

Verleihung des Heinz Maier-Leibnitz-Preises 2023



Laudatio auf den Preisträger Dr. Giulio Malavolta

16. Oktober 2023

Es gilt das gesprochene Wort!

Deutsche Forschungsgemeinschaft

Kennedyallee 40 · 53175 Bonn · Postanschrift: 53170 Bonn

Telefon: + 49 228 885-1 · Telefax: + 49 228 885-2777 · postmaster@dfg.de · www.dfg.de



Sicherheit und Privatheit sind grundlegende Bürgerrechte in demokratische Gesellschaften und daher auch zentrale Anforderungen an moderne IT-Systeme. Datenschutz, Anonymität und Pseudonymität, Vertrauen und Reputation sowie deren benutzungsfreundliche Umsetzung in Computern und Netzwerken sind bedeutende Aspekte moderner Informatikforschung.

Der diesjährige Heinz Maier-Leibnitz-Preisträger Giulio Malavolta hat im Gebiet der Kryptographie hierzu in außergewöhnlicher Breite und Tiefe beigetragen, wobei er sich insbesondere mit dem Schutz von Berechnung statt (nur) mit dem Schutz statischer Daten beschäftigt. Er widmet sich in seinen Arbeiten drei der aktuellsten, technisch anspruchsvollsten und dynamischsten Gebiete der Kryptographie. Dies sind zum einen Privatheit-wahrende Techniken wie Zero-Knowledge- und nicht interaktive Beweise sowie Multi-Party-Berechnungen, die auch bei Block Chains und Kryptowährungen zum Einsatz kommen. Zum anderen hat er voll-homomorphe Verschlüsselungsverfahren entwickelt. Diese ermöglichen es, mit hoher Effizienz Funktionen auf verschlüsselten Daten zu berechnen, wodurch aufwändige Berechnungen auch an nicht vertrauenswürdige Dienstleister übertragen werden können. Schließlich forscht Herr Malavolta an kryptographischen Verfahren wie Verschlüsselung und digitalen Signaturen, die auch Angriffen mit Quantencomputern widerstehen. In verschiedenen Arbeiten hat er neue und originelle Techniken für die Konstruktion oder die Sicherheitsbeweise sogenannter postquantensicherer Verfahren entwickelt. Dass er in all diesen Bereichen nicht nur theoretisch fundierte Beiträge liefert, sondern auch die Brücke zur praktischen Anwendung schlägt, hebt ihn besonders hervor. So hat er kürzlich ein erstes effizientes registration-based Encryption-Verfahren vorgestellt, das die sonst aufwändigen Vertraulichkeitsanforderungen an die Public-Key-Infrastruktur minimiert.

Herr Malavolta konnte seine Forschungsergebnisse in exzellenter Qualität und Quantität sowohl auf den angesehensten Konferenzen der Kryptographie als auch in den kompetitivsten Konferenzen im allgemeineren Gebiet der Sicherheit und Privatheit vorstellen. Viele seiner Artikel haben das Gebiet der Kryptographie bereits jetzt nachhaltig beeinflusst und Herr Malavolta zählt international zu den herausragenden jüngeren Forscher*innen in der IT-Sicherheit.

Schon der Lebenslauf von Giulio Malavolta zeigt eine hohe Leistungsbereitschaft und ein großes Maß an Internationalität. Nach einem Studium der Bioinformatik an der Universität Bologna wurde er 2019 an der Friedrich-Alexander-Universität Erlangen-Nürnberg mit Auszeichnung in Informatik promoviert. Seine Dissertation zu „Cryptographic Clocks and Applications“ wurde mit dem Promotionspreis der Staedtler-Stiftung ausgezeichnet. Nach Postdoc-Aufenthalt an der Carnegie Mellon University, am Simons Institute for the Theory of Computing und an der University of California, Berkeley wurde er 2020 Gruppenleiter mit Tenure-Track am Max-Planck-Institut für Sicherheit und Privatsphäre in Bochum. An der Ruhr-Universität Bochum lehrt er an der Fakultät Informatik und ist im Exzellenzcluster „Cyber Security in the Age of Large-Scale Adversaries“ (CASA) als co-PI eingebunden. Darüber hinaus hat Herr Malavolta bereits auch erfolgreich Drittmittel aus der Industrie und vom BMBF sowie einen Starting Grant der European Research Commission eingeworben.

Im Jahr 2023 kommt nun der Heinz Maier-Leibnitz-Preis hinzu – als Würdigung der bisherigen herausragenden wissenschaftlichen Leistungen von Dr. Giulio Malavolta und als weiterer Ansporn für eine erfolgreiche akademische Zukunft.

Wir gratulieren sehr herzlich und wünschen weiterhin viel Erfolg bei der Forschung!