Available online at www.sciencedirect.com
SCIENCE DIRECT®
ELSEVIER Applied Mathematics and Computation 162 (2005) 29–35
APPLIED MATHEMATICS AND COMPUTATION
www.elsevier.com/locate/amc

A randomness test for block ciphers

Vasilios Katos

Department of Information Systems and Computer Applications, University of Portsmouth, 1-8 Burnaby Road, Portsmouth P01 3AE, UK

Abstract

This paper describes a randomness test which can be used to measure the cryptographic strength of a block cipher or its underlying cryptographic primitive(s). Cryptographic strength in the context of this paper is related to the ability of the round function to produce a random output which in turn is defined as the distance between a theoretical calculation and an experimental measure. The measurements are based on the diffusion characteristic of the cipher. Potentially, the test for randomness proposed in this paper could be used as a distinguisher based on diffusion.

Keywords: Statistical randomness test; Diffusion; Block cipher

1. Introduction

Statistical tests for randomness [1–3] are of a particular interest in cryptography, since they are one of the approaches for assessing the cryptographic strength of a cipher. The main focus on statistical randomness tests in cryptography was on stream ciphers where a pseudorandom sequence is combined with the plaintext using a mixing function, such as the modulo-2 addition.

Research in theoretical cryptography on the other hand, revolves around the provable security paradigm. A typical example is the notion of pseudorandom functions first described by Goldreich et al. [4] and utilised by Luby and Rackoff [5], which revealed an interesting path for theoretical research.

E-mail address: vasilios.katos@port.ac.uk (V. Katos).

0096-3003/$ - see front matter
doi:10.1016/j.amc.2003.12.122

However, for some ciphers a provable security approach may be difficult if not impossible. Therefore, in order to ensure provable security, many constructions are based on cryptographic primitives which maintain the desirable provably secure properties, e.g. [6].

From a practical perspective, Biham and Shamir [7] developed the method of differential cryptanalysis which exploits the inability of a block cipher to map input to output differences in a statistically uniformal manner. This inability is responsible for leaking key bit information. The study of discovering linear relations between the (plaintext and key) inputs and the output was developed and presented in [8], which is the so-called linear cryptanalysis.

If a cipher is secure against all known cryptanalytic attacks, it could be considered secure, until it is realised otherwise. Provable security strengthens the secure cipher claim 'beyond reasonable doubt'. The design and analysis of the latest cryptographic standard AES [9] follows both practices.

Typically when investigating the security of a cryptographic primitive, the objective is to find patterns between the plaintext, key and output which do not appear uniformly. This paper describes a statistical test which measures the randomness behaviour—as defined in this paper—of a block cipher, by systematically constructing one bit input differences. If the cipher does not pass the randomness test, then some form of relation exists between the inputs and output. The proposed method does not reveal the actual relations, but rather is an indication of the cryptographic quality of the cipher [10]. The test can be applied both to the block cipher as a whole, as well as to the round function, in case where the block cipher is a Feistel construction [11].

2. Diffusion instances

A block cipher can be viewed as a function with two input independent variables, namely the plaintext (or ciphertext) and the encrypting (or decrypting) key, and one output dependent variable, the ciphertext (or plaintext).

Diffusion is the property where a given input plaintext bit has the chance to affect the output bits. The higher the diffusion, the more output bits can be affected by a certain input bit. In the described method, the diffusion instance is defined. The diffusion instance is a *snapshot* of the diffusion capacity of a cipher.

The diffusion instance is generated as follows. Given a random plaintext $p_0 \in_U GF(2)^n$, $n-1$ plaintexts are generated, such that the Hamming distance between p_i and p_0 for $1 \leqslant i \leqslant n$ is one and $p_i \neq p_j$ for all $i \neq j$. Furthermore, $i-1$ denotes the position where the difference occurs.