

# Cryptology ePrint Archive: Report 2011/550

## A New Distinguisher for CubeHash-8/b and CubeHash-15/b Compression Functions

*Javad Alizadeh and Abdolrasoul Mirghadri*

**Abstract:** CubeHash is one of the round 2 candidates of the public SHA-3 competition hosted by NIST. It was designed by Bernstein. In this paper we find a new distinguisher to distinguish CubeHash compression function from a random function. This distinguisher principle is based on rotational analysis that formally introduced by Khovratovich and Nikolic. In order to use this technique, we need to compute the probability that four swap functions in CubeHash round function preserve the rotational property for any input pair. We compute these probabilities and find a new distinguisher that distinguish CubeHash-8/b and CubeHash-15/b compression function from a random function with probability greater than  $\frac{1}{2}$  and  $\frac{1}{4}$ , respectively. Until we know this is the first distinguisher for CubeHash compression function with more than 14 rounds.

**Category / Keywords:** SHA-3 candidate, CubeHash, rotational analysis, distinguisher

**Date:** received 5 Oct 2011, last revised 12 Oct 2011

**Contact author:** alizadja at gmail com

**Available formats:** [PDF](#) | [BibTeX Citation](#)

**Note:** There is an writing mistake in published version (Appendix in the paper was written before references)

**Version:** 20111012:064901 ([All versions of this report](#))

**Discussion forum:** [Show discussion](#) | [Start new discussion](#)

---

[ [Cryptology ePrint archive](#) ]