Rishab Goyal

Assistant Professor, UW-Madison

+1 (512) 815 6840
✉ rishab@cs.wisc.edu
pages.cs.wisc.edu/~rishab
Last updated: Jan 02, 2025

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.

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

Professional Experience

Summer 2020 – 2022 **Massachusetts Institute of Technology**, Cambridge, USA
Postdoctoral Researcher

Spring 2020 **Simons Institute for the Theory of Computing**, Berkeley, USA
Visiting Research Scientist

Summer 2016 **Microsoft Research**, Bangalore, India
Research Intern

Summer 2013 **Microsoft Research**, Bangalore, India
Research Intern

Summer 2012 **Max Planck Institute for Software Systems**, Saarbrücken, Germany
Research Intern

Awards and Distinctions

2020 Simons-Berkeley Research Fellowship
2020 Bert Kay Dissertation Award for best doctoral thesis at UT Austin
2018 IBM Ph.D. Fellowship
2018 UT Austin Graduate Dean's Prestigious Fellowship
2018 SIAM Journal of Computing (SICOMP) Special Issue Invitation

Manuscripts and Preprints

[1] Abtin Afshar, Jiaqi Cheng, Rishab Goyal, Aayush Yadav, and Saikumar Yadugiri. Encrypted RAM delegation: Applications to rate-1 extractable arguments, homomorphic NIZKs, MPC, and more. Cryptology ePrint Archive, Paper 2024/1806, 2024.

[2] Rishab Goyal. Mutable batch arguments and applications. Cryptology ePrint Archive, Paper 2024/737, 2024.

[3] Abtin Afshar, Jiaqi Cheng, and Rishab Goyal. Multi-hop multi-key homomorphic signatures with context hiding from standard assumptions. Cryptology ePrint Archive, Paper 2024/931, 2024.

[4] Jiaqi Cheng and Rishab Goyal. Boosting SNARKs and rate-1 barrier in arguments of knowledge. Cryptology ePrint Archive, Paper 2024/1603, 2024.

[5] Abtin Afshar and Rishab Goyal. Verifiable streaming computation and step-by-step zero-knowledge. Cryptology ePrint Archive, Paper 2025/251, 2025.

[6] Rishab Goyal, Venkata Koppula, and Mahesh Sreekumar Rajasree. A note on adaptive security in hierarchical identity-based encryption. Cryptology ePrint Archive, Paper 2025/291, 2025.

[7] Foteini Baldimtsi, Rishab Goyal, and Aayush Yadav. Practical non-interactive & batched blind signatures from lattices. (under review), 2025.

[8] Rishab Goyal and Saikumar Yadugiri. Delegatable ABE with full security from witness encryption. Cryptology ePrint Archive, Paper 2025/407, 2025.

[9] Rishab Goyal and Saikumar Yadugiri. Multi-authority functional encryption: Corrupt authorities, dynamic collusion, lower bounds, and more. Cryptology ePrint Archive, Paper 2025/412, 2025.

[10] Shashwatha Ghante Banuprakash, Rishab Goyal, and Aditya Jain. Succinct arguments for batchqma and friends under 8 rounds. (under review), 2025.

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

Conference Publications

[12] Rishab Goyal, Fuyuki Kitagawa, Venkata Koppula, Ryo Nishimaki, Mahesh Sreekumar Rajasree, and Takashi Yamakawa. Non-committing attribute and identity based encryption: Constructions and applications. In *Public-Key Cryptography - **PKC** 2025 - 28th IACR International Conference on Practice and Theory of Public-Key Cryptography*, 2025.

[13] Rishab Goyal, Venkata Koppula, Mahesh Sreekumar Rajasree, and Aman Verma. Incompressible functional encryption. In *16th Innovations in Theoretical Computer Science - **ITCS** 2025*, 2025.

[14] Foteini Baldimtsi, Jiaqi Cheng, Rishab Goyal, and Aayush Yadav. Non-interactive blind signatures: Post-quantum and stronger security. In *Theory and Application of Cryptology and Information Security - **ASIACRYPT** 2024 - 30th International Conference*, 2024.

[15] Kaartik Bhushan, Rishab Goyal, Venkata Koppula, Varun Narayanan, Manoj Prabhakaran, and Mahesh Sreekumar Rajasree. Leakage-resilient incompressible cryptography: Constructions and barriers. In *Theory and Application of Cryptology and Information Security - **ASIACRYPT** 2024 - 30th International Conference*, 2024.

[16] Rishab Goyal and Saikumar Yadugiri. Multi-authority functional encryption with bounded collusions from standard assumptions. In *Theory of Cryptography - **TCC** 2024 - 22nd International Conference*, 2024.

[17] Rachit Garg, Rishab Goyal, and George Lu. Dynamic collusion functional encryption and multi-authority attribute-based encryption. In *Public-Key Cryptography - **PKC** 2024 - 27th IACR International Conference on Practice and Theory of Public-Key Cryptography*, 2024.

[18] 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.

[19] 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.

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

[21] 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.

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

[23] 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.

[24] 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.

[25] 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.

[26] 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.

[27] 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.

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

[29] 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.

[30] 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.

[31] 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.

[32] 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.

[33] 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.

[34] 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.

[35] 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.

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

[37] 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.

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

[39] 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.

[40] 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.

[41] 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.

[42] 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

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

Advising

PhD student advisees listed below:

2022 – Now Jiaqi Cheng, Ph.D. student Computer Science, UW-Madison.

2023 – Now Abtin Ashfar Shandi, Ph.D. student Computer Science, UW-Madison.

2023 – Now Saikumar Yadugiri, Ph.D. student Computer Science, UW-Madison.

MS student advisees listed below:

2023 – 2024 Aditya Jain, M.S. Computer Science, UW-Madison.

2023 – Now Shashwatha Ghante Banuprakash, M.S. student Computer Science, UW-Madison.

Invited talks

Oct 2024 Shonan Workshop on Encrypted Computation, Japan

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 2025 **Instructor**, *CS880 - Topics in Theoretical Computer Science: Foundations of Post-Quantum Cryptography (Graduate)*, UW-Madison

Fall 2024 **Instructor**, *CS435 - Cryptography*, UW-Madison

Spring 2024 **Instructor**, *CS639 - Modern Cryptography*, UW-Madison

Fall 2023 **Instructor**, *CS880 - Topics in Theoretical Computer Science: Foundations of Cryptographic Proofs (Graduate)*, UW-Madison

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**, *CS598 - 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

Service

Program Committees: EUROCRYPT (2020, 2023), TCC (2021, 2022), PKC (2022, 2024), FOCS 2023, ASIACRYPT 2024, ITCS 2025

Editorial Board: SIAM Journal on Computing (Associate Editor)

ACM India Doctoral Dissertation Award Committee 2022, 2023, 2024
Graduate Admissions Committee: UT Austin, UW-Madison