



## **Kolloquium des Graduiertenkollegs „Mathematische und ingenieurwissenschaftliche Methoden der sicheren Datenübertragung“**

20. November 2003, 15.00 Uhr c. t.  
FernUniversität in Hagen, Universitätsstr. 11, 58084 Hagen  
Raum C 13, 3. Etage im TGZ

### **„The Rolling Computing Platform“**

**Prof. Dr. Ahmad-Reza Sadeghi**

Lehrstuhl für Kommunikationssicherheit

Fakultät für Elektro- und Informationstechnik, Ruhr-Universität Bochum

#### **Zusammenfassung:**

Im Vortrag werden verschiedene Aspekte von "Digital Rights Management (DRM)", insbesondere im Zusammenhang mit dem Einsatz neuer Technologien in Autos, betrachtet. Diese betreffen u.a. technische und rechtliche Grundlagen von DRM und Trusted Computing in eingebetteten Umgebungen.

### **„Identity Based Signatures“**

**PhD Weidong Qiu**

Lehrgebiet Kommunikationssysteme

Fachbereich Elektro- und Informationstechnik, FernUniversität in Hagen

#### **Zusammenfassung:**

Identity based cryptosystems can greatly reduce the reliance on the current public key certificates which needed to be obtained in advance, by deriving public key from identification information such as an email address or a public IP address which can uniquely identify the entity.

In this talk, we present a new identity based signature (IBS) scheme based on quadratic residue problem (IBS-QR). It is a combination of identity based and mediated cryptography. Furthermore, it can solve the public key revocation problem easily.