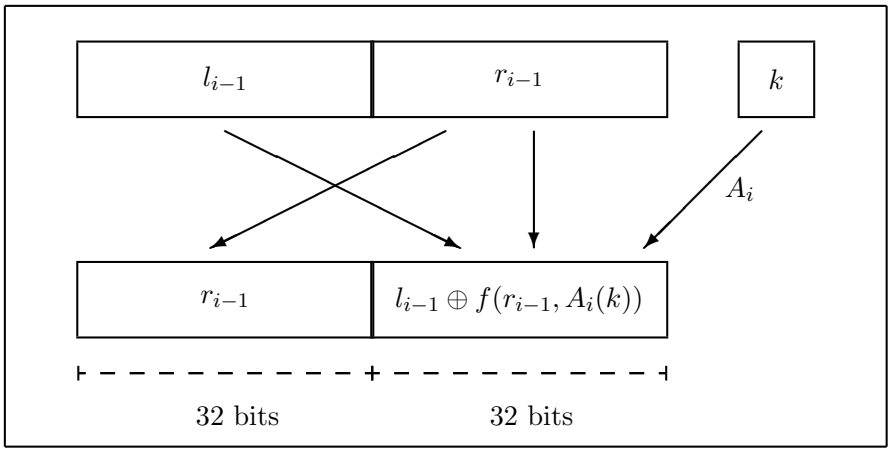
4.3 The Rounds

The 16 rounds of DES consist of maps

$$R_i \colon \mathbb{F}_2^{64} \times \mathbb{F}_2^{56} \longrightarrow \mathbb{F}_2^{64} \quad (i = 1, \ldots, 16),$$

that are defined in the following figure, using the i-th key selection

$$A_i \colon \mathbb{F}_2^{56} \longrightarrow \mathbb{F}_2^{48} \quad (i = 1, \ldots, 16).$$



The rounds only differ by their key selections $A_i(k)$. We recognize the Feistel scheme.