# 北京大学信息工程学院学术讲座

主讲人： Zhong Shao

时间： 7月14日（周六）14:30-15:30

地点： 西丽大学城北京大学深圳研究生院 C303

## CertiKOS: From Hacker-Resistant OS to Certified Heterogeneous Systems

## CertiKOS: 从反黑客攻击操作系统到认证异构系统

**Zhong Shao （邵中）**

**Thomas L. Kempner Professor & Chair of Computer Science, Yale University**

**（耶鲁大学计算机科学系主任、Thomas L. Kempner教授）**

## Abstract

New exciting "vertical" themes in the field of computer science often require complex computing platforms with strong properties such as safety, security, resilience, resource efficiency, fairness, and privacy. In this talk, we present a novel compositional approach for building certified heterogeneous systems that aim to provide many such trustworthiness guarantees. Also, we have successfully developed the CertiKOS certified OS kernel and verified its contextual functional correctness in the Coq proof assistant, which is the world's first proof of functional correctness of a complete, general-purpose concurrent OS kernel with fine-grained locking. We show how to extend our base kernel with new features such as virtualization, interrupts and device drivers, and end-to-end information flow security, and how to quickly adapt existing verified layers to build new certified kernels for modern heterogeneous platforms.

在计算机科学领域，新兴的“垂直型”课题通常需要复杂的计算平台，对安全性、弹性、资源效率、公平性和私密性等有着极高的要求。为了达到这些性能，我们提出了一种新的构造认证异构系统的方法。此外，我们成功研发了认证操作系统内核CertiKOS，并在Coq证明助手中验证了语境功能正确性。这是世界上首个对完整、通用的，采用细粒度锁的并发操作系统内核的功能正确性证明。我们还展示了如何在我们的基础内核上增加虚拟化、中断和设备驱动等特性和保证端到端的信息流安全性，以及如何快速调整现有认证层以构建适用于现代化认证平台的新内核。

## Biography

Zhong Shao earned his PhD in Computer Science from Princeton University in 1994. He currently leads the FLINT group which aims to develop new languages and tools for building large-scale certified system software. During the last 15 years, Shao and his FLINT group have led and pioneered work on language-based approaches to safety and security, certified OS kernels and hypervisors, compositional resource bound analysis, certified compilation, and formal methods. Shao's work on CertiKOS is widely considered as a breakthrough toward building hacker-resistant operating systems that are provably free from cyber vulnerabilities. Shao is also a co-founder of a new blockchain startup, CertiK, which aims to develop a formal verification platform for next-generation smart contracts and blockchain ecosystems.

北京大学信息工程学院

School of Electronic and Computer Engineering

Peking University