



海外学者学术报告



The transistor: exponential growth and securing our world for 75 years of existence

主讲人: Makoto Ikeda 日本东京大学 教授

报告时间: 2023年7月19日 (周三) 16:00-17:00

报告地点: 海山楼 A331

校内邀请人: 张建伟, 电信学部 人工智能学院

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. Also this talk will overview on 75-year of transistor invention.

Biography: Makoto Ikeda received the B.S., M.S., and Ph.D. degrees in electronic engineering from the University of Tokyo, Tokyo, Japan, in 1991, 1993, and 1996, respectively. He joined the Electronic Engineering Department, University of Tokyo, as a Faculty Member in 1996, and he is currently a full Professor with the Systems Design Lab, at the University of Tokyo. His research interests include the hardware security, including cryptographic engine design, asynchronous system design and smart image sensor designs. He served numerous positions in conferences including ISSCC 2021 ITPC Chair, Symposium on VLSI Circuits 2017 Program Chair and 2019 Symposium Chair, and A-SSCC 2025 Program Chair. Also he served IEEE SSCS Distinguished Lecturer in 2015 and 2016, and Commemorative Lecturers for Transistor 75th Anniversary, in 2023. He is a senior member of IEEE, IEICE Japan, and a member of IPSJ and ACM.