Preface

Douglas Stebila*

McMaster University,
1280 Main St W, Hamilton,
ON L8S 4L8, Canada
Email: stebilad@mcmaster.ca
*Corresponding author

Ernest Foo

Queensland University of Technology,
George St, Brisbane City, QLD 4000, Australia
Email: e.foo@qut.edu.au

Biographical notes: Douglas Stebila is an Assistant Professor in Cryptography at McMaster University in Hamilton, Ontario, Canada. His research focuses on improving the security of internet cryptography protocols such as SSL/TLS and SSH and developing practical quantum-resistant cryptosystems. He holds an MSc from the University of Oxford and a PhD from the University of Waterloo.

Ernest Foo's research interests can be broadly grouped into the field of secure cryptographic protocols with an active interest in network security applications. These include specific applications in the areas of wireless sensor networks security and security in industrial controls systems such as SCADA and the smart grid. His SCADA research has investigated vulnerabilities in Modbus and DNP3 protocols as well as the use of process mining, machine learning and data mining for attack detection in SCADA systems. He has published over 85 refereed papers including 19 journal papers.

This special issue of the *International Journal of Applied Cryptography* contains extended versions of six papers originally published in the 20th Australasian Conference on Information Security and Privacy (ACISP), held at the Queensland University of Technology in Brisbane, Australia, from June 29 to July 1, 2015.

ACISP is Australia and New Zealand's pre-eminent academic conference on information security, cryptography, and privacy, and for more than 20 years it has served to bring together Australasian security researchers and practitioners while serving the international academic community at a high standard.

ACISP 2015 received 112 submissions, of which 28 were accepted for publication in the conference based on the efforts of our 34 program committee members and with the assistance of 90 external reviewers. Based on scores provided by the program committee, we invited the authors of 12 papers to submit extended versions of their work to *IJACT*, and six accepted the invitation. These extended papers include additional constructions and analysis, and more detailed proofs than appeared in the conference proceedings; all received fresh reviews and some underwent multiple rounds of revisions.

We are pleased to present this special issue of *IJACT* highlighting papers from ACISP 2015, and showcasing the work of research teams from Australia, India, and Japan, in the areas of public key and symmetric authenticated encryption, identity-based encryption, cryptographic protocols, and cryptanalysis of symmetric encryption. We thank the editors-in-chief of *IJACT* for giving us the opportunity to present these works.