CORA – patterns and probabilities

Publication date: October 28, 2025

Joseph Latouf
CORA Cyber Security Inc.
519-254-4703
Windsor, Ontario

Abstract

One-Time Pads (OTPs) represent the gold standard of cryptographic security. They are mathematically unbreakable, immune to brute-force attacks, and resistant to quantum computing threats. However, they have significant operational drawbacks, namely, they must be as long as the message, cannot be reused, and do not scale well for distributed networks and cloud platforms.

Multiple Use Pads (MUPs) are a simple evolution of the OTP concept. They retain the core advantages of OTPs while overcoming their operational limitations. MUPs introduce a probabilistic architecture that allows for key reuse without compromising security. They simplify key management by assembling keys dynamically in memory, eliminating the need for pre-distributed, fixed-length keys.

The evolution from OTPs to MUPs is simple – remove language and plain text patterns! As a basic example, use AES encryption which removes patterns, and then the pad can be reused, even if the pad is not truly random. With MUPs the pad may be shorter than the message.

There are numerous approaches to remove these patterns. CORA has optimized the removal of these patterns!

MUP – a basic example

A first step towards recognizing that MUPs are possible is found at https://github.com/goCORA/MUP_basic_example. This demonstration uses a fast and simple 16-byte (128 bit) AES-CTR encryption which operates on both messages, and then the same MUP (pad) operates on these ciphertext.

While crib dragging works in this demo on the OTP, it does not work on the MUP. Furthermore, when one of the messages is obtained and XORed with the original cyphertext, the key is obtained. Since neither ciphertexts are decrypted, the original MUP is secure.

CORA: A Distributed, Quantum-Safe Encryption Framework

CORA (Context Ordered Replacement Algorithm) is a sophisticated implementation of MUPs designed for modern cloud and distributed environments. In contrast to the simple example cited above, CORA implements a novel method of pad morphing to further ensure that CORA is unbreakable.

CORA is a distributed, quantum-safe framework which, unlike blockchains (which rely on decentralized consensus and are vulnerable to theft and irrecoverability), is centrally managed. This architecture ensures that encrypted data cannot be stolen and rendered unrecoverable by malicious actors.

CORA's design offers several transformative benefits:

- **Simplified Key Management**: Keys are never stored in full and are assembled contextually, reducing exposure and operational overhead.
- **Cloud Compatibility**: CORA is optimized for distributed systems, making it ideal for securing cloud services, autonomous platforms, and financial infrastructures.
- **Ransomware Elimination**: By decoupling access from static key storage and enabling centralized recovery, CORA renders ransomware attacks ineffective.
- **Hack Irrelevance**: Even if data is exfiltrated, the encryption remains unbreakable, and the system can restore access without compromise.

MUP Architecture and CORA Threat Model

Multiple Use Pads (MUPs): Architecture and Design Principles

MUPs are designed to retain the theoretical strength of One-Time Pads while introducing practical enhancements that make them viable for modern systems. Their architecture is built on the following principles:

- **Dynamic Key Assembly**: Keys are not stored or transmitted in full. Instead, they are assembled in memory during encryption and decryption, based on contextual parameters and pad fragments.
- **Probabilistic Key Structure**: Each pad varies in length, distribution, and entropy. The removal of language patterns from the messages, removes the need for the MUP to be as large as the data being encrypted. This randomness ensures that even reused pads do not produce predictable patterns.
- **Contextual Binding**: Encryption keys are bound to specific contexts—such as user identity, device fingerprint, or session metadata—making unauthorized reuse or replay attacks ineffective.
- **Pad Fragmentation and Rotation**: Pads are segmented and rotated across sessions, allowing reuse without compromising secrecy. This fragmentation also supports distributed deployment across cloud nodes.

CORA Implementation: Enhancing MUPs for Distributed Systems

CORA (Context Ordered Replacement Algorithm) builds on the MUP foundation with a distributed, cloud-native architecture that addresses real-world deployment challenges:

- **Centralized Pad Management**: Unlike blockchains, which rely on decentralized consensus, CORA uses a centralized controller to manage pad distribution and recovery. This prevents pad theft and ensures recoverability.
- **Immutable Context Chains**: CORA maintains a chain of contextual metadata for each encryption event. This chain is cryptographically signed and stored in a secure ledger, enabling auditability and rollback.
- **Redundant Pad Catalogs**: Pad fragments are cataloged across multiple nodes, ensuring fault tolerance and high availability. Each fragment is encrypted and indexed without revealing its structure.
- **Zero-Knowledge Recovery**: In the event of a breach or ransomware attack, CORA can restore access without revealing pad contents or compromising encrypted data.

Threat Model and Security Guarantees

CORA is designed to withstand a wide range of attack vectors, including:

Threat Type	Mitigation Strategy
Key Theft	Keys are never stored in full; fragments are distributed and context bound.
Pad Reuse Exploits	Probabilistic pad structure and contextual binding prevent pattern leakage.
Quantum attacks	No reliance on factorization or discrete log problems; encryption is quantum safe.
Ransomware	Centralized pad recovery and strict contextual integrity renders data hostage scenarios and ransomware propagation ineffective.
Insider Threats	Immutable context chains and audit logs detect unauthorized access or tampering.
Man-in-the-Middle	Contextual binding and session-specific pads prevent replay or injection attacks.

CORA's architecture ensures that even if encrypted data is exfiltrated, it remains inaccessible without the correct contextual pad assembly. This makes traditional hacking methods irrelevant and positions CORA as a future-proof solution for high-security environments.

Integration Workflows

Deployment Patterns

Hardware Integration: CORA is ideally suited to ASIC implementations in devices so that everything is encrypted in an efficient and unbreakable manner. This improves cyber hygiene while inoculating against ransomware.

Gateway Integration: Deploy CORA as an inline encryption gateway for legacy applications with minimal code changes.

SDK Integration: Embed CORA client SDK in applications for native encryption and contextual binding of sessions.

Cloud-Native: Run CORA services as microservices with auto-scaling, load balancing, and secure service mesh integration.

Key Operational Flows

Pad Provisioning: Central controller fragments pads, catalogs fragments by context identifiers, and distributes encrypted fragments to authorized nodes.

Encryption Flow: Client requests contextual pad assembly; node assembles fragments in memory, performs XOR encryption, writes ciphertext to storage, and securely zeroes fragments.

Decryption Flow: Authorized client requests context-bound assembly; node reconstitutes the pad, XORs with ciphertext, returns plain text, and purges memory.

Recovery Flow: In compromise scenarios, administrators trigger zero-knowledge recovery; controller re-issues context bindings without exporting raw pad material.

Access Control and Auditing

Contextual Authorization: Access is granted by contextual policies such as identity, device posture, geolocation, and time windows.

Immutable Audit Trails: Each encryption event appends a cryptographically signed context record to a secure ledger to enable nonrepudiable audits.

Use Cases

Cloud Storage and Backups

Benefit: Protects stored data against exfiltration and ransomware while enabling fast, centralized recovery.

Impact: Eliminates the need to pay ransoms for encrypted backups.

Financial Systems and Exchanges

Benefit: Secures transaction streams and ledger snapshots against future quantum attacks.

Impact: Preserves regulatory compliance and customer trust without radically changing existing infrastructure.

Autonomous Systems and Edge Devices

Benefit: Context-bound pads protect telemetry and command channels; pad fragments distributed across edge nodes increase resilience.

Impact: Prevents unauthorized command injection and secures over-the-air updates.

Healthcare and Critical Infrastructure

Benefit: Ensures patient records and control-plane data remain confidential and recoverable after compromise.

Impact: Reduces downtime and legal exposure from data breaches.

Security and Compliance Considerations

Cryptographic Assurances

Quantum Safety: No reliance on hardness assumptions vulnerable to quantum computing.

Statistical Robustness: Probabilistic pad construction prevents pattern leakage under reuse.

Ephemeral Keys: Pads assembled only in volatile memory and wiped after use.

Regulatory Mapping

Data Residency: Centralized catalog supports policy-driven fragment placement for residency requirements.

Auditability: Immutable context chains satisfy strict audit and nonrepudiation demands.

Standards Alignment: CORA complements existing standards by providing confidentiality and can be combined with authenticated protocols to satisfy integrity requirements.

Conclusion

Simple MUPs are easy to produce and verify; CORA builds on that simplicity with a set of orthogonal, probabilistic mechanisms that collectively harden security. CORA's design choices include randomized key lengths, per-bloc ephemeral headers, pad morphing, non-uniform, random block sizing, and probabilistic block distribution; these factors multiply the effective search space and eliminate predictable patterns attackers' exploit.

This probabilistic approach renders conventional and quantum-driven attacks ineffective. Embedded at the hardware level, CORA protects the whole device, turning ransomware and similar threats from a pressing problem into an irrelevant one.

CORA makes the hack irrelevant!