









Loïc Rouquette

DOCTEUR-INGÉNIEUR EN SCIENCES DE L'INFORMATIQUE




INFORMATIONS

 9 Fév. 1990
 + 33 (6) 79 21 98 71
 contact@loicrouquette.fr
 Lentilly (69) - France





SOCIAL

 loicrouquette.fr
 loicrouquette.fr/cg-profile
 github.com/rloic
 loicrouquette

LANGUES

 Langue Maternelle
 B2 - TOEIC : 915/990
 Lu/écrit : B1 - Oral : A2

LOISIRS

 Intelligence Artificielle
 Algorithmique
 Informatique
 Karaté

OUTILS

 bib_search

Un CLI pour rechercher des entrées bibtex dans de grands fichiers .bib

 bib_fetch

Un CLI pour télécharger des entrées bibtex depuis DBLP ou HAL.

 pandoc

Une librairie rust pour créer des filtres pandoc avec rust.

COMPÉTENCES

Algorithmique IA Git
Optimisation Apprentissage
Adaptabilité Rust Kotlin
Java Constraint Programming
Choco Solver Python 2/3
Cryptographie Autonomie
Cryptanalyse différentielle

FORMATION

DOCTORAT LIRIS / CITI - ED INFOMATHS - INSA, LYON (69) 2022
Approfondissement des compétences scientifiques liées à l'informatique.
Domaine de recherche : IA / Optimisation / Programmation par contraintes / Cryptographie.

DIPLÔME D'INGÉNIEUR SPÉCIALITÉ INFORMATIQUE - INSA, LYON 2019
Apprentissage des compétences scientifiques liées à l'informatique.
Développement du travail collaboratif.

DUT INFORMATIQUE - IUT LYON 1, LYON (69) 2016
Apprentissage des compétences techniques, particulièrement en conception et en développement logiciel.

PUBLICATIONS

Loïc Rouquette (2022). Improving scalability and reusability of differential cryptanalysis models using constraint programming (INSA Lyon). *Thèse*

Virginie Lallemand, Marine Minier & Loïc Rouquette (2022). Automatic Search of Rectangle Attacks on Feistel Ciphers: Application to WARP. IACR Trans. Symmetric Cryptol., 2022(2), 113–140. *Conférence*

Loïc Rouquette, David Gerault, Marine Minier & Christine Solnon (2022). And Rijndael? Automatic Related-key Differential Analysis of Rijndael. In AfricaCrypt 2022 - 13th International Conference on Cryptology AfricaCrypt. *Conférence*

Loïc Rouquette & Christine Solnon. Utilisation de la Programmation par contrainte appliquée à la cryptanalyse différentielle. In 23^{ème} congrès annuel de la Société Française de Recherche Opérationnelle et d'Aide à la Décision, INSA Lyon, Feb 2022, Villeurbanne - Lyon, France. *Conférence*

Loïc Rouquette & Christine Solnon (2020). abstractXOR: A global constraint dedicated to differential cryptanalysis. In Principles and Practice of Constraint Programming - 26th International Conference, CP 2020, Louvain-la-Neuve, Belgium, September 7-11, 2020, Proceedings (pp. 566–584). Springer. *Conférence*

Loïc Rouquette & Christine Solnon. In Contrainte globale abstractXOR : résultats de complexité et algorithmes de propagation. Journées Francophones de Programmation par Contraintes (JFPC), 2019, Albi, France. *Conférence*

EXPÉRIENCES

UNIVERSITÉ DE LORRAINE, NANCY (54) En cours - Décembre 2022
CHERCHEUR POSTDOCTORAL - INTELLIGENCE ARTIFICIELLE / CRYPTOGRAPHIE & SÉCURITÉ
Amélioration et extension d'outils automatiques pour la résolution de problèmes de cryptanalyse.

Kotlin Java Rust Choco Solver MiniZinc Algorithmique SPN Feistel Automatisation
Conception Modélisation

LIRIS CNRS, LYON (69) 3 ans - Octobre 2019
DOCTORANT - INTELLIGENCE ARTIFICIELLE / CRYPTOGRAPHIE & SÉCURITÉ
Modélisation et résolution de problèmes de cryptanalyse différentielle sur des chiffrements SPN et Feistel.

Kotlin Java Rust Choco Solver MiniZinc Algorithmique SPN Feistel Modélisation

LIRIS CNRS / CITI INRIA, LYON (69) 6 mois - Février 2019
INGÉNIEUR DE RECHERCHE STAGIAIRE - INTELLIGENCE ARTIFICIELLE / CRYPTOGRAPHIE & SÉCURITÉ
Développement d'une nouvelle approche de raisonnement abstrait pour aider à la modélisation et la résolution de problèmes de cryptanalyse différentielle sur AES.

Kotlin Java Rust Choco Solver MiniZinc Algorithmique AES Midori

2^E RÉGIMENT D'INFANTRIE DE MARINE, LE MANS (72) 5 ans - Septembre 2009
SOLDAT > CHEF D'ÉQUIPE > ADJOINT CHEF DE GROUPE
Diriger et travailler en équipe, autonomie, sens des responsabilités, organisation de planning, gestion d'effectifs, respect des délais.