Table 1 shows the number of indicators for $N$ different patterns. The density function of $I_K$ is:

$$f_{I_K}(x) = \frac{1}{p} \left( \frac{1}{e} \right) \frac{x^{\frac{1}{2}}}{2} \exp \left( \frac{-x}{2N} \right)$$

where $p = \frac{1}{2}$, and $N$ is the number of patterns. The density function of the other indicators are:

$$f_{R}(x) = \frac{1}{p} \left( \frac{1}{e} \right) \frac{x^{\frac{1}{2}}}{2} \exp \left( \frac{-x}{2N} \right)$$

The probability that $jI_Kj$ is one of the $n$ highest indicators (rather than the maximal one) is:

$$P_n(N) = \int_{0}^{\infty} f_{I_K}(x) dx$$

Our goal is to calculate the success rate of our attack $P_j(N)$. The density function

$$P_j(N) = \int_{0}^{\infty} f_{I_K}(x) dx$$

with a high probability $P_j(N)$. The density function

$$P_j(N) = \int_{0}^{\infty} f_{I_K}(x) dx$$
In this appendix we present the details of the calculations of the success rate of our attack versus its data complexity. These calculations were used to generate Table 2.

References


[4] Kwangjo Kim, Sangjun Park, Sajin Lee, How to Strengthen DES Against 5-

Summary

...
Table 1: Comparison of the success probability of differential cryptanalysis, linear cryptanalysis, Davies' attack, and the improved attack.
the distribution generated with the particular value of the key is increased by the value of the corresponding counter. In order to make DES-like S-boxes immune to the differential property of the DES, we suggest additional design principles to minimize the differential property in S-boxes. Davies estimates that the correlations of the outputs of the pairs of the S-boxes were reduced in DES. He claims that much stronger reductions are possible. In this section we suggest additional design principles to make DES-like S-boxes immune to Davies' attacks.

A S-box is immune to Davies' attacks if and only if it has uniform joint distribution:

\[ D_1(x,y) = D_1(x'y') \]

\[ D_0(x,y) = D_0(x'y') \]

The success of Davies' attack is repeated twice, once for the even rounds and once for the odd rounds.

Discussion

Davies estimates that the correlations of the outputs of the pairs of the S-boxes were reduced in DES. He claims that much stronger reductions are possible. In this section we suggest additional design principles to make DES-like S-boxes immune to Davies' attacks.

S-boxes immune to Davies' attacks must have uniform joint distribution:

\[ D_1(x,y) = D_1(x'y') \]

\[ D_0(x,y) = D_0(x'y') \]

In order to make DES-like S-boxes immune to Davies' attacks, we suggest additional design principles to minimize the differential property in S-boxes. Davies estimates that the correlations of the outputs of the pairs of the S-boxes were reduced in DES. He claims that much stronger reductions are possible. In this section we suggest additional design principles to make DES-like S-boxes immune to Davies' attacks.

\[ D_1(x,y) = D_1(x'y') \]

\[ D_0(x,y) = D_0(x'y') \]
In the efficient algorithm the attack incorporates a data collection phase and a data analysis phase. Only 10 ciphertext bits are required for the partial decryption. The data collection phase counts the number of occurrences of each possible value of the eight distribution bits (which are received as XOR of plaintext and ciphertext) together with these ten ciphertext bits (entering the pair of S-boxes in the last round), and outputs an array of 98 counters. Note that the data collection phase of the efficient algorithm is more than 90% 7-4. 27/4, 10/1. Since we should distinguish the right distribution from the 10 random distributions, we use a statistical technique (see the Appendix) to distinguish the right distribution. We get 90% success rate in the partial decryption. Once we get 90% success rate, we will detect our efficient algorithm to solve this problem. One way we get 90% success rate is performed, the complexity of this attack is more than 90%. 7-4. 27/4, 10/1. Success rate for m key bits found (\%)

<table>
<thead>
<tr>
<th>complexity</th>
<th>success rate for m key bits found (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table 2:</td>
<td>complexity for the improved Davies attack for different number of key bits found.</td>
</tr>
</tbody>
</table>
3 The Improved Attack

Table 1: The complexities of Davies' attack.

<table>
<thead>
<tr>
<th>Rounds</th>
<th>Distribution</th>
<th>1/6</th>
<th>2/7</th>
<th>3/8</th>
<th>4/9</th>
<th>5/10</th>
<th>6/11</th>
<th>7/12</th>
<th>8/13</th>
<th>9/14</th>
<th>10/15</th>
<th>11/16</th>
<th>12/17</th>
<th>13/18</th>
<th>14/19</th>
<th>15/20</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/6</td>
<td>D</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2/7</td>
<td>D</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3/8</td>
<td>D</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>4/9</td>
<td>D</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>5/10</td>
<td>D</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>6/11</td>
<td>D</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>7/12</td>
<td>D</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>8/13</td>
<td>D</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>9/14</td>
<td>D</td>
<td>9</td>
<td>9</td>
<td>9</td>
<td>9</td>
<td>9</td>
<td>9</td>
<td>9</td>
<td>9</td>
<td>9</td>
<td>9</td>
<td>9</td>
<td>9</td>
<td>9</td>
<td>9</td>
<td>9</td>
</tr>
<tr>
<td>10/15</td>
<td>D</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>12/17</td>
<td>D</td>
<td>12</td>
<td>12</td>
<td>12</td>
<td>12</td>
<td>12</td>
<td>12</td>
<td>12</td>
<td>12</td>
<td>12</td>
<td>12</td>
<td>12</td>
<td>12</td>
<td>12</td>
<td>12</td>
<td>12</td>
</tr>
<tr>
<td>13/18</td>
<td>D</td>
<td>13</td>
<td>13</td>
<td>13</td>
<td>13</td>
<td>13</td>
<td>13</td>
<td>13</td>
<td>13</td>
<td>13</td>
<td>13</td>
<td>13</td>
<td>13</td>
<td>13</td>
<td>13</td>
<td>13</td>
</tr>
<tr>
<td>14/19</td>
<td>D</td>
<td>14</td>
<td>14</td>
<td>14</td>
<td>14</td>
<td>14</td>
<td>14</td>
<td>14</td>
<td>14</td>
<td>14</td>
<td>14</td>
<td>14</td>
<td>14</td>
<td>14</td>
<td>14</td>
<td>14</td>
</tr>
<tr>
<td>15/20</td>
<td>D</td>
<td>15</td>
<td>15</td>
<td>15</td>
<td>15</td>
<td>15</td>
<td>15</td>
<td>15</td>
<td>15</td>
<td>15</td>
<td>15</td>
<td>15</td>
<td>15</td>
<td>15</td>
<td>15</td>
<td>15</td>
</tr>
</tbody>
</table>

In this section we present an improved version of Davies' attack which breaks the full 16-round DES faster than an exhaustive search.
Davies found that this distribution depends only on the parity of the four key bits which are mixed with the shared data bits. We denote this parity by \( p \) and the mean value of the various values of the distribution by \( E(\mathcal{D}) \). The distribution of the output of a pair of S-boxes can be written as:

\[
\mathcal{D}(x; y; p) = E(\mathcal{D}) + p \cdot E(\mathcal{D})
\]

where \( x \) is the output of the left S-box of the pair and \( y \) is the output of the right S-box. The XOR of the outputs of the \( F \)-functions in the even (odd) rounds can be calculated by XORing of the right (left) half of the plaintext with the left (right) half of the ciphertext and applying the inverse permutation \( P^{-1} \).

Davies found that the \( n \)-fold XOR distributions of the outputs of adjacent pairs of S-boxes have a form similar to equation (1):

\[
\mathcal{D}(x; y; p_n) = E(\mathcal{D}) + p_n \cdot E(\mathcal{D})
\]

where \( p_n \) is the parity of the \( 4n \) subkey bits which are mixed with the data bits in the even (odd) rounds, and

\[
E(\mathcal{D}) = \frac{1}{2^n} \sum_{x, y} \mathcal{D}(x; y; p_n)
\]

Davies suggested to use the indicator function:

\[
I = \begin{cases} 
1 & \text{if } \mathcal{D}(x; y; p_n) > 0 \\
0 & \text{otherwise}
\end{cases}
\]

whose sign observes the parity bit of the key: if \( I > 0 \) the parity is zero and if \( I < 0 \) the parity is one.

\( \mathcal{D}(x; y; p_n) \) is the empirical distribution received from the data collection phase of Davies' attack. Given sufficiently many known plaintexts, the sign in the \( \mathcal{D} \) distribution can be identified, along with one parity bit of the key.

Davies estimated the required amount of data for this attack as:

\[
N = 2^{64} \cdot E(\mathcal{D}) \cdot \sum_{x, y} \mathcal{D}(x; y; p_n)
\]

With this amount of data, a 97.5% success rate is achieved. Table 1 summarizes the complexities of Davies attack on different pairs of S-boxes and different numbers of rounds:

<table>
<thead>
<tr>
<th>S-box Pair</th>
<th>Even Rounds</th>
<th>Odd Rounds</th>
</tr>
</thead>
<tbody>
<tr>
<td>( S_7 )</td>
<td>2.16 \times 10^{29}</td>
<td>1.4 \times 10^{26}</td>
</tr>
</tbody>
</table>

Therefore, Davies' attack is not practical and is only of theoretical interest.
An Improvement of Davies’ Attack on DES

Abstract

In this paper we improve Davies’ attack to break the full 16-round DES faster than brute force. We describe a tradeoff between the number of plain texts, the success rate and the time of analysis. The best tradeoff requires 2^4 known plain texts and finds 2^4 key bits for which it requires 2^14 known plain texts. The data analysis phase is independent of the number of rounds and runs only several minutes on a SPARC. Therefore, this is the third successful attack on DES, faster than brute force, after differential and linear cryptanalysis. We also suggest criteria which make the S-boxes immune to this attack.

1 Introduction

Davies’ attack

In this paper we improve Davies’ attack to break the full 16-round DES faster than brute force. We describe a tradeoff between the number of plain texts, the success rate and the time of analysis. The best tradeoff requires 2^4 known plain texts and finds 2^4 key bits for which it requires 2^14 known plain texts. The data analysis phase is independent of the number of rounds and runs only several minutes on a SPARC. Therefore, this is the third successful attack on DES, faster than brute force, after differential and linear cryptanalysis. We also suggest criteria which make the S-boxes immune to this attack.