# PhD on the topic: Post-quantum cryptography for emerging computing platforms

**The REACT MSCA DN Project:** Self-awareness in humans is an innate capability, arising from the brain's ability to process a multitude of sensory inputs. Emulating this functionality in electronic systems—commonly referred to as neuromorphic computing—holds the potential to create highly intelligent machines capable of supporting a wide range of everyday applications, from autonomous vehicles to smart navigation systems. However, realizing neuromorphic computing in practice presents significant challenges, particularly in the areas of energy efficiency, reliability, and security.

The REACT MSCA Doctoral Network addresses these challenges by developing a neuromorphic platform that is inherently self-aware in terms of energy consumption, secure operation, and system reliability. As part of this initiative, 15 doctoral students/candidates (DS) will be trained through a comprehensive, interdisciplinary program spanning material science, device physics, computer architecture, hardware prototyping, compiler design, simulation and emulation tools, as well as cybersecurity, reliability, and system verifiability.

REACT offers a uniquely structured training environment, combining academic excellence with industrial collaboration. Doctoral students/candidates will benefit from close mentorship by leading researchers and industry experts, while also developing essential skills in scientific writing, research ethics, time management, and entrepreneurship.

By the conclusion of the REACT project, participants will be well-equipped to pursue impactful careers across academia and industry, with the REACT program serving as a strong foundation for their future success.

**Organization:**

ISEC, the Institute of Information Security, is the largest university institute in Austria for research and education in security and privacy. It has been active in this field for more than 30 years and currently employs more than 60 researchers. The institute is part of the Faculty of Computer Science and Biomedical Engineering at Graz University of Technology (TU Graz).

The Cryptographic Engineering research team "CryptEng" is based at ISEC and is supervised by Associate Professor Sujoy Sinha Roy. The goal of 'CryptEng' is to make mathematical concepts of emerging cryptographic algorithms practical and more secure on hardware and software platforms.

A PhD at ISEC typically takes around 4 years. The new PhD student will become a member of the CryptEng group at ISEC. The PhD position is funded by MSCA DN for 36 months and the remaining 12 months will be covered by other funding sources. The candidate is expected to undertake secondment(s) during the first three years of the project. Roadmap to PhD at ISEC is available at https://www.isec.tugraz.at/wp-content/uploads/2025/01/PhD_at_ISEC_20250117.pdf

**Qualification & Eligibility:**

- Mobility Rule: Candidates must not have resided or carried out their main activity in "**host country**" for more than 12 months in the 3 years immediately before the recruitment date.
- PhD Rule: Applicants must not already possess a doctoral degree at the date of recruitment.
- Master degree or equivalent in Electrical Engineering, Computer Science, or related field with excellent grades.
- The ideal candidate for the PhD position will hold a master's degree in Computer/Electronics Engineering or equivalent with project experience in the implementation aspects cryptography (e.g., efficient hardware or software implementation or side-channel analysis or fault analysis, etc.)
- Excellent English communication, presentation, and writing skills.
- Must be a team player.
- Knowledge of computing-in-memory is an added advantage.

**Conditions of employment:**

We offer you in accordance with the Collective Labour Agreement for Austrian Universities:

- A basic salary of € 3.714,80 (salary scale PhD students) gross per month in the first year, up to a maximum of € 4.403,80 gross per month in the fourth and final year, based on a full-time position (14 x per year).
- A temporary position of one year with the option of renewal for another three years; prolongation of the contract is contingent on sufficient progress in the first year to indicate that you will successfully complete your PhD thesis within the next three years. A PhD training programme is part of the agreement.
- Intended start date: November 1, 2025

**Application:**

Please submit the following material, concatenated in a single PDF file and upload this file as your 'CV' by means of the application form at Vacancies – project-react.eu.

- A cover letter motivating your application and detailing the motivation to apply for this specific PhD project (in this case "Post Quantum Cryptography" and around 1 page long).
- An academic CV.
- A research statement (2 pages max) describing your personal research interests and previous research projects.
- A certified list of grades from your undergraduate degree(s) up to the moment of application (in case your MSc degree has not yet been awarded).
- The names and e-mail addresses of 2 academic referees who are willing and able to write recommendation letters for you, including the supervisor of your MSc research project.

You may apply for this position until October 31 11:59pm / before 1st November 2025 Dutch local time (CET) by means of the project website Vacancies – project-react.eu Applications will be evaluated as received.

The overall objective of this doctoral education is neutral to gender, ethnicity, religion, or political beliefs, and the project does not involve any study on them. The activities of this education will benefit all demographic segments in an equal manner. In the context of women's empowerment, the Graz University of Technology has an active plan (https://www.tugraz.at/en/research/research-at-tu-graz/services-fuer-forschende/more-services-for-research#c71049) to ensure gender equality and establish an environment where women have equal access to all university activities.

**For information you can contact:**

- Dr Sujoy Sinha Roy, sujoy.sinharoy@tugraz.at

Please do not use the e-mail address(es) above for applications.