令和３（２０２１）年度　卒業研究報告書概要

課程，学籍番号，氏名	課程：電気・電子情報工学課程，学籍番号：B203238，氏名：千葉　歩武
工学分野名：情報通信システム	指導教員名：市川　周一

題　　目：和

気象データと LFSR による乱数生成手法の検討

（英　A Study on Random Number Generation from Weather Data and LFSR　）

Abstract

The purpose of this study is to design a TRN (True Random Number) that utilizes natural phenomena as entropy sources. This study examines weather data which has the highest entropy. In this study, random numbers are generated by combining wind direction data and the method proposed by Kamogari et al. (2021) . Kamogari et al. simulated a fluctuation in the sampling cycle of 32-bit LFSR (Linear Feedback Shift Register) . This study examines the LFSR whose sampling cycle is determined by the wind direction data. The derived random numbers were confirmed to pass the NIST test under the appropriate conditions. The results indicate that wind direction data can be used as an entropy source to generate TRN by adopting appropriate hash function.

概　　要

乱数には，物理現象を用いて生成される真性乱数（True Random Number: TRN）と数値的処理で生成される疑似乱数（Pseudo Random Number: PRN）がある．乱数生成器はそれぞれ真性乱数生成器(TRN Generator: TRNG)，疑似乱数生成器（PRN Generator: PRNG）とよばれる．また，PRNG を拡張した URNG (Unpredictable Random Number Generator) と呼ばれる RNG も存在する．正岡ら(2021)は URNG を実現するために線形帰還シフトレジスタ（Linear Feedback Shift Register: LFSR）回路をプロセッサに実装した．鴨狩ら(2021)は，正岡らが扱った LFSR の仕様（タップ数・LFSR のビット数）が限定的であることやサンプリング周期の検討をしていないことを指摘した．これらを解決するためにシミュレーションを行い適切な LFSR の条件を絞り込んだ．また，サンプリング周期に揺らぎを与えるシミュレーションも同時に行い，揺らぎによって乱数品質が向上することを報告した．

本研究の目的は，自然現象をエントロピー源とした TRN の生成である．自然情報には気象データを利用した．データの要素は風向・風速に決め，データを 16 進数と 2 進数に変換しエントロピーを調べた．風向・風速ともに 9 割以上の相対エントロピーがあることが分かり，よりエントロピーが高かった風向データをエントロピー源とした．しかし，風向データだけではデータ量が少なく乱数性が低い．解決法として風向データと鴨狩らの手法を組み合わせ，32 ビット LFSR のサンプリング周期を風向データによって変化させることにより乱数を生成した．風向データの使い方として，ハッシュ関数の除算法と乗算法を利用した 4 つの方法（Method）を提案した．

乱数の評価は DIEHARD テストと NIST テストでおこなった．DIEHARD テストの結果から，基本周期 29 サイクル以上のときすべての Method で 18 テストほぼすべてが PASS もしくは WEAK になることが確認された．NIST テストでは基本周期 32 サイクルのとき，Method 3（乗算法で切り捨てられる小数部の下位 21 ビットをハッシュ値とする方法 ）と Method 4（乗算法によってハッシュ値を求める方法）の 2 つの Method で 15 テストすべてを PASS することが確認された．各 Method の揺らぎの大きさ（標準偏差）はほぼ同じであることから，Method 1, 2 と 3, 4 の差はハッシュ関数の性質によるものと考えられる．以上の結果より，適切なハッシュ関数を使用することにより，風向データをエントロピー源として TRN を生成することができると考えられる．

本研究では風向データのみを取り扱ったが，その他の自然情報や社会情報からも乱数生成が可能であると考えられる．今後の課題は，それらを利用した乱数生成手法を調査することである．

発表する際の課程を記入　　電気・電子情報工学　課程　　発表番号　46

（学籍が他課程所属の学生も発表する課程を記入すること）