ATNA-CIPHER, LLC.*(ACL)*

ATNA Cipher-Mode Business Plan 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 encryption cipher-mode ***"atnaCM".***
  - *Innovation:* Coeval Authenticated Encryption *"CAE"*

CTR mode based ✓	**Accordion** ✓	**Tweakable** ✓	**BBB Security** ✓

- The extended system (ES) solves important challenges with current networking designs.
- After a successful proof of concept (PoC), ACL is seeking funding or early licensing to expand.

Foundational Problems

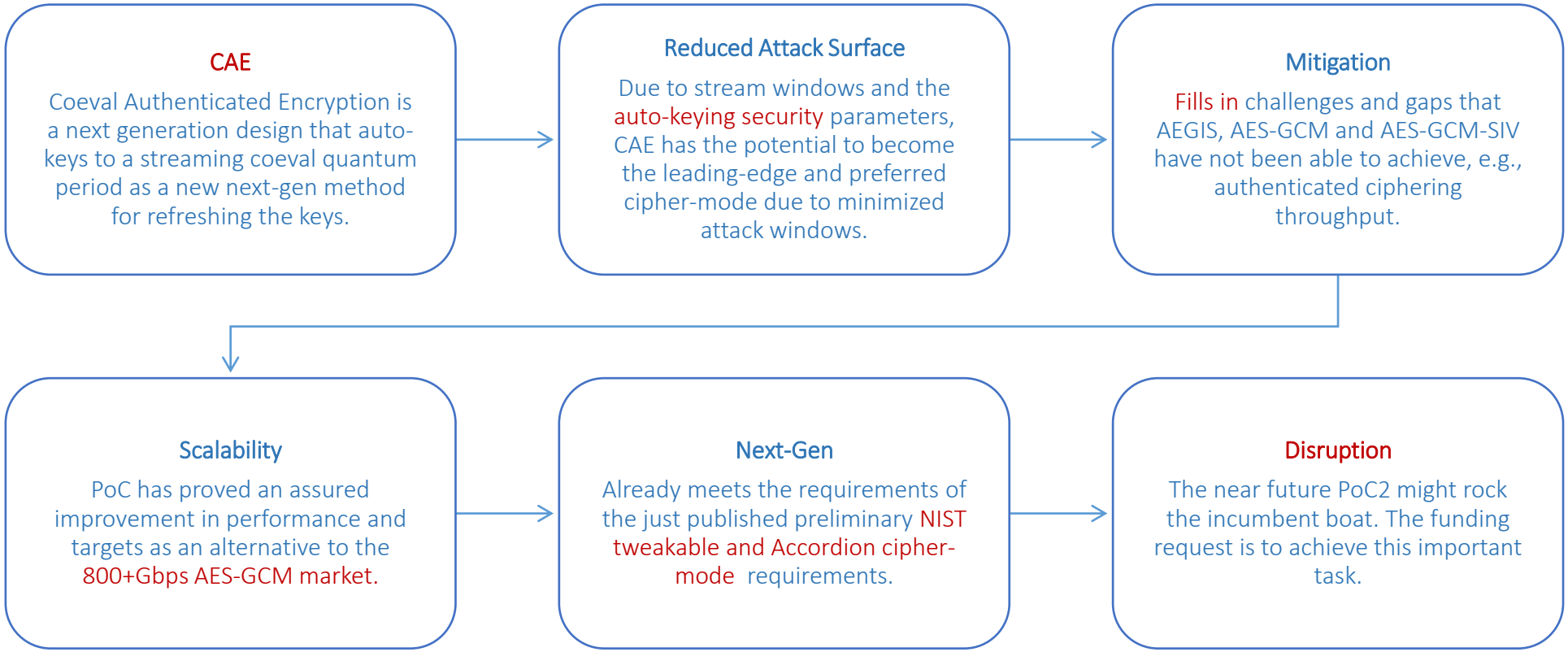
- Both NIST conferences
  - 1) The 3rd Conference on Block Ciphers and
  - 2) The Accordion Mode Conference

  have indicated a clear need for a new cipher-mode and Accordion mode cipher.
- Alongside, cipher-modes are disjoint for next-generation networking security systems.
- Experts forecast major attack vectors over the next few years due to a) Quantum Computing (QC), b) AI/ML based Security Scrutiny and c) Large Key dataset due to Crypto/FinTech.

Primary Technical Asks

- Beyond Birthday Bound Security ✓
- All or None decryption ✓
- Key Dependent Message and Key Dependent Input Security ✓
- Tweakable Cipher-Mode (block size & wide-block size) ✓
- Must deliver the Three types of encryption.
  - Authenticated Encryption with (AEAD) Encryption ✓
  - Storage Encryption ✓
  - Deterministic Authenticated Encryption✓

Paradigm Shifters



Extended System (ES)

Fast Bot Attack Anomaly and Attack Detection

Retrofits into most cryptographic networking protocols, e.g., MACSec, IPsec, TLS, SSHv2

Potential to disrupt current network packet flow and routing with new ingress/egress semantics for better security and performance.

Six Market Segments (6MS)

1. *Non-classified* Cryptographic Networking, CNSA 2.0

2. *Classified or Subject to classification systems*, e.g., Law Enforcement, Loss Prevention, FIPS-CC, DoD

3. *Financial systems*, Banking, Payments, PCI, E-Commerce, Cryptocurrency, FinTech

4. *STEM model*, Retargetable CHIPS/FW, New Models/Topologies, Optimize

5. Data Line-Rate Ultra *High-Speed Encryption at rates higher than 1.2 Billion Packets/Second or more*

6. Size Preserving *Database Encryption and File Storage*

ATNA-CIPHER, LLC. Consultancy

- We intend to offer a cipher-mode product that can/will be integrated into existing secure protocols like MACSec, TLS, IPsec/IKE v2/v3, SSH, etc.
- Addressing today's complex VXLAN, Mesh, (OF)DPA, OpenFlow & SDN networks,
  - The consultancy offers the necessary application validation
  - The migration from the existing to this potentially disruptive service
  - Eliminating performance hazards. incompatibilities and solution hazards along the way.
- Your app is your domain where this solution and relevant consultancy is non-synergic and will be a value add providing level-up leverage until full certification.

Financial Market

Global HW encryption market was 293.3 Billion in 2022

"The closest financial exit was Cryptographic Research Inc. (CRI). to Rambus. Review Crunchbase and Google for CRI exit details."

AES segment has a CAGR of 33% and is the fastest growing Encryption segment.

**We do not mimic the CRI exit directly as this solution is more refined and may supersede the CRI exit criteria.

**We hold firm and can prove that the atnaCM solution is better.

**We can and will get independent analysis completed on request.

Competition

Google – HCTR2, AES-SIV-GCM, AEGIS, other plans.

Many Large company area leads have venture funding wings to improvise similarly

NIST Lightweight Cryptography may change paradigm (ASCON now)

***Cisco** – Started **GCM**, there will be definite plans here, NIST is updating SP800-38D*

NIST Accordion cipher-mode event may bring in competition

Stealth mode startups might exist; seems curtailed currently. *Some like AEGIS exist.*

Team

Backed by a vicennium of 100% successful track record in FIPS-CC and DoD STIG certifications.

30+ year cryptography, cybersecurity and networking field background.

My personal work includes Pioneering, Leadership, Security Advising for Cryptographic Certifications.

Hands-on development for HW accelerated, SW and FW solutions in this field.

atnaCM PCT Patent:

WO [WO2023150248A1]

Advisors are well-known area leaders in ultra high-speed encryption with a very firsthand extensive career in the field.

Planned Team (for hire):

+ ~ 14 hires

(Available on request)

Risks and Challenges

HW Projects can be cumbersome and costly

Once atnaCM is fully published, others will try to copy.

128-bit AES can break in the future (due to Grover/QC), hurdled chaos may result due to adaption to new cipher/block size

Some failure, staff turnover or unexpected changes stemming from market shifts

NIST, IETF, IEEE and RFC can be slow to adapt and accept

NIST Accordion and Lightweight Cipher events may lead to competition

Intellectual Property Protection in the current SW/HW/FW environment is challenging in multiple facets.

Customer Commitment Point

- The customer commitment point is about a revenue of 27 to 30 million (today's dollars) so that customers can be assured 7 years of support.
- This should scale upwards to address new markets and requirements incrementally.
- 4 Development Phases (about 5 to 7 years for the full solution)
  - PoC (phase 0): SW (Completed, self-funded)
  - Pivot1(phase1): Primary SW (Bidding in Progress)
  - Thrust 1(phase2): Primarily HW
  - Thrust 2(phase 3): Mainline phase
  - Note: There is always the possibility of making additional arrangements to speed-up or bring-in schedules.
- We will wait for security and implementation proofs prior to any claims or assertions beyond the PoC.

Business Justification (One Aspect)

Internet is about 333EBs/month, i.e., 3996EBs/yr. with a 27% yearly growth

Assuming a 5% traffic market share, in 5 yrs. It would be 13,202 x .05 x 8 = 5280Eb

The current IPsec rate is 2.7Gbps at about $189,000 per unit

Transistor cost varies from $2.65 (7mm) to $2.16 (3mm) per billion transistors

In 5 years, it would require about 62,019 units to service traffic at a cost of $11,721,591,000

Based on PoC, ATNA is 9% faster (multiplier of 4 on average plus 10% markup) requiring 18,225 units for the same task at a cost of $3,444,525,000 (Transistor count increase may less than $100,000)

The saving in equipment for to-and-fro is **about 2 x $8,277,066,000 ~= $16B**

Early: ATNA potential is higher than this. These are estimates and very forward looking subject to Market fluctuations and development costs relating to new dies and supply chains.

Data Center cost at $1450/sq. ft. with 2 units per rack and 6ft per rack to-and-fro leads to a **5 yr. saving of about 2 x $111,338,580 = $381.007 Million**
Energy, maintenance, etc. are additional reduced saving.

Development and Finance Plan

PoC (Complete, self-funded)

- PoC (Completed, at 10% assured speedup)
- ATNA has 14 sub-specifications.
- Other legacy docs, etc.

Pivot 1 (This Request)

Office Space, SW Product, HW Work/license ready, OpenSSL Integration, MACSec, IPsec, TLS and SSHv2 work.

- Ask is for about 22 million (1 to 3 years)
- Detailed ask is available on an interest to invest after an NDA.

Thrust 1/Thrust 2 (Future)

Thrust 1: Early to commit due to dependency on Pivot1 for ASIC design, HW design specifics, etc.)

Thrust2: Based on HW traction or alternatively, HW licensing. Incorporation phase.

Important Milestones

- Achieving 10x or 20X annual burn rate to assure the business can keep its commitment.
- IP Protection services for allowing safe Security Analysis of cipher-mode.
- Staff hiring of 15 members
- RFC: MACSec, IPsec, SSH, IKEv2/3
- Ports: OpenSSL, Apple, Windows, Google and other similar ports

- Compliance
  - FIPS140-3, CC/NDcPP
  - DoD STIG, DoD in UPL
  - IEEE
  - IETF
  - ENISA
  - ISO
  - NCSC?CESG
  - UCC (UAE)

Return Offer and Potential

- You will be an important pedestal facilitator in this new science and innovation area.
- On meeting design goals, we speculate very good financial rewards and possibly cyber infrastructure unicorn status for us and your entity.
- If we reach the 10X or 20X funding goal, Your customers are assured improvisation and support resilience for the committed validity period.
- Facilitate leaping over your competitor with this advanced design and level-up your encryption profile.
- Optionally participate as a joint venture or partner with an equity stake of ACL.
- The egress system is designed with Law Enforcement in mind, should it be necessary.
- Networking design scales within the limits of existing TCAM support, e.g., Renesas 768 Gbps.
- It speculatively can support Fixed deposit Fintech and Crypto ledger designs using this cipher-mode.
- Funding Terms are Negotiable based on facilitation, e.g., providing location, benefits, services, etc.

Current Effort

- 10% encryption and decryption speedup is realized
- Pivot 1(Phase 2) PoC2 in progress assures more speedup, disruption is possible.
- Some new presentations in prep for the NIST Accordion Mode Submissions
  - Details available by request from si@atnacipher.com after NDA.
- Current Specifications, PoC, Code and Proofs. (1 Lead Architect, 1 Advisor, IP Legal)

NIST Cipher-Mode Compliance Summary

This is documented in section 2.3 of the atnaCM Mode of Operations Abstract at

https://atnacipher.com/mode-of-operations

“atnaCM” Technical Comparative Analysis

This is documented in section 3.3 of the atnaCM Mode of Operations Abstract at

https://atnacipher.com/mode-of-operations

Recent Updates

- Design reviews are complete as a strong contender in the 1.2 Billion packets/second Ultra High-Speed encryption market, generally, MACSec and IPsec.
  - While restricting protocol indication data bloats to allow maximum efficiency.
- Meets the NIST preliminary accordion mode requirements.
- Adding support allowing IoT and smaller devices to be cryptographic pre-processing free.
- Adding assurance for compliance with existing cipher modes. **This assurance permits to start developing prior to cipher-mode approval.
- Presented at the the NIST Accordion Mode Conference.

Final Summary

Technical Rationale:

1. *Invent the highest or on par cipher-mode*
2. *Implement a CTR based Accordion mode*
3. *Use proven techniques for innovation to product transition*
4. *Deliver Performance Results and HW/SW/FW IP Modules*
5. *Stability of dense chip transistor counts at rates higher than 1.2 Billion Pkts./Second*

ACL
ATNA-CIPHER, LLC.
COEVAL AUTHENTICATED ENCRYPTION

Pre-Work (Phase 0)	**Cost Summary**	Pivot 1 (Phase 1)	Thrust 1 (Phase 2)	Thrust 2 (Phase 3)
Business Valuation: ~750K with $295K Asset Build up	Proposed	$,~22 Million	Available: End of Pivot 1	Available: End of Thrust 1

1. *No fundamental Research*
2. *New Science Area*
3. *Incorporates a patented PCT WO2023150248A1*
4. *No foreign Entities*
5. *Patented for IP Defensive protection*
6. *Nothing other than financing.*
7. *No Human Subject Research*
8. *Valuation available on request*

Acknowledgements

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

ATNA-CIPHER, LLC.
COEVAL AUTHENTICATED ENCRYPTION

Market References

1. *Publicly on Google*

Technical References/Tools:
NIST CSRC: PQC, Block Cipher Modes, Accordion Cipher-mode
SBiR, NSF, DoD Funding, Venture Funding.