Journal of Information Processing Vol.25 288–295 (Mar. 2017)

[DOI: 10.2197/ipsjjip.25.288]

Regular Paper

Proposal of WEP Operation with Strong IV and Its Implementation

Yuhei Watanabe[1,a)] Takahiro Iriyama[1] Masakatu Morii[1]

Received: May 30, 2016, Accepted: December 1, 2016

Abstract: WEP has serious vulnerabilities, and they cause various key recovery attacks. Although a more secure protocol such as WPA2 is recommended, according to each research by IPA and Keymans NET, WEP is still widely used because of the lack of knowledge about security of the wireless LAN. On the other hand, it takes large costs to replace a wireless LAN equipment in large-scale facilities. They need a secure method which can be used on their equipment by updating the firmware of WEP. In 2011, Morii, one of us, et al. showed IVs which prevented the Klein attack, the PTW attack, and the TeAM-OK attack. However, they did not present how to obtain such IVs and evaluate security of them. This paper shows the secure method of WEP and how to use it as fast as WEP. We show an IV which prevents the establishment of previous key recovery attacks. Moreover, we show how to use our IV efficiently on the operation of WEP. Our method requires about 1.1 times the processing time for the encryption than WEP. As a result, our method can prevent previous key recovery attacks and realize communication as fast as WEP.

Keywords: wireless LAN, WEP, RC4, IV, Strong IV

1. Introduction

Wired Equivalent Privacy (WEP) was designed as the security protocol for the wireless LAN by using RC4. WEP uses a secret key including a 3-byte initialization vector (IV), and encrypts data by RC4 algorithm. WEP has some serious vulnerabilities, and many key recovery attacks were proposed.

In 2001, the first key recovery attack was shown by Fluhrer, Mantin, and Shamir (called the FMS attack) [1]. This attack utilizes a specific vulnerable IV (called a weak IV) to recover the secret key. The FMS attack was expanded by Korek in 2004 (called the Korek attack) [2]. In 2006, Klein showed the key recovery attack (called the Klein attack) based on a statistical property [3]. The Klein attack recovers consecutively secret key bytes by using IVs and keystreams. Tews, Weinmann, and Pyshkin showed the improvement of the Klein attack in 2008 (called the PTW attack) [4]. Ohigashi, Kuwakado, and Morii showed the attack which used 19 to 31th bytes of a keystream (called the OKM attack) [5]. In 2010, Teramura et al. showed the attack which used the Klein attack, the PTW attack, and the OKM attack at the same time (called the TeAM-OK attack) [6]. Sepehrdad et al. showed the key recovery attack which used 22 statistical properties at the same time (call the Tornado attack) in 2013 [7]. The Tornado attack recovers the secret key by using 22,500 packets with probability 0.5.

From the above discussion, WEP is not a secure protocol. A more secure protocol such as Wi-Fi Protected Access2 (WPA2) [8] is recommended on the wireless LAN. Despite such a situation, according to each research by IPA and Keymans NET, WEP is still widely used [9], [10]. This is because it takes many costs to change the device which has the more secure protocol. Also, this is because the lack of knowledge about security of the wireless LAN. We consider that we need a secure method which can be used on a previous wireless LAN equipment by updating the firmware of WEP. If we would like to use WEP safely, we update the secret key whenever a certain number of packets are communicated. Previous key recovery attacks are difficult to recover the secret key by observing 10,000 packets. If we update the secret key every 10,000 packets, we can prevent a key recovery attack on WEP. However the throughput of communication is decreased by updating frequently the secret key. On the other hand, we can avoid the key recovery attack by removing the cause of the attack such as the weak IV or the statistical property. The way of removing the weak IV is realized by WEPplus [11]. WEPplus is introduced to the wireless LAN equipment by updating the firmware. There is an IV which prevents the establishment of the statistical property for the attack. When we use such IVs on WEP, we can avoid key recovery attacks based on the statistical property. There is a secure WEP operation by using a specific IV. In 2011, Morii, one of us, et al. showed the existence of IVs which prevented the Klein attack, the PTW attack, and the TeAM-OK attack [12]. They called such the IV the Strong IV. However, they did not present how to obtain the Strong IV and evaluate security of it.

1.1 Our Contribution

This paper shows the secure method of WEP. We also show how to use our method as fast as WEP. We show an IV which prevents previous key recovery attacks. Our method uses a specific IV which does not fulfill conditions of the Klein attack, the Korek attack, and the SVV_10 bias [13]. This IV can prevent the

[1] Graduate School of Engineering, Kobe University, Kobe 657–8501, Japan.

[a)] yuheiwatanabe@stu.kobe-u.ac.jp

establishment of major statistical properties on previous key recovery attacks. Therefore, we can avoid key recovery attacks by using our IV. In this paper, we call such IVs improved Strong IVs. We also show how to obtain the improved Strong IV efficiently. In order to suppress the reduction of the throughput, we have to efficiently examine an IV. In the case of the key recovery attack based on the statistical properties, if all conditions for the attack are fulfilled, attackers guess the candidate of the secret key. Since the Korek attack has multiple conditions, we have to choose properly avoiding conditions. In this paper, we choose conditions so as to avoid many attack functions by using a small number of conditions. We construct the filtering pattern of the IV based on the chosen conditions. Since the improved Strong IV is generated with high probability, it can be obtained with short time. Moreover, we show the method of WEP with the improved Strong IV to avoid the reduction of the throughput.

In order to achieve the improvement of the throughput, we examine the improved Strong IV and encrypt a packet at the same time. In the secure WEP operation, we assume that we update the secret key every 100,000 packets. Then, we use 100,000 IVs including 50,000 improved Strong IVs and 50,000 IVs which prevent the Korek attack and the SVV_10 bias (called the semi-improved Strong IV). This is because we prevent the leakage of the secret key by using the statistical attack for WEP with the Strong IV. We evaluate the processing time to examine IVs and encrypt 50,000 packets. When the packet size is 1,472 bytes, we take 338 millisecond for the encryption of 50,000 packets by using improved Strong IVs. We also take 320 millisecond for the encryption of 50,000 packets by using semi-improved Strong IVs. If we use generic WEP, we take 306 millisecond for the encryption of 50,000 packets. Therefore, our method requires 1.1-1.2 times the processing time for the encryption. As a result, our method can prevent all previous attacks and realize high speed operation. We can realize our method by introducing the process of the distinction of the IV and the process of the replacement of the secret key. Therefore, our method can be introduced to the device by updating the firmware as well as WEPplus.

This paper is organized as follows. In Section 2, we explain the description of WEP. In Section 3, we describe previous key recovery attacks on WEP and countermeasures for them. In Section 4, we show a new secure WEP operation. Section 5 concludes this paper.

2. Wired Equivalent Privacy

2.1 RC4 Stream Cipher

The stream cipher RC4 is designed by Ronald Rivest in 1987. RC4 has the high performance on the software, and is widely used in commercial applications, SSL/TLS and WEP [14].

RC4 consists of a key scheduling algorithm (KSA) and a pseudo-random number generation algorithm (PRGA). Let S be the internal state of RC4. S has N elements. The KSA initializes state S consisting of a permutation of $\{0, 1, \ldots, N-1\}$ by using a ℓ-byte secret key K. Typically, N is equal to 256 and ℓ is equal to 16. $S_{r'}$ represents the r'-th state on the KSA. The PRGA generates a keystream $Z_1, Z_2, \ldots, Z_r, \ldots$ from S, where r is a round number of the PRGA. Z_r is XOR-ed with the r-th plaintext word P_r to obtain the ciphertext word C_r. The algorithms of RC4 are shown in Algorithm 1 and 2, where + is an arithmetic addition modulo N.

Algorithm 1 Key Scheduling Algorithm

KSA($K[0, \ldots, \ell-1]$)**:**
  for $i = 0$ to $N-1$ **do**
    $S[i] \leftarrow i$
  end for
  $j \leftarrow 0$
  for $i = 0$ to $N-1$ **do**
    $j \leftarrow j + S[i] + K[i \bmod \ell]$
    Swap $S[i]$ and $S[j]$
  end for

Algorithm 2 Pseudo-Random Generation Algorithm

PRGA(K)**:**
  $i \leftarrow 0$
  $j \leftarrow 0$
  $S' \leftarrow KSA(K)$
  loop
    $i \leftarrow i + 1$
    $j \leftarrow j + S'[i]$
    Swap $S'[i]$ and $S'[j]$
    Output $Z \leftarrow S'[S'[i] + S'[j]]$
  end loop

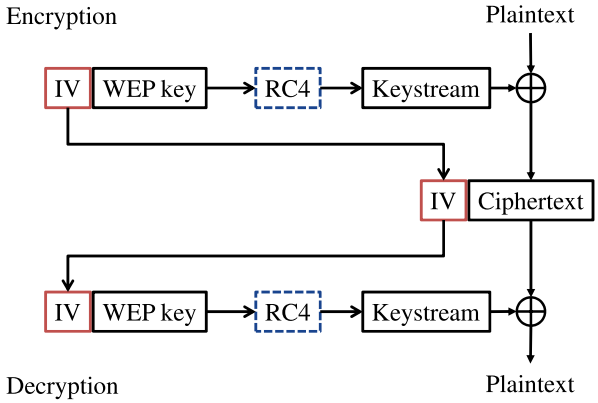

Fig. 1 WEP operation.

2.2 WEP

WEP is the wireless LAN encryption scheme based on RC4. **Figure 1** shows a WEP operation. The secret key of WEP consists of a 24-bit Initialization vector (IV) and a 40- or a 104-bit WEP key. This paper assume the 104-bit WEP key. The secret key of WEP is given as follows:

$$\begin{aligned} K &= K[0]||K[1]||K[2]||K[3]||\cdots||K[15] \\ &= IV_0||IV_1||IV_2||K[3]||\cdots||K[15], \end{aligned}$$

where IV_i represents the $(i+1)$-th byte of the IV and $K[3]||\cdots||K[15]$ represents the WEP key. When using WEP, the value of the IV is changed for each packet. This operation is to prevent the same keystream to be generated by using different secret keys for each packet. Since the IV has to be shared between two parties that communicate, the IV is communicated along with the ciphertext. Then, the IV is not encrypted. Moreover, since the length of the IV is 24-bit, the IV area is small. These properties

of the IV cause vulnerability on WEP.

3. Previous Key Recovery Attacks and Its Countermeasures

WEP has several vulnerabilities. They are divided into two categories: One uses weak IVs, and the other uses the statistical properties between the internal states and keystreams. Attackers utilize these vulnerabilities to recover the WEP key. On the other hand, countermeasures for key recovery attacks are shown. This section briefly describes previous key recovery attacks for WEP and countermeasures for them.

3.1 Previous Key Recovery Attacks on WEP

3.1.1 Key Recovery Attacks Based on Weak IV

In 2001, Fluher, Mantin and Shamir proposed the key recovery attack that depended on the IV [1]. This attack is called the FMS attack. The FMS attack guesses the internal state of RC4 by using the weak IV and recovers the WEP key. Since this attack is valid only for packets that are encrypted with the weak IV, a large number of packets are required. The FMS attack requires about four million to six million packets to recover the WEP key.

In 2004, Korek presented the extended attack of the FMS attack [2]. This attack can use more IVs as weak IVs than the FMS attack. Thus, this attack can reduce the number of packets required for the attack. The Korek attack requires about five hundred thousand to one million packets to recover the WEP key.

3.1.2 Key Recovery Attacks Based on Statistical Properties

The key recovery attack based on statistical properties is proposed by Klein in 2006 [3]. The Klein attack guesses the internal state of the KSA and the PRGA with the IV and the first 15 bytes of the keystream and recovers one byte WEP key consecutively.

The Klein attack has two conditions to recover the WEP key. Let x be an index of the WEP key. When attackers analyze the WEP key $K[x]$, conditions are given as follows. First each j do not touch the index x from round $x+1$ to N on the KSA and from round 1 to $x-1$ on the PRGA, respectively. This condition is described as follows,

$$S_{x+1}[x] = S'_{x-1}[x].$$

This paper defines this event as Condition 1. Second condition is that the value of $S'_{x-1}[x]$ is uniquely determined. This condition is given as follows,

$$S'_{x-1}[x] = x - Z_x.$$

This paper defines this event as Condition 2. **Figure 2** shows Condition 1 and 2. If Condition 1 and 2 are established at the same time, the following equation is obtained.

$$\begin{aligned} K[x] &= f_{Klein}(K[0], \ldots, K[x-1], Z_x) \\ &= S_x^{-1}[x - Z_x] - j_x - S_x[x] \end{aligned} \tag{1}$$

When attackers have the IV, the keystream Z_x and WEP key bytes $K[3], K[4], \ldots, K[x-1]$, the candidate of $K[x]$ is obtained from the equation (1). Then, one candidate is determined from one packet. The success probability of the Klein attack is given as follows.

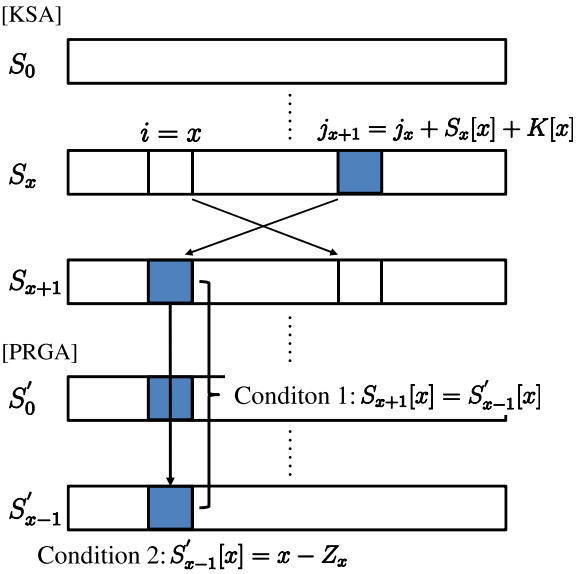

Fig. 2 Conditions of Klein attack.

$$\begin{aligned} Prob_{Klein} &= \left(\frac{255}{256}\right)^{254} \cdot \frac{2}{256} \\ &\quad + \left(1 - \left(\frac{255}{256}\right)^{254}\right) \cdot \frac{254}{256 \cdot 255} \\ &\approx \frac{1.36}{256} \end{aligned}$$

Attackers vote on Eq. (1) by using many packets and guess one WEP key byte from the candidate that is obtained most frequently. When the attacker intercepts 60,000 packets, the Klein attack can obtain the WEP key with probability 0.5.

In 2008, Tews, Weinmann and Pyshkin showed the PTW attack [4]. The PTW attack also uses IVs and keystreams to recover the WEP key. This attack uses the approximation of the state to analyze the WEP key. Except for the approximation, the attack function of the PTW attack is similar to that of the Klein attack. The attack function of the PTW attack is given as follows,

$$\begin{aligned} \sigma_x &= f_{PTW}(K[0], K[1], K[2], Z_x) \\ &= S_3^{-1}[x - Z_x] - j_3 - \sum_{l=3}^{x} S_3[l], \end{aligned}$$

where σ_x represents the sum from $K[3]$ to $K[x]$. The success probability of the PTW attack is

$$\begin{aligned} Prob_{(PTW,x)} &= q_x \cdot \left(\frac{255}{256}\right)^{254} \cdot \frac{2}{256} \\ &\quad + \left(1 - q_x \cdot \left(\frac{255}{256}\right)^{254}\right) \cdot \frac{254}{256 \cdot 255}, \end{aligned}$$

where

$$q_x = \left(\frac{255}{256}\right)^{x-3} \cdot \left(\frac{256 - x + 3}{256}\right) \cdot \prod_{k=1}^{x-3} \left(\frac{256 - k}{256}\right).$$

This attack can derive the sum of the WEP key in parallel. When the attacker intercepts 40,000 packets, the PTW attack can obtain the WEP key with probability 0.5.

In 2010, Teramura et al. proposed the TeAM-OK attack [6]. This attack uses attack functions of the Klein attack, the PTW

Table 1 The biases for RC4, exploitable against Tornado attack [7].

row	reference	attack function	conditions for the vote
x	Klein-Improved	$S_t^{-1}[x - Z_x] - \sigma_x(t)$	$(x - Z_x) \notin \{S_t[t+1], \ldots, S_t[x-1]\}$
$x \neq 1$	MP-Improved	$Z_{x+1} - \sigma_x(t)$	$x \neq 1,\ z_{x+1} \geq x,\ \forall 0 \leq i' \leq t : j_{i'} \neq z_{x+1}$
16	SVV_10 [13]	$S_t^{-1}[0] - \sigma_{16}(t)$	$S_t^{-1}[0] < t+1$ or $S_t^{-1}[0] > 15,\ Z_{16} = -16,\ j_2 \notin \{t+1, \ldots, 15\}$
x	A_u15	$2 - \sigma_x(t)$	$S_t[x] = 0,\ Z_2 = 0$
x	A_s13	$S_t^{-1}[0] - \sigma_x(t)$	$S_t[1] = x,\ (S_t^{-1}[0] < t+1$ or $S_t^{-1}[0] > x-1),\ Z_1 = x$
x	A_u13_1	$S_t^{-1}[Z_1] - \sigma_x(t)$	$S_t[1] = x,\ (S_t^{-1}[Z_1] < t+1$ or $S_t^{-1}[Z_1] > x-1),\ Z_1 = 1 - x$
x	A_u13_2	$1 - \sigma_x(t)$	$S_t[x] = x,\ S_t[1] = 0,\ Z_1 = x$
x	A_u13_3	$1 - \sigma_x(t)$	$S_t[x] = x,\ S_t[1] = 1 - x,\ Z_1 = 1 - x$
x	A_s5_1	$S_t^{-1}[Z_1] - \sigma_x(t)$	$S_t[1] < t+1,\ S_t[1] + S_t[S_t[1]] = x,$ $Z_1 \neq \{S_t[1], S_t[S_t[1]]\},$ $(S_t^{-1}[Z_1] < t+1$ or $S_t^{-1}[Z_1] > x-1)$
x	A_s5_2	$S_t^{-1}[S_t[1] - S_t[2]] - \sigma_x(t)$	$S_t[2] + S_t[1] = x,\ S_t^{-1}[S_t[1] - S_t[2]] \neq \{1,2\},$ $(S_t^{-1}[S_t[1] - S_t[2]] < t+1$ or $S_t^{-1}[S_t[1] - S_t[2]] > x-1),$ $Z_2 = S_t[1]$
x	A_s5_3	$S_t^{-1}[Z_2] - \sigma_x(t)$	$S_t[2] + S_t[1] = x,\ S_t^{-1}[Z_2] \neq \{1,2\},$ $(S_t^{-1}[Z_2] < t+1$ or $S_t^{-1}[Z_2] > x-1),$ $Z_2 = 2 - S_t[2]$
x	A_u5_1	$S_t^{-1}[S_t^{-1}[Z_1] - x] - \sigma_x(t)$	$S_t[1] = x,\ S_t^{-1}[Z_1] < t+1,\ S_t^{-1}[S_t^{-1}[Z_1] - x] \neq 1,$ $(S_t^{-1}[S_t^{-1}[Z_1] - x] < t+1$ or $S_t^{-1}[S_t^{-1}[Z_1] - x] > x-1),$ $Z_1 \neq \{x, 1-x, S_t^{-1}[Z_1] - x\},\ S_t^{-1}[Z_1] \neq 2x$
x	A_u5_2	$1 - \sigma_x(t)$	$S_t[x] = 1,\ Z_1 = S_t[2]$
x	A_u5_3	$1 - \sigma_x(t)$	$S_t[x] = x,\ S_t^{-1}[Z_1] \neq 1,\ S_t^{-1}[Z_1] < t+1,\ Z_1 = S_t[S_t[1] + x]$
x	A_s3	$S_t^{-1}[Z_2] - \sigma_x(t)$	$S_t[1] \neq 2,\ S_t[2] \neq 0,\ S_t[2] + S_t[1] < t+1,$ $S_t[2] + S_t[S_t[2] + S_t[1]] = x,\ S_t^{-1}[Z_2] \neq \{1,2,S_t[1] + S_t[2]\},$ $S_t[1] + S_t[2] \neq \{1,2\},\ (S_t^{-1}[Z_2] < t+1$ or $S_t^{-1}[Z_2] > x-1)$
4	A_4_s13	$S_t^{-1}[0] - \sigma_4(t)$	$S_t[1] = 2,\ S_t[4] \neq 0,\ (S_t^{-1}[0] < t+1$ or $S_t^{-1}[0] > x-1),\ Z_2 = 0$
4	A_4_u5_1	$S_t^{-1}[254] - \sigma_4(t)$	$S_t[1] = 2,\ Z_2 \neq 0,\ Z_2 \neq 254,\ (S_t^{-1}[254] < t+1$ or $S_t^{-1}[254] > 3)$
4	A_4_u5_2	$S_t^{-1}[255] - \sigma_4(t)$	$S_t[1] = 2,\ Z_2 \neq 0,\ (S_t^{-1}[255] < t+1$ or $S_t^{-1}[255] > 3),\ Z_2 = S_t[2]$
x	A_neg_1	$1 - \sigma_x(t)$ or $2 - \sigma_x(t)$	$S_t[2] = 0,\ S_t[1] = 2,\ Z_1 = 2$
x	A_neg_2	$2 - \sigma_x(t)$	$S_t[2] = 0,\ S_t[1] \neq 2,\ Z_2 = 0$
x	A_neg_3	$1 - \sigma_x(t)$ or $2 - \sigma_x(t)$	$S_t[1] = 1,\ Z_1 = S_t[2]$
x	A_neg_4	$-\sigma_x(t)$ or $1 - \sigma_x(t)$	$S_t[1] = 0,\ S_t[0] = 1,\ Z_1 = 1$

attack, and the OKM attack [5]. Let w be an index of the keystream. The attack function of the OKM attack is represented as follows:

$$K[w-16] = f_{OKM}(K[0], \ldots, K[w-17], \sigma_{15}, Z_w),$$

where $w = 19, 20, \ldots, 31$. The success probability of the OKM attack is

$$Prob_{(OKM,w)} = q_w' \cdot \left(\frac{255}{256}\right)^{254} \cdot \frac{2}{256} + \left(1 - q_w' \cdot \left(\frac{255}{256}\right)^{254}\right) \cdot \frac{254}{256 \cdot 255},$$

where

$$q_w' = \left(\frac{255}{256}\right)^{32-w} \cdot \left(\frac{256 - 32 + w}{256}\right) \cdot \prod_{k=w-15}^{16} \left(\frac{256 - w - 1 + k}{256}\right).$$

The OKM attack assumes that the sum of WEP key bytes is known. When attackers intercept 36,500 packets, the TeAM-OK attack can obtain the WEP key with probability of 0.5.

Both the PTW attack and the TeAM-OK attack require conditions of the Klein attack. Therefore, when conditions of the Klein attack are not fulfilled, these attacks do not succeed.

3.1.3 Tornado Attack

Sepehrdad et al. presented the Tornado attack at FSE 2013 [7]. This attack uses 22 attack functions to recover the WEP key. These attack functions include the improved version of the Klein attack (Klein-Improved), the improved version of the Maitra-Paul attack (MP-Improved) in Ref. [15], the improved version of 19 biases by Korek, and the improved bias of Sepehrdad, Vaudenay, and Vuagnoux (SVV_10) in Ref. [13]. **Table 1** shows attack functions and its conditions for the vote. Let t be the index of the last known state. For instance, since attackers know $K[0]$, $K[1]$, and $K[2]$ in the WEP protocol, they can assume $t = 2$. In Table 1, $\sigma_x(t)$ is

$$\sigma_x(t) = \sum_{j=0}^{t} S_{j-1}[x] + \sum_{j=t+1}^{x} S_t[j].$$

When conditions for the vote are established, attackers obtain the candidate of the WEP key by using an attack function. When attackers intercept 22,500 packets, the Tornado attack can obtain the WEP key with probability 0.5.

3.2 Countermeasures for Previous Key Recovery Attacks on WEP

3.2.1 WEPplus

WEPplus enhances WEP security by avoiding weak IVs [11]. Then, WEPplus can prevent a key recovery attack based on the weak IV. When WEPplus is used at both ends of the wireless

connection, WEPplus is completely effective. WEPplus, however, can not prevent a key recovery attack based on the statistical properties.

At SCIS 2006, Yoshida, Kobara, and Imai showed the efficient way to avoid weak IVs of the FMS attack [16]. Their method can eliminate almost all weak IVs for FMS attack.

3.2.2 Strong IV

According to Section 3.1, if attackers intercept less than 20,000 packets, it is difficult to recover the WEP key by previous key recovery attacks. Moreover, previous key recovery attacks can not recover the WEP key from intercepting 10,000 packets. If we want to prevent a key recovery attack based on statistical properties, we update the WEP key whenever 10,000 packets are communicated. However, since 10,000 packets are very few, the throughput of communication is decreased.

As the solution to this problem, Morii, one of us, et al. proposed the Strong IV in 2011 [12]. The Strong IV is the IV that fail to the Klein attack. When the Strong IV is used, the condition of the Klein attack is not fulfilled, and then it is difficult to recover the WEP key by using the Klein attack. The Strong IV can also prevent the PTW attack and the TeAM-OK attack because these attacks have same conditions of the Klein attack. However, they did not present how to obtain such IVs by the practical way and the evaluation of the security.

4. Secure WEP Operation with New Strong IV

In this section, we show the secure WEP operation. We show how to prevent the key recovery attack by using a new Strong IV. Moreover, we evaluate the processing time for the encryption on the our technique.

4.1 How to Prevent Key Recovery Attack for WEP

4.1.1 Definition of Strong IV

We show the new definition of the Strong IV in order to obtain it with high probability. We define the Strong IV as the IV which does not fulfill either Condition 1 or Condition 2 of the Klein attack. The condition of the Strong IV for $K[x]$ is given as follows:

$$S_{x+1}[x] \neq S'_{x-1}[x] \; or \; S'_{x-1}[x] \neq x - Z_x.$$

Since the Strong IV depends on the value of the WEP key to be used, it is necessary to make a determination of the Strong IV for each byte of the WEP key. Our method uses the Strong IV that protects 13 bytes of the WEP key. Let $Prob_{StrongIV_{13}}$ be the generation probability of the Strong IV for the 13-byte WEP key. The generation probability of the Strong IV is given as follows,

$$Prob_{StrongIV_{13}} = \left(1 - \left(\frac{255}{256}\right)^{254} \cdot \frac{2}{256}\right)^{13} \approx 0.96.$$

Since our Strong IV is obtained with high probability, we can generate it with short time.

If we use only Strong IVs on WEP, the conditions of the Klein attack are not happen. As mentioned in Section 3.2.2, the PTW attack and the OKM attack has same conditions. Therefore, the success probability of the Klein attack, the PTW attack, and the OKM attack are given as follows,

$$Prob'_{Klein} = \left(1 - \left(\frac{255}{256}\right)^{254}\right) \cdot \frac{254}{256 \cdot 255} \approx \frac{0.63}{256}.$$

$$Prob'_{(PTW,x)} = \left(1 - q_x \cdot \left(\frac{255}{256}\right)^{254}\right) \cdot \frac{254}{256 \cdot 255}.$$

$$Prob'_{(OKM,w)} = \left(1 - q'_w \cdot \left(\frac{255}{256}\right)^{254}\right) \cdot \frac{254}{256 \cdot 255}.$$

Since this probability is lower than a random distribution, attackers can get information of the WEP key by observing the candidate with a low probability.

4.1.2 Filtering for Korek Attack

The Tornado attack consists of 22 attack functions as shown in Table 1. When all conditions for the vote on the attack function are fulfilled, attackers guess a candidate of the WEP key. If one condition for the vote is not fulfilled, the attack function is disabled on the Tornado attack. Therefore, we can prevent the Tornado attack by avoiding some conditions for the vote. We can prevent the Klein-Improved by using the same way of our Strong IV. As shown in Section 3.1.3, we assume $t = 2$ in Table 1 because attackers know $K[0]$, $K[1]$, and $K[2]$. We consider that attack functions based on the Korek attack can be prevented by avoiding some IVs. According to Table 1, if the last known state fulfills following conditions, attack functions based on the Korek attack are disabled except for A_u5_3.

$$S_2[x] \neq 0,$$
$$S_2[x] \neq 1,$$
$$S_2[2] \neq 0,$$
$$15 < S_2[1] < 241,$$
$$15 < S_2[1] + S_2[2],$$

where $3 \leq x \leq 15$. The last known state is obtained after processing the KSA by the IV. We can determine the establishment of conditions by the IVs. About 78 percent of the whole of the IV generate the last known state which fulfills these conditions. We remove remaining IVs by a filtering pattern as shown in later. Let $j_{r'}$ be a pointer j on r'-th round of the KSA. In order to fulfill conditions $S_2[x] \neq 0$, $S_2[x] \neq 1$, $S_2[2] \neq 0$, and $15 < S_2[1] < 241$, we remove $3 \leq IV_0 \leq 15$. According to the algorithm of the KSA, if IV_0 is 0, j_0 is 0. In this case, j_1 is $j_1 = 0 + 1 + IV_1 = IV_1 + 1$. We swap $S_1[1]$ and $S_1[IV_1 + 1]$. In order to fulfill conditions $S_2[x] \neq 1$ and $15 < S_2[1] < 241$, $j_2 \neq 1$, and IV_1 is $14 < IV_1 < 240$. Then, we remove following IV_1.

$$0 \leq IV_1 \leq 14, \; 240 \leq IV_1 \leq 255.$$

In this case, j_2 is $j_2 = IV_1 + IV_2 + 3$. In order to fulfill the condition $S_2[2] \neq 0$, j_2 is $j_2 = IV_1 + IV_2 + 3 \neq 0$. Then, $IV_1 + IV_2 \neq 253$. As mentioned before, since $j_2 \neq 1$, j_2 is $IV_1 + IV_2 + 3 \neq 1$. Then, $IV_1 + IV_2 \neq 254$. We swap $S_2[2]$ and $S_2[j_2]$. After swapping, $S_2[1] = IV_1 + 1$ and $S_2[2] = IV_1 + IV_2 + 3$. In order to fulfill condition $15 < S_2[1] + S_2[2] (< 256)$, this condition given as follows,

$$15 < IV_1 + 1 + IV_1 + IV_2 + 3 < 256$$

$\rightarrow 11 < 2IV_1 + IV_2 < 252.$

Therefore, we remove $0 \leq 2IV_1 + IV_2 \leq 11$ and $252 \leq 2IV_1 + IV_2 \leq 255$. If $IV_2 = 254$, j_2 is $j_2 = IV_1 + 1$. In this case, $S_2[2]$ is one after swapping. Since $S_2[1]$ fulfills $15 < S_2[1] < 241$, the condition $15 < S_2[1] + S_2[2]$ is established. We summarize above conditions of IVs.

Case 1 $IV_0 = 0$

If IV_1 and IV_2 fulfill following conditions, we remove such IV_1 and IV_2.

$$0 \leq IV_1 \leq 14,\ 240 \leq IV_1 \leq 255,$$
$$0 \leq 2IV_1 + IV_2 \leq 11,\ 252 \leq 2IV_1 + IV_2 \leq 255,$$
$$IV_1 + IV_2 = 253,\ 254,$$

where $IV_2 = 254$ is not removed.

When IV_0 is another value, the filtering pattern of IV_1 and IV_2 is given as follows. In other cases, we obtain conditions of IVs as well as Case 1.

Case 2 $IV_0 = 1$

If IV_1 and IV_2 fulfill following conditions, we remove such IV_1 and IV_2.

$$0 \leq IV_1 \leq 14,\ 240 \leq IV_1 \leq 255,$$
$$0 \leq 2IV_1 + IV_2 \leq 11,\ 252 \leq 2IV_1 + IV_2 \leq 255,$$
$$IV_1 + IV_2 = 254,$$
$$IV_2 = 254.$$

Case 3 $IV_0 = 2$

If IV_1 and IV_2 fulfill following conditions, we remove such IV_1 and IV_2.

$$0 \leq IV_1 \leq 12,\ 238 \leq IV_1 \leq 255,$$
$$0 \leq 2IV_1 + IV_2 \leq 9,\ 250 \leq 2IV_1 + IV_2 \leq 255,$$
$$0 \leq IV_1 + IV_2 \leq 12,\ 254 \leq IV_1 + IV_2 \leq 255,$$

where $IV_2 = 0$ is not removed.

Case 4 $IV_0 = 16$

If IV_1 fulfills following conditions, we remove such IV_1.

$$224 \leq IV_1 \leq 238,$$
$$240 \leq IV_1 \leq 255.$$

In this case, there are three filtering patterns of IV_2 depending on the value of IV_1.

Case 4-1 $IV_1 = 223$

If IV_2 fulfills following conditions, we remove such IV_2.

$$30 \leq IV_2 \leq 45,$$
$$IV_2 = 14, 15.$$

Case 4-2 $IV_1 = 239$

If IV_2 fulfills following conditions, we remove such IV_2.

$$238 \leq IV_2 \leq 253,$$
$$IV_2 = 14, 255.$$

Case 4-3 Other values of IV_1

If IV_2 fulfills following conditions, we remove such IV_2.

$$220 \leq 2IV_1 + IV_2 \leq 235,$$
$$IV_1 + IV_2 = 238, 253,$$

where $IV_2 = 254$ is not removed.

Case 5 $IV_0 = 17, 18, \ldots, 240$

If IV_1 fulfills following conditions, we remove such IV_1.

$$0 \leq IV_0 + IV_1 \leq 14,$$
$$240 \leq IV_0 + IV_1 \leq 254,$$
$$IV_1 = 255.$$

In this case, there are three filtering patterns of IV_2 depending on the value of IV_1.

Case 5-1 $0 \leq 2IV_0 + IV_1 \leq 14$ or $2IV_0 + IV_1 = 255$

If IV_2 fulfills following conditions, we remove such IV_2.

$$0 \leq 2(IV_0 + IV_1) + IV_2 \leq 11,$$
$$252 \leq 2(IV_0 + IV_1) + IV_2 \leq 255,$$
$$IV_0 + IV_1 + IV_2 = 253, 254.$$

Case 5-2 $IV_0 + IV_1 = 255$

If IV_2 fulfills following conditions, we remove such IV_2.

$$IV_1 - 1 \leq IV_2 \leq IV_1 + 14,$$
$$IV_1 + IV_2 = 253,$$
$$IV_0 + IV_1 + IV_2 = 254.$$

Case 5-3 Other values of IV_1

If IV_2 fulfills following conditions, we remove such IV_2.

$$0 \leq 2(IV_0 + IV_1) + IV_2 \leq 11,$$
$$252 \leq 2(IV_0 + IV_1) + IV_2 \leq 255,$$
$$IV_1 + IV_2 = 253,$$
$$IV_0 + IV_1 + IV_2 = 254,$$

where $IV_2 = 254$ is not removed.

Case 6 $IV_0 = 241, 242, \ldots, 255$

If IV_1 fulfills following conditions, we remove such IV_1.

$$0 \leq IV_0 + IV_1 \leq 14,$$
$$240 \leq IV_0 + IV_1 \leq 255.$$

In this case, there are two filtering patterns of IV_2 depending on the value of IV_1.

Case 6-1 $0 \leq 2IV_0 + IV_1 \leq 14$ or $2IV_0 + IV_1 = 255$

If IV_2 fulfills following conditions, we remove such IV_2.

$$0 \leq 2(IV_0 + IV_1) + IV_2 \leq 11,$$
$$252 \leq 2(IV_0 + IV_1) + IV_2 \leq 255,$$
$$IV_0 + IV_1 + IV_2 = 253, 254.$$

Case 6-2 Other values of IV_1

If IV_2 fulfills following conditions, we remove such IV_2.

$$0 \leq 2(IV_0 + IV_1) + IV_2 \leq 11,$$
$$252 \leq 2(IV_0 + IV_1) + IV_2 \leq 255,$$

$$IV_1 + IV_2 = 253,$$
$$IV_0 + IV_1 + IV_2 = 254,$$

where $IV_2 = 254$ is not removed.

4.1.3 How to Get Improved Strong IV

We observe the internal state and the keystream and confirm the establishment of conditions for major attack functions such as the Klein-Improved, the A_u5_3 bias, and the SVV_10 bias. We call this IV an improved Strong IV. We obtain an improved Strong IV as follows.

Step1 Avoid a weak IV

We randomly generate an IV, and confirm an establishment of conditions for the IV as described above. If a condition is fulfilled, we generate another IV and execute Step 1.

Step2 Avoid the A_u5_3 bias and the SVV_10 bias

We obtain a state and a keystream from RC4, and confirm the establishment of conditions for the vote.

Step3 Avoid the Klein-Improved

We obtain a state and a keystream from RC4, and confirm the establishment of Condition 1 and 2 on the Klein attack.

Step4 Determine an improved Strong IV

When all attack functions are avoided, the IV is the improved Strong IV. If an attack function is established, we generate another IV and go back to Step 1.

As a result, we generate the improved Strong IV. Since the improved Strong IV prevents major attack functions from establishing, we can avoid all previous key recovery attacks on WEP.

4.2 Secure WEP Operation with Improved Strong IV

We describe the WEP operation with the improved Strong IV. We assume that we update the WEP key every 100,000 packets. When we use only the improved Strong IV on WEP, the probability of the candidate of the WEP key is lower than $1/256$ and the information of the WEP key is disclosed. Then, we combine the improved Strong IV and the generic IV in order to prevent the leakage of the WEP key in the communication of 100,000 packets. Let y be the number of the improved Strong IV. In the communication of the combined IV, the success probability of the Klein attack is given as follows,

$$\frac{y \cdot \frac{0.63}{256} + (100{,}000 - y) \cdot \frac{1.36}{256}}{100{,}000} = \frac{1}{256},$$
$$y = \frac{100{,}000}{1.36 - 0.63} \cdot 0.36,$$
$$y = 49{,}315.$$

Since the success probability of the Klein attack is constant, y is uniquely determined. We also derive the number of the improved Strong IV in order to prevent the leakage of the WEP key by the PTW attack or the OKM attack as well as the case of the Klein attack. We obtain y from following equations.

$$\frac{y \cdot Prob'_{(PTW,x)} + (100{,}000 - y) \cdot Prob_{(PTW,x)}}{100{,}000} = \frac{1}{256}.$$
$$\frac{y \cdot Prob'_{(OKM,w)} + (100{,}000 - y) \cdot Prob_{(OKM,w)}}{100{,}000} = \frac{1}{256}.$$

Since the success probability of these attacks depends on x and w, we show the maximum and the minimum number of the improved Strong IV. **Table 2** shows the number of the improved Strong IV to prevent the establishment of the PTW attack and the OKM attack, respectively. As a result, if we merge 50,000 improved strong IVs and 50,000 generic IVs, the success probability of the Klein attack, PTW attack, and the OKM attack becomes about $1/256$. When we use 50,000 improved Strong IVs and 50,000 generic IVs, the success probability of attacks is $1/256$. Since attackers don't know the WEP key, they can not distinguish improved Strong IVs from generic IVs. Therefore, they have to perform attacks by using 100,000 packets, and the success probability of their attacks is $1/256$. Therefore, we can prevent the Klein attack, the PTW attack, and the TeAM-OK attack in the communication of the 100,000 packets. Moreover, in order to prevent the Tornado attack, we use 50,000 improved Strong IVs and 50,000 semi-improved Strong IVs. **Figure 3** shows the process of the encryption on WEP with the improved strong IV. We confirm the IV by using the method as shown in Section 4.1. If an IV is a generic one, we generate a different IV by the method which is implemented on the equipment of WEP. On the other hand, if an IV is an improved Strong IV or a semi-improved Strong IV, we encrypt the packet and translate it. We obtain the improved Strong IV with probability $0.96 \cdot 0.78 = 0.749$ and the semi-improved Strong IV with probability 0.78, respectively. We consider that these probabilities are enough high. As a result, we generate mixed IVs and encrypt a packet at the same time.

We evaluate the processing time required for the encryption. We assume the case of using 50,000 improved strong IVs, 50,000 semi-improved Strong IVs, and 50,000 generic IVs, respectively. The length of a plaintext is 256, 1,024, and 1,472 byte. We perform the encryption for 1,024 randomly chosen WEP keys and evaluate the average of the processing time. We use Core i3 530 for this simulation. We show that our method can be performed on a home computer. **Table 3** shows results of simulation. Ac-

Table 2 The number of the improved Strong IVs for the PTW attack and the OKM attack.

PTW Attack	Maximum	Minimum
#improved Strong IVs	49,660	46,745
OKM Attack	Maximum	Minimum
#improved Strong IVs	49,586	49,208

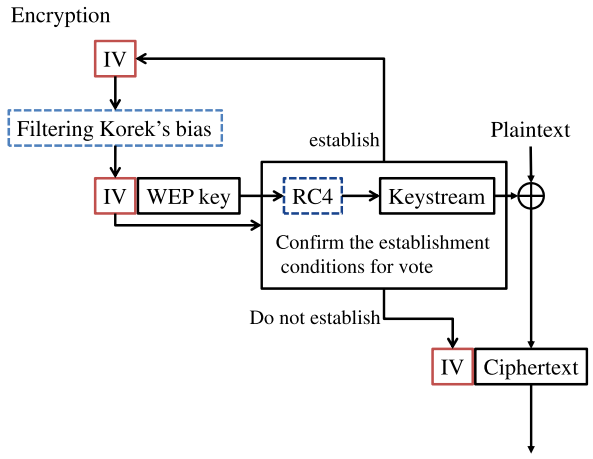

Fig. 3 Our method.

Table 3 Required time to encrypt 50,000 packets.

Data length (byte)	256	1,024	1,472
RC4 (ms)	104	232	306
Improved Strong IV (ms)	125	260	338
Semi-Improved Strong IV (ms)	111	243	320

cording to Table 3, our method requires 1.1 to 1.2 times the time for the encryption than WEP. Therefore, our method can secure and fast communication on WEP among transmitting 100,000 packets.

5. Conclusion

This paper showed the secure operation of WEP. We showed IVs which prevented conditions of the Klein attack, the Korek attack, and the SVV_10 bias. We defined this IV as the improved Strong IV and showed how to efficiently obtain it. Our method could perform the secure operation in communicating 100,000 packets. We evaluated the processing time for the encryption on our method by using computer simulation. As a result, our method required 1.1 to 1.2 times the processing time for the encryption than WEP. Therefore, our method could prevent all previous key recovery attacks and realize high speed operation. We could realize our method by introducing the process of the distinction of the IV and the process of the replacement of the secret key. Our method could be introduced to the device by updating the firmware as well as WEPplus.

According to key recovery attacks based on the statistical properties, we consider that a future attack also uses conditions of the Klein attack. Our method might prevent a such attack.

Acknowledgments We would like to thank to Tsukaune and Todo for their first contribution of the study of the improvement of the security of WEP by using the Strong IV. This work was supported in part by Grant-in-Aid for Scientific Research (C) (KAKENHI 26330155) for Japan Society for the Promotion of Science.

References

[1] Fluhrer, S.R., Mantin, I. and Shamir, A.: Weaknesses in the Key Scheduling Algorithm of RC4, *Selected Areas in Cryptography, 8th Annual International Workshop, SAC 2001, Toronto, Ontario, Canada, Revised Papers*, pp.1–24 (2001).
[2] Chaabouni, R.: Break WEP Faster with Statistical Analysis, Technical Report, EPFL, LASEC (2006).
[3] Klein, A.: Attacks on the RC4 stream cipher, *Des. Codes Cryptography*, Vol.48, No.3, pp.269–286 (2008).
[4] Tews, E., Weinmann, R. and Pyshkin, A.: Breaking 104 Bit WEP in Less Than 60 Seconds, *Information Security Applications, 8th International Workshop, WISA 2007, Jeju Island, Korea, Revised Selected Papers*, pp.188–202 (2007).
[5] Ohigashi, T., Kuwakado, H. and Morii, M.: A Key Recovery Attacks on WEP with Less Packets, Technical Report of IEICE, ISEC (2007).
[6] Teramura, R., Asakura, Y., Ohigashi, T., Kuwakado, H. and Morii, M.: Fast WEP-Key Recovery Attack Using Only Encrypted IP Packets, *IEICE Trans.*, Vol.93-A, No.1, pp.164–171 (2010).
[7] Sepehrdad, P., Susil, P., Vaudenay, S. and Vuagnoux, M.: Smashing WEP in a Passive Attack, *Fast Software Encryption - 20th International Workshop, FSE 2013, Singapore, Revised Selected Papers*, pp.155–178 (2013).
[8] Society, I.C.: 802.1X-Port Based Network Access Control, IEEE Std 802.11 (2001).
[9] IPA: Survey of Awareness for IT Security at 2015 (2015), available from ⟨https://www.ipa.go.jp/files/000050002.pdf⟩ (in Japanese).
[10] Keymans NET: Status of Introduction of Wireless LAN (2015), available from ⟨http://www.keyman.or.jp/at/30007875/⟩ (in Japanese).
[11] Orinoco: WEPplus white paper (Oct. 2001).
[12] Tsukaune, T., Todo, Y. and Morii, M.: A Proposal of a WEP Operation Secure Against the Key-Recovery Attack, *IEICE Technical Report*, Vol.111, No.209, pp.11–16 (2011).
[13] Sepehrdad, P., Vaudenay, S. and Vuagnoux, M.: Discovery and Exploitation of New Biases in RC4, *Selected Areas in Cryptography - 17th International Workshop, SAC 2010, Waterloo, Ontario, Canada, Revised Selected Papers*, pp.74–91 (2010).
[14] IEEE Computer Society: Wireless lan medium access control (MAC) and physical layer (PHY) specifications, IEEE Std 802.11 (1999).
[15] Maitra, S. and Paul, G.: New Form of Permutation Bias and Secret Key Leakage in Keystream Bytes of RC4, *Fast Software Encryption, 15th International Workshop, FSE 2008*, pp.253–269 (2008).
[16] Yoshida, M., Kobara, K. and Imai, H.: WEP Implementation Secure Against The Key Recovery Attacks Based On Weak IV, *Proc. Symposium on Cryptography and Information Security* (*SCIS*) (2006).

Yuhei Watanabe received his B.E. and M.E. degrees from Kobe University, Japan in 2012 and 2013, respectively. Since 2013, he has been a doctoral candidate in Graduate School of Engineering, Kobe University. His current research interests are in cryptography and information security. He received SCIS 2013 Innovation Paper Award from ISEC group of IEICE in 2014.

Takahiro Iriyama received his B.E. and M.E. degrees from Kobe University, Japan in 2014 and 2016, respectively. His research interests are in cryptography and information security.

Masakatu Morii received his B.E. degree in electrical engineering and the M.E. degree in electronics engineering from Saga University, Saga, Japan, and D.E. degree in communication engineering from Osaka University, Osaka, Japan, in 1983, 1985, and 1989, respectively. From 1989 to 1990 he was an Instructor in the Department of Electronics and Information Science, Kyoto Institute of Technology, Japan. From 1990 to 1995 he was an Associate Professor at the Department of Electronics and Information Science, Faculty of Engineering at Ehime University, Japan. From 1995 to 2005 he was a Professor at the Department of Intelligent Systems and Information Science, Faculty of Engineering at the University of Tokushima, Japan. Since 2005, he has been a Professor at the Department of Electrical and Electronics Engineering, Faculty of Engineering at Kobe University, Japan. His research interests are in error correcting codes, cryptography, discrete mathematics, computer networks and information security. He is a member of IEEE.