Cube Test Analysis of the Statistical Behavior of CubeHash and Skein

http://www.firstlight.cn 2010-05-07

This work analyzes the statistical properties of the SHA-3 candidate cryptographic hash algorithms CubeHash and Skein to try to find nonrandom behavior. Cube tests were used to probe each algorithm's internal polynomial structure for a large number of choices of the polynomial input variables. The cube test data were calculated on a 40-core hybrid SMP cluster parallel computer. The cube test data were subjected to three statistical tests: balance, independence, and off-by-one. Although isolated statistical test failures were observed, the balance and off-by-one tests did not find nonrandom behavior overall in either CubeHash or Skein. However, the independence test did find nonrandom behavior overall in both CubeHash and Skein.

存档文本

北京雷速科技有限公司 版权所有 2003-2008 Email: leisun@firstlight.cn