The Attack

Relation To Truncated Differential Attack

ヘロト ヘポト ヘヨト ヘヨト

э

1/24

Conclusion

# Cryptanalysis of PRINTCIPHER: The Invariant Subspace Attack

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

**DTU Mathematics** 

CRYPTO 2011

Description	PRINTCIPHER

The Attack

Relation To Truncated Differential Attack

## Outline



2 The Attack

3 Relation To Truncated Differential Attack

## 4 Conclusion



Description	of	PRIN	TCIPHER

The Attack

Relation To Truncated Differential Attack

## Outline



- 2 The Attack
- 3 Relation To Truncated Differential Attack

## 4 Conclusion



The Attack

Relation To Truncated Differential Attack

Conclusion

## 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.



The Attack

Relation To Truncated Differential Attack

Conclusion

4/24

# One round of PRINTCIPHER-48



- 48-bits block size, 48 rounds that use the same 80-bit key.
- Each two bits of k<sub>2</sub> permute 3 state bits in a certain way.
- Only 4 out of 6 possible permutations are allowed:

$$p$$
: $|||$  $X|$  $|X|$  $X$  $X$  $X$  $k_2$ :00011011Invalid

Description of PRINTCIPHER	The Attack	Relation To Truncated Differential Attack	Conclusion
Simplify Things			

<ロ> (四) (四) (日) (日) (日)

э

5/24

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

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

Description of PRINTCIPHER 000●0	The Attack	Relation To Truncated Differential Attack	Conclusion
Sbox Property			

Modified Sbox:

S(000) = 000 S(001) = 001S(010) = 010 S(100) = 100

Can be written as:

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

#### Remark

The original Sbox fulfils something similar.



The Attack

Relation To Truncated Differential Attack

Conclusion

DTU

7/24

э

# **Simplified Version**



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

Description	PRINTCIPHER

The Attack

Relation To Truncated Differential Attack

## Outline

## Description of PRINTCIPHER

- 2 The Attack
- 8 Relation To Truncated Differential Attack

## 4 Conclusion



Description of PRINTCIPHER	The Attack	Relation To Truncated Differential Attack	C
Let's Focus			



DTU

9/24

・ロト ・ 日 ・ ・ 目 ・ ・

#### Invariant Subspace for P

Set of highlighted bits is mapped onto itself.

	00000	
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.



The Attack

Relation To Truncated Differential Attack

Conclusion

# Simplified Version



UTU 북태 《 마 〉 《 문 〉 《 문 〉 《 문 〉 이 이 이 11/24

The Attack

Relation To Truncated Differential Attack

Conclusion

# **Simplified Version**



UTU ま ペロン ペラン ペミン ミン ミ のへで 11/24

The Attack

Relation To Truncated Differential Attack

Conclusion

# Simplified Version



UTU ま ペロン ペラン ペミン ミン ミ のへで 11/24

The Attack

Relation To Truncated Differential Attack

Conclusion

# **Simplified Version**



UTU 북북 《미》《문》《문》 문 외익은 11/24

The Attack

Relation To Truncated Differential Attack

Conclusion

# **Simplified Version**



UTU ま ペロン ペラン ペミン ミン ミ のへで 11/24

The Attack

Relation To Truncated Differential Attack

Conclusion

# **Simplified Version**



UTU ま ペロン ペラン ペミン ミン ミ のへで 11/24

The Attack

Relation To Truncated Differential Attack

Conclusion

# **Simplified Version**



The Attack

Relation To Truncated Differential Attack

Conclusion

## **Simplified Version**



The Attack

Relation To Truncated Differential Attack

Conclusion

DTU

11/24

э

(a)

## Simplified Version



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

The Attack

Relation To Truncated Differential Attack

Conclusion

# Simplified Version



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

э

< 日 > < 同 > < 回 > < 回 > < □ > <

The Attack

Relation To Truncated Differential Attack

Conclusion

# Simplified Version



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

э

< 日 > < 同 > < 回 > < 回 > < □ > <

The Attack

Relation To Truncated Differential Attack

Conclusion

# 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

Relation To Truncated Differential Attack

Conclusion

## The Attack on PRINTCIPHER-48



13/24

The Attack

Relation To Truncated Differential Attack

Conclusion

14/24

# **PRINTCIPHER-48 Attack**

#### Summary

- Prob 1 distinguisher for full cipher
- 2<sup>50</sup> out of 2<sup>80</sup> 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

Description	PRINTCIPHER

The Attack

Relation To Truncated Differential Attack

## Outline



- 2 The Attack
- 3 Relation To Truncated Differential Attack

### 4 Conclusion



The Attack

Relation To Truncated Differential Attack

Conclusion

# 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<sup>r</sup>

#### Hypothesis of Stochastic Equivalence

All keys behave similarly.



The Attack

Relation To Truncated Differential Attack

Conclusion

# **Two Round Characteristics**



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

"A is the set of good pairs"

Two Rounds, fixed Key

Probability of the characteristic for a key K:

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



The Attack

Relation To Truncated Differential Attack

Conclusion

☱

18/24

э

## Two Rounds, fixed Key



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



The Attack

Relation To Truncated Differential Attack

Conclusion

# Two Rounds, fixed Key



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



18/24

☱

The Attack

Relation To Truncated Differential Attack

Conclusion

୬ ର ୍ଦ 19/24

# **Back To PRINTCIPHER-48**



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

#### Observations for special $\alpha$

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

Probability (scaled):

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

The Attack

Relation To Truncated Differential Attack

э

20/24

Conclusion

# Two Rounds, fixed Key: PRINTCIPHER-48



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

	A	
R(A)+K		

The Attack

Relation To Truncated Differential Attack

Conclusion

# Two Rounds, fixed Key: PRINTCIPHER-48



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

	A	
R(A)+K		

	R( <i>A</i> 4)+K	



Description of PRINTCIPHER	The Attack	Relation To Truncated Differential Attack	Conclusion
PRINTCIPHER-4	8		

#### There exist a r-round differential characteristic

$$\alpha \to \alpha \to \dots \to \alpha$$

#### such that

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

<ロ> (四) (四) (日) (日) (日)

21/24

#### Remarks

- Probabilities do not multiply.
- Keys behave very differently

Description	PRINTCIPHER

The Attack

Relation To Truncated Differential Attack

Conclusion

## Outline

## Description of PRINTCIPHER

2 The Attack

3 Relation To Truncated Differential Attack

# 4 Conclusion



Description	PRINT	CIPHER

The Attack

Relation To Truncated Differential Attack

<ロ> <回> <回> <回> < 回> < 回>

Conclusion

23/24

# 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

Description of PRINTCIPHER	The Attack	Relation To Truncated Differential Attack	Conclusion
The End			

# Thanks!