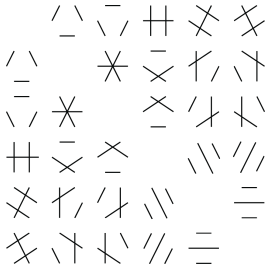
Mathematics Seminar



Rocky Mountain Algebraic Combinatorics Seminar

Post-Quantum Key Exchange from the LWE

Jintai Ding
University of Cincinnati

In this lecture, we present practical and provably secure (authenticated) key exchange protocol and password authenticated key exchange protocol, which are based on the learning with errors problems. These protocols are conceptually simple and have strong provable security properties. This type of new constructions were started in 2011-2012. These protocols are shown indeed practical. We will explain that all the existing LWE based key exchanges are variants of this fundamental design. In addition, we will explain some issues with key reuse and how to use the signal function invented for KE for authentication schemes.

Discrete Means: generalizing a theorem of Kolmogorov and social choice.

Curtis Bennett
Loyola-Marymount University

According to the U.S. Census Bureau, the “average" American household consists of 2.53 people and while this number is understood to be an average over all households in the U.S., it also leaves us unable to select an example of such a family. This is a problem of discrete means. In 1930, Kolmogorov gave an elegant axiomatization and classification of all means on the real numbers, and in this talk we will discuss Kolmogorov’s theorem and discuss different generalizations to his axioms when we restrict the mean to map on and into the integers. We will also discuss how the issues raised by discrete means confront us when we design social choice systems.

This talk will be accessible to a wide audience (including undergraduate mathematics majors).

Weber 223
4–6 pm
Friday, March 3, 2017
(Refreshments in Weber 117, 3:30–4 pm)
Colorado State University

This is a joint Denver U / UC Boulder / UC Denver / U of Wyoming / CSU seminar that meets biweekly.
Anyone interested is welcome to join us at a local restaurant for dinner after the talks.

Colorado State University
Department of Mathematics
Fort Collins, Colorado 80523