[Prof. Dr. Jörn Müller-Quade // **Kryptographie und Sicherheit**]

Nach dem Studium der Informatik in Erlangen und Karlsruhe promovierte Jörn Müller-Quade 1998 an der Universität Karlsruhe (TH) im Bereich Computeralgebra und arbeitete von 1999 bis 2001 als Postdoc am Imai-Laboratory der Universität von Tokyo. In den Jahren 2001 bis 2003 leitete er den Karlsruher Teil des BMBF-Verbundprojekts Quantenkryptographie. Als Emmy Noether-Nachwuchsgruppenleiter erforschte er 2003 bis 2008 langfristig sichere Kryptographie.

In den Jahren 2008 und 2014 wurde Jörn Müller-Quade und seiner Arbeitsgruppe der Deutsche IT-Sicherheitspreis für das Wahlverfahren „Bingo Voting“ und das Softwareschutz-Verfahren „Blurry Box“ verliehen. Er wurde 2008 als Experte vom Bundesverfassungsgericht zu Wahlmaschinen angehört. Jörn Müller-Quade trat 2009 die Professur für Kryptographie und Sicherheit am Karlsruher Institut für Technologie (KIT) an und ist seit 2010 ein Direktor am FZI Forschungszentrum Informatik. Im Jahr 2011 initiierte er das Kompetenzzentrum KASTEL, das 2020 über die Helmholtzgemeinschaft verstetigt wurde. Bei der nationalen Akademie für Technikwissenschaften acatech fungiert er seit 2017 als Sprecher des Themennetzwerks Sicherheit und seit 2018 als Gruppenleiter in der Plattform Lernende Systeme.

Im Dialog mit der Öffentlichkeit über Kryptographie veröffentlichte Jörn Müller-Quade u. a. Werke im Zentrum für Kunst und Medientechnlogie (ZKM) in den Ausstellungen „Future Cinema“, „Lichtkunst aus Kunstlicht“, „Global Control and Censorship“ und „Open Codes“.

// Überblick und Allgemeines

In der Kryptographie und IT-Sicherheit schützt man Systeme vor einem intelligenten Angreifer. Sich lediglich gegen bekannte Angriffe abzusichern, führt nur zu einer kurzfristigen Sicherheit, bis neue Angriffe gefunden werden. Wir folgen daher dem Paradigma der beweisbaren Sicherheit: Mathematische Beweise zeigen, dass in einem Modell der Wirklichkeit unter explizit gegebenen Annahmen die klar definierten Sicherheitsziele nicht verletzt werden können. Werden dennoch Angriffe bekannt, so waren das zugrundeliegende Modell oder die verwendeten Annahmen nicht realistisch genug. Mit diesem Erkenntnisgewinn können nun das Modell verbessert oder einige Annahmen verworfen werden.

Ein Ziel unserer Forschung ist es, Protokolle für verteilte Berechnungen auf geheimen Daten zu entwickeln. Verfahren zur sicheren Mehrparteienberechnung (MPC) erlauben es z. B., Statistiken über sensible Daten zu berechnen, ohne die einzelnen Daten zu erfahren.
Es ist aber nicht ausreichend, einzelne Bausteine nur für sich genommen zu betrachten. Sicherheitslücken können sich auch aus dem Zusammenwirken von Komponenten eines Systems ergeben. Das „Universal Composability“-Framework (UC) ist ein Sicherheitsmodell, das speziell entwickelt wurde, um eine modulare Herangehensweise zu ermöglichen: Sind einzelne Komponenten als sicher bewiesen, dann bleibt die Sicherheit bewiesenermaßen auch beim Zusammenspiel der Komponenten erhalten.

// Projekte und Erfolge

Um den starken Begriff der UC-Sicherheit zu erreichen, sind Voraussetzungen notwendig, die oft nicht garantiert werden können. Wir konnten unter der erstmaligen Verwendung von „timed assumptions" einen UC-ähnlichen Sicherheitsbegriff entwickeln, der im betrachteten Setting bisher nicht erreichte wichtige Eigenschaften hat (TCC 2021).
Im Umfeld der sicheren Mehrparteienberechnungen haben wir auf der PETS 2021 einen Sicherheitsbegriff und ein Protokoll veröffentlicht, das erstmals die Vertraulichkeit und Integrität von Geheimnissen ehrlicher Parteien schützt, selbst wenn diese während der Protokollausführung korrumpiert werden.
Dies konnte mithilfe von „unhackbaren" Hardwarebausteinen wie z. B. Datendioden oder Schaltern erreicht werden.
Mit MPC oder vertrauenswürdiger Hardware können auf sensiblen Daten sichere Berechnungen durchgeführt werden.
Wir haben eine generische Methode für eine privatsphäre-schützende Datenanalyse entwickelt und diese zur Erkennung von Betrug im digitalen Zahlungsverkehr verwendet (PETS 2022).

Der Aspekt der langfristigen Sicherheit gewinnt immer mehr Bedeutung, u. a. durch mögliche Angriffe mit zukünftigen Quantencomputern. Im BMBF-Projekt PQC4MED werden Lösungen zur langfristigen Sicherheit von eingebetteten Systemen in der Medizintechnik erarbeitet. Ein Fokus liegt auf der Modellierung von atomaren Updates der einzelnen Komponenten auf quanten-resistente Kryptographie. Mit Hilfe von post-quanten-sicheren Verschlüsselungsverfahren haben wir eine effiziente Konstruktion eines neuen beweisbaren Sicherheitsbegriffs für kryptographische Authentifikation gefunden (PKC 2022).

Im BMBF-Projekt VE-ASCOT sind wir dabei eine „Chain of Trust" Plattform zu entwickeln, die eine vertrauenswürdige Produktionskette und eine sichere Inbetriebnahme von Halbleiterkomponenten ermöglicht.

Gemeinsam mit SAP SR entwickeln wir im Projekt „Secure Federated Machine Learning" ein Protokoll, mit dem ein neuronales Netz so auf Trainingsdaten mehrerer Parteien trainiert werden kann, dass die Daten jeder Partei vor den anderen Parteien geheim bleiben.

// Ausgewählte Publikationen

W. Beskorovajnov, F. Dörre, G. Hartung, A. Koch, J. Müller-Quade, T. Strufe: ConTra Corona: Contact Tracing against the Coronavirus by Bridging the Centralized–Decentralized Divide for Stronger Privacy. ASIACRYPT 2021, Ed.: M. Tibouchi, Vol. 2, 665–695, Springer Verlag.

W. Beskorovajnov, R. Gröll, J. Müller-Quade, A. Ottenhues, R. Schwerdt: A New Security Notion for PKC in the Standard Model: Weaker, Simpler, and Still Realizing Secure Channels. PKC 2022, Ed.: G. Hanaoka. Vol. 2, 316–344, Springer Verlag.

B. Broadnax, A. Koch, J. Mechler, T. Müller, J. Müller-Quade, M. Nagel: Fortified Multi-Party Computation: Taking Advantage of Simple Secure Hardware Modules. PETS 2021 (4), 312–338.

B. Broadnax, J. Mechler, J. Müller-Quade: Environmentally Friendly Composable Multi-party Computation in the Plain Model from Standard (Timed) Assumptions. TCC 2021, Ed.: K. Nissim, Vol. 1, 750–781, Springer Verlag.

V. Fetzer, M. Keller, S. Maier, M. Raiber, A. Rupp, R. Schwerdt: PUBA: Privacy-Preserving User-Data Bookkeeping and Analytics. PETS 2022 (2), 447–516.

// Mitarbeiterinnen und Mitarbeiter

Verwaltungspersonal
Carmen Manietta

Wissenschaftliches Personal
Dr. Thomas Agrikola
Saskia Bayreuther
Laurin Benz
Robin Marius Berger
Felix Dörre
Valerie Fetzer
Clemens Friedrich Fruböse
Dr. Willi Geiselmann
Michael Klooß
Dr. Alexander Koch
Sven Maier
Jeremias Mechler
Augusto Modanese
Astrid Ottenhues
Markus Raiber
Rebecca Schwerdt
Marcel Tiepelt
Dr. Thomas Worsch

Technisches Personal
Holger Hellmuth

// Website

crypto.iti.kit.edu