Multiple Modular Additions and Crossword Puzzle Attack on NLSv2

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 a stream cipher which was submitted to eSTREAM project. A linear distinguishing attack against NLS was presented by Cho and Pieprzyk, which was called as Crossword Puzzle (CP) attack. NLSv2 is the tweak version of NLS which aims mainly at avoiding the CP attack. In this paper, a new distinguishing attack against NLSv2 is presented. The attack exploits high correlation amongst neighboring bits of the cipher. The paper first shows that the modular addition preserves pairwise correlations as demonstrated by existence of linear approximations with large biases. Next it shows how to combine these results with the existence of high correlation between bits 29 and 30 of the S-box to obtain a distinguisher whose bias is around 2^{-37}. Consequently, we claim that NLSv2 is distinguishable from a random process after observing around 2^{74} keystream words.
Keywords : Distinguishing Attacks, Crossword Puzzle Attack, Stream Ciphers, eSTREAM, NLS, NLSv2.

1 Introduction

NLS is one of stream ciphers submitted to the eSTREAM project [5]. The second phase of the eSTREAM included NLS in both profiles 1 (Software) and 2 (Hardware). During the first phase, a distinguishing attack against NLS was presented in [3]. The attack requires around 2^{60} keystream observations.

NLSv2 is a tweaked version of NLS to counter the distinguishing attack mentioned above. Unlike in the orignal NLS, NLSv2 periodically updates the value $Konst$ every 65537 clock. The new value of $Konst$ is taken from the output of the non-linear filter. In [4], the linear approximation from non-linear feedback shift register (NFSR) was derived and the sign of bias can be either positive or negative depending on the value of $Konst$. Thus, a randomly updated $Konst$ is expected to “neutralize” the overall bias of approximations, which eventually minimizes the bias of distinguisher.

In [3], the authors presented a distinguishing attack on NLS by Crossword Puzzle attack (or shortly CP attack) method. The CP attack is a variant of the linear distinguishing attack which was specifically designed to work for NFSR based stream ciphers. The attack concentrates on finding approximations and combining them in such a way that the internal states of NFSR cancel each other.

Being more specific, the authors showed that, for the attack on NLSv2, the effect of $Konst$ could be eliminated by using ’even’ number of NFSR approximations. A distinguisher was constructed by combining eight NFSR approximations and two NLF approximations, for which 2^{96} observations of keystream are required. However, due to the explicit upper limit of 2^{80} on the number of observed keystream imposed by the designers of the cipher, this attack does not break the cipher.

In this paper, we have improved the linear distinguishing attack on NLSv2 presented in the latter part of [3]. We still use the CP attack from [3] for our distinguisher. However, we have observed that there are linear approximations of S-boxes whose biases are much higher than those used in the previous attack.

Using those more effective approximations, we can now construct a distinguisher whose bias is around 2^{-37}. Therefore, we claim that NLSv2 is distinguishable from a truly random cipher after observing around 2^{74} keystream words which are within the limit of permitted observations during the session with a single key.

This paper is organized as follows. Section 2 presents some properties of multiple modular additions which are useful for our attack. Section 3 presents the structure of NLSv2. Section 4 presents the technique we use to construct linear approximations required in our attack. Section 5 contains the main part of the paper and presents the CP attack against NLSv2. Section 6 concludes the work.

Notation :

1. $\boxplus$ denotes the addition modulo 2^{32},
2. $x^{\lll k}$ represents the 32-bit x which is left-rotated by k-bit,
3. $x_{(i)}$ stands for i-th bit of the 32-bit string x,

These notations will be used throughout this paper.

2 Probabilistic properties of multiple modular additions

The attack explores a correlation between two neighboring bits. This Section describes the behavior of neighboring bits in modular additions and establishes the background for our further considerations. Suppose that $z = x \boxplus y$ where $x, y, z \in \{0,1\}^{32}$ are independently uniformly random. According to [2], there exist the following relations among $x_{(i)}$,$y_{(i)}$ and $z_{(i)}$:

$$z_{(0)} = x_{(0)} \oplus y_{(0)}, \quad z_{(i)} = x_{(i)} \oplus y_{(i)} \oplus x_{(i-1)}y_{(i-1)} \oplus \sum_{j=0}^{i-2} x_{(j)}y_{(j)} \prod_{k=j+1}^{(i-1)} (x_{(k)} \oplus y_{(k)}), \quad 1 \le i \le 31$$

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, given 32-bit x, $\Gamma_i \cdot x = x_{(i)} \oplus x_{(i+1)}$, where $\cdot$ denote the standard inner product.*

Definition 2. *The carry $R(x, y)$ generated in modular addition is defined as follows.*

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

It is clear that $R(x, y)_{(i)}$ can be determined using the following recursive relation:

$$R(x,y)_{(i)} = x_{(i)}y_{(i)} \oplus (x_{(i)} \oplus y_{(i)})R(x,y)_{(i-1)}$$

Now we are ready to present a collection of properties that are formulated in the lemmas given below. These results are essential for setting up our attack. In the following, we assume that all the variables are independently uniformly random.

Lemma 1. *Given* $x, y \in \{0,1\}^{32}$*, then the probability distribution of the carry bits can be expressed as follows*

$$Pr[R(x,y)_{(i)} = 0] = \frac{1}{2} + 2^{-i-2} \quad \textit{for } i = 0, \dots, 30.$$

Proof. The proof is given by induction.

(1) Let $i = 0$. Then the carry occurs only if $x_{(0)} = 1$ and $y_{(0)} = 1$ so $Pr[R(x,y)_{(0)} = x_{(0)}y_{(0)} = 0] = \frac{3}{4} = \frac{1}{2} + 2^{-2}$

(2) In the induction step we assume that $Pr[R(x,y)_{(i-1)} = 0] = \frac{1}{2} + 2^{-i-1}$. Then, from the recursive relation, we have

$$Pr[R(x,y)_{(i)} = 0] = \begin{cases} Pr[x_{(i)}y_{(i)} = 0] = \frac{3}{4}, & \text{if } R(x,y)_{i-1} = 0 \\ Pr[x_{(i)}y_{(i)} \oplus (x_{(i)} \oplus y_{(i)}) = 0] = \frac{1}{4}, & \text{if } R(x,y)_{(i-1)} = 1 \end{cases}$$

Hence, the following equation holds

$$Pr[R(x,y)_{(i)} = 0] = \frac{3}{4} \cdot (\frac{1}{2} + 2^{-i-1}) + \frac{1}{4} \cdot (\frac{1}{2} - 2^{-i-1}) = \frac{1}{2} + 2^{-i-2}.$$

This proves our lemma. □

Corollary 1. *Given* $x, y \in \{0,1\}^{32}$*, the following approximation holds with the constant probability as*

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

Proof. By definition, we obtain

$$\Gamma_{i-1} \cdot R(x,y) = R(x,y)_{(i-1)} \oplus R(x,y)_{(i)} = x_{(i)}y_{(i)} \oplus (x_{(i)} \oplus y_{(i)} \oplus 1)R(x,y)_{(i-1)}$$

Hence, from Lemma 1, we get

$$Pr[\Gamma_{i-1} \cdot R(x,y) = 0] = \frac{3}{4} \cdot (\frac{1}{2} + 2^{-i-1}) + \frac{3}{4} \cdot (\frac{1}{2} - 2^{-i-1}) = \frac{3}{4}$$

and the corollary holds. □

Due to Corollary 1, the following approximation has the probability of $\frac{3}{4}$, as stated in [3].

$$\Gamma_i \cdot (x \boxplus y) = \Gamma_i \cdot (x \oplus y), \quad i = 0, \dots, 30$$

Lemma 2. *Suppose that* $x, y, z \in \{0,1\}^{32}$*. Then, the following linear approximation*

$$\Gamma_i \cdot (x \boxplus y \boxplus z) = \Gamma_i \cdot (x \oplus y \oplus z)$$

holds with the probability of $\frac{2}{3} - \frac{1}{3}2^{-2i-1}$ *for* $i = 0, \dots, 30$.

Proof. See Appendix B.

Lemma 3. *Suppose that* $x_1, x_2, \dots, x_n, k \in \{0,1\}^{32}$ *where* n *is an even number. Then, the following linear approximation*

$$\Gamma_i \cdot (x_1 \boxplus k) \oplus \Gamma_i \cdot (x_2 \boxplus k) \oplus \cdots \oplus \Gamma_i \cdot (x_n \boxplus k) = \Gamma_i \cdot (x_1 \oplus x_2 \oplus \cdots \oplus x_n)$$

holds with the probability of around $\frac{n+2}{2(n+1)}$ *for* $i = 1, \dots, 30$.

Proof. See Appendix E.

Corollary 2. *Given* $x, y, z \in \{0,1\}^{32}$*, the following linear approximation*

$$\Gamma_i \cdot (x \boxplus y) \oplus \Gamma_i \cdot (x \boxplus z) = \Gamma_i \cdot (y \oplus z)$$

holds with the probability of $\frac{2}{3} + \frac{1}{3}2^{-2i-2}$ *for* $i = 0, \ldots, 30$*.*

Proof. See Appendix F.

Lemma 4. *Given* $x, y, z, w \in \{0,1\}^{32}$*, the following linear approximation*

$$\Gamma_i \cdot (x \boxplus y) \oplus \Gamma_i \cdot (z \boxplus w) = \Gamma_i \cdot (x \boxplus z) \oplus \Gamma_i \cdot (y \boxplus w)$$

has the probability of $\frac{2}{3} + \frac{1}{3}2^{-2i-2}$ *for* $i = 0, \ldots, 30$*.*

Proof. See Appendix C.

Corollary 3. *Let* $x, y, z, w \in \{0,1\}^{32}$*, then the following linear approximation*

$$\Gamma_i \cdot (x \boxplus y) \oplus \Gamma_i \cdot (x \boxplus z) \oplus \Gamma_i \cdot (y \boxplus w) = \Gamma_i \cdot (z \oplus w)$$

holds with the probability of $\frac{29}{48} + \frac{1}{3}2^{-2i-4}$ *for* $i = 0, \ldots, 30$*.*

Proof. See Appendix D.

For convenience, in the rest of the paper we are going to use bias of approximation rather than probability that an approximation holds.

3 Brief description of NLSv2

NLS is a synchronous, word-oriented stream cipher controlled by a secret key of the size up to 128 bits. The keystream generator of NLS is composed of a non-linear feedback shift register (NFSR) and a non-linear filter (NLF) with a counter. In this section, we describe only the part of NLS which is necessary to understand our attack. The structure of NLSv2 is exactly the same as that of NLS except a periodically updated $Konst$ [5]. For more details, refer to [5] and [6].

3.1 Non-linear Feedback Shift Register (NFSR)

At time t, the state of NFSR is denoted by $\sigma_t = (r_t[0], \ldots, r_t[16])$ where $r_t[i]$ is a 32-bit word. $Konst$ is a key-dependent 32-bit word, which is set at the initialization stage and is updated periodically. 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 $t \equiv 0$ (modulo f16), then
  (a) $r_{t+1}[2]$ is modified by adding t (modulo 2^{32}),
  (b) $Konst$ is changed to the output of NLF,
  (c) the output of NLF at $t = 0$ is not used as a keystream word,
  where $f16$ is a constant integer $2^{16} + 1 = 65537$.

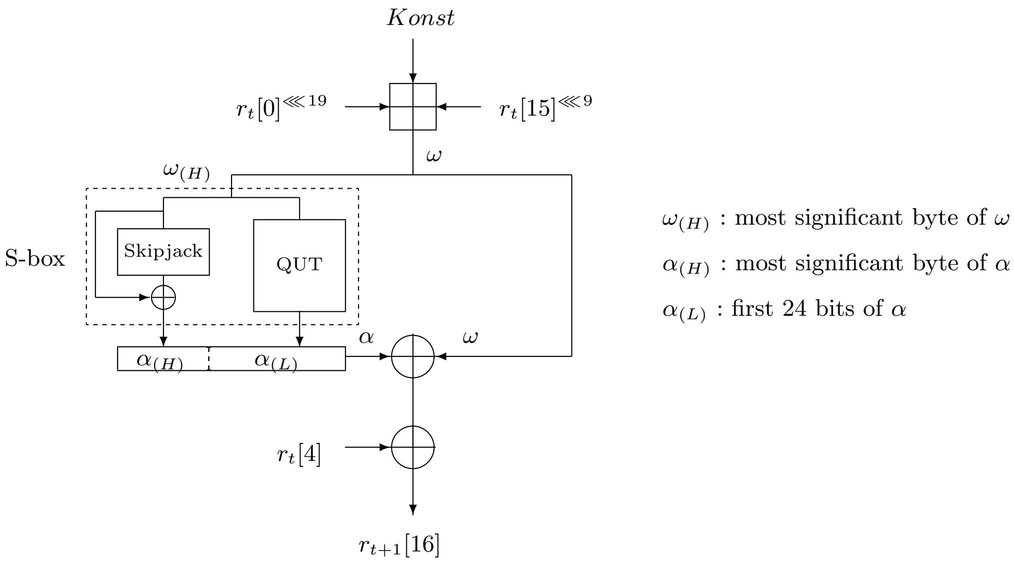

Fig. 1. The update function of NFSR

The f function The function f is 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. The main S-box is composed of two independent smaller S-boxes: the Skipjack S-box (with 8-bit input and 8-bit output) [8] and a custom-designed QUT S-box (with 8-bit input and 24-bit output). The output of main S-box in NLSv2 is defined as a concatenation of outputs of the two smaller S-boxes. Note that the input of Skipjack S-box (that is $\omega_{(H)}$) is added to the output of Skipjack S-box in advance for fast implementation. Since the output of the main S-box is added to ω again, the original output of Skipjack S-box is restored. See Figure 1 for details.

3.2 Non-linear Filter (NLF)

Each output keystream word ν_t of NLF is generated by the following equation.

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

Note that there is no output word when $t = 0$ modulo $f16$.

4 Building linear approximations

In this section, linear approximations of NLF and NFSR are developed for the CP attack against NLS and NLSv2. The main effort is to derive new approximations of NFSR which have a higher bias than those presented in [3]. Note that we adapt the following definition of the bias for analysis.

Definition 3. *A bias ϵ is defined as follows.*

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

[1] ϵ is also known in the literature as the correlation or the imbalance.

where P is the probability that an approximation holds.

The advantage of the definition is that the bias of the combination of n independent approximations each of bias ϵ is equal to ϵ^n as asserted by the Piling-up lemma. [7]

4.1 Linear approximations of NFSR

We investigate the bias of the approximation of linear combination of two neighboring bits of $\alpha = \text{S-box}(\omega_{(H)})$. As $\omega_{(H)}$ is an 8-bit input, the bias ϵ_i can be calculated as follows

$$\epsilon_i = \frac{\#(\Gamma_i \cdot \alpha = 0) - \#(\Gamma_i \cdot \alpha = 1)}{256}, \quad i = 0, \ldots, 30.$$

Table 1 shows the results obtained by exhaustive search.

$i, i+1$	ϵ_i	$i, i+1$	ϵ_i	$i, i+1$	ϵ_i	$i, i+1$	ϵ_i
$0, 1$	0	$8, 9$	$-2^{-3.678}$	$16, 17$	0	$24, 25$	-2^{-6}
$1, 2$	2^{-5}	$9, 10$	-2^{-5}	$17, 18$	$2^{-4.415}$	$25, 26$	-2^{-4}
$2, 3$	2^{-4}	$10, 11$	$2^{-3.678}$	$18, 19$	-2^{-6}	$26, 27$	-2^{-6}
$3, 4$	0	$11, 12$	0	$19, 20$	-2^{-5}	$27, 28$	2^{-5}
$4, 5$	-2^{-4}	$12, 13$	2^{-5}	$20, 21$	$-2^{-4.415}$	$28, 29$	-2^{-5}
$5, 6$	$-2^{-3.678}$	$13, 14$	2^{-6}	$21, 22$	$-2^{-4.415}$	$\mathbf{29, 30}$	$\mathbf{-2^{-2.3}}$
$6, 7$	0	$14, 15$	-2^{-6}	$22, 23$	$2^{-4.415}$	$30, 31$	0
$7, 8$	-2^{-6}	$15, 16$	$-2^{-3.678}$	$23, 24$	-2^{-6}		

Table 1. Bias of linear approximations of two adjacent output bits of S-box

According to Table 1, the linear approximation $\alpha_{29} \oplus \alpha_{30} = 1$ has the largest bias of $2^{-2.3}$. We notice that these two bits are involved in Skipjack S-box and this weakness has already been observed by Biham *et al.* in 1998. [1]

Since $f(\omega) = \text{S-box}(\omega_{(H)}) \oplus \omega$, it is clear that the following output approximation has the bias of $2^{-2.3}$.

$$\Gamma_{29} \cdot (\omega \oplus f(\omega)) = 1 \tag{2}$$

Having Approximation (2), we derive the best approximation of the NLF function. From the structure of NLF, the following relation is always true.

$$\Gamma_{29} \cdot (f(\omega)_t \oplus r_t[4] \oplus r_{t+1}[16]) = 0$$

By combining the above relation with Approximation (2), we obtain the approximation

$$\Gamma_{29} \cdot (\omega_t \oplus r_t[4] \oplus r_{t+1}[16]) = 1 \tag{3}$$

that has the bias of $2^{-2.3}$.

4.2 Linear approximations of NLF

The best linear approximation of NLF for our attack is similar to the one which was given in [3] except that we use the bit position 29 and 30 instead of $12, 13, 22$ and 23. However, we provide a proof of the bias of the approximation which was not given in [3].

Lemma 5. *Given two consecutive outputs of NLF which are ν_t and ν_{t+1}, the following approximation.*

$$\Gamma_i \cdot (\nu_t \oplus \nu_{t+1}) = \Gamma_i \cdot (r_t[0] \oplus r_t[2] \oplus r_t[6] \oplus r_t[7] \oplus r_t[13] \oplus r_t[14] \oplus r_t[16] \oplus r_{t+1}[16])$$

has the bias of $\frac{1}{36}(1 + 2^{-2i-1})^2$.

Proof. From the non-linear filter function (1), we know that

$$\begin{aligned}\nu_t \oplus \nu_{t+1} = &(r_t[0] \boxplus r_t[16]) \oplus (\mathbf{r_t[1]} \boxplus r_t[13]) \oplus (r_t[6] \boxplus \mathbf{Konst}) \\ &\oplus (\mathbf{r_{t+1}[0]} \boxplus r_{t+1}[16]) \oplus (r_{t+1}[1] \boxplus r_{t+1}[13]) \oplus (r_{t+1}[6] \boxplus \mathbf{Konst})\end{aligned}$$

for two consecutive clocks $(t, t+1)$. Note that $r_t[1]$ and $Konst$ are used twice in above expression. Hence, according to Corollary 2, the following two approximations have the probability of $\frac{1}{2}(1 + \frac{1}{3} + \frac{1}{3}2^{-2i-1})$ each.

$$\Gamma_i \cdot (r_t[6] \boxplus \mathbf{Konst}) \oplus \Gamma_i \cdot (r_{t+1}[6] \boxplus \mathbf{Konst}) = \Gamma_i \cdot (r_t[6] \oplus r_{t+1}[6])$$
$$\Gamma_i \cdot (\mathbf{r_t[1]} \boxplus r_t[13]) \oplus \Gamma_i \cdot (\mathbf{r_{t+1}[0]} \boxplus r_{t+1}[16]) = \Gamma_i \cdot (r_t[13] \oplus r_{t+1}[16])$$

In addition, due to Corollary 1, the approximation given below has the probability of $\frac{1}{2}(1 + 2^{-1})$, respectively.

$$\Gamma_i \cdot (r_t[0] \boxplus r_t[16]) = \Gamma_i \cdot (r_t[0] \oplus r_t[16])$$
$$\Gamma_i \cdot (r_{t+1}[1] \boxplus r_{t+1}[13]) = \Gamma_i \cdot (r_{t+1}[1] \oplus r_{t+1}[13])$$

Hence, the overall bias is $(\frac{1}{3} + \frac{1}{3}2^{-2i-1})^2 \times 2^{-2} = \frac{1}{36}(1 + 2^{-2i-1})^2$. □

Therefore, the best linear approximation of NLF for our attack is

$$\Gamma_{29} \cdot (\nu_t \oplus \nu_{t+1}) = \Gamma_{29} \cdot (r_t[0] \oplus r_t[2] \oplus r_t[6] \oplus r_t[7] \oplus r_t[13] \oplus r_t[14] \oplus r_t[16] \oplus r_{t+1}[16] \quad (4)$$

that has the bias of $\frac{1}{36}(1 + 2^{-2\times 29-1})^2 \approx 2^{-5.2}$.

4.3 Linear property of NFSR

Due to the update rule of NFSR, $r_{t+i}[j] = r_{t+j}[i]$ where $i, j > 0$.

5 Crossword Puzzle (CP) Attack on NLSv2

In NLSv2, the $Konst$ is updated by taking the output of NLF at every 65537 clock. In [3], authors showed that $Konst$ terms could be removed from the distinguisher by combining two consecutive approximations of NLF. In this section, the similar technique is adapted for our attack. That is, the distinguisher are derived by combining the approximations of NFSR and NLF appropriately in such a way that the internal states of the shift register are canceled out.

However, we develop more efficient attack on NLSv2 using Approximation (3) and (4) at clock positions η which are

$$\eta = \{0, 2, 6, 7, 13, 14, 16, 17\}$$

Note that Approximation (3) consists of non-linear terms and linear terms: $\Gamma_{29} \cdot \omega_t$ and $\Gamma_{29} \cdot (r_t[4] \oplus r_{t+1}[16])$, respectively. In the following section, we develop the bias of two approximations X_t and Y_t separately which are defined as

$$X_t = \bigoplus_{k \in \eta} \Gamma_{29} \cdot (r_{t+k}[4] \oplus r_{t+k+1}[16]), \quad Y_t = \bigoplus_{k \in \eta} \Gamma_{29} \cdot \omega_{t+k}.$$

5.1 Bias of X_t

Due to Approximation (4) and the linear property of NFSR, we know that

$$X_t = \bigoplus_{k\in\eta} \varGamma_{29} \cdot (r_{t+k}[4] \oplus r_{t+k+1}[16]) = \bigoplus_{k\in\eta} \varGamma_{29} \cdot (r_{t+4}[k] \oplus r_{t+17}[k])$$
$$= \varGamma_{29} \cdot (\nu_{t+4} \oplus \nu_{t+5} \oplus \nu_{t+17} \oplus \nu_{t+18}) \quad (5)$$

The bias of (5) is $2^{-8.6}$. The calculations of the bias are given below. The definition of ν_t from Equation (1) gives the following equation

$$\begin{aligned}
&\varGamma_{29} \cdot (\nu_{t+4} \oplus \nu_{t+5} \oplus \nu_{t+17} \oplus \nu_{t+18})\\
&= \varGamma_{29} \cdot (r_{t+4}[0] \boxplus r_{t+4}[16]) \oplus \varGamma_{29} \cdot (\mathbf{r_{t+4}[1]} \boxplus \mathbf{r_{t+4}[13]}) \oplus \varGamma_{29} \cdot (r_{t+4}[6] \boxplus \mathbf{Konst})\\
&\oplus \varGamma_{29} \cdot (\mathbf{r_{t+5}[0]} \boxplus r_{t+5}[16]) \oplus \varGamma_{29} \cdot (r_{t+5}[1] \boxplus \mathbf{r_{t+5}[13]}) \oplus \varGamma_{29} \cdot (r_{t+5}[6] \boxplus \mathbf{Konst})\\
&\oplus \varGamma_{29} \cdot (\mathbf{r_{t+17}[0]} \boxplus r_{t+17}[16]) \oplus \varGamma_{29} \cdot (\mathbf{r_{t+17}[1]} \boxplus r_{t+17}[13]) \oplus \varGamma_{29} \cdot (r_{t+17}[6] \boxplus \mathbf{Konst})\\
&\oplus \varGamma_{29} \cdot (\mathbf{r_{t+18}[0]} \boxplus r_{t+18}[16]) \oplus \varGamma_{29} \cdot (r_{t+18}[1] \boxplus r_{t+18}[13]) \oplus \varGamma_{29} \cdot (r_{t+18}[6] \boxplus \mathbf{Konst})
\end{aligned}$$

We can see that several terms are shared due to the linear property of NFSR. Hence, the approximations are applied separately into four groups as follows.

1. According to Corollary 3, we get

$$\begin{aligned}
&\varGamma_{29} \cdot (\mathbf{r_{t+4}[1]} \boxplus \mathbf{r_{t+4}[13]}) \oplus \varGamma_{29} \cdot (\mathbf{r_{t+17}[0]} \boxplus r_{t+17}[16]) \oplus \varGamma_{29} \cdot (\mathbf{r_{t+5}[0]} \boxplus r_{t+5}[16])\\
&= \varGamma_{29} \cdot r_{t+17}[16] \oplus \varGamma_{29} \cdot r_{t+5}[16]
\end{aligned}$$

   that has the probability of $\frac{29}{48} + \frac{1}{3}2^{-2\times 29-4} \approx \frac{1}{2}(1 + 2^{-2.3})$.
2. Due to Lemma 3, the approximation

$$\begin{aligned}
&\varGamma_{29} \cdot (r_{t+5}[1] \boxplus \mathbf{r_{t+5}[13]}) \oplus \varGamma_{29} \cdot (\mathbf{r_{t+18}[0]} \boxplus r_{t+18}[16]) \oplus \varGamma_{29} \cdot (\mathbf{r_{t+17}[1]} \boxplus r_{t+17}[13])\\
&= \varGamma_{29} \cdot (r_{t+5}[1] \oplus r_{t+5}[13] \oplus r_{t+18}[16] \oplus r_{t+17}[13])
\end{aligned}$$

   has the probability of around $\frac{5}{8} = \frac{1}{2}(1 + 2^{-2})$.
3. Lemma 3 also asserts that the approximation

$$\begin{aligned}
&\varGamma_{29} \cdot (r_{t+4}[6] \boxplus \mathbf{Konst}) \oplus \varGamma_{29} \cdot (r_{t+5}[6] \boxplus \mathbf{Konst}) \oplus \varGamma_{29} \cdot (r_{t+17}[6] \boxplus \mathbf{Konst})\\
&\oplus \varGamma_{29} \cdot (r_{t+18}[6] \boxplus \mathbf{Konst}) = \varGamma_{29} \cdot (r_{t+4}[6] \oplus r_{t+5}[6] \oplus r_{t+17}[6] \oplus r_{t+18}[6])
\end{aligned}$$

   has the probability of around $\frac{3}{5} = \frac{1}{2}(1 + 2^{-2.3})$.
4. Corollary 1 says that the approximation

$$\begin{aligned}
&\varGamma_{29} \cdot (r_{t+4}[0] \boxplus r_{t+4}[16]) \oplus \varGamma_{29} \cdot (r_{t+18}[1] \boxplus r_{t+18}[13])\\
&= \varGamma_{29} \cdot (r_{t+4}[0] \oplus r_{t+4}[16]) \oplus \varGamma_{29} \cdot (r_{t+18}[1] \oplus r_{t+18}[13])
\end{aligned}$$

   has the probability of $\frac{1}{2}(1 + 2^{-2})$.

Therefore, the bias of Approximation (5) is $2^{-2.3} \times 2^{-2} \times 2^{-2.3} \times 2^{-2} = 2^{-8.6}$.

5.2 Bias of Y_t

Recall that

$$\omega_t = (r_t[0]^{\lll 19}) \boxplus (r_t[15]^{\lll 9}) \boxplus Konst$$

Due to Lemma 2, ω_t has the following approximation.

$$\begin{aligned} \Gamma_{29} \cdot \omega &= \Gamma_{29} \cdot (r_t[0]^{\lll 19} \oplus r_t[15]^{\lll 9} \oplus Konst) \\ &= \Gamma_{10} \cdot r_t[0] \oplus \Gamma_{20} \cdot r_t[15] \oplus \Gamma_{29} \cdot Konst \end{aligned}$$

that has the probability of $\frac{2}{3} - \frac{1}{3}2^{-2\times 29-1} \approx \frac{1}{2}(1 + 2^{-1.6})$. Due to Lemma 5, Y_t can be approximated as

$$\begin{aligned} Y_t &= \bigoplus_{k\in\eta} \Gamma_{29} \cdot \omega_{t+k} = \bigoplus_{k\in\eta} (\Gamma_{10} \cdot r_{t+k}[0] \oplus \Gamma_{20} \cdot r_{t+k}[15] \oplus \Gamma_{29} \cdot Konst) \\ &= \Gamma_{10} \cdot (\nu_t \oplus \nu_{t+1}) \oplus \Gamma_{20} \cdot (\nu_{t+15} \oplus \nu_{t+16}) \end{aligned} \quad (6)$$

The bias of (6) is at least $2^{-10.4}$. The detail analysis on the bias will be discussed in Section 5.4.

Notice that $Konst$ terms have disappeared since the binary addition of eight approximations cancels $Konst$ as presented in [3]. Due to the lack of a keystream word at every f16-th clock, we can see precisely when $Konst$ is updated. Since the updated $Konst$ has been effective to all states of registers after the first 17 clocks, the observations generated from the first 17 clocks should not be counted for the bias. Hence, $Konst$ is regarded as a constant in all approximations [2].

5.3 Bias of the distinguisher

The bias of distinguisher for NLSv2 is derived as follows. From (3), the following approximation has the bias of $2^{-2.3\times 8}$ by the Piling-up Lemma [7].

$$\bigoplus_{k\in\eta} \Gamma_{29} \cdot (\omega_{t+k} \oplus r_{t+k}[4] \oplus r_{t+1+k}[16]) = X_t \oplus Y_t = 0 \quad (7)$$

On the contrary, by adding up the approximations of (5) and (6), we obtain the following approximation

$$X_t \oplus Y_t = \Gamma_{29} \cdot (\nu_{t+4} \oplus \nu_{t+5} \oplus \nu_{t+17} \oplus \nu_{t+18}) \oplus \Gamma_{10} \cdot (\nu_t \oplus \nu_{t+1}) \oplus \Gamma_{20} \cdot (\nu_{t+15} \oplus \nu_{t+16}) \quad (8)$$

that has the bias equal to $2^{-8.6} \times 2^{-10.4}$. Therefore, by combining (7) and (8), the distinguisher on NLSv2 is described by the approximation

$$\Gamma_{29} \cdot (\nu_{t+4} \oplus \nu_{t+5} \oplus \nu_{t+17} \oplus \nu_{t+18}) \oplus \Gamma_{10} \cdot (\nu_t \oplus \nu_{t+1}) \oplus \Gamma_{20} \cdot (\nu_{t+15} \oplus \nu_{t+16}) = 0 \quad (9)$$

that has the bias of around $2^{-2.3\times 8} \times 2^{-8.6} \times 2^{-10.4} = 2^{-37.4}$.

---

[2] By this reason, the notation $Konst_t$ is not used in the approximations.

5.4 The bias of Approximation (6)

According to the definition of ν_t given by (1), we can write the following approximation

$$\begin{aligned}
&\Gamma_{10} \cdot (\nu_t \oplus \nu_{t+1}) \oplus \Gamma_{20} \cdot (\nu_{t+15} \oplus \nu_{t+16}) \\
&= \Gamma_{10} \cdot (r_t[0] \boxplus r_t[16]) \oplus \Gamma_{10} \cdot (r_t[1] \boxplus r_t[13]) \Gamma_{10} \cdot (r_t[6] \boxplus Konst) \\
&\oplus \Gamma_{10} \cdot (r_{t+1}[0] \boxplus r_{t+1}[16]) \oplus \Gamma_{10} \cdot (r_{t+1}[1] \boxplus r_{t+1}[13]) \oplus \Gamma_{10} \cdot (r_{t+1}[6] \boxplus Konst) \\
&\oplus \Gamma_{20} \cdot (r_{t+15}[0] \boxplus r_{t+15}[16]) \oplus \Gamma_{20} \cdot (r_{t+15}[1] \boxplus r_{t+15}[13]) \oplus \Gamma_{20} \cdot (r_{t+15}[6] \boxplus Konst) \\
&\oplus \Gamma_{20} \cdot (r_{t+16}[0] \boxplus r_{t+16}[16]) \oplus \Gamma_{20} \cdot (r_{t+16}[1] \boxplus r_{t+16}[13]) \oplus \Gamma_{20} \cdot (r_{t+16}[6] \boxplus Konst) \\
&\triangleq \Delta_1 \oplus \Delta_2 \oplus \Delta_3
\end{aligned}$$

where

$$\begin{aligned}
\Delta_1 &= \Gamma_{10} \cdot (r_t[0] \boxplus r_t[16]) \oplus \Gamma_{20} \cdot (r_{t+15}[0] \boxplus r_{t+15}[16]) \\
&\quad \oplus \Gamma_{10} \cdot (r_{t+1}[1] \boxplus r_{t+1}[13]) \oplus \Gamma_{20} \cdot (r_{t+16}[1] \boxplus r_{t+16}[13]) \\
\Delta_2 &= \Gamma_{10} \cdot (r_t[1] \boxplus r_t[13]) \oplus \Gamma_{20} \cdot (r_{t+15}[1] \boxplus r_{t+15}[13]) \\
&\quad \oplus \Gamma_{10} \cdot (r_{t+1}[0] \boxplus r_{t+1}[16]) \oplus \Gamma_{20} \cdot (r_{t+16}[0] \boxplus r_{t+16}[16]) \\
\Delta_3 &= \Gamma_{10} \cdot (r_t[6] \boxplus Konst) \oplus \Gamma_{20} \cdot (r_{t+15}[6] \boxplus Konst) \\
&\quad \oplus \Gamma_{10} \cdot (r_{t+1}[6] \boxplus Konst) \oplus \Gamma_{20} \cdot (r_{t+16}[6] \boxplus Konst)
\end{aligned}$$

In order to determine the bias of Δ_1, Δ_2 and Δ_3, the following two lemmas are required.

Lemma 6. *Given $x, y, a, b, c, d, k \in \{0,1\}^{32}$, the following approximation has the bias of $2^{-3.1}$ when $i > 0$.*

$$\begin{aligned}
&\Gamma_i \cdot (x \boxplus a) \oplus \Gamma_i \cdot (y \boxplus b) \oplus \Gamma_i \cdot (x \boxplus c) \oplus \Gamma_i \cdot (y \boxplus d) \\
&= \Gamma_i \cdot (a \boxplus b \boxplus k) \oplus \Gamma_i \cdot (c \boxplus d \boxplus k)
\end{aligned}$$

Proof. (*Sketch*) *We assume that $x = 0$ and $y = 0$ since the variables x and y are independent on the expressions $(a \boxplus b \boxplus k)$ and $(c \boxplus d \boxplus k)$. Then, the approximation being considered is simplified as follows.*

$$\begin{aligned}
&\Gamma_i \cdot (x \boxplus a) \oplus \Gamma_i \cdot (y \boxplus b) \oplus \Gamma_i \cdot (x \boxplus c) \oplus \Gamma_i \cdot (y \boxplus d) \oplus \Gamma_i \cdot (a \boxplus b \boxplus k) \oplus \Gamma_i \cdot (c \boxplus d \boxplus k) \\
&= \Gamma_{i-1} \cdot (R(a,b) \oplus R(a \boxplus b, k)) \oplus \Gamma_{i-1} \cdot (R(c,d) \oplus R(c \boxplus d, k))
\end{aligned}$$

By using the recursive relation (11) in Appendix B and by counting appropriate probabilities, we get

$$Pr[(R(a,b) \oplus R(a \boxplus b, k))_{(i)} \oplus (R(c,d) \oplus R(c \boxplus d, k))_{(i)} = 0] \approx \frac{33}{59} = \frac{1}{2}(1 + 2^{-3.1})$$

Since $Pr[(R(a,b) \oplus R(a \boxplus b, k))_{(i)} \oplus (R(c,d) \oplus R(c \boxplus d, k))_{(i)} = 0]$ is identical to $Pr[\Gamma_{i-1} \cdot (R(a,b) \oplus R(a \boxplus b, k)) \oplus \Gamma_{i-1} \cdot (R(c,d) \oplus R(c \boxplus d, k)) = 0]$, the lemma holds. See Appendix G for details.

Lemma 7. *Given $x, y, z, w, a, b, c, d, k \in \{0,1\}^{32}$, the following approximation has the bias of $2^{-4.2}$ when $i > 0$.*

$$\begin{aligned}
&\Gamma_i \cdot (x \boxplus a) \oplus \Gamma_i \cdot (y \boxplus b) \oplus \Gamma_i \cdot (z \boxplus c) \oplus \Gamma_i \cdot (w \boxplus d) \\
&= \Gamma_i \cdot (x \boxplus y \boxplus k) \oplus \Gamma_i \cdot (a \boxplus b \boxplus k) \oplus \Gamma_i \cdot (z \boxplus w \boxplus k) \oplus \Gamma_i \cdot (c \boxplus d \boxplus k) \qquad (10)
\end{aligned}$$

Proof. *(Sketch) Suppose $k = 0$. Then, the approximation (10) is divided into two independent approximations as follows.*

$$\Gamma_i \cdot (x \boxplus a) \oplus \Gamma_i \cdot (y \boxplus b) = \Gamma_i \cdot (x \boxplus y) \oplus \Gamma_i \cdot (a \boxplus b)$$
$$\Gamma_i \cdot (z \boxplus c) \oplus \Gamma_i \cdot (w \boxplus d) = \Gamma_i \cdot (z \boxplus w) \oplus \Gamma_i \cdot (c \boxplus d)$$

By applying Lemma 4 twice, we see that above approximation has the bias of $\frac{1}{9}(1+2^{-2i-2})^2 \approx 2^{-3.2}$ for $i > 0$.
For $k = 1, 2, \ldots, 2^i$, the bias of (10) has the following properties.

- *the bias decreases monotonously for $k = 1, 2, \ldots, 2^{i-1}$.*
- *the bias increases monotonously for $k = 2^{i-1} + 1, \ldots, 2^i$.*
- *the bias is the highest at $k = 2^i$ and is the lowest (around zero) at $k = 2^{i-1}$.*

This bias pattern is repeated for $k = 2^i + 1, \ldots, 2^{i+2} - 1$. If $i > 0$, the overall bias of (10) is around a half of the highest bias, which is $2^{-3.2} * 2^{-1} = 2^{-4.2}$. Hence, the lemma holds.

$\mathbf{\Delta_1}$: From the definition of the rotations, we know that

$$\begin{aligned}\Delta_1 = &\Gamma_{29} \cdot (r_t[0]^{\lll 19} \boxplus r_t[16]^{\lll 19}) \oplus \Gamma_{29} \cdot (r_{t+15}[0]^{\lll 9} \boxplus r_{t+15}[16]^{\lll 9}) \\ &\oplus \Gamma_{29} \cdot (r_{t+1}[1]^{\lll 19} \boxplus r_{t+1}[13]^{\lll 19}) \oplus \Gamma_{29} \cdot (r_{t+16}[1]^{\lll 9} \boxplus r_{t+16}[13]^{\lll 9})\end{aligned}$$

According to Lemma 7, the following approximation has a bias of $2^{-4.2}$.

$$\begin{aligned}\Delta_1 &= \Gamma_{29} \cdot (r_t[0]^{\lll 19} \boxplus r_{t+15}[0]^{\lll 9} \boxplus Konst) \oplus \Gamma_{29} \cdot (r_t[16]^{\lll 19} \boxplus r_{t+15}[16]^{\lll 9} \boxplus Konst) \\ &\quad \oplus \Gamma_{29} \cdot (r_{t+1}[1]^{\lll 19} \boxplus r_{t+16}[1]^{\lll 9} \boxplus Konst) \oplus \Gamma_{29} \cdot (r_{t+1}[13]^{\lll 19} \boxplus r_{t+16}[13]^{\lll 9} \boxplus Konst) \\ &= \Gamma_{29} \cdot (\omega_t \oplus \omega_{t+16} \oplus \omega_{t+2} \oplus \omega_{t+14})\end{aligned}$$

$\mathbf{\Delta_2}$ and $\mathbf{\Delta_3}$: Due to Lemma 6, we can write the approximations

$$\begin{aligned}\Delta_2 &= \Gamma_{29} \cdot (r_t[1]^{\lll 19} \boxplus r_{t+15}[1]^{\lll 9}) \oplus \Gamma_{29} \cdot (r_t[13]^{\lll 19} \boxplus r_{t+15}[13]^{\lll 9}) \\ &\quad \oplus \Gamma_{29} \cdot (r_{t+1}[0]^{\lll 19} \boxplus r_{t+16}[0]^{\lll 9}) \oplus \Gamma_{29} \cdot (r_{t+1}[16]^{\lll 19} \boxplus r_{t+16}[16]^{\lll 9}) \\ &= \Gamma_{29} \cdot (r_t[13]^{\lll 19} \boxplus r_{t+15}[13]^{\lll 9} \boxplus Konst) \oplus \Gamma_{29} \cdot (r_{t+1}[16]^{\lll 19} \boxplus r_{t+16}[16]^{\lll 9} \boxplus Konst) \\ &= \Gamma_{29} \cdot (\omega_{t+13} \oplus \omega_{t+17}) \\ \Delta_3 &= \Gamma_{29} \cdot (r_t[6]^{\lll 19} \boxplus r_{t+15}[6]^{\lll 9}) \oplus \Gamma_{29} \cdot (Konst^{\lll 19} \boxplus Konst^{\lll 9}) \\ &\quad \oplus \Gamma_{29} \cdot (r_{t+1}[6]^{\lll 19} \boxplus r_{t+16}[6]^{\lll 9}) \oplus \Gamma_{29} \cdot (Konst^{\lll 19} \boxplus Konst^{\lll 9}) \\ &= \Gamma_{29} \cdot (r_t[6]^{\lll 19} \boxplus r_{t+15}[6]^{\lll 9} \boxplus Konst) \oplus \Gamma_{29} \cdot (r_{t+1}[6]^{\lll 19} \boxplus r_{t+16}[6]^{\lll 9} \boxplus Konst) \\ &= \Gamma_{29} \cdot (\omega_{t+6} \oplus \omega_{t+7})\end{aligned}$$

with the same bias of $2^{-3.1}$. Thus, Approximation (6) has the bias of $2^{-(4.2+3.1\times 2)} = 2^{-10.4}$.

5.5 Experiments

The verification of the bias of Distinguisher (9) is not directly applicable due to the requirement of large observations of keystream. Instead, our experiments have been focused on verifying the biases of Approximation (5) and (6) independently. Figure 2 shows that the graphs follow the expected biases of those approximations.

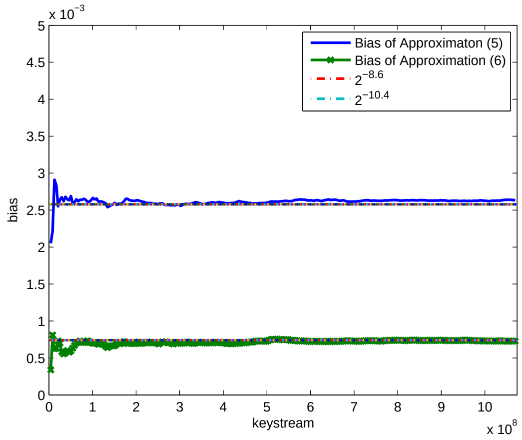

Fig. 2. The biases of Approximation (5) and (6)

6 Conclusion

In this paper, we present a Crossword Puzzle (CP) attack against NLSv2 that is a tweaked version of NLS. Even though the designers of NLSv2 aimed to avoid the distinguishing attack that was constructed for the NLS, we have shown that the CP attack can be applied for NLSv2. The distinguisher has a bias higher than 2^{-40} and consequently, the attack requires less than 2^{80} observations which was given as the security benchmark by the designers.

Acknowledgment We are grateful to anonymous referees of FSE 2007 for their comments. The authors were supported by ARC grants DP0451484 and DP0663452.

References

1. E. Biham, A. Biryukov, O. Dunkelman, and E. Richardson. Initial observations on Skipjack: Cryptanalysis of Skipjack-3XOR. In *Selected Areas in Cryptography - SAC'98*, volume 1556 of *Lecture Notes in Computer Science*, pages 362–376, February 1999.
2. J. Y. Cho and J. Pieprzyk. Algebraic attacks on SOBER-t32 and SOBER-t16 without stuttering. In *Fast Software Encryption - FSE 2004*, volume 3017 of *Lecture Notes in Computer Science*, pages 49 – 64. Springer-Verlag, July 2004.
3. J. Y. Cho and J. Pieprzyk. Crossword puzzle attack on NLS. In *Proceedings of Selected Areas in Cryptography - SAC 2006*, Montreal, Quebec, Canada, August 2006.
4. J. Y. Cho and J. Pieprzyk. Linear distinguishing attack on NLS. SASC 2006 workshop, 2006. Available at http://www.ecrypt.eu.org/stvl/sasc2006/.
5. P. Hawkes, M. Paddon, G. Rose, and M. W. de Vries. Primitive specification for NLS. Available at http://www.ecrypt.eu.org/stream/nls.html, April 2005.
6. P. Hawkes, M. Paddon, G. Rose, and M. W. de Vries. Primitive specification for NLSv2. eSTREAM, March 2006. Available at http://www.ecrypt.eu.org/stream/nls.html.
7. M. Matsui. Linear cryptoanalysis method for DES cipher. In *Advances in Cryptology - EUROCRYPT '93*, volume 765 of *Lecture Notes in Computer Science*, pages 386–397. Springer, 1993.
8. NIST. SKIPJACK and KEA algorithm specifications. Available at http://csrc.nist.gov/CryptoToolkit/skipjack/skipjack.pdf, May 1998.

A Recursion Relation

Let us remind a calculus on recursion relation. Assume that we have the recursive relation

$$x_n = r \cdot x_{n-1} + c$$

then, we can write

$$x_1 = r \cdot x_0 + c, \quad x_2 = r \cdot x_1 + c = r^2 \cdot x_0 + rc + c, \cdots, \quad x_n = r^n \cdot x_0 + c(1 + r + \cdots + r^{n-1}).$$

If $r \neq 1$, we get

$$1 + r + r^2 + \cdots + r^{n-1} = \frac{1 - r^n}{1 - r}.$$

Thus, x_n can be expressed as follows.

$$x_n = \frac{c(1 - r^n)}{1 - r} + x_0 \cdot r^n$$

If $r = 1$, then $x_n = x_0 + c \cdot n$.

B Proof of Lemma 2

From Definition 2, we obtain

$$\Gamma_i \cdot (x \boxplus y \boxplus z) = \Gamma_i \cdot (x \oplus y \oplus z) \oplus \Gamma_{i-1} \cdot (R(x, y) \oplus R(x \boxplus y, z)).$$

Thus, our task is to find $Pr[\Gamma_{i-1} \cdot (R(x, y) \oplus R(x \boxplus y, z)) = 0]$. Let us denote

- $L_i = x_{(i)} \oplus y_{(i)} \oplus z_{(i)}$
- $Q_i = x_{(i)} y_{(i)} \oplus y_{(i)} z_{(i)} \oplus z_{(i)} x_{(i)}$
- $T_i = x_{(i)} y_{(i)} z_{(i)}$

Assume further that X_i and Y_i are defined as follows.

$$\begin{aligned}
X_i &\triangleq R(x, y)_{(i)} \oplus R(x \boxplus y, z)_{(i)} \\
&= x_{(i)} y_{(i)} \oplus y_{(i)} z_{(i)} \oplus z_{(i)} x_{(i)} \oplus (x_{(i)} \oplus y_{(i)} \oplus z_{(i)})(R(x, y)_{(i-1)} \oplus R(x \boxplus y, z)_{(i-1)}) \oplus \\
&\quad R(x, y)_{(i-1)} R(x \boxplus y, z)_{(i-1)} \\
&= Q_i \oplus L_i X_{i-1} \oplus Y_{i-1} \\
Y_i &\triangleq R(x, y)_{(i)} R(x \boxplus y, z)_{(i)} \\
&= x_{(i)} y_{(i)} z_{(i)} (R(x, y)_{(i-1)} \oplus R(x \boxplus y, z)_{(i-1)}) \oplus \\
&\quad (x_{(i)} y_{(i)} \oplus y_{(i)} z_{(i)} \oplus z_{(i)} x_{(i)}) R(x, y)_{(i-1)} R(x \boxplus y, z)_{(i-1)} \\
&= T_i X_{i-1} \oplus Q_i Y_{i-1}
\end{aligned}$$

Since $Q_i \cdot L_i = T_i$, the following relation between X_i and Y_i holds

$$Y_i = Q_i X_i \oplus Q_i.$$

Let us find out the $Pr[X_i = 0]$. We start from the equation $X_i = Q_i \oplus L_i X_{i-1} \oplus Y_{i-1}$ and replace Y_{i-1} by $Y_{i-1} = Q_{i-1} X_i \oplus Q_{i-1}$, so we find

$$X_i = Q_i \oplus L_i X_{i-1} \oplus Y_{i-1} = Q_i \oplus Q_{i-1} \oplus (L_i \oplus Q_{i-1}) X_{i-1}. \tag{11}$$

This gives us

$$Pr[X_i = 0] = \frac{1}{2}Pr[X_{i-1} = 0] + \frac{1}{4}(1 - Pr[X_{i-1} = 0]) = \frac{1}{4} + \frac{1}{4}Pr[X_{i-1} = 0]$$

Therefore, applying the recursion relation from Appendix A, we obtain

$$Pr[X_i = 0] = \frac{1}{3} + \frac{1}{3}2^{-2i-1}. \tag{12}$$

Note that $Pr[X_0 = 0] = Pr[x_{(0)}y_{(0)} \oplus y_{(0)}z_{(0)} \oplus z_{(0)}x_{(0)} = 0] = \frac{1}{2}$. From our definitions, we can write that

$$\begin{aligned} \Gamma_{i-1} \cdot (R(x,y) \oplus R(x \boxplus y, z)) &= X_{i-1} \oplus X_i = Q_i \oplus (L_i \oplus 1)X_{i-1} \oplus Y_{i-1} \\ &= Q_i \oplus Q_{i-1} \oplus (L_i \oplus Q_{i-1} \oplus 1)X_{i-1} \end{aligned}$$

Therefore,

$$Pr[\Gamma_{i-1} \cdot (R(x,y) \oplus R(x \boxplus y, z)) = 0] = \begin{cases} Pr[Q_i \oplus Q_{i-1} = 0] = \frac{1}{2}, & \text{if } X_{i-1} = 0, \\ Pr[Q_i \oplus L_i \oplus 1 = 0] = \frac{3}{4}, & \text{if } X_{i-1} = 1 \end{cases}$$

By applying Equation (12), we get the final result

$$\begin{aligned} Pr[\Gamma_{i-1} \cdot (R(x,y) \oplus R(x \boxplus y, z))] &= \frac{1}{2}Pr[X_{i-1} = 0] + \frac{3}{4}(1 - Pr[X_{i-1} = 0]) \\ &= \frac{3}{4} - \frac{1}{4}Pr[X_{i-1} = 0] \\ &= \frac{2}{3} - \frac{1}{3}2^{-2i-1} \end{aligned}$$

C Proof of Lemma 4

Our task is to determine the probability that the following approximation is true:

$$\Gamma_i \cdot (x \boxplus y) \oplus \Gamma_i \cdot (z \boxplus w) = \Gamma_i \cdot (x \boxplus z) \oplus \Gamma_i \cdot (y \boxplus w).$$

We add both sides of the approximation and are going to find the probability that it becomes zero. So we have

$$\begin{aligned} &\Gamma_i \cdot (x \boxplus y) \oplus \Gamma_i \cdot (z \boxplus w) \oplus \Gamma_i \cdot (x \boxplus z) \oplus \Gamma_i \cdot (y \boxplus w) \\ &= \Gamma_{i-1} \cdot (R(x,y) \oplus R(z,w) \oplus R(x,z) \oplus R(y,w)) \\ &= x_{(i)}y_{(i)} \oplus z_{(i)}w_{(i)} \oplus x_{(i)}z_{(i)} \oplus y_{(i)}w_{(i)} \oplus (x_{(i)} \oplus y_{(i)} \oplus 1)R(x,y)_{(i-1)} \\ &\oplus (z_{(i)} \oplus w_{(i)} \oplus 1)R(z,w)_{(i-1)} \oplus (x_{(i)} \oplus z_{(i)} \oplus 1)R(x,z)_{(i-1)} \oplus (y_{(i)} \oplus w_{(i)} \oplus 1)R(y,w)_{(i-1)} \\ &\triangleq \Lambda_i \end{aligned}$$

Then, Λ_i can be split into eight cases according to the values of $(x_{(i)}, y_{(i)}, z_{(i)}, w_{(i)})$ as follows:

- (0,0,0,0),(1,1,1,1) : $R(x,y)_{(i-1)} \oplus R(z,w)_{(i-1)} \oplus R(x,z)_{(i-1)} \oplus R(y,w)_{(i-1)}$
- (0,0,0,1),(1,1,1,0) : $R(x,y)_{(i-1)} \oplus R(x,z)_{(i-1)}$
- (0,0,1,0),(1,1,0,1) : $R(x,y)_{(i-1)} \oplus R(y,w)_{(i-1)}$
- (0,1,0,0),(1,0,1,1) : $R(x,z)_{(i-1)} \oplus R(z,w)_{(i-1)}$
- (1,0,0,0),(0,1,1,1) : $R(y,w)_{(i-1)} \oplus R(z,w)_{(i-1)}$

- (0,0,1,1),(1,1,0,0) : $R(x,y)_{(i-1)} \oplus R(z,w)_{(i-1)} \oplus 1$
- (0,1,0,1),(1,0,1,0) : $R(x,z)_{(i-1)} \oplus R(y,w)_{(i-1)} \oplus 1$
- (0,1,1,0),(1,0,0,1) : 0

In order to compute $Pr[\Lambda_i = 0]$, the following three probabilities are required.

- $\alpha_i = Pr[R(x,y)_{(i)} \oplus R(z,w)_{(i)} \oplus 1 = 0]$
- $\beta_i = Pr[R(x,y)_{(i)} \oplus R(x,z)_{(i)} = 0]$
- $\gamma_i = Pr[R(x,y)_{(i)} \oplus R(z,w)_{(i)} \oplus R(x,z)_{(i)} \oplus R(y,w)_{(i)} = 0]$

They can be used to state that

$$Pr[\Lambda_i = 0] = \frac{1}{4}\alpha_{i-1} + \frac{1}{2}\beta_{i-1} + \frac{1}{8}\gamma_{i-1} + \frac{1}{8} \tag{13}$$

Now the probabilities α_i, β_i and γ_i are computed as follows.

(1) From Lemma 1, we get

$$\alpha_i = \frac{3}{8} + \frac{1}{4}\alpha_{i-1} \quad \Rightarrow \quad \alpha_i = \frac{1}{2} - 2^{-2i-3}$$

(2) Using Appendix F, we write

$$\beta_i = \frac{1}{2} + \frac{1}{4}\beta_{i-1} \quad \Rightarrow \quad \beta_i = \frac{2}{3} + \frac{1}{3}2^{-2i-2}$$

(3) By definition, we see that

$$\begin{aligned}
&R(x,y)_{(i)} \oplus R(z,w)_{(i)} \oplus R(x,z)_{(i)} \oplus R(y,w)_{(i)} \\
&= x_{(i)}y_{(i)} \oplus z_{(i)}w_{(i)} \oplus x_{(i)}z_{(i)} \oplus y_{(i)}w_{(i)} \oplus (x_{(i)} \oplus y_{(i)})R(x,y)_{(i-1)} \\
&\oplus (z_{(i)} \oplus w_{(i)})R(z,w)_{(i-1)} \oplus (x_{(i)} \oplus z_{(i)})R(x,z)_{(i-1)} \oplus (y_{(i)} \oplus w_{(i)})R(y,w)_{(i-1)}
\end{aligned}$$

According to the values of $(x_{(i)}, y_{(i)}, z_{(i)}, w_{(i)})$, we consider the following cases:
- (0,0,0,0),(1,1,1,1) : 0
- (0,0,0,1),(1,1,1,0) : $R(z,w)_{(i-1)} \oplus R(y,w)_{(i-1)}$
- (0,0,1,0),(1,1,0,1) : $R(z,w)_{(i-1)} \oplus R(x,z)_{(i-1)}$
- (0,1,0,0),(1,0,1,1) : $R(x,y)_{(i-1)} \oplus R(y,w)_{(i-1)}$
- (1,0,0,0),(0,1,1,1) : $R(x,y)_{(i-1)} \oplus R(x,z)_{(i-1)}$
- (0,0,1,1),(1,1,0,0) : $1 \oplus R(x,z)_{(i-1)} \oplus R(y,w)_{(i-1)}$
- (0,1,0,1),(1,0,1,0) : $1 \oplus R(x,y)_{(i-1)} \oplus R(z,w)_{(i-1)}$
- (0,1,1,0),(1,0,0,1) : $R(x,y)_{(i-1)} \oplus R(z,w)_{(i-1)} \oplus R(x,z)_{(i-1)} \oplus R(y,w)_{(i-1)}$

Hence, we establish that

$$\begin{aligned}
\gamma_i &= \frac{1}{4}\alpha_{i-1} + \frac{1}{2}\beta_{i-1} + \frac{1}{8}\gamma_{i-1} + \frac{1}{8} \\
&= \frac{1}{4}\sum_{j=0}^{i-1}\alpha_j 2^{-3(i-j-1)} + \frac{1}{2}\sum_{j=0}^{i-1}\beta_j 2^{-3(i-j-1)} + 2^{-3i}\gamma_0 + \frac{1}{7}(1 - 2^{-3i}) \\
&= \frac{2}{3} + \frac{1}{3}2^{-2i-2}
\end{aligned}$$

Therefore, the probability given in Equation (13) becomes

$$\begin{aligned} Pr[\Lambda_i = 0] &= \frac{1}{4}\alpha_{i-1} + \frac{1}{2}\beta_{i-1} + \frac{1}{8}\gamma_{i-1} + \frac{1}{8} \\ &= \frac{1}{4}(\frac{1}{2} - 2^{-2i-1}) + \frac{1}{2}(\frac{2}{3} + \frac{1}{3}2^{-2i}) + \frac{1}{8}(\frac{2}{3} + \frac{1}{3}2^{-2i}) + \frac{1}{8} \\ &= \frac{2}{3} + \frac{1}{3}2^{-2i-2} \end{aligned}$$

and gives the final result.

D Proof of Corollary 3

We take both sides of the approximation, add them and find the probability when it becomes zero so

$$\begin{aligned} &\Gamma_i \cdot (x \boxplus y) \oplus \Gamma_i \cdot (x \boxplus z) \oplus \Gamma_i \cdot (y \boxplus w) \oplus \Gamma_i \cdot (z \oplus w) \\ &= \Gamma_{i-1} \cdot (R(x,y) \oplus R(x,z) \oplus R(y,w)) \\ &= x_{(i)}y_{(i)} \oplus (x_{(i)} \oplus y_{(i)} \oplus 1)R(x,y)_{(i-1)} \oplus x_{(i)}z_{(i)} \oplus (x_{(i)} \oplus z_{(i)} \oplus 1)R(x,z)_{(i-1)} \\ &\oplus y_{(i)}w_{(i)} \oplus (y_{(i)} \oplus w_{(i)} \oplus 1)R(y,w)_{(i-1)} \end{aligned}$$

Next, the expression $\Gamma_i \cdot (R(x,y) \oplus R(x,z) \oplus R(y,w))$ is split into the following cases according to $(x_{(i)}, y_{(i)}, z_{(i)}, w_{(i)})$:

- $(0,0,0,0) : R(x,y)_{(i-1)} \oplus R(x,z)_{(i-1)} \oplus R(y,w)_{(i-1)}$
- $(1,1,1,1) : 1 \oplus R(x,y)_{(i-1)} \oplus R(x,z)_{(i-1)} \oplus R(y,w)_{(i-1)}$
- $(1,0,0,0) : R(y,w)_{(i-1)}, \quad (0,1,1,1) : 1 \oplus R(y,w)_{(i-1)}$
- $(0,1,0,0) : R(x,z)_{(i-1)}, \quad (1,0,1,1) : 1 \oplus R(x,z)_{(i-1)}$
- $(0,0,1,1) : R(x,y)_{(i-1)}, \quad (1,1,0,0) : 1 \oplus R(x,y)_{(i-1)}$
- $(0,0,1,0), (1,1,0,1) : R(x,y)_{(i-1)} \oplus R(y,w)_{(i-1)}$
- $(0,1,0,1), (1,0,1,0) : 1 \oplus R(x,z)_{(i-1)} \oplus R(y,w)_{(i-1)}$
- $(0,0,0,1), (1,1,1,0) : R(x,y)_{(i-1)} \oplus R(x,z)_{(i-1)}$
- $(0,1,1,0), (1,0,0,1) : 0$

Note that there are four pairs which are complement of each other. Using the notation of Appendix C, we get

$$\begin{aligned} \alpha_i &= Pr[1 \oplus R(x,z)_i \oplus R(y,w)_i = 0] = \frac{1}{2} - 2^{-2i-3} \\ \beta_i &= Pr[R(x,y)_i \oplus R(x,z)_i = 0] = Pr[R(x,y)_i \oplus R(y,w)_i = 0] = \frac{2}{3} + \frac{1}{3}2^{-2i-2} \end{aligned}$$

Therefore, we get the final result

$$\begin{aligned} &Pr[\Gamma_{i-1} \cdot (R(x,y) \oplus R(x,z) \oplus R(y,w)) = 0] \\ &= \frac{3}{8} + \frac{1}{4}\beta_{(i-1)} + \frac{1}{16}\alpha_{(i-1)} = \frac{3}{8} + \frac{1}{4}(\frac{2}{3} + \frac{1}{3}2^{-2i}) + \frac{1}{8}(\frac{1}{2} - 2^{-2i-1}) \\ &= \frac{29}{48} + \frac{1}{3}2^{-2i-4} \end{aligned}$$

E Proof of Lemma 3

Let us denote $\Phi_{n,(i)}$ as

$$\Phi_{n,(i)} = R(x_1,k)_{(i)} \oplus R(x_2,k)_{(i)} \oplus \cdots \oplus R(x_n,k)_{(i)}$$

E.1 $\mathbf{Pr[\Phi_{n,(i)} = 0]}$

By definition, $R(x,k)_{(i)} = x_{(i)}k_{(i)} \oplus (x_{(i)} \oplus k_{(i)})R(x,k)_{(i-1)}$. Thus,

$$\begin{aligned}\Phi_{n,(i)} = k_{(i)}(x_{1,(i)} \oplus x_{2,(i)} \oplus \cdots \oplus x_{n,(i)}) \oplus (x_{1,(i)} \oplus k_{(i)})R(x_1,k)_{(i-1)} \oplus \\ (x_{2,(i)} \oplus k_{(i)})R(x_2,k)_{(i-1)} \oplus \cdots \oplus (x_{n,(i)} \oplus k_{(i)})R(x_n,k)_{(i-1)}\end{aligned}$$

Then, $\Phi_{n,(i)}$ has the following properties.

- If $\bigoplus_{t=1}^{n} x_{t,(i)} = 0$, then there exists a pair of $(x_{1,(i)}, x_{2,(i)}, \ldots, x_{n,(i)}, k_{(i)})$ which generate the same $\Phi_{n,(i)}$. For instance, $(x_{1,(i)}, x_{2,(i)}, \ldots, x_{n,(i)}, k_{(i)})$ and $(1 \oplus x_{1,(i)}, \ldots, 1 \oplus x_{n,(i)}, 1 \oplus k_{(i)})$ produce the identical $\Phi_{n,(i)}$.
- If $\bigoplus_{t=1}^{n} x_{t,(i)} = 1$, then there exists a pair of $(x_{1,(i)}, x_{2,(i)}, \ldots, x_{n,(i)}, k_{(i)})$ whose $\Phi_{n,(i)}$s are complement each other. For instance, $(x_{1,(i)}, x_{2,(i)}, \ldots, x_{n,(i)}, k_{(i)})$ and $(1 \oplus x_{1,(i)}, 1 \oplus x_{2,(i)}, \ldots, 1 \oplus x_{n,(i)}, 1 \oplus k_{(i)})$ produce a complement $\Phi_{n,(i)}$ each other.

Hence, by defining, $P_{r,(i)} = Pr[\bigoplus_{t=1}^{r} R(x_t,k)_{(i)} = 0]$, we get

$$P_{n,(i)} = \frac{1}{2^{n+1}}[\sum_{r=0}^{n/2} \binom{n}{2r} 2P_{2r,(i-1)} + \sum_{r=0}^{n/2-1} \binom{n}{2r+1}] = \frac{1}{4} + \frac{1}{2^n} \sum_{r=0}^{n/2} \binom{n}{2r} P_{2r,(i-1)}$$

where $P_0 = 1$.
Hence, when i is much bigger than 0,

$$P_{n,(i)} \approx \frac{n+2}{2(n+1)}$$

E.2 $\mathbf{Pr[\Phi_{n,(i-1)} \oplus \Phi_{n,(i)} = 0]}$

By definition, we can write $(x \boxplus k)_{(i)} = x_{(i)} \oplus k_{(i)} \oplus R(x,k)_{(i-1)}$. Thus, we get

$$\begin{aligned}&\Gamma_i \cdot (x_1 \boxplus k) \oplus \Gamma_i \cdot (x_2 \boxplus k) \oplus \cdots \oplus \Gamma_i \cdot (x_n \boxplus k) \oplus \Gamma_i \cdot (x_1 \oplus x_2 \oplus \cdots \oplus x_n) \\ &= \Gamma_{i-1} \cdot (R(x_1,k) \oplus R(x_2,k) \oplus \cdots \oplus R(x_n,k)) \\ &= \Phi_{n,(i-1)} \oplus \Phi_{n,(i)} \\ &= k_{(i)}(x_{1,(i)} \oplus x_{2,(i)} \oplus \cdots \oplus x_{n,(i)}) \oplus (x_{1,(i)} \oplus k_{(i)} \oplus 1)R(x_1,k)_{(i-1)} \oplus \\ &(x_{2,(i)} \oplus k_{(i)} \oplus 1)R(x_2,k)_{(i-1)} \oplus \cdots \oplus (x_{n,(i)} \oplus k_{(i)} \oplus 1)R(x_n,k)_{(i-1)}\end{aligned}$$

As before, we can get the following equation

$$\begin{aligned}Pr[\Phi_{n,(i-1)} \oplus \Phi_{n,(i)} = 0] &= \frac{1}{4} + \frac{1}{2^n} \sum_{r=0}^{n/2} \binom{n}{2r} P_{n-2r,(i-1)} \\ &= \frac{1}{4} + \frac{1}{2^n} \sum_{r=0}^{n/2} \binom{n}{n-2r} P_{n-2r,(i-1)} \\ &= P_{n,(i)}\end{aligned}$$

Therefore, when i is much bigger than 0, we have

$$Pr[\Phi_{n,(i-1)} \oplus \Phi_{n,(i)} = 0] \approx \frac{n+2}{2(n+1)}$$

which concludes the proof.

F Proof of Corollary 2

From Definition 2, we write

$$R(x,y)_{(i)} \oplus R(x,z)_{(i)} = x_{(i)}y_{(i)} \oplus (x_{(i)} \oplus y_{(i)})R(x,y)_{(i-1)} \oplus x_{(i)}z_{(i)} \oplus (x_{(i)} \oplus z_{(i)})R(x,z)_{(i-1)}$$

Then, according to $(x_{(i)}, y_{(i)}, z_{(i)})$, the expression $R(x,y)_{(i)} \oplus R(x,z)_{(i)}$ is split as follows.

- $(0,0,0),(1,1,1) : 0$
- $(0,1,1),(1,0,0) : R(x,y)_{(i-1)} \oplus R(x,z)_{(i-1)}$
- $(0,0,1) : R(x,z)_{(i-1)},\quad (0,1,0) : R(x,y)_{(i-1)}$
- $(1,1,0) : 1 \oplus R(x,z)_{(i-1)},\ (1,0,1) : 1 \oplus R(x,y)_{(i-1)}$

We can see that the third and fourth are pairwise complement with the probability of $\frac{1}{8}$ each. Hence,

$$\begin{aligned} Pr[R(x,y)_{(i)} \oplus R(x,z)_{(i)} = 0] &= \frac{1}{4} + 2 \cdot \frac{1}{8} + \frac{1}{4} Pr[R(x,y)_{(i-1)} \oplus R(x,z)_{(i-1)} = 0] \\ &= \frac{1}{2} + \frac{1}{4} Pr[R(x,y)_{(i-1)} \oplus R(x,z)_{(i-1)} = 0] \end{aligned}$$

Using the recursion relation from Appendix A, we state that

$$Pr[R(x,y)_{(i)} \oplus R(x,z)_{(i)} = 0] = \frac{2}{3} + \frac{1}{3} 2^{-2i-2}$$

Applying Definition 2, we can get

$$\begin{aligned} &\Gamma_i \cdot (x \boxplus y) \oplus \Gamma_i \cdot (x \boxplus z) \oplus \Gamma_i \cdot (y \oplus z) \\ &= \Gamma_{i-1} \cdot (R(x,y) \oplus R(x,z)) \\ &= x_{(i)}y_{(i)} \oplus (x_{(i)} \oplus y_{(i)} \oplus 1)R(x,y)_{(i-1)} \oplus x_{(i)}z_{(i)} \oplus (x_{(i)} \oplus z_{(i)} \oplus 1)R(x,z)_{(i-1)} \end{aligned}$$

Therefore, arguing in similar way as above, we establish that

$$\begin{aligned} Pr[\Gamma_i \cdot (R(x,y) \oplus R(x,z)) = 0] &= \frac{1}{2} + \frac{1}{4} Pr[R(x,y)_{(i-1)} \oplus R(x,z)_{(i-1)} = 0] \\ &= \frac{2}{3} + \frac{1}{3} 2^{-2i-2}. \end{aligned}$$

G Proof of Lemma 6

From the approximation being considered, w.l.g we assume that $x = 0$ and $y = 0$ since the variables x and y are independent on the expressions $(a \boxplus b \boxplus k)$ and $(c \boxplus d \boxplus k)$.

Then, the approximation is simplified as follows.

$$\Gamma_i \cdot (x \boxplus a) \oplus \Gamma_i \cdot (y \boxplus b) \oplus \Gamma_i \cdot (x \boxplus c) \oplus \Gamma_i \cdot (y \boxplus d) \oplus \Gamma_i \cdot (a \boxplus b \boxplus k) \oplus \Gamma_i \cdot (c \boxplus d \boxplus k)$$
$$= \Gamma_{i-1} \cdot (R(a,b) \oplus R(a \boxplus b, k)) \oplus \Gamma_{i-1} \cdot (R(c,d) \oplus R(c \boxplus d, k))$$

Using the recursive relation (11) in Appendix B, we have

$$(R(a,b) \oplus R(a \boxplus b, k))_{(i)} \oplus (R(c,d) \oplus R(c \boxplus d, k))_{(i)}$$
$$= Q_{1,(i)} \oplus Q_{1,(i-1)} \oplus (L_{1,(i)} \oplus Q_{1,(i-1)})(R(a,b)_{(i-1)} \oplus R(a \boxplus b, k)_{(i-1)}) \oplus$$
$$Q_{2,(i)} \oplus Q_{2,(i-1)} \oplus (L_{2,(i)} \oplus Q_{2,(i-1)})(R(c,d)_{(i-1)} \oplus R(c \boxplus d, k)_{(i-1)})$$

where $Q_{1,(i)} = a_{(i)}b_{(i)} \oplus b_{(i)}k_{(i)} \oplus k_{(i)}a_{(i)}$, $Q_{2,(i)} = c_{(i)}d_{(i)} \oplus d_{(i)}k_{(i)} \oplus k_{(i)}c_{(i)}$, $L_{1,(i)} = a_{(i)} \oplus b_{(i)} \oplus k_{(i)}$ and $L_{2,(i)} = c_{(i)} \oplus d_{(i)} \oplus k_{(i)}$.
According to the values of ten variables $(a_{(i)}, b_{(i)}, c_{(i)}, d_{(i)}, k_{(i)}, a_{(i-1)}, b_{(i-1)}, c_{(i-1)}, d_{(i-1)}, k_{(i-1)})$, the above expression is simplified as a function of $(R(a,b)_{(i-1)} \oplus R(a \boxplus b, k)_{(i-1)})$ and $(R(c,d)_{(i-1)} \oplus R(c \boxplus d, k)_{(i-1)})$.
Hence, by counting appropriate probabilities, we get

$$Pr[(R(a,b) \oplus R(a \boxplus b, k))_{(i)} \oplus (R(c,d) \oplus R(c \boxplus d, k))_{(i)} = 0]$$
$$= \frac{35}{64} - \frac{3}{64} \cdot Pr[(R(a,b) \oplus R(a \boxplus b, k))_{(i-1)} = 0] - \frac{3}{64} \cdot Pr[(R(c,d) \oplus R(c \boxplus d, k))_{(i-1)} = 0]$$
$$+ \frac{5}{64} \cdot Pr[(R(a,b) \oplus R(a \boxplus b, k))_{(i-1)} \oplus (R(c,d) \oplus R(c \boxplus d, k))_{(i-1)} = 0]$$

From Lemma 2, we know that

$$Pr[(R(a,b) \oplus R(a \boxplus b, k))_{(i-1)} = 0] = Pr[(R(c,d) \oplus R(c \boxplus d, k))_{(i-1)} = 0] = \frac{1}{3} + \frac{1}{3}2^{-2i+1}$$

Therefore, by the recursive relation of Appendix A, for $i > 0$,

$$Pr[(R(a,b) \oplus R(a \boxplus b, k))_{(i)} \oplus (R(c,d) \oplus R(c \boxplus d, k))_{(i)} = 0] \approx \frac{33}{59} = \frac{1}{2}(1 + 2^{-3.1})$$

Since $Pr[(R(a,b) \oplus R(a \boxplus b, k))_{(i)} \oplus (R(c,d) \oplus R(c \boxplus d, k))_{(i)} = 0]$ is identical to $Pr[\Gamma_{i-1} \cdot (R(a,b) \oplus R(a \boxplus b, k)) \oplus \Gamma_{i-1} \cdot (R(c,d) \oplus R(c \boxplus d, k)) = 0]$, the lemma holds.