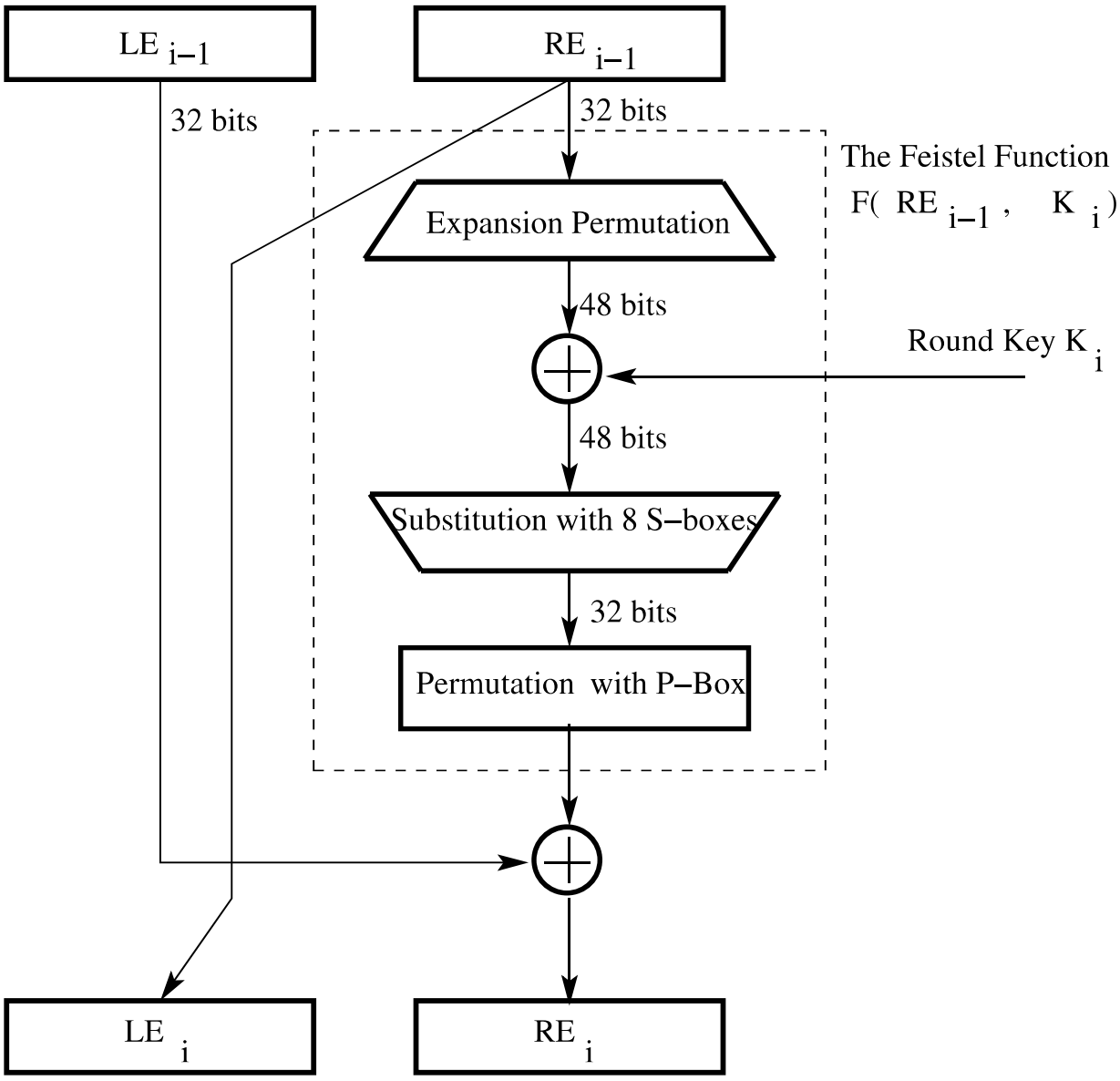

Figure 4: *One round of processing in DES.* (*This figure is from Lecture 3 of "Lecture Notes on Computer and Network Security" by Avi Kak*)

Back to TOC

3.3.2 The S-Box for the Substitution Step in Each Round

- As shown in Figure 5, the 48-bit input word is divided into eight 6-bit words and each 6-bit word fed into a separate S-box. Each S-box produces a 4-bit output. Therefore, the 8 S-boxes together generate a 32-bit output. As you can see, the overall substitution step takes the 48-bit input back to a 32-bit output.

- Each of the eight S-boxes consists of a 4×16 table lookup for an output 4-bit word. The first and the last bit of the 6-bit input word are decoded into one of 4 rows and the middle 4 bits decoded into one of 16 columns for the table lookup.

- The goal of the substitution carried out by an S-box is to enhance **diffusion**, as mentioned in the previous subsection. As you will recall from the E-step described in Section 3.3.1, the expansion-permutation step (the E-step) expands a 32-bit block into a 48-bit block by attaching a bit at the beginning and a bit at the end of each 4-bit sub-block, the two bits needed for these attachments belonging to the adjacent blocks.

- Thus, the row lookup for each of the eight S-boxes becomes a

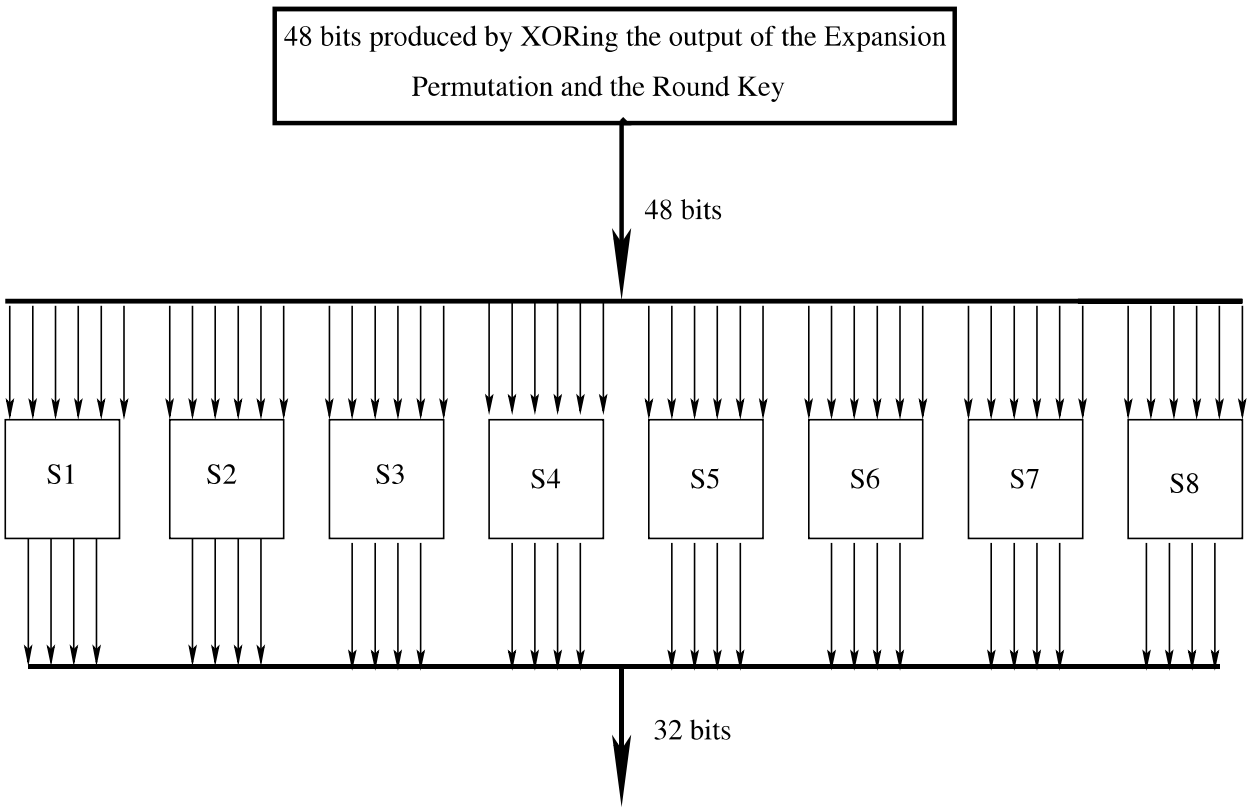

Figure 5: *The 48 bits coming out of the expansion permutation are first XORed with the round key and then, as shown, fed into the 8 S-boxes of DES.* (*This figure is from Lecture 3 of "Lecture Notes on Computer and Network Security" by Avi Kak*)

function of the input bits for the previous S-box and the next S-box.

- In the design of the DES, the S-boxes were tuned to enhance the resistance of DES to what is known as the **differential cryptanalysis attack**, or, sometimes more briefly as **differential attack**. [As will be explained in much greater detail (and also demonstrated) in Section 8.9 of Lecture 8, differential cryptanalysis of block ciphers consists of presenting to the encryption algorithm pairs of plaintext bit patterns with known differences between them and examining the differences between the corresponding cyphertext outputs. The outputs are usually recorded at the input to the last round of the cipher. Let's represent one plaintext bit block by $X = [X_1, X_2, ..., X_n]$ where X_i denotes the i^{th} bit in the block, and let's represent the corresponding output bit block by $Y = [Y_1, Y_2, ..., Y_n]$. By the difference between two plaintext bit blocks X' and X'' we mean $\Delta X = X' \oplus X''$. The difference between the corresponding outputs Y' and Y'' is given by $\Delta Y = Y' \oplus Y''$. The pair $(\Delta X, \Delta Y)$ is known as a **differential**. In an ideally randomizing block cipher, the probability of ΔY being a particular value for a given ΔX is $1/2^n$ for an n-bit block cipher. What is interesting is that the probabilities of ΔY taking on different values for a given ΔX can be shown to be independent of the encryption key because of the properties of the XOR operator, but these probabilities are strongly dependent on the S-box tables. By feeding into a cipher several pairs of plaintext blocks with known ΔX and observing the corresponding ΔY, it is possible to establish constraints on the round key bits encountered along the different paths in the encryption processing chain. (By constraints I mean the following: Speaking hypothetically for the purpose of illustrating a point and focusing on just one round of DES, suppose we can show that the following condition can be expected to be obeyed with high probability: $\Delta X_i \oplus \Delta Y_i \oplus K_i = 0$ for some bit K_i of the encryption key, then it must be the case that $K_i = \Delta X \oplus \Delta Y$.) Note that differential cryptanalysis is a **chosen plaintext attack**, meaning that the attacker will feed known plaintext bit patterns into the cipher and analyze the corresponding outputs in order to figure out the encryption