The Second SHA-3 Candidate Conference

August 23-24, 2010
University of California, Santa Barbara [Corwin Pavilion]

First Day ***Monday, August 23, 2010***	
9:00 – 9:10 (10 minutes)	**Opening Remarks** William Burr, *Manager, Security Technology Group, Computer Security Division, National Institute of Standards and Technology*
9:10 – 10:30 (80 minutes)	**Session I: Security Analysis (Part A)** (15 minutes each) **Session Chair:** Lily Chen, NIST **1. Deterministic Differential Properties of the BMW Compression Function** *Presented by:* Søren S. Thomsen, *Technical University of Denmark* **2. Distinguisher for Full Final Round of Fugue-256** *Presented by:* Jean-Philippe Aumasson, Nagravision SA **3. New Non-Ideal Properties of AES-Based Permutations Applications to ECHO and Grøstl** *Presented by:* Yu Sasaki, NTT Corporation **4. Subspace Distinguisher for 5/8 Rounds of the ECHO-256 Hash Function** *Presented by:* Martin Schläffer, IAIK, TU Graz **5. Rotational Rebound Attacks on Reduced Skein** *Presented by:* Christian Rechberger, KU Leuven and IBBT
10:30 – 10:55 (25 minutes)	**Coffee Break**

10:55 – 12:15 (80 minutes)	**Session II: Security Analysis (Part B)** (15 minutes each) **Session Chair:** John Kelsey, NIST **1. Cryptanalysis of the Compression Function of SIMD** *Presented by:* Hongbo Yu, Institute for Advanced Study, Tsinghua University Beijing **2. Message Recovery and Pseudo-Preimage Attacks on the Compression Function of Hamsi-256** *Presented by:* Cagdas Calik, Institute of Applied Mathematics, Middle East Technical University **3. Symmetric States and their Structure – Improved Analysis of CubeHash** *Presented by:* Kerry McKay, George Washington University **4. Building power analysis resistant implementations of Keccak** *Presented by:* Guido Bertoni, STMicroelectronics **5. Duplexing the sponge – authenticated encryption and other applications** *Presented by:* Joan Daemen, STMicroelectronics
12:15 – 13: 45 (90 minutes)	**Lunch** ***De La Guerra Dining Commons***

13:45 – 15:05 (80 minutes)	**Session III: Hardware Implementations – Surveys** (15 minutes each) **Session Chair:** Lawrence Bassham, NIST **1. Uniform Evaluation of Hardware Implementations of the Round-Two SHA-3 Candidates** *Presented by:* Stefan Tillich, University of Bristol **2. Fair and Comprehensive Performance Evaluation of 14 Second Round SHA-3 ASIC Implementations** *Presented by:* Patrick Schaumont, Virginia Tech **3. FPGA Implementations of the Round Two SHA-3 Candidates** *Presented by:* Brian Baldwin, Claude Shannon Institute for Discrete Mathematics, Coding and Cryptography **4. How Can We Conduct Fair and Consistent Hardware Evaluation for SHA-3 Candidate** *Presented by:* Shin'ichiro Matsuo, National Institute of Information and Communications Technology **5. Comprehensive Comparison of Hardware Performance of Fourteen Round 2 SHA-3 Candidates with 512-bit Outputs Using Field Programmable Gate Arrays** *Presented by:* Kris Gaj, George Mason University **ATHENa – Automated Tool for Hardware EvaluatioN – Toward Fair and Comprehensive Benchmarking of Cryptographic Algorithms using FPGAs** *Presented by:* Kris Gaj, George Mason University
15:05 – 15:30 (25 minutes)	**Coffee Break**

15:30 – 16:35 (65 minutes)	**Session IV: Hardware Implementations – Selected Algorithms** (12 minutes each) **Session Chair:** Andrew Regenscheid, NIST **1. Sharing Resources Between AES and the SHA-3 Second Round Candidates Fugue and Grøstl** *Presented by:* Kimmo Järvinen, Aalto University, School of Science and Technology **2. Efficient Hardware Implementations of High Throughput SHA-3 Candidates Keccak, Luffa and Blue Midnight Wish for Single- and Multi-Message Hashing** *Presented by:* Erkay Savas, Sabanci University **3. Resource-Efficient Implementation of Blue Midnight Wish-256 Hash Function on Xilinx FPGA Platform** *Presented by:* Mohamed El Hadedy, Norwegian University of Science and Technology **4. Unfolding Method for Shabal on Virtex-5 FPGAs – Concrete Results** *Presented by:* Céline Thuillet, EADS Defence & Security, France **5. A Skein-512 Hardware Implementation** *Presented by:* Jesse Walker, Intel Corporation
16:35 – 16:40 (5 minutes)	**Short Break**
16:40 – 17:30 (50 minutes)	**Session V: Open Discussion – SHA-3 Competition Strategies and Timeline** **Session Chair:** William Burr**,** *Manager, Security Technology Group, Computer Security Division, National Institute of Standards and Technology*
17:30	**Adjourn for Day**
19:00 – 21:00 (2 hours)	**Reception** ***The Faculty Club***

Second Day *Tuesday, August 24, 2010*	
9:00 – 9:50 (50 minutes)	**Session VI: Software Implementations – Surveys** (15 minutes each) **Session Chair:** Rene Peralta, NIST 1. **Comparative Performance Review of the SHA-3 Second-Round Candidates** *Presented by:* Thomas Pornin, Cryptolog International 2. **Software speed of SHA-3 candidates** *Presented by:* Daniel J. Bernstein, University of Illinois at Chicago 3. **Benchmarking SHA-3 Candidates on Embedded Platforms** *Presented by:* Christian Wenzel-Benner, ITK Engineering AG
9:50 – 10:20 (30 minutes)	**Session VII: Software Implementations – Embedded/Lightweight** (15 minutes each) **Session Chair:** Rene Peralta, NIST 1. **Evaluation of SHA-3 Candidates for 8-bit Embedded Processors** *Presented by:* Stefan Heyse, Ruhr-University Bochum 2. **Serialized Keccak Architecture for Lightweight Applications** *Presented by:* 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)	**Session VIII: Software Implementations – Selected Algorithms** (12 minutes each) **Session Chair:** John Kelsey, NIST 1. **Optimizing Blue Midnight Wish for size** *Presented by:* Daniel Otte 2. **An Efficient Software Implementation of Fugue** *Presented by:* Cagdas Calik, Institute of Applied Mathematics, Middle East Technical University

11:10 – 12:15 (65 minutes)	**Session IX: Security Analysis (Part C)** (15 minutes each) **Session Chair:** John Kelsey, NIST 1. **Practical Near-Collisions for Reduced Round Blake, Fugue, Hamsi and JH** *Presented by:* Meltem Turan, NIST 2. **A SAT-based preimage analysis of reduced KECCAK hash functions** *Presented by:* Pawel Morawiecki, Sec. of Informatics, Kielce University of Commerce 3. **Pseudo-Linear Approximations for ARX Ciphers With Application to Threefish** *Presented by:* 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] *Presented by:* Bart Mennink, KULeuven, Belgium
12:15 – 13: 45 (90 minutes)	**Lunch** ***De La Guerra Dining Commons***
13:45 – 15:15 (90 minutes)	**Session X: Round 2 Candidates Update (Part A)** (12 minutes each) **Session Chair:** Ray Perlner, NIST 1. **Blake** *Presented by:* Jean-Philippe Aumasson, Nagravision SA 2. **BMW** *Presented by:* Svein Johan Knapskog, Norwegian University of Science and Technology 3. **CubeHash** *Presented by:* D.J. Bernstein, University of Illinois at Chicago 4. **ECHO** *Presented by:* Thomas Peyrin, Ingenico 5. **Fugue** *Presented by:* Charanjit S. Jutla, IBM Watson Research Center 6. **Groestl** *Presented by:* Christian Rechberger, KU Leuven and IBBT 7. **Hamsi** *Presented by:* Ozgul Kucuk, KULeuven, Belgium
15:15 – 15:40 (25 minutes)	**Coffee Break**

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

Update History:

8/16/10

- Added links to presentations and papers that were received by August 15

8/17/10

- Added paper “valuation of SHA-3 Candidates for 8-bit Embedded Processors”
- Added presentation “Subspace Distinguisher for 5/8 Rounds of the ECHO-256 Hash Function”

8/22/10

- Updated paper “Evaluation of SHA-3 Candidates for 8-bit Embedded Processors”
- Updated paper “Fair and Comprehensive Performance Evaluation of 14 Second Round SHA-3 ASIC Implementations”
- Updated paper and presentation for “FPGA Implementations of the Round Two SHA-3 Candidates”
- Added “ECHO” presentation
- Added “Shabal” presentation
- Added “BMW” presentation

8/23/10

- Added “Rotational Rebound Attacks on Reduced Skein” presentation
- Updated “A Skein-512 Hardware Implementation” presentation
- Added “Cryptanalysis of the Compression Function of SIMD” paper
- Added Day 1 Wrap-Up Presentation
- Updated “Uniform Evaluation of Hardware Implementations of the Round-Two SHA-3 Candidates” presentation
- Updated “Subspace Distinguisher for 5/8 Rounds of the ECHO-256 Hash Function”
- Updated “Benchmarking SHA-3 Candidates on Embedded Platforms” presentation and paper
- Updated “Resource-Efficient Implementation of BLUE MIDNIGHT WISH-256 Hash Function on Xilinx FPGA Platform” presentations
- Updated “Comprehensive Comparison of Hardware Performance of Fourteen Round 2 SHA-3 Candidates with 512-bit Outputs Using Field Programmable Gate Arrays” & “ATHENa – Automated Tool for Hardware EvaluatioN – Toward Fair and Comprehensive Benchmarking of Cryptographic Algorithms using FPGAs” presentation
- Added “SHAvite-3” presentation
- Updated “Evaluation of SHA-3 Candidates for 8-bit Embedded Processors” presentations

8/24/10

- Updated “Blake”, “BlueMidnightWish”, “ECHO” and “SHAvite-3” presentations
- Added “Optimizing Blue Midnight Wish for Size” presentation
- Updated “SIMD Update and Security Analysis of SIMD” presentation
- Added “Skein”, “Luffa”, “Fugue”, “Hamsi” and “JH” presentations
- Updated “Pseudo-Linear Approximations for ARX Ciphers With Application to Threefish” and “Symmetric States and their Structure – Improved Analysis of CubeHash” presentations
- Updated “Practical Near-Collisions for Reduced Round Blake, Fugue, Hamsi and JH” and “An Efficient Software Implementation of Fugue”
- Added “Groestl” and “CubeHash” presentations
- Updated “Shabal” presentation