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. 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. Die beweisbare Sicherheit ermöglicht es so, große Klassen von Angriffen auszuschließen. Werden dennoch Angriffe bekannt, so waren das zugrundeliegende Modell oder die verwendeten Annahmen nicht realistisch genug. Mit diesem Erkenntnisgewinn kann nun das Modell verbessert oder es können einige Annahme verworfen werden.

Ein Ziel unserer Forschung ist es, Protokolle für verteilte Berechnungen auf geheimen Daten zu entwickeln. Verfahren zur sicheren Mehrparteienberechnung (MPC) erlauben es beispielsweise, 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" (UC) Framework ist ein Sicherheitsmodell, das speziell entwickelt wurde, um eine modulare Herangehensweise zu ermöglichen, bei der einzelne Komponenten für sich genommen als sicher bewiesen werden können und garantiert ist, dass ihre Sicherheit auch im Zusammenwirken mit anderen Komponenten erhalten bleibt.

ERGEBNISSE UND ERFOLGE

Ein Nachteil des UC Frameworks ist, dass starke Annahmen getroffen werden müssen, um Komponenten als sicher zu beweisen. Durch eine Erweiterung des Sicherheitsmodells konnten wir nachweisen, dass Protokolle auch ohne diese Annahmen sicher sein können.

Einen weiteren Forschungsschwerpunkt bilden beweisbar privatsphäreschonende und praxistaugliche Protokolle zur Realisierung von Bezahlsystemen. Die Einsatzmöglichkeiten solcher Protokolle sind vielfältig: so ist es möglich, Bus- und Bahnfahrten zu bezahlen, Mautgebühren zu begleichen, oder Strom für/von Elektroautos („Vehicle to Grid") zu kaufen/verkaufen, ohne dass dabei ein Tracking der Kunden möglich ist. Die Praxistauglichkeit des Systems wurde durch einen ersten Demonstrator auf der CeBiT 2018 nachgewiesen. Das Bezahlsystem stieß dabei auf ein sehr großes

Medienecho. Diese Arbeiten wurden federführend von der Nachwuchsgruppe „CyPhyCrypt“ unter der Leitung von Dr. Andy Rupp durchgeführt.

Das Kompetenzzentrum für angewandte Sicherheitstechnologie KASTEL, eines von deutschlandweit drei Kompetenzzentren für IT-Sicherheit, wurde 2017 von der Helmholtz-Gemeinschaft evaluiert. Die Gutachtergruppe war sowohl von den theoretischen Ergebnissen als auch von den praktischen Umsetzungen und den Demonstratoren beeindruckt und bescheinigte den Arbeiten hohe Relevanz und exzellente Qualität.

2015 wurde das BMBF-Verbundprojekt secUnity eingeworben, dessen Ziel in der Stärkung der Zusammenarbeit der deutschen IT-Sicherheitsforscher besteht. Daraus ist unter Anderem eine Roadmap „Cybersecurity Research“ entstanden, die die größten Forschungsfragen und Herausforderungen von IT-Sicherheit zusammenstellt. Die Roadmap wurde am 05.02.2019 in Brüssel veröffentlicht.

AUSGEWÄHLTE PUBLIKATIONEN

B. Broadnax, V. Fetzer, J. Müller-Quade, A. Rupp: Non-malleability vs. CCA-Security: The Case of Commitments. Public Key Cryptography (2)2018. S. 312-337, 2018.

D. Hofheinz, J. Müller-Quade, D. Unruh: On the (Im-)Possibility of Extending Coin Toss. J. Cryptology 31(4). S. 1120-1163, 2018.

B. Broadnax, N. Döttling, G. Hartung, J. Müller-Quade, M. Nagel: Concurrently Composable Security with Shielded Super-Polynomial Simulators. EUROCRYPT (1) 2017. S. 351-381, 2017.

G. Hartung, M. Hoffmann, M. Nagel, A. Rupp: BBA+: Improving the Security and Applicability of Privacy-Preserving Point Collection. ACM Conference on Computer and Communications Security 2017. S. 1925-1942, 2017.

V. Fetzer, J. Müller-Quade, T. Nilges: A Formal Treatment of Privacy in Video Data. ESORICS (2) 2016. S. 406-424, 2016.

MITARBEITERINNEN UND MITARBEITER

Verwaltungspersonal

Carmen Manietta

Wissenschaftliches Personal

Lukas Beeck
Brandon Broadnax
Valerie Fetzer
Dr. Matthias Gabel
Dr. Willi Geiselmann
Dr. Anna-Louise Grensing
Gunnar Hartung
Björn Kaidel
Michael Klooß
Alexander Koch
Dr. Bernhard Löwe
Sven Maier
Jeremias Mechler
Augusto Modanese
Matthias Nagel
Kathrin Noack
Stefan Röhrich
Dr. Andy Rupp
Rebecca Schwerdt
Dr. Mario Strefler
Dr. Thomas Worsch

Technisches Personal

Holger Hellmuth