4040-849 Optimization Methods

Project Proposal: Optimizing Boolean Function Constructions

Christopher Wood

April 14, 2012

Abstract

Cryptographically secure block ciphers are based around Shannon's principles of confusion and diffusion [1]. 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, an 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. We now present a series of definitions that are pertinent to the design of cryptographically strong S-Boxes [2].

Definition 1. The Hamming weight of an element $a \in \mathbb{F}_2^n$ is defined as $\text{wt}(x) = \sum x_i$.

Definition 2. 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 3. The *branch number* of an $n \times n$-bit S-Box is

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

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

Definition 4. A function $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ exhibits the avalanche effect if and only if

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

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 5. 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.

Strong S-Boxes also exhibit strong non-linearity properties [1]. 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, minimizing its differential propagation probability, 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.

In this work we will seek to abstract the construction of S-Boxes away from the Boolean functions that they represent and optimize the representation of this function in order to achieve ideal values for aforementioned metrics. In other words, we focus on the construction of a function f with finite domain and range (both of the same cardinality) that could potentially be realized by a mathematical operation or construction. Only the forward version of f shall be considered in this construction. However, in practical settings, f must be invertible to be applied in symmetric key cryptosystems.

References

[1] K. Kim, "A study on the construction and analysis of substitution boxes for symmetric cryptosystems," 1990.

[2] P. P. Mar and K. M. Latt, "New analysis methods on strict avalanche criterion of s- boxes."