# CubeHash round-2 modifications

Daniel J. Bernstein *

Department of Computer Science
University of Illinois at Chicago
Chicago, IL 60607–7045
cubehash@box.cr.yp.to

This document describes changes from the round-1 CubeHash submission package to the round-2 CubeHash submission package.

**CubeHash specification (2.B.1)** (`spec.pdf`) defines CubeHash$r/b$–$h$ using exactly the same text as the original CubeHash submission; CubeHash$r/b$–$h$ is exactly the same function in round 2 that it was in round 1. However, the recommendations for parameters $(r, b)$ have been updated as described in my note "CubeHash parameter tweak: 16 times faster":

- CubeHash16/32–224 is proposed for SHA–3–224,
- CubeHash16/32–256 is proposed for SHA–3–256,
- CubeHash16/32–384 is proposed for SHA–3–384–normal,
- CubeHash16/32–512 is proposed for SHA–3–512–normal,
- CubeHash16/1–384 is proposed for SHA–3–384–formal, and
- CubeHash16/1–512 is proposed for SHA–3–512–formal.

There is also a new subsection "Additional comments on symmetries" extending the symmetry paragraph in the original submission.

**CubeHash efficiency estimates (2.B.2)** (`estimates.pdf`) now summarizes eBASH Core 2 Duo benchmarks for CubeHash, confirming the original efficiency estimates. The document also adds a paragraph discussing microarchitectural variability among Core 2 Duo CPUs and recommending that NIST specify which CPU is actually the reference platform.

**CubeHash expected strength (2.B.4)** (`strength.pdf`) has been modified to note the expected impact of quantum computers. Grover's algorithm will find (e.g.) 224-bit preimages for any of the SHA–3 candidates in only about $2^{112}$ quantum operations. This quantum computer

- has a much higher success chance than a conventional computer performing $2^{200}$ operations and
- is much more likely to be available to future attackers than a conventional computer performing $2^{200}$ operations,

so considering the conventional threat while ignoring the quantum threat makes no sense from a risk-analysis perspective.

* The author was supported by the National Science Foundation under grant ITR–0716498. Date of this document: 2009.09.15.

**CubeHash attack analysis (2.B.5)** (`attacks.pdf`) has been reorganized and expanded. The document includes the description of narrow-pipe attacks that had appeared in the original submission as "CubeHash appendix: complexity of generic attacks." The document also reviews various third-party analyses of CubeHash that have been announced by Aumasson, Bloom, Brier, Dai, Janis, Kaminsky, Khazaei, Khovratovich, Meier, Naya-Plasencia, Nikolic, Peyrin, Rao, Salaev, Wang, Weinmann, and Wilson. The most recent third-party analysis is the Brier–Khazaei–Meier–Peyrin paper "Linearization framework for collision attacks: application to CubeHash and MD6" to appear at Asiacrypt 2009.

**CubeHash features (2.B.6)** (`features.pdf`) has been extended to include subsections "Unified implementation across output sizes," "Small code size and vector-code size," and "Good security/speed tradeoff."