

Einladung zum
**Kolloquium des
Instituts für Informatik**
07.11.2008, 13:30 Uhr
Übungsraum Ü2 des Instituts für Informatik (Vorbau Ludwig-Meyn-Str. 2)

Es spricht
Martin Novotny
Faculty of Electrical Engineering of the Czech Technical University in Prague

über das Thema
**Calculation of Time-Memory Trade-off (TMTO) tables for
cryptanalysis of A5/1**

Zusammenfassung:

Der Time-Memory Trade-off (TMTO) ist eine in der Kryptoanalyse angewandte Methode zum Angriff auf Verschlüsselungsverfahren. Hierbei wird ein Kompromiss zwischen Rechenzeit und Speicherplatz gefunden, welcher auf der gegebenen Hardware eine größt mögliche Ausschöpfung an Rechenleistung ergibt. Immer wiederkehrende Teilrechnungen werden einmalig vorberechnet und deren Terabyte große Mengen an Zwischenergebnissen in so genannten Rainbow-Tabellen auf Festplatten abgelegt. Diese Vorberechnungen sind äußerst zeitaufwändig, können jedoch mit Hardware beschleunigt werden. Der Vortrag gibt eine Einführung in das Thema der TMTO-Angriffe und behandelt die Möglichkeiten die Berechnung der Rainbow-Tabellen mittels Hardware zu beschleunigen.

Die Professoren und Dozenten
des Instituts für Informatik