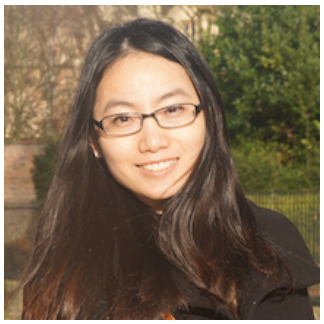
## The University of Chicago Computer Science Department

## PRESENTS:

# "Secure Computer Hardware in the Age of Pervasive Security Attacks"




**Mengjia Yan**

*University of Illinois at Urbana-Champaign*



**Abstract:**

Recent attacks such as Spectre and Meltdown have shown how vulnerable modern computer hardware is. The root cause of the problem is that computer architects have traditionally focused on performance and energy efficiency. Security has never been a first-class requirement. Moving forward, however, this has to radically change: we need to rethink computer architecture from the ground-up for security.

As an example of this vision, in this talk, I will focus on speculative execution in out-of-order processors --- a core computer architecture technology that is the target of the recent attacks. I will describe InvisiSpec, the first robust hardware defense mechanism against speculative (a.k.a transient) execution attacks. The idea is to make loads invisible in the cache hierarchy, and only reveal their presence at the point when they are safe. Once an instruction is deemed safe, our hardware is able to cheaply modify the cache coherence state in a consistent manner. Further, to reduce the cost of InvisiSpec and increase its protection coverage, I propose Speculative Taint Tracking (STT). This is a novel form of information flow tracking that is specifically designed for speculative execution. It reduces cost by allowing tainted instructions to become safe early, and by effectively leveraging the predictor hardware that is ubiquitous in modern processors. Further improvements of InvisiSpec-STT can be attained with new compiler techniques. Finally, I will conclude my talk by describing ongoing and future directions towards designing secure processors.


**Bio:**

*Mengjia Yan is a Ph.D. student at the University of Illinois at Urbana-Champaign (UIUC), working with Professor Josep Torrellas. Her research interest lies in the areas of computer architecture and hardware security, with a focus on defenses against transient execution attacks and cache-based side channel attacks. Her work has appeared in some of the top venues in computer architecture and security, and has sparked a large research collaboration initiative between UIUC and Intel. Mengjia received the UIUC College of Engineering Mavis Future Faculty Fellow, the Computer Science W.J. Poppelbaum Memorial Award, a MICRO TopPicks in Computer Architecture Honorable Mention, and was invited to participate in two Rising Stars workshops.*

**Monday, March 11, 2019**
**3:30 pm**
**JCL 390**
**Host: Shan Lu**