RFC 10032 : The AEGIS Family of Authenticated Encryption Algorithms

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 19 septembre 2026

Date de publication du RFC : Septembre 2026

https://www.bortzmeyer.org/10032.html

L'imagination des cryptologues est sans fin, voici une nouvelle famille d'algorithmes de chiffrement, fondés sur le classique AES, la famille AEGIS (qui, au moment d'écrire cet article, n'a pas encore de page Wikipédia). AEGIS permet de réutiliser le jeu d'instructions AES mais est plus rapide qu'AES et fournit du chiffrement intègre.

AEGIS <https://competitions.cr.yp.to/round3/aegisv11.pdf> est issu du concours CAESAR. Il existe en plusieurs versions, AEGIS-128, AEGIS-128L, AEGIS-128X, AEGIS-256 et AEGIS-256X (ils sont désormais dans le registre IANA <https://www.iana.org/assignments/aead-parameters/aead-parameters.xml#aead-parameters-2> des algorithmes de chiffrement intègre). Comme leurs noms l'indiquent, ces algorithmes diffèrent par la taille des clés utilisées mais tous utilisent les fonctions de base d'AES (norme NIST.FIPS.197-upd1 <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197-upd1.pdf>), ce qui leur permet d'utiliser les mises en œuvre matérielles d'AES. AEGIS peut être vu comme de l'AES plus rapide.

En outre, AEGIS est normalement plus sûr qu'AES en mode GCM (les autres modes d'AES n'offrent pas de chiffrement intègre et ne sont donc pas vraiment comparables). Avec AES-GCM, on peut trouver des textes chiffrés qui se déchiffrent correctement avec plusieurs clés, ce qui facilite certaines attaques (cf. ≪ *"Partitioning Oracle Attacks"* <https://www.usenix.org/conference/usenixsecurity21/presentation/len>). Ce n'est pas possible avec AEGIS. D'autre part, la clé utilisée ne sert qu'au tout début, le chiffrement ou déchiffrement sera fait après une dérivation, on pourra donc effacer la clé de la mémoire rapidement, diminuant les risques qu'un méchant ne la copie.

Si vous voulez en savoir plus, ne comptez pas sur mes faibles connaissances en cryptographie, lisez les sections 2 à 8 du RFC, qui expliquent les algorithmes de la famille AEGIS, avec pseudo-code. Puis, pour approfondir, ≪ *"Analyzing the Linear Keystream Biases in AEGIS"* <https://doi.org/10.13154/tosc.v2019.i4.348-368> ≫, ≪ *"Guess-and-Determine Attacks on AEGIS"* <https://doi.org/10.

1093/comjnl/bxab059> », « *"Weak Keys in Reduced AEGIS and Tiaoxin"* <https://doi.org/10.46586/tosc.v2021.i2.104-139> » ou « *"MILP-based security evaluation for AEGIS/Tiaoxin-346/Rocca"* <https://doi.org/10.1049/ise2.12109> ».

AEGIS est aujourd'hui mis en œuvre dans plusieurs bibliothèques logicielles <https://github.com/cfrg/draft-irtf-cfrg-aegis-aead/blob/main/README.md>, dans de très nombreux langages de programmation. Si vous voulez contribuer à ces codes, ou bien en créer un nouveau, n'oubliez pas de tester avec les vecteurs de test de l'annexe A (également disponibles en ligne <https://github.com/cfrg/draft-irtf-cfrg-aegis-aead/tree/d3ef99846e957f5533cef51b4d15a5d55af086
test-vectors>).

Les fans de cryptologie liront avec plaisir la section 9 qui analyse les problèmes de sécurité potentiels d'AEGIS. J'ai noté que cette section estime qu'AEGIS est résistant aux calculateurs quantiques, en tout cas s'il n'y a pas de lien quantique avec le système qui fait tourner AEGIS (ce qu'on appelle traditionnellement le « modèle Q1 d'attaquant », le modèle Q2 étant un attaquant complètement quantique).