

$$= 2 \quad 859433 \quad - 1$$
 (258 716 Ziffern)
 ist Primzahl

Institut für Experimentelle Mathematik

Institute for Experimental Mathematics

Um Mathematikern, Computerexperten und Nachrichtentechnikern 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 Alfred 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 Alfred Krupp von Bohlen and Halbach Foundation Chair on 1 January 1999, the Institute was expanded in the area of “Computer Networking Technology.” The areas of finite 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. 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

Die Netz- und Informationssicherheit ist ein zentrales Thema aller Arbeitsgruppen des IEM. Sie liefern zu dem Gesamthema gemeinsame Beiträge, die spezifisch sind für ihre unterschiedlichen fachlichen Ausrichtungen.

Die Arbeitsgruppe Mathematische Methoden der Datenübertragung beschäftigt sich mit Problemen der Informations- und Kommunikationstheorie sowie der Datensicherheit. Prof. Trung van Tran hat sich mit der Entwicklung von Public-Key-Verfahren befasst und neue Ansätze zur Realisierung praktischer Kryptoverfahren vorgeschlagen und beschrieben. Zweiter Schwerpunkt der Arbeitsgruppe ist die Forschung auf dem Gebiet der Digitalen Kommunikation.

Die Arbeitsgruppe Technik der Rechnernetze konzentriert seine Forschungsaktivitäten auf neue Netztechnologien, Netzkonzepte und Protokolle. Neben Projekten zur Evolution der UMTS-Netze und zu Architekturen für das Internet der nächsten Generation wurden auch Architekturfragen für Peer-to-Peer- und Sensornetze bearbeitet. Ein längerfristig angelegtes Projekt behandelt die Definition, Bewertung und Weiterentwicklung des neuen Internet-Transportprotokolls SCTP und des darauf aufbauenden Reliable Server Pooling Konzepts. Zusätzlich zu Veröffentlichungen und Dissertationen hat dieses Projekt zu offiziellen Internet-Standards geführt. Diese Aktivitäten leisten einen Beitrag dazu, das Internet auf die künftigen Sprach- und Multimedia-Anwendungen vorzubereiten. Der zweite Schwerpunktbereich ist die Netzsicherheit. Hier werden neue Protokolle zur sicheren und vertraulichen



Geschäftsführender Direktor / Managing Director: Prof. Dr. A. J. Han Vinck

The primary objective of the Institute is to foster interactions between the fields of mathematics, computer science and the engineering sciences.

Several of the activities carried out by scientists at IEM in pursuit of this objective are listed below:

- basic research in algebra, theory of numbers, and algebraic and technical coding theory
- improvement of possibilities for using computers in mathematic research by development algorithms and more efficient software
- development of methods for digital communication data backup for theoretical and practical applications.

Research

Network and information security is a central concern of all the working groups at the IEM. Problems



Kommunikation über das Internet sowie neuartige Konzepte für den Schutz von Internet-Infrastrukturen entwickelt. Prof. Erwin Rathgeb ist Initiator und Sprecher der ITG-Fachgruppe „Sicherheit in Netzen“. Die Arbeitsgruppe erhielt umfangreiche Fördergelder von DFG und BMBF für ihre Forschungsaktivitäten und kooperiert intensiv mit Partnern aus der Industrie.

Das Arbeitsgebiet der Gruppe Zahlentheorie ist die Arithmetische Geometrie. Neben theoretischer Grundlagenarbeit wird die algorithmische Seite der Theorie von der Entwicklung effektiver Methoden bis hin zur Implementierung schneller Algorithmen vorangetrieben. Dieser Forschungsansatz ist eng verbunden mit Anwendungen bei Problemen der Datensicherheit. Die Einführung von Konzepten der Arithmetischen Geometrie ermöglichte große Fortschritte in der Public-Key-Kryptographie. Mitglieder der Gruppe entwickelten in zahlreichen Dissertationen und Veröffentlichungen Konstruktionsmethoden für geeignete Kurven und analysierten Angriffsmöglichkeiten durch Weil-Descent und bilineare Strukturen (Tate-Paarung), ohne die die gegenwärtig verwendete Kryptographie nicht auskommt.

Die Forschungsschwerpunkte der Arbeitsgruppe Diskrete Mathematik liegen im Wesentlichen in der Algebraischen Geometrie und in der Gruppen- und Darstellungstheorie. In beiden Bereichen werden sowohl theoretische Grundlagen erforscht als auch effiziente Algorithmen zur Lösung aktueller Problemstellungen entwickelt und implementiert. Damit liefert die Gruppe unter anderem auch Beiträge in Form von Programmsystemen für die Computeralgebrasysteme GAP und MAGMA. Aktuell wird an der Erstellung einer Datenbank für Überlagerungen der Riemannschen Zahlenkugel gearbeitet. Zusammen mit anderen Arbeitsgruppen des IEM untersucht man hier auch aktuelle Probleme aus dem Schnittstellenbereich von Diskreter Mathematik, Codierungstheorie und Kryptographie.

Kooperationen und Internationales

Ein umfangreiches Gästeprogramm mit 35 bis 40 Besuchern und regelmäßig stattfindenden internationalen Tagungen knüpfen Verbindungen zu

in this area are tackled jointly, with each group making a contribution based on its particular expertise.

The Working Group on Digital Communications focuses on problems in the areas of information theory, communication theory and data security. Prof. Trung van Tran has been involved in the development of public key methods; he has developed public key algorithms and proposed and described new approaches to the realization of practical cryptographic algorithms. The group also concentrates its research on the area of digital communications.

The Alfried Krupp von Bohlen und Halbach Chair for Computer Networking Technology focuses on new network technologies, architectures and protocols. Besides carrying out projects on UMTS evolution and next-generation Internet architecture, the group is concerned with architectural issues of peer-to-peer and sensor network concepts. A long-term project deals with the definition, evaluation and further development of the new Internet transport protocol SCTP and the reliable server pooling framework based on it. In addition to research publications and doctoral dissertations, this project has resulted in official Internet standards. These activities contribute to the effort to make the Internet fit for telephony and multimedia applications. The second area of focus is network security. Here the group is developing new protocols to ensure secure and confidential communication via the Internet as well as innovative concepts to protect future Internet infrastructure. Prof. Rathgeb is the initiator and chairman of the ITG specialist group on network security. This working group has received substantial public funding (DFG, BMBF) and also cooperates intensively with partners in industry.

The research area of the Working Group on Theory of Numbers is arithmetic geometry. In addition to investigations in the realm of pure mathematics, the explicit aspects play a crucial role ranging from developing effective methods up to the implementation of fast algorithms. This research approach is closely linked to applications in the area of data security. The introduction of concepts from the area of arithmetic geometry has laid the foundation for major advances in public key cryptography. In numerous doctoral theses and publications, the



Wissenschaftler Researchers

- Prof. Dr. Dr. h.c. Gerhard Frey
- 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
- Junior Prof. Dr. Gabor Wiese

Externe Mitglieder External Members

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

Forschern aus aller Welt. Hier einige Beispiele für Kooperationen und Internationalität des IEM:

- federführende Beteiligung an der Organisation internationaler Tagungen
- Mitgliedschaften im Vorstand internationaler Gremien
- Kooperationsverträge mit zahlreichen internationalen Universitäten
- Beteiligung an zahlreichen internationalen Forschungsprojekten
- Mitherausgeberschaften internationaler Fachzeitschriften.

Preise und Ehrungen

- Prof. A. J. Han Vinck wurde 2004 zum IEEE Fellow für sein wissenschaftliches Werk im Bereich der Kodierungstechnik ernannt und 2006 erhielt er den IEEE-Award für die bedeutende Rolle als Gründer der ISPLC (International Symposium of Power Line Communications).
- Prof. Gerhard Frey erhielt 2007 die Ehrendoktorwürde der Universität Tübingen.
- Prof. Trung van Tran ist Fellow des Institute of Combinatorics and its Applications (Hauptsitz: Winnipeg, Canada).

Studium und Öffentlichkeit

Auf die Ausbildung von Studierenden und Doktoranden sowie auf die Durchführung von Weiterbildungsveranstaltungen legt das IEM besonderes Gewicht. Vorlesungen, Praktika, Kontakte zu führenden Wissenschaftlern und Instituten im In- und

members of this group have developed methods for the construction of appropriate curves and have discussed the possibility of attacks due to Weil descent and bilinear structures (Tate Pairing) essential for contemporary cryptography.

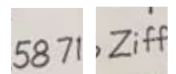
The main research interests of the Working Group on Finite Mathematics are in the areas of algebraic geometry and group and representation theory. In both areas research efforts not only concentrate on the theoretical underpinnings of the subject but also deal with the development and implementation of efficient algorithms to solve present-day problems. In this way, the group has made contributions in the form of programme systems (e.g. BRAID) for the computer algebra systems GAP and MAGMA.

Currently, work is in progress on a data base for problems related to Riemann spheres and Riemann surfaces. Furthermore, the group is investigating problems lying in the area of intersection between finite mathematics, coding theory and cryptography in collaboration with other groups at the IEM.

National and International Collaboration

By welcoming 35 to 40 guests each year as part of its visiting scholars programme and by organizing international workshops on a regular basis, the IEM maintains contact to researchers around the world. Some examples for this national and international collaboration are listed below:

- The IEM plays a leading role in the organization of international conferences.





Zentrale 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.
- Frey, G. (2006): Duality Theorems in Arithmetic Geometry and Applications, Coxeter Lectures Series, Fields Institute, Toronto.
- Jungmaier, A., E. P. Rathgeb (2006): On SCTP Multihoming Performance. Telecommunication Systems 31/ (Special Issue: Next Generation Networks – Architectures, Protocols, Performance), 141-161.
- Lempken, W., T. v. Tran (2005): On Minimal Logarithmic Signatures of Finite Groups. Experimental Mathematics 14, 257-269.
- Staszewski, R., H. Völklein, G. Wiesend (2005): Counting Generating Systems of a Finite Group from Given Conjugacy Classes. Computational Aspects of Algebraic Curves. Lecture Notes Series on Computing 13, World Scientific, 256-263.
- Tödtmann, B., E. P. Rathgeb (2007): Anticipatory Distributed Packet Filter Configuration for Carrier-Grade IP Networks. Elsevier J. on Computer Networks (COMNET) 51, 2565-2579.
- Tran, T. van, C. J. Colbourn, S. S. Martirosyan, R. A. Walker II (2006): Roux-type Constructions for Covering Arrays of Strengths Three and Four. Designs, Codes and Cryptography 41, 35-57.
- Vinck, A. J. Han, Yuan Luo, C. Mitrpant (2006): An Achievable Region for the Gaussian Wiretap Channel with Side Information., IEEE Transactions on Information Theory, May, 2181-2190

- Members of the IEM sit on the executive boards of international committees.
- The IEM has entered into contracts of cooperation with international universities.
- It takes part in international research projects.
- Members of the IEM are co-editors of international journals.

Prices and Awards

- Prof. A. J. Han Vinck was named an IEEE Fellow in 2004 for his scientific work in the field of coding theory and techniques. In 2006 he received the IEEE Award for his pioneering work as founder of the International Symposium of Power Line Communications (ISPLC).
- Prof. Gerhard Frey was awarded an honorary doctorate from the University of Tübingen in 2007.
- Prof. Trung van Tran is a Fellow of the Institute of Combinatorics and its Applications (Head Office: Winnipeg, Canada).

Academic Programs and Public Relations

The IEM places special importance on the education of students enrolled in master's and PhD programs and on postgraduate education. 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 the relevance of these developments 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 establish connections between mathematical theory and professional practice.

In recent years IEM made key contributions during the development and introduction of new courses of studies, e.g. the bachelor's and master's programs in Applied Computer Science/Systems Engineering and Mathematical Engineering.

Outlook

In cooperation with scientists at the University of Duisburg-Essen and the University of Bochum, the IEM is currently working to introduce a new

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.

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

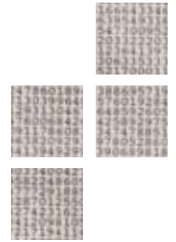
Perspektiven

In Kooperation mit Wissenschaftlern der Universitäten Duisburg-Essen und Bochum arbeitet das



IEM zurzeit an der Initiierung eines Forschungsprojektes mit dem Schwerpunkt „Mehr-Nutzer-Aspekte in der Kryptographie“. Dieses Projekt basiert auf den Erfahrungen, die seit Bestehen des IEM in der Kryptographie gesammelt wurden.

research project focused on “Multi-user Aspects of Cryptography.” This project is based on the experience in cryptography gained by the IEM since its founding.



Kontakt Contact

Institut für Experimentelle Mathematik
Institute for Experimental Mathematics

Prof. Dr. A. J. Han Vinck
Geschäftsführender Direktor **Managing Director**

Ellernstr. 29
45326 Essen

☎ +49 (0)201 183-7658
☎ +49 (0)201 183-7668
@ direktor@iem.uni-due.de
🌐 www.iem.uni-due.de

