SEMINAR ANNOUNCEMENT

DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING
COLLEGE OF DESIGN AND ENGINEERING
Website: https://cde.nus.edu.sg/ece

Area: Integrated Circuits & Embedded Systems

Host: Associate Professor Jerald Yoo

IEEE Solid-State Circuit Society (SSCS) Technical Seminar

TOPIC	:	**Hardware Acceleration of Functional Encryption and Its Security Measure**
SPEAKER	:	**Professor Makoto Ikeda** **The University of Tokyo, Japan**
DATE	:	**Tuesday, 13 December 2022**
TIME	:	**3:20PM to 4:20PM**
VENUE	:	**E5-02-32** **NUS College of Design and Engineering, NUS**

ABSTRACT

This talk will introduce basics of elliptic curve-based encryption algorithms, and discuss on optimization of their hardware implementation, including, algorithm selection, architecture, scheduling, and measured results. This talk will also cover applications to functional encryption acceleration, such as attribute-based encryption, and also cover hardware acceleration of post-quantum encryption. In addition, security measures of such functional encryption will be also discussed.

BIOGRAPHY

Makoto Ikeda received his BE, ME, and PhD degrees all from Electrical Engineering of the University of Tokyo, in 1991, 1993, and 1996, respectively, He joined the University of Tokyo as a faculty member in 1996, and is now full professor there.

For past 26 years as a faculty member, he belongs to Electrical Engineering for education and research, and VLSI Design and Education Center for chip design platform activities for entire Japanese Universities. His research interests including hardware security, smart image sensor designs, and time-domain signal processing. He has been belonging to numerous international conference activities, including ISSCC, for 18-year as committee member and ISSCC 2021 ITPC Chair, VLSI Symposium for more than 24-year as committee member and 2017 Program Chair and 2019 Symposium Chair, and A-SSCC from the beginning as committee member and 2015 Program Chair, and many others. He served IEEE SSCS Distinguished Lecturer in 2015 and 2016. He is a Senior member of IEEE.

https://cde.nus.edu.sg/ece/highlights/events/