



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

10. Juli 2003, 15.00 Uhr c.t.
FernUniversität in Hagen, Universitätsstr. 11, 58084 Hagen
Raum C 12, 3. Etage im TGZ

"Geteilte Geheimnisse in Graphen"

Prof. Werner Poguntke

FTK – Forschungsinstitut für Telekommunikation an der FernUniversität in Hagen

Zusammenfassung:

Es wird über zwei Ansätze berichtet, Methoden der Graphentheorie auf *Secret Sharing Schemes* anzuwenden. Im ersten Fall wird die Zugriffsstruktur auf das Gesamtgeheimnis durch die nicht-unabhängigen Knotenmengen eines Graphen beschrieben; zentraler Untersuchungsgegenstand ist dabei die erzielbare Informationsrate. Beim zweiten Ansatz wird ein Kommunikationsnetz durch einen Graphen modelliert, dessen Knoten und Kanten unzuverlässig sind; es geht um das Problem, Teilgeheimnisse so auf Knoten zu verteilen, dass das Gesamtgeheimnis von einem vorgegebenen Knoten aus durch Einsammeln von Teilgeheimnissen entlang funktionsfähiger Wege mit hoher Wahrscheinlichkeit rekonstruiert werden kann.

Datenkompression – Grundlagen, Geschichte und Verfahren

Olaf Ehlert

Lehrgebiet Nachrichtentechnik, FernUniversität in Hagen)

Zusammenfassung:

Der Vortrag erläutert zunächst die Grundlagen der Informationstheorie nach Shannon sowie der algorithmischen Informationstheorie nach Kolmogorov. Unter anderem werden die Zusammenhänge zwischen Zufall, Informationsgehalt, Redundanz und Zeitaufwand in den Theorien erläutert.

In geschichtlicher Reihenfolge werden häufig genutzte verlustfreie Datenkompressionsverfahren (Huffmann, Arithmetic, LZ77, BWT, PPM) aufgeführt und eine Darstellung der Funktionsweise der Algorithmen gegeben. Der praktische Teil schliesst mit Vergleichstabellen über erzielbare Datenkompressionsraten, Zeitaufwände und Speicherbräuche.

Der abschliessende Teil führt in die irreversible Datenkompression für Bilder, Audio und Video ein.