4040-849 Optimization Methods

Project Proposal

Christopher Wood

April 13, 2012

Abstract

Cryptographically secure block ciphers are based around Shannon's principles of confusion and diffusion (CITE HERE). It is important to optimize these characteristics in order to make ciphers less susceptible to linear and differential cryptanalysis. The most traditional way to integrate mathematical structures that improve the confusion of a block cipher is to use a substitution box (or simply, an S-box). Recent research efforts have revealed practical measurements of S-box constructions that indicate their susceptibility to linear and differential cryptanalysis. In this work, we attempt to formulate the problem of cryptographically strong S-box designs into an integer programming problem that can be optimized to yield the highest confusion dividends in resulting cipher implementations.

1 Problem Statement

Mathematically, a S-box can be represented as a function f that maps input values a to output values b such that $a, b \in \mathbb{F}_2^n$. In cryptographic terms, such a function f must be bijective in order to avoid bias towards any specific output element in the field.

Definition 1. Let S be an S-Box with $m = |S|$ input values. Let n be the number of elements x that satisfy $S(x \oplus \Delta_i) = S(x) \oplus \Delta_o$. Then, $\frac{n}{m}$ is the *differential probability* p of the characteristic $S_D(\Delta_i \rightarrow \Delta_o)$.

Definition 2. Branch number

Definition 3. Strict avalanche criterion