Práce se zaměřuje na teorii, která stojí za post-kvantovými algoritmy pro výměnu klíče CSIDH a SIDH. Předpokládáme základní znalost teorie eliptických křivek, ačkoliv na začátku práce představíme základní teorii eliptických křivek a izogenií. Poté si vybudujeme pomocí této teorie znalost okruhu endomorfizmů eliptických křivek. Dále představíme akci ideálů třídové grupy na eliptických křivkách nad komplexními čísly a následně vysvětlíme, jak se dá aplikovat na eliptické křivky nad konečnými tělesy. Nakonec představíme výše zmíněné algoritmy a vysvětlíme proč a jak fungují pomocí vybudované teorie a příkladů. Současně s tím stručně zmíníme bezpečností analýzu daných algoritmů. V celé práci také rozšíříme a upravíme důkazy důležitých tvrzení a zformulujeme některá vlastní.