Statistical Analysis of Advanced Encryption Standard

David Josephs
Southern Methodist University
Dallas, Texas
Email: josephsd@smu.edu

Hannah Kosinovsky
Southern Methodist University
Dallas, Texas
Email: hkosinovsky@mail.smu.edu

Carson Drake
Southern Methodist University
Dallas, Texas
Email: drakec@smu.edu

Volodymyr Orlov
Southern Methodist University
Dallas, Texas
Email: vorlov@smu.edu

***Abstract*—Advanced Encryption Standard (AES) is one of the most common and widely used specification for the encryption of electronic data. AES is a block cipher with 128-bit internal state and 128/192/256-bit key (AES-128, AES-192, AES-256, respectively). No efficient attacks against AES are known up to date and the standard is considered practically secure. In this paper we perform an extensive statistical analysis of AES-128 output using NIST Statistical Test Suite and additional randomness tests with a goal to identify any bias in either the entirety of the encrypted output or in sequences of encryption blocks generated from input values created using a counter or a linear feedback shift register (LFSR).**

I. Introduction

Advanced Encryption Standard is a symmetric key block cipher method established by the U.S. National Institute of Standards and Technology (NIST) in 2001. In AES the same key is used for both encrypting and decrypting the data. Since its introduction, AES has been adopted by the U.S. government and is now used for a variety of applications worldwide. There are three variants of AES: AES-128, AES-192 and AES-256, where the number after AES indicates the key length used for encryption and decryption process. Since its adoption, the world saw little progress in the cryptanalysis of this cipher.

One of the basic properties of AES is indistinguishability of its output from a random sequence of bits. An evaluation of the cipher's output using randomness tests is an important tool in cryptanalysis that helps to ensure the algorithm produces no distinguishable patterns which can be used to deduce an encryption key or a plain text input. For this reason, the evaluation of the output of the AES by means of statistical randomness tests is of great importance. This paper will analyze randomness of the output produced by the AES-128 block cipher using NIST statistical test suite and the Diehard test battery.

II. Statistical Randomness Tests

Statistical tests for randomness take arbitrary length input sequence and analyze its distribution to see if it is random and contains no recognizable patterns or regularities. Usually these tests produce a real number between 0 and 1, the p-value, which shows a probability of finding the observed, or more extreme, results with respect to certain randomness properties of the given input. There exists some Notable software implementations, like NIST Statistical Test Suite or Diehard tests that can be used to analyze output of AES-128.

The NIST Test Suite consists of 15 tests specially designed to analyze binary sequences. All NIST tests examine randomness for the whole binary sequence. In addition to that several tests are also able to detect local regularities.

Aside from the NIST test suites, there are a few other test suites for testing the randomness of cryptographic pseudorandom numbers, such as the Dieharder test suit, SPRNG, and the tests mentioned in

```
\cite{Demirhanetal}
```

(Statistical Testing of Cryptographic Randomness, Demirhan et al., 2016), which combines the Knuth, Helsinki, Diehard, and SPRNG test batteries.

The reason for including these various tests is to cover a wider array of statistical methods in order to detect a lack of randomness in AES-128. The NIST test suite tests for various metrics such as entropy, frequency within a block, random excursions, etcetera. In contrast, the 26-test Dieharder battery tests for distributions, bit distances, overlapping permutations and sums, while the SPRNG battery (13 tests) covers more stochastic processes such as random walks and the Ising model (a mathematical model of ferromagnetism), and the Helsinki test looks for correlations and blocks within the pseudorandom data. The Knuth battery contains a different set of tests, with sme overlap with the others, however still including some unique tests.

In this paper, the SMU ManeFrame II supercomputer will be used to first generate the necesary datasets consisting of nine different categories of data, then ManeFrame II will evaluate each algorithm of the NIST statistical test suite against each of the nine categories of data sets. ManeFrame's supercomuting capabilities will be leveraged to generate nine data for each statistical test.

The nine categories of datasets have been selected because of their usefulness in evaluating the randomness of an algorithm's output. These nine categories are 128-bit key avalanche, Cipher Block Chaining Mode, Plaintext Avalanche, Low Density Plaintext, Low Density 128-Bit Keys, High Density Plaintext, High Density 128-Bit Keys, Plaintext/Ciphertext Correlation, and Random Plaintext/Random 128-Bit Keys.