

### 3 Die Runden

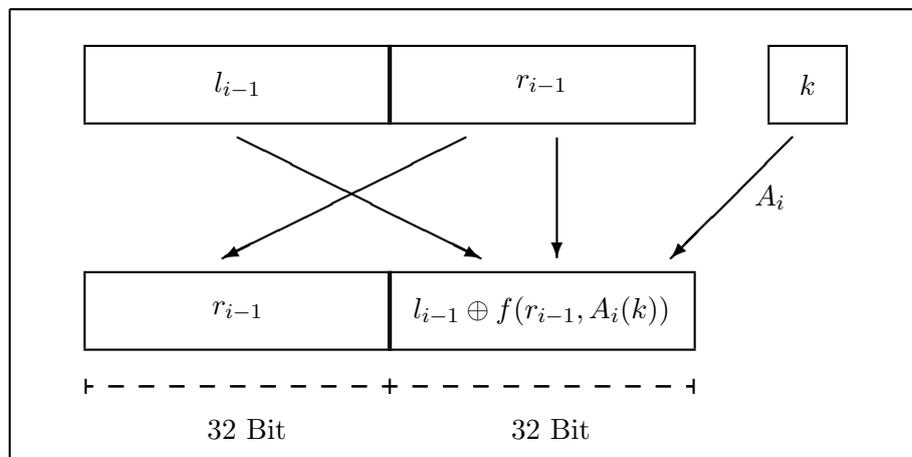
Die 16 Runden im DES bestehen aus je einer Abbildung

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

die mit Hilfe der  $i$ -ten Schlüsselauswahl

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

wie in der folgenden Abbildung beschrieben wird.



Die Runden unterscheiden sich also nur durch den verwendeten Teilschlüssel  $A_i(k)$ . Man erkennt hier das FEISTEL-Schema.