乱数の発生法・性能評価法の開発と応用

１．代表研究者名

［統計数理研究所］田村義保

２．共同研究者

［統計数理研究所］伊庭幸人、柳本武美

［理化学研究所］泰地真弘人（統計数理研究所客員）

［国立極地研究所］岡田雅樹

［国立情報学研究所］三浦謙一、松本啓史

３．平成 17 年度の研究実績報告

3-1. 研究目標

物理乱数を核として、擬似乱数を含めた新しい乱数の発生法、その応用と評価について研究することを目的とする。物理乱数は擬似乱数とは異なり、周期が無く、そのほかの性質についても信頼性が高い。高精度の乱数としての物理乱数の研究・開発・実用化はそれ自身重要であるが、近年の情報技術の進展によって、あらたな用途が期待されている。特に重要なのは（１）並列計算における利点、（２）セキュリティ技術における利点、である。（１）についていえば、並列計算機で擬似乱数を使う場合においては、異なった CPU で使用する乱数間に相関性が無いことを確かめてから利用するべきであるが、相関性についての検証は必ずしも容易ではない。物理乱数については、複数の CPU で同時に使用しても相関性はないことが保証されており、並列計算のために安心して用いることができる。また（２）については、擬似乱数の場合、乱数の種(seed)を解読されると、その後発生される列を予測されてしまうという問題がある。これに対して、物理乱数は発生方式がわかっていても将来の系列を予測することは困難であり、セキュリティ的に安全であるといえる。物理乱数発生方法の再検討し、高精度な物理乱数を高速に発生させるための方法を確立すること、及び、物理乱数の利用を促進するために、物理乱数発生装置の小型化することを主な目標とした。

3-2. H17 年度の研究成果（概要）

小型であるが高速（24MB/秒）の USB 接続可能な装置を FDK と共同で開発した。パソコンで、シミュレーションを行う研究者が急増しているが、市販されている USB 接続式の装置は 30KB/秒程度の速度しかなく、擬似乱数の代わりに使えるようなものではない。24MB/秒程度になると、擬似乱数発生速度の 1/5 から 1/2 倍程度となり、精度を重視する研究者には利用していただけるものと考る。また、泰地客員教授の協力を得て、東京エレクトロンデバイスと共同で、乱数発生源の見直しのためのテストボードを作成した。

理論面においては、定期的に会合を持ち、物理乱数の応用面と擬似乱数の最新の発展について議論した。メンバーの三浦氏は新しい擬似乱数発生方法（MRG 法）と並列乱数発生法についての研究を発表し、また、小柴埼玉大助教授には暗号用乱数についてのレビュー

をお願いした。一研究所のレベルを超えて、機構の研究者に外部の研究者も加えて議論を重ねることにより、並列計算への応用とセキュリティ・暗号関係への応用を中心に、統計科学・情報学に幅広く貢献できる方向性が見いだすことができた。

3-3. 今後の展開

泰地客員教授と共同して高速の乱数発生ボードのテスト版を開発する。速度を犠牲にすれば、特質を良くすることは容易であるが、高速性を保ちつつ、特質も良くすることは難しい問題である。この困難な問題を解決するためには、乱数ボード開発の経験を有した研究者が共同して研究を行うことが必須である。泰地氏と共同で行った平成 17 年度の研究成果を活かし、さらに、東芝の乱数ボードの開発者である小野寺氏の協力を得て PCI-X 仕様のボードで 200MB/秒以上の発生速度を有する製品の開発することを最終目標としたい。

理論面・応用面では、情報研、極地研の研究者と協力して、擬似乱数を並列に発生させる有効な方法について研究し、そのアルゴリズムを公表するとともに、並列に発生した乱数の独立性を、物理乱数を用いた場合との結果の比較により、検定する方法の研究も行って行きたい。セキュリティへの応用に関しては、暗号用乱数の発生方法及び暗号用乱数としての物理乱数の有用性についての研究を行う。また、量子論的な乱数や情報圧縮、非線形モデルを用いた検定法についても引き続き研究したい。

3-4. 成果発表及び執筆論文

- 田村 義保、小野寺 徹、中畑 昌也、清水 隆邦、“日本における物理乱数発生装置の現状”日本統計学会誌・和文誌、第 35 巻、シリーズ J、第 2 号、210-212、2006
- 田村 義保、“物理乱数と擬似乱数”、大分統計談話会・第 32 回大会、
  富士通大分システムラボラトリ、2005 年 10 月 7 日
- 田村 義保、“物理乱数の生成法”、ISM オープンフォーラム、
  統計数理研究所講堂、2006 年 2 月 17 日
- 泰地 真弘人、“科学計算専用ハードウェア～専用計算機、物理乱数”
  ISM オープンフォーラム、統計数理研究所講堂、2006 年 2 月 17 日