SEMINAR ANNOUNCEMENT

DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING
Faculty of Engineering
Website: https://www.eng.nus.edu.sg/ece/

Area: Integrated Circuits & Embedded Systems

Host: Dr Lin Longyang

TOPIC	**:**	**Machine learning-based strategy for Side-channel analysis countermeasure**
SPEAKER	**:**	**Mr Fang Qiang** **Graduate student, ECE Dept, NUS**
DATE	**:**	**22 June 2020, Monday**
TIME	**:**	**4pm to 5pm**
WEBINAR	**:**	**https://nus-sg.zoom.us/j/97438133014?pwd=dG5TWWtDZ1RLS1JxZHBPQzZPZGNIZz09** **Meeting ID: 974 3813 3014** **Password: 447285**

ABSTRACT

Side channel attack (SCA) has become one of the major threats to cryptographic devices as it can noninvasively reveal the key by performing statistical analysis to the side-channel information such as power or electromagnetic field. Consequently, hardware countermeasures for side channel attack have been extensively studied to protect crypto circuits and systems. Machine learning-based countermeasure is an attractive and powerful solution but yet to be investigated.

The objective of this seminar is to discuss a new machine learning-based side-channel attack countermeasure technique. Run-time data traces are adopted to develop and test the machine learning techniques, which also proved the effectiveness of machine learning techniques on side channel attack countermeasure.

BIOGRAPHY

Fang Qiang received his Bachelor's Degree in Electrical Engineering & Automation from Xi'an Jiaotong University in China and Master' Degree in Electrical & Computer Engineering department from National University of Singapore. He is currently pursuing a PhD degree in the Green IC Group at NUS. His research interest includes machine learning techniques for secure intra-chip communication and counteraction of Power Analysis attacks.

https://www.eng.nus.edu.sg/ece/highlights/events/