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

Imagine a world without encryption. Anyone with access to a computer could steal your money, impersonate you, or learn your secrets. Privacy would be dead. The inability to secure information might even lead to police states, where governments will have to resort to desparate measures to protect their secrets. Fortunately, we do not live in such a world. We live in a world where encryption is a very real part of our daily lives. Whether banking online, shopping for new items or chatting to your friends on your favourite social network, you are indirectly using various forms of encryption to keep your messages safe, and indicate to computer servers that you are who you say you are.

So if our data is all secure and encrypted, why should we worry more about the subject of Cryptography? In short, our data isn't secure. Attackers find more and more ingenious ways of breaking implementations and protocols, even when the encryption method is said to be secure. The premier algorithm for encrypting electronic data from 1979 onwards, known as the Data Encryption Standard (DES), was broken in 1997. [citation needed] Today's encryption standards are tomorrow's broken algorithms. So we, as cryptographers, have the responsibility to make encryption more secure; even in some cases, to improve the manner in which these algorithms are implemented! How can we do this? By doning a black hat and thinking like an attacker. In this paper, we will be looking at an attack on block ciphers, specifically known as differential cryptanalysis. But first, we should probably define some unfamiliar terminology.

1.1 Terminology

Remark: Note, this paper assumes that you have an adequate knowledge of 3rd year university level Mathematics, but a knowledge of Cryptography or Probability theory is not required, as all concepts necessary for understanding this paper will be explained.

As you might already know, **Cryptography** is the discipline concerned with keeping data secret, or more formally, it is the study and practice of techniques and algorithms for securing the transference of data in the presence of third parties, known as attackers or adversaries. **Cryptanalysis** however, deals with the breaking of these techniques and retrieval of the secret data.

In cryptography, **encryption** refers to the process of converting plaintext, or data that is easily understandable, into ciphertext, that is unintelligible data. The reverse process of converting the cipher text back into plaintext is known as **decryption**. In most cases, this encryption or decryption occurs with the aid of a **key**, a parameter that determines the functional output of the cryptographic algorithm.

Furthermore, there are two main types which come up when discussing key-based cryptography, namely Symmetric-key, and Asymmetric-key or Public-key cryptography. In the case of **Symmetric-key**, the same key is used for encryption and decryption, while with **Asymmetric-key**, a key is made available to the public for encryption, and only those posessing the secret or private key will be able to decrypt messages encrypted with the matching public key.

A **block cipher** is a type of Symmetric-key encryption cipher that operates on a fixed-length "block" of data. This is in contrast to a **stream cipher**, which operates on a potentially infinite stream of data. For the purposes of this paper, we will define a block cipher in more depth later, but at the moment we have enough of a vocabulary to delve into a bit of supporting knowledge.

Chapter 2

Background

We will start by looking at some basic Probability Theory, and then move on to Block Ciphers and interesting properties surrounding them. Since the amount of Boolean Algebra required to understand this paper is minimal, a short comment on this topic will be included in the Block Ciphers section. We will only define concepts that are needed as stepping stones to explaining Differential Cryptanalysis of Block Ciphers, and thus exclude some fundamental theorems to certain sections that are not needed. [1]

2.1 Probability Theory

What does it mean for an event having a probability of occurring? You probably have some intuitive understanding of what this means. For example, you will probably be aware that when you flip a regular coin, you have a 50% chance that it will land with heads facing up, and a 50% chance that it will land with tails facing up. It is also easy to see that if you roll an unweighted die, you have a 1 in 6 chance of landing on a particular number that was chosen before hand.

What if I ask you what the probability of you getting an even number on a die is after you roll it. Most people would say there is a 50% chance, since half of the numbers are even and half of the numbers are odd. With this very intuitive understanding of probability, we will define probability more rigorously below.

Firstly, a **random experiment** is a procedure where the outcome cannot

be determined before the procedure is completed. In our examples above, tossing a coin or rolling a die can be considered random experiments. The set of all possible outcomes to a random experiment is called the **sample space** and a particular instance of conducting the random experiment is known as a **trial** [2] . An **event** in this context is a subset of the sample space. So the coin landing with heads facing upwards, or the die landing on a 3, or even the die landing on an even number would all be examples of events occurring. However, an event that is a singleton in terms of being a subset of the sample space is called an **elementary event**. Thus, only getting heads on a coin toss, or getting a 3 on a die roll can be considered elementary events. Finally we will end of with a definition about how events relate to each other.

Definition: For S, some sample space, let $A, B \subset S$ be events. Then they are called **mutually exclusive** if $A \cap B = \emptyset$.

So what is probability then? Kolmogorov, often considered the Father of probability, defined it as follows [2]:

Definition: Suppose S is a sample space for a random experiment. Then, for all events $A \subset S$, we define the **probability** of A, denoted $Pr(A)$, to be a real number with the following properties:

1. $0 \leq Pr(A) \leq 1$
2. $Pr(S) = 1$ and $Pr(\emptyset) = 0$, where $\emptyset$ is the empty set or **null event**.
3. For $A, B \subset S$, if $A \cap B = \emptyset$ then $Pr(A \cup B) = Pr(A) + Pr(B)$

Now that we have made precise the definition of probability, we can look into calculating probabilities of events occurring.

Theorem 2.1.1. *If $A_1, A_2, ..., A_n$ are pairwise mutually exclusive, or rather for $i \neq j, A_i \cap A_j = \emptyset$, then*

$$Pr(A_1 \cup A_2 \cup ... \cup A_n) = \ Pr(A_1) + Pr(A_2) + ... + Pr(A_n) \tag{2.1}$$

This can be written concisely as

$$Pr\left(\bigcup_{i=1}^{n} A_i\right) = \sum_{i=1}^{n} A_i \tag{2.2}$$

Proof: This proof can be obtained by the repeated use of Axiom 3.

We know that for any $A_i, A_j \in \{A_1, A_2, ..., A_n\}$, A_i and A_j are mutually exclusive.

Thus, by use of Axiom 3, we have

$$Pr\left(\bigcup_{i=1}^{n} A_i\right) = Pr\left(\bigcup_{i=1}^{n-1} A_i\right) + Pr(A_n) \tag{2.3}$$

But it can also be noted that

$$Pr\left(\bigcup_{i=1}^{n-1} A_i\right) = Pr\left(\bigcup_{i=1}^{n-2} A_i\right) + Pr(A_{n-1}) \tag{2.4}$$

In general, for any $3 \leq k \leq n$

$$Pr\left(\bigcup_{i=1}^{k} A_i\right) = Pr\left(\bigcup_{i=1}^{k-1} A_i\right) + Pr(A_{n-1}) \tag{2.5}$$

Thus

Lead up into calculating probabilities from first principles, namely number of elementary events in A over number of elementary events in S.

Definition: Events are called **independent** if the outcome of one event does not affect the outcome of another. (Needs proper def for later)

How to multiply independent probabilities together etc.

2.2 Boolean Algebra

In order to understand how many Block Ciphers work, we will have to take a look at Boolean Algebra, that is, the logical calculus of truth values. In particular we will look at the operation known as the 'exclusive or', commonly known as XOR and represented by the symbol '$\oplus$'.

Definition: The XOR of two boolean values is true if either one of the values is true, and is false if both are true, or both are false.

In simpler terms, we can view it as a function that takes two inputs, and returns true if either the one value or the other is true, but not both. As we are dealing with True and False values, we will use the more compact notation of representing $True$ as 1, and $False$ as 0.

Thus, the truth table for the XOR operation is given as follows:

A	B	$A \oplus B$
0	0	0
0	1	1
1	0	1
1	1	0

This can be compactly noted in the mutliplication table below:

	0	1
0	0	1
1	1	0

What this above table is saying, is that $0 \oplus 0 = 1 \oplus 1 = 0$. Likewise, $0 \oplus 1 = 1 \oplus 0 = 1$.

Remark: It is easy to see that this operation is equivalent to addition in $\mathbb{F}_2$, that is, the finite field of order 2.

2.3 Bits

Firstly, recapping some terminology:

- A **bit** or binary digit is varible which holds either a 0 or a 1
- A **bit string** is a sequence of 1 or more bits.

We can see that the definition of a bit fits well with our representation of boolean values in the previous section. Thus, our definition of XOR applies to bits as well. Furthermore, a bit string can be bit-wise XOR'd with a string of the same length.

Example: Suppose we wanted to XOR 101011 with 011010. We would move through both bit strings, bit by bit, and XOR the individual bits together. Thus, $101011 \oplus 011010 = (1 \oplus 0) + (0 \oplus 1) + (1 \oplus 1) + (0 \oplus 0) + (1 \oplus 1) + (1 \oplus 0) = 110001$ where + represents the concatenation of strings.

You might notice that this operation can be described as taking the first bit string, and flipping the bit whenever you see a 1 as the corresponding bit in the second bit string.

2.4 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 can be defined as algorithms that operate on a fixed amount of bits, using some sort of symmetric key. [citation needed]

Alright, let's take a step back and try understand what that means.

There are different types of block ciphers, but for the purposes of this paper, we will hone in on Substitution-Permutation Networks (SPN). Other block ciphers include Iterated block ciphers, and Feistel ciphers, which are beyond the scope of our discussion.

Thus, in a typical block cipher, our plaintext is broken up to fixed-length groups of bits, called blocks. What makes SPNs different from other block cipher implementations, is the way the symmetric key is mixed in with the plaintext to form ciphertext.

In particular, a block cipher is a combination of 2 paired algorithms, E for encryption, and D for decryption. Both algorithms accept 2 inputs, an input box of size n bits, and a key of size k bits and both yield a n-bit output block.

How could we make this definition more precise though? With our intutive understanding of a Block Cipher, we can define it mathematically as follows:

Definition: For any K, an input key of bit length k, and P is a string of input bits Let us consider a function

$$E_K(P) := E(K, P) : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n \tag{2.6}$$

of length n. We label the output of this function, a string of n bits, C. For each K, the function $E_K(P)$ is required to be an invertible mapping on $\{0,1\}^n$, with the inverse defined as:

$$E_K^{-1}(C) := D(K, C) : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n \tag{2.7}$$

such that

$$\forall K \ D_K(E_K(P)) = P \tag{2.8}$$

holds.

Then the pair $(E_K, D_K = E_K^{-1})$ constitutes a block cipher.

Remark: In the above:

- k is known as the **key size**
- n is known as the **block size**
- C is known as the **ciphertext**
- P is known as the **plaintext**

2.4.1 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.

Example: Let's consider a simple 3 bit S-box. Since there are only 3 bits, we have $2^3 = 8$ possible inputs. Since S-boxes are bijections, we can only have 8 possible outputs. Thus, we can think of an S-box as a type of look-up table.

x	$y = S(x)$
000	010
001	110
010	000
011	100
100	011
101	001
110	111
111	101

We can however reverse the S-box, taking x to be the subject of our formula. So instead of $y = S(x)$, we get $x = S^{-1}(y)$. Looking at the previous table like this, we get:

y	$x = S^{-1}(y)$
000	010
001	101
010	000
011	100
100	011
101	111
110	000
111	110

2.4.2 P-boxes

S-boxes provide good confusion. What about diffusion? P-boxes. Refer to S-box followed immediately by P-box as SP-box.

2.5 Differential Properties of SP-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.

2.5.1 Probabilities of Differential Trails

The previous properties discussed can be combined to give us insight into the probabilities 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 probabilities of differentials, as well as practical examples of cases where probabilities do not conform to the norm.

All of this however, is based on the assumption that these probabilities are linearly independent. If they are not, then we can't be sure of what the final probability is.

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.

So before we begin, we would want to clarify what assumptions need to be made in order to mount a successful attack against the type of Block Cipher discussed in the previous chapter.

We can reduce them to the following list:

1. We can choose some plaintext.
2. We know the corresponding ciphertext.

Accepting those assumptions, we are ready to note down our algorithm for attacking Block Ciphers with Differential Cryptanalysis.

1. Choose some plaintext/ciphertext pairs.
2. Compute the differentials
3.
4.
5.

3.1 Choosing Plaintext/Ciphertext Pairs

3.2 Computing Differentials

	000	001	010	011	100	101	110	111
001								
010								
011								
100								
101								
110								
111								

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] Alko Meijer. "Coin flipping by telphone". *??*, ??(?):?, ??

[2] Les Underhill and Dave Bradfield. *Introstat*. University of Cape Town, 2009.