Andreea Beatrice Alexandru

aalexandru@dualitytech.com
https://andreea-alexandru.github.io
https://github.com/andreea-alexandru

Summary

- Researcher with expertise in privacy-preserving strategies for data processing, fully homomorphic encryption and multi-party computation for distributed cryptographic protocols and cyber-physical systems
- Goal: shape security and privacy research and deployment for real-world impact

Professional Experience

Cryptography Scientist at Duality Technologies
https://dualitytech.com/ 01.2023–present

- Conduct research in privacy-preserving technologies
- Develop and optimize software libraries for encrypted computations

Postdoctoral Associate at the University of Maryland, College Park
Department of Computer Science, Maryland Cybersecurity Center 07.2021–01.2023

- Conducted research in consensus algorithms, robust differential privacy, privacy-preserving control algorithms using homomorphic encryption and garbled circuits
- Managed research projects with faculty and students and organized seminars

Research Assistant at the University of Pennsylvania
Department of Electrical and Systems Engineering, GRASP Lab, PRECISE, Seclab 08.2015–05.2021

- Designed and implemented privacy-preserving algorithms for cyber-physical systems using homomorphic encryption and secure multi-party computation
- Designed and analyzed algorithms for local observability of distributed systems
- Organized seminars and co-managed group research meetings

Cryptography Intern at Duality Technologies
https://dualitytech.com/ 05.2019–08.2019

- Designed applications of encrypted computing technologies, prototyped and implemented encrypted computing applications
- Developed and optimized computing software libraries for fully homomorphic encryption

Teaching Assistant at the University of Pennsylvania
Introduction to Linear Optimization ESE 504 08.2017–12.2017
Modern Convex Optimization ESE 605 01.2017–05.2017

- Held office hours, tutorials and taught classes

Research Intern at Philips Research Netherlands
Department of Chronic Disease Management 06.2014–09.2014

- Data mining for Impedance Cardiography
- Automated diagnosis and classification of heart failure

Research Assistant at the Laboratory of Numerical Modeling
Department of Electrical Engineering, University Politehnica of Bucharest 10.2012–10.2013

- Geometric information processing for electric circuits, code optimization

Education

University of Pennsylvania
Ph.D. in Electrical and Systems Engineering 2015–2021

- Thesis: *Cryptographic Foundations for Control and Optimization—Making Cloud-based and Networked Decisions on Encrypted Data*
- Advisors: George J. Pappas, Ali Jadbabaie (year I)
- Committee members: Manfred Morari, Tal Rabin, Sebastian Angel
- GPA 4.00/4

University Politehnica of Bucharest
B.Eng. in Automatic Control and Computer Science 2011–2015

- Thesis: *An analysis of performance measures for prediction algorithms in telemonitoring systems*
- GPA 9.78/10, valedictorian in Systems Engineering major

Honors

- Charles Hallac and Sarah Keil Wolf Award for Best Doctoral Dissertation 2022
- Fellowship for the Diversity, Equity and Inclusion Committee in the UPenn ESE Department 2021
- EECS Rising Star 2019
- ACM Student Research Competition, Grace Hopper Celebration 2019
- Finalist for best paper award, International Conference on Cyber-Physical Systems, ACM/IEEE 2019
- Finalist for student best paper award, American Control Conference, IEEE 2019
- NSF iREDEFINE Professional Development Award 2019
- Full scholarship, Women in CyberSecurity Conference 2018
- Erasmus Mobility Placement grant 2014
- First prize at Student Scientific Communications Session, University Politehnica of Bucharest 2013,2015
- Finalist for student best paper award, Advanced Topics in Electrical Engineering Conference, IEEE 2013
- Annual merit scholarships in college and high school 2007–2015
- Travel awards: Maryland Cybersecurity Center Travel Award, University of Maryland Postdoctoral Conference Support Award 2022, 2021, Conference on Decision and Control (CDC) Travel Award 2020, 2017, Grace Hopper Celebration 2019

Publications

Conferences:

- **Alexandru A. B.**, Blum E., Katz J. and Loss J., *State Machine Replication under Changing Network Conditions*, in International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT), Cham: Springer Nature Switzerland, pp. 681–710, 2022.
- **Alexandru A. B.**, Burbano L., Celiktuğ M. F., Gomez J., Cardenas A. A., Kantarcioglu M., Katz J., *Private Anomaly Detection in Linear Controllers: Garbled Circuits vs. Homomorphic Encryption*, in Proceedings of the 61st Conference on Decision and Control, pp. 7746–7753, IEEE, 2022.
- **Alexandru A. B.**, Tsiamis A. and Pappas G. J., *Encrypted Distributed Lasso for Sparse Data Predictive Control*, in Proceedings of 60th IEEE Conference on Decision and Control, pp. 4895–4900, 2021.
- **Alexandru A. B.**, Tsiamis A. and Pappas G. J., *Towards Private Data-driven Control*, in Proceedings of 59th IEEE Conference on Decision and Control, pp. 5449–5456, 2020.
- **Alexandru A. B.** and Pappas G. J., *Private Weighted Sum Aggregation for Distributed Control Systems*, 21st International Federation of Automatic Control (IFAC) World Congress, Elsevier, pp. 11081–11088, 2020.
- **Alexandru A. B.**, Schulze Darup M. and Pappas G. J., *Encrypted Cooperative Control Revisited*, in Proceedings of 58th IEEE Conference on Decision and Control, pp. 7196–7202, 2019.
- **Alexandru A. B.** and Pappas G. J., *Encrypted LQG using Labeled Homomorphic Encryption*, in Proceedings of 10th ACM/IEEE International Conference on Cyber-Physical Systems, pp. 129–140, 2019. **Best paper award finalist**.
- Tsiamis, A., **Alexandru, A. B.** and Pappas, G. J., *Motion Planning with Secrecy*, in Proceedings of the IEEE American Control Conference (ACC), pp. 784–791, 2019. **Best student paper award finalist.**
- **Alexandru A. B.**, Morari M. and Pappas G. J., *Cloud-based MPC with Encrypted Data*, in Proceedings of the 57th IEEE Conference on Decision and Control, pp. 5014–5019, 2018.

- **Alexandru A. B.**, Pequito S., Jadbabaie A. and Pappas G. J., *On the Limited Communication Analysis and Design for Decentralized Estimation*, in Proceedings of the 56th IEEE Conference on Decision and Control, pp. 1713–1718, 2017.
- **Alexandru A. B.**, Gatsis K. and Pappas G. J., *Privacy preserving Cloud-based Quadratic Optimization*, in Proceedings of the 55th IEEE Allerton Conference on Communication, Control, and Computing, pp. 1168–1175, 2017.
- **Alexandru A. B.**, Pequito S., Jadbabaie A. and Pappas G. J., *Decentralized observability with limited communication between sensors*, in Proceedings of the 55th IEEE Conference on Decision and Control, pp. 885–890, 2016.
- **Alexandru A. B.**, Lup S., Dita B., *GDS2M: Preprocessing Tool for MEMS Devices*, in Proceedings of the 8th IEEE International Symposium on Advanced Topics in Electrical Engineering, pp. 1–4, 2013. **Best student paper award finalist.**

Journals and book chapters:

- Geva R., Gusev A., Polyakov Y., Liram L., Rosolio O., **Alexandru A. B.** Blatt M., Duchin Z., Waissengrin B., Mirelman D., Bukstein F., Blumenthal D. T., Wolf I., Pelles S., Schaffer T., Lavi L. A., Micciancio D., Vaikuntanathan V., Al Badawi A., and Goldwasser S., *Collaborative Privacy-Preserving Analysis of Oncological Data using Multiparty Homomorphic Encryption*, Proceedings of the National Academy of Sciences, 120(33), e2304415120, 2023.
- **Alexandru A. B.** and Pappas G. J., *Private Weighted Sum Aggregation*, IEEE Transactions on Control of Networked Systems, 9(1), pp. 219–230, 2021.
- Schulze Darup M., **Alexandru A. B.**, Quevedo D. E. and Pappas G. J., *Encrypted control for networked systems – An illustrative introduction and current challenges*, IEEE Control Systems, 41(3), pp. 58–78, 2021.
- **Alexandru A. B.**, Pappas G. J., *Secure Multi-party Computation for Cloud-Based Control.* In: Farokhi F. (eds) Privacy in Dynamical Systems, pp. 179–207, 2020, Springer, Singapore.
- **Alexandru A. B.**, Gatsis K., Shoukry Y., Seshia S. A., Tabuada P. and Pappas G. J., *Cloud-based Quadratic Optimization with Partially Homomorphic Encryption*, IEEE Transactions on Automatic Control (TAC), 66(5), pp. 2357–2364, 2020.

Preprints:

- **Alexandru A. B.**, Loss J., Papamanthou C. and Tsimos G., *Sublinear-round Broadcast without trusted setup against dishonest majority*, eprint `https://eprint.iacr.org/2022/1383.pdf`.
- **Alexandru A. B.**, Tsiamis A. and Pappas G. J., *Data-driven Control on Encrypted Data*, arXiv preprint `https://arxiv.org/abs/2008.12671`.

Invited talks and posters (excluding conference presentations)

- *Building blocks for Threshold FHE*, NIST Workshop on Multi-party Threshold Schemes, virtual — Sep 2023
- *State Machine Replication under Changing Network Conditions*, MongoDB Advanced Cryptography Group, New York City, NY — Jul 2023
- *Opportunities and Challenges of using Cryptography for CPS Security*, Workshop on CPS security, CDC, Cancun, Mexico — Dec 2022
- *Data-Driven Control over Encrypted Data*, Autonomous Systems Laboratory, Stanford University, virtual — Jul 2021
- *Privacy for Cyber-Physical Systems*, EECS Rising Stars at UIUC, Champaign, IL — Oct 2019
- *Private Cooperative Control*, Grace Hopper Celebration, ACM Student Research Competition, Orlando, FL — Oct 2019
- *Privacy for Cyber-Physical Systems*, iREDEFINE workshop, ECEDHA Annual Conference and ECExpo, Tucson, AZ — Mar 2019
- *Cloud-based Model Predictive Control on Encrypted Data*, ESE Department PhD Colloquium, University of Pennsylvania, Philadelphia, PA — Oct 2018
- *Privacy preserving Cloud-based Quadratic Optimization*, 5th Annual Women in Cybersecurity Conference, Chicago, IL — Mar 2018

- *Privacy Preserving Cloud-based Quadratic Optimization*, ESE Department PhD Colloquium, University of Pennsylvania, Philadelphia, PA — Oct 2017
- *Secure Cloud-outsourced Optimization Problems through Homomorphic Encryption*, Intel-NSF Center on Cyber Physical System Security, Hillsboro, OR — Aug 2017
- *GDS2M: Preprocessing Tool for MEMS Devices*, Scientific Communications Session, "Politehnica" University of Bucharest, Romania — May 2015
- *Analysis of performance measures for prediction algorithms in telemonitoring systems*, Scientific Communications Session, "Politehnica" University of Bucharest, Romania — May 2013

Skills

- Programming: Python, C/C++, MATLAB (proficient), Oracle SQL, Java (past experience)
- Languages: Romanian (native), English (proficient), French (conversational), Spanish (beginner)

Professional service

- Reviewer: Elsevier Annual Reviews in Control 2023, IEEE Transactions of Automatic Control 2017–2022, IEEE Transactions on Control of Network Systems 2019, 2020, 2022, IEEE Transactions on Cloud Computing 2022, IEEE Transactions on Dependable and Secure Computing 2021, IEEE Open Journal of Control Systems 2022, IEEE Control System Letters 2021, 2022, IFAC Automatica 2020, 2021, IEEE Conference on Decision and Control 2016–2022, IEEE American Control Conference 2017–2021, ACM/IEEE International Conference on Cyber-Physical Systems 2018, IFAC World Congress 2020, 2023, ACM Conference on Computer and Communications Security 2022
- Program committee: CONTROLLO'2022, WAHC 2023
- Co-organizer and co-chair of the invited sessions "Encrypted Control and Optimization" at the 58th, 59th, 60th, 61st and 62nd Conference on Decision and Control 2019–2023
- Co-organizer of the DC area crypto-day in 2021 `https://dcareacryptoday.wordpress.com/`.

Outreach

- Fellow of the Electrical and Systems Engineering Diversity, Equity and Inclusion Committee — 2021
- Presenter at Grace Hopper Celebration (GHC) — 2019
- Instructor of Electrical Engineering at Girls in Engineering, Math and Science (GEMS) — 2018
- Presenter at Women in Cybersecurity Conference (WiCyS) — 2018
- Member of UPenn Women Community in Science, Technology, and Engineering — 2015-2021

Workshops and Certificates

- Lattices: Algorithms, Complexity, and Cryptography Workshops at the Simons Institute for the Theory of Computing — 2020
- Deep Learning specialization by deeplearning.ai on Coursera (5 courses) — 2019
- Optimization with IBM ILOG OPL Training by Linux Competence Center and IBM — 2014
- National Instruments Certified LabVIEW Associate Developer (CLAD) — 2014
- Applied Electronics Training by EAP InGear Laboratory and Microchip — 2013–2014