International Mathematical Forum, 5, 2010, no. 42, 2071 - 2075

The Vulnerability Analysis and the Security Evaluation of Block Ciphers

Davood Rezaeipour and Mohamad Rushdan Md. Said

Institute for Mathematical Research
University Putra Malaysia
43400 UPM Serdang , Malaysia
davreza@inspem.upm.edu.my, davreza45@yahoo.com
mrushdan@putra.upm.edu.my

Abstract

The first step for evaluation of block ciphers is the confidence on attainment of some properties such as completeness, strict avalanche criterion and static information leakage. The attainment of these properties causes the strength of confusion and diffusion properties in block ciphers. In this paper, we describe the computational efficiency of these properties for doing of security evaluation on the different classes of block ciphers. This paper contains the latest scientific results which are used for evaluation of output sequences of cryptosystems.

Mathematics Subject Classification: 94A60, 14G50

Keywords: Block Cipher, Security Evaluation, Completeness, Avalanche, Static Information Leakage.

1. Introduction

Cryptography is only a small part of the security system, but it is a very critical part. Cryptography is the part that has to provide access to some people but not to others. It takes on the role of the lock: it has to distinguish between “good” access and “bad” access. In real life, even bad cryptography is invariably much better than the rest of the security system.

With enough effort, any cryptographic system can be attacked successfully. A new system designed today is, if successful, quite likely to be in operation 30 years from now.
Block ciphers are one of the fundamental building blocks for cryptographic systems. A block cipher processes an input block of elements at a time, producing an output block for each input block. An attack on a block cipher is a nontrivial method of distinguishing the block cipher from an ideal block cipher (a random permutation).
Claude Shannon introduced the ideas of confusion and diffusion (Shannon, 1949), notionally provided by S-boxes and P-boxes (in conjunction with S-boxes).These terms capture the two basic building blocks for any cryptographic system. Every block cipher involves a transformation of a block of plaintext into a block of ciphertext, where the transformation depends on the key. The mechanism of diffusion seeks to make the statistical relationship between the plaintext and ciphertext as complex as possible in order to thwart attempts to deduce the key. Confusion seeks to make the relationship between the statistics of the ciphertext and the value of the encryption key as complex as possible, again to thwart attempts to discover the key.
The *completeness* (Kam, 1979), *avalanche* (Tavares, 1995) and *static information leakage* (Zhang, 1994) are three important properties. These properties have basic role in strengthen of confusion, diffusion and attainment of security for block ciphers.
In this paper, we describe the computational efficiency of these three properties for doing of security evaluation of block ciphers.
Sections 2,3 and 4 elaborate on three important properties; completeness, avalanche and static information leakage. In these sections, also, evaluation procedures are explained.

2. Completeness

The Completeness captures the essential idea of complexity of cipher algorithm.

2.1. Definition

A boolean function is said to be ***complete*** if the value of each output bit depends on *all* input bits. The function $f:\{0,1\}^n \rightarrow \{0,1\}^n$ is said "Complete" if $\forall i,j \in \{1,\ldots,k\}$, it exists two n-bit vector X_1,X_2 such that X_1 and X_2 have difference only in i^{th} bit, $f(X_1)$ and $f(X_2)$ are different at least in j^{th} bit.
A S-box is called "complete" if its transformation function be complete.
A cipher algorithm is said "complete" whenever for all keys, its transformation function be complete.
This is a desirable property to have in cryptography, so that if one bit of the input is changed, every bit of the output has an average of 50% probability of changing.

2.2. Evaluation procedure for completeness property

For completeness test of function $f:\{0,1\}^n \rightarrow \{0,1\}^n$, let $D_{n\times n}$ denote the Correlation Matrix which D(i,j) is defined as the correlation of j^{th} bit from output to i^{th} bit from input. For doing of evaluation, first we set initial value 0 for all elements of correlation matrix, then for completing this matrix, some inputs are chosen from $\{0,1\}^n$, randomly. For each optional input X , let the n-bit sequence X_i has difference with X only in i^{th} bit and $Y=f(X)$ and $Y_i=f(X_i)$, if Y and Y_j has difference only in j^{th} bit , then we set D(i,j)=1 , for each i. These operations are stopped whenever the correlation matrix becomes complete. If the all elements of correlation matrix are "1", then f is complete, otherwise $wt(D)/ n^2$ denotes the percent of completeness, where wt(…) is the numbers of "1" in matrix.

For doing this, we write a correlation matrix which the number of rows is the number of bits of input/key and the number of columns is the number of bits of output for block cipher. This table is completed by making of input-output. If the element $(i,j)^{th}$ is "1" , it means that j^{th} bit of output depend upon i^{th} bit of input/key.

3. Strict Avalanche Criterion

3.1. Definition

The *avalanche* effect is evident if, when an input is changed slightly, the output changes significantly (e.g., half the output bits flip). In the block ciphers, such a small change in either the key or the plaintext should cause a drastic change in the ciphertext.

If a block cipher does not exhibit the avalanche effect to a significant degree, then it has weak randomization property, and thus a cryptanalyst can make predictions about the input, being given only the output. This property has close relation with diffusion. It's proven that increment of diffusion property and also, using of scattered linear transformations causes the increment of avalanche in structure (Tavares, 1995).

3.2. Evaluation procedure for avalanche property

To do this evaluation, we construct an avalanche matrix which the number of rows are the number of bits of input/key and the number of columns are the number of bits of output (Tavares, 1995). The element $(i,j)^{th}$ of this matrix denotes the number of times which the changing of i^{th} bit from input/key causes the changing of j^{th} bit from output. The elements of this matrix are completed by using either plaintext−ciphertext with fixed key-all bits are zero- or key−ciphertext with plaintext-all bits are zero. If each element from this table is

equal with half of the evaluated pairs, then algorithm supplies the property of avalanche and if the average value of table is ½ , so it supplies the property of avalanche . This property is accepted with α% as assurance factor if the elements of table are settle in the interval: *"The number of pair × (1 ± (1−α))"*.
In ideal case, we expect that in half of instances, the changing of each bit from input/key causes the changing of each bit from output. The evaluation can be done with assurance factor of 99%, since the occurrence of error is natural in the random sequences.
For facility, we subtract the ideal number of expecting in correlation matrix from their quantities. We construct the difference table which the number of rows is the number of bits of input/key and the number of columns is the number of output bits. For assurance factor 99%, the criterion of acceptance is setting in interval of ±100. This criterion is computable with using the assurance factor (a.f.) and the number of assessable sequences, as it follows:

Maximum distance=[±(1−a.f.) × (Number of evaluated sequences/2)]

4. Static Information Leakage

One factor, which helps to cryptanalyst for breaking of cryptosystems, is the guess of some output bits with the knowledge about input bits.
If attacker can analyze the cryptosystem with this way, it is said to be the system has *Static information leakage*. So, one cryptosystem is good if and only if any knowledge about the input bits do not help to recognition of output bits.

4.1. Evaluation procedure for avalanche property

To do this property, we construct the static leakage matrix which the number of rows is the number of bits of input/key and the number of columns is the number of bits of output.
In this matrix, each element is a 2×2 table, and the element of Information(i,j,m,n) is the determinant for the number of times which i^{th} bit of input/key is equal with m and j^{th} bit of output is equal with n.
If the all of probabilities become ½ , then the quantity of static information leakage will be zero in the mentioned structure.

5. Conclusion

The target of the security evaluation is detecting of vulnerability points in block ciphers. We described the important properties for this evaluation. We also can do these capabilities with changing of the algorithm characters such as block length,

key length and so on.
This article helps you evaluate the generated sequences of a cryptosystem, and also different sub-algorithms.

References

[1] B. Kam and I. Davida, Structured Design of Substitution-Permutation Encryption Network, IEEE Transactions on Computers, 28 (1979), 747-753.

[2] C. E. Shannon, Communication Theory of Secrecy Systems, The Bell System Technical Journal, 28 (1949), 656-715.

[3] S. E. Tavares and M. Heyse, Avalanche Characteristics of Substitution Permutation Encryption Network, IEEE Transactions on Computers, 44 (1995), 1131-1139.

[4] M. Zhang, S. E. Tavares and L. L. Campbell, Information Leakage of Boolean Functions and its Relationship to Other Cryptographic Criteria, ACM Conference and Communications Security(1994), 156-165.

Received: November, 2009