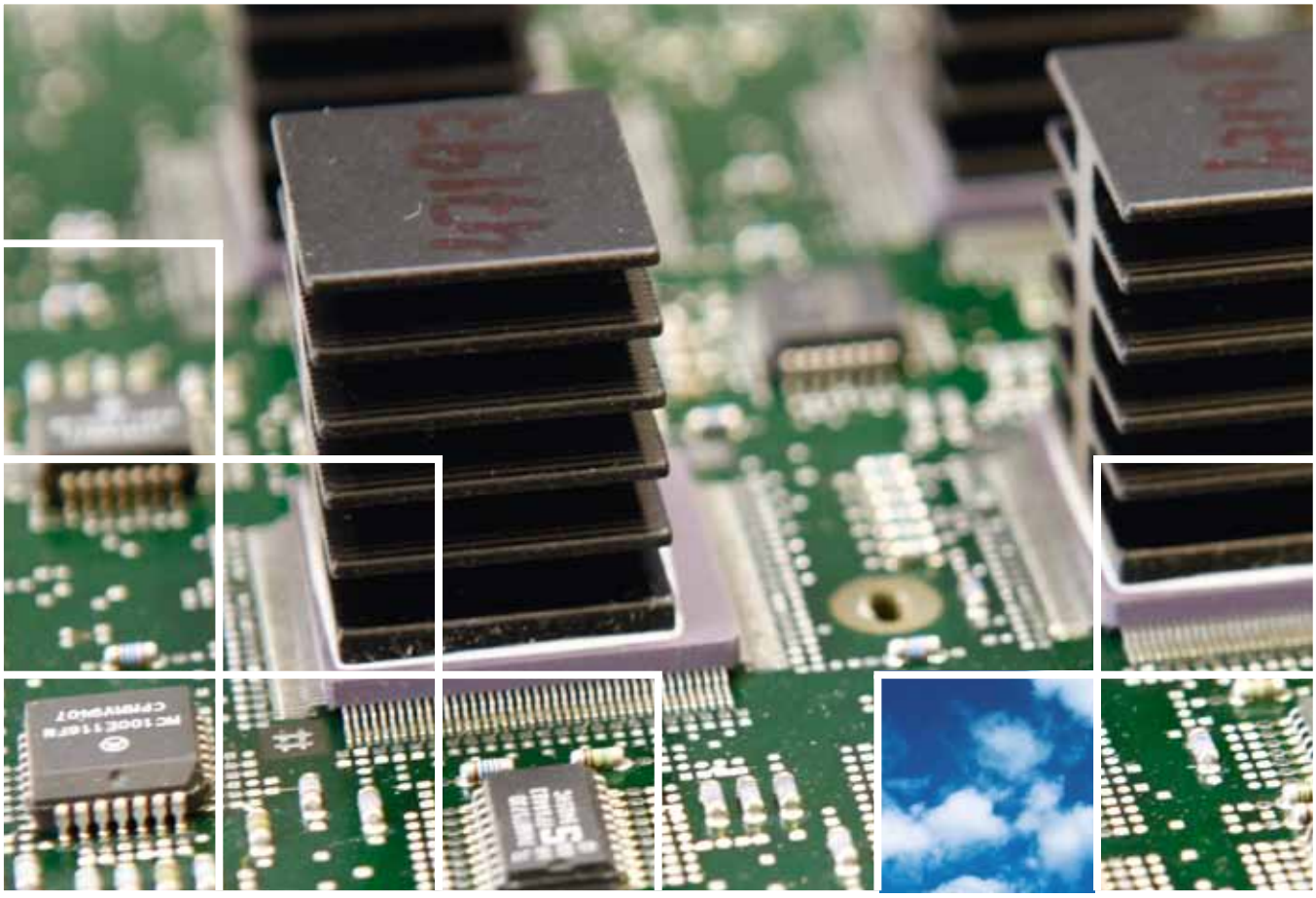

Institut für Experimentelle Mathematik

Institute for Experimental Mathematics

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

To enable mathematicians, computer experts and communications specialists to engage in straightforward and transdisciplinary collaboration under one roof, the Institute for Experimental Mathematics (IEM) was founded with the support of the Volkswagen Foundation in 1989 as a central scientific facility of the former University of Essen. With the addition of the Alfried Krupp von Bohlen und Halbach Chair for Computer Networking Technology on 1 January 1999, the Institute was strengthened in this particular field of research. The areas of Discrete Mathematics, Digital Communications, Computer Networking Technology and Theory of Numbers are all represented at the IEM.

Hauptaufgabe des Instituts ist die Verstärkung der Wechselwirkung zwischen Mathematik, Informatik und Ingenieurwissenschaften. Insbesondere umfasst dies die Bereiche:

- Algorithmen und Verfahren für die elektronische Kommunikation sowie sichere und schnelle Datenübertragung
- Algorithmische Aspekte in der Algebra, der Diskreten Mathematik und der Zahlentheorie sowie wissenschaftliches Rechnen
- Mathematische Grundlagenforschung.

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 hochsymmetrische algebraische Kurven und Riemannsche Flächen, das Umkehrproblem der Galoistheorie, Charakter- und Darstellungstheorie endlicher Gruppen, explizite Konstruktionen von Präsentationen und Darstellungen, Permutationsgruppen mit fixpunktarmen Elementen, Kodierungstheorie und Kryptographie.

An dem Lehrstuhl für Mathematische Methoden der Datenübertragung wird die mathematische

The primary objective of the Institute is to foster interactions between the fields of mathematics, computer science and the engineering sciences. Its main areas of research include:

- Algorithms and mechanisms for electronic communication, and secure and fast data communication
- Algorithmic aspects in algebra, discrete mathematics, number theory and scientific computing
- Basic research in mathematics.

Research

A balanced mixture of basic and applied research representing the interdisciplinary perspective of the IEM offers excellent opportunities for rapid practical exploitation of the research results.

The activities of the Discrete Mathematics Research Group are rooted in a fundamental principle of mathematics, which says that a mathematical structure can be better understood by studying its symmetry group. Group theory methods – which are discrete by nature – can thus be used to study problems from geometry, algebra, number theory, topology, theory of functions and areas of application such as coding theory and cryptography.

The research group works on developing the necessary group theory tools and their application in other areas, much of which relies on the use of modern computer algebra systems like GAP, MAGMA and MAPLE.

Concrete research themes include highly symmetric algebraic curves and Riemann surfaces, invariant theory of binary forms, character and representation theory of finite groups, explicit constructions of presentations and representations, permutation groups with almost fixed point free elements, coding theory and cryptography.

The Digital Communications Research Group concentrates on the development of cryptography, information and communication theory. The founder of this discipline and the group's role model is Claude Elwood Shannon (1916–2001). His 1948 paper "A Mathematical Theory of Communication" laid the foundation for the field of digital communications.

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.

Die Arbeitsgruppe versucht – ähnlich wie Shannon damals – das Problem unzuverlässiger 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 im Rahmen der 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.

In einem weiteren aktuellen Forschungsprojekt werden die Grundlagen sicherer Übertragung biometrischer Daten erforscht. 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 Ver-

One of the main research topics of the group is attempting, like Shannon before them, to solve the problem of unreliable digital communication. They are working, for example, on the question of how a message, coded and transmitted by a sender but disrupted or corrupted in communication, can be decoded at the receiver end without any loss of data. This basic research is becoming increasingly important in today's digitalized world.

In addition to the theory of digital communications, the research group has four other focal points: communication technology; multi-user communication and networking; coding; and data security. One long-running major research project on technical communication concerned the development of communication methods and coding techniques for Powerline Communications (PLC).

In a current project relating to data security, new public key systems are being investigated and developed on the basis of factorization of finite groups. In contrast to the public key systems used today, the security of such a well designed system would also be guaranteed for the coming generation of quantum computers.

Another project is currently investigating the principles of safe transmission of biometric data. Whether fingerprints or facial physiognomy, biometric data change and thus make it more difficult for security systems to identify them with absolute reliability. Safe storage of biometric data is another important issue for society. Optimizing security systems and protecting critical infrastructures such as energy, telephone and transport networks are other tasks which involve the work of data transmission experts.

The Alfried Krupp von Bohlen und Halbach Chair for Computer Networking Technology has two focus areas in its research: new network technologies, architectures and their protocols; and current network security issues. In the area of internet protocols, the group conducted successful research into the systematic evaluation and evolution of the transport protocol SCTP in a joint project with the University of Applied Sciences Münster funded by the German Research Foundation (DFG). In particular, the work on

kehrsnetze zu schützen, beinhalten auch immer Aufgaben für Datenübertragungsexperten.

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 auf der einen Seite, und aktuelle Aspekte der Netzsicherheit auf der anderen. Im Bereich der Internetprotokolle forschte der Lehrstuhl erfolgreich in einem gemeinsamen DFG-Projekt mit der Hochschule Münster an der systematischen Bewertung und Weiterentwicklung des Transportprotokolls SCTP. Besonders die Arbeiten zur gleichzeitigen Nutzung mehrerer Netzwerkpfade (Concurrent Multipath Transfer) führten zu wichtigen Ergebnissen und entsprechend hochrangigen Veröffentlichungen.

In einem durch das BMBF geförderten Projekt zu grundlegenden Architektur- und Sicherheitsfragen für das „Future Internet“ wurden die beiden Kompetenzbereiche des Lehrstuhls zusammengeführt und mit Fraunhofer Fokus und der TU Kaiserslautern im Rahmen der deutschen G-Lab-Initiative weiter entwickelt.

Erkennung von Betrugs- und Missbrauchsversuchen bei der IP-basierten Telefonie (Voice over IP) sowie die Entwicklung entsprechender Schutzverfahren sind weitere Gebiete, auf denen erfreuliche Erfolge erzielt wurden. Hier konnte unter anderem zusammen mit Frauenhofer Fokus und mehreren mittelständischen Unternehmen ein neues, vom BMBF gefördertes Projekt begonnen werden.

Daneben sind Forschungsarbeiten zur Sicherheit von Peer-to-Peer-Netzen ein weiteres Schwerpunktthema. 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.

Geschäftsführender Direktor/Managing Director: Prof. Dr.-Ing. Erwin P. Rathgeb

the concurrent use of multiple network paths (Concurrent Multipath Transfer) yielded important results and led to important publications.

In a project funded by the Federal Ministry of Education and Research (BMBF), the group's two competence areas were 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.

Detecting attempted fraud and misuse in IP-based telephony (Voice over IP) and the development of suitable mitigation mechanisms are other areas in which substantial achievements were made. Among them is the launch of a new BMBF-funded project in which the group is working with Fraunhofer Fokus and several SMEs.

Das Arbeitsgebiet der Arbeitsgruppe Zahlentheorie ist die arithmetische Geometrie und algebraische Zahlentheorie.

Das grundsätzliche Anliegen der algebraischen Geometrie ist, die Struktur der Lösungsmenge von polynomialen Gleichungen geometrisch zu verstehen. Ein einfaches Beispiel ist die Gleichung $y^2=x^3+Ax+B$, mit ganzen Zahlen A und B, die in der Regel elliptische Kurven definieren. Ein gutes Verständnis elliptischer Kurven und ihrer Parameterräume ist in der theoretischen Zahlentheorie ebenso von großer Bedeutung wie bei Anwendungen in der Kryptographie.

Anstelle von Kurven kann man auch analog definierte höher-dimensionale Abelsche Varietäten betrachten. Ein reizvoller Aspekt ist der, dass man mit der modernen algebraischen Geometrie geometrische Intuition auch auf zahlentheoretische Fragen anwenden kann. Ein Ziel ist der Beweis der im Langlands-Programm festgehaltenen Vermutungen über die Symmetrie der Nullstellenmengen von Polynomen in einer Unbestimmten mit ganzzahligen Koeffizienten. Neben klassischen Resultaten wie dem Satz, dass es für Polynome vom Grad mindestens 5 eine allgemeine Lösungsformel wie für quadratische Gleichungen nicht geben kann, gab es auf diesem Gebiet auch in den letzten Jahren noch große Fortschritte, und es gibt weiterhin viele offene Fragen.

Die Arbeitsgruppe Zahlengruppe befasst sich sowohl mit der Forschung an aktuellen theoretischen Fragestellungen, als auch 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.

Kooperationen und Internationales

Ein umfangreiches Gästeprogramm mit jährlich 35 bis 40 Besucherinnen und Besuchern und regelmäßig stattfindende internationale Tagungen

Research on the security of peer-to-peer networks is another focus topic. The research activities of the group are thus contributing to making the current and the future internet better and more secure for the various multimedia applications.

An explicit goal of the Chair – in addition to international publication – is to contribute its research results directly to the relevant standardization to ensure their practical application on a global scale.

The research area of the Number Theory Research Group is arithmetic geometry and algebraic number theory.

The fundamental concern of algebraic geometry is how to understand the structure of the solution set of polynomial equations geometrically. A simple example is the equation $y^2=x^3+Ax+B$, where A and B are integers, which typically define elliptic curves. A sound understanding of elliptic curves and their parameter spaces is of crucial significance not only in theoretical number theory but also for applications in cryptography.

Rather than curves, it is also possible to examine analogous varieties of higher dimension known as Abelian varieties. One compelling aspect here is that modern algebraic geometry permits geometric intuition to also be applied to problems of number theory. One goal is to prove the conjectures recorded in the Langlands program regarding the symmetry of the roots of polynomials in one indeterminate with integral coefficients. While this is a classical topic with interesting results dating back hundreds of years, such as the proposition that there cannot exist a general formula (as that for quadratic equations) for the solutions of polynomials of degree greater or equal to 5, major progress has also been made in this field over the past years. However, numerous questions still remain unanswered.

The Number Theory Research Group is engaged in researching current theoretical problems and in the extensive application of explicit, algorithmic and experimental methods: deep insight is often gained through knowledge of paradigms that can be calculated exclusively on the computer; at the same time, a sound understanding of abstract correlations often proves to be extremely fruitful

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
- 15. Internationale GI/ITG Konferenz „Messung, Modellierung und Bewertung von Rechensystemen“ und „Verlässlichkeit und Fehlertoleranz“ (MMB & DFT 2010)
- Essener Workshop zur Netzsicherheit 2010 und 2011
- Tagung Algebraische Geometrie und Arithmetik (IEM) im Februar 2010
- 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 Fundamentals of Electronics, Communication and Computer Sciences.

Preise und Ehrungen

- Jun.-Prof. Gabor Wiese ist mit dem Gottschalk-Diederich-Baedeker-Preis der Universität Duisburg-Essen ausgezeichnet worden.

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

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. Helmut Völklein
- Prof. Dr. ir. A. J. Han Vinck
- Prof. Dr. Gabor Wiese

Externe Mitglieder
External Members

- Prof. Dr. Gebhard Böckle, Universität Heidelberg
- Prof. Dr. Hélène Esnault, Universität Duisburg-Essen
- Prof. Dr. Marc Levine, Universität Duisburg-Essen
- Prof. Dr. Kees Schouhamer-Immink, Turing Machines, Niederlande

or even indispensable in performing heretofore impossible calculations and opening up novel potential applications.

Cooperation and International News

By welcoming between 35 and 40 guests every year as part of its visiting scholars programme and organizing international workshops on a regular basis, the IEM maintains contact to researchers around the world.

Some examples of its national and international collaborations are listed below:

- The IEM plays a leading role in the organization of international conferences, including the
  - 15th International GI/ITG Conference on “Measurement, Modelling and Evaluation of Computing Systems” and “Dependability and Fault Tolerance” (MMB & DFT 2010)
  - Essen Workshop on Network Security 2010 and 2011
  - Conference on “Algebraische Geometrie und Arithmetik” (IEM) in February 2010
- Members of the IEM serve on the executive boards of international committees such as the Scientific Board CRM (Barcelona), ITG FA 5.2 Committee “Communication networks and systems”, Working Group 6.2 on Broadband Communications of the IFIP-TC6, IEEE Communication Society (Powerline Communications)

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.

Das IEM hat in den letzten Jahren durch entscheidende Impulse maßgeblich zur Entwicklung

Ausgewählte Publikationen
Selected Publications

- Balakirsky, V. B., A. J. H. Vinck (2010): A Simple Scheme for Constructing Fault-Tolerant Passwords from Biometric Data, Eurasip Journal on Information Security, Volume 2010, Article ID 819376.
- Dreibholz, T.; X. Zhou, M. Becke, M., J. Pulithanath, E. P. Rathgeb (2010): On The Securtiy of Reliable Server Pooling Systems. International Journal on Intelligent Information and Database Systems (IJIIDS), 4 (6), 552–578.
- Dreibholz, T., M. Becke, E. P. Rathgeb, M. Tüxen (2010): On the Use of Concurrent Multipath Transfer over Asymmetric Paths. Proceedings of the IEEE Global Communications Conference (GLOBECOM).
- Dreibholz, T., I. Rüngeler, R. Seggelmann, M. Tüxen, E. P. Rathgeb, R. Stewart (2011): Stream Control Transmission Protocol: Past, Current, and Future Standardization Activities. IEEE Communications Magazine 4.
- Görtz, U., T. Wedhorn (2010): Algebraic Geometry I. Schemes, with Examples and Exercises, Vieweg 2010.
- Görtz, U., X. He (2010): Dimensions of affine Deligne-Lusztig varieties in affine flag varieties, Documenta Math. 15, 1009–1028.
- Kato T., K. Magaard, H. Völklein (2011): Bi-elliptic Weierstrass points on curves of genus 5. Indagationes Math. 22, 116–130.
- Lempken, W., L. Miao (2009): On M-supplemented subgroups of finite groups, J. Group Theory 12, 271–287.
- Maas, L.(2010): On a construction of the basic spin representations of symmetric groups, Comm. Alg. 38, 4545–4552.
- Marquardt, P., P. Svaba, T. van Trung (2011): Pseudorandom number generators based on random covers for finite groups, Des. Codes Cryptogr. DOI 10.1007/s10623-011-9485-1.
- Svaba, P., T. van Trung (2010): Public key cryptosystem MST3: cryptanalysis and realization, J. Math. Cryptol. 4, 271-315 DOI 10.1515/JMC.2010.011.
- Terstiege, U. (2011): Intersections of arithmetic Hirzebruch-Zagier cycles, Mathematische Annalen 349, 161–213.

- The IEM has entered into cooperation agreements with numerous 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, e.g. 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

- Junior Professor Gabor Wiese received the Gottschalk-Diederich-Baedeker Prize of the University of Duisburg-Essen.

Education and Training

The IEM places particular emphasis on the education of students enrolled in Master's and PhD programmes and on organizing training and further education events. Lectures, seminars, work placements and contact to leading scientists and institutes at home and abroad provide the upcoming generation of scientists with a broad view of the latest developments in the field of experimental mathematics and the relevance of these developments to problems of data transfer and security. Cooperation partners in industry round off the students' education and help them to make the link between mathematical theory and professional practice.

In recent years, the IEM has made key contributions to the development and introduction of new study programmes, such as the Bachelor's and Master's programmes in Applied Computer Science/Systems Engineering and Mathematical Engineering.

Outlook

The main focus of the IEM is on its research activities, which will be continued and extended at a high level. New research projects and workshops for 2012 have already been initiated. An eminent appointment to the currently vacant

und Einführung neuer Studiengänge, zum Beispiel der Bachelor-/Master-Studiengänge „Angewandte Informatik/Systems Engineering“ oder „Mathematical Engineering“ beigetragen.

Perspektiven

Der Kern der Arbeit des IEM sind seine Forschungsaktivitäten, die auf hohem Niveau fortgeführt und ausgebaut werden sollen. Neue Forschungsprojekte und Workshops 2012 wurden dazu bereits initiiert. Auch die hochkarätige Neubesetzung der vakanten Professur „Diskrete Mathematik“ wird erheblich zur Steigerung der Leistungsfähigkeit des IEM in den nächsten Jahren beitragen.

Chair of Discrete Mathematics will also significantly contribute to strengthening the IEM in the years to come.

Kontakt

Contact

Institut für Experimentelle Mathematik
Institute for Experimental Mathematics

Prof. Dr.-Ing. Erwin P. Rathgeb
Geschäftsführender Direktor Managing Director

Ellernstr. 29
45326 Essen

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