New Linear Correlations related to State Information of RC4 PRGA using IV in WPA

Ryoma Ito and Atsuko Miyaji*

Japan Advanced Institute of Science and Technology
1-1 Asahidai, Nomi-shi, Ishikawa, 923-1292, Japan
{s1310005,miyaji}@jaist.ac.jp

Abstract. RC4 is a stream cipher designed by Ron Rivest in 1987, and is widely used in various applications. WPA is one of these applications, where TKIP is used for a key generation procedure to avoid weak IV generated by WEP. In FSE 2014, two different attacks against WPA were proposed by Sen Gupta et al. and Paterson et al. Both focused correlations between the keystream bytes and the first 3 bytes of the RC4 key in WPA. In this paper, we focus on linear correlations between *unknown* internal state and the first 3 bytes of the RC4 key in both generic RC4 and WPA, where the first 3 bytes of the RC4 key is *known* in WPA. As a result, we could discover various new linear correlations, and prove these correlations theoretically.

Keywords: RC4, WPA, linear correlations

1 Introduction

RC4 is a stream cipher designed by Ron Rivest in 1987, and is widely used in various applications 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 become a hot cryptanalysis target since its specification was made public on the internet in 1994.

WEP is a security protocol for IEEE 802.11 wireless networks, standardized in 1999. Various attacks against WEP, however, have been proposed in [7, 16, 17] after Fluhrer et al. showed a class of weak IV in 2001 [3], and WEP is considered to be broken completely today. In order to avoid the attack by Fluhrer et al. [3], WEP had been superseded by WPA in 2003. WPA improves a key scheduling procedure known as Temporary Key Integrity Protocol (TKIP) to avoid a class of weak IV generated in WEP. One of characteristic features in TKIP is that the first 3 bytes of the RC4 key $K[0]$, $K[1]$, and $K[2]$ are derived from IV, and then, they are public. The range of $K[1]$ is limited to either $[32, 63]$ or $[96, 127]$ in order to avoid the known WEP attacks by Fluhrer et al. [3].

In FSE 2014, Sen Gupta et al. showed a probability distribution of an addition of the first two bytes of the RC4 key, $K[0] + K[1]$, in detailed, and found that

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

some characteristic features including $K[0]+K[1]$ must be always even [4]. They also showed some linear correlations between the keystream bytes and the first *known* 3 bytes of the RC4 key in WPA. They applied these linear correlations to the existing plaintext recovery attack against SSL/TLS [6] with WPA, and improve its computational complexity required for the attack. In [13], Paterson et al. showed the specific correlations in WPA between the keystream bytes and a combination of IV by a different idea from [4]. They also improved the computational complexity required for the attack against WPA in comparison with the existing attack against SSL/TLS [1].

In this paper, we investigated new linear correlations among four *unknown* values $S_r[i_{r+1}]$, $S_r[j_{r+1}]$, j_{r+1} and t_{r+1} and the first *known* 3 bytes of the RC4 key $K[0]$, $K[1]$, and $K[2]$ in both generic RC4 and WPA. An important differences between ours and previous works [4, 13] is to whether analysis target is the internal states or the keystream bytes. The previous works are effective for the plaintext recovery attacks [1, 6]. On the other hand, our investigation is effective for the state recovery attacks [2, 8, 12]. In addition, we also focus on the difference between generic RC4 and WPA, and then, discover that there exist some different correlations between generic RC4 and WPA, which exactly reflect difference of distributions of the first 3 bytes of the RC4 key. Our motivation is to prove these linear correlations theoretically. Some of our proved significant biases are given as follows:

Theorem 1: $\Pr(S_0[i_1] = K[0])_{\mathrm{RC4}} \approx \frac{1}{N}\left(1-\frac{1}{N}\right)^{N-2}$;

Theorem 2: $\Pr(S_0[i_1] = K[0])_{\mathrm{WPA}} = 0$;

Theorem 3: $\Pr(S_0[i_1] = K[0] - K[1] - 3)$

$$\approx \begin{cases} \frac{2}{N}\alpha_1 + \frac{1}{N}\left(1-\frac{2}{N}\right)(1-\alpha_1) & \text{for RC4,} \\ \frac{4}{N}\alpha_1 + \frac{1}{N}\left(1-\frac{4}{N}\right)(1-\alpha_1) & \text{for WPA;} \end{cases}$$

Theorem 4: $\Pr(S_0[i_1] = K[0] - K[1] - 1)$

$$\approx \begin{cases} \frac{1}{N}\left(1+\frac{2}{N}\right)\alpha_1 + \frac{1}{N}\left(1-\frac{2}{N}\right)(1-\alpha_1) & \text{for RC4,} \\ \frac{4}{N}\alpha_1 + \frac{1}{N}\left(1-\frac{4}{N}\right)(1-\alpha_1) & \text{for WPA;} \end{cases}$$

Theorem 5: $\Pr(S_{255}[i_{256}] = K[0])$

$$\approx \alpha_0\left(1-\tfrac{1}{N}\right)^{255} + \tfrac{1}{N}(1-\alpha_0)\left(1-\left(1-\tfrac{1}{N}\right)^{255}\right);$$

Theorem 6: $\Pr(S_{255}[i_{256}] = K[1])$

$$\approx \delta\left(1-\tfrac{1}{N}\right)^{255} + \tfrac{1}{N}(1-\delta)\left(1-\left(1-\tfrac{1}{N}\right)^{255}\right);$$

Theorem 7: $\Pr(S_r[i_{r+1}] = K[0] + K[1] + 1)$ $(0 \le r \le N)$

$$\approx \begin{cases} \alpha_1 & \text{if } r = 0, \\ \alpha_1\gamma_1 + (1-\beta_1)\epsilon_2 & \text{if } r = 1, \\ \epsilon_0\left(1-\frac{1}{N}\right)^{N-1} + \frac{1}{N}(1-\epsilon_0)\left(1-\left(1-\frac{1}{N}\right)^{N-1}\right) & \text{if } r = N-1, \\ \zeta_1\left(1-\frac{1}{N}\right)^{N-1} + \frac{1}{N}(1-\zeta_1)\left(1-\left(1-\frac{1}{N}\right)^{N-1}\right) & \text{if } r = N, \\ \zeta_{r+1}\left(1-\frac{1}{N}\right)^{r-1} + \frac{1}{N}\sum_{x=1}^{r-1}\eta_x\left(1-\frac{1}{N}\right)^{r-x-1} & \text{otherwise,} \end{cases}$$

where $\alpha_0 = \Pr(S_0[0] = K[0])$, $\alpha_1 = \Pr(S_0[1] = K[0] + K[1] + 1)$, $\beta_1 = \Pr(S_0[S_0[1]] = K[0]+K[1]+1)$, $\gamma_1 = \Pr(K[0]+K[1] = 1)$, $\delta = \Pr(S_0[0] = K[1])$, $\epsilon_0 = \Pr(S_0[0] = K[0] + K[1] + 1)$, $\zeta_r = \Pr(S_1[r] = K[0] + K[1] + 1)$ and $\eta_r = \Pr(S_r[i_{r+1}] = K[0] + K[1] + 1)$. Both α_0 and α_1 are Roos' biases [15], and β_1 is one of Nested Roos' biases [9].

These newly demonstrated correlations could be added to the known set of biases for $S_r[i_{r+1}]$, $S_r[j_{r+1}]$, j_{r+1} and t_{r+1} for $r \geq 0$ on *known* key bytes in WPA, and could improve some state recovery attacks against RC4.

This paper is organized as follows: Section 2 briefly summarizes notation, RC4 algorithms and key scheduling procedure in WPA. Section 3 presents the previous works on Roos' biases [14, 15], Nested Roos' biases [9] and the distribution of $K[0] + K[1]$ in WPA [4]. Section 4 first discusses some linear correlations observed by our experiments, and shows theoretical proofs. Section 5 demonstrates experimental simulations. Section 6 concludes this paper.

2 Preliminary

2.1 Description of RC4

The following notation is used in this paper.

K, l : secret key, the length of secret key (bytes)
r : number of rounds
N : number of arrays in state (typically $N = 256$)
S_r^K : state of KSA after the swap in the r-th round
S_r : state of PRGA after the swap in the r-th round
i, j_r^K : indices of S_r^K for the r-th round
i_r, j_r : indices of S_r for the r-th round
Z_r : one output keystream for the r-th round
t_r : index of Z_r

RC4 consists of two algorithms: Key Scheduling Algorithm (KSA) and Pseudo Random Generation Algorithm (PRGA). KSA generates the state S_N^K from a secret key K of l bytes as described in Algorithm 1. Then, the final state S_N^K in KSA becomes the input of PRGA as S_0. Once the state S_0 is computed, PRGA generates a keystream byte Z_r in each round as described in Algorithm 2. The keystream byte Z_r will be XORed with a plaintext to generate a ciphertext.

Algorithm 1 KSA

for $i = 0$ to $N - 1$ **do**
  $S_0^K[i] \leftarrow i$
end for
$j_0^K \leftarrow 0$
for $i = 0$ to $N - 1$ **do**
  $j_{i+1}^K \leftarrow j_i^K + S_i^K[i] + K[i \mod l]$
  Swap$(S_i^K[i], S_i^K[j_{i+1}^K])$
end for

Algorithm 2 PRGA

$r \leftarrow 0$, $i_0 \leftarrow 0$, $j_0 \leftarrow 0$
loop
  $r \leftarrow r + 1$, $i_r \leftarrow i_{r-1} + 1$
  $j_r \leftarrow j_{r-1} + S_{r-1}[i_r]$
  Swap$(S_{r-1}[i_r], S_{r-1}[j_r])$
  $t_r \leftarrow S_r[i_r] + S_r[j_r]$
  Output: $Z_r \leftarrow S_r[t_r]$
end loop

2.2 Description of WPA

In order to generate a 16-byte RC4 secret key, WPA uses two key scheduling procedures: a key management scheme and the TKIP, which includes a temporal key hash function [5] to generate RC4 secret key and a message integrity code function to ensure integrity of the message. The key management scheme after the authentication based on IEEE 802.1X generates a 16-byte Temporal Key (TK). Then, the TK, a 6-byte Transmitter Address and a 48-bit IV, which is a sequence counter, are given as the inputs to the temporal key hash function. The temporal key hash function generates the last 13 bytes of the RC4 key. The remaining RC4 key, the first 3 bytes, is computed by the last 16 bits of IV (IV16) as follows:

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

Note that the range of $K[1]$ is limited to either $[32, 63]$ or $[96, 127]$ in order to avoid the known WEP attack by Fluhrer et al. [3].

3 Previous works

In 1995, Roos' biases [15], correlations between RC4 key bytes and the initial state S_0 of PRGA, are proved in [14] and given as follows:

Proposition 1 ([14, Corollary 2]). *In the initial state of PRGA for* $0 \le y \le N-1$*, we have*

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

In FSE 2008, Maitra and Paul showed correlations similar to Roos' biases [9], so called Nested Roos' biases in [10]. Nested Roos' biases are given as follows:

Proposition 2 ([9, Theorem 2]). *In the initial state of PRGA for* $0 \le y \le 31$*,* $\Pr(S_0[S_0[y]] = f_y)$ *is approximately*

$$\left(\frac{y}{N} + \frac{1}{N}\left(1 - \frac{1}{N}\right)^{2-y} + \left(1 - \frac{y}{N}\right)^{2}\left(1 - \frac{1}{N}\right)\right)\left(1 - \frac{1}{N}\right)^{\frac{y(y+1)}{2} + 2N - 4},$$

where $f_y = \frac{y(y+1)}{2} + \sum_{x=0}^{y} K[x]$.

In FSE 2014, Sen Gupta et al. showed that the distribution of $K[0] + K[1]$ has biases from a relation between $K[0]$ and $K[1]$ generated by the temporal key hash function in WPA [4]. This distribution is given as follows:

Proposition 3 ([4, 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:*

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

They also showed that Proposition 3 combining Roos' biases shown in Proposition 1 induced a characteristic bias on the distribution of the initial state $S_0[1]$ of PRGA, which deeply influences on the biases of the first keystream byte Z_1, etc.

4 New linear correlations

4.1 Experimental observation

Let us investigate new correlations of four unknown values $S_r[i_{r+1}]$, $S_r[j_{r+1}]$, j_{r+1} and t_{r+1} for $r \ge 0$. Other linear correlations of the keystream bytes Z_r are investigated in [4]. Let $X_r \in \{S_r[i_{r+1}], S_r[j_{r+1}], j_{r+1}, t_{r+1}\}$, $a,b,c,d \in \{0,\pm 1\}$ and $e \in \{0,\pm 1,\pm 2,\pm 3\}$,

$$X_r = a \cdot Z_{r+1} + b \cdot K[0] + c \cdot K[1] + d \cdot K[2] + e. \tag{1}$$

These biases by Eq. (1) can be added to the known set of biases for $S_r[i_{r+1}]$, $S_r[j_{r+1}]$, j_{r+1} and t_{r+1} for $r \ge 0$ on known keys in WPA such as $K[0]$, $K[1]$ and $K[2]$, and may reduce the computational complexity of the existing state recovery attacks against RC4 [2, 8, 12] especially in WPA.

We have examined all $4 \cdot 3^4 \cdot 7$ equations defined by Eq. (1) in each round with 2^{32} randomly generated 16-byte keys in both generic RC4 and WPA. Some notable experimental results are presented in Tables 1 and 3. Due to lack of space, only the results of correlations with more than 0.0048 or less than 0.0020 in either generic RC4 or WPA are listed. We stress that the case of $S_0[i_1] = K[0]$ in WPA becomes an impossible condition (probability 0), and thus, $S_0[i_1]$ is varied from $[0, N-1] \backslash \{K[0]\}$. Our motivation is to prove these linear correlations theoretically shown in Table 1.

In order to prove the following theorems, we often use Roos' biases (Proposition 1), Nested Roos' biases (Proposition 2) and the probability of $K[0]+K[1] = v$ (Proposition 3), which are denoted by $\alpha_y = \Pr(S_0[y] = \frac{y(y+1)}{2} + \sum_{x=0}^{y} K[x])$, $\beta_y = \Pr(S_0[S_0[y]] = \frac{y(y+1)}{2} + \sum_{x=0}^{y} K[x])$ and $\gamma_v = \Pr(K[0]+K[1]=v)$, respectively. From uniform randomness of RC4 stream cipher, we assume that the probability of certain events (e.g. the state information) that we have confirmed experimentally that there are no significant biases is $\frac{1}{N}$ due to random association for the proofs. Furthermore, we assume that the RC4 key is generated uniformly at random in generic RC4.

Table 1. Notable linear correlations in Eq. (1) for both generic RC4 and WPA

X_r	Linear correlations	RC4	WPA	Remarks
$S_0[i_1]$	$K[0]$	0.001450	0	Theorems 1 and 2
	$K[0] - K[1] - 3$	0.005337	0.007848	Theorem 3
	$K[0] - K[1] - 1$	0.003922	0.007877	Theorem 4
$S_{255}[i_{256}]$	$K[0]$	0.137294	0.138047	Theorem 5
	$K[1]$	0.003911	0.037189	Theorem 6
$S_r[i_{r+1}]$	$K[0] + K[1] + 1$	Fig. 1		Theorem 7

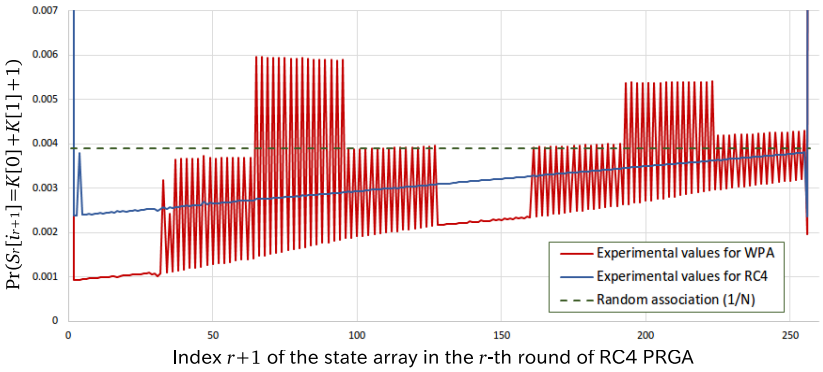

Fig. 1. Observation result of event $(S_r[i_{r+1}] = K[0] + K[1] + 1)$

4.2 Bias in $S_0[i_1]$ for both generic RC4 and WPA

In this section, we prove Theorems 1-4. Theorems 1 and 2 shows that $S_0[i_1] = K[0]$ holds with low probability and 0 in generic RC4 and WPA, respectively. Theorems 3 and 4 show that both $S_0[i_1] = K[0] - K[1] - 3$ and $K[0] - K[1] - 1$ in WPA hold twice as frequently as probability $\frac{1}{N}$ due to random association. Theorem 3 also shows that event $(S_0[i_1] = K[0] - K[1] - 3)$ provides a case with positive bias in generic RC4.

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

$$\Pr(S_0[i_1] = K[0])_{\mathrm{RC4}} \approx \frac{1}{N}\left(1 - \frac{1}{N}\right)^{N-2}.$$

Proof. Fig. 2 shows a state transition diagram in the first 2 rounds of KSA. From step 6 in Algorithm 1, both $j_1^K = j_0^K + S_0^K[0] + K[0] = 0 + 0 + K[0] = K[0]$ and $j_2^K = j_1^K + S_1^K[1] + K[1] = K[0] + K[1] + S_1^K[1]$ hold. The probability of event $(S_0[i_1] = K[0])$ can be decomposed in three paths: $K[0] + K[1] = 0$ (Path 1), $K[0] + K[1] = 255$ (Path 2) and $K[0] + K[1] \neq 0, 255$ (Path 3). Both Paths 1 and 2 are further divided into two subpaths: $K[0] = 1$ (Paths 1-1 and 2-1) and

$K[0] \neq 1$ (Paths 1-2 and 2-2), respectively. In the following proof, we use $S_0[1]$ instead of $S_0[i_1]$ ($i_1 = 1$) and $S_N^K[1]$ for simplicity.

Path 1-1. Fig. 3 shows a state transition diagram in Path 1-1. After the second round of KSA, $S_2^K[1] = K[0]$ always holds since $j_1^K = K[0] = 1$ and $j_2^K = K[0]+K[1]+S_1^K[1] = 0+0 = 0$. Furthermore, $S_r^K[1] = S_2^K[1]$ for $3 \leq r \leq N$ if $j_r^K \neq 1$ during the subsequent $N-2$ rounds, whose probability is $\left(1-\frac{1}{N}\right)^{N-2}$ approximately. Thus, the probability in Path 1-1 is given as follows:

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

Path 1-2. Fig. 4 shows a state transition diagram in Path 1-2. $S_2^K[0] = K[0]$ always holds since $j_1^K = K[0] \neq 1$ and $j_2^K = (K[0]+K[1])+S_1^K[1] = 0+1 = 1$. Then, event $(S_0[1] = K[0])$ never occurs because $S_r^K[1] \neq K[0]$ always holds for $r \geq 2$. Thus, the probability in Path 1-2 is 0.

Path 2-1. Fig. 5 shows a state transition diagram in Path 2-1. $S_2^K[0] = K[0]$ always holds in the same way as Path 1-2. Then, event $(S_0[1] = K[0])$ never occurs. Thus, the probability in Path 2-1 is 0.

Path 2-2. Fig. 6 shows a state transition diagram in Path 2-2. $S_2^K[1] = K[0]$ always holds in the same way as Path 1-1. Then, event $(S_0[1] = K[0])$ occurs if $S_r[1] = S_2^K[1]$ for $3 \leq r \leq N$. Thus, the probability in Path 2-2 is given as follows:

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

Path 3. Fig. 2 shows a state transition diagram in Path 3. $S_2^K[0] = K[0]$ always holds in the same way as Paths 1-2 and 2-1. Then, event $(S_0[1] = K[0])$ never occurs. Thus, the probability in Path 3 is 0.

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

$$\begin{aligned}\Pr(S_0[i_1] = K[0]) &= \Pr(S_0[i_1] = K[0] \mid \text{Path 1-1}) \cdot \Pr(\text{Path 1-1}) \\ &\quad + \Pr(S_0[i_1] = K[0] \mid \text{Path 2-2}) \cdot \Pr(\text{Path 2-2}) \\ &\approx \left(1 - \frac{1}{N}\right)^{N-2} \cdot \frac{1}{N^2} + \left(1 - \frac{1}{N}\right)^{N-2} \cdot \frac{1}{N}\left(1 - \frac{1}{N}\right) = \frac{1}{N}\left(1 - \frac{1}{N}\right)^{N-2}. \quad \square\end{aligned}$$

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

$$\Pr(S_0[i_1] = K[0])_{\text{WPA}} = 0.$$

Proof. Note that event $(S_0[1] = K[0])$ occurs if and only if either $K[0]+K[1] = 0$ or 255, and that Proposition 3 shows that neither $K[0]+K[1] = 0$ nor 255 holds in WPA. Thus, the probability of event $(S_0[1] = K[0])$ in WPA is 0. $\square$

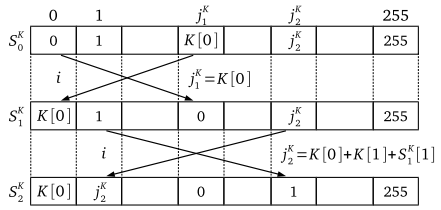

Fig. 2. A state transition diagram in the first 2 rounds of KSA

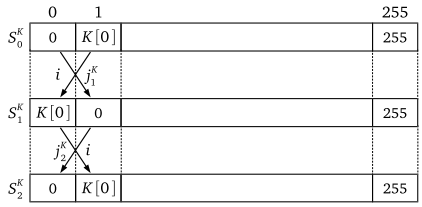

Fig. 3. Path 1-1 in Theorem 1

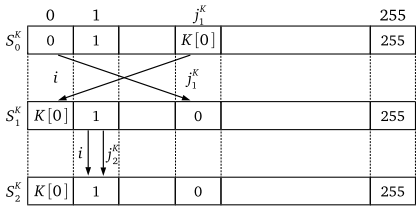

Fig. 4. Path 1-2 in Theorem 1

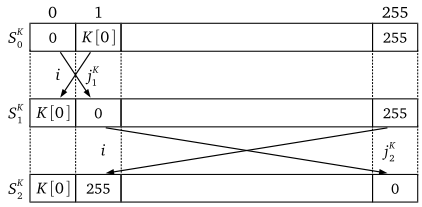

Fig. 5. Path 2-1 in Theorem 1

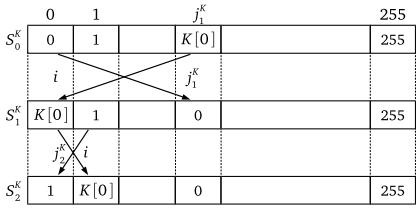

Fig. 6. Path 2-2 in Theorem 1

Theorem 3. *In the initial state of PRGA, we have*

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

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

Path 1. In $K[1] = 126, 254$, event $(S_0[1] = K[0] - K[1] - 3)$ occurs if and only if $S_0[1] = K[0] + K[1] + 1$. Thus, the probability in Path 1 is given as follows:

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

Path 2. In $K[1] \neq 126, 254$, 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 probability $\frac{1}{N}$ due to random association. Thus, the probability in Path 2 is given as follows:

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

In summary, we get

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

where $\alpha_1 = \Pr(S_0[1] = K[0] + K[1] + 1) \approx \left(\frac{N-1}{N}\right)^{N+2} + \frac{1}{N}$. □

The probability of $K[1] = 126$ or 254 in generic RC4 is $\frac{1}{N}$ in order to be generated uniformly at random. On the other hand, that of $K[1] = 126$ or 254 in WPA is $\frac{4}{N}$ or 0, respectively. Thus, Theorem 3 reflects the difference of $\Pr(K[1] = 126, 254)$ in both generic RC4 and WPA.

Theorem 4. *In the initial state of PRGA, we have*

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

Proof. The probability of event $(S_0[i_1] = K[0] - K[1] - 1)$ can be decomposed in three paths: $K[1] = 127$ (Path 1), $K[1] = 255$ (Path 2) and $K[1] \neq 127, 255$ (Path 3). In the following proof, we use $S_0[1]$ instead of $S_0[i_1]$ $(i_1 = 1)$ for simplicity.

Path 1. In $K[1] = 127$, event $(S_0[1] = K[0] - K[1] - 1)$ occurs if and only if $S_0[1] = K[0] + K[1] + 1$. Thus, the probability in Path 1 is given as follows:

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

Path 2. In $K[1] = 255$, event $(S_0[1] = K[0] - K[1] - 1)$ occurs if and only if $S_0[1] = K[0]+K[1]+1$, and $K[0]+K[1]+1 = K[0]-K[1]-1 = K[0]$. Then, from the discussion in Theorem 1, event $(S_0[1] = K[0])$ occurs if and only if either $(K[0] + K[1] = 0 \wedge K[0] = 1)$ or $(K[0] + K[1] = 255 \wedge K[0] \neq 1)$. So, assuming that both $K[1] = 255$ and $S_0[1] = K[0] + K[1] + 1$ hold, event $(S_0[1] = K[0] - K[1] - 1)$ occurs if and only if either $K[0] = 0$ or 1. Thus, the probability in Path 2 is given as follows:

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

Path 3. In $K[1] \neq 127, 255$, event $(S_0[1] = K[0] - K[1] - 1)$ 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 $(S_0[1] = K[0] - K[1] - 1)$ occurs with probability $\frac{1}{N}$ due to random association. Thus, the probability in Path 3 is given as follows:

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

In summary, we get

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

where $\alpha_1 = \Pr(S_0[1] = K[0] + K[1] + 1) \approx \left(\frac{N-1}{N}\right)^{N+2} + \frac{1}{N}$. □

For WPA, Theorems 3 and 4 show that $\Pr(S_0[i_1] = K[0] - K[1] - 3) = \Pr(S_0[i_1] = K[0] - K[1] - 1)$ holds. This is because the probability of $K[1] = 127$ or 255 in WPA is $\frac{4}{N}$ or 0, respectively.

4.3 Biases in $S_{255}[i_{256}]$ for both generic RC4 and WPA

Theorem 5 shows that $S_{255}[i_{256}] = K[0]$ holds with high probability in both generic RC4 and WPA. On the other hand, Theorem 6 shows $S_{255}[i_{256}] = K[1]$ holds with high probability only in WPA.

Theorem 5. *After the* 255*-th round of PRGA, we have*

$$\Pr(S_{255}[i_{256}] = K[0]) \approx \alpha_0\left(1 - \frac{1}{N}\right)^{255} + \frac{1}{N}(1 - \alpha_0)\left(1 - \left(1 - \frac{1}{N}\right)^{255}\right).$$

Proof. The probability of event $(S_{255}[i_{256}] = K[0])$ can be decomposed in two paths: $S_0[0] = K[0]$ (Path 1) and $S_0[0] \neq K[0]$ (Path 2). In the following proof, we use $S_{255}[0]$ instead of $S_{255}[i_{256}]$ $(i_{256} = 0)$ for simplicity.

Path 1. In $S_0[0] = K[0]$, event $(S_{255}[0] = K[0])$ occurs if $S_r[0] = S_0[0]$ for $1 \leq r \leq 255$, whose probability is $\left(1 - \frac{1}{N}\right)^{255}$ approximately. Thus, the probability in Path 1 is given as follows:

$$\Pr(S_{255}[0] = K[0] \mid \text{Path 1}) \approx \left(1 - \frac{1}{N}\right)^{255}.$$

Path 2. In $S_0[0] \neq K[0]$, event $(S_{255}[0] = K[0])$ never occurs if $S_r[0] = S_0[0]$ for $1 \leq r \leq 255$. Except when $S_r[0] = S_0[0]$ for $1 \leq r \leq 255$, whose probability is $\left(1 - \left(1 - \frac{1}{N}\right)^{255}\right)$ approximately, we assume that event $(S_{255}[0] = K[0])$ occurs with probability $\frac{1}{N}$ due to random association. Thus, the probability in Path 2 is given as follows:

$$\Pr(S_{255}[0] = K[0] \mid \text{Path 2}) \approx \frac{1}{N}\left(1 - \left(1 - \frac{1}{N}\right)^{255}\right).$$

In summary, we get

$$\begin{aligned}\Pr(S_{255}[i_{256}] = K[0]) &= \Pr(S_{255}[i_{256}] = K[0] \mid \text{Path 1}) \cdot \Pr(\text{Path 1}) \\ &\quad + \Pr(S_{255}[i_{256}] = K[0] \mid \text{Path 2}) \cdot \Pr(\text{Path 2}) \\ &\approx \alpha_0\left(1 - \frac{1}{N}\right)^{255} + \frac{1}{N}(1 - \alpha_0)\left(1 - \left(1 - \frac{1}{N}\right)^{255}\right),\end{aligned}$$

where $\alpha_0 = \Pr(S_0[0] = K[0]) \approx \left(1 - \frac{1}{N}\right)^N + \frac{1}{N}$. □

Before showing Theorem 6, we will show in Lemma 1 that $S_0[0] = K[1]$ with high probability only in WPA.

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

$$\Pr(S_0[0] = K[1]) \approx \begin{cases} \frac{1}{N} - \frac{1}{N^2}\left(1 - \alpha_0\right) & \textit{for RC4,} \\ \frac{1}{4}\left(\frac{3}{N} + \left(1 - \frac{3}{N}\right)\alpha_0\right) & \textit{for WPA.} \end{cases}$$

Proof. The probability of event $(S_0[0] = K[1])$ can be decomposed in two paths: $K[1] = K[0]$ (Path 1) and $K[1] \neq K[0]$ (Path 2).

Path 1. In $K[1] = K[0]$, event $(S_0[0] = K[1])$ occurs if and only if $S_0[0] = K[0]$. Thus, the probability in Path 1 is given as follows:

$$\Pr(S_0[0] = K[1] \mid \text{Path 1}) = \alpha_0.$$

Path 2. In $K[1] \neq K[0]$, event $(S_0[0] = K[1])$ never occurs if $S_0[0] = K[0]$. If $S_0[0] \neq K[0]$, then we assume that event $(S_0[0] = K[1])$ occurs with probability $\frac{1}{N}$ due to random association. Thus, the probability in Path 2 is given as follows:

$$\Pr(S_0[0] = K[1] \mid \text{Path 2}) \approx \frac{1}{N} \cdot (1 - \alpha_0).$$

In summary, we get

$$\begin{aligned}\Pr(S_0[0] = K[1]) &= \Pr(S_0[0] = K[1] \mid \text{Path 1}) \cdot \Pr(\text{Path 1}) \\ &\quad + \Pr(S_0[0] = K[1] \mid \text{Path 2}) \cdot \Pr(\text{Path 2}) \\ &\approx \begin{cases} \alpha_0 \cdot \frac{1}{N} + \frac{1}{N}(1 - \alpha_0) \cdot \left(1 - \frac{1}{N}\right) = \frac{1}{N} - \frac{1}{N^2}\left(1 - \alpha_0\right) & \text{for RC4,} \\ \alpha_0 \cdot \frac{1}{4} + \frac{1}{N}(1 - \alpha_0) \cdot \frac{3}{4} = \frac{1}{4}\left(\frac{3}{N} + \left(1 - \frac{3}{N}\right)\alpha_0\right) & \text{for WPA,} \end{cases}\end{aligned}$$

where $\alpha_0 = \Pr(S_0[0] = K[0]) \approx \left(1 - \frac{1}{N}\right)^N + \frac{1}{N}$. □

Lemma 1 reflects that the probability of event $(K[1] = K[0])$ in WPA, $\frac{1}{4}$, is higher than that in generic RC4, $\frac{1}{N}$.

Theorem 6. *After the* 255*-th round of PRGA, we have*

$$\Pr(S_{255}[i_{256}] = K[1]) \approx \delta\left(1 - \frac{1}{N}\right)^{255} + \frac{1}{N}(1-\delta)\left(1 - \left(1 - \frac{1}{N}\right)^{255}\right),$$

where δ *is* $\Pr(S_0[0] = K[1])$ *given as Lemma 1.*

Proof. The proof itself is similar to Theorem 5, and used the probability of event $(S_0[0] = K[1])$ given as Lemma 1 instead of the probability of event $(S_0[0] = K[0])$. Therefore, we get

$$\begin{aligned}\Pr(S_{255}[i_{256}] = K[1]) &= \Pr(S_{255}[0] = K[1] \mid S_0[0] = K[1]) \cdot \Pr(S_0[0] = K[1]) \\ &\quad + \Pr(S_{255}[0] = K[1] \mid S_0[0] \neq K[1]) \cdot \Pr(S_0[0] \neq K[1]) \\ &\approx \delta\left(1 - \frac{1}{N}\right)^{255} + \frac{1}{N}(1-\delta)\left(1 - \left(1 - \frac{1}{N}\right)^{255}\right),\end{aligned}$$

where δ is $\Pr(S_0[0] = K[1])$ given as Lemma 1. □

4.4 Bias in $S_r[i_{r+1}]$ $(0 \leq r \leq N)$ for both generic RC4 and WPA

Theorem 7 shows $\Pr(S_r[i_{r+1}] = K[0] + K[1] + 1)$ for $0 \leq r \leq N$, whose experimental result is listed Fig. 1 in Section 4.1. Before showing Theorem 7, Lemmas 2 and 3, distribution of the state in the first 2 rounds of PRGA, are proved.

Lemma 2. *In the initial state of PRGA for* $0 \leq x \leq N-1$*, we have*

$$\begin{aligned}&\Pr(S_0[x] = K[0] + K[1] + 1) \\ &\approx \begin{cases} \left(1 - \frac{1}{N}\right)^{N+2} + \frac{1}{N} & \text{if } x = 1 \\ \frac{1}{N^2}\left(1 - \frac{1}{N}\right)^2 & \text{if } x = 0 \text{ for WPA} \\ \frac{1}{N}\left(1 - \frac{1}{N}\right)\left(\frac{1}{N}\left(1 - \frac{x+1}{N}\right) + \left(1 - \frac{1}{N}\right)^{N-x-2}\right) & \text{otherwise.} \end{cases}\end{aligned}$$

Proof. First, the probability of event $(S_0[1] = K[0] + K[1] + 1)$ follows the result in Proposition 1, that is, $\Pr(S_0[1] = K[0] + K[1] + 1) \approx \left(1 - \frac{1}{N}\right)^{N+2} + \frac{1}{N}$.

Next, the probability of event $(S_0[x] = K[0] + K[1] + 1)$ for $x \in [0, N] \backslash \{1\}$ can be decomposed in two paths: $S_x^K[j_{x+1}^K] = K[0] + K[1] + 1$ (Path 1) and $S_x^K[j_{x+1}^K] \neq K[0] + K[1] + 1$ (Path 2).

Path 1. In $S_x^K[j_{x+1}^K] = K[0]+K[1]+1$, $S_{x+1}^K[x] = K[0]+K[1]+1$ always holds due to swap operation. Furthermore, if $S_r^K[x] = S_{x+1}^K[x]$ for $x+2 \le r \le N$, whose probability is $\left(1-\frac{1}{N}\right)^{N-x-1}$ approximately, then $S_0[x] = K[0] + K[1] + 1$ always holds. Thus, the probability in Path 1 is given as follows:

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

Path 2. Let y be satisfied with $S_x^K[y] = K[0]+K[1]+1$. In $S_x^K[j_{x+1}^K] \neq K[0]+K[1]+1$, $S_{x+1}^K[x] = K[0]+K[1]+1$ never holds due to swap operation. After the $x+1$-th round, if $x \ge y$, then event $(S_0[x] \neq K[0]+K[1]+1)$ occurs because $S_r^K[x] \neq K[0]+K[1]+1$ always holds for $x+1 \le r \le N$. Else if $x < y$, then we assume that event $(S_0[x] = K[0]+K[1]+1)$ occurs with probability $\frac{1}{N}$ due to random association, and the probability of $x < y$ is $1-\frac{x+1}{N}$. In order to be satisfied $x < y$, we further consider $K[0] = 1$, whose probability is $\frac{1}{N}$. If $K[0] \neq 1$, then $S_2^K[1] = K[0]+K[1]+1$ always holds from the discussion in Theorem 1, and thus, $S_r^K[x] \neq K[0]+K[1]+1$ holds for $2 \le r \le N$. In summary, the probability in Path 2 is given as follows:

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

In summary, we get

$$\begin{aligned}
&\Pr(S_0[x] = K[0]+K[1]+1) \\
&\quad = \Pr(S_0[x] = K[0]+K[1]+1 \mid \text{Path 1}) \cdot \Pr(\text{Path 1}) \\
&\qquad + \Pr(S_0[x] = K[0]+K[1]+1 \mid \text{Path 2}) \cdot \Pr(\text{Path 2}) \\
&\quad \approx \frac{1}{N}\left(1-\frac{1}{N}\right)\left(\frac{1}{N}\left(1-\frac{x+1}{N}\right)+\left(1-\frac{1}{N}\right)^{N-x-2}\right).
\end{aligned}$$

In the case of $x = 0$ in WPA, event $(S_0[0] = K[0]+K[1]+1)$ never occurs in $S_0^K[j_1^K] = K[0]+K[1]+1$ (Path 1) since $S_0^K[j_1^K] = K[0]$ from step 6 in Algorithm 1. Then, $K[1] = 255$ never holds in WPA. Thus, $\Pr(S_0[0] = K[0]+K[1]+1)$ occurs if and only if Path 2, whose probability is given simply as $\frac{1}{N^2}\left(1-\frac{1}{N}\right)^2$. □

Lemma 3. *After the first round of PRGA for $0 \le x \le N-1$, we have*

$$\Pr(S_1[x] = K[0]+K[1]+1) = \begin{cases} \beta_1 & \text{if } x = 1 \\ \alpha_1\gamma_{x-1} + (1-\beta_1)\epsilon_x & \text{otherwise,} \end{cases}$$

where ϵ_x is $\Pr(S_0[x] = K[0]+K[1]+1)$ given as Lemma 2.

Proof. First, the probability of event $(S_1[1] = K[0]+K[1]+1)$ follows the result in Proposition 2 because $S_1[1] = S_1[i_1] = S_0[j_1] = S_0[S_0[1]]$ from steps 4 and 5 in Algorithm 2, that is, $\Pr(S_1[1] = K[0]+K[1]+1) = \beta_1$.

Next, the probability of event $(S_1[x] = K[0]+K[1]+1)$ for $x \in [0, N-1]\backslash\{1\}$ can be decomposed in two paths: $S_0[1] = K[0]+K[1]+1$ (Path 1) and $S_0[x] = K[0]+K[1]+1$ (Path 2).

Path 1. In $S_0[1] = K[0]+K[1]+1$, if $j_1 = x$, then event $(S_1[x] = K[0]+K[1]+1)$ always occurs due to swap operation. Although both $S_0[1] = K[0]+K[1]+1$ and $j_1 = x$ are not independent, both $S_0[1] = K[0]+K[1]+1$ and $K[0]+K[1]+1 = x$ become independent by converting $j_1 = x$ into $j_1 = S_0[1] = K[0]+K[1]+1 = x$. Thus, the probability in Path 1 is given as follows:

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

Path 2. In $S_0[x] = K[0]+K[1]+1$, if $j_1 = x$, then event $(S_1[x] = K[0]+K[1]+1)$ never occurs due to swap operation. If $j_1 \neq x$, then $S_1[x] = S_0[x] = K[0]+K[1]+1$ always holds, and $S_1[1] \neq K[0]+K[1]+1$ holds since $S_1[1] = S_0[j_1] \neq S_0[x]$ from swap operation in the first round. So, we assume that both $S_0[x] = K[0]+K[1]+1$ and $S_1[1] \neq K[0]+K[1]+1$ are mutually independent. Thus, the probability in Path 2 is given as follows:

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

In summary, we get

$$\begin{aligned}
&\Pr(S_1[x] = K[0]+K[1]+1) \\
&\quad = \Pr(S_1[x] = K[0]+K[1]+1 \mid \text{Path 1}) \cdot \Pr(\text{Path 1}) \\
&\qquad + \Pr(S_1[x] = K[0]+K[1]+1 \mid \text{Path 2}) \cdot \Pr(\text{Path 2}) \\
&\quad = \alpha_1\gamma_{x-1} + (1-\beta_1)\epsilon_x,
\end{aligned}$$

where $\alpha_1 = \Pr(S_0[1] = K[0]+K[1]+1)$, $\beta_1 = \Pr(S_0[S_0[1]] = K[0]+K[1]+1)$, $\gamma_{x-1} = \Pr(K[0]+K[1] = x-1)$ and $\epsilon_x = \Pr(S_0[x] = K[0]+K[1]+1)$ is given as Lemma 2. □

Theorem 7. *After the r-th round of PRGA for $0 \leq x \leq N$, we have*

$$\begin{aligned}
&\Pr(S_r[i_{r+1}] = K[0]+K[1]+1) \\
&\approx \begin{cases}
\alpha_1 & \text{if } r = 0, \\
\alpha_1\gamma_1 + (1-\beta_1)\epsilon_2 & \text{if } r = 1, \\
\epsilon_0\left(1-\frac{1}{N}\right)^{N-1} + \frac{1}{N}(1-\epsilon_0)\left(1-\left(1-\frac{1}{N}\right)^{N-1}\right) & \text{if } r = N-1, \\
\zeta_1\left(1-\frac{1}{N}\right)^{N-1} + \frac{1}{N}(1-\zeta_1)\left(1-\left(1-\frac{1}{N}\right)^{N-1}\right) & \text{if } r = N, \\
\zeta_{r+1}\left(1-\frac{1}{N}\right)^{r-1} + \frac{1}{N}\sum_{x=1}^{r-1}\eta_x\left(1-\frac{1}{N}\right)^{r-x-1} & \text{otherwise,}
\end{cases}
\end{aligned}$$

where ϵ_r is $\Pr(S_0[r] = K[0]+K[1]+1)$ given as Lemma 2, ζ_r is $\Pr(S_1[r] = K[0]+K[1]+1)$ given as Lemma 3 and η_r is $\Pr(S_r[i_{r+1}] = K[0]+K[1]+1)$ given as this theorem.

Proof. First, the probability of events $(S_0[i_1] = K[0] + K[1] + 1)$ and $(S_1[i_2] = K[0] + K[1] + 1)$ follow the result in Lemmas 2 and 3, respectively.

Next, both events $(S_{N-1}[i_N] = K[0] + K[1] + 1)$ and $(S_N[i_{N+1}] = K[0] + K[1] + 1)$ can be proved in the same way as the proof of Theorem 5.

Finally, the probability of event $(S_r[i_{r+1}] = K[0]+K[1]+1)$ for $2 \le r \le N-2$ can be decomposed in two paths: $S_1[i_{r+1}] = K[0] + K[1] + 1$ (Path 1) and $S_x[i_{x+1}] = K[0] + K[1] + 1$ $(1 \le x \le r-1)$ (Path 2).

Path 1. In $S_1[i_{r+1}] = K[0] + K[1] + 1$, event $(S_r[i_{r+1}] = K[0] + K[1] + 1)$ occurs if $S_y[i_{y+1}] = S_1[i_{r+1}]$ for $2 \le y \le r$, whose probability is $\left(1 - \frac{1}{N}\right)^{r-1}$ approximately. Thus, the probability in Path 1 is given as follows:

$$\Pr(S_r[i_{r+1}] = K[0] + K[1] + 1 \mid \text{Path 1}) \approx \left(1 - \frac{1}{N}\right)^{r-1}.$$

Path 2. In $S_x[i_{x+1}] = K[0] + K[1] + 1$ $(1 \le x \le r-1)$, if $j_{x+1} = i_{r+1}$, then $S_{x+1}[i_{r+1}] = K[0]+K[1]+1$ always holds due to swap operation. After the $x+1$-th round, event $(S_r[i_{r+1}] = K[0]+K[1]+1)$ occurs if $S_y[i_{y+1}] = S_{x+1}[i_{r+1}]$ for $x+2 \le y \le r$, whose probability is $\left(1 - \frac{1}{N}\right)^{r-x-1}$ approximately. Thus, the probability in Path 2 is given as follows:

$$\Pr(S_r[i_{r+1}] = K[0] + K[1] + 1 \mid \text{Path 2}) \approx \frac{1}{N}\left(1 - \frac{1}{N}\right)^{r-x-1}.$$

Note that the range of x varies depending on the value of r in Path 2. In summary, we get

$$\begin{aligned}
&\Pr(S_r[i_{r+1}] = K[0] + K[1] + 1) \\
&\quad = \Pr(S_r[i_{r+1}] = K[0] + K[1] + 1 \mid \text{Path 1}) \cdot \Pr(\text{Path 1}) \\
&\qquad + \sum_{x=1}^{r-1} \Pr(S_r[i_{r+1}] = K[0] + K[1] + 1 \mid \text{Path 2}) \cdot \Pr(\text{Path 2}) \\
&\quad \approx \zeta_{r+1}\left(1 - \frac{1}{N}\right)^{r-1} + \frac{1}{N}\sum_{x=1}^{r-1} \eta_x \left(1 - \frac{1}{N}\right)^{r-x-1},
\end{aligned}$$

where $\zeta_r = \Pr(S_1[r] = K[0]+K[1]+1)$ and $\eta_r = \Pr(S_r[i_{r+1}] = K[0]+K[1]+1)$, which is recursive probability in this theorem.

5 Experimental results

In order to check the accuracy of notable linear correlations shown in Theorems 1 to 7, the experiments are conducted using 2^{40} randomly generated keys of 16 bytes in both generic RC4 and WPA, which mean $2^{40}(= N^5)$ trials. Note that $\mathcal{O}(N^3)$ trials are reported to be sufficient to identify the biases with constant probability of success. This is why each correlation has a relative bias with the

probability of at least about $\frac{1}{2N}$ with respect to a base event of probability $\frac{1}{N}$ (refer to [11, Theorem 2] in detail). Our experimental environment is as follows: Ubuntu 12.04 machine with 2.6 GHz CPU, 3.8 GiB memory, gcc 4.6.3 compiler and C language. We also evaluate the percentage of relative error ϵ of experimental values compared with theoretical values:

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

Table 2 shows experimental and theoretical values and the percentage of relative errors ϵ, which indicates ϵ is small enough in each case such as $\epsilon \leq 4.589$ (%). Fig. 7 shows comparison between experimental and theoretical values in Theorem 7, and these distributions match on the whole. Therefore, we have convinced that theoretical values closely reflects the experimental values.

Table 2. Comparison between experimental and theoretical values

Results		Experimental value	Theoretical value	ϵ(%)
Theorem 1		0.001449605	0.001445489	0.284
Theorem 2		0	0	0
Theorem 3	for RC4	0.005332558	0.005325263	0.137
	for WPA	0.007823541	0.008182569	4.589
Theorem 4	for RC4	0.003922530	0.003898206	0.620
	for WPA	0.007851853	0.008182569	4.212
Theorem 5		0.138038917	0.138325988	0.208
Theorem 6	for RC4	0.003909105	0.003893102	0.409
	for WPA	0.037186225	0.037105932	0.216

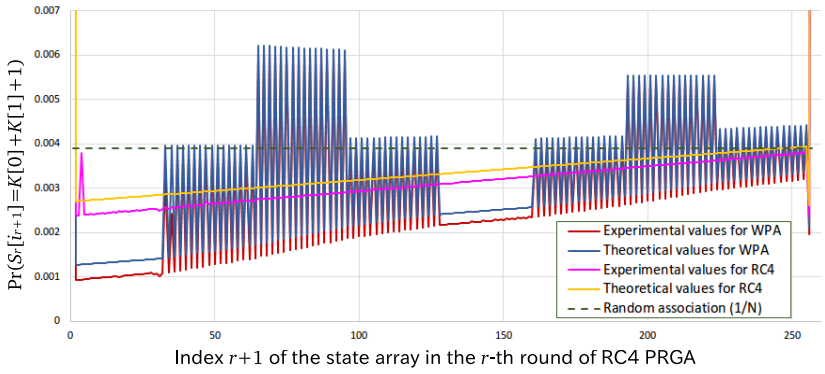

Fig. 7. Comparison between experimental and theoretical values shown in Theorem 7 for both generic RC4 and WPA

6 Conclusion

In this paper, we have focused on the state information and investigated various linear correlations among the *unknown* state information, the first 3 bytes of the RC4 key, and a keystream byte in both generic RC4 and WPA. Particularly, those linear correlations are effective for the state recovery attack since they include the first *known* 3-byte keys (IV-related). As a result, we have discovered more than 150 correlations with positive or negative biases. We have also proved six notable linear correlations theoretically, these are biases in $S_0[i_1]$, $S_{255}[i_{256}]$ and $S_r[i_{r+1}]$ for $0 \leq r \leq N$. For example, we have proved that the probability of $(S_0[i_1] = K[0])$ in WPA is 0 (shown in Theorem 2), and thus, $S_0[i_1]$ is varied from $[0, 255] \setminus K[0]$.

These new linear correlations could contribute to the improvement of the state recovery attack against RC4 especially in WPA. It is still an open problem to prove various linear correlations shown in Table 3 theoretically. It is also given to an open problem to apply newly discovered linear correlations to the state recovery attack.

References

1. Nadhem J. AlFardan, Daniel J. Bernstein, Keneth G. Paterson, Bertram Poettering, and Jacob C. N. Schuldt. On the Security of RC4 in TLS. In *USENIX Security Symposium 2013*, 2013.
2. 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.
3. 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.
4. 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.
5. Russ Housley, Doug Whiting, and Niels Ferguson. *Alternate Temporal Key Hash*. doc.: IEEE 802.11-02/282r2, April 2002.
6. 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.
7. Andreas Klein. Attacks on the RC4 stream cipher. *Designs, Codes and Cryptography*, 48(3):269–286, April 2008.
8. 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.

9. Subhamoy Maitra and Goutam Paul. New Form of Permutation Bias and Secret Key Leakage in Keystream Bytes of RC4. In Kaisa Nyberg, editor, *Fast Software Encryption - FSE 2008*, volume 5086 of *Lecture Notes in Computer Science*, pages 253–269. Springer Berlin Heidelberg, 2008.
10. Subhamoy Maitra, Goutam Paul, Santanu Sarkar, Michael Lehmann, and Willi Meier. New Results on Generalization of Roos-Type Biases and Related Keystreams of RC4. In Amr Youssef, Abderrahmane Nitaj, and Aboul Ella Hassanien, editors, *Progress in Cryptology - AFRICACRYPT 2013*, volume 7918 of *Lecture Notes in Computer Science*, pages 222–239. Springer Berlin Heidelberg, 2013.
11. 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.
12. 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.
13. Kenneth G. Paterson, Bertram Poettering, and Jacob C.N. Schuldt. Plaintext Recovery Attacks Against WPA/TKIP. In *Fast Software Encryption - FSE 2014*. To appear, 2014.
14. 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.
15. Andrew Roos. A class of weak keys in the RC4 stream cipher. Posts in sci.crypt, http://marcel.wanda.ch/Archive/WeakKeys, 1995.
16. Pouyan Sepehrdad, Petr Susil, Serge Vaudenay, and Martin Vuagnoux. Smashing WEP in a Passive Attack. In Shiho Moriai, editor, *Fast Software Encryption - FSE 2013*, volume 8424 of *Lecture Notes in Computer Science*, pages 155–178. Springer Berlin Heidelberg, 2014.
17. Ryoichi Teramura, Yasuo Asakura, Toshihiro Ohigashi, Hidenori Kuwakado, and Masakatsu Morii. Fast WEP-Key Recovery Attack Using Only Encrypted IP Packets. *IEICE Trans. Fundamentals*, E93-A(1):164–171, jan 2010.

A Newly obtained linear correlations

In this part, Table 3 shows notable linear correlations newly discovered by our experiment shown in Section 4.1.

Table 3. Notable linear correlations in Eq. (1) for both generic RC4 and WPA

X_r	Linear correlations	RC4	WPA
$S_0[i_1]$	$-Z_1+1$	0.007584	0.007660
$(=j_1)$	$-K[0]-K[1]-K[2]$	0.005361	0.005360
	$-K[0]-K[1]-3$	0.005336	0.008437
	$-K[0]-K[1]+1$	0.005350	0.002600
	$-K[0]-K[1]+3$	0.005331	0.002605
	$-K[0]-1$	0.003823	0.005254
	$-K[0]+2$	0.003902	0.005340
	$-K[0]+K[1]-3$	0.005334	0.005240
	$-K[0]+K[1]-1$	0.005331	0.005229
	$K[1]+1$	0.006765	0.004322
	$K[0]-K[1]+1$	0.005324	0.002221
	$K[0]-K[1]+3$	0.005333	0.002640
	$K[0]+K[1]+K[2]+3$	0.001492	0.001491
	$Z_1-K[0]-K[1]-K[2]-2$	0.005326	0.004753
$S_1[i_2]$	$-Z_2-K[0]+K[1]$	0.003905	0.004957
	$-Z_2-K[0]+K[1]+2$	0.003906	0.004839
	$-Z_2-K[1]+K[2]-3$	0.005314	0.005327
	$-Z_2$	0.007768	0.007791
	$-Z_2+2$	0.007751	0.007749
	$-Z_2+K[1]+K[2]+3$	0.005317	0.005328
	$-Z_2+K[0]-K[1]$	0.003907	0.004958
	$-Z_2+K[0]-K[1]+2$	0.003906	0.004839
	$-K[0]-K[1]-K[2]+1$	0.005348	0.005351
	$-K[0]-K[1]-K[2]+3$	0.005281	0.005290
	$-K[0]-K[1]+3$	0.005329	0.004036
	$-K[0]-K[1]+K[2]-3$	0.005307	0.002491
	$-K[0]-K[1]+K[2]-1$	0.005305	0.008197
	$-K[0]-K[1]+K[2]+1$	0.005317	0.002491
	$-K[0]-K[1]+K[2]+3$	0.005305	0.002474
	$-K[0]+K[2]-2$	0.003904	0.005311
	$-K[0]+K[2]+1$	0.003906	0.005326
	$-K[0]+K[1]-K[2]-3$	0.005293	0.004616
	$-K[0]+K[1]-K[2]-1$	0.005296	0.005885
	$-K[0]+K[1]-K[2]+1$	0.005301	0.005279
	$-K[0]+K[1]-K[2]+3$	0.005300	0.005289
	$-K[0]+K[1]+K[2]-3$	0.005308	0.005322
	$-K[0]+K[1]+K[2]-1$	0.005305	0.005333
	$-K[0]+K[1]+K[2]+1$	0.005306	0.005326
	$-K[0]+K[1]+K[2]+3$	0.005310	0.004261
	$-K[1]-K[2]-3$	0.006748	0.006767
	$-K[2]-1$	0.006127	0.007571
	$-K[2]+1$	0.003915	0.005308
	$-K[2]+3$	0.003904	0.005306
	$K[2]-3$	0.003910	0.005309
	$K[2]-1$	0.003910	0.005321
	$K[2]+1$	0.003909	0.005331
	$K[2]+3$	0.006219	0.003886
	$K[1]+K[2]+3$	0.008157	0.006755
	$K[0]-K[1]-K[2]-1$	0.005309	0.005895
	$K[0]-K[1]-K[2]+1$	0.005302	0.005314
	$K[0]-K[1]-K[2]+3$	0.005308	0.005318
	$K[0]-K[1]+K[2]-3$	0.005295	0.008163
	$K[0]-K[1]+K[2]-1$	0.005290	0.008171
	$K[0]-K[1]+K[2]+1$	0.005309	0.008171
	$K[0]-K[1]+K[2]+3$	0.005310	0.002838
	$K[0]$	0.001455	0.001452
	$K[0]+K[1]-K[2]-3$	0.005312	0.005340
	$K[0]+K[1]-K[2]+1$	0.005291	0.005295
	$K[0]+K[1]-K[2]+3$	0.005304	0.005309
	$Z_2-K[1]-K[2]-3$	0.005323	0.005333
	$Z_2+K[1]+K[2]+3$	0.005322	0.005332
$S_2[i_3]$	$-Z_3-K[0]+K[1]+3$	0.003906	0.004878
	$-Z_3+3$	0.007825	0.007819
	$-Z_3+K[0]-K[1]+3$	0.003907	0.004877
	$-K[0]-K[1]+2$	0.005335	0.005539
	$-K[0]+K[1]+3$	0.003901	0.004983
	$K[0]$	0.001463	0.001458
$S_3[i_4]$	$-K[0]-K[1]-K[2]$	0.005324	0.005325
	$-K[0]-K[1]+3$	0.006721	0.005513
$S_{28}[i_{29}]$	$-Z_{29}-K[0]+K[1]-3$	0.003906	0.004861
$S_{29}[i_{30}]$	$-Z_{30}-K[0]+K[1]-2$	0.003906	0.004863
$S_{30}[i_{31}]$	$-Z_{31}-K[0]+K[1]-1$	0.003907	0.004863
$S_{31}[i_{32}]$	$-Z_{32}-K[0]+K[1]$	0.003906	0.004862
$S_{32}[i_{33}]$	$-Z_{33}-K[0]+K[1]+1$	0.003907	0.004860
$S_{33}[i_{34}]$	$-Z_{34}-K[0]+K[1]+2$	0.003906	0.004860
$S_{34}[i_{35}]$	$-Z_{35}-K[0]+K[1]+3$	0.003907	0.004863
$S_{92}[i_{93}]$	$-Z_{93}+K[0]-K[1]-3$	0.003904	0.004877
$S_{93}[i_{94}]$	$-Z_{94}+K[0]-K[1]-2$	0.003906	0.004877
$S_{94}[i_{95}]$	$-Z_{95}+K[0]-K[1]-1$	0.003907	0.004875
$S_{95}[i_{96}]$	$-Z_{96}+K[0]-K[1]$	0.003906	0.004878
$S_{96}[i_{97}]$	$-Z_{97}+K[0]-K[1]+1$	0.003906	0.004875
$S_{97}[i_{98}]$	$-Z_{98}+K[0]-K[1]+2$	0.003906	0.004875
$S_{98}[i_{99}]$	$-Z_{99}+K[0]-K[1]+3$	0.003906	0.004876
$S_{124}[i_{125}]$	$-Z_{125}-K[0]+K[1]-3$	0.003908	0.004874
	$-Z_{125}+K[0]+K[1]-3$	0.003906	0.004872
$S_{125}[i_{126}]$	$-Z_{126}-K[0]+K[1]-2$	0.003907	0.004876
	$-Z_{126}+K[0]-K[1]-2$	0.003907	0.004876
$S_{126}[i_{127}]$	$-Z_{127}-K[0]+K[1]-1$	0.003906	0.004874
	$-Z_{127}+K[0]-K[1]-1$	0.003906	0.004876
$S_{127}[i_{128}]$	$-Z_{128}-K[0]+K[1]$	0.003908	0.004875
	$-Z_{128}+K[0]-K[1]$	0.003907	0.004876
$S_{128}[i_{129}]$	$-Z_{129}-K[0]+K[1]+1$	0.003906	0.004875
	$-Z_{129}+K[0]-K[1]+1$	0.003907	0.004875
$S_{129}[i_{130}]$	$-Z_{130}-K[0]+K[1]+2$	0.003906	0.004875
	$-Z_{130}+K[0]-K[1]+2$	0.003906	0.004876
$S_{130}[i_{131}]$	$-Z_{131}-K[0]+K[1]+3$	0.003903	0.004876
	$-Z_{131}+K[0]-K[1]+3$	0.003906	0.004875
$S_{156}[i_{157}]$	$-Z_{157}-K[0]+K[1]-3$	0.003904	0.004876
$S_{157}[i_{158}]$	$-Z_{158}-K[0]+K[1]-2$	0.003906	0.004877
$S_{158}[i_{159}]$	$-Z_{159}-K[0]+K[1]-1$	0.003906	0.004875
$S_{159}[i_{160}]$	$-Z_{160}-K[0]+K[1]$	0.003906	0.004876
$S_{160}[i_{161}]$	$-Z_{161}-K[0]+K[1]+1$	0.003906	0.004876
$S_{161}[i_{162}]$	$-Z_{162}-K[0]+K[1]+2$	0.003907	0.004875
$S_{162}[i_{163}]$	$-Z_{163}-K[0]+K[1]+3$	0.003907	0.004874
$S_{220}[i_{221}]$	$-Z_{221}+K[0]-K[1]-3$	0.003907	0.004860
$S_{221}[i_{222}]$	$-Z_{222}+K[0]-K[1]-2$	0.003907	0.004858
$S_{222}[i_{223}]$	$-Z_{223}+K[0]-K[1]-1$	0.003906	0.004861
$S_{223}[i_{224}]$	$-Z_{224}+K[0]-K[1]$	0.003907	0.004859
$S_{224}[i_{225}]$	$-Z_{225}+K[0]-K[1]+1$	0.003908	0.004861
$S_{225}[i_{226}]$	$-Z_{226}+K[0]-K[1]+2$	0.003907	0.004861
$S_{226}[i_{227}]$	$-Z_{227}+K[0]-K[1]+3$	0.003907	0.004859
$S_{252}[i_{253}]$	$-Z_{253}-K[0]+K[1]-3$	0.003907	0.004876
	$-Z_{253}-3$	0.007813	0.007815
	$-Z_{253}+K[0]-K[1]-3$	0.003906	0.004875
$S_{253}[i_{254}]$	$-Z_{254}-K[0]+K[1]-2$	0.003906	0.004875
	$-Z_{254}-2$	0.007814	0.007812
	$-Z_{254}+K[0]-K[1]-2$	0.003906	0.004875
$S_{254}[i_{255}]$	$-Z_{255}-K[0]+K[1]-1$	0.003905	0.004875
	$-Z_{255}-1$	0.007816	0.007815
	$-Z_{255}+K[0]-K[1]-1$	0.003905	0.004876
$S_{255}[i_{256}]$	$-Z_{256}-K[0]+K[1]$	0.003908	0.004875
	$-Z_{256}$	0.007861	0.007810
	$-Z_{256}+K[0]-K[1]$	0.003909	0.004875
$S_r[i_{r+1}]$	$-K[1]-1$	Fig. 8	
	$K[0]$	Fig. 9	
$S_0[j_1]$	$-Z_1+K[0]+K[1]+1$	0.005330	0.005280
	$-K[0]-K[1]-3$	0.004339	0.005513
	$-K[0]-K[1]+1$	0.005791	0.003417
	$K[1]+1$	0.004933	0.004087
	$K[0]-K[1]-3$	0.004403	0.005342
	$K[0]-K[1]-1$	0.004431	0.005346
	$Z_1-K[0]-K[1]-K[2]-2$	0.005295	0.004726
	$Z_1-K[0]-K[1]-1$	0.005188	0.005115
$S_1[j_2]$	$-Z_2+K[0]+K[1]+1$	0.005316	0.005335
	$-K[0]-K[1]+1$	0.005318	0.005408
	$Z_2-K[0]-K[1]-K[2]-3$	0.005686	0.005694
	$Z_2+K[0]+K[1]+1$	0.005321	0.005344
j_2	$-Z_2+K[0]+K[1]+1$	0.005318	0.005336
	$-Z_2+K[0]+K[1]+3$	0.005302	0.005310
	$-K[0]-K[1]-K[2]+2$	0.005333	0.005856
	$-K[0]-K[1]+K[2]$	0.003919	0.005573
	$-K[0]+K[1]+K[2]$	0.003921	0.005501
	$-K[1]+K[2]-2$	0.003911	0.005479
	$-K[1]+K[2]+3$	0.003899	0.005476
	$K[2]$	0.004428	0.005571
	$K[0]-K[1]+K[2]$	0.003918	0.005618
	$K[0]+K[1]+3$	0.005309	0.003889
t_1	$-Z_1-K[0]-K[1]+1$	0.005251	0.005333
	$-K[0]-K[1]+2$	0.005310	0.003902
	$K[0]$	0.005291	0.004806
	$Z_1-K[0]-K[1]-K[2]-1$	0.006639	0.006094
t_2	$-Z_2-K[0]-K[1]-K[2]+1$	0.005301	0.005306
	$-Z_2+K[0]+K[1]+1$	0.005339	0.005341
	$K[0]+K[1]+1$	0.005317	0.005349
t_3	$K[0]+K[1]+K[2]+3$	0.005297	0.005310
t_r	Z_r	Fig. 10	

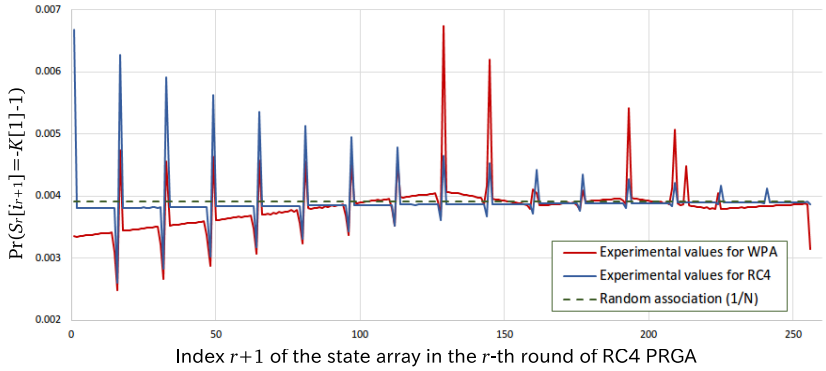

Fig. 8. Experimental result of event $(S_r[i_{r+1}] = -K[1] - 1)$

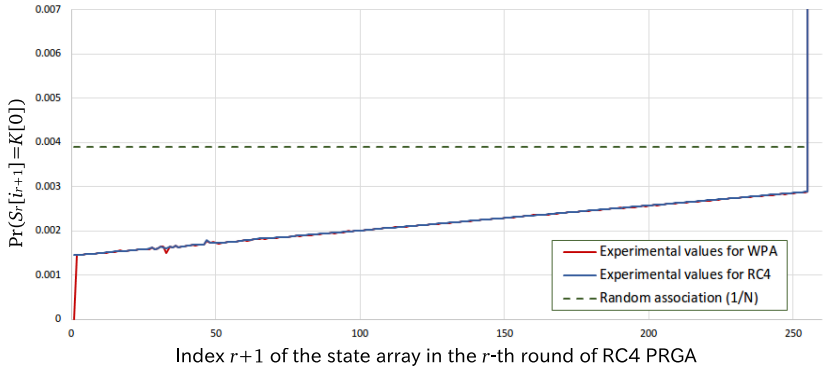

Fig. 9. Experimental result of event $(S_r[i_{r+1}] = K[0])$

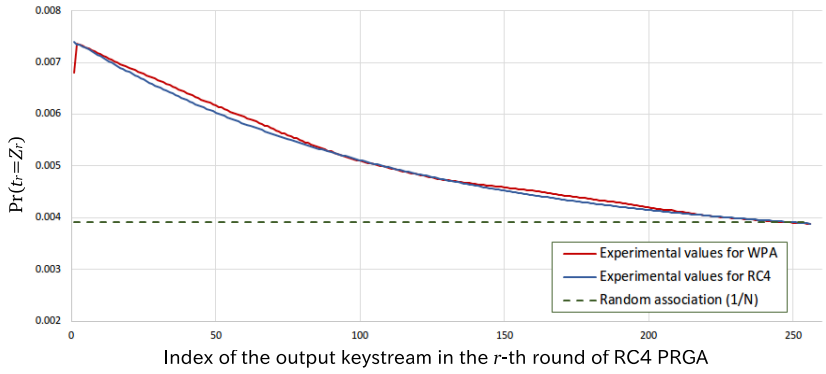

Fig. 10. Experimental result of event $(t_r = Z_r)$