| Fişa suspiciunii de plagiat / Sheet of plagiarism's suspicion | Indexat la: 39/01 |
|---|---|

| Opera suspicionată (OS) | Opera autentică (OA) |
|---|---|
| Suspicious work | Authentic work |

| | |
|---|---|
| OS | MANG, Erica, MANG, Ioan, POPESCU, Constantin. Cryptanalise aspects on the block ciphers of RC5 and RC6. *Proceedings of International Symposium on System Theory.* SINTES'11, Craiova, 2003, p.1-6, Disponibil la: http :// ace . ucv . ro / sintes11 / Volume2 / 4%20COMPUTERS % 20ENGINEERING / IC10_Mang _ Erica _ 1.pdf. |
| OA | SHIMOYAMA, T., TAKEUCHI, K., HAYAKAWA, J. Correlation atack to the block cipher RC5 and the simplified variantes of RC6. 2001. p.2-15, Disponibil la: http: // www . google . ro / url ? sa = t&rct = j&q = &esrc = s&source = web&cd = 1&ved = 0CHMQFjAA&url = http%3A%2F%2Fciteseerx . ist . psu . edu % 2Fviewdoc % 2Fdownload % 3Fdoi % 3D10.1.1.31.2917 % 26rep % 3Drep1 % 26type % 3Dpdf&ei = h0ipT82GCPOK4gT _ hbHMCQ & usg = AFQjCNFqjSpnl64zpjr-m6g3K2FgHssXIA |

| Incidența minimă a suspiciunii / Minimum incidence of suspicion | | | |
|---|---|---|---|
| p.1:1s – p.1:16s. | p.1:10 – p.1:21 | p.1:19s – p.6: 21 | p.1:22 – p.13:6 |
| p.2:Table 1 | p.3:Table 1 | p.3:Table 2 | p.5:Table2 |

SINTES 11:

AUTOMATION:



COMPUTERS ENGINEERING:

- COLLABORATIVE DISTANCE LEARNING WITHIN LABORATORIES BY USING VIRTUAL ENVIRONMENT - Ileana Hamburg, Oleg Cernian, Dan Mancas, Nicolae Cismaru, Lucian Bărbulescu
- THE INFORMATION QUALITY- SOME CONSIDERATIONS - Augustin-Iulian Ionescu, Eugen Dumitrascu
- CNC FOR EDM MACHINE TOOL – HARDWARE STRUCTURE - Ioan Lemeni
- MOBILE DISTRIBUTED SOLUTION FOR DELIVERY AUTOMATION: DESIGN AND PARTICULARITIES - Anita Lungu
- ANALYZING TRAFFIC TOOLS ON AN IPsec COMMUNICATION LINK - Marin Lungu
- CRYPTANALISE ASPECTS ON THE BLOCK CIPHERS OF RC5 AND RC6 - Erica Mang, Ioan Mang, Constantin Popescu
- TWO DIFFERENT ARCHITECTURES FOR THE HARDWARE IMPLEMENTATION OF THE RIJNDAEL ALGORITHM - Erica Mang
- “ON LINE” TESTING FOR SOFTWARE DESIGN - Marian Gheorghe, Mihaiu Ilie Mircea Dumitrascu Eugen, Enescu Nicolae-Iulian
- Support for public-key infrastructures in DNS - Marius Marian, Diana Berbecaru
- A DIGITAL EQUIPMENT FOR MEASURING, RECORDING AND CONTROL OF THE RAILWAY VEHICLES’ SPEED - Constantin Patrascu
- IMPLEMENTING LARGE DATASET SYNCHRONIZATION ON RESOURCE LIMITED MOBILE TERMINALS - Constantin Pistol
- BOUNDARY SCAN STANDARD – A PREREQUISITE THAT ENSURE GLOBAL HARDWARE SYSTEM QUALITY - Corneliu Popescu
- THE PERFORMABILITY ANALYSIS FOR DIFFERENT KIND OF ADDERS - Daniela Elena Popescu
- XML MESSAGING: SIMPLE OBJECT ACCESS PROTOCOL (SOAP) - Gabriel Toma-Tumbar, Dan-Ovidiu Andrei
- A ROUTING ALGORITHM FOR URBAN ADVISORY SYSTEM - Honoriu Valean, Tiberiu Letia, Adina Astilean

ELECTRONICS:

- SELECTING THE RIGHT SENSOR FOR TEMPERATURE MEASUREMENT - Mihai Bogdan, Maria Vintan
- QUALITY ASSURANCE BY AUTOMATED DEFECT DETECTION OF TEXTILE FABRICS - Raluca Brad, Remus Brad
- THE ANALYSIS OF THE THREE PHASE RECTIFIER WITH SEVERAL PULSES - Danila Cerbulescu
- ADAPTIVE NOTCH IIR FILTERS. AN IMPLEMENTATION ON MOTOROLA SC140 - Silviu Ciochina, Cristina Ciochina, Andrei Roman
- NUMERICAL OSCILLATIONS IN ELECTROMAGNETIC TRANSIENTS PROGRAMS - Liana Cipcigan
- SIGNALLING IN TELECOMMUNICATION NETWORKS - Pompiliu Constantinache, Adrian Constantinache
- A HIGH-FREQUENCY AND LOW-VOLTAGE CMOS AMPLIFIER - Elena Doicaru, Traian-Titi Serban
- METHOD OF COMPUTATIONAL INTELLIGENCE IN POWER ELECTRONICS - Adriana Florescu, Dan Alexandru Stoichescu, Dumitru Stanciu
- BIOMEDICAL SIGNAL ACQUISITION EQUIPMENT USING LABVIEW ENVIRONMENT - Beriliu Ilie
- GAS EXCHANGE CONCENTRATION RESPONSES DURING STRESS TEST WITH BRUCE PROTOCOL EXERCISE - Beriliu Ilie
- STEADY-STATE ANALYSIS OF COUPLED-INDUCTOR CUK PWM CONVERTER Part I: Continuous Conduction Mode - Elena Niculescu
- STEADY-STATE ANALYSIS OF COUPLED-INDUCTOR CUK PWM CONVERTER Part II: Discontinuous Conduction Mode - Elena Niculescu
- SHAPE RECOGNITION METHOD BASED ON THE k-NEAREST NEIGHBOR RULE - Dorina Purcaru
- NOVEL CURRENT AND VOLTAGE SENSORS FOR DIGITAL INSTRUMENTATION IN POWER STATIONS - Traian-Titi Serban, Elena Doicaru
- PHASE SHIFT AND POWER FACTOR DIGITAL METER - Traian-Titi Serban
- A GENERALIZED SOLUTION FOR SLIDING MODE CONTROL - Dumitru Stanciu, Dan Alexandru Stoichescu, Adriana Florescu
- TRANSMISSION TOWER POTENTIALS DURING GROUND FAULTS - Maria VINTAN, Mihai BOGDAN

MECHATRONICS:

- SOME RESULTS IN THE EVALUATION OF A SONAR SYSTEM FOR RECOGNITION OF THE ENVIRONMENT BY MOBILE ROBOTS - Dorel Aiordachioaie, Herbert Peremans, Andre Boen
- ON ESTIMATION OF THE ORIENTATION OF MOBILE ROBOTS USING SONAR INFORMATION AND TURNING FUNCTIONS - Dorel Aiordachioaie, Herbert Peremans, Andre Boen
- CONVENTIONAL CONTROL OF A SHAPE MEMORY ALLOY ROBOTICS UNIT - Nicu-George Bizdoaca, Elvira Bizdoaca, Sonia Degeratu

- SINGLE LINK ROBOT ACTUATED WITH SHAPE MEMORY ALLOY - Nicu-George Bizdoaca, Daniela Pana, Sonia Degeratu, Elvira Bizdoaca, Cristina Pana, Marius Niculescu
- A MECHATRONICS APPLICATION - Dorian Cojocaru, Claudiu Milosi
- Virtual Robot Center – E_LABORATORY SOLUTION - Ciprian Comsa, Robert Mitrica, Mircea Nitulescu, Gabriel Vladut
- THE IMPLEMENTATION OF A PROGRAMMABLE LOGIC CONTROLLER FOR THE AUTOMATION OF THE BELT CONVEYOR - Mihai Dobriceanu, Alexandru Bitoleanu, Mihaela Popescu
- EXPERIMENTAL RESULTS CONCERNING THE MONITORING OF THE MACHINES' DRIVES IN CARBON EXPLOITATIONS - Mihai Dobriceanu, Alexandru Bitoleanu, Mihaela Popescu
- SUR L'ANALYSE DES SYSTEMES HYBRIDES A L'AIDE DE RESEAUX DE PETRI - Mircea Adrian Drighiciu
- APPLICATION DES RESEAUX DE PETRI HYBRIDES A L'ETUDE DES SYSTEMES DE PRODUCTION A HAUTE CADENCE - Mircea Adrian Drighiciu, Gheorghe Manolea
- SLIDING MODE CONTROL FOR AN ELECTRORHEOLOGICAL FLUID ACTUATOR - Mihaela Cecilia Florescu, Anca Petrisor
- KNOWLEDGE EXTRACTION WITH COMPETITIVE NEURAL NETWORKS IN MATLAB ENVIRONMENT - Luminita Giurgiu
- HIGH PERFORMANCE ALGORITHMS IN FEEDFORWARD NEURAL NETWORKS BACKPROPAGATION TRAINING - Luminita Giurgiu
- ON NEURAL NETWORK CLASSIFIERS WITH SUPERVISED TRAINING - Marius Kloetzer, Octavian Pastravanu
- ROLE OF ANIMATION IN TEACHWARE FOR CONTROL ENGINEERING – A CASE STUDY - Cristian Mahulea, Mihaela-Hanako Matcovschi, Octavian Pastravanu
- THE MATHEMATICAL MODEL OF A WALKING ROBOT WITH THREE FREE JOINTS - Constantin Marin, Anca Petrisor
- Pilotage a distance de systemes automatises et robotises - problemes poses et solutions envisagees - Serge Monchaud, Gabriel Vladut
- GENERAL DESIGN OF A DRIVEN WHEEL MOBILE ROBOT WITH A PATH STRORED IN MEMORY - Mircea Nitulescu
- FUZZY CONTROL FOR ROBOT'S DRIVINGS - Anca Petrisor, Marius Popescu, Mihaela Florescu
- REAL ROBOT REMOTE CONTROL VERSUS SIMULATIONS - Dorin Popescu, Dan Selisteanu
- PARACLINIC INVESTIGATION METHOD OF STATIC DEFORMATION HUMAN LEG - Ovidiu Spatari, Anton Policec
- FORCE PLATFORM FOR STATIC AND DYNAMIC HUMAN STUDY - Ovidiu Spatari, Anton Policec
- A CONTROLLER FOR A HANDICAPPED MEN VEHICLE SEAT WITH ERFLUID-BASED DAMPER - Viorel Stoian
- APPLIED MATHEMATICS FOR HEAT TRANSFER - Razvan Tudor Tanasie

SOFTWARE ENGINEERING:

- ABOUT THE WAY CAI CAN CHANGE A DIFFICULT TRAINING PROCESS INTO A PLEASANT AND USEFUL EXPERIMENT - Rodica Baciu, Dorin Sima
- GRAPHICAL MODELING OF RECURSION - Rodica Baciu, Dorin Sima
- BUSINSS PROCESS MODELLING USING ROLE ACTIVITY DIAGRAMS - Costin Badica, Amalia Badica
- INDICATORS FOR TEXT RELEVANCE USING TECHNIQUES FROM INFORMATION THEORY FIELD - Alina Bogan-Marta, Nicolae Robu
- ASPECTS OF AUTOMATIC SPEECH RECOGNITION BASED ON CONTEXT FREE GRAMMARS FOR NON-NATIVE SPEAKERS - Alina Bogan-Marta, Nicolae Robu
- NEAR-LOSSLESS LZW IMAGE COMPRESSION - Macarie Breazu, Antoniu Pitic, Daniel Volovici, Remus Brad
- XML, A SOLUTION FOR OPTIMISING DATA TRAFFIC IN N-TIER APPLICATIONS - Catalin Cerbulescu
- DYNAMIC SOFTWARE WATERMARKING BY ALTERING THE NUMERIC RESULTS OF THE PROGRAM - Claudiu Chiru
- STATIC SOFTWARE WATERMARKING - Claudiu Chiru
- DIGITAL IMAGE PROCESSING IN MEDICINE - Doru Cioata, Cristian Iacob, Mihaela Cioata
- A SIMPLE WAY TO CAPTURE NETWORK TRAFFIC: THE WINDOWS PACKET CAPTURE (WINPCAP) ARCHITECTURE - Mihai Dorobantu, Mihai L. Mocanu
- IDENTIFICATION IN A DISTRIBUTED DATABASE SYSTEM - Gabriel Dragomir
- IMPOSED CONDITIONS TO DATABASE SCHEMA IN DISTRIBUTED DATABASE DESIGN - Gabriel Dragomir
- IMAGE - SHAPE RECOGNITION - Eugen Ganea, Mihai L.Mocanu
- A COMPARATIVE STUDY OF DISTRIBUTED ALGORITHMS IN MINING ASSOCIATION RULES - Cornelia Gyorodi
- DATABASE SECURITY MECHANISM - Dorin Iordache
- DATABASE SECURITY POLICIES FOR INTERNET ARCHITECTURE - Dorin Iordache

- GEOMETRIC SHAPE RECOGNITION USING FUZZY AND NEURAL TECHNIQUES - Ioan Mihu, Arpad Gellert, Cosmin Suciu
- DESIGN AND EVALUATION OF A HIERARCHICAL ARCHITECTURE FOR HANDWRITTEN CHARACTER RECOGNITION - Ioan Mihu, Horia Caprita
- MMDB:NICE - MULTIMEDIA IMAGE DATABASE WITH IMAGE CONTENT SEARCHING - Muguras Mocofan
- DATA MODELS FOR VIRTUAL REALITY - Gabriel Muresan, Liana Stanescu, Dumitru Dan Burdescu
- INFORMATION ARCHITECTURE FOR STEEL - Madhurak Rajagopal, Gabriel Vladut
- ALGORITHM FOR OPTIMAL IMPLEMENTATION OF MULTIPLE-VALUED FUNCTIONS USING SWITCHES - Dorin Sima, Rodica Baciu
- SEARCHING THE WEB WITH HAND-HANDLED DEVICES - Dorin Sima, Rodica Baciu
- SINGLE AND MULTIPLE REGIONS QUERY WITH ABSOLUTE SPATIAL LOCALIZATION - Liana Stanescu, Dumitru Dan Burdescu, Gabriel Muresan

# CRYPTANALISE ASPECTS ON THE BLOCK CIPHERS OF RC5 AND RC6

Erica Mang, Ioan Mang, Constantin Popescu
University of Oradea, Romania
Department of Computers Science
3-5 Armatei Romane St., 3700 Oradea, Romania
E-mail: emang@uoradea.ro, imang@uoradea.ro, ppopescu@uoradea.ro

**Abstract.** In August 1999, Knudsen and Meier proposed an attack to the block cipher RC6 by using correlations derived from $x^2$ tests. In this paper, we improve the attack and apply this method to the block cipher RC5 and simplified variants of RC6, and show some experimental results. We show this approach distinguish the random permutation and RC5 with of up to 20 rounds by using chosen ciphertexts attack. We also show our approach for deriving the last round key of up to 17 rounds RC5 by using chosen plaintext attack. Moreover, we show full rounds RC5 with some weak key can be broken by using lesser complexity than that of the exhaustive search. Additionally, this method can be applicable to simplified variants of RC6, that is, RC6-INFR, RC6-NFR, RC6-I, we observe the attack to these block ciphers.

***Key words***: RC5, RC6, chosen ciphertexts attack, chosen plaintext attack, weak key

## 1. Introduction

RC5 is a block cipher designed by R. Rivest in 1994 (Rivest 1995). One of the reasons that many cryptographers were interested in cryptanalysis of RC5 comes from its simple structure.

Kaliski and Yin evaluated RC5 with respect to differential and linear crypt-analysis (Kaliski 1995). The paper shows that linear cryptanalysis is applicable for versions of RC5 with a small number of rounds. Moriai et al., found some weak key against linear attack (Rivest 1995). An improvement of Kaliski and Yin's attack by a factor of up to 512 was given by Knudsen and Meier (Knudsen 1996). Biryukov and Kushilevitz proposed drastic improvement of the previous results due to a novel practical differential approach (Biryukov 1998). Their attack requires $2^{44}$ chosen plaintexts which is smaller than complexity of exhaustive key search. In their approach, they study more complex differentials than in previous works, and defined a more general notation, so called “good pair," with respect to data dependent rotations. In their method, good pairs were searched by using Hamming weights of differences for each round, then the key of last round were derived. Their attacking algorithm, however, is rather complicated and it does not seem so easy to distinguish good pair and others correctly, because of influences of addition of key to the hamming weights of differentials.

In August 1999, Knudsen and Meier posted to the internet news an information of their new paper dealing with cryptanalysis of RC6 (Knudsen et al. 1999). In the paper, they used extremely different technique from the previous approach, that is, correlations obtained from $x^2$ test. In their approach, for fixing each of the least significant five bits in some words of plaintexts and investigate the statistics of the 10-bit integer obtained by concatenating each of the least significant five bits in some words of ciphertexts. To measure the effect of the distribution of the target bits, they forced the values of 10 bits by taking appropriate plaintexts and they computed the $x^2$-value of the 10 bit integers, then they compared to $x^2$-distribution with 1023 freedom, and distinguished RC6 from a random permutation. They estimated from systematic experimental results that version of RC6 whose round is reduced can be distinguished from a random permutation. Moreover, they constructed a key-recovery method for RC6 with up to 15 rounds which is faster than exhaustive key search.

In this paper, we improve the Knudsen and Meier's attacking algorithm obtained from $x^2$ tests, and apply this to the RC5 encryption algorithm. Then we show the experimental results of attacking the RC5 with reduced rounds. Our computatinal experiments show that RC5 with up to 20 half rounds can be distinguished from a random permutation by using $2^{54}$ chosen ciphertext. Moreover, we show that full round RC5 with a weak key which is available one in $2^{20}$ keys is distinguishable from random permutation with less than complexity of exhaustive key search.

Furthermore, we construct an algorithm for key recovery using the correlation and show the computational experiments. From our experiments, we conclude that the last round key of RC5 with up to 17 half rounds, or RC5 with up to full round with respect to a weak key can be recovered by using $2^{54}$ chosen plaintext attack with success probability 80%.

At last, we observe the strength of the simple variants of RC6 demonstrated in (Contini 1999), that is RC6-INFR, RC6-NFR and RC6-I, against our improved attacking algorithms. Then we show RC6-INFR, RC6-NFR with up to 19 rounds, and RC6- I with up to 15 rounds are breakable for our improved distinguishing algorithm. Moreover we show full round RC6-INFR, RC6-NFR with respect to a weak key existing in a ratio of one to $2^{45}$ are breakable by using our distinguishing attack.

## 2. Preliminary

In this section, we note some notations and definitions. At first, we recall the $x^2$ tests for distinguishing a random sequence taking from uniform distribution and non-random sequence (Contini 1999).

*Proposition 2.1.* Let A be a set $\{a_0,\ldots,a_{m-1}\}$. Let $X=X_0,\ldots,X_{n-1}$ be independent and identically distributed random variables taking from the set A uniformly. Let $N_{aj}(X)$ be the cardinality of variables in X which is equal to $a_j$.

Table 1. The chi-square distributions with and 1023 degrees of freedom

| Level | 0.5 | 0.90 | 0.95 | 0.99 | 0.999 |
|---|---|---|---|---|---|
| $X^2$ | 30.33 | 41.42 | 44.99 | 52.19 | 61.09 |

$X^2$ distribution of 31 degrees of freedom

| Level | 0.5 | 0.90 | 0.95 | 0.99 | 0.999 |
|---|---|---|---|---|---|
| $X^2$ | 1022.0 | 1080.94 | 1098.92 | 1130.89 | 1168.85 |

$X^2$ distribution of 1023 degrees of freedom

The $X^2$ statistic $X^2(X)$ of X is defined by

$$X^2(X)=\sum_{i=0}^{m-1}\left(N_{ai}(X)-\frac{n}{m}\right)^2$$

Then, the distributions of $X^2(X)$ can be approximated to the chi-square distribution with m-1 degrees of freedom for large n.

Table 1 shows the chi-square distributions with 31 degrees and 1023 degrees of freedom, which we will use in the following sections.

For example, level=0:999 and _2 = 61.09 in Table 1 means that $X^2$ values of 99.9% of random sequences with n elements taking from the set of 32 elements uniformly will not exceed 61.09 for large *n*. We comment that, for $X^2$ tests, n should be large enough such that each expected value of $N_{ai}$ (X) (that is, *n/m*) is larger than 4 or 5, in practical.

ls5(A): least significant 5 bits of a 32 a bits word A
(A, B): plaintext of RC5 (32 bits * 2)
(A', B'): ciphertext of RC5 (32 bits * 2)
$(A_i, B_i)$: output of $i^{th}$ half round, especially,
$(A_0, B_0) = (A, B)$ and $(A_r, B_r) = (A, B)$
$x_i$: amounts of data dependent rotation in the i-th half round, that is $ls5(A_i)$
$y_i$: $x_{r-i+1}$

## 3. $X^2$ Tests of RC5

In this section, we explain the $X^2$ tests for plaintexts and ciphertexts of RC5. The notations are followed from the previous section. We examine 4 different types of $X^2$ tests. For each test, we observe the $X^2$ statistics of 5 bit in the plaintexts or ciphertexts.

*Test1:* Fix least significant 5 bits of plaintext A to 0, and compute $X^2$ of least significant 5 bits of ciphertext A'.

*Test2:* Fix least significant 5 bits of plaintext A and B to 0 and compute $X^2$ of least significant 5 bits of ciphertext A'.

*Test3:* Fix least significant 5 bits of ciphertext B' to 0, and compute $X^2$ of least significant 5 bits of plaintext B.

*Test4:* Fix least significant 5 bits of ciphertext A' and B' to 0 and compute $X^2$ of least significant 5 bits of plaintext B.

If RC5 was ideal random permutation, the distribution of the $X^2$ value is similar to the $X^2$ distribution of $31=2^5-1$ degrees of freedom. So, we set up the threshold by 45 in order to distinguish from a random permutation. The sequence whose $X^2$ value extends more than 45 can be distinguished from a random permutation in a probability of 95 %. (Table 1).

Table 2 shows the results of $X^2$ tests. Each entry of $X^2$ value is an average of 100 $X^2$ values of different 100 keys.

The numbers denoted by bold character are the $X^2$ values at the first coming over 45. These experiments show that each additional two half rounds require about $2^6$ times as many texts to get about the same $X^2$ value. The results of the Test 1 and Test 3 show that the each number of required data is almost same. On the other hand, each the number of required elements in Test 2 is $2^3$ times as many as corresponding one of Test 4, because of the influences of the initial key S[1]. It means that if the value of data dependent rotation at the first round is fixed 0, the $X^2$ value of the target bits in the output of last round becomes much larger.

## 4. Distinguishing Algorithm and Weak Key

By the examination described in the previous section, we conclude that the better way in order to distinguish the RC5 encryption and a random permutation in the four conditions described in Test1 to Test4, is the condition in Test4. We consider a following algorithm. It is one of the chosen ciphertext attacks.

*Algorithm 4.1. (Distinguishing attack)*

Input: RC5 algorithm permutation, n: a number;
Output: answer that Input is RC5or not ;

```
for i  from 1 to n
    Let A',B' be a random number such that
      ls5(A') =  ls5(B') = 0;
     (A, B)  = decrypted message of (A', B');
         count up the counter map[ls5(B)];
calculate X^2 of the map;
if x^2≥45
   then return the answer "Input is RC5";
else return the answer "Input is a random
   permutation";
```

Table 2. Evaluations of the $X^2$ tests (Test1,...,Test4, average of 100 keys)

Test 1(fix ls5(A) = 0)

| | | | | | | |
|---|---|---|---|---|---|---|
| 4 half rounds | | | | | | |
| #data | $2^{10}$ | $2^{11}$ | $2^{12}$ | $2^{13}$ | $2^{14}$ | $2^{15}$ |
| $X^2$ | 30 | 33 | 37 | 41 | **47** | 66 |
| 6 half rounds | | | | | | |
| #data | $2^{16}$ | $2^{17}$ | $2^{18}$ | $2^{19}$ | $2^{20}$ | $2^{21}$ |
| $X^2$ | 30 | 31 | 34 | 41 | **52** | 70 |
| 8 half rounds | | | | | | |
| #data | $2^{22}$ | $2^{23}$ | $2^{24}$ | $2^{25}$ | $2^{26}$ | $2^{27}$ |
| $X^2$ | 29 | 31 | 31 | 34 | **46** | 63 |
| 10 half rounds | | | | | | |
| #data | $2^{28}$ | $2^{29}$ | $2^{30}$ | $2^{31}$ | $2^{32}$ | $2^{33}$ |
| $X^2$ | 31 | 31 | 32 | 35 | **51** | 72 |

Test 2 (fix ls5(A) = ls5(B) = 0)

| | | | | | | |
|---|---|---|---|---|---|---|
| 4 half rounds | | | | | | |
| #data | $2^{6}$ | $2^{7}$ | $2^{8}$ | $2^{9}$ | $2^{10}$ | $2^{11}$ |
| $X^2$ | 31 | 31 | 34 | 40 | **57** | 82 |
| 6 half rounds | | | | | | |
| #data | $2^{12}$ | $2^{13}$ | $2^{14}$ | $2^{15}$ | $2^{16}$ | $2^{17}$ |
| $X^2$ | 29 | 32 | 35 | 40 | **47** | 61 |
| 8 half rounds | | | | | | |
| #data | $2^{18}$ | $2^{19}$ | $2^{20}$ | $2^{21}$ | $2^{22}$ | $2^{23}$ |
| $X^2$ | 32 | 32 | 36 | 42 | **55** | 81 |
| 10half rounds | | | | | | |
| #data | $2^{24}$ | $2^{25}$ | $2^{26}$ | $2^{27}$ | $2^{28}$ | $2^{29}$ |
| $X^2$ | 32 | 33 | 36 | 42 | **55** | 81 |

Test 3 (fix ls5 (A') = 0)

| | | | | | | |
|---|---|---|---|---|---|---|
| 4 half rounds | | | | | | |
| #data | $2^{10}$ | $2^{11}$ | $2^{12}$ | $2^{13}$ | $2^{14}$ | $2^{15}$ |
| $X^2$ | 31 | 32 | 34 | 38 | **47** | 59 |
| 6 half rounds | | | | | | |
| #data | $2^{16}$ | $2^{17}$ | $2^{18}$ | $2^{19}$ | $2^{20}$ | $2^{21}$ |
| $X^2$ | 30 | 33 | 35 | 40 | **49** | 66 |
| 8 half  rounds | | | | | | |
| #data | $2^{22}$ | $2^{23}$ | $2^{24}$ | $2^{25}$ | $2^{26}$ | $2^{27}$ |
| $X^2$ | 29 | 31 | 31 | 34 | **46** | 63 |
| 10 half rounds | | | | | | |
| #data | $2^{28}$ | $2^{29}$ | $2^{30}$ | $2^{31}$ | $2^{32}$ | $2^{33}$ |
| $X^2$ | 30 | 31 | 33 | 35 | **50** | 69 |

Test 4 (fix ls (A') = ls5(B') = 0)

| | | | | | | |
|---|---|---|---|---|---|---|
| 4 half rounds | | | | | | |
| #data | $2^{3}$ | $2^{4}$ | $2^{5}$ | $2^{6}$ | $2^{7}$ | $2^{8}$ |
| $X^2$ | 12 | 11 | 39 | 48 | **62** | 94 |
| 6 half rounds | | | | | | |
| #data | $2^{9}$ | $2^{10}$ | $2^{11}$ | $2^{12}$ | $2^{13}$ | $2^{14}$ |
| $X^2$ | 32 | 34 | 36 | 39 | **47** | 60 |
| 8 half rounds | | | | | | |
| #data | $2^{15}$ | $2^{16}$ | $2^{17}$ | $2^{18}$ | $2^{19}$ | $2^{20}$ |
| $X^2$ | 32 | 34 | 38 | 44 | **65** | 101 |
| 10 half rounds | | | | | | |
| #data | $2^{21}$ | $2^{22}$ | $2^{23}$ | $2^{24}$ | $2^{25}$ | $2^{26}$ |
| $X^2$ | 32 | 34 | 35 | 42 | **56** | 85 |

In order to estimate the complexity of Algorithm 4.1, we compute the number of required elements that the $X^2$ value exceeds the 45 more precisely, for each rounds of RC5. Table 3 shows the results. From Table 3, we calculate the relation between the number of required elements and the number of rounds by using the method of least squares;

$$\log_2(\#data) = \alpha + \beta r + \varepsilon,$$

where $r$ is a number of half rounds and $\varepsilon$ is a bias. Then we have $\alpha$=-5.33, $\beta$=2.97, $\varepsilon$=0.17. This means that each additional one half rounds, Algorithm 4.1 requires almost $2^3$ times as many texts to get about the same $X^2$ value on average.

Table 4 shows that the estimated number of required texts for Algorithm 4.1. In Algorithm 4.1, since the 10 bits in cipher text bits are fixed zero, the total amounts of admissible texts is $2^{54}$. From Table 4, (by omitting the small bias) our distinguish attack can be applicable reduced RC5 with up to 20 half rounds.

Now, we consider the weak key. From the assumption of Algorithm 4.1, amount of a data dependent rotation in the last round is fixed 0. Moreover if the condition $ls5(S[r+1])=0$ holds, the amount of rotations of last two rounds are 0. In this case, the last round does not influence the $X^2$ value, that is the security level is equal to that of r-1 rounds RC5. This case happen every one in $2^5$ keys. In the same way, if the condition

$$ls5(S[r+1]) = \ldots = ls5(S[r-t+2]) = 0$$

holds, the security level against Algorithm 4.1 is as same as r - t rounds RC5. There is one weak key in $2^{5t}$.

Since, it is easy to check whether the key is a weak key or not, we can find the following weak key.

$key_0$ = $\{5b,2d,16,0b,7a,3d,9e,cf,7e,3f,9f,cf,af,d7,eb,75\}_{16}$

In this key, we can check:

$$ls5(S[19])=\ldots= ls5(S[25])=0.$$

Therefore the 24 half round RC5 encryption with *key*0 has the same security as 17=24-7 half rounds RC5. From Table 4, this RC5 encryption algorithm is distinguished from random permutation in $2^{45.16}$ numbers of data.

Table 3. Precisely examination of $x^2$ and number of data in Test 4

| # half rounds | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|
| # data (log 2) | 12.32 | 15.71 | 18.58 | 21.31 | 24.09 | 27.81 | 30.17 |
| $X^2$ | 45 | 46 | 46 | 45 | 45 | 46 | 45 |

Table 4. Estimation of the number of required text for distinguishing attack

| #half rounds | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| #data (log2) | 36.25 | 36.25 | 39.22 | 42.19 | 45.16 | 51.1 | 51.1 | **54.07** | 57.04 | 60.01 | 62.98 | 65.95 |
| 1 in $2^5$ keys | 30.31 | 33.28 | 36.25 | 39.22 | 42.19 | 45.16 | 48.13 | 51.1 | **54.07** | 57.04 | 60.01 | 62.98 |
| 1 in $2^{10}$ keys | 27.34 | 30.31 | 33.28 | 36.25 | 39.22 | 42.19 | 45.16 | 48.13 | 51.1 | **54.07** | 57.04 | 60.01 |
| 1 in $2^{15}$ keys | 24.37 | 27.34 | 30.31 | 33.28 | 36.25 | 39.22 | 42.19 | 45.16 | 48.13 | 51.1 | **54.07** | 57.04 |
| 1 in $2^{20}$ keys | 21.4 | 24.37 | 27.34 | 30.31 | 33.28 | 36.25 | 39.22 | 42.19 | 45.16 | 48.13 | 51.1 | **54.07** |
| 1 in $2^{25}$ keys | 18.43 | 21.4 | 24.37 | 27.34 | 30.31 | 33.28 | 36.25 | 39.22 | 42.19 | 45.16 | 48.13 | 51.1 |
| 1 in $2^{30}$ keys | 15.46 | 18.43 | 21.4 | 24.37 | 27.34 | 30.31 | 33.28 | 36.25 | 39.22 | 42.19 | 45.16 | 48.13 |
| 1 in $2^{35}$ keys | 12.49 | 15.46 | 18.43 | 21.4 | 24.37 | 27.34 | 30.31 | 33.28 | 36.25 | 39.22 | 42.19 | 45.16 |
| 1 in $2^{40}$ keys | 9.52 | 12.49 | 15.46 | 18.43 | 21.4 | 24.37 | 27.34 | 30.31 | 33.28 | 36.25 | 39.22 | 42.19 |

## 5. Key Recovery Algorithm

In this section, we propose a key recovery algorithm by using the $X^2$ statistics of RC5 with *r* half rounds.

### *5.1. Knudsen, Meier's Approach*

Knudsen proposed an algorithm for key recover of the extended key of the first round of RC6 by using $X^2$ statistics. His approach uses the property that the 0 amounts of the first rounds data dependent rotation growths the $X^2$ value. First of all, we try to modify this approach to a key recovery of RC5.

*Algorithm 5.1. (Knudsen,Meier-modified)*

Input: RC5 encryption algorithm of unknown secret key

Output: candidate of ls5(S[1])
for each plaintext (A, B),where ls5b(A)=0
  compute ciphertext $(A', B')$;
    $s_0 = 32 - ls5(B') \bmod 32$;
    $y_1 = ls5(A')$;
    count up the memory map $[s_0][y_1]$;
for each $s_0$
    $X^2[s_0] = X^2$ of map $[s_0]$;
return s such that $X^2[s] = \max\{X^2[s_0] | s_0 = 0,\ldots,31\}$;

In order to obtain the high success rate of the above key recovery algorithm, the average of $X^2$ is far smaller than the amount of $X^2$ in the case of zero rotation.

Table 5 shows the experiment of $X^2$ value of each rotation nearly equal to 0. Though the amount of $X^2$ at the 0 rotation always highest, $X^2$ values near of 0 still large, so the average of $X^2$ is not small. By this reason, we cannot obtain high success rate of this algorithm.

In fact, from the experimental results of the algorithm, we have only 20-30% of success probability.

Table 5. Data dependent rotation of 1st round and $X^2$ values 6 half round of RC5 (average of 500 tests)

| date | 26 | 27 | 28 | 29 | 30 | 31 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $2^{12}$ | 31 | 31 | 32 | 34 | 36 | 38 | 43 | 40 | 35 | 33 | 31 | 31 | 31 |
| $2^{13}$ | 31 | 32 | 33 | 39 | 41 | 45 | 55 | 49 | 39 | 38 | 33 | 31 | 31 |
| $2^{14}$ | 32 | 33 | 37 | 47 | 51 | 61 | 79 | 69 | 48 | 46 | 35 | 33 | 32 |
| $2^{15}$ | 34 | 35 | 44 | 62 | 73 | 91 | 127 | 106 | 67 | 61 | 40 | 35 | 35 |

### *5.2. Recovering the Least Significant 5 Bits of the Last Round Key*

In this section, we show an algorithm for recovering the least significant 5 bits of the last round key $S[r+1]$ by using chosen plaintext attack.

Suppose the least significant 5 bits of each words of plaintexts is fixed 0. (Namely ($ls5(A)=ls5(B)=0$).) In this section, we only use the ciphertexts (A', B') corresponding to the plaintext (A,B) which satisfy the condition $ls5(A')=0$. (In the next section, we also use the texts such that $ls5(A')\neq 0$ for constructing the whole procedure recovering the last round 32 bits key). We note that the amount of last round data dependent rotation $y_1$ is always 0. Then, we have:

$$y_2 = ls5(B') - ls5(S[r+1]) \bmod 32.$$

Therefore, $ls5(A_{r-2} = ((A' - S[r]) \lll y_2) \bmod 32$. Since $S[r]$ is fixed value, the $X^2$ values of $((A' - S[r]) \lll y_2) \bmod 32$ and $(A' \lll y_2) \bmod 32$ are almost same. In general, the $X^2$ statistics of $ls5(A_{r-2})$ is much larger than $X^2$ statistics of $ls5(A_r)$. Now, we consider the $X^2$ value of $ls5(A_{r-2})$. We mention that, since we suppose that $ls5(A')=0$, when $y_2$ satisfies $y_2 \leq 4$ or $28 \leq y_2$, some of bits in the $ls5(A_{r-2})$ are fixed. Therefore, it is meaningless for compute the $X^2$ value of $ls5(A_{r-2})$ except for the case of $5 \leq y_2 \leq 27$. The algorithm is described in Algorithm 5.2. The memory requirement of this procedure is $2^{15}$ words (at most 128 Kbyte), and the dominant step of computational complexity is the encryption stage.

*Algorithm 5.2. (Shimoyama, Takeuchi, Hayakawa (1))*

```
Input: RC5 encryption algorithm of
        unknown key;
Output: candidates ls5 (S[r + 1]);
for each plaintext (A,B), where ls5b(A)=ls5b(B) = 0
      compute ciphertext (A′, B′);
      if ls5(A′) = 0
           for each candidates s0∈{0,…,31}
           of ls5(S[r + 1])
                y2 = ls5(B′) – s0 mod 32;
                 if y2 ≥ 5 and y2 ≤ 27;
                  z2 = ls5(A′ >>> y2);
                  count up the memory map[so][y2][z2];
for each s0, y2
       χ2 [s0][y2] = χ2 of map[s0][y2];
for each s0
      ave[s0] = average of χ2 [s0][y2];
return s such that ave[s]=max{ ave [s0]|so=0,…,31};
```

Occasionally, there is a case that the each counter satisfied the condition

$$map[s_0][y_2] = \ldots = map[s_0][y_2][31] = 0$$

for some $s_0$, $y_2$. In this case, the correct key is $(y_2+s_0)$ mod 32 in high probability. So return $y_2+s_0$ mod 32. By using this criterion, we can easily obtain the solution, in this special case.

For 6 rounds, we have success probability more than 50% by using $2^{18}$ data, and 70% by using $2^{20}$. Moreover, the probability that the bias is at most ± 1, is more than 80% with $2^{20}$ data, and 90% with $2^{21}$ data. In 8 rounds, for each success probability, the corresponding number of plaintexts is increased by a constant factor of about $2^6$.

### *5.3. Recovery of the Last Round Key*

In this section, we construct an algorithm for recovering the all bits of last round key. Suppose $ls5(A')=i$. Then the amount of last round data dependent rotation $y_1$ is equal to $i$, so $y_2=((B'-S[r+1])\gg i)\oplus i$ mod32. Let $s_i=(S[r+1])\gg i)$ mod 32. Since that the difference of $y_i$ and $((B'-(s_i\ll i))\gg i)\oplus i$ mod 32 is at most ±, we use $((B'-(s_i\ll i))\gg i)\oplus i$ mod32 instead of $y_i$. The algorithm, described below, is constructed by the same way described in the previous section.

*Algorithm 5.3. (Shimoyama, Takeuchi, Hayakawa (2))*

```
Input: RC5 encryption algorithm of
        unknown secret key;
Output :candidates S[r+1];
for each plaintext (A′,B′), where sl5b(A) = ls5b(B) = 0
          compute ciphertext (A′,B′);
         y1 = ls5(A′);
            for each candidates sy1∈{0,…,31}
                           of ls5(S[r+1]>>>y1 )
               y2= ls5((B′-(sy1<<<y1)) mod32;
               if y2 ≥ 5 and y2 ≤ 27;
                      z2 = ls5(A′ >>> y2);
                      count up the memory
map[y1][sy1]][y2][z2];
    for each y1, sy1, y2
          χ2[y1][sy1][y2]= χ2 of map[y1][sy1][y2];
    for each y1, sy1
           ave[y1][sy1]= average of χ2[y1][sy1][y2];
     for each y1
          key[y1]=s0 such that
ave[s0]=max{ave[i]|i=0,…,31};
concatenate key[y1] and derive 32 bit key S;
       return S;
```

We comment that for concatenate the 32 candidates of 5bits to 32 bit integer, we can use any error correcting algorithm, by using the property that each 5 bits solution is different from the correct value at most ±1 in high probability.

At the end of this section, we discuss the weak key. The key recovering algorithm described in this section, we suppose the least significant 5 bits of each words of plaintexts are fixed zero. From the same reason of the existence of weak keys against distinguishing attack, if the condition $ls5(S[0])=\ldots=ls5(S[t])=0$ holds, the security of the $r$ rounds RC5 encryption using this key is as same as the security level of $r$-$t$+1 half round RC5. For example, in the case that the key satisfy

$$ls5(S[0])=\ldots=ls5(S[8])=0,$$

24 round RC5 with this key has the same security of 17 half rounds. This key can be found every one in $2^{45}$ keys.

## 6. Application to the Simplified Variants of RC6

Contini presented the some simplified variants of RC6, that is RC6-I, RC6-NFR, RC6-INFR, and the cryptanalysis to these families. Knudsen proposed the attacking method to RC6 in (Knudsen et al. 1999).

In this section, we consider the security against the attack using $X^2$ statistics for the simplified variants RC6-I, RC6-NFR, RC6-INFR. Each variant has reduced round function $F$ compared with RC6 (Table 6). Every one of simplified variants is not one of the real world block cipher, but prototype block cipher for comparing the security with that of RC6, however, we think that cryptanalysis of these variants may be meaningful.

We mention that the least significant 5 bits of the output of the round function of 3 variants are obtain from only 5 input bits. Therefore, we can apply the Algorithm 5.2 to each variant with a little modification. The remaining problem is a relation of $X^2$ value and number of rounds.

Let observe the following two tests.

*Test1:* Fix least significant 5 bits of plaintext A and C to 0, and compute $X^2$ of least significant 5 bits of ciphertext A and C.

*Test2:* Fix least significant 5 bits of plaintext A, B, C and D to 0, and compute $X^2$ of least significant 5 bits of ciphertext A and C.

Table 6. Round function F of variants of RC6

| | | RC6-INFR | RC6-1 | RC6-NFR | RC6 |
|---|---|---|---|---|---|
| $F(x)=$ | | $x$ | $x<<<5$ | $x \times (2x+1)$ | $(x \times (2_x+1))<<<5$ |

Table 7. $X^2$ tests to the RC6 variants

Tests 1 : (fix lsb(A), lsb(C))

| #rounds | INFR | NFR | I | RC6 |
|---|---|---|---|---|
| 2 | $2^{14}$(1159) | $2^{13}$(1122) | $2^{13}$(1107) | $2^{14}$(1178) |
| 4 | $2^{25}$(1152) | $2^{26}$(1126) | $2^{29}$(1171) | $2^{30}$(1156) |

Test 2 : (fix lsb(A), lsb(B), lsb(C), lsb(D))

| #rounds | INFR | NFR | I | RC6 |
|---|---|---|---|---|
| 2 | $2^{7}$ (1193) | $2^{7}$(1122) | $2^{13}$(1100) | $2^{13}$(1100) |
| 4 | $2^{16}$(1109) | $2^{17}$(1102) | $2^{22}$(1141) | $2^{29}$(1171) |
| 6 | $2^{28}$(1164) | $2^{30}$(1141) | | |

In these tests, we set up the threshold by 1099. The sequence whose $X^2$ value extends more than 1099 can be distinguished from a random permutation in probability 95 %. (Table 1) Table 7 shows the results of the first number of $X^2$ coming up with 1099, and corresponding the number of data. (They are averages of 50 times computer experiments.)

In the roughly consideration, from Table 7, we estimate that each additional 2 rounds require $2^{12}$, $2^{13}$ and $2^{16}$ times as many number of texts to obtain the same $X^2$ value for the variants RC6-INFR, RC6-NFR and RC6-I, respectively against the Test 1. For the results of Test 2, the condition in the Test 2 makes decreasing the initial values of the number of required data about $2^9$, $2^9$, $2^7$ times of those conditions in Test 1, for RC6-INFR, RC6-NFR and RC6-I. By using either the assumption used in Test 1, Test 2, it is estimated that we can cryptanalysis up to 19 rounds of RC6-INFR, RC6-NFR, and up to 15 rounds of RC6-I. Moreover, in assumption of Test 2, there is a weak key as the same reason of the case in RC5. For example, a key satisfied the following condition has the same security level as 20-*i* round,

$$ls5(S[0]) = \ldots = ls5(S[2i+1]) = 0.$$

Especially, in the case that

$$ls5(S[0])=\ldots= ls5(S[3])=0,$$

20 round RC6-INFR, RC6-NFR can be distinguished from the random permutation by using lesser complexity compared with exhaustive search.

**7. Conclusion**

In this paper, we improved the Knudsen and Meier's attacking algorithm obtained from $X^2$ tests, and applied this to the RC5 encryption algorithm. Then we showed the experimental results of attacking the RC5 with reduced rounds. Our computational experiments showed that RC5 with up to 20 half rounds can be distinguished from a random permutation by using $2^{54}$ chosen ciphertext. Moreover, we showed that full round RC5 with a weak key which is available one in $2^{20}$ keys is distinguishable from random permutation with less than complexity of exhaustive key search. Furthermore, we constructed an algorithm for key recovery using the correlation and showed the computational experiments. From our experiments, we concluded that the last round key of RC5 with up to 17 half rounds, or RC5 with up to full round with respect to a weak key can be recovered by using $2^{54}$ chosen plaintext attack with success probability 80%.

At last, we observed the strength of the simple variants of RC6 demonstrated (Contini 1999), that is RC6-INFR, RC6-NFR and RC6-I, against our improved attacking algorithms. Then we showed RC6-INFR, RC6-NFR with up to 19 rounds, and RC6-I with up to 15 rounds are breakable for our improved distinguishing algorithm. Moreover we showed full round RC6-INFR, RC6-NFR with respect to a weak key existing in a ratio of one to $2^{45}$ are breakable by using our distinguishing attack. We remark that further improvement of this attack will be considered. It may be also interesting that the similar attacks can be applicable or not to another type of block cipher, for example MARS. Furthermore, it still remain some important problem of how to protect or design block ciphers to be secure, especially to have provable security, against the attacks by using $X^2$ statistics, but these are future works.

**References**


A. Biryukov, E. Kushilevitz*: Improved Cryptanalysis of RC5*, Advances in Cryptology – Eurocrypto'98, Lecture Notes in Computer Science 1403, pp. 85-99, Springer Verlag, 1998.

S. Contini, R.L. Rivest, M.J.B. Robshaw and Y.L. Yin: *Improved Analysis of Some Simplified Variants of RC6,* Fast Software Encryption, Lecture Notes in Computer Science, 1636 pp.1-16,Springer Verlag, 1999.

B. Kaliski, Y. Yin: *On Differential and Linear Cryptanalysis of the RC5 Encryption Algorithm***,** CRYPTO'95, Lecture Notes in Computer Science 963, pp. 171-184, Springer-Verlag, 1995.

L. Knudsen, W. Meier, *Improved Differential Attacks on RC5***,** Crypto'96, Lecture Notes in Computer Science 1109, pp. 216-228, Springer-Verlag, 1996.

L. Knudsen, W. Meier, *Correlations in RC6***,** 1999. http://www.ii.uib.no/~larsr/papers/rc6.ps

R. Rivest, *"The RC5 Encryption Algolithm*", Fast Software Encryption, Lecture Notes in Computer Science 1008, pp. 86-96, Springer-Verlag, 1995.