2.5 Feistel Networks

Horst Feistel was the first (in the open world) who explicitly applied Shannon's design principles when he constructed the Lucifer ciphers.

The Kernel Map

Assume the blocksize is even: $n = 2s$. Decompose blocks $a \in \mathbb{F}_2^n$ into their left and right halves:

$$a = (L, R) \in \mathbb{F}_2^s \times \mathbb{F}_2^s$$

(We use uppercase letters to avoid confusion with the dimension l of the keyspace.) Moreover we have to agree on the order of the bits in a block:

- The **natural order** has the LSB (Least Significant Bit) always at the right end and assigns it the index 0, the MSB (Most Significant Bit) at the left end with index $n-1$:

  $$b = (b_{n-1}, \ldots, b_0) \in \mathbb{F}_2^n.$$

  This corresponds to the base 2 representation of natural numbers in the integer interval $[0 \ldots 2^n[$:

  $$b_{n-1} \cdot 2^{n-1} + \cdots + b_1 \cdot 2 + b_0 \in \mathbb{N}$$

  This is the order we use in most situations.

- The **IBM order** has the bits in reverse (LSB at left, MSB at right) and assigns them the indices 1 to n:

  $$a = (a_1, \ldots, a_n) \in \mathbb{F}_2^n.$$

  This corresponds to the usual indexing of the components of a vector. Sometimes, in exceptional cases, the indices 0 to $n-1$ are used.

The elemantery building blocks of a Feistel cipher are represented by a **kernel map**

$$f \colon \mathbb{F}_2^s \times \mathbb{F}_2^q \longrightarrow \mathbb{F}_2^s,$$

that need not fulfill any further formal requirements. In particular we don't require that the $f(\bullet, k)$ be bijective.

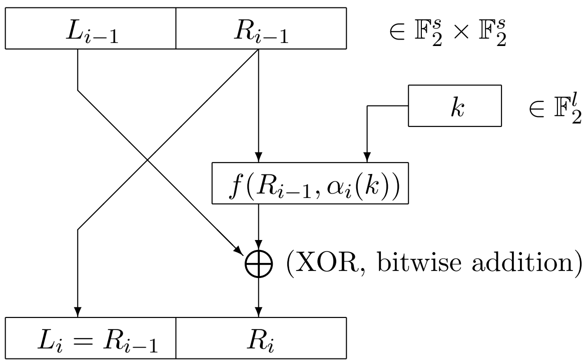
> However to get a useful cipher we should choose a kernel map f that already provides good confusion and diffusion. It should consist of a composition of substitutions and transpositions and be highly nonlinear.

Description of the Rounds

A FEISTEL cipher consists or r rounds. Each round uses a q-bit round key that is derived from the key $k \in \mathbb{F}_2^l$ by a process called the **key schedule**:

$$\alpha_i \colon \mathbb{F}_2^l \longrightarrow \mathbb{F}_2^q \quad \text{for } i = 1, \ldots, r.$$

Then round i has this form:



We recognize the autokey principle in form of the addition of the left half and the transformed right half of a bitblock.

Algorithmic Description

From the graphical description we easily derive an algorithmic description:

$$\begin{array}{lcccl}
\textbf{Input} & \longrightarrow & a & = & (a_0, a_1) \in \mathbb{F}_2^s \times \mathbb{F}_2^s \\
 & & a_2 & := & a_0 + f(a_1, \alpha_1(k)) \\
 & & & & \qquad \text{– 1st round, result } (a_1, a_2) \\
 & & \vdots & & \vdots \\
 & & a_{i+1} & := & a_{i-1} + f(a_i, \alpha_i(k)) \\
 & & & & \qquad \text{– } i\text{-th round, result } (a_i, a_{i+1}) \\
 & & & & \qquad \text{– } [a_i = R_{i-1} = L_i,\ a_{i+1} = R_i] \\
 & & \vdots & & \vdots \\
\textbf{Output} & \longleftarrow & c & = & (a_r, a_{r+1}) =: F(a, k)
\end{array}$$

Decryption

The decryption is done by the formula

$$a_{i-1} = a_{i+1} + f(a_i, \alpha_i(k)) \quad \text{for } i = 1, \ldots, r.$$

This boils down to the same algorithm, but the rounds in reverse order. Or in other words: The key schedule follows the reverse direction.

In particular we proved:

Theorem 3 (Feistel) *Let $F\colon \mathbb{F}_2^{2s} \times \mathbb{F}_2^l \longrightarrow \mathbb{F}_2^{2s}$ be the block cipher with kernel map $f\colon \mathbb{F}_2^s \times \mathbb{F}_2^q \longrightarrow \mathbb{F}_2^s$ and key schedule $\alpha = (\alpha_1, \ldots, \alpha_r)$, $\alpha_i\colon \mathbb{F}_2^l \longrightarrow \mathbb{F}_2^q$.*

Then the encryption function $F(\bullet, k)\colon \mathbb{F}_2^{2s} \longrightarrow \mathbb{F}_2^{2s}$ is bijective for every key $k \in \mathbb{F}_2^l$.

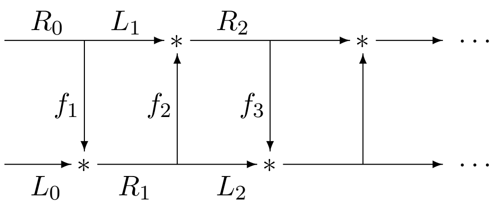
Addendum. *Decryption follows the same algorithm with the same kernel map f but the reverse key schedule $(\alpha_r, \ldots, \alpha_1)$.*

Note When the deryption starts with $c = (a_r, a_{r+1})$, then as a first step *the two halves must be swapped* because the algorithm starts with (a_{r+1}, a_r). To simplify this, in the last round of a Feistel cipher the interchange of L and R is usually dropped.

Remarks

- If f and the α_i are linear so is F.
- Usually the α_i are only selections, hence as maps projections $\mathbb{F}_2^l \longrightarrow \mathbb{F}_2^q$.
- Other graphical descriptions of the Feistel scheme are:

a) a ladder

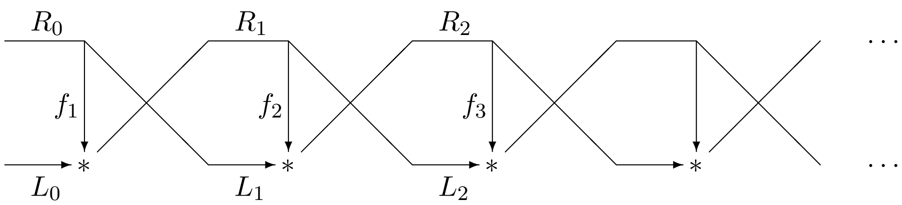


$$R_i = L_{i-1} * f_i(R_{i-1})$$

$$f_i = f(\bullet, \alpha_i(k))$$

$$L_i = R_{i-1}$$

b) a twisted ladder



Generalizations

1. Replace the group $(\mathbb{F}_2^s, +)$ by an arbitrary group $(G, *)$. Then the formulas for encryption and decryption are:

$$\begin{aligned} a_{i+1} &= a_{i-1} * f(a_i, \alpha_i(k))), \\ a_{i-1} &= a_{i+1} * f(a_i, \alpha_i(k)))^{-1}. \end{aligned}$$

2. Unbalanced FEISTEL ciphers (SCHNEIER/KELSEY): Divide the blocks into two different halves: $\mathbb{F}_2^n = \mathbb{F}_2^s \times \mathbb{F}_2^t$, $x = (\lambda(x), \rho(x))$. Then the encryption formula is:

$$\begin{aligned} L_i &= \rho(L_{i-1}, R_{i-1}) && \in \mathbb{F}_2^s, \\ R_i &= \lambda(L_{i-1}, R_{i-1}) + f(L_i, \alpha_i(k))) && \in \mathbb{F}_2^t. \end{aligned}$$

Examples

1. LUCIFER II (FEISTEL 1971, published in 1975),
2. DES (COPPERSMITH et al. for IBM in 1974, published as US standard in 1977),
3. many newer bitblock ciphers.

The usefulness of FEISTEL networks relies on the empirical observations:

- By the repeated execution through several rounds the "(s, q)-bit security" (or "local security") of the kernel map f is expanded to "(n, l)-bit security" (or "global security") of the complete FEISTEL cipher F.
- The complete cipher is composed of manageable pieces that may be "locally" optimized for security.

LUBY/RACKOFF underpinned the first of these observations by a theoretical result: A FEISTEL cipher with at least four rounds is not efficiently distinguishable from a random permutation, if its kernel map is random. This means that by FEISTEL's construction a map with good random properties but too small block length expands to a map with good random properties and sufficient block length.

> Michael LUBY, Charles RACKOFF: How to construct pseudorandom permutations from pseudorandom functions. SIAM Journal on Computing 17 (1988), 373–386

Two words of caution about the LUBY/RACKOFF result:

- It doesn't say anything about an attack with known or chosen plaintext.
- It holds for true random kernel maps. However concrete FEISTEL ciphers usually restrict the possible kernel maps to a subset defined by a choice of 2^q keys.