SHA-2 will soon retire

The SHA-3 Song

Michael Naehrig Christiane Peters Peter Schwabe *

Department of Mathematics and Computer Science
Technische Universiteit Eindhoven, P.O. Box 513, 5600 MB Eindhoven, Netherlands
michael@cryptojedi.org, c.p.peters@tue.nl, peter@cryptojedi.org

Abstract

Sing to the melody of [31], lyrics and chords are also available at [42].

1 Introduction

G D Em C G D Em C

2 Lyrics

G   **D**
Cheetah[33] and Dynamic-SHA[59], CHI[26], Lux[43], Luffa[13], Lesamnta[27],
Em   **C**
BLAKE[4], LANE[29], Hamsi[45], Skein[19], NKS2D[46].
G   **D**
All repeat SHAvite-3[9], Mikhail Maslennikov,
Em   **D**
is the man behind MCSSHA-3[39].

G D Em C

G   **D**
ECHO[5], ECOH[12], EDON-R[22], Spectral Hash[50] and Aurora[30],
Em   **D**
MD6[48] and ARIRANG[14] do not rhyme with anythang.
G   **D**
SWIFFTX[2], VORTEX[34], FSB[3], Sgàil[40], Fugue[24] and TIB-3[41],
Em   **C**
No one knows their fate, Shabal[11] plays at number 8.

G   **D**
SHA-2 will soon retire,
        Am   **C**
because NIST is learning and SHA-1 is burning.
G   **D**
SHA-2 will soon retire,
      Am   **C**
no we didn't light it but we tried to fight it.

*Permanent ID of this document: 5894e5a7cb65f7cb51c5a5077d99cddd. Date: June 22, 2009

G D
JH[58] and Blue Midnight Wish[21], Grøstl[20] is a breakfast dish,
Em C
CRUNCH[23] and SIMD[36], SANDstorm[53]... we will see.
G D
Twister[17], Blender[10] and Keccak[8], Sarmal[15], do they rock?
Em C
CubeHash[6] really sucks. Dan, do you agree?

G D
Martin, Knudsen, Misarsky, Indesteege, Jason Lee,
Em C
Hirotaka Yoshida, Küçük, Lim, Vidyasagar,
G D
Finiasz, Fay, the Keccak Team, Jutla and Jacques Patarin,
Em C
Bernstein, Biham, trouble with the benchmarks[7].

G D
SHA-2 will soon retire,
Am C
because NIST is learning and SHA-1 is burning.
G D
SHA-2 will soon retire,
Am C
no we didn't light it but we tried to fight it.

C Am
Abacus[52], Waterfall[25], StreamHash[54], Tangle[47], WAMM[56] and Boole[49],
Em D
Ponic[51], Shamata[1], DCH[57] and Maraca[32],
C Am
MeshHash[18], HASH 2X[35], didn't really meet the specs.
Em D
ZK-Crypt[16], Khichidi-1[55], they're all already gone.

G D
NaSHA[37], ESSENCE[38], Kara, Neil Sholer, Sean O'Neil,
Em C
Gligoroski, Varici, Schroeppel and Watanabe,
G D
Khovratovich, Hattersley, Leurent, Koç and Markovski,
Em C
Eurocrypt now you know, where the competition goes.

G D
SHA-2 will soon retire,
Am C
because NIST is learning and SHA-1 is burning.
G D
SHA-2 will soon retire,
Am C
no we didn't light it but we tried to fight it.

G D
26a 52d 798f1c
Em C
8a 9b d84823
G D
84d422d 6892abc
Em C
15 323 9259a6d
G D
Who will break this hash, we can say it's not just trash,
Em C
EnRUPT[44] blown away[28], what else do I have to say?

G D
SHA-2 will soon retire,
Am C
because NIST is learning and SHA-1 is burning.
G D
SHA-2 will soon retire,
Am C
no we didn't light it but we tried to fight it.

3 Outroduction

G D Em C G D Em C

4 Acknowledgement

We would like to thank Roberto Avanzi, Paulo Barreto, Leila Batina, Aurélie Bauer, Daniel J. Bernstein, Gaëtan Bisson, Steven Galbraith, Duncan Garrett, Praveen Gauravaram, Benedikt Gierlichs, Tim Güneysu, Antoine Joux, Eike Kiltz, Tanja Lange, Stefan Lucks, Amir Moradi, Christian Rechberger, Greg Rose, Francesco Sica, Hans van Tilburg, Joana Treger, Michael Vielhaber, Vanessa Vitse, Moti Yung, and the people we don't know for their kind support on stage. We furthermore thank Tanja Lange, Daniel J. Bernstein and Rémy Martin for fruitful inspirations.

References

[1] Ferhat Karakoc Adem Atalay, Orhun Kara and Cevat Manap. SHAMATA hash function algorithm specifications. Submission to NIST, 2008. `http://www.uekae.tubitak.gov.tr/uekae_content_files/crypto/SHAMATA%20Specification.pdf`.

[2] Yuriy Arbitman, Gil Dogon, Vadim Lyubashevsky, Daniele Micciancio, Chris Peikert, and Alon Rosen. SWIFFTX: A proposal for the SHA-3 standard. Submission to NIST, 2008. `http://www.eecs.harvard.edu/~alon/PAPERS/lattices/swifftx.pdf`.

[3] Daniel Augot, Matthieu Finiasz, Philippe Gaborit, Stéphane Manuel, and Nicolas Sendrier. SHA-3 proposal: FSB. Submission to NIST, 2008. `http://www-rocq.inria.fr/secret/CBCrypto/fsbdoc.pdf`.

[4] Jean-Philippe Aumasson, Luca Henzen, Willi Meier, and Raphael C.-W. Phan. SHA-3 proposal BLAKE. Submission to NIST, 2008. `http://131002.net/blake/blake.pdf`.

[5] Ryad Benadjila, Olivier Billet, Henri Gilbert, Gilles Macario-Rat, Thomas Peyrin, Matt Robshaw, and Yannick Seurin. SHA-3 proposal: ECHO. Submission to NIST, 2008. `http://ehash.iaik.tugraz.at/uploads/9/91/Echo.pdf`.

[6] Daniel J. Bernstein. CubeHash specification (2.B.1). Submission to NIST, 2008. `http://cubehash.cr.yp.to/submission/spec.pdf`.

[7] Daniel J. Bernstein and Tanja Lange (editors). eBASH: ECRYPT benchmarking of all submitted hashes, 2008. `http://bench.cr.yp.to/ebash.html` (accessed May 7, 2009).

[8] G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche. Keccak specifications. Submission to NIST, 2008. `http://keccak.noekeon.org/Keccak-specifications.pdf`.

[9] Eli Biham and Orr Dunkelman. The SHAvite-3 hash function. Submission to NIST, 2008. `http://ehash.iaik.tugraz.at/uploads/f/f5/Shavite.pdf`.

[10] Colin Bradbury. BLENDER: A proposed new family of cryptographic hash algorithms. Submission to NIST, 2008. `http://ehash.iaik.tugraz.at/uploads/5/5e/Blender.pdf`.

[11] Emmanuel Bresson, Anne Canteaut, Benoît Chevallier-Mames, Christophe Clavier, Thomas Fuhr, Aline Gouget, Thomas Icart, Jean-François Misarsky, Marìa Naya-Plasencia, Pascal Paillier, Thomas Pornin, Jean-René Reinhard, Céline Thuillet, and Marion Videau. Shabal, a submission to NIST's cryptographic hash algorithm competition. Submission to NIST, 2008. `http://ehash.iaik.tugraz.at/uploads/6/6c/Shabal.pdf`.

[12] Daniel R. L. Brown, Adrian Antipa, Matt Campagna, and Rene Struik. ECOH: the elliptic curve only hash. Submission to NIST, 2008. `http://ehash.iaik.tugraz.at/uploads/a/a5/Ecoh.pdf`.

[13] Christophe De Canniere, Hisayoshi Sato, and Dai Watanabe. Hash function Luffa: Specification. Submission to NIST, 2008. `http://ehash.iaik.tugraz.at/uploads/e/ea/Luffa_Specification.pdf`.

[14] Donghoon Chang, Seokhie Hong, Changheon Kang, Jinkeon Kang, Jongsung Kim, Changhoon Lee, Jesang Lee, Jongtae Lee, Sangjin Lee, Yuseop Lee, Jongin Lim, and Jaechul Sung. ARIRANG. Submission to NIST, 2008. `http://ehash.iaik.tugraz.at/uploads/2/2c/Arirang.pdf`.

[15] Kerem Varıcı, Onur Özen, and Çelebi Kocair. Sarmal: SHA-3 proposal. Submission to NIST, 2008. `http://www.metu.edu.tr/~e127761/Supporting_Documentation/SarmaL.pdf`.

[16] Nicolas T. Courtois, Carmi Gressel, Avi Hecht, Gregory V. Bard, and Ran Granot. The ZK-Crypt algorithm specification - the FortressGB SHA3 candidate. Submission to NIST, 2008. `http://www.fortressgb.com/var/1774/182238-00%20AA%20ZK-Crypt%20Algorithmic%20Spec%20090115.pdf`.

[17] Christian Forler Ewan Fleischmann and Michael Gorski. The Twister hash function family. Submission to NIST, 2008. `http://ehash.iaik.tugraz.at/uploads/3/39/Twister.pdf`.

[18] Björn Fay. MeshHash. Submission to NIST, 2008. http://ehash.iaik.tugraz.at/uploads/5/5a/Specification_DIN-A4.pdf.

[19] Niels Ferguson, Stefan Lucks, Bruce Schneier, Doug Whiting, Mihir Bellare, Tadayoshi Kohno, Jon Callas, and Jesse Walker. The Skein hash function family. Submission to NIST, 2008. http://www.schneier.com/skein.pdf.

[20] Praveen Gauravaram, Lars R. Knudsen, Krystian Matusiewicz, Florian Mendel, Christian Rechberger, Martin SchlXXXffer, and SXXXren S. Thomsen. Grøstl – a SHA-3 candidate. Submission to NIST, 2008. http://www.groestl.info/Groestl.pdf.

[21] Danilo Gligoroski, Vlastimil Klima, Svein Johan Knapskog, Mohamed El-Hadedy, Jørn Amundsen, and Stig Frode Mjølsnes. Cryptographic hash function BLUE MIDNIGHT WISH. Submission to NIST, 2008. http://people.item.ntnu.no/~danilog/Hash/BMW/Supporting_Documentation/BlueMidnightWishDocumentation.pdf.

[22] Danilo Gligoroski, Rune SteinsmoXXXrd, Marija Mihova, Svein Johan Knapskog, Ljupco Kocarev, AleXXX DrXXXpal, and Vlastimil Klima. Cryptographic hash function EDON-R. Submission to NIST, 2008. http://people.item.ntnu.no/~danilog/Hash/Edon-R/Supporting_Documentation/EdonRDocumentation.pdf.

[23] Louis Goubin, Mickael Ivascot, William Jalby, Olivier Ly, Valerie Nachef, Jacques Patarin, Joana Treger, and Emmanuel Volte. CRUNCH. Submission to NIST, 2008. http://www.voltee.com/crunch/cdrom/Supporting_Documentation/crunch_specifications.pdf.

[24] Shai Halevi, William E. Hall, and Charanjit S. Jutla. The hash function Fugue. Submission to NIST, 2008. http://domino.research.ibm.com/comm/research_projects.nsf/pages/fugue.index.html/$FILE/{NIST}-submission-Oct08-fugue.pdf.

[25] Bob Hattersley. Waterfall Hash - algorithm specification and analysis. Submission to NIST, 2008. http://ehash.iaik.tugraz.at/uploads/1/19/Waterfall_Specification_1.0.pdf.

[26] Phil Hawkes and Cameron McDonald. Submission to the SHA-3 competition: The CHI family of cryptographic hash algorithms. Submission to NIST, 2008. http://ehash.iaik.tugraz.at/uploads/2/2c/Chi_submission.pdf.

[27] Shoichi Hirose, Hidenori Kuwakado, and Hirotaka Yoshida. SHA-3 proposal: Lesamnta. Submission to NIST, 2008. http://ehash.iaik.tugraz.at/uploads/5/5c/Lesamnta.pdf.

[28] Sebastiaan Indesteege. Collisions for EnRUPT. Available online, 2008. http://homes.esat.kuleuven.be/~sindeste/enrupt.html.

[29] Sebastiaan Indesteege. The LANE hash function. Submission to NIST, 2008. http://www.cosic.esat.kuleuven.be/publications/article-1181.pdf.

[30] Tetsu Iwata, Kyoji Shibutani, Taizo Shirai, Shiho Moriai, and Toru Akishita. AURORA: A cryptographic hash algorithm family. Submission to NIST, 2008. http://ehash.iaik.tugraz.at/uploads/b/ba/AURORA.pdf.

[31] Billy Joel. We didn't start the fire. In *Storm Front*. Columbia Records, 1989.

[32] Robert J. Jenkins Jr. Algorithm specification. Submission to NIST, 2008. http://burtleburtle.net/bob/crypto/maraca/nist/Supporting_Documentation/specification.pdf.

[33] Dmitry Khovratovich, Alex Biryukov, and Ivica Nikolić. The hash function Cheetah: Specification and supporting documentation. Submission to NIST, 2008. http://ehash.iaik.tugraz.at/uploads/c/ca/Cheetah.pdf.

[34] Michael Kounavis and Shay Gueron. Vortex: A new family of one way hash functions based on Rijndael rounds and carry-less multiplication. Submission to NIST, 2008. http://eprint.iacr.org/2008/464.pdf.

[35] Jason Lee. HASH 2X. Submission to NIST, 2008.

[36] Gaëtan Leurent, Charles Bouillaguet, and Pierre-Alain Fouque. SIMD is a message digest. Submission to NIST, 2008. http://www.di.ens.fr/~leurent/files/SIMD.pdf.

[37] Smile Markovski and Aleksandra Mileva. 2.B.1 algorithm specification. Submission to NIST, 2008. http://inf.ugd.edu.mk/images/stories/file/Mileva/part2b1.pdf.

[38] Jason Worth Martin. ESSENCE: A candidate hashing algorithm for the NIST competition. Submission to NIST, 2008. http://www.math.jmu.edu/~martin/essence/Supporting_Documentation/essence_{NIST}.pdf.

[39] Mikhail Maslennikov. Secure hash algorithm MCSSHA-3. Submission to NIST, 2008. http://registercsp.nets.co.kr/MCSSHA/MCSSHA-3.pdf.

[40] Peter Maxwell. The Sgàil cryptographic hash function. Submission to NIST, 2008. http://www.allicient.co.uk/files/sgail/Supporting_Documentation/specification.pdf.

[41] Miguel Montes and Daniel Penazzi. The TIB3 hash. Submission to NIST, 2008. http://www.famaf.unc.edu.ar/~penazzi/tib3/submitted/Supporting_Documentation/TIB3_Algorithm_Specification.pdf.

[42] Michael Naehrig, Christiane Peters, and Peter Schwabe. SHA-2 will soon retire, 2009. http://cryptojedi.org/music/sha2-retire.shtml.

[43] Ivica Nikolić, Alex Biryukov, and Dmitry Khovratovich. Hash family LUX - algorithm specifications and supporting documentation. Submission to NIST, 2008. http://ehash.iaik.tugraz.at/uploads/f/f3/LUX.pdf.

[44] Sean O'Neil, Karsten Nohl, and Luca Henzen. EnRUPT hash function specification. Submission to NIST, 2008. http://enrupt.com/SHA3/Supporting_Documentation/EnRUPT_Specification.pdf.

[45] Özgül Küçük. The hash function Hamsi. Submission to NIST, 2008. http://ehash.iaik.tugraz.at/uploads/9/95/Hamsi.pdf.

[46] Geoffrey Park. NKS 2D cellular automata hash. Submission to NIST, 2008. http://geoffrey.park.googlepages.com/SHA3Submission01.pdf.

[47] Gary McGuire Rafael Alvarez and Antonio Zamora. The Tangle hash function. Submission to NIST, 2008. http://ehash.iaik.tugraz.at/uploads/4/40/Tangle.pdf.

[48] Ronald L. Rivest. The MD6 hash function – a proposal to NIST for SHA-3. Submission to NIST, 2008. http://groups.csail.mit.edu/cis/md6/submitted-2008-10-27/Supporting_Documentation/md6_report.pdf.

[49] Gregory G. Rose. Design and primitive specification for Boole. Submission to NIST, 2008. http://seer-grog.net/BoolePaper.pdf.

[50] Gokay Saldamlı, Cevahir Demirkıran, Megan Maguire, Carl Minden, Jacob Topper, Alex Troesch, Cody Walker, and Çetin Kaya Koç. Spectral Hash. Submission to NIST, 2008. http://www.cs.ucsb.edu/~koc/shash/sHash.pdf.

[51] Peter Schmidt-Nielsen. The Ponic hash function. Submission to NIST, 2008. http://ehash.iaik.tugraz.at/uploads/3/3c/PonicSpecification.pdf.

[52] Neil Sholer. Abacus: A candidate for SHA-3. Submission to NIST, 2008. http://ehash.iaik.tugraz.at/uploads/b/be/Abacus.pdf.

[53] Mark Torgerson, Richard Schroeppel, Tim Draelos, Nathan Dautenhahn, Sean Malone, Andrea Walker, Michael Collins, and Hilarie Orman. The SANDstorm hash. Submission to NIST, 2008. http://www.sandia.gov/scada/documents/SANDstorm_Submission_2008_10_30.pdf.

[54] Michal Trojnara. StreamHash algorithm specifications and supporting documentation. Submission to NIST, 2008. http://ehash.iaik.tugraz.at/uploads/0/09/Streamhash.pdf.

[55] Natarajan Vijayarangan. A new hash algorithm: Khichidi-1. Submission to NIST, 2008. http://ehash.iaik.tugraz.at/uploads/d/d4/Khichidi-1.pdf.

[56] John Washburn. WAMM: A candidate algorithm for the SHA-3 competition. Submission to NIST, 2008. http://www.washburnresearch.org/cryptography/archive/WaMM-SHA3.pdf.

[57] David A. Wilson. The DCH hash function. Submission to NIST, 2008. http://web.mit.edu/dwilson/www/hash/dch/Supporting_Documentation/dch.pdf.

[58] Hongjun Wu. The hash function JH. Submission to NIST, 2008. http://icsd.i2r.a-star.edu.sg/staff/hongjun/jh/jh.pdf.

[59] Zijie Xu. Dynamic SHA. Submission to NIST, 2008. http://ehash.iaik.tugraz.at/uploads/e/e2/DyamicSHA.pdf.