Independent Study Notes

Aaron L. Paolini

Introduction

The following is a summary on selected topics from a 2006 winter session independent study. Over the course of the winter, numerous academic papers and texts were read in order to gain some insight into the practice of cryptanalysis.

One common practice when analyzing a particular cipher is the intentional weakening of the cipher to be studied. Not only does this make analysis feasible, it is also useful in that it may reveal weakness pertaining specifically to certain elements within the cipher. Such weaknesses can be used to attack a fuller version of the cipher, as well as improve the cipher's security by fixing that particular element.

The following document attempts to summarize a select number of common attacks that have been used with some degree of success against certain block ciphers. At the end of the document is a list of works that have been read.

A Statement about Modern Cryptanalysis

Unlike the cryptanalysis of the last few decades, modern cryptanalysis is largely theoretical in nature. Keys that were once 56 bits (for DES) have since grown to as high as 256 bits (or more in some cases), making many attacks infeasible to test experimentally. Of course, such attacks are important, but remain impractical to carry out due to the limits of modern computing equipment.

Contents

Classical Cryptanalysis

Overview

While ciphers of the past have been thoroughly broken, the practice of performing cryptanalysis on early ciphers serves as a gentle introduction to this field of study.

Frequency Analysis (substitution, affine)

Both monoalphabetic substitution and affine ciphers succumb easily to a method of attack known as frequency analysis. Essentially, by recording the frequency of single characters, digrams, and trigrams in a particular ciphertext and comparing these results against previously obtained frequency characteristics for that particular language, one can attempt to decode the ciphertext.

For a large enough ciphertext (so that unique decipherability is obtainable) and for a fine enough expected frequency distribution, this method certainly works. Of course, some additional manual analysis may be necessary to fully recover the plaintext, but for the most part, high frequency characteristics usually hold well enough to make the attempted decoding readable, albeit with minor errors. Correcting such errors is trivial.

Differential Cryptanalysis

Overview

Differential cryptanalysis is one of the earlier methods of block cipher cryptanalysis that proved to be effective against certain block ciphers such as FEAL and reduced-round DES. In general, this attack examines how a given change in the input of a cipher will affect the resultant plaintext. This "difference" is usually defined to be the XOR of two bitstrings (two plaintexts or two ciphertexts).

Consider the f-function input of a given Feistel algorithm, such as DES. Given two plaintexts (X_1 and X_2) with a given XOR (X_1 XOR X_2), there exists a non-uniform output XOR (Y_1 XOR Y_2) distribution. That is to say, for the entire range of possible plaintext pairs with a given XOR value, there exists an output XOR value that occurs with a probability P_{out} that is greater than other possible output XOR values.

This characteristic is the basis for a chosen plaintext cryptanalytic attack against a algorithm that exhibits this behavior.

On Multiple Rounds and Differential Characteristics

For an n-round cipher, there exists an *n-round differential characteristic* with an associated probability p. This *n-round differential characteristic* is simply the concatenation of n *single round differential characteristics,* each with an associated probability p_i. The overall probability p is said to be the multiplication of all per-round differential probabilities, although this only holds true if the rounds are considered independent of one another. While this not the case, p, as calculated, is considered to be close enough to its actual value.

At this point, it may be beneficial to clarify the concept of the probability p for a given *n-round differential characteristic.* Essentially, the probability that for a given round input XOR (X_1 XOR X_2), an expected round output XOR (Y_1 XOR Y_2) will occur with a probability p_i. The probability that the desired per-round characteristics will hold over all rounds in the cipher is given by p.

Obviously, the higher this overall probability is, the more favorable the conditions for a cryptanalytic attack. Thus, it is wise to choose carefully the input XOR of the plaintext pair and desired output XOR to yield the highest overall *n-round differential characteristic probability* p. For example, in a differential attack on the Data Encryption Standard (DES) it is beneficial for the right half of the input XOR to evaluate to zero. Such a technique greatly improves the differential characteristic's probability, as an f-function input XOR of zero will result in an f-function output of zero with probability 1.

On Differential Cryptanalysis and DES

In the case of DES, key bits are calculated by considering the final f-function input (essentially the left half of the ciphertext) and an expected f-function output that holds with probability p. The f-round output cannot be known for certain as it is masked by the left half of the previous round input to give the right half of the ciphertext.

One of the first effective methods of cryptanalysis on the Data Encryption Standard was differential cryptanalysis, if only reduced round versions (usually 3 to 12). Cryptanalysis of higher round versions of DES requires an exceedingly large amount of plaintext pairs (2^{47} pairs for all rounds), making cryptanalysis somewhat infeasible. With very careful selection of differential characteristics, it is possible to break DES in less time than a brute force attack, although it has been said that this characteristic is no good if the input of the cipher is known to be ASCII encoded text.

On Impossible Differentials

While most attacks are concerned with finding a high probability differential, it is worth noting that *any* probability that deviates from a uniform probability distribution is potentially useful. This includes so-called “impossible differentials,” or, differential characteristics that have a zero probability of occurring.

Linear Cryptanalysis

Overview

Linear cryptanalysis attempts to construct linear and affine approximations for nonlinear portions of the cipher, and from that, attempts to characterize the entirety of the cipher's behavior. The approximations relate the input bits, output bits, and key bits in the cipher. Like differential cryptanalysis, it is probabilistic in nature, insofar that constructed linear approximations are said to hold with some probability p.

Notes on the Probabilistic Nature of Linear Cryptanalysis

In an ideally secure cipher, the probability that any given linear expression will hold is said to be $p = ½$. The amount by which this probability varies from ½ is known as the *probability bias;* generally, the attacker desires a greater bias magnitude, as this suggests that the constructed linear approximation is more useful.

DES and Constructing Linear Approximations

Like differential cryptanalysis, linear cryptanalysis of DES generally focuses on the behavior of the s-boxes. Whereas differential cryptanalysis attempts to construct a probability distribution of output XORS for all possible input pairs that have a fixed input XOR, linear cryptanalysis attempts to relate input an output bits of the S-box via a linear expression (using the XOR operator). A probability distribution for this behavior can easily be determined by testing this relationship experimentally.

From this relationship, this linear approximation is then extended to the entire round. The probabilistic s-box expressions obtained in the previous step is used when considering the expansion function E and the permutation P at the end of the round. This relationship is assumed to still hold with the same probability as the s-box linear approximation.

Additional linear approximations, each with their own probability p_i, where i is the round number, can be constructed and concatenated with other per-round linear characteristics. Obviously, as the number of rounds increases, the overall probability bias for the linear characteristic that has been constructed decreases.

The Attack

The attack is probabilistic in nature. As such, a suitably large pool of plaintexts, based on the overall linear characteristic's probability of holding, is needed. At this point, plaintexts are run through the encryption process, and are checked for conformance to the linear characteristic. Inputs that do not conform are thrown out, while inputs that conform are used to calculate the key bits used in the expression, which may or may not be correct. It is assumed that the most frequently occurring key bit values are correct.

Results

For 3 to 12 round DES, the entire can be calculated within a reasonable about of time (from 20 seconds to a day or two, based on the number of rounds). 16 Round DES can be broken in less time than an exhaustive key search.

Slide Attacks

Overview

Slide Attacks are largely motivated by the need to find round-independent attacks, as some newer ciphers include a large number of rounds in an attempt to thwart differential and linear attacks, which are probabilistic in nature. As we will see, there exist other possible vulnerabilities that can be used to compromise certain ciphers, regardless of whether it has two or 32 rounds.

A Brief Description

Slide attacks attempt to exploit the periodic behavior of certain ciphers. This periodicity is usually introduced by way of a repeating key schedule. For example, if a certain cipher with 32 rounds has a key schedule that repeats every two rounds, it can be described in terms of 16 identical rounds. From this stems a major weakness.

Slide attacks attempt to find so called "slid pairs" of plaintext, where the first plaintext, when passed through one "period" of the cipher, results in producing the second plaintext. Similarly, decrypting the second ciphertext through one "period" of the cipher may produce the first ciphertext, also resulting in the discovery of a "slid pair." Thus, a 32 round attack becomes a 2 round attack, greatly weakening the cipher.

Sliding with a Twist

"Sliding with a Twist" is a modification of a traditional slide attack in that one looks for a pair of plaintexts pairs where one period of encryption of one yields the ciphertext of another. It is this method of attack used to perform cryptanalysis on DESX, an extension of DES, and vice versa. This attack effectively eliminates the K2 subkey (the key external to the original DES encryption).

Boomerang Attacks

Overview

Boomerang attacks are a style of differential cryptanalysis that attempt to overcome attempts to ensure an arbitrarily high worst-case differential characteristic. In a sense, they are similar to slide attacks in that they overcome an otherwise low *n-round differential characteristic*. In the words of the author, “it attempts to generate a quartet structure at an intermediate value halfway through the cipher.”

The quartet structure that is generated allows truncated differentials to be used in order to attack the cipher. Thus, even if the entire of the cipher has excellent differential behavior, a truncated differential can be used if the half-cipher’s differential characteristic holds with a high enough probability.

Meet in the Middle Attacks

Overview

Meet in the middle attacks are an extremely generic form of attack that can be used when there exists certain structural characteristics.

Example of Vulnerable Ciphers

Double DES is a prime example of a cipher that is vulnerable to a meet in the middle attack. It is essentially DES encryption under two independent keys. While the complexity of a brute force attack is effectively 2^{112}, with a meet in the middle attack, it can be greatly reduced, to less than 2^{57}. Essentially, given a pool of known plaintext-ciphertext pairs, one performs a single round of encryption on the plaintext for all keys, and a single round of decryption on the ciphertext pools all keys. Matching pairs and the associated key that produced them are recovered from the table. These keys are then tested.

Additionally, TDES is also susceptible to such an attack, although the complexity reduction is only to about 2^{113}.

Feasibility

Certainly, such an attack requires a large amount of storage. As such, with current technology, such an attack on TDES is infeasible, although with enough resources, an attack of this nature can perhaps be carried out on Double DES.

Side-Channel Attacks

Overview

While not necessarily related to cryptology, the nature of these attacks is interesting.

Side-Channel attacks are essentially attacks on the hardware-level implementation of the cipher. Techniques include Differential Power Analysis (observation of power usage by a device at certain point), Timing Attacks (observation of the timing between certain operations), van Eck Phreaking (interception and use of electromagnetic radiation from hardware implementations), and more.

Currently, Government-defined guidelines regarding limits on the electromagnetic emissions of devices exist in order to prevent such attacks.

On Khinchin's *Mathematical Foundations of Information Theory*

Overview

Khinchin's paper offers a mathematically rigorous treatment of Shannon's 1949 monograph. In addition to proof, it offer a mathematically concise model of an ergodic source and the channel to which it is connected, as well as

On A Set of Measure Zero (A possible explanation)

Many papers dealing with ergodic sources contain such phases as "except for a set of measure zero." In order to understand this statement, it is necessary to realize that a ergodic source is defined by a probabilistic characterization of the system in terms of a set of elements X, a set of events consisting of these elements A, and an associated event probability μ. A "set of measure zero" in this context essentially describes a set of events that occur with probability zero. Conversely, the set of all possible events A^I, occurs with probability $\mu(A^I) = 1$.

From the perusal of several articles making mention of "except for sets of measure zero," it seems that an alternative to this type of expression involves "statistical ensembles," an older and apparently more confusing way of discussing probability distribution of states within a system.

Of course, this more research on my part is required.

On **Common Block Cipher Elements**

Overview

The goal for this section is to discuss the common elements of a block cipher in an information theoretic manner. By doing so, it may be possible to motivate insight into the aspects of block cipher design. All of the below elements are used in the DES block cipher.

Permutations

"Permutations" here are said to be a simple rearrangement of the bits in a given string (transposition), although the term can certainly be applied in a broader sense. Even though a hypothetical, random, secret permutation may be used to rearrange the bits in a string of significant length (say, 64 to 1024 bits), it offers little security by itself.

As an example, given a 32 bit string (limited in size for this demonstration)

10110101000111000110101000100011 (0xB51C6A23)

and the results of a "random," permutation

10100110010001001011100111101000 (0xA644B9E8)

it may seem to some that this is one permutation offers a good deal of security. Yet, even if the secret permutation description may be large enough to forbid a brute force attack, this method of obfuscation has a critical flaw when used by itself. It is worth noting that even if one were to apply successively a large number of unique permutations, security would not be improved, as the application of two permutations A and B are equivalent to the application of a single permutation C.

Back to the topic at hand, one critical flaw lay in the fact that the resultant ciphertext from the permutation reveals the bit distribution of the plaintext, that is, the number of ones and zeros. Knowing this, an attacker can effectively eliminate a large portion of possible plaintext (if it is known that only permutations have been used).

Thus, instead of 2^{32} plaintexts corresponding to the known ciphertext, there exists only

binomial(32, 15)

possible plaintexts (that is to say, 32 choose 15). This latter is significantly less than the former. The difference between these two values only becomes more pronounced as the length of the bit string to be permuted increases.

Essentially, permutations alone will result in a ciphertext that leaks a significant amount of information about the plaintext, and is therefore undesirable.

While this is a major flaw, there exists an even greater threat is a known or chosen plaintext attack is feasible. Given enough random plaintexts, the description of the permutation should readily become apparent. Additionally, an N bit permutation can be computed in its entirety with N chosen plaintexts (100…00, 010…00, …, 000…01).

Mixing in Key Material

Key material is frequently introduced into the ciphertext by way of linear operations such as modular addition (RC5) or an XOR operation (DES). This alone, of course, does little for security (representing little more than classical cryptanalysis). Combined with permutations (transposition), the security of the system increases somewhat, but still remains very vulnerable to both linear and differential attacks.

S-Boxes and other Non-Linear Elements

When combined properly with the above two elements, non-linear and dynamic elements in the cipher, such as s-boxes, can greatly increase security, as seen with DES. Essentially, these elements, notwithstanding any critical design flaws, will cause linear approximations to fail with some probability, as well as cause expected differential characteristics not to hold.

Through intelligent combination of such elements, a fairly secure cipher may be obtained; however with advances in computing technology, as well as advancements cryptanalytic attacks, more rounds in such ciphers are needed for security (some ciphers, such a Blowfish, still resist cryptanalysis). This increase in rounds, however, introduces performance issues, especially given the problem of in-software permutations.

As such, there exists a need for stronger per-round security (for less rounds) or more efficient per-round performance (allowing more rounds). Both of these techniques can be seen in action when looking at the recent finalists for the Advanced Encryption Standard.

Bibliography

Eli Biham, Adi Shamir, *Differential cryptanalysis of DES-like cryptosystems*, Journal of Cryptology, Volume 4, Issue 1, Jan 1991, Pages 3 – 72

Eli Biham, Orr Dunkelman. Nathan Keller, *Related-Key Boomerang and Rectangle Attacks*, Lecture Notes in Computer Science, Volume 3494, Jan 2005, Pages 507 – 525

Eli Biham, Alex Biryukov, Adi Shamir, *Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials*, Lecture Notes in Computer Science, Volume 1592, Jan 1999, Page 12

Alex Biryukov, Christophe De Cannière, Michaël Quisquater, *On Multiple Linear Approximations*, Lecture Notes in Computer Science, Volume 3152, Jan 2004, Pages 1 – 22

Alex Biryukov, Eyal Kushilevitz, *From Differential Cryptanalysis to Ciphertext-Only Attacks*, Lecture Notes in Computer Science, Volume 1462, Jan 1998, Page 72

Alex Biryukov, David Wagner, *Slide Attacks*, Lecture Notes in Computer Science, Volume 1636, Jan 1999, Page 245

Alex Biryukov, David Wagner, *Advanced Slide Attacks*, Lecture Notes in Computer Science, Volume 1807, Jan 2000, Page 589

Dan Boneh, Richard A. DeMillo, Richard J. Lipton, *On the Importance of Checking Cryptographic Protocols for Faults*, Lecture Notes in Computer Science, Volume 1233, Jan 1997, Page 37

Johan Borst, Lars R. Knudsen, Vincent Rijmen, *Two Attacks on Reduced IDEA*, Lecture Notes in Computer Science, Volume 1233, Jan 1997, Page 1

Brice Canvel, Alain Hiltgen, Serge Vaudenay, Martin Vuagnoux, *Password Interception in a SSL/TLS Channel*, Lecture Notes in Computer Science, Volume 2729, Oct 2003, Pages 583 – 599

Florent Chabaud, Serge Vaudenay, *Links between Differential and Linear Cryptanalysis*, Lecture Notes in Computer Science, Volume 950, Jan 1995, Page 356

Burton S. Kaliski, M. J. B. Robshaw, *Linear cryptanalysis using multiple approximations and FEAL*, Lecture Notes in Computer Science, Volume 1008, Jun 1995, Pages 249 – 264

Joe Kilian, *How to Protect DES Against Exhaustive Key Search (an Analysis of DESX)*, Journal of Cryptology, Volume 14, Issue 1, Jan 2001, Pages 17 – 35

Jongsung Kim, Seokhie Hong, Jaechul Sung, Sangjin Lee, Jongin Lim, Soohak Sung, *Impossible Differential Cryptanalysis for Block Cipher Structures*, Lecture Notes in Computer Science, Volume 2904, Jan 2003, Pages 82 – 96

A.I. Khinchin, *Mathematical Foundations of Information Theory*, Mineola: Dover Press, 1957.

Yi Lu, Serge Vaudenay, *Faster Correlation Attack on Bluetooth Keystream Generator E0*, Lecture Notes in Computer Science, Volume 3152, Jan 2004, Pages 407 – 425

J. A. Reeds, J. L. Manferdelli, *DES Has No Per Round Linear Factors*, Lecture Notes in Computer Science, Volume 196, Jan 1985, Page 377

Mitsuru Matsui, *On Correlation between the Order of S-Boxes and the Strength of DES*, Lecture Notes in Computer Science, Volume 950, Jan 1995, Page 366

Mitsuru Matsui, *Linear Cryptanalysis Method for DES Cipher*, Lecture Notes in Computer Science, Volume 765, Jan 1994, Page 386

Adam Young, Moti Yung, *Kleptography: Using Cryptography against Cryptography*, Lecture Notes in Computer Science, Volume 1233, Jan 1997, Page 62

Jacques Patarin, *Generic Attacks on Feistel Schemes*, Lecture Notes in Computer Science, Volume 2248, Jan 2001, Page 222

Jacques Patarin, *Security of Random Feistel Schemes with 5 or More Rounds*, Lecture Notes in Computer Science, Volume 3152, Jan 2004, Pages 106 – 122

Bruce Schneier, *Applied Cryptography Second Edition*, John Wiley & Sons, 1996.

Ali Aydin Selçuk, Ali Biçak, *On Probability of Success in Linear and Differential Cryptanalysis*, Lecture Notes in Computer Science, Volume 2576, Jan 2003, Pages 174 – 185

Claude E. Shannon, *A Mathematical Theory of Communication*, Bell System Technical Journal, July/October 1948.

Douglas R. Stinson, *Cryptography: Theory and Practice*, New York: CRC Press, 1994.

David Wagner, *Towards a Unifying View of Block Cipher Cryptanalysis*, Lecture Notes in Computer Science, Volume 3017, Jan 2004, Pages 16 – 33

Xun Yi, Kwok Yan Lam, Yongfei Han, *Differential Cryptanalysis of a Block Cipher*, Lecture Notes in Computer Science, Volume 1438, Jan 1998, Page 58