Prof. Dr. PREDA MIHAILESCU
Email: preda@uni-math.gwdg.de

tel. P. 0551/4887864 G. 0551/397792
Ewaldstr. 79, DE-37075 Göttingen

Curriculum Vitae
Preda Mihailescu

General information

- **Personal**: Born on May, 23-d, 1955 in Bucharest. Married. One nine years old daughter.
- **Schools**: 1962-73 in Bucharest; 1973-75, Maturität at the Oberrealschule Rämibüehl, Zürich.
- **University**: 1975-80, Mathematics ETH Zürich; 1983-88, Computer Science, ETH Zürich.
- **Phd** 1997, ETH Zürich, in mathematics.
- **Industry:** working with interruptions between 1977-1988.

  Full time: 1988-2000.
- **Recent academic career:** Habilitation 2003, WS 2003-WS2004: Substitute Professor, Uni Paderborn, Since April 2005: VW-Stiftungs-Professor, Uni Göttingen**.**
- **Cityzenship**: Swiss and Romanian (not actualized !)
- **Languages written and spoken**: German, Swiss German, French, English, Italian and Romanian.

Academic details

- 1981. Diplom (~ Masters Thesis) in Mathematics ETH Zürich, Subject: „Lucas Sequences and application to primality testing.
- 1984. PhD in numerical analysis on : „Computation of conformal maps on domains with discontinuous border, using Newton iterations“ - completed, accepted but not submitted due to the premature retirement of the PhD professor on a non academic position. The thesis developed an adapted family of operators, proved convergence and revealed by computation the instability of the recent Newton iteration that had been proposed for the PhD.
- 1988. Diplom in Computer Scienceat the ETH Zürich. Thesis: „Investigation and Implementation of the Elliptic Curve Method for Factoring Integers.“
- 1997. PhD in Computational Number Theory: „Cyclotomy of Rings and Primality Testing“. At the time of completion, the leading algorithm for primality proving.
- 2003. Habilitation at the University Paderborn.
- 2003-2005 Professor at the University Paderborn
- 2005- Professor at Mathematisches Institut, University of Göttingen

Teaching

- 1976-78: Substitute teacher for mathematics at the Oberrealschule Rämibüehl, Zürich; Liceo Cantonale, Lugano; Scuola di Commercio, Bellinzona.
- 1980-84: Teaching assistant at the ETH, teaching in various areas. Like algebra, functional analysis, complex analysis, numerical Mathematics.
- 1984-88: Coordinating the assistant teaching in complex and numerical analyis at the faculty of Electroengineering of the ETH Zürich.
- 2000-02: Teaching assistant „mathematics for computer scientist“, at the Uni Paderborn.
- 2003-05: Substitue professor at the Uni Paderborn – main domain of teaching: computational number theory.
- 2002-04: Organising and leading the Göttingen – Paderborn Seminar on fingerpring recognition, together with Prof. A. Munk.

Consulting

- 1988 – Consulting for the bank UBS on behalf of the comapny HTS Technology.
- 1995-96. Security consulting at numerous Swiss companies, on behalf of R^3 Security AG.
- 1997. Security consulting for the Swiss Union Bank (SBV) for an Online Broker System.
- 2000. Consulting with the RSALabs of the RSASecuriy company in Boston MA.

Practical Achievements

- Conception and development of the cryptographic system underlaying the Swiss online ATM System. Still in use.
- Development of software and concept for the in-house security of applications at the bank UBS. Partially still in use.
- Developing and pattenting of a fast arithmetic with application in public key cryptography. The system has been shortly used by RSA, but the pattent failed to be taken over by them due to the „dotcom“ stock crisis.

Detailed projects

- 1984-85. Deevelopment of numerical models for computation of reference data to solutions of differential equations related to gas turbine flow computations. The numerical results were connected with an interactive graphical representation of parameters and results, using some of the first graphical softwares available: commercial software.
- 1985-86. Project and development of an interactive CAD program for representation of load flow and short cut computations, for Brown Boveri AG: commercial software.
- 1988. Security design and development of a personal identification token for interactive banking under appointment for the bank UBS. Commercial design and software.
- 1989-92. Conception and implementation of the cryptographical system for the BANCOMAT90, Swiss ATM System. (Mainframe, ATM and chip – programming, schooling for the maintenance, etc.)
- 1992-95. Designing and implementing security solutions for applications in the intranet of the bank SBG (UBS) . Assesment of security guidelines and policies, schooling and manager consulting.
- 1996. Development and implementation of the SSL 2/3 standardds for the company R^3 Security, in applications for the Swissonline AG and a consortium of Swiss banks.
- 1997. Development and implementation in Java of an SSL-based security model for an online application for stock trading for the SBV Bank.
- 1998-2000. Development and implementation of algorithms for fingerpring recognition for FingerPIN AG.

Community recognition and activities

- 30-th Kuwait Lecture, Cambridge Institute of Mathematics.
- Seminaire Bourbaki on the proof of Catalan's Conjecture.
- Invited Lecture at the 4-th European Congress of Mathematics.
- Plenary lecture, Congress of the British Mathematical Society, Newcastle 2006.
- Several position accepted as invited professor.
- Sporadic communications for the Newsletters of the EMS.
- Organisation of symposia, conferences and summer schools (not very numerous …)

Mathematical interests

- Computational Number Theory – algorithms for problems related to cryptography, arithmetic with focus on applications of Galois theory in computations.
- Diophantine equations – investigation of particular exponential Diophantine equations by an extensive use of cyclotomic methods. Examples: the equations of Catalan, Nagell-Ljunggren, Binary and Ternary Thue equations, Fermat-Catalan.
- Long standing problems in one dimensional Iwasawa Theory: conjectures of Iwasawa, Greenberg, Leopoldt, Gross, Vandiver.
- Practical applications of fingerprint recognition and mathematical-statistical modelling of the information in fingerprints with application to modelling of attacks and security.