5.9 Die Idee der differenziellen Kryptoanalyse

Bei der differenziellen Kryptoanalyse wird analog zur linearen Kryptoanalyse die Approximation durch lineare Strukturen verwendet. Man betrachtet einen Differenzenvektor vor Anwendung einer Rundenabbildung und seine möglichen Werte nach Anwendung der Rundenabbildung. Zusammenpassende Folgen von Differenzenvektoren über die Runden einer iterierten Bitblock-Chiffre werden als **differenzieller Pfad** oder **Charakteristik** [Biham/Shamir 1990] bezeichnet; das Potenzial eines differenziellen Pfades ist nach Definition das Produkt der Potenziale der einzelnen Schritte. Eine **differenzielle Hülle** oder ein **Differential** [Lai/Massey/Murphy 1991] ist die Menge aller Pfade von einer gegebenen Input-Differenz der gesamten Chiffre zu einer gegebenen Output-Differenz. Es gilt eine analoge Faustregel, auf der die Methode der differenziellen Kryptoanalyse beruht:

> *Entlang eines differenziellen Pfades multiplizieren sich die differenziellen Potenziale (nach Definition). Das Potenzial einer differenziellen Hülle wird durch das Potenzial des dominanten differenziellen Pfades ausreichend approximiert.*

Dieses Potenzial wiederum ergibt die Wahrscheinlichkeit, mit der eine Gleichung für Schlüsselbits hergeleitet werden kann.