IEICE TRANS. FUNDAMENTALS, VOL.E90–A, NO.1 JANUARY 2007

PAPER Special Section on Cryptography and Information Security

Evaluation of the Security of RC6 against the χ^2-Attack**

Atsuko MIYAJI[†*a)], ***Member and*** **Yuuki TAKANO**[†b)], ***Nonmember***

SUMMARY Knudsen and Meier applied the χ^2-attack to RC6. The χ^2-attack recovers a key by using high correlations measured by χ^2-value. Up to the present, the success probability of any χ^2-attack has not been evaluated theoretically without using experimental results. In this paper, we discuss the success probability of χ^2-attack and give the theorem that evaluates the success probability without using any experimental result, for the first time. We make sure the accuracy of our theorem by demonstrating it on both 4-round RC6 without post-whitening and 4-round RC6-8. We also evaluate the security of RC6 theoretically and show that a variant of the χ^2-attack is faster than an exhaustive key search for the 192-bit-key and 256-bit-key RC6 with up to 16 rounds. As a result, we succeed in answering such an open question that a variant of the χ^2-attack can be used to attack RC6 with 16 or more rounds.

key words: *block cipher, RC6, χ^2-attacks*

1. Introduction

The χ^2-attack makes use of correlations between input (plaintext) and output (ciphertext) measured by the χ^2-test, which was originally proposed by Vaudenay as an attack on the Data Encryption Standard (DES) [14], and Handschuh *et al*. applied that to SEAL [4]. To find correlations measured by the χ^2-test, we have to handle plaintexts in such a way that the χ^2-value of part of ciphertexts becomes significantly a high value. The distinguishing search finds the the condition for the good correlation and computes the necessary number of plaintexts for the χ^2-value with a certain level under the condition. The χ^2-attack rules out all wrong keys, and single out exactly a correct key by using the distinguishing search. Therefore, the χ^2-attack requires more work and memory than the distinguishing search.

RC6 is a fully parameterized family of a block cipher [12]. This paper focuses on the 128-bit RC 6 with keys of 128, 192, and 256 bits, whose spec was required to the candidates of AES. In [3], [8], a χ^2-attack was applied to RC6. They use the fact that a specific rotation in RC6 causes correlations between input and output, and estimated the security of RC6 against χ^2-attack only from results of the distinguishing search [8]. That is, they just focus on only the χ^2-value, strictly speaking, which is given as the average of χ^2-value measured over part of set of plaintexts. χ^2-attacks to a simplified variant of RC6 such as RC6 without pre- or post-whitening or RC6 without only post-whitening are further improved in [11] or [5], respectively. The variance as well as the average of χ^2-value is taken into account to recover a key in their attack. Thus, their χ^2-attack can recover a correct key in the high probability with a rather lower χ^2-value than [8]. They also pointed out that the χ^2-attack does not necessarily succeed even if the distinguishing search results in the high χ^2-value. This indicates that the security against the χ^2-attack cannot be estimated directly from the results of the distinguishing search. Table 1 summarizes the previous attacks on RC6.

Table 1 Attacks on RC6.

Attack	Target RC6	Rounds	#Texts
Linear Attack [1]	RC6	16	2^{119}
Multiple Linear Attack [15]	192-bit-key RC6	14[1]	$2^{119.68}$
χ^2 Attack [8]	128-bit-key RC6	12	2^{94}
	192-bit-key RC6	14	2^{108}
	256-bit-key RC6	15	2^{119}
χ^2 Attack [11]	128-bit key RC6W[2]	17	$2^{123.9}$
χ^2 Attack [5]	128-bit key RC6P[3]	16	$2^{117.84}$
Our result	192-bit-key RC6	16	$2^{127.20}$
	256-bit-key RC6	16	$2^{127.20}$

1: A weak key of 18-round RC6 with 256-bit key can be recovered by $2^{126.936}$ plaintexts with the probability of about $1/2^{90}$.
2: RC6W means RC6 without pre- or post-whitening.
3: RC6P means RC6 without post-whitening.

Theoretical analysis on χ^2-attack has been done by [10], [16]. In [16], the average of χ^2-value used in the distinguishing search of [8] is theoretically computed, by which the necessary number of plaintexts for the χ^2-value with a certain level can be estimated theoretically in each round. However, this is not enough to evaluate the success probability of χ^2-attack itself since there is the significant difference between the distinguishing search and the χ^2-attack as mentioned above. On the other hand, theoretical difference between a distinguishing search and a χ^2-attack on RC6 without post-whitening [5] has been discussed in [10]. They make use of the idea of the theoretical and experimental complexity analysis on the linear cryptanalysis [6], [13] to fit it in the theoretical and experimental complexity analysis on the χ^2-attack. They also present the theorem to compute the success probability of χ^2-attacks by using the results of distinguishing search, and, thus, they can succeed to estimate the security against χ^2-attack on RC6 with rather less work and memory. However, their estimation re-

Manuscript received March 27, 2006.
Manuscript revised July 2, 2006.
Final manuscript received August 21, 2006.
†The authors are with Japan Advanced Institute of Science and Technology, Nomi-shi, 923-1292 Japan.
*Supported partly by Inamori Foundation.
**A preliminary version was presented at ACISP'05.
a) E-mail: miyaji@jaist.ac.jp
b) E-mail: ytakano@jaist.ac.jp
DOI: 10.1093/ietfec/e90–a.1.22

quires experimental results of distinguishing search. Up to the present, the success probability of a χ^2-attack has not been evaluated theoretically without any assumption of experimental results.

In this paper, we investigate the success probability of a χ^2-attack, for the first time, and give the theorem that evaluates the success probability without any experimental result. First, we deal with a χ^2-attack on RC6 without post-whitening [5] and give the theorem that evaluates the success probability theoretically. We make sure the accuracy of our theorem by comparing our approximation with the experimental results [5]. With our theory, we also confirm that 16-round 128-bit-key RC6 without post-whitening can be broken, which reflects the experimental approximation [5]. Then, we improve the χ^2-attack to work on RC6 itself. The primitive extension to RC6 are shown in [5], but it does not seem to work. We give the theorem that evaluates the success probability of the χ^2-attack on RC6 theoretically. We also demonstrate our theorem on 4-round RC6-8 and make sure the accuracy by comparing our approximation with the experimental results. With our theory, we confirm that 16-round 192-bit-key and 256-bit key RC6 can be broken. As a result, we can answer the open question of [8], that is, whether χ^2-attack can be used to attack RC6 with 16 or more rounds.

This paper is organized as follows. Section 2 summarizes the notation, RC6 algorithms, the χ^2-test, and statistical facts used in this paper. Section 3 reviews the χ^2-attack against RC6 without post-whitening and the theoretical relation between a distinguishing search and a χ^2-attack. Section 4 presents the theorem of success probability of χ^2-attacks on RC6 without post-whitening and investigates the accuracy by comparing the approximations of success probability to 4-round RC6 without post-whitening with implemented results. Section 5 improves the χ^2-attack on RC6 without post-whitening to that on RC6 and presents the theorem of the success probability of the χ^2-attack on RC6. We investigate the accuracy by demonstrating the key recovery algorithm on RC6-8. We also discuss the applicable round of χ^2-attack. A conclusion is given in Sect. 6.

2. Preliminary

We summarize the χ^2-test, statistical facts, and RC6 algorithm [12], used in this paper.

2.1 Statistical Facts

We make use of the χ^2-statistic [9] to distinguish a distribution with an unknown probability distribution $\mathbf{p}$ from an expected distribution with a probability distribution π. Let $X = X_0, ..., X_{n-1}$ be a sequence of $\forall X_i \in \{a_0, \cdots, a_{m-1}\}$ with unknown probability distribution $\mathbf{p}$, and $N_{a_j}(X)$ be the number of X which takes on the value a_j. The χ^2-statistic of X which estimates the distance between the observed distribution and the expected distribution $\pi = (\pi_1, \cdots, \pi_m)$ is defined:

$$\chi^2 = \sum_{i=0}^{m-1} \frac{(N(a_i) - n\pi_i)^2}{n\pi_i}. \tag{1}$$

After computing the χ^2-statistic of X, we decide which hypothesis holds.

$$\begin{cases} H_0 : \mathbf{p} = \pi & \text{(null hypothesis)} \\ H_1 : \mathbf{p} \neq \pi & \text{(alternate hypothesis)} \end{cases} \tag{2}$$

The following Theorems 1 and 2 on χ^2-statistic are known.

Theorem 1 ([17]): When H_0 is true, χ^2 statistic given by Eq. (1) follows χ^2 distribution whose freedom is $m-1$ approximately. In addition, the expected mean or variance is calculated by $E_{H_0}(\chi^2) = m-1$ or $V_{H_0}(\chi^2) = 2(m-1)$, respectively.

Theorem 2 ([17]): When H_1 is true, χ^2 statistic given by Eq. (1) follows non-central χ^2 distribution whose freedom is $m-1$ approximately. In addition, the mean or variance is computed by $E_{H_1}(\chi^2) = m-1+n\theta$ or $V_{H_1}(\chi^2) = 2(m-1) + 4n\theta$, respectively, where $n\theta$ so called non-central parameter is $n\theta = n\sum_{i=0}^{m-1} \frac{(\pi_i - P(a_i))^2}{\pi_i}$, where $P(a_i)$ is the probability of occurrence of a_i.

In our case of which distinguishes a non-uniformly random distribution from uniformly random distribution [7]–[9], the probability π is equal to $\frac{1}{m}$ and, thus, Eq. (1) is simply described as follows.

$$\chi^2 = \frac{m}{n} \sum_{i=0}^{m-1} \left(n_i - \frac{n}{m}\right)^2. \tag{3}$$

Table 2 presents threshold for a 63 degrees of freedom. For example, (level, χ^2_{63}) = (0.95, 82.53) in Table 2 means that the value of the χ^2-statistic exceeds 82.53 in the probability of 5% if the observation X is uniform.

Let us describe other statistical facts together with the notation.

Theorem 3 (Central Limit Theorem [2]): Choose a random sample from a population which mean or variance is μ or σ^2, respectively. If the sample size n is large, then the sampling distribution of the mean is closely approximated by the normal distribution, regardless of the population, where the mean or variance is given by μ or σ^2/n, respectively.

We also follow commonly used notation: the probability density and the cumulative distribution functions of the standard normal distribution are denoted by $\phi(x)$ and $\Phi(x)$; the probability of distribution X in the range $X \leq I$ is denoted by $\Pr(X \leq I)$; and $\mathcal{N}$ is used for the normal distributions. The probability density function of the normal distribution with the mean μ and the variance σ^2, $\mathcal{N}(\mu, \sigma^2)$, is

Table 2 χ^2-distributions with a 63 degree of freedom.

Level	0.50	0.60	0.70	0.80	0.90	0.95	0.99
χ^2_{63}	62.33	65.20	68.37	72.20	77.75	82.53	92.01

given by the following equation,

$$\phi_{(\mu,\sigma^2)}(x) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left[-\frac{(x-\mu)^2}{2\sigma^2}\right].$$

2.2 Block Cipher RC6

Before showing the encryption algorithm of RC6, we give some notation.

$\{0,1\}^k$:	k-bit data
$\mathrm{lsb}_n(X)$:	least significant n-bit of X;
$\mathrm{msb}_n(X)$:	most significant n-bit of X;
$\oplus$:	bit-wise exclusive OR;
$a \lll b$:	cyclic rotation of a to the left by b-bit;
S_i :	i-th subkey (S_{2i} and S_{2i+1} are subkeys of the i-th round);
r :	number of rounds;
(A_i, B_i, C_i, D_i) :	input of the i-th round ;
(A_0, B_0, C_0, D_0) :	plaintext;
$(A_{r+2}, B_{r+2}, C_{r+2}, D_{r+2})$:	ciphertext after r-round encryption;
$f(x)$:	$x \times (2x+1)$;
$F(x)$:	$f(x) \pmod{2^{32}} \lll 5$;
$x\|\|y$:	concatenated value of x and y.

The detailed algorithm of RC6 is given:

Algorithm 1 (RC6 Encryption Algorithm):

1. $A_1 = A_0$; $B_1 = B_0 + S_0$; $C_1 = C_0$; $D_1 = D_0 + S_1$;
2. for $i = 1$ to r do:
   $t = F(B_i)$; $u = F(D_i)$; $A_{i+1} = B_i$;
   $B_{i+1} = ((C_i \oplus u) \lll t) + S_{2i+1}$; $C_{i+1} = D_i$;
   $D_{i+1} = ((A_i \oplus t) \lll u) + S_{2i}$;
3. $A_{r+2} = A_{r+1} + S_{2r+2}$; $B_{r+2} = B_{r+1}$;
   $C_{r+2} = C_{r+1} + S_{2r+3}$; $D_{r+2} = D_{r+1}$.

Steps 1 and 3 of Algorithm 1 are called pre-whitening and post-whitening, respectively. RC6 is specified as RC6-$w/r/b$, which means that four w-bit-word plaintexts are encrypted with r rounds by b-byte keys. In this paper, we simply write RC6 if we deal with RC6 of 32-bit-word plaintexts. We also call RC6 without post-whitening to, simply, RC6P.

Hereafter, we discuss the success probability of a χ^2-attack against RC6, RC6P, or RC6-8, which means the probability of recovering a correct key in the attack.

2.3 A Transition Matrix

A transition matrix describes input-output transition, which was introduced in [14] and applied to RC6-8 and RC6-32 in [16]. In [16], the transition matrix can compute the expected χ^2-values on $\mathrm{lsb}_5(A_{r+2})||\mathrm{lsb}_5(C_{r+2})$ when plaintexts with $\mathrm{lsb}_5(A_0) = \mathrm{lsb}_5(C_0) = 0$ are chosen, which is denoted by TM in this paper. So TM also gives the probability of occurrence of $\mathrm{lsb}_5(A_{r+2})||\mathrm{lsb}_5(C_{r+2})$. We apply TM to compute the expected χ^2-values and the variance on $\mathrm{lsb}_3(A_{r+2})||\mathrm{lsb}_3(C_{r+2})$ when plaintexts with a fixed value of $\mathrm{lsb}_5(B_0) = \mathrm{lsb}_5(D_0)$ are chosen.

3. χ^2 Attack on RC6P

In this section, we review χ^2-attack on RC6P [5], called Attack 1 in this paper, and then the success probability [10] based on the experimental results of the distinguishing search.

Intuitively, Attack 1 fixes some bits out of $\mathrm{lsb}_n(B_0)||\mathrm{lsb}_n(D_0)$, computes the characteristic value based on the χ^2-value of $\mathrm{lsb}_3(A_r)||\mathrm{lsb}_3(C_r)$ and recovers $\mathrm{lsb}_2(S_{2r})||\mathrm{lsb}_2(S_{2r+1})$ of r-round RC6P. Let us set:
$(y_b, y_d) = (\mathrm{lsb}_3(B_{r+1}), \mathrm{lsb}_3(D_{r+1}))$,
$(x_c, x_a) = (\mathrm{lsb}_5(F(A_{r+1})), \mathrm{lsb}_5(F(C_{r+1})))$,
$(s_a, s_c) = (\mathrm{lsb}_2(S_{2r}), \mathrm{lsb}_2(S_{2r+1}))$ and $s = s_a||s_c$, where x_a (resp. x_c) is the rotation amounts on A_r (resp. C_r) in the r-th round.

Attack 1 ([5]):

1. Choose a plaintext (A_0, B_0, C_0, D_0) with $(\mathrm{lsb}_5(B_0), \mathrm{lsb}_5(D_0)) = (0,0)$ and encrypt it.
2. For each (s_a, s_c), decrypt $y_d||y_b$ with a key $0||s_a, 0||s_c$ by 1 round to $z_a||z_c$, which are denoted by a 6-bit integer $z = z_a||z_c$.
3. For each s, x_a, x_c, and z, update each array by incrementing count$[s][x_a][x_c][z]$.
4. For each s, x_a, and x_c, compute $\chi^2[s][x_a][x_c]$.
5. Compute the average $ave[s]$ of $\{\chi^2[s][x_a] \cdot [x_c]\}_{x_a,x_c}$ for each s and output s with the highest $ave[s]$ as $\mathrm{lsb}_2(S_{2r})||\mathrm{lsb}_2(S_{2r+1})$.

We may note that Attack 1 can be easily generalized to recover an e-bit key for an even e. In such a case, z is an $(e+2)$-bit number, on which χ^2-value is computed. The success probability of Attack 1 is derived theoretically from Theorem 4.

Theorem 4 ([5]): Let $n \geq 10$ and $r \geq 4$. The success probability Ps of Attack 1 on r-round RC6P with 2^n plaintexts can be evaluated by using the distribution of χ^2-values as follows,

$$Ps = \int_{-\infty}^{\infty} f_{c[r,n]}(x) \cdot \left(\int_{-\infty}^{x} f_{w[r,n]}(u)du \right)^{2^e-1} dx, \tag{4}$$

where $f_{c[r,n]}(x)$ or $f_{w[r,n]}$ is a probability density function of distribution of χ^2-values on a correct or wrong key in Attack 1, given by

$$f_{c[r,n]}(x) = \phi_{(\mu_{d[r-1,n-10]}, \sigma^2_{d[r-1,n-10]}/2^{10})}(x) \tag{5}$$

or

$$f_{w[r,n]}(x) = \phi_{(\mu_{d[r+1,n-10]}, \sigma^2_{d[r+1,n-10]}/2^{10})}(x), \tag{6}$$

respectively, and $\mu_{d[r,n]}(\sigma^2_{d[r,n]})$ is mean (variance) of distribution of χ^2-values on $\mathrm{lsb}_3(A_{r+1})||\mathrm{lsb}_3(C_{r+1})$ of r-round RC6P with $\mathrm{lsb}_5(B_0)||\mathrm{lsb}_5(D_0) = 0$ by using 2^n plaintexts.

4. Success Probability of χ^2-Attack on RC6P

This section gives the theorem to compute the success probability of Attack 1 without any experimental result of distinguishing search.

4.1 Theoretical Mean and Variance of χ^2-values

To compute the success probability of Attack 1 without any experimental results of distinguishing search, we have to compute the mean and variance, $\mu_{d[r,n]}$ and $\sigma^2_{d[r,n]}$, theoretically, that is, we have to compute θ_r. In our case, θ_r is given as

$$\theta_r = 2^6 \sum \left(P(\mathrm{lsb}_3(A_{r+1}) \| \mathrm{lsb}_3(C_{r+1})) - \frac{2^n}{2^6} \right)^2, \qquad (7)$$

where the summation is over $\mathrm{lsb}_3(A_{r+1})\|\mathrm{lsb}_3(C_{r+1}) \in \{0,1\}^6$ and $P(\mathrm{lsb}_3(A_{r+1})\|\ \mathrm{lsb}_3(C_{r+1}))$ is the probability of occurrence of $\mathrm{lsb}_3(A_{r+1})\|\mathrm{lsb}_3(C_{r+1})$. θ_r can be given by computing $P(\mathrm{lsb}_3(A_{r+1})\|\mathrm{lsb}_3(C_{r+1}))$ and, thus, derived theoretically by TM in Sect. 2, which follows the discussion below.

Attack 1 is based on a distinguishing search that chooses $\mathrm{lsb}_5(B_0) = \mathrm{lsb}_5(D_0) = 0$ and computes the χ^2-value on $\mathrm{lsb}_3(A_{r+1})\|\mathrm{lsb}_3(C_{r+1})$, which are outputs of r-round RC6P. Therefore, we can apply TM to our distinguishing search by assuming that (A_1, B_1, C_1, D_1) is a plaintext since $A_1 = B_0, C_1 = D_0$, and both B_1 and D_1 are random number. On the other hand, we compute the χ^2-value on $(e+2)$-bit $\mathrm{lsb}_{e/2+1}(A_{r+1})\|\mathrm{lsb}_{e/2+1}(C_{r+1})$ in e-bit-key-recovery Attack 1, whose probability of occurrence is derived by using TM from the following Lemma 1.

Lemma 1: The probability of occurrence of $\mathrm{lsb}_{e/2+1}(A_{r+1})\|$ $\mathrm{lsb}_{e/2+1}(C_{r+1})$, denoted by $P(\mathrm{lsb}_{e/2+1}(A_{r+1})\|\mathrm{lsb}_{e/2+1}(C_{r+1}))$, is computed from the probability of occurrence of $\mathrm{lsb}_5(A_{r+1})\|\mathrm{lsb}_5(C_{r+1})$ as follows

$$P(\mathrm{lsb}_{e/2+1}(A_{r+1})\|\mathrm{lsb}_{e/2+1}(C_{r+1})) = \sum_{i=0}^{2^\beta-1} \sum_{j=0}^{2^\beta-1} P(i\|\mathrm{lsb}_{e/2+1}(A_{r+1})\|j\|\mathrm{lsb}_{e/2+1}(C_{r+1})),$$

where $\beta = 5 - (e/2+1)$ and e is an even integer from 2 to 10.

Proof 1: Lemma 1 holds because

$$\mathrm{lsb}_5(A_{r+1})\|\mathrm{lsb}_5(C_{r+1}) = \mathrm{msb}_\beta(\mathrm{lsb}_5(A_{r+1}))\|\mathrm{lsb}_{e/2+1}(A_{r+1}) \|\mathrm{msb}_\beta(\mathrm{lsb}_5(C_{r+1}))\|\mathrm{lsb}_{e/2+1}(C_{r+1}).$$

∎

We show theoretical and experimental results of mean and variance of χ^2-values of 3- or 5-round RC6P in Table 3, respectively. Experiments are done by using 100 keys × 100 sets of texts. We see that both mean and variance of χ^2-value can be computed theoretically.

4.2 Success Probability of Attack 1 on RC6P

By using the theoretical mean and variance in Sect. 4.1, the success probability of Attack 1 is proved as follows.

Theorem 5: The success probability of e-bit-key-recovery Attack 1 of r-round RC6P is given as follows,

$$Ps_{rc6p,e}(n) = \int_{-\infty}^{\infty} \phi_{((k-1)+m\theta_{r-1},(2(k-1)+4m\theta_{r-1})/2^{10})}(x) \cdot \left(\int_{-\infty}^{x} \phi_{((k-1)+m\theta_{r+1},(2(k-1)+4m\theta_{r+1})/2^{10})}(u)du \right)^{2^e-1} dx, \qquad (8)$$

where 2^n is the number of texts; $m = 2^{n-10}$; $k = 2^{e+2}$; $m\theta_r$ is r-round non-central parameter; and e is an even integer from 2 to 10.

Proof 2: Ps in Theorem 4 is derived by mean $\mu_{d[r,n]}$ and variance $\sigma^2_{d[r,n]}$ of distribution of χ^2-values, which are computed by non-central parameter from Theorem 2. On the other hand, θ_r is computed by using Lemma 1. Thus we get $Ps_{rc6p,e}(n)$. ∎

Table 4 shows the success probability of Attack 1. According to Table 4, the theoretical estimation gives the upper bound of results. It seems rather rough upper bound. We will discuss the reason in Sect. 5.

4.3 Applicable Rounds of RC6P

By computing θ_r of each round r, we derive the number of texts to recover a correct key with the probability of more than 95% by Attack 1. We approximate Eq. (8) to reduce the computation amount to get (8) for an even large e.

Theorem 6: The sufficient condition for $Ps_{rc6p,e}(n) \geq 0.95$ is given as

$$\widetilde{Ps}_{rc6p,e}(n) \geq 1 - \frac{1}{20(2^e-1)}, \qquad (9)$$

where

Table 4 Theoretical and experimental success probabilities of 4-round RC6P ($e = 4$).

# texts	2^{18}	2^{19}	2^{20}	2^{21}	2^{22}
Theoretical	0.16	0.31	0.70	0.99	1.00
Experimental	0.10	0.17	0.34	0.75	1.00

Table 3 χ^2-values of 3- or 5-round RC6P.

3 rounds					5 rounds				
#texts	Theoretical		Experimental		#texts	Theoretical		Experimental	
	mean	variance	mean	variance		mean	variance	mean	variance
2^8	63.20	126.82	63.18	126.50	2^{24}	63.20	126.80	63.30	125.72
2^9	63.41	127.64	63.27	126.78	2^{25}	63.40	127.60	63.43	128.48
2^{10}	63.82	129.29	63.79	125.02	2^{26}	63.80	129.19	63.72	128.94
2^{11}	64.64	132.57	64.33	130.48	2^{27}	64.60	132.34	64.50	132.11
2^{12}	66.29	139.14	65.92	139.85	2^{28}	66.19	138.78	66.16	141.22

$$\widetilde{Ps}_{rc6p,e}(n) = \int_{-\infty}^{\infty} \phi_{(k-1+m\theta_{r-1},(2(k-1)+4m\theta_{r-1})/2^{10})}(x) \cdot \int_{-\infty}^{x} \phi_{(k-1+m\theta_{r+1},(2(k-1)+4m\theta_{r+1})/2^{10})}(u)du\,dx;$$

$m = 2^{n-10}$; $k = 2^{e+2}$; $m\theta_r$ is r-round non-central parameter; and e is an even integer from 2 to 10.

Proof 3: We show that n satisfied with Eq. (9) is sufficient for $Ps_{rc6p,e}(n) \geq 0.95$. First, we introduce the following monotonically increasing function for $e \geq 1$,

$$F(e) = \left(1 - \frac{1}{20(2^e - 1)}\right)^{2^e - 1},$$

which satisfies $F(e) \geq 0.95$ for $e \geq 1$. On the other hand, Eq. (8) satisfies

$$\begin{aligned} P_{s_{rc6,e}}(n) &= \int_{-\infty}^{\infty} \phi_{(k-1+m\theta_{r-1},(2(k-1)+4m\theta_{r-1})/2^{10})}(x) \cdot \left(\int_{-\infty}^{x} \phi_{(k-1+m\theta_{r+1},(2(k-1)+4m\theta_{r+1})/2^{10})}(u)du\right)^{2^e-1} dx \\ &\geq \left(\int_{-\infty}^{\infty} \phi_{(k-1+m\theta_{r-1},(2(k-1)+4m\theta_{r-1})/2^{10})}(x) \cdot \int_{-\infty}^{x} \phi_{(k-1+m\theta_{r+1},(2(k-1)+4m\theta_{r+1})/2^{10})}(u)du\,dx\right)^{2^e-1} \end{aligned}$$

since $\phi_{(k-1+m\theta_{r-1},(2(k-1)+4m\theta_{r-1})/2^{10})}(x)$ or $\phi_{(k-1+m\theta_{r+1},(2(k-1)+4m\theta_{r+1})/2^{10})}(x)$ is a probability density function of distribution of χ^2-values on a correct or wrong key, respectively. Thus, if $m = 2^{n-10}$ satisfies

$$\left(\int_{-\infty}^{\infty} \phi_{(k-1+m\theta_{r-1},(2(k-1)+4m\theta_{r-1})/2^{10})}(x) \cdot \int_{-\infty}^{x} \phi_{(k-1+m\theta_{r+1},(2(k-1)+4m\theta_{r+1})/2^{10})}(u)du\,dx\right)^{2^e-1} \geq F(e),$$

then $Ps_{rc6p,e}(n) \geq 0.95$. Therefore, if n satisfies

$$\begin{aligned} \widetilde{Ps}_{rc6p,e}(n) &= \int_{-\infty}^{\infty} \phi_{(k-1+m\theta_{r-1},(2(k-1)+4m\theta_{r-1})/2^{10})}(x) \cdot \int_{-\infty}^{x} \phi_{(k-1+m\theta_{r+1},(2(k-1)+4m\theta_{r+1})/2^{10})}(u)du\,dx \\ &\geq 1 - \frac{1}{20(2^e - 1)}, \end{aligned}$$

then $Ps_{rc6p,e}(n) \geq 0.95$. ∎

Here we set $e = 4$. Table 5 shows theoretical and experimental number of texts necessary for $Ps_{rc6p,e}(n) \geq 0.95$ in each r round. From Table 5, Attack 1 is faster than exhaustive search for 128-bit-key RC6P with up to 16 rounds. It corresponds with the previous experimental result [5]. Our theorem estimates the number of texts necessary for recovering r-round RC6P with the success probability of more than 95% to

$$\log_2(\#\text{texts}) = 8.01r - 11.63. \quad (10)$$

Table 5 Theoretical and estimated #texts for $Ps_{rc6p,4}(n) \geq 0.95$ or $Ps \geq 0.95$.

round	Theoretical (Th.6) # texts	Theoretical (Th.6) time‡	Estimated (Th.4) # texts	Estimated (Th.4) time‡
4	$2^{20.69}$	$2^{24.69}$	†$2^{21.60}$	†$2^{25.60}$
6	$2^{36.73}$	$2^{39.67}$	$2^{37.64}$	$2^{41.64}$
8	$2^{52.76}$	$2^{56.76}$	$2^{53.68}$	$2^{57.68}$
10	$2^{68.79}$	$2^{72.79}$	$2^{69.72}$	$2^{73.72}$
12	$2^{84.81}$	$2^{88.81}$	$2^{85.76}$	$2^{89.76}$
14	$2^{100.82}$	$2^{104.82}$	$2^{101.80}$	$2^{105.80}$
16	$2^{116.83}$	$2^{119.77}$	$2^{117.84}$	$2^{121.84}$
18	$2^{132.85}$	$2^{136.85}$	$2^{133.88}$	$2^{137.88}$

† : experimental result [5]
‡ : the number of incrementing a counter `count`.

Table 6 Theoretical and experimental success probability of 4-round RC6P-8 by using Attack 1.

# texts	Theoretical	Experimental
2^{12}	0.742	0.228
2^{13}	1.000	0.481
2^{14}	1.000	0.888
2^{15}	1.000	1.000

On the other hand, it is estimated in [5] heuristically as

$$\log_2(\#\text{texts}) = 8.02r - 10.48. \quad (11)$$

We see that both estimations are pretty close each other.

4.4 Success Probability of Attack 1 on RC6P-8

We also demonstrate our theorem on 4-round RC6P-8 whose word size is 8-bit. Table 6 shows the theoretical and experimental results of Attack 1 on RC6P-8. In the same way as 4-round RC6P, we see that theoretical estimation gives the upper bound of experimental results.

5. χ^2 Attack against RC6

This section improves Attack 1 to a key recovery attack against RC6, Attack 2, and then gives the theorem that computes the success probability. We also implement Attack 2 on 4-round RC6-8 and demonstrate the accuracy of the theorem. Furthermore we also discuss the difference between Theorem 5 and 7 in view of accuracy.

5.1 Key Recovery Attack and Theoretical Success Probability

The primitive extension of Attack 1 to a key recovery attack on RC6 is to decrypt $y_a||y_d$ for each key candidate of s, S_{2r+2} and S_{2r+3}, which is shown in [5]. Apparently it is rather straightforward since it means that it decrypts each ciphertext by each 2^{68} key. So we improve Attack 1 such that it does not have to decrypt each ciphertext. Before showing the algorithm, let us use the following notation:
$\mathcal{U} = \{u \in \{0,1\}^{32} | \text{msb}_5(u \times (2u+1)) = 0\}$,
$(u_a, u_c) \in \mathcal{U} \times \mathcal{U}, t_a = A_{r+2} - u_a, t_c = C_{r+2} - u_a$,
$v = \text{lsb}_5(B_0)||\text{lsb}_5 D_0, z = \text{lsb}_3(B_{r+2})||\text{lsb}_3(D_{r+2})$.

Attack 2:

1. Choose a plaintext $(A_0,\ B_0,\ C_0,\ D_0)$ and encrypt it to $(A_{r+2},\ B_{r+2},\ C_{r+2},\ D_{r+2})$.
2. For each (u_a, u_c), compute both t_a and t_c and update each array by incrementing $\mathrm{count}[t_a][t_c][v][z]$.
3. For each t_a, t_c and v, compute the χ^2-value $\chi^2[t_a][t_c][v]$.
4. Compute the average $ave[t_a][t_c]$ of $\{\chi^2[t_a][t_c][v]\}_v$ for each t_a, t_c and output t_a, t_c with the highest $ave[t_a][t_c]$ as S_{2r+2}, S_{2r+3}.

Attack 2 computes the χ^2-value on 6-bit z, which follows the idea of Attack 1. Compared with [8], in which the χ^2-value is computed on 10-bit data, Attack 2 seems to recover a correct key more efficiently.

We may note that Attack 2 calculates the χ^2-value on $z = \mathrm{lsb}_3(B_{r+2}) \| \mathrm{lsb}_3(D_{r+2})$ by using such plaintexts that make the final-round-rotation 0 for each key candidate. For a correct key, this is exactly equivalent to compute the χ^2-value on $\mathrm{lsb}_3(A_r) \| \mathrm{lsb}_3(C_r)$, which is output of $(r-1)$-round RC6P because the addition keeps the χ^2-value. Thus, we succeed to skip the post-whitening and get that the probability density function of distribution of χ^2-value with a correct key in r-round RC6 is equal to $f_{c[r,n]}$ defined in Theorem 4. On the other hand, in the case of wrong keys, this is exactly equivalent to compute the χ^2-value on $\mathrm{lsb}_3(A_{r+2}) \| \mathrm{lsb}_3(C_{r+2})$, which is output of $(r+1)$-round RC6P. Thus, we get that the probability density function of distribution of χ^2-value with a wrong key in r-round RC6 is equal to $f_{w[r,n]}$ defined in Theorem 4. From the above discussion, we've proved the following theorem.

Theorem 7: The success probability of Attack 2 on r-round RC6 is given theoretically as

$$Ps_{rc6}(n) = \int_{-\infty}^{\infty} \phi_{(2^6-1+m\theta_{r-1},(2(2^6-1)+4m\theta_{r-1})/2^{10})}(x) \cdot \left(\int_{-\infty}^{x} \phi_{(2^6-1+m\theta_{r+1},(2(2^6-1)+4m\theta_{r+1})/2^{10})}(u)du \right)^{2^{64}-1} dx, \tag{12}$$

where 2^n is the number of texts, $m = 2^{n-20}$ and $m\theta_r$ is r-round non-central parameter.

We approximate Eq. (12) to reduce the computation amount to get (12) in the same way as Theorem 5. Theorem 8 eliminates the computation of exponentiation $2^{64}-1$ on an integral part in (12) and, thus, enables effective computation of n with $Ps_{rc6}(n) \geq 0.95$.

Theorem 8: The sufficient condition for $Ps_{rc6}(n) \geq 0.95$ is

$$\widetilde{Ps}_{rc6}(n) \geq 1 - \frac{1}{20(2^{64}-1)},$$

where

$$\widetilde{Ps}_{rc6}(n) = \int_{-\infty}^{\infty} \phi_{(2^6-1+m\theta_{r-1},(2(2^6-1)+4m\theta_{r-1})/2^{10})}(x) \cdot \int_{-\infty}^{x} \phi_{(2^6-1+m\theta_{r+1},(2(2^6-1)+4m\theta_{r+1})/2^{10})}(u)du\ dx,$$

$m = 2^{n-20}$ and $m\theta_r$ is r-round non-central parameter.

Table 7 #texts necessary for $Ps_{rc6}(n) \geq 0.95$ (From Th.8).

r	4	6	8	10	12	14	16	18
# texts	$2^{31.06}$	$2^{47.10}$	$2^{63.13}$	$2^{79.15}$	$2^{95.17}$	$2^{111.19}$	$2^{127.20}$	$2^{143.21}$
time complexity†	$2^{85.06}$	$2^{101.10}$	$2^{117.13}$	$2^{133.15}$	$2^{149.17}$	$2^{165.19}$	$2^{181.20}$	$2^{197.21}$

†: the number of incrementing a counter count.

Table 8 Theoretical and experimental success probability of 4-round RC6-8 (Alg. 2).

# texts	2^{17}	2^{18}	2^{19}	2^{20}
Theoretical	0.00	0.05	0.73	1.00
Experimental	0.00	0.04	0.76	1.00

Table 7 shows the necessary number of texts and time complexity which make success probability of Attack 2 on RC6 95% or more. The necessary number of texts is computed by Theorem 8. Time complexity is estimated by the number of incrementing a counter count, which is the dominant step of Attack 2. The number of available texts is bounded by 2^{128} in Attack 2 and that the time complexity is #texts$\times 2^{27\times 2}$ since Attack 2 recovers both post-whitening keys at once. In [8], they estimated heuristically that 192-bit-key or 256-bit-key RC6 are broken up to 14 or 15 rounds by their key recovery algorithm, respectively. We've now proved theoretically that 192-bit-key and 256-bit-key RC6 can be broken up to 16 rounds. Attack 2 works on an 128-bit-key RC6 with up to 8 rounds. Thus, our results can answer the open question of [8], that is whether or not the χ^2 attack works on RC6 with 16 rounds or more.

5.2 Success Probability of Attack 2 on RC6-8

We also demonstrate Theorem 7 on 4-round RC6-8. Table 8 shows the theoretical and experimental results. We see that theoretical estimation gives a pretty good approximation compared with Table 6. Let us discussion the reason. In Attack 1, we assume that the χ^2-values of wrong keys in r-round RC6P equals that in $(r+1)$-round RC6P to estimate $Ps_{rc6p,e}(n)$. However, this is exactly upper bound of χ^2-values of wrong keys. In the case of Attack 2, the χ^2-values of wrong keys in r-round RC6 are equal to that in $(r+1)$-round RC6P. Thus, we see that theoretical estimation of Theorem 7 is much better than that of Theorem 5.

6. Concluding Remarks

In this paper, we have improved the χ^2-attack on RC6P to the χ^2-attack on RC6 and proved the theorems that evaluate the success probability in the χ^2-attacks on RC6P and RC6. The derived formulae can be computed efficiently and provide a theoretical analysis of the success probability in the

χ^2-attack. We have also demonstrated that our theorems can well estimate success probability in the χ^2-attacks against 4-round RC6P, RC6P-8, and RC6-8. Furthermore we have shown theoretically that our χ^2-attack is applicable to 192-bit-key and 256-bit-key RC6 with up to 16 rounds.

Acknowledgments

The authors express our gratitude to anonymous referees for invaluable comments.

References

[1] S. Contini, R. Rivest, M. Robshaw, and Y. Yin, "The security of the RC6 block cipher. v 1.0," Aug. 1998. Available at http://www.rsasecurity.com/rsalabs/rc6/
[2] R.J. Freund and W.J. Wilson, Statistical Method, Academic Press, San Diego, 1993.
[3] H. Gilbert, H. Handschuh, A. Joux, and S. Vaudenay, "A statistical attack on RC6," FSE 2000, LNCS 1978, pp.64–74, Springer-Verlag, 2000.
[4] H. Handschuh and H. Gilbert, "χ^2 cryptanalysis of the SEAL encryption algorithm," FSE '97, LNCS 1267, pp.1–12, Springer-Verlag, 1997.
[5] N. Isogai, T. Matsunaka, and A. Miyaji, "Optimized χ^2-attack against RC6," ANCS 2003, LNCS 2846, pp.16–32, Springer-Verlag, 2003.
[6] P. Junod, "On the complexity of Matsui's attack," SAC 2001, LNCS 2259, pp.199–211, Springer-Verlag, 2001.
[7] J. Kelsey, B. Schneier, and D. Wagner, "Mod n cryptanalysis, with applications against RC5P and M6," FSE '99, LNCS 1636, pp.139–155, Springer-Verlag, 1999.
[8] L. Knudsen and W. Meier, "Correlations in RC6 with a reduced number of rounds," FSE 2000, LNCS 1978, pp.94–108, Springer-Verlag, 2000.
[9] D. Knuth, The art of computer programming, vol.2, Seminumerical Algorithms, 2nd ed., Addison-Wesley, Reading, Mass., 1981.
[10] T. Matsunaka, A. Miyaji, and Y. Takano, "Success probability in χ^2-attacks," ACNS 2004, LNCS 3089, pp.310–325, Springer-Verlag, 2004.
[11] A. Miyaji and M. Nonaka, "Cryptanalysis of the reduced-round RC6," ICICS 2002, LNCS 2513, pp.480–494, Springer-Verlag, 2002.
[12] R. Rivest, M. Robshaw, R. Sidney, and Y. Yin, "The RC6 block cipher. v1.1," Aug. 1998. Available at http://www.rsasecurity.com/rsalabs/rc6/
[13] A.A. Selcuk and A. Bicak, "On probability of success in differential and linear cryptanalysis," SCN 2002, LNCS 2576, pp.174–185, Springer-Verlag, 2003.
[14] S. Vaudenay, "An experiment on DES statistical cryptanalysis," ACM-CCS '96, pp.139–147, ACM Press, 1996.
[15] T. Shimoyama, M. Takenaka, and T. Koshiba, "Multiple linear cryptanalysis of a reduced round RC6," FSE 2002, LNCS 2365, pp.76–88, Springer-Verlag, 2002.
[16] M. Takenaka, T. Shimoyama, and T. Koshiba, "Theoretical analysis of χ^2 attack on RC6," IEICE Trans. Fundamentals, vol.E87-A, no.1, pp.28–35, Jan. 2004.
[17] B. Ryabko, "Adaptive chi-square test and its application to some cryptographic problems," Cryptology ePrint Archive, Report 2002/030 (2003), http://eprint.iacr.org/

Atsuko Miyaji received the B.Sc., the M.Sc., and Dr. Sci. degrees in mathematics from Osaka University, Osaka, Japan in 1988, 1990, and 1997 respectively. She joined Matsushita Electric Industrial Co., LTD from 1990 to 1998 and engaged in research and development for secure communication. She has been an associate professor at JAIST(Japan Advanced Institute of Science and Technology) since 1998. She has joined the computer science department of University of California, Davis since 2002. Her research interests include the application of projective varieties theory into cryptography and information security. She received the IPSJ Sakai Special Researcher Award in 2002, the Standardization Contribution Award in 2003, and Engineering Sciences Society: Certificate of Appreciation in 2005. She is a member of the International Association for Cryptologic Research, the Institute of Electronics, Information and Communication Engineers, the Information Processing Society of Japan, and the Mathematical Society of Japan.

Yuuki Takano received the B.E. degree from National Institution for Academic Degrees and University Evaluation, Japan in 2003, and M. info. Sc. degree from Japan Advanced Institute of Science and Technology (JAIST) in 2005. He is currently a Ph.D. student at School of Information Science of JAIST. His main research topics are security and peer-to-peer network.