Research Statement

Chuhan Lu

My research focuses on quantum pseudorandomness, quantum cryptography, and quantum algorithms. Quantum pseudorandom objects, such as pseudorandom states (PRSs) and pseudorandom unitaries (PRUs), serve as computational substitutes for Haar randomness, which is costly to sample exactly and central to many algorithmic and cryptographic 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 have now resolved the construction of fully secure PRUs. Prior to these developments, my work contributed an approach based on the parallel Kac's walk, whose rapid mixing played a key role in exploring how to move beyond PRSs toward stronger pseudorandom primitives. This line of research is also motivated by Kretschmer's oracle separation [Kre21], which shows that PRSs (and PRUs) can exist even if BQP = QMA, suggesting that quantum pseudorandomness may rely on assumptions strictly weaker than classical one-way functions. More broadly, my work fits within the Microcrypt perspective, which seeks to understand the landscape of cryptographic primitives in settings that diverge fundamentally from the classical world.

Pseudorandom State Scramblers via the Parallel Kac's Walk One of my main contributions introduces pseudorandom state scramblers (PRSSs), a new computational pseudorandom primitive whose defining property is that it maps any n-qubit pure state to a pseudorandom state. This capability is shared with PRUs but absent in PRSs. In this work, we construct PRSSs from an $O(n)$-step parallel Kac's walk, a random walk on the unit sphere shown to mix exponentially faster than the classical Kac's walk.

A key technical contribution is that we analyze this walk using the path-coupling method, which yields rapid convergence guarantees and enables an efficient implementation. By replacing the randomness in each step with a quantum-secure PRF, we obtain a PRSS and prove its computational pseudorandomness. At the time of this work, this provided a new intermediate primitive that helped clarify the gap between PRSs and the then-unknown construction of fully secure PRUs.

Pseudorandom Unitaries from Parallel Kac's Walk In subsequent breakthroughs, Metger et al. and Ma-Huang established fully secure PRUs using the PFC construction and the path-recording method [MPSY24, MH24]. Building on the same period of progress, our second main result shows that our parallel Kac's walk construction also leads to PRU secure against adaptive adversaries, with or without inverse queries.

In this work, we apply the path-recording technique to the parallel Kac's walk and show that an $O(n)$-step walk suffices to achieve adaptive security. Although this construction is not as simple as PFC, it consists of modular single-step components, relies on fewer cryptographic primitives, and provides an alternative approach. Together with the PRSS result, this work demonstrates how fast-mixing random walks can serve as a foundation for constructing both state- and unitary-level pseudorandomness.

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

Impossibility for S-NIZKs. In this work, we build on Pass's classical impossibility result [**?**] and employ the meta-reduction paradigm in a quantum setting. Our model allows quantum computation and quantum advice but does not allow superposition adversarial queries, which keeps the setting aligned with the classical-query framework. Under the assumption of post-quantum one-way functions secure against quantum advice, 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.

Hidden Subgroup Problem over $\mathbb{Z}^n$. In this work, we revisit Mosca's algorithm [**?**] for the HSP on $\mathbb{Z}^n$ and present a more accessible lattice-theoretic analysis. The algorithm is decomposed into three modular steps: recovering an orthogonal sublattice via one-dimensional HSPs, identifying the quotient group, and computing a basis using lattice tools. This lattice-based perspective is intended to make the structure of the algorithm more transparent to readers not familiar with abstract group theory.

Future Research Directions Looking forward, I aim to pursue several directions that naturally follow from my research:

1. Improving the practicality of parallel Kac-based constructions. I plan to explore localized circuit architectures and restricted gate sets to better align these constructions with near-term hardware.

2. Understanding black-box amplification of security properties. I am interested in whether adaptivity, invertibility, or related guarantees can be strengthened using black-box techniques, paralleling classical results.

3. Exploring applications enabled by PRSSs and PRUs. Because PRSSs can scramble arbitrary states and exhibit a dispersing property, I plan to investigate new cryptographic applications that go beyond what PRSs alone can support.

4. Investigating assumptions weaker than quantum-secure one-way functions. A central question in Microcrypt is whether pseudorandom primitives can be based on strictly weaker assumptions. I aim to examine quantum-native hardness assumptions and clarify their relationships to classical ones.

My long-term goal is to deepen the theory of quantum pseudorandomness, improve constructions based on fast-mixing processes, understand the limits of quantum reductions, and develop new applications in quantum cryptography and complexity theory.

References

[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

[MH24] Fermi Ma and Hsin-Yuan Huang. How to construct random unitaries. *arXiv preprint arXiv:2410.10116*, 2024. 1

[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. 1