

The Second SHA-3 Candidate Conference

August 23-24, 2010

University of California, Santa Barbara [Corwin Pavilion]

Zip files of the [presentations](#) and [papers](#) are now available.

<i>First Day</i> <i>Monday, August 23, 2010</i>	
9:00 – 9:10 (10 minutes)	Opening Remarks William Burr, <i>Manager, Security Technology Group, Computer Security Division, National Institute of Standards and Technology</i>
9:10 – 10:30 (80 minutes)	Session I: Security Analysis (Part A) (15 minutes each) Session Chair: Lily Chen, NIST <ol style="list-style-type: none">1. Deterministic Differential Properties of the BMW Compression Function [paper] <i>Presented by:</i> Søren S. Thomsen, <i>Technical University of Denmark</i>2. Distinguisher for Full Final Round of Fugue-256 [paper] <i>Presented by:</i> Jean-Philippe Aumasson, <i>Nagravision SA</i>3. New Non-Ideal Properties of AES-Based Permutations Applications to ECHO and Grøstl [paper] <i>Presented by:</i> Yu Sasaki, <i>NTT Corporation</i>4. Subspace Distinguisher for 5/8 Rounds of the ECHO-256 Hash Function [paper] <i>Presented by:</i> Martin Schläffer, <i>IAIK, TU Graz</i>5. Rotational Rebound Attacks on Reduced Skein [paper] <i>Presented by:</i> Christian Rechberger, <i>KU Leuven and IBBT</i>
10:30 – 10:55 (25 minutes)	Coffee Break

<p>10:55 – 12:15 (80 minutes)</p>	<p>Session II: Security Analysis (Part B) (15 minutes each) Session Chair: John Kelsey, NIST</p> <ol style="list-style-type: none"> 1. Cryptanalysis of the Compression Function of SIMD [paper] <i>Presented by:</i> Hongbo Yu, Institute for Advanced Study, Tsinghua University Beijing 2. <u>Message Recovery and Pseudo-Preimage Attacks on the Compression Function of Hamsi-256</u> [paper] <i>Presented by:</i> Cagdas Calik, Institute of Applied Mathematics, Middle East Technical University 3. <u>Symmetric States and their Structure – Improved Analysis of CubeHash</u> [paper] <i>Presented by:</i> Kerry McKay, George Washington University 4. <u>Building power analysis resistant implementations of Keccak</u> [paper] <i>Presented by:</i> Guido Bertoni, STMicroelectronics 5. <u>Duplexing the sponge – authenticated encryption and other applications</u> [paper] <i>Presented by:</i> Joan Daemen, STMicroelectronics
<p>12:15 – 13: 45 (90 minutes)</p>	<p>Lunch <i>De La Guerra Dining Commons</i></p>

<p>13:45 – 15:05 (80 minutes)</p>	<p>Session III: Hardware Implementations – Surveys (15 minutes each) Session Chair: Lawrence Bassham, NIST</p> <ol style="list-style-type: none"> 1. <u>Uniform Evaluation of Hardware Implementations of the Round-Two SHA-3 Candidates</u> [paper] <i>Presented by:</i> Stefan Tillich, University of Bristol 2. <u>Fair and Comprehensive Performance Evaluation of 14 Second Round SHA-3 ASIC Implementations</u> [paper] <i>Presented by:</i> Patrick Schaumont, Virginia Tech 3. <u>FPGA Implementations of the Round Two SHA-3 Candidates</u> [paper] <i>Presented by:</i> Brian Baldwin, Claude Shannon Institute for Discrete Mathematics, Coding and Cryptography 4. <u>How Can We Conduct Fair and Consistent Hardware Evaluation for SHA-3 Candidate</u> [paper] <i>Presented by:</i> Shin'ichiro Matsuo, National Institute of Information and Communications Technology 5. <u>Comprehensive Comparison of Hardware Performance of Fourteen Round 2 SHA-3 Candidates with 512-bit Outputs Using Field Programmable Gate Arrays</u> [paper] <i>Presented by:</i> Kris Gaj, George Mason University <p><u>ATHENa – Automated Tool for Hardware Evaluation – Toward Fair and Comprehensive Benchmarking of Cryptographic Algorithms using FPGAs</u> [paper] <i>Presented by:</i> Kris Gaj, George Mason University</p>
<p>15:05 – 15:30 (25 minutes)</p>	<p>Coffee Break</p>

<p>15:30 – 16:35 (65 minutes)</p>	<p>Session IV: Hardware Implementations – Selected Algorithms (12 minutes each) Session Chair: Andrew Regenscheid, NIST</p> <ol style="list-style-type: none"> 1. <u>Sharing Resources Between AES and the SHA-3 Second Round Candidates Fugue and Grøstl</u> [paper] <i>Presented by:</i> Kimmo Järvinen, Aalto University, School of Science and Technology 2. <u>Efficient Hardware Implementations of High Throughput SHA-3 Candidates Keccak, Luffa and Blue Midnight Wish for Single- and Multi-Message Hashing</u> [paper] <i>Presented by:</i> ErKay Savas, Sabanci University 3. <u>Resource-Efficient Implementation of Blue Midnight Wish-256 Hash Function on Xilinx FPGA Platform</u> [paper] <i>Presented by:</i> Mohamed El Hadedy, Norwegian University of Science and Technology 4. <u>Unfolding Method for Shabal on Virtex-5 FPGAs – Concrete Results</u> [paper] <i>Presented by:</i> Céline Thuillet, EADS Defence & Security, France 5. <u>A Skein-512 Hardware Implementation</u> [paper] <i>Presented by:</i> Jesse Walker, Intel Corporation
<p>16:35 – 16:40 (5 minutes)</p>	<p>Short Break</p>
<p>16:40 – 17:30 (50 minutes)</p>	<p>Session V: <u>Open Discussion – SHA-3 Competition Strategies and Timeline</u> Session Chair: William Burr, <i>Manager, Security Technology Group, Computer Security Division, National Institute of Standards and Technology</i></p>
<p>17:30</p>	<p>Adjourn for Day</p>
<p>19:00 – 21:00 (2 hours)</p>	<p>Reception <i>The Faculty Club</i></p>

<i>Second Day</i> <i>Tuesday, August 24, 2010</i>	
9:00 – 9:50 (50 minutes)	<p>Session VI: Software Implementations – Surveys (15 minutes each) Session Chair: Rene Peralta, NIST</p> <ol style="list-style-type: none"> 1. Comparative Performance Review of the SHA-3 Second-Round Candidates [paper] <i>Presented by:</i> Thomas Pornin, Cryptolog International 2. Software speed of SHA-3 candidates [paper] <i>Presented by:</i> Daniel J. Bernstein, University of Illinois at Chicago 3. Benchmarking SHA-3 Candidates on Embedded Platforms [paper] <i>Presented by:</i> Christian Wenzel-Benner, ITK Engineering AG
9:50 – 10:20 (30 minutes)	<p>Session VII: Software Implementations – Embedded/Lightweight (15 minutes each) Session Chair: Rene Peralta, NIST</p> <ol style="list-style-type: none"> 1. Evaluation of SHA-3 Candidates for 8-bit Embedded Processors [paper] <i>Presented by:</i> Stefan Heyse, Ruhr-University Bochum 2. Serialized Keccak Architecture for Lightweight Applications <i>Presented by:</i> Tolga Yalcin, Department of Cryptography, Institute of Applied Mathematics, Middle East Technical University
10:20 – 10:45 (25 minutes)	Coffee Break
10:45 – 11:10 (25 minutes)	<p>Session VIII: Software Implementations – Selected Algorithms (12 minutes each) Session Chair: John Kelsey, NIST</p> <ol style="list-style-type: none"> 1. Optimizing Blue Midnight Wish for size [paper] <i>Presented by:</i> Daniel Otte 2. An Efficient Software Implementation of Fugue [paper] <i>Presented by:</i> Cagdas Calik, Institute of Applied Mathematics, Middle East Technical University

<p>11:10 – 12:15 (65 minutes)</p>	<p>Session IX: Security Analysis (Part C) (15 minutes each) Session Chair: John Kelsey, NIST</p> <ol style="list-style-type: none"> 1. Practical Near-Collisions for Reduced Round Blake, Fugue, Hamsi and JH [paper] <i>Presented by:</i> Meltem Turan, NIST 2. A SAT-based preimage analysis of reduced KECCAK hash functions [paper] <i>Presented by:</i> Pawel Morawiecki, Sec. of Informatics, Kielce University of Commerce 3. Pseudo-Linear Approximations for ARX Ciphers With Application to Threefish [paper] <i>Presented by:</i> Kerry McKay, George Washington University 4. Security Reductions of the SHA-3 Candidates; On the Indifferentiability of the Grøstl Hash Function [paper 1][paper b] <i>Presented by:</i> Bart Mennink, KULeuven, Belgium
<p>12:15 – 13: 45 (90 minutes)</p>	<p>Lunch <i>De La Guerra Dining Commons</i></p>
<p>13:45 – 15:15 (90 minutes)</p>	<p>Session X: Round 2 Candidates Update (Part A) (12 minutes each) Session Chair: Ray Perlner, NIST</p> <ol style="list-style-type: none"> 1. Blake <i>Presented by:</i> Jean-Philippe Aumasson, Nagravision SA 2. BMW <i>Presented by:</i> Svein Johan Knapskog, Norwegian University of Science and Technology 3. CubeHash <i>Presented by:</i> D.J. Bernstein, University of Illinois at Chicago 4. ECHO <i>Presented by:</i> Thomas Peyrin, Ingenico 5. Fugue <i>Presented by:</i> Charanjit S. Jutla, IBM Watson Research Center 6. Groestl <i>Presented by:</i> Christian Rechberger, KU Leuven and IBBT 7. Hamsi <i>Presented by:</i> Ozgul Kucuk, KULeuven, Belgium
<p>15:15 – 15:40 (25 minutes)</p>	<p>Coffee Break</p>

<p>15:40 – 17:10 (90 minutes)</p>	<p>Session XI: Round 2 Candidates Update (Part B) (12 minutes each) Session Chair: Lily Chen, NIST</p> <p>8. <u>JH</u> <i>Presented by:</i> Honjun Wu, Institute for Infocomm Research</p> <p>9. <u>Keccak Update and (Optional) Presentation</u> <u>On the security of the keyed sponge construction</u> [paper] <i>Presented by:</i> Gilles Van Assche, STMicroelectronics</p> <p>10. <u>Luffa</u> <i>Presented by:</i> Dai Watanabe, Hitachi, Ltd.</p> <p>11. <u>Shabal Update and (Optional) Presentation</u> <u>Internal Distinguishers in Indifferentiable Hashing - The Shabal Case</u> [paper] <i>Presented by:</i> Anne Canteaut, INRIA Paris-Rocquencourt</p> <p>12. <u>Shavite-3</u> <i>Presented by:</i> Orr Dunkelman, ENS</p> <p>13. <u>SIMD Update and (Optional) Presentation</u> <u>Security Analysis of SIMD</u> [paper] <i>Presented by:</i> Gaëtan Leurent, ENS</p> <p>14. <u>Skein</u> <i>Presented by:</i> Doug Whiting, Exar</p>
<p>17:10 – 17:30 (20 minutes)</p>	<p>Closing Remarks William Burr, <i>Manager, Security Technology Group, Computer Security Division, National Institute of Standards and Technology</i></p>
<p>17:30</p>	<p>Adjourn</p>