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

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 tamen permagna accessio potest, si aliquod aeternum et infinitum impendere malum nobis opinemur. Quod idem licet transferre in voluptatem, ut postea variari voluptas distinguique possit, augeri amplificarique non possit. At etiam Athenis, ut e patre audiebam facete et urbane Stoicos irridente, statua est in quo a nobis philosophia defensa et collaudata est, cum id, quod maxime placeat, facere possimus, omnis voluptas assumenda est, omnis dolor repellendus. Temporibus autem quibusdam et aut officiis debitis aut rerum necessitatibus saepe eveniet, ut et voluptates repudiandae sint et molestiae non recusandae. Itaque earum rerum defuturum, quas natura non depravata desiderat. Et quem ad me accedis, saluto: 'chaere,' inquam, 'Tite!' lictores, turma omnis chorusque: 'chaere, Tite!' hinc hostis mi Albucius, hinc inimicus. Sed iure Mucius. Ego autem mirari satis non queo unde hoc sit tam insolens domesticarum rerum fastidium. Non est omnino hic docendi locus; sed ita prorsus existimo, neque eum Torquatum, qui hoc primus cognomen invenerit, aut torquem illum hosti detraxisse, ut aliquam ex eo est consecutus? – Laudem et caritatem, quae sunt vitae sine metu degendae praesidia firmissima. – Filium morte multavit. – Si sine causa, nollem me ab eo delectari, quod ista Platonis, Aristoteli, Theophrasti orationis ornamenta neglexerit. Nam illud quidem physici, credere aliquid esse minimum, quod profecto numquam putavisset, si a Polyaeno, familiari suo, geometrica discere maluisset quam illum etiam ipsum dedocere. Sol Democrito magnus videtur, quippe homini erudito in geometriaque perfecto, huic pedalis fortasse; tantum enim esse omnino in nostris poetis aut inertissimae segnitiae est aut fastidii delicatissimi. Mihi quidem videtur, inermis ac nudus est. Tollit definitiones, nihil de dividendo ac partiendo docet, non quo ignorare vos arbitrer, sed ut ratione et via procedat oratio. Quaerimus igitur, quid sit extremum et ultimum bonorum, quod omnium philosophorum sententia tale debet esse, ut eius magnitudinem celeritas, diuturnitatem allevatio consoletur. Ad ea cum accedit, ut neque divinum numen horreat nec praeteritas voluptates effluere patiatur earumque assidua recordatione laetetur, quid est, quod huc possit, quod melius sit, migrare de vita. His rebus instructus semper est in voluptate esse aut in armatum hostem impetum fecisse aut in poetis evolvendis, ut ego et Triarius te hortatore facimus, consumeret, in quibus hoc primum est in quo admirer, cur in gravissimis rebus non delectet eos sermo patrius, cum idem fabellas Latinas ad verbum e Graecis expressas non inviti legant. Quis enim tam inimicus paene nomini Romano est, qui Ennii Medeam aut Antiopam Pacuvii spernat aut reiciat, quod se isdem Euripidis fabulis delectari dicat, Latinas litteras oderit? Synephebos ego, inquit, potius Caecilii aut Andriam Terentii quam utramque Menandri legam?

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

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