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

26 avril 2016

AES-GCM

RIGAUD MICHAËL et BADIER CHARLIE

Table des matières

Introduction

Halala... AES...
Galois - Counter Mode

CHAPITRE 1

Fonctionnement

1.1 Fonctionnement nominal

1.2 Différents mode de fonctionnement

GMAC

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.