Vol. 48 No. 9 IPSJ Journal Sep. 2007

Regular Paper

The security of RC6 against Asymmetric Chi-square Test Attack

Tomohiko Hinoue,[†,††] Atsuko Miyaji[†] and Takatomi Wada[†,††]

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. The best χ^2-attacks to RC6 whose security is guaranteed theoretically works on 16-round RC6 with 192- and 256-bit key but just 8-round RC6 with 128-bit key, because it recovers keys of RC6 symmetrically, which requires a time complexity of #plaintexts $\times 2^{54}$ and a memory complexity of 2^{80} for recovering one key. In this paper, we improve the χ^2-attack to reduce the time complexity. We give the theorem that evaluates the success probability of the χ^2-attack on RC6 without using any experimental result. Our key recovery attack recovers keys asymmetrically, which requires a time complexity of #plaintexts $\times 2^{31}$ and a memory complexity of 2^{52} for recovering one key. As a result, our key recovery attack works on 16-round RC6 with 192- and 256-bit key and 12-round RC6 with 128-bit key. In the case both of 196- and 256-bit keys, our attack surprisingly reduces the time and memory complexity compared with that of the previous attack. We also demonstrate our theorem on RC6-8/4/8 and make sure of the accuracy by comparing our approximation with the experimental results.

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) [15], 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 a significantly high value. The distinguishing search finds a condition for 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 singles 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 and has a symmetric structure [13]. This paper focuses on the 128-bit RC 6 with keys of 128, 192, and 256 bits, whose spec was required by the candidates of AES. A χ^2-attack [3],[8] was applied to RC6 by using the fact that a specific rotation in RC6 causes correlations between input and output, and the security of RC6 against the χ^2-attack is estimated only from the results of the distinguishing search [8]. That is, they focus on the χ^2-value, strictly speaking, which is given as the average of χ^2-value measured over part of a set of plaintexts. The χ^2-attacks to a simplified variant of RC6 such as RC6 without pre- or post-whitening [11] or RC6 without only post-whitening [5] have been further improved. The variance as well as the average of χ^2-value is taken into account when recovering a key in their attacks [5],[11]. 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. Thus, their χ^2-attack can recover a correct key in the high probability with a rather lower χ^2-value than the previous attack which uses only the average of χ^2-value [8]. In 2005 [12], they improve their attack to RC6 itself, which works on 16-round RC6 with 192- and 256-bit key. This gives a positive answer to an open question [8], that is, whether the χ^2-attack can be used to attack RC6 with 16 or more rounds. **Table 1** summarizes the previous attacks on RC6.

A theoretical analysis on χ^2-attack has been done [10],[12],[17]. The average of χ^2-value used in the distinguishing search [8] is theoretically computed by estimating the necessary number of plaintexts for the χ^2-value with a certain level theoretically in each round [17]. However, this is not enough to evaluate the success probability of χ^2-attack itself since there is a significant difference between the distinguishing search and the χ^2-attack as mentioned above. On the other hand, the theoretical difference between a distinguishing search and a χ^2-attack [5] on RC6 without post-whitening has been discussed [10].

† Japan Advanced Institute Science and Technology
†† This work was done when the author was in JAIST.

Table 1 Attacks on RC6.

attack	target RC6	rounds	#texts	memory
linear attack [1]	RC6	16	2^{119}	
multiple linear attack [16]	192-bit-key RC6	$14^{\dagger}$	$2^{119.68}$	
χ^2 attack [8]	128-bit-key RC6	$12^{\ddagger}$	2^{94}	2^{42}
	192-bit-key RC6	$14^{\ddagger}$	2^{108}	2^{74}
	256-bit-key RC6	$15^{\ddagger}$	2^{119}	2^{138}
χ^2 attack [11]	128-bit key RC6W$^{\diamond}$	17	$2^{123.9}$	2^{20}
χ^2 attack [5]	128-bit key RC6P[4]	16	$2^{117.84}$	2^{20}
χ^2 attack [12]	128-bit-key RC6	8	$2^{63.13}$	2^{80}
	192-bit-key RC6	16	$2^{127.20}$	
	256-bit-key RC6	16	$2^{127.20}$	
our χ^2 attack	128-bit-key RC6	12	$2^{109.21}$	2^{52}
	192-bit-key RC6	16	$2^{127.57}$	
	256-bit-key RC6	16	$2^{127.57}$	

†: A weak key of 18-round RC6 with 256-bit key can be recovered by $2^{126.936}$ plaintexts with the probability of about $1/2^{90}$.
‡: Estimation is done by using the experimental result of the distinguishing search.
$^{\diamond}$: RC6W means RC6 without pre- or post-whitening.
4: RC6P means RC6 without post-whitening.

They make use of the idea of the theoretical and experimental complexity analysis on the linear cryptanalysis [6),14)] 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 the distinguishing search, and, thus, they can succesfully estimate the security against χ^2-attack on RC6 with rather less work and memory. However, their estimation requires the experimental results of the distinguishing search. The theoretical success probability of a χ^2-attack was done for the first time in 2005 [12]. They give the theorem that evaluates the success probability of χ^2-attack [5] on RC6 without post-whitening and their χ^2-attack on RC6 itself.

In summary, the best attacks to RC6 whose security is guaranteed theoretically work on 16-round RC6 with 192- and 256-bit key but just 8-round RC6 with 128-bit key. Because their attack computes the χ^2-values on a symmetric part for each 54-bit key of the post-whitening keys at once and, thus, it requires the time complexity of the number of plaintexts $\times 2^{54}$ to recover one key. As a result, in the case of 128-bit key, it just works on 8 rounds with $2^{63.13}$ plaintexts and $2^{117.13}$ time complexity; in the case of 196- and 256-bit key, it works on 16 rounds with $2^{127.20}$ plaintexts, $2^{181.20}$ time complexity, and 2^{80} memory complexity.

In this paper, we improve the χ^2-attack to reduce the time and memory complexity. We give the theorem that evaluates the success probability of the χ^2-attack on RC6 without using any experimental result. Our key recovery attack is totally different from the previous researches because our attack computes the χ^2-values on an asymmetric part and recovers 1 post-whitening key and 2-bit of both another whitening key and a subkey in the final round. As a result, our attack particularly improves the time and memory complexity to the number of plaintexts $\times 2^{31}$ and 2^{52} memory complexity to recover one key, respectively. For example, in the case of RC 6 with 128-bit key, our attack works on 12-round RC6 with a 128-bit key by using $2^{95.52}$ plaintexts and $2^{126.52}$ time complexity. In the cases of both 196- and 256-bit keys, our attack works on 16-round RC6 with a time complexity of $2^{158.57}$, which is suprisingly less than that of the previous attack [12]. We also demonstrate our theorem on RC6-8/4/8 and make sure of the accuracy by comparing our approximation with the experimental results.

This paper is organized as follows. Section 2 summarizes the notation, RC6 algorithms, the χ^2-test, and the statistical facts used in this paper. Section 3 reviews the previous χ^2-attack against RC6. Section 4 improves the χ^2-attack on RC6 to reduce the time complexity 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 RC6-8/4/8. A conclusion 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 in Section 5.

2. Preliminary

We summarize the χ^2-test, statistical facts, and RC6 algorithm [13], 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:

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

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

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

The following Theorems 1 and 2 on χ^2-statistic are used in this paper:

Theorem 1 [18] 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 [18] 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 $V_{H_1}(\chi^2) = 2(m-1) + 4\,n\theta$, 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 research 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.

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

Table 2 presents the threshold for 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 whose 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 the 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 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 notations.

- $\{0,1\}^k$:k-bit data
- $\mathrm{lsb}_n(X)$: least significant n-bit of X;
- $\mathrm{msb}_n(X)$: most significant n-bit of X;
- $X^{[i,j]}$: i-th to j-th 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;
- $f(x)$: $x \times (2x+1)$;
- $F(x)$: $f(x) \pmod{2^w} \lll \log_2 w$;
- $x \parallel y$: 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:
   $t = F(B_i)$; $u = F(D_i)$;
   $A_{i+1} = B_i$; $C_{i+1} = D_i$;
   $B_{i+1} = ((C_i \oplus u) \lll t) + S_{2i+1}$;
   $D_{i+1} = ((A_i \oplus t) \lll u) + S_{2i}$;
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 write simply RC6 if we deal with RC6 of 32-bit-word plaintexts.

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

2.3 A Transition Matrix

A transition matrix describes the input-output transition, which was introduced by Vaudenay [15]. The transition matrix is applied to RC6-8 and RC6-32 [17]: it computes 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. The Previous χ^2 Attack against RC6

This section reviews the previous key recovery attack against RC6, Attack 1, together with the theorem that computes the success probability.

Before reviewing the algorithm, let us use the following notation:

- $\mathcal{U}_0 = \{u \in \{0,1\}^{32} | \mathrm{msb}_5(u \times (2u+1)) = 0\}$,
- $(u_a, u_c) \in \mathcal{U}_0 \times \mathcal{U}_0$,
- $t_a = A_{r+2} - u_a$,
- $t_c = C_{r+2} - u_a$,
- $v = \mathrm{lsb}_5(B_0) \parallel \mathrm{lsb}_5(D_0)$,
- $z = \mathrm{lsb}_3(B_{r+2}) \parallel \mathrm{lsb}_3(D_{r+2})$.

Attack 1 [12]

1. Encrypt a plaintext (A_0, B_0, C_0, D_0) 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. For each t_a and t_c, compute the average $ave[t_a][t_c]$ of $\{\chi^2[t_a][t_c][v]\}_v$.
5. Output (t_a, t_c) with the highest $ave[t_a][t_c]$ as (S_{2r+2}, S_{2r+3}).

Attack 1 calculates the χ^2-value on $z = \mathrm{lsb}_3(B_{r+2}) \parallel \mathrm{lsb}_3(D_{r+2})$ 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 $\mathrm{lsb}_3(A_r) \parallel \mathrm{lsb}_3(C_r)$, which is output of $(r-1)$-round RC6P because the addition keeps the χ^2-value. Thus, we succeed in skipping the post-whitening and arrive at the probability density function of distribution of χ^2-value with a correct key in r-round RC6 is given by

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

where $\mu_{d[r,n]}(\sigma^2_{d[r,n]})$ is mean (variance) of distribution of χ^2-values on $\mathrm{lsb}_3(A_{r+1}) \parallel \mathrm{lsb}_3(C_{r+1})$ of r-round RC6P by using 2^n plaintexts. The mean and variance, $\mu_{d[r,n]}$ and $\sigma^2_{d[r,n]}$, are derived theoretically, by computing

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

where the summation is over $\mathrm{lsb}_3(A_{r+1}) \parallel \mathrm{lsb}_3(C_{r+1}) \in \{0,1\}^6$ and $P(\mathrm{lsb}_3(A_{r+1}) \parallel \mathrm{lsb}_3(C_{r+1}))$ is the probability of occurrence of $\mathrm{lsb}_3(A_{r+1}) \parallel \mathrm{lsb}_3(C_{r+1})$. $\theta_{1,r}$ can be derived theoretically by TM in Section 2.

In the case of wrong keys, this is exactly equivalent to computing the χ^2-value on $\mathrm{lsb}_3(A_{r+2}) \parallel \mathrm{lsb}_3(C_{r+2})$, which is the output of $(r+1)$-round RC6P. Thus, we arrive at the probability density function of distribution of χ^2-value with a wrong key in r-round RC6 is given as

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

The next success probability follows from the above discussion.

Theorem 4 [12] The success probability of Attack 1 on r-round RC6 is given theoretically as

$$\begin{aligned} & Ps_{rc6}(n) \\ &= \int_{-\infty}^{\infty} f_{c[r,n]}(x) \cdot \left(f_{w[r,n]}(u) du \right)^{2^{64}-1} dx \\ &= \int_{-\infty}^{\infty} \phi_{(2^6 - 1 + m\theta_{1,r-1}, (2(2^6-1) + 4\, m\theta_{1,r-1})/2^{10})}(x) \end{aligned}$$

Table 3 #texts necessary for $Ps_{rc6}(n) \geq 0.95$ (From Theorem 4 [12]).

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†	$2^{85.06}$	$2^{101.10}$	$2^{117.13}$	$2^{133.15}$	$2^{149.17}$	$2^{165.19}$	$2^{181.20}$	$2^{197.21}$
memory‡	2^{80}							

†: the number incrementing a counter `count`.
‡: the size of a counter `count`.

Table 4 Theoretical and experimental success probability of RC6-8/4/8 (Attack 1) [12].

#texts	2^{17}	2^{18}	2^{19}	2^{20}	memory
Theoretical	0.00	0.05	0.73	1.00	2^{28}
Experimental	0.00	0.04	0.76	1.00	
Time	–	15.3	30.6	61.1	

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

where 2^n is the number of texts, $\theta_{1,r} = 2^6 \sum \left(P(\mathrm{lsb}_3(A_{r+1}) \parallel \mathrm{lsb}_3(C_{r+1})) - \frac{2^n}{2^6}\right)^2$, and $m = 2^{n-20}$.

Table 3 shows the necessary number of texts computed by Theorem 4 and the time complexity which makes the success probability of Attack 1 on RC6 95% or more. The time complexity is estimated by the number incrementing a counter `count`, which is the dominant step of Attack 1. The memory complexity is estimated by the size of `count`, which is equal to 2^{80}. The number of available texts is bounded by 2^{128} in Attack 1 and the time complexity is #texts $\times\, 2^{27\times 2}$ since Attack 1 recovers both post-whitening keys at once. Therefore, Attack 1 works on an 128-bit-key RC6 with up to only 8 rounds.

Table 4 shows the theoretical and experimental results of Attack1 against 4-round RC6-8. Our platforms are Cray XT3(AMD Opteron150 2.4GHz × 20). All attacks use 100 keys and $2^{17}, 2^{18}, 2^{19}$, or 2^{20} kinds of plaintexts, denoted by #texts, and thus conduct $10^2 \times$ #texts trials in total.

4. Our χ^2 Attack against RC6

This section improves a key recovery attack against RC6, Attack 2, and then gives the theorem that computes the success probability. We also implement Attack 2 on RC6-8/4/8 and demonstrate the accuracy of the theorem. **Figure 1** shows an overview of Atrack 2.

4.1 Key Recovery Attack

The main feature of Attack 2 is to deal with RC 6 asymmetrically and recover S_{2r+2}, $\mathrm{lsb}_2(S_{2r+3})$, and $\mathrm{lsb}_2(S_{2r+1})$ by decrypting $\mathrm{lsb}_3(B_{r+2})$ with 1 round, set to z_c, and measuring the characteristic value based on the χ^2-value of $z_c \parallel \mathrm{lsb}_3(D_{r+2})$ for each key candidate. Before showing the algorithm, let us use the following notation:

- $\mathcal{U}_{27} = \{u \in \{0,1\}^{32} | \mathrm{msb}_5(u \times (2u+1)) = 27\} \ni u$,
- $(y_b, y_d) = (\mathrm{lsb}_3(B_{r+2}), \mathrm{lsb}_3(D_{r+2}))$,
- $(x_c, x_a) = (\mathrm{lsb}_5(F(A_{r+1})), \mathrm{lsb}_5(F(C_{r+1})))$,
- $v = \mathrm{lsb}_5(B_0) \parallel \mathrm{lsb}_5(D_0)$
- $(s_1, s_2, s_3) = (S_{2r+2}, \mathrm{lsb}_2(S_{2r+3}), \mathrm{lsb}_2(S_{2r+1}))$,
- $s = s_1 \parallel s_2 \parallel s_3$,
- z_c is the decryption of y_b by $(0 \parallel s_2, 0 \parallel s_3)$,

where x_a (resp. x_c) is the rotation amounts on A_r (resp. C_r) in the r-th round. Note here that we can decrypt y_b by using $(0 \parallel s_2, 0 \parallel s_3)$ whenever $x_c = 27$.

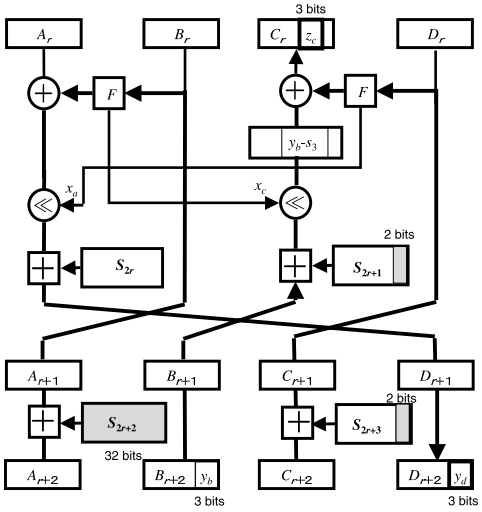


Fig. 1 The overview of Algorithm 2.

Attack 2

1. Encrypt a plaintext (A_0, B_0, C_0, D_0) to $(A_{r+2}, B_{r+2}, C_{r+2}, D_{r+2})$.
2. For each u, s_2, and s_3,
   - set both $s_1 = A_{r+2} - u$ and $s = s_1 \parallel s_2 \parallel s_3$;
   - decrypt y_b with a key of $(0 \parallel s_2,\ 0 \parallel s_3)$ to z_c;

- set $z = z_c \parallel y_d$; and
- update each array by incrementing count$[s][v][z]$.

3. For each s and v, compute the χ^2-value $\chi^2[s][v]$.
4. For each s, compute the average $ave[s]$ of $\{\chi^2[s][v]\}_v$.
5. Output s with the highest $ave[s]$ as $(S_{2r+2}, \mathrm{lsb}_2(S_{2r+3}), \mathrm{lsb}_2(S_{2r+1}))$.

Attack 2 calculates the χ^2-value on $z = z_c \parallel \mathrm{lsb}_3(D_{r+2})$ by using such plaintexts that make the final-round rotation 27 for each key candidate of S_{2r+2}. For a correct key, z_c is exactly equal to $C_r^{[5,7]} = D_{r-1}^{[5,7]}$ and, thus, Attack 2 computes the χ^2-value on $D_{r-1}^{[5,7]} \parallel \mathrm{lsb}_3(D_{r+2}) = D_{r-1}^{[5,7]} \parallel \mathrm{lsb}_3(D_{r+1})$ for a correct key. For a wrong key, z_c is not equal to $D_{r-1}^{[5,7]}$, thus, wrong keys output lower χ^2-value on $z_c \parallel \mathrm{lsb}_3(D_{r+2})$ compared to a correct key. Attack 2 recovers a correct key by using such differences in the χ^2-value of z.

Remark:

1. The most significant bit of z_c is useless from the point of view of χ^2-value since it outputs the same χ^2-value in each case of $(0 \parallel s_2, 0 \parallel s_3)$, $(1 \parallel s_2, 0 \parallel s_3)$, $(0 \parallel s_2, 1 \parallel s_3)$, and, $(1 \parallel s_2, 1 \parallel s_3)$. This is why we have to evaluate the χ^2-value on one-additional bits.
2. The correlations between plaintext and ciphertext can be measured by the χ^2-value on concatenation of $A_r \parallel C_r$ or $B_r \parallel D_r$. This is why we need y_d in addition to y_b to measure the correlations even if y_d is independent from the recovered key s.

4.2 Theoretical Success Probability

Here we discuss the theoretical success probability of our attack. There exists an important difference between Attacks 1 and 2 in the probability density function of distribution of χ^2-value with a wrong key. In the case of Attack 1, each distribution of χ^2-value with each wrong key is assumed to be independent and approximately equal to each other, which is used in the theoretical analysis of the previous attacks to RC6 [5),10)~12)]. In fact, Attack 1 uses the condition of which the final-round rotation is 0 for a key candidate in the same way as other previous attacks. Therefore, any wrong key influences the output of F function and makes the final-round rotation random even if it is different from a correct key with only 1 bit.

However, our attack cannot assume that each distribution of χ^2-value with each wrong key is independent and approximately equal to each other. Our attack recovers S_{2r+2}, $\mathrm{lsb}_2(S_{2r+3})$, and $\mathrm{lsb}_2(S_{2r+1})$, of which only S_{2r+2} is input of F-function. Therefore, we have to deal with wrong keys separately according to whether S_{2r+2} is a wrong key or a correct key. Where S_{2r+2} is a wrong key, a wrong S_{2r+2} influences the output of F function and makes the final-round rotation random. Therefore, we could estimate the χ^2-value of z_c by that of the 1-round encryption of y_b, which means that the χ^2-value of $z = z_c \parallel y_d$ may be estimated by that of $\mathrm{lsb}_3(D_{r+3}) \parallel \mathrm{lsb}_3(D_{r+2}) = \mathrm{lsb}_3(D_{r+3}) \parallel \mathrm{lsb}_3(D_{r+1})$[☆]. Where S_{2r+2} is a correct key, $z_c = C_r^{[5,7]}$ is not necessarily a random number in the following reason. Let us assume that S_{2r+2} is correct and focus on each least bit of $y_b^{[0,0]}$, $z_c^{[0,0]} = C_r^{[5,5]}$, $S_{2r+1}^{[0,0]}$, and $S_{2r+3}^{[0,0]}$. Then, $C_r^{[5,5]}$ can be decrypted correctly if both $S_{2r+1}^{[0,0]}$ and $S_{2r+3}^{[0,0]}$ have only to be correct. On the other hand, $C_r^{[6,6]}$ becomes a random bit under the randomness of $S_{2r+1}^{[1,1]}$ and $S_{2r+3}^{[1,1]}$ even if both $S_{2r+1}^{[0,0]}$ and $S_{2r+3}^{[0,0]}$ are correct. **Table 5** summarizes the correct-wrong relation between $\mathrm{lsb}_2(S_{2r+1}) \parallel \mathrm{lsb}_2(S_{2r+3})$ and $C_r^{[5,6]}$ in the case of which S_{2r+2} is correct[☆☆]. Thus, if S_{2r+2} is correct; and $\mathrm{lsb}_2(S_{2r+1}) \parallel \mathrm{lsb}_2(S_{2r+3}) =$ wcwc, ccwc, wccc, then $C_r^{[5,6]}$ can be decrypted correctly (resp. wrongly) in each probability of 50 % and the χ^2-value of $z = z_c \parallel y_d$ can be estimated by that of $\mathrm{lsb}_3(D_{r+3}) \parallel \mathrm{lsb}_3(D_{r+2}) = \mathrm{lsb}_3(D_{r+3}) \parallel \mathrm{lsb}_3(D_{r+1})$ (resp. that of $D_{r-1}^{[5,7]} \parallel \mathrm{lsb}_3(D_{r+2}) = D_{r-1}^{[5,7]} \parallel \mathrm{lsb}_3(D_{r+1})$).

Table 5 The relation between $\mathrm{lsb}_2(S_{2r+1}) \parallel \mathrm{lsb}_2(S_{2r+3})$ and $C_r^{[5,6]}$ in the case of a correct S_{2r+2}.

$S_{2r+1}^{[1,1]} S_{2r+1}^{[0,0]} S_{2r+3}^{[1,1]} S_{2r+3}^{[0,0]}$	$C_r^{[6,6]} C_r^{[5,5]}$
*w*w	*w
*w*c	*w
*c*w	*w
*c*c	*c

w, c, or * means a wrong, a correct, or a random bit, respectively.

The above discussion on the probability density function of the distribution of χ^2-value with a wrong key is summarized as follows.

(1) The χ^2-value of z is estimated by that

☆ $(A_{r+3}, B_{r+3}, C_{r+3}, D_{r+3})$ is the output after $r+2$-round encryption.

☆☆ The most significant bit of z_c, $C_r^{[7,7]}$, has no effect on recovering a key as mentioned in Section 4.1.

of $\mathrm{lsb}_3(D_{r+3}) \parallel \mathrm{lsb}_3(D_{r+1})$ if S_{2r+2} is wrong.

(2) The χ^2-value of z is estimated by that of $\mathrm{lsb}_3(D_{r+3}) \parallel \mathrm{lsb}_3(D_{r+1})$ in the probability of 50% and that of $D_{r-1}^{[5,7]} \parallel \mathrm{lsb}_3(D_{r+1})$ in the probability of 50% if S_{2r+2}, $\mathrm{lsb}_1(S_{2r+1})$ and $\mathrm{lsb}_1(S_{2r+3})$ are correct.

(3) The χ^2-value of z is estimated by that of $\mathrm{lsb}_3(D_{r+3}) \parallel \mathrm{lsb}_3(D_{r+1})$ if S_{2r+2} is correct; and either $\mathrm{lsb}_1(S_{2r+1})$ or $\mathrm{lsb}_1(S_{2r+3})$ is wrong.

From the above discussion, the following theorem follows.

Theorem 5 The success probability of Attack 2 on r-round RC6 is given theoretically as

$$\begin{aligned} & Ps_{rc6}(n) \\ &= \int_{-\infty}^{\infty} \phi_{(2^6-1+m\tilde{\theta}_r,(2(2^6-1)+4m\tilde{\theta}_r)/2^{10})}(x) \\ &\cdot \left(\int_{-\infty}^{x} \phi_{(2^6-1+m\bar{\theta}_r,(2(2^6-1)+4m\bar{\theta}_r)/2^{10})}(u)du \right)^3 \\ &\cdot \left(\int_{-\infty}^{x} \phi_{(2^6-1+m\theta_r,(2(2^6-1)+4m\theta_r)/2^{10})}(u)du \right)^{2^{36}-4} dx, \end{aligned} \tag{5}$$

where 2^n is the number of texts, $m = 2^{n-15}$, $\theta_r = 2^6 \sum \left(P(\mathrm{lsb}_3(D_{r+3}) \parallel \mathrm{lsb}_3(D_{r+1})) - \frac{2^n}{2^6}\right)^2$ with the summation over $\mathrm{lsb}_3(D_{r+3}) \parallel \mathrm{lsb}_3(D_{r+2}) \in \{0,1\}^6$, $\tilde{\theta}_r = 2^6 \sum \left(P(D_{r-1}^{[5,7]} \parallel \mathrm{lsb}_3(D_{r+1})) - \frac{2^n}{2^6}\right)^2$ with the summation over $D_{r-1}^{[5,7]} \parallel \mathrm{lsb}_3(D_{r+1}) \in \{0,1\}^6$, and $\bar{\theta}_r = (\theta_r + \tilde{\theta}_r)/2$.

Remark: Theorem 5 gives the success probability of Attack 2 on r-round RC6 assuming that the χ^2-value of $z_c \parallel y_d$ is that of $\mathrm{lsb}_3(D_{r+3}) \parallel y_d$ if S_{2r+2} is wrong, where $\mathrm{lsb}_3(D_{r+3})$ is the 1-round encryption of y_b. So, we still use the assumption on the distribution of χ^2-value in wrong keys although the assumption seems to be reasonable. We remark that the higher bound of χ^2-value of $z_c \parallel y_d$ is that of $y_b \parallel y_d$ in the case of wrong keys.

In order to evaluate Eq. (5), we have to compute the exponentiation $2^{36} - 4$ on an integral part, which needs much time complexity. Therefore, we use the following approximation to reduce the time complexity.

Lemma 1 The success probability of $Ps_{rc6}(n)$ is approximated to $\widetilde{Ps}_{rc6}(n)$, that is $Ps_{rc6}(n) \simeq \widetilde{Ps}_{rc6}(n)$, where

$$\begin{aligned} & \widetilde{Ps}_{rc6}(n) \\ &= \left\{ \int_{-\infty}^{\infty} \phi_{(2^6-1+m\tilde{\theta}_r,(2(2^6-1)+4m\tilde{\theta}_r)/2^{10})}(x) \right. \\ &\quad \left. \left(\int_{-\infty}^{x} \phi_{(2^6-1+m\bar{\theta}_r,(2(2^6-1)+4m\bar{\theta}_r)/2^{10})}(u)du \right) dx \right\}^3 \\ &\cdot \left\{ \int_{-\infty}^{\infty} \phi_{(2^6-1+m\tilde{\theta}_r,(2(2^6-1)+4m\tilde{\theta}_r)/2^{10})}(x) \right. \\ &\quad \left. \left(\int_{-\infty}^{x} \phi_{(2^6-1+m\theta_r,(2(2^6-1)+4m\theta_r)/2^{10})}(u)du \right) dx \right\}^{2^{36}-4}, \end{aligned}$$

$m = 2^{n-15}$; θ_r and $\tilde{\theta}_r$ are defined in Theorem 5.

proof: The following approximation stands since $\phi_{(2^6-1+m\tilde{\theta}_r,(2(2^6-1)+4m\tilde{\theta}_r)/2^{10})}(x)$, $\phi_{(2^6-1+m\bar{\theta}_r,(2(2^6-1)+4m\bar{\theta}_r)/2^{10})}(x)$, or $\phi_{(2^6-1+m\theta_r,(2(2^6-1)+4m\theta_r)/2^{10})}(u)$ is a probability density function of distribution of χ^2-values on each key candidate:

$$\begin{aligned} & Ps_{rc6}(n) \\ &= \int_{-\infty}^{\infty} \phi_{(2^6-1+m\tilde{\theta}_r,(2(2^6-1)+4m\tilde{\theta}_r)/2^{10})}(x) \\ &\cdot \left(\int_{-\infty}^{x} \phi_{(2^6-1+m\bar{\theta}_r,(2(2^6-1)+4m\bar{\theta}_r)/2^{10})}(u)du \right)^3 \\ &\cdot \left(\int_{-\infty}^{x} \phi_{(2^6-1+m\theta_r,(2(2^6-1)+4m\theta_r)/2^{10})}(u)du \right)^{2^{36}-4} dx \\ &\simeq \left\{ \int_{-\infty}^{\infty} \phi_{(2^6-1+m\tilde{\theta}_r,(2(2^6-1)+4m\tilde{\theta}_r)/2^{10})}(x) \right. \\ &\quad \left. \cdot \left(\int_{-\infty}^{x} \phi_{(2^6-1+m\bar{\theta}_r,(2(2^6-1)+4m\bar{\theta}_r)/2^{10})}(u)du \right) dx \right\}^3 \\ &\cdot \left\{ \int_{-\infty}^{\infty} \phi_{(2^6-1+m\tilde{\theta}_r,(2(2^6-1)+4m\tilde{\theta}_r)/2^{10})}(x) \right. \\ &\quad \left. \cdot \left(\int_{-\infty}^{x} \phi_{(2^6-1+m\theta_r,(2(2^6-1)+4m\theta_r)/2^{10})}(u)du \right) dx \right\}^{2^{36}-4} \\ &= \widetilde{Ps}_{rc6}(n) \end{aligned}$$

∎

Table 6 shows both θ_r and $\tilde{\theta}_r'$ on RC6 in each round, where $\tilde{\theta}_r'$ is computed by the value of

$$\tilde{\theta}_r' = 2^6 \sum \left(P(\mathrm{lsb}_3(D_{r-1}) \parallel \mathrm{lsb}_3(D_{r+1})) - \frac{2^n}{2^6} \right)^2$$

Table 6 θ_r and $\tilde{\theta}_r$ for RC6 in each round (estimation).

rounds	θ_r	$\tilde{\theta}_r'$ (estimation of $\tilde{\theta}_r$)
4	0.603×10^{-9}	0.452×10^{-4}
6	0.873×10^{-14}	0.735×10^{-9}
8	0.143×10^{-18}	0.915×10^{-14}
10	0.253×10^{-23}	0.129×10^{-18}
12	0.311×10^{-28}	0.208×10^{-23}
14	0.683×10^{-33}	0.273×10^{-28}
16	0.834×10^{-38}	0.471×10^{-33}
18	0.134×10^{-42}	0.666×10^{-38}

Table 7 #texts necessary for $Ps_{rc6}(n) \geq 0.95$ (From Lemma 1).

r	4	6	8	10	12	14	16	18
# texts	$2^{31.29}$	$2^{47.20}$	$2^{63.49}$	$2^{79.61}$	$2^{95.52}$	$2^{111.75}$	$2^{127.57}$	$2^{143.68}$
time complexity†	$2^{62.29}$	$2^{78.20}$	$2^{94.49}$	$2^{110.61}$	$2^{126.52}$	$2^{142.75}$	$2^{158.57}$	$2^{174.68}$
memory‡	2^{52}							

†: the number incrementing a counter `count`.
‡: the size of a counter `count`.

Table 8 Theoretical and experimental success probability of RC6-8/4/8 (Attack 2)(the average of 100 trials).

#texts	2^{18}	2^{19}	2^{20}	2^{21}	2^{22}	memory
Theoretical	0.01	0.09	0.30	0.90	1.00	2^{24}
Experimental	0.00	0.03	0.15	0.78	1.00	
Time(sec)	9.7	19.4	38.8	82.2	165.6	

with the summation over $\mathrm{lsb}_3(D_{r-1}) \parallel \mathrm{lsb}_3(D_{r+1}) \in \{0,1\}^6$. In Theorem 5, $\tilde{\theta}_r$ is defined as

$$\tilde{\theta}_r = 2^6 \sum \left(P(D_{r-1}^{[5,7]} \parallel \mathrm{lsb}_3(D_{r+1})) - \frac{2^n}{2^6} \right)^2 ,$$

in which the computation of `TM` requires too much memory compared with the above $\tilde{\theta}_r'$. Therefore, we use the estimation $\tilde{\theta}_r'$ instead of $\tilde{\theta}_r$. Compared with $\tilde{\theta}_r$, $\tilde{\theta}_r'$ is slightly higher than $\tilde{\theta}_r$ in the lower round r since bias of input influences that of output in the lower round. However, the higher the round r is, the fewer the difference between $\tilde{\theta}_r'$ and $\tilde{\theta}_r$ would be.

By using the results of Table 6, **Table 7** shows the necessary number of texts and time complexity which make the success probability of Attack 2 on RC6 95% or more. The necessary number of texts is computed by Lemma 1. The time complexity is estimated by the number incrementing a counter `count`, which is the dominant step of Attack 2. The memory complexity is estimated by the size of `count`, which is equal to 2^{52}. The number of available texts is bounded by 2^{128} in Attack 2 and the time complexity is $\#\text{texts} \times 2^{27+4}$ since Attack 2 recovers 1 post-whitening key, 2 bits of another post-whitening key, and 2 bits of 1 subkey in the final round at once. Compared with Attack 1 in Section 3, whose time or memory complexity is $\#\text{texts} \times 2^{27\times 2}$ or 2^{80}, our attack surprisingly reduces the time or memory complexity, respectively. In fact, the previous attack works on a 128-bit-key RC6 with up to 8 rounds by using $2^{63.1}$ plaintexts and $2^{117.1}$ time complexity. However, our attack can recover a key on an 128-bit-key RC6 with up to 12 rounds by using $2^{95.52}$ plaintexts and $2^{126.52}$ time complexity.

4.3 Success Probability of Attack 2 on RC6-8

We also demonstrate Theorem 5 on RC6-8/4/8. **Table 8** shows the theoretical and experimental results. Our platforms are the same as that of the experimental results on Attack 1, described in Section 3. The theoretical success probability is slightly higher than the experimental success probability for the following reason:

1. The χ^2-value of correct keys is estimated to be slightly higher by using $\tilde{\theta}_r'$ instead of $\tilde{\theta}_r$. In fact, the experiments are done in the 4th round, and, thus, $\tilde{\theta}_r'$ seems to be higher than $\tilde{\theta}_r$.
2. The theoretical success probability is estimated by setting the χ^2-value of $z_c \parallel y_d$ is that of $\mathrm{lsb}_3(D_{r+3}) \parallel y_d$ if S_{2r+2} is wrong.

Let us compare Attack 2 to RC6-8/4/8 with Attack 1 to RC6-8/4/8. Our algorithm runs with the memory of 2^{24} while Attack 1 needs the memory of 2^{28}. The time of Attack 2 (resp. Attack 1) is about 2^{5+4} encryptions (resp. 2^{5+5} encryptions) of RC6-8/4/8, and so we expect that Attack 2 runs half as much as that of Attack 1. We see that Attack 2 runs slightly longer than half of the time of Attack 1 when both use the same number of plain texts. This is because Attack 2 needs to decrypt ciphertexts by 1 round in addition to the same procedure as Attack 1. Attack 2 needs # texts to make the success probability 100 % more than Attack 1. In fact, Attack 1 can be expected to have more correlation than Attack 2 because the χ^2-value of correct keys in Attack 1 (resp. Attack 2) is evaluated by that on $\mathrm{lsb}_3(A_r) \parallel \mathrm{lsb}_3(C_r)$ (resp. $\mathrm{lsb}_3(D_{r+1}) \parallel C_r^{[5,7]}$). Therefore, especially in the case of lower rounds such as RC6-8/4/8, the difference influences the necessary number

of texts. However, in the case of higher rounds such as RC6 with 10 rounds or more, the difference seems to make only a little impact on the necessary number of texts. Instead, the memory size and the time complexity become more important and serious as we see in Table 3 and Table 7.

5. Concluding Remarks

In this paper, we have improved the χ^2-attack on RC6 to reduce the time and memory complexity and proved the theorem that evaluates the success probability in the χ^2-attacks. 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 effectively estimate the success probability in the χ^2-attacks against RC6-8/4/8.

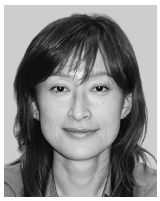
Acknowledgments The authors express our gratitude to anonymous referees for invaluable comments.

References

1) Contini, S., Rivest, R., Robshaw, M. and Yin, Y.: The Security of the RC6 Block Cipher. v 1.0, (Aug. 20, 1998). Available at http://www.rsasecurity.com/rsalabs/rc6/
2) Freund, R.J. and Wilson, W.J.: *Statistical Method*, Academic Press, San Diego (1993).
3) Gilbert, H., Handschuh, H., Joux, A. and Vaudenay, S.: A Statistical Attack on RC6, *FSE 2000*, LNCS, Vol.1978, pp.64–74, Springer-Verlag (2000).
4) Handschuh, H. and Gilbert, H.: χ^2 Cryptanalysis of the SEAL Encryption Algorithm, *FSE '97*, LNCS, Vol.1267, pp.1–12, Springer-Verlag (1997).
5) Isogai, N., Matsunaka, T. and Miyaji, A.: Optimized χ^2-attack against RC6, *ANCS 2003*, LNCS, Vol.2846, pp.16–32, Springer-Verlag (2003).
6) Junod, P.: On the Complexity of Matsui's Attack, *SAC 2001*, LNCS, Vol.2259, pp.199–211, Springer-Verlag (2001).
7) Kelsey, J., Schneier, B. and Wagner, D.: Mod n Cryptanalysis, with applications against RC5P and M6, *FSE '99*, LNCS, Vol.1636, pp.139–155, Springer-Verlag (1999).
8) Knudsen, L. and Meier, W.: Correlations in RC6 with a reduced number of rounds, *FSE 2000*, LNCS, Vol.1978, pp.94–108, Springer-Verlag (2000).
9) Knuth, D.: *The art of computer programming*, Vol.2, Seminumerical Algorithms, 2nd ed., Addison-Wesley, Reading, Mass (1981).
10) Matsunaka, T., Miyaji, A. and Takano, Y.: Success probability in χ^2-attacks, *ACNS 2004*, LNCS, Vol.3089, pp.310–325, Springer-Verlag (2004).
11) Miyaji, A. and Nonaka, M.: Cryptanalysis of the Reduced-Round RC6, *ICICS 2002*, LNCS, Vol.2513, pp.480–494, Springer-Verlag (2002).
12) Miyaji, A. and Takano, Y.: On the Success Probability of χ^2-attack on RC6, *ACISP 2005*, LNCS, Vol.3574, pp.61–75, Springer-Verlag (2005).
13) Rivest, R., Robshaw, M., Sidney, R. and Yin, Y.: The RC6 Block Cipher. v1.1, (Aug. 1998). Available at http://www.rsasecurity.com/rsalabs/rc6/
14) Selcuk, A.A. and Bicak, A.: On probability of success in differential and linear cryptanalysis, *SCN 2002*, LNCS, Vol.2576, pp.174–185, Springer-Verlag (2003).
15) Vaudenay, S.: An Experiment on DES Statistical Cryptanalysis, *ACM-CCS '96*, pp.139–147, ACM Press (1996).
16) Shimoyama, T., Takenaka, M. and Koshiba, T.: Multiple linear cryptanalysis of a reduced round RC6, *FSE 2002*, LNCS, Vol.2365, pp.76–88, Springer-Verlag (2002).
17) Takenaka, M., Shimoyama, T. and Koshiba, T.: Theoretical Analysis of χ^2 Attack on RC6, *IEICE Trans.*, Vol.E87-A, No.1, pp.28–35 (2004).
18) Ryabko, B.: Adaptive chi-square test and its application to some cryptographic problems, *Cryptology ePrint Archive, Report 2002/030* (2003). http://eprint.iacr.org/

(Received December 11, 2006)
(Accepted June 5, 2007)
(Online version of this article can be found in the IPSJ Digital Courier, Vol.3, pp.000–000.)

Tomohiko Hinoue received the B.Eng. degree from the Shimane University in 2004 and the M.Info.Sci. degree from the Japan Advanced Institute of Science and Technology in 2006.



Atsuko Miyaji received the B. Sc., the M. Sc., and the 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 the University of California, Davis since 2002. Her research interests include the application of number theory into cryptography and information security. She received the IPSJ Sakai Special Researcher Award in 2002, the Standardization Contribution Award in 2003, Engineering Sciences Society: Certificate of Appreciation in 2005, the AWARD for the contribution to CULTURE of SECURITY in 2007, and the IPSJ/ITSCJ Project Editor Award in 2007. 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.

Takatomi Wada received the B.Eng. degree from the National Defense Academy in 2002 and the M.Info.Sci. degree from the Japan Advanced Institute of Science and Technology in 2007.