

IWCC 2009

The second International Workshop on Coding & Cryptology

1-5 June 2009

Katian International Hotel, WuLingYuan, ZhangJiaJie, China

Program

June 1, 2009 (Monday)	
08:20- 08:30 Opening	
Session Chair: San Ling	
08:30 - 09:15	Zeta Functions of the Pseudocodewords of LDPC Codes Winnie Li, Pennsylvania State University, USA
09:15 - 10:00	A Geometric Approach on Bilinear Pairings Tatsuaki Okamoto, NTT Labs, Japan
10:00- 10:30 Group Photo Taking and Coffee Break	
Session Chair: Winnie Li	
10:30 - 11:15	Hunting for Curves with Many Points G. van der Geer, University of Amsterdam, Netherland
11:15 - 12:00	Equal-Weight Fingerprinting Codes Ilya Dumer, University of California Riverside, USA
12:00- 14:00 Lunch Time	
Session Chair: Yeow Meng Chee	
14:00 - 14:45	On the Applicability of Combinatorial Designs to Key Predistribution for Wireless Sensor Networks Keith Martin, University of London, UK
14:45 - 15:30	Problems on Two-Dimensional Synchronization Patterns Tuvi Etzion, Technion--Israel Institute of Technology, Israel
15:30 - 16:00 Coffee Break	

Session Chair: Keqin Feng	
16:00 - 16:45	Recent Progress on MAC Xiaoyun Wang, Tsinghua University, China
16:45 - 17:30	Classical, Quantum and Post-quantum Cryptography Artur Ekert, National University of Singapore, Singapore
June 2, 2009 (Tuesday)	
Session Chair: Serge Vaudenay	
08:30 - 09:15	Binary Covering Arrays and Existentially Closed Graphs Charles Colbourn, Arizona State University, USA
09:15 - 10:00	Unconditionally Secure Approximate Message Authentication Reihaneh Safavi-Naini, University of Calgary, Canada
10:00 - 10:30 Coffee Break	
Session Chair: Reihaneh Safavi-Naini	
10:30 - 11:15	On the Impossibility of Strong Encryption over \aleph_0 Serge Vaudenay, Swiss Federal Institute of Technologies, Switzerland
11:15 - 12:00	Binary Additive Counter Stream Ciphers Cunsheng Ding, Hong Kong University of Science and Technology, China
12:00 - 14:00 Lunch Time	
14:00 - 17:30 Tour	
June 3, 2009 (Wednesday)	
08:30 - 17:30 Tour	
June 4, 2009 (Thursday)	
Session Chair: Dingyi Pei	
08:30 - 09:15	Characteristic Set Algorithms for Equation Solving in Finite Fields and Applications in Cryptanalysis of Stream Ciphers Xiao-Shan Gao, Academia Sinica, China
09:15 - 10:00	List Decoding of Binary Codes Venkatesan Guruswami, University of Washington, USA

10:00 - 10:30 Coffee Break	
Session Chair: Venkatesan Guruswami	
10:00 – 11:15	A Survey of Algebraic Unitary Codes Frederique Oggier, Nanyang Technological University, Singapore
11:15 – 12:00	On Cayley Graphs, Surface Codes, and the Limits of Homological Coding for Quantum Error Correction Gilles Zemor, Universite Bordeaux 1, France
12:00- 14:00 Lunch Time	
Session Chair: G. van der Geer	
14:00 – 14:45	New Family of Non-Cartesian Perfect Authentication Codes Dingyi Pei, Guangzhou University, China
14:45 – 15:30	An Infinite Class of Balanced Vectorial Boolean Functions with Optimum Algebraic Immunity and Good Nonlinearity Claude Carlet, University of Paris 8, France
15:30 - 16:00 Coffee Break	
Session Chair: Xiao-Shan Gao	
16:00 – 16:45	A New Client-to-Client Password-Authenticated Key Agreement Protocol Dengguo Feng, Institute of Software, Chinese Academy of Science, China
16:45 – 17:30	Ramsey Theory: a View from Logic Guohua Wu, Nanyang Technological University, Singapore
June 5, 2009 (Friday)	
Session Chair: Huaxiong Wang	
08:30 – 09:15	A Polynomial Based Hashing Algorithm Kumar Murty, University of Toronto, Canada
09:15 – 10:00	Separation and Witnesses Gerard Cohen, ENST-CNRS, France
10:00 - 10:10 Closing	