UDC 003.26

Pseudorandomness Analysis of Ciphertexts in the AJPS-2 Cryptosystem

Yurii Doroshenko[1], Dariya Yadukha[1]

[1]*National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Institute of Physics and Technology*

Abstract

This paper investigates the post-quantum cryptographic primitive AJPS-2 based on arithmetic modulo Mersenne numbers. We describe modified versions of this cryptosystem that utilize generalized Mersenne numbers and Crandall numbers as moduli. We conduct a comparative analysis of ciphertext pseudorandomness for the original cryptosystem and its modifications using the NIST SP 800-22 pseudorandomness test suite. The results show that the use of alternative moduli increases the overall stability and parameters variability of the AJPS-2 cryptosystem.

Keywords: AJPS cryptosystem, post-quantum cryptography, Mersenne numbers, generalized Mersenne numbers, Crandall numbers

Introduction

The advent of scalable quantum computers, which may compromise modern asymmetric cryptosystems, creates an urgent need for new cryptographic primitives that can ensure security in the presence of quantum computing. Post-quantum cryptography is a field that develops primitives resistant to attacks using both classical and quantum computers.

In 2017, the U.S. National Institute of Standards and Technology (NIST) launched an open competition on post-quantum cryptographic primitives, aiming to identify secure quantum-resistant schemes and establish the first standards for post-quantum cryptography [1].

Among the early research efforts in this area was the cryptosystem AJPS-2, designed around modular arithmetic with Mersenne numbers [2]. This paper focuses on the AJPS-2 cryptosystem and its modifications.

The AJPS family of cryptosystems is built on arithmetic modulo Mersenne numbers, which is advantageous as it provides numerous optimizations for computationally intensive modular operations [3].

1. Terms and Notation

- M_n — Mersenne number of the form $2^n - 1$, where $n \in \mathbb{N}$;
- $M_{n,c}$ — Crandall number of the form $2^n - c$, where n and c are positive integers and $\log_2 c \leq \frac{n}{2}$;
- $M_{n,m}$ — generalized Mersenne number of the form $2^n - 2^m - 1$, where n, m are positive integers and $m < n$;
- The Hamming weight of a number x is defined as the number of 1's in its binary representation.

2. The AJPS-2 Cryptosystem

The security of the AJPS-2 cryptosystem is based on the *Mersenne Low Hamming Combination Search Problem* (MLHCSP).

Definition 1. *(MLHCSP) Let the following be given: a Mersenne number M_n, an integer $h < n$, and a pair of numbers (R, T), where R is a randomly chosen residue modulo M_n, and T is computed as*

$$T = F \cdot R + G \bmod M_n,$$

where F and G are residues modulo M_n with Hamming weight h. The problem is to find such F and G given M_n, h, R, and T.

The AJPS-2 cryptosystem encrypts a message block of length λ, where λ is the security parameter. In practice, it is reasonable to choose the block length equal to the security parameter. Thus, below we describe a scheme for encrypting a message block $M \in \{0,1\}^\lambda$.

The public parameters of the cryptosystem are:

- the Mersenne number $M_n = 2^n - 1$;
- an integer $h \in \mathbb{N}$ satisfying $h = \lambda$, $10h^2 < n \leq 16h^2$;
- the encoding and decoding algorithms of an error correcting code:

$$\mathcal{E} : \{0,1\}^\lambda \to \{0,1\}^n;$$

$$\mathcal{D} : \{0,1\}^n \to \{0,1\}^\lambda.$$

For the cryptosystem to be $(1-\delta)$-correct, where δ is the error probability, it must hold that

$$\forall M \in \{0,1\}^\lambda :$$

$$\Pr\left(\mathcal{D}((C_1 \cdot F \bmod M_n) \oplus C_2) = M\right) \geq 1 - \delta.$$

Key Generation. Randomly choose F and G – residues modulo M_n with Hamming weight h. Randomly select R modulo M_n and compute

$$T = F \cdot R + G \bmod M_n.$$

The public key is the pair (R, T); the secret key is F.

Encryption. To encrypt a message M, independently and uniformly choose A, B_1, B_2 – residues modulo M_n with Hamming weight h, and compute

$$C_1 = A \cdot R + B_1 \bmod M_n,$$

$$C_2 = (A \cdot T + B_2 \bmod M_n) \oplus \mathcal{E}(M).$$

The ciphertext is the pair (C_1, C_2).

Decryption. Recover the message as

$$M = \mathcal{D}\big((C_1 \cdot F \bmod M_n) \oplus C_2\big).$$

The choice of the error-correcting code $(\mathcal{E}, \mathcal{D})$ plays a crucial role in ensuring the reliability and correctness of the AJPS-2 cryptosystem.

Claim 1. [2] *The AJPS-2 cryptosystem is $(1-\delta)$-correct if the error correction code $(\mathcal{E}, \mathcal{D})$ corrects up to*

$$(4h^2 + 2h)(1 + \varepsilon)$$

errors for some value ε, $0 < \varepsilon < 1$, which satisfies the following condition:

$$2^{-\frac{(2h^2-1)\varepsilon^2}{6}} < \delta.$$

3. Modifications of the AJPS-2 Cryptosystem

As noted earlier, arithmetic modulo a Mersenne number can be efficiently implemented using specialized algorithms for computationally expensive operations such as inversion, multiplication, and others. However, Mersenne numbers are not the only class of numbers for which efficient modular algorithms exist. In fact, many algorithms originally developed for Mersenne numbers can also be adapted to Crandall numbers and generalized Mersenne numbers [3].

In cryptography, the use of prime moduli is not only advantageous but often also a strict requirement, since composite moduli introduce zero divisors that can be exploited in attacks. A prime modulus ensures that the residue ring forms a field, guaranteeing uniform value distribution and the existence of multiplicative inverses for all nonzero elements.

However, the set of available Mersenne primes is limited: currently only 52 are known, with the most recent (the 52nd) discovered at the end of 2024 [4]. Most of these primes are either too large for efficient use in cryptographic primitives or too small to satisfy modern security requirements. To address this limitation, alternative number classes can be employed.

For practical validation, the implementation of AJPS-2 with alternative moduli was developed and tested. The code, including algorithms for parameter search and modular arithmetic with generalized Mersenne and Crandall numbers, is publicly available in the accompanying repository [5].

3.1. AJPS-2 Modifications Based on Alternative Moduli

The AJPS-2 cryptosystem can be adapted to work with alternative moduli, namely generalized Mersenne numbers $M_{n,m}$ and Crandall numbers $M_{n,c}$. In both cases, the security of the scheme is based on the hardness of a corresponding low Hamming weight combination problem.

Definition 2 (GMLHCSP)**.** *Let a generalized Mersenne number $M_{n,m}$, an integer h, and a pair (R, T) be given, where R is a random residue modulo $M_{n,m}$ and*

$$T = F \cdot R + G \bmod M_{n,m},$$

with F, G residues modulo $M_{n,m}$ of Hamming weight h. The problem is to recover F and G given $M_{n,m}, h, R$, and T.

Definition 3 (CLHCSP)**.** *Let a Crandall number $M_{n,c}$, an integer h, and a pair (R, T) be given, where R is a random residue modulo $M_{n,c}$ and*

$$T = F \cdot R + G \bmod M_{n,c},$$

with F, G residues modulo $M_{n,c}$ of Hamming weight h. The problem is to recover F and G given $M_{n,c}, h, R$, and T.

Note (*Notation $M_{n,m/c}$*): In what follows, the notation $M_{n,m/c}$ is used as a shorthand to indicate that the described operation or construction can be applied with either a generalized Mersenne modulus $M_{n,m}$ or a Crandall modulus $M_{n,c}$, depending on the chosen variant of the cryptosystem.

Key Generation. Randomly select F, G with Hamming weight h modulo the chosen modulus $M_{n,m/c}$. Randomly choose R modulo the same modulus, and compute

$$T = F \cdot R + G \bmod M_{n,m/c}.$$

The public key is (R, T); the secret key is F.

Encryption. To encrypt M, select A, B_1, B_2 uniformly at random with Hamming weight h modulo M, and compute

$$C_1 = A \cdot R + B_1 \bmod M_{n,m/c},$$

$$C_2 = (A \cdot T + B_2 \bmod M_{n,m/c}) \oplus \mathcal{E}(M).$$

Decryption. Decrypt the message as

$$M = \mathcal{D}((C_1 \cdot F \bmod M_{n,m/c}) \oplus C_2).$$

Building on the original AJPS-2 construction, further modifications were proposed by adapting the scheme to alternative moduli, such as generalized Mersenne numbers. These variants inherit the same design principles but require adjusted correctness conditions, as established in [6].

Claim 2. *A modification of the AJPS-2 cryptosystem using arithmetic modulo generalized Mersenne number $M_{n,m}$ is $(1-\delta)$-correct if the error correction code $(\mathcal{E}, \mathcal{D})$ corrects up to*

$$(4h^2 + 4mh - 2h)(1 + \varepsilon)$$

errors for some value ε, $0 < \varepsilon < 1$, which satisfies the following condition:

$$2^{-2(h^2+(m-1)h)\frac{\varepsilon^2}{3}} \left(1 + 2^{-\frac{2h\varepsilon^2}{3}}\right) < \delta.$$

Similarly, when the AJPS-2 cryptosystem is modified to operate modulo a Crandall number, the correctness guarantee depends on more complex parameter interactions. The corresponding result, proven in [6], is stated below.

Claim 3. *A modification of the* AJPS-2 *cryptosystem using arithmetic modulo Crandall number $M_{n,c}$ is $(1-\delta)$-correct if the error correction code $(\mathcal{E}, \mathcal{D})$ corrects up to*

$$(4(c - 2^m)h^2 + 2h(2m + 2c + 2^{m+1} - 3) + 2(c - 2^m - 1))(1 + \varepsilon)$$

errors, where $c = 2^m + 1 + k$, $m, k \in \mathbb{N}$, and ε, $0 < \varepsilon < 1$, which satisfies the following condition:

$$2^{-2\left((c-2^m)h^2+(m+c-2^m-2)h\right)\frac{\varepsilon^2}{3}} \times \times \left(1 + 2^{-(h+c-2^m-1)\frac{\varepsilon^2}{3}}\right) < \delta.$$

4. NIST SP 800-22 Tests

NIST SP 800-22 is a suite of 15 statistical tests developed by the U.S. National Institute of Standards and Technology (NIST) to evaluate the randomness of bit sequences, particularly those used in cryptography. The standard provides methods for detecting deviations from truly random behavior. A detailed description of each test can be found on the NIST website [7].

The p-value represents the probability that, for a truly random sequence, the test result would be at least as extreme as that obtained for the sequence under investigation. Within the NIST SP 800-22 framework, the minimum acceptable p-value for all tests is 0.01.

For all subsequent evaluations of each cryptosystem variant, files containing 16 million bits were generated. To obtain statistically significant results, each file was divided into blocks of length 1,000,000 bits, producing 16 independent blocks. This approach increases the reliability of the results by enabling the analysis of statistical characteristics over a larger number of independent samples.

Overview of NIST SP 800-22 Statistical Tests

- **Frequency (Monobit) Test:** Evaluates whether the total number of ones and zeros in the entire sequence is approximately equal, as expected for a random sequence.
- **Frequency Within a Block Test:** Checks whether each fixed-size block contains roughly $\frac{M}{2}$ ones. This test detects local deviations from uniformity.
- **Runs Test:** Counts runs of consecutive identical bits. It verifies whether the sequence switches between zeros and ones too frequently or too rarely.
- **Longest Run of Ones in a Block Test:** Examines the longest run of ones in each M-bit block and compares it with the distribution expected for a random sequence.
- **Random Binary Matrix Rank Test:** Analyzes ranks of fixed-size binary matrices formed from the sequence to detect linear dependencies among substrings.
- **Discrete Fourier Transform (Spectral) Test:** Uses FFT peak analysis to detect periodicities or repeating patterns that would indicate non-random structure.
- **Non-Overlapping Template Matching Test:** Counts occurrences of a given non-overlapping m-bit pattern. An excessive number of matches suggests structural bias.
- **Overlapping Template Matching Test:** Similar to the previous test, but windows overlap. It evaluates whether the number of overlapping occurrences of a pattern is consistent with randomness.
- **Maurer's Universal Statistical Test:** Measures sequence compressibility. Highly compressible sequences contain patterns inconsistent with randomness.
- **Linear Complexity Test:** Checks whether the sequence requires a sufficiently long linear feedback shift register (LFSR) for generation. A short LFSR indicates low complexity.
- **Serial Test:** Counts occurrences of all possible overlapping m-bit patterns and verifies whether frequencies match the expected distribution.
- **Approximate Entropy Test:** Compares the frequency of overlapping patterns of lengths m and $m+1$, evaluating predictability and local structural regularity.
- **Cumulative Sums (Cusum) Test:** Analyzes the maximal deviation in the random walk defined by mapping bits to $\{-1, +1\}$. Large excursions from zero indicate non-random behavior.
- **Random Excursions Test:** Counts how many times a cumulative-sum random walk completes cycles visiting a given state exactly K times. Deviations suggest irregularity in walk behavior.
- **Random Excursions Variant Test:** Counts the total number of visits to each state in the cumulative-sum random walk. It detects finer trajectory-level irregularities than the standard excursions test.

4.1. Search of suitable parameters

During the testing of AJPS-2, it was necessary to find prime generalized Mersenne and Crandall numbers of the recommended length ($n = 756839$). Primality testing with the Miller-Rabin algorithm proved too slow, requiring at least 20 minutes per candidate number.

To overcome this, the parameter size was reduced to: $n = 11213$, $h = 33$, $\lambda = 33$, $c = 7713$, $m = 9953$.

Under these conditions, suitable parameters were found in under an hour, but the maximum encrypted block length was decreased to 33 bits instead of the original 264 bits.

For the comparative analysis of AJPS-2 and its modular modifications, pseudorandomness testing was performed on the ciphertexts C_1 and C_2 obtained by encrypting a randomly chosen message.

4.2. AJPS-2 Tests Results

As shown in Tables 1 and 2, all three modulus variants pass every NIST SP 800-22 test for both ciphertext components C_1 and C_2 with comfortably high p-values (in all cases $p \geq 0.15$ for significance level $\alpha = 0.01$). Thus, for each modulus choice and for each component of the AJPS-2 ciphertext, the null hypothesis of randomness cannot be rejected for any test in the suite.

A consistent pattern across both tables is that the generalized Mersenne modulus $M_{n,m}$ yields the most stable and typically the highest p-values in the majority of tests.

Table 1
AJPS-2: Pseudorandomness results for ciphertext C_1

Test	M_n	$M_{n,c}$	$M_{n,m}$
Frequency (Monobit)	0.2131	0.5025	0.2976
Frequency within Block	0.3467	0.4518	0.6837
Runs Test	0.7941	0.5833	0.4956
Longest Run of Ones	0.7553	0.8010	0.5639
Binary Matrix Rank	0.6121	0.3904	0.7342
Spectral Test	0.4327	0.4486	0.6791
Non-overlapping Temp.	0.8824	0.1531	0.7234
Overlapping Template	0.6180	0.4891	0.6883
Universal Statistical Test	0.1938	0.7657	0.6081
Linear Complexity	0.2012	0.3824	0.7006
Serial Test (1)	0.5825	0.2450	0.8422
Serial Test (2)	0.5373	0.3051	0.8013
Approximate Entropy	0.4696	0.3682	0.8115
Cumulative Sums (F)	0.2741	0.5286	0.4594
Cumulative Sums (B)	0.2968	0.3447	0.4967

Table 2
AJPS-2: Pseudorandomness results for ciphertext C_2

Test	M_n	$M_{n,c}$	$M_{n,m}$
Frequency (Monobit)	0.2097	0.5376	0.2829
Frequency within Block	0.3094	0.4783	0.6724
Runs Test	0.7515	0.5967	0.4994
Longest Run of Ones	0.7610	0.8179	0.5405
Binary Matrix Rank	0.6075	0.3721	0.7166
Spectral Test	0.4264	0.4616	0.6596
Non-overlapping Temp.	0.8543	0.1514	0.7333
Overlapping Temp.	0.6056	0.4829	0.6867
Universal Statistical Test	0.1870	0.7730	0.6089
Linear Complexity	0.1935	0.3410	0.7142
Serial Test (1)	0.5714	0.2340	0.8488
Serial Test (2)	0.5261	0.2938	0.7920
Approximate Entropy	0.4605	0.3582	0.8026
Cumulative Sums (F)	0.2663	0.5109	0.4516
Cumulative Sums (B)	0.2875	0.3316	0.4802

For C_1, $M_{n,m}$ notably improves the block-oriented and structural statistics, with *Frequency within Block* equal to 0.6837, *Serial Test (1)* equal to 0.8422, *Approximate Entropy* equal to 0.8115, and *Linear Complexity* equal to 0.7006. A similar effect is observed for C_2, where the corresponding values are 0.6724, 0.8488, 0.8026, and 0.7142, respectively. These values are not only far above the rejection threshold but also well away from the extremes of the $[0, 1]$ interval, which is typically interpreted as an indication of stable, non-pathological behavior of the test statistics.

The Crandall modulus $M_{n,c}$ exhibits slightly more variability. In particular, it shows lower but still acceptable p-values in the template-based tests, with *Non-overlapping Template* equal to 0.1531 for C_1 and 0.1514 for C_2. These values remain well above the 0.01 cutoff and therefore do not constitute evidence of a systematic deviation from randomness; however, they indicate that the template structure is somewhat more sensitive to this choice of modulus. By contrast, the original Mersenne modulus M_n tends to produce the lowest p-values in several complexity-oriented tests, most visibly in the *Universal Statistical Test* (0.1938 for C_1 and 0.1870 for C_2) and *Linear Complexity* (0.2012 for C_1 and 0.1935 for C_2). Even in these cases, the results remain comfortably above the rejection threshold, but they highlight that $M_{n,m}$ and, to a lesser extent, $M_{n,c}$ lead to a more favorable distribution of p-values.

Table 3
AJPS-2: Random Excursions results for C_1

State	M_n	$M_{n,c}$	$M_{n,m}$
-4	0.2973	0.3485	0.3823
-3	0.3417	0.3252	0.3720
-2	0.3221	0.3287	0.3862
-1	0.3490	0.3462	0.3684
+1	0.3345	0.3114	0.3971
+2	0.3511	0.3637	0.3515
+3	0.3594	0.3321	0.3743
+4	0.3410	0.3209	0.3829

The Random Excursions test results, summarized separately for C_1 and C_2 in Tables 3 and 4, lie in a relatively tight band (approximately 0.31-0.40 across all states and all modulus variants). This behavior is consistent for both ciphertext components and shows no trajectory-level anomalies in the underlying random walk induced by the partial sums of the bitstream.

Table 4
AJPS-2: Random Excursions results for C_2

State	M_n	$M_{n,c}$	$M_{n,m}$
-4	0.2962	0.3480	0.3881
-3	0.3389	0.3226	0.3680
-2	0.3199	0.3258	0.3826
-1	0.3454	0.3422	0.3653
+1	0.3297	0.3156	0.3933
+2	0.3502	0.3575	0.3536
+3	0.3575	0.3312	0.3674
+4	0.3395	0.3198	0.3750

The generalized Mersenne modulus $M_{n,m}$ again tends to produce slightly more concentrated and centred p-values (for example, 0.3515-0.3971 for C_1 and 0.3536-0.3933 for C_2), while M_n and $M_{n,c}$ track closely behind with comparable stability.

Table 5
AJPS-2: Random Excursions Variant results for C_1

State	M_n	$M_{n,c}$	$M_{n,m}$
-9	0.3284	0.2877	0.3674
-8	0.3561	0.3140	0.3799
-7	0.4622	0.3458	0.4057
-6	0.3825	0.4923	0.4271
-5	0.3276	0.3593	0.4435
-4	0.4010	0.2991	0.3827
-3	0.3983	0.3852	0.4411
-2	0.3617	0.3247	0.4539
-1	0.3554	0.3743	0.3497
+1	0.3185	0.3415	0.4276
+2	0.3923	0.3723	0.4098
+3	0.3675	0.3466	0.3784
+4	0.3121	0.3044	0.4035
+5	0.2926	0.3412	0.4263
+6	0.4045	0.3182	0.3891
+7	0.3430	0.3622	0.4055
+8	0.2843	0.3445	0.3437
+9	0.3127	0.3073	0.3468

Table 6
AJPS-2: Random Excursions Variant results for C_2

State	M_n	$M_{n,c}$	$M_{n,m}$
-9	0.3291	0.2834	0.3628
-8	0.3583	0.3110	0.3745
-7	0.4427	0.3557	0.4001
-6	0.3805	0.4847	0.4215
-5	0.3248	0.3559	0.4380
-4	0.3986	0.2883	0.3795
-3	0.3965	0.3780	0.4386
-2	0.3596	0.3198	0.4521
-1	0.3521	0.3712	0.3541
+1	0.3148	0.3391	0.4237
+2	0.3904	0.3683	0.4043
+3	0.3650	0.3414	0.3753
+4	0.3086	0.3038	0.4009
+5	0.2897	0.3375	0.4258
+6	0.4072	0.3133	0.3875
+7	0.3476	0.3595	0.4040
+8	0.2819	0.3389	0.3412
+9	0.3097	0.3022	0.3444

Random Excursions Variant results are reported in Tables 5 and 6. Here the p-values span a somewhat broader but still healthy range of roughly 0.28-0.49 across states. The $M_{n,m}$ variant remains consistently strong, typically achieving $p \geq 0.34$ for both C_1 and C_2, which further supports the conclusion that this modulus choice leads to particularly robust trajectory-level behavior. The Crandall modulus $M_{n,c}$ shows occasional lower values (for instance, 0.2877 for C_1 at state -9 and 0.2834 for C_2 at state -9), but these remain well above the 0.01 significance threshold and do not indicate statistically significant irregularities.

Overall, the disaggregated analysis of C_1 and C_2 confirms that both ciphertext components exhibit very similar pseudorandomness profiles under all three modulus families. At the same time, the use of generalized Mersenne moduli $M_{n,m}$ systematically improves the centrality and stability of the p-values across the NIST SP 800-22 test suite, suggesting that this choice of modulus enhances the robustness of the AJPS-2 ciphertext pseudorandomness without introducing detectable biases in either component.

Conclusions

In this paper, we analyzed the AJPS-2 cryptosystem together with its modified versions constructed using Crandall numbers and generalized Mersenne numbers. The primary goal of this research was to investigate how alternative modulus families influence the statistical properties of ciphertexts, with a particular emphasis on pseudorandomness. To this end, all implementations were evaluated using the NIST SP 800-22 statistical test suite, which provides a comprehensive set of benchmarks for assessing the randomness of binary sequences.

The experimental results demonstrate that all AJPS-2 variants achieve consistently high p-values across the entire test suite, significantly exceeding the standard rejection threshold of 0.01. This confirms that neither the choice of modulus nor the structural modifications introduce detectable statistical weaknesses into the ciphertexts. Among the examined modulus families, the generalized Mersenne modulus stands out as the most stable option: it produces the strongest and most uniform outcomes in the majority of tests, particularly in those sensitive to structural regularities, such as the Serial, Approximate Entropy, and Linear Complexity tests. The Crandall modulus also performs well overall, although occasional minor reductions in template-based tests suggest slightly increased sensitivity to local bit-pattern distributions. Nevertheless, all such outliers remain comfortably above the rejection threshold and therefore do not indicate any statistically significant anomalies.

- All tested implementations of AJPS-2 satisfy the requirements of the NIST SP 800-22 test suite, with no cases of statistical rejection.
- Variants based on generalized Mersenne numbers exhibit the most stable behavior, producing the highest and most uniform p-values across all examined statistical tests.
- The consistency of results across both ciphertext components (C_1 and C_2) demonstrates the internal robustness of the AJPS-2 design and confirms that modulus substitutions do not disrupt the cryptosystem's structural balance.
- The introduction of alternative modulus families (especially generalized Mersenne numbers) appears to be a promising direction for enhancing the flexibility, implementation efficiency, and statistical resilience of AJPS-family post-quantum schemes.

Overall, the conducted analysis confirms the correctness of the AJPS-2 modifications based on Crandall and generalized Mersenne numbers, as well as their ability to generate ciphertexts that exhibit strong and stable pseudorandomness. These findings support the feasibility of further extending the AJPS framework using non-standard modulus classes without compromising its statistical or structural security properties.

References

[1] National Institute of Standards and Technology, "Post-quantum cryptography standardization." https://csrc.nist.gov/pqc-standardization, 2025. Accessed: 2025-11-01.

[2] D. Aggarwal, A. Joux, A. Prakash, and M. Santha, "A New Public-Key Cryptosystem via Mersenne Numbers," IACR Cryptology ePrint Archive, 2017.

[3] J.-C. Bajard, L. Imbert, and T. Plantard, "Modular Number Systems: Beyond the Mersenne Family," in Selected Areas in Cryptography, vol. 3357 of Lecture Notes in Computer Science, Springer, 2004.

[4] I. Mersenne Research, "52nd Known Mersenne Prime Discovered." https://www.mersenne.org/primes/press/M136279841.html, 2024. Accessed: 2025-11-01.

[5] Y. Doroshenko, "Analysis of AJPS-Family Cryptosystems." https://github.com/lol1chan/ajps_analysis, 2024. Accessed: 2025-06-07.

[6] D. Yadukha, "The Forgery Attack on the Post-Quantum AJPS-2 Cryptosystem and Modification of the AJPS-2 Cryptosystem by Changing the Class of Numbers Used as a Module," Theoretical and Cryptographic Problems of Cybersecurity, vol. 1, 2023.

[7] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo, "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications," no. SP 800-22, 2010.