PROPERTIES OF CRYPTOGRAPHIC PRIMITIVES:

INTEGER RECURRENCE RELATIONS & PERMUTATIONS

YOGESH KUMAR

DEPARTMENT OF MATHEMATICS
INDIAN INSTITUTE OF TECHNOLOGY DELHI

OCTOBER 2017

PROPERTIES OF CRYPTOGRAPHIC PRIMITIVES: INTEGER RECURRENCE RELATIONS & PERMUTATIONS

by

YOGESH KUMAR

Department of Mathematics

Submitted

in fulfillment of the requirements of the degree of Doctor of Philosophy

to the

Indian Institute of Technology Delhi
OCTOBER 2017

Dedicated to

My Family

Certificate

This is to certify that the thesis entitled **"Properties of Cryptographic Primitives: Integer Recurrence Relations & Permutations"** submitted by **Mr. Yogesh Kumar** to the Indian Institute of Technology Delhi, for the award of the degree of **Doctor of Philosophy**, is a record of the original bona fide research work carried out by him under my supervision and guidance. The thesis has reached the standards fulfilling the requirements of the regulations relating to the degree.

The results contained in this thesis have not been submitted in part or full to any other university or institute for the award of any degree or diploma.

Dr. R. K. Sharma
Professor
Department of Mathematics
Indian Institute of Technology Delhi
New Delhi 110 016

Acknowledgements

Any achievement, no matter how big or small, is not just an individual endeavour but the fructification of the efforts of a lot of people. This thesis is no exception. I hereby acknowledge the people whose involvement, direct or indirect, helped in this thesis seeing the light of the day.

First and foremost, I would like to express my deep sense of respect and gratitude to my thesis supervisor Prof. R. K. Sharma, who has been a constant source of inspiration during the course of this thesis work. He has always been patient and kept encouraging me to work in a better way. Without his help and support, I might have not been able to write this thesis.

I would like to give my special thanks to my SRC (Student Research Committee) members Prof S. Dharmaraja, Prof. Ritumoni Sarma, and Prof Arun Kumar for their valuable time and suggestions. I would also like to thank all the faculty members and staff of Department of Mathematics, IIT Delhi for their co-operation and support.

I would like to express special thanks and heartiest gratitude to Dr. P. R. Mishra (Working in Scientific Analysis Group, DRDO) for his guidance and encouragement. He helped me in programming and verification of proofs of the conjectures made based on the experimental results. He is known to be a workaholic in the laboratory.

I wish to express my sincere thanks to the current Director, Mrs. Anu Khosla and the former Director, Dr. P. K. Saxena, Scientific Analysis Group (SAG), DRDO for their continuous encouragement and suggestions.

I would like to express my sincere respect and heartiest gratitude to Dr. N. Rajesh Pillai for his guidance, encouragement from the day one of joining his group. I have been working with him since

last twelve years in SAG. His inputs concerning analytical reasoning and experimental aspects of cryptology have been of great help.

I am also thankful to Dr. Nupur Gupta for her valuable suggestions and comments in improving the quality of my research papers. She also provided company and facility to make comfortable visits to IIT Delhi.

I would like to thank all my colleagues at DRDO and especially to Dr. S. S. Bedi, Mrs. Neelam Verma (Associate Director), Mrs. Pratibha Yadav (Divisional Head), Dr. Indiver Gupta (Group Head), Mr. Bhartendu Nandan (who reviewed my articles in SAG), Mr. Manoj Kumar, Mrs. Hetal Borisagar, Dr. D. Dey, Dr. Sartaj Ul Hasan, Dr. Gireesh Pandey, Mrs. Rachita Juneja, Mr. Jasbir Singh, Mr. D. Upadhyay, Mr. Girish Mishra for their support and encouragement.

I also thank all my friends at IIT Delhi and especially to Vishal, Ambrish, Harish, Alok, Anju, Ankita, Rohit, Chirag, Yogesh and Rahul for their support.

It would be unfair, if I leave my revered parents as they devoted their whole youth for my well being and progress. They have instilled in me the value of hard work. The contribution of my in-laws deserve my regards and heartiest gratitude as they supported and encouraged continuously. I would like to express my gratitude to my Chacha ji who has been very supporting from my school days. I am also thankful to my brothers and sisters who have provided their helping hands in each and every walk of my life.

Last, but not the least is the dedicated sacrifice of my loving wife, Payal Singh who calmly and patiently did everything possible on her part, leaving aside all her comforts and ease of life, just to support me through my research work. I draw a superb and delightful stream of strength from my lovely son, Ayansh, who has always made the atmosphere at my home very lively and entertaining.

Most importantly, I thank almighty God for his blessings.

New Delhi *Yogesh Kumar*

Abstract

The present thesis is a study of two important crypto-primitives being used in modern day crypto-designs namely Integer Recurrence Relations (IRRs) modulo 2^e, $e \geq 1$ and permutations. IRRs are mainly used for generation of pseudo-random bit stream in stream ciphers while permutations are the simplest tools to achieve confusion and diffusion, primarily in block ciphers.

An arbitrary IRR may not be of much interest for cryptographic purposes. The IRRs attaining maximum possible period are the preferred candidates for cryptographic designs. Such IRRs are termed as primitive IRRs. Needless to say, why enumeration and construction of primitive IRRs are interesting cryptographic problems.

Condition for primitivity of IRRs was proposed by Brent. We enumerate primitive polynomials and corresponding shift distinct sequences using Brent's condition.

We study permutations on the ring $\mathbb{Z}_n$ with respect to important cryptographic properties viz, non-linearity and differential uniformity. There are different notions for non-linearity of permutations. The notion we consider is proposed by Mishra et. al.. By non-linearity of a permutation, we mean the minimum distance from all affine permutations over $\mathbb{Z}_n$.

Affine equivalence [34] is a property of permutations that preserves non-linearity and differential uniformity. We propose an efficient algorithm to check affine equivalence of permutations of length n, of complexity $O(n^2)$ in best case. Direct sum and skew

sum are the way to combine two or more permutations of different lengths. We construct permutations of larger length with known bound of non-linearity from the permutations of smaller length by the use of direct sum and skew sum. We also generalize the notion of non-linearity and affine equivalence of permutations to an arbitrary finite commutative ring with unity and prove several results analogous to those given for $\mathbb{Z}_n$.

We explore the existence and non-linearity of affine k-cycle permutations over $\mathbb{Z}_n$ for different values of k and n and derived results for special case when n is a prime. Arbitrary permutations over $\mathbb{Z}_n$ or $GF(2^n)$ have not been much explored for their cryptographic properties. We analyse various cases of permutations over $\mathbb{Z}_n$ for non-linearity and differential uniformity and their inter-relations.

The inversion permutation over finite field $GF(2^{2m})$ is known to have good cryptographic properties and is used in many cryptosystems. We consider the inversion permutation over finite ring $\mathbb{Z}_p$ and derive several results for its non-linearity and differential uniformity. We also construct new classes of differential 4 and 6 uniform permutations by swapping two positions in the inversion permutation and determine the non-linearity for these permutations. Further, we extend the notion of inversion permutation from $\mathbb{Z}_p$ to $\mathbb{Z}_{p^2}$ and derive expression for its non-linearity and differential uniformity.

Exponential Welch Costas (EWC) and Logarithmic Welch Costas (LWC) permutations over $\mathbb{Z}_{p-1}$ are Almost Perfect Non-linear (APN) having good cryptographic. We construct new classes of differential 4 and 6 uniform permutations from these permutations by swapping two positions.

The cryptographic implication of the work can be seen on permutation based stream ciphers like RC4 and its variants. We apply this study on RC4 cipher and conclude that increasing the key size for RC4 does not mean that increase in the security or saturation after a limit but security may even fall down as key size increases.

क्रिप्टोग्राफीय प्रिमोटिवों के गुण : पूर्णांक पुनरावृत्तिक सम्बन्ध एवं क्रमचय
(प्रॉपर्टीज़ ऑफ़ क्रिप्टोग्राफिक प्रिमिटिव्स : इंटीजऱ रिकरेन्स रिलेशंस एन्ड पेरमुटेशन्स)

सारांश

प्रस्तुत शोध प्रबंध आधुनिक युग की क्रिप्टो-डिज़ाइनों में प्रयुक्त होने वाले दो प्रमुख क्रिप्टो-प्रिमिटिवों -पूर्णांक पुनरावृत्तिक सम्बन्ध मॉड्युलो 2^e, e ≥ 1(आई० आर० आर०) एवं क्रमचयों, का अध्ययन है। आई० आर० आर० मुख्यतया धारा साईफरों के लिए छद्म यादृक्षिक बिट धारा के जनन में प्रयुक्त होता है जबकि क्रमचय ब्लॉक साईफरों में कन्फ़ूज़न और डिफ्यूज़न लाने के लिए एक सरलतम साधन है।

एक यादृक्षिक आई० आर० आर० क्रिप्टोग्राफीय उद्देश्यों के लिए हमेशा उपयोगी नहीं होता है। जो आई० आर० आर० महत्तम सम्भाव्य पीरियड रखते हैं, क्रिप्टोग्राफीय डिज़ाइनों के लिए उपयुक्त होते हैं। ऐसे आई० आर० आर० प्रिमिटिव आई० आर० आर० कहे जाते हैं। कहने की आवश्यकता नहीं कि प्रिमिटिव आई० आर० आर० का निर्माण और गणन क्यों एक रुचिकर क्रिप्टोग्राफीय विषय है।
आई० आर० आर० की प्रिमिटिविटी के लिए शर्त ब्रेंट द्वारा दी गयी थी। हम ब्रेंट की शर्त के सापेक्ष प्रिमिटिव बहुपदों और उनके संगत शिफ्ट डिस्टिंक्ट अनुक्रमों की गणना करते हैं।

हम रिंग Z_n पर परिभाषित क्रमचयों का प्रमुख क्रिप्टोग्राफीय गुणों यथा नॉन-लिनियरिटी और डिफरेंसियल यूनिफॉर्मिटी के सापेक्ष अध्ययन करते हैं। इसके लिए हम जिस अवधारणा को लेकर चल रहे हैं, वह मिश्रा एवं अन्य द्वारा प्रस्तावित है। नॉन-लिनियरिटी से हमारा तात्पर्य, Z_n पर परिभाषित अफाईन क्रमचयों से न्यूनतम दूरी से है।

अफाईन समतुल्यता [37] वह गुण है जो नॉन-लिनियरिटी और डिफरेंसियल यूनिफॉर्मिटी को संरक्षित करता है। हम n लम्बाई के क्रमचयों में अफाईन समतुल्यता जांचने के लिए एक कुशल अल्गोरिथम प्रस्तावित करते हैं, जिसकी सर्वोपयुक्त दशा में जटिलता O(n^2) है।

डाइरेक्ट योग और स्क्यू योग भिन्न भिन्न लम्बाइयों के दो या दो से अधिक क्रमचयों को आपस में मिलाने के तरीक़े हैं। हम डाइरेक्ट योग और स्क्यू योग की सहायता से छोटे क्रमचयों को लेकर नॉन-लिनियरिटी के ज्ञात निम्न-परिबंधों वाले बड़े क्रमचयों का निर्माण करते हैं। हम क्रमचयों के लिए नॉन-लिनियरिटी और अफाईन समतुल्यता की अवधारणों को एक यादृक्छिक परिमित क्रमविनिमेय रिंग जिसमे इकाई का अस्तित्व हो, के लिए व्यापकीकृत भी करते है और साथ ही इसके लिए Z_n के परिणामों के अनुरूप कई परिणामो को सिद्ध करते हैं।

हम k और n के विभिन्न मानों के लिए Z_n पर परिभाषित अफाईन k-साईकिल क्रमचयों के अस्तित्व और उनकी नॉन-लिनियरिटी का अन्वेषण करते हैं और एक विशेष दशा में जब n एक अभाज्य संख्या हो, कई परिणामों के व्युत्पत्ति करते हैं। Z_n या GF(2^n) पर परिभाषित यादृक्छिक क्रमचयों के क्रिप्टोग्राफीय गुणों का अधिक अन्वेषण अभी तक नहीं हुआ है। हम Z_n पर परिभाषित क्रमचयों की नॉन-लिनियरिटी और डिफरेंसियल यूनिफॉर्मिटी और उनके अन्तर्सम्बन्धों का विभिन्न दशाओं में विश्लेषण करते हैं।

परिमित फील्ड GF(2^2m) पर परिभाषित इनवर्ज़न क्रमचय अपने श्रेष्ठ क्रिप्टोग्राफीय गुणों के लिए जाने जाते हैं और कई क्रिप्टो सिस्टमों में प्रयुक्त किये गए हैं। हम परिमित रिंग Z_p पर परिभाषित इनवर्ज़न क्रमचय को लेते हैं और इसकी नॉन-लिनियरिटी और डिफरेंसियल यूनिफॉर्मिटी से सम्बंधित कई परिणामों की व्युत्पत्ति करते हैं। हम इनवर्ज़न क्रमचय के दो स्थानों की अदला-बदली करके डिफरेंसियल 4 और 6 यूनिफॉर्म क्रमचयों के नए वर्गों का निर्माण करते हैं तथा इनकी नॉन-लिनियरिटी की गणना करते हैं। इसके अलावा Z_p के लिए इनवर्ज़न क्रमचय की अवधारणा का Z_{p^2} के लिए विस्तार करते हैं और इसकी नॉन-लिनियरिटी और डिफरेंसियल यूनिफॉर्मिटी की व्युत्पत्ति करते हैं।

Z_{p-1} पर परिभाषित चरघातांकीय वेल्च कोस्टास (EWC) और लघुगणकीय वेल्च कोस्टास (LWC) क्रमचय, आलमोस्ट परफेक्ट नॉन लीनियर होते हैं और अच्छे क्रिप्टोग्राफीय गुण रखते हैं। हम इन क्रमचयों के दो स्थानों की अदला-बदली करके डिफरेंसियल 4 और 6 यूनिफॉर्म क्रमचयों के नए वर्गों निर्माण करते हैं।

प्रस्तुत कार्य का क्रिप्टोग्राफीय प्रभाव क्रमचय आधारित धारा साईफरों जैसे आर० सी० 4 (RC4) और इसके संशोधित रूपों पर देखा जा सकता है। हम इस अध्ययन को आर० सी० 4 पर लागू करते हैं और इस निष्कर्ष पर पहुंचते है कि आर० सी० 4 की कुंजी के आकर को बढ़ाने का मतलब इसकी सुरक्षा बढ़ाना या इसे संतृप्त करना नहीं है, वरन कुंजी का आकर बढ़ाना सुरक्षा स्तर को गिरा भी कर सकता है।

Contents

List of Symbols

$\mathbb{N}$	the set of natural numbers
$\mathbb{Z}$	the set of integers
$\mathbb{Q}$	the set of rational numbers
$a \mid b$	a divides b
$a \nmid b$	a does not divide b
$\forall x$	for all x
$\lvert S \rvert$	the cardinality (= number of elements) of the finite set S
$x \in X$	x is a member of X
$x \notin X$	x is not a member of X
$A \subseteq X$	A is a subset of X
$a \equiv b \pmod{n}$	a congruent to b modulo n
$a \not\equiv b \pmod{n}$	a not-congruent to b modulo n
$gcd(k_1, k_2, \ldots, k_n)$	the greatest common divisor of $k_1, \ldots, k_n$
$\phi(n)$	Euler's totient function of n
$\mathbb{Z}_n$	ring of integers modulo n
$\mathbb{U}_n$	the multiplicative group of integers modulo n
$< a >$	the cyclic group generated by a
$\mathbb{F}_q, \mathbb{GF}(q)$	finite field with q elements
(x/y)	the Legendre Symbol