5.9 The Idea of Differential Cryptanalysis

Differential cryptanalysis has some similarities with linear cryptanalysis but instead of linear relations it uses approximations of Boolean maps by linear structures (see Appendix C). The idea is to consider a difference vector before applying a round map, and its possible values thereafter. Sequences of difference vectors that fit together over all the rounds of an iterated bitblock cipher are called a **differential path** or a **characteristic** [Biham/Shamir 1990]. The potential of a differential path is approximated by the product of the potentials of the single steps. A **differential hull** or a **differential** [Lai/Massey/Murphy 1991] is the collection of all paths between a given input difference (of the entire cipher) and a given output difference. The success of differential cryptanalysis relies on an analoguous rule of thumb:

> *Along a differential path the differential potentials are multiplicative. The potential of a differential hull is approximated by the potential of a dominant differential path.*

This potential reflects the probability for getting an equation for some key bits.