氏　　名	MD ARSHAD ALI
授与した学位	博　士
専攻分野の名称	工　学
学位授与番号	博甲第６０５０号
学位授与の日付	２０１９年　９月２５日
学位授与の要件	自然科学研究科　産業創成工学専攻 （学位規則第４条第１項該当）
学位論文の題目	A Study of Pseudo Random Sequence Generated by Cascaded Trace and Legendre Symbol Over Finite Field （連結したトレース計算とルジャンドルシンボルを用いて生成される有限体上の擬似乱数系列に関する研究）
論文審査委員	教授　野上保之　　教授　豊田啓孝　　准教授　栗林　稔

学位論文内容の概要

This dissertation presents a pseudo random sequence which generated by cascaded trace function and Legendre symbol over finite field. There are several applications of pseudo random numbers in enormous applications in information security, especially cryptography. Such applications choose random sequences having unpredictability and good statistical properties such as long period, low correlation (both autocorrelation and cross-correlation), high linear complexity, and uniform distribution of bit patterns. In addition, many statistical tests (such as NIST statistical test suite) are available to judge the randomness in pseudo random sequence. This thesis theoretically proves period, autocorrelation, cross-correlation, and distribution of bit pattern properties of the proposed pseudo random sequence. Furthermore, all the above-mentioned properties are experimentally observed along with fair comparison with related works are also introduced. This dissertation is organized as follows:

Chapter 1 introduces the background, motivation, and contributions of the study in this thesis.

Chapter 2 describes and defines the fundamental mathematical concepts behind the generation of a pseudo random sequence. Additionally, a pseudo random sequence also introduces along with its properties.

Chapter 3 introduces the proposed pseudo random sequence along with the NTU (Nogami-Tada-Uehara) sequence.

Chapter 4 contains a discussion of period, autocorrelation, and cross-correlation properties regarding a pseudo random sequence (including a binary and multi-value sequence) defined over the sub extension field. These properties are theoretically shown along with experimental results.

Chapter 5 focuses on the distribution of bit pattern property in a binary sequence. This property is theoretically proven along with experimental observation. In addition, fair comparison with related works are also introduces.

Chapter 6 explains the linear complexity and NIST statistical test experimentally.

Chapter 7 presents how same binary sequence can be generated by using an irreducible polynomial instead of a primitive polynomial, whereas, primitive polynomial is a foremost requirement during the proposed sequence generation procedure, and it is a time-consuming operation for finding such polynomial. The relationship between the irreducible and generated sequences are explained both theoretically and experimentally.

Finally, Chapter 8 concludes the dissertation along with an outline of the future works.

論文審査結果の要旨

本論文では，近年の情報セキュリティ技術を実現する上で必要不可欠である擬似乱数の生成法に関するものであり，新しい生成法の提案と性能評価を行っている。セキュリティを観点とする乱数の評価において，様々な着目点がある中で，とくに周期，自己・相互相関，線形複雑度（Linear Complexity），およびビット分布の一様性について議論を展開している。

まず，擬似乱数の生成法として広く知られているM系列およびLegendre系列に注目し，それぞれの特徴をセキュリティの観点から長所・短所として整理している。そして，それぞれの長所だけを引き継ぐような擬似乱数の生成法を開発することを目標とし，有限体上の部分体構造を利用したトレース関数（Cascaded Trace）およびLegendre記号を定義し，それらを組み合わせる生成法を考案した。この生成法は，先行研究であるNTU系列と呼ばれる擬似乱数生成法を理論的に包含し，加えてNTU系列がもっていた幾らかの問題点を改善するものとなっている。具体的には，NTU系列の相関特性およびビット分布の一様性について改善が図られており，前者については大きなピーク値を複数もたないように，後者については一様性がさらに増すように改善されている。特筆すべき点は，このような性質について理論的な証明を与えている点であり，その上で乱数の性能を評価する世界標準のプログラムであるNISTテストをクリアする擬似乱数系列を生成できていることである。

以上のような成果は，申請者を筆頭著者とするジャーナル論文5本，国際会議論文8本にまとめられており，さらに申請者を共著者とする論文や国際会議発表も6本を数え，広く当該分野の研究者に認められているものである。本博士論文は，そのような複数の研究成果について整理して詳述されており，博士（工学）の称号を与えるとともに，早期修了するに相応しいものであると判断する。