WAIFI 2012 Program
Bochum, Germany. July 16-19, 2012

Monday, July 16, 2012	
18:00	Reception Cocktail
Tuesday, July 17, 2012	
09:00-09:45	Registration
09:45-10:00	Welcome
Invited Talk 1	
10:00-11:00	Invited Talk by **Florian Hess** Generalised Jacobians in Cryptography and Coding Theory
11:00-11:30	Coffee Break
Session T1: Coding theory and code-based cryptography	
11:30-12:00	Gerardo Vega and Carlos A. Vázquez: The Weight Distribution of a Family of Reducible Cyclic Codes
12:00-12:30	Olav Geil, Stefano Martin and Ryutaroh Matsumoto: A new method for constructing small-bias spaces from Hermitian codes
12:30-13:00	Pierre-Louis Cayrel, Sidi Mohamed El Yousfi Alaoui, Gerhard Hoffmann and Pascal Véron: An improved threshold ring signature scheme based on error correcting codes
13:00-14:30	Lunch Break
Invited Talk 2	
14:30-15:30	Invited Talk by **Alexander Pott** Sequences and functions derived from projective planes and their difference sets
15:30-16:00	Coffee Break
Session T2: Boolean functions	
16:00-16:30	Lin Sok and Patrick Solé: On Formally Self-dual Boolean Functions in 2, 4 and 6 variables
16:30-17:00	Boris Batteux: On the Algebraic Normal Form and Walsh Spectrum of Symmetric Functions Over Finite Rings
17:00-17:30	Oleksandr Kazymyrov and Lilya Budaghyan: Verification of Restricted EA-equivalence for Vectorial Boolean Functions
19:00	Conference Dinner
Wednesday, July 18, 2012	
Invited Talk 3	
10:00-11:00	Invited Talk by **Shay Gueron** Software Implementation of Modular Exponentiation, Using Advanced Vector Instructions Architectures
11:00-11:30	Coffee Break

Session W1: Finite field arithmetic	
11:30-12:00	Nadia El Mrabet and Nicolas Gama: Efficient Multiplication over Extension Fields
12:00-12:30	Danuta Pamula and Arnaud Tisserand: Towards *GF(2^m)* Finite-Field Multipliers with Reduced Activity Variations
12:30-13:00	Razvan Barbulescu, Jérémie Detrey, Nicolas Estibals and Paul Zimmermann: Finding Optimal Formulae for Bilinear Maps
13:00-14:30	Lunch Break
Session W2: Equations and functions	
14:30-15:00	Benedikt Driessen and Christof Paar: Solving Binary Linear Equation Systems over the Rationals and Binaries
15:00-15:30	Sami Omar, Raouf Ouni and Saber Bouanani: Hashing with Elliptic Curve *L*-functions
15:30-16:00	Coffee Break
Abstracts and Short Presentations Session W3 (ASP)	
16:00-17:30	ASP Session program will be posted later (coffee & pastries during the session)
Thursday, July 19, 2012	
Invited Talk 4	
10:00-11:00	Invited Talk by **Emmanuel Thomé** Square Root Algorithms for the Number Field Sieve
11:00-11:30	Coffee Break
Session TH1: Polynomial factorization and permutation polynomials	
11:30-12:00	Ryuichi Harasawa, Yutaka Sueyoshi and Aichi Kudo: Improving the Berlekamp algorithm for binomials $x^n - a$
12:00-12:30	Sumanta Sarkar, Srimanta Bhattacharya and Ayca Cecsmelioglu: On Some Permutation Binomials of the Form $x^{(2^n-1/k)+1} + ax$ over F_{2^n} : Existence and Count
12:30-13:00	Lunch Break