# Towards a Framework for the Design of Nonlinear Combiners in Ternary Logic

Slobodan Petrović

Norwegian University of Science and Technology (NTNU),
P.O. box 191, N-2802 Gjøvik, Norway
slobodan.petrovic@ntnu.no

**Abstract.** Ternary logic is gaining popularity since it enables realization of complex electronic circuits with fewer active elements than with binary logic. In this short paper we draw the contours of a framework for finding nonlinear combining switching functions for cryptographic applications realized on ternary IoT hardware platforms. We review the theoretical results and criteria related to ternary switching function adequacy for use in cryptography. Our framework computes the Algebraic Normal Form (ANF) of such functions and uses the Vilenkin-Chrestenson spectrum to test their non-linearity and correlation immunity.

**Keywords:** Cryptographic Engineering · Ternary Logic · Switching Functions · Vilenkin-Chrestenson Transform.

## 1 Introduction

In cryptographic applications, it is of interest to implement complex algorithms on IoT hardware platforms. This is often difficult, since the requirements for security level are strict and complexity of the algorithms steadily increases. Therefore, switching to non-binary hardware platforms (in particular ternary) could help in improving security even on tiny devices, whose resources are severely limited. One of the essential primitives contained in many cryptographic algorithms is a switching function with adequate properties, such as balancedness, good correlation immunity, high non-linearity, and high algebraic degree. The theoretical results needed to determine these parameters for the given non-binary switching function have been obtained by generalizing the results that hold for binary (i.e., Boolean) functions. In this short paper, we sketch the contours of a framework for searching for the best switching functions for cryptographic applications on ternary hardware platforms. We review the relevant theoretical results that are valid in a field with the characteristic $p$ and apply them in the ternary environment. We explain how to search for a balanced, $m$-resilient, non-linear ternary switching combiner of high algebraic degree.

The paper is organized as follows: In Section 2, we review the relevant theoretical results that can be used in a non-binary environment to search for the convenient switching functions. In Section 3, we give an example of searching for a ternary switching combiner acceptable for use in a stream cipher for IoT. Section 4 concludes the paper.

## 2 Theoretical background

For a switching function in a Galois field with the characteristic $p$, $p > 2$, balancedness is easily checked by inspecting the table of values. To determine the algebraic degree $d$ of such a function, we have to compute its Algebraic Normal Form (ANF). It can be obtained by generalizing the algorithm used for computing ANF of Boolean functions (see for example [1]). We start with a function of 1 variable and form a matrix, whose columns are $j$-th powers of all the possible values $(0, 1, \ldots, p-1)$ of this variable, $j = 0, 1, \ldots, p-1$. The obtained matrix is

$$\mathbf{A}_1 = \begin{bmatrix} 1\ 0 & 0 & \cdots 0 \\ 1\ 1 & 1 & \cdots 1 \\ 1\ 2 & 2^2 \bmod p & \cdots 2^{p-1} \bmod p \\ \vdots & & \cdots \\ 1\ p-1 & (p-1)^2 \bmod p & \cdots (p-1)^{p-1} \bmod p \end{bmatrix}.$$

Let $\mathbf{F}$ be the value vector of the given switching function $f$. Let $\mathbf{B}_1 = \mathbf{A}_1^{-1}$ and let $\mathbf{B}_n = \bigotimes_{j=1}^{n-1} \mathbf{B}_1$, where $\bigotimes$ is the Kronecker product of matrices. Then $\mathbf{S} = \mathbf{B}_n \cdot \mathbf{F}$ is the vector of coefficients of the ANF. All the operations are taken modulo $p$. Let $s_u$ be a component of the vector $\mathbf{S}$, $u = 0, \ldots, p^n - 1$, and let $(u_1, \ldots, u_n)$ be the representation of $u$ in the form of a vector of digits modulo $p$. Then the ANF of the switching function $f$ of $n$ variables, whose value vector is $\mathbf{F}$ is $f(x_1, \ldots, x_n) = \sum_{u=0}^{p^n-1} s_u \prod_{j=1}^{n} x_j^{u_j}$, where the sum is taken modulo $p$.

To study the non-linearity (i.e., the distance of the given function to the affine functions) and correlation immunity of non-binary switching functions, we can use the Vilenkin-Chrestenson transform [4, 5], which is a generalization of the Walsh transform used in the binary environment for this purpose[1]. The transform matrix of the Vilenkin-Chrestenson transform is a matrix of complex numbers. In a Galois field with the characteristic $p$, to obtain the Vilenkin-Chrestenson transform matrix, we start with the complex primitive $p$-th roots of unity $a_k = e^{2k\pi i/p}$, $k = 0, \ldots, p-1$, where $i = \sqrt{-1}$. We map the function values $0, 1, \ldots, p-1$ to the complex numbers $a_0, a_1, \ldots, a_{p-1}$, respectively. Then, from the Vandermonde matrix of dimension $p \times p$

$$\mathbf{V} = \begin{bmatrix} a_0 & a_0 & a_0^2 & \ldots a_0^{p-1} \\ a_0 & a_1 & a_1^2 & \ldots a_1^{p-1} \\ a_0 & a_2 & a_2^2 & \ldots a_2^{p-1} \\ \vdots & & & \\ a_0 & a_{p-1} & a_{p-1}^2 & \ldots a_{p-1}^{p-1} \end{bmatrix},$$

we obtain the basis matrix $\mathbf{V}_1$ of the Vilenkin-Chrestenson transform, which is the conjugate transpose (the Hermitian) of the matrix $\mathbf{V}$. From the basis matrix,

[1] Sometimes, for example in [2, 6], the generalization of the Walsh transform is also called the Walsh/Walsh-Hadamard transform.

the Vilenkin-Chrestenson transform matrix for a function $f$ of $n$ variables is obtained by computing $\mathbf{V}_n = \bigotimes_{j=1}^{n-1} \mathbf{V}_1$. By multiplying the obtained matrix $\mathbf{V}_n$ by the value vector $\mathbf{F}$ of the function $f$ we get the vector $\mathbf{W}$ of the Vilenkin-Chrestenson transform coefficients of $f$.

The maximally non-linear switching functions in a Galois field of characteristic $p$ are bent functions, whose Vilenkin-Chrestenson spectrum has the components, whose absolute values are all equal to $p^{n/2}$. Unfortunately, bent functions are never balanced. Since we need balanced functions in most cases, we have to find switching functions with small absolute values of the components of the Vilenkin-Chrestenson transform. These functions possess non-linearity lower than bent functions, but they are balanced, which increases the possibility of their application in cryptography. In many cases, the search for such functions starts from bent functions.

In the binary environment, the following theorem (see for example [3]) is used for studying the correlation immunity of functions:

**Theorem 1.** *A Boolean function $f$ in $n$ variables is correlation immune of order $m$ if and only if $\mathbf{W}(j) = 0$, $1 \leq wt(j) \leq m$*

where $wt(j)$ is the Hamming weight of the binary representation of $j$.

A generalization of Theorem 1 to a Galois field with the characteristic $p$ was proved in [7] using perfect 2-colorings of hypercubes. Thus, as in a binary environment, a switching function in a Galois field of characteristic $p$ is correlation immune of order $m$ if and only if $\mathbf{W}(j) = 0$, $1 \leq wt(j) \leq m$, where $wt(j)$ is the Hamming weight of the representation of $j$ in the base $p$.

By applying the theoretical results exposed above, we can compute the values of the corresponding properties of a given switching function in a Galois field with the characteristic $p$. In such a way, we can search for a balanced switching function that is adequate for use as a combiner in cryptography since it possesses the best compromise between non-linearity, correlation immunity, and algebraic degree.

## 3 Searching for an adequate ternary switching combiner

The theoretical background exposed in the Section 2 has served as a fundament of our software framework for search for adequate stream cipher combiners in the ternary environment. For computing ANF, in ternary, we have $\mathbf{A}_1 = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 2 & 1 \end{bmatrix}$ and $\mathbf{B}_1 = \mathbf{A}_1^{-1} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 2 & 2 & 2 \end{bmatrix}$. Thus, for a ternary switching function $f$ of $n = 2$ variables, we have $\mathbf{B}_2 = \bigotimes_{j=1}^{1} \mathbf{B}_1$, which is a matrix of dimension $9 \times 9$. As an example, for the balanced function $f$, whose vector of function values is $\mathbf{F} = (1, 2, 0, 0, 1, 2, 0, 2, 1)$, we obtain the ANF $f(x_1, x_2) = 1 + x_2 + x_1x_2 + 2x_1^2 + 2x_1^2x_2$. The algebraic degree of this function is $d = 3$.

To study the non-linearity and correlation properties of the given ternary switching function, we use the Vilenkin-Chrestenson transform. In ternary, $a_0 = 1$, $a_1 = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$, $a_2 = -\frac{1}{2} - i\frac{\sqrt{3}}{2}$, and the following identities hold: $a_0^* = a_0$, $a_1^* = a_2$, $a_2^* = a_1$, $a_0 + a_1 + a_2 = 0$, where $*$ denotes conjugate complex. Thus, we get the Hermitian of the Vandermonde matrix $\mathbf{V}_1 = \begin{bmatrix} a_0 & a_0 & a_0 \\ a_0 & a_2 & a_1 \\ a_0 & a_1 & a_2 \end{bmatrix}$. For example, for the same function, whose ANF we have computed above, the coefficients of its Vilenkin-Chrestenson spectrum (divided by the real constant 3) are $(0, -a_2, a_0, 0, -a_0, a_1, 0, 2a_1, a_2)$. The absolute values of all the components of the spectrum are $\leq 1$, except the component $2a_1$. Consequently, the non-linearity properties of this function can be acceptable in many cases. But this function is not correlation immune even of order 1, since not all the necessary components of the Vilenkin-Chrestenson spectrum are equal to zero (see Theorem 1).

Our framework can be used for search for the best ternary function for the particular application. In practice, we can enumerate all the functions if the number of variables is small (which is most often the case with IoT combiners) and for each function, we can compute the ANF and the Vilenkin-Chrestenson spectrum. Then we can choose the balanced function that offers the best trade-off between non-linearity and correlation immunity.

## 4 Conclusion

In this paper, we have reviewed the theoretical background for computing the relevant properties (algebraic degree, non-linearity, and correlation immunity) of non-binary switching functions. We have given the contours of a software framework for searching for adequate ternary switching functions possessing the best trade-off between these properties. Then we can use such functions as combiners in stream ciphers implemented on ternary IoT platforms.

## References

1. Stanković R., Astola J., Moraga C.: Representation of multiple-valued logic functions. Springer Nature, Switzerland (2022).
2. Budaghyan L.: Construction and analysis of cryptographic functions. Springer, Heidelberg (2014).
3. Cusick T.W., Stănică P.: Cryptographic Boolean functions and applications. Academic Press, San Diego (2009).
4. Vilenkin N., Agaev G., and Dzafarli G.: Towards a theory of multiplicative orthogonal systems of functions. DAN Azerb. SSR, **18**(9), pp. 3–7, (1962).
5. Chrestenson H.: A class of generalized Walsh functions. Pacific J. Math., **5**(5), pp. 17–31, (1955).
6. Potapov V.N.: On $q$-ary bent and plateaued functions. Designs, Codes, and Cryptography, **88**, pp 2037–2049, (2020).
7. Potapov V.N.: On perfect 2-colorings of the $q$-ary $n$-cube. Discret. Math. **312**(6), pp. 1269–1272, (2012).