The First SHA-3 Candidate Conference
Program

Wednesday, February 25, 2009

10:30 am – 12:00 pm and 1:00 pm – 5:00 pm	**Registration** Registration will open during the FSE 2009 Conference *Location: Museumzaal*
	Opening Remarks William Burr, *Manager, Security Technology Group, Computer Security Division, National Institute of Standards and Technology*
2:15 pm – 3:45 pm	**Session I: Presentations of First Round Candidates** **Session Chair:** Donna Dodson, *NIST* 1. ECHO, *presented by: Thomas Peyrin** 2. Grøstl, *presented by: Christian Rechberger* 3. Cheetah, *presented by: Dmitry Khovratovich* *4.* Lesamnta, *presented by: Hirotaka Yoshida* 5. ARIRANG, *presented by: Jongsung Kim*
3:45 pm – 4:15 pm	**Break** *Location: Museumzaal*
4:15 pm – 5:45 pm	**Session II: Presentations of First Round Candidates** **Session Chair:** Mridul Nandi, *NIST* 1. Twister*, presented by: Ewan Fleischmann* 2. Luffa, *presented by: Dai Watanabe* 3. JH, *presented by: Hongjun Wu* *4.* Sarmal, *presented by: Kerem Varici*
	Adjourn for Day

**Presenter affiliations are listed on the last page.*

Last Updated: 3/5/09

Thursday, February 26, 2009

8:30 am – 5:00 pm	**Registration** *Location: Museumzaal*
	Session III: Presentations of First Round Candidates **Session Chair:** Rene Peralta, *NIST* 1. CubeHash*, presented by: D. J. Bernstein* 2. Fugue*, presented by: Charanjit S. Jutla* 3. Keccak*, presented by: Guido Bertoni, Joan Daemen, Michael Peeters and Gilles Van Assche* 4. LUX*, presented by: Ivica Nikolic* 5. Vortex*, presented by: Shay Gueron and Michael Kounavis*
10:30 am – 11:00 am	**Break** *Location: Museumzaal*
11:00 am – 12:00 pm	**Session IV: System Priorities** **Session Chair:** Donna Dodson, *NIST* • Application contexts • Performance and implementations tradeoffs
12:00 pm - 1:30 pm	**LUNCH [1.5 hours]** *Location: Salons Georges*
1:30 pm – 3:00 pm	**Session V: Presentations of First Round Candidates** **Session Chair:** Souradyuti Paul, *NIST* 1. BLAKE*, presented by: Jean-Philippe Aumasson* 2. LANE*, presented by: Sebastiaan Indesteege* 3. SHAvite-3*, presented by: Orr Dunkelman* 4. Skein*, presented by: Jon Callas* 5. SWIFFTX*, presented by: Vadim Lyubashevsky*
3:00 pm – 3:30 pm	**Break** *Location: Museumzaal*
3:30 pm – 4:45 pm	**Session VI: Presentations of First Round Candidates** **Session Chair:** Lily Chen, *NIST* 1. ECOH*, presented by: Daniel R. L. Brown* 2. ESSENCE*, presented by: Jason Worth Martin* 3. MD6*, presented by: Ronald L. Rivest* 4. SANDstorm*, presented by: Rich Schroeppel*
4:45 pm – 5:45 pm	**Session VII: Security Evaluation** **Session Chair:** Rene Peralta, *NIST* • NIST's views on SHA-3's security requirements, *presented by: Mridul Nandi* • Evaluation of attacks, *presented by: Mridul Nandi* • Q&A, *moderated by: Rene Peralta*
7:00 pm	**Dinner / Reception** *Location: Faculty Club*

**Presenter affiliations are listed on the last page.*

Friday, February 27, 2009

8:30 am – 5:00 pm	**Registration** *Location: Museumzaal*
	Session VIII: Presentations of First Round Candidates **Session Chair:** Donna Dodson, *NIST* 1. AURORA*, presented by: Tetsu Iwata* 2. CHI*, presented by: Phillip Hawkes* 3. SIMD*, presented by: Gaetan Leurent* 4. TIB3*, presented by: Daniel Penazzi* 5. Shabal*, presented by: Anne Canteaut*
10:30 am – 11:00 am	**Break** *Location: Museumzaal*
11:00 am – 12:00 pm	**Session IX: Security-Performance Tradeoff** **Session Chair:** Souradyuti Paul, *NIST* • NIST's plan for handling tunable parameters, *presented by: Souradyuti Paul* • Role of performance in the first cut, *presented by: Souradyuti Paul* • Q&A, *moderated by: Souradyuti Paul and William Burr*
12:00 pm - 1:30 pm	**LUNCH [1.5 hours]** *Location: Salons Georges*
1:30 pm – 2:45 pm	**Session X: Presentations of First Round Candidates** **Session Chair:** Rene Peralta*, NIST* 1. NaSHA*, presented by: Aleksandra Mileva* 2. EDON-R*, presented by: Danilo Gligoroski* 3. FSB*, presented by: Matthieu Finiasz* 4. Spectral Hash*, presented by: Cetin Kaya Koc*
2:45 pm – 4:00 pm	**Session XI: Presentations of First Round Candidates** **Session Chair:** Lily Chen, *NIST* 1. Blue Midnight Wish*, presented by: Svein Johan Knapskog* 2. EnRUPT*, presented by: Sean O'Neil* 3. Hamsi*, presented by: Ozgul Kucuk* 4. CRUNCH*, presented by: Emmanuel Volte*
4:00 pm – 4:30 pm	**Break** *Location: Museumzaal*
4:30 pm – 5:30 pm	**Session XII: The Way Forward** **Session Chair:** William Burr, *NIST*
5:30 pm	**Adjourn for Day**

**Presenter affiliations are listed on the last page.*

Saturday, February 28, 2009

9:00 am – 10:20 am **A First Look at the First Round Candidates**
Session Chair: Mridul Nandi, *NIST*

- Classification of the SHA-3 Candidates*, presented by: Christian Forler*
- SHA-3 Zoo*, presented by: Christian Rechberger*
- Engineering Comparison of the SHA-3 Candidates*, presented by: Niels Ferguson*
- eBASH*, presented by: D. J. Bernstein*

Break
Location: Museumzaal

10:50 am – 12:00 pm **RUMP Session**
Session Chair: William Burr, *NIST*

1. Cryptanalysis of Dynamic SHA, *presented by Sebastiaan Indesteege*
2. Lane, *presented by Sebastiaan Indesteege* (2 min)
3. Second preimage attack on SHAMATA-512, *presented by Kota Ideguchi and Dai Watanabe*
4. Observations of non-randomness in the ESSENCE compression function, *presented by Nicky Mouha, Søren S. Thomsen, Meltem Sönmez Turan and Bart Preneel*
5. Length extension of Keccak cryptanalysis prize, *presented by Guido Bertoni, Joan Daemen, Michaël Peeters and Gilles Van Assche* (2 min)
6. More engineering considerations for the SHA-3 hash function, *presented by Orr Dunkelman*
7. Bit attack, *presented by Dan Bernstein*
8. Ponic algorithm, *presented by Peter Schmidt Nielsen*
9. Data, Clarification, Opinion, and a Challenge, *presented by Shay Gueron*
10. ERINDALE family of hash functions, *presented by Nikolajs Volkovs*
11. Thoughts on Permutation Based Hashes (Theoretical), *presented by Martijn Stam*
12. Replay attack on a one-way hash function, *presented by Dan Bernstein*

12:00 pm **Adjourn**

The following algorithms will not be presented at the First SHA-3 Candidate Conference; however, presentation materials that have been submitted and will be posted on the Hash Competition website [http://csrc.nist.gov/groups/ST/hash/sha-3/Round1/Feb2009/program.html].

- Blender, *principal submitter: Dr. Colin Bradbury*
- Dynamic SHA, *principal submitter: Xu Zijie*
- Dynamic SHA2, *principal submitter: Xu Zijie*
- MCSSHA-3, *principal submitter: Mikhail Maslennikov*
- Sgàil, *principal submitter: Peter Maxwell*

**Presenter affiliations are listed on the last page.*

SHA-3 PRESENTER AFFILIATIONS

Aumasson, Jean-Phillipe	FHNW
Bernstein, Dan	University of Illinois at Chicago
Bertoni, Guido	STMicroelectronics
Brown, Daniel R.L.	Certicom
Callas, Jon	PGP Corporation
Canteaut, Anne	INRIA project-team SECRET
Daemen, Joan	STMicroelectronics
Dunkelman, Orr	ENS
Finiasz, Matthieu	ENSTA
Fleischmann, Ewan	Bauhaus-University Weimar, Germany
Forler, Christian	Sirrix AG Security Technologies
Gligoroski, Danilo	NTNU – Norway
Gueron, Shay	Intel Corporation
Hawkes, Phillip	Qualcomm International
Indesteege, Sebastiaan	K.U. Leuven, Dept. ESAT/SCD-COSIC
Iwata, Tetsu	Nagoya University
Jutla, Charanjit	IBM T.J. Watson Research Center
Khovratovich, Dmitry	University of Luxembourg
Kim, Jongsung	CIST, Korea University
Koc, Cetin Kaya	University of California Santa Barbara
Kounavis, Michael	Intel Corporation
Knapskog, Svein Johan	Norwegian University of Science and Technology/Q2S
Kucuk, Ozgul	K.U. Leuven, Dept. ESAT/SCD-COSIC
Leurent, Gaetan	École Normale Supérieure
Lyubashevsky, Vadim	Tel-Aviv University
Martin, Jason Worth	James Madison University
Mileva, Aleksandra	Faculty of Informatics, University of “Goce Delčev”
Nikolic, Ivica	University of Luxembourg
O'Neil, Sean	VEST Corporation
Peeters, Michael	NXP Semiconductors
Penazzi, Daniel	Universidad Nacional de Córdoba
Peyrin, Thomas	INGENICO
Rechberger, Christian	Graz University of Technology
Rivest, Ron L.	Massachusetts Institute of Technology
Schroeppel, Rich	Sandia National Laboratories
Van Assche, Gilles	STMicroelectronics
Varici, Kerem	K.U. Leuven
Volte, Emmanuel	University of Cergy-Pontoise and Versailles-Saint Quentin
Watanabe, Dai	Hitachi, Ltd.
Wu, Hongjun	Institute for Infocomm Research
Yoshida, Hirotaka	Hitachi, Ltd.