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 research aimed to investigate and reveal the construction mechanism of a component-based nonlinear S-box (substitution box). The S-box operates within a Boolean space, performing substitution through nonlinear mapping between input and output vectors to enhance confusion in the encryption process. The proposed nonlinear S-box (vectorial Boolean function) can be straight, compressible, and expandable when utilized in modern block ciphers. To engage the attention of scientific readers, this article explains how to construct a component-based nonlinear S-box using the n-variable affine, linear, and nonlinear Boolean functions. In essence, this procedure alludes to an action of the S-box, which is a mathematical function. The primary motivation for conducting this research was to review several existing S-box construction techniques and apply innovative ideas mathematically to construct a new S-box. The study employed both computational and exploratory research methods. The data collection methods included conducting a literature review, using critical thinking strategies, and facilitating focus group discussions to capture the mathematical notion underlying the nonlinear S-box construction technique. The research population included graduate and doctoral students as well as academic professors from Novosibirsk State University.

Index Terms- cryptology, cryptography, nonlinear s-box, nonlinearity, vectorial Boolean function, affine function, Boolean space.

I. INTRODUCTION

Cryptology is the study of the science of secure communication techniques. It includes both the terms cryptography and cryptanalysis. Cryptanalysis involves discovering weaknesses and breaking the encrypted texts to reveal their original meaning. In contrast, cryptography creates nonreadable messages, i.e., encrypted texts. In general, we classify cryptography into two categories: classical and modern cryptography. We notice the application of cryptography in our daily lives: computer passwords, digital currencies, secure web browsing, digital signatures, authentication, and so on. Our current digital security system uses symmetric, asymmetric, and hash-based cryptography. In symmetric cryptography, symmetric ciphers fall into two categories: stream ciphers and block ciphers. Symmetric encryption ciphers use S-box as a substitution cipher. 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 nonlinearity components of a cryptosystem implement the confusion technique. On the other hand, diffusion is achieved by making a slight change in the input. Nonlinear Boolean functions also play an important role in one-way hash functions and stream ciphers. Developing an S-box aims to understand the construction mechanism of an S-box in block ciphers. Let's see some concrete definitions of Boolean functions and their related short summaries.

A. Boolean function

A Boolean function accepts inputs and outputs values from the two-element set $\{0 = \text{false}, 1 = \text{true}\}$. The Boolean function, also known as a switching function, refers to an electric circuit. An arbitrary mapping from $\mathbb{Z}_2{}^n$ to $\mathbb{Z}_2$ defines an n-variable Boolean function (*f*), denoted as $f : f_{2^n} \to f_2$. Cryptographic Boolean functions fall into various categories [1, 2, 3]. But what type of Boolean function do we need to use to construct the S-box? It actually depends on the type of S-box. Boolean functions and S-box construction play a fundamental role in designing symmetric-key ciphers. We use the formula, i.e., $2^{2^n} = 2^{2^4} = 65536$, to determine the number of Boolean functions for degree 4. Among them, the number of linear Boolean functions totals $2^n = 2^4 = 16$. To find the number of nonlinear Boolean functions, we simply subtract the number of linear Boolean functions from the total number of Boolean functions: $2^{2^n} - 2^n = 2^{2^4} - 2^4 = 65520$. Furthermore, we can use the formula, i.e., $A_n = 2^{n+1} = 2^{4+1} = 32$ in order to determine the number of affine Boolean functions in a four-dimensional vector space.

This publication is licensed under Creative Commons Attribution CC BY.

B. Single-valued Boolean function

A function that accepts multiple inputs and returns a single output is known as a single-valued Boolean function. For example, when $n = 2$, we use the transformation $f: \mathbb{Z}_2^2 \to \mathbb{Z}_2$ or$f: \mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_2$ or $f: \{0,1\} \times \{0,1\} \to \{0,1\} \Mapsto f: \{00,01,10,11\} \to \{0,1\}$ to represent a single-valued Boolean function.

C. Multi-valued Boolean function

A function that takes multiple inputs and returns multiple outputs is known as a multi-valued Boolean function. A multi-valued Boolean function, for instance, would be $f: \mathbb{Z}_2^n \to \mathbb{Z}_2^m \Mapsto f: \mathbb{Z}_2^2 \to \mathbb{Z}_2^2$ or $f: \mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_2 \times \mathbb{Z}_2$ or $f: \{0,1\} \times \{0,1\} \to \{1,0\} \times \{0,1\} \Mapsto f: \{00,01,10,11\} \to \{10\}, \{11\}, \{00\}, \{01\}$.

D. Linear versus nonlinear Boolean function

Linear and nonlinear Boolean functions differ in their linearity. 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 functions f_1 and f_4 represent linear Boolean functions because both of them satisfy the linearity property: $f(x \oplus y) = f(x) \oplus f(y)$. In contrast, the functions f_2 and f_3 exhibit nonlinear Boolean functions.

E. Balanced Boolean function

A Boolean function *f* (*x*) of *n*-variables becomes balanced if it takes each of the values 0 and 1 exactly 2^{n-1} times. This demonstrates that a balanced Boolean function uniformly distributes its output over F_2. One of the fundamental test criteria is an S-box's balanced output distribution [4], and defining nonlinearity requires a balanced Boolean function [5]. In contrast, an attacker can exploit an unbalanced function because it exhibits statistical bias.

F. Degree of Boolean function

The number of variables in the longest item of the algebraic normal form (ANF) determines the algebraic degree of a Boolean function. Furthermore, the highest degree of the Boolean function determines the degree of an S-box. Additionally, S-boxes that have the highest degree can effectively prevent differential attacks.

G. Affine Boolean function

The affine Boolean function is a Boolean function that has an almost one-degree algebraic expression. When we express any Boolean function f as $l_{a,b}(x) = \langle a, x \rangle \oplus b$, where a $\in F_{2^n}$ and $b \in F_2$, it transforms into an affine function. This affine-function can represent itself as a vector-valued function, i.e., $f_{affine} = (x_n \ldots x_2 . x_1) = a_n x_n + a_{n-1} x_{n-1} + \ldots + a_1 x_1 + a_0$. From a Boolean perspective, this representation establishes a general form of the *n*-variable affine function [6].

H. Algebraic normal form of Boolean function

Some Boolean functions have a unique representation in their ring sum normal form or algebraic normal form (ANF), i.e., $f(x_n \ldots x_2 . x_1) = a_n x_n \oplus a_{n-1} x_{n-1} \oplus \ldots \oplus a_1 x_1 \oplus a_0$. In this representation, all sets {...} are pairwise distinct, and all subsets are nonempty [7].

I. Nonlinearity of Boolean function

The strength of a function refers to its maximum nonlinearity. Minimum nonlinearity of a Boolean function (N_f) of *n*-variables refers to the Hamming distance between the nonlinear Boolean function or Boolean function and the set of all affine functions. Conversely, we can compute the highest nonlinearity of a Boolean function using the Walsh spectrum [8]. The following are the mathematical representations of minimum and maximum nonlinearity:

Minimum nonlinearity: $\left(N_{f_i}\right) = \min d(f_i, A_{f_i})$;

Maximum nonlinearity: $N_{f_i} = 2^{n-1} - \frac{1}{2} \max_{W \in \mathbb{Z}_{2^n}} |S_{f_i}(W)|$.

This publication is licensed under Creative Commons Attribution CC BY.
https://dx.doi.org/10.29322/IJSRP.14.01.2024.p14539

J. Vectorial Boolean function

In cryptography, an S-box can utilize any mathematical function. But this research will use the vectorial Boolean function that is frequently employed in block ciphers [9]. It serves as a fundamental component of a block cipher. To construct a vectorial Boolean function (𝔽), we combine 2^{n-1} Boolean functions *(f)* using Boolean logic, whereas n denotes the n-dimensional vector space [10]. A vectorial Boolean function (𝔽) consists of Boolean functions, so we can express it mathematically as a vector-valued function as follows:

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

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

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

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

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

K. Vectorial Boolean space

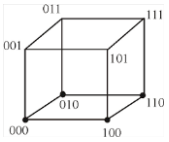
Boolean Space (B^n): $n = 0,1,2 \dots\dots\dots\dots\dots\dots\dots\dots n-1$

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

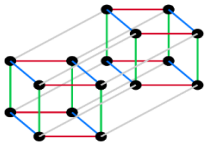
One-dimensional Boolean space (B^1): $2^1 = 2$

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 act as a substitution box (S-box).

L. Application of Boolean function

The Boolean function has various applications in modern cryptography. The Boolean function performs logical calculations on Boolean inputs to generate a Boolean output. Such kinds of Boolean functions play an important 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 ciphers (s-boxes) or symmetric key algorithms [11].

This research holds immense importance in the cryptographic security context as new technologies continue to emerge rapidly. Quantum technologies, in particular, pose a serious threat to the security of our digital communication system. Therefore, we need to construct a quantum-safe cipher in order to survive in the quantum world. Considering these concepts, I focused on Boolean functions, especially vectorial Boolean functions, to create nonlinear S-boxes.

The article outlines the subsequent roadmap: The second section reviews the literature, the third section presents a mechanism for constructing S-boxes, the fourth section illustrates the research outcomes, the fifth section explains the s-box's output measurement procedure, the sixth section provides conclusions followed by recommendations and the author's request to readers, and the final section includes references and evidence of research practice.

This publication is licensed under Creative Commons Attribution CC BY.
https://dx.doi.org/10.29322/IJSRP.14.01.2024.p14539

II. LITERATURE REVIEW

Since, this research focused on nonlinear S-box construction, we must construct an *n*-variable affine function to build an S-box. We must have a clear understanding of an n-variable affine function since it is used in the construction process of a vectorial Boolean function. 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. An affine function maps a function *f(x)* from the input domain to the output range if there exists $\mathbb{Z} \epsilon \mathbb{R}^m$. A linear transformation from real number to real number in matrix form is defined by $\mathbb{R} \xrightarrow{Linear\ transformation} \mathbb{R}^m$. For instance, an affine function *(f)* acts on $(\alpha x + \beta y)$ by transforming it into $\alpha f(x) + \beta f(y) + Z$, i.e., $f(\alpha x + \beta y) = \alpha f(x) + \beta f(y) + Z$. Similarly, from the Boolean perspective, we can consider that function *(f)* as operating on (x ⊕ y) by turning it into $f(x) \oplus f(y) \oplus Z$, i.e., $f\ (x \oplus y) = f\ (x) \oplus f(y) \oplus Z$, whereas α, β, and Z are all equal to 1.

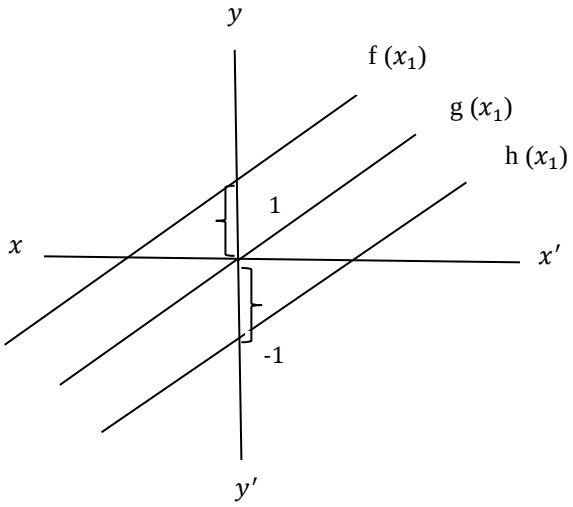


Figure 1. Affine Function

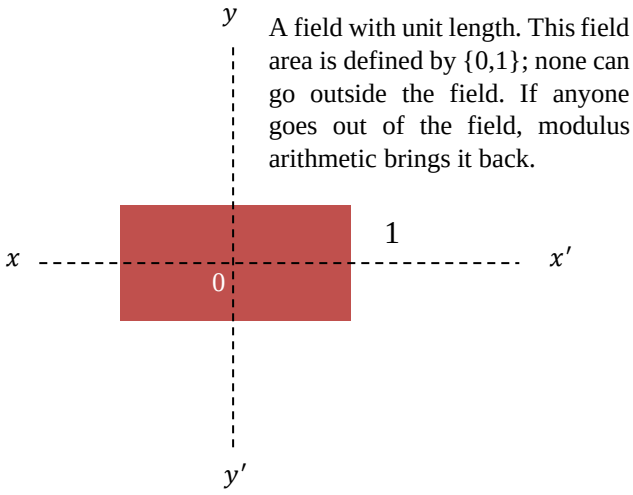


Figure 2. Affine Boolean function

When we transform the linear function $g(x_1)$ passing through the origin by adding Z equal to $+1$ and Z equal to -1, it becomes two affine functions: $f(x_1)$ and $h(x_1)$. In addition, the function $g(x_1)$ may intercept zero and be an affine function. Accordingly, all linear functions are affine functions, but not all affine functions are linear functions. If a linear function intercepts a point, it indicates that the function has been transformed into an affine function [12]. We usually use these concepts to build S-boxes. To build S-Boxes, we need to achieve a Boolean function transformation technique, i.e., $\{0,1\}^m \rightarrow \{0,1\}^n$. In some cases, a Boolean function transformation is bound to $\{0,1\}^m \rightarrow \{0,1\}^n$. A Boolean function has 2^n possible combinations of the given inputs. Such kinds of functions provide a single binary output, either 0 or 1. Boolean functions play a crucial role in cryptography and are considered an essential key to the digital security system.

In the late 1940s, Claude Shannon first introduced the concepts of confusion and diffusion techniques and published these ideas in a seminal paper [13]. He also introduced the concept of the substitution box in 1949 [14]. In general, the S-box is invertible and a one-to-one (bijective) function [15]. An affine equivalent bijective S-box defines S as a mapping from $GF(2^m)$ to $GF(2^n)$, i.e., S: $GF(2^m) \rightarrow GF(2^n)$ [16]. A nonlinear S-box comprises a collection of n-variable nonlinear Boolean functions using Boolean logic.

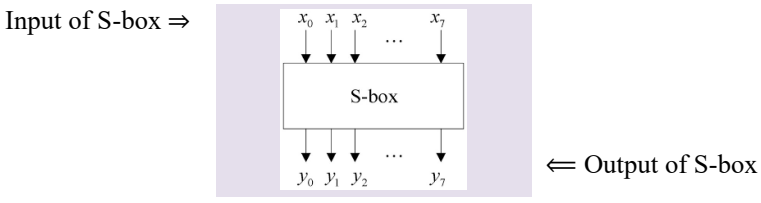


Figure 3. Substitution Box

One study demonstrated how to implement a bijective S-box using quasi-cyclic codes, whereas the cyclic codes are determined by the cyclic shift. The quasi-cyclic codes pose NP-hard problems [17]. Several cryptographic criteria guarantee the correctness of an S-box,

This publication is licensed under Creative Commons Attribution CC BY.
https://dx.doi.org/10.29322/IJSRP.14.01.2024.p14539

including APN, SAC, balancedness, nonlinearity, algebraic immunity, differential uniformity, and high-order algebraic degree. The SAC measures the maximum confusion ability of a specific Boolean function. The bit independence criterion checks dependency bits between plaintext and ciphertext in a block cipher. Nonlinearity resists differential power attack (DPA). DPA is an effective method for disclosing private information. However, the nonlinear operation of the S-box provides resistance against first-order differential power analysis (DPA).

Building an S-box that is secure against algebraic, differential, and linear cryptanalysis is a very challenging task. The S-box is an essential and important component of block ciphers. Creating an action of S-box aims to protect block ciphers from known and potential cryptanalytic attacks [18]. Therefore, S-boxes must possess various cryptographic properties to ensure a high level of protection against such attacks. The block ciphers rely on the S-boxes as one of their most essential components to prevent potential cryptanalytic threats. The strength of S-box depends on high-order algebraic degree, balanced Boolean function, strict avalanche criterion (SAC), differential uniformity, algebraic degree, nonlinearity, almost perfect nonlinearity (APN), bit independence criterion (BIC), and linear and differential cryptanalysis [19].

One research unit explained an S-box construction based on Boolean functions and permutations [20]. The importance of the Boolean function from a cryptographic perspective is immense. The use of the Boolean function appears in numerous scientific fields, including cryptography, combinatorics, complexity theory, coding theory, graph theory, etc. Designing a new S-box in cryptography requires knowledge of the Boolean function and the construction of nonlinear Boolean functions [21]. Some well-known block ciphers, such as AES, DES, and CAST, incorporate a nonlinearly transformed S-box to provide confusion [22]. The nonlinearity ensures the strengthening of the S-box and increases its confusion capacity [23]. However, a dynamic S-box produces more confusion compared to a static S-box. Restricted devices and lightweight cryptography might benefit from this S-Box [24]. The insecure DES S-box is no longer secure, leading encryption algorithms to disallow its use [25]. The DES algorithm utilizes a compressible and expandable S-box [26], while the modern cipher AES employs a 8×8 straight S-box [27]. IDEA and AES S-box have been widely used in secure communication systems.

A chaos-based S-box is useful for image encryption. One study showed that the logistic chaotic transformation technique can assist in designing a high-quality S-box, especially for image encryption algorithms. One can use chaotic Boolean functions to construct an effective nonlinear substitution component that is valuable for image encryption [28]. Additionally, another study found that utilizing both the tent and logistic chaotic maps, one can construct a group of Boolean functions known as an S-box. Moreover, the chaotic Bent function, generated by a chaotic function, is beneficial for the S-box [29]. One study showed how one-dimensional chaotic maps can be used to create an S-box that is valuable in AES. The study evaluated the S-box using test criteria, including completeness, balancedness, strict avalanche criteria (SAC), and invertibility [30].

One researcher developed an S-box construction technique based on Feistel and Lai-Massey structures. The construction of this S-box relies on the inversion technique of the Galois field, non-bijective functions, finite field multiplication, and permutations [31]. A research team developed a technique to construct S-boxes by determining the multiplicative inverse of an input using an irreducible polynomial. They then multiplied the multiplicative inverse by a specific matrix and added the multiplication result to a specific vector [32].

A research unit demonstrated the construction of the S-box using linear fractional transformation and permutation functions [33]. An almost perfect nonlinear function (APN) plays an important role in modern block ciphers. If an S-box fulfills the criteria of the APN function, it is deemed to be an effective S-box capable of resisting differential cryptanalysis attacks [34].

Based on literature review and mathematical analysis, my research focuses on constructing a nonlinear S-box by using the concepts of linear function construction, affine function construction, Boolean function construction, nonlinear Boolean function construction, Boolean vector space, vector-valued functions, and equation construction.

A. AIMS AND OBJECTIVES

The overall research aims were to investigate and explore S-box construction, get familiarized with different mathematical functions required for a nonlinear S-box, and build a straight nonlinear S-box. Consequently, the following research questions have been formulated from the research objectives for conducting 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?

This publication is licensed under Creative Commons Attribution CC BY.
https://dx.doi.org/10.29322/IJSRP.14.01.2024.p14539

III. S-BOX CONSTRUCTION MECHANISM

This mechanism constructs a component-based nonlinear S-box. Different types of S-box construction processes exist, depending on the function used. This section demonstrates a five-step procedure for constructing a straight S-box for vectorial Boolean functions.

STEP 1 (Affine function construction): The construction of an n-variable affine function using combinatorics rules is available on the internet. So, we do not need to explain the affine function construction processes. Instead, we require a 4-dimensional vector space $\mathbb{Z}_2^4$ to create a 4-variable S-box. There are $2^4 = 16$ possible binary input string combinations for 4-variable unit vectors. Thus, a 4-variable affine function can be expressed as a linear combination of those bit strings: $f(x) = a_{1,2,3,4}x_1x_2x_3x_4 \oplus a_{2,3,4}x_2x_3x_4 \oplus a_{1,3,4}x_1x_3x_4 \oplus a_{1,2,4}x_1x_2x_4 \oplus a_{1,2,3}x_1x_2x_3 \oplus a_{3,4}x_3x_4 \oplus a_{2,4}x_2x_4 \oplus a_{2,3}x_2x_3 \oplus a_{1,4}x_1x_4 \oplus a_{1,3}x_1x_3 \oplus a_{1,2}x_1x_2 \oplus a_4x_4 \oplus a_3x_3 \oplus a_2x_2 \oplus a_1x_1 \oplus a_0$

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

Table I: The 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 permutation (random arrangement) of inputs.

STEP 3 (Equation construction): The process of constructing an equation involves using an n-variable affine function and a linear component function, i.e., $a_{1,2,3,4}x_1x_2x_3x_4 \oplus a_{2,3,4}x_2x_3x_4 \oplus a_{1,3,4}x_1x_3x_4 \oplus a_{1,2,4}x_1x_2x_4 \oplus a_{1,2,3}x_1x_2x_3 \oplus a_{3,4}x_3x_4 \oplus a_{2,4}x_2x_4 \oplus a_{2,3}x_2x_3 \oplus a_{1,4}x_1x_4 \oplus a_{1,3}x_1x_3 \oplus a_{1,2}x_1x_2 \oplus a_4x_4 \oplus a_3x_3 \oplus a_2x_2 \oplus a_1x_1 \oplus a_0 = f_i$, whereas $i = 1 \ldots .15$

STEP 4 (Nonlinear Boolean function construction): We can construct the nonlinear Boolean function using the aforementioned equation. The input of the above equation is the 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. Now, let's explore how to construct those nonlinear Boolean functions.

This publication is licensed under Creative Commons Attribution CC BY.
https://dx.doi.org/10.29322/IJSRP.14.01.2024.p14539

The nonlinear Boolean function construction technique (Nf_1):

$a_{1,2,3,4}x_1x_2x_3x_4 \oplus a_{2,3,4}x_2x_3x_4 \oplus a_{1,3,4}x_1x_3x_4 \oplus a_{1,2,4}x_1x_2x_4 \oplus a_{1,2,3}x_1x_2x_3 \oplus a_{3,4}x_3x_4 \oplus a_{2,4}x_2x_4 \oplus a_{2,3}x_2x_3 \oplus a_{1,4}x_1x_4 \oplus a_{1,3}x_1x_3 \oplus a_{1,2}x_1x_2 \oplus a_4x_4 \oplus a_3x_3 \oplus a_2x_2 \oplus a_1x_1 \oplus a_0 = f_1$ .....equation no. (1)

Table II: Inputs of the equation number (1)

a_i	Affine coordinate vectors				Component	L_i
	X_4	X_3	X_2	X_1	f_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	
	1	0	0	0	0	
	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 determine the value of the coefficients for the equation (1), let's successively substitute each affine coordinate vector combination on the left side of the equation and their corresponding component vector on the right side. This helps us systematically derive the necessary 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 $x_1 = x_2 = x_3 = 0$, $a_4x_4 = 0 \oplus a_0 \mapsto a_4.1 = 0 \oplus 0 \mapsto a_4 = 0$
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 $x_2 = x_4 = 0$, $a_{1,3}x_1x_3 = 1 \oplus 0 \oplus 1 \oplus 1 \mapsto a_{1,3}.1.1 = 1 \mapsto a_{1,3} = 1$
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:
$0.(x_1x_2x_3x_4) \oplus 1.(x_2x_3x_4) \oplus 0.(x_1x_3x_4) \oplus 1.(x_1x_2x_4) \oplus 1.(x_1x_2x_3) \oplus 1.(x_3x_4) \oplus 0.(x_2x_4) \oplus 0\,(x_2x_3) \oplus 0.(x_1x_4) \oplus 1.(x_1x_3) \oplus 0.(x_1x_2) \oplus 0.x_4 \oplus 1.x_3 \oplus 1.x_2 \oplus 1.x_1 \oplus 0 = f_1(x_4x_3x_2x_1) = x_2x_3x_4 \oplus x_1x_2x_4 \oplus x_1x_2x_3 \oplus x_3x_4 \oplus x_1x_3 \oplus x_3 \oplus x_2 \oplus x_1$

This publication is licensed under Creative Commons Attribution CC BY.
https://dx.doi.org/10.29322/IJSRP.14.01.2024.p14539

The nonlinear Boolean function construction technique (Nf_2):

$a_{1,2,3,4}x_1x_2x_3x_4 \oplus a_{2,3,4}x_2x_3x_4 \oplus a_{1,3,4}x_1x_3x_4 \oplus a_{1,2,4}x_1x_2x_4 \oplus a_{1,2,3}x_1x_2x_3 \oplus a_{3,4}x_3x_4 \oplus a_{2,4}x_2x_4 \oplus a_{2,3}x_2x_3 \oplus a_{1,4}x_1x_4 \oplus a_{1,3}x_1x_3 \oplus a_{1,2}x_1x_2 \oplus a_4x_4 \oplus a_3x_3 \oplus a_2x_2 \oplus a_1x_1 \oplus a_0 = f_2$ .....equation no. (2)

Table III: Inputs of the equation number (2)

	Affine coordinate vectors				Component	
	X_4	X_3	X_2	X_1	f_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 determine the value of the coefficients for the equation (2), let's successively substitute each affine coordinate vector combination on the left side of the equation and their corresponding component vector on the right side. This helps us systematically derive the necessary 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 ⟨0000⟩ and its corresponding component vector ⟨1⟩. 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 $x_1 = 0$, $a_{2,3,4}x_2x_3x_4 = 0 \oplus a_0 \oplus a_2 \oplus a_3 \oplus a_4 \oplus a_{2,3} \oplus a_{2,4} \oplus a_{3,4} \mapsto a_{2,3,4}1.1.1 = 0 \oplus 1 \oplus 0 \oplus 1 \oplus 0 \oplus 0 \oplus 0 \oplus 1 \oplus 1 \mapsto a_{2,3,4} = 0$
When $x_1 = x_2 = x_3 = x_4 = 1$, $a_{1,2,3,4}x_1x_2x_3x_4 = 0 \oplus a_0 \oplus a_2 \oplus a_3 \oplus a_4 \oplus a_{1,2} \oplus a_{1,3} \oplus a_{1,4} \oplus a_{2,3} \oplus a_{2,4} \oplus a_{3,4} \oplus a_{1,2,3} \oplus a_{1,2,4} \oplus a_{1,3,4} \oplus a_{2,3,4} \mapsto a_{1,2,3,4}1.1.1.1 = 0 \oplus 1 \oplus 1 \oplus 0 \oplus 1 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 1 \oplus 1 \oplus 0 \oplus 0 \oplus 1 \oplus 0 \mapsto a_{1,2,3,4} = 0$

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

This publication is licensed under Creative Commons Attribution CC BY.
https://dx.doi.org/10.29322/IJSRP.14.01.2024.p14539

The nonlinear Boolean function construction technique (Nf_3):

$a_{1,2,3,4}x_1x_2x_3x_4 \oplus a_{2,3,4}x_2x_3x_4 \oplus a_{1,3,4}x_1x_3x_4 \oplus a_{1,2,4}x_1x_2x_4 \oplus a_{1,2,3}x_1x_2x_3 \oplus a_{3,4}x_3x_4 \oplus a_{2,4}x_2x_4 \oplus a_{2,3}x_2x_3 \oplus a_{1,4}x_1x_4 \oplus a_{1,3}x_1x_3 \oplus a_{1,2}x_1x_2 \oplus a_4x_4 \oplus a_3x_3 \oplus a_2x_2 \oplus a_1x_1 \oplus a_0 = f_3$ .....equation no. (3)

Table IV: Inputs of the equation number (3)

a_i	Affine coordinate vectors				Component	L_i
	X_4	X_3	X_2	X_1	f_3	
	0	0	0	0	0	
	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 determine the value of the coefficients for the equation (3), let's successively substitute each affine coordinate vector combination on the left side of the equation and their corresponding component vector on the right side. This helps us systematically derive the necessary 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:
$0.(x_1x_2x_3x_4) \oplus 1.(x_2x_3x_4) \oplus 0.(x_1x_3x_4) \oplus 1.(x_1x_2x_4) \oplus 0.(x_1x_2x_3) \oplus 1.(x_3x_4) \oplus 1.(x_2x_4) \oplus 0.(x_2x_3) \oplus 0.(x_1x_4) \oplus 1.(x_1x_3) \oplus 0.(x_1x_2) \oplus 0.x_4 \oplus 0.x_3 \oplus 1.x_2 \oplus 1.x_1 \oplus 0 = f_3(x_4x_3x_2x_1) = x_2x_3x_4 \oplus x_1x_2x_4 \oplus x_3x_4 \oplus x_2x_4 \oplus x_1x_3 \oplus x_2 \oplus x_1$

This publication is licensed under Creative Commons Attribution CC BY.
https://dx.doi.org/10.29322/IJSRP.14.01.2024.p14539

The nonlinear Boolean function construction technique (Nf_4):

$a_{1,2,3,4}x_1x_2x_3x_4 \oplus a_{2,3,4}x_2x_3x_4 \oplus a_{1,3,4}x_1x_3x_4 \oplus a_{1,2,4}x_1x_2x_4 \oplus a_{1,2,3}x_1x_2x_3 \oplus a_{3,4}x_3x_4 \oplus a_{2,4}x_2x_4 \oplus a_{2,3}x_2x_3 \oplus a_{1,4}x_1x_4 \oplus a_{1,3}x_1x_3 \oplus a_{1,2}x_1x_2 \oplus a_4x_4 \oplus a_3x_3 \oplus a_2x_2 \oplus a_1x_1 \oplus a_0 = f_4$ .....equation no. (4)

Table V: Inputs of the equation number (4)

	Affine coordinate vectors				Component	
	X_4	X_3	X_2	X_1	f_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 determine the value of the coefficients for the equation (4), let's successively substitute each affine coordinate vector combination on the left side of the equation and their corresponding component vector on the right side. This helps us systematically derive the necessary 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 ⟨0000⟩ and its corresponding component vector ⟨0⟩. 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:
$0.(x_1x_2x_3x_4) \oplus 1.(x_2x_3x_4) \oplus 1.(x_1x_3x_4) \oplus 1.(x_1x_2x_4) \oplus 1.(x_1x_2x_3) \oplus 0.(x_3x_4) \oplus 1.(x_2x_4) \oplus 0.(x_2x_3) \oplus 0.(x_1x_4) \oplus 0.(x_1x_3) \oplus 1.(x_1x_2) \oplus 1.x_4 \oplus 1.x_3 \oplus 0.x_2 \oplus 0.x_1 \oplus 0 = f_4(x_4x_3x_2x_1) = x_2x_3x_4 \oplus x_1x_3x_4 \oplus x_1x_2x_4 \oplus x_1x_2x_3 \oplus x_2x_4 \oplus x_1x_2 \oplus x_4 \oplus x_3$

This publication is licensed under Creative Commons Attribution CC BY.
https://dx.doi.org/10.29322/IJSRP.14.01.2024.p14539

The nonlinear Boolean function construction technique (Nf_5):

$a_{1,2,3,4}x_1x_2x_3x_4 \oplus a_{2,3,4}x_2x_3x_4 \oplus a_{1,3,4}x_1x_3x_4 \oplus a_{1,2,4}x_1x_2x_4 \oplus a_{1,2,3}x_1x_2x_3 \oplus a_{3,4}x_3x_4 \oplus a_{2,4}x_2x_4 \oplus a_{2,3}x_2x_3 \oplus a_{1,4}x_1x_4 \oplus a_{1,3}x_1x_3 \oplus a_{1,2}x_1x_2 \oplus a_4x_4 \oplus a_3x_3 \oplus a_2x_2 \oplus a_1x_1 \oplus a_0 = f_5$ .....equation no. (5)

Table VI: Inputs of the equation number (5)

a_i	Affine coordinate vectors				Component	L_i
	X_4	X_3	X_2	X_1	f_5	
	0	0	0	0	1	
	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 determine the value of the coefficients for the equation (5), let's successively substitute each affine coordinate vector combination on the left side of the equation and their corresponding component vector on the right side. This helps us systematically derive the necessary 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 ⟨0000⟩ and its corresponding component vector ⟨1⟩. 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 $x_3 = 0$, $a_{1,2,4}x_1x_2x_4 = 0 \oplus a_0 \oplus a_1 \oplus a_2 \oplus a_4 \oplus a_{1,2} \oplus a_{1,4} \oplus a_{2,4} \mapsto a_{1,2,4}1.1.1 = 0 \oplus 1 \oplus 0 \oplus 1 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 1 \mapsto a_{1,2,4} = 1$
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 $x_1 = x_2 = x_3 = x_4 = 1$, $a_{1,2,3,4}x_1x_2x_3x_4 = 0 \oplus a_0 \oplus a_2 \oplus a_3 \oplus a_4 \oplus a_{1,2} \oplus a_{1,3} \oplus a_{1,4} \oplus a_{2,3} \oplus a_{2,4} \oplus a_{3,4} \oplus a_{1,2,3} \oplus a_{1,2,4} \oplus a_{1,3,4} \oplus a_{2,3,4} \mapsto a_{1,2,3,4}1.1.1.1 = 0 \oplus 1 \oplus 0 \oplus 1 \oplus 0 \oplus 0 \oplus 0 \oplus 1 \oplus 0 \oplus 0 \oplus 1 \oplus 0 \oplus 1 \oplus 1 \oplus 1 \mapsto a_{1,2,3,4} = 0$

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

This publication is licensed under Creative Commons Attribution CC BY.
https://dx.doi.org/10.29322/IJSRP.14.01.2024.p14539

The nonlinear Boolean function construction technique (Nf_6):

$a_{1,2,3,4}x_1x_2x_3x_4 \oplus a_{2,3,4}x_2x_3x_4 \oplus a_{1,3,4}x_1x_3x_4 \oplus a_{1,2,4}x_1x_2x_4 \oplus a_{1,2,3}x_1x_2x_3 \oplus a_{3,4}x_3x_4 \oplus a_{2,4}x_2x_4 \oplus a_{2,3}x_2x_3 \oplus a_{1,4}x_1x_4 \oplus a_{1,3}x_1x_3 \oplus a_{1,2}x_1x_2 \oplus a_4x_4 \oplus a_3x_3 \oplus a_2x_2 \oplus a_1x_1 \oplus a_0 = f_6$ .....equation no. (6)

Table VII: Inputs of the equation number (6)

	Affine coordinate vectors				Component	
	X_4	X_3	X_2	X_1	f_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 determine the value of the coefficients for the equation (6), let's successively substitute each affine coordinate vector combination on the left side of the equation and their corresponding component vector on the right side. This helps us systematically derive the necessary 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 ⟨0000⟩ and its corresponding component vector ⟨0⟩. 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 $x_3 = 0$, $a_{1,2,4}x_1x_2x_4 = 1 \oplus a_0 \oplus a_1 \oplus a_2 \oplus a_4 \oplus a_{1,2} \oplus a_{1,4} \oplus a_{2,4} \mapsto a_{1,2,4}1.1.1 = 1 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 1 \mapsto a_{1,2,4} = 0$
When $x_1 = x_3 = x_4 = 1$ and $x_2 = 0$, $a_{1,3,4}x_1x_3x_4 = 1 \oplus a_0 \oplus a_1 \oplus a_3 \oplus a_4 \oplus a_{1,3} \oplus a_{1,4} \oplus a_{3,4} \mapsto a_{1,3,4}1.1.1 = 1 \oplus 0 \oplus 0 \oplus 1 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \mapsto a_{1,3,4} = 0$
When $x_2 = x_3 = x_4 = 1$ and $x_1 = 0$, $a_{2,3,4}x_2x_3x_4 = 0 \oplus a_0 \oplus a_2 \oplus a_3 \oplus a_4 \oplus a_{2,3} \oplus a_{2,4} \oplus a_{3,4} \mapsto a_{2,3,4}1.1.1 = 0 \oplus 0 \oplus 0 \oplus 1 \oplus 0 \oplus 0 \oplus 0 \oplus 1 \oplus 0 \mapsto a_{2,3,4} = 0$
When $x_1 = x_2 = x_3 = x_4 = 1$, $a_{1,2,3,4}x_1x_2x_3x_4 = 1 \oplus a_0 \oplus a_2 \oplus a_3 \oplus a_4 \oplus a_{1,2} \oplus a_{1,3} \oplus a_{1,4} \oplus a_{2,3} \oplus a_{2,4} \oplus a_{3,4} \oplus a_{1,2,3} \oplus a_{1,2,4} \oplus a_{1,3,4} \oplus a_{2,3,4} \mapsto a_{1,2,3,4}1.1.1.1 = 1 \oplus 0 \oplus 0 \oplus 0 \oplus 1 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 1 \oplus 0 \oplus 0 \oplus 1 \oplus 0 \oplus 0 \oplus 0 \mapsto a_{1,2,3,4} = 0$

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

This publication is licensed under Creative Commons Attribution CC BY.
https://dx.doi.org/10.29322/IJSRP.14.01.2024.p14539

The nonlinear Boolean function construction technique (Nf_7):

$a_{1,2,3,4}x_1x_2x_3x_4 \oplus a_{2,3,4}x_2x_3x_4 \oplus a_{1,3,4}x_1x_3x_4 \oplus a_{1,2,4}x_1x_2x_4 \oplus a_{1,2,3}x_1x_2x_3 \oplus a_{3,4}x_3x_4 \oplus a_{2,4}x_2x_4 \oplus a_{2,3}x_2x_3 \oplus a_{1,4}x_1x_4 \oplus a_{1,3}x_1x_3 \oplus a_{1,2}x_1x_2 \oplus a_4x_4 \oplus a_3x_3 \oplus a_2x_2 \oplus a_1x_1 \oplus a_0 = f_7$ .....equation no. (7)

Table VIII: Inputs of the equation number (7)

	Affine coordinate vectors				Component	
	X_4	X_3	X_2	X_1	f_7	
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	0	
	0	1	0	1	0	
	0	1	1	0	1	
	0	1	1	1	0	
	1	0	0	0	1	
	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 determine the value of the coefficients for the equation (7), let's successively substitute each affine coordinate vector combination on the left side of the equation and their corresponding component vector on the right side. This helps us systematically derive the necessary 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 ⟨0000⟩ and its corresponding component vector ⟨0⟩. 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 $x_1 = 0$, $a_{2,3,4}x_2x_3x_4 = 0 \oplus a_0 \oplus a_2 \oplus a_3 \oplus a_4 \oplus a_{2,3} \oplus a_{2,4} \oplus a_{3,4} \mapsto a_{2,3,4}1.1.1 = 0 \oplus 0 \oplus 1 \oplus 0 \oplus 1 \oplus 0 \oplus 0 \oplus 1 \oplus 1 \mapsto a_{2,3,4} = 0$
When $x_1 = x_2 = x_3 = x_4 = 1$, $a_{1,2,3,4}x_1x_2x_3x_4 = 0 \oplus a_0 \oplus a_2 \oplus a_3 \oplus a_4 \oplus a_{1,2} \oplus a_{1,3} \oplus a_{1,4} \oplus a_{2,3} \oplus a_{2,4} \oplus a_{3,4} \oplus a_{1,2,3} \oplus a_{1,2,4} \oplus a_{1,3,4} \oplus a_{2,3,4} \mapsto a_{1,2,3,4}1.1.1.1 = 0 \oplus 1 \oplus 0 \oplus 1 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 1 \oplus 0 \oplus 0 \oplus 1 \oplus 0 \oplus 0 \oplus 1 \oplus 1 \oplus 1 \oplus 1 \mapsto a_{1,2,3,4} = 0$

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

This publication is licensed under Creative Commons Attribution CC BY.
https://dx.doi.org/10.29322/IJSRP.14.01.2024.p14539

The nonlinear Boolean function construction technique (Nf_8):

$a_{1,2,3,4}x_1x_2x_3x_4 \oplus a_{2,3,4}x_2x_3x_4 \oplus a_{1,3,4}x_1x_3x_4 \oplus a_{1,2,4}x_1x_2x_4 \oplus a_{1,2,3}x_1x_2x_3 \oplus a_{3,4}x_3x_4 \oplus a_{2,4}x_2x_4 \oplus a_{2,3}x_2x_3 \oplus a_{1,4}x_1x_4 \oplus a_{1,3}x_1x_3 \oplus a_{1,2}x_1x_2 \oplus a_4x_4 \oplus a_3x_3 \oplus a_2x_2 \oplus a_1x_1 \oplus a_0 = f_8$ .....equation no. (8)

Table IX: Inputs of the equation number (8)

	Affine coordinate vectors				Component	
	X_4	X_3	X_2	X_1	f_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 determine the value of the coefficients for the equation (8), let's successively substitute each affine coordinate vector combination on the left side of the equation and their corresponding component vector on the right side. This helps us systematically derive the necessary 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 ⟨0000⟩ and its corresponding component vector ⟨1⟩. 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 $x_1 = x_2 = x_3 = x_4 = 1$, $a_{1,2,3,4}x_1x_2x_3x_4 = 1 \oplus a_0 \oplus a_2 \oplus a_3 \oplus a_4 \oplus a_{1,2} \oplus a_{1,3} \oplus a_{1,4} \oplus a_{2,3} \oplus a_{2,4} \oplus a_{3,4} \oplus a_{1,2,3} \oplus a_{1,2,4} \oplus a_{1,3,4} \oplus a_{2,3,4} \mapsto a_{1,2,3,4}1.1.1.1 = 1 \oplus 1 \oplus 0 \oplus 1 \oplus 1 \oplus 0 \oplus 0 \oplus 1 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 1 \oplus 1 \oplus 1 \mapsto a_{1,2,3,4} = 0$

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

This publication is licensed under Creative Commons Attribution CC BY.
https://dx.doi.org/10.29322/IJSRP.14.01.2024.p14539

The nonlinear Boolean function construction technique (Nf_9):

$a_{1,2,3,4}x_1x_2x_3x_4 \oplus a_{2,3,4}x_2x_3x_4 \oplus a_{1,3,4}x_1x_3x_4 \oplus a_{1,2,4}x_1x_2x_4 \oplus a_{1,2,3}x_1x_2x_3 \oplus a_{3,4}x_3x_4 \oplus a_{2,4}x_2x_4 \oplus a_{2,3}x_2x_3 \oplus a_{1,4}x_1x_4 \oplus a_{1,3}x_1x_3 \oplus a_{1,2}x_1x_2 \oplus a_4x_4 \oplus a_3x_3 \oplus a_2x_2 \oplus a_1x_1 \oplus a_0 = f_9$ .....equation no. (9)

Table X: Inputs of the equation number (9)

	Affine coordinate vectors				Component	
	X_4	X_3	X_2	X_1	f_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 determine the value of the coefficients for the equation (9), let's successively substitute each affine coordinate vector combination on the left side of the equation and their corresponding component vector on the right side. This helps us systematically derive the necessary 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 ⟨0000⟩ and its corresponding component vector ⟨1⟩. 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 $x_1 = x_2 = x_3 = 0$, $a_4x_4 = 0 \oplus a_0 \mapsto a_4.1 = 0 \oplus 1 \mapsto a_4 = 1$
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 $x_2 = x_4 = 0$, $a_{1,3}x_1x_3 = 0 \oplus 1 \oplus 1 \oplus 0 \mapsto a_{1,3}.1.1 = 0 \mapsto a_{1,3} = 0$
When $x_1 = x_4 = 1$ and $x_2 = x_3 = 0$, $a_{1,4}x_1x_4 = 1 \oplus 1 \oplus 1 \oplus 1 \mapsto a_{1,4}.1.1 = 0 \mapsto a_{1,4} = 0$
When $x_2 = x_3 = 1$ and $x_1 = x_4 = 0$, $a_{2,3}x_2x_3 = 1 \oplus 1 \oplus 0 \oplus 0 \mapsto a_{2,3}.1.1 = 0 \mapsto a_{2,3} = 0$
When $x_2 = x_4 = 1$ and $x_1 = x_3 = 0$, $a_{2,4}x_2x_4 = 0 \oplus 1 \oplus 0 \oplus 1 \mapsto a_{2,4}.1.1 = 0 \mapsto a_{2,4} = 0$
When $x_3 = x_4 = 1$ and $x_1 = x_2 = 0$, $a_{3,4}x_3x_4 = 1 \oplus 1 \oplus 0 \oplus 1 \mapsto a_{3,4}.1.1 = 1 \mapsto a_{3,4} = 1$
When $x_1 = x_2 = x_3 = 1$ and $x_4 = 0$, $a_{1,2,3}x_1x_2x_3 = 0 \oplus a_0 \oplus a_1 \oplus a_2 \oplus a_3 \oplus a_{1,2} \oplus a_{1,3} \oplus a_{2,3} \mapsto a_{1,2,3}1.1.1 = 0 \oplus 1 \oplus 1 \oplus 0 \oplus 0 \oplus 1 \oplus 0 \oplus 0 \mapsto a_{1,2,3} = 1$
When $x_1 = x_2 = x_4 = 1$ and $x_3 = 0$, $a_{1,2,4}x_1x_2x_4 = 1 \oplus a_0 \oplus a_1 \oplus a_2 \oplus a_4 \oplus a_{1,2} \oplus a_{1,4} \oplus a_{2,4} \mapsto a_{1,2,4}1.1.1 = 1 \oplus 1 \oplus 1 \oplus 0 \oplus 1 \oplus 1 \oplus 0 \oplus 0 \mapsto a_{1,2,4} = 1$
When $x_1 = x_3 = x_4 = 1$ and $x_2 = 0$, $a_{1,3,4}x_1x_3x_4 = 0 \oplus a_0 \oplus a_1 \oplus a_3 \oplus a_4 \oplus a_{1,3} \oplus a_{1,4} \oplus a_{3,4} \mapsto a_{1,3,4}1.1.1 = 0 \oplus 1 \oplus 1 \oplus 0 \oplus 1 \oplus 0 \oplus 0 \oplus 1 \mapsto a_{1,3,4} = 0$
When $x_2 = x_3 = x_4 = 1$ and $x_1 = 0$, $a_{2,3,4}x_2x_3x_4 = 0 \oplus a_0 \oplus a_2 \oplus a_3 \oplus a_4 \oplus a_{2,3} \oplus a_{2,4} \oplus a_{3,4} \mapsto a_{2,3,4}1.1.1 = 0 \oplus 1 \oplus 0 \oplus 0 \oplus 1 \oplus 0 \oplus 0 \oplus 1 \mapsto a_{2,3,4} = 1$
When $x_1 = x_2 = x_3 = x_4 = 1$, $a_{1,2,3,4}x_1x_2x_3x_4 = 0 \oplus a_0 \oplus a_2 \oplus a_3 \oplus a_4 \oplus a_{1,2} \oplus a_{1,3} \oplus a_{1,4} \oplus a_{2,3} \oplus a_{2,4} \oplus a_{3,4} \oplus a_{1,2,3} \oplus a_{1,2,4} \oplus a_{1,3,4} \oplus a_{2,3,4} \mapsto a_{1,2,3,4}1.1.1.1 = 0 \oplus 1 \oplus 1 \oplus 0 \oplus 0 \oplus 1 \oplus 1 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 1 \oplus 1 \oplus 1 \oplus 0 \oplus 1 \mapsto a_{1,2,3,4} = 0$

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

This publication is licensed under Creative Commons Attribution CC BY.
https://dx.doi.org/10.29322/IJSRP.14.01.2024.p14539

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

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

Table XI: Inputs of the equation number (10)

	Affine coordinate vectors				Component	
	X_4	X_3	X_2	X_1	f_{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 determine the value of the coefficients for the equation (10), let's successively substitute each affine coordinate vector combination on the left side of the equation and their corresponding component vector on the right side. This helps us systematically derive the necessary 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 ⟨0000⟩ and its corresponding component vector ⟨0⟩. 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 $x_1 = x_2 = x_3 = x_4 = 1$, $a_{1,2,3,4}x_1x_2x_3x_4 = 1 \oplus a_0 \oplus a_2 \oplus a_3 \oplus a_4 \oplus a_{1,2} \oplus a_{1,3} \oplus a_{1,4} \oplus a_{2,3} \oplus a_{2,4} \oplus a_{3,4} \oplus a_{1,2,3} \oplus a_{1,2,4} \oplus a_{1,3,4} \oplus a_{2,3,4} \mapsto a_{1,2,3,4}1.1.1.1 = 1 \oplus 0 \oplus 1 \oplus 1 \oplus 1 \oplus 1 \oplus 1 \oplus 0 \oplus 0 \oplus 0 \oplus 1 \oplus 1 \oplus 0 \oplus 1 \oplus 0 \mapsto a_{1,2,3,4} = 0$

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

This publication is licensed under Creative Commons Attribution CC BY.
https://dx.doi.org/10.29322/IJSRP.14.01.2024.p14539

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

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

Table XII: Inputs of the equation number (11)

	Affine coordinate vectors				Component	
	X_4	X_3	X_2	X_1	f_{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 determine the value of the coefficients for the equation (11), let's successively substitute each affine coordinate vector combination on the left side of the equation and their corresponding component vector on the right side. This helps us systematically derive the necessary 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 ⟨0000⟩ and its corresponding component vector ⟨1⟩. 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 $x_1 = x_2 = x_3 = x_4 = 1$, $a_{1,2,3,4}x_1x_2x_3x_4 = 1 \oplus a_0 \oplus a_2 \oplus a_3 \oplus a_4 \oplus a_{1,2} \oplus a_{1,3} \oplus a_{1,4} \oplus a_{2,3} \oplus a_{2,4} \oplus a_{3,4} \oplus a_{1,2,3} a_{1,2,4} \oplus a_{1,3,4} \oplus a_{2,3,4} \mapsto a_{1,2,3,4}1.1.1.1 = 1 \oplus 1 \oplus 1 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 1 \oplus 1 \oplus 0 \oplus 1 \oplus 0 \mapsto a_{1,2,3,4} = 0$

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

This publication is licensed under Creative Commons Attribution CC BY.
https://dx.doi.org/10.29322/IJSRP.14.01.2024.p14539

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

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

Table XIII: Inputs of the equation number (12)

	Affine coordinate vectors				Component	
	X_4	X_3	X_2	X_1	f_{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 determine the value of the coefficients for the equation (12), let's successively substitute each affine coordinate vector combination on the left side of the equation and their corresponding component vector on the right side. This helps us systematically derive the necessary 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 ⟨0000⟩ and its corresponding component vector ⟨1⟩. 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 $x_1 = x_2 = x_3 = x_4 = 1$, $a_{1,2,3,4}x_1x_2x_3x_4 = 0 \oplus a_0 \oplus a_2 \oplus a_3 \oplus a_4 \oplus a_{1,2} \oplus a_{1,3} \oplus a_{1,4} \oplus a_{2,3} \oplus a_{2,4} \oplus a_{3,4} \oplus a_{1,2,3} \oplus a_{1,2,4} \oplus a_{1,3,4} \oplus a_{2,3,4} \mapsto a_{1,2,3,4}1.1.1.1 = 0 \oplus 1 \oplus 0 \oplus 1 \oplus 1 \oplus 1 \oplus 1 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \mapsto a_{1,2,3,4} = 0$

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

This publication is licensed under Creative Commons Attribution CC BY.
https://dx.doi.org/10.29322/IJSRP.14.01.2024.p14539

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

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

Table XIV: Inputs of the equation number (13)

	Affine coordinate vectors				Component	
	X_4	X_3	X_2	X_1	f_{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 determine the value of the coefficients for the equation (13), let's successively substitute each affine coordinate vector combination on the left side of the equation and their corresponding component vector on the right side. This helps us systematically derive the necessary 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 ⟨0000⟩ and its corresponding component vector ⟨0⟩. 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 $x_1 = x_2 = x_3 = x_4 = 1$, $a_{1,2,3,4}x_1x_2x_3x_4 = 1 \oplus a_0 \oplus a_2 \oplus a_3 \oplus a_4 \oplus a_{1,2} \oplus a_{1,3} \oplus a_{1,4} \oplus a_{2,3} \oplus a_{2,4} \oplus a_{3,4} \oplus a_{1,2,3} \oplus a_{1,2,4} \oplus a_{1,3,4} \oplus a_{2,3,4} \mapsto a_{1,2,3,4}1.1.1.1 = 1 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 1 \oplus 1 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 1 \oplus 1 \oplus 1 \mapsto a_{1,2,3,4} = 0$

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

This publication is licensed under Creative Commons Attribution CC BY.
https://dx.doi.org/10.29322/IJSRP.14.01.2024.p14539

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

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

Table XV: Inputs of the equation number (14)

	Affine coordinate vectors				Component	
	X_4	X_3	X_2	X_1	f_{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 determine the value of the coefficients for the equation (14), let's successively substitute each affine coordinate vector combination on the left side of the equation and their corresponding component vector on the right side. This helps us systematically derive the necessary 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:
$0.(x_1x_2x_3x_4) \oplus 0.(x_2x_3x_4) \oplus 0.(x_1x_3x_4) \oplus 0.(x_1x_2x_4) \oplus 1.(x_1x_2x_3) \oplus 0.(x_3x_4) \oplus 1.(x_2x_4) \oplus 0.(x_2x_3) \oplus 0.(x_1x_4) \oplus 1.(x_1x_3) \oplus 1.(x_1x_2) \oplus 1.x_4 \oplus 0.x_3 \oplus 1.x_2 \oplus 0.x_1 \oplus 1 = f_{14}(x_4x_3x_2x_1) = x_1x_2x_3 \oplus x_2x_4 \oplus x_1x_3 \oplus x_1x_2 \oplus x_4 \oplus x_2 \oplus 1$

This publication is licensed under Creative Commons Attribution CC BY.
https://dx.doi.org/10.29322/IJSRP.14.01.2024.p14539

The nonlinear Boolean function construction technique (Nf_{15}):

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

Table XVI: Inputs of the equation number (15)

	Affine coordinate vectors				Component	
	X_4	X_3	X_2	X_1	f_{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 determine the value of the coefficients for the equation (15), let's successively substitute each affine coordinate vector combination on the left side of the equation and their corresponding component vector on the right side. This helps us systematically derive the necessary 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 $x_3 = x_4 = 0$, $a_{1,2}x_1x_2 = 1 \oplus 1 \oplus 0 \mapsto a_{1,2}.1.1 = 1 \mapsto a_{1,2} = 1$
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:
$0.(x_1x_2x_3x_4) \oplus 1.(x_2x_3x_4) \oplus 0.(x_1x_3x_4) \oplus 1.(x_1x_2x_4) \oplus 0.(x_1x_2x_3) \oplus 1.(x_3x_4) \oplus 1.(x_2x_4) \oplus 0.(x_2x_3) \oplus 0.(x_1x_4) \oplus 0.(x_1x_3) \oplus 1.(x_1x_2) \oplus 1.x_4 \oplus 1.x_3 \oplus 0.x_2 \oplus 1.x_1 \oplus 1 = f_{15}(x_4x_3x_2x_1) = x_2x_3x_4 \oplus x_1x_2x_4 \oplus x_3x_4 \oplus x_2x_4 \oplus x_1x_2 \oplus x_4 \oplus x_3 \oplus x_1 \oplus 1$

This publication is licensed under Creative Commons Attribution CC BY.
https://dx.doi.org/10.29322/IJSRP.14.01.2024.p14539

STEP 5 (Creating an action of S-box): A linear combination of $2^n - 1$ numbers of nonlinear Boolean functions make it possible to construct an action of S-box using Boolean logic. Each of these nonlinear Boolean functions contributes to the complexity and nonlinearity of the S-box, which is crucial for creating strong cryptographic algorithms. A nonlinear S-box comprises a carefully selected set of these nonlinear Boolean functions. It is a meticulously crafted structure that consists of a thoughtfully chosen set of these nonlinear Boolean functions. A nonlinear S-box is essentially an intricate assembly of these carefully chosen nonlinear Boolean functions. Therefore, this nonlinear S-box consists 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. RESEARCH OUTCOMES

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

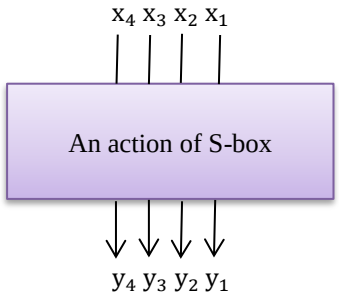


Figure 4: Action of S-box

This publication is licensed under Creative Commons Attribution CC BY.
https://dx.doi.org/10.29322/IJSRP.14.01.2024.p14539

V. Output Measurement

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

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

14 13 12 11 10 9 8 7 6 5 4 3 2 1 0 ← $index\ number(in)$

⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ × $= bs \times binary\ base^{in} = 1 \times 2^{13} + 1 \times 2^{10} +$

0 1 0 0 1 0 0 1 1 0 1 1 0 1 1 ← $Bit\ sequence(bs)$

$1 \times 2^7 + 1 \times 2^6 + 1 \times 2^4 + 1 \times 2^3 + 1 \times 2^1 + 1 \times 2^0 = 8192 + 1024 + 128 + 64 + 64 + 16 + 8 + 2 + 1 =$

$9435_{10} = 9435_{10} \bmod 16 = 11$= 0xB =1011 =1 ⊕ 0 ⊕ 1⊕ 1 = 1

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

1 1 1 0 0 0 1 0 1 1 1 0 0 0 1

⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ 14 13 12 11 10 9 8 7 6 5 4 3 2 1 0 ← $index\ number(in)$

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 ← $Bit\ sequence(bs)$

1 0 1 0 1 0 1 1 0 1 0 1 0 1 0

$= bs \times binary\ base^{in} = 1 \times 2^{14} + 1 \times 2^{12} + 1 \times 2^{10} + 1 \times 2^8 + 1 \times 2^7 + 1 \times 2^5 + 1 \times 2^3 + 1 \times 2^1 = 16384 +$

$4096 + 1024 + 256 + 128 + 32 + 8 + 2 = 9435_{10} = 21930_{10} \bmod 16 = 10$ = 0xA = 1010 = 1 ⊕ 0 ⊕ 1 ⊕ 0 = 0

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

1 0 1 0 1 0 1 1 0 1 0 1 0 1 0

⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ 14 13 12 11 10 9 8 7 6 5 4 3 2 1 0 ← $index\ number(in)$

0 1 0 0 1 0 0 1 1 0 1 1 0 1 1 = ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ×

− − − − − − − − − − − − − − − 1 1 1 0 0 0 1 0 1 1 1 0 0 0 1 ← $Bit\ sequence(bs)$

1 1 1 0 0 0 1 0 1 1 1 0 0 0 1

$= bs \times binary\ base^{in} = 1 \times 2^{14} + 1 \times 2^{13} + 1 \times 2^{12} + 1 \times 2^8 + 1 \times 2^6 + 1 \times 2^5 + 1 \times 2^4 + 1 \times 2^0 = 16384 + 8192 +$

$4096 + 256 + 64 + 32 + 16 + 1 = 9435_{10} = 29041_{10} \bmod 16 = 1$ = 0x1 = 0001 = 0 ⊕ 0 ⊕ 0 ⊕ 1 = 1

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

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 = 14 13 12 11 10 9 8 7 6 5 4 3 2 1 0 ← $index\ number(in)$

0 1 0 0 1 0 0 1 1 0 1 1 0 1 1 ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ×

0 0 0 1 0 0 1 0 1 1 0 1 1 1 1 ← $Bit\ sequence(bs)$

$= bs \times binary\ base^{in} = 1 \times 2^{11} + 1 \times 2^8 + 1 \times 2^6 + 1 \times 2^5 + 1 \times 2^3 + 1 \times 2^2 + 1 \times 2^1 + 1 \times 2^0 = 2048 + 256 +$

$64 + 32 + 8 + 4 + 2 + 1 = 2415_{10} = 2415_{10} \bmod 16 = 15$ = 0xF = 1111 = 1 ⊕ 1 ⊕ 1 ⊕ 1 = 0

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

1 1 0 1 0 1 0 1 0 1 0 1 0 0 1

⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ 14 13 12 11 10 9 8 7 6 5 4 3 2 1 0 ← $index\ number(in)$

0 1 0 0 1 0 0 1 1 0 1 1 0 1 1 = ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ×

− − − − − − − − − − − − − − − 1 0 0 1 1 1 0 0 1 1 1 0 0 1 0 ← $Bit\ sequence(bs)$

1 0 0 1 1 1 0 0 1 1 1 0 0 1 0

$= bs \times binary\ base^{in} = 1 \times 2^{14} + 1 \times 2^{11} + 1 \times 2^{10} + 1 \times 2^9 + 1 \times 2^6 + 1 \times 2^5 + 1 \times 2^4 + 1 \times 2^1 = 16384 +$

$2048 + 1024 + 512 + 64 + 32 + 16 + 2 = 9435_{10} = 20082_{10} \bmod 16 = 2$ = 0x2 = 0010 = 0 ⊕ 0 ⊕ 1⊕ 0 = 1

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

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 = 14 13 12 11 10 9 8 7 6 5 4 3 2 1 0 ← $index\ number(in)$

0 1 0 0 1 0 0 1 1 0 1 1 0 1 1 ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ×

1 1 0 1 0 1 0 1 0 1 0 1 0 0 1 ← $Bit\ sequence(bs)$

1 1 0 1 0 1 0 1 0 1 0 1 0 0 1

$= bs \times binary\ base^{in} = 1 \times 2^{14} + 1 \times 2^{13} + 1 \times 2^{11} + 1 \times 2^9 + 1 \times 2^7 + 1 \times 2^5 + 1 \times 2^3 + 1 \times 2^0 = 16384 +$

$8192 + 2048 + 512 + 128 + 32 + 8 + 1 = 27305_{10} = 27305_{10} \bmod 16 = 9$ = 0x9 =1001=1⊕ 0 ⊕ 0 ⊕1 = 0

This publication is licensed under Creative Commons Attribution CC BY.
https://dx.doi.org/10.29322/IJSRP.14.01.2024.p14539

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

This publication is licensed under Creative Commons Attribution CC BY.
https://dx.doi.org/10.29322/IJSRP.14.01.2024.p14539

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

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

$= bs \times binary\ base^{in} = 1 \times 2^{14} + 1 \times 2^{13} + 1 \times 2^9 + 1 \times 2^8 + 1 \times 2^7 + 1 \times 2^6 + 1 \times 2^2 + 1 \times 2^1 = 16384 + 8192 + 512 + 256 + 128 + 64 + 4 + 2 = 25542_{10} = 25542_{10} \bmod 16 = 6 = 0x6 = 0110 = 0 \oplus 1 \oplus 1 \oplus 0 = 0$

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

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

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

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

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

$= bs \times binary\ base^{in} = 1 \times 2^{13} + 1 \times 2^{12} + 1 \times 2^{11} + 1 \times 2^{10} + 1 \times 2^9 + 1 \times 2^8 + 1 \times 2^1 + 1 \times 2^0 = 8192 + 4096 + 2048 + 1024 + 512 + 256 + 2 + 1 = 16131_{10} = 16131_{10} \bmod 16 = 3 = 0x3 = 0011 = 0 \oplus 0 \oplus 1 \oplus 1 = 0$

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

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

$= bs \times binary\ base^{in}$

$= 0$

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

This publication is licensed under Creative Commons Attribution CC BY.
https://dx.doi.org/10.29322/IJSRP.14.01.2024.p14539

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

$$\times \qquad = bs \times binary\ base^{in}$$

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

VI. Conclusions

To conclude the investigation into a nonlinear S-box construction, different S-box construction techniques were analyzed, and their functionalities were examined. And then, the research successfully accomplished its objective by designing a component-based nonlinear S-box. The research on component-based nonlinear S-box construction with various mathematical interpretations came to an end through literature review, problem-solving efforts, analysis, and discussion with researchers. By studying numerous research papers, it was possible to gain a thorough understanding of the construction mechanism of a component-based nonlinear S-box. The purpose of the publication was to disseminate scientific knowledge to scientific readers scattered around the world. One reason for constructing the nonlinear S-box is to meet the needs of scientific students and researchers, allowing them to benefit from reading this article. I believe this article will attract the attention of scientific readers. The article emphasizes presenting complex mathematical concepts in a simple way to help scientific readers, educators, and students understand 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*

Based on the conclusions, I recommend that anyone interested in designing an S-box should read this article several times with full attention and internalize the functional idea of the S-box construction mechanism. I believe that everyone will be able to build large-scale S-boxes after they capture the concept of the proposed 4×4 nonlinear S-box. However, I suggest that students analyze this matter internally and 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 intended for educational purposes rather than professional work.

Acknowledgement

First of all, I express my gratitude to almighty Allah for allowing 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. Special thanks go 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 creating a wonderful research atmosphere for me to conduct my research on the "S-box construction in modern cipher." They helped me explore how to use discrete mathematical knowledge in cryptography and discover new creative mathematical ideas. I am grateful to them for their support. I am really excited to have successfully completed this scientific task.

This publication is licensed under Creative Commons Attribution CC BY.
https://dx.doi.org/10.29322/IJSRP.14.01.2024.p14539

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 in India Hyderabad, India, December 16–18, 2002 Proceedings 3*, Springer, 2002, pages 246–259.
[3] Anne Canteaut, "Lecture notes on cryptographic Boolean functions," In: *Inria, Paris, France*, vol. 3, 2016.
[4] Maram K Balajee and JM Gnanasekar, "Evaluation of key dependent s-box based data security algorithm using hamming distance and balanced output," In: *Tem Journal*, 5(1):67-75, 2016.
[5] Pedro Miguel Sosa, "Calculating nonlinearity of Boolean functions with Walsh Hadamard transform," In: *UCSB, Santa Barbara*, pages 1–4, 2016.
[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] Thomas W Cusick and Pantelimon Stanica, *Cryptographic Boolean functions and applications*. Academic Press, 2017. ISBN: 0128111305, 9780128111307
[9] Claude Carlet, "Boolean models and methods in mathematics, Computer Science and Engineering," In: *Vectorial Boolean functions for cryptography*. Cambridge University Press: Cambridge, UK, 2010 pages 398–470. doi:10.1017/CBO9780511780448.012
[10] Dar'ya Aleksandrovna Zyubina and Natalia Nikolaevna Tokareva. "Cryptographic properties of a simple s-box construction based on a Boolean function and a Permutation," In: *Applied Discrete Mathematics. Application*, (13):41–43, 2020. Doi: 10.17223/2226308X/13/13
[11] Claude E Shannon, "A mathematical theory of cryptography," In: *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," In: *The Bell system technical journal*, 28(4):656–715, 1949.
[14] Pavol Zajac and Mat´u˘s J´okay, "Multiplicative complexity of bijective 4× 4 S-boxes," In: *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," In: *104th European Study Group with Industry*, Sofia, Bulgaria, 23-27 Sept 2014. https://parallel.bas.bg/ESGI104/final_reports/problem4.pdf
[16] Dusan Bikov, Iliya Bouyukliev, and Stefka Bouyuklieva, "Bijective s-boxes of different sizes obtained from quasi-cyclic codes," In: *Journal of Algebra Combinatorics Discrete Structures and Applications*, 6(3):123–134, 2019. Doi: 10.13069/jacodesmath.617232
[17] Data Encryption Standard et al, "Data encryption standard," In: *Federal Information Processing Standards Publication*, 112:3, Information Technology Laboratory Gaithersburg, MD, USA, 1999. https://academickids.com/encyclopedia/index.php/Data_Encryption_Standard
[18] Reynier Antonio de la Cruz Jim´enez, "On some methods for constructing almost optimal s-boxes and their resilience against sidechannel attacks," In*:Cryptology ePrint Archive*, 2018.
[19] Iqtadar Hussain, Amir Anees, Temadher Alassiry Al-Maadeed, and Muham- mad Tahir Mustafa, "Construction of s-box based on chaotic map and algebraic structures," In*: Symmetry*, 11(3):351, 2019. MDPI. Doi: 10.3390/sym11030351
[20] 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.
[21] Majid Khan, Tariq Shah, and Syeda Iram Batool, "Construction of s-box based on chaotic Boolean functions and its application in image encryption," In: *Neural Computing and Applications*, Springer. 27:677–685, 2016
[22] Musheer Ahmad, Ishfaq Ahmad Khaja, Abdullah Baz, Hosam Alhakami and Wajdi Alhakami, "Particle swarm optimization based highly nonlinear substitution-boxes generation for security applications," In: *IEEE Access*, 8:116132–116147, 2020. Doi:10.1109/ACCESS.2020.3004449.
[23] 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. https://csrc.nist.gov/CSRC/media/Publications/sp/800-67/rev-2/draft/documents/sp800-67r2-draft.pdf
[24] Christian Kaspers and Yue Zhou, "The number of almost perfect nonlinear functions grows exponentially," In: *Journal of Cryptology*, 34:1–37, 2021.
[25] Liyana Chew Nizam Chew and Eddie Shahril Ismail, "S-box construction based on linear fractional transformation and permutation function," In: *Symmetry*, 12(5):826, 2020. Doi:10.3390/sym12050826
[26] 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.
[27] Joan Daemen and Vincent Rijmen, *AES Proposal: Rijndael*.1999. https://www.cs.miami.edu/home/burt/learning/Csc688.012/rijndael/rijndael_doc_V2.pdf
[28] Zijing Jiang and Qun Ding, "Construction of an s-box based on chaotic and bent functions," In: *Symmetry*, 13(4):671, 2021. Doi:10.3390/sym13040671
[29] Joan Daemen and Vincent Rijmen, *The design of Rijndael*, volume 2. Springer, 2002.
[30] 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
[31] W Eltayeb Ahmed, "A modern method for constructing the s-box of advanced encryption standard," In: *Applied Mathematics*,10(4):234–244, 2019.
[32] Musheer Ahmad, Mohammad Najam Doja, and MM Sufyan Beg, "ABC optimization-based construction of strong substitution boxes," In: *Wireless Personal Communications*, 101:1715–1729, 2018.
[33] Pavol Zajac and Matus Jokay, "Multiplicative complexity of bijective 4× 4 S-boxes," In: *Cryptography and Communications*, 6(3):255–277, 2014.
[34] Erdener Uyan, *Analysis of Boolean functions with respect to Walsh spectrum*.Middle East Technical University. 2013. http://etd.lib.metu.edu.tr/upload/12616246/index.pdf

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

This publication is licensed under Creative Commons Attribution CC BY.
https://dx.doi.org/10.29322/IJSRP.14.01.2024.p14539

APPENDIX A: ASSESSMENT FORM

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

This publication is licensed under Creative Commons Attribution CC BY.
https://dx.doi.org/10.29322/IJSRP.14.01.2024.p14539

APPENDIX B: APPROVAL FORM

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. Novosibirsk, 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

This publication is licensed under Creative Commons Attribution CC BY.
https://dx.doi.org/10.29322/IJSRP.14.01.2024.p14539

APPENDIX C: APPLICATION FOR INDUSTRIAL PRACTICE

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. _____
(подпись обучающегося)

Согласовано:

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

This publication is licensed under Creative Commons Attribution CC BY.
https://dx.doi.org/10.29322/IJSRP.14.01.2024.p14539

APPENDIX D: AGREEMENT FORM

Задание утверждено на заседании кафедры ____Faculty of Information Technology _____
(наименование кафедры)
протокол от «___» _____ 20__г. **Дата выдачи задания: «___»** _____ 20__г.

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

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

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

Задание принял(а) к исполнению: _____ **Md. Shamim Hossain Biswas**
(подпись обучающегося) (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: _____ ____ Marina Derzho_____
(подпись)* (ФИО, должность)

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

This publication is licensed under Creative Commons Attribution CC BY.
https://dx.doi.org/10.29322/IJSRP.14.01.2024.p14539