
電子情報通信学会東北支部講演会

「格子最短ベクトル問題における遺伝的アルゴリズムについて」

講演者：深瀬 道晴　氏（東北学院大学）

■開催日：2023 年 2 月 24 日（金）　13:30～14:30

■会場：東北学院大学　多賀城キャンパス　2 号館 2 階 2201 教室
　　および、ZOOM によるハイブリッド開催

■講演タイトル：「格子最短ベクトル問題における遺伝的アルゴリズムについて」

■講師：　深瀬 道晴　氏（東北学院大学）

■講演概要：

米国国立標準技術研究所 NIST による耐量子計算機暗号標準化候補の一つである格子暗号の安全性評価の道具として、格子最短ベクトル問題（SVP）のアルゴリズムがあります。SVP アルゴリズムはいくつかに分類され、最も高速なものが Sieving、その他に BKZ、ENUM、Sampling などがあります。これらの主な分類に含まれないものとして、遺伝的アルゴリズム（GA）があります。GA には、低メモリ消費などいくつか良い性質があります。

本講演では、SVP における GA の手法を紹介します。また、講演者による SVP における GA の高速化の研究と今後の展望について説明します。

■主催：電子情報通信学会東北支部

■共催：東北学院大学工学会

■参加費：無料

■事前申込：要（以下のフォームにて参加登録をお願いします）
　https://forms.gle/w12ib158hJAtwqr87

■参加定員：現地会場参加 15 名、Zoom 参加 100 名

■申込期限：2023 年 2 月 20 日（月）
　　※但し、参加定員を超える場合は期限前に受付を終了する場合があります。

■問合せ先：吉川 英機（東北学院大学）
　　hyoshi[at]mail.tohoku-gakuin.ac.jp

　　※メール送信の際は[at]を@に変換してお送りください。