ENSTA Bretagne
2, rue François Verny
29806 BREST cedex
FRANCE
Tel +33 (0)2 98 34 88 00
www.ensta-bretagne.fr

UV4.8

promo 2017

30 avril 2016

AES-GCM

RIGAUD MICHAËL et BADIER CHARLIE

Table des matières

Introduction

GCM ou Galois Counter Mode est un mode d'opération de chiffrement par bloc en cryptographie symétrique. C'est un algorithme de chiffrement authentifié qui garanti l'intégrité et l'authenticité des données. Lors des opérations que nous verrons plus loin, cet algorithme demande de chiffrer avec un autre algorithme de chiffrement. D'après la norme IEEE 802.1AE, on utilise l'algorithme AES (Advanced Encryption Standard). On appelle donc cet algorithme AES-GCM .

Dans ce rapport, nous expliquerons dans un premier temps le fonctionnement de AES-GCM ainsi que de ses autres modes. Puis nous le comparerons à d'autres algorithmes semblable en termes de complexité. Enfin nous essayerons de voir quels sont les principaux vecteur d'attaques de cet algorithme dans les applications usuelles.

CHAPITRE 1

Fonctionnement

L'algorithme AES-GCM possède deux modes, le premier est le mode courant GCM et le second est le GMAC.

1.1 GCM

Avantanges de GCM

AES-GCM est un algorithme qui assure un haut niveau de sécurité grâce à AES, mais surtout il assure authenticité et l'intégrité des données. C'est à dire que si Alice essaye de communiquer avec Bob, elle est assuré que Charlie ne pourra pas lire ses données mais également qu'il ne pourra pas les modifier sans que Bob sans aperçoive.

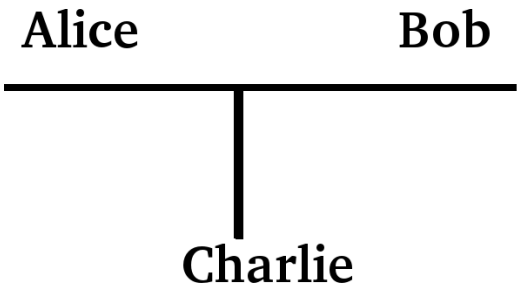

FIGURE 1.1: Bob et Alice

De plus, GCM est un algorithme parallélisable qui assure une implémentation à haut débit à la fois matériel et logiciel.

Acronymes

Tout d'abord pour bien expliquer le fonctionnement de AES-GCM il nous faut définir certains acronymes.

Plaintext	le texte à chiffrer
Ciphertext	le texte chiffré
auth Data	des données supplémentaires à authentifier
K	la clé de chiffrement
H	Sous clé de hachage
IV	Vecteur d'initialisation supposé aléaoire
Mult	une multiplication dans l'espace de Galois

Chiffrement

AES-GCM est composé deux blocs distincts, le bloc de chiffrement et le bloc d'authentification.

Dans un premier temps on va parler du bloc de chiffrement. Dans GCM il y C pour « counter », c'est-à-dire que AES-GCM s'appuie sur un mode qu'on nomme de CTR [1]. Ce mode fait passer dans un bloc de chiffrement une clé (K) avec un compter initialisé à 0. Ensuite il réalise une opération de type XOR (ou exclusif) sur le texte clair pour obtenir le texte chiffré.

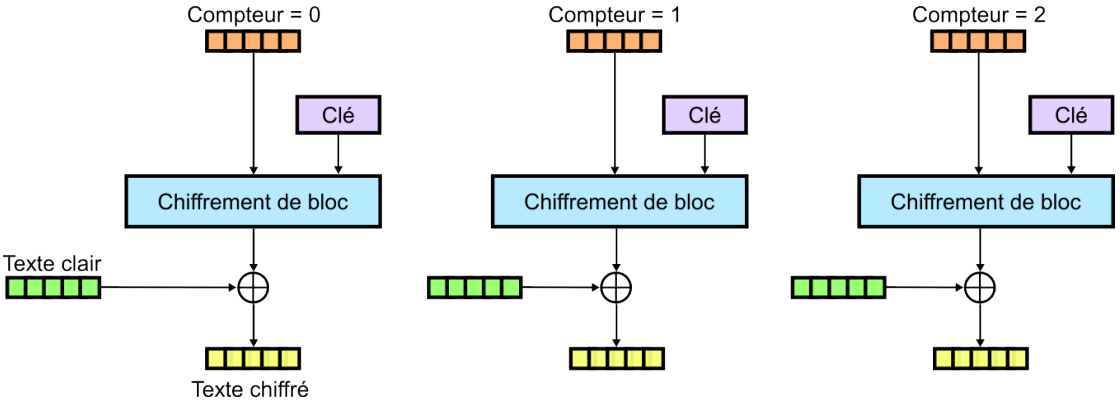

FIGURE 1.2: schéma CTR [4]

Ce mode combine les avantages du chiffrement par flots, est pré-calculable et est parallélisable. En effet il est possible de calculer à l'avance en parallèle tous les chiffrés des compteurs. Il ne restera plus qu'a les passer dans la fonction XOR avec le clair pour obtenir le chiffré.

Dans le cas de AES-GCM le bloc de chiffrement est l'algorithme AES, et le compteur est le vecteur d'initialisation pseudo aléatoire IV qu'on incrémente.

Authentification

Lors de l'algorithme GCM il y a plusieurs chose qui sont authentifié. Pour mieux comprendre nous avons découpé cette opération pour voir tous les éléments qui sont authentifiés.

Tout d'abord la première chose dont on cherche a assurer est l'intégrité des données chiffré que nous envoyons. En effet, nous avons chiffré notre texte mais rien ne nous protège contre une modification intentionnelle ou accidentelle du message envoyé. Ainsi, si Charlie cherche a gêner la communication de Bob et Alice et qu'il change certains bit on voudrait s'en rendre compte.

On pourrait réaliser un hash de notre message avec des fonctions comme sha ou md5, mais si on fait cela on ne pourra pas être protéger contre les modifications intentionnelles. Charlie n'aurait qu'a remplacer le hash par le hash du message contenant sa modification.

La solution retenu dans GCM est d'utiliser des multiplications dans l'espace de Galois avec une autre clef nommé H. On fait donc passé le premier bloc de chiffré dans un bloc de multiplication avec H. Puis on réalise un XOR du résultat avec le bloc de chiffré suivant. Enfin on refait la multiplication comme on peut le voir sur l'image 1.3.

1. CounTeR

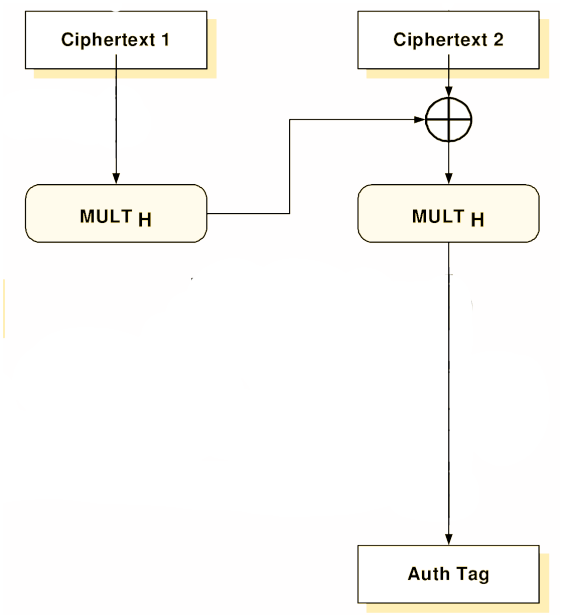

FIGURE 1.3: authentification du message chiffré

Mais on ne veut pas seulement vérifier l'intégrité du message mais également du vecteur d'initialisation IV. Pour cela on réalise un « et » logique entre la longueur de message et la longueur de l'IV puis un XOR avec le tag précédent. Enfin on effectue un bloc de Multiplication dans l'espace de Galois comme on peut le voir sur l'image 1.4.

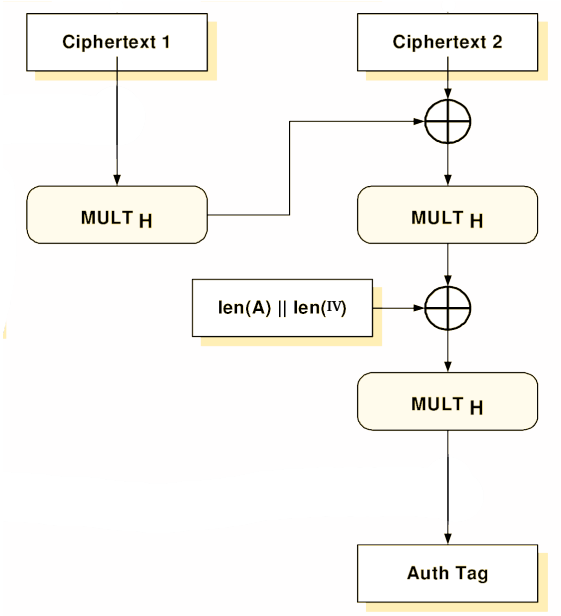

FIGURE 1.4: authentification de la longueur du message et de IV

Ensuite, lors d'une communication entre Alice et Bob il y a des protocole qui sont utilisé pour communiquer comme TCP/IP. Il y a donc des données qui vont entourer le message comme l'adresse IP ou le port de destination. Pour être certain que le message n'a pas été intercepté, on va intégrer ces données a notre tag d'intégrité. Pour cela ils sont rajoutés au début de l'algorithme. On fait passer ces données dans un bloc de multiplication puis on réalise un XOR avec le premier bloc chiffré comme on peut le voir

sur l'image 1.5.

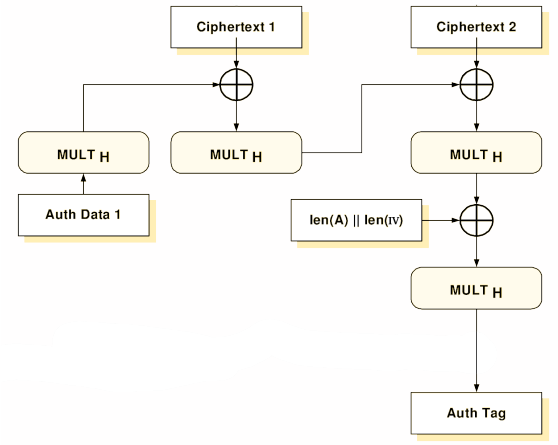

FIGURE 1.5: authentification de data supplémentaire

Nous avons donc l'intégrité du message, de la longueur de IV, de la longueur du message, et des données périphérique au message, mais pour terminer l'intégrité des données on va ajouter a ceci l'IV pour être certain que personne n'a touché a notre vecteur d'initialisation ainsi que la clef K.

Pour cela nous chiffrons l'IV avec un compteur a 0 avec la clef K à travers l'algorithme AES. Puis nous réalisons un XOR avec le tag précédent comme on peut le voir sur l'image 1.6.

On obtient donc un tag qui permet de vérifier l'intégrité de tout les paramètre du message.

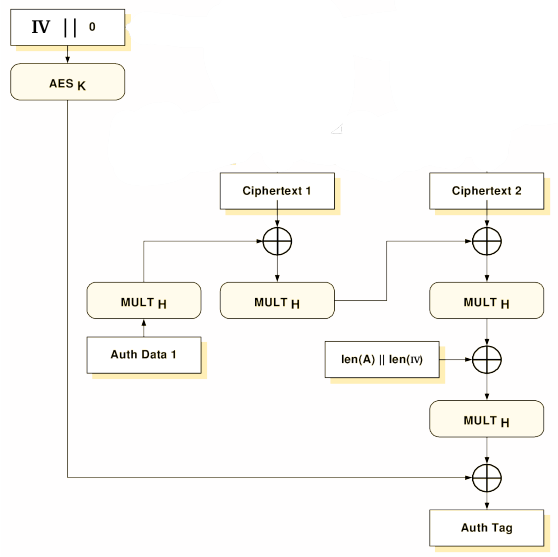

FIGURE 1.6: authentification de la clef K

Le fonctionnement global de AES-GCM est résumé sur l'image 1.7.

1.2 GMAC

GMAC est un cas particulier de GCM ou aucun texte brut n'est présenté.

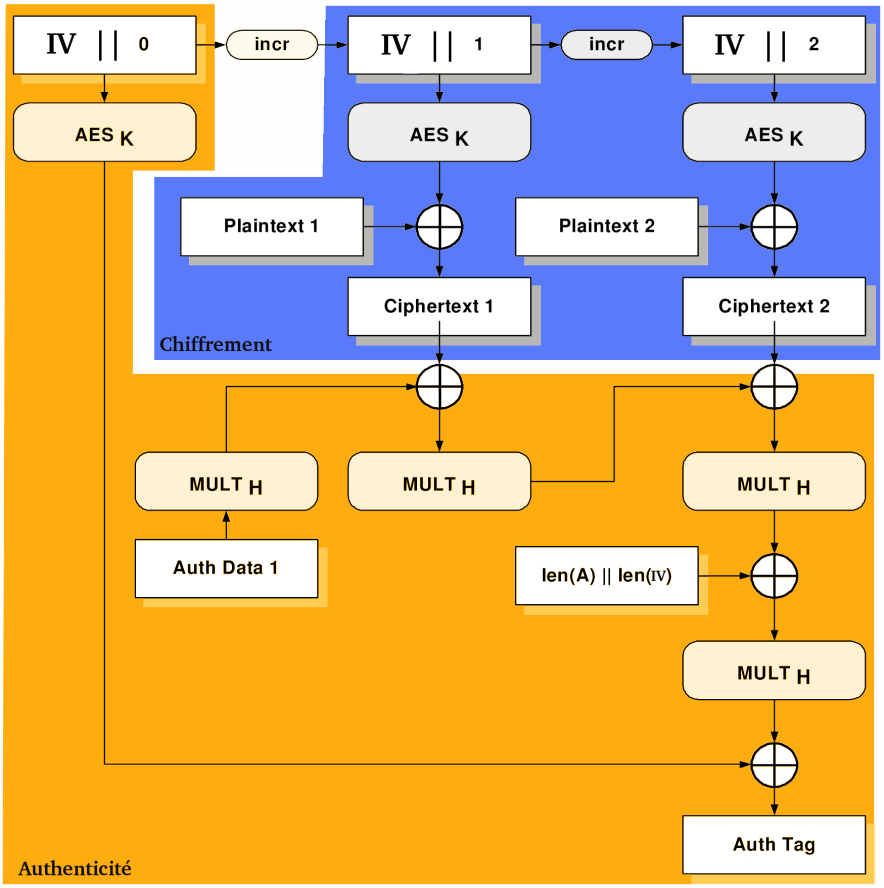

FIGURE 1.7: Fonctionnement de GCM

CHAPITRE 2

Et le reste du monde...

Pas du tout sur...

2.1 OCB

2.2 IAPM

2.3 EAX

2.4 CWC

2.5 CCM

CHAPITRE 3

Vecteurs d'attaques

Le chapter Bonus ! ! ! !

3.1 Les erreurs courantes

Conclusion

Table des figures

Bibliographie

[1] Morris DWORKIN. « Recommendation for Block Cipher Modes of Operation : Galois/Counter Mode (GCM) and GMAC ». Technical Report, NIST, 2007.

[2] David SORIA. « Implementation d'AES : La nitroglycérine ». *MISC*, Mai 2016.

[3] Standford University. *AES-GCM for Efficient Authenticated Encryption – Ending the Reign of HMAC-SHA-1 ?* Shay Gueron, Janvier 2013.

[4] WIKIPÉDIA. « Mode d'opération (cryptographie) », 2016.

[5] David WRONG. « What is GCM ? Galois Counter Mode (of operation) (usually seen as AES-GCM) ». Youtube, 2015.