IEICE TRANS. FUNDAMENTALS, VOL.E100–A, NO.1 JANUARY 2017

PAPER Special Section on Cryptography and Information Security

Refined Construction of RC4 Key Setting in WPA**

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

SUMMARY The RC4 stream cipher is widely used including WEP and WPA, which are the security protocols for IEEE 802.11 wireless standard. WPA improved a construction of the RC4 key setting known as TKIP to avoid the known WEP attacks. The first 3-byte RC4 keys generated by IV in WPA are known since IV can be obtained by observing packets. The weaknesses in TKIP using the known IV were reported by Sen Gupta et al. at FSE 2014 and by Ito and Miyaji at FSE 2015. Both showed that TKIP induces many RC4 key correlations including the keystream bytes or the unknown internal states. Ideally TKIP should be constructed in such a way that it can keep the security level of generic RC4. In the first part of this paper, we will provide newly theoretical proofs of 17 correlations remain unproven in our previous work theoretically. Our theoretical analysis can make clear how TKIP induces biases of internal states in generic RC4. In the second part of this paper, we will further provide a refined construction of the RC4 key setting. As a result, we can reduce the number of correlations in the refined construction by about 70% in comparison with that in the original setting.

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

1. Introduction

RC4 is the stream cipher designed by Rivest in 1987, and is widely used in various security protocols such as Secure Socket Layer/Transport Layer Security (SSL/TLS), Wired Equivalent Privacy (WEP), Wi-fi Protected Access (WPA). After the disclosure of RC4 algorithm in 1994, RC4 has been intensively analyzed over the past two decades. There are mainly two approaches to the cryptanalysis on RC4. One is to demonstrate the existence of events with non-randomness known as *bias* involving the RC4 key, the internal state variables, and the output pseudo-random sequence (keystream) bytes [11], [13], [18]. Now, we refer to the event with the probability significantly higher or lower than the probability of random association as the *positive bias* or the *negative bias*, respectively. The other is to attack on RC4 using biases in order to recover the RC4 key (key recovery attacks) [17], [19], the internal state variables (state recovery attacks) [1], [10], [14] and the plaintexts (plaintext recovery attacks) [11], [13]. In addition, many cryptanalysis on the security protocols have been reported such as the plaintext recovery attacks on SSL/TLS [6], [15], the key recovery attacks on WEP [3], [9], [20] and the plaintext recovery attacks on WPA [4], [16].

1.1 Description of RC4

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 initializes the initial state from a secret key K of l bytes to become the input of the PRGA. Once the internal state is initialized in the KSA, the PRGA outputs a keystream byte $Z_1, Z_2, \ldots, Z_r$ in each round, 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**

Manuscript received March 23, 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.

[**]The part of this paper was presented at ACISP 2015 [7].

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

DOI: 10.1587/transfun.E100.A.138

1.2 Description of WPA

WPA is the security protocol for IEEE 802.11 wireless networks standardized as a substitute for WEP in 2003. It improves a construction of a 16-byte RC4 key setting, which is known as Temporal Key Integrity Protocol (TKIP), from that in WEP. 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). 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 then, 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 keys, $K[0]$, $K[1]$ and $K[2]$, are derived from the last 16-bit IV (IV16) as follows:

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

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

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

We note that the first 3-byte RC4 key in WPA are known since IV can be obtained by observing packets.

1.3 Our Motivations and Contributions

In 2014, Sen Gupta et al. demonstrated a probability distribution of $K[0] + K[1]$ in WPA [4]. They further found some linear correlations between the keystream byte 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. Their linear correlations can be applied to a plaintext recovery attack on WPA in the same way as the existing attack on SSL/TLS [6], and contribute to reduce the computational complexity necessary for the attack. In 2015, Ito and Miyaji further extended the linear correlations by including unknown internal state variables, which mean $S_r[i_{r+1}]$, $S_r[i_{r+1}]$, j_{r+1} and t_{r+1} for $r \geq 0$, in both generic RC4 and WPA [8]. As a result, more than 150 linear correlations have been found experimentally, although they have proved only the following 6 correlations theoretically: $S_0[i_1] = K[0]$, $K[0] - K[1] - 3$ or $K[0] - K[1] - 1$; $S_{255}[i_{256}] = K[0]$ or $K[1]$; $S_r[i_{r+1}] = K[0] + K[1] + 1$ $(0 \leq r \leq N)$.

We focus on the linear correlations that remain unproven theoretically. Actually, linear correlations including unknown internal state variables could be applied to a state recovery attack on WPA in the same way as the existing attacks on generic RC4 [1], [10], [14]. In addition, theoretical proofs of linear correlations can make clear how TKIP induces biases as pointed out above. If we demonstrate how many rounds these biases have been kept in the internal states, then the RC4 key setting in WPA can be reconstructed securely while keeping congruity with TKIP. TKIP should have been constructed in such a way that it can keep original security level of generic RC4. Our analysis would be also useful to investigate a generic construction of key setting including the known IV in such a way that it can keep security level of original encryption.

In this paper, we will provide theoretical proofs of 17 cases out of our linear correlations remain unproven theoretically. Our contributions of 13 theorems can be summarized as follows:

- Theorems 1 and 2 show $\Pr(S_0[i_1] = -K[0] - K[1] - 3)$ in generic RC4 and WPA, respectively. Theorems 5 and 7 show $\Pr(S_1[i_2] = -K[0] - K[1] + K[2] - 1)$ and $\Pr(S_1[i_2] = K[0] - K[1] + K[2] + x)$ $(x \in \{-3, -1, 1\})$. These theorems only in WPA provide about double probabilities of random association $\frac{1}{N}$.
- Theorem 3 shows $\Pr(S_0[i_1] = K[0] + K[1] + K[2] + 3)$ is less than half of the probability of random association $\frac{1}{N}$ in both generic RC4 and WPA.
- Theorem 4 shows $\Pr(S_1[i_2] = K[0] + K[1] + K[2] + 3)$ is pretty high probability in comparison to the probability of random association $\frac{1}{N}$ in both generic RC4 and WPA. This is induced by Roos' bias, that is $\Pr(S_0[2] = K[0] + K[1] + K[2] + 3) \approx (1 - \frac{2}{N}) \cdot (1 - \frac{1}{N})^{N+3} + \frac{1}{N}$.
- Theorem 6 shows $\Pr(S_1[i_2] = K[1] + K[2] + 3)$ is about double probabilities of random association $\frac{1}{N}$.
- Theorem 8 shows $\Pr(S_1[i_2] = K[0] - K[1] + K[2] + 3)$ is a positive bias in generic RC4 but a negative bias in WPA.
- Theorems 9–13 provide theoretical analysis related to the second round index j_2.

Theorems 1, 2 and 9–13 have been refined from our preliminary version [7], whereas Theorems 6 and 8 have been newly proved.

We will further provide a refined construction of the RC4 key setting in WPA in such a way that it can keep the security level of generic RC4. In order to find the refined construction, we carefully set the 3-byte RC4 key, $K[x]$, $K[y]$ and $K[z]$, derived from the known IV in the same way as original setting (Eqs. (1)–(3)) as follows:

$$K[x] = (\mathrm{IV16} >> 8)\ \&\ \mathrm{0xFF},$$

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

$$K[z] = \mathrm{IV16}\ \&\ \mathrm{0xFF}.$$

As a result of our experiments, the number of linear correlations in our setting (e.g. $x = 9$, $y = 12$ and $z = 15$) can be reduced by about 70% in comparison with that in the original setting.

1.4 Organization of This Paper

This paper is organized as follows: Section 2 summarizes the previous works for both theoretical proofs and experiments. Section 3 shows the theoretical proofs of our linear correlations and the experimental results. Section 4 presents the refined construction of the RC4 key setting in WPA. Section 5 concludes this paper.

2. Preliminary

Let us summarize some previous results which will be used in both theoretical proofs and experiments. Proposition 1 shows Roos' biases [18], correlations between the RC4 key bytes and S_0, proved by Paul and Maitra [17]. Proposition 2 shows biases of S_0, proved by Mantin [12]. Proposition 3 shows a distribution of $K[0] + K[1]$ in WPA, proved by Sen Gupta et al. [4]. By combining Proposition 3 with Proposition 1 (Roos' biases), a characteristic bias on the distribution of $S_0[1]$ is given as Proposition 4 [4]. Finally, Mantin and Shamir showed Proposition 5 related to the number of samples necessary for distinguishing two distributions with a constant probability of success [13].

Proposition 1 ([17]): In the initial state of the PRGA for $0 \le y \le N-1$, 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 ([12]): In the initial state of the PRGA for $0 \le u \le N-1$, $0 \le v \le N-1$, we have

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

Proposition 3 ([4]): For $0 \le v \le N-1$, the distribution of the sum v of $K[0]$ and $K[1]$ generated by the temporal key hash function in WPA is given as follows:

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

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

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

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

Proposition 5 ([13]): 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 Proved Linear Correlations

3.1 Experimental Observations

In 2014, linear correlations including the keystream bytes Z_r were investigated by Sen Gupta et al. [4], and used a general linear equation

$$Z_r = a \cdot K[0] + b \cdot K[1] + c \cdot K[2] + d, \tag{4}$$

where $a, b, c \in \{0, \pm 1\}$ and $d \in \{0, \pm 1, \pm 2, \pm 3\}$ for $r \ge 1$.

In 2015, Ito and Miyaji further extended the linear correlations by including unknown internal states variables $X_r \in \{S_r[i_{r+1}], S_r[j_{r+1}], j_{r+1}, t_{r+1}\}$

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

where $a, b, c, d \in \{0, \pm 1\}$, and $e \in \{0, \pm 1, \pm 2, \pm 3\}$ for $r \ge 0$ [8]. In addition, they examined all $4 \cdot 3^4 \cdot 7$ equations of Eq. (5) in each round in both generic RC4 and WPA. As a result, they discovered more than 150 correlations with positive or negative biases, and proved the following 6 cases theoretically:

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

In this paper, we will provide newly theoretical proofs of 17 linear correlations listed in Table 1. Our linear correlations including unknown internal state variables could contribute to finding a correct internal state of RC4 in WPA. Actually, the first state recovery attack proposed by Knudsen et al. reconstructs the internal state of RC4 by computing optimum solutions of four unknown variables in each round such as $S_r[i_{r+1}]$, $S_r[j_{r+1}]$, j_{r+1} and t_{r+1} for $r \ge 0$ [10].

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

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

X_r	Linear correlations	RC4	WPA	Remarks
$S_0[i_1]$	$-K[0] - K[1] - 3$	0.005336	0.008437	Theorems 1 and 2
	$K[0] + K[1] + K[2] + 3$	0.001492	0.001491	Theorem 3
$S_1[i_2]$	$K[0] + K[1] + K[2] + 3$	0.360357	0.361718	Theorem 4
	$-K[0] - K[1] + K[2] - 1$	0.005305	0.008197	Theorem 5
	$K[1] + K[2] + 3$	0.008157	0.008092	Theorem 6
	$K[0] - K[1] + K[2] - 3$	0.005295	0.008163	Theorem 7
	$K[0] - K[1] + K[2] - 1$	0.005290	0.008171	Theorem 7
	$K[0] - K[1] + K[2] + 1$	0.005309	0.008171	Theorem 7
	$K[0] - K[1] + K[2] + 3$	0.005310	0.002838	Theorem 8
j_2	$K[2]$	0.004428	0.005571	Theorem 9
	$-K[0] - K[1] + K[2] - 2$	0.003921	0.004574	Theorem 10
	$-K[0] - K[1] + K[2]$	0.003919	0.005573	Theorem 10
	$-K[0] - K[1] + K[2] + 2$	0.003912	0.004545	Theorem 10
	$-K[0] + K[1] + K[2]$	0.003921	0.005501	Theorem 11
	$-K[1] + K[2] - 2$	0.003911	0.005479	Theorem 12
	$-K[1] + K[2] + 3$	0.003899	0.005476	Theorem 12
	$K[0] - K[1] + K[2]$	0.003918	0.005618	Theorem 13

WPA, except $K[0]$, $K[1]$ and $K[2]$ in WPA generated by IV using a sequence counter.

3.2 Biases in $S_0[i_1]$

In this section, we prove Theorems 1–3 theoretically. Theorems 1 and 2 show 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 $\frac{1}{N}$ in WPA, respectively. We note that Theorem 2 means the first round internal state $S_0[i_1]$ can be guessed in a double probability of random association $\frac{1}{N}$ by using known $K[0]$ and $K[1]$ in WPA. Theorem 3 shows event $S_0[i_1] = K[0]+K[1]+K[2]+3$ yields a negative bias in both generic RC4 and WPA. In addition, Theorems 1 and 2 are revised precisely from our preliminary version [7].

Theorem 1: In the initial state of the PRGA in generic RC4, we have

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

Proof : The probability of event $S_0[i_1] = -K[0]-K[1]-3$ in generic RC4 can be decomposed in two paths: $K[0]+K[1] = 126, 254$ (Path 1) and $K[0]+K[1] \neq 126, 254$ (Path 2). These paths include all events in order to compute $\Pr(S_0[i_1] = -K[0] - K[1] - 3)_{\mathrm{RC4}}$. In the following proof, we use $S_0[1]$ instead of $S_0[i_1]$ ($i_1 = 1$) for simplicity.

Path 1. Since $-K[0] - K[1] - 3 = K[0] + K[1] + 1$ under the condition of Path 1, event $S_0[1] = -K[0] - K[1] - 3$ always occurs when $S_0[1] = K[0] + K[1] + 1$. In addition, 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

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

Path 2. Since $-K[0] - K[1] - 3 \neq K[0] + K[1] + 1$ under the condition of Path 2, event $S_0[1] = -K[0]-K[1]-3$ never occurs when $S_0[1] = K[0] + K[1] + 1$. If $S_0[1] \neq K[0] + K[1] + 1$ holds, then we assume that event $S_0[1] = -K[0] - K[1] - 3$ occurs with the probability of random association $\frac{1}{N}$. Therefore, we get

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

In summary, since we assume that K is generated uniformly at random in generic RC4, we get

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

□

Before showing Theorem 2, we describe a corollary of Proposition 3. In the preliminary version [7], the relative error of event $S_0[i_1] = -K[0] - K[1] - 3$ in WPA is slightly large such as 2.658 %. This is because we proved the event in WPA in the same way as the theoretical proof of that in generic RC4 since we could not treat with a probability distribution of $-K[0] - K[1]$. Corollary 1 improves the relative error of the event in WPA in Theorem 2. Table 2 shows the probability distribution of $-K[0] - K[1]$ in WPA.

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

$K[0]$	$K[1]$ (depends on $K[0]$)		$-K[0] - K[1]$ (only even)	
Range	Value	Range	Value	Range
0 – 31	$K[0] + 32$	32 – 63	$-2K[0] - 32$	161 – 224
32 – 63	$K[0]$	32 – 63	$-2K[0]$	129 – 192
64 – 95	$K[0] + 32$	96 – 127	$-2K[0] - 32$	33 – 96
96 – 127	$K[0]$	96 – 127	$-2K[0]$	1 – 64
128 – 159	$K[0] - 96$	32 – 63	$-2K[0] + 96$	35 – 96
160 – 191	$K[0] - 128$	32 – 63	$-2K[0] + 128$	1 – 64
192 – 223	$K[0] - 96$	96 – 127	$-2K[0] + 96$	161 – 224
224 – 255	$K[0] - 128$	96 – 127	$-2K[0] + 128$	129 – 192

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

$$\begin{aligned}&\Pr(-K[0] - K[1] = v) = 0 && \text{if } v \text{ is odd,}\\ &\Pr(-K[0] - K[1] = v) = 0 && \text{if } v \text{ is even and}\\ &&& v \in [97, 128] \cup [225, 256],\\ &\Pr(-K[0] - K[1] = v) = \tfrac{2}{256} && \text{if } v \text{ is even and}\\ &&& v \in [1, 32] \cup [65, 96] \cup\\ &&& \quad [129, 160] \cup [193, 224],\\ &\Pr(-K[0] - K[1] = v) = \tfrac{4}{256} && \text{if } v \text{ is even and}\\ &&& v \in [33, 64] \cup [161, 192].\end{aligned}$$

Theorem 2: In the initial state of the PRGA in generic RC4 for $0 \leq x \leq N-1$, we have

$$\begin{aligned}&\Pr(S_0[i_1] = -K[0] - K[1] - 3)_{\mathrm{WPA}}\\ &\approx \tfrac{4}{N}(\alpha_1 + \tfrac{1}{N}(1-\alpha_1)) + \tfrac{1}{N}\textstyle\sum_{x \neq 2,130} \Pr(-K[0] - K[1] = x)(1-\tfrac{1}{N})^{x-5}.\end{aligned}$$

Proof : The probability of event $S_0[i_1] = -K[0] - K[1] - 3$ in WPA can be decomposed in two paths: $-K[0] - K[1] = 2, 130$ (Path 1) and $-K[0] - K[1] \neq 2, 130$ (Path 2). These paths include all events in order to compute $\Pr(S_0[i_1] = -K[0] - K[1] - 3)_{\mathrm{WPA}}$. Under such conditions, we have

$$-K[0] - K[1] = x \Leftrightarrow K[0] + K[1] = N - x. \tag{6}$$

In the following proof, we use $S_0[1]$ instead of $S_0[i_1]$ ($i_1 = 1$) for simplicity.

Path 1. Since $-K[0] - K[1] - 3 = K[0] + K[1] + 1$ from Eq. (6) under the condition of Path 1, event $S_0[1] = -K[0] - K[1] - 3$ always occurs when $S_0[1] = K[0] + K[1] + 1$. In addition, 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

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

Path 2. Let $-K[0] - K[1] = x$. Since $-K[0] - K[1] - 3 \neq K[0] + K[1] + 1$ from Eq. (6) under the condition of Path 2, event $S_0[1] = -K[0] - K[1] - 3$ $(= x - 3)$ never occurs when $S_0[1] = K[0] + K[1] + 1$. After the second round of the KSA, we note that both $S_2^K[1] = K[0]+K[1]+1 = N-x+1$ and $S_2^K[x-3] = x-3$ hold from Eq. (6) and Algorithm 1. Thereafter, if $S_r^K[x-3] \neq S_2^K[x-3]$ for $3 \leq r \leq x-3$, event $S_0[1] = -K[0] - K[1] - 3$ $(= x - 3)$ never occurs. When $S_r^K[x-3] = S_2^K[x-3] = x-3$ is satisfied, whose probability is $(1-\frac{1}{N})^{x-5}$ approximately, we assume that event $S_0[1] = -K[0] - K[1] - 3$ occurs with the probability of random association $\frac{1}{N}$ since $S_{x-2}[1]$ may be swapped from $S_{x-3}[x-3]$. Therefore, we get

$$\Pr(S_0[1] = -K[0] - K[1] - 3 \mid \text{Path 2}) \approx \tfrac{1}{N}(1-\tfrac{1}{N})^{x-5}.$$

In summary, we get

$$\begin{aligned}
&\Pr(S_0[1] = K[0] - K[1] - 3)_{\text{WPA}} \\
&= \Pr(S_0[1] = K[0] - K[1] - 3 \mid \text{Path 1}) \cdot \Pr(\text{Path 1}) \\
&\quad + \Pr(S_0[1] = K[0] - K[1] - 3 \mid \text{Path 2}) \cdot \Pr(\text{Path 2}) \\
&\approx \tfrac{4}{N}(\alpha_1 + \tfrac{1}{N}(1-\alpha_1)) + \tfrac{1}{N}\textstyle\sum_{x \neq 2,130} \Pr(-K[0]-K[1]=x)(1-\tfrac{1}{N})^{x-5},
\end{aligned}$$

where $\Pr(-K[0] - K[1] = x)$ follows Lemma 1. □

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

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

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

$$j_1^K = K[0], \tag{7}$$

$$j_2^K = K[0] + K[1] + S_1^K[1] = K[0] + K[1] + 1, \tag{8}$$

$$\begin{aligned}
j_3^K &= K[0] + K[1] + K[2] + S_1^K[1] + S_2^K[2] \qquad (9)\\
&= K[0] + K[1] + K[2] + 3. \qquad (10)
\end{aligned}$$

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

Path 1. If $j_1^K = 1$, then $S_1^K[1] \neq 1$ from step 7 in Algorithm 1. Thus, $S_3^K[2] \neq K[0] + K[1] + K[2] + 3$ always holds since $j_3^K \neq K[0] + K[1] + K[2] + 3$ from Eq. (10) under the condition of Path 1. Similarly, if $j_1^K = 2$, then $S_3^K[2] \neq K[0] + K[1] + K[2] + 3$ always holds. We then assume that event $S_0[1] = K[0] + K[1] + K[2] + 3$ occurs with the probability of random association $\frac{1}{N}$. Therefore, we get

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

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

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

Path 2-2. Except in the above paths, Eqs. (7)–(10) always hold since we get both $S_1^K[1] = 1$ and $S_2^K[2] = 2$. Now, if $K[2] = 254$, then $j_2^K = j_3^K = K[0] + K[1] + K[2] + 3$ holds since $K[2] + 3 = 1$. Thus, we get both $S_3^K[1] = K[0] + K[1] + K[2] + 3$ and $S_3^K[2] = 1$ from step 7 in Algorithm 1. After the third round of the KSA, $S_r^K[1] = S_3^K[1]$ for $4 \leq r \leq N$ if $j_r^K \neq 1$ during the subsequent $N - 3$ rounds, whose probability is $(1 - \frac{1}{N})^{N-3}$ approximately since we assume that $j_r^K = 1$ holds with the probability of random association $\frac{1}{N}$. Therefore, we get

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

Path 2-3. As with the discussion in Path 2-2, Eqs. (7)–(10) always hold, and $j_2^K \neq j_3^K$ since $K[2] \neq 254$ under the condition of Path 2-3. Therefore, since event $S_0[i_1] = K[0] + K[1] + K[2] + 3$ never occurs, we get

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

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

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

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

3.3 Biases in $S_1[i_2]$

In this section, we prove Theorems 4–8 theoretically. Theorem 4 shows event $S_1[i_2] = K[0] + K[1] + K[2] + 3$ occurs with pretty high probability in both generic RC4 and WPA. It is induced by Roos' bias, that is $\alpha_2 = \Pr(S_0[2] = K[0]+K[1]+K[2]+3)$. Theorems 5 and 7 show 4 events on $S_1[i_2]$ yield a positive bias in both generic RC4 and WPA. In addition, Theorems 6 and 8 are newly proved here after we

presented in our preliminary version [7]. Theorem 6 shows event $S_1[i_2] = K[1]+K[2]+3$ occurs with a double probability of random association $\frac{1}{N}$ in both generic RC4 and WPA. Theorem 8 shows event $S_1[i_2] = K[0] - K[1] + K[2] + 3$ yields a positive bias in generic RC4 but a negative bias in WPA. We note that Theorems 4–7 mean the second round internal state $S_1[i_2]$ can be guessed in high probability by using known $K[0]$, $K[1]$ and $K[2]$ in WPA. In order to prove the following theorems, let us denote the results of Theorems 3 and 4 as $\beta = \Pr(S_0[1] = K[0] + K[1] + K[2] + 3)$ and $\gamma = \Pr(S_1[2] = K[0] + K[1] + K[2] + 3)$, respectively.

Theorem 4: After the first round of the PRGA, we have

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

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

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

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

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

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

In summary, we get

$$\begin{aligned}
&\Pr(S_1[2]=K[0]+K[1]+K[2]+3)\\
&= \Pr(S_1[2]=K[0]+K[1]+K[2]+3\,|\,\text{Path 1})\cdot\Pr(\text{Path 1})\\
&\quad + \Pr(S_1[2]=K[0]+K[1]+K[2]+3\,|\,\text{Path 2})\cdot\Pr(\text{Path 2})\\
&\approx \beta\cdot\Pr(j_1=2) + \alpha_2\cdot(1-\Pr(j_1=2))\\
&= \beta\cdot\Pr(S_0[1]=2) + \alpha_2\cdot(1-\Pr(S_0[1]=2)),
\end{aligned}$$

where $\Pr(S_0[1] = 2)$ follows Propositions 2 and 4 in generic RC4 and WPA, respectively. □

Theorem 5: After the first round of the PRGA, we have

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

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

Path 1. Since $-K[0]-K[1]+K[2]-1 = K[0]+K[1]+K[2]+3$ under the condition of Path 1, event $S_1[2] = -K[0] - K[1] + K[2] - 1$ always occurs when $S_1[2] = K[0] + K[1] + K[2] + 3$. In addition, if $S_0[1] \neq K[0] + K[1] + 1$ holds, then we assume that event $S_1[2] = -K[0] - K[1] + K[2] - 1$ occurs with the probability of random association $\frac{1}{N}$. Therefore, we get

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

Path 2. Since $-K[0]-K[1]+K[2]-1 \neq K[0]+K[1]+K[2]+3$ under the condition of Path 2, event $S_1[2] = -K[0] - K[1]+K[2]-1$ never occurs when $S_1[2] = K[0]+K[1]+K[2] + 3$. If $S_1[2] \neq K[0] + K[1] + K[2] + 3$, then we assume that event $S_1[2] = -K[0] - K[1] + K[2] - 1$ occurs with the probability of random association $\frac{1}{N}$. Therefore, we get

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

The probability of $K[0] + K[1] = 126$ and 254 in WPA is $\frac{2}{N}$ from Proposition 3, respectively. On the other hand, that in generic RC4 is $\frac{1}{N}$ since K is generated uniformly at random. By substituting each $\Pr(K[0] + K[1] = 126, 254)$ in both generic RC4 and WPA, we get

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

□

Before showing Theorem 6, we prove Lemma 1. Lemma 1 shows event $S_0[2] = K[1] + K[2] + 3$ yields a positive bias in both generic RC4 and WPA. In order to prove the following theorems, let us denote the result of Lemma 1 as $\eta = \Pr(S_0[2] = K[1] + K[2] + 3)$.

Lemma 1: After the first round of the PRGA, we have

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

Proof : The probability of event $S_0[2] = K[1] + K[2] + 3$ can be decomposed in four paths: $j_1^K = 0$ (Path 1), $j_1^K = 1$ (Path 2), $j_1^K = 2$ (Path 3) and $j_1^K \neq 0, 1, 2$ (Path 4). Paths 1-3 are further divided into two subpaths: $j_2^K = 2$ (Paths 1-1, 2-1 and 3-1) and $j_2^K \neq 2$ (Paths 1-2, 2-2 and 3-2). These paths include all events in order to compute $\Pr(S_1[i_2] = -K[0] - K[1] + K[2] - 1)$. In the following proof, we assume that the values of index j^K are distributed with the probability of random association $\frac{1}{N}$.

Path 1-1. Since $K[0] = 0$, $S_1^K[1] = 1$ and $S_2^K[2] = 1$ under the condition of Path 1-1, $j_3^K = K[1] + K[2] + 2$ holds from Eq. (9). Then, $S_3^K[0] = 0$, $S_3^K[1] = 2$ and $S_3^K[2] = K[1] + K[2] + 2$ from step 7 in Algorithm 1. If $K[1] + K[2] + 3 = 0$ or 2, event $S_0[2] = K[1] + K[2] + 3$ never occurs. When $K[1] + K[2] + 3 \neq 0$ and 2 are satisfied, we assume that event $S_0[2] = K[1] + K[2] + 3$ occurs with the probability of random association $\frac{1}{N}$. Therefore, we get

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

Similarly, the probability of event $S_0[2] = K[1] + K[2] + 3$ under the conditions of Paths 2-1, 3-1 and 4 can be computed.

Path 1-2. Since $K[0] = 0$, $S_1^K[1] = 1$ and $S_2^K[2] = 2$ under the condition of Path 1-2, $j_3^K = K[1] + K[2] + 3$ holds from Eq. (9). Then, $S_3^K[2] = K[1] + K[2] + 2$ from step 7 in Algorithm 1. After the third round of the KSA, $S_r^K[2] = S_3^K[2]$ for $4 \leq r \leq N$ if $j_r^K \neq 2$ during the subsequent $N - 3$ rounds, whose probability is $(1 - \frac{1}{N})^{N-3}$ approximately. Therefore, we get

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

Similarly, the probability of event $S_0[2] = K[1] + K[2] + 3$ under the conditions of Paths 2-2 and 3-2 can be computed.

In summary, we get

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

□

Theorem 6: After the first round of the PRGA, we have

$$\Pr(S_1[i_2] = K[1] + K[2] + 3) \approx \eta(1 - \tfrac{1}{N}) + \tfrac{1}{N^2}.$$

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

Path 1. Since $S_1[2] = S_0[1]$ from step 5 in Algorithm 2 under the condition of Path 1, event $S_1[i_2] = K[1] + K[2] + 3$ always occurs if and only if $S_0[1] = K[1] + K[2] + 3$. We then assume that $K[1] + K[2] + 3 = 2$ ($j_1 = S_0[1]$) holds with the probability of random association $\frac{1}{N}$. Therefore, we get

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

Path 2. Since $S_1[2] = S_0[2]$ from step 5 in Algorithm 2 under the condition of Path 2, event $S_1[i_2] = K[1] + K[2] + 3$ always occurs if and only if $S_0[2] = K[1] + K[2] + 3$. We then assume that both $j_1 \neq 2$ and $S_0[2] = K[1] + K[2] + 3$ are mutually independent events. Therefore, we get

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

In summary, we get

$$\begin{aligned}
&\Pr(S_1[2] = K[1] + K[2] + 3) \\
&= \Pr(S_1[2] = K[1] + K[2] + 3 \mid \text{Path 1}) \cdot \Pr(\text{Path 1}) \\
&\quad + \Pr(S_1[2] = K[1] + K[2] + 3 \mid \text{Path 2}) \cdot \Pr(\text{Path 2}) \\
&\approx \eta(1 - \tfrac{1}{N}) + \tfrac{1}{N^2}.
\end{aligned}$$

□

Theorem 7: After the first round of the PRGA for $x \in \{-3, -1, 1\}$, we have

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

We can prove Theorem 7 in the same way as Theorem 5.

Theorem 8: After the first round of the PRGA, we have

$$\begin{aligned}
&\Pr(S_1[i_2] = K[0] - K[1] + K[2] + 3) \\
&\quad \approx \begin{cases} \frac{2}{N}(\gamma + \frac{1}{N}(1 - \gamma)) + \frac{1}{N}(1 - \frac{2}{N})(1 - \gamma) & \text{for RC4,} \\ \frac{1}{4N}((1 - \frac{1}{N})^{N-2} + (4 - \frac{1}{N})(1 - \gamma)) & \text{for WPA.} \end{cases}
\end{aligned}$$

Proof : The probability of event $S_1[i_2] = K[0] - K[1] + K[2] + 3$ in generic RC4 are proved in the same way as Theorem 5. The probability of event $S_1[i_2] = K[0] - K[1] + K[2] + 3$ in WPA can be decomposed in two paths: $K[0] = K[1]$ (Path 1) and $K[0] \neq K[1]$ (Path 2). Path 1 is further divided into two subpaths: $K[2] = 254$ (Path 1-1) and $K[2] \neq 254$ (Path 1-2). These paths include all events in order to compute $\Pr(S_1[i_2] = K[0] - K[1] + K[2] + 3)$. In the following proof, we use $S_1[2]$ instead of $S_1[i_2]$ ($i_2 = 2$) for simplicity.

Path 1-1. $K[0] - K[1] + K[2] + 3 = 1$ and Eqs. (7), (8) and (10) always hold under the condition of Path 1-1. Then, $S_3^K[2] = S_2^K[j_3^K] = S_2^K[j_2^K] = S_1^K[i_1] = S_1^K[1] = S_0^K[1] = 1$ ($= K[0] - K[1] + K[2] + 3$) from Algorithm 1 since $j_3^K = j_2^K = K[0] + K[1] + 1$ (note that $K[2] = 254$). After the third round of the KSA, $S_1[2] = S_3^K[2]$ if the values of index j are not equal to 2 during the subsequent $N - 2$ rounds, whose probability is $(1 - \frac{1}{N})^{N-2}$. Therefore, we get

$$\Pr(S_1[2] = K[0] - K[1] + K[2] + 3 \mid \text{Path 1-1}) \approx (1 - \tfrac{1}{N})^{N-2}.$$

Path 1-2. Since $K[0] - K[1] + K[2] + 3 \neq K[0] + K[1] + K[2] + 3$ under the condition of Path 1-2 (note that $K[1] \neq 0, 128$ in WPA from Proposition 3), event

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

$$\Pr(S_1[2] = K[0] - K[1] + K[2] + 3 \mid \text{Path 1-2}) \approx \tfrac{1}{N}(1-\gamma).$$

Similarly, the probability of event $S_1[2] = K[0] - K[1] + K[2] + 3$ under the condition of Path 2 can be computed.

The probability of $K[0] = K[1]$ in WPA is $\frac{1}{4}$ from Proposition 3. Therefore, we get

$$\begin{aligned}
&\Pr(S_1[2] = K[0] - K[1] + K[2] + 3)_{\text{WPA}} \\
&= \Pr(S_1[2] = K[0] - K[1] + K[2] + 3 \mid \text{Path 1-1}) \cdot \Pr(\text{Path 1-1}) \\
&\quad + \Pr(S_1[2] = K[0] - K[1] + K[2] + 3 \mid \text{Path 1-2}) \cdot \Pr(\text{Path 1-2}) \\
&\quad + \Pr(S_1[2] = K[0] - K[1] + K[2] + 3 \mid \text{Path 2}) \cdot \Pr(\text{Path 2}) \\
&\approx \tfrac{1}{4N}((1 - \tfrac{1}{N})^{N-2} + (4 - \tfrac{1}{N})(1 - \gamma)).
\end{aligned}$$

□

3.4 Biases in j_2

In this section, we prove Theorems 9–13 theoretically. Theorem 9 shows event $j_2 = K[2]$ yields a positive bias in both generic RC4 and WPA. By contrast, Theorems 10–13 show 7 events on j_2 yield positive biases only in WPA but those are not biases in generic RC4. Now, we present only the proof of Theorem 9 since Theorems 10–13 are proved in the same way as Theorem 9. Theorems 9–13 are refined precisely by further analyzing a condition that an event occurs (see Path 1 in the proof of Theorem 9) from our preliminary version [7]. In order to prove the following theorems, let us denote the result of Theorem 4 as $\gamma = \Pr(S_1[2] = K[0] + K[1] + K[2] + 3)$.

Theorem 9: After the second round of the PRGA, we have

$$\Pr(j_2 = K[2]) \approx \begin{cases} \frac{1}{N} + \frac{1}{N}\alpha_1\gamma & \text{for RC4,} \\ \frac{1}{N} + \frac{3}{N}\alpha_1\gamma & \text{for WPA.} \end{cases}$$

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

Path 1. Assuming that both $S_0[1] = K[0] + K[1] + 1$ and $S_1[2] = K[0] + K[1] + K[2] + 3$ occur simultaneously, we get

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

When the above condition is satisfied, event $j_2 = K[2]$ always occurs since $K[2] = 2K[0] + 2K[1] + K[2] + 4$ under the condition of Path 1. By contrast, if the above condition is not satisfied, then we assume that event $j_2 = K[2]$ occurs with the probability of random association $\frac{1}{N}$. We also assume that both $S_0[1] = K[0] + K[1] + 1$ and $S_1[2] = K[0] + K[1] + K[2] + 3$ are mutually independent events. Therefore, we get

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

Path 2. Since $K[2] \neq 2K[0] + 2K[1] + K[2] + 4$ under the condition of Path 2, event $j_2 = K[2]$ never occurs when both $S_0[1] = K[0] + K[1] + 1$ and $S_1[2] = K[0] + K[1] + K[2] + 3$ occur simultaneously. If either $S_0[1] \neq K[0] + K[1] + 1$ or $S_1[2] \neq K[0] + K[1] + K[2] + 3$ hold, then we assume that event $j_2 = K[2]$ occurs with the probability of random association $\frac{1}{N}$. Therefore, we get

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

The probability of $K[0] + K[1] = 126$ and 254 in WPA is $\frac{2}{N}$ from Proposition 3, respectively. On the other hand, that in generic RC4 is $\frac{1}{N}$ since K is generated uniformly at random. By substituting each $\Pr(K[0] + K[1] = 126, 254)$ in both generic RC4 and WPA, we get

$$\begin{aligned}
\Pr(j_2 = K[2]) &= \Pr(j_2 = K[2] \mid \text{Path 1}) \cdot \Pr(\text{Path 1}) \\
&\quad + \Pr(j_2 = K[2] \mid \text{Path 2}) \cdot \Pr(\text{Path 2}) \\
&\approx \begin{cases} \frac{2}{N}(\alpha_1\gamma + \frac{1}{N}(1 - \alpha_1\gamma)) + \frac{1}{N}(1 - \frac{2}{N})(1 - \alpha_1\gamma) & \text{for RC4,} \\ \frac{4}{N}(\alpha_1\gamma + \frac{1}{N}(1 - \alpha_1\gamma)) + \frac{1}{N}(1 - \frac{4}{N})(1 - \alpha_1\gamma) & \text{for WPA} \end{cases} \\
&= \begin{cases} \frac{1}{N} + \frac{1}{N}\alpha_1\gamma & \text{for RC4,} \\ \frac{1}{N} + \frac{3}{N}\alpha_1\gamma & \text{for WPA.} \end{cases}
\end{aligned}$$

□

Theorem 10: After the second round of the PRGA for $x \in \{-2, 0, 2\}$, we have

$$\Pr(j_2 = -K[0] - K[1] + K[2] + x) \approx \begin{cases} \frac{1}{N} & \text{for RC4,} \\ \frac{1}{N} + \frac{1}{N}\alpha_1\gamma & \text{if } x = \pm 2 \text{ for WPA,} \\ \frac{1}{N} + \frac{3}{N}\alpha_1\gamma & \text{if } x = 0 \text{ for WPA.} \end{cases}$$

Theorem 11: After the second round of the PRGA, we have

$$\Pr(j_2 = -K[0] + K[1] + K[2]) \approx \begin{cases} \frac{1}{N} & \text{for RC4,} \\ \frac{1}{N} + \frac{3}{N}\alpha_1\gamma & \text{for WPA.} \end{cases}$$

Theorem 12: After the second round of the PRGA for $x \in \{-2, 3\}$, we have

$$\Pr(j_2 = -K[1] + K[2] + x) \approx \begin{cases} \frac{1}{N} & \text{for RC4,} \\ \frac{1}{N} + \frac{3}{N}\alpha_1\gamma & \text{for WPA.} \end{cases}$$

Theorem 13: After the second round of the PRGA, we have

$$\Pr(j_2 = K[0] - K[1] + K[2]) \approx \begin{cases} \frac{1}{N} & \text{for RC4,} \\ \frac{1}{N} + \frac{3}{N}\alpha_1\gamma & \text{for WPA.} \end{cases}$$

3.5 Experimental Results

We have conducted experiments on Theorems 1–13 in the following environment in order to confirm the accuracy of theorems: Intel(R) Core(TM) i3-3220M CPU with 3.30 GHz, 3.8 GiB memory, gcc 4.8.2 compiler and C language. The number of samples necessary for our experiments is at least $O(N^3)$ according to Proposition 5. This is why each correlation has a relative bias with the probability of at least $O(\frac{1}{N})$. Then, we have used N^5 randomly generated RC4 keys in both generic RC4 and WPA. The number of these samples satisfies a condition to distinguish each correlation from random distribution with constant probability of success. We also evaluate the percentage of the relative error ϵ of the experimental values compared with the theoretical values in the same way as our preliminary version [7]:

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

Tables 3 and 4 show the experimental and the theoretical values and the percentage of the relative error ϵ in both generic RC4 and WPA, respectively.

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

We also see that ϵ is small enough in $S_0[i_1]$ and $S_1[i_2]$ in WPA such as $\epsilon \leq 0.754$ (%). ϵ in Theorem 1 is refined from 2.658 (%) to 0.393 (%). Therefore, we have convinced that the theoretical values closely reflect the experimental values in $S_0[i_1]$ and $S_1[i_2]$ in WPA. The theoretical values in j_2 in WPA produce slightly large ϵ such as 3.178 (%). We will continue to refine the theoretical values in j_2 in WPA.

Table 3 Comparison between the experimental and the theoretical values for generic RC4.

Linear correlation		Experimental value	Theoretical value	ϵ (%)
$S_0[i_1]$	$-K[0] - K[1] - 3$	0.005333309	0.005344544	0.211
	$K[0] + K[1] + K[2] + 3$	0.001490745	0.001479853	0.730
$S_1[i_2]$	$K[0] + K[1] + K[2] + 3$	0.360360690	0.362016405	0.459
	$-K[0] - K[1] + K[2] - 1$	0.005305673	0.005320377	0.277
	$K[1] + K[2] + 3$	0.008158548	0.008150313	0.101
	$K[0] - K[1] + K[2] - 3$	0.005295155	0.005320377	0.476
	$K[0] - K[1] + K[2] - 1$	0.005289180	0.005320377	0.590
	$K[0] - K[1] + K[2] + 1$	0.005309594	0.005320377	0.203
	$K[0] - K[1] + K[2] + 3$	0.005310594	0.005302926	0.144
j_2	$K[2]$	0.004430372	0.004426926	0.078
	$-K[0] - K[1] + K[2] - 2$	0.003920799	0.003906250	0.371
	$-K[0] - K[1] + K[2]$	0.003919381	0.003906250	0.335
	$-K[0] - K[1] + K[2] + 2$	0.003910929	0.003906250	0.120
	$-K[0] + K[1] + K[2]$	0.003920399	0.003906250	0.361
	$-K[1] + K[2] - 2$	0.003910053	0.003906250	0.097
	$-K[1] + K[2] + 3$	0.003897939	0.003906250	0.213
	$K[0] - K[1] + K[2]$	0.003917895	0.003906250	0.297

Table 4 Comparison between the experimental and the theoretical values for WPA.

Linear correlation		Experimental value	Theoretical value	ϵ (%)
$S_0[i_1]$	$-K[0] - K[1] - 3$	0.008408305	0.008375244	0.393
	$K[0] + K[1] + K[2] + 3$	0.001491090	0.001479853	0.754
$S_1[i_2]$	$K[0] + K[1] + K[2] + 3$	0.361751935	0.362723221	0.268
	$-K[0] - K[1] + K[2] - 1$	0.008174625	0.008148630	0.318
	$K[1] + K[2] + 3$	0.008173397	0.008150313	0.282
	$K[0] - K[1] + K[2] - 3$	0.008140906	0.008148630	0.095
	$K[0] - K[1] + K[2] - 1$	0.008147205	0.008148630	0.017
	$K[0] - K[1] + K[2] + 1$	0.008150390	0.008148630	0.022
	$K[0] - K[1] + K[2] + 3$	0.002835497	0.002849060	0.478
j_2	$K[2]$	0.005560613	0.005471358	1.605
	$-K[0] - K[1] + K[2] - 2$	0.004573276	0.004427953	3.178
	$-K[0] - K[1] + K[2]$	0.005562336	0.005471358	1.636
	$-K[0] - K[1] + K[2] + 2$	0.004543826	0.004427953	2.550
	$-K[0] + K[1] + K[2]$	0.005490766	0.005471358	0.353
	$-K[1] + K[2] - 2$	0.005468425	0.005471358	0.054
	$-K[1] + K[2] + 3$	0.005468472	0.005471358	0.053
	$K[0] - K[1] + K[2]$	0.005607004	0.005471358	2.419

4. Refined RC4 Key Setting

Many key recovery attacks on WEP using specific IVs have been proposed over past 15 years [3], [9], [20]. One of the greatest factors to enable the attacks is that the first 3-byte RC4 key, $K[0]$, $K[1]$ and $K[2]$, are derived from the known IV. Actually, IV can be obtained easily by observing packets. For example, Fluhrer, Mantin and Shamir pointed out that the information on the remaining RC4 key ($K[3]$, ..., $K[15]$) is derived from the keystream bytes when specific IV is used, and showed the RC4 key recovery attack by observing about 4,000,000–6,000,000 packets [3].

WPA improved a construction of the RC4 key setting known as TKIP to avoid the known WEP attacks. However, the weaknesses in TKIP using the known IV were reported by Sen Gupta et al. [4] and by us [8]. Both showed that TKIP induces many linear correlations including the keystream bytes or the internal state variables. Ideally TKIP should be constructed in such a way that it can keep the security level of generic RC4.

In this section, let us investigate a construction of the RC4 key setting in such a way that it can keep the security level of generic RC4. If the construction was refined, it would be hard to induce the linear correlations. In order to find the refined construction, we use the following linear equations

$$Z_{r+1} = b \cdot K[x] + c \cdot K[y] + d \cdot K[z] + e, \quad (11)$$

$$X_r = a \cdot Z_{r+1} + b \cdot K[x] + c \cdot K[y] + d \cdot K[z] + e, \quad (12)$$

where $X_r \in \{S_r[i_{r+1}], S_r[j_{r+1}], j_{r+1}, t_{r+1}\}$, $a, b, c, d \in \{0, \pm 1\}$, $e \in \{0, \pm 1, \pm 2, \pm 3\}$, and $x, y, z \in \{0, 1, 2, \ldots, 15\}$ for $r \geq 0$. Namely, we carefully need to set the 3-byte RC4 key, $K[x]$, $K[y]$ and $K[z]$, derived from the known IV as follows:

$$K[x] = (\text{IV16} \ >> \ 8) \ \& \ \text{0xFF}, \quad (13)$$

$$K[y] = ((\text{IV16} \ >> \ 8) \mid \text{0x20}) \ \& \ \text{0x7F}, \quad (14)$$

$$K[z] = \text{IV16} \ \& \ \text{0xFF}. \quad (15)$$

We have examined all equations defined by Eqs. (11) and (12) in each round with 2^{32} randomly generated 16-byte RC4 keys in the constructions with the following cases of x, y and z.

Case 1. $x = 9$, $y = 12$ and $z = 15$.
Case 2. $x = 11$, $y = 12$ and $z = 13$.
Case 3. $x = 11$, $y = 13$ and $z = 15$.
Case 4. $x = 13$, $y = 14$ and $z = 15$.

The reason why we set the above 4 cases is that the constructions using the first half of the RC4 key bytes may be

Table 5 The number of linear correlations including the keystream bytes and the unknown internal state variables by the RC4 key setting in TKIP and Cases 1–4.

Linear correlation	TKIP	Case 1	Case 2	Case 3	Case 4
Z_{r+1}	22	3	3	3	3
$S_r[i_{r+1}]$	362	104	103	104	103
$S_r[j_{r+1}]$	12	2	2	2	2
j_{r+1}	26	5	5	5	5
t_{r+1}	462	160	161	161	161
sum	884	274	274	275	274

easy to induce many linear correlations in the same way as TKIP.

Table 5 presents the number of linear correlations which are induced by the RC4 key setting in TKIP and Cases 1–4. We have summarized the correlations including the keystream bytes Z_r or unknown internal state variables X_r with more than 0.00395 and 0.0048 (positive biases) or less than 0.00385 and 0.0020 (negative biases), respectively. From the table, we can confirm that the number of linear correlations in Cases 1–4 can be reduced by about 70% in comparison with that in TKIP. Therefore, we have refined the construction of the RC4 key setting in WPA. In this study, we investigated it only in four cases. We will continue to investigate the refined construction in more cases, which remains an open problem.

5. Conclusion

This paper has provided newly theoretical proofs of 17 linear correlations including unknown internal states: $S_0[i_1]$, $S_1[i_2]$ and j_2. Our theoretical analysis can make clear how TKIP induces biases of internal states in generic RC4. We have further provided the refined construction of the RC4 key setting in WPA. As a result of our investigations, we can reduce the number of linear correlations in the refined construction by about 70% in comparison with that in the original setting.

Our analysis are expected to contribute from the following two viewpoints. One is to contribute to recover a correct internal state of RC4 by using our linear correlations in WPA. The other is to contribute to securely operate WPA in such a way that it can keep the security level of generic RC4.

Acknowledgements

This work is supported by the Grant-in-Aid for Scientific Research (C) (15K00183) and (15K00189).

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, Berlin, Heidelberg, 2011.
[2] N. Ferguson, "Michael: an improved MIC for 802.11 WEP," doc.:IEEE 802.11-02/020r0, April 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, 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, 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, Berlin, Heidelberg, 2014.
[7] R. Ito and A. Miyaji, "How TKIP induces biases of internal states of generic RC4," Information Security and Privacy, Lecture Notes in Computer Science, vol.9144, pp.329–342, Springer International Publishing, Cham, 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, 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, Berlin, Heidelberg, 1998.
[11] 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, Berlin, Heidelberg, 2011.
[12] I. Mantin, "Analysis of the stream cipher RC4," Master's thesis, The Weizmann Institute of Science, Israel, 2001. http://www.wisdom.weizmann.ac.il/~itsik/RC4/rc4.html
[13] 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, Berlin, Heidelberg, 2002.
[14] 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, Berlin, Heidelberg, 2008.
[15] 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, Berlin, Heidelberg, 2014.
[16] 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, Berlin, Heidelberg, 2015.
[17] 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, Berlin, Heidelberg, 2007.
[18] A. Roos, "A class of weak keys in the RC4 stream cipher," Posts in sci.crypt, http://marcel.wanda.ch/Archive/WeakKeys, 1995.
[19] 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, Berlin, Heidelberg, 2011.
[20] R. Teramura, Y. Asakura, T. Ohigashi, H. Kuwakado, and M. Morii, "Fast WEP-key recovery attack using only encrypted IP packets," IEICE Trans. Fundamentals, vol.E93-A, no.1, pp.164–171, Jan. 2010.

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, and International Conference on Applications and Technologies in Information Security (ATIS 2016) Best Paper Award. 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.