4040-849 Optimization Methods

Optimizing Cryptographic Strength of Substitution Layers in Symmetric-Key Cryptosystems

Christopher Wood

April 18, 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 a mixed integer programming problem that can be optimized to yield the high diffusion and confusion dividends in resulting cipher implementations.

1 Block Cipher Security and Linear Cryptanalysis

Ever since the application of linear cryptanalysis on the FEAL and DES block ciphers in the early ninties, nonlinearity has become a essential characteristic of any secure symmetric-key cryptographic algorithm design (especially block ciphers) [2]. Linear cryptanalysis is a cryptanalytic attack that attempts to take advantage of high probability occurrences of linear expressions involving plaintext bits, ciphertext bits, and subkey bits. Mathematically, the attack is based on the idea of approximating the operation of a portion of the block cipher in question with an expression that is linear in terms of the bits of the inputs (X) and outputs (Y) involved, as shown below [2]:

$$X_{i_1} \oplus X_{i_2} ... \oplus X_{i_r} \oplus Y_{j_1} \oplus Y_{j_2} ... \oplus Y_{j_s} \oplus = 0$$

Using this expression, attackers can guage the amount of randomness introduced by the cipher. That is, if such an expression occurrs frequently with a relatively high probability, then we know that the probability of the expression holding for any two values $a, b \in \mathbb{F}_2^n$ is approximately $\frac{1}{2}$. However, when this probability shifts away from $\frac{1}{2}$, the amount of known plaintexts required to determine the key (or key block) that was used to reproduce the output goes down dramatically. Thus, such a deviation from the expected probability of $\frac{1}{2}$ for any expression of the form above, which is referred to as the *linear bias*, determines the susceptibility of the block cipher to known plaintext attacks. Consequently, it is important to introduce a great deal of nonlinearity into the block cipher in order to thwart such attacks.

In traditional block ciphers based on substitution-permitatuon networks (such as the DES and AES), the S(ubstitution)-box is the primary source of nonlinearity that is designed to thwart such cryptanalysis attacks. An S-box is a bijective function f defined over $\mathbb{F}_2^n$ that maps elements in its domain to distinct elements in the range. Rijndael, the AES algorithm, was selected as the finalist in the AES competition due to its simplistic design, implementation metrics, and strong security properties. Perhaps the most notable element of its security is the S-box design it uses to achieve nonlinearity. Mathematically, the substitution of a single element $a \in \mathbb{F}_2^n$ is computed by performing an affine transformation on a^{-1} (the multiplicative inverse of a). The affine transformation was carefully constructed to yield high resistance against known cryptanalytic attacks of the time, including both linear and differential cryptanalysis [3].

S-boxes are not the only proposed source of nonlinearity, however. One other notable deisgn technique is based on the notion of modular (2^n) addition, bit-wise rotation, and XOR operations. Separate, these simple routines are very easy to invert and fit to a linear model. However, when brought together in the right way using information from the secret key as an operand, an artificial degree of nonlinearity begins to emerge in the result. Threefish, the block cipher inside Skein (one of final candidates for the SHA-3 hash function competition), relies on the ARX operation for nonlinear behavior between rounds of the cipher. However, such designs are also susceptible to similar cryptanalytic attacks, as was shown in [4]. Therefore, the focus and scope of this project will be geared towards S-box design due to its simplicity and cryptographic maturity.

Linear cryptanalysis is not the only attack that threatens existing block ciphers. Differential cryptanalysis is a very powerful attack technique that attempts to break symmetric key ciphers by exploiting high probability of certain occurrences of plaintext differences and ciphertext differences[2].

2 Cryptographic Strength

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 (and any confusion layer) [5].

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. 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

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

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 *Strict 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.

Definition 6. TODO: define nonlienarity measurement here

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

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.

3 Optimization Candidate Description

Cryptographically secure primitives utilize diffusion and confusion layers that provide 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. $|\mathbb{R}^*| = 2^4 = 16$).

4 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] H. M. Heys, "A tutorial on linear and differential cryptanalysis," Tech. Rep., 2001.

[3] J. Daemen and V. Rijmen, *The design of Rijndael: AES — the Advanced Encryption Standard*. Springer-Verlag, 2002.

[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

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

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