The Improbable Differential Attack: Cryptanalysis of Reduced Round CLEFIA

http://www.firstlight.cn 2010-08-08

In this paper we present a new statistical cryptanalytic technique that we call improbable differential cryptanalysis which uses a differential that is less probable when the correct key is used. We provide data complexity estimates for this kind of attacks and we also show a method to expand impossible differentials to improbable differentials. By using this expansion method, we cryptanalyze 13, 14, and 15-round CLEFIA for the key sizes of length 128, 192, and 256 bits, respectively. These are the best cryptanalytic results on CLEFIA up to this date.

存档文本