ミニワークショップ 「理論・計算数学との融合アプローチによる 暗号学の新展開」

開催時期: 2020-02-04 10:30 - 2020-02-04 16:30

場所: 九州大学伊都キャンパス・ウエスト1 号館C棟 5 階中講義室（W1-C-512）

ミニワークショップ**「理論・計算数学との融合アプローチによる暗号学の新展開」**
※ この研究集会はマス・フォア・インダストリ研究所共同利用・共同研究の公開プログラムです.

【開催日時】
2020年2月4日(火)

【開催場所】
九州大学 伊都キャンパス ウエスト1号館 C棟 5階 中講義室(W1-C-512)

【プログラム】2020 年2 月4 日(火)
(全3講演)

10:30-11:00 池松泰彦(九州大学マス・フォア・インダストリ研究所)
オープニングトーク

11:10-12:10 横山俊一(首都大学東京)
Advanced topics and new features in Magma

12:10-13:40 昼休憩

13:40-14:40 Mehdi Tibouchi (NTT Secure Platform Laboratories)
Lattice-based signatures and timing leakage: attacks and countermeasures

14:50-15:50 山口純平(富士通研究所)
アニーリング計算を用いた次世代暗号の解読

16:00-16:30 議論

16:30 閉会

アブストラクト

※研究実施期間：2020年2月3日（月）-2月7日（金）
※2月4日（火）のみ公開