The Analysis of a New Class of Unbalanced CAST Ciphers

X. Zhu and H. M. Heys

Faculty of Engineering and Applied Science
Memorial University of Newfoundland
St. John's, Newfoundland, Canada, A1B 3X5
Email: howard@engr.mun.ca

Abstract

The original CAST cipher is an efficient and secure private-key block cipher designed to be an alternative to DES. In this paper, we present a new class of unbalanced CAST ciphers which employ the same structure of S-box and round function as the original CAST cipher but has a lower memory requirement. Furthermore, we investigate the security of the ciphers with respect to differential and linear cryptanalysis. The result of analysis shows that unbalanced CAST ciphers with appropriate parameters are resistant to differential and linear cryptanalysis.

1. Introduction

The most widely used private-key block encryption algorithm, the Data Encryption Standard (DES) [8], is nearing the end of its useful life and is theoretically breakable by two powerful cryptanalytic attacks, differential and linear cryptanalysis [2][5]. In addition, DES was explicitly designed for fast hardware implementation and has a slow software performance because of its extensive use of permutations and small S-boxes [6].

The original CAST cipher [1] appears to be resistant to differential and linear cryptanalysis [4][3]. It is easily implemented by software and has good encryption/decryption performances on 32-bit microprocessors because of using four large 8×32 S-boxes and eliminating the need of permutations. However, large S-boxes require more memory to store their lookup tables. This might be unacceptable in some implementations where the memory is extremely restricted.

In this paper, we present a family of ciphers referred to as unbalanced CAST ciphers, which employ the same type of S-box and round function as the original CAST cipher, and which require a variable amount of memory depending on the chosen parameters. Furthermore, we examine the ciphers' resistance to differential and linear cryptanalysis.

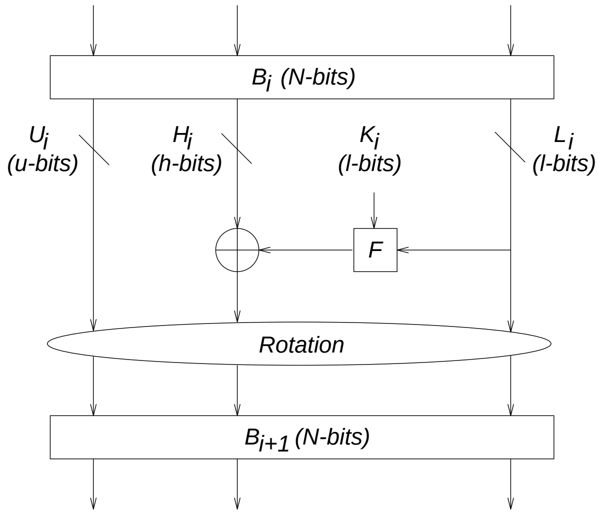

Figure 1: The i-th Round Operation

2. Description of the Algorithm

The unbalanced CAST cipher is a product cipher which iterates a round operation R times. The round operation of the general cipher may be conceptualized as in Figure 1. Let N be the block size of the cipher. In the i-th round, an N-bit input B_i is first split into three pieces, L_i, H_i, and U_i. L_i is input to the round function F keyed with an l-bit subkey K_i, H_i is XORed with the output of the round function, and U_i bypasses the round function. Finally, L_i, the XOR sum of the output of the round function and H_i, and U_i are processed by a rotation operation and result in an N-bit output, B_{i+1}. The round function has the same structure as the one of the original CAST cipher [1]. Let M be the number of $m \times n$ S-boxes used in the round function with $m < n$, then the cipher has $l = M \times m$, $h = n$, and $u = N - l - h$, where $l \leq h$. The round function F is keyed by XORing the l-bit K_i with L_i before L_i is applied to inputs of S-boxes. The n-bit outputs of all M S-boxes are bit-wise XORed to form the n-bit round function output $F(L_i, K_i)$. In our analysis, we shall assume that the S-boxes are randomly generated.

In general the unbalanced CAST ciphers can be characterized entirely by the parameters N, M, m, n and the rotation operation. For example, the original CAST cipher [1] can be characterized by $N = 64$, $M = 4$, $m = 8$, $n = 32$, and a 32-bit rotation in the form of swapping the two half blocks. Khafre [6] can be characterized by $N = 64$, $M = 1$, $m = 8$, $n = 32$, and a rotation of eight or sixteen bits specified according to the round number. We refer to the ciphers as unbalanced since, in general, $l \neq N/2$ necessarily. A balanced CAST cipher, such as the original CAST cipher, has $l = n = N/2$, and $u = 0$.

If round functions from two ciphers, Cipher 1 and Cipher 2, are constructed by the same type of S-boxes and the following equation holds:

$$M_1 \cdot R_1 = M_2 \cdot R_2, \tag{1}$$

where the subscript is used to indicate the cipher number, then the two ciphers may be considered to be roughly equivalent in efficiency if the S-box table lookup is considered the dominant operation (i.e. assuming data rotation in CPU registers may be ignored). For example, an 8-round original CAST cipher with four 8×32 S-boxes may be considered roughly equivalent in efficiency to a 32-round unbalanced CAST cipher with one 8×32 S-box. However, Equation (1) does not imply that the two ciphers have an equivalent level of security.

Based on Figure 1, we propose a rotation operation as well as the round operation, which is effective in ensuring that ciphertext bits are influenced by plaintext bits as quickly as possible. It is described as the following:

1. B_i is divided into two halves, the right half and the left half.
2. L_i, taken from the l least significant bits of the right half, is input into the F round function whose output is XORed with H_i which is the h least significant bits of the left half.
3. The right half is right cyclically rotated by l bits.
4. Two halves are swapped to form B_{i+1}.

The swapping of two half blocks is still necessary in an unbalanced CAST cipher because H_i XORed with the output of the round function can be immediately brought to the input position of the round function at the next round, which has all ciphertext bits influenced faster by all plaintext bits.

In [7], it is shown that the 8×32 S-box utilized by the original CAST cipher exhibits good cryptographic properties. In the following sections, we will mainly focus on 64-bit unbalanced CAST ciphers with one and two 8×32 S-boxes since both ciphers require only 1/4 and 1/2 the memory of the original CAST cipher, respectively. Other scenarios are examined in [9].

3. Differential Cryptanalysis

In this section we consider applying the methods of [4] to the differential cryptanalysis of unbalanced CAST ciphers. If there is a zero output XOR caused by a non-zero input XOR with a differential probability for a round function, there exists an N/l-round iterative characteristic for the unbalanced CAST cipher. Table 1 gives an example of a possible 8-round iterative characteristic for the unbalanced CAST cipher with one 8×32 S-box. The letter A represents a non-zero XOR value

Rnd	Left Half				Right Half				Output XOR				Probability
Ω_P	A	0	0	0	0	0	0	0					
1	A	0	0	0	0	0	0	0	0	0	0	0	
2	0	0	0	0	A	0	0	0	0	0	0	0	
3	0	A	0	0	0	0	0	0	0	0	0	0	
4	0	0	0	0	0	A	0	0	0	0	0	0	
5	0	0	A	0	0	0	0	0	0	0	0	0	
6	0	0	0	0	0	0	A	0	0	0	0	0	
7	0	0	0	A	0	0	0	0	0	0	0	0	
8	0	0	0	0	0	0	0	A	0	0	0	0	with p
Ω_C	A	0	0	0	0	0	0	0					

Table 1: An 8-round Iterative Characteristic for the Unbalanced CAST Cipher with One 8×32 S-box

and the plaintext XOR difference is given by $A0000000$. The XOR values to the right side of double vertical lines represent input XORs to the round function, while the output XOR column represents the output XORs of the round function. The p is a probability with which the input XOR value of A may cause the output XOR value of 0000 in the XOR table of the round function.

Denote $N_E(\Delta X, \Delta Z) = v$ as an entry in the XOR table of the round function corresponding to the input XOR of ΔX, the output XOR of ΔZ, and the entry value of v. Then, the result of analysis in [4] has shown that the probability of $N_E(\Delta X, 0) = 2$ is $2^7/2^{32} = 2^{-25}$, where $\Delta X \neq 0$. Assume that the occurrence of ΔZs for different ΔXs are independent. Since there are totally $(2^8 - 1)$ non-zero ΔXs, the expected number of entries in the XOR table which satisfy $N_E(\Delta X, 0) = 2$ is $(2^8 - 1) \cdot 2^{-25} \approx 2^{-17}$, which is so small that it would be difficult to find the 8-round iterative characteristic of Table 1 with a differential probability of $p = 2/2^8 = 2^{-7}$ when we randomly generate an 8×32 S-box.

Similarly, for the unbalanced CAST cipher with two 8×32 S-boxes, the probability of $N_E(\Delta X, 0) = 4$ is $(2^7)^2/2^{32} = 2^{-18}$. The expected number of entries in the XOR table which satisfy $N_E(\Delta X, 0) = 4$ is $(2^8 - 1)^2 \cdot 2^{-18} \approx 2^{-2}$. This entry can be used to construct a 4-round iterative characteristic with a differential probability of $p = 4/2^{16} = 2^{-14}$ as in Table 2. We assume that the best iterative characteristic for the unbalanced CAST cipher with two 8×32 S-boxes is a 4-round iterative characteristic with a differential probability of 2^{-14}. Screening a pair of S-boxes to prevent

*R*nd	Left Half	Right Half	Output XOR	Probability
Ω_P	A B 0 0	0 0 0 0		
1	A B 0 0	0 0 0 0	0 0 0 0	
2	0 0 0 0	A B 0 0	0 0 0 0	
3	0 0 A B	0 0 0 0	0 0 0 0	
4	0 0 0 0	0 0 A B	0 0 0 0	with 2^{-14}
Ω_C	A B 0 0	0 0 0 0		

Table 2: A 4-round Iterative Characteristic for the Unbalanced CAST Cipher with Two 8×32 S-boxes

the characteristic from occurrence would be possible although time-consuming since about 2^{30} XOR pairs would have to be examined.

It seems unlikely that the unbalanced CAST cipher with one 8×32 S-box has an iterative characteristic constructed by an entry of $N_E(\Delta X, 0)$ in the XOR table of the round function since the likelihood of occurrence of this entry is too small. We further investigate the possibility that there exist other kinds of characteristics similar in nature to iterative characteristics, but not strictly iterative. We refer to these characteristics as pseudo-iterative characteristics. Table 3 displays such an 8-round pseudo-iterative characteristic. The differential probability of this characteristic is 2^{-28} for eight rounds. The characteristic requires that the XOR table must have entries of the forms of $00XX$, $X000X$, and $XX00$, where X can be a byte of any XOR value except zero. The probability that the XOR table has entries of this form is an upper bound on the probability that an S-box can be used to produce the characteristic of Table 3 and is approximately 2^{-4}. Since the likelihood of occurrence of Table 3 is not low enough, we conclude that an 8-round pseudo-iterative characteristic with a differential probability of 2^{-28} for the unbalanced CAST cipher with one 8×32 S-box is possible.

*R*nd	Left Half	Right Half	Output XOR	Probability
Ω_P	A B 0 0	C D 0 0		
1	A B 0 0	C D 0 0	0 0 0 0	
2	0 C D 0	A B 0 0	0 0 0 0	
3	0 A B 0	0 C D 0	0 0 0 0	
4	0 0 C D	0 A B 0	0 0 0 0	
5	0 0 A B	0 0 C D	0 0 a_1 b_1	with 2^{-7}
6	D 0 0 C	0 0 A_1 B_1	d_1 0 0 c_1	with 2^{-7}
7	B_1 0 0 A_1	D_1 0 0 C_1	b_2 0 0 a_2	with 2^{-7}
8	C_1 D_1 0 0	B_2 0 0 A_2	c_2 d_2 0 0	with 2^{-7}
Ω_C	A_2 B_2 0 0	C_2 D_2 0 0		

Table 3: An 8-round Pseudo-iterative Characteristic for the Unbalanced CAST Cipher with one 8×32 S-box

In summary, by applying the best iterative or pseudo-iterative characteristic and using an $(R-N/l)$-round attack on an R-round cipher [2], the 32-round unbalanced CAST cipher with one 8×32 S-box and the 24-round unbalanced CAST cipher with two 8×32 S-boxes are resistant to differential cryptanalysis, requiring at least 2^{84} and 2^{70} pairs of chosen plaintexts, respectively.

4. Linear Cryptanalysis

The objective of linear cryptanalysis is to find a linear approximation of a cipher only derived from plaintext, ciphertext, and key terms [3]. We consider an N/l-round iterative linear approximation [9], which has a form that the value of the XOR sum of a subset of output bits of a round function is equal to 0 or 1 with a probability significantly different from 1/2. Since an iterative linear approximation does not involve any input bits of the round function, concatenating an iterative linear approximation to itself any number of times does not introduce any intermediate terms, and has a fixed reduction rate of the probability for each additional iterative linear approximation.

Each output bit of an $m \times n$ S-box is an m-bit boolean function. If an unbalanced CAST cipher has $M = 1$, the output bits of the round function are directly the output bits of the S-box. Then the probability that the XOR sum of a subset of output bits of the round function is equal to 0 or 1 can be derived by calculating the hamming weight of the XOR sum of the corresponding subset of m-bit boolean functions of the S-box. If an unbalanced CAST cipher has $M > 1$, the output bits of the round function are derived from the XOR sum of the corresponding output bits of all S-boxes. Then the probability that the XOR sum of a subset of output bits of the round function is equal to 0 or 1 can be determined by calculating the hamming weight of the XOR sum of the corresponding subset of m-bit boolean functions of every S-box and combining them with Matsui's Piling-up Lemma [5]. An unbalanced CAST cipher can have many iterative linear approximations. The best one has the probability farthest from 1/2.

Let $f(X)$ be a randomly generated m-bit boolean function, where $X \in \{0,1\}^m$. Then the probability that the hamming weight of $f(X)$ is less than w is given by

$$P(wt(f(X)) < w) = \sum_{j=0}^{j=w-1} \binom{2^m}{j} / 2^{2^m}. \qquad (2)$$

Assuming that there are 2^n randomly and independently generated m-bit boolean functions for an $m \times n$ S-box [3], the probability that the S-box has at least one m-bit boolean function whose hamming weight is less than w or greater than $2^m - w$ is given by

$$p = 1 - (1 - 2 \cdot \rho)^{2^n}, \qquad (3)$$

where $\rho = P(wt(f) < w)$ and $w \leq 2^{m-1}$.

For an 8×32 S-box, assuming that $w = 72$, we have $\rho = 3.4 \times 10^{-13}$ and $p = 2.9 \times 10^{-3}$. Therefore, all 8-bit boolean functions of the 8×32 S-box are expected to have the hamming weight greater than 71 and less than 185 with a probability of 99.7%.

Let $f_i(X)$ be an m-bit boolean function generated by XORing a subset of output bits of an S-box S_i and w_i be the hamming weight of $f_i(X)$, where $i = 1, \cdots, M$. For a randomly selected X, the probability of $f_i(X) = 0$ is given by

$$P(f_i(X) = 0) = 1 - \frac{w_i}{2^m}. \tag{4}$$

Since each S-box is independently and randomly selected, using Matsui's Piling-up Lemma, we have a linear approximation for the round function

$$\bigoplus_{i=1}^{M} f_i(X) = 0 \tag{5}$$

which holds with a probability

$$p_e = \frac{1}{2} + 2^{M-1} \prod_{i=1}^{M} (\frac{1}{2} - \frac{w_i}{2^m}), \tag{6}$$

where all $f_i(X)$ must involve the same subset of output bits.

Assume that $w = 72$ for the unbalanced CAST cipher with one 8×32 S-box. Then $|p_e - 1/2| = 2^{-2.2}$ by Equation (6). Since each plaintext bit is XORed with the output of the round function four times for each eight rounds, assuming that the output of the round function of every two rounds is independent and using Matsui's Piling-up Lemma, the probability of an 8-round iterative linear approximation, P_E, is bounded by $|P_E - 1/2| \leq 2^{-5.8}$. Therefore, the number of plaintexts required to determine one equivalent key bit is at least 2^{60} for a 48-round cipher with a 97.7% confidence level [3].

Also, assume that $w = 72$ for the unbalanced CAST cipher with two 8×32 S-boxes. Then $|p_e - 1/2| = 2^{-3.4}$ by Equation (6). Since each plaintext bit is XORed with the output of the round function two times for each four rounds, the probability of a 4-round iterative linear approximation, P_E, is bounded by $|P_E - 1/2| \leq 2^{-5.8}$. Therefore, the number of plaintexts required to determine one equivalent key bit is at least 2^{60} for a 24-round cipher with a 97.7% confidence level.

Note that the probabilities of N/l-round iterative linear approximations are the upper bounds. The real probabilities will be much smaller in a practical linear cryptanalysis. This is because the rotation operation causes the plaintext bit positions to be changed every round and to be XORed with different output bits of the round function in different rounds. If one of the output bit boolean functions has a hamming weight close to 1/2, the probability of the N/l-round iterative linear approximation will become close to 1/2 rapidly, and the iterative linear approximation will be useless for linear cryptanalysis. Therefore, we conclude that the 48-round unbalanced CAST cipher with one 8×32 S-box and the 24-round unbalanced CAST cipher with two 8×32 S-boxes are secure against linear cryptanalysis.

5. Summary

In this paper, we present a new class of private-key encryption algorithms referred to as unbalanced CAST ciphers. The result of analysis shows that the 48-round unbalanced CAST cipher with one 8×32 S-box and the 24-round unbalanced CAST cipher with two 8×32 S-boxes, which are equivalent to the 12-round original CAST cipher in efficiency but require only 1/4 and 1/2 the memory of the original CAST cipher, are resistant to both differential and linear cryptanalysis. Further cases with different parameter values for unbalanced CAST ciphers are analyzed in [9].

References

[1] C. M. Adams and S. E. Tavares, *Designing S-Boxes for Ciphers Resistant to Differential Cryptanalysis*, Proceedings of the 3rd Symposium on State and Progress of Research in Cryptography, pp. 181-190, Rome, Italy, February 1993.

[2] E. Biham and A. Shamir, *Differential Cryptanalysis of DES-Like Cryptosystems*, Journal of Cryptology, vol. 4, no. 1, pp. 3-72, 1991.

[3] H. M. Heys and S. E. Tavares, *On the Security of the CAST Encryption Algorithm*, Canadian Conference on Electrical and Computer Engineering, pp. 332-335, Halifax, Nova Scotia, Canada, September 1994.

[4] J. Lee, H. M. Heys and S. E. Tavares, *On the Resistance of the CAST Encryption Algorithm to Differential Cryptanalysis*, Workshop on Selected Areas in Cryptography (SAC '95), pp. 107-120, Carleton University, Ottawa, Ontario, Canada, May 1995.

[5] M. Matsui, *Linear Cryptanalysis Method for DES Cipher*, Advances in Cryptology, Proceedings of EUROCRYPT '93, pp. 386-397, Springer-Verlag, 1993.

[6] R. C. Merkle, *Fast Software Encryption Functions*, Advances in Cryptology, Proceedings of CRYPTO '90, pp. 627-638, Springer-Verlag, 1990.

[7] S. Mister and C. M. Adams, *Practical S-Box Design*, Workshop on Selected Areas in Cryptography (SAC '96), pp. 61-76, Queen's University, Kingston, Ontario, Canada, August 1996.

[8] National Bureau of Standards, *Data Encryption Standard*, Federal Information Processing Standard Publication 46, 1977.

[9] X. Zhu, *A New Class of Unbalanced CAST Ciphers and its Security Analysis*, Master's Thesis in Preperation, Memorial University of Newfoundland, St. John's, Newfoundland, Canada, 1997.