J. Cryptol. (2014) 27: 67–108
DOI: 10.1007/s00145-012-9138-1

Journal of
CRYPTOLOGY

(Non-)Random Sequences from (Non-)Random Permutations—Analysis of RC4 Stream Cipher*

Sourav Sen Gupta and Subhamoy Maitra
Applied Statistics Unit, Indian Statistical Institute, Kolkata 700 108, India
sg.sourav@gmail.com; subho@isical.ac.in

Goutam Paul
Department of Computer Science and Engineering, Jadavpur University, Kolkata 700 032, India
goutam.paul@ieee.org

Santanu Sarkar
Applied Statistics Unit, Indian Statistical Institute, Kolkata 700 108, India
sarkar.santanu.bir@gmail.com

Communicated by Willi Meier.

Received 2 January 2012
Online publication 5 December 2012

Abstract. RC4 has been the most popular stream cipher in the history of symmetric key cryptography. Its internal state contains a permutation over all possible bytes from 0 to 255, and it attempts to generate a pseudo-random sequence of bytes (called keystream) by extracting elements of this permutation. Over the last twenty years, numerous cryptanalytic results on RC4 stream cipher have been published, many of which are based on non-random (biased) events involving the secret key, the state variables, and the keystream of the cipher.

Though biases based on the secret key are common in RC4 literature, none of the existing ones depends on the length of the secret key. In the first part of this paper, we investigate the effect of RC4 keylength on its keystream, and report significant biases involving the length of the secret key. In the process, we prove the two known empirical biases that were experimentally reported and used in recent attacks against WEP and WPA by Sepehrdad, Vaudenay and Vuagnoux in EUROCRYPT 2011. After our current work, there remains no bias in the literature of WEP and WPA attacks without a proof.

In the second part of the paper, we present theoretical proofs of some significant initial-round empirical biases observed by Sepehrdad, Vaudenay and Vuagnoux in SAC 2010.

* This is a substantially revised and extended version of the papers [16] of FSE 2011 and [28] of SAC 2011. Sects. 2 and 3 are based on Ref. [28], with major revision in Lemma 1 and a generalization in Theorem 1, along with substantial new contributions in Sect. 2. Section 4.2 is based on Ref. [16] with major revision in the proof of Theorem 14. Section 2.2, Theorem 6 of Sect. 2.3, and Sects. 4.1 and 4.3 are completely new technical contributions in this paper.

In the third part, we present the derivation of the complete probability distribution of the first byte of RC4 keystream, a problem left open for a decade since the observation by Mironov in CRYPTO 2002. Further, the existence of positive biases towards zero for all the initial bytes 3 to 255 is proved and exploited towards a generalized broadcast attack on RC4. We also investigate for long-term non-randomness in the keystream, and prove a new long-term bias of RC4.

Key words. Bias, Distinguisher, Keylength recovery, Probability distribution, Pseudo-random sequences, RC4, Stream ciphers.

1. Introduction

In the domain of symmetric key cryptology, the stream ciphers are considered to be one of the most important primitives. A stream cipher aims to output a *pseudo-random sequence* of bits, called the *keystream*, and encryption is done by masking the plaintext (considered as a sequence of bits) by the keystream. The masking operation is just a simple XOR in general, and so the ciphertext is also a sequence of bits of the same length as that of the plaintext. For ideal information theoretic 'perfect secrecy' of the scheme, it is desired that the masking is done using a *one-time pad*, where a unique sequence of bits is used as a mask for each plaintext. In reality, however, a one-time pad is not practically feasible, as it requires a key as large as the length of the plaintext. Instead, a computational notion of secrecy is ensured by the pseudo-random nature of the output sequence (keystream) generated by a stream cipher. Any non-random event in the internal state or the keystream of a stream cipher is not desired from a cryptographic point of view, and rigorous analysis is performed to identify the presence of any such non-randomness in its design.

The most important and cryptographically significant goal of a stream cipher is to produce a pseudo-random sequence of bits or words using a fixed-length secret key (or a secret key paired with an initialization vector). Over the last three decades of research and development in stream ciphers, a number of designs have been proposed and analyzed by the cryptology community. One of the main ideas for building a stream cipher relies on constructing a *pseudo-random permutation* and thereafter extracting a pseudo-random sequence from this permutation. Interestingly, even if the underlying permutation is pseudo-random, if the method of extracting the words from the permutation is not carefully designed, then it may be possible to identify certain biased events in the final keystream of the cipher.

To date, the most popular stream cipher has been RC4, which follows the design principle of extracting pseudo-random bytes from pseudo-random permutations. This cipher gains its popularity for its intriguing simplicity that has made it widely accepted for numerous software and web applications. In this paper, we study and analyze some important non-random events of the RC4 stream cipher, thereby illustrating some key design vulnerabilities in the shuffle-exchange paradigm.

1.1. *RC4 Stream Cipher*

RC4 is the most widely deployed commercial stream cipher, having applications in network protocols such as SSL, WEP, WPA and in Microsoft Windows, Apple OCE, Secure SQL, etc. It was designed in 1987 by Ron Rivest for RSA Data Security (now

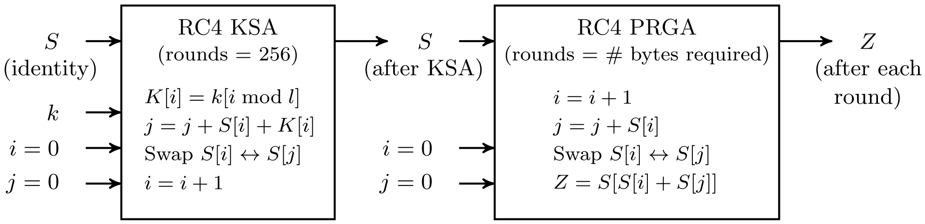

Fig. 1. Key Scheduling Algorithm (KSA) and Pseudo-Random Generation Algorithm (PRGA) of RC4.

RSA Security). The design was a trade secret since then, and was anonymously posted on the web in 1994. Later, the public description was verified by comparing the outputs of the posted design with those of the licensed systems using proprietary versions of the original cipher, although the public design has never been officially approved or claimed by RSA Security to be the original cipher.

The cipher consists of two major components, the Key Scheduling Algorithm (KSA) and the Pseudo-Random Generation Algorithm (PRGA). The internal state of RC4 contains a permutation of all 8-bit words, i.e., a permutation of $N = 256$ bytes, and the KSA produces the initial pseudo-random permutation of RC4 by scrambling an identity permutation using the secret key k. The secret key k of RC4 is of length typically 5 to 32 bytes, which generates the expanded key K of length $N = 256$ bytes by simple repetition. If the length of the secret key k is l bytes (typically $5 \le l \le 32$), then the expanded key K is constructed as $K[i] = k[i \bmod l]$ for $0 \le i \le N - 1$. The initial permutation S produced by the KSA acts as an input to the PRGA that generates the keystream. The RC4 algorithms KSA and PRGA are as shown in Fig. 1.

Notation For round $r = 1, 2, \ldots$ of RC4 PRGA, we denote the indices by i_r, j_r, the permutations before and after the swap by S_{r-1} and S_r respectively, the output byte-extraction index as $t_r = S_r[i_r] + S_r[j_r]$, and the keystream output byte by $Z_r = S_r[t_r]$. After r rounds of KSA, we denote the state variables by adding a superscript K to each variable. By S_0^K and S_0 we denote the initial permutations before KSA and PRGA, respectively. Note that S_0^K is the identity permutation and $S_0 = S_N^K$ is the permutation obtained right after the completion of KSA. We denote the length of the secret key k as l. In this paper, all arithmetic operations in the context of RC4 are to be considered modulo N, unless specified otherwise.

1.2. *An Overview of RC4 Cryptanalysis*

The goal of RC4, like all stream ciphers, is to produce a pseudo-random sequence of bits from the internal permutation. Hence, one of the main ideas for RC4 cryptanalysis is to investigate for *biases*, that is, statistical weaknesses that can be exploited to computationally distinguish the keystream of RC4 from a truly random sequence of bytes with a considerable probability of success.

The target of an attack may be to exploit the non-randomness in the internal state of RC4, or the non-randomness of byte-extraction from the internal permutation. Both ideas have been put to practice in various ways in the literature, and the main theme of attacks on RC4 can be categorized in four major directions, as follows.

1. *Weak keys and Key recovery from state*: Weaknesses of RC4 keys and KSA have attracted quite a lot of attention from the community. In particular, Roos [27] and Wagner [37] showed that for specific properties of a 'weak' secret key, certain undesirable biases occur in the internal state and in the keystream. Grosul and Wallach [11] demonstrated that certain related-key pairs generate similar output bytes in RC4. Later, Matsui [21] reported colliding key pairs for RC4 for the first time and then stronger key collisions were found by Chen and Miyaji [5].

   A direct approach for key recovery from the internal permutation of RC4 was first proposed by Paul and Maitra [26], and was later studied by Biham and Carmeli [4], Khazaei and Meier [13], Akgün, Kavak and Demirci [1], and Basu, Maitra, Paul and Talukdar [3].
2. *Key recovery from the keystream*: Key recovery from the keystream primarily exploits the use of RC4 in WEP and WPA. The analysis by Fluhrer, Mantin and Shamir [7] and Mantin [20] are applicable towards RC4 in WEP mode, and there are quite a few practical attacks [14,29–31,35,36] on the WEP protocol as well. After a practical breach of WEP by Tews, Weinmann and Pyshkin [34] in 2007, the new variant WPA came into the picture. This too used RC4 as a backbone, and the most recent result published by Sepehrdad, Vaudenay and Vuagnoux [31] mounts a distinguishing attack as well as a key recovery attack on RC4 in WPA mode. Sepehrdad's Ph.D. thesis [29] presents a thorough and revised analysis of the most recent WEP and WPA attacks published in Refs. [30,31].
3. *State recovery attacks*: The huge state-space of RC4 ($256! \times 256^2 \approx 2^{1700}$ for $N = 256$) makes a state-recovery attack quite challenging for this cipher. The first important state recovery attack was due to Knudsen, Meier and Preneel [15], with complexity 2^{779}. After a series of improvements by Mister and Tavares [24], Golic [9], Shiraishi, Ohigashi and Morii [32], and Tomasevic, Bojanic and Nieto-Taladriz [33], the best attack with complexity 2^{241} was published by Maximov and Khovratovich [22]. Due to this, a secret key of length beyond 30 bytes is not practically meaningful. A contemporary result by Golic and Morgari [10] claims to improve the attack of Ref. [22] even further by iterative probabilistic reconstruction of the RC4 internal states.
4. *Biases and Distinguishers*: Most of the results in this category are targeted towards specific short-term (involving only the initial few bytes of the output) biases and correlations [8,12,16,18,23,25,27,30], while there exist only a few important results for long-term (prominent even after discarding an arbitrary number of initial bytes of the output) biases [2,6,8,19].

Figure 2 gives a chronological summary of the important cryptanalytic results on RC4 to date.

Before summarizing our contributions, let us now present a brief outline explaining how many keystream bytes are required to identify a bias with a good success probability. For a stream cipher, if there is an event such that the probability of occurrence of the event is different from that in case of a uniformly random sequence of bits, the event is said to be *biased*. If there exists a biased event based only on the bits of the keystream, then such an event gives rise to a *distinguisher* for the cipher that can computationally differentiate between the keystream of the cipher and a random sequence of bits. The

	Weak keys and Key recovery from state	Key recovery from keystream	State recovery attacks	Biases and Distinguishers
1995	◇ Roos weak keys [29] ◇ Wagner weak keys [39]			◇ Roos biases [29]
1996				◇ Glimpse bias [12]
1997				◇ Golic long-term bias [8]
1998			◇ Branch and Bound [15] ◇ Cycle structures [25]	
2000	◇ Related-keys [11]		◇ Iterative probabilistic cryptanalysis [9]	◇ Digraph probabilities [6]
2001		◇ FMS WEP attack [7]		◇ Broadcast attack [19]
2002				◇ Non-random Z_1 [24]
2003			◇ Partial known state [34]	
2005		◇ Mantin WEP att. [21]		◇ Mantin's *ABSAB* [20]
2006		◇ Klein WEP attack [14]		
2007	◇ Modular Equations [28]	◇ TWP WEP attack [36] ◇ VV WEP attack [38]	◇ Hill climbing search [35]	◇ Key-Keystream correlation [27]
2008	◇ Difference Equations [4] ◇ Bit by bit approach [13] ◇ Key Byte Grouping [1]		◇ Generative pattern [23] ◇ Iterative probabilistic reconstruction [10]	◇ Nested state entries [16] ◇ New long-term bias (conditional) [2]
2009	◇ Key collisions [22] ◇ Bidirectional search [3]	◇ TB WEP & WPA attacks [37]		
2010				◇ SVV biases in key and state variables [32]
2011	◇ Key collisions [5]	◇ SVV WEP & WPA attacks [33]		◇ Keylength biases [30] ◇ Broadcast revisited [17] ◇ WPA distinguisher [33]
2012		◇ SVV WEP & WPA attacks (revised) [31]		

Fig. 2. A chronological summary of RC4 cryptanalysis.

efficiency of the distinguishers is mostly judged by the number of samples required to identify the bias.

Let E be an event based on some key bits or state bits or keystream bits or a combination of them in a stream cipher. Suppose, $\Pr(E) = p$ for a uniformly random sequence of bits, and $\Pr(E) = p(1 + q)$ for the keystream of the stream cipher under consideration. The cryptanalytic motivation of studying a stream cipher is to distinguish these two sequences in terms of the difference in the above probabilities when p is small and $q \neq 0$. One may refer to Ref. [18] to note that one requires approximately $1/pq^2$ many samples to identify the bias with a success probability 0.78 which is reasonably higher than half.

1.3. *Our Contributions*

In this paper, we extend and supplement the literature of RC4 cryptanalysis by introducing the concept of keylength-dependent biases, identifying new short-term biases, and by investigating for new long-term biases in RC4. Sections 2, 3 and 4 contain the technical results of this paper.

Section 2: In SAC 2010, Sepehrdad, Vaudenay and Vuagnoux [30] reported the empirical bias $\Pr(S_{16}[j_{16}] = 0 \mid Z_{16} = -16) = 0.038488$ and mentioned that no explanation of this bias could be found. A related bias of the same order involving the event $(S_{17}^K[16] = 0 \mid Z_{16} = -16)$ has been empirically reported in Ref. [29, Sect. 6.1], and this has been used to mount WEP and WPA attacks on RC4. Our detailed experimentation suggests that the number 16 in both the events comes from the keylength of 16 bytes with which the experiments were performed in Refs. [29,30] and similar biases hold for any length of the secret key. *For the first time, we present a proof of these keylength-dependent conditional biases in RC4.*

Along the same line of investigation, we establish some new keylength-dependent conditional biases. These include a strong correlation between the length l of the secret key and the lth byte in the keystream (typically, for $5 \leq l \leq 32$), and thus we propose a method to *predict the keylength of the cipher by observing the keystream.*

Section 3: In this section, we provide *theoretical proofs for some significant empirical biases* of RC4 involving the state variables in the initial rounds, that were reported by Sepehrdad, Vaudenay and Vuagnoux [30] in SAC 2010. In addition, we rigorously study the non-randomness of index j to find a strong bias of j_2 towards 4. We further use this bias to establish a correlation between the state variable $S_2[2]$ and the output keystream byte Z_2.

Section 4: In this section, we investigate and discuss biases related to the RC4 keystream.

4.1 In CRYPTO 2002, Mironov [23] observed that the first byte Z_1 of RC4 keystream has a negative bias towards zero, and also found an interesting non-uniform probability distribution (similar to a sine curve) for all other values of this byte. However, the theoretical proof remained open for almost a decade. In Sect. 4.1, for the first time we derive the *complete theoretical distribution of* Z_1.

4.2 In FSE 2001, Mantin and Shamir [18] proved the bias $\Pr(Z_2 = 0) \approx \frac{2}{N}$, and claimed that no such bias exists in any subsequent byte in the keystream. Contrary to this claim, we prove in Sect. 4.2 that *all the bytes* 3 *to* 255 *of RC4 initial keystream are biased towards zero.*

4.3 Biases in initial rounds of RC4 have no effect if one throws away some initial bytes from the keystream of RC4. This naturally motivates a quest for *long-term* biases in the RC4 output, if any exists. In Sect. 4.3, we observe and prove a *new long-term bias* in RC4 keystream.

2. Biases Based on the Length of the Secret Key

In this section, we present a family of biases in RC4 that are dependent on the length of the secret key, and thereby try to predict the keylength of RC4. Our motivation arises from the conditional bias $\Pr(S_{16}[j_{16}] = 0 \mid Z_{16} = -16) \approx 0.038488$ observed by Sepehrdad, Vaudenay and Vuagnoux [30]. They also mentioned in Ref. [30, Sect. 3] that no explanation for this bias could be found. For direct exploitation in WEP and WPA attacks, a related KSA version of this bias (of the same order) was reported in Ref. [29, Sect. 6.1] for the event $(S_{17}^K[16] = 0 \mid Z_{16} = -16)$.

While exploring these conditional biases in RC4 PRGA, we ran extensive experiments (1 billion runs of RC4 with randomly chosen keys in each case) with $N = 256$ and keylength $5 \le l \le 32$. We could observe that the biases actually correspond to the keylength l:

$$\begin{aligned} &\Pr\big(S_l[j_l] = 0 \mid Z_l = -l\big) \approx \eta_l^{(1A)}/256, \\ &\Pr\big(S_{l+1}^K[l] = 0 \mid Z_l = -l\big) \approx \eta_l^{(1B)}/256, \end{aligned} \tag{1}$$

where each of $\eta_l^{(1A)}$ and $\eta_l^{(1B)}$ decreases from 12 to 7 (approx.) as l increases from 5 to 32. In this section, we present proofs of these two biases for the first time.

We also observe and prove a *family of new conditional biases*. Experimenting with 1 billion runs of RC4 in each case, we observed that:

$$\begin{aligned} &\Pr\big(Z_l = -l \mid S_l[j_l] = 0\big) \approx \eta_l^{(2)}/256, \\ &\Pr\big(S_l[l] = -l \mid S_l[j_l] = 0\big) \approx \eta_l^{(3)}/256, \\ &\Pr\big(t_l = -l \mid S_l[j_l] = 0\big) \approx \eta_l^{(4)}/256, \\ &\Pr\big(S_l[j_l] = 0 \mid t_l = -l\big) \approx \eta_l^{(5)}/256, \end{aligned} \tag{2}$$

where $\eta_l^{(2)}$ decreases from 12 to 7 (approx.), each of $\eta_l^{(3)}$ and $\eta_l^{(4)}$ decreases from 34 to 22 (approx.), and $\eta_l^{(5)}$ decreases from 30 to 20 (approx.) as l increases from 5 to 32.

We also find a *keylength distinguisher* for RC4, based on the following event.

$$(Z_l = -l) \quad \text{for } 5 \le l \le 32. \tag{3}$$

2.1. *Technical Results Required to Prove the Biases*

For the proofs of the biases in this section we need some additional technical results that we present here. Some of these results would also be referred for our results in subsequent sections. We start with Ref. [17, Theorem 6.2.1], restated as Proposition 1 below.

Proposition 1. *At the end of RC4 KSA, for* $0 \le u \le N-1$, $0 \le v \le N-1$,

$$\Pr\big(S_0[u] = v\big) = \begin{cases} \frac{1}{N}\big((\frac{N-1}{N})^v + (1 - (\frac{N-1}{N})^v)(\frac{N-1}{N})^{N-u-1}\big), & \textit{if } v \le u; \\[2ex] \frac{1}{N}\big((\frac{N-1}{N})^{N-u-1} + (\frac{N-1}{N})^v\big), & \textit{if } v > u. \end{cases}$$

Now, we extend the above result to the end of the first round of the PRGA. Since the KSA ends with $i^K = N-1$ and the PRGA begins with $i = 1$, skipping the index 0 of RC4 permutation, this extension is non-trivial, as would be clear from the proof of Lemma 1. Note that this is a revised version of Ref. [28, Lemma 1].

Lemma 1. *After the first round of RC4 PRGA, the probability* $\Pr(S_1[u]=v)$ *is*:

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

Proof. First, let us represent the probability as $\Pr(S_1[u]=v)=\sum_{X=0}^{N-1}\Pr(S_0[1]=X\wedge S_1[u]=v)$. The goal is to reduce all probabilities in terms of expressions over S_0. After the first round of RC4 PRGA, all positions of S_0, except for $i_1=1$ and $j_1=S_0[1]=X$, remain fixed in S_1. So, we need to be careful about the cases where $X=1,u,v$. Let us separate these cases and write

$$\begin{aligned}\Pr\big(S_1[u]=v\big)=&\Pr\big(S_0[1]=1\wedge S_1[u]=v\big)+\Pr\big(S_0[1]=u\wedge S_1[u]=v\big)\\ &+\Pr\big(S_0[1]=v\wedge S_1[u]=v\big)\\ &+\sum_{X\neq 1,u,v}\Pr\big(S_0[1]=X\wedge S_1[u]=v\big).\end{aligned}\tag{4}$$

Now, depending on the values of u,v, we get a few special cases. In the first PRGA round,

$$S_1[u]=\begin{cases}S_1[i_1]=S_0[j_1]=S_0[S_0[1]], & u=i_1=1;\\ S_1[j_1]=S_0[i_1]=S_0[1]=u, & u=j_1=S_0[1];\\ S_0[u], & \text{otherwise}.\end{cases}$$

This indicates that one needs to consider two special cases, $u=1$ and $u=v$, separately. However, there is an overlap within these two cases at the point $(u=1,v=1)$, which in turn, should be considered on its own. In total, we have fours cases to consider for (4), as shown in Fig. 3.

Common point $u=1,v=1$**:** In this case, $S_0[1]=X=1$ implies no swap, resulting in $S_1[u]=S_1[1]=S_0[1]$. If $X\neq 1$, we have $S_1[u]=S_1[1]=S_0[X]$. Thus, (4) reduces

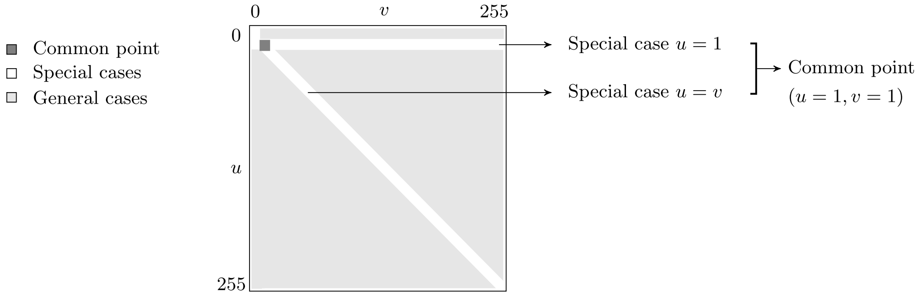

Fig. 3. u,v dependent special cases and range of sums for evaluation of $\Pr(S_1[u]=v)$ in terms of S_0.

to

$$\begin{aligned}\Pr\bigl(S_1[1]=1\bigr) &= \Pr\bigl(S_0[1]=1 \wedge S_0[1]=1\bigr) + \sum_{X\neq 1} \Pr\bigl(S_0[1]=X \wedge S_0[X]=1\bigr)\\ &= \Pr\bigl(S_0[1]=1\bigr) + \sum_{X\neq 1} \Pr\bigl(S_0[1]=X \wedge S_0[X]=1\bigr).\end{aligned}$$

Special case $u=1, v\neq 1$: In this case, $S_0[1]=X=1$ implies $S_1[u]=S_1[1]=S_0[1]$, as before, and $S_0[1]=X=v$ implies $S_1[u]=S_1[1]=S_0[v]$. If $X\neq 1, v$, we have $S_1[u]=S_1[1]=S_0[X]$. Thus,

$$\begin{aligned}\Pr\bigl(S_1[1]=v\bigr) &= \Pr\bigl(S_0[1]=1 \wedge S_0[1]=v\bigr) + \Pr\bigl(S_0[1]=1 \wedge S_0[v]=1\bigr)\\ &\quad + \sum_{X\neq 1,v} \Pr\bigl(S_0[1]=X \wedge S_0[X]=v\bigr)\\ &= 0+0+\sum_{X\neq 1,v} \Pr\bigl(S_0[1]=X \wedge S_0[X]=v\bigr).\end{aligned}$$

Special case $u\neq 1, v=u$: In this case, $S_0[1]=X=1$ implies no swap, resulting in $S_1[u]=S_0[u]$. Again, $S_0[1]=X=u$ implies $S_1[u]=S_0[1]$, and if $X\neq 1, u$, we have $S_1[u]=S_0[u]$. Thus,

$$\begin{aligned}\Pr\bigl(S_1[u]=u\bigr) &= \Pr\bigl(S_0[1]=1 \wedge S_0[u]=u\bigr) + \Pr\bigl(S_0[1]=u \wedge S_0[1]=u\bigr)\\ &\quad + \sum_{X\neq 1,u} \Pr\bigl(S_0[1]=X \wedge S_0[u]=u\bigr)\\ &= \Pr\bigl(S_0[1]=u\bigr) + \sum_{X\neq u} \Pr\bigl(S_0[1]=X \wedge S_0[u]=u\bigr).\end{aligned}$$

General case $u\neq 1, v\neq u$: In this case, $S_0[1]=X=1$ implies no swap, resulting in $S_1[u]=S_0[u]$. Again, $S_0[1]=X=u$ implies $S_1[u]=S_0[1]$, and if $X\neq 1, u$, we have $S_1[u]=S_0[u]$. Thus,

$$\begin{aligned}\Pr\bigl(S_1[u]=v\bigr) &= \Pr\bigl(S_0[1]=1 \wedge S_0[u]=v\bigr) + \Pr\bigl(S_0[1]=u \wedge S_0[1]=v\bigr)\\ &\quad + \Pr\bigl(S_0[1]=v \wedge S_0[u]=v\bigr) + \sum_{X\neq 1,u,v} \Pr\bigl(S_0[1]=X \wedge S_0[u]=v\bigr)\\ &= \Pr\bigl(S_0[1]=1 \wedge S_0[u]=v\bigr) + 0 + 0\\ &\quad + \sum_{X\neq 1,u,v} \Pr\bigl(S_0[1]=X \wedge S_0[u]=v\bigr)\\ &= \sum_{X\neq u,v} \Pr\bigl(S_0[1]=X \wedge S_0[u]=v\bigr).\end{aligned}$$

Combining all the above cases together, we obtain the desired result. □

The probabilities depending on S_0 can be derived from Proposition 1. The estimation of the joint probabilities $\Pr(S_0[u] = v \wedge S_0[u'] = v')$ is also required for our next result, i.e., Theorem 1, as well as for our results in Sect. 4.1. This estimation is explained in detail in Sect. 4.1.3.

In Theorem 1, we find the probability distribution of $S_{u-1}[u] = v$, just before index i touches the position u during PRGA. This is a generalization of Ref. [28, Theorem 4].

Theorem 1. *In RC4 PRGA, for* $3 \leq u \leq N - 1$,

$$\Pr\big(S_{u-1}[u] = v\big) \approx \Pr\big(S_1[u] = v\big)\left(1 - \frac{1}{N}\right)^{u-2} + \sum_{t=2}^{u-1}\sum_{w=0}^{u-t} \frac{\Pr(S_1[t] = v)}{w! \cdot N}\left(\frac{u-t-1}{N}\right)^{w}\left(1 - \frac{1}{N}\right)^{u-3-w}.$$

Proof. From Lemma 1, we know that the event $\Pr(S_1[u] = v)$ is positively biased for all u. Hence the natural path for investigation is as follows:

$$\Pr\big(S_{u-1}[u] = v\big) = \Pr\big(S_{u-1}[u] = v \mid S_1[u] = v\big) \cdot \Pr\big(S_1[u] = v\big) + \Pr\big(S_{u-1}[u] = v \mid S_1[u] \neq v\big) \cdot \Pr\big(S_1[u] \neq v\big).$$

Case $(S_1[u] = v)$: Index i varies from 2 to $(u - 1)$ during the evolution of S_1 to S_{u-1}, and hence never touches the uth index. Thus, the index u will retain its value $S_1[u]$ if index j does not touch it. The probability of this event is $(1 - 1/N)^{u-2}$ over all the intermediate rounds. Hence we get:

$$\Pr\big(S_{u-1}[u] = v \mid S_1[u] = v\big) \cdot \Pr\big(S_1[u] = v\big) = \left(1 - \frac{1}{N}\right)^{u-2} \cdot \Pr\big(S_1[u] = v\big).$$

Case $(S_1[u] \neq v)$: Suppose that $S_1[t] = v$ for some $t \neq u$. In such a case, only a swap between the positions u and t during rounds 2 to $(u - 1)$ of PRGA can result in $(S_{u-1}[u] = v)$. If index i does not touch the tth location, then the value at $S_1[t]$ can only go to some position behind $i \leq u - 1$, and can never reach $S_{u-1}[u]$. Thus we must have i touching the tth position, i.e., $2 \leq t \leq u - 1$.

Now suppose that it requires $(w + 1)$ hops for v to reach from $S_1[t]$ to $S_{u-1}[u]$. The transfer will never happen if the position t swaps with any index which is not touched by i later. This fraction of favorable positions start from $(u - t - 1)/N$ for the first hop and decreases approximately to $(u - t - 1)/(lN)$ at the lth hop. It is also required that j does not touch the position u for the remaining $(u - 3 - w)$ rounds. Thus, the second part of the probability for a specific position t is:

$$\Pr\big(S_1[t] = v\big)\left(\prod_{l=1}^{w} \frac{u-t-1}{lN}\right)\left(1 - \frac{1}{N}\right)^{u-3-w} = \frac{\Pr(S_1[t] = v)}{w! \cdot N}\left(\frac{u-t-1}{N}\right)^{w}\left(1 - \frac{1}{N}\right)^{u-3-w}.$$

Finally, the number of hops is bounded as $1 \le w+1 \le u-t+1$ (here $w+1=1$ or $w=0$ denotes a single-hop transfer), depending on the initial gap between t and u positions. Summing over all t,k with their respective bounds, we get the desired expression for $\Pr(S_{u-1}[u]=v)$. □

2.2. *Proofs of the Keylength-Dependent Biases in (2)*

Observation of the biases (2) was first reported in Ref. [28, Sect. 3], but without any proof. In this section, we present complete proofs of all these biases. Although the biases are all conditional in nature, for ease of understanding we first compute the associated joint probabilities and then discuss how the conditional probabilities can be computed. All the biases that we are interested in are related to $(S^K_{l+1}[l-1] = -l \wedge S^K_{l+1}[l] = 0)$. So we first derive the probability for this event.

Lemma 2. *Suppose that l is the length of the secret key of RC4. Then we have*

$$\Pr\big(S^K_{l+1}[l-1] = -l \wedge S^K_{l+1}[l] = 0\big) \approx \frac{1}{N^2} + \left(1 - \frac{1}{N^2}\right)\alpha_l,$$

$$\textit{where } \alpha_l = \frac{1}{N}\left(1 - \frac{3}{N}\right)^{l-2}\left(1 - \frac{l+1}{N}\right).$$

Proof. The major path that leads to the target event is as follows.

- In the first round of the KSA, when $i^K_1 = 0$ and $j^K_1 = K[0]$, the value 0 is swapped into the index $S^K[K[0]]$ with probability 1.
- The index $j^K_1 = K[0] \notin \{l-1, l, -l\}$, so that the values $l-1, l, -l$ at these indices respectively are not swapped out in the first round of the KSA. We as well require $K[0] \notin \{1, \ldots, l-2\}$, so that the value 0 at index $K[0]$ is not touched by these values of i^K during the next $l-2$ rounds of the KSA. This happens with probability $(1 - \frac{l+1}{N})$.
- From round 2 to $l-1$ (i.e., for $i^K = 1$ to $l-2$) of the KSA, none of $j^K_2, \ldots, j^K_{l-1}$ touches the three indices $\{l, -l, K[0]\}$. This happens with probability $(1 - \frac{3}{N})^{l-2}$.
- In round l of the KSA, when $i^K_l = l-1$, j^K_l becomes $-l$ with probability $\frac{1}{N}$, thereby moving $-l$ into index $l-1$.
- In round $l+1$ of the KSA, when $i^K_{l+1} = l$, j^K_{l+1} becomes $j^K_l + S^K_l[l] + K[l] = -l + l + K[0] = K[0]$, and as discussed above, this index contains the value 0. Hence, after the swap, $S^K_{l+1}[l] = 0$. Since $K[0] \neq l-1$, we have $S^K_{l+1}[l-1] = -l$.

Considering the above events to be independent, the probability that all of above occur together is given by $\alpha_l = \frac{1}{N}(1 - \frac{3}{N})^{l-2}(1 - \frac{l+1}{N})$. If the above path does not occur, then the target event happens due to random association, with probability $\frac{1}{N^2}$, thus contributing a probability of $(1-\alpha_l)\frac{1}{N^2}$. Adding the two contributions, the result follows. □

Now we may derive the joint probabilities associated with the conditional events of (2), as follows.

Theorem 2. *Suppose that l is the length of the secret key of RC4. Then we have*

$$\Pr\big(S_l[l] = -l \wedge S_l[j_l] = 0\big) = \Pr\big(t_l = -l \wedge S_l[j_l] = 0\big) \approx \frac{1}{N^2} + \left(1 - \frac{1}{N^2}\right)\beta_l,$$

where $\beta_l = \frac{1}{N}(1 - \frac{1}{N})(1 - \frac{2}{N})^{N-3}(1 - \frac{3}{N})^{l-2}(1 - \frac{l+1}{N})$.

Proof. From the proof of Lemma 2, consider the major path with probability α_l for the event $(S^K_{l+1}[l-1] = -l \wedge S^K_{l+1}[l] = 0)$. For the remaining $N - l - 1$ rounds of the KSA and for the first $l - 2$ rounds of the PRGA (i.e., for a total of $N - 3$ rounds), none of the values of j^K (corresponding to the KSA rounds) or j (corresponding to the PRGA rounds) should touch the indices $\{l-1, l\}$. This happens with a probability of $(1 - \frac{2}{N})^{N-3}$.

Now, in round $l - 1$ of PRGA, $i_{l-1} = l - 1$, from where the value $-l$ moves to index j_{l-1} due to the swap. In the next round, $i_l = l$ and $j_l = j_{l-1} + S_{l-1}[l] = j_{l-1}$, provided the value 0 at index l had not been swapped out by j_{l-1}, the probability of which is $1 - \frac{1}{N}$. So during the next swap, the value $-l$ moves from index j_l to index l and the value 0 moves from index l to j_l. The probability of the above major path leading to the event $(S_l[l] = -l \wedge S_l[j_l] = 0)$ is given by $\beta_l = \alpha_l(1 - \frac{2}{N})^{N-3}(1 - \frac{1}{N})$. If this path does not occur, then there is always a chance of $\frac{1}{N^2}$ for the target event to happen due to random association. Adding the two contributions and substituting the value of α_l from Lemma 2, the result follows.

Further, as $t_l = S_l[l] + S_l[j_l]$, the event $(S_l[l] = -l \wedge S_l[j_l] = 0)$ is equivalent to the event $(t_l = -l \wedge S_l[j_l] = 0)$, and hence the result. □

Theorem 3. *Suppose that l is the length of the secret key of RC4. Then we have*

$$\Pr\big(Z_l = -l \wedge S_l[j_l] = 0\big) \approx \frac{1}{N^2} + \left(1 - \frac{1}{N^2}\right)\gamma_l,$$

where $\gamma_l = \frac{1}{N^2}(1 - \frac{l+1}{N})\sum_{x=l+1}^{N-1}(1 - \frac{1}{N})^x(1 - \frac{2}{N})^{x-l}(1 - \frac{3}{N})^{N-x+2l-4}$.

Proof. From the PRGA update rule, we have $j_l = j_{l-1} + S_{l-1}[l]$. Hence, $S_l[j_l] = S_{l-1}[l] = 0$ implies $j_l = j_{l-1}$ as well as $Z_l = S_l[S_l[l] + S_l[j_l]] = S_l[S_{l-1}[j_l] + 0] = S_l[S_{l-1}[j_{l-1}]] = S_l[S_{l-2}[l-1]]$. Thus, the event $(Z_l = -l \wedge S_l[j_l] = 0)$ is equivalent to the event $(S_l[S_{l-2}[l-1]] = -l \wedge S_{l-1}[l] = 0)$.

From the proof of Lemma 2, consider the major path with probability α_l for the joint event $(S^K_{l+1}[l-1] = -l \wedge S^K_{l+1}[l] = 0)$. This constitutes the first part of our main path leading to the target event. The second part, having probability α'_l, can be constructed as follows.

- For an index $x \in [l+1, N-1]$, we have $S^K_x[x] = x$. This happens with probability $(1 - \frac{1}{N})^x$.
- For the KSA rounds $l + 2$ to x, the j^K values do not touch the indices $l - 1$ and l. This happens with probability $(1 - \frac{2}{N})^{x-l-1}$.

- In round $x+1$ of KSA, when $i^K_{x+1} = x$, j^K_{x+1} becomes $l-1$ with probability $\frac{1}{N}$. Due to the swap, the value x moves to $S^K_{x+1}[l-1]$ and the value $-l$ moves to $S^K_{x+1}[x] = S^K_{x+1}[S^K_{x+1}[l-1]]$.
- For the remaining $N-x-1$ rounds of the KSA and for the first $l-1$ rounds of the PRGA, none of the j^K or j values should touch the indices $\{l-1, S[l-1], l\}$. This happens with a probability of $(1-\frac{3}{N})^{N-x+l-2}$.
- So far, we have $(S_{l-1}[S_{l-2}[l-1]] = -l \wedge S_{l-1}[l] = 0)$. Now, we should also have $j_l \notin \{l-1, S[l-1]\}$ for $S_l[S_{l-2}[l-1]] = S_{l-1}[S_{l-2}[l-1]] = -l$. The probability of this condition is $(1-\frac{2}{N})$.

Assuming all the individual events in the above path to be mutually independent, we get $\alpha'_l = \frac{1}{N}\sum_{x=l+1}^{N-1}(1-\frac{1}{N})^x(1-\frac{2}{N})^{x-l}(1-\frac{3}{N})^{N-x+l-2}$. Thus, the probability of the entire path is given by $\gamma_l = \alpha_l \cdot \alpha'_l = \frac{1}{N^2}(1-\frac{l+1}{N})\sum_{x=l+1}^{N-1}(1-\frac{1}{N})^x(1-\frac{2}{N})^{x-l}$ $(1-\frac{3}{N})^{N-x+2l-4}$.

If this path does not occur, then there is always a chance of $\frac{1}{N^2}$ for the target event to happen due to random association. Adding the two contributions, we get the result. □

In order to calculate the conditional probabilities of (2), we need to compute the marginals $\delta_l = \Pr(S_l[j_l] = 0)$ and $\tau_l = \Pr(t_l = -l)$. Our experimental observations reveal that in $5 \le l \le 32$, δ_l does not change much with l, and has a slightly negative bias: $\delta_l \approx 1/N - 1/N^2$. On the other hand, as l varies from 5 to 32, τ_l changes approximately from $1.13/N$ to $1.08/N$. We can derive the exact expression for δ_l as a corollary to Theorem 1, and an expression for τ_l using δ_l.

Corollary 1. *For any keylength l, with $3 \le l \le N-1$, the probability $\Pr(S_l[j_l] = 0)$ is given by*

$$\delta_l \approx \Pr\big(S_1[l] = 0\big)\left(1-\frac{1}{N}\right)^{l-2} + \sum_{t=2}^{l-1}\sum_{w=0}^{l-t}\frac{\Pr(S_1[t]=0)}{w!\cdot N}\left(\frac{l-t-1}{N}\right)^w\left(1-\frac{1}{N}\right)^{l-3-w}.$$

Proof. Note that $S_l[j_l]$ is assigned the value of $S_{l-1}[l]$ due to the swap in round l. Hence, by substituting $u = l$ and $v = 0$ in Theorem 1, we get the result. □

Theorem 4. *Suppose that l is the length of the secret key of RC4. Then we have*

$$\tau_l = \Pr(t_l = -l) \approx \frac{1}{N^2} + \left(1-\frac{1}{N^2}\right)\beta_l + (1-\delta_l)\frac{1}{N},$$

where β_l is given in Theorem 2 and δ_l is given in Corollary 1.

Proof. We can write $\Pr(t_l = -l) = \Pr(t_l = -l \wedge S_l[j_l] = 0) + \Pr(t_l = -l \wedge S_l[j_l] \neq 0)$, where the first term is given by Theorem 2. When $S_l[j_l] \neq 0$, the event $(t_l = -l)$ can be assumed to occur due to random association. Hence the second term can be computed as $\Pr(S_l[j_l] \neq 0) \cdot \Pr(t_l = -l \mid S_l[j_l] \neq 0) \approx (1-\delta_l)\frac{1}{N}$. Adding the two terms, we get the result. □

Theoretical values for both δ_l and τ_l match closely with the experimental ones for all values of l.

Computing the Conditional Biases in (2) When we divide the joint probabilities $\Pr(S_l[l] = -l \wedge S_l[j_l] = 0)$ and $\Pr(t_l = -l \wedge S_l[j_l] = 0)$ of Theorem 2, and $\Pr(Z_l = -l \wedge S_l[j_l] = 0)$ of Theorem 3 by the appropriate marginals $\delta_l = \Pr(S_l[j_l] = 0)$ of Corollary 1 and $\tau_l = \Pr(t_l = -l)$ of Theorem 4, we get theoretical values for all the biases in (2). The theoretical values closely match with the experimental observations reported in the beginning of Sect. 2.

2.3. *Bias in* $(Z_l = -l)$ *and Keylength Prediction from Keystream*

First, we prove the bias in (3) and thereby show how to predict the length l of RC4 secret key. Next, we use the marginal probability $\Pr(Z_l = -l)$ to derive the conditional probabilities of (1).

Theorem 5. *Suppose that l is the length of the secret key of RC*4. *Then we have*

$$\Pr(Z_l = -l) \approx \frac{1}{N^2} + \left(1 - \frac{1}{N^2}\right)\gamma_l + (1 - \delta_l)\frac{1}{N},$$

where γ_l is given in Theorem 3 *and δ_l is given in Corollary* 1.

Proof. We can write $\Pr(Z_l = -l) = \Pr(Z_l = -l \wedge S_l[j_l] = 0) + \Pr(Z_l = -l \wedge S_l[j_l] \neq 0)$, where the first term is given by Theorem 3. When $S_l[j_l] \neq 0$, the event $(Z_l = -l)$ can be assumed to occur due to random association. Hence the second term can be computed as $\Pr(S_l[j_l] \neq 0) \cdot \Pr(Z_l = -l \mid S_l[j_l] \neq 0) \approx (1 - \delta_l)\frac{1}{N}$. Adding the two terms, we get the result. □

It is important to note that the estimate of $\Pr(Z_l = -l)$ is always greater than $1/N + 1/N^2 \approx 0.003922$ for $N = 256$ and $5 \leq l \leq 32$. In Fig. 4, we plot the theoretical as well as the experimental values of $\Pr(Z_l = -l)$ against l for $5 \leq l \leq 32$, where the experiments have been run over 1 billion trials of RC4 PRGA, with randomly generated keys.

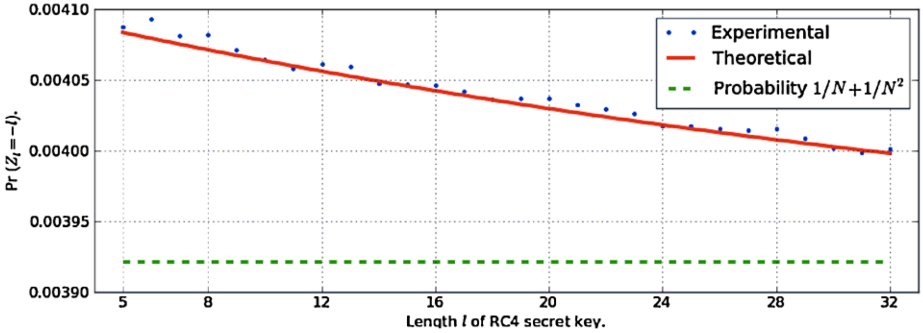

Fig. 4. Distribution of $\Pr(Z_l = -l)$ for different lengths $5 \leq l \leq 32$ of the RC4 secret key.

Keylength Distinguisher From this estimate, we immediately get a distinguisher of RC4 that can effectively distinguish the output keystream of the cipher from a random sequence of bytes. For the event $E : (Z_l = -l)$, the bias proved in Theorem 5 can be written as $p(1 + q)$, where $p = 1/N$ and $q > 1/N$ for $5 \le l \le 32$ and $N = 256$. Thus, the number of samples required to distinguish RC4 from random sequence of bits with a constant probability of success is approximately $\frac{1}{pq^2} = N^3$. Using this distinguisher, one may predict the length l of RC4 secret key from the output keystream.

Proofs of the Keylength-Dependent Biases in (1) To prove the conditional biases in (1), we first compute the associated joint probabilities $\Pr(S_l[j_l] = 0 \wedge Z_l = -l)$ and $\Pr(S^K_{l+1}[l] = 0 \wedge Z_l = -l)$, and then use the marginal $\Pr(Z_l = -l)$ to obtain the final results. The first joint probability is already computed in Theorem 3, and the second one is computed as follows.

Theorem 6. *Suppose that l is the length of the secret key of RC4. Then we have*

$$\begin{aligned}&\Pr\big(Z_l = -l \wedge S^K_{l+1}[l] = 0\big)\\ &\approx \left(\frac{1}{N^2} + \left(1 - \frac{1}{N^2}\right)\alpha_l\right) \cdot \alpha'_l + \left(1 - \frac{1}{N} - \left(1 - \frac{1}{N^2}\right)\alpha_l\right) \cdot \frac{1}{N^2},\end{aligned}$$

where α_l is given in Lemma 2 and α'_l is given in Theorem 3.

Proof. We consider the main path in this case to be $\Pr(S^K_{l+1}[l-1] = -l \wedge S^K_{l+1}[l] = 0)$, which occurs with probability $\frac{1}{N^2} + (1 - \frac{1}{N^2})\alpha_l$, as in Lemma 2. We also need to compute $\Pr(S^K_{l+1}[l-1] = -l)$. Since i^K in round $l+1$ has touched the index l, the value at this position can be assumed to be random. Thus, we may assume $\Pr(S^K_{l+1}[l] = 0) \approx \frac{1}{N}$, and hence

$$\begin{aligned}&\Pr\big(S^K_{l+1}[l-1] = -l\big)\\ &\quad= \Pr\big(S^K_{l+1}[l-1] = -l \wedge S^K_{l+1}[l] = 0\big) + \Pr\big(S^K_{l+1}[l-1] = -l \wedge S^K_{l+1}[l] \neq 0\big)\\ &\quad= \frac{1}{N^2} + \left(1 - \frac{1}{N^2}\right)\alpha_l + \Pr\big(S^K_{l+1}[l] \neq 0\big) \cdot \Pr\big(S^K_{l+1}[l-1] = -l \mid S^K_{l+1}[l] \neq 0\big)\\ &\quad\approx \frac{1}{N^2} + \left(1 - \frac{1}{N^2}\right)\alpha_l + \left(1 - \frac{1}{N}\right)\frac{1}{N} = \frac{1}{N} + \left(1 - \frac{1}{N^2}\right)\alpha_l.\end{aligned}$$

Now, we may compute the main probability $\Pr(Z_l = -l \wedge S^K_{l+1}[l] = 0)$, as follows:

$$\begin{aligned}&\Pr\big(Z_l = -l \wedge S^K_{l+1}[l] = 0 \wedge S^K_{l+1}[l-1] = -l\big)\\ &\qquad+ \Pr\big(Z_l = -l \wedge S^K_{l+1}[l] = 0 \wedge S^K_{l+1}[l-1] \neq -l\big)\\ &\quad= \Pr\big(S^K_{l+1}[l] = 0 \wedge S^K_{l+1}[l-1] = -l\big) \cdot \Pr\big(Z_l = -l \mid S^K_{l+1}[l] = 0 \wedge S^K_{l+1}[l-1] = -l\big)\\ &\qquad+ \Pr\big(S^K_{l+1}[l-1] \neq -l\big) \cdot \Pr\big(Z_l = -l \wedge S^K_{l+1}[l] = 0 \mid S^K_{l+1}[l-1] \neq -l\big).\end{aligned}$$

From Lemma 2 and proof of Theorem 3, the first part is approximated by $(\frac{1}{N^2} + (1 - \frac{1}{N^2})\alpha_l) \cdot \alpha'_l$. In the second part, we assume that when $S^K_{l+1}[l-1] \neq -l$, with probability $1 - \frac{1}{N} - (1 - \frac{1}{N^2})\alpha_l$, then the event $(Z_l = -l \wedge S^K_{l+1}[l] = 0)$ happens due to random association, with probability $\frac{1}{N^2}$. Adding the contributions from the two parts as above, we obtain the result. □

If we divide $\Pr(S_l[j_l] = 0 \wedge Z_l = -l)$ of Theorem 3 and $\Pr(S^K_{l+1}[l] = 0 \wedge Z_l = -l)$ of Theorem 6 by $\Pr(Z_l = -l)$ of Theorem 5, we get the desired conditional probabilities of $(S_l[j_l] = 0 \mid Z_l = -l)$ and $(S^K_{l+1}[l] = 0 \mid Z_l = -l)$ respectively. These theoretical estimates closely match with our experimental observations. For example, in case of $l = 16$, from simulations with 1 billion randomly generated secret keys, we obtained the experimental values of the above probabilities as 9.7/256 and 9.5/256 (approx.) respectively, whereas the theoretical values are close to 9.6/256 for both cases.

3. Biases Involving State Variables in Initial Rounds of RC4 PRGA

In this section, we discuss and prove some empirically observed biases that involve the state variables i, j and S along with to the output keystream Z. We investigate some significant empirical biases discovered and reported by Sepehrdad, Vaudenay and Vuagnoux [30]. We provide theoretical justification only for the biases which are of the approximate order of $2/N$ or more, as in Table 1.

3.1. *Bias at Specific Initial Rounds*

In this section, we first prove the bias labeled "New_noz_014" in Ref. [30, Figs. 3 and 4] and Table 1.

Table 1. Significant biases observed in Ref. [30] and proved in this paper.

Type of bias	Label as in [30]	Biased events observed in [30]*	Probabilities reported in [30]
Bias at specific initial rounds	"New_004"	$j_2 + S_2[j_2] = S_2[i_2] + Z_2$	$2/N$
	"New_noz_007"	$j_2 + S_2[j_2] = 6$	$2.37/N$
	"New_noz_009"	$j_2 + S_2[j_2] = S_2[i_2]$	$2/N$
	"New_noz_014"	$j_1 + S_1[i_1] = 2$	$1.94/N$
Bias at all rounds (round-independent)	"New_noz_001"	$j_r + S_r[i_r] = i_r + S_r[j_r]$	$2/N$
	"New_noz_002"	$j_r + S_r[j_r] = i_r + S_r[i_r]$	$2/N$
Bias at all initial rounds, $1 \leq r \leq N-1$ (round-dependent)	"New_000"	$S_r[t_r] = t_r$	$1.9/N$ at $r = 3$
	"New_noz_004"	$S_r[i_r] = j_r$	$1.9/N$ at $r = 3$
	"New_noz_006"	$S_r[j_r] = i_r$	$2.34/N$ at $r = 3$

*Note that the authors of Ref. [30] denoted the PRGA variables by primed indices, but we do not use that notation.

Theorem 7. *After the first round* $(r = 1)$ *of RC4 PRGA,*

$$\Pr\big(j_1 + S_1[i_1] = 2\big) = \Pr\big(S_0[1] = 1\big) + \sum_{X \neq 1} \Pr\big(S_0[X] = 2 - X \wedge S_0[1] = X\big).$$

Proof. We have $j_1 + S_1[i_1] = S_0[1] + S_0[j_1] = S_0[1] + S_0[S_0[1]]$. We compute the desired probability using the following two conditional paths depending on the value of $j_1 = S_0[1]$:

$$\begin{aligned}\Pr\big(j_1 + S_1[i_1] = 2\big) &= \Pr\big(S_0[1] + S_0\big[S_0[1]\big] = 2 \mid S_0[1] = 1\big) \cdot \Pr\big(S_0[1] = 1\big)\\ &\quad + \sum_{X \neq 1} \Pr\big(S_0[1] + S_0\big[S_0[1]\big] = 2 \mid S_0[1] = X\big) \cdot \Pr\big(S_0[1] = X\big)\\ &= \Pr\big(1 + S_0[1] = 2 \mid S_0[1] = 1\big) \cdot \Pr\big(S_0[1] = 1\big)\\ &\quad + \sum_{X \neq 1} \Pr\big(X + S_0[X] = 2 \mid S_0[1] = X\big) \cdot \Pr\big(S_0[1] = X\big)\\ &= 1 \cdot \Pr\big(S_0[1] = 1\big) + \sum_{X \neq 1} \Pr\big(S_0[X] = 2 - X \wedge S_0[1] = X\big).\end{aligned}$$

□

If we consider the RC4 permutation after the KSA, the probabilities involving S_0 in the expression for $\Pr(j_1 + S_1[i_1] = 2)$ should be evaluated using Proposition 1 and the joint probability should be estimated in the same manner as in Sect. 4.1.3, giving a total probability of approximately $1.937/N$ for $N = 256$. This closely matches the observed value $1.94/N$. If we assume that RC4 PRGA starts with a random initial permutation S_0, the probability turns out to be approximately $2/N - 1/N^2 \approx 1.996/N$ for $N = 256$, i.e., almost twice that of a random occurrence.

Next, we prove the biases “New_noz_007,” “New_noz_ 009” and “New_004,” as in Ref. [30] and Table 1.

Theorem 8. *After the second round* $(r = 2)$ *of RC4 PRGA, the following probability relations hold between the index* j_2 *and the state variables* $S_2[i_2]$, $S_2[j_2]$:

$$\Pr\big(j_2 + S_2[j_2] = 6\big) \approx \Pr\big(S_0[1] = 2\big) + \sum_{X \text{ even},\, X \neq 2} (2/N) \cdot \Pr\big(S_0[1] = X\big), \tag{5}$$

$$\Pr\big(j_2 + S_2[j_2] = S_2[i_2]\big) \approx 2/N - 1/N^2, \tag{6}$$

$$\Pr\big(j_2 + S_2[j_2] = S_2[i_2] + Z_2\big) \approx 2/N - 1/N^2. \tag{7}$$

Proof. We have $j_2 + S_2[j_2] = (j_1 + S_1[i_2]) + S_1[i_2] = S_0[1] + 2 \cdot S_1[2]$ in RC4 PRGA. Now for (5), we have the following paths depending on the value of $j_1 = S_0[1]$:

$$\begin{aligned}\Pr\big(j_2 + S_2[j_2] = 6\big) &= \Pr\big(S_0[1] + 2 \cdot S_1[2] = 6 \mid S_0[1] = 2\big) \cdot \Pr\big(S_0[1] = 2\big)\\ &\quad + \sum_{X \neq 2} \Pr\big(S_0[1] + 2 \cdot S_1[2] = 6 \mid S_0[1] = X\big) \cdot \Pr\big(S_0[1] = X\big).\end{aligned}$$

We explore the conditional events in each of the above paths as follows:

$$\begin{aligned} S_0[1]=2 \quad &\Rightarrow \quad S_0[1]+2\cdot S_1[2] \\ &\qquad = 2+2\cdot S_1[j_1] = 2+2\cdot S_0[i_1] = 2+2\cdot S_0[1]=6, \\ S_0[1]=X\neq 2 \quad &\Rightarrow \quad S_0[1]+2\cdot S_1[2] = X+2\cdot S_1[2]. \end{aligned}$$

To satisfy $X+2\cdot S_1[2]=6$ in the second path, the value of X must be even and for each such value of X, the variable $S_1[2]$ can take two different values, namely $(3+N/2-X/2)$ and $(3+N-X/2)$ modulo N. Thus, we have the following:

$$\Pr\bigl(j_2+S_2[j_2]=6\bigr) = 1\cdot\Pr\bigl(S_0[1]=2\bigr) + \sum_{X \text{ even}, X\neq 2} (2/N)\cdot\Pr\bigl(S_0[1]=X\bigr).$$

In case of (6), we have the following conditional paths depending on the value of $S_1[2]$:

$$\begin{aligned} \Pr\bigl(j_2+S_2[j_2]=S_2[i_2]\bigr) &= \Pr\bigl(S_0[1]+2\cdot S_1[2]=S_1[j_2] \mid S_1[2]=0\bigr)\cdot\Pr\bigl(S_1[2]=0\bigr) \\ &\quad + \Pr\bigl(S_0[1]+2\cdot S_1[2]=S_1[j_2] \mid S_1[2]\neq 0\bigr)\cdot\Pr\bigl(S_1[2]\neq 0\bigr). \end{aligned}$$

In the first case, the condition holds with probability 1, since

$$S_1[2]=0 \quad \Rightarrow \quad \begin{cases} S_0[1]+2\cdot S_1[2]=S_0[1], \text{ and} \\ S_1[j_2]=S_1[S_0[1]+S_1[2]]=S_1[S_0[1]]=S_1[j_1]=S_0[i_1]=S_0[1]. \end{cases}$$

For all other cases in the second path, with $S_1[2]=X\neq 0$, we can assume the condition to hold with probability approximately $1/N$. Thus, we have:

$$\Pr\bigl(j_2+S_2[j_2]=S_2[i_2]\bigr) \approx 1\cdot(1/N)+(1/N)\cdot(1-1/N) = 2/N-1/N^2.$$

For (7), the condition is almost identical to the condition of (6) apart from the inclusion of Z_2. However, our first path $S_1[2]=0$ gives $\Pr(Z_2=0 \mid S_1[2]=0)=1$ (as in [18]), which implies the following:

$$\Pr\bigl(j_2+S_2[j_2]=S_2[i_2]+Z_2 \mid S_1[2]=0\bigr) = \Pr\bigl(j_2+S_2[j_2]=S_2[i_2] \mid S_1[2]=0\bigr).$$

In all other cases with $S_1[2]\neq 0$, we assume the conditions to match uniformly at random. Therefore:

$$\Pr\bigl(j_2+S_2[j_2]=S_2[i_2]+Z_2\bigr) \approx (1/N)\cdot 1+(1-1/N)\cdot(1/N) = 2/N-1/N^2. \quad \square$$

In case of (5), if we assume S_0 to be the initial state for RC4 PRGA, and substitute all probabilities involving S_0 using Proposition 1, we get the total probability equal to $2.36/N$ for $N=256$. This value closely matches with the observed probability $2.37/N$. If we assume S_0 to be a random permutation in (5), we get probability $2/N-2/N^2 \approx 1.992/N$ for $N=256$. The theoretical results are summarized in Table 2 along with the experimentally observed probabilities from Ref. [30].

Table 2. Theoretical and observed biases at specific initial rounds of RC4 PRGA.

Label [30]	Event	Observed probability (reported in [30])	Theoretical probability (for $N=256$)	
			S_0 of RC4	Random S_0
"New_noz_014"	$j_1+S_1[i_1]=2$	$1.94/N$	$1.937/N$	$1.996/N$
"New_noz_007"	$j_2+S_2[j_2]=6$	$2.37/N$	$2.363/N$	$1.992/N$
"New_noz_009"	$j_2+S_2[j_2]=S_2[i_2]$	$2/N$	$1.996/N$	$1.996/N$
"New_noz_004"	$j_2+S_2[j_2]=S_2[i_2]+Z_2$	$2/N$	$1.996/N$	$1.996/N$

3.2. *Round-Independent Biases at All Initial Rounds*

In this section, we turn our attention to the biases labeled "New_ noz_001" and "New_noz_002." In Ref. [30] it was observed that both of these biases exist for all initial rounds ($1 \le r \le N-1$) of RC4 PRGA. In Theorem 9 below, we prove a more general result. We show that actually these biases do not change with r and they continue to persist at the same order of $2/N$ at any arbitrary round of PRGA. Thus, the probabilities for "New_noz_001" and "New_noz_002" from Ref. [30] turn out to be special cases (for $1 \le r \le N-1$) of Theorem 9.

Theorem 9. *At any round* $r \ge 1$ *of RC4 PRGA, the following two relations hold between the indices* i_r, j_r *and the state variables* $S_r[i_r]$, $S_r[j_r]$:

$$\Pr\bigl(j_r + S_r[j_r] = i_r + S_r[i_r]\bigr) \approx 2/N, \tag{8}$$

$$\Pr\bigl(j_r + S_r[i_r] = i_r + S_r[j_r]\bigr) \approx 2/N. \tag{9}$$

Proof. We denote the events as $E_1 : (j_r + S_r[j_r] = i_r + S_r[i_r])$ and $E_2 : (j_r + S_r[i_r] = i_r + S_r[j_r])$. For both the events, we shall take the conditional paths as follows for computing the probabilities:

$$\Pr(E_1) = \Pr(E_1 \mid i_r = j_r) \cdot \Pr(i_r = j_r) + \Pr(E_1 \mid i_r \ne j_r) \cdot \Pr(i_r \ne j_r),$$

$$\Pr(E_2) = \Pr(E_2 \mid i_r = j_r) \cdot \Pr(i_r = j_r) + \Pr(E_2 \mid i_r \ne j_r) \cdot \Pr(i_r \ne j_r).$$

We have $\Pr(i_r = j_r) \approx 1/N$ and $\Pr(E_1 \mid i_r = j_r) = \Pr(E_2 \mid i_r = j_r) = 1$. In the case where $i_r \ne j_r$, we have $S_r[j_r] \ne S_r[i_r]$, as S_r is a permutation. Thus in case $i_r \ne j_r$, the values of $S_r[i_r]$ and $S_r[j_r]$ can be chosen in $N(N-1)$ ways (drawing from a permutation without replacement) to satisfy the events E_1, E_2. This gives the total probability for each event E_1, E_2 approximately as:

$$\Pr(E_1) \approx \Pr(E_2) \approx 1 \cdot \frac{1}{N} + \sum_{j_r \ne i_r} \frac{1}{N(N-1)} = \frac{1}{N} + (N-1) \cdot \frac{1}{N(N-1)} = \frac{2}{N}. \qquad \square$$

Our theoretical results match the probabilities reported in Ref. [30, Fig. 2] for the initial rounds $1 \le r \le N-1$. One may note that the biases in Theorem 9 look somewhat similar to Jenkin's correlations [12]:

$$\Pr\bigl(Z_r = j_r - S_r[i_r]\bigr) \approx 2/N \quad \text{and} \quad \Pr\bigl(Z_r = i_r - S_r[j_r]\bigr) \approx 2/N.$$

However, the biases proved in Theorem 9 do not contain the keystream byte Z_r, and one may check that the results do not follow directly from Jenkin's correlations [12] either.

3.3. *Round-Dependent Biases at All Initial Rounds*

Next, we consider the biases that are labeled as "New_000," "New_ noz_004" and "New_noz_006" [30, Fig. 2]. We prove the biases for rounds 3 to 255 in RC4 PRGA, and we show that all of these decrease in magnitude with increase in r, as observed experimentally in Ref. [30].

The bias labeled "New_noz_006" in Ref. [30] can be derived as a corollary to Theorem 1 as follows.

Corollary 2. *For PRGA rounds* $3 \le r \le N-1$,

$$\Pr\big(S_r[j_r] = i_r\big) \approx \Pr\big(S_1[r] = r\big)\left(1 - \frac{1}{N}\right)^{r-2} + \sum_{t=2}^{r-1}\sum_{w=0}^{r-t} \frac{\Pr(S_1[t] = r)}{w! \cdot N}\left(\frac{r-t-1}{N}\right)^{w}\left(1 - \frac{1}{N}\right)^{r-3-w}.$$

Proof. $S_r[j_r]$ is assigned the value at $S_{r-1}[r]$ due to the swap in round r. Hence substituting $u = r$ and $v = i_r = r$ in Theorem 1, we get the result. □

In Fig. 5, we illustrate the experimental observations (each data point represents the average obtained from over 100 million experimental runs with 16-byte key in each case) and the theoretical values for the distribution of $\Pr(S_r[j_r] = i_r)$ over the initial rounds $3 \le r \le 255$ of RC4 PRGA. It is evident that our theoretical formula, as derived in Corollary 2, matches the experimental observations.

Next we take a look at the other two round-dependent biases of RC4, observed in Ref. [30]. We state the related result in Theorem 10, corresponding to observations "New_noz_004" and "New_000."

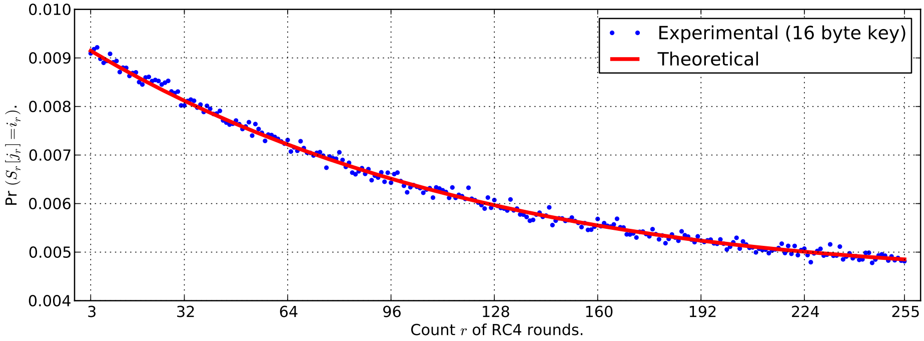

Fig. 5. Distribution of $\Pr(S_r[j_r] = i_r)$ for initial rounds $3 \le r \le 255$ of RC4 PRGA.

Theorem 10. *For PRGA rounds* $3 \le r \le N-1$,

$$\begin{aligned}\Pr\bigl(S_r[i_r]=j_r\bigr) &\approx \Pr\bigl(S_r[t_r]=t_r\bigr)\\ &\approx \frac{r}{N^2}+\sum_{X=r}^{N-1}\frac{1}{N}\Biggl(\Pr\bigl(S_1[X]=X\bigr)\biggl(1-\frac{1}{N}\biggr)^{r-2}\\ &\quad+\sum_{u=2}^{r-1}\sum_{w=0}^{r-u}\frac{\Pr(S_1[u]=r)}{w!\cdot N}\biggl(\frac{r-u-1}{N}\biggr)^{w}\biggl(1-\frac{1}{N}\biggr)^{r-3-w}\Biggr).\end{aligned}$$

Proof. We can write the two events under consideration as $E_3 : (S_{r-1}[j_r]=j_r)$ and $E_4 : (S_r[t_r]=t_r)$, where j_r and t_r can be considered as pseudo-random variables for all $3 \le r \le N-1$. We consider the following conditional paths for the first event E_3, depending on the range of values j_r may take:

$$\Pr(E_3)=\sum_{X=0}^{r-1}\Pr(E_3 \mid j_r=X)\cdot\Pr(j_r=X)+\sum_{X=r}^{N-1}\Pr(E_3 \mid j_r=X)\cdot\Pr(j_r=X).$$

Case I. In this case, we assume that j_r takes a value X between 0 and $r-1$. Each position in this range is touched by index i, and may also be touched by index j. Thus, irrespective of any initial condition, we may assume that $\Pr(E_3 \mid j_r=X)\approx 1/N$ in this case. Hence, this part contributes:

$$\sum_{X=0}^{r-1}\Pr(E_3 \mid j_r=X)\cdot\Pr(j_r=X)\approx\sum_{X=0}^{r-1}\frac{1}{N}\cdot\frac{1}{N}=\frac{r}{N^2}.$$

Case II. Here we suppose that j_r assumes a value $r \le X \le N-1$. In this case, the probability calculation can be split into two paths, as follows:

$$\begin{aligned}\Pr(E_3 \mid j_r=X)&=\Pr\bigl(E_3 \mid j_r=X\wedge S_1[X]=X\bigr)\cdot\Pr\bigl(S_1[X]=X\bigr)\\ &\quad+\Pr\bigl(E_3 \mid j_r=X\wedge S_1[X]\ne X\bigr)\cdot\Pr\bigl(S_1[X]\ne X\bigr).\end{aligned}$$

If $S_1[X]=X$, similarly to the logic in Theorem 1, we get the following:

$$\Pr\bigl(E_3 \mid j_r=X\wedge S_1[X]=X\bigr)\cdot\Pr\bigl(S_1[X]=X\bigr)\approx\Pr\bigl(S_1[X]=X\bigr)\biggl(1-\frac{1}{N}\biggr)^{r-2}.$$

If we suppose that $S_1[u]=X$ for some $u\ne X$, then one may note the following two sub-cases:

- Sub-case $2\le u\le r-1$: The probability for this path is similar to that in the proof of Theorem 1:

$$\sum_{u=2}^{r-1}\sum_{w=0}^{r-u}\frac{\Pr(S_1[u]=r)}{w!\cdot N}\biggl(\frac{r-u-1}{N}\biggr)^{w}\biggl(1-\frac{1}{N}\biggr)^{r-3-w}.$$

- Sub-case $r \le u \le N-1$: In this case the value X will always be behind the position of $i_r = r$, whereas $X > r$ as per assumption, i.e., the value X can never reach index position X from initial position u. Thus the probability is 0 in this case.

Assuming $\Pr(j_r = X) = 1/N$ for all X, and combining all contributions from the above-mentioned cases, we get the value of $\Pr(S_{r-1}[j_r] = j_r) = \Pr(S_r[i_r] = j_r)$, as desired.

In case of $\Pr(S_r[t_r] = t_r)$, t_r is a random variable just like j_r, and may take all values from 0 to $N-1$ with approximately the same probability $1/N$. Thus we can approximate $\Pr(S_r[t_r] = t_r) \approx \Pr(S_{r-1}[j_r] = j_r)$ to obtain the desired expression. □

Remark 1. The approximation $\Pr(S_r[t_r] = t_r) \approx \Pr(S_{r-1}[j_r] = j_r)$, as in Theorem 10, is particularly close for higher values of r because the effect of a single state change from S_{r-1} to S_r is low in such a case. For smaller values of r, it is more accurate to approximate $\Pr(S_{r-1}[t_r] = t_r) \approx \Pr(S_{r-1}[j_r] = j_r)$ and critically analyze the effect of the rth round of PRGA thereafter.

In Fig. 6, we show the experimental observations (averages taken over 100 million runs with 16-byte key) and the theoretical values for the distributions of $\Pr(S_r[i_r] = j_r)$ and $\Pr(S_r[t_r] = t_r)$ over the initial rounds $3 \le r \le 255$ of RC4 PRGA. It is evident that our theoretical formulae closely match with the experimental observations in both the cases.

3.4. *(Non-)Randomness of j in the Initial Rounds*

Two indices, i and j, are used in RC4 PRGA—the first is deterministic and the second one is pseudo-random. Index j depends on the values of i and $S[i]$ simultaneously, and the pseudo-randomness of the permutation S causes the pseudo-randomness in j. In this section, we attempt to analyze the pseudo-random behavior of j more clearly.

In RC4 PRGA, we know that for $r \ge 1$, $i_r = r \bmod N$ and $j_r = j_{r-1} + S_{r-1}[i_r]$, starting with $j_0 = 0$. Thus, we can recursively write the values of j at different rounds $1 \le r \le N-1$:

$$j_0 = 0, \qquad j_1 = S_0[1], \quad \ldots,$$

$$j_r = j_{r-1} + S_{r-1}[i_r] = S_0[1] + S_1[2] + \cdots + S_{r-1}[r] = \sum_{x=1}^{r} S_{x-1}[x].$$

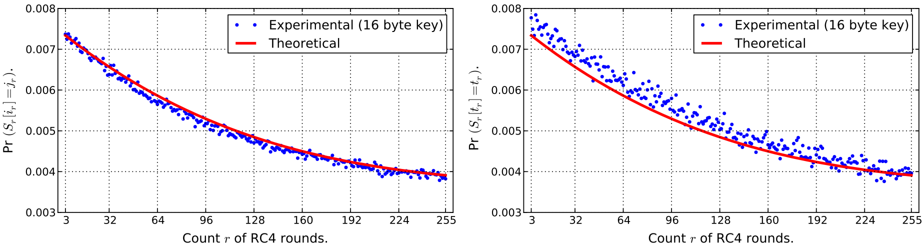

Fig. 6. Distributions of $\Pr(S_r[i_r] = j_r)$ and $\Pr(S_r[t_r] = t_r)$ for initial rounds $3 \le r \le 255$ of RC4 PRGA.

Non-randomness of j_1 In the first round of PRGA, $j_1 = S_0[1]$ follows a probability distribution which is determined by S_0. According to Proposition 1, we have:

$$\Pr(j_1 = v) = \Pr\big(S_0[1] = v\big) = \begin{cases} \frac{1}{N}, & \text{if } v = 0; \\ \frac{1}{N}(\frac{N-1}{N} + \frac{1}{N}(\frac{N-1}{N})^{N-2}), & \text{if } v = 1; \\ \frac{1}{N}((\frac{N-1}{N})^{N-2} + (\frac{N-1}{N})^{v}), & \text{if } v > 1. \end{cases}$$

This clearly tells us that j_1 is *not* random. This is also portrayed in Fig. 7.

Non-Randomness of j_2 In the second round of PRGA, however, we have $j_2 = S_0[1] + S_1[2]$, which demonstrates better randomness, as per the following discussion. We have:

$$\Pr(j_2 = v) = \Pr\big(S_0[1] + S_1[2] = v\big) = \sum_{w=0}^{N-1} \Pr\big(S_0[1] = w \wedge S_1[2] = v - w\big). \tag{10}$$

The following cases may arise with respect to (10).

- Case I: Suppose that $j_1 = S_0[1] = w = 2$. Then, $S_1[i_2] = S_1[2] = S_1[j_1] = S_0[i_1] = S_0[1] = 2$. In this case, we have:

$$\Pr(j_2 = v) = \begin{cases} \Pr(S_0[1] = 2), & \text{if } v = 4; \\ 0, & \text{otherwise.} \end{cases}$$

- Case II: Suppose that $j_1 = S_0[1] = w \neq 2$. Then $S_0[2]$ will not get swapped in the first round, and hence $S_1[2] = S_0[2]$. In this case, $\Pr(S_0[1] = w \wedge S_1[2] = v - w) = \Pr(S_0[1] = w \wedge S_0[2] = v - w)$.

We substitute the results obtained from these cases into (10) to obtain:

$$\Pr(j_2 = v) = \begin{cases} \Pr(S_0[1] = 2) + \sum_{w \neq 2} \Pr(S_0[1] = w \wedge S_0[2] = v - w), & \text{if } v = 4; \\ \sum_{w \neq 2} \Pr(S_0[1] = w \wedge S_0[2] = v - w), & \text{if } v \neq 4. \end{cases} \tag{11}$$

Equation (11) completely specifies the exact probability distribution of j_2, where the exact values of the probabilities $\Pr(S_0[x] = y)$ can be substituted from Proposition 1 with the adjustment as in Sect. 4.1.3 for estimating the joint probabilities. However, the expression suffices to exhibit the non-randomness of j_2 in the RC4 PRGA, having a large bias for $v = 4$. We found that the theoretical probabilities from (11) match almost exactly with the experimental data plotted in Fig. 7. For the sake of clarity, we do not show the theoretical curve in Fig. 7.

Randomness of j_r for $r \geq 3$ It is possible to compute the explicit probability distributions of $j_r = \sum_{x=1}^{r} S_{x-1}[x]$ for $3 \leq r \leq 255$ as well. We do not present the complicated expressions for $\Pr(j_r = v)$ for $r \geq 3$ here, but it turns out that j_r becomes closer to be random as r increases.

The probability distributions of j_1, j_2 and j_3 are shown in Fig. 7, where the experiments have been run over 1 billion trials of RC4 PRGA, with randomly generated keys of size 16 bytes. One may note that the randomness in j_2 is more than that of j_1 (apart

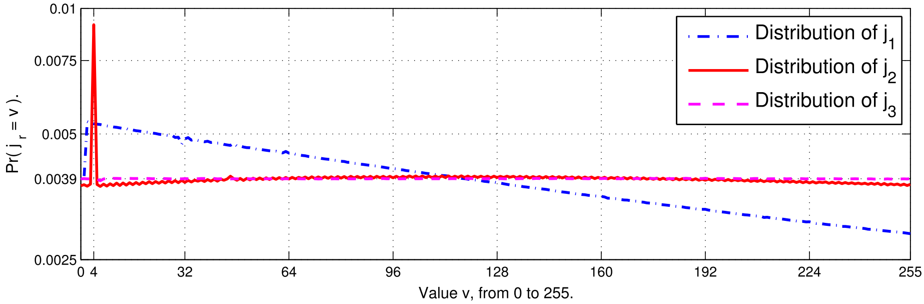

Fig. 7. Probability distribution of j_r for $1 \le r \le 3$.

from the case $v = 4$), and j_3 is almost uniformly random. This trend continues for the later rounds of PRGA as well. However, we do not plot the graphs for the probability distributions of j_r with $r \ge 4$, as these distributions are almost identical to that of j_3, i.e., almost uniformly random in behavior.

3.5. *Correlation Between Z_2 and $S_2[2]$*

We now explore the bias in $(j_2 = 4)$ more deeply and establish a correlation between the state S_2 and the keystream. Let us first evaluate $\Pr(j_2 = 4)$:

$$\begin{aligned}\Pr(j_2 = 4) &= \Pr\big(S_0[1] = 2\big) + \sum_{w \neq 2} \Pr\big(S_0[1] = w \wedge S_0[2] = 4 - w\big)\\ &= \frac{1}{N}\left[\left(\frac{N-1}{N}\right)^{N-2} + \left(\frac{N-1}{N}\right)^{2}\right] + \sum_{w \neq 2} \Pr\big(S_0[1] = w \wedge S_0[2] = 4 - w\big).\end{aligned}$$

Following Proposition 1 and the estimation of joint probabilities as in Sect. 4.1.3, the sum in the above expression evaluates approximately to $0.965268/N$ for $N = 256$. Thus, we get:

$$\Pr(j_2 = 4) \approx \frac{1}{N}\left[\left(\frac{N-1}{N}\right)^{N-2} + \left(\frac{N-1}{N}\right)^{2}\right] + \frac{0.965268}{N} \approx \frac{7/3}{N}.$$

This closely matches with our experimental observation, as depicted in Fig. 7. To exploit this bias in $(j_2 = 4)$, we focus on the event $(S_2[i_2] = 4 - Z_2)$ or $(S_2[2] = 4 - Z_2)$, and prove the following.

Theorem 11. *After completion of the second round of RC4 PRGA with $N = 256$,*

$$\Pr\big(S_2[2] = 4 - Z_2\big) \approx \frac{1}{N} + \frac{4/3}{N^2}.$$

Proof. We can write Z_2 in terms of the state variables as follows:

$$Z_2 = S_2\big[S_2[i_2] + S_2[j_2]\big] = S_2\big[S_1[j_2] + S_1[i_2]\big] = S_2\big[S_1[j_2] + S_1[2]\big].$$

Thus, we can write the probability of the target event $(S_2[2] = 4 - Z_2)$ as follows:

$$\begin{aligned}
&\Pr\bigl(S_2[2] = 4 - Z_2\bigr) \\
&\quad = \Pr\bigl(S_2[i_2] = 4 - S_2\bigl[S_1[j_2] + S_1[2]\bigr]\bigr) \\
&\quad = \Pr\bigl(S_1[j_2] + S_2\bigl[S_1[j_2] + S_1[2]\bigr] = 4\bigr) \\
&\quad = \Pr\bigl(S_1[j_2] + S_2\bigl[S_1[j_2] + S_1[2]\bigr] = 4 \wedge j_2 = 4\bigr) \\
&\qquad + \Pr\bigl(S_1[j_2] + S_2\bigl[S_1[j_2] + S_1[2]\bigr] = 4 \wedge j_2 \neq 4\bigr).
\end{aligned}$$

Computing the First Term The probability for the first event can be calculated as follows:

$$\begin{aligned}
&\Pr\bigl(S_1[j_2] + S_2\bigl[S_1[j_2] + S_1[2]\bigr] = 4 \wedge j_2 = 4\bigr) \\
&\quad = \Pr\bigl(S_1[4] + S_2\bigl[S_1[4] + S_1[2]\bigr] = 4 \wedge j_2 = 4\bigr) \\
&\quad = \sum_{y=0}^{N-1} \Pr\bigl(S_1[4] + S_2[y] = 4 \wedge S_1[4] + S_1[2] = y \wedge j_2 = 4\bigr) \\
&\quad = \Pr(j_2 = 4) \cdot \sum_{y=0}^{N-1} \Pr\bigl(S_1[4] + S_2[y] = 4 \wedge S_1[4] + S_1[2] = y\bigr).
\end{aligned}$$

In the last expression, the values taken from S_1 are independent of the value of j_2, and thus the events $(S_1[4] + S_2[y] = 4)$ and $(S_1[4] + S_1[2] = y)$ are both independent of the event $(j_2 = 4)$. Also, if $y = 4$, we obtain $S_1[4] + S_2[y] = S_1[4] + S_2[4] = S_1[4] + S_2[j_2] = S_1[4] + S_1[i_2] = S_1[4] + S_1[2]$, which results in the events $(S_1[4] + S_2[y] = 4)$ and $(S_1[4] + S_1[2] = y)$ being identical. In all other cases, we have $S_1[4] + S_2[y] \neq S_1[4] + S_1[2]$ and thus the values are chosen distinctly independent at random. Hence, we obtain:

$$\Pr\bigl(S_1[4] + S_2[y] = 4 \wedge S_1[4] + S_1[2] = y\bigr) = \begin{cases} \frac{1}{N}, & \text{if } y = 4; \\ \frac{1}{N(N-1)}, & \text{if } y \neq 4. \end{cases}$$

Thus, the probability $\Pr(S_1[j_2] + S_2[S_1[j_2] + S_1[2]] = 4 \wedge j_2 = 4)$ for the first event turns out to be:

$$\begin{aligned}
\Pr(j_2 = 4) \cdot \left(\frac{1}{N} + \sum_{y \neq 4} \frac{1}{N(N-1)}\right) &= \frac{7/3}{N} \cdot \left(\frac{1}{N} + \frac{N-1}{N(N-1)}\right) \\
&= \frac{7/3}{N} \cdot \frac{2}{N}.
\end{aligned}$$

Computing the Second Term The probability calculation follows a similar path:

$$
\begin{aligned}
&\Pr\big(S_1[j_2] + S_2\big[S_1[j_2] + S_1[2]\big] = 4 \wedge j_2 \neq 4\big) \\
&\quad = \sum_{x \neq 4} \Pr\big(S_1[x] + S_2\big[S_1[x] + S_1[2]\big] = 4 \wedge j_2 = x\big) \\
&\quad = \sum_{x \neq 4} \sum_{y=0}^{N-1} \Pr\big(S_1[x] + S_2[y] = 4 \wedge S_1[x] + S_1[2] = y \wedge j_2 = x\big).
\end{aligned}
$$

The case $y = x$ poses an interesting situation. On the one hand, we obtain $S_1[x] + S_2[y] = S_1[x] + S_2[x] = S_1[x] + S_2[j_2] = S_1[x] + S_1[i_2] = S_1[x] + S_1[2] = 4$, while on the other hand, we get $S_1[x] + S_1[2] = x \neq 4$. We rule out this case to get $\Pr(S_1[j_2] + S_2[S_1[j_2] + S_1[2]] = 4 \wedge j_2 \neq 4)$:

$$
\sum_{x \neq 4} \sum_{y \neq x} \Pr\big(S_1[x] + S_2[y] = 4 \wedge S_1[x] + S_1[2] = y\big) \cdot \Pr(j_2 = x).
$$

As before, the values taken from S_1 are independent of the value of j_2, and thus the events $(S_1[x] + S_2[y] = 4)$ and $(S_1[x] + S_1[2] = y)$ are both independent of the event $(j_2 = x)$.

If $y = 4$, we have $S_1[x] + S_2[4] = 4$, while $S_1[x] + S_1[2] = 4$. One may note that $S_1[4]$ does not get swapped to obtain S_2, as $i_2 = 2$ and $j_2 = x \neq 4$. Thus, $S_2[4] = S_1[4]$ and we get $S_1[x] + S_1[4] = 4$ and $S_1[x] + S_1[2] = 4$. This indicates $S_1[4] = S_1[2]$, which is impossible as S_1 is a permutation. All other cases $(y \neq 4)$ deal with two distinct locations of the permutation S_1. Therefore, we obtain:

$$
\Pr\big(S_1[x] + S_2[y] = 4 \wedge S_1[x] + S_1[2] = y\big) = \begin{cases} 0, & \text{if } y = 4; \\ \frac{1}{N(N-1)}, & \text{otherwise.} \end{cases}
$$

Thus, the probability $\Pr(S_1[j_2] + S_2[S_1[j_2] + S_1[2]] = 4 \wedge j_2 \neq 4)$ of the second event turns out to be:

$$
\begin{aligned}
\sum_{x \neq 4} \Pr(j_2 = x) \cdot \left(0 + \sum_{y \neq x, 4} \frac{1}{N(N-1)}\right) &= \frac{N-2}{N(N-1)} \cdot \sum_{x \neq 4} \Pr(j_2 = x) \\
&= \frac{N-2}{N(N-1)} \cdot \left(1 - \frac{7/3}{N^2}\right).
\end{aligned}
$$

Calculation for $\Pr(S_2[2] = 4 - Z_2)$ Combining the probabilities for the first and second events, we get the following:

$$
\Pr\big(S_2[2] = 4 - Z_2\big) = \frac{7/3}{N^2} \cdot \frac{2}{N} + \frac{N-2}{N(N-1)} \cdot \left(1 - \frac{7/3}{N^2}\right) \approx \frac{1}{N} + \frac{4/3}{N^2}. \qquad \square
$$

This establishes a correlation between the state byte $S_2[2]$ and the keystream byte Z_2. For $N = 256$, the result matches with our experimental data generated from 1 billion runs of RC4 with randomly selected 16-byte keys.

4. Biases in Keystream Bytes of RC4 PRGA

In the previous section, we discussed some biases involving the RC4 state variables S, i, j, during RC4 PRGA. A few of those biases involved the keystream bytes also. In this section, we concentrate on biases exhibited by RC4 keystream bytes towards constant values in $\{0, \dots, 255\}$.

4.1. *Probability Distribution of* Z_1

Here we derive the complete probability distribution of the first RC4 keystream byte Z_1, as observed by Mironov [23, Fig. 6] in CRYPTO 2002. Before proceeding to prove the general result, we start with a specific case, namely, the negative bias of Z_1 towards 0.

4.1.1. *Negative Bias in* Z_1 *Towards Zero*

The special case of Z_1's negative bias towards 0 is contained in the complete probability distribution of Z_1 to be proved shortly. However, we present a separate proof for this special case because, unlike the proof for the complete case, this special case has a much simpler proof which reveals a different relationship of the RC4 state variables. This is elaborated further in Remark 2 later.

Theorem 12. *Assume that the initial permutation* S_0 *of RC*4 *PRGA is randomly chosen from the set of all permutations of* $\{0, 1, \dots, N-1\}$. *Then the probability that the first output byte of RC*4 *keystream is* 0 *is approximately* $1/N - 1/N^2$.

Proof. We explore the probability $\Pr(Z_1 = 0)$ using the following conditional paths:

$$\begin{aligned}\Pr(Z_1 = 0) = {} & \Pr\bigl(Z_1 = 0 \mid S_0[j_1] = 0\bigr) \cdot \Pr\bigl(S_0[j_1] = 0\bigr) \\ & + \Pr\bigl(Z_1 = 0 \mid S_0[j_1] \neq 0\bigr) \cdot \Pr\bigl(S_0[j_1] \neq 0\bigr).\end{aligned}$$

Case I: $S_0[j_1] = 0$. Suppose that $j_1 = S_0[1] = X \neq 1$ and $S_0[j_1] = S_0[S_0[1]] = 0$. Then we have

$$Z_1 = S_1\bigl[S_1[1] + S_1[X]\bigr] = S_1\bigl[S_0[X] + S_0[1]\bigr] = S_1[0 + X] = S_0[1] = X \neq 0,$$

as S_0 is a permutation, where X and 0 belong to two different indices 1 and X. Thus, in this case we have $\Pr(Z_1 = 0 \mid S_0[j_1] = 0) \approx 0$.

Case II: $S_0[j_1] \neq 0$. In this case, output byte Z_1 can be considered uniformly random, and thus

$$\Pr\bigl(Z_1 = 0 \mid S_0[j_1] \neq 0\bigr) \approx 1/N.$$

Combining the two cases, the total probability that the first output byte is 0 is given by

$$\Pr(Z_1 = 0) \approx 0 \cdot 1/N + 1/N \cdot (1 - 1/N) = 1/N - 1/N^2. \qquad \square$$

From Theorem 12, we immediately get a distinguisher of RC4 that can effectively distinguish the output keystream of the cipher from a random sequence of bytes. For the event $E : (Z_1 = 0)$, the bias proved above can be written as $p(1 + q)$, where $p = 1/N$ and $q = -1/N$. The number of samples required to distinguish RC4 from random sequence of bits with a constant probability of success in this case is approximately N^3.

4.1.2. *Complete Distribution of* Z_1

In this section, we turn our attention to the complete probability distribution of the first byte Z_1. In Ref. [23, Fig. 6], the empirical plot of Z_1 has a peculiar sine-curve-like pattern which is not observed for any other variables or events related to RC4. In Theorem 13, we theoretically derive this interesting distribution.

Theorem 13. *The probability distribution of the first output byte of RC*4 *keystream is as follows, where* $v \in \{0,\dots,N-1\}$, $\mathcal{L}_v = \{0,1,\dots,N-1\} \setminus \{1,v\}$ *and* $\mathcal{T}_{v,X} = \{0,1,\dots,N-1\} \setminus \{0,X,1-X,v\}$.

$$\Pr(Z_1 = v) = Q_v + \sum_{X\in\mathcal{L}_v} \sum_{Y\in\mathcal{T}_{v,X}} \Pr\big(S_0[1] = X \wedge S_0[X] = Y \wedge S_0[X+Y] = v\big),$$

$$\textit{with } Q_v = \begin{cases} \Pr(S_0[1] = 1 \wedge S_0[2] = 0), & \textit{if } v = 0; \\ \Pr(S_0[1] = 0 \wedge S_0[0] = 1), & \textit{if } v = 1; \\ \Pr(S_0[1] = 1 \wedge S_0[2] = v) + \Pr(S_0[1] = v \wedge S_0[v] = 0) & \\ \quad + \Pr(S_0[1] = 1 - v \wedge S_0[1-v] = v), & \textit{otherwise}. \end{cases}$$

Proof. The first output byte Z_1 can be explicitly written as

$$Z_1 = S_1\big[S_1[i_1] + S_1[j_1]\big] = S_1\big[S_0[j_1] + S_0[i_1]\big] = S_1\big[S_0\big[S_0[1]\big] + S_0[1]\big] = S_1[Y+X],$$

where we denote $j_1 = S_0[1]$ by X and $S_0[S_0[1]] = S_0[X]$ by Y. Thus, we have

$$\Pr(Z_1 = v) = \sum_{X=0}^{N-1} \sum_{Y=0}^{N-1} \Pr\big(S_0[1] = X \wedge S_0[X] = Y \wedge S_1[X+Y] = v\big).$$

Special Cases Depending on X, Y Our goal is to write all probability expressions in terms of S_0. To express $S_1[X+Y]$ in terms of S_0, we observe that the state S_1 is different from S_0 in at most two places, $i_1 = 1$ and $j_1 = X$. Thus, we need to treat specially the case $X + Y = 1$, which holds if and only if $Y = 1 - X$, and $X + Y = X$, which holds if and only if $Y = 0$. Another special case to consider is $X = 1$, which holds if and only if $Y = X$, where no swap occurs from S_0 to S_1. These special cases result in the following values of Z_1:

$$\begin{aligned} &X + Y = 1, \quad \text{if and only if} \quad Y = 1 - X, \\ &\quad \text{implies} \quad Z_1 = S_1[1] = S_1[i_1] = S_0[j_1] = S_0[X] = Y = 1 - X, \\ &X + Y = X, \quad \text{if and only if} \quad Y = 0, \\ &\quad \text{implies} \quad Z_1 = S_1[X] = S_1[j_1] = S_0[i_1] = S_0[1] = X, \\ &X = 1, \quad \text{if and only if} \quad Y = X, \\ &\quad \text{implies} \quad Z_1 = S_1[X+Y] = S_0[X+Y] = S_0[1+1] = S_0[2]. \end{aligned}$$

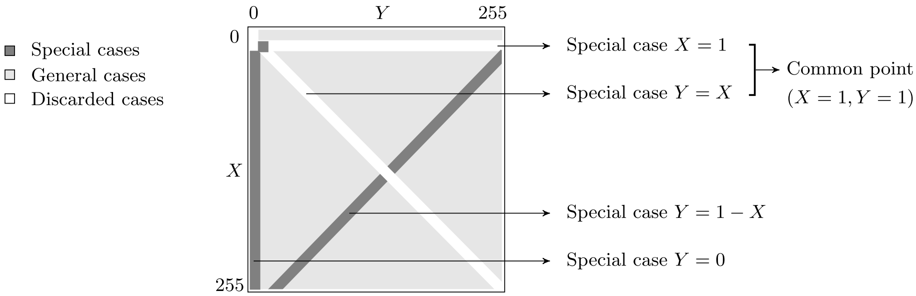

Fig. 8. X, Y dependent special cases and range of sums for evaluation of $\Pr(Z_1 = v)$ in terms of S_0.

In all other circumstances, we would have $Z_1 = S_1[X + Y] = S_0[X + Y]$. Considering all the special cases as discussed above, we obtain $\Pr(Z_1 = v)$ in terms of S_0 as follows:

$$\begin{aligned}
&\sum_{X=0}^{N-1} \Pr\big(S_0[1] = X \wedge S_0[X] = 1 - X \wedge 1 - X = v\big) \\
&\quad + \sum_{X=0}^{N-1} \Pr\big(S_0[1] = X \wedge S_0[X] = 0 \wedge X = v\big) \\
&\quad + \Pr\big(S_0[1] = 1 \wedge S_0[2] = v\big) \\
&\quad + \sum_{X \neq 1} \sum_{Y \neq 0, X, 1-X} \Pr\big(S_0[1] = X \wedge S_0[X] = Y \wedge S_0[X + Y] = v\big).
\end{aligned}$$

The first sum refers to the special case $Y = 1 - X$ and the second one refers to $Y = 0$. The special case $X = 1$, which holds if and only if $Y = X$, merges to produce the third term, common point $(X = 1, Y = 1)$. All other points on $X = 1$ and $Y = X$ are discarded. The last double summation term denotes all other general cases. One may refer to Fig. 8 to obtain a clearer exposition of the ranges of sums.

Special Cases Depending on v The first summation term reduces to a single point $(X = 1 - v, Y = v)$, as we fix $1 - X = v$ and $Y = 1 - X$. The second summation, similarly, reduces to the point $(X = v, Y = 0)$. Furthermore, we have two impossible cases in the double summation:

$$\begin{aligned}
&(X = v, Y \neq 0) \quad \text{which implies } S_1[v] = v, \\
&X + Y \neq v \quad \Rightarrow \quad Z_1 = S_1[X + Y] \neq v, \\
&(X \neq 1 - v, Y = v) \quad \text{which implies } S_1[1] = S_0[X] = v, \\
&X + Y \neq 1 \quad \Rightarrow \quad Z_1 = S_1[X + Y] \neq v.
\end{aligned}$$

Hence, the most general form for the probability $\Pr(Z_1 = v)$ can be written as follows:

$$\Pr(Z_1 = v) = Q_v + \sum_{X \in \mathcal{L}_v} \sum_{Y \in \mathcal{T}_{v,X}} \Pr\bigl(S_0[1] = X \wedge S_0[X] = Y \wedge S_0[X+Y] = v\bigr),$$

where $Q_v = \Pr(S_0[1] = 1 - v \wedge S_0[1-v] = v) + \Pr(S_0[1] = v \wedge S_0[v] = 0) + \Pr(S_0[1] = 1 \wedge S_0[2] = v)$.

Value of Q_v State S_0 being a permutation, some of the probability terms in Q_v are 0 when v takes particular values. We have the following three cases in this regard.

- Case $v = 0$: We have $Q_0 = \Pr(S_0[1] = 1 \wedge S_0[1] = 0) + \Pr(S_0[1] = 0 \wedge S_0[0] = 0) + \Pr(S_0[1] = 1 \wedge S_0[2] = 0) = \Pr(S_0[1] = 1 \wedge S_0[2] = 0)$, as S_0 is a permutation.
- Case $v = 1$: We have $Q_v = \Pr(S_0[1] = 0 \wedge S_0[0] = 1) + \Pr(S_0[1] = 1 \wedge S_0[1] = 0) + \Pr(S_0[1] = 1 \wedge S_0[2] = 1) = \Pr(S_0[1] = 0 \wedge S_0[0] = 1)$, as S_0 is a permutation.
- Case $v \neq 0, 1$: Here we have no conflicts or special conditions as in the previous cases, and hence the general form of Q_v holds.

Combining the general formula for $\Pr(Z_1 = v)$ and all three cases for Q_v, we obtain the desired theoretical probability distribution for the first output byte Z_1. □

4.1.3. *Estimation of the Joint Probabilities and Numeric Values*

We consider two special cases while computing the numeric values of $\Pr(Z_1 = v)$. First, we investigate RC4 PRGA where S_0 is fed from the output of RC4 KSA, as in practice. Next, we probe into the scenario when the initial permutation S_0 is random.

Assume that the initial permutation S_0 of RC4 PRGA is constructed from the regular KSA, i.e., the probabilities $\Pr(S_0[u] = v)$ follow the distribution mentioned in Proposition 1. However, we require the joint probabilities like $\Pr(S_0[1] = X \wedge S_0[X] = Y \wedge S_0[X+Y] = v)$ in our formula derived in Theorem 13, and we devise the following estimates for these joint probabilities.

- Consider the joint probability $\Pr(S_0[u] = v \wedge S_0[u'] = v')$ where $u \neq u'$ and $v \neq v'$. We can represent this by $\Pr(S_0[u] = v \wedge S_0[u'] = v') = \Pr(S_0[u] = v) \cdot \Pr(S_0[u'] = v' \mid S_0[u] = v)$. The first term is estimated directly from Proposition 1. For the second term, $S_0[u] = v \;\Rightarrow\; S_0[u'] \neq v$. Thus we normalize $\Pr(S_0[u'] = v)$ and estimate the second term as

$$\Pr\bigl(S_0\bigl[u'\bigr] = v' \mid S_0[u] = v\bigr) \approx \Pr\bigl(S_0\bigl[u'\bigr] = v'\bigr) + \frac{\Pr(S_0[u'] = v)}{N-1}.$$

- For the joint probability $\Pr(S_0[u] = v \wedge S_0[u'] = v' \wedge S_0[u''] = v'')$, we can represent it by $\Pr(S_0[u] = v) \cdot \Pr(S_0[u'] = v' \mid S_0[u] = v) \cdot \Pr(S_0[u''] = v'' \mid S_0[u'] = v' \wedge S_0[u] = v)$. The first term comes from Proposition 1 and the second term as above. The third term is estimated as

$$\begin{aligned}\Pr\bigl(S_0\bigl[u''\bigr] = v'' \mid S_0\bigl[u'\bigr] = v' \wedge S_0[u] = v\bigr)\\ \approx \Pr\bigl(S_0\bigl[u''\bigr] = v''\bigr) + \frac{\Pr(S_0[u''] = v')}{N-2} + \frac{\Pr(S_0[u''] = v)}{N-2}.\end{aligned}$$

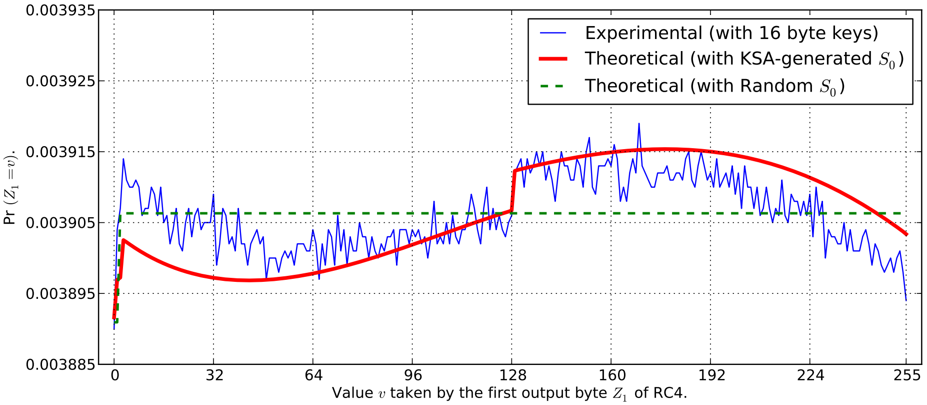

Fig. 9. The probability distribution of the first output byte Z_1.

We compute the theoretical values of $\Pr(Z_1 = v)$ using Theorem 13 and Proposition 1, along with the estimations for joint probabilities discussed above. Figure 9 shows the theoretical and experimental probability distributions of Z_1, where the experimental data is generated over 100 million runs of RC4 PRGA using 16-byte secret keys. The figure clearly shows that our theoretical justification closely matches the experimental data, and justifies the observation by Mironov [23].

As an alternative to the *additive correction* described above for estimating the conditionals, one may consider *multiplicative correction* by normalizing the probabilities as follows:

- Estimate $\Pr(S_0[u'] = v' \mid S_0[u] = v)$ as $\frac{\Pr(S_0[u']=v')}{1-\Pr(S_0[u']=v)}$.
- Estimate $\Pr(S_0[u''] = v'' \mid S_0[u'] = v' \wedge S_0[u] = v)$ as $\frac{\Pr(S_0[u'']=v'')}{1-\Pr(S_0[u'']=v')-\Pr(S_0[u'']=v)}$.

We found that the numeric values of $\Pr(Z_1 = v)$ estimated using the two different models (additive and multiplicative) almost coincide and the graphs fall right on top of one another.

If the initial permutation S_0 of RC4 PRGA is considered to be random, then we would have $\Pr(S_0[u] = v) \approx 1/N$ for all u, v, and the joint probabilities can be computed directly (samples drawn without replacement). Substituting all the relevant probability values, we get

$$\Pr(Z_1 = 0) \approx \Pr(Z_1 = 1) \approx \frac{1}{N} - \frac{1}{N(N-1)}, \quad \text{and}$$

$$\Pr(Z_1 = v) \approx \frac{1}{N} + \frac{1}{N(N-1)(N-2)} \quad \text{for } 2 \leq v \leq 255,$$

which is almost a uniform distribution for $2 \leq v \leq 255$. The dashed line in Fig. 9 shows the graph for this theoretical distribution, and it closely matches our experimental data as well (we omit the experimental curve for random S_0 as it coincides with the theoretical one).

Remark 2. Theorem 12 is the special case $v = 0$ of Theorem 13 and hence may seem redundant. However, we like to point out that the former has a simple and straightforward proof assuming S_0 to be random and the latter has a rigorous general proof without any assumption on S_0. The result of Theorem 12 signifies that this negative bias is not an artifact of non-random S_0 produced by RC4 KSA, rather it would be present, even if one starts PRGA with a uniform random permutation.

4.2. *Biases of Keystream Bytes 3 to 255 Towards Zero*

In FSE 2001, Mantin and Shamir [18] proved the famous $2/N$ bias towards the value 0 for the second byte of RC4 keystream. In addition, they made the following claims:

- MS-Claim-1: $\Pr(Z_r = 0) = \frac{1}{N}$ at PRGA rounds $3 \le r \le 255$.
- MS-Claim-2: $\Pr(Z_r = 0 \mid j_r = 0) > \frac{1}{N}$ and $\Pr(Z_r = 0 \mid j_r \neq 0) < \frac{1}{N}$ for $3 \le r \le 255$.

It is reasoned in Ref. [18] that the two biases in MS-Claim-2 cancel each other to produce no bias in the event $(Z_r = 0)$ in rounds 3 to 255, thereby justifying MS-Claim-1. In this section, contrary to MS-Claim-1, we show (in Theorem 14) that $\Pr(Z_r = 0) > \frac{1}{N}$ for all rounds r from 3 to 255.

To prove the main result, we will require Corollary 2. For ease of reference, we restate another version of this corollary below.

Corollary 2. *For PRGA rounds* $3 \le r \le N-1$,

$$\Pr\bigl(S_{r-1}[r] = r\bigr) \approx \Pr\bigl(S_1[r] = r\bigr)\left(1 - \frac{1}{N}\right)^{r-2} + \sum_{t=2}^{r-1}\sum_{w=0}^{r-t} \frac{\Pr(S_1[t] = r)}{w! \cdot N}\left(\frac{r-t-1}{N}\right)^{w}\left(1 - \frac{1}{N}\right)^{r-3-w}.$$

Theorem 14. *For PRGA rounds* $3 \le r \le N-1$, *the probability that* $Z_r = 0$ *is given by*

$$\Pr(Z_r = 0) \approx \frac{1}{N} + \frac{c_r}{N^2},$$
$$\textit{where } c_r = \begin{cases} \frac{N}{N-1}(N \cdot \Pr(S_{r-1}[r] = r) - 1) - \frac{N-2}{N-1}, & \textit{for } r = 3; \\ \frac{N}{N-1}(N \cdot \Pr(S_{r-1}[r] = r) - 1), & \textit{otherwise.} \end{cases}$$

Proof. The expression for c_r has an extra term $(-\frac{N-2}{N-1})$ in the case $r = 3$, and everything else is the same as in the general formula for $4 \le r \le N-1$. We shall first prove the general formula for $4 \le r \le N-1$, and then justify the extra term for the special case $r = 3$. We may write:

$$\Pr(Z_r = 0) = \Pr\bigl(Z_r = 0 \wedge S_{r-1}[r] = r\bigr) + \Pr\bigl(Z_r = 0 \wedge S_{r-1}[r] \neq r\bigr). \tag{12}$$

We will use $Z_r = S_r[S_r[i_r] + S_r[j_r]] = S_r[S_r[r] + S_{r-1}[i_r]] = S_r[S_r[r] + S_{r-1}[i_r]] = S_r[S_r[r] + S_{r-1}[r]]$.

Calculation of $\Pr(Z_r = 0 \wedge S_{r-1}[r] = r)$ In this case, $Z_r = 0 \Rightarrow S_r[S_r[r] + r] = 0$, and thus:

$$\Pr\bigl(Z_r = 0 \wedge S_{r-1}[r] = r\bigr) = \sum_{x=0}^{N-1} \Pr\bigl(S_r[x + r] = 0 \wedge S_r[r] = x \wedge S_{r-1}[r] = r\bigr).$$

Now the events $(S_r[x + r] = 0)$ and $(S_r[r] = x)$ are both independent of $(S_{r-1}[r] = r)$, as a state update has occurred in the process, and $S_{r-1}[r] = r$ is one of the values that got swapped. Hence,

$$\begin{aligned}&\Pr\bigl(Z_r = 0 \wedge S_{r-1}[r] = r\bigr)\\ &\quad= \sum_{x=0}^{N-1} \Pr\bigl(S_r[x + r] = 0\bigr) \cdot \Pr\bigl(S_r[r] = x \mid S_r[x + r] = 0\bigr) \cdot \Pr\bigl(S_{r-1}[r] = r\bigr).\end{aligned}$$

We note that if there exists any bias in the event $(S_r[x + r] = 0)$, then it must propagate from a similar bias in $(S_0[x + r] = 0)$, as was the case for $(S_{r-1}[r] = r)$ in Corollary 2. However, $\Pr(S_0[x + r] = 0) = 1/N$ by Proposition 1, and thus we assume $\Pr(S_r[x + r] = 0) \approx 1/N$ as well. For $\Pr(S_r[r] = x \mid S_r[x + r] = 0)$, we have the following two cases:

$$x = 0 \quad\Rightarrow\quad x + r = r \quad \text{which in turn gives} \quad \bigl(S_r[x + r] = 0\bigr) \quad\Leftrightarrow\quad \bigl(S_r[r] = x = 0\bigr),$$

and

$$x \neq 0 \quad\Rightarrow\quad x + r \neq r \quad \text{which in turn gives} \quad \bigl(S_r[x + r] = 0\bigr) \quad\Leftrightarrow\quad \bigl(S_r[r] = x \neq 0\bigr).$$

Moreover, in the second case, the value of $S_r[r]$ is independent of $S_{r-1}[r]$ because $[r] = [i_r]$ position got swapped to generate S_r from S_{r-1}. Thus we have:

$$\Pr\bigl(S_r[x + r] = 0 \mid S_r[r] = x\bigr) = \begin{cases} 1, & \text{if } x = 0;\\ 1/(N-1), & \text{if } x \neq 0.\end{cases} \tag{13}$$

Combining all the above probability values, we get

$$\begin{aligned}\Pr\bigl(Z_r = 0 \wedge S_{r-1}[r] = r\bigr) &\approx \frac{1}{N} \cdot \Pr\bigl(S_{r-1}[r] = r\bigr) \cdot \sum_{x=0}^{N-1} \Pr\bigl(S_r[x + r] = 0 \mid S_r[r] = x\bigr)\\ &= \frac{1}{N} \cdot \Pr\bigl(S_{r-1}[r] = r\bigr) \cdot \left(1 + (N-1) \cdot \frac{1}{N-1}\right) = \frac{2}{N} \cdot \Pr\bigl(S_{r-1}[r] = r\bigr).\end{aligned} \tag{14}$$

Calculation of $\Pr(Z_r = 0 \wedge S_{r-1}[r] \neq r)$ Similarly to the previous case, we can derive

$$\Pr\bigl(Z_r = 0 \wedge S_{r-1}[r] \neq r\bigr) = \sum_{y \neq r} \sum_{x=0}^{N-1} \Pr\bigl(S_r[x + y] = 0 \wedge S_r[r] = x \wedge S_{r-1}[r] = y\bigr).$$

In the above expression, we have

$$\{y \neq r \text{ and } x = r - y\} \quad \Rightarrow \quad \big\{S_r[x+y] = S_r[r] = 0 \text{ and } S_r[r] = x = r - y \neq 0\big\},$$

which is a contradiction. Moreover, the events $(S_r[x+y] = 0)$ and $(S_r[r] = x)$ are both independent of $(S_{r-1}[r] = y)$, as $S_{r-1}[r]$ got swapped in the state update. Thus we get:

$$\Pr\big(Z_r = 0 \wedge S_{r-1}[r] \neq r\big) = \sum_{y \neq r} \sum_{x \neq r-y} \Pr\big(S_r[x+y] = 0 \wedge S_r[r] = x\big) \cdot \Pr\big(S_{r-1}[r] = y\big).$$

Similarly to the derivation of (13), we obtain:

$$\Pr\big(S_r[x+y] = 0 \wedge S_r[r] = x\big) = \begin{cases} 0 \cdot (1/N) = 0, & \text{if } x = 0; \\ (1/(N-1)) \cdot (1/N) = 1/(N(N-1)), & \text{if } x \neq 0. \end{cases} \tag{15}$$

The only difference occurs in the case $x = 0$. Here we get

$$\{y \neq r \text{ and } x = 0\} \quad \Rightarrow \quad \big\{S_r[x+y] = S_r[y] = 0 \text{ and } S_r[r] = x = 0\big\},$$

which is a contradiction as $y \neq r$ are distinct locations in the permutation S_r. In all other cases $(x \neq 0)$, the argument is same as before. Combining the above probabilities, we get:

$$\begin{aligned} &\Pr\big(Z_r = 0 \wedge S_{r-1}[r] \neq r\big) \\ &\quad \approx \sum_{y \neq r} \Pr\big(S_{r-1}[r] = y\big) \left(0 + \sum_{x \neq r-y,0} \frac{1}{N(N-1)}\right) \\ &\quad = \sum_{y \neq r} \Pr\big(S_{r-1}[r] = y\big) \cdot (N-2) \cdot \frac{1}{N(N-1)} = \frac{N-2}{N(N-1)} \cdot \big(1 - \Pr\big(S_{r-1}[r] = r\big)\big). \end{aligned} \tag{16}$$

Calculation for $\Pr(Z_r = 0)$ Combining (12), (14) and (16), we obtain

$$\begin{aligned} \Pr(Z_r = 0) &\approx \frac{2}{N} \cdot \Pr\big(S_{r-1}[r] = r\big) + \frac{N-2}{N(N-1)} \cdot \big(1 - \Pr\big(S_{r-1}[r] = r\big)\big) \\ &= \frac{1}{N} + \frac{c_r}{N^2}, \end{aligned} \tag{17}$$

where $c_r = \frac{N}{N-1}(N \cdot \Pr(S_{r-1}[r] = r) - 1)$, as required in the general case.

Special Case for $r = 3$ The expression for $\Pr(Z_r = 0 \wedge S_{r-1}[r] = r)$ is identical to that in the general case, that is, the same as in (14). However, for $\Pr(Z_r = 0 \wedge S_{r-1}[r] \neq r)$ we have a special case. For $r = 3$, if $S_{r-1}[r] = S_2[3] = 0$, we have $j_3 = j_2 + S_2[3] = j_2$, and thus

$$\left\{ \begin{array}{l} Z_3 = 0 \\ S_2[3] = 0 \end{array} \right\} \quad \Rightarrow \quad \left\{ \begin{array}{l} S_3[S_3[3]] = S_3[S_2[j_3]] = S_3[S_2[j_2]] = S_3[S_1[2]] = 0 \\ S_2[3] = S_3[j_3] = S_3[j_2] = S_3[j_1 + S_1[2]] = 0 \end{array} \right\}$$

$$\Rightarrow \quad j_1 = S_0[1] = 0.$$

This poses a contradiction, as $S_0[1] = S_1[0] = 0$ can only produce $S_2[i_2] = S_2[2] = 0$ in the case $j_2 = 0$, and may never result in $S_2[3] = 0$. Thus, for $r = 3$, (16) changes as follows:

$$\begin{aligned}\Pr\bigl(Z_r = 0 \wedge S_{r-1}[r] \neq r\bigr) &\approx \frac{N-2}{N(N-1)} \cdot \bigl(1 - \Pr\bigl(S_{r-1}[r] = r\bigr) - \Pr\bigl(S_{r-1}[r] = 0\bigr)\bigr) \\ &= \frac{N-2}{N(N-1)} \cdot \bigl(1 - \Pr\bigl(S_{r-1}[r] = r\bigr)\bigr) \\ &\quad - \frac{N-2}{N^2(N-1)}, \quad \text{by Proposition 1.}\end{aligned}$$

This gives rise to the special expression of $c_r = \frac{N}{N-1}(N \cdot \Pr(S_{r-1}[r] = r) - 1) - \frac{N-2}{N-1}$.

The extra term does not appear in the general case $4 \le r \le N - 1$, because we have

$$\begin{aligned}&\left\{\begin{array}{l} Z_r = 0 \\ S_{r-1}[r] = 0 \end{array}\right\} \\ &\Rightarrow \quad \left\{\begin{array}{l} S_r[S_r[r]] = S_r[S_{r-1}[j_r]] = S_r[S_{r-1}[j_{r-1}]] = S_r[S_{r-2}[r-1]] = 0 \\ S_{r-1}[r] = S_r[j_r] = S_r[j_{r-1}] = S_r[j_{r-2} + S_{r-2}[r-1]] = 0 \end{array}\right\} \\ &\Rightarrow \quad j_{r-2} = 0,\end{aligned}$$

which does not pose any contradiction for $r > 3$, as we can assume j_{r-2} to be random and independent to the condition $S_{r-1}[r] = y = 0$ in these cases. □

Corollary 3. *For $N = 256$ and $3 \le r \le 255$, the probability $\Pr(Z_r = 0)$ is bounded as follows:*

$$\frac{1}{N} + \frac{1.337057}{N^2} \ \ge\ \Pr(Z_r = 0)\ \ge\ \frac{1}{N} + \frac{0.242811}{N^2}.$$

Numerical calculation of c_r for $N = 256$ and $3 \le r \le 255$ gives that c_r decreases for $4 \le r \le 255$ (as in Fig. 10). Thus, $c_4 = 1.337057 \ge c_r \ge 0.242811 = c_{255}$ for $4 \le r \le 255$, and the special case $c_3 = 0.351089$ for $r = 3$ also falls within the same bounds. Hence the bounds on $\Pr(Z_r = 0)$.

Figure 11 depicts a comparison between the theoretical and experimental values of $\Pr(Z_r = 0)$ plotted against r, where $N = 256$ and $3 \le r \le 255$, and the experimentation is performed over 1 billion runs of RC4, each with a randomly generated 16-byte key.

Let E_r denote the event $(Z_r = 0)$ for some $3 \le r \le 255$. If we write $p = 1/N$ and $q = c_r/N$, then to distinguish RC4 keystream from random sequence based on event E_r, one would need number of samples of the order of $(1/N)^{-1} \cdot (c_r/N)^{-2} \sim N^3$. It will be interesting to see if one can combine the effect of all these distinguishers to have a stronger one.

In this section, we have contradicted MS-Claim-1 by proving the biases in $\Pr(Z_r = 0)$ for all $3 \le r \le 255$. If the supporting statement MS-Claim-2 was correct, then one would have a positive bias $\Pr(Z_r = 0 \mid j_r = 0) > \frac{1}{N}$. However, we have run extensive experiments to confirm that $\Pr(Z_r = 0 \mid j_r = 0) \approx \frac{1}{N}$, thereby contradicting MS-Claim-2 as well.

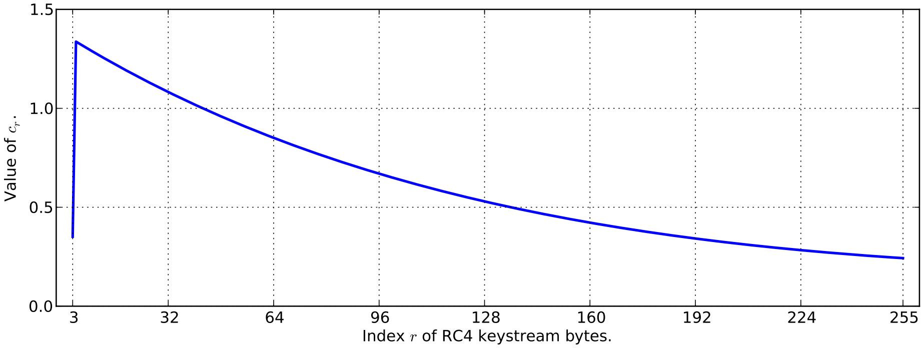

Fig. 10. Value of c_r versus r during RC4 PRGA ($N = 256$ and $3 \le r \le 255$).

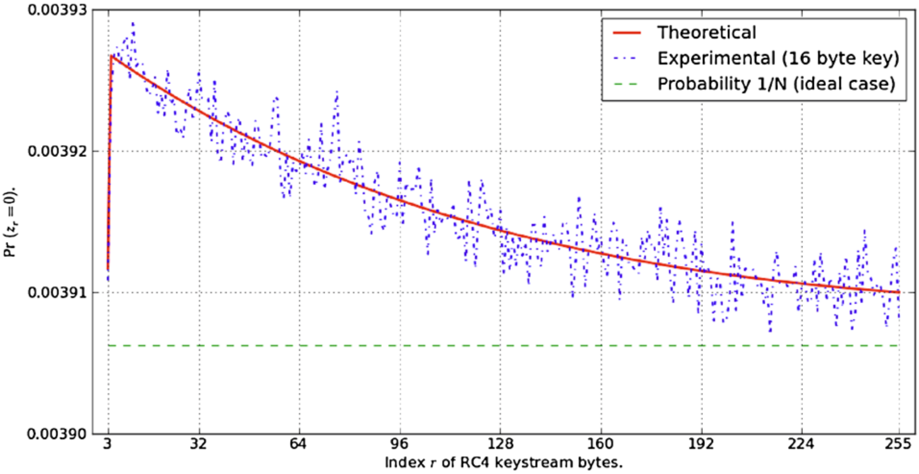

Fig. 11. $\Pr(Z_r = 0)$ versus r during RC4 PRGA ($3 \le r \le 255$).

4.2.1. *Guessing State Information Using the Bias in Z_r*

Mantin and Shamir [18] used the bias of the second byte of RC4 keystream to guess some information regarding $S_0[2]$, based on the following:

$$\Pr\bigl(S_0[2] = 0 \mid Z_2 = 0\bigr) = \frac{\Pr(S_0[2] = 0)}{\Pr(Z_2 = 0)} \cdot \Pr\bigl(Z_2 = 0 \mid S_0[2] = 0\bigr) \approx \frac{1/N}{2/N} \cdot 1 = \frac{1}{2}.$$

Note that in the above expression, no randomness assumption is required to obtain $\Pr(S_0[2] = 0) = 1/N$. This probability is exact and can be derived by substituting $u = 2, v = 0$ in Proposition 1. Hence, on every occasion we obtain $Z_2 = 0$ in the keystream, we can guess $S_0[2]$ with probability $1/2$, and this is significantly more than a random guess with probability $1/N$.

In this section, we use the biases in bytes 3 to 255 (observed in Theorem 14) to extract similar information about the state array S_{r-1} using the RC4 keystream byte Z_r.

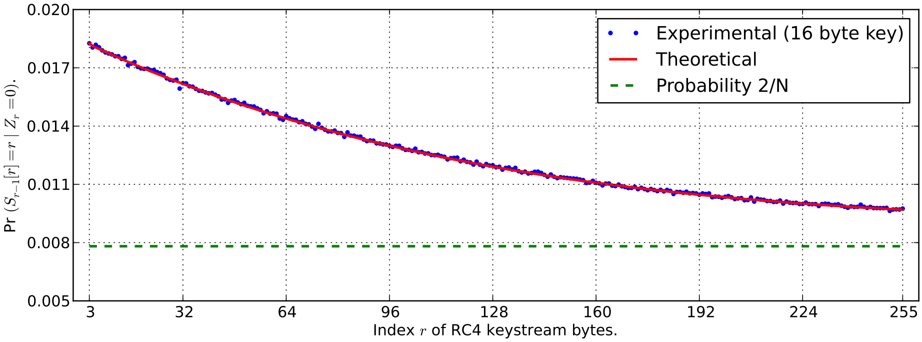

Fig. 12. $\Pr(S_{r-1}[r] = r \mid Z_r = 0)$ versus r during RC4 PRGA ($3 \le r \le 255$).

In particular, we try to explore the conditional probability $\Pr(S_{r-1}[r] = r \mid Z_r = 0)$ for $3 \le r \le 255$, as follows:

$$\Pr\bigl(S_{r-1}[r] = r \mid Z_r = 0\bigr) = \frac{\Pr(Z_r = 0 \wedge S_{r-1}[r] = r)}{\Pr(Z_r = 0)} \approx \frac{\Pr(S_{r-1}[r] = r) \cdot \frac{2}{N}}{\frac{1}{N} + \frac{c_r}{N^2}}.$$

In the above expression, c_r is as in Theorem 14, and one may write:

$$\Pr\bigl(S_{r-1}[r] = r\bigr) = \begin{cases} 1/N + (1/N - 1/N^2) \cdot (c_r + (N-2)/(N-1)), & \text{for } r = 3; \\ 1/N + (1/N - 1/N^2) \cdot c_r, & \text{for } 3 < r \le N-1. \end{cases}$$

In Fig. 12, we plot the theoretical values of $\Pr(S_{r-1}[r] = r \mid Z_r = 0)$ for $3 \le r \le 255$ and $N = 256$, and the corresponding experimental values over 1 billion runs of RC4 with random 16-byte keys. It clearly shows that all values of $\Pr(S_{r-1}[r] = r \mid Z_r = 0)$ for $N = 256$ and $3 \le r \le 255$ (both theoretical and experimental) are greater than $2/N$. Thus, one can guess $S_{r-1}[r]$ with probability more than twice of that of a random guess, every time we obtain $Z_r = 0$ in the keystream.

Remark 3. In proving Corollary 2, we use the initial condition $S_1[r] = r$ to branch out the probability paths, and not $S_0[r] = r$ as in Ref. [16, Lemma 1]. This is because the probability of $S[r] = r$ takes a leap from around $1/N$ in S_0 to about $2/N$ in S_1, and this turns out to be the actual cause behind the bias in $S_{r-1}[r] = r$. Consideration of this issue eventually corrects the mismatches observed in the graphs of Ref. [16, Figs. 2 and 3]. Note that Theorem 14, Fig. 11 and Fig. 12 are, respectively, the corrected versions of Theorem 1, Fig. 2 and Fig. 3 in Ref. [16].

4.2.2. *Attacking the RC4 Broadcast Scheme*

We revisit the famous attack of Mantin and Shamir [18] on broadcast RC4, where the same plaintext is encrypted using multiple secret keys, and then the ciphertexts are broadcast to a group of recipients. In Ref. [18], the authors propose a practical attack against an RC4 implementation of the broadcast scheme, based on the bias observed in the second keystream byte. They prove that an attacker that collects $\Omega(N)$ number of ciphertexts corresponding to the same plaintext M, can easily deduce the second byte of M, by exploiting the bias in Z_2.

In a similar line of action, we may exploit the bias observed in bytes 3 to 255 of the RC4 keystream to mount a similar attack on RC4 broadcast scheme. Notice that we obtain a bias of the order of $1/N^2$ in each of the bytes Z_r where $3 \le r \le 255$. Thus, roughly speaking, if the attacker obtains about N^3 ciphertexts corresponding to the same plaintext M (from the broadcast scheme), then he can check the frequency of occurrence of bytes to deduce the rth ($3 \le r \le 255$) byte of M. We can formally state our result (analogous to Ref. [18, Theorem 3]) as follows.

Theorem 15. *Let M be a plaintext,and let $C_1, C_2, \ldots, C_w$ be the RC4 encryptions of M under w uniformly distributed keys. Then if $w = \Omega(N^3)$, the bytes 3 to 255 of M can be reliably extracted from $C_1, C_2, \ldots, C_w$.*

Proof. Recall from Theorem 14 that $\Pr(Z_r = 0) \approx 1/N + c_r/N^2$ for all $3 \le r \le 255$ in RC4. Thus, for each encryption key chosen during broadcast, the rth plaintext byte $M[r]$ has probability $1/N + c_r/N^2$ to be XOR-ed with 0. Due to this bias, $(1/N + c_r/N^2)$ fraction of the rth ciphertext bytes will have the same value as the rth plaintext byte. When $w = \Omega(N^3)$, the attacker can identify the most frequent byte in $C_1[r], C_2[r], \ldots, C_w[r]$ as $M[r]$ with constant probability of success. □

The attack on broadcast RC4 is applicable to many modern Internet protocols (such as group emails encrypted under different keys, group-ware multi-user synchronization, etc.). Note that Mantin and Shamir's attack [18] works at the byte level. It can recover only the second byte of the plaintext under some assumptions. On the other hand, our attack can recover an additional 253 bytes (namely, bytes 3 to 255) of the plaintext as well.

4.3. *A New Long-Term Bias in RC4 Keystream*

The biases discussed so far are prevalent in the initial bytes of the RC4 keystream, and are generally referred to as the short-term biases. It is a common practice to discard a few hundred initial bytes of the keystream to avoid these biases, and this motivates the search for long-term biases in RC4 that are present even after discarding an arbitrary number of initial bytes.

The first result in this direction was observed in 1997 by Golic [8], where certain correlation was found between the least significant bits of the two non-consecutive output bytes Z_r and Z_{r+2}, for all rounds r of RC4. In 2000, a set of results was proposed by Fluhrer and McGrew [6], where the biases depend upon the frequency of occurrence of certain digraphs in the RC4 keystream. Later in 2005, Mantin [19] improved these to obtain the $ABSAB$ distinguisher, which depends on the repetition of digraph AB in the keystream after a gap of string S having G bytes. This is the best long-term distinguisher of RC4 to date. In 2008, Basu et al. [2] identified another conditional long-term bias, depending on the relationship between two consecutive bytes in the keystream.

In this section, we prove that the event $(Z_{wN+2} = 0 \wedge Z_{wN} = 0)$ is positively biased for all $w \geq 1$. After the first long-term bias observed by Golic [8] in 1997, this is the only one that involves non-consecutive bytes of RC4 keystream. Golic [8] proved a strong bitwise correlation between the least significant bits of Z_{wN} and Z_{wN+2}, while we prove a byte-wise correlation between Z_{wN} and Z_{wN+2}, as follows.

Theorem 16. *For any integer $w \geq 1$, assume that the permutation S_{wN} is randomly chosen from the set of all possible permutations of $\{0, \ldots, N-1\}$. Then*

$$\Pr(Z_{wN+2} = 0 \wedge Z_{wN} = 0) \approx 1/N^2 + 1/N^3.$$

Proof. The positive bias in Z_2, proved in Ref. [18], propagates to round $(wN+2)$ if $j_{wN} = 0$. Mantin and Shamir's observation [18, Theorem 1] implies

$$\Pr(Z_{wN+2} = 0 \mid j_{wN} = 0) \approx 2/N - 1/N^2. \tag{18}$$

If $j_{wN} \neq 0$, we observe that Z_{wN+2} does not take the value 0 by uniform random association. In particular, we get the following:

$$\Pr(Z_{wN+2} = 0 \mid j_{wN} \neq 0) \approx 1/N - 1/N^2. \tag{19}$$

For Z_{wN}, we have $i_{wN} = 0$, and when $j_{wN} = 0$ (this happens with probability $1/N$), no swap takes place and the output is $Z_{wN} = S_{wN}[2 \cdot S_{wN}[0]]$. Two cases may arise from here. If $S_{wN}[0] = 0$, then $Z_{wN} = S_{wN}[0] = 0$ for sure. Otherwise if $S_{wN}[0] \neq 0$, the output Z_{wN} takes the value 0 only due to random association. Combining the cases,

$$\Pr(Z_{wN} = 0 \mid j_{wN} = 0) \approx 1/N \cdot 1 + (1 - 1/N) \cdot 1/N = 2/N - 1/N^2. \tag{20}$$

Similarly to $\Pr(Z_{wN+2} = 0 \mid j_{wN} \neq 0)$, it is easy to show that

$$\Pr(Z_{wN} = 0 \mid j_{wN} \neq 0) \approx 1/N - 1/N^2. \tag{21}$$

Now, we may compute the joint probability $\Pr(Z_{wN+2} = 0 \wedge Z_{wN} = 0)$, which is equal to

$$\Pr(Z_{wN+2} = 0 \wedge Z_{wN} = 0 \wedge j_{wN} = 0) + \Pr(Z_{wN+2} = 0 \wedge Z_{wN} = 0 \wedge j_{wN} \neq 0).$$

Given $j_{wN} = 0$, the random variables Z_{wN+2} and Z_{wN} can be considered independent. Using (18) and (20), we get $\Pr(Z_{wN+2} = 0 \wedge Z_{wN} = 0 \wedge j_{wN} = 0)$ as

$$\Pr(Z_{wN+2} = 0 \mid j_{wN} = 0) \cdot \Pr(Z_{wN} = 0 \mid j_{wN} = 0) \cdot \Pr(j_{wN} = 0)$$
$$\approx \left(2/N - 1/N^2\right) \cdot \left(2/N - 1/N^2\right) \cdot (1/N) \approx 4/N^3 - 4/N^4.$$

Using (19) and (21), one has $\Pr(Z_{wN+2} = 0 \wedge Z_{wN} = 0 \wedge j_{wN} \neq 0)$ as

$$\Pr(Z_{wN+2} = 0 \mid j_{wN} \neq 0) \cdot \Pr(Z_{wN} = 0 \mid j_{wN} \neq 0) \cdot \Pr(j_{wN} \neq 0)$$
$$\approx \left(1/N - 1/N^2\right)^2 \cdot (1 - 1/N) \approx 1/N^2 - 3/N^3 + 3/N^4.$$

Adding the two expressions, we have $\Pr(Z_{wN+2} = 0 \wedge Z_{wN} = 0) \approx 1/N^2 + 1/N^3$. □

This is the *first long-term byte-wise correlation* to be observed between *two non-consecutive bytes* (Z_{wN}, Z_{wN+2}). The gap between the related bytes in this case is 1, and we could not find any other significant long-term bias with this gap. An interesting direction for experimentation and analysis would be to look for similar long-term biases with larger gaps between the related bytes.

5. Conclusion

In this paper, we have explored several classes of non-random events in RC4—from key correlations to keystream-based distinguishers, and from short-term biases to long-term non-randomness.

Keylength-Dependent Non-Randomness [*Sect.* 2] In practice, RC4 uses a small secret key of length l that is typically much less than the permutation size N, and this is the source of several key-correlations and biases in the keystream. However, no biases that depend on the length l of the secret key were reported in the literature. In this paper, we demonstrate the first keylength-dependent biases in the RC4 literature. In the process, we prove all the empirical biases used to mount the WEP and WPA attacks [29,31], whose proofs were left open so far. Thus, our current theoretical work complements the practical WEP attacks nicely and completes the whole picture.

Short-Term and Long-Term Non-Randomness [*Sects.* 3 *and* 4] The permutation after the RC4 KSA is non-random, and this is the source of many biases in the initial keystream bytes, including the observations in Refs. [18,23,30]. We prove all significant empirical biases observed in Ref. [30] and also provide theoretical justification for the sine-curve distribution of the first byte observed in Ref. [23]. We also extend the observation of second-byte bias in Ref. [18] to all initial bytes 3 to 255 in the RC4 keystream, and hence generalize the attack on broadcast RC4 protocol. We also discover a new long-term bias in the RC4 keystream.

Future Direction In the search for non-random events in RC4, or other stream ciphers in general, our results open up the following interesting directions of research.

- What are the implications of using a secret key with length relatively small compared to the internal secret state of the cipher? How is the keylength related to the biases?
- Is there a general pattern in the non-random events generated from the initial non-random state produced by the KSA? Can we find more short-term biases in this direction?
- How does one generalize the concept of digraph biases to related bytes with arbitrary gaps in between? Are there more long-term biases of this kind in the RC4 keystream?

Acknowledgements

We are sincerely thankful to the anonymous reviewers for their detailed review reports containing invaluable feedback and kind suggestions. These reports helped in substantially improving the technical quality as well as the editorial aspects of our paper. We are also grateful to the Centre of Excellence in Cryptology (CoEC), Indian Statistical Institute, Kolkata, funded by the Government of India, for partial support towards this project.

References

[1] M. Akgün, P. Kavak, H. Demirci, New results on the key scheduling algorithm of RC4, in *INDOCRYPT'08*. Lecture Notes in Computer Science, vol. 5365 (2008), pp. 40–52

[2] R. Basu, S. Ganguly, S. Maitra, G. Paul, A complete characterization of the evolution of RC4 pseudo random generation algorithm. *J. Math. Cryptol.* **2**(3), 257–289 (2008)

[3] R. Basu, S. Maitra, G. Paul, T. Talukdar, On some sequences of the secret pseudo-random index j in RC4 key scheduling, in *AAECC'09*. Lecture Notes in Computer Science, vol. 5527 (2009), pp. 137–148

[4] E. Biham, Y. Carmeli, Efficient reconstruction of RC4 keys from internal states, in *FSE'08*. Lecture Notes in Computer Science, vol. 5086 (2008), pp. 270–288

[5] J. Chen, A. Miyaji, How to find short RC4 colliding key pairs, in *ISC'11*. Lecture Notes in Computer Science, vol. 7001 (2011), pp. 32–46

[6] S.R. Fluhrer, D.A. McGrew, Statistical analysis of the alleged RC4 keystream generator, in *FSE'00*. Lecture Notes in Computer Science, vol. 1978 (2000), pp. 19–30

[7] S.R. Fluhrer, I. Mantin, A. Shamir, Weaknesses in the key scheduling algorithm of RC4, in *SAC'01*. Lecture Notes in Computer Science, vol. 2259 (2001), pp. 1–24

[8] J.D. Golic, Linear statistical weakness of alleged RC4 keystream generator, in *EUROCRYPT'97*. Lecture Notes in Computer Science, vol. 1233 (1997), pp. 226–238

[9] J.D. Golic, Iterative probabilistic cryptanalysis of RC4 keystream generator, in *ACISP'00*. Lecture Notes in Computer Science, vol. 1841 (2000), pp. 220–233

[10] J.D. Golic, G. Morgari, Iterative probabilistic reconstruction of RC4 internal states. *IACR Cryptology ePrint Archive*, Report 2008/348 (2008). Available at http://eprint.iacr.org/2008/348

[11] A.L. Grosul, D.S. Wallach, A related-key cryptanalysis of RC4. Technical Report TR-00-358, Department of Computer Science, Rice University (2000)

[12] R.J. Jenkins, ISAAC and RC4 (1996). Published on the Internet at http://burtleburtle.net/bob/rand/isaac.html

[13] S. Khazaei, W. Meier, On reconstruction of RC4 keys from internal states, in *MMICS'08*. Lecture Notes in Computer Science, vol. 5393 (2008), pp. 179–189

[14] A. Klein, Attacks on the RC4 stream cipher. *Des. Codes Cryptogr.* **48**(3), 269–286 (2008)

[15] L.R. Knudsen, W. Meier, B. Preneel, V. Rijmen, S. Verdoolaege, Analysis methods for (alleged) RC4, in *ASIACRYPT'98*. Lecture Notes in Computer Science, vol. 1514 (1998), pp. 327–341

[16] S. Maitra, G. Paul, S. Sen Gupta, Attack on broadcast RC4 revisited, in *FSE'11*. Lecture Notes in Computer Science, vol. 6733 (2011), pp. 199–217

[17] I. Mantin, Analysis of the stream cipher RC4. Master's Thesis, The Weizmann Institute of Science, Israel (2001). Available at http://www.wisdom.weizmann.ac.il/~itsik/RC4/rc4.html

[18] I. Mantin, A. Shamir, A practical attack on broadcast RC4, in *FSE'01*. Lecture Notes in Computer Science, vol. 2355 (2002), pp. 152–164

[19] I. Mantin, Predicting and distinguishing attacks on RC4 keystream generator, in *EUROCRYPT'05*. Lecture Notes in Computer Science, vol. 3494 (2005), pp. 491–506

[20] I. Mantin, A practical attack on the fixed RC4 in the WEP mode, in *ASIACRYPT'05*. Lecture Notes in Computer Science, vol. 3788 (2005), pp. 395–411

[21] M. Matsui, Key collisions of the RC4 stream cipher, in *FSE'09*. Lecture Notes in Computer Science, vol. 5665 (2009), pp. 38–50

[22] A. Maximov, D. Khovratovich, New state recovery attack on RC4, in *CRYPTO'08*. Lecture Notes in Computer Science, vol. 5157 (2008), pp. 297–316

[23] I. Mironov, (Not so) random shuffles of RC4, in *CRYPTO'02*. Lecture Notes in Computer Science, vol. 2442 (2002), pp. 304–319

[24] S. Mister, S.E. Tavares, Cryptanalysis of RC4-like ciphers, in *SAC'98*. Lecture Notes in Computer Science, vol. 1999 (1998), pp. 131–143

[25] S. Paul, B. Preneel, Analysis of non-fortuitous predictive states of the RC4 keystream generator, in *INDOCRYPT'03*. Lecture Notes in Computer Science, vol. 2904 (2003), pp. 52–67

[26] G. Paul, S. Maitra, Permutation after RC4 key scheduling reveals the secret key, in *SAC'07*. Lecture Notes in Computer Science, vol. 4876 (2007), pp. 360–377

[27] 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://www.impic.org/papers/WeakKeys-report.pdf

[28] S. Sen Gupta, S. Maitra, G. Paul, S. Sarkar, Proof of empirical RC4 biases and new key correlations, in *SAC'11*. Lecture Notes in Computer Science, vol. 7118 (2011), pp. 151–168

[29] P. Sepehrdad, Statistical and algebraic cryptanalysis of lightweight and ultra-lightweight symmetric primitives. Ph.D. Thesis, No. 5415, École Polytechnique Fédérale de Lausanne (EPFL) (2012). Available at http://lasecwww.epfl.ch/~sepehrdad/Pouyan_Sepehrdad_PhD_Thesis.pdf

[30] P. Sepehrdad, S. Vaudenay, M. Vuagnoux, Discovery and exploitation of new biases in RC4, in *SAC'10*. Lecture Notes in Computer Science, vol. 6544 (2011), pp. 74–91

[31] P. Sepehrdad, S. Vaudenay, M. Vuagnoux, Statistical attack on RC4—distinguishing WPA, in *EUROCRYPT'11*. Lecture Notes in Computer Science, vol. 6632 (2011), pp. 343–363

[32] Y. Shiraishi, T. Ohigashi, M. Morii, An improved internal-state reconstruction method of a stream cipher RC4, in *Communication, Network, and Information Security*. Track 440-088, New York, USA, December 10–12 (2003)

[33] V. Tomasevic, S. Bojanic, O. Nieto-Taladriz, Finding an internal state of RC4 stream cipher. *Inf. Sci.* **177**, 1715–1727 (2007)

[34] E. Tews, R.-P. Weinmann, A. Pyshkin, Breaking 104 bit WEP in less than 60 seconds, in *WISA'07*. Lecture Notes in Computer Science, vol. 4867 (2007), pp. 188–202

[35] E. Tews, M. Beck, Practical attacks against WEP and WPA, in *WISEC'09* (ACM, New York, 2009), pp. 79–86

[36] S. Vaudenay, M. Vuagnoux, Passive-only key recovery attacks on RC4, in *SAC'07*. Lecture Notes in Computer Science, vol. 4876 (2007), pp. 344–359

[37] D.A. Wagner, My RC4 weak keys (1995). http://www.cs.berkeley.edu/~daw/my-posts/my-rc4-weak-keys