

Differential CryptAnalysis

Ramkumar Natarajan

Department of Electrical & Computer Engineering,
Oregon State University, Corvallis, Oregon 97331 -USA.

E-mail: *natarara@enr.orst.edu*

Abstract— This paper attempts to throw light on Crypt-analysis with emphasis on Differential Cryptanalysis. It gives the reader an idea about how ciphers which were considered traditionally secure, when specified as mathematical functions are not really secure in real world implementations. In this paper, I try to analyze various research papers and techniques that have been proposed in the area of differential cyrptanalysis and try to propose my scheme for defeating these kinds of differential cyrptanalysis.

KEYWORDS: CRYPTANALYSIS, DIFFERENTIAL CRYPT-ANALYSIS,CIPHERS,QUANTUM CRYPTOGRAPHY)

I. INTRODUCTION

With the exponential growth of computing power and electronic systems, the need and urge for developing an efficient and fool proof way of securing them have also increased proportionately. Cryptographic research has been a very active field of research for some time now and as the need for developing new encryption algorithms keeps increasing, several new and interesting block ciphers have been developed. One of the ways of testing these block ciphers would be differential cryptanalysis.

It is a powerful tool for analyzing and testing block ciphers and the new block ciphers that are being developed should be designed so that these new block ciphers are resistant to it. In this paper we would discuss some key concepts in differential cryptanalysis and take a look at some of the work done in this area and suggest a few changes in the design of the crypto systems so that they become resistant to these kind of attacks.

In Section 2 I give a brief overview of Differential Crypt-analysis. In section 3, talks about the extensions to Differential Cryptanalysis and in section 4, gives the techniques for defeating Differential CryptAnalysis and in section5, I give my Idea for future trends.

II. DIFFERENTIAL CRYPTANALYSIS

A. Overview

The study of taking a cipher, ciphertext, or other information about the cipher and using it to defeat the purpose of the cryptography is called CryptAnalysis. Defeating in this case can be seen as eliminating privacy, as well as fooling non-repudiation systems (such as digital signatures). Essentially, cryptanalysts are the "other side" of the Great Cryptography War.

Author is a graduate student at the Department of Electrical & Computer Engineering, Oregon State University, Corvallis, Oregon 97331. E-mail: *natarara@enr.orst.edu*

The basic idea of Differential Cryptanalysis is to first cipher some plaintext, then make particular changes in that plaintext and cipher it again. Particular ciphertext differences occur more frequently with some key values than others, so when those differences occur, particular keys are (weakly) indicated. With huge numbers of tests, false indications will be distributed randomly, but true indications always point at the same key values and so will eventually rise above the noise to indicate some part of the key.

The basic concept can be applied to virtually any sort of statistic which relates ciphertext changes to key values, even in relatively weak ways. But because the probabilities involved are generally quite small, success generally depends upon having very substantial amounts of known plaintext. Thus, in practice, Differential Cryptanalysis would seem to be defeated by the simple use of message keys and limitations on the amount of material ciphered under a single message key.

Differential cryptanalysis was basically introduced as an approach to analyze the security of DES-like cryptosystems. Differential Cryptanalysis was first described by Biham and Shamir in [1], and in greater detail in [2]. These described the general technique, and its application to the analysis of the DES and the Generalised DES. We will discuss the various works on this field in the following section.

III. RELATED WORK

In 1990 Biham and Shamir described a new kind of attack in [1] that can be applied to many DES-like iterated cryptosystems. This is a chosen plaintext attack which uses only the resultant ciphertexts. The basic tool of the attack is the ciphertext pair which is a pair of ciphertexts whose plaintexts have particular differences. The two plaintexts can be chosen at random, as long as they satisfy the difference condition, and the cryptanalyst does not have to know their values. The attack is statistical in nature and can fail in rare instances.

Iterated cryptosystems are a family of cryptographically strong functions based on iterating a weaker function n times. Each iteration is called a round and the cryptosystem is called an n round cryptosystem. The round function is a function of the output of the previous round and of a subkey which is a key dependent value calculated via a key scheduling algorithm. The round function is usually based on S boxes, bit permutations, arithmetic operations and the exclusive-or (denoted by $+$ and XOR) operations. The S boxes are nonlinear translation tables mapping a small number of input bits to a small number of output bits.

They are usually the only part of the cryptosystem which is not linear and thus the security of the cryptosystem crucially depends upon their choice. The bit permutation is used to rearrange the output bits of the S boxes in order to make the input bits of each S box in the following round depend upon the output of as many S boxes as possible.

Differential cryptanalysis is a method which analyzes the effect of particular differences in plaintext pairs on the differences of the resultant ciphertext pairs. These differences can be used to assign probabilities to the possible keys and to locate the most probable key. This method usually works on many pairs of plaintexts with the same particular difference using only the resultant ciphertext pairs. For DES-like cryptosystems the difference is chosen as a fixed XORed value of two plaintexts.

In this paper [1] Biham and Shamir analyzed DES and found out that; although DES seems to be very non linear in its input bits, when particular combinations of input bits are modified simultaneously, particular intermediate bits are modified in a usable way with a relatively high probability after several rounds. So for every input XOR of an S box suggests a probabilistic distribution of the possible output XORs. In this distribution several output XORs have a relatively high probability.

Biham and Shamir used this property as a tool to identify key bits. If the output XOR of the F function of the last round was found out, the set of possible subkeys entering this F function when the pair of ciphertexts can be deciphered. Using both ciphertexts it is easy to calculate the input XOR of the F function of the last round and its output XOR. Then the input XOR and output XOR of each S box in the last round are known. In case k input pairs can lead to that entry in the table, exactly k values of the corresponding six subkey bits are possible. Most subkey values are suggested by only a few pairs. However, the real value of the subkey bits is suggested by all the pairs and can be identified. In Differential Cryptanalysis, a table showing the distribution of the XOR of input pairs against the XOR of output pairs is used to determine probabilities of a particular observed output pair being the result of some input pair. To attack a multiround block cipher, the XOR profile is used to build n round characteristics, which have a given probability of occurring. These characteristics specify a particular input XOR, a possible output XOR, the necessary intermediate XOR's, and the probability of this occurring.

Biham and Shamir describe 1,2,3 and 5 round characteristics which may be used to directly attack versions of DES up to 7 rounds. Knowing a characteristic, it is possible to infer information about the outputs for the next two rounds. To utilise this attack, a number of pairs of inputs, having the nominated input XOR, are tried, until an output XOR results which indicates that the pattern specified in the characteristic has occurred. Since an n round characteristic has a probability of occurrence, for most keys we can state on average, how many pairs of inputs need to be trialed before the characteristic is successfully matched. Once a suitable pair, known as a right pair, has been found,

information on possible keys which could have been used, is deduced. Once this is done we have two plaintext-ciphertext pairs. We know from the ciphertext, the input to the last round. Knowing the input XOR and output XOR for this round, we can thus restrict the possible key bits used in this round, by considering those outputs with an XOR of zero, providing information on the outputs of some of the Sboxes. By then locating additional right pairs we can eventually either uniquely determine the key, or deduce sufficient bits of it.

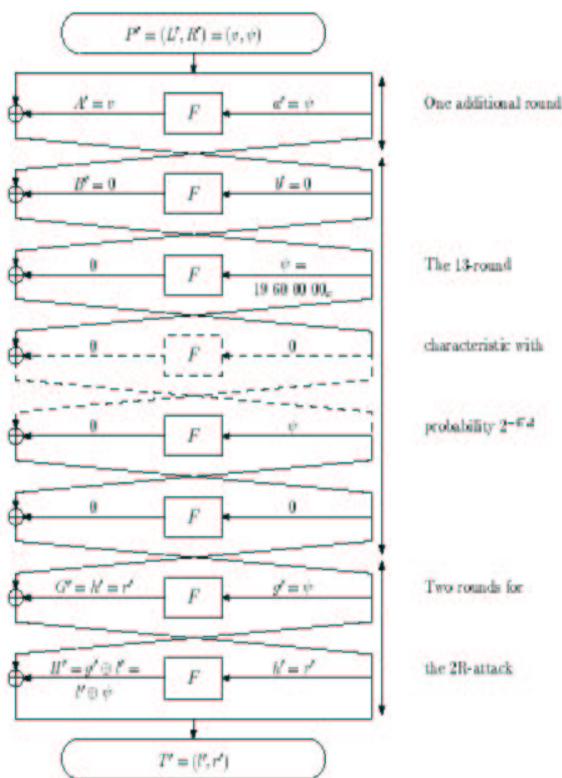


Figure2: Extension of attack to 16 rounds in DES.

In [2] Biham and Shamim developed an improved version of differential cryptanalysis which can break the full 16-round DES in 2^{37} time and negligible space by analyzing 2^{36} ciphertexts obtained from a larger pool of 2^{47} chosen plaintexts. An interesting feature of this attack was that it could be applied with the same complexity and success probability even if the key is frequently changed and thus the collected ciphertexts are derived from many different keys. Any pair of plaintexts which gives rise to the intermediate XORs specified by this characteristic is called a right pair. The attack tries many pairs of plaintexts, and eliminates any pair which is obviously wrong due to its known input and output values.

Rounds	Chosen Texts	Analyzed Texts	Complexity
8	2^{14}	4	2^9
9	2^{24}	2	2^{32}
10	2^{24}	2^{14}	2^{15}
11	2^{31}	2	2^{32}
12	2^{31}	2^{21}	2^{21}
13	2^{39}	2	2^{32}
14	2^{39}	2^{29}	2^{29}
15	2^{47}	2^7	2^{37}
16	2^{47}	2^{36}	2^{37}

Table 1: Summary of Results on DES

In earlier versions of differential cryptanalysis, each surviving pair suggested several possible values for certain key bits. Right pairs always suggest the correct value for these key bits (along with several wrong values), while wrong pairs suggest random values. When sufficiently many right pairs are analyzed, the correct value (signal) overcomes the random values (noise) by becoming the most frequently suggested value. The actual algorithm is to keep a separate counter for the number of times each value is suggested, and to output the index of the counter with the maximal final value. This approach requires a huge memory (with up to 2^{42} counters in the attack on the 15-round variant of DES), and has a negligible probability of success when the number of analyzed pairs is reduced below the threshold implied by the signal to noise ratio.

In this paper Biham and Shamir have suggested a list of complete 56-bit keys rather than possible values for a subset of key bits. As a result, we can immediately test each suggested key via trial encryption, without using any counters. These tests can be carried out in parallel on disconnected processors with very small local memories, and the algorithm is guaranteed to discover the correct key as soon as the first right pair is encountered. Since the processing of different pairs are unrelated, they can be generated by different keys at different times due to frequent key changes, and the discovery of a key can be announced in real time while it is still valid (e.g., in order to forge authenticators for banking messages).

A. Differential Cryptanalysis Extensions

Differential cryptanalysis was introduced as an approach to analyze the security of DES-like cryptosystems. The first example of a DES-like cryptosystem was Lucifer, the direct predecessor of DES, which was believed by many people to be much more secure than DES, since it has 128 key bits, and since no attacks against the full variant of Lucifer were ever reported in the cryptographic literature. In [3] a new extension of differential cryptanalysis, devised to extend the class of vulnerable cryptosystems was introduced. This new extension suggests key-dependent characteristics, called conditional characteristics, selected to enlarge the characteristics' probabilities for keys in subsets of the key space. The application of conditional characteristics to Lucifer shows that more than half of the keys of Lucifer are insecure, and the attack requires about 2^{36} complexity and

chosen plaintexts to find those keys. The same extension can also be used to attack a new variant of DES, called RDES, which was designed to be immune against differential cryptanalysis. These new attacks showed new light on the design of DES, and show that the transition of Lucifer to DES strengthened the later cryptosystem.

In this paper [3] differential cryptanalysis was extended in several directions: The main extension of this paper lets differential cryptanalysis to analyze a wider set of cryptosystems. Conditional characteristics was defined as key-dependent characteristics selected to maximize the characteristic's probability (the fraction of right pairs) for only a specific subset of the key space. The required coverage of (almost) all the key space is done via selection of several conditional characteristics designed for different fractions of the key space.

IV. AVOIDING DIFFERENTIAL CRYPTANALYSIS

As told in the previous section, as more and more cryptographic schemes are being developed more and more cryptanalysis schemes are being developed too. So it always constantly remains as a challenge to the cryptologists to develop new schemes that are not vulnerable and are not prone to attacks.

Several researchers studied how to make cryptosystems immune against differential analysis, but till now, this effort was not very successful. Many of them suggested the use of S boxes whose difference distribution tables are uniform, and in particular they suggested the use of bent functions. However, the application of this suggestion to DES was studied in and it was shown that the resultant cryptosystems become much weaker than DES.

Differential cryptanalysis [1] is based on the fact that in many s-boxes certain input XORs (i.e., certain fixed changes in the s-box input vector) lead to certain output XORs (fixed changes in the s-box output vector) with fairly high probability and to certain other output XORs with very low or zero probability. Chosen plaintext attacks can be mounted which take advantage of the relatively high probabilities to reduce the search space for the key in use. It is obvious, therefore, that if all output XORs occurred with similar (ideally, equal) probability, differential cryptanalysis would have no greater chance of success than exhaustive search.

s-boxes with equiprobable output XORs, can be designed through the use of bent functions. These s-boxes cannot be $n \times n$ bijective s-boxes since columns in the representative matrix are bent and bent functions are not weight balanced. Therefore, SPN cryptosystems taking advantage of this work must be constructed such that it is never required to go 'backwards' through any of their component s-boxes.

Lai and Massey also observed that for the success of differential cryptanalysis it is not necessary to fix the values of input and output differences for the intermediate rounds in a characteristic. They introduced the notion of differentials. The probability of an r -round differential is the conditional probability that given an input difference at the first round, the output difference at the r th round will be

some fixed value. Note that the probability of an r -round differential with input difference A and output difference B is the sum of the probabilities of all r -round characteristics with input difference A and output difference B . For $r = 2$ the probabilities for a differential and for the corresponding characteristic are equal, but in general the probabilities for differentials would be higher.

In order to make a successful attack on a DES-like iterated cipher by differential cryptanalysis the existence of good characteristics is sufficient. On the other hand to prove security against differential attacks for DES-like iterated ciphers we must ensure that there is no differential with a probability high enough to enable successful attacks.

V. FUTURE TRENDS

With the emergence of increasing and pressing needs for safer and lesser vulnerable encryption systems, cryptography research has been heading in the direction of quantum physics. In the age of Quantum Computing, a normal quantum desktop can break a 512 bit encryption in less than a day. Hence My suggestion to the problem to designing ciphers which are resistant to cryptanalysis techniques like differential cryptanalysis would be to develop a quantum cryptographic system which is not prone to cryptanalytic attack.

Another interesting idea that I propose for the design of highly secure cryptographic design would be to use radioactive carbon isotopes for encryption. The carbon atoms at various isotopic form would act as bits for the encryption and would work exactly like the radio-active carbon dating. The radio-active carbon isotopes that are being produces for encryption would be unique and can be decrypted only by the corresponding atom present in the receiver side. Thus this scheme is less vulnerable to differential cryptanalysis type of attacks.

REFERENCES

- [1] Eli Biham and Adi Shamir "Differential cryptanalysis of DES-like cryptosystems," in *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 1991, pp. 3-72, Germany.
- [2] Eli Biham and Adi Shamir "Differential Cryptanalysis of the Full 16-round DES," in *Advances in Cryptology - CRYPTO'92*, Micheal Wiener, Ed. 1992, pp. 487-496, Springer,verlag.
- [3] Ben-Aroya, I. and E. Biham. "Differential Cryptanalysis of Lucifer," in *Advances in Cryptology - CRYPTO '93*, 1993,pp. 186-199, Springer-Verlag.
- [4] Nyberg, K. and L. Knudsen. "Provable Security Against Differential Cryptanalysis," in *Advances in Cryptology CRYPTO'92*, Micheal Wiener, Ed. 1992, pp. 566-574, Springer,verlag.
- [5] Adams, C. " 1992. On immunity against Biham and Shamir's "differential cryptanalysis," in *Information Processing Letters*, 1992, pp. 77-80.