

WISSENSCHAFT UND WIRTSCHAFT IN EINEM JOB GEHT NICHT.

DOCH.

Finden Sie es heraus bei Fraunhofer.

IT-SICHERHEIT IST IHR THEMA? WIR BEIM FRAUNHOFER SIT BIETEN IHNEN AB SOFORT EINE SPANNENDE TÄTIGKEIT ALS

Wissenschaftliche*r Mitarbeiter*in – Post-Quantum-Kryptografie

Das Nationale Forschungszentrum für angewandte Cybersicherheit ATHENE ist eine Forschungseinrichtung der Fraunhofer-Gesellschaft unter Beteiligung der Fraunhofer-Institute SIT und IGD sowie der Hochschulen TU Darmstadt und Hochschule Darmstadt. Im Fokus stehen die angewandte Forschung und die Entwicklung innovativer Lösungen für reale Sicherheits- und Datenschutzfragen.

So viel ist sicher: Der Quantencomputer kommt, wir wissen nur nicht wann. Er wird in der Lage sein, viele der gegenwärtig verwendeten Kryptoverfahren wie RSA und ECC zu brechen. ATHENE befasst sich mit der Analyse, Entwicklung und Implementierung neuartiger kryptografischer Verfahren, die sowohl der Rechenleistung eines Quantencomputers standhalten als auch sicher vor klassischen Angriffen sein werden. Dabei wird insbesondere auch die Performanz und Benutzbarkeit in der praktischen Anwendung betrachtet. Außerdem trägt ATHENE zur Standardisierung dieser zukunftsweisenden Technologien durch internationale Gremien wie das National Institute of Standards and Technology, kurz NIST, bei.

Das Fraunhofer SIT sucht in diesem Zusammenhang eine*n engagierte*n Mitarbeiter*in für die Abteilung Advanced Cryptographic Engineering, um sich der Herausforderung zu stellen.

Was Sie bei uns tun

- Angewandte Forschungsprojekte im Bereich im Bereich IT-Sicherheit und Kryptografie
- Mitarbeit in öffentlich geförderten und/oder direkt durch Industriepartner beauftragten Projekten
- Konzeptentwicklung und Projektmanagementaufgaben
- Anfertigen von Projektberichten und wissenschaftlichen Veröffentlichungen
- Präsentation von Forschungsergebnissen im Rahmen von Publikationen und Vorträgen auf nationalen und internationalen Fachkonferenzen

Was Sie mitbringen

- Master of Science im Fachgebiet Informatik, Mathematik, Elektrotechnik oder einem anderen Fachgebiet mit Bezug zur Cybersicherheit
- Sie haben fundiertes Wissen im Bereich der IT-Sicherheit und Kryptographie und idealerweise Post-Quantum-Kryptografie vorzuweisen
- Sie besitzen Kenntnisse in der Programmierung von Mikrocontrollern bzw. eingebetteten Systemen in C und/oder Assembler oder FPGA Programmierung in VHDL oder Verilog
- Wünschenswert sind zudem Erfahrungen mit Implementierungsangriffen (insb. Seitenkanalangriffen) sowie Python, Sage, Latex, git und Linux
- Sie beherrschen die deutsche und englische Sprache in Wort und Schrift

Was Sie erwarten können

- Sie arbeiten an einem renommierten, international führenden Institut im Bereich Cybersicherheit
- Sie arbeiten in innovativen Forschungs- und Entwicklungsprojekten mit Partnern aus Industrie, Verwaltung und anderen Forschungseinrichtungen
- Sie erhalten eine systematische Karriereplanung mit individuellen Qualifizierungen sowie Möglichkeit zur Promotion
- Sie arbeiten in einem freundlichen, offenen und kollegialen Arbeitsumfeld mit dynamischer und kreativer Arbeitsatmosphäre
- Wir leben eine familienfreundliche Kultur mit flexiblen Arbeitszeiten und der Möglichkeit, regelmäßig tageweise im Home-Office zu arbeiten

Die Stelle ist zunächst auf 2 Jahre befristet. Eine langfristige Beschäftigung wird angestrebt. Die wöchentliche Arbeitszeit beträgt 39 Stunden. Die Stelle kann auch in Teilzeit besetzt werden. Schwerbehinderte Menschen werden bei gleicher Eignung bevorzugt eingestellt. Wir weisen darauf hin, dass die gewählte Berufsbezeichnung auch das dritte Geschlecht miteinbezieht. Die Fraunhofer-Gesellschaft legt Wert auf eine geschlechtsunabhängige berufliche Gleichstellung. Anstellung, Vergütung und Sozialleistungen basieren auf dem Tarifvertrag für den öffentlichen Dienst (TVöD). Zusätzlich kann Fraunhofer leistungs- und erfolgsabhängige variable Vergütungsbestandteile gewähren.

Kennziffer: 4223