ERC Starting Grants for Maria Eichlseder & Fariba Karimi

Two TU Graz computer scientists have been awarded the prestigious EU funding prize of almost 1.5 million euros each for their research into more efficient encryption systems and the influence of artificial intelligence on discrimination in online social networks.

Philipp Jarke and Falko Schoklitsch

Improvements to keyless encryption and the increasing discrimination and social inequality in online social networks through the use of AI – these are the two research topics with which the top researchers Maria Eichlseder and Fariba Karimi are bringing highly endowed Starting Grants from the European Research Council to Graz University of Technology (TU Graz). The two computer scientists will each receive funding of almost 1.5 million euros over the next five years, the European Research Council announced today.

Of the 494 Starting Grants awarded across the EU, a total of 24 went to researchers from Austrian institutions. This puts Austria in eighth place in Europe. “The two ERC Starting Grants for Maria Eichlseder and Fariba Karimi underline TU Graz’s position as one of Europe’s leading universities in the research fields of IT security, artificial intelligence and data science. The plans in both projects – resource-saving, secure IT systems and fair algorithms – are pioneering,” says Andrea Höglinger, Vice Rector for Research at TU Graz. “I am extremely pleased that two women researchers, Maria Eichlseder and Fariba Karimi, have come out on top in this highly competitive funding programme.”

MARIA EICHLSEDER

Maria Eichlseder’s ERC Starting Grant is the third to be awarded to researchers from the Institute of Applied Information Processing and Communications at TU Graz since 2016. Her project – KEYLESS – deals with encryption, but without the eponymous key. The focus is on the core component of cryptographic systems, the so-called primitive, which is responsible for the security of the entire system. For a long time, it was mainly primitives with keys, so-called block ciphers, that were used and scientifically analysed. In recent years, however, primitives without keys have become very popular, as these components offer a number of advantages. “The latest cryptographic standards, for example for quantum computer-secure or particularly lightweight cryptography, largely use such keyless components internally,” says Maria Eichlseder. “But there is an open problem, namely the precise safety analysis of these components.” There is still a need for research in this area and Maria Eichlseder’s ERC project KEYLESS addresses precisely this. The requirements for keyless components are currently still based on idealised assumptions. These assumptions influence, for example, how often a cryptographic function has to be repeated as part of the encryption process until it is demonstrably secure against attackers. The current solution is a fairly generous number of repetitions to prevent security problems. “That costs resources, of course. If I carry out three times as many rounds as I actually need to protect myself against attacks, then I use three times as much energy. That’s why I want to look at all levels of a cryptographic system, analyse these idealised assumptions and find out whether they can be replaced by more precise assumptions that come closer to reality, “ says Maria Eichlseder.

Fariba Karimi

Oliver Wolf - TU Graz

FARIBA KARIMI: FAIR ALGORITHMS FOR SOCIAL NETWORKS

There is evidence that the use of artificial intelligence in online social networks – for example in recommendations and timelines on platforms such as LinkedIn or Google Scholar – leads to discrimination and increases social inequality. Fariba Karimi from the Institute of Interactive Systems and Data Science wants to get to the bottom of these trends in her project NetFair – Network Fairness and develop methods to analyse and eliminate these new mechanisms of inequality and discrimination.

Social inequality and marginalisation are based on a complex interplay of different social characteristics such as gender, origin and income – the social sciences speak of intersectionality in this context. “So far, there have only been qualitative findings on intersectional inequality in social networks,” says Fariba Karimi. In her ERC project, she wants to make intersectionality quantitatively measurable and then apply it to AI-based online social platforms in order to identify possible biases in their algorithms.

To this end, Fariba Karimi will first develop improved models of social networks and use data analyses and experiments to clarify which factors play a role in the design of the networks and influence each other. “Building on these improved network models, we will investigate their effects on algorithms and online social platforms and analyse the effects over a longer period of time,” says Fariba Karimi. But that is not the end of the story. In her project, Fariba Karimi wants to develop methods that reduce rather than reinforce inequalities and discrimination in online networks. “That’s the big goal: fair algorithms for social networks.” ■

SHORT BIOGRAPHY

Fariba Karimi has been a full professor at the Institute of Interactive Systems and Data Science at TU Graz since October 2023 and also heads the Computational Social Science working group at the Complexity Science Hub in Vienna. Born in Tehran, Iran, in 1981 she studied physics at Shiraz University, Shahid Beheshti University in Tehran and Lund University in Sweden. in 2015, she completed her doctorate in physics and computer science at Umeå University in Sweden and was subsequently a postdoc at the Leibniz Institute for the Social Sciences in Cologne. Her research focuses on computational social sciences, the analysis of networks and algorithms and the modelling of human behaviour. In 2023, she received the Young Scientist Award from the German Physical Society for her research on inequality in complex networks.

SHORT BIOGRAPHY

Maria Eichlseder was born in Graz in February 1988. She was brought up in Steyr and Bavaria before she matriculated in Graz in 2006. This was followed by a bachelor’s degree in computer science and technical mathematics as well as the master’s and doctoral degree in computer science at TU Graz. In 2018, she was one of the first two women at TU Graz to receive her doctorate sub auspiciis praesidentis and is currently assistant professor of cryptography at the Institute of Applied Information Processing and Communications (IAIK) at TU Graz. Her doctoral thesis entitled “Differential cryptanalysis of symmetric primitives” was awarded a State Prize for the Best Doctoral Theses in 2018 by the Federal Ministry of Education, Science and Research and the 2019 Sponsorship Prize for Doctoral Theses of Special Social Relevance by the Technology and Society Forum. One of her greatest research successes to date is the selection of the algorithm ASCON, which she co-developed, as the new standard for lightweight cryptography by the National Institute of Standards and Technology (NIST) in the USA. In addition to her research activities at TU Graz, she was a visiting researcher at Ruhr University Bochum (2020) and Radboud University Nijmegen (2022).