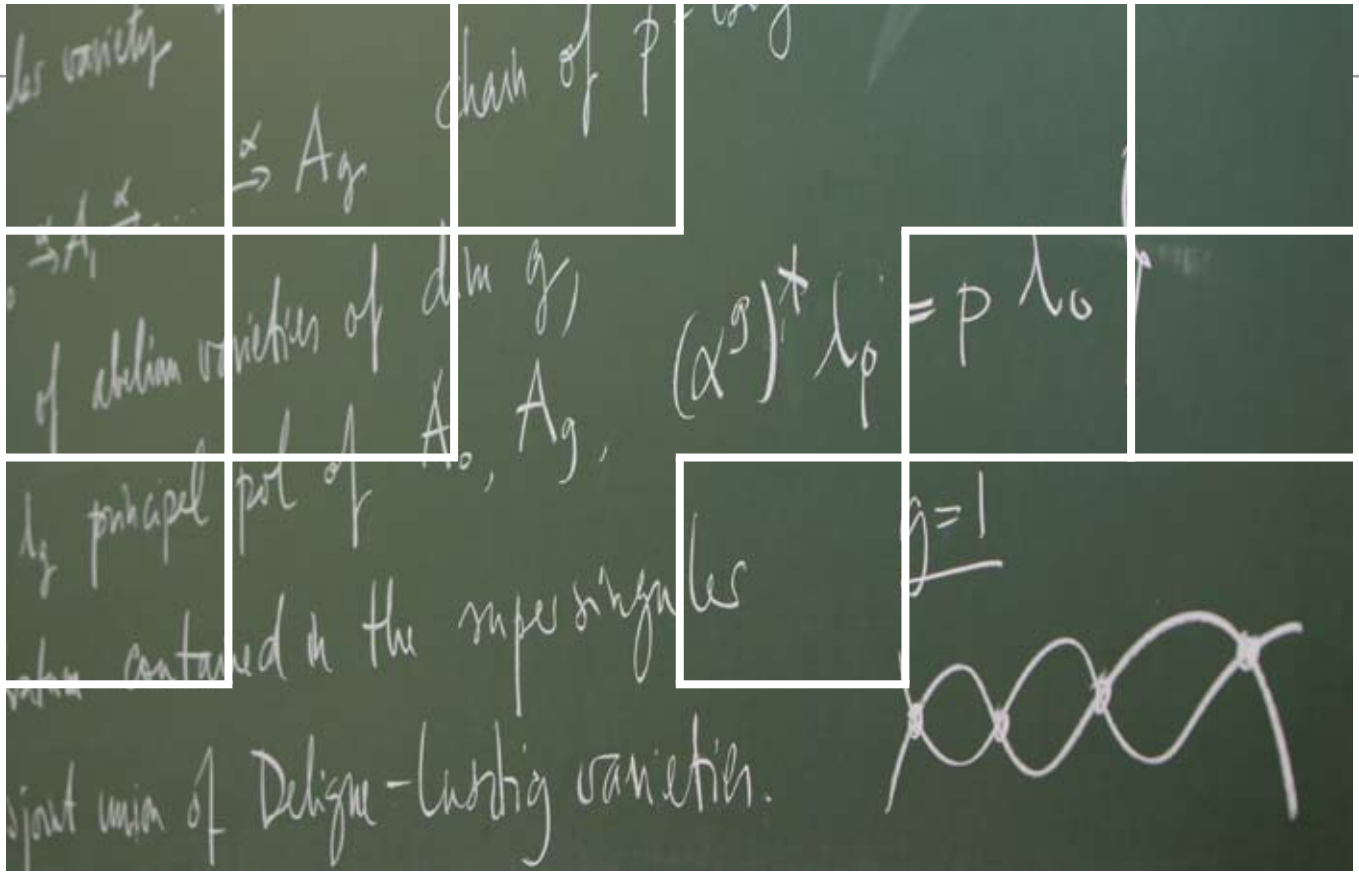
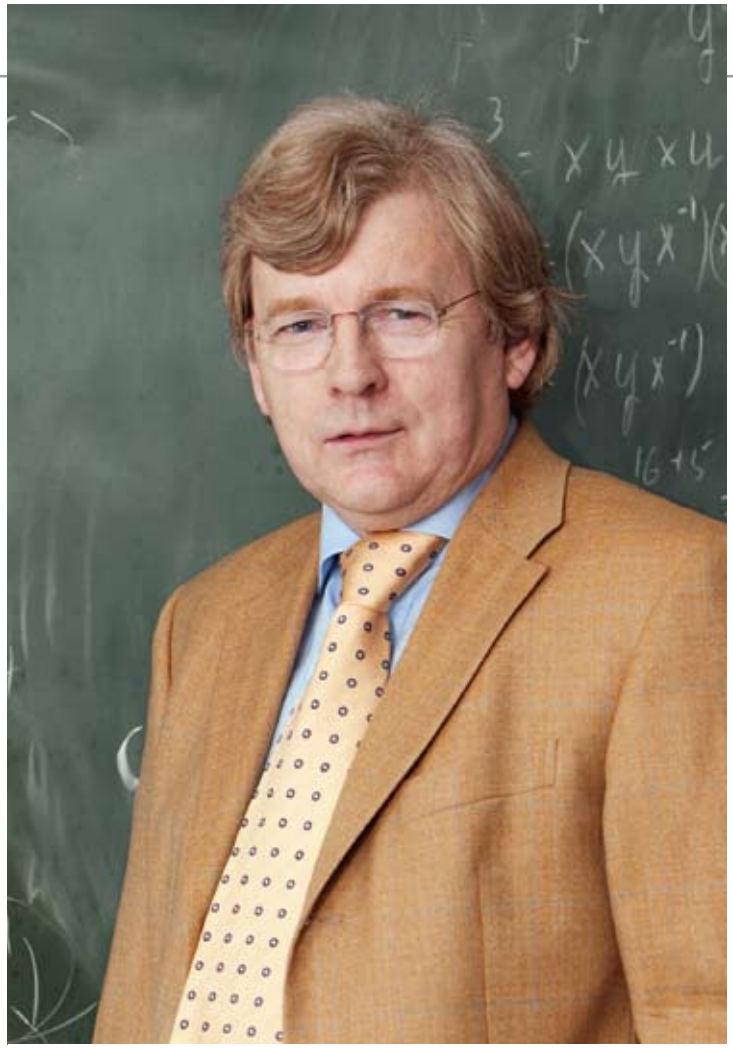


Institut für Experimentelle Mathematik

Institute for Experimental Mathematics

Um Forscherinnen und Forscher aus der Mathematik, Computerexpertinnen und -expertinnen und Nachrichtentechnikerinnen und -technikern die fachübergreifende und unkomplizierte Zusammenarbeit unter einem Dach zu ermöglichen, wurde das Institut für Experimentelle Mathematik (IEM) als eine zentrale wissenschaftliche Einrichtung der damaligen Universität Essen 1989 mit Unterstützung der Volkswagen-Stiftung ins Leben gerufen. Am 1. Januar 1999 wurde das Institut um den Lehrstuhl „Technik der Rechnernetze“ durch eine Alfried Krupp von Bohlen und Halbach-Stiftungsprofessur erweitert. Die Fachgebiete Diskrete Mathematik, Mathematische Methoden der Datenübertragung, Technik der Rechnernetze und Zahlentheorie sind im IEM vertreten.

To enable mathematicians, computer experts and telecommunications engineers to engage in uncomplicated and transdisciplinary collaboration under one roof, the institute for Experimental Mathematics (IEM) was founded, with the support of the Volkswagen Foundation, as a central scientific facility of the former University of Essen in 1989. With the addition of the Alfried Krupp von Bohlen und Halbach Foundation Chair on 1 January 1999, the institute was expanded to include Computer Networking Technology. The areas of Discrete Mathematics, Digital Communications, Computer Networking Technology and Number Theory are all represented at the IEM.



Geschäftsführender Direktor / Managing Director:
Prof. Dr. Wolfgang Lempken

Hauptaufgabe des Instituts ist die Verstärkung der Wechselwirkung zwischen Mathematik, Informatik und Ingenieurwissenschaften. Hierzu gehören die Aufgabengebiete:

- Grundlagenforschung in Algebra, Zahlentheorie, algebraischer und technischer Codierungstheorie,
- Verbesserung der Anwendungsmöglichkeiten von Rechnern in der mathematischen Forschung durch Entwicklung von Algorithmen und leistungsfähiger Software,
- Entwicklung mathematischer Methoden der Datenübertragung und -sicherung für Theorie und Praxis.

Forschung

Eine ausgewogene Mischung von Grundlagenforschung und anwendungsorientierten Forschungsbeiträgen gemäß der interdisziplinären Konzeption des IEM bieten hervorragende Möglichkeiten zur schnellen Nutzbarmachung der Forschungsergebnisse.

Die Forschungsaktivitäten der Arbeitsgruppe Diskrete Mathematik wurzeln in einem Grundprinzip der Mathematik, das besagt, dass eine mathematische Struktur durch das Studium ihrer Symmetriegruppe besser verstanden werden kann. Dadurch können gruppentheoretische Methoden – die diskreter Natur sind – zum Studium von Fragen aus Geometrie, Algebra, Zahlentheorie, Topologie, Funktionstheorie und verschiedenen Anwendungsgebieten wie Kodierungstheorie und Kryptographie eingesetzt werden.

Die Arbeitsgruppe arbeitet sowohl an der Bereitstellung der benötigten gruppentheoretischen Hilfsmittel als auch an deren Anwendung in anderen Disziplinen. Vieles davon beruht wesentlich auf dem Einsatz moderner Computeralgebrasysteme wie GAP, MAGMA und MAPLE.

Konkrete Forschungsthemen sind so genannte hochsymmetrische algebraische Kurven und Riemannsche Flächen, Invariantentheorie binärer Formen, das Umkehrproblem der Galoistheorie, Charakter- und Darstellungstheorie endlicher Gruppen, Permutationsgruppen mit fixpunktarmen Elementen, Kodierungstheorie und Kryp-

The primary objective of the institute is to foster interaction between Mathematics, Computer Science and Engineering. The activities undertaken by IEM scientists in pursuit of this objective include:

- basic research in algebra, number theory, and algebraic and technical coding theory
- improving possibilities for the use of computers in mathematical research by developing algorithms and more efficient software
- developing mathematical methods of data transmission and data backup for theoretical and practical applications.

Research

A balanced mix of basic and applied research in line with the interdisciplinary concept behind

Ausgewählte Publikationen

Selected Publications

- Avanzi, R., H. Cohen, C. Doche, G. Frey, T. Lange, K. Nguyen, F. Vercauteren (2005): The Handbook of Elliptic and Hyperelliptic Curve Cryptography, CRC.
- Chen, Y., A.J. Han Vinck, (2008): Wiretap Channel With Side Information. IEEE Transactions on Information theory, 395–402.
- Dreibholz, T., E.P. Rathgeb, X. Zhou (2008): On Robustness and Countermeasures of Reliable Server Pooling Systems against Denial of Service Attacks. IFIP Networking, Singapore, Mai 2008.
- Koo, T.-L., W. Stein, G. Wiese (2008): On the generation of the coefficient field of a newform by a single Hecke eigenvalue. Journal de Théorie des Nombres de Bordeaux 20), 373–384.
- Korte, U., M. Krawczak, U. Martini, J. Merkle, R. Plagal, M. Niesing, C. Tiemann, H. Vinck (2008): A cryptographic biometric authentication system based on genetic fingerprints (extended version). In: GI-Edition – Lecture Notes in Informatics (LNI) P-128, Bonn: Köllen Verlag, 263–276.
- Lempken, W., T. v. Tran, S. Magliveras, W. Wei (2009): A public key cryptosystem based on non-abelian finite groups. J. Cryptology 22, 62–74.
- Magaard, K., G. Wiesend, H. Völklein (2008): The combinatorics of degenerate covers and an application for generic curves of genus 3. Albanian Journal of Mathematics 2 (3), 145–158.
- Martirosyan, S., T.v. Tran (2008): Explicit constructions for perfect hash families. Designs, Codes and Cryptography 46, 97–112.
- Tüxen, M., I. Rüngeler, R. Stewart, E.P. Rathgeb (2008): Network Address Translation for the Stream Control Transmission Protocol. IEEE Network 22 (5), 26–32.

tographie. Es wird gerade ein Projekt vorbereitet, in dem die expliziten Formen gewisser Invarianten in einer Datenbank gesammelt und verschiedene Anwendungen abgeleitet werden sollen. Am Lehrstuhl für Mathematische Methoden der Datenübertragung wird die mathematische Theorie der Kommunikation erforscht. Gründungsvater dieser Disziplin und Vorbild für die Arbeitsgruppe ist Claude Elwood Shannon (1916–2001), der 1948 das Standardwerk „A Mathematical Theory of Communication“ veröffentlichte und damit den mathematischen Grundstein der digitalen Kommunikation legte.

the IEM offers excellent opportunities for quick utilisation of research results.

The research activities of the Discrete Mathematics Group are rooted in a fundamental mathematical principle, according to which a mathematical structure can be understood better by studying its symmetry group. Methods of group theory – which are discrete – can thus be used to study problems from geometry, algebra, number theory, topology and theory of function, and in various areas of application such as coding theory and cryptography.

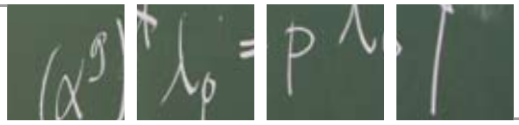
The team works on providing the necessary group theory tools and their application in other disciplines, much of which depends heavily on the use of modern computer algebra systems such as GAP, MAGMA and MAPLE.

Current research themes include highly symmetric algebraic curves and Riemann surfaces, invariant theory of binary forms, the inverse problem of Galois theory, character and representation theory of finite groups, permutation groups with almost fixed point free elements, coding theory and cryptography. A research project is currently being prepared in which the explicit forms of certain invariants are to be collected in a database for various applications.

The Digital Communications Group concentrates on the mathematical theory of communication. The founder of this discipline and the group's role model is Claude Elwood Shannon (1916–2001), whose 1948 standard work "A Mathematical Theory of Communication" laid the mathematical cornerstone of digital communications.

One of the group's main research concerns, like Shannon before them, is solving the problem of unreliable digital communication. They are looking into the question of how to reconstruct a transmitted message which has been disrupted or corrupted during transmission, at the receiver end without any loss of information. Such basic research is becoming increasingly important in today's digitalised world.

In addition to the theory of digital communication, the research group has four other focal



Die Arbeitsgruppe versucht – ähnlich wie Shannon damals – das Problem misslungener digitaler Kommunikation zu lösen. Sie arbeitet unter anderem an der Frage: Wie kann eine Nachricht, die von einem Sender kodiert und versandt, aber durch eine Störung im Kommunikationskanal unvollständig übermittelt wurde, vom Empfänger ohne Informationsverlust dekodiert werden? – Grundlagenforschung, die in der heutigen digitalisierten Welt zunehmend an Bedeutung gewinnt.

Neben der Kommunikationstheorie der Datenübertragung setzt der Lehrstuhl vier weitere Schwerpunkte: Technische Kommunikation, Mehrnutzerkommunikation, Kodierungstechniken und Datensicherheit. Ein großes, langjähriges Forschungsprojekt zur Technischen Kommunikation war die Entwicklung von Übertragungs- und Kodierungsmethoden für die Übertragung von Daten via Stromnetz.

In einem aktuellen Projekt zum Thema Datensicherheit werden neue Public-Key-Verfahren auf der Basis der Faktorisierung von endlichen Gruppen untersucht und entwickelt. Die Sicherheit eines solchen gut entworfenen Systems wäre im Gegensatz zu den heute benutzten Public-Key-Verfahren auch noch für das kommende Zeitalter des Quantencomputers garantiert.

Ein weiteres aktuelles Forschungsprojekt erforscht die Grundlagen sicherer Übertragung biometrischer Daten. Denn ob Fingerprint oder das Erfassen der Physiognomie von Gesichtern – biometrische Daten verändern sich und erschweren somit die einwandfreie Erkennung durch Sicherheitssysteme. Außerdem ist die sichere Speicherung der biometrischen Daten für die Gesellschaft von großer Bedeutung. Sicherheitssysteme zu optimieren und kritische Infrastrukturen wie Energie-, Telefon- oder Verkehrsnetze zu schützen, beinhalten auch immer Aufgaben für Datenübertragungsexpertinnen und -experten.

Der Alfried Krupp von Bohlen und Halbach-Stiftungslehrstuhl Technik der Rechnernetze konzentriert seine Forschungsaktivitäten auf zwei Bereiche: neue Netztechnologien, ihre Netzkonzepte und die zugehörigen Protokolle

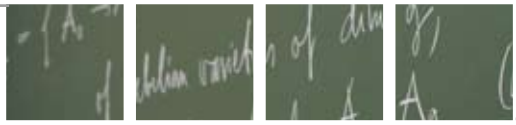
points: communication technology, multi-user communication and networking, coding, and data security. One of the major long-term research projects in communication technology concerned the development of communication methods and coding techniques for power line communications (PLC).

An ongoing project on the subject of data security is investigating and developing new public key systems based on the factorisation of finite groups. In contrast to the public key systems used today, the security of such a well-designed new system would also be guaranteed for the coming generation of quantum computers.

Another current project is looking into the safe transmission of biometric data. Whether they are collected from fingerprints or facial physiognomy, biometric data can change, making failsafe verification by security systems difficult. Safe storage of biometric data is another subject of major importance to society.

Optimising security systems and protecting critical infrastructures such as energy, telephone or transport networks are other areas which always involve tasks for data transmission specialists.

The Alfried Krupp von Bohlen und Halbach Foundation Chair for Computer Networking Technology has two areas of focus in its research: new network technologies, architectures and their protocols, and current network security issues. Research activities related to a novel IETF (Internet Engineering Task Force) concept for Reliable Server Pooling were successfully completed together with the corresponding project funded by the German Research Foundation (DFG). The PhD thesis written by Thomas Dreibholz in connection with the project was recognised with the Research Award of the Sparkasse Essen, while Pascal Schöttle's Bachelor dissertation also relating to the work received the CAST award for IT security. Contributions and active editorial participation made a significant contribution to final approval of the corresponding IETF standards at the end of 2008. Research on the development of the new internet transport protocol



auf der einen Seite, und aktuelle Aspekte der Netzsicherheit auf der anderen. Die Arbeiten zu einem von der IETF (Internet Engineering Task Force) standardisierten Konzept zur Unterstützung hoch verfügbarer Dienste (Reliable Server Pooling) konnten mit dem erfolgreichen Abschluss des entsprechenden DFG-Projektes ebenfalls erfolgreich abgeschlossen werden. Die in diesem Zusammenhang entstandene Dissertation von Thomas Dreibholz wurde mit dem Wissenschaftspreis der Sparkasse Essen ausgezeichnet, die ebenfalls im Rahmen des Projektes angefertigte Bachelorarbeit von Pascal Schöttle mit dem CAST-Preis für IT-Sicherheit. Inhaltliche Beiträge und aktive Mitarbeit bei der Ausarbeitung haben maßgeblich zur endgültigen Verabschiedung der zugehörigen IETF-Standards Ende 2008 beigetragen. Die Forschungsarbeiten zur Weiterentwicklung des neuen Internet-Transportprotokolls SCTP (Stream Control Transmission Protocol) werden in Kooperation mit der Hochschule Münster in einem gemeinsamen DFG-Projekt weitergeführt. In einem durch das BMBF geförderten Projekt zu grundlegenden Architektur- und Sicherheitsfragen für das „Future Internet“ werden die beiden Kompetenzbereiche des Lehrstuhls zusammengeführt und mit Fraunhofer Fokus und der TU Kaiserslautern im Rahmen der deutschen G-Lab-Initiative weiter entwickelt. Daneben sind Forschungsarbeiten zur Sicherheit von Peer-to-Peer-Netzen und zum Schutz der IP-basierten Telefonie (Voice over IP) weitere Schwerpunktthemen. Die Forschungsaktivitäten des Lehrstuhls leisten damit einen Beitrag dazu, das heutige und das künftige Internet für die vielfältigen Sprach- und Multimedia-Anwendungen besser und sicherer nutzbar zu machen. Ziel des Lehrstuhls ist es, die Forschungsergebnisse – neben der Publikation in internationalen Veröffentlichungen – auch direkt in die relevante Standardisierung einzubringen um sie weltweit praktisch nutzbar zu machen.

Das Arbeitsgebiet der Arbeitsgruppe Zahlentheorie ist die arithmetische Geometrie und algebraische Zahlentheorie. Zu einem großen Teil lassen sich die behandelten Fragen einordnen in das so genannte Langlands-Programm, ein beherr-

SCTP (Stream Control Transmission Protocol) is continuing in cooperation with the University of Applied Sciences Münster in a joint DFG project. In a project funded by the German Ministry of Education and Research (BMBF), the two competence areas of the group are being combined and further developed in cooperation with Fraunhofer Fokus and the TU Kaiserslautern. The consortium focuses its research on basic architectural and security issues for the “Future Internet” within the German research initiative G-Lab. The security of peer-to-peer networks and the protection of IP-based telephony (Voice over IP) are other current research topics. In this way, the research activities of the group are contributing to improving the usability and security of the present and future internet for the many voice and multimedia applications. One of the group’s explicit aims, in addition to international publication of its research findings in the scientific press, is to directly incorporate them in the relevant standardisation to ensure their practical application on a global scale.

The core of the activities of the Number Theory Group is research in arithmetic geometry and algebraic number theory. A large proportion of the research questions are related to the Langlands programme, a dominant and very topical subject in number theory. The principle concern of algebraic geometry is to obtain a geometric understanding of the structure of the solution set of polynomial equations. A simple example is $x^2+y^2=1$, whose solution set (the real plane) is the circle of all points with a distance of 1 from the origin. Generally speaking, describing the geometric properties of a given system of equations is very complicated. A particularly interesting aspect of this problem is that geometric intuition can be applied with this theory to questions of number theory.

There are close connections between the current theoretical research of the Number Theory Group and the broad application of explicit, algorithmic and experimental methods: deep insights are often founded on knowledge of examples that can only be obtained from computer

schendes und hochaktuelles Thema der Zahlentheorie.

Das grundsätzliche Anliegen der algebraischen Geometrie ist, die Struktur der Lösungsmenge von polynomialen Gleichungen geometrisch zu verstehen. Ein einfaches Beispiel ist die Gleichung $x^2+y^2=1$, deren Lösungsmenge (in der reellen Zahlenebene) der Kreis aller Punkte mit Abstand 1 vom Ursprung ist. Im Allgemeinen ist es sehr kompliziert, geometrische Eigenschaften eines gegebenen Systems von Gleichungen zu beschreiben. Ein besonders reizvoller Aspekt ist der, dass man mit dieser Theorie geometrische Intuition auch auf zahlentheoretische Fragen anwenden kann.

Es besteht ein intensives Miteinander von Forschung an aktuellen theoretischen Fragestellungen und dem weitreichenden Einsatz expliziter, algorithmischer und experimenteller Methoden: Tiefe Einblicke beruhen oft auf der Kenntnis nur mit dem Computer berechenbarer Beispiele, und andererseits erweist sich ein fundiertes Verständnis theoretischer Zusammenhänge häufig als sehr fruchtbar oder gar unerlässlich, um bislang unmögliche Berechnungen durchzuführen und neuartige Anwendungsmöglichkeiten zu erschließen. Anwendungen bestehen vor allem im Gebiet der Datensicherheit, das die Kryptographie und die Kodierungstheorie umfasst.

Kooperationen und Internationales

Ein umfangreiches Gästeprogramm mit jährlich 35 bis 40 Besuchern und regelmäßig stattfindenden internationale Tagungen knüpfen Verbindungen zu Forscherinnen und Forschern aus aller Welt. Hier einige Beispiele für Kooperationen und Internationalität des IEM:

- Federführende Beteiligung an der Organisation internationaler Tagungen, zum Beispiel Workshop Arithmetic Geometry, IEM, 22.–23.01.2008; Essener Workshop zur Netzsicherheit, IEM, 03.–04.04.2008; Workshop „Factoring Large Numbers, Discrete Logarithms and Cryptanalytical Hardware, IEM, 22.–23.04.2008; IEEE GERMAN-AFRICA Workshop on Information and Communication Technology Workshop, IEM, 11.–13.11.2008.

Wissenschaftlerinnen und Wissenschaftler
Researchers

- Prof. em. Dr. Dr. h.c. Gerhard Frey
- Prof. Dr. Ulrich Görtz
- Prof. Dr. Wolfgang Lempken
- Prof. Dr.-Ing. Erwin P. Rathgeb
- Prof. Dr. Trung van Tran
- Prof. Dr. ir. A. J. Han Vinck
- Prof. Dr. Helmut Völklein
- Prof. Dr. Gabor Wiese

Externe Mitglieder
External Members

- Prof. Dr. Gebhard Böckle, Universität Duisburg-Essen
- Prof. Dr. Hélène Esnault, Universität Duisburg-Essen
- Prof. Dr. Eckart Viehweg †, Universität Duisburg-Essen
- Prof. Dr. Kees Schouhamer-Immink, Turing Machines, Niederlande

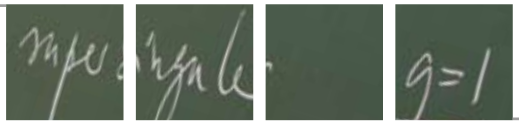
calculations; at the same time, profound theoretical knowledge often proves beneficial or even indispensable for performing otherwise impossible computations and discovering new applications. Data security, which comprises cryptography and coding theory, is a particular area in which applications exist.

Collaboration and International Contacts

The IEM maintains contact to researchers around the world by playing host to between 35 and 40 guests each year under its visiting scholars programme and by holding international workshops on a regular basis.

Some examples of its collaboration and contacts at national and international level are listed below:

- The IEM plays a leading role in the organisation of international conferences, e.g. Workshop on Arithmetic Geometry, IEM, 22.–23.01.2008; Essen Network Security Workshop, IEM, 03.–04.04.2008; Workshop on Factoring Large Numbers, Discrete Logarithms and Cryptanalytical Hardware, IEM, 22.–23.04.2008; IEEE GERMAN-AFRICA Workshop on Information and Communication Technology, IEM, 11.–13.11.2008.



- Mitgliedschaften im Vorstand internationaler Gremien, zum Beispiel Scientific Board CRM (Barcelona), ITG-Fachausschuss 5.2 „Kommunikationsnetze und -systeme“, Working Group 6.2 on Broadband Communications des IFIP-TC6, IEEE Communication Society (Powerline Communications).
- Kooperationsverträge mit zahlreichen Universitäten und Forschungseinrichtungen in den USA, Kanada, Südafrika, Südkorea, China und den Niederlanden.
- Mitherausgeberschaften internationaler Fachzeitschriften, zum Beispiel International Journal on Communication Systems, Journal of Mathematical Cryptology, Journal of Combinatorial Designs, Journal of Discrete Mathematical Sciences and Cryptography, Japanese IEICE Transactions on Fundamental of Electronics, Communications and Computer Sciences.

Preise und Auszeichnungen

- Dr. Thomas Dreibholz wurde 2008 für seine Dissertation „Reliable Server Pooling – Evaluation, Optimization and Extension of a Novel IETF Architecture“ mit dem Wissenschaftspreis der Sparkasse Essen ausgezeichnet.
- Prof. Dr. Ulrich Görtz erhielt 2008 den Von-Kaven-Ehrenpreis der DFG.
- Prof. Dr. ir. A. J. Vinck wurde zum Distinguished Lecturer der IEEE Communication Society für 2008/2009 gewählt.

Studium und Öffentlichkeit

Auf die Ausbildung von Studierenden und Doktorandinnen und Doktoranden sowie auf die Durchführung von Weiterbildungsveranstaltungen legt das IEM besonderes Gewicht. Vorlesungen, Praktika, Kontakte zu führenden Wissenschaftlerinnen und Wissenschaftlern und Instituten im In- und Ausland vermitteln dem wissenschaftlichen Nachwuchs ein umfassendes Bild aktueller Fragestellungen auf dem Gebiet der Experimentellen Mathematik und ihrer Zusammenhänge mit Problemen der Datenübertragung und -sicherung. Kooperationspartner aus der Industrie ergänzen die Ausbildung anwendungsorientiert.

- Members of the IEM sit on the executive boards of international committees, including the Scientific Board CRM (Barcelona), ITG Technical Committee 5.2 “Kommunikationsnetze und -systeme” [Communication Networks and Systems], Working Group 6.2 on Broadband Communications of IFIP-TC6, IEEE Communication Society (Powerline Communications).
- The IEM has cooperation agreements with numerous international universities and research institutions in the USA, Canada, South Africa, South Korea, China and the Netherlands.
- Members of the IEM are co-editors of international journals, including the International Journal on Communication Systems, Journal of Mathematical Cryptology, Journal of Combinatorial Designs, Journal of Discrete Mathematical Sciences and Cryptography, Japanese IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences.

Awards and Distinctions

- Dr. Thomas Dreibholz received the Research Award of the Sparkasse Essen in 2008 for his thesis “Reliable Server Pooling – Evaluation, Optimization and Extension of a Novel IETF Architecture”.
- Prof. Dr. Ulrich Görtz was awarded the von Kaven Prize of the DFG in 2008.
- Prof. Dr. ir. A. J. Vinck was elected Distinguished Lecturer of the IEEE Communication Society for 2008/2009.

Education and Public Relations

The IEM places special importance on graduate, postgraduate and continuing education. Its lectures, seminars, work placements and contacts to leading scientists and institutes at home and abroad provide the upcoming generation of mathematicians with a broad view of the latest developments in the field of experimental mathematics and their relevance to problems in the areas of data transfer and security. Contacts to cooperation partners in industry round off the students’ education and encourage them to

Das IEM hat in den letzten Jahren durch entscheidende Impulse maßgeblich zur Entwicklung und Einführung neuer Studiengänge beigetragen; zum Beispiel der Bachelor-/Master-Studiengänge „Angewandte Informatik/Systems Engineering“ oder „Mathematical Engineering“.

Perspektiven

Der Kern der Arbeit des IEM sind seine Forschungsaktivitäten, die auf hohem Niveau fortgeführt und ausgebaut werden sollen. Dazu dient unter anderem auch die Ausrichtung mehrerer internationaler Tagungen im ersten Halbjahr 2010.

establish connections between mathematical theory and professional practice.

In recent years the IEM has played a key role in the development and introduction of new courses of study, including Bachelor and Master programmes in Applied Computer Science/Systems Engineering and Mathematical Engineering.

Outlook

The core of the IEM's work are its research activities, which it intends to continue on the same high level and expand in future. As part of this process, the institute is organising a number of international conferences in the first half of 2010.

Kontakt
Contact

Institut für Experimentelle Mathematik (IEM)
Institute for Experimental Mathematics (IEM)

Prof. Dr. Wolfgang Lempken
Geschäftsführender Direktor Managing Director

Ellernstr. 29
45326 Essen

✆ +49 (0) 201 / 183 - 76 58
🖷 +49 (0) 201 / 183 - 76 68
@ direktor@iem.uni-due.de
🖳 www.iem.uni-due.de