# 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 is invariant under:
   - Expansion $E$ to get $S_E$.
   - Key mixing with subkey $S_K$ to get $S_I = S_E \oplus S_K$.
   - Permutation on $S_O$ after S boxes.

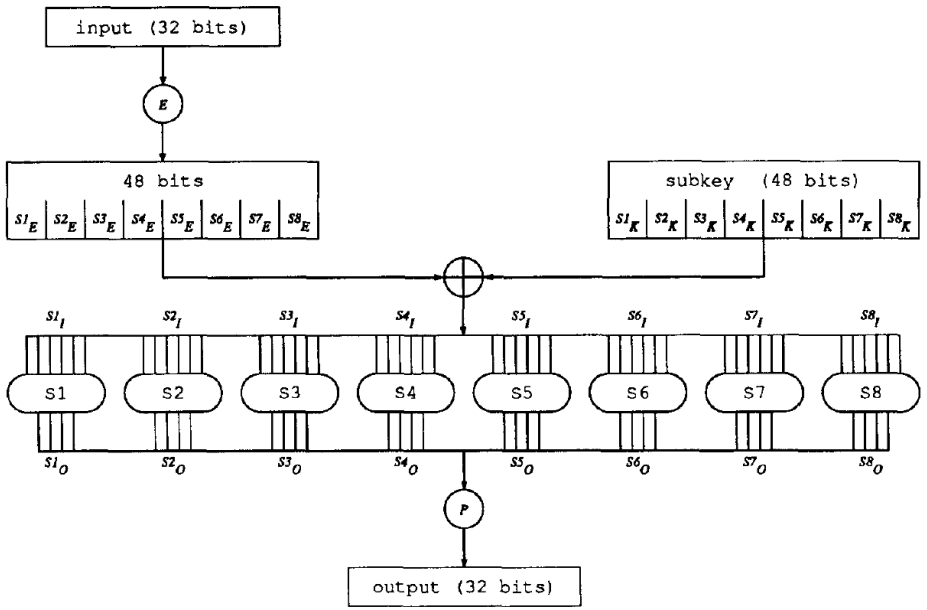


Figure 1: $F$ function of DES.

# Differential Cryptanalysis

1. Chosen plaintext attack.
2. Exploit XOR between plaintext pairs to find key bits.
3. Per DES round, XOR is invariant under:
   - Expansion $E$ to get $S_E$.
   - Key mixing with subkey $S_K$ to get $S_I = S_E \oplus S_K$.
   - Permutation on $S_O$ after S boxes.
4. S boxes are *nonlinear*. Probability analysis performed on XOR of S box inputs and outputs.

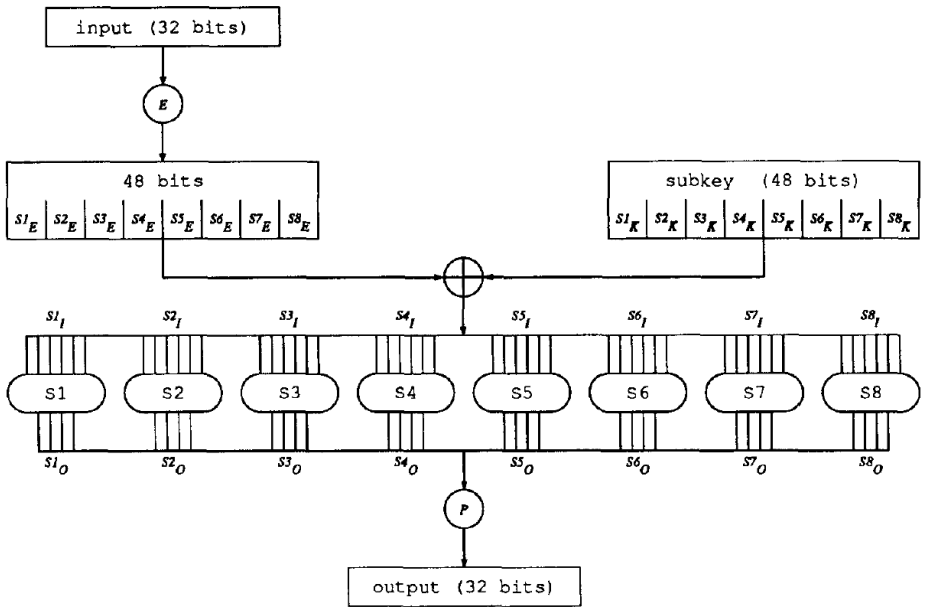


Figure 1: $F$ function of DES.