Collisions For SHA-3

Stefan Kölbl, Florian Mendel, Tomislav Nad, Martin Schläffer

Institute for Applied Information Processing and Communications (IAIK)
Graz University of Technology
Inffeldgasse 16a, A-8010 Graz, Austria

New SHA-3 Variants

At CT-RSA 2013, NIST announced the possible standardization of alternative SHA-3 variants with a:

- smaller capacity
  ($c = n$ instead of $c = 2n$ bits)
- smaller permutation
  (Keccak-f[800] instead of Keccak-f[1600])

Practical Collisions for these Variants

(on 24 rounds)

Practical Collisions for these Variants

(on ~~2~~4 rounds)

New Practical Collisions for these Variants

(on ~~2~~4 rounds)

New Practical Collisions for these Variants

(on ~~2~~4 rounds using a different technique)

New Practical Collisions for these Variants

(on ~~2~~4 rounds using a different technique)