Institute of mathematics & its applications

18TH IMA INTERNATIONAL CONFERENCE ON CRYPTOGRAPHY AND CODING

ONLINE EVENT

14 – 15 DECEMBER 2021

CONFERENCE PROGRAMME

Institute of mathematics & its applications

18th IMA International Conference on Cryptography and Coding

CONFERENCE PROGRAMME

Day One - Tuesday 14th December 2021

10.55	**Welcome, Introduction and Housekeeping**
11.00	**Invited Talk - Juliane Krämer - Security in the Quantum Age**
12.00	***Break***
12.30	*A note on quantum collision resistance of double-block-length compression functions, Shoichi Hirose*
12.55	*An extension of Kannan's embedding for solving ring-based LWE problems, Satoshi Nakamura*
13.20	**Short Break**
13.30	*An isogeny-based ID protocol using structured public keys, Daniele Cozzo*
13.55	*On the tightness of multi-user PKE notions, Hans Heum*
14.20	**Networking Session**
14.40	*Cryptanalysis of the Rank Preserving Signature, Maxime Bros*
15.05	*Black-box accumulation based on lattices, Sebastian H. Faller*
15.30	*Batch codes from affine cartesian codes and quotient spaces, Felice Manganiello*
15.55	**Short Break**

16.05	**Invited Talk – David Jao - The Problem Landscape of SIDH The Problem Landscape of SIDH**
17.05	**Networking Session**
17.30	**Conference Ends**

Day Two - Wednesday 15th December 2021

10.55	**Welcome, Introduction and Housekeeping**
11.00	**Invited Talk – Colin Boyd - Forward Secrecy without Diffie-Hellman**
12.00	**Break**
12.30	*Asymptotically tight lower bounds in anonymous broadcast encryption and authentication, Hirokazu Kobayashi*
12.55	*Attacks on a privacy-preserving publish-subscribe system and a ride-hailing service, Srinivas Vivek*
13.20	**Short Break**
13.30	*How to find ternary LWE keys using locality sensitive hashing, Elena Kirshanova*
13.55	*Structural properties of self-dual monomial codes with application to code-based cryptography, V.-F. Dragoi*
14.20	**Networking Session**
14.40	*Optimizing registration-based encryption, Kelong Cong*
15.05	*When HEAAN meets FV: a new somewhat homomorphic encryption with reduced memory overhead, Ilia Iliashenko*
15.30	*Secure multi-party computation in the bounded storage model, Jiahui Liu*
15.55	**Conference Ends**