VERSITA

TATRA MOUNTAINS
Mathematical Publications
DOI: 10.2478/v10127-012-0037-5
Tatra Mt. Math. Publ. **53** (2012), 21–32

ON DISTINGUISHING ATTACK AGAINST THE REDUCED VERSION OF THE CIPHER NLSv2

Michal Braško — Jaroslav Boor

ABSTRACT. The Australian stream cipher NLSv2 [Hawkes, P.—Paddon, M.––Rose, G. G.—De Vries, M. W.: *Primitive specification for NLSv2*, Project eSTREAM web page, 2007, 1–25] is a 32-bit word oriented stream cipher that was quite successful in the stream ciphers competition—the project eSTREAM. The cipher achieved Phase 3 and successfully accomplished one of the main requirements for candidates in Profile 1 (software oriented proposals)—to have a better performance than AES in counter mode. However the cipher was not chosen into the final portfolio [Babbage, S.–De Cannière, Ch.–Canteaut, A.–Cid, C.––Gilbert, H.–Johansson, T.–Parker, M.–Preneel, B.–Rijmen, V.–Robshaw, M.: *The eSTREAM Portfolio*, Project eSTREAM web page, 2008], because its performance was not so perfect when comparing with other finalist. Also there is a security issue with a high correlation in the used S-Box, which some effective distinguishers exploit. In this paper, a practical demonstration of the distinguishing attack against the smaller version of the cipher is introduced. In our experiments, we have at disposal a machine with four cores (Intel$^{®}$ Core^{TM} Quad @ 2.66 GHz) and single attack lasts about 6 days. We performed successful practical experiments and our results demonstrate that the distingushing attack against the smaller version is working.

1. Introduction

The cipher NLSv2 is a synchronous, word-oriented stream cipher developed by Australian researchers Philip Hawkes, Cameron McDonald, Michael Paddon, Gregory G. Rose and Miriam Wiggers de Vreis in 2007 [6]. The "word-oriented" means that the cipher's algorithms use 32-bit operations on 32-bit words (e.g., XOR or modular addition). The internal state consists of 18 words (17 words in register and a special word *Konst*).

2010 Mathematics Subject Classification: 62K05.
Keywords: distinguish, stream cipher, attack, nonlinear, algorithm.
This material is based upon work supported under the grants APVV-0586–11 and APVV--0513–10.

To continue further, look at Table 1 with the definitions and notations used in this paper.

Table 1. Notations and definitions.

$+$	addition modulo 2^{32}
$<<<$ $(>>>)$	bitwise rotation to the left (right)
$\oplus$	exclusive or (xor)
$f16$	the 16th Fermat number, $2^{16}+1=65537$
σ_t	register state in time t, divided into seventeen 32-bit words $\sigma_t=(r_t[0],\ldots,r_t[16])$
$Konst$	32-bit key-depended word, part of the internal state
f	nonlinear feedback S-box function
t	counter (time)
$NLF(\sigma_t)$	nonlinear filter function
v_t	32-bit output value, $v_t=NLF(\sigma_t)$

1.1. Internal structure and construction

The NLSv2 structure consists of three parts: nonlinear feedback shift register (NFSR), nonlinear filter function (NLF) and counter function (Figure 1).

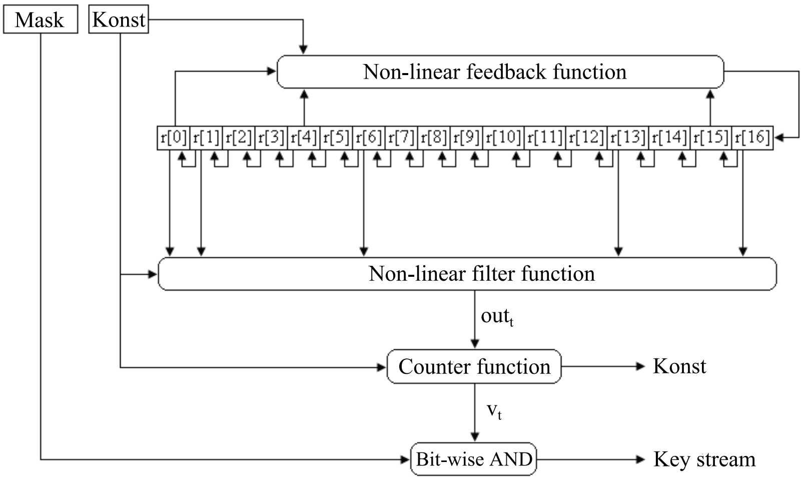
Mask
Konst
Non-linear feedback function
r[0] r[1] r[2] r[3] r[4] r[5] r[6] r[7] r[8] r[9] r[10] r[11] r[12] r[13] r[14] r[15] r[16]
Non-linear filter function
out_t
Counter function
Konst
v_t
Bit-wise AND
Key stream

Figure 1. Simplified scheme of the NLSv2 internal structure.

The NFSR uses nonlinear feedback function to shift the register from the state σ_t to the state σ_{t+1}. The first sixteen words are just shifted to the left and the 17th word is updated by the equation (1).

$$r_{t+1}[16] = f\Big(\big(r_t[0] <<< 19\big) + \big(r_t[15] <<< 9\big) + Konst\Big) \oplus r_t[4]. \qquad (1)$$

In each round one word out_t is computed by nonlinear filter function

$$out_t = NLF(\sigma_t) = \big(r_t[0] + r_t[16]\big) \oplus \big(r_t[1] + r_t[13]\big) \oplus \big(r_t[6] + Konst\big). \qquad (2)$$

Function counter decides whether out_t goes into the keystream. It is so besides the every f 16th round, when the out_t updates the $Konst$ and keystream is not appended.

1.2. Security and distinguishing attacks

The authors guarantee the cipher provides 128-bit security if following requirements are met:

- at least 128-bit long key is used,
- no pair key + IV is ever used more than once,
- no more than 2^{80} words are generated from a single key,
- no more than 2^{48} words are generated from a single pair key + IV.

For more detailed analysis about NLSv2 security see [6, p. 15].

Despite the authors' assurance of the cipher resistance to various attacks, cryptanalysis showed weaknesses of the first and also the second version of the cipher NLS. Joo Yeon Cho and Josef Pieprzyk [5] utilized weaknesses in a high correlation between adjacent bits of the register and a nonlinear filter and presented distinguishing "crossword puzzle" attacks on the cipher.

Table 2. The cipher NLS distinguishing attacks comparison.

	Distinguisher bias	How many words is required to distinguish them from a truly random sequence
First attack on NLSv1	2^{-30}	2^{60}
First attack on NLSv2	2^{-48}	2^{96}
Second attack on NLSv2	2^{-37}	2^{74}

The first attack worked very well with the first version of the NLS, which is not updating the value $Konst$ regularly. The attack is based on an existing correlation between adjacent bits in modular addition and a high correlation between the bits 29 and 30 in the S-box [5, p. 6]. Accordingly, there is a good linear approximation of feedback and filter functions. The bias of such distinguisher is approximately 2^{-30} and distinguishing attack requires to generate 2^{60} words [3], [4].

Because of this attack, the authors strengthened cipher and marked as NLS version 2. The value $Konst$ is updated regularly by NLF output to neutralize the distinguisher bias. This is partly succeeded and bias is about 2^{-48}. Since the cipher closely meets the security word limit 2^{80}, we can say that the NLS v2 is resistant to the first attack.

But the improved "crossword puzzle" attack no. 2 is successful also against the NLS v2. It uses linear approximations in a much better way and the resulting distinguisher bias is approximately 2^{-37} [5].

2. NLSv2 smaller version proposal

Given that we would need at least 2^{74} generated words to realize the attack, which is impossible with our computing power in real time, we proposed a reduced version of the cipher. Reduced version of the cipher has to retain all the essential characteristics of the cipher needed in the attack. The proposal was developed according to the process describing the full version attack [5]. The goal was to have such resulting distinguisher bias that needs maximum 2^{44} generated words. This value was estimated upon the following facts:

- The generation of 2^{44} words with full cipher version takes approximately 4 days within the testing environment.
- The reduced version was expected to generate faster.
- The generation time is increased by running distinguisher.

The cipher reduction is based on three points that are constructed in this manner because of the reduced distinguishing attack (explained in the next section):

(1) The number of words in register is reduced from 17 to 11.
Reason: Smaller register occupies less memory and is faster regarding generation and attack algorithms.

(2) The NFSR feedback function is slightly changed

$$r_{t+1}[10] = f\Big(\big(r_t[0] <<< 19\big) + \big(r_t[9] <<< 9\big) + Konst\Big) \oplus r_t[2]. \qquad (3)$$

There are only necessary changes in “tap” positions. The S-Box function is unchanged, although it has the biggest impact on the bias. But it is an essential property of the cipher used by attack and we cannot modify it. *Reason:* The “tap” positions are changed due to reduced register size and changed approximations equations of the attack.

(3) Filter function is reduced from three to two terms

$$out_t = NLF(\sigma_t) = \big(r_t[0] + r_t[10]\big) \oplus \big(r_t[1] + Konst\big). \tag{4}$$

Here must be considered such formula form, which annuls value $Konst$ in linear approximations of the attack.
Reason: The smaller equation is faster to be computed and there are changed approximations equations of the attack. which depend on the filter function.

3. Attack definition

We proposed distinguishing attack on the reduced version of the cipher upon the original attack and we used the same linear approximations based on a replacement of modular additions by xors with certain probability [5, p. 2–4]. There are used three base terms in the attack description defined by definitions 1, 2 and 3.

Definition 1. Γ_i denotes a linear masking vector over $GF(2)$ which has ‘1’ only on the bit positions of i and $i+1$. Then, $\Gamma_i.x = x_{(i)} \oplus x_{(i+1)}$, where ‘.’ denotes the standard inner product and $x_{(i)}$ is the ith bit of the 32-bit word x.

Definition 2. A bias ϵ is defined as follows

$$P = \tfrac{1}{2}(1+\epsilon), |\epsilon| > 0$$

where P is the probability that an approximation holds.

Definition 3. The carry $R(x,y)$ generated in modular addition $z = x + y$, where $x, y, z \in \{0,1\}^{32}$, is defined as follows

$$\begin{aligned} R(x,y)_{(0)} &= x_{(0)}y_{(0)},\ R(x,y)_{(i)} \\ &= x_{(i)}y_{(i)} \oplus \sum_{j=0}^{i-1} x_{(j)}y_{(j)} \prod_{k=j+1}^{i} x_{(k)}y_{(k)}, \quad i = 1, 2, \ldots \end{aligned} \tag{5}$$

3.1. NFSR linear approximation

Authors of the original attack analyzed adjacent bits in S-Box and found out, that the greatest bias is between the bits 29 and 31. The linear approximation $\alpha_{29} \oplus \alpha_{30} = 1$ has a bias approximately $2^{-2.3}$, which means that a probability that the bits 29 and 30 are same is 0.4. These two bits come from the Skipjack S-Box and are known from 1998 [2].

Lemma 1. *Let ω is denoted as an argument of the S-Box function f in equation* (3)*. Then according to the bias between bits 29 and 30 we can approximate $f(\omega)$ by ω with a bias $2^{-2.3}$*

$$\Gamma_{29}.(\omega \oplus f(\omega)) = 1. \tag{6}$$

Based on equation (3), following relation is always true

$$\Gamma_{29}.\big(f(\omega)_t \oplus r_t[2] \oplus r_{t+1}[10]\big) = 0. \tag{7}$$

Combining (6) and (7), we have an approximation with bias $2^{-2.3}$

$$\Gamma_{29}.\big(\omega_t \oplus r_t[2] \oplus r_{t+1}[10]\big) = 1, \epsilon \approx 2^{-2.3}. \tag{8}$$

In the next approximations, we used a linear property of the NFSR that is done by shifting character of the register

$$r_{t+i}[j] = r_{t+j}[i], \quad \text{where} \quad i, j > 0.$$

3.2. NLF linear approximation

In the NLF linear approximation, we used similar approach as in [4], but we used bit positions 29 and 30 instead of 12, 13, 22 and 23.

Lemma 2. *Let have two consecutive outputs from the NLF v_t and v_{t+1}. Then approximation* (9) *has bias $2^{-3.585}$.*

$$\Gamma_{29}.(v_t \oplus v_{t+1}) = \Gamma_{29}.\big(r_t[0] \oplus r_t[2] \oplus r_t[10] \oplus r_{t+1}[10]\big). \tag{9}$$

To prove Lemma 2 we need two corollaries[1] and a fact that

$$r_{t+1}[i] = r_t[i+1] \qquad \text{for} \quad i = 0, \dots, 15.$$

Corollary 1. *Let $x, y \in \{0,1\}^{32}$, then XOR of arbitrary consecutive bits is zero with constant probability*

$$Pr\big[\Gamma_{i-1}.R(x,y) = 0\big] = \frac{3}{4}, \qquad \textit{for} \quad i = 1, \dots, 31. \tag{10}$$

Upon the corollary, following approximation has probability $\frac{3}{4}$, $\epsilon = 2^{-1}$,

$$\Gamma_i(x+y) = \Gamma_i(x \oplus y), \qquad i = 0, \dots, 30. \tag{11}$$

Corollary 2. *Let $x, y, z \in \{0,1\}^{32}$, then following approximation is true with the probability*

$$Pr = \frac{2}{3} + \frac{1}{3}2^{-2i-2}, \qquad i = 0, \dots, 30, \ i = 29, \ \epsilon \approx 2^{-1.585}$$

$$\Gamma_i.(x+y) \oplus \Gamma_i.(x+z) = \Gamma_i.(y \oplus z). \tag{12}$$

[1] Lemmas and corollaries together with proofs can be found in [5].

Proof. Two consecutive outputs from the NLF are calculated as

$$\begin{aligned} v_t \oplus v_{t+1} = \big(r_t[0] + r_t[10]\big) \\ \oplus \big(r_t[1] + Konst\big) \oplus \big(r_{t+1}[0] + r_{t+1}[10]\big) \oplus \big(r_{t+1}[1] + Konst\big). \end{aligned} \tag{13}$$

Using the equations (11) and (12) we have

$$\begin{aligned} \Gamma_{29}.\big(r_t[1] + Konst\big) \oplus \big(r_{t+1}[1] + Konst\big) &= \Gamma_{29}.\big(r_t[1] \oplus r_{t+1}[1]\big), \quad \epsilon \approx 2^{-1.585}; \\ \Gamma_{29}.\big(r_t[0] + r_t[10]\big) &= \Gamma_{29}.\big(r_t[0] \oplus r_t[10]\big), \qquad \epsilon \approx 2^{-1}; \\ \Gamma_{29}.\big(r_{t+1}[0] + r_{t+1}[10]\big) &= \Gamma_{29}.\big(r_{t+1}[0] \oplus r_{t+1}[10]\big), \quad \epsilon \approx 2^{-1}. \end{aligned} \tag{14}$$

In (14) $r_t[1]$ and $r_{t+1}[0]$ are discarded and the proof is done. □

For comparison, the best NLF linear approximation in the full version of the cipher was [5, p. 7]

$$\begin{aligned} \Gamma_{29}.(v_t \oplus v_{t+1}) = \Gamma_{29}.\big(r_t[0] \oplus r_t[2] \oplus r_t[6] \oplus r_t[7] \oplus \\ \oplus r_t[13] \oplus r_t[14] \oplus r_t[16] \oplus r_{t+1}[16]\big), \qquad \epsilon \approx 2^{-5.2}. \end{aligned} \tag{15}$$

3.3. The bias of distinguisher

The attack is developed from the approximation (8) using time positions that come from approximation (9) $\eta = \{0, 2, 10, 11\}$. It is an important fact that the approximation (8) consists from a linear part $\Gamma_{29}.\big(r_t[2] \oplus r_{t+1}[10]\big)$ and a nonlinear part $\Gamma_{29}.\omega_t$. Their biases are analyzed independently by the following terms

$$X_t = \bigoplus_{k \in \eta} \Gamma_{29}.(r_{t+k}[2] \oplus r_{t+k+1}[10]), \quad Y_t = \bigoplus_{k \in \eta} \Gamma_{29}.\omega_{t+k}. \tag{16}$$

The bias of linear part

According to the linear property of the NFSR, we can state X_t as

$$X_t = \bigoplus_{k \in \eta} \Gamma_{29}.\big(r_{t+k}[2] \oplus r_{t+k+1}[10]\big) = \bigoplus_{k \in \eta} \Gamma_{29}.\big(r_{t+2}[k] \oplus r_{t+11}[k]\big). \tag{17}$$

Question is what bias has the following approximation of X_t,

$$X_t = \bigoplus_{k \in \eta} \Gamma_{29}.\big(r_{t+2}[k] \oplus r_{t+11}[k]\big) = \Gamma_{29}.\big(v_{t+2} \oplus v_{t+3} \oplus v_{t+11} \oplus v_{t+12}\big)? \tag{18}$$

The term (18) can be splitted into several parts

$$\begin{aligned} X_t =& \Gamma_{29}.\big(v_{t+2} \oplus v_{t+3} \oplus v_{t+11} \oplus v_{t+12}\big) \\ =& \Gamma_{29}.\big(r_{t+2}[0] + r_{t+2}[10]\big) \oplus \Gamma_{29}.\big(r_{t+2}[1] + Konst\big) \\ & \oplus \Gamma_{29}.\big(r_{t+3}[0] + r_{t+3}[10]\big) \oplus \Gamma_{29}.\big(r_{t+3}[1] + Konst\big) \\ & \oplus \Gamma_{29}.\big(r_{t+11}[0] + r_{t+11}[10]\big) \oplus \Gamma_{29}.\big(r_{t+11}[1] + Konst\big) \\ & \oplus \Gamma_{29}.\big(r_{t+12}[0] + r_{t+12}[10]\big) \oplus \Gamma_{29}.\big(r_{t+12}[1] + Konst\big). \end{aligned} \tag{19}$$

Corollary 3. *Let $x, y, z, w \in \{0,1\}^{32}$, then following approximation is true with probability*

$$Pr = \frac{29}{48} + \frac{1}{3}2^{-2i-4},\ i = 0, \dots, 30\ (i = 29, \epsilon \approx 2^{-2.263}),$$

$$\Gamma_i.(x + y) \oplus \Gamma_i(x + z) \oplus \Gamma_i(y + w) = \Gamma_i(z \oplus w). \tag{20}$$

Using the equations (11), (12) and (20), we can have these particular approximations with biases:

$$\begin{aligned} &\big(r_{t+3}[0] + r_{t+3}[10]\big) \oplus \big(r_{t+2}[1] + Konst\big) \oplus \big(r_{t+3}[1] + Konst\big) \\ &= \big(r_{t+3}[1] \oplus r_{t+3}[10]\big), && \epsilon \approx 2^{-2.263}, \\ &\big(r_{t+2}[10] + Konst\big) \oplus \big(r_{t+12}[1] + Konst\big) \\ &= \big(r_{t+2}[10] \oplus r_{t+12}[1]\big), && \epsilon \approx 2^{-1.585}, \\ &\big(r_{t+2}[0] + r_{t+2}[10]\big) \oplus \big(r_{t+12}[0] + r_{t+12}[10]\big) \\ &= \big(r_{t+2}[0] \oplus r_{t+12}[10]\big), && \epsilon \approx 2^{-1.585}, \\ &\big(r_{t+11}[0] + r_{t+11}[10]\big) \\ &= \big(r_{t+11}[0] \oplus r_{t+11}[10]\big), && \epsilon = 2^{-1}. \end{aligned} \tag{21}$$

When biases from the equations (21) are given together, we can see that bias of X_t is $\epsilon \approx 2^{-6.433}$.

For comparison, such bias in full version of the cipher is $\epsilon \approx 2^{-8.6}$.

The bias of nonlinear part

The analysis in this part goes from the relation for the ω_t as the argument of S-Box function f

$$\omega_t = \big(r_t[0]^{<<<19}\big) + \big(r_t[9]^{<<<9}\big) + Konst. \tag{22}$$

We use following Corollary

Corollary 4. *Let $x, y, z \in \{0,1\}^{32}$, then following approximation is true with probability*

$$\begin{aligned} Pr = \frac{2}{3} + \frac{1}{3} 2^{-2i-1}! \; i = 0, \dots, 30 \; (i = 29, \epsilon \approx 2^{-1.585}), \\ \Gamma_i.(x + y + z) = \Gamma_i.(x \oplus y \oplus z). \end{aligned} \tag{23}$$

By applying the corollary (23) onto the relation (22), we have bias $\epsilon \approx 2^{-1.585}$,

$$\begin{aligned} \Gamma_{29}.\omega_t &= \Gamma_{29}\big(r_t[0]^{<<<19} + r_t[9]^{<<<9} + Konst\big) \\ &= \big(\Gamma_{10}.r_t[0]\big) \oplus \big(\Gamma_{20}.r_t[9]\big) \oplus (\Gamma_{29}.Konst). \end{aligned} \tag{24}$$

By combining nonlinear part Y_t with (24), we have

$$Y_t = \bigoplus_{k \in \eta} \Gamma_{29}.\omega_{t+k} = \bigoplus_{k \in \eta} \big((\Gamma_{10}.r_{t+k}[0]) \oplus (\Gamma_{20}.r_{t+k}[9]) \oplus (\Gamma_{29}.Konst)\big). \tag{25}$$

Question is what bias has the following approximation of Y_t

$$\begin{aligned} Y_t &= \bigoplus_{k \in \eta} \Big(\big(\Gamma_{10}.r_{t+k}[0]\big) \oplus \big(\Gamma_{20}.r_{t+k}[9]\big) \oplus \big(\Gamma_{29}.Konst\big)\Big) \\ &= \Gamma_{10}.(v_t \oplus v_{t+1}) \oplus \Gamma_{20}.(v_{t+9} \oplus v_{t+10})? \end{aligned} \tag{26}$$

The term (26) can be splitted into several parts

$$\begin{aligned} Y_t &= \Gamma_{10}.(v_t \oplus v_{t+1}) \oplus \Gamma_{20}.(v_{t+9} \oplus v_{t+10}) \\ &= \Gamma_{10}.\big(r_t[0] + r_t[10]\big) \oplus \Gamma_{10}.\big(r_t[1] + Konst\big) \\ &\quad \oplus \Gamma_{10}.\big(r_{t+1}[0] + r_{t+1}[10]\big) \oplus \Gamma_{10}.\big(r_{t+1}[1] + Konst\big) \\ &\quad \oplus \Gamma_{20}.\big(r_{t+9}[0] + r_{t+9}[10]\big) \oplus \Gamma_{20}.\big(r_{t+9}[1] + Konst\big) \\ &\quad \oplus \Gamma_{20}.\big(r_{t+10}[0] + r_{t+10}[10]\big) \oplus \Gamma_{20}.\big(r_{t+10}[1] + Konst\big). \end{aligned} \tag{27}$$

When approximating particular parts from (27), we have following terms with biases:

$$\begin{aligned} \Gamma_{10}.\big(r_{t+1}[0] + r_{t+1}[10]\big) \oplus \Gamma_{10}.\big(r_t[1] + Konst\big) \oplus \Gamma_{10}.\big(r_{t+1}[1] + Konst\big) = \Delta_1, \\ \Delta_1 = \Gamma_{10}.\big(r_{t+1}[10] \oplus r_{t+1}[1]\big), \qquad \epsilon \approx 2^{-2.263}. \end{aligned}$$

$$\begin{aligned} \Gamma_{20}.\big(r_{t+10}[0] + r_{t+10}[10]\big) \oplus \Gamma_{20}.\big(r_{t+9}[1] + Konst\big) \oplus \Gamma_{20}.\big(r_{t+10}[1] + Konst\big) = \Delta_2, \\ \Delta_2 = \Gamma_{20}.\big(r_{t+10}[10] \oplus r_{t+10}[1]\big), \qquad \epsilon \approx 2^{-2.263}. \end{aligned}$$

$$\begin{aligned} \Gamma_{10}.\big(r_t[0] + r_t[10]\big) &= \Gamma_{10}.\big(r_t[0] \oplus r_t[10]\big), \qquad \epsilon \approx 2^{-1}. \\ \Gamma_{20}.\big(r_{t+9}[0] + r_{t+9}[10]\big) &= \Gamma_{20}.\big(r_{t+9}[0] \oplus r_{t+9}[10]\big), \qquad \epsilon \approx 2^{-1}. \end{aligned} \tag{28}$$

When biases from equations (28) are given together, we can see that bias of Y_t is $\epsilon \approx 2^{-6.526}$.

For comparison, such bias in full version of the cipher is $\epsilon \approx 2^{-10.4}$.

The overall bias

The overall distinguisher bias is derived from previously computed results. The approximation (29) is derived from (8) and its bias is approximately $\epsilon \approx 2^{-2.3\times 4}$. Multiple $\times 4$ is because we are using four time positions $\eta = \{0, 2, 10, 11\}$.

$$\bigoplus_{k\in\eta} \Gamma_{29}.\big(\omega_{t+k} \oplus r_{t+k}[2] \oplus r_{t+1+k}[10]\big) = X_t \oplus Y_t = 0. \tag{29}$$

By combining (18) and (26) we have an approximation with bias

$$\epsilon \approx \big(2^{-6.433} \times 2^{-6.526}\big)$$

$$\begin{aligned} X_t \oplus Y_t = {} & \Gamma_{29}.(v_{t+2} \oplus v_{t+3} \oplus v_{t+11} \oplus v_{t+12}) \\ & \oplus \Gamma_{10}.(v_t + v_{t+1}) \oplus \Gamma_{20}.(v_{t+9} \oplus v_{t+10}). \end{aligned} \tag{30}$$

Lemma 3. *Let us have a stream cipher described by* [6] *with re-defined feedback function* (3)*and filter function* (4)*. Then a distinguishing attack exists with bias approximately*

$$\epsilon \approx \big(2^{-2.3\times 4} \times 2^{-6.433} \times 2^{-6.526}\big) \approx 2^{-22.16}$$

and is given by the following equation

$$\begin{aligned} & \Gamma_{29}.(v_{t+2} \oplus v_{t+3} \oplus v_{t+11} \oplus v_{t+12}) \\ & \qquad \oplus \Gamma_{10}.(v_t + v_{t+1}) \oplus \Gamma_{20}.(v_{t+9} \oplus v_{t+10}) = 0. \end{aligned} \tag{31}$$

Proof. The proof is done by all the previous analysis from the current chapter and their deductions. □

From Lemma 3 it results that it is needed to generate at least 2^{44} words to perform such a distinguisher attack. That is to say that the attack can be practically realized according to our predictions.

For comparison, the distinguisher for the full version has bias approximately

$$\epsilon \approx \big(2^{-2.3\times 8} \times 2^{-8.6} \times 2^{-10.4}\big) \approx 2^{-37.4},$$

needs to generate 2^{74} words and is done by the following equation

$$\begin{aligned} & \Gamma_{29}.(v_{t+4} \oplus v_{t+5} \oplus v_{t+17} \oplus v_{t+18}) \oplus \Gamma_{10}.(v_t + v_{t+1}) \\ & \qquad \oplus \Gamma_{20}.(v_{t+15} \oplus v_{t+16}) = 0. \end{aligned} \tag{32}$$

Table 3. Testing machine configuration.

Operating system	Microsoft Windows 7 64 bit
CPU	Intel Core Quad @ 2.66 GHz
Memory	4 GB RAM

Table 4. Tests results.

Test	Count	Count ratio
Distinguisher – zeros	8 804 416 580 426	50.0473 %
Distinguisher – ones	8 787 769 463 976	49.9527 %
Generated sequence – zeros	281 474 969 724 665	49.9999 %
Generated sequence – ones	281 474 983 696 583	50.0001 %

4. Distinguishing attack realization and results

Implementation and testing environment

We based our attack realization on the reference code of the original version of the cipher NLSv2. We adapted the source code, reduced cipher's internal state and generation algorithm. Unlike storing whole generated sequence in memory in the original version, we store only a small needed part in a cycling array and compute distinguisher's output for each generated word.

The testing machine configuration is shown in Table 3. Each single test includes generation of 2^{44} words (2^{46} bytes) and computation how many zeros and ones were contained in generated sequence and produced by the distinguisher. One test lasts almost 6 days and we performed 20 tests. The whole testing lasted about one month on quad-core processor with four tests running in parallel.

Tests results

Table 4 shows average tests results after 20 completed tests. We can see that tests confirm our assumptions and number of zeros in distinguisher is higher than ones. Percentage number of zeros is 50.0473 % zeros and it is much different from 50 % when comparing with the generated keystreams (49.9999 % zeros in keystream).

5. Conclusion

We discussed distinguishing attacks on the cipher NLSv2 in this paper. Seeing that the original attack on the full version of the cipher is rather theoretical and its practical verification is not possible with our resources in real time (year 2012), we proposed a reduced attack on the reduced version of the cipher. Such attack exists and was practically realized. We performed 20 tests, each one lasts about 6 days. The results obtained from the tests confirmed our assumptions and number of zeros was notable higher than number of ones (50.0473 % zeros in distinguisher).

Acknowledgements. We are grateful to an anonymous referee for helpful comments.

REFERENCES

[1] BABBAGE, S.—DE CANNIÈRE, CH.—CANTEAUT, A.—CID, C.—GILBERT, H.–JOHANSSON, T.—PARKER, M.—PRENEEL, B.—RIJMEN, V.—ROBSHAW, M.: *The eSTREAM Portfolio*, Project eSTREAM web page, 2008, `http://www.ecrypt.eu.org/stream/portfolio.pdf`.

[2] BIHAM, E.—BIRYUKOV, A.—DUNKELMAN, O.—RICHARDSON, E.—SHAMIR, A.: *Initial observations on skipjack: Cryptanalysis of Skipjack-3XOR*, in: Selected Areas in Cryptography—SAC '98, 5th Annual Internat. Workshop (S. Tavares et al., eds.), Kingston, Ontario, Canada, 1998, Lecture Notes in Comput. Sci., Vol. 1556, Springer, Berlin, 1999, pp. 362–375.

[3] CHO, J. Y.—PIERPRZYK, J.: *Crossword puzzle attack on NLS*, Sel. Areas in Cryptogr. 2006, 1–15, `research.ics.tkk.fi/publications/jcho/cpa-nls.pdf`.

[4] CHO, J. Y.—PIERPRZYK, J.: *Linear distinguishing attack on NLS*, Project eSTREAM web page, 2006, 1–10, `http://www.ecrypt.eu.org/stream/papersdir/2006/018.pdf`.

[5] CHO, J. Y.—PIERPRZYK, J.: *Multiple modular additions and crossword puzzle attack on NLSv2*, Project eSTREAM web page, 2006, 1–19, `http://www.ecrypt.eu.org/stream/papersdir/2006/051.pdf`.

[6] HAWKES, P.—PADDON, M.—ROSE, G. G.—DE VRIES, M. W.: *Primitive specification for NLSv2*, Project eSTREAM web page, 2007, 1–25, `http://www.ecrypt.eu.org/stream/p3ciphers/nls/nls_p3.pdf`.

Received August 29, 2012

Institute of Computer Science
and Mathematics
Faculty of Electrical Engineering
and Information Technology
Slovak University of Technology
Ilkovičova 3
SK–812-19 Bratislava
SLOVAKIA

E-mail: michal.brasko@gmail.com
xboorj@stuba.sk