Differential Cryptanalysis

Debdeep Mukhopadhyay

Assistant Professor
Department of Computer Science and Engineering
Indian Institute of Technology Kharagpur
INDIA -721302

Objectives

• Concept of Differentials

• Propagation Ratio

• The Differential Attack
Some Points

• Similar to linear cryptanalysis

• Main “difference” is that it uses the information about the xor of two inputs and the xor of corresponding two outputs

• Chosen PlainText Attack (CPA)

Algorithm

• Input, \( x: \{0,1\}^m \), \( K_0: \{0,1\}^m \)
• Output, \( y: \{0,1\}^m \)
• Key-schedule: generates \( (K_0, K_1, \ldots, K_{N_r}) \)

\[
\begin{align*}
    w_0 &= x \\
    \text{for } r=1 \text{ to } N_r-1 \\
    u_r &= w_{r-1} \oplus K_{r-1} \\
    v_r &= S(u_r) \\
    w_r &= v_{P(1)}^r, v_{P(2)}^r, \ldots, v_{P(m)}^r \\
    u_{N_r} &= v_{N_r-1} \oplus K_{N_r-1} \\
    \text{for } i = 1 \text{ to } m \\
    v_{N_r} &= S(u_{N_r}) \\
    y &= v_{N_r} \oplus K_{N_r}
\end{align*}
\]
Example: GPig Cipher

- \( l=m=N_r=4 \)
- Thus plain text size is 16 bits
- It is divided into 4 groups of 4 bits each.
- S-Box works on each of the 4 bits
- Consider a S-Box (substitution table)

<table>
<thead>
<tr>
<th>input</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>output</td>
<td>E</td>
<td>4</td>
<td>D</td>
<td>1</td>
<td>2</td>
<td>F</td>
<td>B</td>
<td>8</td>
<td>3</td>
<td>A</td>
<td>6</td>
<td>C</td>
<td>5</td>
<td>9</td>
<td>0</td>
<td>7</td>
</tr>
</tbody>
</table>

G Pig (contd.)

- The Permutation Table is as follows:

<table>
<thead>
<tr>
<th>input</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>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
<th>16</th>
</tr>
</thead>
<tbody>
<tr>
<td>output</td>
<td>1</td>
<td>5</td>
<td>9</td>
<td>13</td>
<td>2</td>
<td>6</td>
<td>10</td>
<td>14</td>
<td>3</td>
<td>7</td>
<td>11</td>
<td>15</td>
<td>4</td>
<td>8</td>
<td>12</td>
<td>16</td>
</tr>
</tbody>
</table>

- Permutation is the transposition of bits
- There are \( l=m=16 \) bits, which are transposed using the above table
Modifications or Variations of the SPN Structure

- Examples: DES, AES
- Different S-Boxes instead of a single one
  - As done in DES, there are 8 different S-Boxes
- Have an additional invertible linear transformation
  - As done in AES
- Is the GPlg Cipher secure?
Key Scheduling

• Consider the key to be 32 bits (too small)
• A simple key schedule:
  – $K_r$ is made by taking 16 successive bits from the key starting at $(4r + 1)$ bit position.
• Example: Input Key, $K$:
  – 0011 1010 1001 0100 1101 0110 0011 1111
  – $K^0$ = 0011 1010 1001 0100
  – $K^1$ = 1010 1001 0100 1101
  – $K^2$ = 1001 0100 1101 0110
  – $K^3$ = 0100 1101 0110 0011
  – $K^4$ = 1101 0110 0011 1111

Informal Working of the Attack

• Attacker chooses an input XOR, $x'$
• He has several tuples : $(x, x^*, y, y^*)$ st $x^\oplus x^* = x'$
• For each pair of $y$ and $y^*$, he guesses the key value of the last round
• Decrypts the pair, and checks the XOR at the last but one round.
Informal Working of the Attack

• He checks out whether the result matches with the most probable outcome (which he has found out using some probabilistic approach, analogous to the finding of the best linear approximation in case of linear attack)
• He maintains a frequency table, for each key noting the number of matches.
• It is expected that the candidate key will have the highest number of matches.

Obtaining differential characteristics of the S-Box

• Let S: \(\{0,1\}^m \rightarrow \{0,1\}^n\) be an S-Box. Consider an ordered pair of bit-strings of length m, say \((x,x^*)\)
  • Input xor: \(x \oplus x^*\)
  • Output xor: \(y \oplus y^* = S(x) \oplus S(x^*)\)
  • Note that the xor is an n bit string
  • Define \(\Delta(x')\) to be the set of all ordered pairs, \((x,x^*)\) such that \(x \oplus x^* = x'\)
The Delta Set

\[\Delta(x') = \{(x, x \oplus x') : x \in \{0, 1\}^m\}.\]

- Observe that the number of elements in the set is \(2^m\).
- For each pair in the set, the number of values which the output xor can take is \(2^n\).
- Thus the \(2^m\) output pairs are distributed among \(2^n\) values.
- The non-uniformity in the distribution is exploited in the attack.

An Example Set

- \(\Delta(1011) = \{(0000, 1011), (0001, 1010), \ldots, (1111, 0100)\}\)

<table>
<thead>
<tr>
<th>(x)</th>
<th>(x^*)</th>
<th>(y)</th>
<th>(y^*)</th>
<th>(y')</th>
</tr>
</thead>
<tbody>
<tr>
<td>0000</td>
<td>1011</td>
<td>1110</td>
<td>1100</td>
<td>0010</td>
</tr>
<tr>
<td>0001</td>
<td>1010</td>
<td>0100</td>
<td>0110</td>
<td>0010</td>
</tr>
<tr>
<td>0010</td>
<td>1001</td>
<td>1101</td>
<td>1010</td>
<td>0111</td>
</tr>
<tr>
<td>0011</td>
<td>1000</td>
<td>0001</td>
<td>0111</td>
<td>0010</td>
</tr>
<tr>
<td>0100</td>
<td>1111</td>
<td>0010</td>
<td>0111</td>
<td>0101</td>
</tr>
<tr>
<td>0101</td>
<td>1110</td>
<td>1111</td>
<td>0000</td>
<td>1111</td>
</tr>
<tr>
<td>0110</td>
<td>1101</td>
<td>1011</td>
<td>1001</td>
<td>0010</td>
</tr>
<tr>
<td>0111</td>
<td>1100</td>
<td>1000</td>
<td>0101</td>
<td>1101</td>
</tr>
<tr>
<td>1000</td>
<td>0011</td>
<td>0011</td>
<td>0001</td>
<td>0010</td>
</tr>
<tr>
<td>1001</td>
<td>0010</td>
<td>1010</td>
<td>1101</td>
<td>0111</td>
</tr>
<tr>
<td>1010</td>
<td>0001</td>
<td>0110</td>
<td>0100</td>
<td>0010</td>
</tr>
<tr>
<td>1011</td>
<td>0000</td>
<td>1100</td>
<td>1110</td>
<td>0010</td>
</tr>
<tr>
<td>1100</td>
<td>0111</td>
<td>0101</td>
<td>1000</td>
<td>1101</td>
</tr>
<tr>
<td>1101</td>
<td>0110</td>
<td>1001</td>
<td>1011</td>
<td>0010</td>
</tr>
<tr>
<td>1110</td>
<td>0101</td>
<td>0000</td>
<td>1111</td>
<td>1111</td>
</tr>
<tr>
<td>1111</td>
<td>0100</td>
<td>0111</td>
<td>0010</td>
<td>0101</td>
</tr>
</tbody>
</table>
Non-uniform distribution of the output XORs of an S-Box

- Frequency Distribution of the Output XORs show that only 5 out of the 16 possible XORs occur
- Non-uniform distribution
- In an uniform distribution, all the output XORs would have occurred once.
- This attack exploits this property, which serves as the distinguisher

Difference Distribution Table

<table>
<thead>
<tr>
<th>$a'$</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>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>4</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>6</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>6</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>4</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>7</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>8</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>4</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>9</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>A</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>B</td>
<td>0</td>
<td>0</td>
<td>8</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>C</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>6</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>D</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>E</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>6</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>F</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>6</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
</tbody>
</table>

Any entry is denoted by $N_D(\Delta x, \Delta y)$

Thus $N_D(B, 2) = 8$
Effect of the key on the Differential

- The Key has no effect on the XOR because it is mixed using XOR function, which is also used to compute the XOR.

Propagation Ratio

- Propagation Ratio (Prop Ratio) is the probability that an input XOR \( a' \) gives an output XOR \( b' \).
- The pair \( (a',b') \) is called a Differential.
- Thus Prop ratio for \( (a',b') \):

\[
R_p(a', b') = \frac{N_D(a', b')}{2^m}.
\]
Differential Trail

• Since the intermediate keys has no effect on the XORs, we may neglect them for now.

• We wish to combine those propagation ratios for which the input XOR of a differential in any round is equal to the output XOR of the last round differential

• To be precise, the output XOR is actually the permuted XOR of the last round differential

• The Prop ratios are assumed to be independent

Thus we may multiply the prop-ratios.

- In $S^1_2$, $R_p(1011, 0010) = 1/2$
- In $S^3_2$, $R_p(0100, 0110) = 3/8$
- In $S^3_2$, $R_p(0010, 0101) = 3/8$
- In $S^3_3$, $R_p(0010, 0101) = 3/8$

Thus resultant Prop-ratio is obtained as:

$$R_p(0000 \ 1011 \ 0000 \ 0000, 0000 \ 0101 \ 0101 \ 0000) = \frac{1}{2} \times \left(\frac{3}{8}\right)^3 = \frac{27}{1024}.$$
Obtaining the Differential for 4-1=3 rounds

- Thus we have, if \( x' = 0000\ 1011\ 0000\ 0000 \), then \( (v^3)' = 0000\ 0100\ 0101\ 0000 \) with a probability of \( 27/1024 \).
- Also note that the key has no effect on the XOR \( (v^3)' \)
- Thus, we have \( (v^3)' = (u^4)' \)
- Hence it follows that if \( x' = 0000\ 1011\ 0000\ 0000 \), then \( (u^4)' = 0000\ 0110\ 0000\ 0110 \) with a probability of \( 27/1024 \).
- Note that \( (u^4)' \) is the input differential at the input of the last round S-Box

The Attack

- Choose say 5000 Plaintexts with the input XOR equal to: \( (0000,1011,0000,0000) \)
- The corresponding ciphertexts are noted
- The key is guessed. Note that we need to guess 8 bits of the key.
The Attack

- Decrypt the last round and verifying whether the differential at the input of the last round S-Box is 0000 0110 0000 0110
- Make a frequency table for the keys

<table>
<thead>
<tr>
<th>partial subkey $[K_{5,5}, K_{5,6}, K_{5,13}, K_{5,16}]$</th>
<th>prob</th>
<th>partial subkey $[K_{5,5}, K_{5,6}, K_{5,13}, K_{5,16}]$</th>
<th>prob</th>
</tr>
</thead>
<tbody>
<tr>
<td>1C</td>
<td>0.0000</td>
<td>2A</td>
<td>0.0032</td>
</tr>
<tr>
<td>1D</td>
<td>0.0000</td>
<td>2B</td>
<td>0.0022</td>
</tr>
<tr>
<td>1E</td>
<td>0.0000</td>
<td>2C</td>
<td>0.0000</td>
</tr>
<tr>
<td>1F</td>
<td>0.0000</td>
<td>2D</td>
<td>0.0000</td>
</tr>
<tr>
<td>20</td>
<td>0.0000</td>
<td>2E</td>
<td>0.0000</td>
</tr>
<tr>
<td>21</td>
<td>0.0136</td>
<td>2F</td>
<td>0.0000</td>
</tr>
<tr>
<td>22</td>
<td>0.0068</td>
<td>30</td>
<td>0.0004</td>
</tr>
<tr>
<td>23</td>
<td>0.0068</td>
<td>31</td>
<td>0.0000</td>
</tr>
<tr>
<td>24</td>
<td>0.0244</td>
<td>32</td>
<td>0.0004</td>
</tr>
<tr>
<td>25</td>
<td>0.0000</td>
<td>33</td>
<td>0.0004</td>
</tr>
<tr>
<td>26</td>
<td>0.0068</td>
<td>34</td>
<td>0.0000</td>
</tr>
<tr>
<td>27</td>
<td>0.0068</td>
<td>35</td>
<td>0.0004</td>
</tr>
<tr>
<td>28</td>
<td>0.0030</td>
<td>36</td>
<td>0.0000</td>
</tr>
<tr>
<td>29</td>
<td>0.0024</td>
<td>37</td>
<td>0.0008</td>
</tr>
</tbody>
</table>

From this observation we conclude 24 is the correct key, with a proportion of around 27/1024 = 0.0264, which is close to the experimental value of 0.0244.
Immunity Against DC

- Build the S-Box with a uniform distribution.
- Note that the number of pairs of plaintext and ciphertext required is roughly inversely proportional to the probability of the differential.

Immunity Against DC

- So, a low probability of the differential is desirable.
- The S-Boxes are built to ensure that all the differentials have a prop-ratio which is less than a bound.
Exercise

• For each of the eight S-Boxes of DES, compute the bias of the random variable:

\[ X_2 \oplus Y_1 \oplus Y_2 \oplus Y_3 \oplus Y_4 \]

Further Reading

• B. A. Forouzan, “Cryptography and Network Security”, TMH
• Howard Heys, “A Tutorial on Linear and Differential Cryptanalysis”, 2001
Next Days Topic

- Some Other Cryptanalytic Techniques