MUNICH AEROSPACE – NEW HORIZONS IN AVIATION AND SPACE

In 2010, through Munich Aerospace and its pooling of research, graduate programmes and teaching, an alliance has been formed between the **Technical University Munich** (TUM), the **Bundeswehr University Munich** (UniBwM), the **German Aerospace Center** (DLR), as well as **Bauhaus Luftfahrt** (BHL).

To promote excellent, scientific young academics, Munich Aerospace awards a PhD scholarship on

Lightweight Code-based Quantum-Resistant Cryptography

The research group **"Multiaccess and Security Coding for Massive IoT Satellite Systems"** is led by Prof. Gerhard Kramer from the Institute for Communications Engineering at the Technical University of Munich (TUM), and involves the COD group of Prof. Antonia Wachter-Zeh at TUM and the ITX group at the Institute of Communications and Navigation at the German Aerospace Center (DLR). The research aims at developing new key technologies for next generation satellite networks for the Internet-of-Things (IoT). Building on an existing research line within Munich Aerospace (where the group devised new advanced techniques for coding and modulation for short packet transmission), the group aims at addressing two fundamental elements of future satellite (and, more generally, wireless) communication systems: the design of uncoordinated multiple access schemes for massive satellite IoT networks, and the construction of lightweight quantum-resistant cryptographic primitives to ensure a long-term secure communication. Relying on a long-lasting and strong collaboration on several research topics, the groups at TUM and DLR will bring together their expertise and tightly collaborate within this activity.

Your tasks and qualifications

The topic addresses the design and analysis of code-based public-key cryptosystems for low-complexity devices (e.g., IoT nodes). Public-key cryptosystems based on the hardness of decoding linear block codes are currently considered to be secure with respect to quantum attacks, whereas cryptosystems based on integer factorization or on the discrete logarithm problem are vulnerable to quantum computers (via Shor's algorithm). The prime example is given by the McEliece cryptosystem, which more than 40 years since its introduction, is still unbroken. Code-based cryptosystems have the additional merit of a reduced complexity of the encryption and the decryption tasks, as compared to "classical" public key cryptosystems such as RSA. The main drawback with respect to RSA is the larger public key size of McEliece-like cryptosystems. An open problem is to find code-based cryptosystems that are capable of resisting classical/quantum attacks while relying on small-size public keys. The work will require the derivation of algebraic properties on linear block codes in both the Hamming and the rank metric. The ideal candidate should have a basic background on coding theory and a good knowledge of linear algebra.

The Institute for Communications Engineering offers an excellent research environment with up to date laboratory equipment to realize your ideas. The group consists of a highly motivated and interdisciplinary team that will support you during your personal and scientific development.

The Scholarship

The Munich Aerospace scholarship amount is 1.575 € per month granted for a minimum of 12 months and limited to a maximum of 3 years. Munich Aerospace scholarship holders are entitled to attend the Munich Aerospace Graduate School, formed by the TUM Graduate School and the DLR_Graduate_Program, and have access to special events and trainings. An additional grant of up to € 6.100 per year will be available to cover expenses that are directly related to the PhD project (e.g. textbooks, laptop, conference travels, public transport, housing subsidy). The scholarship holder is part of a Munich Aerospace research group and receives additional technical support from the research group head. The candidates receive their PHD from TUM or UniBwM.

Interested?

Please send us your application including relevant documents (cover letter, CV, diplomas, transcript of records) in PDF format to antonia.wachter-zeh@tum.de. The application deadline is April 14, 2021.

We are looking forward to your application!

Technical University of Munich

DLR Deutsches Zentrum für Luft- und Raumfahrt German Aerospace Center