CS5760: Topics in Cryptanalysis **2025**

Lecture 3: 22 January 2025

Instructors: Maria Francis and M. V. Panduranga Rao *Scribe: Gautam Singh*

3.1 Cryptanalysis of DES Reduced to 8 Rounds

DES reduced to 8 rounds uses a 5-round characteristic with probability approximately $\frac{1}{10486}$ as shown in Figure 3.1.

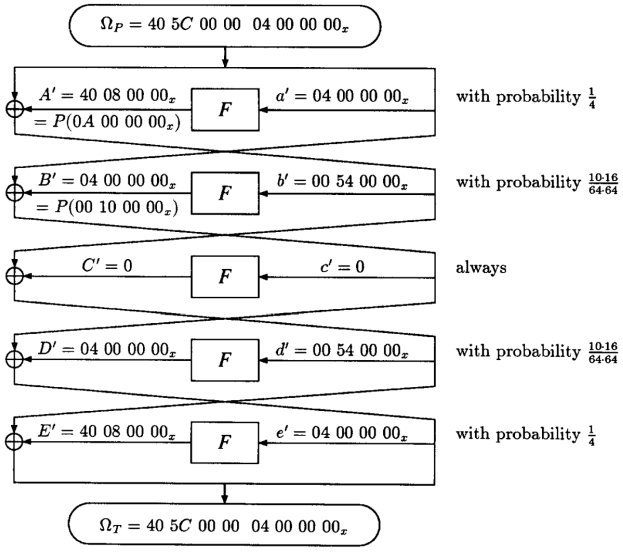

Figure 3.1: 5 round characteristic used to cryptanalyze DES reduced to 8 rounds.

From the characteristic, it is evident that

$$f' = d' \oplus E' = b' \oplus A' = L' = \texttt{40 5C 00 00}. \tag{3.1}$$

Thus, for a right pair, five S boxes S2, S5, ..., S8 have zero input XORs in the sixth round. Using

$$H' = l' \oplus g' = l' \oplus e' \oplus F' \tag{3.2}$$

and the fact that $h' = r'$, we can count on $5 \cdot 6 = 30$ key bits of $K8$. The signal to noise ratio is $S/N = \frac{2^{30}}{4^5 \cdot 10486} \approx 100$. However, due to the large memory requirement of 2^{30} locations, we count on fewer key bits. Further, due to the small probability of the characteristic, we require many plaintexts, which makes the clique method slow. Notice that each S box discards 20 % of wrong pairs. Thus, counting on 24 key bits has $S/N = \frac{2^{24}}{4^4 \cdot 0.8 \cdot 10486} \approx 7.8$ and counting on 18 key bits has $S/N = \frac{2^{18}}{4^3 \cdot 0.8^2 \cdot 10486} \approx 0.6$.

3.1.1 Modifying the Characteristic

By reducing the number of key bits to count, we can also choose which key bits are to be counted in order to improve the signal to noise ratio. Notice that

$$e' = \texttt{04 00 00 00} \rightarrow E' = P(\texttt{0W 00 00 00}) = \texttt{X0 0Y Z0 00} \tag{3.3}$$

where $W \in \{0, 1, 2, 3, 8, 9, A, B\},\ X, Z \in \{0, 4\},\ Y \in \{0, 8\}$. Hence, we have $f' = d' \oplus E' = \texttt{X0 5V Z0 00}$ where $V = Y \oplus 4$. If $Z = 0$, then necessarily $E' = \texttt{40 08 00 00}$ and this happens with probability $\frac{16}{64}$. All other combinations involving $Z = 4$ occur with probability $\frac{20}{64}$.

Although we cannot count on $S5_{Kh}$, one can check $S5'_{Eh} \rightarrow S5'_{Oh}$ which is satisfied by approximately 80 % of the pairs. Thus, the modified probability of $e' \rightarrow E'$ is $\frac{16}{64} + 0.8\frac{20}{64} = \frac{1}{2}$. This doubles the probability of the characteristic Ω_P to $\frac{1}{5243}$ and consequently doubles the S/N for counting on 24 bits and 18 bits of $K8$ to 15.6 and 1.2 respectively.