Designs, Codes and Cryptography manuscript No.
(will be inserted by the editor)

Proving TLS-attack related open biases of RC4

Santanu Sarkar · Sourav Sen Gupta · Goutam Paul · Subhamoy Maitra

Received: date / Accepted: date

Abstract After a series of results on RC4 cryptanalysis in flagship cryptology conferences and journals, one of the most significant recent attacks on the cipher has been the discovery of vulnerabilities in the SSL/TLS protocol, by AlFardan et al. (USENIX 2013). Through extensive computations, they identified some new significant short-term single-byte biases in RC4 keystream sequence, and utilized those, along-with existing biases, towards the TLS attack. The current article proves these new and unproved biases in RC4, and in the process discovers intricate non-randomness within the cipher. In this connection, we also prove the anomaly in the 128th element of the permutation after the Key Scheduling Algorithm. Finally, the proof for the extended key-length dependent biases in RC4 keystream sequence, a problem attempted and partially solved by Isobe et al. in FSE 2013, has also been completed in this work.

Keywords Anomaly · Biases · RC4 · Pseudo-randomness · Sequence · Stream Cipher · TLS

Mathematics Subject Classification (2010) 94A60

CR Subject Classification (2012) Block and stream ciphers, Cryptanalysis and other attacks

1 Introduction

Over the last three decades of research in stream ciphers, several designs have been proposed and analyzed by the community. The RC4 stream cipher, 'allegedly' designed by Rivest in 1987, has sustained to be one of the most popular ciphers in this category for more than 25

S. Sarkar
Chennai Mathematical Institute, Chennai 603 103, India
E-mail: sarkar.santanu.bir@gmail.com

S. Sen Gupta and G. Paul
Cryptology and Security Research Unit, R. C. Bose Centre for Cryptology and Security, Indian Statistical Institute, Kolkata 700 108, India
E-mail: sg.sourav@gmail.com, goutam.paul@isical.ac.in

S. Maitra
Applied Statistics Unit, Indian Statistical Institute, Kolkata 700 108, India
E-mail: subho@isical.ac.in

years. The cipher has continued gaining its fabled popularity for its intriguing simplicity that has made it widely accepted in the community for various software and web applications.

A stream cipher produces a pseudo-random sequence of words, called the keystream, and the encryption is performed by bitwise XOR-ing it with the plaintext. One important primitive for building a stream cipher is pseudo-random permutation based on a secret key. For keystream generation, one can extract a pseudo-random sequence from this permutation. Ensuring pseudo-randomness of the permutation is not enough to guarantee pseudo-randomness in the keystream. In such a scenario, it may be possible to identify certain biased events in the keystream.

An ideal stream cipher is expected to produce a uniformly random keystream, i.e., for any event involving the keystream, the associated random variable would have maximum entropy. If there is a bias in any event, then the associated random variable has strictly less than the maximum possible entropy, which in turn implies that the condition for information-theoretic secrecy is violated. In RC4, we not only have many short-term and few long-term biases in the keystream, we also have biases of the keystream bytes and the internal state variables towards the secret key. These biases are the source of vulnerabilities of RC4, particularly so in the TLS protocol.

RC4 consists of two major components, the Key Scheduling Algorithm (KSA) and the Pseudo-Random Generation Algorithm (PRGA). The internal permutation of RC4 is of $N = 256$ bytes, and so is the key K. The original secret key is of length typically between 5 to 32 bytes, and is repeated to form the final key K. The KSA produces the initial permutation of RC4 by scrambling an identity permutation using key K. The initial permutation S produced by the KSA acts as an input to the next procedure PRGA that generates the output keystream. The RC4 algorithm is as shown in Figure 1.

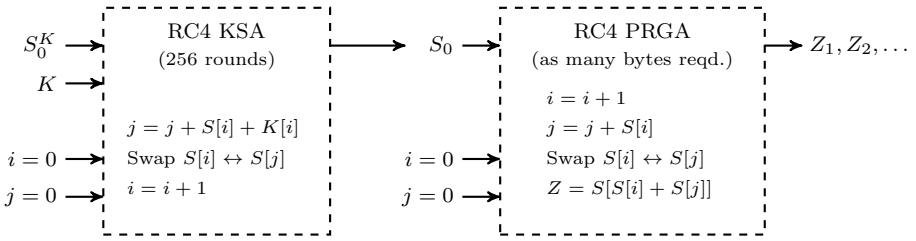

Fig. 1 Key-Scheduling Algorithm and Pseudo-Random Generation Algorithm of RC4. The additions are modulo $N = 256$.

Notation: For round $r \geq 1$ of RC4 PRGA, we denote the indices by i_r, j_r, the output byte by Z_r, the index location of output Z_r as t_r, and the permutations before and after the swap by S_{r-1} and S_r respectively. Thus, round r of RC4 PRGA is defined by $i_r = i_{r-1} + 1$, $j_r = j_{r-1} + S_{r-1}[i_r]$, swap $S_{r-1}[i_r] \leftrightarrow S_{r-1}[j_r]$, $t_r = S_r[i_r] + S_r[j_r]$, and $Z_r = S_r[t_r]$. After $r \geq 1$ 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. Throughout this paper, all operations in context of RC4 are to be considered modulo N. Throughout this paper, N has the value 256. In some of the expressions for biases, we have used the form $\frac{1}{N} \pm \frac{\epsilon}{N^a}$, where ϵ is a numerical constant (based on the substitution $N = 256$ in some part of the expression) and a is an integer, which is typically 1 or 2. This form helps in comprehending the extent of the bias with respect to $\frac{1}{N}$. We approximate the term $1 - \frac{a}{N}$ by $\left(1 - \frac{1}{N}\right)^a$, whenever a is very small compared to N.

Assumptions: At many places, we approximate the distribution (or conditional distribution) of a random variable to be uniform. The assumptions of uniform randomness have been verified by extensive experimentation. Moreover, when we replace the joint distribution of two or more random variables by the product of their marginal distributions, their statistical independence is implicitly assumed.

1.1 Motivation of our work

In a recent paper [26] at FSE 2013, Sepehrdad, Susil, Vaudenay, and Vuagnoux have rightly claimed:

> *For some people, attacking WEP is like beating a dead horse, but this horse is still running wildly in many countries all over the world. Also, some companies are selling hardware using modified versions of the WEP protocol, they claim to be secure.*

IEEE WiFi security protocol WEP is based on the stream cipher RC4, and hence the same statement applies to RC4 as well. The history of RC4 cryptanalysis is more than 20 years old. However, in recent times, there is a renewed surge of interest in RC4 cryptanalysis in the cryptographic community. For example, significant cryptanalytic results on WEP and WPA have been published in Eurocrypt 2011 by Sepehrdad, Vaudenay, and Vuagnoux [28]. Recently, RC4 has attracted quite a few publications [1, 8, 11–13, 19, 22, 24, 26, 29]. In spite of this, many problems are still open and the cipher is not yet broken. One may safely use RC4 if some precautions are taken (i.e., initial few hundreds bytes are thrown away).

As a stream cipher, RC4 promises to deliver pseudo-random bytes as keystream output. Thus, any lapse in that goal creates interesting consequences towards the security of the cipher. This is the reason why statistical weaknesses like biases and their application as distinguishers have attracted the main focus of RC4 cryptanalysis to date. There have been numerous results on RC4 biases over years, and the trend still continues.

Most of the existing results are targeted towards specific short-term (involving only the initial few bytes of the output) biases and correlations [1, 6–8, 10, 14, 17, 18, 21, 24, 25, 27, 28], 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 [3, 5, 6, 10, 16].

In this paper, we concentrate on the short-term traits of non-random behavior in the initial keystream bytes of RC4, especially in the first N output bytes. The prominent results on the short-term biases of RC4 include Mantin and Shamir second byte bias [17], Mironov first byte sine-curve-like distribution [18], Maitra, Paul and Sen Gupta short-term biases towards zero [14], Sen Gupta, Maitra, Paul and Sarkar proof of first byte bias [24], Sarkar second byte negative bias [22], Isobe, Ohigashi, Watanabe and Morii full broadcast attack [8], and the most recent results by AlFardan, Bernstein, Paterson, Poettering and Schuldt [1, 4].

Broadcast attack by AlFardan et. al. [1,4]: The most prominent attempt at identifying all possible single-byte short-term biases in the initial keystream bytes of RC4 was recently made by AlFardan, Bernstein, Paterson, Poettering and Schuldt [1, 4]. They ran extensive experiments, using more than 2^{44} random keys, to generate a list of approximately 65536 single-byte short-term biases of RC4, including the previously known ones [8,14,17,18,24]. This search provides a comprehensive list of non-random behavior of the initial keystream bytes (bytes 1 to $N = 256$) of RC4 when a 16-byte key is used.

The main goal of this analysis [1] was to exploit those in a practical attack against the SSL/TLS protocol that uses RC4 for confidentiality. The authors could use all of the above-mentioned 65536 initial short-term biases of RC4 to mount a plaintext recovery attack on the SSL/TLS protocol that recovers the first 256 bytes of the plaintext from the knowledge of

only 2^{32} ciphertexts generated using random keys, with no prior plaintext knowledge. This attack by AlFardan, Bernstein, Paterson, Poettering and Schuldt [1] is undoubtedly the most extensive attack on any RC4-based protocol to date, with far-reaching consequences. This attack alone is sufficient to highlight the practical importance of identifying and exploiting short-term biases in RC4.

RC4 short-term landscape : The extensive experimental results by AlFardan, Bernstein, Paterson, Poettering and Schuldt [1] identified several non-randomness in the short-term output keystream of RC4. Figure 2 presents a 3D model of the probabilities $\Pr(Z_r = v)$ for $r = 1, \ldots, N$ and $v = 0, \ldots, N-1$, which we call the RC4 landscape of initial keystream bytes. This is based on the data generated from [1, 4].

Note that this landscape is for the most practical version of RC4 that uses a 16-byte key, and is not identical for RC4 initial keystream patterns generated by secret keys of various other lengths. For example, the non-random peaks and troughs present in the 16-byte key landscape reduce to a certain extent if one uses a full length $N = 256$ bytes key.

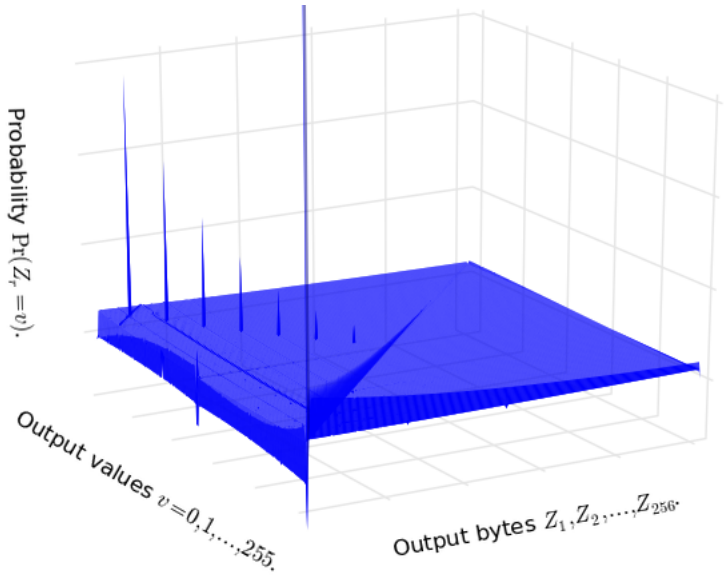

Fig. 2 The RC4 landscape of initial keystream bytes (data from [1, 4]).

The visible vertical walls and spikes in Figure 2 identify the prominent short-term bias patterns in the RC4 landscape. The main ones are for the events $Z_2 = 0$ (largest positive spike), $Z_2 = 2$ (largest negative spike), $Z_1 = v$ where $v = 0, \ldots, N-1$ (sine-curve-like vertical wall on the left side), $Z_r = 0$ (decreasing vertical wall on the right side), $Z_r = r$ (decreasing vertical wall at the center) and $Z_r = -r$ (decreasing series of spikes at the center), where $r = 1, \ldots, N$ denotes the number of the round in RC4 PRGA.

The proofs for most of these major non-random events are present in the literature. The biases in $Z_2 = 0$ and $Z_2 = 2$ have been proved by Mantin and Shamir [17] in 2001 and Sarkar [22] in 2013 respectively. The sine-curve-like pattern of Z_1 for full-length key, including the negative biases in $Z_1 = 0, 1$, have been proved by Sen Gupta, Maitra, Paul and Sarkar [24] in 2013, and the general proof for $Z_r = 0$ has been done by Maitra, Paul and Sen Gupta [14]

in 2011. Sen Gupta, Maitra, Paul and Sarkar [24] proved the $Z_r = -r$ case for $r = 16$ (key-length), and in 2013, the general pattern for $Z_r = -r$ was partially proved by Isobe, Ohigashi, Watanabe and Morii [8]. In the same paper of 2013, Isobe, Ohigashi, Watanabe and Morii [8] attempted the proof for the bias pattern for $Z_r = r$, and proved the slightly weaker single-byte bias of $Z_3 = 131$.

Table 1 Identified and/or proved short-term keystream biases of RC4.

Bias in event	Type of bias	Discovered	Proved
Isolated short-term biases			
$Z_1 = 0$	Negative	[18]	[24]
$Z_1 = 1$	Negative	[24]	[24]
$Z_1 = 129$	Negative (16-byte key)	[1]	Open
$Z_2 = 0$	Positive	[17]	[17]
$Z_2 = 2$	Negative	[1, 22]	[22]
$Z_2 = 129$	Negative	[1, 22]	Open
$Z_2 = 172$	Positive	[1]	Open
$Z_3 = 131$	Positive	[1, 8]	[8]
$Z_4 = 2$	Positive	[1]	Open
$Z_{256} = 0$	Negative	[1, 8]	Open
$Z_{257} = 0$	Positive	[8]	Open
Patterns of short-term biases			
$Z_1 = v$	Sinusoidal ($v = 0, \ldots, 255$)	[18]	[24]
$Z_r = 0$	Positive ($r = 3, \ldots, N-1$)	[14]	[14]
$Z_r = r$	Positive ($r = 3, \ldots, N-1$)	[1, 8]	Open*
$Z_\ell = -\ell$	Positive (ℓ is the key-length)	[23]	[23, 24]
$Z_{x\ell} = -x\ell$	Positive (ℓ is the key-length)	[8]	Open**.

*This has been attempted in [8].
**Another proof of this has been presented in [9] very recently. However, we were not aware of [9] when we proved it during May 2013.

A consolidated account of the current state-of-the-art in terms of identified and/or proved short-term keystream biases of RC4 is presented in Table 1.1. Our motivation for this paper is to prove all "Open" (or partially proved) problems listed in Table 1.1. To prove the existing correlations in RC4, often researchers try to find several paths or a significant path that ends up in the biased relation. Then, they compute the probability of the path. Finding all such paths is not an easy task in practice in RC4. Since our theoretical estimates matches closely with the experimental data, we believe that we have been able to find all the influential paths towards the biases.

1.2 Contributions of our work

We can summarize the contributions of our work as follows.

- In Section 2, we prove all open isolated short-term single-byte keystream biases reported and exploited by AlFardan, Bernstein, Paterson, Poettering and Schuldt in their recent attack [1, 4] on the SSL/TLS protocol. This includes the biases in the events $Z_1 = 129$, $Z_2 = 129$, $Z_2 = 172$, $Z_4 = 2$, $Z_{256} = 0$ and $Z_{257} = 0$.
- There are some long-standing mysterious problem of "anomalies" in the distribution of the state array after the RC4 KSA, first pointed out in [15]. In this connection, we prove the anomaly in $S_0[128] = 127$ which has been open for more than a decade.

– In Section 4, we complete the proof for the extended key-length dependent biases in RC4, i.e., biases in the events $Z_{x\ell} = -x\ell$ for any positive integer x and key-length ℓ. This problem was attempted and partially solved by Isobe, Ohigashi, Watanabe and Morii in [8]. However, the proof was left incomplete which we settle here. Note that the particular case of $x = 1$ in this class of biases reduces to the key-length dependent biases of [24].

2 Proof of some isolated short-term biases

In this section, we prove all open isolated short-term biases of Table 1.1. We first list some existing results that will be needed in our proofs.

Proposition 1 *[15, Theorem 6.2.1] At the end of RC4 KSA, for* $0 \le u \le N-1$, $0 \le v \le N-1$,

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

Proposition 2 *[24, Lemma 1] After the first round of RC4 PRGA, for* $0 \le u \le N-1$, $0 \le v \le N-1$, *the probability* $\Pr(S_1[u] = v)$ *is:*

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

Proposition 3 *[24, Theorem 1] In RC4 PRGA, for* $3 \le u \le N-1$ *and* $0 \le v \le N-1$,

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

2.1 Proof of bias in $(Z_1 = 129)$

The negative bias in $Z_1 = 129$ was observed in [1, 4], but not in [18, 24]. While investigating this discrepancy, we first noticed that the length of the secret key used in the experiments of [1, 4] was consistently $\ell = 16$, whereas the same for [18, 24] had been different. This hinted that the bias in $Z_1 = 129$ may be key-length dependent. Our experiments revealed that the negative bias of $Z_1 = 129$ is prominent only when key-length ℓ is a non trivial divisor of N, i.e., when $\ell = 2, 4, 8, 16, 32, 64, 128$. For other key-lengths, $\Pr(Z_1 = 129) \approx 1/N$ except $\ell = 1$. For $\ell = 1$, we observed that Z_1 is always different from 129. This behavior is depicted in Figure 3.

Now we will justify these observations in Theorem 1.

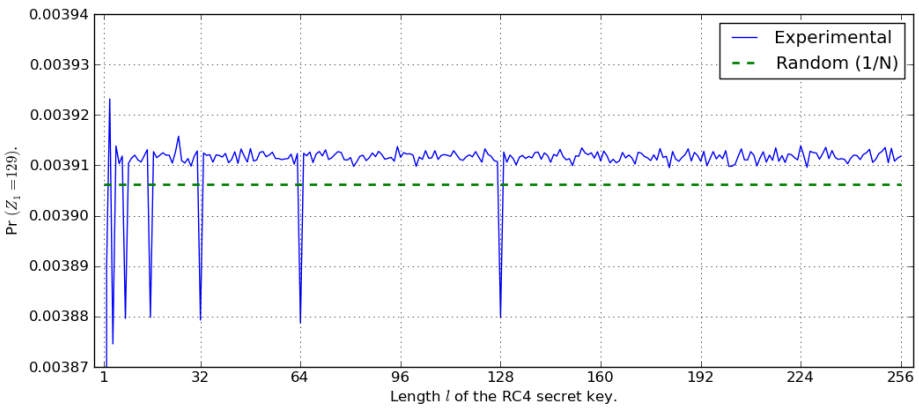

Fig. 3 Bias in the event $(Z_1 = 129)$ for key-length $1 \leq \ell \leq 256$.

Theorem 1 *In RC4 with* $N = 256$, $\Pr(Z_1 = 129) \approx 1/N - 1.73/N^2$ *when key-length is a non trivial divisor of* N.

Proof We consider three significant paths as follows.

P1. First consider the following negative path.

(a) Let $K[0] \neq 1, K[1] \neq N-1$ and $1 + K[0] + K[1] \neq 0$. This happens with probability $(\frac{N-1}{N})^3$.

(b) None of $j_1^K, \ldots, j_{\frac{N}{2}+x}^K$ is equal to $\frac{N}{2} + x$ for $x = 0, 1$. This happens with probability $(\frac{N-2}{N})^{\frac{N}{2}} \cdot (N-1)/N$.

(c) Note that as key-length ℓ divides $N/2$, $K[N/2] = K[0]$ and $K[N/2+1] = K[1]$, and so $j_{\frac{N}{2}+2}^K = j_{\frac{N}{2}}^K + K[0] + K[1] + 1$.

(d) Suppose $j_{\frac{N}{2}+2}^K < \frac{N}{2} + 1$. This happens with probability $\frac{N/2+1}{N}$.

(e) None of $j_{\frac{N}{2}+3}^K, \ldots, j_N^K$ will be equal to $j_{\frac{N}{2}+2}^K$. This happens with probability $\left(1 - \frac{1}{N}\right)^{\frac{N}{2}-2}$.

(f) There is an integer $T > \frac{N}{2} + 1$ such that none of $j_1^K, \ldots, j_T^K$ will touch T. Also none of $j_3^K, \ldots, j_T^K$ will touch 1. The associated probability is $(\frac{N-1}{N})^2 \cdot (\frac{N-2}{N})^{T-2}$.

(g) j_{T+1}^K is equal to 1 with probability $\frac{1}{N}$. Hence after swap we have $S_{T+1}^K[1] = T$ and $S_{T+1}^K[T] = 1 + K[0] + K[1]$.

(h) None of $j_{T+2}^K, \ldots, j_N^K$ is equal to 1 or T, with probability $(\frac{N-2}{N})^{N-T-1}$.

(i) So $S_0[1] = T$ and $S_0[T] = 1 + K[0] + K[1]$. Since by our condition $j_{\frac{N}{2}}^K \neq T$, we have $S_0[1] + S_0[T] = 1 + K[0] + K[1] + T \neq j_{\frac{N}{2}}^K + K[0] + K[1] + 1$. Also $S_1[j_{\frac{N}{2}}^K + K[0] + K[1] + 1] = \frac{N}{2} + 1$. Hence $Z_1 = S_1[T + 1 + K[0] + K[1]] \neq \frac{N}{2} + 1$.

Total probability of the above path P1 is approximately

$$\sum_{T=N/2+2}^{N-1} \left(1 - 1/N\right)^{3.5N-2} \cdot \frac{N/2+1}{N} \cdot \frac{1}{N} = \frac{1.92}{N}.$$

P2. Now consider the following positive path.

(a) Let $K[1] = N-1$ and $K[0] \neq 1$. Hence $j_2^K = K[0] + 1 + K[1] = K[0]$. So after second swap $S_2^K[1] = 0$. The probability of this is $1/N \cdot (N-1)/N$.

(b) None of $j_3^K, \ldots, j_N^K$ will be equal to 1. This happens with probability $(\frac{N-1}{N})^{N-2}$.
(c) None of $j_1^K, \ldots, j_{\frac{N}{2}}^K$ will be equal to $\frac{N}{2}$ or $\frac{N}{2}+1$. This happens with probability $(\frac{N-2}{N})^{\frac{N}{2}}$.
(d) $j_{\frac{N}{2}+1}^K$ will be equal to $\frac{N}{2}+1$ with probability $\frac{1}{N}$. Hence after swap we have $S_{\frac{N}{2}+1}^K[N/2] = N/2+1$ and $S_{\frac{N}{2}+1}^K[N/2+1] = N/2$.
(e) $j_{\frac{N}{2}+2}^K = j_{\frac{N}{2}+1}^K + S_{\frac{N}{2}+1}^K[N/2+1] + K[1] = N/2+1+N/2+N-1 = 0$. So $S_{\frac{N}{2}+2}^K[0] = N/2$.
(f) None of $j_{\frac{N}{2}+3}^K, \ldots, j_N^K$ will be equal to 0 or $N/2$ with probability $\left(1-\frac{2}{N}\right)^{\frac{N}{2}-2}$.
(g) Since by our conditions $S_0[0] = N/2, S_0[1] = 0$ and $S_0[N/2] = N/2+1$, Z_1 will be equal to $N/2+1$

Total probability of the above path P2 is approximately $\left(1-1/N\right)^{3N-5} \frac{1}{N^2} = \frac{0.05}{N^2}$

P3. Also take another event. P3$=\Big\{K[1] = N-2 \wedge j_1^K \neq N/2 \cdots \wedge j_{\frac{N}{2}}^K \neq N/2 \wedge j_1^K \neq N/2+1 \wedge \cdots \wedge j_{\frac{N}{2}}^K \neq N/2+1 \wedge j_{\frac{N}{2}+1}^K = 1 \wedge j_{\frac{N}{2}+3}^K \neq 1 \wedge \cdots \wedge j_N^K \neq 1 \wedge j_{\frac{N}{2}+3}^K \neq N/2 \wedge \cdots \wedge j_N^K \neq N/2\Big\}$.
It can be shown that if P3 holds, Z_1 will be always equal to $N/2+1$.
Now probability of P3 is approximately $\left(1-1/N\right)^{2N-3} \frac{1}{N^2} = \frac{0.14}{N^2}$.

Let us combine the aforesaid paths to obtain $\Pr(Z_1 = N/2+1)$ as

$$\begin{aligned}\Pr(Z_1 = N/2+1) &= \Pr(Z_1 = N/2+1 \mid \mathrm{P1}) \cdot \Pr(\mathrm{P1}) + \Pr(Z_1 = N/2+1 \mid \mathrm{P2}) \cdot \Pr(\mathrm{P2}) \\ &\quad + \Pr(Z_1 = N/2+1 \mid \mathrm{P3}) \cdot \Pr(\mathrm{P3}) \\ &\quad + \Pr(Z_1 = N/2+1 \mid \overline{\mathrm{P1} \vee \mathrm{P2} \vee \mathrm{P3}}) \cdot \Pr(\overline{\mathrm{P1} \vee \mathrm{P2} \vee \mathrm{P3}}) \\ &= 0 \cdot \frac{1.92}{N} + 1 \cdot \frac{0.05}{N^2} + 1 \cdot \frac{0.14}{N^2} + \left(1 - \frac{1.92}{N} - \frac{0.05}{N^2} - \frac{0.14}{N^2}\right) \cdot \frac{1}{N} \\ &= \frac{1}{N} - \frac{1.73}{N^2}\end{aligned}$$

□

2.2 Proof of bias in $(Z_2 = 129)$

We notice that the bias in $(Z_2 = 129)$ for $N = 256$ is a special case of the general bias in $(Z_2 = N/2+1)$ for any even value of N. We present the general result as follows.

Theorem 2 *In RC4 with $N = 256$,*

$$\Pr(Z_2 = 129) \approx \begin{cases} 1/N - 1.96/N^2, \textit{ when key-length } \ell \textit{ does not divide } N/2; \\ 1/N - 1.90/N^2, \textit{ when key-length } \ell \textit{ divided } N/2. \end{cases}$$

Proof **Part I**: First, we consider the case when the key-length l does not divide N/2.
We consider two mutually exclusive paths from the initial state S_0.

P1. Consider $S_0[2] = 0$ and $S_0[1] \neq 2$, with probability $1/N \cdot (N-1)/N$. From the analysis of Mantin and Shamir [17] for the bias in $(Z_2 = 0)$, we know that $Z_2 = 0$ in this situation. Thus, $Z_2 \neq N/2+1$.

P2. Consider $S_0[2] = N/2+1$ and $S_0[1] \neq 2$, with probability $1/N \cdot (N-1)/N$. After the first round, $j_1 = S_0[1] = X \neq 2$, and thus $S_1[2] = N/2+1$ and $S_1[X] = X$. In the second round, we get $j_2 = (N/2+1) + X$, and let us say $S_1[j_2] = S_1[(N/2+1)+X] = Z$. Since S_1 is a permutation, $X = S_1[X] \neq S_1[(N/2+1)+X] = Z$. After the swap in the second round, we get $Z_2 = S_2[(N/2+1)+Z] \neq S_2[(N/2+1)+X] = N/2+1$. Figure 4 illustrates the scenario.

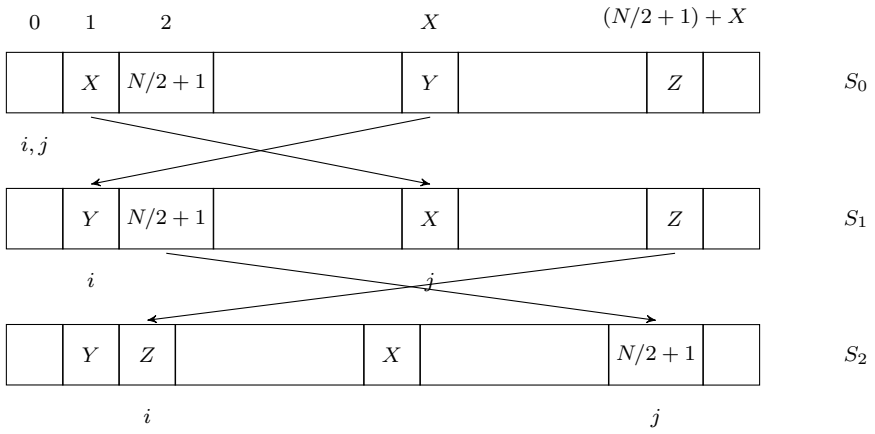

Fig. 4 The first two rounds of RC4 main cycle when $S_0[2] = N/2+1$ and $S_0[1] \neq 2$.

Let us denote the aforesaid mutually exclusive events as $A \doteq (S_0[2] = 0 \wedge S_0[1] \neq 2)$ and $B \doteq (S_0[2] = N/2+1 \wedge S_0[1] \neq 2)$ to obtain $\Pr(Z_2 = N/2+1)$ as

$$\begin{aligned}
&\Pr(Z_2 = N/2+1 \mid A) \cdot \Pr(A) + \Pr(Z_2 = N/2+1 \mid B) \cdot \Pr(B) \\
&\quad + \Pr(Z_2 = N/2+1 \mid \overline{A} \wedge \overline{B}) \cdot \Pr(\overline{A} \wedge \overline{B}) \\
&\approx 0 + 0 + \Pr(Z_2 = N/2+1 \mid \overline{A} \wedge \overline{B}) \cdot \\
&\quad \Big[1 - \big(\Pr(S_0[2] = 0) + \Pr(S_0[2] = N/2+1)\big) \cdot \Pr(S_0[1] \neq 2)\Big].
\end{aligned}$$

Assuming $\Pr(Z_2 = N/2+1 \mid \overline{A} \wedge \overline{B}) \approx 1/N$, and using the formula of Mantin [15], we get the desired probability as $\Pr(Z_2 = N/2+1) \approx 1/N - 1.96/N^2$.

Part II: Now we consider the case when the key-length ℓ divides $N/2$. Consider the following events:

- Let $K[0] \notin \{1, 2, 1+K[0]+K[1], 3+K[0]+K[1]+K[2]\}, 1+K[0]+K[1] \notin \{2, 3+K[0]+K[1]+K[2]\}$ with $K[2] = \frac{N}{2} - 2$. This happens with probability $\frac{N-4}{N} \cdot \frac{N-2}{N} \cdot \frac{1}{N}$.
- Due to the above conditions $S_2^K[1] = 1+K[0]+K[1]$ and $S_3^K[2] = 3+K[0]+K[1]+K[2] = 1+\frac{N}{2}+K[0]+K[1]$
- None of $j_4^K, \ldots, j_N^K$ is equal to 1 or 2. This happens with probability $(\frac{N-2}{N})^{(N-3)}$.
- Also none of $j_1^K, \ldots, j_{\frac{N}{2}+x}^K$ is equal to $\frac{N}{2}+x$ for $x = 1, 2$. This happens with probability $(1-\frac{2}{N})^{\frac{N}{2}+1} \cdot (1-\frac{1}{N})$.
- Since ℓ divides $N/2$, $K[N/2] = K[0]$ and $K[N/2+1] = K[1]$.

– Hence $j^K_{\frac{N}{2}+2} = j^K_{\frac{N}{2}+1} + K[1] + \frac{N}{2} + 1$. Also $j^K_{\frac{N}{2}+3} = j^K_{\frac{N}{2}+2} + \frac{N}{2} + 2 + K[2] = j^K_{\frac{N}{2}+2}$, since $K[2] = \frac{N}{2} - 2$. So after swap, we have $S^K_{\frac{N}{2}+3}[\frac{N}{2} + 2] = \frac{N}{2} + 1$.
– None of $j^K_{\frac{N}{2}+4}, \ldots, j^K_N$ is equal to $\frac{N}{2} + 2$. This occurs with probability $\left(1 - \frac{1}{N}\right)^{\frac{N}{2}-3}$
– Hence after KSA, we have $S_0[1] = 1 + K[0] + K[1], S_0[2] = 1 + \frac{N}{2} + K[0] + K[1]$ and $S_0[\frac{N}{2} + 2] = \frac{N}{2} + 1$.
– Now if $K[0]+K[1] = \frac{N}{4}$, $j_2 = 1+K[0]+K[1]+1+\frac{N}{2}+K[0]+K[1] = 2$. So $Z_2 = S_2[2S_2[2]] = S_2\big[2(1 + \frac{N}{2} + K[0] + K[1])\big] = S_2[\frac{N}{2} + 2] = \frac{N}{2} + 1$. Similarly if $K[0] + K[1] = \frac{3N}{4}$, Z_2 will be $\frac{N}{2} + 1$.

Above path holds with probability approximately $\left(1 - \frac{1}{N}\right)^{3.5N} \frac{2}{N^2} = \frac{0.06}{N^2}$. So when ℓ divides $N/2$, we have $\Pr(Z_2 = 129) \approx 1/N - 1.96/N^2 + 0.06/N^2 = 1/N - 1.90/N^2$. □

2.3 Proof of bias in $(Z_2 = 172)$

Theorem 3 *In RC4 with $N = 256$, $\Pr(Z_2 = 172) \approx 1/N + 0.16/N^2$.*

Proof We consider the following mutually exclusive paths from the initial state S_0.

P1. Consider $S_0[2] = 0$. If $S_0[1] \neq 2$, from the analysis of Mantin and Shamir [17] for the bias in $(Z_2 = 0)$, we know that $Z_2 = 0$ in this situation. Thus, $Z_2 \neq 172$. In case $S_0[1] = 2$, we may assume that $Z_2 = 172$ occurs with probability $\frac{1}{N-1}$ as in this case Z_2 will always be different from 2. Thus,

$$\Pr(Z_2 = 172 \mid S_0[2] = 0) \approx \frac{1}{N-1} \Pr(S_0[1] = 2).$$

P2. Consider $S_0[2] = 86$. In this case, we have the following sub-paths.
   (a) Consider $S_0[1] = 172$. In this case, $j_1 = S_0[1] = 172$ results in a swap to produce $S_1[172] = 172$, while $S_1[2] = 86$ remains untouched. In the next round, $j_2 = j_1 + S_1[2] = 172 + 86 = 258 = 2 = i_2$ ensures that there is no swap in the S-array. Thus, $Z_2 = S_2[S_2[i_2] + S_2[j_2]] = S_1[86 + 86] = S_1[172] = 172$. Note that this path is possible for any X in $S_0[1] = X$ and $S_0[2] = X/2$, and if $X + X/2 = 2$. Thus, this path results in the modular equation $3X \equiv 4 \bmod N$, which has a unique solution $X = 172$ for $N = 256$.
   (b) Consider $S_0[1] \neq 172$ and $S_0[S_0[1] + 86] = 172$. In the first round, $S_1[2] = 86$ remains untouched, and $j_2 = j_1+S_1[2] = S_0[1]+86$ results in a swap to produce $S_2[2] = S_1[j_2] = S_1[S_0[1]+86] = S_0[S_0[1]+86] = 172$ and $S_2[S_0[1]+86] = 86$. Thus, in the second round, we get $Z_2 = S_2[S_2[i_2] + S_2[j_2]] = S_2[172 + 86] = S_2[2] = 172$. Figure 5 illustrates the scenario.

   Let us denote the aforesaid events as $B = (S_0[2] = 86)$, $C = (S_0[1] = 172)$, and $D = (S_0[S_0[1] + 86] = 172)$. This results in

$$\begin{aligned}
&\Pr(Z_2 = 172 \mid S_0[2] = 86) = \Pr(Z_2 = 172 \mid B)\\
&\approx \Pr(Z_2 = 172 \mid B \wedge C) \cdot \Pr(C) + \Pr(Z_2 = 172 \mid B \wedge \overline{C}) \cdot \Pr(\overline{C})\\
&\approx 1 \cdot \Pr(S_0[1] = 172) + \big(\Pr(Z_2 = 172 \mid B \wedge \overline{C} \wedge D) \cdot \Pr(D)\\
&\qquad + \Pr(Z_2 = 172 \mid B \wedge \overline{C} \wedge \overline{D}) \cdot \Pr(\overline{D})\big) \cdot (1 - \Pr(S_0[1] = 172))\\
&\approx \Pr(S_0[1] = 172) + \left(1 \cdot \frac{1}{N} + \frac{1}{N} \cdot \big(1 - \frac{1}{N}\big)\right) \cdot (1 - \Pr(S_0[1] = 172)).
\end{aligned}$$

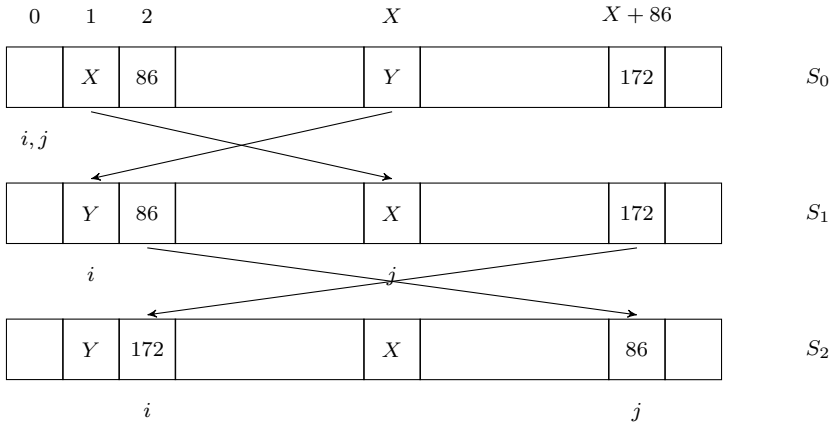

Fig. 5 The first two rounds of RC4 main cycle when $S_0[2] = 86$, $S_0[1] \neq 2, 172$ and $S_0[S_0[1] + 86] = 172$.

P3. Consider $S_0[2] = 172$. In this situation, $Z_2 = 172$ if and only if $S_0[1] = 2$ and $S_0[4] = N-1$, and in all other cases, $Z_2 \neq 172$. Thus, $\Pr(Z_2 = 172 \mid S_0[2] = 172) = \Pr(S_0[1] = 2 \wedge S_0[4] = N-1)$.

Let us combine the aforesaid paths to obtain $\Pr(Z_2 = 172)$ as

$$\begin{aligned}
&\Pr(Z_2 = 172 \mid S_0[2] = 0) \cdot \Pr(S_0[2] = 0) + \Pr(Z_2 = 172 \mid S_0[2] = 86) \cdot \Pr(S_0[2] = 86) \\
&\quad + \Pr(Z_2 = 172 \mid S_0[2] = 172) \cdot \Pr(S_0[2] = 172) \\
&\quad + \frac{1}{N}\Big(1 - \Pr(S_0[2] = 0) - \Pr(S_0[2] = 86) - \Pr(S_0[2] = 172)\Big) \\
&\approx \frac{1}{N-1} \Pr(S_0[1] = 2) \cdot \Pr(S_0[2] = 0) \\
&\quad + \left[\Pr(S_0[1] = 172) + \left(\frac{2}{N} - \frac{1}{N^2}\right) \cdot (1 - \Pr(S_0[1] = 172))\right] \cdot \Pr(S_0[2] = 86) \\
&\quad + \Pr(S_0[1] = 2 \wedge S_0[4] = N-1) \cdot \Pr(S_0[2] = 172).
\end{aligned}$$

In the above equation, computing the probability terms involving S_0 using the formula of Mantin [15], we get $\Pr(Z_2 = 172) \approx 1/N + 0.16/N^2$. □

2.4 Proof of bias in $(Z_4 = 2)$

Theorem 4 *In RC4 with* $N = 256$, $\Pr(Z_4 = 2) \approx 1/N + 0.83/N^2$.

Proof First we discuss a path P1 in which $Z_4 \neq 2$.
Let $K[0..y]$ denote the sum $K[0] + K[1] + \cdots + K[y] + y(y+1)/2$.

– Let $K[0] \notin \Big\{1, 2, 3, 4, K[0..1], K[0..2], K[0..3], K[0..4]\Big\}$,
$K[0..1] \notin \Big\{0, 2, 3, 4, K[0..2], K[0..3], K[0..4]\Big\}$,
$K[0..2] \notin \Big\{0, 1, 3, 4, K[0..3], K[0..4]\Big\}$,

$K[0..3] \notin \Big\{0, 1, 2, 4, K[0..4]\Big\}$,

$K[0..4] \notin \Big\{0, 1, 2, 3\Big\}$.

This happens with probability $\frac{N-8}{N} \cdot \frac{N-7}{N} \cdot \frac{N-6}{N} \cdot \frac{N-5}{N} \cdot \frac{N-4}{N}$.

- Due to the above conditions $S_2^K[1] = 1 + K[0] + K[1], S_4^K[3] = 6 + K[0] + K[1] + K[2] + K[3], S_5^K[4] = 10 + K[0] + K[1] + K[2] + K[3] + K[4]$.
- None of $j_6^K, \ldots, j_N^K$ should be equal to 1 or 4. This occurs with probability $\left(1 - \frac{2}{N}\right)^{N-5}$
- Hence we have $S_0[1] \neq 2$ and $S_0[4] \neq 2$
- Now if $S_4[4] = 2$, then $Z_4 \neq 2$ as $j_4 \neq 4$.

Thus, $\Pr(\text{P1}) = \big(1 - 1/N\big)^{30}\big(1 - 1/N\big)^{2N-10}\frac{1}{N} = \big(1 - 1/N\big)^{2N+20}\frac{1}{N}$.

If P1 does not happen, then Z_4 may be equal to 2 in two mutually exclusive ways: along with $j_4 = 4$ or with $j_4 \neq 4$

Case $j_4 = 4$. $Z_4 = S_4[S_4[4] + S_4[j_4]] = S_4[2 \cdot S_4[4]]$. We may further consider some sub-paths within this case.

1. $S_4[4] = 2$ gives $Z_4 = S_4[4] = 2$ with probability 1. However, the event $(S_4[4] = 2 \mid j_4 = 4)$ occurs with probability more than $1/N$, as follows.
   (a) If $S_0[1] = 2$ and $S_0[3] = N-2$, it can be shown that we always have $S_4[4] = 2, j_4 = 4$.
   (b) If $S_0[1] = 2$ and $S_0[3] \neq N-2$, it can be shown that $S_4[4] = 2, j_4 = 4$ can not occur simultaneously.
   (c) If $S_0[1] \neq 2$ and $S_0[3] = N-2$, it can be shown that $S_4[4] = 2, j_4 = 4$ occur if and only if $S_0[1] = 3, S_0[2] = N-4$ and $S_0[4] = 2$.
   (d) Consider $S_0[1] \neq 2$ and $S_0[3] \neq N-2$. Now if $S_0[4] \neq 2$, $\Big(S_4[4] = 2, j_4 = 4\Big)$ can not occur simultaneously.
      i. If $S_0[4] = 2$ and $S_0[3] = N-1$, $\Big(S_4[4] = 2, j_4 = 4\Big)$ can occur if and only if $S_0[1] = 3, S_0[2] = N-4$.
      ii. Let $S_0[4] = 2$ and $S_0[3] \neq N-1$. If any one j_1, j_2, j_3 become 4, then the event $\Big(S_4[4] = 2, j_4 = 4\Big)$ can not occur simultaneously. Hence we need $j_1 \neq 4, j_2 \neq 4$ and $j_3 \neq 4$.

   Hence,

$$\begin{aligned}\Pr(S_4[4] = 2 \wedge\ j_4 = 4 \mid \overline{\text{P1}}) \approx\ & \Pr(S_0[1] = 2)\Pr(S_0[3] = N-2) + \\ & (1 - \Pr(S_0[1] = 2)\Pr(S_0[3] = N-2)\Pr(S_0[1] = 3)\Pr(S_0[2] = N-4) \\ & \Pr(S_0[4] = 2) + \big(1 - \Pr(S_0[1] = 2)\big)\big(1 - \Pr(S_0[3] = N-2)\big)\Pr(S_0[4] = 2) \\ & \Big(\Pr(S_0[3] = N-1)\Pr(S_0[1] = 3)\Pr(S_0[2] = N-4) + \\ & (1 - \Pr(S_0[3] = N-1))\left(1 - \frac{1}{N}\right)^3\frac{1}{N}\Big) \approx \frac{1.98}{N^2}\end{aligned}$$

   Considering $\Pr(j_4 = 4) = \frac{1}{N}$, we get $\Pr(S_4[4] = 2 \mid j_4 = 4 \wedge \overline{\text{P1}}) \approx \frac{1.98}{N}$.
   Hence we have

$$\Pr(Z_4 = 2 \wedge S_4[4] = 2 \mid j_4 = 4 \wedge \overline{\text{P1}}) \approx \frac{1.98}{N}.$$

2. $S_4[4] = N/2 + 2$ gives $Z_4 = S_4[N+4] = S_4[4] = N/2 + 2 \neq 2$. So,

$$\Pr(Z_4 = 2 \wedge S_4[4] = N/2 + 2 \mid j_4 = 4 \wedge \overline{\text{P1}}) = 0.$$

3. Now let $S_4[4] \neq 2, N/2+2$. In this situation if $S_0[1] = 2$, Z_4 will be always different from 2. Also, $\Pr(S_4[4] \neq 2, N/2+2, S_0[1] \neq 2 \mid j_4 = 4 \wedge \overline{\mathrm{P1}})$
$\approx \Pr(S_0[1] \neq 2)\left(1 - \frac{1}{N}\right)\left(1 - \frac{1.98}{N}\right) \approx \frac{252}{N}$.
So, $\Pr(Z_4 = 2 \wedge S_4[4] \neq 2, N/2+2 \mid j_4 = 4 \wedge \overline{\mathrm{P1}}) \approx \frac{252}{N^2} \approx \frac{0.98}{N}$.

Combining all the sub-paths mentioned above, we get $\Pr(Z_4 = 2 \wedge j_4 = 4 \mid \overline{\mathrm{P1}})$ as

$$\begin{aligned}
&\Pr(Z_4 = 2 \wedge S_4[4] = 2 \mid j_4 = 4 \wedge \overline{\mathrm{P1}}) \cdot \Pr(j_4 = 4) \\
&\quad + \Pr(Z_4 = 2 \wedge S_4[4] = N/2+2 \mid j_4 = 4 \wedge \overline{\mathrm{P1}}) \cdot \Pr(j_4 = 4) \\
&\quad + \Pr(Z_4 = 2 \wedge S_4[4] \neq 2, N/2+2 \mid j_4 = 4 \wedge \overline{\mathrm{P1}}) \cdot \Pr(j_4 = 4) \\
&= (1.98/N) \cdot (1/N) + 0 + (0.98/N) \cdot (1/N) \approx \frac{2.96}{N^2}.
\end{aligned}$$

Case $j_4 \neq 4$. We have $Z_4 = S_4[S_4[4] + S_4[j_4]] = S_4[S_4[4] + X]$, where $X = S_4[j_4] \neq S_4[4]$, say. Here we may consider two sub-paths, as follows.

1. $S_4[4] = 2$ gives $Z_4 = S_4[2 + X] \neq S_4[4] = 2$, as $X = S_4[j_4] \neq S_4[4] = 2$ for $j_4 = 4$. Thus, $\Pr(Z_4 = 2 \wedge S_4[4] = 2 \mid j_4 \neq 4 \wedge \overline{\mathrm{P1}}) = 0$.
2. Assuming $S_4[4] \neq 2$ to be uniformly distributed, we get $Z_4 = 2$ with probability $\frac{1}{N}$. Thus, $\Pr(Z_4 = 2 \wedge S_4[4] \neq 2 \mid j_4 \neq 4 \wedge \overline{\mathrm{P1}}) \approx 1/N \cdot (1 - 1/N) = (1/N - 1/N^2)$.

Combining the sub-paths mentioned above, we have

$$\begin{aligned}
\Pr(Z_4 = 2 \wedge j_4 \neq 4 \mid \overline{\mathrm{P1}}) &\approx \Pr(Z_4 = 2 \wedge S_4[4] = 2 \mid j_4 \neq 4 \wedge \overline{\mathrm{P1}}) \cdot \Pr(j_4 \neq 4) \\
&\quad + \Pr(Z_4 = 2 \wedge S_4[4] \neq 2 \mid j_4 \neq 4 \wedge \overline{\mathrm{P1}}) \cdot \Pr(j_4 \neq 4) \\
&= 0 + (1/N - 1/N^2) \cdot (1 - 1/N) = 1/N - 2/N^2 + 1/N^3.
\end{aligned}$$

Adding the contributions from the two mutually exclusive paths above, we get

$$\begin{aligned}
\Pr(Z_4 = 2 \mid \overline{\mathrm{P1}}) &= \Pr(Z_4 = 2 \wedge j_4 = 4 \mid \overline{\mathrm{P1}}) + \Pr(Z_4 = 2 \wedge j_4 \neq 4 \mid \overline{\mathrm{P1}}) \\
&\approx \frac{2.96}{N^2} + \frac{1}{N} - \frac{2}{N^2} = 1/N + 0.96/N^2.
\end{aligned}$$

Hence we get overall

$$\begin{aligned}
\Pr(Z_4 = 2) &= \Pr(\mathrm{P1}) \Pr(Z_4 = 2 \mid \mathrm{P1}) + (1 - \Pr(\mathrm{P1})) \Pr(Z_4 = 2 \mid \overline{\mathrm{P1}}) \\
&= 0 + \left(1 - \left(1 - 1/N\right)^{2N+20} \frac{1}{N}\right) \cdot \left(\frac{1}{N} + \frac{0.96}{N^2}\right) \\
&= 1/N + 0.83/N^2.
\end{aligned}$$

□

2.5 Proof of bias in $(Z_{256} = 0)$

Theorem 5 *In RC4 with $N = 256$, $\Pr(Z_N = 0) \approx 1/N - 0.37/N^2$.*

Proof Let us consider the following two paths.

P1. Consider $S_1[0] = 0$. In this case, if $j_2, \ldots, j_{N-1}$ are all non zero, then one can check that $Z_N \neq 0$. In all other cases, one may assume $\Pr(Z_N = 0 \mid S_1[0] = 0) \approx 1/N$. Thus, $\Pr(Z_N = 0 \mid S_1[0] = 0) \approx \left(1 - (1 - 1/N)^{N-2}\right) \cdot (1/N)$.

P2. Consider $S_1[0] \neq 0$. In this case, we may again consider the following sub-paths, depending on the state S_{N-3}.

$$\begin{aligned}
&\Pr(Z_N = 0 \mid S_1[0] \neq 0)\\
&= \Pr(Z_N = 0 \mid S_1[0] \neq 0 \wedge S_{N-3}[0] = 0) \cdot \Pr(S_{N-3}[0] = 0 \mid S_1[0] \neq 0)\\
&\quad + \Pr(Z_N = 0 \mid S_1[0] \neq 0 \wedge S_{N-3}[N-2] = 0) \cdot \Pr(S_{N-3}[N-2] = 0 \mid S_1[0] \neq 0)\\
&\quad + \Pr(Z_N = 0 \mid S_1[0] \neq 0 \wedge S_{N-3}[N-1] = 0) \cdot \Pr(S_{N-3}[N-1] = 0 \mid S_1[0] \neq 0)\\
&\quad + \sum_{x=1}^{N-3} \Pr(Z_N = 0 \mid S_1[0] \neq 0 \wedge S_{N-3}[x] = 0) \cdot \Pr(S_{N-3}[x] = 0 \mid S_1[0] \neq 0).
\end{aligned}$$

(a) If $S_{N-3}[0] = 0$ and $j_{N-2}, j_{N-1} \neq 0$, we have $S_{N-1}[0] = 0$, which implies $j_N = j_{N-1}$ and $S_{N-1}[j_{N-1}] \neq j_{N-1}$. Thus, $Z_N = S_N[S_{N-1}[j_N] + S_{N-1}[0]] = S_N[S_{N-1}[j_{N-1}]] \neq S_N[j_{N-1}] = S_N[j_N] = S_{N-1}[0] = 0$. Thus for $Z_N = 0$, we must have either $j_{N-2} = 0$ or $j_{N-1} = 0$ in this case, and in each case, $Z_N = 0$ may be assumed to occur with probability $1/N$. Hence $\Pr(Z_N = 0 \mid S_1[0] \neq 0 \wedge S_{N-3}[0] = 0) \approx 2/N^2$.

(b) If $S_{N-3}[N-2] = 0$ and $j_{N-2} = 0$, we have $S_{N-2}[0] = 0$ and $j_{N-1} = S_{N-2}[N-1] \neq 0$. Thus, $S_{N-1}[0] = 0$ and $j_N = j_{N-1}$, which gives $Z_N = S_N[S_{N-1}[0] + S_{N-1}[j_N]] = S_N[S_{N-1}[j_{N-1}]] = S_N[S_{N-2}[N-1]] = S_N[j_{N-1}] = S_N[j_N] = S_{N-1}[0] = 0$. So, $\Pr(Z_N = 0 \mid S_1[0] \neq 0 \wedge S_{N-3}[N-2] = 0 \wedge j_{N-2} = 0) = 1$. On the other hand, if $S_{N-3}[N-2] = 0$ and $j_{N-2} \neq 0$, then $Z_N \neq 0$ where $j_{N-1} \neq 0$ and $S_{N-1}[j_N] = 0$, and due to randomness assumption, $Z_N = 0$ in all other cases. So, $\Pr(Z_N = 0 \mid S_1[0] \neq 0 \wedge S_{N-3}[N-2] = 0 \wedge j_{N-2} \neq 0) \approx 1/N - 1/N^2$. Combining the two items as above, we get

$$\Pr(Z_N = 0 \mid S_1[0] \neq 0 \wedge S_{N-3}[N-2] = 0) \approx 2/N - 2/N^2.$$

(c) Similarly for $S_{N-3}[N-1] = 0$, it can be proved that $\Pr(Z_N = 0 \mid S_1[0] \neq 0 \wedge S_{N-3}[N-1] = 0) \approx 2/N - 2/N^2$.

(d) Now consider the case $S_{N-3}[x] = 0$ for $1 \leq x \leq N-3$. If $j_{N-2} \neq x$, $j_{N-1} \neq x$ and $j_N = x$, one can verify that $Z_N \neq 0$. In all other cases, $Z_N = 0$ may be assumed to occur with probability $1/N$. Thus for $1 \leq x \leq N-3$, $\Pr(Z_N = 0 \mid S_1[0] \neq 0 \wedge S_{N-3}[x] = 0) \approx 1/N - 1/N^2$.

Now, let us consider the conditional events $(S_{N-3}[x] = 0 \mid S_1[0] \neq 0)$, for $0 \leq x \leq N-1$, to complete the picture. Starting with $S_1[0] \neq 0$, if $j_2, \ldots, j_{N-3}$ are all non zero, we have $S_{N-3}[0] \neq 0$ as well. So, $\Pr(S_{N-3}[0] = 0 \mid S_1[0] \neq 0) = \left(1 - (1-1/N)^{N-4}\right) \cdot (1/N) = P_A$, say. For all $x \neq 0$, we may now assume

$$\Pr(S_{N-3}[x] = 0 \mid S_1[0] \neq 0) \approx (1 - P_A)/(N-1) = P_B.$$

Taking into account the contributions from all four sub-cases within this path, we get

$$\begin{aligned}
\Pr(Z_N = 0 \mid S_1[0] \neq 0) &= (2/N^2) \cdot P_A + (2/N - 2/N^2) \cdot P_B\\
&\quad + (2/N - 2/N^2) \cdot P_B + (1/N - 1/N^2) \cdot (1 - P_A - 2P_B)\\
&= (1/N - 1/N^2) - (1/N - 3/N^2) \cdot P_A + (2/N - 2/N^2) \cdot P_B.
\end{aligned}$$

Combining the above two paths, we get $\Pr(Z_N = 0)$ as

$$\begin{aligned}
&\Pr(Z_N = 0 \mid S_1[0] = 0) \cdot P(S_1[0] = 0) + \Pr(Z_N = 0 \mid S_1[0] \neq 0) \cdot P(S_1[0] \neq 0)\\
&\approx \left(1 - (1-1/N)^{N-2}\right) \cdot (1/N) \cdot (2/N) + ((1/N - 1/N^2) - (1/N - 3/N^2) \cdot P_A\\
&\quad + (2/N - 2/N^2) \cdot P_B) \cdot (1 - 2/N) \approx 1/N - 0.37/N^2,
\end{aligned}$$

for $N = 256$, as in the case with RC4. □

2.6 Proof of bias in $(Z_{257} = 0)$

Theorem 6 *In RC4 with $N = 256$, $\Pr(Z_{N+1} = 0) \approx 1/N + 0.36/N^2$.*

Proof We may write $Z_{N+1} = S_{N+1}[S_N[1] + S_N[j_{N+1}]]$, and consider the following two paths.

P1. Consider the case $S_N[1] = 1$, where we may write $Z_{N+1} = S_{N+1}[1 + S_N[j_{N+1}]]$. If $S_N[j_{N+1}] = 0$, we have $Z_{N+1} = S_{N+1}[1] = S_N[j_{N+1}] = 0$. Otherwise if $S_N[j_{N+1}] = X \neq 0$, we have $Z_{N+1} = S_{N+1}[1 + X] = 0$ is assumed to be uniformly distributed. Let us denote events $A \doteq (S_N[1] = 1)$ and $B \doteq (S_N[j_{N+1}] = 0)$ to get

$$\begin{aligned}\Pr(Z_{N+1} = 0 \mid A) &\approx \Pr(Z_{N+1} = 0 \mid A \wedge B) \cdot \Pr(B) + \Pr(Z_{N+1} = 0 \mid A \wedge \overline{B}) \cdot \Pr(\overline{B}) \\ &\approx 1 \cdot (1/N) + (1/N) \cdot (1 - 1/N) = 2/N - 1/N^2.\end{aligned}$$

P2. Consider the case $S_N[1] = X \neq 1$. Here we have $Z_{N+1} = S_{N+1}[X + S_N[j_{N+1}]]$. If $S_N[j_{N+1}] = 0$, we will get $Z_{N+1} = S_{N+1}[X] \neq S_{N+1}[1] = S_N[j_{N+1}] = 0$. Otherwise, for $S_N[j_{N+1}] = Y \neq 0$, we assume that $Z_{N+1} = S_{N+1}[X + Y] = 0$ is uniformly distributed. Let us denote events $A \doteq (S_N[1] = 1)$ and $B \doteq (S_N[j_{N+1}] = 0)$ to get

$$\begin{aligned}\Pr(Z_{N+1} = 0 \mid \overline{A}) &\approx \Pr(Z_{N+1} = 0 \mid \overline{A} \wedge B) \cdot \Pr(B) + \Pr(Z_{N+1} = 0 \mid \overline{A} \wedge \overline{B}) \cdot \Pr(\overline{B}) \\ &\approx 0 + (1/N) \cdot (1 - 1/N) = 1/N - 1/N^2.\end{aligned}$$

From [24, Theorem 1], we have $\Pr(S_N[1] = 1) \approx 0.00532$ when $N = 256$. Thus,

$$\begin{aligned}\Pr(Z_{N+1} = 0) &= \Pr(Z_{N+1} = 0 \mid A) \cdot \Pr(A) + \Pr(Z_{N+1} = 0 \mid \overline{A}) \cdot \Pr(\overline{A}) \\ &\approx (2/N - 1/N^2) \cdot (0.00532) + (1/N - 1/N^2) \cdot (1 - 0.00532) \\ &\approx 1/N + 0.36/N^2,\end{aligned}$$

for $N = 256$, as in the case with RC4. □

3 Proof of the anomaly in $S_0[128] = 127$

Our experiments with the specific key-lengths $\ell = 2, 4, \ldots, 128$ revealed that there exists a negative bias in $S_0[128] = 127$ for these key-lengths. Figure 6 shows the key-length dependence of this bias. This bias had been pointed out quite a few years ago [15, 20] as an "anomaly" in the otherwise smooth distribution of $S_0[u] = v$, but it was never observed as a key-length dependent phenomenon.

This is the motivation why we got interested in analyzing the $S_0[128] = 127$ anomaly. We prove it in this section. We will require the following technical results to prove the main theorem later.

Lemma 1 *In RC4 with $N = 256$, for $1 \leq r \leq N$, $\Pr(S^K_{r-1}[r] = r) \approx 1/N + (1 - 1/N)^r$.*

Proof We know that S^K_0 is the identity permutation of $\{0, \ldots, N-1\}$, and thus $S^K_0[r] = r$. This value will remain at the same index till round $(r-1)$ if none of $j^K_1, j^K_2, \ldots, j^K_{r-1}$ touches the index r, which occurs with probability $(1 - 1/N)^{r-1}$, or otherwise with uniform probability of $1/N$. Hence, we get $\Pr(S^K_{r-1}[r] = r) \approx (1 - 1/N)^{r-1} \cdot 1 + (1 - (1 - 1/N)^{r-1}) \cdot (1/N) = 1/N + (1 - 1/N)^r$. □

Lemma 2 *In RC4 with $N = 256$, $\Pr(S^K_{127}[128] = -K[128]) \approx 0.39/N$ if and only if ℓ, the length of the RC4 secret key, is a non trivial divisor of N.*

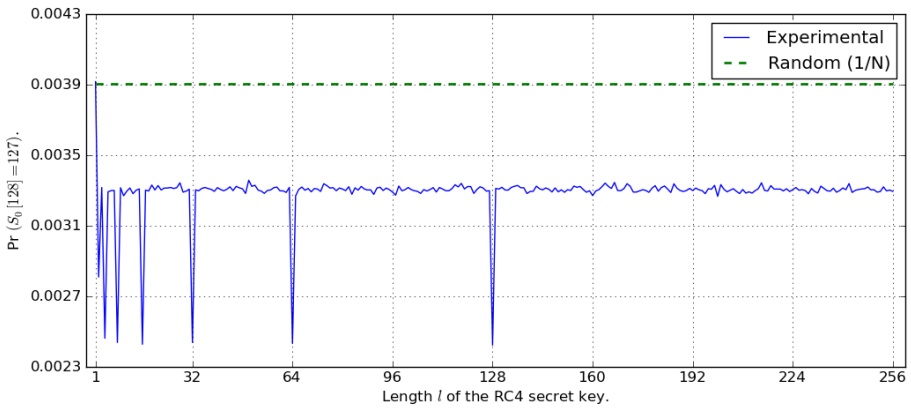

Fig. 6 Bias in the event $(S_0[128] = 127)$ for key-length $1 \le \ell \le 256$.

Proof Let us consider the following two paths.

P1. Consider $S_{127}^K[128] = 128$. In this case, we surely require $K[128] = -128 = 128$ (modulo $N = 256$). Now, if $\ell = 2, 4, \ldots, 128$, then $K[128] = K[0] = 128$. This implies $j_1^K = j_0^K + S_0^K[0] + K[0] = 0+0+128 = 128$, which in turn results in $S_1^K[0] = 128$ and $S_1^K[128] = 0$ after swap in the first round. As i^K does not touch index locations 0 or 128 during rounds 2 to 127, we can not have $S_{127}^K[128] = 128$, a contradiction. If ℓ does not divide 128, then $K[128]$ may not be equal to $K[0]$, and in this case $S_{127}^K[128] = 128$ may occur with probability $1/N$. In summary, $\Pr(S_{127}^K[128] = -K[128] \mid S_{127}^K[128] = 128) = 0$ if $\ell = 2, 4, \ldots, 128$. Otherwise, $\Pr(S_{127}^K[128] = -K[128] \mid S_{127}^K[128] = 128) \approx 1/N$.

P2. In case $S_{127}^K[128] \neq 128$, there is no special behavior dependent on the key-length ℓ, and we may assume that $\Pr(S_{127}^K[128] = -K[128] \mid S_{127}^K[128] \neq 128) \approx 1/N$.

Combining the two paths, we get

$$\begin{aligned} & \Pr(S_{127}^K[128] = -K[128]) \\ = \; & \Pr(S_{127}^K[128] = -K[128] \mid S_{127}^K[128] = 128) \cdot \Pr(S_{127}^K[128] = 128) \\ & + \Pr(S_{127}^K[128] = -K[128] \mid S_{127}^K[128] \neq 128) \cdot \Pr(S_{127}^K[128] = 128) \\ \approx \; & 0 \cdot (156/N) + (1/N) \cdot (1 - 156/N) \approx 0.39/N, \end{aligned}$$

if $\ell = 2, 4, \ldots, 128$, where $\Pr(S_{127}^K[128] = 128) \approx 156/N$ is by Lemma 1 with $r = 128$. For all other values of ℓ, we get $\Pr(S_{127}^K[128] = -K[128]) \approx (1/N)\cdot(156/N)+(1/N)\cdot(1-156/N) = 1/N$. □

Theorem 7 *In RC4 with $N = 256$, $\Pr(S_0[128] = S_N^K[128] = 127) \approx 0.62/N$ if and only if ℓ, the length of the RC4 secret key, is a non trivial divisor of N.*

Proof Let us first compute $\Pr(S_{128}^K[128] = 127)$, using the following paths.

P1. Consider $S_{127}^K[128] = -K[128]$. In this case, $j_{128} = j_{127} + S_{127}^K[128] + K[128] = j_{127}$. So, $S_{128}^K[128] = S_{127}^K[j_{128}] = S_{127}^K[j_{127}] = S_{126}^K[127]$. Now, by Lemma 1 with $r = 127$, we get $\Pr(S_{126}^K[127] = 127) \approx 156/N$. Thus, $\Pr(S_{128}^K[128] = 127 \mid S_{127}^K[128] = -K[128]) \approx 156/N$.

P2. Consider $S_{127}^K[128] \neq -K[128]$. In this case, $S_{128}^K[128] = S_{126}^K[X]$ for some $X \neq 127$. Thus by normalization over the probability values $\Pr(S_{126}^K[X] = 127)$ for $X \neq 127$, we get $\Pr(S_{128}^K[128] = 127 \mid S_{127}^K[128] \neq -K[128]) \approx (1 - 156/N)/(N-1) \approx 0.39/N$.

Combining the two paths as above, we get

$$\begin{aligned}
&\Pr(S_{128}^K[128] = 127) \\
&= \Pr(S_{128}^K[128] = 127 \mid S_{127}^K[128] = -K[128]) \cdot \Pr(S_{127}^K[128] = -K[128]) \\
&\quad + \Pr(S_{128}^K[128] = 127 \mid S_{127}^K[128] \neq -K[128]) \cdot \Pr(S_{127}^K[128] \neq -K[128]) \\
&\approx (156/N) \cdot (0.39/N) + (0.39/N) \cdot (1 - 0.39/N) \approx 0.63/N,
\end{aligned}$$

if $\ell = 2, 4, \ldots, 128$. For all other values of ℓ, we get $\Pr(S_{128}^K[128] = 127) \approx (156/N) \cdot (1/N) + (0.39/N) \cdot (1 - 1/N) \approx 1/N$. In both cases, the value of $\Pr(S_{127}^K[128] = -K[128])$ comes from Lemma 2.

Once we have $S_{128}^K[128] = 127$, we know that $S_0[128] = S_N^K[128] = 127$ if none of $j_{129}, \ldots, j_N$ touches the index 128. If otherwise $S_{128}^K[128] \neq 127$ and the value 127 is in any index less than 128, then $S_N^K[128] \neq 127$. If $S_{128}^K[128] \neq 127$ and the value 127 is in any index I greater than 128, then $S_N^K[128] = 127$ may occur by one step due to the following association.

1. Indices $j_{129}, \ldots, j_{I-1}$ do not touch location I before $i = I$.
2. When $i = I$, we have j equal to 128, so that the appropriate swap occurs.
3. Moreover, none of $j_{I+1}, \ldots, j_N$ touches the location 128 after the previous event.

Similarly if $S_{128}^K[128] \neq 127$ and the value 127 is in any index I greater than 128, then $S_N^K[128] = 127$ may occur by more than one steps.

Thus, the probability of the above path is
$\sum_{I=129}^{N} \Pr(S_{128}^K[I] = 127) \cdot \frac{1}{N} \cdot (1 - \frac{1}{N})^{127} + \sum_{I=129}^{N} \sum_{Y=I+1}^{N} \Pr(S_{128}^K[I] = 127) \cdot \frac{1}{N^2} \cdot (1 - \frac{1}{N})^{127} + \cdots$
$\approx \Pr(S_{128}^K[I] = 127) \cdot (1 - 1/N)^{127} \cdot (\frac{1}{2} + \frac{1}{8} + \frac{1}{48}) = 0.393 \cdot \Pr(S_{128}^K[I] = 127)$.

Note that $\Pr(S_{128}^K[I] = 127)$ will not be $\frac{1}{N}$ for $129 \leq I \leq N-1$. Since if any one of $j_1, \ldots, j_{127}$ is equal to 127, then $\Pr(S_{128}^K[I] = 127) = 0$. Hence $\Pr(S_{128}^K[I] = 127) = (1 - \frac{1}{N})^{127} \frac{1}{N} = \frac{0.61}{N}$.

Thus,

$$\begin{aligned}
\Pr(S_N^K[128] = 127) &= \Pr(S_{128}^K[128] = 127) \cdot \big(1 - \frac{1}{N}\big)^{128} + \Pr(S_{128}^K[128] \neq 127) \cdot 0.393 \cdot \frac{0.61}{N} \\
&\approx (0.63/N) \cdot (155/N) + (1 - 0.63/N) \cdot (0.24/N) \approx 0.62/N,
\end{aligned}$$

if $\ell = 2, 4, \ldots, 128$. For other values of ℓ, we get $\Pr(S_0[128] = S_N^K[128] = 127)$ following the value predicted by the distribution of $S_0[u] = v$ by Mantin [15, 17]. Hence the "anomaly". □

The theoretical results regarding the anomaly in $S_0[128] = 127$, as above, closely match with the experimental results, both from our own experiments, as well as that reported in the literature [20]. This hints at the possibility that all "anomalies" or deviations of probabilities in the distribution of S_0 from that predicted by Mantin [15], may actually result from intricate key-length dependence in the cipher.

4 Complete proof of the generalized key-length dependent biases

In [24, Section 2], Sen Gupta et al. presented a family of biases in RC4 that are dependent on the length of the secret key. The most important of those biases was a key-length distinguisher based on the positive bias in the event $(Z_\ell = -\ell)$, where ℓ is the length of RC4 secret key in bytes.

Subsequently, in [8, Section 3.4], Isobe, Ohigashi, Watanabe and Morii observed[1] that similar bias also exists in the class of events $(Z_{x\ell} = -x\ell)$ for any positive integer x. However, they could not prove all the paths and substituted experimental values to compute what they referred as *semi-theoretical values*. They also commented the following.

> Since semi-theoretical value are partially based on experimental results, we can not claim that the proof of these bias are given.

We observe that instead of following the approach of [8], if one follows the approach in [24], then the theoretical derivation of the generalized key-length dependent biases become much simpler. In this section, we generalize all the key-length dependent biases of [24] for any key-length $\ell \in [3, N-1]$ and any integer $x \in [1, \lfloor \frac{N}{\ell} \rfloor]$ and thereby complete the proof of the extended key-length distinguisher that was left open in [8]. As a result, the biases in [24] become special cases of our results here with $x = 1$. Note that though the general proof follows the same approach as in [24], the extension is not obvious. A general proof always imply the special cases, but the converse need not be true. We experimentally verified all the intermediate claims and assumptions related to the events involving "$x\ell$" and we found them to be consistent with our theoretical claims. We present the general theorems below with the proofs.

All the biases that we are interested in are related to $(S^K_{x\ell+1}[x\ell-1] = -x\ell \wedge S^K_{x\ell+1}[x\ell] = 0)$, where x is an integer between 1 and $\lfloor \frac{N}{\ell} \rfloor$. So we first derive the probability for this event in Lemma 3.

Lemma 3 *Suppose that ℓ is the length of the secret key of RC4. Then for $1 \le x \le \lfloor \frac{N}{\ell} \rfloor$, we have*

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

where $\alpha_{x,\ell} = \frac{1}{N}\left(1 - \frac{3}{N}\right)^{x\ell-2}\left(1 - \frac{x\ell+1}{N}\right)$.

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

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

Considering the above events to be independent, the probability that all of above occur together is given by

$$\alpha_{x,\ell} = \frac{1}{N}\left(1 - \frac{3}{N}\right)^{x\ell-2}\left(1 - \frac{x\ell+1}{N}\right).$$

[1] This was independently observed by AlFardan, Bernstein, Paterson, Poettering and Schuldt [1, 4] as well.

If the above path does not occur, then we assume that the target event is uniformly distributed and hence occurs probability $\frac{1}{N^2}$, thus contributing a probability of $(1-\alpha_{x,\ell})\frac{1}{N^2}$. Adding the two contributions, the result follows. □

Theorem 8 *Suppose that ℓ is the length of the secret key of RC4. Then for $1 \le x \le \lfloor \frac{N}{\ell} \rfloor$, we have*

$$\Pr(S_{x\ell}[x\ell] = -x\ell \ \wedge \ S_{x\ell}[j_{x\ell}] = 0) = \Pr(t_{x\ell} = -x\ell \ \wedge \ S_{x\ell}[j_{x\ell}] = 0) \approx \frac{1}{N^2} + \left(1 - \frac{1}{N^2}\right)\beta_{x,\ell},$$

where $\beta_{x,\ell} = \frac{1}{N}\left(1-\frac{1}{N}\right)\left(1-\frac{2}{N}\right)^{N-3}\left(1-\frac{3}{N}\right)^{x\ell-2}\left(1-\frac{x\ell+1}{N}\right)$.

Proof From the proof of Lemma 3, consider the major path with probability $\alpha_{x,\ell}$ for the event $(S^K_{x\ell+1}[x\ell-1] = -x\ell \ \wedge \ S^K_{x\ell+1}[x\ell] = 0)$. For the remaining $N - x\ell - 1$ rounds of the KSA and for the first $x\ell - 2$ 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 $\{x\ell-1, x\ell\}$. This happens with a probability of $\left(1-\frac{2}{N}\right)^{N-3}$.

Now, in round $x\ell - 1$ of PRGA, $i_{x\ell-1} = x\ell - 1$, from where the value $x\ell - 1$ moves to index $j_{x\ell-1}$ due to the swap. In the next round, $i_{x\ell} = x\ell$ and $j_{x\ell} = j_{x\ell-1} + S_{x\ell-1}[x\ell] = j_{x\ell-1}$, provided the value 0 at index $x\ell$ had not been swapped out by $j_{x\ell-1}$, the probability of which is $1-\frac{1}{N}$. So during the next swap, the value $-x\ell$ moves from index $j_{x\ell}$ to index $x\ell$ and the value 0 moves from index $x\ell$ to $j_{x\ell}$. The probability of the above major path leading to the event $(S_{x\ell}[x\ell] = -x\ell \ \wedge \ S_{x\ell}[j_{x\ell}] = 0)$ is given by $\beta_{x,\ell} = \alpha_{x,\ell}\left(1-\frac{2}{N}\right)^{N-3}\left(1-\frac{1}{N}\right)$. If this path does not occur, then we assume that the target event is uniformly distributed, i.e., with probability $\frac{1}{N^2}$. Adding the two contributions and substituting the value of $\alpha_{x,\ell}$ from Lemma 3, the result follows.

Further, as $t_{x\ell} = S_{x\ell}[x\ell] + S_{x\ell}[j_{x\ell}]$, the event $(S_{x\ell}[x\ell] = -x\ell \ \wedge \ S_{x\ell}[j_{x\ell}] = 0)$ is equivalent to the event $(t_{x\ell} = -x\ell \ \wedge \ S_{x\ell}[j_{x\ell}] = 0)$, and hence the result. □

Theorem 9 *Suppose that ℓ is the length of the secret key of RC4. Then for $1 \le x \le \lfloor \frac{N}{\ell} \rfloor$, we have* $\Pr(Z_{x\ell} = -x\ell \ \wedge \ S_{x\ell}[j_{x\ell}] = 0) \approx \frac{1}{N^2} + \left(1-\frac{1}{N^2}\right)\gamma_{x,\ell}$, *where*
$\gamma_{x,\ell} = \frac{1}{N^2}\left(1-\frac{x\ell+1}{N}\right)\sum_{u=x\ell+1}^{N-1}\left(1-\frac{1}{N}\right)^{u}\left(1-\frac{2}{N}\right)^{u-x\ell}\left(1-\frac{3}{N}\right)^{N-u+2x\ell-4}$.

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

From the proof of Lemma 3, consider the major path with probability $\alpha_{x\ell}$ for the joint event $(S^K_{x\ell+1}[x\ell-1] = -x\ell \wedge S^K_{x\ell+1}[x\ell] = 0)$. This constitutes the first part of our main path leading to the target event. The second part, having probability $\alpha'_{x,\ell}$, can be constructed as follows.

1. For an index $u \in [x\ell+1, N-1]$, we have $S^K_u[u] = u$. This happens with probability $\left(1-\frac{1}{N}\right)^u$.
2. For the KSA rounds $x\ell+2$ to u, the j^K values do not touch the indices $x\ell-1$ and $x\ell$. This happens with probability $\left(1-\frac{2}{N}\right)^{u-x\ell-1}$.
3. In round $u+1$ of KSA, when $i^K_{u+1} = u$, j^K_{u+1} becomes $x\ell-1$ with probability $\frac{1}{N}$. Due to the swap, the value u moves to $S^K_{u+1}[x\ell-1]$ and the value $-x\ell$ moves to $S^K_{u+1}[u] = S^K_{u+1}[S^K_{u+1}[x\ell-1]]$.
4. For the remaining $N-u-1$ rounds of the KSA and for the first $x\ell-1$ rounds of the PRGA, none of the j^K or j values should touch the indices $\{x\ell-1, S[x\ell-1], x\ell\}$. This happens with a probability of $\left(1-\frac{3}{N}\right)^{N-u+x\ell-2}$.

5. So far, we have $(S_{x\ell-1}[S_{x\ell-2}[x\ell-1]] = -x\ell \ \wedge \ S_{x\ell-1}[x\ell] = 0)$. Now, we should also have $j_{x\ell} \notin \{x\ell-1, S[x\ell-1]\}$ for $S_{x\ell}[S_{x\ell-2}[x\ell-1]] = S_{x\ell-1}[S_{x\ell-2}[x\ell-1]] = -x\ell$. The probability of this condition is $\left(1-\frac{2}{N}\right)$.

Assuming all the individual events in the above path to be mutually independent, we get

$$\alpha'_{x,\ell} = \frac{1}{N}\sum_{u=x\ell+1}^{N-1}\left(1-\frac{1}{N}\right)^{u}\left(1-\frac{2}{N}\right)^{u-x\ell}\left(1-\frac{3}{N}\right)^{N-u+x\ell-2}.$$

Thus, the probability of the entire path is given by

$$\gamma_{x,\ell} = \alpha_{x,\ell}\cdot\alpha'_{x,\ell} = \frac{1}{N^2}\left(1-\frac{x\ell+1}{N}\right)\sum_{u=x\ell+1}^{N-1}\left(1-\frac{1}{N}\right)^{u}\left(1-\frac{2}{N}\right)^{u-x\ell}\left(1-\frac{3}{N}\right)^{N-u+2x\ell-4}.$$

If this path does not occur, then we assume that the target event is uniformly distributed, i.e., occurs with probability $\frac{1}{N^2}$. Adding the two contributions, we get the result. □

Theorem 10 *For any key-length $\ell \in [3, N-1]$ and any integer $x \in [1, \lfloor \frac{N}{\ell} \rfloor]$, the probability $\Pr(S_{x\ell}[j_{x\ell}] = 0)$ is given by*
$\delta_{x,\ell} \approx \Pr(S_1[x\ell] = 0)\left(1-\frac{1}{N}\right)^{x\ell-2} + \sum_{y=2}^{x\ell-1}\sum_{w=0}^{x\ell-y}\frac{\Pr(S_1[y]=0)}{w!\cdot N}\left(\frac{x\ell-y-1}{N}\right)^{w}\left(1-\frac{1}{N}\right)^{x\ell-3-w}$.

Proof Note that $S_{x\ell}[j_{x\ell}]$ is assigned the value of $S_{x\ell-1}[x\ell]$ due to the swap in round $x\ell$. Hence, by substituting $u = x\ell$ and $v = 0$ in Proposition 3, we get the result. □

Theorem 11 *Suppose that ℓ is the length of the secret key of RC4. Then for $1 \le x \le \lfloor \frac{N}{\ell} \rfloor$, we have $\tau_{x,\ell} = \Pr(t_{x\ell} = -x\ell) \approx \frac{1}{N^2} + \left(1-\frac{1}{N^2}\right)\beta_{x,\ell} + (1-\delta_{x,\ell})\frac{1}{N}$, where $\beta_{x,\ell}$ is given in Theorem 8 and $\delta_{x,\ell}$ is given in Theorem 10.*

Proof We can write $\Pr(t_{x\ell} = -x\ell) = \Pr(t_{x\ell} = -x\ell \wedge S_{x\ell}[j_{x\ell}] = 0) + \Pr(t_{x\ell} = -x\ell \wedge S_{x\ell}[j_{x\ell}] \neq 0)$, where the first term is given by Theorem 8. When $S_{x\ell}[j_{x\ell}] \neq 0$, the event $(t_{x\ell} = -x\ell)$ can be assumed to be uniform. Hence the second term can be computed as $\Pr(S_{x\ell}[j_{x\ell}] \neq 0)\cdot\Pr(t_{x\ell} = -x\ell \mid S_{x\ell}[j_{x\ell}] \neq 0) \approx (1-\delta_{x,\ell})\frac{1}{N}$. Adding the two terms, we get the result. □

By dividing the joint probabilities $\Pr(S_{x\ell}[x\ell] = -x\ell \ \wedge \ S_{x\ell}[j_{x\ell}] = 0)$ and $\Pr(t_{x\ell} = -x\ell \ \wedge S_{x\ell}[j_{x\ell}] = 0)$ of Theorem 8, and $\Pr(Z_{x\ell} = -x\ell \wedge S_{x\ell}[j_{x\ell}] = 0)$ of Theorem 9 by the appropriate marginals $\delta_{x,\ell} = \Pr(S_{x\ell}[j_{x\ell}] = 0)$ of Theorem 10 and $\tau_{x,\ell} = \Pr(t_{x,\ell} = -x\ell)$ of Theorem 11, we get theoretical values of the following conditional biases

1. $\Pr(S_{x\ell}[x\ell] = -x\ell \mid S_{x\ell}[j_{x\ell}] = 0) = \Pr(t_{x\ell} = -x\ell \mid S_{x\ell}[j_{x\ell}] = 0)$.
2. $\Pr(S_{x\ell}[j_{x\ell}] = 0 \mid t_{x\ell} = -x\ell)$.
3. $\Pr(Z_{x\ell} = -x\ell \mid S_{x\ell}[j_{x\ell}] = 0)$.

Theorem 12 *Suppose that ℓ is the length of the secret key of RC4. Then for $1 \le x \le \lfloor \frac{N}{\ell} \rfloor$,*

$$\Pr(Z_{x\ell} = -x\ell) \ \approx \ \frac{1}{N^2} + \left(1-\frac{1}{N^2}\right)\gamma_{x,\ell} + (1-\delta_{x,\ell})\frac{1}{N},$$

where $\gamma_{x,\ell}$ is given in Theorem 9 and $\delta_{x,\ell}$ is given in Theorem 10.

Proof We can write $\Pr(Z_{x\ell} = -x\ell) = \Pr(Z_{x\ell} = -x\ell \wedge S_{x\ell}[j_{x\ell}] = 0) + \Pr(Z_{x\ell} = -x\ell \wedge S_{x\ell}[j_{x\ell}] \neq 0)$, where the first term is given by Theorem 9. When $S_{x\ell}[j_{x\ell}] \neq 0$, the event $(Z_{x\ell} = -x\ell)$ can be assumed to be uniformly distributed. Hence the second term can be computed as $\Pr(S_{x\ell}[j_{x\ell}] \neq 0)\cdot\Pr(Z_{x\ell} = -x\ell \mid S_{x\ell}[j_{x\ell}] \neq 0) \approx (1-\delta_{x,\ell})\frac{1}{N}$. Adding the two terms, we get the result. □

By dividing the joint probability $\Pr(Z_{x\ell} = -x\ell \wedge S_{x\ell}[j_{x\ell}] = 0)$ of Theorem 9 by $\Pr(Z_{x\ell} = -x\ell)$ as given above, we get the theoretical value of $\Pr(S_{x\ell}[j_{x\ell}] = 0 \mid Z_{x\ell} = -x\ell)$.

In Figure 7, we compare the experimental values of $(Z_{x\ell} = -x\ell)$, obtained from the data of [1, 4], with our theoretical values derived from Theorem 12, for key-length $\ell = 16$ and $x = 1, 2, \ldots, 15$. We have obtained almost similar results for other key-lengths as well.

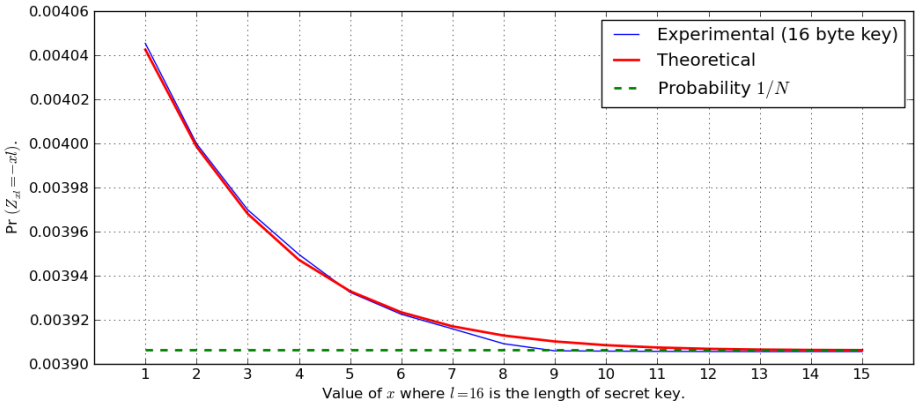

Fig. 7 Bias in the event $(Z_{x\ell} = -x\ell)$ for key-length $\ell = 16$ and $x = 1, 2, \ldots, 15$.

5 Conclusion

We have proved all open short-term single-byte biases that have been exploited in the recent TLS attack [1, 4]. We have also given complete proof of the 'extended key-length biases' from [8]. Table 2 compares our theoretical results with the experimental data. Except the last two rows of Table 2, all the experimental data is taken from [2] that estimated the probability with 2^{45} randomly chosen secret keys of length 16 bytes. The last row corresponds to $\ell = 16$ for TLS and under the "Theoretical proof" column of this row, we write "Theorem 12", since the expression is too complicated to fit in the table.

Table 2 Proved short-term single-byte keystream biases of RC4 in TLS (16 byte key).

Bias in event	Discovered	Theoretical proof (this paper)	Experimental
$Z_1 = 129$	[1]	$1/N - 1.73/N^2$	$1/N - 1.72/N^2$ [2]
$Z_2 = 129$	[1, 22]	$1/N - 1.90/N^2$	$1/N - 1.82/N^2$ [2]
$Z_2 = 172$	[1]	$1/N + 0.16/N^2$	$1/N + 0.20/N^2$ [2]
$Z_4 = 2$	[1]	$1/N + 0.83/N^2$	$1/N + 0.81/N^2$ [2]
$Z_{256} = 0$	[1, 8]	$1/N - 0.37/N^2$	$1/N - 0.38/N^2$ [2]
$Z_{257} = 0$	[8]	$1/N + 0.36/N^2$	$1/N + 0.35/N^2$ [8, Table 3]
$Z_{x\ell} = -x\ell$	[8]	Theorem 12 [this paper]	Figure 7 [this paper]

In the context of long-standing open issue of 'anomalies' in RC4 initial state, we could prove an important anomaly regarding the bias in $S_0[128] = 127$. Our work reveals that a thorough analysis of the "anomaly pairs" is necessary, not only for their independent theoretical interest, but also to investigate their connection with key-length.

Acknowledgments

We sincerely thank the anonymous reviewers whose feedback and suggestions helped in substantial improvement of the technical as well as the editorial quality of our paper. We are also grateful to the Project CoEC (Centre of Excellence in Cryptology), Indian Statistical Institute, Kolkata, funded by the Government of India, for partial support towards this project.

References

1. N. AlFardan, D. Bernstein, K. Paterson, B. Poettering, and J. Schuldt, "On the security of RC4 in TLS," Published online at `http://www.isg.rhul.ac.uk/tls/`, 2013, presented at the FSE 2013 invited talk [4] by Dan Bernstein. Accepted in USENIX 2013.
2. N. AlFardan, D. Bernstein, K. Paterson, B. Poettering, and J. Schuldt, "Distribution of RC4 keystream bytes," Available online at `http://www.isg.rhul.ac.uk/tls/RC4_keystream_dist_2_45.txt`.
3. R. Basu, S. Ganguly, S. Maitra, and G. Paul, "A complete characterization of the evolution of RC4 pseudo random generation algorithm," *J. Mathematical Cryptology*, vol. 2, no. 3, pp. 257–289, 2008.
4. D. Bernstein, "Failures of secret-key cryptography," Invited talk at FSE 2013, session chaired by Bart Preneel.
5. S. R. Fluhrer and D. A. McGrew, "Statistical analysis of the alleged RC4 keystream generator," in *FSE*, ser. Lecture Notes in Computer Science, B. Schneier, Ed., vol. 1978. Springer, 2000, pp. 19–30.
6. J. D. Golic, "Linear statistical weakness of alleged RC4 keystream generator," in *EUROCRYPT*, ser. Lecture Notes in Computer Science, W. Fumy, Ed., vol. 1233. Springer, 1997, pp. 226–238.
7. J. D. Golic, "Linear models for a time-variant permutation generator," *IEEE Transactions on Information Theory*, vol. 45, no. 7, pp. 2374–2382, 1999.
8. T. Isobe, T. Ohigashi, Y. Watanabe, and M. Morii, "Full plaintext recovery attack on broadcast RC4," in *Fast Software Encryption (FSE)*, 2013, to appear in Lecture Notes in Computer Science, Springer.
9. T. Isobe, T. Ohigashi, Y. Watanabe, and M. Morii, "Comprehensive Analysis of Initial Keystream Biases of RC4," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E97-A, no. 1, pp. 139–151, 2014.
10. R. J. J. Jr., "ISAAC and RC4," Published on the Internet at `http://burtleburtle.net/bob/rand/isaac.html`, 1996.
11. J. Lv and D. Lin, "L-P states of RC4 stream cipher," *IACR Cryptology ePrint Archive*, year 2013, no. 266, 2013.
12. J. Lv, B. Zhang, and D. Lin, "Distinguishing attacks on RC4 and a new improvement of the cipher," *IACR Cryptology ePrint Archive*, year 2013, no. 176, 2013.
13. S. Maitra, G. Paul, S. Sarkar, M. Lehmann, and W. Meier, "New results on generalization of Roos-type biases and related keystream of RC4," in *Africacrypt*, ser. Lecture Notes in Computer Science, A. Youssef, A. Nitaj, A. E. Hassanien, Eds., vol. 7918. Springer, 2013, pp. 222–239.
14. S. Maitra, G. Paul, and S. Sengupta, "Attack on broadcast RC4 revisited," in *FSE*, ser. Lecture Notes in Computer Science, A. Joux, Ed., vol. 6733. Springer, 2011, pp. 199–217.
15. 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`.
16. I. Mantin, "Predicting and distinguishing attacks on RC4 keystream generator," in *EUROCRYPT*, ser. Lecture Notes in Computer Science, R. Cramer, Ed., vol. 3494. Springer, 2005, pp. 491–506.
17. I. Mantin and A. Shamir, "A practical attack on broadcast RC4," in *FSE*, ser. Lecture Notes in Computer Science, M. Matsui, Ed., vol. 2355. Springer, 2001, pp. 152–164.
18. I. Mironov, "(not so) random shuffles of RC4," in *CRYPTO*, ser. Lecture Notes in Computer Science, M. Yung, Ed., vol. 2442. Springer, 2002, pp. 304–319.
19. M. A. Orumiehchiha, J. Pieprzyk, E. Shakour, and R. Steinfeld, "Cryptanalysis of RC4(n, m) stream cipher," *IACR Cryptology ePrint Archive*, year 2013, no. 178, 2013.
20. G. Paul, S. Maitra, and R. Srivastava, "On non-randomness of the permutation after RC4 key scheduling," in *AAECC*, ser. Lecture Notes in Computer Science, S. Boztas and H. feng Lu, Eds., vol. 4851. Springer, 2007, pp. 100–109.
21. 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`.
22. S. Sarkar, "Further non-randomness in RC4, RC4A and VMPC," in *International Workshop on Coding and Cryptography (WCC)*, 2013.

23. S. Sen Gupta, S. Maitra, G. Paul, and S. Sarkar, "Proof of empirical RC4 biases and new key correlations," in *Selected Areas in Cryptography*, ser. Lecture Notes in Computer Science, A. Miri and S. Vaudenay, Eds., vol. 7118. Springer, 2011, pp. 151–168.
24. S. Sen Gupta, S. Maitra, G. Paul, and S. Sarkar, "(Non–)random sequences from (non–)random permutations – analysis of RC4 stream cipher," *Journal of Cryptology*, 2013, to appear. Published online in December 2012, with DOI: 10.1007/s00145-012-9138-1.
25. P. Sepehrdad, "Statistical and Algebraic Cryptanalysis of Lightweight and Ultra-lightweight Symmetric Primitives," PhD thesis No. 5415, École Polytechnique Fédérale de Lausanne (EPFL), 2012, available at `http://lasecwww.epfl.ch/~sepehrdad/Pouyan_Sepehrdad_PhD_Thesis.pdf`.
26. P. Sepehrdad, P. Susil, S. Vaudenay, and M. Vuagnoux, "Smashing WEP in a passive attack," in *Fast Software Encryption (FSE)*, 2013, to appear.
27. P. Sepehrdad, S. Vaudenay, and M. Vuagnoux, "Discovery and exploitation of new biases in RC4," in *Selected Areas in Cryptography*, ser. Lecture Notes in Computer Science, A. Biryukov, G. Gong, and D. R. Stinson, Eds., vol. 6544. Springer, 2010, pp. 74–91.
28. P. Sepehrdad, S. Vaudenay, and M. Vuagnoux, "Statistical attack on RC4 - distinguishing WPA," in *EUROCRYPT*, ser. Lecture Notes in Computer Science, K. G. Paterson, Ed., vol. 6632. Springer, 2011, pp. 343–363.
29. J. Striömbergson and S. Josefsson, "The perils of repeating patterns: Observation of some weak keys in RC4," *IACR Cryptology ePrint Archive*, year 2013, no. 241, 2013.