[Prof. Dr. Bernhard Beckert // **Anwendungsorientierte formale Verifikation**]

Bernhard Beckert leitet die Forschungsgruppe „Anwendungsorientierte formale Verifikation" am KASTEL – Institut für Informationssicherheit und Verlässlichkeit des KIT und ist Dekan der KIT-Fakultät für Informatik. Er ist einer der Principal Investigators des Kompetenzzentrums für Angewandte Sicherheitstechnologie KASTEL, Mitglied des KIT-Zentrums „Information · Systeme · Technologien" (KCIST) und zudem Direktor am FZI Forschungszentrum Informatik.

Er studierte von 1987 bis 1993 Informatik an der Universität Karlsruhe (TH), dem heutigen Karlsruher Institut für Technologie (KIT), und promovierte dort 1998 mit einer Arbeit über automatische Deduktion. Von 2003 bis 2009 war er zunächst Juniorprofessor für Künstliche Intelligenz und dann Universitätsprofessor für Formale Methoden und Künstliche Intelligenz an der Universität Koblenz-Landau. Seit 2009 ist er Professor am Institut für Theoretische Informatik (ITI), seit 2021 am Institut für Informationssicherheit und Verlässlichkeit (KASTEL) des KIT.

Beckert publizierte international über 170 Artikel. Von 2008 bis 2012 war er Chair der European COST Action on Formal Verification of Object-oriented Software.

Zudem ist er Vertrauensdozent der Studienstiftung des deutschen Volkes.

// Überblick und Allgemeines

Forschungsgebiet der Professur ist die Anwendung formaler, logikbasierter Methoden zur Spezifikation, Verifikation und Analyse von Software. Das Ziel ist, die Verlässlichkeit und Sicherheit kritischer Systeme zu erhöhen.

Die Forschung folgt dem Grundgedanken anwendungsorientierter theoretischer Informatik. Sie reicht von den theoretischen Grundlagen über die Entwicklung neuer formaler Methoden für funktionale Korrektheit und IT-Sicherheit bis zu deren Erschließung für die Praxis und der Entwicklung von Verifikationswerkzeugen.

Eine wesentliche Gemeinsamkeit der entwickelten Methoden ist, dass sie auf der Quellcodeebene ansetzen, also die Software selbst statt eines abstrakten Modells verifizieren. Aushängeschild ist dabei das „KeY-System" zur Verifikation von Java-Programmen, ein langjähriges gemeinsames Projekt mit Partnern an der TU Darmstadt und der Chalmers University in Göteborg.

Zu den betrachteten Praxisszenarien gehören Anwendungen wie objektorientierte Software, Software zur Steuerung cyber-physikalischer Systeme, Wahlverfahren und -systeme, Quantensoftware und Blockchain-basierte Smart Contracts.

Die Professur koordiniert den Lehramtsstudiengang Informatik, betreibt das Lehr-Lern-Labor Informatik und betreut die Veranstaltung „Teamprojekt Lehramt Informatik". An der Lehre beteiligt sie sich auch mit den Vorlesungen „Formale Systeme I/II" und hat mit dem Lehrkonzept „Praxis der Forschung" einen Schwer-

punkt in der Stärkung forschungsorientierter und interdisziplinärer Lehre.

// Ergebnisse und Erfolge

Mit dem Ziel, die Skalierbarkeit und Benutzbarkeit deduktiver Verifikation zu verbessern, wurden Möglichkeiten entwickelt, diese mit Typprüfern und Bounded Model Checking zu kombinieren, sowie die Korrektheit eines nur teilweise verifizierten Programms probabilistisch zu bemessen.

Als neues Anwendungsgebiet für deduktive Verifikation wurden Blockchain-basierte Smart Contracts erschlossen und Methoden entwickelt, um deren Sicherheit zu erhöhen. Dazu zählen eine Spezifikationssprache für Frame-Bedingungen und Methoden für beweisbar korrekte Zugriffskontrolle.

Außerdem wurde ein kompositionales Verfahren entwickelt, das automatisch bewiesen faire Wahlauszählverfahren mit formal korrekter Software generiert. Ein weiteres Verfahren generiert automatisch minimale Spielkarten-basierte kryptografische Protokolle zur sicheren Mehrparteienberechnung.

Als weiteres Anwendungsgebiet wurde Quantensoftware erschlossen. Da diese inhärent schwer zu testen und zu debuggen ist, bietet es sich an, ihre Korrektheit formal zu beweisen. Hierzu wurde im Rahmen des Kompetenzzentrums Quantencomputing Baden-Württemberg ein Ansatz zur vollautomatischen Fehlersuche entwickelt.

// Ausgewählte Publikationen

Beckert, B., J. Budurushi, A. Grunwald, R. Krimmer, O. Kulyk, R. Küsters, A. Mayer, J. Müller-Quade, S. Neumann und M. Volkamer. Aktuelle Entwicklungen im Kontext von Online-Wahlen und digitalen Abstimmungen. Techn. Ber. 46.23.01; LK 01. 2021.

Beckert, B., M. Herda, M. Kirsten und S. Tyszberowicz. Integration of Static and Dynamic Analysis Techniques for Checking Noninterference. In: Deductive Software Verification: Future Perspectives. Springer, LNCS 12345, 2020.

de Boer, M., S. de Gouw, J. Klamroth, C. Jung, M. Ulbrich und A. Weigl. Formal Specification and Verification of JDK's Identity Hash Map Implementation. In: iFM, 17th Int. Conf. Springer, LNCS 13274, 2022. Best Paper Award.

Koch, A., M. Schrempp und M. Kirsten. Card-Based Cryptography Meets Formal Verification. In: New Gener. Comput. 39.1: Spec. Issue on Card-Based Cryptography, 2021.

Krämer, J., L. Blatter, E. Darulova und M. Ulbrich. Inferring Interval-Valued Floating-Point Preconditions. In: TACAS, 28th Int. Conf. Springer, LNCS 13243, 2022.

Lanzinger, F., A. Weigl, M. Ulbrich und W. Dietl. Scalability and Precision by Combining Expressive Type Systems and Deductive Verification. In: PACMPL 5. OOPSLA, 2021.

Schiffl, J., M. Grundmann, M. Leinweber, O. Stengele, S. Friebe und B. Beckert. Towards Correct Smart Contracts: A Case Study on Formal Verification of Access Control. In: SACMAT, 26th ACM Symp., 2021.

Standl, B., A. Bentz, M. Ulbrich, A. Vielsack und I. Wagner. Design- and Evaluation-Concept for Teaching and Learning Laboratories in Informatics Teacher Education. In: ISSEP, 13th Int. Conf. Springer, LNCS 12518, 2020.

// Mitarbeiterinnen und Mitarbeiter

Verwaltungspersonal
Simone Meinhart

Wissenschaftliches Personal
Dr. Lionel Blatter
Dr. Michael Kirsten
Jonas Klamroth
Florian Lanzinger
Wolfram Pfeifer
Jonas Schiffl
Samuel Teuber
Dr. Mattias Ulbrich
Annika Vielsack
Dr. Alexander Weigl

Technisches Personal
Ralf Kölmel

// Website

formal.kastel.kit.edu