Dragoș Rotaru

r.dragos0@gmail.com • https://rdragos.github.io
dragos-alin-rotaru • DragosRotaru • rdragos

Research Interests

I am interested in applying cryptography to solve real world problems. In the last years my focus was to improve, develop and implement multiparty computation protocols. These protocols allow several parties to compute on private data without revealing it.

Education

University of Bristol **Bristol, UK**
Ph.D. candidate in Computer Science *2016 – Mar 2020 (expected)*
Open source contributor to SPDZ and SCALE-MAMBA, two privacy preserving frameworks which compute on secret data without revealing it.
From the beginning of 2018 I have been working in the COSIC research group of KU Leuven University.
- Thesis title (submitted): Optimizing Secure Multiparty Computation Protocols for Dishonest Majority.
- Advisor: Prof. Nigel Smart.

Faculty of Mathematics and Informatics, University of Bucharest **Bucharest, Romania**
B.Sc. in Computer Science *2012–2015*

Work Experience

Microsoft Research **Redmond, WA, USA**
Research Intern *06/2019-09/2019*
- Worked closely with a senior .NET developer to speed-up an internal cryptographic library.
- Research on privacy preserving analytics.

BitDefender **Bucharest, Romania**
Junior Researcher *07/2015–01/2016*
- Studied techniques to efficiently compute on encrypted data.
- Helped the security team in some Capture the Flag competitions. Amongst the various tasks I did there, one was to break some implementations of random number generators (*rand()* function) in various compilers.

Adobe **Bucharest, Romania**
Tech intern *06/2014-09/2014*
- Researched and implemented new methods for image keyword retrieval. Check the release here!

Honors and Achievements

Qualification for ACM-ICPC NWERC with a team from University of Bristol *2016*
Finalist, National Programming Contest 'Algoritmiada', Romania *2014*
Qualification for ACM-ICPC SEERC with a team from University of Bucharest *2013*
Silver medal (8'th place) at the National Olympiad in Informatics, Romania *2012*
Qualification for the National Olympiad in Informatics, Romania *2010, 2011*

Teaching Experience

University of Bristol **Bristol, UK**
Teaching Assistant *2016 – 2018*

- Theory of Computation.
- Introduction to ACM-ICPC contests.
- Data Structures and Algorithms.
- Cryptography A.

University of Bucharest **Bucharest, Romania**
Teaching Assistant *2014-2016*

- Introduction to Competitive Programming.
- Graph Algorithms.
- Data Structures and Algorithms.

Community Projects

Romanian National Informatics Committee **Romania**
Member *2013 – 2014*

Part of the group responsible with the organization of National Olympiad in Informatics and selection of contestants which represent Romania at the International Olympiad.

- I proposed some algorithmic tasks and helped others by implementing and testing alternative solutions.

CDL **Bucharest, Romania**
Student *2013 – 2014*

- Contributed to a project which posts relevant statistics of the Romanian Members of Parliament, mostly by building crawlers for various websites. Dealt with PyQuery, Flask, HTML, Git.

Programming Languages

C/C++, Python, LaTeX.

Additional information

- External Reviewer for PKC 2017, ASIACRYPT 2018, CCS 2018, CRYPTO 2018, CT-RSA 2019, EUROCRYPT 2019, EUROCRYPT 2020, PKC 2020.
- Conference talks at CCS 2016, ACNS 2017, FSE 2018, EUROCRYPT 2018, WAHC 2019, INDOCRYPT 2019.

Publications

Throughout my doctoral studies I have been a co-author of 12 papers out of which 9 are already published at conferences. For a complete list please check out my website.

References

Available upon request.