



**Kolloquium des Graduiertenkollegs
„Mathematische und ingenieurwissenschaftliche Methoden für sichere
Datenübertragung und Informationsvermittlung“**

21. November 2002, 15.00 Uhr

Fachbereich Elektrotechnik und Informationstechnik
Lehrgebiet Kommunikationssysteme (TGZ, 3. Etage, Raum C13)
FernUniversität Hagen
Universitätsstrasse 11, 58084 Hagen

**15.15 Uhr Dipl.-Inform. Sonja Schaup (LG Kommunikationssysteme, Univ. Hagen)
„Benutzerauthentifikation durch Analyse der Tippdynamik“**

Zusammenfassung:

Methoden zur Überprüfung der Identität von Personen zum Zweck der Zugangsbeschränkung sind ein wesentlicher Bestandteil sicherer Systeme. Klassische Methoden beruhen darauf, daß eine Person über bestimmtes Wissen (z.B. Paßwort, PIN) oder Besitz (z.B. Chipkarte) verfügt. Besitz und Wissen sind allerdings übertragbar und können ausspioniert oder gestohlen werden.

Biometrische Verfahren analysieren physiologische oder verhaltensbasierte Eigenschaften einer Person. Hierbei handelt es sich um persönliche Merkmale, die mit der entsprechenden Person verbunden sind, jederzeit reproduziert und weder verloren, noch gestohlen werden können. Ein Vertreter der verhaltensbasierten Biometrien ist die Analyse der Tippdynamik, die - wie die handschriftliche Unterschrift - erfolgreich zur Authentifikation eingesetzt werden kann. Von Vorteil ist hierbei, daß es sich bei dem verwendeten Sensor um die Tastatur des Computers handelt, zusätzliche Hardware im Gegensatz zu anderen biometrischen Verfahren nicht erforderlich ist.

Der Vortrag gibt einen ersten Einblick in die Thematik, den Aufbau der Tippdynamik, Analysemöglichkeiten und verschiedene Arbeiten auf diesem Gebiet.

16.00 Uhr Kaffeepause

**16.15 Uhr MSc. Mingxing He (LG Kommunikationssysteme, FernUniversität Hagen)
„Access Key Distribution Scheme for Level-based Hierarchy“**

Abstracts:

This talk focuses on a new access key distribution scheme for applications where users are in a level-based hierarchy. Based on Chinese Remainder Theorem (CRT) and Rabin-based secure public key system, the proposed scheme has the following characteristics: (1) each user can derive the secret key for users in a lower security level and the inversion is not allowed; (2) the key generation and derivation algorithm are simple; (3) the user and secret key selection are flexible; (4) semantic security can be ensured to prevent attacking from users with lower privileges or external adversary.

Key words: access control, key distribution, CRT, hash function, cryptosystem