UNIVERSITATEA TEHNICĂ "GHEORGHE ASACHI" DIN IAŞI
Facultatea de Automatică şi Calculatoare
Departamentul de Tehnologia Informației
Concurs pentru ocuparea postului de şef de lucrări, poz. 34
Disciplinele postului: Criptologie, Algoritmi paraleli şi distribuiţi

Tematica de concurs
privind
Prelegerea din aria tematică a postului

pentru ocuparea postului de şef de lucrări poziţia 34
din Statul de funcţii al Departamentului de Calculatoare
pe anul universitar 2023-2024

Criptologie

- Elemente matematice folosite în criptologie: teoria numerelor (ex. congruență, aritmetica modulo, etc.), câmpuri Galois, curbe eliptice
- Criptografie simetrică
- Cifruri orientate pe fluxuri de date
- Rețele Feistel
- Cifruri orientate pe blocuri de date
- Moduri de criptare ale cifrurilor orientate pe blocuri de date
- Criptografie asimetrică
- Cifru asimetric bazat pe problema factorizării numerelor întregi
- Schimbul de chei Diffie-Hellman
- Cifru asimetric bazat pe curbe eliptice
- Funcții HASH, autentificarea mesajelor criptate
- Probleme de securitatea a sistemelor criptografice
- Semnătura digitală
- Certificat digital
- Criptanaliza liniară
- Criptanaliza diferențială

Algoritmi paraleli şi distribuiţi

- Arhitecturi de calcul paralele/distribuite
- Modele de calcul paralele/distribuite
- Calcul de înaltă performanţă
- Comunicarea în sistemele de calcul paralel/distribuit
- Algoritmi paraleli fundamentali
- Sortare paralelă
- Algoritmi paraleli pentru calculul matricial
- Algoritmi paraleli pentru rezolvarea sistemelor de ecuații liniare
- Alegerea liderului

- Excluderea mutuală
- Echilibrarea încarcării
- Alocarea sarcinilor
- Programare OpenMP
- Programare Open MPI

Bibliografie:

1. D. Buşneag, F. Chirteş, D. Piciu, *Complemente de aritmetică şi teoria numerelor*, Ed. Gil, 2007
2. A. T. Murgan, R. Rădescu, *Corpuri finite - câmpuri Galois*, Ed. Printech, Bucureşti, 1998
3. C. Paar, J. Pelzl, *Understanding Cryptography - A Textbook for Students and Practitioners*, Springer-Verlag Berlin Heidelberg, 2010
4. R. G. Underwood, *Cryptography for Secure Encryption*, Springer, 2022
5. J. Antoine, *Algorithmic cryptanalysis*, Taylor and Francis Group, 2009
6. B. I. Groza, *Introducere în criptografie: funcţii criptografice, fundamente matematice şi computaţionale*, Ed. Politehnică, 2012
7. H. Attiya, J. Welch, *Distributed Computing: Fundamentals, Simulations and Advanced Topics,* John Wiley & Sons, 2004
8. K. Berman, J. Paul, *Algorithms: Sequential, Parallel, and Distributed,* Thomson Learning, 2005
9. V. Kumar, A. Grama A. Gupta, G Karypis, *Introduction to Parallel Computing: Design and Analysis of Algorithms,* Addison Wesley, 2003
10. T. Mattson, B. Sanders, B. Massingill, *Patterns for Parallel Programming*, Addison Wesley, 2005

Decan,
Prof. Vasile-Ion Manta

Director de departament,
Conf. Andrei Stan