FSE 2006 Program

Wednesday, March 15th

08:00 - 08:50	*Registration*
08:50 - 09:00	***Welcome notes by Vincent Rijmen***
Session 1	**Stream Ciphers (I) (S. Lucks)**
09:00 - 09:25	"Cryptanalysis of Achterbahn" by T.Johansson, W.Meier, and F.Muller
09:25 - 09:50	"Cryptanalysis of Grain" by C.Berbain, H.Gilbert, and A.Maximov
09:50 - 10:15	"Cryptanalysis of Stream Cipher DECIM" by H.Wu and B.Preneel
	Break
Session 2	**Block Ciphers (C. Cid)**
10:45 - 11:10	"On Feistel Structure Using a Diffusion Switching Mechanism" by T.Shirai and K.Shibutani
11:10 - 11:35	"Pseudo-Random Permutation Families Over Abelian Groups" by L.Granboulan, É.Levieil, and G.Piret
11:35 - 12:00	"A Zero-Dimensional Groebner Basis for AES-128" by J.Buchmann, A.Pychkine, and R.Weinmann
	Lunch at "Schlossberg-Restaurant"
Session 3	**Hash Functions (I) (H. Raddum)**
14:00 - 14:25	"Cryptanalysis of the Full HAVAL with 4 and 5 Passes" by H.Yu, X.Wang, A.Yun, and S.Park
14:25 - 14:50	"Collisions and Near-Collisions for Reduced-Round TIGER" by J.Kelsey and S.Lucks
14:50 - 15:15	"Analysis of Step-Reduced SHA-256" by F.Mendel, N.Pramstaller, C.Rechberger, and V.Rijmen
	Break
Session 4	**Analysis (M. Matsui)**
15:45 - 16:10	"Improved Linear Distinguishers for SNOW 2.0" by K.Nyberg and J.Wallén
16:10 - 16:35	"Reducing the Space Complexity of BDD-Based Attacks" by M.Krause and D.Stegemann
16:35 - 17:00	"Breaking the ICE: Finding Multicollisions in Iterated Concatenated and Expanded (ICE) Hash Functions" by J.Hoch and A.Shamir
19:00 -	*Welcome Reception at "Burg"*

Thursday, March 16th

Session 5	**Proposals (K. Nyberg)**
09:00 - 09:25	"A New Dedicated 256-bit Hash Function: FORK-256" by D.Hong, J.Sung, S.Lee, D.Moon, S.Chee
09:25 - 09:50	"Some Plausible Constructions of Double-Block-Length Hash Functions" by S.Hirose
09:50 - 10:15	"Provably Secure MACs from Differentially-Uniform Permutations and AES-Based Implementations" by K.Minematsu and Y.Tsunoo
	Break
Session 6	**Hash Functions (II) (W. Meier)**
10:45 - 11:10	"Searching for Differential Paths in MD4" by M.Schläffer and E.Oswald
11:10 - 11:35	"A Study of the MD5 Attacks" by J.Black, M.Cochran, and T.Highland
11:35 - 12:00	"The Impact of Carries on the Complexity of Collision Attacks" by F.Mendel, N.Pramstaller, C.Rechberger, and V.Rijmen
	Lunch at "Schlossberg-Restaurant"
Session 7	**Invited Speaker and Rump Session**
14:00 - 14:45	"How to Make a Difference: the History of Differential Cryptanalysis" by **Eli Biham**
15:00 - 16:00	Rump Session
	City Tour Graz
departure 17:15	*Conference Dinner at Schloss Obermayerhofen*

Friday, March 17th

Session 8	**Modes and Models (K. Aoki)**
09:00 - 09:25	"A New Mode of Encryption Secure Against Symmetric Nonce Respecting Adversaries" by D.Chakraborty and P.Sarkar
09:25 - 09:50	"New Blockcipher Modes of Operation with Beyond the Birthday Bound Security" by T.Iwata
09:50 - 10:15	"The Ideal-Cipher Model, Revisited: An Uninstantiable Blockcipher-Based Hash Function" by J.Black
	Break
Session 9	**Implementation and Bounds (E. Oswald)**
10:45 - 11:10	"How Far Can We Go on the x64 Processors?" by M.Matsui
11:10 - 11:35	"Computing the Algebraic Immunity Efficiently" by F.Didier and J.Tillich
11:35 - 12:00	"Upper Bounds on Algebraic Immunity of Power Functions" by Y.Nawaz, G.Gong, and K.Gupta
	Lunch at "Schlossberg-Restaurant"
Session 10	**Stream Ciphers (II) (A. Canteaut)**
14:00 - 14:25	"Chosen Ciphertext Attacks Against MOSQUITO" by A.Joux and F.Muller
14:25 - 14:50	"Distinguishing Attack on the Stream Cipher Ry" by G.Sekar, S.Paul, and B.Preneel
14:50 - 15:15	"Resynchronization Attack on WG and LEX" by H.Wu and B.Preneel
	Workshop Closing by Matt Robshaw