applied sciences

MDPI

Article

A Secure Random Number Generator with Immunity and Propagation Characteristics for Cryptography Functions

Rahul Saha [1], Ganesan Geetha [1,*], Gulshan Kumar [1], William J. Buchanan [2] and Tai-hoon Kim [3,*]

[1] School of Computer Science and Engineering, Lovely Professional University, Phagwara 144411, Punjab, India; rahul.18818@lpu.co.in (R.S.); gulshan3971@gmail.com (G.K.)
[2] BlockPass ID Lab, Edinburgh Napier University, Edinburgh EH10 5DT, UK; B.Buchanan@napier.ac.uk
[3] Glocal Campus of Konkuk University, 268, Chungwon-daero, Chungju-si 27478, Korea
* Correspondence: geetha@advancedcomputingresearchsociety.org (G.G.); taihoonn@daum.net (T.-h.K.)

Abstract: Cryptographic algorithms and functions should possess some of the important functional requirements such as: non-linearity, resiliency, propagation and immunity. Several previous studies were executed to analyze these characteristics of the cryptographic functions specifically for Boolean and symmetric functions. Randomness is a requirement in present cryptographic algorithms and therefore, Symmetric Random Function Generator (SRFG) has been developed. In this paper, we have analysed SRFG based on propagation feature and immunity. Moreover, NIST recommended statistical suite has been tested on SRFG outputs. The test values show that SRFG possess some of the useful randomness properties for cryptographic applications such as individual frequency in a sequence and block-based frequency, long run of sequences, oscillations from 0 to 1 or vice-versa, patterns of bits, gap bits between two patterns, and overlapping block bits. We also analyze the comparison of SRFG and some existing random number generators. We observe that SRFG is efficient for cryptographic operations in terms of propagation and immunity features.

Keywords: cryptography; random; propagation; symmetric; immunity; function; boolean

Citation: Saha, R.; Geetha, G.; Kumar, G.; Buchanan, W. J.; Kim, T.-h. A Secure Random Number Generator with Immunity and Propagation Characteristics for Cryptography Functions. *Appl. Sci.* **2021**, *11*, 8073. https://doi.org/10.3390/app11178073

Academic Editor: Arcangelo Castiglione

Received: 5 June 2021
Accepted: 5 July 2021
Published: 31 August 2021

1. Introduction

Cryptographic functions [1,2] are an integral part of cryptographic algorithms. The applications of these functions are observed in the round functions of the bock cipher, key generation algorithms, stream ciphers, message digest algorithms and many more [1]. The cryptographic functions must possess some of the important characteristics such as non linearity, symmetricity, resiliency, propagation criterion, immune to correlation etc. Moreover, the introduction to the pseudo random number generator (PRNG) helps to provide randomness in the cipher outputs to increase confusion-diffusion property in the algorithm. Such randomness of the function provides robustness to withstand with correlation attacks [3]. However, PRNGs have also faced different attacks in recent times [4]. Therefore, there is an urge of generating a new random function which can provide the robustness against the attacks of evaluating differential, linear or non-linear cryptanalysis process for understanding the plaintext bits or key bits. In this paper, an analysis is executed on the properties of Symmetric Random Function Generator(SRFG).

Symmetric Boolean functions are very important for cryptography [5]. Their outputs posses sepcial characteristics in cryptographic developments. Hamming distances of these outputs make use of proper correlation features as required. As the desirable properties of a cryptographic function is in objective, we have evaluated the propagation characteristics of the differentiations of SRFG outputs. Moreover, we have also analysed the immunity strength of SRFG: correlation immunity and algebraic immunity.

The organization of the paper is coherences in several sections. Introductory problem statement has been already shown in Section 1. In the upcoming sections, Section 2 reviews

the works in the direction of cryptographic functional properties. Section 3 shows the mathematical model of SRFG. Section 4 describes explains the propagation criterion of SRFG. Section 5 discusses about immunity of the functions. Section 6 analyses the results, shows the statistical interpretaion and validation and, Section 7 provides a logical conclusion.

2. Related Work

The algorithms in cryptography uses various types of cryptographic functions and transformations; these possess different factors which are important for designing such functions [6]. For example, algebraic, random and heuristic contsructions of functions are important in this case. In paper [7], the authors have discussed the propagation properties of Boolean functions. New properties are also identified which have the high strict avalanche criterion. The research work in [8] analyses the inverse permutation on the field component functions. The weights of derivatives of the component functions also use Kloosterman sums. The authors in the paper [9] show the property of aperiodic autocorrelation in Boolean function aspect and define the Aperiodic Propagation Criteria (APC). The work also shows the relation between aperiodic autocorrelation and the first derivative of the function.

The concept of correlation immunity in Boolean functions was introduced by Siegenthaler [10]. Furthermore, this feature of Boolean functions has been considered to be an important characteristics for strong cryptographic algorithms and has been researched with concern as shown in [11–14]. Some of the contemporary research has been done to provide immunity to the functions both as correlation aspect and algebraic aspect. High algebraic immunity is a required factor for cryptographic algorithms to prevent algebraic attacks. Algebraic immunity must have a lower bound failing which functions must not be used in cryptography. Such a lower bound in evaluated in [15]. The relation of algebraic immunity and extended algebraic immunity is researched in [16,17]. The bent functions are also in use for construction of a class of functions in infinity [18]. The authors have considered only odd number of variables. Decomposition of the first-order correlation-immune Boolean functions is researched significantly [19]. Following this, an enumerative encoded Boolean function is designed [20]. In the paper [21] , optimal algebraic immunity construction strategy has been shown using vector spaces and m-sequences. Boolean functions can be presented into two hybrid classes [22]. The magnitude of the inter-class algebraic immunity is maximum. It also prohibits resistance against algebraic attacks with high non-linearity. 1-resilient functions are also in existence. Algebraic immunity on balanced functions has been shown in the papers [23,24]. Vector valued functions over finite field has also experimented for maximum algebraic immunity in [25].

Some of the recent developments in field of random and pseudo-random number generators have been reviewed. For example, the random number generation in [26,27] show the applications in BIST and IoT Applications. The later one is based on chaos and is validated by statistical tests. A pseudo random generator for cryptographic applications has been shown in [28]. Several studies were carried out in this domain for validation of random numbers and generation of random numbers as shown in [29–33]. Such studies show that random numbers are in real need for various applications and their design factors are also very important.

Symmetric Random Function Generator (SRFG) is random bit generator that produces the symmetric and balanced outputs [34]. The authors have analysed the nonlinearity, resiliency, balancedness properties of SRFG. In our present work, we have extended the feature analsyis of SRFG with the explanation for propagation and immunity characteristics, security analysis and statistical testing. The main contribution of the presented research work are:

1. The analysis of propagation and immunity characteristics of SRFG.
2. Statistical testing on SRFG output-based NIST recommendations.
3. Security analysis for SRFG as a random number generator.

3. Symmetric Random Function Generator (SRFG)

The mathematical model of Symmetric Random Function Generator (SRFG) is shown in [34]. It produces the balanced and symmetric outputs in consideration of number of 1's and number of 0's in the output string with variable input patterns. In this section we have mentioned some important mathematical expression as shown in [34] to make a clear understanding of propagation and immunity characteristic in next sections. The generalized mathematical expression for SRFG is given as:

$$f() = \otimes f_i^L \tag{1}$$

where i is number of gates (here, AND, OR, NOT and XOR GATEs are used with randomized selection) used in SRFG; L represents the expression length. Expression length is defined as the number of the combined terms used in f and $\otimes$ symbolizes the random combination. We show the logical model of SRFG in Figure 1.

As randomness is the main criteria for a random number generator [35], the SRFG generalized equation can be further granulated with N input variables' following a random selection as shown in Equation (2).

$$f(V_1, V_2 \ldots, V_N) = \otimes f_i^L \left[rand(V_1, V_2 \ldots, V_N) \right] \tag{2}$$

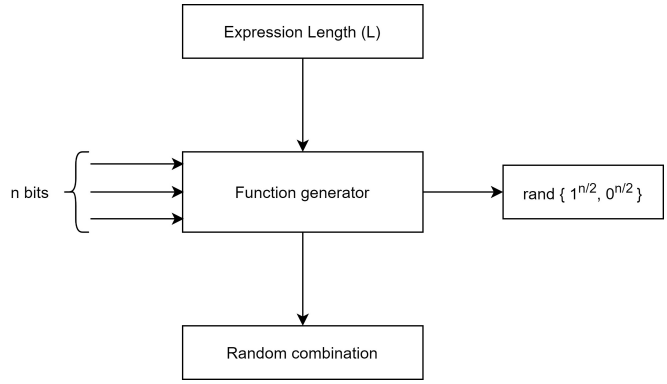


Figure 1. Logical block structure of SRFG.

The expanded structure and chaining of functions is shown in Figure 2.

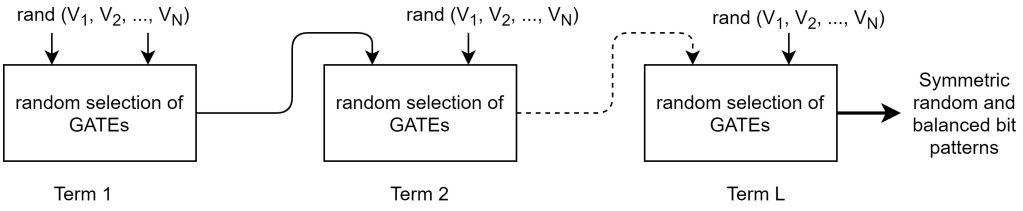


Figure 2. Chaining of randomization.

As per the shown model of SRFG in the literature, it uses a finite field $F_2^{0,1}$ and $\otimes$ denoted an operation on the field. SRFG inputs N variables, each of n bit vector $V = v_1, v_2, \ldots, v_n$. As the values in the vector is either 1 or 0, V_i is a binary vector.

Furthermore, SRFG embodies a set of functions it generates as B_N is. All the functions map the elements from F_2^N into F_2 where $F_2^N = \{(V_1, V_2, \ldots, V_N) | V_i \in F_2\}$. The output of SRFG is a vector which is a combination of 2^N with N variables. This vector is comprised

of all the values $f(y), y \in F_2^N$ as the variables are randomly selected and represented as polynomial form of Algebraic Normal Form (ANF) [36]. It is mathematically interpreted as:

$$f(V_1, V_2, ..., V_N) = \otimes \lambda_u \left(\prod_{i=1}^{N} rand(V_i)^{u_i} \right)^L, \quad \lambda_u \in F_2,\ u \in F_2^N \text{ and } L \in \mathbb{Z} \tag{3}$$

with,

$$\lambda_u = \otimes f(v),\ v \preceq u\ ,\ \forall\ V_i = \{v_{i_1}, v_{i_2}, ..., v_{i_n}\} \tag{4}$$

where

$$(v_{i_1}, v_{i_2}, ..., v_{i_n}) \preceq (u_1, u_2, ..., u_n) \iff \forall i, j, v_{i_j} \leq u_i \tag{5}$$

In coding theory and in cryptography, ANF considers a Boolean function as a multivariate polynomial. As the N inputs contain values in F_2, modulo $X^2 + X$ must be considered. Therefore, this polynomial has degree at most 1 in each input variable following that any monomial of this polynomial is the product of some input variables. For any $u \in F_2^N$, $(V_i)^{u_i}$ defines monomial as: $\left(\prod_{i=1}^{N} (V_i)^{u_i} \right)$. Extending this monomial for L terms and random basis we obtain $\left(\prod_{i=1}^{N} (V_i)^{u_i} \right)^L$.The proofs are given in [36].

In SRFG, the outputs and input mapping correspond to a function $g : 0, 1, \ldots, n \to F_2$ such that $\forall x \in F_2^N$, $f(x) = g(w(x))$. Following this, Equation (3) is reconstructed as in Equation (6).

$$f(V_1, V_2, ..., V_N) = \otimes \lambda_f\ (j) \otimes \left(\prod_{i=1}^{N} rand(V_i)^{u_i} \right)^L \tag{6}$$

$$= \otimes \lambda_f\ (j) X_{j,N} \tag{7}$$

where $\lambda_f(j), u \in F_2^N$ and $L \in \mathbb{Z}$, $j = 1, ..., N$. $X_{j,N}$ is the elementary polynomial of degree j with N variables. $\lambda(f) = \lambda_f(0), \lambda_f(1), ..., \lambda_f(N)$ known as a simplified vector.

4. Propagation Criterion of SRFG

The derivatives of the cryptographic properties help in determining the propagation characteristics. All derivatives of the combined functions that output from SRFG are linearly equivalent. This is due to the equal number of 0s and 1s in the outputs equating with a hamming weight of $\frac{n}{2}$. This is fixed for all the outputs of SRFG. The function f satisfies the propagation criterion of degree k and order m if any affine function is obtained from f with constant m input bits.

Let $f \in B_N$ and let $x, y \in F_2^N$ be such that $w(x) = w(y) = \frac{n}{2}$. Then, $D_x f$ and $D_y f$ are linearly equivalent. This signifies a linear permutation μ of F_2^N such that $D_x f = D_y f \circ \mu$, where $\circ$ is composite function. The permutation μ exists on $1, 2, ..., N$ such that $y = \mu(x)$. Since, f is symmetric and balanced, we can have,

$$\begin{aligned} D_y f(\mu(a)) &= f(\mu(a)) \boxplus f(\mu(a) + y) \\ &= f(a) \boxplus f(\mu(a) + \mu(x)) \\ &= f(a) \boxplus f(\mu(a + x)) \\ &= f(a) \boxplus f(a + x) \\ &= D_x f(a) \end{aligned} \tag{8}$$

where $\boxplus$ denotes addition over F_2.

Let k be an integer, $1 \leq k \leq n - 1$, $\bar{V}_i = (v_{i_1}, v_{i_2}, ..., v_{i_{n-k}})$ and $\epsilon_k = v_{n-k+1} + ... + v_n$. Then the restriction of $D_{\epsilon_k} f$ to all affine subspaces $y + V, y \in (v_{i_1}, v_{i_2}, ..., v_{i_{n-k}})$ is given by:

$$g_y : V \to F_2 \tag{9}$$

$$x \mapsto D_{\epsilon_k} f(a+y) \tag{10}$$

The differential functions obtained from SRFG are also symmetric functions of $(n-k)$ variables and weight is $\frac{n}{2}$. Moreover, simplified value vectors and ANF vectors for those differential symmetric are given for all $0 \leq i \leq n-k$ by

$$g_{g_y}(i) = g(i + w(y)) \boxplus g(i + k - w(y)) \tag{11}$$

$$\lambda_{g_y}(i) = \otimes_{j \preceq k - wt(y)} \otimes_{j \preceq w(y)} \lambda_f(i+j) \boxplus \otimes \lambda_f(i+j) \tag{12}$$

Let $y \in \bar{V}_i$. For any $z = a + y$ with $a \in \bar{V}_i$, SRFG have the following relation.

$$w(z) = w(a) + w(y) \tag{13}$$

$$w(z + \epsilon_k) = w(a) + w(y + \epsilon_k) = w(a) + k - w(y) \tag{14}$$

Thus, $\forall\ a \in V$,

$$\begin{aligned} D_{\epsilon_k} f(a+y) &= f(a+b) \boxplus f(a + \epsilon_k + y) \\ &= w(a) + w(y + \epsilon_k) \\ &= w(a) + k - w(y) \\ &= g(w(a) + w(y)) \boxplus (w(a) + k - w(y)) \end{aligned} \tag{15}$$

Equation (15) signifies g_{g_y} also follows the symmetric property. This infers that the partial derivatives of f are also propagated with the propagation features. To calculate simplified ANF vector of g_{g_y} , we have decomposed the ANF of f as given below.

$$f(a+b) = \otimes_{u \in F_2^{n-k}} \otimes_{v \in F_2^k} \lambda_{u,v} \prod_{i=1}^{n-k} a_i^{u_i} \prod_{j=n-k+1}^{n-k} b_j^{v_j}, \forall (a,b) \in (V, \bar{V}) \tag{16}$$

Then, for any $y \in \bar{V}$ and $a \in V$, we have,

$$\begin{aligned} & g_{g_y}(a) = D_{\epsilon_k} f(a+y) \\ &= \otimes_{u \in F_2^{n-k}} \otimes_{v \in F_2^k} \lambda_{u,v} \prod_{i=1}^{n-k} a_i^{u_i} \times \prod_{i=1}^{k} (y_i \boxplus 1)^{v_i} \boxplus \prod_{i=1}^{k} y_i^{v_i} \end{aligned} \tag{17}$$

In Equation (16), $f(a+b)$ is used to show that if any biased bit vector b is included in SRFG function f, it does not have any effect on output to disrupt the randomness features. $\prod_{i=1}^{n-k} a_i^{u_i}$ and $\prod_{j=n-k+1}^{n-k} b_j^{v_j}$ are used for selection of random bit patterns from the set of variables. In Equations (11)–(15), $g_{g_y}(a)$ deals with the derivatives showing that in the presence of any other bit vector y, propagation feature is still preserved.

5. Immunity Feature of SRFG

Now, let's discuss about the correlation immunity characteristics exhibited by the function generator's outputs. Considering each of the N input variable V_i as n bit binary vector $V_i = \{v_1, v_2, \ldots, v_n\}, i = 1, 2, ..., N$ for the combined symmetric and balanced function f, f is correlation immune if the following condition satisfies:

$$Prob(f = v_i) = \frac{1}{2}, 1 \leq i \leq n \tag{18}$$

The set of all correlation immune functions of N variables of n bits each is denoted by CI_N^n. Furthermore, the weight of correlation immune function f of the generator is given by:

$$a = w(f) = \frac{n}{2}, f \in CI_N^n \tag{19}$$

Let f^u and f^l be the upper and lower halves of equal length $\frac{n}{2}$ for the function generator's outputs as shown in Figure 3. As, $f \in CI_N^n$, $w(f^u) = w(f^l) = \frac{n}{4}$. If there are k places out of $\frac{n}{4}$ 1's in the f^u where the corresponding positions in reverse of f^l, denoted as $(f^l)^r$, do not match. Therefore, the number of bits match with respect to 1 for the function is given as:

$$M_1(f^u, (f^l)^r) = \frac{n}{4} - k \tag{20}$$

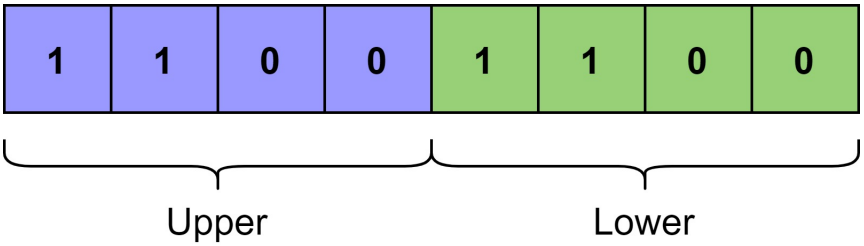


Figure 3. Concept of lower and upper halves of bitstring.

Following Equation (20), we can also say that there are k places out of $\frac{n}{4}$ 1's in the f^u where the corresponding positions in $(f^l)^r$ do not match. Therefore, the number of bits match with respect to 0 for the function is given as:

$$M_0(f^u, (f^l)^r) = \frac{n}{4} - k \tag{21}$$

Hence, we can write:

$$\begin{aligned} M(f_c, (f)^r) &= 2M(f^u, (f^l)^r) \\ &= 2\left(\frac{n}{4} - k + \frac{n}{4} - k\right) = n - 4k \end{aligned} \tag{22}$$

The correlation immune functions with the same values of $M(f, (f)^r)$ form an equivalence class.

Proposition 1: Let $f \in CI_N^n$ and $M(f, (f)^r) = m$. Then $\forall$ $M_0(f, (f)^r)$ and $M_1(f, (f)^r)$,

$$min[M_0(f, (f)^r) - M_1(f, (f)^r)] = min[m] \mapsto 0 \tag{23}$$

Apart from the correlation immunity, algebraic immunity is also a requirement for cryptographic algorithms. Algebraic immunity also is related with the annihilator of a function [37]. This property helps the algorithm to prevent algebraic attacks [38,39] against the cryptographic algorithms.

We use the annihilators here. If $f \in B_N$, any function of the set $A(f) = \{g \in B_N | gf = 0\}$ is the annihilator of the function f. The algebraic immunity of f is denoted by $AI(f)$. It is defined as the minimum degree of all the nonzero annihilators of f or f_1. The value of $AI(f)$ is given as:

$$AI(f_c) = min[deg(g) | g \neq 0, g \in A(f) \cup A(f_1)] \tag{24}$$

The idea is that for a given function f on N-variables, a reduced set of homogeneous linear equations is required by solving which one can decide whether there exist annihilators of f at a specific degree [40]. The experimented value for good designs of functions must possess the f or f_1 must not have any annihilator of degree more than $\frac{n}{2}$. SRFG exhibits this feature as the degree of SRFG functions is $\frac{n}{2}$. as they are balanced. As the SRGF outputs the symmetric function which are balanced and therefore minimum degree is always $\frac{n}{2}$. Therefore, the algebraic immunity of the outputs from SRGF is always $\frac{n}{2}$ which is always optimal.

6. Results

We have executed an experiment for the SRFG to analyze the above mentioned properties. To evaluate these properties for SRFG and its output functions, we have implemented the model using concerning for two variable metrics: number of bits n and number of expressions L. The other parameters and metrics used for the experiments are summarized in Table 1.

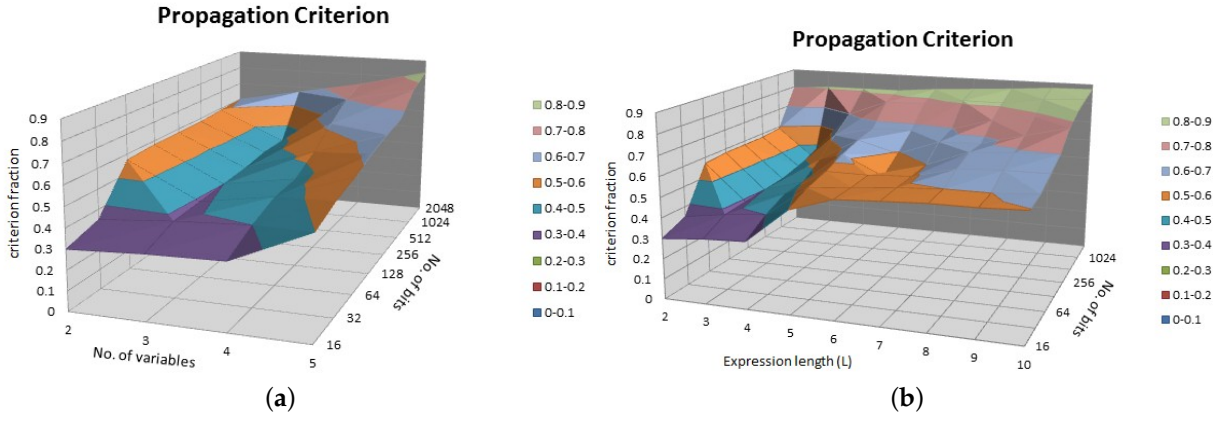
Table 1. Metric set-up.

Metrics	Values
No. of variables (N)	2 to 5
No. of bits (n)	16,32, 64, 128, 256, 512, 1024 and 2048
No. of Expressions (L)	2 to 10
Boolean functions	AND, XOR, NOT, OR
Sample size	800
Sample technique	Random

6.1. Performance of SRFG

The evaluation for the propagation criterion was measured with the introduced metric of criterion fraction. Criterion fraction is defined as: $\frac{m}{k}$, where m is the number of bits in the input variable kept constant to get the propagation criterion of degree k. For the SRFG function generator as the output functions are balanced always, the value of $k = \frac{n}{2}$ and maximum number of bits we can keep constant is also $\frac{n}{2}$. These values give the upper bound of criterion fraction as 1.

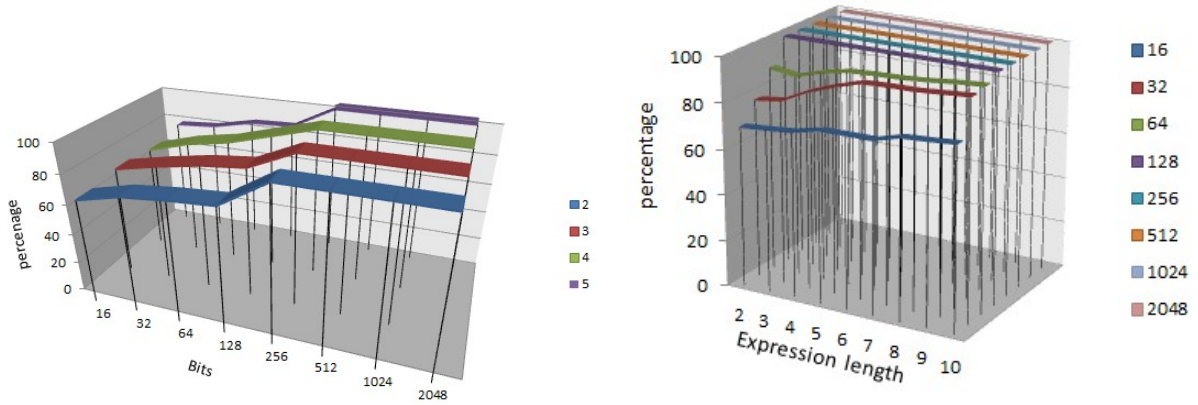
In Figure 4, we showed the results of the propagation criterion for SRFG. Figure 4a shows the result by varying the number of variables and number of bits of each variable. Similarly, Figure 4b shows the result by varying the number of expression length and number of bits of each variable. It shows that more number of variables are providing more propagation; however, with the increasing number of bits propagation follows a steady output of 0.8 approximately. In both the cases, the results achieve more than 80% propagation criterion effect which reflects the strictly avalanche effect.



(**a**) (**b**)

Figure 4. Propagation criterion. (**a**) Varying number of bits and variables; (**b**) Varying number of bits and expression length.

The correlation immunity characteristics were plotted in Figure 5. Figure 5a shows the result by varying the bits and number of variables from 2 to 5. It notifies that increasing number of bits is able to generate more immunity. Figure 5b shows the result by varying the bits from 16 to 2048 and expression length from 2 to 10. We have noticed a new feature in both the cases that irrespective of the expression length and number of variables, SRFG is capable of producing 100% correlation immune functions with and after 128 bits. This makes the SRFG efficient and suitable for cryptographic algorithms.



(**a**) (**b**)

Figure 5. Correlation Immunity. (**a**) Correlation immunity with varying bits and input variables; (**b**) Correlation immunity with varying bits and expression length%.

The algebraic immunity of the SRFG generated functions are always at $\frac{n}{2}$ irrespective of the number of bits and number of expression length and therefore these parameters is not shown graphically explicitly.

6.2. Comparative Analysis

We chose some recent works from the literature for comparing the results and to validate the randomness efficiency of SRFG. The algorithms described in [26,27,29,31–33] exhibit true randomness and therefore have been considered for the comparison with SRFG. Another recent algorithm depicted in [18] is also considered for comparison due to its related features. The comparison results shown in Table 2 notify the order of the parameters considered for the evaluation. Percentage calculation in the table is based on 500 outputs of bit sequences from the random number generators.

Table 2. Comparative feature analysis.

	Propagation Criterion	**Correlation Immunity**	**Algebraic Immunity**
SRFG	$\frac{n}{2}$	100%	$\frac{n}{2}$
Wang et al. [18]	$\sqrt{\frac{n}{2}} - 1$	57.63%	0
Kumar et al. [26]	$\frac{n}{4}$	87.50%	0
Hsueh et al. [27]	$\frac{n}{4}$	85.33%	0
Vigna [29]	$\log n$	76.67%	0
Kaya [31]	$\frac{n}{2}$	92.30%	$\frac{n}{2}$
Stanchieri et al. [32]	$\log n$	76.67%	0
Martirosyan et al. [33]	$\frac{n}{2}$	94.33%	0

Table 2 shows the fact that SRFG possess the three features significantly. 100% correlation immunity is possible because of balanced functions. The symmetric and balanced function in SRFG is therefore efficient for cryptographic primitives.

6.3. Statistical Analysis

The validation of the randomness has been executed by the test suite suggested by the NIST in the NIST 800-r1 document [41]. To perform the tests the hypothesis has been set up for all the tests as:

Hypothesis 1. *(null hypothesis): SRFG output sequences are significant for randomness.*

Hypothesis 2. *(alternate hypothesis): SRFG output sequences are non-significant for randomness.*

For each of the applied tests, a choice or end is taken that acknowledges or dismisses the invalid theory which implies whether the SRFG is (or isn't) ready to deliver randomness features, in light of the grouping that was created. For each test, an applicable randomness measurement is chosen and used to decide the value of acceptance or rejection of the invalid speculation. A test measurement esteem (p-value) is figured on the information or arrangement of bits created by the SRFG. Practically, the explanation that factual theory testing works is that the reference appropriation and the basic worth are reliant on and created under a speculative suspicion of irregularity. In the event that the arbitrariness supposition that is, truth be told, valid for the current information, at that point the subsequent determined test measurement esteem on the information will have an extremely low likelihood (e.g., 0.01) of surpassing the basic worth. This estimation of 0.01 is likewise known as level of criticalness or level of significance. In the event that p-value is more noteworthy than the degree of noteworthiness, we can acknowledge the invalid theory. The outline of the p-values of the above said tests is given in Table 3. We can observe that in all the above tests, the p-values of the tests are greater than 0.01, the significance level of the tests. Therefore, the null hypothesis is accepted. This signifies that the SRFG has passed all the tests as per the recommendations by NIST test suite and the SRFG provides randomness in true significance.

Table 3. p-values of statistical tests on SRFG.

	Monobit Test	**Frequency Test within a Block**	**Runs Test**	**Test for Longest Run in the Block**	**Binary Matrix Rank Test**
Test on SRFG and their p-values	1.00	1.00	0.723	0.1933	0.5320
	Spectral test	Non overlapping template matching test	Overlapping template matching test	Maurer's test	Linear complexity test
	0.300	0.300	0.280	0.777	Applicable only for LFSR
	Serial test	Approximate entropy test	Cumulative sum test	Random excursions test	Random excursions variant test
	NA as per NIST recommendation	0.2770	0.433	0.777	0.777

SRFG is quite an interesting random number generator that possess all the required features of being used for cryptographic derivations with randomness features. The statistical test suite also validates the same. It can also be considered to be a post processing method for any other random number generators to provide immunity and eliminating bias and correlations. Furthermore, to validate the tests proportion of sequences passing, a test and uniformity was evaluated as per the NIST standards [41]. The formula shown in the document to calculate the confidence interval level is used here. The confidence interval becomes:

$$\hat{p} \pm 3\sqrt{\frac{\hat{p}(1-\hat{p})}{m}} = 0.99 \pm 3\sqrt{\frac{0.99(1-0.99)}{800}} = 0.99 \pm 0.01055 \quad (25)$$

where $\hat{p} = 1 - \alpha$, α is the significance level (0.01) and m is the number of samples of bit sequences which is 800 in the experimented process. The Equation (25) suggests that the proportion of the sequences under test should be more than 0.9794466. Out of 800 random

samples tested, 799 samples have passed the tests of significance levels providing p-values greater than 0.01 and thus, the proportion becomes $799 \setminus 800 = 0.99875$ which is more than the confidence interval. Hence, SRFG is validated in proportioning the pass sequences to exhibit random features. The uniformity of the p-values is also checked. Following the Goodness of Fit Distributional test as formulated in NIST document [41], the $p\text{-}value_T$ for SRFG is measured as 0.001437 which is more than 0.0001. Hence, it is validated that the p-values are uniformly distributed. The distribution uniformity of the p-values with 10 intervals and corresponding frequencies of p-values are shown in Figure 6.

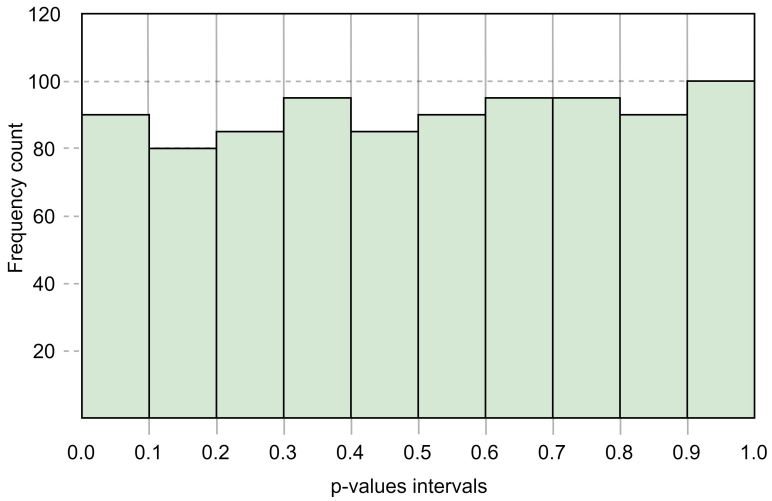


Figure 6. Distribution of p-values.

6.4. Security Analysis

Generally, random number generators are a great help in key management of cryptosystems. Forward secrecy and backward secrecy are two important features that the random number generators should have to be used for key processing. Forward security ensures that any attacker who knows a sequential subset of old bit patterns is unable to derive the subsequent bit patterns. Backward security is defined with the assurance that an attacker with the knowledge of contiguous subset of bit patterns is unable to trace back the preceding bit patterns.

Let us assume two contiguous bit patterns as B_1 and B_2 each of n number of bits. As per the propagation criteria, at least $\frac{n}{2}$ bits are changed from an initial bit pattern B_0 to B_1 and $\frac{n}{2}$ bits from B_1 to B_2. With the increasing number of iterations, the change of bits also increases. The maximum probability that a bit pattern of n bits can be derived from B_1 and B_2 is calculated as:

$P([B_1 : B_2] \rightarrow B_3) = \frac{(n-r)!}{r!(n/2)!}$, where r is the difference of bits in two contiguous bit patterns. For large number of bits and more differences in bit patterns $P([B_1 : B_2] \rightarrow B_3) \rightarrow 0$. It signifies that SRFG is able to provide forward security.

Similarly, if an attacker knows bit pattern B_N and B_{N+1} and wants to trace B_{N-i} bit pattern with a random bit difference of r, the probability that the bit pattern is revealed is:

$$P(B_{N-i} \leftarrow [B_N, B_{N+1}]) = \frac{2^n}{n!.ir.(n-r)!}. \tag{26}$$

Here, we assume that the attacker tries with i_th sequence assuming that each sequence has bit difference r. Therefore, overall, bit difference becomes ir. With large number of bit differences between two contiguous bit patterns, the probability of discovering any previous bit pattern eventually becomes 0 and thus, SRFG preserves backward security.

For any random number generator, it is very important in cryptography to be immune against any distinguishing attack. Such an attack cryptanalyses on data encrypted or output by the system and distinguish it from random data. The correlation immunity and

algebraic immunity provides strength to SRFG on this point. The statistical validation also supports SRFG's indistinguishable property irrespective of inputs. For example: let us consider, E is an encrypted output from SRFG and S is a random bit pattern both of n bits. By the immunity property, SRFG develops a difference of difference of $\frac{n}{2}$ bits propagated from initial difference. Therefore, the probability of distinguishing attack is:

$$P(D) = \frac{2^{(n/2)}}{n!} \rightarrow 0 \quad with\ large\ n \tag{27}$$

Therefore, SRFG is able to provide security parameters significantly and robust against cryptanalysis attacks; thus, efficient for cryptographic operations.

7. Conclusions

Several studies were executed to identify the different valuable features of cryptographic functions. Randomness is one of the important characteristics which is in demand for various security operations. Many random number generators have been developed so far and SRFG is one of them. In the present work, we analysed the effect of randomness for SRFG outputs based on propagation characteristics and immunity features. The experimented results confirm the fact that the symmetric and balanced outputs of SRFG provide more than 85% of propagation on average with $\frac{n}{2}$ bits and 10% correlation immunity which is significantly better than some of the recent works in this direction. SRFG is tested based on the statistical test suite recommended by NIST which validates the randomness of the model. Moreover, security analysis shows the robustness of SRFG against certain types of attacks. Therefore, SRFG is well suited for cryptographic functions, exhibits its efficiency in designing security algorithms and opens up a new dimension of functions for cryptographic research.

Author Contributions: R.S. derived the conceived the idea and analyzed the data. He also wrote the manuscript in consultation with G.K., W.J.B. and T.-h.K.; G.G. supervised the work. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Stallings, W. Cryptography and Network Security: Principles and Practices. *Cryptogr. Netw. Secur.* **2005**. [CrossRef]
2. Cusick, T.W.; Stănică, P. *Cryptographic Boolean Functions and Applications*, 2nd ed.; Academic Press: Cambridge, MA, USA, 2017.
3. Chepyzhov V.; Smeets B. On a fast correlation attack on certain stream ciphers. *Lect. Notes Comput. Sci.* **1991**, *547*, 176–185.
4. Kelsey, J.; Schneier, B.; Wagner, D.; Hall, C. Cryptanalytic Attacks on Pseudorandom Number Generators. In *International Workshop on Fast Software Encryption 1998 Mar 23*; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 1998; Volume 1372, pp. 168–188.
5. Cunkle, C.H. Symmetric Boolean Functions. *Am. Math. Mon.* **1963**, *70*, 833–836. [CrossRef]
6. Picek, S.; Jakobovic, D.; Miller, J.F.; Batina, L.; Cupic, M. Cryptographic Boolean functions: One output, many design criteria. *Appl. Soft Comput. J.* **2016**, *40*, 635–653. [CrossRef]
7. Preneel, B.; Leekwijck, W.V.; Linden, L.V. Propagation Characteristics of Boolean Functions. *Adv. Cryptol. Eurocrypt* **1990**, *473*, 161–173.
8. Charpin, P.; Helleseth, T.; Zinoviev, V.Propagation characteristics of $X \mapsto X^{-1}$ and Kloosterman sums. *Finite Fields Their Appl.* **2007**, *13*, 366–381. [CrossRef]
9. Danielsen, L.E.; Gulliver, T.A.; Parker, M.G. Aperiodic Propagation Criteria for Boolean functions. *Inf. Comput.* **2006**, *204*, 741–770. [CrossRef]
10. Siegenthaler, T. Correlation-immunity of nonlinear combining functions for cryptographic applications (Corresp.). *IEEE Trans. Inf. Theory* **1984**, *30*, 776–780. [CrossRef]
11. Mitchell, C. Enumerating Boolean functions of cryptographic significance. *J. Cryptol.* **1990**, *2*, 155–170. [CrossRef]

12. Yang, Y.X.; Guo, B. Further enumerating Boolean functions of cryptographic significance. *J. Cryptol.* **1995**, *8*, 115–122.
13. Park, S.M.; Lee, S.; Sung, S.H.; Kim, K. Improving bounds for the number of correlation immune Boolean functions. *Inf. Process. Lett.* **1997**, *61*, 209–212. [CrossRef]
14. Hebisz T.; Koscielny, C. A method of Constructing Symmetric-key Block Cryptosystem Resistant to Manipulations on Ciphertext. *Bull. Pol. Acad. Sci. Tech. Sci.* **2002**, *50*, 375–387.
15. Xu, L.Q.; Chen, H. Some results on the algebraic immunity of Boolean functions. *J. China Univ. Posts Telecommun.* **2011**, *18*, 102–105. [CrossRef]
16. Xiong, X.; Wei, A.; Yang, Z. Analysis of Extended Algebraic Immunity of Boolean Functions. *IERI Procedia* **2012**, *2*, 383–388. [CrossRef]
17. Zhang, P.; Dong, D.; Fu, S.; Li, C. New constructions of even-variable rotation symmetric Boolean functions with maximum algebraic immunity. *Math. Comput. Model.* **2012**, *55*, 828–836. [CrossRef]
18. Wang, Q.; Tan, C.H. A new method to construct Boolean functions with good cryptographic properties. *Inf. Process. Lett.* **2013**, *113*, 567–571. [CrossRef]
19. Bars, J.-M.L.; Viola, A. Equivalence classes of Boolean Functions for first-order correlation. *IEEE Trans. Inf. Theory* **2010**, *56*, 1247–1261. [CrossRef]
20. Carrasco, N.; Le Bars, J.M.; Viola, A. Enumerative encoding of correlation-immune Boolean functions. *Theor. Comput. Sci.* **2013**, *487*, 23–36. [CrossRef]
21. Zhang J.; Wen Q.Y. On the construction of odd-variable boolean functions with optimal algebraic immunity. *J. China Univ. Posts Telecommun.* **2013**, *20*, 73–77. [CrossRef]
22. Ahmed Khan, M.; Özbudak, F. Hybrid classes of balanced Boolean functions with good cryptographic properties. *Inf. Sci.* **2014**, *273*, 319–328. [CrossRef]
23. Wang, Q.; Tan, C.H. Balanced Boolean functions with optimum algebraic degree, optimum algebraic immunity and very high nonlinearity. *Discret. Appl. Math.* **2014**, *167*, 25–32. [CrossRef]
24. Sarkar, P.; Maitra, S. Balancedness and correlation immunity of symmetric Boolean functions. *Discret. Math.* **2007**, *307*, 2351–2358. [CrossRef]
25. Zhenhua, L.; Jie, Z.; Qiaoyan, W. Algebraic immunities of vector-valued functions over finite fields. *J. China Univ. Posts Telecommun.* **2015**, *22*, 16–21. [CrossRef]
26. Kumar, G.S.; Saminadan, V. Fuzzy logic based Truly Random number generator for high-speed BIST applications. *Microprocess. Microsyst.* **2019**, *69*, 188–197. [CrossRef]
27. Hsueh, J.-C.; Chen, V.H.-C. An ultra-low voltage chaos-based true random number generator for IoT applications. *Microelectron. J.* **2019**, *87*, 55–64. [CrossRef]
28. Ayubi, P.; Setayeshi, S.; Rahmani, A.M. Deterministic chaos game: A new fractal based pseudo-random number generator and its cryptographic application. *J. Inf. Secur. Appl.* **2020**, *52*, 102472. [CrossRef]
29. Vigna, S. On the probability of overlap of random subsequences of pseudorandom number generators. *Inf. Process. Lett.* **2020**, *158*, 105939. [CrossRef]
30. Kolonko, M.; Gu, F.; Wu, Z. Improving the statistical quality of random number generators by applying a simple ratio transformation. *Math. Comput. Simul.* **2019**, *157*, 130–142. [CrossRef]
31. Kaya, T. Memristor and Trivium-based true random number generator. *Phys. Stat. Mech. Appl.* **2020**, *542*, 124071. [CrossRef]
32. Stanchieri, G.D.P.; Marcellis, A.D.; Palange, E.; Faccio, M. A true random number generator architecture based on a reduced number of FPGA primitives. *AEU Int. J. Electron. Commun.* **2019**, *105*, 15–23. [CrossRef]
33. Martirosyan, N.; Savvidy, K.; Savvidy, G. Spectral test of the MIXMAX random number generators. *Chaos Solitons Fractals* **2019**, *118*, 242–248. [CrossRef]
34. Saha, R.; Geetha, G. Symmetric random function generator (SRFG): A novel cryptographic primitive for designing fast and robust algorithms. *Chaos Solitons Fractals* **2017**, *104*, 371–377. [CrossRef]
35. Nisan, N.; Wigderson, A. Hardness vs randomness. *J. Comput. Syst. Sci.* **1994**, *49*, 149–167. [CrossRef]
36. Canteaut, A. Lecture Notes on Cryptographic Boolean Functions. 2016. Available online: https://www.rocq.inria.fr/secret/Anne.Canteaut/ (accessed on 16 February 2021)
37. De Oliveira, O.R.B. An Alternative Method for the Undetermined Coefficients and the Annihilator Methods. *arXiv* **2011**, arXiv:abs/1110.4425.
38. Armknecht, F. Improving Fast Algebraic Attacks. In *Fast Software Encryption, Proceedings of the 11th International Workshop, FSE 2004, Delhi, India, 5–7 February 2004*; Springer: Berlin/Heidelberg, Germany, 2004; Volume 3017, pp. 65–82
39. Courtois, N.; Meier W. Algebraic attacks on stream ciphers with linear feedback. In *Advances in Cryptology: Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT'03), LNCS 2656, Warsaw, Poland, 4–8 May 2003*; Springer, Berlin, Heidelberg, 2003; pp. 345–359.
40. Dalai, D.K.; Maitra, S. Construction of Rotation Symmetric Boolean Functions with optimal Algebraic Immunity. *Comput. Sist.* **2009**, *12*, 297–321.
41. Rukhin, A.; Soto, J.; Nechvatal, J.; Smid, M.; Barker, E.; Leigh, S.; Levenson, M.; Vangel, M.; Banks, D.; Heckert, A.; et al. *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*; NIST Special Publication 800-22 Revision 1a; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2010.