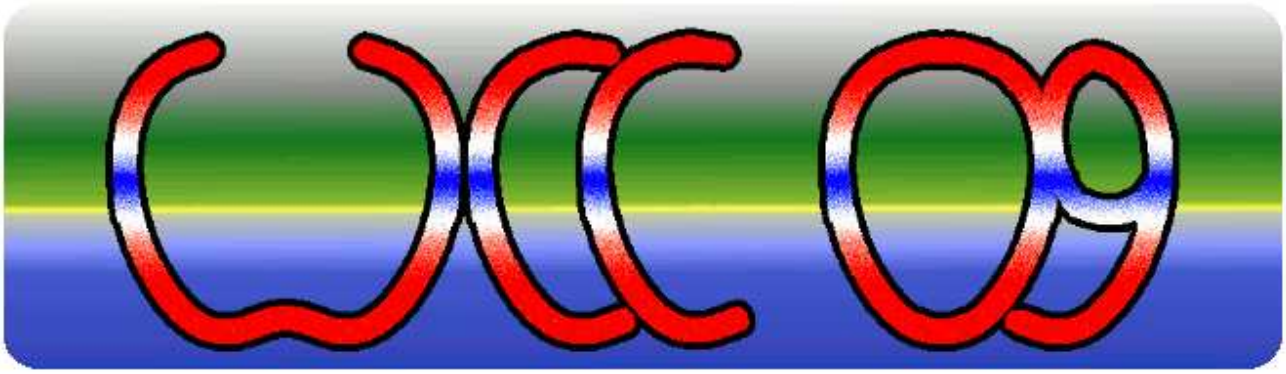

Technical Program

International Workshop on Coding and Cryptography

May 10-15, 2009, Ullensvang (Norway)

Monday 8:45-8:50 Welcome

Monday 8:50-9:50 Invited Talk 1

C. Carlet, "Relating three nonlinearity characteristics of vectorial functions, constructing bent functions and using them to build APN functions".

Monday 10:00-12:50 Bent Functions (Coffee break: 11:00–11:20)

S. Mesnager, "A new class of bent Boolean functions in polynomial forms".

L. Budaghyan and C. Carlet, "On CCZ-equivalence and its use in secondary constructions of bent functions".

P. Beelen and G. Leander, "Bounds and constructions of highly nonlinear S-boxes".

A. Pott, Y. Tan, T. Feng, and S. Ling, "Association schemes arising from bent functions".

P. Langevin and G. Leander, "Counting all bent functions in dimension 8".

Monday 12:50-14:00 Lunch

Monday 14:00-17:20 Coding Theory 1 (Coffee break: 15:30–15:50)

R. Jurrius and R. Pellikaan, "Extended and generalized weight enumerators".

I. Siap, "m-spotty weight enumerators of linear codes over $F_2 + uF_2$".

F. Caruso and M. Giorgetti, "A combinatorial approach for the computation of the distance of binary nth-root codes".

D. Danev, S. Dodunekov, and D. Radkova, "A family of constacyclic ternary quasi-perfect codes with covering radius 3".

T. Kløve, “Lower bounds on the size of spheres of permutations under the infinity norm”.

L. E. Danielsen and M. G. Parker, “Directed graph representation of half-rate additive codes over GF(4)”.

Tuesday 9:00-10:00 Invited Talk 2

B. Schneier, “The design of the Skein hash function”.

Tuesday 10:00-12:50 Public-Key Cryptography (Coffee break: 11:00–11:20)

M. Joye, “How (not) to design strong-RSA signatures”.

S. Maitra and S. Sarkar, “Deterministic polynomial-time equivalence of computing the CRT-RSA secret keys and factoring”.

D. J. Bernstein, T. Lange, C. Peters, and H. van Tilborg, “Explicit bounds for generic decoding algorithms for code-based cryptography”.

M. P. Jhanwar and R. Barua, “A semantically secure public-key encryption in the standard model”.

I. Semaev, “Sparse Boolean equations and circuit lattices”.

Tuesday 12:50-14:00 Lunch

Tuesday 14:00-17:50 Cryptography (Coffee break: 15:30–15:50)

S. Nikova and V. Nikov, “Efficient perfectly secure verifiable secret sharing and distributed commitment schemes”.

S. Manuel, “Classification and generation of disturbance vectors for collision attacks against SHA-1”.

S. Eskeland and V. Oleshchuk, “Collusion-resistant threshold cryptosystems”.

D. G. Harris, “Generic ciphers are more vulnerable to related-key attacks than previously thought”.

E. K. Özbudak, F. Özbudak, and Z. Saygi, “A class of authentication codes with secrecy”.

J. C. Hernandez-Castro, J. M. Estevez-Tapiador, P. Peris-Lopez, T. Li, and J.-J. Quisquater, “Cryptanalysis of the SASI ultralightweight RFID authentication protocol with modular rotations”.

Y. E. Salehani, S. A. H. A. E. Tabatabaei, M. R. S. Abyaneh, and M. M. Hassanzadeh, “NESHA-256, NEw 256-bit secure hash algorithm”.

Wednesday 9:00-10:00 Invited Talk 3

B. Preneel, "On SHA-x, with x a small integer".

Wednesday 10:00-12:20 Coding Theory 2 (Coffee break: 11:00–11:20)

V. Junnila and T. Laihonen, "Codes for identification in $\mathbf{Z}^2$ with Euclidean balls".

C. Chabot, "Reconstruction of families of codes, application to cyclic codes".

D. Alquié and F. Landelle, "Branch number of linear automaton and recursive systematic convolutional codes".

M. O. Damen, H. El Gamal, and A. A. Badr, "A new class of TAST codes with a simplified tree structure".

Wednesday 12:30-14:00 Lunch

Wednesday 15:00-18:00 Parallel session: Excursion

Alternative 1, "Guided tour in Lofthus...apple cake included".

Alternative 2, "Guided tour in the hills...no apple cake included". Session chair: Matthew.

Thursday 9:00-10:00 Invited Talk 4

J. Jedwab, "New constructions of Golay complementary sequences".

Thursday 10:00-12:20 Sequences (Coffee break: 11:00–11:20)

K.-U. Schmidt, "On the correlation distribution of Delsarte-Goethals sequences".

P. Lisoněk and M. Moisio, "On Kloosterman zeros in subfields".

N. Brandstätter, G. Pirsic, and A. Winterhof, "Two-prime Sidelnikov sequences".

G. Leander and F. Rodier, "Bounds on the degree of APN polynomials. The case of $x^{-1}+g(x)$".

Thursday 12:30-14:00 Lunch

Thursday 14:00-17:20 Block Ciphers (Coffee break: 15:30–15:50)

A. Bogdanov, "On the differential trails of unbalanced Feistel networks with contracting MDS diffusion".

M. Gomathisankaran and R. B. Lee, "Maya: A novel block encryption function".

C. Blondeau and B. Gérard, "On the data complexity of statistical attacks against block ciphers".

N. Courtois, "Self-similarity attacks on block ciphers and application to KeeLoq".

R. Fourquet, P. Loidreau, and C. Tavernier, "Finding good linear approximations of block ciphers and its application to cryptanalysis of reduced round DES".

A. Levina, "Algorithm based on wavelet decomposition of splines".

Friday 9:00-10:00 Invited Talk 5

P. R. J. Östergård, "The perfect binary one-error-correcting codes of length 15".

Friday 10:00-11:00 Stream Ciphers

S. Maitra, G. Paul, and S. Raizada, "Some observations on HC-128".

T. E. Bjørstad, "Cryptanalysis of Grain using time / memory / data tradeoffs".

Boat leaves 11:30, lunch is served on board