# Offre n°2025-08955

# Doctorant F/H Nouveaux outils pour la cryptanalyse symétrique quantique

**Type de contrat :** CDD

**Niveau de diplôme exigé :** Bac + 5 ou équivalent

**Fonction :** Doctorant

## A propos du centre ou de la direction fonctionnelle

Le centre Inria de l'Université de Rennes est un des neuf centres d'Inria et compte plus d'une trentaine d'équipes de recherche. Le centre Inria est un acteur majeur et reconnu dans le domaine des sciences numériques. Il est au cœur d'un riche écosystème de R&D et d'innovation : PME fortement innovantes, grands groupes industriels, pôles de compétitivité, acteurs de la recherche et de l'enseignement supérieur, laboratoires d'excellence, institut de recherche technologique.

## Contexte et atouts du poste

Le développement des dispositifs de calcul quantique affecte fortement les garanties de sécurité de la cryptographie asymétrique, entraînant une transition en cours vers des cryptosystèmes post-quantiques, c'est-à-dire résistants aux attaques quantiques. Heureusement, les primitives symétriques couramment utilisées sont considérées comme robustes face à des adversaires quantiques hypothétiques. Toutefois, notre confiance dans la sécurité des cryptosystèmes symétriques repose sur un effort rigoureux de cryptanalyse. Cet effort doit se poursuivre dans le contexte de la sécurité post-quantique.

Ce poste de doctorat s'inscrit dans le cadre du projet QATS, qui étudie la cryptanalyse des primitives symétriques (chiffrements par blocs, fonctions de hachage, etc.) à l'aide d'algorithmes quantiques. QATS se concentre à la fois sur la systématisation de nouvelles techniques d'attaque et sur le développement d'outils automatiques permettant de trouver des attaques.

## Mission confiée

Le ou la doctorant·e étudiera les attaques basées sur des algorithmes de convolution quantique (qui ont été utilisés récemment en cryptanalyse linéaire), ainsi que leur application à la cryptanalyse des chiffrements par blocs, ainsi que l'automatisation de ces techniques.

Des informations supplémentaires sur ce projet ainsi que des références bibliographiques sont disponibles sur ce document.

## Principales activités

Le ou la doctorant·e contribuera aux activités de recherche de l'équipe CAPSULE et du projet QATS.

- Concevoir de nouveaux algorithmes d'attaque basés sur les convolutions quantiques
- Analyser les attaques existantes et nouvelles, et concevoir des outils automatiques pour les identifier

Le ou la candidat·e communiquera également ses travaux par le biais de publications et d'interventions dans des conférences, ateliers ou séminaires.

## Compétences

Le ou la candidat·e idéal·e possédera les compétences suivantes :

- Un bon niveau d'anglais, à l'écrit comme à l'oral
- Des compétences relationnelles (travail en équipe)
- Une formation en cryptographie et/ou en algorithmique
- Des compétences en programmation en Python ou dans d'autres langages
- Des notions d'informatique quantique

## Avantages

- Restauration subventionnée
- Transports publics remboursés partiellement
- Congés: 7 semaines de congés annuels + 10 jours de RTT (base temps plein) + possibilité d'autorisations d'absence exceptionnelle (ex : enfants malades, déménagement)
- Possibilité de télétravail (après 6 mois d'ancienneté) et aménagement du temps de travail
- Équipements professionnels à disposition (visioconférence, prêts de matériels informatiques, etc.)

- Prestations sociales, culturelles et sportives (Association de gestion des œuvres sociales d'Inria)
- Accès à la formation professionnelle

## Rémunération

Salaire brut : 2200€

## Informations générales

- **Thème/Domaine :** Algorithmique, calcul formel et cryptologie
- **Ville :** Rennes
- **Centre Inria :** Centre Inria de l'Université de Rennes
- **Date de prise de fonction souhaitée :** 2025-09-15
- **Durée de contrat :** 3 ans
- **Date limite pour postuler :** 2025-07-31

## Contacts

- **Équipe Inria :** CAPSULE
- **Directeur de thèse :**
  Schrottenloher Andre / andre.schrottenloher@inria.fr

## A propos d'Inria

Inria est l'institut national de recherche dédié aux sciences et technologies du numérique. Il emploie 2600 personnes. Ses 215 équipes-projets agiles, en général communes avec des partenaires académiques, impliquent plus de 3900 scientifiques pour relever les défis du numérique, souvent à l'interface d'autres disciplines. L'institut fait appel à de nombreux talents dans plus d'une quarantaine de métiers différents. 900 personnels d'appui à la recherche et à l'innovation contribuent à faire émerger et grandir des projets scientifiques ou entrepreneuriaux qui impactent le monde. Inria travaille avec de nombreuses entreprises et a accompagné la création de plus de 200 start-up. L'institut s'e?orce ainsi de répondre aux enjeux de la transformation numérique de la science, de la société et de l'économie.

**Attention**: Les candidatures doivent être déposées en ligne sur le site Inria. Le traitement des candidatures adressées par d'autres canaux n'est pas garanti.

## Consignes pour postuler

Déposer en ligne CV et lettre de motivation

**Sécurité défense :**
Ce poste est susceptible d'être affecté dans une zone à régime restrictif (ZRR), telle que définie dans le décret n°2011-1425 relatif à la protection du potentiel scientifique et technique de la nation (PPST). L'autorisation d'accès à une zone est

délivrée par le chef d’établissement, après avis ministériel favorable, tel que défini dans l’arrêté du 03 juillet 2012, relatif à la PPST. Un avis ministériel défavorable pour un poste affecté dans une ZRR aurait pour conséquence l’annulation du recrutement.

**Politique de recrutement :**
Dans le cadre de sa politique diversité, tous les postes Inria sont accessibles aux personnes en situation de handicap.