Andreea Beatrice Alexandru

https://andreea-alexandru.github.io
Google Scholar page

Summary

• Researcher specializing in privacy-preserving data processing, fully homomorphic encryption, and multi-party computation for distributed protocols and cyber-physical systems
• Goal: Advance security and privacy technologies toward real-world deployment and impact

Professional Experience

Senior Scientist at Duality Technologies
Hoboken, New Jersey 02.2025–present

• Co-Principal Investigator of the SHARE program, awarded by the Advanced Research Projects Agency for Health (ARPA-H)
  – Leading research on scalable and secure collaboration for privacy-preserving medical pipelines
  – Directing the implementation of a computational open-source framework for performing encrypted medical analytics over federated data
  – Managing project execution and cross-organizational collaboration
• Leading research in privacy-preserving technologies for secure data querying and evaluation
• Developing and optimizing open-source software libraries (OpenFHE, NVFlare) for encrypted computations using fully homomorphic encryption and federated learning

Scientist at Duality Technologies
Hoboken, New Jersey 01.2023–02.2025

• Technical project lead for the DPRIVE TREBUCHET program, awarded by the Defense Advanced Research Projects Agency (DARPA)
  – Designed and implemented conversion algorithms between homomorphic encryption and symmetric ciphers
  – Designed and implemented solutions for performing batched functional bootstrapping for arbitrary function evaluations over encrypted data
• Conducted research in privacy-preserving technologies
• Developed and optimized software libraries (OpenFHE) for encrypted computations using fully homomorphic encryption and garbled circuits

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
Newark, New Jersey 05.2019–08.2019

• Designed applications of encrypted computing technologies, prototyped and implemented encrypted computing applications

- Developed and optimized software libraries (PALISADE) 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 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 (first year)
- GPA 4.00/4

University Politehnica of Bucharest
B.Eng. in Automatic Control and Computers 2011–2015
- Thesis: *An analysis of performance measures for prediction algorithms in telemonitoring systems*
- GPA 9.78/10

Honors

- Charles Hallac and Sarah Keil Wolf Award for Best Doctoral Dissertation 2022
- 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
- Valedictorian in Dept. of Automatic Control and Systems Engineering, "Politehnica" University 2015
- 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

Publications

Conferences:

• Dumezy J., **Alexandru A. B.**, Polyakov Y., Clet P.-E., Chakraborty O., and Boudguiga A., *Evaluating Larger Lookup Tables using CKKS*, accepted to Transactions of Cryptographic Hardware and Embedded Systems (TCHES) 2025.

• Adamek J., Aikata A., Al Badawi A., **Alexandru A. B.**, Arakelov A., Binfet P., Correa V., Dumezy J., Gomenyuk S., Kononova V., Lekomtsev D., Maloney V., Nguyen C.-H., Polyakov Y., Pianykh D., Shaul H., Schulze Darup M., Teichrib D., Tronin D. and Arakelov G., *FHERMA Cookbook: FHE Components for Privacy-Preserving Applications*, in Proceedings of the 13th Workshop on Encrypted Computing & Applied Homomorphic Computing (WAHC), pp. 68–76, 2025.

• **Alexandru A. B.**, Kim A. and Polyakov Y., *General functional bootstrapping using CKKS*, in Annual International Cryptology Conference (CRYPTO), Cham: Springer Nature Switzerland, pp. 304–337, 2025.

• **Alexandru A. B.**, Loss J., Papamanthou C., Tsimos G. and Wagner B., *Sublinear-Round Broadcast without Trusted Setup*, in Proceedings of the 2025 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA), Society for Industrial and Applied Mathematics, pp. 4132–4171, 2025.

• **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. and 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:

• **Alexandru A. B.**, Al Badawi A., Micciancio D. and Polyakov Y., *Application-aware approximate homomorphic encryption: Configuring FHE for practical use*, IACR Communications in Cryptology (CiC), 2(4), 2026.

• 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.** and 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.

Technical Reports:

• Al Badawi A., **Alexandru A. B.**, Bates J., Bergamaschi F., Cousins D. B., Erabelli S., Genise N., Halevi S., Hunt H., Kim A., Lee Y., Liu Z., Micciancio D., Pascoe C., Polyakov Y., Quah I., R.V. S., Rohloff K., Saylor J., Suponitsky D., Triplett M., Vaikuntanathan V. and Zucca V., *OpenFHE: Open-Source Fully Homomorphic Encryption Library*, Cryptology ePrint Archive `https://eprint.iacr.org/2022/915`

Preprints:

• **Alexandru A. B.**, Kim A., Polyakov Y. and Zheng H., *Sparse Hermite Interpolation Method for Discrete-CKKS Functional Bootstrapping*, eprint `https://eprint.iacr.org/2026/1026`.

• Al Badawi A., **Alexandru A. B.**, Polyakov Y. and Vaikuntanathan V., *SoK: Private LLM Inference using Approximate Homomorphic Encryption*, eprint `https://eprint.iacr.org/2026/935`.

• **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)

• *A New Benchmarking Suite for FHE*, FHE.org Conference, Taipei, Taiwan 03.2026

• *Latest trends and results in PPML using FHE*, CRYPTO PPML Workshop, Santa Barbara, CA 08.2025

• *Privacy-Preserving Data Sharing across Financial Institutions*, NIST Workshop on Privacy-Enhancing Cryptography (WPEC2024), virtual 09.2024

• *Building blocks for Threshold FHE*, NIST Workshop on Multi-party Threshold Schemes (MPTS2023), virtual 09.2023

• *State Machine Replication under Changing Network Conditions*, MongoDB Advanced Cryptography Group, New York City, NY 07.2023

• *Opportunities and Challenges of using Cryptography for CPS Security*, Workshop on CPS security, CDC, Cancun, Mexico 12.2022

• *Data-Driven Control over Encrypted Data*, Autonomous Systems Laboratory, Stanford University, virtual 07.2021

• *Privacy for Cyber-Physical Systems*, EECS Rising Stars at UIUC, Champaign, IL 10.2019

• *Private Cooperative Control*, Grace Hopper Celebration, ACM Student Research Competition, Orlando, FL 10.2019

• *Privacy for Cyber-Physical Systems*, iREDEFINE workshop, ECEDHA Annual Conference and ECExpo, Tucson, AZ 03.2019

• *Cloud-based Model Predictive Control on Encrypted Data*, ESE Department PhD Colloquium, University of Pennsylvania, Philadelphia, PA 10.2018

• *Privacy preserving Cloud-based Quadratic Optimization*, 5th Annual Women in Cybersecurity Conference, Chicago, IL 03.2018

• *Privacy Preserving Cloud-based Quadratic Optimization*, ESE Department PhD Colloquium, University of Pennsylvania, Philadelphia, PA 10.2017

• *Secure Cloud-outsourced Optimization Problems through Homomorphic Encryption*, Intel-NSF Center on Cyber Physical System Security, Hillsboro, OR 08.2017

Skills

• Research Expertise: advanced cryptography (fully homomorphic encryption; secure multi-party computation; post-quantum), privacy-preserving machine learning, information retrieval and distributed algorithms

• Programming & Scientific Computing: C/C++, Python (proficient), MATLAB, Oracle SQL, Java (prior experience)

• Cryptographic Libraries & Applied ML: OpenFHE (core developer), NVFlare, PyTorch (working knowledge)

• Languages: Romanian (native), English (proficient), French (conversational), Spanish (beginner)

Professional service

• Co-manager of the Use Cases and Benchmarks workgroup as part of HomomorphicEncryption.org `https://homomorphicencryption.org/` 2024–present.

• Co-organizer of the invited sessions "Encrypted Control and Optimization" at the Conference on Decision and Control 2019–2025, and co-chair for 2019–2022.

• Program committee: CONTROLO'2022, WAHC'2023 and 2025, FHE.org'2026.

• Challenge committee member for FHERMA challenges `https://fherma.io/challenges` 2024–present.

• Co-organizer of the DC area crypto-day in 2021 `https://dcareacryptoday.wordpress.com/`.

• Reviewer: IEEE Transactions on Dependable and Secure Computing 2024, 2021, Elsevier Annual Reviews in Control 2023, IEEE Transactions of Automatic Control 2017–2022, 2024, IEEE Transactions on Control of Network Systems 2019, 2020, 2022, IEEE Transactions on Cloud Computing 2022, 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, 2024–2026, 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, ACM ASIA Conference on Computer and Communications Security 2024, EUROCRYPT 2026, ASIACRYPT 2026.