On the Security of the 128-Bit Block Cipher DEAL

Stefan Lucks[*]

Theoretische Informatik
University of Mannheim, 68131 Mannheim A5, Germany
lucks@th.informatik.uni-mannheim.de

Abstract. DEAL is a DES-based block cipher proposed by Knudsen. The block size of DEAL is 128 bits, twice as much as the DES block size. The main result of the current paper is a certificational attack on DEAL-192, the DEAL variant with a 192-bit key. The attack allows a trade-off between the number of plaintext/ciphertext pairs and the time for the attacker's computations. Nevertheless, the DEAL design principle seems to be a useful way of doubling the block size of a given block cipher.

1 Introduction

The "data encryption standard" (DES) is the world's most well known symmetric cipher. Formally, the standard defines a 64-bit key, but 8 bits are defined as "parity bits" and only 56 bits are actually used as the encryption key, i.e., the DES key size is 56 bits. Brute-force attacks for recovering a key are feasible, today – and considered the only practical way of breaking DES. Thus, while the DES itself cannot be considered secure, it is still attractive to use it as a component for designing another cipher with an increased key size, such as triple DES. A concern both for DES and for triple DES is the block size of only 64 bits, which may lead to matching ciphertext attacks.

In [1], Knudsen proposes the r-round Feistel cipher DEAL with a block size of 128 bits. It uses DES in the round function and accepts three different key sizes, namely 128, 192, and 256 bits. For the first two sizes, the author recommends $r = 6$, for 256 bit keys, the number r of rounds should be 8. Depending on the key size, the three variants of DEAL are denoted DEAL-128, DEAL-192, and DEAL-256. DEAL is suggested as a candidate for the NIST AES standard.

This paper is organised as follows. In Section 2, a description of DEAL itself is given, Section 3 presents attacks on the six-round version of DEAL, and Section 4 deals with further concerns and conclusions.

[*] Supported by German Science Foundation (DFG) grant KR 1521/3-1.

L. Knudsen (Ed.): FSE'99, LNCS 1636, pp. 60–70, 1999.

2 A Description of DEAL

Next, we describe the block cipher DEAL and the key schedules for DEAL-128, DEAL-192, and DEAL-256.

2.1 The DEAL Core

A 128-bit plaintext is split up into two halves $(x_0, y_0) \in (\{0,1\}^{64})^2$. Two consecutive rounds j and $j+1$ of DEAL take the 128-bit block $(x_{j-1}, y_{j-1}) \in (\{0,1\}^{64})^2$ and the two round keys R_j and R_{j+1} as the input to compute the output block $(x_{j+1}, y_{j+1}) \in (\{0,1\}^{64})^2$ by

$$\begin{array}{llcll} x_j & := x_{j-1}, & & y_j & := y_{j-1} \oplus E_{R_j}(x_{j-1}), \\ x_{j+1} & := x_j \oplus E_{R_{j+1}}(y_j), & \text{and} & y_{j+1} & := y_j, \end{array}$$

where $\oplus$ describes the bit-wise xor-operation for 64-bit strings and j is odd. By E, we denote the DES encryption function. Two rounds j and $j+1$ are also described in Figure 1.

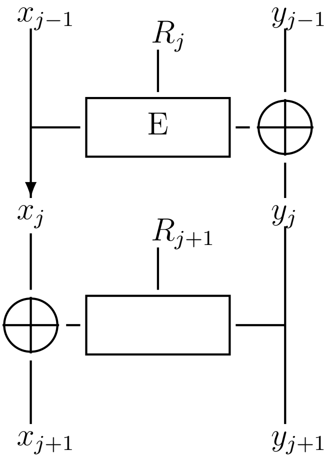

Fig. 1. Round j and $j+1$ of DEAL, j odd

Thus, for DEAL-128 and DEAL-192 we need 6 round keys $R_1, \ldots R_6$, for DEAL 256 we need 8 round keys $R_1, \ldots R_8$. Internally, every round key is used as a DES key, ignoring the “parity bits” and hence consists of 56 bits. We need three “key scheduling” algorithms to generate the round keys from the given master key of 128, 192, or 256 bits.

See Figure 2 for a visual description of six rounds of DEAL.

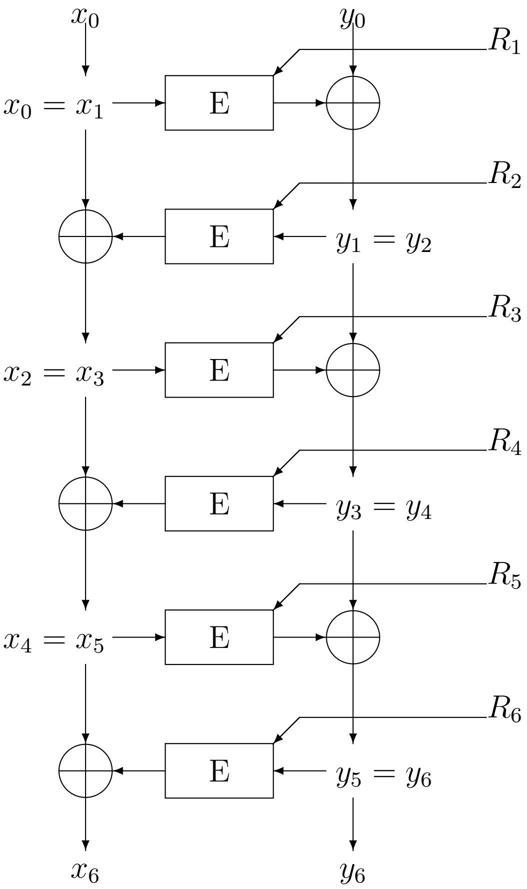

Fig. 2. The six-round version of DEAL

2.2 The DEAL Key Schedule

The key schedule of DEAL takes s keys K_1, ..., K_s of 64 bits each ($s \in \{2, 3, 4\}$) and returns r round keys R_1, ..., R_r of 56 bits each ($r \in \{6, 8\}$). The round keys are generated using DES encryption under a fixed DES-key R_* (which is $R_* =$ `0123456789abcdef` in hexadecimal notation). $\underline{1}$, ..., $\underline{4}$ are four different constant 64-bit strings, where none is `000...0`. The DEAL-128 round keys are generated from K_1, K_2 as follows:

$$\begin{aligned}
R_1 &:= E_{R_*}(K_1)\\
R_2 &:= E_{R_*}(K_2 \oplus R_1)\\
R_3 &:= E_{R_*}(K_1 \oplus R_2 \oplus \underline{1})
\end{aligned}$$

$$\begin{aligned}
R_4 &:= E_{R_*}(K_2 \oplus R_3 \oplus \underline{2}) \\
R_5 &:= E_{R_*}(K_1 \oplus R_4 \oplus \underline{3}) \\
R_6 &:= E_{R_*}(K_2 \oplus R_5 \oplus \underline{4})
\end{aligned}$$

The DEAL-192 round keys are generated from K_1, K_2, and K_3 like this:

$$\begin{aligned}
R_1 &:= E_{R_*}(K_1) \\
R_2 &:= E_{R_*}(K_2 \oplus R_1) \\
R_3 &:= E_{R_*}(K_3 \oplus R_2) \\
R_4 &:= E_{R_*}(K_1 \oplus R_3 \oplus \underline{1}) \\
R_5 &:= E_{R_*}(K_2 \oplus R_4 \oplus \underline{2}) \\
R_6 &:= E_{R_*}(K_3 \oplus R_5 \oplus \underline{3})
\end{aligned}$$

Given K_1, K_2, K_3, and K_4, the DEAL-256 round keys are:

$$\begin{aligned}
R_1 &:= E_{R_*}(K_1) \\
R_2 &:= E_{R_*}(K_2 \oplus R_1) \\
R_3 &:= E_{R_*}(K_3 \oplus R_2) \\
R_4 &:= E_{R_*}(K_4 \oplus R_3) \\
R_5 &:= E_{R_*}(K_1 \oplus R_4 \oplus \underline{1}) \\
R_6 &:= E_{R_*}(K_2 \oplus R_5 \oplus \underline{2}) \\
R_7 &:= E_{R_*}(K_3 \oplus R_6 \oplus \underline{3}) \\
R_8 &:= E_{R_*}(K_4 \oplus R_7 \oplus \underline{4})
\end{aligned}$$

The parity bits of the 64-bit values R_i are ignored when R_i is used as a DES-key (i.e., a DEAL round key), but relevant for computing R_{i+1}.

3 Attacking DEAL

Well known meet-in-the-middle techniques can be used to recover the DEAL round keys. This was stressed by Knudsen himself. The six-round version of DEAL is vulnerable to a meet-in-the-middle attack requiring roughly $(2^{56})^3 = 2^{168}$ encryptions. For the eight-round version, the attack needs roughly $(2^{56})^4 = 2^{224}$ encryptions.

Thus the theoretical key size of DEAL is approximately no more than 168 for the six-round version and 224 for the eight-round version. This bounds the theoretical key size of DEAL-192 (six rounds) and DEAL-256 (eight rounds). Due to their memory requirements, these meet-in-the-middle techniques are quite unrealistic, though trade-off techniques to save storage space at the cost of increased running time are known [3].

Note that finding a DEAL-n key by exhaustive key search (by "brute force") takes about $c * 2^n/2$ single DES encryptions with $c = 8$ for DEAL-192, $c = 9$ for DEAL-128, and $c = 11$ for DEAL-256. (One can reject most combinations of round keys *before* the last round. I.e., rejecting a combination of round keys takes about 5 DES encryptions for the six-round variants of DEAL and about 7 DES encryptions for the eight-round variant. In the case of DEAL-192, we need to generate the first two round keys at most every 2^{64} steps, while the round keys R_3, R_4, and R_5 are generated every step. This takes about 3 DES encryptions. The reasoning for DEAL-128 and DEAL-256 is similar.)

3.1 A Chosen Ciphertext Attack for the Six-Round Version

In addition to meet-in-the-middle attacks, Knudsen describes a chosen plaintext attack to recover the round keys of the six-round version of DEAL. His attack requires about 2^{121} DES-encryptions using roughly 2^{70} chosen plaintexts. This is significantly faster than the average number of DES-encryptions needed to break DEAL-128 by exhaustive key search (i.e., 2^{127} encryptions) and greatly faster than the number of DES-encryptions to break DEAL-192 (2^{191}). Due to the huge amount of chosen plaintexts, Knudsen claims that exhaustive key search nevertheless is less unrealistic than this attack.

We will use the same technique, but we are going backwards, i.e., our attack is a chosen ciphertext attack to gain information about the first round key R_1. Given the first 56-bit round key R_1, there are only 2^8 possible choices for the first sub-key K_1 of the master key. Knowing the last 56-bit round key instead of the first one, is somewhat less helpful for the attacker, due to the DEAL key schedule.

Recall the last five rounds of six-round DEAL. The round keys in use are $R_2, \ldots, R_6$, the input is the pair (x_1, y_1) of 64-bit strings (where $x_1 = x_0$ is the left half of the plaintext and y_1 is generated in the first round by $y_1 = y_0 \oplus E_{R_1}(x_1)$), and the output is the ciphertext (x_6, y_6). Consider two input/output pairs $((x_1, y_1), (x_6, y_6))$ and $((x'_1, y'_1), (x'_6, y'_6))$ with $y_1 = y'_1$, $y_6 = y'_6$, $x_1 \oplus x'_1 = \alpha = x_6 \oplus x'_6$ and $\alpha \neq 0$.

First, we show that two such input/output pairs cannot both exist: Since $y_1 = y'_1$ and $y_6 = y'_6$, we have $x_3 \oplus x'_3 = \alpha = x_5 \oplus x'_5$. On the other hand, $y_1 = y_2 = y'_1 = y'_2$ and $x_1 \neq x'_1$, thus $y_3 = y_2 \oplus E_{R_3}(x_2) \neq y'_3$ and hence $E_{R_4}(y_3) \neq E_{R_4}(y'_3)$. If $x_3 \oplus x'_3 = \alpha$, then $x_5 \oplus x'_5 = \alpha \oplus E_{R_4}(y_3) \oplus E_{R_4}(y'_3) \neq \alpha$, in contradiction to the above.

Next, we exploit their non-existence to narrow down the number of possibilities for R_1 and hence K_1:

- Choose a fixed value $y_6 \in \{0,1\}^{64}$ and 2^{64} ciphertexts (s, y_6), where $s \in \{0,1\}^{64}$. Let $(x_0[s], y_0[s])$ denote the corresponding plaintexts. Then we expect to find about 2^{63} two-sets $\{s,t\} \subset \{0,1\}^{64}$ with $s \neq t$ and $x_0[s] \oplus x_0[t] = s \oplus t$.
- Check all possible 56-bit DES keys R, whether

  $$y_0[s] \oplus E_R(x_0[s]) = y_0[t] \oplus E_R(x_0[t]).$$

  As we have shown above, this is impossible if $R = R_1$. Hence, if "=" holds, we know $R \neq R_1$, which limits further key search. If $R \neq R_1$, the operation $E_R : \{0,1\}^{64}$ can be viewed as a random permutation, hence in this case "=" holds with a probability of 2^{-64}. Given 2^{63} such two-sets $\{s,t\}$, we expect to have reduced the possible choices for R_1 by 50%.

At first, we have 2^{56} choices for R_1, and the attack takes about $2^{63} * 2^{65} * 2 = 2^{120}$ DES-encryptions to reduce the number of choices for R_1 down to 2^{55}. Repeating the attack, we need another 2^{119} DES encryptions to reduce the number of choices down to 2^{54}, another 2^{118} DES encryptions to reduce it to 2^{53}, ..., hence we may pin down R_1 by doing no more than 2^{121} DES encryptions. This leaves open 2^8 choices for K_1.

Now, the complete master key can easily be recovered by exhaustive key search techniques. In the case of DEAL-128, we need $2^{64} * 2^8 = 2^{72}$ trials to find (K_1, K_2). For DEAL-192, we need $2^{64} * 2^{64} * 2^8 = 2^{136}$ trials to recover (K_1, K_2, K_3). Here though, exhaustive key search is not optimal. Since we have found the first round key of a six-round Feistel cipher, recovering the second round key requires a similar attack on a five-round Feistel cipher and hence is even simpler.

Theoretically, this attack is much better than exhaustive key search, and meet-in-the-middle. But due to the huge amount of chosen ciphertexts required, it is quite impractical.

3.2 A Dedicated Attack for DEAL-192

Next, we describe another chosen ciphertext attack. This attack takes more time than the previous one, but only needs $2^{32+\tau}$ chosen ciphertexts (with $0 < \tau \leq 32$) instead of 2^{64}. E.g., for $\tau = 0.5$ the keyspace is reduced by about 50 %.

Recall the last four rounds of six-round DEAL, using the round keys R_3, R_4, R_5, and R_6. The input to the last four rounds is $(x_2, y_2) \in \{0,1\}^{64}$, the output is $(x_6, y_6) \in \{0,1\}^{64}$. Consider two input/output pairs $((x_2, y_2), (x_6, y_6))$ and $((x_2', y_2'), (x_6', y_6'))$ with $y_6 = y_6'$, $x_2 \oplus x_2' = \alpha = x_6 \oplus x_6'$ and $\alpha \neq 0$. (The value $y_2 \oplus y_2'$ may be arbitrary.)

Two such input/output pairs cannot both exist: Since $x_6 \oplus x_6' = \alpha$ and $y_6 = y_6'$, we have $x_5 \oplus x_5' = \alpha = x_4 \oplus x_4'$, and hence $y_4 \oplus y_4' \neq 0$. On the other hand, since $x_2 \oplus x_2' = x_3 \oplus x_3' = \alpha$, and $x_5 \oplus x_5' = \alpha = x_4 \oplus x_4'$, we need $y_3 \oplus y_3' = 0$. This is in contradiction to $y_4 = y_3$ and $y_4' = y_3'$.

As above, we exploit the non-existence of such pairs for key recovery purposes:

- Choose a fixed value $y_6 = y_6' \in \{0,1\}^{64}$ and $2^{32+\tau}$ different values $s \in \{0,1\}^{64}$, which gives $2^{32+\tau}$ different ciphertexts (s, y_6). Consider two such ciphertexts (x_6, y_6) and $(x_6', y_6'))$ with $x_6 \neq x_6'$ and the corresponding plaintexts (x_0, y_0) and (x_0', y_0').
- For all possible 56-bit round keys R, compute $y_1 = y_0 \oplus E_R(x_0)$ and $y_1' = y_0' \oplus E_R(x_0')$.
- For all possible 56-bit round keys S, compute $x_2 = x_1 \oplus E_S(y_1)$, and $x_2' = x_1' \oplus E_S(y_1')$. If
$$x_2 \oplus x_2' = x_6 \oplus x_6',$$
then the key pair (R, S) can be discarded, i.e., $(R_1, R_2) \neq (R, S)$.
If (R, S) is the wrong key pair, we expect "=" to hold with a probability of 2^{-64}. Since we have $2^{32+\tau}$ chosen ciphertexts and thus $\binom{2^{32+\tau}}{2} \approx 2^{2(32+\tau)}/2 \approx 2^{64} * 2^{2\tau-1}$ sets of exactly two ciphertexts, we expect the fraction of the candidates for (R_1, R_2) to be discarded to be roughly $1 - 2^{-2\tau}$, e.g. roughly 50 % for $\tau = 0.5$.

On a first look, the attack seems to require $2^{32+\tau} * 2^{56} * 2^{56} = 2^{144+\tau}$ single encryptions. Actually, if either of the round keys R and S is wrong, we expect to find values x_2, x_2', x_6, and x_6' with

$$x_2 \oplus x_2' = x_6 \oplus x_6',$$

after considering less than 2^{33} plaintext ciphertext pairs, on the average. No more encryption operations (or decryption operations) are needed to reject the pair (R, S) of round keys. Hence, the expected number of single encryptions is below $2^{33} * 2^{112} = 2^{145}$. Since $145 > 128$, this attack is not useful for DEAL-128.

On the other hand, the attack actually is useful for DEAL-192, the DEAL-variant with a key size of 192 bit. Note that the attack only narrows down the number of 192-bit keys from 2^{192} to about $2^{192-2\tau}$, i.e., on the average $8 * 2^{192-2\tau}/2$ additional single DES encryption are needed to find the correct key by brute force.

3.3 The Memory Requirements

For the attack described in Section 3.1, we need to store about 2^{64} plaintexts, each of 128 bit. This requires 2^{71} bits of memory – all other memory requirements are negligible, compared to this.

For the attack described in Section 3.2, the attacker apparently has to store all those about $2^{112-2\tau}$ 56-bit keys for the first two rounds, which are not discarded. The correct 56-bit key pair is not discarded, and can be found by further testing. Given a 56-bit key pair $(R, S) \in (\{0,1\}^{56})^2$, the "further testing" can be done by exhaustively searching $2^{8+8+64} = 2^{80}$ 64-bit key triples corresponding to (R, S) to find the correct one. If all 2^{80} key triples corresponding to the pair (R, S) are wrong, then (R, S) is wrong, too. Instead of storing the pairs (R, S) and later do the "further testing", one may test immediately and save the storage space.

What then dominates the storage space for the attack described in Section 3.2 is the necessity to store $2^{32+\tau}$ plaintexts, i.e., $2^{39+\tau}$ bits. The attack in Section 3.2 improves on the attack in Section 3.1 both with respect to storage space and to the number of chosen ciphertexts.

Table 1 shows the requirements for the attack in Section 3.2, depending on the parameter τ, i.e., the required number of chosen ciphertexts, the approximate number of single DES encryptions, and the approximate number of storage bits.

Table 1. Requirements for the attack from Section 3.2

parameter	chosen ciphertexts	single encryptions	memory
τ	$2^{32+\tau}$	$8 * 2^{191-2\tau} + 2^{145}$	$2^{39+\tau}$ bit
0.5	$2^{32.5}$	$8 * 2^{190}$	$2^{39.5}$ bit
1	2^{33}	$8 * 2^{189}$	2^{40} bit
8	2^{40}	$8 * 2^{175}$	2^{47} bit
16	2^{48}	$8 * 2^{159}$	2^{55} bit
24	2^{56}	$8 * 2^{143} + 2^{145}$	2^{63} bit

3.4 Chosen Plaintext Attacks

The chosen ciphertext attacks we described in Sections 3.1 and 3.2 target on the first round key R_1 or the first two round keys R_1 and R_2. In principle, these attacks do not depend on any key schedule but work well with DEAL-versions with independent round keys. For reasons of symmetry, they can also be run backwards as chosen plaintext attacks, then recovering the last round key or the last two round keys. In fact, the attack described in Section 3.1 can be viewed as the backward version of the chosen plaintext attack on DEAL with independent round keys, described by Knudsen [1]. (The attack in section 3.2 is new, though.)

The reason why we considered chosen ciphertext attacks instead of the possibly more natural chosen plaintext attacks, is the DEAL key schedule. It enables a more simple exploitation of knowing the first or the first two round keys, than knowing the last or the last two ones.

4 Final Remarks

4.1 The Effective Key Size

From a general point of view, the designer of a new cryptosystem should be pessimistic. I.e., when trying to evaluate the effective key size of a cipher, known standard techniques (such as meet in the middle) should be taken into consideration, even if they appear to be very unrealistic. This defines a safety margin, valuable if new and more practical attacks are found.

Thus, we consider the effective key size of DEAL-128 to be 121 bits (or less) and the effective key size of DEAL-256 to be no more than 224 bits. The effective key size of DEAL-192 is 121 bits (or less). In this sense, DEAL-192 does not improve on DEAL-128. If a variant of DEAL is needed faster than DEAL-256 but with an effective key-size of more than 121 bits, a seven-round version of DEAL would be appropriate.

4.2 The DEAL Key Schedule

The DEAL key-schedule is based on using slow but powerful encryption operations. On the other hand, the first round key R_1 does not depend on all (master-)sub-keys K_i (neither does R_2 depend on all sub-keys of DEAL-192 and DEAL-256, neither does R_3 depend on all sub-keys of DEAL-256). Once we have recovered R_1 (and/or R_2, R_3), recovering the complete master key is more easy than necessary. Under ideal circumstances, with randomly chosen keys $K_i \in \{0,1\}^{64}$, independently and according to the uniform probability distribution, this is a minor concern.

But Vaudenay [4] observed the following:

If the choice of the keys K_i is restricted, the attacks described in this paper can be improved. Think of the bytes of the keys K_i being restricted to a set of $c < 2^7$ printable characters. This indicates that there are only c^8 choices for K_i, and c^{24} choices for a DEAL-192 key. Since the number of choices for R_1 is reduced to c^8 instead of 2^{56} the attack in Section 3.1 becomes $2^{56}/c^8$ times faster. (Note that there is no speed-up for corresponding chosen plaintext attack described by Knudsen [1], since the number of choices for R_6 still is 2^{56}.) Similarly, the required number single encryptions for the attack in Section 3.2 is reduced to $8 * c^{24} * 2^{-2\tau} * 2^{-1} + 2^{33} * c^{16}$, instead of $8 * 2^{3*64} * 2^{-2\tau} * 2^{-1} + 2^{33} * 2^{2*56}$.

If we think of, say, $c = 64 = 2^6$, the effective key size of DEAL-192 is reduced to 144 bit. The attack in Section 3.1 would become 2^8 times faster. Depending on τ, the speed-up for the attack in Section 3.2 would be between 2^{16} and 2^{48}.

Also note that if a part of the key is compromised, then the security of DEAL depends on *which part* is compromised. E.g., if 64 bits of a DEAL-192 key are compromised, the remaining security should still be about the security of DEAL-128. Apparently, this is no problem if the 64 bits of K_3 are compromised. But if the attacker knows K_1, she effectively has to attack a five-round variant of DEAL with a 128-bit key, instead of something comparable to six-round DEAL-128.

Our concern regarding the key schedule could easily be fixed, requiring one additional encryption for DEAL-128, two for DEAL-192, and three for DEAL-256, applying the the same general design principle all DEAL key schedules are based on. For DEAL-128, we propose to use $R_2, \ldots, R_7$ as the round keys (and hence throwing away R_1 after running the key schedule), where

$$R_7 := E_{R_*}(K_1 \oplus R_6 \oplus \underline{5}),$$

where $\underline{5}$ is a constant different from $000\ldots0$, $\underline{1}$, $\underline{2}$, $\underline{3}$, and $\underline{4}$. Similar modifications for DEAL-192 and DEAL-256 are obvious.

Note that the additional encryption operations require only between 1/6 and 3/8 of the time for the original key schedule, hence the slow-down for the above modification should be acceptable.

4.3 Conclusions and Open Problem

In spite of these concerns, DEAL is a simple but useful way of constructing a new block cipher based on another block cipher E, doubling the block size. There is no limitation to E=DES. One could as well view DEAL as a "mode of operation" of the underlying block cipher E, instead of a block cipher of its own right.

One may reasonably expect DEAL to be significantly more secure than its building block DES. It would be interesting to actually *prove* this, assuming the security of the underlying building block. This has been done before for cryptographic primitives based on other primitives, e.g. for the DES-based 64-bit block cipher DESX [2]. Such a result may seen as a justification of the construction's soundness, though the actual security of the construction also depends on the security of the underlying block cipher.

Acknowledgements

After discussing the DEAL security with me, Rüdiger Weis was perpetually nagging, waiting for the first version of this paper to be finished. I also thank Don Coppersmith for suggesting an improvement of the attack in Section 3.2 and Richard Outerbridge for discussing the key schedule. I appreciate the comments from the members of the program committee and their help in improving this presentation.

References

1. L. Knudsen: "DEAL – a 128-bit Block Cipher", February 21, 1998, revised May 15, 1998: `http://www.ii.uib.no/~larsr/aes.html`.
2. J. Kilian, P. Rogaway: "How to Protect DES Against Exhaustive Key Search", Neal Koblitz (ed.), Advances in Cryptology: Crypto '96, Springer LNCS 1109, 252–267, full version online:
`http://wwwcsif.cs.ucdavis.edu/~rogaway/papers/list.html`.
3. P. van Oorschot, M. Wiener, "Improving Implementable Meet-in-the-Middle Attacks by Orders of Magnitude", Crypto '96 Springer LNCS 1109, 229–236.
4. S. Vaudenay, "On Comparing the Security of Block Ciphers", manuscript, 1998.