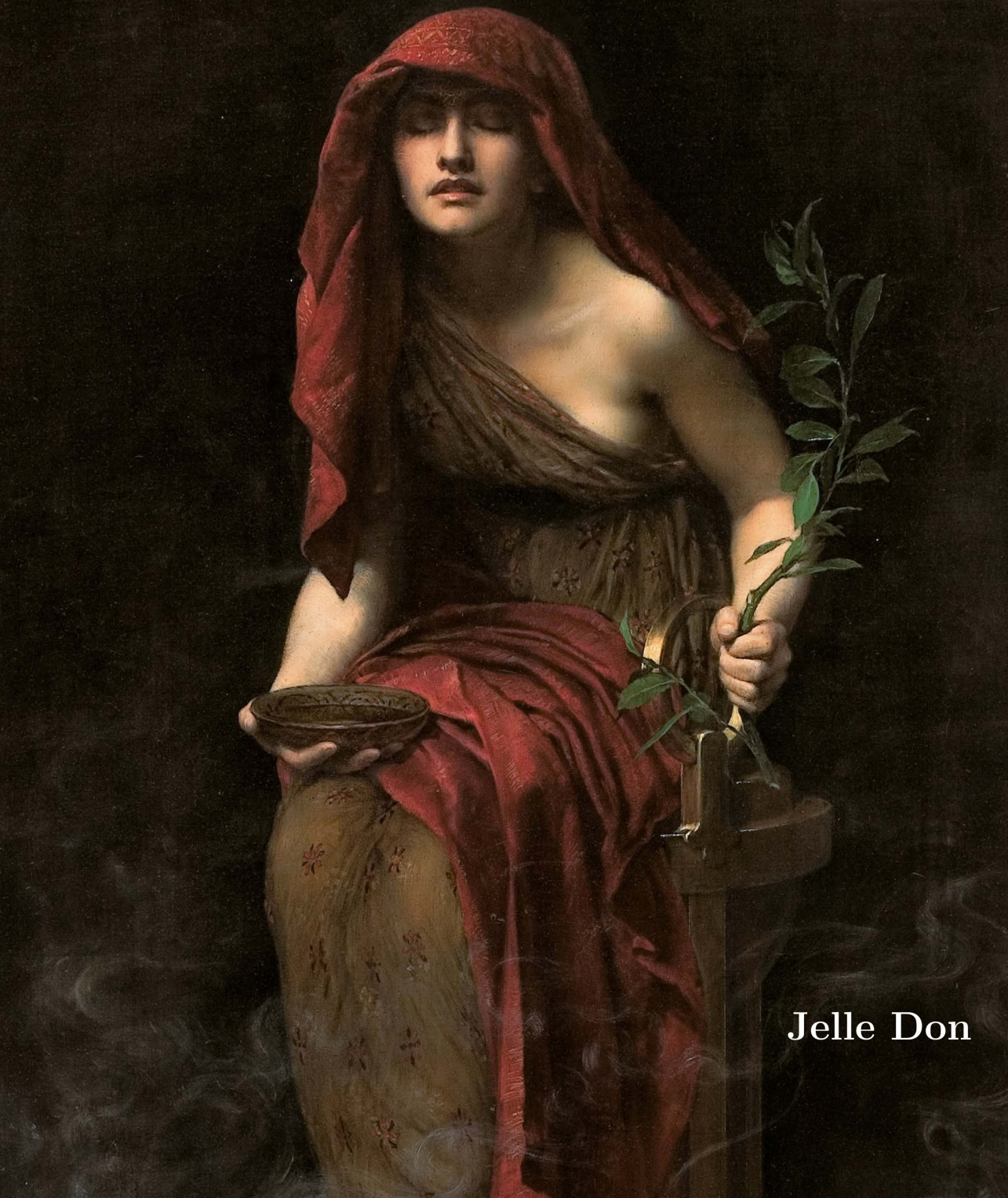
Knowledge extraction in the quantum random-oracle model

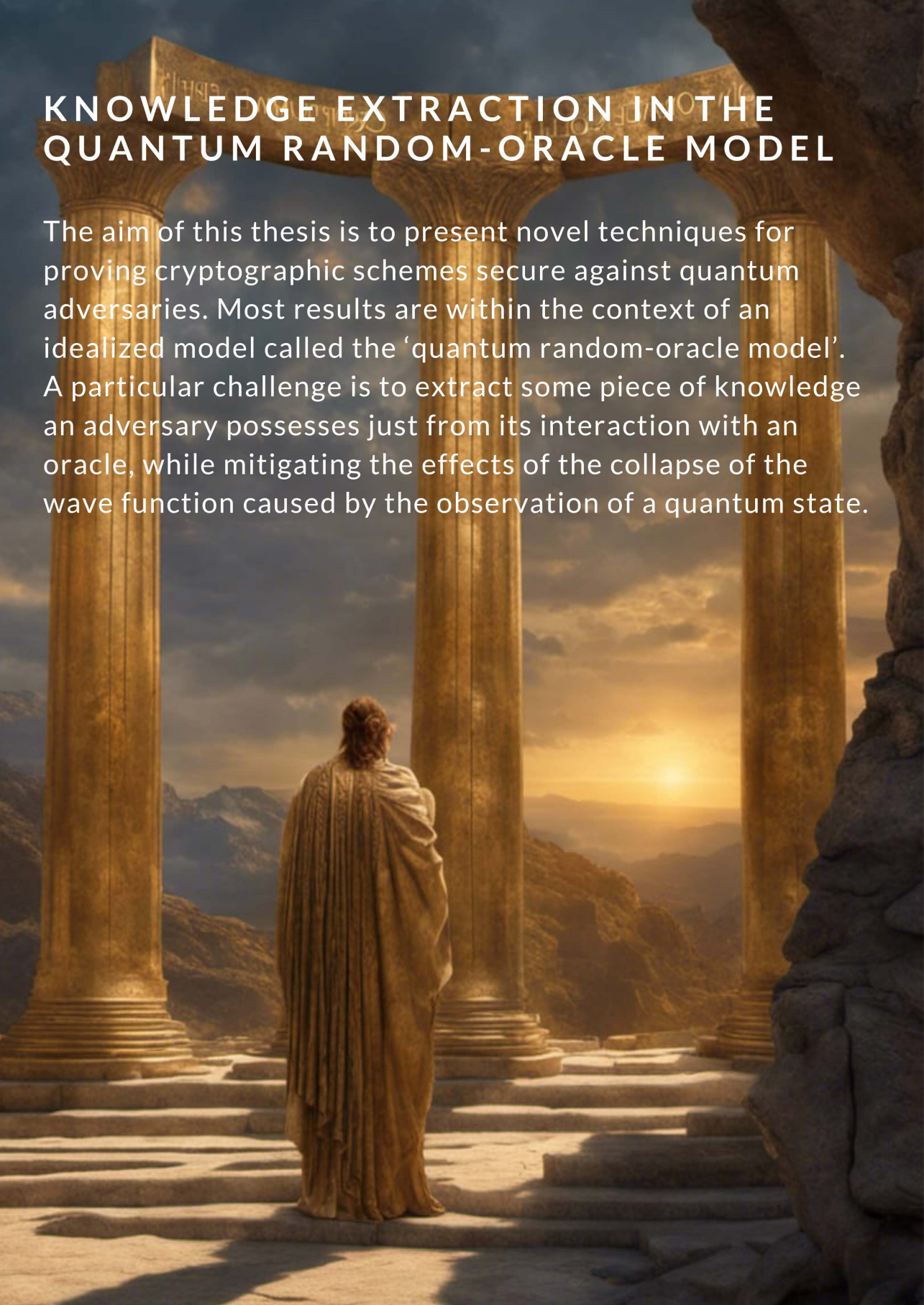
Don, J.W.

Knowledge Extraction

in the Quantum Random-Oracle Model



Jelle Don



KNOWLEDGE EXTRACTION IN THE QUANTUM RANDOM-ORACLE MODEL

The aim of this thesis is to present novel techniques for proving cryptographic schemes secure against quantum adversaries. Most results are within the context of an idealized model called the ‘quantum random-oracle model’. A particular challenge is to extract some piece of knowledge an adversary possesses just from its interaction with an oracle, while mitigating the effects of the collapse of the wave function caused by the observation of a quantum state.