Fachbereich Mathematik

Mathematisches Kolloquium

Im Rahmen des Kolloquiums spricht: **Prof. Dr. Jintai Ding**
University of Cincinnati
z. Z. Technische Universität Darmstadt

über das Thema: **Multivariante Public Key Cryptography**

Abstract: Public key cryptography is an indispensable part of our modern communication systems. However, quantum computers can break the most commonly-used public key cryptosystems like RSA, which are based on "hard" number theory problems. Recently a great effort has been put into the search for alternative public key cryptosystems. Multivariate public key cryptosystems (MKPC), whose public key is a set of multivariate polynomials over a finite field, provide one such promising alternative. The theoretical security assumption comes from the fact that solving a system of polynomial equations over a finite field is in general NP-complete and quantum computers are not yet effective in solving this problem. Furthermore, computations in a finite field can be more efficient, therefore MPKCs also have the potential in application for devices with limited computing power.

In this talk, we will first present an systematic introduction of the recent development in this new area, the focus will be on the the Matsumoto-Imai cryptosystems, the Sflash cryptosystems, the HFE cryptosystems, the Oil-Vinegar cryptosystems, the HFEv cryptosystems, the TTM cryptosystems, the cryptosystems of internal perturbation and the Rainbow cryptosystems, the related multivariate polynomial solving algorithms, and we will also present the main challenges we are currently facing.

Termin: Montag, **22. Januar 2007, 17:00 Uhr**
Ort Hörsaal, M E28
Kaffee/Tee: 16:30 Uhr, Raum M 614/616

Zu diesem Vortrag laden die Dozenten der Mathematik ein.