AN IMPROVED NUMEROV METHOD FOR THE SOLUTION OF SPECIAL SECOND ORDER IN ORDINARY DIFFERENTIAL EQUATIONS

by

Abdu MasanawaSagir

Hassan Usman Katsina Polytechnic, Katsina. Katsina State. Nigeria.

E-mail: amsagir@yahoo.com

Abstract

Linear multistep method using power series as the basis function was used to develop an improved Numerov method which is suitable for generating direct solution of the special second order ordinary differential equations of the form $y^{"} = f(x, y),\ a \le x \le b$ *with associated initial or boundary conditions. The continuous hybrid formulations enable us to differentiate and evaluate at some grids and off – grid points to obtain four discrete schemes of order* $(4,4,4)^T$*, which were used in block form for parallel or sequential solutions of the problems. The computational burden and computer time wastage involved in the usual reduction of second order problem into system of first order equations are avoided by this approach. Furthermore, a stability analysis and efficiency of the block method are tested on linear and non-linear ordinary differential equations whose solutions are oscillatory or nearly periodic in nature, and the results obtained compared favourably with the exact solution.*

Keywords: *Block Method, Hybrid, Linear Multistep Method, Self – starting, Special Second Order*

INTRODUCTION

Let us consider the numerical solution of the special second order ordinary differential equation of the form

$$y^{"} = f(x, y), x \le x \le b \tag{1}$$

with associated initial or boundary conditions. The mathematical models of most physical phenomena especially in mechanical systems without dissipation leads to special second order initial value problem of type (1). Solutions to initial value problem of type (1) according to Fatunla (1991; 1995) are often highly oscillatory in nature and thus, severely restrict the mesh size of the conventional linear multistep method. Such system often occurs in mechanical systems without dissipation, satellite tracking and celestial mechanics.

Lambert (1973) and several authors such as (Onumanyi*et al., 1994*;Awoyemi, 1998; Yahaya and Adegboye, 2008; Fudziah*et al*., 2009; Aladeselu, 2007; Yahaya and Mohammed, 2010; Yakusak and Owolanka, 2018; Abdelrahim and Omar, 2016 and Adesanya*et al.,* 2015) have written on conventional linear multistep method

$$\sum_{j=0}^{k} \propto_j y_{n+j} = h^2 \sum_{j=0}^{k} \beta_j f_{n+j}, k \ge 2 \tag{2}$$

or compactly in the form

$$\rho(E) y_n = h^2 \delta(E) f_n \tag{3}$$

where$E$ is the shift operator specified by $E^j y_n = y_{n+j}$ while ρ and δ are characteristics polynomials and are given as

$$\rho(\xi) = \sum_{j=0}^{k} \propto_j \xi^j, \delta(\xi) = \sum_{j=0}^{k} \beta_j \xi^j \tag{4}$$

$y_n$is the numerical approximation to the theoretical solution y(x) and $f_n = f(x_n, y_n)$.

In the present consideration, our motivations for the study of this approach is a further advancement in efficiency, i.e obtaining the most accuracy per unit of computational effort, that can be secured with the group of methods proposed in this paper over (Awoyemi, 1998) and (Yahaya and Mohammed, 2010).

Definition 1. Consistent:

The linear multistep method (2) is said to be consistent if it has order $p \geq 1$, that is, if

$$\sum_{j=0}^{k} \propto_j = 0 \text{and} \sum_{j=0}^{k} j \propto_j - \sum_{j=0}^{k} \beta_j = 0 \qquad (5)$$

Introducing the first and second characteristics polynomials (4), we have from (5) LMM type (2) is consistent if $\rho(1) = 0, \rho^1(1) = \delta(1)$

Definition 2. Zero stability:

A linear multistep method type (2) is zero stable provided the roots $\xi_j, j = 0(1)k$ of first characteristics polynomial $\rho(\xi)$ specified as $\rho(\xi) = \det\left|\sum_{j=0}^{k} A(i)\xi^{(k-i)}\right| = 0$ satisfies $|\xi_j| \leq 1$ and for those roots with $|\xi_j| = 1$ the multiciplicity must not exceed two. The principal root of $\rho(\xi)$ is denoted by$\xi_1 = \xi_2 = 1$.

Definition 3. Convergence:

The necessary and sufficient conditions for the linear multistep method type (2) is said to be convergent if it is consistent and zero stable.

Definition 4. Order and Error Constant:

The linear multistep method type (2) is said to be of order p if $c_0 = c_1 = \cdots c_{P+1} = 0$ but $c_{p+2} \neq 0$ andc_{p+2} is called the error constant,

where $c_0 = \sum_{j=0}^{k} \propto_j = \propto_0 + \propto_1 + \propto_2 + \ \ldots \ + \propto_k$

$c_1 = \sum_{j=0}^{k} j \propto_j = (\propto_1 + \ 2 \propto_2 + 3 \propto_3 + \ \ldots \ + k \propto_k)$

$$-(\beta_0 + \beta_1 + \beta_2 + \cdots + \beta_k)$$

$c_2 = \sum_{j=0}^{k} \frac{1}{2!} j^2 \propto_j - \sum_{j=0}^{k} \beta_j$

$$= \left\{ \begin{matrix} \frac{1}{2!}(\propto_1 + \ 2^2 \propto_2 + 3^3 \propto_3 + \ \ldots \ + k^2 \propto_k) \\ -(\beta_1 + 2\beta_2 + 3\beta_3 + \ \ldots + k\beta_k) \end{matrix} \right\}$$

.

.

.

$c_q = \sum_{j=1}^{k} \{\frac{1}{q!} j^q \propto_j - \frac{1}{(q-2)!} j^{q-2} \beta_j\}$

$$= \left\{ \begin{matrix} \frac{1}{q!}(\propto_1 + \ 2^q \propto_2 + 3^q \propto_3 + \ \ldots \ + k^q \propto_k) \\ -\frac{1}{(q-1)!}\left(\beta_1 + 2^{(q-1)}\beta_2 + 3^{(q-1)}\beta_3 + \cdots + k^{(q-1)}\beta_k\right) \end{matrix} \right\} \qquad (6)$$

Theorem 1:

Let $f(x, y)$ be defined and continuous for all points (x, y) in the region D defined by$\{(x, y) : a \leq x \leq b, -\infty < y < \infty\}$ where *a and b* finite, and let there exist a constant L such that for every x, y, y^* such that (x, y) *and* (x, y^*) are both in D:

$$|f(x, y) - f(x, y^*)| \leq L|y - y \qquad (7)$$

Then if η is any given number, there exist a unique solution $y(x)$ of the initial value problem (1), where $y(x)$ is continuous and differentiable for all (x, y) *in D*. The inequality (7) is known as a Lipschitz condition and the constant L as a Lipschitz constant.

Consequently, this paper is organized as follows: in first section we will show the

introduction, this lead to second section which shows how the method was derived, third section presents stability analysis of the method with some numerical experiments, while the fourth and last section of this paper concludes the work and references respectively.

DERIVATION OF THE PROPOSED METHOD

The researcher proposed an approximate solution to (1) in the form

$$y(x) = \sum_{j=0}^{t+m-1} a_j x^i = y_{n+j}, i = 0(1)m+t-1 \quad (8)$$

$$y^{"}(x) = \sum_{j=0}^{t+m-1} i(i-1)a_j x^{i-2} = f_{n+j}, i = 2(3)m+t-1 \quad (9)$$

with $m = 4,\ t = 3$ *and* $p = m+t-1$

where the a_j, $j = 0,1,(m+t-1)$ are the parameters to be determined, t and m are points of interpolation and collocation respectively. Where p, is the degree of the polynomial interpolant of our choice.

Specifically, we collocate equation (9) at $x = x_{n+j}$, $j = 0(1)k$ and interpolate equation (8) at $x = x_{n+j},\ j = 0(1)k - \frac{4}{3}$ using the method described above. Putting in the matrix equation form and then solved to obtain the values of parameters α_j's, j =0, 1, … which is substituted in (8) yields, after some algebraic manipulation, the new continuous form for the solution

$$y(x) = \sum_{j=0}^{k-\frac{4}{3}} \propto_j (x) y_{n+j} + \sum_{j=0}^{k} \beta_j (x) f_{n+j} \quad (10)$$

We set $\gamma = (x - x_{n+1})$

If we let k = 2, after some algebraic manipulations we obtain a continuous form of solution

$$\begin{aligned} y(x) &= \left\{-\left(\frac{x - x_{n+1}}{h}\right)\right\} y_n + \left\{\left(\frac{h + x - x_{n+1}}{h}\right)\right\} y_{n+1} \\ &+ \left\{\frac{-9(x - x_{n+1})^5 + 20h(x - x_{n+1})^4 - 10h^2(x - x_{n+1})^3 + 39h^4(x - x_{n+1})}{480h^3}\right\} f_n \\ &+ \left\{\frac{9(x - x_{n+1})^5 - 5h(x - x_{n+1})^4 - 30h^2(x - x_{n+1})^3 + 30h^3(x - x_{n+1})^2 + 46h^4(x - x_{n+1})}{60h^3}\right\} f_{n+1} \\ &+ \left\{\frac{-27(x - x_{n+1})^5 + 90h^2(x - x_{n+1})^3 - 63h^4(x - x_{n+1})}{160h^3}\right\} f_{n+\frac{4}{3}} \\ &+ \left\{\frac{9(x-x_{n+1})^5 + 10h(x-x_{n+1})^4 - 10h^2(x-x_{n+1})^3 + 11h^4(x-x_{n+1})}{240h^3}\right\} f_{n+2} \end{aligned} \quad (11)$$

Evaluating the continuous scheme of equation (11) at some selected points and its second derivative at an off - grid point respectively yield the following schemes:

$$y_{n+\frac{4}{3}} - \frac{4}{3} y_{n+1} + \frac{1}{3} y_n = \frac{h^2}{486}\{13f_n + 142f_{n+1} - 54f_{n+4/3} + 7f_{n+2}\} \quad (12)$$

$$y_{n+2} - 2y_{n+1} + y_n = \frac{h^2}{12}\{f_n + 10f_{n+1} + f_{n+2}\} \quad (13)$$

Interestingly, at $x = x_{n+2}$, the already known Numerov's scheme was recovered.

Differentiating equation (11) w.r.t. x once and substituting at $x = x_0$ yields:

$$hz_0 - y_{n+1} + y_n = \frac{h^2}{120}\{-29f_n - 78f_{n+1} + 54f_{n+4/3} - 7f_{n+2}\} \quad (14)$$

Equations (12), (13) and (14) constitute the member of a zero stable block integrators of order $(4,4,4)^T$ with

$c_6 = \left(-\frac{313}{262440}, -\frac{1}{240}, \frac{23}{4320}\right)$. The application of the block integrators with n = 0 gives the accurate values of unknown as shown in tables 1 and 2 of third section of this paper.

To start the IVP integration on the sub interval $[X_0, X_3]$, we combine equations (12), (13) and (14), when n = 0 i.e the 1-block 3-point method are given in equation (14). Thus produces simultaneously values for y_1, y_2, y_3 and $y_{\frac{4}{3}}$ without recourse to any predictor like (Awoyemi, 1998) to provide y_1 and y_2 in the main method. Hence this is an improvement over these reported works. Though, this does not becloud the contribution of these authors.

STABILITY ANALYSIS

Recall, that, it is a desirable property for a numerical integrator to produce solution that behave similar to the theoretical solution to a problem at all times. Thus, several definitions, which call for the method to posses some "adequate" region of absolute stability can be found in several literatures, see (Lambert, 1973; Fatunla, 1991).

Following Fatunla (1991; 1995), the four integrator proposed in this report in equation (12), (13) and (14) are put in the matrix equation form and for easy analysis the result was normalized to obtain;

$$\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix}\begin{bmatrix}y_{n+1}\\y_{n+\frac{4}{3}}\\y_{n+2}\end{bmatrix} = \begin{bmatrix}0&-\frac{1}{3}&\frac{2}{3}\\0&-1&2\\0&-1&2\end{bmatrix}\begin{bmatrix}y_{n-1}\\y_{n-\frac{2}{3}}\\y_n\end{bmatrix} + h^2\left\{\begin{bmatrix}-\frac{1}{9}&\frac{7}{486}&-\frac{14}{81}\\0&\frac{1}{12}&-1\\\frac{9}{20}&-\frac{7}{120}&\frac{1}{6}\end{bmatrix}\begin{bmatrix}f_{n+1}\\f_{n+\frac{4}{3}}\\f_{n+2}\end{bmatrix} + \begin{bmatrix}0&\frac{13}{486}&-\frac{13}{243}\\0&\frac{1}{12}&-\frac{1}{6}\\0&-\frac{29}{120}&\frac{29}{60}\end{bmatrix}\begin{bmatrix}f_{n-1}\\f_{n-\frac{2}{3}}\\f_n\end{bmatrix}\right\} \quad (15)$$

with $y_0 = \begin{pmatrix} y_0 \\ hz_0 \end{pmatrix}$ usually giving along the initial value problem. Equation (15) is the 1- block 3 – point method. The first characteristics polynomial of the proposed 1- block 3 – point method is given by

$$\rho(\lambda) = \det\left[\lambda I - A_1^{(1)}\right] \quad (16)$$

$$\rho(\lambda) = \det\begin{bmatrix}\lambda&\frac{1}{3}&-\frac{2}{3}\\0&\lambda+1&-2\\0&1&\lambda-2\end{bmatrix} \quad (17)$$

Solving the determinant of equation (17), yields

$$\rho(\lambda) = \lambda^2(\lambda - 1) \quad (18)$$

which implies, $\lambda_1 = \lambda_2$ or $\lambda_3 = 1$

By definition of zero stable and equation (17), the 1 - block 3 - point method is zero stable and is also consistent as its order $(4,4,4)^T > 1$, thus, it is convergent following (Henrici, 1962) and (Fatunla, 1995).

NUMERICAL EXPERIMENTS

In what follows, we present some numerical results on some problems.

Problem 1: Consider a Non-Linear IVP; $y'' = 2y^3; y(1) = 1, y'(1) = -1$, whose exact solution is $y(x) = 1/x$

Table 1: Results for the Proposed Method with one Off - Grid Point at Interpolation

N	x	Exact Value	Approximate Value	Awoyemi (1998)	Error of Proposed Method
0	1	1	1	0	0
1	1.1	0.909090109	0.9090914832	2.8483722E-03	1.37420E-08
2	1.2	0.833333333	0.8333348886	2.2688344E-01	1.55560E-08
3	1.3	0.769230769	0.7692330281	7.3968630E+00	2.25910E-08
4	1.4	0.714285714	0.7142880973	2.1168783E-01	2.38330E-08
5	1.5	0.666666667	0.6666693038	3.3156524E-01	2.63680E-08
6	1.6	0.625000000	0.6250029082	4.3968593E-01	2.90820E-07
7	1.7	0.588235294	0.5882382539	5.3903097E-01	2.95990E-07
8	1.8	0.555555556	0.5555586407	6.3121827E-01	3.08470E-06
9	1.9	0.526315789	0.5263190456	7.1723621E-01	3.25660E-06
10	2.0	0.500000000	0.5000032878	7.9776590E-01	3.28780E-06

Problem 2: Consider the BVP $y'' = 3x + 4y;\ y(0) = 0,\ y(1) = 1$,whose exact solution is $y(x) = \frac{7}{4(e^2 - e^{-2})}[e^{2x} - e^{-2x}] - \frac{3}{4}x$

Table 2: Results for the Proposed Method with one Off - Grid Point at Interpolation

x	Exact Value	Approximate Value	Yahaya and Mohammed (2010)	Error of Proposed Method
0	0.00000000000	0.00000000000	0.000000000E+00	0.000000000E+00
0.2	0.04819251100	0.04819008513	1.828560000E-04	2.425870000E-06
0.4	0.12852089500	0.1285138496	3.931120000E-04	7.045400000E-06
0.6	0.27833169000	0.2783207232	6.672570000E-04	1.096680000E-05
0.8	0.54623764000	0.5463115949	1.050930000E-03	7.395490000E-05
1.0	1.00000000000	1.000042276	0.000000000E+00	4.227600000E-05

CONCLUSION

Onumanyi et al. (1994) and Awoyemi (1998) discussed in some detailed theoretical and practical aspects of collocation with piecewise polynomial function. Roughly, their results particularly Awoyemi (1998) indicated that the solution of a second order non linear problem can be approximated with linear multistep methods. In this paper, the researcher developed a uniform order 1 – block 3 – point integrators of order $(4,4,4)^T$. The resultant numerical integrators posses the following desirable properties:

i. Zero stability i.e. stability at the origin
ii. Convergent schemes
iii. An addition of equation from the use of first derivative
iv. Being self – starting as such it eliminate the use of predictor – corrector method
v. Facility to generate solutions at 3 points simultaneously
vi. Produce solution over sub intervals that do not overlaps
vii. Apply uniformly to both IVP_s and BVP_s with adjustment to the boundary conditions

In addition, the new schemes compares favourably with the theoretical solution and the results are more accurate than (Awoyemi, 1998) and (Yahaya and Mohammed, 2010), see table 1 and 2. Hence, the proposed method is an improvement over other cited works.

REFERENCES

Abdelrahim R. & Omar Z. (2016). Direct solution of second order ordinary differential Equation using a single-step hybrid block method of order five. *Journal of Mathematical and Computational Applications,* 21(2), 1-7.

Adesanya A.O., Fotta A.U. &Abdulkadri B. (2015). Hybrid One Step Block Method for the Solutn oiof Fourth Order Initial Value Problems of Ordinary Differential Equations.*International Journal of Pure and Applied Mathematics*, 104(2), 159-169.

Aladeselu N. A. (2007). Improved family of block methods for I.V.P. *Journal of the Nigeria Association of Mathematical Physics*, 11(1), 153 – 158.

Awoyemi D.O. (1998). A class of Continuous Stormer–Cowell Type Methods for Special Second Order Ordinary Differential Equations. *Journal of Nigerian Mathematical Society*, 5(1), 100 – 108.

Fatunla S.O. (1991). Block Method for Second Order Initial Value Problem. *International Journal of Computer Mathematics,* England, 41(1-2), 55 – 63.

Fatunla S.O. (1995). A class of block methods for second order IVPs.*International Journal of Computer Mathematics*, 55(1-2), 119-133.

Fatunla S.O, Ikhile M.N.O, &Otunta F.O. (1999). A class of p – stable linear multistep numerical methods. *International Journal of computer mathematics*,72(1), 1 – 13.

Fudziah I. Yap L. K. & Mohammad O. (2009). Explicit and Implicit 3 – point Block Methods for Solving Special Second Order Ordinary Differential Equations Directly. *International Journal of math. Analysis*, 3(9), 239 – 254.

Henrici P. (1962). Discrete Variable Methods for ODE_s.John Willey New York U.S.A.

Lambert J.D. (1973). Computational Methods in Ordinary Differential Equations. JohnWilley and Sons, New York, USA.

Lie I. &Norsett S.P. (1989). Super Convergence for Multistep Collocation. Mathematics of Computation, 52(185), 65 – 79.

Onumanyi P., Awoyemi D.O, Jator S.N. & Sirisena U.W. (1994). New linear Multistep with Continuous Coefficient for first order initial value problems. *Journal of Mathematical Society,* 13, 37 – 51.

Yahaya Y.A &Adegboye, Z.A. (2008). *A family of 4 – step Block Methods for Special Second Order in Ordinary Differential Equations*. Proceedings Mathematical Association of Nigeria, 23 – 32.

Yahaya Y.A & Mohammed U. (2010). A 5 – Step Block Method for Special Second Order Ordinary Differential Equations. *Journal of Nigerian Mathematical Society*.29, 113 – 126.

Yakusak N.S. &Owolanke A.O. (2018). A Class of Linear Multi-step Method for Direct Solution of Second Order InitialValue Problems in Ordinary Differential Equations by Collocation Method. *Journal of Advances in Mathematics and Computer Science,* 26(1), 1-11.

CRYPTOGRAPHIC REQUIREMENTS OF BOOLEAN FUNCTIONS

by

Aliyu DanladiHina, Abdullahi M. Auwal, & Rakiya M.K. Adamu and Bala Umar
Basic Studies Department, Federal Polytechnic, Bauchi, Computer science Department, Federal Polytechnic, Bauchi, General Studies Department, Federal Polytechnic, Bauchi
auwal2gga@yahoo.com

Abstract
Boolean functions are the building blocks of symmetric cryptographic algorithms. Symmetrical cryptographic algorithms are fundamental tools in the design of all types of digital security systems. Cryptographic applications of Boolean functions are meant to have some cryptographic properties, those properties are built to thwart cryptanalysis of certain kinds, and multiple crypto-graphic properties are usually required for a Boolean function to be used in cryptographic algorithm design, expected to resist some known attacks. Nonlinear Boolean functions are considered for a long time to construct symmetric cryptosystems. In order to resist the known attacks, many properties of Boolean functions must be utilized. In this paper we analyse some major properties according to different attacks. Therefore, the primary applications of cryptographic Boolean functions are the design of cryptographic algorithms, particularly stream cipher and block cipher algorithms. We discussed some applications of Boolean functions with cryptographic properties, where the involved Boolean functions are primary building blocks.

Keyword*: Boolean functions, symmetric cryptosystems, stream cipher and block cipher algorithms*

1. Introduction
Cryptography, originally from the Greek words 'kryptos = to hide' and 'graphein = to write' is the combination of all processes aimed at denying an intruder called an adversary, to make meaning of a message sent through an unsecure channel. Prior to the modern age, it was synonymous with encryption, the conversion of information from a readable state to apparent nonsense. Encryption does not itself prevent interference, but denies the intelligible content to the adversary. Plaintext messages (M) are encrypted into unintelligible content called ciphertext (C)using an encryption key (K_e). The original message (M) is recovered back through a process called decryption using a decryption key(K_d). [18].

$K_e(M) = C$; and $M = K_d(C)$	(1)

Cryptography could be symmetric or asymmetric. With symmetric cryptography, two separate keys are used for encryption and decryption $K_e \neq K_d$ (Fig. 1a), example of which includes the commonly used AES (Advanced Encryption Standard) which replaced the older DES (Data Encryption Standard). In an event where both encryption and decryption are done with a single key$K_e = K_d = k$,then we have what is called a asymmetric cryptography (Fig. 1b), e.g. RSA (Rivest-Shamir-Adleman), and ECC (Elliptic Curve Cryptography).

T he security of cryptographic algorithms is about successful transmission of the information without it being intercepted by an adversary. The security largely a function of the encryption key/keys. This is supported by the Kirchhoff 's principle, which states that: a cryptosystem should be secure even if everything about the system, except the key, is public knowledge [17]. The idea is that, if any part of a cryptosystem (except the individual secret key) has to be kept secret then the cryptosystem is indeed not secure. That's because if the simple act of disclosing some detail of the system were to make it suddenly insecure then

you've got a problem on your hands. The generation of the key stream is thus an issue of concern. In a stream cipher, the keystream, is the sequence which is combined, digit by digit, to the plaintext sequence for obtaining the cipher-text sequence $C = M$ The keystream is generated by a nite state automaton called the keystream generator. keystreams are required to pass prescribed statistical tests. The statistical analysis of the random sequences (keystream) is very important but alongside the application of statistical tests that assess the outcome of a randomness generator, there must be a serious analysis of the source the generator extracts randomness from [10]. The quality of a keystream by way of its randomness/complexity, largely depends on the nonlinearity of the generating function used [4]. One function that has stand out as an efficient tool in this regard is the Boolean function.

The study of Boolean functions has been a branch of cryptography for many decades. In 1949 Shannon established the foundations of modern cryptography by formulating the notion of product ciphers which use two basic cryptographic transformations: permutations and substitutions. These transformationsuse Boolean functions with desirable cryptographic properties [8, 2].

Boolean functions are the building blocks of symmetric cryptographic systems [6]. Symmetrical cryptographic algorithms are fundamental tools in the design of all types of digital security systems. A concise reference on how Boolean functions are used in cryptography. Currently, practitioners who need to apply Boolean functions in the design of cryptographic algorithms and protocols need to insight into detailed properties and/or characteristics of Boolean functions.

The most important part of a stream cipher is the key stream generator, which provides the overall security for stream ciphers. Nonlinear Boolean functions were preferred for a long time to construct the key stream generator. In order to resist several known attacks, many requirements have been proposed on the Boolean functions [7]. Attacks against the cryptosystems have forced deep research on Boolean function to allow us a more secure encryption.

Symmetric cryptosystems' security is strongly influenced by the Boolean functions deployed. Hence, the knowledge about cryptographic properties of Boolean functions will hence guide the systems' designer with regards the choice of the most suitable Boolean function to use. With a cryptographic mind, one needs to have the following knowledge about Boolean functions:

The properties of Boolean functions;

The design and implementation of Boolean functions;

The existence, distribution, construction of Boolean functions with certain properties;

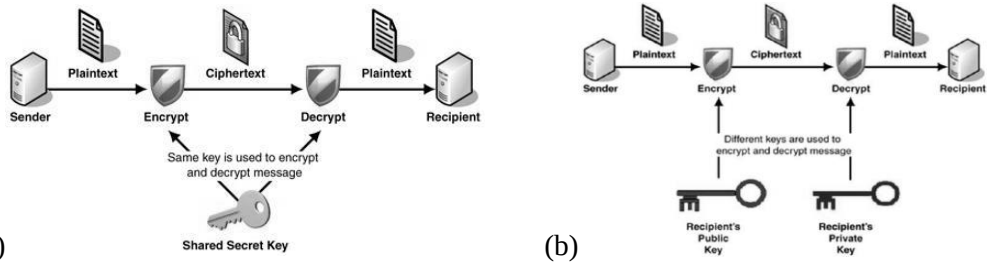


Figure 1: Cryptographic Algorithms.

The trade-off between various required properties of Boolean functions, with a view to maximize quality and improve the performance of cryptosystems;

The study of new properties according to new attacksthatwill be emerging with time.

2. Preliminaries

A Boolean function f of $n$variables is a set of all possible mappings $f: \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ where $\mathbb{F}_{2^n}$ is a Galois field of order n and $\mathbb{F}_2^n$ is its corresponding vector space [19]. Such a Boolean function can be represented as a polynomial viz:

$$f(x) = f(x_1, x_2, \dots, x_n) = \oplus_{u \epsilon \mathbb{F}_2^n} a^u X^u \qquad (2)$$

where$a \epsilon \mathbb{F}_2$ and $x, u \epsilon \mathbb{F}_2^n$. This representation is known as algebraic normal form (ANF) and its degree is called the algebraic degree.

The field of all Boolean functions B_n of order n has cardinality 2^{2n}. A Boolean function $f(x) = f(x_1, x_2, \dots, x_n)$ of n variables is usually represented by its truth table, of dimension 2^n The number of 1s in the truth table (TT) is called the Hamming weight $w_H(f)$, of the function f.

$w_H(f) = \{X: f(x) = 1, X \in \mathbb{F}_2\}$	(3)

A Boolean function is said to be balanced if $w_H(f) = 2^{n-1}$. Given two Boolean functions $f, g \in B_n$, their Hamming distance is given by $d_H(f, g) = w_H(f \oplus g)$.

$d_H(f, g) = w_H(f x_2 g) = \{X \in \mathbb{F}_2^n / f(X) \neq g(Xx)\}$	(4)

The desirable cryptographic properties of Boolean functions include among others, nonlinearity, correlation immunity, algebraic degree, linear structure, Strict avalanche criterion, Balancedness and resiliency etc. Some of these properties can be best studied using the Walsh transform.

Let $X = (x_1, x_2, \dots, x_n), w = (w_1, w_2, \dots, w_n) \in \mathbb{F}_2^n$.

Definition 2.1 (Walsh Transform) the Walsh transform of an n-variable Boolean function $f$is an integer valued function, $W_f = \mathbb{F}_2^n \rightarrow \mathbb{R}$ defined by

$W_f(w) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+(w.x)}$(5)

where$(w.x) = w_1 x_1 \oplus w_2 x_2 \oplus \dots \oplus w_n x_n$.

The term $W_f(w)$ is called the Walsh coefficient of f at the point w which satisfies the Parseval's equation:

$\sum_{w \in \mathbb{F}_2^n} W_f^2(w) = 2^{2^N}$.

The set of all the Walsh coefficients is referred as the Walsh spectrum of f.

The derivative of a Boolean function f with wrt to a $d_f(a)$ is define by $d_f(a) = f(x) \oplus f(x \oplus a)$. The periodic autocorrelation function of f is a real-valued function defined on all $a \in \mathbb{F}_2^n$ given by

$$C_f(a) = \sum_{x \in \mathbb{F}_2^n} (-1)^{d_{f(a)}} (6)$$

3.Complexity Requirements of Boolean functions for Cryptographic Application

3.1 Nonlinearity

The equivalence of Nonlinearity to the principle of confusion introduced by Claude Elwood Shannon in 1949 [15] allows it to be used as a measure of complexity of Boolean functions and for measuring linear attacks involved in stream and block. These linear attacks are due to the existence of affine approximations of the Boolean functions used in the systems. The Measure of the nonlinearity of the Boolean functions determines the complexity of the system developed, the measure of this nonlinearity could either be algebraic: the degree of the ANF, or functional: the minimal distance from the function to the set of all affine functions.

Definition 3.1 (Nonlinearity). The nonlinearity N_f of a Boolean function is its minimum Hamming distance to the set of all affine functions with n-variables

$$N_f = min_{\ell_a \in A_n} d_H(f, \ell_a) \quad (7)$$

where $A_n \subset B_n$ is the set of all affine functions.

In terms of the Walsh transform

$$\square_{\square} = 2^{\square-1} - \frac{1}{2} \square \square \square_{\square \in \square_2^{\square}} |\square_{\square}(\square)| \quad (8)$$

It is widely reported in literature that $\square_{\square} \leq 2^{\square-1} - 2^{\square/2-1}$

3.2 Correlation Immunity

The concept of correlation immune functions was introduced by Siegenthaler [16], they are primarily designed to resist a correlation attack.

Definition 3.2 A Boolean function $\square$ is called $\square - \square\square$ order correlation immune iff $\square_{\square}(\square) = 0$ for all vectors $\square \in \square_2^{\square}$ such that $1 \leq \square_{\square}(\square) \leq \square$.

A balanced $\square - \square\square$ order correlation immune Boolean function $\square$ is called $\square$-resilient. In other words, the function $\square$ is $\square - \square\square$ order correlation immune if $\square_{\square}(\square) = 0$ for all $1 \leq \square_{\square}(\square) \leq \square$.

3.3 Algebraic Immunity

An annihilator of the function $\square \in \square_{\square}$ is a nonzero function $\square \in \square_{\square}$ such that $\square\ \square = 0$. Given a Boolean function $\square$, the algebraic immunity of $\square$, $\square\square(\square)$is the minimum degree of all annihilators of $\square$or $\square + 1$. As has been reported by [5, 11, 3], $\square\square(\square) \leq [\square/2]$. In order to resist an algebraic attack, the Boolean function $\square(\square)$ should have the property that there is no non-zero Boolean function $\square(\square)$ such that $\square(\square)\square(\square) = \square(\square)\square\ \square\ \square\square(\square)$has a low algebraic degree.

$$\mathcal{AI}(f) = min\{(\deg(g(X)|f(X)g(X) = 0)\} \quad (9)$$

4. Stream Ciphers

Symmetric cryptography is split into block ciphers and stream ciphers. A stream cipher is a symmetric cipher which operates with a time-varying transformation on individual plaintext digits. Stream ciphers can encrypt plaintext messages of variable length. Fig. 2 shows a general structure of a synchronous (keystream is generated independent of the plaintext stream) stream cipher showing both encryption and decryption. The keystream k = (O_1, O_2, …)isusedtoencryptthemessageM to produce the cipher-textC_i.

$$C_i = M_i \oplus O_i \quad (10)$$

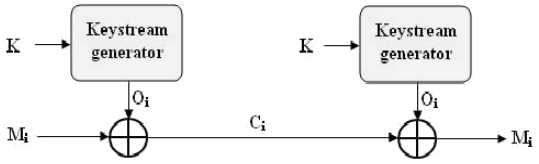


Figure 2: A stream Cipher.

The one-time pad can be thought of as an example - each message uses a portion of the key with length equal to the length of the plaintext message. (Then that portion of the key is never re-used.)

4.1 Construction Using Boolean Functions

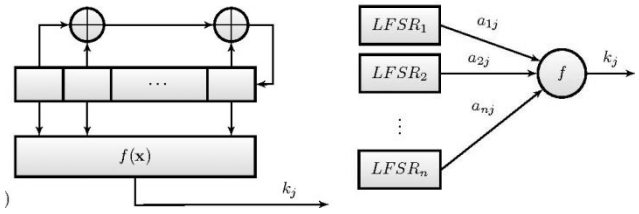
The combination of a key stream generator and an encryption algorithm makes up what is called a stream cipher [13]. The encryption algorithm XORs the plaintext with the key stream. Since the plaintext is of public knowledge, hence, the security of the stream cipher depends on the security of the key stream. The key stream generator (Fig. 3) is considered as a combination of two parts [13], the first part, referred to as the driven part consists of Linear Feedback Shift registers (LFSRs). By design, the operation of the LFSR is linear [9], thus therefore the security of the key stream generator depends on the nonlinear part, which controls the states of the generator [1, 9]. The design of the driven part is relatively simple, since the theory of LFSR is mature, especially that we have a maximum length sequence with good pseudo-randomness. The nonlinear combination part combines the sequences from the driven part into a sequence with good cryptographic properties. The use of Boolean functions in the nonlinear part of the key stream generators has been for quite some times now [12, 14]. The nonlinear Boolean functions used in the generation of the key streams could either be filter functions of combining functions. With filter functions, one LFSR is used as the driven part (Fig.3a), while the combining generator uses several LFSRs as the driven part (Fig. 3b). The corresponding key stream generators are called nonlinear filter sequence generators (see Fig.3a) and nonlinear combination sequence generators (see Fig. 3b).

4.2 Attacks and Required Properties

If we consider the nonlinear combination sequence generator (Fig. 3b), the correlation between the output sequence $\{\square_{\square}\}$ and every input sequence $\{\square_{\square\,\square}\}(1 \leq \square \leq \square)$, enables one to recover the initial states and the feedback function of $LFSR_i$ using statistical methods. This kind of attack is called correlation attack.

Another form of attack peculiar to sequence generators is the linear attack. This attacks sequence of high complexity using a sequence of low complexity. The efficiency of such an attack is proportional to the value of the Walsh transform of the Boolean function $\square_{\square}(\square)$ used.

Figure 3: Key Stream Generators



Consequently, we require a high nonlinearity of the Boolean function to resist linear attacks. In LFSR-based stream ciphers, the performance of Boolean functions against algebraic attack received considerable attention since the year 2003. Boolean functions with big algebraic immunity can resists algebraic attacks to certain extend. However, no matter how high the algebraic immunity of a Boolean function is, it may not resist a fast algebraic attack [5]. Fast algbraic attack is an improvement of algebraic attack.

In the fast algebraic attack, the Boolean function □(□) must not have a low degree multiple. The fast algebraic attack will still be efficient even if there exists a low degree (less than □□(□)) of the function □(□) such that the degree of □(□)□(□) = □(□) is not too big. If the degree of □(□)is □(□ < □/2), then fast algebraic attack can be converted to solve a system of equations with degree less than □. The research in fast algebraic attack shows that for any Boolean function □(□) andintegers □; □ such that □ + □ ≥ □, there exists Boolean function□ such that □(□)□(□) = □(□), with deg(□(□)) ≤ e and deg(□(□ □ □)) ≤ □. So there are no Boolean functions which can totally resist fast algebraic attacks, but we can choose some special Boolean functions which have high complexity against a fast algebraic attack.

Details of how the tow attacks works can be found in [5, 11] and references contained therein. Thus therefore with stream ciphers, the Boolean function used in the keystream generating algorithm should have the following properties corresponding to the kind of attack.

Statistic analysis: The Boolean function should be balanced.
Linear attack: The function used should have high nonlinearity.
Correlation attack: High correlation immunity.
Algebraic attack: High algebraic immunity.

5. Conclusions

Boolean functions are the most important part in symmetric cryptosystems. In this paper, we summarized some major properties of Boolean functions which make them resist to several attacks. One may want to find a Boolean function that holds all the security properties, but a trade-off is certainly necessary. The construction of Boolean functions with certain properties is the main research subject of cryptographic Boolean functions. We may also require new properties because attacks never stop. The quantitative evaluation of Boolean functions regarding security applications and the relation between different properties remain an important research topic.

References

Henry Beker and Fred Piper. Cipher systems: the protection of communications. Northwood Books, 1982.

Claude Carlet. Boolean functions for cryptography and error correcting codes. Boolean models and methods in mathematics, computer science, and engineering, 2:257{397, 2010.

Claude Carlet, Deepak Kumar Dalai, Kishan Chand Gupta, and SubhamoyMaitra. Algebraic immunity for cryptographically significant boolean functions: analysis and construction. IEEE Transactions on Information Theory, 52(7):3105{3121, 2006.

Henry Corrigan-Gibbs, Wendy Mu, Dan Boneh, and Bryan Ford. Ensuring high-quality randomness in

cryptographic key generation. In Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security, pages 685{696. ACM, 2013.
Nicolas T Courtois. Fast algebraic attacks on stream ciphers with linear feedback. In Annual International Cryptology Conference, pages 176{194. Springer, 2003.
Thomas W Cusick and PantelimonStanica. Cryptographic Boolean functions and applications. Pages 7 – 23. Academic Press, 2017.
Cunsheng Ding, Guozhen Xiao, and Weijuan Shan. The stability theory of stream ciphers, volume 561. Springer Science & Business Media, 1991.
Solomon Golomb. On the classification of Boolean functions. IRE transactions on circuit theory, 6(5):176{186, 1959.
Peizhong Lu and Lianzhen Huang. A new correlation attack on LFSR sequences with high error tolerance. In Coding, Cryptography and Combinatorics, pages 67{83. Springer, 2004.
KingaMarton, AlinSuciu, and IosifIgnat. Randomness in digital cryptography: A survey. Romanian Journal of Information Science and Technology, 13(3):219{240, 2010.
Willi Meier, EnesPasalic, and Claude Carlet. Algebraic attacks and decomposition of Boolean functions. In International Conference on the Theory and Applications of Cryptographic Techniques, pages 474{491. Springer, 2004.
Willi Meier and OthmarStaffelbach. Nonlinearity criteria for cryptographic functions. In Workshop on the Theory and Application of Cryptographic Techniques, pages 549{562. Springer, 1989.
Rainer ARueppel. Stream ciphers. In Analysis and Design of Stream Ciphers, pages 5{16. Springer, 1986.
Jennifer Seberry, Xian-Mo Zhang, and YuliangZheng. On constructions and nonlinearity of correlation immune functions. In Workshop on the Theory and Application of Cryptographic Techniques, pages 181{199. Springer, 1993.
Claude Elwood Shannon. Communication in the presence of noise. Proceedings of the IRE, 37(1):10{21, 1949.
Thomas Siegenthaler. Decrypting a class of stream ciphers using ciphertext only. IEEE Transactions on computers, 1(C-34):81{85, 1985.
Nigel Paul Smart et al. Cryptography: an introduction, volume 3. McGraw-Hill New York, 2003.
Douglas R Stinson. Cryptography: theory and practice. Pages 26 – 37, Third edition, CRC press, 2005.
Zhe-Xian Wan. Lectures on finite fields and Galois rings. World Scientific Publishing Com