World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:9, No:03, 2015

On the Analysis of Pseudorandom Partial Quotient Sequences Generated from Continued Fractions

Authors : T. Padma, Jayashree S. Pillai

Abstract : Random entities are an essential component in any cryptographic application. The suitability of a number theory based novel pseudorandom sequence called Pseudorandom Partial Quotient Sequence (PPQS) generated from the continued fraction expansion of irrational numbers, in cryptographic applications, is analyzed in this paper. An approach to build the algorithm around a hard mathematical problem has been considered. The PQ sequence is tested for randomness and its suitability as a cryptographic key by performing randomness analysis, key sensitivity and key space analysis, precision analysis and evaluating the correlation properties is established.

Keywords : pseudorandom sequences, key sensitivity, correlation, security analysis, randomness analysis, sensitivity analysis
Conference Title : ICISET 2015 : International Conference on Information Science, Engineering and Technology
Conference Location : Singapore, Singapore
Conference Dates : March 29-30, 2015