Linear Sequential Circuit Approximation of Achterbahn Stream Cipher

Shazia Afreen

[1]Research Associate, National University of Science and Technology, Pakistan
shazaf21@gmail.com

ABSTRACT
Achterbahn stream cipher is proposed as a candidate for ECRYPT eSTREAM project which deals with key of length 80-bit. The linear distinguishing attack,which aims at distinguishing the keystream from purely random keystream,is employed to Achterbahn stream cipher. A linear distinguishing attack is based on linear sequential circuit approximation technique which distinguishes statistical bias in the keystream. In order to build the distinguisher, linear approximations of both non-linear feedback shift register (NLFSR) and the non-linear Boolean combining function $R: F_2^8 \rightarrow F_2$ are used. The keystream sequence generated by this algorithm consist a distinguisher with its probability bias 2^{-1809}. Thus, to distinguish the Achterbahn, we only need $\frac{1}{\varepsilon^2} = (2^{1809})^2 = 2^{3618}$ keystream bits and the time complexity is about $\frac{10}{\varepsilon^2} = 2^{3621.3}$ which is much higher than the exhaustive key search $O(2^{80})$.

Keywords
Linear Distinguishing Attack, Linear Sequential Circuit Approximation, Achterbahn Stream Cipher

1. INTRODUCTION

1.1 Background

A linear distinguishing cryptanalysis technique for stream ciphers was presented by Golic in 1994[3] which enable us to distinguish the keystream from a truly random sequence. The main idea in distinguishing attack is to introduce some biased noise component and form linear approximations of nonlinear parts of the cipher with linear functions to build linear distinguisher. The efficiency of linear approximation functions is then measured by its correlation. Such correlation is used for distinguishing the keystream sequence from a random sequence by a standard chi-square frequency statistical test. To distinguish a sequence from purely random binary sequence with error probability less than 10^{-3}, the length of the observed keystream sequence should not be larger than $\frac{10}{\varepsilon^2}$where ε is the correlation coefficient of the random variable$x$, defined as $\varepsilon = 1 - 2\Pr[x = 1]$. If the key length is$k$, the statistical weakness is effective if and only if the correlation coefficient is greater than $2^{-k/2}$.
Bias linear relations are usually found by replacing the nonlinear components in the cipher by appropriate linear approximation. Efficient techniques for finding biased linear relations among the keystream bits are presented in [3, 4]. General method for establishing such relation is the correlation attack against the combiner functions or the filter functions and linear sequential circuit approximation introduced by Golic [1].

1.2 Contribution of the Paper

Our contribution in this paper is to mount a distinguishing attack based on linear sequential circuit approximation i.e. use linear approximations of the cipher on Achterbahn stream cipher. First, we linearize the behavior of the nonlinear update state functions by considering linear approximation of each function. Next, we linearize combining function, like the output function. Then we describe how to get the bias of all these linear approximations. The keystream sequence generated by Achterbahn with its probability bias 2^{-1809} shows that there is a distinguisher. Thus, we only need $\frac{1}{\varepsilon^2} = (2^{1809})^2 = 2^{3618}$keystream bits and the time complexity is about $\frac{10}{\varepsilon^2} = 2^{3621.3}$to distinguish the keystream of Achterbahn which is much higher than the exhaustive key search of $O(2^{80})$.

2. BRIEF DESCRIPTION OF ACHTERBAHN STREAM CIPHER

The stream cipher Achterbahn is a binary additive stream cipher with 80-bits of key length and 64-bits of initial vector [5]. The core of the keystream generator consists of eight primitive binary nonlinear feedback shift registers (NLFSR) labeled with capital letters $A, B, \ldots, H$. The output of each NLFSR contributes with a linear feedforward logic described by filter polynomials $a(x), b(x), \ldots, h(x)$. The linear feedforward logics then contribute the Boolean combining function $R(y_1, y_2, \ldots, y_8)$which then produces the output keystream.

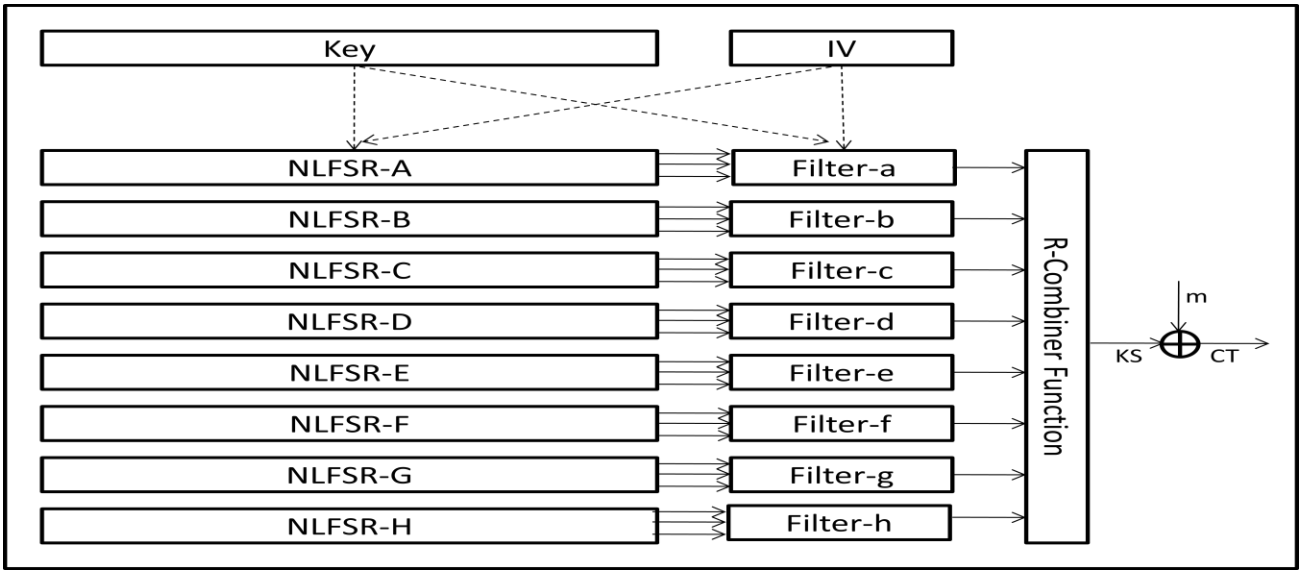

Figure 1: Block Diagram of Achterbahn Stream Cipher

2.1 The Boolean combining function

The Boolean combining function $R: F_2^8 \to F_2$ has algebraic degree 3. The algebraic normal form of R is:

$$R(y_1, y_2, \dots, y_8) = y_1 + y_2 + y_3 + y_4 + y_5y_7 + y_6y_7 + y_6y_8 + y_5y_6y_7 + y_6y_7y_8$$

2.2 The feedback shift registers

The keystream generator (KSG) consistsofeight binary primitive nonlinear feedback shift registers, labeled by the capital letters $A, B, \dots, H$. The feedback functions of the eight NLFSR's are given by

$$A(x_0, x_1, \dots, x_{21}) = x_0 + x_5 + x_6 + x_7 + x_{10} + x_{11} + x_{12} + x_{13} + x_{17} + x_{20} + x_2x_7 + x_4x_{14} + x_8x_9 + x_{10}x_{11} + x_1x_4x_{11} + x_1x_4x_{13}x_{14}$$

$$B(x_0, x_1, \dots, x_{22}) = x_0 + x_6 + x_7 + x_9 + x_{11} + x_{12} + x_{14} + x_{15} + x_{17} + x_{19} + x_{21} + x_1x_4 + x_2x_7 + x_5x_9 + x_6x_{10} + x_2x_4x_8 + x_1x_3x_5x_{10} + x_4x_{11}x_{12}x_{13}$$

$$C(x_0, x_1, \dots, x_{24}) = x_0 + x_1 + x_3 + x_5 + x_6 + x_7 + x_9 + x_{12} + x_{14} + x_{15} + x_{17} + x_{18} + x_{22} + x_1x_6 + x_4x_{13} + x_8x_{16} + x_{12}x_{15} + x_5x_{11}x_{14} + x_1x_4x_{11}x_{15} + x_2x_5x_8x_{10}$$

$$D(x_0, x_1, \dots, x_{25}) = x_0 + x_1 + x_4 + x_5 + x_7 + x_8 + x_9 + x_{13} + x_{14} + x_{16} + x_{20} + x_{24} + x_1x_6 + x_4x_7 + x_{12}x_{16} + x_{15}x_{17} + x_4x_{15}x_{17} + x_7x_9x_{10} + x_1x_3x_{14}x_{16} + x_8x_{11}x_{12}x_{17}$$

$$E(x_0, x_1, \dots, x_{26}) = x_0 + x_1 + x_2 + x_6 + x_8 + x_9 + x_{10} + x_{13} + x_{14} + x_{16} + x_{19} + x_{21} + x_{23} + x_1x_8 + x_3x_{12} + x_{11}x_{17} + x_{15}x_{18} + x_5x_6x_{15} + x_3x_5x_{16}x_{17} + x_7x_{12}x_{14}x_{15}$$

$$F(x_0, x_1, \dots, x_{27}) = x_0 + x_1 + x_2 + x_7 + x_{15} + x_{17} + x_{19} + x_{20} + x_{22} + x_{27} + x_9x_{17} + x_{10}x_{18} + x_{11}x_{14} + x_{12}x_{13} + x_5x_{14}x_{19} + x_6x_{10}x_{12} + x_6x_9x_{17}x_{18} + x_{10}x_{12}x_{19}x_{20}$$

$$G(x_0, x_1, \dots, x_{28}) = x_0 + x_2 + x_3 + x_5 + x_6 + x_9 + x_{14} + x_{15} + x_{16} + x_{18} + x_{21} + x_{27} + x_5x_7 + x_6x_{20} + x_{10}x_{14} + x_{13}x_{18} + x_8x_{19}x_{21} + x_{11}x_{16}x_{18} + x_1x_5x_{15}x_{21} + x_2x_7x_{17}x_{20}$$

$$H(x_0, x_1, \dots, x_{30}) = x_0 + x_3 + x_5 + x_7 + x_{10} + x_{16} + x_{17} + x_{18} + x_{19} + x_{20} + x_{21} + x_{24} + x_{30} + x_5x_{15} + x_{11}x_{18} + x_{16}x_{22} + x_{17}x_{21} + x_1x_2x_{19} + x_1x_{12}x_{14}x_{17} + x_2x_5x_{13}x_{20}$$

2.3 Linear feedforward functions

Linear feedforward output function takes input from nonlinear feedback shift registers $A, B, \dots, H$. The linear feedforward output function can be described by the filter polynomial. The binary filter polynomial for example $a(x)$ for *NLFSR-A* has degree at most 6. All filter polynomials will have nonzero constant terms. Thus the polynomial $a \epsilon F_2(x)$ has the form

$$a(x) = a_6x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + 1$$

3. A BRIEF DESCRIPTION OF LINEAR SEQUENTIAL CIRCUIT APPROXIMATION

In order to find all non-balanced linear functions of at most$M + 1$ consecutive output bits whose existence is established in Theorem [2], which is given below, one should determine the correlation coefficient for 2^M Boolean functions of Mvariables.

Theorem:

Let the next state function of a binary autonomous finite state machine with M bits of memory be balanced. Then there exist a linear function $L$of $M + 1$binary variable effectively depending on the first variable such that the function $L(z_t, \dots, z_{t-M})$of at most $M + 1$consecutive output bits is a non-balanced function of the initial state variable for each $t \geq M$.

A binary autonomous finite state machine or sequential circuit is defined as:

$$S_t = F(S_{t-1}), t \geq 1 \quad (1)$$

and

$$z_t = f(S_t), t \geq 1 \quad (2)$$

Where $F: GF(2)^M \rightarrow GF(2)^M$ is a next state vector Boolean function, $f: GF(2)^M \rightarrow GF(2)$ is an output Boolean function, $S_t = (s_{1t}, \dots, s_{Mt})$ is the state vector at time$t$, M is the number of memory bits, $z_t$is the output bit at time $t$and $S_0 = (s_{10}, \dots, s_{M0})$is the initial state. A binary keystream generator can be defined as a binary autonomous finite state machine whose initial state, the next state and output functions are controlled by secret key.

3.1 A Framework for Linear Distinguishing Attack

The attack is composed by three stages:

Stage 1:

Find a linear approximation of the output function $f$and each of the component functions of the next state function F. This enables us to express each of these $M+1$ functions as the sum of a linear function and a non-balanced function. The degree of approximation is measured by the corresponding correlation coefficient, which should be different from zero. Note that to determine all linear approximations of Boolean function effectively depending on Mvariables; one may use the Walsh transformation technique which has $O(M2^M)$ computational complexity. In practice, both the output function and the component next state functions effectively depends on small number of variables or can be expressed in terms of such functions. Therefore, the computational complexity of obtaining all the linear approximation along with the corresponding correlation coefficients is considerably smaller than $O((M+1)M2^M)$

Stage 2:

By virtue of obtained linear approximations, the basic equations (1) and (2) becomes

$$S_t = AS_{t-1} + \Delta(S_{t-1}), \quad t \geq 1 \quad (3)$$

$$z_t = BS_t + \varepsilon(S_t), \quad t \geq 1 \quad (4)$$

where$S_t$is $M \times 1$vector, $A$is $M \times M$matrix, B is $1 \times M$vector, Δ is $M \times 1$noise vector, ε is a scalar noise component. Then by using the generating function technique, we obtain a linear function of at most $M+1$consecutive output bits that is expressed as the sum of unbalanced functions of the initial state variable. The linear function

$$u_t = \sum_{i=0}^{M} \varphi_i \, z_{t+i} = \sum_{i=0}^{M} \varphi_i \, \varepsilon(S_{t+i}) + \sum_{j=1}^{M} \sum_{i=0}^{M} c_{i,j} \, \delta_j(S_{t+i-1}) \quad (5)$$

where
$\varphi(x) = \sum_{i=0}^{m} \varphi_i x^i, (m \leq M)$corresponds to the reciprocal of the characteristic polynomial of state transition Matrix $A$of the linear sequential circuit and $c_{i,j} (0 \leq i \leq m, 1 \leq j \leq M)$is the j^{th}element of the M-bit row vector$\sum_{k=0}^{m-i} \varphi_{k+i} BA^k$

Stage 3:

Under the independence assumption of the noise terms, the correlation coefficient of $u_t$denoted by

$\mathcal{E} = \mathcal{E}_i^{hw(\varphi_i)} \prod_{i=0}^{7} \mathcal{E}_i^{hw(c_i)}$, where $hw(.)$ is the weight of a given polynomial. $\varepsilon = \varepsilon_i^{hw(\varphi_i)} \prod_{i=0}^{7} \varepsilon_i^{hw(c_i)}$

The standard chi-square frequency statistical test can then be applied to $\{u_t\}$ to distinguish this sequence from a purely random binary sequence. The distinguishing error probability is less than about 10^{-3}, if the segment length is about $10/\varepsilon^2$. The computational complexity of processing this amount of keystream is $O(10\varepsilon^{-2})$

4. LINEAR SEQUENTIAL CIRCUIT APPROXIMATION OF ACHTERBAHN STREAM CIPHER

In this section, we derive the linear sequential circuit approximation of Achterbahn stream cipher. Let S_t be 211-bit binary column vector which contains the state of eight NLFSRs of Achterbahn at time t, i.e. $(a_0, a_1, \dots, a_{21}, \dots, h_0, h_1, \dots, h_{29})^T$ in the pseudo-code introduced in section 2. The feedback functions of each NLFSR's are the nonlinear parts of the next state functions andthe combining function $R$is nonlinear function.

Stage1:

Let $\varepsilon_{A,o}, \varepsilon_{B,p}, \dots, \varepsilon_{H,v}$be the correlation coefficient of noise vector corresponding to the next state update functions $L_{A,o}, L_{B,p}, \dots, L_{H,v}$,and $\varepsilon_{R,w}$ be the correlation coefficient ofthe scalar noise term corresponding to the linear approximation $L_{R,w}$of R. We can compute the bias of each update function and combing function by exhaustive search over all possible choices for linear approximations for the feedback function and combining function to find the greatest correlation coefficient. The correlation coefficient for the next update functions and nonlinear combiner function is achieved by the following choice:-

Find a linear approximation of each of the next state functions $A, B, \dots, H$and output combining function R. Transform$A(x_0, x_1, \dots, x_{21})$ into multi variable as $L_{A,o}(y_0, y_1, \dots, y_{15}) = O_{15}y_{15} + O_{14}y_{14} + \cdots + O_0 y_0$, where$(y_0, y_1, \dots, y_{15}) =$

$(x_0, x_1, x_2x_4, x_5, \dots, x_{14}, x_{17}, x_{20})$. Thecorrelation coefficient of $A(x_0, x_1, \dots, x_{21})$is $\varepsilon_{A,o} = 2^{-6}$ with the linear approximation$L_{A,o} = x_0 + x_1 + x_5 + x_6 + x_{12} + x_{17} + x_{20}$

Similarly, transform $B(x_0, x_1, \dots, x_{22})$ into multi variable as $L_{B,p}(y_0, y_1, \dots, y_{18}) = p_{18}y_{18} + p_{17}y_{17} + \cdots + p_0y_0$,where $(y_0, y_1, \dots, y_{18}) = (x_0, x_1, , \dots, x_{15}, x_{17}, x_{19}, x_{21})$.The correlation coefficient of $B(x_0, x_1, \dots, x_{22})$is $\varepsilon_{B,p} = 2^{-7}$ with the linear approximation $L_{B,p} = x_0 + x_3 + x_7 + x_{14} + x_{15} + x_{17} + x_{19} + x_{21}$.

Transform$C(x_0, x_1, \dots, x_{24})$into multi variables as$L_{C,q}(y_0, y_1, \dots, y_{19}) = q_{19}y_{19} + q_{18}y_{18} + \cdots + q_0y_0$,where $(y_0, y_1, \dots, y_{19}) = (x_0, x_1, , \dots, x_{18}, x_{22})$.The correlation coefficient of $C(x_0, x_1, \dots, x_{24})$ is $\varepsilon_{c,q} = 2^{-6}$ with the linear approximation $L_{C,q} = x_0 + x_1 + x_3 + x_7 + x_9 + x_{17} + x_{18} + x_{22}$.

Transform $D(x_0, x_1, \dots, x_{25})$ into multi variable as $L_{D,r}(y_0, y_1, \dots, y_{18}) = r_{18}y_{18} + r_{17}y_{17} + \cdots + r_0y_0$,where$(y_0, y_1, \dots, y_{18}) = (x_0, x_1, x_3, \dots, x_{17}, x_{20}, x_{24})$. The correlation coefficient of $D(x_0, x_1, \dots, x_{25})$is $\varepsilon_{D,r} = 2^{-9}$ with the linear approximation $L_{D,r} = x_0 + x_5 + x_6 + x_{13} + x_{20} + x_{24}$.

Transform $E(x_0, x_1, \dots, x_{26})$ into multi variable as$L_{E,s}(y_0, y_1, \dots, y_{20}) = s_{20}y_{20} + s_{19}y_{19} + \cdots + s_0y_0$,where$(y_0, y_1, \dots, y_{20}) = (x_0, x_1, x_2, x_3, x_5, \dots, x_{19}, x_{21}, x_{23})$. The correlation coefficient of $E(x_0, x_1, \dots, x_{26})$is $\varepsilon_{E,s} = 2^{-5}$ with the linear approximation $L_{E,s} = x_0 + x_2 + x_6 + x_9 + x_{10} + x_{11} + x_{12} + x_{13} + x_{14} + x_{19} + x_{21} + x_{23}$.

Transform $F(x_0, x_1, \dots, x_{27})$ into multi variable as $L_{F,t}(y_0, y_1, \dots, y_{18}) = t_{18}y_{18} + t_{17}y_{17} + \cdots + t_0y_0$,where$(y_0, y_1, \dots, y_{18}) = (x_0, x_1, x_2, x_5, \dots, x_7, x_9, \dots, x_{15}, x_{17}, x_{18}, x_{19}, x_{20}, x_{22}, x_{27})$.The correlation coefficient of $F(x_0, x_1, \dots, x_{27})$is $\varepsilon_{F,t} = 2^{-7}$with the linear approximation $L_{F,t} = x_0 + x_1 + x_2 + x_7 + x_{13} + x_{15} + x_{22}+x_{27}$

Transform $\mathrm{G}(x_0, x_1, \dots, x_{28})$ into multi variable as$L_{G,u}(y_0, y_1, \dots, y_{20}) = u_{20}y_{20} + u_{19}y_{19} + \cdots + u_0y_0$,where$(y_0, y_1, \dots, y_{20}) = (x_0, x_1, x_2, x_3, x_5, \dots, x_{11}, x_{13}, \dots, x_{21}, x_{27})$. The correlation coefficient of $\mathrm{G}(x_0, x_1, \dots, x_{28})$is $\varepsilon_{G,u} = 2^{-10}$ with the linear approximation $L_{G,u} = x_0 + x_3 + x_9 + x_{13}+x_{27}$

Transform $H(x_0, x_1, \dots, x_{30})$ into multi variable as $L_{H,v}(y_0, y_1, \dots, y_{20}) = v_{20}y_{20} + v_{19}y_{19} + \cdots + v_0y_0$,where$(y_0, y_1, \dots, y_{20}) = (x_0, x_1, x_2, x_3, x_5, x_7, x_{10}, \dots, x_{22}, x_{24}, x_{30})$. The correlation coefficient of $H(x_0, x_1, \dots, x_{30})$is $\varepsilon_{H,v} = 2^{-7}$ with the linear approximation $L_{H,v} = x_0 + x_1 + x_2 + x_3+x_7 + x_{10} + x_{15} + x_{16} + x_{17}+x_{19} + x_{21} + x_{22} + x_{24}+x_{30}$

Transform $R(x_0, x_1, \dots, x_7)$ into multi variable as $L_{R,w}(y_0, y_1, \dots, y_7) = w_7y_7 + w_6y_6 + \cdots + w_0y_0$,where $(y_0, y_1, \dots, y_7) = (x_0, x_1, \dots, x_7)$. The correlation coefficient of $R(x_0, x_1, \dots, x_7)$is $\varepsilon_{R,w} = 2^{-2}$ with the linear approximation $L_{R,w} = x_0 + x_1 + x_2 + x_3+x_4$

Stage2:

Using the decomposition function of nonlinear function, the linear approximation of (3) and (4) for the Achterbahn could be written as:

$$S_t = AS_{t-1} + H\Delta_t, \quad t \geq 1 \tag{6}$$

$$z_t = BS_t + \gamma_t, \quad t \geq 1 \tag{7}$$

where$H = [h_i]_{211\times 8}$ is a binary matrix whose all entries are zero, except $h_{0,0}$, $h_{22,1}$, $h_{45,2}$, $h_{70,3}$, $h_{96,4}, h_{123,5}$, $h_{151,6}, h_{180,7}$

$$\Delta_t = \left[\delta_{1,t}\delta_{2,t}\delta_{3,t}\delta_{4,t}\delta_{5,t}\delta_{6,t}\delta_{7,t}\delta_{8,t}\right]^T$$

$$\Delta_t = [\delta_0(S_{t-1})\delta_{22}(S_{t-1})\ \ \delta_{45}(S_{t-1})\delta_{70}(S_{t-1})\ \ \delta_{96}(S_{t-1})\ \ \delta_{123}(S_{t-1})\delta_{151}(S_{t-1})\delta_{180}(S_{t-1})]^T$$

is the 8-bit column noise vector corresponding to the next state update function and $\gamma_t = \gamma(S_t)$ is the scalar noise term corresponding to the linear approximation $L_{R,w}$of $R$and $A$and$B$ are as follows:

where$A = [\mathrm{e_i}]_{211\times 211}$ is the identity matrix and each $\mathrm{e_i}, 0 \leq \mathrm{i} \leq 210$ denotes the $(i+1)^{th}$row of identity matrix and

$$e_0 = o_A, e_{22} = p_B, e_{45} = q_C, e_{70} = r_D, e_{96} = s_E, e_{123} = t_F, e_{151} = u_G, e_{180} = v_H$$

Where

$$o_A = o_{15}e_{21} + o_{14}e_{20} + o_{13}e_{19} + o_{12}e_{17} + o_{11}e_{16} + o_{10}e_{15} + o_9e_{14} + o_8e_{13} + o_7e_{12} + o_6e_{11} + o_5e_{10} + o_4e_9 + o_3e_8 + o_2e_7 + o_1e_4 + o_0e_1$$

$$p_B = p_{18}e_{44} + p_{17}e_{43} + p_{16}e_{42} + p_{15}e_{41} + p_{14}e_{40} + p_{13}e_{39} + p_{12}e_{38} + p_{11}e_{37} + p_{10}e_{36} + p_9e_{35} + p_8e_{34} + p_7e_{33} + p_6e_{32} + p_5e_{31} + p_4e_{30} + p_3e_{29} + p_2e_{27} + p_1e_{25} + p_0e_{23}$$

$$q_C = q_{19}e_{69} + q_{18}e_{68} + q_{17}e_{67} + q_{16}e_{66} + q_{15}e_{65} + q_{14}e_{64} + q_{13}e_{63} + q_{12}e_{62} + q_{11}e_{61} + q_{10}e_{60} + q_9e_{59} + q_8e_{58} + q_7e_{57} + q_6e_{56} + q_5e_{55} + q_4e_{54} + q_3e_{53} + q_2e_{52} + q_1e_{51} + q_0e_{47}$$

$$r_D = r_{18}e_{95} + r_{17}e_{94} + r_{16}e_{92} + r_{15}e_{91} + r_{14}e_{90} + r_{13}e_{89} + r_{12}e_{88} + r_{11}e_{87} + r_{10}e_{86} + r_9e_{85} + r_8e_{84} + r_7e_{83} + r_6e_{82} + r_5e_{81} + r_4e_{80} + r_3e_{79} + r_2e_{78} + r_1e_{75} + r_0e_{71}$$

$$s_E = s_{20}e_{122} + s_{19}e_{121} + s_{18}e_{120} + s_{17}e_{119} + s_{16}e_{117} + s_{15}e_{116} + s_{14}e_{115} + s_{13}e_{114} + s_{12}e_{113} + s_{11}e_{112} + s_{10}e_{111} + s_9e_{110} + s_8e_{109} + s_7e_{108} + s_6e_{107} + s_5e_{106} + s_4e_{105} + s_3e_{104} + s_2e_{103} + s_1e_{101} + s_0e_{99}$$

$$t_F = t_{18}e_{150} + t_{17}e_{149} + t_{16}e_{148} + t_{15}e_{145} + t_{14}e_{144} + t_{13}e_{143} + t_{12}e_{141} + t_{11}e_{140} + t_{10}e_{139} + t_9e_{138} + t_8e_{137} + t_7e_{136} + t_6e_{135} + t_5e_{133} + t_4e_{132} + t_3e_{131} + t_2e_{130} + t_1e_{128} + t_0e_{123}$$

$$u_G = u_{20}e_{179} + u_{19}e_{178} + u_{18}e_{177} + u_{17}e_{176} + u_{16}e_{174} + u_{15}e_{173} + u_{14}e_{172} + u_{13}e_{171} + u_{12}e_{170} + u_{11}e_{169} + u_{10}e_{168} + u_9e_{166} + u_8e_{165} + u_7e_{164} + u_6e_{163} + u_5e_{162} + u_4e_{161} + u_3e_{160} + u_2e_{159} + u_1e_{158} + u_0e_{152}$$

$$v_H = v_{20}e_{210} + v_{19}e_{209} + v_{18}e_{208} + v_{17}e_{207} + v_{16}e_{205} + v_{15}e_{203} + v_{14}e_{200} + v_{13}e_{199} + v_{12}e_{198} + v_{11}e_{197} + v_{10}e_{196} + v_9e_{195} + v_8e_{194} + v_7e_{193} + v_6e_{192} + v_5e_{191} + v_4e_{190} + v_3e_{189} + v_2e_{188} + v_1e_{186} + v_0e_{180}$$

$$B = w_{63}e_{210} + w_{62}e_{209} + w_{61}e_{208} + w_{60}e_{207} + w_{59}e_{206} + w_{58}e_{205} + w_{57}e_{204} + w_{56}e_{203} + w_{55}e_{202} + w_{54}e_{201} + w_{53}e_{179} + w_{52}e_{178} + w_{51}e_{177} + w_{50}e_{176} + w_{49}e_{175} + w_{48}e_{174} + w_{47}e_{173} + w_{46}e_{172} + w_{45}e_{171} + w_{44}e_{150} + w_{43}e_{149} + w_{42}e_{148} + w_{41}e_{147} + w_{40}e_{146} + w_{39}e_{145} + w_{38}e_{144} + w_{37}e_{143} + w_{36}e_{142} + w_{35}e_{122} + w_{34}e_{121} + w_{33}e_{120} + w_{32}e_{119} + w_{31}e_{118} + w_{30}e_{117} + w_{29}e_{116} + w_{28}e_{115} + w_{27}e_{95} + w_{26}e_{94} + w_{25}e_{93} + w_{24}e_{92} + w_{23}e_{91} + w_{22}e_{90} + w_{21}e_{89} + w_{20}e_{88} + w_{19}e_{69} + w_{18}e_{68} + w_{17}e_{67} + w_{16}e_{66} + w_{15}e_{65} + w_{14}e_{64} + w_{13}e_{63} + w_{12}e_{44} + w_{11}e_{43} + w_{10}e_{42} + w_9e_{41} + w_8e_{40} + w_7e_{39} + w_6e_{38} + w_5e_{21} + w_4e_{20} + w_3e_{19} + w_2e_{18} + w_1e_{17} + w_0e_{16}$$

Using the general relation (5), the basic linear sequential circuit approximation of Achterbahn corresponding to the decompositions A and B can be expressed as

$$u_t = \sum_{i=0}^{m} \varphi_i z_{t+i} = \sum_{i=0}^{m} \varphi_i \gamma_{t+i} + \sum_{i=0}^{m} c_i \delta_{t+i}$$

which can be represented in generating function domain as:-

$$u_t = \varphi(D) z_t = \varphi(D)\gamma_t + c(D)\delta_t$$

Where

$\varphi(x) = \sum_{i=0}^{m} \varphi_i x^i$is the reciprocal of the characteristic polynomial of $A$and $c_j(x) = \sum_{i=0}^{m} c_{j,i} x^i$, $1 \le j \le 8$whose coefficient are defined by$[c_{1,i} c_{2,i} \ \dots \ c_{8,i}] = \sum_{k=0}^{m-i} \varphi_{k+i} B A^k H$.

Reciprocal of characteristic polynomial $\varphi(x)$of matrix $A$is as follows:

$$\varphi(x) = 1 + x + x^4 + x^5 + x^8 + x^9 + x^{12} + x^{13} + x^{64} + x^{65} + x^{68} + x^{69} + x^{72} + x^{73} + x^{76} + x^{77} + x^{128} + x^{129} + x^{132} + x^{133} + x^{136} + x^{137} + x^{140} + x^{141} + x^{192} + x^{193} + x^{196} + x^{197} + x^{200} + x^{201} + x^{204} + x^{205}$$

The $c_j(x)$, for $1 \le j \le 8$polynomials are as follows:

$$c_1(x) = x + x^2 + x^5 + x^9 + x^{10} + x^{13} + x^{14} + x^{65} + x^{66} + x^{68} + x^{69} + x^{71} + x^{73} + x^{74} + x^{77} + x^{96} + x^{101} + x^{128} + x^{130} + x^{133} + x^{137} + x^{141} + x^{142} + x^{190} + x^{191} + x^{193} + x^{195} + x^{197} + x^{198} + x^{200} + x^{201} + x^{204}$$

$$c_2(x) = x + x^2 + x^5 + x^9 + x^{10} + x^{13} + x^{14} + x^{40} + x^{42} + x^{45} + x^{68} + x^{72} + x^{73} + x^{77} + x^{78} + x^{128} + x^{129} + x^{132} + x^{133} + x^{140} + x^{141} + x^{142} + x^{151} + x^{154} + x^{157} + x^{160} + x^{161} + x^{169} + x^{189} + x^{194} + x^{200} + x^{201} + x^{202}$$

$$c_3(x) = x^5 + x^9 + x^{10} + x^{13} + x^{15} + x^{17} + x^{21} + x^{26} + x^{39} + x^{41} + x^{42} + x^{45} + x^{69} + x^{70} + x^{73} + x^{74} + x^{76} + x^{78} + x^{79} + x^{80} + x^{81} + x^{83} + x^{89} + x^{100} + x^{102} + x^{105} + x^{107} + x^{117} + x^{119} + x^{120}$$

$$c_4(x) = x + x^4 + x^5 + x^7 + x^9 + x^{10} + x^{11} + x^{13} + x^{15} + x^{17} + x^{23} + x^{26} + x^{28} + x^{29} + x^{31} + x^{32} + x^{33} + x^{34} + x^{35} + x^{37} + x^{39} + x^{69} + x^{84} + x^{89} + x^{96} + x^{97} + x^{98} + x^{104} + x^{107} + x^{109}$$

$$c_5(x) = x + x_2 + x_3 + x_{17} + x_{19} + x_{20} + x_{21} + x_{31} + x_{33} + x_{37} + x_{39} + x_{40} + x_{43} + x_{51} + x_{54} + x_{61} + x_{69} + x_{71} + x_{76} + x_{77} + x_{79} + x_{81} + x_{83} + x_{87} + x_{91} + x_{98} + x_{102} + x_{110} + x_{112} + x_{124} + x_{146}$$

$$c_6(x) = x^9 + x^{10} + x^{13} + x^{15} + x^{21} + x^{25} + x^{31} + x^{35} + x^{38} + x^{39} + x^{41} + x^{45} + x^{47} + x^{63} + x^{71} + x^{79} + x^{81} + x^{89} + x^{96} + x^{102} + x^{118} + x^{134} + x^{149} + x^{161} + x^{169} + x^{178} + x^{188} + x^{189}$$

$$c_7(x) = x^5 + x^9 + x^{11} + x^{31} + x^{41} + x^{42} + x^{45} + x^{61} + x^{63} + x^{64} + x^{66} + x^{67} + x^{71} + x^{75} + x^{82} + x^{85} + x^{86} + x^{89} + x^{93} + x^{94} + x^{95} + x^{98} + x^{99} + x^{100} + x^{117} + x^{118} + x^{123} + x^{131} + x^{200}$$

$$c_8(x) = x^4 + x^5 + x^8 + x^{26} + x^{41} + x^{42} + x^{45} + x^{48} + x^{49} + x^{51} + x^{52} + x^{53} + x^{54} + x^{55} + x^{56} + x^{57} + x^{58} + x^{59} + x^{60} + x^{61} + x^{63} + x^{64} + x^{68} + x^{89} + x^{90} + x^{91} + x^{102} + x^{119} + x^{120} + x^{123} + x^{128} + x^{131} + x^{169}$$

Stage3:

Under the independence assumption of the noise terms, the correlation coefficient of u_t denoted by $\varepsilon = \varepsilon_i^{hw(\varphi_i)} \prod_{i=0}^{7} \varepsilon_i^{hw(c_i)}$, where $hw(.)$ is the weight of a given polynomial and ε_i is the noise terms corresponding to linear approximations. Assuming the terms are independent, the correlation coefficient of u_t is 2^{-1809}.

The keystream sequence generated by Achterbahn consist a distinguisher with its probability bias 2^{-1809}. Thus, to distinguish the Achterbahn we only need $\frac{1}{\varepsilon^2} = (2^{1809})^2 = 2^{3618}$ keystream bits and the time complexity is about $\frac{10}{\varepsilon^2} = 2^{3621.3}$ which is much higher than the exhaustive key search $O(2^{80})$. The standard chi-square frequency statistical test can then be applied to u_t to distinguish this sequence from a purely random binary sequence.

From this analysis we see that there are three factors determining the power of our attack.

1. The correlation coefficient ε of linear approximations.
2. The weight of the polynomial of state transition Matrix $A$of the linear sequential circuit.
3. The weight of the polynomial of linear approximation of feedback function

It is favorable to look for polynomials that are of low weight.

5. CONCLUSION

In this paper, we have utilizes the concept of linear sequential circuit approximation to mount distinguishing attack on Achterbahn stream cipher. We derive the linear functions of consecutive output bits with the correlation coefficient of about 2^{-1809}. It shows that output sequence of Achterbahn Stream cipher can be distinguished from a purely random sequence. In our attack, we only need 2^{3618}keystream bits with error probability less than 10^{-3} for distinguishing the output sequence from a purely random sequence. The time complexity is about $2^{3621.3}$ which is much higher than the exhaustive key search i.e. $O(2^{80})$.

6. REFERENCES

[1] Golic, J. Dj.1993. Correlation via linear sequential circuit approximation of combiners with memory. Advance in Cryptology-EUROCRYPT'92. Lecture Notes in Computer Science, vol. 658, Springer-Verlag, Berlin, 113-123.

[2] Golic, J. Dj. 1996.Linear Models for Keystream Generators. IEEE Trans. Comput., vol. C-45, 41-49.

[3] Golic, J.Dj. 1994. Linear Cryptanalysis of Stream Ciphers. Fast Software Encryption 1994, Lecture Notes in Computer Science, vol. 1008, B. Preneel. Springer-Verlag, Berlin, 154–169.

[4] Coppersmith, D., Halevi, S and Jutla, C. 2002. Cryptanalysis of Stream Ciphers with Linear Masking. Advances in Cryptology—CRYPTO 2002, Lecture Notes in Computer Science, vol. 2442, M. Yung. Springer-Verlag, Berlin, 515–532.

[5] Gammel, B.M., Gottfert, R., Kniffler, O. 2006. Achterbahn-128/80, eSTREAM, ECRYPT Stream Cipher Project http://www.ecrypt.eu.org/stream.