PAPER *Special Section on Cryptography and Information Security*

Generalized Classes of Weak Keys on RC4 Using Predictive State

Ryoichi TERAMURA†a), ***Student Member***, **Toshihiro OHIGASHI**††, **Hidenori KUWAKADO**†, ***Members***,
and* Masakatu MORII**†, ***Senior Member

SUMMARY Conventional class of weak keys on RC4 stream cipher is defined as a specific case that combinations of the first three bytes of secret key satisfy two relational equations. This paper expands and generalizes the classes of weak keys using generalized relational equations and special classes of the internal state (called predictive state). We derive the probability that generalized classes of weak keys leak the information of bytes of the secret key. Furthermore, we enumerate the generalized classes of weak keys and show that most of them leak more information of the secret key than Roos' one.

key words: *cryptanalysis, stream cipher, RC4, weak key, predictive state*

1. Introduction

RC4 [1] is the stream cipher designed by Rivest in 1987. It is adopted by part of encrypting protocols such as Secure Sockets Layer (SSL), Transport Layer Security (TLS) [2], Wired Equivalent Privacy (WEP) [3], Wi-Fi Protected Access (WPA) [4] etc. The internal state of RC4 consists of the permutation array of the $N(= 2^n)$ elements with the size of n bits. RC4 generally has very large internal state of approximately 1,700 bits when $n = 8$ is used. In addition, the length of the secret key is variable, and 40-256 bits are usually used.

Several vulnerabilities of RC4 have been reported. These are divided into two classes. One is the vulnerability of the protocol using RC4 and the other is that of RC4 itself. The typical example of the former is the attack against WEP. The previous works concluded that WEP is not secure [5]–[11], but these cannot affect the security of RC4 itself.

Many attacks on RC4 itself have been proposed, but so far no one has found an attack on RC4 which is even close to being practical. As the attack for RC4 itself, some internal state reconstruction attacks have been proposed [12]–[16]. These attacks exploit the special classes of RC4 partial states called predictive state. The predictive state creates unique patterns in the output stream and allows a viewer of the output stream to recover parts of the internal state with a non-negligible probability. In addition, several key recovery attacks on RC4 have been proposed. Most of them recover a secret key from an internal state when the Key Scheduling Algorithm (KSA) was finished (called initial state) [17]–[20]. They used the relational equations between an initial state and a secret key for these attacks. These attacks need the information of the initial state, but it is generally not observable. This means that a key recovery attack from an initial state does not immediately pose an additional threat to the security of RC4. Unlike the initial state, it is relatively easy for an adversary to get the output stream. Thus, the key recovery attack from output stream poses more serious threat to the security of RC4 than that from an initial state. The key recovery attack from output stream has been proposed by Roos [21]. This attack exploits the class of weak keys. The class of weak keys proposed by Roos satisfies two relational equations between the bytes of the secret key and leaks the information of 8 bits of the secret key with probability $2^{-2.9}$. However, Roos has used only two specific equations and has not mentioned other equations between the bytes of the secret key.

Our motivation comes from the suspicion such that another relational equation must be included between the bytes of the secret key. In this paper, we present generalized classes of weak keys on RC4 using predictive state. First, we generalize relational equations between the bytes of the secret key, and analyze internal states obtained by the secret key that satisfies the generalized equations. Next, considering the relation between the analyzed internal state and the predictive state, we show that many secret keys satisfy the generalized relational equations. Hence, we obtain many secret keys whose the output stream leaks the information of them. Furthermore, we distinguish the classes with respect to the probability that a class of weak keys leaks the information of bytes of secret key, and enumerate the number of classes when the number of predictive state is small. It is revealed that most of them leak more information of bytes of the secret key than conventional one. For example, one of the generalized classes of weak keys that satisfies the five relational equations between the key bytes leaks the information of 40 bits of the secret key with probability $2^{-7.1}$.

This paper is organized as follows: In Sect. 2, we review the algorithm of RC4 and class of weak keys proposed by Roos. We expand and generalize the class of weak keys and derive the probability the weak keys leaks these information in Sect. 3. We show the number of generalized class of weak keys and an example in Sect. 4. Finally, we conclude this paper in Sect. 5.

Manuscript received March 23, 2010.
Manuscript revised July 15, 2010.

†The authors are with the Graduate School of Engineering, Kobe University, Kobe-shi, 657-8501 Japan.
††The author is with Information Media Center, Hiroshima University, Higashihiroshima-shi, 739-8511 Japan.
a) E-mail: teramura@stu.kobe-u.ac.jp

DOI: 10.1587/transfun.E94.A.10

2. RC4

In this section, we briefly review the algorithm of the stream cipher RC4.

2.1 Description of RC4

The stream cipher RC4 consists of two algorithms: Key Scheduling Algorithm (KSA) and Pseudo-Random number Generation Algorithm (PRGA). The KSA initializes an internal state from a secret key K of l words of n bits and the PRGA generates a pseudo-random output stream Z from the initialized internal state as described in Fig. 1. RC4's internal state consists of an N-byte permutation array S and two indices i and j. Let $S_i[x]$ be the value of the array S at the index x and $S_i^{-1}[y]$ be the index of the value y in the array S after the i-th round in the PRGA, respectively. Then j_i is the value of j during the i-th round where the rounds are indexed with respect to i. We will use S^* for the array S during the KSA (i.e. $S_0 = S^*_N$). We define Z_i as the output stream after the i-th round in the PRGA. In this paper, all operations are carried out under modulo N.

2.2 Roos' Weak Key

In 1995, Roos [21] defined a class of weak keys that satisfies the following equations,

$$K[0] + K[1] = 0, \tag{1}$$

$$K[2] = X, \tag{2}$$

where $X \in \{0, 1, \dots, N-1\}$. When a secret key is included in such a class, the output stream generated from the key satisfies $Z_1 = X + 3$ with probability $2^{-2.9}$. This implies that the information of one secret key byte is leaked.

In 2007, Paul and Maitra [17], [18] theoretically analyzed the Roos' weak key. First, they showed that the equation

$$S^*_{t+1}[t] = \sum_{x=0}^{t}\left(S^*_0[x] + K[x]\right) \tag{3}$$

holds if the following two conditions are satisfied:

```
RC4 KSA:
for $\forall x \in \{0, 1, \dots, N-1\}$
    $S^*[x] \leftarrow x$
end for
$j \leftarrow 0$
for $\forall i \in \{0, 1, \dots, N-1\}$
    $j \leftarrow j + S^*[i] + K[i \bmod l]$
    Swap $S^*[i]$ and $S^*[j]$
end for
```

```
RC4 PRGA:
$i \leftarrow 0$
$j \leftarrow 0$
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 The RC4 algorithm.

Condition 2.1 $S^*_r[r] = r$ for all $r \in \{0, \dots, t\}$ (i.e., the value of $S^*[r]$ was not swapped before the r-th iteration).

Condition 2.2 $S^*_t[j^*_{t+1}] = j^*_{t+1}$.

If j is a random variable, then the probability that the element $S^*_{t+1}[t]$ is assigned the value of $\sum_{x=0}^{t}\left(S^*_0[x] + K[x]\right)$;

$$P\left[S^*_{t+1}[t] = \sum_{x=0}^{t}\left(S^*_0[x] + K[x]\right)\right] \approx \left(\frac{N-1}{N}\right)^{\frac{t(t+1)}{2}} \cdot \left(\frac{N-t}{N}\right) + \frac{1}{N}. \tag{4}$$

From this equation, $S^*_2[1] = K[0] + K[1] + 1$ and $S^*_3[2] = K[0]+K[1]+K[2]+3$ hold with a high probability. Next, they presented the equation $S_0[t] = S^*_{t+1}[t]$ holds if the following condition is satisfied:

Condition 2.3 $j^*_r \neq t$ for all $r \in \{t+1, \dots, N-1\}$

.

If j is a random variable, then the probability that a particular single element of S^*_t will not be indexed by j at any time of the KSA is

$$P\left[S_0[t] = S^*_{t+1}[t]\right] \approx \left(\frac{N-1}{N}\right)^{N-t-1}. \tag{5}$$

From Eqs. (4) and (5), the following equation

$$\begin{aligned} S_0[t] &= \sum_{x=0}^{t}(K[x] + S^*_0[x]) \\ &= \sum_{x=0}^{t} K[x] + \frac{t \cdot (t+1)}{2} \end{aligned} \tag{6}$$

holds for $t = 1, 2$ with the probability

$$P\left[S_0[t] = \sum_{x=0}^{t} K[x] + \frac{t \cdot (t+1)}{2}\right] \approx \left(\frac{N-t}{N}\right) \cdot \left(\frac{N-1}{N}\right)^{\frac{t(t+1)}{2}+N} + \frac{1}{N}. \tag{7}$$

Suppose that $N = 256$. From Eq. (7), the probability that $S_0[1] = K[0] + K[1] + 1$ holds is approximately 0.368 and that $S_0[2] = K[0] + K[1] + K[2] + 3$ holds is 0.362. If a secret key satisfies Eqs. (1) and (2), then $S_0[1] = 0 + 1 = 1$ and $S_0[2] = 0 + X + 3 = X + 3$ hold. Hence, $Z_1 = S_1[S_1[i_1] + S_1[j_1]] = S_1[2] = X + 3$ is output at the 1st round on the PRGA. This probability is approximately $0.368 \cdot 0.362 \approx 2^{-2.9}$.

2.3 Key Recovery Attack from Initial State

Although initial states using Eq. (6) are applied for the key recovery attack in the cases $t = 1, 2$ in [21], Paul and Maitra expanded the attack from the initial state in all cases $t = 0, \ldots, N-1$ in [17], [18], Their attack algorithm needs the information of the initial state as the input and tries to find the correct key. This attack is improved by Biham and Carmeli in [19].

However, their attacks have some faults. First, an adversary must know the information of initial state in advance. In general, it is difficult to observe the initial states. Second, Eq. (6) cannot be used to recover the secret key from the initial state satisfying the following condition[†]:

$$S_0[t] < t \ \text{ for } \ t \in \{0, \ldots, N-1\}. \tag{8}$$

2.4 Predictive State

Fluhrer and McGrew have observed stronger correlations between output streams and the internal states, and introduced the notion as fortuitous state [13]. This is a special class of internal states defined by the values of i_t, j_t, and some state elements of array S at the t-th round, which can predict the output streams. Mantin and Shamir expanded and generalized the notion of fortuitous state as predictive state [14]. The predictive state is defined as follows.

Definision 1: An a-state is a partially specified RC4 states, that includes i_t, j_t and a elements of array S at the t-th round $(S_t[x_1], \ldots, S_t[x_a])$.

Definision 2: Let X_a be a set of internal states that include an a-state and let S_a be an arbitrary internal state in X_a. If every S_a outputs a same sequence of b bytes then a-state is said to be b-predictive.

When $n = 8$, an example of $(b = 4)$-predictive $(a = 4)$-state is given as

$$\begin{cases} S_0[1] = 4, \\ S_0[2] = 1, \\ S_0[3] = 255, \\ S_0[4] = 0, \end{cases} \tag{9}$$
$$i_0 = 0, j_0 = 0.$$

If four elements of the internal state satisfy Eq. (9), the internal state necessarily outputs $Z_1 = 4$, $Z_3 = 4$, $Z_4 = 255$, and $Z_5 = 4$ regardless of the values of other 252 elements. In general, such a b-predictive a-state can induce some biases in the output distribution. Mantin and Shamir [14] proposed a distinguish attack and an internal state recovery attack using the characteristic of predictive state.

In this section, we explain the internal state recovery attack. The existence of b-predictive a-state is important for the cryptanalyst since the information of b elements of the internal state are leaked. If an internal state includes a b-predictive a-state, a elements of S_t and j_t (note that i_t is always available to the cryptanalyst) can be extracted with a non-negligible probability by observing b specific output bytes in the output stream. Let E_{pre} be the event that the internal state includes b-predictive a-state S^A, and E_{out} be the event that b bytes of the output stream are corresponding to that of S^A predicts. If j_t is a random value and S is a random array, then the probability that E_{pre} happens is $((N-a)!/N!) \cdot N^{-1}$ and the probability that E_{out} happens is N^{-b}. Assuming that a is much smaller than N, we can derive the probability $P[E_{pre}|E_{out}]$ by applying Bayes' theorem.

$$\begin{aligned} P[E_{pre}|E_{out}] &= \frac{P[E_{pre}]}{P[E_{out}]} \cdot P[E_{out}|E_{pre}] \\ &\approx \frac{N^{-(a+1)}}{N^{-b}} \cdot 1 \\ &= N^{b-a-1}. \end{aligned} \tag{10}$$

The predictive state tends to satisfy Eq. (8). About 50% of 3-predictive 4-state and about 90% of 4-predictive 5-state satisfy Eq. (8). Moreover, all 3-predictive 3-state, 4-predictive 4-state, and 5-predictive 5-state satisfy Eq. (8). This means that the number of weak keys that satisfy all conditions is very small.

3. Generalization of Weak Key

The class of weak keys presented by Roos is merely a specific case which satisfies the two equations given by Eq. (1) and Eq. (2). We expand the class by generalizing the equations and the number of them using the predictive state proposed by Mantin and Shamir.

3.1 Idea

The two relational equations between the bytes of secret key were proposed by Roos. We generalize the relational equation as follows:

$$\sum_{x=0}^{L-1} w_{x,y} K[x] = W_y, \tag{11}$$

where $w_{x,y} \in \{0, 1\}$, $W_y \in \{0, 1, \ldots, N-1\}$ and $y = 0, 1, 2, \ldots$. For example, in Roos' case,

$$\begin{aligned} \mathbf{w} &= \begin{bmatrix} w_{0,0} & w_{0,1} & w_{0,2} & w_{0,3} & \ldots & w_{0,L-1} \\ w_{1,0} & w_{1,1} & w_{1,2} & w_{1,3} & \ldots & w_{1,L-1} \end{bmatrix} & (12) \\ &= \begin{bmatrix} 1 & 1 & 0 & 0 & \ldots & 0 \\ 1 & 1 & 1 & 0 & \ldots & 0 \end{bmatrix}, & (13) \end{aligned}$$

and

$$\mathbf{W} = \begin{bmatrix} W_0 \\ W_1 \end{bmatrix} \tag{14}$$

[†] The value of the element pointed by i or j is swapped from S_0^* (the case of $i = j$ is excepted, but the probability of the case is very low). For satisfying Condition 2.2, j_{t+1}^* must point the element that has not been pointed by i or j yet. But if the values of elements are less than t at S_0^*, such elements must be pointed by i or j and the values have already been changed (Remember $i = t$ and see the KSA algorithm). Therefore, the values less than i are hardly assigned to $S_{t+1}^*[t]$. In addition, assuming that Condition 2.3 is satisfied, the value of $S_t[t]$ holds till the end of the KSA. If Eq. (8) is satisfied, therefore, Condition 2.2 and 2.3 are not satisfied simultaneously, and Eq. (6) cannot hold.

$$= \begin{bmatrix} 0 \\ X \end{bmatrix}. \tag{15}$$

We try to expand the weak key class using the predictive states. The procedure is divided into three steps. At first, we check if a values of $S^*_{x+1}[x]$ at the KSA can be determined uniquely by given a relational equations whose successful probability is denoted by $P[E_{S_1}]$. Then, we check if the determined a values of $S^*_{x+1}[x]$ can be assigned to a elements of $S_0[x]$ at the PRGA whose successful probability is denoted by $P[E_{S_2}]$. Finally, we check if the assigned a values of $S_0[x]$ can be assigned to a values of $S_t[x]$ that satisfy the condition of a b-predictive a-state whose successful probability is denoted by $P[E_{S_3}]$. If we succeed to operate these three steps, then the output stream must include the information of b relational equations between the bytes of secret key. Thus, the information of b bytes of secret key is leaked with probability $P[leak] = P[E_{S_1}] \cdot P[E_{S_2}] \cdot P[E_{S_3}] + P[rand]$, where $P[rand]$ is the probability that the information leaks by accident.

We define the generalized weak key as follows:

Definision 3: Let $x_1, \ldots, x_a$ be a indices satisfying $0 \leq x_1 \leq \cdots \leq x_a \leq L-1$. Let $S_t[x_1], \ldots, S_t[x_a]$ be a values of a b-predictive a-state, and let $S^*_{x_1+1}[x_1], \ldots, S^*_{x_a+1}[x_a]$ be a values generated by a secret key K_w at the KSA. If $S^*_{x_1+1}[x] = S_t[x]$ is satisfied for all $x \in \{x_1, \ldots, x_a\}$ on the KSA, K_w is in the generalized class of weak key.

3.2 Step 1

We discuss how to derive the relational equations that assign an arbitrary value X_1 to $S^*_{x_1+1}[x_1]$. From the operation of the KSA described in Fig. 1, we can represent the value of $j^*_{x_1+1}$ as follows:

$$\begin{aligned} j^*_{x_1+1} &= j^*_{x_1} + S^*_{x_1}[x_1] + K[x_1] = \ldots \\ &= \sum_{t=0}^{x_1} K[t] + \sum_{t=0}^{x_1} S^*_t[t]. \end{aligned} \tag{16}$$

Remember that the value of $S^*_{x_1}[j^*_{x_1+1}]$ is assigned to $S^*_{x_1+1}[x_1]$. Thus, $X = S^*_{x+1}[x]$ is satisfied if the following equation holds.

$$S^{*\,-1}_{x_1}[X] = j^*_{x_1+1} = \sum_{t=0}^{x_1} K[t] + \sum_{t=0}^{x_1} S^*_t[t] \tag{17}$$

where $S^{*\,-1}_{x_1}[X]$ is the index of the value X in the array S^* in the x_1-th round in the KSA.

From Eq. (17), we derive the relational equation:

$$\sum_{x=0}^{L-1} w_{x,y} K[x] = W_y, \tag{18}$$

where $w_{x,y}$ and W_y are

$$w_{x,y} = \begin{cases} 1 & \text{if } (0 \leq x \leq x_1) \\ 0 & \text{if } (x_1 + 1 \leq x \leq L-1), \end{cases} \tag{19}$$

and

$$W_y = S^{*\,-1}_{x_1}[X_1] - \sum_{t=0}^{x_1} S^*_t[t], \tag{20}$$

respectively. Here X_1 is an arbitrary value and x_1 is an index satisfying $0 \leq x_1 \leq L-1$. If Eqs. (19) and (20) are satisfied, $S^*_{x_1+1}[x_1]$ is always assigned a value X_1.

We assume that a following relational equations for $x' \in \{x_1, x_2, \ldots, x_a\}$ hold in next steps.

$$w_{x,y} = \begin{cases} 1 & \text{if } (0 \leq x' \leq x_1) \\ 0 & \text{if } (x_1 + 1 \leq x' \leq L-1), \end{cases} \tag{21}$$

and

$$W_y = S^{*\,-1}_{x'}[X'] - \sum_{t=0}^{x'} S^*_t[t]. \tag{22}$$

where $X' \in \{X_1, X_2, \ldots, X_a\}$. Unlike Eq. (3), Eq. (22) holds whether Condition 2.1 and 2.2 are satisfied or not. Therefore, X' is always assigned to $S^*_{x'+1}[x']$ for $x' \in \{x_1, x_2, \ldots, x_a\}$, hence $P[E_{S_1}] = 1$.

3.3 Step 2

The value of $S^*_{x+1}[x]$ is unchanged if Condition 2.3 is satisfied. From Eq. (5), the probability that $S^*_{x+1}[x]$ is unchanged until the KSA was finished is approximately $((N-1)/N)^{N-x-1}$.

Let E_{S_1} be the event that satisfies Eqs. (21) and (22). Then, a values of $(X_1, X_2, \ldots, X_a)$ are assigned to a elements of an internal state in the KSA $(S^*_{x_1+1}[x_1], S^*_{x_2+1}[x_2], \ldots, S^*_{x_{a+1}}[x_a])$. Let E_{S_2} be the event that the values of $(X_1, X_2, \ldots, X_a)$ are assigned to a elements of an initial state in the KSA $(S_0[x_1], S_0[x_2], \ldots, S_0[x_a])$. From Eq. (5), we can derive

$$\begin{aligned} P[E_{S_2}] &\approx \left(\frac{N-1}{N}\right)^{N-x_1-1} \cdot \left(\frac{N-1}{N}\right)^{N-x_2-1} \\ &\quad \cdots \cdot \left(\frac{N-1}{N}\right)^{N-x_a-1} \\ &\approx \left(\frac{N-1}{N}\right)^{a\cdot(N-1)-A} \end{aligned} \tag{23}$$

where A is sum of the indices $\{x_1, x_2, \ldots, x_a\}$.

3.4 Step 3

Suppose that a b-predictive a-state at the t-th round $(S_t[x'_1], S_t[x'_2], \ldots, S_t[x'_a])$ and j'_t satisfies following two conditions;

Condition 3.1 $t + 1 = x'_1 < \cdots < x'_a < L$,
Condition 3.2 j'_t does not point $\{x'_1, x'_2, \ldots, x'_a\}$.

Then, we discuss the initial state that generates above predictive state.

(a) $t = 0$

A b-predictive a-state at the 0-th round is represented by $(S_0[1], S_0[x'_2], \ldots, S_0[x'_a])$ and $j'_0 = 0$. It is obvious that a b-predictive a-state at the 0-th round is a part of an initial state. Thus, we can derive $P[E_{S_3}] = 1$.

From Eqs. (21) and (22), we consider that a relational equations for $x' \in \{1, x'_2, \ldots, x'_a\}$ hold and $X' \in \{S_0[1], S_0[x'_2], \ldots, S_0[x'_a]\}$. Then, we can derive

$$P[leak] \approx \left(\frac{N-1}{N}\right)^{a\cdot(N-1)-A} + P[rand], \tag{24}$$

where

$$P[rand] \approx \left(1 - \left(\frac{N-1}{N}\right)^{a\cdot(N-1)-A}\right) \cdot N^{-b}. \tag{25}$$

(b) $t = 1$

A b-predictive a-state at the 1st round is represented by $(S_1[2], S_1[x'_2], \ldots, S_1[x'_a])$ and j'_1. From the operation of the PRGA, $j'_1 = S_0[1]$. Since j'_1 cannot point $\{2, x'_2, \ldots, x'_a\}$ from Condition 3.2, the values of $(S_1[2], S_1[x'_2], \ldots, S_1[x'_a])$ are not swapped at the 1st round. Thus, we can derive $P[E_{out}|E_{ini}] = 1$ where E_{ini} is the event that $a + 1$ elements of an initial state $(S_0[1], S_0[2], S_0[x'_2], \ldots, S_0[x'_a])$ are assigned to $(j'_1, S_1[2], S_1[x'_2], \ldots, S_1[x'_a])$.

In the similar way for $t = 0$, we consider that $a + 1$ relational equations and we can derive

$$P[leak] \approx \left(\frac{N-1}{N}\right)^{(a+1)\cdot(N-1)-A} + P[rand], \tag{26}$$

where

$$P[rand] \approx \left(1 - \left(\frac{N-1}{N}\right)^{(a+1)\cdot(N-1)-A}\right) \cdot N^{-b}. \tag{27}$$

(c) $t \geq 2$

A b-predictive a-state at the t-th round is represented by $(S_t[t+1], S_t[x'_2], \ldots, S_t[x'_a])$ and j'_t. Let j be a random variable. In the similar way for the KSA, the probability that $S_0[x] = S_t[x]$ for $x \in \{t+1, x'_2, \ldots, x'_a\}$ hold is $\left(\frac{N-1}{N}\right)^{a\cdot(t-1)}$, and the probability that $j'_t = j$ is $1/N$. Then, we can derive

$$P[E_{S_3}] \approx \frac{1}{N} \cdot \left(\frac{N-1}{N}\right)^{a\cdot(t-1)}. \tag{28}$$

In the similar way for $t = 1, 2$, we consider a relational equations and we can get

$$P[leak] = P[E_S] + P[rand], \tag{29}$$

where

$$P[E_S] \approx \left(\frac{N-1}{N}\right)^{a\cdot(N-1)-A} \cdot \frac{1}{N} \cdot \left(\frac{N-1}{N}\right)^{a\cdot(t-1)}, \tag{30}$$

and

$$P[rand] \approx (1 - P[E_S]) \cdot N^{-b}. \tag{31}$$

From Eq. (29),

$$\begin{aligned} P[leak] &= P[E_S] + P[rand] && (32)\\ &\approx P[E_S]\left(1 - N^{-b}\right) + N^{-b}. && (33) \end{aligned}$$

3.5 Relationship with Roos' Class

Assuming that the initial state satisfy following conditions;

$$\begin{cases} S_0[1] = 1, \\ S_0[2] = X, \end{cases} \tag{34}$$

then this state always outputs

$$Z_1 = X \tag{35}$$

This implies that the initial state that satisfies Eq. (34) is 1-predictive 2-state at the 0-th round. From Eq. (34), we derive the weak key class

$$\mathbf{w} = \begin{bmatrix} 1 & 1 & 0 & 0 & \ldots & 0 \\ 1 & 1 & 1 & 0 & \ldots & 0 \end{bmatrix}, \tag{36}$$

and

$$\mathbf{W} = \begin{bmatrix} S_1^{*\,-1}[1] - \sum_{t=0}^{1} S_t^*[t] \\ S_2^{*\,-1}[X] - \sum_{t=0}^{2} S_t^*[t] \end{bmatrix}. \tag{37}$$

This class leaks the information of one secret key byte with probability $P[leak] \approx 2^{-2.9}$. If $K[0] \notin \{1, 2, X\}$, this class is equivalent to Roos' class[†] (see Eqs. (13) and (15)). This means that the class of weak keys proposed by Roos is included in the generalized class of weak key. Roos presented some classes of weak keys in appendix of [21] but those are also included in the generalized class of weak keys.

4. Evaluation

The generalized class of weak keys exists on every b-predictive a-state. Thus, we can evaluate the number of generalized classes to enumerate b-predictive a-state. In this section, we present the number of generalized classes of weak keys to enumerate the b-predictive a-state experimentally. Furthermore, we show an example of generalized class that leaks the information of 40 bits of the secret key with a high probability.

[†] If $K[0] \in \{1, 2, X\}$, the information leakage of key bytes does not happen on the class defined by Roos.

Table 1 Number of the classes of weak keys.

a	b	$t = 0$	$t = 1$	$t = 2$	$t = 3$	$t = 4$	$t = 5$	$t = 6$	$t = 7$	$t = 8$	$t = 9$	$t = 10$
2	1	283	9,664	9,156	8,138	7,630	6,612	6,104	5,086	4,578	3,560	3,052
	2	1	3	2	2	2	2	2	2	2	2	2
3	2	69	7,214	3,849	3,602	3,284	3,059	2,473	2,004	1,672	1,447	1,118
	3	0	1	0	0	0	0	0	0	0	0	0
4	2	145,349	2,882,351	2,388,781	2,114,698	1,693,504	1,454,229	1,159,297	1,007,916	766,487	620,566	439,567
	3	1,213	7,411	7,747	7,798	5,806	6,633	5,471	5,027	4,664	4,727	4,355
	4	8	26	29	48	24	26	24	24	24	24	24
5	3	1,049,576	10,442,977	8,860,621	8,075,515	6,171,544	5,508,191	4,098,573	3,538,017	2,479,340	1,725,972	907,819
	4	18,618	72,685	67,019	83,981	44,013	41,237	34,906	30,048	25,625	18,165	9,870
	5	71	275	249	363	142	139	101	99	101	91	79

4.1 Number of Generalized Classes

Paul and Preneel [15] have proposed the algorithm to find the class of a-predictive a-state for small a. We implemented the algorithm to find b-predictive a-state based on the algorithm proposed by Paul et al. This algorithm is described in appendix. We enumerated the number of b-predictive a-state for $n = 8$ experimentally, whose result is shown in Table 1.

We can see that the number of classes of weak keys that satisfies $a = 2$ relational equations and leaks the information of $b = 1$ bytes at $t = 0$ round is 283. Roos' class is included in those. Hence, other numerous number represents the number of classes of weak keys that we discover. If $b \geq 2$, the classes of weak keys leak more information of two bytes of the secret key. From Table 1, thus, most of generalized classes leak more information of the secret key than Roos' class. We show an example of the classes we discover in the following section.

4.2 Experimental Result

In order to confirm the accuracy of the probability evaluation, we carried out the experiment. Before the experiment, we derived the class of weak key from the predictive state which we found in Sect. 4.1. In the experiment, we use 10^9 secret keys in the class of weak key for each a, b, and $t^\dagger$. We enumerated how many keys leak their information and calculated the probability. Table 2 shows the experimental values and the theoretical values for each t when $a = 5$ and $b = 5$. We can see that the theoretical values agree well with the experimental values.

In a similar way, we confirmed that the theoretical values agree well with the experimental values for all a and b. Due to limitation space, we have added only two results when $a = 5$ and $b = 4$ and when $a = 4$ and $b = 4$ to Table 2.

Table 2 The experimentally measured probability that b bytes of the secret key are leaked, where the number enclosed in parentheses stands for the theoretical value ($P[leak]$) and Rands. stands for the probability that b bytes of the secret key are output by accident.

(a, b)	$(5, 5)$	$(5, 4)$	$(4, 4)$
$t = 0$	$2^{-7.09}$ $(2^{-7.12})$	$2^{-7.08}$ $(2^{-7.12})$	$2^{-5.70}$ $(2^{-5.70})$
$t = 1$	$2^{-8.47}$ $(2^{-8.53})$	$2^{-8.50}$ $(2^{-8.53})$	$2^{-7.11}$ $(2^{-7.12})$
$t = 2$	$2^{-15.10}$ $(2^{-15.09})$	$2^{-15.07}$ $(2^{-15.09})$	$2^{-13.75}$ $(2^{-13.68})$
$t = 3$	$2^{-15.06}$ $(2^{-15.09})$	$2^{-15.09}$ $(2^{-15.09})$	$2^{-13.66}$ $(2^{-13.68})$
$t = 4$	$2^{-15.06}$ $(2^{-15.09})$	$2^{-15.07}$ $(2^{-15.09})$	$2^{-13.67}$ $(2^{-13.68})$
$t = 5$	$2^{-15.13}$ $(2^{-15.09})$	$2^{-15.10}$ $(2^{-15.09})$	$2^{-13.70}$ $(2^{-13.68})$
$t = 6$	$2^{-15.08}$ $(2^{-15.09})$	$2^{-15.07}$ $(2^{-15.09})$	$2^{-13.68}$ $(2^{-13.68})$
$t = 7$	$2^{-15.05}$ $(2^{-15.09})$	$2^{-15.09}$ $(2^{-15.09})$	$2^{-13.66}$ $(2^{-13.68})$
$t = 8$	$2^{-15.09}$ $(2^{-15.09})$	$2^{-15.05}$ $(2^{-15.09})$	$2^{-13.69}$ $(2^{-13.68})$
$t = 9$	$2^{-15.09}$ $(2^{-15.09})$	$2^{-15.09}$ $(2^{-15.09})$	$2^{-13.69}$ $(2^{-13.68})$
$t = 10$	$2^{-15.06}$ $(2^{-15.09})$	$2^{-15.09}$ $(2^{-15.09})$	$2^{-13.69}$ $(2^{-13.68})$
Rand.	2^{-40}	2^{-32}	2^{-32}

4.3 Example

We give an example of generalized classes of weak keys for $n = 8$. The algorithm described in appendix finds a 5-predictive 5-state at the 0-th round as follows;

$$\begin{cases} S_0[1] = 1, \\ S_0[2] = 2, \\ S_0[3] = 255, \\ S_0[4] = 254, \\ S_0[5] = 3. \end{cases} \tag{38}$$

An initial state that satisfies Eq. (38) predicts

$$\begin{cases} Z_1 = 2, \\ Z_2 = 1, \\ Z_3 = 2, \\ Z_4 = 1, \\ Z_5 = 3. \end{cases} \tag{39}$$

[†] The parameter A is a different value every class of weak key. The result that we have shown in the paper is carried out under the condition that $A = \sum_{x=t+1}^{t+a+1} x$. We confirmed the theoretical values agree well with the experimental values for other A.

From Eq. (38), we derive the weak key class

$$\mathbf{w} = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & \dots & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & \dots & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & \dots & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & \dots & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & \dots & 0 \end{bmatrix}, \qquad (40)$$

and

$$\mathbf{W} = \begin{bmatrix} S_1^{*\,-1}[1] - \sum_{t=0}^{1} S_t^*[t] \\ S_2^{*\,-1}[2] - \sum_{t=0}^{2} S_t^*[t] \\ S_3^{*\,-1}[255] - \sum_{t=0}^{3} S_t^*[t] \\ S_4^{*\,-1}[254] - \sum_{t=0}^{4} S_t^*[t] \\ S_5^{*\,-1}[3] - \sum_{t=0}^{5} S_t^*[t] \end{bmatrix}. \qquad (41)$$

If combinations of secret key bytes satisfy Eqs. (40) and (41), the secret key leaks 40 bits of that information with probability $P[leak] \approx 2^{-7.1}$ from Eq. (24).

The above result implies that an adversary can get the information of 40 bits of the secret key when he/she observes b bytes of output stream which satisfy Eq. (39). Let E_{key} be the event that combinations of secret key bytes satisfy Eqs. (40) and (41). Let E_{out} be the event that b bytes of output stream which satisfy Eq. (39). We can derive the probability $P[E_{key}|E_{out}]$ by applying Bayes' theorem as follows.

$$\begin{aligned} P[E_{key}|E_{out}] &= \frac{P[E_{key}]}{P[E_{out}]} \cdot P[leak] \\ &\approx \frac{2^{-40}}{2^{-40}} \cdot 2^{-7.1} \\ &\approx 2^{-7.1}. \end{aligned} \qquad (42)$$

As the consequence, an adversary can recover 40 bits of the secret key with probability $2^{-7.1}$. This is the just one example of 71 classes (see Table 1).

On the other hand, this probability of Roos' case is described as follows,

$$\begin{aligned} P[E_{key}|E_{out}] &= \frac{P[E_{key}]}{P[E_{out}]} \cdot P[leak] \\ &\approx \frac{2^{-16}}{2^{-8}} \cdot 2^{-2.9} \\ &\approx 2^{-10.9}. \end{aligned} \qquad (43)$$

As the consequence, an adversary can recover 16 bits of the secret key with probability $2^{-10.9}$.

5. Conclusion

In this paper, we have generalized the class of weak keys on RC4 using b-predictive a-state. The generalized class of weak keys satisfies generalized relational equations between bytes of secret key, and leaks the information of secret key with a high probability. We have shown that the numerous number of generalized classes of weak keys exist among the secret keys. It is revealed that most of them leak more information of the secret key than conventional class of weak keys.

Acknowledgements

We thank anonymous reviewers and Associate Editor Toshinobu Kaneko for their helpful comments. We are deeply grateful to Dr. Minoru Kuribayashi for useful discussions.

References

[1] B. Schneier, Applied Cryptography, Wiley, New York, 1996.

[2] A. Freier, P. Karlton, and P. Kocher, The SSL 3.0 protocol, Netscape Communications, 1996.

[3] Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Computer Society, 1999.

[4] W.F. Alliance, "Wi-fi protected access." http://www.weca.net/opensection/protected_access.asp

[5] S. Fluhrer, I. Mantin, and A. Shamir, "Weaknesses in the key scheduling algorithm of RC4," Proc. SAC2001, LNCS, vol.2259, pp.1–24, Springer-Verlag, 2001.

[6] Korek, "Next generation of WEP attacks?." http://www.netstumbler.org/showpost.php?p=93942&postcount=35

[7] R. Chaabouni, "Break WEP faster with statistical analysis," Tech. Rep., École Polytechnique Fédérale de Lausanne, 2006.

[8] A. Klein, "Attacks on the RC4 stream cipher," Designs, Codes and Cryptography, vol.48, no.3, pp.269–286, 2008.

[9] E. Tews, R.P. Weinmann, and A. Pyshkin, "Breaking 104 bit WEP in less than 60 seconds," Proc. WISA2007, LNCS, vol.4867, pp.188–202, Springer-Verlag, 2008.

[10] S. Vaudenay and M. Vuagnoux, "Passive-only key recovery attacks on RC4," Proc. SAC2007, LNCS, vol.4876, pp.344–359, Springer-Verlag, 2007.

[11] 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.

[12] L.R. Knudsen, W. Meier, B. Preneel, V. Rijmen, and S. Verdoolaege, "Analysis methods for (alleged) RC4," Proc. ASIACRYPT98, LNCS, vol.1514, pp.327–341, Springer-Verlag, 1998.

[13] S. Fluhrer and D. McGrew, "Statiscal analysis of the alleged RC4 keystream generator," Proc. FSE2000, LNCS, vol.1978, pp.19–30, Springer-Verlag, 2001.

[14] I. Mantin and A. Shamir, "A practical attack on broadcast RC4," Proc. FSE2001, LNCS, vol.2355, pp.152–164, Springer-Verlag, 2001.

[15] S. Paul and B. Preneel, "Analysis of non-fortuitous predictive states of the RC4 keystream generator," Proc. INDOCRYPT2003, LNCS, vol.2904, pp.52–67, Springer-Verlag, 2003.

[16] I. Mantin, "Predicting and distinguishing attacks on RC4 keystream generator," Proc. EUROCRYPT2005, LNCS, vol.3494, pp.491–506, Springer-Verlag, 2005.

[17] G. Paul and S. Maitra, "Permutation after RC4 key scheduling reveals the secret key," Proc. SAC2007, LNCS, vol.4876, pp.360–377, Springer-Verlag, 2007.

[18] G. Paul and S. Maitra, "RC4 state information at any stage reveals the secret keys." http://eprint.iacr.org/2007/208.pdf

[19] E. Biham and Y. Carmeli, "Efficient reconstruction of RC4 keys

Table A· 1 Number of the classes of weak keys using Eq. (6).

a	b	$t=0$	$t=1$	$t=2$	$t=3$	$t=4$	$t=5$	$t=6$	$t=7$	$t=8$	$t=9$	$t=10$
2	1	268	9,356	8,601	7,599	6,852	5,860	5,121	4,138	3,645	2,909	2,420
	2	0	2	2	2	2	2	2	2	2	2	2
3	2	32	3,354	3,061	2,795	2,516	2,260	1,969	1,739	1,472	1,228	969
	3	0	0	0	0	0	0	0	0	0	0	0
4	2	73,704	1,765,272	1,415,469	1,205,064	984,517	852,226	695,534	612,728	485,755	395,875	298,993
	3	775	3,912	3,103	3,040	2,997	2,967	2,940	2,935	2,918	2,909	2,894
	4	0	0	0	0	0	0	0	0	0	0	0
5	3	721,737	6,228,513	4,831,342	4,157,951	3,555,290	3,014,843	2,490,721	2,004,433	1,503,338	1,028,981	545,105
	4	4,291	1,933	995	459	228	247	169	217	140	205	117
	5	0	0	0	0	0	0	0	0	0	0	0

from internal states," Proc. FSE2008, LNCS, vol.5086, pp.270–288, Springer-Verlag, 2008.

[20] T. Ohigashi, Y. Shiraishi, and M. Morii, "New weakness in the key-scheduling algorithm of RC4," IEICE Trans. Fundamentals, vol.E91-A, no.1, pp.3–11, Jan. 2008.

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

Appendix A: Algorithm to Find Predictive States

We show that the algorithm to find b-predictive a-state at the t-th round satisfying two conditions in Sect. 3.4. Let a_t be number of the assigned candidates and let b_t be the number of predicted output bytes. As initialization process, suppose that the elements whose indices are $\{x_1, \ldots, x_a\}$ where $x_1 = t + 1$ are marked as "known" and two indices $i_t = t$ and $j_t \in \{0, \ldots, N-1\} \backslash \{x_1, \ldots, x_a\}$. Then the following recursive procedure is forwarded.

Step 1 Increment i_t.

Step 2 It is checked whether $S_{t-1}[i_t]$ has been assigned a value:

(a) if it has, proceed to Step 3.
(b) if it has not, then assign the candidate $2^n - a_t$ remaining values to $S_{t-1}[i_t]$, increment a_t and go to Step 3.

Step 3 Calculate j_t, and it is checked whether $S_{t-1}[j_t]$ has been marked as known:

(a) if it has, proceed to Step 4.
(b) if it has not, swap and update, and go to Step 8.

Step 4 It is checked whether $S_{t-1}[j_t]$ has been assigned a value:

(a) if it has, proceed to Step 5.
(b) if it has not, then assign the candidate $2^n - a_t$ remaining values to $S_{t-1}[j_t]$, increment a_t and go to Step 5.

Step 5 Swap $S_{t-1}[i_t]$ and $S_{t-1}[j_t]$ and update.

Step 6 Calculate $z_t = S_t[i_t] + S_t[j_t]$, and it is check whether $S_t[z_t]$ has been marked as known:

(a) if it has, proceed to Step 7.
(b) if it has not, and go to Step 8.

Step 7 It is checked whether $S_t[z_t]$ has been assigned a value:

(a) if it has, increment b_t and go to Step 8.
(b) if it has not, then assign the candidate $2^n - a_t$ remaining values to $S_{t-1}[j_t]$, increment a_t and b_t and go to Step 8.

Step 8 It is checked whether $S_t[i_t + 1]$ has been marked as known:

(a) if it is, $t \leftarrow t + 1$ and go to Step 1.
(b) if it is not, return.

During above procedure, if two conditions $a_t = a$ and $b_t = b$ are satisfied, then we reverse the PRGA (RC4's PRGA can reverse) and get the b-predictive a-state at the t-th round. Then we can get the class of weak key in the similar way in Sect. 3.

Appendix B: Number of Classes Using Roos' Equation

We enumerated the number of b-predictive a-state satisfying Eq. (8). This number means that of classes of weak key which can be derived by using Eq. (6) instead of Step 1 and Step 2. Table A· 1 shows this result. Comparing Table 1 to Table A· 1, we can see that the number of classes of weak keys derived by the propose method is much larger than that of the method using Roos' equation instead of Step 1 and Step 2.

Ryoichi Teramura received the B.E. and M.E. degrees from Kobe University, Japan, in 2007 and 2009 respectively. Since 2009, he has been a doctoral student in Graduate School of Engineering, Kobe University. His current research interests are in cryptography and information security. He was awarded one of the SCIS2009 paper prizes and the CSS2009 student paper prizes.

Toshihiro Ohigashi received the B.E. and M.E. degrees from the University of Tokushima, Japan, and the D.E. degree from Kobe University in 2002, 2004, and 2008, respectively. Since 2008, he has been an Assistant Professor in Information Media Center, Hiroshima University. His current research interests include information security and cryptography. He received the SCIS 20th Anniversary Award from ISEC group of IEICE in 2003. He is a member of the Information Processing Society of Japan.

Hidenori Kuwakado received the B.E., M.E. and D.E. degrees from Kobe University in 1990, 1992, and 1999, respectively. He worked for Nippon Telegraph and Telephone Corporation from 1992 to 1996. From 1996 to 2002 he was a Research Associate in the Faculty of Engineering, Kobe University. From 2002 to 2007, he was an Associate Professor in the Faculty of Engineering, Kobe University. Since 2007, he has been an Associate Professor in Graduate School of Engineering, Kobe University. His research interests are in cryptography and information security.

Masakatu Morii received the B.E. degree in electrical engineering and the M.E. degree in electronics engineering from Saga University, Saga, Japan, and the 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 Computer 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 and computer networks and information security. He is a member of the IEEE, the Information Processing Society of Japan and the Society of Information Theory and Its Applications.