Contents

Malicious Hashing: Eve’s Variant of SHA-1 ................................. 1
    Ange Albertini, Jean-Philippe Aumasson, Maria Eichlseder,
    Florian Mendel, and Martin Schläffer

Binary Elligator Squared .................................................. 20
    Diego F. Aranha, Pierre-Alain Fouque, Chen Qian, Mehdi Tibouchi,
    and Jean-Christophe Zapalowicz

Batch NFS ................................................................. 38
    Daniel J. Bernstein and Tanja Lange

An Improvement of Linear Cryptanalysis with Addition Operations
with Applications to FEAL-8X .............................................. 59
    Eli Biham and Yaniv Carmeli

Colliding Keys for SC2000-256 ........................................... 77
    Alex Biryukov and Ivica Nikolić

Faster Binary-Field Multiplication and Faster Binary-Field MACs .......... 92
    Daniel J. Bernstein and Tung Chou

OMD: A Compression Function Mode of Operation
for Authenticated Encryption ................................................ 112
    Simon Cogliani, Diana-Ştefania Maimuț, David Naccache,
    Rodrigo Portella do Canto, Reza Reyhanitabar,
    Serge Vaudenay, and Damian Vizár

Security Amplification for the Composition of Block Ciphers:
Simpler Proofs and New Results ........................................... 129
    Benoit Cogliati, Jacques Patarin, and Yannick Seurin

Improved Differential Cryptanalysis of Round-Reduced Speck ............ 147
    Itai Dinur

Differential Cryptanalysis of SipHash ..................................... 165
    Christoph Dobraunig, Florian Mendel, and Martin Schläffer

Weak Instances of PLWE .................................................. 183
    Kirsten Eisenträger, Sean Hallgren, and Kristin Lauter

The Usage of Counter Revisited: Second-Preimage Attack
on New Russian Standardized Hash Function ................................ 195
    Jian Guo, Jérémy Jean, Gaëtan Leurent, Thomas Peyrin, and Lei Wang
Selected Areas in Cryptography -- SAC 2014
21st International Conference, Montreal, QC, Canada, August 14-15, 2014, Revised Selected Papers
Joux, A.; Youssef, A. (Eds.)
2014, X, 381 p. 66 illus., Softcover
ISBN: 978-3-319-13050-7