Improved characteristics for differential cryptanalysis of hash functions based on block ciphers

Vincent Rijmen* Bart Preneel**

Katholieke Universiteit Leuven
ESAT-COSIC
K. Mercierlaan 94, B-3001 Heverlee, Belgium

{bart.preneel,vincent.rijmen}@esat.kuleuven.ac.be

Abstract. In this paper we present an improvement of the differential attack on hash functions based on block ciphers. By using the specific properties of the collision attack on hash functions, we can greatly reduce the work factor to find a pair that follows the characteristic. We propose a new family of differential characteristics that is especially useful in combination with our improvement. Attacks on a hash function based on DES variants reduced to 12, 13 or 15 rounds become faster than brute force collision attacks.

1 Introduction

Hash functions are functions that compress inputs of arbitrary length to an output of fixed length n. For cryptographic applications, we impose the following properties:

1. *one-wayness:* given Y, it is difficult to find an X such that $h(X) = Y$, and given X and $h(X)$, it is difficult to find $X' \neq X$ such that $h(X') = h(X)$
2. *collision resistance:* it is difficult to find X and $X' \neq X$ such that $h(X) = h(X')$.

Most hash functions are *iterated* hash functions: the input X is divided into t blocks X_i, where each block contains b bits. The length of the input should be appended at the end. If the length of X is not a multiple of b, one uses an unambiguous *padding scheme* to extend the input. The hash function h can then be described as:

$$H_i = f(X_i, H_{i-1}) \qquad i = 1, 2, \ldots, t.$$

Here f is called the round function, H_0 is specified together with the scheme, and H_t is the hashcode.

* N.F.W.O. research assistant, sponsored by the National Fund for Scientific Research (Belgium).

** N.F.W.O. postdoctoral researcher, sponsored by the National Fund for Scientific Research (Belgium).

Appeared in *Fast Software Encryption, FSE 1994*, Lecture Notes in Computer Science 1008, B. Preneel (ed.), Springer-Verlag, pp. 242–248, 1995.
©1995 Springer-Verlag

Hash functions can be constructed from a block cipher algorithm, e.g., the DES [FI46-77]. The main motivation for this type of construction is the minimization of design and implementation effort. An example of a well established construction is based on the following round function f:

$$f(X_i, H_{i-1}) = \mathrm{DES}(H_{i-1}, X_i) \oplus X_i \,, \tag{1}$$

where $\mathrm{DES}(H_{i-1}, X_i)$ denotes the DES encryption of the plaintext X_i with the key H_{i-1}. This scheme was proposed by S. Matyas, C. Meyer and J. Oseas in [MMO85], and is described in [P93a] together with eleven variants with an equivalent security level. The differential attack however works only for four of these variants, since it requires that the cryptanalyst has explicit control over the plaintext input of the block cipher and that the key is fixed.

2 Differential cryptanalysis of hash functions

Differential cryptanalysis is a powerful cryptographic tool. Its application to block ciphers (e.g., the DES) is described in [BS93]. We assume that the reader is familiar with the basic ideas of this method. Differential cryptanalysis can be applied to hash functions in the same way as to the corresponding block ciphers, but there are some important differences [P93b].

- For the case of a collision attack, we control the plaintext input. This makes the differential attack on the hash function feasible. The differential attack on a block cipher used as an encryption device, on the contrary, is only of theoretic interest.
- We know the key, and sometimes we can choose the key or choose the best alternative out of a set of possible keys. We can exploit this in several ways. First, when searching for a collision, we can select those input values that follow the characteristic with probability one in certain rounds. Precomputation of a few tables allows us to choose the inputs of four or five consecutive rounds (cf. Sect. 3). Second, the probability of some characteristics is key-dependent. If we have some control over the key, we choose it to be optimal for our characteristic, otherwise we can select a characteristic with optimal probability for the given key. Third, we can use an early abort strategy: as soon as we see that the pair is a wrong pair, we can discard it. For most inputs we need to compute only a few rounds.
- There are more restrictions on the characteristic: in block cipher analysis we only want to know the output of the most probable characteristic. For hash functions, we need a characteristic that produces a collision, i.e., the output exor of the round function f must be zero. For our example, this means that the output exor of the block cipher has to match the input exor. Moreover, the characteristic must cover all the rounds: 1R-, 2R-, or 3R-attacks do not apply. This reduces the probability of the characteristic.
- We need only one right pair to find a collision or a second preimage.

In the rest of this paper we will only consider collision attacks.

Appeared in *Fast Software Encryption, FSE 1994*, Lecture Notes in Computer Science 1008, B. Preneel (ed.), Springer-Verlag, pp. 242–248, 1995.
©1995 Springer-Verlag

3 Choosing inputs

In a collision attack, we can choose the input values (or messages) arbitrarily. We can use this freedom to enhance our chance of success. A naive approach is to select messages that will follow the proposed characteristic in the first two rounds with probability one. In this section we present an algorithm that enables us to pass four rounds with probability one. By a very simple extension of the algorithm, it is possible to pass five rounds. Fig. 1 defines the notation for intermediate values of the hashing.

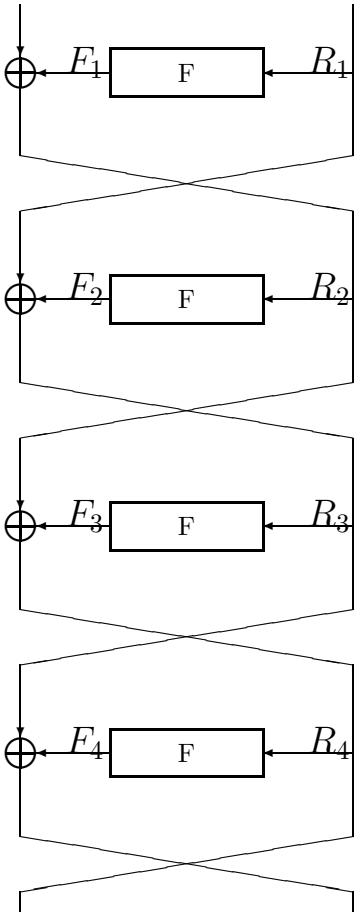

Fig. 1. Four rounds of the DES.

Algorithm:

Appeared in *Fast Software Encryption, FSE 1994*, Lecture Notes in Computer Science 1008, B. Preneel (ed.), Springer-Verlag, pp. 242–248, 1995.
©1995 Springer-Verlag

Step 1: Calculate table T_1 that lists all values of R_1 that follow the characteristic in round 1. Idem for tables T_2 and T_3 that list the values of F_2 and R_3 respectively. Since in each round only a few S-boxes are active, these tables can be reduced in size by the use of "don't cares": we don't care what the inputs are of non-active S-boxes and thus we do not specify these values.

Step 2: Match these three tables and look for all possible values of (R_1, F_2, R_3).

Step 3: Calculate table T_4 with all values for R_4. For every (R_1, F_2, R_3) "invert" round two and try to match the possible values of R_2, $F(R_3)$ and R_4.

Step 4: For each match found, calculate the inputs to the first round.

By calculating an extra table we can precede these four rounds with an extra round before round one.

4 Good characteristics

It has already been observed in [P93b,Kn94] that it is a non trivial problem to find good even-round characteristics for the hash function (1). One-round iterative characteristics can have an arbitrary number of rounds, but they have a very low probability of $\frac{1}{234}$ per round (cf. Fig. 2). Two-round iterative characteristics have the highest probability for seven rounds or more [Ma94], but in hash functions they can only be applied to DES variants with an odd number of rounds. This can be concluded from Fig. 2. Each $0 \leftarrow \chi$ round has on average a probability of $\frac{1}{234}$. Dependent on the round key, this probability becomes $\frac{1}{146}$ or $\frac{1}{585}$. For 13 rounds, the attack requires the same number of encryptions as a brute-force collision attack based on the birthday paradox ($\approx 2^{32.5}$). However, since the DES has 16 rounds, any serious attack requires a characteristic with an even number of rounds.

$(\chi \ , \ \chi)$	$(\chi \ , \ 0)$
$0 \leftarrow \chi$	$0 \leftarrow 0$
$0 \leftarrow \chi$	$0 \leftarrow \chi$
$0 \leftarrow \chi$	$0 \leftarrow 0$
$0 \leftarrow \chi$	$0 \leftarrow \chi$
$0 \leftarrow \chi$	$0 \leftarrow 0$
$(\chi \ , \ \chi)$	$(\chi \ , \ 0)$

Fig. 2. One-round and two-round iterative characteristics.

In [P93b], B. Preneel proposed to search for an input value χ that is a good fix-point ($\chi \leftarrow \chi$) and a good building block for an iterative characteristic ($0 \leftarrow \chi$). In [Kn94], L. Knudsen shows that such a characteristic cannot have a high probability. The problem is that all χ with a good probability for $0 \leftarrow \chi$

Appeared in *Fast Software Encryption, FSE 1994*, Lecture Notes in Computer Science 1008, B. Preneel (ed.), Springer-Verlag, pp. 242–248, 1995.
©1995 Springer-Verlag

have low probability for $\chi \leftarrow \chi$, and vice versa. L. Knudsen therefore proposes the use of an iterative characteristic based on a special four round building block (cf. Fig. 3). This building block has probability $2^{-23.6}$ averaged over all keys, and $2^{-23.0}$ for optimal keys. For a DES variant with 8 rounds the workfactor is comparable to a brute-force collision search.

$$
\begin{array}{l}
(\texttt{E0000004}_\texttt{x}\ ,\ \texttt{E0000004}_\texttt{x}) \\
\texttt{00000002}_\texttt{x} \leftarrow \texttt{E0000004}_\texttt{x} \\
\texttt{00000002}_\texttt{x} \leftarrow \texttt{E0000006}_\texttt{x} \\
\texttt{00000002}_\texttt{x} \leftarrow \texttt{E0000006}_\texttt{x} \\
\texttt{00000002}_\texttt{x} \leftarrow \texttt{E0000004}_\texttt{x} \\
(\texttt{E0000004}_\texttt{x}\ ,\ \texttt{E0000004}_\texttt{x})
\end{array}
$$

Fig. 3. The 4-round iterative characteristic of L. Knudsen.

Our idea is the following: we take a χ with good probability for $0 \leftarrow \chi$. Instead of inserting one $\chi \leftarrow \chi$ round, we insert five 'transient' rounds (cf. Fig. 4). These five rounds have a low probability that is however better than the fix-point construction. This is not a problem since we choose the input values of these transient rounds in such a way that they are passed with probability one. A computer search has indicated that the best transient rounds have a symmetrical pattern. For our computer search, we considered the 50 χ's with the best $\chi \leftarrow 0$ probability. For each χ all possible α's and β's were examined. The best combination is $\chi = 00196000$ and $\alpha = \beta = 04450180$. The probabilities of the different rounds are given in Table 1. Note that there exist χ's that yield a lower probability, for which the optimal α and β are different.

Table 1. The different rounds in our characteristic and their probabilities.

structure	probability	comments
$0 \leftarrow \chi$	2^{-8}	key independent
$\alpha \leftarrow \chi$	$2^{-10.8}$	$2^{-9.95}$ for 50% of the keys
$\chi \oplus \alpha \leftarrow \alpha$	$2^{-20.5}$	$2^{-18.1}$ for 4.7% of the keys

The fact that the probability of these rounds depends on the key, can be exploited to reduce the work/success ratio: we can eliminate the keys that give the characteristic a low (or zero) probability. We call keys that give a non-zero probability near-optimal. For our choice of χ and α (cf. Fig 1), 4.5% of the keys are near-optimal. Stronger criteria for near-optimal keys are possible. Table 2 gives the theoretical probabilities and workfactors for DES variants with various number of rounds. The probability of the characteristic is given for near-optimal keys. The workfactors are calculated as follows: the reciprocal of the probability

Appeared in *Fast Software Encryption, FSE 1994*, Lecture Notes in Computer Science 1008, B. Preneel (ed.), Springer-Verlag, pp. 242–248, 1995.
©1995 Springer-Verlag

of the rounds where we do not choose the input values multiplied by a reduction factor that takes the early abort strategy into account. The numbers for DES variants with an odd number of rounds are obtained by choosing input values for five arbitrarily chosen consecutive rounds. The characteristic is the best 2-round iterative characteristic of [BS93].

$$
\begin{array}{rcl}
(\chi & , & 0) \\
0 & \leftarrow & 0 \\
0 & \leftarrow & \chi \\
\dots & & \dots \\
\chi & \leftarrow & \chi \\
0 & \leftarrow & \chi \\
\dots & & \dots \\
 & & \\
 & & \\
(\chi & , & 0)
\end{array}
\qquad\qquad
\begin{array}{rcl}
(\chi & , & 0) \\
0 & \leftarrow & 0 \\
0 & \leftarrow & \chi \\
\dots & & \dots \\
\alpha & \leftarrow & \chi \\
\chi \oplus \beta & \leftarrow & \alpha \\
\chi \oplus \alpha & \leftarrow & \beta \\
\beta & \leftarrow & \chi \\
0 & \leftarrow & 0 \\
(\chi & , & 0)
\end{array}
$$

Fig. 4. Two alternatives for the transient part of an iterative characteristic.

Table 2. A survey of probabilities of the characteristics and theoretical workfactors for reduced versions of the DES.

# rounds	probability ($\log_2$)	workfactor ($\log_2$)
8	-65.8	8
9	-28.8	5
12	-81.8	21.4
13	-43.2	18.9
14	-89.8	29.2
15	-50.3	25.9
16	-97.8	37.0

5 Further work

For less than seven rounds of the DES, iterative characteristics are not the best ones. Instead of building upon the iterative characteristic one could search for a characteristic of the form: optimal six round characteristic – four transient rounds (inputs chosen) – optimal six round characteristic.

With the current even-round characteristics, we make no use of the fact that we can pass five rounds. This can easily be seen on Fig. 4: the four central rounds with the worst probability are flanked by two rounds with probability

Appeared in *Fast Software Encryption, FSE 1994*, Lecture Notes in Computer Science 1008, B. Preneel (ed.), Springer-Verlag, pp. 242–248, 1995.
©1995 Springer-Verlag

one. Nothing can be gained by calculating one of these two rounds. Maybe there exist good characteristics of the form: optimal five round characteristic – five transient rounds (inputs chosen) – optimal six round characteristic. We believe this could bring the work factor of the differential attack on the variant with 16 rounds down to the value of a brute force collision attack.

References

[BS93] E. Biham and A. Shamir, *"Differential Cryptanalysis of the Data Encryption Standard,"* Springer-Verlag, 1993.

[FI46-77] FIPS 46, *"Data Encryption Standard,"* National Bureau of Standards, 1977.

[Kn92] L. R. Knudsen, "Iterative characteristics of DES and s^2–DES," *Advances in Cryptology, Proc. Crypto'92, LNCS 740*, E.F. Brickell, Ed., Springer-Verlag, 1993, pp. 497–511.

[Kn94] L. Knudsen, "Block ciphers – analysis, design and applications," *PhD. Thesis, DAIMI PB 485*, Aarhus University, 1994.

[LMM91] X. Lai, J.L. Massey, and S. Murphy, "Markov ciphers and differential cryptanalysis," *Advances in Cryptology, Proc. Eurocrypt'91, LNCS 547*, D.W. Davies, Ed., Springer-Verlag, 1991, pp. 17–38.

[Ma94] M. Matsui, "On correlation between the order of S-boxes and the strength of DES," *Advances in Cryptology, Proc. Eurocrypt'94, LNCS*, A. De Santis, Ed., Springer-Verlag, to appear.

[MMO85] S. M. Matyas, C. H. Meyer, and J. Oseas, "Generating strong one-way functions with cryptographic algorithm," *IBM Techn. Disclosure Bull.,* Vol. 27, No. 10A, 1985, pp. 5658–5659.

[P93a] B. Preneel, R. Govaerts, and J. Vandewalle, "Hash functions based on block ciphers: a synthetic approach," *Advances in Cryptology, Proc. Crypto'93, LNCS 773*, D. Stinson, Ed., Springer-Verlag, 1994, pp. 368–378.

[P93b] B. Preneel, "Differential cryptanalysis of hash functions based on block ciphers," *Proceedings of the 1st ACM Conference on Computer and Communications Security*, 1993, pp. 183-188.

Appeared in *Fast Software Encryption, FSE 1994*, Lecture Notes in Computer Science 1008, B. Preneel (ed.), Springer-Verlag, pp. 242–248, 1995.
©1995 Springer-Verlag