Settling the mystery of $Z_r = r$ in RC4

Sabyasachi Dey and Santanu Sarkar

Department of Mathematics
Indian Institute of Technology Madras,
Sardar Patel Road,
Chennai 600 036, India
sabya.ndp@gmail.com,sarkar.santanu.bir@gmail.com

Abstract. In this paper, using probability transition matrix, at first we revisit the work of Mantin on finding the probability distribution of RC4 permutation after the completion of KSA. After that, we extend the same idea to analyse the probabilities during any iteration of Pseudo Random Generation Algorithm. Next, we study the bias $Z_r = r$ (where Z_r is the r-th output keystream bit), which is one of the significant biases observed in RC4 output keystream. This bias has played an important role in the plaintext recovery attack proposed by Isobe et al. in FSE 2013. However, the accurate theoretical explanation of the bias of $Z_r = r$ is still a mystery. Though several attempts have been made to prove this bias, none of those provides accurate justification. Here, using the results found with the help of probability transition matrix we justify this bias of $Z_r = r$ accurately and settle this issue. The bias obtained from our proof matches perfectly with the experimental observations.

Keywords: Cryptanalysis, KSA, PRGA, RC4, Bias, Stream Cipher

1 Introduction

RC4 has been one of the most famous ciphers for research in last twenty years. Since 1994 when it was made public, it has gone through rigorous cryptanalysis from cryptologists around the world [1, 2, 11, 7, 26, 25, 28]. Several weaknesses of this cipher have been found, and some of them still do not have proper theoretical justification. Due to so many weaknesses RC4 has been dropped by Google recently. But it is still an active area of research. The importance of research on this cipher can be observed in the recently published works on this cipher [29, 7, 17, 18, 21]. In 2017, two works [4, 20] on RC4 are going to appear in Designs, Codes and Cryptography.

RC4 is the most used stream cipher in last two decades. It has been widely used in different areas by different companies. It was designed by Ron Rivest in 1987, but was made public after 1994. First being adopted by TLS, RC4 was used in various applications later. In 1997, it was used in WEP. After that, it was used by Microsoft Lotus, Oracle Secure, WPA.

Due to its huge application and very simple structure, RC4 became the source of attention in last two decades. There are so many attacks proposed

against it. Here we are going to mention only a few of them. The attacks have several directions. For example, distinguishing attacks [6, 16, 12], state recovery attacks [10, 15], etc. The attacks are mostly based on the correlations found between keystream and keys, or between keystream and some constant values. In FSE 2001, Mantin and Shamir presented a broadcast attack using a bias of Z_2 [13]. Another influential attack was provided by Fluhrer et al. [5], which was based on the biases in Key Scheduling Algorithm. Some more interesting results and attacks are provided in [29, 23, 17–19, 27]. The biases obtained in RC4 keystreams resulted attack on protocol WEP [5, 10]. This led to the introduction of a new protocol WPA, which was designed to block the attacks against WEP. Though both of them used RC4, WPA had better key mixing features. But, WPA also faced attack after a period. Based on the attacks proposed against RC4, in 2014 Crypto, Rivest and Schuldt proposed a variant of RC4, named Spritz [22]. It was designed mostly to defend the attacks against RC4. Proposal of ciphers like Spritz even after so many years of proposal of RC4 shows the usefulness of the design model of RC4-like structures. However, in FSE 2015, Banik et al. [3] attacked Spritz based on a short term bias and a long term bias of keystream.

Among all the biases used in attacks against RC4, most have been theoretically explained. However, both the biases of $Z_r = 0$ and $Z_r = r$ did not have proper justification for a long period. But both have significant contribution in attacks against RC4. In FSE 2013, Isobe et al. [8] provided a full plaintext recovery attack where they used the bias of $Z_r = r$. Also, bias of $Z_r = 0$ has been used by Maitra et al. [12] in attacks on broadcast RC4.

After severe analysis, in Journal of Cryptology (2014), the explanation of $Z_r = 0$ has was given by Sen Gupta et al. [24], which very closely matched with the experimental result. But the bias of $Z_r = r$ is still not properly explained.

We describe the structure of the RC4 cipher here in short. It has two phases, namely Key scheduling algorithm (KSA) & Pseudo Random Generation algorithm (PRGA). In KSA, the 256 byte key is given as input. The algorithm starts with an identity permutation of 0 to 255. A scrambling is performed over this permutation using the key and finally another permutation of 0 to 255 is achieved. In this phase, no output keystream is generated. After this, the scrambled permutation of KSA goes to the PRGA phase. Here, the output keystreams $Z_1, Z_2, \ldots$ are produced using the scrambled permutation. Table 1 describes briefly the KSA and PRGA, where all operations are over $\mathbb{Z}_N$.

Our contribution: As already mentioned, the reason behind this bias of $Z_r = r$ is not properly known. In [8], Isobe et al. provided a theoretical (Theorem 8) justification for this. The theoretical result is plotted against the experimental result in a graph. But the probability $\mathrm{P}(Z_r = r)$ achieved by their theory does not match properly with the experimental result. As mentioned in that paper:

> "Since the theoretical values do not exactly coincide with the experimental values, we do not claim that Theorem 8 completely prove this bias".

Table 1. Description of the RC4 Algorithm – KSA and PRGA.

KSA	**PRGA**
Initialization:	*Initialization*:
For $i = 0, \ldots, N-1$	$i = j = 0$;
$S[i] = i$;	
$j = 0$;	*Keystream Generation Loop*:
	$i = i + 1$;
Scrambling:	$j = j + S[i]$;
For $i = 0, \ldots, N-1$	Swap($S[i]$, $S[j]$);
$j = (j + S[i] + K[i])$;	$t = S[i] + S[j]$;
Swap($S[i], S[j]$);	Output $Z = S[t]$;

After this, in FSE 2014, Sen Gupta et al. [23] gave another theoretical explanation of this bias. Their values provided better result than [8]. In our paper, we further improve this result which matches perfectly with experiment.

In 2001, Mantin [14] found the expression for probability $\mathrm{P}(S[u] = v)$ after the completion of KSA. We analyse this probability using matrix form. Though both ideas are actually same, our presentation is different. We use matrix form so that one can visualize the transition probabilities easily. Though the probability $\mathrm{P}(S[u] = v)$ after the completion of KSA has been found by Mantin, the probability $\mathrm{P}(S[u] = v)$ during any iteration of PRGA was not studied in his work. Here, we also study these probabilities using same idea.

In Journal of Cryptography 2014 [24], Sen Gupta et al. attempted to find the probability for $S_{u-1}[u] = v$. Applying our probability transition matrix, we can find the probability $\mathrm{P}(S_r[u] = v)$ for any u, v at any iteration r of PRGA. After finding the probability during any iteration of PRGA, we use that in this paper to prove the probability $Z_r = r$.

Paper Organisation:

- In Section 2.1, we explain the idea of probability transition matrix in RC4. We describe its properties and structure after transition.
- After that, in Section 2.2 we apply these properties to find the probability $\mathrm{P}(S[u] = v)$ after any iteration of KSA and PRGA. Also we plot the heat maps for our obtained result.
- In Section 3, we give theoretical explanation of the bias $Z_r = r$. We compare our result with experimentally observed result and the theory given by [8] and [23].

2 Probability Transition Matrix and its application

2.1 Idea of Probability Transition in RC4

For any N, let S be a permutation of integers from 0 to $N-1$. The value at r-th position of permutation S is denoted by $S[r]$ (starting from 0-th position $S[0]$). Now, suppose we choose a particular position i of the permutation. Next, we randomly choose a number j from 0 to $N-1$. Now, we interchange $S[i]$ and $S[j]$, i.e., we interchange the positions of the values located at i-th and j-th position. We call this new permutation S'. Using the transition matrix we find the change of probability for presence of v at u-th position from initial permutation S to final permutation S', i.e., from $\mathrm{P}(S[u] = v)$ to $\mathrm{P}(S'[u] = v)$ for any u and v after the interchange.

Let $p_{u,v}$ be the probability $\mathrm{P}(S[u] = v)$, and $p'_{u,v}$ be the probability $\mathrm{P}(S'[u] = v)$. Let $\mathbf{M_S}$ be an $N \times N$ matrix. We number the columns and rows starting from 0 and ending at $N-1$. In this matrix, at (u, v)-th cell, i.e., at the cell located at u-th row and v-th column, we put the probability $\mathrm{P}(S[u] = v) = p_{u.v}$. Similarly, $\mathbf{M_{S'}}$ is the respective matrix for the probabilities of final permutation S'. So, we fill the (u, v)-th cell of $\mathbf{M_{S'}}$ by $p'_{u,v}$. Now, we try to find the relation between the entries of $\mathbf{M_S}$ and $\mathbf{M_{S'}}$.

$$\mathbf{M_S}=\begin{bmatrix} p_{0,0} & p_{0,1} & \cdots & p_{0,N-1} \\ p_{1,0} & p_{1,1} & \cdots & p_{1,N-1} \\ \vdots & \vdots & \ddots & \vdots \\ p_{N-1,0} & p_{N-1,1} & \cdots & p_{N-1,N-1} \end{bmatrix} \xrightarrow{\text{transition}} \mathbf{M_{S'}}=\begin{bmatrix} p'_{0,0} & p'_{0,1} & \cdots & p'_{0,N-1} \\ p'_{1,0} & p'_{1,1} & \cdots & p'_{1,N-1} \\ \vdots & \vdots & \ddots & \vdots \\ p'_{N-1,0} & p'_{N-1,1} & \cdots & p'_{N-1,N-1} \end{bmatrix}.$$

Lemma 1. *For any chosen position i which interchanges value with some j, the probabilities $p'_{u,v}$ are of the form:*

$$p'_{u,v} = \begin{cases} p_{u,v}(1 - \frac{1}{N}) + \frac{1}{N} p_{i,v}, & \text{if } u \neq i \\ \frac{1}{N}, & \text{if } u = i \end{cases}$$

Proof. Let i be the chosen position. So, we focus on the i-th row of $\mathbf{M_S}$. It contains the probabilities of presence for any $v \in [0, N-1]$ at i-th position. Now, since j is arbitrary, for any $j_0 \in [0, N-1]$, $\mathrm{P}(j = j_0) = \frac{1}{N}$. Now, suppose we want to find p'_{j_0,v_0} for some v_0. For this, we consider the following two cases:

Case 1: $j_0 \neq i$: Now, after the interchange, v_0 can come at position j_0 by two possible disjoint ways:

1. $S[j_0] = v_0$ and $j \neq j_0$: If in the initial permutation S, v_0 is located at position j_0 and $j \neq j_0$, then the swap between position i and j does not effect j_0. So, v_0 remains at j_0. Probability of this event is

$$\mathrm{P}(S[j_0] = v_0) \cdot \mathrm{P}(j \neq j_0) = p_{j_0,v_0} \cdot \left(1 - \frac{1}{N}\right)$$

.

2. $S[i] = v_0$ and $j = j_0$: In this case, in the initial matrix S, v_0 was at position i. Since $j = j_0$, due to swap, $S'[j_0]$ becomes v_0. The probability of this event is

$$\mathrm{P}(S[i] = v_0) \cdot \mathrm{P}(j = j_0) = p_{i,v_0} \cdot \frac{1}{N}.$$

So, total probability: $p'_{j_0,v_0} = p_{j_0,v_0}(1 - \frac{1}{N}) + p_{i,v_0}\frac{1}{N}$.

Case 2: $j_0 = i$: For any j, if $S[j] = v_0$, then after swap, $S'[i]$ becomes v_0. We know, for any $j' \in 0, 1, \cdots, N-1$, $\mathrm{P}(j = j')$ is $\frac{1}{N}$, since j is random. Now, $\mathrm{P}(S[j] = v_0) = p_{j,v_0}$. So, total probability $p'_{i,v_0} = \frac{1}{N}\left(\sum_{j=0}^{N-1} p_{j,v_0}\right) = \frac{1}{N}$. (since $\sum_{j=0}^{N-1} p_{j,v_0} = 1$)

So, the entries $p'_{u,v}$'s of matrix $\mathbf{M'_S}$ can be expressed by the entries of matrix $\mathbf{M_S}$ as follows:

$$\mathbf{M_{S'}} = \begin{bmatrix} p_{0,0}(1-\frac{1}{N})+\frac{1}{N}p_{i,0} & p_{0,1}(1-\frac{1}{N})+\frac{1}{N}p_{i,1} & \cdots & p_{0,N-1}(1-\frac{1}{N})+\frac{1}{N}p_{i,N-1} \\ p_{1,0}(1-\frac{1}{N})+\frac{1}{N}p_{i,0} & p_{1,1}(1-\frac{1}{N})+\frac{1}{N}p_{i,1} & \cdots & p_{1,N-1}(1-\frac{1}{N})+\frac{1}{N}p_{i,N-1} \\ \vdots & \vdots & \ddots & \vdots \\ p_{i-1,0}(1-\frac{1}{N})+\frac{1}{N}p_{i,0} & p_{i-1,1}(1-\frac{1}{N})+\frac{1}{N}p_{i,1} & \cdots & p_{i-1,N-1}(1-\frac{1}{N})+\frac{1}{N}p_{i,N-1} \\ \frac{1}{N} & \frac{1}{N} & \cdots & \frac{1}{N} \\ p_{i+1,0}(1-\frac{1}{N})+\frac{1}{N}p_{i,0} & p_{i+1,1}(1-\frac{1}{N})+\frac{1}{N}p_{i,1} & \cdots & p_{i+1,N-1}(1-\frac{1}{N})+\frac{1}{N}p_{i,N-1} \\ \vdots & \vdots & \ddots & \vdots \\ p_{N-1,0}(1-\frac{1}{N})+\frac{1}{N}p_{i,0} & p_{N-1,1}(1-\frac{1}{N})+\frac{1}{N}p_{i,1} & \cdots & p_{N-1,N-1}(1-\frac{1}{N})+\frac{1}{N}p_{i,N-1} \end{bmatrix}.$$

2.2 Explanation of the probabilities after KSA phase and during PRGA of RC4:

Using the idea of probability transition matrix, we can achieve the probability of $S[u] = v$ for any $u, v \in \{0, 1, 2, \cdots, N\}$ during any iteration of KSA in RC4 and also after any iteration of PRGA. For this, we start with a genral matrix $\mathbf{M_0}$ with the initial probabilities $p_{i,j}$'s and check how the entries of the matrix change with each iteration. For convenience, we study for only a single column of the matrix. During the transition, the column changes independently, i.e., the transition of each entry is not effected by any entry of the other column. So, we can study the change for a single column and the other columns will also change in similar manner. So, suppose, C_0 be a particular column of the initial matrix.

$$C_0 = \begin{bmatrix} p_0^{(0)} \\ p_0^{(1)} \\ p_0^{(2)} \\ \vdots \\ p_0^{(N-1)} \end{bmatrix} = \begin{bmatrix} p^{(0)} \\ p^{(1)} \\ p^{(2)} \\ \vdots \\ p^{(N-1)} \end{bmatrix}.$$

In RC4, the i-th position swaps value with j-th position at iteration i. So, both the iteration and the chosen can be denoted by same variable i. Let $C^{(i)}$ be the respective column after i iterations. Then, the entries of $C^{(i)}$ can be given as in the following:

Theorem 1. *Let $p_i^{(u)}$ be the u-th entry of $C^{(i)}$ where $u \in [0, N-1]$, then*

$$p_i^{(u)} = \begin{cases} p^{(u)}\left(1-\frac{1}{N}\right)^i + \frac{1}{N}\sum_{r=0}^{i-1} p^{(r)}\left(1-\frac{1}{N}\right)^r, & \text{if } u \geq i \\ \frac{1}{N}, & \text{if } u = i-1 \\ \frac{1}{N}\left(1-\frac{1}{N}\right)^{i-u-1} + \frac{1}{N}\left[\sum_{r=u+1}^{i} p^{(r)}\left(1-\frac{1}{N}\right)^r\right] & \\ \quad + \sum_{r=0}^{u}\left[\frac{p^{(r)}}{N^2}.\left(1-\frac{1}{N}\right)^r.\sum_{j=0}^{i-u-1}\left(1-\frac{1}{N}\right)^j\right], & \text{if } u < i-1 \end{cases}$$

Proof. We prove it by induction on i.

For $u \geq i$: When $i = 0$, the expression given for $p_i^{(u)}$ becomes $p^{(u)}$. So, for $i = 0$, it is true. Now, suppose for some $i = k$, $p_i^{(u)} = p^{(u)}\left(1-\frac{1}{N}\right)^i + \frac{1}{N}\sum_{r=0}^{i-1} p^{(r)}\left(1-\frac{1}{N}\right)^r$ for all $u \geq k$. We show that this is also true for the next iteration $i = k+1$.

Now from Lemma 1, $p_{k+1}^{(u)} = p_k^{(u)}\left(1-\frac{1}{N}\right) + \frac{1}{N}.p_k^{(k)}$. Here, $p_k^{(u)} = p^{(u)}\left(1-\frac{1}{N}\right)^k + \frac{1}{N}\sum_{r=0}^{k-1} p^{(r)}\left(1-\frac{1}{N}\right)^r$ and $p_k^{(k)} = p^{(k)}\left(1-\frac{1}{N}\right)^k + \frac{1}{N}\sum_{r=0}^{k-1} p^{(r)}\left(1-\frac{1}{N}\right)^r$. For convenience of the reader and to shorten the calculations, we introduce variables x and y where x denotes the term $1-\frac{1}{N}$ and y denotes $\frac{1}{N}$. So, $(x+y) = 1$.

Therefore,

$$\begin{aligned} p_{k+1}^{(u)} &= x\left[p^{(u)}x^k + y\sum_{r=0}^{k-1} p^{(r)}x^r\right] + y\left[p^{(k)}x^k + y\sum_{r=0}^{k-1} p^{(r)}x^r\right] \\ &= p^{(u)}x^{k+1} + xy\sum_{r=0}^{k-1} p^{(r)}x^r + y.p^{(k)}x^k + y^2\sum_{r=0}^{k-1} p^{(r)}x^r \\ &= p^{(u)}x^{k+1} + (xy+y^2)\sum_{r=0}^{k-1} p^{(r)}x^r + yp^{(k)}x^k \\ &= p^{(u)}x^{k+1} + y\sum_{r=0}^{k-1} p_r x^r + yp^{(k)}x^k \\ &= p^{(u)}x^{k+1} + y\sum_{r=0}^{k} p^{(r)}x^r \\ &= p^{(u)}\left(1-\frac{1}{N}\right)^{k+1} + \frac{1}{N}\sum_{r=0}^{k} p^{(r)}\left(1-\frac{1}{N}\right)^r \end{aligned}$$

So, the result is true for $i = k+1$.

For $u = (i-1)$**:** It comes directly from Lemma 1.

For $u \leq (i-1)$**:** When $i = u+1$, $p_i^{(u)} = p_i^{(i-1)} = \frac{1}{N}$. So the result is true for $u = i-1$.

Next, when $i = u+2$, we know from Lemma 1,

$$\begin{aligned} p_{u+2}^{(u)} &= p_{u+1}^{(u)}\Big(1-\frac{1}{N}\Big) + \frac{1}{N}p_{u+1}^{(u+1)} \\ &= \frac{1}{N}\Big(1-\frac{1}{N}\Big) + \frac{1}{N}\Big[p^{(u+1)}\Big(1-\frac{1}{N}\Big)^{u+1} + \frac{1}{N}\sum_{r=0}^{u} p^{(r)}\Big(1-\frac{1}{N}\Big)^{r}\Big] \end{aligned}$$

So, it satisfies for $i = u+2$. Now, suppose, for some $i = k$, it is true. This means,

$$p_k^{(u)} = \frac{1}{N}\Big(1-\frac{1}{N}\Big)^{k-u-1} + \frac{1}{N}\Big[\sum_{r=u+1}^{k} p^{(r)}\Big(1-\frac{1}{N}\Big)^{r}\Big] + \sum_{r=0}^{u}\Big[\frac{p^{(r)}}{N^2}\Big(1-\frac{1}{N}\Big)^{r}\sum_{j=0}^{k-u-1}\Big(1-\frac{1}{N}\Big)^{j}\Big].$$

So, for $i = k+1$,

$$p_{k+1}^{(u)} = p_k^{(u)}x + yp_k^{(k)}$$

where

$$\begin{aligned} p_k^{(u)}x &= x\Big[yx^{k-u-1} + y\Big(\sum_{r=u+1}^{k} p^{(r)}x^r\Big) + \sum_{r=0}^{u}\Big(p^{(r)}y^2x^r\sum_{j=0}^{k-u-1}x^j\Big)\Big] \\ &= yx^{k-u} + xy\Big(\sum_{r=u+1}^{k} p^{(r)}x^r\Big) + x\sum_{r=0}^{u}\Big(p^{(r)}y^2x^r\sum_{j=0}^{k-u-1}x^j\Big) \end{aligned}$$

and

$$\begin{aligned} yp_k^{(k)} &= y\Big[p^{(k)}x^k + y\sum_{r=0}^{k-1} p^{(r)}x^r\Big] \\ &= y[p^{(k)}x^k + y\sum_{r=0}^{u} p^{(r)}x^r + y\sum_{r=u+1}^{k-1} p^{(r)}x^r] \\ &= yp^{(k)}x^k + y^2\sum_{r=0}^{u} p^{(r)}x^r + y^2\sum_{r=u+1}^{k-1} p^{(r)}x^r \end{aligned}$$

Adding these two, we have:

$$
\begin{aligned}
p_{k+1}^{(u)} &= yx^{k-u} + xy\Big(\sum_{r=u+1}^{k} p^{(r)}x^r\Big) + x\sum_{r=0}^{u}\Big(p^{(r)}y^2x^r\sum_{j=0}^{k-u-1}x^j\Big) + yp^{(k)}x^k \\
&\quad + y^2\sum_{r=0}^{u}p^{(r)}x^r + y^2\sum_{r=u+1}^{k-1}p^{(r)}x^r \\
&= yx^{k-u} + (xy+y^2)\Big(\sum_{r=u+1}^{k}p^{(r)}(x)^r\Big) + yp^{(k)}(x)^k + \Big[\sum_{r=0}^{u}\Big(p^{(r)}y^2x^r\sum_{j=1}^{k-u}x^j\Big) + y^2\sum_{r=0}^{u}p^{(r)}x^r\Big] \\
&= yx^{k-u} + y\Big(\sum_{r=u+1}^{k}p^{(r)}x^r\Big) + yp^{(k)}x^k + \Big[\sum_{r=0}^{u}\Big(p^{(r)}y^2x^r\sum_{j=1}^{k-u}x^j\Big) + \Big(\sum_{r=0}^{u}p^{(r)}y^2x^r\Big)\Big] \\
&= yx^{k-u} + y\Big(\sum_{r=u+1}^{k+1}p^{(r)}x^r\Big) + \Big[\sum_{r=0}^{u}\Big(p^{(r)}y^2x^r\sum_{j=0}^{k-u}x^j\Big)\Big] \\
&= \tfrac{1}{N}(1-\tfrac{1}{N})^{k+1-u-1} + \tfrac{1}{N}\Big(\sum_{r=u+1}^{k+1}p^{(r)}(1-\tfrac{1}{N})^r\Big) + \Big[\sum_{r=0}^{u}\Big(\tfrac{p^{(r)}}{N^2}(1-\tfrac{1}{N})^r\sum_{j=0}^{k+1-u-1}(1-\tfrac{1}{N})^j\Big)\Big]
\end{aligned}
$$

$\mathbf{P}(S[u] = v)$ after KSA: In key scheduling algorithm, j is updated as $j = j+S[i]+k[i]$. Since a keybit is involved in the sum and keybits are random, j can be treated as random, without caring about the other variables involved in the sum. This is because for any $j_0 \in [0, N-1]$, $= \mathrm{P}(j = j_0) = \mathrm{P}(j+S[i]+k[i] = j_0) = \mathrm{P}(k[i] = j_0-j-S[i]) = \frac{1}{N}$, since $k[i]$ is random. Now, in KSA, i starts from 0 and at each iteration increases by 1. Here we find the probability transition matrix for the permutation S after each round of KSA. The permutation obtained after r-th iteration is denoted by S_r. We denote the probability matrix corresponding to the initial permutation S_0 as $\mathbf{M(S_0)}$ and the matrix corresponding to any S_r as $\mathbf{M(S_r)}$. Also, the entries of the matrix $M(S_r)$ are denoted as $p_{u,v}^{(r)}$. After each iteration, the probability transition matrix is updated by the probability transition formula given in Lemma 1. We denote this transition operation as $\mathcal{TR}$. So, $\mathcal{TR}(\mathbf{M(S_r)}) = \mathbf{M(S_{r+1})}$.
Since initially KSA starts with the identity permutation, we can express the probability $\mathrm{P}(S[u] = v)$ for any u, v as follows:

1. $\mathrm{P}(S[u] = v) = 1$ if $u = v$
2. $\mathrm{P}(S[u] = v) = 0$ if $u \neq v$

So, the matrix $\mathbf{M(S_0)}$ is basically an identity permutation.

Initial Matrix:

$$
\mathbf{M_{S_0}} = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix}.
$$

Now, after each iteration, we update the matrix by the transition operation. After the first transition, $\mathcal{TR}(\mathbf{M_{S_0}}) = \mathbf{M_{S_1}}$.

In the next iteration, $i = 1$ and then by the same transition formula (Lemma 1) on $\mathbf{M_{S_1}}$, we can obtain the matrix $\mathbf{M_{S_2}}$. Thus, by consecutive application of transition for each iteration, at the end we can achieve the final transition matrix $\mathbf{M_{S_N}}$.

$$\mathbf{M_{S_0}} \xrightarrow{\mathcal{TR}} \mathbf{M_{S_1}} \xrightarrow{\mathcal{TR}} \mathbf{M_{S_2}} \cdots \xrightarrow{\mathcal{TR}} \mathbf{M_{S_N}}$$

Therefore, the entries of the matrix obtained after any number of iterations can be directly found by Theorem 1. Here, in particular, we find the entries after the final iteration and show that it matches with Mantin's result [14].

One important point to note is that, in every transition update, each entry is effected by the entries of same column only. The entries of other columns do not have any influence on it. So, to find any entry $p^{(r)}_{u,v}$ of the final matrix $\mathbf{M_{S_N}}$, we can only concentrate on the respective column only, i.e., v-th column. Let us denote the v-th column of any transition matrix $\mathbf{M_{S_r}}$ as $C_v(\mathbf{M_{S_r}})$. Now, in the initial matrix $\mathbf{M_{S_0}}$, the entries of v-th column $C_v(\mathbf{M_{S_0}})$ was as follows:

$$C_v(\mathbf{M_{S_0}}) = \begin{bmatrix} p^{(0)}_{0,v} \\ p^{(0)}_{1,v} \\ \vdots \\ p^{(0)}_{u-1,u} \\ p^{(0)}_{u,u} \\ p^{(0)}_{u+1,u} \\ \vdots \\ p^{(0)}_{N-1,u} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

Now, after N iterations, the probability $\mathrm{P}(S[u] = v)$ can be directly found by Theorem 1. So, we use the formula:

$$p^{(u)}_i = \frac{1}{N}(1 - \frac{1}{N})^{i-u-1} + \frac{1}{N}\Big(\sum_{r=u+1}^{i} p^{(r)}(1 - \frac{1}{N})^r\Big) + \sum_{r=0}^{u}\Big(\frac{p^{(r)}}{N^2}.(1 - \frac{1}{N})^r.\sum_{j=0}^{i-u-1}(1 - \frac{1}{N})^j\Big)$$

Here, $i = N$ and $p^{(v)} = 1$. So, if $v > u$, the third term in the sum becomes 0 (since all p_i for $i = 1, 2, \cdots, u$ are 0).

So,

$$\begin{aligned}
\mathrm{P}(S[u] = v) &= \frac{1}{N}(1 - \frac{1}{N})^{N-u-1} + \frac{1}{N}\Big(\sum_{r=u+1}^{N} p^{(r)}(1 - \frac{1}{N})^r\Big) \\
&= \frac{1}{N}(1 - \frac{1}{N})^{N-u-1} + \frac{1}{N}\Big(p^{(v)}(1 - \frac{1}{N})^v\Big) \\
&= \frac{1}{N}(1 - \frac{1}{N})^{N-u-1} + \frac{1}{N}(1 - \frac{1}{N})^v \\
&= \frac{1}{N}\Big((1 - \frac{1}{N})^{N-u-1} + (1 - \frac{1}{N})^v\Big)
\end{aligned}$$

For, $v \leq u$, the second term in the sum vanishes, since for all $r > v$, $p^{(r)} = 0$. So,

$$\begin{aligned}
\mathrm{P}(S[u] = v) &= \frac{1}{N}(1-\frac{1}{N})^{N-u-1} + \sum_{r=0}^{u}\left(\frac{p^{(r)}}{N^2}(1-\frac{1}{N})^{r}\sum_{j=0}^{N-u-1}(1-\frac{1}{N})^{j}\right) \\
&= \frac{1}{N}(1-\frac{1}{N})^{N-u-1} + \frac{p^{(v)}}{N^2}(1-\frac{1}{N})^{v}\sum_{j=0}^{N-u-1}(1-\frac{1}{N})^{j} \\
&= \frac{1}{N}(1-\frac{1}{N})^{N-u-1} + \frac{1}{N^2}(1-\frac{1}{N})^{v}\sum_{j=0}^{N-u-1}(1-\frac{1}{N})^{j} \\
&= \frac{1}{N}(1-\frac{1}{N})^{N-u-1} + \frac{1}{N}(1-\frac{1}{N})^{v}(1-(1-\frac{1}{N})^{N-u}) \\
&= \frac{1}{N}\left((1-\frac{1}{N})^{N-u-1} + (1-\frac{1}{N})^{v}(1-(1-\frac{1}{N})^{N-u})\right)
\end{aligned}$$

So, we have:

$$\mathrm{P}(S[u] = v) = \begin{cases} \frac{1}{N}\left((1-\frac{1}{N})^{N-u-1} + (1-\frac{1}{N})^{v}\right) & \text{if } v \geq u \\ \frac{1}{N}\left((1-\frac{1}{N})^{N-u-1} + (1-\frac{1}{N})^{v}(1-(1-\frac{1}{N})^{N-u})\right), & \text{if } v < u \end{cases}$$

This matches exactly with the result obtained by Mantin [14]. Here, we show the transition of the column in the diagram.

Probabilities during PRGA: Using the idea of probability transition matrix, we can find the probability $\mathrm{P}(S_r[u] = v)$ for any u and v after r-th round. However, here the procedure is slightly tricky. In PRGA, we know that the iteration starts with $i = 1$, unlike KSA. And, here j is updated as $j = j + S[i]$. So, $j_1 = S[1]$, which cannot be taken as uniformly distributed. However,in FSE 2011[12], Maitra et al showed that as r increases, the distribution of j_r gets closer to $\frac{1}{N}$. They have shown that j_2 has much more randomness than j_1, and from j_3 onwards almost uniformly randomness is observed. So for first two iteration we take care of the distribution of j, and from third iteration we take it distribution to be $\frac{1}{N}$.

First Iteration: We start with the matrix achieved after the first iteration. The probabilities $\mathrm{P}(S[u] = v)$ after first iteration can be found in [24] in the following lemma.

Lemma 2. *After the first round of RC4 PRGA, the probability $P(S_1[u] = v)$ is:*

$$P(S_1[u] = v) = \begin{cases} P(S_0[1] = 1) + \sum_{X \neq 1} P(S_0[1] = X \ \wedge \ S_0[X] = 1), & u = 1, v = 1; \\ \sum_{X \neq 1, v} P(S_0[1] = X \ \wedge \ S_0[X] = v), & u = 1, v \neq 1; \\ P(S_0[1] = u) + \sum_{X \neq u} P(S_0[1] = X \ \wedge \ S_0[u] = u), & u \neq 1, v = u; \\ \sum_{X \neq u, v} P(S_0[1] = X \ \wedge \ S_0[u] = v), & u \neq 1, v \neq u. \end{cases}$$

From this, we find the entries of the matrix after first iteration. Now, the second iteration is $i = 2$. Then, to deal with iteration starting from $i = 2$, we just change the position of the rows of the matrix. The row corresponding to $i = 2$ comes to the first. Each of the rows are shifted upwards by 2 rows, and the 0-th and 1-st row go to the last. So, in this new matrix the iteration starts from the first row.

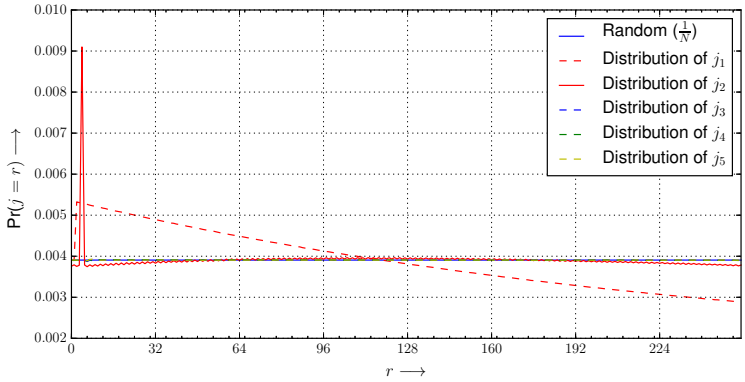

Fig. 1. Probability distribution of j_r for $1 \leq r \leq 5$.

Second iteration: In [12], the probability distribution of j_2 is given as follows:

$$\mathrm{P}(j_2 = v) = \begin{cases} \mathrm{P}(S_0[1] = 2) + \sum\limits_{\substack{w=0 \\ w \neq 2}}^{N-1} \mathrm{P}(S_0[1] = w)\mathrm{P}(S_0[2] = v - w), & \text{if } v = 4 \\ \sum\limits_{\substack{w=0 \\ w \neq 2}}^{N-1} \mathrm{P}(S_0[1] = w)\mathrm{P}(S_0[2] = v - w), & \text{if } v \neq 4 \end{cases}$$

So, instead if using the values $\frac{1}{N}$ and $(1 - \frac{1}{N})$, we use the expressions given in the above equations to update the matrix. From third iteration, since j_3 behaves almost uniformly random, we can apply the formulas achieved in Theorem 1 to find the probabilities after any round. Thus,using the idea of probability transition matrix, we find the probability of $S[u] = v$ after any iteration of KSA and PRGA. Probability distributions of few j values are given in Figure 1.

We provide the heat maps in Figure 2 for the probabilities for PRGA for round $i = 0, 1, 256$ and 512.

Recently in 2017, Paul et al. [21] did a detail study of the probabilities at every iteration of KSA and PRGA. In [21], for the analysis of PRGA distribution, the authors have taken j to be uniformly random. But this is not the case in

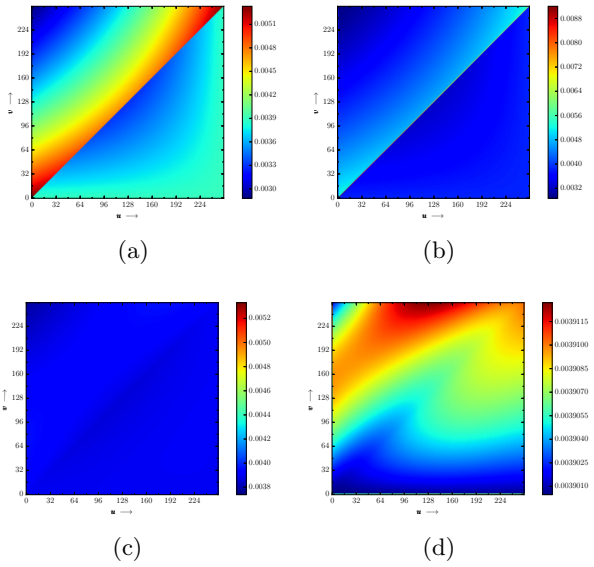

Fig. 2. Probability $\mathrm{P}(S[u] = v)$ for $1 \leq u \leq 255, 0 \leq v \leq 255$ in PRGA. Here (a) Round $i = 0$ (b) Round $i = 1$ (c) Round $i = 256$ (d) Round $i = 512$.

reality, which has been also mentioned by the authors. The value of j in the first iteration is a function of KSA permutation and this cannot be taken as random. The value of j_2 also is not random. However, in the next iterations, the distribution of j becomes very close to random. In conclusion of [21], the authors clearly mentioned that their rigorous analysis on PRGA distribution is based on the assumption that j is random. They raised an open problem to find the actual distribution of PRGA. In our matrix approach, we are able to deal with this very easily. So, this approach improves the result of the PRGA distribution from [21].

3 Theoretical Explanation of $Z_r = r$

Here we prove the bias of $Z_r = r$ for $r \geq 3$. In the following lemma we show some events. In few of them $Z_r = r$ is the only possible output. In some paths Z_r can never be equal to r. After discussing these paths, we find their respective probabilities of occurrence. Finally, in Theorem 2, we find the probability of $Z_r = r$. For convenience, we denote by $\mathrm{KSA}(u, v)$ the probability of $S_{KSA}[u] = v$ after the completion of KSA.

Notations:

- $S_r[u]$: value at u-th position after r-th round of PRGA.
- $KSA(u, v)$: Probability of occurrence of v at u-th position after KSA.

– j_r: j at r-th iteration.
– $S_{KSA}[u]$: value at u-th position after KSA.

Lemma 3. *During PRGA,*

$$P\bigg(Z_r = r \mid (S_{r-2}[r-1] = r \cap S_{r-2}[r] = 0 \cap j_{r-1} \neq r)\bigg) = 1,$$
$$P\bigg(Z_r = r \mid (S_{r-1}[r] \neq 0 \cap S_{r-1}[j_r] = r)\bigg) = 0.$$

Proof. Here we have $S_{r-2}[r-1] = r, S_{r-2}[r] = 0$ and $j_{r-1} \neq r$. Since $j_{r-1} \neq r$ and $S_{r-2}[r] = 0$, we have $j_r = j_{r-1}$. Thus when $i = r$, after swap, we have $S_r[r] = r$ and $S_r[j_r] = 0$. Thus

$$Z_r = S_r[S_r[r] + S_r[j_r]] = S_r[r] = r.$$

Please see the path in Figure 3. Thus

$$\mathrm{P}\bigg(Z_r = r \mid (S_{r-2}[r-1] = r \cap S_{r-2}[r] = 0 \cap j_{r-1} \neq r)\bigg) = 1.$$

Also

$$\mathrm{P}(S_{r-2}[r-1] = r \cap S_{r-2}[r] = 0 \cap j_{r-1} \neq r) = \mathrm{P}(S_{r-2}[r-1] = r)\mathrm{P}(S_{r-2}[r] = 0)\big(1 - \frac{1}{N}\big),$$

where $\mathrm{P}(S_{r-2}[r-1] = r), \mathrm{P}(S_{r-2}[r] = 0)$ can be calculated using the idea of Section 2.

Similarly

$$\mathrm{P}\bigg(Z_r = r \mid (S_{r-1}[r] \neq 0 \cap S_{r-1}[j_r] = r)\bigg) = 0$$

and

$$\mathrm{P}(S_{r-1}[r] \neq 0 \cap S_{r-1}[j_r] = r) = \frac{1}{N}\bigg(1 - \mathrm{P}(S_{r-1}[r] = 0)\bigg),$$

assuming j_r is random.

Lemma 4. *Consider the events:*

1. $\mathcal{E}_1 : S_{KSA}[1] = r \geq 3$
2. $\mathcal{E}_2 : j_2 \notin [3, r]$
3. $\mathcal{E}_3 : j_l \neq j_2,\ l \in [3, r-1]$
4. $\mathcal{E}_4 : j_l \neq r,\ l \in [3, r-1]$
5. $\mathcal{E}_5 : j_r = j_2$
6. $\mathcal{E}_6 : S_{KSA}[2] \neq j_r - r$

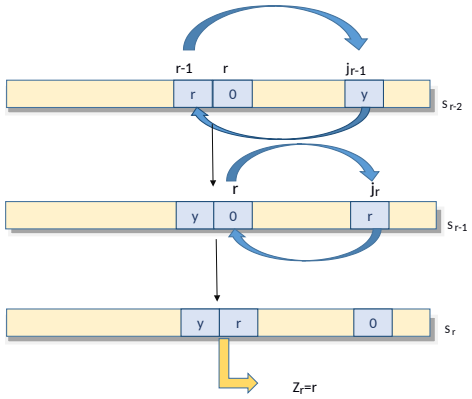

Fig. 3. Path for $Z_r = r$ given $S_{r-2}[r-1] = r, S_{r-2}[r] = 0$ and $j_{r-1} \neq r$.

Then $P(Z_r = r \mid \cap_{i=1}^{5} \mathcal{E}_i) = 1$, $P(Z_r = r \mid \mathcal{E}_1 \cap \mathcal{E}_2 \cap \mathcal{E}_3^c \cap \mathcal{E}_4 \cap \mathcal{E}_5) = 0$,

$$P(Z_r = r \mid \mathcal{E}_1 \cap (\mathcal{E}_2 \cap \mathcal{E}_3)^c \cap \mathcal{E}_4 \cap \mathcal{E}_6) = \begin{cases} \frac{KSA(j_r, j_r - r)}{1 - KSA(j_r, r)}(1 - \frac{1}{N})^{r-3} \text{ if } j_r > r \ \& j_r \neq 2r \\ \frac{1}{N-1}(1 - \frac{1}{N})^{r-j_r-1} \text{ if } j_r < r \\ 0 \text{ if } j_r = r, 2r. \end{cases}$$

The probabilities are as follows:

1. $P(\mathcal{E}_1) = KSA(1, r)$
2. $P(\mathcal{E}_2) = \frac{N-r-2}{N}$
3. $P(\mathcal{E}_3) = P(\mathcal{E}_4) = (1 - \frac{1}{N})^{r-3}$
4. $P(\mathcal{E}_5) = \frac{1}{N}$
5. $P(\mathcal{E}_6) = 1 - P(KSA(2, j_r - r))$

Proof. Due to the event $\mathcal{E}_1$, $j_1 = r$. After the swap, $S_1[r] = r$. Now, $j_2 = j_1 + S_1[2] = r + S_{KSA}[2]$. (since $r > 2$, the first swap cannot involve the position $S_{KSA}[2]$). Let us denote $S_{KSA}[2]$ by w. So, $j_2 = r + w$. So, after the next swap, $S_2[r] = r$ and $S_2[r + w] = w$. Then, due to event $\mathcal{E}_3$, the positions r and $r + w$ are not affected upto $(r - 1)$-th iteration. Next, at r-th iteration, $j_r = j_2 = r + w$ due to event $\mathcal{E}_4$. So, after swap, $S_r[r] = w$ and $S_r[r + w] = r$. So, $Z_r = S_r[S_r[r] + S_r[r + w]] = S_r[z + w] = r$.

Now, the probabilities of the events are $\mathrm{P}(\mathcal{E}_1) = KSA(1, r), \mathrm{P}(\mathcal{E}_2) = \frac{N-r-2}{N}$, $\mathrm{P}(\mathcal{E}_3) = \mathrm{P}(\mathcal{E}_4) = (1 - \frac{1}{N})^{r-3}, \mathrm{P}(\mathcal{E}_5) = \frac{1}{N}$.

Assuming the $\mathcal{E}_i$'s are independent,

$$\mathrm{P}(\cap_{i=1}^{5} \mathcal{E}_i) \approx KSA(1, r) \frac{N - r - 2}{N} \left(1 - \frac{2}{N}\right)^{r-3} \frac{1}{N}.$$

Now, on the other side, if $\mathcal{E}_3^c$ occurs, this means some j_l is equal to j_2 for $l \in [3, r-1]$. As a result, the value at position j_2 changes. Once it changes, there is no chance of getting back that value upto $(r-1)$-th iteration because i moves towards the right side at each iteration and it cannot reach the position where the value has been swapped. As a result, the output Z_r cannot be r.

The probability $\mathrm{P}(\mathcal{E}_3^c) = \left(1 - (1 - \frac{1}{N})^{r-3}\right)$.

Now if $\mathcal{E}_1$ and $\mathcal{E}_4$ hold, $S_{r-1}[r] = r$. Now if $S_{r-1}[j_r] = j_r - r$, $Z_r = r$. Now we have two cases:

Case 1: $j_r > r$: The only possibility of this is if after KSA, position j_r is occupied by $j_r - r$, and $j_3, j_4 \cdots j_{r-1}$ does not touch this position. In this case, the probability is

$$\frac{KSA(j_r, j_r - r)}{1 - KSA(j_r, r)} \left(1 - \frac{1}{N}\right)^{r-3}$$

as by the condition $\mathcal{E}_1$, $S_{KSA}[1] = r$.

In any other case, this would not occur. Suppose, at the end of KSA, j_r is not occupied by $j_r - r$. Then, in order to bring $j_r - r$ to j_r-th position, at some iteration between 1 to r, $j_r - r$ has to come to j_r-th position by swap. This is possible only if at some iteration either i or j becomes equal to j_r. Since $j_r > r$, i cannot be equal to j_r in first r iterations. Suppose, at some iteration $m < r$, j_m become equal to j_r. This means, when $i = m$, the m-th position contains $j_r - r$ and after the swap between m and j_m, it comes to position j_m. But, according to the update rule, $j_m = j_{m-1} + S[m] = j_{m-1} + j_r - r$. Since $j_m = j_r$, we have $j_{m-1} = r$, which is not possible by assumption $\mathcal{E}_4$. So, this event is not possible.

Case 2: $j_r < r$: In this situation, when $i = j_r$, due to swap $S_{j_r}[j_r] = j_r - r$. This happens with probability $\frac{1}{N-1}$ as $S_{j_r}[r] = r$ and $j_r \neq 2r$. Also remaining j_l cannot be j_r for $l = j_r + 1, \ldots, l = r - 1$. Thus total probability is

$$\frac{1}{N-1} \left(1 - \frac{1}{N}\right)^{r-j_r-1}$$

.

Lemma 5. *Consider the events:*

1. $\mathcal{E}_7 : S_{KSA}[r] = r \geq 3$
2. $\mathcal{E}_8 : j_l \neq r,\ l \in [2, r-1]$

Then

$$P(Z_r = r \mid \mathcal{E}_7 \cap \mathcal{E}_8) = \begin{cases} \frac{KSA(j_r, j_r - r)}{1 - KSA(j_r, r)} (1 - \frac{1}{N})^{r-1} \text{ if } j_r > r \ \& j_r \neq 2r \\ \frac{1}{N-1} (1 - \frac{1}{N})^{r-j_r-1} \text{ if } j_r < r \\ 0 \text{ if } j_r = r, 2r. \end{cases}$$

Proof. Proof is similar to the second part of the proof of Lemma 4. Also $\mathrm{P}(\mathcal{E}_7) = KSA(r, r)$ and $\mathrm{P}(\mathcal{E}_8) = \left(1 - \frac{1}{N}\right)^{r-2}$.

Lemma 6. *Consider the events:*

1. $\mathcal{E}_9^x : S_{KSA}[x] = r \geq 3$ *for* $x \in [2, r-2]$
2. $\mathcal{E}_{10}^x : j_1, j_2, \ldots, j_{x-1} \neq x$
3. $\mathcal{E}_{11}^x : j_x = r$
4. $\mathcal{E}_{12}^x : j_{x+1} \notin [x+2, r]$
5. $\mathcal{E}_{13}^x : j_l \neq r,\ l \in [x+2, r-1]$
6. $\mathcal{E}_{14}^x : j_l \neq j_{x+1},\ l \in [x+2, r-1]$
7. $\mathcal{E}_{15}^x : j_r = j_{x+1}$

Then $P(Z_r = r \mid \cap_{i=9}^{15} \mathcal{E}_i^x) = 1$, $P(Z_r = r \mid \mathcal{E}_9^x \cap \mathcal{E}_{10}^x \cap \mathcal{E}_{11}^x \cap \mathcal{E}_{12}^x \cap \mathcal{E}_{13}^x \cap (\mathcal{E}_{14}^x)^c \cap \mathcal{E}_{15}^x) = 0$

Proof. Proof is similar to the first part of the proof of Lemma 4. Also $\mathrm{P}(\mathcal{E}_9^x) = KSA(x, r),\ \mathrm{P}(\mathcal{E}_{10}^x) = \left(1 - \frac{1}{N}\right)^{x-1},\ \mathrm{P}(\mathcal{E}_{11}^x) = \frac{1}{N},\ \mathrm{P}(\mathcal{E}_{12}^x) = 1 - \frac{r-x-1}{N},\ \mathrm{P}(\mathcal{E}_{13}^x) = \left(1 - \frac{1}{N}\right)^{r-x-2},\ \mathrm{P}(\mathcal{E}_{14}^x) = \left(1 - \frac{1}{N}\right)^{r-x-2}, \mathrm{P}(\mathcal{E}_{15}^x) = \frac{1}{N}$.

Now we will prove the main result.

Theorem 2. *In PRGA phase of RC4, the probability* $P(Z_r = r)$ *for* $3 \leq r \leq 255$ *is given by*

$$
\begin{aligned}
P(Z_r = r) = \prod_{i=1}^{5} P(\mathcal{E}_i) + \Big[\sum_{\substack{j_r = r+1 \\ j_r \neq 2r}}^{N-1} \frac{KSA(j_r, j_r - r)}{1 - KSA(j_r, r)} \Big(1 - \frac{1}{N}\Big)^{r-3} \\
+ \sum_{j_r=0}^{r-1} \frac{1}{N-1} \Big(1 - \frac{1}{N}\Big)^{r-j_r-1} \Big] P(\mathcal{E}_1)\big(1 - P(\mathcal{E}_2)P(\mathcal{E}_3)\big) P(\mathcal{E}_4) P(\mathcal{E}_6) \\
+ \Big[\sum_{\substack{j_r = r+1 \\ j_r \neq 2r}}^{N-1} \frac{KSA(j_r, j_r - r)}{1 - KSA(j_r, r)} \Big(1 - \frac{1}{N}\Big)^{r-1} + \sum_{j_r=0}^{r-1} \frac{1}{N-1} \Big(1 - \frac{1}{N}\Big)^{r-j_r-1} \Big] P(\mathcal{E}_7) P(\mathcal{E}_8) \\
+ \Big(\sum_{x=2}^{r-2} \prod_{i=9}^{15} P(\mathcal{E}_i^x) \Big) + P(S_{r-2}[r-1] = r) P(S_{r-2}[r] = 0) \Big(1 - \frac{1}{N}\Big) \\
+ \Big(1 - \prod_{\substack{i=1 \\ i \neq 4}}^{5} P(\mathcal{E}_i) - P(\mathcal{E}_1)\big(1 - P(\mathcal{E}_2)P(\mathcal{E}_3)\big) P(\mathcal{E}_4) P(\mathcal{E}_6) - P(\mathcal{E}_7) P(\mathcal{E}_8) - \prod_{\substack{i=9 \\ i \neq 14}}^{15} P(\mathcal{E}_i^x) \\
- P(S_{r-2}[r-1] = r) P(S_{r-2}[r] = 0)\big(1 - \frac{1}{N}\big) - \big(1 - P(S_{r-1}[r] = 0)\frac{1}{N}\Big) \frac{1}{N}.
\end{aligned}
$$

Proof. Major paths are coming from Lemma 3, Lemma 4, Lemma 5 and Lemma 6. The first term $\prod_{i=1}^{5} \mathrm{P}(\mathcal{E}_i)$ comes from Lemma 4, where we assume that

$$\mathrm{P}(\cap_{i=1}^{5}(\mathcal{E}_i)) = \prod_{i=1}^{5} \mathrm{P}(\mathcal{E}_i)$$

due to independence.

Similarly in other cases also we assume the independence and find the probability of the intersection of events by the product. In the complementary path, we assume that $Z_r = r$ holds with probability $\frac{1}{N}$. Hence the proof.

Experimental results: We run our experiment for 2^{41} random 256 bit key. The graph obtained in experiment has been shown in Figure 4. We compare our theoretical result with the experimental result as well as the theories provided by [8] and [23]. Where the graph of [8] and [23] have significant difference from the experimental curve, our theory matches the curve exactly. Thus, our work provides the accurate justification of the bias observed for $Z_r = r$.

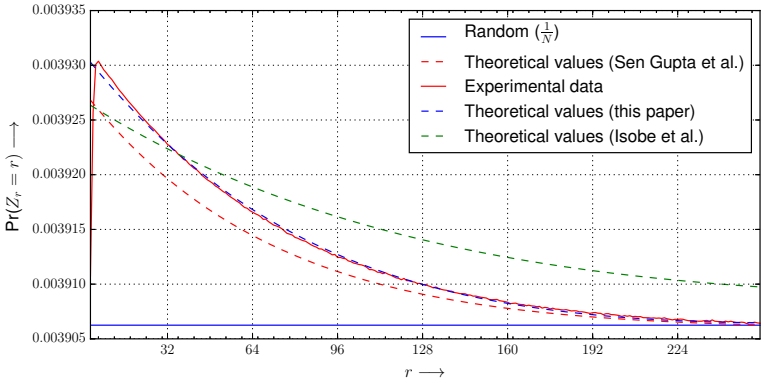

Fig. 4. Index r of RC4 keystream bytes.

4 Conclusion

In this paper, we accurately justify the bias of $Z_r = r$ theoretically. In our proof, we use the probability distribution of RC4 permutation during PRGA, which we obtain by the idea of transition matrix. The proof of this bias was attempted before in FSE 2013 and FSE 2015. But previous theoretical curves did not match accurately with experimental curve. Our work finally puts an end to this research by an exact explanation of the bias.

References

1. N. AlFardan, D. Bernstein, K. Paterson, B. Poettering and J. Schuldt. On the security of RC4 in TLS. In USENIX 2013, pp. 305–320, 2013. Published online at: `http://www.isg.rhul.ac.uk/tls/`.
2. E. Biham and Y. Carmeli. Efficient Reconstruction of RC4 Keys from Internal States. In FSE 2008, LNCS 5086, pp. 270–288, 2008.
3. S. Banik and T. Isobe. Cryptanalysis of the Full Spritz Stream Cipher. In FSE 2016, LNCS 9783, pp. 63–77. Available at: `https://eprint.iacr.org/2016/092`.

4. R. Bricout, S. Murphy, K. G. Paterson and T. van der Merwe. Analysing and Exploiting the Mantin Biases in RC4. To appear at Designs, Codes and Cryptography. Available at: https://eprint.iacr.org/2016/063.
5. S. R. Fluhrer, I. Mantin and A. Shamir. Weaknesses in the Key Scheduling Algorithm of RC4. SAC 2001 Toronto, Ontario, Canada, August 16-17, 2001
6. S. R. Fluhrer and D. A. McGrew. Statistical Analysis of the Alleged RC4 Keystream Generator. In FSE 2000, LNCS 1978, pp. 19–30.
7. S. Jha, S. Banik, T. Isobe and T. Ohigashi. Some Proofs of Joint Distribution of Keystream Biases in RC4. In INDOCRYPT 2016, LNCS, 10095, pp. 305–321, 2016.
8. T. Isobe, T. Ohigashi, Y. Watanabe and M. Morii. Full plaintext recovery attack on broadcast RC4. In FSE 2013, LNCS 8424, pp. 179–202.
9. A. Klein. Attacks on the RC4 stream cipher. Designs Codes and Cryptography, vol. 48(3), pp. 269-286, 2008.
10. L. R. Knudsen, W. Meier, B. Preneel, V. Rijmen and S. Verdoolaege. Analysis Methods for (Alleged) RC4. In ASIACRYPT 1998, LNCS 1514, pp. 327–341.
11. S. Maitra and G. Paul. New Form of Permutation Bias and Secret Key Leakage in Keystream Bytes of RC4. In FSE 2008, LNCS 5086, pp. 253–269, 2008.
12. S. Maitra, G. Paul and S. Sengupta. Attack on Broadcast RC4 Revisited. In FSE 2011, LNCS 6733, pp. 199–217.
13. I. Mantin and A. Shamir. A practical attack on broadcast RC4. In FSE 2001, LNCS 2355, pp. 152–164.
14. I. Mantin. Analysis of the stream cipher RC4. Master's Thesis, The Weizmann Institute of Science, Israel (2001).
15. A. Maximov and D. Khovratovich. New State Recovery Attack on RC4. In CRYPTO 2008, LNCS 5157, pp. 297–316.
16. I. Mironov. (Not So) Random Shuffles of RC4. In CRYPTO 2002, LNCS 2442, pp. 304–319.
17. K. G. Paterson, B. Poettering and J. C. N. Schuldt. Big Bias Hunting in Amazonia: Large-Scale Computation and Exploitation of RC4 Biases (Invited Paper). In Asiacrypt 2014, LNCS 8873, pp. 398–419.
18. K. G. Paterson, J. Schuldt and B. Poettering. Plaintext Recovery Attacks Against WPA/TKIP. In FSE 2014, LNCS 8540, pp. 325–349, 2014.
19. G. Paul and S. Maitra. Permutation after RC4 Key Scheduling Reveals the Secret Key. In SAC 2007, LNCS 4876, pp. 360–377.
20. G. Paul and S. Ray. On data complexity of distinguishing attacks versus message recovery attacks on stream ciphers. To be appear in Designs, Codes and Cryptography. Available at: https://eprint.iacr.org/2015/1174.
21. G. Paul and S. Ray. Analysis of Burn-in period for RC4 State Transition. IACR Cryptology ePrint Archive, 2017. Available at: https://eprint.iacr.org/2017/175.pdf
22. R. L. Rivest and J. C. N. Schuldt. Spritz - a spongy RC4-like stream cipher and hash function. Available at: https://people.csail.mit.edu/rivest/pubs/RS14.pdf.
23. S. Sengupta, S. Maitra, W. Meier, G. Paul and S. Sarkar. Dependence in IV-Related Bytes of RC4 Key Enhances Vulnerabilities in WPA. In FSE 2014, LNCS 8540, pp. 350–369. Available at: https://eprint.iacr.org/2013/476.pdf.
24. S. Sengupta, S. Maitra, G. Paul and S. Sarkar. (Non-)Random Sequences from (Non-)Random Permutations - Analysis of RC4 stream cipher. Journal of Cryptology, vol. 27(1), pp. 67–108, 2014. Available at http://eprint.iacr.org/2011/448.

25. P. Sepehrdad, S. Vaudenay and M. Vuagnoux. Discovery and Exploitation of New Biases in RC4. In SAC 2010, LNCS 6632, pp. 343–363.
26. P. Sepehrdad, S. Vaudenay, and M. Vuagnoux. Statistical Attack on RC4 - Distinguishing WPA. In EUROCRYPT 2011, LNCS 6632, pp. 343–363.
27. P. Sepehrdad, P. Susil, S. Vaudenay and M. Vuagnoux. Smashing WEP in a Passive Attack. In FSE 2013, LNCS 8424, pp. 155–178.
28. P. Sepehrdad, P. Susil, S. Vaudenay and M. Vuagnoux. Tornado Attack on RC4 with Applications to WEP & WPA. IACR Cryptology ePrint Archive, 2015. Available at `https://eprint.iacr.org/2015/254.pdf`
29. M. Vanhoef and F. Piessens. All Your Biases Belong to Us: Breaking RC4 in WPA-TKIP and TLS. USENIX 2016, pp. 1–16, 2016. Available at `https://www.rc4nomore.com/vanhoef-usenix2015.pdf`.