ATNA-CIPHER, LLC.*(ACL)*

ATNA Cipher-Mode Design Summary

Tushar Patel
Lead Architect/Owner

ATNA-CIPHER, LLC.
(408)242-5016
si@atnacipher.com
P/O. Box 2130, Sunnyvale, CA 94087

Solution Theory is Rooted in New Science and Innovation

- Coevalogy - *This is the science of establishing mutually exclusive binding cryptographic properties between peers based on time and other associated security domain parameters, properties or attributes.*
- All network protocol use timers for defining refresh, however, getting these semantics has been a challenge for many years, hence, a Coeval paradigm simplifies much of this confusion.
- Coevalance – *These are the definitions of the mandatory coeval domain parameters or properties for CAE.*
- Coevalancity – *Are the individual application's set of qualitative and quantitative properties measured as a vectored representation of the coeval properties in relation to a primal event and associated factors or subsequent isochronal events and indicates the relationship metric of the coeval property with reference to the specific primal or successive isochronal point.*
- Coeval Terminology– *An entity be it a state, grouped properties or functionalities that collectively represented as a single to meet the definitions covered by the presented covalence properties*
- *** This topic is covered in detail within the atnaCM specifications.*
- *The innovation is the novel science, methods of creating and defining the architect for the scalable multipliers as properties of an interconnection topology and the minimalistic overhead methods.*

Definition Changes

- ACD – Authenticated Clear-pass Data – This is like AAD (Additional Authenticated Data), however, is a superset to AAD with many additional important security properties.
- UD – Unencrypted Data – This is the part of data that will get encrypted.
- Plaintext – This is ACD + UD
- ED – This is the encrypted version of UD, need not be th same size as ED.
- Ciphertext – ACD + ED
- FDT/EDFT – Fast Drop Tag and Extended Fast Drop Tag for parallel processing and attack prevention.
- Integrity Tag – The integrity check over the Ciphertext
- Verification Tag – The combination of FDT/EFDT + Integrity Tag

Motivation (Cipher-Mode Design and Attacks)

- Comply to Accordion Tweakable cipher-modes, Authenticated Encryption/AEAD, Counter-Mode (CTR).
- Address attacks based on zero byte padding after Sweet32
- Mitigate the concern where a big data correlation map of known plaintext and ICVs can identify keys due to the AES-GCM hash key design.
- Provide an optimal solution for IV reuse attacks.
- Moving the needle beyond the current pipelined encryption designs.
- Additionally, we see a window of opportunity to address concerns and skepticism over AES-GCM(-SIV)
- Mitigate using different cipher-modes for transport, at rest and size-preservation.
- Establishing Accordion compliant Coeval Authenticated Encryption (CAE) as one of the most viable cipher-modes for PQC Era encryption.
- Support Safe Speculated Decryption (no it is not a form allowing Spectre and Meltdown style attacks.)

Motivation (Advanced/Quantum Computer Attacks)

- Future “Store and decrypt Later” issues using Shor’s general number field-sieve polynomial factorization.
- AES-GCM Polynomial may get impacted by quantum computing. “atnaCM” is polynomial free
- Grover’s Algorithm based attacks impacting 128-bit ciphers. “atnaCM” supports scales to any bit size
- We see a window of opportunity currently to ride alongside the PQC Transition.
- Key Dependent Input/Message Security (KDI/M)
- Beyond Birthday Bound Security (BBB)
- Accordion All or None (AIoN) – Accordion requirement preventing implementations to allow partial decrypted blocks in case any bit(s) of the ciphertext are corrupted.
- Accordion types,1) AEAD, 2) Tweakable Decryption and 3) Deterministic Authenticated Encryption.

Motivation (Networking Issues)

- Solve the nightmare of confidentiality offsetting absence which hinders routing, switching and load-balancing in networks.
- Optimally solve the Protocol PKT-ID based CTR Block encryption issue
  - 32-bit counters face future attacks and larger counters have flow control issues.
- Work within existing TCAM bounds, however, provide a next generation TCAM design.
- Support HW, FW and SW applications.
- Edge-Intermediate routing: Property allowing edge or intermediate to perform re-routing (no loss of security.)
- Facilitate efficient high-scale networking ingress/egress designs.
- **Scalable, secure, and efficient data solutions** for ultra high-speed transport symmetric encryption designs at **rates exceeding 1.2 billion pkts./second or more**, about 800+Gbps
- Support VMDOS networks (VMDOS: VXLAN/LAN/VPN, Mesh (VM/Cloud/Container), DPA, OpenFlow, SDN)

Core Feature List: 1

1. Three most prominent features
   - **Cryptographic coeval state for keys.**
   - **Solving single ciphering tasks using parallel multi-processing and pipelines** without **deadlocks.**
   - **Accordion mode Compliance a) Three types, b) KDI/M Security , c) BBB, 4) All or None Decryption**
2. Interpolated random-access resynchronization
   - The **segmentation stream allowing access to ciphered segments selectively controlled through cryptographic authorization in varying granularities.**
3. Protocol Compatibility
   - Albeit coeval, “atnaCM” designs are compatible with existing key agreement methods for most used protocols, e.g., MACSec, IPsec, IKEv2/3, TLS1.2/1.3, SSHv2.
4. Supports Forward symmetric with per-payload Parallel and Pipelined CTR mode.
   - ATNA performs multi-processed encryption where the number of cores is a power of 2 **within the range 1 (i.e., 2^0) <= 2^T <= 4096 (i.e., 2^{12})** and the **decryption** on **any power of 2 <= 4096.**

Feature List: 2

5. Full Spectrum
   - Supports a) **“data in transit,”/Accordion 1** b) **“data at rest,”/Accordion 2, and** c) **“size-preserving for sizes >= 16 (or other similar cipher-block length)”and/or Accordion 3 enciphering.**
6. **Inbuilt Cipher-mode Specific Ciphertext Adaptation and Reassembly**
   - Frame sequence counters and AAL logic are ciphertext
   - Traditionally these are cleartext metadata.
   - **Supports simplified multi-protocol adaptation**
   - **Prevents the need for cleartext protocols** markers which can be **identifiers for DoS attacks**.
7. Auto-keying with Stream Ciphering
   - Incorporates specialized **stream ciphering** preventing any weak cryptographic elements or clear text sequencing.

Feature List: 3

8. Supports **efficient ciphering** for **multiple apps and platform architectures** like **Links**, **IoT devices, Streaming (e.g., MPEG), Files/Databases to Networking Protocols**.
9. Byte or Bit Mode support
   - Operates in either **byte-mode** and **bit-mode** with a cipher-block-length minimum size. Bit-mode is for MPEG/SI and IoT type applications.
10. Wide Accordion Style Tweakable Macro Blocks
    - Cipher-Block Length (cbl) – A definition of a tweakable cipher block
    - Cache-Line-Length (cll) – Tweakable **multiple** of **the cipher-block length**
      - "acll" for tweaking Authenticated Clearpass Data processing.
      - "ecll" for tweaking encrypted data and is the **unit of parallelism.**
    - Additionally, it supports tweaks specific to individual payloads.

Feature List: 4

11. Speculative Decryption
    - Supports speculative decryption in terms of both keys and payload lengths (unrelated to the spectre and meltdown model)
12. Virtual Halo Padding
    - **Stream cipher pseudo random padding** supporting **optional expansion** modes for lengths greater than 16-bytes.
13. The design introduces a novel and first of its kind design specific TCAM improvising network egress and ingress interface designs.
14. (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.

Feature List: 5

15. Integrity Key Confirmation
    - Supports Integrity Tag based **Integrity key confirmation verification.**
16. Encryption Key Confirmation
    - Supports Integrity Tag based **encryption key early indication** to reduce or eliminate decryption failures.
17. Fast Drop tags
    - Supports **multi-processing** decryption state **markers**, **egress/ingress coeval validation** and **bit-mode padding** indicators.
18. **Integrity Modes**
    - Supports two integrity calculation modes, namely**, a) contiguous block, i.e., source chunked or b) interleaved blocks, i.e., $acll$/partial "call" round-robin** supporting most peer-to-peer system online integrity designs.
    - The design allows validation of integrity at intermediary points within a relay.
    - The Integrity keys are safe to share with intermediaries and do not map directly to encryption keys.

Feature List: 6

19. Multi-Core KCM
    - Topology based parallel MAC convolved non-blocking into the final MAC.
20. 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.
21. Conclusive and Inconclusive
    - "atnaCM" is online in that integrity calculations can start as soon as data begins to arrive.
    - "atnaCM" also supports inconclusive mode where the cipher-mode can work as a true in-line system without requiring ACD or Ciphering Data segment lengths when processing starts.
22. High-Speed Inline Encryption
    - Supports encryption payload rates of 1.2 Billion pkts. /sec. corresponding to 800+Gbps links.

Feature List: 7

23. Disruption
    - This design plans to disrupt the existing fire-wall security system, load-balancing and DLP security systems be it on appliances, cloud virtual machines or containers.
    - The disruption permits migration from existing to new methods.
24. Ledger Compression
    24. One of the goals of atnaCM is to facilitate smaller digital cryptocurrency and fintech ledgers.
    25. This is in progress speculative work and hope designs incorporate this alternative design.
    26. 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
        - minimizing the size of an individual ledger entry and permitting enroute arbitration assurances within the ledger while optionally supporting or restricting mining.

Feature List: 8

25. Compatibility Model
    - Implementations **must implement** the **one mandatory hypercube model** (physically or virtually) such that the **solution** assures any **N-to-M including 1-to-1 peer-to-peer core computational compatibility**.
    - "atnaCM" supports additional Topologies.
26. Processor Bit-size agnostic
    - Specifically designed to support 64-bit, 128-bit or higher processor architectures.
    - It scales and can leverage AVX-512 systems.
    - It can be work on processor bit-sizes lower than 64-bits.
27. Cipher Block Design
    - 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, however, *"atnaCM" is cipher and cipher-block-size agnostic.*

Technical Comparative Analysis

This is documented in section 3.3 of the atnaCM Mode of Operations Abstract at https://atnacipher.com/mode-of-operations

Technical NIST Summary

This is documented in section 2.3 of the atnaCM Mode of Operations Abstract at https://atnacipher.com/mode-of-operations

Acknowledgements

- *Thank you for attending.*
- *Design Details, Questions, Concerns, Licensing? Info*
  - si@atnacipher.com

Technical References/Tools:
NIST CSRC: PQC, Block Cipher Modes, Accordion Cipher-mode
SBiR, NSF, DoD Funding, Venture Funding.
**SLOCCount is Open-Source Software/Free Software, licensed under the GNU GPL.