How TKIP induces biases of internal states of generic RC4

Ryoma Ito and Atsuko Miyaji*

Japan Advanced Institute of Science and Technology
1-1 Asahidai, Nomi-shi, Ishikawa, 923-1292, Japan
ryoma.ito.shs@gmail.com, miyaji@jaist.ac.jp

Abstract. RC4, designed by Rivest, is widely used including WPA, which is one of the security protocols for IEEE 802.11 wireless standard. The first 3-byte RC4 keys in WPA generated by IV are *known* since IV can be obtained by observing a packet. In 2014, Sen Gupta et al. found linear correlations between the keystream byte and *known* RC4 key bytes. In 2015, Our previous work extended linear correlations to include *unknown* internal states as well as the keystream byte and *known* RC4 key bytes. They found more than 150 linear correlations experimentally, and proved only 6 cases theoretically. In this paper, we will provide theoretical proof of 15 cases out of their unproven linear correlations. These theoretical results demonstrated how TKIP key generation procedure in WPA induces biases on internal states different from generic RC4.

Keywords: RC4, WPA, TKIP, linear correlation

1 Introduction

RC4 is the stream cipher designed by Rivest in 1987, and is widely used in various standard protocols such as Secure Socket Layer/Transport Layer Security (SSL/TLS), Wired Equivalent Privacy (WEP) and Wi-fi Protected Access (WPA), etc. Due to its popularity and simplicity, RC4 has been intensively analyzed since its specification was made public on the internet in 1994 [1–11]. RC4 consists of two algorithms: the Key Scheduling Algorithm (KSA) and the Pseudo Random Generation Algorithm (PRGA). Both the KSA and the PRGA update a secret internal state S which is a permutation of all N (typically, $N = 2^8$) possible bytes and two 8-bit indices i and j. The KSA generates the initial state from a secret key K of l bytes to become the input of the PRGA. Once the initial state is generated in the KSA, the PRGA outputs a pseudo-random sequence (keystream) $Z_1, Z_2, \ldots, Z_r$, where r is the number of rounds. The KSA and the PRGA are shown in Algorithms 1 and 2, respectively, where $\{S_i^K, i, j_i^K\}$ and $\{S_r, i_r, j_r\}$ are $\{S, i, j\}$ in the i-th and r-th round of the KSA and the PRGA, respectively; t_r is a 8-bit index of Z_r. All addition used in both the KSA and the PRGA are arithmetic addition modulo N.

* Supported by the project "The Security infrastructure Technology for Integrated Utilization of Big Data" of Japan Science and Technology Agency CREST.

Algorithm 1 KSA

1: **for** $i = 0$ to $N - 1$ **do**
2: $S_0^K[i] \leftarrow i$
3: **end for**
4: $j_0^K \leftarrow 0$
5: **for** $i = 0$ to $N - 1$ **do**
6: $j_{i+1}^K \leftarrow j_i^K + S_i^K[i] + K[i \mod l]$
7: $\mathrm{Swap}(S_i^K[i], S_i^K[j_{i+1}^K])$
8: **end for**

Algorithm 2 PRGA

1: $r \leftarrow 0$, $i_0 \leftarrow 0$, $j_0 \leftarrow 0$
2: **loop**
3: $r \leftarrow r + 1$, $i_r \leftarrow i_{r-1} + 1$
4: $j_r \leftarrow j_{r-1} + S_{r-1}[i_r]$
5: $\mathrm{Swap}(S_{r-1}[i_r], S_{r-1}[j_r])$
6: $t_r \leftarrow S_r[i_r] + S_r[j_r]$
7: **Output:** $Z_r \leftarrow S_r[t_r]$
8: **end loop**

WPA is the security protocol for IEEE 802.11 wireless networks standardized as a substitute for WEP in 2003, and uses RC4 for encryption. WPA improves a 16-byte RC4 key generation procedure known as the Temporary Key Integrity Protocol (TKIP) to prevent an attack against WEP by Fluhrer et al. [2]. One of characteristic features in TKIP is that the first 3-byte RC4 keys, $K[0]$, $K[1]$ and $K[2]$, are generated by the last 16-bit Initialization Vector (IV16), which is a sequence counter as follows:

$$K[0] = (\mathrm{IV16} >> 8) \ \& \ \mathrm{0xFF},$$
$$K[1] = ((\mathrm{IV16} >> 8) \mid \mathrm{0x20}) \ \& \ \mathrm{0x7F},$$
$$K[2] = \mathrm{IV16} \ \& \ \mathrm{0xFF}.$$

Note that these RC4 key bytes in WPA are *known* since IV can be obtained by observing a packet.

In 2014, Sen Gupta et al. showed that there exists a characteristic distribution related to $K[0] + K[1]$ in WPA [3]. They also found some linear correlations between the keystream byte and *known* RC4 key bytes in WPA such as $Z_1 = -K[0] - K[1]$, $Z_3 = K[0] + K[1] + K[2] + 3$, etc. They applied these linear correlations to a plaintext recovery attack against WPA in the same way as the attack against SSL/TLS by Isobe et al. [4], and reduced the computational complexity necessary for the attack. In 2015, We extended linear correlations to include *unknown* internal states as well as the keystream byte and *known* RC4 key bytes [5]. Here, *unknown* internal states mean $S_r[i_{r+1}]$, $S_r[j_{r+1}]$, j_{r+1} and t_{r+1} for $r \geq 0$. Then, more than 150 linear correlations have been found experimentally, although only 6 correlations have been proved theoretically such as: $S_0[i_1] = K[0]$, $K[0] - K[1] - 3$ or $K[0] - K[1] - 1$; $S_{255}[i_{256}] = K[0]$ or $S_{255}[i_{256}] = K[1]$; $S_r[i_{r+1}] = K[0] + K[1] + 1$ $(0 \leq r \leq N)$.

We focus on these correlations remain unproven theoretically. [5]. Actually, linear correlations including internal states could contribute to reducing the computational complexity necessary for the state recovery attacks against RC4 proposed in [1, 6, 9] especially with WPA. Furthermore, theoretical proofs on linear correlations including internal states can make clear how TKIP induces biases as pointed out above. In the previous results, biases related to the first round internal state $S_0[i_1]$ were intensively investigated but other internal states in more than second round are still unknown. If we see how many round these biases have been kept in internal states, then key generation procedure in WPA could be

reconstructed securely while keeping congruity with TKIP. In fact, TKIP should have been constructed in such a way that it can keep or further enhance original security level of generic RC4. Our analysis would be also useful to investigate a generic construction of key generation procedure including IV in such a way that it can keep or further enhance security level of an original encryption.

In this paper, we will provide theoretical proofs of 15 cases out of remaining linear correlations. Our contributions of 10 theorems can be summarized as follows:

- Theorems 1, 4 and 5 show that $\Pr(S_0[i_1] = -K[0] - K[1] - 3)$, $\Pr(S_1[i_2] = -K[0] - K[1] + K[2] - 1)$ and $\Pr(S_1[i_2] = K[0] - K[1] + K[2] + x)$ ($x \in \{-3, -1, 1\}$) are double probabilities of random association $\frac{1}{N}$ in WPA.
- Theorem 2 shows that $\Pr(S_0[i_1] = K[0] + K[1] + K[2] + 3)$ is less than half of the probability of random association $\frac{1}{N}$ in both generic RC4 and WPA.
- Theorem 3 shows that $\Pr(S_1[i_2] = K[0] + K[1] + K[2] + 3)$ is pretty high probability in comparison to the probability of random association $\frac{1}{N}$ in both generic RC4 and WPA. This probability is induced by Roos' bias, that is

$$\Pr(S_0[i_2] = K[0] + K[1] + K[2] + 3) \approx \left(1 - \tfrac{2}{N}\right) \cdot \left(1 - \tfrac{1}{N}\right)^{N+3} + \tfrac{1}{N}.$$

- Theorems 6-10 provide theoretical analysis related to the second round index j_2.

This paper is organized as follows: Section 2 summarizes the previous works necessary for both theoretical proofs and experiments such as Roos' biases [10, 11], biases of the initial state of the PRGA in generic RC4 [7], the distribution of $K[0]+K[1]$ and the initial state of PRGA in WPA [3] and the number of samples necessary for distinguishing two distributions [8]. Section 3 shows the theoretical proofs of biases based on linear equations and the experimental results. Section 4 concludes this paper.

2 Preliminary for our proofs and experiments

Let us summarize some previous results which will be used in both theoretical proofs and experiments. Proposition 1 shows Roos' biases [11], correlations between the RC4 key bytes and S_0, proved by Paul and Maitra [10]. Proposition 2 shows biases of S_0, proved by Mantin [7]. Proposition 3 shows a distribution of $K[0] + K[1]$ in WPA, proved by Sen Gupta et al. [3]. By combining Proposition 3 with Proposition 1 (Roos' biases), a characteristic bias on the distribution of $S_0[1]$ is given as Proposition 4 [3]. Finally, Mantin and Shamir showed Proposition 5 related to the number of samples necessary for distinguishing two distributions with a constant probability of success [8].

Proposition 1 ([10, Corollary 2]). *In the initial state of the PRGA for* $0 \leq y \leq N - 1$*, we have*

$$\Pr(S_0[y] = \tfrac{y(y+1)}{2} + \textstyle\sum_{x=0}^{y} K[x]) \approx \left(1 - \tfrac{y}{N}\right) \cdot \left(1 - \tfrac{1}{N}\right)^{\left[\frac{y(y+1)}{2} + N\right]} + \tfrac{1}{N}.$$

Proposition 2 ([7, Theorem 6.2.1]). *In the initial state of the PRGA for $0 \le u \le N-1$, $0 \le v \le N-1$, we have*

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

Proposition 3 ([3, Theorem 1]). *For $0 \le v \le N-1$, the distribution of the sum v of $K[0]$ and $K[1]$ generated by the temporal key hash function in WPA is given as follows:*

$$\begin{aligned} &\Pr(K[0]+K[1]=v) = 0 && \text{if } v \text{ is odd}, \\ &\Pr(K[0]+K[1]=v) = 0 && \text{if } v \text{ is even and } v \in [0,31] \cup [128,159], \\ &\Pr(K[0]+K[1]=v) = 2/256 && \text{if } v \text{ is even and} \\ & && v \in [32,63] \cup [96,127] \cup [160,191] \cup [224,255], \\ &\Pr(K[0]+K[1]=v) = 4/256 && \text{if } v \text{ is even and } v \in [64,95] \cup [192,223]. \end{aligned}$$

Proposition 4 ([3, Theorem 2]). *In the initial state of the PRGA in WPA for $0 \le v \le N-1$, we have*

$$\begin{aligned} \Pr(S_0[1] = v) = {} & \alpha \cdot \Pr(K[0]+K[1] = v-1) \\ & + (1-\alpha) \cdot (1 - \Pr(K[0]+K[1] = v-1)) \cdot \Pr(S_0[1] = v)_{\mathrm{RC4}} \\ & + \tfrac{(1-\alpha)}{N-1} \cdot \textstyle\sum_{x \ne v} \Pr(K[0]+K[1] = x-1) \cdot \Pr(S_0[1] = x)_{\mathrm{RC4}}. \end{aligned}$$

where, $\alpha = \frac{1}{N} + \left(1-\frac{1}{N}\right)^{N+2}$, and both $\Pr(S_0[1] = v)_{\mathrm{RC4}}$ and $\Pr(S_0[1] = x)_{\mathrm{RC4}}$ are taken from Proposition 2.

Proposition 5 ([8, Theorem 2]). *Let X and Y be two distributions, and suppose that the event e occurs in X with a probability p and Y with a probability $p \cdot (1+q)$. Then, for small p and q, $\mathcal{O}(\frac{1}{p \cdot q^2})$ samples suffice to distinguish X from Y with a constant probability of success.*

3 Newly proved linear correlations

3.1 Biases based on linear equations

In 2014, Sen Gupta et al. found some linear correlations between the keystream byte and *known* RC4 key bytes in WPA using the following linear equations for $a, b, c \in \{0, \pm 1\}$ and $d \in \{0, \pm 1, \pm 2, \pm 3\}$:

$$Z_r = a \cdot K[0] + b \cdot K[1] + c \cdot K[2] + d \quad \text{for } r \ge 1 \text{ [3]}. \tag{1}$$

In 2015, we further extended linear correlations on *known* RC4 key bytes in both generic RC4 and WPA to those among *unknown* state information, *known* RC4 key bytes and the keystream byte such as

$$X_r = a \cdot Z_{r+1} + b \cdot K[0] + c \cdot K[1] + d \cdot K[2] + e \quad \text{for } r \ge 1, \tag{2}$$

where $X_r \in \{S_r[i_{r+1}], S_r[j_{r+1}], j_{r+1}, t_{r+1}\}$, $a, b, c, d \in \{0, \pm 1\}$, and $e \in \{0, \pm 1, \pm 2, \pm 3\}$ [5]. Then, 6 correlations out of more than 150 linear correlations have been shown theoretically as follows:

$S_0[i_1] = K[0], K[0] - K[1] - 3$ or $K[0] - K[1] - 1$;
$S_{255}[i_{256}] = K[0]$ or $K[1]$;
$S_r[i_{r+1}] = K[0] + K[1] + 1$ for $0 \leq r \leq N$.

In this paper, we will provide newly theoretical proofs of 15 linear correlations listed in Table 1. Actually, the first state recovery attack proposed by Knudsen et al. reconstructs the internal state of RC4 by computing optimum solutions of four *unknown* variables in each round such as $S_r[i_{r+1}]$, $S_r[j_{r+1}]$, j_{r+1} and t_{r+1} for $r \geq 0$ [6]. Therefore, these linear correlations could contribute to finding a correct internal state of RC4 in WPA.

We often use Roos' biases shown in Proposition 1 through proofs. Roos' biases are denoted by $\alpha_y = \Pr(S_0[y] = \frac{y(y+1)}{2} + \sum_{x=0}^{y} K[x])$. We assume through proofs that the probability of certain events, confirmed experimentally that there are no significant biases, is that of random association $\frac{1}{N}$ (e.g. events related to the internal state). We also assume that the RC4 key K is generated uniformly at random in both generic RC4 and WPA, except $K[0]$, $K[1]$ and $K[2]$ in WPA generated by IV using a sequence counter.

3.2 Proof of biases in $S_0[i_1]$

In this section, we prove Theorems 1 and 2 theoretically. Theorem 1 shows that event $(S_0[i_1] = -K[0] - K[1] - 3)$ yields a positive bias in both generic RC4 and

Table 1. Newly proved linear correlations in both generic RC4 and WPA

X_r	Linear correlations	RC4	WPA	Remarks
$S_0[i_1]$	$-K[0] - K[1] - 3$	0.005336	0.008437	Theorem 1
	$K[0] + K[1] + K[2] + 3$	0.001492	0.001491	Theorem 2
$S_1[i_2]$	$K[0] + K[1] + K[2] + 3$	0.360357	0.361718	Theorem 3
	$-K[0] - K[1] + K[2] - 1$	0.005305	0.008197	Theorem 4
	$K[0] - K[1] + K[2] - 3$	0.005295	0.008163	Theorem 5
	$K[0] - K[1] + K[2] - 1$	0.005290	0.008171	Theorem 5
	$K[0] - K[1] + K[2] + 1$	0.005309	0.008171	Theorem 5
j_2	$K[2]$	0.004428	0.005571	Theorem 6
	$-K[0] - K[1] + K[2] - 2$	0.003921	0.004574	Theorem 7
	$-K[0] - K[1] + K[2]$	0.003919	0.005573	Theorem 7
	$-K[0] - K[1] + K[2] + 2$	0.003912	0.004545	Theorem 7
	$-K[0] + K[1] + K[2]$	0.003921	0.005501	Theorem 8
	$-K[1] + K[2] - 2$	0.003911	0.005479	Theorem 9
	$-K[1] + K[2] + 3$	0.003899	0.005476	Theorem 9
	$K[0] - K[1] + K[2]$	0.003918	0.005618	Theorem 10

WPA. We note that Theorem 1 means the first round internal state $S_0[i_1]$ can be guessed in a double probability of random association $\frac{1}{N}$ by using *known* $K[0]$ and $K[1]$ in WPA. Theorem 2 shows that event $(S_0[i_1] = K[0]+K[1]+K[2]+3)$ yields a negative bias in both generic RC4 and WPA.

Theorem 1. *In the initial state of the PRGA, we have*

$$\Pr(S_0[i_1] = -K[0] - K[1] - 3) \approx \begin{cases} \frac{2}{N}\alpha_1 + \frac{1}{N}\left(1 - \frac{2}{N}\right)(1 - \alpha_1) & \textit{for RC4,} \\ \frac{4}{N}\alpha_1 + \frac{1}{N}\left(1 - \frac{4}{N}\right)(1 - \alpha_1) & \textit{for WPA.} \end{cases}$$

Proof. The probability of event $(S_0[i_1] = -K[0]-K[1]-3)$ can be decomposed in two paths: $K[0]+K[1] = 126, 254$ (Path 1) and $K[0]+K[1] \neq 126, 254$ (Path 2). These paths include all events in order to compute $Pr(S_0[i_1] = -K[0]-K[1]-3)$. In the following proof, we use $S_0[1]$ instead of $S_0[i_1]$ $(i_1 = 1)$ for simplicity.

Path 1. In $K[0] + K[1] = 126, 254$, event $(S_0[1] = -K[0] - K[1] - 3)$ occurs if and only if $S_0[1] = K[0] + K[1] + 1$. Therefore, we get

$$\Pr(S_0[1] = -K[0] - K[1] - 3 \mid \text{Path 1}) = \alpha_1.$$

Path 2. In $K[0] + K[1] \neq 126, 254$, event $(S_0[1] = -K[0] - K[1] - 3)$ never occurs if $S_0[1] = K[0] + K[1] + 1$. If $S_0[1] \neq K[0] + K[1] + 1$ holds, then we assume that event $(S_0[1] = -K[0] - K[1] - 3)$ occurs with the probability of random association $\frac{1}{N}$. Therefore, we get

$$\Pr(S_0[1] = -K[0] - K[1] - 3 \mid \text{Path 2}) = \tfrac{1}{N} \cdot (1 - \alpha_1).$$

The probability of $K[0]+K[1] = 126$ and 254 in WPA is $\frac{2}{N}$, twice as high as that of random association, although that in generic RC4 is $\frac{1}{N}$ since K is generated uniformly at random. By substituting each $\Pr(K[0] + K[1] = 126, 254)$ in both generic RC4 and WPA, we get

$$\begin{aligned} &\Pr(S_0[i_1] = K[0] - K[1] - 3) \\ &\quad = \Pr(S_0[1] = K[0] - K[1] - 3 \mid \text{Path 1}) \cdot \Pr(\text{Path 1}) \\ &\qquad + \Pr(S_0[1] = K[0] - K[1] - 3 \mid \text{Path 2}) \cdot \Pr(\text{Path 2}) \\ &\quad \approx \begin{cases} \frac{2}{N}\alpha_1 + \frac{1}{N}\left(1 - \frac{2}{N}\right)(1 - \alpha_1) & \text{for RC4,} \\ \frac{4}{N}\alpha_1 + \frac{1}{N}\left(1 - \frac{4}{N}\right)(1 - \alpha_1) & \text{for WPA.} \end{cases} \end{aligned}$$

□

Theorem 2. *In the initial state of the PRGA, we have*

$$\Pr(S_0[i_1] = K[0]+K[1]+K[2]+3) \approx \tfrac{1}{N}\left(1 - \tfrac{2}{N}\right)\left(1 - \tfrac{1}{N}\right)^{N-2} + \tfrac{1}{N^2}\left(3 - \tfrac{2}{N}\right).$$

Proof. Since both $S_1^K[1] = 1$ and $S_2^K[2] = 2$ hold with high probability from Algorithm 1, we get

$$j_1^K = K[0], \tag{3}$$
$$j_2^K = K[0] + K[1] + S_1^K[1] = K[0] + K[1] + 1, \tag{4}$$
$$j_3^K = K[0] + K[1] + K[2] + S_1^K[1] + S_2^K[2] = K[0] + K[1] + K[2] + 3. \tag{5}$$

In this case, $S_3^K[2] = K[0]+K[1]+K[2]+3$ always holds from step 7 in Algorithm 1, and thus, event $(S_0[i_1] = K[0]+K[1]+K[2]+3)$ never occurs because $S_r^K[i_1] \neq K[0] + K[1] + K[2] + 3$ always holds for $r \geq 3$. Then, the probability of event $(S_0[i_1] = K[0] + K[1] + K[2] + 3)$ can be decomposed in two paths: $j_1^K = 1, 2$ (Path 1) and $j_1^K \neq 1, 2$ (Path 2). Path 2 is further divided into three subpaths: $j_2^K = 2$ (Path 2-1), $j_2^K \neq 2 \wedge K[2] = 254$ (Path 2-2) and $j_2^K \neq 2 \wedge K[2] \neq 254$ (Path 2-3). These paths include all events in order to compute $Pr(S_0[i_1] = K[0] + K[1] + K[2] + 3)$. In the following proof, we use $S_0[1]$ instead of $S_0[i_1]$ $(i_1 = 1)$ for simplicity.

Path 1. If $j_1^K = 1$, then $S_1^K[1] \neq 1$ from step 7 in Algorithm 1. Thus, $S_3^K[2] \neq K[0] + K[1] + K[2] + 3$ always holds since $j_3^K \neq K[0] + K[1] + K[2] + 3$ from Eq. (5). Similarly, if $j_1^K = 2$, then $S_3^K[2] \neq K[0] + K[1] + K[2] + 3$ always holds. Then, we assume that event $(S_0[1] = K[0] + K[1] + K[2] + 3)$ occurs with the probability of random association $\frac{1}{N}$. Therefore, we get

$$\Pr(S_0[1] = K[0] + K[1] + K[2] + 3 \mid \text{Path 1}) \approx \tfrac{1}{N}.$$

Path 2-1. As with the discussion in Path 1, if $j_2^K = 2$, then $S_3^K[2] \neq K[0] + K[1] + K[2] + 3$ always holds. We then assume that event $(S_0[1] = K[0] + K[1] + K[2] + 3)$ with the probability of random association $\frac{1}{N}$. Therefore, we get

$$\Pr(S_0[1] = K[0] + K[1] + K[2] + 3 \mid \text{Path 2-1}) \approx \tfrac{1}{N}.$$

Path 2-2. Except the cases in Paths 1 and 2-1, Eqs. (3)-(5) always hold since we get both $S_1^K[1] = 1$ and $S_2^K[2] = 2$. Here, if $K[2] = 254$, then $j_2^K = j_3^K = K[0] + K[1] + K[2] + 3$ holds since $K[2] + 3 = 1$. Thus, we get both $S_3^K[1] = K[0] + K[1] + K[2] + 3$ and $S_3^K[2] = 1$ from step 7 in Algorithm 1. After the third round of KSA, $S_r^K[1] = S_3^K[1]$ for $4 \leq r \leq N$ if $j_r^K \neq 1$ during the subsequent $N - 3$ rounds, whose probability is approximately $\left(1 - \frac{1}{N}\right)^{N-3}$ since we assume that $j_r^K = 1$ holds with the probability of random association $\frac{1}{N}$. Therefore, we get

$$\Pr(S_0[1] = K[0] + K[1] + K[2] + 3 \mid \text{Path 2-2}) \approx \left(1 - \tfrac{1}{N}\right)^{N-3}.$$

Path 2-3. As with the discussion in Path 2-2, Eqs. (3)-(5) always hold, and $j_2^K \neq j_3^K$ since $K[2] \neq 254$ from the assumption in Path 2-3. Thus, event $(S_0[i_1] = K[0] + K[1] + K[2] + 3)$ never occurs since $S_3^K[2] = K[0] + K[1] + K[2] + 3$ always holds. Therefore, we get

$$\Pr(S_0[1] = K[0] + K[1] + K[2] + 3 \mid \text{Path 2-3}) = 0.$$

In summary, event $(S_0[i_1] = K[0] + K[1] + K[2] + 3)$ occurs only in Paths 1, 2-1 and 2-2. Therefore, we get

$$\begin{aligned}
&\Pr(S_0[1] = K[0] + K[1] + K[2] + 3) \\
&\quad = \Pr(S_0[1] = K[0] + K[1] + K[2] + 3 \mid \text{Path 1}) \cdot \Pr(\text{Path 1}) \\
&\qquad + \Pr(S_0[1] = K[0] + K[1] + K[2] + 3 \mid \text{Path 2-1}) \cdot \Pr(\text{Path 2-1}) \\
&\qquad + \Pr(S_0[1] = K[0] + K[1] + K[2] + 3 \mid \text{Path 2-2}) \cdot \Pr(\text{Path 2-2}) \\
&\quad \approx \tfrac{1}{N} \cdot \tfrac{2}{N} + \tfrac{1}{N} \cdot \tfrac{1}{N}\big(1 - \tfrac{2}{N}\big) + \big(1 - \tfrac{1}{N}\big)^{N-3} \cdot \tfrac{1}{N}\big(1 - \tfrac{1}{N}\big)\big(1 - \tfrac{2}{N}\big) \\
&\quad = \tfrac{1}{N}\big(1 - \tfrac{2}{N}\big)\big(1 - \tfrac{1}{N}\big)^{N-2} + \tfrac{1}{N^2}\big(3 - \tfrac{2}{N}\big),
\end{aligned}$$

where we assume that 4 events, $(j_1^K = 1)$, $(j_1^K = 2)$, $(j_2^K = 2)$ and $(K[2] = 254)$, occur with the probability of random association $\frac{1}{N}$, respectively. □

3.3 Proof of biases in $S_1[i_2]$

In this section, we prove Theorems 3-5 theoretically. Theorem 3 shows that event $(S_1[i_2] = K[0] + K[1] + K[2] + 3)$ occurs with pretty high probability in both generic RC4 and WPA. This high probability is induced by Roos' bias, that is $\alpha_2 = \Pr(S_0[2] = K[0] + K[1] + K[2] + 3)$. Theorems 4 and 5 show that 4 events related to $S_1[i_2]$ yield a positive bias in both generic RC4 and WPA. We note that Theorems 3-5 mean the second round internal state of $S_1[i_2]$ can be guessed in pretty high probability or double probabilities of random association $\frac{1}{N}$ by using *known* $K[0]$, $K[1]$ and $K[2]$ in WPA. Here, we show only the proofs of Theorems 3 and 4. Theorem 5 is proved in the same way as Theorem 4. In order to prove the following theorems, let us denote the results of Theorems 2 and 3 as $\beta = \Pr(S_0[1] = K[0]+K[1]+K[2]+3)$ and $\gamma = \Pr(S_1[2] = K[0]+K[1]+K[2]+3)$, respectively.

Theorem 3. *After the first round of the PRGA, we have*

$$\Pr(S_1[i_2]=K[0]+K[1]+K[2]+3) \approx \beta\cdot\Pr(S_0[1]=2) + \alpha_2\cdot\big(1 - \Pr(S_0[1]=2)\big).$$

Proof. The probability of event $(S_1[i_2] = K[0] + K[1] + K[2] + 3)$ can be decomposed in two paths: $j_1 = 2$ (Path 1) and $j_1 \neq 2$ (Path 2). These paths include all events in order to compute $Pr(S_1[i_2] = K[0] + K[1] + K[2] + 3)$. Note that $j_1 = S_0[1]$ from step 4 in Alforithm 2. In the following proof, we use $S_1[2]$ instead of $S_1[i_2]$ $(i_2 = 2)$ for simplicity.

Path 1. In $j_1 = 2$, event $(S_1[2] = K[0] + K[1] + K[2] + 3)$ occurs if and only if $S_0[1] = K[0] + K[1] + K[2] + 3$ from step 5 in Algorithm 2. We assume that both events $(j_1 = 2)$ and $(S_0[1] = K[0] + K[1] + K[2] + 3)$ are mutually independent. Therefore, we get

$$\Pr(S_1[2] = K[0] + K[1] + K[2] + 3 \mid \text{Path 1}) = \beta.$$

Path 2. In $j_1 \neq 2$, event $(S_1[2] = K[0] + K[1] + K[2] + 3)$ occurs if and only if $S_0[2] = K[0] + K[1] + K[2] + 3$ from step 5 in Algorithm 2. We assume that both events $(j_1 \neq 2)$ and $(S_0[2] = K[0] + K[1] + K[2] + 3)$ are mutually independent. Therefore, we get

$$\Pr(S_1[2] = K[0] + K[1] + K[2] + 3 \mid \text{Path 2}) = \alpha_2.$$

In summary, we get

$$\begin{aligned}
&\Pr(S_1[i_2] = K[0] + K[1] + K[2] + 3) \\
&\quad = \Pr(S_1[2] = K[0] + K[1] + K[2] + 3 \mid \text{Path 1}) \cdot \Pr(\text{Path 1}) \\
&\qquad + \Pr(S_1[2] = K[0] + K[1] + K[2] + 3 \mid \text{Path 2}) \cdot \Pr(\text{Path 2}) \\
&\quad \approx \beta \cdot \Pr(S_0[1] = 2) + \alpha_2 \cdot \big(1 - \Pr(S_0[1] = 2)\big),
\end{aligned}$$

where the probability of event $(S_0[1] = 2)$ is taken from Propositions 2 and 4 in generic RC4 and WPA, respectively. □

Theorem 4. *After the first round of the PRGA, we have*

$$\Pr(S_1[i_2] = -K[0] - K[1] + K[2] - 1) \approx \begin{cases} \frac{2}{N}\gamma + \frac{1}{N}\big(1 - \frac{2}{N}\big)(1 - \gamma) & \textit{for RC4,} \\ \frac{4}{N}\gamma + \frac{1}{N}\big(1 - \frac{4}{N}\big)(1 - \gamma) & \textit{for WPA.} \end{cases}$$

Proof. The probability of event $(S_1[i_2] = -K[0] - K[1] + K[2] - 1)$ can be decomposed in two paths: $K[0] + K[1] = 126, 254$ (Path 1) and $K[0] + K[1] \neq 126, 254$ (Path 2). These paths include all events in order to compute $Pr(S_1[i_2] = -K[0] - K[1] + K[2] - 1)$. In the following proof, we use $S_1[2]$ instead of $S_1[i_2]$ $(i_2 = 2)$ for simplicity.

Path 1. In $K[0] + K[1] = 126, 254$, event $(S_1[2] = -K[0] - K[1] + K[2] - 1)$ occurs if and only if $S_1[2] = K[0] + K[1] + K[2] + 3$. Therefore, we get

$$\Pr(S_1[2] = -K[0] - K[1] + K[2] - 1 \mid \text{Path 1}) = \gamma.$$

Path 2. In $K[0] + K[1] \neq 126, 254$, event $(S_1[2] = -K[0] - K[1] + K[2] - 1)$ never occurs if $S_1[2] = K[0]+K[1]+K[2]+3$. If $S_1[2] \neq K[0]+K[1]+K[2]+3$ holds, then we assume that event $(S_1[2] = -K[0] - K[1] + K[2] - 1)$ occurs with the probability of random association $\frac{1}{N}$. Therefore, we get

$$\Pr(S_1[2] = -K[0] - K[1] + K[2] - 1 \mid \text{Path 2}) = \tfrac{1}{N} \cdot (1 - \gamma).$$

The probability of $K[0]+K[1] = 126$ and 254 in WPA is $\frac{2}{N}$, twice as high as that of random association, although that in generic RC4 is $\frac{1}{N}$ since K is generated uniformly at random. By substituting each $\Pr(K[0] + K[1] = 126, 254)$ in both generic RC4 and WPA, we get

$$\begin{aligned}
&\Pr(S_1[i_2] = -K[0] - K[1] + K[2] - 1) \\
&\quad = \Pr(S_1[2] = -K[0] - K[1] + K[2] - 1 \mid \text{Path 1}) \cdot \Pr(\text{Path 1}) \\
&\qquad + \Pr(S_1[2] = -K[0] - K[1] + K[2] - 1 \mid \text{Path 2}) \cdot \Pr(\text{Path 2}) \\
&\quad \approx \begin{cases} \frac{2}{N}\gamma + \frac{1}{N}\big(1 - \frac{2}{N}\big)(1 - \gamma) & \text{for RC4,} \\ \frac{4}{N}\gamma + \frac{1}{N}\big(1 - \frac{4}{N}\big)(1 - \gamma) & \text{for WPA.} \end{cases}
\end{aligned}$$

□

Theorem 5. *After the first round of the PRGA for $x \in \{-3, -1, 1\}$, we have*

$$\Pr(S_1[i_2] = K[0] - K[1] + K[2] + x) \approx \begin{cases} \frac{2}{N}\gamma + \frac{1}{N}\left(1 - \frac{2}{N}\right)(1-\gamma) & \textit{for RC4,} \\ \frac{4}{N}\gamma + \frac{1}{N}\left(1 - \frac{4}{N}\right)(1-\gamma) & \textit{for WPA.} \end{cases}$$

3.4 Proof of biases in j_2

In this section, we prove Theorems 6-10 theoretically. Theorem 6 shows that event $(j_2 = K[2])$ yields a positive bias in both generic RC4 and WPA. On the other hand, Theorems 7-10 show that 7 events related to j_2 yield positive biases in WPA but those are not biases in generic RC4. Here, we show only the proof of Theorem 6. Theorems 7-10 are proved in the same way as Theorem 6. In order to prove the following theorems, let us denote the result of Theorem 3 as $\gamma = \Pr(S_1[2] = K[0] + K[1] + K[2] + 3)$.

Theorem 6. *After the second round of the PRGA, we have*

$$\Pr(j_2 = K[2]) \approx \begin{cases} \frac{2}{N}\alpha_1\gamma + \frac{1}{N}\left(1 - \frac{2}{N}\right)(1-\alpha_1\gamma) & \textit{for RC4,} \\ \frac{4}{N}\alpha_1\gamma + \frac{1}{N}\left(1 - \frac{4}{N}\right)(1-\alpha_1\gamma) & \textit{for WPA.} \end{cases}$$

Proof. The probability of event $(j_2 = K[2])$ can be decomposed in two paths: $K[0]+K[1] = 126, 254$ (Path 1) and $K[0]+K[1] \neq 126, 254$ (Path 2). These paths include all events in order to compute $Pr(j_2 = K[2])$. Note that $j_2 = S_0[1]+S_1[2]$ from step 4 in Algorithm 2.

Path 1. If two events $(S_0[1] = K[0] + K[1] + 1)$ and $(S_1[2] = K[0] + K[1] + K[2] + 3)$ occur simultaneously, we get

$$\begin{aligned} j_2 = S_0[1] + S_1[2] &= (K[0] + K[1] + 1) + (K[0] + K[1] + K[2] + 3) \\ &= 2K[0] + 2K[1] + K[2] + 4. \end{aligned}$$

Then, in $K[0] + K[1] = 126, 254$, event $(j_2 = K[2])$ occurs if and only if $j_2 = 2K[0] + 2K[1] + K[2] + 4$, that is both $S_0[1] = K[0] + K[1] + 1$ and $S_1[2] = K[0] + K[1] + K[2] + 3$ hold simultaneously. We assume that both events $(S_0[1] = K[0] + K[1] + 1)$ and $(S_1[2] = K[0] + K[1] + K[2] + 3)$ are mutually independent. Therefore, we get

$$\Pr(j_2 = K[2] \mid \text{path 1}) = \alpha_1\gamma.$$

Path 2. In $K[0] + K[1] \neq 126, 254$ event $(j_2 = K[2])$ never occurs if and only if $j_2 = 2K[0] + 2K[1] + K[2] + 4$. If either $S_0[1] \neq K[0] + K[1] + 1$ or $S_1[2] \neq K[0] + K[1] + K[2] + 3$ hold, then we assume that event $(j_2 = K[2])$ occurs with the probability of random association $\frac{1}{N}$. Therefore, we get

$$\Pr(j_2 = K[2] \mid \text{Path 2}) = \tfrac{1}{N} \cdot (1 - \alpha_1\gamma).$$

The probability of $K[0]+K[1] = 126$ and 254 in WPA is $\frac{2}{N}$, twice as high as that of random association, although that in generic RC4 is $\frac{1}{N}$ since K is generated uniformly at random. By substituting each $\Pr(K[0] + K[1] = 126, 254)$ in both generic RC4 and WPA, we get

$$\begin{aligned}\Pr(j_2 = K[2]) &= \Pr(j_2 = K[2] \mid \text{Path 1}) \cdot \Pr(\text{Path 1}) \\ &\quad + \Pr(j_2 = K[2] \mid \text{Path 2}) \cdot \Pr(\text{Path 2}) \\ &\approx \begin{cases} \frac{2}{N}\alpha_1\gamma + \frac{1}{N}\left(1 - \frac{2}{N}\right)(1 - \alpha_1\gamma) & \text{for RC4,} \\ \frac{4}{N}\alpha_1\gamma + \frac{1}{N}\left(1 - \frac{4}{N}\right)(1 - \alpha_1\gamma) & \text{for WPA.} \end{cases}\end{aligned}$$

□

Theorem 7. *After the second round of the PRGA for $x \in \{-2, 0, 2\}$, we have*

$$\begin{aligned}&\Pr(j_2 = -K[0] - K[1] + K[2] + x) \\ &\quad \approx \begin{cases} \frac{1}{N}\alpha_1\gamma + \frac{1}{N}\left(1 - \frac{1}{N}\right)(1 - \alpha_1\gamma) & \textit{for RC4,} \\ \frac{2}{N}\alpha_1\gamma + \frac{1}{N}\left(1 - \frac{2}{N}\right)(1 - \alpha_1\gamma) & \textit{if } x = -2, 2 \textit{ for WPA,} \\ \frac{4}{N}\alpha_1\gamma + \frac{1}{N}\left(1 - \frac{4}{N}\right)(1 - \alpha_1\gamma) & \textit{if } x = 0 \textit{ for WPA.} \end{cases}\end{aligned}$$

Theorem 8. *After the second round of the PRGA, we have*

$$\Pr(j_2 = -K[0] + K[1] + K[2]) \approx \begin{cases} \frac{1}{N}\alpha_1\gamma + \frac{1}{N}\left(1 - \frac{1}{N}\right)(1 - \alpha_1\gamma) & \textit{for RC4,} \\ \frac{4}{N}\alpha_1\gamma + \frac{1}{N}\left(1 - \frac{4}{N}\right)(1 - \alpha_1\gamma) & \textit{for WPA.} \end{cases}$$

Theorem 9. *After the second round of the PRGA for $x \in \{-2, 3\}$, we have*

$$\Pr(j_2 = -K[1] + K[2] + x) \approx \begin{cases} \frac{1}{N}\alpha_1\gamma + \frac{1}{N}\left(1 - \frac{1}{N}\right)(1 - \alpha_1\gamma) & \textit{for RC4,} \\ \frac{4}{N}\alpha_1\gamma + \frac{1}{N}\left(1 - \frac{4}{N}\right)(1 - \alpha_1\gamma) & \textit{for WPA.} \end{cases}$$

Theorem 10. *After the second round of the PRGA, we have*

$$\Pr(j_2 = K[0] - K[1] + K[2]) \approx \begin{cases} \frac{1}{N}\alpha_1\gamma + \frac{1}{N}\left(1 - \frac{1}{N}\right)(1 - \alpha_1\gamma) & \textit{for RC4,} \\ \frac{4}{N}\alpha_1\gamma + \frac{1}{N}\left(1 - \frac{4}{N}\right)(1 - \alpha_1\gamma) & \textit{for WPA.} \end{cases}$$

3.5 Experimental results

We have conducted experiments on Theorems 1-10 in the following environment in order to confirm the accuracy of theorems: Intel(R) Core(TM) i3-3220M CPU with 3.30 GHz, 3.8 GiB memory, gcc 4.8.2 compiler and C language. The number of samples necessary for our experiments is at least $\mathcal{O}(N^3)$ according to Proposition 5. This is why each correlation has a relative bias with the probability of at least $\mathcal{O}(\frac{1}{N})$. Then, we have used N^5 randomly generated RC4 keys in both generic RC4 and WPA. The number of these samples satisfies a condition to distinguish each correlation from random distribution with constant probability

of success. We also evaluate the percentage of relative error ϵ of experimental values compared with theoretical values in the same way as [5]:

$$\epsilon = \frac{|\text{experimental value} - \text{theoretical value}|}{\text{experimental value}} \times 100(\%).$$

Tables 2 and 3 show experimental and theoretical values and percentage of relative error ϵ in both generic RC4 and WPA.

Table 2. Comparison between experimental and theoretical results for generic RC4

Linear correlation		Experimental value	Theoretical value	ϵ (%)
$S_0[i_1]$	$-K[0] - K[1] - 3$	0.005333309	0.005325263	0.151
	$K[0] + K[1] + K[2] + 3$	0.001490745	0.001479853	0.730
$S_1[i_2]$	$K[0] + K[1] + K[2] + 3$	0.360360690	0.362016405	0.459
	$-K[0] - K[1] + K[2] - 1$	0.005305673	0.005302926	0.052
	$K[0] - K[1] + K[2] - 3$	0.005295155	0.005302926	0.147
	$K[0] - K[1] + K[2] - 1$	0.005289180	0.005302926	0.260
	$K[0] - K[1] + K[2] + 1$	0.005309594	0.005302926	0.126
j_2	$K[2]$	0.004430372	0.004401230	0.658
	$-K[0] - K[1] + K[2] - 2$	0.003920799	0.003893028	0.708
	$-K[0] - K[1] + K[2]$	0.003919381	0.003893028	0.672
	$-K[0] - K[1] + K[2] + 2$	0.003910929	0.003893028	0.458
	$-K[0] + K[1] + K[2]$	0.003920399	0.003893028	0.698
	$-K[1] + K[2] - 2$	0.003910053	0.003893028	0.435
	$-K[1] + K[2] + 3$	0.003897939	0.003893028	0.126
	$K[0] - K[1] + K[2]$	0.003917895	0.003893028	0.635

Table 3. Comparison between experimental and theoretical results for WPA

Linear correlation		Experimental value	Theoretical value	ϵ (%)
$S_0[i_1]$	$-K[0] - K[1] - 3$	0.008408305	0.008182569	2.685
	$K[0] + K[1] + K[2] + 3$	0.001491090	0.001479853	0.754
$S_1[i_2]$	$K[0] + K[1] + K[2] + 3$	0.361751935	0.362723221	0.268
	$-K[0] - K[1] + K[2] - 1$	0.008174625	0.008115732	0.720
	$K[0] - K[1] + K[2] - 3$	0.008140906	0.008115732	0.309
	$K[0] - K[1] + K[2] - 1$	0.008147205	0.008115732	0.386
	$K[0] - K[1] + K[2] + 1$	0.008150390	0.008115732	0.425
j_2	$K[2]$	0.005560613	0.005417633	2.571
	$-K[0] - K[1] + K[2] - 2$	0.004573276	0.004401230	3.762
	$-K[0] - K[1] + K[2]$	0.005562336	0.005417633	2.601
	$-K[0] - K[1] + K[2] + 2$	0.004543826	0.004401230	3.138
	$-K[0] + K[1] + K[2]$	0.005490766	0.005417633	1.332
	$-K[1] + K[2] - 2$	0.005468425	0.005417633	0.929
	$-K[1] + K[2] + 3$	0.005468472	0.005417633	0.930
	$K[0] - K[1] + K[2]$	0.005607004	0.005417633	3.377

We see that ϵ is small enough in each case in generic RC4 such as $\epsilon \leq 0.730$ (%). From this results, we have convinced that theoretical values closely reflects the experimental values in generic RC4.

We also see that theoretical biases in $S_0[i_1]$ and j_2 in WPA produce slightly big ϵ such as 3.762 (%) but those in $S_1[i_2]$ in WPA is quite small in the same way as generic RC4. Let us investigate why such differences on the percentage of relative error are produced between generic RC4 and WPA. Actually, difference between generic RC4 and WPA exist only in a relation between $K[0]$ and $K[1]$. Therefore, these difference influence theoretical biases in the early round, but seem to attenuate in the second or more round as we see in results to $S_0[i_1]$ and $S_1[i_2]$.

4 Conclusion

In this paper, we have focused on linear correlations including *unknown* internal states as well as the keystream byte and *known* RC4 key bytes in both generic RC4 and WPA, and provided newly theoretical proofs of 15 linear correlations related to $S_0[i_1]$, $S_1[i_2]$ and j_2. For example, event $(S_1[i_2] = K[0]+K[1]+K[2]+3)$ yields a pretty high probability in both generic RC4 and WPA, influenced directly by Roos' bias; and the probability of 5 linear correlations such as $\Pr(S_0[i_1] = -K[0] - K[1] - 3)$, $\Pr(S_1[i_2] = -K[0] - K[1] + K[2] - 1)$ and $\Pr(S_1[i_2] = K[0] - K[1] + K[2] + x)$ for $x \in \{-3, -1, 1\}$ is a double probability of random association $\frac{1}{N}$ in WPA.

Our theoretical analysis are expected to contribute from the following two viewpoints. One is to contribute to reducing the computational complexity necessary for the state recovery attacks against RC4 proposed in [1, 6, 9] especially with WPA since our linear correlations includes internal states. The other is to contribute to construct a key generation procedure with IV in such a way that it keeps or further enhance the security level of its original symmetric cipher. In our analysis, we have seen how TKIP downgrades security level of generic RC4 theoretically. These discussions could be generalized to reconstruct a key generation procedure with IV.

References

1. Apurba Das, Subhamoy Maitra, Goutam Paul, and Santanu Sarkar. Some Combinatorial Results towards State Recovery Attack on RC4. In Sushil Jajodia and Chandan Mazumdar, editors, *Information Systems Security - ICISS 2011*, volume 7093 of *Lecture Notes in Computer Science*, pages 204–214. Springer Berlin Heidelberg, 2011.
2. Scott Fluhrer, Itsik Mantin, and Adi Shamir. Weaknesses in the Key Scheduling Algorithm of RC4. In Serge Vaudenay and Amr M. Youssef, editors, *Selected Areas in Cryptography - SAC 2001*, volume 2259 of *Lecture Notes in Computer Science*, pages 1–24. Springer Berlin Heidelberg, 2001.

3. Sourav Sen Gupta, Subhamoy Maitra, Willi Meier, Goutam Paul, and Santanu Sarkar. Dependence in IV-related bytes of RC4 key enhances vulnerabilities in WPA. In *Fast Software Encryption - FSE 2014*. To appear, 2014.
4. Takanori Isobe, Toshihiro Ohigashi, Yuhei Watanabe, and Masakatu Morii. Full Plaintext Recovery Attack on Broadcast RC4. In Shiho Moriai, editor, *Fast Software Encryption - FSE 2013*, volume 8424 of *Lecture Notes in Computer Science*. Springer Berlin Heidelberg, 2014.
5. Ryoma Ito and Atsuko Miyaji. New Linear Correlations related to State Information of RC4 PRGA using IV in WPA. In *Fast Software Encryption - FSE 2015*. To appear.
6. Lars R. Knudsen, Willi Meier, Bart Preneel, Vincent Rijmen, and Sven Verdoolaege. Analysis Methods for (Alleged) RC4. In Kazuo Ohta and Dingyi Pei, editors, *Advances in Cryptology - ASIACRYPT '98*, volume 1514 of *Lecture Notes in Computer Science*, pages 327–341. Springer Berlin Heidelberg, 1998.
7. Itsik Mantin. Analysis of the Stream Cipher RC4. Master's thesis, The Weizmann Institute of Science, Israel, 2001. http://www.wisdom.weizmann.ac.il/ itsik/RC4/rc4.html.
8. Itsik Mantin and Adi Shamir. Practical Attack on Broadcast RC4. In Mitsuru Matsui, editor, *Fast Software Encryption - FSE 2001*, volume 2355 of *Lecture Notes in Computer Science*, pages 152–164. Springer Berlin Heidelberg, 2002.
9. Alexander Maximov and Dmitry Khovratovich. New State Recovery Attack on RC4. In David Wagner, editor, *Advances in Cryptology - CRYPTO 2008*, volume 5157 of *Lecture Notes in Computer Science*, pages 297–316. Springer Berlin Heidelberg, 2008.
10. Goutam Paul and Subhamoy Maitra. Permutation After RC4 Key Scheduling Reveals the Secret Key. In Carlisle Adams, Ali Miri, and Michael Wiener, editors, *Selected Areas in Cryptography - SAC 2007*, volume 4876 of *Lecture Notes in Computer Science*, pages 360–377. Springer Berlin Heidelberg, 2007.
11. Andrew Roos. A class of weak keys in the RC4 stream cipher. Posts in sci.crypt, http://marcel.wanda.ch/Archive/WeakKeys, 1995.