Front. Electr. Electron. Eng. China 2007, 2(4): 435–439
DOI 10.1007/s11460-007-0081-0

RESEARCH ARTICLE

LI Chao, WANG Wenling, HU Pengsong

Differential attack on nonlinear combined sequences

Abstract By using the coding properties and statistic properties of the plaintext, the differential properties of the key stream sequences generated by a nonlinear combined generator were analyzed. Then a differential attack algorithm on the nonlinear combined sequences was proposed. At last, an attack example adopting the differential attack algorithm was presented.

Keywords combined generator, differential attack, differential position set, differential validity

1 Introduction

Nonlinear combined generators based on linear feedback shift register (LFSR) and nonlinear combined function have wide applications in the design and analysis of stream ciphers. Currently, two kinds of the most efficient attack approaches to such systems are correlation attacks and linear cryptanalysis, both of which make use of certain correlation properties between the input and output of the combined function f. A correlation attack called "divide-and-conquer" was proposed in Ref. [1], and a fast correlation attack by using low-density parity codes to conduct iterative probability decoding was presented in Ref. [2]. Some improvements on correlation attacks have been discussed in Refs. [3,4].

The differential attack proposed by Biham and Shamir in the early 1990s has wide applications in the research of block ciphers [5]. However, it has rarely been used in the analysis of stream ciphers for a long time [6–8]. The differential attack proposed in this paper is a kind of cipher-text-only cryptanalysis. By using the coding properties and the statistic properties of the plaintext, the differential properties of the key stream sequences which are generated by a nonlinear combined generator are analyzed. Then a differential attack algorithm on the nonlinear combined sequences is proposed, and an attack example using the differential attack algorithm is presented.

Translated from *Journal of National University of Defense Technology*, 2006, 28(4): 78–82 [译自: 国防科技大学学报]

LI Chao (✉), WANG Wenling, HU Pengsong
College of Science, National University of Defense Technology, Changsha 410073, China
E-mail: Lichao_nudt@sina.com

2 Basic concepts of difference

Definition 1 Let $A = \{a_1, a_2,\ldots,a_r\}$ be a binary sequence of length r, and $S = \{(i_1, j_1), (i_2, j_2),\ldots,(i_t, j_t)\}$, where the elements of the set S are two-dimensional arrays in the set of positive integers. If $1 \leqslant i_k, j_k \leqslant r$ holds for any $1 \leqslant k \leqslant t$, then the set $\left\{a_{i_k} \oplus a_{j_k} \middle| (i_k, j_k) \in S\right\}$ is called a differential set of A with respect to S, and S is called a differential position set of A. The whole differential position sets of A is denoted as U_A.

Definition 2 Let $A = \{a_1, a_2,\ldots,a_r\}$ be a binary sequence of length r. S is a differential position set of A and $\Delta_s A$ is a differential set of A with respect to S. Let $P_s A = P\{x = 0 | x \in \Delta_s A\} = 1/2 + \delta$. If $|\delta| > 0$, then A is called δ-differential validity with respect to S. Otherwise, it is called differential invalidity with respect to S. Similarly, differential validity can be defined by $P_s A = P\{x = 1 | x \in \Delta_s A\}$.

First, the coding properties and statistic properties of the plaintext should be briefly introduced. As is well known, the plaintext needs to be encoded into binary stream data before it is encrypted. The plaintext stream data always reflect some designated information in a certain circumstance and consequently it displays some statistical features. For example, word-based stream data can reflect the distinct style or manner of writing. The stream data based on voice signals and pictures also have obvious statistical features. As a result, it is supposed that the plaintext stream data $M = \{m_1, m_2,\ldots,m_r\}$ has the following property T: plaintext stream data M is the sum of all the efficient information expressed in some certain coding modes. The coding mode of the plaintext is not emphasized for the sake of convenience.

Definition 3 Let plaintext stream $M = \{m_1, m_2,\ldots,m_r\}$ possess the property T and U_M be the whole differential position set of M. For any positive integer i, S^* is called the plaintext differentially optimal for i. If S^* is a subset of U_M, then $|S^*| = i$ and $|P_S M - 1/2| = \max\{|P_S M - 1/2| | S \in U_M, |S| = i\}$.

3 Differential attack

The conditions and models for cryptanalysis will be given at first. For a nonlinear combined generator (Fig. 1), suppose that the characteristic polynomials of those LFSRs are known, and they are primitive polynomials with degree $r_i(1\leqslant i\leqslant n)$ respectively. Let nonlinear combined function $f(x_1, x_2,\ldots,x_n)$ be non-correlation-immune balanced function. The cipher-text stream is denoted by $C=\{c_1,c_2,\ldots,c_n\}$. The output signals for the former N steps of LFSR are denoted by $\left\{x_1^i,\ x_2^i,\ldots,x_N^i\right\}\left(1\leqslant i\leqslant n\right)$ and the corresponding initial state is X^i, which means $X^i=\left(x_1^i,\ x_2^i,\ldots,x_{r_i}^i\right)\in F_2^{r_i}$. The output of $f(x_1, x_2,\ldots,x_n)$ (i.e. key stream sequence) is denoted as $Z=\{z_1, z_2,\ldots,z_N\}$.

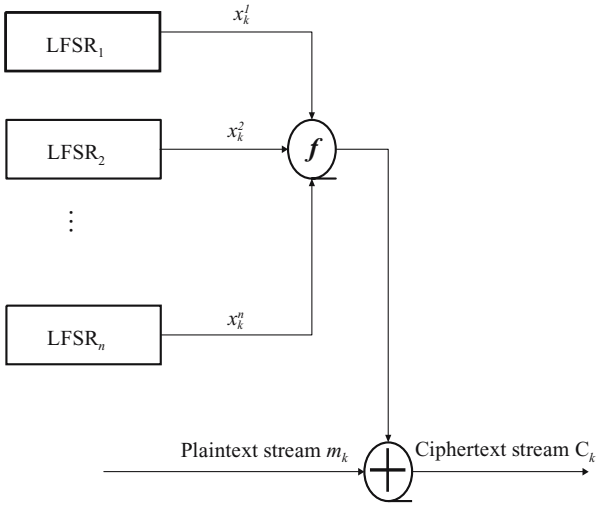

Fig. 1 Nonlinear combined sequence cipher

Due to the primitive polynomials of LFSRs, the periods of the output sequences generated by these LFSRs with the non-zero initial states are maximal. Therefore, it can be assumed that the inputs of combined function f are all independent binary random variables with the same distribution. Furthermore, for any $1\leqslant i\leqslant n$ and $1\leqslant k\leqslant N$, $P\left(x_k^i=0\right)=P\left(x_k^i=1\right)=1/2$ holds. Generally speaking, as a key stream sequence, it should have favorable pseudo-random characteristics. Therefore, the outputs of the combined function f can also be considered as some independent binary random variables with the same distribution for any $k(1\leqslant k\leqslant N)$. Thus $P(z_k=0)=P(z_k=1)=1/2$ is approximately obtained.

Definition 4 If the sequence $\left\{x_1^i,\ x_2^i,\ldots,x_N^i\right\}\left(1\leqslant i\leqslant n\right)$ is generated by the ith LFSR with the initial state $X^i\in F_2^{r_i}$, then a set of two-dimensional vectors $\lambda_{X^i}\left(1\leqslant i\leqslant n\right)$ is defined as follows:

$$\lambda_{X^i}=\left\{(k,l)\middle|x_k^i\oplus x_l^i=0,1\leqslant k,l\leqslant N\right\} \tag{1}$$

Lemma 1 Let the key stream sequence $Z=\{z_1,z_2,\ldots,z_N\}$ be generated by the above model with the initial state $X^i\in F_2^{r_i}\left(1\leqslant i\leqslant n\right)$, and the set λ_{X^i} defined by Eq. (1). Then there exists $i(1\leqslant i\leqslant n)$ and $\varepsilon(0<\varepsilon\leqslant 1/2)$ such that $P\left\{z_k\oplus z_l=0\middle|(k,l)\in\lambda_{X^i}\right\}=1/2+\varepsilon$.

Proof Because $x_k^i\left(1\leqslant i\leqslant n,1\leqslant k\leqslant N\right)$ can be considered as some independent binary random variables with the same distribution, then $P\left(x_k^i=0\right)=P\left(x_k^i=1\right)=1/2$ and note that $f(x_1,\ldots,x_n)$ is a non-correlation-immune balanced function, there exists $i(1\leqslant i\leqslant n)$ and $\xi(0<|\xi|\leqslant 1/2)$ such that $P\left\{f(x_k^1,\ldots,x_k^n)\oplus x_k^i=0\right\}=1/2+\xi$. Thus

$$\begin{aligned}
&P\left\{z_k\oplus z_l=0\middle|(k,l)\in\lambda_{X^i}\right\}\\
&=P\left\{f(x_k^1,\ldots,x_k^n)\oplus f(x_l^1,\ldots,x_l^n)=0\middle|(k,l)\in\lambda_{X^i}\right\}\\
&=P\left\{f(x_k^1,\ldots,x_k^n)\oplus x_k^i\oplus f(x_l^1,\ldots,x_l^n)\right.\\
&\quad\left.\oplus x_l^i=0\middle|(k,l)\in\lambda_{X^i}\right\}\\
&=P\left\{f(x_k^1,\ldots,x_k^n)\oplus x_k^i=0\right\}\bullet P\left\{f(x_l^1,\ldots,x_l^n)\oplus x_l^i=0\right\}\\
&\quad+P\left\{f(x_k^1,\ldots,x_k^n)\oplus x_k^i=1\right\}\bullet P\left\{f(x_l^1,\ldots,x_l^n)\oplus x_l^i=1\right\}\\
&=\left(\frac{1}{2}+\xi\right)^2+\left(\frac{1}{2}-\xi\right)^2\\
&=\frac{1}{2}+2\xi^2
\end{aligned}$$

$0<2\xi^2\leqslant 1/2$ is obtained as $0<|\xi|\leqslant 1/2$. Let $\varepsilon=2\xi^2$, then Lemma 1 is proved.

Lemma 2 Let $Z=\{z_1,z_2,\ldots,z_N\}$ be generated by the above model with the initial state $X^i\in F_2^{r_i}\left(1\leqslant i\leqslant n\right)$. Then for any i and $\tilde{X}^i\in F_2^{r_i}$, if $\tilde{X}^i\neq X^i$, $P\left\{z_k\oplus z_l=0\middle|(k,l)\in\lambda_{\tilde{X}^i}\right\}=1/2$ is obtained, where $\lambda_{\tilde{X}^i}$ is defined by Eq. (1).

Proof For any i and $\tilde{X}^i\in F_2^{r_i}$, let $\left\{\tilde{x}_1^i,\tilde{x}_2^i,\ldots,\tilde{x}_N^i\right\}$ be generated by the ith LFSR in the above model with the initial state $\tilde{X}^i$, so the following formula can be obtained:

$$\begin{aligned}
&P\left\{z_k\oplus z_l=0\middle|(k,l)\in\lambda_{\tilde{X}^i}\right\}\\
&=P\left\{f(x_k^1,\ x_k^2,\ldots,x_k^n)\right.\\
&\quad\left.\oplus f(x_l^1,\ x_l^2,\ldots,x_l^n)=0\middle|(k,l)\in\lambda_{\tilde{X}^i}\right\}\\
&=P\left\{f(x_k^1,\ x_k^2,\ldots,x_k^n)\oplus f(x_l^1,\ x_l^2,\ldots,x_l^n)\right.\\
&\quad\left.\oplus\tilde{x}_k^i\oplus\tilde{x}_l^i=0\middle|(k,l)\in\lambda_{\tilde{X}^i}\right\}\\
&=P\left\{f(x_k^1,\ x_k^2,\ldots,x_k^n)\oplus\tilde{x}_k^i=0\right\}\\
&\quad\bullet P\left\{f(x_l^1,\ x_l^2,\ldots,x_l^n)\oplus\tilde{x}_l^i=0\right\}\\
&\quad+P\left\{f(x_k^1,\ x_k^2,\ldots,x_k^n)\oplus\tilde{x}_k^i=1\right\}\\
&\quad\bullet P\left\{f(x_l^1,\ x_l^2,\ldots,x_l^n)\oplus\tilde{x}_l^i=1\right\}\\
&=\left(\frac{1}{2}\right)^2+\left(\frac{1}{2}\right)^2=\frac{1}{2}
\end{aligned}$$

Theorem 1 Denote the cipher-text by $C = \{c_1, c_2,\ldots,c_N\}$. Suppose that the plaintext is δ_S-differential validity about differential position set S. If $Z = \{z_1,z_2,\ldots,z_N\}$ is generated by the above model with initial state $X^i \in F_2^{r_i}\ (1 \leqslant i \leqslant n)$, then there exists $i(1 \leqslant i \leqslant n)$ and $\varepsilon(0 \leqslant \varepsilon \leqslant 1/2)$ such that

$$P\left\{c_k \oplus c_l = 0 \middle| (k,l) \in \lambda_{X^i} \cap S\right\} = \frac{1}{2} + 2\delta_S\varepsilon$$

Proof Denote the plaintext stream by $M = \{m_1, m_2, \ldots,m_N\}$. Then $C = \{c_1, c_2,\ldots,c_N\} = \{z_1 \oplus m_1, z_2 \oplus m_2,\ldots, z_N \oplus m_N\}$. Because the plaintext is δ_S-differential validity with respect to differential position set S, the following formula can be obtained

$$P_S M = P\left\{m_k \oplus m_l = 0 \middle| (k,l) \in S\right\} = \frac{1}{2} + \delta_S$$

According to Lemma 1, there exists $i(1 \leqslant i \leqslant n)$ and $\varepsilon(0 < \varepsilon \leqslant 1/2)$ such that

$$P\left\{z_k \oplus z_l = 0 \middle| (k,l) \in \lambda_{X^i}\right\} = \frac{1}{2} + \varepsilon$$

Therefore

$$\begin{aligned}
&P\left\{c_k \oplus c_l = 0 \middle| (k,l) \in \lambda_{X^i} \cup S\right\} \\
&= P\left\{z_k \oplus m_k \oplus z_l \oplus m_l = 0 \middle| (k,l) \in \lambda_{X^i} \cup S\right\} \\
&= P\left\{z_k \oplus z_l = 0\right\} \bullet P\left\{m_k \oplus m_l = 0\right\} \\
&\quad + P\left\{z_k \oplus z_l = 1\right\} \bullet P\left\{m_k \oplus m_l = 1\right\} \\
&= \left(\frac{1}{2} + \varepsilon\right)\left(\frac{1}{2} + \delta_S\right) + \left(\frac{1}{2} - \varepsilon\right)\left(\frac{1}{2} - \delta_S\right) \\
&= \frac{1}{2} + 2\delta_S\varepsilon
\end{aligned}$$

Theorem 2 Denote the cipher-text by $C = \{c_1, c_2,\ldots,c_N\}$. If $Z = \{z_1,z_2,\ldots,z_N\}$ is generated by the above model with initial state $X^i \in F_2^{r_i}\ (1 \leqslant i \leqslant n)$, then for any i and $X^i \neq \not{X}^i \in F_2^{r_i}$, the following formula can be obtained $P\left\{c_k \oplus c_l = 0 \middle| (k,l) \in \lambda_{\not{X}^i} \cap S\right\} = \frac{1}{2}$.

Proof Denote the plaintext stream by $M = \{m_1, m_2,\ldots,m_N\}$. Then $C = \{c_1, c_2,\ldots,c_N\} = \{z_1 \oplus m_1, z_2 \oplus m_2,\ldots, z_N \oplus m_N\}$. According to Lemma 2, for any $\not{X}^i \in F_2^{r_i}$, $\not{X}^i \neq X^i$ $(1 \leqslant i \leqslant n)$, $P\left\{z_k \oplus z_l = 0 \middle| (k,l) \in \lambda_{X^i}\right\} = 1/2$. Therefore

$$\begin{aligned}
&P\left\{c_k \oplus c_l = 0 \middle| (k,l) \in \lambda_{\not{X}^i} \cup S\right\} \\
&= P\left\{z_k \oplus m_k \oplus z_l \oplus m_l = 0 \middle| (k,l) \in \lambda_{\not{X}^i} \cup S\right\} \\
&= P\left\{z_k \oplus z_l = 0\right\} \bullet P\left\{m_k \oplus m_l = 0\right\} \\
&\quad + P\left\{z_k \oplus z_l = 1\right\} \bullet P\left\{m_k \oplus m_l = 1\right\} \\
&= \frac{1}{2} P\left\{m_k \oplus m_l = 0\right\} + \frac{1}{2} P\left\{m_k \oplus m_l = 1\right\} = \frac{1}{2}
\end{aligned}$$

From Theorems 1 and 2, the following corollaries can be obtained.

Corollary 1 Denote the cipher-text by $C = \{c_1, c_2,\ldots,c_N\}$. Suppose that the plaintext is δ_S-differential validity about differential positional set S. If $Z = \{z_1,z_2,\ldots,z_N\}$ is generated by the above model with initial state $X^i \in F_2^{r_i}\ (1 \leqslant i \leqslant n)$ while let $\Delta_N^i = \Delta_{\lambda_{X^i} \cap S} C$, then there exists $i(1 \leqslant i \leqslant n)$ and $\varepsilon(0 \leqslant \varepsilon \leqslant 1/2)$ such that

$$\lim_{N\to\infty} \frac{\sum_{x \in \Delta_N^i} x}{\left|\Delta_N^i\right|} = \frac{1}{2} - 2\delta_S\varepsilon$$

Corollary 2 Denote the cipher-text by $C = \{c_1, c_2,\ldots, c_N\}$. If $Z = \{z_1,z_2,\ldots,z_N\}$ is generated by the above model with initial state $X^i \in F_2^{r_i}\ (1 \leqslant i \leqslant n)$, then as to $\forall i$ and $\not{X}^i \in F_2^{r_i}$, let $\not{\Delta}_N^i = \Delta_{\lambda_{\not{X}^i} \cap S} C$ and if $\not{X}^i \neq X^i$, the following formula will be obtained:

$$\lim_{N\to\infty} \frac{\sum_{x \in \not{\Delta}_N^i} x}{\left|\not{\Delta}_N^i\right|} = \frac{1}{2}$$

4 Differential attack algorithm

In a nonlinear combined generator (Fig. 1), suppose that the plaintext is δ_S-differential validity with respect to differential position set S and $f(x_1, x_2,\ldots,x_n)$ is a non-correlation-immune balanced function. Then the distinct input x_i that presents certain correlations with the output signals of function f can be found out. Consequently, $2\delta_S\varepsilon$ can be solved by calculating the value of $\xi = P\{f(x_1, x_2,\ldots,x_n) \oplus x_i = 0\} - 1/2$. As is well known, the plaintext streams have some properties such as δ_S-differential efficiency. Therefore, based on Theorems 1 and 2 and their corollaries, the initial states of $\mathrm{LFSR_i}$ can be found via utilizing the known cipher-text $C = \{c_1, c_2,\ldots,c_N\}$ according to the following algorithm.

Step 1 Choose a $X^i \in F_2^{r_i}$, $X^i \neq 0$ randomly. Employ $\mathrm{LFSR_i}$ to produce a stream $\left\{x_1^i, x_2^i,\ldots,x_r^i\right\}$ in which $r = 2^{r_i} - 1$ and the period of the stream is $2^{r_i} - 1$.

Step 2 Set the initial value of WZ as 0.

Step 3 Take WZ as the starting point to obtain N signals $\left\{y_1, y_2,\ldots,y_N\right\} = \left\{x_{\mathrm{WZ}+1}^i, x_{\mathrm{WZ}+2}^i,\ldots,x_{\mathrm{WZ}+N}^i\right\}$ from $\left\{x_1^i, x_2^i,\ldots,x_r^i\right\}$. Use $Y = \left(y_1, y_2,\ldots,y_{r_i}\right)$ to obtain two-dimensional arrays set $\lambda_Y \cap S$ according to differential position set S of the plaintext and Definition 4.

Step 4 Calculate the differential set $\Delta_{\lambda_Y \cap S} C$ of cipher-text $C = \{c_1, c_2,\ldots,c_N\}$ about new differential position set $\lambda_Y \cap S$ and let P_{WZ} denote the probability of zero in this set. If $P_{\mathrm{WZ}} \to 1/2 + 2\delta_S\varepsilon$, accept $\left(y_1, y_2,\ldots,y_{r_i}\right)$ derived from Step 3 as the initial state of $\mathrm{LFSR_i}$, i.e. the sub-key.

Step 5 Let $\mathrm{WZ} = \mathrm{WZ} + 1$. If $\mathrm{WZ} > 2^{r_i} - 1$, proceed to Step 6; otherwise, go to Step 3.

Step 6 End the algorithm.

The above differential attack algorithm is a divide-and-conquer cryptanalysis actually. It identifies the sub-key to a LFSR by making some conditional judgment. The algorithm that can be brought into effect depends on various conditions given in Section 2. In fact, the assumptions of these conditions are all reasonable [7].

5 An cryptanalysis example

Suppose that there are eight LFSRs in the model. The feedback polynomials respectively are $g_1(x)=x^{17}+x^3+1$, $g_2(x)=x^{20}+x^3+1$, $g_3(x)=x^{23}+x^{20}+1$, $g_4(x)=x^{29}+x^{26}+1$, $g_5(x)=x^{25}+x^{20}+x^{12}+x^8+1$, $g_6(x)=x^{31}+x^{24}+x^{16}+x^{12}+1$, $g_7(x)=x^{33}+x^{28}+x^{24}+x^4+1$, $g_8(x)=x^{39}+x^{36}+x^{28}+x^4+1$. The combined function is

$$f=\{\text{E25047C342F8061638519519862819536 5}\\ \text{DD937F5BF4B702B17EFED92E2D83B7}\}$$

Some words are chosen from the introduction of this paper as the plaintext for the sake of convenient analysis. GB code is used to encode the plaintext stream. Thus the plaintext stream is

$$M=\{\text{B7C7CFDFD0D4D7E9BACFC9FAB3}\\ \text{C9C6F7D4DAD0F2C1D0C3DCC}\ldots\}$$

Now one set of initial states is chosen randomly to encrypt this plaintext. The initial states chosen randomly are as follows:

187F7, 856BD, F2ACF, 649F525, 19F037E, 31F62B97, 1974D1905, 64F89DDB22

Each character in the above-mentioned initial states is a Hex digit. If the initial state is longer than its LFSR, some bits will be cut off from the beginning to ensure that its length is equivalent to that of the LFSR. Otherwise, some 0s will be added at the beginning of the initial states.

According to the statistic results, for integers k, M is 1/2-differential validity about position set $S_k=\{8(i,i+j)\ |1\leqslant j\leqslant k,8(i+j)\leqslant|\text{M}|\}$. For f, the following conclusions are obtained.

1) f is a balanced function.

2) If the inputs of f are independent binary random variables with symmetrical distribution, then $P\{f\oplus x_1=0\}\approx 0.601\ 56$. In the following examples, let $S=S_3$ be differential positional set of the plaintext. Thus $2\delta_S\varepsilon\approx 0.020\ 63$ can be obtained.

According to the algorithm described in Section 4, any $X^1\in F_2^{17}, X^1\neq 0$ is chosen first to generate a stream $\{x_1^1,\ldots,x_{2^{17}-1}^1\}$ whose length is $2^{17}-1$. Calculate P_{WZ} for each position of this stream and analyze the frequency distribution of P_{WZ} in each small probability interval (Suppose that continuous 10 000 bits of cipher-text can be obtained from the experimental data). Table 1 shows the frequency distribution of P_{WZ}.

Table 1 Frequency distribution of P_{WZ}

Distribution interval	Frequency of P_{WZ}
[0.498 5, 0.499 5]	69
[0.499 5, 0.500 5]	7 924
[0.500 5, 0.501 5]	50 950
[0.501 5, 0.502 5]	44 295
[0.502 5, 0.503 5]	18 598
[0.503 5, 0.504 5]	6 338
[0.504 5, 0.505 5]	1 982
[0.505 5, 0.506 5]	634
[0.506 5, 0.507 5]	189
[0.507 5, 0.508 5]	68
[0.508 5, 0.509 5]	15
[0.509 5, 0.510 5]	6
[0.510 5, 0.511 5]	1
[0.512 5, 0.513 5]	2
[0.515 5, 0.516 5]	1

For the right initial state of LFSR_1, $P_{\text{WZ}}\approx 0.516\ 47\rightarrow 0.5+0.020\ 63$ can be obtained. While for the others, P_{WZ}s all distribute inside the interval [0.489 5, 0.513 5]. These experimental data show that the differential attack algorithm proposed in this paper can be taken into effect for acquiring the initial state (sub-key) of the shift register sequence in the above model.

6 Conclusion

A kind of cipher-text-only cryptanalysis is presented in the above. By using the coding properties and the statistic property of the plaintext, the differential properties of the cipher-text sequences generated by a nonlinear combined generator are analyzed. A differential attack algorithm on the nonlinear combined sequences was proposed. It is also proved that this method could always be effective provided that $2\delta_S\varepsilon\neq 0$ and the length of the cipher-text sequence is long enough. In fact, there are still some questions that need to be further resolved about the algorithm proposed in this paper, for instance, how to choose a differential position set of plaintext and achieve differential optimization under a certain statistic value; how long about the cipher-text should be obtained to make this differential cryptanalysis effective and how to take advantage of the process relationships of the shift register to quickly determine differential positional set $\lambda_Y\bigcap S$ of cipher C and to calculate P_{WZ}.

Acknowledgements This work was supported by the National Natural Science Foundation of China (No. 60573028) and Research Foundation of National University of Defense Technology (No. JC-02-02).

References

1. Siegenthaler T. Correlation immunity of nonlinear combining function for cryptographic application. IEEE Transactions on Information Theory, 1984, 30(6): 776−780

2. Meier W, Staffelbach O. Fast correlation cryptanalysis on certain stream ciphers. In: Advances in Cryptology- EUROCRYPT`88. Berlin: Springer-Verlag, 1988, 301−314
3. Golic J D, Salmasizadeh M, Dawson E. Fast correlation cryptanalysis on the summation generator. Journal of Cryptology, 2000, 13: 245−262
4. Zhang Weiming, Li Shiqu. Muiti-linear correlation cryptanalysis of the combiner sequence. Chinese Journal of Electronics, 2005, 33(3): 427−432 (in Chinese)
5. Biham E, Shamir A. Differential Cryptanalysis of the Data Encryption Standard. Berlin: Springer-Verlag, 1993
6. Feng Dengguo, Wu Wenling. Design and Analysis of Block Ciphers. Beijing: Tsinghua University Press, 2000 (in Chinese)
7. Feng Dengguo. Cryptanalysis. Beijing: Tsinghua University Press, 2000 (in Chinese)
8. Li Chao, Huang Jianzhong, Xiang Panpan. Applying the differential cryptanalysis in the analysis of sequence ciphers. Applied Science Sinica, 2004, 22(2): 127−131 (in Chinese)