“Symbolic Computations and Post-Quantum Cryptography”
Online Seminar

Camilla Hollanti

(Aalto University, Finland)

“Confusing Eavesdroppers with Algebraic Number Theory.”

Mar 22, 12:00pm (New York Time).

Abstract:

The error probability of various coding schemes based on algebraic lattice constellations is evaluated. This is done by using the Dedekind zeta functions of the algebraic number fields involved in the lattice constructions. In particular, it is shown how to upper bound the error performance of a finite constellation on a Raighley fading channel and the probability of eavesdropper's correct decision on the wiretap channel. As a byproduct, an estimate of the number of elements with a certain algebraic norm is derived.

Next presentation: **Apr 05, 2012.** Continuous hard-to-invert functions based on tropical constructions
Sergey Nikolenko (Academic University, St.-Petersburg)

Algebraic Cryptography Center