Linear Distinguishing Attack on NLS

Joo Yeon Cho and Josef Pieprzyk

Centre for Advanced Computing – Algorithms and Cryptography,
Department of Computing,
Macquarie University,
NSW, Australia, 2109
{jcho,josef}@ics.mq.edu.au

Abstract. We present a distinguishing attack on NLS which is one of the stream ciphers submitted to the eSTREAM project. We build the distinguisher by using linear approximations of both the non-linear feedback shift register (NFSR) and the non-linear filter function (NLF). Since the bias of the distinguisher depends on the $Konst$ value, which is a key-dependent word, we estimate the average bias to be around $O(2^{-34})$. Therefore, we claim that NLS is distinguishable from truly random cipher after observing $O(2^{68})$ keystream words on the average. In addition, we present how to reduce a fraction of $Konst$ values for which our attack fails.
Keywords : Distinguishing Attacks, Stream Ciphers, Linear Approximations, eSTREAM, Modular Addition, NLS.

1 Introduction

The European Network of Excellence in Cryptology (ECRYPT) launched a stream cipher project called eSTREAM [1] whose aim is to come up with a collection of stream ciphers that can be recommended to industry and government institutions as secure and efficient cryptographic primitives. It is also likely that some or perhaps all recommended stream ciphers may be considered as de facto industry standards. It is interesting to see a variety of different approaches used by the designers of the stream ciphers submitted to the eSTREAM call. A traditional approach for building stream ciphers is to use a linear feedback shift register (LFSR) as the main engine of the cipher. The outputs of the registers are taken and put into a nonlinear filter that produces the output stream that is added to the stream of plaintext.

One of the new trends in the design of stream ciphers is to replace LFSR by a nonlinear feedback shift register (NFSR). From the ciphers submitted to the eSTREAM call, there are several ciphers that use the structure based on NFSR amongst them the NLS cipher follows this design approach. The designers of the NLS cipher are Gregory Rose, Philip Hawkes, Michael Paddon and Miriam Wiggers de Vries from Qualcomm Australia.

The paper studies the NLS cipher and its resistance against distinguishing attacks using linear approximation. Typically, distinguishing attacks do not allow to recover any secret element of the cipher such as the cryptographic key or the secret initial state of the NFSR but instead they permit to tell apart the cipher from the truly random cipher. In this sense these attacks are relatively weak. However, the existence of a distinguishing attack is considered as an early warning sign of possible major security flaws.

In our analysis, we derive linear approximations of both NFSR and the nonlinear filter (NLF). The main challenge has been to combine the obtained linear approximations in a such way that the internal state bits of NFSR have been eliminated leaving the observable

output bits only. Our approach is an extension of the linear masking method introduced by Coppersmith, Halevi, and Jutla in [3]. Note that the linear masking method was applied for the traditional stream ciphers based on LFSR so it is not directly applicable for the ciphers with NFSR.

The work is structured as follows. Section 2 briefly describes the NLS cipher. In Section 3, we study best linear approximations for both NFSR and NLF. A simplified NLS cipher is defined in Section 4 and we show how to design a distinguisher for it. Our distinguisher for the original NLS cipher is examined in Section 5. We show how it works and also discuss its limitations. Section 6 concludes our work.

2 Brief description of NLS stream cipher

As we said the NLS keystream generator uses NFSR whose outputs are given to the nonlinear filter NLF that produces output keystream bits. Note that we concentrate on the cipher itself and ignore its message integrity function as irrelevant to our analysis. For details of the cipher, the reader is referred to [2].

NLS has two components: NFSR and NLF whose work is synchronised by a clock. The state of NFSR at time t is denoted by $\sigma_t = (r_t[0], \ldots, r_t[16])$ where $r_t[i]$ is a 32-bit word. The state is determined by 17 words (or equivalently 544 bits). The transition from the state σ_t to the state σ_{t+1} is defined as follows:

1. $r_{t+1}[i] = r_t[i+1]$ for $i = 0, \ldots, 15$;
2. $r_{t+1}[16] = f((r_t[0] \lll 19) \boxplus (r_t[15] \lll 9) \boxplus Konst) \oplus r_t[4]$;
3. if $t = 0$ (modulo f16), $r_{t+1}[2] = r_{t+1}[2] \boxplus t$;

where $f16$ is 65537 and $\boxplus$ is the addition modulo 2^{32}. The *Konst* value is a 32-bit key-dependent constant. The function $f : \{0,1\}^{32} \to \{0,1\}^{32}$ is constructed using an S-box with 8-bit input and 32-bit output and defined as $f(a) = \text{S-box}(a_H) \oplus a$ where a_H is the most significant 8 bits of 32-bit word a. Each output keystream word ν_t of NLF is obtained as

$$\nu_t = NLF(\sigma_t) = (r_t[0] \boxplus r_t[16]) \oplus (r_t[1] \boxplus r_t[13]) \oplus (r_t[6] \boxplus Konst). \quad (1)$$

The cipher uses 32-bit words to ensure a fast keystream generation.

3 Analysis of NFSR and NLF

Unlike a LFSR that applies a connection polynomial, the NFSR uses a much more complex nonlinear transition function f that mixes the XOR addition (linear) with the addition modulo 2^{32} (nonlinear). According to the structure of the non-linear shift register, the following equation holds for the least significant bit. Let us denote α_t to be a 32-bit output of the S-box that defines the transition function f. Then, we observe that for the least significant bit, the following equation holds

$$\alpha_{t,(0)} \oplus r_t[0]_{(13)} \oplus r_t[15]_{(23)} \oplus Konst_{(0)} \oplus r_t[4]_{(0)} \oplus r_{t+1}[16]_{(0)} = 0 \quad (2)$$

where $\alpha_{t,(0)}$ and $x_{(i)}$ stand for the i-th bits of the 32-bit words α_t and x, respectively.

To make our analysis simpler we assume initially that *Konst* is zero. This assumption is later dropped (i.e. *Konst* is non-zero) when we discuss our distinguishing attack on the NLS stream cipher.

3.1 Linear approximations of $\alpha_{t,(0)}$

Recall that α_t is the 32-bit output taken from the S-box and $\alpha_{t,(0)}$ is its least significant bit. The input to the S-box comes from the eight most significant bits of the addition $((r_t[0] \lll 19) \boxplus (r_t[15] \lll 9) \boxplus Konst)$. Assuming that $Konst$=0, the input to S-box is $(r_t[0]' \boxplus r_t[15]')$, where $r_t[0]' = r_t[0] \lll 19$ and $r_t[15]' = r_t[15] \lll 9$. Thus, $\alpha_{t,(0)}$ is completely determined by the contents of two registers $r_t[0]'$ and $r_t[15]'$. Observe that the input of the S-box is affected by the eight most significant bits of the two registers $r_t[0]'$ (we denote the 8 most significant bits of the register by $r_t[0]'_{(H)}$) and $r_t[15]'$ (the 8 most significant bits of the register are denoted by $r_t[15]'_{(H)}$) and by the carry bit c generated by the addition of two 24 least significant bits of $r_t[0]'$ and $r_t[15]'$. Therefore

$$\text{the input of the S-box} = r_t[0]'_{(H)} \boxplus r_t[15]'_{(H)} \boxplus c.$$

Now we would like to find the best linear approximation for $\alpha_{t,(0)}$. We build the truth table with 2^{17} rows and 2^{16} columns. Each row corresponds to the unique collection of input variables (8 bits of $r_t[0]'_{(H)}$, 8 bits of $r_t[15]'_{(H)}$, and a single bit for c). Each column relates to the unique linear combination of bits from $r_t[0]'_{(H)}$ and $r_t[15]'_{(H)}$. Table 1 displays a collection of best linear approximations that are going to be used in our distinguishing attack. In particular, the third row of Table 1 has relatively high bias. This seems to be caused by the reason that $r_t[0]_{(12)} \oplus r_t[15]_{(22)}$ is the only input to the MSB of input of the S-box that is not diffused to other order bits. Note that $r_t[0]'_{(H)} = (r_t[0] \lll 19)_{(H)} = (r_t[0]_{(12)}, \ldots, r_t[0]_{(5)})$

linear approximations of $\alpha_{t,(0)}$	bias
$r_t[0]_{(10)} \oplus r_t[0]_{(6)} \oplus r_t[15]_{(20)} \oplus r_t[15]_{(16)} \oplus r_t[15]_{(15)}$	1/2+0.024414
$r_t[0]_{(10)} \oplus r_t[0]_{(6)} \oplus r_t[0]_{(5)} \oplus r_t[15]_{(20)} \oplus r_t[15]_{(16)}$	1/2+0.024414
$r_t[0]_{(12)} \oplus r_t[15]_{(22)}$	1/2-0.022705
$r_t[0]_{(11)} \oplus r_t[15]_{(21)}$	1/2+0.002441
$r_t[0]_{(10)} \oplus r_t[15]_{(20)}$	1/2-0.017578

Table 1. Linear approximations for $\alpha_{t,(0)}$ when $Konst = 0$

and $r_t[15]'_{(H)} = (r_t[15] \lll 9)_{(H)} = (r_t[15]_{(22)}, \ldots, r_t[15]_{(15)})$. Note also that none of the approximations contains the carry bit c, in other words, the approximations do not depend on c.

3.2 Linear approximations for NFSR

Having a linear approximation of $\alpha_{t,(0)}$, it is easy to obtain a linear approximation for NFSR. Let us choose the first approximation from Table 1, so we are getting the following linear equation:

$$\alpha_{t,(0)} = r_t[0]_{(10)} \oplus r_t[0]_{(6)} \oplus r_t[15]_{(20)} \oplus r_t[15]_{(16)} \oplus r_t[15]_{(15)} \tag{3}$$

with the bias $0.024414 = 2^{-5.35}$. Now we combine Equations (2) and (3) and as the result we have the following approximation for NFSR

$$\begin{aligned} &r_t[0]_{(10)} \oplus r_t[0]_{(6)} \oplus r_t[15]_{(20)} \oplus r_t[15]_{(16)} \oplus r_t[15]_{(15)} \\ &\oplus r_t[0]_{(13)} \oplus r_t[15]_{(23)} \oplus Konst_{(0)} \oplus r_t[4]_{(0)} \oplus r_{t+1}[16]_{(0)} = 0 \end{aligned} \tag{4}$$

with the bias of $2^{-5.35}$.

3.3 Linear approximation for NLF

Recall that Equation (1) defines the output keystream generated by NLF. As we have assumed that $Konst$ is zero, we get

$$\nu_t = (r_t[0] \boxplus r_t[16]) \oplus (r_t[1] \boxplus r_t[13]) \oplus r_t[6]$$

Let us take a closer look at the addition $\boxplus$, we know that the least significant bits are linear so the following equation holds $(r[x] \boxplus r[y])_{(0)} = r[x]_{(0)} \oplus r[y]_{(0)}$. Consequently, we obtain the relation for the least significant bits in the following form

$$\nu_{t,(0)} = (r_t[0]_{(0)} \oplus r_t[16]_{(0)}) \oplus (r_t[1]_{(0)} \oplus r_t[13]_{(0)}) \oplus (r_t[6]_{(0)}) \tag{5}$$

that holds with probability one.
All consecutive bits $i > 0$ of $\boxplus$ are nonlinear. Consider the function $(r[x] \boxplus r[y])_{(i)} \oplus (r[x] \boxplus r[y])_{(i-1)}$. The function has a linear approximation as follows

$$(r[x] \boxplus r[y])_{(i)} \oplus (r[x] \boxplus r[y])_{(i-1)} = r[x]_{(i)} \oplus r[y]_{(i)} \oplus r[x]_{(i-1)} \oplus r[y]_{(i-1)} \tag{6}$$

that has the bias of 2^{-2}. Using the above approximation we can argue that, for $2 \leq i \leq 31$, NLF function possesses a linear approximation of the following form

$$\begin{aligned} \nu_{t,(i)} \oplus \nu_{t,(i-1)} = {} & (r_t[0]_{(i)} \oplus r_t[16]_{(i)} \oplus r_t[0]_{(i-1)} \oplus r_t[16]_{(i-1)}) \\ & \oplus (r_t[1]_{(i)} \oplus r_t[13]_{(i)} \oplus r_t[1]_{(i-1)} \oplus r_t[13]_{(i-1)}) \\ & \oplus (r_t[6]_{(i)} \oplus r_t[6]_{(i-1)}) \end{aligned} \tag{7}$$

with the bias of $2(2^{-2})^2 = 2^{-3}$.

4 Distinguishing attack on a simplified NLS

In this section we assume that the structure of NFSR is unchanged but the structure of NLF is modified by replacing the addition $\boxplus$ by $\oplus$. Thus, Equation (1) that describes the keystream becomes

$$\mu_t = (r_t[0] \oplus r_t[16]) \oplus (r_t[1] \oplus r_t[13]) \oplus (r_t[6] \oplus Konst). \tag{8}$$

This linear function is valid for 32-bit words so it can be equivalently re-written as a system of 32 equations each equation valid for the particular ith bit. Hence, for $0 \leq i \leq 31$,

$$\mu_{t,(i)} = (r_t[0]_{(i)} \oplus r_t[16]_{(i)}) \oplus (r_t[1]_{(i)} \oplus r_t[13]_{(i)}) \oplus (r_t[6]_{(i)} \oplus Konst_{(i)}). \tag{9}$$

To build a distinguisher we combine approximations of NFSR given by Equation (4) with linear equations defined by (9). For the clocks t, $t+1$, $t+6$, $t+13$, and $t+16$, consider the following approximations of NFSR

$$\begin{aligned} & r_t[0]_{(10)} \oplus r_t[0]_{(6)} \oplus r_t[15]_{(20)} \oplus \cdots \oplus r_{t+1}[16]_{(0)} = 0 \\ & r_{t+1}[0]_{(10)} \oplus r_{t+1}[0]_{(6)} \oplus r_{t+1}[15]_{(20)} \oplus \cdots \oplus r_{t+2}[16]_{(0)} = 0 \\ & r_{t+6}[0]_{(10)} \oplus r_{t+6}[0]_{(6)} \oplus r_{t+6}[15]_{(20)} \oplus \cdots \oplus r_{t+7}[16]_{(0)} = 0 \\ & r_{t+13}[0]_{(10)} \oplus r_{t+13}[0]_{(6)} \oplus r_{t+13}[15]_{(20)} \oplus \cdots \oplus r_{t+14}[16]_{(0)} = 0 \\ & r_{t+16}[0]_{(10)} \oplus r_{t+16}[0]_{(6)} \oplus r_{t+16}[15]_{(20)} \oplus \cdots \oplus r_{t+17}[16]_{(0)} = 0 \end{aligned} \tag{10}$$

Since $r_{t+p}[0] = r_t[p]$, we can rewrite the above system of equations (10) equivalently as follows:

$$\begin{array}{l} r_t[0]_{(10)} \oplus r_t[0]_{(6)} \oplus r_{t+15}[0]_{(20)} \oplus \cdots \oplus r_{t+17}[0]_{(0)} = 0 \\ r_t[1]_{(10)} \oplus r_t[1]_{(6)} \oplus r_{t+15}[1]_{(20)} \oplus \cdots \oplus r_{t+17}[1]_{(0)} = 0 \\ r_t[6]_{(10)} \oplus r_t[6]_{(6)} \oplus r_{t+15}[6]_{(20)} \oplus \cdots \oplus r_{t+17}[6]_{(0)} = 0 \\ r_t[13]_{(10)} \oplus r_t[13]_{(6)} \oplus r_{t+15}[13]_{(20)} \oplus \cdots \oplus r_{t+17}[13]_{(0)} = 0 \\ r_t[16]_{(10)} \oplus r_t[16]_{(6)} \oplus r_{t+15}[16]_{(20)} \oplus \cdots \oplus r_{t+17}[16]_{(0)} = 0 \end{array} \tag{11}$$

Consider the columns of the above system of equations. Each column describes a single bit output of the filter (see Equation (9)), therefore the system (11) gives the following approximation:

$$\begin{array}{l} \mu_{t,(10)} \oplus \mu_{t,(6)} \oplus \mu_{t+15,(20)} \oplus \mu_{t+15,(16)} \oplus \mu_{t+15,(15)} \oplus \mu_{t,(13)} \\ \oplus \mu_{t+15,(23)} \oplus \mu_{t+4,(0)} \oplus \mu_{t+17,(0)} = K \end{array} \tag{12}$$

where $K = Konst_{(10)} \oplus Konst_{(6)} \oplus Konst_{(20)} \oplus Konst_{(16)} \oplus Konst_{(15)} \oplus Konst_{(13)} \oplus Konst_{(23)}$. Note that the bit K is constant (zero or one) during the session. Therefore, by the piling-up lemma, the bias of (12) is $\mathbf{2} \cdot \mathbf{2^4} \cdot (\mathbf{2^{-5.35}})^{\mathbf{5}} = \mathbf{2^{-22}}$.

5 Distinguishing attack on NLS

In this Section, we describe a distinguishing attack on the real NLS. The main idea is to find the best combination of approximations for both NFSR and NLF, while the state bits of the shift register vanish and the bias of the resulting approximation is as big as possible. We study the case for $Konst = 0$ at first and then, extend our attack to the case for $Konst \neq 0$. Note that only a non-zero most significant byte of $Konst$ is allowed in NLS cipher.

5.1 Case for $Konst = 0$

The linear approximations of $\alpha_{t,(0)}$ are given in Table 1. We choose this time the third approximation from the table so

$$\alpha_{t,(0)} = r_t[0]_{(12)} \oplus r_t[15]_{(22)} \tag{13}$$

and the bias of this approximation is $0.022705 = 2^{-5.46}$. By combining Equations (2) and (13), we have the following approximation

$$r_t[0]_{(12)} \oplus r_t[15]_{(22)} \oplus r_t[0]_{(13)} \oplus r_t[15]_{(23)} \oplus r_t[4]_{(0)} \oplus r_{t+1}[16]_{(0)} = 0 \tag{14}$$

that has the same bias. Let us now divide (14) into two parts : the least significant bit and the other bits, so we get

$$\begin{array}{l} l_1(r_t) = r_t[4]_{(0)} \oplus r_{t+1}[16]_{(0)} \\ l_2(r_t) = r_t[0]_{(12)} \oplus r_t[0]_{(13)} \oplus r_t[15]_{(22)} \oplus r_t[15]_{(23)} \end{array} \tag{15}$$

Clearly, $l_1(r_t) \oplus l_2(r_t) = 0$ with the bias $2^{-5.46}$. Since $l_1(r_t)$ has only the least significant bit variables, we apply (5) which is true with probability one. Then, we obtain

$$\begin{array}{l} l_1(r_t) = r_t[4]_{(0)} \oplus r_{t+1}[16]_{(0)} \\ l_1(r_{t+1}) = r_{t+1}[4]_{(0)} \oplus r_{t+2}[16]_{(0)} \\ l_1(r_{t+6}) = r_{t+6}[4]_{(0)} \oplus r_{t+7}[16]_{(0)} \\ l_1(r_{t+13}) = r_{t+13}[4]_{(0)} \oplus r_{t+14}[16]_{(0)} \\ l_1(r_{t+16}) = r_{t+16}[4]_{(0)} \oplus r_{t+17}[16]_{(0)} \end{array} \tag{16}$$

If we add up all approximations of (16), then, by applying Equation (5), we can write

$$l_1(r_t) \oplus l_1(r_{t+1}) \oplus l_1(r_{t+6}) \oplus l_1(r_{t+13}) \oplus l_1(r_{t+16}) = \nu_{t+4,(0)} \oplus \nu_{t+17,(0)} \tag{17}$$

Now, we focus on $l_2(r_t)$ where the bit positions are 12, 13, 22, and 23 so

$$\begin{array}{l} l_2(r_t) = r_t[0]_{(12)} \oplus r_t[0]_{(13)} \oplus r_t[15]_{(22)} \oplus r_t[15]_{(23)} \\ l_2(r_{t+1}) = r_{t+1}[0]_{(12)} \oplus r_{t+1}[0]_{(13)} \oplus r_{t+1}[15]_{(22)} \oplus r_{t+1}[15]_{(23)} \\ l_2(r_{t+6}) = r_{t+6}[0]_{(12)} \oplus r_{t+6}[0]_{(13)} \oplus r_{t+6}[15]_{(22)} \oplus r_{t+6}[15]_{(23)} \\ l_2(r_{t+13}) = r_{t+13}[0]_{(12)} \oplus r_{t+13}[0]_{(13)} \oplus r_{t+13}[15]_{(22)} \oplus r_{t+13}[15]_{(23)} \\ l_2(r_{t+16}) = r_{t+16}[0]_{(12)} \oplus r_{t+16}[0]_{(13)} \oplus r_{t+16}[15]_{(22)} \oplus r_{t+16}[15]_{(23)} \end{array} \tag{18}$$

Since $r_{t+p}[0] = r_t[p]$, the above approximations can be presented as follows

$$\begin{array}{l} l_2(r_t) = r_t[0]_{(12)} \oplus r_t[0]_{(13)} \oplus r_{t+15}[0]_{(22)} \oplus r_{t+15}[0]_{(23)} \\ l_2(r_{t+1}) = r_t[1]_{(12)} \oplus r_t[1]_{(13)} \oplus r_{t+15}[1]_{(22)} \oplus r_{t+15}[1]_{(23)} \\ l_2(r_{t+6}) = r_t[6]_{(12)} \oplus r_t[6]_{(13)} \oplus r_{t+15}[6]_{(22)} \oplus r_{t+15}[6]_{(23)} \\ l_2(r_{t+13}) = r_t[13]_{(12)} \oplus r_t[13]_{(13)} \oplus r_{t+15}[13]_{(22)} \oplus r_{t+15}[13]_{(23)} \\ l_2(r_{t+16}) = r_t[16]_{(12)} \oplus r_t[16]_{(13)} \oplus r_{t+15}[16]_{(22)} \oplus r_{t+15}[16]_{(23)} \end{array} \tag{19}$$

Recall the approximation (7) of NLF. If we combine (19) with (7), then we have

$$\begin{array}{l} l_2(r_t) \oplus l_2(r_{t+1}) \oplus l_2(r_{t+6}) \oplus l_2(r_{t+13}) \oplus l_2(r_{t+16}) = \\ \nu_{t,(12)} \oplus \nu_{t,(13)} \oplus \nu_{t+15,(22)} \oplus \nu_{t+15,(23)} \end{array} \tag{20}$$

By combining the approximations (17) and (20), we obtain the final approximation that defines our distinguisher, i.e.

$$\begin{array}{l} l_1(r_t) \oplus l_1(r_{t+1}) \oplus l_1(r_{t+6}) \oplus l_1(r_{t+13}) \oplus l_1(r_{t+16}) \\ \oplus l_2(r_t) \oplus l_2(r_{t+1}) \oplus l_2(r_{t+6}) \oplus l_2(r_{t+13}) \oplus l_2(r_{t+16}) \\ = \nu_{t,(12)} \oplus \nu_{t,(13)} \oplus \nu_{t+15,(22)} \oplus \nu_{t+15,(23)} \oplus \nu_{t+4,(0)} \oplus \nu_{t+17,(0)} \\ = 0 \end{array} \tag{21}$$

The second part of the approximation can be computed from the output keystream that can be observed by the adversary. The bias can be computed using the piling-up lemma. As we use the approximation (14) five times and the approximation (7) twice, the bias of the approximation (21) is $\mathbf{2} \cdot (\mathbf{2^4}(\mathbf{2^{-5.46}})^{\mathbf{5}}) \cdot (\mathbf{2}(\mathbf{2^{-3}})^{\mathbf{2}}) = \mathbf{2^{-27.3}}$.

5.2 Case for $Konst \neq 0$

Recall that $Konst$ takes part in the input of NFSR and NLF. If $Konst$ is not zero, then, the biases of linear approximations for $\alpha_{t,(0)}$ and NLF are changed according to the values of $Konst$. Let us denote that $Konst_{(H)} = (Konst_{(31)}, \ldots, Konst_{(24)})$, and $Konst_{(L)} = (Konst_{(23)}, \ldots, Konst_{(0)})$.

Biases of linear approximations of $\alpha_{t,(0)}$ and NLF with $Konst_{(H)}$ Since the most significant 8 bits of $Konst$ contribute to form of the bit $\alpha_{t,(0)}$, the bias of the approximation (13) fluctuates mostly according to the 8-bit $Konst_{(H)}$. This relation is illustrated in Figure 1. From this figure, we can see that (13) has the smallest bias when $Konst_{(H)} = 51$ and 179, even though the bias of (13) is $\mathbf{2^{-6.4}}$ on the average.

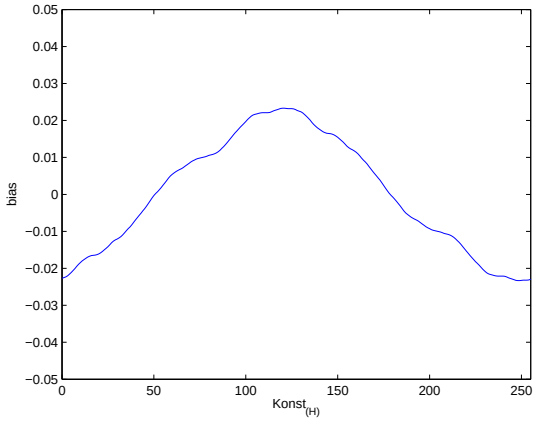

Fig. 1. Bias of $\alpha_{t,(0)} = r_t[0]_{(12)} \oplus r_t[15]_{(22)}$ with $Konst_{(H)}$

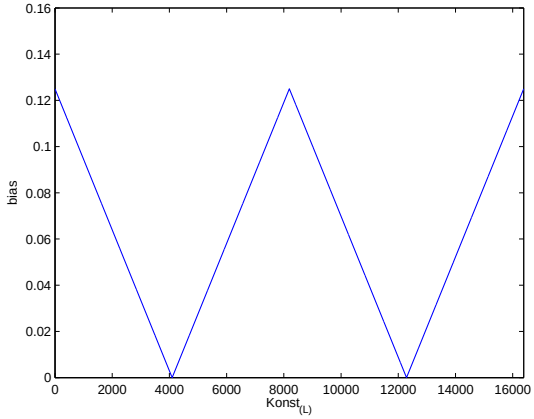

Fig. 2. Bias of (22) with $Konst_{(L)}$ when $i = 13$

$Konst_{(H)}$	best linear approximations of $\alpha_{t,(0)}$	bias
1	$r_t[0]_{(12)} \oplus r_t[15]_{(22)}$	$1/2 - 0.022522$
51	$r_t[0]_{(12)} \oplus r_t[0]_{(11)} \oplus r_t[0]_{(10)} \oplus r_t[15]_{(22)} \oplus r_t[15]_{(21)} \oplus r_t[15]_{(20)}$	$1/2 + 0.011353$
120	$r_t[0]_{(12)} \oplus r_t[15]_{(22)}$	$1/2 + 0.023315$
179	$r_t[0]_{(12)} \oplus r_t[0]_{(11)} \oplus r_t[0]_{(10)} \oplus r_t[15]_{(22)} \oplus r_t[15]_{(21)} \oplus r_t[15]_{(20)}$	$1/2 - 0.011353$

Table 2. A partial table of best approximations for $\alpha_{t,(0)}$ with $Konst_{(H)}$

Hence, in order to maximize the bias of our distinguisher, we need to find the best approximations for $\alpha_{t,(0)}$ when $Konst_{(H)}$ runs through all possible values, i.e. from 0 to 255. Note that the best approximation of $\alpha_{t,(0)}$ means one which results in maximum bias of distinguisher when the approximation of NLF is combined. Table 2 shows a partial table for approximations of $\alpha_{t,(0)}$. When $Konst_{(H)}$ is around 1 or 120, we use the following approximation for NLF.

$$\begin{aligned}\nu_{t,(i)} \oplus \nu_{t,(i-1)} = &(r_t[0]_{(i)} \oplus r_t[16]_{(i)} \oplus r_t[0]_{(i-1)} \oplus r_t[16]_{(i-1)}) \\ &\oplus (r_t[1]_{(i)} \oplus r_t[13]_{(i)} \oplus r_t[1]_{(i-1)} \oplus r_t[13]_{(i-1)}) \\ &\oplus (r_t[6]_{(i)} \oplus Konst_{(i)} \oplus r_t[6]_{(i-1)} \oplus Konst_{(i-1)})\end{aligned} \tag{22}$$

On the other side, when $Konst_{(H)}$ is around 51 or 179, we use the following approximation:

$$\begin{aligned}\nu_{t,(i)} \oplus \nu_{t,(i-1)} \oplus \nu_{t,(i-2)} \oplus \nu_{t,(i-3)} = \\ &(r_t[0]_{(i)} \oplus r_t[16]_{(i)} \oplus r_t[0]_{(i-1)} \oplus r_t[16]_{(i-1)} \\ &\oplus r_t[0]_{(i-2)} \oplus r_t[16]_{(i-2)} \oplus r_t[0]_{(i-3)} \oplus r_t[16]_{(i-3)}) \\ &\oplus (r_t[1]_{(i)} \oplus r_t[13]_{(i)} \oplus r_t[1]_{(i-1)} \oplus r_t[13]_{(i-1)} \\ &\oplus r_t[1]_{(i-2)} \oplus r_t[13]_{(i-2)} \oplus r_t[1]_{(i-3)} \oplus r_t[13]_{(i-3)}) \\ &\oplus (r_t[6]_{(i)} \oplus Konst_{(i)} \oplus r_t[6]_{(i-1)} \oplus Konst_{(i-1)} \\ &\oplus r_t[6]_{(i-2)} \oplus Konst_{(i-2)} \oplus r_t[6]_{(i-3)} \oplus Konst_{(i-3)})\end{aligned} \tag{23}$$

Instead of Approximation (6), we need the following linear approximation in order to compute the bias of (23),

$$\begin{aligned}&(r[x] \boxplus r[y])_{(i)} \oplus (r[x] \boxplus r[y])_{(i-1)} \oplus (r[x] \boxplus r[y])_{(i-2)} \oplus (r[x] \boxplus r[y])_{(i-3)} = \\ &r[x]_{(i)} \oplus r[y]_{(i)} \oplus r[x]_{(i-1)} \oplus r[y]_{(i-1)} \oplus r[x]_{(i-2)} \oplus r[y]_{(i-2)} \oplus r[x]_{(i-3)} \oplus r[y]_{(i-3)}\end{aligned} \tag{24}$$

that has the bias of 2^{-3}.

Biases of linear approximations of NLF with $Konst_{(L)}$ In Approximation (22), the bias of the following approximation fluctuates depending on $Konst_{(L)}$.

$$(r_t[6] \boxplus Konst)_i \oplus (r_t[6] \boxplus Konst)_{i-1} = (r_t[6]_{(i)} \oplus Konst_{(i)} \oplus r_t[6]_{(i-1)} \oplus Konst_{(i-1)}) \tag{25}$$

Figure 2 displays the bias distribution according to $Konst_{(L)}$ in (22) when $i = 13$. Note that this graph shows the distribution from 14 LSBs of $Konst_{(L)}$ (that is, 2^{14}) since the bits $Konst_{(23)}, \ldots, Konst_{(14)}$ have not effect on the bias for $i = 13$. We should consider 24 bits of $Konst_{(L)}$ when $i = 23$ in (22). However, the distribution graph is similar to Figure 2 with only the slope changed. On the average, the bias of (22) is $\mathbf{2^{-4}}$. A very similar analysis is possible for Approximation (23). The bias of (23) is $\mathbf{2^{-7}}$ on the average.

Average bias of distinguisher From both Approximations (22) and (23) with biases shown in Table 2, we can build two distinguishers as follows.

$$\nu_{t,(12)} \oplus \nu_{t,(13)} \oplus \nu_{t+15,(22)} \oplus \nu_{t+15,(23)} \oplus \nu_{t+4,(0)} \oplus \nu_{t+17,(0)} = 0 \tag{26}$$

$$\begin{aligned}&\nu_{t,(10)} \oplus \nu_{t,(11)} \oplus \nu_{t,(12)} \oplus \nu_{t,(13)} \oplus \nu_{t+15,(20)} \oplus \nu_{t+15,(21)} \\ &\oplus \nu_{t+15,(22)} \oplus \nu_{t+15,(23)} \oplus \nu_{t+4,(0)} \oplus \nu_{t+17,(0)} = 0\end{aligned} \tag{27}$$

The bias of best distinguisher for each $Konst_{(H)}$ is displayed in Table 3. We take the average biases of Approximations (22) and (23).

$Konst_{(H)}$	distinguisher	details	bias	data complexity
1	(26)	$2 \cdot (2^4(2^{-5.47})^5) \cdot (2(2^{-4})^2)$	$2^{-29.4}$	$2^{58.8}$
51	(27)	$2 \cdot (2^4(2^{-6.46})^5) \cdot (2(2^{-7})^2)$	$2^{-40.3}$	$2^{80.6}$
120	(26)	$2 \cdot (2^4(2^{-5.42})^5) \cdot (2(2^{-4})^2)$	$2^{-29.1}$	$2^{58.2}$
179	(27)	$2 \cdot (2^4(2^{-6.46})^5) \cdot (2(2^{-7})^2)$	$2^{-40.3}$	$2^{80.6}$

Table 3. A partial table of biases for distinguisher with $Konst_{(H)}$

If we select the distinguisher (26), then, the average bias of approximation of $\alpha_{t,(0)}$ over $Konst_{(H)}$ is $2^{-6.4}$. Therefore, the bias of distinguisher appears to be around $\mathbf{2} \cdot (\mathbf{2^4}(\mathbf{2^{-6.4}})^{\mathbf{5}}) \cdot (\mathbf{2}(\mathbf{2^{-4}})^{\mathbf{2}}) = \mathbf{2^{-34}}$ on the average. Note that an adversary should avoid the keystream that is produced around clock $t = 0 \pmod{65537}$ as the feedback has an additional step at this clock. (See Step 3 at Section 2)

For some values of $Konst_{(H)}$ (e.g. $Konst_{(H)} = 51$ or 179), the bias of the distinguisher (26) becomes less than 2^{-40}. In order to compensate this "small-bias" area, an adversary observes the distinguisher (26) and (27) simultaneously in such a way that a bigger bias among those are always chosen. Note that the amount of the keystream for both distinguishers is not increased since the keystream is produced by words.

Therefore, the minimum bias observable by both distinguisher (26) and (27) will be $2^{-40.3}$ even $Konst_{(H)}$ is close to 51 or 179.

5.3 When does our distinguishing attack fail?

Let us denote the bias of the approximation of $\alpha_{t,(0)}$ by ϵ_1, the bias of the approximation of a single addition (for example, Approximations (6) and (24)) by ϵ_2 and the bias of the approximation of $(r_t[6] \boxplus Konst)$ by ϵ_3. Since the specification of the NLS cipher allows the adversary to observe up to 2^{80} keystream words per one key/nonce pair, we assume that our attack is not successful if the bias of distinguisher satisfies the following condition:

$$\left.\begin{array}{l}\text{bias of linear approx. of } \alpha_{t,(0)} \ : d_1 = 2^4(\epsilon_1^5) \\ \text{bias linear approx. of NLF} : d_2 = 2^2(\epsilon_2)^2\epsilon_3\end{array}\right\} \Rightarrow 2 \cdot d_1 \cdot 2 \cdot (d_2)^2 < 2^{-40}. \quad (28)$$

Note that ϵ_1 is affected by $Konst_{(H)}$, and ϵ_3 by $Konst_{(L)}$.

When the bias becomes zero? In Figure 2, the bias of (25) becomes zero when

1. $Konst_{(L)} = (b_{31}, \ldots, b_{23}, 1, 0, \ldots, 0)$
2. $Konst_{(L)} = (b_{31}, \ldots, b_{13}, 1, 0, \ldots, 0)$

where b_i can have any bit (0 or 1). Hence, the bias of this distinguisher is zero for around 2^{19} out of 2^{32} possible values of $Konst$.

5.4 Multiple distinguishers

Since the NLS produces 32-bit keystream words per a clock, we may reduce the unsuccessful portion of $Konst$ by considering multiple distinguishers without increasing the necessary volume of observed data. For example, let us consider the following approximation of $\alpha_{t,(0)}$

$$\alpha_{t,(0)} = r_t[0]_{(11)} \oplus r_t[15]_{(21)} \quad (29)$$

whose bias on the average is around $0.012911 = 2^{-6.28}$. The corresponding approximation of NLF is

$$\begin{aligned}\nu_{t,(i)} \oplus \nu_{t,(i-2)} = &(r_t[0]_{(i)} \oplus r_t[16]_{(i)} \oplus r_t[0]_{(i-2)} \oplus r_t[16]_{(i-2)}) \\ &\oplus (r_t[1]_{(i)} \oplus r_t[13]_{(i)} \oplus r_t[1]_{(i-2)} \oplus r_t[13]_{(i-2)}) \\ &\oplus (r_t[6]_{(i)} \oplus Konst_{(i)} \oplus r_t[6]_{(i-2)} \oplus Konst_{(i-2)})\end{aligned} \tag{30}$$

and the bias of this approximation is around $2^2(2^{-3})^3 = 2^{-7}$.

As in Section 5.1, an another distinguisher based on a different relation can be built. The relation is as follows:

$$\nu_{t,(11)} \oplus \nu_{t,(13)} \oplus \nu_{t+15,(21)} \oplus \nu_{t+15,(23)}\nu_{t+4,(0)} \oplus \nu_{t+17,(0)} = 0 \tag{31}$$

The bias for the distinguisher on the average is around $2 \cdot (2^4(2^{-6.28})^5) \cdot (2(2^{-7})^2) = 2^{-39.4}$. It is a known fact that the bias of this distinguisher also fluctuates depending on the actual value of $Konst$. However, this time, the phase of fluctuation has been shifted from that of the distinguisher (26).

Even though our attack based on the distinguisher (26) fails for some values of $Konst$, it may be still successful by observing the bias of the other distinguisher (31). Note that the number of observations of keystream required for multiple distinguishers remains same as for a single distinguisher.

We intend to investigate our attack in more detail, in particular, we would like to determine the fraction of the values of $Konst$ for which the distinguishing attack works.

6 Conclusion

In this paper, we presented a linear distinguishing attack on NLS. The bias of distinguisher appears to be 2^{-34} on the average so that NLS is distinguishable from a random function by observing 2^{68} keystream words. Even though there are a fraction of $Konst$ which requires the data complexity bigger than 2^{80}, we show that it is possible for attacker to reduce the fraction of $Konst$ by combining multiple distinguishers which have biases of less than 2^{-40} on the average.

Acknowledgment We are grateful to Philip Hawkes and anonymous referees of SASC 2006 for their very helpful comments. The second author acknowledges the support received from Australian Research Council (projects DP0451484 and DP0663452).

References

1. http://www.ecrypt.eu.org/stream/.
2. http://www.ecrypt.eu.org/stream/nls.html.
3. Don Coppersmith, Shai Halevi, and Charanjit Jutla. Cryptanalysis of stream ciphers with linear masking. Cryptology ePrint Archive, Report 2002/020, 2002. http://eprint.iacr.org/.