Multiple Linear Cryptanalysis of a Reduced Round RC6

Takeshi Shimoyama, Masahiko Takenaka, and Takeshi Koshiba

Secure Computing Lab., Fujitsu Laboratories Ltd.,
4-1-1, Kamikodanaka Nakahara-ku Kawasaki 211-8588, Japan
{shimo,takenaka,koshiba}@flab.fujitsu.co.jp

Abstract. In this paper, we apply multiple linear cryptanalysis to a reduced round RC6 block cipher. We show that 18-round RC6 with weak key is breakable by using the multiple linear attack.

1 Introduction

The block cipher RC6 was proposed by Rivest et al. in [17] to meet the requirements of the Advanced Encryption Standard (AES) and is one of the finalists of the AES candidates. It has been admired for its high-level security and high-speed software implementation especially on Intel CPU. RC6 enters also the NESSIE Project selection and it has been nominated to the Phase II evaluation.

RC6 is designed based on the block cipher RC5 [16] which makes essential use of arithmetic key additions and data-dependent rotations. Kaliski and Robshaw [7] evaluated the resistance of RC5, which introduced data-dependent rotations as primitive operations, against Linear Attack [14]. Borst, Preneel, and Vandewalle [2] refined the linear attack of RC5. As additional primitive operations to RC6, the inclusion of arithmetic multiplications and fixed rotations is believed to contribute the strength of the security of RC6. There are some cryptanalyses of RC6: resistance against Differential Attack, Linear Attack, and Related Key Attack by Contini *et al.* [3], Mod n Attack [11], Linear Attack [2], and Statistical Attack [5]. One of most effective attacks is χ^2 attack by Knudsen and Meier [13] which can break up to 15-round RC6 with general keys and 17-round RC6 with weak keys. We note that their estimation is inferred from experimental results for at most 6-round RC6 and is not relied on any theoretical evidence. The cryptanalysis by Contini *et al.* [4] is actually is not only of RC6 itself but also of reduced variants of RC6. We enumerate attacks on RC6 in Table 1.

In [3], Contini *et al.* showed some upper bound of complexity to break RC6 against the linear attack on the assumption that the attacker uses the bias of the linear equations with respect to 1-bit masks both on input and output to arithmetic additive operations and the number of equations among multiple linear approximation, which are derived based on the notion of “linear hulls”, to advantage.

In this paper, we evaluate the resistance of RC6 with 256-bit key against multiple linear attack. In order to do this, we use the technique of the linear

Attack	Rounds	Data size	Comments
Linear Attack [2]	16	2^{119}	Upper bound of complexity
Differential Attack [3]	12	2^{117}	Upper bound of complexity
Mod n Cryptanalysis [11]	—	—	—
χ^2 Cryptanalysis [13]	15	$2^{119.0}$	Lower bound of complexity (estimation)
	17	$\leq 2^{118}$	Lower bound (estimation, $1/2^{80}$ weak keys)
Multiple Linear Attack [This paper]	18	$2^{127.423}$	Lower bound ($1/2^{90}$ weak keys)

Table 1. Attacks on RC6

probability that we obtain by taking multiple paths into account and the theory of multiple linear approximation and evaluate rigorously the complexity to break RC6. To do that, we introduce a novel technique to use a "Matrix Representation" that is a generalization of the piling up lemma to obtain the linear probability. This technique ease us to count the multiple path and to estimate more exactly the linear probability that might depend on the extended-keys. As a result, we show that the target key of 14-round RC6 can be recovered and also that the target key of 18-round RC6 with weak keys, which exists with probability $1/2^{90}$ at least, can be recovered.

2 Preliminary

For any function $Y = F(X)$, input mask ΓX and output mask ΓY, we define the bias of linear equations $Bias_F()$ and the linear probability $LP_F()$ as follows.

$$Bias_F(\Gamma X \to \Gamma Y) = 2 \cdot \frac{\#\{X|(\Gamma X \cdot X)\oplus(\Gamma Y \cdot F(X)) = 0\}}{\#\{X\}} - 1$$
$$LP_F(\Gamma X \to \Gamma Y) = (Bias_F(\Gamma X \to \Gamma Y))^2$$

It is well known that for any r functions $X_{i+1} = F_i(X_i)$ $(i = 1, ..., r)$ the composite function $H(X) = F_r \circ \cdots \circ F_1(X)$ has the expected (w.r.t. keys) linear probability satisfying[1]

$$LP_H(\Gamma X_1 \to \Gamma X_{r+1}) = \sum_{\Gamma X_2,...,\Gamma X_r} \{\prod_{i=1}^{r} LP_{F_i}(\Gamma X_i \to \Gamma X_{i+1})\}.$$

Let $e_0, ..., e_{31}$ denote unit vectors over $GF(2)^{32}$ such that the ith element of e_i is 1 and the other elements of e_i are 0. Here we adopt the description of the descending order for vectors (e.g., $e_0 = (0, ..., 0, 1)$).

In this paper, we identify 32-bit values, which are used in RC6 encryption, with elements of $GF(2)^{32}$, unless otherwise specified.

[1] Strictly speaking, we need more structural information of functions F_i for holding the equation.

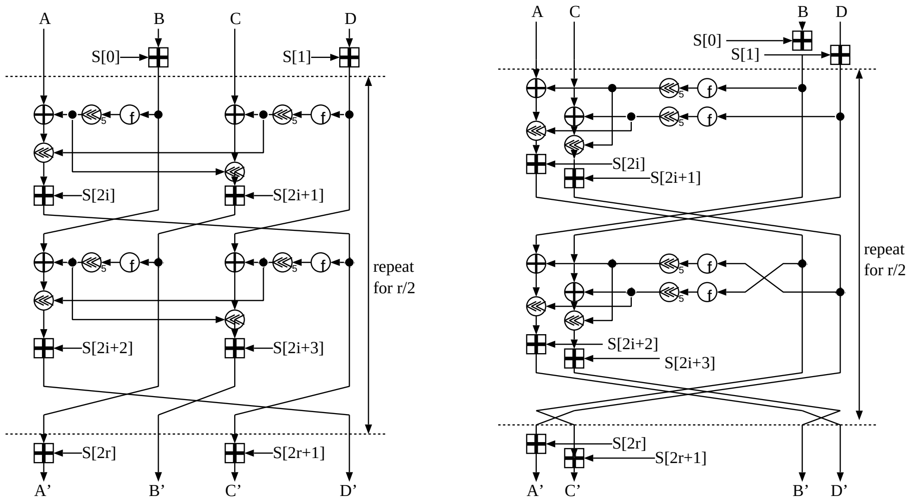

Fig. 1. Original RC6 and its equivalent transformation

3 RC6 and Its Equivalent Transformation

RC6 is a block cipher proposed by Rivest *et al.* [17]. It has a variable number of rounds denoted r and key size of $8b$ bits. The design is word-oriented for word sizes w and the block size is $4w$. Currently RC6 with $r = 20$, $4w = 128$ and $8b = 128, 192, 256$ is recommended to give sufficient resistance against possible attacks. (See Figure 1). In this paper, we refer n-round RC6 to RC6$_{(n)}$. We leave the key scheduling of RC6, which generates extended keys from private keys, out of consideration.

In this paper, we use a Feistel-like description of RC6 which is obtained by exchanging input-output words B and C equivalently. It is easy to see that the new description help us to capture structural properties of RC6. (As long as the authors know, the new description is not shown.)

We consider a block cipher RC6⊕ that is obtained by replacing arithmetic additions of extended-keys of RC6 by exclusive-oring of extended-keys.

Moreover, we consider weak-keys of $2r$-round RC6. We define two types of weak keys. "Type I weak keys" are ones such that $lsb_5(S[4i-3]) = lsb_5(S[4i-4]) = 0$, and "Type II weak keys" are ones such that $lsb_4(S[4i-3]) = lsb_4(S[4i-4]) = 0$. It is easy to see that Type I weak-keys is of the fraction 2^{-10r}, and Type II weak-keys is of the fraction 2^{-8r}. Later, we will show that those of weak-keys are actually "weak".

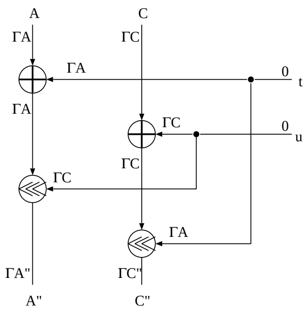

Fig. 2. Linear mask of R

4 Linear Probabilities of Data-Dependent Rotation

We consider a partial function R of $RC6$ as follows. (See also Figure 2).

$$R : (A, C, t, u) \in (GF(2)^{32})^4 \to (A'', C'') \in (GF(2)^{32})^2.$$
$$A'' = (A \oplus t) \lll u$$
$$C'' = (C \oplus u) \lll t$$

Let $\Gamma A, \Gamma C, \Gamma t, \Gamma u, \Gamma A'', \Gamma A''$ be masks for the variables A, C, t, u, A'', C'' of R, respectively. We consider linear approximation with significant linear probability such that $\Gamma t = \Gamma u = 0$.

Let us consider, for example, the case where $\Gamma A = \Gamma C = \Gamma A'' = \Gamma C'' = e_0$. Then, if $lsb_5(t) = lsb_5(u) = 0$ then $Ae_0 \oplus A''e_0 = 0$ and $Ce_0 \oplus C''e_0 = 0$. Only if the case where $lsb_5(t) = lsb_5(u) = 0$ occurs (its probability is 2^{-10}), the probability that the equation $Ae_0 \oplus Ce_0 \oplus A''e_0 \oplus C''e_0 = 0$ holds is biased. Thus, we have

$$LP_R((e_0, e_0, 0, 0) \to (e_0, e_0)) = 2^{-20}.$$

Similarly, we obtain the following equations for $i, j, k, l \in \{0, 1, 2, 3, 4\}$

$$LP_R((e_i, e_j, 0, 0) \to (e_k, e_l)) = 2^{-20}.$$

5 Linear Probability of RC6 with weak keys

In this section, we consider the linear probability of $2r$-round RC6 with Type II weak keys by taking "multiple paths". In general, the linear characteristic probability depends on the key-value. Here, for simplicity, we consider RC6⊕. We assume that key is randomly distributed. In the case that the least significant five bits of extended-key related to linear approximation is fixed (especially, in the case of weak-keys), we can calculate the precise linear probability for each linear approximation. We will discuss how to calculate it in Section 7.

round	output mask of (A, C)
0	(e_i, e_j)
	$\swarrow$ ... $\searrow$
2	(e_0, e_0) .... (e_4, e_4)
	$\searrow$ ... $\swarrow$
4	(e_k, e_l)
LP	2^{-40} ... 2^{-40}

Table 2. 4-round multiple linear path of RC6⊕

Let us consider 4-round RC6⊕. If we set the input mask for (A, C) being (e_i, e_j) $(i, j \in \{0, ..., 4\})$ and its output mask being (e_k, e_l) $(k, l \in \{0, ..., 4\})$, then for any $i, j, s, t \in \{0, ..., 4\}$ the following holds:

$$|Bias_R((e_i, e_j, 0, 0) \rightarrow (e_s, e_t))| = 2^{-10}.$$

Thus we can show that the absolute value of linear characteristic per path of 4-round RC6⊕ is 2^{-40} by the piling up lemma in average of the key.

Since there exist at least $25 = 5^2$ linear characteristic paths such that input mask (e_i, e_j) and output mask (e_k, e_l) are equal but any other intermediate masks are different from the input mask, we can calculate linear characteristic over multiple paths. (See Table 2.)

$$\begin{aligned} & LP_{RC6\oplus_{(4)}}((e_0, e_0, 0, 0) \rightarrow (e_0, e_0, 0, 0)) \\ & = \sum_{s,t} LP_R((e_0, e_0) \rightarrow (e_s, e_t)) LP_R((e_s, e_t) \rightarrow (e_0, e_0)) \\ & = 25 \cdot (2^{-40}) = 2^{-35.356} \end{aligned}$$

Moreover, the linear probability of $2r$-round RC6⊕ is derived as follows.

$$\begin{aligned} LP_{RC6\oplus_{(2r)}}&((e_i, e_j, 0, 0) \rightarrow (e_k, e_l, 0, 0)) \\ & \geq 2^{-20}(25 \cdot (2^{-20}))^{r-1} \\ & = 2^{-20-15.356(r-1)} \end{aligned}$$

It is easy to consider the linear approximation of $(2r + 1)$-round RC6⊕ from the linear approximation of $2r$-round RC6⊕ obtained above. (See Table 3.)

Next, we consider Type II weak-keys of RC6. It is easy to see that if $lsb_4(K) = 0$ then arithmetic addition of some fixed 32-bit value K (say, $Y = X + K \bmod 2^{32}$) does not cause any carry-over in the least significant 5 bits. In this case, the equation $LP_{add_K}(e_i \rightarrow e_i) = 1$ always holds for $i \in \{0, ..., 4\}$. Such keys can be generated with probability 2^{-4} if K is randomly distributed.

This implies that the linear probability of RC6 with weak key of Type II is independent of keys. Thus, we can say that the resistance of RC6 with such keys against multiple linear attack is reduced to the one of RC6⊕ against multiple linear attack. In this sense, we can regard such keys as weak ones. (For example, some weak keys of 3-round RC6 are characterized as ones with least significant four bits each of $S[0], S[1], S[4], S[5]$ is 0. So, the fraction of such weak keys is 2^{-16}.)

round	input mask	output mask	linear probability ($\log_2$)	fraction of weak keys of RC6
3	$(0,0,e_i,e_j)$	$(e_k,e_l,0,0)$	-20.000	2^{-16}
5	$(0,0,e_i,e_j)$	$(e_k,e_l,0,0)$	-35.356	2^{-24}
7	$(0,0,e_i,e_j)$	$(e_k,e_l,0,0)$	-50.712	2^{-32}
9	$(0,0,e_i,e_j)$	$(e_k,e_l,0,0)$	-66.068	2^{-40}
11	$(0,0,e_i,e_j)$	$(e_k,e_l,0,0)$	-81.424	2^{-48}
13	$(0,0,e_i,e_j)$	$(e_k,e_l,0,0)$	-96.780	2^{-56}
15	$(0,0,e_i,e_j)$	$(e_k,e_l,0,0)$	-112.136	2^{-64}
17	$(0,0,e_i,e_j)$	$(e_k,e_l,0,0)$	-127.492	2^{-72}

Note that i,j,k,l range over $\{0,...,4\}$.

Table 3. The linear probability of RC6 with Type II weak keys (or RC6⊕)

Input mask $(\Gamma A, \Gamma C)$	(e_i,e_j), $i,j \in \{0,...,4\}$			
Output mask $(\Gamma A', \Gamma C')$	(e_0,e_0)	(e_k,e_0)	(e_0,e_l)	(e_k,e_l)
Linear prob. of addition	1	2^{-2}	2^{-2}	2^{-4}
Linear prob. of 1-round RC6	2^{-20}	2^{-22}	2^{-22}	2^{-24}

Note that $k \neq 0, l \neq 0$.

Table 4. The linear probability of 2-round RC6

6 Linear Probability of RC6

There are several researches about success probability of linear approximation for arithmetic addition $Y = X + K$ on the assumption that K is randomly chosen but fixed ([7, 10, 15, 4]). In this paper, we consider linear approximation only of the form $Xe_i \oplus Ye_i = 0$, which is a relation between a 1-bit of input and a 1-bit of output. Let us see it more precisely.

It is well known that the expectation (w.r.t. keys) of the bias of linear equations satisfies that $LP_{add_K}(e_0 \to e_0) = 1$, and $LP_{add_K}(e_i \to e_i) = 2^{-2}, (i \neq 0)$ on the average of K. By utilizing these equations, it is easy to calculate the linear probability of 2-round RC6 with the key addition. We note that the linear probability of key addition can be obtained only from output masks. The linear probability of 2-round RC6 follows from the linear probability of addition, the linear probability of 1-round RC6⊕, obtained in the previous section, and the piling up lemma. (See Table 4.)

Any output mask $(\Gamma A', \Gamma C')$ corresponds with one of $(e_0,e_0), (e_k,e_0), (e_0,e_l)$ and (e_k,e_l). The number of output masks of each type is $1, 4, 4$ and 16, respectively. Thus we have the linear probability of 4-round RC6 over multiple paths such that the input mask is of the form $(e_i,e_j,0,0)$ and the output mask is of the form $(e_0,e_0,0,0)$ as follows.

$$
\begin{aligned}
&LP_{RC6_{(4)}}((e_i,e_j,0,0) \to (e_0,e_0,0,0)) \\
&= 2^{-20}(2^{-20} + 4 \cdot 2^{-22} + 4 \cdot 2^{-22} + 16 \cdot 2^{-24}) \\
&= 2^{-38}
\end{aligned}
$$

round	input mask (A, C, B, D)	output mask (A',C',B',D')	linear probability ($\log_2$)
3	$(0, 0, e_i, e_j)$	$(e_k, e_l, 0, 0)$	$-20 - 2\mu(\{i, j, k, l\})$
5	$(0, 0, e_i, e_j)$	$(e_k, e_l, 0, 0)$	$-38 - 2\mu(\{i, j, k, l\})$
7	$(0, 0, e_i, e_j)$	$(e_k, e_l, 0, 0)$	$-56 - 2\mu(\{i, j, k, l\})$
9	$(0, 0, e_i, e_j)$	$(e_k, e_l, 0, 0)$	$-74 - 2\mu(\{i, j, k, l\})$
11	$(0, 0, e_i, e_j)$	$(e_k, e_l, 0, 0)$	$-92 - 2\mu(\{i, j, k, l\})$
13	$(0, 0, e_i, e_j)$	$(e_k, e_l, 0, 0)$	$-110 - 2\mu(\{i, j, k, l\})$

Note that $i, j, k, l \in \{0, ..., 4\}$, $\mu(X) = \#\{x \neq 0 | x \in X\}$.

Table 5. The linear probability of RC6

Similarly, we have the linear probability of $2r$-round RC6 over the same multiple paths as follows.

$$LP_{RC6_{(2r)}}((e_i, e_j, 0, 0) \to (e_0, e_0, 0, 0)) \geq 2^{-20-18(r-1)}$$

Furthermore, we have the linear probability of $2r$-round RC6 over multiple paths of the other types.

$$LP_{RC6_{(2r)}}((e_i, e_j, 0, 0) \to (e_k, e_0, 0, 0)) \geq 2^{-22-18(r-1)}$$
$$LP_{RC6_{(2r)}}((e_i, e_j, 0, 0) \to (e_0, e_l, 0, 0)) \geq 2^{-22-18(r-1)}$$
$$LP_{RC6_{(2r)}}((e_i, e_j, 0, 0) \to (e_k, e_l, 0, 0)) \geq 2^{-24-18(r-1)}$$

By utilizing the linear approximation of $2r$-round RC6, it is not hard to consider the linear approximation of $2r + 1$-round RC6, We note that the linear probability is affected by the extended-key that is added to input data B and D to the first round. Namely, we have to take into account that the linear probability depends on the bit position of the input mask. We illustrate an estimation of the linear probability of reduced-round RC6 in Table 5.

7 Linear Probability of a Fixed Key

In this section, we give a way to calculate the more precise linear probability of the linear approximation $Ae_i \oplus Ce_j \oplus A'e_k \oplus C'e_l = 0$ for RC6 with any fixed key. In Section 5 and Section 6, we calculated the linear probability in average of keys.

On the other hand, especially as in the case of Type I weak keys, that is the least significant five bits of the extended key is 0, then, by keeping the sign of the bias of linear equation in mind when summing the bias of linear equation, we can generalize the piling up lemma to calculate the bias of linear equation more precisely.

Now, we consider the linear probability of RC6 with Type I weak key. For a simpler exposition, we calculate the linear probability of 4-round RC6 with the weak keys such that the input and the output mask are both $(e_0, e_0, 0, 0)$. We show the bias of each linear characteristic in Table 6. For example, the linear characteristic for paths from the 0th round through the second round to the

Input mask	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
1st R. Bias ($\times 2^{-10}$)	1	-1	1	-1	1	-1	1	-1	1	-1	1	-1	1	-1	1	-1	1	-1	1	-1	1	-1	1	-1	1
2nd R. mask	00	01	02	03	04	10	11	12	13	14	20	21	22	23	24	30	31	32	33	34	40	41	42	43	44
3rd R. Bias ($\times 2^{-10}$)	1	-1	1	-1	1	-1	1	1	-1	-1	1	1	1	1	1	-1	-1	1	1	1	1	-1	1	1	1
Output mask	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
Total Bias ($\times 2^{-20}$)	1	1	1	1	1	1	1	-1	-1	1	1	-1	1	-1	1	1	-1	-1	1	-1	1	1	1	-1	1

Table 6. The bias of linear characteristic path such that the input and output masks are both $(e_0, e_0, 0, 0)$ (4-round RC6 with Type I weak key)

Input	Output Mask (k, l)																								
(i, j)	00	01	02	03	04	10	11	12	13	14	20	21	22	23	24	30	31	32	33	34	40	41	42	43	44
00	1	-1	1	-1	1	-1	1	-1	1	-1	1	-1	1	-1	1	-1	1	-1	1	-1	1	-1	1	-1	1
01	-1	1	-1	1	-1	-1	1	-1	1	-1	1	-1	1	-1	1	1	-1	1	-1	1	-1	1	-1	1	-1
02	1	-1	1	-1	1	1	-1	1	-1	1	1	-1	1	-1	1	1	-1	1	-1	1	-1	1	-1	1	-1
03	-1	1	-1	1	-1	-1	1	-1	1	-1	-1	1	-1	1	-1	-1	1	-1	1	-1	-1	1	-1	1	-1
04	1	-1	1	-1	1	1	-1	1	-1	1	1	-1	1	-1	1	1	-1	1	-1	1	1	-1	1	-1	1
10	-1	-1	1	1	-1	1	1	-1	-1	1	-1	-1	1	1	-1	1	1	-1	-1	1	-1	-1	1	1	-1
11	1	-1	-1	1	1	-1	1	1	-1	-1	-1	1	1	-1	-1	1	-1	-1	1	1	1	-1	-1	1	1
12	1	1	-1	-1	1	-1	-1	1	1	-1	-1	-1	1	1	-1	-1	-1	1	1	-1	-1	-1	1	1	-1
13	-1	1	1	-1	-1	1	-1	-1	1	1	1	-1	-1	1	1	1	-1	-1	1	1	1	-1	-1	1	1
14	-1	-1	1	1	-1	1	1	-1	-1	1	1	1	-1	-1	1	1	1	-1	-1	1	1	1	-1	-1	1
20	1	1	1	1	-1	-1	-1	-1	-1	1	1	1	1	1	-1	-1	-1	-1	-1	1	1	1	1	1	-1
21	1	-1	-1	-1	-1	1	-1	-1	-1	-1	-1	1	1	1	1	-1	1	1	1	1	1	-1	-1	-1	-1
22	1	1	-1	-1	-1	1	1	-1	-1	-1	-1	-1	1	1	1	-1	-1	1	1	1	-1	-1	1	1	1
23	1	1	1	-1	-1	1	1	1	-1	-1	-1	-1	-1	1	1	-1	-1	-1	1	1	-1	-1	-1	1	1
24	1	1	1	1	-1	1	1	1	1	-1	-1	-1	-1	-1	1	-1	-1	-1	-1	1	-1	-1	-1	-1	1
30	-1	-1	-1	-1	-1	1	1	1	1	1	-1	-1	-1	-1	-1	1	1	1	1	1	-1	-1	-1	-1	-1
31	-1	1	1	1	1	1	-1	-1	-1	-1	1	-1	-1	-1	-1	-1	1	1	1	1	-1	1	1	1	1
32	1	1	-1	-1	-1	1	1	-1	-1	-1	1	1	-1	-1	-1	-1	-1	1	1	1	-1	-1	1	1	1
33	1	1	1	-1	-1	1	1	1	-1	-1	1	1	1	-1	-1	-1	-1	-1	1	1	-1	-1	-1	1	1
34	1	1	1	1	-1	1	1	1	1	-1	1	1	1	1	-1	-1	-1	-1	-1	1	-1	-1	-1	-1	1
40	1	1	1	1	1	-1	-1	-1	-1	-1	1	1	1	1	1	-1	-1	-1	-1	-1	1	1	1	1	1
41	-1	1	1	1	1	-1	1	1	1	1	1	-1	-1	-1	-1	1	-1	-1	-1	-1	-1	1	1	1	1
42	1	1	-1	-1	-1	1	1	-1	-1	-1	1	1	-1	-1	-1	1	1	-1	-1	-1	-1	-1	1	1	1
43	1	1	1	-1	-1	1	1	1	-1	-1	1	1	1	-1	-1	1	1	1	-1	-1	-1	-1	-1	1	1
44	1	1	1	1	-1	1	1	1	1	-1	1	1	1	1	-1	1	1	1	1	-1	-1	-1	-1	-1	1

Table 7. Matrix M of the bias $(\times 2^{-10})$ of linear equations for 2-round RC6 with weak key

fourth round trace $(e_0, e_0) \to (e_1, e_1) \to (e_0, e_0)$ is $(-2^{-10}) \cdot (-2^{-10}) = +2^{-20}$. The number of linear characteristic for paths through $(e_s, e_t, 0, 0)$ in the second round is totally $5^2 = 25$. Among them, there are 17 positive $(= 2^{-10})$ bias of linear characteristics and 8 negative $(= -2^{-10})$ bias of linear characteristics. By taking account of the sign of linear characteristic of each path, we obtain the linear characteristic and the linear probability as follows. (The validity of this observation is demonstrated by computer experiments.)

$$\begin{aligned} &Bias_{RC6(\text{Type I weak key})}((e_0, e_0, 0, 0) \to (e_0, e_0, 0, 0)) \\ &\qquad\qquad\qquad = (17 - 8) \cdot (2^{-10} 2^{-10}) = 2^{-16.83} \\ &LP_{RC6(\text{Type I weak key})}((e_0, e_0, 0, 0) \to (e_0, e_0, 0, 0)) = 2^{-33.66} \end{aligned}$$

We note that linear probability obtained here is much higher than the linear probability of RC6 with average keys (2^{-38}) and of RC6⊕ $(2^{-35.356})$.

Next, we generalize the above method to calculate precisely the linear probability of the input mask and the output mask pattern $(e_i, e_j, 0, 0) \to (e_k, e_l, 0, 0)$ for $2r$-round RC6 with Type I weak key.

For $i, j, k, l \in \{0, ..., 4\}$, let $m = (k - i)(\text{mod}32), n = (l - j)(\text{mod}32)$. We consider the 25×25 matrix $M = (a_{(ij)(kl)})$ such that $a_{(ij)(kl)} = (-1)^{n \cdot e_i \bigoplus m \cdot e_j}$.

lsb_5	k_4	k_3	k_2	k_1	k_0	lsb_5	k_4	k_3	k_2	k_1	k_0	lsb_5	k_4	k_3	k_2	k_1	k_0	lsb_5	k_4	k_3	k_2	k_1	k_0
0	16	16	16	16	16	8	0	-16	16	16	16	16	-16	16	16	16	16	24	0	-16	16	16	16
1	14	12	8	0	-16	9	-2	-12	8	0	-16	17	-14	12	8	0	-16	25	2	-12	8	0	-16
2	12	8	0	-16	16	10	-4	-8	0	-16	16	18	-12	8	0	-16	16	26	4	-8	0	-16	16
3	10	4	-8	0	-16	11	-6	-4	-8	0	-16	19	-10	4	-8	0	-16	27	6	-4	-8	0	-16
4	8	0	-16	16	16	12	-8	0	-16	16	16	20	-8	0	-16	16	16	28	8	0	-16	16	16
5	6	-4	-8	0	-16	13	-10	4	-8	0	-16	21	-6	-4	-8	0	-16	29	10	4	-8	0	-16
6	4	-8	0	-16	16	14	-12	8	0	-16	16	22	-4	-8	0	-16	16	30	12	8	0	-16	16
7	2	-12	8	0	-16	15	-14	12	8	0	-16	23	-2	-12	8	0	-16	31	14	12	8	0	-16

Table 8. The bias ($\times 2^{-4}$) of linear equation for addition(+)

(See Table 7.) Then, the bias of linear equation of $2r$-round RC6 with Type I weak key can be calculated as follows.

$$\Phi^{(r)} = 2^{-10r} M^r,$$
$$Bias_{RC6(\text{Type I weak key})_{(2r)}}((e_i, e_j, 0, 0) \to (e_k, e_l, 0, 0)) = \Phi^{(r)}{}_{(ij)(kl)},$$

where M^r means the exponentiation of the integer matrix M.

In case of RC6 with arbitrary key, for the least significant five bits of extended key $lsb_5(S[4i-2])$, $lsb_5(S[4i-1])$, we calculate (k_{i4}, k_{i3}, k_{i2}, k_{i1}, k_{i0}) and (h_{i4}, h_{i3}, h_{i2}, h_{i1}, h_{i0}) by using Table 8, and also calculate the following matrix.

$$K_i = diag(k_{i0}h_{i0}, k_{i0}h_{i1}, ..., k_{i4}h_{i4}),$$

where $diag(a_0, a_1, ...)$ is the 25×25 matrix whose diagonal elements are $a_0, a_1, ...$ and other elements are all 0. For example, when $lsb_5(S[2]) = 4$ and $lsb_5(S[3]) = 26$, then K_1 is calculated as follows.

$$K_1 = diag(2^{-3}, -2^{-2}, 0, -2^{-1}, 2^{-1}, 0, 0, 0, 0, 0, -2^{-2}, 2^{-1}, ..., -1, 1)$$

Then, the bias of linear equation of $2r$-round RC6 can be calculated by using a "Generalized Piling up lemma" of matrix representation as follows.

$$Bias_{RC6_{(2r)}}((e_i, e_j, 0, 0) \to (e_k, e_l, 0, 0))$$
$$= \Psi^{(r)}[K]_{(ij)(kl)}$$
$$\Psi^{(r)}[K] = \prod_{i=1}^{r} (2^{-10} M \cdot K_i)$$

Table 9 shows linear masks that take the maximum linear probability of RC6 with Type I weak key in the elements of 25×25 matrix calculated as above. Now, we can get the maximal linear probability of $(2r+1)$-round RC6 with the weak keys by combining the discussion in the case of $2r$-round RC6 and one-round addition to the input side.

8 Multiple Linear Approximation of RC6

"Multiple Linear Approximation", which is proposed by Kaliski and Robshaw, is a technique to enable to attack ciphers using less amount of data. This technique

Rounds	Input Mask (i,j)	Output Mask (k,l)	Bias	LP	comment
3	(*,*)	(*,*)	$1 \cdot 2^{-10}$	2^{-20}	1 in 2^{20}
5	(3,8)	(2,2)	$21 \cdot 2^{-20}$	$2^{-31.214}$	1 in 2^{30}
7	(1,1)	(3,3)	$101 \cdot 2^{-30}$	$2^{-46.682}$	1 in 2^{40}
9	(1,1)	(0,0)	$633 \cdot 2^{-40}$	$2^{-61.386}$	1 in 2^{50}
11	(1,1)	(2,2)	$4449 \cdot 2^{-50}$	$2^{-75.760}$	1 in 2^{60}
13	(2,2)	(2,2)	$24798 \cdot 2^{-60}$	$2^{-90.804}$	1 in 2^{70}
15	(2,2)	(0,0)	$134645 \cdot 2^{-70}$	$2^{-105.922}$	1 in 2^{80}
17	(2,2)	(0,0)	$942657 \cdot 2^{-80}$	$2^{-120.306}$	1 in 2^{90}

Table 9. The maximum linear probability of RC6 with Type I weak key

linear approximation	linear probability	number
$Be_0 \oplus De_0 \oplus A'e_0 \oplus C'e_0 = 0$	$2^{-20-18(r-1)}$	1
$Be_i \oplus De_0 \oplus A'e_0 \oplus C'e_0 = 0$	$2^{-22-18(r-1)}$	4
$Be_0 \oplus De_j \oplus A'e_0 \oplus C'e_0 = 0$	$2^{-22-18(r-1)}$	4
$Be_0 \oplus De_0 \oplus A'e_k \oplus C'e_0 = 0$	$2^{-22-18(r-1)}$	4
$Be_0 \oplus De_0 \oplus A'e_0 \oplus C'e_l = 0$	$2^{-22-18(r-1)}$	4

Table 10. Linear approximations of $2r$-round RC6 for multiple linear approximation

is quite effective if there exist several linear approximations that have almost maximum linear probability.

Let ϵ_i be the bias of linear equation $L_i : X\Gamma_{X_i} \oplus Y\Gamma_{Y_i} = 0$, $(i = 1, ..., n)$ with respect to $Y = F(X)$. Then we define *weight* according to ϵ_i as being $w_i = \epsilon_i/(\epsilon_0 + ... + \epsilon_n)$. Let N be the number of known plaintexts and N_i the number of known plaintexts that satisfy linear approximation L_i. Then by utilizing the difference between $w_i N_i$ and $N/2$ it is not hard to distinguish a cipher from random permutations. The necessary number N of known plaintexts to distinguish a cipher from random permutations is $C/(\sum_{i=1}^{n} \epsilon_i^2)$, where C is a parameter which determines the success probability (e.g., $C = 4$ implies that the success probability is 95%).

By careful consideration of multiple linear approximation, we can see that it is sufficient for estimating necessary number of plaintexts to break a cipher that we get linear approximations whose linear equations are linearly independent. Recall the linear approximations which are discussed in the previous section. The linear approximations we should consider are all of the form $Be_i \oplus De_j \oplus A'e_k \oplus C'e_l = 0$. It is not difficult to see that there are at most 17 linearly independent linear approximations. We utilize 17 linear approximations (shown in Table 10), which are linearly independent and whose linear probabilities are comparatively high, in order to improve the efficiency of breaking RC6.

We estimate the necessary number N of plaintexts to distinguish RC6 from random permutations by applying linear approximations shown in Table 10 to the technique of multiple linear approximation. We note that the coefficients in the equations below are introduced in order to increase the success probability up to 95%.

round	RC6	RC6(Type II weak key)	RC6(Type I weak key)
3	$2^{21.68}$	$2^{17.912}$ (1 in 2^{16})	$2^{17.912}$ (1 in 2^{20})
5	$2^{39.68}$	$2^{33.268}$ (1 in 2^{24})	$2^{30.1261}$ (1 in 2^{30})
7	$2^{57.68}$	$2^{48.624}$ (1 in 2^{32})	$2^{45.712}$ (1 in 2^{40})
9	$2^{75.68}$	$2^{63.980}$ (1 in 2^{40})	$2^{60.260}$ (1 in 2^{50})
11	$2^{93.68}$	$2^{79.336}$ (1 in 2^{48})	$2^{75.111}$ (1 in 2^{60})
13	$2^{111.68}$	$2^{94.692}$ (1 in 2^{56})	$2^{90.061}$ (1 in 2^{70})
15	$2^{129.68}$	$2^{110.048}$ (1 in 2^{63})	$2^{104.701}$ (1 in 2^{80})
17	$2^{147.68}$	$2^{125.404}$ (1 in 2^{70})	$2^{119.423}$ (1 in 2^{90})
19	$2^{165.68}$	$2^{140.760}$ (1 in 2^{78})	$2^{134.227}$ (1 in 2^{100})

Table 11. Distinguishing attack of RC6

$$\begin{aligned} N &= 4 \cdot (1/(2^{-20-18(r-1)} + 16 \cdot 2^{-22-18(r-1)})) \\ &= 4 \cdot 1/((1+2^{-2}) \cdot 2^{-18r}) = 2^{3.68+18r} \end{aligned}$$

Similarly, we estimate the necessary number N of plaintexts to distinguish RC6⊕ (or RC6 with Type II weak key) from random permutations by seeing Table 3.

$$N = 4/(17 \cdot 2^{-20-15.356(r-1)}) = 2^{2.556+(15.356)r}$$

Moreover, in case of RC6 with Type I weak key, we can pick up linearly independent 17 linear approximations according to the estimation for the linear probability of each input-output masks in Section 8.

Our attacking method, described in this section, is a known plaintext attack. It means that we do not restrict the form of inputs and thus that we can make full use of inputs, that is, the number 2^{128} of plaintexts. Therefore, we can say that 13-round RC6 is distinguishable from random permutations and also that 15-round RC6⊕, 17-round RC6 with weak keys whose fraction is 2^{-90} is distinguishable from random permutations. We summarize these results in Table 11.

9 Key Recovery of RC6

In this section, we consider the key recovery of $(2r+2)$-round RC6 by utilizing the distinguishability result of $(2r+1)$-round RC6. We adopt a typical method "1-round elimination attack" as same as the method by Knudsen and Meier [13] for key recovery in the following: apply multiple linear approximation to RC6 through the 2nd round to the $2r+2$th round, search exhaustively for the extended key $S[0], S[1]$ (64 bits in total), and use them and the value in the position before key addition of the first round to find a target key. (See Figure 3.)

Since the necessary data size for distinguishing attacker to success the attack is $4p^{-1}$ with probability 95%, (which is calculated using the linear approximation with the linear probability p), we claim by our experience that we need the number $4np^{-1}$ of known plaintexts and the number $4p^{-1}2^n$ of computation of the round-function for the number $n(= 64)$ of the target key bits with probability

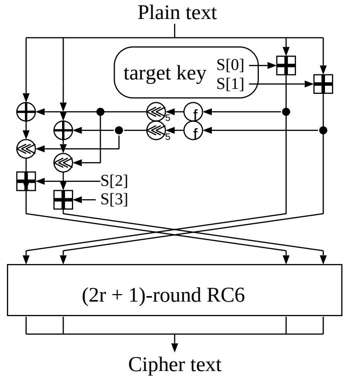

Fig. 3. 1-round elimination attack

Rounds	Target	#Texts	Complexity	Comments
4	RC6	$2^{29.68}$	$2^{95.68}$	
6	RC6	$2^{47.68}$	$2^{113.68}$	
8	RC6	$2^{65.68}$	$2^{131.68}$	
10	RC6	$2^{83.68}$	$2^{149.68}$	
12	RC6	$2^{101.68}$	$2^{167.68}$	
14	RC6	$2^{119.68}$	$2^{185.68}$	
16	RC6 weak key	$2^{118.048}$	$2^{184.048}$	1 in 2^{64} (Type II)
18	RC6 weak key	$2^{127.423}$	$2^{193.423}$	1 in 2^{90} (Type I)

Table 12. Key recovery of RC6

95% by the one-round elimination method. Thus, we can summarize the necessary data size and complexity to find the target extended key by the one-round elimination method in Table 12.

Thus we conclude that the 64-bit target extended key of 14-round RC6 can be recovered with probability 95% by Multiple Linear Attack with the number $2^{119.68}$ of known plaintexts and the number $2^{185.68}$ of computation of the round-function. Also that the 64-bit target extended key of 18-round RC6 with weak key, (the fraction is 2^{-90}), can be recovered with probability 95% by Multiple Linear Attack with the number $2^{127.423}$ of known plaintexts and the number of 2^{64} of memory, and the number $2^{193.423}$ of computation of the round-function.

References

1. A. Biryukov and E. Kushilevitz. Improved cryptanalysis of RC5. EUROCRYPT'98, LNCS 1403, pp.85–99, 1998.
2. J. Borst, B. Preneel, and J. Vandewalle. Linear cryptanalysis of RC5 and RC6. FSE'99, LNCS 1636, pp.16–30, 1999.
3. S. Contini, R.L. Rivest, M.J.B. Robshaw, and Y.L. Yin. The security of the RC6 block cipher. v.1.0, August 20, 1998.
   Available at `http://www.rsasecurity.com/rsalabs/rc6/`.

4. S. Contini, R.L. Rivest, M.J.B. Robshaw, and Y.L. Yin. Improved analysis of some simplified variants of RC6. FSE'99, LNCS 1636, pp.1–15, 1999.
5. H. Gilbert, H. Handschuh, A. Joux and S. Vaudenay, A Statistical Attack on RC6. FSE 2000, LNCS 1978, pp.64–74, 2001.
6. M.H. Heys. Linearly weak keys of RC5. *IEE Electronic Letters*, Vol.33, pp.836–838, 1997.
7. B.S. Kaliski Jr. and M.J.B. Robshaw. Linear cryptanalysis using multiple approximations. CRYPTO'94, LNCS 839, pp.26–39, 1994.
8. B.S. Kaliski Jr. and M.J.B. Robshaw. Linear cryptanalysis using multiple approximations and FEAL. FSE'94, LNCS 1008, pp.249–264, 1995.
9. B.S. Kaliski Jr. and Y.L. Yin. On differential and linear cryptanalysis of the RC5 encryption algorithm. CRYPTO'95, LNCS 963, pp.171–184, 1995.
10. B.S. Kaliski Jr. and Y.L. Yin. On the security of the RC5 encryption algorithm. Available at `http://www.rsasecurity.com/rsalabs/rc6/`.
11. J. Kelsey, B. Schneier, and D. Wagner. Mod n cryptanalysis, with applications against RC5P and M6. FSE'99, LNCS 1363, pp.139–155, 1999.
12. L.R. Knudsen and M.J.B. Robshaw. Non-linear approximations in linear cryptanalysis. EUROCRYPT'96, LNCS 1070, pp.224–236, 1996.
13. L.R. Knudsen and W. Meier. Correlations in RC6 with a reduced number of rounds. FSE 2000, LNCS 1978, pp.94–108, 2001.
14. M. Matsui. Linear cryptanalysis method for DES cipher. EUROCRYPT'93, LNCS 765, pp.386–397, 1993.
15. S. Moriai, K. Aoki and K. Ohta. Key-dependency of linear probability of RC5. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, Vol.E80-A, No.1, 1997.
16. R.L. Rivest. The RC5 encryption algorithm. FSE'94, LNCS 1008, pp.86–96, 1995.
17. R.L. Rivest, M.J.B. Robshaw, R. Sidney and Y.L. Yin. The RC6 block cipher. v1.1, August 20, 1998. Available at `http://www.rsasecurity.com/rsalabs/rc6/`.
18. K. Nyberg. Linear approximation of block ciphers. EUROCRYPT'94, LNCS 950, pp.439–444, 1994.
19. A.A. Selcuk. New results in linear cryptanalysis of RC5. FSE'98, LNCS 1372, pp.1–16, 1998.