CLAUDE CRÉPEAU, McGill University

Relativistic Commitments and Zero-Knowledge Proofs

We present techniques for zero-knowledge proofs of NP statements using very few relativistic commitments, making it possible for two synchronized verifiers, far enough from each other, to test two synchronized provers, close enough to the verifiers, in such a way that

* under the assumption that information cannot travel faster than the speed of light, only valid statements can be demonstrated by the provers (soundness)

* the answers obtained by the verifiers are useless to convince an off-line third party of the validity of the statement (zero-knowledge).

We achieve this by presenting a new interactive proof for NP languages that uses only 6 commitments at any point in the proof to be perfect zero-knowledge.

Joint work with Lucas Stinchcombe and Nan Yang