Whitepaper for Unified Advanced Cipher (UAC)

1. Introduction

The Unified Advanced Cipher (UAC) is a symmetric encryption method tailored to meet the evolving demands of secure data transmission. Leveraging robust cryptographic principles, UAC integrates dynamic components to ensure resilience against modern attack vectors, including quantum computing threats and side-channel attacks. This whitepaper outlines the design, functionality, and security considerations of the UAC algorithm, with emphasis on its key length, initialization vector (IV) handling, and core cryptographic features.

Note: This encryption method, including the algorithm is generated by Artificial Intelligence

---

2. Goals and Motivation

The UAC algorithm is engineered to:

- **Provide Flexible Security Parameters**: Supports configurable block sizes, key lengths, and initialization vectors to cater to diverse security needs.
- **Enhance Resilience**: Offers protection against side-channel attacks such as timing or power analysis.
- **Prepare for Quantum Threats**: Employs cryptographic design elements that strengthen resistance to quantum-based attacks.
- **Maintain Practicality**: Optimized for performance across software and hardware environments.

---

3. Algorithm Overview

3.1 Key Length and IV Length

The UAC algorithm specifies key and IV lengths critical for secure operation. Key

aspects include:

1. **Key Length**:
    - Minimum required length: **32 bytes (256 bits)**.
    - The flexibility to use longer keys strengthens security, enabling resistance against brute-force attacks, including those leveraging Grover's algorithm in a quantum context.
2. **Initialization Vector (IV)**:
    - Fixed at **32 bytes (256 bits)**.
    - The IV is used for dynamic elements of the algorithm, including generating subkeys and the substitution-permutation network (SPN).
    - Ensures uniqueness for encryption operations, mitigating risks of ciphertext patterns that could lead to cryptanalysis.

3.2 Core Components

Dynamic Subkey Generation

UAC uses the **SHA-512 hash function** to derive subkeys for each encryption round. The process includes:

- Concatenation of the key and IV to form a seed.
- Iterative hashing to produce a unique subkey for every round.
- Key size scalability ensures adaptability for stronger cryptographic requirements.

Dynamic S-Box Construction

A **dynamic S-box** is generated for each encryption session:

- Seeded by a combination of the key and IV.
- Randomized using a custom shuffle mechanism based on a pseudorandom number generator (PRNG).

- Provides non-repeating substitution patterns for enhanced resistance to differential cryptanalysis.

Substitution-Permutation Network (SPN)

UAC employs a robust SPN structure, featuring:

- Byte substitution via the S-box.
- Block permutation through a reversible byte-order transformation.
- XOR operation with subkeys to introduce diffusion.

3.3 Encryption and Decryption Process

The encryption and decryption processes involve:

1. **Block-Based Processing**:
    - Input data is padded to align with the block size (32 bytes).
    - Blocks are processed iteratively through multiple rounds of substitution, permutation, and XOR operations.
2. **Symmetric Decryption**:
    - Inverts the encryption process, ensuring reversibility by using reverse substitution and inverse transformations.

---

4. Security Analysis

4.1 Strengths

- **Dynamic Elements**: The use of dynamic S-boxes and subkeys derived from both the key and IV ensures that encryption remains unique for each session.
- **Key and IV Lengths**: The 256-bit lengths for both key and IV exceed typical requirements, offering robustness against brute-force and cryptographic attacks.
- **Multiple Rounds**: The algorithm executes 32 rounds of encryption,

increasing the computational complexity for attackers.

4.2 Resistance to Known Attacks

- **Side-Channel Attacks**: Uniform operations across all inputs reduce vulnerabilities to timing or power analysis.
- **Differential and Linear Cryptanalysis**: Dynamic substitution and multiple rounds increase resistance to statistical methods of attack.

---

5. Practical Considerations

5.1 Performance

Despite its robust security features, UAC is designed to balance computational overhead and throughput. Its structure allows for:

- **Parallel Processing**: Blocks can be encrypted independently, optimizing performance in parallelized environments.
- **Hardware Acceleration Compatibility**: The algorithm can leverage modern cryptographic acceleration hardware.

5.2 Use Cases

UAC is suitable for:

- High-security applications requiring customizable encryption parameters.
- Quantum-resistant systems.
- Scenarios involving large-scale data encryption with unique IVs per session.

---

6. Conclusion

The Unified Advanced Cipher (UAC) offers a secure and flexible approach to symmetric encryption. Its emphasis on configurable key and IV lengths, dynamic cryptographic components, and multi-round processing ensures resilience

against current and future threats. Designed for adaptability, UAC is a strong candidate for secure communication in the post-quantum era.