同種写像問題に基づく暗号技術

Cryptographic Techniques Based on the Isogeny Problem

松浦栄亮・システム分科会・情報セキュリティ大学院大学

1年次の進捗
- 同種写像についての数学的な背景の理解
- SIDH・CSIDH鍵共有, SQIsign署名の学習

2年次の予定
- 先行研究の調査を基に手法の提案・仮説の証明
- 計算量や安全性の評価

期待される成果（新規性）
- 同種写像と量子マネーの新たな融合による暗号技術の発展
- 量子コンピュータ時代に適応可能な新たなプロトコルの提案

2, 3	4	5	6	7	8	9	10	11	12	1	2
		輪講発表				中間発表					修士発表
基礎の整理 ・CSIDH ・SQIsign	先行研究調査 ・量子マネー ・同種写像		手法の提案・仮説の証明				内容の改善・発展 ・中間発表の改善点		修論準備		