JFES CRYPTOGRAPHIC FOUNDATION COMPARISON

An Experiment Comparing JFES with Established High-Quality Cryptographic Transformations

Foundation Quality Report • Portalz JFES • October 2026

Executive Summary

JFES is built on a different foundation from conventional cryptographic engines. Its transformation material is derived from recursive navigation through the Mandelbrot field, whose boundary has been mathematically established as having Hausdorff dimension two—the maximum possible dimension for a subset of the complex plane. The companion paper, “Unpredictability as the Optimal Measure of Entropy,” develops the resulting proposition: infinite mathematical complexity provides an enormous space of possible trajectories; recursive navigation through that space provides access to unpredictable transformation material; that unpredictability is the operational quality sought from entropy.

JFES then turns that principle into an engineered cryptographic method. It does not use a random-number generator as the source of its transformation stream. The JFES transformation engine recursively evaluates the Mandelbrot field and uses the resulting values to determine subsequent locations and transformation material. The separate UUID mechanism supplies the single-use OTP prefix; that RNG-dependent framing mechanism is not the source of the JFES transformation engine.

The purpose of this Foundation Quality Report is to test the resulting cryptographic output against established high-quality reference transformations. The comparison is deliberately direct. JFES was evaluated alongside AES-256-CTR, ChaCha20, an operating-system cryptographically secure random source, x86 RDRAND, AES-256-GCM, and ChaCha20-Poly1305 under the same controlled output-size conditions.

The resulting comparison matrix is the central empirical evidence in this report. Across 210 analysed samples per method, JFES produced byte-level statistical characteristics alongside the reference methods. Its mean entropy was 7.973129 bits per byte, its mean serial correlation was 0.000239, and its mean DEFLATE ratio was 1.001591. The reference methods occupied the same narrow region of measured behaviour. The selected SP 800-22-formula battery likewise produced no suite-adjusted alert for JFES.

These results do not constitute a complete cryptanalysis or a formal proof of cryptographic security. They do, however, establish a substantial empirical foundation for the proposition that JFES’s infinitely-complex fractal transformation method produces cryptographic-quality output. The significance is the combination: an independently grounded mathematical entropy source, an engineered method for recursively extracting and applying that source, and observed output characteristics comparable with established cryptographic transformations.

1. The JFES Foundation

1.1 Infinite Complexity Is the Entropy Source

The starting point is not simply that the Mandelbrot set is “complex.” The relevant mathematical result is that the boundary of the Mandelbrot set has Hausdorff dimension two, established by Mitsuhiro Shishikura. For a subset of the complex plane, two is the maximum possible Hausdorff dimension. The companion paper uses this result as the foundation for describing the Mandelbrot field as an infinitely complex mathematical structure.

1.2 JFES Is the Engineered Extraction Method

JFES does not linearly scan the Mandelbrot set. It recursively navigates it. A selected location is evaluated through Mandelbrot iteration. Values produced during that evaluation determine the next location. That location is evaluated again, and the process continues. The field therefore determines the trajectory through the field.

The essential logic is straightforward: infinite mathematical complexity provides a vast space of possible trajectories; recursive navigation provides a method for traversing that space; the future trajectory is obtained through continued transformation rather than being presented as a precomputed random sequence. JFES has therefore engineered a repeatable standard method for extracting transformation material from the underlying fractal source and applying it to payload transformation.

1.3 From Complexity to Unpredictability

The central proposition of the companion paper is that the cryptographic value of entropy is its unpredictability. A sequence can have balanced statistics and still be predictable. Conversely, an unpredictable outcome can contain substantial structure. The relevant question is therefore not simply whether output looks random, but whether an observer can determine the future transformation trajectory from the information available to them.

For JFES, the proposed chain is: Infinite Complexity → Recursive Trajectory Space → Unpredictability → Entropy. The Foundation Quality Report examines the next consequence of that chain: whether the resulting transformation material exhibits the measurable characteristics expected of high-quality cryptographic output.

2. Experimental Comparison

The controlled experiment compared the captured public JFES implementation with seven available methods: AES-256-CTR, ChaCha20, operating-system CSPRNG output, x86 RDRAND, AES-256-GCM, and ChaCha20-Poly1305, together with JFES. Each method contributed 210 analysed samples, giving 1,470 samples across the seven methods.

It is important to distinguish the design objectives of the reference technologies from those of JFES. AES-256-CTR, ChaCha20, operating-system CSPRNGs, RDRAND, AES-256-GCM, and ChaCha20-Poly1305 are mature cryptographic or cryptographically oriented technologies whose designs are *specifically intended* to produce outputs with strong statistical properties and resistance to observable structure. Their performance against statistical tests used in this comparison is therefore an intentional consequence of their design.

JFES was not developed by tuning its output against this statistical test battery. Its transformation mechanism derives from the recursive navigation of the Mandelbrot field and the extraction and application of transformation material from that process. The statistical behavior observed in this experiment is therefore not the result of optimizing JFES against the tests being applied.

This makes the comparison significant. A fundamentally different entropy generation architecture, using Infinite Complexity as its entropy source and recursive navigation as its extraction mechanism, produces output whose measured statistical properties occupy the same statistical territory as mature cryptographic technologies specifically engineered to exhibit those properties.

The comparison therefore does not merely establish that JFES can pass statistical tests. It establishes that the JFES transformation produces statistically comparable output despite arriving at that result through a fundamentally different mechanism.

Seven frozen 6,912-byte ASCII-safe inputs were used for each method: all-zero, repeated-a, repeated-b, repeated-zero-digit, repeated-z, ascending 7-bit data, and random printable data. Thirty trials were run for each input and method. The JFES public source and default silo were freshly captured, and the public Gauge settings were matched: default silo, two passes, fractal S-box enabled, and OTP enabled.

For JFES, the raw output is 6,928 bytes. The first 16 bytes are the UUID-derived OTP prefix and were separately preserved. The remaining 6,912-byte body was used for the length-matched comparison. This prevents the known framing material from being mistaken for evidence about the JFES transformation body.

3. The Comparison Matrix

This matrix is the primary comparison in this report. It places JFES directly beside the highest quality established cryptographic transformations and cryptographic random sources using identical sample counts and length-matched output bodies.

Comparison Matrix

Method ↓ Test →	Mean Chi-Square χ^2	Mean entropy (bits/byte)	Min entropy	Max entropy	Compressibility	Mean serial correlation
Optimal Value	255	**7.973388**	**7.973388**	**7.973388**	**1.001591**	**0**
Portalz JFES	255.746	7.973129	7.966659	7.979306	1.001591	0.000239
AES-256-CTR	254.993	7.973231	7.966920	7.979853	1.001591	0.000378
ChaCha20	255.940	7.973135	7.965631	7.978882	1.001591	0.000476
OS CSPRNG	255.617	7.973138	7.964177	7.979721	1.001591	0.001457
RDRAND instruction	258.732	7.972839	7.966061	7.979168	1.001591	0.000913
AES-256-GCM	253.734	7.973348	7.962663	7.979747	1.001591	0.000107
ChaCha20-Poly1305	256.091	7.973140	7.963443	7.979186	1.001591	0.000182

Matrix Info:

- **Chi-Square χ^2 — frequency conformity.**
  Tests whether the observed byte-frequency distribution departs materially from the expected uniform distribution. With 256 bins, the reference expectation is approximately **255**. JFES's mean of **255.746** sits within the same empirical region as the contemporary reference methods.
- **Entropy — distributional quality.**
  Measures how evenly the 256 possible byte values are represented. At 6,912 bytes, the appropriate finite-sample reference is approximately **7.973388 bits/byte**, rather than the theoretical 8. JFES's observed mean of **7.973129** is therefore in the expected region for a uniformly distributed byte source.
- **Compressibility — structural floor.**
  Tests whether exploitable structure remains in the byte stream. All compared methods produced essentially the same DEFLATE ratio, **1.001591**, indicating practical incompressibility (expansion). This is therefore regarded as a **minimum structural requirement**, rather than a discriminator between high-quality transformations. JFES must match this to be in the club.
- **Serial correlation — sequential independence.**
  Tests whether adjacent byte values exhibit detectable linear dependence. JFES's mean absolute serial

correlation of **0.000239** is close to the ideal of zero and lies within the range occupied by the reference technologies.

4. Why the Matrix Matters

The central aim of this experiment is to establish relative randomness quality of JFES.

A single entropy number cannot establish this. The matrix shows several independent characteristics together: entropy, compressibility, and serial correlation, across repeated trials and across deliberately structured inputs. This compliments the JFES Gauge instrumentation with a comprehensive analysis.

More importantly, the comparison is not limited to mean values. Across measured characteristics, observed ranges of contemporary reference methods overlap, or closely approach, observed JFES ranges. JFES therefore does not appear as an isolated statistical profile separated from the reference technologies; its observed output characteristics occupy the same general empirical region across the comparison matrix.

These measures deliver a verdict of ***optimal quality*** for JFES randomness. This is a critical result from the perspective of the first requirement of **Shannon OTP** compliance.

5. Structured Inputs and Transformation

The inputs were deliberately not restricted to already-random data. Repeated characters, repeated digits, repeated letters, ascending 7-bit data, and random printable data were transformed. This matters because a cryptographic transformation should suppress obvious structure in its input rather than merely reproduce the statistical character of the source data.

The JFES result demonstrates that highly structured inputs can be transformed into output whose measured byte-level characteristics sit alongside those of established cryptographic streams. This is direct empirical evidence relevant to the cryptographic quality of the transformation.

6. Selected Statistical Test Battery

The experiment also applied a selected battery based on NIST SP 800-22 formulas: monobit, block frequency, runs, longest run of ones, approximate entropy, serial tests, binary matrix rank, and cumulative sums. Ten component p-value streams were retained per method. The analysis used a predeclared multiple-comparison treatment across the resulting method/test summaries.

For JFES, none of the ten component summaries produced a suite-adjusted alert. Individual alpha-level failures occurred within the 210-sample population, as they also did for conventional reference methods. These individual observations were retained rather than averaged away.

There was one suite-adjusted alert among the 70 method/test summaries: AES-256-CTR Runs. This does not establish a weakness in AES-256-CTR. It demonstrates an important property of the experiment itself: a conventional reference stream can produce a statistical alert under a finite selected test battery. The battery therefore also functions as a comparative quality screen.

7. What the Results Establish

The experiment establishes a substantial empirical foundation for JFES cryptographic quality. The JFES transformation produces output with entropy, compressibility, correlation, and selected statistical-test behavior that sits alongside and overlaps with the leading reference methods, tested under the same experimental framework.

The result is especially significant because the JFES transformation engine does not obtain its transformation stream from an RNG. Its transformation material is produced through the engineered recursive navigation of the Mandelbrot field. The separate UUID-derived OTP prefix is a framing mechanism and should not be confused with the source of the JFES transformation stream.

Accordingly, the observed quality is evidence about the fractal entropy generation itself. The experiment provides an empirical bridge from fractal entropy-extraction to measurable cryptographic output.

8. What Remains for Cryptanalysis

The foundation established by JFES is not dependent upon a further cryptanalysis program conducted by Portalz.

JFES accesses the infinite complexity of the Mandelbrot field through recursive navigation. The statistical comparison demonstrates the resulting transformation behavior against established cryptographic transformations. The theoretical paper establishes the relationship between infinite complexity, recursive trajectory space, unpredictability and entropy.

From these foundations follows a specific prediction:

The cryptographic quality observed at the statistical layer will persist under deeper independent analysis because it originates in the fractal infinite-complexity source and the JFES method of recursively extracting and applying that complexity.

Portalz will not attempt to establish this prediction through an additional internally generated cryptanalysis report. Such analysis would necessarily be performed by the system's creator and would therefore carry limited independent evidentiary weight.

Instead, **JFES Gauge provides an open avenue for independent researchers to investigate the transformation.** Researchers can automate, observe and measure JFES behavior directly and apply their own analytical methods, attack models and cryptanalytic techniques.

9. Relationship to the Companion Paper

“Unpredictability as the Optimal Measure of Entropy” provides the higher-level engineering foundation. It explains why unpredictability is the operational property of interest, why infinite complexity matters, how this maps to entropy and why recursive navigation through the Mandelbrot field is fundamentally different from deterministic expansion of a finite random seed.

The present report takes the next step. It asks whether the engineered JFES extraction method produces output whose observable cryptographic characteristics compare directly with established premium cryptographic transformations. The result from this experiment affirms JFES optimal randomness quality.

10. Conclusion

JFES begins with an unusual but clearly defined foundation: the infinite complexity of the Mandelbrot mathematical field. It then provides an engineered method for recursively navigating that field and applying the resulting transformation material to payload data.

The Foundation Quality Report provides the empirical comparison. Under controlled conditions, JFES output stands alongside AES-256-CTR, ChaCha20, operating-system CSPRNG output, RDRAND, AES-256-GCM, and ChaCha20-Poly1305 across the measured byte-level characteristics and the selected statistical test battery.

The resulting proposition is coherent from foundation through observation: infinite complexity supplies the source; recursive navigation provides the extraction method; the resulting trajectory provides unpredictability; unpredictability provides entropy quality; and that entropy quality is manifested in cryptographic transformation output whose measured characteristics compare with established high-quality cryptographic systems.

This is the foundation on which deeper JFES cryptanalysis should proceed.

Foundation Architecture — Plain-English Summary

- Infinite Complexity — the Mandelbrot field supplies the underlying mathematical entropy source.
- Recursive Trajectory Space — JFES recursively navigates that field rather than scanning a finite random table.
- Unpredictability — the resulting trajectory is not available to an observer, only the complex stream values.
- Entropy — the unpredictable transformation material provides the entropy quality required by the JFES architecture.
- Cryptographic Quality — the resulting output demonstrates measurable characteristics alongside established high-quality cryptographic transformations.

The comparison matrix is therefore not an accessory to the argument. It is the empirical instrument that connects the foundation to the cryptographic result.

References

- Wolfgang Flatow, “Unpredictability as the Optimal Measure of Entropy: Linking Complexity to Entropy — The Infinite Complexity of the Mandelbrot Fractal and How JFES Extracts Entropy from the Mandelbrot Fractal,” 2026.
- M. Shishikura, “The boundary of the Mandelbrot set has Hausdorff dimension two,” Astérisque 222, 389–405, 1994.
- M. Shishikura, “The Hausdorff dimension of the boundary of the Mandelbrot set and Julia sets,” Annals of Mathematics, 147, 225–267, 1998.
- C. E. Shannon, “Communication Theory of Secrecy Systems,” Bell System Technical Journal, 28(4), 656–715, 1949.
- JFES Gauge: https://portalz.solutions/jfesGauge/JFES-Gauge.html
- JFES public engine: https://portalz.solutions/jfes/js/jfes.js?v=2