Security Analysis Submissions

ARXtools: A Toolkit for ARX Analysis
Gaëtan Leurent

Provable Security of BLAKE with Non-Ideal Compression Function
Bart Mennink, Elena Andreeva, Atul Luykx

Pseudorandomness of Keyed Sponge Construction under a Practical Assumption
Donghoon Chang, Morris Dworkin, Seokhie Hong, John Kelsey, Mridul Nandi

On the Algebraic Degree of some SHA-3 Candidates
Christina Boura, Anne Canteaut

A Study of Practical-time Distinguishing Attacks against Round-reduced Threefish-256
Aron Gohr

Batteries Included- Features and Modes for Next Generation Hash Functions
Stefan Lucks, David McGrew, Doug Whiting

Side Channel Analysis of the SHA-3 Finalists
Michael Zohner, Michael Kasper, Marc Stottinger

Security Reductions of the SHA-3 Finalists: New Results and a Status Update
Bart Mennink Elena Andreeva, Bart Preneel, Marjan Skrobot

Improved Indifferentiability Security Bound for the JH Mode
Souradyuti Paul, Dustin Moody, Daniel Smith-Tone

Implementation/Performance-Oriented Submissions

Performance of the SHA-3 Candidates in Java
Christian Hanser

BLAKE and 256-bit Advanced Vector Extensions
Jean –Philippe Aumasson, Samuel Neves,

Lessons Learned from Designing a 65nm ASIC for Evaluating Third Round SHA-3 Candidates
Frank Gurkaynak, Kris Gaj, Beat Muheim, Ekawat Homsirikamol, Christoph Keller, Marcin Rogawski, Hubert Kaeslin, Jens-Peter Kaps

1001 Ways to Implement Keccak
Guido Bertoni, Joan Daemen, Michaël Peeters, Gilles Van Assche, Ronny Van Keer

SHA-3 on ARM11 Processors
Peter Schwabe, Bo-Yin Yang, Shang-Yi Yang

Comprehensive Evaluation of High-Speed and Medium-Speed Implementations of Five SHA-3 Finalists Using Xilinx and Altera FPGAs
Kris Gaj, Ekawat Homsirikamol, Marcin Rogawski, Rabia Shahid, Malik Umar Sharif

The New SHA-3 Software Shootout
Dan Bernstein, Tanja Lange

Evaluation Of Compact FPGA Implementations For All SHA-3 Finalists
Bernhard Jungk

XBX Benchmarking Results January 2012
Christian Wenzel-Benner, Jens Graef, John Pham, Jens Peter Kaps

Grøstl Implementation Guide
Martin Schlaffer, Krystian Matusiewicz, Soren S. Thomsen

On the Suitability of SHA-3 Finalists for Lightweight Applications
Tolga Yalcin, Elif Kavun

Lightweight Implementations of SHA-3 Finalists on FPGAs
Jens Peter Kaps, Panasayya Yalla, Kishore Kumar Surapathi, Bilal Habib, Susheel Vadlamudi, Smriti Gurung

Efficient Hardware Implementations and Hardware Performance Evaluation of SHA-3 Finalists
Kashif Latif, M. Rao Muzaffar, Arshad Aziz, Athar Mahboob

These papers are accepted, but will not be presented in the SHA-3 Conference because they are being presented in FSE 2012

Improved Rebound Attack on the Finalist Grostl
Jeremy Jean, Maria Naya-Plasencia, Thomas Peyrin

Differential Propagation Analysis of Keccak
Joan Daemen, Gilles Van Assche

New Attacks on Keccak-224 and Keccak-256
Itai Dinur, Orr Dunkelman, Adi Shamir

Preimage Attack on Skein-512
Alexandra Savelieva, Dmitry Khovratovich, Christian Rechberger

Conference Website:
http://csrc.nist.gov/groups/ST/hash/sha-3/Round3/March2012/index.html