PROGRAM - WAIFI 2018 (14-16 June 2018, Bergen)

Thursday, 14th June

Invited Talk

09:30 - 10:30 **Benjamin Smith**: Pre- and post-quantum Diffie–Hellman protocols. Abstract

10:30 - 11:00 Coffee break

Elliptic Curves

11:00 - 11:30 Michael Scott and Aurore Guillevic: *A New Family of Pairing-Friendly elliptic curves*. Full Paper

11:30 - 12:00 Momonari Kudo and Shushi Harashita: *Superspecial Hyperelliptic Curves of Genus 4 over Small Finite Fields*. Full Paper

12:00 - 12:30 Anand Kumar Narayanan: *Fast Computation of Isomorphisms Between Finite Fields Using Elliptic Curves*. Full Paper

12:30 - 14:00 Lunch

Invited Talk

14:00 - 15:00 **Ferruh Özbudak:** Construction of Some Codes Suitable for Countermeasures to Both Side Channel Attacks and Fault Injection Attacks. Abstract

15:00 - 15:30 Coffee break

Hardware Implementations

15:30 - 16:00 Mustafa Khairallah, Anupam Chattopadhyay, Bimal Mandal and Subhamoy Maitra: *On Hardware Implementation of Tang-Maitra Boolean Functions*. Full Paper

16:00 - 16:30 Nusa Zidaric, Mark Aagaard and Guang Gong: *Rapid hardware design for cryptographic modules with filtering structure over small finite fields*. Full Paper

PROGRAM - WAIFI 2018 (14-16 June 2018, Bergen)

Friday, 15th June (Date for Banquet)

Invited Talk

09:30 - 10:30 **Daniel Katz**: Sequences with low correlation. Abstract

10:30 - 11:00 Coffee break

Arithmetic and Applications of Finite Fields (I)

11:00 - 11:30 Yoshinori Hamahata: *Vector-valued modular forms on finite upper half planes*. Full Paper

11:30 - 12:00 Lucia Moura, Daniel Panario and David Thomson: *Normal basis exhaustive search: 10 years later*. Full Paper

12:00 - 12:30 Domingo Gómez-Pérez and László Mérai: *Algebraic dependence in generating functions and expansion complexity*. Full Paper

12:30 - 14:00 Lunch

Invited Talk **Anwar Hasan**: Low-cost arithmetic in extended finite fields using structured matrices. Abstract

14:00 - 15:00

15:00 - 15:30 Coffee break

Boolean Functions

15:30 - 16:00 Thor Martinsen, Wilfried Medil, Alexander Pott and Pantelimon Stanica: *On symmetry and differential properties of generalized Boolean functions*. Full Paper

16:00 - 16:30 Sihem Mesnager, Ferruh Özbudak and Ahmet Sinak: *Characterizations of Partially bent and plateaued functions over finite fields*. Full Paper

Banquet

19:00 - 21:30 Fløien Folkerestaurant (Website, Map)

PROGRAM - WAIFI 2018 (14-16 June 2018, Bergen)

Saturday, 16th June

Invited Talk

09:30 - 10:30 **Daniel Panario:** The dynamics of iterating functions over finite fields. Abstract

10:30 - 11:00 Coffee break

Arithmetic and Applications of Finite Fields (II)

11:00 - 11:30 Torleiv Kløve: *Codes of length two correcting single errors of limited size II*. Full Paper

11:30 - 12:00 Federico Amadio Guidi and Giacomo Micheli: *Fractional jumps: complete characterisation and an explicit infinite family*. Full Paper

12:00 - 12:30 Motoko Qiu Kawakita: *Some sextics of genera five and seven attaining the Serre bound*. Full Paper

12:30 - 14:00 Lunch

Invited Talk

14:00 - 15:00 **Simon Blackburn:** Reducing the download complexity of Private Information Retrieval schemes. Abstract

15:00 - 15:30 Coffee break

Cryptography

15:30 - 16:00 Qiuping Li, Baofeng Wu and Zhuojun Liu: *Direct Constructions of (Involutory) MDS Matrices from Block Vandermonde and Cauchy-like Matrices*. Full Paper

16:00 - 16:30 Benjamin Pring: *Exploiting preprocessing for quantum search to break parameters for MQ cryptosystems*. Full Paper