Mémoire de Master

Université de Limoges

Université de Limoges - Master Cryptis

Mémoire pour l'obtention du grade de Master
SÉCURITÉ DE L'INFORMATION ET CRYPTOLOGIE - MENTION INFORMATIQUE

Présenté et soutenu par
Prénom NOM

Le Date de soutenance

TITRE DU MANUSCRIT

Etablissement d'accueil
Lieu de stage ou d'accueil

Encadrants
Mme Premier ENCADRANT, Responsable du service
M. Second ENCADRANT, Ingenieur de recherche

Encadrants Académique
Pr. Pénultième ENCADRANT, Professeur des Universités, XLIM, CNRS
Pr. Dernier ENCADRANT, Maître de Conférences, XLIM, CNRS

Texte de l'épigraphe
Auteur de l'épigraphe

Remerciements

Cette partie est écrite dans un autre fichier et est incluse dans le fichier principal. Vous pouvez diviser votre document en plusieurs fichiers .typ

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magnam aliquam quaerat voluptatem. Ut enim aeque doleamus.

This section is written in another file and is included in the main file. You can divide your document in several .typ file

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magnam aliquam quaerat voluptatem. Ut enim aeque doleamus.

Table des matières,

Table des figures,

Table des tableaux,

Introduction

Partie 1: Titre de la partie 1

Sous titre de la partie 1

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magnam aliquam quaerat voluptatem. Ut enim aeque doleamus animo, cum corpore dolemus, fieri.

Figure 1: Une image d'exemple

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magnam aliquam quaerat voluptatem. Ut enim aeque doleamus animo, cum corpore dolemus, fieri.

Sous titre de la partie 1

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magnam aliquam quaerat voluptatem. Ut enim aeque doleamus animo, cum corpore dolemus, fieri.

Sous titre de la partie 1

```
#Define MAX_SIZE 45

int i = 0;

for (i=0; i<MAX_SIZE; i++)
  printf("Bonjour le monde");
```

Code 1: Légende manquante

Partie 2: Titre de la partie 2

HQC[1]

Encryption: $\boldsymbol{c} = \boldsymbol{m} * \boldsymbol{G} + \boldsymbol{e}$

Syndrome: $\boldsymbol{s} = \boldsymbol{c} * \boldsymbol{H}^T$

Hamming weight of a error vector: $\mathrm{wt}_{H(\boldsymbol{e})} = w$

Quasi-cyclic structure (rotation) : $\boldsymbol{m} * \boldsymbol{G} = \sum_{\{i=0\}}^{\{n-1\}} m_i * \mathrm{rot}_{i(\boldsymbol{g})}$

Fundamental problem (syndrome decoding) : $\boldsymbol{H} * \boldsymbol{e}^T = \boldsymbol{s}$

Decryption: $\widehat{\boldsymbol{m}} = \boldsymbol{c} - \hat{\boldsymbol{e}} * \boldsymbol{G}$

Sous titre de la partie 2

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magnam aliquam quaerat voluptatem. Ut enim aeque doleamus animo, cum corpore dolemus, fieri.

Sous titre de la partie 2

Sous titre de la partie 2

Partie 3: Titre de la partie 3

Sous titre de la partie 3

t	1	2	3
y	0.3	0.7	0.5

Table 1: Example de tableau

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magnam aliquam quaerat voluptatem. Ut enim aeque doleamus animo, cum corpore dolemus, fieri.[1]

Sous titre de la partie 3

Sous titre de la partie 3

[1]This a foonote

Conclusion

Références Bibliographiques

[1] N. ARAGON, O. BLAZY, and P. GABORIT, “Hamming Quasi-Cyclic (HQC) Fourth round version Updated version 19/02/2025.”

Annexes