Further Clarification on Mantin's Digraph Repetition Bias in RC4

Pranab Chakraborty · Subhamoy Maitra

Abstract In this paper we provide a theoretical argument towards an unsolved question related to Mantin's "Digraph Repetition Bias" (Eurocrypt 2005) that is observed in the key-stream of RC4. The open question, that depends on the observation that arrival of four consecutive same bytes (of the form $AAAA$) in RC4 key-stream is slightly negatively biased, was posed by Bricout et al [Des. Codes Cryptogr. (2018) 86:743-770] in 2016. Moreover, for the first time, we consider the "Reverse Digraph Repetition Bias" and show that there is significant negative bias in arrival of $ABBA$ (A, B two distinct bytes) in RC4 key-stream.

Keywords RC4 · Non-randomness · Sequence · Stream Cipher.

1 Introduction

RC4 is possibly the most popular stream cipher and it attracted huge attention in the domain of cryptanalysis (see for example [4–6] and the references therein). Recently there are evidences of almost practical attacks on this cipher and thus the cipher is not recommended to be deployed in new systems. However, this cipher still handles considerable traffic in different networks and thus of interest to cryptologic community. At the same time, the cipher is a very interesting combinatorial object to study. Even after serious efforts for around four decades, we are still amazed with novel results continuously coming in this domain of research.

The best long term bias observed in RC4 keystream was provided by Mantin long back [3]. It says that the probability of obtaining a substring of the form $AB\mathcal{T}AB$ (A, B 8-bit characters and $\mathcal{T}$ is a short string of such characters) in RC4 stream is greater than what should be obtained in a true random situation. This bias is famously referred to as the "Digraph Repetition Bias" in RC4. A detailed

Pranab Chakraborty
Learning and Development, Human Resources, Wipro Limited, Doddakannelli, Sarjapur Road, Bangalore 560035, India. E-mail: kojagori@gmail.com

Subhamoy Maitra
Applied Statistics Unit, Indian Statistical Institute, 203 B T Road, Kolkata 700108, India, E-mail: subho@isical.ac.in

study in this regard has been presented recently in [1], which is referred as the fine-grained analysis. Through this analysis it has been theoretically argued in [1, Theorem 1] that the bias should be little more in the case when $A = B$. However, all the cases under this situation could not be clarified in [1] and in particular, when $A = B$ and $\mathcal{T}$ is null, then the bias could not be observed at all through experiments. The authors of [1] thus commented,

> "However, when $A = B$, we do not see the positive bias behaviour predicted by [1, Theorem 1], but instead a small, negative bias. We do not currently have an explanation for this behaviour."

In this paper, we answer this question with detailed theoretical analysis of RC4 evolution during the pseudo-random key-stream generation process.

As it is interesting to consider the patterns of the form $AB\mathcal{T}AB$, one may also explore the "Reverse Digraph Repetition Bias" of the form $AB\mathcal{T}BA$. We study this in a disciplined manner in this paper and note that when $\mathcal{T}$ is null, that is the string is of the form $ABBA$, then there is significant negative bias. However, such significant biases could not been observed for non-null $\mathcal{T}$.

Before proceeding further, let us first quickly describe the RC4 algorithm. In RC4, we have an $N = 256$ length array of 8-bit integers 0 to $N - 1$, that works as a permutation. There is also an l length array of bytes K (the secret key), where l may vary from 5 to 32, depending on the key length. There are also two bytes i, j, where i is the deterministic index that increases by 1 in each step and j is updated in a manner so that it behaves pseudo-randomly. The Key Scheduling Algorithm (KSA) of RC4 is as follows:

- $j = 0$; for $i = 0$ to $N - 1$: $S[i] = i$;
- for $i = 0$ to $N - 1$:
  $j = j + S[i] + K[i \bmod l]$; swap$(S[i], S[j])$;

Next, the pseudo-random bytes z are generated during the Pseudo Random Generator Algorithm (PRGA) as follows:

- $i = j = 0$;
- for $i = 0$ to $N - 1$:
  $i = i + 1$; $j = j + S[i]$; swap$(S[i], S[j])$; $z = S[S[i] + S[j]]$;

All the additions here are modulo N.

The work of [3] presented the first distinguisher for RC4 when any amount of initial keystream bytes are thrown away. This distinguisher is based on the digraph distribution of RC4. The term digraph means a pair of consecutive keystream words. In [3, Section 3], it has been shown that getting strings of the pattern $AB\mathcal{T}AB$ (where A, B are bytes and $\mathcal{T}$ is a string of bytes of small length $G \leq 16$), is more probable in RC4 keystream than in random stream. The exact theoretical result [3, Theorem 1] is as follows.

Theorem 1 *During RC4 PRGA, for small integer values of* $G \geq 0$

$$\Pr((z_{r+G+2} = A) \wedge (z_{r+G+3} = B) | (z_r = A, z_{r+1} = B)) = \frac{1}{N^2}(1 + \frac{e^{\frac{-8-8G}{N}}}{N}).$$

This result is true for most of the cases under some logical assumptions on independence. However, it should be noted that being a deterministic stream cipher on

a classical paradigm, the states of RC4 actually dependent on each other, whatever less the influence may be. Thus, there are cases, where the bias is not exactly the same as in Theorem 1. In this direction detailed analysis has been presented in [1] and it has been observed that when $A = B$, the bias is more prominent.

Theorem 2 *During RC4 PRGA, for small integer values of* $G \geq 0$

$$\Pr((z_{r+G+2} = A) \wedge (z_{r+G+3} = A) | (z_r = A, z_{r+1} = A)) = \frac{1}{N^2}(1 + \frac{e^{\frac{-4-6G}{N}}}{N}).$$

Interestingly, this bias could not be observed for $G = 0$ in experiments as explained following [1, Figure 2].

In RC4 related research, the biases are generally identified in two ways.

- One can run some experiments to observe the biases and then try to prove them.
- One can theoretically inspect the algorithm to obtain the bias, prove it theoretically and then supplement it with experiments.

As we have commented earlier, the proofs are completed based on certain assumptions. Thus, in specific cases, due to incorrect assumptions, the reported biases may not exist. These are identified later through more disciplined studies. This is exactly what has been pointed out in [1] and left as an open question. In fact, in this case we actually do not concentrate on showing the bias. Rather we try to argue with detailed theoretical analysis that the bias is indeed negligible.

1.1 Organization & Contribution

This paper is on further study related to Mantin's "Digraph Repetition Bias" [3]. In Section 2, we explain the technical background that had been studied in [3, 1].

- In that context, we present the solution of an unsolved question posed in [1] in Section 3. We show that the arrival of strings of the form $AAAA$ in RC4 key-stream is slightly negatively biased.
- As a natural consequence, we explore the "Reverse Digraph Repetition Bias" in Section 4. We show that the arrival of strings of the form $ABBA$ is significantly negatively biased (same order of $ABAB$ as in [3]). However, we could not observe such high negative bias for $AB\mathcal{T}BA$, when $\mathcal{T}$ is non-null.

Section 5 concludes the paper.

2 Background: Explanation of Mantin's Bias [3]

In this section we first explain in details the arguments presented by Mantin in Lemma 2 and Theorem 1 in [3] and then describe additional refinements of the result by Bricout et. al. in [1]. While experimenting on the refinements of the proposed results, Bricout et. al. identified a deviation in the observed behavior (from the expected behavior predicted by Theorem 1 in [1]) for a specific form of digraph repetition sequence that has the form $AAAA$. To the best of our knowledge, this deviation remained unexplained so far. In this section, We present a theoretical explanation to this behavior.

2.1 Revisiting Mantin's result [3]

It appears that due to a possible typographical error, the statement of [3, Theorem 1] is not exactly correct, and it differs slightly from the proof. As given correctly in the proof, during RC4 PRGA, for small integer values of $G \geq 0$

$$\Pr((z_{r+G+2} = A) \wedge (z_{r+G+3} = B) | (z_r = A, z_{r+1} = B)) = \frac{1}{N^2}(1 + \frac{e^{\frac{-8-8G}{N}}}{N}).$$

However, the theorem statement says,

$$\Pr((z_{r+G+2} = A) \wedge (z_{r+G+3} = B) | (z_r = A, z_{r+1} = B)) = \frac{1}{N^2}(1 + \frac{e^{\frac{-4-8G}{N}}}{N}),$$

where -4 is misprinted instead of -8 in the exponent. This misprint is carried in [1, Result 2] too, where [3, Theorem 1] is referred.

Let us now describe the approach that Mantin had used to prove the stated result and in the process we point out additional clarifications for specific cases that demand refinements of the result. The key observation made by Mantin is the fact that if, with respect to an arbitrary round r of RC4 PRGA, $S_r[i_r + 1] = 1$ and $S_{r-1}[i_r] = x$ is any byte-value other than 1, then at the end of round $r + 1$, the permutation byte pair $(x, 1)$ would move to the location indexed by $(j_r, j_r + 1)$ and if the byte pair remains undisturbed till round $(r + G + 2)$ (where $G \geq 0$ is an integer signifying the gap between the source and destinations pairs), then under an additional condition that $j_{r+G+2} = i_r$, the key-stream byte pair (z_r, z_{r+2}) would repeat as the byte pair (z_{r+G+2}, z_{r+G+3}).

Note that unless specifically mentioned, $S_r[y]$ is the y-th element of the S array, after the swap is done in the r-th round. To be more specific, for a given G, the conditions for the event to occur are as follows:

1. $j_r = i_{r+G+2}$,
2. $S_r[i_r + 1] = 1$,
3. $j_{r+G+2} = i_r$,
4. the locations indexed by i_r, i_{r+1}, i_{r+G+2} and i_{r+G+3} are undisturbed in the intermediate G rounds,
5. the location of the key-stream byte z_r indexed by $S_r[i_r] + S_r[i_{r+G+2}]$ remains unchanged in $G + 2$ rounds $(r + 1, \ldots, r + G + 2)$ and the location of the key-stream byte z_{r+1} indexed by $S_{r+1}[i_{r+1}] + S_{r+1}[i_{r+G+3}]$ remains unchanged in $G + 2$ rounds $(r + 2, \ldots, r + G + 3)$.

Incidentally, Mantin stated the conditions of the theorem by referring to the gap with the variable $g = j_r - i_r$ and later introduced the variable $G = (g - 2)$ and called it the real gap. If $g = 0$, $i_r = j_r$ and the permutation byte pair $(x, 1)$ stays in the same locations at the end of round $r + 1$. Similarly, $g = 1$ is forbidden in real RC4 as Finney cycles [2] can't occur. Therefore, we only consider the case $g \geq 2$ or in other words $G \geq 0$.

The probability associated with the Conditions (1–3) is clearly $\frac{1}{N^3}$. Using [3, Lemma 1], we find that the probability for condition 4 is around $e^{(-4G)/N}$ for small values of G. Similarly, the probability corresponding to the condition 5 is $(1 - \frac{G+2}{N})^2 \cdot e^{\frac{-2(G+2)}{N}} \approx e^{\frac{-4(G+2)}{N}}$. Hence, the combined probability of the desired event according to Conditions (1–5) is $e^{\frac{-8-8G}{N}} \cdot \frac{1}{N^3}$.

On the other hand, for the complimentary scenario with probability $(1 - \frac{1}{N^3})$, in which one or more of the Conditions (1–3) do not hold, we consider the event probability as the fair chance of $\frac{1}{N^2}$. So the combined probability for the complimentary scenario is $(1 - \frac{1}{N^3}) \cdot \frac{1}{N^2}$.

By using the above probability values one can obtain the desired result,

$$\Pr((z_{r+G+2} = A) \wedge (z_{r+G+3} = B) | (z_r = A, z_{r+1} = B)) = \frac{1}{N^2}(1 + \frac{e^{\frac{-8-8G}{N}}}{N}).$$

2.2 Revisiting Bricout et. al. result [1]

Mantin (in [3]) mentioned that for the sake of simplicity he made certain heuristic assumptions. However, those were not elaborated in [3]. Bricout et. al. [1], while performing a fine grained analysis of the proof, showed that there are certain special cases in which one should not expect any digraph repetition bias. For example, Mantin's result would not be applicable for the following cases:

1. $A = 1$
2. $B = 1$
3. $A = (N - 3)$ and $G = 0$
4. $B = (N - 3)$ and $G = 0$

The reason that these cases do not demonstrate digraph repetition bias as per Mantin's result is due to the fact that in each of these cases the condition 5 as required by Mantin's [3, Theorem 1] as stated in Theorem 1 above, gets violated. In addition to the above cases, Bricout et al. [1] also showed that for a generic pattern of the form $AA\mathcal{T}AA$, there should be a stronger digraph repetition bias than the bias given by Mantin's result. We here outline the proof of Theorem 2.

The crucial observation for this result is that when $A = B$, the requirement of condition 5 as per the proof given above for [3, Theorem 1] reduces to the condition of non-disturbance of one target permutation byte position instead of two byte positions. Hence the probability increases by a multiplicative factor of $e^{\frac{2G+4}{N}}$. This brings us to the modified result:

$$\Pr((z_{r+G+2} = A) \wedge (z_{r+G+3} = A) | (z_r = A, z_{r+1} = A)) = \frac{1}{N^2}(1 + \frac{e^{\frac{-4-6G}{N}}}{N}).$$

One should note that the above result is not applicable for certain specific values of A and B [1]. All these deviations, as identified by Bricout et. al. [1], have been experimentally verified in their paper, except one specific class of patterns. For the pattern of the form $AAAA$, the experimental result showed slight negative bias instead of the strong positive bias as expected in Theorem 2. It has been mentioned in [1] that no explanation could be found out for such a deviation. We solve this issue in the next section (Theorem 3) by proving the slight negative bias. We also prove that there is a dependence of the extent of this bias on certain special values of index i_r around which this digraph repetition is observed.

3 Explanation of the Small Negative Bias in the *AAAA* Sequence

We first prove two results (Lemma 1 and Lemma 2) and demonstrate that the probability of two consecutive key-stream bytes to be equal may substantially differ from the fair chance of $\frac{1}{N}$ depending upon the value of the permutation array-byte $S_r[i_r + 1]$. Next, Lemma 1 and Lemma 2 are referred to prove the final result, i.e., Theorem 3.

While proving the these results, we have taken an approach of dividing each proof into various scenarios and conditions. The scenarios are qualified by the values of the deterministic index i and the conditions are constraints on the values of the pseudo-random index j and/or the values of certain permutation array bytes. Some of the scenarios are applicable to special cases of i (e.g., 0 or 1 etc.), while the other scenarios are applicable to either all values of i (designated by "All") or for most values of i (designated by "All but ..."). That is, for a particular value of i, multiple scenarios could be applicable. Finally, for configurations that do not belong to any scenario, we assume a fair chance assumption, i.e., computed the probabilities by assuming uniform random distribution for the values under consideration. Here we have explored deeper towards the analysis. Thus, the level at which we assume such fair probability is quite fine-tuned. This provides a more transparent analysis of the biases.

Lemma 1 *During RC4 PRGA,*

1. $\Pr(z_r = z_{r+1} | S_r[i_r + 1] = 0, i_r \neq 1) = \frac{2}{N^2}$ *and*
2. $\Pr(z_r = z_{r+1} | S_r[i_r + 1] = 0, i_r = 1) = \frac{3}{N^2}$.

Proof Let us assume $S_r[i_r] = p$ and $S_r[j_r] = q$, where p and q are two arbitrary byte values. Hence, $z_r = S_r[p+q]$. In case j_r coincides with i_r, $p = q$. Based on the given condition $S_r[i_r + 1] = 0$, it's evident that $p \neq 0$. We now investigate what happens in round $r + 1$.

- **Before swap:** Since $S_r[i_r + 1] = 0$, $j_{r+1} = j_r$. Thus, $S_{r+1}[i_{r+1}] = 0$ and $S_{r+1}[j_{r+1}] = q$.
- **After swap:** $S_{r+1}[i_{r+1}] = q$ and $S_{r+1}[j_{r+1}] = 0$.

Therefore, $z_{r+1} = S_{r+1}[q + 0] = S_{r+1}[q]$. As $p \neq 0$, $(p + q) \neq q$. So $(p + q)$ and q must point to two different array byte positions of S. The expected condition of $z_r = z_{r+1}$ can be achieved only if $z_r (= S_r[p + q])$ gets swapped in round $r + 1$ and moves to a new position pointed to by q. We now identify the three scenarios that lead to the desired condition of $z_r = z_{r+1}$. For no other configuration the desired condition would hold.

Scenario	i_r	**Event conditions**	$z_r = S_r[p + q]$	$z_{r+1} = S_{r+1}[q]$
1	All	$i_{r+1} = (p + q)$ and $j_{r+1} = q$	0	0
2	All	$i_{r+1} = q$ and $j_{r+1} = (p + q)$	q	q
3	1	$j_r = i_r$ and $p = q = 1$	0	0

In each of these scenarios, we obtain the event probability as $\frac{1}{N^2}$ with the fair chance assumption. By considering the scenario 1 and 2, we obtain $\Pr(z_r = z_{r+1} | S_r[i_r + 1] = 0, i_r \neq 1) = \frac{2}{N^2}$ and by considering all the three scenarios we get $\Pr(z_r = z_{r+1} | S_r[i_r + 1] = 0, i_r = 1) = \frac{3}{N^2}$. □

Lemma 2 *During RC4 PRGA,*

1. $\Pr(z_r = z_{r+1} | S_r[i_r + 1] = (N-1), i_r \notin \{(N-3), (N-2)\}) \approx \frac{2}{N} - \frac{3}{N^2}$ *and*
2. $\Pr(z_r = z_{r+1} | S_r[i_r + 1] = (N-1), i_r \in \{(N-3), (N-2)\}) \approx \frac{2}{N} - \frac{2}{N^2}$.

Proof Let us assume $S_r[i_r] = p$ where p is an arbitrary byte value. Since the given condition states that $S_r[i_r + 1] = (N-1)$, $p \neq (N-1)$. We now investigate the following scenario.

Event condition	i_{r+1}	j_{r+1}	z_r	z_{r+1}
$j_r = i_r + 1$	j_r	i_r	$S_r[p + N - 1] = S_r[p - 1]$	$S_{r+1}[N - 1 + p] = S_{r+1}[p - 1]$

Since $S_r[i_r + 1] = (N-1)$ and $j_r = i_r + 1$, the indices (i and j) swap their positions from round r to round $r+1$, implying $i_{r+1} = j_r$ and $j_{r+1} = i_r$. If the array byte position indexed by $(p-1)$ does not coincide with i_r or j_r, we arrive at the desired condition of $z_r = z_{r+1}$. For almost all values of i_r, the chance of $(p-1)$ not coinciding with i_r or j_r is $(1 - \frac{2}{N-1})$. However, for $i_r = (N-2)$, it is not possible for $(p-1)$ to have the same value as i_r, since p can't be $(N-1)$. Similarly for $i_r = (N-3)$ (which means $i_{r+1} = (N-2)$), it is not possible for $(p-1)$ to have the same value as i_{r+1}. Therefore, for $i_r \in \{(N-3), (N-2)\}$, the chance of $(p-1)$ not coinciding with i_r or j_r is $(1 - \frac{1}{N-1})$. Hence, the probability associated with this scenario is $\frac{1}{N} \cdot (1 - \frac{1}{N-1})$ for $i_r \in \{(N-3), (N-2)\}$ and the probability equals $\frac{1}{N} \cdot (1 - \frac{2}{N-1})$ for rest of the i_r values.

Apart from these three scenarios, in all other cases we consider the probability associated with the desired event to be same as the fair chance of $\frac{1}{N}$. This leads to the final result $\Pr(z_r = z_{r+1} | S_r[i_r + 1] = (N-1), i_r \notin \{(N-3), (N-2)\}) \approx \frac{1}{N} - \frac{2}{N^2} + (1 - \frac{1}{N}) \cdot \frac{1}{N} = \frac{2}{N} - \frac{3}{N^2}$. Similarly, $\Pr(z_r = z_{r+1} | S_r[i_r + 1] = (N-1), i_r \in \{(N-3), (N-2)\}) \approx \frac{1}{N} - \frac{1}{N^2} + (1 - \frac{1}{N}) \cdot \frac{1}{N} = \frac{2}{N} - \frac{2}{N^2}$. □

Now let us present our main theorem. In this regard, we refer to a comment from [1].

> "Aside from the special case of $A = B$ and $G = 0$, we did not observe any additional significant deviations from the behaviour predicted by Result 2 and our refinements of that result. However, a larger-scale computation might well reveal further fine structure. For example, as suggested by a reviewer, it is possible that there is a dependence of biases on i. Since i is known to the attacker, if such biases were present and of significant size, then this would result in exploitable behaviour."

We study such behavior in this paper. Theorem 3 points out that while there is a dependence of the result on the actual value of i, there exists no significant bias that can be considered as exploitable.

Theorem 3 *During RC4 PRGA, assuming that the RC4 state is in a random permutation in the r-th round,*

1. $\Pr((z_r, z_{r+1}) = (z_{r+2}, z_{r+3}) | z_r = z_{r+1}, i_{r+1} \notin \{0, 1, (N-4), (N-3), (N-2)\})$ $\approx \frac{1}{N^2} - \frac{2}{N^4} - \frac{5}{N^5}$,

2. $\Pr((z_r, z_{r+1}) = (z_{r+2}, z_{r+3}) | z_r = z_{r+1}, i_{r+1} \in \{0, 1, (N-4)\}) \approx \frac{1}{N^2} - \frac{1}{N^4} - \frac{5}{N^5}$,
3. $\Pr((z_r, z_{r+1}) = (z_{r+2}, z_{r+3}) | z_r = z_{r+1}, i_{r+1} = (N-3)) \approx \frac{1}{N^2} - \frac{1}{N^4} - \frac{3}{N^5}$,
4. $\Pr((z_r, z_{r+1}) = (z_{r+2}, z_{r+3}) | z_r = z_{r+1}, i_{r+1} = (N-2)) \approx \frac{1}{N^2} - \frac{2}{N^4} - \frac{3}{N^5}$,

Proof We prove this result by analyzing the following scenarios. Since the desired event is centered around four rounds (r, $r+1$, $r+2$ and $r+3$), where the probability of a pattern for key-stream bytes in the third and fourth rounds are analyzed based on a given pattern for the key-stream bytes in the first two rounds, the scenarios are expressed with respect to i_{r+1}.

Scenario	i_{r+1}	**Conditions**	**Probability**
1	All	$S_r[i_{r+1}] = 1$, $j_r = i_{r+2}$ and $j_{r+2} = i_r$	$\frac{1}{N^3}$
2(a)	All but 1	$S_{r+1}[i_{r+2}] = 0$	$\frac{1}{N}$
2(b)	1	$S_{r+1}[i_{r+2}] = 0$	$\frac{1}{N}$
3(a)	All but 0	$S_{r+2}[i_{r+3}] = 0$	$\frac{1}{N}$
3(b)	0	$S_{r+2}[i_{r+3}] = 0$	$\frac{1}{N}$
4(a)	All but $(N-3)$ or $(N-2)$	$S_{r+1}[i_{r+2}] = (N-1)$ and $j_{r+1} = i_{r+2}$	$\frac{1}{N^2}$
4(b)	$(N-3)$ or $(N-2)$	$S_{r+1}[i_{r+2}] = (N-1)$ and $j_{r+1} = i_{r+2}$	$\frac{1}{N^2}$
5(a)	All but $(N-4)$ or $(N-3)$	$S_{r+2}[i_{r+3}] = (N-1)$ and $j_{r+2} = i_{r+3}$	$\frac{1}{N^2}$
5(b)	$(N-4)$ or $(N-3)$	$S_{r+2}[i_{r+3}] = (N-1)$ and $j_{r+2} = i_{r+3}$	$\frac{1}{N^2}$

In each of these scenarios we now analyze the probability of the desired event $(z_r, z_{r+1}) = (z_{r+2}, z_{r+3})$. Since, $z_r = z_{r+1}$ as per the given condition, we get the pattern $AAAA$ in the key-stream under the desired event.

[**Scenario 1:**] This corresponds to the configuration that was originally used by Mantin in [1] to prove the $AB\mathcal{T}AB$ bias. These conditions lead to the outcome of $z_r = z_{r+2}$ and $z_{r+1} = z_{r+3}$ provided the location of the key-stream byte $z_r (= z_{r+1})$ remains undisturbed. As per Mantin's result (in [3], Lemma 2) this probability appears to be $e^{-\frac{8}{N}}$ (since $g = 2$ or $G = 0$). However, as pointed to by Bricout et al. in [1], for a pattern of the form $AAAA$, this probability would be higher. To ensure that the location of the key-stream byte $z_r (= z_{r+1})$ remains undisturbed, it should not coincide with any of the array byte locations indexed by (i_r, i_{r+1}, i_{r+2} and i_{r+3}) in round r, the probability of which is around $(1 - \frac{4}{N})$. This probability when multiplied with the probability of the condition ($\frac{1}{N^3}$) gives us the event probability. Hence, the probability associated with the desired event is $(1 - \frac{4}{N}) \cdot \frac{1}{N^3} = (\frac{1}{N^3} - \frac{4}{N^4})$.

[**Scenarios 2(a), 2(b):**] The probability of the condition associated with these scenarios is $\frac{1}{N}$. Based on Lemma 1, we know that $\Pr(z_{r+2} = z_{r+1} | S_{r+1}[i_{r+1} + 1] = 0, i_{r+1} \neq 1) = \frac{2}{N^2}$ and $\Pr(z_{r+2} = z_{r+1} | S_{r+1}[i_{r+1} + 1] = 0, i_{r+1} = 1) = \frac{3}{N^2}$. Subsequently, we consider $\Pr(z_{r+3} = z_{r+2}) = \frac{1}{N}$ under the fair chance assumption. Hence, for scenario 2(a), the probability of getting the desired outcome of $AAAA$ is $\frac{1}{N} \cdot \frac{2}{N^2} \cdot \frac{1}{N} = \frac{2}{N^4}$ and for scenario 2(b), the probability of getting the desired outcome of $AAAA$ is $\frac{1}{N} \cdot \frac{3}{N^2} \cdot \frac{1}{N} = \frac{3}{N^4}$.

[**Scenarios 3(a), 3(b):**] The probability of the condition associated with these scenarios is $\frac{1}{N}$. Based on Lemma 1, we know that $\Pr(z_{r+3} = z_{r+2}|S_{r+2}[i_{r+2}+1] = 0, i_{r+2} \neq 1) = \frac{2}{N^2}$ and $\Pr(z_{r+3} = z_{r+2}|S_{r+2}[i_{r+2}+1] = 0, i_{r+2} = 1) = \frac{3}{N^2}$. Subsequently, we consider $\Pr(z_{r+2} = z_{r+1}) = \frac{1}{N}$ under the fair chance assumption. Hence, for scenario 3(a), the probability of getting the desired outcome of $AAAA$ is $\frac{1}{N} \cdot \frac{2}{N^2} \cdot \frac{1}{N} = \frac{2}{N^4}$ and for scenario 3(b), the probability of getting the desired outcome of $AAAA$ is $\frac{1}{N} \cdot \frac{3}{N^2} \cdot \frac{1}{N} = \frac{3}{N^4}$.

[**Scenarios 4(a), 4(b):**] The probability of the condition associated with these scenarios is $\frac{1}{N^2}$. This configuration satisfies $z_{r+2} = z_{r+1}$ with a probability of $(1 - \frac{2}{N-1}) \approx (1 - \frac{2}{N})$ for $i_{r+1} \notin \{(N-3), (N-2)\}$ and with a probability of $(1 - \frac{1}{N-1}) \approx (1 - \frac{1}{N})$ for $i_{r+1} \in \{(N-3), (N-2)\}$ as per the analysis of Lemma 2. Now we need to investigate the probability of occurrence of $z_{r+3} = z_{r+2}$. Based on the condition of these scenarios, we can say that in round r, j_r must have been equal to $i_r + 3$. Let $S_r[i_r] = p$ and $S_r[j_r] = q$ where p and q are two arbitrary byte-values. In that case $z_r = S_r[p+q]$. The given configuration also implies that in round $(r+2)$, $j_{r+2} = i_{r+1}$ where $S_{r+2}[j_{r+2}] = (N-1)$. Therefore, in round $(r+3)$, it would not be possible to have $S_{r+3}[i_{r+3}] + S_{r+3}[j_{r+3}] = (p+q)$, instead it would become $(q+s)$ for some arbitrary byte value $s \neq p$ in position $S_{r+3}[j_{r+3}]$ before the swap operation or $S_{r+3}[i_{r+3}]$ after the swap operation. So $z_{r+3} = S_{r+3}[q+s]$. The only way for z_{r+3} to be equal to z_r is if the permutation array byte indexed by $(p+q)$ moves to the new position indexed by $(q+s)$ in round $r+3$. Using the argument similar to that used in Lemma 1 we get the probability of this occurrence as $\frac{2}{N^2}$. Hence, the probability of getting the desired outcome of $AAAA$ in scenario 4(a) is approximately $\frac{1}{N^2} \cdot (1 - \frac{2}{N}) \cdot \frac{2}{N^2} = \frac{2}{N^4} - \frac{4}{N^5}$.Similarly, the probability of getting the desired outcome of $AAAA$ in scenario 4(b) is approximately $\frac{1}{N^2} \cdot (1 - \frac{1}{N}) \cdot \frac{2}{N^2} = \frac{2}{N^4} - \frac{2}{N^5}$

[**Scenario 5(a), 5(b):**] The probability of the condition associated with each of these scenarios is $\frac{1}{N^2}$. This configuration satisfies $z_{r+3} = z_{r+2}$ with a probability of $(1 - \frac{2}{N-1}) \approx (1 - \frac{2}{N})$ for $i_{r+2} \notin \{(N-3), (N-2)\}$ and with a probability of $(1 - \frac{1}{N-1}) \approx (1 - \frac{1}{N})$ for $i_{r+2} \in \{(N-3), (N-2)\}$ as per the analysis of Lemma 2. Unlike scenario 4(a) or 4(b), there does not appear to be any constraint for the event $z_{r+1} = z_{r+2}$ and hence by considering a fair chance of $\frac{1}{N}$, we get the probability of getting the desired outcome of $AAAA$ for scenario 5(a) as $\frac{1}{N^3} - \frac{2}{N^4}$. Similarly, the probability of getting the desired outcome of $AAAA$ for scenario 5(b) is $\frac{1}{N^3} - \frac{1}{N^4}$

[**Scenario 6:**] We now consider the rest of the conditions (i.e., complimentary to all other scenarios from 1 to 5(b)). Clearly, the scenarios that are applicable to different values of i_{r+1} are as follows -

- For $i_{r+1} \notin \{0, 1, (N-4), (N-3), (N-2)\}$: 1, 2(a), 3(a), 4(a) and 5(a)
- For $i_{r+1} = 0$: 1, 2(a), 3(b), 4(a) and 5(a)
- For $i_{r+1} = 1$: 1, 2(b), 3(a), 4(a) and 5(a)
- For $i_{r+1} = (N-4)$: 1, 2(a), 3(a), 4(a) and 5(b)
- For $i_{r+1} = (N-3)$: 1, 2(a), 3(a), 4(b) and 5(b)
- For $i_{r+1} = (N-2)$: 1, 2(a), 3(a), 4(b) and 5(a)

Therefore, the probability associated with scenario 6 for any value of i_{r+1} is $(1 - \frac{2}{N} - \frac{2}{N^2} - \frac{1}{N^3})$. For each of these situations we consider that the desired configuration of $z_r = z_{r+2}$ and $z_{r+1} = z_{r+3}$ has the fair chance of $\frac{1}{N^2}$. By combining all the cases we get the result for the desired outcome as

1. $\Pr((z_r, z_{r+1}) = (z_{r+2}, z_{r+3}) | z_r = z_{r+1}, i_{r+1} \notin \{0, 1, (N-4), (N-3), (N-2)\}) \approx \frac{1}{N^2} - \frac{2}{N^4} - \frac{5}{N^5}$,
2. $\Pr((z_r, z_{r+1}) = (z_{r+2}, z_{r+3}) | z_r = z_{r+1}, i_{r+1} \in \{0, 1, (N-4)\}) \approx \frac{1}{N^2} - \frac{1}{N^4} - \frac{5}{N^5}$,
3. $\Pr((z_r, z_{r+1}) = (z_{r+2}, z_{r+3}) | z_r = z_{r+1}, i_{r+1} = (N-3)) \approx \frac{1}{N^2} - \frac{1}{N^4} - \frac{3}{N^5}$,
4. $\Pr((z_r, z_{r+1}) = (z_{r+2}, z_{r+3}) | z_r = z_{r+1}, i_{r+1} = (N-2)) \approx \frac{1}{N^2} - \frac{2}{N^4} - \frac{3}{N^5}$,

□

All these three probabilities are less than $\frac{1}{N^2}$, where $\frac{1}{N^2}$ corresponds to the uniform random case.

4 Reverse Digraph Repetition Bias

As a natural extension of Mantin's digraph repetition bias, we explore whether there exists any significant bias for the reverse digraph repetition of the form $AB\mathcal{T}BA$. To the best of our knowledge, this result has not been studied earlier. In this section, Theorem 4 proves that there is a persistent long-term significant negative bias for the reverse digraph repetition in case $\mathcal{T}$ is null corresponding to the key-stream pattern of $ABBA$. The magnitude of the bias is of the same order as Mantin's digraph repetition bias [3] corresponding to the pattern of $ABAB$. We have also verified the result experimentally for $N = 256$.

Theorem 4 *During RC4 PRGA, assuming that the RC4 state is in a random permutation in the r-th round,*

1. $\Pr((z_{r+2} = B) \wedge (z_{r+3} = A) | z_r = A, z_{r+1} = B, i_{r+1} \notin \{1, (N-3), (N-2)\}) = \frac{1}{N^2} - \frac{1}{N^3} + \frac{4}{N^4} - \frac{5}{N^5}$,
2. $\Pr((z_{r+2} = B) \wedge (z_{r+3} = A) | z_r = A, z_{r+1} = B, i_{r+1} = 1) = \frac{1}{N^2} - \frac{1}{N^3} + \frac{5}{N^4} - \frac{5}{N^5}$,
3. $\Pr((z_{r+2} = B) \wedge (z_{r+3} = A) | z_r = A, z_{r+1} = B, i_{r+1} \in \{(N-3), (N-2)\}) = \frac{1}{N^2} - \frac{1}{N^3} + \frac{4}{N^4} - \frac{3}{N^5}$.

Proof To prove this result, we use the same approach as that of Theorem 3. Hence, we first analyze the following scenarios. Since the desired event is centered around four rounds (r, $r+1$, $r+2$ and $r+3$) where the probability of a pattern for key-stream bytes in the third and fourth rounds are analyzed based on a given pattern for the key-stream bytes in the first two rounds, the scenarios are expressed with respect to i_{r+1}.

In each of these scenarios we now analyze the probability of the desired event $(z_r, z_{r+1}) = (z_{r+3}, z_{r+2})$. in which we get the pattern $ABBA$ in the key-stream. It is important to note that the configuration that was originally used by Mantin in [1] to prove the $AB\mathcal{T}AB$ bias cannot be utilized here and hence we don't observe any positive bias in general for reverse digraph repetition scenario of the form $AB\mathcal{T}BA$. The reason for the presence of negative bias when $\mathcal{T}$ is null, becomes evident after analyzing the following scenarios.

[**Scenarios 1(a), 1(b):**] The probability of the condition associated with these

Scenario	i_{r+1}	Conditions	Probability
1(a)	All but 1	$S_{r+1}[i_{r+2}] = 0$	$\frac{1}{N}$
1(b)	1	$S_{r+1}[i_{r+2}] = 0$	$\frac{1}{N}$
2(a)	All but $(N-3)$ or $(N-2)$	$S_{r+1}[i_{r+2}] = (N-1)$ and $j_{r+1} = i_{r+2}$	$\frac{1}{N^2}$
2(b)	$(N-3)$ or $(N-2)$	$S_{r+1}[i_{r+2}] = (N-1)$ and $j_{r+1} = i_{r+2}$	$\frac{1}{N^2}$
3	All	$S_{r+1}[i_{r+1}] = (\frac{N}{2}+1)$, $S_{r+1}[i_{r+2}] = 1$ and $j_{r+1} = i_{r+1}$	$\frac{1}{N^3}$

scenarios is $\frac{1}{N}$. Based on Lemma 1, we know that $\Pr(z_{r+2} = z_{r+1} | S_{r+1}[i_{r+1}+1] = 0, i_{r+1} \neq 1) = \frac{2}{N^2}$ and $\Pr(z_{r+2} = z_{r+1} | S_{r+1}[i_{r+1}+1] = 0, i_{r+1} = 1) = \frac{3}{N^2}$. Subsequently, we consider $\Pr(z_{r+3} = z_r) = \frac{1}{N}$ under the fair chance assumption. Hence, for scenario 1(a), the probability of getting the desired outcome of $ABBA$ is $\frac{1}{N} \cdot \frac{2}{N^2} \cdot \frac{1}{N} = \frac{2}{N^4}$ and for scenario 1(b), the probability of getting the desired outcome is $\frac{1}{N} \cdot \frac{3}{N^2} \cdot \frac{1}{N} = \frac{3}{N^4}$.

[**Scenarios 2(a), 2(b):**] The probability of the condition associated with these scenarios is $\frac{1}{N^2}$. This configuration satisfies $z_{r+2} = z_{r+1}$ with a probability of $(1 - \frac{2}{N-1}) \approx (1 - \frac{2}{N})$ for $i_{r+1} \notin \{(N-3), (N-2)\}$ and with a probability of $(1 - \frac{1}{N-1}) \approx (1 - \frac{1}{N})$ for $i_{r+1} \in \{(N-3), (N-2)\}$ as per the analysis of Lemma 2. Now we need to investigate the probability of occurrence of $z_{r+3} = z_r$. Based on the condition of these scenarios, we can say that in round r, j_r must have been equal to $i_r + 3$. Let $S_r[i_r] = p$ and $S_r[j_r] = q$ where p and q are two arbitrary byte-values. In that case $z_r = S_r[p+q]$. The given configuration also implies that in round $(r+2)$, $j_{r+2} = i_{r+1}$ where $S_{r+2}[j_{r+2}] = (N-1)$. Therefore, in round $(r+3)$, it would not be possible to have $S_{r+3}[i_{r+3}] + S_{r+3}[j_{r+3}] = (p+q)$, instead it would become $(q+s)$ for some arbitrary byte value $s \neq p$ in position $S_{r+3}[j_{r+3}]$ before the swap operation or $S_{r+3}[i_{r+3}]$ after the swap operation. So $z_{r+3} = S_{r+3}[q+s]$. The only way for z_{r+3} to be equal to z_r is if the permutation array byte indexed by $(p+q)$ moves to the new position indexed by $(q+s)$ in round $r+3$. Using the argument similar to that used in Lemma 1 we get the probability of this occurrence as $\frac{2}{N^2}$. Hence, the probability of getting the desired outcome of $ABBA$ in scenario 2(a) is approximately $\frac{1}{N^2} \cdot (1 - \frac{2}{N}) \cdot \frac{2}{N^2} = \frac{2}{N^4} - \frac{4}{N^5}$.Similarly, the probability of getting the desired outcome of $ABBA$ in scenario 2(b) is approximately $\frac{1}{N^2} \cdot (1 - \frac{1}{N}) \cdot \frac{2}{N^2} = \frac{2}{N^4} - \frac{2}{N^5}$.

[**Scenario 3:**] The probability of the condition associated with this scenario is $\frac{1}{N^3}$. In this scenario $z_{r+1} = S_{r+1}[2]$ and $z_{r+2} = S_{r+2}[2]$. Since no array byte changes position in the two rounds ($r+1$ and $r+2$), we get $z_{r+1} = z_{r+2}$. Subsequently, we consider $\Pr(z_{r+3} = z_r) = \frac{1}{N}$ under the fair chance assumption. Hence, for scenario 3, the probability of getting the desired outcome of $ABBA$ is $\frac{1}{N^3} \cdot \frac{1}{N} = \frac{1}{N^4}$.

[**Scenario 4:**] We now consider the rest of the conditions (i.e., complimentary to all other scenarios from 1 to 3). Clearly, the scenarios that are applicable to different values of i_{r+1} are as follows.

- For $i_{r+1} \notin \{1, (N-3), (N-2)\}$: 1(a), 2(a) and 3
- For $i_{r+1} = 1$: 1(b), 2(a) and 3
- For $i_{r+1} = (N-3)$ or $i_{r+1} = (N-2)$: 1(a), 2(b) and 3

Therefore, the probability associated with scenario 4 for any value of i_{r+1} is $(1 - \frac{1}{N} - \frac{1}{N^2} - \frac{1}{N^3})$. For each of these situations we consider that the desired configuration of $z_r = z_{r+3}$ and $z_{r+1} = z_{r+2}$ has the fair chance of $\frac{1}{N^2}$. By combining all the cases we get the result for the desired outcome as

1. $\Pr((z_{r+2} = B) \wedge (z_{r+3} = A) | z_r = A, z_{r+1} = B, i_{r+1} \notin \{1, (N-3), (N-2)\}) = \frac{1}{N^2} - \frac{1}{N^3} + \frac{4}{N^4} - \frac{5}{N^5}$,
2. $\Pr((z_{r+2} = B) \wedge (z_{r+3} = A) | z_r = A, z_{r+1} = B, i_{r+1} = 1) = \frac{1}{N^2} - \frac{1}{N^3} + \frac{5}{N^4} - \frac{5}{N^5}$,
3. $\Pr((z_{r+2} = B) \wedge (z_{r+3} = A) | z_r = A, z_{r+1} = B, i_{r+1} \in \{(N-3), (N-2)\}) = \frac{1}{N^2} - \frac{1}{N^3} + \frac{4}{N^4} - \frac{3}{N^5}$.

□

However, we could not observe such significant bias for $AB\mathcal{T}BA$, when $\mathcal{T}$ is non-null. Thus, we did not proceed with the proof of that.

5 Conclusion

In this paper, we solve an open question that is related to Mantin's bias [3] in RC4 key-stream. This bias is till date the most significant long term one to distinguish RC4 key-stream from uniform random distribution. However, this is mostly a generic result with a few logical assumptions. Unfortunately, in a very few cases, the assumptions are not correct and such issues have been studied in great detail in [1]. The theoretical analysis could be formalized in [1], except one experimental observation, that could not be supported by theoretical argument. This is related to $\Pr((z_r, z_{r+1}) = (z_{r+2}, z_{r+3}) | z_r = z_{r+1})$, that is for the sub-string of the form $AAAA$. While the analysis of [1] could only point out to a positive bias, the experiments show that it is actually slightly negative in such a case. Here we prove this result with proper theoretical justification. Further, as a natural extension, we study the "Reverse Digraph Repetition Bias" and show that there is significant negative bias of $ABBA$ (A, B distinct) in RC4 key-stream. Thus, considering the four consecutive byte patterns with some symmetry in RC4, we now have the following summary.

- Arrival of $ABAB$ is significantly positively biased [3].
- Arrival of $AAAA$ is slightly negatively biased (not completely studied in [3], analysed more carefully in [1] but the cause could not be identified, finally solved in this paper).
- Arrival of $ABBA$ is significantly negative biased (explored and solved in this paper).

References

1. R. Bricout, S. Murphy, K. G. Paterson, T. van der Merwe. Analysing and exploiting the Mantin biases in RC4. Designs Codes and Cryptography, 86:743-770, 2018.
2. H. Finney. An RC4 cycle that can't happen. Post in sci.crypt, September 1994.
3. I. Mantin. Predicting and Distinguishing Attacks on RC4 Keystream Generator. EUROCRYPT 2005, pages 491506, vol. 3494, Lecture Notes in Computer Science, Springer.
4. K. G. Paterson, B. Poettering and J. C. N. Schuldt. Big Bias Hunting in Amazonia: Large-scale Computation and Exploitation of RC4 Biases. ASIACRYPT 2014. LNCS, Part 1, pp. 398–419, Vol. 8873, 2014.

5. S. SenGupta, S. Maitra, G. Paul, S. Sarkar. (Non–)Random Sequences from (Non–)Random Permutations – Analysis of RC4 stream cipher. Journal of Cryptology, 27(1):67–108, 2014
6. P. Sepehrdad, S. Vaudenay, and M. Vuagnoux. Statistical Attack on RC4 - Distinguishing WPA. EUROCRYPT 2011. LNCS pp. 343–363, Vol. 6632, 2011.