Research Statement

Chuhan Lu

Jan, 2025

My research is in quantum cryptography, especially in quantum pseudorandomness.

References

[ABF+22] Scott Aaronson, Adam Bouland, Bill Fefferman, Soumik Ghosh, Umesh Vazirani, Chenyi Zhang, and Zixin Zhou. Quantum pseudoentanglement. *arXiv preprint arXiv:2211.00747v2*, 2022.

[AGQY22] Prabhanjan Ananth, Aditya Gulati, Luowen Qian, and Henry Yuen. Pseudorandom (function-like) quantum state generators: New definitions and applications. In *20th Theory of Cryptography Conference – TCC 2022*, pages 237–265. Springer, 2022.

[AQY22] Prabhanjan Ananth, Luowen Qian, and Henry Yuen. Cryptography from pseudorandom quantum states. In *Advances in Cryptology – CRYPTO 2022*, pages 208–236. Springer, 2022.

[BBSS23] Amit Behera, Zvika Brakerski, Or Sattath, and Omri Shmueli. Pseudorandomness with proof of destruction and applications. In Guy Rothblum and Hoeteck Wee, editors, *Theory of Cryptography*, pages 125–154, Cham, 2023. Springer Nature Switzerland.

[BBV24] James Bartusek, Zvika Brakerski, and Vinod Vaikuntanathan. Quantum state obfuscation from classical oracles. In *Proceedings of the 56th Annual ACM Symposium on Theory of Computing*, pages 1009–1017, 2024.

[BCHJ+21] Fernando G.S.L. Brandão, Wissam Chemissany, Nicholas Hunter-Jones, Richard Kueng, and John Preskill. Models of quantum complexity growth. *PRX Quantum*, 2:030316, Jul 2021.

[BCQ23] Zvika Brakerski, Ran Canetti, and Luowen Qian. On the Computational Hardness Needed for Quantum Cryptography. In *14th Innovations in Theoretical Computer Science Conference – ITCS 2023*, volume 251 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 24:1–24:21. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2023.

[BFV20] Adam Bouland, Bill Fefferman, and Umesh Vazirani. Computational pseudorandomness, the wormhole growth paradox, and constraints on the AdS/CFT duality. In *11th Innovations in Theoretical Computer Science Conference – ITCS 2020*. Schloss Dagstuhl-Leibniz-Zentrum für Informatik, 2020.

[BHHP24] John Bostanci, Jonas Haferkamp, Dominik Hangleiter, and Alexander Poremba. Efficient quantum pseudorandomness from hamiltonian phase states. *arXiv preprint arXiv:2410.08073*, 2024.

[BKNY23] James Bartusek, Fuyuki Kitagawa, Ryo Nishimaki, and Takashi Yamakawa. Obfuscation of pseudo-deterministic quantum circuits. In *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*, pages 1567–1578, 2023.

[BM21] James Bartusek and Giulio Malavolta. Indistinguishability obfuscation of null quantum circuits and applications. *arXiv preprint arXiv:2106.06094*, 2021.

[BMS16] Michael J Bremner, Ashley Montanaro, and Dan J Shepherd. Average-case complexity versus approximate simulation of commuting quantum computations. *Physical review letters*, 117(8):080501, 2016.

[BS19] Zvika Brakerski and Omri Shmueli. (Pseudo) random quantum states with binary phase. In *17th Theory of Cryptography Conference – TCC 2019*, pages 229–250. Springer, 2019.

[BS20] Amit Behera and Or Sattath. Almost public quantum coins. *arXiv preprint arXiv:2002.12438*, 2020.

[CBB+24] Chi-Fang Chen, Adam Bouland, Fernando GSL Brandão, Jordan Docter, Patrick Hayden, and Michelle Xu. Efficient unitary designs and pseudorandom unitaries from permutations. *arXiv preprint arXiv:2404.16751*, 2024.

[CCZZ21] Nai-Hui Chia, Chi-Ning Chou, Jiayu Zhang, and Ruizhe Zhang. Quantum meets the minimum circuit size problem. *arXiv preprint arXiv:2108.03171*, 2021.

[CDSZ22] Sourav Chatterjee, Persi Diaconis, Allan Sly, and Lingfu Zhang. A phase transition for repeated averages. *The Annals of Probability*, 50(1):1 – 17, 2022.

[CGGH24] Bruno P Cavalar, Eli Goldin, Matthew Gray, and Peter Hall. A meta-complexity characterization of quantum cryptography. *arXiv preprint arXiv:2410.04984*, 2024.

[CKV10] Kai-Min Chung, Yael Kalai, and Salil Vadhan. Improved delegation of computation using fully homomorphic encryption. In *Advances in Cryptology–CRYPTO 2010: 30th Annual Cryptology Conference, Santa Barbara, CA, USA, August 15-19, 2010. Proceedings 30*, pages 483–501. Springer, 2010.

[CLLZ21] Andrea Coladangelo, Jiahui Liu, Qipeng Liu, and Mark Zhandry. Hidden cosets and applications to unclonable cryptography. In *Advances in Cryptology–CRYPTO 2021: 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16–20, 2021, Proceedings, Part I 41*, pages 556–584. Springer, 2021.

[Col23] Andrea Coladangelo. Quantum trapdoor functions from classical one-way functions. *arXiv preprint arXiv:2302.12821*, 2023.

[HBM+25] Tobias Haug, Nikhil Bansal, Wai-Keong Mok, Dax Enshan Koh, and Kishor Bharti. Pseudorandom quantum authentication. *arXiv preprint arXiv:2501.00951*, 2025.

[HM24] Taiga Hiroka and Tomoyuki Morimae. Quantum cryptography and meta-complexity. *arXiv preprint arXiv:2410.01369*, 2024.

[HO24] William He and Ryan O'Donnell. Pseudorandom permutations from random reversible circuits. *arXiv preprint arXiv:2404.14648*, 2024.

[Imp95] R. Impagliazzo. A personal view of average-case complexity, 1995.

[IRS21] Rahul Ilango, Hanlin Ren, and Rahul Santhanam. Hardness on any samplable distribution suffices: New characterizations of one-way functions by meta-complexity. In *Electron. Colloquium Comput. Complex*, volume 28, page 82, 2021.

[JLS18] Zhengfeng Ji, Yi-Kai Liu, and Fang Song. Pseudorandom quantum states. In *Advances in Cryptology – CRYPTO 2018*, pages 126–152. Springer, 2018.

[JMW23] Fernando Granha Jeronimo, Nir Magrafta, and Pei Wu. Subset states and pseudorandom states. *arXiv preprint arXiv:2312.15285*, 2023.

[Kac56] Mark Kac. Foundations of kinetic theory. In *Third Berkeley symposium on mathematical statistics and probability*, volume 3, pages 171–197, 1956.

[Kre21] William Kretschmer. Quantum pseudorandomness and classical complexity. In *16th Conference on the Theory of Quantum Computation, Communication and Cryptography – TQC 2021*, pages 2:1–2:20. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2021.

[KT24] Dakshita Khurana and Kabir Tomer. Founding quantum cryptography on quantum advantage. *arXiv preprint arXiv:2409.15248*, 2024.

[KTP20] Isaac Kim, Eugene Tang, and John Preskill. The ghost in the radiation: Robust encodings of the black hole interior. *Journal of High Energy Physics*, 2020(6):1–65, 2020.

[LP21] Yanyi Liu and Rafael Pass. Cryptography from sublinear-time average-case hardness of time-bounded kolmogorov complexity. In *Proceedings of the 53rd Annual ACM SIGACT Symposium on Theory of Computing*, pages 722–735, 2021.

[LQS+24a] Chuhan Lu, Minglong Qin, Fang Song, Penghui Yao, and Mingnan Zhao. Quantum pseudorandom scramblers. In *Theory of Cryptography Conference*, pages 3–35. Springer, 2024.

[LQS+24b] Chuhan Lu, Minglong Qin, Fang Song, Penghui Yao, and Mingnan Zhao. Quantum pseudorandom scramblers. *Manuscript*, 2024.

[LR86] Michael Luby and Charles Rackoff. Pseudo-random permutation generators and cryptographic composition. In *Proceedings of the Eighteenth Annual ACM Symposium on Theory of Computing*, pages 356–363, 1986.

[LV24] Romi Levy and Thomas Vidick. Prs length expansion. *arXiv preprint arXiv:2411.03215*, 2024.

[Mau02] Ueli Maurer. Indistinguishability of random systems. In *Advances in Cryptology—EUROCRYPT 2002: International Conference on the Theory and Applications of Cryptographic Techniques Amsterdam, The Netherlands, April 28–May 2, 2002 Proceedings 21*, pages 110–132. Springer, 2002.

[MH24] Fermi Ma and Hsin-Yuan Huang. How to construct random unitaries. *arXiv preprint arXiv:2410.10116*, 2024.

[MOPS06] Ueli Maurer, Yvonne Anne Oswald, Krzysztof Pietrzak, and Johan Sjödin. Luby-rackoff ciphers from weak round functions? In *Advances in Cryptology-EUROCRYPT 2006: 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, St. Petersburg, Russia, May 28-June 1, 2006. Proceedings 25*, pages 391–408. Springer, 2006.

[MP04] Ueli Maurer and Krzysztof Pietrzak. Composition of random systems: When two weak make one strong. In *Theory of Cryptography Conference*, pages 410–427. Springer, 2004.

[MPR06] Ueli Maurer, Krzysztof Pietrzak, and Renato Renner. Indistinguishability amplification. Cryptology ePrint Archive, Paper 2006/456, 2006. https://eprint.iacr.org/2006/456.

[MPSY24] Tony Metger, Alexander Poremba, Makrand Sinha, and Henry Yuen. Simple constructions of linear-depth t-designs and pseudorandom unitaries. *arXiv preprint arXiv:2404.12647*, 2024.

[MSW22] Ramis Movassagh, Mario Szegedy, and Guanyang Wang. Repeated averages on graphs. *arXiv:2205.04535*, 2022.

[MX24] Tomoyuki Morimae and Keita Xagawa. Quantum group actions. *arXiv preprint arXiv:2410.04777*, 2024.

[MY22a] Tomoyuki Morimae and Takashi Yamakawa. One-wayness in quantum cryptography. Cryptology ePrint Archive, Paper 2022/1336, 2022. https://eprint.iacr.org/2022/1336.

[MY22b] Tomoyuki Morimae and Takashi Yamakawa. Quantum commitments and signatures without one-way functions. In *Advances in Cryptology – CRYPTO 2022*, pages 269–295. Springer, 2022.

[Mye01] Steven Myers. Efficient amplification of the security of weak pseudo-random function generators. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 358–372. Springer, 2001.

[Mye04] Steven Myers. Black-box composition does not imply adaptive security. In *Advances in Cryptology-EUROCRYPT 2004: International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, May 2-6, 2004. Proceedings 23*, pages 189–206. Springer, 2004.

[Pie05] Krzysztof Pietrzak. Composition does not imply adaptive security. In *Annual International Cryptology Conference*, pages 55–65. Springer, 2005.

[Pie06] Krzysztof Pietrzak. Composition implies adaptive security in minicrypt. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 328–338. Springer, 2006.

[SHH24] Thomas Schuster, Jonas Haferkamp, and Hsin-Yuan Huang. Random unitaries in extremely low depth. *arXiv preprint arXiv:2407.07754*, 2024.

[Vau00] Serge Vaudenay. Adaptive-attack norm for decorrelation and super-pseudorandomness. In *Selected Areas in Cryptography: 6th Annual International Workshop, SAC'99 Kingston, Ontario, Canada, August 9–10, 1999 Proceedings 6*, pages 49–61. Springer, 2000.

[YE23] Lisa Yang and Netta Engelhardt. The complexity of learning (pseudo)random dynamics of black holes and other chaotic systems. arXiv:2302.11013, 2023. https://arxiv.org/abs/2302.11013.