A brief look at the 56 SHA-3 submissions

Michael Naehrig, Christiane Peters, Peter Schwabe

Eindhoven University of Technology

April 28, 2009

Eurocrypt 2009, Rump Session

Outline

- ARIRANG
- AURORA
- BLAKE
- Blender
- Blue Midnight Wish
- Cheetah
- CHI
- CRUNCH
- CubeHash
- Dynamic SHA
- Dynamic SHA2
- ECHO
- ECOH
- Edon-R
- EnRUPT
- ESSENCE
- FSB
- Fugue
- Grøstl
- Hamsi
- JH
- Keccak
- LANE
- Lesamnta
- Luffa
- LUX
- MCSSHA-3
- MD6
- NaSHA
- SANDstorm
- Sarmal
- Sgàil
- Shabal
- SHAvite-3
- SIMD
- Skein
- Spectral Hash
- SWIFFTX
- TIB3
- Twister
- Vortex
- Abacus
- Boole
- DCH
- HASH 2X
- Khichidi-1
- Maraca
- MeshHash
- NKS2D
- Ponic
- SHAMATA
- StreamHash
- Tangle
- WaMM
- Waterfall
- ZK-Crypt

Cheetah and Dynamic-SHA, CHI, Lux, Luffa, Lesamnta, Blake, Lane, Hamsi, Skein, NKS2D.

All repeat Shavite-3 Mikhail Maslennikov, is the man behind MCSSHA-3.

Cheetah and Dynamic-SHA, CHI, Lux, Luffa, Lesamnta,
Blake, Lane, Hamsi, Skein, NKS2D.

All repeat Shavite-3 Mikhail Maslennikov,
is the man behind MCSSHA-3.

ECHO, ECOH, Edon-R, Spectral Hash and Aurora,
MD6 and ARIRANG do not rhyme with anythang.

SWIFFTX, VORTEX, FSB, Sgàil, Fugue and TIB-3,
No one knows their fate, Shabal plays at number 8.

SHA-2 will soon retire,
because NIST is learning and SHA-1 is burning.

SHA-2 will soon retire,
no we didn't light it but we tried to fight it.

JH and Blue Midnight Wish, Grøstl is a breakfast dish,
CRUNCH and SIMD, SANDstorm... we will see.

Twister, Blender and Keccak, Sarmal, do they rock?
CubeHash really sucks. Dan, do you agree?

JH and Blue Midnight Wish, Grøstl is a breakfast dish,
CRUNCH and SIMD, SANDstorm... we will see.

Twister, Blender and Keccak, Sarmal, do they rock?
CubeHash really sucks. Dan, do you agree?

Martin, Knudsen, Misarsky, Indesteege, Jason Lee,
Hirotaka Yoshida, Küçük, Lim, Vidyasagar,
Finiasz, Fay, the Keccak Team, Jutla and Jacques Patarin,
Bernstein, Biham, trouble with the benchmarks.

SHA-2 will soon retire,
because NIST is learning and SHA-1 is burning.

SHA-2 will soon retire,
no we didn't light it but we tried to fight it.

Abacus, Waterfall, StreamHash, Tangle, WaMM and Boole,
Ponic, Shamata, DCH and Maraca,
MeshHash, HASH 2X, didn't really meet the specs.
ZK-Crypt, Khichidi-1, they're all already gone.

Abacus, Waterfall, StreamHash, Tangle, WaMM and Boole,
Ponic, Shamata, DCH and Maraca,
MeshHash, HASH 2X, didn't really meet the specs.
ZK-Crypt, Khichidi-1, they're all already gone.

NaSHA, ESSENCE, Kara, Neil Sholer, Sean O'Neil,
Gligoroski, Varici, Schroeppel and Watanabe,

Khovratovich, Hattersley, Leurent, Koç and Markovski,
Eurocrypt now you know, where the competition goes.

SHA-2 will soon retire,
because NIST is learning and SHA-1 is burning.

SHA-2 will soon retire,
no we didn't light it but we tried to fight it.

0x26a52d798f1c8a9bd8482384d422d6892abc153239259a6d

0x26a52d798f1c8a9bd8482384d422d6892abc153239259a6d

Who will break this hash, we can say it's not
just trash,
EnRUPT blown away, what else do I have to say?

SHA-2 will soon retire
because NIST is learning and SHA-1 is burning

SHA-2 will soon retire
no we didn't light it but we tried to fight it.