Chapter 3
Neutrosophic Analysis of Rejection Sampling in Post Quantum Cryptography (PQC)

Shashi Kant Pandey
https://orcid.org/0000-0002-0818-6984
Society for Electronic Transaction and Security, Chennai, India

ABSTRACT

Digital authentication and key encapsulation mechanisms (KEM) are two basic primitives for the security level of all robotic and IoT systems. Dilithium and Kyber are two post-quantum algorithms to establish secure communication. The use of uniform random sampling in these algorithms is very important. The finalists Dilithium and Kyber use SHAKE and AES to generate the random sequence at multiple stages of the algorithm. Here, the authors characterize one of the sampling techniques available in Dilithium with the help of the neutrosophic Boolean function. The idea of the neutrosophic Boolean function came from the theory of neutrosophy, and it is useful to study any ternary distributions. The authors present the non-existence of neutrobalanced bent functions specifically with respect to the sampling named SampleInBall in Dilithium.

1. INTRODUCTION

Any equation or a function having class symbols $x, y, \ldots$ is termed a "logical equation" or a "logical function" by Georg Boole (1815-1864). Every logical function f(x) can be written as $f(x) = ax + b(1 - x)$, under the convention for the law of

DOI: 10.4018/979-8-3693-2085-3.ch003

symbols by George Boole (Boole,1957). If a and b are equal then this function is a balanced function. The extension of the idea of Boole's representation of a Boolean function for two variables x and y is

$$f(x,y) = f(1,1)xy + f(1,0)x(1-y) + f(0,1)(1-x)y + f(0,0)(1-x)(1-y)$$

With the abuse of notation, a Boolean function in cryptography is termed as a function f from an n dimensional vector space F_2^n to the base field F_2 of order 2. Later on, the development of cryptography produces many such mathematical properties of Boolean functions (Kolmogorov et al,1992; Carlet,2020; Dillon,1974; Kavut,2008; Cusick et al,2009). To a certain extent, the enumeration of cryptographic properties of a Boolean function starts with an important transformation of a Boolean function named Walsh transformation(*WT*). This transformation depends on the first-order correlation of a bit stream of a Boolean function. Another important cryptographic requirement of a Boolean function is its nonlinearity *(NL)* and it is based on the maximum value of the Walsh transformation. Those Boolean functions having maximum nonlinearity are called bent Boolean functions. Other than the correlation nature of the input-output of a Boolean function, there is a well-known feature of algebraic resistance and it is named Algebraic immunity (AI) (Courtois,2003;Carlet et al,2006). The generalization of the Boolean function and its other cryptographic features is an interesting area of work. These functions are named as Generalized Boolean function (GBF) in the literature (Tăndăreanu,1981;Budaghyan et al,2018;-Carlet et al, 2006;Stanica et al, 2011). The generalization of the bent Boolean function proposed by O.S. Rothus in (Rothaus,1976). A generalization of Boolean function based on neutrosophy and logic is presented in (Smarandache, 2003;Vadiraja et al, 2022) and termed as a neutrosphic Boolean function.

The idea of neutrosophy came from the classification of a set (Smarandache et al, 2020; Smarandache et al, 2019; Smarandache et al, 2003; Smarandache et al, 2020). An imagination of three disjoint classifications refers that any set S can be classified as P_1, P_2 and P_3 such that the given condition for a set is satisfied by elements in P_1, not satisfied by elements in P_2 and undefined or not decidable for elements in P_3. In this way, any set with any condition uniformly obeys the idea of neutrality or neutrosophy. This partition leads us to define a neutrosphic function ψ from any set S to any arbitrary set K, where ψ is defined on the partition P_1, not defined on P_2 and indeterminate on P_3. The same analogy is useful for studying every rejection sampling where some condition is fixed for the selection of the sample. In particular, any arbitrary evaluation of a function $f(x)$ can be used to reject or accept in the sampling procedure. One simple example for the partition of the sample can be seen as three sets $P_0 = \{x{:}0 = f(x) mod 2\}, P_1 = \{x{:}0 \neq f(x) mod 2\}$ and $P_3 =$