Cryptology ePrint Archive: Report 2011/261

OBSERVATION: An explicit form for a class of second preimages for any message M for the SHA-3 candidate Keccak

Danilo Gligoroski and Rune Steinsmo Ødeård and Rune Erlend Jensen

Abstract: In this short note we give an observation about the SHA- 3 candidate Keccak[r,c,d], where the parameters r,c and d receive values from the formal proposal for the Keccak hash function (with the hash output of n = c bits). We show how an attacker that will spend a one-time effort to find a second preimage for the value z0 = Keccak[r, c, d](0^r) will actually get infinite number of second preimages for free, for any message M. Our observation is an adaptation of similar attacks that have been reported by Aumasson et.al and Ferguson et.al for the SHA-3 candidate CubeHash. By this observation we do not contradict security claims present in the official Keccak submission, but we allocate a property in the design of the function: we get an explicit form for a class of second preimages for any message M. As far as we know, this kind of property is not known neither for MD5, SHA-1, SHA-2 nor the other SHA-3 candidates.

Category / Keywords: hash functions, keccak, sha-3

Publication Info: NIST maling list

Date: received 25 May 2011

Contact author: rune odegard at q2s ntnu no