IMACC 2011 Programme

12th to 15th of December 2011
Lady Margaret Hall, University of Oxford, the UK

Monday December 12

18:30 – 19:30 Registration

19:30 – 20:30 Buffer dinner for residents only

Tuesday December 13

08:45 – 09:10 Registration

09:10 – 09:15 Opening remarks

09:15 – 10:15 Invited talk: David Naccache – chaired by Kyeongcheol Yang
Can a Program Reverse-Engineer Itself?

10:15 – 10:20 Short break

10:20 – 11:10 Homomorphic encryption – chaired by Michael Ward

Improved Key Generation For Gentry's Fully Homomorphic Encryption Scheme
Peter Scholl and Nigel Smart

On Constructing Homomorphic Encryption Schemes from Coding Theory
Frederik Armknecht, Daniel Augot, Ludovic Perret and Ahmad-Reza Sadeghi

11:10 – 11: 30 Coffee

11:30 – 12:45 Coding theory I – chaired by Felix Ulmer

Generalised complementary arrays
Matthew Parker and Constanza Riera

Binary Kloosterman Sums with Value 4
Jean-Pierre Flori, Sihem Mesnager and Gerard Cohen

On the Triple-Error-Correcting Cyclic Codes with Zero Set $\{1, 2^i+1, 2^j+1\}$
Vincent Herbert and Sumanta Sarkar

12:45 – 14:00 Lunch

14:00 – 15:00 Invited talk: Paddy Farrell – chaired by Matthew Parker
Non-Statistical Soft-in, Soft-out Decoding with the Euclidean Metric

15:00 – 15:05 Short break

15:05 – 15:55 Knowledge proof – chaired by Frederik Armknecht

A Secure and Efficient Proof of Integer in an Interval Range
Kun Peng

Bit Commitment in the Bounded Storage Model: Tight Bound and Simple Optimal Construction
Junji Shikata and Daisuke Yamanaka

15:55 – 16:15 Tea

16:15 – 17:30 Cryptographic functions – chaired by Steve Babbage

Self-Correctors for Cryptographic Modules
Go Yamamoto and Tetsutaro Kobayashi

The Symbiosis between Collision and Preimage Resistance
Martijn Stam and Elena Andreeva

Enhanced Count of Balanced Symmetric Functions and Balanced Alternating Functions
Marc Mouffron and Guillaume Vergne

18:00 – 19:30 Drinks reception

Wednesday December 14

09:00 – 10:00 Invited talk: Ivan Damgård – chaired by Kenny Paterson
Using unconditionally secure authentication in multiparty computation with dishonest majority

10:00 – 10:05 Short break

10:05 – 10:55 Public key cryptosystem – chaired by Kenny Paterson

Ciphertext-Policy Delegatable Hidden Vector Encryption and Its Application to Searchable Encryption in Multi-user Setting
Mitsuhiro Hattori, Takato Hirano, Takashi Ito, Nori Matsuda, Takumi Mori, Yusuke Sakai and Kazuo Ohta

Constructing Secure Hybrid Encryption from Key Encapsulation Mechanism with Authenticity
Yuki Shibuya and Junji Shikata

10:55 – 11:15 Coffee

11:15 – 12:30 Coding theory II – Chaired by Matthew Parker

A note on the dual codes of module skew codes
Delphine Boucher and Felix Ulmer

Ensuring message embedding in wet paper steganography
Daniel Augot, Morgan Barbier and Caroline Fontaine

On the Stability of m-Sequences
Alex Burrage, Ana Salagean and Raphael Phan

12:30 – 14:00 Lunch

14:00 – 15:40 Pairing and ECC implementation – chaired by Martijn Stam

Parallelizing the Weil and Tate Pairings
Diego Aranha, Edward Knapp, Alfred Menezes and Francisco Rodriguez-Henriquez.

On the Efficient Implementation of Pairing-Based Protocols
Michael Scott

Efficient Pairing Computation on Ordinary Elliptic Curves of Embedding Degree 1 and 2
Xusheng Zhang and Dongdai Lin

Improved Precomputation Scheme for Scalar Multiplication on Elliptic Curves
Duc-Phong Le and Chik-How Tan

15:40 – 16:00 Tea

16:00 – 17:15 Security analysis – chaired by Colin Boyd

Breaking an Identity-Based Encryption Scheme based on DHIES
Kenneth Paterson and Martin Albrecht

Analysis of the SSH Key Exchange Protocol
Stephen C. Williams

Cryptanalysis of the Light-Weight Cipher A2U2
Mohamed Ahmed Abdelraheem, Julia Borghoff, Erik Zenner and Mathieu David

19:00 Cryptomathic sponsored banquet

Thursday December 15

9:00 – 10:00 Invited talk: Jonathan Jedwab – chaired by Chris Mitchell
Emerging methods in the analysis of aperiodic autocorrelations

10:00 – 10:05 Short break

10:05 – 10:55 Symmetric key cryptosystem – chaired by Chris Mitchell

Building Blockcipher from Tweakable Blockcipher: Extending FSE 2009 Proposal
Kazuhiko Minematsu and Tetsu Iwata

Security of Hash-then-CBC Key Wrapping Revisited

Yasushi Osaki and Tetsu Iwata

10:55 – 11:15 Coffee

11:15 – 12:30 Cryptographic protocols – chaired by Michael Scott

Block-wise P-Signatures and Non-Interactive Anonymous Credentials with Efficient Attributes
Malika Izabachene, Benoit Libert and Damien Vergnaud

On Forward Secrecy in One-Round Key Exchange
Colin Boyd and Juan Gonzalez Nieto

Designated Confirmer Signatures with Unified Verification
Guilin Wang, Fubiao Xia and Yunlei Zhao

12:30 – 12:35 Closing remarks

12:40 – 14:00 Lunch