**Abstract**

If large-scale quantum computers can be built, then we need to replace our most commonly used public key cryptosystems with post-quantum public key cryptosystems. These are the public key cryptosystems that are believed to remain secure even if large-scale quantum computers can be built. One relatively recent proposal for such a cryptosystem is the Supersingular isogeny Diffie-Hellman (SIDH) key exchange by Jao and De Feo. The purpose of this thesis is to explain the theoretical background of SIDH and to evaluate the current status of the cryptosystem. Along the way we will discuss how the isogenies in SIDH give rise to non-backtracking walks in supersingular isogeny graphs and we perform simulations in order to study the behaviour of these walks. To our knowledge such simulations have not been documented elsewhere in the literature about SIDH. We also study a simple reduction between two computational problems related to SIDH on supersingular isogeny graphs. A very similar reduction was recently mentioned in independent work by Galbraith and Vercauteren. While studying the implementation status of SIDH we describe a KEM built on SIDH that is IND-CCA2 secure in the random oracle model. To our knowledge, in doing so we answer an open question posed by Kirkwood et al. in the context of SIDH. Finally we give theoretical estimates of computational work, memory usage and key sizes in different variants of SIDH as functions of the quantum security level. This is straightforward thanks to analyses by earlier authors in work on SIDH.