# 第 10 回有限体理論とその擬似乱数系列生成への応用ワークショップ開催報告

開催場所：昼神空間（現地/オンライン）
開催期間：2024 年 9 月 16 日（月）～17 日（火）

実行委員長　野上保之（岡山大学）

2024 年 9 月 16 日（月）から 17 日（火）の 2 日間、第 10 回有限体理論とその擬似乱数系列生成への応用ワークショップ（FFTPRS 2024）を開催しました。このワークショップは、情報理論とその応用シンポジウム（SITA）あるいは、International Symposium on Information Theory and Its Applications（ISTA)などにおいて、日頃より有限体理論とその擬似乱数系列生成への応用に関連する研究の成果発表をしている研究者、またそのようなテーマに興味を持っている研究者が一堂に会し、日々の研究活動の中で得られた成果の報告をはじめ、疑問に思っている事柄、あるいは個人的な興味から深く掘り下げているテーマなどを、十分な時間をかけてお互いに紹介、共有し、密な議論を展開するための場を提供することを意図したワークショップです。

世界的に流行した新型コロナウイルス感染症へ配慮し、一時全面オンラインでの開催となりましたが、オンライン参加の利便性もあり現地での様子をオンライン配信しつつ開催しています。今回は 10 周年の記念大会であり、本ワークショップの発起人らを繋ぐきっかけとなった信州を開催地とし，信州大学の柴田先生に会場手配等をご尽力いただき開催することができました。この場をお借りして御礼を申し上げます。

さて、ワークショップですが、16 名（一般 10 名、学生 6 名）の参加があり、7 件の一般講演の発表がありました。いずれの発表においても、熱心かつ有意義なディスカッションが行われました。

発表者と発表題目は以下の通りです（敬称略)。

一般講演 1）髙市康平（九州工業大学）
「ローレンツ方程式を用いた動的ランダム鍵生成器の整数化に関する研究」

一般講演 2）武内友希（岡山大学）
「Grostl の概念を基にした可変長ハッシュの提案」

一般講演 3）小嶋徹也（東京工業高等専門学校）
「有限体上のアダマール型行列を愛でる」

一般講演 4）安部泰志（北九州市立大学）
「Jacobian 座標の 3 倍点公式を利用した Joye's 3-ary Ladder アルゴリズムの一考察 」

一般講演 5) LI KEXIN（岡山大学）
「An Implementation of AES Algorithm using Composite Field on FPGA」

一般講演 6）本多華（九州工業大学）
「整数上のロジスティック写像における制御変数の値域による出力値系列に関する考察」

一般講演 7）宮﨑武（九州情報大学）

「外壁の無い確定的な迷路法による擬似乱数生成法に関する一考察」

参加者同士で忌憚のない活発な議論や交流の場を設けることができた有意義なワークショップとなりました。なお、予稿集は PDF として参加者各位へ配布しております。


図 1　発表の様子