universität innsbruck
Institut für Informatik

Vorträge im Rahmen des Besetzungsverfahrens der Laufbahnstelle „Kryptographie“

Donnerstag 05. August 2021, 08:45 Uhr

Dr. Kakvi Saquib (Universität Wuppertal)

Lehrevortrag „Introduction to Asymmetric Cryptography“ (15 Minuten) und anschließend der Forschungsvortrag mit dem Titel:

Cryptography: Securing the Present and the Future

Abstract:

In this modern day age, more and more of our communication is becoming digital, bringing privacy and security issues into sharper focus. One key tool in preserving both security and privacy is cryptography. In this talk, I will present selected research results which show how cryptography secures our present, while also setting up a secure future. In the first part of my presentation, I will recap selected research results which have shown the security of cryptographic primitives that are currently in use in our day-to-day lives.
Specifically, I will talk about a series of results which concern standardised signatures built using RSA. In the second part of my presentation, I will briefly sketch current research work for new primitives that will provide us with secure communication in the future.

Donnerstag 05. August 2021, 11:00 Uhr

Dr. Paul Rösler (TU Darmstadt)

Lehrevortrag „Introduction to Asymmetric Cryptography“ (15 Minuten) und anschließend der Forschungsvortrag mit dem Titel:

From Natural to Practical Security Definitions, Automatically

Abstract:

Cryptographic analyses often begin with selecting an appropriate definition of security. Established ways for finding such a notion comprise (1) using human intuition, (2) capturing the guarantees that one particular protocol achieves, or (3) defining security as strong as theoretically possible. In contrast to the former two, the latter approach is considered natural and systematic. However, optimally strong security often entails impractical, undesired performance limits for protocols that fulfill the requirements of such a definition. This gap between ambiguous definition styles on the one side and impractically strong requirements on the other side exposes the goal of my work:
finding a practical yet systematic definition methodology.

In this talk, I will present a new, natural and systematic way to define security sub-optimally strong. For this, I first clarify the crucial role of syntax notions in cryptography. I then reveal the counter-intuitive nature of current concepts for deriving optimally strong security definitions from such syntax notions. Finally, I sketch how my new methodology can automatize as of yet error-prone, manual work in this process. With this research project, I make an important step towards an unambiguous methodology with which practically useful security definitions can be obtained. As a result, I build a methodical foundation for future analyses of cryptography in the real-world.

Donnerstag 05. August 2021, 15:00 Uhr

Christian Weinert (TU Darmstadt)

Lehrevortrag „Introduction to Asymmetric Cryptography“ (15 Minuten) und anschließend der Forschungsvortrag mit dem Titel:

Efficient Cryptographic Protocols for Privacy-Preserving Applications

Abstract:

Cryptographic protocols from the area of secure computation are powerful tools that allow for privacy-preserving evaluation of arbitrary computable functions. Unfortunately, existing generic protocol designs and implementations incur an impractical computation and/or communication overhead when applied to real-world problem sizes and deployment scenarios.

In this talk, I will present efficient cryptographic protocols for applications such as privacy-preserving machine learning and mobile private contact discovery. Additionally, I will discuss open challenges towards the omnipresent deployment of cryptographic protocols for privacy-preserving applications.

Ort der Vorträge: Großer Hörsaal – Technische Fakultät, Technikerstraße 13b

!!! Für den Besuch der Vorträge im Großen Hörsaal ist 3G Nachweis notwendig.
Zutritt nur mit Nachweis über Impfung/Genesung oder Vorlage eines Covid-Tests !!!