Time Schedule: Aug 19, 2022 (GMT+8)

9:00-9:30 **Fan Wei** TBD

9:30-10:00 **Peng Zhang** Hardness Results for Weaver’s Discrepancy Problem

10:00-10:30 **Jiahui Liu** Quantum Copy Protection and Unclonable Cryptography

10:30-11:00 **Shunhua Jiang** TBD

11:00-12:00 Panel Discussion

Basic information:

Fan Wei: <https://sites.google.com/view/fan-wei/home> (Instructor @Princeton, extremal combinatorics)

Peng Zhang: <https://sites.google.com/site/pengzhang27182/> (Faculty@Rutgers, algorithms)

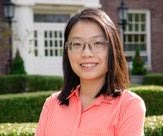
Jiahui Liu: <https://www.cs.utexas.edu/~jiahui/> (PhD student@UT Austin, crypto)

Shunhua Jiang: <https://www.cs.columbia.edu/~jiangsh/> (PhD student@Columbia, data structures)

Forum information: TBA

Title, abstract and bio:

Fan Wei:



Title: TBD

Abstract: TBD

Bio: Fan Wei completed her PhD in mathematics in 2019 from Stanford University, where she was advised by Jacob Fox. She spent one year as a post-doctoral member at the Institute for Advanced Study where she was part of Avi Wigderson's CSDM (computer science and discrete math) program and funded through Founders’ Circle Member. She is currently an instructor at Princeton University math department, where she has and is funded by Simons Foundation, Algorithms & Geometry Unit, and NSF grant. She will join Duke University as assistant professor in mathematics next year.

Prior to that, she received bachelors degree in Mathematics from MIT, and a Master of Advanced Study with Distinction from Cambridge University, UK. She has also had internships at Microsoft Research New England and Microsoft Research Redmond Theory group.

Fan Wei's research is on extremal combinatorics, probabilistic combinatorics, applications of combinatorics to computer science. She is especially interested in using tools from probability, analysis and algebra to analyze large networks or other combinatorial objects.

Jiahui Liu:



Title: Quantum Copy Protection and Unclonable Cryptography

Talk Abstract: The unclonability of quantum information has been applied to quantum cryptography. In 1963, Wiesner put forward the pioneering idea of quantum money: banknotes encoded as quantum states that cannot be forged simply due to quantum mechanics. The idea was later used in the well-known BB84 quantum key distribution(QKD) protocol.

In this talk, I will present applications of unclonable quantum states beyond information-theoretic constructions such as Wiesner quantum money and QKD: we use and improve some past tools for quantum money and combine with techniques from classical cryptography to achieve more applications of computationally unclonable states.

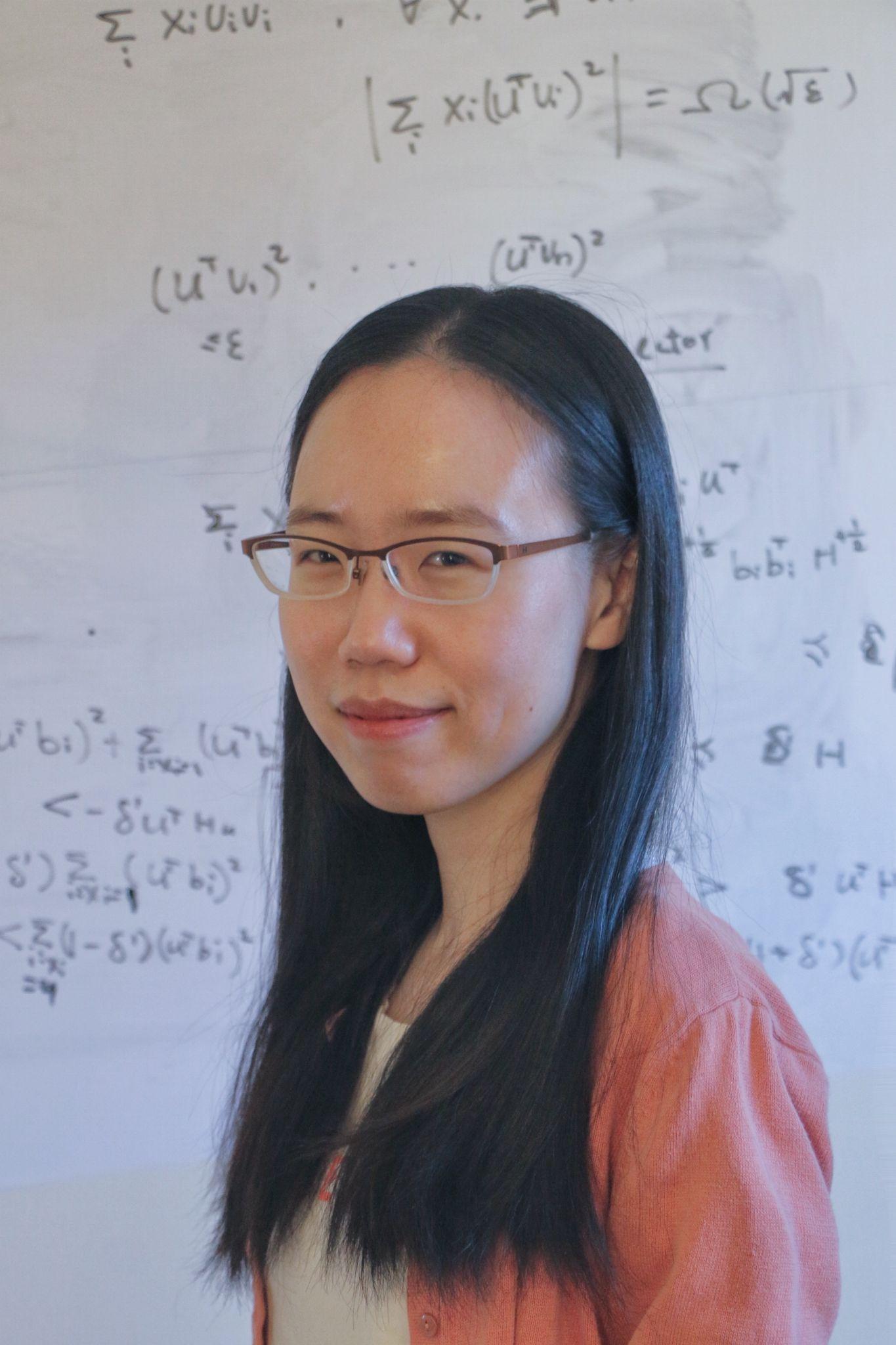
One of these applications is quantum copy protection, first proposed by Aaronson in 2009: one can encode classical functional information into a quantum state so that this state can be used to evaluate a classical functionality but cannot be copied into two. Aaronson gave an open question on whether we can build a quantum copy protection scheme relative to a classical oracle.

I will then present a quantum copy protection scheme, using a classical oracle inspired by the 2012 Aaronson and Christiano's public key quantum money scheme. Furthermore, we can in fact replace the use of structured oracles with well-founded cryptographic primitives, when copy protecting specific functionalities that can lead to broad applicability.

Bio:

Jiahui Liu is a fourth-year PhD student at UT Austin. Her main research interests are in the intersection of quantum information and cryptography, especially applications of quantum information in building cryptographic tools unrealizable by classical information. She is also interested in post-quantum security of cryptography and quantum information science in general.

Peng Zhang



Title: Hardness Results for Weaver’s Discrepancy Problem

Abstract: Marcus, Spielman and Srivastava (Annals of Mathematics, 2015) solved the Kadison-Singer Problem by proving a strong form of Weaver’s conjecture: They showed that for all $\alpah > 0$ and all lists of vectors of norm at most $\sqrt{\alpha}$ whose outer products sum to the identity, there exists a signed sum of those outer products with operator norm at most $\sqrt{8 \alpha} + 2 \alpha$. Besides its relation to the Kadison-Singer problem, Weaver’s discrepancy problem has applications in graph sparsification and randomized experimental design.

We prove that it is NP-hard to distinguish such a list of vectors for which there is a signed sum that equals the zero matrix from those in which every signed sum has operator norm at least $k \sqrt{\alpha}$, for some absolute constant $k > 0$. Thus, it is NP-hard to construct a signing that is a constant factor better than that guaranteed to exist.

This talk will be based on joint work with Daniel Spielman.

Bio: Peng Zhang is an assistant professor in Computer Science at Rutgers University. Before joining Rutgers, she obtained her Ph.D. from Georgia Tech and then was a postdoc at Yale University. Her research lies broadly in the design of efficient algorithms, including solving structured linear equations and linear programs, discrepancy theory and its applications in randomized experimental design.

Shunhua Jiang

Title: TBD

Abstract: TBD

Bio: TBD