2025 年 12 月 1 日

電気・電子情報工学専攻	学籍番号	M223233
申請者氏名	工藤 典佑	

指導教員氏名	市川 周一

論　文　要　旨（修士）

論文題目	Generative Adversarial Network と Linear Feedback Shift Register を用いた乱数生成手法

乱数生成は，特にセキュリティ技術・暗号化技術・シミュレーションなどの分野において極めて重要である．乱数には大きく 2 種類が存在する．1 つは真性乱数（TRN; True Random Number）で，物理現象を利用するため将来値の予測は困難だが，専用ハードウェアが必要である．もう 1 つは疑似乱数（PRN; Pseudo Random Number）で，決定的アルゴリズムで生成されるため高速に生成できるが，アルゴリズムや内部状態が推測された場合に予測が可能になる．

これらに加えて，PRN を拡張した Unpredictable Random Number（URN） と呼ばれる乱数が提案されている．URN は内部的には決定的アルゴリズムで動作するものの，外部エントロピー源を取り込むことで実質的に予測困難な乱数列を生成する．URN は TRN に近い性質を持ちながらも専用ハードウェアを必要としない．千葉と市川 (2023) は風向データを用いて LFSR のサンプリング間隔に揺らぎを付与する URN 生成法を提案したが，風向データは 1 時間に 1 サンプルしか得られないため，生成速度に制限があった．

本研究では，エントロピー源として気温データを用い，URN を生成する．使用したのは金沢市の 1 時間単位の気温観測データ 3 年間分である．日時と気温（0.1 ℃刻み）からなる時系列データを，その特性に合わせて前処理及び離散化し，LFSR のサンプリング間隔を変動させるために用いた．評価には DIEHARD テスト及び NIST テストを用いた．

DIEHARD テストでは，気温データの小数部分を利用する手法（Method2）及び気温変化量を利用する手法（Method3）において，32-bit LFSR の基本サンプリング間隔が 32 以上の条件で良好な結果が得られた．一方，より厳格な NIST テストは 32-bit LFSR では合格できなかった.，48-bit 及び 64-bit の LFSR を用いた場合，気温変化量を用いる手法（Method3-Pattern1-mod4，Method3-Pattern2）が，初期値やタップ設定を変更しても安定して合格した．

気温データの測定周期は 1 時間であり，風向データと変わらないので，エントロピー生成速度には依然として制約がある．そこで本研究では，気象データと類似した性質をもつデータ列を Generative Adversarial Networks（GAN） で生成した．GAN は，生成器（Generator）と識別器（Discriminator）が競合しながら学習を行うことで，高品質なデータを生成するモデルである．本研究では複数のモデルを構築・比較し，最終的に最も高い生成精度が得られた RNN-CGAN（Recurrent Neural Networks Conditional GAN） を採用した．学習には過去 12 年分の気温データを使用し，生成された 3 年分の疑似気象データを用いて URN を生成した．

その結果，DIEHARD テストにおいては実気温データと同様に Method2 及び Method3 を用いた場合に良好な結果が得られた．NIST テストでも全体として類似した傾向が見られ，特に Method2，Method3-Pattern2 を用いた場合は 48-bit 及び 64-bit LFSR の両方で安定して合格することを確認した．

今後の課題としては，気温データが持つ連続性や周期性をさらに除去し，より高いランダム性を有する揺らぎを抽出する前処理手法の検討，及び GAN による疑似気象データ生成の精度向上が挙げられる．