

ATNA-CIPHER, LLC.(ACL)
*Accordion Cipher-mode
Preferable Features*



ATNA-CIPHER, LLC.
COEVAL AUTHENTICATED ENCRYPTION

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. (aka ACL) is the incubation entity for the development of an accordion and tweakable style encryption cipher(+/-mode.)
- As NIST is not seeking a full proposal submission at this time; ACL would like to highlight some key features as recommendations for an Accordion Mode.
 1. **Enciphering Properties** like Key Sizes, Block Cipher Sizes and Tweakable Block sizes
 2. **Confirmation** of keys like encryption, integrity, etc.
 3. **Parallelism** relating to large input sizes
 4. **Fast Drop Tags** for Authenticated Encryption
 5. **Padding Attacks Prevention** for all tweaks and enciphering properties
- Subsequent slides present each ones of these topics in some light detail.
- Note: In the slides, messages like payloads/packets are 1-unit of encryption from a possible larger set.

Enciphering Properties

- **Cryptography is consistently changing; however, future adaptability has been difficult,**
 - e.g., PQC finalization, Legacy RSA deprecation or Next-gen Cryptographic Adaptation of ECDHE ECDSA,
- Currently, Cipher Blocks are 128-bits or most probably its multiples, AES-128 or Rijndael-256 (i.e., 2*128-bit.)
- Cipher Key Sizes and generally multiples of 16-bytes, 24-bytes or 32-bytes, i.e., AES-(128/192/256).
- Recommended hash sizes as per CNSA 2.0 are (SHA-384) 48-bytes or (SHA-512) 64-bytes or SHA-3 Hashes are 128-bit multiples.
- Disk or Container Block Sizes are in Powers of Two, i.e., 2^n where, $n \in \{9,10, \dots, (n-1), n\}$ (*multiples of 128-bits*)
 - (*note: blocks can be smaller than 512 in smaller systems*)
- Due to interoperability between HW registers and Encryption units,
 - Architectures define Blocks in multiples or Cipher Block Sizes (i.e., 128-bits), e.g., AES-NI/ARM: AES-128, AES-256, AES-512, etc.
- Most implementations are stuck at 4096 cipher blocks, (e.g., TLS, Missing Jumbo in MACSec)
- Given these factors, it would be highly preferable to,
 - Define Accordion Cipher-Blocks, Hashes and Keys as multiples of 128-bits. (90% cases)
 - For other sizes, padding rules must be defined and security validated/assured. (10% cases)
 - Update number of cipher blocks to 16384 (i.e., 2^{14}) from 4096 (i.e., 2^{12}), with Rijndael-256, it has the necessary future proof support.
- This seems an acceptable RISC style approach to keep Accordion HW efficient and within HW design bounds.

Confirmations

- The penalties of missing failing a decryption in a pipeline (e.g., HW) are
 - Costly in proportion to speed.
 - Most HW complete ops. in two passes. (HW packet recirculation is common.)
 - Using Key Confirmations prevent such penalties
- All the message operational keys should be confirmed, e.g., Both Integrity and Enciphering Keys, however, some applications may keep them optional.
 - Persistent or resident encryption like disk and storage may not need this.
- Implementations can include other confirmations like enciphering or domain parameters for better application related security assurances.
- This will be a highly preferable feature for the Accordion mode, missing in many modes.

Parallelism

- Current architectures support **three** levels of Parallelism.
 - **Key Schedule Parallelism** (like AES key schedules)
 - **Encryption Stage Parallelism** like the 14 stages of AES (128-bit block, 256-bit keys)
 - **Tweakable Block** (like AES-NI encryption in multiples of 128-bit)
- There are **two** stages that are possible, yet, missing in most of today's designs.
 - **Per Message Parallelism**
 - For large packets, implementations can support multi-processing across multiple AES units.
 - **Integrity or MAC parallelism**
 - Most implementations miss multi-processing MACs or integrity checks.
- It is recommended that Accordion Modes support at least **5-levels of parallelism.**

Fast Drop Tagging

- Fast drop tags permit message parallel cross-compatibility and confirmations (e.g., keys.)
- Many current modes push items like Flow Control and Attack Prevention to the upper layers.
 - These layers may allow DoS attacks if not using AEAD ciphers over upper-layer headers,
 1. Online – DoS as packets can get queued in the stack until flow control processing.
 2. No upper bound – An attacker can DoS replay in leaps shortening the window.
- In compromised and mirrored hypervisors, VMs and containers, it may be possible to mirror ciphertext based on protocol knowledge, e.g., SPI, RTSP headers to a compromised unit with an upper layer side-channel in JavaScript, e.g., attacks on multicast groups.
 - While subject to bad implementations, such attacks have been known to occur in the past.
 - Not all systems can incur the costs of Enclaves, TPMs and HSMs.
- Fast Drop Tags implementing bounds on flow control and providing service segmentation adaptation and assembly in ciphers can thwart or prevent such attacks.
- It would be highly preferable for Accordion designs to include this functionality.

Prevention of Padding Attacks

- The previous list of modes had failures with the first-two blocks (CTR/CBC) leading to
 - The introduction of authenticated encryption like AES-GCM.
 - Repetition Padding Attacks due to Chosen Plaintext and Chosen Ciphertexts + padding.
- Padding and enciphering must support, both bits and byte modes.
 - Bit-Mode is for IoT and other stream applications like MPEG bit-fields.
 - Variable Bit-padded cipher blocks are more difficult to crack than Byte-padded cipher blocks.
 - Currently less than 96-bits can be brute-forced. This applies to certain fields securely encrypted, however, the field itself can be brute-forced or rainbow tabled.
- Use different padding bits for Integrity Calculations and Enciphering Padding Schemes.
 - Supports integrity checking at intermediate nodes in transport without decryption.
- It should be a must for submission to provide alongside submissions to include
 - Theoretical Proofs of IND CCA1, CCA2 and IND-CPA, IND-CPA2
 - Formalized testing of the same and provided under a NEW FIPS ACTS (i.e., CAVP test)
- This is already a required property of an Accordion mode.

Accordion Compliance

Section 3

- Mode parameters must permit selectable parameters to comply with the 3 Section 3 types.
 - **ACL choses to postpone the full discussion to the finalization of the Accordion mode**, however, complies as discussed in the next few slides.
 - Approaches of Accordion Mode should support
 - **Segmentation** – Property to allow or prevent access to sub-segments of ciphertext.
 - Such support should **allow random-access to ciphertext sub-segments**.
 - As kernel sk-buffs (Linux), mbufs (BSD) only **allow a tail increment of (36/40)-bytes**.
 - Current Verification Tags or MAC(s) must be within this limit to prevent performance loss due to fragmenting an sk-buff in two.
 - Also simplifies message exchange across the OS kernel to user space interfaces.
 - Should **support extendibility and adaptability** methods due to diverse application needs.
 - Should facilitate backdoor free, **data search in the encrypted form** and **law enforcement**.

References

1. SP800-38A, B, C, D, E, F, G.
2. NIST SP800-90Ar1, NIST SP800-90B, NIST PQC through Round 5, NIST SP800-131Ar2
3. Proposal of Requirements for an Accordion Mode – NIST, April 2024
4. FIPS 180-1,180-2,180-3,180-4, FIPS 198-1, SP800-108. other FIPS and Common Criteria Specifications.
5. Thomas Leighton – Morgan Kaufmann Publishers, Parallel Algorithm Architectures, 1992.
6. Dr. Donald Knuth – Addison Wesley Publishers, The Art of Computer Programming, Vol. 1 through 4B.
7. William Stallings – Cryptography and Networking Security
8. The Crossed Cube Architecture for Parallel Computation – Kemal Efe, Transactions on Parallel and Distributed Systems, Vol. 3, 0.5, Sept. 1992.
9. GCM Multiple: a) The Galois/Counter Mode of Operation (GCM), D. McGrew, J Viega, b) Development of the Advanced Encryption Standard Aug 16, 2001, c) Authentication Weakness in AES-GCM, Neil Ferguson, 2005, d) Authentication Failures in NIST version of GCM, Antoine Joux
10. Misc.: a) On the Construction of Variable-Input-Length Ciphers, M. Bellare, P. Rogaway, b) Padding Oracle Attacks on CBC-mode Encryption with Secret and Random IVs, c) A Tweakable Encryption Mode, S. Halevi and P. Rogaway, d) There are many other cryptanalysis papers and websites.
11. Related: a) Bit Twiddling Hacks, Sean Eron Anderson, Stanford., b) Digital Design – Nicholas L. Pappas. C) Arithmetic Tutorial Collection, Douglas W. Jones – University of IOWA – 2001 d) Operating Systems Concepts – 10th Edition, Silberschatz, Galvin, Gagne – Wiley 2018.
12. PQC impact:
 1. Shor's Algorithm: <https://www.nccoe.nist.gov/sites/default/files/2023-12/pqc-migration-nist-sp-1800-38b-preliminary-draft.pdf>
 2. Grover's Algorithm : <https://csrc.nist.gov/csrc/media/Events/2024/fifth-pqc-standardization-conference/documents/papers/on-practical-cost-of-grover.pdf>
13. There are many other documents over the years and hence, a full list is not possible to reproduce here.

Acknowledgements

- ACL hopes this presentation helps towards the final requirements of the Accordion Mode.
- *Thank you for attending.*
- *Details, Questions, Concerns? Info*
 - si@atnacipher.com

