Chaos, Solitons and Fractals 104 (2017) 371–377

Contents lists available at ScienceDirect

Chaos, Solitons and Fractals

Nonlinear Science, and Nonequilibrium and Complex Phenomena

journal homepage: www.elsevier.com/locate/chaos

Symmetric random function generator (SRFG): A novel cryptographic primitive for designing fast and robust algorithms

Rahul Saha[a,*], Geetha G[b]

[a] Research Scholar, School of Computer Science and Engineering, Lovely Professional University, India
[b] Professor and Associate Dean, Division of Research and Development, Lovely Professional University, India

ARTICLE INFO

Article history:
Received 4 March 2017
Revised 3 July 2017
Accepted 22 August 2017

Keywords:
Randomness
Resiliency
Symmetric
Balanced
Non linearity

ABSTRACT

Cryptanalysis analyses various combinations among plaintexts, ciphertexts and random keys; even using differential methods or analog methods, the attackers can interpret the keys depending upon the operations in the round functions or any subset of the algorithm. The previous research emphasizes on creation of different cryptographic functions, however the randomness of such functions has not been researched significantly so far. In this paper, we have shown a random function generator which can be used for any cryptographic algorithm. This generator outputs the combination of functions in random and cannot be traced back due its randomness. The objective of our research work is not to identify a particular boolean function that is balanced or symmetric based on its input variables, our proposed work provides a random combination of generic boolean functions as used in MD5 or SHA series, block cipher round functions and stream ciphers. Moreover, the random selection of input variables for a particular function also makes it desirable for cryptographic function modules. The results of our experimentation show that the functions generated by the proposed generator provide a good non-linearity, resiliency and balanced effect.

1. Introduction

Cryptographic algorithms [1] depend on the internal structure of the algorithms and their corresponding effect of the boolean functions used in the cryptographic functions [2]. Along with basic gates such as AND, OR, NOT, XOR, NOR, NAND used in the algorithms, researchers also have shown to have a specialized Boolean function that exhibits the symmetric property. The generic Boolean functions create the basic platform of generating any cryptographic algorithm. However, the technology progress of the attackers has urged a need of introducing randomness in the function generators. This would help against the attacks which evaluate the pattern of Boolean functions in an algorithm to get into the identification process of the key bits or plaintext bits by reverse engineering [3]. In this paper, therefore, we have shown such a random function generator that will provide the output as a combination of basic universal gates. The unique feature of this function generator is that it provides the output in symmetric way and also the number of 1's and 0's in the output is equal.

Symmetric Boolean functions [4] are distinguished by their outputs that only depend on the Hamming weights of their inputs. This category of functions is represented in a very compact way both for their algebraic normal forms and for their value vectors. The two important cryptographic parameters: algebraic degree and the nonlinearity, cannot be simultaneously optimized for symmetric functions. The researchers have proved in [5,6] that the highest possible nonlinearity for a symmetric function is only achieved by quadratic functions. As in comparison, symmetric functions with suboptimal nonlinearity exist and create an interest for designing fast and robust cryptographic primitives. Besides the Hamming distance to linear functions, some other criteria, such as correlation immunity or propagation characteristics, are also required in some applications and need to be addressed in the context of symmetric functions.

The rest of the paper has been organized as follows. Section 2 summarizes the recent research on cryptographic function properties. Section 3 explains the proposed symmetric balanced random function generator (SRFG) and Section 4 describes about the properties that the SRFG exhibits. Section 5 provides an analysis of the SRFG and its related results. Finally, Section 6 concludes the paper.

* Corresponding author.
E-mail addresses: rsahaaot@gmail.com (R. Saha), gitaskumar@yahoo.com (Geetha G).

http://dx.doi.org/10.1016/j.chaos.2017.08.020
0960-0779/

2. Related work

Cryptographic algorithms are dependable on a number of cryptographic functions [2] and transformations. Different types of factors are considered for designing such functions [7].For example, resiliency [8] and non-linearity [9] of the functions receives a major concern. Bruer [10] has suggested considering the same importance for all the inputs so that the properties of the cryptographic functions are evaluated significantly. The highest probable non-linearity factor is achieved for quadratic functions as shown in [5,6].

The existence of correlation-immune and resilient symmetric functions has been investigated in [11–13]. Randomness in the bits of the input as well as output is also necessary in the algorithms of cryptography. These algorithms deal with pseudorandom number generators. Recent research dealing with quantum based and automata based pseudorandom generators have been shown in [14–16].

Chaotic cryptography is also been improved by random and pseudo-random sequences as shown in [17,18]. Chaos based random number generator is also used for S-box applications and cryptographic operations as shown in [19].

A new linearization method has been observed in the work [20]. The proposed method works for nonlinear feedback shift registers used for stream ciphers. The authors introduce a novel state transition matrix for an NFSR, which is computed from the truth table of its feedback function. Hamming weight is an important metric for the cryptographic functions. This metric is researched in [21] and a number of properties have been identified. These properties are helpful to analyze a novel design for cryptographic function. In this paper, A novel technique for constructing balanced Boolean functions on even numbers of variables has been shown in [22]. The proposed technique uses a set of disjoint spectra functions and a special Boolean permutation to construct a balanced Boolean function with high nonlinearity and optimal algebraic degree.

Another method for balanced Boolean functions construction has been shown in [23]. The proposed approach uses even number of variables as previous research work with a bound that the even number is greater than 10. It also satisfies the strict avalanche criterion, and has a high algebraic degree. Following the same line of research, another method is proposed recently in [24] to construct resilient Boolean functions on even number of variables satisfying strict avalanche criterion with nonlinearity. Another two construction methods for balanced boolean functions are provided in [25]. It achieves high nonlinearity and satisfies strict avalanche criterion. Both local and global avalanche characteristics property are followed by the proposed methods.

The algebraic immunity of the constructed functions is also considered by the authors. The work described in [26] discusses about the perturbation effect on the symmetric boolean functions. Precisely, the work presented, establishes a relation between exponential sums of these perturbations and Diophantine equations of a particular form.

From the above recent works, some of the dominant research orientations have been identified such as balanced property, nonlinearity of boolean functions, even number of variables for the symmetric boolean functions research. The working on randomness of the function has been not yet researched significantly. Therefore, our present research work has proposed a symmetric random function generator which outputs a combined function of randomly selected boolean functions. The main contributions of our research work are as follows.

1. Random selection of boolean functions and random selection of variable inputs for the functions.
2. Generating a combined function to use in different cryptographic modules.
3. Confirming high nonlinearity, resiliency and balance in outputs.
4. Non-dependency of input variables on the output analysis except variable length and expression length.

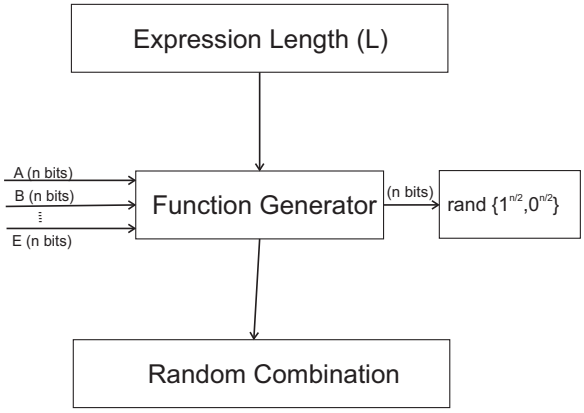

Fig. 1. Structure of the SRFG.

3. Proposed symmetric random function generator (SRFG)

The aim of this present work is to introduce a function generator that produces the symmetric balanced output in the sense of the number of 1s and 0s in the output string irrespective of the input string. The concept of the proposed work must not be confused with the existing symmetric Boolean function. Both the concepts are distinguished by a line of difference: Symmetric Boolean functions consider the hamming weight of the input string, whereas our proposed work considers the hamming distance of output string. Moreover, symmetric boolean function is a specialized function whereas, our proposed work outputs a combined function comprised of basic boolean functions as shown in Fig. 1. This would help the hash algorithms, stream ciphers and round function module of block ciphers to be more robust. The expression for the proposed combined function generator can be given as:

$$f_c = \otimes f_i^L \tag{1}$$

where, $i = 1, 2, \ldots 4$ four logic GATES: AND, OR, NOT and XOR; L represents the expression length (Number of terms in the combined function f_c) and $\otimes$ represents the random combination.

To emphasize the randomness [27] in such combined function generator, the above equation can be further expressed in terms of N input variables' randomness in selection, as shown in Eq. (2).

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

The structure shown in the Fig. 1 can be expanded as the function generator can be used for any N variables of n bits each as shown in Fig. 2.

Let F_2 is the finite field of two elements 0,1 and $\oplus$ is any operation of the field F_2. N variables are used and each variable is considered to be a n bit vector $v = v_1, v_2, \ldots, v_n$. In the further discussion each variable V_i is considered as a binary vector v.

The Hamming Weight [21] of such a binary vector v is given by:

$$wt(v) = \sum_{i=1}^{n} v_i \tag{3}$$

Proposition 1: A combined function f_c using n bit variables and generating an output v_o of n bits is symmetric iff $\sum_{i=1}^{n} v_{o_i} = \frac{n}{2}$ where, $v_{o_i} \in 0, 1$.