Differential Cryptanalysis of Block Ciphers

Matthew Laten

Third Year Maths Project

Supervisor: Dr Christine Swart

“Two can keep a secret if one is dead...” - Anon

Abstract

We begin by discussing basic Probability Theory, along with Block Ciphers and Differential Properties of S-Boxes. We then move on to explaining how a Differential Attack works, and the properties of involved that make it work. Furthermore, we include and implemented case of a Block Cipher break.

Contents

Chapter 1

Introduction

To introduce this paper, I will give a short discussion of why we need encryption, speak about block ciphers and differential attacks there-on. Furthermore, I will outline what will be discussed in this paper, namely background information on Probability Theory, Block Ciphers and Vectorial Boolean Functions (S-boxes), Differential Properties of S-boxes and how Probability Theory relates. This will build up to Differential Attacks, which will discuss the various stages of an attack, and culminate in a Toy Example in which a simple Block Cipher is broken. Finally there will be a conclusion in which I summarize the paper.

Chapter 2

Background

I am assuming that the readers of this paper will have studied, or be presently studying at least 3rd year level Mathematics, and thus will discuss these subsections in Mathematical language, without explaining the obvious.

2.1 Probability Theory

By 3rd year level however, a student will not have covered enough Probability Theory to understand what the premise behind a differential attack is; which means that Probability Theory will be discussed in this section. Topics include what it means for and event to have a probability of occuring, how we calculate an event's probability of occuring, and how likely an event is, or string of random events are to occur.

2.2 Block Ciphers

We will be considering Attacks on Block Ciphers later, and thus it makes sense to introduce Block Ciphers as part of the background. In short, Block Ciphers will be defined as algorithms that operate on a fixed amount of bits, using some sort of symmetric key. They will further be explained and examples will be given.

2.2.1 Vectorial Boolean Functions (S-boxes)

A large part of understanding Block Ciphers, and how to attack them, will be tied up in understanding S-boxes, (which are types of Vectorial Boolean Functions). This section will deal with introducing and explaining them, along with a few examples.

2.3 Differential Properties of S-boxes

Next will be discussed the various differential properties of S-boxes which allow cryptanalysts to mount an attack against a block cipher. These include the property that XORs do not affect differentials, as well as ways to find relationships between input differentials and output differentials of an S-box.

2.3.1 Probabilities of Differential Trails

The previous properties discussed can be combined to give us insight into the probabilites of differentials trails, or in plain English: Given an input differential, how likely or probable is it that a certain output differential occurs. This section will discuss the theory behind probabilites of differentials, as well as practical examples of cases where probabilities do not conform to the norm.

Chapter 3

Differential Attacks

In this chapter, I will discuss the process whereby a differential attack can be mounted against a block cipher. Perhaps the easiest way to do this would be by means of working through the process in various subsections, and then putting it all together in the form of a theoretical discussion of why it works.

Thus, the following subheadings might be useful:

3.1 Choosing Plaintext/Ciphertext Pairs

3.2 Computing Differentials

3.3 Statistical Analysis on Differentials

3.4 Breaking Each Round Key

3.5 Combining it all together

3.6 The Theory Behind It or Why It Works

Chapter 4

Toy Example

In this section, I will expand upon a given toy example and discuss an implementation of a differential cryptanalysis attack on it. Furthermore, I will implement the attack and hope to break the block cipher.

Chapter 5

Conclusion

In the conclusion, I will wrap up what has been discussed in my paper, and mention what can be improved upon in the future.

Bibliography

[1] Eric Bach and Jeffrey Shallit. *Algorithmic Number Theory, Volume 1: Efficient Algorithms*. MIT Press, 1996.

[2] Manuel Blum. "Coin flipping by telephone". *Whatever it appeared in*, ?(?):?, 19??

[3] H.E. Rose. *A Course in Number Theory*. Oxford Science Publications, 2nd edition, 1994.