Cryptanalysis of PRINTCIPHER: The Invariant Subspace Attack

Gregor Leander, Mohamed Abdelraheem, Huda AlKhzaimi, and Erik Zenner

DTU Mathematics

CRYPTO 2011

Outline

Outline

Introduction

PRINTcipher

Lightweight SPN block cipher proposed at CHES 2010.

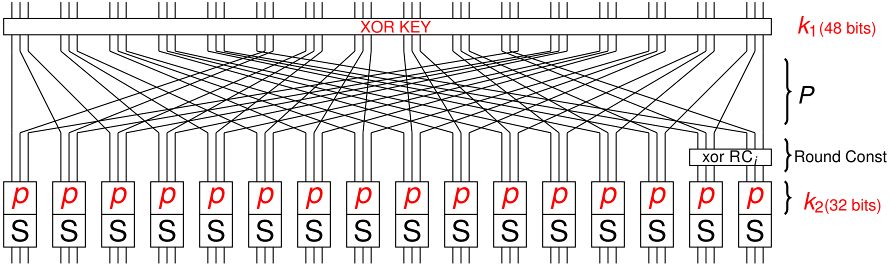
Idea: Take advantage of a key.

Claim

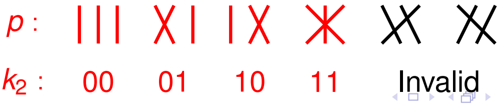
Secure against known attacks.

So far: Attacks on reduced-round variants.

One round of PRINTcipher-48



- 48-bits block size, 48 rounds that use the same 80-bit key.
- Each two bits of k_2 permute 3 state bits in a certain way.
- Only 4 out of 6 possible permutations are allowed:



Simplify Things

In this talk (not in the paper!): A simpler variant of PRINTcipher.

- Block size 24
- Fix the permutation key
- Modified Sbox

Sbox Property

Modified Sbox:

$$S(000) = 000 \qquad S(001) = 001$$
$$S(010) = 010 \qquad S(100) = 100$$

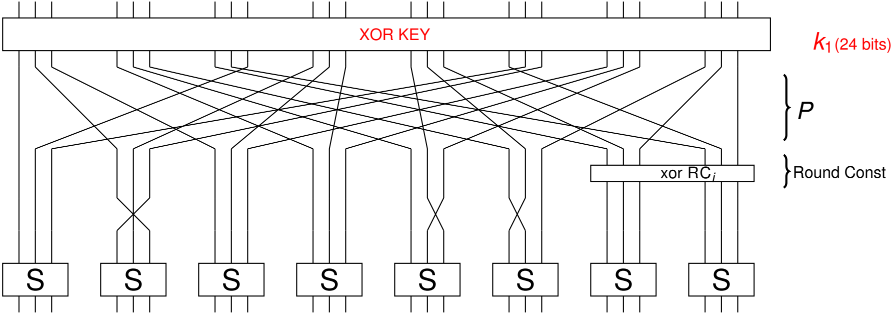
Can be written as:

$$\begin{aligned} S(00*) &= 00* \\ S(0*0) &= 0*0 \\ S(*00) &= *00 \end{aligned}$$

Remark

The original Sbox fulfils something similar.

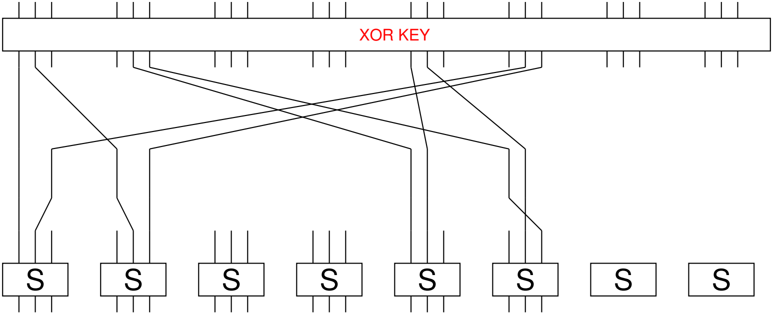
Simplified Version



$$
\begin{aligned}
S(00*) &= 00* \\
S(0*0) &= 0*0 \\
S(*00) &= *00
\end{aligned}
$$

Outline

Let's Focus



Invariant Subspace for *P*

Set of highlighted bits is mapped onto itself.

What about S

An Invariant Subspace alone is not a problem!

Question

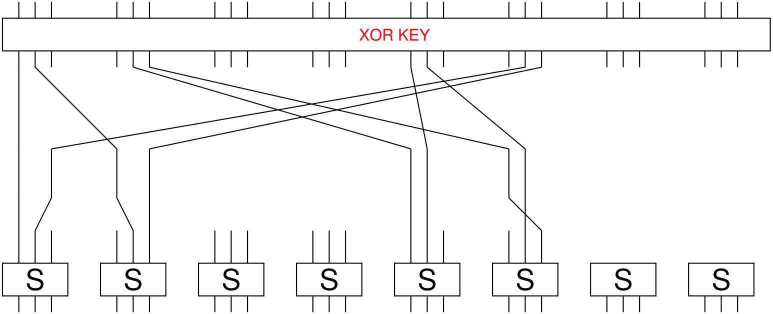
What about the S-layer?

For this: we fix some bits

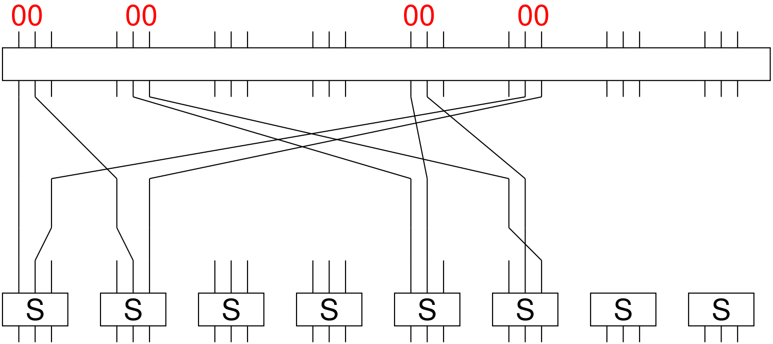
- in the plaintext
- in the (XOR)-key

$\Rightarrow$ The attack does not work for all keys.

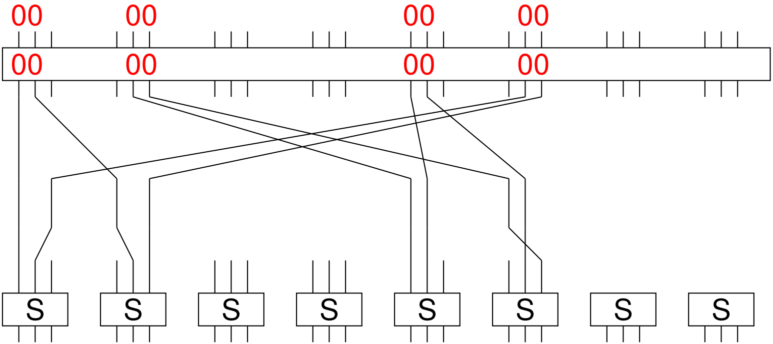
Simplified Version



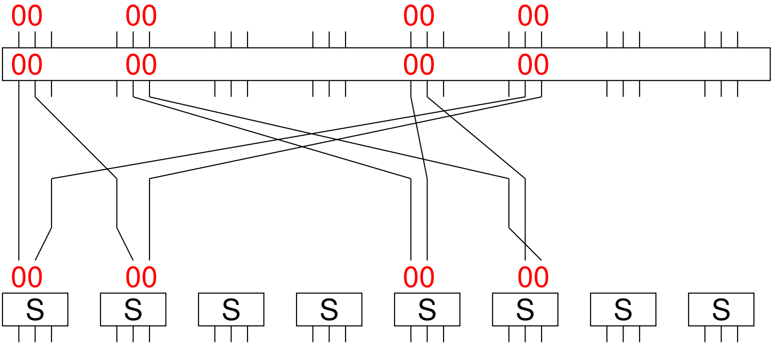
Simplified Version



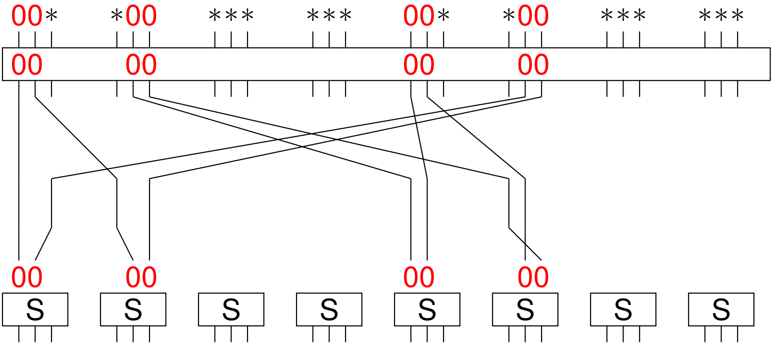
Simplified Version



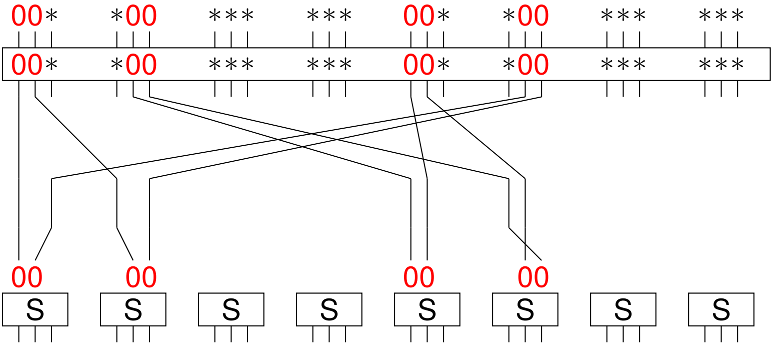
Simplified Version



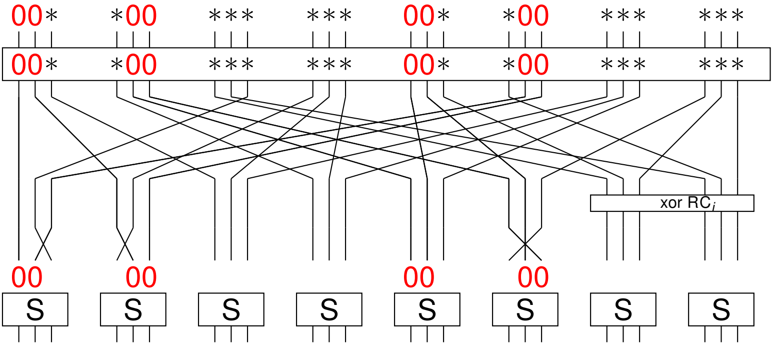
Simplified Version



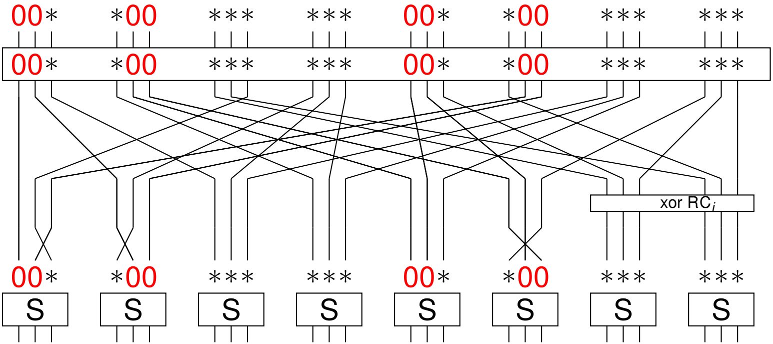
Simplified Version



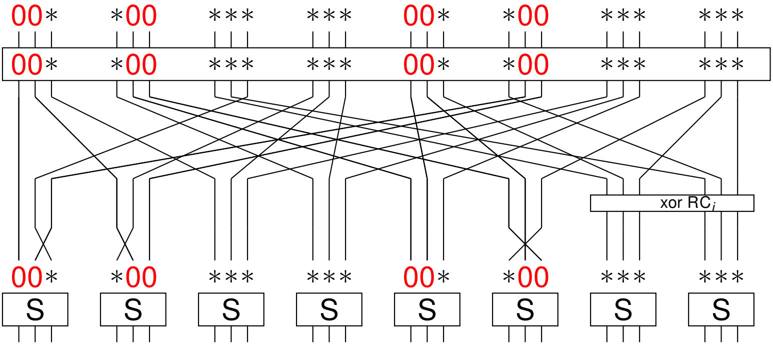
Simplified Version



Simplified Version

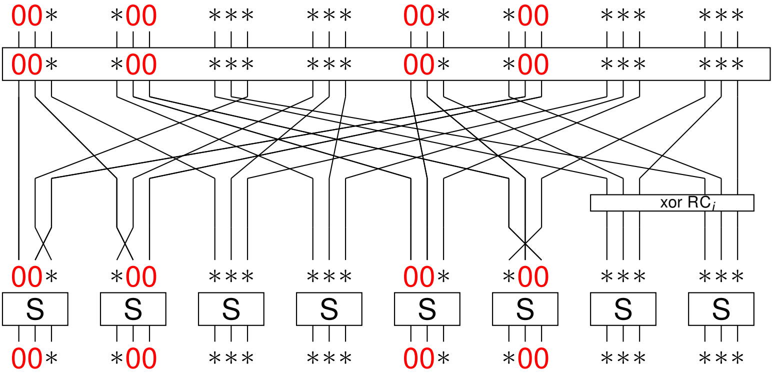


Simplified Version



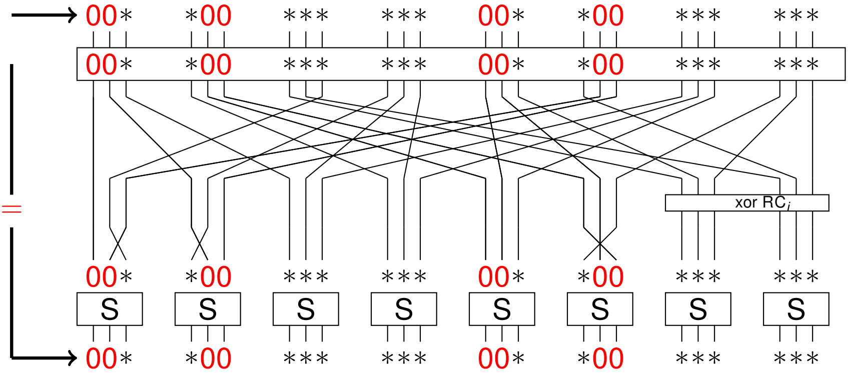
$$S(00*) = 00* \quad S(0*0) = 0*0 \quad S(*00) = *00$$

Simplified Version



$$S(00*) = 00* \quad S(0*0) = 0*0 \quad S(*00) = *00$$

Simplified Version



$$S(00*) = 00* \quad S(0*0) = 0*0 \quad S(*00) = *00$$

An Iterative One-Round Distinguisher

If certain key bits are zero:

Distinguisher

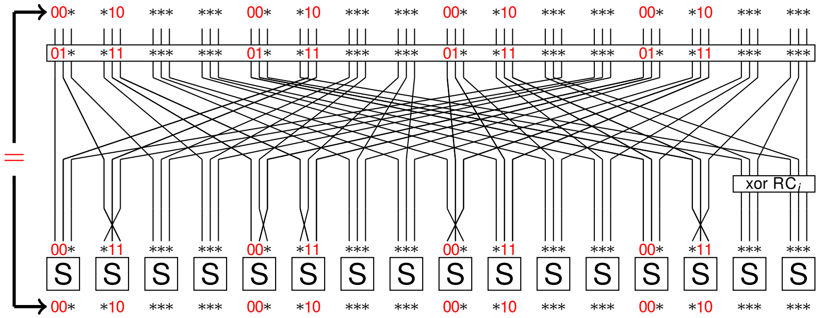
Zero bits in the plaintext $\Rightarrow$ zero bits in the ciphertext.

Some Remarks:

- Round-constant does not help
- Works for the whole cipher

Let's look at PRINTCIPHER-48

The Attack on PRINTcipher-48



$$S(00*) = 00*$$
$$S(1*0) = 1*1$$
$$S(*11) = *10$$

PRINTCIPHER-48 Attack

Summary

- Prob 1 distinguisher for full cipher
- 2^{50} out of 2^{80} keys weak.
- Similar for PRINTCIPHER-96

Abstraction:

$$R(U \oplus d) = U \oplus c$$

If $k \in U \oplus (d \oplus c)$

$$R_k(U \oplus d) = U \oplus d$$

Thus an invariant subspace

Outline

The Probability of A Characteristic

Given a r-round differential characteristic

$$\alpha \xrightarrow{p} \alpha \xrightarrow{p} \cdots \xrightarrow{p} \alpha$$

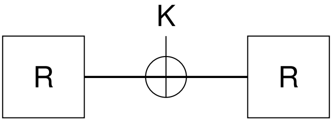
Theorem

Given independent round keys the average probability is p^r

Hypothesis of Stochastic Equivalence

All keys behave similarly.

Two Round Characteristics



$$\alpha \longrightarrow \alpha \longrightarrow \alpha$$

$$A := \{x \mid R(x) \oplus R(x \oplus \alpha) = \alpha\}$$

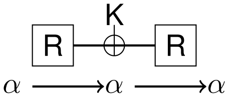
"*A* is the set of good pairs"

Two Rounds, fixed Key

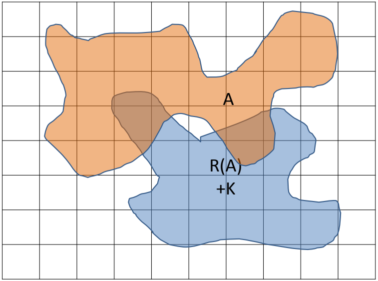
Probability of the characteristic for a key K:

$$\frac{|\,(R(A) \oplus K) \bigcap A|}{2^n}$$

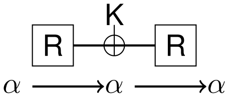
Two Rounds, fixed Key



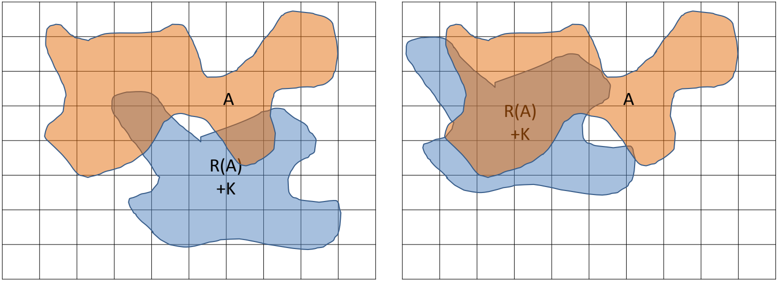
Good Pairs: $A := \{x \mid R(x) \oplus R(x \oplus \alpha) = \alpha\}$
Probability (scaled): $|\,(R(A) \oplus K) \bigcap A|$



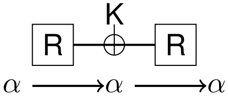
Two Rounds, fixed Key



Good Pairs: $A := \{x \mid R(x) \oplus R(x \oplus \alpha) = \alpha\}$
Probability (scaled): $|\,(R(A) \oplus K) \bigcap A|$



Back To PRINTCIPHER-48



Good Pairs: $A := \{x \mid R(x) \oplus R(x \oplus \alpha) = \alpha\}$

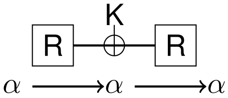
Observations for special α

- A is an affine subspace $U \oplus d$
- U is invariant under R
- $\Rightarrow \; R(A) = U \oplus c$

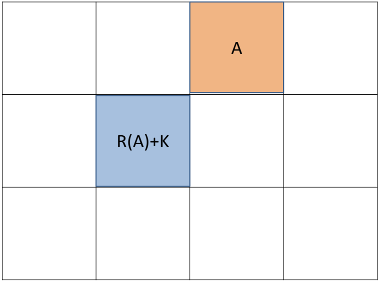
Probability (scaled):

$$\left|(R(A) \oplus K) \bigcap A\right| = \left|(U \oplus c \oplus K) \bigcap (U \oplus d)\right|$$

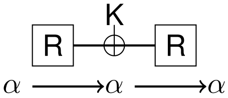
Two Rounds, fixed Key: PRINTCIPHER-48



Good Pairs: $A := \{x \mid R(x) \oplus R(x \oplus \alpha) = \alpha\}$
Probability (scaled): $|\,(R(A) \oplus K) \bigcap A|$

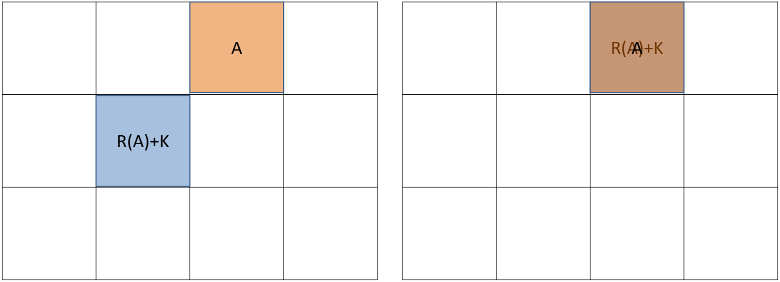


Two Rounds, fixed Key: PRINTCIPHER-48



Good Pairs: $A := \{x \mid R(x) \oplus R(x \oplus \alpha) = \alpha\}$

Probability (scaled): $|\,(R(A) \oplus K) \bigcap A|$



PRINTCIPHER-48

There exist a r-round differential characteristic

$$\alpha \to \alpha \to \cdots \to \alpha$$

such that

$$p_k = \begin{cases} 2^{-16} & \text{if} \quad k \text{ is weak} \\ 0 & \text{if} \quad k \text{ is not weak} \end{cases}$$

Remarks

- Probabilities do not multiply.
- Keys behave very differently

Outline

Conclusion

Summary: Invariant Subspace Attack

- Weak keys for full PRINTCIPHER-48 and PRINTCIPHER-96
- Strange behavior of differential characteristics
- Similar observation for linear attacks

Future Work

- Generalize the attack
- Key recovery variant
- Explain linear biases directly

The End

Thanks!