HAL
archives-ouvertes.fr

Revisiting Roos Bias in RC4 Key Scheduling Algorithm

Santanu Sarkar, Ayineedi Venkateswarlu

▶ **To cite this version:**

Santanu Sarkar, Ayineedi Venkateswarlu. Revisiting Roos Bias in RC4 Key Scheduling Algorithm. Pascale Charpin, Nicolas Sendrier, Jean-Pierre Tillich. WCC2015 - 9th International Workshop on Coding and Cryptography 2015, Apr 2015, Paris, France. 2016, Proceedings of the 9th International Workshop on Coding and Cryptography 2015. <hal-01275377>

HAL Id: hal-01275377
https://hal.inria.fr/hal-01275377

Submitted on 17 Feb 2016

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Revisiting Roos Bias in RC4 Key Scheduling Algorithm

Santanu Sarkar[1] and Ayineedi Venkateswarlu[2]

[1] Department of Mathematics, Indian Institute of Technology Madras, Chennai - 600036, INDIA.
santanu@iitm.ac.in

[2] Computer Science Unit, Indian Statistical Institute - Chennai Centre, MGR Knowledge City Road, Taramani, Chennai - 600113, INDIA.
venku@isichennai.res.in

Abstract. RC4 is one of the most popular stream cipher with wide industrial applications, it has received serious attention in cryptology literature in the last two decades. In 1995, Roos pointed out that the elements $S_N[y]$ of the permutation S_N after the Key Scheduling Algorithm for the first few values of y are biased to certain combinations of secret key bytes. These correlations were theoretically studied by Paul and Maitra (SAC 2007). The formula for the correlation probabilities provided by them gives a wrong impression that the probabilities decrease as the value of y becomes larger, which is not true. In this paper, we point out some gaps in their analysis and present a detailed analysis of Roos Bias. We provide a more accurate formula for the correlation probabilities.

Keywords: Stream Cipher, Cryptanalysis, RC4, Roos Bias.

1 Introduction

The stream cipher RC4 was designed by Ron Rivest in 1987. It is one of the simplest of all commercial ciphers, requiring only a few lines of code for its implementation. It is found in many applications like WEP, WPA, SSL, TLS etc.. The algorithm was kept secret initially and was revealed in 1994 anonymously over an internet newsgroup. Since then it has received serious attention by cryptology community. However, none of the existing cryptanalytic attacks on RC4 proves to be a serious threat to cipher and it continues to be of significant interest in the cryptology community.

The RC4 stream cipher has two components, namely, the Key Scheduling Algorithm (KSA) and the Pseudo-Random Generation Algorithm (PRGA). The data structure used in RC4 is as follows.

- The state consists of an array S of size N (typically, 256), which contains a permutation of the integers $\{0, \ldots, N-1\}$, two indices i (deterministic) and j (pseudo-random) and a secret key array K.

– Given a secret key key of l bytes (typically 5 to 32), the array K of size N is such that $K[y] = key[y \bmod l]$ for any y, $0 \leq y \leq N-1$.

Note that all additions in both the KSA and the PRGA are additions modulo N. The KSA uses an l-byte secret key $key[0, \ldots, (l-1)]$ to scramble an identity permutation S over $\mathbb{Z}_N$. The PRGA uses the scrambled permutation to generate a pseudo-random sequence of keystream bytes, $z_1, z_2, \ldots$, that are bitwise XOR-ed with the plaintext to generate the ciphertext at the sender end and bitwise XOR-ed with the ciphertext to get back the plaintext at the receiver end.

Both the KSA and the PRGA uses two indices i and j to access the permutation entries and swap a pair at every round. A brief description is given below.

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

In the last two decades many attacks on RC4 have been proposed. In 2001, Mantin and Shamir [7] proved that the second output byte of RC4 is biased towards zero. Correlations between the RC4 keystream bytes and the key were presented in [4]. In Eurocrypt 2011, Sepehrdad et al. [17] presented both distinguishing attack and key recovery attack on RC4 in WPA mode. In FSE 2011, Maitra et al. [6] observed that all the initial output bytes from 3 to 255 have positive bias towards zero. In FSE 2013, Isobe et al. [3] showed r-th output byte has positive bias towards r for $3 \leq r \leq 255$. AlFardan et al. [1](USENIX Security 2013) and Paterson et al. [13] (FSE 2014) exploited KSA keystream biases to recover plaintext in TLS and WPA. In Asiacrypt 2014, Paterson et al. [14] improved the plaintext recovery attack of [13].

Let S_r, i_r, j_r denote the permutation and the two indices after round r of RC4 KSA. Thus, the initial identity permutation is given by S_0 and the final permutation after the KSA is given by S_N. By f_y, we denote the expression $\frac{y(y+1)}{2} + \sum_{x=0}^{y} K[x]$, $0 \leq y \leq N-1$.

In 1995, Roos [15] pointed out a specific class of weak keys in RC4. It was shown in [15] that the values in the initial locations of S_N are correlated to some linear combination of the secret key bytes. So the permutation S_N leaks the secret key bytes with probability significantly higher than random association. This observation has immediate applications in WEP [18] and WPA [19] securities where RC4 is used as a building block.

Roos [15] argued that the most likely value of the y-th element of the permutation S_N after the KSA for the first few values of y is given by $S_N[y] = f_y$.

The experimental values of the probabilities $P(S_N[y] = f_y)$ for y reported in [15] steadily decrease from 0.37 to 0.006 as y varies from 0 to 47 and then slowly settles down to the random association of $1/N \approx 0.003906$. A theoretical justification appeared in [12] much later. In [12], authors also discussed how to reconstruct key from the final permutation S_N after KSA. Later Biham et al. [2] improved the reconstruction algorithm of [12]. Generalizing Roos-type biases, in [9] the probabilities of $P(S_N[y] = f_y - t)$ were studied for small t. It was also shown in [5] that not only the permutation bytes $S_N[y]$, but the nested permutation bytes, e.g., the bytes $S_N[S_N[y]]$, $S_N[S_N[S_N[y]]]$, and so on, are also biased to f_y. These types of biases are used to reconstruct key from the permutation S_N for better success probability. Experimental values of Roos biases reported in [15] are given in the Table 1.

y	$P(S_N[y] = f_y)$
0-15	.370 .368 .362 .358 .349 .340 .330 .322 .309 .298 .285 .275 .260 .245 .229 .216
16-31	.203 .189 .173 .161 .147 .135 .124 .112 .101 .090 .082 .074 .064 .057 .051 .044
32-47	.039 .035 .030 .026 .023 .020 .017 .014 .013 .012 .010 .009 .008 .007 .006 .006

Table 1. The probabilities experimentally observed by Roos [15].

Our Contribution: It appears that researchers have looked at only the initial bytes of the state S_N because of the strong bias (observed by Roos as given in Table 1), and ignored the bias that may be of significance in the latter part. The theoretical analysis of Roos bias by Paul and Maitra also concentrate on the initial part and it was claimed in [12] that the probabilities $P(S_N[y] = f_y)$ for

> "index 48 onwards, both the theoretical as well as the experimental values tend to $\frac{1}{N}$ $(= 0.0039$ for $N = 256)$."

Moreover, the formula for the correlation probabilities provided in [12] (see also Proposition 1) gives a wrong impression that the probabilities decrease as the value of y becomes larger. In this paper, we will show that the above claim is not correct. In fact, when $y = 59$ the experimental value $P(S_N[y] = f_y)$ is approximately 82% of $\frac{1}{N}$. Experimental analysis establishes that the biases show wavy tendency rather than a steady decrease from the index $y = 45$ onwards. We will present a detailed analysis of Roos bias, and we will also see that certain assumptions lead to less accurate probabilities in the work of [12]. Our analysis gives much a better approximation of Roos bias.

2 Analysis of Roos Biases

As mentioned in the previous section, Roos biases relate the permutation entry $S_N[y]$ to the key combination f_y. The proof sketches of this relation appeared

in [15] and later in [10]. A detailed theoretical justification and analytical formula for the correlation probabilities was first provided in [12].

2.1 Analysis of Roos Biases by Paul and Maitra

We will now briefly discuss theoretical analysis and formula for the correlation probabilities given by Paul and Maitra.

Proposition 1. *[12, Theorem 1] Assume that the index j takes its value from $\mathbb{Z}_N$ independently and uniformly at random at each round of KSA. Then, on completion of RC4 KSA, we have for $0 \leq y \leq N-1$,*

$$P(S_N[y] = f_y) \approx \frac{1}{N} + \left(1 - \frac{y}{N}\right) \cdot \left(1 - \frac{1}{N}\right)^{\frac{y(y+1)}{2}+N}.$$

The authors consider the following three events in their analysis and derivation of the above formula. For any fixed y,

1. Event X : $S_t[t] = t$ for $1 \leq t \leq y$
2. Event Y : $j_{y+1} \notin \{0, \ldots, y-1\}$ and also j_{y+1} is not touched by $j_1, \ldots, j_y$
3. Event Z : $j_t \neq y$ for $y+2 \leq t \leq N$

The first event X is same as the event $j_t \notin \{t, \ldots, y\}$ for $1 \leq t \leq y$. In this case we get

$$j_{y+1} = \sum_{t=0}^{y} \big(K[t] + S_t[t]\big) = \sum_{t=0}^{y} \big(K[t] + t\big) = \frac{y(y+1)}{2} + \sum_{t=0}^{y} K[t] = f_y.$$

If the second event occurs then $S_y[j_{y+1}] = j_{y+1}$. Hence after swap we get $S_{y+1}[y] = j_{y+1}$. The third event makes the value in y-th location of the state is not disturbed after the y-th round of KSA. Hence if all the three events X, Y and Z occur simultaneously then we get $S_N[y] = S_{y+1}[y] = j_{y+1} = f_y$.

In [12], it is estimated that $P(j_{y+1} = f_y) \approx \left(\frac{N-1}{N}\right)^{1+\frac{y(y+1)}{2}} + \frac{1}{N}$ assuming random association on the complementary path of the event X. Probability of the second and third events hold jointly is estimated as $\left(\frac{N-y}{N}\right)\left(\frac{N-1}{N}\right)^{N-1}$. The formula given in Proposition 1 is derived by Paul and Maitra by assuming again random association on the complementary path of $Y \cap Z \cap \{j_{y+1} = f_y\}$.

2.2 Our Concern

We can see that from Proposition 1

$$\mathrm{P}(S_N[y] = f_y) > \frac{1}{N}$$

for any y, and the probabilities decrease as the index y becomes larger. We observe that this is not true, and the probabilities show wavy tendency over the line $\frac{1}{N}$. In fact, when we take $y = 59$ we get $P(S_N[y] = f_y) = 0.004183$ according to Proposition 1. However, we have observed experimentally that

$$P(S_N[y] = f_y) = 0.003204 = \frac{41}{50} \cdot \frac{1}{N}$$

for $y = 59$. This less accurate estimation is due to certain events for which $P(S_N[y] = f_y)$ is assumed to be $\frac{1}{N}$ in [12], which is not the case. To be specific, it is assumed in [12] that $P(j_{y+1} = f_y) \approx \frac{1}{N}$ even when $X^c : j_t \in \{t, \ldots, y\}$ for some $t \in [1, y]$ holds. But this is not true. Experimentally we see that $P(j_{51} = f_{50}) = \frac{37}{100} \cdot \frac{1}{N}$. In the analysis of [12] the authors have taken $P(j_{y+1} = f_y \mid X^c \cap Y) = \frac{1}{N}$. However, experiments show that $P(j_{51} = f_{50} \mid X^c \cap Y) < \frac{0.01}{N}$, and so this event is very unlikely. This is because if $j_t \in \{t, \ldots, y\}$ for exactly one $t \in [1, y]$ and Y holds then j_{y+1} will always be different from f_y. Our analysis takes care of this scenario.

Also in [12], the probability of the first event X is estimated as $P(X) = \prod_{i=1}^{y} \left(1 - \frac{1}{N}\right)^i$. But one can see that this probability should be $\prod_{i=1}^{y} \left(1 - \frac{i}{N}\right)$.

We will now present our analysis of Roos bias. We will first find $P(S_{y+1}[y] = f_y)$. Then we use this probability to derive formula for $S_N[y] = f_y$.

2.3 Probability of $S_{y+1}[y] = f_y$

Consider the following three events:

1. Event $A : j_t \notin \{t, \ldots, y\}$ for $1 \leq t \leq y$
2. Event $B : f_y \notin \{0, 1, \cdots, y-1\}$
3. Event $C : j_t \neq f_y$ for $1 \leq t \leq y$.

We always assume that j_t is uniformly distributed over $\mathbb{Z}_N$. We can estimate the probabilities of the above three events as given below.

$$P(A) = \prod_{i=1}^{y} \left(1 - \frac{i}{N}\right), \qquad P(B) = \left(1 - \frac{y}{N}\right) \quad \text{and} \quad P(C) = \left(1 - \frac{1}{N}\right)^y.$$

It is not difficult to see that if the events A, B and C occur simultaneously then $S_{y+1}[y]$ will always be equal to f_y. That is

$$P(S_{y+1}[y] = f_y \mid A \cap B \cap C) = 1. \tag{1}$$

On the other hand it can also be seen that

$$P(S_{y+1}[y] = f_y \mid A \cap B^c \cap C) = P(S_{y+1}[y] = f_y \mid A \cap B \cap C^c) = 0, \tag{2}$$

where B^c and C^c are complement of B and C respectively. As discussed we need to treat the case carefully where the event A^c occurs. In particular we

analyse the event $A^c \cap B \cap C$. For this purpose, we introduce a new variable $v_y = \sum_{i=0}^{y}(i - S_i[i])$ to keep track of the gap between j_{y+1} and f_y.

One can see that $S_i[i] \leq i$ for $i \leq y$. Thus we must always have $v_y \geq 0$. Also $v_y = \sum_{i=0}^{y}\Big(i - S_i[i]\Big) \leq \sum_{i=0}^{y} i = \frac{y(y+1)}{2}$. It is easy to see that v_y measures the difference between f_y and j_{y+1}. That is $f_y \equiv j_{y+1} + v_y \mod N$. Thus if $v_y \not\equiv 0 \mod N$ then j_{y+1} will be different from f_y. Since B and C hold, we get $S_y[f_y] = f_y$. Hence $S_{y+1}[y] \neq f_y$. Therefore we have

$$P(S_{y+1}[y] = f_y \mid \{v_y \not\equiv 0 \mod N\} \cap B \cap C) = 0. \tag{3}$$

On the other hand if $v_y \equiv 0 \mod N$ then $j_{y+1} = f_y$. Therefore we have

$$P(S_{y+1}[y] = f_y \mid \{v_y \equiv 0 \mod N\} \cap B \cap C) = 1. \tag{4}$$

Observe that if $v_y = 0$ then we must have $S_i[i] = i$ for $i \leq y$, and this is equivalent to the event A. The identity (4) includes occurrence of the event A. This way we get one negative path and another positive path for Roos bias. Thus our interest is to find out $P\big(\{v_y \not\equiv 0 \mod N\}\big)$ and $P\big(\{v_y \equiv 0 \mod N\} \cap \{v_y \neq 0\}\big)$. Let us denote the latter event by A'. To estimate these probabilities, we first calculate the expected value $E(v_y)$ and the variance $Var(v_y)$ of v_y and then use Central Limit Theorem to obtain the probabilities. Let us first state an useful result [8, Claim C.3.2].

Lemma 1. *For $b > a$, $P(S_b[b] = a) = \Big(1 - \frac{1}{N}\Big)^{a}\frac{1}{N}$*

Now we estimate the values $E(v_y)$ and $Var(v_y)$.

Theorem 1. *The expected value of v_y is given by*

$$E(v_y) = \sum_{r=0}^{y}\sum_{x=0}^{r-1}\Big(1 - \frac{1}{N}\Big)^{x}\frac{1}{N}\Big(r - x\Big)$$

with variance

$$Var(v_y) = \sum_{r=0}^{y}\Bigg[\sum_{x=0}^{r-1}\Big(1 - \frac{1}{N}\Big)^{x}\frac{1}{N}\Big(r - x\Big)^2 - \Bigg(\sum_{x=0}^{r-1}\Big(1 - \frac{1}{N}\Big)^{x}\frac{1}{N}\Big(r - x\Big)\Bigg)^2\Bigg].$$

Proof. Let us set $v_{r,y} = r - S_r[r]$ for $0 \leq r \leq y$. Clearly $v_y = \sum_{r=0}^{y} v_{r,y}$. So $E(v_y) = \sum_{r=0}^{y} E(v_{r,y})$. Hence we first calculate $E(v_{r,y})$. Now from Lemma 1, we have $P(S_r[r] = x) = \Big(1 - \frac{1}{N}\Big)^{x}\frac{1}{N}$ for $x < r$. Also $S_r[r]$ can not be larger than r. Therefore we get

$$E(v_{r,y}) = \sum_{x=0}^{r-1} P(S_r[r] = x) \cdot (r - x) = \sum_{x=0}^{r-1}\Big(1 - \frac{1}{N}\Big)^{x}\frac{1}{N}\Big(r - x\Big).$$

Thus

$$E(v_y) = \sum_{r=0}^{y} \sum_{x=0}^{r-1} \Big(1 - \frac{1}{N}\Big)^x \frac{1}{N} \Big(r - x\Big).$$

Also

$$\begin{aligned} Var(v_{r,y}) &= E(v_{r,y}^2) - (E(v_{r,y}))^2 \\ &= \sum_{x=0}^{r-1} \Big(1 - \frac{1}{N}\Big)^x \frac{1}{N} \Big(r - x\Big)^2 - \Big(\sum_{x=0}^{r-1} \Big(1 - \frac{1}{N}\Big)^x \frac{1}{N} \Big(r - x\Big)\Big)^2. \end{aligned}$$

If we assume $\{v_{r,y}\}_{r=0}^{y}$ are independent then we get $Var(v_y) = \sum_{r=0}^{y} Var(v_{r,y})$ and it is given by

$$\sum_{r=0}^{y} \Big[\sum_{x=0}^{r-1} \Big(1 - \frac{1}{N}\Big)^x \frac{1}{N} \Big(r - x\Big)^2 - \Big(\sum_{x=0}^{r-1} \Big(1 - \frac{1}{N}\Big)^x \frac{1}{N} \Big(r - x\Big)\Big)^2\Big].$$

□

From Central Limit Theorem [11], we can assume that v_y follows Truncated Normal distribution and lies within the interval $[0, b]$ with mean $\mu = E(v_y)$ and variance $\sigma^2 = Var(v_y)$, where $b = \frac{y(y+1)}{2}$. So we have

$$P(v_y \not\equiv 0 \bmod N) \approx \sum_{c=0}^{\infty} \frac{1}{\Phi(\frac{b-\mu}{\sigma}) - \Phi(\frac{0-\mu}{\sigma})} \cdot \frac{1}{\sigma} \int_{0.5+cN}^{\min\{(c+1)N-0.5, b\}} \phi\big(\frac{x-\mu}{\sigma}\big),$$

$$P(A') \approx \sum_{c=1}^{\infty} \frac{1}{\Phi(\frac{b-\mu}{\sigma}) - \Phi(\frac{0-\mu}{\sigma})} \cdot \frac{1}{\sigma} \int_{cN-0.5}^{\min\{cN+0.5, b\}} \phi\big(\frac{x-\mu}{\sigma}\big),$$

where $\phi(x) = \frac{e^{-\frac{x^2}{2}}}{\sqrt{2\pi}}$ is the probability density function of the standard Normal distribution and $\Phi(\cdot)$ is its cumulative distribution function. Recall that the event $v_y = 0$ is exactly same as A. Hence we exclude the case $v_y = 0$.

Thus from identities (1), (2), (3) and (4) and considering random situation in the other cases, the probability $P(S_{y+1}[y] = f_y)$ can be expressed as:
$P(S_{y+1}[y] = f_y \mid A \cap B \cap C)P(A \cap B \cap C) +$
$P(S_{y+1}[y] = f_y \mid A \cap B^c \cap C)P(A \cap B^c \cap C) +$
$P(S_{y+1}[y] = f_y \mid A \cap B \cap C^c)P(A \cap B \cap C^c) +$
$P(S_{y+1}[y] = f_y \mid \{v_y \not\equiv 0 \bmod N\} \cap B \cap C)P(\{v_y \not\equiv 0 \bmod N\} \cap B \cap C) +$
$P(S_{y+1}[y] = f_y \mid A' \cap B \cap C)P(A' \cap B \cap C) +$
$\frac{1}{N}\big(1 - P(A \cap B \cap C) - P(A \cap B^c \cap C) - P(A \cap B \cap C^c) - P(A' \cap B \cap C) - P(A' \cap B \cap C)\big)$
$= P(A \cap B \cap C) + P(A' \cap B \cap C) + \frac{1}{N}\big(1 - P(A \cap B \cap C) - P(A \cap B^c \cap C) -$
$P(A \cap B \cap C^c) - P(\{v_y \not\equiv 0 \bmod N\} \cap B \cap C) - P(A' \cap B \cap C)\big).$

By putting all the probabilities in the above identity we get a formula for $P(S_{y+1}[y] = f_y)$ as stated in the following lemma.

Lemma 2. *The probability of $P(S_{y+1}[y] = f_y)$ can be given by*

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

where

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

2.4 Probability of $P(S_N[y] = f_y)$ and Comparative Study

Now one can easily find the value of $P(S_N[y] = f_y)$ from $P(S_{y+1}[y] = f_y)$ as given below.

Theorem 2. *We get*

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

Proof. We have two cases:

- Case 1: Let $S_{y+1}[y] = f_y$. Then if any $j_{y+2}, \cdots, j_N$ touches the y-th location then $S_N[y] \neq f_y$. And $j_{y+2}, \cdots, j_N$ all are different from y happens with probability $\big(1-\frac{1}{N}\big)^{N-1-y}$.
- Case 2: Let $S_{y+1}[y] \neq f_y$. If suppose $S_{y+1}[t] = f_y$ for some $t < y$ then f_y can not moved to yth location in further rounds of KSA. So let us consider the scenario where $S_t[t] = f_y$ for some $t > y$. Suppose that $j_{t+1} = y$ and $j_{t+2}, \cdots, j_N$ all are different from y. Hence after the swap we get $S_{t+1}[y] = f_y$

and this location is not disturbed in further rounds of KSA. This path holds with probability $\frac{1}{N^2} \cdot \big(1 - \frac{1}{N}\big)^{N-1-t}$. Since $t \in [y+1, N-1]$, we have

$$P\big(S_N[y] = f_y \mid S_{y+1}[y] \neq f_y\big) = \sum_{t=y+1}^{N-1} \frac{1}{N^2}\big(1 - \frac{1}{N}\big)^{N-1-t}$$

Adding the cases we get the formula as stated. □

Using Table 2 we present our comparative study of the correlation probabilities. We present theoretical values of $\mathrm{P}(S_N[y] = f_y)$ for $0 \leq y \leq 95$ according to Theorem 2 and also according to the formula of [12, Theorem 1]. We have calculated the values p_1 and p_2 in Lemma 2 using numerical methods available in Sage [16]. The experimental values are averaged over 10 billion key schedulings, where the key is of length 16 and are randomly generated.

From Table 2, it is clear that our estimation gives a much better approximation than [12]. One can note that from Table 2, $P(S_N[y] = y) < \frac{1}{N}$ for $y \in [51, 69]$. After that it again becomes positive up to $y = 83$.

y		$P(S_N[y] = f_y)$							
0-7	Paul et al. [12]	0.371066	0.368203	0.363945	0.358342	0.351457	0.343369	0.334169	0.323958
	Exp.	0.368563	0.365907	0.361276	0.356108	0.348788	0.340914	0.331431	0.321580
	Thm. 2	0.371066	0.368203	0.363940	0.358320	0.351403	0.343264	0.333990	0.323680
8-15	Paul et al. [12]	0.312847	0.300951	0.288393	0.275297	0.261789	0.247991	0.234026	0.220008
	Exp.	0.309965	0.298342	0.285258	0.272382	0.258284	0.244326	0.230165	0.216406
	Thm. 2	0.312443	0.300396	0.287661	0.274365	0.260635	0.246600	0.232383	0.218108
16-23	Paul et al. [12]	0.206048	0.192248	0.178701	0.165492	0.152696	0.140375	0.128583	0.117363
	Exp.	0.201742	0.188135	0.174017	0.161007	0.147677	0.135578	0.123297	0.112364
	Thm. 2	0.203887	0.189829	0.176034	0.162589	0.149575	0.137059	0.125099	0.112486
24-31	Paul et al. [12]	0.106748	0.096759	0.087412	0.078711	0.070654	0.063231	0.056426	0.050219
	Exp.	0.101313	0.091684	0.081978	0.073656	0.065246	0.058080	0.051557	0.045035
	Thm. 2	0.101762	0.091699	0.082310	0.073601	0.065568	0.058199	0.051478	0.045380
32-39	Paul et al. [12]	0.044586	0.039497	0.034923	0.030830	0.027186	0.023956	0.021106	0.018604
	Exp.	0.039709	0.034941	0.030516	0.026688	0.023179	0.020069	0.017615	0.015267
	Thm. 2	0.039878	0.034941	0.030534	0.026621	0.023165	0.020130	0.017478	0.015173
40-47	Paul et al. [12]	0.016416	0.014512	0.012862	0.01144	0.010218	0.009174	0.008285	0.007532
	Exp.	0.013233	0.011523	0.010019	0.008734	0.007606	0.006747	0.006056	0.005372
	Thm. 2	0.013180	0.011466	0.009999	0.008752	0.007696	0.006807	0.006063	0.005444
48-55	Paul et al. [12]	0.006897	0.006363	0.005917	0.005545	0.005237	0.004982	0.004773	0.004602
	Exp.	0.004929	0.004502	0.004142	0.003866	0.003650	0.003481	0.003370	0.003276
	Thm. 2	0.004931	0.004509	0.004165	0.003886	0.003665	0.003492	0.003362	0.003271
56-63	Paul et al. [12]	0.004462	0.004349	0.004257	0.004183	0.004124	0.004077	0.004040	0.004010
	Exp.	0.003220	0.003199	0.003190	0.003203	0.003235	0.003295	0.003360	0.003455
	Thm. 2	0.003216	0.003192	0.003198	0.003229	0.003282	0.003352	0.003433	0.003522
64-71	Paul et al. [12]	0.003986	0.003968	0.003954	0.003943	0.003934	0.003927	0.003922	0.003918
	Exp.	0.003484	0.003576	0.003667	0.003740	0.003817	0.003886	0.003945	0.003988
	Thm. 2	0.003612	0.003699	0.003779	0.003849	0.003907	0.003950	0.003981	0.003998
72-79	Paul et al. [12]	0.003915	0.003913	0.003911	0.003910	0.003909	0.003908	0.003908	0.003907
	Exp.	0.004024	0.004045	0.004057	0.004054	0.004047	0.004033	0.004014	0.003992
	Thm. 2	0.004003	0.003998	0.003987	0.003970	0.003952	0.003933	0.003916	0.003901
80-87	Paul et al. [12]	0.003907	0.003907	0.003907	0.003907	0.003906	0.003906	0.003906	0.003906
	Exp.	0.003970	0.003948	0.003931	0.003912	0.003899	0.003891	0.003886	0.003883
	Thm. 2	0.003891	0.003884	0.003880	0.003880	0.003882	0.003885	0.003890	0.003894
88-95	Paul et al. [12]	0.003906	0.003906	0.003906	0.003906	0.003906	0.003906	0.003906	0.003906
	Exp.	0.003881	0.003886	0.003888	0.003892	0.003895	0.003900	0.003899	0.003909
	Thm. 2	0.003897	0.003900	0.003902	0.003904	0.003904	0.003905	0.003905	0.003905
96-103	Paul et al. [12]	0.003906	0.003906	0.003906	0.003906	0.003906	0.003906	0.003906	0.003906
	Exp.	0.003892	0.003897	0.003899	0.003898	0.003899	0.003902	0.003902	0.003902
	Thm. 2	0.003905	0.003905	0.003905	0.003905	0.003905	0.003905	0.003905	0.003906

Table 2. Comparison of our work with the work of [12] and experimental values.

To emphasize the difference, we also compare pictorially in Figure 1 for the index y values between 45 and 103. One can see that from the Figure 1 our formula gives a much better approximation of Roos bias. To be specific, our analysis captures the wavy tendency of the experimental values.

The theoretical estimation according to [12, Theorem 1] becomes $\approx \frac{1}{N}$ when $y \geq 81$. But according to our analysis, the estimation becomes $\approx \frac{1}{N}$ when $y \geq 104$. However, we have observed experimentally that there are still significant biases beyond $y \geq 104$. With 16 byte key, our experimental data shows that maximum positive value occurring $P(S_N[127] = f_{127}) = \frac{1}{N} + \frac{1.6}{N^2}$ and maximum negative value occurring $P(S_N[128] = f_{128}) = \frac{1}{N} - \frac{2.8}{N^2}$ for $y \geq 104$. We do not see such significant biases when the key length is of 17 bytes. It seems that these biases at locations beyond 104 are dependent on the key length. We take this opportunity to present our experimental values pictorially in Figure 2 for both 16 bytes and 17 bytes key.

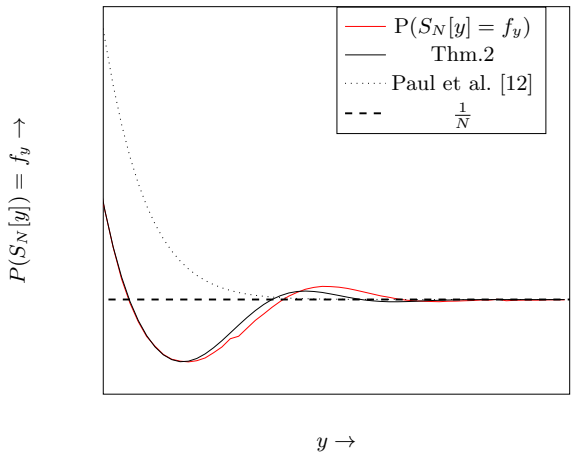

Fig. 1. Distribution of $P(S_N[y] = f_y)$ for $y \in [45, 103]$.

Remark: Maitra and Paul studied Roos-type nested biases $\mathrm{P}(S_N[S_N[y]] = f_y)$ in FSE-2008 paper. We observe that there is significant difference between theoretical values and empirical values. We would like to work on this in the future.

References

1. N. AlFardan, D. Bernstein, K. Paterson, B. Poettering, and J. Schuldt. On the security of RC4 in TLS. In USENIX 2013, pp. 305–320, 2013. Published online at `http://www.isg.rhul.ac.uk/tls/`.
2. E. Biham and Y. Carmeli. Efficient Reconstruction of RC4 Keys from Internal States. In FSE 2008, vol. 5086 of LNCS, pp. 270–288.
3. T. Isobe, T. Ohigashi, Y. Watanabe, and M. Morii. Full plaintext recovery attack on broadcast RC4. In FSE 2013, vol. 8424 of LNCS, pp. 179–202, 2013.
4. A. Klein. Attacks on the RC4 stream cipher. Des. Codes Cryptography, 48(3), pp. 269–286, 2008.
5. S. Maitra and G. Paul. New Form of Permutation Bias and Secret Key Leakage in Keystream Bytes of RC4. In FSE 2008, vol. 5086 of LNCS, pp. 253–269, 2008.

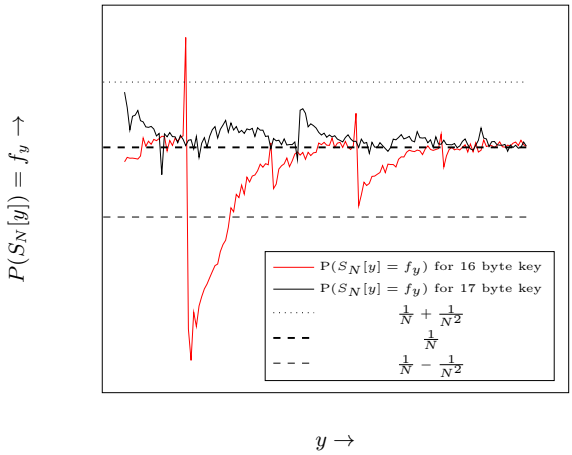

Fig. 2. Distribution of $P(S_N[y] = f_y)$ for $y \in [104, 255]$.

6. S. Maitra, G. Paul, and S. Sen Gupta. Attack on broadcast RC4 Revisited. In FSE 2011, vol. 6733 of LNCS, pp. 199–217, 2011.
7. I. Mantin and A. Shamir. A Practical Attack on Broadcast RC4. In FSE 2001, vol. 2355 of LNCS, pp. 152164, 2002.
8. I. Mantin. Analysis of the stream cipher RC4. Masters Thesis, The Weizmann Institute of Science, Israel (2001).
9. S. Maitra, G. Paul, S. Sarkar, M. Lehmann, W. Meier. New Results on Generalization of Roos-Type Biases and Related Keystreams of RC4. In Africacrypt 2008, vol. 7918 of LNCS, pp. 222239, 2002.
10. M. E. McKague. Design and Analysis of RC4-like Stream Ciphers. Master's Thesis, University of Waterloo, Canda, 2005.
11. J. K. Patel and C. B. Read. Handbook of the Normal Distribution. CRC Press, 1996.
12. G. Paul and S. Maitra. Permutation after RC4 Key Scheduling Reveals the Secret Key. In SAC 2007, vol. 4876 of LNCS, pp. 360–377.
13. K. G. Paterson, J. Schuldt and B. Poettering. Plaintext Recovery Attacks Against WPA/TKIP. Accepted in FSE 2014.
14. K. G. Paterson, B. Poettering and J. C. N. Schuldt. Big Bias Hunting in Amazonia: Large-Scale Computation and Exploitation of RC4 Biases (Invited Paper). In ASIACRYPT 2014, vol. 8873 of LNCS, pp. 398–419, 2014.
15. A. Roos. A class of weak keys in the RC4 stream cipher. Two posts in sci.crypt, message-id `43u1eh$1j3@hermes.is.co.za`, `44ebge$llf@hermes.is.co.za`, 1995.
16. Sage: Open Source Mathematics Software. `http://www.sagemath.org/`.
17. P. Sepehrdad, S. Vaudenay, and M. Vuagnoux. Statistical Attack on RC4 - Distinguishing WPA. In EUROCRYPT 2011, vol. 6632 of LNCS, pp. 343–363.
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)