Classical proofs of quantum knowledge

INTRODUCTION
A proof of knowledge allows a prover machine to prove to a less knowledgeable or less powerful verifier that it ‘knows’ or ‘possesses’ some piece of secret information (for example, the password to an account). In this work, we study the setting where the verifier is entirely classical, but the prover is quantum, and where the ‘secret information’ (witness) is a quantum state.

A NEW DEFINITION
The usual formulation of a proof of classical knowledge has already been translated into the quantum setting in prior work. However, this usual formulation, where the knowledge extractor is required to use the prover as a black box, is inadequate in the setting with which we are concerned, because the black-box extractor would be in the position of trying to reconstruct a quantum state from the prover’s purely classical output, which may be as hard as state tomography. A new definition is therefore required, and our first contribution is to provide a workable definition for our setting with a non-black-box extractor that is allowed to access the prover’s circuit and internal state. We state our definition for several settings in which it may be useful.

SIMPLE PROPERTIES
One of the ways the new definition may prove useful is that it might provide a framework which can be studied fruitfully independently of specific protocols that instantiate it. We prove two examples of simple properties which the new definition has, including that nondestructive classical proofs of quantum knowledge are impossible, and that proofs of knowledge for hard-to-clone states can be used as (destructive) quantum money verification protocols.

EXAMPLE INSTANTIATIONS
We prove, using techniques based on nonlocal games, that two simple protocols inspired by classical private-key quantum money schemes are classical proofs of quantum knowledge under our definition. We also show that the classical verification protocol for QMA problem instances introduced by Mahadev in 2018 is a classical argument of quantum knowledge under our definition.