4040-849 Optimization Methods

Optimizing Cryptographic Boolean Function Constructions

Christopher Wood

April 15, 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 attacks. 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 (and subsequently, any confusion layer design) into an integer programming problem that can be optimized to yield the highest confusion dividends in resulting cipher implementations.

1 Problem Description and Background Information

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 (or confusion layers) [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 f be a bijective function with range $\mathbb{R}^*$, where $|\mathbb{R}^*| = m$. Let n be the number of elements x that satisfy $f(x \oplus \Delta_i) = f(x) \oplus \Delta_o$. Then, $\frac{n}{m}$ is the *differential probability* p of the characteristic $f_D(\Delta_i \to \Delta_o)$.

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 $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ 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).

Designers of cryptographically secure cryptographic primitives (e.g. block ciphers, hash functions, etc) use these measurements as a basis for their susceptibility to linear and differential cryptanalysis when constructing their algorithms. However, they place the additional constraint on such primitives that fast and simple mathematical operations must be used to emulate a bijective function f that exhbits ideal properties for all of these values.

As previously mentioned, S-Boxes have been the primary source of confusion in most cryptographic primitives. However, some recently proposed cryptographic primitives (e.g. the Skein hash function [3]) are making use of an ARX (Addition, Rotation, and XOR) layer to provide similar results. This design decision was driven by the lack of strict security proofs for S-Boxes and the implementation efficiency of the ARX design. However, at an abstract level, an ARX layer can be represented by a bijective function f as well, thus making it applicable to this problem. However, because the security of ARX confusion layers is not well understood and has only recently faced considerable cryptanalysis research [4], we restrict ourselves to S-Box designs.

2 Optimization Candidate Description

Cryptographically secure primitives utilize confusion layers that offer the following characteristics:

1. Low differential propagation probability
2. High branch number
3. Satisfaction of the SAC criterion
4. High degree of non-linearity

Therefore, it is natural to reduce the problem of finding an optimal confusion layer for cryptographic primitives to an integer programming problem that seeks to optimize each one of these construction dimensions. In other words, optimal confusion layer construction can be thought of an integer programming problem with multiple cost functions that share a single, balanced solution. The common solutions to these objectives (if they exist) are thus contained within the Pareto set for the problem.

In this work we will seek to abstract the construction of confusion layers 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.

Therefore, the design variables pair-wise mappings of the bijective function f. In order to manage the complexity of the problem, only 4-bit layers will be considered (i.e. $|\mathbb{R}^*| = 2^4 = 16$).

3 Programming Language Use

The Optimization Toolkit will be utilized in conjunction with MatLab in order to perform the mathematical computations. In addition, Mathematica will be utilized to allow for easy data collection management and visualization during the course of the project.

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.”

[3] N. Ferguson, S. Lucks, B. Schneier, D. Whiting, M. Bellare, T. Kohno, J. Callas, and J. Walker, "The skein hash function family," 2009.

[4] D. Khovratovich and I. Nikolić, "Rotational cryptanalysis of arx," in *Proceedings of the 17th international conference on Fast software encryption*, ser. FSE'10. Berlin, Heidelberg: Springer-Verlag, 2010, pp. 333–346. [Online]. Available: http://dl.acm.org/citation.cfm?id=1876089.1876116