



UNIVERSITETET I BERGEN

**University of  
Bergen**  
Department of  
Informatics

**Jobbnorge ID:** 246889

**Deadline:** 9/15/2023

**Website:** <https://www.uib.no/om/84775/ledige-stillinger-ved-uib>

**Scope:** Fulltime

**Duration:** Fixed Term

## PhD Research Fellow in Informatics - Cryptology (up to 3 positions)

### UiB - Knowledge that shapes society

Through robust and close interaction with the world around us - globally, nationally and locally - we shall be instrumental in building a society based on knowledge, skills and attitudes.

Do you want to take part in shaping the future?

Video: <https://www.youtube.com/watch?v=oYaThmlq6Kg>

### PhD Research Fellow in Informatics - Cryptology (up to 3 positions)

There is a vacancy for up to 3 positions as PhD Research Fellow in Informatics - Cryptology at the [Department of Informatics](#). The positions are for a fixed-term period of 3 years with the possibility of a 4th year with compulsory other work (e.g. teaching duties at the Department). The positions are financed by the University of Bergen.

### About the project/work tasks

All employees are expected to contribute to leading-edge research and teaching of high international quality. All PhD students at the department are members of our [research school in ICT](#), which provides an opportunity to interact with PhD students across the research fields. The school has annual meetings, monthly lunches and offers courses in scientific writing and application writing.

The working environment for this position will be at the Selmer Center in Secure Communication. The Selmer Center is one of the top ICT research groups with main research in areas of sequence design, coding theory, cryptology, Boolean functions, information security, and quantum information theory.

The successful candidates will be supervised by one of the faculty members at the Selmer center, depending on their interests and the nature of the research project.

Potential work tasks related to some of the topics:

- Statistical and algebraic cryptanalysis of modern block and stream ciphers
- Cryptanalysis of lattice-based postquantum cryptography protocols
- Construction of cryptographically optimal functions and related objects
- Design and analysis of symmetric ciphers, cryptographic hash functions and other related primitives
- Design and analysis of error-correcting codes and code-based cryptographic schemes

### Qualifications and personal qualities

- Applicants must hold a master's degree or equivalent education in mathematics, computer science, or a related area, or must have submitted his/her master's thesis for assessment prior to 15.09.2023. It is a condition of employment that the master's degree has been awarded.
- Experience with general-purpose programming languages is a requirement.
- A basic level of knowledge of discrete mathematics, linear algebra and probability theory is a requirement.
- A basic level of knowledge of cryptographic schemes and protocols, error-correcting codes, Boolean functions or another closely related field is a requirement.
- Experience with the C and Magma programming languages is an advantage.
- Experience with cryptography, finite field theory, abstract algebra is an advantage.
- Applicants must be able to work independently and in a structured manner and demonstrate good collaborative skills.
- Applicants must be proficient in both written and oral English.

Personal and relational qualities will be emphasized. Ambitions and potential will also count when evaluating the candidates.

**Special requirements for the position:**

The University of Bergen is subjected to the regulation for export control system. The regulation will be applied in the processing of the applications.

## About the PhD position

### About the PhD Research Fellow

The fellowship will be for a period of 3 years, with the possibility for a 4th year, consisting of 25 % compulsory work (e.g. teaching responsibilities at the department) distributed over the employment period. The 4th year is contingent on the qualifications of the candidate and the teaching needs of the department and will be decided by the head of department upon appointment.

The employment period may be reduced if you have previously been employed in a qualifying post (e.g. research fellow, research assistant).

### About the research training

As a PhD Research Fellow, you must participate in an approved educational programme for a PhD degree within a period of 3 years. The deadline for applying for admission to the PhD programme at The Faculty of Mathematics and Natural Sciences is 2 months after you start your position or after the start of the research project that will lead to the PhD degree. It is a condition that you satisfy [the enrolment requirements for the PhD programme](#) at the University of Bergen.

## We can offer

- a good and professionally stimulating working environment
- salary as PhD research fellow (code 1017) in the state salary scale. This constitutes a gross annual salary of NOK 532 200 (equivalent to pay grade 54). Further increases in salary are made according to length of service in the position.
- enrolment in the Norwegian Public Service Pension Fund
- good [welfare benefits](#)

## Your application must include

- a brief account of the applicant's research interests and motivation for applying for the position
- the names and contact information for two referees. One of these should be the main advisor for the master's thesis or equivalent thesis
- CV
- transcripts and diplomas showing completion of the bachelor's and master's degrees. If you have not yet completed your master's degree, please submit a statement from your institution confirming the expected date of award of your master's degree. Your master's degree must be documented with transcripts and/or diploma, alternatively a confirmation from your institution on completed degree and your grade, by 15.09.2023.
- relevant certificates/references
- approved documentation of proficiency in English (if required, cf. [English language requirements for PhD admission](#))
- a list of any works of a scientific nature (publication list)
- any publications in your name

The application and appendices with certified translations into English or a Scandinavian language must be uploaded at Jobbnorge.

## General information

For further details about the position, please contact associate professor [Nikolay Kaleyski](#), or [Head of Department Inge Jonassen](#).

For HR related questions, contact [Karoline Christiansen](#).

The state labour force shall reflect the diversity of Norwegian society to the greatest extent possible. Age and gender balance among employees is therefore a goal. It is also a goal to recruit people with immigrant backgrounds. People with immigrant backgrounds and people with disabilities are encouraged to apply for the position.

We encourage women to apply. If multiple applicants have approximately equivalent qualifications, the rules pertaining to moderate gender quotas shall apply.

The University of Bergen applies the principle of public access to information when recruiting staff for academic positions.

Information about applicants may be made public even if the applicant has asked not to be named on the list of persons who have applied. The applicant must be notified if the request to be omitted is not met.

For further information about the recruitment process, click [here](#).

## Life as a PhD candidate at UiB

Marion Claireaux tells about life and work as a PhD candidate at UiB.

Video: <https://www.youtube.com/watch?v=nrtP6VxMeJ4&index=2&list=PLf8ZIYfAO0qjhROTj6SthDbSScg0ISO6G>

## About UiB

The University of Bergen is a renowned educational and research institution, organised into seven faculties and approximately 54 institutes and academic centres. Campus is located in the centre of Bergen with university areas at Nygårdshøyden, Haukeland, Marineholmen,

Møllendalsveien and Årstad.

There are seven departments and several centres at Faculty of Mathematics and Natural Sciences. [Read more about the faculty](#) and [departments](#).

## **Additional information**

### **Place of service:**

Institutt for informatikk 5020 Bergen (Bergen Municipality)