A Model for Structure Attacks, with Applications to PRESENT and Serpent

Meiqin Wang[1], Yue Sun[2], Elmar Tischhauser[3] and Bart Preneel[3]

[1]Shandong University, [2]Tsinghua University, [3]KU Leuven and IBBT

FSE 2012
March 19, 2012

Outline

1. Motivation
2. Modeling structure attacks
3. Attacking PRESENT and Serpent
4. Conclusions and outlook

Motivation: How to leverage multiple differentials?

Using multiple differentials has advantages

- More likely to hit right pair $\Rightarrow$ decrease data complexity
- Unlike linear cryptanalysis: always constructive
- Success stories: DES, Serpent

Caveats

- Too many differentials can increase complexity
- Multiple input, multiple output, both?
- How many active bits/S-boxes at input/output?

$\Longrightarrow$ General model needed for evaluation

Motivation: How to leverage multiple differentials?

Using multiple differentials has advantages

- More likely to hit right pair $\Rightarrow$ decrease data complexity
- Unlike linear cryptanalysis: always constructive
- Success stories: DES, Serpent

Caveats

- Too many differentials can increase complexity
- Multiple input, multiple output, both?
- How many active bits/S-boxes at input/output?

$\Longrightarrow$ General model needed for evaluation

Motivation: How to leverage multiple differentials?

Using multiple differentials has advantages

- More likely to hit right pair $\Rightarrow$ decrease data complexity
- Unlike linear cryptanalysis: always constructive
- Success stories: DES, Serpent

Caveats

- Too many differentials can increase complexity
- Multiple input, multiple output, both?
- How many active bits/S-boxes at input/output?

$\Longrightarrow$ General model needed for evaluation

State of the art: What we know

Historical introduction

- Biham and Shamir 1990: Quartets, Octets, etc.
- ... widespread informal use ...
- Blondeau and Gérard, FSE 2011: Comprehensive framework for multiple differentials

What's left to do then?

- Model of FSE'11: Analysis requires fairly restrictive condition on differentials
  - Can this be avoided?
- Some small technical problems with the attack on 18-round PRESENT

State of the art: What we know

Historical introduction

- Biham and Shamir 1990: Quartets, Octets, etc.
- ... widespread informal use ...
- Blondeau and Gérard, FSE 2011: Comprehensive framework for multiple differentials

What's left to do then?

- Model of FSE'11: Analysis requires fairly restrictive condition on differentials
  - Can this be avoided?
- Some small technical problems with the attack on 18-round PRESENT

State of the art: What we know

Historical introduction

- Biham and Shamir 1990: Quartets, Octets, etc.
- . . . widespread informal use . . .
- Blondeau and Gérard, FSE 2011: Comprehensive framework for multiple differentials

What's left to do then?

- Model of FSE'11: Analysis requires fairly restrictive condition on differentials
  - Can this be avoided?
- Some small technical problems with the attack on 18-round PRESENT

State of the art: What we know

Historical introduction

- Biham and Shamir 1990: Quartets, Octets, etc.
- ... widespread informal use ...
- Blondeau and Gérard, FSE 2011: Comprehensive framework for multiple differentials

What's left to do then?

- Model of FSE'11: Analysis requires fairly restrictive condition on differentials
  - Can this be avoided?
- Some small technical problems with the attack on 18-round PRESENT

Structure attacks

Structure attacks

- Use multiple input, single output differences
- Proper subclass of multiple differential cryptanalysis
- Allow avoiding the condition of [Blondeau and Gérard, FSE'11]

Structures

- Consider set $\{\Delta_0^1, \ldots, \Delta_0^t\}$ of input differences
- Structure: collection of plaintexts of the form

$$\bigcup_x \{x \oplus \Delta \mid \Delta \in \mathrm{span}\{\Delta_0^1, \ldots, \Delta_0^t\}\}$$

Here: focus on SPNs

Structure attacks

Structure attacks

- Use multiple input, single output differences
- Proper subclass of multiple differential cryptanalysis
- Allow avoiding the condition of [Blondeau and Gérard, FSE'11]

Structures

- Consider set $\{\Delta_0^1, \ldots, \Delta_0^t\}$ of input differences
- Structure: collection of plaintexts of the form

$$\bigcup_x \{x \oplus \Delta \mid \Delta \in \mathsf{span}\{\Delta_0^1, \ldots, \Delta_0^t\}\}$$

Here: focus on SPNs

Structure attacks

Structure attacks

- Use multiple input, single output differences
- Proper subclass of multiple differential cryptanalysis
- Allow avoiding the condition of [Blondeau and Gérard, FSE'11]

Structures

- Consider set $\{\Delta_0^1, \ldots, \Delta_0^t\}$ of input differences
- Structure: collection of plaintexts of the form

$$\bigcup_x \{x \oplus \Delta \mid \Delta \in \mathrm{span}\{\Delta_0^1, \ldots, \Delta_0^t\}\}$$

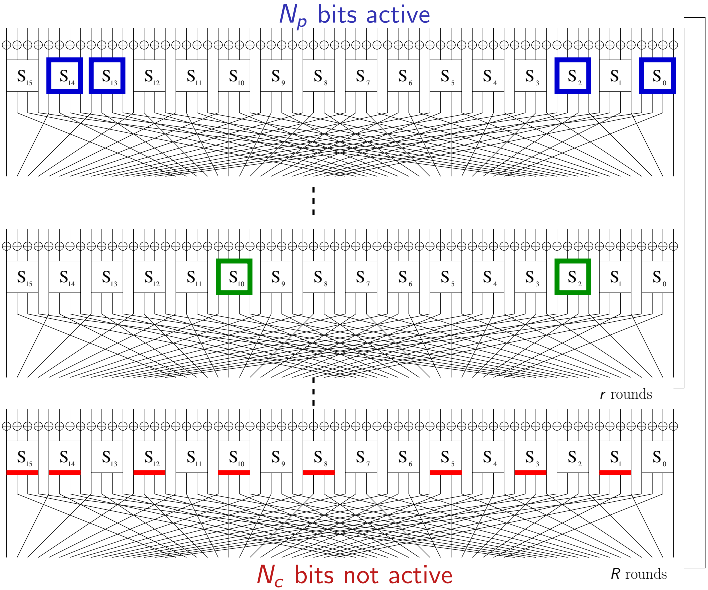
Here: focus on SPNs

Modeling structure attacks: The setting

Notation

- m-bit block cipher, k bit key
- Attack on R rounds with r-round differentials
- Set Δ_0 of input differences, one output difference Δ_r

Modeling structure attacks: The setting



Structure of the structures

In each structure:

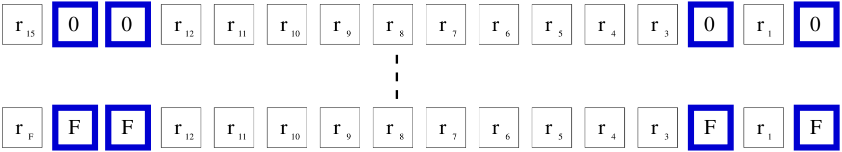
- $m - N_p$ bits fixed,
- N_p bits take on all N_p-bit values

Structure of the structures

In each structure:

- $m - N_p$ bits fixed,
- N_p bits take on all N_p-bit values

Structure 1:

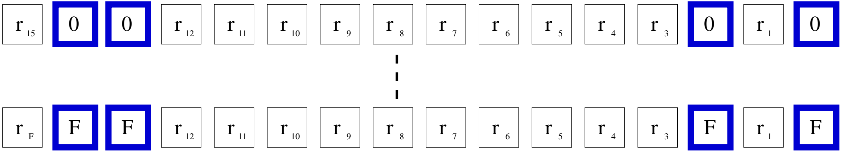


Structure of the structures

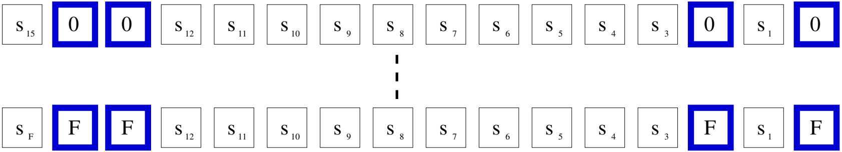
In each structure:

- $m - N_p$ bits fixed,
- N_p bits take on all N_p-bit values

Structure 1:

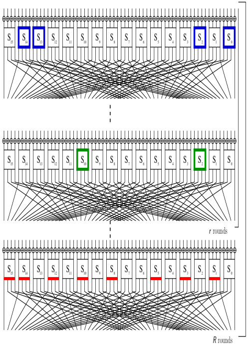


Structure 2:



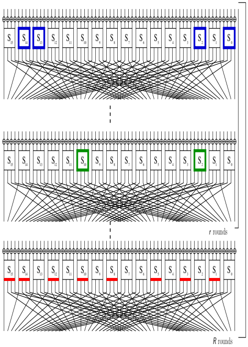
and so on

Anatomy of a structure attack



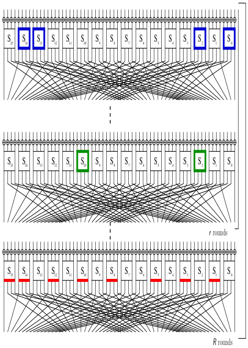
1. For each of the N_{st} structures:
   (a) Insert ciphertexts into hash table indexed by N_c
   (b) For each entry: Check if input difference matches Δ_0
   (c) If yes: For each pair, filter by output difference in active S-boxes in round R
   (d) If pair survives filter: Guess n_k subkey bits, decrypt to round r, maintain counters.
2. Search through the ℓ best key candidates, find master key.

Anatomy of a structure attack



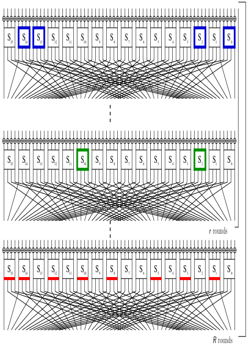
1. For each of the N_{st} structures:
   (a) Insert ciphertexts into hash table indexed by N_c
   (b) For each entry: Check if input difference matches Δ_0
   (c) If yes: For each pair, filter by output difference in active S-boxes in round R
   (d) If pair survives filter: Guess n_k subkey bits, decrypt to round r, maintain counters.
2. Search through the ℓ best key candidates, find master key.

Anatomy of a structure attack



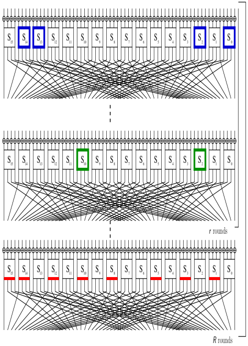
1. For each of the N_{st} structures:
   (a) Insert ciphertexts into hash table indexed by N_c
   (b) For each entry: Check if input difference matches Δ_0
   (c) If yes: For each pair, filter by output difference in active S-boxes in round R
   (d) If pair survives filter: Guess n_k subkey bits, decrypt to round r, maintain counters.
2. Search through the ℓ best key candidates, find master key.

Anatomy of a structure attack



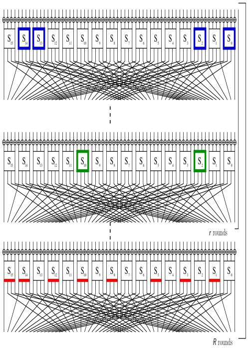
1. For each of the N_{st} structures:
   (a) Insert ciphertexts into hash table indexed by N_c
   (b) For each entry: Check if input difference matches Δ_0
   (c) If yes: For each pair, filter by output difference in active S-boxes in round R
   (d) If pair survives filter: Guess n_k subkey bits, decrypt to round r, maintain counters.
2. Search through the ℓ best key candidates, find master key.

Anatomy of a structure attack



1. For each of the N_{st} structures:
   (a) Insert ciphertexts into hash table indexed by N_c
   (b) For each entry: Check if input difference matches Δ_0
   (c) If yes: For each pair, filter by output difference in active S-boxes in round R
   (d) If pair survives filter: Guess n_k subkey bits, decrypt to round r, maintain counters.
2. Search through the ℓ best key candidates, find master key.

Anatomy of a structure attack



1. For each of the N_{st} structures:
   (a) Insert ciphertexts into hash table indexed by N_c
   (b) For each entry: Check if input difference matches Δ_0
   (c) If yes: For each pair, filter by output difference in active S-boxes in round R
   (d) If pair survives filter: Guess n_k subkey bits, decrypt to round r, maintain counters.
2. Search through the ℓ best key candidates, find master key.

The time complexity of a structure attack

1. For each of the N_{st} structures:
   (a) Insert ciphertexts into hash table indexed by N_c — $T_a = 2^{N_{st}+N_p}$
   (b) For each entry: Check if input difference matches Δ_0 — $T_b = 2^{N_{st}+2N_p-N_c}$
   (c) If yes: For each pair, filter by output difference in active S-boxes in round R — $T_c = |\Delta_0| \cdot 2^{N_{st}+N_p-N_c}$
   (d) If pair survives filter: Guess n_k subkey bits, decrypt to round r, maintain counters. — $T_d \approx |\Delta_0| \cdot 2^{N_{st}+N_p-N_c}$
2. Search through the ℓ best key candidates, find master key. — $T_2 = \ell \cdot 2^{k-n_k}$

The time complexity of a structure attack

1. For each of the N_{st} structures:
   (a) Insert ciphertexts into hash table indexed by N_c
   (b) For each entry: Check if input difference matches Δ_0
   (c) If yes: For each pair, filter by output difference in active S-boxes in round R
   (d) If pair survives filter: Guess n_k subkey bits, decrypt to round r, maintain counters.
2. Search through the ℓ best key candidates, find master key.

$T_a = 2^{N_{st}+N_p}$

$T_b = 2^{N_{st}+2N_p-N_c}$

$T_c = |\Delta_0| \cdot 2^{N_{st}+N_p-N_c}$

$T_d \approx |\Delta_0| \cdot 2^{N_{st}+N_p-N_c}$

$T_2 = \ell \cdot 2^{k-n_k}$

The time complexity of a structure attack

1. For each of the N_{st} structures:
   (a) Insert ciphertexts into hash table indexed by N_c — $T_a = 2^{N_{st}+N_p}$
   (b) For each entry: Check if input difference matches Δ_0 — $T_b = 2^{N_{st}+2N_p-N_c}$
   (c) If yes: For each pair, filter by output difference in active S-boxes in round R — $T_c = |\Delta_0| \cdot 2^{N_{st}+N_p-N_c}$
   (d) If pair survives filter: Guess n_k subkey bits, decrypt to round r, maintain counters. — $T_d \approx |\Delta_0| \cdot 2^{N_{st}+N_p-N_c}$
2. Search through the ℓ best key candidates, find master key. — $T_2 = \ell \cdot 2^{k-n_k}$

The time complexity of a structure attack

1. For each of the N_{st} structures:
   (a) Insert ciphertexts into hash table indexed by N_c
   (b) For each entry: Check if input difference matches Δ_0
   (c) If yes: For each pair, filter by output difference in active S-boxes in round R
   (d) If pair survives filter: Guess n_k subkey bits, decrypt to round r, maintain counters.
2. Search through the ℓ best key candidates, find master key.

$T_a = 2^{N_{st}+N_p}$

$T_b = 2^{N_{st}+2N_p-N_c}$

$T_c = |\Delta_0| \cdot 2^{N_{st}+N_p-N_c}$

$T_d \approx |\Delta_0| \cdot 2^{N_{st}+N_p-N_c}$

$T_2 = \ell \cdot 2^{k-n_k}$

The time complexity of a structure attack

1. For each of the N_{st} structures:
   (a) Insert ciphertexts into hash table indexed by N_c — $T_a = 2^{N_{st}+N_p}$
   (b) For each entry: Check if input difference matches Δ_0 — $T_b = 2^{N_{st}+2N_p-N_c}$
   (c) If yes: For each pair, filter by output difference in active S-boxes in round R — $T_c = |\Delta_0| \cdot 2^{N_{st}+N_p-N_c}$
   (d) If pair survives filter: Guess n_k subkey bits, decrypt to round r, maintain counters. — $T_d \approx |\Delta_0| \cdot 2^{N_{st}+N_p-N_c}$
2. Search through the ℓ best key candidates, find master key. — $T_2 = \ell \cdot 2^{k-n_k}$

Using the model as guidance

Dominating term depends on relation between N_p and N_c:

$$T_a + T_b + T_c + T_d + T_2 \simeq \begin{cases} T_a + T_2 & \text{if } N_p < N_c, \\ T_b + T_2 & \text{if } N_p > N_c, \\ 2T_a + T_2 & \text{if } N_p = N_c. \end{cases}$$

$$T_a = 2^{N_{st}+N_p},\ T_b = 2^{N_{st}+2N_p-N_c},\ T_2 = \ell \cdot 2^{k-n_k}$$

Implications

- If many differentials have probability close to 2^{-m} (requires large ℓ and hence T_2): Increase N_p, use more differentials
- If probabilites $\gg 2^{-m}$ (hence small ℓ and T_2): Take $N_p = N_c$

Success probability: use model of FSE'11 without restrictive condition.

Using the model as guidance

Dominating term depends on relation between N_p and N_c:

$$T_a + T_b + T_c + T_d + T_2 \simeq \begin{cases} T_a + T_2 & \text{if } N_p < N_c, \\ T_b + T_2 & \text{if } N_p > N_c, \\ 2T_a + T_2 & \text{if } N_p = N_c. \end{cases}$$

$$T_a = 2^{N_{st}+N_p},\ T_b = 2^{N_{st}+2N_p-N_c},\ T_2 = \ell \cdot 2^{k-n_k}$$

Implications

- If many differentials have probability close to 2^{-m} (requires large ℓ and hence T_2): Increase N_p, use more differentials
- If probabilites $\gg 2^{-m}$ (hence small ℓ and T_2): Take $N_p = N_c$

Success probability: use model of FSE'11 without restrictive condition.

Using the model as guidance

Dominating term depends on relation between N_p and N_c:

$$T_a + T_b + T_c + T_d + T_2 \simeq \begin{cases} T_a + T_2 & \text{if } N_p < N_c, \\ T_b + T_2 & \text{if } N_p > N_c, \\ 2T_a + T_2 & \text{if } N_p = N_c. \end{cases}$$

$$T_a = 2^{N_{st}+N_p},\ T_b = 2^{N_{st}+2N_p-N_c},\ T_2 = \ell \cdot 2^{k-n_k}$$

Implications

- If many differentials have probability close to 2^{-m} (requires large ℓ and hence T_2): Increase N_p, use more differentials
- If probabilites $\ggg 2^{-m}$ (hence small ℓ and T_2): Take $N_p = N_c$

Success probability: use model of FSE'11 without restrictive condition.

Using the model as guidance

Dominating term depends on relation between N_p and N_c:

$$T_a + T_b + T_c + T_d + T_2 \simeq \begin{cases} T_a + T_2 & \text{if } N_p < N_c, \\ T_b + T_2 & \text{if } N_p > N_c, \\ 2T_a + T_2 & \text{if } N_p = N_c. \end{cases}$$

$$T_a = 2^{N_{st}+N_p},\ T_b = 2^{N_{st}+2N_p-N_c},\ T_2 = \ell \cdot 2^{k-n_k}$$

Implications

- If many differentials have probability close to 2^{-m} (requires large ℓ and hence T_2): Increase N_p, use more differentials
- If probabilites $\ggg 2^{-m}$ (hence small ℓ and T_2): Take $N_p = N_c$

Success probability: use model of FSE'11 without restrictive condition.

Using the model as guidance

Dominating term depends on relation between N_p and N_c:

$$T_a + T_b + T_c + T_d + T_2 \simeq \begin{cases} T_a + T_2 & \text{if } N_p < N_c, \\ T_b + T_2 & \text{if } N_p > N_c, \\ 2T_a + T_2 & \text{if } N_p = N_c. \end{cases}$$

$$T_a = 2^{N_{st}+N_p},\ T_b = 2^{N_{st}+2N_p-N_c},\ T_2 = \ell \cdot 2^{k-n_k}$$

Implications

- If many differentials have probability close to 2^{-m} (requires large ℓ and hence T_2): Increase N_p, use more differentials
- If probabilites $\ggg 2^{-m}$ (hence small ℓ and T_2): Take $N_p = N_c$

Success probability: use model of FSE'11 without restrictive condition.

On the ratio of weak keys for structure attacks

Differential probabilities vary over the keys: Implications?

Daemen and Rijmen 2006: Fixed-key cardinality of a (single) differential follows a Poisson distribution.

$\Rightarrow$ Theorem: Characterisation of the weak key ratio

Consider differentials $\Delta_0^i \rightarrow \Delta_r$ with probability p_i, $1 \leq i \leq |\Delta_0|$. Then only a ratio of

$$r_w \stackrel{\text{def}}{=} 1 - \sum_{x=0}^{\mu-1} \text{Poisson}(x, 2^{m-1} \sum_{j=1}^{|\Delta_0|} p_i)$$

"weak" keys produces μ right pairs or more.

On the ratio of weak keys for structure attacks

Differential probabilities vary over the keys: Implications?

Daemen and Rijmen 2006: Fixed-key cardinality of a (single) differential follows a Poisson distribution.

$\Rightarrow$ Theorem: Characterisation of the weak key ratio

Consider differentials $\Delta_0^i \rightarrow \Delta_r$ with probability p_i, $1 \leq i \leq |\Delta_0|$. Then only a ratio of

$$r_w \stackrel{\text{def}}{=} 1 - \sum_{x=0}^{\mu-1} \text{Poisson}(x, 2^{m-1} \sum_{j=1}^{|\Delta_0|} p_i)$$

"weak" keys produces μ right pairs or more.

On the ratio of weak keys for structure attacks

Differential probabilities vary over the keys: Implications?

Daemen and Rijmen 2006: Fixed-key cardinality of a (single) differential follows a Poisson distribution.

$\Rightarrow$ Theorem: Characterisation of the weak key ratio

Consider differentials $\Delta_0^i \to \Delta_r$ with probability p_i, $1 \leq i \leq |\Delta_0|$. Then only a ratio of

$$r_w \stackrel{\text{def}}{=} 1 - \sum_{x=0}^{\mu-1} \text{Poisson}(x, 2^{m-1} \sum_{j=1}^{|\Delta_0|} p_i)$$

"weak" keys produces μ right pairs or more.

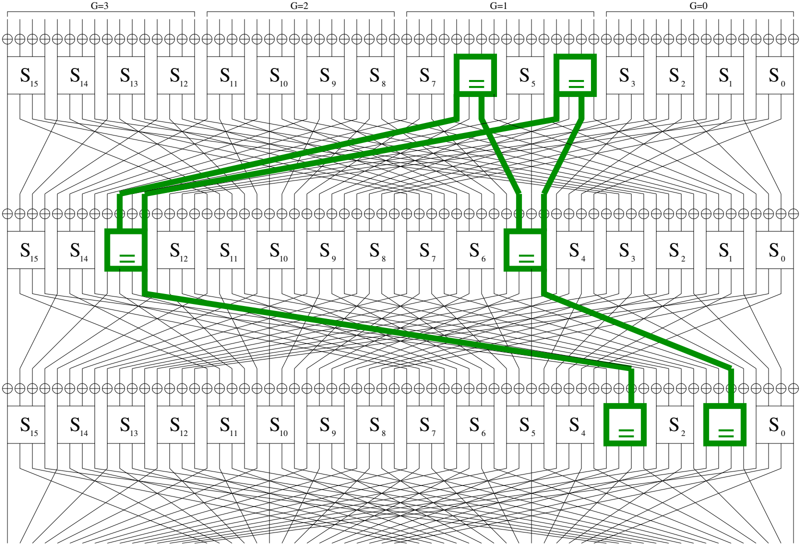
Applying the structure attack

PRESENT

- 64-bit SPN block cipher with 80-bit key
- By Bogdanov et al (CHES 2007), now ISO standard
- Best attack: [Cho 2010], Multidimensional linear, 26 rounds
- Best differential attack: [Blondeau and Gérard 2011], multiple differential, 18 rounds (+ minor corrections)

Attacking PRESENT: Differential pattern propagation

Focus on trails with two active S-boxes per round



Applying the structure attack to 18-round PRESENT

Parameters

- $|\Delta_0| = 36$ 16-round differentials
- 2^{24} structures, $N_p = 40$, $N_c = 32$
- key candidate list size $\ell = 2^{36}$

Complexities

- Time 2^{76}, data 2^{64}
- Success probability 86%
- Weak key ratio 57%

Applying the structure attack to 18-round PRESENT

Parameters

- $|\Delta_0| = 36$ 16-round differentials
- 2^{24} structures, $N_p = 40$, $N_c = 32$
- key candidate list size $\ell = 2^{36}$

Complexities

- Time 2^{76}, data 2^{64}
- Success probability 86%
- Weak key ratio 57%

Comparison to multiple differential attacks on PRESENT

Best previous differential attack: 18 rounds, revised multiple differential attack of Blondeau and Gérard, eprint 2011/115

Multiple differential		Structure attack			
ℓ	P_S	ℓ	P_S	data	time
2^{38}	65.27%	2^{36}	85.94%	2^{64}	2^{76}
2^{39}	79.68%	2^{37}	92.30%	2^{64}	2^{77}
2^{41}	94.62%	2^{39}	98.36%	2^{64}	2^{79}

Second example: Serpent

Serpent

- 128-bit block cipher, 128 to 256-bit key
- By Anderson et al (1998), AES finalist
- Best attack: Differential-linear attack on 12 rounds, Dunkelman et al 2008

Differential attacks

	Biham et al (2001)		Structure attack	
rounds	time	data	time	data
7	2^{85}	2^{84}	2^{75}	2^{71}
8	2^{213}	2^{84}	2^{203}	2^{71}

Second example: Serpent

Serpent

- 128-bit block cipher, 128 to 256-bit key
- By Anderson et al (1998), AES finalist
- Best attack: Differential-linear attack on 12 rounds, Dunkelman et al 2008

Differential attacks

	Biham et al (2001)		Structure attack	
rounds	time	data	time	data
7	2^{85}	2^{84}	2^{75}	2^{71}
8	2^{213}	2^{84}	2^{203}	2^{71}

Conclusions and outlook

Summary

- We propose a complete model for the analysis of structure attacks
- This leads to an explicit characterisation of the ratio of weak keys
- Structure attacks provide the currently best differential attacks on PRESENT and Serpent.

Future work

- More study is needed on the necessity of the restrictive condition in the model of FSE'11
- Applying structure attacks to other ciphers

Conclusions and outlook

Summary

- We propose a complete model for the analysis of structure attacks
- This leads to an explicit characterisation of the ratio of weak keys
- Structure attacks provide the currently best differential attacks on PRESENT and Serpent.

Future work

- More study is needed on the necessity of the restrictive condition in the model of FSE'11
- Applying structure attacks to other ciphers

The End

Thank you for your attention!