Department of Electrical Engineering
香港城市大學
City University of Hong Kong

CityU Architecture Lab for Arithmetic and Security (CALAS)
Seminar Series

Security of Semiconductor Chips: Threats, Attacks and Emerging Defences

University of Southampton

Dr. Basel Halak, Associate Professor
Director of the Cyber Security Academy with the University of Southampton

Abstract:

The globalization of supply chains, driven by the pursuit of cost reductions and competitive advantages, has reshaped the hardware industry into a multinational, distributed enterprise. While this transformation has unlocked significant efficiencies, it has also exposed critical vulnerabilities. The hardware supply chain now faces escalating challenges such as intellectual property (IP) piracy, counterfeiting, and the proliferation of hardware Trojan (i.e. malicious modifications that can severely compromise systems). The consequences of these threats are far-reaching. Financially, counterfeiting alone drains billions of dollars from the global economy annually. Operationally, compromised hardware presents grave security risks, particularly when deployed in critical infrastructure and military applications, where breaches can have catastrophic consequences. This presentation will explore these pressing issues, examining the security challenges that affect modern electronic systems. It will highlight emerging mitigation strategies, with a particular focus on machine learning (ML) technologies. Additionally, the talk will explore recent initiatives and regulatory advancements designed to combat these vulnerabilities and fortify the security of the global hardware supply chain.

Biography:

Dr Basel Halak an Associate Professor of secure electronics and the Director of the Cyber Security Academy with the University of Southampton. He is also leading European Masters in Embedded Computing Systems (EMECS) . Dr Halak is a visiting scholar at the Technical University of Kaiserslautern, Norwegian University of Science and Technology , and Polytechnic di Torino. He previously served as a visiting professor at the Kazakh-British Technical University 2017. Dr. Halak's expertise spans Digital Systems Design, Hardware Security and Applied Cryptography. and he has authored over 100-refereed conference and journal papers, and seven books, including the first textbook on Physically Unclonable Functions, and the first book on Hardware Supply Chain Security. Beyond academia, Dr. Halak has collaborated extensively with industry such as ARM, Arqit, Schneider Electric, and Ericsson. Dr Halak is the recipient of the industrial fellowship from the Royal Academy of Engineering and the National Teaching Fellowship awarded by the Advance Higher Education(HE) Academy . He actively contributes to the global research community as a member of technical program committees for leading conferences such as HOST, IEEE DATE, IEEE DAC, IVSW, ICCCA, ICCCS, MTV and EWME. He is an Associate Editor of IEEE access and a Guest Editor of the IET circuit devices and system journal.

28 January 2026 (Wednesday); HKT 4pm – 6pm; LT-8; Zoom link (https://cityu.zoom.us/j/96742093029)