令和４（２０２２）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：B213262　　，氏名：別役 拓哉
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 を用いた URNG の改良

（英　　Improvement of the URNG using weather data and LFSR　　）

Abstract

Chiba et al. proposed a random number generation method using 32-bit LFSR and weather data. They used wind direction data as meteorological data and succeeded in improving the random number quality by adding fluctuations to the LFSR. Chiba et al. proposed four different methods and considered that the quality of random numbers could be improved by using more complex hash functions for the fluctuations. However, the method of Chiba et al. requires a large amount of meteorological data. In this study, we propose and evaluate a method to reduce the amount of weather data by employing a new hash function.

The method of Chiba et al. requires at least two years of meteorological data, but by employing MD5 and SHA256, it passes the randomness test with only one year of data. This study revealed that the order of meteorological data has a significant impact on random number quality. By using the new order of data, the necessary data was reduced compared to that of Chiba et al. Weather data is constantly being updated. We evaluated the random number quality when weather data is updated in three stages of random number generation: 10, 100, and 500.

概　　要

多くのセキュリティ技術において乱数は重要な役割を果たしている．乱数には TRN (True Random Number) と PRN (Pseudo Random Number)がある．PRN を拡張したものとして URN (Unpredictable Random Number)があり，実質的に予測不可能な乱数を生成する事が可能である．正岡らは LFSR (Linear Feedback Shift Register)を組込みシステムに実装し，LFSR の下位 32 ビットを専用レジスタから読み出すことによって URN を生成する手法を提案した．鴨狩らは LFSR のビット数・サンプリング周期・帰還多項式を変化させることで正岡らの問題を解決し，高品質の乱数を生成する手法を提案した．千葉らは 32 ビット LFSR と，気象データを用いた乱数生成手法を提案した．気象データとして風向データを使用し，LFSR に揺らぎを与えることで乱数品質を向上させることに成功している．千葉らは 4 種類の手法を提案し，揺らぎに使用するハッシュ関数をより複雑にすることで乱数品質を向上させることができると考えた．しかし千葉らの手法では，必要な気象データ量が大きいという問題がある．

本研究では，新たなハッシュ関数を採用することにより，必要な気象データの量を削減する手法を提案し，評価を行う．ハッシュ関数には MD5 と SHA256 を用い，千葉らの手法と比較した．また気象データの使用方法と更新手法を提案する．評価方法には DIEHARD テストを用いて乱数品質の評価を行った．

千葉らの手法では最低でも 2 年分の気象データが必要であったが，MD5 と SHA256 を採用することにより 1 年分で乱数検定に合格することが確認できた．気象データの並べ方が乱数品質に影響する可能性を考え，2 種類の検証を行った．1 つ目は 1 年単位で積み重ねる並べ方であり，2 つ目は各地点を 1 つずつ交互に並べる方法である．気象データの順番により乱数品質に大きな影響があることが検証で判明した．千葉らの手法で最低限必要な年数を減らすことに成功した．

気象データは常に更新され続けるデータである．乱数生成時に 10，100，500 の 3 段階に分けて気象データを更新した場合の乱数品質を評価した．気象データを更新することで乱数品質に大きな変化はなく，DIEHARD テストに合格することは可能であった．

乱数品質を維持し，最低量の気象データで乱数を生成できることを確認できたが，実際のシステムで運用した際に乱数品質が保たれるかについては今後の課題である．

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　79

（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）