RM2023 Program (Updated May 1,2023)

Opening: (13:20 – 13:25) T. Sasao

Session 1: (13:25 – 14:35) Chair: T. Sasao

A Side-Channel Attack on CRYSTALS-Kyber Using Single Ciphertext per Module Rank,

Ruize Wang and Elena Dubrova

Polynomial Formal Verification of Adder Circuits Using Answer Set Programming,

Mohamed Nadeem, Jan Kleinekathöfer and Rolf Drechsler

Polynomial Formal Verification of KFDD Circuits,

Martha Schnieber and Rolf Drechsler

Enumeration of Symmetric Boolean Functions by Sensitivity,

Jon Butler, Tsutomu Sasao and Shinobu Nagayama

Break: (14:35 – 14:45)

Session 2: (14:45 – 15:55) Chair: M. Miller

Area Minimization Using Decision Diagrams Without Constructing Them,

Kristina Cherevko and Alan Mishchenko

A Note on the Haar Spectra of Bent Functions,

Radomir Stankovic, Milena Stankovic, Claudio Moraga and Jaakko Astola

On a case of Family Resemblance of Reed-Muller and Reed-Muller-Fourier Transforms,

Claudio Moraga, Radomir Stankovic and Milena Stankovic

X (mod 2^k – 1) calculation based on Reed-Muller expansions of symmetric Boolean functions,

Danila Gorodecky

Break: (15:55 – 16:05)

Session 3: (16:05 – 16:40) Chair: Mitchell Thornton

Circuit Division based on the Orientation of CNOT Gates for NNA-Compliant Circuit Synthesis by Steiner-Gauss Elimination,

Huan Yu, Zhengton Han, Zanhe Qi and Shigeru Yamashita

A Study of Extending Transformation-based Synthesis to Incompletely-specified Functions,

D. Michael Miller and Mitchell A. Thornton

Closing: (16:40 – 16:45) T. Sasao and M. Miller