National Cyber Security Centre

Requirements for an Accordion Mode

Guy B

UK NCSC

June 2024

Introduction

NCSC is the UK National Technical Authority on cryptography

Our research focuses on high-threat use-cases:

- Data requiring long-term security
- Low tolerance of risk to transmission and storage of data

Very supportive of NIST initiative to standardise new modes [5]

Recently published our own relevant designs [4]:
“GLEVIAN and VIGORNIAN: Robust beyond-birthday AEAD modes”

National Cyber Security Centre

Our requirements

Our high-priority requirements

A mode for AEAD (essential), and DAE (desirable)

“Secure by design” philosophy
- Security should not depend on end-users being experts in cryptography

Prioritise confidence over efficiency
- Robustness over performance
- Simplicity of security analysis

Interoperability requirement
- Compatibility with AES is essential

Secure at high data volumes across a deployment

We expect our design goals to be relevant to the wider community, although the priorities will differ

High priority requirement: Robustness over optimality

Nonce misuse resistance (MRAE)

RUP security
- See our other talk

Usable security results:
- Birthday security with AES likely insufficient for our use cases
- Proofs should yield costings we can use
- See our other talk

Avoid complexity where possible
- A simple algorithm is more likely to match what is actually implemented
- A simple security analysis is less likely to contain mistakes

These are essential requirements for our use cases

Medium Priority: Would like to have

- Black-box reductions in the standard model
  - For post quantum security
  - Caution is necessary applying ideal cipher model to AES

- Performance

- Key/context commitment

We would like as many of these as possible, but accept achieving all of them together may be impossible

Low Priority: Nice to have, but not essential

- Nonce hiding
- Leakage resilience
- Security when encrypting key dependent data

While these are still goals we would like to attain, it should not be at the cost of our higher priority goals

National Cyber Security Centre

Complications and trade-offs

Birthday security and AES compatibility

	AES-compatible	Wider primitive
Birthday Accordion	Insufficient security bounds for large-scale deployments	Future value
Beyond-Birthday Accordion	Current Requirement	Excessive complexity / overhead

AES in a birthday-security mode provides insufficient security for large deployments

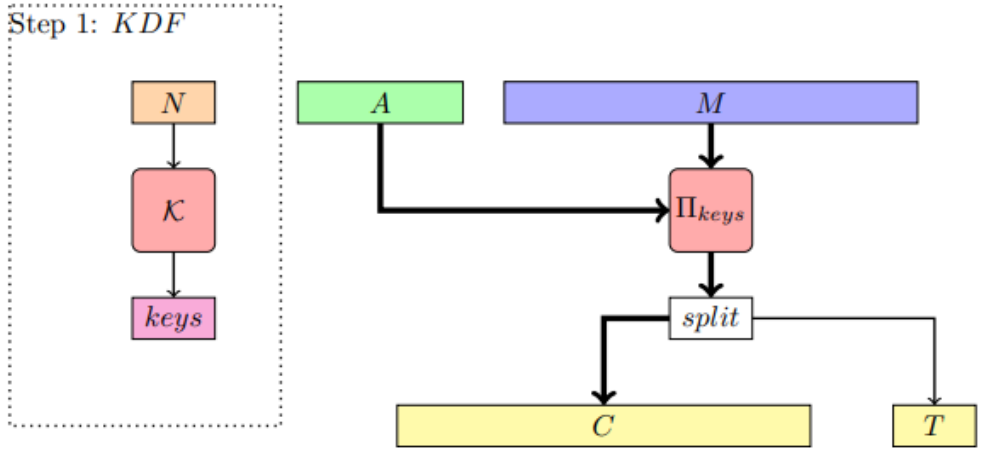
- See other talk for full justification

A possible approach might be to build a mode of a wider primitive

- Cleaner security analysis
- Does not meet our high priority requirement for AES compatibility

One option to overcome birthday bounds: nonce-based key derivation [7]

Summary
- Derive a key for each nonce, for use in an existing algorithm
- Upgrades birthday-bound security to beyond-birthday



Advantages:
- Strong security bounds
- Feasible security analysis

Disadvantages:
- Performance:
  - Poor short message performance
  - Requires many rederivations of block cipher key schedule
- No guarantee of beyond-birthday security when nonces are misused or unverified plaintext is released
- Limitation: nonce reuse cannot be prevented with decrypt queries

MRAE necessitates two-pass schemes

Security notion MRAE [10]:

- Requires AEAD schemes to be indistinguishable from ideal even when nonces are repeated

NCSC regards MRAE security as essential

Drawbacks:

- MRAE security is impossible to meet without at least two passes over the input [8]
- Care needs to be taken with the interaction between MRAE, RUP and birthday bounds

Ideal cipher model, post-quantum security, AES compatibility

Applying the ideal cipher model to AES can be difficult to justify

- e.g. AES admits related-key attacks [e.g. 1]

Security proofs are our preferred route to justify post-quantum security

- For ideal cipher model proofs, this entails moving to the Quantum Random Oracle Model (QROM) [3]
- Translating ideal cipher model proofs to the QROM introduces significant complexity
- By contrast, most AEAD security reductions in the standard model naturally justify post-quantum security

Context commitment

This is the idea that a ciphertext and tag should effectively be a commitment to the “context” (i.e. the key, nonce, associated data, and message) that produced them

This seems desirable in principle

What is the impact?

- Vulnerabilities have been found that arise from a lack of context commitment [e.g. 6,8]
- However, all examples so far have been in fairly limited scenarios:
  - one of the parties holding the symmetric key is corrupted; or
  - the key has low entropy
- This is a relatively new research area, so more significant examples may be found in future

Context commitment concerns

Proof Model

- Security games for context commitment proofs cannot involve a secret key
- This rules out the standard model for these proofs
- As a result, security proofs for context committing modes are typically given in the ideal cipher model

Additional Expansion

- For a context committing scheme with n-bit tags, a generic attack suggests that an attacker can produce repeated tags after approximately $n/2$ bits of work
- So, immediate methods for context commitment often require increased ciphertext expansion
- Techniques to mitigate this are being invented, but they are currently complex and novel [2]

We feel the area is too new to be more than medium priority at this stage

One set of trade-offs: VIGORNIAN

In designing GLEVIAN and VIGORNIAN [4], we attempted to make trade-offs suitable for our use-cases

They use nonce-based key derivation and the encode-then-encipher construction with an underlying VIL-SPRP

We prioritised:
- Beyond-birthday security (when not misused)
- Robustness to nonce misuse and RUP
- AES compatibility and a security result in the standard model
- A simple design and security analysis

We traded off:
- Short message performance
- Context commitment
- Leakage resilience, nonce hiding

Remarks and Discussion Points

NIST's proposal to provide AEAD via Encode-then-Encipher offers strong security and robustness properties

There are many security goals, and it likely will not be possible to achieve them all with a single scheme

We believe our use-cases may be shared, and we offer our designs and research in the hope they will be of use to others

Summary

We require:

- Two Derived Functions: AEAD (essential), DAE (desirable, for keywrap)
- An Accordion from AES
- High confidence and “Secure by design”
  - Robustness over performance
  - Simplicity of security analysis
- Security greater than that of 128-bit birthday bound

We expect other users will have different requirements

The range of security goals being discussed in this community suggest that standardising more than one Accordion mode may be helpful

We hope our ePrint and submissions support NIST’s effort, and we welcome the opportunity to discuss these topics further

Bibliography

[1] A. Biryukov, D. Khovratovich, and I. Nikolic. Distinguisher and related-key attack on the full AES-256. In S. Halevi, editor, CRYPTO 2009, volume 5677 of LNCS, pages 231–249. Springer, Heidelberg, Aug. 2009.
[2] M. Bellare and V. T. Hoang. Succinctly-committing authenticated encryption. Springer-Verlag, 2024.
[3] D. Boneh, Ö. Dagdelen, M. Fischlin, A. Lehmann, C. Schaffner, and M. Zhandry. Random oracles in a quantum world. In D. H. Lee and X. Wang, editors, ASIACRYPT 2011, volume 7073 of LNCS, pages 41–69. Springer, Heidelberg, Dec. 2011.
[4] P. Campbell. GLEVIAN and VIGORNIAN: Robust beyond-birthday AEAD modes. Cryptology ePrint Archive, Report 2023/1379, 2023. https://eprint.iacr.org/2023/1379.
[5] Y. L. Chen, M. Davidson, M. Dworkin, J. Kang, J. Kelsey, Y. Sasaki, M. S. Turan, D. Chang, N. Mouha, and A. Thompson. Proposal of requirements for an accordion mode, 2024.
[6] Y. Dodis, P. Grubbs, T. Ristenpart, and J. Woodage. Fast message franking: From invisible salamanders to encryptment. In H. Shacham and A. Boldyreva, editors, CRYPTO 2018, Part I, volume 10991 of LNCS, pages 155–186. Springer, Heidelberg, Aug. 2018.
[7] S. Gueron, A. Langley, and Y. Lindell. AES-GCM-SIV: Specification and analysis. Cryptology ePrint Archive, Report 2017/168, 2017. https://eprint.iacr.org/2017/168.
[8] J. Len, P. Grubbs, and T. Ristenpart. Partitioning oracle attacks. In M. Bailey and R. Greenstadt, editors, USENIX Security 2021, pages 195–212. USENIX Association, Aug. 2021.
[9] K. Minematsu. Fast decryption: a new feature of misuse-resistant AE. IACR Trans. Symm. Cryptol., 2020(3):87–118, 2020.
[10] P. Rogaway and T. Shrimpton. A provable-security treatment of the key-wrap problem. In S. Vaudenay, editor, EUROCRYPT 2006, volume 4004 of LNCS, pages 373–390. Springer, Heidelberg, May / June 2006.

With thanks to the Cryptobib effort for references