Cílem této práce je implementovat softwarovou knihovnu, která umožní šifrovat interaktivní síťovou komunikaci pomocí kryptografického protokolu podobného SSL nebo TLS, jehož bezpečnost není ohrožena útočníkem vlastnícím kvantový počítač. Pro dosážení dané úrovně bezpečnosti výsledný software používá algoritmus na výměnu klíčů zvaný Supersingular Isogeny Diffie Hellman (SIDH). Software je poměrně jednoduchý, přenosný a nezávislý na specifikách konkrétního operačního systému. Práce také podává zhuštěný úvod do teorie, na které je algoritmus SIDH postaven, psaný pro cílovou skupinu studentů bakalářských a magisterských kurzů informatiky.