

Im Rahmen eines

Kolloquiums des Fachbereiches

hält

Herr Prof. Dr. Jörg Keller
(Fernuniversität Hagen
Fakultät für Mathematik und Informatik)

am Donnerstag, dem 11. Mai, 16.00 Uhr s.t.
Ort: Informatikgebäude, von- Seckendorff-Platz 1
Hörsaal 1.26

einen Vortrag zum Thema:

**„Test von Generatoren für Stromverschlüssler und Pseudozufallszahlen durch
parallele Exploration des Zustandsraums“**

Kurzfassung:

Generatoren für Stromverschlüssler wie A5/1 und Pseudozufallszahlen sind normalerweise endliche Automaten, die nach der Initialisierung eine vollständig deterministische Zustandsfolge annehmen, und in jedem Zustand ein oder mehrere Bits ausgeben. Ihr Zustandsraum kann daher als endlicher gerichteter Graph modelliert werden, bei dem jeder Knoten genau eine ausgehende Kante zum Folgezustand hat. Jede schwache Zustandskomponente eines solchen Graphen besteht aus einem Zyklus und einer Reihe von zur Wurzel gerichteten Bäumen, wobei die Wurzeln auf dem Zyklus sitzen. Man ist normalerweise aus Sicherheitsaspekten an den Längen der Zyklen (Periodenlängen) sowie den Größen der Zusammenhangskomponenten interessiert: weichen diese zu sehr von den Erwartungswerten eines zufälligen Graphen ab, so könnte dies auf eine Designschwäche oder eine Hintertür hinweisen. Diese Größen können aber in der Regel nicht analytisch ermittelt werden, außerdem kann der Graph wegen seiner Größe nicht im Speicher konstruiert werden. Wir präsentieren einen parallelen Algorithmus, der einen solchen Graphen bei beschränktem Speicherplatz exploriert. Wir berichten über Laufzeiten sowie über die Strukturen der Graphen mehrerer Generatoren.

Alle Interessenten sind herzlich eingeladen.

Prof. Dr. L. Staiger
Dekan

