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

27 avril 2016

AES-GCM

RIGAUD MICHAËL et BADIER CHARLIE

Table des matières

Table des matières **1**

Introduction **2**

1 Fonctionnement **3**
1.1 Fonctionnement nominal (GCM) 3
1.2 GMAC 3

2 Et le reste du monde... **5**
2.1 OCB 5
2.2 IAPM 5
2.3 EAX 5
2.4 CWC 5
2.5 CCM 5

3 Vecteurs d'attaques **6**
3.1 Les erreurs courantes 6

Conclusion **7**

Table des figures **8**

Bibliographie **9**

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 Fonctionnement nominal (GCM)

1.2 GMAC

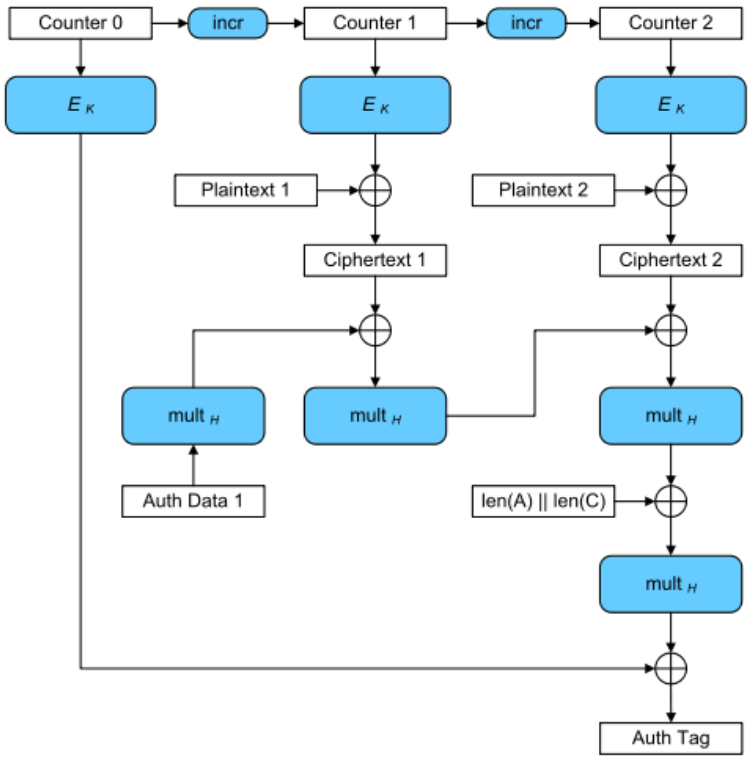

FIGURE 1.1: Fonctionnement de GCM

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

1.1 Fonctionnement de GCM 4

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.