Raport de activitate

Seminarul stiintific studentesc

Coordonator seminar: **Vlad-Florin Dragoi**
Facultatea de Stiinte Exacte
Universitatea Aurel Vlaicu din Arad

Septembrie 2020 – Decembrie 2023

Sumar. Activitatile seminarului stiintific au fost coordonate de catre Conf. univ. Dragoi Vlad-Florin cu sprijin din partea Lect. univ. Cowell R. Simon. Seminarul s-a tinut in general Vineri dupa-masa intre orele 14:00-18:00. Temele abordate au fost Teoria fiabilitatii retelelor, coduri corectoare de erori, criptografie post-cuantica. In primul an (2020-2021) s-au remarcat 3 studenti, Alin Lacatus, Alexandru Popovici si Andreea Szocs care au aprofundat tema criptografiei post-cuantice bazate pe coduri corectoare de erori. Acestia au avut rezultate ce au fost acceptate pentru prezentare si mai apoi publicate in proceedings la doua conferinte internationale. In anul urmator (2021-2022) Andreea Szocs si-a continuat activitatea de cercetare si a ajuns sa fie in prezent student doctorand la Universitatea din Szeged sub indrumare profesorului Gyorgy Turan. Anul urmator (2022-2023) studentii s-au dirijat spre o alta tema, mai exact, teoria fiabilitatii. Unele simulari facute de acestia sunt in prezent considerate pentru propunere in cadrul unei conferinte/jurnal international. Aici s-a remarcat Tibor Hegyi care a reusit sa implementeza si sa analizeze algoritmi de selectie eficienti bazati pe conceptul de beta-expansion.

1 Scopul seminarului stiintific

Indrumarea studentilor din cadrul Facultatii de Stiinte Exacte spre activitati de cercetare stiintifica

Activitatile noastre sunt indreptate spre realizarea acestui obiectiv. Motivatia principala este de a reda gust studentilor pentru stiinta. Acest aspect este bineinteles greu de cuantificat, prin urmare am stabilit urmatoarele obiective tangibile:

1. Cresterea capacitatii de a intelege si reproduce rezultate stiintifice
2. Imbunatatirea calitatii implementarilor de algoritmi
3. Familiarizarea si cresterea capacitatii de tehnoredactare a articolelor stiintifice

Pentru realizarea acestora am propus urmatoarele activitati:

1. Am organizat urmatoarele sesiuni tehnice de lucru:
   - Sesiune de explicatii/demonstratii a continutului unui articol
   - Sesiuni de implementare a algoritmilor

- Sesiuni de analiza a datelor
- Sesiuni de instruire pentru generarea de figuri/tabele pentru tehnoredactare/prezentare

2. Am sustinut interactiunea studentilor cu cercetatori din alte laboratoare si centre de cercetare:
   - Am sustinut participare studentilor din cadrul seminarului la conferinte nationale si internationale (SOFA, CBCrypto, IMACC, WSTC)
   - Am sprijinit financiar din cadrul proiectelor de cercetare (PN-III-P1-1.1-PD-2019-0285, PN-III-P4-ID-PCE-2020-2495)
   - Am indrumat si coordonat realizarea prezentarilor pentru conferinte
   - Am facilitat legatura studentilor cu alti cercetatori, atat din cadrul facultatii, precum si cercetatori din afara universitatii (colegi de proiecte sau colaboratori din Romania si Franta)

2 Activitati realizate

Rezultate stiintifice

Structura codurilor de tip self-dual monomial: A fost analizata in detaliu structura codurilor monomiale descrescatoare auto-duale folosite intr-o schema de tip McEliece. Resultatele arata un nivel de securitate identic cu cel al codurilor de tip Reed-Muller in anumite cazuri. Publicarea acestor rezultate a fost facuta in cadrul conferintei IMACC.

Analiza securitatii practica a criptosistemului McEliece: S-a analizat securitatea criptosistemelor propuse spre standardizare in cadrul competitiei internationale organizata de NIST. Mai exact, s-a analizat o optimizare combinatorica a unui algoritm pentru problema sindromului intreg. Rezultatul a fost prezentat la conferinta SOFA2020, in cadrul uneu sesiuni speciale pe criptografie.

Algoritmi eficienti de ordonare a fiabilitatii retelelor S-au implementat solutii de ordonare a fiabilitatii retelelor de tip Matchstick Minimal Networks. Problema aceasta desi a fost abordata in mai multe articole, este una dificila. Algoritmii propusi combina metode eficiente de ordonare a vectorilor binari, metode compatibile cu fiabillitatea retelelor mai sun mentionate. In momentul dat suntem in curs de redactare a cestor rezultate.

Comunicare si diseminare - Participari conferinte

In ciuda faptului ca activitatea seminarului a fost demarata in timpul pandemiei mondiale de COVID19, fapt ce a impus o serie de restrictii legate de modalitatile de deplasare si organizare evenimente, am reusit totusi sa participam fizic la conferinte si workshopuri.

- **Noiembrie 2020**: Sofa 2020 (`https://www.sofa-org.eu/2020/`) Virtual, Arad, Romania. In cadrul unei sesiuni speciale pe criptografie (Advances in Cryptology), studentul Alexandru Popovici a prezentat rezultatele obtinute impreuna cu colegul sau Alin Lacatus. Interactiunea cu participantii de la cele doua sesiuni a fost extrem de interesanta si promitatoare pentru studenti. Cercetatori din Romania, Franta si Slovacia au fost curiosi si au propus colaborari pe subiecte de interes comun cum ar fi: analiza schemelor de criptare bazate pe coduri corectoare de erori, sau analiza unor structuri prezente in teoria informatiei cuantice (teorie prezenta in tendintele criptografiei moderne).

- **Decembrie 2021**: Imacc 2021 (IMACC2021) Virtual, Oxford, UK. Aceasta conferinta internationala pe coduri si criptografie este organizata de Institutul de Matematica si Aplicatii din Regatul Unit al Marii Britanii. Acolo am fost prezenti cu un articol realizat de catre Andreea Szoca impreuna cu Vlad-Florin Dragoi.
- **Martie 2022**: WSTC 2022 - Spring `https://www.wstc.flt-info.eu/spring2022/` Sinaia, Romania. Acesta este primul workshop organizat la nivel national pe subiectul cryptografiei post-cuantice. Au participat cercetatori din Franta si Romania scopul fiind initierea si dezvoltarea unei nucleu de cercetatori pe subiecte de actualitate in criptografie. In cadrul acestui eveniment am difuzat posibile proiecte de cercetare si colaborari precum si subiecte de teze de doctorat pentru studenti. Studenta Andreea Szocs a participat la acesta conferinta unde a facut o prezentare legata de rezultatele ei de la IMACC 2021.
- **Mai 2022**: CBCrypto 2022 `https://www.cb-crypto.org/home` Virtual/Trondheim, Norvegia. La acesat conferinta Andreea Szocs a prezentat ultimele ei rezultate legate de coduri monomiale descrescatoare aplicate in criptografie.

Cercetatori, universitati implicate: Vizibilitatea seminarului si a studentilor, prin prisma rezultatelor lor este adusa de numarul si calitatea laboratoarelor de cercetare precum si a cercetatorilor cu care acestia interactioneaza. Fie in cadrul lucrarilor publicate, ori in cadrul conferintelor/intalnirilor la care studentii au participat, am incercat sa implicam universitati si cercetatori de renume alaturi de studenti. Au fost implicate 2 universitati din Franta: Universitatea Jean-Monet din Saint-Etienne prin cativa membrii ai echipei SESAM (Pierre-Louis Cayrel, Vincent Grosso, Lilian Bossuet), Universitatea din Grenoble prin echipa TIMA (Brice Colombier). Din Romania mentionam 2 universitati, mai exact Universitatea Aurel Vlaicu din Arad (Vlad-Florin Dragoi, Andreea Szocs, Dominic Bucerzan, Valeriu Beiu, Sorin Hoara, Alin Lacatus, Alexandru Popovici), Universitatea Alexandru Ioan Cuza din Iasi (Ferucio Laurentiu Tiplea).

Actuale/viitoare grupuri de cercetare: Activitatile seminarului nu doar ca s-au aliniat cu doua grupuri de cercetare dar au si alimentat activitati comune, in special legate de grupul de cercetare pe criptografie post-cuantica. Acest grup a reusit sa coalizeze studenti si viitori doctoranzi, precum Andreea Szocs, Alin Lacatus, Alexandru Popovici. Dintre acesti studenti unul a optat pentru o viitoare cariera in cercetare, mai precis Andreea Szocs care a aplicat pentru o teza de doctorat la Universitatea din Szeged, unde studiaza in prezent felul in care Inteligenta Artificiala poate raspunde unor intrebari dificile din Teoria Codurilor corectoare de erori.

Lista articole/abstracturi:

- Vlad-Florin Dragoi, Andreea Szocs, Structural properties of self-dual monomial codes with application to code-based cryptography. *IMA International Conference on Cryptography and Coding, IMACC 2021*, Dec. 2021, Virtual (Rank B in CORE).
- Vlad-Florin Dragoi, Alin Tiberiu Lacatus, Alexandru Popoviciu: Algorithms for integer syndrome decoding problem, *9th International Workshop on Soft Computing Applications,SOFA 2020*, Nov. 2020 Arad, Romania (Rank C in CORE)
- Vlad-Florin Dragoi, Andreea Szocs: Cryptanalysis of some McEliece Variants based on Monomial Codes *CBCrypto 2022*

Participari/prezentari la conferinte unde au fost acceptate articole sau abstracte

1. CBCrypto 2022, May 2022, Trontheim, Norway (2 abstracturi)
2. WSTC 2022, Mars 2022, Sinaia, Romania (2 abstracturi)
3. SOFA 2020, Dec. 20202, Arad, Romania (1 articol)