4040-849 Optimization Methods

Optimizing Cryptographic Strength of Substitution Layers in Symmetric-Key Cryptosystems

Christopher Wood

May 9, 2012

Abstract

The cryptographic security of symmetric-key block ciphers and other related primitives is based upon their adherence to Shannon's principles of confusion and diffusion [**?**]. Confusion can be defined as the statistical relationship between the ciphertext and private key of a cipher, while diffusion refers to the statistical redundancy of plaintext bits in the ciphertext bits. Consequently, it is increasingly important to optimize these characteristics in order to make them less susceptible to attacks based on linear and differential cryptanalysis. S(ubstitution)-boxes are the most traditional mathematical structures that are used to improve the levels of diffusion and confusion within symmetric-key cryptographic algorithms. 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 substitution layers in symmetric-key block ciphers with S-box designs into a mixed integer programming problem that can be optimized to yield the high diffusion and confusion dividends in resulting cipher implementations.

1 Problem Description

Cryptographic algorithms are deemed secure if they are resistant to known attacks (including brute force collision searches). Therefore, it is important to understand such attacks in order to construct cryptographically secure S-boxes for use in practice. This section introduces the two most common forms of cryptanalysis techniques that are used to guage the strength of symmetric-key block cipher designs. It then introduces several mathematical definitions that can be used to measure the security of S-boxes based on the goal of such cryptanalysis techniques, which subsequently become the target objective functions for this optimization project.

TODO: discuss cryptanalysis efforts and how it can break s-boxes

1.1 Cryptographic Strength of Substitution Layers

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 the context of cryptographic applications, 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 [**?**].

Definition 1. The *Hamming weight* of an element $x \in \mathbb{F}_2^n$ 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 *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 $f(x) \oplus f(x \oplus c_i^n)$ is balanced for every element in $\mathbb{F}_2^n$ with Hamming distance of 1.

Definition 6. The *degree of non-linearity* of an $n \times n$-bit S-Box from $\mathbb{F}_2^n \to \mathbb{F}_2^n$ can be measured by

$$P_S = \max_{0 \neq a,b} |\{x \in \mathbb{F}_2^n : S(x + a) - S(x) = b\}|$$

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

Designers of cryptographically secure cryptographic primitives (e.g. block ciphers, hash functions, etc) use all of these measurements as a theoretical basis for their susceptibility to linear and differential cryptanalysis (among other attacks). Specifically, it has been shown that cryptographically secure symmetric-key algorithms utilize diffusion and confusion layers that provide the following characteristics:

1. Low differential propagation probability
2. High branch number

3. High satisfaction of the SAC criterion

4. High degree of nonlinearity

However, in practice the additional constraints that fast and simple mathematical operations must be used to emulate represent such a bijective function f that exhibits ideal values for all of these measurements.

2 Optimization Candidate and Problem Formation

The design goals for S-boxes used inside cryptographic algorithms can easily be represented using mixed integer nonlinear opitmization problems as follows:

They are mixed-integer nonlinear optimization problems.

Minimize

$$BN'(X) = -BN(X) = -\min_{i,j \neq i}(\mathrm{wt}(i \oplus j) + \mathrm{wt}(X(i) \oplus X(j))),$$

subject to the constraints

$$0 \leq X(i) \leq 2^n - 1,$$

where n is the number of design variables.

Minimize

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

subject to the constraints

$$0 \leq X(i) \leq 2^n - 1,$$

where n is the number of design variables.

Minimize

$$BN'(X) = -BN(X) = -\min_{i,j \neq i}(\mathrm{wt}(i \oplus j) + \mathrm{wt}(X(i) \oplus X(j))),$$

subject to the constraints

$$0 \leq X(i) \leq 2^n - 1,$$

where n is the number of design variables.

3 MINLP Algorithms

This is a discrete optimization problem.

Due to the nature of the solutions to these objective functions,

Some common constrained mixed-integer nonlinear optimization problem solver algorithms include the branch and bound and genetic algorithms.

4 Optimization Results

5 Conclusions and Future Work