Let , denote the null and alternative hypothesis and denote sample data.

Then ,

Assuming , and can be compared via the Bayes factor .

Note for independent data samples ,

or where is the Bayes factor based on sample . This allows the aggregation of multiple test results.

CryptoStat derives test data series from output data series partitions the data bit positions into disjoint bit groups and tests randomness on each bit group. The bit group values are integers in where is the bit group size.

: the big group values are uniformly distributed.

CryptoStat uses run tests and noncolliding block tests to test uniformity which can be turned into testing if a discrete random variable follows a certain distribution .

Through a Kolmogorov-Smirnov type operation, the test can be turned into a binomial test with successes out of trials.

CryptoStat uses to specify and derives the Bayes factor as .