Alexander R. Block

July 22, 2024

alexander.r.block@gmail.com

alexblock.io

Current Position

- **Postdoctoral Research Fellow**. Department of Computer Science, Georgetown University, Washington DC (*Host: Justin Thaler*). September 2022 – October 2024.

Education

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

Advisor: Jeremiah Blocki (Purdue University)

Committee: 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. Computer Science, Purdue University, May 2019.

B.S. Mathematics and Information & Computer Science, University of California, Irvine, June 2015. Graduate with Honors from the Campuswide Honors Collegium and the Department of Mathematics.

Research

Interests
Cryptography, Coding Theory, Concrete Security, Zero-knowledge

Conference Publications
All authors listed alphabetically unless specified otherwise. Entries appear in reverse chronological order.

[c14] **Alexander R. Block**, Pratyush Ranjan Tiwari, *On the Concrete Security of Non-interactive FRI*. to appear in SCN 2024. 2024

[c13] **Alexander R. Block**, Zhiyong Fang, Jonathan Katz, Justin Thaler, Hendrik Waldner, Yupeng Zhang, *Field-Agnostic SNARKs from Expand-Accumulate Codes*. to appear in CRYPTO 2024. 2024

[c12] **Alexander R. Block**, Albert Garreta, Jonathan Katz, Justin Thaler, Pratyush Ranjan Tiwari, Michał Zając, "Fiat-Shamir Security of FRI and Related SNARKs". In: *Advances in Cryptology – ASIACRYPT 2023*. Ed. by Jian Guo and Ron Steinfeld. Singapore: Springer Nature Singapore, 2023, pp. 3–40. DOI: 10.1007/978-981-99-8724-5_1

[c11] **Alexander R. Block**, Jeremiah Blocki, Kuan Cheng, Elena Grigorescu, Xin Li, Yu Zheng, Minshen Zhu, “On Relaxed Locally Decodable Codes for Hamming and Insertion-Deletion Errors”. In: *38th Computational Complexity Conference (CCC 2023)*. Ed. by Amnon Ta-Shma. Vol. 264. Leibniz International Proceedings in Informatics (LIPIcs). Dagstuhl, Germany: Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2023, 14:1–14:25. doi: 10.4230/LIPIcs.CCC.2023.14

[c10] **Alexander R. Block**, Jeremiah Blocki, “Computationally Relaxed Locally Decodable Codes, Revisited”. In: *IEEE International Symposium on Information Theory, ISIT 2023, Taipei, Taiwan, June 25-30, 2023*. IEEE, 2023, pp. 2714–2719. doi: 10.1109/ISIT54713.2023.10206655

[c9] Mohammad Hassan Ameri, **Alexander R. Block**, Jeremiah Blocki, “Memory-Hard Puzzles in the Standard Model with Applications to Memory-Hard Functions and Resource-Bounded Locally Decodable Codes”. In: *Security and Cryptography for Networks - 13th International Conference, SCN 2022, Amalfi, Italy, September 12-14, 2022, Proceedings*. Ed. by Clemente Galdi and Stanislaw Jarecki. Vol. 13409. Lecture Notes in Computer Science. Springer, 2022, pp. 45–68. doi: 10.1007/978-3-031-14791-3_3

[c8] **Alexander R. Block**, Justin Holmgren, Alon Rosen, Ron D. Rothblum, 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

[c7] **Alexander R. Block**, Simina Brânzei, Hemanta K. Maji, Himanshi Mehta, Tamalika Mukherjee, 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

[c6] **Alexander R. Block**, 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

[c5] **Alexander R. Block**, Jeremiah Blocki, Elena Grigorescu, Shubhang Kulkarni, 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

[c4] **Alexander R. Block**, Justin Holmgren, Alon Rosen, Ron D. Rothblum, 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

[c3] **Alexander R. Block**, Hemanta K. Maji, 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

[c2] **Alexander R. Block**, Divya Gupta, Hemanta K. Maji, 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

[c1] **Alexander R. Block**, Hemanta K. Maji, 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. Vol. 10402. Lecture Notes in Computer Science. Springer, 2017, pp. 3–32. DOI: 10.1007/978-3-319-63715-0_1

Journal Publications All authors listed alphabetically unless specified otherwise. Entries appear in reverse chronological order.

[j1] **Alexander R. Block**, Albert Garreta, Pratyush Ranjan Tiwari, Michał Zając, *On Soundness Notions for Interactive Oracle Proofs*. to appear in Journal of Cryptology: Topical Collection on Modern Zero-Knowledge Protocols 2024. 2024

Preprints

All authors listed alphabetically unless specified otherwise. Entries appear in reverse chronological order.

[p1] **Alexander R. Block**, Christina Garman, *Honest Majority Multi-Prover Interactive Arguments*. Cryptology ePrint Archive, Report 2022/557. https://eprint.iacr.org/2022/557. 2022

Professional Activities

Program Committees

- IEEE Symposium on Security and Privacy (2024, 2025)
- ZKProof Workshop Edition 6 (2024)

Conference Reviews

- ACM Conference on Computer and Communications Security CCS (2022)
- ACM Symposium on Theory of Computing STOC (2023)
- Conference on Security and Cryptography for Networks SCN (2020)
- IACR Advances in Cryptology CRYPTO (2020, 2021, 2022, 2024)
- IACR Advances in Cryptology EUROCRYPT (2023, 2024)
- IACR Theory of Cryptography Conference TCC (2016-B, 2017, 2020, 2021, 2024)

- IEEE Symposium on Security and Privacy (2022)
- IMA International Conference on Cryptography and Coding (2021)
- Innovations in Theoretical Computer Science ITCS (2019, 2020)
- Network and Distributed System Security Symposium NDSS (2020, 2021)
- USENIX Security Symposium (2022)

Journal Reviews

- IACR Journal of Cryptology (2022)
- IEEE Transactions on Dependable and Secure Computing (2022)
- Information Processing Letters (2021)
- Theoretical Computer Science (2024)
- Theory of Computing (2023)

Past Positions

- **Postdoctoral Researcher**. Department of Computer Science, University of Maryland, College Park MD (*Host: Jonathan Katz*). September 2022 – May 2024.
- **Graduate Research Fellow**. FACT Center, Reichmann University, Herzilya, Israel. June 2019 – August 2019.
- **Graduate Research Assistant**. Department of Computer Science, Purdue University, West Lafayette IN. January 2016 – August 2022.
- **Graduate Teaching Assistant**. Department of Computer Science, Purdue University, West Lafayette IN. August 2016 – December 2019.

Talks

- Fiat-Shamir Security of FRI and Related SNARKs. ASIACRYPT, December 2023.
- Fiat-Shamir Security of FRI and Related SNARKs. UMD Cyrpto Reading Group, October 2023.
- Computationally Relaxed Locally Decodable Codes, Revisited. ISIT 2023.
- Honest Majority Multi-Prover Interactive Arguments. UMD Cyrpto Reading Group, April 2023.
- Polynomial Commitments. UMD Crypto Reading Group, October 2022.
- 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.

Academic 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.