Cryptology ePrint Archive: Report 2011/641

Collision for 75-step SHA-1: Intensive Parallelization with GPU

E.A. Grechnikov and A.V. Adinetz

Abstract: We present a brief report on the collision search for the reduced SHA-1. With a few improvements to our previous work, directed at efficient parallelization on a GPU cluster, we managed to construct a new collision for 75-step reduced SHA-1 hash function.

Category / Keywords: hash functions, SHA-1, collisions, characteristics, GPU

Date: received 29 Nov 2011

Contact author: grechnik at mccme ru