2.4 SP Networks

In an ideal world we would know how to reliably measure the security of a bitblock cipher

$$F\colon \mathbb{F}_2^n \times \mathbb{F}_2^l \longrightarrow \mathbb{F}_2^n$$

for realistic values of the block length n and the key length l, say of an order of magnitude of 128 bits or more.

In fact we know explicit measures of security, for example the linear potential, or the differential potential, that quantify the deviation from linearity, or the algebraic immunity, or others. Unfortunately all of these only give necessary, not sufficient, conditions for security, and moreover the efficient computability of these measures is limited to small block lengths n, about 8 or slightly larger.

Lacking a general efficient approach to security the design of bitblock ciphers usually relies on a structure that, although not obligatory, in practice seems to provide plausible security according to verifiable criteria. Most of the generally approved standard ciphers, such as DES and AES, follow this approach.

Rounds of Bitblock Ciphers

This common design scheme starts by constructing Boolean maps of small dimensions and then extending them to the desired block length in several steps:

1. Define one or more Boolean maps of small dimension q (= block length of the definition domain), say $q = 4$, 6, or 8, that are good for several security criteria. These maps are called **S-boxes** (“S” stands for Substitution), and are the elementary building blocks of the cipher.

2. Mix the round input with some of the key bits and then apply m S-boxes in parallel (or apply the one S-box m times in parallel) to get a map with the desired input width $n = mq$.

3. Then permute the complete resulting bitblock over its total width.

4. These steps together are a **“round”** of the complete scheme. Asset the weaknesses of the round map, that mainly result from using S-boxes of small dimension. Then reduce these weaknesses in a reasonably controlled way by iterating the scheme over several rounds of the same structure but with a changing choice of key bits.

5. Don’t stop as soon as the security measures give satisfying values but add some surplus rounds to get a wide security margin.

Figure 2.1 outlines the scheme for a single round.

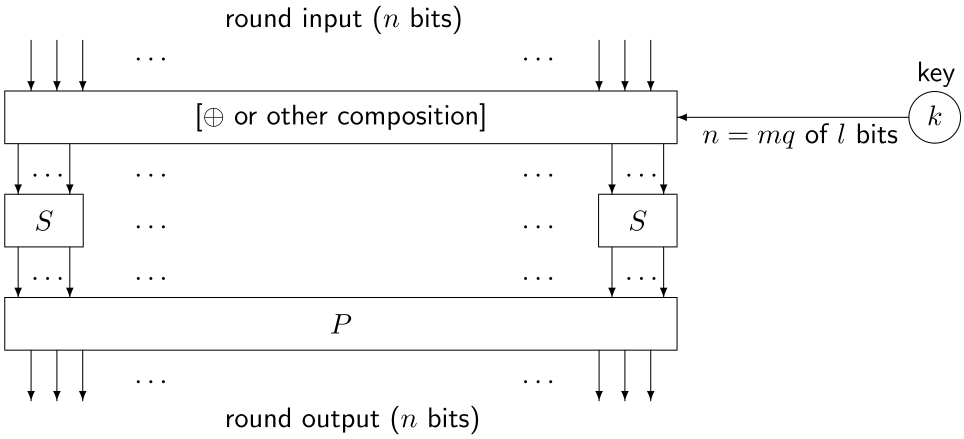

Figure 2.1: A single round of a bitblock cipher (S is a, maybe varying, S-box, P, a permutation, k, the key)

Shannon's Design Principles

The complete scheme is a special case of a somewhat more general proposal that goes back to Shannon who required two basic features of block ciphers:

Diffusion The bits of the plaintext block "smear" over all parts of the block. This is done by applying permutations (a. k. a. as transpositions).

Confusion (complex dependencies) The interrelation between plaintext block and key on the one hand, as well as ciphertext block on the other hand should be as complex as possible (in particular as nonlinear as possible). Basic building blocks for this are substitutions.

The overall effect of both requirements, taken together, should result in an unforeseeable change of ciphertext bits for a slight change of the key.

> *The attacker should have no means to recognize whether a guessed key is "nearly correct".*

Product Ciphers after Shannon

For the construction of strong block ciphers Shannon proposed an alternating sequence of **S**ubstitutions and transpositions (= **P**ermutations), so-called **SP-networks**:

$$\mathbb{F}_2^n \xrightarrow{S_1(\bullet,k)} \mathbb{F}_2^n \xrightarrow{P_1(\bullet,k)} \mathbb{F}_2^n \longrightarrow \ldots$$
$$\ldots \longrightarrow \mathbb{F}_2^n \xrightarrow{S_r(\bullet,k)} \mathbb{F}_2^n \xrightarrow{P_r(\bullet,k)} \mathbb{F}_2^n$$

depending on a key $k \in \mathbb{F}_2^l$. In this scheme

$$\begin{aligned} S_i &= i\text{-th substitution} \\ P_i &= i\text{-th permutation} \\ P_i \circ S_i &= i\text{-th } \textbf{round} \end{aligned}$$

Alltogether the encryption function consists of r rounds.

Example: Lucifer I (Feistel 1973)

Note that the permutations are special linear maps $P\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^n$. Some recent bitblock ciphers, the most prominent being AES, replace permutations by more general linear maps that provide an even better diffusion. However the proper term **"LP-network"** is not yet in use.