Institute of mathematics & its applications

17th IMA International Conference on Cryptography and Coding

PROGRAMME: Monday 16 December

09:10 - 09:40	Registration
09:40 - 10:40	**Invited Talk: Cas Cremers: Security Standardisation and Secure Messaging** (Session Chair: Martin Albrecht)
10:40 - 11:10	Break
	FHE Security (Session Chair: Martin Albrecht)
11:10 - 11:35	Hyang-Sook Lee and Jeongeun Park. **On the Security of Multikey Homomorphic Encryption**
11:35 - 12:00	Shyam Murthy and Srinivas Vivek. **Cryptanalysis of a Protocol for Efficient Sorting on SHE Encrypted Data**
12:00 - 13:00	Lunch
	Coding (Attacks) (Session Chair: Martin Albrecht)
13:00 - 13:25	Terry Shue Chien Lau, Chik How Tan and Theo Fanuela Prabowo. **Key Recovery Attack on Rank Metric Code-based Signatures**
13:25 - 13:50	Claire Delaplace, Andre Esser and Alexander May. **Improved Low-Memory Subset Sum and LPN Algorithms via Multiple Collisions**
13:50 - 14:15	Rowena Alma Betty and Akihiro Munemasa. **Classification of self-dual codes of length 20 over $\mathbb{Z}_4$ and length at most 18 over $\mathbb{F}_2 + u\mathbb{F}_2$**
14:15 - 14:45	Break
	Adversarial Quantum Queries (Session Chair: Alex Davidson)
14:45 - 15:10	Shingo Sato and Junji Shikata. **Quantum-Secure (Non-)Sequential Aggregate Message Authentication Codes**
15:10 - 15:35	Shingo Sato and Junji Shikata. **SO-CCA secure PKE from KEM in the QROM and the QICM**
	(Presentations) Lattices (Session Chair: Ciara Rafferty)
15:35 - 16:00	James Howe, Marco Martinoli, Elisabeth Oswald and Francesco Regazzoni. **Optimised Lattice-Based Key Encapsulation in Hardware**
16:00 - 16:25	Anamaria Costache, Kim Laine and Rachel Player. **Homomorphic noise growth in practice: comparing BGV and FV**
17:00	Drinks Reception

Institute of mathematics & its applications

17th IMA International Conference on Cryptography and Coding

PROGRAMME: Tuesday 17 December

09:40 - 10:40	**Invited Talk: Nadia Heninger: The Cryptographic Legacy of Old RNG Designs** (Session Chair: Martin Albrecht)
10:40 - 11:10	Break
MPC (Session Chair: Alex Davidson)	
11:10 - 11:35	Ivan Damgård, Helene Haagh, Michael Nielsen and Claudio Orlandi. **Commodity-Based 2PC for Arithmetic Circuits**
11:35 - 12:00	Nigel Smart and Younes Talibi Alaoui. **Distributing any Elliptic Curve Based Protocol**
12:00 - 13:00	Lunch
Constructions (Session Chair: Liz Quaglia)	
13:00 - 13:25	Daniele Cozzo and Nigel Smart. **Sharing the LUOV: Threshold Post-Quantum Signatures**
13:25 - 13:50	Jan Camenisch, Maria Dubovitskaya and Patrick Towa. **Efficient Fully Secure Leakage-Deterring Encryption**
13:50 - 14:15	Behzad Abdolmaleki, Hamidreza Khoshakhlagh and Daniel Slamanig. **A Framework for UC-Secure Commitments from Publicly Computable Smooth Projective Hashing**
14:15 - 14:40	Pedro Branco, Jintai Ding, Manuel Goulão and Paulo Mateus. **A Framework for Universally Composable Oblivious Transfer from One-Round Key-Exchange**
14:40 - 15:10	Break
(Presentations) Attacks (Session Chair: Ciara Rafferty)	
15:10 - 15:35	Gabrielle De Micheli, Remi Piau and Cecile Pierrot. **A Tale of Three Signatures: practical attack of ECDSA with wNAF**
15:35 - 16:00	Jake Massimo. **Primality Testing in Cryptographic Applications**
16:00 - 16:25	Monika Trimoska, Sorina Ionica and Gilles Dequen. **A SAT-based approach for index calculus on binary elliptic curves**
16:30 - 17:30	**Invited Talk: Francesca Musiani: Nuancing the 'User' of Secure Messaging Tools** (Session Chair: Martin Albrecht)
19:00	Conference Dinner

Institute of mathematics & its applications

17th IMA International Conference on Cryptography and Coding

PROGRAMME: Wednesday 18 December

Attacks on AEAD Primitives (Session Chair: Martin Albrecht)	
09:40 – 10:05	Marcel Armour and Bertram Poettering. **Decryption Algorithm Substitution Attacks**
10:05 - 10:30	Maria Eichlseder, Daniel Kales and Markus Schofnegger. **Forgery Attacks on FlexAE and FlexAEAD**
10:30 – 11:10	Break
ZK (Session Chair: Alex Davidson)	
11:10 – 11:35	Ramiro Martínez and Paz Morillo. **RLWE-based Zero-Knowledge Proofs for linear and multiplicative relations**
11:35 – 12:00	Karim Baghery. **Subversion-Resistant Simulation (Knowledge) Sound NIZKs**
12:00 - 13:00	Lunch
Presentations (Session Chair: Ciara Rafferty)	
13:00 – 13:25	Woojoo Na, Alexander Allin and Christophe Petit. **Trapdoor attacks on Cayley hash function parameters proposed at the NutMiC 2019 conference**
13:25 – 13:50	Nina Bindel, Mike Hamburg, Andreas Hülsing and Edoardo Persichetti. **Tighter proofs of CCA security in the quantum random oracle model**
13:50 – 14:15	Lydia Garms and Anja Lehmann. **Group Signatures with Selective Linkability**
14:15 – 14:20	Closing Remarks