MODE OF OPERATIONS ABSTRACT

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

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

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

Purpose Summary

The design goals for the ATNA Cipher-mode, aka, "ATNA," "atnaCM" are to exceed or be on-par to the best approved cipher-modes while adding new features and enhancing security for PQC-Gen Cryptography.

- Augmenting cipher-modes with well-established missing enhanced ciphering and integrity properties.
- Addressing pitfalls in the best of class ciphers (Authenticated Encryption, i.e., /AES-GCM.)
- Exceeding the speed-performance aspects of NIST approved cipher-modes.
- Additional new features for establishing the cipher-mode the better choice for security.

This document is the Mode of Operation Abstract, one of the specifications from the full set of atnaCM series of documents describing the cipher-mode.

This document should be self-contained and allows a simple executive overview of the cipher-mode.

1.1 References

1. NIST CSRC Cipher Mode Specifications (Available through licensing request)
2. 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=OAC

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	12-24-2023	Tushar J. Patel	Updates with new details.

*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 **ATNA (i.e., Authenticating, Threading, Normalizing -IV and Auto-keying) cipher-mode (aka ATNA, atnaCM)** is a new very advanced disposition cipher mode introducing 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, coeval authenticated encryption (AE) and coeval authenticated encryption with associated Data (CAEAD). This a new area of science based on the following fundamental pronciples.

The fundamental property coordinates peers with a random access cryptographic **coeval period,** an abstract time quantum bounding period for a period specific set of keys, IV, reassembly markers and parallelization constructs. This random access and authorization permits controlled (or blocked) access to past, current, and future segments of a cryptographically protected payload and the cryptographic boundary restricts attacks to the specific segment within a specific coeval period. A full scope Quantum attack needs to scale from, N to (NC), where N is the qubits required for a single quantum attack and C is the number of coeval periods.
It additionally defines a comprehensive set of definitions namely, Coevalogy, Coevalance, Coevalancity and other related Coeval Terminology covering the comprehensive specification and mathematical representations available through a license request on atnacipher.com.

Subsequently, it introduces Coeval Authenticated Encryption with ACD (Authenticated ClearPass Data) Data **(i.e.,** CAE and CAEAD**) cipher-mode** shifting paradigms from **traditional IV based (IV, K, Hash-key) to time-factored (Time, IV, Key, Integrity-Key)** system with coeval periods, auto-keyed key and IV refreshing cycles at deterministic intervals with the necessary, mandatory, and adept approved **security assurance**s **missing** in **traditional cipher-modes** for **PQC (aka OQC-Gen (Post-Quantum Cryptography Gen) and FIPS-CC (FPS 140-3/NDcPP, ISO-27001) relevancy**.

This document provides a light overview and justification for the rich feature 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, ATNA 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.

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

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, similarly independently encrypted data, or unencrypted data in payloads. 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 supports distributed application centric DLP.
3. Optionally, supports ATNA 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.
4. ACD length support does not need to be conclusive 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.

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

** The design treats the alignment as separate than normal ACD to support online integrity for in-packet multi-processing. (*1)

Hence, ATNA 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) d. Encryption – Byte or Bit Level at least 128-bits 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 time-period specific and supports scaling.
9. *Ciphertext Expansion*	a. ATNA expands packets from less than 16-bytes to a 16-bytes 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 padded. d. ACD (Cleartext) retains its original size except in the case of specific operational modes.
10. *PQC Relevancy*	1. Coeval Authenticated Encryption is PQC relevant as Grover's Algorithm may only brute force AES-256 sub-sections at AES-128 strength, however, the atnaCM methods thwart this and full stream decryption should be computationally impossible. 2. There are no elements of this specification subject to Shor's factorization algorithm and the implementation follows current and will follow 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 ATNA 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. Integrity and Encryption Key Confirming MAC. c. Fast Drop Tags for parallel processing and drop validation. d. Supports aligning of ACD and Unencrypted data separately. e. Extensible STEM model – Cipher-Mode allows improvements over the initial design and the study of performance of parallel, parallel blocking factors, scatter gather Counters, others. f. Coeval Key Tree and KDFs are available (*1) g. Assures heath tests for the IV and Keying Material sources. 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. ATNA 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 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.

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

   a. Keys support **interpolated random-access resynchronization** within the **stream segmentation allowing access to ciphered segments selectively controlled through cryptographic authorization.**
   b. Albeit coeval, ATNA designs are compatible with existing key agreements methods currently in use like MACSec, IPsec, IKEv2/3, TLS1.2/1.3, SSHv2, and other likewise protocols.
3. **Supports Forward symmetric** encryption and per-packet **Parallel CTR-Mode.**
   a. ATNA 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 protocols** 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.
   b. The Integrity keys are safe to share with intermediaries and do not map directly to encryption keys.
10. Integrity Key Confirmation – ATNA 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 – ATNA supports **peer svc identification (SVCID)** within **clusters, meshes, stacks or similar multicast/broadcast domains**, however, ATNA **uniquely supports** this **cryptographically** at the **individual message level** of an aggregate connection.
17. Conclusive and Inconclusive – ATNA is online in that integrity calculations can start as soon as data begins to arrive. ATNA 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 ATNA is unconditionally secure as no amount of ciphertext can lead to knowledge of the plaintext.

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

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 egress and ingress 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 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 ATNA is cipher agnostic. ATNA 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 ATNA 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.

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

2. Next, online verification validates the transmitted KCM is against the calculated MAC or parallelly computed MAC using Key Confirmation for minimized errors.
3. Finally, the system performs 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.
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 ATNA with GCM and CCM

Feature	CIPH-GCM	CIPH-CCM	CIPH-ATNA	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 ATNA 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, ATNA 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 messages. Most specifications allude the specifics of allocations, processing, routing topologies or core-designs and leave it ambiguous or to protocol layers; contrarily, ATNA has them inbuilt.
7. In-Pkt Parallel	??	??	✓	ATNA 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, ATNA 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 ATNA 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	×	×	✓ ≥	ATNA 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

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

				implementations, here, ATNA 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. ATNA 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. ATNA is configurable with bit, byte and additionally atnaCM padding is random, optional, and used in calculations.
15. Coeval/Time-Synchronization	×	×	✓	ATNA is the first of its kind Coeval Authenticated Encryption (with ACD data)
16. Embedded Adaptation and Reassembly	×	×	✓	ATNA simplifies protocol operations with inbuilt secure methods for both single unit and parallel unit adaptation and reassembly, thereby, preventing attacks.
17. Parallel Path Aware	×??	×??	✓≥≥	ATNA is the first of its kind cipher-mode than has coeval parallel and multi-processing properties – Very Advanced
18. Random Bytes Source	×	×	✓ (	ATNA 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. ATNA 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. ATNA 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 ATNA 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)	ATNA is not yet an approved cipher-mode, however building blocks are approved methods.
24. Alignment Support	×	×	✓	ATNA supports preamble and mid-amble alignments.
25. Bit-Mode	×	✓	✓	ATNA, 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	×	×	✓	ATNA 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. ATNA 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.
32. Patent	x	×	✓ (Filed)	

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

33. ACaaS	??	??	✓	ATNA 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	ATNA 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, ATNA is agnostic to these procedures.

4 Size-Preserving Applications

ATNA by design has the added benefit that encryption data elements >= 16 can benefit from the size-preserving properties of ATNA 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.

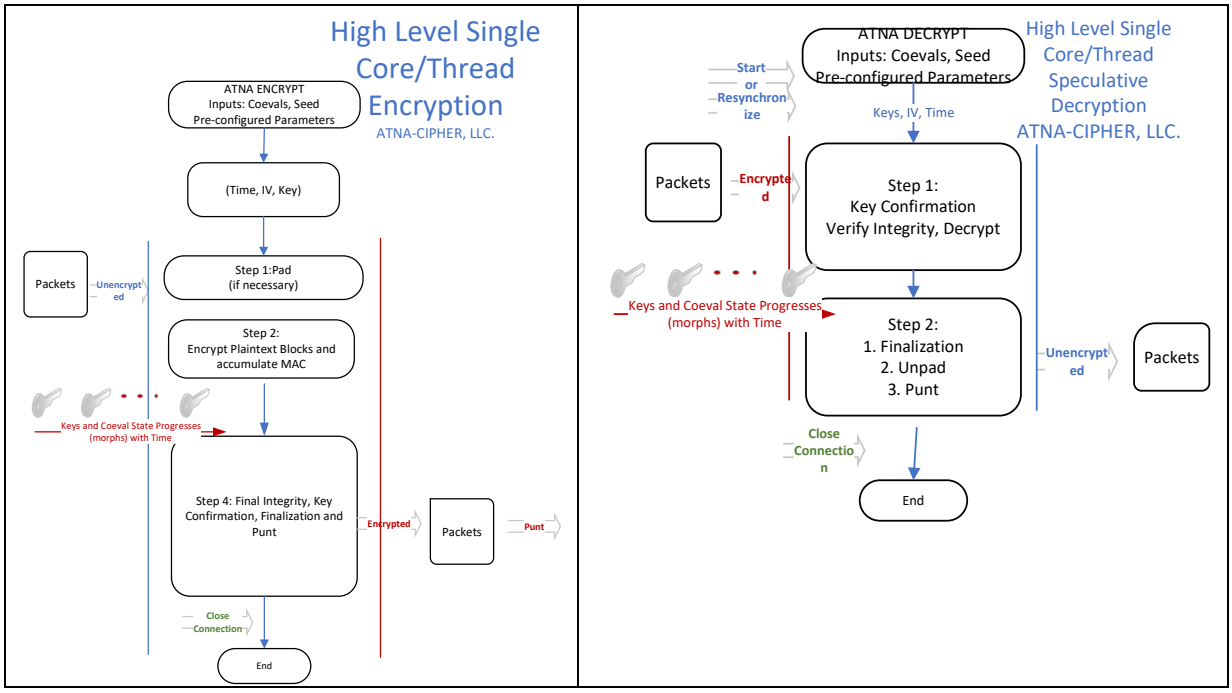
**Comparative to AES-FF1 and AES-FF2, there is no format preserving, however, size preserving (>= 16), however, the output is a unique token (32-bytes) that must be available when decrypting. Please note that ATNA does address the issue requiring minimum entropy in the data fields (e.g., AES-FF1 would 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)

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

The transfer complies with protected exchanges over mediums like wires (e.g., Ethernet, PON, …), wireless (e.g., 802.11xx, Bluetooth, …) and other OTAR methods. **Note: The keys change with coeval periods.**



*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

5.1.1.1 Pros

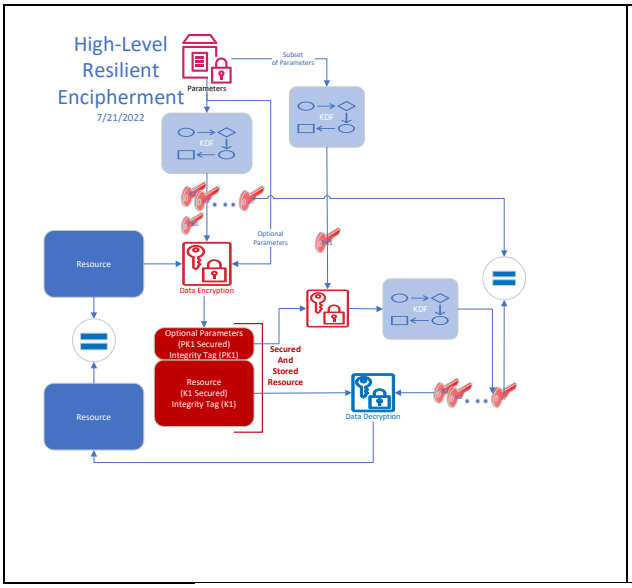
1. This transfer is PQC relevant for the reduction of AES-256 to AES-128 due to QKD/Grover's Algorithm requiring brute force on every coeval key set, hence, raising the bar for Quantum attacks.

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 packets pe 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. ATNA 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. ATNA 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.

6 Resilient Encipherment (Data at Rest)

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



1. Under ATNA the system has equivalency with currently approved Resilient Encipherment methods.
2. The difference is that Coeval Counters allow the auto-keying to vary the key across the data segments.
3. The Integrity Tag must be available at decryption, and it is optional to store it with the protected resource.
4. Why is ATNA an excellent choice for Data at Rest Applications?
    a. Unlike traditional ciphers, a compromise of one key under ATNA is only a partial resource loss.
    b. The Counter 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 is available in case SP800-38G/Tokenization or similar where data needs to be clear.
    d. Supports both bit-mode (like parts of stored MPEG) and byte mode (like files/database).
    e. Databases benefit with the added security of IV/padding without requiring length adjustments.
    f. Unattached padding are tokenized elements of the data, caveat, a 16-byte minimum requirement.

Figure 3. High-Level Resilient Encipherment

*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, LLC.,

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