On Non-Randomness of the Permutation after RC4 Key Scheduling

Goutam Paul[1], Subhamoy Maitra[2], Rohit Srivastava[3]

[1] Department of Computer Science and Engineering, Jadavpur University,
Kolkata 700 032, India.
goutam_paul@cse.jdvu.ac.in

[2] Applied Statistics Unit, Indian Statistical Institute,
203, B T Road, Kolkata 700 108, India.
subho@isical.ac.in

[3] Department of Computer Science and Engineering, Institute of Technology,
Banaras Hindu University, Varanasi 221 005 (UP), India.
rohit.engg@gmail.com

Abstract. Here we study a weakness of the RC4 Key Scheduling Algorithm (KSA) that has already been noted by Mantin and Mironov. Consider the RC4 permutation S of N (usually 256) bytes and denote it by S_N after the KSA. Under reasonable assumptions we present a simple proof that each permutation byte after the KSA is significantly biased (either positive or negative) towards many values in the range $0, \ldots, N-1$. These biases are independent of the secret key and thus present an evidence that the permutation after the KSA can be distinguished from random permutation without any assumption on the secret key. We also present a detailed empirical study over Mantin's work when the theoretical formulae vary significantly from experimental results due to repetition of short keys in RC4. Further, it is explained how these results can be used to identify new distinguishers for RC4 keystream.

Keywords: Bias, Cryptography, Cryptanalysis, Key Scheduling Algorithm, RC4, Stream Cipher.

1 Introduction

RC4, one of the most popular stream ciphers till date, was proposed by Rivest in 1987. The cipher gained its popularity from its extremely simple structure and substantially good strength in security, as even after lots of explored weaknesses in the literature (see [1–7, 9–14] and the references in these papers), it could not be thoroughly cracked. Studying weaknesses of RC4 received serious attention in the literature and these studies are believed to be quite useful in further development of stream ciphers that exploit shuffle-exchange paradigm.

Before getting into our contribution, let us briefly present the Key Scheduling Algorithm (KSA) and the Pseudo Random Generation Algorithm (PRGA) of RC4. The data structure consists of (1) an array of size N (in practice 256 which is followed in this paper) which contains a permutation of $0, \dots, N-1$, (2) two indices i, j and (3) the secret key array K. Given a secret key k of l bytes (typically 5 to 32), the array K of size N is such that $K[i] = k[i \bmod l]$ for any i, $0 \le i \le N-1$. All additions used in the description of the algorithm are modulo N additions.

```
Algorithm KSA
Initialization:
    For $i = 0, \dots, N-1$
        $S[i] = i$;
    $j = 0$;
Scrambling:
    For $i = 0, \dots, N-1$
        $j = (j + S[i] + K[i])$;
        Swap($S[i], S[j]$);
```

```
Algorithm PRGA
Initialization:
    $i = j = 0$;
Output Keystream Generation Loop:
        $i = i + 1$;
        $j = j + S[i]$;
        Swap($S[i]$, $S[j]$);
        $t = S[i] + S[j]$;
        Output $z = S[t]$;
```

RC4 KSA has been analysed deeply in [13, 14, 2, 11]. All these works discuss the relationship of the permutation bytes after the KSA with the secret key. For a proper design, the permutation S after the KSA should not have any correlation with the secret keys. However, weaknesses of RC4 in this aspect have already been reported [13, 14, 2, 11]. These weaknesses, in turn, leak information about RC4 secret key in the initial keystream output bytes [10].

Another approach of study is to look at the permutation after the KSA in a (secret) key independent manner and try to distinguish it from random permutations. In [9], the sign of the permutation after the KSA has been studied (see [9] for the definition of the sign of a permutation). There it has been shown that, after the KSA, the sign of the permutation can be guessed with probability 56%.

In [8, Chapter 6 and Appendix C] and later in [9], the problem of estimating $P(S_N[u] = v)$ has been discussed. A complete proof for these results has been presented in [8, Chapter 6 and Appendix C]. We present an independent proof technique in this paper which looks simpler. We argue in more detail in Section 2 how our technique is different from that in [8]. Due to the small keys (say 5 to 32 bytes) generally used in RC4, some of the assumptions differ from practice and hence the theoretical formulae do not match with the experimental results. We also detail this over the already identified anomalies in [8]. Further, we discuss applications to show how these results can be used to present new distinguishers for RC4. The distinguishers discussed in this paper are different from the earlier ones [1, 3, 5, 7, 12].

2 Bias in Each Permutation Byte

We denote the initial identity permutation by S_0 and the permutation at the end of the r-th round of the KSA by S_r, $1 \le r \le N$ (note that $r = i + 1$, for the deterministic index i, $0 \le i \le N-1$). Thus, the permutation after the KSA will be denoted by S_N. By j_r, we denote the value of the index j after it is updated in round r. We consider the index j of each round to be distributed uniformly at random. Further, we replace the joint probabilities with the product of the probabilities of the individual events, assuming that the events under consideration are statistically independent.

Lemma 1. $P(S_2[0] = 1) = \frac{2(N-1)}{N^2}$.

Proof. In the first round, we have $i = 0$, and $j_1 = 0 + S[0] + K[0] = K[0]$. In the second round, $i = 1$ and $j_2 = j_1 + S_1[1] + K[1]$. We consider two mutually exclusive and exhaustive cases, namely, $K[0] = 1$ and $K[0] \neq 1$.

1. Take $K[0] = 1$. So, after the first swap, $S_1[0] = 1$ and $S_1[1] = 0$. Now, $j_2 = K[0] + 0 + K[1] = K[0] + K[1]$. Thus, after the second swap, $S_2[0]$ will remain 1, if $K[0] + K[1] \neq 0$. Hence the contribution of this case to the event $(S_2[0] = 1)$ is $P(K[0] = 1) \cdot P(K[0] + K[1] \neq 0) = \frac{1}{N} \cdot \frac{N-1}{N} = \frac{N-1}{N^2}$.
2. Take $K[0] \neq 1$. Then after the first swap, $S_1[1]$ remains 1. Now, $j_2 = K[0] + 1 + K[1] = K[0] + K[1] + 1$. Thus, after the second swap, $S_2[0]$ will get the value 1, if $K[0] + K[1] + 1 = 0$. Hence the contribution of this case to the event $(S_2[0] = 1)$ is $P(K[0] \neq 1) \cdot P(K[0] + K[1] + 1 = 0) = \frac{N-1}{N} \cdot \frac{1}{N} = \frac{N-1}{N^2}$.

Adding the two contributions, we get the total probability as $\frac{2(N-1)}{N^2}$. □

We here calculate $P(S_{v+1}[u] = v)$ for the special case $u = 0$, $v = 1$. Note that the form of $P(S_{v+1}[u] = v)$ for $v \geq u + 1$ in general (see Lemma 2 later) does not work for the case $u = 0, v = 1$ only. This will be made clear in Remark 1 after the proof of Lemma 2.

Proposition 1. $P(S_v[v] = v) = (\frac{N-1}{N})^v$, *for* $v \geq 0$.

Proof. In the rounds 1 through v, the deterministic index i touches the permutation indices $0, 1, \ldots, v-1$. Thus, after round v, $S_v[v]$ will remain the same as $S_0[v] = v$, if v has not been equal to any of the v many pseudo-random indices $j_1, j_2, \ldots, j_v$. The probability of this event is $(\frac{N-1}{N})^v$. So the result holds for $v \geq 1$. Furthermore, $P(S_0[0] = 0) = 1 = (\frac{N-1}{N})^0$. Hence, for any $v \geq 0$, we have $P(S_v[v] = v) = (\frac{N-1}{N})^v$. □

Proposition 2. *For* $v \geq u + 1$, $P(S_v[u] = v) = \frac{1}{N} \cdot (\frac{N-1}{N})^{v-u-1}$.

Proof. In round $u + 1$, the permutation index u is touched by the deterministic index i for the first time and the value at index u is swapped with the value at a random location based on j_{u+1}. Hence, $P(S_{u+1}[u] = v) = \frac{1}{N}$. The probability that the index u is not touched by any of the subsequent $v - u - 1$ many j values, namely, $j_{u+2}, \ldots, j_v$, is given by $(\frac{N-1}{N})^{v-u-1}$. So, after the end of round v, $P(S_v[u] = v) = \frac{1}{N} \cdot (\frac{N-1}{N})^{v-u-1}$. □

Lemma 2. *For* $v \geq u+1$ (except for the case "$u = 0$ and $v = 1$"), $P(S_{v+1}[u] = v) = \frac{1}{N} \cdot (\frac{N-1}{N})^{v-u} + \frac{1}{N} \cdot (\frac{N-1}{N})^v - \frac{1}{N^2} \cdot (\frac{N-1}{N})^{2v-u-1}$.

Proof. In round $v+1$, $i = v$ and $j_{v+1} = j_v + S_v[v] + K[v]$. The event $(S_{v+1}[u] = v)$ can occur in two ways.

1. $S_v[u]$ already had the value v and the index u is not involved in the swap in round $v+1$.
2. $S_v[u] \neq v$ and the value v comes into the index u from the index v (i.e., $S_v[v] = v$) by the swap in round $v+1$.

From Proposition 1, we have $P(S_v[v] = v) = (\frac{N-1}{N})^v$ and from Proposition 2, we have $P(S_v[u] = v) = \frac{1}{N} \cdot (\frac{N-1}{N})^{v-u-1}$. Hence, $P(S_{v+1}[u] = v)$
$= P(S_v[u] = v) \cdot P(j_v + S_v[v] + K[v] \neq u)$
$\quad + P(S_v[u] \neq v) \cdot P(S_v[v] = v) \cdot P(j_v + S_v[v] + K[v] = u)$
(except for the case "$u = 0$ and $v = 1$", see Remark 1)
$= \left(\frac{1}{N} \cdot (\frac{N-1}{N})^{v-u-1}\right) \cdot (\frac{N-1}{N}) + \left(1 - \frac{1}{N} \cdot (\frac{N-1}{N})^{v-u-1}\right) \cdot (\frac{N-1}{N})^v \cdot \frac{1}{N}$
$= \frac{1}{N} \cdot (\frac{N-1}{N})^{v-u} + \frac{1}{N} \cdot (\frac{N-1}{N})^v - \frac{1}{N^2} \cdot (\frac{N-1}{N})^{2v-u-1}$. □

Remark 1. Case 1 in the proof of Lemma 2 applies to Lemma 1 also. In case 2, i.e., when $S_v[u] \neq v$, in general we may or may not have $S_v[v] = v$. However, for $u = 0$ and $v = 1$, $(S_1[0] \neq 1) \iff (S_1[1] = 1)$, the probability of each of which is $\frac{N-1}{N}$ (note that there has been only one swap involving the indices 0 and $K[0]$ in round 1). Hence the contribution of case 2 except for "$u = 0$ and $v = 1$" would be $P(S_v[u] \neq v) \cdot P(S_v[v] = v) \cdot P(j_v + S_v[v] + K[v] = u)$, and for "$u = 0$ and $v = 1$" it would be $P(S_1[0] \neq 1) \cdot P(j_1 + S_1[1] + K[1] = 0)$ or, equivalently, $P(S_1[1] = 1) \cdot P(j_1 + S_1[1] + K[1] = 0)$.

Lemma 3. *Let $p_r^{u,v} = P(S_r[u] = v)$, for $1 \leq r \leq N$. Given $p_t^{u,v}$, i.e., $P(S_t[u] = v)$ for any intermediate round t, $max\{u, v\} < t \leq N$, $P(S_r[u] = v)$ after the r-th round of the KSA is given by*
$p_t^{u,v} \cdot (\frac{N-1}{N})^{r-t} + (1 - p_t^{u,v}) \cdot \frac{1}{N}(\frac{N-1}{N})^v \cdot \left(1 - (\frac{N-1}{N})^{r-t}\right)$, $t \leq r \leq N$.

Proof. After round t ($> max\{u, v\}$), there may be two different cases: $S_t[u] = v$ and $S_t[u] \neq v$. Both of these can contribute to the event $(S_r[u] = v)$ in the following ways.

1. $S_t[u] = v$ and the index u is not touched by any of the subsequent $r - t$ many j values. The contribution of this part is $P(S_t[u] = v) \cdot (\frac{N-1}{N})^{r-t}$ $= p_t^{u,v} \cdot (\frac{N-1}{N})^{r-t}$.
2. $S_t[u] \neq v$ and for some x in the interval $[t, r-1]$, $S_x[x] = v$ which comes into the index u from the index x by the swap in round $x+1$, and after that the index u is not touched by any of the subsequent $r - 1 - x$ many j values. So the contribution of the second part is given by
$$P(S_t[u] \neq v) \cdot \left(\sum_{x=t}^{r-1} P(S_x[x] = v) \cdot P(j_{x+1} = u) \cdot (\frac{N-1}{N})^{r-1-x}\right).$$

Suppose, the value v remains in location v after round v. By Proposition 1, this probability, i.e., $P(S_v[v] = v)$, is $(\frac{N-1}{N})^v$. The swap in the next round moves the value v to a random location $x = j_{v+1}$. Thus, $P(S_{v+1}[x] = v) = P(S_v[v] = v) \cdot P(j_{v+1} = x) = (\frac{N-1}{N})^v \cdot \frac{1}{N}$. For all $x > v$, until x is touched by the deterministic index i, i.e., until round $x+1$, v will remain randomly distributed. Hence, for all $x > v$, $P(S_x[x] = v) = P(S_{v+1}[x] = v) = \frac{1}{N}(\frac{N-1}{N})^v$ and

$$P(S_t[u] \neq v) \cdot \Big(\sum_{x=t}^{r-1} P(S_x[x] = v) \cdot P(j_{x+1} = u) \cdot (\tfrac{N-1}{N})^{r-1-x}\Big)$$

$$= (1 - p_t^{u,v}) \cdot \Big(\sum_{x=t}^{r-1} \tfrac{1}{N}(\tfrac{N-1}{N})^v \cdot \tfrac{1}{N} \cdot (\tfrac{N-1}{N})^{r-1-x}\Big)$$

$$= (1 - p_t^{u,v}) \cdot \tfrac{1}{N^2}(\tfrac{N-1}{N})^v \cdot \Big(\sum_{x=t}^{r-1} (\tfrac{N-1}{N})^{r-1-x}\Big) = (1 - p_t^{u,v}) \cdot \tfrac{1}{N^2}(\tfrac{N-1}{N})^v \cdot \Big(\tfrac{1-a^{r-t}}{1-a}\Big),$$

where $a = \frac{N-1}{N}$. Substituting the value of a and simplifying, we get the above probability as $(1 - p_t^{u,v}) \cdot \frac{1}{N}(\frac{N-1}{N})^v \cdot \Big(1 - (\frac{N-1}{N})^{r-t}\Big)$.

Now, combining the above two contributions, we get

$$p_r^{u,v} = p_t^{u,v} \cdot (\tfrac{N-1}{N})^{r-t} + (1 - p_t^{u,v}) \cdot \tfrac{1}{N}(\tfrac{N-1}{N})^v \cdot \Big(1 - (\tfrac{N-1}{N})^{r-t}\Big). \qquad \square$$

Corollary 1. *Given $p_t^{u,v}$, i.e., $P(S_t[u] = v)$ for any intermediate round t, $max\{u, v\} < t \leq N$, $P(S_N[u] = v)$ after the complete KSA is given by*

$$p_t^{u,v} \cdot (\tfrac{N-1}{N})^{N-t} + (1 - p_t^{u,v}) \cdot \tfrac{1}{N}(\tfrac{N-1}{N})^v \cdot \Big(1 - (\tfrac{N-1}{N})^{N-t}\Big).$$

Proof. Substitute $r = N$ in Lemma 3. □

Theorem 1.

(1) *For $0 \leq u \leq N-2$, $u+1 \leq v \leq N-1$,*

$$P(S_N[u] = v) = p_{v+1}^{u,v} \cdot (\tfrac{N-1}{N})^{N-1-v} + (1 - p_{v+1}^{u,v}) \cdot \tfrac{1}{N} \cdot \Big((\tfrac{N-1}{N})^v - (\tfrac{N-1}{N})^{N-1}\Big), \textit{ where}$$

$$p_{v+1}^{u,v} = \begin{cases} \frac{2(N-1)}{N^2} & \textit{if } u = 0 \textit{ and } v = 1; \\ \frac{1}{N} \cdot (\frac{N-1}{N})^{v-u} + \frac{1}{N} \cdot (\frac{N-1}{N})^v - \frac{1}{N^2} \cdot (\frac{N-1}{N})^{2v-u-1} & \textit{otherwise.} \end{cases}$$

(2) *For $0 \leq v \leq N-1$, $v \leq u \leq N-1$,*

$$P(S_N[u] = v) = \tfrac{1}{N} \cdot (\tfrac{N-1}{N})^{N-1-u} + \tfrac{1}{N} \cdot (\tfrac{N-1}{N})^{v+1} - \tfrac{1}{N} \cdot (\tfrac{N-1}{N})^{N+v-u}.$$

Proof. First we prove item (1). Since $v > u$, so for any $t > v$, we will have $t > max\{u, v\}$. Substituting $t = v+1$ in Corollary 1, we have

$$P(S_N[u] = v) = p_{v+1}^{u,v} \cdot (\tfrac{N-1}{N})^{N-1-v} + (1 - p_{v+1}^{u,v}) \cdot \tfrac{1}{N}(\tfrac{N-1}{N})^v \cdot \Big(1 - (\tfrac{N-1}{N})^{N-1-v}\Big)$$

$= p_{v+1}^{u,v} \cdot (\frac{N-1}{N})^{N-1-v} + (1 - p_{v+1}^{u,v}) \cdot \frac{1}{N} \cdot \Big((\frac{N-1}{N})^v - (\frac{N-1}{N})^{N-1}\Big)$. Now, from Lemma 2, we get $p_{v+1}^{u,v} = \frac{1}{N} \cdot (\frac{N-1}{N})^{v-u} + \frac{1}{N} \cdot (\frac{N-1}{N})^v - \frac{1}{N^2} \cdot (\frac{N-1}{N})^{2v-u-1}$, except for "$u = 0$ and $v = 1$". Also, Lemma 1 gives $p_2^{0,1} = \frac{2(N-1)}{N^2}$. Substituting these values of $p_{v+1}^{u,v}$, we get the result.

Now we prove item (2). Here we have $u \geq v$. So for any $t > u$, we will have $t > max\{u, v\}$. Substituting $t = u+1$ in Corollary 1, we have

$$P(S_N[u] = v) = p_{u+1}^{u,v} \cdot (\tfrac{N-1}{N})^{N-1-u} + (1 - p_{u+1}^{u,v}) \cdot \tfrac{1}{N}(\tfrac{N-1}{N})^v \cdot \Big(1 - (\tfrac{N-1}{N})^{N-1-u}\Big).$$

As $p_{u+1}^{u,v} = P(S_{u+1}[u] = v) = \frac{1}{N}$ (see proof of Proposition 2), substituting this in the above expression, we get

$$P(S_N[u] = v) = \tfrac{1}{N} \cdot (\tfrac{N-1}{N})^{N-1-u} + (1 - \tfrac{1}{N}) \cdot \tfrac{1}{N}(\tfrac{N-1}{N})^{v} \cdot \Big(1 - (\tfrac{N-1}{N})^{N-1-u}\Big)$$
$$= \tfrac{1}{N} \cdot (\tfrac{N-1}{N})^{N-1-u} + \tfrac{1}{N} \cdot (\tfrac{N-1}{N})^{v+1} - \tfrac{1}{N} \cdot (\tfrac{N-1}{N})^{N+v-u}. \qquad \square$$

We like to mention that our final formulae in Theorem 1 are very close to the results presented in [8] apart from some minor differences as terms with N^2 in the denominator or a difference in 1 in the power. These differences are negligible and we have also checked by calculating the numerical values of the theoretical results that for $N = 256$, the maximum absolute difference between our results and the results of [8] is 0.000025 as well as the average of absolute differences is 0.000005.

However, our approach is different from that of [8]. In [8], the idea of relative positions is introduced. If the current deterministic index is i, then relative position a means the position $(i + 1 + a) \bmod N$. The transfer function $T(a, b, r)$, which represents the probability that value in relative position a in S will reach relative position b in the permutation generated from S by executing r RC4 rounds, has the following explicit form by [8, Claim C.3.3]: $T(a, b, r) = p(q^a + q^{r-(b+1)} - q^{a+r-(b+1)})$ if $a \le b$ and $T(a, b, r) = p(q^a + q^{r-(b+1)})$ if $a > b$, where $p = \frac{1}{N}$ and $q = (\frac{N-1}{N})$. This solution is obtained by solving a recurrence [8, Equation C.3.1] which expresses $T(a, b, r)$ in terms of $T(a-1, b-1, r-1)$. Instead, we use the probabilities $P(S_t[u] = v)$ in order to calculate the probabilities $P(S_r[u] = v)$ which immediately gives $P(S_N[u] = v)$ with $r = N$. When $v > u$, we take $t = v + 1$ and when $v \le u$, we take $t = u + 1$ (see Theorem 1). However, the values $u + 1$ and $v + 1$ are not special. If we happen to know the probabilities $P(S_t[u] = v)$ at any round t between $max\{u, v\} + 1$ and N, then we can arrive at the probabilities $P(S_r[u] = v)$ using Lemma 3. The recurrence relation in [8] is over three variables a, b and r, and at each step each of these three variables is reduced by one. On the other hand, our model has the following features.

1. It relates four variables u, v, t and r which respectively denote any index u in the permutation (analogous to b), any value $v \in [0, \ldots N-1]$ (analogous to the value at a), any round $t > max\{u, v\}$ and a particular round $r \ge t$.
2. Though in our formulation we do not solve any recurrence relation and provide a direct proof, it can be considered analogous to a recurrence over a single variable r, the other two variables u and v remaining fixed.

3 Anomaly Pairs and New Distinguishers

To evaluate how closely our theoretical formulae tally with the experimental results, we use average percentage absolute error $\bar{\epsilon}$. Let $p_N^{u,v}$ and $q_N^{u,v}$ respectively denote the theoretical and the experimental value of the probability $P(S_N[u] = v)$, $0 \le u \le N-1$, $0 \le v \le N-1$. We define $\epsilon_{u,v} = \Big(\frac{|p_N^{u,v} - q_N^{u,v}|}{q_N^{u,v}}\Big) \cdot 100\%$ and $\bar{\epsilon} = \frac{1}{N^2} \sum\limits_{u=0}^{N-1} \sum\limits_{v=0}^{N-1} \epsilon_{u,v}$. We ran experiments for 100 million randomly chosen secret keys of 32 bytes and found that $\bar{\epsilon} = 0.22\%$. The maximum of the $\epsilon_{u,v}$'s was 35.37% and it occured for $u = 128$ and $v = 127$. Though the maximum error is quite high, we find that out of $N^2 = 65536$ (with $N = 256$) many $\epsilon_{u,v}$'s, only 11 ($< 0.02\%$ of 65536) exceeded the 5% error margin. These cases are summarized Table 1 below. We call the pairs (u, v) for which $\epsilon_{u,v} > 5\%$ as *anomaly pairs.*

u	v	$p_N^{u,v}$	$q_N^{u,v}$	$p_N^{u,v} - q_N^{u,v}$	$\epsilon_{u,v}$ (in %)
38	6	0.003846	0.003409	0.000437	12.82
38	31	0.003643	0.003067	0.000576	18.78
46	31	0.003649	0.003408	0.000241	7.07
47	15	0.003774	0.003991	0.000217	5.44
48	16	0.003767	0.003974	0.000207	5.21
66	2	0.003882	0.003372	0.000510	15.12
66	63	0.003454	0.002797	0.000657	23.49
70	63	0.003460	0.003237	0.000223	6.89
128	0	0.003900	0.003452	0.000448	12.98
128	127	0.003303	0.002440	0.000863	35.37
130	127	0.003311	0.003022	0.000289	9.56

Table 1. The anomaly pairs for key length 32 bytes.

The experimental values of $P(S_N[u] = v)$ match with the theoretical values given by our formula except at these few anomaly pairs. For example, $q_N^{38,v}$ follows the pattern predicted by $p_N^{38,v}$ for all v's, $0 \leq v \leq 255$ except at $v = 6$ and $v = 31$ as pointed out in Table 1.

l	$\bar{\epsilon}$ (in %)	ϵ_{max} (in %)	u_{max}	v_{max}	n_5	n_{10}	n_5 (in %)	n_{10} (in %)
5	0.75	73.67	9	254	1160	763	1.770	1.164
8	0.48	42.48	15	255	548	388	0.836	0.592
12	0.30	21.09	23	183	293	198	0.447	0.302
15	0.25	11.34	44	237	241	2	0.368	0.003
16	0.24	35.15	128	127	161	7	0.246	0.011
20	0.20	5.99	30	249	3	0	0.005	0.000
24	0.19	4.91	32	247	0	0	0.000	0.000
30	0.19	6.54	45	29	1	0	0.002	0.000
32	0.22	35.37	128	127	11	6	0.017	0.009
48	0.18	4.24	194	191	0	0	0.000	0.000
64	0.26	35.26	128	127	6	4	0.009	0.006
96	0.21	4.52	194	191	0	0	0.000	0.000
128	0.34	37.00	128	127	3	2	0.005	0.003
256	0.46	2.58	15	104	0	0	0.000	0.000

Table 2. The number and percentage of anomaly pairs along with the average and maximum error for different key lengths.

We experimented with different key lengths (100 million random keys for each key length) and found that the location of the anomaly pairs and the total number of anomaly pairs vary with the key lengths in certain cases. Table 2 shows the number n_5 of anomaly pairs (when $\epsilon_{u,v} > 5\%$) for different key lengths l (in bytes) along with the average $\bar{\epsilon}$ and the maximum ϵ_{max} of the $\epsilon_{u,v}$'s. u_{max} and v_{max} are the (u, v) values which correspond to ϵ_{max}. Though for some key lengths there are more than a hundred anomaly pairs, most of them have $\epsilon_{u,v} \leq$ 10%. To illustrate this, we add the column n_{10} which shows how many of the anomaly pairs exceed the 10% error margin. The two rightmost columns show what percentage of $256^2 = 65536$ (total number of (u, v) pairs) are the numbers n_5 and n_{10}.

These results indicate that as the key length increases, the proportion of anomaly pairs tends to decrease. With 256 bytes key, we have no anomaly pair with $\epsilon_{u,v} > 5\%$, i.e., $n_5 = 0$. It has also been pointed out in [8] that as the key length increases, the actual random behaviour of the key is demonstrated and that is why the number of anomaly pairs decrease and experimental results match the theoretical formulae. In [8, Section 6.3.2] the anomalies are discussed for rows and columns 9, 19 and also for the diagonal given short keys as 5 bytes. We now discuss these results with more details and how they can be applied to distinguish the RC4 keystream from random streams.

We denote the permutation after r-th round of PRGA by S_r^G for $r \geq 1$.

Lemma 4. *Consider* $B \subset [0, \ldots, N-1]$ *with* $|B| = b$. *Let* $P(S_N[r] \in B) = \frac{b}{N} + \epsilon$, *where* ϵ *can be positive or negative. Then* $P(S_{r-1}^G[r] \in B) = \frac{b}{N} + \delta$, *where* $\delta = (\frac{b}{N} + \epsilon) \cdot \Big((\frac{N-1}{N})^{r-1} + \big(1 - (\frac{N-1}{N})^{r-1}\big) \cdot (\frac{b-1}{N-1} - \frac{b}{N}) \Big) - \frac{b}{N} \cdot (\frac{N-1}{N})^{r-1}$, $r \geq 1$.

Proof. The event $(S_{r-1}^G[r] \in B)$ can occur in three ways.

1. $S_N[r] \in B$ and the index r is not touched by any of the $r-1$ many j values during the first $r-1$ rounds of the PRGA. The contribution of this part is $(\frac{b}{N} + \epsilon) \cdot (\frac{N-1}{N})^{r-1}$.
2. $S_N[r] \in B$ and index r is touched by at least one of the $r-1$ many j values during the first $r-1$ rounds of the PRGA. Further, after the swap(s), the value $S_N[r]$ remains in the set B. This will happen with probability $(\frac{b}{N} + \epsilon) \cdot \big(1 - (\frac{N-1}{N})^{r-1}\big) \cdot \frac{b-1}{N-1}$.
3. $S_N[r] \notin B$ and index r is touched by at least one of the $r-1$ many j values during the first $r-1$ rounds of the PRGA. Due to the swap(s), the value $S_N[r]$ comes to the set B. This will happen with probability $(1 - \frac{b}{N} - \epsilon) \cdot \big(1 - (\frac{N-1}{N})^{r-1}\big) \cdot \frac{b}{N}$.

Adding these contributions, we get the total probability as $(\frac{b}{N} + \epsilon) \cdot \Big((\frac{N-1}{N})^{r-1} + \big(1 - (\frac{N-1}{N})^{r-1}\big) \cdot (\frac{b-1}{N-1} - \frac{b}{N}) \Big) + \frac{b}{N} - \frac{b}{N} \cdot (\frac{N-1}{N})^{r-1}$. □

Lemma 5. *If* $P(S_{r-1}^G[r] \in B) = \frac{b}{N} + \delta$, *then* $P(z_r \in C) = \frac{b}{N} + \frac{2\delta}{N}$, *where* $C = \{c' | c' = r - b' \text{ where } b' \in B\}$, $r \geq 1$.

Proof. The event $(z_r \in C)$ can happen in two ways.

1. $S_{r-1}^G[r] \in B$ and $z_r = r - S_{r-1}^G[r]$. From Glimpse theorem [4, 6], we have $P(z_r = r - S_{r-1}^G[r]) = \frac{2}{N}$ for $r \geq 1$. Thus, the contribution of this part is $\frac{2}{N}(\frac{b}{N} + \delta)$.
2. $S_{r-1}^G[r] \notin B$ and still $z_r \in C$ due to random association. The contribution of this part is $(1 - \frac{2}{N})\frac{b}{N}$.

Adding these two contributions, we get the result. □

Theorem 2. *If* $P(S_N[r] \in B) = \frac{b}{N} + \epsilon$, *then* $P(z_r \in C) = \frac{b}{N} + \frac{2}{N} \cdot \Big[(\frac{b}{N} + \epsilon) \cdot \Big((\frac{N-1}{N})^{r-1} + \big(1 - (\frac{N-1}{N})^{r-1}\big) \cdot (\frac{b-1}{N-1} - \frac{b}{N}) \Big) - \frac{b}{N} \cdot (\frac{N-1}{N})^{r-1} \Big]$, *where* $C = \{c' | c' = r - b' \textit{ where } b' \in B\}$, $r \geq 1$.

Proof. The proof immediately follows by combining Lemma 4 and Lemma 5. □

From the above results, it follows that for a single value v, if $P(S_N[r] = v) = \frac{1}{N} + \epsilon$, then $P(z_r = r - v) = \frac{1}{N} + \frac{2\delta}{N}$, where the value of δ can be calculated by substituting $b = 1$ in Lemma 5. This presents a non-uniform distribution of the initial keystream output bytes z_r for small r.

In [9, Section 6], it has been pointed out that z_1 (referred as z_0 in [9]) may not be uniformly distributed due to non-uniform distribution of $S_N[1]$. The experimental results presented in [9, Figure 6] show some bias which does not match with our theoretical as well as experimental results. According to our Theorem 2, if $P(S_N[1] = v) = \frac{1}{N} + \epsilon$, then $P\big(z_1 = (1 - v) \mod 256\big) = \frac{1}{N} + \frac{2\epsilon}{N}$ and this presents the theoretical distribution of z_1.

When the bias of $S_N[r]$ towards a single value v is propagated to z_r, the final bias at z_r is very small and difficult to observe experimentally. Rather, if we start with the bias of $S_N[r]$ towards many values in some suitably chosen set B, then a sum of $b = |B|$ many probabilities is propagated to z_r according to Theorem 2, making the bias of z_r empirically observable too. For example, given $1 \leq r \leq 127$, consider the set B as the set of integers $[r+1, \ldots, r+128]$, i.e., $b = |B| = 128$. The theoretical formulae as well as the experimental results give $P(S_N[r] \in B) > 0.5$, and in turn we get $P(z_r \in C) > 0.5$, which is observable at the r-th keystream output byte of RC4. We have experimented with key length 32 bytes and 100 million runs for different r's and the experimental results support this theoretical claim. It is important to note that the non-uniform distribution can be observed even at the 256-th output byte z_{256}, since the deterministic index i at round 256 becomes 0 and $S_N[0]$ has a non-uniform distribution as follows from Theorem 1. For random association, $P(z_r \in C)$ should be $\frac{b}{N}$, which is not the case here and thus all these results provide distinguishers for RC4.

We have earlier pointed out that for short key lengths, there exist many anomaly pairs. We can exploit these to construct some additional distinguishers by including in the set B those values which are far away from being random. We illustrate this in the two examples below. For 5 byte secret keys, we experimentally observe over 100 million runs that $P(S_N[9] \in B) = 0.137564$ (which is much less than the theoretical value 0.214785), where B is the set of all even integers greater than or equal to 128 and less than 256, i.e., $b = |B| = 64$ and $\frac{b}{N} = 0.25$. Using Theorem 2 we get $P(z_9 \in C) = 0.249530 < 0.25$, where $C = \{c' | c' = 9 - b' \text{ where } b' \in B\}$. Again, for 8 byte secret keys, we observe that $P(S_N[15] \in B) = 0.160751$ (which is much less than the theoretical value 0.216581), where B is the set of all odd integers greater than or equal to 129 and less than 256, i.e., $b = |B| = 64$ once again. Theorem 2 gives $P(z_{15} \in C) = 0.249340 < 0.25$, where $C = \{c' | c' = 15 - b' \text{ where } b' \in B\}$. Direct experimental observations also confirm these biases of z_9 and z_{15}. Further, given the values of δ approximately -0.1 in the above two examples, one can get new linear distinguishers for RC4 with 5 byte and 8 byte keys.

It is interesting to note that since the anomaly pairs are different for different key lengths, by suitably selecting the anomaly pairs in the set B, one can also distinguish among RC4 of different key lengths.

Acknowledgments: We thank the anonymous reviewers for detailed comments that improved editorial as well as technical presentation of this paper.

References

1. S. R. Fluhrer and D. A. McGrew. Statistical Analysis of the Alleged RC4 Keystream Generator. FSE 2000, pages 19-30, vol. 1978, Lecture Notes in Computer Science, Springer-Verlag.
2. S. R. Fluhrer, I. Mantin and A. Shamir. Weaknesses in the Key Scheduling Algorithm of RC4. Selected Areas in Cryptography 2001, pages 1-24, vol. 2259, Lecture Notes in Computer Science, Springer-Verlag.
3. J. Golic. Linear statistical weakness of alleged RC4 keystream generator. EUROCRYPT 1997, pages 226-238, vol. 1233, Lecture Notes in Computer Science, Springer-Verlag.
4. R. J. Jenkins. ISAAC and RC4. 1996
   Available at `http://burtleburtle.net/bob/rand/isaac.html`.
5. I. Mantin and A. Shamir. A Practical Attack on Broadcast RC4. FSE 2001, pages 152-164, vol. 2355, Lecture Notes in Computer Science, Springer-Verlag.
6. I. Mantin. A Practical Attack on the Fixed RC4 in the WEP Mode. ASIACRYPT 2005, pages 395-411, vol. 3788, Lecture Notes in Computer Science, Springer-Verlag.
7. I. Mantin. Predicting and Distinguishing Attacks on RC4 Keystream Generator. EUROCRYPT 2005, pages 491-506, vol. 3494, Lecture Notes in Computer Science, Springer-Verlag.
8. I. Mantin. Analysis of the stream cipher RC4. Master's Thesis, The Weizmann Institute of Science, Israel, 2001.
9. I. Mironov. (Not So) Random Shuffles of RC4. CRYPTO 2002, pages 304-319, vol. 2442, Lecture Notes in Computer Science, Springer-Verlag.
10. G. Paul, S. Rathi and S. Maitra. On Non-negligible Bias of the First Output Byte of RC4 towards the First Three Bytes of the Secret Key. Proceedings of the International Workshop on Coding and Cryptography 2007, pages 285-294.
11. G. Paul and S. Maitra. Permutation after RC4 Key Scheduling Reveals the Secret Key. 14th Annual Workshop on Selected Areas in Cryptography, SAC 2007, August 16-17, Ottawa, Canada.
12. S. Paul and B. Preneel. A New Weakness in the RC4 Keystream Generator and an Approach to Improve the Security of the Cipher. FSE 2004, pages 245-259, vol. 3017, Lecture Notes in Computer Science, Springer-Verlag.
13. A. Roos. A class of weak keys in the RC4 stream cipher. Two posts in sci.crypt, message-id `43u1eh$1j3@hermes.is.co.za` and `44ebge$llf@hermes.is.co.za`, 1995. Available at `http://marcel.wanda.ch/Archive/WeakKeys`.
14. D. Wagner. My RC4 weak keys. Post in sci.crypt, message-id `447o1l$cbj@cnn.Princeton.EDU`, 26 September, 1995. Available at `http://www.cs.berkeley.edu/~daw/my-posts/my-rc4-weak-keys`.