Nonlinear S-box construction in modern Cipher

Md. Shamim Hossain Biswas*

* Faculty of Information Technology, Novosibirsk State University
1, Pirogova str., Novosibirsk, 630090, Siberia, Russia

DOI: 10.29322/IJSRP.14.01.2024.p14539
https://dx.doi.org/10.29322/IJSRP.14.01.2024.p14539

Paper Received Date: 19th December 2023
Paper Acceptance Date: 22nd January 2024
Paper Publication Date: 30th January 2024

Abstract- The aim of the research was to investigate and reveal the construction mechanism of a component-based nonlinear S-box. The nonlinear S-box is a vectorial Boolean function. When a vectorial Boolean function is used as an S-box, it can be straight, compressible, and expandable. The application of S-boxes is noticeable in modern block ciphers. In this article, the construction of a nonlinear S-box based on a vectorial Boolean function is presented for scientific readers. Actually, the substitution box is a Boolean space where substitution takes place through an action of the S-box (mathematical function) and provides confusion in block cipher. Computational and exploratory research methods were applied in this research. Reviewing a number of current S-box construction techniques and applying ideas mathematically to construct a new S-box was the primary initiative to conduct this research. Critical thinking was the main key to capturing the mathematical notion behind the nonlinear S-box. Data collection methods were a literature review, an online survey questionnaire, and a focus group discussion. The population of the research work was doctoral students and professors.

Index Terms- Cryptography, S-box, Nonlinearity, vectorial Boolean function, Boolean Space.

I. Introduction

Cryptology is the study of the of the science of secure communication techniques. It includes both the terms cryptography and cryptanalysis. Cryptography is used to create nonreadable code (messages). In general, we classify cryptography into two categories: classical and modern cryptography. Symmetric, asymmetric, and hash-based cryptography are used in our current digital security system. Further, the symmetric ciphers are categorized into two categories: stream ciphers and block ciphers. We notice the application of cryptography in our daily lives: computer passwords, digital currencies, secure web browsing, digital signatures, authentication, and so on. The encryption and decryption are done to achieve security in a cryptosystem. One of the aims of developing an S-box is to understand the construction mechanism of an S-box in block ciphers. S-box is a substitution cipher where symmetric encryption ciphers are used. The substitution box (S-box) is the main component of many modern symmetric encryption ciphers and provides confusion between the secret key and ciphertext. Boolean functions have the capability to provide both confusion and diffusion. The confusion technique is achieved by the nonlinearity parts of a cryptosystem. On the other hand, diffusion is achieved by making a small change in the input.

A. *Boolean function*

A boolean function is a function whose arguments and result assume values from a two-element set $\{0 = false, 1 = true\}$. The Boolean function is also called a switching function in an electric circuit. A boolean function *f* of *n* variables is an arbitrary mapping from $\mathbb{Z}_2{}^n$ to $\mathbb{Z}_2$. An n-variable Boolean function can be defined as $f : f_{2^n} \to f_2$. There are different categories of cryptographic Boolean functions [1,2,3]. But which type of Boolean function needs to be used in the construction of the S-box actually depends on the type of S-box. Boolean functions and S-box construction play a fundamental role in the design of the symmetric-key cipher. The number of Boolean functions of degree 4 is $2^{2^n} = 2^{2^4} = 65536$ where the number of linear Boolean functions is $2^n = 2^4 = 16$ and the number of nonlinear Boolean functions is $2^{2^n} - 2^n = 2^{2^4} - 2^4 = 65520$, the number of affine functions of 4-dimensional vector space is $A_n = 2^{n+1} = 2^{4+1} = 32$.

B. *Single-valued Boolean Function*

A single-valued Boolean function is a function that gives us a single output after taking multiple inputs. For example, when $n = 2$, a single-valued Boolean function will be $f\colon \mathbb{Z}_2^2 \to \mathbb{Z}_2$ or $f\colon \mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_2$ or $f\colon \{0,1\} \times \{0,1\} \to \{0,1\} \Rightarrow f\colon \{00,01,10,11\} \to \{0,1\}$.

C. *Multi-valued Boolean function*

A multi-valued boolean function is a function that generates multiple outputs after taking multiple inputs. For example, when $n = 2$, a multi-valued Boolean function will be $f\colon \mathbb{Z}_2^n \to \mathbb{Z}_2^m \mapsto f\colon \mathbb{Z}_2^2 \to \mathbb{Z}_2^2$ or $f\colon \mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_2 \times \mathbb{Z}_2$ or $f\colon \{0,1\} \times \{0,1\} \to \{1,0\} \times \{0,1\} \mapsto f\colon \{00,01,10,11\} \to \{10\},\{11\},\{00\},\{01\}$.

D. *Vectorial Boolean Function*

In cryptography, a substitution box (S-box) can be any function. The function that is going to be used in this research is the vectorial Boolean function [4]. This is basically used in block ciphers. It is a basic component of a block cipher. A vectorial boolean function ($\mathbb{F}$) is constructed by combining the 2^{n-1} numbers of boolean functions *(f)*. Where *n* is denoted by the *n*-dimensional vector space [5]. Since a vectorial Boolean function ($\mathbb{F}$) is a collection of boolean functions, it can be represented mathematically as a vector-valued function.

$$\mathbb{F}(x_n \dots x_2, x_1) = f_n(x_n \dots x_2, x_1) \oplus f_{n-1}(x_n \dots x_2, x_1) \oplus \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots \oplus f_2(x_n \dots x_2, x_1) \oplus f_1(x_n \dots x_2, x_1)$$

$$f_1(x_n \dots x_2, x_1) = (a_n x_n \oplus a_{n-1} x_{n-1} \oplus \dots \oplus a_1 x_1 \oplus a_0)$$

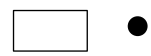
$$f_2(x_n \dots x_2, x_1) = (a_n x_n \oplus a_{n-1} x_{n-1} \oplus \dots \oplus a_1 x_1 \oplus a_0)$$

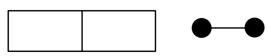
$$\vdots \qquad\qquad \vdots$$

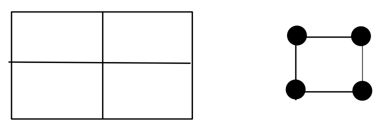
$$f_n(x_n \dots x_2, x_1) = (a_n x_n \oplus a_{n-1} x_{n-1} \oplus \dots \oplus a_1 x_1 \oplus a_0),$$

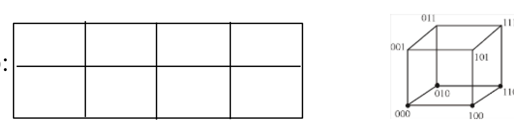
E. *Boolean Space*

Boolean Space (B^n): $n = 0,1,2 \dots \dots \dots \dots \dots \dots \dots \dots n-1$

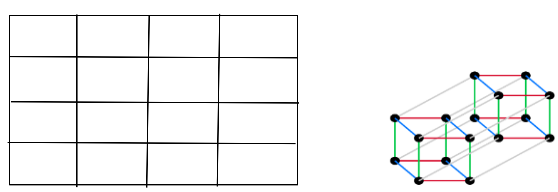
Zero-dimensional Boolean space or Zero-degree Boolean space (B^0):  $2^0 = 1$

One-dimensional Boolean space (B^1):  $2^1 = 2$

Two-dimensional Boolean space (B^2):  $2^2 = 4$

Three-dimensional Boolean space (B^3): 

$2^3 = 8$

Four-dimensional Boolean space (B^4):  $2^4 = 16$

Boolean spaces above are treated as a substitution box.

F. *Linear Vs Nonlinear Boolean function*

The boolean function *f* in *n* variable is said to be linear if it satisfies the linearity property: for example, $f(x \oplus y) = f(x) \oplus f(y)$.

x	f_1(Constant 0 function)	$f_2 = x$	$f_3 = \overline{x}$	f_4 Constant 1 function)
0	0	0	1	1
1	0	1	0	1

The function (f_1, f_4) is a linear Boolean function because both f_1 and f_4 satisfy the linearity property $f(x \oplus y) = f(x) \oplus f(y)$. On the other hand, the functions f_2 and f_3 are nonlinear Boolean functions.

G. *Affine Boolean function*

The boolean function with an algebraic expression where the degree is almost one is called an affine boolean function. Any boolean function f is called affine if it can be represented as `$l_{a,b}(x) = \langle a, x \rangle \oplus b$, where a $\in F_{2^n}$ and $b \in F_2$. So, the representation of an affine function as a vector-valued function of the form $f_{affine} = (x_n \dots x_2 . x_1) = a_n x_n + a_{n-1} x_{n-1} + \dots + a_1 x_1 + a_0$. This is called a general form of the n-variable affine function from a boolean perspective [6].

H. *Algebraic Normal Form*

There are some Boolean functions that can be uniquely represented by their algebraic normal form (ANF): $f(x_n \dots x_2 . x_1) = a_n x_n \oplus a_{n-1} x_{n-1} \oplus . \dots \dots \dots \dots \dots \dots \dots \dots \oplus a_1 x_1 \oplus a_0$. where all sets $\{\dots\}$ are pairwise distinct and all subsets are nonempty[7].

I. *Algebraic Degree*

The algebraic degree of a Boolean function is the number of variables in the longest item of its algebraic normal form (ANF). Similarly, the degree of an S-box is determined by the highest degree of its Boolean function. S-boxes with the highest degree thwart differential attack.

J. *Balanced:*

A Boolean function *f* (*x*) of *n* variables is called balanced if it takes each of the values 0 and 1 exactly 2^{n-1} times. It means the output of a balanced Boolean function is uniformly distributed over F_2. Unbalanced functions present a statistical bias that can be exploited in the attack. The balanced output distribution of S-box is one of the essential test criteria [8]. A balanced Boolean function is the requirement for defining nonlinearity [9].

K. *Nonlinearity*

It refers to the strength of a function. (Minimum) Nonlinearity of a Boolean function (N_f) of *n* variables is defined as the Hamming distance between the nonlinear Boolean function or Boolean function and the set of all affine functions. The mathematical representation of minimum nonlinearity and maximum nonlinearity is as follows:
Minimum Nonlinearity $\left(N_{f_i}\right) = \min d(f_i, A_{f_i})$,
Maximum **N**onlinearity: $N_{f_i} = 2^{n-1} - \frac{1}{2} \max_{W \in \mathbb{Z}_{2^n}} |S_{f_i}(W)|$.
The highest nonlinearity of a Boolean function can be computed by the Walsh spectrum [10].

L. *Application of Boolean function:*

The boolean function has various applications in modern cryptography. A boolean function is used to determine a boolean output based on some logical calculation of boolean inputs. Such kinds of boolean functions play a basic role in the questions of complexity theory, sequence design, combinatorics, and the design of circuits and chips for digital computers. The properties of Boolean functions play a critical role in cryptography, particularly in the design of substitution cipher (s-box) or symmetric key algorithms [11].

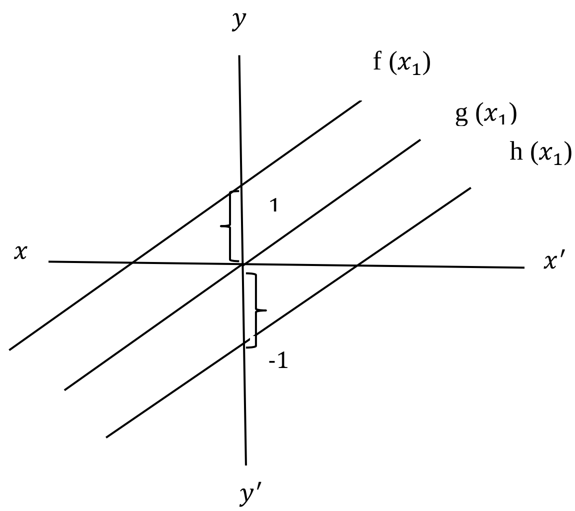
The importance of this research in the cryptographic security context is immense. The new technologies are emerging continuously, and quantum technologies are going to break the major security in our digital communication system. As a result, a quantum safe cipher construction is necessary in order to survive in the quantum world.

The road map for this article has been organized as follows: The first section is the introduction section; the second section consists of a literature review; the third section contain an S-box construction mechanism; the fourth section represents the outcome of research; the fifth section is the output measurement procedure; the sixth section contains a conclusion, recommendation, author's request to readers, and limitation; and the last section shows references and proof of research practice.

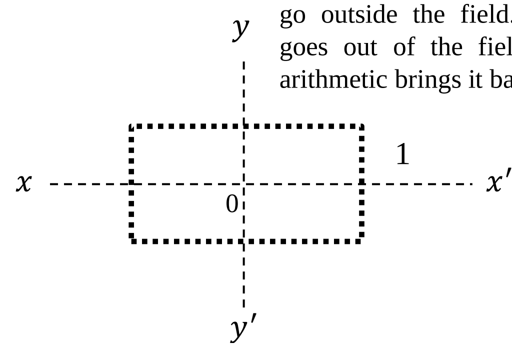
https://dx.doi.org/10.29322/IJSRP.14.01.2024.p14539

II. Literature Review

This research focuses on nonlinear S-box construction. To construct an S-box, an n-variable affine function must be constructed. Since a vectorial Boolean function is constructed by using an n-variable affine function, a clear understanding of an affine function is required. An affine function is a transformation of a linear function. A linear function does not have any intercepting points. It just goes through the origin of the horizontal and vertical axes. A function *f* that is mapped (transformed) from the input-domain to the output-range is an affine function if there exists $\mathbb{Z} \in \mathbb{R}^m$. A linear transformation from real number to real number in matrix form is defined by $\mathbb{R} \xrightarrow{linear\ transformation} \mathbb{R}^m$. Affine function $f\ (\alpha x\ + \beta y) =\ \alpha f\ (x)\ + \beta f(y) + Z$, for Boolean function perspective $f\ (x \oplus y) = f\ (x) \oplus f(y) \oplus Z$, where α, β and $Z\ = 1$

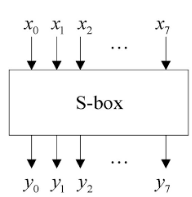


A field with unit length. This field area is defined by {0,1}; none can go outside the field. If anyone goes out of the field, modulus arithmetic brings it back.



The function *g* (x_1) is a linear function that passes through the origin. For example, if we make a transformation of this function, let's say we add z equal to 1 and add z equal to -1, and we make two functions, which are *f* (x_1) and *h* (x_1), then these two functions are affine functions. By the way, the function *g* (x_1) can also be an affine function where it intercepts zero. This means all affine functions are not necessarily linear functions, but all linear functions are affine functions. If a linear function has an intercept, it means it is a transformation of a linear function, and we call it an affine function [12].

To construct S-Boxes, we need to achieve a boolean function transformation technique $\{0,1\}^m \rightarrow \{0,1\}^n$. In some cases, a boolean function transformation is bound to $\{0,1\}^m \rightarrow \{0,1\}$. There are 2^n numbers of possible combinations of the given inputs of a boolean function. Such kinds of functions provide a single output, either 0 or 1. Boolean functions are an important property of cryptography, and they are considered the key to a digital security system. The confusion and diffusion concepts are logical concepts. Claud Shannon published those concepts in the late 1940s [13]. However, Claud Shannon introduced the concept of the substitution box in 1949 [14]. In general, the S-box is invertible. It is a one-to-one function (bijective [15]).



It takes some number of input bits *(m)*, and transforms them into some number of output bits *(n)*. The sophisticated nonlinear layer is called the S-box. The nonlinear layer plays an important role in deceiving fraudsters. There are some cryptographic criteria that ensure a good s-box: APN, SAC, balancedness, nonlinearity, algebraic immunity, differential uniformity, high order algebraic degree, etc. It is really a difficult task to construct an s-box that is safe from linear cryptanalysis, differential, and algebraic cryptanalysis. A detailed description of s-box construction based on boolean functions and permutations is given in [16].

A nonlinear s-box is a collection of n-variable nonlinear Boolean functions. The S-box is an essential and important component of block ciphers. The actions of S-box are created to protect block ciphers against known and potential cryptanalytic attacks [17].

https://dx.doi.org/10.29322/IJSRP.14.01.2024.p14539

An S-box construction technique based on Feistel and Lai-Massey structures can be found in [18]. This construction is shown based on the inversion technique of the Galois field, non-bijective functions, finite field multiplication, and permutations. Another method of S-box construction is to find the multiplicative inverse of an input based on the irreducible polynomial and multiply the multiplicative inverse by a specific matrix, then add the multiplication result to a specific vector [19].

Some well-known block ciphers are AES, DES, CAST, etc. In these block ciphers, a nonlinearly transformed S-box provides confusion [20, 21]. An S-box creation using a one-dimensional chaotic map can be used in AES. It was tested on the test criteria of the S-box, like balancedness, SAC, invertibility, and completeness. A dynamic S-box creates better confusion than a static S-box. This S-Box may be useful for lightweight cryptography and restricted devices [22].

APN function for block cipher perspective: An almost perfect nonlinear function plays an important role in modern block cipher. If any S-box fulfills the criteria of the APN function, it is considered to be an effective S-box. Because it is capable of resisting differential cryptanalysis [23].

The importance of the boolean function from a cryptographic perspective is immense. The use of the boolean function appears in many scientific disciplines, including cryptography, combinatorics, complexity theory, coding theory, graph theory, etc. In cryptography, the Boolean function and nonlinear Boolean function construction are required for designing a new S-box [24].

The logistic chaotic transformation technique can be used to design a quality S-box, especially for image encryption algorithms. A chaos-based S-box is used for image encryption. A chaotic boolean function is used to construct a nonlinear substitution component that is useful for image encryption [25]. An S-box is a group of boolean functions. An S-box can be constructed using a combination of Tent and logistic chaotic map. The chaotic Bent function is useful for the S-box. It can be generated using a chaotic function [26].

IDEA and AES S-box have been widely used in secure communication systems. The strength of S-box depends on high-order algebraic degree, balanced boolean function, strict avalanche criterion, differential uniformity, algebraic degree, nonlinearity, almost perfect nonlinearity, bit independence criterion, and linear and differential cryptanalysis [27].

The SAC is used to measure the maximal confusion ability of a particular Boolean function. The bit independence criterion is used to check dependency bits between plaintext and ciphertext in block cipher. The nonlinearity is the strength of the S-box. It increases the confusion capacity of the S-box [28]. DES S-box is no longer secure and is prohibited from the use of further encryption algorithms [29]. A construction of the S-box using linear fractional transformation and permutation functions [30].

DPA is a powerful technique to reveal sensitive information. The nonlinear operation of the S-box provides resistance against first-order differential power analysis (DPA). An affine equivalent bijective S-box can be defined as $S: GF(2^n) \rightarrow GF(2^n)$ [31]. There is one more bijective S-box implementation using quasi-cyclic codes. The cyclic codes are obtained from the cyclic shift. The quasi-cyclic codes are NP-hard problems [32].

The S-boxes are one of the most essential components of the block ciphers. S-boxes are used to prevent possible cryptanalytic attacks on block ciphers. DES is a compressible S-box [33]. Modern cipher AES uses a 8×8 straight S-box [34]. S-Boxes should satisfy various good cryptographic properties in order to ensure a high level of protection against potential attacks. The purpose of this study was to investigate and implement a modern substitution box that is quantum-safe.

A. Aims and Objectives

The overall research focus, or overrated goal of the current research, is to investigate, formulate, and explore the mathematics of nonlinear S-box construction and construct a nonlinear S-box. Therefore, the following research questions have been formulated from the research objectives to conduct the study:

Research Questions:

1. How do I construct a nonlinear S-box in modern cipher?
2. What types of the mathematical functions are required to construct a nonlinear S-box?

https://dx.doi.org/10.29322/IJSRP.14.01.2024.p14539

III. S-BOX CONSTRUCTION MECHANISM

This is a component-based nonlinear s-box construction mechanism. There are different types of S-box construction processes. It really depends on what kind of function is used to construct an S-box. In this section, a straight S-box construction mechanism for vectorial Boolean functions is shown. This is a five-step procedure.

STEP 1: Affine function construction: The construction of an n-variable affine function using combinatorics rules is available on the internet. So, those mathematical explanations are not necessary to explain here. To construct a 4-variable S-box, a 4-dimensional vector space $\mathbb{Z}_2{}^4$ is required. There are $2^4 = 16$ possible binary input string combinations for 4-variable unit vectors. So, a 4-variable affine function can be written as a linear combination of those bit strings: $a_{1,2,3,4}x_1x_2x_3x_4 \oplus a_{2,3,4}x_2x_3x_4 \oplus a_{1,3,4}x_1x_3x_4 \oplus a_{1,2,4}x_1x_2x_4 \oplus a_{1,2,3}x_1x_2x_3 \oplus a_{3,4}x_3x_4 \oplus a_{2,4}x_2x_4 \oplus a_{2,3}x_2x_3 \oplus a_{1,4}x_1x_4 \oplus a_{1,3}x_1x_3 \oplus a_{1,2}x_1x_2 \oplus a_4x_4 \oplus a_3x_3 \oplus a_2x_2 \oplus a_1x_1 \oplus a_0$

STEP 2: Linear component function construction: The table below shows the process of linear combination of component functions from a random choice of components, which are considered the basis of the S-box.

Table I: A linear combination of component functions

f_1	f_2	f_3	f_4	$f_5 = (f_1 \oplus f_2) \bmod 2$	$f_6 = (f_1 \oplus f_3) \bmod 2$	$f_7 = (f_1 \oplus f_4) \bmod 2$	$f_8 = (f_2 \oplus f_3) \bmod 2$	$f_9 = (f_2 \oplus f_4) \bmod 2$	$f_{10} = (f_3 \oplus f_4) \bmod 2$	$f_{11} = (f_1 \oplus f_2 \oplus f_3) \bmod 2$	$f_{12} = (f_1 \oplus f_2 \oplus f_4) \bmod 2$	$f_{13} = (f_1 \oplus f_3 \oplus f_4) \bmod 2$	$f_{14} = (f_2 \oplus f_3 \oplus f_4) \bmod 2$	$f_{15} = (f_1 \oplus f_2 \oplus f_3 \oplus f_4) \bmod 2$
0	1	0	0	1	0	0	1	1	0	1	1	0	1	1
1	0	1	0	1	0	1	1	0	1	0	1	0	1	0
1	1	1	0	0	0	1	0	1	1	1	0	0	0	1
0	0	0	1	0	0	1	0	1	1	0	1	1	1	1
1	0	0	1	1	1	0	0	1	1	1	0	0	1	0
1	1	0	1	0	1	0	1	0	1	0	1	0	0	1
0	0	1	1	0	1	1	1	1	0	1	1	0	0	0
1	1	1	1	0	0	0	0	0	0	1	1	1	1	0
0	1	0	1	1	0	1	1	0	1	1	0	1	0	0
1	0	1	1	1	0	0	1	1	0	0	0	1	0	1
1	0	0	0	1	1	1	0	0	0	1	1	1	0	1
1	1	0	0	0	1	1	1	1	0	0	0	1	1	0
0	1	1	0	1	1	0	0	1	1	0	1	1	0	0
0	1	1	1	1	1	1	0	0	0	0	0	0	1	1
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	1	0	0	1	0	1	0	1	1	0	1	1	1

There exist 2^{n-1} numbers of nonlinear Boolean functions for every possible random arrangement of components.

STEP 3: An equation construction: Construction of an equation using an n-variable linear affine function and a linear component function: $a_{1,2,3,4}x_1x_2x_3x_4 \oplus a_{2,3,4}x_2x_3x_4 \oplus a_{1,3,4}x_1x_3x_4 \oplus a_{1,2,4}x_1x_2x_4 \oplus a_{1,2,3}x_1x_2x_3 \oplus a_{3,4}x_3x_4 \oplus a_{2,4}x_2x_4 \oplus a_{2,3}x_2x_3 \oplus a_{1,4}x_1x_4 \oplus a_{1,3}x_1x_3 \oplus a_{1,2}x_1x_2 \oplus a_4x_4 \oplus a_3x_3 \oplus a_2x_2 \oplus a_1x_1 \oplus a_0 = LCf_i$.

STEP 4: Nonlinear Boolean function (Nf_i) construction: The aforesaid equation is used to construct a nonlinear Boolean function. The input of the above equation is the number of 4-variable unit-vector combinations and their corresponding component vectors. Since the 4-variable unit-vector combinations are used for the affine function, it can be labeled as an affine coordinate vector.

The nonlinear Boolean function construction technique (Nf_1):

$a_{1,2,3,4}x_1x_2x_3x_4 \oplus a_{2,3,4}x_2x_3x_4 \oplus a_{1,3,4}x_1x_3x_4 \oplus a_{1,2,4}x_1x_2x_4 \oplus a_{1,2,3}x_1x_2x_3 \oplus a_{3,4}x_3x_4 \oplus a_{2,4}x_2x_4 \oplus a_{2,3}x_2x_3 \oplus a_{1,4}x_1x_4 \oplus a_{1,3}x_1x_3 + a_{1,2}x_1x_2 \oplus a_4x_4 \oplus a_3x_3 \oplus a_2x_2 \oplus a_1x_1 \oplus a_0 = LCf_1$ ....equation no (1)

Table II: Inputs of equation number (1)

	Affine coordinate vector				Component	
	X_4	X_3	X_2	X_1	LCf_1	
	0	0	0	0	0	
	0	0	0	1	1	
	0	0	1	0	1	
	0	0	1	1	0	
	0	1	0	0	1	
	0	1	0	1	1	
	0	1	1	0	0	
	0	1	1	1	1	
a_i	1	0	0	0	0	L_i
	1	0	0	1	1	
	1	0	1	0	1	
	1	0	1	1	1	
	1	1	0	0	0	
	1	1	0	1	0	
	1	1	1	0	0	
	1	1	1	1	0	

To calculate the coefficients of equation (1), let's successively substitute the affine coordinate vector on the left side of the equation and the component vector on the right side of the equation. This process has to be repeated 16 times to get 16 coefficients. For instance, when $x_1 = x_2 = x_3 = x_4 = 0$ and $L_0 = 0$. The equation returns $a_0 = 0$ for the 1st input string $\langle 0000 \rangle$ and its corresponding component vector $\langle 0 \rangle$. Similarly, the rest of the coefficients are calculated as follows:

When $x_1 = 1$ and $x_2 = x_3 = x_4 = 0$, $a_1x_1 = 1 \oplus a_0 \mapsto a_1.1 = 1 \oplus 0 \mapsto a_1 = 1$
When $x_2 = 1$ and $x_1 = x_3 = x_4 = 0$, $a_2x_2 = 1 \oplus a_0 \mapsto a_2.1 = 1 \oplus 0 \mapsto a_2 = 1$
When $x_3 = 1$ and $x_1 = x_2 = x_4 = 0$, $a_3x_3 = 1 \oplus a_0 \mapsto a_3.1 = 1 \oplus 0 \mapsto a_3 = 1$
When $x_4 = 1$ and $x_1 = x_2 = x_3 = 0$, $a_4x_4 = 0 \oplus a_0 \mapsto a_4.1 = 0 \oplus 0 \mapsto a_4 = 1$
When $x_1 = x_2 = 1$ and $x_3 = x_4 = 0$, $a_{1,2}x_1x_2 = 0 \oplus 0 \oplus 1 \oplus 1 \mapsto a_{1,2}.1.1 = 0 \mapsto a_{1,2} = 0$
When $x_1 = x_3 = 1$ and $x_2 = x_4 = 0$, $a_{1,3}x_1x_3 = 1 \oplus 0 \oplus 1 \oplus 1 \mapsto a_{1,3}.1.1 = 1 \mapsto a_{1,3} = 1$
When $x_1 = x_4 = 1$ and $x_2 = x_3 = 0$, $a_{1,4}x_1x_4 = 1 \oplus 0 \oplus 1 \oplus 0 \mapsto a_{1,4}.1.1 = 0 \mapsto a_{1,4} = 0$
When $x_2 = x_3 = 1$ and $x_1 = x_4 = 0$, $a_{2,3}x_2x_3 = 0 \oplus 0 \oplus 1 \oplus 1 \mapsto a_{2,3}.1.1 = 0 \mapsto a_{2,3} = 0$
When $x_2 = x_4 = 1$ and $x_1 = x_3 = 0$, $a_{2,4}x_2x_4 = 1 \oplus 0 \oplus 1 \oplus 0 \mapsto a_{2,4}.1.1 = 0 \mapsto a_{2,4} = 0$
When $x_3 = x_4 = 1$ and $x_1 = x_2 = 0$, $a_{3,4}x_3x_4 = 0 \oplus 0 \oplus 1 \oplus 0 \mapsto a_{3,4}.1.1 = 1 \mapsto a_{3,4} = 1$
When $x_1 = x_2 = x_3 = 1$ and $x_4 = 0$, $a_{1,2,3}x_1x_2x_3 = 1 \oplus a_0 \oplus a_1 \oplus a_2 \oplus a_3 \oplus a_{1,2} \oplus a_{1,3} \oplus a_{2,3} \mapsto a_{1,2,3}1.1.1 = 1 \oplus 0 \oplus 1 \oplus 1 \oplus 1 \oplus 0 \oplus 1 \oplus 0 \mapsto a_{1,2,3} = 1$
When $x_1 = x_2 = x_4 = 1$ and $x_3 = 0$, $a_{1,2,4}x_1x_2x_4 = 1 \oplus a_0 \oplus a_1 \oplus a_2 \oplus a_4 \oplus a_{1,2} \oplus a_{1,4} \oplus a_{2,4} \mapsto a_{1,2,4}1.1.1 = 1 \oplus 0 \oplus 1 \oplus 1 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \mapsto a_{1,2,4} = 1$
When $x_1 = x_3 = x_4 = 1$ and $x_2 = 0$, $a_{1,3,4}x_1x_3x_4 = 0 \oplus a_0 \oplus a_1 \oplus a_3 \oplus a_4 \oplus a_{1,3} \oplus a_{1,4} \oplus a_{3,4} \mapsto a_{1,3,4}1.1.1 = 0 \oplus 0 \oplus 1 \oplus 1 \oplus 0 \oplus 1 \oplus 0 \oplus 1 \mapsto a_{1,3,4} = 0$
When $x_2 = x_3 = x_4 = 1$ and $x_1 = 0$, $a_{2,3,4}x_2x_3x_4 = 0 \oplus a_0 \oplus a_2 \oplus a_3 \oplus a_4 \oplus a_{2,3} \oplus a_{2,4} \oplus a_{3,4} \mapsto a_{2,3,4}1.1.1 = 0 \oplus 0 \oplus 1 \oplus 1 \oplus 0 \oplus 0 \oplus 0 \oplus 1 \mapsto a_{2,3,4} = 1$
When $x_1 = x_2 = x_3 = x_4 = 1$, $a_{1,2,3,4}x_1x_2x_3x_4 = 0 \oplus a_0 \oplus a_2 \oplus a_3 \oplus a_4 \oplus a_{1,2} \oplus a_{1,3} \oplus a_{1,4} \oplus a_{2,3} \oplus a_{2,4} \oplus a_{3,4} \oplus a_{1,2,3} \oplus a_{1,2,4} \oplus a_{1,3,4} \oplus a_{2,3,4} \mapsto a_{1,2,3,4}1.1.1.1 = 0 \oplus 0 \oplus 1 \oplus 1 \oplus 1 \oplus 0 \oplus 0 \oplus 1 \oplus 0 \oplus 0 \oplus 0 \oplus 1 \oplus 1 \oplus 1 \oplus 0 \oplus 1 \mapsto a_{1,2,3,4} = 0$

The following first nonlinear Boolean function is derived from substituting all coefficients into the 4-variable affine function:
$0.(x_1x_2x_3x_4) \oplus 1.(x_2x_3x_4) \oplus 0.(x_1x_3x_4) \oplus 1.(x_1x_2x_4) \oplus 1.(x_1x_2x_3) \oplus 1.(x_3x_4) \oplus 0.(x_2x_4) \oplus 0\ (x_2x_3) \oplus 0.(x_1x_4) 1.(x_1x_3) \oplus 0.(x_1x_2) \oplus 0.x_4 \oplus 1.x_3 \oplus 1.x_2 \oplus 1.x_1 \oplus 0 = f_1(x_4x_3x_2x_1) = x_2x_3x_4 \oplus x_1x_2x_4 \oplus x_1x_2x_3 \oplus x_3x_4 \oplus x_1x_3 \oplus x_3 \oplus x_2 \oplus x_1$

The nonlinear Boolean function construction (Nf_2):

$a_{1,2,3,4}x_1x_2x_3x_4 + a_{2,3,4}x_2x_3x_4 + a_{1,3,4}x_1x_3x_4 + a_{1,2,4}x_1x_2x_4 + a_{1,2,3}x_1x_2x_3 + a_{3,4}x_3x_4 + a_{2,4}x_2x_4 + a_{2,3}x_2x_3 + a_{1,4}x_1x_4 + a_{1,3}x_1x_3 + a_{1,2}x_1x_2 + a_4x_4 + a_3x_3 + a_2x_2 + a_1x_1 + a_0 = LCf_2$ .... equation no. (2)

Table III: Inputs of equation number (2)

	Affine coordinate vector				Component	
	X_4	X_3	X_2	X_1	LCf_2	
a_i	0	0	0	0	1	L_i
	0	0	0	1	0	
	0	0	1	0	1	
	0	0	1	1	0	
	0	1	0	0	0	
	0	1	0	1	1	
	0	1	1	0	0	
	0	1	1	1	1	
	1	0	0	0	1	
	1	0	0	1	0	
	1	0	1	0	0	
	1	0	1	1	1	
	1	1	0	0	1	
	1	1	0	1	1	
	1	1	1	0	0	
	1	1	1	1	0	

To calculate the coefficients of equation (2), let's successively substitute the affine coordinate vector on the left side of the equation and the component vector on the right side of the equation. This process has to be repeated 16 times to get 16 coefficients. For instance, when $x_1 = x_2 = x_3 = x_4 = 0$ and $L_0 = 1$. The equation returns $a_0 = 1$ for the 1st input string $\langle 0000 \rangle$ and its corresponding component vector $\langle 1 \rangle$. Similarly, the rest of the coefficients are calculated as follows:

When $x_1 = 1$ and $x_2 = x_3 = x_4 = 0$, $a_1x_1 = 0 \oplus a_0 \mapsto a_1.1 = 0 \oplus 1 \mapsto a_1 = 1$
When $x_2 = 1$ and $x_1 = x_3 = x_4 = 0$, $a_2x_2 = 1 \oplus a_0 \mapsto a_2.1 = 1 \oplus 1 \mapsto a_2 = 0$
When $x_3 = 1$ and $x_1 = x_2 = x_4 = 0$, $a_3x_3 = 0 \oplus a_0 \mapsto a_3.1 = 0 \oplus 1 \mapsto a_3 = 1$
When $x_4 = 1$ and $x_1 = x_2 = x_3 = 0$, $a_4x_4 = 1 \oplus a_0 \mapsto a_4.1 = 1 \oplus 1 \mapsto a_4 = 0$
When $x_1 = x_2 = 1$ and $x_3 = x_4 = 0$, $a_{1,2}x_1x_2 = 0 \oplus 1 \oplus 1 \oplus 0 \mapsto a_{1,2}.1.1 = 0 \mapsto a_{1,2} = 0$
When $x_1 = x_3 = 1$ and $x_2 = x_4 = 0$, $a_{1,3}x_1x_3 = 1 \oplus 1 \oplus 1 \oplus 1 \mapsto a_{1,3}.1.1 = 0 \mapsto a_{1,3} = 0$
When $x_1 = x_4 = 1$ and $x_2 = x_3 = 0$, $a_{1,4}x_1x_4 = 0 \oplus 1 \oplus 1 \oplus 0 \mapsto a_{1,4}.1.1 = 0 \mapsto a_{1,4} = 0$
When $x_2 = x_3 = 1$ and $x_1 = x_4 = 0$, $a_{2,3}x_2x_3 = 0 \oplus 1 \oplus 0 \oplus 1 \mapsto a_{2,3}.1.1 = 0 \mapsto a_{2,3} = 0$
When $x_2 = x_4 = 1$ and $x_1 = x_3 = 0$, $a_{2,4}x_2x_4 = 0 \oplus 1 \oplus 0 \oplus 0 \mapsto a_{2,4}.1.1 = 1 \mapsto a_{2,4} = 1$
When $x_3 = x_4 = 1$ and $x_1 = x_2 = 0$, $a_{3,4}x_3x_4 = 1 \oplus 1 \oplus 1 \oplus 0 \mapsto a_{3,4}.1.1 = 1 \mapsto a_{3,4} = 1$
When $x_1 = x_2 = x_3 = 1$ and $x_4 = 0$, $a_{1,2,3}x_1x_2x_3 = 1 \oplus a_0 \oplus a_1 \oplus a_2 \oplus a_3 \oplus a_{1,2} \oplus a_{1,3} \oplus a_{2,3} \mapsto a_{1,2,3}1.1.1 = 1 \oplus 1 \oplus 1 \oplus 0 \oplus 1 \oplus 0 \oplus 0 \oplus 0 \mapsto a_{1,2,3} = 0$
When $x_1 = x_2 = x_4 = 1$ and $x_3 = 0$, $a_{1,2,4}x_1x_2x_4 = 1 \oplus a_0 \oplus a_1 \oplus a_2 \oplus a_4 \oplus a_{1,2} \oplus a_{1,4} \oplus a_{2,4} \mapsto a_{1,2,4}1.1.1 = 1 \oplus 1 \oplus 1 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 1 \mapsto a_{1,2,4} = 0$
When $x_1 = x_3 = x_4 = 1$ and $x_2 = 0$, $a_{1,3,4}x_1x_3x_4 = 1 \oplus a_0 \oplus a_1 \oplus a_3 \oplus a_4 \oplus a_{1,3} \oplus a_{1,4} \oplus a_{3,4} \mapsto a_{1,3,4}1.1.1 = 1 \oplus 1 \oplus 1 \oplus 1 \oplus 0 \oplus 0 \oplus 0 \oplus 1 \mapsto a_{1,3,4} = 1$
When $x_2 = x_3 = x_4 = 1$ and $x_1 = 0$, $a_{2,3,4}x_2x_3x_4 = 0 \oplus a_0 \oplus a_2 \oplus a_3 \oplus a_4 \oplus a_{2,3} \oplus a_{2,4} \oplus a_{3,4} \mapsto a_{2,3,4}1.1.1 = 0 \oplus 1 \oplus 0 \oplus 1 \oplus 0 \oplus 0 \oplus 1 \oplus 1 \mapsto a_{2,3,4} = 0$
When $x_1 = x_2 = x_3 = x_4 = 1$, $a_{1,2,3,4}x_1x_2x_3x_4 = 0 \oplus a_0 \oplus a_2 \oplus a_3 \oplus a_4 \oplus a_{1,2} \oplus a_{1,3} \oplus a_{1,4} \oplus a_{2,3} \oplus a_{2,4} \oplus a_{3,4} \oplus a_{1,2,3} \oplus a_{1,2,4} \oplus a_{1,3,4} \oplus a_{2,3,4} \mapsto a_{1,2,3,4}1.1.1.1 = 0 \oplus 1 \oplus 1 \oplus 0 \oplus 1 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 1 \oplus 1 \oplus 0 \oplus 0 \oplus 1 \oplus 0 \mapsto a_{1,2,3,4} = 0$

The following 2nd nonlinear Boolean function is derived from substituting all coefficients into the 4-variable affine function:
$0.(x_1x_2x_3x_4) \oplus 0.(x_2x_3x_4) \oplus 1.(x_1x_3x_4) \oplus 0.(x_1x_2x_4) \oplus 0.(x_1x_2x_3) \oplus 1.(x_3x_4) \oplus 1.(x_2x_4) \oplus 0.(x_2x_3) \oplus 0.(x_1x_4) \oplus 0.(x_1x_3) \oplus 0.(x_1x_2) \oplus 0.x_4 \oplus 1.x_3 \oplus 0.x_2 \oplus 1.x_1 \oplus 1 = f_2(x_4x_3x_2x_1) = x_1x_3x_4 \oplus x_3x_4 \oplus x_2x_4 \oplus x_3 \oplus x_1 \oplus 1$

https://dx.doi.org/10.29322/IJSRP.14.01.2024.p14539

The nonlinear Boolean function construction (Nf_3):

$a_{1,2,3,4}x_1x_2x_3x_4 + a_{2,3,4}x_2x_3x_4 + a_{1,3,4}x_1x_3x_4 + a_{1,2,4}x_1x_2x_4 + a_{1,2,3}x_1x_2x_3 + a_{3,4}x_3x_4 + a_{2,4}x_2x_4 + a_{2,3}x_2x_3 + a_{1,4}x_1x_4 + a_{1,3}x_1x_3 + a_{1,2}x_1x_2 + a_4x_4 + a_3x_3 + a_2x_2 + a_1x_1 + a_0 = LCf_3$ .... equation no. (3)

Table IV: Inputs of equation number (3)

	Affine coordinate vector				Component	
	X_4	X_3	X_2	X_1	LCf_3	
a_i	0	0	0	0	0	L_i
	0	0	0	1	1	
	0	0	1	0	1	
	0	0	1	1	0	
	0	1	0	0	0	
	0	1	0	1	0	
	0	1	1	0	1	
	0	1	1	1	1	
	1	0	0	0	0	
	1	0	0	1	1	
	1	0	1	0	0	
	1	0	1	1	0	
	1	1	0	0	1	
	1	1	0	1	1	
	1	1	1	0	0	
	1	1	1	1	1	

To calculate the coefficients of equation (3), let's successively substitute the affine coordinate vector on the left side of the equation and the component vector on the right side of the equation. This process has to be repeated 16 times to get 16 coefficients. For instance, when $x_1 = x_2 = x_3 = x_4 = 0$ and $L_0 = 0$. The equation returns $a_0 = 0$ for the 1st input string $\langle 0000 \rangle$ and its corresponding component vector $\langle 0 \rangle$. Similarly, the rest of the coefficients are calculated as follows:

When $x_1 = 1$ and $x_2 = x_3 = x_4 = 0$, $a_1x_1 = 1 \oplus a_0 \mapsto a_1.1 = 1 \oplus 0 \mapsto a_1 = 1$
When $x_2 = 1$ and $x_1 = x_3 = x_4 = 0$, $a_2x_2 = 1 \oplus a_0 \mapsto a_2.1 = 1 \oplus 0 \mapsto a_2 = 1$
When $x_3 = 1$ and $x_1 = x_2 = x_4 = 0$, $a_3x_3 = 0 \oplus a_0 \mapsto a_3.1 = 0 \oplus 0 \mapsto a_3 = 0$
When $x_4 = 1$ and $x_1 = x_2 = x_3 = 0$, $a_4x_4 = 0 \oplus a_0 \mapsto a_4.1 = 0 \oplus 0 \mapsto a_4 = 0$
When $x_1 = x_2 = 1$ and $x_3 = x_4 = 0$, $a_{1,2}x_1x_2 = 0 \oplus 0 \oplus 1 \oplus 1 \mapsto a_{1,2}.1.1 = 0 \mapsto a_{1,2} = 0$
When $x_1 = x_3 = 1$ and $x_2 = x_4 = 0$, $a_{1,3}x_1x_3 = 0 \oplus 0 \oplus 1 \oplus 0 \mapsto a_{1,3}.1.1 = 1 \mapsto a_{1,3} = 1$
When $x_1 = x_4 = 1$ and $x_2 = x_3 = 0$, $a_{1,4}x_1x_4 = 1 \oplus 0 \oplus 1 \oplus 0 \mapsto a_{1,4}.1.1 = 0 \mapsto a_{1,4} = 0$
When $x_2 = x_3 = 1$ and $x_1 = x_4 = 0$, $a_{2,3}x_2x_3 = 1 \oplus 0 \oplus 1 \oplus 0 \mapsto a_{2,3}.1.1 = 0 \mapsto a_{2,3} = 0$
When $x_2 = x_4 = 1$ and $x_1 = x_3 = 0$, $a_{2,4}x_2x_4 = 0 \oplus 0 \oplus 1 \oplus 0 \mapsto a_{2,4}.1.1 = 1 \mapsto a_{2,4} = 1$
When $x_3 = x_4 = 1$ and $x_1 = x_2 = 0$, $a_{3,4}x_3x_4 = 1 \oplus 0 \oplus 0 \oplus 0 \mapsto a_{3,4}.1.1 = 1 \mapsto a_{3,4} = 1$
When $x_1 = x_2 = x_3 = 1$ and $x_4 = 0$, $a_{1,2,3}x_1x_2x_3 = 1 \oplus a_0 \oplus a_1 \oplus a_2 \oplus a_3 \oplus a_{1,2} \oplus a_{1,3} \oplus a_{2,3} \mapsto a_{1,2,3}1.1.1 = 1 \oplus 0 \oplus 1 \oplus 1 \oplus 0 \oplus 0 \oplus 1 \oplus 0 \mapsto a_{1,2,3} = 0$
When $x_1 = x_2 = x_4 = 1$ and $x_3 = 0$, $a_{1,2,4}x_1x_2x_4 = 0 \oplus a_0 \oplus a_1 \oplus a_2 \oplus a_4 \oplus a_{1,2} \oplus a_{1,4} \oplus a_{2,4} \mapsto a_{1,2,4}1.1.1 = 0 \oplus 0 \oplus 1 \oplus 1 \oplus 0 \oplus 0 \oplus 0 \oplus 1 \mapsto a_{1,2,4} = 1$
When $x_1 = x_3 = x_4 = 1$ and $x_2 = 0$, $a_{1,3,4}x_1x_3x_4 = 1 \oplus a_0 \oplus a_1 \oplus a_3 \oplus a_4 \oplus a_{1,3} \oplus a_{1,4} \oplus a_{3,4} \mapsto a_{1,3,4}1.1.1 = 1 \oplus 0 \oplus 1 \oplus 0 \oplus 0 \oplus 1 \oplus 0 \oplus 1 \mapsto a_{1,3,4} = 0$
When $x_2 = x_3 = x_4 = 1$ and $x_1 = 0$, $a_{2,3,4}x_2x_3x_4 = 0 \oplus a_0 \oplus a_2 \oplus a_3 \oplus a_4 \oplus a_{2,3} \oplus a_{2,4} \oplus a_{3,4} \mapsto a_{2,3,4}1.1.1 = 0 \oplus 0 \oplus 1 \oplus 0 \oplus 0 \oplus 0 \oplus 1 \oplus 1 \mapsto a_{2,3,4} = 1$
When $x_1 = x_2 = x_3 = x_4 = 1$, $a_{1,2,3,4}x_1x_2x_3x_4 = 1 \oplus a_0 \oplus a_2 \oplus a_3 \oplus a_4 \oplus a_{1,2} \oplus a_{1,3} \oplus a_{1,4} \oplus a_{2,3} \oplus a_{2,4} \oplus a_{3,4} \oplus a_{1,2,3} \oplus a_{1,2,4} \oplus a_{1,3,4} \oplus a_{2,3,4} \mapsto a_{1,2,3,4}1.1.1.1 = 1 \oplus 0 \oplus 1 \oplus 1 \oplus 0 \oplus 0 \oplus 0 \oplus 1 \oplus 0 \oplus 0 \oplus 1 \oplus 1 \oplus 0 \oplus 1 \oplus 0 \oplus 1 \mapsto a_{1,2,3,4} = 0$

The following 3rd nonlinear Boolean function is derived from substituting all coefficients into the 4-variable affine function:
$0.(x_1x_2x_3x_4) \oplus 1.(x_2x_3x_4) \oplus 0.(x_1x_3x_4) \oplus 1.(x_1x_2x_4) \oplus 0.(x_1x_2x_3) \oplus 1.(x_3x_4) \oplus 1.(x_2x_4) \oplus 0.(x_2x_3) \oplus 0.(x_1x_4) + 1.(x_1x_3) \oplus 0.(x_1x_2) \oplus 0.x_4 \oplus 0.x_3 \oplus 1.x_2 \oplus 1.x_1 \oplus 0 = f_3(x_4x_3x_2x_1) = x_2x_3x_4 \oplus x_1x_2x_4 \oplus x_3x_4 \oplus x_2x_4 \oplus x_1x_3 \oplus x_2 \oplus x_1$

The nonlinear Boolean function construction (Nf_4):

$a_{1,2,3,4}x_1x_2x_3x_4 + a_{2,3,4}x_2x_3x_4 + a_{1,3,4}x_1x_3x_4 + a_{1,2,4}x_1x_2x_4 + a_{1,2,3}x_1x_2x_3 + a_{3,4}x_3x_4 + a_{2,4}x_2x_4 + a_{2,3}x_2x_3 + a_{1,4}x_1x_4 + a_{1,3}x_1x_3 + a_{1,2}x_1x_2 + a_4x_4 + a_3x_3 + a_2x_2 + a_1x_1 + a_0 = LCf_4$ .... equation no. (4)

Table V: Inputs of equation number (4)

	Affine coordinate vector				Component	
	X_4	X_3	X_2	X_1	LCf_4	
a_i	0	0	0	0	0	L_i
	0	0	0	1	0	
	0	0	1	0	0	
	0	0	1	1	1	
	0	1	0	0	1	
	0	1	0	1	1	
	0	1	1	0	1	
	0	1	1	1	1	
	1	0	0	0	1	
	1	0	0	1	1	
	1	0	1	0	0	
	1	0	1	1	0	
	1	1	0	0	0	
	1	1	0	1	1	
	1	1	1	0	0	
	1	1	1	1	0	

To calculate the coefficients of equation (4), let's successively substitute the affine coordinate vector on the left side of the equation and the component vector on the right side of the equation. This process has to be repeated 16 times to get 16 coefficients. For instance, when $x_1 = x_2 = x_3 = x_4 = 0$ and $L_0 = 0$. The equation returns $a_0 = 0$ for the 1st input string $\langle 0000 \rangle$ and its corresponding component vector $\langle 0 \rangle$. Similarly, the rest of the coefficients are calculated as follows:

When $x_1 = 1$ and $x_2 = x_3 = x_4 = 0$, $a_1x_1 = 0 \oplus a_0 \mapsto a_1.1 = 0 \oplus 0 \mapsto a_1 = 0$
When $x_2 = 1$ and $x_1 = x_3 = x_4 = 0$, $a_2x_2 = 0 \oplus a_0 \mapsto a_2.1 = 0 \oplus 0 \mapsto a_2 = 0$
When $x_3 = 1$ and $x_1 = x_2 = x_4 = 0$, $a_3x_3 = 1 \oplus a_0 \mapsto a_3.1 = 1 \oplus 0 \mapsto a_3 = 1$
When $x_4 = 1$ and $x_1 = x_2 = x_3 = 0$, $a_4x_4 = 1 \oplus a_0 \mapsto a_4.1 = 1 \oplus 0 \mapsto a_4 = 1$
When $x_1 = x_2 = 1$ and $x_3 = x_4 = 0$, $a_{1,2}x_1x_2 = 1 \oplus 0 \oplus 0 \oplus 0 \mapsto a_{1,2}.1.1 = 1 \mapsto a_{1,2} = 1$
When $x_1 = x_3 = 1$ and $x_2 = x_4 = 0$, $a_{1,3}x_1x_3 = 1 \oplus 0 \oplus 0 \oplus 1 \mapsto a_{1,3}.1.1 = 0 \mapsto a_{1,3} = 0$
When $x_1 = x_4 = 1$ and $x_2 = x_3 = 0$, $a_{1,4}x_1x_4 = 1 \oplus 0 \oplus 0 \oplus 1 \mapsto a_{1,4}.1.1 = 0 \mapsto a_{1,4} = 0$
When $x_2 = x_3 = 1$ and $x_1 = x_4 = 0$, $a_{2,3}x_2x_3 = 1 \oplus 0 \oplus 0 \oplus 1 \mapsto a_{2,3}.1.1 = 0 \mapsto a_{2,3} = 0$
When $x_2 = x_4 = 1$ and $x_1 = x_3 = 0$, $a_{2,4}x_2x_4 = 0 \oplus 0 \oplus 0 \oplus 1 \mapsto a_{2,4}.1.1 = 1 \mapsto a_{2,4} = 1$
When $x_3 = x_4 = 1$ and $x_1 = x_2 = 0$, $a_{3,4}x_3x_4 = 0 \oplus 0 \oplus 1 \oplus 1 \mapsto a_{3,4}.1.1 = 0 \mapsto a_{3,4} = 0$
When $x_1 = x_2 = x_3 = 1$ and $x_4 = 0$, $a_{1,2,3}x_1x_2x_3 = 1 \oplus a_0 \oplus a_1 \oplus a_2 \oplus a_3 \oplus a_{1,2} \oplus a_{1,3} \oplus a_{2,3} \mapsto a_{1,2,3}1.1.1 = 1 \oplus 0 \oplus 0 \oplus 0 \oplus 1 \oplus 1 \oplus 0 \oplus 0 \mapsto a_{1,2,3} = 1$
When $x_1 = x_2 = x_4 = 1$ and $x_3 = 0$, $a_{1,2,4}x_1x_2x_4 = 0 \oplus a_0 \oplus a_1 \oplus a_2 \oplus a_4 \oplus a_{1,2} \oplus a_{1,4} \oplus a_{2,4} \mapsto a_{1,2,4}1.1.1 = 0 \oplus 0 \oplus 0 \oplus 0 \oplus 1 \oplus 1 \oplus 0 \oplus 1 \mapsto a_{1,2,4} = 1$
When $x_1 = x_3 = x_4 = 1$ and $x_2 = 0$, $a_{1,3,4}x_1x_3x_4 = 1 \oplus a_0 \oplus a_1 \oplus a_3 \oplus a_4 \oplus a_{1,3} \oplus a_{1,4} \oplus a_{3,4} \mapsto a_{1,3,4}1.1.1 = 1 \oplus 0 \oplus 0 \oplus 1 \oplus 1 \oplus 0 \oplus 0 \oplus 0 \mapsto a_{1,3,4} = 1$
When $x_2 = x_3 = x_4 = 1$ and $x_1 = 0$, $a_{2,3,4}x_2x_3x_4 = 0 \oplus a_0 \oplus a_2 \oplus a_3 \oplus a_4 \oplus a_{2,3} \oplus a_{2,4} \oplus a_{3,4} \mapsto a_{2,3,4}1.1.1 = 0 \oplus 0 \oplus 0 \oplus 1 \oplus 1 \oplus 0 \oplus 1 \oplus 0 \mapsto a_{2,3,4} = 1$
When $x_1 = x_2 = x_3 = x_4 = 1$, $a_{1,2,3,4}x_1x_2x_3x_4 = 0 \oplus a_0 \oplus a_2 \oplus a_3 \oplus a_4 \oplus a_{1,2} \oplus a_{1,3} \oplus a_{1,4} \oplus a_{2,3} \oplus a_{2,4} \oplus a_{3,4} \oplus a_{1,2,3} \oplus a_{1,2,4} \oplus a_{1,3,4} \oplus a_{2,3,4} \mapsto a_{1,2,3,4}1.1.1.1 = 0 \oplus 0 \oplus 0 \oplus 0 \oplus 1 \oplus 1 \oplus 1 \oplus 0 \oplus 0 \oplus 0 \oplus 1 \oplus 0 \oplus 1 \oplus 1 \oplus 1 \oplus 1 \mapsto a_{1,2,3,4} = 0$

The following 4th nonlinear Boolean function is derived from substituting all coefficients into the 4-variable affine function:
$0.(x_1x_2x_3x_4) \oplus 1.(x_2x_3x_4) \oplus 1.(x_1x_3x_4) \oplus 1.(x_1x_2x_4) \oplus 1.(x_1x_2x_3) \oplus 0.(x_3x_4) \oplus 1.(x_2x_4) \oplus 0.(x_2x_3) \oplus 0.(x_1x_4) + 0.(x_1x_3) \oplus 1.(x_1x_2) \oplus 1.x_4 \oplus 1.x_3 \oplus 0.x_2 \oplus 0.x_1 \oplus 0 = f_4(x_4x_3x_2x_1) = x_2x_3x_4 \oplus x_1x_3x_4 \oplus x_1x_2x_4 \oplus x_1x_2x_3 \oplus x_2x_4 \oplus x_1x_2 \oplus x_4 \oplus x_3$

The nonlinear Boolean function construction (Nf_5):

$a_{1,2,3,4}x_1x_2x_3x_4 + a_{2,3,4}x_2x_3x_4 + a_{1,3,4}x_1x_3x_4 + a_{1,2,4}x_1x_2x_4 + a_{1,2,3}x_1x_2x_3 + a_{3,4}x_3x_4 + a_{2,4}x_2x_4 + a_{2,3}x_2x_3 + a_{1,4}x_1x_4 + a_{1,3}x_1x_3 + a_{1,2}x_1x_2 + a_4x_4 + a_3x_3 + a_2x_2 + a_1x_1 + a_0 = LCf_5$ .... equation no. (5)

Table VI: Inputs of equation number (5)

	Affine coordinate vector				Component	
	X_4	X_3	X_2	X_1	LCf_5	
a_i	0	0	0	0	1	L_i
	0	0	0	1	1	
	0	0	1	0	0	
	0	0	1	1	0	
	0	1	0	0	1	
	0	1	0	1	0	
	0	1	1	0	0	
	0	1	1	1	0	
	1	0	0	0	1	
	1	0	0	1	1	
	1	0	1	0	1	
	1	0	1	1	0	
	1	1	0	0	1	
	1	1	0	1	1	
	1	1	1	0	0	
	1	1	1	1	0	

To calculate the coefficients of equation (5), let's successively substitute the affine coordinate vector on the left side of the equation and the component vector on the right side of the equation. This process has to be repeated 16 times to get 16 coefficients. For instance, when $x_1 = x_2 = x_3 = x_4 = 0$ and $L_0 = 1$. The equation returns $a_0 = 1$ for the 1st input string $\langle 0000 \rangle$ and its corresponding component vector $\langle 1 \rangle$. Similarly, the rest of the coefficients are calculated as follows:

When $x_1 = 1$ and $x_2 = x_3 = x_4 = 0$, $a_1x_1 = 1 \oplus a_0 \mapsto a_1.1 = 1 \oplus 1 \mapsto a_1 = 0$
When $x_2 = 1$ and $x_1 = x_3 = x_4 = 0$, $a_2x_2 = 0 \oplus a_0 \mapsto a_2.1 = 0 \oplus 1 \mapsto a_2 = 1$
When $x_3 = 1$ and $x_1 = x_2 = x_4 = 0$, $a_3x_3 = 1 \oplus a_0 \mapsto a_3.1 = 1 \oplus 1 \mapsto a_3 = 0$
When $x_4 = 1$ and $x_1 = x_2 = x_3 = 0$, $a_4x_4 = 1 \oplus a_0 \mapsto a_4.1 = 1 \oplus 1 \mapsto a_4 = 0$
When $x_1 = x_2 = 1$ and $x_3 = x_4 = 0$, $a_{1,2}x_1x_2 = 0 \oplus 1 \oplus 0 \oplus 1 \mapsto a_{1,2}.1.1 = 0 \mapsto a_{1,2} = 0$
When $x_1 = x_3 = 1$ and $x_2 = x_4 = 0$, $a_{1,3}x_1x_3 = 0 \oplus 1 \oplus 0 \oplus 0 \mapsto a_{1,3}.1.1 = 1 \mapsto a_{1,3} = 1$
When $x_1 = x_4 = 1$ and $x_2 = x_3 = 0$, $a_{1,4}x_1x_4 = 1 \oplus 1 \oplus 0 \oplus 0 \mapsto a_{1,4}.1.1 = 0 \mapsto a_{1,4} = 0$
When $x_2 = x_3 = 1$ and $x_1 = x_4 = 0$, $a_{2,3}x_2x_3 = 0 \oplus 1 \oplus 1 \oplus 0 \mapsto a_{2,3}.1.1 = 0 \mapsto a_{2,3} = 0$
When $x_2 = x_4 = 1$ and $x_1 = x_3 = 0$, $a_{2,4}x_2x_4 = 1 \oplus 1 \oplus 1 \oplus 0 \mapsto a_{2,4}.1.1 = 1 \mapsto a_{2,4} = 1$
When $x_3 = x_4 = 1$ and $x_1 = x_2 = 0$, $a_{3,4}x_3x_4 = 1 \oplus 1 \oplus 0 \oplus 0 \mapsto a_{3,4}.1.1 = 0 \mapsto a_{3,4} = 0$
When $x_1 = x_2 = x_3 = 1$ and $x_4 = 0$, $a_{1,2,3}x_1x_2x_3 = 0 \oplus a_0 \oplus a_1 \oplus a_2 \oplus a_3 \oplus a_{1,2} \oplus a_{1,3} \oplus a_{2,3} \mapsto a_{1,2,3}1.1.1 = 0 \oplus 1 \oplus 0 \oplus 1 \oplus 0 \oplus 0 \oplus 1 \oplus 0 \mapsto a_{1,2,3} = 1$
When $x_1 = x_2 = x_4 = 1$ and $x_3 = 0$, $a_{1,2,4}x_1x_2x_4 = 0 \oplus a_0 \oplus a_1 \oplus a_2 \oplus a_4 \oplus a_{1,2} \oplus a_{1,4} \oplus a_{2,4} \mapsto a_{1,2,4}1.1.1 = 0 \oplus 1 \oplus 0 \oplus 1 \oplus 0 \oplus 0 \oplus 0 \oplus 1 \mapsto a_{1,2,4} = 1$
When $x_1 = x_3 = x_4 = 1$ and $x_2 = 0$, $a_{1,3,4}x_1x_3x_4 = 1 \oplus a_0 \oplus a_1 \oplus a_3 \oplus a_4 \oplus a_{1,3} \oplus a_{1,4} \oplus a_{3,4} \mapsto a_{1,3,4}1.1.1 = 1 \oplus 1 \oplus 0 \oplus 0 \oplus 0 \oplus 1 \oplus 0 \oplus 0 \mapsto a_{1,3,4} = 1$
When $x_2 = x_3 = x_4 = 1$ and $x_1 = 0$, $a_{2,3,4}x_2x_3x_4 = 0 \oplus a_0 \oplus a_2 \oplus a_3 \oplus a_4 \oplus a_{2,3} \oplus a_{2,4} \oplus a_{3,4} \mapsto a_{2,3,4}1.1.1 = 0 \oplus 1 \oplus 1 \oplus 0 \oplus 0 \oplus 0 \oplus 1 \oplus 0 \mapsto a_{2,3,4} = 1$
When $x_1 = x_2 = x_3 = x_4 = 1$, $a_{1,2,3,4}x_1x_2x_3x_4 = 0 \oplus a_0 \oplus a_2 \oplus a_3 \oplus a_4 \oplus a_{1,2} \oplus a_{1,3} \oplus a_{1,4} \oplus a_{2,3} \oplus a_{2,4} \oplus a_{3,4} \oplus a_{1,2,3} \oplus a_{1,2,4} \oplus a_{1,3,4} \oplus a_{2,3,4} \mapsto a_{1,2,3,4}1.1.1.1 = 0 \oplus 1 \oplus 0 \oplus 1 \oplus 0 \oplus 0 \oplus 0 \oplus 1 \oplus 0 \oplus 0 \oplus 1 \oplus 0 \oplus 1 \oplus 1 \oplus 1 \oplus 1 \mapsto a_{1,2,3,4} = 0$

The following 5th nonlinear Boolean function is derived from substituting all coefficients into the 4-variable affine function:
$0.(x_1x_2x_3x_4) \oplus 1.(x_2x_3x_4) \oplus 1.(x_1x_3x_4) \oplus 1.(x_1x_2x_4) \oplus 1.(x_1x_2x_3) \oplus 0.(x_3x_4) \oplus 1.(x_2x_4) \oplus 0.(x_2x_3) \oplus 0.(x_1x_4) \oplus 1.(x_1x_3)$
$0.(x_1x_2) \oplus 0.x_4 \oplus 0.x_3 \oplus 1.x_2 \oplus 0.x_1 \oplus 1 = f_5(x_4x_3x_2x_1) = x_2x_3x_4 \oplus x_1x_3x_4 \oplus x_1x_2x_4 \oplus x_1x_2x_3 \oplus x_2x_4 \oplus x_1x_3 \oplus x_2 \oplus 1$

https://dx.doi.org/10.29322/IJSRP.14.01.2024.p14539

The nonlinear Boolean function construction (Nf_6):

$a_{1,2,3,4}x_1x_2x_3x_4 + a_{2,3,4}x_2x_3x_4 + a_{1,3,4}x_1x_3x_4 + a_{1,2,4}x_1x_2x_4 + a_{1,2,3}x_1x_2x_3 + a_{3,4}x_3x_4 + a_{2,4}x_2x_4 + a_{2,3}x_2x_3 + a_{1,4}x_1x_4 + a_{1,3}x_1x_3 + a_{1,2}x_1x_2 + a_4x_4 + a_3x_3 + a_2x_2 + a_1x_1 + a_0 = LCf_6$ .... equation no. (6)

Table VII: Inputs of equation number (6)

	Affine coordinate vector				Component	
	X_4	X_3	X_2	X_1	LCf_6	
a_i	0	0	0	0	0	L_i
	0	0	0	1	0	
	0	0	1	0	0	
	0	0	1	1	0	
	0	1	0	0	1	
	0	1	0	1	1	
	0	1	1	0	1	
	0	1	1	1	0	
	1	0	0	0	0	
	1	0	0	1	0	
	1	0	1	0	1	
	1	0	1	1	1	
	1	1	0	0	1	
	1	1	0	1	1	
	1	1	1	0	0	
	1	1	1	1	1	

To calculate the coefficients of equation (6), let's successively substitute the affine coordinate vector on the left side of the equation and the component vector on the right side of the equation. This process has to be repeated 16 times to get 16 coefficients. For instance, when $x_1 = x_2 = x_3 = x_4 = 0$ and $L_0 = 0$. The equation returns $a_0 = 0$ for the 1st input string $\langle 0000 \rangle$ and its corresponding component vector $\langle 0 \rangle$. Similarly, the rest of the coefficients are calculated as follows:

When $x_1 = 1$ and $x_2 = x_3 = x_4 = 0$, $a_1x_1 = 0 \oplus a_0 \mapsto a_1.1 = 0 \oplus 0 \mapsto a_1 = 0$
When $x_2 = 1$ and $x_1 = x_3 = x_4 = 0$, $a_2x_2 = 0 \oplus a_0 \mapsto a_2.1 = 0 \oplus 0 \mapsto a_2 = 0$
When $x_3 = 1$ and $x_1 = x_2 = x_4 = 0$, $a_3x_3 = 1 \oplus a_0 \mapsto a_3.1 = 1 \oplus 0 \mapsto a_3 = 1$
When $x_4 = 1$ and $x_1 = x_2 = x_3 = 0$, $a_4x_4 = 0 \oplus a_0 \mapsto a_4.1 = 0 \oplus 0 \mapsto a_4 = 0$
When $x_1 = x_2 = 1$ and $x_3 = x_4 = 0$, $a_{1,2}x_1x_2 = 0 \oplus 0 \oplus 0 \oplus 0 \mapsto a_{1,2}.1.1 = 0 \mapsto a_{1,2} = 0$
When $x_1 = x_3 = 1$ and $x_2 = x_4 = 0$, $a_{1,3}x_1x_3 = 1 \oplus 0 \oplus 0 \oplus 1 \mapsto a_{1,3}.1.1 = 0 \mapsto a_{1,3} = 0$
When $x_1 = x_4 = 1$ and $x_2 = x_3 = 0$, $a_{1,4}x_1x_4 = 0 \oplus 0 \oplus 0 \oplus 0 \mapsto a_{1,4}.1.1 = 0 \mapsto a_{1,4} = 0$
When $x_2 = x_3 = 1$ and $x_1 = x_4 = 0$, $a_{2,3}x_2x_3 = 1 \oplus 0 \oplus 0 \oplus 1 \mapsto a_{2,3}.1.1 = 0 \mapsto a_{2,3} = 0$
When $x_2 = x_4 = 1$ and $x_1 = x_3 = 0$, $a_{2,4}x_2x_4 = 1 \oplus 0 \oplus 0 \oplus 0 \mapsto a_{2,4}.1.1 = 1 \mapsto a_{2,4} = 1$
When $x_3 = x_4 = 1$ and $x_1 = x_2 = 0$, $a_{3,4}x_3x_4 = 1 \oplus 0 \oplus 1 \oplus 0 \mapsto a_{3,4}.1.1 = 0 \mapsto a_{3,4} = 0$
When $x_1 = x_2 = x_3 = 1$ and $x_4 = 0$, $a_{1,2,3}x_1x_2x_3 = 0 \oplus a_0 \oplus a_1 \oplus a_2 \oplus a_3 \oplus a_{1,2} \oplus a_{1,3} \oplus a_{2,3} \mapsto a_{1,2,3}1.1.1 = 0 \oplus 0 \oplus 0 \oplus 0 \oplus 1 \oplus 0 \oplus 0 \oplus 0 \mapsto a_{1,2,3} = 1$
When $x_1 = x_2 = x_4 = 1$ and $x_3 = 0$, $a_{1,2,4}x_1x_2x_4 = 1 \oplus a_0 \oplus a_1 \oplus a_2 \oplus a_4 \oplus a_{1,2} \oplus a_{1,4} \oplus a_{2,4} \mapsto a_{1,2,4}1.1.1 = 1 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 1 \mapsto a_{1,2,4} = 0$
When $x_1 = x_3 = x_4 = 1$ and $x_2 = 0$, $a_{1,3,4}x_1x_3x_4 = 1 \oplus a_0 \oplus a_1 \oplus a_3 \oplus a_4 \oplus a_{1,3} \oplus a_{1,4} \oplus a_{3,4} \mapsto a_{1,3,4}1.1.1 = 1 \oplus 0 \oplus 0 \oplus 1 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \mapsto a_{1,3,4} = 0$
When $x_2 = x_3 = x_4 = 1$ and $x_1 = 0$, $a_{2,3,4}x_2x_3x_4 = 0 \oplus a_0 \oplus a_2 \oplus a_3 \oplus a_4 \oplus a_{2,3} \oplus a_{2,4} \oplus a_{3,4} \mapsto a_{2,3,4}1.1.1 = 0 \oplus 0 \oplus 0 \oplus 1 \oplus 0 \oplus 0 \oplus 1 \oplus 0 \mapsto a_{2,3,4} = 0$
When $x_1 = x_2 = x_3 = x_4 = 1$, $a_{1,2,3,4}x_1x_2x_3x_4 = 1 \oplus a_0 \oplus a_2 \oplus a_3 \oplus a_4 \oplus a_{1,2} \oplus a_{1,3} \oplus a_{1,4} \oplus a_{2,3} \oplus a_{2,4} \oplus a_{3,4} \oplus a_{1,2,3} \oplus a_{1,2,4} \oplus a_{1,3,4} \oplus a_{2,3,4} \mapsto a_{1,2,3,4}1.1.1.1 = 1 \oplus 0 \oplus 0 \oplus 0 \oplus 1 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 1 \oplus 0 \oplus 1 \oplus 0 \oplus 0 \oplus 0 \mapsto a_{1,2,3,4} = 0$

The following 6th nonlinear Boolean function is derived from substituting all coefficients into the 4-variable affine function:
$0.(x_1x_2x_3x_4) \oplus 0.(x_2x_3x_4) \oplus 0.(x_1x_3x_4) \oplus 0.(x_1x_2x_4) \oplus 1.(x_1x_2x_3) \oplus 0.(x_3x_4) \oplus 1.(x_2x_4) \oplus 0.(x_2x_3) \oplus 0.(x_1x_4) \oplus 0.(x_1x_3) \oplus 0.(x_1x_2) \oplus 0.x_4 \oplus 1.x_3 \oplus 0.x_2 \oplus 0.x_1 \oplus 0 = f_6(x_4x_3x_2x_1) = x_1x_2x_3 \oplus x_2x_4 \oplus x_3$

The nonlinear Boolean function construction (Nf_7):

$a_{1,2,3,4}x_1x_2x_3x_4 + a_{2,3,4}x_2x_3x_4 + a_{1,3,4}x_1x_3x_4 + a_{1,2,4}x_1x_2x_4 + a_{1,2,3}x_1x_2x_3 + a_{3,4}x_3x_4 + a_{2,4}x_2x_4 + a_{2,3}x_2x_3 + a_{1,4}x_1x_4 + a_{1,3}x_1x_3 + a_{1,2}x_1x_2 + a_4x_4 + a_3x_3 + a_2x_2 + a_1x_1 + a_0 = LCf_7$ ………………………………………………… equation no. (7)

Table VIII: Inputs of equation number (7)

	Affine coordinate vector				Component	
	X_4	X_3	X_2	X_1	LCf_7	
	0	0	0	0	0	
	0	0	0	1	1	
	0	0	1	0	1	
	0	0	1	1	1	
	0	1	0	0	0	
	0	1	0	1	0	
	0	1	1	0	1	
	0	1	1	1	0	
a_i	1	0	0	0	1	L_i
	1	0	0	1	0	
	1	0	1	0	1	
	1	0	1	1	1	
	1	1	0	0	0	
	1	1	0	1	1	
	1	1	1	0	0	
	1	1	1	1	0	

To calculate the coefficients of equation (7), let's successively substitute the affine coordinate vector on the left side of the equation and the component vector on the right side of the equation. This process has to be repeated 16 times to get 16 coefficients. For instance, when $x_1 = x_2 = x_3 = x_4 = 0$ and $L_0 = 0$. The equation returns $a_0 = 0$ for the 1st input string $\langle 0000 \rangle$ and its corresponding component vector $\langle 0 \rangle$. Similarly, the rest of the coefficients are calculated as follows:

When $x_1 = 1$ and $x_2 = x_3 = x_4 = 0$, $a_1x_1 = 1 \oplus a_0 \mapsto a_1.1 = 1 \oplus 0 \mapsto a_1 = 1$
When $x_2 = 1$ and $x_1 = x_3 = x_4 = 0$, $a_2x_2 = 1 \oplus a_0 \mapsto a_2.1 = 1 \oplus 0 \mapsto a_2 = 1$
When $x_3 = 1$ and $x_1 = x_2 = x_4 = 0$, $a_3x_3 = 0 \oplus a_0 \mapsto a_3.1 = 0 \oplus 0 \mapsto a_3 = 0$
When $x_4 = 1$ and $x_1 = x_2 = x_3 = 0$, $a_4x_4 = 1 \oplus a_0 \mapsto a_4.1 = 1 \oplus 0 \mapsto a_4 = 1$
When $x_1 = x_2 = 1$ and $x_3 = x_4 = 0$, $a_{1,2}x_1x_2 = 1 \oplus 0 \oplus 1 \oplus 1 \mapsto a_{1,2}.1.1 = 1 \mapsto a_{1,2} = 1$
When $x_1 = x_3 = 1$ and $x_2 = x_4 = 0$, $a_{1,3}x_1x_3 = 0 \oplus 0 \oplus 1 \oplus 0 \mapsto a_{1,3}.1.1 = 1 \mapsto a_{1,3} = 1$
When $x_1 = x_4 = 1$ and $x_2 = x_3 = 0$, $a_{1,4}x_1x_4 = 0 \oplus 0 \oplus 1 \oplus 1 \mapsto a_{1,4}.1.1 = 0 \mapsto a_{1,4} = 0$
When $x_2 = x_3 = 1$ and $x_1 = x_4 = 0$, $a_{2,3}x_2x_3 = 1 \oplus 0 \oplus 1 \oplus 0 \mapsto a_{2,3}.1.1 = 0 \mapsto a_{2,3} = 0$
When $x_2 = x_4 = 1$ and $x_1 = x_3 = 0$, $a_{2,4}x_2x_4 = 1 \oplus 0 \oplus 1 \oplus 1 \mapsto a_{2,4}.1.1 = 1 \mapsto a_{2,4} = 1$
When $x_3 = x_4 = 1$ and $x_1 = x_2 = 0$, $a_{3,4}x_3x_4 = 0 \oplus 0 \oplus 0 \oplus 1 \mapsto a_{3,4}.1.1 = 1 \mapsto a_{3,4} = 1$
When $x_1 = x_2 = x_3 = 1$ and $x_4 = 0$, $a_{1,2,3}x_1x_2x_3 = 0 \oplus a_0 \oplus a_1 \oplus a_2 \oplus a_3 \oplus a_{1,2} \oplus a_{1,3} \oplus a_{2,3} \mapsto a_{1,2,3}1.1.1 = 0 \oplus 0 \oplus 1 \oplus 1 \oplus 0 \oplus 1 \oplus 1 \oplus 0 \mapsto a_{1,2,3} = 0$
When $x_1 = x_2 = x_4 = 1$ and $x_3 = 0$, $a_{1,2,4}x_1x_2x_4 = 1 \oplus a_0 \oplus a_1 \oplus a_2 \oplus a_4 \oplus a_{1,2} \oplus a_{1,4} \oplus a_{2,4} \mapsto a_{1,2,4}1.1.1 = 1 \oplus 0 \oplus 1 \oplus 1 \oplus 1 \oplus 1 \oplus 0 \oplus 1 \mapsto a_{1,2,4} = 0$
When $x_1 = x_3 = x_4 = 1$ and $x_2 = 0$, $a_{1,3,4}x_1x_3x_4 = 1 \oplus a_0 \oplus a_1 \oplus a_3 \oplus a_4 \oplus a_{1,3} \oplus a_{1,4} \oplus a_{3,4} \mapsto a_{1,3,4}1.1.1 = 1 \oplus 0 \oplus 1 \oplus 0 \oplus 1 \oplus 1 \oplus 0 \oplus 1 \mapsto a_{1,3,4} = 1$
When $x_2 = x_3 = x_4 = 1$ and $x_1 = 0$, $a_{2,3,4}x_2x_3x_4 = 0 \oplus a_0 \oplus a_2 \oplus a_3 \oplus a_4 \oplus a_{2,3} \oplus a_{2,4} \oplus a_{3,4} \mapsto a_{2,3,4}1.1.1 = 0 \oplus 0 \oplus 1 \oplus 0 \oplus 1 \oplus 0 \oplus 1 \oplus 1 \mapsto a_{2,3,4} = 0$
When $x_1 = x_2 = x_3 = x_4 = 1$, $a_{1,2,3,4}x_1x_2x_3x_4 = 0 \oplus a_0 \oplus a_2 \oplus a_3 \oplus a_4 \oplus a_{1,2} \oplus a_{1,3} \oplus a_{1,4} \oplus a_{2,3} \oplus a_{2,4} \oplus a_{3,4} \oplus a_{1,2,3} \oplus a_{1,2,4} \oplus a_{1,3,4} \oplus a_{2,3,4} \mapsto a_{1,2,3,4}1.1.1.1 = 0 \oplus 1 \oplus 0 \oplus 1 \oplus 0 \oplus 0 \oplus 0 \oplus 1 \oplus 0 \oplus 0 \oplus 1 \oplus 0 \oplus 1 \oplus 1 \oplus 1 \oplus 1 \mapsto a_{1,2,3,4} = 0$

The following 7th nonlinear Boolean function is derived from substituting all coefficients into the 4-variable affine function:
$0.(x_1x_2x_3x_4) \oplus 0.(x_2x_3x_4) \oplus 1.(x_1x_3x_4) \oplus 0.(x_1x_2x_4) \oplus 0.(x_1x_2x_3) \oplus 1.(x_3x_4) \oplus 1.(x_2x_4) \oplus 0.(x_2x_3) \oplus 0.(x_1x_4) \oplus 1.(x_1x_3) \oplus 1.(x_1x_2) \oplus 1.x_4 \oplus 0.x_3 \oplus 1.x_2 \oplus 1.x_1 \oplus 0 = f_7(x_4x_3x_2x_1 = x_1x_3x_4 \oplus x_3x_4 \oplus x_2x_4 \oplus x_1x_3 \oplus x_1x_2 \oplus x_4 \oplus x_2 \oplus x_1$

The nonlinear Boolean function construction (Nf_8):

$a_{1,2,3,4}x_1x_2x_3x_4 + a_{2,3,4}x_2x_3x_4 + a_{1,3,4}x_1x_3x_4 + a_{1,2,4}x_1x_2x_4 + a_{1,2,3}x_1x_2x_3 + a_{3,4}x_3x_4 + a_{2,4}x_2x_4 + a_{2,3}x_2x_3 + a_{1,4}x_1x_4 + a_{1,3}x_1x_3 + a_{1,2}x_1x_2 + a_4x_4 + a_3x_3 + a_2x_2 + a_1x_1 + a_0 = LCf_8$ .... equation no. (8)

Table IX: Inputs of equation number (8)

	Affine coordinate vector				Component	
	X_4	X_3	X_2	X_1	LCf_8	
a_i	0	0	0	0	1	L_i
	0	0	0	1	1	
	0	0	1	0	0	
	0	0	1	1	0	
	0	1	0	0	0	
	0	1	0	1	1	
	0	1	1	0	1	
	0	1	1	1	0	
	1	0	0	0	1	
	1	0	0	1	1	
	1	0	1	0	0	
	1	0	1	1	1	
	1	1	0	0	0	
	1	1	0	1	0	
	1	1	1	0	0	
	1	1	1	1	1	

To calculate the coefficients of equation (8), let's successively substitute the affine coordinate vector on the left side of the equation and the component vector on the right side of the equation. This process has to be repeated 16 times to get 16 coefficients. For instance, when $x_1 = x_2 = x_3 = x_4 = 0$ and $L_0 = 1$. The equation returns $a_0 = 1$ for the 1st input string $\langle 0000 \rangle$ and its corresponding component vector $\langle 1 \rangle$. Similarly, the rest of the coefficients are calculated as follows:

When $x_1 = 1$ and $x_2 = x_3 = x_4 = 0$, $a_1x_1 = 1 \oplus a_0 \mapsto a_1.1 = 1 \oplus 1 \mapsto a_1 = 0$
When $x_2 = 1$ and $x_1 = x_3 = x_4 = 0$, $a_2x_2 = 0 \oplus a_0 \mapsto a_2.1 = 0 \oplus 1 \mapsto a_2 = 1$
When $x_3 = 1$ and $x_1 = x_2 = x_4 = 0$, $a_3x_3 = 0 \oplus a_0 \mapsto a_3.1 = 0 \oplus 1 \mapsto a_3 = 1$
When $x_4 = 1$ and $x_1 = x_2 = x_3 = 0$, $a_4x_4 = 1 \oplus a_0 \mapsto a_4.1 = 1 \oplus 1 \mapsto a_4 = 0$
When $x_1 = x_2 = 1$ and $x_3 = x_4 = 0$, $a_{1,2}x_1x_2 = 0 \oplus 1 \oplus 0 \oplus 1 \mapsto a_{1,2}.1.1 = 1 \mapsto a_{1,2} = 0$
When $x_1 = x_3 = 1$ and $x_2 = x_4 = 0$, $a_{1,3}x_1x_3 = 1 \oplus 1 \oplus 0 \oplus 1 \mapsto a_{1,3}.1.1 = 1 \mapsto a_{1,3} = 1$
When $x_1 = x_4 = 1$ and $x_2 = x_3 = 0$, $a_{1,4}x_1x_4 = 1 \oplus 1 \oplus 0 \oplus 0 \mapsto a_{1,4}.1.1 = 0 \mapsto a_{1,4} = 0$
When $x_2 = x_3 = 1$ and $x_1 = x_4 = 0$, $a_{2,3}x_2x_3 = 1 \oplus 1 \oplus 1 \oplus 1 \mapsto a_{2,3}.1.1 = 0 \mapsto a_{2,3} = 0$
When $x_2 = x_4 = 1$ and $x_1 = x_3 = 0$, $a_{2,4}x_2x_4 = 0 \oplus 1 \oplus 1 \oplus 0 \mapsto a_{2,4}.1.1 = 0 \mapsto a_{2,4} = 0$
When $x_3 = x_4 = 1$ and $x_1 = x_2 = 0$, $a_{3,4}x_3x_4 = 0 \oplus 1 \oplus 1 \oplus 0 \mapsto a_{3,4}.1.1 = 0 \mapsto a_{3,4} = 0$
When $x_1 = x_2 = x_3 = 1$ and $x_4 = 0$, $a_{1,2,3}x_1x_2x_3 = 0 \oplus a_0 \oplus a_1 \oplus a_2 \oplus a_3 \oplus a_{1,2} \oplus a_{1,3} \oplus a_{2,3} \mapsto a_{1,2,3}1.1.1 = 0 \oplus 1 \oplus 0 \oplus 1 \oplus 1 \oplus 0 \oplus 1 \oplus 0 \mapsto a_{1,2,3} = 0$
When $x_1 = x_2 = x_4 = 1$ and $x_3 = 0$, $a_{1,2,4}x_1x_2x_4 = 1 \oplus a_0 \oplus a_1 \oplus a_2 \oplus a_4 \oplus a_{1,2} \oplus a_{1,4} \oplus a_{2,4} \mapsto a_{1,2,4}1.1.1 = 1 \oplus 1 \oplus 0 \oplus 1 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \mapsto a_{1,2,4} = 1$
When $x_1 = x_3 = x_4 = 1$ and $x_2 = 0$, $a_{1,3,4}x_1x_3x_4 = 0 \oplus a_0 \oplus a_1 \oplus a_3 \oplus a_4 \oplus a_{1,3} \oplus a_{1,4} \oplus a_{3,4} \mapsto a_{1,3,4}1.1.1 = 0 \oplus 1 \oplus 0 \oplus 1 \oplus 0 \oplus 1 \oplus 0 \oplus 0 \mapsto a_{1,3,4} = 1$
When $x_2 = x_3 = x_4 = 1$ and $x_1 = 0$, $a_{2,3,4}x_2x_3x_4 = 0 \oplus a_0 \oplus a_2 \oplus a_3 \oplus a_4 \oplus a_{2,3} \oplus a_{2,4} \oplus a_{3,4} \mapsto a_{2,3,4}1.1.1 = 0 \oplus 1 \oplus 1 \oplus 1 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \mapsto a_{2,3,4} = 1$
When $x_1 = x_2 = x_3 = x_4 = 1$, $a_{1,2,3,4}x_1x_2x_3x_4 = 1 \oplus a_0 \oplus a_2 \oplus a_3 \oplus a_4 \oplus a_{1,2} \oplus a_{1,3} \oplus a_{1,4} \oplus a_{2,3} \oplus a_{2,4} \oplus a_{3,4} \oplus a_{1,2,3} \oplus a_{1,2,4} \oplus a_{1,3,4} \oplus a_{2,3,4} \mapsto a_{1,2,3,4}1.1.1.1 = 1 \oplus 1 \oplus 0 \oplus 1 \oplus 1 \oplus 0 \oplus 0 \oplus 1 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 1 \oplus 1 \oplus 1 \mapsto a_{1,2,3,4} = 0$

The following 8th nonlinear Boolean function is derived from substituting all coefficients into the 4-variable affine function:
$0.(x_1x_2x_3x_4) \oplus 1.(x_2x_3x_4) \oplus 1.(x_1x_3x_4) \oplus 1.(x_1x_2x_4) \oplus 0.(x_1x_2x_3) \oplus 0.(x_3x_4) \oplus 0.(x_2x_4) \oplus 0.(x_2x_3) \oplus 0.(x_1x_4) \oplus 1.(x_1x_3) \oplus 0.(x_1x_2) \oplus 0.x_4 \oplus 1.x_3 \oplus 1.x_2 \oplus 0.x_1 \oplus 1 = f_8 = (x_4x_3x_2x_1) = x_2x_3x_4 \oplus x_1x_3x_4 \oplus x_1x_2x_4 \oplus x_1x_3 \oplus x_3 \oplus x_2 \oplus 1$

https://dx.doi.org/10.29322/IJSRP.14.01.2024.p14539

The nonlinear Boolean function construction (Nf_9):

$a_{1,2,3,4}x_1x_2x_3x_4 + a_{2,3,4}x_2x_3x_4 + a_{1,3,4}x_1x_3x_4 + a_{1,2,4}x_1x_2x_4 + a_{1,2,3}x_1x_2x_3 + a_{3,4}x_3x_4 + a_{2,4}x_2x_4 + a_{2,3}x_2x_3 + a_{1,4}x_1x_4 + a_{1,3}x_1x_3 + a_{1,2}x_1x_2 + a_4x_4 + a_3x_3 + a_2x_2 + a_1x_1 + a_0 = LCf_9$ .... equation no. (9)

Table X: Inputs of equation number (9)

	Affine coordinate vector				Component	
	X_4	X_3	X_2	X_1	LCf_9	
a_i	0	0	0	0	1	L_i
	0	0	0	1	0	
	0	0	1	0	1	
	0	0	1	1	1	
	0	1	0	0	1	
	0	1	0	1	0	
	0	1	1	0	1	
	0	1	1	1	0	
	1	0	0	0	0	
	1	0	0	1	1	
	1	0	1	0	0	
	1	0	1	1	1	
	1	1	0	0	1	
	1	1	0	1	0	
	1	1	1	0	0	
	1	1	1	1	0	

To calculate the coefficients of equation (9), let's successively substitute the affine coordinate vector on the left side of the equation and the component vector on the right side of the equation. This process has to be repeated 16 times to get 16 coefficients. For instance, when $x_1 = x_2 = x_3 = x_4 = 0$ and $L_0 = 1$. The equation returns $a_0 = 1$ for the 1st input string $\langle 0000 \rangle$ and its corresponding component vector $\langle 1 \rangle$. Similarly, the rest of the coefficients are calculated as follows:

When $x_1 = 1$ and $x_2 = x_3 = x_4 = 0$, $a_1x_1 = 0 \oplus a_0 \Rightarrow a_1.1 = 0 \oplus 1 \Rightarrow a_1 = 1$
When $x_2 = 1$ and $x_1 = x_3 = x_4 = 0$, $a_2x_2 = 1 \oplus a_0 \Rightarrow a_2.1 = 1 \oplus 1 \Rightarrow a_2 = 0$
When $x_3 = 1$ and $x_1 = x_2 = x_4 = 0$, $a_3x_3 = 1 \oplus a_0 \Rightarrow a_3.1 = 1 \oplus 1 \Rightarrow a_3 = 0$
When $x_4 = 1$ and $x_1 = x_2 = x_3 = 0$, $a_4x_4 = 0 \oplus a_0 \Rightarrow a_4.1 = 0 \oplus 1 \Rightarrow a_4 = 1$
When $x_1 = x_2 = 1$ and $x_3 = x_4 = 0$, $a_{1,2}x_1x_2 = 1 \oplus 1 \oplus 1 \oplus 0 \Rightarrow a_{1,2}.1.1 = 1 \Rightarrow a_{1,2} = 1$
When $x_1 = x_3 = 1$ and $x_2 = x_4 = 0$, $a_{1,3}x_1x_3 = 0 \oplus 1 \oplus 1 \oplus 0 \Rightarrow a_{1,3}.1.1 = 0 \Rightarrow a_{1,3} = 0$
When $x_1 = x_4 = 1$ and $x_2 = x_3 = 0$, $a_{1,4}x_1x_4 = 1 \oplus 1 \oplus 1 \oplus 1 \Rightarrow a_{1,4}.1.1 = 0 \Rightarrow a_{1,4} = 0$
When $x_2 = x_3 = 1$ and $x_1 = x_4 = 0$, $a_{2,3}x_2x_3 = 1 \oplus 1 \oplus 0 \oplus 0 \Rightarrow a_{2,3}.1.1 = 0 \Rightarrow a_{2,3} = 0$
When $x_2 = x_4 = 1$ and $x_1 = x_3 = 0$, $a_{2,4}x_2x_4 = 0 \oplus 1 \oplus 0 \oplus 1 \Rightarrow a_{2,4}.1.1 = 0 \Rightarrow a_{2,4} = 0$
When $x_3 = x_4 = 1$ and $x_1 = x_2 = 0$, $a_{3,4}x_3x_4 = 1 \oplus 1 \oplus 0 \oplus 1 \Rightarrow a_{3,4}.1.1 = 1 \Rightarrow a_{3,4} = 1$
When $x_1 = x_2 = x_3 = 1$ and $x_4 = 0$, $a_{1,2,3}x_1x_2x_3 = 0 \oplus a_0 \oplus a_1 \oplus a_2 \oplus a_3 \oplus a_{1,2} \oplus a_{1,3} \oplus a_{2,3} \Rightarrow a_{1,2,3}1.1.1 = 0 \oplus 1 \oplus 1 \oplus 0 \oplus 0 \oplus 1 \oplus 0 \oplus 0 \Rightarrow a_{1,2,3} = 1$
When $x_1 = x_2 = x_4 = 1$ and $x_3 = 0$, $a_{1,2,4}x_1x_2x_4 = 1 \oplus a_0 \oplus a_1 \oplus a_2 \oplus a_4 \oplus a_{1,2} \oplus a_{1,4} \oplus a_{2,4} \Rightarrow a_{1,2,4}1.1.1 = 1 \oplus 1 \oplus 1 \oplus 0 \oplus 1 \oplus 1 \oplus 0 \oplus 0 \Rightarrow a_{1,2,4} = 1$
When $x_1 = x_3 = x_4 = 1$ and $x_2 = 0$, $a_{1,3,4}x_1x_3x_4 = 0 \oplus a_0 \oplus a_1 \oplus a_3 \oplus a_4 \oplus a_{1,3} \oplus a_{1,4} \oplus a_{3,4} \Rightarrow a_{1,3,4}1.1.1 = 0 \oplus 1 \oplus 1 \oplus 0 \oplus 1 \oplus 0 \oplus 0 \oplus 1 \Rightarrow a_{1,3,4} = 0$
When $x_2 = x_3 = x_4 = 1$ and $x_1 = 0$, $a_{2,3,4}x_2x_3x_4 = 0 \oplus a_0 \oplus a_2 \oplus a_3 \oplus a_4 \oplus a_{2,3} \oplus a_{2,4} \oplus a_{3,4} \Rightarrow a_{2,3,4}1.1.1 = 0 \oplus 1 \oplus 0 \oplus 0 \oplus 1 \oplus 0 \oplus 0 \oplus 1 \Rightarrow a_{2,3,4} = 1$
When $x_1 = x_2 = x_3 = x_4 = 1$, $a_{1,2,3,4}x_1x_2x_3x_4 = 0 \oplus a_0 \oplus a_2 \oplus a_3 \oplus a_4 \oplus a_{1,2} \oplus a_{1,3} \oplus a_{1,4} \oplus a_{2,3} \oplus a_{2,4} \oplus a_{3,4} \oplus a_{1,2,3} \oplus a_{1,2,4} \oplus a_{1,3,4} \oplus a_{2,3,4} \Rightarrow a_{1,2,3,4}1.1.1.1 = 0 \oplus 1 \oplus 1 \oplus 0 \oplus 0 \oplus 1 \oplus 1 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 1 \oplus 1 \oplus 1 \oplus 0 \oplus 1 \Rightarrow a_{1,2,3,4} = 0$

The following 9th nonlinear Boolean function is derived from substituting all coefficients into the 4-variable affine function:
$0.(x_1x_2x_3x_4) \oplus 1.(x_2x_3x_4) \oplus 0.(x_1x_3x_4) \oplus 1.(x_1x_2x_4) \oplus 1.(x_1x_2x_3) \oplus 1.(x_3x_4) \oplus 0.(x_2x_4) \oplus 0.(x_2x_3) \oplus 0.(x_1x_4) \oplus 0.(x_1x_3) \oplus 1.(x_1x_2) \oplus 1.x_4 \oplus 0.x_3 \oplus 0.x_2 \oplus 1.x_1 \oplus 1 = f_9\,(x_4x_3x_2x_1) = x_2x_3x_4 \oplus x_1x_2x_4 \oplus x_1x_2x_3 \oplus x_3x_4 \oplus x_1x_2 \oplus x_4 \oplus x_1 \oplus 1$

https://dx.doi.org/10.29322/IJSRP.14.01.2024.p14539

The nonlinear Boolean function construction (Nf_{10}):

$a_{1,2,3,4}x_1x_2x_3x_4 + a_{2,3,4}x_2x_3x_4 + a_{1,3,4}x_1x_3x_4 + a_{1,2,4}x_1x_2x_4 + a_{1,2,3}x_1x_2x_3 + a_{3,4}x_3x_4 + a_{2,4}x_2x_4 + a_{2,3}x_2x_3 + a_{1,4}x_1x_4 + a_{1,3}x_1x_3 + a_{1,2}x_1x_2 + a_4x_4 + a_3x_3 + a_2x_2 + a_1x_1 + a_0 = LCf_{10}$ .... equation no. (10)

Table XI: Inputs of equation number (10)

	Affine coordinate vector				Component	
	X_4	X_3	X_2	X_1	LCf_{10}	
a_i	0	0	0	0	0	L_i
	0	0	0	1	1	
	0	0	1	0	1	
	0	0	1	1	1	
	0	1	0	0	1	
	0	1	0	1	1	
	0	1	1	0	0	
	0	1	1	1	0	
	1	0	0	0	1	
	1	0	0	1	0	
	1	0	1	0	0	
	1	0	1	1	0	
	1	1	0	0	1	
	1	1	0	1	0	
	1	1	1	0	0	
	1	1	1	1	1	

To calculate the coefficients of equation (10), let's successively substitute the affine coordinate vector on the left side of the equation and the component vector on the right side of the equation. This process has to be repeated 16 times to get 16 coefficients. For instance, when $x_1 = x_2 = x_3 = x_4 = 0$ and $L_0 = 0$. The equation returns $a_0 = 0$ for the 1st input string $\langle 0000 \rangle$ and its corresponding component vector $\langle 0 \rangle$. Similarly, the rest of the coefficients are calculated as follows:

When $x_1 = 1$ and $x_2 = x_3 = x_4 = 0$, $a_1x_1 = 1 \oplus a_0 \mapsto a_1.1 = 1 \oplus 0 \mapsto a_1 = 1$
When $x_2 = 1$ and $x_1 = x_3 = x_4 = 0$, $a_2x_2 = 1 \oplus a_0 \mapsto a_2.1 = 1 \oplus 0 \mapsto a_2 = 1$
When $x_3 = 1$ and $x_1 = x_2 = x_4 = 0$, $a_3x_3 = 1 \oplus a_0 \mapsto a_3.1 = 1 \oplus 0 \mapsto a_3 = 1$
When $x_4 = 1$ and $x_1 = x_2 = x_3 = 0$, $a_4x_4 = 1 \oplus a_0 \mapsto a_4.1 = 1 \oplus 0 \mapsto a_4 = 1$
When $x_1 = x_2 = 1$ and $x_3 = x_4 = 0$, $a_{1,2}x_1x_2 = 1 \oplus 0 \oplus 1 \oplus 1 \mapsto a_{1,2}.1.1 = 1 \mapsto a_{1,2} = 1$
When $x_1 = x_3 = 1$ and $x_2 = x_4 = 0$, $a_{1,3}x_1x_3 = 1 \oplus 0 \oplus 1 \oplus 1 \mapsto a_{1,3}.1.1 = 1 \mapsto a_{1,3} = 1$
When $x_1 = x_4 = 1$ and $x_2 = x_3 = 0$, $a_{1,4}x_1x_4 = 0 \oplus 0 \oplus 1 \oplus 1 \mapsto a_{1,4}.1.1 = 0 \mapsto a_{1,4} = 0$
When $x_2 = x_3 = 1$ and $x_1 = x_4 = 0$, $a_{2,3}x_2x_3 = 0 \oplus 0 \oplus 1 \oplus 1 \mapsto a_{2,3}.1.1 = 0 \mapsto a_{2,3} = 0$
When $x_2 = x_4 = 1$ and $x_1 = x_3 = 0$, $a_{2,4}x_2x_4 = 0 \oplus 0 \oplus 1 \oplus 1 \mapsto a_{2,4}.1.1 = 0 \mapsto a_{2,4} = 0$
When $x_3 = x_4 = 1$ and $x_1 = x_2 = 0$, $a_{3,4}x_3x_4 = 1 \oplus 0 \oplus 1 \oplus 1 \mapsto a_{3,4}.1.1 = 1 \mapsto a_{3,4} = 1$
When $x_1 = x_2 = x_3 = 1$ and $x_4 = 0$, $a_{1,2,3}x_1x_2x_3 = 0 \oplus a_0 \oplus a_1 \oplus a_2 \oplus a_3 \oplus a_{1,2} \oplus a_{1,3} \oplus a_{2,3} \mapsto a_{1,2,3}1.1.1 = 0 \oplus 0 \oplus 1 \oplus 1 \oplus 1 \oplus 1 \oplus 1 \oplus 0 \mapsto a_{1,2,3} = 1$
When $x_1 = x_2 = x_4 = 1$ and $x_3 = 0$, $a_{1,2,4}x_1x_2x_4 = 0 \oplus a_0 \oplus a_1 \oplus a_2 \oplus a_4 \oplus a_{1,2} \oplus a_{1,4} \oplus a_{2,4} \mapsto a_{1,2,4}1.1.1 = 0 \oplus 0 \oplus 1 \oplus 1 \oplus 1 \oplus 1 \oplus 0 \oplus 0 \mapsto a_{1,2,4} = 0$
When $x_1 = x_3 = x_4 = 1$ and $x_2 = 0$, $a_{1,3,4}x_1x_3x_4 = 0 \oplus a_0 \oplus a_1 \oplus a_3 \oplus a_4 \oplus a_{1,3} \oplus a_{1,4} \oplus a_{3,4} \mapsto a_{1,3,4}1.1.1 = 0 \oplus 0 \oplus 1 \oplus 1 \oplus 1 \oplus 1 \oplus 0 \oplus 1 \mapsto a_{1,3,4} = 1$
When $x_2 = x_3 = x_4 = 1$ and $x_1 = 0$, $a_{2,3,4}x_2x_3x_4 = 0 \oplus a_0 \oplus a_2 \oplus a_3 \oplus a_4 \oplus a_{2,3} \oplus a_{2,4} \oplus a_{3,4} \mapsto a_{2,3,4}1.1.1 = 0 \oplus 0 \oplus 1 \oplus 1 \oplus 1 \oplus 0 \oplus 0 \oplus 1 \mapsto a_{2,3,4} = 0$
When $x_1 = x_2 = x_3 = x_4 = 1$, $a_{1,2,3,4}x_1x_2x_3x_4 = 1 \oplus a_0 \oplus a_2 \oplus a_3 \oplus a_4 \oplus a_{1,2} \oplus a_{1,3} \oplus a_{1,4} \oplus a_{2,3} \oplus a_{2,4} \oplus a_{3,4} \oplus a_{1,2,3} \oplus a_{1,2,4} \oplus a_{1,3,4} \oplus a_{2,3,4} \mapsto a_{1,2,3,4}1.1.1.1 = 1 \oplus 0 \oplus 1 \oplus 1 \oplus 1 \oplus 1 \oplus 1 \oplus 1 \oplus 0 \oplus 0 \oplus 0 \oplus 1 \oplus 1 \oplus 0 \oplus 1 \oplus 0 \mapsto a_{1,2,3,4} = 0$

The following 10th nonlinear Boolean function is derived from substituting all coefficients into the 4-variable affine function:
$0.(x_1x_2x_3x_4) \oplus 0.(x_2x_3x_4) \oplus 1.(x_1x_3x_4) \oplus 0.(x_1x_2x_4) \oplus 1.(x_1x_2x_3) \oplus 1.(x_3x_4) \oplus 0.(x_2x_4) \oplus 0.(x_2x_3) \oplus 0.(x_1x_4) \oplus 1.(x_1x_3) \oplus 1.(x_1x_2) \oplus 1.x_4 \oplus 1.x_3 \oplus 1.x_2 \oplus 1.x_1 \oplus 0 = f_{10} = (x_4x_3x_2x_1) = x_1x_3x_4 \oplus x_1x_2x_3 \oplus x_3x_4 \oplus x_1x_3 \oplus x_1x_2 \oplus x_4 \oplus x_3 \oplus x_2 \oplus x_1$

The nonlinear Boolean function construction (Nf_{11}):

$a_{1,2,3,4}x_1x_2x_3x_4 + a_{2,3,4}x_2x_3x_4 + a_{1,3,4}x_1x_3x_4 + a_{1,2,4}x_1x_2x_4 + a_{1,2,3}x_1x_2x_3 + a_{3,4}x_3x_4 + a_{2,4}x_2x_4 + a_{2,3}x_2x_3 + a_{1,4}x_1x_4 + a_{1,3}x_1x_3 + a_{1,2}x_1x_2 + a_4x_4 + a_3x_3 + a_2x_2 + a_1x_1 + a_0 = LCf_{11}$ .... equation no. (11)

Table XII: Inputs of equation number (11)

	Affine coordinate vector				Component	
	X_4	X_3	X_2	X_1	LCf_{11}	
a_i	0	0	0	0	1	L_i
	0	0	0	1	0	
	0	0	1	0	1	
	0	0	1	1	0	
	0	1	0	0	1	
	0	1	0	1	0	
	0	1	1	0	1	
	0	1	1	1	1	
	1	0	0	0	1	
	1	0	0	1	0	
	1	0	1	0	1	
	1	0	1	1	0	
	1	1	0	0	0	
	1	1	0	1	0	
	1	1	1	0	0	
	1	1	1	1	1	

To calculate the coefficients of equation (11), let's successively substitute the affine coordinate vector on the left side of the equation and the component vector on the right side of the equation. This process has to be repeated 16 times to get 16 coefficients. For instance, when $x_1 = x_2 = x_3 = x_4 = 0$ and $L_0 = 1$. The equation returns $a_0 = 1$ for the 1st input string $\langle 0000 \rangle$ and its corresponding component vector $\langle 1 \rangle$. Similarly, the rest of the coefficients are calculated as follows:

When $x_1 = 1$ and $x_2 = x_3 = x_4 = 0$, $a_1x_1 = 0 \oplus a_0 \mapsto a_1.1 = 0 \oplus 1 \mapsto a_1 = 1$
When $x_2 = 1$ and $x_1 = x_3 = x_4 = 0$, $a_2x_2 = 1 \oplus a_0 \mapsto a_2.1 = 1 \oplus 1 \mapsto a_2 = 0$
When $x_3 = 1$ and $x_1 = x_2 = x_4 = 0$, $a_3x_3 = 1 \oplus a_0 \mapsto a_3.1 = 1 \oplus 1 \mapsto a_3 = 0$
When $x_4 = 1$ and $x_1 = x_2 = x_3 = 0$, $a_4x_4 = 1 \oplus a_0 \mapsto a_4.1 = 1 \oplus 1 \mapsto a_4 = 0$
When $x_1 = x_2 = 1$ and $x_3 = x_4 = 0$, $a_{1,2}x_1x_2 = 0 \oplus 1 \oplus 1 \oplus 0 \mapsto a_{1,2}.1.1 = 0 \mapsto a_{1,2} = 0$
When $x_1 = x_3 = 1$ and $x_2 = x_4 = 0$, $a_{1,3}x_1x_3 = 0 \oplus 1 \oplus 1 \oplus 0 \mapsto a_{1,3}.1.1 = 0 \mapsto a_{1,3} = 0$
When $x_1 = x_4 = 1$ and $x_2 = x_3 = 0$, $a_{1,4}x_1x_4 = 0 \oplus 1 \oplus 1 \oplus 0 \mapsto a_{1,4}.1.1 = 0 \mapsto a_{1,4} = 0$
When $x_2 = x_3 = 1$ and $x_1 = x_4 = 0$, $a_{2,3}x_2x_3 = 1 \oplus 1 \oplus 0 \oplus 0 \mapsto a_{2,3}.1.1 = 0 \mapsto a_{2,3} = 0$
When $x_2 = x_4 = 1$ and $x_1 = x_3 = 0$, $a_{2,4}x_2x_4 = 1 \oplus 1 \oplus 0 \oplus 0 \mapsto a_{2,4}.1.1 = 0 \mapsto a_{2,4} = 0$
When $x_3 = x_4 = 1$ and $x_1 = x_2 = 0$, $a_{3,4}x_3x_4 = 0 \oplus 1 \oplus 0 \oplus 0 \mapsto a_{3,4}.1.1 = 1 \mapsto a_{3,4} = 1$
When $x_1 = x_2 = x_3 = 1$ and $x_4 = 0$, $a_{1,2,3}x_1x_2x_3 = 1 \oplus a_0 \oplus a_1 \oplus a_2 \oplus a_3 \oplus a_{1,2} \oplus a_{1,3} \oplus a_{2,3} \mapsto a_{1,2,3}1.1.1 = 1 \oplus 1 \oplus 1 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \mapsto a_{1,2,3} = 1$
When $x_1 = x_2 = x_4 = 1$ and $x_3 = 0$, $a_{1,2,4}x_1x_2x_4 = 0 \oplus a_0 \oplus a_1 \oplus a_2 \oplus a_4 \oplus a_{1,2} \oplus a_{1,4} \oplus a_{2,4} \mapsto a_{1,2,4}1.1.1 = 0 \oplus 1 \oplus 1 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \mapsto a_{1,2,4} = 0$
When $x_1 = x_3 = x_4 = 1$ and $x_2 = 0$, $a_{1,3,4}x_1x_3x_4 = 0 \oplus a_0 \oplus a_1 \oplus a_3 \oplus a_4 \oplus a_{1,3} \oplus a_{1,4} \oplus a_{3,4} \mapsto a_{1,3,4}1.1.1 = 0 \oplus 1 \oplus 1 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 1 \mapsto a_{1,3,4} = 1$
When $x_2 = x_3 = x_4 = 1$ and $x_1 = 0$, $a_{2,3,4}x_2x_3x_4 = 0 \oplus a_0 \oplus a_2 \oplus a_3 \oplus a_4 \oplus a_{2,3} \oplus a_{2,4} \oplus a_{3,4} \mapsto a_{2,3,4}1.1.1 = 0 \oplus 1 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 1 \mapsto a_{2,3,4} = 0$
When $x_1 = x_2 = x_3 = x_4 = 1$, $a_{1,2,3,4}x_1x_2x_3x_4 = 1 \oplus a_0 \oplus a_2 \oplus a_3 \oplus a_4 \oplus a_{1,2} \oplus a_{1,3} \oplus a_{1,4} \oplus a_{2,3} \oplus a_{2,4} \oplus a_{3,4} \oplus a_{1,2,3}$ $a_{1,2,4} \oplus a_{1,3,4} \oplus a_{2,3,4} \mapsto a_{1,2,3,4}1.1.1.1 = 1 \oplus 1 \oplus 1 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 1 \oplus 1 \oplus 0 \oplus 1 \oplus 0 \mapsto a_{1,2,3,4} = 0$

The following 11th nonlinear Boolean function is derived from substituting all coefficients into the 4-variable affine function:
$0.(x_1x_2x_3x_4) \oplus 0.(x_2x_3x_4) \oplus 1.(x_1x_3x_4) \oplus 0.(x_1x_2x_4) \oplus 1.(x_1x_2x_3) \oplus 1.(x_3x_4) \oplus 0.(x_2x_4) \oplus 0.(x_2x_3) \oplus 0.(x_1x_4) \oplus 0.(x_1x_3) \oplus 0.(x_1x_2) \oplus 0.x_4 \oplus 0.x_3 \oplus 0.x_2 \oplus 1.x_1 \oplus 0 = f_{11}(x_4x_3x_2x_1) = x_1x_3x_4 \oplus x_1x_2x_3 \oplus x_3x_4 \oplus x_1 \oplus 1$

The nonlinear Boolean function construction (Nf_{12}):

$a_{1,2,3,4}x_1x_2x_3x_4 + a_{2,3,4}x_2x_3x_4 + a_{1,3,4}x_1x_3x_4 + a_{1,2,4}x_1x_2x_4 + a_{1,2,3}x_1x_2x_3 + a_{3,4}x_3x_4 + a_{2,4}x_2x_4 + a_{2,3}x_2x_3 + a_{1,4}x_1x_4 + a_{1,3}x_1x_3 + a_{1,2}x_1x_2 + a_4x_4 + a_3x_3 + a_2x_2 + a_1x_1 + a_0 = LCf_{12}$ .... equation no. (12)

Table XIII: Inputs of equation number (12)

	Affine coordinate vector				Component	
	X_4	X_3	X_2	X_1	LCf_{12}	
a_i	0	0	0	0	1	L_i
	0	0	0	1	1	
	0	0	1	0	0	
	0	0	1	1	1	
	0	1	0	0	0	
	0	1	0	1	1	
	0	1	1	0	1	
	0	1	1	1	1	
	1	0	0	0	0	
	1	0	0	1	0	
	1	0	1	0	1	
	1	0	1	1	0	
	1	1	0	0	1	
	1	1	0	1	0	
	1	1	1	0	0	
	1	1	1	1	0	

To calculate the coefficients of equation (12), let's successively substitute the affine coordinate vector on the left side of the equation and the component vector on the right side of the equation. This process has to be repeated 16 times to get 16 coefficients. For instance, when $x_1 = x_2 = x_3 = x_4 = 0$ and $L_0 = 1$. The equation returns $a_0 = 1$ for the 1st input string $\langle 0000 \rangle$ and its corresponding component vector $\langle 1 \rangle$. Similarly, the rest of the coefficients are calculated as follows:

When $x_1 = 1$ and $x_2 = x_3 = x_4 = 0$, $a_1x_1 = 1 \oplus a_0 \mapsto a_1.1 = 1 \oplus 1 \mapsto a_1 = 0$
When $x_2 = 1$ and $x_1 = x_3 = x_4 = 0$, $a_2x_2 = 0 \oplus a_0 \mapsto a_2.1 = 0 \oplus 1 \mapsto a_2 = 1$
When $x_3 = 1$ and $x_1 = x_2 = x_4 = 0$, $a_3x_3 = 0 \oplus a_0 \mapsto a_3.1 = 0 \oplus 1 \mapsto a_3 = 1$
When $x_4 = 1$ and $x_1 = x_2 = x_3 = 0$, $a_4x_4 = 0 \oplus a_0 \mapsto a_4.1 = 0 \oplus 1 \mapsto a_4 = 1$
When $x_1 = x_2 = 1$ and $x_3 = x_4 = 0$, $a_{1,2}x_1x_2 = 1 \oplus 1 \oplus 0 \oplus 1 \mapsto a_{1,2}.1.1 = 1 \mapsto a_{1,2} = 1$
When $x_1 = x_3 = 1$ and $x_2 = x_4 = 0$, $a_{1,3}x_1x_3 = 1 \oplus 1 \oplus 0 \oplus 1 \mapsto a_{1,3}.1.1 = 1 \mapsto a_{1,3} = 1$
When $x_1 = x_4 = 1$ and $x_2 = x_3 = 0$, $a_{1,4}x_1x_4 = 0 \oplus 1 \oplus 0 \oplus 1 \mapsto a_{1,4}.1.1 = 0 \mapsto a_{1,4} = 0$
When $x_2 = x_3 = 1$ and $x_1 = x_4 = 0$, $a_{2,3}x_2x_3 = 1 \oplus 1 \oplus 1 \oplus 1 \mapsto a_{2,3}.1.1 = 0 \mapsto a_{2,3} = 0$
When $x_2 = x_4 = 1$ and $x_1 = x_3 = 0$, $a_{2,4}x_2x_4 = 1 \oplus 1 \oplus 1 \oplus 1 \mapsto a_{2,4}.1.1 = 0 \mapsto a_{2,4} = 0$
When $x_3 = x_4 = 1$ and $x_1 = x_2 = 0$, $a_{3,4}x_3x_4 = 1 \oplus 1 \oplus 1 \oplus 1 \mapsto a_{3,4}.1.1 = 0 \mapsto a_{3,4} = 0$
When $x_1 = x_2 = x_3 = 1$ and $x_4 = 0$, $a_{1,2,3}x_1x_2x_3 = 1 \oplus a_0 \oplus a_1 \oplus a_2 \oplus a_3 \oplus a_{1,2} \oplus a_{1,3} \oplus a_{2,3} \mapsto a_{1,2,3}1.1.1 = 1 \oplus 1 \oplus 0 \oplus 1 \oplus 1 \oplus 1 \oplus 1 \oplus 0 \mapsto a_{1,2,3} = 0$
When $x_1 = x_2 = x_4 = 1$ and $x_3 = 0$, $a_{1,2,4}x_1x_2x_4 = 0 \oplus a_0 \oplus a_1 \oplus a_2 \oplus a_4 \oplus a_{1,2} \oplus a_{1,4} \oplus a_{2,4} \mapsto a_{1,2,4}1.1.1 = 0 \oplus 1 \oplus 0 \oplus 1 \oplus 1 \oplus 1 \oplus 0 \oplus 0 \mapsto a_{1,2,4} = 0$
When $x_1 = x_3 = x_4 = 1$ and $x_2 = 0$, $a_{1,3,4}x_1x_3x_4 = 0 \oplus a_0 \oplus a_1 \oplus a_3 \oplus a_4 \oplus a_{1,3} \oplus a_{1,4} \oplus a_{3,4} \mapsto a_{1,3,4}1.1.1 = 0 \oplus 1 \oplus 0 \oplus 1 \oplus 1 \oplus 1 \oplus 0 \oplus 0 \mapsto a_{1,3,4} = 0$
When $x_2 = x_3 = x_4 = 1$ and $x_1 = 0$, $a_{2,3,4}x_2x_3x_4 = 0 \oplus a_0 \oplus a_2 \oplus a_3 \oplus a_4 \oplus a_{2,3} \oplus a_{2,4} \oplus a_{3,4} \mapsto a_{2,3,4}1.1.1 = 0 \oplus 1 \oplus 1 \oplus 1 \oplus 1 \oplus 0 \oplus 0 \oplus 0 \mapsto a_{2,3,4} = 0$
When $x_1 = x_2 = x_3 = x_4 = 1$, $a_{1,2,3,4}x_1x_2x_3x_4 = 0 \oplus a_0 \oplus a_2 \oplus a_3 \oplus a_4 \oplus a_{1,2} \oplus a_{1,3} \oplus a_{1,4} \oplus a_{2,3} \oplus a_{2,4} \oplus a_{3,4} \oplus a_{1,2,3} \oplus a_{1,2,4} \oplus a_{1,3,4} \oplus a_{2,3,4} \mapsto a_{1,2,3,4}1.1.1.1 = 0 \oplus 1 \oplus 0 \oplus 1 \oplus 1 \oplus 1 \oplus 1 \oplus 1 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \mapsto a_{1,2,3,4} = 0$

The following 12th nonlinear Boolean function is derived from substituting all coefficients into the 4-variable affine function:
$0.(x_1x_2x_3x_4) \oplus 0.(x_2x_3x_4) \oplus 0.(x_1x_3x_4) \oplus 0.(x_1x_2x_4) \oplus 0.(x_1x_2x_3) \oplus 0.(x_3x_4) \oplus 0.(x_2x_4) \oplus 0.(x_2x_3) \oplus 0.(x_1x_4) \oplus 1.(x_1x_3) \oplus 1.(x_1x_2) \oplus 1.x_4 \oplus 1.x_3 \oplus 1.x_2 \oplus 0.x_1 \oplus 1 = f_{12}(x_4x_3x_2x_1) = x_1x_3 \oplus x_1x_2 \oplus x_4 \oplus x_3 \oplus x_2 \oplus 1$

The nonlinear Boolean function construction (Nf_{13}):

$a_{1,2,3,4}x_1x_2x_3x_4 + a_{2,3,4}x_2x_3x_4 + a_{1,3,4}x_1x_3x_4 + a_{1,2,4}x_1x_2x_4 + a_{1,2,3}x_1x_2x_3 + a_{3,4}x_3x_4 + a_{2,4}x_2x_4 + a_{2,3}x_2x_3 + a_{1,4}x_1x_4 + a_{1,3}x_1x_3 + a_{1,2}x_1x_2 + a_4x_4 + a_3x_3 + a_2x_2 + a_1x_1 + a_0 = LCf_{13}$ .... equation no. (13)

Table XIV: Inputs of equation number (13)

	Affine coordinate vector				Component	
	X_4	X_3	X_2	X_1	LCf_{13}	
a_i	0	0	0	0	0	L_i
	0	0	0	1	0	
	0	0	1	0	0	
	0	0	1	1	1	
	0	1	0	0	0	
	0	1	0	1	0	
	0	1	1	0	0	
	0	1	1	1	1	
	1	0	0	0	1	
	1	0	0	1	1	
	1	0	1	0	1	
	1	0	1	1	1	
	1	1	0	0	1	
	1	1	0	1	0	
	1	1	1	0	0	
	1	1	1	1	1	

To calculate the coefficients of equation (13), let's successively substitute the affine coordinate vector on the left side of the equation and the component vector on the right side of the equation. This process has to be repeated 16 times to get 16 coefficients. For instance, when $x_1 = x_2 = x_3 = x_4 = 0$ and $L_0 = 0$. The equation returns $a_0 = 0$ for the 1st input string $\langle 0000 \rangle$ and its corresponding component vector $\langle 0 \rangle$. Similarly, the rest of the coefficients are calculated as follows:

When $x_1 = 1$ and $x_2 = x_3 = x_4 = 0$, $a_1x_1 = 0 \oplus a_0 \mapsto a_1.1 = 0 \oplus 0 \mapsto a_1 = 0$
When $x_2 = 1$ and $x_1 = x_3 = x_4 = 0$, $a_2x_2 = 0 \oplus a_0 \mapsto a_2.1 = 0 \oplus 0 \mapsto a_2 = 0$
When $x_3 = 1$ and $x_1 = x_2 = x_4 = 0$, $a_3x_3 = 0 \oplus a_0 \mapsto a_3.1 = 0 \oplus 0 \mapsto a_3 = 0$
When $x_4 = 1$ and $x_1 = x_2 = x_3 = 0$, $a_4x_4 = 1 \oplus a_0 \mapsto a_4.1 = 1 \oplus 0 \mapsto a_4 = 1$
When $x_1 = x_2 = 1$ and $x_3 = x_4 = 0$, $a_{1,2}x_1x_2 = 1 \oplus 0 \oplus 0 \oplus 0 \mapsto a_{1,2}.1.1 = 1 \mapsto a_{1,2} = 1$
When $x_1 = x_3 = 1$ and $x_2 = x_4 = 0$, $a_{1,3}x_1x_3 = 0 \oplus 0 \oplus 0 \oplus 0 \mapsto a_{1,3}.1.1 = 0 \mapsto a_{1,3} = 0$
When $x_1 = x_4 = 1$ and $x_2 = x_3 = 0$, $a_{1,4}x_1x_4 = 1 \oplus 0 \oplus 0 \oplus 1 \mapsto a_{1,4}.1.1 = 0 \mapsto a_{1,4} = 0$
When $x_2 = x_3 = 1$ and $x_1 = x_4 = 0$, $a_{2,3}x_2x_3 = 0 \oplus 0 \oplus 0 \oplus 0 \mapsto a_{2,3}.1.1 = 0 \mapsto a_{2,3} = 0$
When $x_2 = x_4 = 1$ and $x_1 = x_3 = 0$, $a_{2,4}x_2x_4 = 1 \oplus 0 \oplus 0 \oplus 1 \mapsto a_{2,4}.1.1 = 0 \mapsto a_{2,4} = 0$
When $x_3 = x_4 = 1$ and $x_1 = x_2 = 0$, $a_{3,4}x_3x_4 = 1 \oplus 0 \oplus 0 \oplus 1 \mapsto a_{3,4}.1.1 = 0 \mapsto a_{3,4} = 0$
When $x_1 = x_2 = x_3 = 1$ and $x_4 = 0$, $a_{1,2,3}x_1x_2x_3 = 1 \oplus a_0 \oplus a_1 \oplus a_2 \oplus a_3 \oplus a_{1,2} \oplus a_{1,3} \oplus a_{2,3} \mapsto a_{1,2,3}1.1.1 = 1 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 1 \oplus 0 \oplus 0 \mapsto a_{1,2,3} = 0$
When $x_1 = x_2 = x_4 = 1$ and $x_3 = 0$, $a_{1,2,4}x_1x_2x_4 = 1 \oplus a_0 \oplus a_1 \oplus a_2 \oplus a_4 \oplus a_{1,2} \oplus a_{1,4} \oplus a_{2,4} \mapsto a_{1,2,4}1.1.1 = 1 \oplus 0 \oplus 0 \oplus 0 \oplus 1 \oplus 1 \oplus 0 \oplus 0 \mapsto a_{1,2,4} = 1$
When $x_1 = x_3 = x_4 = 1$ and $x_2 = 0$, $a_{1,3,4}x_1x_3x_4 = 0 \oplus a_0 \oplus a_1 \oplus a_3 \oplus a_4 \oplus a_{1,3} \oplus a_{1,4} \oplus a_{3,4} \mapsto a_{1,3,4}1.1.1 = 0 \oplus 0 \oplus 0 \oplus 0 \oplus 1 \oplus 0 \oplus 0 \oplus 0 \mapsto a_{1,3,4} = 1$
When $x_2 = x_3 = x_4 = 1$ and $x_1 = 0$, $a_{2,3,4}x_2x_3x_4 = 0 \oplus a_0 \oplus a_2 \oplus a_3 \oplus a_4 \oplus a_{2,3} \oplus a_{2,4} \oplus a_{3,4} \mapsto a_{2,3,4}1.1.1 = 0 \oplus 0 \oplus 0 \oplus 0 \oplus 1 \oplus 0 \oplus 0 \oplus 0 \mapsto a_{2,3,4} = 1$
When $x_1 = x_2 = x_3 = x_4 = 1$, $a_{1,2,3,4}x_1x_2x_3x_4 = 1 \oplus a_0 \oplus a_2 \oplus a_3 \oplus a_4 \oplus a_{1,2} \oplus a_{1,3} \oplus a_{1,4} \oplus a_{2,3} \oplus a_{2,4} \oplus a_{3,4} \oplus a_{1,2,3} \oplus a_{1,2,4} \oplus a_{1,3,4} \oplus a_{2,3,4} \mapsto a_{1,2,3,4}1.1.1.1 = 1 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 1 \oplus 1 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 1 \oplus 1 \oplus 1 \mapsto a_{1,2,3,4} = 0$

The following 13th nonlinear Boolean function is derived from substituting all coefficients into the 4-variable affine function:
$0.(x_1x_2x_3x_4) \oplus 1.(x_2x_3x_4) \oplus 1.(x_1x_3x_4) \oplus 1.(x_1x_2x_4) \oplus 0.(x_1x_2x_3) \oplus 0.(x_3x_4) \oplus 0.(x_2x_4) \oplus 0.(x_2x_3) \oplus 0.(x_1x_4) \oplus 0.(x_1x_3) \oplus 1.(x_1x_2) \oplus 1.x_4 \oplus 0.x_3 \oplus 0.x_2 \oplus 0.x_1 \oplus 0 = f_{13}(x_4x_3x_2x_1) = x_2x_3x_4 \oplus x_1x_3x_4 \oplus x_1x_2x_4 \oplus x_1x_2 \oplus x_4$

The nonlinear Boolean function construction (Nf_{14}):

$a_{1,2,3,4}x_1x_2x_3x_4 + a_{2,3,4}x_2x_3x_4 + a_{1,3,4}x_1x_3x_4 + a_{1,2,4}x_1x_2x_4 + a_{1,2,3}x_1x_2x_3 + a_{3,4}x_3x_4 + a_{2,4}x_2x_4 + a_{2,3}x_2x_3 + a_{1,4}x_1x_4 + a_{1,3}x_1x_3 + a_{1,2}x_1x_2 + a_4x_4 + a_3x_3 + a_2x_2 + a_1x_1 + a_0 = LCf_{14}$ .... equation no. (14)

Table XV: Inputs of equation number (14)

	Affine coordinate vector				Component	
	X_4	X_3	X_2	X_1	LCf_{14}	
a_i	0	0	0	0	1	L_i
	0	0	0	1	1	
	0	0	1	0	0	
	0	0	1	1	1	
	0	1	0	0	1	
	0	1	0	1	0	
	0	1	1	0	0	
	0	1	1	1	1	
	1	0	0	0	0	
	1	0	0	1	0	
	1	0	1	0	0	
	1	0	1	1	1	
	1	1	0	0	0	
	1	1	0	1	1	
	1	1	1	0	0	
	1	1	1	1	1	

To calculate the coefficients of equation (14), let's successively substitute the affine coordinate vector on the left side of the equation and the component vector on the right side of the equation. This process has to be repeated 16 times to get 16 coefficients. For instance, when $x_1 = x_2 = x_3 = x_4 = 0$ and $L_0 = 1$. The equation returns $a_0 = 1$ for the 1st input string $\langle 0000 \rangle$ and its corresponding component vector $\langle 1 \rangle$. Similarly, the rest of the coefficients are calculated as follows:

When $x_1 = 1$ and $x_2 = x_3 = x_4 = 0$, $a_1x_1 = 1 \oplus a_0 \mapsto a_1.1 = 1 \oplus 1 \mapsto a_1 = 0$
When $x_2 = 1$ and $x_1 = x_3 = x_4 = 0$, $a_2x_2 = 0 \oplus a_0 \mapsto a_2.1 = 0 \oplus 1 \mapsto a_2 = 1$
When $x_3 = 1$ and $x_1 = x_2 = x_4 = 0$, $a_3x_3 = 1 \oplus a_0 \mapsto a_3.1 = 1 \oplus 1 \mapsto a_3 = 0$
When $x_4 = 1$ and $x_1 = x_2 = x_3 = 0$, $a_4x_4 = 0 \oplus a_0 \mapsto a_4.1 = 0 \oplus 1 \mapsto a_4 = 1$
When $x_1 = x_2 = 1$ and $x_3 = x_4 = 0$, $a_{1,2}x_1x_2 = 1 \oplus 1 \oplus 0 \oplus 1 \mapsto a_{1,2}.1.1 = 1 \mapsto a_{1,2} = 1$
When $x_1 = x_3 = 1$ and $x_2 = x_4 = 0$, $a_{1,3}x_1x_3 = 0 \oplus 1 \oplus 0 \oplus 0 \mapsto a_{1,3}.1.1 = 1 \mapsto a_{1,3} = 1$
When $x_1 = x_4 = 1$ and $x_2 = x_3 = 0$, $a_{1,4}x_1x_4 = 0 \oplus 1 \oplus 0 \oplus 1 \mapsto a_{1,4}.1.1 = 0 \mapsto a_{1,4} = 0$
When $x_2 = x_3 = 1$ and $x_1 = x_4 = 0$, $a_{2,3}x_2x_3 = 0 \oplus 1 \oplus 1 \oplus 0 \mapsto a_{2,3}.1.1 = 0 \mapsto a_{2,3} = 0$
When $x_2 = x_4 = 1$ and $x_1 = x_3 = 0$, $a_{2,4}x_2x_4 = 0 \oplus 1 \oplus 1 \oplus 1 \mapsto a_{2,4}.1.1 = 1 \mapsto a_{2,4} = 1$
When $x_3 = x_4 = 1$ and $x_1 = x_2 = 0$, $a_{3,4}x_3x_4 = 0 \oplus 1 \oplus 0 \oplus 1 \mapsto a_{3,4}.1.1 = 0 \mapsto a_{3,4} = 0$
When $x_1 = x_2 = x_3 = 1$ and $x_4 = 0$, $a_{1,2,3}x_1x_2x_3 = 1 \oplus a_0 \oplus a_1 \oplus a_2 \oplus a_3 \oplus a_{1,2} \oplus a_{1,3} \oplus a_{2,3} \mapsto a_{1,2,3}1.1.1 = 1 \oplus 1 \oplus 0 \oplus 1 \oplus 0 \oplus 1 \oplus 1 \oplus 0 \mapsto a_{1,2,3} = 1$
When $x_1 = x_2 = x_4 = 1$ and $x_3 = 0$, $a_{1,2,4}x_1x_2x_4 = 1 \oplus a_0 \oplus a_1 \oplus a_2 \oplus a_4 \oplus a_{1,2} \oplus a_{1,4} \oplus a_{2,4} \mapsto a_{1,2,4}1.1.1 = 1 \oplus 1 \oplus 0 \oplus 1 \oplus 1 \oplus 1 \oplus 0 \oplus 1 \mapsto a_{1,2,4} = 0$
When $x_1 = x_3 = x_4 = 1$ and $x_2 = 0$, $a_{1,3,4}x_1x_3x_4 = 1 \oplus a_0 \oplus a_1 \oplus a_3 \oplus a_4 \oplus a_{1,3} \oplus a_{1,4} \oplus a_{3,4} \mapsto a_{1,3,4}1.1.1 = 1 \oplus 1 \oplus 0 \oplus 0 \oplus 1 \oplus 1 \oplus 0 \oplus 0 \mapsto a_{1,3,4} = 0$
When $x_2 = x_3 = x_4 = 1$ and $x_1 = 0$, $a_{2,3,4}x_2x_3x_4 = 0 \oplus a_0 \oplus a_2 \oplus a_3 \oplus a_4 \oplus a_{2,3} \oplus a_{2,4} \oplus a_{3,4} \mapsto a_{2,3,4}1.1.1 = 0 \oplus 1 \oplus 1 \oplus 0 \oplus 1 \oplus 0 \oplus 1 \oplus 0 \mapsto a_{2,3,4} = 0$
When $x_1 = x_2 = x_3 = x_4 = 1$, $a_{1,2,3,4}x_1x_2x_3x_4 = 1 \oplus a_0 \oplus a_2 \oplus a_3 \oplus a_4 \oplus a_{1,2} \oplus a_{1,3} \oplus a_{1,4} \oplus a_{2,3} \oplus a_{2,4} \oplus a_{3,4} \oplus a_{1,2,3} \oplus a_{1,2,4} \oplus a_{1,3,4} \oplus a_{2,3,4} \mapsto a_{1,2,3,4}1.1.1.1 = 1 \oplus 1 \oplus 0 \oplus 1 \oplus 0 \oplus 1 \oplus 1 \oplus 1 \oplus 0 \oplus 0 \oplus 1 \oplus 0 \oplus 1 \oplus 0 \oplus 0 \oplus 0 \mapsto a_{1,2,3,4} = 0$

The following 14th nonlinear Boolean function is derived from substituting all coefficients into the 4-variable affine function:
$0.(x_1x_2x_3x_4) \oplus 0.(x_2x_3x_4) \oplus 0.(x_1x_3x_4) \oplus 0.(x_1x_2x_4) \oplus 1.(x_1x_2x_3) \oplus 0.(x_3x_4) \oplus 1.(x_2x_4) \oplus 0.(x_2x_3) \oplus 0.(x_1x_4) \oplus 1.(x_1x_3) \oplus 1.(x_1x_2) \oplus 1.x_4 \oplus 0.x_3 \oplus 1.x_2 \oplus 0.x_1 \oplus 1 = f_{14}(x_4x_3x_2x_1) = x_1x_2x_3 \oplus x_2x_4 \oplus x_1x_3 \oplus x_1x_2 \oplus x_4 \oplus x_2 \oplus 1$

The nonlinear Boolean function construction ($\mathrm{N}f_{15}$):

$a_{1,2,3,4}x_1x_2x_3x_4 + a_{2,3,4}x_2x_3x_4 + a_{1,3,4}x_1x_3x_4 + a_{1,2,4}x_1x_2x_4 + a_{1,2,3}x_1x_2x_3 + a_{3,4}x_3x_4 + a_{2,4}x_2x_4 + a_{2,3}x_2x_3 + a_{1,4}x_1x_4 + a_{1,3}x_1x_3 + a_{1,2}x_1x_2 + a_4x_4 + a_3x_3 + a_2x_2 + a_1x_1 + a_0 = LCf_{15}$ .... equation no. (15)

Table XVI: Inputs of equation number (15)

	Affine coordinate vector				Component	
	X_4	X_3	X_2	X_1	LCf_{15}	
a_i	0	0	0	0	1	L_i
	0	0	0	1	0	
	0	0	1	0	1	
	0	0	1	1	1	
	0	1	0	0	0	
	0	1	0	1	1	
	0	1	1	0	0	
	0	1	1	1	0	
	1	0	0	0	0	
	1	0	0	1	1	
	1	0	1	0	1	
	1	0	1	1	0	
	1	1	0	0	0	
	1	1	0	1	1	
	1	1	1	0	0	
	1	1	1	1	1	

To calculate the coefficients of equation (15), let's successively substitute the affine coordinate vector on the left side of the equation and the component vector on the right side of the equation. This process has to be repeated 16 times to get 16 coefficients. For instance, when $x_1 = x_2 = x_3 = x_4 = 0$ and $L_0 = 1$. The equation returns $a_0 = 1$ for the 1st input string $\langle 0000 \rangle$ and its corresponding component vector $\langle 1 \rangle$. Similarly, the rest of the coefficients are calculated as follows:

When $x_1 = 1$ and $x_2 = x_3 = x_4 = 0$, $a_1x_1 = 0 \oplus a_0 \mapsto a_1.1 = 0 \oplus 1 \mapsto a_1 = 1$
When $x_2 = 1$ and $x_1 = x_3 = x_4 = 0$, $a_2x_2 = 1 \oplus a_0 \mapsto a_2.1 = 1 \oplus 1 \mapsto a_2 = 0$
When $x_3 = 1$ and $x_1 = x_2 = x_4 = 0$, $a_3x_3 = 0 \oplus a_0 \mapsto a_3.1 = 0 \oplus 1 \mapsto a_3 = 1$
When $x_4 = 1$ and $x_1 = x_2 = x_3 = 0$, $a_4x_4 = 0 \oplus a_0 \mapsto a_4.1 = 0 \oplus 1 \mapsto a_4 = 1$
When $x_1 = x_2 = 1$ and $x_3 = x_4 = 0$, $a_{1,2}x_1x_2 = 1 \oplus 1 \oplus 1 \oplus 0 \mapsto a_{1,2}.1.1 = 1 \mapsto a_{1,2} = 1$
When $x_1 = x_3 = 1$ and $x_2 = x_4 = 0$, $a_{1,3}x_1x_3 = 1 \oplus 1 \oplus 1 \oplus 1 \mapsto a_{1,3}.1.1 = 0 \mapsto a_{1,3} = 0$
When $x_1 = x_4 = 1$ and $x_2 = x_3 = 0$, $a_{1,4}x_1x_4 = 1 \oplus 1 \oplus 1 \oplus 1 \mapsto a_{1,4}.1.1 = 0 \mapsto a_{1,4} = 0$
When $x_2 = x_3 = 1$ and $x_1 = x_4 = 0$, $a_{2,3}x_2x_3 = 0 \oplus 1 \oplus 0 \oplus 1 \mapsto a_{2,3}.1.1 = 0 \mapsto a_{2,3} = 0$
When $x_2 = x_4 = 1$ and $x_1 = x_3 = 0$, $a_{2,4}x_2x_4 = 1 \oplus 1 \oplus 0 \oplus 1 \mapsto a_{2,4}.1.1 = 1 \mapsto a_{2,4} = 1$
When $x_3 = x_4 = 1$ and $x_1 = x_2 = 0$, $a_{3,4}x_3x_4 = 0 \oplus 1 \oplus 1 \oplus 1 \mapsto a_{3,4}.1.1 = 1 \mapsto a_{3,4} = 1$
When $x_1 = x_2 = x_3 = 1$ and $x_4 = 0$, $a_{1,2,3}x_1x_2x_3 = 0 \oplus a_0 \oplus a_1 \oplus a_2 \oplus a_3 \oplus a_{1,2} \oplus a_{1,3} \oplus a_{2,3} \mapsto a_{1,2,3}1.1.1 = 0 \oplus 1 \oplus 1 \oplus 0 \oplus 1 \oplus 1 \oplus 0 \oplus 0 \mapsto a_{1,2,3} = 0$
When $x_1 = x_2 = x_4 = 1$ and $x_3 = 0$, $a_{1,2,4}x_1x_2x_4 = 0 \oplus a_0 \oplus a_1 \oplus a_2 \oplus a_4 \oplus a_{1,2} \oplus a_{1,4} \oplus a_{2,4} \mapsto a_{1,2,4}1.1.1 = 0 \oplus 1 \oplus 1 \oplus 0 \oplus 1 \oplus 1 \oplus 0 \oplus 1 \mapsto a_{1,2,4} = 1$
When $x_1 = x_3 = x_4 = 1$ and $x_2 = 0$, $a_{1,3,4}x_1x_3x_4 = 1 \oplus a_0 \oplus a_1 \oplus a_3 \oplus a_4 \oplus a_{1,3} \oplus a_{1,4} \oplus a_{3,4} \mapsto a_{1,3,4}1.1.1 = 1 \oplus 1 \oplus 1 \oplus 1 \oplus 1 \oplus 0 \oplus 0 \oplus 1 \mapsto a_{1,3,4} = 0$
When $x_2 = x_3 = x_4 = 1$ and $x_1 = 0$, $a_{2,3,4}x_2x_3x_4 = 0 \oplus a_0 \oplus a_2 \oplus a_3 \oplus a_4 \oplus a_{2,3} \oplus a_{2,4} \oplus a_{3,4} \mapsto a_{2,3,4}1.1.1 = 0 \oplus 1 \oplus 0 \oplus 1 \oplus 1 \oplus 0 \oplus 1 \oplus 1 \mapsto a_{2,3,4} = 1$
When $x_1 = x_2 = x_3 = x_4 = 1$, $a_{1,2,3,4}x_1x_2x_3x_4 = 1 \oplus a_0 \oplus a_2 \oplus a_3 \oplus a_4 \oplus a_{1,2} \oplus a_{1,3} \oplus a_{1,4} \oplus a_{2,3} \oplus a_{2,4} \oplus a_{3,4} \oplus a_{1,2,3} \oplus a_{1,2,4} \oplus a_{1,3,4} \oplus a_{2,3,4} \mapsto a_{1,2,3,4}1.1.1.1 = 1 \oplus 1 \oplus 1 \oplus 0 \oplus 1 \oplus 1 \oplus 1 \oplus 0 \oplus 0 \oplus 0 \oplus 1 \oplus 1 \oplus 0 \oplus 1 \oplus 0 \oplus 1 \mapsto a_{1,2,3,4} = 0$

The following 15th nonlinear Boolean function is derived from substituting all coefficients into 4-variable affine function:
$0.(x_1x_2x_3x_4) \oplus 1.(x_2x_3x_4) \oplus 0.(x_1x_3x_4) \oplus 1.(x_1x_2x_4) \oplus 0.(x_1x_2x_3) \oplus 1.(x_3x_4) \oplus 1.(x_2x_4) \oplus 0.(x_2x_3) \oplus 0.(x_1x_4) \oplus 0.(x_1x_3) \oplus 1.(x_1x_2) \oplus 1.x_4 \oplus 1.x_3 \oplus 0.x_2 \oplus 1.x_1 \oplus 1 = f_{15}(x_4x_3x_2x_1) = x_2x_3x_4 \oplus x_1x_2x_4 \oplus x_3x_4 \oplus x_2x_4 \oplus x_1x_2 \oplus x_4 \oplus x_3 \oplus x_1 \oplus 1$

STEP 5: The process of creating an action in the S-box: An action of S-box is generated by a linear combination of 2^{n-1} numbers of nonlinear Boolean functions using Boolean logic. Thus, a nonlinear S-box is actually a collection of the following nonlinear Boolean functions:

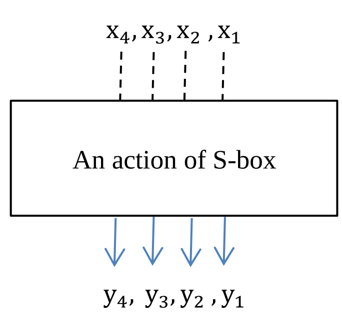
1. $f_1(x_4x_3x_2x_1) = x_2x_3x_4 \oplus x_1x_2x_4 \oplus x_1x_2x_3 \oplus x_3x_4 \oplus x_1x_3 \oplus x_3 \oplus x_2 \oplus x_1$
2. $f_2(x_4x_3x_2x_1) = x_1x_3x_4 \oplus x_3x_4 \oplus x_2x_4 \oplus x_3 \oplus x_1 \oplus 1$
3. $f_3(x_4x_3x_2x_1) = x_2x_3x_4 \oplus x_1x_2x_4 \oplus x_3x_4 \oplus x_2x_4 \oplus x_1x_3 \oplus x_2 \oplus x_1$
4. $f_4(x_4x_3x_2x_1) = x_2x_3x_4 \oplus x_1x_3x_4 \oplus x_1x_2x_4 \oplus x_1x_2x_3 \oplus x_2x_4 \oplus x_1x_2 \oplus x_4 \oplus x_3$
5. $f_5(x_4x_3x_2x_1) = x_2x_3x_4 \oplus x_1x_3x_4 \oplus x_1x_2x_4 \oplus x_1x_2x_3 \oplus x_2x_4 \oplus x_1x_3 \oplus x_2 \oplus 1$
6. $f_6(x_4x_3x_2x_1) = x_1x_2x_3 \oplus x_2x_4 \oplus x_3$
7. $f_7(x_4x_3x_2x_1) = x_1x_3x_4 \oplus x_3x_4 \oplus x_2x_4 \oplus x_1x_3 \oplus x_1x_2 \oplus x_4 \oplus x_2 \oplus x_1$
8. $f_8(x_4x_3x_2x_1) = x_2x_3x_4 \oplus x_1x_3x_4 \oplus x_1x_2x_4 \oplus x_1x_3 \oplus x_3 \oplus x_2 \oplus 1$
9. $f_9(x_4x_3x_2x_1) = x_2x_3x_4 \oplus x_1x_2x_4 \oplus x_1x_2x_3 \oplus x_3x_4 \oplus x_1x_2 \oplus x_4 \oplus x_1 \oplus 1$
10. $f_{10}(x_4x_3x_2x_1) = x_1x_3x_4 \oplus x_1x_2x_3 \oplus x_3x_4 \oplus x_1x_3 \oplus x_1x_2 \oplus x_4 \oplus x_3 \oplus x_2 \oplus x_1$
11. $f_{11}(x_4x_3x_2x_1) = x_1x_3x_4 \oplus x_1x_2x_3 \oplus x_3x_4 \oplus x_1 \oplus 1$
12. $f_{12}(x_4x_3x_2x_1) = x_1x_3 \oplus x_1x_2 \oplus x_4 \oplus x_3 \oplus x_2 \oplus 1$
13. $f_{13}(x_4x_3x_2x_1) = x_2x_3x_4 \oplus x_1x_3x_4 \oplus x_1x_2x_4 \oplus x_1x_2 \oplus x_4$
14. $f_{14}(x_4x_3x_2x_1) = x_1x_2x_3 \oplus x_2x_4 \oplus x_1x_3 \oplus x_1x_2 \oplus x_4 \oplus x_2 \oplus 1$
15. $f_{15}(x_4x_3x_2x_1) = x_2x_3x_4 \oplus x_1x_2x_4 \oplus x_3x_4 \oplus x_2x_4 \oplus x_1x_2 \oplus x_4 \oplus x_3 \oplus x_1 \oplus 1$

IV. OUTCOME OF RESEARCH

Once again, the following action of S-box is constructed by combining all of the above 2^{n-1} numbers of nonlinear Boolean functions using Boolean logic. The following nonlinear S-box is a straight S-box:

Table XVII: Straight Nonlinear S-box

Input $x_4\ x_3\ x_2\ x_1$	*Action of substitution-box* (4×4)	*Output* $y_4\ y_3\ y_2\ y_1$
0000, 0001, 0010, 0011, 0100, 0101, 0110, 0111, 1000, 1001,1010, 1011, 1100, 1101, 1110,1111	$(101110011000101)x_4x_3x_2 \oplus (010110110110100)x_4x_3x_1 \oplus (101110011000101)x_4x_2x_1 \oplus (100111001110010)x_3x_2x_1 \oplus (111000101110001)x_4x_3 \oplus (011111100000011)x_4x_2 \oplus (101010110101010)x_3x_1 \oplus (000100101101111)x_2x_1 \oplus (000100101101111)x_4 \oplus (110101010101001)x_3 \oplus (101010110101010)x_2 \oplus (111000101110001)x_1 \oplus 010010011011011$	1011, 1010, 0001, 1111, 0010, 1001, 1000, 1110, 0100, 0101, 1101, 0110, 1100, 0011, 0000, 0111



https://dx.doi.org/10.29322/IJSRP.14.01.2024.p14539

V. S-BOX'S OUTPUT MEASUREMENT

Let's substitute each binary input string into the action of s-box to measure the output of S-box. The measurement procedure is described below in detail for 4-variable inputs $\langle x_1, x_2, x_3, x_4 \rangle$:

1. When $x_1 = x_2 = x_3 = x_4 = 0, F(x_4x_3x_2x_1) =$ 010010011011011 $=$

$$\begin{array}{l} 14\ 13\ 12\ 11\ 10\ 9\ 8\ 7\ 6\ 5\ 4\ 3\ 2\ 1\ 0 \leftarrow index\ number(in) \\ \vdots\ \ \vdots\ \ \vdots\ \ \vdots\ \ \vdots\ \ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots \qquad \times \\ 0\ \ 1\ \ 0\ \ 0\ \ 1\ \ 0\ 0\ 1\ 1\ 0\ 1\ 1\ 0\ 1\ 1 \leftarrow Bit\ sequence(bs) \end{array} = bs \times binary\ base^{in} = 1 \times 2^{13} + 1 \times 2^{10} +$$

$1 \times 2^7 + 1 \times 2^6 + 1 \times 2^4 + 1 \times 2^3 + 1 \times 2^1 + 1 \times 2^0 = 8192 + 1024 + 128 + 64 + 64 + 16 + 8 + 2 + 1 = 9435_{10} = 9435_{10}$mod 16 $=$ 11 = 0xB =1011 =1 ⊕ 0 ⊕ 1⊕ 1 = 1

2. When $x_1 = 1\ and\ x_2 = x_3 = x_4 = 0,\ F(x_4x_3x_2x_1) =$ 111000101110001 ⊕ 010010011011011

$$\begin{array}{l} 1\ 1\ 1\ 0\ 0\ 0\ 1\ 0\ 1\ 1\ 1\ 0\ 0\ 0\ 1 \\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots \\ 0\ 1\ 0\ 0\ 1\ 0\ 0\ 1\ 1\ 0\ 1\ 1\ 0\ 1\ 1 \\ \hline 1\ 0\ 1\ 0\ 1\ 0\ 1\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0 \end{array} = \begin{array}{l} 14\ 13\ 12\ 11\ 10\ 9\ 8\ 7\ 6\ 5\ 4\ 3\ 2\ 1\ 0 \leftarrow index\ number(in) \\ \vdots\ \ \vdots\ \ \vdots\ \ \vdots\ \ \vdots\ \ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots \qquad \times \\ 1\ \ 0\ \ 1\ \ 0\ \ 1\ \ 0\ 1\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0 \leftarrow Bit\ sequence(bs) \end{array}$$

$= bs \times binary\ base^{in} = 1 \times 2^{14} + 1 \times 2^{12} + 1 \times 2^{10} + 1 \times 2^8 + 1 \times 2^7 + 1 \times 2^5 + 1 \times 2^3 + 1 \times 2^1 = 16384 + 4096 + 1024 + 256 + 128 + 32 + 8 + 2 = 9435_{10} = 21930_{10}$mod 16 $=$ 10 = 0xA = 1010 = 1 ⊕ 0 ⊕ 1 ⊕ 0 = 0

3. When $x_2 = 1\ and\ x_1 = x_3 = x_4 = 0, F(x_4x_3x_2x_1) =$ 101010110101010 ⊕ 010010011011011

$$\begin{array}{l} 1\ 0\ 1\ 0\ 1\ 0\ 1\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0 \\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots \\ 0\ 1\ 0\ 0\ 1\ 0\ 0\ 1\ 1\ 0\ 1\ 1\ 0\ 1\ 1 \\ \hline 1\ 1\ 1\ 0\ 0\ 0\ 1\ 0\ 1\ 1\ 1\ 0\ 0\ 0\ 1 \end{array} = \begin{array}{l} 14\ 13\ 12\ 11\ 10\ 9\ 8\ 7\ 6\ 5\ 4\ 3\ 2\ 1\ 0 \leftarrow index\ number(in) \\ \vdots\ \ \vdots\ \ \vdots\ \ \vdots\ \ \vdots\ \ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots \qquad \times \\ 1\ \ 1\ \ 1\ \ 0\ \ 0\ \ 0\ 1\ 0\ 1\ 1\ 1\ 0\ 0\ 0\ 1 \leftarrow Bit\ sequence(bs) \end{array}$$

$= bs \times binary\ base^{in} = 1 \times 2^{14} + 1 \times 2^{13} + 1 \times 2^{12} + 1 \times 2^8 + 1 \times 2^6 + 1 \times 2^5 + 1 \times 2^4 + 1 \times 2^0 = 16384 + 8192 + 4096 + 256 + 64 + 32 + 16 + 1 = 9435_{10} = 29041_{10}$mod 16 $=$ 1 = 0x1 = 0001 = 0 ⊕ 0 ⊕ 0 ⊕ 1 = 1

4. When $x_1 = x_2 = 1\ and\ x_3 = x_4 = 0,\ F(x_4x_3x_2x_1) =$ 000100101101111 ⊕ 101010110101010 ⊕ 111000101110001 ⊕ 010010011011011 $=$

$$\begin{array}{l} 0\ 0\ 0\ 1\ 0\ 0\ 1\ 0\ 1\ 1\ 0\ 1\ 1\ 1\ 1 \\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0 \\ 1\ 1\ 1\ 0\ 0\ 0\ 1\ 0\ 1\ 1\ 1\ 0\ 0\ 0\ 1 \\ 0\ 1\ 0\ 0\ 1\ 0\ 0\ 1\ 1\ 0\ 1\ 1\ 0\ 1\ 1 \\ \hline 0\ 0\ 0\ 1\ 0\ 0\ 1\ 0\ 1\ 1\ 0\ 1\ 1\ 1\ 1 \end{array} = \begin{array}{l} 14\ 13\ 12\ 11\ 10\ 9\ 8\ 7\ 6\ 5\ 4\ 3\ 2\ 1\ 0 \leftarrow index\ number(in) \\ \vdots\ \ \vdots\ \ \vdots\ \ \vdots\ \ \vdots\ \ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots \qquad \times \\ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ 1\ 0\ 1\ 1\ 0\ 1\ 1\ 1\ 1 \leftarrow Bit\ sequence(bs) \end{array}$$

$= bs \times binary\ base^{in} = 1 \times 2^{11} + 1 \times 2^8 + 1 \times 2^6 + 1 \times 2^5 + 1 \times 2^3 + 1 \times 2^2 + 1 \times 2^1 + 1 \times 2^0 = 2048 + 256 + 64 + 32 + 8 + 4 + 2 + 1 = 2415_{10} = 2415_{10}$mod 16 $=$ 15 = 0xF = 1111 = 1 ⊕ 1 ⊕ 1 ⊕ 1 = 0

5. When $x_3 = 1\ and\ x_1 = x_2 = x_4 = 0, F(x_4x_3x_2x_1) =$ 110101010101001⊕ 010010011011011

$$\begin{array}{l} 1\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 0\ 1 \\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots \\ 0\ 1\ 0\ 0\ 1\ 0\ 0\ 1\ 1\ 0\ 1\ 1\ 0\ 1\ 1 \\ \hline 1\ 0\ 0\ 1\ 1\ 1\ 0\ 0\ 1\ 1\ 1\ 0\ 0\ 1\ 0 \end{array} = \begin{array}{l} 14\ 13\ 12\ 11\ 10\ 9\ 8\ 7\ 6\ 5\ 4\ 3\ 2\ 1\ 0 \leftarrow index\ number(in) \\ \vdots\ \ \vdots\ \ \vdots\ \ \vdots\ \ \vdots\ \ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots \qquad \times \\ 1\ \ 0\ \ 0\ \ 1\ \ 1\ \ 1\ 0\ 0\ 1\ 1\ 1\ 0\ 0\ 1\ 0 \leftarrow Bit\ sequence(bs) \end{array}$$

$= bs \times binary\ base^{in} = 1 \times 2^{14} + 1 \times 2^{11} + 1 \times 2^{10} + 1 \times 2^9 + 1 \times 2^6 + 1 \times 2^5 + 1 \times 2^4 + 1 \times 2^1 = 16384 + 2048 + 1024 + 512 + 64 + 32 + 16 + 2 = 9435_{10} = 20082_{10}$mod 16 $=$ 2 = 0x2 = 0010 = 0 ⊕ 0 ⊕ 1⊕ 0 = 1

6. $When\ x_1 = x_3 = 1\ and\ x_2 = x_4 = 0, F(x_4x_3x_2x_1) =$ 101010110101010 ⊕ 110101010101001⊕ 111000101110001 ⊕ 010010011011011 $=$

$$\begin{array}{l} 1\ 0\ 1\ 0\ 1\ 0\ 1\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0 \\ 1\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 0\ 1 \\ 1\ 1\ 1\ 0\ 0\ 0\ 1\ 0\ 1\ 1\ 1\ 0\ 0\ 0\ 1 \\ 0\ 1\ 0\ 0\ 1\ 0\ 0\ 1\ 1\ 0\ 1\ 1\ 0\ 1\ 1 \\ \hline 1\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 0\ 1 \end{array} = \begin{array}{l} 14\ 13\ 12\ 11\ 10\ 9\ 8\ 7\ 6\ 5\ 4\ 3\ 2\ 1\ 0 \leftarrow index\ number(in) \\ \vdots\ \ \vdots\ \ \vdots\ \ \vdots\ \ \vdots\ \ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots \qquad \times \\ 1\ \ 1\ \ 0\ \ 1\ \ 0\ \ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 0\ 1 \leftarrow Bit\ sequence(bs) \end{array}$$

$= bs \times binary\ base^{in} = 1 \times 2^{14} + 1 \times 2^{13} + 1 \times 2^{11} + 1 \times 2^9 + 1 \times 2^7 + 1 \times 2^5 + 1 \times 2^3 + 1 \times 2^0 = 16384 + 8192 + 2048 + 512 + 128 + 32 + 8 + 1 = 27305_{10} = 27305_{10}$mod 16 $=$ 9 = 0x9 =1001=1⊕ 0 ⊕ 0 ⊕1 = 0

7. When $x_2 = x_3 = 1$ and $x_1 = x_4 = 0, F(x_4x_3x_2x_1) = 000000000000000 \oplus 110101010101001 \oplus 101010110101010 \oplus 010010011011011 =$

$$\begin{array}{c} \text{0 0 0 0 0 0 0 0 0 0 0 0 0 0 0} \\ \text{1 1 0 1 0 1 0 1 0 1 0 1 0 0 1} \\ \text{1 0 1 0 1 0 1 1 0 1 0 1 0 1 0} \\ \underline{\text{0 1 0 0 1 0 0 1 1 0 1 1 0 1 1}} \\ \text{0 0 1 1 0 1 1 1 1 0 1 1 0 0 0} \end{array} = \begin{array}{c} \text{14 13 12 11 10 9 8 7 6 5 4 3 2 1 0} \leftarrow index\ number(in) \\ \vdots \qquad \times \\ \text{0 0 1 1 0 1 1 1 1 0 1 1 0 0 0} \leftarrow Bit\ sequence(bs) \end{array}$$

$= bs \times binary\ base^{in} = 1 \times 2^{12} + 1 \times 2^{11} + 1 \times 2^{9} + 1 \times 2^{8} + 1 \times 2^{7} + 1 \times 2^{6} + 1 \times 2^{4} + 1 \times 2^{3} = 4096 + 2048 + 512 + 256 + 128 + 64 + 16 + 8 = 7128_{10} = 7128_{10} \bmod 16 = 8$ =0x8=1000=$1 \oplus 0 \oplus 0 \oplus 0 = 1$

8. When $x_1 = x_2 = x_3 = 1$ and $x_4 = 0, F(x_4x_3x_2x_1) = 100111001110010 \oplus 000000000000000 \oplus 101010110101010 \oplus 000100101101111 \oplus 110101010101001 \oplus 101010110101010 \oplus 111000101110001 \oplus 010010011011011 =$

$$\begin{array}{c} \text{1 0 0 1 1 1 0 0 1 1 1 0 0 1 0} \\ \text{0 0 0 0 0 0 0 0 0 0 0 0 0 0 0} \\ \text{1 0 1 0 1 0 1 1 0 1 0 1 0 1 0} \\ \text{0 0 0 1 0 0 1 0 1 1 0 1 1 1 1} \\ \text{1 1 0 1 0 1 0 1 0 1 0 1 0 0 1} \\ \text{1 0 1 0 1 0 1 1 0 1 0 1 0 1 0} \\ \text{1 1 1 0 0 0 1 0 1 1 1 0 0 0 1} \\ \underline{\text{0 1 0 0 1 0 0 1 1 0 1 1 0 1 1}} \\ \text{1 1 1 1 0 0 0 0 0 0 1 1 1 1 0} \end{array} = \begin{array}{c} \text{14 13 12 11 10 9 8 7 6 5 4 3 2 1 0} \leftarrow index\ number(in) \\ \vdots \qquad \times \\ \text{1 1 1 1 0 0 0 0 0 0 1 1 1 1 0} \leftarrow Bit\ sequence(bs) \end{array}$$

$= bs \times binary\ base^{in} = 1 \times 2^{14} + 1 \times 2^{13} + 1 \times 2^{12} + 1 \times 2^{11} + 1 \times 2^{4} + 1 \times 2^{3} + 1 \times 2^{2} + 1 \times 2^{1} = 16384 + 8192 + 4096 + 2048 + 16 + 8 + 4 + 2 = 30750_{10} = 30750_{10} \bmod 16 = 14$ = 0xE = 1110 =$1 \oplus 1 \oplus 1 \oplus 0 = 1$

9. When $x_4 = 1$ and $x_1 = x_2 = x_3 = 0, F(x_4x_3x_2x_1) = 000100101101111 \oplus 010010011011011$

$$\begin{array}{c} \text{0 0 0 1 0 0 1 0 1 1 0 1 1 1 1} \\ \vdots \\ \underline{\text{0 1 0 0 1 0 0 1 1 0 1 1 0 1 1}} \\ \text{0 1 0 1 1 0 1 1 0 1 1 0 1 0 0} \end{array} = \begin{array}{c} \text{14 13 12 11 10 9 8 7 6 5 4 3 2 1 0} \leftarrow index\ number(in) \\ \vdots \qquad \times \\ \text{0 1 0 1 1 0 1 1 0 1 1 0 1 0 0} \leftarrow Bit\ sequence(bs) \end{array}$$

$= bs \times binary\ base^{in} = 1 \times 2^{13} + 1 \times 2^{11} + 1 \times 2^{10} + 1 \times 2^{8} + 1 \times 2^{7} + 1 \times 2^{5} + 1 \times 2^{4} + 1 \times 2^{2} = 8192 + 2048 + 1024 + 256 + 128 + 32 + 16 + 4 = 9435_{10} = 11700_{10} \bmod 16 = 4$ = 0x4 = 0100 = $0 \oplus 1 \oplus 0 \oplus 0 = 1$

10. When $x_1 = x_4 = 1$ and $x_2 = x_3 = 0, F(x_4x_3x_2x_1) = 000000000000000 \oplus 000100101101111 \oplus 111000101110001 \oplus 010010011011011 =$

$$\begin{array}{c} \text{0 0 0 0 0 0 0 0 0 0 0 0 0 0 0} \\ \text{0 0 0 1 0 0 1 0 1 1 0 1 1 1 1} \\ \text{1 1 1 0 0 0 1 0 1 1 1 0 0 0 1} \\ \underline{\text{0 1 0 0 1 0 0 1 1 0 1 1 0 1 1}} \\ \text{1 0 1 1 1 0 0 1 1 0 0 0 1 0 1} \end{array} = \begin{array}{c} \text{14 13 12 11 10 9 8 7 6 5 4 3 2 1 0} \leftarrow index\ number(in) \\ \vdots \qquad \times \\ \text{1 0 1 1 1 0 0 1 1 0 0 0 1 0 1} \leftarrow Bit\ sequence(bs) \end{array}$$

$= bs \times binary\ base^{in} = 1 \times 2^{14} + 1 \times 2^{12} + 1 \times 2^{11} + 1 \times 2^{10} + 1 \times 2^{7} + 1 \times 2^{6} + 1 \times 2^{2} + 1 \times 2^{0} = 16384 + 4096 + 2048 + 1024 + 128 + 64 + 4 + 1 = 23749_{10} = 23749_{10} \bmod 16 = 5$ = 0x5 = 0101 = $0 \oplus 1 \oplus 0 \oplus 1 = 0$

11. When $x_2 = x_4 = 1$ and $x_1 = x_3 = 0, F(x_4x_3x_2x_1) = 011111100000011 \oplus 000100101101111 \oplus 101010110101010 \oplus 010010011011011 =$

$$\begin{array}{c} \text{0 1 1 1 1 1 1 0 0 0 0 0 0 1 1} \\ \text{0 0 0 1 0 0 1 0 1 1 0 1 1 1 1} \\ \text{1 0 1 0 1 0 1 1 0 1 0 1 0 1 0} \\ \underline{\text{0 1 0 0 1 0 0 1 1 0 1 1 0 1 1}} \\ \text{1 0 0 0 1 1 1 0 0 0 1 1 1 0 1} \end{array} = \begin{array}{c} \text{14 13 12 11 10 9 8 7 6 5 4 3 2 1 0} \leftarrow index\ number(in) \\ \vdots \qquad \times \\ \text{1 0 0 0 1 1 1 0 0 0 1 1 1 0 1} \leftarrow Bit\ sequence(bs) \end{array}$$

$= bs \times binary\ base^{in} = 1 \times 2^{14} + 1 \times 2^{10} + 1 \times 2^{9} + 1 \times 2^{8} + 1 \times 2^{4} + 1 \times 2^{3} + 1 \times 2^{2} + 1 \times 2^{0} = 16384 + 1024 + 512 + 256 + 16 + 8 + 4 + 1 = 7128_{10} = 18205_{10} \bmod 16 = 13$ = 0xD = 1101 = $1 \oplus 1 \oplus 0 \oplus 1 = 1$

https://dx.doi.org/10.29322/IJSRP.14.01.2024.p14539

12. When $x_1 = x_2 = x_4 = 1$ and $x_3 = 0, F(x_4x_3x_2x_1) = 101110011000101 \oplus 011111100000011 \oplus 000000000000000 \oplus 000100101101111 \oplus 000100101101111 \oplus 101010110101010 \oplus 111000101110001 \oplus 010010011011011 =$

$$\begin{array}{ccccccccccccccc}
1&0&1&1&1&0&0&1&1&0&0&0&1&0&1\\
0&1&1&1&1&1&1&0&0&0&0&0&0&1&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&1&0&1&1&0&1&1&1&1\\
0&0&0&1&0&0&1&0&1&1&0&1&1&1&1\\
1&0&1&0&1&0&1&1&0&1&0&1&0&1&0\\
1&1&1&0&0&0&1&0&1&1&1&0&0&0&1\\
\underline{0}&\underline{1}&\underline{0}&\underline{0}&\underline{1}&\underline{0}&\underline{0}&\underline{1}&\underline{1}&\underline{0}&\underline{1}&\underline{1}&\underline{0}&\underline{1}&\underline{1}\\
\\
1&1&0&0&0&1&1&1&1&0&0&0&1&1&0
\end{array} = \begin{array}{cccccccccccccccl}
14&13&12&11&10&9&8&7&6&5&4&3&2&1&0&\leftarrow index\ number(in)\\
\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\qquad\times\\
1&1&0&0&0&1&1&1&1&0&0&0&1&1&0&\leftarrow Bit\ sequence(bs)
\end{array}$$

$= bs \times binary\ base^{in} = 1 \times 2^{14} + 1 \times 2^{13} + 1 \times 2^9 + 1 \times 2^8 + 1 \times 2^7 + 1 \times 2^6 + 1 \times 2^2 + 1 \times 2^1 = 16384 + 8192 + 512 + 256 + 128 + 64 + 4 + 2 = 25542_{10} = 25542_{10} \text{mod } 16 = 6 = 0\text{x}6 = 0110 = 0 \oplus 1 \oplus 1 \oplus 0 = 0$

13. When $x_3 = x_4 = 1$ and $x_1 = x_2 = 0, F(x_4x_3x_2x_1) = 111000101110001 \oplus 000100101101111 \oplus 110101010101001 \oplus 010010011011011 =$

$$\begin{array}{ccccccccccccccc}
1&1&1&0&0&0&1&0&1&1&1&0&0&0&1\\
0&0&0&1&0&0&1&0&1&1&0&1&1&1&1\\
1&1&0&1&0&1&0&1&0&1&0&1&0&0&1\\
\underline{0}&\underline{1}&\underline{0}&\underline{0}&\underline{1}&\underline{0}&\underline{0}&\underline{1}&\underline{1}&\underline{0}&\underline{1}&\underline{1}&\underline{0}&\underline{1}&\underline{1}\\
\\
0&1&1&0&1&1&0&0&1&1&0&1&1&0&0
\end{array} = \begin{array}{cccccccccccccccl}
14&13&12&11&10&9&8&7&6&5&4&3&2&1&0&\leftarrow index\ number(in)\\
\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\qquad\times\\
0&1&1&0&1&1&0&0&1&1&0&1&1&0&0&\leftarrow Bit\ sequence(bs)
\end{array}$$

$= bs \times binary\ base^{in} = 1 \times 2^{13} + 1 \times 2^{12} + 1 \times 2^{10} + 1 \times 2^9 + 1 \times 2^6 + 1 \times 2^5 + 1 \times 2^3 + 1 \times 2^2 = 8192 + 4096 + 1024 + 512 + 64 + 32 + 8 + 4 = 13932_{10} = 13932_{10} \text{mod } 16 = 12 = 0\text{xC} = 1100 = 1 \oplus 1 \oplus 0 \oplus 0 = 0$

14. When $x_1 = x_3 = x_4 = 1$ and $x_2 = 0,$ $F(x_4x_3x_2x_1) = 010110110110100 \oplus 111000101110001 \oplus 000000000000000 \oplus 101010110101010 \oplus 000100101101111 \oplus 110101010101001 \oplus 111000101110001 \oplus 010010011011011 =$

$$\begin{array}{ccccccccccccccc}
0&1&0&1&1&0&1&1&0&1&1&0&1&0&0\\
1&1&1&0&0&0&1&0&1&1&1&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&1&0&1&0&1&1&0&1&0&1&0&1&0\\
0&0&0&1&0&0&1&0&1&1&0&1&1&1&1\\
1&1&0&1&0&1&0&1&0&1&0&1&0&0&1\\
1&1&1&0&0&0&1&0&1&1&1&0&0&0&1\\
\underline{0}&\underline{1}&\underline{0}&\underline{0}&\underline{1}&\underline{0}&\underline{0}&\underline{1}&\underline{1}&\underline{0}&\underline{1}&\underline{1}&\underline{0}&\underline{1}&\underline{1}\\
\\
0&1&1&1&1&1&1&0&0&0&0&0&0&1&1
\end{array} = \begin{array}{cccccccccccccccl}
14&13&12&11&10&9&8&7&6&5&4&3&2&1&0&\leftarrow index\ number(in)\\
\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\qquad\times\\
0&1&1&1&1&1&1&0&0&0&0&0&0&1&1&\leftarrow Bit\ sequence(bs)
\end{array}$$

$= bs \times binary\ base^{in} = 1 \times 2^{13} + 1 \times 2^{12} + 1 \times 2^{11} + 1 \times 2^{10} + 1 \times 2^9 + 1 \times 2^8 + 1 \times 2^1 + 1 \times 2^0 = 8192 + 4096 + 2048 + 1024 + 512 + 256 + 2 + 1 = 16131_{10} = 16131_{10} \text{mod } 16 = 3 = 0\text{x}3 = 0011 = 0 \oplus 0 \oplus 1 \oplus 1 = 0$

15. When $x_2 = x_3 = x_4 = 1$ and $x_1 = 0,$ $F(x_4x_3x_2x_1) = 101110011000101 \oplus 111000101110001 \oplus 011111100000011 \oplus 000000000000000 \oplus 000100101101111 \oplus 110101010101001 \oplus 101010110101010 \oplus 010010011011011 =$

$$\begin{array}{ccccccccccccccc}
1&0&1&1&1&0&0&1&1&0&0&0&1&0&1\\
1&1&1&0&0&0&1&0&1&1&1&0&0&0&1\\
0&1&1&1&1&1&1&0&0&0&0&0&0&1&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&1&0&1&1&0&1&1&1&1\\
1&1&0&1&0&1&0&1&0&1&0&1&0&0&1\\
1&0&1&0&1&0&1&1&0&1&0&1&0&1&0\\
\underline{0}&\underline{1}&\underline{0}&\underline{0}&\underline{1}&\underline{0}&\underline{0}&\underline{1}&\underline{1}&\underline{0}&\underline{1}&\underline{1}&\underline{0}&\underline{1}&\underline{1}\\
\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0
\end{array} = \begin{array}{cccccccccccccccl}
14&13&12&11&10&9&8&7&6&5&4&3&2&1&0&\leftarrow index\ number(in)\\
\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\qquad\times\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&\leftarrow Bit\ sequence(bs)
\end{array} = bs \times binary\ base^{in}$$

$= 0$

16. $When\ x_1 = x_2 = x_3 = x_4 = 1,$ $F(x_4x_3x_2x_1) = 000000000000000 \oplus 101110011000101 \oplus 010110110110100 \oplus 101110011000101 \oplus 100111001110010 \oplus 111000101110001 \oplus 011111100000011 \oplus 000000000000000 \oplus 000000000000000 \oplus 101010110101010 \oplus 000100101101111 \oplus 000100101101111 \oplus 110101010101001 \oplus 101010110101010 \oplus 111000101110001 \oplus 010010011011011 =$

https://dx.doi.org/10.29322/IJSRP.14.01.2024.p14539

$$\begin{array}{ccccccccccccccc}
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&1&1&1&0&0&1&1&0&0&0&1&0&1\\
0&1&0&1&1&0&1&1&0&1&1&0&1&0&0\\
1&0&1&1&1&0&0&1&1&0&0&0&1&0&1\\
1&0&0&1&1&1&0&0&1&1&1&0&0&1&0\\
1&1&1&0&0&0&1&0&1&1&1&0&0&0&1\\
0&1&1&1&1&1&1&0&0&0&0&0&0&1&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&1&0&1&0&1&1&0&1&0&1&0&1&0\\
0&0&0&1&0&0&1&0&1&1&0&1&1&1&1\\
0&0&0&1&0&0&1&0&1&1&0&1&1&1&1\\
1&1&0&1&0&1&0&1&0&1&0&1&0&0&1\\
1&0&1&0&1&0&1&1&0&1&0&1&0&1&0\\
1&1&1&0&0&0&1&0&1&1&1&0&0&0&1\\
\underline{0}&\underline{1}&\underline{0}&\underline{0}&\underline{1}&\underline{0}&\underline{0}&\underline{1}&\underline{1}&\underline{0}&\underline{1}&\underline{1}&\underline{0}&\underline{1}&\underline{1}\\
0&0&1&0&0&1&0&1&0&1&1&0&1&1&1
\end{array}
= \begin{array}{ccccccccccccccc l}
14&13&12&11&10&9&8&7&6&5&4&3&2&1&0 & \leftarrow index\ number(in)\\
\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots & \qquad\qquad \times\\
0&0&1&0&0&1&0&1&0&1&1&0&1&1&1 & \leftarrow Bit\ sequence(bs)
\end{array} = bs \times binary\ base^{in}$$

$$= 1 \times 2^{12} + 1 \times 2^{9} + 1 \times 2^{7} + 1 \times 2^{5} + 1 \times 2^{4} + 1 \times 2^{2} + 1 \times 2^{1} + 1 \times 2^{0} = 4096 + 512 + 128 + 32 + 16 + 4 + 2 + 1 = 4791_{10} = 4791_{10} \bmod 16 = 7 = 0x7 = 0111 = 0 \oplus 1 \oplus 1 \oplus 1 = 1$$

VI. Conclusion

To conclude the investigation into nonlinear S-box construction, different S-box construction techniques were analyzed. And then the purpose of the component-based nonlinear S-box construction study was completed. Different mathematical interpretations of S-box construction were finalized based on a literature review, mathematical problem solving, analysis, and discussion with researchers. It was possible to understand the concept of the S-box construction mechanism after studying a lot of research papers. The purpose of the study was to disseminate scientific knowledge to scientific readers scattered around the world. The proposed S-box has been developed keeping in mind the needs of scientific students and researchers so that they can benefit from reading this article. I think this article will attract the attention of scientific readers. The article was devoted to presenting complex mathematical concepts in a simple way so that scientific readers could grasp the concept of the nonlinear S-box construction technique. If readers are interested, they can construct a higher-dimensional S-box using the proposed nonlinear S-box construction technique.

A. *Recommendation*

So, based on the conclusion, some recommendations are prepared: If anyone is interested in designing an S-box, I suggest reading this article several times with full attention and internalizing the functional idea of the S-box construction mechanism. I believe everyone will be able to build large-scale S-boxes after capturing the concept of the proposed 4×4 nonlinear S-box. But I recommend that students should analyze this matter internally. They should take the initiative to familiarize themselves with the mathematics required to construct lower- or higher-dimensional S-Boxes.

B. *Author's Request to Readers*

Dear scientific readers, if you benefited from the article, please pray to our God for my physical and mental well-being.

C. *Limitation*

The proposed S-box is a simple 4×4 nonlinear S-box. This is not designed for professional work.

Acknowledgement

First of all, I express my gratitude to almighty Allah, who permits me to complete this task. Next, I express my sincere thanks to my elder brother, Md. Abul Kalam Azad, who provided financial support to study at Novosibirsk State University. I would like to express my special thanks to respected dean D.Sc. Lavrentiev Mikhail Mikhailovich, my teacher Dr. Beterov Ilya Igorevich, Dr. Natalia Tokareva, post-doctoral student Dr. Santu Pal, and lecturer Irina Khilchuk for those who made a wonderful research atmosphere for me to do this wonderful research on the "S-box construction in modern cipher" that helped me in doing a lot of extensive research and I came to know about how to use discrete mathematical knowledge in cryptography and so many new creative mathematical ideas, and therefore I am really grateful to them. I am personally very happy to have completed this scientific task successfully.

REFERENCES

[1] Claude Carlet. Boolean functions for cryptography and coding theory; Cambridge University Press: Cambridge, UK, 2021..

[2] John A Clark, Jeremy L Jacob, Susan Stepney, Subhamoy Maitra, and William Millan. Evolving Boolean functions satisfying multiple criteria. In Progress in Cryptology—INDOCRYPT 2002: Third International Conference on Cryptology at Hyderabad in India, December 16–18, 2002 Proceedings 3, pp. 246–259. Doi:10.1007/3-540-36231-2_20H. Poor, *An Introduction to Signal Detection and Estimation*. New York: Springer-Verlag, 1985, ch. 4.

[3] Anne Canteaut. Lecture notes on cryptographic Boolean functions. Inria, Paris, France, 3, 2016.

[4] Claude Carlet, Yves Crama, and Peter L Hammer. Boolean models and methods in mathematics, Computer Science and Engineering || Vectorial Boolean functions for cryptography. 2010 pages 398–470. doi:10.1017/CBO9780511780448.012

[5] Dar'ya Aleksandrovna Zyubina and Natalia Nikolaevna Tokareva. Cryptographic properties of a simple s-box construction based on a Boolean function and a permutation. *Applied Discrete Mathematics*. Application, (13):41–43, 2020. Doi: 10.17223/2226308X/13/13

[6] Claude Carlet. Boolean functions for cryptography and coding theory. Cambridge University Press, 2021.

[7] Natalia Tokareva. Bent functions: results and applications to cryptography. Academic Press, 2015.

[8] Maram K Balajee and JM Gnanasekar. Evaluation of key dependent s-box based data security algorithm using hamming distance and balanced output. Tem Journal, 5(1):67-75, 2016.

[9] Pedro Miguel Sosa. Calculating nonlinearity of Boolean functions with Walsh Hadamard transform. UCSB, Santa Barbara, pages 1–4, 2016.

[10] Thomas W Cusick and Pantelimon Stanica. Cryptographic Boolean functions and applications. Academic Press, 2017. ISBN: 0128111305, 9780128111307

[11] Claude E Shannon. A mathematical theory of cryptography. Mathematical Theory of Cryptography, 1945.

[12] Stephen Boyd and Lieven Vandenberghe. Introduction to applied linear algebra: vectors, matrices, and least squares. Cambridge university press, 2018.

[13] Claude E Shannon. Communication theory of secrecy systems. The Bell system technical journal, 28(4):656–715, 1949.

[14] Pavol Zajac and Mat´uˇs J´okay. Multiplicative complexity of bijective 4× 4 S-boxes. Cryptography and Communications, 6(3):255–277, 2014.

[15] Tsonka Baicheva, Dusan Bikov, Yuri Borissov, Limonka Koceva Lazarova, Aleksandra Stojanova, Liliya Stoykova, and Stela Zhelezova. Finding an effective metric used for bijective s-box generation by genetic algorithms.2014.

[16] Darya Zyubina, Maxim Zapolskiy, Irina Khilchuk, and Natalia Tokareva.S-box construction based on a boolean function and a permutation. In Fifth Conference on Software Engineering and Information Management (SEIM-2020), pages 24–27, 2020.

[17] Reynier Antonio de la Cruz Jim´enez. On some methods for constructing almost optimal s-boxes and their resilience against sidechannel attacks. Cryptology, 2018.

[18] W Eltayeb Ahmed. A modern method for constructing the s-box of advanced encryption standard. Applied Mathematics,10(4):234–244, 2019.

[19] Musheer Ahmad, Mohammad Najam Doja, and MM Sufyan Beg. ABC optimization-based construction of strong substitution boxes. Wireless Personal Communications, 101:1715–1729, 2018.

[20] Musheer Ahmad, Ishfaq Ahmad Khaja, Abdullah Baz, Hosam Alhakami and Wajdi Alhakami. Particle swarm optimization based highly nonlinear substitution-boxes generation for security applications. IEEE Access, 8:116132–116147, 2020. Doi:10.1109/ACCESS.2020.3004449.

[21] Meryam Saad Fadhil, Alaa Kadhim Farhan, and Mohammad Natiq Fadhil. Designing substitution box based on the 1d logistic map chaotic system. In IOP Conference Series: Materials Science and Engineering, volume 1076, issue 1, page 012041. IOP Publishing, 2021. Doi:10.1088/1757-899X/1076/1/012041

[22] Christian Kaspers and Yue Zhou. The number of almost perfect nonlinear functions grows exponentially. Journal of Cryptology, 34:1–37, 2021.

[23] Erdener Uyan. Analysis of Boolean functions with respect to Walsh spectrum. 2013

[24] Majid Khan, Tariq Shah, and Syeda Iram Batool. Construction of s-box based on chaotic Boolean functions and its application in image encryption. Neural Computing and Applications, 27:677–685, 2016

[25] Zijing Jiang and Qun Ding. Construction of an s-box based on chaotic and bent functions. Symmetry, 13(4):671, 2021. Doi:10.3390/sym13040671

[26] Joan Daemen and Vincent Rijmen. The design of Rijndael, volume 2. Springer, 2002.

[27] Iqtadar Hussain, Amir Anees, Temadher Alassiry Al-Maadeed, and Muham- mad Tahir Mustafa. Construction of s-box based on chaotic map and algebraic structures. Symmetry, 11(3):351, 2019. Doi: 10.3390/sym11030351

[28] Elaine Barker and Nicky Mouha. Recommendation for the triple data encryption algorithm (TDEA) block cipher. Technical report, National Institute of Standards and Technology (NIST), 800, 67. 2017

[29] Liyana Chew Nizam Chew and Eddie Shahril Ismail. S-box construction based on linear fractional transformation and permutation function. Symmetry, 12(5):826, 2020. Doi:10.3390/sym12050826

[30] Pavol Zajac and Matus Jokay. Multiplicative complexity of bijective 4× 4 S-boxes. Cryptography and Communications, 6(3):255–277, 2014.

[31] Dusan Bikov, Iliya Bouyukliev, and Stefka Bouyuklieva. Bijective s-boxes of different sizes obtained from quasi-cyclic codes. Journal of Algebra Combinatorics Discrete Structures and Applications, 6(3):123–134, 2019. Doi: 10.13069/jacodesmath.617232

[32] Data Encryption Standard et al. Data encryption standard. Federal Information Processing Standards Publication, 112:3, 1999.

[33] Andrey Bogdanov, Lars R Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew JB Robshaw, Yannick Seurin and Charlotte Vikkelsoe. Present: An ultra-lightweight block cipher. In Cryptographic Hardware and Embedded Systems-CHES: 9th International Workshop, Vienna, Austria, September 10-13, 2007. Proceedings 9, pages 450–466.

[34] Joan Daemen and Vincent Rijmen. Aes proposal: Rijndael. 1999

AUTHOR BIOGRAPHY

Md. Shamim Hossain Biswas

MSc in Quantum Technology and Cryptography, Novosibirsk State University, Russia
MSc in Software Engineering (Cybersecurity), Daffodil International University
MA in English (TESOL), North South University, Bangladesh
BSc in Computer Science & Engineering, Stamford University
ORCID: 0000-0002-4595-1470, Cell: +7905 934 68 15
E-mail: s.biswas@g.nsu.ru, shamim.biswas@northsouth.edu

APPENDIX A:

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НОВОСИБИРСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ»**

ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Кафедра _____System of Informatics_______________________

Направление подготовки 09.04.01 Информатика и вычислительная техника

Направленность (профиль) Квантовые технологии и криптография

ОТЧЕТ

о прохождении производственной практики, технологической (проектно-технологической) практики
(указывается наименование практики)

Обучающегося _____Md. Shamim Hossain Biswas_____________группы №__22226___ курса 1
(Ф.И.О. полностью)

Тема задания:______ S-box Construction in Modern Cipher ___________________________

Место прохождения практики: Novosibirsk State University, Laboratory of Modern Computer Technologies, 1 pirogova str. Novosibrisk, 630090, Russia ___________________________
(полное наименование организации и структурного подразделения, индекс, адрес)

Сроки прохождения практики: с 23.01.2023 г. по 03.06.2023 г.

Руководитель практики от профильной организации	Tokareva Natalya Nikolaevna (Ф.И.О. полностью, должность)	__Assoc.Prof__ (подпись)
Руководитель практики от НГУ	Marina Derzho (Ф.И.О. полностью, должность)	__Senior Lecturer__ (подпись)
Руководитель ВКР	__ Dr. IlyIgorevich Beterov _ (Ф.И.О. полностью)	_Assoc.Prof__ (должность)

Оценка по итогам защиты отчета: _____________________ отлично______________________
(неудовлетворительно, удовлетворительно, хорошо, отлично)

Отчет заслушан на заседании кафедры ____Faculty of Information Technology_____________
(наименование кафедры)

протокол _________**от** «__17___» __________06. 2023_____г.

Новосибирск 2023

https://dx.doi.org/10.29322/IJSRP.14.01.2024.p14539

APPENDIX B:

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НОВОСИБИРСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ»

ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Кафедра _____System of Informatics_____

Направление подготовки 09.04.01 Информатика и вычислительная техника

Направленность (профиль) Квантовые технологии и криптография

УТВЕРЖДАЮ:

Заведующий кафедрой

_____
(наименование кафедры)

_____
(Ф.И.О.)

_____
(подпись)

ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ

для прохождения производственной практики, технологической (проектно-технологической) практики
(указывается наименование практики)

Обучающегося ___**Md. Shamim Hossain Biswas**_____ **группа №_22226**___
(Ф.И.О. полностью)

Тема задания:__S-box Construction in Modern Cipher_____

Место прохождения практики:___ Novosibirsk State University, Laboratory of Modern Computer Technologies, 1 Pirogova str. Novosibrisk, 630090, Russia

(полное наименование организации и структурного подразделения, индекс, адрес)

Сроки прохождения практики: с 23.01.2023 г. по 03.06.2023 г.

Форма предоставления на кафедру выполненного задания: письменный отчет

Руководитель практики от НГУ	_Marina Derzho _ (Ф.И.О. полностью)	_ Senior Lecturer_ (должность)
Руководитель ВКР	__ Dr. IlyIgorevich Beterov__ (Ф.И.О. полностью)	____Assoc.Prof _____ (должность)

1. **Виды работ и требования к их выполнению:**__**Scientific Research Report**_____
2. **Виды отчетных материалов:** Письменный отчет по установленной форме, отзыв руководителя, электронная презентация

https://dx.doi.org/10.29322/IJSRP.14.01.2024.p14539

APPENDIX C:

Заведующему кафедрой __ Syestem of informatics______

обучающегося факультета информационных технологий

1 курса, группы №__22226_______

направление 09.04.01 Информатика и вычислительная техника
(код и наименование направления)

направленность (профиль) Квантовые технологии и криптография
(наименование профиля)

Md. Shamim Hossain Biswas

(Ф.И.О.)

ЗАЯВЛЕНИЕ.

Прошу направить меня на **производственную практику, технологическую (проектно-технологическую) практику** в организацию*
(*указывается наименование практики*)

Novosibirsk State University, Laboratory of Modern Computer Technologies, 1 Pirogova str. Novosibrisk, 630090, Russia

(*полное название организации с указанием организационно-правовой формы и полного почтового адреса*)

Дата: «____17.06__»_________2023___г. Shamim
(подпись обучающегося)

Согласовано:

Руководитель ВКР ______ (подпись) Dr. IlyIgorevich Beterov (Ф.И.О. полностью) __Assoc.Prof____ (должность)

* Список организаций для прохождения практики, с которыми заключены договоры, размещен на сайте ФИТ. Результаты прохождения практики используются для дальнейшей подготовки выпускной квалификационной работы, поэтому целесообразно выбирать место прохождения практики по месту основной работы руководителя ВКР, либо по его рекомендации.

APPENDIX D:

Задание утверждено на заседании кафедры ____Faculty of Information Technology ____________
(наименование кафедры)

протокол от «___» ____________ 20__ г. **Дата выдачи задания:** «___» ____________ 20__ г.

Руководитель практики от НГУ: ____________ (подпись) ___ Marina Derzho ___ (ФИО, должность)

Руководитель ВКР: ____________ (подпись) __Dr. Ilya Igorevich Beterov__ (ФИО, должность)

Руководитель практики от профильной организации: ____________ (подпись) ___Marina Derzho___ (ФИО, должность)

Задание принял(а) к исполнению: ____________ (подпись обучающегося) **Md. Shamim Hossain Biswas** (ФИО)

Инструктаж обучающегося по ознакомлению с требованиями охраны труда, техники безопасности, пожарной безопасности, а также с правилами внутреннего трудового распорядка проведен с оформлением установленной документации «___» ________ 20 ___ г.

Руководитель практики назначен распорядительным актом от «13» __01__ 2023 г. № 0052-2

(*Для обучающихся, направленных на практику в профильную организацию, указываются данные распорядительного акта профильной организации. Для обучающихся, направленных на практику в НГУ, указывается распорядительный акт по университету*).

Руководитель практики: ____________ (подпись)* ___ Marina Derzho_____ (ФИО, должность)

* *Подпись руководителя практики в профильной организации заверяется в профильной организации.*