DE GRUYTER J. Math. Cryptol. 2018; 12(1): 43–56

Research Article

Sabyasachi Dey and Santanu Sarkar*

# Generalization of Roos bias in RC4 and some results on key-keystream relations

https://doi.org/10.1515/jmc-2016-0061
Received October 28, 2016; revised June 11, 2017; accepted January 6, 2018

**Abstract:** RC4 has attracted many cryptologists due to its simple structure. In [9], Paterson, Poettering and Schuldt reported the results of a large scale computation of RC4 biases. Among the biases reported by them, we try to theoretically analyze a few which show very interesting visual patterns. We first study the bias which relates the key stream byte $z_i$ with $i - k[0]$, where $k[0]$ is the first byte of the secret key. We then present a generalization of the Roos bias. In 1995, Roos observed the bias of initial bytes $S[i]$ of the permutation after KSA towards $f_i = \sum_{r=1}^{i} r + \sum_{r=0}^{i} K[r]$. Here we study the probability of $S[i]$ equaling $f_y = \sum_{r=1}^{y} r + \sum_{r=0}^{y} K[r]$ for $i \neq y$. Our generalization provides a complete correlation between $z_i$ and $i - f_y$. We also analyze the key-keystream relation $z_i = f_{i-1}$ which was studied by Maitra and Paul [6] in FSE 2008. We provide more accurate formulas for the probability of both $z_i = i - f_i$ and $z_i = f_{i-1}$ for different $i$'s than the existing works.

**Keywords:** Cryptanalysis, keystream, RC4, Roos bias, stream cipher

**MSC 2010:** 94A60

## 1 Introduction

RC4 is a stream cipher which has been widely used worldwide and has become one of the most popular ciphers in the world for the last 25 years. RC4 is a very simple cipher and can be implemented only in a few lines of code. This cipher was designed by Ron Rivest in 1987. Its first application was in Data security. It was also used in RSA Lotus Notes. Though RC4 was a trade secret in the beginning, in 1994 it was published. The first adoption of this cipher was done by the network protocol TLS. Later it has been used in WEP in 1997 [18], SSL in 1995, WPA in 2003 [19], etc.

At first, we describe the design of RC4 briefly. It has two components. The first component is the key scheduling algorithm (KSA) and the other one the pseudo-random generation algorithm (PRGA). Here, all the operations are done modulo 256. The KSA takes an identity permutation $S$ of 0 to 255. By using an $\ell$-byte secret key, it scrambles the identity permutation over $\mathbb{Z}_N$, and derives another permutation. After the completion of KSA, PRGA generates a pseudo-random sequence of keystream bytes, using the scrambled permutation of KSA for $z_1, z_2, \ldots$. After each iteration from 0 to 255, an output $z_i$ is produced. These are bitwise XOR-ed with the plaintext to produce the ciphertext. Both for the KSA and the PRGA, two indices $i$ and $j$ are used in the permutation. In both of these, a swap between $S[i]$ and $S[j]$ takes place.

**Sabyasachi Dey,** Indian Institute of Technology, Madras, India, e-mail: sabya.ndp@gmail.com
***Corresponding author: Santanu Sarkar,** Indian Institute of Technology, Madras, India, e-mail: sarkar.santanu.bir@gmail.com

**KSA.**
$N = 256$;
Initialization:
  For $i = 0, \dots, N-1$
    $S[i] = i$;
  $j = 0$;
Scrambling:
  For $i = 0, \dots, N-1$
    $j = (j + S[i] + K[i])$;
    Swap($S[i], S[j]$).

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

We use $S_r^{\mathrm{KSA}}$, $i_r^{\mathrm{KSA}}$ and $j_r^{\mathrm{KSA}}$ to denote the permutation and the two indices after the $r$-th round of RC4 KSA. Hence $S_N^{\mathrm{KSA}}$ is the permutation after the complete key scheduling. By $S_r$, $i_r$, $j_r$ we denote the permutation and the two indices after the $r$-th round of RC4 PRGA. So $S_N^{\mathrm{KSA}} = S_0$. We use $I_{a,b}$ to denote the indicator function. So

$$I_{a,b} = \begin{cases} 1 & \text{for } a = b, \\ 0 & \text{for } a \neq b. \end{cases}$$

Also, by the notation $f_y$ we denote the expression $\frac{y(y+1)}{2} + \sum_{r=0}^{y} K[r]$ $(0 \leq y \leq N-1)$, which plays a vital role in most of the proposed attacks on RC4.

For having such a simple design, many cryptologists have been attracted to this cipher. Throughout the last 25 years, multiple weaknesses of RC4 have been found. One of the most remarkable attacks was presented by Fluhrer, Mantin and Shamir [2] in 2001. This attack was based on the weaknesses in the key scheduling algorithm. In 1995, Roos [12] observed that after the KSA, the most likely value of $S_N^{\mathrm{KSA}}[y]$ for the first few values of $y$ is given by $S_N^{\mathrm{KSA}}[y] = f_y$. The experimentally found values of the probabilities $\mathrm{P}(S_N^{\mathrm{KSA}}[y] = f_y)$ decrease from 0.37 to 0.006 as $y$ increases from 0 to 47. Later, the theoretical proof of this was given by Paul and Maitra in SAC 2007 [11]. Recently, Sarkar and Venkateswarlu [13] improved the analysis of [11]. Paul and Maitra [11] also discussed a reconstruction algorithm to find the key from the final permutation $S_N$ after KSA using Roos biases. Klein [5] observed correlations between keystreams and key using Roos biases. In FSE 2008, Maitra and Paul [6] showed that not only the permutation bytes $S_N^{\mathrm{KSA}}[y]$, but also the bytes $S_N^{\mathrm{KSA}}[S_N^{\mathrm{KSA}}[y]]$, $S_N^{\mathrm{KSA}}[S_N^{\mathrm{KSA}}[S_N^{\mathrm{KSA}}[y]]]$, etc. are biased towards $f_y$. Then in SAC 2010, Sepehrdad, Vaudenay and Vuagnoux [15] showed some biases on the state variables, initial keystream bytes and secret key of RC4. They also gave a key recovery attack on RC4 in WPA. In Eurocrypt 2011, Sepehrdad, Vaudenay and Vuagnoux [16] presented an attack on WEP by using all the previous known attacks in the literature and by introducing a few new correlations.

In USENIX 2013, AlFardan, Bernstein, Paterson, Poettering and Schuldt [1] used a Bayesian statistical method that recovers plaintexts in a broadcast attack model, i.e., plaintexts that are repeatedly encrypted with different keys under RC4. AlFardan et al. successfully used their idea to attack the cryptographic protocol TLS by exploiting biases in RC4 keystreams. In FSE 2014, Paterson, Schuldt and Poettering [10] and Sengupta, Maitra, Meier, Paul and Sarkar [14] exploited independently keystream and key correlations to recover plaintext in WPA since the first three bytes of the RC4 key in WPA are public. In Asiacrypt 2014, Paterson, Poettering and Schuldt [9] improved the attack of [10]. They performed large-scale computations using the Amazon EC2 cloud computing infrastructure to obtain accurate estimates of the single-byte and double-byte distributions.

The recent attacks on RC4-based protocols have led to the consensus that RC4 is insecure and should be phased out. For an example, Vanhoef and Piessens [17] presented an attack on TLS and WPA using RC4 (USENIX 2015). Also, Jha, Banik, Isobe and Ohigashi [4] presented some works on joint distribution of keystream biases. These works show that RC4 is still an active area of research.

**Our contribution and the organisation of the paper.** (i) In Asiacrypt 2014, Paterson et al. [9] showed a significant negative bias of $z_i$ towards $i - K[0]$ (see [9, Figure 2]). But so far there was no theoretical justification behind this. In Section 2, for the first time we give a theoretical justification for this bias.

(ii) In 1995, Roos [12] observed the relation between $S_N^{\mathrm{KSA}}[i]$ and $f_i$. This observation was later justified in [11]. We generalize the Roos bias in Section 3 and study the relation between $S_N^{\mathrm{KSA}}[i]$ and $f_y$ for $i \neq y$.

(iii) In Section 3, our generalized Roos bias gives complete distribution of $z_i$ and $i - f_y$ for $y \neq i$. We observe a significant negative bias between $z_i$ and $i - f_{i+t}$ for a small positive integer $t$.

(iv) Klein discovered the correlation between $z_i$ and $i - f_i$ for $1 \leq i \leq N - 1$. Maitra and Paul [6] proved these biases theoretically in FSE 2008. Using our general result of Theorem 3.7, we revisit this problem. In Table 1, we compare our result to the previous one. Our analysis gives much closer values to the experimental values.

(v) In FSE 2008, Maitra and Paul [6] also studied the biases between $z_i$ and $f_{i-1}$ for $i = 1$ and $3 \leq i \leq N - 1$. In Section 4, we analyze the bias of $z_i$ towards $f_{i-1}$. In Table 3, we present the comparative study between our result and [6]. In this case also, our analysis gives a much better approximation to the experimental values than the work [6].

## 2 Negative bias of $z_i$ towards $i - K[0]$

Let us start with the following lemma.

**Lemma 2.1.** *After KSA, $P(S_N^{\mathrm{KSA}}[i] = K[0]) = \frac{1}{N}(1 - \frac{1}{N})^{(N-1-i)}$ for $i \geq 1$.*

*Proof.* If $S_i^{\mathrm{KSA}}[j_{i+1}^{\mathrm{KSA}}] = K[0]$, after the swap, $S_{i+1}^{\mathrm{KSA}}[i^{\mathrm{KSA}}] = K[0]$. Now

$$\mathrm{P}(S_i^{\mathrm{KSA}}[j_{i+1}^{\mathrm{KSA}}] = K[0]) = \frac{1}{N}$$

since $j_{i+1}^{\mathrm{KSA}}$ is random. Also $S_N^{\mathrm{KSA}}[i]$ will be $K[0]$ only if the $j^{\mathrm{KSA}}$'s cannot touch $i$ again, i.e., if all $j_{i+2}^{\mathrm{KSA}}, \dots, j_N^{\mathrm{KSA}}$ are different from $i$, then $S_N^{\mathrm{KSA}}[i]$ will be $K[0]$. The probability of $j_{i+2}^{\mathrm{KSA}}, j_{i+3}^{\mathrm{KSA}}, \dots, j_N^{\mathrm{KSA}} \neq i$ is $(1 - \frac{1}{N})^{(N-1-i)}$. Therefore, $\mathrm{P}(S_N^{\mathrm{KSA}}[i] = K[0]) = \frac{1}{N}(1 - \frac{1}{N})^{(N-1-i)}$ for $i \geq 1$. □

Now we have the following result.

**Lemma 2.2.** *In PRGA, for $i \geq 1$,*

$$P(S_{i-1}[i] = K[0]) = p_i\Big(1 - \frac{1}{N}\Big)^{i-1} + \frac{1}{N}\Big(1 - \frac{1}{N}\Big)^{i-2}\sum_{l=1}^{i-1} p_l + \sum_{r=2}^{i-1}\frac{1}{N^r}\Big(1 - \frac{1}{N}\Big)^{i-r-1}\sum_{l=1}^{i-1} p_l\binom{i-l-1}{r-1},$$

*where $p_i = \frac{1}{N}(1 - \frac{1}{N})^{(N-1-i)}$.*

*Proof.* We find the probability of this event by breaking it into mutually disjoint events and finding their probabilities separately.

- Event 1: After the completion of KSA, $K[0]$ is in the $i$-th location of the array (whose probability is $p_i$ from Lemma 2.1), and this position is not touched by $j_1, \dots, j_{i-1}$. The probability of this event is $p_i(1 - \frac{1}{N})^{i-1}$.
- Event 2: After the completion of KSA, $K[0]$ is in some $l$-th location of the array (whose probability is $p_l$), where $1 \leq l \leq i - 1$. This position is not touched by $j_1, \dots, j_{l-1}$. Then $j_l = i$. After that, $j_{l+1}, \dots, j_{i-1} \neq i$.

Since $l$ can vary from 1 to $i-1$, the total probability of the above path is

$$\sum_{l=1}^{i-1} \frac{1}{N}\Big(1-\frac{1}{N}\Big)^{i-2} p_l.$$

- Event 3: After the completion of KSA, $K[0]$ is in $l$–th location of the array, where $1 \le l \le i-1$. This position is not touched by $j_1, \dots, j_{l-1}$. Then $j_l = t$ for $l+1 \le t \le i-1$. After that, $j_{l+1}, \dots, j_{t-1} \ne t$. Then $j_t = i$. Also $j_{t+1}, \dots, j_{i-1} \ne i$. The total probability of this path is

$$\sum_{l=1}^{i-1}\sum_{t=l+1}^{i-1} \frac{1}{N^2}\Big(1-\frac{1}{N}\Big)^{i-3} p_l.$$

Similarly, $K[0]$ can come to the $i$-th location with more than two jumps. If it comes through the $(r+1)$-st jump, the total probability will be

$$\begin{aligned}\frac{1}{N^r}\Big(1-\frac{1}{N}\Big)^{i-r-1}\sum_{l_1=1}^{i-1}\sum_{l_2=l_1+1}^{i-1}\sum_{l_3=l_2+1}^{i-1}\cdots\sum_{l_r=l_{r-1}+1}^{i-1} p_{l_1} &= \frac{1}{N^r}\Big(1-\frac{1}{N}\Big)^{i-r-1}\sum_{l_1=1}^{i-1} p_{l_1}\Big(\sum_{l_2=l_1+1}^{i-1}\sum_{l_3=l_2+1}^{i-1}\cdots\sum_{l_r=l_{r-1}+1}^{i-1} 1\Big)\\ &= \frac{1}{N^r}\Big(1-\frac{1}{N}\Big)^{i-r-1}\sum_{l_1=1}^{i-1} p_{l_1}\binom{i-l_1-1}{r-1}.\end{aligned}$$

Thus adding the probabilities of these three disjoint events, we have

$$\mathrm{P}(S_{i-1}[i] = K[0]) = p_i\Big(1-\frac{1}{N}\Big)^{i-1} + \frac{1}{N}\Big(1-\frac{1}{N}\Big)^{i-2}\sum_{l=1}^{i-1} p_l + \sum_{r=2}^{i-1}\frac{1}{N^r}\Big(1-\frac{1}{N}\Big)^{i-r-1}\sum_{l=1}^{i-1} p_l\binom{i-l-1}{r-1}. \qquad \square$$

We can use this lemma to find the probability $\mathrm{P}(z_i = i - K[0])$. The following result gives a bias of $z_i$ towards $(i - K[0])$.

**Theorem 2.3.** *We have*

$$P(z_i = i-K[0]) = \begin{cases} P(S_0[1] = K[0])\cdot\frac{1}{N}\cdot\Big(1-\frac{1}{N}\Big) + \Big(1-\frac{1}{N}+\frac{1}{N^2}\Big)\frac{1}{N} & \text{for } i = 1,\\ P(S_{i-1}[i] = K[0])\cdot\frac{1}{N} + \Big(1-\frac{1}{N}\Big)\frac{1}{N} & \text{for } i > 1.\end{cases}$$

*Proof.* First consider $i > 1$.

(i) Consider the event $A : ((S_{i-1}[i] \ne K[0]) \cap (S_{i-1}[j_i] = i-K[0]))$. So after the swap, $S_i[i] = i - K[0]$ and $S_i[j_i] \ne K[0]$. So $z_i = S_i[S_i[i] + S_i[j_i]] \ne S_i[i] = i - K[0]$.

(ii) Next consider the event $B : ((S_{i-1}[i] = K[0]) \cap (S_{i-1}[j_i] = i-K[0]))$. Then

$$z_i = S_i[S_i[i] + S_i[j_i]] = S_i[i] = i - K[0].$$

(iii) Now consider the event $C = (A \cup B)^c$. In this case, $\mathrm{P}(z_i = i - K[0]) = \frac{1}{N}$, considering a random association. Also $\mathrm{P}(C) = 1 - \mathrm{P}(A\cup B) = 1 - \mathrm{P}(S_{i-1}[j_i] = i - K[0]) = 1 - \frac{1}{N}$.

Thus,

$$\begin{aligned}\mathrm{P}(z_i = i-K[0]) &= \mathrm{P}(z_i = i-K[0] \mid A)\mathrm{P}(A) + \mathrm{P}(z_i = i-K[0] \mid B)\mathrm{P}(B) + \mathrm{P}(z_i = i-K[0] \mid C)\mathrm{P}(C)\\ &= 0\cdot\mathrm{P}(A) + 1\cdot\mathrm{P}(B) + \frac{1}{N}\cdot\mathrm{P}(C)\\ &= \mathrm{P}(S_{i-1}[i] = K[0])\cdot\frac{1}{N} + \Big(1-\frac{1}{N}\Big)\frac{1}{N}.\end{aligned}$$

Now for $i = 1$, we have $j_1 = 1$ when $S_0[1] = 1$. In this case, $B$ is an impossible event. So for $i = 1$ we take

$$\begin{aligned}&A : \big((S_0[1] \ne K[0]) \cap (S_0[j_1] = 1-K[0]) \cap (K[0] \ne 1)\big),\\ &B : \big((S_0[i] = K[0]) \cap (S_0[j_1] = 1-K[0]) \cap (K[0] \ne 1)\big).\end{aligned}$$

In this case,

$$\mathrm{P}(z_1 = 1-K[0]) = \mathrm{P}(S_0[1] = K[0])\cdot\frac{1}{N}\cdot\Big(1-\frac{1}{N}\Big) + \Big(1-\frac{1}{N}+\frac{1}{N^2}\Big)\frac{1}{N}. \qquad \square$$

In Figure 1, we plot the theoretical as well as experimental values of $\mathrm{P}(z_i = i - K[0])$ with key length 16, where the experiments have been run over 100 billion trials of RC4 PRGA with randomly generated keys.

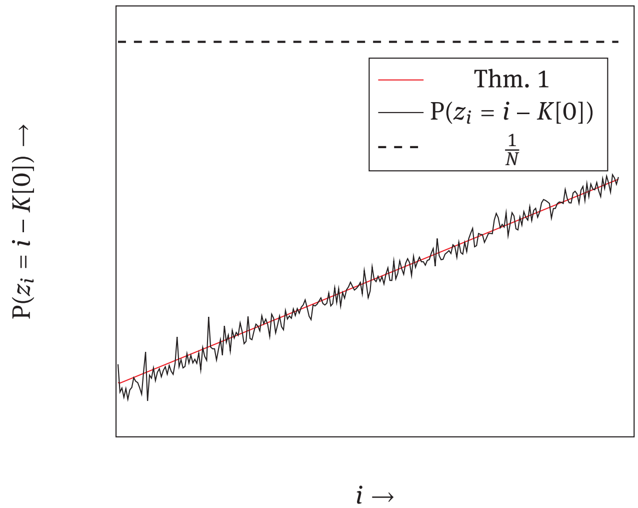



**Figure 1:** Distribution of $P(z_i = i - K[0])$ for $i \in [1, 255]$.

# 3 Generalization of Roos bias and bias of $z_i = i - f_y$

A theoretical justification of the Roos bias has first appeared in [11]. Recently, the work of [11] has been revisited in [13]. We need the following result of [13, Lemma 2].

**Lemma 3.1.** *In KSA, the probability of $P(S_{i+1}^{\mathrm{KSA}}[i] = f_i)$ can be given by*

$$\Big(\prod_{r=1}^{i}\Big(1-\frac{r}{N}\Big)+p_1\Big)\cdot\Big(1-\frac{i}{N}\Big)\cdot\Big(1-\frac{1}{N}\Big)^i+\frac{1}{N}\cdot\Big[1-\Big(\Big(1-\frac{i}{N}\Big)\cdot\Big(1-\frac{1}{N}\Big)^i+\frac{i}{N}\cdot\Big(1-\frac{1}{N}\Big)^i$$
$$+\Big(1-\frac{i}{N}\Big)\cdot\Big(1-\Big(1-\frac{1}{N}\Big)^i\Big)\Big)\cdot\prod_{r=1}^{i}\Big(1-\frac{r}{N}\Big)-(p_1+p_2)\Big(1-\frac{i}{N}\Big)\Big(1-\frac{1}{N}\Big)^i\Big],$$

*where*

$$p_1=\sum_{c=1}^{\infty}\frac{1}{\Phi(\frac{b-\mu}{\sigma})-\Phi(-\frac{\mu}{\sigma})}\cdot\frac{1}{\sigma}\int_{cN-0.5}^{\min\{cN+0.5,\,i(i+1)/2\}}\phi\Big(\frac{x-\mu}{\sigma}\Big)dx,$$
$$p_2=\sum_{c=0}^{\infty}\frac{1}{\Phi(\frac{b-\mu}{\sigma})-\Phi(-\frac{\mu}{\sigma})}\cdot\frac{1}{\sigma}\int_{0.5+cN}^{\min\{(c+1)N-0.5,\,i(i+1)/2\}}\phi\Big(\frac{x-\mu}{\sigma}\Big)dx,$$
$$\mu=\sum_{p=0}^{i}\sum_{x=0}^{p-1}\Big(1-\frac{1}{N}\Big)^x\frac{1}{N}(p-x),$$
$$\sigma^2=\sum_{p=0}^{i}\Big[\sum_{x=0}^{p-1}\Big(1-\frac{1}{N}\Big)^x\frac{1}{N}(p-x)^2-\Big(\sum_{x=0}^{r-1}\Big(1-\frac{1}{N}\Big)^x\frac{1}{N}(p-x)\Big)^2\Big],$$

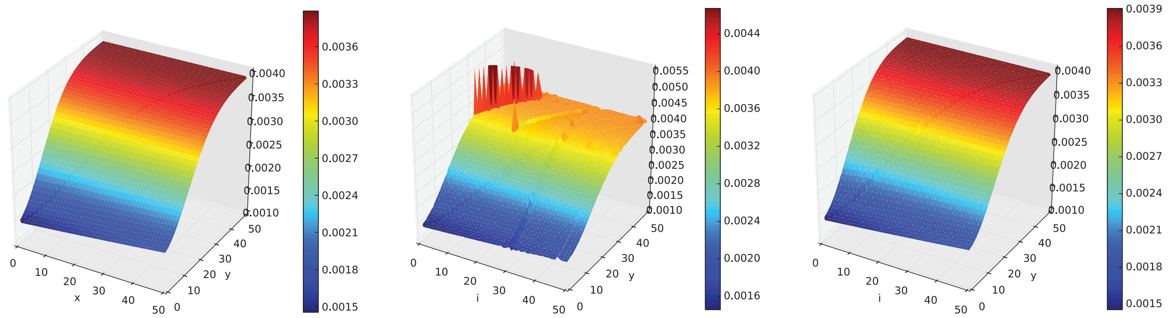
*where $\phi(x)=\frac{e^{-\frac{1}{2}x^2}}{\sqrt{2\pi}}$ is the density function of the standard normal distribution.*

Also the following result is proved in [13, Theorem 2].

**Lemma 3.2.** *We have*

$$P(S_N^{\mathrm{KSA}}[i]=f_i)=P(S_{i+1}^{\mathrm{KSA}}[i]=f_i)\cdot\Big(1-\frac{1}{N}\Big)^{N-1-i}+\big(1-P(S_{i+1}^{\mathrm{KSA}}[i]=f_i)\big)\cdot\sum_{t=i+1}^{N-1}\frac{1}{N^2}\Big(1-\frac{1}{N}\Big)^{N-1-t}.$$

Now we find $P(S_N^{\mathrm{KSA}}[i]=f_y)$ for $0\le i\le N-1$ and $1\le y\le N-1$ with $i\ne y$.




(a) (b) (c)

**Figure 2:** Probability $\mathrm{P}(S_N^{\mathrm{KSA}}[i] = f_y)$ for $0 \le i, y \le 50$ with $i \ne y$. Here (a) are the theoretical values and (b) the experimental results with a 16 byte key, and (c) are the experimental results with a 256 byte key.

**Lemma 3.3.** *For $i \ne y$ with $y \ge 1$, we have*

$$P(S_N^{\mathrm{KSA}}[i] = f_y) = \frac{1}{N}\Big(1 - \frac{1}{N}\Big)^{N-i-1} + \Big(1 - P(S_{y+1}^{\mathrm{KSA}}[y] = f_y) - \frac{1}{N}\Big)\Big(\sum_{t=i+1}^{N-1} \frac{1}{N^2} \cdot \Big(1 - \frac{1}{N}\Big)^{N-1-t}\Big).$$

*Proof.* We have two cases.

(i) Case I: Let $S_i^{\mathrm{KSA}}[j_{i+1}^{\mathrm{KSA}}] = f_y$. This happens with probability $\frac{1}{N}$. So after the swap, $S_{i+1}^{\mathrm{KSA}}[i]$ becomes $f_y$. Also $j_{i+2}^{\mathrm{KSA}}, \dots, j_N^{\mathrm{KSA}} \ne i$. So the probability of this path is $\frac{1}{N}(1 - \frac{1}{N})^{N-i-1}$. On the other hand, if $S_i^{\mathrm{KSA}}[j_{i+1}] = f_y$ and $i \in \{j_{i+2}^{\mathrm{KSA}}, \dots, j_N^{\mathrm{KSA}}\}$, then $S_N^{\mathrm{KSA}}[i]$ will be always different from $f_y$.

(ii) Case II: If $i < y$ and $S_{y+1}^{\mathrm{KSA}}[y] = f_y$, then $S_N^{\mathrm{KSA}}[i]$ cannot be $f_y$ as the $y$-th location of the array $S$ cannot move to the left when the running index is greater than $y$. On the other hand, if $i > y$ and $S_{y+1}^{\mathrm{KSA}}[y] = f_y$, then $S_N^{\mathrm{KSA}}[i]$ can be $f_y$ only through the first event. So we need $S_{y+1}^{\mathrm{KSA}} \ne f_y$. Let us consider the scenario where $S_t^{\mathrm{KSA}}[t] = f_y$ for some $t > i$. This holds with probability $\frac{1}{N}$. Suppose that $j_{t+1}^{\mathrm{KSA}} = i$ and $j_{t+2}^{\mathrm{KSA}}, \dots, j_N^{\mathrm{KSA}}$ are all different from $i$. Hence after the swap we get $S_{t+1}^{\mathrm{KSA}}[i] = f_y$, and this location is not disturbed in further rounds of KSA. This path holds with probability $\frac{1}{N^2} \cdot (1 - \frac{1}{N})^{N-1-t}$.

Thus if $i \ne y$, then

$$\begin{aligned}\mathrm{P}(S_N^{\mathrm{KSA}}[i] = f_y) &= \frac{1}{N}\Big(1 - \frac{1}{N}\Big)^{N-i-1} \cdot 1 + \frac{1}{N}\Big(1 - \Big(1 - \frac{1}{N}\Big)^{N-i-1}\Big) \cdot 0 \\ &\quad + \Big(1 - \mathrm{P}(S_{y+1}^{\mathrm{KSA}}[y] = f_y) - \frac{1}{N}\Big)\Big(\sum_{t=i+1}^{N-1} \frac{1}{N^2} \cdot \Big(1 - \frac{1}{N}\Big)^{N-1-t}\Big).\end{aligned}$$ □

In Figure 2, we present both theoretical and experimental results for $\mathrm{P}(S_N^{\mathrm{KSA}}[i] = f_y)$ for $0 \le i, y \le 50$ with $i \ne y$. From the figure it is clear there are some anomalies when the length of the keys is 16. This is because there are some $f_y$'s whose parities are the same when the key length is 16. We will discuss this issue for key-keystream relations in Theorem 3.9.

**Lemma 3.4.** *In PRGA,*

$$P(S_{i-1}[i] = f_y) = P(S_N^{\mathrm{KSA}}[i] = f_y)\Big(1 - \frac{1}{N}\Big)^{i-1} + \sum_{r=1}^{i-1} \frac{1}{N^r}\Big(1 - \frac{1}{N}\Big)^{i-r-1}\Big(\sum_{l=1}^{i-1} P(S_N^{\mathrm{KSA}}[l] = f_y)\binom{i-l-1}{r-1}\Big)$$

*for $1 \le i \le N-1$ and $1 \le y \le N-1$.*

*Proof.* This is similar to the proof of Lemma 2.2. □

Now consider the following event $C_1$ for an occurrence of $z_i = i - f_i$ for $i \ge 1$:

(i) $S_N^{\mathrm{KSA}}[i] = f_i$,

(ii) $j_1, \dots, j_{i-1} \ne i$,

(iii) $S_{i-1}[j_i] \ne i - f_i$.

Since $S_i[i] + S_i[j_i] \ne f_i + i - f_i = i$, we have $\mathrm{P}(z_i = i - f_i) = \frac{1}{N-1}$. The above path holds with the probability $a_i = \mathrm{P}(S_N^{\mathrm{KSA}}[i] = f_i)(1 - \frac{1}{N})^i$.

Now we prove the following theorems.

**Theorem 3.5.** *We have*

$$P(z_1 = 1 - f_y) = \begin{cases} P(S_0[1] = f_y)\frac{1}{N}\Big(1 - \frac{1}{N}\Big) + a_1\frac{1}{N-1}I_{1,y} + \Big(1 - \frac{1}{N} + \frac{1}{N^2} - a_1 I_{1,y}\Big)\frac{1}{N} & \text{for } y \neq 2, \\ P(S_0[1] = f_y)\cdot\frac{1}{N}\cdot\Big(1 - \frac{1}{N}\Big) + \Big(1 - \frac{1}{N} + \frac{1}{N^2} - \Big(\frac{2}{N} - \frac{1}{N^2}\Big)\cdot P(S_0[2] = f_2)\Big)\frac{1}{N} & \text{for } y = 2, \end{cases}$$

*where* $a_1 = P(S_N^{\mathrm{KSA}}[1] = f_1)(1 - \frac{1}{N})$.

*Proof.* Here the events are

$$A : (S_0[1] \neq f_y \cap S_0[j_1] = 1 - f_y \cap f_y \neq 0) \quad \text{and} \quad B : (S_0[1] = f_y \cap S_0[j_1] = 1 - f_y \cap f_y \neq 0).$$

One can see that $\mathrm{P}(z_1 = 1 - f_y \mid A) = 0$ and $\mathrm{P}(z_1 = 1 - f_y \mid B) = 1$.

Also if $S_0[1] + S_0[S_0[1]] = 2$ and $S_0[2] = f_2$, then $z_1$ will always be different from $1 - f_2$. Also, we have $\mathrm{P}(S_0[1] + S_0[S_0[1]] = 2) = \frac{2}{N} - \frac{1}{N^2}$ as one path comes from $S_0[1] = 1$. Hence the required result follows. □

Similarly, we find the bias of $z_2$ towards $2 - f_y$ in the next theorem.

**Theorem 3.6.** *We have*

$$P(z_2 = 2 - f_y) = \begin{cases} P(S_1[2] = f_y)\cdot\frac{1}{N} + a_2\frac{1}{N-1}I_{2,y} + \Big(1 - \frac{1}{N} - a_2 I_{2,y}\Big)\frac{1}{N} & \text{for } y \leq 2, \\ P(S_1[2] = f_y)\cdot\frac{1}{N} + \beta\cdot\frac{1}{N-1} + \Big(1 - \frac{1}{N} - \alpha - \beta\Big)\frac{1}{N} & \text{for } y > 2, \end{cases}$$

*where*

$$\begin{aligned} \alpha &= \Big(\frac{2}{N} - \frac{1}{N^2}\Big)\Big(\eta + \frac{1}{N}\cdot(1-\eta)\cdot\Big(1 - \frac{1}{N}\Big)\Big), \\ \beta &= \Big(1 - \frac{2}{N} + \frac{1}{N^2}\Big)\Big(\eta + \frac{1}{N}\cdot(1-\eta)\cdot\Big(1 - \frac{1}{N}\Big)\Big), \\ \eta &= \prod_{i=1}^{y}\Big(1 - \frac{i}{N}\Big)\cdot\Big(1 - \frac{y}{N}\Big)\cdot\Big(1 - \frac{1}{N}\Big)^N, \\ a_2 &= P(S_N^{\mathrm{KSA}}[2] = f_2)\Big(1 - \frac{1}{N}\Big)^2. \end{aligned}$$

*Proof.* For $y \leq 2$, the paths are the same as in Theorem 2.3. But for $y > 2$, we have two more paths:

(i) $C : ((S_1[y] = f_y) \cap (f_y \neq 2) \cap (z_2 = 0))$,

(ii) $D : ((S_1[y] = f_y) \cap (f_y \neq 2) \cap (z_2 \neq 0))$.

We have $\mathrm{P}(z_2 = 2 - f_y \mid C) = 0$. Also $\mathrm{P}(z_2 = 2 - f_y \mid D) = \frac{1}{N-1}$ as $z_2 \neq 0, f_y \neq 2$.

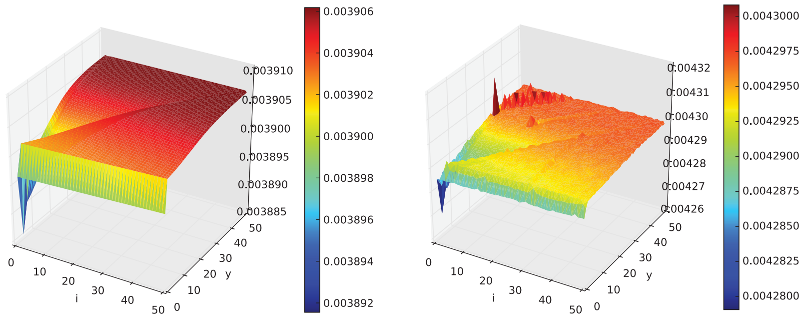
Now consider the events $j_t^{\mathrm{KSA}} \notin \{t, \ldots, y\}$ for $1 \leq t \leq y$, $f_y \notin \{0, 1, \ldots, y-1\}$, $j_t^{\mathrm{KSA}} \neq f_y$ for $1 \leq t \leq y$. Then $S_{y+1}^{\mathrm{KSA}}[y] = f_y$. Also if $j_{y+2}^{\mathrm{KSA}}, \ldots, j_N^{\mathrm{KSA}}, j_1 \neq f_y$, we have $S_1[y] = f_y$. Call this path $E$. Here

$$\mathrm{P}(E) = \prod_{i=1}^{y}\Big(1 - \frac{i}{N}\Big)\cdot\Big(1 - \frac{y}{N}\Big)\cdot\Big(1 - \frac{1}{N}\Big)^N.$$

One can see [11] that $\mathrm{P}(S_1[y] = f_y \mid E) = 1$. Also assume $\mathrm{P}(S_1[y] = f_y \mid E^c) = \frac{1}{N}$. From [8] we know that $\mathrm{P}(z_2 = 0) = \frac{2}{N} - \frac{1}{N^2}$. We have

$$\begin{aligned} \mathrm{P}(C) &= \mathrm{P}(S_1[y] = f_y \cap f_y \neq 2)\mathrm{P}(z_2 = 0) \\ &= \Big(\frac{2}{N} - \frac{1}{N^2}\Big)(\mathrm{P}(S_1[y] = f_y \cap f_y \neq 2 \cap E) + \mathrm{P}(S_1[y] = f_y \cap f_y \neq 2 \cap E^c)) \\ &= \Big(\frac{2}{N} - \frac{1}{N^2}\Big)(\mathrm{P}(E) + \mathrm{P}(S_1[y] = f_y \mid E^c)\cdot\mathrm{P}(E^c)\cdot\mathrm{P}(f_y \neq 2)) \\ &= \Big(\frac{2}{N} - \frac{1}{N^2}\Big)\Big(\mathrm{P}(E) + \frac{1}{N}\cdot(1 - \mathrm{P}(E))\cdot\Big(1 - \frac{1}{N}\Big)\Big). \end{aligned}$$

Similarly, $\mathrm{P}(D) = (1 - \frac{2}{N} + \frac{1}{N^2})(\mathrm{P}(E) + \frac{1}{N}\cdot(1 - \mathrm{P}(E))\cdot(1 - \frac{1}{N}))$. □




**(a)** **(b)**

**Figure 3:** Probability $\mathrm{P}(z_i = i - f_y)$ for $1 \le i \le 50$, $0 \le y \le 50$ with $i \ne y$. Here (a) are the theoretical values and (b) the experimental results with a 16 byte key.

Now, for all $i$ greater than 2, the following theorem gives the probability $\mathrm{P}(z_i = i - f_y)$.

**Theorem 3.7.** *We have*

$$P(z_i = i - f_y) = P(S_{i-1}[i] = f_y) \cdot \frac{1}{N} + a_i \frac{1}{N-1} I_{i,y} + \Big(1 - \frac{1}{N} - a_i I_{i,y}\Big)\frac{1}{N}$$

*for* $3 \le i \le N-1$ *and* $1 \le y \le N-1$, *where* $a_i = P(S_N^{\mathrm{KSA}}[i] = f_i)(1 - \frac{1}{N})^{i-1}(1 - \frac{1}{N})$.

*Proof.* Similarly to the proof of Theorem 2.3, we consider the events $A : ((S_{i-1}[i] \ne K[0]) \cap (S_{i-1}[j_i] = i - K[0]))$ and $B : ((S_{i-1}[i] = K[0]) \cap (S_{i-1}[j_i] = i - K[0]))$. In these cases, $\mathrm{P}(z_i = i - f_y)$ are 0 and 1, respectively.

Next we consider $C = (A \cup B)^c$. Then $\mathrm{P}(C) = (1 - \frac{1}{N})$. But in case of $i = y$, the event $C$ can be divided into two mutually disjoint events $C_1$ and $C_1^c$ (as mentioned just before Theorem 3.5). Evaluating the probabilities of all these events, we get the result. □

In Figure 3, we present both theoretical and experimental results for $\mathrm{P}(z_i = i - f_y)$ for $1 \le i \le 50$, $0 \le y \le 50$ with $i \ne y$. From the figure it is clear that there are some anomalies. Among them the probability of $z_2 = 2 - f_{31}$ is the most significant. We observe $\mathrm{P}(z_2 = 2 - f_{31}) = \frac{1}{N} + \frac{0.82}{N^2}$. However, if the key length is 256, we get $\mathrm{P}(z_2 = 2 - f_{31}) = \frac{1}{N} - \frac{0.11}{N^2}$, which matches exactly with the theoretical value. When the key length is 16, we have the following result.

**Theorem 3.8.** *When the length of the key is* 16, *then*

$$P(z_2 = 2 - f_{31}) = \frac{2}{N}\Big(\frac{2}{N} - \frac{1}{N^2}\Big) + \Big(1 - \frac{2}{N} + \frac{1}{N^2}\Big)\Big(\frac{\frac{N}{2} - 1}{N - 1}\Big)\frac{2}{N}.$$

*Proof.* We divide it into two disjoint events, $A : (z_2 = 0)$ and $B : (z_2 \ne 0)$. We know that $\mathrm{P}(A) = \frac{2}{N} - \frac{1}{N^2}$ and $\mathrm{P}(B) = (1 - \frac{2}{N} + \frac{1}{N^2})$. Also one can see that, if the length of the key is 16, then

$$f_{31} = 496 + 2\sum_{i=0}^{31} K[i] = 496 + 2\sum_{i=0}^{15} K[i]$$

is always even. Hence $\mathrm{P}(f_{31} = 2) = \frac{2}{N}$. So,

$$\begin{aligned}
\mathrm{P}(z_2 = 2 - f_{31}) &= \mathrm{P}(z_2 = 2 - f_{31} \cap z_2 = 0) + \mathrm{P}(z_2 = 2 - f_{31} \cap z_2 \ne 0) \\
&= \mathrm{P}(z_2 = 2 - f_{31} \mid z_2 = 0)\mathrm{P}(z_2 = 0) + \mathrm{P}(z_2 = 2 - f_{31} \mid z_2 \ne 0)\mathrm{P}(z_2 \ne 0) \\
&= \mathrm{P}(f_{31} = 2 \mid z_2 = 0) \cdot \mathrm{P}(z_2 = 0) + \mathrm{P}(z_2 = 2 - f_{31} \mid z_2 \ne 0)\mathrm{P}(z_2 \ne 0) \\
&= \frac{2}{N}\Big(\frac{2}{N} - \frac{1}{N^2}\Big) + \Big(1 - \frac{2}{N} + \frac{1}{N^2}\Big)\Big(\frac{\frac{N}{2} - 1}{N - 1}\Big)\frac{2}{N}.
\end{aligned}$$ □

Theorem 3.8 gives $\mathrm{P}(z_2 = 2 - f_{31}) = \frac{1}{N} + \frac{1}{N^2}$, which matches closely with the experimental value. We also have another set of biases when the key length is 16.

**Theorem 3.9.** *We have*

$$P(z_{3+r} = 3 + r - f_{35+r}) = \Big(\Big(\frac{2}{N} - \frac{1}{N^2}\Big)\frac{2}{N} + \frac{(1-\frac{2}{N})}{N-1}\Big(1 - \frac{2}{N}\Big)\Big)P(S_{3+r-1}[3+r] = f_{3+r}) + \Big(\frac{(1-\frac{2}{N})}{N-1} \cdot \frac{2}{N} + \frac{1}{N}\Big(1-\frac{2}{N}\Big)\Big) \cdot (1 - P(S_{3+r-1}[3+r] = f_{3+r}))$$

*for $r \geq 0$, when the length of the key is* 16.

*Proof.* We have

$$\begin{aligned}
f_{35+r} - f_{3+r} &= \Big(\sum_{i=0}^{35+r}(i + K[i])\Big) - \Big(\sum_{i=0}^{3+r}(i + K[i])\Big)\\
&= \Big(\sum_{i=0}^{35+r} i - \sum_{i=0}^{3+r} i\Big) + \Big(\sum_{i=0}^{35+r} K[i] - \sum_{i=0}^{3+r} K[i]\Big)\\
&= 624 + 32r + \Big(\sum_{i=4+r}^{35+r} K[i]\Big)\\
&= 624 + 32r + \Big(\sum_{i=4+r}^{19+r} K[i] + \sum_{i=20+r}^{35+r} K[i]\Big)\\
&= 624 + 32r + \Big(\sum_{i=4+r}^{19+r} K[i] + \sum_{j=4+r}^{19+r} K[j+16]\Big) \quad (j = (i-16))\\
&= 624 + 32r + \Big(\sum_{i=4+r}^{19+r} K[i] + \sum_{j=4+r}^{19+r} K[j]\Big) \qquad \text{(since the key length is 16 and } K[j+16] = K[j])\\
&= 624 + 32r + 2\Big(\sum_{i=4+r}^{19+r} K[i]\Big).
\end{aligned}$$

One can see that $f_{35+r} - f_{3+r}$ will always be even, which means that $f_{3+r}$ and $f_{35+r}$ will be of the same parity for $r \geq 0$, i.e., either both are even or both are odd (exclusive) when the length of the key is 16. So for one value of $f_{3+r}$, there are $\frac{N}{2}$ possible values for $f_{35+r}$. So $\mathrm{P}(f_{35+r} = f_{3+r}) = \frac{2}{N}$. Also $\mathrm{P}(z_r = r - S_{r-1}[r]) = \frac{2}{N} - \frac{1}{N^2}$ by Jenkins' Correlation [3].

Now,

$$\begin{aligned}
\mathrm{P}(z_{3+r} = 3 + r - f_{35+r}) &= \mathrm{P}(z_{3+r} = 3 + r - f_{35+r} \mid S_{3+r-1}[3+r] = f_{3+r-1})\mathrm{P}(S_{3+r-1}[3+r] = f_{3+r})\\
&\quad + \mathrm{P}(z_{3+r} = 3 + r - f_{35+r} \mid S_{3+r-1}[3+r] \neq f_{3+r})\mathrm{P}(S_{3+r-1}[3+r] \neq f_{3+r})\\
&= (\mathrm{P}(z_{3+r} = 3 + r - f_{35+r} \mid S_{3+r-1}[3+r] = f_{3+r} \cap f_{3+r} = f_{35+r})\\
&\quad \mathrm{P}(f_{3+r} = f_{35+r}) + \mathrm{P}(z_{3+r} = 3 + r - f_{35+r} \mid S_{3+r-1}[3+r] = f_{3+r} \cap f_{3+r} \neq f_{35+r})\\
&\quad \mathrm{P}(f_{3+r} \neq f_{35+r}))\mathrm{P}(S_{3+r-1}[3+r] = f_{3+r})\\
&\quad + (\mathrm{P}(z_{3+r} = 3 + r - f_{35+r} \mid S_{3+r-1}[3+r] \neq f_{3+r} \cap f_{3+r} = f_{35+r})\mathrm{P}(f_{3+r} = f_{35+r})\\
&\quad + \mathrm{P}(z_{3+r} = 3 + r - f_{35+r} \mid S_{3+r-1}[3+r] \neq f_{3+r} \cap f_{3+r} \neq f_{35+r})\mathrm{P}(f_{3+r} \neq f_{35+r}))\\
&\quad \mathrm{P}(S_{3+r-1}[3+r] \neq f_{3+r})\\
&= \Big(\Big(\frac{2}{N} - \frac{1}{N^2}\Big)\frac{2}{N} + \frac{(1-\frac{2}{N})}{N-1}\Big(1-\frac{2}{N}\Big)\Big)\mathrm{P}(S_{3+r-1}[3+r] = f_{3+r})\\
&\quad + \Big(\frac{(1-\frac{2}{N})}{N-1}\frac{2}{N} + \frac{1}{N}\Big(1-\frac{2}{N}\Big)\Big)(1 - \mathrm{P}(S_{3+r-1}[3+r] = f_{3+r})).
\end{aligned}$$

□

Using Lemma 3.4, we can find $\mathrm{P}(S_{3+r-1}[3+r] = f_{3+r})$. From Theorem 3.9 we calculate $\mathrm{P}(z_{3+r} = 3 + r - f_{35+r})$, which is $(\frac{1}{N} + \frac{0.31}{N^2})$ when $r = 0$, and decreases as $r$ increases.

**Remark 3.10.** In Theorem 3.8 and Theorem 3.9, we justified two biases observed in the experiment for key length 16. However, using the same argument, we can generalize the results for any key length. If the key

| $i$ | | $P(z_i = i - f_i)$ | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 1–8 | [6] | 0.005367 | 0.005332 | 0.005305 | 0.005273 | 0.005237 | 0.005196 | 0.005153 | 0.005106 |
| | Exp. | 0.005264 | 0.005298 | 0.005280 | 0.005241 | 0.005211 | 0.005169 | 0.005127 | 0.005077 |
| | Thm. 3.5 | 0.005320 | 0.005298 | 0.005270 | 0.005238 | 0.005202 | 0.005161 | 0.005117 | 0.005070 |
| 9–16 | [6] | 0.005056 | 0.005005 | 0.004951 | 0.004897 | 0.004842 | 0.004787 | 0.004732 | 0.004677 |
| | Exp. | 0.005028 | 0.004974 | 0.004921 | 0.004864 | 0.004808 | 0.004751 | 0.004697 | 0.004639 |
| | Thm. 3.5 | 0.005020 | 0.004968 | 0.004914 | 0.004859 | 0.004803 | 0.004747 | 0.004691 | 0.004636 |
| 17–24 | [6] | 0.004624 | 0.004572 | 0.004521 | 0.004473 | 0.004426 | 0.004382 | 0.00434 | 0.004301 |
| | Exp. | 0.004586 | 0.004532 | 0.004481 | 0.004431 | 0.004385 | 0.004338 | 0.004298 | 0.004256 |
| | Thm. 3.5 | 0.004582 | 0.004529 | 0.004478 | 0.004429 | 0.004382 | 0.004338 | 0.004291 | 0.004252 |
| 25–32 | [6] | 0.004264 | 0.004230 | 0.004198 | 0.004169 | 0.004142 | 0.004117 | 0.004095 | 0.004075 |
| | Exp. | 0.004220 | 0.004184 | 0.004154 | 0.004123 | 0.004097 | 0.004073 | 0.004050 | 0.004031 |
| | Thm. 3.5 | 0.004215 | 0.004181 | 0.004149 | 0.004121 | 0.004094 | 0.004070 | 0.004049 | 0.004029 |
| 33–40 | [6] | 0.004057 | 0.004041 | 0.004026 | 0.004014 | 0.004002 | 0.003993 | 0.003984 | 0.003976 |
| | Exp. | 0.004013 | 0.003998 | 0.003985 | 0.003972 | 0.003962 | 0.003953 | 0.003945 | 0.003938 |
| | Thm. 3.5 | 0.004012 | 0.003997 | 0.003983 | 0.003971 | 0.003961 | 0.003952 | 0.003944 | 0.003937 |
| 41–48 | [6] | 0.003970 | 0.003964 | 0.003959 | 0.003955 | 0.003952 | 0.003949 | 0.003946 | 0.003944 |
| | Exp. | 0.003932 | 0.003927 | 0.003922 | 0.003919 | 0.003916 | 0.003914 | 0.003911 | 0.003910 |
| | Thm. 3.5 | 0.003931 | 0.003926 | 0.003922 | 0.003919 | 0.003916 | 0.003913 | 0.003911 | 0.003909 |
| 49–56 | [6] | 0.003942 | 0.003940 | 0.003939 | 0.003938 | 0.003937 | 0.003937 | 0.003936 | 0.003935 |
| | Exp. | 0.003908 | 0.003907 | 0.003906 | 0.003906 | 0.003905 | 0.003905 | 0.003904 | 0.003904 |
| | Thm. 3.5 | 0.003908 | 0.003907 | 0.003906 | 0.003905 | 0.003905 | 0.003904 | 0.003904 | 0.003904 |
| 57–64 | [6] | 0.003935 | 0.003935 | 0.003934 | 0.003934 | 0.003934 | 0.003934 | 0.003934 | 0.003934 |
| | Exp. | 0.003904 | 0.003904 | 0.003904 | 0.003904 | 0.003904 | 0.003905 | 0.003905 | 0.003905 |
| | Thm. 3.5 | 0.003904 | 0.003904 | 0.003904 | 0.003904 | 0.003904 | 0.003905 | 0.003905 | 0.003905 |

**Table 1:** Comparison of our work with the work [6] and experimental values.

length is $\ell$, we will observe a similar bias in $P(z_2 = 2 - f_{2\ell-1})$ and $P(z_{3+r} = 3 + r - f_{3+2\ell+r})$. These biases can be explained similarly, i.e., $f_{2\ell-1}$ and $(f_{3+2\ell+r} - f_{3+r})$ are always even. So this increases the probabilities $P(f_{2\ell-1} = 2)$ and $P(f_{3+2\ell+r} = f_{3+r})$ to $\frac{2}{N}$.

## 3.1 Probability $z_i = i - f_i$

Let us first start with $y = i$. In this case, results were discovered in [5] and proved rigorously in [6]. It was shown in [6, Theorem 3] that

$$P(z_1 = 1 - f_1) = \frac{1}{N}\Big(1 + \Big(\frac{N-1}{N}\Big)^{N+2} + \frac{1}{N}\Big),$$
$$P(z_i = i - f_i) = \frac{1}{N}\Big(1 + \Big[\Big(\frac{N-i}{N}\Big)\Big(\frac{N-1}{N}\Big)^{[\frac{i(i+1)}{2}+N]} + \frac{1}{N}\Big] \cdot \Big[\Big(\frac{N-1}{N}\Big)^{i-1} - \frac{1}{N}\Big] + \frac{1}{N}\Big) \quad \text{for } i \in [2, N-1].$$

Using Table 1, we present our comparative study of the correlation probabilities. We present the theoretical values of $P(z_i = i - f_i)$ for $1 \le i \le 64$ according to Theorem 3.5 and also according to the above formulas from [6]. We have calculated the values $p_i$, which are required to find the coefficients $a_i$ in $P(z_i = i - f_i)$, using numerical methods available in [20]. The experimental values are averaged over 100 billion key schedulings, where the keys are of length 16 and are randomly generated.

From Table 1 it is clear that our estimation gives a much better approximation than [6]. One can note that from Table 1, $P(z_i = i - f_i) < \frac{1}{N}$ for $i \in [52, 64]$. The formulas of [6] cannot capture this negative bias. For example, when $y = 64$, the formulas of [6] give $P(z_{64} = 64 - f_{64}) = \frac{1}{N} + \frac{1.82}{N^2}$, but actually $P(z_{64} = 64 - f_{64}) < \frac{1}{N}$.

**Remark 3.11.** In [14], Sengupta et al. studied linear relations between the keystream bytes and key. They used these relations to recover plaintexts of WPA as the first three bytes of the key are public. To recover

| $P(z_1 = 1 - f_2)$ | | $P(z_1 = 1 - f_3)$ | | $P(z_1 = 1 - f_4)$ | | $P(z_1 = 1 - f_5)$ | | $P(z_1 = 1 - f_6)$ | |
|---|---|---|---|---|---|---|---|---|---|
| Thm. | Exp. | Thm. | Exp. | Thm. | Exp. | Thm. | Exp. | Thm. | Exp. |
| 0.003886 | 0.003882 | 0.003897 | 0.003897 | 0.003897 | 0.003998 | 0.003898 | 0.003998 | 0.003898 | 0.003998 |
| $P(z_2 = 2 - f_3)$ | | $P(z_2 = 2 - f_4)$ | | $P(z_2 = 2 - f_5)$ | | $P(z_2 = 2 - f_6)$ | | $P(z_2 = 2 - f_7)$ | |
| Thm. | Exp. | Thm. | Exp. | Thm. | Exp. | Thm. | Exp. | Thm. | Exp. |
| 0.003892 | 0.003891 | 0.003892 | 0.003892 | 0.003892 | 0.003892 | 0.003893 | 0.003892 | 0.003893 | 0.003893 |
| $P(z_3 = 3 - f_4)$ | | $P(z_3 = 3 - f_5)$ | | $P(z_3 = 3 - f_6)$ | | $P(z_3 = 3 - f_7)$ | | $P(z_3 = 3 - f_8)$ | |
| Thm. | Exp. | Thm. | Exp. | Thm. | Exp. | Thm. | Exp. | Thm. | Exp. |
| 0.003897 | 0.003897 | 0.003898 | 0.003897 | 0.003898 | 0.003898 | 0.003898 | 0.003898 | 0.003898 | 0.009899 |
| $P(z_4 = 4 - f_5)$ | | $P(z_4 = 4 - f_6)$ | | $P(z_4 = 4 - f_7)$ | | $P(z_4 = 4 - f_8)$ | | $P(z_4 = 4 - f_9)$ | |
| Thm. | Exp. | Thm. | Exp. | Thm. | Exp. | Thm. | Exp. | Thm. | Exp. |
| 0.003898 | 0.003897 | 0.003898 | 0.003898 | 0.003898 | 0.003898 | 0.003898 | 0.003898 | 0.003899 | 0.003898 |

**Table 2:** Theoretical and experimental values of a few $z_i = i - f_y$ for $y > i$.

the first byte of plaintext, they used the relation $z_1 = 1 - f_1$. From Table 1 one can note that our theoretical estimation of $P(z_1 = 1 - f_1)$ is better than the existing work [6].

Theorem 3.7 also gives a negative bias of $P(z_i = i - f_y)$ for $y > i$. In Table 2, we present a few theoretical and experimental values. The experimental values are averaged over 100 billion different keys, where the keys are of length 16 and are randomly generated.

## 4 Biases of $z_i$ towards $f_{i-1}$

In this section, we study the probability $P(z_i = f_{i-1})$. In FSE 2008, Maitra and Paul [6] observed this type of biases. In [6, Theorem 6], it is claimed that

$$P(z_i = f_{i-1}) = \Big(\frac{N-1}{N}\Big)\Big(\frac{N-i}{N}\Big)\Big(\Big(\frac{N-i+1}{N}\Big)\Big(\frac{N-1}{N}\Big)^{\frac{i(i-1)}{2}+i} + \frac{1}{N}\Big)\Big(\frac{N-2}{N}\Big)^{N-i}\Big(\frac{N-3}{N}\Big)^{i-2}\gamma_i + \frac{1}{N},$$

where

$$\gamma_i = \frac{1}{N}\Big(\frac{N-1}{N}\Big)^{N-1-i} + \frac{1}{N}\Big(\frac{N-1}{N}\Big) - \frac{1}{N}\Big(\frac{N-1}{N}\Big)^{N-i}.$$

From [7], we know that $\gamma_i$ is the probability of $S_N^{\mathrm{KSA}}[i]$ equaling zero after KSA.

Let us start with the following lemma.

**Lemma 4.1.** *In PRGA,*

$$P(S_{i-1}[i] = 0) = \begin{cases} \gamma_i\Big(1 - \frac{1}{N}\Big)^{i-1} + \sum\limits_{s=1}^{i-3}\frac{1}{N^s}\Big(1 - \frac{1}{N}\Big)^{i-1-s}\sum\limits_{l=2}^{i-1}\gamma_l\binom{i-l-2}{s-1} & \text{for } i > 3, \\ \gamma_i\Big(1 - \frac{1}{N}\Big)^{i-1} & \text{for } 1 < i \leq 3. \end{cases}$$

*Proof.* For $i > 3$, we have the following paths:

(i) Let $S_N^{\mathrm{KSA}}[i] = 0$. This holds with probability $\gamma_i$. Also all $j_1, \ldots, j_{i-1}$ are different from $i$.

(ii) If $S_N^{\mathrm{KSA}}[0] = 0$ or $S_N^{\mathrm{KSA}}[1] = 0$, then $S_{i-1}[i]$ will be always different from zero. Again if $S_N^{\mathrm{KSA}}[l] = 0$ with $1 < l < i - 1$, zero can move through $s$ jumps with $1 \leq s \leq i - 3$ as zero cannot move forward through $i - 2$ jumps, one jump in each step. This happens with probability

$$\frac{1}{N^s}\Big(1 - \frac{1}{N}\Big)^{i-1-s}\sum_{l=2}^{i-1}\gamma_l\binom{i-l-2}{s-1}.$$

So the total probability for this path is

$$\sum_{s=1}^{i-3}\frac{1}{N^s}\Big(1 - \frac{1}{N}\Big)^{i-1-s}\sum_{l=2}^{i-1}\gamma_l\binom{i-l-2}{s-1}.$$

For $1 < i \leq 3$, we have only the first path. □

| $i$ | | $P(z_i = f_{i-1})$ | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 3–10 | [6] | 0.004413 | 0.004400 | 0.004384 | 0.004368 | 0.004350 | 0.004331 | 0.004312 | 0.004292 |
| | Exp. | 0.004400 | 0.004386 | 0.004376 | 0.004356 | 0.004339 | 0.004321 | 0.004301 | 0.004281 |
| | Thm. 4.2 | 0.004400 | 0.004387 | 0.004372 | 0.004356 | 0.004339 | 0.004320 | 0.004301 | 0.004281 |
| 11–18 | [6] | 0.004271 | 0.00425 | 0.004229 | 0.004209 | 0.004188 | 0.004168 | 0.004148 | 0.004129 |
| | Exp. | 0.004261 | 0.004241 | 0.004220 | 0.004200 | 0.004179 | 0.004162 | 0.004139 | 0.004120 |
| | Thm. 4.2 | 0.004261 | 0.004240 | 0.004220 | 0.004199 | 0.004179 | 0.004159 | 0.004139 | 0.004120 |
| 19–26 | [6] | 0.004111 | 0.004093 | 0.004076 | 0.004061 | 0.004046 | 0.004032 | 0.004019 | 0.004007 |
| | Exp. | 0.004102 | 0.004085 | 0.004068 | 0.004052 | 0.004038 | 0.004024 | 0.004011 | 0.003999 |
| | Thm. 4.2 | 0.004102 | 0.004085 | 0.004068 | 0.004053 | 0.004038 | 0.004024 | 0.004011 | 0.004000 |
| 27–34 | [6] | 0.003996 | 0.003986 | 0.003976 | 0.003968 | 0.003960 | 0.003954 | 0.003948 | 0.003942 |
| | Exp. | 0.003988 | 0.003978 | 0.003969 | 0.003961 | 0.003954 | 0.003950 | 0.003941 | 0.003937 |
| | Thm. 4.2 | 0.003989 | 0.003979 | 0.003970 | 0.003962 | 0.003954 | 0.003948 | 0.003942 | 0.003937 |
| 35–42 | [6] | 0.003937 | 0.003933 | 0.003929 | 0.003926 | 0.003923 | 0.003921 | 0.003919 | 0.003917 |
| | Exp. | 0.003932 | 0.003928 | 0.003924 | 0.003922 | 0.003919 | 0.003917 | 0.003915 | 0.003913 |
| | Thm. 4.2 | 0.003932 | 0.003929 | 0.003925 | 0.003922 | 0.00392 | 0.003917 | 0.003915 | 0.003914 |
| 43–50 | [6] | 0.003915 | 0.003914 | 0.003913 | 0.003912 | 0.003911 | 0.003911 | 0.003910 | 0.003910 |
| | Exp. | 0.003912 | 0.003911 | 0.003910 | 0.003909 | 0.003908 | 0.003907 | 0.003907 | 0.003907 |
| | Thm. 4.2 | 0.003912 | 0.003911 | 0.003910 | 0.003910 | 0.003909 | 0.003908 | 0.003908 | 0.003908 |

**Table 3:** Comparison of our work with the work [6] and experimental values for $z_i = f_{i-1}$.

Now we will prove the following bias of $z_i$ towards $f_{i-1}$.

**Theorem 4.2.** *In PRGA,*

$$P(z_i = f_{i-1}) = \tau\rho\delta\eta\psi + (1 - \tau\rho\delta\eta\psi - \tau\rho\delta(1-\eta)\psi - \tau\rho(1-\delta)\eta\psi - \tau(1-\rho)\delta\eta\psi) \cdot \frac{1}{N},$$

*where* $\tau = P(S_{i-1}[i] = 0)$, $\rho = P(S_N^{\mathrm{KSA}}[S_N^{\mathrm{KSA}}[i-1]] = f_{i-1})$, $\delta = (1 - \frac{1}{N})^{i-2}$, $\eta = (1 - \frac{i}{N})$, $\psi = (1 - \frac{1}{N})^{i-1}$ *and* $i > 2$.

*Proof.* Consider the following five events:
(i) The first event $A_1$ is $S_{i-1}[i] = 0$.
(ii) The second event $A_2$ is $S_N^{\mathrm{KSA}}[S_N^{\mathrm{KSA}}[i-1]] = f_{i-1}$.
(iii) $A_3 = \{(j_1 \neq i-1) \cap \cdots \cap (j_{i-2} \neq i-1)\}$.
(iv) $A_4 = \{(1 \neq S_N[i-1]) \cap \cdots \cap (i \neq S_N[i-1])\}$.
(v) $A_5 = \{(j_1 \neq S_N[i-1]) \cap \cdots \cap (j_{i-1} \neq S_N[i-1])\}$.
Now one can see that

$$\begin{aligned} &\mathrm{P}(z_i = f_{i-1} \mid A_1 \cap A_2 \cap A_3 \cap A_4 \cap A_5) = 1, \quad \mathrm{P}(z_i = f_{i-1} \mid A_1 \cap A_2 \cap A_3 \cap A_4^c \cap A_5) = 0, \\ &\mathrm{P}(z_i = f_{i-1} \mid A_1 \cap A_2 \cap A_3^c \cap A_4 \cap A_5) = 0, \quad \mathrm{P}(z_i = f_{i-1} \mid A_1 \cap A_2^c \cap A_3 \cap A_4 \cap A_5) = 0. \end{aligned}$$

Also,

$$\begin{aligned} \mathrm{P}(A_1) &= \mathrm{P}(S_{i-1}[i] = 0), \\ \mathrm{P}(A_2) &= \mathrm{P}(S_N^{\mathrm{KSA}}[S_N^{\mathrm{KSA}}[i-1]] = f_{i-1}), \\ \mathrm{P}(A_3) &= \Big(1 - \frac{1}{N}\Big)^{i-2}, \\ \mathrm{P}(A_4) &= \Big(1 - \frac{i}{N}\Big), \\ \mathrm{P}(A_5) &= \Big(1 - \frac{1}{N}\Big)^{i-1}. \end{aligned}$$

Assuming $z_i = f_{i-1}$ occurs with $\frac{1}{N}$ in the other cases, we have the required result. □

Now one can find $\mathrm{P}(S_N^{\mathrm{KSA}}[S_N^{\mathrm{KSA}}[i-1]] = f_{i-1})$ by using the following theorem of [13].

**Theorem 4.3.** *After the completion of KSA, the probability* $P(S_N^{\mathrm{KSA}}[S_N^{\mathrm{KSA}}[i]] = f_i)$ *is*

$$\Big(\frac{1}{N}\Big(1-\frac{1}{N}\Big)^{N-1-i} + \beta\Big)P(S_{i+1}^{\mathrm{KSA}}[i] = f_i) + \alpha + \Big(\frac{1-\alpha-\beta}{N}\Big)P(S_{i+1}[i] \neq f_i),$$

*where*

$$\alpha = \Big(1-\frac{2}{N}\Big)^{N-i-1}\prod_{r=1}^{i}\Big(1-\frac{r}{N}\Big)\Big(1-\frac{i}{N}\Big)\Big(1-\frac{1}{N}\Big)^{i-1}\frac{1}{N}\sum_{s=1}^{i}\Big(1-\frac{1}{N}\Big)^{i-s},$$

$$\beta = \Big(\frac{N-i-1}{N}\Big)\Big(1-\frac{1}{N}\Big)^{i+1}\Big(1-\frac{2}{N}\Big)^{N-i-2}.$$

Using Table 3, we present our comparative study of the correlation probabilities. We present the theoretical values of $\mathrm{P}(z_i = f_{i-1})$ for $3 \leq i \leq 64$ according to Theorem 4.2 and also according to the formulas of [6]. The experimental values are averaged over 100 billion key schedulings, where the keys are of length 16 and are randomly generated. From Table 3 it is clear that our estimation gives a much better approximation than [6].

## 5 Conclusion

In this paper, we have given a justification of the negative bias between $z_i$ with $i - k[0]$ which was observed experimentally by Paterson et al. [9, 10]. Next we have considered a generalization of the Roos bias. We have also presented the complete correlation between $z_i$ and $i - f_y$. Our formulas for the probabilities of $z_i = i - f_i$ and $z_i = f_{i-1}$ give a better approximation than the existing works.

## References


[1] N. AlFardan, D. Bernstein, K. Paterson, B. Poettering and J. Schuldt, On the security of RC4 in TLS, in: *Proceedings of the 22nd USENIX conference on Security – SEC'13*, Usenix Association, Berkeley (2013), 305–320.

[2] S. Fluhrer, I. Mantin and A. Shamir, Weaknesses in the key scheduling algorithm of RC4, in: *Selected Areas in Cryptography – SAC 2001*, Lecture Notes in Comput. Sci. 2259, Springer, Berlin (2001), 1–24.

[3] R. J. Jenkins, ISAAC and RC4, preprint (1996), http://burtleburtle.net/bob/rand/isaac.html.

[4] S. Jha, S. Banik, T. Isobe and T. Ohigashi, Some proofs of joint distributions of keystream biases in RC4, in: *Progress in Cryptology – INDOCRYPT 2016*, Lecture Notes in Comput. Sci. 10095, Springer, Cham (2016), 305–321.

[5] A. Klein, Attacks on the RC4 stream cipher, *Des. Codes Cryptogr.* **48** (2008), no. 3, 269–286.

[6] S. Maitra and G. Paul, New form of permutation bias and secret key leakage in keystream bytes of RC4, in: *Fast Software Encryption – FSE 2008*, Lecture Notes in Comput. Sci. 5086, Springer, Berlin (2008), 253–269.

[7] I. Mantin, *Analysis of the stream cipher RC4*, Master's Thesis, The Weizmann Institute of Science, Israel, 2001.

[8] I. Mantin and A. Shamir, A practical attack on broadcast RC4, in: *Fast Software Encryption – FSE 2001*, Lecture Notes in Comput. Sci. 2355, Springer, Berlin (2002), 152–164.

[9] K. G. Paterson, B. Poettering and J. C. N. Schuldt, Big bias hunting in Amazonia: Large-scale computation and exploitation of RC4 biases (invited paper), in: *Advances in Cryptology – ASIACRYPT 2014. Part I*, Lecture Notes in Comput. Sci. 8873, Springer, Heidelberg (2014), 398–419.

[10] K. G. Paterson, J. Schuldt and B. Poettering, Plaintext recovery attacks against WPA/TKIP, in: *Fast Software Encryption – FSE 2014*, Lecture Notes in Comput. Sci. 8540, Springer, Berlin (2014), 325–349.

[11] G. Paul and S. Maitra, Permutation after RC4 key scheduling reveals the secret key, in: *Selected Areas in Cryptography – SAC 2007*, Lecture Notes in Comput. Sci. 4876, Springer, Berlin (2007), 360–377.

[12] 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`, preprint (1995).

[13] S. Sarkar and A. Venkateswarlu, Revisiting (nested) Roos bias in RC4 key scheduling algorithm, *Des. Codes Cryptogr.* **82** (2017), no. 1–2, 131–148.

[14] S. Sengupta, S. Maitra, W. Meier, G. Paul and S. Sarkar, Dependence in IV-related bytes of RC4 key enhances vulnerabilities in WPA, in: *Fast Software Encryption – FSE 2014*, Lecture Notes in Comput. Sci. 8540, Springer, Berlin (2014), 350–369.

[15] P. Sepehrdad, S. Vaudenay and M. Vuagnoux, Discovery and exploitation of new biases in RC4, in: *Selected Areas in Cryptography – SAC 2010*, Lecture Notes in Comput. Sci. 6544, Springer, Berlin (2010), 74–91.

[16] P. Sepehrdad, S. Vaudenay and M. Vuagnoux, Statistical attack on RC4 - distinguishing WPA, in: *Advances in Cryptology – EUROCRYPT 2011*, Lecture Notes in Comput. Sci. 6632, Springer, Berlin (2010), 343–363.

[17] M. Vanhoef and F. Piessens, All your biases belong to us: Breaking RC4, in: *Proceedings of the 24th USENIX Conference on Security Symposium – SEC' 15*, Usenix Association, Berkeley (2016), 97–112.

[18] IEEE 802.11. Wireless LAN medium access control (MAC) and physical layer (PHY) specification, (1997).

[19] IEEE 802.11i. Wireless LAN medium access control (MAC) and physical layer (PHY) specification: Amendment 6: Medium access control (MAC) security enhancements (2004).

[20] Sage: Open Source Mathematics Software, http://www.sagemath.org/.