The ATNA Cipher-Mode (atnaCM)

Plan Summary / Pitch Deck

ATNA-CIPHER, LLC.
(408)242-5016
si@atnacipher.com
P/O. Box 2130, Sunnyvale, CA 94087-0130

Introduction

ATNA-CIPHER, LLC. is the incubation entity for its next-generation encryption cipher-mode *"atnaCM"*

(Authenticating, Threading, Normalizing-IV and Auto-Keying) – Four important predicates for Quantum Computing/Cryptography.

Coeval Authenticated Encryption *"CAE", a speculative science for cryptography*

Over 64 features in a single cipher-mode, unconventional, disruptive, without overcomplexity

Extended System (ES) – A vetted innovative approach in next-gen Cybersecurity, Networking & Cryptography amalgamation

Patented with important business goals in mind

Cryptographic Timeline

Pre 2005
Legacy

DSA,
DHE,...
TDEA,
3DES
RNG
FIPS 140-1

Carry
Forward:
AES,
RSA,
ECDSA,

Identification period of the need for new technologies

2005
*Carry
Forward:*

*AES, GCM,
CTR, CBC,
...*

*RSA,
ECDSA,
EdDSA*

FIPS 140-2

2010
*Carry
Forward:*

*AES, GCM,
CTR, CBC, ...
DRBG*

*RSA,
ECDSA,
EdDSA*

*FIPS 140-2
FIPS 140-3*

2015
Fintech

*Carry
Forward:*
ECC
K-Curves, B-
Curves, ...

Ledgers

No
Certification

2022/2023 /2024

*Carry Forward:
Accordion
(specification),
Lightweight,
Post Quantum
Cryptography (PQC)*

2022-2028,...
atnaCM Development, SW, HW, FW, & ES,
Productization Goal (incrementally 2025 onwards)

2031??
QC
(Speculation)

Purpose

- Summarized across NSA Type 1 & NIST conferences and Initiatives
  - 1) Forward looking and Speculatively though generally falls in place.
  - 2) NSA Type, CNSA 2.0, CSfC   (Testing costs are high)
  - 3)NIST (Affordable and relatively comprehensive)
    - The 3rd Conference on Block Ciphers and
    - The Accordion Mode Conference
  - 4) Quantum Computing and Post Quantum Cryptography (Extreme testing costs, beyond gold)

- Inhibition (functional, performance & scale) to networking and cybersecurity.

- Experts forecast major attack vectors over the next few years due to a) AI/ML identified vulnerabilities b) Large Fintech Key datasets(financial) c) Quantum Computing (QC) (Catastrophic) and d) Networking Consolidation

- A clear indication for the need a new cipher-mode be it Accordion or other.

Technical Asks/ Feature Check

- **Quantum Ready and Resilient** ✓
  - (Uncrackable after Quantum primetime)
- **Beyond Birthday Bound Security** ✓
  - (Padding, Bit-flipping,…, no re-regressions)
- **All or None decryption** ✓
  - (Compromise : none is winning, opportunism is risk/loss)
- **Key Dependent Message and Key Dependent Input Security** ✓
  - (Speed-up the speed-up, failure reduction goes a long way)
- **Tweakable Cipher-Mode** (block size & wide-block size) ✓
  - (Ciphering Lego blocks)
- **Facilitation of all three encryption modes** ✓
  - (Use a versatile tool, lightweight for toolkit, speculatively: jedi-mode light-saber)
  1. Authenticated Encryption (AEAD) ✓   2. Storage Encryption ✓   3. Deterministic Authenticated Encryption ✓
- **Unique Cryptographic features** (not present in any other published solution.) ✓

Associative Asks/Feature Check

- **Better Network Integration** ✓
  - Who likes non-treasure currency coins
- **Bot Detection Improve and Prevent** ✓
  - Current Whac-a-Croc approach cannot sustain
- **Advanced Cybersecurity** ✓
  - Slight of the hand, know what transpires
- **Better Advanced HW Capabilities** ✓
  - Industry is held back, change track, and overtake
  - Moving beyond AES-NI
  - Per-Packet Multi-processing
- **Allocated Cryptography as a Service (ACaaS)** ✓
  - No irrelevant stipends (Data Center HW costs averaged across all customer pricing.)

Core Market Segments

2026 YoY estimates

ACL
ATNA-CIPHER, LLC.®
COEVAL AUTHENTICATED ENCRYPTION

1. *Non-classified :* Cryptographic Networking, CNSA 2.0 **Market about 22B+**

2. *Classified or Subject to classification systems*, e.g., Law Enforcement, Loss Prevention, FIPS-CC, DoD **~$29 B+**

3. *Financial systems*, Banking, Payments, PCI, E-Commerce, Cryptocurrency, FinTech **~22B+**

5. Data Line-Rate Ultra *High-Speed Encryption at rates higher than 1.2 B+ Pkts/Second or more* **~17B+**

4. *STEAM* Tech./High. Ed. (Cryptography, Net., Topology), CHIPS/FW/SW/HW. (Future, invaluable, not free though)

6. Size Preserving *Database Encryption and File Storage* **~500M+**

7. Undisclosed market (no direct players) **~16B+**

Team

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

30+ year cryptography, cybersecurity and networking field.

Advisors and Leaders are well-known area leaders in ultra high-speed encryption with an extensive firsthand field career.

Roles include Advising, Pioneering, Leadership.

Hands-on HW accelerated, SW and FW solutions.

Led dev teams to scale up to yearly >1B products.

Multiple cryptography patents, atnaCM is patented.

Planned Team (for hire):

Model 1: No team Model 2: About 20 hires

Will not hire additional members unless funding is secured (Budget and Hires available on request)

Funding Purpose

- Complete the next phase development to reach certification level.
- Complete FIPS CAVP certification and compliance.
- Additional Patenting (new methods, systems and apparatus)
- Filing the additional solution patents.
- Productize and Commercialize the SW.
- Productize and Commercialize the HW.
- Commercialize the extended systems
  - Cybersecurity, Networking & QC.
- Exit Criteria

Funding Models

- Model 1
  - Licensing, Certification or Purchase Consulting – YoY payment (unstaffed)
- Model 2
  - Full commitment (3 years, USD$) – Licensing, Certification and Products
- Model 3
  - Combinatory hybrid models with above combination.
  - Bringing schedule in under 3 years is possible
    - Renegotiating Costs and Timelines
    - Involves higher risks

Risks, Challenges & Competition

HW Projects can be cumbersome and costly

Once published, others will copy atnaCM.

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

PQC based delays

New NIST Accordion development

NIST has started 256-256 Rijndael, updated SP80038D (GCM)

Large area leading companies have venture funding wings to improvise similarly

Stealth mode startups exist; seems curtailed currently

Intellectual Property Protection in the current SW/HW/FW environment

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

***Cisco** – Started **GCM**, will have definite plans here*

Business Justification
(e.g., Data Center)

Internet is about 333EBs. per 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 estimates are forward looking subject to Market fluctuations, development & supply chain costs.

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.

Plan Summary

PoC (Complete, self-funded)

- **PoC (Completed,** at 10% assured speedup)
- Project has over 10 sub-specifications.
- Other legacy docs, etc.
- New product sloccount estimate is about 7M+

Pivot 1 (This Request)

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

- Ask is for about 28 million (3 years: 6-month release)
- Detailed ask is available on an interest to invest after an NDA.
- Early valuation ~8.2M
- EBITD ~1M (Accounting Value)

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.

Does not cover taper costs.

Return Offer and Potential

- Achieving goals; ACL speculates very good financial rewards and unicorn status for the joint entity.
- When we reach the 10X or 20X goal, customers are assured improvisation and support resilience.
- Can level up your encryption and cybersecurity profile to reach your competition.
- Optionally participate as a joint venture or partner with an equity stake of ACL.
- The egress system is designed with Law Enforcement in mind.
- Networking design scales within the limits of existing TCAM support, e.g., Renesas 768 Gbps.
- "atnaCM" speculatively facilitates efficient fixed deposit fintech and Crypto ledger designs.
- Funding Terms are Negotiable based on facilitation, e.g., providing location, benefits, services, etc.
- Above and Beyond – A design with over 64 unique features (unconventional in a single cipher-mode, allows entering multiple markets with a single mode.)
- Matured, optimized and well-vetted solutions.

Recent Updates

- The bridge from legacy to Quantum Computing is in progress.

- A new 16B+ YoY market was identified, not yet disclosed externally.

- Design reviews are complete as a strong contender in the 1.2 B+ pkts./sec. Ultra High-Speed encryption market, generally, MACSec and IPsec.
  - While restricting protocol indication data bloats to allow maximum efficiency.

- Is beyond the NIST preliminary accordion mode (VIL-SPRP) 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.

- Some guiding elements presented at the NIST Accordion Mode Conference

Final Summary

Technical Rationale:

1. *Invent the highest or on par cipher-mode*
2. *Implement a CTR based Accordion (VIL-SPRP) 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*

1. *No fundamental Research*
2. *New Science Area*
3. *No foreign Entities*
4. *Patented for IP Protection*
5. *Nothing other than financing.*
6. *No Human Subject Research*
7. *Valuation available on request*

Pre-Work (Phase 0)	Cost Summary	Pivot 1 (Phase 1)	Thrust 1 (Phase 2)	Thrust 2 (Phase 3)
Valuation: $1M (EBITDA, 2024)	Cost $750K	$~28 M USD	Available: End of Pivot 1	Available: End of Thrust 1
Valuation : **$8.2M LLC (2025), GUST Estimate**				

Acknowledgements

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

Tushar Patel

Tushar Patel (for Atna-Cipher, LLC.)

Founder/Lead-Architect
Market References: All Public on Google

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