Fractal Encryption Standard (FES)

Security Architecture Overview

Quantum-Proof • Shannon-Compliant • Fractally Unique

Overview

The Fractal Encryption Standard (FES) achieves impenetrability by partitioning its security model into two independent but interoperable domains: **Fractal Stream Generation** and **Overwrite Modes**. Each domain scales without limit, ensuring adaptability across quantum, classical, and hybrid cryptographic environments.

1. Fractal Stream Generation

- **Dimensions:** Each added dimension contributes over 112 bits of keyspace. Dimensions are unbounded, supporting scalable entropy expansion.
- **Fractal OTP (FOTP):** Prevents stream reuse by binding stream generation to message context (e.g., file path or session ID). Infinite FOTP permutations ensure OTP compliance.
- **Silo:** Generates unique fractal mappings using GUID-derived entropy. Silos guarantee dimensional separation and non-interference across use cases.

2. Overwrite Modes

- **Passes:** Any number of transformation passes can be applied. Each uses a new segment of the fractal stream, ensuring uniqueness per pass.
- **Scramble:** Optional per-pass byte reordering based on fractal z-ordering. This introduces a high-performance cost but provides excellent protection against plaintext pattern correlation.
- **XOR + add + BitSplit:** Selectable operations per pass. BitSplit performs dynamic intra-byte bitplane reversal based on stream-derived split points.
- **sub:** Fractal byte substitution.
- **fBlit:** See BitScramble-PB Prime Mutation Layer below.

Impenetrability

Fractal OTP is highly recommended for Shannon OTP compliance, given quality path or session meta-data. BitSplit serves as a critical fallback impenetrability mechanism, preserving FES's one-time-pad-aligned security posture in all operational modes.

3. Recommended Security Profiles

- **Standard Protection (FES-SP):**
  - Dimensions: 8-10
  - Passes: 2
  - Scramble: Off
  - Operations: fBlit + XOR + BitSplit
  - Fractal OTP: optional
- **Advanced Protection (FES-AP):**
  - Dimensions: 12-16
  - Passes: 3–4
  - Scramble: On (last pass)
  - Operations: fBlit + SUB + XOR + ADD + BitSplit
  - Fractal OTP: desirable
- **Quantum-Hardened (FES-QH / Q-DEFCON 1):**
  - Dimensions: 20+
  - Passes: 6+
  - Scramble: On (every pass)
  - Operations: fBlit + SUB + XOR + ADD + BitSplit
  - Fractal OTP: required

Security Positioning

- **Shannon-Compliant:** FES satisfies all conditions of the One-Time Pad proof, delivering perfect secrecy when used with unique streams.
- **Quantum-Proof:** Fractal stream generation and key-path navigation lie outside the scope of possible quantum reversal or simulation.
- **Modular Scalable:** Each security domain can be tuned independently based on mission profile, latency budget, and cryptanalytic risk.

4. BitScramble-PB Prime Mutation Layer

4.1 Overview

BitScramble-PB (abbreviated `fBlit`) is a deterministic, reversible, bit-level mutation protocol designed to introduce high-entropy disruption into the payload prior to and following dynamic fractal stream-based transformations. Unlike classical byte-boundary transformations, `fBlit` operates on arbitrary bit positions, guided by curved prime sequences that scale with payload size and entropy requirements.

4.2 Design Rationale

Conventional substitution and transformation operations (such as XOR, ADD, or S-box-like SUB) operate on predictable patterns and byte-level boundaries. In contrast, `fBlit` introduces:

- **Prime-Guided Bit Displacement:** Deterministic swaps between non-overlapping bit segments defined by entropy-weighted primes (ranging from 2 to 75,000+).
- **Dual-Layer Static Mutation:** Two symmetric deterministic swaps (one forward, one reverse) ensure complete reversibility while disrupting leading and trailing bit segments.
- **Dynamic Stream-Guided Swaps:** Multiple stream-derived swaps occur based on fractal stream values, with scaling logic to ensure non-overlap and high variance.
- **Byte Hostility:** Swap sizes are deliberately misaligned to byte boundaries, preventing any alignment-based cryptanalysis.

4.3 Integration Into FES Pipeline

`fBlit` is applied in the overwrite phase of the FES transformation chain as follows:

1. **Static Pre-Scramble:** A fixed prime is chosen based on payload length. The payload is split and scrambled across the midpoint to prevent structural predictability.
2. **Dynamic Stream Scramble:** A sequence of prime-length swaps is scheduled using 3-byte fragments from the active fractal stream, with boundary and overlap safeguards in place.
3. **Static Post-Scramble:** The reverse order of the static pre-scramble swaps is applied to complete the symmetric transformation.

4.4 Security Benefits

The addition of `fBlit` enhances FES resistance to both classical and quantum attacks by:

- Destroying positional predictability across transformation layers.
- Preventing pattern recovery using known-plaintext or statistical attacks.
- Obfuscating stream reuse via non-linear, non-aligned bit-level disturbance.
- Introducing a configurable entropy domain decoupled from conventional byte logic.

4.5 Operational Limits

To maintain safe and reversible operation, fixed prime swap sizes are constrained to `fixedPrime` $\leq$ `bitLen / 4`. Dynamic stream swaps are guarded against overlap, underflow, and payload overspill.

4.6 Deployment Status

As of FES Core v3.7.0, BitScramble-PB is fully integrated into the FES Web DLL and live on the Portalz encryption demonstration system. Tested successfully to 7 full transformation passes with active substitution, XOR, ADD, and BitSplit layers.

Portalz Encryption – Document Version 1.0