■ 公募情報

公募No.	2027R-77
職種	リサーチアシスタント
部署	サイバーセキュリティ研究所セキュリティ基盤研究室
研究テーマ	ハッシュ関数に基づく耐量子計算機暗号の安全性評価に関する研究
研究テーマ要旨	当研究室では、ハッシュ関数を主要な構成要素として利用する耐量子計算機暗号、特にハッシュベース署名方式の安全性評価に関する研究を行っている。リサーチアシスタントは、担当研究員の指導の下、ハッシュベース署名方式およびその安全性評価に関する最新の研究動向の調査、安全性モデルや安全性証明の分析、ハッシュ関数に仮定される安全性要件の評価などの補助業務に従事する。また、関連する暗号方式やその構成要素について、理論的な安全性評価を行うとともに、必要に応じて計算機を用いた解析・評価を行う。最終的には、得られた調査・分析・評価結果を学術的・科学的観点から整理・体系化し、国内外の学会における論文発表へと繋げる。
科学技術・イノベーション創出の活性化に関する法律第15条の2の対象業務該当の有無	【有】
応募要件	以下の全ての要件を満たす者。 1. 共通鍵暗号、公開鍵暗号、ハッシュ関数等の現代暗号に関する基礎的知識を有していること。 2. ハッシュ関数の基本的な安全性要件（原像計算困難性、第2原像計算困難性、衝突計算困難性、等）について理解していること。 3. 耐量子計算機暗号、特にハッシュベース署名方式に関する基礎的知識を有していること。 4. 暗号方式の安全性モデルおよび安全性証明に関する基礎的知識を有し、数理的な手法を用いた理論的な解析に取り組むことができること。 5. C、C++、Python、SageMath等のプログラミング言語・計算環境のいずれかを用いたプログラムの実装経験を有していること。 6. 暗号技術分野の英語論文や標準化文書を読むことに抵抗がないこと。 7. 配属研究室内外の人員と協力して研究を遂行できるコミュニケーション能力を有すること。 8. 2027年4月現在で博士前期課程に在籍していること。 ※ 応募に際して事前に所属大学・研究室の指導教官から了承を得ること。 ※ 日本学術振興会の特別研究員などの専念義務がある学生は、本業務に従事可能であることを示す承諾書を指導教官名で提出すること。また、本業務に支障がある場合は応募者及び指導教官がその責務を負うこと。
募集人員	1 人
契約期間	採用日　～　令和10年3月31日（更新の可能性：有り）
更新した場合の雇用期間（又は期日）	一定の条件を満たした場合に、採用日より最長5年
給与(本給)	12,720円　～　17,850円/日 学部在籍者は日給12,720円、大学院博士課程前期在籍者は日給15,690円、大学院博士課程後期在籍者は日給17,850円。 ただし、本給については、国家公務員の給与に準拠していることから国家公務員の給与に改正があり、当機構労働組合等の合意後に本給の改定が生じた場合は変更する。
勤務地名称	本部 (東京都小金井市)
勤務頻度	週2日／1日7.5時間 ※時間外労働有

※従事する業務及び勤務地の変更の範囲：原則として変更無し
※部署の名称、勤務地の名称、及び研究テーマや研究テーマ要旨内の表現に関しては、組織改編等により変更となる場合があります。

NICT有期雇用職員公募情報：https://www.nict.go.jp/employment/apply.html