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.