The Second SHA-3 Candidate Conference Accepted Papers

Security Analysis Submissions

- ***Distinguisher for Full Final Round of Fugue-256***
  Jean-Philippe Aumasson and Raphael C.-W. Phan

- ***Message Recovery and Pseudo-Preimage Attacks on the Compression Function of Hamsi-256***
  Çağdaş Çalik and Meltem Sonmez Turan

- ***Duplexing the Sponge: Authenticated Encryption and Other Applications***
  Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche

- ****On the Security of the Keyed Sponge Construction***
  Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche

- ***Building Power Analysis Resistant Implementations of Keccak***
  Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche

- ***Distinguishers for the Compression Function of Blue Midnight Wish with Probability 1***
  Jian Guo and Søren S. Thomsen

- ****Security Analysis of SIMD***
  Charles Bouillaguet, Gaëtan Leurent, and Pierre-Alain Fouque

- ***Symmetric States and their Structure: Improved Analysis of CubeHash***
  Niels Ferguson, Stefan Lucks, and Kerry A. McKay

- ***Pseudo-Linear Approximations for ARX Ciphers With Application to Threefish***
  Kerry A. McKay and Poorvi L. Vora

- ****On the Indifferentiability of the Groestl Hash Function***
  Elena Andreeva, Bart Mennink and Bart Preneel

- ***Security Reductions of the SHA-3 Candidates***
  Elena Andreeva, Bart Mennink and Bart Preneel

- ***A SAT-based Preimage Analysis of Reduced KECCAK Hash Functions***
  Pawel Morawiecki and Marian Srebrny

- ****Internal Distinguishers in Indifferentiable Hashing: The Shabal Case***
  Emmanuel Bresson, Anne Canteaut, Thomas Fuhr, Thomas Icart,
  María Naya-Plasencia, Pascal Paillier, Jean-René Reinhard, Marion Videau

- ***Rotational Rebound Attacks on Reduced Skein***
  Dmitry Khovratovich, Ivica Nikolic, and Christian Rechberger

- ***New Non-Ideal Properties of AES-Based Permutations: Applications to ECHO and Grøstl***
  Yu Sasaki, Yang Li, Lei Wang, Kazuo Sakiyama, and Kazuo Ohta

- ***Subspace Distinguisher for 5/8 Rounds of the ECHO-256 Hash***
  Martin Schläffer

- ***Practical Near-Collisions for Reduced Round Blake, Fugue, Hamsi and JH***
  Meltem Sonmez Turan, Erdener Uyan

- ***Cryptanalysis of the Compression Function of SIMD***
  Hongbo Yu, Xiaoyun Wang

Implementation/Performance-Oriented Submissions

- ***FPGA Implementations of the Round Two SHA-3 Candidates***
  Brian Baldwin, Neil Hanley, Mark Hamilton, Liang Lu,
  Andrew Byrne, Maire O'Neill and William P. Marnane

- ***Software Speed of SHA-3 Candidates***
  Daniel J. Bernstein

- ***An Efficient Software Implementation of Fugue***
  Çağdaş Çalik

- ***Evaluation of SHA-3 Candidates for 8-bit Embedded Processors***
  Thomas Eisenbarth, Stefan Heyse, Ingo von Maurich, Thomas Poeppelmann, Johannes Rave, Cornel Reuber, Alexander Wild

- ***Resource-Efficient Implementation of "Blue Midnight Wish-256" Hash Function on Xilinx FPGA Platform***
  Mohamed El-Hadedy, Martin Margala, Danilo Gligoroski and Svein J. Knapskog

- ***Unfolding Method for Shabal on Virtex-5 FPGAs: Concrete Results***
  Julien Francq and Celine Thuillet

- ***Comprehensive Comparison of Hardware Performance of Fourteen Round 2 SHA-3 Candidates with 512-bit Outputs Using Field Programmable Gate Arrays***
  Kris Gaj, Ekawat Homsirikamol, and Marcin Rogawski

- ****ATHENa – Automated Tool for Hardware EvaluatioN: Toward Fair and Comprehensive Benchmarking of Cryptographic Algorithms using FPGAs***
  Kris Gaj, Jens-Peter Kaps, Venkata Amirineni, Marcin Rogawski, Ekawat Homsirikamol

- ***Sharing Resources Between AES and the SHA-3 Second Round Candidates Fugue and Grøstl***
  Kimmo U. Jarvinen

- ***How Can We Conduct Fair and Consistent Hardware Evaluation for SHA-3 Candidate?***
  Shin'ichiro Matsuo, Miroslav Knezevic, Patrick Schaumont, Ingrid Verbauwhede, Akashi Satoh, Kazuo Sakiyama and Kazuo Ota

- ***Optimizing Blue Midnight Wish for Size***
  Daniel Otte

- ***Comparative Performance Review of the SHA-3 Second-Round Candidates***
  Thomas Pornin

- ***Efficient Hardware Implementation of high Throughput SHA-3 Candidates Keccak, Luffa and Blue Midnight Wish for Single- and Multi-Message Hashing***
  Abdulkadir Akin, Aydin Aysu, Onur Can Ulusel, and Erkay Savas

- ***Fair and Comprehensive Performance Evaluation of 14 Second Round SHA-3 ASIC Implementations***
  X. Guo, S. Huang, L. Nazhandali and P. Schaumont

- ***Uniform Evaluation of Hardware Implementations of the Round-Two SHA-3 Candidates***
  Stefan Tillich, Martin Feldhofer, Mario Kirschbaum, Thomas Plos, Joern-Marc Schmidt, and Alexander Szekely

- ***A Skein-512 Hardware Implementation***
  Jesse Walker, Farhana Sheikh, Sanu K. Mathew, Ram Krishnamurthy

- ***Benchmarking SHA-3 Candidates on Embedded Platforms***
  Christian Wenzel-Benner, Jens Graef, Marcus Himmel

- ***Serialized Keccak Architecture for Lightweight Applications***
  B. Bilgin, E.B. Kavun, T. Yalcin

*These papers were accepted, but will be presented within the time allotted for other presentations.