ANSSI - Agence nationale de la sécurité des systèmes d'information

Stage - Cryptanalyse par réduction de réseaux F/H

Paris 15e Arrondissement, 75, Paris, Île-de-France

Type de contrat	**Niveau d'études**
Stagiaire école	Master 1 ou titre équivalent de niveau Bac +4
Prise de fonction souhaitée	**Date limite de candidature**
03/03/2025	-
Domaine professionnel	**Niveau d'expérience**
Cryptologue	Débutant ou jeune diplômé
Rémunération	**Avantages liés au poste**
A définir selon expérience mensuel net A définir selon expérience annuel brut (selon expérience)	-
Contraintes particulières d'exercice	**Télétravail**
-	Non

Descriptif de l'organisation

Rejoindre l'Agence nationale de la sécurité des systèmes d'information (ANSSI), c'est mettre ses compétences au service de l'intérêt général en participant à une mission capitale, d'actualité et porteuse de grandes responsabilités dans un monde où la cybersécurité est devenue l'affaire de tous !

Au sein de la sous-direction Expertise (SDE) se trouve la Division Scientifique et Technique (DST), les Laboratoires Sécurité des Composants (LSC) et de Cryptographie (LCR) sont respectivement les pôles d'excellences dans le domaine des composants sécurisés et des logiciels qu'ils embarquent et dans celui des algorithmes et architectures cryptographiques. Ils ont pour objectif d'anticiper les risques, de soutenir le centre de certification national lors des évaluations des produits de sécurité, de contribuer à la recherche, à l'analyse des besoins et à la conception de solutions propres à les

satisfaire ainsi qu'à l'élaboration et la mise à jour de référentiels techniques.

Descriptif des missions

Les attaques basées sur les réseaux euclidiens exploitent leur structure mathématique pour attaquer des systèmes cryptographiques. Un tel réseau est un sous-groupe discret de Rn, et des algorithmes de réduction de réseau, tels que le célèbre algorithme Lenstra-Lenstra-Lovász (LLL) et l'algorithme Block Korkin-Zolotarev (BKZ), sont utilisés pour trouver des vecteurs courts et quasi orthogonaux formant une base de ces réseaux. Ces algorithmes sont fondamentaux en cryptanalyse, car ils permettent de résoudre efficacement des variantes approximatives du problème du vecteur le plus court (SVP) ou du problème du vecteur le plus proche (CVP) dans ces réseaux ainsi que de trouver des petites racines d'équations polynomiales modulo un entier via la méthode de Coppersmith. Lors de ce stage, nous nous concentrerons sur l'utilisation de la réduction de réseau dans le cadre d'attaques où des informations supplémentaires sont connues. Le stage suivra ce plan :

• Réaliser une revue approfondie des algorithmes de réduction de réseau existants et de leurs applications en cryptanalyse. Cela inclut la compréhension de leurs fondements mathématiques, des améliorations algorithmiques récentes ainsi que des implications et limitations pratiques ;
• Analyser la vulnérabilité de divers schémas cryptographiques (classiques et post-quantiques) en connaissance d'informations supplémentaires ;
• Implémenter des algorithmes de réduction de réseau et simuler des attaques sur des schémas cryptographiques pour comprendre leur efficacité pratique et leurs limitations ;
• Explorer des améliorations potentielles des méthodes existantes de cryptanalyse basées sur les réseaux ou de nouvelles manières d'attaquer les schémas existants avec ces méthodes.
• Compiler les résultats dans des rapports complets, documenter le processus de recherche et présenter vos résultats au sein de l'équipe de recherche.

Le stage pourra avoir lieu à Rennes ou à Paris.

Profil recherché

Etudiant/e en dernière année d'école d'ingénieur ou cursus universitaire équivalent dans le domaine des nouvelles technologies (informatique/mathématiques). Vous avez une appétence pour le domaine de la sécurité matérielle, et avez envie de manipuler des circuits électroniques en laboratoire.

Compétences requises : • Une maîtrise de la théorie des nombres, de l'algèbre linéaire et des mathématiques discrètes ;
• Compréhension des schémas de cryptographie asymétrique classiques (ECDSA, RSA, DH, etc.) et de leurs fondements mathématiques ;
• Une familiarité avec l'analyse d'algorithmes et de leur complexité ; avoir étudié les algorithmes de réduction de réseau est un plus, mais ce n'est pas obligatoire ;
• Des compétences avancées en programmation en C, Python et dans un système de calcul algébrique (tel que Sage ou Magma).

Savoir-être : • Curiosité d'esprit et rigueur ;
• Autonomie ;
• Appétence pour les sujets techniques ;
• Capacité de rédaction, de communication et de synthèse.

Process de recrutement

• Si votre candidature est présélectionnée, vous serez contacté(e) pour apprécier vos attentes et vos

motivations au cours d'un entretien téléphonique ou physique.
• Des tests techniques pourront vous être proposés.
• Vous ferez l'objet d'une procédure d'habilitation.