PAPER

# IVs to Skip for Immunizing WEP against FMS Attack

**Kazukuni KOBARA**[†], ***Member and*** **Hideki IMAI**[†,††], ***Fellow***

**SUMMARY** The WEP (Wired Equivalent Privacy) is a part of IEEE 802.11 standard designed for protecting over-the-air communication. While almost all of the WLAN (Wireless LAN) cards and the APs (Access Points) support WEP, a serious key recovery attack (aka FMS attack) was identified by Fluhrer et al. The FMS attack can basically be prevented by skipping IVs (Initial Values) used in the attack, but naive skip methods reveal information on the WEP key since most of them depend on the WEP key and the patterns of the skipped IV reveal it. In order to skip IVs safely, the skip patterns must be chosen carefully. In this paper, we review the attack conditions (6) and (7), whose success probability is the highest, $0.05$, amongst all known conditions to guess one key-byte from one packet. Then we identify their safe skip patterns.

***key words:*** *RC4, WEP, IEEE802.11, WLAN, FMS attack*

## 1. Introduction

The WEP (Wired Equivalent Privacy) is a part of IEEE 802.11 standard [14] designed for protecting over-the-air communication. While almost all of the WLAN (Wireless LAN) cards and the APs (Access Points) support WEP, a serious key recovery attack (aka FMS attack) was identified by Fluhrer et al. [8]. The attack was then extended and implemented in [1]–[5], [17]. The FMS attack can basically be prevented* by skipping certain IVs (Initial Values) called weak IVs, but a naive way of skip causes another serious problem. Most of the weak IVs depend on the WEP key and skipping them as they are reveals information on the WEP key. In order to skip IVs safely, the skip patterns must be chosen carefully. In this paper, we review the attack conditions (6) and (7), whose success probability is the highest $0.05$ among ever known conditions to guess one key-byte from one packet. Then we identify their safe skip patterns that do not reveal the information on the WEP key from the skipped patterns.

This paper is organized as follows: In Sec. 2, we briefly review WEP, RC4 and the FMS attack on the WEP. In Sec. 3, we see the patterns of weak IVs and the dependency on the WEP key. In Sec. 4, we identify the safe patterns for skipping weak IVs, which do not reveal the information on the WEP key. Finally in Sec. 5, we check with exhaustive search that the identified patterns successfully remove weak IVs.

Manuscript received August 10, 2006.
Manuscript revised June 06, 2007.

[†]The authors are with the Research Center for Information Security, National Institute of Advanced Industrial Science and Technology, Room 1102, Akihabara Daibiru 11F, 1-18-13, Sotokanda, Chiyoda-ku, Tokyo, 101-0021 Japan.
[††]The author is with the Faculty of Science and Engineering, Chuo University, 1-13-27 Kasuga, Bunkyo-ku, Tokyo, 112-8551, Japan.

*Another option to prevent the attack is to employ the new algorithms such as, TKIP [16] and AES-CCM [16]. It will, however, take some time before all the home users replace their old WLAN cards and APs with new ones.

## 2. WEP and Its Key Recovery Attack

In this section, we briefly review WEP and its key recovery attacks. (For details, cf. the specification [14] and the papers [8], [9], [17].)

### 2.1 Data Encapsulation Format in WEP

Full description of WEP is available from [14]. What is needed here is its data encapsulation format, which is given as follows:

$$\text{IV}||\{(m||\text{CRC}(m)) \oplus \text{RC4}(\text{IV}||K')\}$$

where $||$ denotes concatenation of the right and the left data, and $\oplus$ denotes exclusive-or. A data packet $m$ is encapsulated as follows: first $m$ is concatenated with its 32-bit cyclic redundancy check $\text{CRC}(m)$. Then $(m||\text{CRC}(m))$ is exclusive-ored with a pseudo-random sequence denoted by $\text{RC4}(\text{IV}||K')$ where $\text{RC4}()$ is the RC4 key-stream generator, IV is a $24$-bit initial value and $K'$ is a symmetric-key. IVs should be unique to each other so that $\text{RC4}(\text{IV}||K')$ can be unique even if $K'$ is fixed. $K'$ is a symmetric-key (called WEP key), which is either shared in advance as a password among authorized members or given by another mechanism, such as 802.1x [15] or WPA-PSK [7]. Let $k$ denote the size of $K = (\text{IV}||K')$ in byte, which is either $8$-bytes ($64$-bits) or 16-bytes ($128$-bits) **. In this paper, we assume $k = 16$.

### 2.2 Description of RC4

RC4 is a word oriented stream cipher. Its word size is defined by $n$ and through out this paper we assume $n = 8$, i.e. one word is $8$-bits, which is the most popular setting in RC4 including the case of WEP.

RC4 consists of two algorithms: KSA (Key-Scheduling Algorithm) and PRGA (Pseudo-Random Generation Algorithm). Their algorithms are shown in Fig. 1 and 2 respectively (where $S[i]$ and $K[i]$ denote the $i$-th bytes of $S$ and $K$, respectively). The KSA accepts a key $K$ of $k$ bytes

**Some chips accept 19-bytes (152-bits).

**Input:** a key $K$ of $k$ bytes
**Output:** a buffer $S$ of $2^8$ bytes

$S := (0, 1, \cdots, 2^8 - 1)$
$j := 0$
For$(i = 0; i < 2^8; i++)\{$
  $j := j + S[i]$
    $+K[i \mod k] \mod 2^8$
  Swap $S[i]$ and $S[j]$
$\}$
Return $S$

**Fig. 1** KSA (for $n = 8$).

**Input:** a buffer $S$ of $2^8$ bytes and an output size $s$
**Output:** a sequence $Z$

$j := 0$
For$(v = 1; v \leq s; v++)\{$
  $i := v \mod 2^8$
  $j := j + S[i] \mod 2^8$
  Swap $S[i]$ and $S[j]$
  $Z[v-1] := S[S[i] + S[j] \mod 2^8]$
  Return $Z[v-1]$
$\}$

**Fig. 2** PRGA (for $n = 8$).

and then shuffles its inner buffer $S$ of $2^8$ bytes according to $K$. The PRGA accepts the shuffled $S$ and then generates a pseudo-random sequence while shuffling $S$ again.

The security of RC4 has been studied by a lot of researchers [11]. While some unwanted properties have been identified, such as the distinguishability from a real random stream, no critical vulnerability has been identified yet on the typical usage of RC4. RC4 in WEP is, however, out of the typical usage (since it opens a part of the RC4 key to the public as an IV) and this exposes the rest of the RC4 key (the WEP key $K'$) to the risk of recovery [8].

### 2.3 Key Recovery Attack on WEP

In this subsection, we briefly review the key recovery attack identified by Fluhrer et al. (cf. [8], [9], [17] for details). It uses the correlation between certain positions of the WEP key and the first output byte of the PRGA. The correlation becomes higher than the average for certain IVs (called weak IVs). Thus by collecting a lot of pairs of such weak IVs and the corresponding first output bytes, the WEP key can be recovered. We explain why certain $(\mathrm{IV}[0], \mathrm{IV}[1], \mathrm{IV}[2])$ reveals the information on $K[3]$ (where $(\mathrm{IV}[0], \mathrm{IV}[1], \mathrm{IV}[2]) = (K[0], K[1], K[2])$).

Let $S_i[]$ and $j_i$ denote $S[]$ and $j$ at the round $i$ (before the swap operation is applied in the round) in KSA. And then let $S_i^*[]$ and $j_i^*$ denote $S_i[]$ and $j_i$ in PRGA to distinguish them from those in KSA. Anyone who knows $(\mathrm{IV}[0], \mathrm{IV}[1], \mathrm{IV}[2])$ can know $S_i[]$ and $j_i$ for $i \leq 3$ since they depend only on $(\mathrm{IV}[0], \mathrm{IV}[1], \mathrm{IV}[2])$. Recall that in the round $i$, $S_i[i]$ and $S_i[j_i]$ are swapped with each other and $S_{i+1}[i] = S_i[j_i]$ holds where $j_i \equiv j_{i-1} + S_i[i] + K[i \mod k] \pmod{2^8}$. Accordingly in the round $i = 3$, $S_3[3]$ and $S_3[j_3]$ are swapped with each other and $S_4[3] = S_3[j_3]$ holds where $j_3 \equiv j_2 + S_3[3] + K[3] \pmod{2^8}$. Here $K[3]$ can be obtained from $j_3$ since $j_2$ and $S_3[]$ are known. And then $j_3$ can be obtained from $S_4[3]$ since $S_3$ is known in $S_4[3] = S_3[j_3]$. Interestingly, $S_4[3]$ is given as the first output byte of PRGA if the following two conditions hold:

1. In KSA, three bytes $S_3[1]$, $S_3[S_3[1]]$ and $S_4[3]$ stay in the same position respectively, i.e. the position of $1, S_3[1]$ and $3$ in $S$, and then become $S_1^*[1]$, $S_1^*[S_1^*[1]]$ and $S_1^*[3]$ in PRGA.
2. In PRGA, both (1) and (2) hold:

$$0 \leq S_1^*[1] \leq 2 \tag{1}$$
$$3 \equiv S_1^*[1] + S_1^*[S_1^*[1]] \pmod{2^8}. \tag{2}$$

One can easily verify that $S_1^*[3]$ in PRGA, i.e. $S_4[3]$ in KSA, is given as the first output byte of PRGA if the above two conditions are satisfied. The first condition holds with probability around $0.05$ [8]. Thus (1) and (2) can be rewritten using $S_3[1]$ and $S_3[S_3[1]]$ as follows:

$$0 \leq S_3[1] \leq 2 \tag{3}$$
$$3 \equiv S_3[1] + S_3[S_3[1]] \pmod{2^8}. \tag{4}$$

Then (4) is generalized to

$$t \equiv S_3[1] + S_3[S_3[1]] \pmod{2^8} \tag{5}$$

for guessing not only $K[3]$ but also $K[t]$ s.t. $3 \leq t$.

In practice, some variants exist on the implementation of the key-recovery attack. We categorize them as follows:

**Basic variant:** uses the IVs that lead to both (3) and (5). We call such IVs *key-independent weak IVs* (since they are independent of the WEP key).

**FMS:** uses not only the key-independent weak IVs but also *key-dependent weak IVs*. When $K[0]$ to $K[t']$ s.t. $2 \leq t'$ are known or guessed, the condition for guessing $K[t]$ s.t. $t' < t \leq 15$ (or simply $t = t' + 1$) is given by:

$$0 \leq S_{t'+1}[1] \leq t' \tag{6}$$
$$t \equiv S_{t'+1}[1] + S_{t'+1}[S_{t'+1}[1]] \pmod{2^8} \tag{7}$$

where the condition for the Basic variant corresponds to $t' = 2$. Skipping only the key-independent weak IVs is not enough to prevent this attack since even if $K[3]$ to $K[t']$ are unknown, this attack still works by exhaustively searching $K[3]$ to $K[t']$. This is known as the *guessing-early-key-bytes approach* [17]. Other approaches are also proposed in [12], [13]. The former relaxes the condition so that more IVs can be used in the attack, but this reduces the success probability and makes it difficult to recover the WEP key in practice [13]. The latter guesses the first output byte from the $257$-th output byte. While this might be effective when the fist up to $256$ bytes are thrown as suggested in [6], it does not improve the attacks on WEP since in WEP the first output byte is already known. (In this paper, we focus on countermeasures that are fully compatible with existing WEPs.)

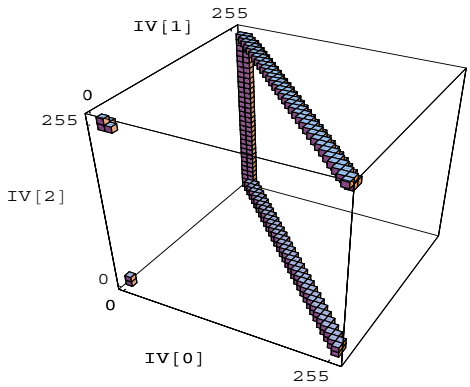



**Fig. 3** Distribution of IVs meeting both (6) and (7) for any $t$ and $t' = 2$. (Note that they are key-independent.)

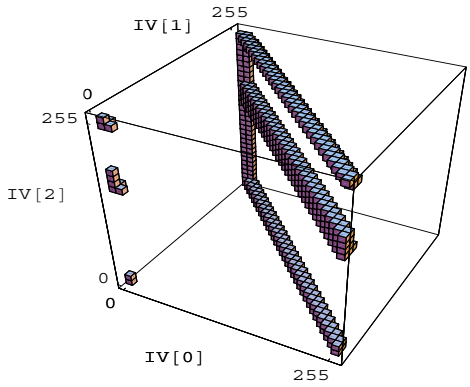



**Fig. 4** Distribution of weak IVs for any $t$, $t' = 3$ and $K[3] = 86$.

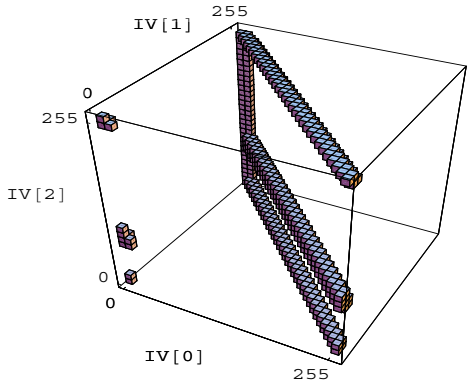



**Fig. 5** Distribution of weak IVs for any $t$, $t' = 3$ and $K[3] = 170$.

**Korek:** uses new conditions identified by Korek. To the best of our knowledge, Korek's result has not been published in a paper but appeared only in the source codes of [1], [2], [5]. Some conditions of this attack are, however, not stable and further analysis is needed.

In this paper, we focus on the FMS attack, especially on the guessing-early-key-bytes approach, i.e. the combination of IVs and WEP keys meeting both (6) and (7). And also for simplicity, we abbreviate "$a \equiv b \mod 2^8$" to "$a = b$" from now on.

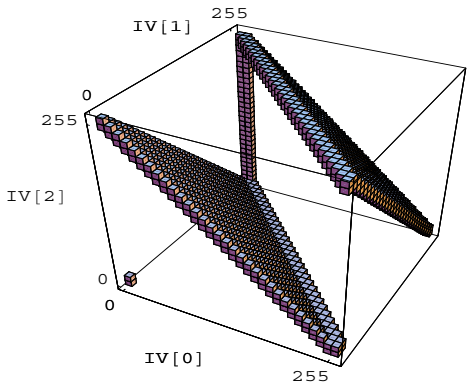



**Fig. 6** Distribution of weak IVs for any $t$, $t' = 3$ and $K[3] = 254$.

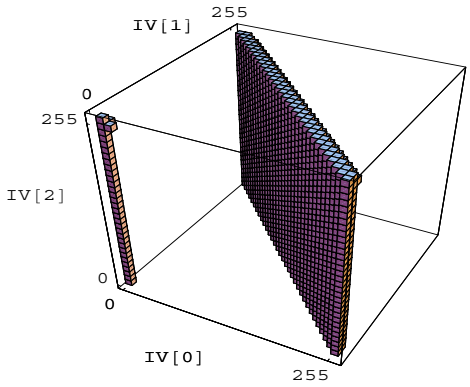



**Fig. 7** Distribution of weak IVs for any $t$, $t' = 3$ and $K[3] = 255$.

## 3. Patterns of Weak IVs in The FMS Attack

In this section, we see the IVs meeting both (6) and (7) and show the dependency on the WEP key. Fig. 3 shows those for $t' = 2$. In Fig. 3 to 7, weak IVs exist in the space where small cubes are drawn. No cube means no such IV there. (Precisely, in these figures, we split the IV space into $32^3$ sub-spaces corresponding to $8^3$ IVs and draw one cube there if the sub-space has at least one IV meeting both (6) and (7) to make the figures easier to see.) The weak IVs for $t' = 2$ are independent of WEP keys and can be obtained with exhaustive search of $(IV[0], IV[1], IV[2])$.

On the other hand, weak IVs for $t' \geq 3$ depend on the WEP key. We show them for $t' = 3$ and $K[3] = 86, 170, 254$ and $255$ in Fig. 4 to 7, respectively. Here, $K[3] = 254$ and $255$ are examples of weak WEP keys where the number of weak IVs becomes larger than the other WEP keys [10]. And then $K[3] = 86$ and $170$ are examples of non-weak WEP keys. (The numbers $86$ and $170$ themselves have no special meaning. They are simply chosen so that the difference can be visually recognized.) As you can see from Fig. 4 to 7, weak IVs depend on the $K[3]$ and hence a naive strategy that skips IVs meeting both (6) and (7) reveals the information on the WEP key. So as not to reveal it, the IVs to skip must be designed to be independent of the WEP key while covering almost all of the key-dependent weak IVs.

To do this, we have to grasp the patterns of IVs and

**Table 1** Patterns of IVs and WEP keys to be weak in the FMS attack where $u$ is any integer meeting $0 \le u \le t' < t \le 15$ except $u = 1$.

| Type | Relationship among $u$, $t-u$ and $t'$ | First constraint on $K[]$ | Second constraint on $K[]$ |
|---|---|---|---|
| $u = 0$ | | | |
| FF | | $K[0] = t$ | $K[1] = 255$ |
| $1 < u$ | | | |
| FF | $t-u < u$ | $K[0] + K[1] = u - 1$ | $K[t-u+1] + \cdots + K[u] = -1 + t(t-2u+1)/2$ |
| | $u < t-u$ | $K[0] + K[1] = u - 1$ | $K[2] + \cdots + K[u] = t - (u+3)u/2$ |
| FK | $u < t-u \le t'$ | $K[0] + K[1] = u - 1$ | $K[2] + \cdots + K[t-u] = u - (t-u)(t-u+1)/2$ |
| KF | $u < t-u \le t'$ | $K[0] + \cdots + K[u] = (2t - 3u - u^2)/2$ | $K[u+1] + \cdots + K[t-u] = (2 - t - t^2 + 2tu)/2$ |
| KK | $u < t-u \le t'$ | $K[0] + \cdots + K[u] = 1 - u(u+1)/2$ | $K[u+1] + \cdots + K[t-u] = (-2 - t - t^2 + 4u + 2tu)/2$ |
| FE | $t-u < u$ | $K[0] + K[1] = t - u - 1$ | $K[2] + \cdots + K[u] = 1 - u(u+1)/2$ |
| | $u < t-u$ | $K[0] + K[1] = t - u - 1$ | $K[2] + \cdots + K[u] = 2 - t - u(u-1)/2$ |
| KE | $1 < t-u < u$ | $K[0] + \cdots + K[t-u] = 1 - (t-u)(t-u+1)/2$ | $K[t-u+1] + \cdots + K[u] = (1+t)(t-2u)/2$ |

WEP keys to be weak first. One method is to try all the combinations of IVs and WEP keys and then check whether they satisfy both (6) and (7). This approach is, however, computationally infeasible for large $t'$. Hence we analyze the weak IV patterns obtained theoretically in [10]. We show them in Table 1 where $u$ is any integer meeting $0 \le u \le t' < t \le 15$ except $u = 1$[†]. $K[]$'s meeting both columns for "First constraint on $K[]$" and "Second constraint on $K[]$" in any row can be used to guess $K[t]$ as long as the column for "Relationship among $u$, $t-u$ and $t'$" is satisfied in addition to the universal constraints $0 \le u \le t' < t \le 15$ except $u = 1$.

## 4. Safe Skip Patterns For Immunizing WEP Against The FMS Attack

In this section, we identify the patterns of IVs to skip that cover almost all of the weak IVs and that do not reveal information of the WEP key from the skipped patterns. Such patterns (we call them safe skip patterns) can be obtained by the union of the key-independent weak IVs and the key-dependent weak IVs for all the WEP keys. This strategy, however, does not work since all the IV space is covered by the key-dependent weak IVs. Therefore in Section 4.1 we try to remove WEP keys whose key-dependent weak IVs cover all the IV space. Then in Section 4.2 we identify the patterns of IVs to remove the rest weak IVs.

### 4.1 WEP Keys to Avoid

In this subsection, we identify the WEP keys whose key-dependent weak IVs cover all the IV space and then obtain the patterns of WEP keys to avoid to remove such catastrophic weak IVs. The catastrophic patterns can be identified by looking for the rows in Table 1 where both columns for "First constraint on $K[]$" and "Second constraint on $K[]$" depend on the WEP key. (Recall that WEP keys correspond to $(K[3], \cdots, K[15])$). Below, we pick all the three types (KF for $u \ge 3$, KK for $u \ge 3$ and KE for $t-u \ge 3$) and their constraints. Catastrophic patterns are patterns of $K[]$'s meeting all the constraints in each type.

**KF for $u \ge 3$:**

- $u < t-u \le t'$
- $K[0] + \cdots + K[u] = (2t - 3u - u^2)/2$
- $K[u+1] + \cdots + K[t-u] = (2 - t - t^2 + 2tu)/2$

**KK for $u \ge 3$:**

- $u < t-u \le t'$
- $K[0] + \cdots + K[u] = 1 - u(u+1)/2$
- $K[u+1] + \cdots + K[t-u] = (-2 - t - t^2 + 4u + 2tu)/2$

**KE for $t-u \ge 3$:**

- $1 < t-u < u$
- $K[0] + \cdots + K[t-u] = 1 - (t-u)(t-u+1)/2$
- $K[t-u+1] + \cdots + K[u] = (1+t)(t-2u)/2$

Fortunately, the third items in each type depend only on the WEP key and can be removed by avoiding WEP keys meeting any of (8), (9) and (10):

[†]When $u = 1$, $t = 2$, i.e. one can guess $IV[2]$ but this is meaningless since $IV[2]$ is known to the public.

```
 1  for(ie=4; ie<=12; ie++){
 2    /*** min(ie,16-ie) ***/
 3    tmp=16-ie;  if(ie < tmp)tmp=ie;
 4    for(is=tmp; is>=4; is--){
 5      /*** K[is]+...+K[ie] ***/
 6      tmp=0;
 7      for(i=is; i<=ie; i++){
 8        tmp+=K[i];
 9      }
10      /*** Conditions ***/
11      cond1=(is*(is-3)-ie*(ie+1))/2+2;
12      cond2=(is*(is+1)-ie*(ie+1))/2-2;
13      cond3=(ie+is)*(is-ie-1)/2;
14      if( tmp == cond1 || tmp == cond2
15                       || tmp == cond3 ){
16        printf("K[%d] is weak!!\n",ie);
17        goto fin;
18      }
19    }
20    printf("K[%d] is OK!!\n",ie);
21  }
22  fin:;
```

**Fig. 8** An algorithm to check whether $K[i_e]$ is weak or not after $K[i_s]$ to $K[i_e-1]$ are not weak for $4 \le i_e \le 12$.

$$\sum_{i=u+1}^{t-u} K[i] = (2-t-t^2+2tu)/2 \quad \text{for } 3 \le u \le 7 \text{ and } 2u < t \tag{8}$$

$$\sum_{i=u+1}^{t-u} K[i] = (-2-t-t^2+4u+2tu)/2 \quad \text{for } 3 \le u \le 7 \text{ and } 2u < t \tag{9}$$

$$\sum_{i=t-u+1}^{u} K[i] = (1+t)(t-2u)/2 \quad \text{for } 3 \le t-u < u \le 12. \tag{10}$$

where the constraints $2u < t$ in both (8) and (9), and $t-u < u$ in (10) come from the first items in each type above, the constraint $u \le 7$ in (8) and (9) is obtained from $t \le 15$ and $2u < t$, and then the constraint $u \le 12$ in (10) comes from $t \le 15$ and $3 \le t-u$.

Furthermore, (8) to (10) can be rewritten as (11) by substituting $i_s$ and $i_e$[†] for $u+1$ and $t-u$ respectively in both (8) and (9), and by substituting $i_s$ and $i_e$ for $t-u+1$ and $u$ respectively in (10).

$$\sum_{i=i_s}^{i_e} K[i] = \frac{i_s(i_s-3)-i_e(i_e+1)}{2}+2 \quad \text{or} \quad \frac{i_s(i_s+1)-i_e(i_e+1)}{2}-2 \quad \text{or} \quad \frac{(i_e+i_s)(i_s-i_e-1)}{2} \tag{11}$$

[†]Subscripts "s" and "e" in $i_s$ and $i_e$ stand for "start" and "end," respectively.

**Table 2** The number of $K[i]$ to avoid. (The number is 0 for $i \in \{3, 13, 14, 15\}$.)

| $i$ | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|
| # of $K[i]$ to avoid | 3 | 6 | 9 | 12 | 15 | 12 | 9 | 6 | 3 |

for $4 \le i_e \le 12$ and $4 \le i_s \le \min(i_e, 16-i_e)$ where the constraint $16-i_e$ comes from $i_s + i_e - 1 = t \le 15$.

In Fig. 8, we show an algorithm to check the weakness of $K[i_e]$ after $K[i_s]$ to $K[i_e-1]$ are not weak. The outline of the algorithm is as follows: First of all, it assumes that $K[i_e]$ for $4 \le i_2 \le 12$ are given. The 1-st to 4-th lines correspond to the loops for checking $\sum_{i=i_s}^{i_e} K[i]$ for $4 \le i_e \le 12$ and $4 \le i_s \le \min(i_e, 16-i_e)$. The 5-th to 9-th and 10-th to 13-th lines are for calculation of $\sum_{i=i_s}^{i_e} K[i]$ and conditions in (11), respectively. The 14-th to 20-th lines are for checking the conditions and then printing out the result.

For reference, we list up all the combinations of $K[4]$, $K[5]$ and $K[6]$ meeting (11) below [††]:

- $K[4] = -6, -4, -2,$
- $K[5] = -8, -5, -2,$
- $K[4] + K[5] = -11, -9, -7,$
- $K[6] = -10, -6, -2,$
- $K[5] + K[6] = -14, -11, -8,$
- $K[4] + K[5] + K[6] = -17, -15, -13,$

We show the number of $K[i]$'s to avoid in Table 2. If all of them are avoided, the probability of a randomly chosen WEP key being accepted is $(256-3)^2 \cdot (256-6)^2 \cdot (256-9)^2 \cdot (256-12)^2 \cdot (256-15)/256^9 = 0.742$ and that after $x$ weak bytes are replaced is lower bounded by $Pr(x) = \sum_{i=0}^{x} \binom{9}{i} \left(\frac{256-15}{256}\right)^{(9-i)} \left(\frac{15}{256}\right)^{i}$ where $Pr(1) = 0.906$, $Pr(2) = 0.987$ and $Pr(3) = 0.999$, respectively. I.e., even if a given WEP key is not accepted, by replacing at most three weak key bytes, it will be accepted with probability more than $0.999$.

The number of remaining WEP keys after (11) is avoided is $256^4 \cdot (256-3)^2 \cdot (256-6)^2 \cdot (256-9)^2 \cdot (256-12)^2 \cdot (256-15) = 2^{103.57}$, which is smaller than the original number $2^{104}$ but still large enough to prevent exhaustive search.

In Table 3, we summarize the patterns of WEP keys to avoid, the remaining WEP key space and the ratio of it to the original space (as well as those for IVs that will be obtained in the next subsection).

### 4.2 IVs to Skip

As explained in the previous subsection, KF for $3 \le u$, KK for $3 \le u$ and KE for $3 \le t-u$ in Table 1 can be removed by avoiding WEP keys meeting (11). Therefore the remaining weak IV types we have to remove are KF for $u = 2$, KK for $u = 2$, KE for $t-u = 2$, FF, FK and FE. Each type can be removed by skipping the following IVs [††]:

[††]Here "$a = b$" stands for "$a \equiv b \mod 2^8$" and we use negative integers, e.g. $-2$, when the evaluation of the function is negative (so that one can verify the results easily).

**Table 3** Patterns of WEP keys to avoid, i.e. (11), and IVs to skip, i.e. (23) and (24).

| | Patterns to Avoid or Skip | Remaining Space (Original) | Ratio of Remaining Space to Original |
|---|---|---|---|
| WEP Keys | $\sum_{i=i_s}^{i_e} K[i] = \frac{i_s(i_s-3)-i_e(i_e+1)}{2} + 2$ or $\frac{i_s(i_s+1)-i_e(i_e+1)}{2} - 2$ or $\frac{(i_e+i_s)(i_s-i_e-1)}{2}$ for $4 \le i_e \le 12$ and $4 \le i_s \le \min(i_e, 16-i_e)$ | 103.57bits (104bits) | 74.2% |
| IVs | $-1 \le \mathrm{IV}[0] + \mathrm{IV}[1] \le 14$ or $-2 \le \mathrm{IV}[0] + \mathrm{IV}[1] + \mathrm{IV}[2] \le 10$ | 23.83bits (24bits) | 89.0% |

**Table 4** The number of IVs meeting both (6) and (7) to guess $K[t]$ for $t' = 2$.

| Skip Pattern \ $t$ | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| No skip | 765 | 254 | 765 | 765 | 765 | 765 | 765 | 765 | 765 | 765 | 765 | 765 | 765 |
| IVs meeting any of (23) and (24) | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

**FF for $u = 0$:**

$$(\mathrm{IV}[0], \mathrm{IV}[1]) = (t, 255) \tag{12}$$

where $3 \le t \le 15$.

**FF for $1 < u$:**

$$\mathrm{IV}[0] + \mathrm{IV}[1] = u - 1 \tag{13}$$

where $2 \le u \le 14$ since $1 < u$ and $u \le t' < t \le 15$, i.e. $u < 15$.

**FK:**

$$\mathrm{IV}[0] + \mathrm{IV}[1] = u - 1 \tag{14}$$

where $2 \le u \le 7$ since $u < t - u$ and $t \le 15$, i.e. $u < 15/2$, and then $1 < u$ and $t - u \le t'$, i.e. $\max(2, \min(t - t')) = \max(2, 1) = 2 \le u$.

**KF for $u = 2$:**

$$\mathrm{IV}[0] + \mathrm{IV}[1] + \mathrm{IV}[2] = t - 5. \tag{15}$$

where $5 \le t \le 15$ since $u < t - u$, $u = 2$ and $t \le 15$.

**KK for $u = 2$:**

$$\mathrm{IV}[0] + \mathrm{IV}[1] + \mathrm{IV}[2] = -2. \tag{16}$$

**FE:**

$$\mathrm{IV}[0] + \mathrm{IV}[1] = t - u - 1 \tag{17}$$

where $1 \le t - u \le 13$ since $t \le 15$ and $1 < u$, i.e. $t - u \le \max(t) - \min(u) = 15 - 2 = 13$, and then $u < t$, i.e. $0 < t - u$.

**KE for $t - u = 2$:**

$$\mathrm{IV}[0] + \mathrm{IV}[1] + \mathrm{IV}[2] = -2. \tag{18}$$

By removing the overlap among (12) to (18), they can be expressed as follows:

$$(K[0], K[1]) = (15, 255) \tag{19}$$

$$0 \le \mathrm{IV}[0] + \mathrm{IV}[1] \le 13 \tag{20}$$

$$0 \le \mathrm{IV}[0] + \mathrm{IV}[1] + \mathrm{IV}[2] \le 10 \tag{21}$$

$$\mathrm{IV}[0] + \mathrm{IV}[1] + \mathrm{IV}[2] = -2. \tag{22}$$

To make the skip rule simpler and also to skip some minor weak IVs [10] that are not covered by Table 1, we recommend to skip IVs meeting any of (23) and (24). We show the ability of them in Section 5.

$$-1 \le \mathrm{IV}[0] + \mathrm{IV}[1] \le 14 \tag{23}$$

$$-2 \le \mathrm{IV}[0] + \mathrm{IV}[1] + \mathrm{IV}[2] \le 10. \tag{24}$$

After skipping (23) and (24), the remaining IV space is 23.83 bits (or $89.0\%$ of the original 24 bit IV space), which might be small but still far larger than the space where WEP keys are replaced frequently, say every after 10,000 packets as suggested in [17], which corresponds to only $0.06\%$ of the original IV space.

In Table 3, we summarize the patterns of IVs to skip, the remaining IV space and the ratio of it to the original space as well as those for WEP keys.

## 5. Count of Weak IVs

In this section, we exactly count the number of weak IVs meeting both (6) and (7) with exhaustive search of all the combinations of IVs and some early bytes of the WEP keys.

Table 4 shows the case for $t' = 2$, i.e. the case where adversaries do not know the WEP key. As you can see, all the weak IVs are removed by skipping IVs meeting any of (23) and (24). Fig. 9 shows the case for $t' = 3$, i.e. the case where adversaries know $K[3]$ or assume $K[3]$ to be a certain value. As shown in Fig. 9, the number of weak IVs for guessing $K[t]$ has a similar trend for almost all of the $K[3]$'s. The exceptions to notice are for $K[3] = 255, 254, 253$ and 252. In these cases, weak IVs for guessing $K[5]$ can be found more frequently than the other $K[3]$'s (since they are weak WEP keys [10]). By skipping IVs meeting any of (23) and (24), all the weak IVs in Fig. 9 are removed completely.

Fig. 10 and 11 show the cases for $t' = 4$, i.e. adversaries know both $K[3]$ and $K[4]$ or assume all or some of them to be certain values. Fig. 10 is for $K[3] = 100$ and then Fig. 11 is for $K[3] = 254$, respectively. The difference between them is whether $K[3]$ is a weak WEP key or not. Fig. 11 shows an example of a weak $K[3]$ and Fig. 10 shows an example of non-weak $K[3]$. Their trends are similar among non-weak WEP keys and among weak WEP keys, respectively. As shown in the lower figures in Fig. 10 and 11, weak IVs can be removed by skipping (23) and (24) except $K[4] = 250, 252, 254 = -6, -4, -2$ for guessing

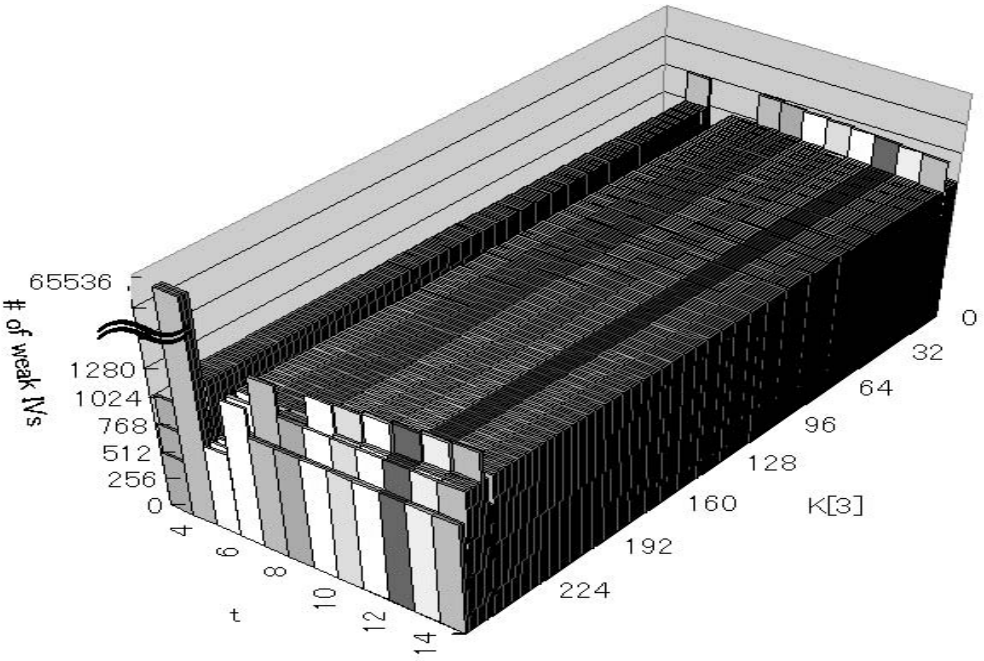



**Fig. 9** The number of IVs meeting both (6) and (7) to guess $K[t]$ for $t' = 3$. After skipping IVs meeting any of (23) and (24), all of them were removed.

$K[7]$. As explained in Sect. 4.1, they must be removed by avoiding WEP keys meeting (11).

In the same way, we confirmed that all the weak IVs for the other $K[3]$'s in $t' = 4$ can be removed by skipping IVs meeting any of (23) and (24) and then avoiding WEP keys meeting (11). These results ensure that adversaries cannot use (6) and (7) even if they perform exhaustiv search for $K[3]$ and $K[4]$.

## 6. Conclusion

We investigated the patterns of IVs and WEP keys known to be weak using both (6) and (7). We identified safe skip patterns that cover them and that do not reveal information on the WEP key. Basically, such safe skip patterns can be obtained by the union of the key-independent weak IVs and the key-dependent weak IVs for all the WEP keys. Unfortunately, this strategy does not work since the union of them covers all the IV space. Therefore we firstly identified the WEP keys whose key-dependent weak IVs cover all the IV space. They are the WEP keys meeting any of (11). By avoiding them, weak IVs are distributed locally. We identified the patterns of IVs covering them. They are the IVs meeting any of (23) and (24).

The remaining WEP key space after avoiding (11) is $103.57$ bits (or $74.2\%$ of the original $104$ bit space), which is large enough to prevent exhaustive-search. And then the remaining IV space after skipping (23) and (24) is $23.83$ bits (or $89.0\%$ of the original $24$ bit IV space), which might be small but still far larger than the space where WEP keys are replaced frequently, say every after 10,000 packets as suggested in [17], which corresponds to only $0.06\%$ of the original IV space.

To obtain safe skip patterns for the other attacks on WEP would be our further study.

## Acknowledgment

We would like to thank the anonymous reviewers for their useful comments.

### References

[1] aircrack. `http://www.cr0.net:8040/code/network/aircrack/`.
[2] AirSnort. `http://airsnort.shmoo.com/`.
[3] dwepcrack. `http://www.e.kth.se/~pvz/wifi/`.
[4] WEPCrack. `http://wepcrack.sourceforge.net/`.
[5] WepLab. `http://weplab.sourceforge.net/`.
[6] "RSA security response to weaknesses in key scheduling algorithm of RC4", 2001.
[7] Wi-Fi Alliance. "Wi-Fi protected access". `http://www.wi-fi.org/opensection/protected_access.asp`, 2003.
[8] S. Fluhrer, I. Mantin, and A. Shamir. "Weaknesses in the key scheduling algorithm of RC4". In *Proc. of SAC'01, LNCS 2259*, pages 1–24, 2001.
[9] S. Fluhrer, I. Mantin, and A. Shamir. Attacks on RC4 and WEP. *CryptoBytes (RSA Laboratories)*, 5(2):26–34, Summer/Fall 2002.
[10] K. Kobara and H. Imai. "Key-dependent weak ivs and weak keys in WEP – how to trace conditions back to their patterns –". *IEICE Trans.*, E89-A(8):2198–2206, August 2006.
[11] I. Mantin. "RC4 page". `http://www.wisdom.weizmann.ac.il/~itsik/RC4/rc4.html`.
[12] I. Mantin. "A practical attack on the fixed RC4 in the WEP mode". In *Proc. of ASIACRYPT '05, LNCS 3788*, pages 395–411, 2005.
[13] T. Ohigashi, Y. Shiraishi, and M. Morii. "Most IVs of FMS Attack-Resistant WEP Implementation Leak Secret Key Information". In *The 2005 Symposium on Cryptography and Information Security*,

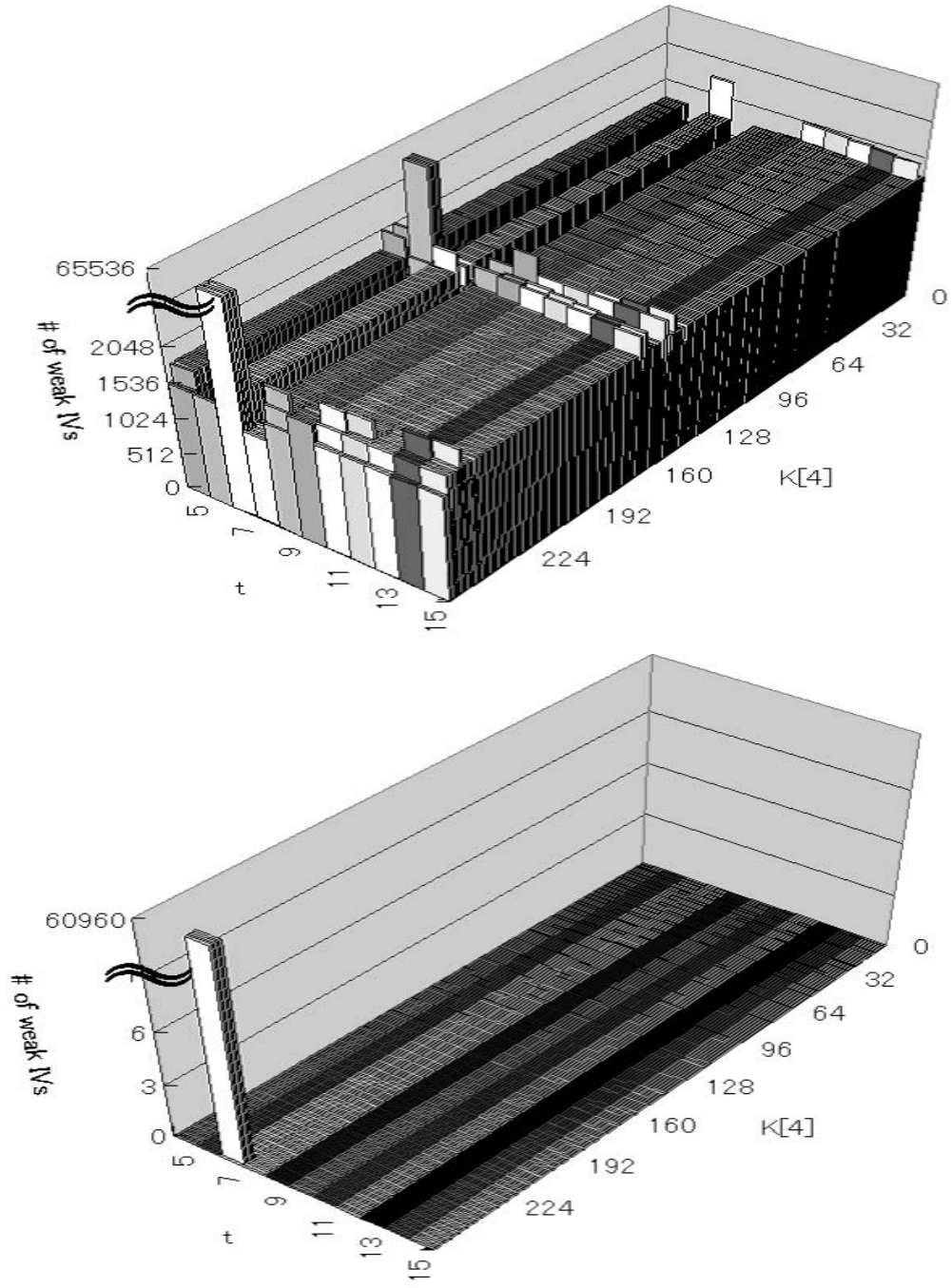



**Fig. 10** The number of IVs meeting both (6) and (7) to guess $K[t]$ for $t' = 4$ and $K[3] = 100$ (upper graph) and those after skipping IVs meeting any of (23) and (24) (lower graph). The left IVs in the lower graph cannot be removed by skipping certain IVs without revealing $K[3]$ since they are in the form of either ($K[0]+K[1]+K[2]+K[3] = -5$ and $K[4] = -2$ or $-4$) or ($K[0]+K[1]+K[2]+K[3] = -2$ and $K[4] = -6$). They must be removed by avoiding $K[4] = -2, -4$ and $-6$.

volume 4, pages 1957–1962, January 2005.

[14] IEEE Computer Society. Wireless lan medium access control (MAC) and physical layer (PHY) specifications. IEEE Std 802.11, 1999 Edition, http://standards.ieee.org/reading/ieee/std/lanman/, 1999.

[15] IEEE Computer Society. IEEE standards for local and metropolitan area networks: Port-based network access control. IEEE 802.1X-2001, http://standards.ieee.org/reading/ieee/std/lanman/, 2001.

[16] IEEE Computer Society. Wireless lan medium access control (MAC) and physical layer (PHY) specifications. IEEE Std 802.11i/D3, http://standards.ieee.org/reading/ieee/std/lanman/, 2003.

[17] A. Stubblefield, J. Ioannidis, and A. Rubin. A key recovery attack on the 802.11b wired equivalent privacy protocol (WEP). *ACM Trans. on Information and System Security*, 7(2):319–332, May 2004.

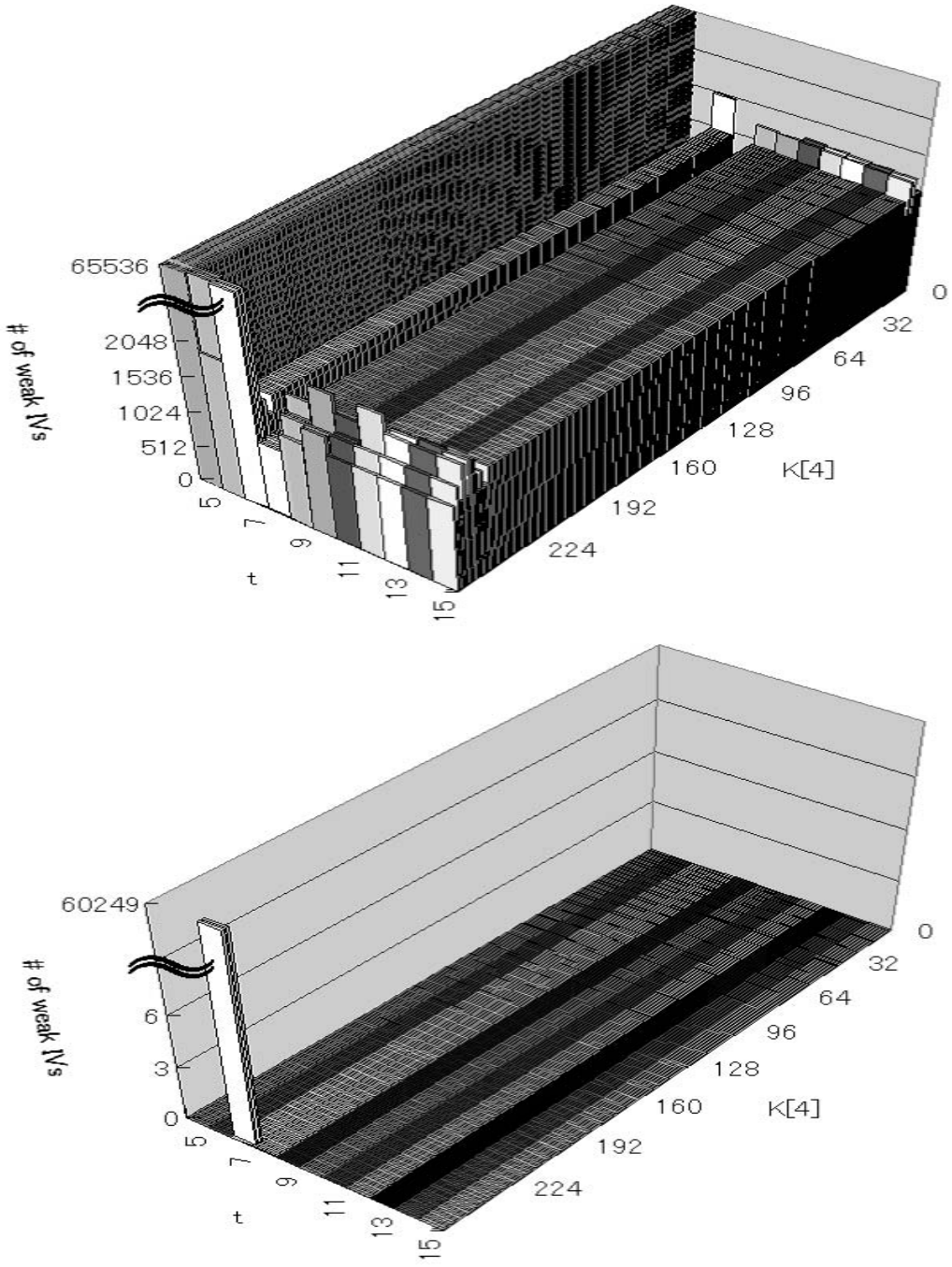
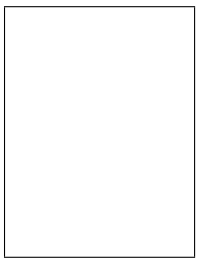
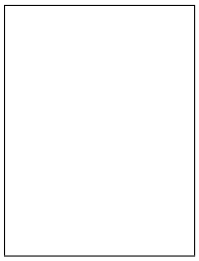



**Fig. 11** The number of IVs meeting both (6) and (7) to guess $K[t]$ for $t' = 4$ and $K[3] = 254$, i.e. a weak WEP key, (upper graph) and those after skipping IVs meeting any of (23) and (24) (lower graph). The left IVs in the lower graph cannot be removed by skipping certain IVs without revealing $K[3]$ since they are in the form of either ($K[0] + K[1] + K[2] + K[3] = -5$ and $K[4] = -2$ or $-4$) or ($K[0] + K[1] + K[2] + K[3] = -2$ and $K[4] = -6$). They must be removed by avoiding $K[4] = -2, -4$ and $-6$.



**Kazukuni Kobara** received his B.E. degree in electrical engineering and M.E. degree in computer science and system engineering from the Yamaguchi University in 1992, 1994, respectively. He also received his Ph.D. degree in engineering from the University of Tokyo in 2003. From 1994 to 2000 and 2000 to 2006 he was a technical associate and a research associate respectively for the Institute of Industrial Science of the University of Tokyo. In 2006, he joined the National Institute of Advanced Industrial Science and Technology (AIST) where he was the leader of the Research Team for Security Fundamentals in the Research Center for Information Security (RCIS). Currently he is a chief research scientist at RCIS. His research interests include cryptography, information and network security. He received the SCIS Paper Award and the Vigentennial Award from ISEC group of IEICE in 1996 and 2003, respectively. He also received the Best Paper Award of WISA, the ISITA Paper Award for Young Researchers, the IEICE Best Paper Award (Inose Award), the WPMC Best Paper Award and the JSSM Best Paper Award in 2001, 2002, 2003, 2005 and 2006 respectively. He is a member of IEICE and IACR. He served as a member of CRYPTREC (2000-present), the vice chairperson of WLAN security committee (2003) and the chief investigator of INSTAC identity management committer (2007-present).



**Hideki Imai** received the B.E., M.E., and Ph.D. degrees in electrical engineering from the University of Tokyo in 1966, 1968, and 1971, respectively. From 1971 to 1992 he was on the faculty of Yokohama National University. From 1992 to 2006 he was a Professor in the Institute of Industrial Science, the University of Tokyo. In 2006 he was appointed as an Emeritus Professor of the University of Tokyo and a Professor of Chuo University. Concurrently he serves as the Director of Research Center for Information Security, National Institute of Advanced Industrial Science and Technology. His current research interests include information theory, coding theory, cryptography, and information security. From IEICE Dr. Imai received Best Book Awards in 1976 and 1991, Best Paper Awards in 1992, 2003 and 2004, Yonezawa Memorial Paper Award in 1992, Achievement Award in 1995, Inose Award in 2003, and Distinguished Achievement and Contributions Award in 2004. He also received Golden Jubilee Paper Award from the IEEE Information Theory Society in 1998, and Official Commendations from the Minster of Internal Affairs and Communications in June 2002 and from the Minister of Economy, Trade and Industry in October 2002. He was awarded Honor Doctor Degree by Soonchunhyang University, Korea in 1999 and Docteur Honoris Causa by the University of Toulon Var, France in 2002. He is also the recipient of the Ericsson Telecommunications Award 2005. Dr. Imai is a member of the Science Council of Japan. He was elected a Fellow of IEEE, IEICE, and IACR in 1992, 2001, and 2007, respectively. He has chaired many committees of scientific societies and organized a number of international conferences. He served as the President of the Society of Information Theory and its Applications in 1997, of the IEICE Engineering Sciences Society in 1998, and of the IEEE Information Theory Society in 2004. He is currently the Chair of CRYPTREC (Cryptography Techniques Research and Evaluation Committee of Japan).