Research Statement

Chuhan Lu

My research focuses on quantum pseudorandomness and quantum cryptography. Quantum pseudorandom objects, such as pseudorandom states (PRSs) and pseudorandom unitaries (PRUs), serve as computational substitutes for Haar randomness, the latter being costly to sample exactly and central to many cryptographic, information-theoretic, and physical tasks. Although PRSs were known to be constructible from post-quantum PRFs, the landscape for PRUs was significantly less developed when I began my work. Recent breakthroughs now give fully secure PRUs, and prior to these, my work explored a construction based on *the parallel Kac's walk*, leveraging its rapid mixing to move beyond PRSs toward stronger primitives. A key development that further highlights the significance of this line of work is Kretschmer's oracle separation [Kre21], which shows that quantum pseudorandomness may exist under assumptions weaker than those needed classically. This result, which emerged after the initial formulations of quantum pseudorandom primitives [JLS18], has broadened the cryptographic relevance of the area and provides additional context for the constructions studied in my work. In parallel, I have also pursued related work in quantum zero-knowledge and the study of the Hidden Subgroup Problem.

Pseudorandom State Scramblers via the Parallel Kac's Walk [LQS⁺25b] One of my main contributions introduces pseudorandom state scramblers (PRSSs), a new quantum pseudorandom primitive whose defining property is the ability to map any n-qubit pure state to a pseudorandom state. This capability is shared with PRUs but absent in PRSs, and at the time of this work, even achieving such a basic property beyond PRSs was poorly understood, let alone constructing a fully secure PRU. Defining PRSSs and giving the first construction therefore clarified a key intermediate point that helped narrow the gap between PRSs and PRUs.

Our construction is based on an $O(n)$-step *parallel* Kac's walk, a new variant we developed that mixes *exponentially* faster than the original Kac's walk [Kac56]. When the randomness in each step is replaced with quantum-secure PRPs and PRFs, the walk naturally supports an efficient quantum implementation. It also exhibits a distinct *dispersing* property not present in other constructions, which we believe may lead to interesting applications.

Pseudorandom Unitaries from Parallel Kac's Walk [LQS⁺25a] Following our work on PRSSs, further progress on PRUs soon appeared. Metger et al. [MPSY24] introduced the PFC construction and proved its non-adaptive security. Shortly thereafter, Ma and Huang [MH25] developed the path-recording technique, which they used to establish adaptive security including in settings that allow inverse queries.

Building on progress from the same period, our second main result shows that the parallel Kac's walk construction yields PRUs secure against adaptive adversaries, even under inverse-query access. By applying the path-recording technique, we show that $O(n)$ steps suffice to obtain such security. Our construction provides a modular alternative that relies on fewer cryptographic primitives and offers a distinct route toward achieving PRUs.

Other Research: Barriers for S-NIZKs in a Quantum Setting [LP24] and HSP on $\mathbb{Z}^n$ [Lu] Beyond pseudorandomness, I have contributed to two further directions.

1. *Impossibility for S-NIZKs.* We build on Pass's classical impossibility result [Pas13] and employ the meta-reduction paradigm in a quantum setting that allows quantum computation and quantum advice but not superposition adversarial queries. Assuming post-quantum OWF, we show that adaptive soundness for S-NIZKs for NP-complete languages cannot be reduced to any falsifiable assumption via a quantum black-box reduction.

2. *Hidden Subgroup Problem over $\mathbb{Z}^n$.* We revisit Mosca's algorithm [Mos99] for the full-rank subgroup case and present a lattice-based analysis that is more accessible. The algorithm decomposes into three steps, each of which can be analyzed independently. This perspective makes the analysis easier to follow for readers less familiar with abstract group theory.

Ongoing Research Projects Here I briefly talk about my current research projects:

1. Proving scalable PRU*.* The security of existing PRU constructions depends on system size, making them less reliable when the system is small. A distinct feature of our construction is that it applies a modular step repeatedly, suggesting a form of scalability in which the security level can be tuned independently of the system size by adjusting the number of steps. We are currently studying how to establish scalability for our construction and examining applications that could benefit from it.

2. Characterizing Microcrypt. We aim to identify complexity-theoretic notions that capture the hardness underlying Microcrypt. As a candidate direction, we are investigating meta-complexity, focusing in particular on time-bounded symmetry of information (SOI), whose existence would imply that classical OWFs are efficiently invertible. Our goal is to develop a quantum analogue of SOI and to determine whether it can serve as a foundation for characterizing one-wayness in quantum settings, including objects such as one-way channels and one-way states.

3. Developing simpler zero-knowledge protocols for promise QMA*.* Prior work shows that constant-round ZK for QMA can be obtained when the underlying complete problem admits local verification. Motivated by this paradigm, we are investigating ZKPs for promise-QMA languages with quantum state inputs [CCHS24], aiming to identify problems that allow such local checks. Recent work by Malavolta [Mal25] achieves ZK under Microcrypt assumptions via an MPC reduction, leading to polynomial-round protocols. Our goal is to obtain constant-round ZKPs under similar assumptions.

4. HSP on $\mathbb{Z}^n$ beyond the full-rank case. Although the non–full-rank case is understood [Kup25], we are revisiting this setting by reformulating the algorithm through lens of QPE on suitable shift operators. We aim to obtain a cleaner and more modular understanding of how approximation errors arise and accumulate, compared to the direct Shor-type analyses used in prior work.

Future Research Directions A broader goal of my future work is to bridge the gap between the abstract landscape of quantum pseudorandom primitives and the practical cryptographic tools they could enable. Current constructions of strong primitives such as PRSSs and PRUs are theoretically powerful but lack clear applications and are difficult to realize on near-term hardware due to their non-local structure and sensitivity to noise. Developing practical constructions, identifying uses that genuinely require these stronger notions, and understanding how their security can be amplified will be central themes of my research moving forward.

1. Improving the practicality of the parallel Kac's walk construction. The current construction requires using non-local permutations and substantial randomness. I plan to investigate whether the walk can be implemented using more localized circuit architectures and whether the randomness can be reduced or partially derandomized. The goal is to obtain versions of the construction that use more restricted gate sets and align better with near-term hardware.

2. Finding cryptographic applications requires PRSS*s/*PRU*.* Our construction exhibits properties not shared by others. Under the truly random version, for any input state, the family of output states forms an ϵ-net of the output space, so the outputs do not concentrate in a small region of the sphere. It is natural to ask whether this property can lead to interesting cryptographic applications.

3. Understanding black-box amplification of quantum security properties. In classical cryptography, weaker security properties of pseudorandom primitives can be strengthened by simple black-box constructions, such as direct sequential or parallel composition [MPR07]. Whether analogous amplifications, or slightly more involved but still black-box modifications, exist in the quantum setting is unclear. I aim to understand whether security amplification can be achieved in a black-box manner for quantum pseudorandom primitives (e.g. constructing adaptive PRUs from non-adaptive ones or upgrading primitives that allow only forward queries to ones secure against inverse queries), or whether inherent separations rule out such possibilities.

References

[CCHS24] Nai-Hui Chia, Kai-Min Chung, Tzu-Hsiang Huang, and Jhih-Wei Shih. Complexity theory for quantum promise problems. *arXiv preprint arXiv:2411.03716*, 2024. 2

[JLS18] Zhengfeng Ji, Yi-Kai Liu, and Fang Song. Pseudorandom quantum states. In *Advances in Cryptology – CRYPTO 2018*, pages 126–152. Springer, 2018. 1

[Kac56] Mark Kac. Foundations of kinetic theory. In *Third Berkeley Symposium on Mathematical Statistics and Probability*, volume 3, pages 171–197, 1956. 1

[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. 1

[Kup25] Greg Kuperberg. The hidden subgroup problem for infinite groups. *arXiv preprint arXiv:2507.1849*, 2025. 2

[LP24] Chuhan Lu and Nikhil Pappu. Notions of quantum reductions and impossibility of statistical NIZK. Cryptology ePrint Archive, Paper 2024/1847, 2024. 1

[LQS$^+$25a] Chuhan Lu, Minglong Qin, Fang Song, Penghui Yao, and Mingnan Zhao. Parallel kac's walk generates PRU. *arXiv preprint arXiv:2504.14957*, 2025. 1

[LQS$^+$25b] Chuhan Lu, Minglong Qin, Fang Song, Penghui Yao, and Mingnan Zhao. Quantum pseudorandom scramblers. In Elette Boyle and Mohammad Mahmoody, editors, *Theory of Cryptography*, pages 3–35, Cham, 2025. Springer Nature Switzerland. 1

[Lu] Chuhan Lu. A note on the hidden subgroup problem on $\mathbb{Z}^n$. https://chuhanlu.github.io/. Manuscript. 1

[Mal25] Giulio Malavolta. The knowledge complexity of quantum problems. *arXiv preprint arXiv:2510.06923*, 2025. 2

[MH25] Fermi Ma and Hsin-Yuan Huang. How to construct random unitaries. In *Proceedings of the 57th Annual ACM Symposium on Theory of Computing*, STOC '25, pages 806–809, New York, NY, USA, June 2025. Association for Computing Machinery. 1

[Mos99] Michele Mosca. Quantum computer algorithms. Ph.D. thesis, University of Oxford, 1999. 1

[MPR07] Ueli Maurer, Krzysztof Pietrzak, and Renato Renner. Indistinguishability amplification. In Alfred Menezes, editor, *Advances in Cryptology – CRYPTO 2007*, pages 130–149, Berlin, Heidelberg, 2007. Springer Berlin Heidelberg. 2

[MPSY24] Tony Metger, Alexander Poremba, Makrand Sinha, and Henry Yuen. Simple Constructions of Linear-Depth t-Designs and Pseudorandom Unitaries. In *2024 IEEE 65th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 485–492, October 2024. 1

[Pas13] Rafael Pass. Unprovable security of perfect NIZK and non-interactive non-malleable commitments. In *Theory of Cryptography Conference*, pages 334–354. Springer, 2013. 1