



Kolloquium

• **Donnerstag, 30. September 1999, 10.00 Uhr, Raum FR5516**
Prof. Dr. Çetin K. Koç
Oregon State University:

New Directions in Public-Key Infrastructures: AADS & ECC

Abstract:

A new methodology for electronic commerce transactions, which is considered as an alternative to SET, is currently being developed. This new methodology is named Accounty Authority Digital Signatures (AADS) which provides an infrastructure for identification and authentication without using a Certificate Authority (CA).

One reason the US Banks & Credit Card Transaction Companies have been slow and in some cases unwilling to embrace SET is that it requires a certificate authority (CA) being built. This has been the main bottleneck for several reasons. While the computer companies, banks, and the US government (NIST) are battling over how to accomplish this, the customers (consumers) are waiting for their smart credit cards.

AADS was developed by computer scientists at First Data Corporation (FDC) which is the largest credit card transactions company in the US. My role has been to develop the best digital signature technology for the AADS. I have influenced the FDC to drop the RSA algorithm and use the elliptic curve cryptosystems (ECC), particularly the ECDSA. With support from FDC, Cybersafe, and SITI, I have developed the essential ingredients of the ECC technology to be embedded within the AADS. Most important features of this technology are scalability, high-speed and area-efficient hardware & software solutions, and ability for on-line selection of the curves. The resulting infrastructure is the first large-scale PKI in the world, and is currently on schedule to be deployed.

Ansprechpartner: DAI-Labor, Stefan Fricke