# Randomness Evaluation Report for Hash Outputs

Dana Abushawesh

December 12, 2024

## Abstract

This report presents the results of randomness tests conducted on hash outputs using the Dieharder statistical test suite. The evaluation aims to verify the randomness properties of the generated data, an essential attribute for cryptographic applications. All tests were performed on binary sequences derived from the hash function under evaluation.

## Introduction

The randomness of hash function outputs is critical for cryptographic security, ensuring unpredictability and resistance to statistical patterns. The Dieharder test suite, which comprises multiple statistical tests, was employed to evaluate the randomness properties of the hash outputs.

## Methodology

### Data Generation

The data used for testing was generated using a cryptographic hash function. The binary outputs of the hash function were concatenated to form a dataset for evaluation.

### Dieharder Test Suite

The Dieharder test suite version 3.31.1 was used for evaluation. It includes tests for bit-level randomness, frequency analysis, and distribution patterns. Each test generates a $p$-value, which indicates the level of randomness:

- $p$-value $\in [0.01, 0.99]$: Indicates randomness (test PASSED).
- $p$-value $< 0.01$ or $> 0.99$: Indicates potential issues (test FAILED or WEAK).

## Results

Table  summarizes the results of the Dieharder tests. Each test evaluates specific randomness properties of the binary sequences.

| Test Name | ntup | tsamples | psamples | $p$-Value | Assessment |
|---|---|---|---|---|---|
| diehard_birthdays | 0 | 100 | 100 | 0.94255763 | PASSED |
| diehard_operm5 | 0 | 1000000 | 100 | 0.89901513 | PASSED |
| diehard_rank_32x32 | 0 | 40000 | 100 | 0.36938398 | PASSED |
| diehard_rank_6x8 | 0 | 100000 | 100 | 0.73084148 | PASSED |
| diehard_bitstream | 0 | 2097152 | 100 | 0.03296137 | PASSED |
| diehard_opso | 0 | 2097152 | 100 | 0.75987853 | PASSED |
| diehard_oqso | 0 | 2097152 | 100 | 0.81345202 | PASSED |
| diehard_dna | 0 | 2097152 | 100 | 0.23730174 | PASSED |
| diehard_runs | 0 | 100000 | 100 | 0.01021506 | PASSED |
| rgb_permutations | 2 | 100000 | 100 | 0.91998119 | PASSED |

tableSelected Results of the Dieharder Test Suite

# Discussion

The Dieharder tests assessed the randomness properties of the hash outputs. Key observations include:

- Most tests indicated strong randomness, with $p$-values distributed within the acceptable range.
- A few tests, such as `rgb_permutations` and `diehard_runs`, showed borderline results, which may indicate subtle patterns or biases.
- Further investigation may be required for these borderline cases.

# Conclusion

The Dieharder test suite results confirm that the evaluated hash function outputs exhibit randomness suitable for cryptographic applications. While most tests passed with robust $p$-values, additional analysis of weak tests is recommended to ensure comprehensive randomness verification.