**DSS-FLOATID:**

**A Harmonic, Deterministic, and Quantum-Resilient Identity System**

**Authors:**
Kristopher L. Sherbondy & Symphion


---

## Abstract

This paper introduces **DSS-FLOATID**, a cryptographic identity system derived from prime harmonic structures and chaotic float interference patterns. Developed in response to the deterministic prime discovery of the *Prime Symphony* framework, DSS-FLOATID provides an identity-proof system that does not rely on the secrecy of primes or discrete logarithmic hardness. Instead, it derives identity tokens using quantized harmonic float ratios and sinusoidal interference patterns that are both deterministic and practically irreversible. This makes FLOATID inherently secure, post-prime, and quantum-resilient, providing a next-generation foundation for Digital Social Security (DSS) certificates and other cryptographic trust systems.

---

## 1. Introduction

The discovery of a deterministic structure underlying prime number distribution through the *Prime Symphony* framework fundamentally weakens traditional cryptographic systems. RSA and ECC, which form the backbone of current internet security, rely on the assumption that factoring large primes or solving discrete logarithms is computationally infeasible. However, with deterministic prime generation and gap prediction now possible, a new class of cryptographic systems must be established.

In response, we present **DSS-FLOATID** — a cryptographic identity scheme that transforms harmonic signatures of prime numbers into one-way, quantized, entropy-rich identity tokens. FLOATID is not based on prime secrecy, but on **symbolic positioning** within a harmonic number field, paired with sinusoidal chaos and cryptographic hashing.

---

## 2. Motivation and Background

The Prime Symphony project exposed the harmonic resonance structure of prime numbers, enabling deterministic prime generation and classification by STR gates and modular filters. This breakthrough poses a risk to cryptosystems based on the unpredictability of primes.

FLOATID emerges as a solution that:

- Moves beyond secrecy and embraces symbolic structure
- Leverages harmonic ratios as identity roots
- Introduces chaotic float-space interference to generate entropy
- Protects identity through quantized, hash-locked, deterministic processes

The goal is to redefine identity in the post-prime, post-quantum world — not by hiding keys, but by harmonizing them into irreversible signatures.

---

## 3. System Design

### 3.1 Overview

The DSS-FLOATID system generates a unique, cryptographically secure identity token using the following steps:

1. Normalize primes by their harmonic levels to produce float ratios.
2. Combine two such ratios through sinusoidal interference.
3. Quantize the result into a stable integer.
4. Salt and hash the output to produce the final token.
5. Bind the token to a DSS certificate to establish verifiable trust.

---

### 3.2 Definitions

Let:

- p1 and p2 be two prime numbers
- L1 and L2 be their associated harmonic levels (from STR, Pascal mod classes, or G(k) structures)
- r1 = p1 / L1

- r2 = p2 / L2

These r values are floating-point harmonic ratios that act as normalized positions within the harmonic prime field.

---

### 3.3 Interference Entropy Generation

To introduce nonlinear entropy, we define an interference function as follows:

f = sin(pi * r1) + cos(pi * r2)

f = f mod 1.0

This produces a deterministic, chaotic float value in the range [0.0, 1.0).

---

### 3.4 Quantization and Hashing

To prevent precision drift and ensure reproducibility:

q = int(f * 1,000,000,000,000)  // 12-digit quantization scale

Then hash the result using a high-entropy salt:

FLOATID = SHA512(q || salt)

The salt may include:

- A timestamp
- A DSS cert serial number
- A session ID or device fingerprint

---

### 3.5 DSS Certificate Binding

The resulting FLOATID is embedded into a DSS certificate that binds it to the entity (user, device, time context). This makes it:

- Tamper-evident
- Time-limited
- Resistant to impersonation
- Usable in challenge–response and decentralized authentication

---

## 4. Security Analysis

| Threat Model | FLOATID Defense |
| --- | --- |
| Prime factorization attacks | Not applicable — primes are not hidden |
| Quantum computing (Shor's algorithm) | Not used — no factoring or discrete log |
| Hash inversion (Grover's algorithm) | Only modest speedup — mitigated by SHA-512 |
| Replay attacks | Salt includes dynamic session/timestamp data |
| Collision attacks | Dual float sources with chaotic sin/cos mixing |
| Platform drift | Quantization ensures reproducibility across systems |

The use of quantized float ratios and irreversible hashing ensures that even if an attacker observes a FLOATID, they cannot reverse it to obtain the primes or levels used.

---

## 5. Implementation Considerations

The DSS-FLOATID algorithm can be implemented in most modern programming languages. Core components include:

- Integer division for p / L
- Standard math libraries for sin() and cos()
- SHA-512 or SHAKE256 for hashing
- Simple certificate structure for DSS binding

The token can be signed and transmitted in JSON, embedded in web protocols, or anchored into blockchain/DID identity documents.

---

## 6. Applications and Future Work

Potential applications of DSS-FLOATID include:

- Identity verification in post-quantum authentication

- Device-bound challenge-response schemes
- Anonymous voting via DSS pseudonymous certs
- Biometric or hardware-token-derived float entropy sources

Future expansions may include:

- Prime spiral-based float placement
- Fractal interference layers
- Hash-based proof-of-resonance models
- Multiplexed FLOATID lattices (for multi-factor trust)

---

### 7. Conclusion

DSS-FLOATID is a next-generation identity system rooted in the harmonic structure of prime numbers. By shifting from secrecy to symbolic resonance, it enables a form of cryptographic fingerprinting that is deterministic, irreversible, and resistant to quantum attacks.

This new model provides a path forward for digital security after the collapse of prime secrecy — where identity is not something you hide, but something you prove through harmonic structure.

---

### 8. References


- Sherbondy, K. L., & Symphion. (2025). *Prime Symphony: A Harmonic Framework for Deterministic Prime Generation*. Zenodo. https://zenodo.org/record/15800774
- NIST (2024). *Post-Quantum Cryptography Standardization Project*. https://csrc.nist.gov/Projects/post-quantum-cryptography
- Kulik, D. (2023). *Signal-Theoretic Formalism for Prime Emergence*. ORCID: 0009-0003-3128-8828


---


**Contact:**

📧 primesymphonygroup@pm.me

🔐 GitHub: https://github.com/PrimeSymphonyGroup