THE UNIVERSITY OF HONG KONG

Institute of Mathematical Research
Department of Mathematics

Number Theory Seminar

Pseudorandom Vectors Generation Using Elliptic Curves Over Finite Fields

Professor Chung Pang MOK
Soochow University

Abstract

Using the arithmetic of elliptic curves over finite fields, we present an algorithm for the efficient generation of sequence of uniform pseudorandom vectors in high dimension with long period, that simulates sample sequence of a sequence of independent identically distributed random variables, with values in the hypercube $[0,1]^d$ with uniform distribution. We illustrate the use of these pseudorandom vectors with Monte Carlo integration.

Date:	January 3, 2023 (Tuesday)
Time:	3:15 – 4:15pm
Venue:	Room 210, Run Run Shaw Bldg., HKU

All are welcome