G. Milton Wing Lecture Series Fall 2014

luction

745 4 2515

Lawrence Washington

9 5

8 7

Department of Mathematics University of Maryland www.math.umd. edu/~lcw/

Washington received his PhD from Princeton University in 1974 and was a Sloan Research Fellow in 1979–81. He has over 60 publications in the areas of number theory and cryptography, including five monographs, and has advised over 24 PhD students.

Cannonballs, Donuts, and Secrets: An Introduction to Elliptic Curve Cryptography Public Lecture

Tuesday, Sept. 30, 5-6:15 p.m. Hoyt Auditorium

Abstract: Elliptic curves have been around for centuries, but recently they have become very important in cryptography. I'll start with a light introduction to elliptic curves and then discuss some recent cryptographic applications.

Manipulating Encrypted Data

Wednesday, Oct. 1, 2–3 p.m. Gavett Hall, Room 202

How can we determine the fair selling price of a commodity, where the buyers and sellers submit their bidding strategies in encrypted form? How can someone search a database without revealing the subject of the search? Solutions to these problems belong to the developing field of performing mathematical operations on encrypted data. I'll discuss examples along with possible future developments.

The Mathematics behind Quantum Computing

Thursday, Oct. 2, 2–3 p.m. Gavett Hall, Room 202

Quantum computers, if ever built, will be able to factor integers and perform searches faster than conventional computers. In this talk, I'll ignore qubits and quantum gates and instead discuss the interesting mathematical ideas involved in these algorithms.

Lecture Series Sponsored by the Department of Mathematics



8

2

955

3