終了年月：2020 年 3 月
専攻名：複雑理工学
氏名：郝 海萍（Hao Haiping）
学生証番号：47-186104
指導教員氏名：郡 宏
指導教員役職：教授
論文題目：複数人鍵共有プロトコル SIBD の実装
キーワード：
耐量子暗号方式，超特異楕円曲線，同種，SIDH 鍵共有方式，SIBD 鍵共有方式
概要：
Diffie-Hellman 方式は二者間鍵共有のための基本的なプロトコルである．
2011 年，Jao らは超特異楕円曲線の間の同種を計算することの難しさに基づく耐量子鍵共有方式（SIDH）を提案した．2018 年，Furukawa らは SIDH 鍵共有プロトコルを拡張し，超特異楕円曲線の間の同種写像を利用した複数人鍵共有方式（SIBD）を提案した．この方式は，SIDH 鍵共有方式と Burmester-Desmedt 鍵共有方式を組み合わせることにより，耐量子性を持つとともに，通信のラウンド数を減らしたn-party 2-round 鍵共有方式である．
しかし，Furukawa らは実装結果は記述しておらず，鍵共有に要する計算時間などは不明であった．
我々は，SIBD プロトコルの実装を行い，十分高速に鍵共有が可能であることを確認した．