Leopoldina
Nationale Akademie
der Wissenschaften

Curriculum Vitae Prof. Dr. Johannes Buchmann

Name: **Johannes Buchmann**
Geboren: **20. November 1953**

Forschungsschwerpunkte: algorithmische Zahlentheorie, IT-Sicherheit, Kryptographie, Post-Quantum-Kryptoverfahren, Datenschutz im Internet

Johannes Buchmann ist Informatiker und forscht insbesondere auf dem Gebiet der Kryptographie. Diese ist eine zentrale Technik für die Sicherheit im Internet. Buchmann entwickelt kryptographische Verfahren, zum Beispiel Verschlüsselungen und elektronische Signaturen. Außerdem beschäftigt er sich mit Fragen des Datenschutzes und der Privatsphäre im Internet.

Akademischer und beruflicher Werdegang

seit 2011	Vizedirektor des Center for Advanced Security Research Darmstadt
2008 - 2011	Gründungsdirektor des Center for Advanced Security Research Darmstadt
seit 1996	Professor (C4/W3) für Informatik und Mathematik, Technische Universität Darmstadt
1988 - 1996	Professor für Informatik, Universität des Saarlandes
1988	Habilitation für das Fach Mathematik an der Universität Düsseldorf
1986 - 1988	Wissenschaftlicher Mitarbeiter an der Universität Düsseldorf
1985 - 1986	Feodor Lynen-Forschungsstipendiat der Alexander von Humboldt-Stiftung an der Ohio State University, USA
1984 - 1985	Wissenschaftlicher Mitarbeiter an der Universität zu Köln
1984	2. Staatsprüfung für das Lehramt an Gymnasien
1983 - 1984	Studienreferendariat
1982	Promotion in Mathematik an der Universität zu Köln
1980 - 1983	Mathematiklehrer an der Fachoberschule für Sozialpädagogik Köln

1979 - 1983	Wissenschaftlicher Assistent an der Universität zu Köln
1979	1. Staatsprüfung für das Lehramt an Gymnasien
1973 - 1979	Studium der Mathematik, Physik, Pädagogik und Philosophie an der Universität zu Köln

Funktionen in wissenschaftlichen Gesellschaften und Gremien

seit 2014	Sprecher des Sonderforschungsbereichs 1119 „Kryptografiebasierte Sicherheitslösungen als Grundlage für Vertrauen in heutigen und zukünftigen IT-Systemen“
seit 2003	Vorsitzender des Competence Center for Applied Security Technology e.V.
2001 - 2007	Vizepräsident der TU Darmstadt
2000 - 2001	Studiendekan des Fachbereichs Informatik der TU Darmstadt
1993 - 1995	Vorsitzender des Fachbereichs Informatik der Universität des Saarlandes
1990 - 1996	Sprecher des Graduiertenkollegs „Effizienz und Komplexität von Algorithmen und Rechenanlagen“ am Fachbereich Informatik der Universität des Saarlandes

Mitglied im Technical Advisory Panel of Center for Information Security and Cryptography Calgary

Mitglied im Kuratorium des Fraunhofer-Instituts SIT

Mitglied im wissenschaftlichen Beirat des Bundeskriminalamtes

Mitglied im Advisory Board des Research center for applied cryptography, University of Waterloo, Kanada

Mitglied im Editorial Board von: Contributions to Discrete Mathematics, International Journal of Mathematics and Computer Science, Teubner Texte zur Informatik, Encyclopaedia of Mathematical Sciences: Number Theory, Industrial Mathematics; Journal of Cryptology (1990-2009)

Gutachter für DFG-Einzelanträge, Forschergruppen, Sonderforschungsbereiche, National Science Foundation (USA), National Sience and Engeneering Research Council (Kanada), Schweizer Nationalfonds

Projektkoordination, Mitgliedschaft in Verbundprojekten

seit 2014	DFG-Projekt „Quantencomputer-resistente Signaturverfahren für die Praxis“
seit 2014	DFG-Projekt „Zukunftssichere Public-Key-Verschlüsselungs- und Signaturverfahren“, Teilprojekt zu SFB 1119 „Kryptografiebasierte Sicherheitslösungen als Grundlage für Vertrauen in heutigen und zukünftigen IT-Systemen“
seit 2014	DFG-Projekt „Langzeit-sichere Archivierung“, Teilprojekt zu SFB 1119

2010 - 2015 DFG-Projekt “Improving and Combining Gröbner bases and SAT solving techniques for algebraic cryptanalysis”, Teilprojekt zu SPP 1489 “Algorithmic and Experimental Methods in Algebra, Geometry and Number Theory”

2010 - 2014 DFG-Projekt „Verfassungskonforme Umsetzung von elektronischen Wahlen“

2010 - 2014 DFG-Projekt „Beweisbar sichere, effiziente und langfristig sichere Varianten des Merkle-Signaturverfahrens“

2010 - 2013 DGF-Projekt „Parallelisieren und Implementieren von Algorithmen für die Kryptanalyse auf Grafikkarten“

2009 - 2013 DFG-Projekt „Juristisch-informatische Modellierung von Internet-Wahlen“

2003 - 2006 DFG-Projekt „Effiziente und sichere Public-Key-Kryptographie für das Zeitalter der Quantencomputer“, Teilprojekt zu SPP 1079 „Sicherheit in der Informations- und Kommunikationstechnik“

1999 - 2004 DFG-Projekt „Kryptosysteme auf der Grundlage elliptischer Kurven“, Teilprojekt zu SPP 1079

1998 - 2006 DFG-Projekt „Kryptosysteme auf der Grundlage algebraischer Zahlkörper“

Auszeichnungen und verliehene Mitgliedschaften

seit 2013 Mitglied des Feldafinger Kreises

2012 Tsungming Tsu Award des National Science Council Taiwan

seit 2011 Mitglied der Nationalen Akademie der Wissenschaften Leopoldina

2008 IT-Sicherheitspreis der Horst Görtz-Stiftung

seit 2008 Mitglied der Deutschen Akademie der Technikwissenschaften acatech

2006 Ehrendoktorwürde der Universität Debrecen, Ungarn

2006 Karl Heinz Beckurts-Preis

seit 2006 Mitglied der Berlin-Brandenburgischen Akademie der Wissenschaften

2003 Innovationspreis des Landes Hessen

seit 2002 Mitglied der Akademie der Wissenschaften und der Literatur Mainz

1997 und 1998 Preis für die beste Lehre, FB Informatik der TU Darmstadt

seit 1996 Korrespondierendes Mitglied der Akademie der Wissenschaften und der Literatur Mainz

1993 Gottfried Wilhelm Leibniz-Preis der Deutschen Forschungsgemeinschaft (DFG)

1985 Feodor Lynen-Forschungsstipendium der Alexander von Humboldt Stiftung

Forschungsschwerpunkte

Johannes Buchmann ist Informatiker. Seine Forschungsschwerpunkte sind algorithmische Zahlentheorie, Algebra, Kryptographie und IT-Sicherheit. Kryptographie ist eine zentrale Technik für die Sicherheit im Internet. Buchmann entwickelt kryptographische Verfahren, wie zum Beispiel Verschlüsselung und elektronische Signaturen. Außerdem beschäftigt er sich mit Fragen des Datenschutzes und der Privatsphäre im Internet.

Die Forschungsgebiete von Johannes Buchmann betreffen unseren modernen Alltag überall dort, wo Sicherheit im Internet eine Rolle spielt. So zum Beispiel in der Gesundheitsversorgung, der öffentlichen Verwaltung, im Finanzsektor und der Energieversorgung. Mit seiner Arbeitsgruppe entwickelt er kryptographische Verfahren. Dazu zählen Verschlüsselung, elektronische Signaturen, Identifikationsverfahren und Hashfunktionen, die eine Art digitalen Fingerabdruck erzeugen. Der Funkschlüssel des Autos oder die verschlüsselte Internetverbindung zur Bank sind solche Prozesse, bei denen die Sicherheit im Hintergrund von kryptographischen Verfahren gewährleistet wird.

Ein Schwerpunkt von Johannes Buchmann ist die Entwicklung von Kryptoverfahren, die auch gegen Angriffe von Quantencomputern bestehen können (Post-Quantum-Kryptoverfahren). Wissenschaftler gehen davon aus, dass es in Zukunft Quantencomputer geben wird, die viele der heutigen kryptologischen Sicherheitsverfahren (RSA, ECC) aushebeln können. In weiteren Arbeiten beschäftigt sich das Team um Johannes Buchmann mit Fragen der Langzeitsicherheit. Insbesondere mit der Langzeitspeicherung vertraulicher Daten, zum Beispiel in Clouds, und der Langzeitarchivierung signierter Dokumente.

In verschiedenen Studien forscht Johannes Buchmann nach den individuellen und gesellschaftlichen Vorstellungen von Privatsphäre im Internet und skizzierte mögliche Gefahren für die Privatsphäre. Außerdem erforscht er mit seiner Arbeitsgruppe anonyme Kommunikation im Internet. Viele Anwendungen untersucht er interdisziplinär mit Juristen, Ethikern, Soziologen und Wirtschaftswissenschaftlern. Weiterhin befasst sich Buchmann mit rechtlichen und ethischen Rahmenbedingungen.