Alexander R. Block
alexander.r.block@gmail.com
block9@purdue.edu

June 21, 2022
alexblock.io

Current Position

(January 2016 - Present)
Graduate Research Assistant
Computer Science Department
Purdue University
West Lafayette, IN 47907

Email: block9@purdue.edu
Homepage: alexblock.io

Past Positions

(June 2019 - August 2019)
Graduate Research Fellow
FACT Center
IDC Herzliya
Herzliya, Israel 4610101

(August 2015 - December 2019)
Graduate Teaching Assistant
Computer Science Department
Purdue University
West Lafayette, IN, USA 47907

Education

Ph.D. in Computer Science, Purdue University, August 2022.

Advisor: Jeremiah Blocki

Committee: Jeremiah Blocki (Purdue University), Mikhail Atallah (Purdue University), Elena Grigorescu (Purdue University), Christina Garman (Purdue University), Ron Rothblum (Technion), David Gleich (Purdue University)

Dissertation Title: Exploring the Composition of Coding Theory and Cryptography through Secure Computation, Succinct Arguments, and Local Codes

M.Sc. in Computer Science, Purdue University, May 2019.

B.S. in Mathematics and Information & Computer Science, University of California, Irvine, June 2015.

Graduate with Honors from the Campuswide Honors Collegium and the Department of Mathematics

Honors Research Thesis: Combined Games

Research

Interests

Succinct Interactive Arguments, Polynomial Commitment Schemes, Zero-Knowledge, Locally Decodable Codes, Applications of Coding Theory to Cryptography, Applications of Cryptography to Coding Theory

Publications

All authors listed alphabetically. Entries appear in reverse chronological order.

Mohammad Hassan Ameri, Alexander R. Block, and Jeremiah Blocki. *Memory-Hard Puzzles in the Standard Model with Applications to Memory-Hard Functions and Resource-Bounded Locally Decodable Codes*. Cryptology ePrint Archive, Report 2021/801. SCN 2022 (to appear). 2021. URL: https://ia.cr/2021/801

Alexander R. Block, Justin Holmgren, Alon Rosen, Ron D. Rothblum, and Pratik Soni. "Time- and Space-Efficient Arguments from Groups of Unknown Order". In: *Advances in Cryptology - CRYPTO 2021 - 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16-20, 2021, Proceedings, Part IV*. ed. by Tal Malkin and Chris Peikert. Vol. 12828. Lecture Notes in Computer Science. Springer, 2021, pp. 123–152. DOI: 10.1007/978-3-030-84259-8_5

Alexander R. Block, Simina Brânzei, Hemanta K. Maji, Himanshi Mehta, Tamalika Mukherjee, and Hai H. Nguyen. "P_4-free Partition and Cover Numbers & Applications". In: *2nd Conference on Information-Theoretic Cryptography (ITC 2021)*. Ed. by Stefano Tessaro. Vol. 199. Leibniz International Proceedings in Informatics (LIPIcs). Dagstuhl, Germany: Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2021, 16:1–16:25. DOI: 10.4230/LIPIcs.ITC.2021.16

Alexander R. Block and Jeremiah Blocki. "Private and Resource-Bounded Locally Decodable Codes for Insertions and Deletions". In: *IEEE International Symposium on Information Theory, ISIT 2021, Melbourne, Australia, July 12-20, 2021*. IEEE, 2021, pp. 1841–1846. DOI: 10.1109/ISIT45174.2021.9518249

Alexander R. Block, Jeremiah Blocki, Elena Grigorescu, Shubhang Kulkarni, and Minshen Zhu. "Locally Decodable/Correctable Codes for Insertions and Deletions". In: *40th IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS 2020)*. Ed. by Nitin Saxena and Sunil Simon. Vol. 182. Leibniz International Proceedings in Informatics (LIPIcs). Dagstuhl, Germany: Schloss Dagstuhl–Leibniz-Zentrum für Informatik, 2020, 16:1–16:17. DOI: 10.4230/LIPIcs.FSTTCS.2020.16

Alexander R. Block, Justin Holmgren, Alon Rosen, Ron D. Rothblum, and Pratik Soni. "Public-Coin Zero-Knowledge Arguments with (almost) Minimal Time and Space Overheads". In: *Theory of Cryptography - 18th International Conference, TCC 2020, Durham, NC, USA, November 16-19, 2020, Proceedings, Part II*. ed. by Rafael Pass and Krzysztof Pietrzak. Vol. 12551. Lecture Notes in Computer Science. Springer, 2020, pp. 168–197. DOI: 10.1007/978-3-030-64378-2_7

Alexander R. Block, Hemanta K. Maji, and Hai H. Nguyen. "Secure Computation with Constant Communication Overhead Using Multiplication Embeddings". In: *Progress in Cryptology - INDOCRYPT 2018 - 19th International Conference on Cryptology in India, New Delhi, India, December 9-12, 2018, Proceedings*. Ed. by Debrup Chakraborty and Tetsu Iwata. Vol. 11356. Lecture Notes in Computer Science. Springer, 2018, pp. 375–398. DOI: 10.1007/978-3-030-05378-9_20

Alexander R. Block, Divya Gupta, Hemanta K. Maji, and Hai H. Nguyen. "Secure Computation Using Leaky Correlations (Asymptotically Optimal Constructions)". In: *Theory of Cryptography - 16th International Conference, TCC 2018, Panaji, India, November 11-14, 2018, Proceedings, Part II*. ed. by Amos Beimel and Stefan Dziembowski. Vol. 11240. Lecture Notes in Computer Science. Springer, 2018, pp. 36–65. DOI: 10.1007/978-3-030-03810-6_2

Alexander R. Block, Hemanta K. Maji, and Hai H. Nguyen. "Secure Computation Based on Leaky Correlations: High Resilience Setting". In: *Advances in Cryptology - CRYPTO 2017 - 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2017, Proceedings,*

Part II. ed. by Jonathan Katz and Hovav Shacham. Lecture Notes in Computer Science. Springer, 2017. DOI: 10.1007/978-3-319-63715-0_1

Under Submission

All authors listed alphabetically. Entries appear in reverse chronological order.

Alexander R. Block and Christina Garman. *Honest Majority Multi-Prover Interactive Arguments*. Cryptology ePrint Archive, Report 2022/557. https://ia.cr/2022/557. 2022

Professional Activities

External Journal & Conference Reviews

IEEE Transactions on Dependable and Secure Computing (2022)

ACM Conference on Computer and Communications Security (2022)

USENIX Security Symposium (2022)

IEEE Symposium on Security and Privacy (2022)

IMA International Conference on Cryptography and Coding (2021)

Information Processing Letters (2021)

IACR Advances in Cryptology CRYPTO (2020, 2021, 2022)

Network and Distributed System Security Symposium NDSS (2020, 2021)

Conference on Security and Cryptography for Networks SCN (2020)

Innovations in Theoretical Computer Science ITCS (2019, 2020)

IACR Theory of Cryptography Conference TCC (2016, 2017, 2020, 2021)

Academic Engagement

Purdue Computer Science Graduate Student Association, President (2020-2022), Vice President (2019-2020)

UC Irvine Campuswide Honors Collegium, Peer Academic Advisor (2014-2015)

UC Irvine Campuswide Honors Student Council, Webmaster (2013-2014)

Talks

Polynomial Commitments. Purdue Theoretical Computer Science Reading Group 2022.

Time- and Space-Efficient Arguments from Groups of Unknown Order. Purdue Theoretical Computer Science Reading Group 2021.

Private and Resource-Bounded Locally Decodable Codes for Insertions and Deletions. IEEE Symposium on Information Theory. ISIT 2021.

Time- and Space-Efficient Polynomial Commitments in the Streaming Model. Purdue Theoretical Computer Science Seminar 2021.

Public-Coin Zero-Knowledge Arguments with (almost) Minimal Time and Space Overheads. Theory of Cryptography Conference. TCC 2020.

Locally Decodable/Correctable Codes for Insertions and Deletions. Foundations of Software Technology and Theoretical Computer Science. FSTTCS 2020.

(Zero-Knowledge) Interactive Proofs. Purdue Theory of Computer Science Reading Group 2019.

Secure Computation using Leaky Correlations (Asymptotically Optimal Constructions). Theory of Cryptography Conference. TCC 2018.

A Sublinear Upper Bound on Certain Tri-Colored Sum-Free Sets. Purdue Theory of Computer Science Reading Group 2017.

Hardness of Computing the Biclique Partition Number. Purdue Cryptography Reading Group 2017.

Randomness Extraction. Purdue Cryptography Reading Group 2016.

Awards, Honors, and Fellowships

Purdue Three Minute Thesis Competition Finalist, 2022.

Emil Stefanov Fellowship in Computer Science, Purdue University, 2021.

Oustanding Service to the Department of Computer Science, Purdue University, 2021 & 2022.

Chancellor's Award of Distinction, University of California, Irvine, 2015.

Campuswide Honors, University of California, Irvine, 2015.

Honors in Mathematics, University of California, Irvine, 2015.

Best Poster and Best Presentation, Pacific Coast Undergraduate Mathematics Conference, Mathematical Association of America, 2015.

Founding member of Pi Mu Epsilon - UC Irvine Chapter, University of California, Irvine, 2014.

Dean's Honors List, University of California, Irvine, 2012-2015.