

Codes correcteurs et stéganographie adaptative

Lambert ROSIQUE

Présentation

7 mars 2013

Parcours Scolaire

Licence

- **Post-BAC** : *CPGE MPSI puis MP au Lycée Thiers de Marseille*

Parcours Scolaire

Licence

- **Post-BAC** : *CPGE MPSI puis MP au Lycée Thiers de Marseille*
- **L3** *Mathématiques-Informatiques (Luminy, Marseille)*

Parcours Scolaire

Licence

- **Post-BAC** : *CPGE MPSI puis MP au Lycée Thiers de Marseille*
- **L3** *Mathématiques-Informatiques (Luminy, Marseille)*

Master

- **M1** *Mathématiques et Applications (Luminy, Marseille)*

Parcours Scolaire

Licence

- **Post-BAC** : *CPGE MPSI puis MP au Lycée Thiers de Marseille*
- **L3** *Mathématiques-Informatiques (Luminy, Marseille)*

Master

- **M1** *Mathématiques et Applications (Luminy, Marseille)*
- **M2** *Mathématiques Fondamentales parcours Recherche (Luminy, Marseille)*

Parcours Scolaire

Licence

- **Post-BAC** : *CPGE MPSI puis MP au Lycée Thiers de Marseille*
- **L3** *Mathématiques-Informatiques (Luminy, Marseille)*

Master

- **M1** *Mathématiques et Applications (Luminy, Marseille)*
- **M2** *Mathématiques Fondamentales parcours Recherche (Luminy, Marseille)*
- **M2** *Cryptologie et Sécurité Informatique parcours Professionnel (Bordeaux)*

Parcours Scolaire

Licence

- **Post-BAC** : *CPGE MPSI puis MP au Lycée Thiers de Marseille*
- **L3** *Mathématiques-Informatiques (Luminy, Marseille)*

Master

- **M1** *Mathématiques et Applications (Luminy, Marseille)*
- **M2** *Mathématiques Fondamentales parcours Recherche (Luminy, Marseille)*
- **M2** *Cryptologie et Sécurité Informatique parcours Professionnel (Bordeaux)*

Travaux

Master

1) **TER** (*Travail Encadré de Recherche*) : *Suites de Billard*

Travaux

Master

1) **TER** (*Travail Encadré de Recherche*) : *Suites de Billard*
 \implies *Analyse de ces suites qui modélisent les rebonds d'une boule de billard, suivant l'angle et les obstacles \iff systèmes dynamiques (suites Sturmiennees, fractions continues, suites de rotation, mots mécaniques, mots de Christoffel).*
Propriétés : apériodiques, denses, équilibrées de complexité minimale)...

Travaux

Master

1) **TER** (*Travail Encadré de Recherche*) : *Suites de Billard*
 \implies *Analyse de ces suites qui modélisent les rebonds d'une boule de billard, suivant l'angle et les obstacles \iff systèmes dynamiques (suites Sturmiennees, fractions continues, suites de rotation, mots mécaniques, mots de Christoffel).*

Propriétés : apériodiques, denses, équilibrées de complexité minimale)...

2) **Mémoire** : *Algorithmes qui détectent les facteurs libres et applications*

Travaux

Master

1) **TER** (*Travail Encadré de Recherche*) : *Suites de Billard*
 \implies *Analyse de ces suites qui modélisent les rebonds d'une boule de billard, suivant l'angle et les obstacles \iff systèmes dynamiques (suites Sturmienne, fractions continues, suites de rotation, mots mécaniques, mots de Christoffel).*

Propriétés : apériodiques, denses, équilibrées de complexité minimale)...

2) **Mémoire** : *Algorithmes qui détectent les facteurs libres et applications*

\implies *Etude de l'algorithme de Puder (mot primitif? groupe = facteur libre?), graphes de Stallings, automorphismes du groupe libre, lien facteur libre \iff préservation de la mesure.*

Travaux

Master

1) **TER** (*Travail Encadré de Recherche*) : *Suites de Billard*
 \implies *Analyse de ces suites qui modélisent les rebonds d'une boule de billard, suivant l'angle et les obstacles \iff systèmes dynamiques (suites Sturmienne, fractions continues, suites de rotation, mots mécaniques, mots de Christoffel).*

Propriétés : apériodiques, denses, équilibrées de complexité minimale)...

2) **Mémoire** : *Algorithmes qui détectent les facteurs libres et applications*

\implies *Etude de l'algorithme de Puder (mot primitif? groupe = facteur libre?), graphes de Stallings, automorphismes du groupe libre, lien facteur libre \iff préservation de la mesure.*

Master

3) **Projet** : *HIBE et ABE*

Master

3) **Projet** : HIBE et ABE

⇒ Chiffrement basé sur l'identité hiérarchique. Un user de niveau k pourra déchiffrer les niveaux inférieurs de sécurité

Master

3) **Projet** : HIBE et ABE

⇒ Chiffrement basé sur l'identité hiérarchique. Un user de niveau k pourra déchiffrer les niveaux inférieurs de sécurité

⇒ politique d'accès + attributs pour déchiffrer, possibilité d'exclusion

(couplages sur les courbes elliptiques)

Personnel

(pour mieux me connaître)

- Publication dans "Pour la Science" (août 2010) sur la non-périodicité des suites fractales

Personnel

(pour mieux me connaître)

- *Publication dans "Pour la Science" (août 2010) sur la non-périodicité des suites fractales*
- *Création de quelques sites web, implémentation de cryptosystèmes (analyse différentielle sur l'AES)*

Personnel

(pour mieux me connaître)

- *Publication dans "Pour la Science" (août 2010) sur la non-périodicité des suites fractales*
- *Création de quelques sites web, implémentation de cryptosystèmes (analyse différentielle sur l'AES)*
- *Recueil de poèmes Songes et Pénombre*

Personnel

(pour mieux me connaître)

- *Publication dans "Pour la Science" (août 2010) sur la non-périodicité des suites fractales*
- *Création de quelques sites web, implémentation de cryptosystèmes (analyse différentielle sur l'AES)*
- *Recueil de poèmes Songes et Pénombre*
- *Passionné par le Japon*

Le Stage

Le Cadre

1) *Encadrants :*

- *Anne Elisabeth Baert*
- *Marc Chaumont*
- *Eleonora Guerrini*

Le Stage

Le Cadre

1) Encadrants :

- Anne Elisabeth Baert
- Marc Chaumont
- Eleonora Guerrini

2) Equipes :

- DALI (ECO)
- MAORE
- ICAR

Le Stage

Le Cadre

1) Encadrants :

- Anne Elisabeth Baert
- Marc Chaumont
- Eleonora Guerrini

2) Equipes :

- DALI (ECO)
- MAORE
- ICAR

3) Durée : du 4 mars au 26 juillet 2013 (5 mois)

Le Stage

Le Cadre

1) Encadrants :

- Anne Elisabeth Baert
- Marc Chaumont
- Eleonora Guerrini

2) Equipes :

- DALI (ECO)
- MAORE
- ICAR

3) Durée : du 4 mars au 26 juillet 2013 (5 mois)

4) Domaine : Codes correcteurs, Stéganographie, Image...

Le Stage

Le Cadre

1) Encadrants :

- Anne Elisabeth Baert
- Marc Chaumont
- Eleonora Guerrini

2) Equipes :

- DALI (ECO)
- MAORE
- ICAR

3) Durée : du 4 mars au 26 juillet 2013 (5 mois)

4) Domaine : Codes correcteurs, Stéganographie, Image...

Codes correcteurs et stéganographie adaptative

Objectif(s) du stage : Le but du stage est de concevoir des algorithmes adaptatifs performants basés sur les codes correcteurs, de les analyser et de les évaluer pour des problèmes de stéganographie/stéganalyse.

Codes correcteurs et stéganographie adaptative

Objectif(s) du stage : Le but du stage est de concevoir des algorithmes adaptatifs performants basés sur les codes correcteurs, de les analyser et de les évaluer pour des problèmes de stéganographie/stéganalyse.

Travail demandé :

Le stage se développera en plusieurs parties :

- 1- Comprendre le contexte de la stéganographie et de la stéganalyse,

Codes correcteurs et stéganographie adaptative

Objectif(s) du stage : Le but du stage est de concevoir des algorithmes adaptatifs performants basés sur les codes correcteurs, de les analyser et de les évaluer pour des problèmes de stéganographie/stéganalyse.

Travail demandé :

Le stage se développera en plusieurs parties :

- 1- Comprendre le contexte de la stéganographie et de la stéganalyse,
- 2- Etudier et classer les codes correcteurs utilisés dans les approches non-adaptatives,

Codes correcteurs et stéganographie adaptative

Objectif(s) du stage : Le but du stage est de concevoir des algorithmes adaptatifs performants basés sur les codes correcteurs, de les analyser et de les évaluer pour des problèmes de stéganographie/stéganalyse.

Travail demandé :

Le stage se développera en plusieurs parties :

- 1- Comprendre le contexte de la stéganographie et de la stéganalyse,
- 2- Etudier et classer les codes correcteurs utilisés dans les approches non-adaptatives,
- 3- Etudier et analyser le code de Filler : STC (Syndrome-Trellis Code, 2011) ainsi que son exploitation par Pevny HUGO (2010).

Codes correcteurs et stéganographie adaptative

Objectif(s) du stage : Le but du stage est de concevoir des algorithmes adaptatifs performants basés sur les codes correcteurs, de les analyser et de les évaluer pour des problèmes de stéganographie/stéganalyse.

Travail demandé :

Le stage se développera en plusieurs parties :

- 1- Comprendre le contexte de la stéganographie et de la stéganalyse,
- 2- Etudier et classer les codes correcteurs utilisés dans les approches non-adaptatives,
- 3- Etudier et analyser le code de Filler : STC (Syndrome-Trellis Code, 2011) ainsi que son exploitation par Pevny HUGO (2010).
- 4- Adapter ou/et transformer les codes des versions non-adaptatives pour produire des algorithmes adaptatifs. Analyser et étudier leurs performances.

Conclusion

Enchanté de vous rencontrer !