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. The Hamming weight of an element $a \in \mathbb{F}_2^n$ is defined as $\mathrm{wt}(x) = \sum x_i$.

Definition 2. The *branch number* of an $n \times n$-bit S-Box is

$$BN = \min_{a,b \neq a}(\mathrm{wt}(a \oplus b) + \mathrm{wt}(S(a) \oplus S(b))),$$

where $a, b \in \mathbb{F}_2^n$.

Definition 3. A function $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ exhibits the avalanche effect if and only if

$$\sum_{x \in \mathbb{F}_2^n} \mathrm{wt}(f(x) \oplus f(x \oplus c_i^n)) = n2^{n-1},$$

for all $i(1 \leq i \leq n)$, where $c_i^n = [0, 0, ..., 1, ..., 0]$ (where a 1 is in the nth position of the vector of cardinality n.

Definition 4. A function $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ satisfies the Strong Avalanche Critertion (SAC) if for all $i(1 \leq i \leq n)$ the following equations hold:

$$\sum_{x \in \mathbb{F}_2^n} f(x) \oplus f(x \oplus c_i^n) = (2^{n-1}, 2^{n-1}, ..., 2^{n-1})$$

This simply means that the $f(x) \oplus f(x \oplus c_i^n)$ is balanced for every element in $\mathbb{F}_2^n$ with Hamming distance of 1.

Ideal construction of cryptographic primitives will utilize internal boolean functions that satisfy the SAC criterion because they result in high levels of confusion, thus thwarting attempts by an attacker to statistically relate the ciphertext of a cipher to the key that was used for encryption or decryption. However, in order to prevent differential cryptanalysis attacks, it is important that these boolean functions also have a high branch number (CITE PAPER ABOVE).

(CITE 65,66 from thesis below) Strong S-Boxes also exhibit strong non-linearity properties. It has been shown by Rueppel that the nonlinearity of a boolean function can be measured by the Hamming distance to the set of affine transformations and is related to the Walsh transform $\hat{F}$ of $\hat{f} : \mathbb{F}_2^n \to \{-1, 1\}$ according to:

$$\delta(f) = 2^{n-1} - \frac{1}{2}\text{max}_w|\hat{F}(w)|,$$

where $\hat{F}(w)$ is the Walsh transformation defined as follows:

$$W_f(a) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+<a,x>},$$

where $< a, x >$ is the scalar product of a and x (if they are thought of as vectors).

It is easy to see that satisfaction of the SAC criterion for a boolean function, improving its branch number, and improving its non-linearity are not mutually exclusive tasks. Therefore, it is natural to reduce the problem of finding an optimal S-Box design based on these conditions to an integer programming problem that seeks to optimize each one of these construction dimensions.

TODO: continue