ATNA-CIPHER, LLC.*(ACL)*

ATNA AEAD Compliance Summary

Tushar Patel
Lead Architect/Owner

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

Introduction

- ATNA-CIPHER, LLC. is the incubation entity for its patented accordion and tweakable style encryption cipher-mode ***"atnaCM"*** introducing Coeval Authenticated Encryption *"CAE" and t*he extended system (ES) solves important challenges with current networking designs.
- The Motivating factors for this work have been
  - The need for something better and relevant in the Post Quantum Computer Era of cryptography.
  - The performance and security that can be achieved with applied CTR modes.
  - Some missing elements or attacks in SP800-38x specifications over almost two decades.
- These slides present the atnaCM high-level compliance details to the requirements of AEAD ciphers.

ATNA-CIPHER, LLC. All rights reserved©

AEAD Compliance Summary

- Fully compliant to draft-irtf-cfg-aead-compliance-properties-06.
- Confirms to Section 3. of the document.
- Confirms to Section 4.1. of this document by supporting a) immutable properties, b) mutable properties and c) Internal Operational Indicators and Configurations.(ref: “atnaCM_GV_v1 specification” and “The atnaCM Accordion Proposal Summary”)
- Next slides cover the individual properties of AEAD.
- It is an advanced CAEAD cipher adding Coeval states over AEAD.

ATNA-CIPHER, LLC. All rights reserved©

AEAD Compliance (Section 4.2)

- Confirms to section 4.2 by using built-in FIPS-CC Power-On and Continuous Tests.
- 4.2.1 Confidentiality – Obviously Yes, it works in co-ordination with approved ciphers.
- 4.2.2 Data-Integrity – Yes, it is authenticated (+ Integrity and Encryption Key confirmed)
- 4.2.3 Authenticated Encryption Security – Yes, the encryption is authenticated using a Verification Tag (i.e., FDT (Fast Drop Tag)/EFDT(Enhanced Fast Drop Tag) + MAC) hat enhances over a plain MAC) and adheres to “encrypt then MAC”.

ATNA-CIPHER, LLC. All rights reserved©

AEAD Compliance (Section 4.3)

- (4.3.1) Block-Wise Security – Yes supports cipher-blocks and tweakable macro blocks
- (4.3.2) Full Commitment – Yes, the internal operational assurance guarantees this
  - Associated data has specialized processing to assure no bit flipping, etc. in the AD data.
- (4.3.3) Key Commitment – Yes, the design assures this, though, a bungled underlying cipher could be an issue, e.g., due to polynomial factorization integer factorization.
- (4.3.4) Leakage Resistance – Yes, the issue is addressed and consists of additional parameters other than the key with separate modes. There are no cleartext parameters other than Authenticated Clear-pass Data (ACD), which, differs to traditional Authenticated Data (AD) and the important aspects are a) virtual topology-based interconnection ID(s) and b) PQC Enhancing Properties, both of which are difficult for an adversary to mimic.

ATNA-CIPHER, LLC. All rights reserved©

AEAD Compliance (Section 4.3, cont'd)

- (4.3.5) Multi-User Security – Yes, Supports a 32-bit Service ID to assure identification and specialized key-gen methods support the 4 models 1 to 1, 1 to Many, Many to one and Many to Many. Note: There will always be system limitations relating to the flow-control in such scenarios, e.g., to validate the replay counters on 1 million nodes, however, this design simplifies this management possibly better than other implementations.
- (4.3.6) Nonce-Hiding – Yes, Nonce, pkt-id (64-bit), etc., do not need to be transmitted, there is a masked header FDT (64-bit or 128-bits depending on modes) that is transmitted.
- (4.3.7) None-Misuse – Not Applicable, Nonce misuse does not apply to atnaCM.
- (4.3.8) Quantum Security – Yes, Fundamentally Quantum Q1, however, design incorporates the ability to interpose PQC elements for Q2 level, this needs further security analysis.

ATNA-CIPHER, LLC. All rights reserved©

AEAD Compliance (Section 4.3, cont'd)

- (4.3.9) Forgeability Resilience – Yes, Forgeability resistance is already incorporated.
  - There is no mandatory sequential pkt-id.
  - The design supports MAC + Per Message Encryption Confirmation
  - It is designed to be optional for specific applications that need it.
  - The estimate for forgery is 96 (unique CCK) x 2^{18} (unique id) x 2^{46} (unique integrity id) x 2^{16} (unique id extension) x 2^{32} (encryption per message confirmation * 2^{128}(logical permutation id) these scale according to the quantum windows.
- (4.3.10) Release of Unverified Plaintext – Does not apply to the atnaCM design.

ATNA-CIPHER, LLC. All rights reserved©

AEAD Compliance (Section 4.4)

- (4.4.1) Hardware Efficient – Hardware scales according to support, features and scale.
- (4.4.2) Inverse Free – Does not require the Cipher Inverse Operation
- (4.4.3) Lightweight – Lightweight implementations are supported through feature select.
- (4.4.4) Parallelizable – This is a primary supported design motivation. It support 4 level of parallelism, 1) key schedule, 2) Cipher stages (AES), 3) Tweakable Macro Block and 3) Multi-processing (this parallelism is not there or is undocumented in other ciphers.)
- (4.4.5) Setup-Free – Yes, it supports auto-keying (RFC definition is a bit vague to answer)
- (4.4.6) Single-Pass – Yes, The design is single-pass.
- (4.4.7) Static Associated Data Efficient – Yes, Supports pre-computations with additional message specific computations, however we disagree with this requirement as it forces apps or protocols to implement AD message replay attacks.
- (4.4.8) Streamable – Yes, The design is stream able and online, additionally it supports intermediate node integrity checks with or without decryption capabilities.

ATNA-CIPHER, LLC. All rights reserved©

AEAD Compliant

- Based on the attributes and presented features of the “atnaCM” cipher-mode, we claim compliance to the currently defined properties of AEAD ciphers.

ATNA-CIPHER, LLC. All rights reserved©

References

1. SP800-38A, B, C, D, E, F, G.
2. FIPS 180-1,180-2,180-3,180-4
3. IETF draft-irtf-cfg-aead-compliance-properties-06.
4. The full set of atnaCM specifications.

ATNA-CIPHER, LLC. All rights reserved©

Acknowledgements

- *First, I thank our BAPS community Gurus and Saint's for their blessings, Advisor Brian Weis, Family's trust in me to move such an effort forward, IP Legal: Mahesh Law, NIST for the Accordion opportunity and the strenuous effort in standardizing submissions and finally the Professors, Teachers, Advisors, Mentors and Colleagues for sharing their knowledge and guidance over the years.*
- *Thank you for attending.*

- *Details, Questions, Concerns? Info*
  - si@atnacipher.com

ATNA-CIPHER, LLC. All rights reserved©