FIRST - Jövő Internet kutatások az elmélettől az alkalmazásig

TÁMOP-4.2.2.C-11/1/KONV-2012-0001

A Jövő Internet elméleti alapjai

Vaszil György

Debreceni Egyetem, Informatikai Kar

MAGYARORSZÁG MEGÚJUL

A projektek az Európai Unió támogatásával, az Európai Szociális Alap társfinanszírozásával valósulnak meg.

Kutatási témák

- Bizalmas adatok védelme, kriptográfiai protokollok

  DE IK Számítógéptudományi Tsz., MTA Atomki

- Informatikai hálózatok elméleti alapjai

  DE IK Számítógéptudományi Tsz., DE IK Alkalmazott Matematika és Valószínűségszámítás Tsz., ETIK

- Molekuláris kapcsolók mint informatikai tároló rendszerek

  DE TTK Elméleti Fizikai Tsz., DE IK Információ Technológia Tsz., MTA Atomki

1. Adatvédelem, kriptográfia

Vezető: Pethő Attila (DE IK Számítógéptudományi Tsz.)

- Kriptográfiai algoritmusok, protokollok analízise
  - Diofantikus egyenletek megoldhatóságán alapuló kulcscsere protokoll vizsgálata (Pethő. A.)
  - Hash függvények tervezése: A gyorsaság nem lehet fő konstrukciós elv
  - Kliens-szerver rendszerek: broadcast üzenetek hitelesítése, protokollok elemzése, módosítása (Pethő A., Herendi T., Folláth J.)
  - A PayWord mikrofizetési rendszer kiterjesztése több-boltos környezetre (fedezet ellenőrzés, fizetési információk titkossága, jóváhagyás, duplaköltés-védelem) (Huszti A.)

1. Adatvédelem, kriptográfia

- Anonimitás: e-szavazás, e-vizsgáztatás
  - Bilineáris leképezéseken alapuló hybrid mixnet tervezése, analízise (Huszti A., Kovács Z.)
- Véletlenszámok: a protokollok, algoritmusok építőelemei
  - Egyenletes eloszlású, nagy periódushosszúságú pszeudo-véletlen bitsorozatok generálása (Herendi T., Folláth J.)
- Automata-hálózatokon alapuló kriptorendszer (Dömösi P.)
  - Blokk titkosító, statisztikai vizsgálatok, lavinahatás (Horváth G.)

1. Adatvédelem, kriptográfia

- Kvantum információ feldolgozás: A biztonságot a fizika törvényei garantálják, emiatt kritikus az implelemntáció.→ Eszközfüggetlen kvantum információ feldolgozás.
  - Nemlokális kvantum korrelációkat kihasználó, biztonságosabb kvantumprotokollok létrehozása (kvantum titkosítás, bizonyítottan véletlen véletlenszám generálás) (Pál K., Vértesi T.)
  - A nemlokalitás és az összefonódottság (entanglement) kapcsolata (Pál K., Vértesi T.)

2. Informatikai hálózatok elméleti alapjai

Vezető: Mihálydeák Tamás (DE IK Számítógép-tudományi Tsz.)

- A bizonyosság hiányát kezelni képes döntési rendszerek elméleti hátterének kutatása. Életlen halmazok (rough sets) mint a homályosság, a nem egzakt sajátosságok modellje
  - Parciális approximációs tér, a fuzzyfikált „eleme”-reláció vizsgálatát lehetővé tevő új logikai rendszer (Csajbók Z., Mihálydeák T.)
  - Korrelációs klaszterezés a halmazapproximáció bázisán (Aszalós L.)

2. Informatikai hálózatok elméleti alapjai

- A halmazapproximáció általánosítása multihalmazokra, és alkalmazása a membrán számításokban, a membrán „határának” absztrakt fogalmi megalkotása (Csajbók Z., Mihálydeák T.)

2. Informatikai hálózatok elméleti alapjai

- Nemhagyományos számítási modellek és architektúrák
  - Párhuzamos számítások elméleti alapjául szolgáló párhuzamos számítási modellek fejlesztése, osztott automaták, Watson-Crick automaták (Nagy B.)
  - Kémiai számítási elv: számítás - egyszerű építőelemek lokális interakciói segítségével „emergens” módon létrejövő globális viselkedés. Membrán rendszerek, „kémiai” kalkulusok (Vaszil Gy., Battyányi P.)

2. Informatikai hálózatok elméleti alapjai

- Nagyméretű hálózatok matematikailag precíz modellezésére szolgáló új elméleti eszközök kidolgozása – szimulációs/kísérleti eredmények matematikai megalapozása
  - Spektrális klaszterezés – spektrális módszerek súlyozott élű gráfok csúcsklasztereinek meghatározására, hálózatokon folyó stratégiai interakciós játékok modelljeinek általánosítása (Bolla M.)
  - Fraktális természetű hálózatok, Apollóniai hálózatok – a való életben előforduló hálózatokhoz hasonló tulajdonságú modellek generálása (Kolossváry I., Vágó L.)

2. Informatikai hálózatok elméleti alapjai

- Barabási féle prioritási modell általánosítása, az emberi viselkedés dinamikájának leírása (Komjáthy J., Simon K., Vágó L.)

- Komplex hálózati folyamatok modellezése és vizsgálata
  - Nagy hálózatok struktúrájának megismerése mintavétellel, tulajdonság tesztelés
  - Csúcspáronkénti legrövidebb utak meghatározása

(Porvázsnyik B., Fazekas I.)

3. Molekuláris kapcsolók mint informatikai tárolórendszerek

Vezető: Vibók Ágnes (DE TTK Elméleti Fizikai Tsz.)

- Molekuláris kapcsoló: egy molekula két jól definiált stabilis állapottal, melyek között külső hatásra kapcsolható
  Mint adattároló: kis méret - nagy adatsűrűség, térbeli struktúra – párhuzamos olvasás lehetősége
  - Nemadiabatikus tulajdonságok vizsgálata – előre meghatározott paraméterekkel és tulajdonságokkal rendelkező kapcsoló kapcsoló molekulák tervezése

(Csehi A., Halász G., Vibók Á.)