Using propagation ratios:

Much like linear cryptanalysis, we want to create a chain—a differential trail—through the network.

We can then (unjustifiably) assume independence between the propagation ratios (Rp values), multiplying them to determine the ratio for the entire trail.

Example: Continuing with our TTS and TTP values from earlier.

Select some ratios to make a trail:

\[
\begin{align*}
S_1' : & \quad Rp(0101, 0010) = \frac{1}{2} \\
S_2' : & \quad Rp(0100, 0110) = \frac{3}{8} \\
S_3 : & \quad Rp(0100, 0101) = \frac{3}{8} \\
S_4 : & \quad Rp(0010, 0101) = \frac{3}{8}
\end{align*}
\]

Draw the trail:

Combine ratios:

\[
Rp(0000, 1011, 0000, 0000, 0101, 0101, 0000) = \frac{1}{2} \times \left(\frac{3}{8}\right)^3 = \frac{27}{1024}
\]

From the network:

\[
x' = 0000, 1011, 0000 \quad \Rightarrow (v^3)' = 0000, 0101, 0101, 0000
\]

Pass through TTP:

\[
(v^3)' = 0000, 0101, 0101, 0000 \quad \Rightarrow (w^4)' = 0000, 0110, 0110, 0000
\]

So:

\[
x' = 0000, 1011, 0000 \quad \Rightarrow (w^4)' = 0000, 0110, 0110, 0000
\]

with \( Pr((w^4)' \mid x') = \frac{27}{1024} \)
The differential attack:

Let \( T \) be a set of 4-tuples \( \{(x, x', y, y')\} \) for a fixed \( x' \).

- Tuples for which:

  - A useful observation:
    - Recall that:
      \[
      u^{(i)} = w^{(i)} \oplus k^{(i)} \implies \hat{u}^{(i)} = \bar{w}^{(i)} \oplus \bar{k}^{(i)}
      \]

    So, the input xor for \( S^i \):
    \[
    \hat{u}^{(i)} \oplus \bar{\hat{u}}^{(i)} = (\bar{w}^{(i)} \oplus \bar{k}^{(i)}) \oplus (\bar{w}^{(i)} \oplus \bar{k}^{(i)})
    \]
    \[
    = \bar{w}^{(i)} \oplus \bar{w}^{(i)}
    \]

    That is, the input xor to each S-box in the differential trail is independent of the subkey bits.

- Again, we will focus on candidate subkeys (2^8 of them) for half of \( K \).
  - Initialize a count for each subkey to 0.

- Filter the set \( T \) to eliminate members for which
  - We seek members of \( T \) for which the differential described by the trail holds: right pairs.

- We can pre-emptively prune the set of some input/output 4-tuples for which we can quickly compute that the differential will not hold. Recall that, at the end of the trail:

  \[
  (u^{(i)})' = (u^{(i)})' = 0000
  \]
\[ x' = 0000 \implies \Delta(x') = \{(0000, 0000), (0001, 0001), (0010, 0010), \ldots, (1111, 1111)\} \]

\[ \implies x' = \{(1110, 1110), (0010, 0010), \ldots, (0110, 0110)\} \]

\[ \implies H_{1/2} : y' = T_{1/2}(x'), \hat{y}' = T_{1/2}(x): y' = 0000 \]

Therefore, \( (u_{11})' = (u_{33})' = 0000 \implies (v_{11})' = (v_{33})' = 0000 \)

Recall our critical observation about subkey bits:

\[ y(i)' = y(i) \oplus \hat{y}(i)' = (v_{(i)}' \oplus k_{(i)}^5) + (\hat{v}_{(i)}' \oplus k_{(i)}^5) \]

\[ = v_{(i)}' \oplus \hat{v}_{(i)}' \]

\[ \implies \hat{v}_{(i)}' = (v_{(i)}')' \]

Therefore:

\[ (v_{(i)}')' = (v_{(3)}')' = 0000 \implies \hat{y}_{(i)} = \hat{y}_{(i)}' \text{ and } \hat{y}_{(3)} = \hat{y}_{(3)}' \]

\[ \implies 8 y(i)' = y(3)' = 0000 \]

\[ \implies y(i)' = \hat{y}(i)' \text{ and } y(3)' = \hat{y}(3)' \]

Thus, if either of these equalities does not hold, we discard the tuple from \( T_2 \) to get \( T_2' \).

\[ \implies \text{For each } (x, x', y, y') \in T_2', \text{ try each possible subkey:} \]

\[ \implies \text{Partially decrypt } y, \hat{y} \text{ for both } y \rightarrow u, \hat{y} \rightarrow \hat{u}. \]

\[ \implies \text{Calculate } (u')' = u + \hat{u}. \]

\[ \implies \text{If } (u_{11})' = u_{13}' = 00110 \implies \text{increment count for that subkey.} \]

\[ \text{The subkey w/ maximum count is correct!} \]