ASIACRYPT 2009 Accepted Papers

(updated 09/09/09)

110. Improved Cryptanalysis of Skein
Jean-Philippe Aumasson, Çağdaş Çalık, Willi Meier, Onur Özen, Raphael C.-W. Phan and Kerem Varıcı

116. Secure Two-Party Computation is Practical
Benny Pinkas, Thomas Schneider, Nigel P. Smart and Stephen C. Williams

128. Security Notions and Generic Constructions for Client Puzzles
Liqun Chen, Paul Morrissey, Nigel P. Smart and Bogdan Warinschi

130. On the Analysis of Cryptographic Assumptions in the Generic Ring Model
Tibor Jager and Jörg Schwenk

134. Fiat-Shamir With Aborts: Applications to Lattice and Factoring-Based Signatures
Vadim Lyubashevsky

145. Rebound Distinguishers: Results on the Full Whirlpool Compression Function
Mario Lamberger, Florian Mendel, Christian Rechberger, Vincent Rijmen and Martin Schläffer

152. PSS is Secure against Random Fault Attacks
Jean-Sébastien Coron and Avradip Mandal

157. Zero Knowledge in the Random Oracle Model, Revisited
Hoeteck Wee

168. Linearization Framework for Collision Attacks: Application to CubeHash and MD6
Eric Brier, Shahram Khazaei, Willi Meier and Thomas Peyrin

173. Improved generic algorithms for 3-collisions
Antoine Joux and Stefan Lucks

189. Non-Malleable Statistically Hiding Commitment from Any One-Way Function
Zongyang Zhang, Zhenfu Cao, Ning Ding and Rong Ma

202+302. Preimages for Step-Reduced SHA-2
Kazumaro Aoki, Jian Guo, Krystian Matusiewicz, Yu Sasaki and Lei Wang

207. Cache-Timing Template Attacks
Billy Brumley and Risto Hakala

221. Related-key Cryptanalysis of the Full AES-192 and AES-256

Alex Biryukov and Dmitry Khovratovich

225. A Modular Design for Hash Functions: Towards Making the Mix-Compress-Mix Approach Practical
Anja Lehmann and Stefano Tessaro

228. Security Bounds for the Design of Code-based Cryptosystems
Matthieu Finiasz and Nicolas Sendrier

231. On Black-Box Constructions of Predicate Encryption from Trapdoor Permutations
Jonathan Katz and Arkady Yerukhimovich

235. Memory Leakage-Resilient Encryption based on Physically Unclonable Functions
Frederik Armknecht, Roel Maes, Ahmad-Reza Sadeghi, Berk Sunar and Pim Tuyls

246. Quantum-Secure Coin-Flipping and Applications
Ivan Damgård and Carolin Lunemann

250. Signature Schemes with Bounded Leakage Resilience
Jonathan Katz and Vinod Vaikuntanathan

255. Simple Adaptive Oblivious Transfer Without Random Oracle
Kaoru Kurosawa and Ryo Nojima

256. Improved Non-Committing Encryption with Applications to Adaptively Secure Protocols
Seung Geol Choi, Dana Dachman-Soled, Tal Malkin and Hoeteck Wee

262. Secure Multi-party Computation Minimizing Online Rounds
Seung Geol Choi, Ariel Elbaz, Tal Malkin and Moti Yung

268. Group Encryption: Non-Interactive Realization in the Standard Model
Julien Cathalo, Benoît Libert and Moti Yung

272. Foundations of Non-Malleable Hash and One-Way Functions
Alexandra Boldyreva, David Cash, Marc Fischlin and Bogdan Warinschi

274. Proofs of Storage from Homomorphic Identification Protocols
Giuseppe Ateniese, Seny Kamara and Jonathan Katz

276. Hierarchical Predicate Encryption for Inner-Products
Tatsuaki Okamoto and Katsuyuki Takashima

289. A Framework for Universally Composable Non-Committing Blind Signatures
Masayuki Abe and Miyako Ohkubo

296. How to Confirm Cryptosystems Security: The Original Merkle-Damgård is Still Alive!
Yusuke Naito, Kazuki Yoneyama, Lei Wang and Kazuo Ohta

303. Efficient Public Key Encryption Based on Ideal Lattices
Damien Stehlé, Ron Steinfeld, Keisuke Tanaka and Keita Xagawa

322. Cryptanalysis of the Square Cryptosystems
Olivier Billet and Gilles Macario-Rat

325. Cascade Encryption Revisited
Peter Gaži and Ueli Maurer

326. Factoring pq^2 with Quadratic Forms: Nice Cryptanalyses
Guilhem Castagnos, Antoine Joux, Fabien Laguillaumie and Phong Q. Nguyen

331. The Key-Dependent Attack on Block Ciphers
Xiaorui Sun and Xuejia Lai

332. On the Power of Two-Party Quantum Cryptography
Louis Salvail, Christian Schaffner and Miroslava Sotakova

343. The Intel AES Instructions Set and the SHA-3 Candidates
Ryad Benadjila, Olivier Billet, Shay Gueron and Matt Robshaw

358. MD5 is Weaker than Weak: Attacks on Concatenated Combiners
Florian Mendel, Christian Rechberger and Martin Schläffer

368. Rebound Attack on the Full LANE Compression Function
Krystian Matusiewicz, María Naya-Plasencia, Ivica Nikolić, Yu Sasaki and Martin Schläffer

370. Hedged Public-Key Encryption: How to Protect Against Bad Randomness
Mihir Bellare, Zvika Brakerski, Moni Naor, Thomas Ristenpart, Gil Segev, Hovav Shacham and Scott Yilek

385. Smooth Projective Hashing and Password-Based Authenticated Key Exchange Based on Lattices
Jonathan Katz and Vinod Vaikuntanathan

404. Attacking Power Generators Using Unravelled Linearization: When Do We Output Too Much?
Mathias Herrmann and Alexander May