社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2006－CSEC－34 (21)
2006／7／20

非対称カイ二乗検定攻撃の解読可能段数の再評価

和田 崇臣† 宮地 充子† 樋上 智彦††

† 北陸先端科学技術大学院大学情報科学研究科
〒923-1293 石川県能美市旭台 1-1
†† オムロン株式会社
〒600-8530 京都市下京区塩小路通堀川東入
E-mail: †t-wada@jasit.ac.jp, ††miyaji@jaist.ac.jp

あらまし RC6 は 1998 年に Rivest らによって提案された算術演算とビットシフトで構成されるソフトウェア実装に適した共通鍵ブロック暗号である．RC6 に対する攻撃では χ^2 攻撃が有効で，数々の χ^2 攻撃の研究が発表されている．SCIS2006 で発表された非対称 χ^2 検定攻撃は効率的に RC6 の鍵を復元する [8]．しかし，その成功確率の理論値は実験値と比較して非常に高く見積もられている．これは誤鍵の χ^2 値の分布はすべて等しいという仮定で成功確率の理論値を求めたためである．そこで，本論文では誤鍵での χ^2 値の分布の仮定を見直し，非対称 χ^2 検定攻撃のより厳密な理論的成功確率を導出した．

キーワード ブロック暗号，RC6，χ^2 攻撃，統計的解析

Reconsideration of the security of RC6 against asymmetric chi-square test attack

Takatomi WADA†, Atsuko MIYAJI†, and Tomohiko HINOUE††

† School of Information Science, Japan Advanced Institute of Science and Technology(JAIST)
1-1, Asahidai, Nomishi, Ishikawa 923-1293 Japan
†† OMRON Corporation
3-4-10 Toranomon Minato-ku, Tokyo, 105-0001 Japan
E-mail: †t-wada@jasit.ac.jp, ††miyaji@jaist.ac.jp

Abstract RC6 is a block cipher proposed by Rivest in 1998, which consistsof the arithmetic operations and bit-shifts. So, it is suitable for the software implementation. χ^2-attacks are known to be effective for RC6, and many researches on χ^2-attacks have been proposed. Asymmetcic χ^2 test attack proposed in SCIS2006 recover the key of RC6 efficiently. However, the theoretical success probability is very higher than the experimental success probability, because the theoretical values are estimated on the assumption that the all distributions of χ^2-value of wrong-keys are same. We reconsider the assumption of distributions of χ^2 valus of wrong-keys, and estimate the success probability more strictly.

Key words block cipher, RC6, χ^2-attack, statistical analysis

1. はじめに

RC6 [1] は Rivest らによって提案された算術演算とビットシフトからなるソフトウェア実装向きの共通鍵ブロック暗号である．AES の候補では最速のソフトウェア処理が実現できた．w ワードサイズ，r ラウンド数，b ビット鍵の RC6 は一般に RC6-$w/r/b$ のように記述される．$r = 20$, $w = 32$, $b = 128$, 192, 256 が推奨される値である．なお，RC6-32 は単に RC6 と表す．また，post-whitening なしの RC6 を RC6P と呼ぶ．

RC6 に対する効果的な攻撃方法としては χ^2 攻撃が挙げられる [2]．χ^2 攻撃は入出力に現れる統計的偏りを χ^2 統計量を用いて計ることにより鍵を推定する攻撃手法である．[2] は第 1 ラウンドでの F 関数による巡回シフトが 0 になるようにとることで鍵を推測した．[5] は，遷移行列を用いて理論的に χ^2 値を求める方法が提案された．[6] では RC6P の最終ラウンドから 1 段復号したときの χ^2 値を利用する χ^2 攻撃が提案され，その

成功確率を Disinguish の結果を用いて理論的に導出する方法が示された. [7] では, [6] のアルゴリズムを RC6 に対して拡張し, RC6/16/192, RC6/16/256 が総当り攻撃よりも効率よく解読可能であることを示した. しかし, このアルゴリズムは 64 ビットの最終拡大鍵を同時に推定するため, 計算量・メモリ量共に大きく 128bit RC6 では 8 段が限界である. なお, 128bit RC6 は χ^2 値の実験値より 12 段まで解読可能であると見積もられている [2].

[8] では既存の χ^2 攻撃を改良し, 2 つの攻撃法を提案した. 1 つは巡回シフトが 0 となる集合を大きくとる Coarse-sieve 攻撃 (アルゴリズム 1) で, 192bit 以上の鍵については 16 ラウンド RC6 の解読に必要な計算量を 2^{181} から 2^{155} に削減した. もう 1 つは検定ビット位置と鍵を非対称に扱う非対称 χ^2 検定攻撃 (アルゴリズム 2) で, 128bit 鍵で 14 段まで解読が可能と見積もられている.

[8] での成功確率は χ^2 値の分布について誤鍵での χ^2 値の分布について仮定をおき, これに基づいた理論値を求めている. しかし, Coarse-sieve 攻撃と比べて非対称 χ^2 検定攻撃は攻撃成功確率の実験値と理論値が大きく異なっている. 本研究では理論値を求める上での誤鍵での χ^2 値の分布についての仮定を細分化することによって, 厳密な理論値を求めた.

2. 準　　備

本説では χ^2 検定をはじめとする統計的基礎知識と, RC6 アルゴリズムについて記述する.

2.1 RC6

以下の表記を用いる.

r:	ラウンド
$a \ll b$:	a を左に $b$bit シフト
$a \gg b$:	a を右に $b$bit シフト
(A_i, B_i, C_i, D_i):	i ラウンド目の入力
$(A_{r+2}, B_{r+2}, C_{r+2}, D_{r+2})$:	r ラウンド暗号化後の暗号文
S_i:	i 番目の拡大鍵
$\mathrm{lsb}_n(X)$:	X の最下位 $n$bit
$\mathrm{msb}_n(X)$:	X の最上位 $n$bit
$X_{[i,j]}$:	X の i から j 番目までの bit
$F(x)$:	$x \times (2x+1) \ll \log 32 \pmod{2^{32}}$
$x \parallel y$:	x, y の連結
$N(\mu, \sigma^2)$:	平均 μ, 分散 σ^2 の正規分布
$\phi(\mu, \sigma^2)$:	$N(\mu, \sigma^2)$ の確率密度関数

次に RC6 のアルゴリズムを記述する.

RC6 暗号化アルゴリズム [1]

(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:

$t = F(B_i)$, $u = F(D_i)$,

$A_{i+1} = B_i$, $B_{i+1} = ((C_i \oplus u) \ll t) + S_{2i+1}$,

$C_{i+1} = D_i$, $D_{i+1} = ((A_i \oplus t) \ll u) + S_{2i}$.

(3) $A_{r+2} = A_{r+1} + S_{2r+2}$, $B_{r+2} = B_{r+1}$,

$C_{r+2} = C_{r+1} + S_{2r+3}$, $D_{r+2} = Dr + 1$.

ステップ 1 及び 3 をそれぞれ pre-whitening, post-whitening と呼ぶ.

2.2 統計に関する事項

ここでは χ^2 統計量に関する事項についてまとめる. 母集団 $\Omega = \{X_1, ..., X_k\}$ の確率分布 p を $P(X_1) = p_1, ..., P(X_k) = p_k$ とする. 母集団 Ω から n 個の標本を取り出したとき, 各事象の観測度数は $n_1, ..., n_k$ であるとする. そのとき, 確率分布 $p = (p_1, ..., p_k)$ が確率分布 $\pi = (\pi_1, ..., \pi_k)$ に等しいかどうか, つまり $H_0 : \mathrm{p} = \pi$ を帰無仮説, $H_1 : \mathrm{p} \neq \pi$ を対立仮説とする H_0 と H_1 のどちらが正しいかを検定するために χ^2 統計量を用いる. このとき χ^2 統計量は次の式で与えられ,

$$\chi^2 = \sum_{i=0}^{k} \frac{(n_i - n\pi_i)^2}{n\pi_i} \tag{1}$$

次の定理を用いて検定が可能である.

定理 1. *[3]* 母集団 $\Omega = \{X_1, ..., X_k\}$ の確率分布 p を $P(X_1) = p_1, ..., P(X_k) = p_k$ とする. この確率分布 $p = (p_1, \cdots, p_k)$ が, ある与えられた確率分布 $\pi = (\pi_1, \cdots, \pi_k)$ に等しいかどうかの検定を行なう. 帰無仮説 H_0 が正しい場合, すなわち $p = \pi$ のとき χ^2 統計量は漸近的に平均 *k-1*, 分散 *2(k-1)*, 自由度 *k-1* の χ^2 分布に従う. また, $p \neq \pi$ のときは, 漸近的に平均 $k - 1 + n\theta$, 分散 $2(k-1) + 4n\theta$, 自由度 *k-1* の非心 χ^2 分布に従う. ただし, $n\theta$ は非心パラメータと呼ばれ

$$n\theta = n \sum_{i=0}^{k} \frac{(n_i - n\pi_i)^2}{n\pi_i} \tag{2}$$

で表される.

なお, χ^2 分布, 非心 χ^2 分布は自由度が大きくなるにつれて正規分布に近づいていく.

定理 2. *[中心極限定理 [4]]* 平均 μ, 分散 σ^2 である任意の分布に従う母集団から, 十分大きな n 個の標本を取り出したとき, その平均値は漸近的に平均 μ, 分散 σ^2/n の正規分布 $N(\mu, \sigma^2/n)$ に従う

2.3 遷移確率行列を用いた χ^2 統計量の理論的導出

χ^2 値の平均と分散を理論的に求めるには, 定理 1 で表される θ を求める必要がある. 暗号文を一様ランダムと仮定して検定を行うため $\pi_i = 1/k$ であり, 平文数は 2^n 個であることから

$$\theta = k \sum_{i=0}^{k} \left(P(a_i) - \frac{2^n}{k} \right)^2 \tag{3}$$

となる. $P(a_i)$ については遷移確率行列を用いると理論的に求めることができる. 遷移確率行列は入力値の各ビットの遷移確率を各演算において理論的に計算し, 各出力値の出現確率の行列として表したものである [5].

3. RC6 への既存 χ^2 攻撃研究

3.1 Coarse-sieve 攻撃 [8]

Coarse-sieve 攻撃 (アルゴリズム 1) は $\mathrm{lsb}_3(B_{r+2}) \parallel \mathrm{lsb}_3(D_{r+2})$ の χ^2 値を利用して r ラウンドでの片側の最終

加算鍵 S_{2r+2} の復元を行なうアルゴリズムである．r ラウンドでのシフト量が 0 となるような鍵の集合を大きくとる，つまり篩い数 l を大きくすることによって計算量を削減している．

アルゴリズム 1.

$U = \{u \in \{0,1\}^{32} | \mathrm{msb}_l(u \times (2u+1)) = 0\}$

$u_a \in U$

$t_a = S_{2r+2} = A_{r+2} - u_a$

$z = \mathrm{lsb}_3(B_{r+2}) \parallel \mathrm{lsb}_3(D_{r+2})$

1. $\mathrm{lsb}_5(B_0) = \mathrm{lsb}_5(D_0) = 0$ となる平文を 2^n 個選択．この平文の集合を P_n とする．
2. for $pt \in P_n (pt = (A_0, B_0, C_0, D_0))$
   （1） pt を暗号化して暗号文を得る
   （2） for $u_a \in U$
   $t_a = A_{r+2} - u_a$,
   $z = \mathrm{lsb}_3(B_{r+2}) \parallel \mathrm{lsb}_3(D_{r+2})$,
   $\mathrm{cnt}[t_a][z]$++.
3. for $t_a = 0, .., 2^{32} - 1$
   （1） $\mathrm{cnt}[t_a][z]$ から,t_a に対する χ^2 値を計算 ($\chi^2[t_a]$)
4. ($\overline{\chi^2}[t_a]$ の値が最大になる t_a を正しい拡大鍵 S_{2r+2} として出力.

アルゴリズム 1 の理論的成功確率を求める際には，正鍵，誤鍵それぞれを用いた時の χ^2 値が必要である．正鍵を用いた時の $\mathrm{lsb}_3(B_{r+2}) \parallel \mathrm{lsb}_3(D_{r+2})$ の χ^2 値の分布は $\mathrm{lsb}_3(C_r) \parallel \mathrm{lsb}_3(A_r)$ の分布と正確に一致すると仮定する．一方，誤鍵の χ^2 値は $\mathrm{lsb}_3(B_{r+2}) \parallel \mathrm{lsb}_3(D_{r+2})$ の χ^2 値と比較して小さい値となる．誤鍵の場合には $\mathrm{lsb}_3(B_{r+2}) \parallel \mathrm{lsb}_3(D_{r+2})$ がさらに攪拌されると考え，$\mathrm{lsb}_3(A_{r+3}) \parallel \mathrm{lsb}_3(C_{r+3})$ の χ^2 値とみなすこととした．また，誤鍵中の 1 ビットの誤りが F 関数によって，他のビットに影響を与えることから，誤鍵の全てのビットを対等とすることで扱いが容易になる．以上より，$\mathrm{lsb}_3(B_{r+2}) \parallel \mathrm{lsb}_3(D_{r+2})$ の χ^2 値の分布に関して次のように仮定する．

仮定 1. r ラウンドの *RC6* に対するアルゴリズム *1* において，

- 正鍵を用いた時の $lsb_3(B_{r+2}) \parallel lsb_3(D_{r+2})$ の χ^2 値は $lsb_3(C_r) \parallel lsb_3(A_r)$ の χ^2 値に一致する．
- 誤鍵での $lsb_3(B_{r+2}) \parallel lsb_3(D_{r+2})$ の χ^2 値は $lsb_3(A_{r+3}) \parallel lsb_3(C_{r+3})$ の χ^2 値に一致する．
- 誤鍵の χ^2 値の分布はすべて等しい．

仮定 1 を用いることでアルゴリズム 1 の成功確率について次の定理が成り立つ．

定理 3. アルゴリズム *1* の成功確率は仮定 *1* のもとで以下の式から導出される．

$$P_{s_{rc6}}(n) = \int_{-\infty}^{\infty} f_c(x) \cdot \left(\int_{-\infty}^{x} f_w(u) du \right)^{2^{32}-1} dx \qquad (4)$$

ここで，$f_c(x), f_w(u)$ はそれぞれ正鍵，誤鍵の χ^2 値が従う分布であり，l を鍵の篩い数，$m = 2^{n-l}$，$m\theta_r$ を r ラウンド目の非心パラメータとしたときに

$$f_c(x) = \phi_{(2^6-1+m\theta_{r-1},(2(2^6-1)+4m\theta_{r-1}))}(x)$$
$$f_w(u) = \phi_{(2^6-1+m\theta_{r+1},(2(2^6-1)+4m\theta_{r+1}))}(u)$$
$$\theta_r = 2^6 \sum_{a \in \{0,1\}^{2^6}} \left(P(a) - \frac{2^n}{2^6} \right)^2 \qquad (5)$$
$$a = lsb_3(A_{r+1}) \parallel lsb_3(C_{r+1})$$

で表される．

Proof. アルゴリズム 1 は最終ラウンドのシフト量が 0 になる平文のみについて $\mathrm{lsb}_3(B_{r+2}) \parallel \mathrm{lsb}_3(D_{r+2})$ の出現頻度を測定しているために，χ^2 値は正しい鍵の場合は B_{r+2}, D_{r+2} は $r-1$ ラウンドでの出力の C_r, A_r に一致する．また，仮定 1 より誤った鍵の場合は一段増加したときの出力 A_{r+3}, C_{r+3} に一致する．それらの出現確率は遷移確率行列で計算可能であり，その出現確率から非心パラメータを求めることが出来る．従って，平文数を決定すると χ^2 値の平均と分散が定理 1，定理 2 より求められ，定理 3 の $Ps_{rc6}(n)$ が導かれる． □

表 2 に示すとおり，鍵の篩い数を 19 まで緩めることで 128Bit 鍵では 14 ラウンドまで解読可能である．表??に示すとおり，4 ラウンド RC6-8 による実験値と理論値は近い値となった．

表 1　6 ビット検定での各ラウンドにおける *0*

rounds	*0*
3	0.802×10^{-3}
5	0.119×10^{-7}
7	0.178×10^{-12}
9	0.266×10^{-17}
11	0.401×10^{-22}
13	0.606×10^{-27}
15	0.919×10^{-32}
17	0.139×10^{-36}
19	0.211×10^{-41}

表 2　アルゴリズム 1 での 14round での平文とシフト量の関係 [8]

篩い数	# text	計算量	篩い数	# text	計算量
6	$2^{108.32}$	$2^{134.32}$	7	$2^{108.78}$	$2^{133.78}$
8	$2^{109.25}$	$2^{133.25}$	9	$2^{109.72}$	$2^{132.72}$
10	$2^{110.21}$	$2^{132.21}$	11	$2^{110.70}$	$2^{131.79}$
12	$2^{111.19}$	$2^{131.19}$	13	$2^{111.68}$	$2^{130.68}$
14	$2^{112.10}$	$2^{130.10}$	15	$2^{112.61}$	$2^{129.61}$
16	$2^{113.10}$	$2^{129.10}$	17	$2^{113.60}$	$2^{128.60}$
18	$2^{114.10}$	$2^{128.10}$	19	$2^{114.67}$	$2^{127.67}$

表 3　4 ラウンド RC6-8 にアルゴリズム 1 を適用したときの成功確率の理論値と実験値 [8]

		平文数			
篩い数		2^{17}	2^{18}	2^{19}	2^{20}
3	理論値	0.47	0.92	1.00	1.00
	実験値	0.41	0.85	0.97	1.00
5	理論値	0.03	0.14	0.47	0.92
	実験値	0.02	0.15	0.64	0.95

3.2 非対称 χ^2 検定攻撃 [8]

非対称検定 χ^2 攻撃では検定ビット位置と鍵を非対称に扱うことにより計算量の削減を実現した．$\mathrm{lsb}_3(C_r) \parallel \mathrm{lsb}_3(D_{r+2})$ の χ^2 値を利用して r ラウンドでの Post-WhiteningS_{2r+2}, $\mathrm{lsb}_2(S_{2r+3})$, そして最終段の鍵 $\mathrm{lsb}_2(S_{2r+1})$ を復元するアルゴリズムを次に示す．このアルゴリズムを用いる際，$\mathrm{lsb}_5(B_0) = \mathrm{lsb}_5(D_5) = 0$ となる平文を選択することにより，$v = \mathrm{lsb}_5(B_0) \parallel \mathrm{lsb}_5(D_5)$ による分類の必要がなくなるため，計算量が削減される．

アルゴリズム 2. *[8]*

$U = \{u \in \{0,1\}^{32} | \mathrm{msb}_5(u \times (2u+1)) = 0\}$

$u \in U \times U$

$t_a = S_{2r+2} = A_{r+2} - u,\ t_x = \mathrm{lsb}_3(S_{2r+3}) \,||\mathrm{lsb}_3(S_{2r+1})$

$v = \mathrm{lsb}_5(B_0) \parallel \mathrm{lsb}_5(D_0)$

$w = lsb_3(F(\mathrm{lsb}_3(C_{r+2}) - \mathrm{lsb}_3(S_{2r+3})))$

$y = \mathrm{lsb}_3(B_{r+2}) - \mathrm{lsb}_3(S_{2r+1}) \oplus w$ (注1)

$z = y \parallel \mathrm{lsb}_3(D_{r+2})$

1. 2^n 個の平文の集合を P_n とする
2. for $pt \in P_n (pt = (A_0, B_0, C_0, D_0))$
   （1） $v = \mathrm{lsb}_5(B_0) \parallel \mathrm{lsb}_5(D_0)$
   （2） pt を暗号化して暗号文を得る
   （3） for $u \in U \times U$
   $t_a = A_{r+2} - u,$
   $t = t_a \parallel t_x,$
   $w = \mathrm{lsb}_3(F(\mathrm{lsb}_3(C_{r+2}) - \mathrm{lsb}_3(S_{2r+3})))$
   $y = \mathrm{lsb}_3(B_{r+2}) - \mathrm{lsb}_3(S_{2r+1}) \oplus w$
   $z = y \parallel \mathrm{lsb}_3(D_{r+2}),$
   cnt[t][v][z]++.
3. for $t = 0, .., 2^{27+6} - 1$
   （1） for $v = 0, .., 2^{10} - 1$
   cnt[t][v][z] から，t, v に対する χ^2 値を計算 ($\chi^2[t][v]$)
   （2） t に対して χ^2 値の平均を計算
   ($\overline{\chi^2}[t] = 1/20^{10} \sum_{z=0}^{2^{10}-1} \chi^2[t][v]$)
4. $\overline{\chi^2}[t]$ の値が最大になる $t = t_a \parallel t_x$ を正しい拡大鍵 S_{2r+2}, $\mathrm{lsb}_2(S_{2r+1})$, $\mathrm{lsb}_2(S_{2r+3})$ として出力．

アルゴリズム 2 の理論的成功確率を求める際には，アルゴリズム 1 同様に誤鍵の χ^2 値についての仮定が必要である．そこで，以下の仮定を用いた．

仮定 2. *r* ラウンドの *RC6* に対するアルゴリズム 2 において，

- 誤鍵での $lsb_3(C_r) \parallel lsb_3(D_{r+2})$ の χ^2 値は $lsb_3(A_{r+3}) \parallel lsb_3(C_{r+3})$ の χ^2 値に一致する．
- 誤鍵の χ^2 値の分布はすべて等しい．

仮定 2 のもとで，アルゴリズム 2 の成功確率について次の定理が成り立つ．

アルゴリズム 2 の理論的な成功確率は次の定理より求めることができる．

(注1)：正鍵のとき，$y = C_{r[5,7]}$ となる．

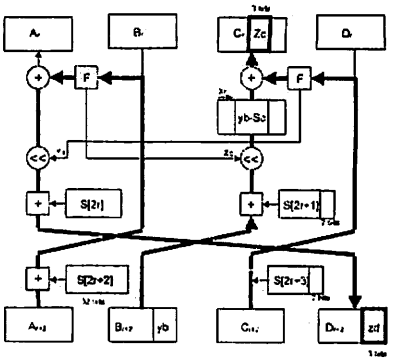

図 1 アルゴリズム 2 の概要

定理 4. *[8]* 仮定 2 のもとで 2^n 個の平文を用いたアルゴリズム 2 の理論的な成功確率 P_{rc6} は次の式より導出することが出来る．

$$P_{s_{rc6}}(n) = \int_{-\infty}^{\infty} f_c(x) \cdot \left(\int_{-\infty}^{x} f_w(u) du \right)^{2^{26}-1} dx \qquad (6)$$

ここで，$f_c(x), f_w(u)$ はそれぞれ正鍵，誤鍵の χ^2 値が従う分布であり，$m = 2^{n-5}$, $m\theta_r$ を r ラウンド目の非心パラメータ，$m\tilde{\theta}_r$ を r ラウンドで正鍵で復元したときの非心パラメータとしたときに

$$\begin{aligned} f_c(x) &= \phi_{(2^6-1+m\tilde{\theta}_r, (2(2^6-1)+4m\tilde{\theta}_r)/2^{10})}(x) \\ f_w(u) &= \phi_{(2^6-1+m\theta_r, (2(2^6-1)+4m\theta_r)/2^{10})}(u) \\ \theta_r &= 2^6 \sum_{a \in \{0,1\}^{26}} \left(P(a) - \frac{2^n}{2^6} \right)^2 \\ \tilde{\theta}_r &= 2^6 \sum_{b \in \{0,1\}^{26}} \left(P(b) - \frac{2^n}{2^6} \right)^2 \\ a &= lsb_3(A_{r+2}) \parallel lsb_3(C_{r+2}) \\ b &= lsb_3(C_r) \parallel lsb_3(C_{r+2}) \end{aligned} \qquad (7)$$

で表される．

Proof. 最終ラウンドで $\mathrm{lsb}_5(F(B_r)) = 27$ になる平文のみについて $C_{r[5,7]}||\mathrm{lsb}_3(D_{r+2})$ の出現頻度を測定しているため，正鍵を復元した場合 D_{r+2} は r ラウンドで XOR がない D_{r+2} の χ^2 値に一致する．また，仮定 2 より誤鍵の場合は B_{r+2}, D_{r+2} の χ^2 値は 1 段多いときの出力 A_{r+3}, C_{r+3} に一致する．それらの出現確率は遷移確率行列で計算可能であり，その出現確率から非心パラメータを求めることができる．また，1 つの鍵に対してシフト量が 27 となる平文が出現する確率は $1/2^5$ である．従って，平文数を決定すると χ^2 値の平均と分散が定理 1，定理 2 より求められ，定理 4 の $Ps_{rc6}(n)$ が導かれる． □

[8] ではアルゴリズム 2 を用いると 192，256 ビット鍵の RC6 に対しては 16 段まで全数探索よりも効率的に鍵を導出できるとしている．しかし，4 ラウンド RC6-8 に対するアルゴリズ

表 4　アルゴリズム 2 の成功確率実験値 (4 ラウンド RC6-8, 3 ビット検定)

任意の平文			$v=0$ となる平文		
#text	理論値	実験値	#text	理論値	実験値
2^{18}	0.01	0.00	2^{16}	0.06	0.00
2^{19}	0.09	0.03	2^{17}	0.53	0.15
2^{20}	0.74	0.15	2^{18}	0.99	0.55
2^{21}	1.00	0.78	2^{19}	1.00	0.95
2^{22}	1.00	0.99	2^{20}	1.00	1.00

ム 2 の攻撃成功確率について定理 4 から導かれる理論値と実験値を比較すると，アルゴリズム 1 と比べて大きな差がみられる (表 4).

4. 成功確率の理論値

4.1 誤鍵の χ^2 値

非対称 χ^2 検定攻撃の成功確率で見られる実験値と理論値に差の原因に，誤鍵の χ^2 値の仮定が考えられる．誤鍵の χ^2 値の仮定において誤鍵の χ^2 値の分布はすべて等しく扱っている．しかし，ビットの位置によっては χ^2 値への影響が大きいものがあると考えられる．誤鍵の中には，一部のビットのみ誤って推定しているものがある．このとき，確率的に正鍵を推定した場合と同じ χ^2 値の分布に従う場合がある．そのため，仮定にもとづいた誤鍵での χ^2 値の分布は実際よりも低い値となる．つまり正鍵の分布と誤鍵の分布との差が広がり，攻撃の成功確率が高くなってしまう．これが実験値と理論値の差の原因である．しかし，Coarse-sieve 攻撃の成功確率では実験値と理論値の差は小さい．非対称 χ^2 検定攻撃では $S_{2r+2}, \mathrm{lsb}_2(S_{2r+3})$, $\mathrm{lsb}_2(S_{2r+1})$ を復元する一方，Coarse-sieve 攻撃では S_{2r+2} のみの復元である．このことから $\mathrm{lsb}_2(S_{2r+3})$, $\mathrm{lsb}_2(S_{2r+1})$ での誤りによる影響が大きいことが推測できる．

次に一部のビットのみ誤って推定した場合について詳しく検討する．そこから誤鍵の分布を厳密に求め，理論値を正確に導出する．

4.2 誤鍵の χ^2 値の再評価

アルゴリズム 2 での推定鍵を S_{2r+2} と $\mathrm{lsb}_2(S_{2r+1})$, $\mathrm{lsb}_2(S_{2r+3})$ に分けて考えることとする．S_{2r+2} は D_{r+2} を求める過程で，F 関数によって 1 ビットの誤りが他のビットへと波及する．また，この経路では $\mathrm{lsb}_2(S_{2r+1})$ と $\mathrm{lsb}_2(S_{2r+3})$ が直接加算されることはない．

次に $\mathrm{lsb}_2(S_{2r+1})$, $\mathrm{lsb}_2(S_{2r+3})$ について考える．S_{2r+2} が正しいとき，$\mathrm{lsb}_2(S_{2r+1})$ と $\mathrm{lsb}_2(S_{2r+3})$ は $\mathrm{lsb}_2(B_{r+2})$ から $C_{r[5,6]}$ を復元する経路で同一のビット位置に影響を及ぼす．この影響について表 5 にまとめる．表 5 中で c, w, *はそれぞれ 1 ビットを表し，c は正しく推定したビット，w は誤って推定したビット，*はランダムであることを示している．

表 5 より S_{2r+2} が正しく，$\mathrm{lsb}_2(S_{2r+1})||\mathrm{lsb}_2(S_{2r+3})$ =wcwc, wccc, ccwc の場合，1/2 の確率で $C_{r[5,6]}$ を正しく復元できることが分かる．従って，C_r, D_{r+2} の χ^2 値は 1/2 の確率で鍵を正しく推定した場合の χ^2 値となる．

表 5　S_{2r+2} が正しいときの $\mathrm{lsb}_2(S_{2r+1})||\mathrm{lsb}_2(S_{2r+3})$ と $C_{r[5,6]}$ の正誤関係

$\mathrm{lsb}_2(S_{2r+1})\|\|\mathrm{lsb}_2(S_{2r+3})$	$C_{r[5,6]}$
*w*w	*w
*w*c	*w
*c*w	*w
*c*c	*c

一方，アルゴリズム 1 について考えた場合，推定する鍵にはアルゴリズム 2 での $\mathrm{lsb}_2(S_{2r+1})||\mathrm{lsb}_2(S_{2r+3})$ のような関係を持つ部分がない．そのため，アルゴリズム 2 で見られるような理論値と実験値の差が出なかったと考えられる．

4.3 修正成功確率

前節での評価に基づき，次の仮定をおく．

仮定 3. *r ラウンドの RC6 に対するアルゴリズム 2 において，誤鍵推定時における $lsb_3(C_r) \,||\, lsb_3(D_{r+2})$ の χ^2 値を次のように仮定する．*

- *S_{2r+2}, $lsb_0(S_{2r+1})$ または $lsb_0(S_{2r+3})$ に誤りを含む場合，$lsb_3(A_{r+3}) \,||\, lsb_3(C_{r+3})$ の χ^2 値に一致する．*
- *$lsb_1(S_{2r+1})$ または $lsb_1(S_{2r+3})$ の誤りのみの場合，1/2 の確率で正しく推定した場合の χ^2 値に，1/2 の確率で $lsb_3(A_{r+3}) \,||\, lsb_3(C_{r+3})$ の χ^2 値に一致する．*

をもとにして，アルゴリズム 2 の理論的成功確率について以下の定理が成り立つ．

定理 5. *仮定 4.3 のもとで 2^n 個の平文を用いたアルゴリズム 2 の理論的な成功確率 P_{rc6} は次の式より導出することが出来る．*

$$P_{s_{rc6}}(n) = \int_{-\infty}^{\infty} f_c(x) \cdot \left(\int_{-\infty}^{x} f_{wc}(u)du \right)^3 \cdot \left(\int_{-\infty}^{x} f_w(u)du \right)^{2^{36}-4} dx \qquad (8)$$

ここで，$f_c(x), f_{wc}(u), f_w(u)$ はそれぞれ正鍵，$lsb_1(S_{2r+1})$ または $lsb_1(S_{2r+3})$ のみ誤った鍵，S_{2r+2}, $lsb_1(S_{2r+1})$ 及び $lsb_1(S_{2r+3})$ に誤りを含む鍵の χ^2 値が従う分布であり，$m = 2^{n-10}$, $m\theta_r$ を r ラウンド目の非心パラメータ，$m\bar{\theta}_r$ を r ラウンドで正鍵で復元したときの非心パラメータ，$\bar{\theta}_r = (\tilde{\theta}_r + \theta_{r+1})/2$ としたときに

表 6 アルゴリズム 2 の成功確率実験値
(4 ラウンド RC6-8, 3 ビット検定)

任意の平文			$v=0$ となる平文		
#text	実験値	修正理論値	#text	実験値	修正理論値
2^{18}	0.00	0.00	2^{16}	0.00	0.02
2^{19}	0.03	0.02	2^{17}	0.15	0.14
2^{20}	0.15	0.19	2^{18}	0.55	0.48
2^{21}	0.78	0.79	2^{19}	0.95	0.77
2^{22}	0.99	0.98	2^{20}	1.00	0.92

表 7 $P_{s_{rc6_{alg2}}} \geqq 0.95$ となる理論値

任意の平文			$v=0$ となる平文		
round	平文数	計算量	round	平文数	計算量
4	$2^{32.58}$	$2^{63.58}$	4	$2^{27.7}$	$2^{58.7}$
6	$2^{48.48}$	$2^{79.48}$	6	$2^{43.6}$	$2^{74.6}$
8	$2^{64.65}$	$2^{95.65}$	8	$2^{59.77}$	$2^{90.77}$
10	$2^{80.37}$	$2^{111.37}$	10	$2^{75.49}$	$2^{106.49}$
12	$2^{96.28}$	$2^{127.28}$	12	$2^{91.4}$	$2^{122.4}$
14	$2^{112.09}$	$2^{143.09}$	14	$2^{109.21}$	$2^{140.21}$
16	$2^{128.39}$	$2^{159.39}$	16	$2^{123.51}$	$2^{154.51}$
18	$2^{144.01}$	$2^{175.01}$	18	$2^{140.32}$	$2^{171.32}$

$$
\begin{aligned}
f_c(x) &= \phi_{(2^6-1+m\delta_r,(2(2^6-1)+4m\delta_r)/2^{10})}(x)\\
f_{wc}(u) &= \phi_{(2^6-1+m\delta_r,(2(2^6-1)+4m\delta_r)/2^{10})}(u)\\
f_w(u) &= \phi_{(2^6-1+m\theta_r,(2(2^6-1)+4m\theta_r)/2^{10})}(u)\\
\theta_r &= 2^6 \sum_{a\in\{0,1\}^{2^6}} \left(P(a)-\frac{2^n}{2^6}\right)^2 \qquad (9)\\
\tilde{\theta}_r &= 2^6 \sum_{b\in\{0,1\}^{2^6}} \left(P(b)-\frac{2^n}{2^6}\right)^2\\
a &= lsb_3(A_{r+2}) \parallel lsb_3(C_{r+2})\\
b &= lsb_3(C_r) \parallel lsb_3(C_{r+2})
\end{aligned}
$$

で表される.

Proof. 最終ラウンドで $\mathrm{lsb}_5(F(B_r)) = 27$ になる平文のみについて $C_{r[5,7]}\|\mathrm{lsb}_3(D_{r+2})$ の出現頻度を測定しているため, 正鍵を復元した場合 D_{r+2} は r ラウンドで XOR がない D_{r+2} の χ^2 値に一致する. また, 仮定 4.3 より誤鍵の場合は C_r, D_{r+2} の χ^2 値は 1 段多いときの出力 A_{r+3}, C_{r+3} に一致する. それらの出現確率は遷移確率行列で計算可能であり, その出現確率から非心パラメータを求めることができる. また, 1 つの鍵に対してシフト量が 27 となる平文が出現する確率は $1/2^5$ である. 従って, 平文数を決定すると χ^2 値の平均と分散が定理 1, 定理 2 より求められ. 定理 5 の $Ps_{rc6}(n)$ が導かれる. □

4 ラウンド RC6-8 に対するアルゴリズム 2 の攻撃成功確率について, 定理 5 から導かれる理論値及び実験値は表 6 の通りである. 表 6 より既存理論値と比較し, 実験値に近い理論値を導いたことが分かる. また, RC6 にアルゴリズム 2 を適用したときに 95% 以上の成功確率で鍵を導出するために必要な平文数と計算量を表 7 に示す. 192, 256 ビット鍵の RC6 に対する攻撃に必要な平文数が増加しており, アルゴリズム 2 で全数探索よりも効率的に鍵を導出できる段数は 14 段までであることが示された. 128 ビット鍵については既存理論値同様に 12 段まで効率的である.

5. Conclusion

我々は χ^2 攻撃の理論的成功確率を導出するために必要な誤鍵の χ^2 値の仮定について再評価を行った. その結果, 推定鍵の異なるビットが同一の検定ビットに影響を及ぼす場合を個別に扱う必要があることが分かった. これにもとづき, 誤鍵における仮定を細分化することによって, より厳密な理論値を求めることができた. 今後の課題として, Coarse-sieve 攻撃における正鍵での χ^2 値の分布の仮定について, 再評価をする必要がある.

文 献

[1] R. Rivest,M. Robshaw,R. Sidney, and Y. Yin, "The RC6 Block Cipher v1.1", August 20, 1998. Available at http://www.rsasecurity.com/rsalabs/rc6/

[2] R. Knudsen, Willi Meier, "Correlations in RC6 with a Reduced Number of Rounds",FSE2000, vol.1978 of Lecture Notes in Computer Science, pp.94-108, Springer-Verlag, 2001.

[3] Boris Ryabko, "Adaptive chi-square test and its application to some cryptographic problems", Cryptology ePrint Archive, Report 2002/030 (2003), http://eprint.iacr.org/.

[4] R.J. Freund and W.J. Wilson, *Statistical Method*, Academic Press, San Diego, 1993.

[5] M. Takenaka, T. Shimoyama, T. Koshiba, "Theoretical Analysis of χ^2 Attack on RC6", IEICE Trans., VOL.E87-A, NO.1(2004), pp.28-35, 2004.

[6] T. Matsunaka, A. Miyaji, and Y. Takano, "Success probability in χ^2-attacks", ACNS 2004, vol. 3089 of Lecture Notes in Computer Science, pp.310-325, Springer-Verlag, 2004.

[7] Atsuko Miyaji, Yuuki Takano, "On the Success Probability of χ^2-attack on RC6",ACISP2005, vol.3574 of Lecture Notes in Computer Science, pp.61-75,Springer-Verlag, 2005.

[8] Tomohiko Hinoue, Atsuko Miyaji, "RC6 のカイ二乗攻撃の効率化へのアプローチについて", SCIS2006, pp.213, 2006.