IEICE TRANS. FUNDAMENTALS, VOL.E99–A, NO.6 JUNE 2016

PAPER Special Section on Discrete Mathematics and Its Applications

Refined RC4 Key Correlations of Internal States in WPA**

Ryoma ITO[†*a)], ***Nonmember and*** **Atsuko MIYAJI**[††,†††,††††b)], ***Member***

SUMMARY WPA is the security protocol for IEEE 802.11 wireless networks standardized as a substitute for WEP in 2003, and uses RC4 stream cipher for encryption. It improved a 16-byte RC4 key generation procedure, which is known as TKIP, from that in WEP. One of the remarkable features in TKIP is that the first 3-byte RC4 key is derived from the public parameter IV, and an analysis using this feature has been reported by Sen Gupta et al. at FSE 2014. They focused on correlations between the keystream bytes and the known RC4 key bytes in WPA, which are called *key correlations* or *linear correlations*, and improved the existing plaintext recovery attack using their discovered correlations. No study, however, has focused on such correlations including the internal states in WPA. In this paper, we investigated new linear correlations including unknown internal state variables in both generic RC4 and WPA. From the result, we can successfully discover various new linear correlations, and prove some correlations theoretically.

key words: *RC4, WPA, TKIP, linear correlations*

1. Introduction

RC4 is the stream cipher designed by Rivest in 1987, and is widely used in Secure Socket Layer/Transport Layer Security (SSL/TLS), Wired Equivalent Privacy (WEP), Wi-fi Protected Access (WPA), and so on. 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. Especially, the input of the permutation S can be considered as the number modulo N. We will be followed this statement in this paper.

Algorithm 1 KSA

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

Algorithm 2 PRGA

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

After the disclosure of RC4 algorithms in 1994, RC4 has been intensively analyzed over past 20 years. There are mainly two approaches to the cryptanalysis on RC4. One is to demonstrate the existence of events with non-randomness, which is known as *bias*, involving the RC4 key, the internal state variables and the keystream bytes [12], [14], [19]. The other is to attack on RC4 using biases in order to recover the RC4 key (key recovery attacks) [18], [20], the internal state variables (state recovery attacks) [1], [10], [15] and the plaintexts (plaintext recovery attacks) [12], [14]. In addition, a number of analyses related to the security protocols have been reported such as the plaintext recovery attacks on SSL/TLS [6], [16], the key recovery attacks on WEP [3], [9] and the plaintext recovery attacks on WPA [4], [17]. Here, we refer to the event with the probability significantly higher or lower than $\frac{1}{N}$ (the probability of random association) as the *positive bias* or the *negative bias*, respectively.

WPA is the security protocol for IEEE 802.11 wireless networks standardized as a substitute for WEP in 2003. It improves a 16-byte RC4 key generation procedure from that in WEP, which is known as Temporal Key Integrity Protocol

Manuscript received September 18, 2015.
Manuscript revised January 7, 2016.

[†]The author is with Japan Air Self-Defence Force, Ministry of Defence, Tokyo, 162-8801 Japan.
[††]The author is with Graduate School of Engineering, Osaka University, Suita-shi, 565-0871 Japan.
[†††]The author is with Japan Advanced Institute of Science and Technology, Nomi-shi, 923-1292 Japan.
[††††]The author is with CREST, Japan Science and Technology Agency, Tokyo, 102-0076 Japan.
[*]This work was conducted when he was with Japan Advanced Institute of Science and Technology.

[**]Preliminary versions were presented at SCIS 2015 [7] and FSE 2015 [8].

a) E-mail: ryoma.ito.shs@gmail.com
b) E-mail: miyaji@comm.eng.osaka-u.ac.jp

DOI: 10.1587/transfun.E99.A.1132

(TKIP). TKIP includes a key management scheme, a temporal key hash function [5] and a message integrity code function. 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 Initialization Vector (IV), which is a sequence counter, are given as the inputs to the temporal key hash function, and the function outputs a 16-byte RC4 key. In addition, TKIP uses MICHAEL [2] to ensure integrity of a message. One of the remarkable features in TKIP is that the first 3-byte RC4 key, $K[0]$, $K[1]$ and $K[2]$, are derived from the last 16-bit IV (IV16) as follows:

$$K[0] = (\text{IV16} >> 8)\ \&\ \text{0xFF}, \tag{1}$$

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

$$K[2] = \text{IV16}\ \&\ \text{0xFF}. \tag{3}$$

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. demonstrated a probability distribution of a sum of the first 2-byte RC4 key, $K[0]$ and $K[1]$, in WPA. From Eqs. (1) and (2), the value of $K[1]$ depends on that of $K[0]$, and its range is limited to either from 32 to 63 or from 96 to 127 in order to avoid the known WEP attack by Fluhrer et al. [3]. In addition, $K[0] + K[1]$ must be always even. Therefore, such a relation between $K[0]$ and $K[1]$ induces biases of $K[0] + K[1]$ in WPA. Furthermore, they also showed some linear correlations between the keystream bytes and the known RC4 key bytes in WPA such as $Z_1 = -K[0] - K[1]$, $Z_3 = K[0] + K[1] + K[2] + 3$, and so on. These correlations could be added to the known set of biases for the keystream bytes. Therefore, they could apply these correlations to the existing plaintext recovery attack on SSL/TLS [6] especially in WPA, and could improve its computational complexity necessary for the attack.

In this paper, we investigate new linear correlations including unknown internal state variables in both generic RC4 and WPA. Here, unknown internal state variables mean $S_r[i_{r+1}]$, $S_r[j_{r+1}]$, j_{r+1} and t_{r+1} for $r \geq 0$. In addition, we also focus on the difference between generic RC4 and WPA, and discover some different correlations. These correlations exactly reflect difference of the distribution of $K[0] + K[1]$ between both generic RC4 and WPA. As a result, we discover more than 150 linear correlations newly and succeed to give proof of some of them. Our contributions can be summarized in the following 9 theorems:

- Theorems 1 and 2 show $\Pr(S_0[i_1] = K[0])$ in generic RC4 and WPA, respectively. In particular, we stress that $\Pr(S_0[i_1] = K[0]) = 0$ in WPA.
- Theorems 3 and 4 show $\Pr(S_0[i_1] = K[0] - K[1] - 3)$, Theorems 5 and 6 show $\Pr(S_0[i_1] = K[0] - K[1] - 1)$ in generic RC4 and WPA, respectively. Only WPA gives double probabilities of random association $\frac{1}{N}$.
- Theorem 7 shows $\Pr(S_{255}[i_{256}] = K[0])$ is pretty high probability in comparison with the probability of random association $\frac{1}{N}$ in both generic RC4 and WPA. On the other hand, Theorem 8 shows $\Pr(S_{255}[i_{256}] = K[1])$ is high probability only in WPA.
- Theorem 9 shows $\Pr(S_r[i_{r+1}] = K[0] + K[1] + 1)$ in generic RC4 and WPA for $0 \leq r \leq N$, which is distributed in the same way as the distribution of $K[0] + K[1]$.

Some theoretical proofs of the preliminary version of this papers [7], [8] rather high relative errors, which are improved in this paper.

This paper is organized as follows: Section 2 summarizes the previous works necessary for both theoretical proofs and experiments such as Roos' biases [18], [19], nested Roos' biases [11], [13], the distribution of $K[0]+K[1]$ in WPA [4] and the number of samples necessary for distinguishing two distributions [14]. Section 3 shows the theoretical proofs of prominent linear correlations and the experimental results. Section 4 concludes this paper.

2. Preliminary

Let us summarize some previous results which will be used in both theoretical proofs and experiments as preliminary. Proposition 1 shows Roos' biases [19], correlations between the RC4 key bytes and the initial state S_0 of the PRGA, proved by Paul and Maitra [18]. Propositions 2 shows nested Roos' biases [11], correlations similar to Roos' biases, proved by Maitra et al. [13]. Proposition 3 shows a distribution of $K[0] + K[1]$ based on a relation between $K[0]$ and $K[1]$ generated by the temporal key hash function in WPA, proved by Sen Gupta et al. [4]. Proposition 4 shows the number of samples necessary for distinguishing two distributions with a constant probability of success, proved by Mantin and Shamir [14].

Proposition 1 ([18]): In the initial state of the PRGA for $0 \leq y \leq N-1$, we have

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

Proposition 2 ([11]): In the initial state of the PRGA for $0 \leq y \leq 31$, $\Pr(S_0[S_0[y]] = f_y)$ is approximately

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

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

Proposition 3 ([4]): For $0 \leq v \leq N-1$, 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:

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

Proposition 4 ([14]): 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, $O(\frac{1}{p \cdot q^2})$ samples suffice to distinguish X from Y with a constant probability of success.

3. Newly Discovered Linear Correlations

3.1 Experimental Observations

Let us investigate some correlations of the following unknown internal state variables in both generic RC4 and WPA: $S_r[i_{r+1}]$, $S_r[j_{r+1}]$, j_{r+1} and t_{r+1} for $r \geq 0$. Linear correlations of the keystream bytes Z_r were investigated by Sen Gupta et al. in 2014 [4], which used a general linear form

$$Z_r = a \cdot K[0] + b \cdot K[1] + c \cdot K[2] + d \quad (4)$$

for $a, b, c \in \{0, \pm 1\}$ and $d \in \{0, \pm 1, \pm 2, \pm 3\}$ for $r \geq 1$. Here, we further extend their linear form by Eq. (4) to

$$X_r = a \cdot Z_{r+1} + b \cdot K[0] + c \cdot K[1] + d \cdot K[2] + e, \quad (5)$$

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 $e \in \{0, \pm 1, \pm 2, \pm 3\}$ for $r \geq 0$. Sen Gupta et al. could apply the biases by Eq. (4) to the plaintext recovery attack on WPA, and could improve its computational complexity necessary for the existing attack on SSL/TLS [6]. Similarly, we should apply the biases by Eq. (5) to the state recovery attack on WPA, and may reduce its computational complexity necessary for the existing attack on generic RC4 [1], [10], [15].

We have examined all $4 \cdot 3^4 \cdot 7$ equations defined by Eq. (5) in each round with 2^{32} randomly generated 16-byte RC4 keys in both generic RC4 and WPA. Some experimental results are presented in Tables 1 and A· 1. We have summarized the correlations with more than 0.0048 or less than 0.0020 in either generic RC4 or WPA. Some correlations happen only in WPA although generic RC4 indicates neither positive nor negative bias. In particular, we stress that an event $S_0[i_1] = K[0]$ yields an impossible condition in WPA, and thus, the probability of the event is 0 (see Table 1). Then, the value of $S_0[i_1]$ is varied from 0 to $N-1$ except $K[0]$.

We will prove these linear correlations theoretically shown in Table 1. In our proofs, we often use Roos' biases (Proposition 1), nested Roos' biases (Proposition 2) and the distribution of $K[0] + K[1]$ (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.

Table 1 New linear correlations by Eq. (5) in 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	Theorems 3 and 4
	$K[0] - K[1] - 1$	0.003922	0.007877	Theorems 5 and 6
$S_{255}[i_{256}]$	$K[0]$	0.137294	0.138047	Theorem 7
	$K[1]$	0.003911	0.037189	Theorem 8
$S_r[i_{r+1}]$	$K[0] + K[1] + 1$	Fig. 1		Theorem 9

We assume through proofs that the probability of certain events, confirmed experimentally[†] that there are no significant biases, is the probability 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 since these are generated by IV using a sequence counter.

3.2 Bias in $S_0[i_1]$

In this section, we prove Theorems 1-6. Theorems 1 and 2 show that an event $S_0[i_1] = K[0]$ yields a negative bias in generic RC4 and never occurs in WPA, respectively. Theorems 3 and 4 show that an event $S_0[i_1] = K[0] - K[1] - 3$ yields a positive bias in generic RC4 and occurs with twice as frequently as the probability of random association $\frac{1}{N}$, respectively. Theorems 5 and 6 show that an event $S_0[i_1] = K[0] - K[1] - 1$ yields a slight bias in generic RC4 and occurs with twice as frequently as the probability of random association $\frac{1}{N}$, respectively. In addition, Theorems 4 and 6 are revised precisely form our preliminary version [8].

Theorem 1: In the initial state of the PRGA, we have

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

Proof : Figure 2 shows a state transition diagram in the first 2 rounds of the 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. Figure 3 shows a state transition diagram in Path

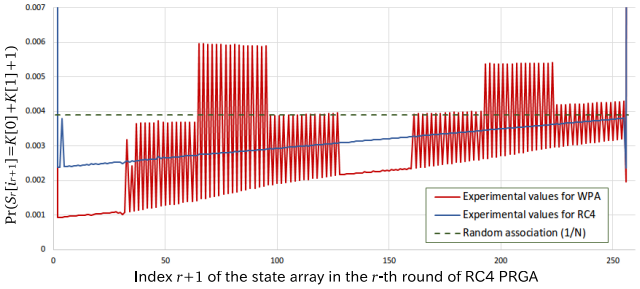

Fig. 1 Observed results of event $S_r[i_{r+1}] = K[0] + K[1] + 1$: The horizontal and the vertical lines represent the value of r and the probability of the event, respectively. The blue and the red lines represents the experimental values in generic RC4 and WPA, respectively.

[†]In order to use this assumption, the experiments are conducted with 2^{32} randomly generated RC4 keys of 16 bytes.

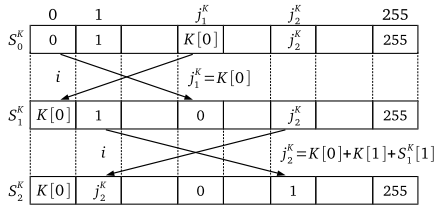

Fig. 2 State transition diagram in the first 2 rounds of KSA.

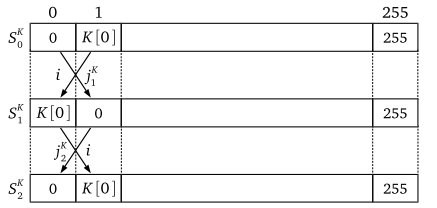

Fig. 3 State transition diagram in Path 1-1 (Theorem 1).

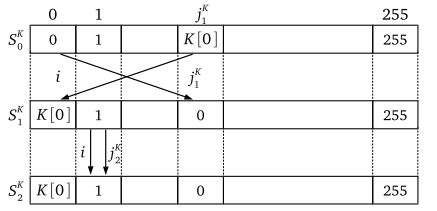

Fig. 4 State transition diagram in Path 1-2 (Theorem 1).

1-1. After the second round of the 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 $3 \le r \le N$ if $j_r^K \ne 1$ during the subsequent $N-2$ rounds, whose probability is $(1-\frac{1}{N})^{N-2}$ approximately since we assume that $j_r^K = 1$ holds for each round with the probability of random association $\frac{1}{N}$. Therefore, we get

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

Path 1-2. Figure 4 shows a state transition diagram in Path 1-2. After the second round of the KSA, $S_2^K[0] = K[0]$ always holds since $j_1^K = K[0] \ne 1$ 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 $S_r^K[1] \ne K[0]$ always holds for $r \ge 2$ from Algorithm 1. Therefore, we get

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

Path 2-1. Figure 5 shows a state transition diagram in Path 2-1. After the second round of the KSA, $S_2^K[0] = K[0]$ always holds in the same way as the case of Path 1-2. Then, event $S_0[1] = K[0]$ never occurs. Therefore, we get

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

Path 2-2. Figure 6 shows a state transition diagram in Path 2-2. After the second round of the KSA, $S_2^K[1] = K[0]$ always holds in the same way as the case of Path 1-1. Then, event $S_0[1] = K[0]$ occurs if $S_r[1] = S_2^K[1]$ for $3 \le r \le N$. Therefore, we get

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

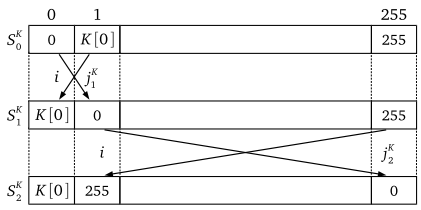

Fig. 5 State transition diagram in Path 2-1 (Theorem 1).

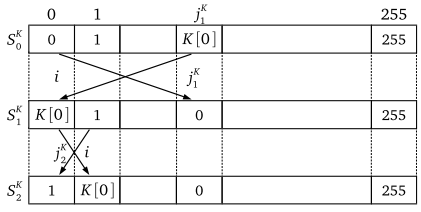

Fig. 6 State transition diagram in Path 2-2 (Theorem 1).

Path 3. Figure 2 shows a state transition diagram in Path 3. After the second round of the KSA, $S_2^K[0] = K[0]$ always holds in the same way as the cases of Paths 1-2 and 2-1. Then, event $S_0[1] = K[0]$ never occurs. Therefore, we get

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

In summary, event $S_0[i_1] = K[0]$ occurs only in either Paths 1-1 or 2-2. Therefore, since we assume that both $K[0]$ and $K[1]$ are generated uniformly at random, we get

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

□

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

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

Proof : Note that event $S_0[i_1] = K[0]$ 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. Therefore, we get

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

□

Theorem 3: In the initial state of the PRGA, we have

$$\Pr(S_0[i_1] = K[0] - K[1] - 3)_{\mathrm{RC4}} \approx \frac{2}{N}\alpha_1 + \frac{1}{N}(1-\frac{2}{N})(1-\alpha_1).$$

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. Since $K[0] - K[1] - 3 = K[0] + K[1] + 1$ if either $K[1] = 126$ or 254, event $S_0[1] = K[0] - K[1] - 3$ occurs if and only if $S_0[1] = K[0] + K[1] + 1$ under the condition of Path 1. Therefore, we get

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

Path 2. Since $K[0] - K[1] - 3 \neq K[0] + K[1] + 1$ if neither $K[1] = 126$ nor 254, event $S_0[1] = K[0] - K[1] - 3$ never occurs if $S_0[1] = K[0] + K[1] + 1$ under the condition of Path 2. 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

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

In summary, since we assume that $K[1]$ is generated uniformly at random, we get

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

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

Before showing Theorems 4 and 6, we prove Lemma 1. In the preliminary version [8], the relative errors of the events $S_0[i_1] = K[0]-K[1]-3$ and $S_0[i_1] = K[0]-K[1]-1$ in WPA are slightly large such as 4.589% and 4.212%, respectively. This is because we have proved them in the same way as the theoretical proofs of those in generic RC4. Furthermore, we could not discover the inherent feature in WPA, which is a probability distribution of $K[0] - K[1]$. Lemma 1 shows the distribution of $K[0] - K[1]$ in WPA. We may improve the relative errors by applying this feature to the theoretical proofs.

Lemma 1: For $0 \leq v \leq N - 1$, the distribution of the difference v between $K[0]$ and $K[1]$ generated by the temporal key hash function in WPA is given as follows:

$$\begin{aligned}
&\Pr(K[0] - K[1] = v) = \tfrac{1}{4} \quad \text{if } v \in \{0, 96, 128, 224\}, \\
&\Pr(K[0] - K[1] = v) = 0 \quad \text{otherwise.}
\end{aligned}$$

Proof : The value of $K[0] - K[1]$ depends on the range of $K[0]$ (see Table 2). Therefore, the probability distribution of $K[0] - K[1]$ may be computed directly from the table. □

Theorem 4: In the initial state of the PRGA in WPA, we have

Table 2 The distribution of $K[0] - K[1]$ in WPA.

$K[0]$ Range	$K[1]$ (depends on $K[0]$) Value	Range	$K[0] - K[1]$ Value
0 – 31	$K[0] + 32$	32 – 63	224
32 – 63	$K[0]$	32 – 63	0
64 – 95	$K[0] + 32$	96 – 127	224
96 – 127	$K[0]$	96 – 127	0
128 – 159	$K[0] - 96$	32 – 63	96
160 – 191	$K[0] - 128$	32 – 63	128
192 – 223	$K[0] - 96$	96 – 127	96
224 – 255	$K[0] - 128$	96 – 127	128

$$\begin{aligned}
\Pr(S_0[i_1] &= K[0] - K[1] - 3)_{\mathrm{WPA}} \\
&\approx \tfrac{4}{N}\alpha_1 + \tfrac{1}{4N}((1-\tfrac{1}{N})^{91} + (1-\tfrac{1}{N})^{123} + (1-\tfrac{1}{N})^{219} \\
&\quad + (1 - \frac{1}{N})^{251})(1 - \frac{4}{N}).
\end{aligned}$$

Proof : We note that the range of $K[1]$ is limited to either from 32 to 63 or from 96 to 127 in WPA (see Table 2). Then, as with the discussion in the proof of Theorem 3, the probability of event $S_0[i_1] = K[0] - K[1] - 3$ in WPA can be decomposed in two paths: $K[1] = 126$ (Path 1) and $K[1] \neq 126$ (Path 2). 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. Since $K[0] - K[1] - 3 = K[0] + K[1] + 1$ if $K[1] = 126$, event $S_0[1] = K[0] - K[1] - 3$ occurs if and only if $S_0[1] = K[0] + K[1] + 1$ under the condition of Path 1. Therefore, we get

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

Path 2. Since $K[0] - K[1] - 3 \neq K[0] + K[1] + 1$ if $K[1] \neq 126$, event $S_0[1] = K[0] - K[1] - 3$ never occurs if $S_0[1] = K[0] + K[1] + 1$ under the condition of Path 2. We then focus on the distribution of $K[0] - K[1]$ in WPA. Assuming that event $S_0[1] = K[0] - K[1] - 3$ occurs, $S_0[1]$ can be one of the following values from Lemma 1: 93, 125, 221 or 253. Then, the probability in Path 2 can be further decomposed in four paths: $K[0] - K[1] = 96$ (Path 2-1), $K[0] - K[1] = 128$ (Path 2-2), $K[0] - K[1] = 224$ (Path 2-3) and $K[0] - K[1] = 0$ (Path 2-4).

Path 2-1. After the second round of the KSA, both $S_2^K[1] = K[0] + K[1] + 1 \neq 93$ (we can compute the sum of $K[0]$ and $K[1]$ from Table 2) and $S_2^K[93] = 93$ hold under the condition of Path 2-1 from Algorithm 1. After that, if $S_r^K[93] \neq S_2^K[93] = 93$ for $3 \leq r \leq 93$, event $S_0[1] = K[0] - K[1] - 3 = 93$ never occurs in the same way as the discussion of Theorem 1 (Path 1-2 in the proof). If $S_r^K[93] = S_2^K[93] = 93$, whose probability is $(1 - \frac{1}{N})^{91}$ approximately since we assume that $j_r^K = 93$ holds for each round with the probability of random association $\frac{1}{N}$, then we also assume that event $S_0[1] = K[0] - K[1] - 3$ occurs with the probability of random association $\frac{1}{N}$. Therefore, we get

$$\Pr(S_0[1] = K[0] - K[1] - 3 \mid \text{Path 2} \wedge \text{Path 2-1}) \approx \tfrac{1}{N}(1 - \tfrac{1}{N})^{91}.$$

The probabilities of event $S_0[1] = K[0] - K[1] - 3$ under the conditions of Path 2-2, Path 2-3 and Path 2-4 can be computed in the same way as the discussion of Path 2-1. Therefore, we get

$$\Pr(S_0[1]=K[0]-K[1]-3 \mid \text{Path } 2 \wedge \text{Path } 2\text{-}2) \approx \tfrac{1}{N}(1-\tfrac{1}{N})^{123},$$
$$\Pr(S_0[1]=K[0]-K[1]-3 \mid \text{Path } 2 \wedge \text{Path } 2\text{-}3) \approx \tfrac{1}{N}(1-\tfrac{1}{N})^{219},$$
$$\Pr(S_0[1]=K[0]-K[1]-3 \mid \text{Path } 2 \wedge \text{Path } 2\text{-}4) \approx \tfrac{1}{N}(1-\tfrac{1}{N})^{251}.$$

The probabilities of these subpaths are taken from Lemma 1. By substituting these probabilities, we get

$$\begin{aligned}
&\Pr(S_0[1]=K[0]-K[1]-3)\\
&= \Pr(S_0[1]=K[0]-K[1]-3 \mid \text{Path } 2 \wedge \text{Path } 2\text{-}1)\cdot\Pr(\text{Path } 2\text{-}1)\\
&\quad + \Pr(S_0[1]=K[0]-K[1]-3 \mid \text{Path } 2 \wedge \text{Path } 2\text{-}2)\cdot\Pr(\text{Path } 2\text{-}2)\\
&\quad + \Pr(S_0[1]=K[0]-K[1]-3 \mid \text{Path } 2 \wedge \text{Path } 2\text{-}3)\cdot\Pr(\text{Path } 2\text{-}3)\\
&\quad + \Pr(S_0[1]=K[0]-K[1]-3 \mid \text{Path } 2 \wedge \text{Path } 2\text{-}4)\cdot\Pr(\text{Path } 2\text{-}4)\\
&\approx \tfrac{1}{4N}((1-\tfrac{1}{N})^{91}+(1-\tfrac{1}{N})^{123}+(1-\tfrac{1}{N})^{219}+(1-\tfrac{1}{N})^{251}).
\end{aligned}$$

Note that the probability of $K[1] = 126$ in WPA is $\frac{1}{4}$ (see Table 2). In summary, we get

$$\begin{aligned}
&\Pr(S_0[1]=K[0]-K[1]-3)\\
&= \Pr(S_0[1]=K[0]-K[1]-3 \mid \text{Path } 1)\cdot\Pr(\text{Path } 1)\\
&\quad + \Pr(S_0[1]=K[0]-K[1]-3 \mid \text{Path } 2)\cdot\Pr(\text{Path } 2)\\
&\approx \tfrac{4}{N}\alpha_1 + \tfrac{1}{4N}((1-\tfrac{1}{N})^{91}+(1-\tfrac{1}{N})^{123}+(1-\tfrac{1}{N})^{219}+(1-\tfrac{1}{N})^{251})(1-\tfrac{4}{N}).
\end{aligned}$$

□

Theorem 5: In the initial state of the PRGA, we have

$$\Pr(S_0[i_1]=K[0]-K[1]-1)_{\text{RC4}} \approx \tfrac{1}{N}(1+\tfrac{2}{N})\alpha_1 + \tfrac{1}{N}(1-\tfrac{2}{N})(1-\alpha_1)$$

Proof : The probability of event $S_0[i_1] = K[0] - K[1] - 1$ can be decomposed in four paths: $K[1] = 0$ (Path 1), $K[1] = 127$ (Path 2), $K[1] = 255$ (Path 3) and $K[1] \neq 0, 127, 255$ (Path 4). In the following proof, we use $S_0[1]$ instead of $S_0[i_1]$ ($i_1 = 1$) for simplicity.

Path 1. In the first 2 round of the KSA, both $j_1^K = K[0]$ and $j_2^K = K[0] + K[1] + S_1^K[1]$ hold (see Fig. 2). If $K[0] = 1$, then $S_2^K[1] = 0$ and $K[0] - K[1] - 1 = 0$ always hold since $j_1^K = 1$ and $S_1^K[1] = 0$. In this case, $S_r^K[1] = S_2^K[1]$ for $3 \le r \le N$ if $j_r^K \neq 1$ during the subsequent $N - 2$ rounds, whose probability is $(1 - \frac{1}{N})^{N-2}$ approximately since we assume that $j_1^K = 1$ holds for each round with the probability of random association $\frac{1}{N}$. Therefore, we get

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

On the other hand, if $K[0] \neq 1$, then $S_2^K[1] = K[0] + 1$ and $K[0] - K[1] - 1 = K[0] - 1$. We then assume that event $S_0[1] = K[0] - K[1] - 1$ occurs with the probability of random association $\frac{1}{N}$. Therefore, we get

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

We assume that $K[0]$ is generated uniformly at random. By substituting these probabilities, we get

$$\begin{aligned}
&\Pr(S_0[i_1] = K[0] - K[1] - 1 \mid \text{Path } 1)\\
&= \Pr(S_0[i_1]=K[0]-K[1]-1 \mid \text{Path } 1 \wedge K[0]=1)\cdot\Pr(K[0]=1)\\
&\quad + \Pr(S_0[i_1]=K[0]-K[1]-1 \mid \text{Path } 1 \wedge K[0]\neq 1)\cdot\Pr(K[0]\neq 1)\\
&\approx (1-\tfrac{1}{N})^{N-2}\cdot\tfrac{1}{N} + \tfrac{1}{N}\cdot(1-\tfrac{1}{N}) = \tfrac{1}{N}(1-\tfrac{1}{N})((1-\tfrac{1}{N})^{N-3}+1).
\end{aligned}$$

Path 2. Since $K[0] - K[1] - 1 = K[0] + K[1] + 1$ if $K[1] = 127$, event $S_0[1] = K[0] - K[1] - 1$ occurs if and only if $S_0[1] = K[0] + K[1] + 1$ under the condition of Path 1. Therefore, we get

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

Path 3. Since $K[0] - K[1] - 1 = K[0] + K[1] + 1$ if $K[1] = 255$, event $S_0[1] = K[0] - K[1] - 1$ occurs if and only if $S_0[1] = K[0] + K[1] + 1$ under the condition of Path 2. 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. Therefore, we get

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

Path 4. Since $K[0] - K[1] - 1 \neq K[0] + K[1] + 1$ if neither $K[1] = 0$, 127 nor 255, event $S_0[1] = K[0] - K[1] - 1$ never occurs if $S_0[1] = K[0] + K[1] + 1$ under the condition of Path 3. 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 the probability of random association $\frac{1}{N}$. Therefore, we get

$$\Pr(S_0[1] = K[0] - K[1] - 1 \mid \text{Path } 4) \approx \tfrac{1}{N}\cdot(1-\alpha_1).$$

In summary, since we assume that $K[1]$ is generated uniformly at random, we get

$$\begin{aligned}
&\Pr(S_0[i_1] = K[0] - K[1] - 1)\\
&\quad = \Pr(S_0[i_1] = K[0] - K[1] - 1 \mid \text{Path } 1)\cdot\Pr(\text{Path } 1)\\
&\qquad + \Pr(S_0[i_1] = K[0] - K[1] - 1 \mid \text{Path } 2)\cdot\Pr(\text{Path } 2)\\
&\qquad + \Pr(S_0[i_1] = K[0] - K[1] - 1 \mid \text{Path } 3)\cdot\Pr(\text{Path } 3)\\
&\qquad + \Pr(S_0[i_1] = K[0] - K[1] - 1 \mid \text{Path } 3)\cdot\Pr(\text{Path } 4)\\
&\quad \approx \tfrac{1}{N^2}(1-\tfrac{1}{N})((1-\tfrac{1}{N})^{N-3}+1)\\
&\qquad + \tfrac{1}{N}(1+\tfrac{2}{N})\alpha_1 + \tfrac{1}{N}(1-\tfrac{2}{N})(1-\alpha_1),
\end{aligned}$$

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

Theorem 6: In the initial state of the PRGA in WPA, we have

$$\begin{aligned}
&\Pr(S_0[i_1] = K[0] - K[1] - 1)_{\text{WPA}}\\
&\approx \tfrac{4}{N}\alpha_1 + \tfrac{1}{4N}((1-\tfrac{1}{N})^{93}+(1-\tfrac{1}{N})^{125}+(1-\tfrac{1}{N})^{221}+(1-\tfrac{1}{N})^{253})(1-\tfrac{4}{N}).
\end{aligned}$$

Proof : The proof itself is similar to Theorem 4. We note that the range of $K[1]$ is limited to either from 32 to 63 or

from 96 to 127 in WPA (see Table 2). Then, as with the discussion in the proof of Theorem 5, the probability of event $(S_0[i_1] = K[0] - K[1] - 1)$ in WPA can be decomposed in two paths: $K[1] = 127$ (Path 1) and $K[1] \neq 127$ (Path 2). 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. Since $K[0] - K[1] - 1 = K[0] + K[1] + 1$ if $K[1] = 127$, event $(S_0[1] = K[0] - K[1] - 1)$ occurs if and only if $S_0[1] = K[0] + K[1] + 1$ under the condition of Path 1. Therefore, we get

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

Path 2. Since $K[0] - K[1] - 1 \neq K[0] + K[1] + 1$ if $K[1] \neq 127$, event $S_0[1] = K[0] - K[1] - 3$ never occurs if $S_0[1] = K[0] + K[1] + 1$ under the condition of Path 2. Assuming that event $S_0[1] = K[0] - K[1] - 1$ occurs, $S_0[1]$ can be one of the following values from Lemma 1: 95, 127, 223 or 255. Then, the probability in Path 2 can be further decomposed in four paths: $K[0] - K[1] = 96$ (Path 2-1), $K[0] - K[1] = 128$ (Path 2-2), $K[0] - K[1] = 224$ (Path 2-3) and $K[0] - K[1] = 0$ (Path 2-4). The probabilities of event $S_0[1] = K[0] - K[1] - 1$ under the conditions of all subpaths can be computed in the same way as the discussion in the proof of Theorem 4. Therefore, we get

$$\begin{aligned}
&\Pr(S_0[1] = K[0] - K[1] - 1 \mid \text{Path 2} \wedge \text{Path 2-2}) \approx \tfrac{1}{N}(1 - \tfrac{1}{N})^{93},\\
&\Pr(S_0[1] = K[0] - K[1] - 1 \mid \text{Path 2} \wedge \text{Path 2-2}) \approx \tfrac{1}{N}(1 - \tfrac{1}{N})^{125},\\
&\Pr(S_0[1] = K[0] - K[1] - 1 \mid \text{Path 2} \wedge \text{Path 2-3}) \approx \tfrac{1}{N}(1 - \tfrac{1}{N})^{221},\\
&\Pr(S_0[1] = K[0] - K[1] - 1 \mid \text{Path 2} \wedge \text{Path 2-4}) \approx \tfrac{1}{N}(1 - \tfrac{1}{N})^{253}.
\end{aligned}$$

The probabilities of these subpaths are taken from Lemma 1. By substituting these probabilities, we get

$$\begin{aligned}
&\Pr(S_0[1] = K[0] - K[1] - 1)\\
&= \Pr(S_0[1] = K[0] - K[1] - 1 \mid \text{Path 2} \wedge \text{Path 2-1}) \cdot \Pr(\text{Path 2-1})\\
&\quad + \Pr(S_0[1] = K[0] - K[1] - 1 \mid \text{Path 2} \wedge \text{Path 2-2}) \cdot \Pr(\text{Path 2-2})\\
&\quad + \Pr(S_0[1] = K[0] - K[1] - 1 \mid \text{Path 2} \wedge \text{Path 2-3}) \cdot \Pr(\text{Path 2-3})\\
&\quad + \Pr(S_0[1] = K[0] - K[1] - 1 \mid \text{Path 2} \wedge \text{Path 2-4}) \cdot \Pr(\text{Path 2-4})\\
&\approx \tfrac{1}{4N}((1 - \tfrac{1}{N})^{93} + (1 - \tfrac{1}{N})^{125} + (1 - \tfrac{1}{N})^{221} + (1 - \tfrac{1}{N})^{253}).
\end{aligned}$$

Note that the probability of $K[1] = 126$ in WPA is $\frac{1}{4}$ (see Table 2). In summary, we get

$$\begin{aligned}
&\Pr(S_0[1] = K[0] - K[1] - 1)\\
&= \Pr(S_0[1] = K[0] - K[1] - 1 \mid \text{Path 1}) \cdot \Pr(\text{Path 1})\\
&\quad + \Pr(S_0[1] = K[0] - K[1] - 1 \mid \text{Path 2}) \cdot \Pr(\text{Path 2})\\
&\approx \tfrac{4}{N}\alpha_1 + \tfrac{1}{4N}((1 - \tfrac{1}{N})^{93} + (1 - \tfrac{1}{N})^{125} + (1 - \tfrac{1}{N})^{221} + (1 - \tfrac{1}{N})^{253})(1 - \tfrac{4}{N}).
\end{aligned}$$

□

3.3 Biases in $S_{255}[i_{256}]$

In this section, we prove Theorems 7 and 8. Theorem 7 shows that event $S_{255}[i_{256}] = K[0]$ occurs with high probability in both generic RC4 and WPA. On the other hand, Theorem 8 shows event $S_{255}[i_{256}] = K[1]$ occurs with high probability only in WPA.

Theorem 7: After the 255-th round of the PRGA, we have

$$\begin{aligned}
&\Pr(S_{255}[i_{256}] = K[0])\\
&\quad \approx \alpha_0(1 - \tfrac{1}{N})^{255} + \tfrac{1}{N}(1 - \alpha_0)(1 - (1 - \tfrac{1}{N})^{255}).
\end{aligned}$$

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 and only if $S_r[0] = S_0[0]$ for $1 \leq r \leq 255$, whose probability is $(1 - \frac{1}{N})^{255}$ approximately since we assume that $j_r = 0$ holds for each round with the probability of random association $\frac{1}{N}$. Therefore, we get

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

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 $(1 - (1 - \frac{1}{N})^{255})$ approximately, we assume that event $S_{255}[0] = K[0]$ occurs with the probability of random association $\frac{1}{N}$. Therefore, we get

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

In summary, we get

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

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

Before showing Theorem 8, we will show in Lemma 2 that event $S_0[0] = K[1]$ occurs with high probability only in WPA.

Lemma 2: In the initial state of the PRGA, we have

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

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 $S_0[0] = K[0]$. Therefore, we get

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

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 the probability of random association $\frac{1}{N}$. Therefore, we get

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

In summary, we get

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

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

Lemma 2 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 8: After the 255-th round of the PRGA, we have

$$\begin{aligned}&\Pr(S_{255}[i_{256}] = K[1]) \\ &\quad \approx \delta(1 - \tfrac{1}{N})^{255} + \tfrac{1}{N}(1-\delta)(1 - (1 - \tfrac{1}{N})^{255}),\end{aligned}$$

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

Proof : The proof itself is similar to Theorem 7, and is used the probability of event $S_0[0] = K[1]$ given as Lemma 2 instead of the probability of event $S_0[0] = K[0]$. Therefore, we get

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

where δ is $\Pr(S_0[0] = K[1])$ given as Lemma 2. □

3.4 Bias in $S_r[i_{r+1}]$ $(0 \le r \le N)$

In this section, we prove Theorem 9. Theorem 9 shows $\Pr(S_r[i_{r+1}] = K[0] + K[1] + 1)$ for $0 \le r \le N$, whose experimental result is listed Fig. 1 in Sect. 3.1. Before showing Theorem 9, Lemmas 3 and 4, distributions of the internal state in the first 2 rounds of the PRGA, are proved.

Lemma 3: In the initial state of the PRGA for $0 \le x \le N-1$, we have

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

Proof : In the case of $x = 1$, the probability of event $S_0[1] = K[0] + K[1] + 1$ follows the result in Proposition 1. Therefore, we get

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

On the other hand, 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. From step 7 in Algorithm 1, $S_{x+1}^K[x] = K[0] + K[1] + 1$ always holds under the condition of Path 1 since $S_{x+1}^K[x]$ must be swapped from $S_x^K[j_{x+1}^K]$. In addition, if $S_r^K[x] = S_{x+1}^K[x]$ for $x + 2 \le r \le N$, whose probability is $(1 - \frac{1}{N})^{N-x-1}$ approximately since we assume that $j_r^K = x$ holds for each round with the probability of random association $\frac{1}{N}$, then event $S_0[x] = K[0] + K[1] + 1$ always occurs. Therefore, we get

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

Path 2. Let y be satisfied with $S_x^K[y] = K[0] + K[1] + 1$. In the same way as the discussion of Path 1, $S_{x+1}^K[x] = K[0] + K[1] + 1$ never holds under the condition of Path 2. After the $x+1$-th round, if $x \ge y$, then event $S_0[x] = K[0] + K[1] + 1$ never occurs because $S_r^K[x] \neq K[0] + K[1] + 1$ always holds for $x+1 \le r \le N$ from Algorithm 1. Else if $x < y$, whose probability is $1 - \frac{x+1}{N}$, then we assume that event $S_0[x] = K[0] + K[1] + 1$ occurs with the probability of random association $\frac{1}{N}$. 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. Thus, $S_r^K[x] \neq K[0] + K[1] + 1$ holds for $2 \le r \le N$. Therefore, we get

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

We assume that event $S_x^K[j_{x+1}^K] = K[0] + K[1] + 1$ occurs with the probability of random association $\frac{1}{N}$. In summary, we get

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

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

Lemma 4: After the first round of the PRGA for $0 \le x \le N-1$, we have

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

where ϵ_x is $\Pr(S_0[x] = K[0] + K[1] + 1)$ given as Lemma 3.

Proof : In the case of $x = 1$, the probability of event $S_1[1] = K[0] + K[1] + 1$ follows the result in Proposition

2 since $S_1[1] = S_1[i_1] = S_0[j_1] = S_0[S_0[1]]$ from steps 4 and 5 in Algorithm 2. Therefore, we get

$$\Pr(S_1[1] = K[0] + K[1] + 1) = \beta_1.$$

On the other hand, 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. From step 5 in Algorithm 2, event $S_1[x] = K[0] + K[1] + 1$ always occurs under the condition of Path 1 if and only if $j_1 = x$ since $S_1[j_1]$ must be swapped from $S_0[i_1] = S_0[1]$. 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 $j_1 = S_0[1] = K[0] + K[1] + 1 = x$. Therefore, we get

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

Path 2. In the same way as the discussion of Path 1, event $S_1[x] = K[0] + K[1] + 1$ never occurs under the condition of Path 2. 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 step 5 in Algorithm 2. 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. Therefore, we get

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

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 3. □

Theorem 9: After the r-th round of the PRGA for $0 \leq x \leq N$, we have

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

where $\epsilon_r = \Pr(S_0[r] = K[0] + K[1] + 1)$ is given as Lemma 3, $\zeta_r = \Pr(S_1[r] = K[0] + K[1] + 1)$ is given as Lemma 4 and $\eta_r = \Pr(S_r[i_{r+1}] = K[0] + K[1] + 1)$ is given as this theorem.

Proof : In the cases of $r = 0$ and 1, 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 3 and 4, respectively. In the cases of $r = N - 1$ and N, 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 7. In any other cases, the probability of event $S_r[i_{r+1}] = K[0] + K[1] + 1$ for $2 \leq r \leq N - 2$ can be decomposed in two paths: $S_1[i_{r+1}] = K[0] + K[1] + 1$ (Path 1) and $S_x[i_{x+1}] = K[0] + K[1] + 1$ ($1 \leq x \leq r - 1$) (Path 2).

Path 1. Event $S_r[i_{r+1}] = K[0] + K[1] + 1$ occurs under the condition of Path 1 if $S_y[i_{r+1}] = S_1[i_{r+1}]$ for $2 \leq y \leq r$, whose probability is $(1 - \frac{1}{N})^{r-1}$ approximately since we assume that $j_y = i_{r+1}$ holds for each round with the probability of random association $\frac{1}{N}$. Therefore, we get

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

Path 2. From step 5 in Algorithm 2, event $S_{x+1}[i_{r+1}] = K[0] + K[1] + 1$ always occurs under the condition of Path 2 if and only if $j_{x+1} = i_{r+1}$ since $S_{x+1}[j_{x+1}] = S_{x+1}[i_{r+1}]$ must be swapped from $S_x[i_{x+1}]$. After the $x + 1$-th round, event $S_r[i_{r+1}] = K[0] + K[1] + 1$ occurs if $S_y[i_{r+1}] = S_{x+1}[i_{r+1}]$ for $x + 2 \leq y \leq r$, whose probability is $(1 - \frac{1}{N})^{r-x-1}$ approximately since we assume that $j_y = i_{r+1}$ holds for each round with the probability of random association $\frac{1}{N}$. Therefore, we get

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

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

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

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. □

3.5 Experimental Results

In order to confirm the accuracy of Theorems 1-9, we have conducted experiments in the following environment: Ubuntu 12.04 machine with 2.6 GHz CPU, 3.8 GiB memory, gcc 4.6.3 compiler and C language. The number of samples necessary for our experiments is at least $O(N^3)$ according to Proposition 4. This is why each correlation has a relative bias with the probability of at least about $\frac{1}{N}$ with respect to a base event of the probability $\frac{1}{N}$. Then, we have used N^5 randomly generated 16-byte 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 the relative error ϵ of the experimental values compared with the theoretical values as follows:

Table 3 Comparison between the experimental and the theoretical values in Theorems 1-8.

Results	Experimental value	Theoretical value	ϵ (%)
Theorem 1	0.001449605	0.001445489	0.284
Theorem 2	0	0	0
Theorem 3	0.005332558	0.005325263	0.137
Theorem 4	0.007823541	0.007788309	0.450
Theorem 5	0.003922530	0.003909411	0.334
Theorem 6	0.007851853	0.007772441	1.010
Theorem 7	0.138038917	0.138325988	0.208
Theorem 8 (RC4)	0.003909105	0.003893102	0.409
Theorem 8 (WPA)	0.037186225	0.037105932	0.216

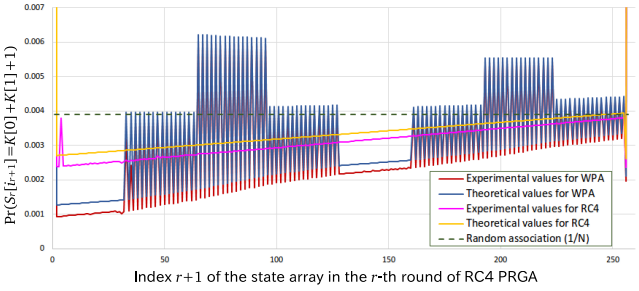

Fig. 7 Comparison between the experimental and the theoretical values in Theorem 9 for both generic RC4 and WPA.

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

Table 3 shows the experimental, the theoretical values and the percentage of the relative error ϵ in Theorems 1-8, which indicates that ϵ is small enough in each case such as $\epsilon \leq 1.010$. In particular, both Theorems 4 and 6 are improved form the results shown in our preliminary version [8]: from 4.589% to 0.450% and from 4.212% to 1.010%, respectively. Therefore, we have convinced that the theoretical values closely reflect the experimental values in Theorems 1-7. Theorem 8 for generic RC4 shows negative bias although the experimental value shows positive bias. We will continue to refine Theorem 8 for generic RC4.

Figure 7 shows a comparison between the experimental and the theoretical values in Theorem 9 for both generic RC4 and WPA. The horizontal and the vertical lines represent the values of r and the probability induced $S_r[i_{r+1}] = K[0]+K[1]+1$, respectively. The red and the blue lines represent the experimental and the theoretical values in WPA. The purple and the yellow lines represent the experimental and the theoretical values in generic RC4. From the figure, these distributions almost match on the whole, but differences between the experimental and the theoretical values in both generic RC4 and WPA are slightly large. Let us investigate why such differences are produced in both generic RC4 and WPA. As far as we have confirmed experimentally, it became clear that there exist differences between the experimental and the theoretical values in Lemma 4. So, we need to prove Lemma 4 again precisely, which remains an open problem.

4. Conclusion

In this paper, we have investigated various linear correlations including unknown internal state variables as well as the keystream bytes and the first 3-byte RC4 key in both generic RC4 and WPA. Actually, those linear correlations may be effective for the state recovery attacks since they include the known (IV-related) RC4 key bytes in WPA. From the result, we have discovered more than 150 correlations with positive or negative biases. Then, We have proved some linear correlations theoretically, which 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, the probability of event $S_0[i_1] = K[0]$ in WPA is 0 (Theorem 2 in Sect. 3.2). Thus, $S_0[i_1]$ is varied from $[0, 255] \setminus K[0]$. Furthermore, we stress that the relative errors of the events $S_0[i_1] = K[0] - K[1] - 3$ and $S_0[i_1] = K[0] - K[1] - 1$ in WPA (Theorems 4 and 6 in Sect. 3.2) could be improved than those in our preliminary version [8] by using the distribution of $K[0] - K[1]$ (Lemma 1 in Sect. 3.2).

New discovered linear correlations could contribute to the improvement of the state recovery attacks on RC4 especially in WPA. It is still an open problem to prove various linear correlations shown in Table A· 1 theoretically. It is also given to an open problem to apply refined linear correlations to the state recovery attacks.

Acknowledgements

This study is partly supported by the Grant-in-Aid for Scientific Research (C)(15K00183) and (15K00189) and Japan Science and Technology Agency (JST), Infrastructure Development for Promoting International S&T Cooperation.

References

[1] A. Das, S. Maitra, G. Paul, and S. Sarkar, "Some combinatorial results towards state recovery attack on RC4," Information Systems Security, Lecture Notes in Computer Science, vol.7093, pp.204–214, Springer Berlin Heidelberg, 2011.
[2] N. Ferugson and MacFergus, "Michael: An improved MIC for 802.11WEP," doc.: IEEE 802.11-02/020r0, Jan. 2002.
[3] S. Fluhrer, I. Mantin, and A. Shamir, "Weaknesses in the key scheduling algorithm of RC4," Selected Areas in Cryptography, Lecture Notes in Computer Science, vol.2259, pp.1–24, Springer Berlin Heidelberg, 2001.
[4] S.S. Gupta, S. Maitra, W. Meier, G. Paul, and S. Sarkar, "Dependence in IV-related bytes of RC4 key enhances vulnerabilities in WPA," Fast Software Encryption, Lecture Notes in Computer Science, vol.8540, pp.350–369, Springer Berlin Heidelberg, 2015.
[5] R. Housley, D. Whiting, and N. Ferguson, "Alternate temporal key hash," doc.: IEEE 802.11-02/282r2, April 2002.
[6] T. Isobe, T. Ohigashi, Y. Watanabe, and M. Morii, "Full plaintext recovery attack on broadcast RC4," Fast Software Encryption, Lecture Notes in Computer Science, vol.8424, pp.179–202, Springer Berlin Heidelberg, 2014.
[7] R. Ito and A. Miyaji, "New linear correlations on state information of RC4 in WPA," 32nd Symposium on Cryptography and Information Security, SCIS 2015 (2015-1). 2E2-3, 2015.
[8] R. Ito and A. Miyaji, "New linear correlations related to state information of RC4 PRGA using IV in WPA," Fast Software Encryption,

Lecture Notes in Computer Science, vol.9054, pp.557–576, Springer Berlin Heidelberg, 2015.

[9] A. Klein, "Attacks on the RC4 stream cipher," Des. Codes Cryptogr., vol.48, no.3, pp.269–286, April 2008.

[10] L.R. Knudsen, W. Meier, B. Preneel, V. Rijmen, and S. Verdoolaege, "Analysis methods for (alleged) RC4," Advances in Cryptology, ASIACRYPT'98, Lecture Notes in Computer Science, vol.1514, pp.327–341, Springer Berlin Heidelberg, 1998.

[11] S. Maitra and G. Paul, "New form of permutation bias and secret key leakage in keystream bytes of RC4," Fast Software Encryption, Lecture Notes in Computer Science, vol.5086, pp.253–269, Springer Berlin Heidelberg, 2008.

[12] S. Maitra, G. Paul, and S.S. Gupta, "Attack on broadcast RC4 revisited," Fast Software Encryption, Lecture Notes in Computer Science, vol.6733, pp.199–217, Springer Berlin Heidelberg, 2011.

[13] S. Maitra, G. Paul, S. Sarkar, M. Lehmann, and W. Meier, "New results on generalization of Roos-type biases and related keystreams of RC4," Progress in Cryptology, AFRICACRYPT 2013, Lecture Notes in Computer Science, vol.7918, pp.222–239, Springer Berlin Heidelberg, 2013.

[14] I. Mantin and A. Shamir, "A practical attack on broadcast RC4," Fast Software Encryption, Lecture Notes in Computer Science, vol.2355, pp.152–164, Springer Berlin Heidelberg, 2002.

[15] A. Maximov and D. Khovratovich, "New state recovery attack on RC4," Advances in Cryptology, CRYPTO 2008, Lecture Notes in Computer Science, vol.5157, pp.297–316, Springer Berlin Heidelberg, 2008.

[16] T. Ohigashi, T. Isobe, Y. Watanabe, and M. Morii, "How to recover any byte of plaintext on RC4," Selected Areas in Cryptography, SAC 2013, Lecture Notes in Computer Science, vol.8282, pp.155–173, Springer Berlin Heidelberg, 2014.

[17] K.G. Paterson, B. Poettering, and J.C.N. Schuldt, "Plaintext recovery attacks against WPA/TKIP," Fast Software Encryption, Lecture Notes in Computer Science, vol.8540, pp.325–349, Springer Berlin Heidelberg, 2015.

[18] G. Paul and S. Maitra, "Permutation after RC4 key scheduling reveals the secret key," Selected Areas in Cryptography, Lecture Notes in Computer Science, vol.4876, pp.360–377, Springer Berlin Heidelberg, 2007.

[19] A. Roos, "A class of weak keys in the RC4 stream cipher," Posts in sci.crypt, http://marcel.wanda.ch/Archive/WeakKeys, 1995.

[20] P. Sepehrdad, S. Vaudenay, and M. Vuagnoux, "Discovery and exploitation of new biases in RC4," Selected Areas in Cryptography, Lecture Notes in Computer Science, vol.6544, pp.74–91, Springer Berlin Heidelberg, 2011.

Appendix: Newly Obtained Linear Correlations

Table A· 1 New linear correlations by Eq. (5) in 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
$S_0[j_1]$	$-Z_1 + K[0] + K[1] + 1$	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

Ryoma Ito received the B.E. degree from the National Defence Academy of Japan in 2009 and the M.S. degree from the Japan Advanced Institute of Science and Technology in 2015. Since 2009, he has worked for the Japan Air Self-Defense Force, Ministry of Defence, Japan. His current research interests include information security and cryptography. He received the SCIS Paper Award from ISEC group of IEICE in SCIS 2015.

Atsuko Miyaji received the B.Sc., the M.Sc., and the Dr. Sci. degrees in mathematics from Osaka University, Osaka, Japan in 1988, 1990, and 1997 respectively. She joined Panasonic Co., LTD from 1990 to 1998 and engaged in research and development for secure communication. She was an associate professor at the Japan Advanced Institute of Science and Technology (JAIST) in 1998. She joined the computer science department of the University of California, Davis from 2002 to 2003. She has been a professor at Japan Advanced Institute of Science and Technology (JAIST) since 2007 and the director of Library of JAIST from 2008 to 2012. She has been a professor at Graduate School of Engineering, Osaka University since 2015. Her research interests include the application of number theory into cryptography and information security. She received Young Paper Award of SCIS'93 in 1993, Notable Invention Award of the Science and Technology Agency in 1997, the IPSJ Sakai Special Researcher Award in 2002, the Standardization Contribution Award in 2003, Engineering Sciences Society: Certificate of Appreciation in 2005, the AWARD for the contribution to CULTURE of SECURITY in 2007, IPSJ/ITSCJ Project Editor Award in 2007, 2008, 2009, 2010, and 2012, the Director-General of Industrial Science and Technology Policy and Environment Bureau Award in 2007, Editorial Committee of Engineering Sciences Society: Certificate of Appreciation in 2007, DoCoMo Mobile Science Awards in 2008, Advanced Data Mining and Applications (ADMA 2010) Best Paper Award, The chief of air staff: Letter of Appreciation Award, Engineering Sciences Society: Contribution Award in 2012, and Prizes for Science and Technology, The Commendation for Science and Technology by the Minister of Education, Culture, Sports, Science and Technology. She is a member of the International Association for Cryptologic Research, the Institute of Electronics, Information and Communication Engineers, the Information Processing Society of Japan, and the Mathematical Society of Japan.