QUANTUM-SAFE PHYSICAL IMPOSSIBILITY ARCHITECTURE FOR CYBERSECURITY SYSTEMS

PROVISIONAL PATENT APPLICATION

Filed: [DATE TO BE INSERTED]
Application No.: [TO BE ASSIGNED]

Inventor: Brian Rutherford
Assignee: MWRASP Technologies, Inc.

TECHNICAL FIELD

This invention relates to cybersecurity systems that utilize physical impossibility principles to achieve information-theoretic security against quantum computing attacks, specifically through geographic distribution of encrypted data fragments across multiple global locations simultaneously.

BACKGROUND OF THE INVENTION

Current State of Cybersecurity

Traditional cybersecurity systems rely on mathematical cryptographic assumptions (e.g., RSA, ECC) that are vulnerable to quantum computing attacks using Shor's algorithm. Current post-quantum cryptography (PQC) standards still rely on mathematical assumptions that may be broken by future quantum algorithms.

Problem Statement

1. **Quantum Threat**: Quantum computers can break all current public-key cryptography using Shor's algorithm

2. **Mathematical Vulnerability**: All current security systems rely on mathematical assumptions that may be compromised

3. **Time Limitations**: Traditional systems have no temporal protection against prolonged quantum attacks

4. **Centralized Vulnerabilities**: Current systems can be compromised by attacking a single location

Prior Art Limitations

- **Traditional Cryptography**: RSA, AES, ECC all vulnerable to quantum attacks

- **Post-Quantum Cryptography**: Still relies on mathematical assumptions (lattices, codes, hash functions)

- **Quantum Key Distribution (QKD)**: Limited to point-to-point links, requires specialized hardware

- **Secret Sharing Schemes**: Mathematical threshold schemes still vulnerable to quantum attacks

SUMMARY OF THE INVENTION

The present invention provides a quantum-safe cybersecurity architecture that achieves information-theoretic security through **physical impossibility** rather than mathematical assumptions. The system fragments encrypted data and distributes fragments across multiple global locations with strict temporal constraints, making it physically impossible for any quantum computer to intercept all fragments simultaneously.

Key Innovation Elements

1. **Physical Impossibility Security Model**: Security based on fundamental physical limitations (speed of light, geographic distribution)

2. **Temporal Fragmentation Engine**: Time-limited fragment existence with automatic expiry

3. **Global Distribution Network**: Simultaneous fragment transport to 5+ global locations

4. **Information-Theoretic Security**: Provably secure regardless of computational advances

DETAILED DESCRIPTION OF THE INVENTION

System Architecture Overview

The Quantum-Safe Physical Impossibility Architecture consists of four primary components:

1. **Temporal Fragmentation Engine** - Creates time-limited data fragments

2. **Geographic Distribution Controller** - Routes fragments to global locations

3. **Physical Security Validator** - Ensures impossibility constraints are met

4. **Reconstruction Engine** - Reassembles fragments at designated location

Component 1: Temporal Fragmentation Engine

Purpose: Create multiple encrypted fragments of sensitive data with strict temporal constraints.

```
Input: Sensitive data D of size N bytes
Process:
1. Fragment D into k fragments: F1, F2, F3, ..., Fk (where k >= 5)
2. Apply temporal constraint T (default: 5 minutes expiry)
3. Encrypt each fragment using AES-256-GCM with unique keys
4. Attach temporal metadata with creation timestamp and expiry time
Output: Set of encrypted, time-limited fragments {EF1(T), EF2(T), ..., EFk(T)}
```

Mathematical Foundation:

```
Security Level = Physical_Distance^k Ã— Temporal_Constraint^-1
Where:
- k = number of global locations (minimum 5)
- Physical_Distance = minimum separation distance (>1000km)
- Temporal_Constraint = fragment lifetime (300 seconds default)
```

Component 2: Geographic Distribution Controller

Purpose: Simultaneously transport fragments to geographically separated global locations.

```
class GeographicDistributionController:
    def __init__(self):
        self.global_locations = {
            'singapore': {'lat': 1.3521, 'lon': 103.8198},
            'switzerland': {'lat': 46.8182, 'lon': 8.2275},
            'japan': {'lat': 35.6762, 'lon': 139.6503},
            'canada': {'lat': 45.4215, 'lon': -75.6972},
            'iceland': {'lat': 64.1466, 'lon': -21.9426},
            'norway': {'lat': 59.9139, 'lon': 10.7522},
            'new_zealand': {'lat': -41.2865, 'lon': 174.7762},
            'chile': {'lat': -33.4489, 'lon': -70.6693}
        }

    def calculate_minimum_separation(self, locations):
        """Ensure minimum 1000km separation between all locations"""
        min_distance = float('inf')
        for i, loc1 in enumerate(locations):
            for j, loc2 in enumerate(locations[i+1:], i+1):
                distance = self.haversine_distance(loc1, loc2)
                min_distance = min(min_distance, distance)
        return min_distance
```

Component 3: Physical Security Validator

Purpose: Validate that physical impossibility constraints are maintained throughout the process.

```
Maximum_Theoretical_Travel_Time = Distance / Speed_of_Light
Required_Travel_Time = Fragment_Expiry_Time / 2

Security_Constraint: Required_Travel_Time < Maximum_Theoretical_Travel_Time
```

```
def validate_physical_impossibility(self, locations, fragment_expiry_time):
    """Validate that no quantum computer can access all fragments"""

    # Calculate minimum travel time between furthest locations
    max_distance = 0
    for i in range(len(locations)):
        for j in range(i+1, len(locations)):
            distance = self.calculate_distance(locations[i], locations[j])
            max_distance = max(max_distance, distance)

    # Speed of light constraint (accounting for infrastructure delays)
    min_travel_time = max_distance / 299792458  # meters per second
    practical_travel_time = min_travel_time * 1000  # Account for routing delays
```

```
    # Validation: Fragment expiry must be less than travel time
    return fragment_expiry_time < practical_travel_time
```

CLAIMS

1. A quantum-safe cybersecurity method comprising:

fragmenting sensitive data into a plurality of encrypted fragments;

assigning temporal constraints to each fragment with automatic expiry;

simultaneously distributing fragments to geographically separated locations with minimum separation distance of 1000 kilometers;

validating physical impossibility constraints based on speed-of-light limitations;

reconstructing original data only when minimum fragment threshold received at designated secure location within temporal window.

2. A cybersecurity system comprising:

a temporal fragmentation engine configured to create time-limited encrypted data fragments;

a geographic distribution controller configured to transport fragments to multiple global locations simultaneously;

a physical security validator configured to ensure speed-of-light constraints prevent simultaneous access to all fragments;

a reconstruction engine configured to reassemble fragments at a designated location after validation.

3. A computer-implemented method for achieving information-theoretic security comprising:

creating n encrypted fragments from sensitive data where n â‰¥ 5;

applying temporal expiry constraints to each fragment;

distributing fragments across geographic locations separated by minimum distance constraints;

validating that no computing device can physically access all fragments within the temporal window based on fundamental physical limitations.

4. The method of claim 1, wherein the temporal constraints comprise automatic fragment expiry between 30 seconds and 30 minutes.

5. The system of claim 2, wherein the geographic distribution controller utilizes Haversine distance calculations to optimize fragment placement across global coordinates.

6. The method of claim 3, wherein the fragments are transported by AI agents with behavioral authentication and zero-knowledge transport protocols.

7. The system of claim 2, further comprising quantum hardware integration for validation of quantum threat detection capabilities.

8. The method of claim 1, wherein security is achieved through physical impossibility rather than mathematical cryptographic assumptions.

9. The system of claim 2, wherein the reconstruction engine implements k-of-n threshold schemes requiring minimum fragment threshold for data recovery.

10. The method of claim 3, further comprising legal jurisdiction routing to create additional barriers through treaty conflicts and diplomatic constraints.

DRAWINGS

Figure 1: System Architecture Overview

â”Œâ”€â
â”, Quantum-Safe Physical Impossibility â”, â”, Architecture â”,
â”œâ”€â
â”, â”Œâ”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”□
â”Œâ”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”□ â”Œâ”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”□
â”, â”, â”, Temporal â”, â”, Geographic â”, â”, Physical â”, â”, â”, â”, Fragmentation â”,â†’ â”, Distribution
â”,â†’ â”, Security â”, â”, â”, â”, Engine â”, â”, Controller â”, â”, Validator â”, â”, â”,
â””â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”˜ â””â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”˜
â””â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”˜ â”, â”, â”, â”, â”, â”, â”, â–¼ â–¼ â–¼ â”, â”,
â”Œâ”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”□ â”Œâ”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”□
â”Œâ”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”□ â”, â”, â”, Fragment 1 â”, â”, Fragment 2 â”, â”,
Fragment 3 â”, â”, â”, â”, Singapore â”, â”, Switzerland â”, â”, Japan â”, â”, â”, â”, (5min expiry) â”, â”, (5min
expiry) â”, â”, (5min expiry) â”, â”, â”, â””â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”˜
â””â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”˜ â””â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”€â”˜
â”,
â””â”€â

Figure 2: Geographic Distribution Map

Global Fragment Distribution Network: Iceland (Fragment 5) â”Œâ”€â”€â”€â”€â”€â”□ â”, ðŸ□”ï¸□ â”,
â””â”€â”€â”€â”€â”€â”˜ â”, â”Œâ”€â”€â”€â”€â”€â”□ â”, â”Œâ”€â”€â”€â”€â”€â”□ â”, ðŸ‡¨ðŸ‡ â”,â†□â”€â”€â”¼â”€â”€â†’â”,
ðŸ‡¯ðŸ‡µ â”, (Switzerland) (Japan) â””â”€â”€â”€â”€â”€â”˜ â”, â””â”€â”€â”€â”€â”€â”˜ â”, â”Œâ”€â”€â”€â”€â”€â”□ â”,
ðŸ‡¸ðŸ‡¬ â”, (Singapore) â””â”€â”€â”€â”€â”€â”˜ â”, â”Œâ”€â”€â”€â”€â”€â”□ â”, â”Œâ”€â”€â”€â”€â”€â”□ â”, ðŸ‡¨ðŸ‡¦
â”,â†□â”€â”€â”¼â”€â”€â†’â”, ðŸ‡³ðŸ‡´ â”, (Canada) (Norway) â””â”€â”€â”€â”€â”€â”˜ â”, â””â”€â”€â”€â”€â”€â”˜ â”,
â”Œâ”€â”€â”€â”€â”€â”□ â”, ðŸ‡³ðŸ‡¿ â”, (New Zealand) â””â”€â”€â”€â”€â”€â”˜ Minimum Separation: >1000km between all locations Maximum Travel Time: <5 minutes for any quantum computer Security Guarantee: Physical impossibility of simultaneous access

ABSTRACT

A quantum-safe cybersecurity architecture achieving information-theoretic security through physical impossibility rather than mathematical assumptions. The system fragments encrypted data and distributes fragments across geographically separated global locations with temporal constraints, making it physically impossible for quantum computers to intercept all fragments simultaneously due to speed-of-light limitations. The architecture comprises a temporal fragmentation engine, geographic distribution controller, physical security validator, and reconstruction engine, providing provably secure protection against quantum computing attacks of any capability level.

--- END OF SPECIFICATION ---