A DIFFERENTIAL ATTACK ON THE CIKS-1 BLOCK CIPHER

Brian J. Kidney, Howard M. Heys and Theodore S. Norvell
Electrical and Computer Engineering
Memorial University of Newfoundland
St. John's, NL A1B 3X5, Canada
Email: {bkidney, howard, theo}@engr.mun.ca

Abstract

In 2002, Moldovyan and Moldovyan introduced a cipher with security based mainly on data-dependent permutations (DDPs) called CIKS-1. The goal of the cipher was to exploit the speed and simplicity of DDPs to create a fast hardware-oriented block cipher. In the original paper, the authors claimed that the cipher is immune to differential cryptanalysis. This paper investigates the propagation of differentials through the cipher. An attack is then presented to reveal the last subkey of the cipher with a data complexity better than previously claimed.

Keywords: *Cryptography; computer security; cryptanalysis; encryption; block cipher.*

1. INTRODUCTION

In 1994, Ron Rivest introduced a new block cipher called RC5 [1]. This cipher was quite simple, depending only on a key schedule and a set of Data Dependant Rotations (DDRs) for its security. RC5 was not the first cipher to use data–dependent rotations, but it did attract interest due to its ability to thwart linear and differential cryptanalysis attacks [2]. Since then, data–dependent rotations and data–dependent permutations (DDPs) have become increasingly popular in ciphers. Two of the final candidate ciphers in the Advanced Encryption Standard (AES), MARS and RC6, used DDRs along with other primitives to produce ciphers resistant to both linear and differential cryptanalysis.

In [3] a new cipher making heavy use of DDPs was introduced. CIKS–1, an 8–round block cipher, was designed for speed in hardware and uses the DDPs to provide nonlinearity while mixing key and data bits. Preliminary analysis of the cipher showed it to be resistant to both linear and differential cryptanalysis.

Two previous attacks on this cipher have been presented. In [4], a chosen plaintext attack was shown to work on a 5–round version of CIKS–1. The authors used selected inputs to effectively bypass the first round and tracked the parity of the data through the cipher to reveal the subkey of the last round. This attack has a complexity of $2^{65.7}$, but is limited in the number of rounds to which it can be applied.

In [5] we presented an attack which exploited the slow rate of hamming weight growth of the data in CIKS-1. The χ^2 test is used to compare the weight of the cipher's output to a binomial distribution when encrypted by a guessed key. It was shown that the weight of the first round subkey can be derived with a time complexity of 2^{52} for a 6–round version of the cipher.

In this paper a differential attack on CIKS–1 is presented. A brief analysis of the CIKS–1 data–dependent permutations are given, discussing the probabilities of a difference passing through them unchanged. An attack that reveals the last subkey of the cipher is then presented.

2. THE CIKS–1 CIPHER

The CIKS–1 cipher is a fast, hardware–oriented cipher, with its principle security component being data–dependent permutations. It is a block cipher with block size 64–bits. The cipher is composed of 8 rounds, each with a 32–bit subkey for a total key size of 256–bits. A single round of the cipher is shown in Figure 1. The solid lines in the diagram show the flow of data and the dashed lines are control vectors. Permutations are labeled $P_{n/m}$, where n is the number of bits permuted and m is the number of bits of control.

The 64–bit data is split into half for input to the left and right sides. Each side is then used as a control vector (CV) for permutations of the data on the opposite side. The left hand side data also plays the role of CV for the permutation of the key. There are two fixed permutations (Π_1 and Π_2) used to further shuffle the CVs for permutations P_2 and P_6. The key is added to the right side data by the XOR. At the end of a round the right side data is added to the left side using 16 parallel 2–bit additions and, with the exception of the last round, the two sides are swapped.

CCECE 2004 - CCGEI 2004, Niagara Falls, May/mai 2004
0-7803-8253-6/04/$17.00 © 2004 IEEE

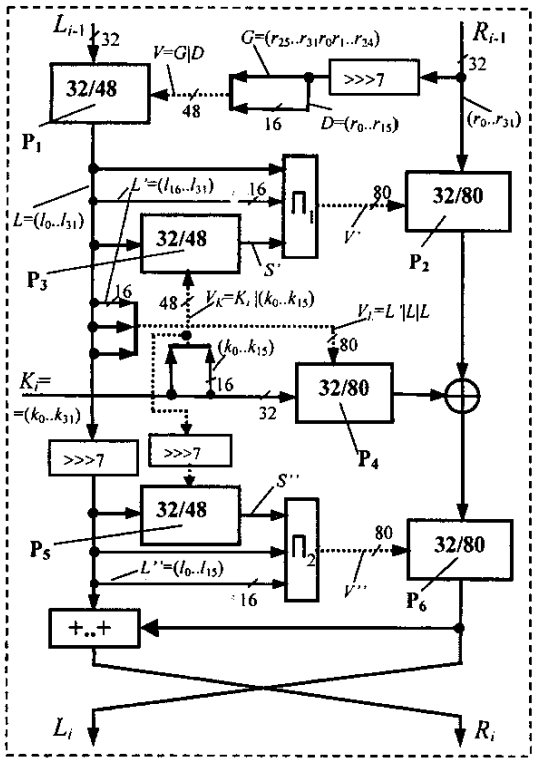

Fig. 1. A single round of the CIKS–1 cipher [3]

3. THE CIKS–1 DATA–DEPENDENT PERMUTATIONS

The label data–dependent permutations refers to a large set of functions. Basically, a data–dependent permutation includes any permutation of data which is directly influenced by another piece of the data. In RC5, the DDP is a simple rotation of one half of the data n bits left, where n is determined by a subset of the bits in the other half of the data. This is known as a data–dependent rotation, one of the simplest DDPs.

The data–dependent permutations in CIKS–1 use a control vector to determine the permutation of the position of the input bits in the output. For example, the 2–bit $P_{2/1}$ DDP requires a CV of only one bit. If the CV is a 0, the bits are swapped, otherwise they pass through the primitive without changing position. These smaller permutation blocks are layered together to form more complex permutations.

Figure 2 shows the "butterfly" pattern that is used to connect the various levels of these permutations. This ensures that bits that are grouped together in the input are not continually swapped with each other as they move through the levels. It also guarantees that a CV which is

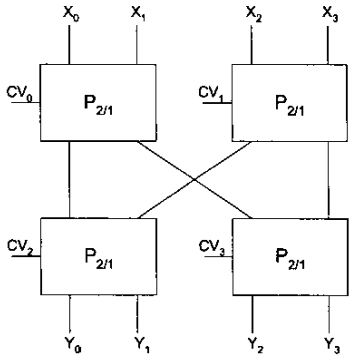

Fig. 2. A $P_{4/4}$ Data–Dependant Permutation

comprised of mostly 1s will not result in a poorly permuted output. Further information on the structure of the data–dependent permutations found in CIKS–1 can be found in [3].

4. DIFFERENTIAL CRYPTANALYSIS

Introduced by Biham and Shamir in [6], differential cryptanalysis is a chosen plaintext attack. The attack classically uses sets of pairs of inputs have a common difference $X' = X_0 \oplus X_1$, where X_0 and X_1 represent two different input values. These pairs, when used as input to the cipher, lead to a detectable output difference $Y' = Y_0 \oplus Y_1$, where Y_0 and Y_1 represent outputs corresponding to to the inputs X_0 and X_1 respectively. The pair, (X', Y') is referred to as a differential. Highly likely differentials can be exploited to determine key bit information.

Once a highly probable differential is found for x rounds of an $x + 1$ round cipher, the last round subkey can be attacked. Many pairs with the specified input difference are encrypted, over $x + 1$ rounds. Each pair is then partially decrypted through the last round using all possible candidate subkeys and a check for the output difference of round x is performed. The actual subkey will result in the largest count of the round x output differences to match the difference predicted by the differentials.

Being the main element of CIKS–1, it might be expected that the DDPs would play a major role in the propagation of differences through the cipher. In fact, other than the parallel addition, DDPs are involved in all operations of the cipher data. On both sides of the cipher, data is scrambled by the permutations and the key itself is scrambled before being added. In our analysis we focus on the hamming weight of differences, rather than actual differences.

Obviously, if the control vector on a DDP is the same in two different instances, then the data will be permuted the same way. When the control vector does change,

the likelihood of an added bit difference depends on the difference at the input. When there is only a difference in the control vector, the input to the $P_{2/1}$ permutation that the particular CV bit affects determines if there is a bit difference created. The swap at this site is only noticeable if the input bits are different. Thus, there is a 50% chance that the data will be unchanged by the control vector difference. In this case the probability that the cipher data will remain unchanged by the DDP is 2^{-n}, where n is the number of different bits in the control vector.

The case where there is a difference in weight of the input, as well as the CV, is more complex. When the CV difference bit is the control for a $P_{2/1}$ permutation where there is also a difference in one of the input bits, there is no new bit difference introduced in the data. In fact, if both input bits are changed, the output will have no new difference. These cases actually increase the chance of a given difference surviving a DDP. In our analysis, a one–bit difference input into a $P_{32/80}$ with a control vector containing two differences has approximately a 28% probability of retaining a one–bit difference at the output.

5. ANALYSIS OF DIFFERENTIALS

In the paper [3] the CIKS–1 authors make the claim that the number of plaintext pairs required for a differential attack on the cipher is in the order of 2^{64}. This analysis is done by ignoring the internal key schedule and permutation P_1 and focusing on P_2 and P_6 (the $P_{32/80}$ permutations on the right hand side of the cipher). Although their analysis is simplified, the authors contend that the assumptions made are to the advantage of the attacker, and even so, the cipher appears to be secure against differential cryptanalysis.

If an analysis of the cipher is done not on strict differentials, but the hamming weight of differentials as they pass through the cipher, it is possible to construct an attack which has much lower complexity than the one in [3]. Three input differences weights were examined for relations to four output difference weights of interest. Those are given in Table I for one round where ($wt(\Delta L_{i-1})$, $wt(\Delta R_{i-1})$) and ($wt(\Delta L_i)$, $wt(\Delta R_i)$) are the left and right halves of the hamming weights of the differences in the input and output respectively.

Taking the case of $(wt(\Delta L_{i-1}) = 1, wt(\Delta R_{i-1}) = 1)$, we see that the right side difference can appear either once or twice in control vector V. Taking into account both cases, the probability of the one–bit difference surviving P_1 is 12.5%. Again, depending on where the one–bit difference in the left side occurs, it can appear in V' either two or three times. Thus, the probability of the one–bit difference on the right side surviving P_2 is approximately 8.1%. When the key is XORed with the right side data, there are many possible cases to examine. Any case where subtraction of the right side and key differences has a

Differentials	Probability
$(wt(\Delta L_{i-1})$=0,$wt(\Delta R_{i-1})$=1) $\rightarrow(wt(\Delta L_i)$=1,$wt(\Delta R_i)$=2)	$2^{-3.4}$
$(wt(\Delta L_{i-1})$=0,$wt(\Delta R_{i-1})$=1) $\rightarrow(wt(\Delta L_i)$=1,$wt(\Delta R_i)$=1)	$2^{-1.83}$
$(wt(\Delta L_{i-1})$=1,$wt(\Delta R_{i-1})$=0) $\rightarrow(wt(\Delta L_i)$=0,$wt(\Delta R_i)$=1)	$2^{-7.25}$
$(wt(\Delta L_{i-1})$=1,$wt(\Delta R_{i-1})$=1) $\rightarrow(wt(\Delta L_i)$=1,$wt(\Delta R_i)$=0)	$2^{-13.7}$
$(wt(\Delta L_{i-1})$=1,$wt(\Delta R_{i-1})$=1) $\rightarrow(wt(\Delta L_i)$=1,$wt(\Delta R_i)$=1)	$2^{-13.7}$
$(wt(\Delta L_{i-1})$=1,$wt(\Delta R_{i-1})$=1) $\rightarrow(wt(\Delta L_i)$=1,$wt(\Delta R_i)$=2)	$2^{-7.75}$

TABLE I
Frequency of occurrence of transitions of interest with random keys.

weight of one could result in the right side having a difference of one–bit. The most dominant of these cases are $(wt(\Delta R_{i-1}) = 1, wt(\Delta K) = 0)$ and $(wt(\Delta R_{i-1}) = 1, wt(\Delta K) = 2)$. To simplify the analysis, we consider only these cases and get a likelihood of the one–bit difference surviving of approximately $2^{-5.7}$. P_6 acts similarly to P_2. Overall, the probability of a $(wt(\Delta L_{i-1}) = 1, wt(\Delta R_{i-1}) = 1)$ difference leading to a $(wt(\Delta L_i) = 1, wt(\Delta R_i) = 0)$ is $2^{-13.7}$.

The other differential probabilities can be calculated in a similar way. Note that in the cases where the difference only appears on one side of the cipher, many of the cipher's elements do not affect the difference on the other side.

These one round differentials can be chained together to get an overall differential for the cipher. To represent this the notation $(L_{i-1}, R_{i-1}) \rightarrow (L_i, R_i)$ is used to represent the difference of each side of the input and output pair. If we use the 7 round chain of differentials (0,1) → (1,1) → (1,0) → (0,1) → (1,1) → (1,0) → (0,1) → (1,1) with probability $2^{-47.39}$. Figure 3 shows the probability of transitions between all of the differentials of interest.

6. PROPOSED ATTACK

As shown in the last section there are certain differentials with a high probability of occurrence. The differentials (0, 1) → (1, 1), (1, 0) → (0, 1), (1, 1) → (1, 2) and (1, 0) → (1, 2) are the most attractive. When chaining together multiple rounds these differentials are reused as frequently as possible to keep the overall probability high. Though the (1, 0) → (1, 2) and (1, 1) → (1, 2) differentials have a high probability, they are not as useful since they can only be used at the end of a chain.

To attack the cipher, we first chose a differential with a relatively high probability of success to use. For example, to attack a 6 round version of the cipher the chain (1, 0) → (0, 1) → (1, 1) → (1, 0) → (0, 1) → (1, 1) could be used with a probability of approximately $2^{-31.86}$. In

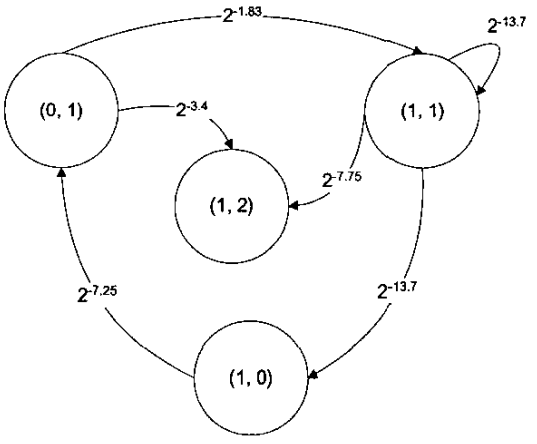

Fig. 3. Probabilities of Transitions of interest

Score	Frequency
0	9760
1	238
2	2

TABLE II
Frequency of occurrence of desired differential with random keys.

this case, the output difference would be expected once in every 4 billion encryptions. Hence, several times more than 4 billion encryptions would be required to clearly distinguish the occurrence of the expected difference. To attack the cipher, for every plaintext pair encrypted, the last round is decrypted using all possible subkeys, keeping a count of the number of times the (1,1) difference appears. The key with the highest count at the end of the process is the most likely to be the actual subkey.

To date, an attack has been implemented on a 3–round reduced version of the cipher using 10000 plaintext pairs. The chain used for the attack was (1, 0) → (0, 1) → (1, 1), with a probability of occurrence of approximately $2^{-9.08}$. The test was run using the actual key, 32 keys different in one bit from the actual key, and 10000 random keys. The actual key returned the expected difference 22 times. The keys with a one–bit difference from the actual key all returned a count of 0, making them quite easily distinguishable from the actual key. The set of random keys produced counts of 0 to 2. The distribution of counts for the random keys is given in Table II. The conclusion is that the correct key is easily distinguishable.

Although only a 3–round version of this attack has been implemented, it could easily be extended to the 6–round version with data complexity of approximately 2^{35}. In fact, it is theoretically possible to extend this attack to the full cipher. For this extension, the differential chain (0, 1) → (1, 1) → (1, 0) → (0, 1) → (1, 1) → (1, 0) → (0, 1) → (1, 1) could be used, with the data complexity of approximately 2^{56} to recover the final round subkey and a time complexity of $2^{32} \times 2^{56} = 2^{88}$. The remaining subkeys can then be found by stripping off the last round and implementing the attack again on the remaining rounds.

7. CONCLUSION

In the original paper for the CIKS–1 cipher, the authors' analysis of the possibility of differential attack on the cipher showed that it would have a data complexity of 2^{64}. In this paper a differential attack has been proposed with data complexity of approximately 2^{56}. To prove the concept of this attack, the attack has been implemented on a 3–round version of the cipher. This attack showed that the actual key could be determined easily from both random keys and keys one–bit different than the actual.

Although preliminary testing of this attack on the 3–round reduced version of the CIKS–1 cipher is quite promising, future work is planned to extend the attack. The 6–round attack given in the paper with data complexity of approximately 2^{35} will be implemented and tested.

References

[1] R. L. Rivest, "The RC5 encryption algorithm," in *K. U. Leuven Workshop on Cryptographic Algorithms*, December 1994.

[2] B. S. Kaliski Jr. and Y. L. Yin, "On differential and linear cryptanalysis of the RC5 encryption algorithm," in *Advances in Cryptology – CRYPTO '95* (D. Coppersmith, ed.), vol. 963 of *Lecture Notes in Computer Science*, pp. 171–184, Springer–Verlag Berlin, 1995.

[3] A. Moldovyan and N. Moldovyan, "A cipher based on data–dependent permutations," *Journal of Cryptology*, vol. 15, pp. 61–72, January 2002.

[4] C. Lee, D. Hong, S. Lee, S. Lee, H. Yang, and J. Lim, "A chosen plaintext linear attack on block cipher CIKS–1," in *Information and Communications Security: 4th International Conference, ICICS 2002, Singapore, December 9-12, 2002. Proceedings*, vol. 2513 of *Lecture Note in Computer Science*, pp. 456–468, Springer-Verlag Heidelberg, January 2002.

[5] B. J. Kidney, H. M. Heys, and T. S. Norvell, "A weight based attack on the ciks–1 block cipher," in *Newfoundland Electrical and Computer Engineering Conference Proceedings*, IEEE Newfoundland and Labrador, November 2003.

[6] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," *Journal of Cryptography*, vol. 4, no. 1, pp. 3–72, 1991.