A New Class of Nonlinear Functions for Running-key Generators

(Extended Abstract)

Shu Tezuka

ATR Communication Systems Research Laboratory

Twin 21 MID Tower, 2-1-61 Shiromi
Higashi-ku, Osaka 540, Japan

ABSTRACT

A systematic approach to the design of running-key generators in stream cipher systems is proposed using a new class of nonlinear functions based on integer arithmetic operations. This approach is applicable to both feedforward- and feedback-types running-key generators. Most practical nonlinear functions that use only one addition and one multiplication are fully analyzed. Cryptographic properties, such as 0-1 balance, linear complexity, and correlation, of the key-sequence generated by this scheme are examined and several important criteria for determining the parameters of such generators are derived. This approach will prove valuable in designing running-key generators.

I . INTRODUCTION

Most common running-key generators in stream cipher systems are based on a combination of shift registers and several nonlinear Boolean functions[1, 3]. According to the method of combination, the generators are mainly divided into two categories; One is of the feedback type and the other, feedforward. The first type of generator is an n-stage shift register together with a feedback loop which computes the next term for the first stage of the shift register based on a nonlinear Boolean function using the previous n terms. The latter consists of n driving linear feedback shift

C.G. Guenther (Ed.): Advances in Cryptology - EUROCRYPT '88, LNCS 330, pp. 317-324, 1988.

registers and a nonlinear Boolean function that operates on the n output sequences to generate a key sequence[8, 10].

Golomb conducted a comprehensive study on the characteristics of feedback-type generators, particularly the distribution of cycle lengths from both theoretical and empirical viewpoints. On the other hand, several authors are continuing their efforts in analyzing the sequences produced by feedforward-type generators. In either case, however, few systematic methods for synthesizing nonlinear functions can be found.

In this paper, a new nonlinear function design approach for running-key generators is proposed on the basis of integer arithmetic operations such as addition, multiplication. This approach is used for both types of feedback and feedforward generators. The paper is organized as follows. In Section 2, we overview the theory of nonlinear functions for running-key generators in stream cipher systems. In Section 3, a new class of nonlinear functions based on integer arithmetic operations is introduced and some fundamental properties are derived. Section 4, using most practical generators that require only one addition and one multiplication, continues the analysis of cryptographic strength, such as 0-1 balance, linear complexity, and correlation. Section 5 describes some examples of running-key generators based on this scheme. The last section summarizes the advantages of this approach and discusses further research topics.

II . Overview of Nonlinear Functions

A nonlinear Boolean function $F(x_1, ..., x_n)$ is represented in the following general form (the so-called algebraic normal form)[8]:

$$F(x_1, ..., x_n) = a_0 + \sum_i a_i x_i + \cdots + \sum_{i,j} a_i a_j x_i x_j + \cdots + a_{12...n} x_1 x_2 \cdots x_n,$$

where $a_0, a_i, a_{ij}, ...$ are in GF(2), the Galois Field with two elements.

In particular, if $F(x_1, ..., x_n)$ has the following form:

$$F(x_1, ..., x_n) = x_1 + F_1(x_2, ..., x_n) \tag{1}$$

it is of great importance.

Golomb[3] obtained important results concerning the characteristics of binary sequences generated by this type of feedback shift registers. Some of the major results are described as follows:

Theorem A. In the case of the feedback type, the nonlinear function has the form of (1) if and only if the cycle of the key-sequence generated has no branch points.

Theorem B. In the feedback type, the truth table of $F_1(x_2, ..., x_n)$ has an odd/even number of 1's if and only if the generator yields an odd/even number of cycles.

The following two theorems are applicable to the feedforward-type generators [5, 10].

Theorem C. In the feedforward type where an M-sequence generator is equipped with a nonlinear function, if the function has the form of (1), then the key-sequence will be 0-1 balanced.

Theorem D. In the feedforward type, the linear complexity L of the key sequence produced by the function of nonlinear order d operating on the contents of an n-stage M-sequence generator is bounded by

$$L \leq \sum_{j=0}^{d} \binom{n}{j}.$$

Moreover, when the function $F_1(x_2, ..., x_n)$ of (1) has a balanced truth table, there are two additional theorems that must be considered[3, 9].

Theorem E. In the feedback type, the function $F_1(x_2, ..., x_n)$ has a balanced truth table if and only if the autocorrelation with delay n of the key-sequence converges zero as the cycle length approaches 2^n.

Theorem F. In the feedforward type, the function $F_1(x_2, ..., x_n)$ has a balanced truth table if and only if probability $P(z = x_i) = 1/2$, for $i = 1, 2, ..., n$, where z is the output of the nonlinear function $F(x_1, ..., x_n)$, provided that $x_1, ..., x_n$ are independent and identically distributed balanced binary variables.

From above results, we can see that when $F(x_1, ..., x_n)$ has the form of (1) it is very significant for both types of feedback and feedforward generators. Therefore, we will concentrate on this type of nonlinear function in this paper.

III . A New Class of Nonlinear Functions

Define f as a mapping; $f : I_n$ to I_n, where $I_n = \{0, 1, ..., 2^n - 1\}$, and $f_m(x) = f(x)(mod 2^m), x \in I_n, m = 1, ..., n$. Consider a set of mappings satisfying the following two conditions for all $m, m = 1, 2, ..., n,$:

1. $f_m(x)$ is bijective on $I_m = \{0, 1, ..., 2^m - 1\}$, and
2. $f_m(x) = f_m(x(mod 2^m))$ for any $x \in I_n$.

Note that $f(x) \equiv f_n(x)$. Denote the set by Γ_n. The next theorem is fundamental.

Theorem 1. Γ_n is a group with respect to the composition of mappings.

The following theorems are important when we apply this set of mappings to the design of stream cipher systems.

Theorem 2. If $f \in \Gamma_n$, then the most significant bit z of $f(x), x \in I_n$, is given in GF(2) as follows:

$$z = x_1 + F_1(x_2, ..., x_n),$$

where x_i is the i-th bit of an integer$x$.

Theorem 3. The following sets of mappings are the subsets of Γ_n as defined above.
(1). $f(x) = ax + b(mod 2^n)$, where a is odd and b is any integer.
(2). $f(x)$ is a polynomial with integer coefficient modulo 2^n such that $f'(x) \neq 0(mod 2)$, for any $x \in I_n$, and $f(0) \neq f(1)(mod 2)$.
(3). $f(x) = [b^{x+a}/4](mod 2^n)$, where $b = 5(mod 8), a$ is any integer, and $[x]$ is the integer part of x.
(4). $f(x) = [(b^{x+a} + 1)/4](mod 2^n)$, where $b = 3(mod 8)$, and a is any integer.
(5). All the inverse mappings of the above ones form a subset of Γ_n.

Example. If $f(x) = x + 1(mod 2^n)$, then the most significant bit z of $f(x)$ is given in GF(2) as

$$z = x_1 + x_2 \cdots x_n,$$

where x_i is the i-th leading bit of an integer x.

The above theorems mean that any mapping $f \in \Gamma_n$ can be exploited as a nonlinear function for running-key generators in stream cipher systems. In the following sections, $f(x)$ is said to be of order d if the nonlinear order of $F_1(x_2, ..., x_n)$ is d.

IV . Analysis of Mapping $f(x) = ax + b(mod 2^n)$

The mapping of $f(x) = ax + b(mod 2^n)$, which we refer to hereafter as an affine mapping, is of great importance from a practical viewpoint. It requires only one addition and one multiplication, thereby making the implementation much easier and speeding up the generation of the key-sequences. Another merit is theoretical due to the fact that the linearity in the integer arithmetic sense makes the analysis of the key-sequence characteristics easier. First, we obtain the theorem that deals with the total number of distinct truth tables provided by affine mappings.

Theorem 4. Let $f_1(x), f_2(x)$ be two affine mappings. For all $x \in I_n$

$$f_1(x) + f_2(x) = 2^{n-1} - 1(mod 2^n)$$

if and only if the truth table associated with $f_1(x)$ is identical with that of $f_2(x)$.

The following corollary is easily obtained.

Corollary 1. The total number of distinct truth tables provided by affine mappings is given as 2^{2n-2}.

The next theorem is important since this theorem holds for not only affine mappings but also for any mappings in Γ_n.

Theorem 5. The number of 1's in the truth table of $F_1(x_2, ..., x_n)$ is given as follows:

$$2^{n-1} - S_n(f),$$

where $S_n(f)$ denotes the number of points $(x, f(x))$ in the range $0 \leq x, f(x) < 2^{n-1}$.

The value of $S_n(f)$ can be calculated by exploiting the exponential sum, which plays a crucial role in calculating the discrepancy in the field of numerical integration[4, 6, 7].

Theorem 6. The truth table of $F_1(x_2, ..., x_n)$ is balanced if and only if

$$\sum_{k=1}^{2^{n-2}} \frac{t_k^{b+1} + t_k^{a-b}}{(t_k^a - 1)(t_k - 1)} = 0,$$

where $t_k = \omega^{2k-1}$, and ω is the 2^n-th root of one.

The next corollary is useful for the practical design of nonlinear functions.

Corollary 2. $F_1(x_2, ..., x_n)$ has a balanced truth table if

$$a - 2b - 1 = 2^{n-1}(mod 2^n),$$

where a is odd and b is any integer with $0 \leq a, b < 2^n$.

As shown in Theorems C and D, the order of nonlinearity is highly associated with the linear complexity of the sequence produced by the feedforward-type generator. As for the feedback-type generator, it is known that nonlinear order is equal to $n - 1$ if the key-sequence is a de Bruijn sequence[2]. The following theorems deal with this property for affine mappings.

Theorem 7. The nonlinear order of $F_1(x_2, ..., x_n)$ is equal to $n - 1$ if $a = 2^s + 1, s > 1, b = odd$, or if $a = 3, b = even$.

This theorem can be generalized to the case of any mapping in Γ_n in the following way.

Theorem 8. Let $f(x) = g(h(x))(mod 2^n)$ for any two mappings $g(x), h(x)$ in Γ_n. Then, the nonlinear order of $f(x)$ is equal to $n - 1$ if and only if one of the two mappings is of order $n - 1$ and the rest is of order less than $n - 1$.

V . Discussions

DES (Data Encryption Standard) can be regarded as a nonlinear function when used in the output-feedback or in cipher-feedback modes. This cipher scheme, as well as classical ones, consists of two basic elements: permutation and substitution. However, in this paper we have proposed a new approach to building nonlinear functions by using integer arithmetic operations such as addition, multiplication. This approach has the following advantages:

1. It makes theoretical analysis of the cryptographic strength of the generated key-sequence easier.
2. It makes the implementation of the system easier and cheaper because integer arithmetic operation units are accessible or available in both software and hardware.
3. It provides wide variety in selecting nonlinear functions when designing a stream cipher system.

Future major research topics will be to analyze the characteristics of other mappings such as those in sets (2) through (5) in Theorem 3, and to determine the order of Γ_n as well as the total number of distinct truth tables provided by Γ_n for any n.

REFERENCES

[1] H.Beker and F.Piper, *Cipher Systems: The Protection of Communications*, Wiley Interscience, New York, 1982.

[2] H.Fredricksen, A Survey of Full Length Nonlinear Shift Register Cycle Algorithms, *SIAM Review*,Vol.24,pp.195-221 (1982).

[3] S.W.Golomb, *Shift Register Sequences*, Holden-Day, San Francisco, Calif., 1967.

[4] G.H.Hardy and E.M.Wright, *An Introduction to the Theory of Numbers*, 5th ed.,Oxford University Press, Oxford, 1983.

[5] E.L.Key, An Analysis of the Structure and Complexity of Nonlinear Binary Sequences Generators, *IEEE Transactions on Information Theory*, Vol. IT-22, pp.732-736 (1976).

[6] D.E.Knuth, *The Art of Computer Programming: Vol.2, Seminumerical Algorithms*, 2nd ed., Addison-Wesley, 1981.

[7] H.Niederreiter, Quasi-Monte Carlo Methods and Pseudorandom Numbers, *Bull. Amer. Math. Soc.*,Vol.84,pp.957-1041 (1978).

[8] R.A.Rueppel, *Analysis and Design of Stream Ciphers*, Springer-Verlag, Berlin, 1986.

[9] T.Siegenthaler, Decrypting A Class of Stream Ciphers Using Ciphertexts Only, *IEEE Transactions on Computers*, Vol.C-34, pp.81-85 (1985).

[10] M.K.Simon, J.K.Omura, R.A.Scholtz, and B.K.Levitt, *Spread Spectrum Communications*, vol. 1, Computer Science Press, Maryland, 1985.