Severe security threats and alerts associated with the use of smart devices have drawn increasing public attentions since the inception of Internet of Things (IoT) in late 1990s. The industry projection of 30 billion connected devices by 2020 with the booming of IoT implies a 300 million strong army waiting to launch a massive destruction if only one percent of them are malicious or fake hardware. Because IoT is a network of heterogeneous “things” that are not customarily associated with the internet, the existing forms of supply-chain tagging or unique identity used for authentication of devices connected to the internet can be easily compromised to create attacks that could introduce catastrophic economic and safety treats. As most IoT devices rely on sensor data to acquire information about users and their environment, the leakage of device identities may also leak physical locations and movements, which can be utilized for criminal attacks.

In this light, silicon Physical Unclonable Function (PUF), a burgeoning technology rooted in 2002, emerges as an inexpensive security primitive to overcome the device tagging problem by its radically different way of generating and processing secret keys in security hardware. A rapid development of PUFs was witnessed in the late 2000s with leapfrog advancement towards their quality enhancement. This effort to overcome the mediocre practicality of ordinary PUFs has a positive impact towards their application development and commercialization. Meanwhile, the commercial viability of PUFs as a security token for device identification has incentivized their attacks. With enhanced speed and precision of measurements made more affordable, side channel analysis is becoming more reachable to recover the integrated secret of the “black box” PUF. The blossoming of machine learning has also led to myth-breaking successes over the last few years in accurately predicting the “unpredictable” responses and physically cloning the “unclonable” PUFs. Identifying the vulnerabilities and new threat landscapes of existing PUF structures has been an active ongoing research effort. Understanding the underpinning of these attacks will impel countermeasures to undermine their chance of success beyond the complexity that makes them possible in the first place.

Biography:
Chip-Hong Chang received the B.Eng. (Hons.) degree from the National University of Singapore, in 1989, and the M. Eng. and Ph.D. degrees from Nanyang Technological University (NTU), Singapore, in 1993 and 1998, respectively. He served as a Technical Consultant in industry prior to joining the School of Electrical and Electronic Engineering (EEE), NTU, in 1999, where he is currently an Associate Professor. He holds joint appointments with the university as Assistant Chair of Alumni of the School of EEE from June 2008 to May 2014, Deputy Director of the Center for High Performance Embedded Systems from 2000 to 2011, and Program Director of the Center for Integrated Circuits and Systems from 2003 to 2009.

Speaker:
Prof. Chip Hong Chang
School of Electrical and Electronic Engineering Nanyang Technological University, Singapore