求和生成器的相关性分析*

冯登国[1+], 马卫局[2]

[1](中国科学院 软件研究所,北京 100080)

[2](中国科学院研究生院 信息安全国家重点实验室,北京 100039)

Correlation Analysis of Summation Generator

FENG Deng-Guo[1+], MA Wei-Ju[2]

[1](Institute of Software, The Chinese Academy of Sciences, Beijing 100080, China)

[2](State Key Laboratory of Information Security, Graduate School of the Chinese Academy of Sciences, Beijing 100039, China)

+ Corresponding author: Phn: 86-10-62654046, E-mail: fengdg@263.net

http://www.iscas.ac.cn

Received 2002-04-10; Accepted 2002-09-06

Feng DG, Ma WJ. Correlation analysis of summation generator. *Journal of Software*, 2003,14(8):1463~1469.
http://www.jos.org.cn/1000-9825/14/1463.htm

Abstract: J. Dj. Golić applied linear sequential circuit approximation (LSCA) method to analyze the summation generator with an arbitrary number of inputs. He conjectured that he could obtain all pairs of mutually correlated input and output linear functions with the maximum possible absolute value of the correlation coefficient by this method, but he did not give any proof. By using Walsh Transformation technique, the conjecture is proved for even n in this paper. The "total correlation" of summation generator is studied which is very similar to that of combiners with one bit memory.

Key words: summation generator; correlation coefficient; memory; stream cipher

摘 要: J. Dj. Golić 运用线性序列电路逼进的方法来分析具有任意个输入的求和生成器.他猜想可以通过这种方法来获得所有具有最大相关系数的输入和输出线性函数对,但是他未给出证明.利用 Walsh 变换技术证明了当 n 是偶数的时候这个猜想成立.另外,还研究了求和生成器的相关系数总和,发现它与带 1 比特组合器的相关系数总和非常类似.

关键词: 求和生成器;相关系数;记忆;流密码

中图法分类号: TP309 **文献标识码**: A

* Supported by the National Grand Fundamental Research 973 Program of China under Grant No.G1999035802 (国家重点基础研究发展规划(973)); the National Science Foundation of China for Distinguished Young Scholars under Grant No.60025205 (国家杰出青年科学基金)

FENG Deng-Guo was born in 1965. He is a professor and doctoral supervisor at the Institute of Software, the Chinese Academy of Sciences. His research areas are design and analysis of block cipher, construction and analysis of nonlinear function and security of computer communication network. **MA Wei-Ju** was born in 1978. He is a Ph.D. candidate at the Graduate School of the Chinese Academy of Sciences. His current research interests include cryptology and information security.

In stream cipher designing, nonlinear Boolean functions are often used as combiners, and the inputs of the combiners are usually linear feedback shift registers (LFSRs). It is the general structure of memoryless stream ciphers. A combiner of such structure must be of some correlation immunity order[1], otherwise the combiner will be vulnerable to divide-and-conquer correlation attacks[2]. For a memoryless combiner, Meier and Staffelbach[3] showed that the sum of the squares of the correlation coefficients between the output bit and all of the linear functions of the input is always 1

$$\sum_i c_i^2 = 1. \tag{1}$$

Choosing combiners to be of some correlation immunity order means that certain of these c_i's vanish. However, by (1) this causes some other correlation coefficients to increase according to which cryptanalyst may apply fast correlation attacks[4,5]. So there is a tradeoff[1] between the nonlinear complexity and the correlation immunity order. The use of combiner with memory is suggested in Ref.[6] to avoid this tradeoff. It is shown that with just one bit of memory, one can achieve the maximum-order correlation immunity regardless of the linear complexity. R. A. Rueppel[6] proposed the summation generator as an example of such combiners with memory.

The correlation properties of combiners with one bit memory (including summation generator with two inputs) have been studied in Ref.[7]. For any n, the corresponding asymptotic correlation coefficients of summation generator with n inputs who has $M=\lceil \log_2 n \rceil$ bit memory are determined in Ref.[8]. Golić[7] applied linear sequential circuit approximation (LSCA) method to the summation generator with arbitrary number of inputs and obtains all pairs of mutually correlated input and output linear functions with the maximum possible absolute value of the correlation coefficient. But he didn't confirm if such linear functions had the maximum absolute value of correlation coefficient to the current output bit. His conjecture was only demonstrated by two examples when n=3 and n=5. We will give a strict proof for even n in this paper. What's more, we will get a result about the "total correlation" of summation generator, which is very similar to the one about combiner with one bit memory.

Attacks on summation generator are given in Refs.[9~11].

Section 1 is a summing-up of the preceding work on summation generator[6~9]. In Section 2, we give a proof of Golić's conjecture for even n and investigate the "total correlation" of summation generator. Conclusions and open questions are given in Section 4.

1 The Summation Generator

The summation generator is a binary nonlinear combiner with memory whose internal state variable, the carry, takes integer values from the set $[0,n-1]$, where n is the number of inputs. The memory size in bits is thus $M=\lceil \log_2 n \rceil$. Let $X_t=(x_{1,t},...,x_{n,t})$ and y_t denote the n input bits and the output bit at time t respectively, and let S_t denote the carry at time t. For simplicity, we keep the same notation for the carry $S_t=\sum_{j=0}^{m-1} s_{j,t}2^j$ and for the binary representation of the carry $S_t=(s_{0,t},...,s_{M-1,t})$. We also use the notation $S_t^{(j)}=s_{j,t}$, $0\le j\le M-1$, $S_t^{(0)}$ being the least significant bit of S_t. Then, for $t\ge 0$, the output and the next-state function of the summation generator are defined by

$$y_t = f_0(X_t,S_t) = \bigoplus_{i=1}^{n} x_{i,t} \oplus S_t^{(0)}, \tag{2}$$

$$S_{t+1} = f_1(X_t,S_t) = \left\lfloor \left(\sum_{i=1}^{n} x_{i,t} + S_t \right) \Big/ 2 \right\rfloor, \tag{3}$$

with the modulo 2 summation in (2) and integer summation in (3).

In correlation analysis, the input $\{x_{i,t}\}_{t=0}^{\infty}$, $1 \le i \le n$, which are produced by LFSRs with distinct primitive feedback polynomials, are assumed to be mutually independent, uniformly distributed and independent sequences of binary variables. However, the next-state function (3) is not balanced, that is to say, the carry S_t is not uniformly distributed among the set $[0, n-1]$, if its input is balanced. It is shown in Ref.[12] that the next-state function defines an ergodic Markov chain whose stationary (asymptotic) probability distribution is given by (see Ref.[1])

$$q(s) = \frac{1}{n!}\sum_{l=0}^{s}(-1)^l (s-l)^n \binom{n+1}{l}. \tag{4}$$

Here $q(s)$ denotes the asymptotic probability that S_t is equal to $s-1$, $1 \le s \le n$. Because S_t becomes arbitrarily close to the stationary probability for increasing j, we can assume that $P(S_o = s-1) = q(s)$.

The correlation coefficient between any two binary random variables a and b is defined as $c(a,b) = P(a=b) - P(a \ne b)$, and the correlation coefficient of a single binary variable a is defined as $c(a) = c(a,0)$. For even S_t, $y_t = \bigoplus_{i=1}^{n} x_{i,t}$, and for odd S_t, $y_t \ne \bigoplus_{i=1}^{n} x_{i,t}$. So $p_0 = P(y_t = \bigoplus_{i=1}^{n} x_{i,t}) = q(1)+q(3)+q(5)+\ldots$, and $P(y_t \ne \bigoplus_{i=1}^{n} x_{i,t}) = q(2)+q(4)+q(6)+\ldots$. Then the (asymptotic) correlation coefficient of the least significant bit $S^{(0)}$ is given as

$$c_n(S^{(0)}) = p_0 - p_1 = \sum_{s=1}^{n}(-1)^{s+1} q(s). \tag{5}$$

Theorem 1.[8] For the asymptotic probability in (4),

$$q(n+1-s) = q(s). \tag{6}$$

When the number of the inputs is even, $c_n(S^{(0)})$=0. When n is odd, we get

$$c_n(S^{(0)}) = 2^{-(n-1)/2} \begin{cases} \sum_{l=1}^{k-1}(-1)^{l+1} q(2l) & \text{if } k \equiv 0 \pmod 4, \\ \sum_{l=0}^{k-1}(-1)^{l} q(2l+1) & \text{if } k \equiv 1 \pmod 4, \\ -\sum_{l=1}^{k-1}(-1)^{l+1} q(2l) & \text{if } k \equiv 2 \pmod 4, \\ -\sum (-1)^{l} q(2l+1) & \text{if } k \equiv 3 \pmod 4. \end{cases} \tag{7}$$

and $c_n(S^{(0)}) < 2^{-(n-1)/2}$. In particular, $\lim_{n\to\infty} c_n(S^{(0)}) = 0$.

Theorem 2.[9] Denote the stationary coefficient between $S_t^{(0)}$ and $\varpi \cdot X_{t-1}$ by $c_n(S^{(0)}, \varpi \cdot X)$, $\varpi \in F_2^n$. For odd n, $c_n(S^{(0)}, x_i) = 0$, and for even n, $n = 2k$,

$$c_n(S^{(0)}, x_i) = 2^{-n/2} \begin{cases} -\sum_{l=0}^{k-1}(-1)^{l} q(2l+1) + \sum_{l=1}^{k}(-1)^{l+1} q(2l) & \text{if } k \equiv 0 \pmod 4, \\ \sum_{l=0}^{k-1}(-1)^{l} q(2l+1) + \sum_{l=1}^{k}(-1)^{l+1} q(2l) & \text{if } k \equiv 1 \pmod 4, \\ \sum_{l=0}^{k-1}(-1)^{l} q(2l+1) - \sum_{l=1}^{k}(-1)^{l+1} q(2l) & \text{if } k \equiv 2 \pmod 4, \\ -\sum_{l=0}^{k-1}(-1)^{l} q(2l+1) - \sum_{l=1}^{k}(-1)^{l+1} q(2l) & \text{if } k \equiv 3 \pmod 4. \end{cases} \tag{8}$$

where $1 \le i \le n$. What' more, for even n, let $W_H(\varpi)$ be the Hamming weight of ϖ. Then $c_n(S^{(0)}, \varpi \cdot X)$ is equal to $c_n(S^{(0)}, x_i)$ if $W_H(\varpi) \equiv 1 \pmod 4$, to $-c_n(S^{(0)}, x_i)$ if $W_H(\varpi) \equiv 3 \pmod 4$, and to zero if $W_H(\varpi)$ is

even.

Let $c(n)$ be define as $c_n(S^{(0)})$ if n is odd and as $c_n(y,x_1)$ if n is even. Then we let $c_{\max}(n)=|c(n)|$.

Theorem 3.[9] For any time $t\geq 1$, assume that the current and the preceding inputs to the summation generator are mutually independent and uniformly distribute and that the preceding carry has the asymptotic probability distribution (4).

If the number n of binary inputs is odd, then the correlation coefficient between the current output bit and the binary sum of the current input bits and any number m, $0\leq m\leq n$, of the preceding input bits is equal to $c(n)$ if $m\equiv 0(\mathrm{mod}\,4)$, to $-c(n)$ if $m\equiv 2(\mathrm{mod}\,4)$, and to zero if m is odd.

If the number n of binary inputs is even, then the correlation coefficient between the current output bit and the binary sum of the current input bits and any number m, $0\leq m\leq n$, of the preceding input bits is equal to $c(n)$ if $m\equiv 1(\mathrm{mod}\,4)$, to $-c(n)$ if $m\equiv 3(\mathrm{mod}\,4)$, and to zero if m is even.

2 Correlation Analysis of Summation Generator

In fact, the output function is a Boolean function with $n+1$ variables. $S_t^{(0)}$ can be regarded as a Boolean function of X_{t-1} and S_{t-1}

$$S_t^o=\left\lfloor\left(\sum_{i=1}^{n}x_{i,t-1}+S_{t-1}^{(0)}\right)\Big/2\right\rfloor^{(0)}\oplus S_{t-1}^{(1)}. \tag{9}$$

We denote the correlation coefficients between the output function and the linear functions by $c_0(\varpi)=c(f_0,\varpi\cdot X)$ and $c_1(\varpi)=c(f_0,\varpi\cdot X+S^{(0)})$. In this section we only concentrate on the condition of even n. When n is even, the stationary probability distribution of $S^{(0)}$ is balanced. Thus we get

$$c_0(\varpi)=S_{(f_0)}(\varpi,0),\quad c_1(\varpi)=S_{(f_0)}(\varpi,1), \tag{10}$$

where $S_{(f_0)}$ is the Walsh transform of f_0

$$S_{(f_0)}(\varpi)=\frac{1}{2^{n+1}}\sum_{X\in F_2^{n+1}}(-1)^{f_0(X)}(-1)^{\varpi\cdot X},\ (\varpi\in F_2^{n+1}). \tag{11}$$

We denote

$$C_0^2=\sum_{\varpi\in F_2^n}c_0(\varpi)^2,\quad C_1^2=\sum_{\varpi\in F_2^n}c_1(\varpi)^2. \tag{12}$$

Then by Parseval's theorem,

$$C_0^2+C_1^2=1. \tag{13}$$

It is easy to know that $C_0^2=0$ and $C_1^2=c_1(1,1,...,1)=1$.

We also denote the correlation coefficients between the next-state function and the linear functions by $d_0(\varpi)=c(f_1,\varpi\cdot X)$ and $d_1(\varpi)=c(f_1,\varpi\cdot X+S^{(0)})$. Then $d_0(\varpi)$ is determined by Theorem 2. Now we investigate all correlation coefficient between the current output bit y_t the linear functions with the form

$$l=\sum_{k=t-i}^{t}\varpi_k X_k. \tag{14}$$

Lemma 1. Suppose that (Ω,F,P) is a probability space, and $Y=(y_1,...,y_n)$ is a random vector of n dimension in (Ω,F,P), then for any $a=(a_1,...,a_n)\in F_2^n$, we have

$$P(y_1=a_1,...,y_n=a_n)=\frac{1}{2^{n-1}}\sum_{\varpi\in F_2^n,\varpi\neq 0}P(\varpi Y=\varpi a)-\frac{2^{n-1}-1}{2^{n-1}}.$$

In particular, for $n=2$, we have

$$P(y_1=a_1,y_2=a_2)=\frac{1}{2}(P(y_1=a_1)+P(y_2=a_2)+P(y_1+y_2=a_1+a_2))-\frac{1}{2}.$$

Theorem 4. The correlation coefficient between y_t and $l=\sum_{k=t-i}^{t}\varpi_k X_k$ is

$$c(y_t,\sum_{k=t-i}^{t}\varpi_k X_k)=c_1(\varpi_t)d_1(\varpi_{t-1})...d_1(\varpi_{t-i+1})d_0(\varpi_{t-i}). \tag{18}$$

Proof. For $i=0$ and every $\varpi\in F_2^n$, $s=\varpi_t\cdot X_t$, $c(y_t,\varpi_t\cdot X_t)$ is equal to zero for $S_t^{(0)}$ is balanced and independent to X_t.

For $i=1$, $s=\varpi_t\cdot X_t+\varpi_{t-1}\cdot X_{t-1}$, we have

$$c(y_t,\varpi_t\cdot X_t+\varpi_{t-1}\cdot X_{t-1}) = 2P(y_t=\varpi_t\cdot X_t+\varpi_{t-1}\cdot X_{t-1})-1. \tag{15}$$

$$\begin{aligned}
&P(y_t=\varpi_t\cdot X_t+\varpi_{t-1}\cdot X_{t-1})=P(f_0(X_t,S_t^{(0)})=\varpi_t\cdot X_t+\varpi_{t-1}\cdot X_{t-1})\\
&=P(f_0(X_t,0)=\varpi_t\cdot X_t+\varpi_{t-1}\cdot X_{t-1},S_t^{(0)}=0)+P(f_0(X_t,1)=\varpi_t\cdot X_t+\varpi_{t-1}\cdot X_{t-1},S_t^{(0)}=1)\\
&=\frac{1}{2}[P(f_0(X_t,0)=\varpi_t\cdot X_t+\varpi_{t-1})+P(S_t^{(0)}=0)+P(f_0(X_t,0)=\varpi_t\cdot X_t+\varpi_{t-1}\cdot X_{t-1}+S_t^{(0)})-1]+\\
&\quad\frac{1}{2}[P(f_0(X_t,1)=\varpi_t\cdot X_t+\varpi_{t-1})+P(S_t^{(0)}=1)+P(f_0(X_t,1)=\varpi_t\cdot X_t+\varpi_{t-1}\cdot X_{t-1}+S_t^{(0)}+1)-1]\\
&=\frac{1}{2}P(f_0(X_t,0)=\varpi_t\cdot X_t+\varpi_{t-1}\cdot X_{t-1}+S_t^{(0)})+\frac{1}{2}P(f_0(X_t,1)=\varpi_t\cdot X_t+\varpi_{t-1}\cdot X_{t-1}+S_t^{(0)}+1)\\
&=\frac{1}{2}[P(f_0(X_t,0)=\varpi_t\cdot X_t,\varpi_{t-1}\cdot X_{t-1}+S_t^{(0)}=0)+P(f_0(X_t,0)=\varpi_t\cdot X_t+1,\varpi_{t-1}\cdot X_{t-1}+S_t^{(0)}=1)]+\\
&\quad\frac{1}{2}[P(f_0(X_t,1)=\varpi_t\cdot X_t,\varpi_{t-1}\cdot X_{t-1}+S_t^{(0)}=1)+P(f_0(X_t,1)=\varpi_t\cdot X_t+1,\varpi_{t-1}\cdot X_{t-1}+S_t^{(0)}=0)]\\
&=\frac{1}{2}[P(f_0(X_t,0)=\varpi_t\cdot X_t)P(\varpi_{t-1}\cdot X_{t-1}+S_t^{(0)}=0)+P(f_0(X_t,0)=\varpi_t\cdot X_t+1)P(\varpi_{t-1}\cdot X_{t-1}+S_t^{(0)}=1)]+\\
&\quad\frac{1}{2}[P(f_0(X_t,1)=\varpi_t\cdot X_t)P(\varpi_{t-1}\cdot X_{t-1}+S_t^{(0)}=1)+P(f_0(X_t,1)=\varpi_t\cdot X_t+1)P(\varpi_{t-1}\cdot X_{t-1}+S_t^{(0)}=0)]\\
&=\frac{1}{2}\{P(\varpi_{t-1}\cdot X_{t-1}+S_t^{(0)}=0)[P(f_0(X_t,0)=\varpi_t\cdot X_t)-P(f_0(X_t,1)=\varpi_t\cdot X_t)]+P(f_0(X_t,1)=\varpi_t\cdot X_t)\}+\\
&\quad\frac{1}{2}\{P(\varpi_{t-1}\cdot X_{t-1}+S_t^{(0)}=0)[P(f_0(X_t,1)=\varpi_t\cdot X_t+1)-P(f_0(X_t,0)=\varpi_t\cdot X_t+1)]+P(f_0(X_t,0)=\varpi_t\cdot X_t+1)\}\\
&=\frac{1}{2}[P(f_0(X_t,1)=\varpi_t\cdot X_t)+P(f_0(X_t,0)=\varpi_t\cdot X_t+1)+\\
&\quad P(\varpi_{t-1}\cdot X_{t-1}+S_t^{(0)}=0)(P(f_0(X_t,0)=\varpi_t\cdot X_t)-P(f_0(X_t,1)=\varpi_t\cdot X_t)+\\
&\quad P(f_0(X_t,1)=\varpi_t\cdot X_t+1)-P(f_0(X_t,0)=\varpi_t\cdot X_t+1))]\\
&=\frac{1}{2}[1-(P(f_0(X_t,0)=\varpi_t\cdot X_t)-P(f_0(X_t,1)=\varpi\cdot X_t)+\\
&\quad 2P(\varpi_{t-1}X_{t-1}+S_{t-1}^{(0)}=0)(P(f_0(X_t,0)=\varpi_t\cdot X_t)-P(f_0(X_t,1)=\varpi_t\cdot X_t))]\\
&=\frac{1}{2}[1+(P(f_0(X_t,0)=\varpi_t\cdot X_t)-P(f_0(X_t,1)=\varpi_t\cdot X_t))(2P(\varpi_{t-1}X_{t-1}+S_{t-1}^{(0)}=0)-1)]\\
&=\frac{1}{2}[1+\frac{1}{2}(P(f_0(X_t,0)=\varpi_t\cdot X_t)-P(f_0(X_t,0)\neq\varpi_t\cdot X_t))+\\
&\quad\frac{1}{2}(P(f_0(X_t,1)\neq\varpi_t\cdot X_t)-P(f_0(X_t,1)=\varpi_t\cdot X_t))]\ (2P(\varpi_{t-1}X_{t-1}+S_{t-1}^{(0)}=0)-1)\\
&=\frac{1}{2}[1+\frac{1}{2^{n+1}}\sum_{X\in F_2^n}(-1)^{f_0(X,0)+\varpi_t\cdot X)}+\frac{1}{2^{n+1}}\sum_{X\in F_2^n}(-1)^{f_0(X,1)+\varpi_t\cdot X+1)}]d_0(\varpi_{t-1})
\end{aligned}$$

$$= \frac{1}{2}[1 + \frac{1}{2^{n+1}} \sum_{X \in F_2^{n+1}} (-1)^{f_0(X)} (-1)^{(\varpi_t, 1) \cdot X}] d_0(\varpi_{t-1})$$

$$= \frac{1}{2}[1 + c_1(\varpi_t)] d_0(\varpi_{t-1}) .$$

By (15), we get

$$c(y_t, \varpi_t \cdot X_t + \varpi_{t-1} \cdot X_{t-1}) = c_1(\varpi_t) d_0(\varpi_{t-1}) . \tag{16}$$

For $i = 2$, if we use the same method and similar procedure, we will get

$$c(y_t, \varpi_t \cdot X_t + \varpi_{t-1} \cdot X_{t-1} + \varpi_{t-2} \cdot X_{t-2}) = c_1(\varpi_t) d_1(\varpi_{t-1}) d_0(\varpi_{t-2}) . \tag{17}$$

$$\vdots$$

By induction, in step *i* we get

$$c(y_t, \sum_{k=t-i}^{t} \varpi_k X_k) = c_1(\varpi_t) d_1(\varpi_{t-1}) ... d_1(\varpi_{t-i+1}) d_0(\varpi_{t-i}) , \tag{18}$$

which completes the proof of the theorem. □

Theorem 1 gives the correlation coefficient between all the linear functions of the inputs. So we can get the following corollaries

Corollary 1. For even n, Theorem 3 gives all the linear functions with maximum correlation coefficients to the current output bit.

Proof. It is because of the fact that, for $i \geq 2$ and $\forall \varpi \in F_2^n$, $|d_1(\varpi_{t-i+1})| < 1$. □

Corollary 2. For even n, the correlation coefficients between the output bit at time t and all the linear functions with form (14) satisfy

$$C^2 = \sum_{\{\varpi_k | t-i \leq k \leq t, \varpi_k \in F_2^n\}} c^2(y_t, \sum_{k=t-i}^{t} \varpi_k X_k) = D_0^2 \frac{1 - D_1^{2i}}{1 - D_1^2} . \tag{19}$$

Proof. For $j = 0,1,...,i$, let $L_j = \{\sum_{k=t-i}^{t} \varpi_k X_k \mid \varpi_{t-j} \neq 0, \varpi_{t-j-1} = ... = \varpi_{t-i} = 0\}$. Then

$$\sum_{l \in L_j} c(y_t, l)^2 = \sum_{\{\varpi_k | t-j \leq k \leq t, \varpi_{t-j} \neq 0\}} c_1(\varpi_t)^2 d_0(\varpi_{t-j})^2 \prod_{k=t-j+1}^{t-1} d_1(\varpi_k)^2 = C_1^2 D_0^2 D_1^{2(j-1)} ,$$

$$C^2 = C_0^2 + \sum_{j=1}^{i} C_1^2 D_0^2 D_1^{2(j-1)} = D_0^2 \frac{1 - D_1^{2i}}{1 - D_1^2} .$$ □

This conclusion about the total correlation is very similar to that of combiners with one memory bit[7].

3 Conclusion

We demonstrate that Theorem 1 gives all the functions with maximum correlation coefficient for even *n*. We also study the "total correlation" of summation generator. However, there are still many problems that haven't been solved. For even n, the values of $d_1(\varpi)$'s haven't been determined. If the values were given, we can compute the correlation coefficients between the current output bit and all the linear functions of the inputs. Golić's conjecture is not proved for odd *n* where the least significant bit of the carry $S_t^{(0)}$ is not balanced. By correlation analysis, we can see that summation generator is not very strong. So good generator with memory should be found. Some new design criterions of combiners with memory were pointed out in Ref.[12], but there are still many important

problems having not been solved. Because combiners with memory have many advantages over memoryless ones, the work in this area is very significant.

References:

[1] Siegenthaler T. Correlation immunity of nonlinear combining functions for cryptographic applications. IEEE Transactions on Information Theory, 1984,IT-30(9):776~780.

[2] Siegenthaler T. Decrypting a class of stream ciphers using ciphertext only. IEEE Transactions on Computers, 1985,C-34(1):81~85.

[3] Meier W, Staffelbach O. Nonlinear criteria for cryptographic functions. In: Advances in Cryptology-Eurocrypt'89. Berlin: Springer-Verlag, 1990. 549~562.

[4] Meier W, Staffelbach O. Fast correlation attacks on certain stream ciphers. Journal of Cryptology, 1989,1(3):159~176.

[5] Chepyzhov V, Smeets B. On a fast attack on stream ciphers. In: Advances in Cryptology-Eurocrypt'91. Lecture Notes in Computer Science. Vol. 547, Berlin: Springer-Verlag, 1991. 176~185.

[6] Rueppel RA. Correlation immunity and the summation generator. In: Advances in Cryptology-Crypto'86. Berlin: Springer-Verlag, 1986. 260~272.

[7] Meier W, Staffelbach O. Correlation properties of combiner with memory in stream cipher. Journal of Cryptology, 1992,15:67~86.

[8] Staffelbach O, Meier W. Cryptographic significance of the carry for ciphers based on integer addition. In: Advances in Cryptology-Crypto'90. Lecture Notes in Computer Science, Vol.537, Berlin: Springer-Verlag, 1991. 601~614.

[9] Golic JD, Salmasizadeh M, Dawson E. Fast correlation attack on the summation generator. Journal of Cryptology, 2000,13: 245~262.

[10] Dawson E, Clark A. Divide and conquer attacks on certain classes of stream ciphers. Cryptologia, 1994,18(1):25~40.

[11] Klapper A, Goresky M. Cryptanalysis based on 2-adic rational approximation. In: Advances in Cryptology-Crypto'95. Lecture Notes in Computer Science, Vol.963, Berlin: Springer-Verlag, 1995. 262~273.

[12] Golić JD. Correlation properties of a general binary combiner with memory. Journal of Cryptology, 1996,9:111~126.