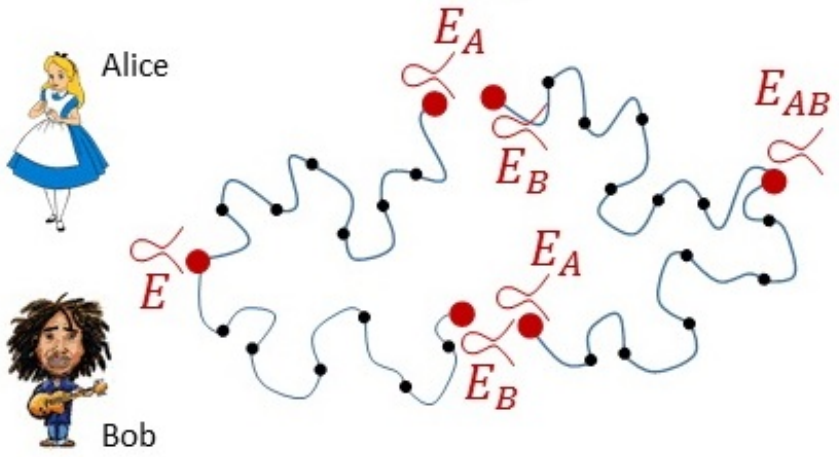
Cryptography from the Supersingular Isogeny Problem

Undergraduate Math Club
CORNELL UNIVERSITY



ABSTRACT

With the potential advent of quantum computers, cryptographers are searching for problems that are hard even if an adversary possesses a quantum computer. We'll analyze one such candidate, the supersingular isogeny problem on elliptic curves: given two (supersingular) elliptic curves, compute an isogeny between them. We'll review the literature for evidence that this problem is hard for quantum adversaries, and give an application to Diffie-Hellman key exchange.

APR 9 at 4:45pm

Malott 532 ⋆ Refreshments