Meghívó

2011. január 12-én (szerdán) a DE IK *Kriptográfiai algoritmusok és protokollok* munkacsoportja workshopot rendez

Erősen párhuzamos algoritmusok prímfaktorizációra és a diszkrét logaritmus kiszámítására

A workshop helye: DE Matematikai Épület M 418 terem. Ideje: 10-17 óra.

Délelőtt olyan számelméleti algoritmusokról tervezünk előadásokat, amelyek a Turing modellben szubexponenciális időben faktorizálnak számokat, illetve számítják ki a diszkrét logaritmust.
Délután kvantum-, membrán- és intervallumszámítási modellekben vizsgáljuk a prímfaktorizáció és a diszkrét logaritmus számításának bonyolultságát.

Program:
10.00-10.05: Pethő Attila, Rövid köszöntő
10.05-10.35 Herendi Tamás (DE IK), Hatványozás gyorsítása tárolt adatok segítségével
10.35-11.05 Pethő Attila (DE IK), A faktorbázis módszer és a kvadratikus szita,
11.05-11.30 Kávészünet
11.30-12.00 Csirmaz László (DE IK, CEU), Számtest szita,
12.00-12.30 Varga Péter (DE IK), Indexkalkulus .

12.30-14.00 Ebédszünet

14.00-14.30 Ivanyos Gábor (MTA SZTAKI), Shor kvantum-algoritmusa diszkrét logaritmusra,
14.30-15.00 Csuhaj Varjú Erzsébet (MTA SZTAKI), Faktorizáció és kapcsolódó problémák membrán rendszerekben I,
15.00-15.30 Kávészünet
15.30-16.00 Vaszil György (MTA SZTAKI), Faktorizáció és kapcsolódó problémák membrán rendszerekben II,
16.00-16.30 Nagy Benedek (DE IK) és Vályi Sándor (NyF), Intervallum-értékű számítások és bonyolult számítási problémák megoldása.
16.30- Kötetlen beszélgetés

A kávészünetek és az ebédszünet fontos része a rendezvénynek, alkalmat ad szakmai beszélgetésekre, problémák megvitatására.