Truncated Differentials

Lars R. Knudsen

DTU Mathematics

Spring 2011

Outline

1. Differential cryptanalysis
2. CipherFOUR
3. Truncated differentials
4. Impossible differentials

Outline

1. Differential cryptanalysis
2. CipherFOUR
3. Truncated differentials
4. Impossible differentials

Differential cryptanalysis: the idea

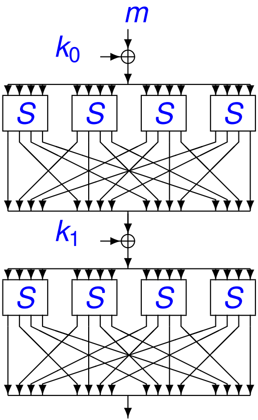
Differential cryptanalysis on iterated ciphers

- trace difference in chosen plaintexts through encryption process;
- predict difference in next to last round of encryption;
- guess key in last round, compute backwards.

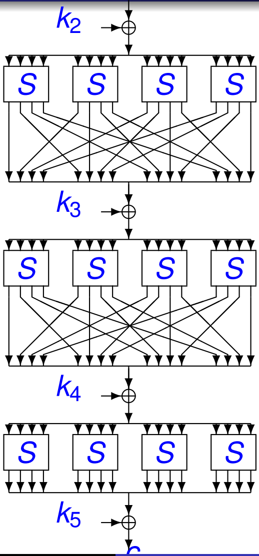
Outline

1. Differential cryptanalysis
2. CipherFOUR
3. Truncated differentials
4. Impossible differentials

CIPHERFOUR



5 rounds of CIPHERFOUR



Characteristic

Consider

$$(0,0,2,0) \overset{(S,S,S,S)}{\longrightarrow} (0,0,2,0)$$

which has probability 6/16 and note that

$$(0,0,2,0) \xrightarrow{P} (0,0,2,0)$$

Thus

$$(0,0,2,0) \xrightarrow{\mathcal{R}} (0,0,2,0)$$

Characteristic

$$(0, 0, 2, 0) \overset{\mathcal{R}}{\to} (0, 0, 2, 0) \overset{\mathcal{R}}{\to} (0, 0, 2, 0)$$

with probability

$$(6/16)^2$$

and

$$(0, 0, 2, 0) \overset{\mathcal{R}}{\to} (0, 0, 2, 0) \overset{\mathcal{R}}{\to} (0, 0, 2, 0) \overset{\mathcal{R}}{\to} (0, 0, 2, 0) \overset{\mathcal{R}}{\to} (0, 0, 2, 0)$$

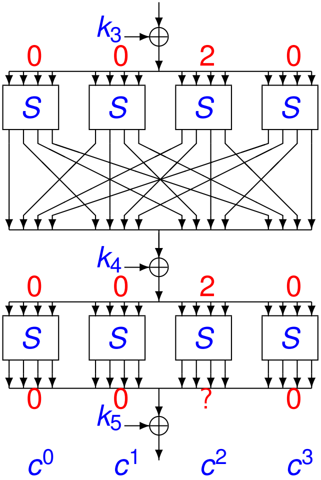
with probability

$$(6/16)^4 \approx 0.02.$$

Example

Attack 5 rounds by guessing (parts of) the last round key.

Differential Attack of CIPHERFOUR



Differentials

Observation

When using

$$(0,0,2,0) \xrightarrow{\mathcal{R}} (0,0,2,0) \xrightarrow{\mathcal{R}} (0,0,2,0) \xrightarrow{\mathcal{R}} (0,0,2,0) \xrightarrow{\mathcal{R}} (0,0,2,0)$$

we do not care about the intermediate differences!

What we are really interested in is

$$(0,0,2,0) \xrightarrow{\mathcal{R}} ? \xrightarrow{\mathcal{R}} ? \xrightarrow{\mathcal{R}} ? \xrightarrow{\mathcal{R}} (0,0,2,0)$$

or

$$(0,0,2,0) \xrightarrow{4\,\mathcal{R}} (0,0,2,0).$$

Differentials

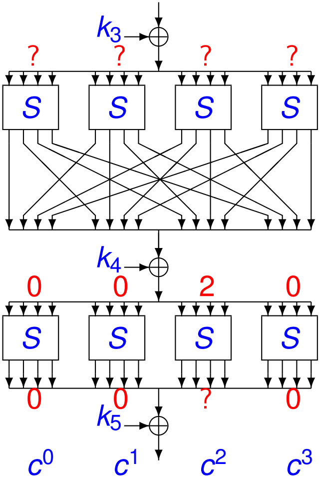
$$(0,0,2,0) \overset{4\mathcal{R}}{\to} (0,0,2,0).$$

There are at least four characteristics involved

$$\begin{aligned}
&(0,0,2,0) \xrightarrow{\mathcal{R}} (0,0,2,0) \xrightarrow{\mathcal{R}} (0,0,2,0) \xrightarrow{\mathcal{R}} (0,0,2,0) \xrightarrow{\mathcal{R}} (0,0,2,0),\\
&(0,0,2,0) \xrightarrow{\mathcal{R}} (0,0,0,2) \xrightarrow{\mathcal{R}} (0,0,0,1) \xrightarrow{\mathcal{R}} (0,0,1,0) \xrightarrow{\mathcal{R}} (0,0,2,0),\\
&(0,0,2,0) \xrightarrow{\mathcal{R}} (0,0,0,2) \xrightarrow{\mathcal{R}} (0,0,1,0) \xrightarrow{\mathcal{R}} (0,0,2,0) \xrightarrow{\mathcal{R}} (0,0,2,0),\\
&(0,0,2,0) \xrightarrow{\mathcal{R}} (0,0,2,0) \xrightarrow{\mathcal{R}} (0,0,0,2) \xrightarrow{\mathcal{R}} (0,0,1,0) \xrightarrow{\mathcal{R}} (0,0,2,0).
\end{aligned}$$

$$P((0,0,2,0) \overset{4\mathcal{R}}{\to} (0,0,2,0)) \approx 0.081 > 0.02.$$

Differential Attack of CIPHERFOUR



CIPHERFOUR: Experimental Results

Differential attack on 5 rounds

Attacker tries to determine four bits of the key

Experiment

Number of texts	Differential attack
32	64%
64	76%
128	85%
256	96%

Outline

1. Differential cryptanalysis
2. CipherFOUR
3. Truncated differentials
4. Impossible differentials

Truncated differentials

Definition

A (differential) characteristic predicts the difference in a pair of texts after each round of encryption.

Definition

A differential is a collection of characteristics.

Truncated differentials

Definition

A truncated characteristic predicts only part of the difference in a pair of texts after each round of encryption.

Definition

A truncated differential is a collection of truncated characteristics.

Truncated differentials

S-box from before

Bit notation:

- $0010 \xrightarrow{S} 0010$ has probability $\frac{6}{16}$.
- $0010 \xrightarrow{S} \star 0 \star \star$ has probability 1.

Distribution table

in \out	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	16	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
1	-	-	6	-	-	-	-	2	-	2	-	-	2	-	4	-
2	-	6	6	-	-	-	-	-	-	2	2	-	-	-	-	-
3	-	-	-	6	-	2	-	-	2	-	-	-	4	-	2	-
4	-	-	-	2	-	2	4	-	-	2	2	2	-	-	2	-
5	-	2	2	-	4	-	-	4	2	-	-	2	-	-	-	-
6	-	-	2	-	4	-	-	2	2	-	2	2	2	-	-	-
7	-	-	-	-	-	4	4	-	2	2	2	2	-	-	-	-
8	-	-	-	-	-	2	-	2	4	-	-	4	-	2	-	2
9	-	2	-	-	-	2	2	2	-	4	2	-	-	-	-	2
a	-	-	-	-	2	2	-	-	-	4	4	-	2	2	-	-
b	-	-	-	2	2	-	2	2	2	-	-	4	-	-	2	-
c	-	4	-	2	-	2	-	-	2	-	-	-	-	-	6	-
d	-	-	-	-	-	-	2	2	-	-	-	-	6	2	-	4
e	-	2	-	4	2	-	-	-	-	-	2	-	-	-	-	6
f	-	-	-	-	2	-	2	-	-	-	-	-	-	10	-	2

Truncated differentials

Input difference 2 to S-box lead only to output differences $1, 2, 9,$ and a. So for one round

$$(0000\,0000\,0010\,0000) \xrightarrow{\mathcal{R}} \begin{cases} (0000\,0000\,0010\,0000) \text{ or} \\ (0000\,0000\,0000\,0010) \text{ or} \\ (0010\,0000\,0010\,0000) \text{ or} \\ (0010\,0000\,0000\,0010) \end{cases}$$

Truncated differentials

$$\begin{array}{l}
(0000 \quad 0000 \quad 0010 \quad 0000) \xrightarrow{\mathcal{R}} (00\star0 \quad 0000 \quad 00\star0 \quad 00\star0) \\
(0000 \quad 0000 \quad 0000 \quad 0010) \xrightarrow{\mathcal{R}} (000\star \quad 0000 \quad 000\star \quad 000\star) \\
(0010 \quad 0000 \quad 0010 \quad 0000) \xrightarrow{\mathcal{R}} (\star0\star0 \quad 0000 \quad \star0\star0 \quad \star0\star0) \\
(0010 \quad 0000 \quad 0000 \quad 0010) \xrightarrow{\mathcal{R}} (\star00\star \quad 0000 \quad \star00\star \quad \star00\star)
\end{array}$$

$$\left.\begin{array}{l}
(0000 \quad 0000 \quad 0010 \quad 0000) \\
(0000 \quad 0000 \quad 0000 \quad 0010) \\
(0010 \quad 0000 \quad 0010 \quad 0000) \\
(0010 \quad 0000 \quad 0000 \quad 0010)
\end{array}\right\} \xrightarrow{\mathcal{R}} (\star0\star\star \quad 0000 \quad \star0\star\star \quad \star0\star\star)$$

Truncated differentials

- Leads to a 2-round truncated differential

$$(0000\,0000\,0010\,0000) \xrightarrow{\mathcal{R}} (\star 0 \star\star\ 0000\ \star 0 \star\star\ \star 0 \star\star)$$

- Adding another round gives

$$(\star 0 \star\star\ 0000\ \star 0 \star\star\ \star 0 \star\star) \xrightarrow{\mathcal{R}} (\star 0 \star\star\ \star\ 0 \star\star\ \star\ 0 \star\star\ \star\ 0 \star\star).$$

Truncated differentials

This leads to a 3-round truncated differential

- $(0000\,0000\,0010\,0000) \xrightarrow{3\mathcal{R}} (\star 0 \star\star \ \star\ 0 \star\star \ \star\ 0 \star\star \ \star\ 0 \star\star)$

of probability 1!

Can we extend this further?

Truncated differentials

- Consider the 1-round characteristic
  $(0000\ 0000\ 0010\ 0000) \xrightarrow{\mathcal{R}} (0000\ 0000\ 0010\ 0000)$.
- A pair will follow this characteristic if $2 \xrightarrow{\mathcal{S}} 2$
- Choose 16 texts

  $$(t_0,\ t_1,\ i,\ t_2),$$

  where $i = 0, \ldots, 15$ and t_0, t_1, t_2 are arbitrary and fixed.
- Any two (different) texts lead to a pair of difference

  $$\begin{array}{llll} (t_0 \oplus t_0 & t_1 \oplus t_1 & i \oplus j & t_2 \oplus t_2) = \\ (0000 & 0000 & \star\star\star\star & 0000). \end{array}$$

Truncated differentials

- How many pairs lead to difference (0000 0000 0010 0000) after the first S-box?
- Exactly eight (distinct pairs)!
- For these eight pairs one gets
  $(0000\ 0000\ \star\star\star\star\ 0000) \xrightarrow{\mathcal{R}} (0000\ 0000\ 0010\ 0000)$.
- With correct guess of four-bit key one can easily identify these eight.

Truncated differentials

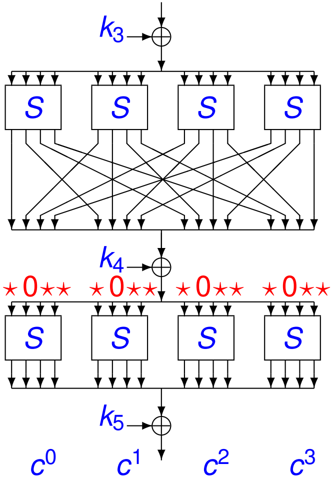
Summing up: yields a 4-round truncated differential

- $(0000\,0000\ \star\star\star\star\,0000) \xrightarrow{4\mathcal{R}} (\star\,0\star\star\ \star\ 0\star\star\ \star\ 0\star\star\ \star\ 0\star\star)$

which for correct guess of 4-bit key in 1st round, gives 8 right pairs from pool of 16 texts.

5-round attack: run attack for all values of 4 bits of k_0 and 4 times 4 bits of k_5.

Differential Attack of CIPHERFOUR



Truncated differentials

5-round attack on CIPHERFOUR

Experiment

Number of texts	Differentials		Truncated differentials	
16	.		28%	(4+4)
32	.		78%	(4+9)
48	.		97%	(4+12)
64	76%	(4)		
128	85%	(4)		
256	96%	(4)		

Numbers in brackets denote the number of key bits identified

Outline

1. Differential cryptanalysis
2. CipherFOUR
3. Truncated differentials
4. Impossible differentials

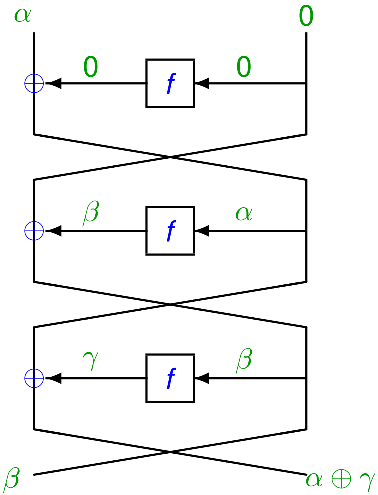
Impossible differentials

- Traditionally in differential attack, aim is to find differential of high probability
- A differential of low probability can be equally useful
- S/N should be different from one:
  - S/N $>$ 1, right value of key suggested the **most**
  - S/N $<$ 1, right value of key suggested the **least**

Truncated differentials - Feistel network

- Consider Feistel network where round function is a bijection for any fixed key
- Consider a differential $(\alpha, 0)$ such that the difference in the left halves of the plaintexts is α and where the right halves are equal
- It follows that after 5 rounds of encryption, the difference in the ciphertexts will never be $(0, \alpha)$
- Can be used in attacks on such ciphers with more than 5 rounds by guessing keys and computing backwards
- For the correct key guesses the computed difference will never be $(0, \alpha)$

Truncated differentials - Feistel network

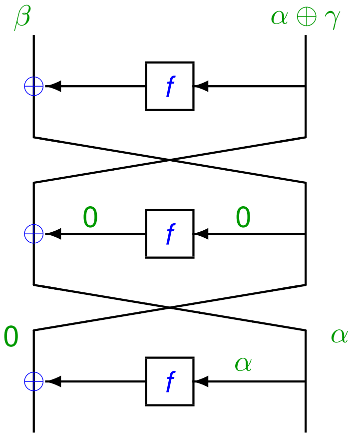


$\alpha \neq 0$

$\beta \neq 0$

$\gamma \neq 0$

Truncated differentials - Feistel network



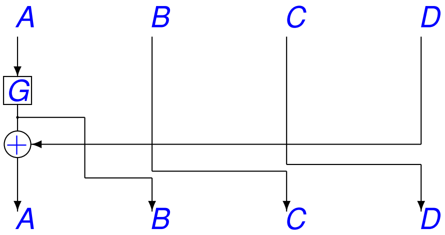
Skipjack (Biham, Biryukov, Shamir)

- Skipjack - a 32-round iterated block cipher by NSA
- there exists truncated differentials of Skipjack
    - for 12 encryption rounds of probability one $(0, a, 0, 0) \xrightarrow{12r} (b, c, d, 0)$
    - for 12 decryption rounds of probability one $$(f, g, 0, h) \xleftarrow{12r} (e, 0, 0, 0)$$
    - for 24 rounds of probability zero $(0, a, 0, 0) \xrightarrow{24r} (e, 0, 0, 0)$
- these can be used to break Skipjack with 31 rounds faster than by an exhaustive key search

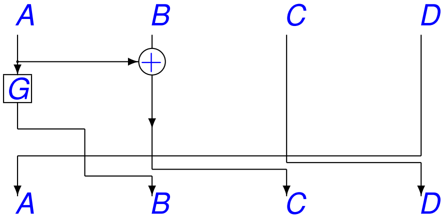
Skipjack (continued)

- Skipjack is an iterated 64-bit block cipher using an 80-bit key and running in 32 rounds, see Figure next page. Encryption of a 64-bit plaintext consists of first applying eight A-rounds, then eight B-rounds, once again eight A-rounds and finally eight B-rounds. A round counter is added to one of the 16-bit words in each round. The key schedule is simple but this and the round counter is not important for the illustration here.
- There is a twelve-round truncated differential of probability one through 4 A-rounds and 8 B-rounds.
- There is a twelve-round truncated differential of probability one through 4 inverse B-rounds and 8 inverse A-rounds.

Skipjack graph (G takes 16-bit round key)



Skipjack A-round



Skipjack B-round

Higher Order Differentials

Lars R. Knudsen

DTU Mathematics

Spring 2011

Outline

1. Higher order differentials
    - Algebraic degree
    - Algebraic degree and higher order differentials
    - Boomerang attack

Higher order differentials (Lai)

1st-order differential

the conventional differential where

$$f(x) \oplus f(x \oplus \alpha)$$

where $\alpha \neq 0$ is well-chosen value.

2nd-order differential

involves tuple of 4 texts and difference

$$f(x) \oplus f(x \oplus \alpha) \oplus f(x \oplus \beta) \oplus f(x \oplus \alpha \oplus \beta)$$

where α, β are distinct, non-zero values.

Higher order differentials

Consider difference $\alpha \neq 0$ through f.

Definition

The (first-order) derivative of f at point α:

$$\Delta_\alpha f(x) = f(x \oplus \alpha) \oplus f(x).$$

Definition

dth order derivative of f at point $\alpha_1, \ldots, \alpha_d$ is defined

$$\Delta_{\alpha_1,\ldots,\alpha_d} f(x) = \Delta_{\alpha_d}(\Delta_{\alpha_1,\ldots,\alpha_{d-1}} f(x)).$$

Higher order differentials

- Consider functions over $GF(2)$.
- A dth order derivative involves 2^d function values of f.
- The points $(\alpha_1, \ldots, \alpha_d)$ must be linearly independent when viewed as bit-vectors.
- The arguments to f form a dth dimensional subspace.

Algebraic degree

Let $f : \{0,1\}^3 \rightarrow \{0,1\}$ be a Boolean function, s.t.,

$$f(x) = f(x_2, x_1, x_0) = x_2 x_1 x_0 + x_0 + 1.$$

The algebraic degree of f is three.

Let $g : \{0,1\}^3 \rightarrow \{0,1\}$ be a Boolean function, s.t.,

$$g(x_2, x_1, x_0) = x_2 x_1 + x_0 x_2 + x_2 + x_1 + 1.$$

The algebraic degree of g is two.

Algebraic degree and higher order differentials

Let $f : \{0,1\}^3 \rightarrow \{0,1\}$ be function, s.t.,

$$f(x_2, x_1, x_0) = x_2 x_1 x_0 + x_0 + 1.$$

Algebraic degree of f is three.

Consider the first order derivative at the point $\mathbb{1} = (0,0,1)$

$$\Delta_{\mathbb{1}} f(x) = x_2 x_1 + 1.$$

The algebraic degree of $\Delta_{\mathbb{1}} f(x)$ is two.

Algebraic degree and higher order differentials

Consider the second order derivative of f

$$\Delta_{1,2} f(x) = x_2.$$

The algebraic degree of $\Delta_{1,2} f(x)$ is one.

Consider the third order derivative of f

$$\Delta_{1,2,4} f(x) = 1.$$

The algebraic degree of $\Delta_{1,2,4} f(x)$ is zero.

Algebraic degree and higher order differentials

Fact

Let f be a Boolean function of algebraic degree d.
The algebraic degree of a dth order derivative of f is zero.

Extension

Let $h : \{0, 1\}^n \rightarrow \{0, 1\}^m$ be function. h can be described as concatenation of m Boolean functions $h_i : \{0, 1\}^n \rightarrow \{0, 1\}$. The h_is are called coordinate functions of h.

Definition

Let $h : \{0, 1\}^n \rightarrow \{0, 1\}^m$ be function. The algebraic degree of h is maximum algebraic degree of the coordination functions h_i.

Algebraic degree and higher order differentials

Definition

Let $h : \{0,1\}^n \rightarrow \{0,1\}^m$ be function. The algebraic degree of h is maximum algebraic degree of the coordination functions h_i.

Fact

Let h be a function of algebraic degree d.
The algebraic degree of a dth order derivative of h is zero.

Fact

Let h be a function of algebraic degree d.
The value of a $(d+1)$st order derivative of h is zero.

Higher order differential attack

- Consider the iterated cipher

$$\begin{tikzcd}
 & k_0 \arrow[d] & k_1 \arrow[d] & k_2 \arrow[d] & k_3 \arrow[d] & & k_4 \arrow[d] & \\
m \arrow[r] & \boxed{g} \arrow[r] & \boxed{g} \arrow[r] & \boxed{g} \arrow[r] & \boxed{g} \arrow[r] & x \arrow[r] & \boxed{g} \arrow[r] & c
\end{tikzcd}$$

- Assume algebraic degree of g is two.
- Algebraic degree of x (as a function of m) is a most 16.
- Specify 17th order differential.
- Guess k_4, compute backwards, check if value is zero.

Boomerang attack - 2nd order differential (Wagner)

- assume encryption process $\textsc{Enc}_k(m)$ can be written

$$\begin{tikzcd}
& k_1 \arrow[d] & & k_A \arrow[d] & & k_2 \arrow[d] & \\
m \arrow[r] & \boxed{E_1} \arrow[r] & x \arrow[r] & \boxed{A_k} \arrow[r] & y \arrow[r] & \boxed{E_2} \arrow[r] & c
\end{tikzcd}$$

  where A_k is key-dependent affine transformation

- suppose there exist differentials of probs p_1 and p_2

  $\alpha \xrightarrow{\textsc{Enc}^1} \beta$ and $\beta \xrightarrow{\textsc{Dec}^1} \alpha$

- suppose there is differential of prob q: $\gamma \xrightarrow{\textsc{Dec}^2} \phi$

- combine to boomerang of probability $p_1 p_2 q^2$

Boomerang attack - a 2nd order differential

- $m \longrightarrow \boxed{E_1} \longrightarrow x_1 \longrightarrow \boxed{A_k} \longrightarrow y_1 \longrightarrow \boxed{E_2} \longrightarrow c$

Boomerang attack - a 2nd order differential

- $m \longrightarrow \boxed{E_1} \longrightarrow x_1 \longrightarrow \boxed{A_k} \longrightarrow y_1 \longrightarrow \boxed{E_2} \longrightarrow c$
- $m \oplus \alpha \longrightarrow \boxed{E_1} \longrightarrow x_2 \longrightarrow \boxed{A_k} \longrightarrow y_2 \longrightarrow \boxed{E_2} \longrightarrow c_2$

Boomerang attack - a 2nd order differential

- $m \longrightarrow \boxed{E_1} \longrightarrow x_1 \longrightarrow \boxed{A_k} \longrightarrow y_1 \longrightarrow \boxed{E_2} \longrightarrow c$
- $m_3 \longleftarrow \boxed{E_1} \longleftarrow x_3 \longleftarrow \boxed{A_k} \longleftarrow y_3 \longleftarrow \boxed{E_2} \longleftarrow c \oplus \gamma$
- $m \oplus \alpha \longrightarrow \boxed{E_1} \longrightarrow x_2 \longrightarrow \boxed{A_k} \longrightarrow y_2 \longrightarrow \boxed{E_2} \longrightarrow c_2$

Boomerang attack - a 2nd order differential

- $m \longrightarrow \boxed{E_1} \longrightarrow x_1 \longrightarrow \boxed{A_k} \longrightarrow y_1 \longrightarrow \boxed{E_2} \longrightarrow c$
- $m_3 \longleftarrow \boxed{E_1} \longleftarrow x_3 \longleftarrow \boxed{A_k} \longleftarrow y_3 \longleftarrow \boxed{E_2} \longleftarrow c \oplus \gamma$
- $m \oplus \alpha \longrightarrow \boxed{E_1} \longrightarrow x_2 \longrightarrow \boxed{A_k} \longrightarrow y_2 \longrightarrow \boxed{E_2} \longrightarrow c_2$
- $m_4 \longleftarrow \boxed{E_1} \longleftarrow x_4 \longleftarrow \boxed{A_k} \longleftarrow y_4 \longleftarrow \boxed{E_2} \longleftarrow c_2 \oplus \gamma$

Boomerang attack - a 2nd order differential

- $m \longrightarrow \boxed{E_1} \longrightarrow x_1 \longrightarrow \boxed{A_k} \longrightarrow y_1 \longrightarrow \boxed{E_2} \longrightarrow c$
- $m_3 \longleftarrow \boxed{E_1} \longleftarrow x_3 \longleftarrow \boxed{A_k} \longleftarrow y_3 \longleftarrow \boxed{E_2} \longleftarrow c \oplus \gamma$
- $m \oplus \alpha \longrightarrow \boxed{E_1} \longrightarrow x_2 \longrightarrow \boxed{A_k} \longrightarrow y_2 \longrightarrow \boxed{E_2} \longrightarrow c_2$
- $m_4 \longleftarrow \boxed{E_1} \longleftarrow x_4 \longleftarrow \boxed{A_k} \longleftarrow y_4 \longleftarrow \boxed{E_2} \longleftarrow c_2 \oplus \gamma$
- if $\sum y_i = 0$ then $\sum x_i = 0$

Boomerang attack - a 2nd order differential

- $m \longrightarrow \boxed{E_1} \longrightarrow x_1 \longrightarrow \boxed{A_k} \longrightarrow y_1 \longrightarrow \boxed{E_2} \longrightarrow c$
- $m_3 \longleftarrow \boxed{E_1} \longleftarrow x_3 \longleftarrow \boxed{A_k} \longleftarrow y_3 \longleftarrow \boxed{E_2} \longleftarrow c \oplus \gamma$
- $m \oplus \alpha \longrightarrow \boxed{E_1} \longrightarrow x_2 \longrightarrow \boxed{A_k} \longrightarrow y_2 \longrightarrow \boxed{E_2} \longrightarrow c_2$
- $m_4 \longleftarrow \boxed{E_1} \longleftarrow x_4 \longleftarrow \boxed{A_k} \longleftarrow y_4 \longleftarrow \boxed{E_2} \longleftarrow c_2 \oplus \gamma$
- if $\sum y_i = 0$ then $\sum x_i = 0$
- if boomerang holds then $m_3 \oplus m_4 = \alpha$

Boomerang attack - a 2nd order differential

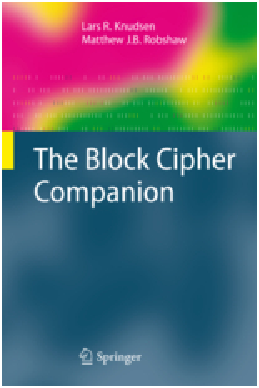
- $m \longrightarrow \boxed{E_1} \longrightarrow x_1 \longrightarrow \boxed{A_k} \longrightarrow y_1 \longrightarrow \boxed{E_2} \longrightarrow c$
- $m_3 \longleftarrow \boxed{E_1} \longleftarrow x_3 \longleftarrow \boxed{A_k} \longleftarrow y_3 \longleftarrow \boxed{E_2} \longleftarrow c \oplus \gamma$
- $m \oplus \alpha \longrightarrow \boxed{E_1} \longrightarrow x_2 \longrightarrow \boxed{A_k} \longrightarrow y_2 \longrightarrow \boxed{E_2} \longrightarrow c_2$
- $m_4 \longleftarrow \boxed{E_1} \longleftarrow x_4 \longleftarrow \boxed{A_k} \longleftarrow y_4 \longleftarrow \boxed{E_2} \longleftarrow c_2 \oplus \gamma$
- if $\sum y_i = 0$ then $\sum x_i = 0$
- if boomerang holds then $m_3 \oplus m_4 = \alpha$
- four half-cipher differentials, boomerang probability $p_1 p_2 q^2$
- note that we pass through A_k “for free”.

Conclusion from me

- modern block ciphers introduced with DES
- differential and linear cryptanalysis started new era
- many advanced attacks on block ciphers today
- many interesting designs, many unbroken proposals
- good understanding of block cipher security
- latest trend: lightweight block ciphers

The Block Cipher Companion

By Lars R. Knudsen and Matt Robshaw.



Lars R. Knudsen
Matthew J.B. Robshaw

The Block Cipher Companion

Springer

Available in a few weeks from now via Springer and Amazon!