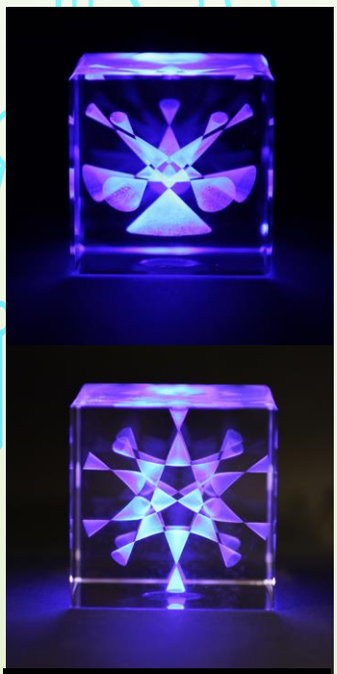
情報数学セミナー（FoPM講演会）

テーマ：ポスト量子暗号の理論



木曜5限 16:50～18:35
東京大学駒場キャンパス
オンライン（Zoom）

量子コンピュータが開発されると現在用いられているRSA暗号などの公開鍵暗号は解読されるため、耐量子計算機暗号が開発されつつあります。その有力な２つの候補について現状を解説していただきます。

（１）講師：　草川　恵太　氏（NTT）
タイトル：**格子暗号理論とその応用**
日時：　２０２２年１月１３日（木）16:50～18:35
場所：　　オンライン（Zoom）

（２）講師：　相川　勇輔　氏（三菱電機）
タイトル：超特異楕円曲線を用いた耐量子計算機暗号の数理とその進展
日時：　２０２２年１月２７日（木）16:50～18:35
場所：　　オンライン（Zoom）

申し込みURL：
https://docs.google.com/forms/d/1WLEbsA2aQTXgdE2ynrumJOG-Z4AVWqcOLC-z42B4nPY

（詳細はSeminar Information（情報数学セミナー）にあります）

東京大学大学院数理科学研究科
Graduate School of Mathematical Sciences, THE UNIVERSITY OF TOKYO

WISE Program FoPM

https://www.ms.u-tokyo.ac.jp/activity/seminar.html