Würdigung von

Herrn Professor Dr. Dr. h.c. Johannes Buchmann

durch Professor Dr.-Ing. (emer.) José L. Encarnação

Johannes Buchmann wurde am 20. November 1953 in Köln geboren. Er studierte von 1973 bis 1979 Mathematik, Physik, Pädagogik und Philosophie an der Universität zu Köln und schloss das Studium mit dem ersten Staatsexamen für das Lehramt an Gymnasien für die Fächer Mathematik und Physik ab. Von 1980 bis 1982 war Johannes Buchmann wissenschaftliche Hilfskraft am mathematischen Institut der Universität zu Köln und gleichzeitig Mathematiklehrer an einer Fachoberschule für Sozialpädagogik. 1982 promovierte Johannes Buchmann mit der Dissertation „Zahlengeometrische Kettenbruchalgorithmen zur Einheitenberechnung“. In dieser Arbeit brachte er Methoden aus Mathematik und Informatik zusammen. Er entwickelte, analysierte und implementierte Algorithmen, die sehr schwere Probleme der Zahlentheorie lösen können. Seine Dissertation weckte die Aufmerksamkeit von Informatikern und Mathematikern, die auf dem Gebiet der algorithmischen Zahlentheorie arbeiteten. Das Gebiet der algorithmischen Zahlentheorie hatte nach der Entdeckung des RSA-Verschlüsselungs- und Signaturverfahrens rapide an Bedeutung gewonnen, weil dort schwere, für die Kryptographie verwendbare Instanzen von Berechnungsproblemen benötigt werden. Johannes Buchmann setzte seine Forschungen fort, absolvierte gleichzeitig in nur einem Jahr das Referendariat und legte 1984 das zweite Staatsexamen für das Lehramt an Gymnasien ab.

Prof. Dr. Johannes Buchmann

Nach kurzer Assistentenzeit in Köln trat Johannes Buchmann 1985 ein Feodor-Lynen Forschungsstipendium der Alexander von Humboldt Stiftung an der Ohio-State University, Columbus Ohio, USA, bei Prof. Hans Zassenhaus an. Hans Zassenhaus war ein berühmter Algebraiker und ein Pionier der algorithmischen Zahlentheorie. Seinen Aufenthalt in den USA nutzte Johannes Buchmann, um sich stärker mit dem neuen Gebiet der Public-Key-Kryptographie zu beschäftigen. Zusammen mit Wissenschaftlern aus Kanada und USA erschloss Johannes Buchmann die algorithmische algebraische Zahlentheorie für kryptographische Anwendungen. Diese Arbeiten inspirierten viele Wissenschaftler auf verwandten Gebieten kryptographische Verfahren zu entwickeln. Gleichzeitig setzte Johannes Buchmann seine Entwicklung von zahlentheoretischen Algorithmen fort. Er wendete die Informatik-Methoden der konkreten Komplexitätstheorie an und konnte hochinteressante Komplexitätsresultate beweisen. In seiner Forschung leistete Johannes Buchmann wichtige Beiträge zur Konvergenz der algorithmischen Mathematik und Informatik. Dies geschah in enger Kooperation internationalen Forscherinnen und Forschern, zum Beispiel mit Hendrik Lenstra, mit dem Johannes Buchmann bei Gastaufenthalten in Berkeley zusammenarbeitete. Nach seiner Rückkehr nach Deutschland habilitierte sich Johannes Buchmann 1988 mit einer Arbeit „Zur Komplexität der Berechnung von Einheiten und Klassengruppen algebraischer Zahlkörper“ für das Fach Mathematik an der Universität Düsseldorf.

Wenige Monate nach seiner Habilitation wurde Johannes Buchmann 1988 auf eine C3-Professur für Informatik an der Universität des Saarlandes berufen. Nach einem C4-Ruf im November desselben Jahres nach Tübingen wurde Johannes Buchmann 1989 C4-Professor an der Universität des Saarlandes. In Saarbrücken konzentrierte sich die Forschungsarbeit von Johannes Buchmann auf die theoretische Kryptographie und die Kryptoanalyse von Zahlentheorie-basierten Publik-Key-Verfahren wie RSA. Hierbei spielte jetzt Hochleistungsrechnen eine wichtige Rolle. Einerseits verwendete die Arbeitsgruppe von Johannes Buchmann Hochleistungsparallelrechner. Andererseits nutzte sie die Rechenzeit auf Workstationclustern mit dem ei-

gens dafür implementierten verteilten System LIPS. Gleichzeitig verwendete die Arbeitsgruppe von Johannes Buchmann das neue Paradigma der Objektorientierung um die Computeralgebra-Algorithmenbibliothek LiDIA zu entwickeln. Diese Bibliothek wurde von vielen Forschern international genutzt. Johannes Buchmann setzte also konsequent seinen Weg fort, moderne Methoden der Informatik mit der algorithmischen Mathematik und Kryptographie zusammenzuführen. In seiner Saarbrücker Zeit gründete Johannes Buchmann auch das erste Graduiertenkolleg der DFG für Informatik und beteiligte sich an dem Sonderforschungsbereich über Parallelität. Im Jahre 1993 verlieh die DFG Johannes Buchmann gemeinsam mit Claus-Peter Schnorr den Leibniz Preis für seine Forschungen. In seiner Zeit in Saarbrücken konnte Johannes Buchmann das Fach Kryptographie und IT-Sicherheit als festen Bestandteil etablieren. Es gehört heute zu einem der Aushängeschilder der Saarbrücker Informatik.

Im Jahr 1996 nahm Johannes Buchmann einen Ruf an die Technische Universität Darmstadt an. Dort begann er, sich auch mehr praktischen Aspekten der Kryptographie zu widmen. Mit zunehmender praktischer Bedeutung der Public-Key-Kryptographie interessierte er sich für die Frage, welche Alternativen zu den herkömmlichen Public-Key-Verfahren existieren und wie bestehende Public-Key-Infrastrukturen flexibel auf die Unsicherheit einzelner kryptographischer Komponenten reagieren können. Es entstand die PKI-Management-Software FlexiTrust. Die Regulierungsbehörde für Telekommunikation und Post (RegTP) (jetzt: Bundesnetzagentur) war an dieser Software für ihre Zertifizierungswurzelinstanz interessiert. So gründete Johannes Buchmann zusammen mit anderen die FlexSecure GmbH, die in Kooperation mit T-Systems FlexiTrust bei der RegTP installierte. FlexiTrust wird inzwischen an vielen Stellen verwendet, zum Beispiel beim Bundesamt für die Sicherheit in der Informationstechnik im Zusammenhang mit dem elektronischen Bundesreisepass. Für diese Leistung erhielt Johannes Buchmann 2006 den Karl Heinz Beckurts-Preis.

1999 veröffentlichte Johannes Buchmann sein Lehrbuch „Einführung in die Kryptographie“. Das Buch liegt inzwischen in Deutschland in der fünften Auflage und international in sieben Sprachen vor (Deutsch, Englisch, Portugiesisch, Französisch, Polnisch, Japanisch, Farsi). Mehrfach bekam Johannes Buchmann Preise für gute Lehre. Er engagierte sich als Gründungsmitglied und Antragsteller in den DFG-Schwerpunkten „Algorithmische Zahlentheorie“, „Sicherheit in der Informationstechnik“ und „Algorithmische und experimentelle Methoden in Algebra, Geometrie und Zahlentheorie“ und beteiligte sich an den Graduiertenkollegs „Infrastrukturen für den elektronischen Markt“ und „Ubiquitäres Rechnen“.

1999 war Johannes Buchmann einer der Gründer des CAST e.V., zunächst ein Forum im Zentrum für graphische Datenverarbeitung e.V. und später ein eingetragener Verein. Von Anfang an war Johannes Buchmann der Vorsitzende dieses Vereins. Aufgabe des Vereins ist der Wissenstransfer und Kommunikation im Bereich der IT-Sicherheit. In monatlichen Workshops für Anwender präsentiert der CAST e.V. aktuelle Entwicklungen der IT-Sicherheit. Mit über hundertfünfzig Unternehmen, Behörden, Forschungseinrichtungen und Privatpersonen ist der CAST e.V. eines der größten europäischen Netzwerke für IT-Sicherheit.

Von 2001 bis 2007 war Johannes Buchmann Vizepräsident für Forschung der TU Darmstadt. In dieser Funktion baute er die Forschungsinfrastruktur der TU Darmstadt völlig neu auf und war damit auch an den Erfolgen der TU Darmstadt in der Exzellenzinitiative des Bundes (ein Cluster und eine Graduiertenschule) und in der LOEWE-Initiative des Landes Hessen (Drei Zentren und ein Schwerpunkt) wesentlich beteiligt. Zwei dieser Exzellenzeinrichtungen sind der Informatik gewidmet. Die Graduiertenschule „Computational Engineering“ und das LOEWE-Zentrum “Center for Advanced Security Research Darmstadt (CASED)” sind auf dem Gebiet der Informatik tätig. Das unterstreicht die Leistungsfähigkeit der Informatik an der TU Darmstadt, an der Johannes Buchmann keinen geringen Anteil hat.

In der Aufbauphase 2008 bis 2011 leitete Johannes Buchmann CASED, eine gemeinsame Initiative der Hochschule Darmstadt, der Fraunhofer Institut für sichere Informationstechnologie und der TU Darmstadt. Die langjährigen Anstrengungen von Johannes Buchmann haben dazu beigetragen, dass mit CASED ein in Deutschland bis jetzt einmaliges Computersicherheitszentrum entstand. In diesem Zentrum arbeiten heute über 250 Wissenschaftlerinnen und Wissenschaftler. Johannes Buchmann war einer der Initiatoren des BMBF-Spritzenclusters „Softwareinnovationen für das digitale Unternehmen“, das 2010 bewilligt wurde und dessen Koordinierungsstelle in Darmstadt bei CASED ist. Johannes Buchmann ist Mitinitiator und Direktoriumsmitglied des BMBF-Kompetenzzentrums European Center for Security and Privacy by Design, das im März 2011 für die TU Darmstadt

bewilligt wurde und 2015 für weitere 4 Jahre verlängert wurde. Seit 2011 konzentrierte sich Johannes Buchmann auf die Einwerbung des Sonderforschungsbereichs CROSSING – Cryptography-Based Security Solutions, der 2014 bewilligt wurde. Es ist der erste Sonderforschungsbereich der DFG im Bereich IT-Sicherheit. Die Erfolge im Bereich IT-Sicherheit motivierten die TU Darmstadt, Johannes Buchmann aufzufordern, für dieses Gebiet einen Antrag auf Etablierung eines Profilbereiches zu stellen. Profilbereiche sind die strategisch wichtigen Themen der TU Darmstadt. Der Antrag wurde positiv evaluiert und wird voraussichtlich im Juli bewilligt. Ebenfalls bewilligt wurde ein Antrag von Johannes Buchmann auf einen Forschungsbau für IT-Sicherheit an der TU Darmstadt. Damit war Johannes Buchmann wesentlich daran beteiligt, IT-Sicherheit zu einem international sichtbaren Schwerpunkt der TU Darmstadt zu machen. Er ist seit 2015 der Sprecher von CYSEC, dem Cybersicherheits-Profilbereich der TU Darmstadt.

In seiner Forschung hat sich Johannes Buchmann inzwischen einem neuen wichtigen Gebiet zugewendet, der „Post-Quantum-Kryptographie“. Es geht dabei um die zentrale Aufgabe, gegen Quantencomputer sichere Public-Key-Verfahren zu konstruieren. Johannes Buchmann hat zusammen mit zwei anderen Autoren ein Buch über den State of the Art der Post-Quantum-Kryptographie herausgegeben und war an der Gründung der International Conference on Post-Quantum-Cryptography wesentlich beteiligt, die 2016 zum siebten Mal stattfindet, nämlich an der Kyushu-Universität in Japan. Für seinen Vorschlag „Future Sign“, ein zukunftssicheres elektronisches Signaturverfahren, erhielt Johannes Buchmann 2008 gemeinsam mit seinem Mitarbeiter Erik Dahmen den zweiten Preis beim Deutschen IT-Sicherheitspreis der Horst-Görtz-Stiftung. Die Forschung an diesem Verfahren führte inzwischen zu einem Internet Draft, der von wichtigen Unternehmen unterstützt wird. Damit ist Johannes Buchmann seinem Ziel treu geblieben, Grundlagenforschung zu betreiben, die schließlich praktische Relevanz hat. In den vergangenen fünf Jahren hat Johannes Buchmann eingeladene Vorträge über Post-Quantum-Kryptographie unter anderem in Japan, USA, Kanada, Marokko, Tunesien, Korea, Taiwan, China, Brasilien und Norwegen gehalten. Das zeigt das große Interesse an diesem Gebiet und den Forschungsbeiträgen von Johannes Buchmann.

Neben technischen Themen beschäftigt sich Johannes Buchmann auch mit den gesellschaftlich-ökonomischen Implikationen der Technik. So leitete er von 2011 bis 2013 das Project „Internet-Privacy“ der Deutschen Akademie der Technikwissenschaften acatech. Das Projekt war eine Kooperation von Wissenschaftlerinnen und Wissenschaftlern aus Informatik, Rechtswissenschaften, Wirtschaftswissenschaften, Philosophie und Soziologie mit Vertretern wichtiger Unternehmen wie Google und Nokia. Ergebnis des Projekts sind mehrere wissenschaftliche Studien und prägnante Empfehlungen. Es hat zu weiteren ähnlichen Aktivitäten des BMBF geführt.

Im Laufe seiner über fast dreißigjährigen Tätigkeit als Professor hat Johannes Buchmann 66 erfolgreiche Doktorarbeiten betreut. Sieben seiner ehemaligen Doktorandinnen und Doktoranden sind Professorinnen und Professoren an Universitäten in Deutschland, Luxemburg, USA, Kanada, Japan, den Vereinigten Arabischen Emiraten, davon drei Frauen. Drei seiner ehemaligen Doktoranden sind Professoren an Fachhochschulen in Deutschland.

Johannes Buchmann engagiert sich in zahlreichen Gremien. Er ist zum Beispiel Mitglied des Feldafinger Kreises, des Münchner Kreises, des wissenschaftlichen Beirats des Bundeskriminalamtes, des Beratungsgremiums zur Umsetzung der Empfehlungen zum Umgang mit sicherheitsrelevanter Forschung der DFG und Leopoldina, des Beirats der AutoUni und der Wissenschaftlichen Kommission Digitalisierte Gesellschaft der Leopoldina.

Die Leistungen von Johannes Buchmann wurden gewürdigt durch den Leibniz-Preis (1993), den Karl Heinz Beckurts-Preis (1996), den IT-Sicherheitspreis (2008), den Tsungmin-Tu-Award (2012), die Aufnahme in die Akademie der Wissenschaften und der Literatur Mainz (1997), die Berlin-Brandenburger Akademie der Wissenschaften (2006), die Deutsche Akademie der Technikwissenschaften (2008) und die Nationale Akademie der Wissenschaften Leopoldina (2011).