W_L(\{c_i + c_j \mid i, j\}) = 64$

The constants are sparse. In particular, $c_i + c_j = \texttt{0xab00000000000000}$.

Prince. $\dim W_L(\{c_i + c_j \mid i, j\}) = 56$

Mantis-7. $\dim W_L(\{c_i + c_j \mid i, j\}) = 42$

The $c_i + c_j \in \mathbb{F}_2^{64}$ are dense (derived from the fractional digits of π).

Very Different Behavior for each Cipher

Skinny-64-64. $\dim W_L(\{c_i + c_j \mid i, j\}) = 64$

The constants are sparse. In particular, $c_i + c_j = \texttt{0xab00000000000000}$.

Prince. $\dim W_L(\{c_i + c_j \mid i, j\}) = 56$

Mantis-7. $\dim W_L(\{c_i + c_j \mid i, j\}) = 42$

The $c_i + c_j \in \mathbb{F}_2^{64}$ are dense (derived from the fractional digits of π).

Are the constants for Prince and Mantis just unluckily chosen?

It's a Property of the Linear Layer

For a single element c:

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

It's a Property of the Linear Layer

For a single element c:

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

$\dim W_L(c)$ equals the smallest d for which there exist $\lambda_0, \ldots, \lambda_d \in \mathbb{F}_2$:

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

It's a Property of the Linear Layer

For a single element c:

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

$\dim W_L(c)$ equals the smallest d for which 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 annihilating polynomial of c.**

It's a Property of the Linear Layer

For a single element c:

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

$\dim W_L(c)$ equals the smallest d for which 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 annihilating polynomial of c.**

Theorem

There exists a $c \in \mathbb{F}_2^n$ such that $\dim W_L(c) = d$ if and only if d is the degree of a divisor of the minimal polynomial m_L of L.

It's a Property of the Linear Layer

For a single element c:

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

$\dim W_L(c)$ equals the smallest d for which 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 annihilating polynomial of c.**

Theorem

There exists a $c \in \mathbb{F}_2^n$ such that $\dim W_L(c) = d$ if and only if d is the degree of a divisor of the minimal polynomial m_L of L.

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

Examples

Skinny-64.

$$m_L = (X+1)^{16} \in \mathbb{F}_2[X]$$

There exists a $c \in \mathbb{F}_2^{64}$ with $\dim W_L(c) = d$ if and only if $d \in \{1, \ldots, 16\}$.

Examples

Skinny-64.

$$m_L = (X+1)^{16} \in \mathbb{F}_2[X]$$

There exists a $c \in \mathbb{F}_2^{64}$ with $\dim W_L(c) = d$ if and only if $d \in \{1, \ldots, 16\}$.

Prince.

$$m_L = (X^4 + X^3 + X^2 + X + 1)^2 (X^2 + X + 1)^4 (X+1)^4 \in \mathbb{F}_2[X]$$

There exists a $c \in \mathbb{F}_2^{64}$ with $\dim W_L(c) = d$ if and only if $d \in \{1, \ldots, 20\}$.

Examples

Skinny-64.

$$m_L = (X+1)^{16} \in \mathbb{F}_2[X]$$

There exists a $c \in \mathbb{F}_2^{64}$ with $\dim W_L(c) = d$ if and only if $d \in \{1, \ldots, 16\}$.

Prince.

$$m_L = (X^4 + X^3 + X^2 + X + 1)^2 (X^2 + X + 1)^4 (X+1)^4 \in \mathbb{F}_2[X]$$

There exists a $c \in \mathbb{F}_2^{64}$ with $\dim W_L(c) = d$ if and only if $d \in \{1, \ldots, 20\}$.

Mantis and Midori.

$$m_L = (X+1)^6 \in \mathbb{F}_2[X]$$

There exists a $c \in \mathbb{F}_2^{64}$ with $\dim W_L(c) = d$ if and only if $d \in \{1, \ldots, 6\}$.

Considering more Constants: The Rational Canonical Form

If $\deg(m_L) = n$, there exists a basis for which the matrix of L is the **companion matrix** of m_L.

Definition: Companion Matrix

Let $p = X^m + \prod_{i=0}^{m-1} p_i X^i \in \mathbb{F}_2[X]$. The companion matrix of p is

$$C(p) := \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & & & & \\ 0 & 0 & 0 & \dots & 1 \\ p_0 & p_1 & p_2 & \dots & p_{m-1} \end{pmatrix}$$

Considering more Constants: The Rational Canonical Form

If $\deg(m_L) = n$, there exists a basis for which the matrix of L is the **companion matrix** of m_L.

Definition: Companion Matrix

Let $p = X^m + \prod_{i=0}^{m-1} p_i X^i \in \mathbb{F}_2[X]$. The companion matrix of p is

$$C(p) := \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & & & & \\ 0 & 0 & 0 & \dots & 1 \\ p_0 & p_1 & p_2 & \dots & p_{m-1} \end{pmatrix}$$

In general, there exists 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 $Q_r \mid Q_{r-1} \mid \cdots \mid Q_1 = m_L$.
$Q_1, Q_2, \dots, Q_r$ are called the **invariant factors of L**.

Considering more Constants: The Rational Canonical Form

Theorem

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

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

In particular, one needs r elements to obtain the maximal dimension $\mathbb{F}_2^n$.

Considering more Constants: The Rational Canonical Form

Theorem

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

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

In particular, one needs r elements to obtain the maximal dimension $\mathbb{F}_2^n$.

Prince. The invariant factor decomposition is

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

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.

Considering more Constants: The Rational Canonical Form

Theorem

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

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

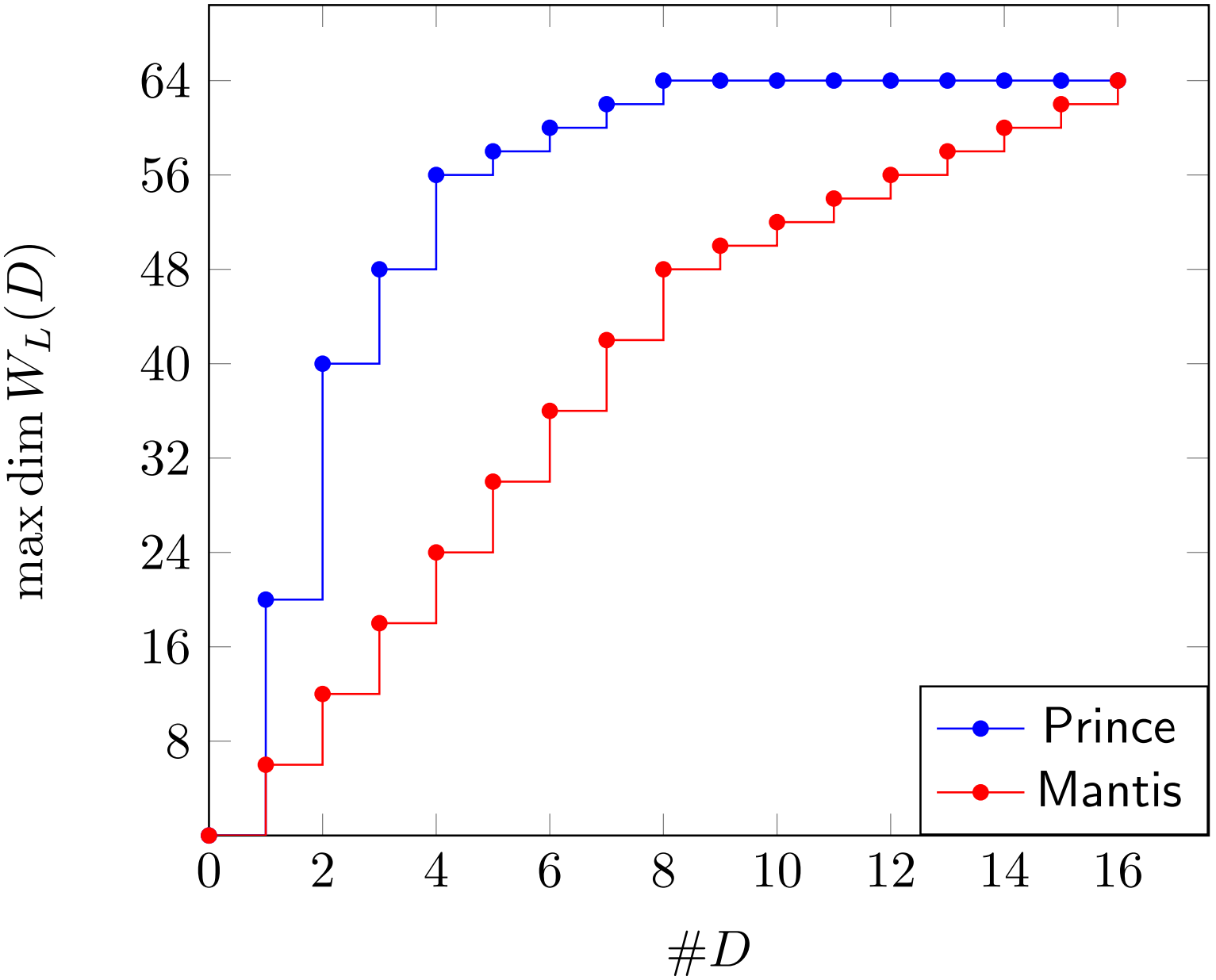
In particular, one needs r elements to obtain the maximal dimension $\mathbb{F}_2^n$.

Mantis and Midori. The invariant factor decomposition is

$$\begin{aligned} Q_1 &= Q_2 = Q_3 = Q_4 = Q_5 = Q_6 = Q_7 = Q_8 = X^6 + 1 \\ Q_9 &= Q_{10} = Q_{11} = Q_{12} = Q_{13} = Q_{14} = Q_{15} = Q_{16} = X^2 + 1 \end{aligned}$$

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

The Maximal Dimension for $\#D$ Constants

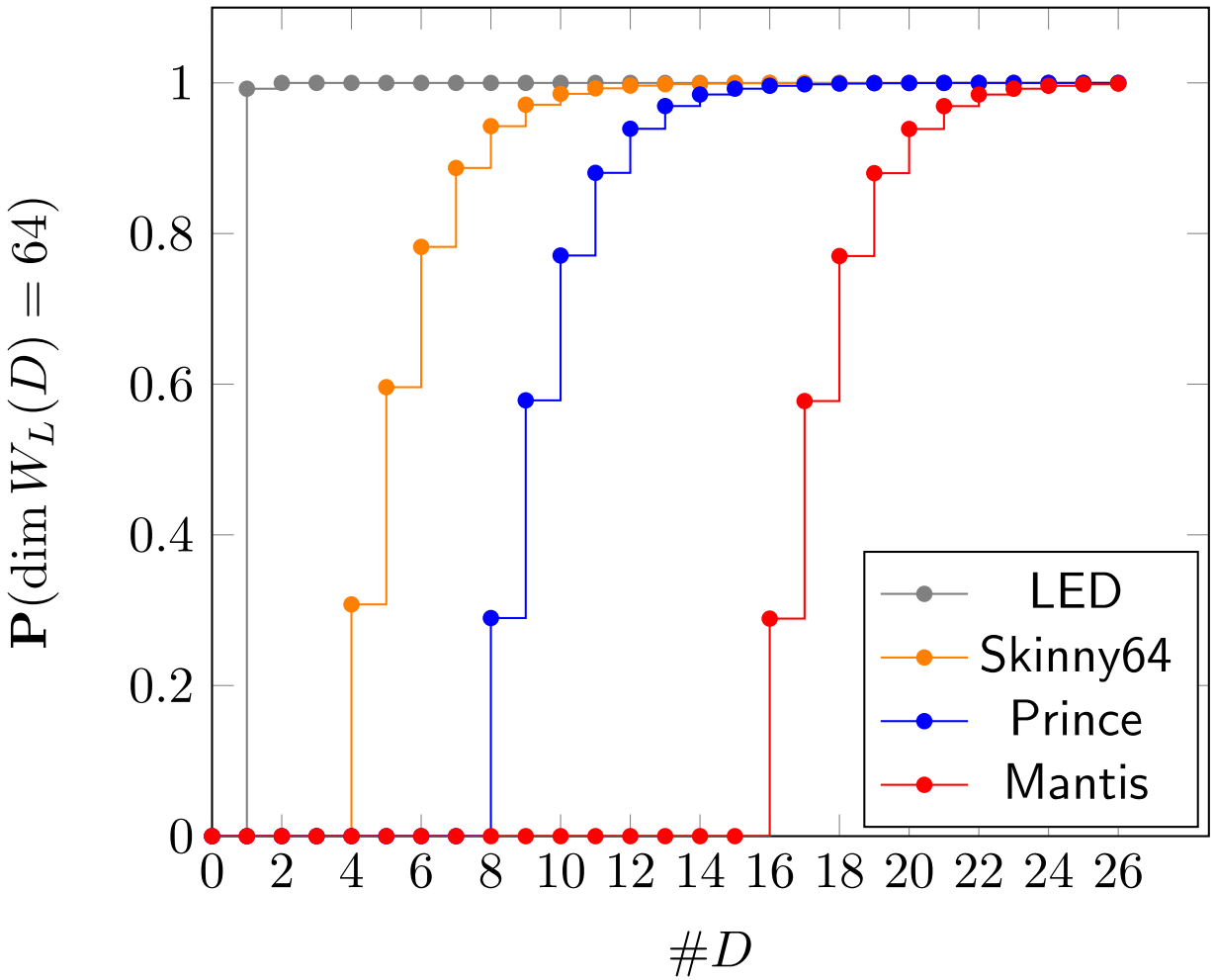


Choosing Random Round Constants

For $t \geq r$, the probability that t uniformly chosen constants c_i generate the whole $\mathbb{F}_2^n$ can be computed from the invariant factors of L.

Choosing Random Round Constants

For $t \geq r$, the probability that t uniformly chosen constants c_i generate the whole $\mathbb{F}_2^n$ can be computed from the invariant factors of L.



Conclusion

- For permutations based on SPNs with round constants, there is a (very simple) algorithmic way to prove the resistance against a large class of invariant attacks.

Conclusion

- For permutations based on SPNs with round constants, there is a (very simple) algorithmic way to prove the resistance against a large class of invariant attacks.

Simple Algorithm

- **Input:** Linear layer L, RC differences $\{c_i + c_j \mid i, j\}$
- check if $\dim\langle\{L^k(c_i + c_j) \mid k < \mathrm{order}(L), i, j\}\rangle \geq n - 1$

Conclusion

- For permutations based on SPNs with round constants, there is a (very simple) algorithmic way to prove the resistance against a large class of invariant attacks.

Simple Algorithm

- **Input:** Linear layer L, RC differences $\{c_i + c_j \mid i, j\}$
- check if $\dim\langle\{L^k(c_i + c_j) \mid k < \mathrm{order}(L), i, j\}\rangle \geq n - 1$

- Depending on the linear layer, one can derive an upper bound on the minimum number of round constants that are necessary for the argument –> Design criteria

Conclusion

- For permutations based on SPNs with round constants, there is a (very simple) algorithmic way to prove the resistance against a large class of invariant attacks.

Simple Algorithm

- **Input:** Linear layer L, RC differences $\{c_i + c_j \mid i, j\}$
- check if $\dim\langle\{L^k(c_i + c_j) \mid k < \mathrm{order}(L), i, j\}\rangle \geq n - 1$

- Depending on the linear layer, one can derive an upper bound on the minimum number of round constants that are necessary for the argument –> Design criteria

Future work:

- Can we avoid the restriction of using the same invariant for each of the constituent building blocks? (see [Beyne 2018])

Conclusion

- For permutations based on SPNs with round constants, there is a (very simple) algorithmic way to prove the resistance against a large class of invariant attacks.

Simple Algorithm

- **Input:** Linear layer L, RC differences $\{c_i + c_j \mid i, j\}$
- check if $\dim\langle\{L^k(c_i + c_j) \mid k < \mathrm{order}(L), i, j\}\rangle \geq n - 1$

- Depending on the linear layer, one can derive an upper bound on the minimum number of round constants that are necessary for the argument –> Design criteria

Future work:

- Can we avoid the restriction of using the same invariant for each of the constituent building blocks? (see [Beyne 2018])

Thanks for your attention! Any questions?