Truncated Differentials

Lars R. Knudsen

June 2014
Outline

1. Truncated differentials

2. 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.
Truncated differentials
Impossible differentials

CipherFOUR

\[ m \]

\[ k_0 \]

\[ k_1 \]

\[ S \]

\[ S \]

\[ S \]

\[ S \]

\[ S \]

\[ S \]

\[ S \]

\[ S \]

\[ S \]

\[ S \]
5 rounds of CipherFour

$k_2$

$k_3$

$k_4$

$k_5$

C

Lars R. Knudsen

Truncated Differentials
Consider

\[(0, 0, 2, 0)^{(S, S, S, S)} \rightarrow (0, 0, 2, 0)\]

which has probability \(\frac{6}{16}\) and note that

\[(0, 0, 2, 0) \xrightarrow{P} (0, 0, 2, 0)\]

Thus

\[(0, 0, 2, 0) \xrightarrow{R} (0, 0, 2, 0)\]
Characteristic

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

with probability

\((\frac{6}{16})^2\)

and

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

with probability

\((\frac{6}{16})^4 \approx 0.02.\)

Example

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

Lars R. Knudsen

Truncated Differentials Impossible 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

\[(0, 0, 2, 0) \xrightarrow{4\mathcal{R}} (0, 0, 2, 0).\]
Truncated differentials

Impossible differentials

Differentials

\((0, 0, 2, 0) \xrightarrow{4_R} (0, 0, 2, 0)\).

There are at least four characteristics involved

\[
\begin{align*}
(0, 0, 2, 0) &\xrightarrow{R} (0, 0, 2, 0) \xrightarrow{R} (0, 0, 2, 0) \xrightarrow{R} (0, 0, 2, 0) \xrightarrow{R} (0, 0, 2, 0), \\
(0, 0, 2, 0) &\xrightarrow{R} (0, 0, 0, 2) \xrightarrow{R} (0, 0, 0, 1) \xrightarrow{R} (0, 0, 1, 0) \xrightarrow{R} (0, 0, 2, 0), \\
(0, 0, 2, 0) &\xrightarrow{R} (0, 0, 0, 2) \xrightarrow{R} (0, 0, 1, 0) \xrightarrow{R} (0, 0, 2, 0) \xrightarrow{R} (0, 0, 2, 0), \\
(0, 0, 2, 0) &\xrightarrow{R} (0, 0, 2, 0) \xrightarrow{R} (0, 0, 0, 2) \xrightarrow{R} (0, 0, 1, 0) \xrightarrow{R} (0, 0, 2, 0).
\end{align*}
\]

\(P((0, 0, 2, 0) \xrightarrow{4_R} (0, 0, 2, 0)) \approx 0.081 > 0.02.\)
Differential Attack of CIPHERFOUR

\[ S \]

\[ k_3 \rightarrow \]

\[ ? \]

\[ ? \]

\[ ? \]

\[ ? \]

\[ S \]

\[ S \]

\[ S \]

\[ S \]

\[ k_4 \rightarrow \]

\[ 0 \]

\[ 0 \]

\[ 2 \]

\[ 0 \]

\[ S \]

\[ S \]

\[ S \]

\[ S \]

\[ k_5 \rightarrow \]

\[ 0 \]

\[ 0 \]

\[ ? \]

\[ 0 \]

\[ c^0 \]

\[ c^1 \]

\[ c^2 \]

\[ c^3 \]
Differential attack on 5 rounds
Attacker tries to determine four bits of the key

<table>
<thead>
<tr>
<th>Number of texts</th>
<th>Differential attack</th>
</tr>
</thead>
<tbody>
<tr>
<td>32</td>
<td>64%</td>
</tr>
<tr>
<td>64</td>
<td>76%</td>
</tr>
<tr>
<td>128</td>
<td>85%</td>
</tr>
<tr>
<td>256</td>
<td>96%</td>
</tr>
</tbody>
</table>
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.
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:

- $0010 \xrightarrow{S} 0001$ has probability $\frac{6}{16}$.
- $0010 \xrightarrow{S} 0010$ has probability $\frac{6}{16}$.
- $0010 \xrightarrow{S} 1001$ has probability $\frac{2}{16}$.
- $0010 \xrightarrow{S} 1010$ has probability $\frac{2}{16}$.
- $0010 \xrightarrow{S} \ast0\ast\ast$ has probability 1.
### Distribution Table

<table>
<thead>
<tr>
<th>in \ out</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
<th>e</th>
<th>f</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>16</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>1</td>
<td>-</td>
<td>-</td>
<td>6</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>2</td>
<td>-</td>
<td>2</td>
<td>-</td>
<td>-</td>
<td>2</td>
<td>-</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td>-</td>
<td>6</td>
<td>6</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>2</td>
<td>2</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>3</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>6</td>
<td>-</td>
<td>2</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>4</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>4</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>2</td>
<td>-</td>
<td>2</td>
<td>4</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>2</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>5</td>
<td>-</td>
<td>2</td>
<td>2</td>
<td>-</td>
<td>4</td>
<td>-</td>
<td>-</td>
<td>4</td>
<td>2</td>
<td>-</td>
<td>-</td>
<td>2</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>6</td>
<td>-</td>
<td>-</td>
<td>2</td>
<td>-</td>
<td>4</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>2</td>
<td>2</td>
<td>-</td>
<td>2</td>
<td>2</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>7</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>4</td>
<td>4</td>
<td>-</td>
<td>-</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>8</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>2</td>
<td>-</td>
<td>2</td>
<td>4</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>4</td>
<td>-</td>
<td>2</td>
<td>-</td>
</tr>
<tr>
<td>9</td>
<td>-</td>
<td>2</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>-</td>
<td>4</td>
<td>2</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>2</td>
</tr>
<tr>
<td>a</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>2</td>
<td>2</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>4</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>b</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>2</td>
<td>2</td>
<td>-</td>
<td>-</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>c</td>
<td>-</td>
<td>4</td>
<td>-</td>
<td>-</td>
<td>2</td>
<td>-</td>
<td>-</td>
<td>2</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>4</td>
<td>-</td>
<td>6</td>
<td>-</td>
</tr>
<tr>
<td>d</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>2</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>6</td>
<td>2</td>
<td>-</td>
<td>4</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>e</td>
<td>-</td>
<td>2</td>
<td>-</td>
<td>4</td>
<td>2</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>2</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>6</td>
<td>-</td>
</tr>
<tr>
<td>f</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>2</td>
<td>-</td>
<td>2</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>10</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>
Input difference 2 to S-box lead only to output differences 1, 2, 9, and a. So for one round

\[(0000 0000 0010 0000) \xrightarrow{R} \begin{cases} (0000 0000 0010 0000) & \text{or} \\ (0000 0000 0000 0010) & \text{or} \\ (0010 0000 0010 0000) & \text{or} \\ (0010 0000 0000 0010) & \end{cases} \]
Truncated differentials

\[
\begin{array}{rccr}
(0000 & 0000 & 0010 & 0000) & \xrightarrow{R} & (00\star0 & 0000 & 00\star0 & 00\star0) \\
(0000 & 0000 & 0000 & 0010) & \xrightarrow{R} & (000\star & 0000 & 000\star & 000\star) \\
(0010 & 0000 & 0010 & 0000) & \xrightarrow{R} & (*0\star0 & 0000 & *0\star0 & *0\star0) \\
(0010 & 0000 & 0000 & 0010) & \xrightarrow{R} & (*00\star & 0000 & *00\star & *00\star) \\
\end{array}
\]
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
  \[(\star 0\star\star 0000 \star 0\star\star \star 0\star\star) \xrightarrow{\mathcal{R}} (\star 0\star\star \star 0\star\star \star 0\star\star \star 0\star\star)\]
This leads to a 3-round truncated differential
\[
(0000 \ 0000 \ 0010 \ 0000) \xrightarrow{3R} (\star \ 0\star\star \ \star \ 0\star\star \ \star \ 0\star\star \ \star)
\]
of probability 1!

Can we extend this further?
Consider the 1-round characteristic
\[(0000\ 0000\ 0010\ 0000) \xrightarrow{R} (0000\ 0000\ 0010\ 0000).\]
A pair will follow this characteristic if \[2 \xrightarrow{S} 2\]
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
\[(t_0 \oplus t_0\ t_1 \oplus t_1\ i \oplus j\ t_2 \oplus t_2) = (0000\ 0000\ \star\star\star\ 0000).\]
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

$$(0000 \ 0000 \ \star \star \star \ 0000) \xrightarrow{R} (0000 \ 0000 \ 0010 \ 0000).$$

With correct guess of four-bit key one can easily identify these eight.
Summing up: yields a 4-round truncated differential

\[
(0000 0000 \star\star\star\star 0000) \xrightarrow{4R} (\star 0\star\star \star 0\star\star \star 0\star\star \star 0\star\star)
\]

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 CipherFours

Truncated differentials
Impossible differentials

$k_3 \rightarrow \oplus$

\[ \begin{array}{cccc} S & S & S & S \\ \end{array} \]

$k_4 \rightarrow \oplus$

\[ \begin{array}{cccc} 0 & 0 & 0 & 0 \\ \end{array} \]

$k_5 \rightarrow \oplus$

\[ \begin{array}{cccc} c^0 & c^1 & c^2 & c^3 \\ \end{array} \]

Lars R. Knudsen
Truncated Differentials
5-round attack on CIPHERFOUR

<table>
<thead>
<tr>
<th>Number of texts</th>
<th>Differentials</th>
<th>Truncated differentials</th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td>.</td>
<td>28% (4+4)</td>
</tr>
<tr>
<td>32</td>
<td>.</td>
<td>78% (4+9)</td>
</tr>
<tr>
<td>48</td>
<td>.</td>
<td>97% (4+12)</td>
</tr>
<tr>
<td>64</td>
<td>76% (4)</td>
<td></td>
</tr>
<tr>
<td>128</td>
<td>85% (4)</td>
<td></td>
</tr>
<tr>
<td>256</td>
<td>96% (4)</td>
<td></td>
</tr>
</tbody>
</table>

Numbers in brackets denote the number of key bits identified.
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**
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 $\alpha$ 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

\[ f \]

\[ \alpha \oplus \gamma \]

\[ \beta \]

\[ \alpha \neq 0 \]

\[ \beta \neq 0 \]

\[ \gamma \neq 0 \]
Truncated differentials - Feistel network

\[ \beta \xleftarrow{\oplus} f \xrightarrow{\oplus} \alpha \oplus \gamma \]

\[ \alpha \oplus \gamma \xleftarrow{\oplus} f \xrightarrow{\oplus} \beta \]

\[ \alpha \oplus \gamma \xleftarrow{\oplus} f \xrightarrow{\oplus} \beta \]

\[ \alpha \oplus \gamma \xleftarrow{\oplus} f \xrightarrow{\oplus} \beta \]
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

Truncated differentials

Impossible differentials

Lars R. Knudsen

Truncated Differentials