Cryptology ePrint Archive: Report 2011/298

Local limit theorem for large deviations and statistical box-tests

Igor Semaev

Abstract: Let n particles be independently allocated into N boxes, where the l-th box appears with the probability a_l. Let μ_r be the number of boxes with exactly r particles and $\mu=[\mu_{r_1},\ldots, \mu_{r_m}]$. Asymptotical behavior of such random variables as N tends to infinity was studied by many authors. It was previously known that if Na_l are all upper bounded and n/N is upper and lower bounded by positive constants, then μ tends in distribution to a multivariate normal low. A stronger statement, namely a large deviation local limit theorem for μ under the same condition, is here proved. Also all cumulants of μ are proved to be $O(N)$.

Then we study the hypothesis testing that the box distribution is uniform, denoted h, with a recently introduced box-test. Its statistic is a quadratic form in variables $\mu-\mathbf{E}\mu(h)$. For a wide area of non-uniform a_l, an asymptotical relation for the power of the quadratic and linear box-tests, the statistics of the latter are linear functions of μ, is proved. In particular, the quadratic test asymptotically is at least as powerful as any of the linear box-tests, including the well-known empty-box test if μ_0 is in μ.

Category / Keywords: secret-key cryptography / hash functions

Date: received 6 Jun 2011

Contact author: igor at ii uib no