講演者　　：桂 利行（東京大学大学院数理科学研究科・特任教授）
講演タイトル：Decomposed Richelot isogenies of curves of genus 3
アブストラクト：
標数 p が 2 ではない代数的閉体 k 上の種数 3 の非特異射影代数曲線に対し、その Jacobian 多様体が分解する Richelot isogeny をもつための必要十分条件を与え、分解する場合の代数曲線の構造を明らかにする。

講演者　　：神戸 祐太（立教大学理学部数学科/すうがくぶんか・講師）
講演タイトル：Solving the constructive Deuring correspondence via the Kohel-Lauter-Petit-Tignol algorithm
アブストラクト：
素数 p について、E_0 を F_{pˆ2} 上の超特異楕円曲線とする。 このとき、 Deuring 対応と呼ばれる End(E_0)の左イデアル I と E_0 を定義域とする同種写像 ¥phi:E_0 → E_I の間の一対一対応が存在する。 タイトルにある構成的 Deuring 対応問題とは、与えられた左イデアル I に対して E_I の j-不変量を計算する問題である。
本講演では構成的 Deuring 対応問題の求解法として Kohel-Lauter-Petit-Tignol アルゴリズム（KLPT アルゴリズム）を用いた方法を紹介し、実際に 25 ビット程度の標数における計算例の紹介やデモンストレーションを行う。

講演者　　：小寺 健太（大阪大学大学院工学研究科/三菱電機情報技術総合研究所・研究員）
講演タイトル：同種写像暗号 CSIDH の高速化に向けた効率的な同種写像計算
アブストラクト：
近年、耐量子暗号と呼ばれる、量子計算機を用いた攻撃に耐えうる暗号の研究が盛んに行われている。耐量子暗号の候補の 1 つの同種写像暗号がある。例えば 2018 年に Castryck らによって提案された CSIDH は、公開鍵長が非常に短いという特長がある一方で実行時間に課題がある。そこで本研究では CSIDH の主要な計算である同種写像の計算手法を改良し、高速化を目指す。
一般に同種写像の計算には核に含まれる点の座標が必要となる。既存の手法では加法公式を用いて核の点のうち約半数の座標を計算していた。本研究では加法公式を元に核の点における関係式を導出し、より少数の点の座標から同種写像を計算する手法を提案する。