Stanford



Mark Zhandry

Associate Professor of Computer Science

Bio

ACADEMIC APPOINTMENTS

- Associate Professor, Computer Science

Teaching

COURSES

2026-27

- Advanced Topics in Cryptography: CS 355 (Spr)
- Quantum Cryptography: CS 258 (Aut)

2025-26

- Big Ideas in Cryptography: CS 25N (Win)
- Quantum Cryptography: CS 258 (Aut)

STANFORD ADVISEES

Yiyi Cai

Doctoral Dissertation Reader (AC)

Jordan Docter

Doctoral Dissertation Co-Advisor (AC)

Matthew Ding

Doctoral (Program)

Itay Shalit

Publications

PUBLICATIONS

- **Optimal Threshold Traitor Tracing**
  Das, S., Datta, P., Partap, A., Sasmal, S., Zhandry, M.
  edited by Daemen, J., Thome, E.
  SPRINGER INTERNATIONAL PUBLISHING AG.2026: 486-516
- **Separating QMA from QCMA with a Classical Oracle**
  Bostanci, J., Haferkamp, J., Nirkhe, C., Zhandry, M.

edited by Bhaskara, A., Czumaj, A.
ASSOC COMPUTING MACHINERY.2026: 595-606

- **On the Cryptographic Foundations of Interactive Quantum Advantage**
  Tomer, K., Zhandry, M.
  edited by Bhaskara, A., Czumaj, A.
  ASSOC COMPUTING MACHINERY.2026: 455-466
- **A Note on Quantum-Secure PRPs** *QUANTUM*
  Zhandry, M.
  2025; 9
- **Composability in Watermarking Schemes**
  Liu, J., Zhandry, M.
  edited by Boyle, E., Mahmoody, M.
  SPRINGER INTERNATIONAL PUBLISHING AG.2025: 400-430
- **Translating Between the Common Haar Random State Model and the Unitary Model**
  Goldin, E., Zhandry, M.
  edited by Kalai, Y. T., Kamara, S. F.
  SPRINGER INTERNATIONAL PUBLISHING AG.2025: 269-300
- **A General Quantum Duality for Representations of Groups with Applications to Quantum Money, Lightning, and Fire**
  Bostanci, J., Nehoran, B., Zhandry, M.
  edited by Koucky, M., Bansal, N.
  ASSOC COMPUTING MACHINERY.2025: 201-212
- **On One-Shot Signatures, Quantum vs. Classical Binding, and Obfuscating Permutations**
  Shmueli, O., Zhandry, M.
  edited by Kalai, Y. T., Kamara, S. F.
  SPRINGER INTERNATIONAL PUBLISHING AG.2025: 350-383
- **Full Quantum Equivalence of Group Action DLog and CDH, and More** *JOURNAL OF CRYPTOLOGY*
  Montgomery, H., Zhandry, M.
  2024; 37 (4)
- **Verifiable Quantum Advantage without Structure** *JOURNAL OF THE ACM*
  Yamakawa, T., Zhandry, M.
  2024; 71 (3)
- **Adaptive Security in SNARGs via iO and Lossy Functions**
  Waters, B., Zhandry, M.
  edited by Reyzin, L., Stebila, D.
  SPRINGER INTERNATIONAL PUBLISHING AG.2024: 72-104
- **A Computational Separation Between Quantum No-Cloning and No-Telegraphing**
  Nehoran, B., Zhandry, M.
  edited by Guruswami
  SCHLOSS DAGSTUHL, LEIBNIZ CENTER INFORMATICS.2024
- **Commitments to Quantum States**
  Gunn, S., Ju, N., Ma, F., Zhandry, M.
  edited by Servedio, R. A., Saha, B.
  ASSOC COMPUTING MACHINERY.2023: 1579-1588
- **Another Round of Breaking and Making Quantum Money: How to Not Build It from Lattices, and More**
  Liu, J., Montgomery, H., Zhandry, M.
  edited by Hazay, C., Stam, M.
  SPRINGER INTERNATIONAL PUBLISHING AG.2023: 611-638

- **The Relationship Between Idealized Models Under Computationally Bounded Adversaries**
  Zhang, C., Zhandry, M.
  edited by Guo, J., Steinfeld, R.
  SPRINGER-VERLAG SINGAPORE PTE LTD.2023: 390-419
- **A Lower Bound on the Length of Signatures Based on Group Actions and Generic Isogenies**
  Boneh, D., Guan, J., Zhandry, M.
  edited by Hazay, C., Stam, M.
  SPRINGER INTERNATIONAL PUBLISHING AG.2023: 507-531
- **Multi-instance Randomness Extraction and Security Against Bounded-Storage Mass Surveillance**
  Guan, J., Wichs, D., Zhandry, M.
  edited by Rothblum, G., Wee, H.
  SPRINGER INTERNATIONAL PUBLISHING AG.2023: 93-122
- **Security-Preserving Distributed Samplers: How to Generate Any CRS in One Round Without Random Oracles**
  Abram, D., Waters, B., Zhandry, M.
  edited by Handschuh, H., Lysyanskaya, A.
  SPRINGER INTERNATIONAL PUBLISHING AG.2023: 489-514
- **Computational Wiretap Coding from Indistinguishability Obfuscation**
  Ishai, Y., Jain, A., Lou, P., Sahai, A., Zhandry, M.
  edited by Handschuh, H., Lysyanskaya, A.
  SPRINGER INTERNATIONAL PUBLISHING AG.2023: 263-293
- **Tracing Quantum State Distinguishers via Backtracking**
  Zhandry, M.
  edited by Handschuh, H., Lysyanskaya, A.
  SPRINGER INTERNATIONAL PUBLISHING AG.2023: 3-36
- **Full Quantum Equivalence of Group Action DLog and CDH, and More**
  Montgomery, H., Zhandry, M.
  edited by Lin, D., Agrawal, S.
  SPRINGER INTERNATIONAL PUBLISHING AG.2022: 3-32
- **Post-Quantum Succinct Arguments: Breaking the Quantum Rewinding Barrier**
  Chiesa, A., Ma, F., Spooner, N., Zhandry, M., IEEE COMP SOC
  IEEE COMPUTER SOC.2022: 49-58
- **Quantum Algorithms for Variants of Average-Case Lattice Problems via Filtering**
  Chen, Y., Liu, Q., Zhandry, M.
  edited by Dunkelman, O., Dziembowski, S.
  SPRINGER INTERNATIONAL PUBLISHING AG.2022: 372-401
- **New Constructions of Collapsing Hashes**
  Zhandry, M.
  edited by Dodis, Y., Shrimpton, T.
  SPRINGER INTERNATIONAL PUBLISHING AG.2022: 596-624
- **Collusion Resistant Copy-Protection for Watermarkable Functionalities**
  Liu, J., Liu, Q., Qian, L., Zhandry, M.
  edited by Kiltz, E., Vaikuntanathan
  SPRINGER INTERNATIONAL PUBLISHING AG.2022: 294-323
- **Adaptive Multiparty NIKE**
  Koppula, V., Waters, B., Zhandry, M.
  edited by Kiltz, E., Vaikuntanathan
  SPRINGER INTERNATIONAL PUBLISHING AG.2022: 244-273

- **Verifiable Quantum Advantage without Structure**
  Yamakawa, T., Zhandry, M., IEEE Comp Soc
  IEEE COMPUTER SOC.2022: 69-74
- **Incompressible Cryptography**
  Guan, J., Wichs, D., Zhandry, M.
  edited by Dunkelman, O., Dziembowski, S.
  SPRINGER INTERNATIONAL PUBLISHING AG.2022: 700-730
- **On the Feasibility of Unclonable Encryption, and More**
  Ananth, P., Kaleoglu, F., Li, X., Liu, Q., Zhandry, M.
  edited by Dodis, Y., Shrimpton, T.
  SPRINGER INTERNATIONAL PUBLISHING AG.2022: 212-241
- **Augmented Random Oracles**
  Zhandry, M.
  edited by Dodis, Y., Shrimpton, T.
  SPRINGER INTERNATIONAL PUBLISHING AG.2022: 35-65
- **To Label, or Not To Label (in Generic Groups)**
  Zhandry, M.
  edited by Dodis, Y., Shrimpton, T.
  SPRINGER INTERNATIONAL PUBLISHING AG.2022: 66-96
- **How to Construct Quantum Random Functions** *JOURNAL OF THE ACM*
  Zhandry, M.
  2021; 68 (5)
- **Decomposable Obfuscation: A Framework for Building Applications of Obfuscation from Polynomial Hardness** *JOURNAL OF CRYPTOLOGY*
  Liu, Q., Zhandry, M.
  2021; 34 (3)
- **Quantum Lightning Never Strikes the Same State Twice. Or: Quantum Money from Cryptographic Assumptions** *JOURNAL OF CRYPTOLOGY*
  Zhandry, M.
  2021; 34 (1)
- **Classical vs Quantum Random Oracles**
  Yamakawa, T., Zhandry, M.
  edited by Canteaut, A., Standaert, F. X.
  SPRINGER INTERNATIONAL PUBLISHING AG.2021: 568-597
- **Hidden Cosets and Applications to Unclonable Cryptography**
  Coladangelo, A., Liu, J., Liu, Q., Zhandry, M.
  edited by Malkin, T., Peikert, C.
  SPRINGER INTERNATIONAL PUBLISHING AG.2021: 556-584
- **Redeeming Reset Indifferentiability and Applications to Post-quantum Security**
  Zhandry, M.
  edited by Tibouchi, M., Wang, H.
  SPRINGER INTERNATIONAL PUBLISHING AG.2021: 518-548
- **Franchised Quantum Money**
  Roberts, B., Zhandry, M.
  edited by Tibouchi, M., Wang, H.
  SPRINGER INTERNATIONAL PUBLISHING AG.2021: 549-574
- **New Approaches for Quantum Copy-Protection**

Aaronson, S., Liu, J., Liu, Q., Zhandry, M., Zhang, R.
edited by Malkin, T., Peikert, C.
SPRINGER INTERNATIONAL PUBLISHING AG.2021: 526-555

- **White Box Traitor Tracing**
  Zhandry, M.
  edited by Malkin, T., Peikert, C.
  SPRINGER INTERNATIONAL PUBLISHING AG.2021: 303-333
- **Disappearing Cryptography in the Bounded Storage Model**
  Guan, J., Zhandry, M.
  edited by Nissim, K., Waters, B.
  SPRINGER INTERNATIONAL PUBLISHING AG.2021: 365-396
- **One-Shot Signatures and Applications to Hybrid Quantum/Classical Authentication**
  Amos, R., Georgiou, M., Kiayias, A., Zhandry, M.
  edited by Makarychev, K., Makarychev, Y., Tulsiani, M., Kamath, G., Chuzhoy, J.
  ASSOC COMPUTING MACHINERY.2020: 255-268
- **Indifferentiability for Public Key Cryptosystems**
  Zhandry, M., Zhang, C.
  edited by Micciancio, D., Ristenpart, T.
  SPRINGER INTERNATIONAL PUBLISHING AG.2020: 63-93
- **Schrodinger's Pirate: How to Trace a Quantum Decoder**
  Zhandry, M.
  edited by Pass, R., Pietrzak, K.
  SPRINGER INTERNATIONAL PUBLISHING AG.2020: 61-91
- **Multiparty Non-Interactive Key Exchange and More From Isogenies on Elliptic Curves** *JOURNAL OF MATHEMATICAL CRYPTOLOGY*
  Boneh, D., Glass, D., Krashen, D., Lauter, K., Sharif, S., Silverberg, A., Tibouchi, M., Zhandry, M.
  2020; 14 (1): 5–14
- **Towards Non-interactive Witness Hiding**
  Kuykendall, B., Zhandry, M.
  edited by Pass, R., Pietrzak, K.
  SPRINGER INTERNATIONAL PUBLISHING AG.2020: 627-656
- **New Techniques for Traitor Tracing: Size N^{1/3} and More from Pairings**
  Zhandry, M.
  edited by Micciancio, D., Ristenpart, T.
  SPRINGER INTERNATIONAL PUBLISHING AG.2020: 652-682
- **The Magic of ELFs** *JOURNAL OF CRYPTOLOGY*
  Zhandry, M.
  2019; 32 (3): 825-866
- **How to Record Quantum Queries, and Applications to Quantum Indifferentiability**
  Zhandry, M.
  edited by Boldyreva, A., Micciancio, D.
  SPRINGER INTERNATIONAL PUBLISHING AG.2019: 239-268
- **New Techniques for Obfuscating Conjunctions**
  Bartusek, J., Lepoint, T., Ma, F., Zhandry, M.
  edited by Ishai, Y., Rijmen
  SPRINGER INTERNATIONAL PUBLISHING AG.2019: 636-666
- **Quantum Lightning Never Strikes the Same State Twice**
  Zhandry, M.

edited by Ishai, Y., Rijmen
SPRINGER INTERNATIONAL PUBLISHING AG.2019: 408-438

- **The Distinction Between Fixed and Random Generators in Group-Based Assumptions**
  Bartusek, J., Ma, F., Zhandry, M.
  edited by Boldyreva, A., Micciancio, D.
  SPRINGER INTERNATIONAL PUBLISHING AG.2019: 801-830
- **On ELFs, Deterministic Encryption, and Correlated-Input Security**
  Zhandry, M.
  edited by Ishai, Y., Rijmen
  SPRINGER INTERNATIONAL PUBLISHING AG.2019: 3-32
- **Revisiting Post-quantum Fiat-Shamir**
  Liu, Q., Zhandry, M.
  edited by Boldyreva, A., Micciancio, D.
  SPRINGER INTERNATIONAL PUBLISHING AG.2019: 326-355
- **New Techniques for Obfuscating Conjunctions**
  Bartusek, J., Lepoint, T., Ma, F., Zhandry, M.
  edited by Ishai, Y., Rijmen
  SPRINGER INTERNATIONAL PUBLISHING AG.2019: 636-666
- **Cutting-edge cryptography through the lens of secret sharing** *INFORMATION AND COMPUTATION*
  Komargodski, I., Zhandry, M.
  2018; 263: 75-96
- **Return of GGH15: Provable Security Against Zeroizing Attacks**
  Bartusek, J., Guan, J., Ma, F., Zhandry, M.
  edited by Beimel, A., Dziembowski, S.
  SPRINGER INTERNATIONAL PUBLISHING AG.2018: 544-574
- **The MMap Strikes Back: Obfuscation and New Multilinear Maps Immune to CLT13 Zeroizing Attacks**
  Ma, F., Zhandry, M.
  edited by Beimel, A., Dziembowski, S.
  SPRINGER INTERNATIONAL PUBLISHING AG.2018: 513-543
- **Impossibility of Order-Revealing Encryption in Idealized Models**
  Zhandry, M., Zhang, C.
  edited by Beimel, A., Dziembowski, S.
  SPRINGER INTERNATIONAL PUBLISHING AG.2018: 129-158
- **Parameter-Hiding Order Revealing Encryption**
  Cash, D., Liu, F., O'Neill, A., Zhandry, M., Zhang, C.
  edited by Peyrin, T., Galbraith, S.
  SPRINGER INTERNATIONAL PUBLISHING AG.2018: 181-210
- **Multiparty Key Exchange, Efficient Traitor Tracing, and More from Indistinguishability Obfuscation** *ALGORITHMICA*
  Boneh, D., Zhandry, M.
  2017; 79 (4): 1233–85
- **New Security Notions and Feasibility Results for Authentication of Quantum Data**
  Garg, S., Yuen, H., Zhandry, M.
  edited by Katz, J., Shacham, H.
  SPRINGER INTERNATIONAL PUBLISHING AG.2017: 342-371
- **Decomposable Obfuscation: A Framework for Building Applications of Obfuscation from Polynomial Hardness**
  Liu, Q., Zhandry, M.
  edited by Kalai, Y., Reyzin, L.

SPRINGER INTERNATIONAL PUBLISHING AG.2017: 138-169

- **Breaking the Sub-Exponential Barrier in Obfustopia**
  Garg, S., Pandey, O., Srinivasan, A., Zhandry, M.
  edited by Coron, J. S., Nielsen, J. B.
  SPRINGER INTERNATIONAL PUBLISHING AG.2017: 156-181

- **Functional Encryption Without Obfuscation**
  Garg, S., Gentry, C., Halevi, S., Zhandry, M.
  edited by Kushilevitz, E., Malkin, T.
  SPRINGER INTERNATIONAL PUBLISHING AG.2016: 480-511

- **Anonymous Traitor Tracing: How to Embed Arbitrary Information in a Key**
  Nishimaki, R., Wichs, D., Zhandry, M.
  edited by Fischlin, M., Coron, J. S.
  SPRINGER INTERNATIONAL PUBLISHING AG.2016: 388-419

- **Annihilation Attacks for Multilinear Maps: Cryptanalysis of Indistinguishability Obfuscation over GGH13**
  Miles, E., Sahai, A., Zhandry, M.
  edited by Robshaw, M., Katz, J.
  SPRINGER INTERNATIONAL PUBLISHING AG.2016: 629-658

- **Order-Revealing Encryption and the Hardness of Private Learning**
  Bun, M., Zhandry, M.
  edited by Kushilevitz, E., Malkin, T.
  SPRINGER INTERNATIONAL PUBLISHING AG.2016: 176-206

- **How to Generate and Use Universal Samplers**
  Hofheinz, D., Jager, T., Khurana, D., Sahai, A., Waters, B., Zhandry, M.
  edited by Cheon, J. H., Takagi, T.
  SPRINGER-VERLAG BERLIN.2016: 715-744

- **Strong Hardness of Privacy from Weak Traitor Tracing**
  Kowalczyk, L., Malkin, T., Ullman, J., Zhandry, M.
  edited by Hirt, M., Smith, A.
  SPRINGER INTERNATIONAL PUBLISHING AG.2016: 659-689

- **How to Avoid Obfuscation Using Witness PRFs**
  Zhandry, M.
  edited by Kushilevitz, E., Malkin, T.
  SPRINGER INTERNATIONAL PUBLISHING AG.2016: 421-448

- **The Magic of ELFs**
  Zhandry, M.
  edited by Robshaw, M., Katz, J.
  SPRINGER-VERLAG BERLIN.2016: 479-508

- **Post-zeroizing Obfuscation: New Mathematical Tools, and the Case of Evasive Circuits**
  Badrinarayanan, S., Miles, E., Sahai, A., Zhandry, M.
  edited by Fischlin, M., Coron, J. S.
  SPRINGER INTERNATIONAL PUBLISHING AG.2016: 764-791

- **Cutting-Edge Cryptography Through the Lens of Secret Sharing**
  Komargodski, I., Zhandry, M.
  edited by Kushilevitz, E., Malkin, T.
  SPRINGER INTERNATIONAL PUBLISHING AG.2016: 449-479

- **Secure Obfuscation in a Weak Multilinear Map Model**
  Garg, S., Miles, E., Mukherjee, P., Sahai, A., Srinivasan, A., Zhandry, M.

edited by Hirt, M., Smith, A.
SPRINGER INTERNATIONAL PUBLISHING AG.2016: 241-268

- **Secure identity-based encryption in the quantum random oracle model** *INTERNATIONAL JOURNAL OF QUANTUM INFORMATION*
  Zhandry, M.
  2015; 13 (4)
- **A NOTE ON THE QUANTUM COLLISION AND SET EQUALITY PROBLEMS** *QUANTUM INFORMATION & COMPUTATION*
  Zhandry, M.
  2015; 15 (7-8): 557-567
- **Semantically Secure Order-Revealing Encryption: Multi-input Functional Encryption Without Obfuscation**
  Boneh, D., Lewi, K., Raykova, M., Sahai, A., Zhandry, M., Zimmerman, J.
  edited by Oswald, E., Fischlin, M.
  SPRINGER-VERLAG BERLIN.2015: 563-594
- **Low Overhead Broadcast Encryption from Multilinear Maps**
  Boneh, D., Waters, B., Zhandry, M.
  edited by Garay, J. A., Gennaro, R.
  SPRINGER-VERLAG BERLIN.2014: 206-223
- **Multiparty Key Exchange, Efficient Traitor Tracing, and More from Indistinguishability Obfuscation**
  Boneh, D., Zhandry, M.
  edited by Garay, J. A., Gennaro, R.
  SPRINGER-VERLAG BERLIN.2014: 480-499
- **Quantum-Secure Message Authentication Codes**
  Boneh, D., Zhandry, M.
  edited by Johansson, T., Nguyen, P. Q.
  SPRINGER-VERLAG BERLIN.2013: 592-608
- **Secure Signatures and Chosen Ciphertext Security in a Quantum Computing World**
  Boneh, D., Zhandry, M.
  edited by Canetti, R., Garay, J. A.
  SPRINGER-VERLAG BERLIN.2013: 361-379
- **How to Construct Quantum Random Functions** *IEEE 53rd Annual Symposium on Foundations of Computer Science (FOCS)*
  Zhandry, M.
  IEEE.2012: 679–687
- **Secure Identity-Based Encryption in the Quantum Random Oracle Model**
  Zhandry, M.
  edited by SafaviNaini, R., Canetti, R.
  SPRINGER-VERLAG BERLIN.2012: 758-775
- **Random Oracles in a Quantum World** *17th Annual International conference on the Theory and Application of Cryptology and Information Security*
  Boneh, D., Dagdelen, O., Fischlin, M., Lehmann, A., Schaffner, C., Zhandry, M.
  SPRINGER.2011: 41–69
- **Random Oracles in a Quantum World**
  Boneh, D., Dagdelen, O., Fischlin, M., Lehmann, A., Schaffner, C., Zhandry, M.
  edited by Lee, D. H., Wang, X. Y.
  SPRINGER.2011: 41-+