Verleihung des
Gottfried Wilhelm-Leibniz-Preises 2024

Laudatio auf den Preisträger
Prof. Dr. Eike Kiltz

13. März 2024

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

Wir vertrauen unsere berufliche und private Kommunikation im Internet digitalen Verschlüsselungstechniken an, die auf der Primfaktorzerlegung großer Zahlen oder auf der Berechnung diskreter Logarithmen beruhen. Skalierbare Quantencomputer aber könnten diese in kürzester Zeit entschlüsseln, sodass einst und aktuell über verschlüsselte Kanäle übertragene Daten plötzlich einsehbar würden. Eike Kiltz hat mit seiner bahnbrechenden Forschung den Weg zu innovativen, quantensicheren Verschlüsselungsverfahren geebnet und neue Standards auf dem Gebiet der Post-Quanten-Kryptographie gesetzt.

Er leistete Pionierarbeit bei der Entwicklung effizienter Public-Key-Kryptographie-Verfahren und der Beweisführung ihrer Angriffssicherheit. Mit der Entwicklung eines neuartigen Verschlüsselungssystems, dessen Sicherheitsniveau nachweislich äquivalent zum Faktorisierungsproblem ist, löste er bereits früh in seiner Karriere ein über zwanzig Jahre bestehendes Forschungsproblem der Kryptographie.

Als Koryphäe seines Fachs etablierte er sich schließlich mit seiner wegweisenden Entwicklung gitterbasierter Algorithmen als Grundlage quantensicherer Kryptographie-Systeme. Zudem entwickelte er innovative Techniken zur Schlüsseldelegation für Gitter, die kryptographischen Protokollen eine vielfältigere Funktionalität ermöglichen. Seine Ergebnisse bilden heute den Kern zahlreicher zeitgemäßer quantenresistenter Verschlüsselungsmethoden und ein von ihm entwickelter Beweis dient weltweit als Basis für den Sicherheitsnachweis neu entwickelter kryptographischer Verfahren.

Eike Kiltz verwebt nicht nur Theorie und Praxis auf virtuose Weise, sondern prägt auch die laufende internationale Standardisierung. Zusammen mit seinem Team hat er maßgeblich an der Entwicklung zweier hocheffizienter gitterbasierter kryptographischer Verfahren mitgewirkt – eines für die Verschlüsselung und eines für die Authentifizierung. Beide Algorithmen wurden jüngst zum neuen internationalen Standard quantensicherer Kryptographie erhoben, der die künftige digitale Sicherheit unserer Gesellschaft wesentlich prägen wird.

Lieber Herr Kiltz, Ihre Forschung erschließt Mittel und Wege, wie wir unser digitales Handeln auch im Zeitalter der Quantencomputer sicher gestalten können. Ich freue mich außerordentlich, Ihnen für Ihre hervorragenden Leistungen den Leibniz-Preis zu überreichen. Herzlichen Glückwunsch!