Lecture Notes in Computer Science 1636

Lars Knudsen (Ed.)

Fast Software Encryption

6th International Workshop, FSE'99
Rome, Italy, March 1999
Proceedings

Springer

Lars Knudsen (Ed.)

Fast Software Encryption

6th International Workshop, FSE'99
Rome, Italy, March 24-26, 1999
Proceedings

Springer

Series Editors

Gerhard Goos, Karlsruhe University, Germany
Juris Hartmanis, Cornell University, NY, USA
Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editor

Lars Knudsen
University of Bergen, Department of Informatics
N-5020 Bergen, Norway
E-mail: lars.knudsen@ii.uib.no

Cataloging-in-Publication data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Fast software encryption : 6th international workshop ; proceedings / FSE '99, Rome, Italy, March 24 - 26, 1999. Lars Knudsen (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Hong Kong ; London ; Milan ; Paris ; Singapore ; Tokyo : Springer, 1999
(Lecture notes in computer science ; Vol. 1636)
ISBN 3-540-66226-X

CR Subject Classification (1998): E.3, F.2.1, E.4, G.4

ISSN 0302-9743
ISBN 3-540-66226-X Springer-Verlag Berlin Heidelberg New York

Typesetting: Camera-ready by author
SPIN: 10703422 06/3142 – 5 4 3 2 1 0 Printed on acid-free paper

Lecture Notes in Computer Science 1636

Edited by G. Goos, J. Hartmanis and J. van Leeuwen

Springer
Berlin
Heidelberg
New York
Barcelona
Hong Kong
London
Milan
Paris
Singapore
Tokyo

Lecture Notes in Computer Science

For information about Vols. 1–1548
please contact your bookseller or Springer-Verlag

Vol. 1549: M. Pettersson, Compiling Natural Semantics. XVII, 240 pages. 1999.

Vol. 1550: B. Christianson, B. Crispo, W.S. Harbison, M. Roe (Eds.), Security Protocols. Proceedings, 1998. VIII, 241 pages. 1999.

Vol. 1551: G. Gupta (Ed.), Practical Aspects of Declarative Languages. Proceedings, 1999. VIII, 367 pgages. 1999.

Vol. 1552: Y. Kambayashi, D.L. Lee, E.-P. Lim, M.K. Mohania, Y. Masunaga (Eds.), Advances in Database Technologies. Proceedings, 1998. XIX, 592 pages. 1999.

Vol. 1553: S.F. Andler, J. Hansson (Eds.), Active, Real-Time, and Temporal Database Systems. Proceedings, 1997. VIII, 245 pages. 1998.

Vol. 1554: S. Nishio, F. Kishino (Eds.), Advanced Multimedia Content Processing. Proceedings, 1998. XIV, 454 pages. 1999.

Vol. 1555: J.P. Müller, M.P. Singh, A.S. Rao (Eds.), Intelligent Agents V. Proceedings, 1998. XXIV, 455 pages. 1999. (Subseries LNAI).

Vol. 1556: S. Tavares, H. Meijer (Eds.), Selected Areas in Cryptography. Proceedings, 1998. IX, 377 pages. 1999.

Vol. 1557: P. Zinterhof, M. Vajteršic, A. Uhl (Eds.), Parallel Computation. Proceedings, 1999. XV, 604 pages. 1999.

Vol. 1558: H. J.v.d. Herik, H. Iida (Eds.), Computers and Games. Proceedings, 1998. XVIII, 337 pages. 1999.

Vol. 1559: P. Flener (Ed.), Logic-Based Program Synthesis and Transformation. Proceedings, 1998. X, 331 pages. 1999.

Vol. 1560: K. Imai, Y. Zheng (Eds.), Public Key Cryptography. Proceedings, 1999. IX, 327 pages. 1999.

Vol. 1561: I. Damgård (Ed.), Lectures on Data Security.VII, 250 pages. 1999.

Vol. 1562: C.L. Nehaniv (Ed.), Computation for Metaphors, Analogy, and Agents. X, 389 pages. 1999. (Subseries LNAI).

Vol. 1563: Ch. Meinel, S. Tison (Eds.), STACS 99. Proceedings, 1999. XIV, 582 pages. 1999.

Vol. 1565: P. P. Chen, J. Akoka, H. Kangassalo, B. Thalheim (Eds.), Conceptual Modeling. XXIV, 303 pages. 1999.

Vol. 1567: P. Antsaklis, W. Kohn, M. Lemmon, A. Nerode, S. Sastry (Eds.), Hybrid Systems V. X, 445 pages. 1999.

Vol. 1568: G. Bertrand, M. Couprie, L. Perroton (Eds.), Discrete Geometry for Computer Imagery. Proceedings, 1999. XI, 459 pages. 1999.

Vol. 1569: F.W. Vaandrager, J.H. van Schuppen (Eds.), Hybrid Systems: Computation and Control. Proceedings, 1999. X, 271 pages. 1999.

Vol. 1570: F. Puppe (Ed.), XPS-99: Knowledge-Based Systems. VIII, 227 pages. 1999. (Subseries LNAI).

Vol. 1571: P. Noriega, C. Sierra (Eds.), Agent Mediated Electronic Commerce. Proceedings, 1998. IX, 207 pages. 1999. (Subseries LNAI).

Vol. 1573: J.M.L.M. Palma, J. Dongarra, V. Hernández (Eds.), Vector and Parallel Processing - VECPAR'98. Proceedings, 1998. XVI, 706 pages. 1999.

Vol. 1572: P. Fischer, H.U. Simon (Eds.), Computational Learning Theory. Proceedings, 1999. X, 301 pages. 1999. (Subseries LNAI).

Vol. 1574: N. Zhong, L. Zhou (Eds.), Methodologies for Knowledge Discovery and Data Mining. Proceedings, 1999. XV, 533 pages. 1999. (Subseries LNAI).

Vol. 1575: S. Jähnichen (Ed.), Compiler Construction. Proceedings, 1999. X, 301 pages. 1999.

Vol. 1576: S.D. Swierstra (Ed.), Programming Languages and Systems. Proceedings, 1999. X, 307 pages. 1999.

Vol. 1577: J.-P. Finance (Ed.), Fundamental Approaches to Software Engineering. Proceedings, 1999. X, 245 pages. 1999.

Vol. 1578: W. Thomas (Ed.), Foundations of Software Science and Computation Structures. Proceedings, 1999. X, 323 pages. 1999.

Vol. 1579: W.R. Cleaveland (Ed.), Tools and Algorithms for the Construction and Analysis of Systems. Proceedings, 1999. XI, 445 pages. 1999.

Vol. 1580: A. Včkovski, K.E. Brassel, H.-J. Schek (Eds.), Interoperating Geographic Information Systems. Proceedings, 1999. XI, 329 pages. 1999.

Vol. 1581: J.-Y. Girard (Ed.), Typed Lambda Calculi and Applications. Proceedings, 1999. VIII, 397 pages. 1999.

Vol. 1582: A. Lecomte, F. Lamarche, G. Perrier (Eds.), Logical Aspects of Computational Linguistics. Proceedings, 1997. XI, 251 pages. 1999. (Subseries LNAI).

Vol. 1583: D. Scharstein, View Synthesis Using Stereo Vision. XV, 163 pages. 1999.

Vol. 1584: G. Gottlob, E. Grandjean, K. Seyr (Eds.), Computer Science Logic. Proceedings, 1998. X, 431 pages. 1999.

Vol. 1585: B. McKay, X. Yao, C.S. Newton, J.-H. Kim, T. Furuhashi (Eds.), Simulated Evolution and Learning. Proceedings, 1998. XIII, 472 pages. 1999. (Subseries LNAI).

Vol. 1586: J. Rolim et al. (Eds.), Parallel and Distributed Processing. Proceedings, 1999. XVII, 1443 pages. 1999.

Vol. 1587: J. Pieprzyk, R. Safavi-Naini, J. Seberry (Eds.), Information Security and Privacy. Proceedings, 1999. XI, 327 pages. 1999.

Vol. 1590: P. Atzeni, A. Mendelzon, G. Mecca (Eds.), The World Wide Web and Databases. Proceedings, 1998. VIII, 213 pages. 1999.

Vol. 1592: J. Stern (Ed.), Advances in Cryptology – EUROCRYPT '99. Proceedings, 1999. XII, 475 pages. 1999.

Vol. 1593: P. Sloot, M. Bubak, A. Hoekstra, B. Hertzberger (Eds.), High-Performance Computing and Networking. Proceedings, 1999. XXIII, 1318 pages. 1999.

Vol. 1594: P. Ciancarini, A.L. Wolf (Eds.), Coordination Languages and Models. Proceedings, 1999. IX, 420 pages. 1999.

Vol. 1595: K. Hammond, T. Davie, C. Clack (Eds.), Implementation of Functional Languages. Proceedings, 1998. X, 247 pages. 1999.

Vol. 1596: R. Poli, H.-M. Voigt, S. Cagnoni, D. Corne, G.D. Smith, T.C. Fogarty (Eds.), Evolutionary Image Analysis, Signal Processing and Telecommunications. Proceedings, 1999. X, 225 pages. 1999.

Vol. 1597: H. Zuidweg, M. Campolargo, J. Delgado, A. Mullery (Eds.), Intelligence in Services and Networks. Proceedings, 1999. XII, 552 pages. 1999.

Vol. 1598: R. Poli, P. Nordin, W.B. Langdon, T.C. Fogarty (Eds.), Genetic Programming. Proceedings, 1999. X, 283 pages. 1999.

Vol. 1599: T. Ishida (Ed.), Multiagent Platforms. Proceedings, 1998. VIII, 187 pages. 1999. (Subseries LNAI).

Vol. 1601: J.-P. Katoen (Ed.), Formal Methods for Real-Time and Probabilistic Systems. Proceedings, 1999. X, 355 pages. 1999.

Vol. 1602: A. Sivasubramaniam, M. Lauria (Eds.), Network-Based Parallel Computing. Proceedings, 1999. VIII, 225 pages. 1999.

Vol. 1603: J. Vitek, C.D. Jensen (Eds.), Secure Internet Programming. X, 501 pages. 1999.

Vol. 1605: J. Billington, M. Diaz, G. Rozenberg (Eds.), Application of Petri Nets to Communication Networks. IX, 303 pages. 1999.

Vol. 1606: J. Mira, J.V. Sánchez-Andrés (Eds.), Foundations and Tools for Neural Modeling. Proceedings, Vol. I, 1999. XXIII, 865 pages. 1999.

Vol. 1607: J. Mira, J.V. Sánchez-Andrés (Eds.), Engineering Applications of Bio-Inspired Artificial Neural Networks. Proceedings, Vol. II, 1999. XXIII, 907 pages. 1999.

Vol. 1609: Z. W. Raś, A. Skowron (Eds.), Foundations of Intelligent Systems. Proceedings, 1999. XII, 676 pages. 1999. (Subseries LNAI).

Vol. 1610: G. Cornuéjols, R.E. Burkard, G.J. Woeginger (Eds.), Integer Programming and Combinatorial Optimization. Proceedings, 1999. IX, 453 pages. 1999.

Vol. 1611: I. Imam, Y. Kodratoff, A. El-Dessouki, M. Ali (Eds.), Multiple Approaches to Intelligent Systems. Proceedings, 1999. XIX, 899 pages. 1999. (Subseries LNAI).

Vol. 1612: R. Bergmann, S. Breen, M. Göker, M. Manago, S. Wess, Developing Industrial Case-Based Reasoning Applications. XX, 188 pages. 1999. (Subseries LNAI).

Vol. 1613: A. Kuba, M. Šámal, A. Todd-Pokropek (Eds.), Information Processing in Medical Imaging. Proceedings, 1999. XVII, 508 pages. 1999.

Vol. 1614: D.P. Huijsmans, A.W.M. Smeulders (Eds.), Visual Information and Information Systems. Proceedings, 1999. XVII, 827 pages. 1999.

Vol. 1615: C. Polychronopoulos, K. Joe, A. Fukuda, S. Tomita (Eds.), High Performance Computing. Proceedings, 1999. XIV, 408 pages. 1999.

Vol. 1617: N.V. Murray (Ed.), Automated Reasoning with Analytic Tableaux and Related Methods. Proceedings, 1999. X, 325 pages. 1999. (Subseries LNAI).

Vol. 1619: M.T. Goodrich, C.C. McGeoch (Eds.), Algorithm Engineering and Experimentation. Proceedings, 1999. VIII, 349 pages. 1999.

Vol. 1620: W. Horn, Y. Shahar, G. Lindberg, S. Andreassen, J. Wyatt (Eds.), Artificial Intelligence in Medicine. Proceedings, 1999. XIII, 454 pages. 1999. (Subseries LNAI).

Vol. 1621: D. Fensel, R. Studer (Eds.), Knowledge Acquisition Modeling and Management. Proceedings, 1999. XI, 404 pages. 1999. (Subseries LNAI).

Vol. 1622: M. González Harbour, J.A. de la Puente (Eds.), Reliable Software Technologies – Ada-Europe'99. Proceedings, 1999. XIII, 451 pages. 1999.

Vol. 1625: B. Reusch (Ed.), Computational Intelligence. Proceedings, 1999. XIV, 710 pages. 1999.

Vol. 1626: M. Jarke, A. Oberweis (Eds.), Advanced Information Systems Engineering. Proceedings, 1999. XIV, 478 pages. 1999.

Vol. 1627: T. Asano, H. Imai, D.T. Lee, S.-i. Nakano, T. Tokuyama (Eds.), Computing and Combinatorics. Proceedings, 1999. XIV, 494 pages. 1999.

Col. 1628: R. Guerraoui (Ed.), ECOOP'99 - Object-Oriented Programming. Proceedings, 1999. XIII, 529 pages. 1999.

Vol. 1629: H. Leopold, N. García (Eds.), Multimedia Applications, Services and Techniques - ECMAST'99. Proceedings, 1999. XV, 574 pages. 1999.

Vol. 1631: P. Narendran, M. Rusinowitch (Eds.), Rewriting Techniques and Applications. Proceedings, 1999. XI, 397 pages. 1999.

Vol. 1632: H. Ganzinger (Ed.), Automated Deduction – Cade-16. Proceedings, 1999. XIV, 429 pages. 1999. (Subseries LNAI).

Vol. 1633: N. Halbwachs, D. Peled (Eds.), Computer Aided Verification. Proceedings, 1999. XII, 506 pages. 1999.

Vol. 1634: S. Džeroski, P. Flach (Eds.), Inductive Logic Programming. Proceedings, 1999. VIII, 303 pages. 1999. (Subseries LNAI).

Vol. 1636: L. Knudsen (Ed.), Fast Software Encryption. Proceedings, 1999. VIII, 317 pages. 1999.

Vol. 1638: A. Hunter, S. Parsons (Eds.), Symbolic and Quantitative Approaches to Reasoning and Uncertainty. Proceedings, 1999. IX, 397 pages. 1999. (Subseries LNAI).

Vol. 1639: S. Donatelli, J. Kleijn (Eds.), Application and Theory of Petri Nets 1999. Proceedings, 1999. VIII, 425 pages. 1999.

Vol. 1653: S. Covaci (Ed.), Active Networks. Proceedings, 1999. XIII, 346 pages. 1999.

Preface

The Fast Software Encryption Workshop 1999 is the sixth in a series of workshops starting in Cambridge in December 1993.

The workshop was organized by General Chair William Wolfowicz, Fondazione U. Bordoni, and Programme Chair Lars Knudsen, University of Bergen, Norway, in cooperation with Securteam, as far as local arrangements were concerned. The workshop was held March 24-26, 1999 in Rome, Italy.

The workshop concentrated on all aspects of fast secret key ciphers, including the design and cryptanalysis of block and stream ciphers, as well as hash functions.

There were 51 submissions, all of them submitted electronically. One submission was later withdrawn by the authors, and 22 papers were selected for presentation. All submissions were carefully reviewed by at least 4 committee members. At the workshop, preliminary versions of all 22 papers were distributed to all attendees. After the workshop there was a final reviewing process with additional comments to the authors.

It has been a challenge for me to chair the committee of this workshop, and it is a pleasure to thank all the members of the programme committee for their hard work. The committee this year consisted of, in alphabetic order, Ross Anderson (Cambridge, UK), Eli Biham (Technion, Israel), Don Coppersmith (IBM, USA), Cunsheng Ding (Singapore), Dieter Gollmann (Microsoft, UK), James Massey (Denmark), Mitsuru Matsui (Mitsubishi, Japan), Bart Preneel (K.U. Leuven, Belgium), Bruce Schneier (Counterpane, USA), and Serge Vaudenay (ENS, France).

It is a great pleasure to thank William Wolfowicz for organising the workshop. Also, it is a pleasure to thank Securteam for the logistics and Telsy and Sun for supporting the conference. Finally, a big thank you to all submitting authors for their contributions, and to all attendees (approximately 165) of the workshop. Finally, I would like to thank Vincent Rijmen for his technical assistance in preparing these proceedings.

April 1999 Lars Knudsen

Table of Contents

Modes of Operation

Analysis of Block Ciphers II

Stream Ciphers

Improved Analysis of Some Simplified Variants of RC6

Scott Contini[1], Ronald L. Rivest[2], M.J.B. Robshaw[1], and Yiqun Lisa Yin[1]

[1] RSA Laboratories, 2955 Campus Drive
San Mateo, CA 94403, USA
{scontini,matt,yiqun}@rsa.com
[2] M.I.T. Laboratory for Computer Science, 545 Technology Square
Cambridge, MA 02139, USA
rivest@theory.lcs.mit.edu

Abstract. RC6 has been submitted as a candidate for the Advanced Encryption Standard (AES). Two important features of RC6 that were absent from its predecessor RC5 are a *quadratic function* and a *fixed rotation*. By examining simplified variants that omit these features we clarify their essential contribution to the overall security of RC6.

1 Introduction

RC6 is an evolutionary improvement of the block cipher RC5 [9] that was designed to meet the requirements of the Advanced Encryption Standard (AES). Like RC5, RC6 makes essential use of data-dependent rotations, but it also includes new features such as the use of four working registers instead of two, and the inclusion of integer multiplication as an additional primitive operation. Two components of RC6 that were absent from RC5 are a *quadratic function* to mix bits in a word more effectively and a *fixed rotation* that is used both to hinder the construction of good differentials and linear approximations and also to ensure that subsequent data dependent rotation amounts are more likely to be affected by any ongoing avalanche of change.

An initial analysis of the security of RC6 and its resistance to the basic forms of differential and linear cryptanalysis was given in [3]. Here we further illustrate how these new operations contribute to the security of RC6 by studying simplified variants (that is, intentionally weakened forms) of RC6. In particular, our approach is to find the best attack on the weakened forms and then try to adapt the attack to the full cipher. Since one of the design principles of RC6 was to build on the experience gained with RC5, the focus of our analysis will be in assessing the relevance to RC6 of the best existing cryptanalytic attacks on RC5. We will often refer to the work of Knudsen and Meier [8] and that of Biryukov and Kushilevitz [2]. These authors in particular have made very significant advances in understanding the security of RC5.

Our work splits naturally into two parts. The first focuses on the usefulness of the fixed rotation and the second on the quadratic function. While our analysis is targeted at RC6 and its simplified variants, some of the results might well be of independent interest. Our analysis starts by considering some of the weakened variants of RC6 that were introduced in [3]. More specifically, by dropping the fixed rotation we derive a cipher that we will denote by RC6-NFR (where NFR stands for no fixed rotation), by dropping the quadratic function we obtain RC6-I (where I stands for the identity function), and by dropping both operations we have RC6-I-NFR.

We will consider characteristics and differentials for RC6-I-NFR and RC6-NFR that have already been described in [3]. We study the relations between certain values of the subkeys and the probability of a characteristic and/or differential. Such phenomena are similar to the "differentially-weak keys" of RC5 observed by Knudsen and Meier [8]. We describe our observations and provide a thorough analysis which suggests that inclusion of the fixed rotation destroys the structure required for such dependencies to form. As a consequence RC6-I and RC6 itself seem to be immune from any direct extension of the results previously obtained on RC5.

Second, we examine the diffusive properties of the quadratic function and other operations that are used in RC6. In this analysis we track the Hamming weight (the number of 1's) of the exclusive-or difference between two quantities as they are encrypted. Quite naturally this leads to the idea of differentials that are constructed using such a measure of difference and this notion is very similar in spirit to earlier work on RC5 [2, 8]. We show that the quadratic function drastically increases the Hamming weight of some input difference when the Hamming weight of an input difference is small. This indicates that the use of both the quadratic function and data-dependent rotations in RC6 make it unlikely that differential attacks similar to those that were useful for RC5 [2, 8] can be effectively extended to RC6.

2 Description of RC6 and variants

A version of RC6 is specified as RC6-$w/r/b$ where the word size is w bits, encryption consists of a nonnegative number of rounds r, and b denotes the length of the encryption key in bytes. Throughout this paper we will set $w = 32$, $r = 20$, $b = 16$, 24, or 32 and we will use RC6 to refer to this particular version. The base-two logarithm of w will be denoted by $\lg w$ and RC6 uses the following six basic operations:

$a + b$	integer addition modulo 2^w
$a - b$	integer subtraction modulo 2^w
$a \oplus b$	bitwise exclusive-or of w-bit words
$a \times b$	integer multiplication modulo 2^w
$a \lll b$	rotate the w-bit word a to the left by the amount given by the least significant $\lg w$ bits of b
$a \ggg b$	rotate the w-bit word a to the right by the amount given by the least significant $\lg w$ bits of b

The user supplies a key of length k bytes which is then expanded to a set of subkeys. The key schedule of RC6 is described in [10]. Since here we are only concerned with encryption, we will assume that the subkeys $S[0]$, …, $S[43]$ are independent and chosen at random. RC6 works with four w-bit registers A, B, C, D which contain the initial input plaintext as well as the output ciphertext at the end of encryption. We use $(A, B, C, D) = (B, C, D, A)$ to mean the parallel assignment of values on the right to registers on the left.

Encryption with RC6-$w/20/b$

Input: Plaintext stored in four w-bit input registers A, B, C, D
w-bit round keys $S[0, \ldots, 43]$

Output: Ciphertext stored in A, B, C, D

Procedure:

```
B = B + S[0]
D = D + S[1]
for i = 1 to 20 do
    {
        t = (B × (2B + 1)) <<< lg w
        u = (D × (2D + 1)) <<< lg w
        A = ((A ⊕ t) <<< u) + S[2i]
        C = ((C ⊕ u) <<< t) + S[2i + 1]
        (A, B, C, D) = (B, C, D, A)
    }
A = A + S[42]
C = C + S[43]
```

The three simplified variants of RC6 that we will consider throughout the paper are distinguished from RC6 in the way the values of t and u are assigned. These differences are summarized in the following table.

The assignment of t and u in RC6 and some weakened variants

	RC6-I-NFR	*RC6-I*	*RC6-NFR*	*RC6*
$t =$	B	$B \lll \lg w$	$B \times (2B+1)$	$(B \times (2B+1)) \lll \lg w$
$u =$	D	$D \lll \lg w$	$D \times (2D+1)$	$(D \times (2D+1)) \lll \lg w$

3 The fixed rotation

In [8] Knudsen and Meier show that the values of some of the subkeys in RC5 can have a direct effect on the probability of whether some differential holds. In this section we show that a similar phenomenon can be observed in weakened variants of RC6 that do not use the fixed rotation. This should perhaps come as little surprise since while the structure of RC6-I-NFR is very different to that of RC5, it uses the same operations and might be expected to have similar behavior at times. We will then consider the role of the fixed rotation used in RC6 and we will demonstrate by analysis and experimentation that the effects seen in RC5 and some simplified variants of RC6 do not seem to exist within RC6 itself.

3.1 Existing analysis on RC6-I-NFR and RC6-NFR

In [3] one potentially useful six-round iterative characteristic was provided for attacking both RC6-I-NFR and RC6-NFR. This is given in Table 1. Here e_t is used to denote the 32-bit word that has all bits set to zero except bit t where $t = 0$ for the least significant bit. We use A_i (respectively B_i, C_i and D_i) to denote the values of registers A (respectively B, C, and D) at the beginning of round i. As an example, A_1, B_1, C_1, and D_1 contain the plaintext input after pre-whitening and for the six-round variants of the cipher, A_7, B_7, C_7 and D_7 contain the output prior to post-whitening. According to [3], when averaged over all possible subkeys, the expected probability that this characteristic holds is 2^{-30} for both RC6-I-NFR and RC6-I.

3.2 Refined analysis of RC6-I-NFR and RC6-NFR

Closer analysis of the characteristic probabilities for RC6-I-NFR and RC6-NFR suggests that the values of some of the subkeys during encryption are important. In particular, the characteristic of interest for RC6-I-NFR and RC6-NFR given in Table 1 can only occur if certain subkey conditions are met. Further, once these subkey conditions hold then the characteristic occurs with probability 2^{-20}, which is much higher than the initial estimate of 2^{-30} that was obtained by averaging over all subkeys.

i	A_i	B_i	C_i	D_i
1	e_{31}	e_{31}	0	0
		↓		
2	e_{31}	0	0	0
		↓		
3	0	0	0	e_{31}
		↓		
4	0	e_{31}	e_{31}	0
		↓		
5	e_{31}	e_{31}	0	e_{31}
		↓		
6	e_{31}	e_{31}	e_{31}	0
		↓		
7	e_{31}	e_{31}	0	0

Table 1. A characteristic for RC6-I-NFR and RC6-NFR.

In the analysis that follows we will concentrate on RC6-NFR. The same arguments and results can be applied to RC6-I-NFR by replacing $f(x) = x \times (2x+1)$ with the identity function $f(x) = x$. We will use the fact that $x \bmod 2^i$ uniquely determines $(x \times (2x+1)) \bmod 2^i$. Furthermore, the notation "$=_{32}$" will be used to indicate when two values are congruent modulo 32.

Lemma 1. *If the characteristic given in Table 1 holds for RC6-NFR, then the following two conditions on the subkeys must hold:*

$$f(-S[9]) =_{32} -S[7],$$
$$f(S[8]) =_{32} -S[11].$$

Proof. First we observe that if the characteristic is to hold, then certain rotation amounts derived from the B and D registers must be zero. Note that we always have that $B_i = A_{i+1}$ and that $D_i = C_{i+1}$. As a consequence, for the characteristic to hold we must have

$$D_2 =_{32} C_3 =_{32} 0, \qquad B_3 =_{32} A_4 =_{32} 0,$$
$$B_4 =_{32} A_5 =_{32} 0, \qquad D_4 =_{32} C_5 =_{32} 0,$$
$$B_5 =_{32} A_6 =_{32} 0, \qquad B_6 =_{32} A_7 =_{32} 0.$$

Using the fact that the rotation amounts are 0, we get the following two equations from rounds three and four and rounds four and five.

$$B_4 = (C_3 \oplus f(D_3)) + S[7], \tag{1}$$
$$B_5 = (C_4 \oplus f(D_4)) + S[9]. \tag{2}$$

Since $B_4 =_{32} 0$, $C_3 =_{32} 0$, $B_5 =_{32} 0$ and $D_4 =_{32} 0$, we have $S[7] =_{32} -f(D_3)$ and $C_4 =_{32} -S[9]$. Since $C_4 = D_3$, we obtain the first condition on subkeys $S[7] =_{32} -f(-S[9])$.

Similarly, looking at the computation from rounds four and five and rounds five and six, we get the following two equations.

$$D_5 = A_4 \oplus f(B_4) + S[8], \tag{3}$$
$$B_6 = C_5 \oplus f(D_5) + S[11]. \tag{4}$$

Since $A_4 =_{32} 0$, $B_4 =_{32} 0$, $B_6 =_{32} 0$ and $C_5 =_{32} 0$, we have $D_5 =_{32} S[8]$ and $S[11] =_{32} -f(D_5)$, and so $S[11] =_{32} -f(S[8])$. □

The subkey dependencies in Lemma 1 were obtained using only four equations (those for B_4, B_5, D_5 and B_6). In total, one could write down 12 equations of the form $B_{i+1} = (((C_i \oplus f(D_i)) \lll f(B_i)) + S[2i+1]$ and $D_{i+1} = (((A_i \oplus f(B_i)) \lll f(D_i)) + S[2i]$ for this characteristic. Although there might be dependencies involving other equations, the four given above will be the focus of the rest of this section. Essentially, each equation involves four variables and the aim is to combine equations to obtain two expressions with a single variable. If the two expressions involve the same variable then we can obtain conditions on the subkeys involved. The four equations we use are the only ones from the set of twelve that allow us to do this.

It is worth noting that given such conditions on the subkeys involved not only does the characteristic hold, but it does so with a higher probability than the expected value given in [3].

Lemma 2. *Assume that the characteristic given in Table 1 holds up to round five. Furthermore suppose that* $f(-S[9]) =_{32} -S[7]$ *and* $f(S[8]) =_{32} -S[11]$. *Then* $B_5 =_{32} 0$ *and* $B_6 =_{32} 0$.

Proof. From Lemma 1, we have that $S[7] =_{32} -f(D_3)$. This is equivalent to $-S[7] =_{32} f(C_4)$. Also, we have that $B_5 =_{32} C_4+S[9]$. So, if $-S[7] =_{32} f(-S[9])$ then $f(C_4) =_{32} f(-S[9])$ which implies that $C_4 =_{32} -S[9]$ and so $B_5 =_{32} 0$. A similar argument can be used to show that $B_6 =_{32} 0$. □

Lemma 2 shows that when the subkey conditions hold, $B_5 =_{32} 0$ and $B_6 =_{32} 0$. In this case the probability of the characteristic will be $2^{-30} \times 2^5 \times 2^5 = 2^{-20}$, since two of the rotation amounts are always zero. Recall that the estimated probability for the characteristic when averaged over all keys is 2^{-30} [3]. Here we have shown (Lemmas 1 and 2) that there is some irregularity in the distribution of the probability: For a fraction of 2^{-10} keys the probability is 2^{-20}, and for the rest of the keys the probability is much smaller than 2^{-30}. This kind of irregular distribution can sometimes be exploited as was demonstrated by Knudsen and Meier with RC5 [8] who showed some techniques for using it in a differential attack. We would expect the same to apply here. Similar subkey dependencies can be observed for some of the other characteristics for RC6-I-NFR and RC6-NFR given in [3]. However in some cases the characteristic must be iterated more than once before dependencies exist.

Note that the behavior of the differential associated with some characteristic is typically of more importance in a differential attack. For RC6-I-NFR, while the characteristic displays the irregular behavior already described, the associated differential has been experimentally verified to hold with the expected probability [3]. However the associated differential for RC6-NFR appears to have the same irregular behavior as the characteristic. Why is there this discrepancy? In [3] it is shown how the introduction of the quadratic function helps to reduce the additional effect of differentials. In short, for RC6-I-NFR there are many equally viable paths that match the beginning and end-points of the characteristic. If the characteristic fails to hold because of some choice of subkey values, other characteristics hold instead thereby maintaining the probability of the differential. However, with RC6-NFR we introduce the quadratic function and this typically reduces differentials to being dominated by the action of a single characteristic. Irregular behavior in the characteristic will therefore manifest itself as irregular behavior in the differential.

3.3 Differential characteristics in RC6-I and RC6

Let us now consider the role of the fixed rotation that was omitted in RC6-I-NFR and RC6-NFR. We will find that this single operation removes the kind of subkey dependencies that occurred in these two variants.

We will focus on RC6-I in the analysis for simplicity, and the same arguments also apply to the full RC6. We will need to make some heuristic assumptions to make headway with our analysis. Nevertheless our experimental results confirm that the differential behavior of RC6-I is pretty much as expected. It also closely matches the behavior described in [3].

Consider the characteristic given in Table 2. This is the characteristic which seemed to be one of the most useful for attacking RC6-I [3]. We first argue that there are no subkey dependencies of the form we described in Section 3.2 for this characteristic and we then broaden our discussion to include other, more general, characteristics.

i	A_i	B_i	C_i	D_i
1	e_{16}	e_{11}	0	0
		↓		
2	e_{11}	0	0	0
		↓		
3	0	0	0	e_{26}
		↓		
4	0	e_{26}	e_{26}	0
		↓		
5	e_{26}	e_{21}	0	e_{26}
		↓		
6	e_{21}	e_{16}	e_{26}	0
		↓		
7	e_{16}	e_{11}	0	0

Table 2. A useful characteristic for RC6-I.

At this stage we need some new notation and the exponent n will be used to denote when some quantity has been rotated to the left by n bit positions. For example, $D_2^5 =_{32} 15$ means that when D_2 is rotated five bits to the left, then the decimal value of the least significant five bits is 15. Of course, this is the same as saying that the most significant five bits of D_2 take the value 15.

For simplicity, we will assume that $(x+y)^j = x^j + y^j$ where j denotes a rotation amount. This is true if, and only if, there is no carry-out when adding the top j bits and no carry-out when adding the bottom $32-j$ bits. For the sake of our analysis however we make this assumption, since it should actually facilitate the construction of any potential subkey dependencies!

Following the arguments in Lemma 1, for the characteristic in Table 2 to hold the following rotation amounts must take the values indicated:

$$D_2^5 =_{32} C_3^5 =_{32} 15, \qquad B_3^5 =_{32} A_4^5 =_{32} 27,$$
$$B_4^5 =_{32} A_5^5 =_{32} 27, \qquad D_4^5 =_{32} C_5^5 =_{32} 27,$$
$$B_5^5 =_{32} A_6^5 =_{32} 17, \qquad B_6^5 =_{32} A_7^5 =_{32} 17.$$

We wish to write down four equations similar to Equations (1), (2), (3) and (4) which cause subkey dependencies in RC6-NFR. From round three to four, the difference e_{26} is copied from register D_3, is changed to e_{31} by the action of the fixed rotation, and then exclusive-ored into the C strand. For it to become the e_{26} that appears in B_4, the data dependent rotation B_3^5 must have the value 27. Hence, we must have $B_3^5 =_{32} 27$ and $B_4 = (C_3 \oplus D_3^5)^{27} + S[7] = C_3^{27} \oplus D_3 + S[7]$.