IEEE CAS Distinguished Lecture Series 2019

2:00 PM, January 24st, 靄雲廳, NCKU

Modular Arithmetic based Circuits and Systems for Emerging Technologies and Applications: Deep Neural Networks and Cryptography

Leonel Sousa, Ph. D.
IST/TU Lisbon (DEEC), Professor
INESC-ID (Associate Laboratory), Researcher
Instituto Superior Técnico (IST)

Abstract: Energy efficiency, limited power consumption and increased performance will drive the design of new architectures and arithmetic units. Unconventional number systems, namely Residue Number Systems (RNS), and modular arithmetic may hold the answer to these emerging challenges. In this talk we show how to use the RNS to improve cryptographic algorithms and engines, making them more efficient and more resistant to side-channel attacks, not only in the context of traditional cryptography but also of emerging post-quantum cryptography. Moreover, the potential of RNS to support the high-performance implementation of deep convolutional neural networks (DCNNs) is unveiled. Emerging technologies are also targeted in this talk, namely the implementation of RNS arithmetic units with reversible logic to improve density, speed and energy efficiency.

Biography: Leonel Sousa is currently Full Professor and Chair of the Electrical and Computer Engineering Department at the IST, Universidade de Lisboa and a Senior Researcher with the INESC-ID in Portugal. He has been vising professor in several universities abroad, he spent a few months in Japan with a prestigious JSPS Invitation Fellowship for Research and he has been at the Carnegie Mellon University. His research interests include high performance computing, computer architectures, computer arithmetic and multimedia systems. He has given more than 30 keynotes, invited talks and tutorials, he has authored or co-authored more than 250 papers appearing in international journals and conferences and edited five special issues of international journals. He served in the organization of several international conferences and he is currently an Associate Editor of the IEEE Transactions on Computers, IEEE Transactions on Multimedia and IEEE Transactions on Circuits and Systems for Video Technology. He is member of the IFIP WG10.3 on concurrent systems, Fellow of the IET and Distinguished Scientist of the ACM.