CS5760: Cryptanalysis of DES and DES-like Iterated Cryptosystems

Gautam Singh

Indian Institute of Technology Hyderabad

February 3, 2025

Differential Cryptanalysis

1. Chosen plaintext attack.
2. Exploit XOR between plaintext pairs to find key bits.

Differential Cryptanalysis

1. Chosen plaintext attack.
2. Exploit XOR between plaintext pairs to find key bits.
3. Per DES round, XOR of respective inputs is:
   - *Linear* in expansion E to get S_E.
   - *Invariant* in key mixing with subkey S_K to get $S_I = S_E \oplus S_K$.
   - *Linear* in permutation P on S_O after S boxes.
   - *Invariant* in XOR operation connecting rounds.

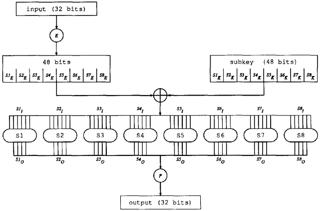

Figure 1: F function of DES.

Differential Cryptanalysis

1. Chosen plaintext attack.
2. Exploit XOR between plaintext pairs to find key bits.
3. Per DES round, XOR of respective inputs is:
    - *Linear* in expansion E to get S_E.
    - *Invariant* in key mixing with subkey S_K to get $S_I = S_E \oplus S_K$.
    - *Linear* in permutation P on S_O after S boxes.
    - *Invariant* in XOR operation connecting rounds.
4. S boxes are *nonlinear*. Probability analysis performed between input and output XOR.

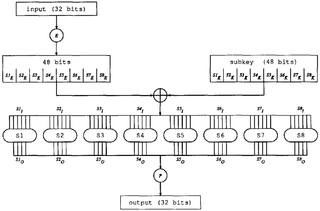

Figure 1: F function of DES.

Probability Analysis of S Boxes

1. Suppose $Si'_I = Si_I \oplus Si^*_I$ is the input XOR to the i-th S box, and Si'_O is the output XOR ($1 \leq i \leq 8$).

Probability Analysis of S Boxes

1. Suppose $Si'_I = Si_I \oplus Si^*_I$ is the input XOR to the i-th S box, and Si'_O is the output XOR $(1 \leq i \leq 8)$.
2. We create a *pairs XOR distribution table* for each S box.
   - Each entry (Si'_I, Si'_O) equals the number of 6-bit key blocks Si_K for which $Si'_I \to Si'_O$.
   - 64-by-16 joint probability mass function.

Probability Analysis of S Boxes

1. Suppose $Si'_I = Si_I \oplus Si^*_I$ is the input XOR to the i-th S box, and Si'_O is the output XOR ($1 \le i \le 8$).
2. We create a *pairs XOR distribution table* for each S box.
   - Each entry (Si'_I, Si'_O) equals the number of 6-bit key blocks Si_K for which $Si'_I \to Si'_O$.
   - 64-by-16 joint probability mass function.
3. This joint PMF can reduce the number of possible (sub)keys. Used to drive choice for the plaintext XOR.
   - $\approx 80\%$ entries are non-zero/possible for each S box (some have lesser percentages).
   - Given Si'_I and Si'_O, we can narrow down Si_K to a few possibilities.

Probability Analysis of S Boxes

1. Suppose $Si'_I = Si_I \oplus Si^*_I$ is the input XOR to the i-th S box, and Si'_O is the output XOR $(1 \leq i \leq 8)$.
2. We create a *pairs XOR distribution table* for each S box.
   - Each entry (Si'_I, Si'_O) equals the number of 6-bit key blocks Si_K for which $Si'_I \to Si'_O$.
   - 64-by-16 joint probability mass function.
3. This joint PMF can reduce the number of possible (sub)keys. Used to drive choice for the plaintext XOR.
   - $\approx 80\%$ entries are non-zero/possible for each S box (some have lesser percentages).
   - Given Si'_I and Si'_O, we can narrow down Si_K to a few possibilities.
4. i-th S box contributes probability p_i for $Si'_I \to Si'_O$.
   - For $X \to Y$ over a round, $P = \prod_i p_i$.
   - Over n rounds, $P = \prod_{i=1}^{n} P_i$.

Probability Analysis of S Boxes

1. Suppose $Si'_I = Si_I \oplus Si^*_I$ is the input XOR to the i-th S box, and Si'_O is the output XOR $(1 \le i \le 8)$.
2. We create a *pairs XOR distribution table* for each S box.
   - Each entry (Si'_I, Si'_O) equals the number of 6-bit key blocks Si_K for which $Si'_I \to Si'_O$.
   - 64-by-16 joint probability mass function.
3. This joint PMF can reduce the number of possible (sub)keys. Used to drive choice for the plaintext XOR.
   - $\approx 80\%$ entries are non-zero/possible for each S box (some have lesser percentages).
   - Given Si'_I and Si'_O, we can narrow down Si_K to a few possibilities.
4. i-th S box contributes probability p_i for $Si'_I \to Si'_O$.
   - For $X \to Y$ over a round, $P = \prod_i p_i$.
   - Over n rounds, $P = \prod_{i=1}^{n} P_i$.

Desirable for cryptanalysis: high P with large n.

Characteristic

Formalizes notion of high-probability plaintext XORs.

Definition (Characteristic)

An *n-round chracteristic* is a tuple $\Omega = (\Omega_P, \Omega_\Lambda, \Omega_T)$ where $\Omega_P = (L', R')$ and $\Omega_T = (l', r')$ are m bit numbers, $\Omega_\Lambda = (\Lambda_1, \dots, \Lambda_n)$, $\Lambda_i = (\lambda_I^i, \lambda_O^i)$ and $\lambda_I^i, \lambda_O^i, L', R', l', r'$ are $\frac{m}{2}$ bit numbers and m is the block size of the cryptosystem satisfying

$$\lambda_I^1 = R' \tag{1}$$

$$\lambda_I^2 = L' \oplus \lambda_O^1 \tag{2}$$

$$\lambda_I^n = r' \tag{3}$$

$$\lambda_I^{n-1} = l' \oplus \lambda_O^n \tag{4}$$

$$\forall\ 1 < i < n,\ \lambda_O^i = \lambda_I^{i-1} \oplus \lambda_I^{i+1} \tag{5}$$