ACADÉMIE MILITAIRE
SAINT-CYR COËTQUIDAN

Intitulé de l'offre de stage : Etude technique des algorithmes génétiques multi-objectifs (MOGA) et mise en œuvre dans un contexte cryptographique.
(À partir de janvier 2025)

Date butoir pour candidater : vendredi 17 décembre 2024

Descriptif du stage :

Au sein du Centre de Recherche de Saint-Cyr Coëtquidan (CReC), Aline Hufschmitt (MCF spécialisée en IA) et Patrice Parraud (MCF spécialisé en Cyber) collaborent sur le projet Genetic Meta-Cipher (GMC), un framework pour le chiffrement symétrique exploitant un algorithme génétique afin de générer une population de protocoles de chiffrement. Les premiers résultats, prometteurs, montrent une capacité des meilleurs individus à générer un aléa similaire à celui d'un protocole comme AES [1].

Actuellement, GMC s'appuie sur l'algorithme NSGA-II. Cet algorithme est maintenant connu pour avoir des difficultés de convergence en présence de nombreux paramètres à optimiser [2]. Afin de poursuivre efficacement le développement de GMC, une étude approfondie des différents algorithmes génétiques multi-objectifs est nécessaire. Ces algorithmes sont très nombreux et présentent beaucoup de variantes (NSGA-III [3, 4, 5, 6], MOEA/D [7], SMS-MOEA [8], C-MOEA/D, PPS-MOEA/D, MOEA/D-PBI, MOEA/DD, RVEA, SparseEA, DEA-GNG, R2HCA-EMOA, PREA, CMME, CMOEA-MS, CCMO, C-TSEA, C-TAEA, GSEMO, SMS-EMOA & HypE, Map-Elite, …).

L'objectif du stage est de réaliser une étude technique de ces algorithmes afin d'exhiber le plus adapté au contexte imposé.

Dans un premier temps, le stagiaire devra faire une recherche bibliographique pour identifier les algorithmes majeurs et leurs articles fondateurs, puis pour chacun d'eux réaliser un document technique expliquant le principe général, ses spécificités (cas favorables ou défavorables), ses variantes et la filiation avec les autres algorithmes existants. Ce document permettra en collaboration avec l'équipe d'identifier les deux/trois algorithmes les plus adaptés au contexte imposé par GMC.

Dans un second temps, le stagiaire implémentera ces deux/trois algorithmes identifiés (ou trouvera une implémentation existante) et mettra en œuvre un exemple simple permettant de vérifier les performances de chaque algorithme et de les comparer entre eux. Le stage s'achèvera par le choix de l'algorithme le plus adapté à la poursuite du développement de GMC.

Une publication sur les travaux réalisés pourra être envisagée selon la portée des résultats obtenus.

Références

[1] A. Husfchmitt et P. Parraud, «Genetic Meta Cipher,» chez Proceedings of the Genetic and Evolutionary Computation Conference (GECCO '24), New York, NY, USA, 1264–1272, 2024.
[2] GECCO, GECCO '24: Proceedings of the Genetic and Evolutionary Computation Conference, vol. ISBN: 9798400704949, Melbourne, VIC, Australia: Association for Computing Machinery, New York, NY, USA, 2024.
[3] A. Ibrahim, S. Rahnamayan, M. V. Martin et K. Deb, «EliteNSGA-III: An improved evolutionary many-objective optimization algorithm,» chez CEC 2016 - IEEE Congress on Evolutionary Computation Proceedings, 2016.
[4] H. Jain et K. Deb, «An Evolutionary Many-Objective Optimization Algorithm Using Reference-point Based Non-dominated Sorting Approach, Part II: Handling Constraints and Extending to an Adaptive Approach,» chez IEEE Transactions on Evolutionary Computation, 2014.
[5] Y. Yuan, H. Xu et B. Wang, «An improved NSGA-III procedure for evolutionary many-objective optimization,» chez GECCO 2014 - Genetic and Evolutionary Computation Conference Proceedings, 2014.

[6] K. Deb et H. Jain, «An Evolutionary Many-Objective Optimization Algorithm Using Reference-point Based Non-dominated Sorting Approach, Part I: Solving Problems with Box Constraints,» chez IEEE Transactions on Evolutionary Computation, 2014.
[7] Q. Zhang et H. Li, MOEA/D: A Multiobjective Evolutionary Algorithm Based on Decomposition. IEEE Transactions on Evolutionary Computation, vol. 11, 2008, pp. 712 - 731.
[8] N. Hochstrate, B. Naujoks et M. Emmerich, «SMS-EMOA: Multiobjective selection based on dominated hypervolume.,» European Journal of Operational Research, vol. 181, pp. 1653-1669, 2007.

Profil du stagiaire H/F :

Le stagiaire doit avoir un niveau Master2 en informatique avec de bonnes bases concernant les Algorithmes Génétiques.
Il doit lire avec aisance en langue anglaise (nécessaire pour pouvoir comprendre les articles scientifiques) et avoir une appétence pour le travail de recherche bibliographique. Il doit également avoir une bonne aisance à l'écrit pour la rédaction des documents techniques (ces documents pourront être en français ou anglais, au choix du stagiaire).
Le stagiaire devra également avoir des compétences dans différents langages de programmation (C, C++, Java, Python) pour être en mesure de relire le code source écrit par d'autres ou pour implémenter lui-même les algorithmes décrits dans les articles.
Quelques connaissances en cryptographie et/ou tests statistiques pourraient compléter l'éventail des compétences du stagiaire.

Descriptif de l'employeur :

Le centre de recherche (CReC Saint-Cyr) de l'Académie militaire de Saint-Cyr Coëtquidan (AMSCC) a pour vocation à produire des connaissances en matière de défense et de sécurité au profit des états-majors, d'irriguer l'enseignement supérieur délivré aux différentes écoles de l'Académie militaire et produire une recherche académique reconnue par la communauté scientifique.

Lieu du stage : AMSCC / DE / CReC / Pôle SDIAT / UR MIRIAD.

Financement et hébergement :

Une compensation financière est prévue pour le/la stagiaire à hauteur de la gratification minimale légale.
Les éventuels déplacements en mission seront pris en charge par le CReC Saint-Cyr.
Des possibilités d'hébergement et de restauration sur le camp sont possibles.

Durée du stage :

A partir de janvier 2025 pour une durée maximale de 6 mois.

Tuteurs de stage : Aline Hufschmitt, Maître de Conférences
Patrice PARRAUD, Maître de Conférences HC

Contacts : aline.hufschmitt@st-cyr.terre-net.defense.gouv.fr
patrice.parraud@st-cyr.terre-net.defense.gouv.fr

Candidater :
Envoi d'un CV et d'une lettre de motivation au contact de l'annonce.