A New Approach to χ^2 Cryptanalysis of Block Ciphers^{*}

Jorge Nakahara Jr.¹, Gautham Sekar^{2,3,**}, Daniel Santana de Freitas⁴, Chang Chiann⁵,
Ramon Hugo de Souza⁴, and Bart Preneel^{2,3}

¹ EPFL, Lausanne, Switzerland.

`jorge.nakahara@epfl.ch`

² Department of Electrical Engineering ESAT/SCD-COSIC, Katholieke Universiteit Leuven,
Kasteelpark Arenberg 10, B-3001 Heverlee, Belgium.

`{Gautham.Sekar,Bart.Preneel}@esat.kuleuven.be`

³ Interdisciplinary Institute for BroadBand Technology (IBBT), Belgium.

⁴ Federal University of Santa Catarina, Brazil.

`{santana,ramonh}@inf.ufsc.br`

⁵ University of São Paulo, Brazil.

`chang@ime.usp.br`

Abstract. The first contribution of this paper is a new approach to χ^2 analyses of block ciphers in which plaintexts are chosen in a manner similar to that in a square/saturation attack. The consequence is a faster detection of χ^2 correlation when compared to conventional χ^2 cryptanalysis. The second contribution of the paper is the application of a technique similar to the aforementioned approach, but aided by linear cryptanalysis, on the RC6-family of block ciphers. Using this technique we *(i)* improve the previously best-known χ^2 attacks on reduced-round RC6, and *(ii)* mount the first attacks on other RC6-like block ciphers - MRC6 and ERC6. The analyses of these fast primitives were also motivated by their low diffusion powers and, in the case of MRC6 and ERC6, their large block sizes that favour construction of hash functions. Our analysis indicates that up to 98 rounds of MRC6 and 44 rounds of ERC6 could be broken. We expect our technique to be applicable to other block ciphers also.

1 Introduction

The block cipher RC6 [24] was designed by Rivest *et al.* for the AES Development Process [1]. The algorithm was one of the five finalists in the AES competition and was also submitted to NESSIE [19] and CRYPTREC [6] projects. It is described in US patents 5,724,428 and 5,835,600 (Apr. 21, 1997). The cipher MRC6, proposed by El-Fishawy *et al.* in 2004 [8], is a wide-block variant of the RC6. The main focus of the redesign was performance enhancement. ERC6 [22] is another wide-block variant of the RC6 block cipher.

In this paper we present a new, generic approach to χ^2 cryptanalysis which combines conventional χ^2 attacks and integral cryptanalysis. In this approach, the input plaintexts are chosen like in a square/saturation attack. In a square attack, a part of the input is fixed and the remaining part is varied exhaustively. In our approach, we fix a part of the input and keep on generating plaintexts till χ^2 correlation is detected. The advantage of our approach is that it allows faster detection of χ^2 correlations in block ciphers. One drawback of this approach is that it is quite complicated to turn the chosen-plaintext setting to a known-plaintext one.

^{*} This work was supported in part by the IAP Programme P6/26 BCRYPT of the Belgian State (Belgian Science Policy), and in part by the European Commission through the ICT programme under contract ICT-2007-216676 ECRYPT II.

^{**} This author is supported by an FWO project.

In our attacks on the RC6-family, the choice of the input bits fixed and the output bits studied is based on some prior linear cryptanalysis. We initially performed linear cryptanalysis of RC6, MRC6 and ERC6. This provided us with the bit positions whose non-uniformity was ultimately analysed by the χ^2 test. Our attacks follow similar methodology as the mod- n attacks against the block ciphers RC5P and M6 [13]. In the latter, a chosen-plaintext χ^2 attack was presented on RC5P without pre- or post-whitening. First, the plaintexts are chosen in a way that creates n^2 fixed partitions of the message space. The probability distribution of the ciphertext is then empirically computed and its bias measured using the χ^2 test.

All considerations and conclusions in this paper are mostly based on empirical data collected through several attack simulations. We have used χ^2 threshold values corresponding to 25% significance level (or 75% specificity). This choice was based on the following reasons.

1. Our aim is to show the effectiveness of our attacks on the RC6-family when compared to χ^2 cryptanalysis with randomly generated plaintexts. Hence, as long as the same significance level is used for the two types of tests, the value of the significance level is irrelevant.
2. Our attack simulations show that the number of chosen-plaintexts required with a better (we considered 10%) significance level could be determined by the number corresponding to 25% level.
3. In the literature 25% seems to be an acceptable value [15].

This paper is organized as follows. Section 2 briefly describes χ^2 cryptanalysis and introduces our technique; Sect. 3 gives the specifications of the RC6-family of ciphers; Sect. 4 provides the experimental results of our χ^2 attacks on the three ciphers. Also, in Sect. 4 comparisons are drawn between our attacks and previously applied methods. Section 5 concludes the paper.

2 The χ^2 Test and Our Generic Approach

The χ^2 statistical test has already been applied to a number of secret-key ciphers, formerly on the DES [20] in [30], but also on SEAL [10]; on M6, MX and RC5P [13]; on RC5, RC6 and many simplified variants [3, 9, 11, 12, 14, 17, 21, 24, 28].

Let us consider an experiment E with k simple, mutually independent outcomes. Let $n_1, n_2, \dots, n_k$ and $x_1, x_2, \dots, x_k$ denote the observed and expected frequencies, respectively, of the k outcomes when E is performed N times. Therefore, $N = \sum_{i=1}^k n_i = \sum_{i=1}^k x_i$. For each outcome, there could be a difference between the observed and the expected frequencies. The idea behind a χ^2 test is to combine all these differences into one overall measure of the distance between the data and the expectations of the model. The χ^2 statistic with $k - 1$ degrees of freedom is defined [2] as,

$$Q = \sum_{i=1}^k \frac{(n_i - x_i)^2}{x_i}, x_i \neq 0. \quad (1)$$

The quantity Q gives a measure of the distance between the observed and expected frequencies; large values of Q indicate that the observed frequencies are far from the expected ones.

In a χ^2 goodness-of-fit test, one defines two hypotheses - the null hypothesis (denoted H_0) and the alternative hypothesis (H_1). The null hypothesis is the one that exists solely to be “falsified” by the sample. If the null hypothesis is rejected, the result is *positive*. When the test result tallies with the actual reality, the result is *true*. The false-negative rate of the test, i.e., the fraction of *positive* instances that were falsely reported as *negative*, is denoted by β . The sensitivity (or power) of the test is the true-positive rate $(1 - \beta)$. The significance of the test is the false-positive rate (α) and the specificity of the test is the true-negative rate $(1 - \alpha)$. Let $\chi^2_{1-\alpha, k-1}$ denote the $(1 - \alpha)$ -th lower quantile of a χ^2 distribution with $k - 1$ degrees of freedom. In a χ^2 test, H_0 is rejected (in other words, H_1 is accepted), if $Q > \chi^2_{1-\alpha, k-1}$ with 100α % error.

In our approach, N is the number of plaintexts - the parameter to be determined. Let E' denote the experiment ‘ E repeated N times’. To minimise error, we consider q randomly generated keys and E' is performed q times. We then estimate the mean and variance of the χ^2 values for the entire key space using the Student’s t-distribution. But this requires that the sample is normally distributed. This is nearly achieved when the number of degrees of freedom $(k - 1)$ is large since when $k \rightarrow \infty$, the χ^2 variate becomes a normal variate. Finally, using q , the q -sample mean and sample variance, a confidence interval is computed, using the t-curve, for the mean of the population. We use 90% confidence interval in our tests. In other words, the chance that the population mean falls below (or above) the interval is 5%. The lower end point of the interval (*minCI*) is taken for the population mean. This means that there is 95% chance that the actual population mean is above this value. In our experiments, we accept H_1 if *minCI* is greater than $\chi^2_{1-\alpha, k-1}$. This automatically implies that the actual population mean is greater than $\chi^2_{1-\alpha, k-1}$ with 95% probability and thus error is small. In this paper, we use the χ^2 test under the following settings:

H_0 : a subset of bits output by r -round ($r > 0$) XRC6 (where XRC6 denotes RC6, MRC6 or ERC6) is uniformly distributed,

H_1 : a subset of bits output by r -round XRC6 is non-uniformly distributed.

Thus, (1) becomes

$$Q = \sum_{i=1}^k \frac{(n_i - N/k)^2}{N/k}. \quad (2)$$

A requirement in χ^2 tests is that $N \geq 5 \cdot (k - 1)$, so that the χ^2 value is significant. In conventional χ^2 cryptanalysis, plaintexts are generated at random. However, plaintexts can be chosen in the following way to yield better attacks. We begin with r rounds of the block cipher whose block size is d bits. Next, we divide the block into words of size t' bits. Since the word size is t' bits, there are $2^{t'}$ possibilities and hence the number of degrees of freedom $k - 1 = 2^{t'} - 1$. The number t' is chosen by a trade-off among d , r , the speed of the block cipher and the computing power available. Let δ denote the quantity $\lceil d/t' \rceil$. Let the δ words of the plaintext A_0 be indexed $A_{0(0)}, \dots, A_{0(\delta-1)}$ (where $A_{0(0)}$ is the least significant); similarly for the output block A_r after r rounds. The t' bits of $A_{0(0)}$ are set to zeros, the remaining $(d - t')$ bits are varied incrementally and encryptions are performed. We record the values of $A_{r(0)}$. The χ^2 value is computed and if it supports acceptance of H_0 , then we assume that the varied $(d - t')$ bits of the plaintext have diffused well into

$A_{r(0)}$, proceed by fixing the bits of $A_{0(1)}$ to zero, incrementally vary the remaining $(d - t')$ bits and observe $A_{r(1)}$ ¹. This process is repeated for all the δ words. Following this we find the least N for which H_1 is accepted and note the corresponding word of A_0 (say, $A_{0(i)}$). Finally, we proceed to a higher r , set the bits of $A_{0(i)}$ to zeros as before and repeat the test fixing bits in this $(i+1)$ -th word alone. Now, while repeating the procedure for $r+x$ rounds, fewer bits of $A_{0(i)}$ may have to be fixed to facilitate ease of computation. Here, we warn that reducing the number of bits makes the approximation of χ^2 distribution with normal distribution more erroneous. If, in the above procedure for r rounds, H_1 is not accepted at all, we conclude that the result of the test for the full-round cipher is negative. The following pseudocode describes the above procedure.

Another advantage of this approach is the higher speed of a reduced-round version when compared to that of the full-round cipher. With lesser encryption time, appropriate plaintext bits are identified which can alone be used for attack simulations on a larger number of rounds.

TEST ($H_0, H_1, \delta, r, q, \alpha$)

- (1) {
- (2) for ($j = 0; j < \delta; j++$)
- (3) {
- (4) for ($i = 1; i \leq q; i++$) // number of tests E'
- (5) {
- (6) set $A_{0(j)}$ to zero while varying the remaining bits incrementally
- (7) for ($s = 1; s \leq N; s++$) // sample size
- (8) {
- (9) encrypt A_0 through r rounds
- (10) let $X = A_{r(j)}$ and increment counter $C[X]$ by 1
- (11) }
- (12) let $Q_i =$ the χ^2 value of $C[X]$'s
- (13) }
- (14) let m be the average over all $Q_i, 1 \leq i \leq q$
- (15) let σ be the standard deviation over all $Q_i, 1 \leq i \leq q$
- (16) let $minCI = m - 1.729 \cdot \sigma / \sqrt{q}$ (lower limit of a 90% confidence interval)
- (17) let $v_{1-\alpha} =$ value at $100(1 - \alpha)\%$ in the χ^2 cumulative distribution
- (18) if ($minCI > v_{1-\alpha}$) choose H_1
- (19) else choose H_0
- (20) }
- (21) }
- (22) note the j corresponding to the minimum N for which H_1 is accepted;
- $r \leftarrow r + x$;
- decrease t' if required;
- perform TEST ($H_0, H_1, \delta', r + x, q, \alpha$) fixing bits in this $(j + 1)$ -th word alone (i.e., without lines (2), (3) and (20));
- (23) if there is no j for which H_1 is accepted, H_0 is accepted for the full-round cipher;

¹ The intuition is that the bits of $A_{0(0)}$ are more likely to affect the bits of $A_{r(0)}$ than the remaining $(d - t')$ bits of the output. Hence, we only observe how the other $(d - t')$ bits of the plaintext affect $A_{r(0)}$

A further consequence of the new approach is a smaller demand for chosen plaintexts (CP), possibly due to weak diffusion in the target cipher. A smaller number of CP implies a smaller encryption time, and thus, faster attacks. Of course, it is also possible to identify suitable plaintext bits through other cryptanalytic techniques, for instance, using mod- n techniques as in [13]. On the RC6-family of ciphers, though, we first applied linear cryptanalysis to find appropriate linear trails. These trails indicated us the bits to be set to zeros in TEST(). It shall be observed that the more bits are under analysis, the better the attack outcome. But, since $N \geq 5 \cdot (k - 1)$, the data (and time) complexities increased quickly beyond our computational resources.

Consequently, we used $t' \in \{10, 20, 40\}$ for the plaintext, but $t' \in \{4, 8, 16\}$ for the ciphertext, unlike in TEST() where both values of t' were identical (here, we have followed the approach of [12, 21]). Secondly, we had selected the t' plaintext bits from different bit positions rather than contiguously as in TEST(). Thirdly, we did not have to perform the experiment δ times because linear cryptanalysis already gave us the appropriate bits to be set to zeros. Other than these minor differences, our attacks on the RC6-family follow the same procedure as TEST().

Bits were chosen from different positions because through linear cryptanalysis we observed that the remaining $d - t'$ bits of the plaintext did not diffuse well into the t' ciphertext bits used for the χ^2 test. The weak diffusion is only advantageous for a small number of rounds. Here, our attacks on the RC6-family and the approach used by Knudsen and Meier in [14] are different. We fix a number of bits to zeros and vary the remaining bits incrementally; whereas in their method, the remaining bits are varied randomly². The result is that, with Knudsen and Meier's method, one can observe random-looking 512-bit strings after one/few rounds itself. Secondly, we use 90% confidence interval to minimise error (see the reasoning above) whereas [14] does not. After enough rounds (that depends on the target cipher), we conjecture that choosing the entire plaintext block instead of just a part of it results, in the long run, in same outcome as [14].

3 The RC6-Family of Block Ciphers

Before we begin with the specifications of the RC6-family of ciphers, we provide the notations used in the rest of the paper. The symbols $\oplus$ and $\boxplus$ denote bitwise exclusive-OR and addition modulo 2^w . The operation $x \lll y$, where x and y are w -bit words, means that x is cyclically shifted to the left by the amount given by least significant $\log_2 y$ bit positions. The function F is given by $F(X) = [X \cdot (2 \cdot X + 1) \bmod 2^w] \lll \log_2 w$, $F : \mathbb{Z}_2^w \rightarrow \mathbb{Z}_2^w$.

3.1 RC6

The RC6 actually stands for a family of ciphers, formally denoted RC6- $w/r/b$, where w is the word size in bits, r is the number of rounds, and b is the key size in bytes. For the AES competition, $w = 32$, $r = 20$, and $b \in \{16, 24, 32\}$, and RC6 is a shorthand for these parameter choices. All internal cipher operations are over w -bit words, where $w \in \{8, 16, 32, 64\}$. Fig. 1 describes one round of the RC6 encryption algorithm with pre- and

² An immediate advantage of incremental generation of plaintexts over random generation is faster attack simulations.

post-whitening. Each text block contains four w -bit words (A , B , C and D) and $(A_i, \dots, D_i)$ denote the words at the i -th round. The w -bit round keys are indexed $S[0], \dots, S[2r + 3]$. The key scheduling algorithm generates the round keys from the b -byte cipher key. We do not exploit the key scheduling algorithm in our analysis; therefore, we omit its description and refer the interested reader to [24]. Former security analyses of RC6 include differential and linear analyses [24], multiple linear relations [27], and χ^2 analyses [3, 14, 24, 28].

Fig. 1. Computational graph of the RC6 cipher for encryption: pre-whitening, one full round and post-whitening

3.2 MRC6

The MRC6 block cipher was proposed in [8], with main focus on performance evaluation. No security analysis was presented. Just like RC6, MRC6 is a parameterized family of ciphers. Thus, formally MRC6 stands for MRC6- $w/r/b$. But, nominal values of these parameters were omitted in [8]; one can find the values $w = 32$, $b = 16$ (128-bit key) and $r = 16$ rounds when the software performance of MRC6 is compared with that of the AES and RC6 (on Pentium-III, with the nominal parameters, MRC6 encrypts at about 19.5 MB/sec making it nearly twice as fast as RC6). Otherwise, these parameters are unspecified. In fact, this also helps adapt MRC6 as a compression function using hash modes [18] such as Miyaguchi-Preneel and Mathyas-Meier-Oseas, where the key and text inputs have different sizes. MRC6 follows a generalized Feistel network structure, similar to RC6, but each text block contains sixteen w -bit words ($A, \dots, P$), instead of the four words in RC6. Moreover, the w -bit round keys are indexed $S[0], \dots, S[8r + 7]$. Like in RC6, there are pre-whitening and post-whitening layers before and after the r rounds of MRC6, respectively. Here again, we omit the description of the key scheduling algorithm and refer the reader to [8]. In these layers the round keys are XOR-ed with intermediate encryption values. Fig. 2 in Appendix B describes one round of the MRC6 encryption algorithm with pre- and post-whitening. In our experiments, we use MRC6 with $w = 32$ and $b = 16$.

3.3 ERC6

The ERC6 block cipher was proposed in [22]. ERC6 is, again, a parameterized family of ciphers. Thus, ERC6 stands for ERC6- $w/r/b$, with $w \in \{16, 32, 64\}$, $r \in \{0, 1, 2, \dots, 255\}$, $b \in \{0, 1, 2, \dots, 255\}$. These parameters appear to be loosely coupled. On Pentium-III, with the parameters $w = 32$, $b = 16$ and $r = 16$, ERC6 encrypts at about 17.3 MB/sec making it about 1.7 times faster than RC6. The ERC6 follows a generalized Feistel network structure, similar to the RC6 and the MRC6, but each block contains eight w -bit words ($A, \dots, H$), instead of the four words in RC6. The w -bit round keys are indexed $S[0], \dots, S[4r+7]$. Here again, there are pre-whitening and post-whitening layers, consisting of the XOR of key-dependent words with intermediate encryption values. Fig. 4 in Appendix C describes one round of the ERC6 encryption algorithm with pre- and post-whitening. In our experiments, we use ERC6 with $w = 32$ and $b = 16$.

4 Experimental Observations

The χ^2 attack operates in a chosen-plaintext setting. Our experiments distinguish r rounds of MRC6 from a random permutation. To exemplify the setting we take MRC6 as an example. We fix up the $8 \cdot \log_2 w$ least significant bits of words $A_0, C_0, E_0, G_0, I_0, K_0, M_0$ and O_0 (that is, including the pre-whitening), and analyse the combined $8 \cdot y$ least significant bits ($y \in \{1, 2\}$) of $A_{2i}, C_{2i}, E_{2i}, G_{2i}, I_{2i}, K_{2i}, M_{2i}$ and O_{2i} , for $i > 0$, that is, after an even number of rounds.

4.1 Reduced-Round RC6

For RC6, the χ^2 test is motivated by an ensemble of linear relations involving up to the five least significant bits of words A_i and C_i for every two rounds [5]. These linear relations are represented by

$$A_i \cdot e_{t_1} \oplus C_i \cdot e_{t_2} = A_{i+2} \cdot e_{t_3} \oplus C_{i+2} \cdot e_{t_4}, \quad (3)$$

where A_i and C_i denote the first and third input words to the i -th round. Each bitmask, e_j , contains only a single bit equal to one, in the j -th least significant bit ($j = 0$ denotes the lsb). This is the lowest possible Hamming weight and is given by $e_j = 2^j$, $0 \leq j \leq 31$. Table 1 shows the result of the experiment on reduced-round RC6 using our method in the case of the 10 bits: $\text{lsb}_5(A)$ and $\text{lsb}_5(C)$. We use $v_{95} = 1098$ (95% specificity) to facilitate comparison, since [14] also uses the same threshold. Moreover, for the same comparison purpose, we did not use confidence intervals here. In Table 1, note that with 2^2 texts we already start to reach (and gradually better) the results of [14] (Table 6), whereas they needed 2^{13} texts instead to arrive at a χ^2 value of 1096 (95% specificity). For four rounds, we noticed very close approximations for the same χ^2 values with 2^{18} texts, while [14] required 2^{29} texts to arrive at data with the same specificity. For six or more rounds we could not detect correlation up to 2^{36} texts.

4.2 MRC6

For MRC6, one (iterative) linear relation that guides the χ^2 attack is $A_i \cdot e_{t_1} \oplus C_i \cdot e_{t_2} \oplus E_i \cdot e_{t_3} \oplus G_i \cdot e_{t_4} \oplus I_i \cdot e_{t_5} \oplus K_i \cdot e_{t_6} \oplus M_i \cdot e_{t_7} \oplus O_i \cdot e_{t_8} = A_{i+2} \cdot e_{t_9} \oplus C_{i+2} \cdot e_{t_{10}} \oplus E_{i+2} \cdot e_{t_{11}} \oplus$

Table 1. χ^2 attack simulations on RC6, $2^{10} - 1$ degrees of freedom and 20 tests

#Rounds	$\log_2 N$	average χ^2	hypothesis
2	2	1071.2	H_0
2	3	1169.6	H_1
2	4	1398.4	H_1
2	5	1561.6	H_1
2	6	2009.6	H_1
4	16	1039.5	H_0
4	17	1066.3	H_0
4	18	1094.2	H_0
4	19	1151.6	H_1
4	20	1267.6	H_1
6	32	1030.6	H_0
6	33	1036.0	H_0
6	34	1020.6	H_0
6	35	1018.1	H_0
6	36	1028.4	H_0

$G_{i+2} \cdot e_{t_{12}} \oplus I_{i+2} \cdot e_{t_{13}} \oplus K_{i+2} \cdot e_{t_{14}} \oplus M_{i+2} \cdot e_{t_{15}} \oplus O_{i+2} \cdot e_{t_{16}}$, where $A_i, C_i, E_i, G_i, I_i, K_i, M_i$ and O_i are input words to the i -th round. In particular, the masks e_j with highest bias are such that $0 \leq j < 5$, that is, the bits in the masks restricted to the five least significant bit (lsb) positions. Fig. 3 in Appendix B illustrates the linear trail for the iterative linear relation mentioned above.

Table 2 shows the result of the experiment in the case of the 8 bits: $\text{lsb}_1(A), \text{lsb}_1(C), \text{lsb}_1(E), \text{lsb}_1(G), \text{lsb}_1(I), \text{lsb}_1(K), \text{lsb}_1(M)$ and $\text{lsb}_1(O)$. We use $v_{75} = 269.85$. Starting from six rounds, the number of texts for which H_0 is rejected starts to increase by a factor of about 2^{10} every two rounds. Thus, for r rounds (r even and $r \geq 6$), the following is expected for N in terms of r : $N = 2^9 \cdot 2^{10 \cdot (r-6)/2} = 2^{5r-21}$ (this linear function in the exponent has to be further confirmed experimentally).

In the extreme situation, $\text{TEST}()$ chooses plaintexts such that the $\text{lsb}_5(A_0), \text{lsb}_5(C_0), \dots, \text{lsb}_5(O_0)$ are set to zero, while the remaining bits may be arbitrary. This implies at most $2^{512-40} = 2^{472}$ plaintext blocks. Thus, this analysis holds as long as $2^{5r-21} \leq 2^{472}$, or $5r \leq 493$, or $r \leq 98$. Since the attack effort is at most 2^{472} plaintext blocks, it means that MRC6 would require at least $r = 99$ rounds, to counter this χ^2 attack; otherwise, one could (theoretically) break it with fewer plaintexts than the code book.

Table 3 shows the result of the experiment in the case of 16 bits: $\text{lsb}_2(A), \text{lsb}_2(C), \text{lsb}_2(E), \text{lsb}_2(G), \text{lsb}_2(I), \text{lsb}_2(K), \text{lsb}_2(M)$, and $\text{lsb}_2(O)$ after an even number of rounds of MRC6. Starting from six rounds, the number of texts for which H_0 is rejected starts to increase by a factor of about 2^{10} every two rounds. Thus, for r rounds (r even and $r \geq 6$), the following is expected for N in terms of r : $N = 2^{12} \cdot 2^{10 \cdot (r-6)/2} = 2^{5r-18}$ (the linear function in the exponent has to be further confirmed experimentally). The analysis is similar to the 8-bit case in the previous paragraph. Following the same rationale, at most $2^{512-40} = 2^{472}$ plaintext blocks will be available. Thus, this analysis holds as long as $2^{5r-18} \leq 2^{472}$, or $5r \leq 490$, or $r \leq 98$. Again, since the attack effort is at most 2^{472} plaintext blocks, MRC6 requires at least 99 rounds to counter this χ^2 attack. In order to compare the approach in Table 2 with an alternative approach used in [14], we provide Table 4. Empirically, we have

Table 2. χ^2 attack simulations on MRC6, $2^8 - 1$ degrees of freedom and 20 tests

#Rounds	$\log_2 N$	average χ^2	minCI	#values > v_{75}	hypothesis
2	1	305.2	264.6	4	H_0
2	2	444.0	376.8	18	H_1
2	3	667.2	622.9	20	H_1
4	3	299.2	262.8	8	H_0
4	4	321.6	303.0	19	H_1
4	5	368.8	353.7	20	H_1
6	8	265.8	256.7	8	H_0
6	9	282.1	270.6	11	H_1
6	12	370.8	343.3	20	H_1
8	18	273.0	265.0	11	H_0
8	19	288.1	279.8	16	H_1
8	20	327.5	311.1	20	H_1
10	27	273.5	265.4	11	H_0
10	28	288.2	275.7	12	H_1
10	33	434.1	374.1	20	H_1

Table 3. χ^2 attack simulations on MRC6, $2^{16} - 1$ degrees of freedom and 20 tests

#Rounds	$\log_2 N$	average χ^2	minCI	#values > v_{75}	hypothesis
2	1	68810.8	63145.2	1	H_0
2	2	80277.6	72615.5	8	H_1
2	4	125731.2	116640.0	20	H_1
4	4	65520.0	65520.0	0	H_0
4	5	66732.8	65828.2	5	H_1
4	8	74035.2	72727.0	20	H_1
6	11	65804.8	65643.3	12	H_0
6	12	66108.8	65941.0	16	H_1
6	13	66850.4	66685.1	20	H_1
8	20	65804.6	65648.0	11	H_0
8	21	66090.0	65912.8	15	H_1
8	23	68275.1	67872.4	20	H_1
10	30	65637.4	65450.0	9	H_0
10	31	65916.7	65760.9	14	H_1
10	35	67043.6	66671.7	19	H_1

Table 4. χ^2 attack simulations on MRC6 using the approach in [14] with $2^8 - 1$ degrees of freedom

#Rounds	$\log_2 N$	average χ^2	minCI	#values > v_{75}	hypothesis
2	21	268.0	262.1	12	H_0
2	22	276.8	271.4	11	H_1
2	24	326.4	320.1	20	H_1
4	29	256.9	250.6	8	H_0
4	30	251.1	245.8	4	H_0
4	31	257.5	252.1	8	H_0
4	32	258.7	254.0	5	H_0
4	33	255.6	251.1	4	H_0
6	25	265.5	258.4	9	H_0
6	26	258.7	253.2	8	H_0
6	27	253.0	247.8	6	H_0
6	28	251.3	246.2	4	H_0
6	29	254.9	248.6	6	H_0

observed that much fewer chosen plaintexts are needed in the new approach than in the conventional approach of [14], at least for two, four and six rounds.

We would like to point out an issue in Table 2 and Table 3, which is the minimum value of N for which H_1 is accepted. This value of N may be less than $5 \cdot (k - 1)$ when the number of rounds is small. For example, observe the values of N for 2, 4 and 6 rounds in Table 2. This phenomenon is particular for a small number of rounds, and is due to the slow diffusion in MRC6. Recall that unlike the AES, in which diffusion is guaranteed by an MDS matrix, in MRC6 the diffusion depends on nonzero rotation at especific points in the cipher (and may take more than six round to be complete). Therefore, we also use these values of N to estimate (by extrapolation) the minimum values of N , for which H_1 is accepted, for higher numbers of rounds. The values (including the extrapolated ones) of N for 8 or more rounds of MRC6 are found to be greater than $5 \cdot (k - 1)$. Besides, they are also smaller than the corresponding values of N obtained using the approach in [14].

4.3 ERC6

For ERC6, (one) iterative linear relation that guides the χ^2 attack is $A_i \cdot e_{t_1} \oplus C_i \cdot e_{t_2} \oplus E_i \cdot e_{t_3} \oplus G_i \cdot e_{t_4} = A_{i+2} \cdot e_{t_5} \oplus C_{i+2} \cdot e_{t_6} \oplus E_{i+2} \cdot e_{t_7} \oplus G_{i+2} \cdot e_{t_8}$, where A_i , C_i , E_i and G_i , are input words to the i -th round. In particular, the masks e_j with highest bias are such that $0 \leq j < \log_2 w$, that is, the bits in the masks restricted to the $\log_2 w$ least significant bit positions. Fig. 5 in Appendix C illustrates the linear trail for the iterative linear relation mentioned above.

Table 5 shows the result of attack simulation in the case of 4 bits: $\text{lsb}_1(A)$, $\text{lsb}_1(C)$, $\text{lsb}_1(E)$ and $\text{lsb}_1(G)$ after an even number of rounds of ERC6. Starting from four rounds, the number of texts for which H_0 is rejected starts to increase by a factor of about 2^{11} every two rounds (although this behaviour still has to be further confirmed experimentally). Thus, for r rounds (r even and $r \geq 4$), the following is expected: $N = 2^{13} \cdot 2^{11 \cdot (r-4)/2} = 2^{5.5r-9}$. The algorithm TEST chooses plaintexts such that the $\text{lsb}_5(A_0)$, $\text{lsb}_5(C_0)$, $\text{lsb}_5(E_0)$, $\text{lsb}_5(G_0)$ are set to zero. This implies at most $2^{256-20} = 2^{236}$ plaintext blocks. Thus, this analysis holds

as long as $2^{5.5r-9} \leq 2^{236}$, or $5.5r \leq 245$, or $r \leq 44$. Since the attack effort is at most 2^{236} plaintext blocks, it means that ERC6 would require at least 45 rounds to counter this χ^2 attack; otherwise, one could (theoretically) break it with fewer plaintexts than the code book. In order to compare the approach in Table 5 with an alternative approach used in

Table 5. χ^2 attack simulations on ERC6, $2^4 - 1$ degrees of freedom and 20 tests

#Rounds	$\log_2 N$	average χ^2	minCI	#values > v_{75}	hypothesis
2	1	18.0	15.25	5	H_0
2	2	26.4	22.44	8	H_1
2	3	37.8	34.20	20	H_1
4	12	26.9	22.08	10	H_0
4	13	38.7	28.95	14	H_1
4	17	446.8	276.82	20	H_1
6	23	26.0	20.23	10	H_0
6	24	37.9	27.31	13	H_1
6	28	375.3	258.18	20	H_1

[14], we provide Table 6. Empirically, we have observed that significantly much fewer chosen

Table 6. χ^2 attack simulations on ERC6 using the approach in [14] with $2^4 - 1$ degrees of freedom and 20 tests

#Rounds	$\log_2 N$	average χ^2	minCI	#values > v_{75}	hypothesis
2	15	17.1	14.1	8	H_0
2	16	26.8	22.9	16	H_1
2	17	35.2	31.3	20	H_1
4	32	14.833	12.03	6	H_0
4	33	16.633	13.87	6	H_0
4	34	14.549	12.56	5	H_0
4	35	15.257	13.20	4	H_0
4	36	13.143	11.25	2	H_0

plaintexts are needed in the new approach than in the conventional approach of [14], at least for two and four rounds.

Table 7 shows the result of analysing the 8-bit value from the concatenation of $\text{lsb}_2(A)$, $\text{lsb}_2(C)$, $\text{lsb}_2(E)$ and $\text{lsb}_2(G)$ after an even number of rounds of ERC6. Starting from four rounds, the number of texts for which H_0 is rejected starts to increase by a factor of about 2^{12} every two rounds (although this behaviour still has to be further confirmed experimentally). Thus, for r rounds (r even and $r \geq 4$), the following is expected: $N = 2^{12} \cdot 2^{12 \cdot (r-4)/2} = 2^{6r-12}$. Following a similar reasoning as in the previous paragraph, this analysis holds as long as $2^{6r-12} \leq 2^{236}$, or $6r \leq 248$, or $r \leq 41$. Since the attack effort is at most 2^{236} plaintext blocks, ERC6 requires at least 42 rounds to counter this χ^2 attack.

Table 7. χ^2 attack simulations on ERC6, $2^8 - 1$ degrees of freedom and 20 tests

#Rounds	$\log_2 N$	average χ^2	minCI	#values $> v_{75}$	hypothesis
2	2	309.6	272.0	7	H_0
2	3	356.8	316.6	15	H_1
2	4	520.0	444.0	20	H_1
4	11	284.5	270.3	9	H_0
4	12	310.0	291.0	14	H_1
4	15	711.6	579.7	20	H_1
6	23	290.5	283.5	14	H_0
6	24	325.6	311.9	18	H_1
6	25	404.5	379.9	19	H_1
6	26	549.3	491.7	20	H_1
8	34	252.9	247.1	1	H_0
8	35	259.5	253.5	0	H_0
8	36	259.1	250.3	2	H_0

5 Conclusions and Open Problems

In this paper, a new approach to the χ^2 statistical test was presented. A modified version of this approach, aided by linear cryptanalysis, was applied to the block ciphers RC6, MRC6 and ERC6. For 2-round and 4-round RC6, our method improves the data complexity of the previously best-known (conventional) χ^2 attacks [14] by a factor of 2^{11} each. Tables 8, 9, 10 and 11 summarise our attacks on the other members of the RC6-family.

The attacks reduced the number of chosen-plaintexts to detect χ^2 correlation when compared to conventional χ^2 attacks. Consequently, we could apply (and check in practice) our predictions on attacks up to ten rounds of MRC6 and ERC6. The reduction in the data complexity of our attacks was somehow influenced by the weak diffusion in our target ciphers. Nonetheless, the approach observed deserves further investigation.

In the analyses of M6, MX and RC5P, the χ^2 tests were supported by evidence collected from mod- n analyses of these ciphers. The nonuniform distribution of residues modulo n of internal cipher components, for n a prime number, was corroborated by experimental χ^2 tests. Likewise, in this paper, our results are supported by linear relations. Maybe the framework of [29] would still apply on MRC6 with our new attack strategy. We leave it as an open problem.

The analysis presented in this paper considered sets of randomly chosen keys, that is, no particular (weak) keys were purposefully used. This implies that even better results could have been achieved with keys that caused null rotation in some rounds under analysis [14]. This issue of weak keys for χ^2 attacks is left as a problem for future work.

Table 8. Summary of χ^2 attacks analysing 8 bits output by MRC6 (CP: Chosen Plaintexts)

#Rounds	Time	Data	Memory	Comment
2	2^2	2^2 CP	2^2	Table 2
4	2^4	2^4 CP	2^4	Table 2
r	2^{5r-21}	2^{5r-21} CP	2^{5r-21}	$6 \leq r < 99$, r even

Table 9. Summary of χ^2 attacks analysing 16 bits output by MRC6 (CP: Chosen Plaintexts)

#Rounds	Time	Data	Memory	Comment
2	2^2	2^2 CP	2^2	Table 3
4	2^5	2^5 CP	2^5	Table 3
r	2^{5r-18}	2^{5r-18} CP	2^{5r-18}	$6 \leq r < 99$, r even

Table 10. Summary of χ^2 attacks analysing 4 bits output by ERC6 (CP: Chosen Plaintexts)

#Rounds	Time	Data	Memory	Comment
2	2^2	2^2 CP	2^2	Table 5
4	2^{13}	2^{13} CP	2^{13}	Table 5
r	$2^{5.5r-9}$	$2^{5.5r-9}$ CP	$2^{5.5r-9}$	$4 \leq r < 45$, r even

Table 11. Summary of χ^2 attacks analysing 8 bits output by ERC6 (CP: Chosen Plaintexts)

#Rounds	Time	Data	Memory	Comment
2	2^3	2^3 CP	2^3	Table 7
4	2^{11}	2^{11} CP	2^{11}	Table 7
r	2^{6r-12}	2^{6r-12} CP	2^{6r-12}	$4 \leq r < 42$, r even

Acknowledgments

We thank the anonymous reviewers of ISC 2009 for their constructive comments on our work.

References

1. AES, “The Advanced Encryption Standard Development Process,” 1997, available at <http://csrc.nist.gov/encryption/aes/>.
2. L.J. Bain, M. Engelhardt, *Introduction to Probability and Mathematical Statistics*, Duxbury Press, Boston, 1987.
3. O. Baudron, H. Gilbert, L. Granboulan, H. Handschuh, A. Joux, P. Nguyen, F. Noilhan, D. Pointcheval, T. Pornin, G. Poupard, J. Stern, S. Vaudenay, “Report on the AES candidates,” available at <http://csrc.nist.gov/encrypt/aes/round1/conf2/papers/baudron1.pdf>.
4. J.L. Beuchat, “FPGA Implementations of the RC6 Block Cipher,” *FPL 2003* (P.Y.K. Cheung *et al.*, eds.), vol. 2778 of *LNCS*, pp. 101-110, Springer-Verlag, 2003.
5. S. Contini, R.L. Rivest, M.J.B. Robshaw, Y.L. Yin, “The Security of the RC6 Block Cipher,” v.1.0, 1998.
6. Cryptography Research and Evaluation Committees (CRYPTREC), available at <http://www.cryptrec.go.jp/english/>.
7. J. Daemen, V. Rijmen, “The Design of Rijndael – AES – The Advanced Encryption Standard,” Springer-Verlag, 2002.

8. N.A. El-Fishawy, T.E. Danaf, O.M.A. Zaid, "A Modification of RC6 Block Cipher Algorithm for Data Security (MRC6)," *International Conference on Electrical, Electronic and Computer Engineering 2004*, pp. 222-226, 2004.
9. H. Gilbert, H. Handschuh, A. Joux, S. Vaudenay, "A Statistical Attack on RC6," *Fast Software Encryption 2000* (B. Schneier, ed.), vol. 1978 of *LNCS*, pp. 64-74, Springer-Verlag, 2000.
10. H. Handschuh, H. Gilbert, " χ^2 Cryptanalysis of the SEAL Encryption Algorithm," *Fast Software Encryption 1997* (E. Biham, ed.), vol. 1267 of *LNCS*, pp. 1-12, Springer-Verlag, 1997.
11. T. Hinoue, A. Miyaji, T. Wada, "The Security of RC6 against Asymmetric Chi-square Test Attack," *IPSI Journal*, 48:(9), pp. 1-10, 2007.
12. N. Isogai, T. Matsunaka, A. Miyaji, "Optimized χ^2 -attack against RC6," *ACNS 2003* (J. Zhou, M. Yung, Y. Han, eds.), vol. 2846 of *LNCS*, pp. 16-32, Springer-Verlag, 2003.
13. J. Kelsey, B. Schneier, D. Wagner, "Mod n Cryptanalysis, with Applications against RC5P and M6," *Fast Software Encryption 1999* (L.R. Knudsen, ed.), vol. 1636 of *LNCS*, pp. 139-155, Springer-Verlag, 1999.
14. L.R. Knudsen, W. Meier, "Correlations in RC6 with a Reduced Number of Rounds," *Fast Software Encryption 2000* (B. Schneier, ed.), vol. 1978 of *LNCS*, pp. 94-108, Springer-Verlag, 2000.
15. D. Knuth, "The Art of Computer Programming," *Seminumerical Algorithms* (3rd ed.), Reading, Massachusetts: Addison-Wesley, 1997.
16. M. Matsui, "Linear Cryptanalysis Method for DES Cipher," *Eurocrypt 1993* (T. Helleseth, ed.), vol. 765 of *LNCS*, pp. 386-397, Springer-Verlag, 1994.
17. T. Matsunaka, A. Miyaji, Y. Takano, "Success Probability in χ^2 Attacks," *ACNS 2004* (M. Jakobsson, M. Yung, eds.), vol. 3089 of *LNCS*, pp. 310-325, Springer-Verlag, 2004.
18. A.J. Menezes, P.C. van Oorschot, S. Vanstone, "Handbook of Applied Cryptography," CRC Press, 1997.
19. New European Schemes for Signatures, Integrity and Encryption (NESSIE), available at <https://www.cosic.esat.kuleuven.be/nessie/>.
20. NIST, "Data Encryption Standard," Federal Information Processing Standards Publication 46-2, 1993.
21. M. Nonaka, A. Miyaji, "A Note on the Security of RC6 Against Correlation Attack," *The 2002 Symposium on Cryptography and Information Security*, pp. 681-686, 2002.
22. A.H.M. Ragab, N.A. Ismail, O.S. Farag Allah, "Enhancements and Implementation of RC6 Block Cipher for Data Security," *IEEE TENCON 2001*, 2001.
23. V. Rijmen, J. Daemen, B. Preneel, A. Bosselaers, E.D. Win, "The Cipher SHARK," *Fast Software Encryption 1996* (D. Gollmann, ed.), vol. 1039 of *LNCS*, pp. 99-112, Springer-Verlag, 1996.
24. R.L. Rivest, M.J.B. Robshaw, R. Sidney, Y.L. Yin, "The RC6 Block Cipher," *1st AES Conference*, 1998, available at <http://csrc.nist.gov/encryption/aes/>.
25. SHA-2, "Federal Information Processing Standard 180-2, Secure Hash Standard," National Institute of Standards and Technology, 2002.
26. C.E. Shannon, "A Mathematical Theory of Communication," *Bell System Technical Journal*, vol. (27):3, pp. 379-423, 623-656, 1948.
27. T. Shimoyama, M. Takenaka, T. Koshida, "Multiple Linear Cryptanalysis of a Reduced-Round RC6," *The 2002 Symposium on Cryptography and Information Security*, pp. 931-936, 2002.
28. T. Shimoyama, K. Takeuchi, J. Hayakawa, "Correlation Attack to the Block Cipher RC5 and the Simplified Variants of RC6," 2001, available at <http://csrc.nist.gov/encryption/aes/>.
29. M. Takenaka, T. Shimoyama, T. Koshida, "Theoretical Analysis of Correlations in RC6," available at <http://eprint.iacr.org/2002/176.pdf>.
30. S. Vaudenay, "An Experiment on DES Statistical Cryptanalysis," technical report LIENS-95-29, Ecole Normale Supérieure, 1995.

A Reference Table for χ^2 Values

Table 12 gives the χ^2 threshold values for various degrees of freedom and specificities.

B MRC6 - Computational Graph and Linear Trail

Fig. 2 describes one full round of MRC6 with pre- and post-whitening. Fig. 3 shows the trail corresponding to the linear attacks briefly outlined in Sect. 4.2.

Table 12. χ^2 threshold values, specificities and degrees of freedom

χ^2	Degrees of Freedom ($k - 1$)					
	$2^4 - 1$	$2^8 - 1$	$2^{12} - 1$	$2^{16} - 1$	$2^{20} - 1$	$2^{24} - 1$
Specificity ($1 - \alpha$)	0.70	17.32	266.34	4141.97	65724.37	1049333.93
	0.75	18.24	269.85	4155.67	65778.82	1049551.40
	0.80	19.31	273.79	4170.96	65839.50	1049793.60
	0.85	20.60	278.43	4188.84	65910.27	1050075.96
	0.90	22.31	284.34	4211.40	65999.39	1050431.31
	0.95	24.99	293.25	4244.99	66131.63	1050958.14
	0.99	30.58	310.46	4308.47	66380.16	1051946.85
						16780252
						16781122
						16782090
						16783219
						16784639
						16786744
						16790690

Fig. 2. Computational graph of the MRC6 cipher for encryption: pre-whitening, one full round and post-whitening

C ERC6 - Computational Graph and Linear Trail

Fig. 4 describes one full round of ERC6 with pre- and post-whitening. Fig. 5 shows the trail corresponding to the linear attacks briefly outlined in Sect. 4.3.

Fig. 3. Linear trail for MRC6

Fig. 4. Computational graph of the ERC6 cipher for encryption: pre-whitening, one full round and post-whitening

Fig. 5. Linear trail for ERC6