abstract

Special Computer Science/Discrete Mathematics Lecture
Topic:

Speaker:

Affiliation:

Date:

Time/Room:

I'll describe a physical implementation of zero knowledge proofs whose goal is to verify that two physical objects are identical, without revealing any information about them. Our motivation is the task of verifying that an about-to-be-dismantled nuclear warhead is authentic without revealing its classified design. This is one of the technical hurdles that arises in implementing nuclear disarmament. I will not assume any background in either cryptography or nuclear disarmament.

Joint work with Alex Glaser and Robert Goldston from Princeton University and the Princeton Plasma Physics Laboratory.