Kryptographie: ERC Consolidator Grant für KIT-Forscher

Dennis Hofheinz entwickelt Kryptographie für das digitale Zeitalter – mehr Sicherheit für Cloud und Big Data – Europäischer Forschungsrat fördert ihn nun mit rund zwei Millionen Euro

Monika Landgraf
Pressesprecherin

Kaiserstraße 12
76131 Karlsruhe
Tel.: +49 721 608-47414
Fax: +49 721 608-43658
E-Mail: presse@kit.edu

Weiterer Kontakt:

Kosta Schinarakis
PKM – Themenscout
Tel.: +49 721 608 41956
Fax: +49 721 608 43658
E-Mail: schinarakis@kit.edu

Der Kryptologe Dennis Hofheinz erhält dieses Jahr einen ERC Consolidator Grant. (Foto: KIT)

Im digitalen Zeitalter steigen die Anforderungen an die Kryptographie. Cloud Computing und Big Data verlangen nach Lösungen, die nicht nur sicher, sondern auch praktikabel sind. Im Rahmen des Projektes „PREP-CRYPTO: Preparing Cryptography for Modern Applications“ entwickelt Dennis Hofheinz vom Karlsruher Institut für Technologie (KIT) neue Systeme, die bewährte Methoden der Kryptographie mit neuen Bausteinen verknüpfen. Der Europäische Forschungsrat (European Research Council, ERC) fördert dieses Projekt in den nächsten fünf Jahren mit rund zwei Millionen Euro.

„Kryptographie ist in Zeiten von Cloud und Big Data weit mehr als sichere Kommunikation“, erklärt Hofheinz. Ging es früher darum, verschlüsselte Nachrichten zu versenden, ist die Herausforderung heute abgestimmte Zugriffsrechte und Bearbeitungsmöglichkeiten auf Daten zu ermöglichen und gleichzeitig die Datensicherheit sicherzustellen. Dienstleistern – zum Beispiel ausgelagerten Rechenzentren – könnte es so ermöglicht werden, auf der Basis sensibler, verschlüsselter Daten von Unternehmen oder Privatpersonen, Berechnungen

und Verarbeitungen anzustellen, ohne diese Daten vorher zu entschlüsseln und so den Datenschutz zu gewährleisten.

Für diese komplexen Szenarien sind in den letzten Jahren verschiedene neue Kryptographie-Bausteine entwickelt worden, zum Beispiel die sogenannte Fully Homomorphic Encryption-Methode (FHE). Sie ermöglicht es, Daten weiter zu verarbeiten, ohne dass ihr Inhalt an irgendeiner Stelle im Prozess entschlüsselt werden muss. Auf diesem Wege könnten beispielsweise Gesundheitsdaten für statistische Auswertungen genutzt werden, ohne dass Dritte Einblick in die Informationen zu den einzelnen betreffenden Patienten bekommen.

„Konzepte wie FHE haben die Tür für Anwendungen geöffnet, die bislang undenkbar waren“, betont Hofheinz. „Aber sie sind bei weitem noch nicht effizient genug für praktische Anwendungen“. Daten mit dieser Methode zu verschlüsseln und sie auszulagern lohne sich derzeit nicht, weil der Aufwand millionenfach höher sei als die Berechnungen im eigenen Haus durchzuführen. Um die Potenziale neuer Kryptographie-Methoden voll auszuschöpfen, sieht der KIT-Experte zwei mögliche technische Hebel, die er mit seinem Forschungsteam weiter entwickeln will: zum einen Szenarien, die klassische algebraische Instrumente und Techniken der Kryptographie mit neuen Methoden kombinieren, zum anderen eng umgrenzte Lösungen für domänenspezifische Anwendungen. Mit dem ERC Consolidator Grant erhält er jetzt für sein Forschungsvorhaben eine der prominentesten Förderungen in Europa.

Dennis Hofheinz ist seit 2015 Professor in der Arbeitsgruppe Kryptographie und Sicherheit des KIT. Nach seinem Informatikstudium an der damaligen Universität Karlsruhe (TH), dem heutigen KIT, das er mit einer Diplomarbeit zum Thema „Ein Seitenkanalangriff auf das Signaturschema QUARZ“ abschloss, begann Hofheinz seine wissenschaftliche Karriere als Doktorand am Institut für Algorithmen und Kognitive Systeme (IAKS) der TH. Dort wurde er 2005 mit einer Arbeit zum Thema „Zur Analyse und Struktur von Sicherheitsbegriffen“ promoviert. Anschließend arbeitete er vier Jahre als Postdoktorand am Centrum Wiskunde en Informatica (CWI) in Amsterdam. 2009 kehrte er als Juniorprofessor ans KIT zurück. Im diesem Jahr gewann er auch den Fakultätslehrpreis des KIT für herausragende Lehre. Mehr dazu in einem Video (ab Min. 4:35) unter http://www.kit.edu/foerdern/19689.php

Informationen zum Consolidator Grant 2016:

Insgesamt hat der ERC in der aktuellen Ausschreibungsrunde 314 Wissenschaftler mit einem Consolidator Grant ausgezeichnet, die

aus 2.274 Forschungsanträgen ausgewählt wurden, was einer Bewilligungsquote von 13,8 Prozent entspricht. Es werden insgesamt rund 605 Millionen Euro aus dem Forschungsrahmenprogramm Horizon 2020 ausgeschüttet. Mit ERC Consolidator Grants fördert der Europäische Forschungsrat (European Research Council, ERC) Projekte exzellenter Wissenschaftler, deren Promotion zwischen sieben und zwölf Jahre zurückliegt. Der ERC wurde 2007 als Institution zur Finanzierung grundlagenorientierter Pionierforschung in Europa gegründet.

Das Karlsruher Institut für Technologie (KIT) verbindet seine drei Kernaufgaben Forschung, Lehre und Innovation zu einer Mission. Mit rund 9 300 Mitarbeiterinnen und Mitarbeitern sowie 25 000 Studierenden ist das KIT eine der großen natur- und ingenieurwissenschaftlichen Forschungs- und Lehreinrichtungen Europas.

KIT – Die Forschungsuniversität in der Helmholtz-Gemeinschaft

Das KIT ist seit 2010 als familiengerechte Hochschule zertifiziert.

Diese Presseinformation ist im Internet abrufbar unter: www.kit.edu

Das Foto steht in druckfähiger Qualität auf www.kit.edu zum Download bereit und kann angefordert werden unter: presse@kit.edu oder +49 721 608-47414. Die Verwendung des Bildes ist ausschließlich in dem oben genannten Zusammenhang gestattet.