On the statistical testing of block ciphers

Author(s):
De Moliner, Richard J.

Publication Date:
1999

Permanent Link:

https://doi.org/10.3929/ethz-a-003811807 →

Diss. ETH No. 13106

On the Statistical Testing of Block Ciphers

A dissertation submitted to the
SWISS FEDERAL INSTITUTE OF TECHNOLOGY
ZURICH

for the degree of
Doctor of Technical Sciences

presented by
RICHARD J. DE MOLINER
Dipl. El.-Ing. ETH
Dipl. Informatik-Ing. ETH
born February 5, 1962
citizen of Zug ZG

accepted on the recommendation of
Prof. Dr. James L. Massey, referee
Dr. Markus Dichtl, co-referee
Prof. Dr. Ueli Maurer, co-referee

1999

Abstract

Tests that are capable of analyzing any practical block cipher, no matter what the internal structure of the block cipher may be, are the subject of this work. It is argued that such tests must be statistical.

A discrete memoryless source producing a fixed-length sequence of output digits from a finite alphabet is considered. The problem of deciding whether the single letter probability distribution of the discrete memoryless source is equal to a given probability distribution or not is analyzed in detail. For this problem of statistical hypothesis testing the Pearson statistic is used. What can validly be concluded from statistical hypothesis testing is carefully considered.

We show that if a cryptanalyst cannot solve at least one of two basic problems for a given block cipher, then he cannot "break" this block cipher. These two basic problems are (1) to find an algorithm that is *distinguishing* for the given block cipher and (2) to find an algorithm that is *key-subset distinguishing* for the given block cipher and for a given decomposition of the key space.

An approach to finding an algorithm that is distinguishing for a given block cipher as well as an approach to finding an algorithm that is key-subset distinguishing for a given block cipher and for a given decomposition of the key space are described. These two approaches form the framework for the statistical testing of block ciphers.

A family of tests called bit-dependency tests is presented. The aim of a bit-dependency test is to say as much as possible about the quality of a block cipher when only a given subset of bits of the plaintext blocks and a given subset of bits of the corresponding ciphertext blocks

are observed.

Keywords: cryptography, cryptanalysis, block ciphers, bit-dependency tests, statistical hypothesis testing, statistical tests, Pearson statistic.

Kurzfassung

Der Gegenstand dieser Arbeit sind Tests, welche praktische Blockverschlüssler analysieren, ohne deren interne Struktur zu berücksichtigen. Es wird begründet, weshalb solche Tests statistisch sind.

Wir betrachten eine diskrete, gedächtnislose Quelle, welche eine Folge fester Länge von Ausgangssymbolen aus einem endlichen Alphabet generiert. Das Problem, zu entscheiden, ob die Wahrscheinlichkeitsverteilung der Ausgangssymbole gleich einer vorgegebenen Wahrscheinlichkeitsverteilung ist oder nicht, wird im Detail analysiert. Für dieses Problem des Testens statistischer Hypothesen verwenden wir die Pearsonstatistik. Dabei wird gründlich überlegt, was vom Testen statistischer Hypothesen wirklich gefolgert werden kann.

Wir zeigen, dass so lange ein Kryptoanalyst nicht zumindest eines von zwei grundlegenden Problemen für einen vorgegebenen Blockverschlüssler lösen kann, so lange wird dieser Kryptoanalyst diesen Blockverschlüssler auch nicht "brechen" können. Diese beiden grundlegenden Probleme sind (1) einen Algorithmus zu finden, der für den vorgegebenen Blockverschlüssler *unterscheidend* ist, und (2) einen Algorithmus zu finden, der für den vorgegebenen Blockverschlüssler und eine vorgegebene Unterteilung des Schlüsselraumes *schlüsselteilmengeunterscheidend* ist.

Im Folgenden beschreiben wir ein Verfahren, um einen Algorithmus zu finden, der für einen vorgegebenen Blockverschlüssler unterscheidend ist; ebenfalls wird ein Verfahren angegeben, um einen Algorithmus zu finden, der für einen vorgegebenen Blockverschlüssler und für eine vorgegebene Unterteilung des Schlüsselraumes schlüsselteilmengeunterschei-

dend ist. Diese beiden Verfahren bilden den Rahmen für das statistische Testen von Blockverschlüsslern.

Schliesslich wird eine Familie von Tests, sogenannte Bitabhängigkeitstests, vorgestellt. Das Ziel von Bitabhängigkeitstests ist, so viel wie möglich über die Qualität eines Blockverschlüsslers auszusagen, wenn nur eine vorgegebene Untermenge von Bits der Klartextblöcke und nur eine vorgegebene Untermenge von Bits der Kryptogrammblöcke beobachtet werden.

Stichworte: Kryptographie, Kryptoanalyse, Blockverschlüssler, Bitabhängigkeitstests, Testen statistischer Hypothesen, statistische Tests, Pearsonstatistik.