Crossword Puzzle 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. NLS is one of the stream ciphers submitted to the eSTREAM project. We present a distinguishing attack on NLS by Crossword Puzzle (CP) attack method which is introduced in this paper. We build the distinguisher by using linear approximations of both the non-linear feedback shift register (NFSR) and the nonlinear filter function (NLF). Since the bias of the distinguisher depends on the *Konst* value, which is a key-dependent word, we present the graph showing how the bias of distinguisher vary with *Konst*. In result, we estimate the bias of the distinguisher to be around $O(2^{-30})$. Therefore, we claim that NLS is distinguishable from truly random cipher after observing $O(2^{60})$ keystream words. The experiments also show that our distinguishing attack is successful on 90.3% of *Konst* among 2^{32} possible values. We extend the CP attack to NLSv2 which is a tweaked version of NLS. In result, we build a distinguisher which has the bias of around 2^{-48}. Even though this attack is below the eSTREAM criteria (2^{-40}), the security margin of NLSv2 seems to be too low.

Keywords: Distinguishing Attacks, Crossword Puzzle Attack, Stream Ciphers, Linear Approximations, eSTREAM, Modular Addition, NLS, NLSv2.

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

E. Biham and A.M. Youssef (Eds.): SAC 2006, LNCS 4356, pp. 249–265, 2007.

eSTREAM call, there are several ciphers that use the structure based on NFSR. Amongst them the NLS cipher follows this design approach [4]. The designers of the NLS cipher are Philip Hawkes, Gregory Rose, 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. [1] 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 for both NFSR and the non-linear 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 attack can be seen as a variant of the linear distinguishing attack, and we call it **"Crossword Puzzle" attack** (or shortly CP attack). The name is aligned with the intuition behind the attack in which the state bits of approximations vanish by combining them twice, horizontally and vertically.

Our approach is an extension of the linear distinguishing attack with linear masking (shortly, linear masking method) that was 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 presents a framework of CP attack. Section 3 briefly describes the NLS cipher. In Section 4, we study best linear approximations for both NFSR and NLF. A simplified NLS cipher is defined in Section 5 and we show how to design a distinguisher for it. Our distinguisher for the original NLS cipher is examined in Section 6 and an improvement using multiple distinguishers is in Section 7. In Section 8, CP attack is applied to NLSv2 which is a tweaked version of NLS. Section 9 concludes our work.

2 Framework of Crossword Puzzle (CP) Attack

In the CP attack, we construct a distinguisher based on linear approximations of both the non-linear feedback shift register (NFSR) and the non-linear filter (NLF). The attack is general and is applicable to the class of stream ciphers that combine a NFSR with nonlinear filters as long as there are "good enough" linear approximations. The roles of the two non-linear components are as follows.

- NFSR transforms the current state $\boldsymbol{s_i}$ into the next state $\boldsymbol{s_{i+1}}$ in a non-linear way using the appropriate function $NF1$, i.e. $\boldsymbol{s_{i+1}} := NF1(\boldsymbol{s_i})$ where $\boldsymbol{s_0}$ is the initial state and $i = 0, 1, 2, \ldots$.
- NLF produces an output $\boldsymbol{z_i}$ from the current state $\boldsymbol{s_i}$ through a non-linear function $NF2$, i.e. $\boldsymbol{z_i} := NF2(\boldsymbol{s_i})$.

[1] This is an extended version of [2].

$$
\begin{array}{rcccccc}
l_1(\boldsymbol{s_{i_1}}) = & u_1(\boldsymbol{s_{i_1}}) & + u_2(\boldsymbol{s_{i_1}}) & + \cdots + u_n(\boldsymbol{s_{i_1}}) & = \boldsymbol{s_{i_1+1}} \\
l_1(\boldsymbol{s_{i_2}}) = & u_1(\boldsymbol{s_{i_2}}) & + u_2(\boldsymbol{s_{i_2}}) & + \cdots + u_n(\boldsymbol{s_{i_2}}) & = \boldsymbol{s_{i_2+1}} \\
\cdots & \cdots & & & \\
l_1(\boldsymbol{s_{i_m}}) = & u_1(\boldsymbol{s_{i_m}}) & + u_2(\boldsymbol{s_{i_m}}) + \cdots + u_n(\boldsymbol{s_{i_m}}) & & = \boldsymbol{s_{i_m+1}} \\
& || & || & || & || \\
& l_3(\boldsymbol{z_{j_1}}) & l_3(\boldsymbol{z_{j_2}}) & l_3(\boldsymbol{z_{j_n}}) & \boldsymbol{z_{j_{n+1}}}
\end{array}
$$

Fig. 1. An example of crossword puzzling

Let us define a bias ϵ of an approximation as $p = \frac{1}{2}(1+\epsilon), |\epsilon| > 0$ where p is the probability of the approximation.[2] The CP attack consists of the following steps (note that the operation + is a binary (XOR) addition).

1. Find a linear approximation of the non-linear state transition function $NF1$ used by NFSR : $l_1(\boldsymbol{s_i}) = \boldsymbol{s_{i+1}}$ with bias of ϵ_1.
2. Find a linear approximation of the non-linear function $NF2$ applied by NLF : $l_2(\boldsymbol{s_j}) + l_3(\boldsymbol{z_j}) = 0$ with bias of ϵ_2.
3. Obtain two sets of clocks I and J such that $\sum_{i\in I}(l_1(\boldsymbol{s_i})+\boldsymbol{s_{i+1}}) = \sum_{j\in J} l_2(\boldsymbol{s_j})$.
4. Build a distinguisher by computing

$$\sum_{i\in I}(l_1(\boldsymbol{s_i}) + \boldsymbol{s_{i+1}}) + \sum_{j\in J}(l_2(\boldsymbol{s_j}) + l_3(\boldsymbol{z_j})) = \sum_{j\in J} l_3(\boldsymbol{z_j}) = 0$$

   which has bias of $\epsilon_1^{|I|} \cdot \epsilon_2^{|J|}$.

For the CP attack, it is an important task to find the approximations in Step 1 and Step 2 which have the relation required in Step 3. We describe a basic framework for achieving this task.

Given $l_1(\boldsymbol{s_i}) = \boldsymbol{s_{i+1}}$ from NFSR, we divide l_1 into n linear sub-functions $u_1, \ldots, u_n$. Then,

$$l_1(\boldsymbol{s_i}) = u_1(\boldsymbol{s_i}) + u_2(\boldsymbol{s_i}) + \cdots + u_n(\boldsymbol{s_i}) = \boldsymbol{s_{i+1}} \tag{1}$$

Suppose we set up a system of m approximations of l_1 on the clocks $i = i_1, \ldots, i_m$ as in Figure 1.

Now, we seek a linear approximation of NLF which has a form of $l_2(\boldsymbol{s_j}) = l_3(\boldsymbol{z_j})$ such that $l_2(\boldsymbol{s_j})$ corresponds to each column of m approximations of l_1. If there exist a set of such approximations which covers all columns of m approximations as Figure 1, then, those are

$$l_2(\boldsymbol{s_{j_t}}) = \sum_{k=1}^{m} u_t(\boldsymbol{s_{i_k}}) = l_3(\boldsymbol{z_{j_t}}), \quad t = 1, \ldots, n \tag{2}$$

and $\sum_{k=1}^{m} \boldsymbol{s_{i_k+1}} = \boldsymbol{z_{j_{n+1}}}$. Note that Approximation (2) corresponds each column of Approximation in Figure 1.

[2] This definition is useful for computing the bias of multiple approximations when the piling-up lemma [6] is applied. If we have n independent approximations, the probability of n approximations becomes $\frac{1}{2}(1+\epsilon^n)$.

By composing (or "Cross Puzzling") Approximations (1) and (2) in such a way that all the states vanish (as each state occurs twice), we compute a linear approximation

$$\sum_{i=1}^{n} l_3(\boldsymbol{z_{j_i}}) = \boldsymbol{z_{j_{n+1}}} \tag{3}$$

that is true with a non-zero bias. Clearly, Approximation (3) defines our distinguisher.

Discussion. There are more issues in regard to the bias of the distinguisher. Firstly, we assume that all approximations are independent. However, this may not be true since terms in the approximations could be related. The precise value of the bias can be computed by analysis of conditional probabilities of random variables of states involved in the approximations.

Secondly, when we set up a system of m approximations, we may choose different forms of approximations instead of a single approximation $l_1(\boldsymbol{s_i})$ that is used m times. In general, it is of interest to find approximations for both NFSR and NLF in order to maximize the bias of the distinguisher.

Note that the CP attack is reducible to the linear masking method [3] when the NFSR is replaced by a linear feedback shift register (LFSR) with $\epsilon_1 = 1$.

3 Brief Description of NLS Stream Cipher

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 [4].

NLS has two components: NFSR and NLF that are 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 $f(\omega) = \text{S-box}(\omega_{(H)}) \oplus \omega$ where $\omega_{(H)}$ is the most significant 8 bits of 32-bit word ω. Refer to Figure 2. Each output keystream word ν_t of NLF is obtained as

$$\nu_t = NLF(\sigma_t) = (r_t[0] \boxplus r_t[16]) \oplus (r_t[1] \boxplus r_t[13]) \oplus (r_t[6] \boxplus Konst). \tag{4}$$

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

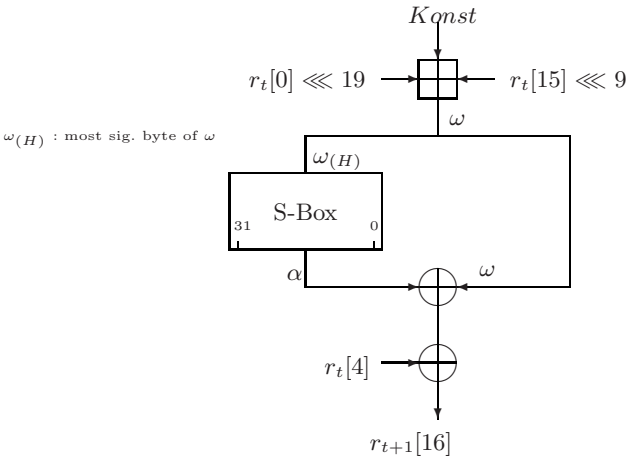

Fig. 2. The f function

4 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 the following equation holds for the least significant bit.

$$\alpha_{t,(0)} \oplus r_t[0]_{(13)} \oplus r_t[15]_{(23)} \oplus Konst_{(0)} \oplus r_t[4]_{(0)} \oplus r_{t+1}[16]_{(0)} = 0 \qquad (5)$$

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

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.

4.1 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* is zero, 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

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

linear approximations of $\alpha_{t,(0)}$	bias
$r_t[0]_{(10)} \oplus r_t[0]_{(6)} \oplus r_t[15]_{(20)} \oplus r_t[15]_{(16)} \oplus r_t[15]_{(15)}$	$1/2(1 + 0.048828)$
$r_t[0]_{(10)} \oplus r_t[0]_{(6)} \oplus r_t[0]_{(5)} \oplus r_t[15]_{(20)} \oplus r_t[15]_{(16)}$	$1/2(1 + 0.048828)$
$r_t[0]_{(12)} \oplus r_t[15]_{(22)}$	$1/2(1 - 0.045410)$
$r_t[0]_{(12)} \oplus r_t[0]_{(11)} \oplus r_t[0]_{(10)} \oplus r_t[15]_{(22)} \oplus r_t[15]_{(21)} \oplus r_t[15]_{(20)}$	$1/2(1 - 0.020020)$

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, we see that the third approximation of Table 1 has high bias with only two terms. This seems to be caused by the fact 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 $r_t[0]'_{(H)} = (r_t[0] \lll 19)_{(H)} = (r_t[0]_{(12)}, \ldots, r_t[0]_{(5)})$ 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.

4.2 Linear Approximations for NFSR

Having a linear approximation of $\alpha_{t,(0)}$, it is easy to obtain a linear approximation for NFSR. For example, let us choose the first approximation from Table 1. Then, we have the following linear equation:

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

with the bias $0.048828 = 2^{-4.36}$. Now we combine Equations (5) and (6) and as the result we have the following approximation for NFSR

$$\begin{aligned} &r_t[0]_{(10)} \oplus r_t[0]_{(6)} \oplus r_t[15]_{(20)} \oplus r_t[15]_{(16)} \oplus r_t[15]_{(15)} \\ &\oplus r_t[0]_{(13)} \oplus r_t[15]_{(23)} \oplus Konst_{(0)} \oplus r_t[4]_{(0)} \oplus r_{t+1}[16]_{(0)} = 0 \end{aligned} \tag{7}$$

with the bias of $2^{-4.36}$.

4.3 Linear Approximations of Modular Addition

Let us take a look at the modular addition $\boxplus$. We know that the least significant bits are linear so the following equation holds

$$(r[x] \boxplus r[y])_{(0)} = r[x]_{(0)} \oplus r[y]_{(0)}. \tag{8}$$

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

$$(r[x] \boxplus r[y])_{(i)} \oplus (r[x] \boxplus r[y])_{(i-1)} = r[x]_{(i)} \oplus r[y]_{(i)} \oplus r[x]_{(i-1)} \oplus r[y]_{(i-1)} \quad (9)$$

that has the bias of 2^{-1}.

In a similar way, we also observe that the function $(r[x] \boxplus r[y])_{(i)} \oplus (r[x] \boxplus r[y])_{(i-1)} \oplus (r[x] \boxplus r[y])_{(i-2)} \oplus (r[x] \boxplus r[y])_{(i-3)}$ has the following approximation. For $i > 2$,

$$\begin{aligned}&(r[x] \boxplus r[y])_{(i)} \oplus (r[x] \boxplus r[y])_{(i-1)} \oplus (r[x] \boxplus r[y])_{(i-2)} \oplus (r[x] \boxplus r[y])_{(i-3)} = \\ &r[x]_{(i)} \oplus r[y]_{(i)} \oplus r[x]_{(i-1)} \oplus r[y]_{(i-1)} \oplus r[x]_{(i-2)} \oplus r[y]_{(i-2)} \oplus r[x]_{(i-3)} \oplus r[y]_{(i-3)}\end{aligned} \quad (10)$$

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

4.4 Linear Approximation for NLF

Recall that Equation (4) defines the output keystream generated by NLF. By Equation (8), we obtain the relation for the least significant bits of NLF that takes the following form

$$\nu_{t,(0)} = (r_t[0]_{(0)} \oplus r_t[16]_{(0)}) \oplus (r_t[1]_{(0)} \oplus r_t[13]_{(0)}) \oplus (r_t[6]_{(0)} \oplus Konst_{(0)}). \quad (11)$$

This relation holds with probability one.

For $2 \leq i \leq 31$ and using Equation (9), we can argue that NLF function has linear approximations of the following form:

$$\begin{aligned}\nu_{t,(i)} \oplus \nu_{t,(i-1)} = &(r_t[0]_{(i)} \oplus r_t[16]_{(i)} \oplus r_t[0]_{(i-1)} \oplus r_t[16]_{(i-1)}) \\ &\oplus (r_t[1]_{(i)} \oplus r_t[13]_{(i)} \oplus r_t[1]_{(i-1)} \oplus r_t[13]_{(i-1)}) \\ &\oplus (r_t[6]_{(i)} \oplus Konst_{(i)} \oplus r_t[6]_{(i-1)} \oplus Konst_{(i-1)})\end{aligned} \quad (12)$$

with the bias of $(2^{-1})^2 = 2^{-2}$ under the condition that $Konst = 0$.

Also applying Approximation (10), for $i > 2$, we get the following expression

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

that has the bias of $(2^{-2})^2 = 2^{-4}$ when $Konst = 0$.

For non-zero $Konst$, the bias of Approximations (12) and (13) will be studied in Section 6.2.

5 CP Attack on a Simplified NLS

In this Section we present the CP attack on a simplified NLS. This is a preliminary stage of our attack in which we apply the initial idea of crossword puzzle

attack that will be later developed and generalized. 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 (4) that describes the keystream becomes

$$\mu_t = (r_t[0] \oplus r_t[16]) \oplus (r_t[1] \oplus r_t[13]) \oplus (r_t[6] \oplus Konst). \tag{14}$$

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 $0 \le i \le 31$, we can write

$$\mu_{t,(i)} = (r_t[0]_{(i)} \oplus r_t[16]_{(i)}) \oplus (r_t[1]_{(i)} \oplus r_t[13]_{(i)}) \oplus (r_t[6]_{(i)} \oplus Konst_{(i)}). \tag{15}$$

To build a distinguisher we combine approximations of NFSR given by Equation (7) with linear equations defined by Equation (15). For the clocks t, $t+1$, $t+6$, $t+13$, and $t+16$, consider the following approximations of NFSR

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

Since $r_{t+p}[0] = r_t[p]$, we can rewrite the above system of equations (16) equivalently as follows:

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

Consider the columns of the above system of equations. Each column describes a single bit output of the filter (see Equation (15)), therefore the system (17) gives the following approximation:

$$\begin{array}{l}
\mu_{t,(10)} \oplus \mu_{t,(6)} \oplus \mu_{t+15,(20)} \oplus \mu_{t+15,(16)} \oplus \mu_{t+15,(15)} \oplus \mu_{t,(13)} \\
\oplus \mu_{t+15,(23)} \oplus \mu_{t+4,(0)} \oplus \mu_{t+17,(0)} = K
\end{array} \tag{18}$$

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, the bias of Approximation (18) is $(\mathbf{2^{-4.36}})^{\mathbf{5}} = \mathbf{2^{-21.8}}$.

6 The CP Attack on NLS

In this section, we describe the CP 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 $Konst \neq 0$. Since NLS allows only a non-zero most significant byte of $Konst$, the second case corresponds to the real NLS.

6.1 Case for $Konst = 0$

The linear approximations of $\alpha_{t,(0)}$ are given in Table 1. For the most effective distinguisher, we choose this time the third approximation from the table which is

$$\alpha_{t,(0)} = r_t[0]_{(12)} \oplus r_t[15]_{(22)} \tag{19}$$

and the bias of this approximation is $0.045410 = 2^{-4.46}$. By combining Equations (5) and (19), we have the following approximation

$$r_t[0]_{(12)} \oplus r_t[15]_{(22)} \oplus r_t[0]_{(13)} \oplus r_t[15]_{(23)} \oplus r_t[4]_{(0)} \oplus r_{t+1}[16]_{(0)} = 0 \tag{20}$$

that has the same bias.

Let us now divide (20) into two parts : the least significant bits and the other bits, so we get

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

Clearly, $l_1(r_t) \oplus l_2(r_t) = 0$ with the bias $2^{-4.46}$. Since $l_1(r_t)$ has only the least significant bit variables, we apply (11) which is true with the probability one. Then, we obtain

$$\begin{array}{lll} l_1(r_t) & = r_t[4]_{(0)} & \oplus\, r_{t+1}[16]_{(0)} \\ l_1(r_{t+1}) & = r_{t+1}[4]_{(0)} & \oplus\, r_{t+2}[16]_{(0)} \\ l_1(r_{t+6}) & = r_{t+6}[4]_{(0)} & \oplus\, r_{t+7}[16]_{(0)} \\ l_1(r_{t+13}) & = r_{t+13}[4]_{(0)} & \oplus\, r_{t+14}[16]_{(0)} \\ l_1(r_{t+16}) & = r_{t+16}[4]_{(0)} & \oplus\, r_{t+17}[16]_{(0)} \end{array} \tag{22}$$

If we add up all approximations of (22), then, by applying Equation (11), we can write

$$l_1(r_t) \oplus l_1(r_{t+1}) \oplus l_1(r_{t+6}) \oplus l_1(r_{t+13}) \oplus l_1(r_{t+16}) = \nu_{t+4,(0)} \oplus \nu_{t+17,(0)} \tag{23}$$

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

$$\begin{array}{llllll} l_2(r_t) & = r_t[0]_{(12)} & \oplus\, r_t[0]_{(13)} & \oplus\, r_t[15]_{(22)} & \oplus\, r_t[15]_{(23)} \\ l_2(r_{t+1}) & = r_{t+1}[0]_{(12)} & \oplus\, r_{t+1}[0]_{(13)} & \oplus\, r_{t+1}[15]_{(22)} & \oplus\, r_{t+1}[15]_{(23)} \\ l_2(r_{t+6}) & = r_{t+6}[0]_{(12)} & \oplus\, r_{t+6}[0]_{(13)} & \oplus\, r_{t+6}[15]_{(22)} & \oplus\, r_{t+6}[15]_{(23)} \\ l_2(r_{t+13}) & = r_{t+13}[0]_{(12)} & \oplus\, r_{t+13}[0]_{(13)} & \oplus\, r_{t+13}[15]_{(22)} & \oplus\, r_{t+13}[15]_{(23)} \\ l_2(r_{t+16}) & = r_{t+16}[0]_{(12)} & \oplus\, r_{t+16}[0]_{(13)} & \oplus\, r_{t+16}[15]_{(22)} & \oplus\, r_{t+16}[15]_{(23)} \end{array} \tag{24}$$

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

$$\begin{array}{llllll} l_2(r_t) & = r_t[0]_{(12)} & \oplus\, r_t[0]_{(13)} & \oplus\, r_{t+15}[0]_{(22)} & \oplus\, r_{t+15}[0]_{(23)} \\ l_2(r_{t+1}) & = r_t[1]_{(12)} & \oplus\, r_t[1]_{(13)} & \oplus\, r_{t+15}[1]_{(22)} & \oplus\, r_{t+15}[1]_{(23)} \\ l_2(r_{t+6}) & = r_t[6]_{(12)} & \oplus\, r_t[6]_{(13)} & \oplus\, r_{t+15}[6]_{(22)} & \oplus\, r_{t+15}[6]_{(23)} \\ l_2(r_{t+13}) & = r_t[13]_{(12)} & \oplus\, r_t[13]_{(13)} & \oplus\, r_{t+15}[13]_{(22)} & \oplus\, r_{t+15}[13]_{(23)} \\ l_2(r_{t+16}) & = r_t[16]_{(12)} & \oplus\, r_t[16]_{(13)} & \oplus\, r_{t+15}[16]_{(22)} & \oplus\, r_{t+15}[16]_{(23)} \end{array} \tag{25}$$

Recall the approximation (12) of NLF. If we combine (25) with (12), then we have the following approximation.

$$\begin{aligned} &l_2(r_t) \oplus l_2(r_{t+1}) \oplus l_2(r_{t+6}) \oplus l_2(r_{t+13}) \oplus l_2(r_{t+16}) = \\ &\nu_{t,(12)} \oplus \nu_{t,(13)} \oplus \nu_{t+15,(22)} \oplus \nu_{t+15,(23)} \end{aligned} \tag{26}$$

By combining the approximations (23) and (26), we obtain the final approximation that defines our distinguisher, i.e.

$$\begin{aligned} &l_1(r_t) \oplus l_1(r_{t+1}) \oplus l_1(r_{t+6}) \oplus l_1(r_{t+13}) \oplus l_1(r_{t+16}) \\ &\oplus l_2(r_t) \oplus l_2(r_{t+1}) \oplus l_2(r_{t+6}) \oplus l_2(r_{t+13}) \oplus l_2(r_{t+16}) \\ &= \nu_{t,(12)} \oplus \nu_{t,(13)} \oplus \nu_{t+15,(22)} \oplus \nu_{t+15,(23)} \oplus \nu_{t+4,(0)} \oplus \nu_{t+17,(0)} \\ &= 0 \end{aligned} \tag{27}$$

The second part of the approximation can be computed from the output keystream that is observable to the adversary. As we use Approximation (20) five times and Approximation (12) twice, the bias of the approximation (27) is $(\mathbf{2^{-4.46}})^{\mathbf{5}} \cdot (\mathbf{2^{-2}})^{\mathbf{2}} = \mathbf{2^{-26.3}}$.

6.2 Case for $Konst \neq 0$

Since the word $Konst$ occurs in NFSR and NLF as a parameter, the biases of linear approximations of both $\alpha_{t,(0)}$ and NLF vary with $Konst$. If we divide $Konst$ into two parts as $Konst = (Konst_{(H)}, Konst_{(L)})$ where $Konst_{(H)} = (Konst_{(31)}, \ldots, Konst_{(24)})$, and $Konst_{(L)} = (Konst_{(23)}, \ldots, Konst_{(0)})$, then, linear approximations of $\alpha_{t,(0)}$ mainly depend on $Konst_{(H)}$ and those of NLF depend on $Konst_{(L)}$.

Biases of $\alpha_{t,(0)}$ with non-zero $Konst_{(H)}$. Since the most significant 8 bits of $Konst$ mainly contribute to the form of the bit $\alpha_{t,(0)}$, the bias of Approximation (19) fluctuates according to the 8-bit $Konst_{(H)}$. This relation is illustrated in Figure 3.

From this figure, we can see that the bias of Approximation (19) becomes the smallest when $Konst_{(H)}$ is around 51 and 179 and the biggest when $Konst_{(H)}$ is around 127 and 255. The average bias of (19) with $Konst_{(H)}$ is $2^{-5.19}$.

Biases of NLF with $Konst_{(L)}$. Figure 4 displays the bias variation of Approximation (12) according to $Konst_{(L)}$ at $i = 13$. Note that the graph shows the bias distribution from 14 LSBs of $Konst_{(L)}$ (that is, 2^{14}) since the bits $Konst_{(23)}, \ldots, Konst_{(14)}$ do not effect the bias for $i = 13$. We do not display the graph of Approximation (12) at $i = 23$ because the graph is similar to Figure 4 with the slope changed as we consider 24 bits of $Konst_{(L)}$ only. On the average, the bias of (12) is 2^{-3} for any $i > 0$.

6.3 Bias of the Distinguisher

Let us denote the bias of Approximation (19) for NFSR by ϵ_1, the bias of Approximation (12) for NLF at $i = 13$ and $i = 23$ by $\epsilon_{2,13}$ and $\epsilon_{2,23}$ respectively.

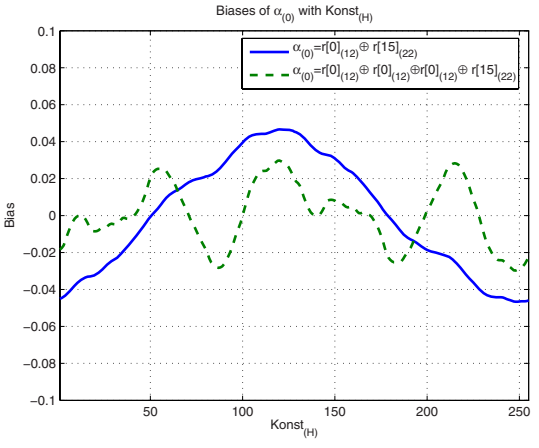

Fig. 3. Variation of biases of two $\alpha_{t,(0)}$ approximations with $Konst_{(H)}$

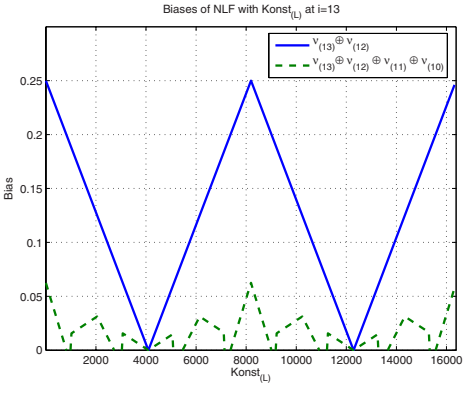

Fig. 4. Variation of biases of NLF with $Konst_{(L)}$ at $i = 13$

Note that all biases are $Konst$-dependent values. Since the $Konst$ is generated by randomization process at the initialization stage, it is reasonable assumption that all the $Konst$ values are equiprobable.

Hence, the bias of the distinguisher ϵ can be calculated as follows.

$$\epsilon = 2^{-32} \sum_{k=0}^{2^{32}-1} (\epsilon_1^5 \cdot \epsilon_{2,13} \cdot \epsilon_{2,23} | Konst = k)$$

See Appendix A for detail algorithm to compute the bias with a low complexity. Experiments shows that the bias of distinguisher appears to be 2^{-30}.

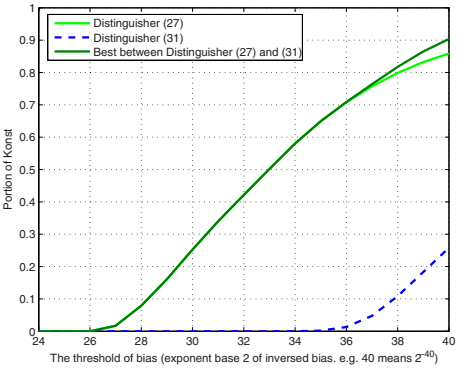

Fig. 5. The success rate of attack

6.4 The Success Rate of Distinguishing Attack

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 successful if the bias of distinguisher satisfies the following condition:

$$\epsilon_1^5 \cdot \epsilon_{2,13} \cdot \epsilon_{2,23} > 2^{-40}. \tag{28}$$

The experiments show that the bias of Distinguisher (27) satisfies the condition (28) on around 85.9% of $Konst$. See Figure 5.

7 Improving Distinguishing Attack by Multiple Distinguishers

In this section, we present multiple distinguishing attack for the purpose of reducing the portion of $Konst$ for which our attack fails. multiple approximations of $\alpha_{(0)}$. Since the NLS produces 32-bit keystream word per a clock, the actual volume of data required for the attack with multiple distinguishers is not increased even though more computation is required.

The motivation for multiple distinguishers is the fact that Approximation (19) is not always best for a distinguisher for all the possible values of $Konst$. For instance, the bias of the distinguisher based on Approximation (19) is very small for some values of $Konst_{(H)}$ (e.g. $Konst_{(H)} = 51$ or 179). In order to address this problem, we choose the fourth approximation from Table 1. Then, we have

$$\alpha_{t,(0)} = r_t[0]_{(12)} \oplus r_t[0]_{(11)} \oplus r_t[0]_{(10)} \oplus r_t[15]_{(22)} \oplus r_t[15]_{(21)} \oplus r_t[15]_{(20)} \tag{29}$$

which has the smallest bias when $Konst_{(H)}$ is around 41, 139 and 169 whereas the biggest when $Konst_{(H)}$ is around 57 and 185. The average bias of (29) is $2^{-6.2}$ when only absolute values are taken (see Figure 3).

Using this approximation, we build an approximation of NFSR as follows

$$r_t[0]_{(10)} \oplus r_t[0]_{(11)} \oplus r_t[0]_{(12)} \oplus r_t[0]_{(13)} \oplus r_t[15]_{(20)} \oplus r_t[15]_{(21)} \oplus r_t[15]_{(22)} \oplus r_t[15]_{(23)} \oplus Konst_{(0)} \oplus r_t[4]_{(0)} \oplus r_{t+1}[16]_{(0)} = 0. \tag{30}$$

Then, we can construct a new distinguisher by combining Approximation (13) on NLF. We omit the detail process due to the similarity of Distinguisher (27). In result, we have the following new distinguisher

$$\nu_{t,(10)} \oplus \nu_{t,(11)} \oplus \nu_{t,(12)} \oplus \nu_{t,(13)} \oplus \nu_{t+15,(20)} \oplus \nu_{t+15,(21)} \oplus \nu_{t+15,(22)} \oplus \nu_{t+15,(23)} \oplus \nu_{t+4,(0)} \oplus \nu_{t+17,(0)} = 0. \tag{31}$$

The bias of Distinguisher (31) can be calculated with a similar way to Section 6.3. In result, the bias of distinguisher appears to be $2^{-27.8} \cdot 2^{-10} = 2^{-37.8}$.

By observing two distinguishers together and selecting always the better bias among them, we improve the success rate of the distinguishing attack. The experiments show that the combined bias for Distinguishers (27) and (31) satisfies the condition (28) for around 90.3% of $Konst$ (see Figure 5).

8 The CP Attack on NLSv2

NLSv2 is a tweaked version of NLS [5]. The major difference from NLS is that $Konst$ is set to the output of the non-linear filter at every 65537 clock of the NFSR. This output is not used in the keystream.

Since Approximation (19) is biased positively or negatively according to $Konst$ (see Figure 3), the sign of the bias of distinguisher (27) also varies with $Konst$ value. Since the distinguisher (27) uses Approximation (20) five times, randomly changed $Konst$ could reduce the bias of distinguisher on the average.

However, this tweak version does not seem to have enough security margin against the CP attack. If a distinguisher uses the "even" number of linear approximations for NFSR then, the bias of the distinguisher becomes always positive irrespective of the sign of Approximation (27).

The smallest even number of approximations we found is eight, which is obtained by the addition of two consecutive outputs of NLF. Then, we apply the CP attack to NLSv2 with eight approximations of NFSR where the state positions are determined by two consecutive outputs of NLF. For detail approach to the CP attack against NLSv2, see Appendix B.

In summary, we estimate the bias of distinguisher by the similar way to Section 6.3. Experiments using the algorithm in Appendix A show that the bias is around $2^{-37.6} \cdot 2^{-10.4} = 2^{-48}$. Note that the bias of the distinguisher is always positive since $\epsilon_1^8 = (-\epsilon_1)^8 > 0$.

9 Conclusion

We presented a distinguishing attack on the NLS cipher using Crossword Puzzle attack. The bias of our distinguisher appears to be 2^{-30} so the NLS cipher is

distinguishable from a random function by observing 2^{60} keystream words. Even though there is a fraction of the $Konst$ values which requires the data complexity bigger than 2^{80}, we show that it is possible for attacker to reduce this fraction of $Konst$ substantially by combining multiple distinguishers which have biases of less than 2^{-40}. We also have constructed a distinguisher for the tweaked version of the cipher called NLSv2. Although the distinguisher does not break the cipher, it shows that the security margin is too small to guarantee the claimed security level for the near future.

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

References

1. eSTREAM project. `http://www.ecrypt.eu.org/stream/`
2. Cho, J.Y., Pieprzyk, J.: Linear distinguishing attack on NLS. In: SASC 2006 workshop (2006)
3. Coppersmith, D., Halevi, S., Jutla, C.: Cryptanalysis of stream ciphers with linear masking. In: Yung, M. (ed.) CRYPTO 2002. LNCS, vol. 2442, pp. 515–532. Springer, Heidelberg (2002)
4. Hawkes, P., Paddon, M., Rose, G., de Vries, M.W.: Primitive specification for NLS (April 2005), `http://www.ecrypt.eu.org/stream/nls.html`
5. Hawkes, P., Paddon, M., Rose, G., de Vries, M.W.: Primitive specification for NLSv2 (March 2006), `http://www.ecrypt.eu.org/stream/nls.html`
6. Matsui, M.: Linear cryptanalysis method for DES cipher. In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 386–397. Springer, Heidelberg (1994)

A Low Complexity Algorithm for the Bias of Distinguisher

According to Section 6.2, the bias of the distinguisher (27) can be computed using the following algorithm. Note that $Konst$ is expressed in hexadecimal.

1. Set $Konst = 01000000h$ (Note that non-zero $Konst_{(H)}$ is allowed in NLS.)
2. Find the bias ϵ_1 of Approximation (19) for NFSR.
3. Find the bias ϵ_2 of Approximation (12) for NLF.
4. Compute and store the bias ϵ of the distinguisher (27) by $\epsilon = \epsilon_{\mathbf{1}}^{\mathbf{5}} \cdot \epsilon_{\mathbf{2}}^{\mathbf{2}}$.
5. Increase $Konst$ by 1 and repeat Step 2,3 and 4 until $Konst = fffffffffh$.
6. Compute the estimation of ϵ.

In order to reduce the complexity of computing the estimation of ϵ, we assume that ϵ_1 is affected by only $Konst_{(H)}$, not by $Konst_{(L)}$ in Step 2. Then, ϵ_1 and

ϵ_2 can be computed independently. Therefore, the above algorithm is amended as follows.

1. Set $Konst_{(H)} = 01h$
2. Find the bias ϵ_1 of Approximation (19) and store $\epsilon_1^* = \epsilon_1^5$.
3. Increase $Konst_{(H)}$ by 1 and repeat Step 2 until $Konst_{(H)} = ffh$.
4. Set $Konst_{(L)} = 000000h$
5. Find two biases of Approximation (12) at $i = 13$ and $i = 23$, which is called $\epsilon_{2,13}$ and $\epsilon_{2,23}$ respectively.
6. Store ϵ_2^* by calculating $\epsilon_2 = \epsilon_{2,13} \cdot \epsilon_{2,23}$.
7. Increase $Konst_{(L)}$ by 1 and repeat Step 5 and 6 until $Konst_{(L)} = 00ffffffh$.
8. Compute the estimation of the bias of distinguisher (27) under the assumption that $Konst$ is equiprobable.

B The CP Attack on NLSv2

NLSv2 is a tweaked version of NLS [5]. We apply the CP attack to NLSv2 with eight approximations of NFSR where the state positions are determined by two consecutive outputs of NLF.

B.1 Linear Approximations of NLSv2

Suppose we have two consecutive outputs of NLF as follows.

$$\begin{aligned}
\nu_{t,(i)} \oplus \nu_{t,(i-1)} &= (r_t[0]_{(i)} \oplus r_t[16]_{(i)} \oplus r_t[0]_{(i-1)} \oplus r_t[16]_{(i-1)}) \\
&\oplus (r_t[1]_{(i)} \oplus r_t[13]_{(i)} \oplus r_t[1]_{(i-1)} \oplus r_t[13]_{(i-1)}) \\
&\oplus (r_t[6]_{(i)} \oplus Konst_{(i)} \oplus r_t[6]_{(i-1)} \oplus Konst_{(i-1)}) \\
\nu_{t+1,(i)} \oplus \nu_{t+1,(i-1)} &= (r_{t+1}[0]_{(i)} \oplus r_{t+1}[16]_{(i)} \oplus r_{t+1}[0]_{(i-1)} \oplus r_{t+1}[16]_{(i-1)}) \\
&\oplus (r_{t+1}[1]_{(i)} \oplus r_{t+1}[13]_{(i)} \oplus r_{t+1}[1]_{(i-1)} \oplus r_{t+1}[13]_{(i-1)}) \\
&\oplus (r_{t+1}[6]_{(i)} \oplus Konst_{(i)} \oplus r_{t+1}[6]_{(i-1)} \oplus Konst_{(i-1)}) \\
&= (r_t[1]_{(i)} \oplus r_t[17]_{(i)} \oplus r_t[1]_{(i-1)} \oplus r_t[17]_{(i-1)}) \\
&\oplus (r_t[2]_{(i)} \oplus r_t[14]_{(i)} \oplus r_t[2]_{(i-1)} \oplus r_t[14]_{(i-1)}) \\
&\oplus (r_t[7]_{(i)} \oplus Konst_{(i)} \oplus r_t[7]_{(i-1)} \oplus Konst_{(i-1)})
\end{aligned} \tag{32}$$

By adding up two approximations, we have

$$\begin{aligned}
\nu_{t,(i)} \oplus \nu_{t,(i-1)} \oplus \nu_{t+1,(i)} \oplus \nu_{t+1,(i-1)} &= \\
&= (r_t[0]_{(i)} \oplus r_t[16]_{(i)} \oplus r_t[0]_{(i-1)} \oplus r_t[16]_{(i-1)}) \\
&\oplus (r_t[1]_{(i)} \oplus r_t[13]_{(i)} \oplus r_t[1]_{(i-1)} \oplus r_t[13]_{(i-1)}) \\
&\oplus (r_t[6]_{(i)} \oplus Konst_{(i)} \oplus r_t[6]_{(i-1)} \oplus Konst_{(i-1)}) \\
&\oplus (r_t[1]_{(i)} \oplus r_t[17]_{(i)} \oplus r_t[1]_{(i-1)} \oplus r_t[17]_{(i-1)}) \\
&\oplus (r_t[2]_{(i)} \oplus r_t[14]_{(i)} \oplus r_t[2]_{(i-1)} \oplus r_t[14]_{(i-1)}) \\
&\oplus (r_t[7]_{(i)} \oplus Konst_{(i)} \oplus r_t[7]_{(i-1)} \oplus Konst_{(i-1)}) \\
&= (r_t[0]_{(i)} \oplus r_t[0]_{(i-1)}) \oplus (r_t[2]_{(i)} \oplus r_t[2]_{(i-1)}) \\
&\oplus (r_t[6]_{(i)} \oplus r_t[6]_{(i-1)}) \oplus (r_t[7]_{(i)} \oplus r_t[7]_{(i-1)}) \\
&\oplus (r_t[13]_{(i)} \oplus r_t[13]_{(i-1)}) \oplus (r_t[14]_{(i)} \oplus r_t[14]_{(i-1)}) \\
&\oplus (r_t[16]_{(i)} \oplus r_t[16]_{(i-1)}) \oplus (r_t[17]_{(i)} \oplus r_t[17]_{(i-1)})
\end{aligned} \tag{33}$$

The experiment shows that Approximation (33) has bias of around $2^{-5.2}$. Since $r_t[1]_{(i)} \oplus r_t[1]_{(i-1)}$ and $Konst_{(i)} \oplus Konst_{(i-1)}$ are canceled out, the bias of (33) is higher than the multiplication of bias of two approximation in (32). Hence, we use (33) for the approximation of NLF where the state position are $0, 2, 6, 7, 13, 14, 16, 17$. Note that the bias of (33) is still dependent on the value of $Konst$.

According to these state positions, the least significant bits have the following relation.

$$\nu_{t,(0)} \oplus \nu_{t+1,(0)} = r_t[0]_{(0)} \oplus r_t[2]_{(0)} \oplus r_t[6]_{(0)} \oplus r_t[7]_{(0)} \oplus r_t[13]_{(0)} \oplus r_t[14]_{(0)} \oplus r_t[16]_{(0)} \oplus r_t[17]_{(0)} \tag{34}$$

This relation also holds with probability one.

B.2 Building Distinguisher

This section is similar to Section 6 except that the eight (instead of five) approximations from the state position $0, 2, 6, 7, 13, 14, 16, 17$ are used for the CP attack.

Let us recall Approximation (21). For the least significant bits, we can write

$$\begin{array}{ll}
l_1(r_t) & = r_t[4]_{(0)} \oplus r_{t+1}[16]_{(0)} \\
l_1(r_{t+2}) & = r_{t+2}[4]_{(0)} \oplus r_{t+3}[16]_{(0)} \\
l_1(r_{t+6}) & = r_{t+6}[4]_{(0)} \oplus r_{t+7}[16]_{(0)} \\
l_1(r_{t+7}) & = r_{t+7}[4]_{(0)} \oplus r_{t+8}[16]_{(0)} \\
l_1(r_{t+13}) & = r_{t+13}[4]_{(0)} \oplus r_{t+14}[16]_{(0)} \\
l_1(r_{t+14}) & = r_{t+14}[4]_{(0)} \oplus r_{t+15}[16]_{(0)} \\
l_1(r_{t+16}) & = r_{t+16}[4]_{(0)} \oplus r_{t+17}[16]_{(0)} \\
l_1(r_{t+17}) & = r_{t+17}[4]_{(0)} \oplus r_{t+18}[16]_{(0)}
\end{array} \tag{35}$$

If we add up all approximations of (35), then, by applying Equation (34), we obtain

$$l_1(r_t) \oplus l_1(r_{t+2}) \oplus l_1(r_{t+6}) \oplus l_1(r_{t+7}) \oplus l_1(r_{t+13}) \oplus l_1(r_{t+14}) \oplus l_1(r_{t+16}) \oplus l_1(r_{t+17}) = \nu_{t+4,(0)} \oplus \nu_{t+5,(0)} \oplus \nu_{t+17,(0)} \oplus \nu_{t+18,(0)} \tag{36}$$

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

$$\begin{array}{lllll}
l_2(r_t) & = r_t[0]_{(12)} & \oplus r_t[0]_{(13)} & \oplus r_t[15]_{(22)} & \oplus r_t[15]_{(23)} \\
l_2(r_{t+2}) & = r_{t+2}[0]_{(12)} & \oplus r_{t+2}[0]_{(13)} & \oplus r_{t+2}[15]_{(22)} & \oplus r_{t+2}[15]_{(23)} \\
l_2(r_{t+6}) & = r_{t+6}[0]_{(12)} & \oplus r_{t+6}[0]_{(13)} & \oplus r_{t+6}[15]_{(22)} & \oplus r_{t+6}[15]_{(23)} \\
l_2(r_{t+7}) & = r_{t+7}[0]_{(12)} & \oplus r_{t+7}[0]_{(13)} & \oplus r_{t+7}[15]_{(22)} & \oplus r_{t+7}[15]_{(23)} \\
l_2(r_{t+13}) & = r_{t+13}[0]_{(12)} & \oplus r_{t+13}[0]_{(13)} & \oplus r_{t+13}[15]_{(22)} & \oplus r_{t+13}[15]_{(23)} \\
l_2(r_{t+14}) & = r_{t+14}[0]_{(12)} & \oplus r_{t+14}[0]_{(13)} & \oplus r_{t+14}[15]_{(22)} & \oplus r_{t+14}[15]_{(23)} \\
l_2(r_{t+16}) & = r_{t+16}[0]_{(12)} & \oplus r_{t+16}[0]_{(13)} & \oplus r_{t+16}[15]_{(22)} & \oplus r_{t+16}[15]_{(23)} \\
l_2(r_{t+17}) & = r_{t+17}[0]_{(12)} & \oplus r_{t+17}[0]_{(13)} & \oplus r_{t+17}[15]_{(22)} & \oplus r_{t+17}[15]_{(23)}
\end{array} \tag{37}$$

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

$$\begin{array}{lllll}
l_2(r_t) & = r_t[0]_{(12)} & \oplus\, r_t[0]_{(13)} & \oplus\, r_{t+15}[0]_{(22)} & \oplus\, r_{t+15}[0]_{(23)} \\
l_2(r_{t+2}) & = r_t[2]_{(12)} & \oplus\, r_t[2]_{(13)} & \oplus\, r_{t+15}[2]_{(22)} & \oplus\, r_{t+15}[2]_{(23)} \\
l_2(r_{t+6}) & = r_t[6]_{(12)} & \oplus\, r_t[6]_{(13)} & \oplus\, r_{t+15}[6]_{(22)} & \oplus\, r_{t+15}[6]_{(23)} \\
l_2(r_{t+7}) & = r_t[7]_{(12)} & \oplus\, r_t[7]_{(13)} & \oplus\, r_{t+15}[7]_{(22)} & \oplus\, r_{t+15}[7]_{(23)} \\
l_2(r_{t+13}) & = r_t[13]_{(12)} & \oplus\, r_t[13]_{(13)} & \oplus\, r_{t+15}[13]_{(22)} & \oplus\, r_{t+15}[13]_{(23)} \\
l_2(r_{t+14}) & = r_t[14]_{(12)} & \oplus\, r_t[14]_{(13)} & \oplus\, r_{t+15}[14]_{(22)} & \oplus\, r_{t+15}[14]_{(23)} \\
l_2(r_{t+16}) & = r_t[16]_{(12)} & \oplus\, r_t[16]_{(13)} & \oplus\, r_{t+15}[16]_{(22)} & \oplus\, r_{t+15}[16]_{(23)} \\
l_2(r_{t+17}) & = r_t[17]_{(12)} & \oplus\, r_t[17]_{(13)} & \oplus\, r_{t+15}[17]_{(22)} & \oplus\, r_{t+15}[17]_{(23)}
\end{array} \tag{38}$$

If we combine (38) with (33), then we have the following approximation.

$$l_2(r_t) \oplus l_2(r_{t+2}) \oplus l_2(r_{t+6}) \oplus l_2(r_{t+7}) \oplus l_2(r_{t+13}) \oplus l_2(r_{t+14}) \oplus l_2(r_{t+16}) \oplus l_2(r_{t+17}) = \nu_{t,(12)} \oplus \nu_{t,(13)} \oplus \nu_{t+1,(12)} \oplus \nu_{t+1,(13)} \oplus \nu_{t+15,(22)} \oplus \nu_{t+15,(23)} \oplus \nu_{t+16,(22)} \oplus \nu_{t+16,(23)} \tag{39}$$

By combining the approximations (36) and (39), we obtain the final approximation that defines our distinguisher, i.e.

$$\begin{array}{ll}
 & l_1(r_t) \oplus l_1(r_{t+1}) \oplus l_1(r_{t+6}) \oplus l_1(r_{t+13}) \oplus l_1(r_{t+16}) \\
 & \oplus l_2(r_t) \oplus l_2(r_{t+1}) \oplus l_2(r_{t+6}) \oplus l_2(r_{t+13}) \oplus l_2(r_{t+16}) \\
= & \nu_{t+4,(0)} \oplus \nu_{t+5,(0)} \oplus \nu_{t+17,(0)} \oplus \nu_{t+18,(0)} \oplus \nu_{t,(12)} \oplus \nu_{t,(13)} \\
 & \oplus \nu_{t+1,(12)} \oplus \nu_{t+1,(13)} \oplus \nu_{t+15,(22)} \oplus \nu_{t+15,(23)} \oplus \nu_{t+16,(22)} \oplus \nu_{t+16,(23)} \\
= & 0
\end{array} \tag{40}$$

The second part of the approximation is observable to the adversary.

The bias of the distinguisher. We compute the bias of Approximation (40) with a similar way to Section 6.3. Let us denote ϵ_1 as the bias of Approximation (20) for NFSR, the bias of Approximation (33) for NLF at $i = 13$ and $i = 23$ by $\epsilon_{3,13}$ and $\epsilon_{3,23}$ respectively.

Then, the bias of the distinguisher ϵ can be calculated as follows.

$$\epsilon = 2^{-32} \sum_{k=0}^{2^{32}-1} (\epsilon_1^8 \cdot \epsilon_{3,13} \cdot \epsilon_{3,23} | Konst = k)$$

Experiment shows that the bias of Approximation (40) is around 2^{-48}.