In cryptography, an **SP-network**, or **substitution-permutation network** (SPN), is a series of linked mathematical operations used in block cipher algorithms such as AES (Rijndael).

Such a network takes a block of the plaintext and the key as inputs, and applies several alternating "rounds" or "layers" of substitution boxes (S-boxes) and permutation boxes (P-boxes) to produce the ciphertext block. The S-boxes and P-boxes transform (sub-)blocks of input bits into output bits. It is common for these transformations to be operations that are efficient to perform in hardware, such as exclusive or (XOR) and bitwise rotation. The key is introduced in each round, usually in the form of "round keys" derived from it. (In some designs, the S-boxes themselves depend on the key.)

Decryption is done by simply reversing the process (using the inverses of the S-boxes and P-boxes and applying the round keys in reversed order).

An **S-box** substitutes a small block of bits (the input of the S-box) by another block of bits (the output of the S-box). This substitution should be one-to-one, to ensure invertibility (hence decryption). In particular, the length of the output should be the same as the length of the input (the picture on the right has S-boxes with 4 input and 4 output bits), which is different from S-boxes in general that could also change the length, as in DES (Data Encryption Standard), for example. An S-box is usually not at all just a permutation of the bits. Rather, a good S-box will have the property that changing one input bit will change about half of the output bits (or an avalanche effect). It will also have the property that each output bit will depend on every input bit.

A **P-box** is a permutation of all the bits: it takes the outputs of all the S-boxes of one round, permutes the bits, and feeds them into the S-boxes of the next round. A good P-box has the property that the output bits of any S-box are distributed to as many S-box inputs as possible.

At each round, the **round key** (obtained from the key with some simple operations, for instance, using S-boxes and P-boxes) is combined using some group operation, typically XOR.

A single typical S-box or a single P-box alone does not have much cryptographic strength: an S-box could be thought of as a substitution cipher, while a P-box could be thought of as a transposition cipher. However, a well-designed SP network with several alternating rounds of S- and P-boxes already satisfies Shannon's **confusion and diffusion properties**:

- The reason for **diffusion** is the following: If one changes one bit of the plaintext, then it is fed into an S-box, whose output will change at several bits, then all these changes are distributed by the P-box among several
S-boxes, hence the outputs of all of these S-boxes are again changed at several bits, and so on. Doing several rounds, each bit changes several times back and forth, therefore, by the end, the ciphertext has changed completely, in a pseudorandom manner. In particular, for a randomly chosen input block, if one flips the $i$-th bit, then the probability that the $j$-th output bit will change is approximately a half, for any $i$ and $j$, which is the Strict Avalanche Criterion.

- The reason for confusion is exactly the same as for diffusion: changing one bit of the key changes several of the round keys, and every change in every round key diffuses over all the bits, changing the ciphertext in a very complex manner. Vice versa, changing one bit in the ciphertext will change the key completely.

Although a Feistel network that uses S-boxes (such as DES) is quite similar to SP networks, there are some differences that make either this or that more applicable in certain situations. For a given amount of confusion and diffusion, an SP network has more "inherent parallelism"[1] and so — given a CPU with a large number of execution units — can be computed faster than a Feistel network. [2] CPUs with few execution units — such as most smart cards — cannot take advantage of this inherent parallelism.

References
