Abstract
Cryptographic protocols have been developed for a variety of tasks, including electronic auctions, electronic voting systems, privacy preserving data mining and more. The Internet allows for the concurrent execution of cryptographic protocols. Such concurrency severely challenges their security.

In this talk we introduce a novel technique for transforming any "stand-alone" secure protocol (i.e., one whose security is only guaranteed if executed in isolation) into one that is secure under concurrent executions. Contrary to previous results in the literature, this result is established without relying on additional trusted infrastructure or cryptographic hardness assumptions.

Biography
Huijia Lin is a Ph.D. candidate in the Department of Computer Science at Cornell. Her research interests are in the field of Cryptography. She is a recipient of the Microsoft Graduate Student Fellowship.