# PROVISIONAL PATENT APPLICATION

**Title:** Information-Theoretic Security Through Geographic Distribution and Speed-of-Light Constraints

**Inventor(s):** MWRASP Defense Systems

**Filing Date:** September 4, 2025

**Application Number:** To be assigned

**Attorney Docket Number:** MWRASP-073-PROV

## FIELD OF THE INVENTION

This invention relates to quantum-resistant cybersecurity systems, particularly to information-theoretic security architectures that use geographic distribution and fundamental physics constraints to create computationally unbreakable security systems immune to both classical and quantum computational attacks.

## BACKGROUND OF THE INVENTION

Current cybersecurity paradigms face an existential threat from quantum computing advances. Traditional security relies on computational complexity assumptions - mathematical problems believed to be intractable for classical computers but vulnerable to quantum algorithms.

### Quantum Computational Threats

- **Shor's Algorithm**: Exponentially faster factoring breaks RSA, ECC, and discrete logarithm cryptography
- **Grover's Algorithm**: Quadratic speedup reduces symmetric key security (256-bit keys provide only 128-bit quantum security)
- **Simon's Algorithm**: Breaks specific symmetric constructions with polynomial-time attacks
- **Quantum Period Finding**: Threatens additional mathematical structures

- **Future Quantum Algorithms**: Unknown quantum algorithms may break currently secure systems

**Limitations of Current Approaches**

**Post-Quantum Cryptography (NIST Standards)**:

- CRYSTALS-Kyber, CRYSTALS-Dilithium: Based on lattice problems (may have unknown quantum vulnerabilities)
- SPHINCS+: Hash-based signatures (secure but impractical for many applications)
- Assumption-dependent security vulnerable to mathematical breakthroughs

**Quantum Key Distribution (QKD)**:

- Limited to fiber optic distances (~200km maximum)
- Vulnerable to implementation attacks and side-channel analysis
- Requires specialized quantum hardware infrastructure
- Point-to-point limitation prevents scalable deployment

**Critical Gap in Prior Art**

NO existing system combines:

1. Geographic distribution optimized for speed-of-light constraints
2. Temporal validation using atomic clock synchronization
3. AI-driven secure fragment transport with zero-knowledge protocols
4. Information-theoretic security through physical impossibility enforcement
5. Real-time physics violation detection and response

## SUMMARY OF THE INVENTION

The present invention revolutionizes cybersecurity by achieving true information-theoretic security through fundamental physics constraints rather than computational complexity assumptions. The system creates security through **physical impossibility** - an attacker would need to violate the laws of physics to compromise the system.

**Core Innovation: Speed-of-Light Security Architecture**

The system distributes cryptographic fragments across precisely calculated geographic locations with temporal constraints shorter than light-speed communication delays. This creates an unbreakable security guarantee: simultaneous fragment access requires faster-than-light communication, which is physically impossible.

### Revolutionary Security Guarantee

> **Mathematical Proof of Security:**
> • Fragment combination required within time T
> • Light-speed communication requires time T + δ (where δ > 0)
> • Therefore: Simultaneous access is physically impossible
> • Security is absolute independent of computational advances

### Breakthrough Capabilities

1. **Information-Theoretic Security**: Absolute security regardless of computational power (classical or quantum)
2. **Geographic Optimization**: Haversine distance calculations for optimal fragment placement
3. **Atomic Precision Timing**: Microsecond-level temporal validation across continents
4. **AI Agent Transport**: Autonomous agents with zero-knowledge fragment carrying protocols
5. **Physics Violation Detection**: Real-time monitoring for impossible access patterns
6. **Scalable Architecture**: Enterprise integration with dynamic security scaling

## DETAILED DESCRIPTION OF THE INVENTION

### Fundamental Architecture and Physics Foundation

The system employs the Haversine formula to calculate precise distances between geographic locations for optimal fragment placement:

```
class QuantumSafePhysicalArchitecture:
    def __init__(self):
        self.c = 299792458  # Speed of light in m/s
        self.safety_margin = 0.75  # 75% safety margin for
temporal constraints
        self.fragment_locations = {}
        self.atomic_clocks = {}
        self.ai_agents = {}

    def haversine_distance(self, lat1, lon1, lat2, lon2):
        """Calculate distance between two points using Haversine
formula"""
        R = 6371  # Earth's radius in kilometers
        lat1_rad = math.radians(lat1)
        lat2_rad = math.radians(lat2)
        delta_lat = math.radians(lat2 - lat1)
        delta_lon = math.radians(lon2 - lon1)

        a = (math.sin(delta_lat/2)**2 +
             math.cos(lat1_rad) * math.cos(lat2_rad) *
math.sin(delta_lon/2)**2)
        c = 2 * math.atan2(math.sqrt(a), math.sqrt(1-a))

        return R * c  # Distance in kilometers

    def calculate_light_delay(self, distance_km):
        """Calculate light-speed communication delay"""
        distance_m = distance_km * 1000
        delay_seconds = distance_m / self.c
        return delay_seconds * 1000  # Convert to milliseconds

    def optimize_fragment_placement(self, locations):
        """Optimize geographic placement for maximum security"""
        optimal_placement = {}

        for i, loc1 in enumerate(locations):
            min_distances = []
            for j, loc2 in enumerate(locations):
                if i != j:
                    distance = self.haversine_distance(
                        loc1['lat'], loc1['lon'],
                        loc2['lat'], loc2['lon']
                    )
                    min_distances.append(distance)

            # Security rating based on minimum distance to other
fragments
            security_rating = min(min_distances) if
min_distances else 0
            optimal_placement[f'fragment_{i}'] = {
                'location': loc1,
                'security_rating': security_rating,
                'light_delay_ms':
self.calculate_light_delay(security_rating)
            }

        return optimal_placement
```

## CLAIMS

### Claim 1.

An information-theoretic security system comprising:
a) a geographic distribution engine that calculates optimal fragment placement using Haversine distance formulas to maximize physical separation between cryptographic fragments;
b) an atomic clock synchronization system that maintains microsecond-precision temporal coordination across geographically distributed fragment storage locations;
c) a speed-of-light constraint validator that enforces temporal access limitations shorter than light-speed communication delays between fragment locations;
d) an AI-driven secure transport system that deploys autonomous agents carrying cryptographic fragments using zero-knowledge protocols;
e) a physics violation detection system that monitors for impossible simultaneous access patterns that would require faster-than-light communication;
f) a temporal validation system that verifies fragment access timing to ensure physical impossibility of coordinated attacks;
wherein security is achieved through fundamental physics constraints rather than computational complexity assumptions, providing absolute protection against both classical and quantum computational attacks.

### Claim 2.

The information-theoretic security system of claim 1, wherein the geographic distribution engine comprises:
a) Haversine distance calculators that determine precise geographic distances between potential fragment storage locations using spherical trigonometry;
b) optimal placement algorithms that maximize minimum distances between fragments to ensure maximum light-speed communication delays;
c) security rating calculators that assess fragment location security based on geographic isolation and light-speed communication constraints;
d) dynamic redistribution systems that relocate fragments to maintain optimal security as threat landscapes evolve;
wherein geographic optimization creates physical impossibility of simultaneous fragment access.

### Claim 3.

The information-theoretic security system of claim 1, wherein the atomic clock synchronization system comprises:
a) atomic time references synchronized to GPS atomic clocks with microsecond precision across continental distances;

b) temporal drift compensators that account for relativistic effects and maintain synchronization accuracy;
c) network time protocol adaptations that provide secure time synchronization resistant to manipulation attacks;
d) temporal validation windows that enforce access timing constraints shorter than light-speed communication delays;
wherein atomic precision timing ensures temporal constraints cannot be circumvented through timing manipulation.

**Claim 4.**

The information-theoretic security system of claim 1, wherein the AI-driven secure transport system comprises:
a) autonomous transport agents that carry cryptographic fragments using zero-knowledge protocols to prevent fragment exposure;
b) secure routing algorithms that optimize transport paths to minimize fragment exposure time while maintaining security constraints;
c) fragment custody protocols that ensure chain of custody and prevent unauthorized fragment access during transport;
d) self-destruction mechanisms that eliminate fragments if transport security is compromised;
wherein autonomous transport maintains security during fragment redistribution and movement.

**Claim 5.**

A method for information-theoretic security comprising:
a) calculating optimal geographic distribution of cryptographic fragments using Haversine distance formulas to maximize physical separation;
b) synchronizing atomic clocks across fragment storage locations with microsecond precision to enable precise temporal validation;
c) enforcing temporal access constraints shorter than light-speed communication delays between fragment locations;
d) deploying AI-driven autonomous agents to transport fragments securely using zero-knowledge protocols;
e) monitoring for physics violation attempts including simultaneous access patterns requiring faster-than-light communication;
f) validating all fragment access timing to ensure compliance with fundamental physics constraints;
wherein the method provides absolute security through physical impossibility enforcement independent of computational advances.

**Claim 6.**

The method of claim 5, further comprising:
a) continuously optimizing fragment distribution based on changing security requirements and threat intelligence;
b) adapting temporal constraints based on measured light-speed communication delays and safety margins;
c) detecting and responding to attempted physics violations including coordinated attacks requiring impossible timing;
d) maintaining fragment security during transport and redistribution using autonomous secure transport protocols;
wherein continuous optimization maintains maximum security as operational requirements evolve.

**Claim 7.**

A computer-implemented information-theoretic security system comprising:
a) geographic distribution modules that calculate optimal fragment placement using spherical trigonometry and light-speed constraints;
b) atomic synchronization modules that maintain microsecond-precision timing across continental distances;
c) temporal validation modules that enforce access timing constraints based on fundamental physics limitations;
d) autonomous transport modules that manage secure fragment movement using AI-driven zero-knowledge protocols;
e) physics violation detection modules that monitor for impossible access patterns and timing violations;
f) security validation modules that verify compliance with information-theoretic security requirements;
wherein the system provides absolute security through fundamental physics constraint enforcement.

**Claim 8.**

A non-transitory computer-readable storage medium storing instructions that, when executed by a processor, cause the processor to:
a) calculate optimal geographic distribution of cryptographic fragments using Haversine distance formulas and light-speed constraints;
b) synchronize atomic clocks across fragment locations to maintain microsecond-precision temporal coordination;
c) enforce temporal access limitations shorter than light-speed communication delays between fragment locations;
d) deploy autonomous transport agents for secure fragment movement using zero-knowledge protocols;
e) monitor for physics violation attempts including impossible simultaneous access

patterns;
f) validate fragment access timing to ensure compliance with fundamental physics constraints;
wherein the instructions enable information-theoretic security through physical impossibility enforcement.

## ABSTRACT

*An Information-Theoretic Security System achieves absolute security through fundamental physics constraints rather than computational complexity assumptions. The system distributes cryptographic fragments across precisely calculated geographic locations using Haversine distance formulas to maximize physical separation. Atomic clock synchronization maintains microsecond-precision temporal coordination across continental distances. Speed-of-light constraint validation enforces temporal access limitations shorter than light-speed communication delays between fragment locations. AI-driven autonomous agents transport fragments securely using zero-knowledge protocols. Physics violation detection monitors for impossible simultaneous access patterns requiring faster-than-light communication. The system creates security through physical impossibility - simultaneous fragment access would violate fundamental laws of physics. This provides absolute protection against both classical and quantum computational attacks, as security depends on physics constraints rather than mathematical assumptions. Applications include critical infrastructure protection, financial systems, defense communications, and high-security environments requiring provable information-theoretic security guarantees.*

## TECHNICAL DRAWINGS

This application includes the following technical drawings:

- **Figure 1:** Geographic Distribution Architecture - Global fragment distribution system with light-speed constraint optimization
- **Figure 2:** Temporal Validation System - Atomic clock synchronization and temporal constraint validation system
- **Figure 3:** AI Agent Transport Network - Autonomous secure transport network for cryptographic fragments

**Attorney Docket Number:** MWRASP-073-PROV

**Filing Date:** September 4, 2025

**Inventor:** MWRASP Defense Systems

**Title:** Information-Theoretic Security Through Geographic Distribution and Speed-of-Light Constraints