Choosing Round Constants in Lightweight Block Ciphers

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

January 8, 2019

Radboud University

Results

Block ciphers:

- Proving Resistance against Invariant attacks, CRYPTO 2017, with C. Beierle, A. Canteaut and G. Leander.

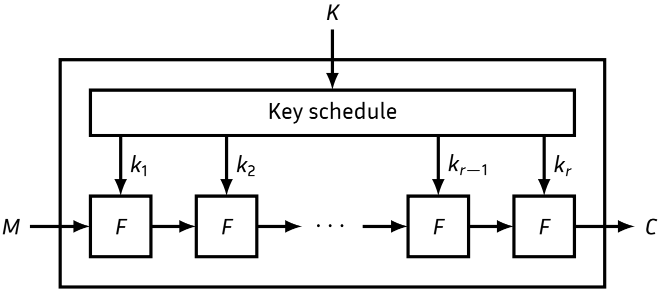
Stream ciphers and PRNG:

- Cryptanalysis of Filter generators, FSE 2016, with A. Canteaut;
- Cryptanalysis of FLIP, CRYPTO 2016, with S. Duval and V. Lallemand;
- Design of Restricted Boolean functions, ToSC 2017, with C. Carlet and P. Méaux;
- Cryptanalysis of Goldreich's PRG, ASIACRYPT 2018, with G. Couteau, A. Dupin, P. Méaux and M. Rossi.

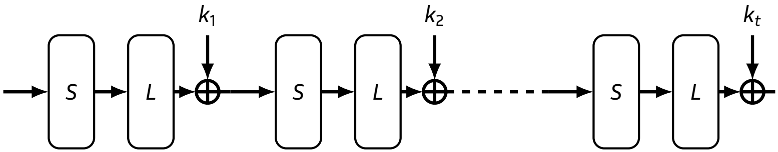
Authenticated Encryption:

- Cryptanalysis of Ketje, ToSC 2018, with T. Fuhr and M. Naya-Pasencia;
- Cryptanalysis of MORUS, ASIACRYPT 2018, with T. Ashur, M. Eichlseder, M. M. Lauridsen, G. Leurent, B. Minaud, Y. Sasaki and B. Viguier.

Block Ciphers



Substitution Permutation Network

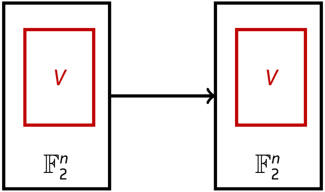


Structure of this Talk

Plan of this Section

The invariant subspace attack [Leander et al. 11]

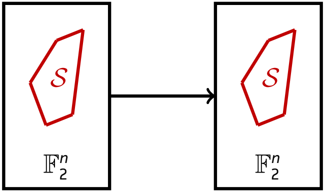
Affine subspace V invariant under E_k.



$$E_k(V) = V$$

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

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



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

Definition (Invariant)

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

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

g is called an **invariant for E_k**.

Vulnerable Lightweight Ciphers

- 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]

Goal

Definition (Invariant)

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

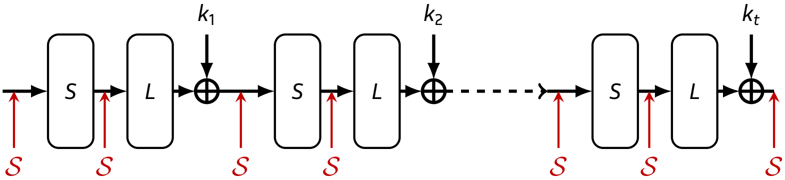
$$\forall x \in \mathbb{F}_2^n, g \circ E_k(x) + g(x) = c \text{ with } c = 0 \text{ or } c = 1$$

g is called an **invariant for E_k.**

We want to prove the absence of such invariants g

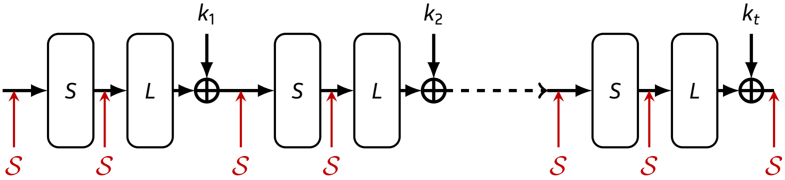
The case of SPN ciphers

- Finding all invariants for the whole round is computationnaly hard.
- Main attacks exploits invariants for S **and** $\mathrm{Add}_{k_i} \circ L$.



We restrict our study to invariant that are invariants for both S and $\mathrm{Add}_{k_i} \circ L$

The case of SPN ciphers



Definition (linear structure)

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

Two conditions on g

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

Simple key schedule

If $k_i = k + \mathrm{RC}_i$,

$$\text{Let } D = \{(\mathrm{RC}_i + \mathrm{RC}_j)\} \text{ and}$$

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

Question

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

$$W_L(D) \subseteq \mathrm{LS}(g)\,?$$

Plan of this Section

The simple case

If $\mathbf{dim}\ \boldsymbol{W_L(D)} \geq \boldsymbol{n-1}$, then the invariant attack does not apply.

For example :

- Skinny-64 ($n = 64$). $\mathbf{dim}\ \boldsymbol{W_L(D) = 64}$ ✓
- Prince. $\mathbf{dim}\ \boldsymbol{W_L(D) = 56}$
- Mantis-7. $\mathbf{dim}\ \boldsymbol{W_L(D) = 42}$
- Midori-64. $\mathbf{dim}\ \boldsymbol{W_L(D) = 16}$

The general case ($\dim W_L(D) < n - 1$)

An invariant g must satisfy $W_L(D) \subseteq \mathrm{LS}(g)$.

- $\mathrm{LS}_0(g) = \{\alpha, \forall x, g(x) + g(\alpha + x) = 0\}$
- $\mathrm{LS}_1(g) = \{\alpha, \forall x, g(x) + g(\alpha + x) = 1\}$

Proposition

Let g be an invariant for an n-bit permutation S such that $\mathrm{LS}_0(g) \supseteq Z$ for some given subspace $Z \subset \mathbb{F}_2^n$. Then

- *g is constant on each coset of Z;*
- *g is constant on $S(Z)$.*

The general case ($\dim W_L(D) < n-1$)

Lemma

Let g be an invariant for $\mathrm{Add}_{k_i} \circ L$ for some k_i. Then, for any $v \in \mathrm{LS}(g)$, $v + L(v) \in \mathrm{LS}_0(g)$.

$D = \{\mathrm{RC}_i + \mathrm{RC}_j\}$

- $Z = \{d + L(d), d \in D\}$

Results on some Lightweight ciphers

- Skinny-64 ($n = 64$). $\dim W_L(D) = 64$ ✓
- Prince. $\dim W_L(D) = 56$ ✓
- Mantis-7. $\dim W_L(D) = 42$ ✓
- Midori-64. $\dim W_L(D) = 16$ ✗

Plan of this Section

Why the dimensions are so different ?

- Skinny-64 ($n = 64$). $\dim W_L(D) = 64$
- Prince. $\dim W_L(D) = 56$
- Mantis-7. $\dim W_L(D) = 42$
- Midori-64. $\dim W_L(D) = 16$

If $D = \{c\}$ (single element)

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

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 with respect to L

If $D = \{c\}$ (single element)

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

$\dim W_L(c) =$ 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 with respect to L

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.

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

Examples

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

Rational canonical form

- When $\mathbf{deg}(\mathrm{Min}_L) = n$, L is similar 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,

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

$Q_1 = \mathrm{Min}_L, Q_2, \dots, Q_r$ are the invariant factors of L, with $Q_i | Q_{i-1}$ for all $1 \leq i \leq r$.

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 $W_L(c_1, \dots, c_t)$

Theorem

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

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

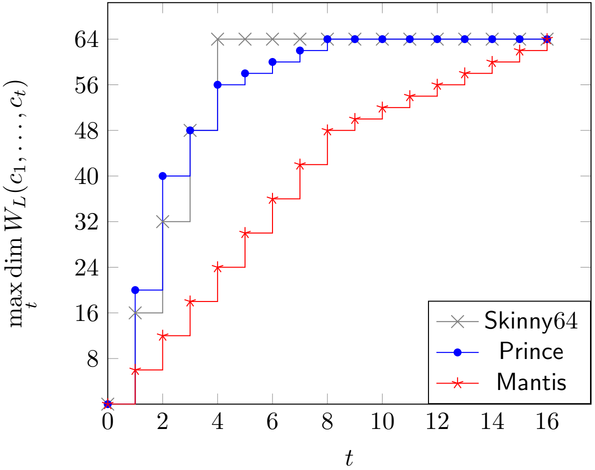
We need r elements to get $W_L(D) = \mathbb{F}_2^n$.

For Prince.

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

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

Maximum dimension for #*D* constants



For random constants

For $t \geq r$,

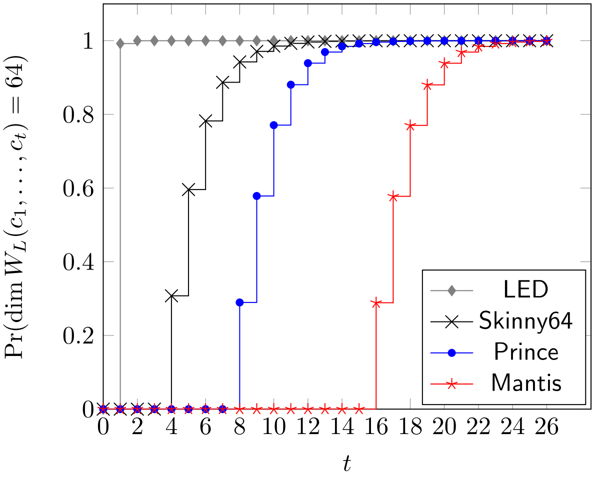
$$\Pr_{c_1,\ldots,c_t \xleftarrow{\$} \mathbb{F}_2^n} [W_L(c_1, \cdots, c_t) = \mathbb{F}_2^n]$$

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

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

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

Probability to achieve the full dimension



Plan of this Section

1. Context
2. Introduction and first observations
3. Proving resistance against the attack
4. How to choose the round constants
5. Conclusion

Conclusion

Easy to prevent the attack:

- by choosing a linear layer which does not have many invariant factors.
- by choosing appropriate round constants

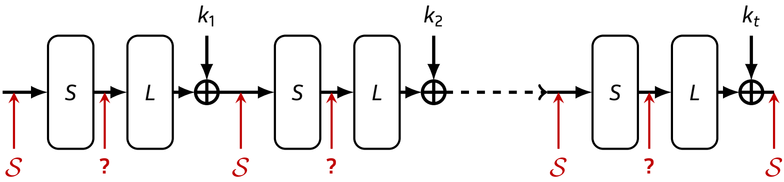
Conclusion

Easy to prevent the attack:

- by choosing a linear layer which does not have many invariant factors.
- by choosing appropriate round constants

Perspectives:

- Use different invariants for the Sbox-layer and the linear layer [Beyne, 2018, Asiacrypt] ?
- Generalized Invariants : $g(x + a_i) + g(E_k(x) + a_j) = c$ [Wei, Ye, Wu, Pasalic, 2018, IACR ToSC]



Thank You

Questions ?