MODE OF OPERATIONS ABSTRACT

Authenticating, Threading, Normalizing-IV, and Auto-keying Cipher Mode
("atnaCM": The Coeval Authenticated Encryption Cipher-mode)

SCOPE: NIST ATNACM CIPHER-MODE MODE PRE-SUBMISSION, ARCHITECTURE AND FUNDING REQUEST REVIEWS

ATNA-CIPHER
www.atnacipher.com, si@atnacipher.com
(408)-242-5016

1 Purpose Summary

The **design goals** for the atnaCM Cipher-mode, aka, "atnaCM," "atnaCM" are to exceed or be on-par to the best approved cipher-modes while adding new features and enhancing security as a PQC relevant symmetric solution over the current asymmetric PQC Cryptography.

- **Adding cipher-mode features enhancing ciphering, integrity, and security assurance.**
- Addressing exploitable elements in the current modes i.e., AES- (GCM | CBC | CTR | ...)
- Exceeding the speed-performance aspects of the current NIST approved cipher-modes.
- Compliant advancements over *NIST IR 8552, IETF RFC 9771, CESG, ENISA, ITSP40.111, ENISA, ...*

This document is a light executive summarization of the atnaCM series cipher-mode documents.

1.1 References

1. The atnaCM Cipher mode specifications (Available through licensing request)
2. The Hypercube and Crossed-Cube Specifications.
3. Mentioned standards.
4. https://csrc.nist.gov/Projects/block-cipher-techniques/BCM/Guidelines-for-Submitting-Modes (7/11/2022),
5. https://nsf.gov/funding/programs.jsp?org=OACTechnical

Technical Goal

1. *Authenticating – All modern cipher-modes mandate implied or explicit authentication.*
2. *Threading – Multiprocessing with a minimal critical serialization allows beyond Moore speedup.*
3. *Normalizing-IV - IV is very important, though IV normalization method ex.*
   To convert to a standard form or measure; adjust the value or values so as to conform to a standard measure or pattern; as, Post normalization probability adds up to 1.00. *From Collaborative International dictionary of English*
4. *Auto-keying – Performance trade-offs of key-exchanges are essential across different markets.*

1.2 Intellectual Property

[CURRENT WORK IS FILED UNDER EFS-ID AND INTERNATIONAL APPL. NO. PCT. WO 20231502488A1]

1.3 Version History

Version	Date	Author	Purpose
1.0	01-23-2026	Tushar J. Patel	First Corporate Cut

*1 – Reviewers/Designers can request 1) licensing pre-step and 2) design docs through the atnacipher.com website.

Table of Contents

*1 – Reviewers/Designers can request 1) licensing pre-step and 2) design docs through the atnacipher.com website.

2 Mode Specification Abstract

The **atnaCM Cipher-mode (i.e., Authenticating, Threading, Normalizing -IV and Auto-keying) cipher-mode (atnaCM)** is a new very advanced disposition cipher mode introducing many important features on top of the current NIST and industry requirements and recommendations for symmetric cipher-modes while also categorizing as an advanced form of CTR encryption, NIST IR8552, Accordion mode, and introducing coeval authenticated encryption (CAE) and coeval authenticated encryption with associated Data (CAEAD). This is a new area of science based on the following fundamental principles.

The fundamental property coordinates peers, enciphering states with independent cryptographic random-access zones represented by a **coeval state and specific coeval periodicity is composite and not just restricted to time,**

1. An abstract top-down, bottom-up or hybrid quantum bounding period for a set of keys, IV, reassembly markers and parallelization facilitating sliding cryptographic envelopes.
2. This random access and authorization permit controlled (or blocked) access to past, current, and future segments of a cryptographically protected payload and the cryptographic boundary restricts attacks to the coeval state specific protected segment or as an inverse definition, prevents total comprise of an enciphered payload.
3. Quantum attacks under atnaCM need to scale from N (current) to MNC $(atnaCM)$, where M is the multiprocessing factor, N represents the qubits required for a single segment quantum attack, C is the number of coeval periods.

Additional scientific terminology introduces Coevalogy (the science and subject matter), Coevalance, Coevalancity and other terms providing unique elements and properties that provide the logical and mathematical representations alongside the methodology for obtaining both theoretical and computational cryptographic security assurances.

Subsequently, **Coeval Authenticated Encryption with ACD (Authenticated ClearPass Data) Data (i.e., CAE and CAEAD) cipher-mode** shifts the paradigm from the **traditional IV based Enc./Dec.(IV, K, Hash-key, Message) to the Coeval-factored Enc./Dec.(Coeval (IV, Key, Integrity-Key)., Message)** system with coeval periods, auto-keyed key and IV refreshing cycles at deterministic intervals with the necessary, mandatory, and adept approved new **security assurance**s.

This document provides a light overview and justification for the rich feature set of the atnaCM cipher-mode, however, does not provide full details which are available by request or license (*1).

2.1 NIST/Industry Recommendation Compliance and Functional Summary

As recommended by NIST, atnaCM meets the following called-out requirements excerpted from the NIST CSRC Site on Block-Mode Ciphers and the NSF requirements on Cryptography/Block-Mode Ciphers.

*1 – Reviewers/Designers can request 1) licensing pre-step and 2) design docs through the atnacipher.com website.

Ref 1. https://csrc.nist.gov/Projects/block-cipher-techniques/BCM/Guidelines-for-Submitting-Modes (7/11/2022),

Ref 2. https://nsf.gov/funding/programs.jsp?org=OAC

Ref 3. https://csrc.nist.gov/pubs/ir/8552/final

2.2 Difference between AAD and ACD

ACD (Authenticated ClearPass Data) described in this document resembles the concept of GCM **AAD (Additional Authenticated Data)** field, however, comparatively,

1. It supports both bytes and bits while AAD is a size in bytes.
2. Like AAD applications, **ACD** allows passing SP800-38G format-preserving or similarly independently encrypted data, or unencrypted data in payload. This prevents.
   a) double encryption across the stack layers in well-designed applications,
   b) decryption at the security system perimeter for E2E encrypted applications (integrity and admission control is still an available security service) and
   c) large Data Loss Prevention at the security system and distributed application centric DLP. The differentiation in this is the formatting mechanics that reduce the complexity of upper layer protocols and applications.
3. Optionally, the semantics support atnaCM Virtual Halo Padding (VHP), a feature supporting padding in the cipher-mode while not mandating the need to transmit the padded bits or use 0-bit pads, however, it supports flexibly and distinguishing semantics to traditional padding methods.
4. ACD length support does not need to be conclusive (i.e., precinct) or restricted to fixed ACD sizes.
5. ACD supports an alignment section which can be a leading unprocessed preamble to the actual ACD data to allow traffic forwarding or processing, e.g., passing an unaltered Ethernet Header and SEC Tag in MACSec frames.
6. The design treats the alignment as separate than normal ACD to support online integrity and confidentiality for
   a. in-packet – Enciphering and authentication of a single payload, message or packet can multi-processed as opposed to just pipelined.
   b. Inline – Enciphering and authentication of a single payload, message and performing these tasks as data exits or arrives in a system. (*1)
   c. Online – Enciphering and authentication of a single payload, message as data traverses across the network with the ability to react to traversing anomalies without the need to store state information. (*1)
7. The semantics for ACD support essential malleability properties that are essential for security assurance, e.g., a method to prevent access to decrypted data prior to integrity verification or an optional feature override.
8. The semantics facilitate well-designed applications to perform inline encryption efficiently; this is different in that this element relates to the HW caching and memory fetching properties.

Hence, atnaCM terms it as ACD to distinguish it from AAD which does not include these properties.

*1 – Reviewers/Designers can request 1) licensing pre-step and 2) design docs through the atnacipher.com website.

2.3 Compliance Summary

Capability	Description
1. ***Security Function/Specific Function***	a. CAE/CAEAD – Coeval Authenticated Encryption with ACD data, PQC relevant advanced authenticated CTR mode with security assured unexchanged IV and auto-keying Key-Tree. b. It assures the missing FIPS assertions on runtime randomness quality/security strength of IV, Keys and Uniqueness of Counter-Block IDs, Key Confirmation, Data Driven key search
2. ***Error Propagation***	None, it is coeval authenticated.
3. ***Synchronization***	a. Coeval Integrity IV and Keys (i.e., periodic rekeying) and Coeval Encryption IV and Keys with random access capabilities. b. Fast Drop Tags (Programmable in SW/HW and FW)
4. ***Parallelizability and Scaling***	a. Parallel Processing (Solving N to M, where N and M are any $2^{T,}$ e.g., $2^0 = 1$ (i.e., T = 0). Current design for up to T <= 4096 individual cores/threads/processors. b. Parallel MAC synchronization and non-blocking MAC Reduction. c. Integral multiple of Cipher-Block Length (i.e., 16-Byte (for AES) or larger) and also supports block free designs. d. Encryption – Byte or Bit Level at least 128-bits (as per NIST recommendation) and Authentication – Byte or Bit Level
5. ***Keying and IV Material***	a. Seed, exchanged or pre-negotiated (minimum) b. Pre-configured or exchanged parameters used in KEY Derivations. c. Dual Keys – i.e., Different Integrity and Encryption keys.
6. ***Memory Requirements***	a. Scalable from Block Cipher to Ultra-High Performance b. Key Tree can scale to Ultra-High Performance
7. ***Preprocessing***	a. Key Tree and Counter Blocks can be precomputed. b. Accelerating algorithms are available. (***1**)
8. ***Message Length***	a. Single Pkt/block Up with improvement to 2^{14}, i.e., 16,384 Cipher Blocks of cipher-block-length. b. Single Pkt/block ACD can be up to 4G-Bytes. c. Aggregate is (about 2^{76}), in coeval max lengths are coeval period specific and supports scaling.
9. ***Ciphertext Expansion***	a. atnaCM expands messages from less than 16-bytes to a 16-byte minimum length. b. Supports 16, 24-, 32-Byte KCM and 8- or 16-Byte Fast Drop Tags (FDT), future versions may support additional sizes. c. Ciphertext can be same length as plaintext or support padding. d. ACD (Cleartext) retains its original size except in the case of specific operational modes.

***1** – Reviewers/Designers can request 1) licensing pre-step and 2) design docs through the atnacipher.com website.

10. PQC Relevancy	1. Due to Grover's Algorithm and/or Simon's Reduction attacks 128-bit AES blocks irrespective of the 256-key and PQC unsafe. 256-bit Rijn-Rijn (AES 256-bit equivalent) is quantum safe however requires substantial industry wide changes. CAE works with any cipher-block size (> 128-bit as per NIST advisories) and hence has potential candidacy for Quantum Resilience with the additional design to thwart AES 128-bit attacks and full stream compromise prevention (subject to operational caveats.) **2.** There are no elements of this specification subject to Shor's factorization algorithm and the implementation follows current and future NIST recommendations to use PQC approved methods.
11. Manufacturing and Fabrication	a. Systems can implement the methods in gate arrays, content addressable memory, application specific ICs, trusted platform modules, physical layer transceivers, network Processors, other similar Software, Hardware, or Firmware applicability including retargeting applications. b. It is possible to manufacture atnaCM HW, material fabrication estimates will be available later.
12. Firewall, Traffic Control and Law Enforcement	Supports the paradigms mentioned and introducing a new egress paradigm for Law Enforcement and Data Loss Prevention and fast receiver hand-offs to the application layer.
13. Other Features	a. Virtual Halo Padding and no fixed bit or byte paddings. b. An Integrity and Encryption Key Confirming MAC design. c. Fast Drop Tags for parallel processing and drop validation. d. Supports aligning ACD and unencrypted data separately. e. Extensible STEAM model – Cipher-Mode allows improvements over the initial design and the performance study of parallel, parallel blocking factors, scatter gather counters & other such elements. f. Coeval Key Tree and KDFs are available (***1**) g. Assurance through health tests for the IV and Keying Material. h. Defines the new FIPS-CC Vmap64 Continuous Test assuring that Coeval CTR blocks never repeat. i. Incorporates a new type of TCAM design.

Figure 1. atnaCM Cipher-mode summary

2.4 Features

1. The two most prominent features are a) **cryptographic coeval state for keys** and b) **the ability to solve single ciphering tasks using parallel multi-processing** without **pipeline deadlocks.**
2. Coeval state is the rolling auto-keying system that periodically resynchronizes for random access ciphering using the established coeval cryptographic elements, a) communication

***1** – Reviewers/Designers can request 1) licensing pre-step and 2) design docs through the atnacipher.com website.

amongst one or multiple peers, b) resilient subsequent decryption later. Coeval bound the payload enciphering Cryptographic Elements while supporting random access to past, present, and future coeval states.

a. Keys support **interpolated random-access resynchronization** within the **stream segmentation allowing access to ciphered segments selectively controlled through cryptographic authorization.**
b. Albeit coeval, atnaCM designs are compatible with existing key agreements methods currently in use like MACSec, IPsec, IKEv2/3, TLS1.2/1.3, SSHv2, and other protocols likewise.

3. **Supports Forward symmetric** encryption and per-packet **Parallel CTR-Mode.**
    a. atnaCM performs multi-processed encryption where the number of cores is a power of 2 ranging from **1 (i.e., 2^0) <= 2^T <= 4096 (i.e., 2^{12})** and the **decryption** on **any power of 2 <= 4096.**
4. Full Spectrum – Supports a) **"data in transit,"** b) **"data at rest,"** and c) **"size-preserving for sizes >= 16 (or other similar cipher-block length)" enciphering.**
5. **Ciphertext Adaptation and Reassembly** are cipher-mode specific where the frame sequence counters and AAL logic are ciphertext, while as, traditionally this is cleartext metadata. The **inbuilt service layer** allows **simplified multi-protocol adaptation** preventing the need for **protocols** to **implement cleartext protocol** markers **subject to identification and DoS attacks**.
    a. Using specialized **stream ciphering** preventing any weak cryptographic elements or clear text sequencing.
6. Byte or Bit – Operates in both **byte-mode** and **bit-mode** with a cipher-block-length minimum size. Bit-mode is for MPEG/SI and IoT type applications.
7. Wide Tweakable Macro Block (Cache-Line-Length) – Supports a macro block, namely, **cache-line-length** as a **multiple** of **the cipher-block length** separate for ACD and Encrypted Data referred to as ACD cache-line-length and Encryption Cache-line-length ($ecll$). This is the **unit of parallelism** to support **efficient ciphering** to match **multiple platform architectures** with applicability's ranging from **Links**, **IoT devices, Bit-Streams like MPEG, Audio, Streaming, File Encryption, Databases to Networking Protocols**.
    a. Additionally, it has support to allow such tweaks specific to individual payloads.
8. Virtual Halo Padding – It supports **stream cipher pseudo random padding** under the concept of **"Virtual Halo Padding"** supporting **optional expansion** modes for lengths greater than 16-bytes.
9. **Integrity Modes** - Additionally, the design supports two integrity calculation modes, namely**, a) contiguous block, i.e., commencement chunking or b) interleaved blocks, i.e., $acll$/partial acll block round-robin hence** supporting a wide range of peer-to-peer system designs for online integrity.
    a. The design allows validation of integrity at intermediary points within a relay.

*1 – Reviewers/Designers can request 1) licensing pre-step and 2) design docs through the atnacipher.com website.

   b. The Integrity keys are safe to share with intermediaries and do not map directly to encryption keys.
10. Integrity Key Confirmation – atnaCM supports **integrity verification by** with integrity **key confirmation as part of the Integrity tag verification.**
11. Encryption Key Confirmation – Supports an **encryption key early indication** within the integrity tag to reduce or eliminate decryption failures.
12. Fast Drop tags - Supports **Fast Drop Tags**, a **multi-processing** decryption **marker**, **egress and ingress coeval validation** and **bit-mode padding** indicator.
13. Speculative Decryption – Supports speculative decryption in terms of both keys and payload lengths.
14. Multi-Core KCM – Topology based parallel MAC convolved non-blocking into the final MAC.
15. Compatibility Model – Implementations **must implement** the **one mandatory hypercube model** (physically or virtually) such that the **solution** assures any **N-to-M including 1-t-1 peer-to-peer core computational compatibility**.
16. SVCID – atnaCM supports **peer svc identification (SVCID)** within **clusters, meshes, stacks or similar multicast/broadcast domains**, however, atnaCM **uniquely supports** this **cryptographically** at the **individual message level** of an aggregate connection.
17. Conclusive (i.e., prescient) and Inconclusive (i.e., non-presciect) – atnaCM is online in that integrity calculations can start as soon as data begins to arrive. atnaCM supports an additional inconclusive design where the cipher-mode can work as a true in-line system without requiring ACD or Ciphering Dat segment lengths at message ciphering commencement.
18. (Unconditionally Secure Symmetric (speculation) – A speculative thought is that atnaCM is unconditionally secure as no amount of ciphertext can lead to knowledge of the plaintext.
19. ***CAE(AD)*** *–This is the PQC generation Coeval Authenticated Encryption based on the use of coeval states and properties to perform ciphering and Coeval Authenticated Encryption with ACD (aka Authenticated ClearPass Data) Data to facilitate safeguarding ClearPass stack elements like TCP/IP headers and similar SDN, OpenFlow, Route, Switching and other similar networking or forwarding elements.*
20. The design introduces a novel and first of its kind design specific TCAM that improves the network ingress and egress switching fabric interface designs.
21. Design supports capabilities of high-speed encryption requiring 1.2 Billion pkts. /sec. or more data encryption rates corresponding to an 800Gbps encryption link.
22. This design plans to disrupt the existing fire-wall security system, load-balancing and DLP security systems be it appliances, cloud virtual machines, or containers.
23. (Speculation) Ledger Compression – One of the goals of atnaCM is to facilitate smaller digital cryptocurrency and other digital fintech ledgers. A ledger entry is about the size of a private key, some data/metadata and some form of a private key hash signature, we approximate that an atnaCM based solution can reduce this by reducing the initial size of participating in a digital ledger and b) minimizing the size of an individual ledger entry while additionally permitting enroute arbitration and embedding necessary assurances within the ledger entries itself and optionally support or restrict the mining capabilities itself. This is a

*1 – Reviewers/Designers can request 1) licensing pre-step and 2) design docs through the atnacipher.com website.

work in progress and hope systems would consider this alternative ledger organization within their individual ledgers.

NOTE: The approved symmetric cipher is the Advanced Encryption Standard (AES/Rijndael), a 128-bit block cipher. Hence, within this document the stems "CIPH"/" AES" are interchangeable with each other as atnaCM is cipher agnostic.
atnaCM is bit-size agnostic, however, specifically designed to support 64-bit or higher processor architectures. It scales and can leverage AVX-512 systems.

3 Mode of Operation Abstracts

The atnaCM Cipher-mode augments and advances the fundamental CTR mode specifications in SP800-38A, and addresses known limitations in the Authenticated Encryption specification of SP800-38D.

3.1 Performing Encryption and Integrity Calculation

1. By applying a key (K) generated as part of a periodic rolling window key tree (***1)** to a series of counter blocks (T_1, T_2, ..., T_n)), where each counter block is comprises of the Coeval state incorporating the standard incrementing counter (1 ... n).
2. The Coeval state counter derivations use a unique non-sequential mathematical algorithm (***1**)
3. When using multiple cores, the Integrity tag includes a distribution root allowing intermediaries or receivers to infer ids of the other cores using mathematical and logical of the topology. (***1**)
4. During counter block encryption, systems can calculate the MAC on a single unit or in parallel with multiple units (i.e., thread, cores, processor, ciphering units.) using deadlock free algorithmic reduction of per unit multiple MACs.
5. The system supports Integrity Tag comprising of MAC and Fast Drop tags that allow a) payload integrity, b) integrity and encryption key confirmation and c) drop period validation.
6. Initiators can be conclusive (indicating length) inconclusive (no length indications) in exclusive Authentication, Confidentiality or Authentication and Confidentiality combined Modes with support for markers and a remapping system allowing intermediate nodes and endpoints to process inconclusive frames.
7. One of the most prominent features is Fast Drop Tags at the head of the frame to support online integrity (validation of integrity as frames arrive) and highly probable key asserted speculative decryption (online encryption) alongside integrity.

3.2 Performing Integrity Verification and Decryption

1. Evaluating the FDT and discarding the message if it is not valid.
2. Next, online verification validates that the MAC confirms both i) the keys and ii) the integrity of the transmission against the calculated MAC or parallelly computed MAC.
3. Finally, the system performs atnaCM specialized counter mode encryption with K and counter blocks (T_1, T_2, ..., T_n), note: the key confirmation steps assures that the decryption will have the right keys.
4. AtnaCM is online system with speculative decryption to eliminate recirculation or dual key processing. Speculative decryption allows decrypting alongside integrity calculation using the current coeval integrity and encryption keys.

***1** – Reviewers/Designers can request 1) licensing pre-step and 2) design docs through the atnacipher.com website.

5. Non-blocking reduction is the topology-based design that convolves multi-processed individual MAC calculations based on the contiguous or interleaved integrity selection into the final MAC.
6. Receiving can be both conclusive (lengths are known when payload processing commences) or non-conclusive (as payload arrives) without requiring any additional support.

3.3 Comparing atnaCM with GCM and CCM

Feature	CIPH-GCM	CIPH-CCM	CIPH-atnaCM	Details ✓ (Supported), × (Unsupported), ≥ Advanced, ±(subjective), ?? inadequate info. ≅ (Almost equivalent)
1. HW/FW/SW	✓✓✓	✓✓✓	✓✓✓	FW, HW or SW Implementations can all use the ATNA Cipher-mode
2. **AEAD/AAD/ACD**	✓(AAD)	×	✓ (CAEAD) ≥ (AEAD)	Coeval Authenticated Encryption with ACD Data atnaCM supports advancements over traditional AAD
3. **Counter - Forward**	✓	✓	✓	Forward Symmetric Ciphers with no inverse cipher operations necessary.
4. **Parallel Integrity**	×??	×??	✓	ATNA supports a parallel Integrity model with the proprietary Simple Threaded Networking MAC (**STNMAC.**)
5. **MAC**	✓GMAC/GHASH	None	✓STNMAC	**The parallel design of AES-GCM appears hindered by the ordering dependency of the previous block in the GHASH multiplier, atnaCM instead has a parallel collection that still applies a data dependent transformation, however, should be a performance improvement over the GCM Tag.**
6. **Parallel Encryption**	✓??	✓??	✓	Methods in the atnaCM articulate methods supporting encryption in parallel, i.e., the capability to encrypt multiple payloads or blocks of a single payload message. Most specifications allude to the specifics of allocations, processing, routing topologies, or core-designs and leave it ambiguous or to protocol layers; contrarily, atnaCM has them inbuilt.
7. **In-Pkt Parallel**	??	??	✓	atnaCM defines a multiprocessing model for encrypting or decrypting payload cipher blocks because most specifications do not cover payload specific allocations, processing, routing. topologies or core designs, e.g., **GCM does not define any schedule/topology for payload specific parallel models. Here, atnaCM does and while the model may look cumbersome, it is at least equivalent or better than undisclosed parallel system communications between encrypting devices and decryption devices (i.e., compute/verify tag and decrypt)**
8. **Topology Based Parallel**	??	??	✓	Albeit specifying the base Hypercube and Twisted-Cube topologies atnaCM supports topology-based extendibility. This is necessary because the GCM and CCM specifications do not cover processing, routing topologies, or core-design.
9.				
10. **Integrity Finalization and Key Confirming MAC**	×	×	✓ ≥	atnaCM is the first of its kind MAC to introduce early key confirmation within Integrity finalization.
11. **Integrity**	Mapped key. Online	Not online No-Integrity Key	Online Dual-unmapped	GCM Hash key is a fixed map of the Encryption Key Online – Integrity as data arrives. Dual-Key – Independent keys for integrity and encryption Unmapped – Independently derived.
12. **IV in Pkt.**	✓	✓	X ≥ (Advantage)	Traditionally, HW inserts frame headers or IV at the head of the packet hindering the packet pipeline in implementations, here, atnaCM rids of this leading extra preceding frame or explicit IV.
13. **Head of Packet insertion**	✓	✓	X ≥ (Advantage)	SPI, sequence numbers, and similar attack prone elements are necessary at the head of packet.

*1 – Reviewers/Designers can request 1) licensing pre-step and 2) design docs through the atnacipher.com website.

				atnaCM incorporates methods preventing such attacks.
14. Padding	×	×	✓/×/ ≥ (Optional)	Padding allows aligning partial blocks to the cipher block. While modes like GCM and CCM do not require explicit padding, most networking protocols implement padding externally (e.g., IPsec ESP) when using these modes. Also, short segments can leak information in most single key block ciphers based on transmission length. atnaCM is configurable with bit, byte and additionally atnaCM padding is random, optional, and used in calculations.
15. Coeval/Time-Synchronization	×	×	✓	atnaCM is the first of its kind Coeval Authenticated Encryption (with ACD data)
16. Embedded Adaptation and Reassembly	×	×	✓	atnaCM simplifies protocol operations with inbuilt secure methods for both single unit and parallel unit adaptation and reassembly, thereby, preventing attacks.
17. Parallel Path Aware	×??	×??	✓≥≥	atnaCM is the first of its kind cipher-mode than has coeval parallel and multi-processing properties – Very Advanced
18. Random Bytes Source	×	×	✓ (	atnaCM mandates approved randomness sources.
19. Complexity Operation	MAC Multiplication	Formatting and Cipher-Operations	ALU (no multiplication)	Assuming all implementations have AES Cost, the complexity cost is based on the other requirements.
20. Ingress Filter	×	×	✓	Most cipher-modes do not provide methods to Ingress Check (keys/iv) on interfaces. atnaCM is the first of its kind that does a key confirmation step. Ingress is based on Integrity Keys, so implementations can check the integrity without full decryption.
21. Egress Filter	×	×	✓	Most cipher-modes do not provide methods to Egress check (keys/iv) on interfaces. atnaCM supports an Egress check based on Integrity Keys and Encryption Keys, so implementations can check the integrity with or without full decryption.
22. Ingress/Egress Filtering Advantage	×	×	✓	Ingress and Egress networks need to bind the keys to the interface. One Advantage in atnaCM is that the Ingress and Egress filters can bind the payload to the consuming application without knowing the interface, reducing the necessary networking prefix match, e.g., fast punt of socket data to an application without going through the full interface/socket domain layering (though protocol checksums should be validated by implementations.)
23. Approved	✓	✓ (not for widespread use)	× (To submit)	atnaCM is not yet an approved cipher-mode, however building blocks are approved methods.
24. Alignment Support	×	×	✓	atnaCM supports preamble and mid-amble alignments.
25. Bit-Mode	×	✓	✓	atnaCM, like CCM, support both bit-mode and byte-mode, GCM is byte mode.
26. Byte-Mode	✓	✓	✓	All implementations support byte-mode
27. Cache-Line Adjusted	×	×	✓	atnaCM supports wide block cache-line lengths (might be only AES cipher-mode supporting it)
28. Speculative Decryption	✓≅	✓≅	✓	All implementations can support safe speculative decryption and is the only one that pre-confirms the key. Ingress checking assures encryption key matches.
29. Session Multi-Key	×	×	✓	In GCM and CCM, the key is the same throughout the session or with a rekey. atnaCM has multiple keys in a session with/without an external rekey.
30. In-Flight (Data in Flight)	✓	✓	✓	Supported
31. Resilient/Persistent (Data at Rest)	✓±	✓±	✓±	Supported – Though there are quirks in each.

*1 – Reviewers/Designers can request 1) licensing pre-step and 2) design docs through the atnacipher.com website.

32. Patent	x	×	✓ (Filed)	
33. ACaaS	??	??	✓	atnaCM can allocate/distribute multi-core to specific services, connections, VMs, containers, interfaces, or similar abstractions. This in combination with the ingress/egress filtering is very advantageous.
34. Pitfalls	Few	More	Provided later	atnaCM may have pitfalls that will slowly be evident over time, however, the initial analysis seems acceptable.

3.4 Key Establishment

NIST articulates the approved KDFs and key agreements within the SP-800-56 and SP800-57 set of standards and the new PQC standards. These are part of the upper protocols and apart from provisioning, atnaCM is agnostic to these procedures.

4 Size-Preserving Applications

atnaCM by design has the added benefit that encryption data elements >= 16 can benefit from the size-preserving properties of atnaCM if implementation retain the integrity tag (or FDT at least) and hence, available at decryption. Methods also support the use of fixed elements to simplify such retention. Implementations can store individual MACs in case such storage is efficient or store the cumulative final MAC. The MAC is also a tokenized or pseudonym representation (non-secure hash) of the data. One application is to store this in a permanent store archive and pass it for decryption on or off the permanent store (HSM.) This is different than CTR which is not coeval authenticated and requires HMAC/CMAC for non-coeval authentication.

**Comparative to AES-FF1 and AES-FF2, there is no format preserving, however, size preserving (>= 16), however, the output is a unique token (32-bytes) that must be available when decrypting. Please note that atnaCM does address the issue requiring minimum entropy in the data fields (e.g., AES-FF1 would leak data on data elements < 1,000,000 in entropy.) This is essential for database type applications where the column records of a fixed size. The 32-byte tag is necessary for decryption. There is no secrecy required for the tag.

Note: Though not exact format preserving, it is easy to map combinations of 16-byte fields for format preservations.

5 In Transit Encipherment (Data in Transit)

atnaCM is versatile for Data in Transit ciphering applications, with the simplest forms shown below,

The data in transit encryption (aka CAEAD) is designed to protected exchanges over mediums like wires (e.g., Ethernet, PON, ...), wireless (e.g., 802.11xx, Bluetooth, ...) and other OTAR methods with rolling cryptographic mutually independent coeval state properties providing the necessary quantum proofing (not mandatory). **Note: The keys change according to the application specific coeval settings.**

[Maybe blank due to diagram paging]

*1 – Reviewers/Designers can request 1) licensing pre-step and 2) design docs through the atnacipher.com website.

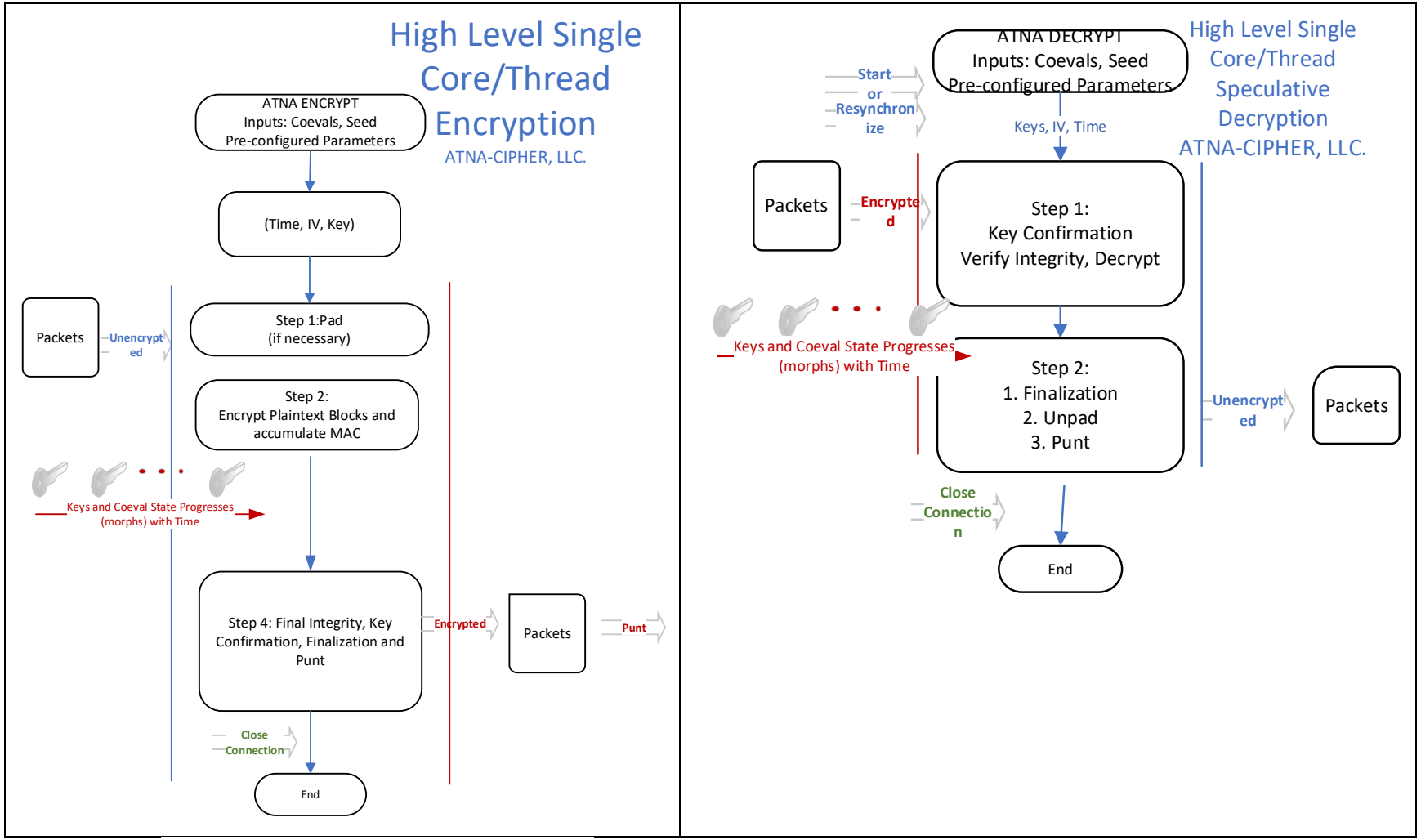

Figure 2. High Level "In-Transit" Encipherment

*1 – Reviewers/Designers can request 1) licensing pre-step and 2) design docs through the atnacipher.com website.

5.1.1.1 Pros

1. This transfer is PQC relevant for the reduction of AES-256 to AES-128 due to QKD/Grover's Algorithm requiring brute force on every coeval key set, hence, raising the bar for Quantum attacks.

The configurable key and rekey periods support most connection bandwidths, e.g., a) broad connections like 800+GB (80 x 10GB with 24-hour period) channels) MACSec, b) extremely deep VPN connections (like 1 10GB for 1 year or more) and c) space applications like long-haul satellites with 2 Mb/sec. *At the current time, high speed systems support about 1.2 billion messages per second after proofing and hardware implementation, the theoretical max of this mode is more than the above rate.*

2. The design can work alongside systems that do not have any Shor susceptibility. CAE additionally augments this with specialized functionality. The recommendation is to use PQC for coeval key Establishment.
3. The transit stream random access synchronization of a coeval period is one of the most important properties in transit encipherment allowing service guarantees for re-establishment.
4. atnaCM supports groups methods allowing,
    a. For groups – New Joins can inhibit the new joiners from access to previously transmitted data.
    b. For groups – Leave actions can inhibit access to later data segments.
    c. Seeding for groups, random access synchronization
5. Support for bit-mode applications like the different MPEG or Audio streams including Authenticated ClearPass Data that allows the outer layers to skip any prior encrypted sections or data that must transit in the clear while supporting authentication of the payload. (Tokenization/SP800-38G AES-FF1/AES-FF3)
6. Transit in traditional HW or FW based accelerated ciphering requires a subset of three inserts, a) IV at head of payload triggering data movement during in-line in-place encryption, b) Padding and c) Integrity Tags. AtnaCM restricts this to a single trailer with lengths supported by most OS kernel buffering.
7. atnaCM a) no explicit IV, a) Padding is optional when $len >= 16\ bytes$ and b) Integrity Tag support compatible 16,24- and 32-byte Key Confirming MAC Tags.

*1 – Reviewers/Designers can request 1) licensing pre-step and 2) design docs through the atnacipher.com website.

6 Resilient Encipherment (Data at Rest)

atnaCM is versatile for "Data at rest" applications and the simplest form using coeval counters is below.

1. The primary security requirement is to establish one or more identical coevals for the complete encryption task.
2. If the coeval cannot be reestablished, then decryption is not possible.

[Maybe blank due to diagram paging]

*1 – Reviewers/Designers can request 1) licensing pre-step and 2) design docs through the atnacipher.com website.

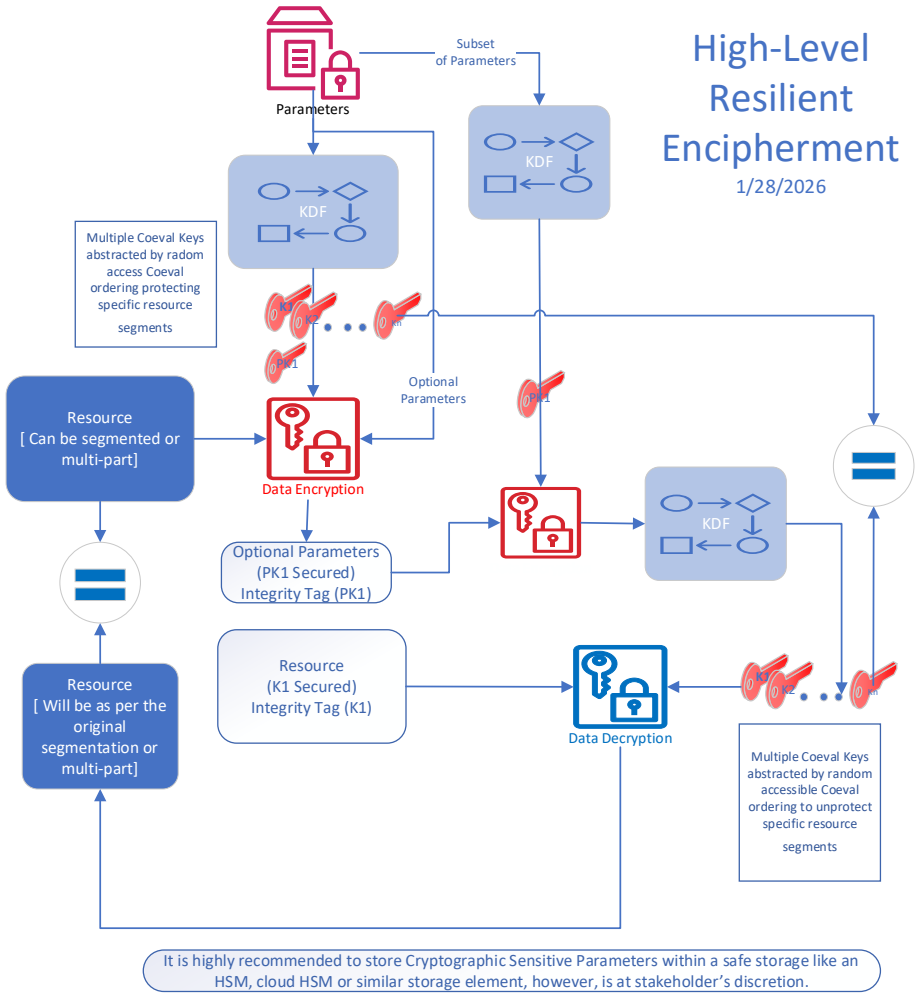

Figure 3. High-Level Resilient Encipherment

1. Under atnaCM the system has equivalency with currently approved encipherment methods.
2. The difference is that Coevals allow the auto-keying to vary the key across the resource segments.
3. The Integrity Tag is optional for decryption.
4. Why is atnaCM an excellent choice for Data at Rest Applications?
    a. Unlike traditional ciphers, a compromise of one key under atnaCM is only a partial resource loss.
    b. The Coeval system is flexible and full resource loss is a compromise of the complete set of parameters and KDF, in short, an internal attack.
    c. ACD support permits transparency for SP800-38G, tokens or other data needs.
    d. Supports both bit-mode (like parts of stored MPEG) and byte mode (like files/database).
    e. Size preservation is also supported.

Unattached padding are tokenized elements of the data, caveat, a 16-byte minimum requirement.

*1 – Reviewers/Designers can request 1) licensing pre-step and 2) design docs through the atnacipher.com website.

7 Conclusion

As seen atnaCM has the potential to be the primary choice in cipher-modes augmenting the current disposition of cipher-modes while introducing new advanced features addressing the known exploitable weak elements in other cipher modes. The current PoC results show a good speed-up over the baseline GCM and are available at atnacipher.com and subsequent potential to exceed that number. It also is a true cryptographic application that can work with advanced vector extension architectures like AVX-512.

We appreciate any feedback, requests to present or requests for additional information and subsequent support for facilitating NIST's approval of the atnaCM cipher-mode or collaborating with us for the first-generation advanced end-to-end ciphering and security services.

Also, we cannot succeed without the support of the cryptographic community, and we welcome peers or industry veterans to join in this effort to help facilitate one futuristic core element for the PGC-Gen era of data protection.

Thank you,

Tushar J. Patel
Owner, Lead Architect,
https://www.atnacipher.com
ATNA-CIPHER

*1 – Reviewers/Designers can request 1) licensing pre-step and 2) design docs through the atnacipher.com website.