北京大学前沿计算研究中心
Center on Frontiers of Computing Studies, Peking University

静园5号院
科 研 讲 座
2019年第11号

Logic Encryption for Hardware IP Protection: Trilemma and Solutions

Prof. Hai Zhou

Department of Electrical & Computer Engineering
Northwestern University

Host: 梁云 副教授，CECA
2019年7月31日 星期三 10:00–11:00
北京大学静园五院102

Abstract

With the increases of fabrication outsourcing and supply chain complexity, unauthorized chip overproduction and IP piracy via reverse engineering have become big headaches for semiconductor industry. Logic encryption, a technique to modify a circuit with extra key-inputs to lock it from unauthorized use, has the potential to relieve these pains. However, after more than a decade of research, the first batch of proposed solutions have been shown to be vulnerable to an oracle-based SAT attack. Post SAT-attack proposals have also been shown to have various drawbacks. The most serious one is the vulnerability under structural analysis.

In this talk, I will discuss a trilemma among locking robustness, structural security, and encryption efficiency in existing solutions. I will also present our solutions to both locking robustness and structural security. A roadmap for completely solving the trilemma will be discussed at the end.

Biography

Hai Zhou is a professor in the ECE department at Northwestern University. His research interests are in algorithm design and formal methods, and their applications to security and electronic design automation. He has published more than 150 papers in conferences and journals in these areas. His research has been supported by NSF, SRC, and semiconductor industry. He was a recipient of an NSF CAREER award.

http: //cfcs.pku.edu.cn/