Related-Key Attacks

See:

Block Ciphers
1. Block ciphers usually iterate a weak function many times, in order to get a strong function.
2. Each round function takes the data from the previous round, and a subkey.
3. A key scheduling algorithm derives the list of the subkeys, one for each round, from the key.

Related-Key attacks use properties of key scheduling algorithms.
They show how small details can affect the strength of a cipher.

Modified DES
In the study of related-key attacks, we assume that the key scheduling of DES is slightly modified, and whose all shift figures are replaced by a fixed number (say 2).

Outline of DES and of its Key Scheduling Algorithm

The Numbers of Shifts in the Key Scheduling Algorithm
The Numbers of Shifts in the Key Scheduling Algorithm of DES, and the Modified Variant

<table>
<thead>
<tr>
<th>Round</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>Shifts</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Modified variant</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>
<td></td>
</tr>
</tbody>
</table>

Related Keys
Both the encryption function and the key scheduling algorithm are iterative.
The transformation of each round (in both parts) is fixed in all the rounds (after modification).
We base the attacks on this fact: We use pairs of encryptions, which compute the same intermediate data, but with a shift of one (or more) rounds.

Types of Attacks
1. Ciphertext only attack
2. Known plaintext attack
3. Chosen plaintext attack
4. Adaptive chosen plaintext attack
5. Chosen key attack

Relations of Subkeys in the Key Scheduling Algorithm

Outline of DES and of its Key Scheduling Algorithm

The Numbers of Shifts in the Key Scheduling Algorithm
The Numbers of Shifts in the Key Scheduling Algorithm of DES, and the Modified Variant

<table>
<thead>
<tr>
<th>Round</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>Shifts</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Modified variant</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>
<td>2</td>
</tr>
</tbody>
</table>

Related Keys
Both the encryption function and the key scheduling algorithm are iterative.
The transformation of each round (in both parts) is fixed in all the rounds (after modification).
We base the attacks on this fact: We use pairs of encryptions, which compute the same intermediate data, but with a shift of one (or more) rounds.

Types of Attacks
1. Ciphertext only attack
2. Known plaintext attack
3. Chosen plaintext attack
4. Adaptive chosen plaintext attack
5. Chosen key attack
The Chosen Plaintext Attack – Complementation Property

1. Choose \( P \). Let \( P' = P \).
2. Ask for the ciphertexts \( C_0 = E_K(P_1) \) and \( C_1 = E_K(P_2) \).
3. Examine the two pairs \( (P_1, C_0) \) and \( (P_2, C_1) \) whose right halves are the left half of \( P_1 \) and \( P_2 \) whose left halves receive all the possible values by XORing all the possible 32-bit values \( k \) to the right half of \( P_1 \) and \( P_2 \).
4. If \( E_K(P_1) = C_0 \), then probably \( K = K' \).
5. If \( E_K(P_2) = C_1 \), then probably \( K = K' \).
6. Otherwise, neither \( K \) nor \( K' \) is the key \( K \).
7. Since comparisons are much faster than tell侥幸, this attack is twice faster than exhaustive search.

We will now a related-key extension which requires only a third of the complexity (1.4 \cdot 2^{32}).

Chosen Key Attacks

1. Chosen key attacks are not attacks in which the attacker chooses the key.

2. In the chosen key attacks we present, the attacker chooses the relation between two keys, used to encrypt two sets of plaintexts.

3. We describe two types of chosen key attacks: chosen key chosen plaintext attacks and chosen key known plaintext attacks.

The New Chosen Plaintext Attack (cont.)

2: Preprocessing

Preprocessing is used to optimize the computation of the list of keys we test.

1. Consider only the 28-bit half-keys whose most significant bit is zero.
2. Define the next operation as taking a 28-bit half-key, and rotates it by 2 bits to the left (as is applied in the key scheduling algorithm). If the most significant bit of the result is 1, it complements the result.
3. This operation inherits cycles on the half-keys, mostly of size 14.
4. (Pre)process a list of half-keys \( L_k \), including exactly one of the values from each cycle.

The New Chosen Plaintext Attack (cont.)

The Chosen Key Chosen Plaintext Attack

1. Assume \( K \) and \( K' \) are related such that the subkeys satisfy \( K_j = K_{j+1} \).

2. Choose 2^{19} plaintexts \( P_1 \) and 2^{19} plaintexts \( P_1' \) such that \( P_1 = P_1' \), chosen constant for any \( i \) and \( j \).

3. Ask for the ciphertexts \( C_i = E_K(P_i) \) and \( C_i' = E_{K'}(P_i) \) (where \( K \) is the modified-DES encryption).

4. Identify all the pairs \( C_i \) and \( C_i' \) for which \( C_i = C_i' \).

5. For each such pair, find the values of \( K \) satisfying

\[
F(P_i, K_1) = P_i \oplus P_1,
\]

and

\[
F(C_i, K_1') = C_i \oplus C_i'.
\]

6. Complete \( K \).

The Chosen Key Known Plaintext Attack

1. Assume \( K \) and \( K' \) are related such that the subkeys satisfy \( K_j = K_{j+1} \).

2. Collect 2^{19} plaintexts \( P_1 \) and 2^{19} plaintexts \( P_1' \).

3. Collect the ciphertexts \( C_i = E_K(P_i) \) and \( C_i' = E_{K'}(P_i) \).

4. Identify all the pairs \( C_i \) and \( C_i' \) for which \( P_i = P_1 \) and \( C_i = C_i' \).

5. For each such pair, find the values of \( K \) satisfying

\[
F(P_i, K_1) = P_i \oplus P_1,
\]

and

\[
F(C_i, K_1') = C_i \oplus C_i'.
\]

6. Complete \( K \).

The New Chosen Plaintext Attack

1: The Data

1. Choose \( P \). Let \( P_1 = P \).

2. For each plaintext \( P_i \) \((i \in \{0, 1\})\), choose the additional 2^{27} plaintexts \( P_j = (P_i \oplus k, P_i) \) whose right halves receive all the possible values by XORing all the possible 32-bit values \( k \) to the left half of \( P_i \).

3. For each plaintext \( P_i \), choose the additional 2^{32} plaintexts \( P_j = (P_i \oplus k, P_i) \) whose right halves are the left half of \( P_i \) and whose left halves receive all the possible values by XORing all the possible 32-bit values \( k \) to the right half of \( P_i \).
The New Chosen Plaintext Attack (cont.)

3: The Attack

Given the ciphertexts \( \{C_i\}, \{C_{i,k}\}, \{\bar{C}_{i,k}\} \):

1. Generate the trial keys one by one. An optimal procedure performs:
   - For each pair of half-keys \((L_i, L_j)\), try all the 140 keys \(K'\) of the forms
     \(K' = (\text{ROL}_m(L_i), \text{ROL}_n(L_j))\), and
     \(K' = (\text{ROL}_m(L_i), \bar{\text{ROL}}_n(L_j))\), where \(m\) is a multiple of two and \(n\) is one of \(\{0, 6, 12, 18, 24\}\).

2. Encrypt the plaintext \(P_0\) under each trial key \(K'\) into \(C' = E_{K'}(P_0)\).

3. If \(C'\) equals either \(C_0\) or \(\bar{C}_1\), the original key is likely to be either \(K = K'\) or \(\bar{K} = \bar{K}'\), respectively.

4. Fix \(k\) to be the output of the \(F\) function in the first round of the encryption of \(P_0\) under the key \(K'\). If \(C'_L\) equals either \(C_{0,R}\) or \(\bar{C}_{1,R}\), continue encryption of \(P_0\) with a seventeenth round (just calculate one additional round from \(C'\) using the subkey \(K_{17}'\) which can be easily derived from the key \(K'\)), and if the result \(C''\) equals \(C_{0,k}\) or \(\bar{C}_{1,k}\), then the original key is likely to be
   \(K = (\text{ROL}_2(K'_R), \text{ROL}_2(K'_L))\) or its complement, respectively.

5. Calculate one additional round backwards from \(P_0\) using the subkey \(K'_0\) which can be easily derived from the key \(K'\), and fix \(k\) to be the output of the \(F\) function in this round. If the data after the fifteenth round during the encryption of \(P_0\) under the key \(K'\) equals either \(C_{0,k}\) or \(\bar{C}_{1,k}\), the original key is likely to be
   \(K = (\text{ROR}_2(K'_R), \text{ROR}_2(K'_L))\) or its complement, respectively.

We have to show that all the keys are tried:
1. All keys of the form of \(K'\) and their complement.
2. All others are either \(\text{ROL}_2\) or \(\text{ROR}_2\) of the above (rotation in both halves of the key).

Results of the Related-Key Attacks

<table>
<thead>
<tr>
<th>Chosen Plaintext: Related Keys</th>
<th>Complexity of Attack</th>
<th>Chosen Plaintexts Required</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(1.4 \cdot 2^{53})</td>
<td>(2^{53})</td>
</tr>
</tbody>
</table>

Other known attacks

- Differential Cryptanalysis: \(2^{47}\)
- Linear Cryptanalysis: \(2^{43}\)
- Complementation Properties: \(2^{55}\)
- Exhaustive Search: \(2^{56}\)

All these attacks are independent of the number of rounds of the block ciphers.

Extensions of Related-Key Attacks

2. Attack on LOKI and generalizations (Knudsen).
3. Differential related-key attacks (Kelsey, Schneier, Wagner).
4. Related-key timing attacks (Kelsey, Schneier, Wagner).