WAIFI 2010 Program

Sunday, June 27, 2010	
19:30-21:30	Reception Cocktail
Monday, June 28, 2010	
08:30-09:15	Registration
09:15-09:30	Welcome
09:30-10:30	Invited Talk by Henning Stichtenoth
10:30-11:00 Coffee Break	
Session M1: Efficient Finite Field Arithmetic	
11:00-11:30	Joppe Bos: High-Performance Modular Multiplication on the Cell Processor
11:30-12:00	Reza Azarderakhsh and Arash Reyhani-Masoleh: A Modified Low Complexity Digit-Level Gaussian Normal Basis Multiplier
12:00-12:30	Daniel Bernstein and Tanja Lange: Type-II Optimal Polynomial Bases
12:30-14:00 Lunch Break	
Session M2: Pseudorandom Numbers and Sequences	
14:00-14:30	Alina Ostafe: Triangular Polynomial Systems and Pseudorandom Sequences
14:30-15:00	Zhixiong Chen, Alina Ostafe and Arne Winterhof: Structure of Pseudorandom Numbers Derived from Fermat Quotients
15:00-15:30 Coffee Break	
Session M3: Boolean Functions	
15:30-16:00	Stéphanie Dib: Distribution of Boolean Functions According to Their Second-order Nonlinearity
16:00-16:30	Sihem Mesnager: Hyper-bent Boolean Functions with Multiple Trace Terms
18:00 Reception and Banquet	
Tuesday, June 29, 2010	
09:30-10:30	Invited Talk by Alfred Menezes
10:30-11:00 Coffee Break	
Session T1: Functions, Equations and Modular Multiplication	
11:00-11:30	Alexander Pott and Yue Zhou: Switching Construction of Planar Functions on Finite Fields
11:30-12:00	Thorsten Ernst Schilling and Håvard Raddum: Solving Equation Systems by Agreeing and Learning
12:00-12:30	Miroslav Knezevic, Frederik Vercauteren and Ingrid Verbauwhede: Speeding Up Bipartite Modular Multiplication
12:30-14:00 Lunch Break	

Session T2: Finite Field Arithmetic for Pairing Based Cryptography	
14:00-14:30	Naomi Benger and Michael Scott: Constructing Tower Extensions of Finite Fields for Implementation of Pairing-Based Cryptography
14:30-15:00	Craig Costello, Colin Boyd, Juan Manuel Gonzalez Nieto and Kenneth Koon-Ho Wong: Delaying Mismatched Field Multiplications in Pairing Computations
15:00-15:30 Coffee Break	
Abstracts and Short Presentations Session T3 (ASP)	
15:30-17:00 ASP Session program will be posted later [coffee & pastries during the session]	
Wednesday, June 30, 2010	
09:30-10:30	Invited Talk by P. Vijay Kumar
10:30-11:00 Coffee Break	
Session W1: Finite Fields, Cryptography and Coding	
11:00-11:30	Roger Oyono and Ritzenthaler Christophe: On Rationality of the Intersection Points of a Line with a Plane Quartic
11:30-12:00	Ulrich Tamm: Reflections about a Single Checksum
12:00-12:30	Mohamed Hassan and Mohammed Benaissa: Efficient Time-Area Scalable ECC Processor Using Micro-coding Technique
12:30-14:00 Lunch Break	