Invited Speakers

**Daniel Bernstein**  
(University of Illinois at Chicago)

**Ernie Brickell**  
(Intel)

**Steven Galbraith**  
(University of Auckland)

**Masahide Sasaki**  
(Quantum ICT Laboratory, NICT)

Winter School


Invited Lecturers

**Phong Nguyen**  
(Inria and CNRS/JFLI and the University of Tokyo)  
Lattice-Based Cryptography

**Tanja Lange**  
(Eindhoven University of Technology)  
Code-Based Cryptography

**Jintai Ding**  
(University of Cincinnati)  
MQ-Based Cryptography

**Andreas Hülsing**  
(Eindhoven University of Technology)  
Hash-Based Cryptography

**Michele Mosca**  
(University of Waterloo)  
Quantum Algorithms

**Ludovic Perret**  
(University Pierre and Marie Curie)  
Algebraic Attacks

Sponsors