Cryptography: ERC Consolidator Grant for KIT Researcher

Dennis Hofheinz Develops Cryptography for the Digital Era – Enhanced Security of Cloud Computing and Big Data – European Research Council Grants Funding of About EUR 2 Million

Monika Landgraf
Chief Press Officer

Kaiserstraße 12
76131 Karlsruhe, Germany
Phone: +49 721 608-47414
Fax: +49 721 608-43658
Email: presse@kit.edu

Cryptologist Dennis Hofheinz is awarded an ERC Consolidator Grant this year. (Photo: KIT)

For further information, please contact:

Kosta Schinarakis
PKM – Science Scout
Phone: +49 721 608 41956
Fax: +49 721 608 43658
Email: schinarakis@kit.edu

In the digital era, requirements on cryptography increase. Cloud computing and big data require solutions that are not only secure, but also practicable. Under the project "PREP-CRYPTO: Preparing Cryptography for Modern Applications," Dennis Hofheinz of Karlsruhe Institute of Technology (KIT) develops new systems combining established cryptography methods with new elements. The European Research Council (ERC) will fund this project with about EUR 2 million in the next five years.

"In times of cloud computing and big data, cryptography is far more than secure communication," Hofheinz explains. While past work focused on sending encrypted messages, the challenge today is to provide agreed access rights to and processing options of data while ensuring data security. In this way, providers, such as outsourced computing centers, may be enabled to make calculations and carry out data processing based on sensitive, encoded data of companies or private persons without having to decode these data before. Thus, data security is ensured.

In the past years, various new cryptography elements were developed for these complex scenarios. An example is the so-called fully homomorphic encryption method (FHE). By means of this method, data can be further processed without their contents having to be decoded at any point in the process. For example, health data may be used for statistic evaluations without third parties gaining insight into the information on the individual patient.

“Concepts like FHE have opened the door for applications that were infeasible so far,” Hofheinz says. “But they are far from being efficient enough for practical applications.” The KIT expert thinks that encoding data with this method and archiving them externally is not worthwhile at the moment, because the expenditure is a million times higher than making calculations in house. To fully exploit the potentials of new cryptography methods, he wants to further develop two technical approaches with his team: Combinations of classical algebraic instruments and cryptography techniques with new methods and defined solutions for domain-specific applications. With the ERC Consolidator Grant, he now receives highly renowned European funding for his research project.

Since 2015, Dennis Hofheinz has been professor in the Cryptography and Security Group of KIT. Hofheinz completed his studies of informatics at then Universität Karlsruhe (TH), today’s KIT, by a diploma thesis on “Ein Seitenkanalangriff auf das Signaturschema QUARTZ” (A Side-channel Attack on the QUARTZ Signature Scheme). Then, he started his scientific career as a doctoral student at the Institute for Algorithms and Cognitive Systems (IAKS) of the TH. In 2005, he was conferred his doctorate for his thesis entitled “Zur Analyse und Struktur von Sicherheitsbegriffen” (On the Analysis and Structure of Security Notions). Then, he spent four years as post-doc at the Centrum Wiskunde en Informatica (CWI) in Amsterdam. In 2009, he returned to KIT as Junior Professor.

Information on the 2016 Consolidator Grant:

In the recent round, the ERC granted the Consolidator Grant to a total of 314 scientists selected from 2274 proposals, which corresponds to an approval rate of 13.8 percent. The total amount of funding financed from the Horizon 2020 research framework programme is about EUR 605 million. The European Research Council awards ERC Consolidator Grants to fund projects of excellent scientists who were conferred their doctorates between seven and twelve years ago. In 2007, the ERC was established as an institution to fund fundamental pioneer research in Europe.

Karlsruhe Institute of Technology (KIT) pools its three core tasks of research, higher education, and innovation in a mission. With about 9,300 employees and 25,000 students, KIT is one of the big institutions of research and higher education in natural sciences and engineering in Europe.

KIT – The Research University in the Helmholtz Association

Since 2010, the KIT has been certified as a family-friendly university.

This press release is available on the internet at www.kit.edu.

The photo of printing quality may be downloaded under www.kit.edu or requested by mail to presse@kit.edu or phone +49 721 608-4 7414. The photo may be used in the context given above exclusively.