Rishab Goyal

Assistant Professor, UW-Madison

+1 (512) 815 6840
✉ *rishab@cs.wisc.edu*
pages.cs.wisc.edu/~rishab

Last updated: Mar 15, 2023

Research Interests

My main area of research is Cryptography and Computer Security. In particular, I am interested in post-quantum and lattice-based cryptography with a focus on building secure systems with advanced capabilities. I am also interested in studying the impact of advanced cryptography on influencing public policy and law.

Current Position

Fall 2022 – Present **University of Wisconsin-Madison**, Madison, WI, USA
Assistant Professor, Department of Computer Science

Education

2014 – 2019 **Ph.D. in Computer Science**, *University of Texas at Austin*
Advisor: Brent Waters
Thesis: Collusion Resistant Traitor Tracing Systems

2010 – 2014 **B.Tech. in Computer Science**, *Indian Institute of Technology, Delhi*
Advisors: Ragesh Jaiswal and Raghav Bhaskar
Thesis: Password Authenticated Secret Sharing

Recent Awards and Distinctions

2020 Simons-Berkeley Research Fellowship

2020 Bert Kay Dissertation Award for best doctoral thesis in computer science at UT Austin

2018 IBM Ph.D. Fellowship

2018 UT Austin Graduate Dean's Prestigious Fellowship Supplement

2018 STOC 2018 paper invited to the SIAM Journal of Computing (SICOMP) Special Issue

Professional Experience

Summer 2020 – 2022 **Massachusetts Institute of Technology**, Cambridge, USA
Postdoctoral Researcher
Built novel paradigms for advanced cryptographic systems.

Spring 2020 **Simons Institute for the Theory of Computing**, Berkeley, USA
Apple Research Fellow
Part of the Simons program on Lattices: Algorithms, Complexity, and Cryptography.

Summer 2016 **Microsoft Research**, Bangalore, India
Research Intern
Devised tools to bypass cryptographic impossibilities by leveraging blockchains.

Summer 2013 **Microsoft Research**, Bangalore, India
Research Intern
Developed faster algorithms for large-scale distributed convex optimizations.

Summer 2012 **Max Planck Institute for Software Systems**, Saarbrücken, Germany
Research Intern
Studied methods for detecting and preventing privacy leaks in Android.

Conference Publications

[1] Shweta Agrawal, Rishab Goyal, and Junichi Tomida. Multi-Input Quadratic Functional Encryption: Stronger Security, Broader Functionality. In *Theory of Cryptography - **TCC** 2022 - 20th International Conference*, 2022.

[2] Lalita Devadas, Rishab Goyal, Yael Kalai, and Vinod Vaikuntanathan. Rate-1 Non-Interactive Arguments for Batch-NP and Applications. In *63rd IEEE Annual Symposium on Foundations of Computer Science, **FOCS** 2022*, 2022.

[3] Rishab Goyal and Vinod Vaikuntanathan. Locally Verifiable Signature and Key Aggregation. In *Advances in Cryptology - **CRYPTO** 2022 - 42nd Annual International Cryptology Conference*, 2022.

[4] Rachit Garg, Rishab Goyal, George Lu, and Brent Waters. Dynamic Collusion Bounded Functional Encryption from Identity-Based Encryption. In *Advances in Cryptology - **EUROCRYPT** 2022 - 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques*, 2022.

[5] Shweta Agrawal, Rishab Goyal, and Junichi Tomida. Multi-Party Functional Encryption. In *Theory of Cryptography - **TCC** 2021 - 19th International Conference*, 2021.

[6] Rishab Goyal, Jiahui Liu, and Brent Waters. Adaptive Security via Deletion in Attribute-Based Encryption: Solutions from Search Assumptions in Bilinear Groups. In *Theory and Application of Cryptology and Information Security - **ASIACRYPT** 2021 - 27th International Conference*, 2021.

[7] Rishab Goyal, Ridwan Syed, and Brent Waters. ABE for TMs with bounded collusion. In *Theory and Application of Cryptology and Information Security - **ASIACRYPT** 2021 - 27th International Conference*, 2021.

[8] Rishab Goyal, Sam Kim, Brent Waters, and David J. Wu. Beyond Software Watermarking: Traitor-Tracing for Pseudorandom Functions. In *Theory and Application of Cryptology and Information Security - **ASIACRYPT** 2021 - 27th International Conference*, 2021.

[9] Shweta Agrawal, Rishab Goyal, and Junichi Tomida. Multi-input quadratic functional encryption from pairings. In *Advances in Cryptology - **CRYPTO** 2021 - 41st Annual International Cryptology Conference*, 2021.

[10] Rishab Goyal, Venkata Koppula, Satyanarayana Vusirikala, and Brent Waters. On Perfect Correctness in (Lockable) Obfuscation. In *Theory of Cryptography - **TCC** 2020 - 18th International Conference*, 2020.

[11] Rishab Goyal and Satyanarayana Vusirikala. Verifiable registration-based encryption. In *Advances in Cryptology - **CRYPTO** 2020 - 40th Annual International Cryptology Conference*, 2020.

[12] Rishab Goyal, Satyanarayana Vusirikala, and Brent Waters. New Constructions of Hinting PRGs, OWFs with Encryption, and More. In *Advances in Cryptology - **CRYPTO** 2020 - 40th Annual International Cryptology Conference*, 2020.

[13] Rishab Goyal, Venkata Koppula, and Brent Waters. New Approaches to Traitor Tracing with Embedded Identities. In *Theory of Cryptography - **TCC** 2019 - 17th International Conference*, 2019.

[14] Rishab Goyal, Willy Quach, Brent Waters, and Daniel Wichs. Broadcast and Trace with N^ϵ Ciphertext Size from Standard Assumptions. In *Advances in Cryptology - **CRYPTO** 2019 - 39th Annual International Cryptology Conference*, 2019.

[15] Rishab Goyal, Sam Kim, Nathan Manohar, Brent Waters, and David J. Wu. Watermarking Public-Key Cryptographic Primitives. In *Advances in Cryptology - **CRYPTO** 2019 - 39th Annual International Cryptology Conference*, 2019.

[16] Rishab Goyal, Satyanarayana Vusirikala, and Brent Waters. Collusion Resistant Broadcast and Trace from Positional Witness Encryption. In *Public-Key Cryptography - **PKC** 2019 - 22nd IACR International Conference on Practice and Theory of Public-Key Cryptography*, 2019.

[17] Rishab Goyal, Venkata Koppula, Andrew Russell, and Brent Waters. Risky Traitor Tracing and New Differential Privacy Negative Results. In *Advances in Cryptology - **CRYPTO** 2018 - 38th Annual International Cryptology Conference*, 2018.

[18] Rishab Goyal, Venkata Koppula, and Brent Waters. Collusion resistant traitor tracing from learning with errors. In *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing, **STOC** 2018*. ACM, 2018.
SIAM Journal of Computing (SICOMP) Special Issue for selected papers from STOC 2018.

[19] Rishab Goyal and Vipul Goyal. Overcoming Cryptographic Impossibility Results Using Blockchains. In *Theory of Cryptography - **TCC** 2017 - 15th International Conference*, 2017.

[20] Rishab Goyal, Susan Hohenberger, Venkata Koppula, and Brent Waters. A Generic Approach to Constructing and Proving Verifiable Random Functions. In *Theory of Cryptography - **TCC** 2017 - 15th International Conference*, 2017.

[21] Rishab Goyal, Venkata Koppula, and Brent Waters. Lockable Obfuscation. In *58th IEEE Annual Symposium on Foundations of Computer Science, **FOCS** 2017*, 2017.

[22] Cody Freitag, Rishab Goyal, Susan Hohenberger, Venkata Koppula, Eysa Lee, Tatsuaki Okamoto, Jordan Tran, and Brent Waters. Signature Schemes with Randomized Verification. In *Applied Cryptography and Network Security - **ACNS** 2017 - 15th International Conference*, 2017.

[23] Rishab Goyal, Venkata Koppula, and Brent Waters. Separating Semantic and Circular Security for Symmetric-Key Bit Encryption from the Learning with Errors Assumption. In *Advances in Cryptology - **EUROCRYPT** 2017 - 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, 2017.

[24] Rishab Goyal, Venkata Koppula, and Brent Waters. Separating IND-CPA and Circular Security for Unbounded Length Key Cycles. In *Public-Key Cryptography - **PKC** 2017 - 20th IACR International Conference on Practice and Theory in Public-Key Cryptography*, 2017.

[25] Rishab Goyal, Venkata Koppula, and Brent Waters. Semi-adaptive Security and Bundling Functionalities Made Generic and Easy. In *Theory of Cryptography - **TCC** 2016-B - 14th International Conference*, 2016.

Journal Publications

[26] Rishab Goyal, Venkata Koppula, and Brent Waters. Collusion resistant traitor tracing from learning with errors. *SIAM Journal on Computing*, 49(5):STOC18–94, 2019.

Manuscripts and Preprints

[27] Rishab Goyal. Locally verifiable and privacy preserving batch arguments, 2023. Under submission.

[28] Rishab Goyal and Venkata Koppula. Quantum watermarking and software leasing, 2023. In preparation.

[29] Rachit Garg, Rishab Goyal, and George Lu. A simple and generic approach to dynamic collusion model, 2022. Under submission.

[30] Rishab Goyal and Venkata Koppula. Multi-party lockable obfuscation: Applications to patchability, anonymity, and more, 2023. In preparation.

[31] Rishab Goyal. Quantum multi-key homomorphic encryption for polynomial-sized circuits. Cryptology ePrint Archive, Report 2018/443, 2018. https://eprint.iacr.org/2018/443.

Service

Program Committees: EUROCRYPT 2020, TCC 2021, PKC 2022, TCC 2022, EUROCRYPT 2023, FOCS 2023

Conference/Journal Refereeing: External reviewer for Journal of Cryptology, STOC, FOCS, CRYPTO, EUROCRYPT, TCC, ASIACRYPT, PKC, CANS.

Graduate Admissions Committee: UT Austin, UW-Madison

2022 ACM India Doctoral Dissertation Award Committee

Invited talks

Jan 2023	Crypto seminar, IISc and Microsoft Research India
Jan 2023	CS Colloquium, IIT Delhi
Jul 2021	Charles River Crypto Day, Northeastern University
Apr 2021	CS Colloquium, New York University
Mar 2020	Lattices: New Cryptographic Capabilities Workshop, Simons Institute
Nov 2019	Cryptography and Information Security (CIS) seminar, MIT
Nov 2019	Crypto seminar, UC Berkeley
Nov 2019	Crypto seminar, Stanford University
Mar 2019	Tokyo Crypto Day, NTT Research
Jan 2019	Crypto seminar, IIT Delhi
May 2018	Workshop on Lattice Crypto and Algorithms, Bertinoro
May 2018	Crypto seminar, ENS
Jan 2017	Center for Encrypted Functionalities (CEF) seminar, UCLA
Jun 2016	Crypto seminar, Microsoft Research India

Teaching

Spring 2023	**Instructor**, *CS435 - Cryptography*, UW-Madison.
Fall 2022	**Instructor**, *CS880 - Topics in Theoretical Computer Science: Cryptography and Foundations of Post-Quantum Security (Graduate)*, UW-Madison.
Spring 2021	**Guest Lecturer**, *CS598DK - Special Topics in Cryptography (Graduate)*, UIUC.
Spring 2017	**Teaching Assistant**, *CS388H - Cryptography (Graduate)*, UT Austin.
Fall 2016	**Teaching Assistant**, *CS346 - Cryptography (Undergraduate)*, UT Austin.
Spring 2015	**Teaching Assistant**, *CS346 - Cryptography (Undergraduate)*, UT Austin.
Fall 2014	**Teaching Assistant**, *CS331 - Algorithms and Complexity (Undergraduate)*, UT Austin.
Summer 2011	**Teacher**, *High School Math - Limits and Differential Calculus*, Vidyamandir Classes.

References

Brent Waters

Professor
Department of Computer Science
The University of Texas at Austin
✉ bwaters@cs.utexas.edu

Vinod Vaikuntanathan

Professor
Department of Electrical Engineering
and Computer Science
Massachusetts Institute of Technology
✉ vinodv@csail.mit.edu

Shweta Agrawal

Associate Professor
Department of Computer Science
and Engineering
Indian Institute of Technology, Madras
✉ shwetaag@cse.iitm.ac.in

Amit Sahai

Professor
Department of Computer Science
University of California at Los Angeles
✉ sahai@cs.ucla.edu

Daniel Wichs

Associate Professor
Department of Computer Science
Northeastern University
✉ wichs@ccs.neu.edu

Mentorship

Advised multiple undergraduate, masters, and younger graduate students while at UT Austin. Student advisees listed below:

2021 – Now Rachit Garg, Ph.D. student Computer Science, UT Austin.

2021 – Now George Lu, Ph.D. student Computer Science, UT Austin.

2017 – 2021 Satyanarayana Vusirikala, Ph.D. Computer Science, UT Austin.

2018 – 2019 Jiahui Liu, Ph.D. student Computer Science, UT Austin.

2018 – 2019 Ridwan Syed, M.S. Computer Science, UT Austin.

2017 – 2018 Andrew Russell, M.S. Computer Science, UT Austin.

2015 – 2016 Cody Freitag, B.S. Computer Science, UT Austin. Now a Ph.D. student at Cornell University.

2015 – 2016 Eysa Lee, B.S. Computer Science, UT Austin. Now a Ph.D. student at Northeastern University.

2015 – 2016 Jordan Tran, B.S. Computer Science, UT Austin.