International Scientific Conference 20 UNITECH 26

INTERNATIONAL SCIENTIFIC CONFERENCE
19-21 November 2026
GABROVO

INVESTIGATION OF ROUND-COUNT-DEPENDENT STATISTICAL DIFFERENCES IN CHACHA8, CHACHA12 AND CHACHA20 KEYSTREAMS

Fatma BÜYÜKSARAÇOĞLU SAKALLI[1]

[1]*Trakya University, Computer Engineering Department, Edirne, TÜRKİYE*

**Corresponding author: fbuyuksaracoglu@trakya.edu.tr*

Abstract

ChaCha is a stream cipher widely used in software-based applications due to its ARX design based on addition, rotation, and XOR operations. This study investigates whether reducing the number of rounds produces measurable differences in the basic statistical properties of the generated keystreams by comparing ChaCha8, ChaCha12, and ChaCha20. For each variant, 1,500 independent 256-bit keys were generated, and five 128 KB keystreams were produced per key using different nonce values, yielding 22,500 keystreams in total. The five samples generated from the same key were aggregated at the key level, and the analyses were conducted on 1,500 independent observations per variant. The Kruskal–Wallis test showed no significant overall difference in bit ratio, bit transition ratio, Shannon entropy, or lag-1 autocorrelation ($p = 0.207–0.743$; $\varepsilon^2 \leq 0.000256$). The absolute magnitudes of the pairwise standardized differences did not exceed approximately 0.073, and the standardized multivariate distances based on all four features also remained low. The findings indicate that the selected output statistics do not exhibit a strong and consistent separation associated with the number of rounds. However, this output-level similarity should not be interpreted as cryptographic security equivalence; structural cryptanalytic results for reduced-round ChaCha represent a separate dimension of security.

Keywords: ChaCha, Stream Cipher, Keystream, Reduced-Round, Statistical Distinguishability, Kruskal–Wallis Test.

INTRODUCTION

A fundamental property expected of a stream cipher is that its keystream resembles a random bit sequence and does not exhibit obvious patterns [2]. Keystreams are therefore commonly examined in terms of bit distribution, entropy, transition behavior between consecutive bits, and autocorrelation [3]. These measures alone are not sufficient to establish the security of a cryptographic algorithm; their role is limited to identifying observable statistical deviations in the output [4].

ChaCha is a family of stream ciphers built on an ARX structure composed of addition, rotation, and XOR operations [1]. Its internal state consists of 16 32-bit words, and the main mixing operation is performed through the quarter-round function [1], [12]. ChaCha20 applies this structure for 20 rounds, whereas ChaCha12 and ChaCha8 use the same basic transformations with fewer rounds [5]. Because the underlying structure is retained, the effect of reducing the round count can be examined directly in terms of measurable statistical changes in the generated keystreams.

Reducing the number of rounds lowers computational cost but also changes the security margin of the algorithm [6]. Reduced-round ChaCha has therefore long been a subject of cryptanalytic research [7]. The probability behavior of key-recovery attacks based on probabilistic neutral bits has been investigated [7], and subsequent studies have developed differential-linear techniques in several directions. For seven-round ChaCha256, the attack complexity was reduced from 2^230.86 to 2^218.95, while attacks on 7.25-round ChaCha256 and 6.5-round ChaCha128 were reported with time complexities of 2^244.85 and

This is an open access article licensed under Creative Commons Attribution 4.0 International
Print ISSN: 1313-230X, Online ISSN: 3033-1404

2^121.40, respectively [8]. Within a higher-order differential-linear framework, time complexities of 2^39.07 and 2^135.07 were reported for ChaCha6 and ChaCha7, respectively, improving on previous results [9]. A more recent study revisited the data requirement of an earlier seven-round result; seven-round ChaCha was analyzed with 2^101.15 data and 2^192.15 time complexity, while 7.5-round ChaCha was considered with 2^101.14 data and 2^230.58 time complexity [10]. Recent work indicates that cryptanalytic results on the ChaCha permutation raise a security-margin discussion around eight rounds [11]. The effect of the round count can be studied not only through attack costs but also through the statistical behavior of the output sequences. Unlike cryptanalytic attacks, the present study focuses on selected statistical manifestations of round-count reduction directly in the keystream.

The keystreams generated by ChaCha8, ChaCha12, and ChaCha20 were compared in terms of bit ratio, bit transition ratio, Shannon entropy, and autocorrelation. For each variant, 1,500 independent keys were used, and the analyses were conducted at the key level to account for the dependence introduced by multiple streams generated from the same key. The primary analysis was based on the Kruskal–Wallis test and epsilon-squared effect size. To examine whether the results were sensitive to the choice of statistical method, complementary parametric analyses based on summary statistics were also performed, together with pairwise standardized differences, 95% confidence intervals for the means, and descriptive standardized multivariate distances. These additional evaluations made it possible to consider not only statistical significance but also the magnitude of the observed differences.

2. MATERIALS AND METHODS

2.1. ChaCha Variants

This study examined the 8-, 12-, and 20-round configurations of the ChaCha family. The variants use the same ARX structure and differ primarily in the number of rounds applied. The ChaCha state matrix consists of 16 32-bit words: four constants, eight words for the 256-bit key, one block counter, and three words for the 96-bit nonce [12].

The fundamental ChaCha transformation is the quarter-round operation, in which modular addition, XOR, and 32-bit rotations are performed in a specific sequence. In each double round, the quarter-round is first applied to the columns and then to the diagonal elements [12].

ChaCha8 and ChaCha12 were implemented using the same quarter-round and state-update logic, whereas ChaCha20 keystreams were generated with the implementation provided by the PyCryptodome library.

The correctness of the Python implementations of ChaCha8 and ChaCha12 was additionally verified using known-answer test (KAT) vectors. First, the common ChaCha block function in both implementations was run for 20 rounds and matched the ChaCha20 block-function test vector in RFC 8439 exactly at the byte level [12]. The reduced-round implementations were then tested against the 256-bit-key ChaCha8 and ChaCha12 test vectors published by Strömbergson; both variants exactly matched the expected outputs [13]. The validation tests were performed using Python 3.13.14 and PyCryptodome 3.23.0.

2.2. Data Generation

For each ChaCha variant, 1,500 independent 256-bit keys were generated. Five different keystreams were produced for each key, with a new 96-bit nonce generated for every sample. Keys and nonce values were generated using the Crypto.Random.get_random_bytes function and no fixed random seed was defined at the application level. Each keystream was 128 KB long. This yielded 7,500 keystreams per variant and 22,500 keystreams in total across the three ChaCha variants.

The five samples generated from the same key were retained under the same key_id during data generation, while a new nonce was generated for each sample. In the

ChaCha8 and ChaCha12 implementations, the 32-bit block counter was initialized to 0 and incremented after each 64-byte output block. The raw-stream interface of the PyCryptodome ChaCha20 implementation used for ChaCha20 generation also starts with block counter 0; therefore, keystream generation for all three variants began at the same block position. The generation setup was identical across the variants: 1,500 keys, five samples per key, and 128 KB of output per sample.

2.3. Statistical Feature Extraction

Four features were used to compare the generated keystreams: bit ratio, bit transition ratio, Shannon entropy, and autocorrelation. Each feature was calculated separately for every 128 KB keystream.

The bit ratio is the proportion of bits equal to 1 in the sequence; for a balanced binary sequence, this value is expected to be close to 0.5 [14]. In this study, the bit ratio was calculated as shown in Equation (1).

$$B = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{1}$$

The bit transition ratio is the proportion of positions at which two consecutive bits differ and is expressed by Equation (2):

$$T = \frac{1}{N-1}\sum_{i=1}^{N-1} I(x_i \neq x_{i+1}) \tag{2}$$

Here, I(·) takes the value 1 when the condition is true and 0 otherwise.

Shannon entropy was calculated from the observed bit probabilities as shown in Equation (3) [15]:

$$H = -p_0 log_2(p_0) - p_1 log_2(p_1) \tag{3}$$

For a balanced binary sequence, the maximum Shannon entropy per bit is 1 [15].

Autocorrelation was calculated using the lag-1 autocorrelation coefficient to assess the linear relationship between consecutive bits. This coefficient corresponds to the Pearson correlation coefficient between the bit sequence and a one-bit-shifted version of itself; for an independent and balanced binary sequence, a value close to zero is expected [16].

These four measures were not selected to constitute a comprehensive randomness test suite, but rather to determine whether a change in the round count leaves an observable trace in the keystream at a basic statistical level.

2.4. Statistical Analysis

Because five keystreams were generated from each key using five different nonces, treating samples from the same key as fully independent observations was considered inappropriate. For each feature, the five samples sharing the same key_id were averaged, and the statistical analysis was performed at the key level. The key_id label was added to the feature dataset during preprocessing and retained throughout the subsequent steps.

After aggregation, each variant was represented by 1,500 independent key-level observations, for a total of 4,500 observations.

For each feature, the central tendency and distribution of the groups were examined, and differences among the three groups were assessed using the nonparametric Kruskal–Wallis test [17]. To evaluate not only statistical significance but also the magnitude of the differences, epsilon-squared (ε^2) effect size was calculated [18]. The significance level was set at $\alpha = 0.05$ [19]; accordingly, $p < 0.05$ was interpreted as evidence of a statistically significant overall difference among the groups.

The Kruskal–Wallis test was used as the primary inferential analysis. In addition, one-way ANOVA and eta-squared (η^2) were calculated from the key-level sample sizes, means, and standard deviations reported in Table 1 and treated as a complementary sensitivity check [20]. Differences between pairs of variants were standardized using the pooled standard deviation, with the Hedges g correction applied [21]. For each variant,

95% confidence intervals for the mean were calculated using mean ± 1.96×SD/√n [22]. To summarize the joint separation across the four features, the Euclidean norm of the pairwise standardized differences was also calculated. This value was reported solely as a descriptive measure of the joint profile difference across the selected features.

Sample-size sensitivity was also examined. For a three-group one-way ANOVA with $\alpha = 0.05$, 80% power, and $f = 0.10$, which Cohen defines as a small effect [23], the G*Power approach requires approximately 969 observations per group [24]. The 1,500 observations per group in this study exceed this requirement. This calculation was used as a sample-size check separate from the primary Kruskal–Wallis analysis.

3. RESULTS AND DISCUSSION

ChaCha8, ChaCha12, and ChaCha20 keystreams were compared in terms of bit ratio, bit transition ratio, Shannon entropy, and autocorrelation. The feature values of the five streams generated from the same key were averaged, yielding 1,500 key-level observations for each variant. Differences among the groups were evaluated using the Kruskal–Wallis test, and effect size was reported as epsilon-squared (ε^2).

3.1. Bit Distribution and Transition Behavior

The mean bit ratio remained close to 0.5 for all three variants: 0.500009 for ChaCha8, 0.499998 for ChaCha12, and 0.500008 for ChaCha20. The difference among the groups did not reach statistical significance ($H = 2.441$, $p = 0.295$), and the effect size was limited to 0.000098.

A similar pattern was observed for the bit transition ratio. The means of the three variants were confined to the range 0.500003–0.500011, the difference was again not significant ($H = 0.593$, $p = 0.743$), and the effect size remained below 0.000001. Taken together, these two measures indicate that reducing the round count from 20 to 12 or 8 did not leave a measurable trace in bit balance or in the frequency of transitions between consecutive bits.

The key-level distributions of the four features for the ChaCha variants are shown together in Figure 1. The substantial overlap among the distributions is consistent with the descriptive finding that the variants do not exhibit a clear separation.

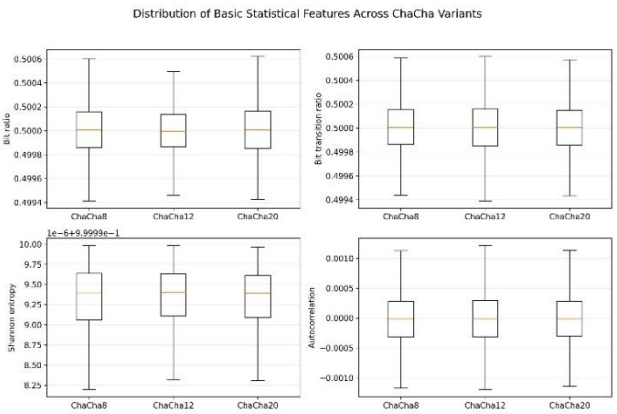


Figure 1. *Key-Level Distributions of Bit Ratio, Bit Transition Ratio, Shannon Entropy and Autocorrelation for ChaCha8, ChaCha12 and ChaCha20 Keystreams*

3.2. Shannon Entropy

Shannon entropy remained close to the theoretical upper bound of 1 bit per bit for all variants. The mean values were 0.999999301 for ChaCha8, 0.999999331 for ChaCha12, and 0.999999300 for ChaCha20. The difference was not statistically significant ($H = 3.152$, $p = 0.207$), and the effect size was 0.000256. All three variants therefore exhibited similar entropy behavior with respect to the distribution of 0 and 1 bits.

This result should be interpreted with the caveat that high entropy alone does not imply cryptographic security. Entropy is a measure based on the probabilities of the bit distribution; statistical tests do not replace cryptanalysis and cannot, by themselves, establish cryptographic security [25].

3.3. Autocorrelation

The mean lag-1 autocorrelation coefficients for ChaCha8, ChaCha12, and ChaCha20 were −0.000023, −0.000011, and −0.000008, respectively. All values were

close to zero, indicating no evident linear relationship between consecutive bits in the examined streams; the difference among the groups was also not significant (H = 0.593, p = 0.743). When the four features were considered together in terms of their deviations from the reference values, no clear separation among the variants was observed; the relative deviations are shown in Figure 2.

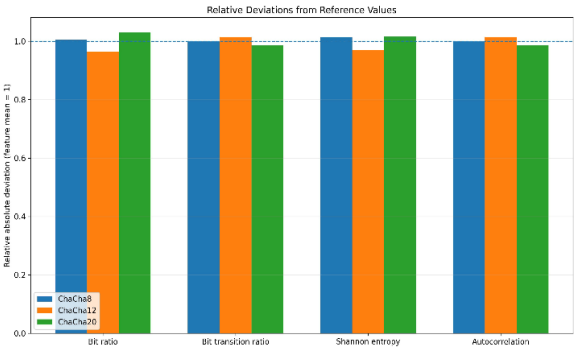


Figure 2. *Relative Deviations of The Statistical Features From Their Expected Reference Values for ChaCha8, ChaCha12 and ChaCha20*

3.4. Statistical Comparison and Overall Assessment of the Variants

The primary comparison was performed using the Kruskal–Wallis test on the observations aggregated at the key level. Each variant was represented by 1,500 independent observations, and the resulting H, p, and epsilon-squared values are summarized in Table 1.

Table 1. Key-Level Statistical Comparison of the ChaCha Variants (Mean ± SD)

Feature	ChaCha8 (Mean ± SD)	ChaCha12 (Mean ± SD)	ChaCha20 (Mean ± SD)	H	p	ε^2
Bit Ratio	0.500009 ± 0.000221	0.499998 ± 0.000213	0.500008 ± 0.000224	2.441	0.295	0.000098
Bit Transition Ratio	0.500011 ± 0.000220	0.500005 ± 0.000223	0.500003 ± 0.000218	0.593	0.743	<0.000001
Shannon Entropy	0.999999301 ± 0.000000439	0.999999331 ± 0.000000410	0.999999300 ± 0.000000441	3.152	0.207	0.000256
Autocorrelation	−0.000023 ± 0.000439	−0.000011 ± 0.000447	−0.000008 ± 0.000437	0.593	0.743	<0.000001

None of the four features showed a significant overall separation among the groups. All epsilon-squared values were 0.000256 or lower, while the highest η^2 value in the complementary analysis was 0.001117. Thus, the differences among the groups were limited in terms of both statistical significance and the reported effect sizes.

When the four measures are considered together, bit ratio and bit transition ratio remain around 0.5, Shannon entropy remains close to 1, and lag-1 autocorrelation remains around 0. These results indicate that reducing the number of rounds from 20 to 12 or 8 does not produce a strong univariate trace in the four selected output measures; however, this assessment is limited to these measures and the experimental setup used here.

3.4.1. Complementary Robustness and Effect-Size Analysis

The one-way ANOVA and eta-squared (η^2) results calculated from the summary statistics in Table 1 are presented in A of Table 2. None of the four features showed a significant overall difference at $\alpha = 0.05$, and the η^2 values remained low. These results are consistent with the Kruskal–Wallis findings.

The 95% confidence intervals calculated for the mean values also indicated closely spaced estimates across the variants. In the pairwise comparisons, the absolute magnitude of the standardized differences corrected with Hedges g did not exceed approximately 0.073. The largest differences were observed for Shannon entropy in the ChaCha8–ChaCha12 and ChaCha12–ChaCha20 pairs (Table 2, B).

Table 2. Complementary Robustness, Effect-Size and Standardized Profile-Distance Results

A. Parametric Robustness Analysis

Feature	F	p	η^2
Bit ratio	1.153	0.316	0.000513
Bit transition ratio	0.536	0.585	0.000238
Shannon entropy	2.515	0.081	0.001117
Autocorrelation	0.486	0.615	0.000216

B. Pairwise Effect Size and Profile Distance

Variant Pair	Max. |g|	Std. distance	Dominant feature
ChaCha8–ChaCha12	0.071	0.0950	Entropy
ChaCha8–ChaCha20	0.037	0.0503	Bit Transition
ChaCha12–ChaCha20	0.073	0.0867	Entropy

Note: ANOVA and η^2 values are complementary robustness results calculated from the summary statistics in Table 1. The standardized distance is the Euclidean norm of the pairwise standardized differences across the four features and was not used as a cryptographic security metric.

3.4.2. Standardized Multivariate Profile Distance

The standardized distances summarizing the joint profile of the four features are presented in B of Table 2. The values remained low, with the smallest distance obtained for the ChaCha8–ChaCha20 pair. For the four selected measures, the profile distance did not increase systematically with the numerical difference in round count.

Bit ratio, bit transition ratio, Shannon entropy, and lag-1 autocorrelation reflect bit-level and short-lag properties. Structural methods such as RX-differences, which generalize rotational differences, are also used in the analysis of ARX constructions [26]. The present result does not indicate that the round count has no effect; rather, it shows that the effect does not become evident in the selected basic statistical measures.

Previous studies on reduced-round ChaCha have investigated key-recovery attacks on 7- and 7.25-round ChaCha using differential-linear cryptanalysis [6]; these studies reported time complexities of 2^189.7 and 2^223.9 for 7- and 7.25-round ChaCha, respectively, corresponding to improvements of 2^17.1 and 2^14.44 over the previous best attacks. Within the higher-order differential-linear framework, attacks on ChaCha6 and ChaCha7 were reported with time complexities of 2^39.07 and 2^135.07, respectively, again improving on previous results [9]. These studies analyze the internal structure of the algorithm using cryptanalytic methods, whereas the present work examines the observable statistical behavior of the generated keystreams. The two approaches do not answer the same question. The absence of a difference in the selected statistical features does not imply that ChaCha8 and ChaCha12 provide the same level of cryptographic security as ChaCha20 [25]. Recent reduced-round ChaCha literature likewise shows that the round count constitutes a separate cryptanalytic dimension of the security margin [11].

The comparison has two main limitations. First, the four measures used here do not cover the full NIST SP 800-22 test suite. That suite comprises multiple statistical tests for randomness assessment [4]; because of the computational cost and the focus of this study, four basic measures were used instead, which narrows the scope of the conclusions. Second, the analyses were based on 128 KB keystreams generated from 1,500 independent keys per variant and five different nonces per key. The findings therefore constitute a comparison within the selected data structure and measures rather than general proof of cryptographic security. Higher-order bit patterns, autocorrelation coefficients at different lags, or more advanced statistical distinguishers may reveal weaker round-dependent differences.

CONCLUSION

This study compared ChaCha8, ChaCha12, and ChaCha20 keystreams using bit ratio, bit transition ratio, Shannon entropy, and lag-1 autocorrelation. Each variant was represented by 1,500 independent keys; the five streams generated from the same key using different nonce values were aggregated at the key level rather than treated as independent observations. The primary Kruskal–Wallis analysis revealed no significant overall difference in any of the four features, and all epsilon-squared values remained below

0.000256.

The complementary analyses supported the same overall pattern. ANOVA p-values ranged from 0.081 to 0.615, η^2 values ranged from 0.000216 to 0.001117, and the absolute pairwise standardized differences did not exceed approximately 0.073. The low multivariate profile distances likewise indicate limited separation among the variants with respect to the selected features.

These findings indicate output-level statistical similarity; they do not establish that ChaCha8 and ChaCha12 provide cryptographic security equivalent to ChaCha20 [25]. Future work may examine higher-order bit patterns, autocorrelation at additional lags, a broader subset of the NIST SP 800-22 tests, and validated multivariate distinguishers applied directly to raw streams to investigate weaker effects of the round count on output behavior.

REFERENCE

[1] D. J. Bernstein, "ChaCha, a variant of Salsa20," in Workshop Record of SASC 2008: The State of the Art of Stream Ciphers, 2008.

[2] M. S. Turan, "On Statistical Analysis of Synchronous Stream Ciphers," Ph.D. dissertation, Middle East Technical University, Ankara, Turkey, 2008.

[3] K. Bhattacharjee and S. Das, "A search for good pseudo-random number generators: Survey and empirical studies," Computer Science Review, vol. 45, Art. no. 100471, 2022, doi: 10.1016/j.cosrev.2022.100471.

[4] L. E. Bassham III et al., A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, NIST Special Publication 800-22 Rev. 1a, National Institute of Standards and Technology, 2010, doi: 10.6028/NIST.SP.800-22r1a.

[5] J. Pfau, M. Reuter, T. Harbaum, K. Hofmann, and J. Becker, "A Hardware Perspective on the ChaCha Ciphers: Scalable ChaCha8/12/20 Implementations Ranging from 476 Slices to Bitrates of 175 Gbit/s," in Proc. 2019 32nd IEEE International System-on-Chip Conference (SOCC), pp. 294–299, 2019, doi: 10.1109/SOCC46988.2019.1570548289.

[6] Z. Xu, H. Xu, L. Tan, and W. Qi, "Differential-Linear Cryptanalysis of Reduced Round ChaCha," IACR Transactions on Symmetric Cryptology, vol. 2024, no. 2, pp. 166–189, 2024, doi: 10.46586/tosc.v2024.i2.166-189.

[7] N. K. Sharma and S. Dey, "Analyzing the Probability of Key Recovery in the Differential Attacks Against ChaCha," IEEE Access, vol. 12, pp. 37000–37011, 2024, doi: 10.1109/ACCESS.2024.3372857.

[8] S. Dey, H. K. Garai, S. Sarkar, and N. K. Sharma, "Enhanced Differential-Linear Attacks on Reduced Round ChaCha," IEEE Transactions on Information Theory, vol. 69, no. 8, pp. 5318–5336, 2023, doi: 10.1109/TIT.2023.3269790.

[9] N. Ghafoori and A. Miyaji, "Higher-Order Differential-Linear Cryptanalysis of ChaCha Stream Cipher," IEEE Access, vol. 12, pp. 13386–13399, 2024, doi: 10.1109/ACCESS.2024.3356868.

[10] S. Sahoo, D. Chakraborty, and S. Sarkar, "Chasing Shadows: Advancements in Differential-Linear Cryptanalysis for ChaCha," IEEE Transactions on Information Theory, vol. 71, no. 8, pp. 6451–6469, 2025, doi: 10.1109/TIT.2025.3577784.

[11] Y. Okada, R. Watanabe, N. Ghafoori, and A. Miyaji, "Improved Differential-Linear Cryptanalysis of Reduced Rounds of ChaCha Permutation," IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol. E108-A, no. 9, pp. 1175–1195, Sep. 2025, doi: 10.1587/transfun.2024DMP0008.

[12] Y. Nir and A. Langley, "ChaCha20 and Poly1305 for IETF Protocols," RFC 8439, Jun. 2018, doi: 10.17487/RFC8439.

[13] J. Strömbergson, "Test Vectors for the Stream Cipher ChaCha," Internet-Draft draft-strombergson-chacha-test-vectors-01, Dec. 2013. [Online]. Available: https://datatracker.ietf.org/doc/draft-strombergson-chacha-test-vectors/ (accessed Sep. 30, 2026).

[14] D. J. C. MacKay, Information Theory, Inference, and Learning Algorithms. Cambridge, U.K.: Cambridge University Press, 2003.

[15] T. M. Cover and J. A. Thomas, Elements of Information Theory, 2nd ed. Hoboken, NJ, USA: Wiley-Interscience, 2006, doi: 10.1002/047174882X.

[16] G. E. P. Box, G. M. Jenkins, G. C. Reinsel, and G. M. Ljung, Time Series Analysis: Forecasting and Control, 5th ed. Hoboken, NJ, USA: Wiley, 2015.
[17] A. Vargha and H. D. Delaney, "The Kruskal-Wallis Test and Stochastic Homogeneity," Journal of Educational and Behavioral Statistics, vol. 23, no. 2, pp. 170–192, 1998, doi: 10.3102/10769986023002170.
[18] M. Tomczak and E. Tomczak, "The need to report effect size estimates revisited. An overview of some recommended measures of effect size," Trends in Sport Sciences, vol. 21, no. 1, pp. 19–25, 2014.
[19] J. S. Spence and D. Stanley, "Concise, Simple, and Not Wrong: In Search of a Short-Hand Interpretation of Statistical Significance," Frontiers in Psychology, vol. 9, Art. no. 2185, 2018, doi: 10.3389/fpsyg.2018.02185.
[20] D. Lakens, "Calculating and reporting effect sizes to facilitate cumulative science: a practical primer for t-tests and ANOVAs," Frontiers in Psychology, vol. 4, Art. no. 863, 2013, doi: 10.3389/fpsyg.2013.00863.
[21] L. V. Hedges, "Distribution Theory for Glass's Estimator of Effect Size and Related Estimators," Journal of Educational Statistics, vol. 6, no. 2, pp. 107–128, 1981, doi: 10.3102/10769986006002107.
[22] G. Cumming, "The New Statistics: Why and How," Psychological Science, vol. 25, no. 1, pp. 7–29, 2014, doi: 10.1177/0956797613504966.
[23] J. Cohen, Statistical Power Analysis for the Behavioral Sciences, 2nd ed. Hillsdale, NJ, USA: Lawrence Erlbaum Associates, 1988.
[24] F. Faul, E. Erdfelder, A.-G. Lang, and A. Buchner, "G*Power 3: A flexible statistical power analysis program for the social, behavioral, and biomedical sciences," Behavior Research Methods, vol. 39, no. 2, pp. 175–191, 2007, doi: 10.3758/BF03193146.
[25] E. Simion, "The Relevance of Statistical Tests in Cryptography," IEEE Security & Privacy, vol. 13, no. 1, pp. 66–70, 2015, doi: 10.1109/MSP.2015.16.
[26] T. Ashur and Y. Liu, "Rotational Cryptanalysis in the Presence of Constants," IACR Transactions on Symmetric Cryptology, vol. 2016, no. 1, pp. 57–70, 2016, doi: 10.46586/tosc.v2016.i1.57-70.