SRIC/06

INDIAN INSTITUTE OF TECHNOLOGY, ROORKEE
(Name of Dept./Centre)

Dated: 15-06-2026

ADVERTISEMENT TO FILL UP PROJECT POSITIONS*

Applications are invited from Indian nationals only for project position(s) as per the details given below for the consultancy/research project(s) under the Principal investigator (Name: **Dr. Raghvendra Singh Rohit**), Dept./Centre **Computer Science and Engineering**, Indian Institute of Technology, Roorkee.

1. Title of project: **A comprehensive security analysis of NIST Accordion mode proposals and their implications to hash functions over Galois fields.**
2. Sponsor of the project: **ANRF-ARG**
3. Project position(s) and number: **Junior Research Fellow (1) and Research Associate-I (1)**
4. Qualifications:

Position	Essential	Desirable
Junior Research Fellow	1. M.E./M.Tech. in Information Tech./Computer Science & Engineering OR B.E. / B.Tech. in Computer Sc. & Engineering / Information Technology/ Mathematics and Computing or equivalent OR Five years integrated BS-MS in Mathematics and Computing or equivalent. 2. CGPA above 8 (or 80% marks). 3. GATE qualified in CS OR UGC-NET qualified.	1. Experience in cryptography and cybersecurity along with a solid backg in programming is preferred.
Research Associate-I	1. PhD degree in Computer Science and Engineering/Mathematics & Computing or related disciplines with specialization in cryptography or security.	1. Publications in top-tier cryptography and security venues. 2. Background in programming is preferred.

5. Emoluments:
   Junior Research Fellow: Rs. 37,000 + HRA
   Research Associate-I: Rs. 58,000 + HRA
6. Duration:
   Junior Research Fellow: Initially for 1 year (extendable till the end of project based on performance review every 6 months).
   Research Associate-I: Initially for 1 year (extendable till the end of project based on performance review every 6 months).

7. Job description

Junior Research Fellow	Rijndael-256 security analysis, Accordion mode classical and quantum cryptanalysis with automated tools, accordion mode implementation and benchmarking in software and hardware platforms, new 256-bit block cipher design, analysis of hash functions over Galois Fields.
Research Associate-I	**Research tasks:** Rijndael-256 security analysis, Accordion mode classical and quantum cryptanalysis with automated tools, accordion mode implementation and benchmarking in software and hardware platforms, new 256-bit block cipher design, analysis of hash functions over Galois Fields. **Project monitoring:** Monitor progress of the project at participating institutes.

1. Candidates before appearing for the interview shall ensure that they are eligible for the position they intend to apply.
2. Candidates desiring to appear for the Interview should submit their applications with the following documents to the office of Principal Investigator through email, by post or produce at the time of Interview:
   - Application in a plain paper with detailed CV including chronological discipline of degree/certificates obtained.
   - Experience including research, industrial field and others.
   - Attested copies of degree/certificate and experience certificate.
3. Candidate shall bring along with them the original degree(s)/certificate(s) and experience certificate(s) at the time of interview for verification.
4. Preference will be given to SC/ST candidates on equal qualifications and experience.
5. Please note that no TA/DA is admissible for attending the interview.

Note: The selected JRF candidate may get an opportunity for PhD admission.
The last date for application to be submitted to office of Principal Investigator is **30th June 2026, by 5 PM.**
(*not applicable for walk in interview*)

The shortlisted candidates will be notified regarding the interview schedule via the email.

Approved

Dean
Sponsored Research & Industrial Consultancy
Indian Institute of Technology Roorkee
Roorkee-247 667 (INDIA)
15/06/2026

15/6/26

Raghvendra Singh Rohit
15/06/2026

Tel: +91-1332-285663 **Fax:**

Email:

Name and signature of Principal Investigator

*To be uploaded on IIT Roorkee website and copy may be sent to appropriate addresses by PI for wider circulation.