FSE 2010 List of Accepted Papers*

103. Cryptanalysis of ESSENCE
Maria Naya-Plasencia, Andrea Röck, Jean-Philippe Aumasson, Yann Laigle-Chapuy, Gaëtan Leurent, Willi Meier, Thomas Peyrin

104. Constructing Rate-1 MACs from Unpredictable Block Ciphers: PGV Model Revisited
Liting Zhang, Wenling Wu, Peng Wang, Lei Zhang, Shuang Wu, Bo Liang

106. How to Thwart Birthday Attacks against MACs via Small Randomness
Kazuhiko Minematsu

110. Super-Sbox Cryptanalysis: Improved Attacks for AES-like Permutations
Henri Gilbert, Thomas Peyrin

113. Differential and Invertibility Properties of BLAKE (Short Presentation)
Jean-Philippe Aumasson, Jian Guo, Simon Knellwolf, Krystian Matusiewicz, Willi Meier

119. Rebound Attack on Reduced-Round Versions of the JH
Vincent Rijmen, Deniz Toz, Kerem Varici

122. Domain Extension for Enhanced Target Collision-Resistant Hash Functions
Ilya Mironov

123. Higher Order Differential Attack on Step-Reduced Variants of Luffa v1
Dai Watanabe, Yasuo Hatano, Tsuyoshi Yamada, Toshinobu Kaneko

124. A Unified Method for Improving PRF Bounds for a Class of Blockcipher based MACs
Mridul Nandi

129. Enhanced Security Notions for Dedicated-Key Hash Functions: Definitions and Relationships
Mohammad Reza Reyhanitabar, Willy Susilo, Yi Mu

133. Pseudo-cryptanalysis of the Original Blue Midnight Wish (Short Presentation)
Søren Steffen Thomsen

138. Rotational Cryptanalysis of ARX
Dmitry Khovratovich, Ivica Nikolic

139. Improving the Generalized Feistel
Tomoyasu Suzaki, Kazuhiko Minematsu

146. Security Analysis of the Mode of JH Hash Function
Rishiraj Bhattacharyya, Avradip Mandal, Mridul Nandi

151. Fast Software AES Encryption
Dag Arne Osvik, Joppe W. Bos, Deian Stefan, David Canright

152. Lightweight Privacy Preserving Authentication for RFID Based on a Stream Cipher
Olivier Billet, Jonathan Etrog, Henri Gilbert

153. Finding Preimages of Tiger Up to 23 Steps
Lei Wang, Yu Sasaki

155. Nonlinear Equivalence of Stream Ciphers
Sondre Rønjom, Carlos Cid

*The final version that will appear at the workshop and (pre-)proceedings is subject to change.

156. Attacking the Knudsen-Preneel Compression Function
Onur Özen, Thomas Shrimpton, Martijn Stam

163. Another Look at Complementation Properties
Charles Bouillaguet, Orr Dunkelman, Gaëtan Leurent, Pierre-Alain Fouque

166. Cryptanalysis of the DECT Standard Cipher
Karsten Nohl, Erik Tews, Ralf-Philipp Weinmann