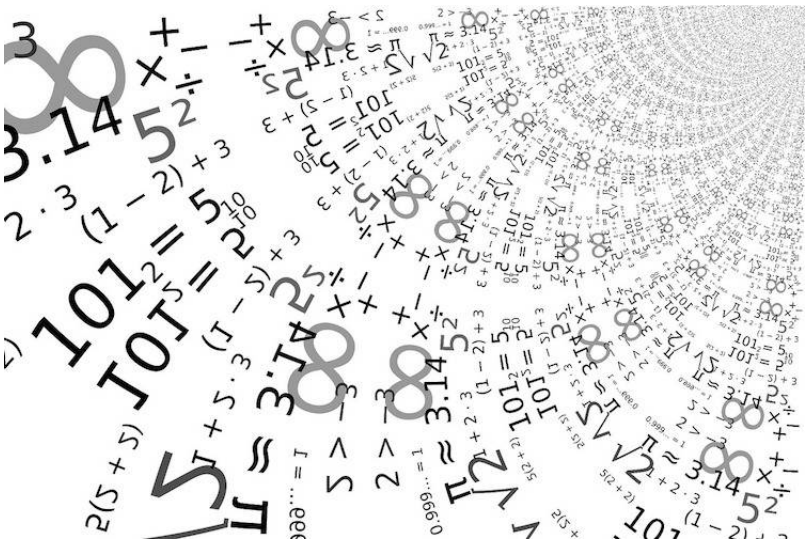
Effect of Randomness Evaluation on Linear and Differential Attacks



Linear and differential attacks are fundamental tools in modern cryptanalysis, as they allow researchers to exploit statistical patterns in block ciphers to recover secret keys more efficiently than brute-force methods. On the other hand, randomness analysis has played a crucial role in cryptographic standardization efforts. It was conducted during the Advanced Encryption Standard (AES) selection process in 1999 and 2000, in 2011 for the SHA-3 candidate evaluation, and later in 2018 during the standardization of lightweight cryptographic algorithms. The 1999 analysis focused exclusively on testing the 128-bit key variant (with a 128-bit block size) of each encryption algorithm.

The methodology for generating data across nine dataset categories and performing 188 statistical tests has been well-defined for cryptographic algorithms with a 128-bit block size. However, a standardized approach for analyzing block sizes other than 128 bits has not yet been established. Many lightweight block ciphers operate with block sizes different from 128 bits.

The primary objective of this project is to systematically redefine the NIST dataset categories for different key and block sizes and to introduce additional statistical tests that address the limitations of the current evaluation framework. Additionally, it aims to identify and implement the necessary modifications in the NIST test suite to enhance its effectiveness in assessing the randomness of data across different cryptographic configurations. Most importantly, this study also explores the relationship between randomness and two fundamental cryptographic attacks, namely linear and differential attacks on block ciphers.

Practicalities

Promotor:	Vincent Rijmen
Daily supervisor:	Anum Sajjad asajjad@esat.kuleuven.be office B01.03
Nature of the work:	30% literature, 20% theoretical work, 50% software
Number of students:	1

 © 2025 – 2026 COSIC