



Indian Institute of Science Education and Research Bhopal

Junior Research Fellows (JRFs)/Project Associate-I at IISER Bhopal

Applications are invited from Indian nationals for the post of Project Associate-I at IISER Bhopal in the DRDO-funded Research Project “New designs of post-quantum cryptographic candidates”.

Project description: The project involves a study of computationally hard mathematical problems relevant to post-quantum cryptography. More specifically, the project aims to study the hard lattice problems and their applications in the design of a digital signature scheme (DSS). The project further seeks to implement a DSS scheme which is post-quantum secure.

Duration: 1 Year, further extendable to the end of the project.

Last date for applications: The last date for application is Feb 22, 2024.

Essential Qualifications:

1. BS-MS/M.Sc. in Mathematics or BS-MS/MTech/ME in Computer Science or related disciplines with an excellent academic record. Outstanding candidates with strong CS backgrounds and having BTech/BE or equivalent degrees in any discipline and MSc in Maths and Statistics are also eligible to apply.
2. Candidates with experience with computer programming and mathematical aspects of public key cryptography will be preferred.

How to Apply: To apply to the position, please fill out the following Google Form

<https://forms.gle/UFgjhMvSxBWLeZdL9>.

Shortlisted candidates will be called for an interview (online/offline). For more details and context, see Dr. Shashank Singh's homepage.