Jacobson, Michael J. jun. (ed.); **Rijmen, Vincent (ed.)**; **Safavi-Naini, Reihaneh (ed.)**
Selected areas in cryptography. 16th annual international workshop, SAC 2009, Calgary, Alberta, Canada, August 13–14, 2009. Revised selected papers. (English) Zbl 1177.94012
Lecture Notes in Computer Science 5867. Berlin: Springer (ISBN 978-3-642-05443-3/pbk). xiii, 467 p. (2009).

The articles of this volume will be reviewed individually. The preceding workshop has been reviewed (see Zbl 1173.94003).

Indexed articles:

Indesteege, Sebastiaan; Mendel, Florian; Preneel, Bart; Schläffer, Martin, Practical collisions for SHAMATA-256, 1-15 [Zbl 1267.94066]

Mendel, Florian; Peyrin, Thomas; Rechberger, Christian; Schläffer, Martin, Improved cryptanalysis of the reduced Grøstl compression function, ECHO permutation and AES block cipher, 16-35 [Zbl 1267.94084]

Sasaki, Yu, Cryptanalyses of narrow-pipe mode of operation in AURORA-512 hash function, 36-52 [Zbl 1267.94093]

Gennaro, Rosario; Halevi, Shai, More on key wrapping, 53-70 [Zbl 1267.94061]

Patra, Arpita; Choudhary, Ashish; Rangan, C. Pandu, Information theoretically secure multi party set intersection re-visited, 71-91 [Zbl 1267.94090]

Chow, Sherman S. M., Real traceable signatures, 92-107 [Zbl 1267.94115]

Khovratovich, Dmitry, Cryptanalysis of hash functions with structures, 108-125 [Zbl 1267.94074]

Wu, Shuang; Feng, Dengguo; Wu, Wenling, Cryptanalysis of the LANE hash function, 126-140 [Zbl 1267.94103]

Guo, Jian; Matusiewicz, Krystian; Knudsen, Lars R.; Ling, San; Wang, Huaxiong, Practical pseudo-collisions for hash functions ARIRANG-224/384, 141-156 [Zbl 1267.94063]

Canright, David; Osvik, Dag Arne, A more compact AES, 157-169 [Zbl 1267.94047]

Loebenberger, Daniel; Putzka, Jens, Optimization strategies for hardware-based cofactorization, 170-181 [Zbl 1267.11121]

Krause, Matthias; Stegemann, Dirk, More on the security of linear RFID authentication protocols, 182-196 [Zbl 1267.94077]

Kircanski, Aleksandar; Youssef, Amr M., Differential fault analysis of Rabbit, 197-214 [Zbl 1267.94076]

Tsow, Alex, An improved recovery algorithm for decayed AES key schedule images, 215-230 [Zbl 1267.94100]

Wang, Meiqin; Nakahara, Jorge jun.; Sun, Yue, Cryptanalysis of the full MMB block cipher, 231-248 [Zbl 1267.94101]

Ohkuma, Kenji, Weak keys of reduced-round PRESENT for linear cryptanalysis, 249-265 [Zbl 1267.94088]

Sun, Xiaorui; Lai, Xuejia, Improved integral attacks on MISTY1, 266-280 [Zbl 1267.94097]

Mala, Hamid; Shakiba, Mohsen; Dakhilalian, Mohammad; Bagherikaram, Ghadamali, New results on impossible differential cryptanalysis of reduced-round Camellia-128, 281-294 [Zbl 1267.94082]

Bellare, Mihir; Ristenpart, Thomas; Rogaway, Phillip; Stegers, Till, Format-preserving encryption, 295-312 [Zbl 1267.94037]

Iwata, Tetsu; Yasuda, Kan, BTM: a single-key, inverse-cipher-free mode for deterministic authenticated encryption, 313-330 [Zbl 1267.94067]

Järvinen, Kimmo U., On repeated squarings in binary fields, 331-349 [Zbl 1267.94069]

Joye, Marc, Highly regular m-ary powering ladders, 350-363 [Zbl 1267.94071]

Sasaki, Yuta; Nishina, Satsuki; Shirase, Masaaki; Takagi, Tsuyoshi, An efficient residue group multiplication for the η_T pairing over $\mathbb{F}_{3^m}$, 364-375 [Zbl 1267.94094]

Misoczki, Rafael; Barreto, Paulo S. L. M., Compact McEliece keys from Goppa codes, 376-392 [Zbl 1267.94086]

Andreeva, Elena; Bouillaguet, Charles; Dunkelman, Orr; Kelsey, John, Herding, second preimage and Trojan message attacks beyond Merkle-Damgård, 393-414 [Zbl 1267.94029]

Aumasson, Jean-Philippe; Dunkelman, Orr; Indesteege, Sebastiaan; Preneel, Bart, Cryptanalysis of dynamic SHA(2), 415-432 [Zbl 1267.94035]

Arnault, François; Berger, Thierry; Lauradoux, Cédric; Minier, Marine; Pousse, Benjamin, A new approach for FCSRs, 433-448 [Zbl 1267.94032]

Zhang, Bin, New cryptanalysis of irregularly decimated stream ciphers, 449-465 [Zbl 1267.94106]

MSC:

94-06 Proceedings, conferences, collections, etc. pertaining to information and communication theory
94A60 Cryptography
00B25 Proceedings of conferences of miscellaneous specific interest

Full Text: DOI