ELSEVIER

Signal Processing 80 (2000) 211–217

SIGNAL PROCESSING

www.elsevier.nl/locate/sigpro

On an improved summation generator with 2-bit memory

Hoon Jae Lee[a,*], Sang Jae Moon[b]

[a]*Department of Computer Engineering, Kyungwoon University, San 5-1 Induk-ri, Sandong-Myun, Kumi, Kyungbuk 730-850, South Korea*
[b]*School of Electronic and Electrical Engineering, Kyungpook National University 1370, Sankyuk-Dong, Taegu 702-701, South Korea*

Abstract

The summation generator is a real adder generator with a maximum period, near-maximum linear complexity and maximum order of correlation immunity. However it is neither secure against and nor immune to correlation attack between its output sequences and carry sequences in special cases. A modified summation generator, secure against such an attack, has recently been proposed, but no proof is given about its period and linear complexity. In this paper, we propose a new modified summation generator immune to correlation attack. Moreover, we conclude that its period is maximum and that its linear complexity is the same as that of the original summation generator. © 2000 Elsevier Science B.V. All rights reserved.

Zusammenfassung

Der Summierungsgenerator ist ein reeler Addierer-Generator mit maximaler Periodendauer, fast maximaler linearer Komplexität und maximaler Ordnung von Korrelationsunempfindlichkeit. Allerdings ist er in manchen Fällen nicht sicher und unempfindlich gegenüber Korrelationsattacken zwischen seinen Ausgangsfolgen und Trägerfolgen. Ein modifizierter Summierungsgenerator, der robust gegenüber derartigen Attacken ist, wurde kürzlich vorgeschalgen. Es existiert jedoch kein Beweis bezügloch seiner Periodenlänge und seiner linearen Komplexität. In dieser Arbeit schlagen wir einen neuen modifizierten Summierungsgenerator vor, der unempfindlich gegen Korrelationsattacken ist. Ausserdem gelingt es uns zu zeigen, daß seine Periode maximal ist und seine lineare Komplexität mit der des ursprünglichen Summeirungsgenerators übereinstimmt. © 2000 Elsevier Science B.V. All rights reserved.

Résumé

Un générateur de sommations est un générateur additionneur réel avec une période maximale, une complexité linéaire presque maximale et une immunité d'ordre de corrélation maximale. Cependant il n'est pas sûr résistant aux attaques par corrélation entre sa séquence de sortie et des séquences porteuses dans des cas spéciaux. Un générateur de sommations modifié, sûr contre de telles attaques, a été proposé récemment mais il n'y a pas de preuve quant à sa période et sa complexité linéaire. Dans cet article, nous proposons un nouveau générateur de sommations modifié, résistant aux attaques par corrélation. De plus, nous concluons que sa période maximale et sa complexité linéaire sont les mêmes que ceux du générateur de sommations original © 2000 Elsevier Science B.V. All rights reserved.

Keywords: Keystream generator; Period; Linear complexity; Randomness; Summation generator

1. Introduction

In cryptographic and spread-spectrum communication systems [1,14], the running-key generator

* Corresponding author. Tel.: + 82-546-479-1222; fax: + 82-546-479-1029.
E-mail address: hjlee@kyungwoon.ac.kr (H.J. Lee)

0165-1684/00/$ - see front matter
PII: S0165-1684(99)00123-1

in the stream cipher needs to be secure. There are four main characteristics of a secure stream cipher: period, randomness, and linear complexity of the output sequences (according to Beker and Piper [1]), and correlation immunity (according to Siegenthaler [11]).

In general, a running-key generator, such as Geffe's generator [11], consists of N driving linear feedback shift registers (LFSRs) and a nonlinear combiner on N output sequences in order to produce the running key. The most common running-key generator, the summation generator [8,9], is used in stream cipher ("pseudo-noise," or PN sequence generators) and in spread-spectrum systems. The summation generator, when combined with two or more LFSR sequences using 1-bit memory, has some cryptographically good properties. It produces random binary sequences whose period is proved to be maximum and whose linear complexity is conjectured to be near to its period. Moreover, it is easily implemented by a hardware or software approach. For hardware implementation, little memory and few logical gates are required: $L_1 + L_2$ memory bits (D flip-flops), one full adder, a number of XOR gates in feedback taps, and one AND gate.

However, the summation generator is not yet entirely secure [2]. In generating long, consecutive-zero output sequences, it is subject to correlation attack: the correlation between the generator's output sequences and carry sequences can easily be estimated by an outside party. A modified summation generator, which is secure against this correlation attack, has recently been proposed [2], but no proof has been given concerning its period and linear complexity.

In this paper, we propose a new modified summation generator, which is immune to correlation attack. Moreover, we prove that it has a maximum period and near-maximum linear complexity, the same as those of original generator.

2. Improved summation generator with 2-bit memory

2.1. Analysis of the summation generator

Rueppel's summation generator [8,9] outputs z_j and c_j from each LFSR outputs a_j and b_j and previous carry c_{j-1} as in Fig. 1.

$$z_j = a_j \oplus b_j \oplus c_{j-1},$$

$$c_j = a_j b_j \oplus (a_j \oplus b_j) c_{j-1}, \quad j = 0, 1, 2, \ldots .$$

where a is the output sequence of LFSR 1, b is the output sequence of LFSR 2, c is the carry sequence, with carry initialization value $c_{-1} = 0$.

Theorem 1. *The cryptographical properties of Rueppel's summation generator are as follows* [8].
(1) *Period*, $P = (2^{L1} - 1)(2^{L2} - 1)$.
(2) *Good randomness*.
(3) *Linear complexity*, $\mathrm{LC} \leqslant \mathrm{P}$.
(4) *The order of correlation immunity*, $m = 1$.

Theorem 2. (Meier and Staffelbach [7]). (1) *Suppose that the output of the basic summation combiner satisfies* $z_{j+1} = z_{j+2} = \cdots = z_{j+s} = 0$ *and* $z_{j+s+1} = 1$. *Then, for every* t *with* $1 \leqslant t \leqslant s$, *the* $s - t + 2$ *equations*

$$\begin{aligned} z_{j+t+1} &= a_{j+t+1} + b_{j+t+1} + 1 = 0, \\ z_{j+t+2} &= a_{j+t+2} + b_{j+t+2} + 1 = 0, \\ &\cdots, \\ z_{j+s+1} &= a_{j+s+1} + b_{j+s+1} + 1 = 1, \\ z_{j+s+2} &= a_{j+s+2} + b_{j+s+2} + a_{j+s+1} \end{aligned} \tag{1}$$

are simultaneously satisfied with probability at least $1 - 2^{-t}$.

(2) *Suppose that the output of the basic summation combiner satisfies* $z_{j+1} = z_{j+2} = \cdots = z_{j+s} = 1$ and $z_{j+s+1} = 0$. *Then, for every* t *with* $1 \leqslant t \leqslant s$, *the*

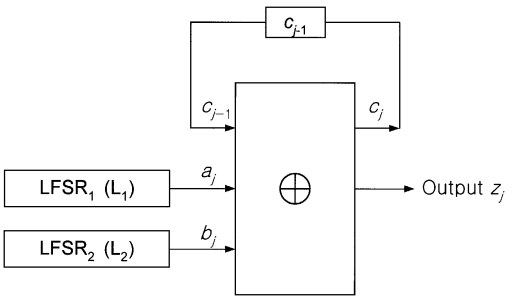

Fig. 1. The summation generator (SUM-BSG).

$s - t + 2$ *equations*

$$z_{j+t+1} = a_{j+t+1} + b_{j+t+1} = 1,$$
$$z_{j+t+2} = a_{j+t+2} + b_{j+t+2} = 1,$$
$$\cdots, \qquad (2)$$
$$z_{j+s+1} = a_{j+s+1} + b_{j+s+1} = 0,$$
$$z_{j+s+2} = a_{j+s+2} + b_{j+s+2} + a_{j+s+1}$$

are simultaneously satisfied with probability at least $1 - 2^{-t}$.

Observe that Theorem 2, which states that (1) and (2) are simultaneously satisfied with a certain probability, is much stronger than the statement that these equations are individually satisfied with the same probability.

2.2. Dawson's generator

Dawson's generator [2] outputs z_j and c_j from each LFSR outputs a_j and b_j and previous carry c_{j-1}:

$$z_j = a_j \oplus b_j \oplus c_{j-1},$$
$$c_j = b_j \oplus (a_j \oplus b_j) c_{j-1}, \quad j = 0, 1, 2, \cdots,$$

where a is the output sequence of LFSR 1, b is the output sequence of LFSR 2, c is the carry sequence, with carry initialization value $c_{-1} = 0$.

However, this generator was not analyzed in terms of cryptographical security.

2.3. An improved summation generator with 2-bit memory

An improved summation generator with 2-bit memory outputs z_j, c_j and d_j from each of LFSR outputs a_j and b_j, previous carry $c_j - 1$ and previous memory $d_j - 1$ as in Fig. 2.

$$z_j = y_j \oplus d_{j-1},$$
$$d_j = f(a_j, b_j, d_{j-1}) = b_j \oplus (a_j \oplus b_j) d_{j-1},$$
$$j = 0, 1, 2 \ \ldots,$$

where y is the output sequence of summation generator, a is the output sequence of LFSR 1, b is the output sequence of LFSR 2, c is the carry sequence,

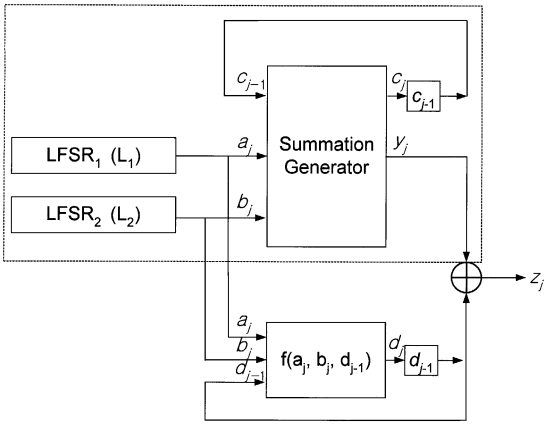

Fig. 2. An improved summation generator with 2-bit memory (ISUM-BSG).

carry initialization value $c_{-1} = 0$, d is memory sequences, memory initialization value $d_{-1} = 0$.

Because the summation generator has a probability of a carry-output correlation of 1/4, highly correlated, it can be vulnerable to correlation attack [2,7] when it outputs consecutive zeros or ones. But the proposed generator is secure by having an additional 0–1 balanced nonlinear memory function, exclusive-ored of the output of the summation generator.

2.3.1. Correlation properties

We refer to the input–output correlation and carry–output correlation in the summation generator in Table 1, which gives us an input-output correlation probability of $\frac{1}{2}$, balanced, and a carry-output correlation probability of $\frac{1}{4}$, not balanced. But in the proposed generator, input(a_j, b_j, c_{j-1} or d_{j-1})–output(z_j) correlation probability is $\frac{1}{2}$, and memory(c_j or d_j)-output(z_j) correlation probability is $\frac{1}{2}$ too, as shown in Table 2. Therefore, the proposed generator is improved in terms of input–, carry–, or memory–output correlation probability. It is safe against correlation attack in a special cases(a long consecutive zero-output).

2.3.2. Security

We analyzed the proposed generator in terms of period, linear complexity, and the order of correlation immunity.

Theorem 3. *In an improved summation generator with 2-bit memory which has two LFSRs of length L_1 and L_2, $\gcd(L_1, L_2) = 1$, the period of output sequences is $(2^{L_1} - 1)(2^{L_2} - 1)$, except null initial state of two LFSRs each, and two LFSRs make $d_j = 0$, only when initial state.*

Proof. Let $j \geqslant 0$, period of a_j, P_a, period of b_j, P_b, expected period of z_j, $P = \mathrm{lcm}(P_a, P_b)$, then

$$\begin{aligned} d_j &= b_j \oplus (a_j \oplus b_j) d_{j-1} \\ &= b_j \oplus (a_j \oplus b_j)[b_{j-1} \oplus (a_{j-1} \oplus b_{j-1}) \oplus d_{j-2}] \\ &= b_j \oplus (a_j \oplus b_j)[b_{j-1} \oplus b_{j-2}(a_{j-1} \oplus b_{j-1}) \oplus \\ &\quad b_{j-3}(a_{j-2} a_{j-1} \oplus a_{j-2} b_{j-1} \oplus \cdots \oplus b_{j-2} b_{j-1}) \\ &\quad \oplus \cdots \oplus b_0 (a_1 \cdots a_{j-1} \oplus b_1 \cdots b_{j-1})] \end{aligned}$$

Table 1
Correlation probability of the summation generator

a_j	b_j	c_{j-1}	c_j	z_j	Correlation probability
0	0	0	0	0	* Input–output:
0	0	1	0	1	$P[a_j = z_j] = \frac{1}{2}$
0	1	0	0	1	$P[b_j = z_j] = \frac{1}{2}$
0	1	1	1	0	$P[c_{j-1} = z_j] = \frac{1}{2}$
1	0	0	0	1	
1	0	1	1	0	* Carry–output:
1	1	0	1	0	$P[c_j = z_j] = \frac{1}{4}$
1	1	1	1	1	

$$\begin{aligned} d_{j+P} &= b_{j+P} \oplus (a_{j+P} \oplus b_{j+P}) \\ &\quad \times [b_{j-1+P} \oplus b_{j-2+P}(a_{j-1+P} \oplus b_{j-1+P}) \\ &\quad \oplus b_{j-3+P}(a_{j-2+P} a_{j-1+P} \oplus a_{j-2+P} b_{j-1+P} \\ &\quad \oplus \cdots \oplus b_{j-2+P} b_{j-1+P}) \oplus \cdots \\ &\quad \oplus b_P (a_{1+P} \ldots a_{j-1+P} \\ &\quad \oplus \cdots \oplus b_{1+P} \ldots b_{j-1+P}) \oplus d_P] \end{aligned}$$

and $d_P = 0$ (in case of two LFSRs are all initial states), $b_{j+P} = b_j$, $a_{j+P} = a_j$, and $d_{j+P} = d_j$ therefore, period of d_{j-1}, is $P_d = P = \mathrm{lcm}(P_a, P_b)$. □

On the other hand, the period of y_j in summation generator is $P_y = \mathrm{lcm}(P_a, P_b)$ by Rueppel [8,9] and $z_j = y_j \oplus d_{j-1}$, therefore, the period of z_j is $P = \mathrm{lcm}(P_y, P_d) = \mathrm{lcm}(P_a, P_b) = (2^{L_1} - 1)(2^{L_2} - 1)$ in cases of $\gcd(L_1, L_2) = 1$.

Theorem 4. *In an improved summation generator with 2-bit memory, linear complexity of output sequence z_j is approximately equal to the period of z_j.*

For a small size of L_1 and L_2, simulation examples of period and LC for the summation generator and the proposed generator are as shown in Table 3. By computing in the Berlekamp–Massey algorithm [5], linear complexities of output

Table 2
Correlation probability of the proposed generator

a_j	b_j	c_{j-1}	d_{j-1}	c_j	y_j	d_j	z_j	Correlation probability
0	0	0	0	0	0	0	0	
0	0	0	1	0	0	0	1	
0	0	1	0	0	1	0	1	* Input–output:
0	0	1	1	0	1	0	0	$P[a_j = z_j] = \frac{1}{2}$
0	1	0	0	0	1	1	1	$P[b_j = z_j] = \frac{1}{2}$
0	1	0	1	0	1	0	0	$P[d_{j-1} = z_j] = \frac{1}{2}$
0	1	1	0	1	0	1	0	$P[d_{j-1} = z_j] = \frac{1}{2}$
0	1	1	1	1	0	0	1	
1	0	0	0	0	1	0	1	
1	0	0	1	0	1	1	0	
1	0	1	0	1	0	0	0	
1	0	1	1	1	0	1	1	
1	1	0	0	1	0	1	0	* Carry–output:
1	1	0	1	1	0	1	1	$P[c_j = z_j] = \frac{1}{2}$
1	1	1	0	1	1	1	1	$P[d_j = z_j] = \frac{1}{2}$
1	1	1	1	1	1	1	0	

sequences in the two generators are close to their periods.

Theorem 5. *In an improved summation generator with 2-bit memory, the order of correlation immunity is* 1.

Proof. The result of computing in the Walsh transform [7] is the following table. In the table for all w except $w = 0000_B$ and $w = 1111_B$, $F(w) = 0$, and so it has the third order of correlation immunity containing a carry and a memory. On the other hand, the maximum order of correlation immunity is $m_{\max} = N - 1 = 2 - 1 = 1$ by Meier and Staffelbach [7]; therefore, the order of correlation immunity is 1 by subtracting 2 (a carry and a memory) from 3 (Table 4). □

2.3.3. Randomness test

Because the sequence of the proposed generator has large period in practice, we choose the method of local randomness [1]. After choosing the significance level = 0.05 and Chi-square distribution [1], the frequency test, serial test, generalized serial test [4], poker test and autocorrelation test [2] are adapted.

We sampled about 160,000 bits of the output sequences randomly for the following three examples(generators): the (31, 33), (63, 65) and (127, 131) stages of LFSR pairs.

Example

(1) $P_1(X) = X^{31} + X^3 + 1$

(IV = 10101010 … 101),

$Q_1(X) = X^{33} + X^{13} + 1$

(IV = 11111111 … 111).

(2) $P_2(X) = X^{63} + X^1 + 1$ (IV = random),

$Q_2(X) = X^{65} + X^{18} + 1$ (IV = random).

(3) $P_3(X) = X^{127} + X^1 + 1$ (IV = random).

$Q_3(X) = X^{131} + X^{13} + X^2 + X^1 + 1$

(IV = random).

The three kinds of sampled data display a good randomness, as shown in Table 5, in terms of the result of the frequency test, serial test, generalized serial test ($t = 3, 4, 5$), poker test ($m = 3, 4, 5$), and autocorrelation test.

2.3.4. Comparison

Because the summation generator had a carry–output correlation probability of 1/4, not uncorrelated, it was broken by correlation attack [2,7] when the output had many consecutive zeros or ones. But the proposed generator has an input(a_j, b_j, c_{j-1} or d_{j-1})-output(z_j) correlation probability of $\frac{1}{2}$ and a memory(c_j or d_j)–output(z_j) correlation probability of $\frac{1}{2}$, and so it is secure and will not incur carry bits from the output of a long sequence of consecutive zeros and ones. In other words, it is secure by adding one bit of memory in nonlinear combine function based on the summation generator (Table 6).

Table 3
Simulation examples of the period and LC for ISUM-BSG

Stage of LFSRs		SUM-BSG		ISUM-BSG	
L_1	L_2	P	LC	P	LC
3	4	105	100	105	103
3	5	217	208	217	217
4	5	465	455	465	463

Table 4
The result of the Walsh transform for ISUM-BSG function

w	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$F(w)$	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	−8

Table 5
The result of random tests for ISUM-BSG

Items	Threshold	Test results		
		Sample 1	Sample 2	Sample 3
(1) Frequency test	3.84	0.027	0.005	2.042
(2) Serial test	5.99	1.390	0.023	2.233
(3) Generalized t-serial test				
$t = 3$	9.48	6.919	1.836	3.696
$t = 4$	15.50	12.459	3.412	5.462
$t = 5$	29.29	23.057	12.727	7.762
(4) Poker test				
$m = 3$	14.067	6.185	7.035	6.850
$m = 4$	24.996	17.287	7.617	17.510
$m = 5$	44.654	37.304	24.487	20.592
(5) Autocorrelation test	max. $\leqslant 0.05$	max = 0.0060	max = 0.0063	max = 0.0072

Table 6
Comparison of similar summation generators

Items	SUM-BSG	ISUM-BSG
Period	$P = (2^{L1} - 1)(2^{L2} - 1)$	$P = (2^{L1} - 1)(2^{L2} - 1)$
Randomness	Random	Random
Linear complexity	LC $\fallingdotseq P$	LC $\fallingdotseq P$
Correlation immunity	CI = 1	CI = 1
Correlation attack	Correlation breakable (consecutive "0" or "1" output)	Secure

3. Conclusion

In this paper, we have proposed an improved summation generator with 2-bit memory and have analyzed it. Because the original summation generator had a carry–output correlation probability of $\frac{1}{4}$, not uncorrelated, it was broken by correlation attack when it generated many consecutive zeros or ones. But the proposed generator has an input (a_j, b_j, c_{j-1} or d_{j-1})–output(z_j) correlation probability of $\frac{1}{2}$ and a memory (c_j or d_j)–output(z_j) correlation probability of $\frac{1}{2}$, so it is secure and will not incur carry bits from the output of a long sequence of consecutive zeros and ones. Therefore, it is secure by adding one bit of memory in nonlinear combine function based on the summation generator.

4. Further reading

The following references are also of interest to the reader: [3]; [6]; [10]; [12]; [13]; [15].

References

[1] H.J. Beker, F.C. Piper, Cipher Systems: The Protection of Communications, Northwood Books, London, 1982.
[2] E. Dawson, Cryptanalysis of Summation Generator, Advances in Cryptology – AUSCRYPT'92, Lecture Notes in Computer Science, Springer, Berlin, 1993, 209–215.
[3] P. R. Geffe, How to protect data with ciphers that are really hard to break, Electronics, (January 1973) 99–101.
[4] M. Kimberley, Comparison of two statistical tests for keystream sequences, Electron. Lett. 23(8) (April 1987) 365–366.
[5] J. L. Massey, Shift-register synthesis and BCH decoding, IEEE Trans. Inform. Theory Vol. IT-15 (1) (January 1969) 122–127.
[6] W. Meier, O. Staffelbach, Fast correlation attacks on stream ciphers, J. Cryptol. (1) (1989) 159–176.
[7] W. Meier, O. Staffelbach, Correlation properties of combiners with memory in stream ciphers, J. Cryptol. 5 (1992) 67–86.

[8] R. A. Rueppel, Correlation immunity and the summation generator, Advances in Cryptology, Proceedings of CRYPTO'85, 1985, 260–272.
[9] R.A. Rueppel, Analysis and Design of Stream Ciphers, Springer, Berlin, 1986.
[10] R. A. Rueppel, O. J. Stafflebach, Products of linear recurring sequences with maximum complexity, IEEE Trans. Inform. Theory IT-33 (1) (January 1987) 124–131.
[11] T. Siegenthaler, Correlation-immunity of nonlinear combining functions for cryptographic applications, IEEE Trans. Inform. Theory IT-30 (5) (September 1984) 776–780.
[12] T. Siegenthaler, Design of combiners to prevent divide and conquer attacks, Advances in Cryptology, Proceedings of CRYPTO'85, 1985, 273–279.
[13] T. Siegenthaler, Decrypting a class of stream ciphers using ciphertext only, IEEE Trans. Comput. C-34 (1) (January 1985) 81–85.
[14] H.C.A. van Tilborg, An Introduction to Cryptology, Kluwer, Boston, 1982.
[15] X. G. Zhen, J.L. Massey, A Spectral Characterization of Correlation – Immune Combining Functions, IEEE Trans. Inform. Theory 34 (3) (May 1988).