Key-dependent S-boxes, Differential Cryptanalysis, and Twofish

Extended Abstract

Abstract. Key-dependent S-boxes have recently gained prominence as a component in block cipher design. In this paper we make some observations on how the cryptanalyst might work with key-dependent S-boxes, we begin to develop a framework for the differential cryptanalysis of key-dependent S-boxes, and we introduce some basic techniques that were used in an analysis of reduced-round Twofish.

1 Introduction

Since the publication of DES [7] it has become widely accepted that carefully designed S-boxes can be a very effective security mechanism. Key-dependent S-boxes are a development of this idea and have gained considerable attention as a major component in Twofish [9], one of the finalists for the Advanced Encryption Standard. Previous work on this topic includes the block cipher Blowfish [8] and the work of Vaudenay [10].

Since key-dependent S-boxes change from encryption to encryption, off-line analysis of an attack under the action of one particular set of S-boxes is unlikely to be much help since a completely different set of S-boxes might be used. Thus, intuitively, it seems that key-dependent S-boxes must make life much more difficult for the cryptanalyst. How can one even start when one does not know the details of the encryption mechanism? The purpose of this paper is to query whether this intuition is necessarily correct. In fact, at an abstract level, we observe that the notion of S-boxes that change from encryption to encryption can be quite useful to an attacker. We sum up the approach in this paper as follows:

> *Instead of choosing the attack to fit the S-box, we choose the S-box to fit the attack.*

2 Differential cryptanalysis and Twofish

For the rest of this paper we will need a basic understanding of differential cryptanalysis and the structure of Twofish.

2.1 Differential cryptanalysis

Differential cryptanalysis is a very powerful cryptanalytic tool. Devised by Biham and Shamir [1], the expected evolution in the difference between two plaintexts is used to derive information about the encryption key. Off-line analysis is used

to identify particularly useful pairs of inputs. These pairs differ by some chosen amount, where the notion of difference can be adapted to suit the cipher under attack. Then, as the inputs are encrypted from round to round, the difference in the intermediate data during these two parallel encryptions can be predicted according to some probability. The expected evolution of the difference is called a *characteristic*. There are many sophisticated variants on differential cryptanalysis, but provided the number of pairs that follow the characteristic, so-called *right pairs*, can be identified as being in some sense unusual, then information about the encryption key used in the last round can typically be deduced.

The most important information for the attacker is the probability that a given difference in the output from a characteristic appears when the specified input difference has been used. A characteristic specifies one particular evolution of differences through the cipher. However there may well be others that would yield the same output difference. A *differential* [6] is used to capture this notion. The probability of the differential—which is what the cryptanalyst will use—can be significantly higher than the probability of one of the constituent characteristics.

This brief overview shows why key-dependent S-boxes might be considered a strong design feature. Since the S-boxes used during encryption are not known ahead of time, it should be difficult to predict how the differences between two plaintext inputs will evolve during encryption.

2.2 Twofish and key-dependent S-boxes

The round function in Twofish is illustrated in Figure 1. It consists of many different components; some fixed rotations, a *Pseudo-Hadamard Transform (PHT)* which is the transformation $(X, Y) \rightarrow (X+Y, X+2Y)$, an MDS matrix denoted by M, and four key-dependent S-boxes.

Throughout this paper we will only consider the version of Twofish with 128-bit encryption keys, though similar results will apply to other key lengths. When the 128-bit key version is considered, the the final S-boxes are defined using two bytes of user-defined key material in each S-box. (See [9] for more details.) Thus we can search each S-box exhaustively for certain types of differential behaviour and this will provide the basis for our empirical evidence.

Currently the best attack on Twofish is thought to be one that uses impossible differentials that only applies to six rounds of the 256-bit version of the cipher and requires a work effort of 2^{256} steps [3].

3 General differential model of the S-boxes in Twofish

In this section we provide a model for the differential behaviour of an S-box of the type used in Twofish. Note that it is easy to generalise this approach to S-Boxes of different sizes.

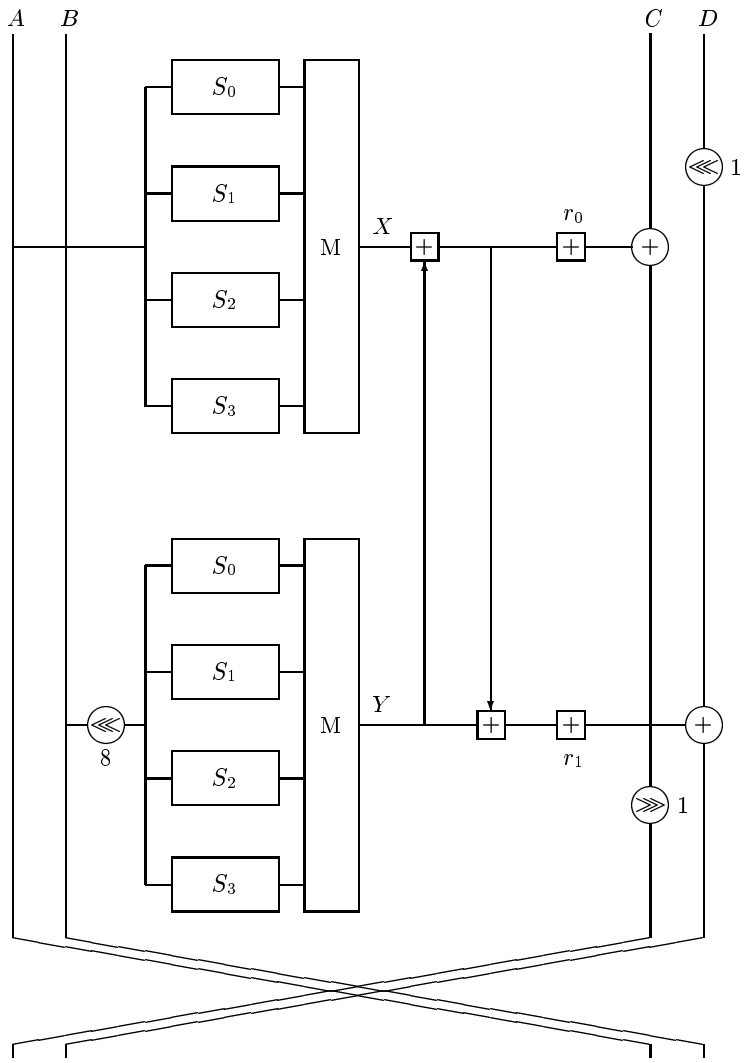

Fig. 1. One round of Twofish. The two additive subkeys used are labeled r_0 and r_1.

3.1 A single differential for an S-Box

Let $S_{\mathbf{k}} : \mathbf{Z}_2^8 \to \mathbf{Z}_2^8$ be a Twofish S-box defined by a Twofish S-box (16-bit) subkey $\mathbf{k}$. The differential count for $S_{\mathbf{k}}$ for input difference a and output difference b $(a \to b)$ is defined by

$$N_{\mathbf{k}}(a,b) = \#\{x \in \mathbf{Z}_2^8 | S_{\mathbf{k}}(x) \oplus S_{\mathbf{k}}(x \oplus a) \oplus b = 0\} \quad [a,b \in \mathbf{Z}_2^8].$$

The probability of the differential $a \to b$ is given by $2^{-8}N_{\mathbf{k}}(a,b)$. Clearly, $N_{\mathbf{k}}(a,0) = N_{\mathbf{k}}(0,b) = 0$ for $a, b \neq 0$ with $N_{\mathbf{k}}(0,0) = 2^8$. We consider $N_{\mathbf{k}}(a,b)$ when $a, b \neq 0$.

Consider the quotient space $U_a = \mathbf{Z}_2^8/\{0,a\}$, and define $W_x \in U_a$ to be the coset $\{x, x \oplus a\}$. We can now define $F : U_a \to \mathbf{Z}_2^8$ by

$$F(W_x) = S_{\mathbf{k}}(x) \oplus S_{\mathbf{k}}(x \oplus a) \oplus b.$$

It is reasonable to regard F as a random function mapping uniformly into an 8-bit space, so the indicator function I_{W_x} for the event $F(W_x) = 0$ takes the value 1 with probability 2^{-8} and 0 with probability $1 - 2^{-8}$. Furthermore, to a very good approximation, I_{W_x} are independent random variables. Thus, summing over all 2^7 elements of U_a, we obtain

$$\sum_{W_x \in U_a} I_{W_x} \sim Bin(2^7, 2^{-8}) \approx Poi(1/2).$$

However, $N_{\mathbf{k}}(a,b) = 2\sum_{W_x \in U_a} I_{W_x}$. Thus, if X is a $2 \cdot Poi(1/2)$ random variable, so

$$P(X = 2n) = \frac{e^{-\frac{1}{2}}\frac{1}{2}^n}{n!}, \qquad P(X = 2n+1) = 0, \qquad [n \geq 0],$$

then $N_{\mathbf{k}}(a,b)$ has approximately the same distribution as X.

We have seen that for a fixed S-Box subkey $\mathbf{k}$, $N_{\mathbf{k}}(a,b)$ takes the value $2n$ with probability $P(X = 2n)$. However, we can regard $N_{\mathbf{k}}(a,b)$ and $N_{\mathbf{k}'}(a,b)$ as independent for $\mathbf{k} \neq \mathbf{k}'$. Thus, equivalently, we can say that $N_{\mathbf{k}}(a,b)$ takes the value $2n$ for a proportion of $P(X = 2n)$ of the 2^{16} S-Box subkeys $\mathbf{k}$. Probabilities for X are tabulated in the appendix. They are in very close agreement with simulated distributions for $N_{\mathbf{k}}(a,b)$.

3.2 Multiple differentials for the same S-Box

To conduct a differential cryptanalysis of Twofish, we require a number of differentials $a_1 \to b_1, \cdots, a_l \to b_l$ to hold across an S-Box with the same S-Box subkey k. As $N_{\mathbf{k}}(a_i, b_i)$ are essentially independent, the total count for all these differentials simultaneously is given by

$$M_{\mathbf{k}}(\mathbf{a}, \mathbf{b}) = \prod_{i=1}^{l} N_{\mathbf{k}}(a_i, b_i).$$

If $X_1, \cdots, X_l$ are independent $2 \cdot Poi(1/2)$ random variables (as discussed above), then $M_{\mathbf{k}}(\mathbf{a}, \mathbf{b})$ has approximately the same distribution as $Y_l = \prod_{i=1}^{l} X_i$. Note that Y_l is 2^l times the product of l independent $Poi(1/2)$ random variables. As above, we can say that $M_{\mathbf{k}}(\mathbf{a}, \mathbf{b})$ takes the value $2^l n$ for a proportion of $P(Y_l = 2^l n)$ of the 2^{16} Twofish S-Box subkeys $\mathbf{k}$. We note that this argument generalises to any number of S-Box keys. Probabilities for Y_l $(l = 2, \cdots, 4)$ are tabulated below, and are in very close agreement with simulated distributions for $M_{\mathbf{k}}(\mathbf{a}, \mathbf{b})$. It is interesting to note that these distributions have many modes

(ie. they do not decay monotonically). This is because the distributions are a product of a discrete (non-negative integer-valued) distribution. This multimodal property could have implications when constructing an analysis of such block ciphers.

In analysing Twofish, we may use exactly the same differential across the same S-Box simultaneously. Thus we may require the differential $a_{l-1} \rightarrow b_{l-1}$ to hold *twice* simultaneously with the differentials $a_1 \rightarrow b_1, \cdots, a_{l-2} \rightarrow b_{l-2}$ across an S-Box with the same S-Box subkey k. This distribution is different from that described above and is given by

$$M^*_{\mathbf{k}}(\mathbf{a}, \mathbf{b}) = N^2_{\mathbf{k}}(a_{l-1}, b_{l-1}) \prod_{i=1}^{l-2} N_{\mathbf{k}}(a_i, b_i).$$

As above, if $X_1, \cdots, X_{l-1}$ are independent $2 \cdot Poi(1/2)$ random variables (as discussed above), then $M^*_{\mathbf{k}}(\mathbf{a}, \mathbf{b})$ has approximately the same distribution as $Y^*_l = X^2_l \prod_{i=1}^{l-2} X_i$. Note that Y^*_l is 2^l times the product of $(l-2)$ independent $Poi(1/2)$ random variables and an independent squared $Poi(1/2)$ random variables. The values of Y^*_l are tabulated below for $l = 2, \cdots, 5$. It is interesting to note the discrepancy between Y_l and Y^*_l. For example, the former distribution has expected value 1 and the latter 3. The latter distribution offers greater assistance to the cryptanalyst.

The tables in the Appendix represent a first step to devising tools to analyse the Twofish key-dependent S-Boxes. In obtaining the theoretical bounds for differential probabilities, these tables have been used in a crude manner by "thresholding" differential probabilities for S-Boxes. It is obviously possible to adopt more sophisticated and accurate techniques using these tables.

4 Specific characteristics constructed for Twofish

Here we present a selection of characteristics for Twofish. Throughout, our approach was to fit the characteristic around the different components of Twofish while essentially ignoring the action of the S-boxes. We chose the form of the characteristic across the PHT in a round of Twofish, and then mapped this back through the inverse of the MDS matrix, M. Provided the same S-boxes were active and inactive on the input and output to the S-box transformation, the actual values of the input and output difference were immaterial. We anticipated that there would be some key, or hopefully a sizeable class of keys, that would provide the required differential behaviour required across the S-boxes.

4.1 A five-round characteristic

The difference in each 32-bit input word is represented in hexadecimal notation. Full account is taken of all details in Twofish, including the fixed rotations. The two words to the left in each row are the input differences to the two sets of S-boxes (with the second word being rotated by eight bit positions). The associated probabilities will be discussed in the following sections.

A	B		C	D
80000000	00000000		A0E080A0	AF8FBFAF
		↓		
00000000	FFFFFFFF		80000000	00000000
		↓		
00000000	00000000		00000000	FFFFFFFF
		↓		
00000000	FFFFFFFF		00000000	00000000
		↓		
40000000	00000000		00000000	FFFFFFFF
		↓		
50704050	5F1F7F5F		40000000	00000000

Table 1. A five-round characteristic for Twofish. We will refer to this characteristic as *Characteristic 1*.

The evolution of *Characteristic 1* over the third round is clear and holds with probability one. The other rounds are outlined here.

Rounds 2 and 4. The observation that we rely on is the following. Consider the two 32-bit input words to the PHT transformation, say (X, Y). The output from the PHT is then $(X + Y, X + 2Y)$. If we set a difference in (X, Y) to be (00000000, 80000000) then the difference in the output of the PHT will be (80000000, 00000000) with probability one. This difference will also propagate across the additive subkeys that follow, with probability one.

Our aim then is to ensure that the difference in the output from the second MDS matrix is 80000000. It is straightforward to use the inverse of the MDS matrix to give the input difference 8CA32FA3. We notice that all four S-boxes need to be active (a property due to the form of the MDS matrix) yet since the S-boxes are key-dependent we do not know which input differences to consider. However, we can use the property of key-dependent S-boxes to our advantage. In reality it does not matter which input difference we use (provided it is non-zero) since there will be some key values that will provide an S-box giving us the characteristic we want, and quite possibly with a reasonable probability.

Since the input form of the difference to the S-boxes does not matter, we will choose one that is convenient to us. By choosing FFFFFFFF we have a difference that is invariant across the single-bit and eight-bit rotations. We further note that the Hamming weight of differences on the input side of the S-boxes is immaterial since they are not involved in any integer addition operations.

In summary, to make characteristics of the form described we have a condition for each S-box; namely that FF $\rightarrow$ A3, FF $\rightarrow$ 2F, FF $\rightarrow$ A3, and FF $\rightarrow$ 8C for S-

boxes 0 through 3 respectively.

Round 1. The input to the round function is of the form (80000000, 00000000). This means that there will be one active S-box and due to the MDS matrix there will be four active output bytes. Since we can rely on the key-dependent S-boxes to give us any output difference from the S-box that we like, we can search over all 255 possible non-zero input differences into the MDS matrix to find a useful output. We choose an output that gives a good probability p that the characteristic $(\Delta, 0) \rightarrow (\Delta, \Delta)$ holds over the PHT and integer additions. By choosing $\Delta =$ A0E080A0 we accomplish this with p determined experimentally to be 2^{-14} when averaged over random texts and random additive round keys. For $\Delta =$ A0E080A0 the input difference to the MDS is 80000000 and so we merely require the characteristic 80 $\rightarrow$ 80 to hold across S-box 3 with non-zero probability in addition to satisfying any other S-box conditions from other rounds.

Round 5. Along similar lines to Round 1, we now need the additional difference 40 $\rightarrow$ 80 to hold across S-box 3.

All rounds. To derive the five-round differential described we have three conditions on the evolution of a characteristic across S-box 3 (with one repeated), and one condition (repeated twice) across S-boxes 0, 1, and 2.

Experimentally we derived the following results for the S-boxes alone, by searching (experimentally) over individual S-boxes, and then combining the results. We will consider the fuller implications in potential attacks on Twofish in Section 5. For a fraction of (at least) 2^{-40} of the S-boxes, *Characteristic 1* in Table 1 holds with an estimated probability greater than 2^{-53} (maximum 2^{-50}) across the S-boxes alone. There is obviously a trade-off between the probability of the characteristic across the S-boxes and the number of keys (S-boxes) for which the characteristic will give the stated probability or higher. For this particular case, if we are willing to let the probability of the characteristic across the S-boxes drop from 2^{-53} to 2^{-60}, then experiments suggest the characteristic will hold for more than 2^{-20} of the key space. The tables derived in Section 3 give us the theoretical estimates quoted here. Different trade-offs for the theoretical estimates will be explored in the final paper.

	probability	*proportion of key space*
experimental	$> 2^{-53}$	$> 2^{-40}$
experimental	$> 2^{-60}$	$> 2^{-20}$
theoretical estimate	$> 2^{-61}$	$> 2^{-21}$

4.2 Another five-round characteristic

In Figure 2 we show another five-round characteristic for Twofish. It has a different evolution to *Characteristic 1* and is of some independent interest.

A	B		C	D
00000000	00000000		00100038	0E000400
		↓		
0008001C	1C000800		00000000	00000000
		↓		
00000000	70101060		0008001C	1C000800
		↓		
0044004E	39001100		00000000	70101060
		↓		
00000000	00000000		0044004E	39001100
		↓		
00220027	72002200		00000000	00000000

Fig. 2. A second five-round characteristic for Twofish. We will refer to this as *Characteristic 2*.

The evolution of *Characteristic 2* over the first and fifth rounds is clear and holds with probability one. Now it is the intervening rounds that are not that obvious.

Round 2. Due to the fixed rotations the same inputs will be used to the same S-boxes in round two. This helps reduce the conditions that might be needed on the S-boxes. One choice was to derive the same output from both instances of the MDS matrix; in this case 70101060. There may well be other choices that would be better. (There are at least fifteen easily identified choices that would be useful in similar ways.) Mapping this word back through the inverse of the MDS gives 008000C0. Thus we have our first set of conditions on the S-boxes; 1C $\rightarrow$ C0 for S-box 0 and 08 $\rightarrow$ 80 for S-box 2. Note that this characteristic is applied twice to the two active active S-boxes in this round. The output from both MDS matrices is 70101060 by construction and by experimentation the differential (70101060, 70101060) $\rightarrow$ (00000000, 70101060) holds with probability 2^{-14} on average when computed over random texts and random additive round keys.

Round 3. The input to the round function is of the form (00000000 70101060). Four S-boxes in this round will be active, and four inactive. Once again we start from the output from the MDS matrices. Clearly one MDS has to give the output 00000000. We choose the second to have the output 00800080. This choice is particularly interesting because we can use the PHT to our advantage. In order to keep the probability of the characteristic high we aim to keep the number of active S-boxes in the next round low. Yet when we consider the right-hand side of the input difference to this round (0008001C AC000800) we

see that it will be difficult to get an output from the MDS matrix that does not increase the number of active S-boxes in the following round. However across the PHT the characteristic (00000000, 00800080) $\rightarrow$ (00800080, 01000100) holds (experimentally) with average probability 2^{-4} across random texts and random additive round keys. This satisfies our requirements. Mapping 00800080 back through the inverse of the MDS matrix gives us C2A3B33F and so we now have another set of conditions on the S-boxes. Namely; 70 $\rightarrow$ 3F, 60 $\rightarrow$ B3, 10 $\rightarrow$ A3, 10 $\rightarrow$ C2 for S-boxes 0, 1, 2, and 3 respectively.

Round 4. For this round we work backwards. We aim to cancel out the difference on the right of the input to the round. To do this, while taking account of the fixed rotation by one bit position, we need to get as output from the PHT a difference of the form (00000000, E02020C0). This can be accomplished, with probability 2^{-12}, on average, by taking the input to the PHT of the form (E02020C0, E02020C0). If we map E02020C0 back through the inverse of the MDS matrix we get 006900E9. What is nice about this is that exactly S-boxes 0 and 2 need to be active on the output, and these are exactly the S-boxes active on the input. In short we have the conditions 4E $\rightarrow$ E9 and 39 $\rightarrow$ E9 for S-box 0 and for S-box 2 we have 44 $\rightarrow$ 69 and 11 $\rightarrow$ 69.

All rounds. To get this five-round characteristic[1] we have four different conditions on the evolution of a differential across S-boxes 0 and 2, with one of the conditions repeated twice. There is one condition across S-boxes 1 and 3.

The techniques (experimental and theoretical) used to obtain estimates for this characteristic are as described for the previous characteristic. Again, we will use Section 5 to consider the fuller implications. For a fraction of (at least) 2^{-42} of the S-boxes this characteristic holds with an estimated probability of between 2^{-63} and 2^{-70}. Again there is a trade-off between the probability of the characteristic across the S-boxes and the number of keys for which the characteristic will give the stated probability or higher. For this particular case, if we are willing to let the probability of the characteristic across the S-boxes drop from 2^{-70} to 2^{-80}, then experiments suggest that the characteristic will hold for more than 2^{-27} of the key space. Different trade-offs for the theoretical estimates will be explored in the final paper.

	probability	*proportion of key space*
experimental	$> 2^{-63}$	$> 2^{-42}$
experimental	$> 2^{-80}$	$> 2^{-27}$
theoretical estimate	$> 2^{-74}$	$> 2^{-38}$

[1] The starting values to round 2, 002C000C and its rotation, were chosen to increase the probability across the S-boxes. Many other choices for the bytes 2C and 0C would have sufficed. Some may lead to much larger classes of keys, even though the maximum probability might be somewhat reduced. There are many different ways of finding such characteristics for Twofish due to the flexibility that key-dependent S-boxes offer the attacker.

4.3 Six-round characteristics for Twofish

The five-round characteristics in Sections 4.1 and 4.2 can be extended to six-round characteristics in the obvious way. In principle these should lead directly to attacks on seven-round of Twofish. In particular, if we were to extend *Characteristic 2* by one extra round we would add an extra condition (twice) to S-box 2, and two additional conditions to S-box 0. However a less obvious approach might also be of some interest.

Consider adding another round to *Characteristic 1*. We see that all eight S-boxes in the following round are going to be active. This would traditionally be viewed as a major problem since either a great many more conditions will be added to those we already have (so the fraction of applicable S-boxes will drop) or the probability of the combined characteristics propagating across the S-boxes will drop.

Instead we observe that having four active bytes going into the MDS allows us to have one active byte coming out, and we can choose that byte to have Hamming weight 1. Thus, we can choose 1024 possible sets of output from the pair of MDS matrices that will have a combined Hamming weight of 2. The hope is that the light differences will not propagate too much across the PHT and the additive subkeys, and that the very light weight of what will therefore become the left side of the text—denoted here by `U` and `V`—will provide sufficient distinguishing information to launch an attack. The six-round characteristic would then have the form shown in Figure 3 where `U` and `V` will have low Hamming weight.

Details

Here we describe in some detail what happens in round six and some of the associated probabilities. Denote the output from the two MDS matrices as (X, Y). All we require is that X and Y have Hamming weight one. We can map both X and Y back through the MDS matrix using its inverse and this gives us a set of output differences from the two sets of four S-boxes. We know the input differences since they are inherited from the previous round. Therefore we have 1024 sets of possible differences across the S-boxes that will be useful.

It turns out that for a fraction of (at least) 2^{-20} of the S-boxes, the characteristic as described over six rounds (leading to X and Y each of weight one) holds with estimated probability between 2^{-72} and 2^{-85} for the S-boxes alone. In deriving these biases the computation involved characteristics in the first five rounds. By considering differentials improvements can be expected. We also need to account for the probability of crossing two active sets of PHT and the additive subkeys in the first five rounds, and we already know that this takes place with probability 2^{-28} on average. The final step is to account for (X, Y) as these words pass through the PHT and the additive subkeys. On average, the two words that result will have a combined Hamming weight of 9 or less 82% of the time, by experiment. These words are then exclusive-ored with `40000000` and `00000000` and potentially rotated by one bit position.

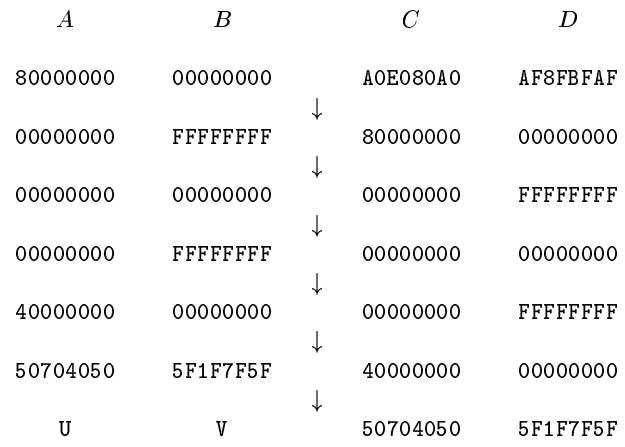

Fig. 3. A six-round characteristic for Twofish where `U` and `V` have "low" Hamming weight. Constructions like this demonstrate some of the additional flexibility available to an attacker. We call this *Characteristic 3*.

Clearly there is considerable structure in the output from this six-round characteristic, particularly since the difference on the right-hand side is fully defined over 64-bit bits. It is an open question whether such a technique is useful to a cryptanalyst.

5 Attacks on reduced-round Twofish

So far we have only considered the behaviour of characteristics across the S-boxes of Twofish. To develop attacks on Twofish we would need to take account of the other features in a round of Twofish.

Since we are using exclusive-or as our notion of difference, the PHT and the use of the additive subkeys will have a significant impact on the probability of our characteristic. We performed experiments to obtain an average behaviour of the characteristics as they passed across the PHT and the key addition. Note that the drop in the probability of the characteristic is not that great. This is because we were able to choose the detailed specification of the characteristic to suit our needs. We then relied on the S-boxes to link together the two halves of the characteristic once we knew the input to, and the output from, a single round of Twofish. The additional effect of these other aspects of Twofish are summarised in Table 2.

On discovering a characteristic for r rounds of a cipher it is typically prudent to assume that a key-recovery attack on $r + 2$ rounds of the cipher will follow. This may, or may not, actually be the case and needs additional work which will

characteristic	*S-box probability*	*other contributions*	*overall probability*	*fraction of key space*
1	$> 2^{-53}$	2^{-28}	$> 2^{-81}$	$> 2^{-40}$
1	$> 2^{-60}$	2^{-28}	$> 2^{-88}$	$> 2^{-20}$
2	$> 2^{-63}$	2^{-30}	$> 2^{-91}$	$> 2^{-42}$
2	$> 2^{-80}$	2^{-30}	$> 2^{-110}$	$> 2^{-27}$
3	$> 2^{-85}$	2^{-28}, 0.82	$> 2^{-113}$	$> 2^{-20}$

Table 2. A summary of the expected probability of the five- and six-round characteristics that we have identified. The additional drop in the probability listed under "other contributions" is due to the action of the PHT and the additive round keys and the values given in this table are average values that were derived experimentally.

be described in the full paper. We note that the characteristics in this note were constructed in a very rudimentary fashion. More sophisticated techniques should yield improved results. We believe it is likely that much improved characteristics, either in terms of probability, or in terms of the fraction of the key space to which they apply, can be derived. Further, the extent of any differential effect is very important and we have not yet begun to quantify this. Certainly it seems possible that six-round and even seven-round characteristics and differentials along the lines described in this note could be identified. This gives good evidence to support our belief that eight rounds of Twofish can be compromised. Of course, this would not be in any practical sense, but within the allowable data requirements of the AES.

Finally, we note that the existence of characteristics that apply to only a fraction of the key space, leads directly to what might be termed *weak keys*. This idea, and any potential link with the phenomenon of key separation [5] will be explored in the final paper.

6 Conclusions

In this paper we have questioned the intuition that key-dependent S-boxes are likely to offer improved security over well-designed fixed S-boxes. We describe some preliminary work on the AES finalist Twofish and present 5- and 6-round characteristics which clearly demonstrate that the current best exist attack on Twofish can be improved. We have also presented good evidence that, within the parameters of the AES, it could be possible to compromise an eight-round version of Twofish.

It seems that the use of key-dependent S-boxes can potentially improve the range of options available to the attacker. While we have concentrated on the application of differential cryptanalysis in our work. It is an open question whether other techniques will also gain from the approach we have adopted.

References

1. E. Biham and A. Shamir. Differential cryptanalysis of the data encryption standard. Springer Verlag, 1993.
2. N. Ferguson. Upper bounds on differential characteristics in Twofish. Counterpane Systems. August 17, 1998.
3. N. Ferguson. Impossible differentials in Twofish. Counterpane Systems. October 19, 1999.
4. J. Kelsey. Key separation in Twofish. Counterpane Systems. April 7, 2000.
5. F. Mirza and S. Murphy. An observation on the key schedule of Twofish. Proceedings of 2nd AES Candidate Conference, Rome, pages 151-154, March 1999.
6. X. Lai, J. Massey, and S. Murphy. Markov ciphers and differential cryptanalysis. In D.W. Davies, editor, Advances in Cryptology, Eurocrypt '91, LNCS 547, pages 17-38, Springer Verlag, 1992.
7. National Bureau of Standards. The data encryption standard, FIPS 46, January 1977.
8. B. Schneier. Description of a new variable-length key, 64-bit block cipher (Blowfish). In, R. Anderson editor, Proceedings of FSE 1, LNCS 809, pages 191-204, 1994.
9. B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, and N. Ferguson. Twofish: A 128-bit Block Cipher. 15 June, 1998.
10. S. Vaudenay. On the weak keys of Blowfish. In, D. Gollmann editor, Proceedings of FSE 3, LNCS 1039, pages 27-32, 1996.

Appendix

Single Differential
Double Poisson
Parameter $\frac{1}{2}$

Differential Count	Differential Probability	Proportion of Subkeys	Expected No of 2^{16} Subkeys	Cumulative Proportion Subkeys	Cumulative No of 2^{16} Subkeys
0	$0 \cdot 2^{-7}$	0.606531	39749	1.000000	65536
2	$1 \cdot 2^{-7}$	0.303265	19874	0.393469	25786
4	$2 \cdot 2^{-7}$	0.075816	4968	0.090204	5911
6	$3 \cdot 2^{-7}$	0.012636	828	0.014388	942
8	$4 \cdot 2^{-7}$	0.001580	103	0.001752	114
10	$5 \cdot 2^{-7}$	0.000158	10	0.000172	11
12	$6 \cdot 2^{-7}$	0.000013	0	0.000014	0
14	$7 \cdot 2^{-7}$	0.000001	0	0.000001	0
16	$8 \cdot 2^{-7}$	0.000000	0	0.000000	0

2 Differentials
2-fold Double Poisson Product
Parameter $\frac{1}{2}$

Differential Count	Differential Probability	Proportion of Subkeys	Expected No of 2^{16} Subkeys	Cumulative Proportion Subkeys	Cumulative No of 2^{16} Subkeys
0	$0 \cdot 2^{-14}$	0.845182	55389	1.000000	65536
4	$1 \cdot 2^{-14}$	0.091970	6027	0.154818	10146
8	$2 \cdot 2^{-14}$	0.045985	3013	0.062848	4118
12	$3 \cdot 2^{-14}$	0.007664	502	0.016863	1105
16	$4 \cdot 2^{-14}$	0.006706	439	0.009199	602
20	$5 \cdot 2^{-14}$	0.000096	6	0.002493	163
24	$6 \cdot 2^{-14}$	0.001924	126	0.002397	157
28	$7 \cdot 2^{-14}$	0.000001	0	0.000473	31
32	$8 \cdot 2^{-14}$	0.000240	15	0.000473	30
36	$9 \cdot 2^{-14}$	0.000160	10	0.000233	15
40	$10 \cdot 2^{-14}$	0.000024	1	0.000074	4
44	$11 \cdot 2^{-14}$	0.000000	0	0.000050	3
48	$12 \cdot 2^{-14}$	0.000042	2	0.000050	3
52	$13 \cdot 2^{-14}$	0.000000	0	0.000008	0
56	$14 \cdot 2^{-14}$	0.000000	0	0.000008	0
60	$15 \cdot 2^{-14}$	0.000004	0	0.000008	0
64	$16 \cdot 2^{-14}$	0.000002	0	0.000004	0

3 Differentials
3-fold Double Poisson Product
Parameter $\frac{1}{2}$

Differential Count	Differential Probability	Proportion of Subkeys	Expected No of 2^{16} Subkeys	Cumulative Proportion Subkeys	Cumulative No of 2^{16} Subkeys
0	$0 \cdot 2^{-21}$	0.939084	61543	1.000000	65536
8	$1 \cdot 2^{-21}$	0.027891	1827	0.060916	3992
16	$2 \cdot 2^{-21}$	0.020918	1370	0.033025	2164
24	$3 \cdot 2^{-21}$	0.003486	228	0.012107	793
32	$4 \cdot 2^{-21}$	0.005665	371	0.008620	564
40	$5 \cdot 2^{-21}$	0.000044	2	0.002955	193
48	$6 \cdot 2^{-21}$	0.001747	114	0.002911	190
56	$7 \cdot 2^{-21}$	0.000000	0	0.001164	76
64	$8 \cdot 2^{-21}$	0.000654	42	0.001164	76
72	$9 \cdot 2^{-21}$	0.000145	9	0.000510	33
80	$10 \cdot 2^{-21}$	0.000022	1	0.000365	23
88	$11 \cdot 2^{-21}$	0.000000	0	0.000343	22
96	$12 \cdot 2^{-21}$	0.000256	16	0.000343	22
104	$13 \cdot 2^{-21}$	0.000000	0	0.000087	5
112	$14 \cdot 2^{-21}$	0.000000	0	0.000087	5
120	$15 \cdot 2^{-21}$	0.000004	0	0.000087	5
128	$16 \cdot 2^{-21}$	0.000030	1	0.000084	5
136	$17 \cdot 2^{-21}$	0.000000	0	0.000054	3
144	$18 \cdot 2^{-21}$	0.000037	2	0.000054	3
152	$19 \cdot 2^{-21}$	0.000000	0	0.000017	1
160	$20 \cdot 2^{-21}$	0.000003	0	0.000017	1
168	$21 \cdot 2^{-21}$	0.000000	0	0.000014	0
176	$22 \cdot 2^{-21}$	0.000000	0	0.000014	0
184	$23 \cdot 2^{-21}$	0.000000	0	0.000014	0
192	$24 \cdot 2^{-21}$	0.000009	0	0.000014	0
200	$25 \cdot 2^{-21}$	0.000000	0	0.000005	0
208	$26 \cdot 2^{-21}$	0.000000	0	0.000005	0
216	$27 \cdot 2^{-21}$	0.000002	0	0.000005	0
224	$28 \cdot 2^{-21}$	0.000000	0	0.000003	0
232	$29 \cdot 2^{-21}$	0.000000	0	0.000003	0
240	$30 \cdot 2^{-21}$	0.000001	0	0.000003	0
248	$31 \cdot 2^{-21}$	0.000000	0	0.000002	0
256	$32 \cdot 2^{-21}$	0.000001	0	0.000002	0
264	$33 \cdot 2^{-21}$	0.000000	0	0.000001	0
272	$34 \cdot 2^{-21}$	0.000000	0	0.000001	0
280	$35 \cdot 2^{-21}$	0.000000	0	0.000001	0
288	$36 \cdot 2^{-21}$	0.000001	0	0.000001	0

4 Differentials
4-fold Double Poisson Product
Parameter $\frac{1}{2}$

Differential Count	Differential Probability	Proportion of Subkeys	Expected No of 2^{16} Subkeys	Cumulative Proportion Subkeys	Cumulative No of 2^{16} Subkeys
0	$0 \cdot 2^{-28}$	0.976031	63965	1.000000	65536
16	$1 \cdot 2^{-28}$	0.008458	554	0.023969	1570
32	$2 \cdot 2^{-28}$	0.008458	554	0.015510	1016
48	$3 \cdot 2^{-28}$	0.001410	92	0.007052	462
64	$4 \cdot 2^{-28}$	0.003348	219	0.005642	369
80	$5 \cdot 2^{-28}$	0.000018	1	0.002294	150
96	$6 \cdot 2^{-28}$	0.001059	69	0.002276	149
112	$7 \cdot 2^{-28}$	0.000000	0	0.001218	79
128	$8 \cdot 2^{-28}$	0.000661	43	0.001218	79
144	$9 \cdot 2^{-28}$	0.000088	5	0.000557	36
160	$10 \cdot 2^{-28}$	0.000013	0	0.000469	30
176	$11 \cdot 2^{-28}$	0.000000	0	0.000455	29
192	$12 \cdot 2^{-28}$	0.000287	18	0.000455	29
208	$13 \cdot 2^{-28}$	0.000000	0	0.000168	11
224	$14 \cdot 2^{-28}$	0.000000	0	0.000168	11
240	$15 \cdot 2^{-28}$	0.000002	0	0.000168	11
256	$16 \cdot 2^{-28}$	0.000067	4	0.000166	10
272	$17 \cdot 2^{-28}$	0.000000	0	0.000098	6
288	$18 \cdot 2^{-28}$	0.000044	2	0.000098	6
304	$19 \cdot 2^{-28}$	0.000000	0	0.000054	3
320	$20 \cdot 2^{-28}$	0.000004	0	0.000054	3
336	$21 \cdot 2^{-28}$	0.000000	0	0.000050	3
352	$22 \cdot 2^{-28}$	0.000000	0	0.000050	3
368	$23 \cdot 2^{-28}$	0.000000	0	0.000050	3
384	$24 \cdot 2^{-28}$	0.000033	2	0.000050	3
400	$25 \cdot 2^{-28}$	0.000000	0	0.000017	1
416	$26 \cdot 2^{-28}$	0.000000	0	0.000017	1
432	$27 \cdot 2^{-28}$	0.000002	0	0.000017	1
448	$28 \cdot 2^{-28}$	0.000000	0	0.000015	0
464	$29 \cdot 2^{-28}$	0.000000	0	0.000015	0
480	$30 \cdot 2^{-28}$	0.000001	0	0.000015	0
496	$31 \cdot 2^{-28}$	0.000000	0	0.000014	0
512	$32 \cdot 2^{-28}$	0.000003	0	0.000014	0
528	$33 \cdot 2^{-28}$	0.000000	0	0.000010	0
544	$34 \cdot 2^{-28}$	0.000000	0	0.000010	0
560	$35 \cdot 2^{-28}$	0.000000	0	0.000010	0
576	$36 \cdot 2^{-28}$	0.000007	0	0.000010	0

2 Differentials (One Repeated)
Squared Double Poison Product
Parameter $\frac{1}{2}$

Differential Count	Differential Probability	Proportion of Subkeys	Expected No of 2^{16} Subkeys	Cumulative Proportion Subkeys	Cumulative No of 2^{16} Subkeys
0	$0 \cdot 2^{-14}$	0.606531	39749	1.000000	65536
4	$1 \cdot 2^{-14}$	0.303265	19874	0.393469	25786
8	$2 \cdot 2^{-14}$	0.000000	0	0.090204	5911
12	$3 \cdot 2^{-14}$	0.000000	0	0.090204	5911
16	$4 \cdot 2^{-14}$	0.075816	4968	0.090204	5911
20	$5 \cdot 2^{-14}$	0.000000	0	0.014388	942
24	$6 \cdot 2^{-14}$	0.000000	0	0.014388	942
28	$7 \cdot 2^{-14}$	0.000000	0	0.014388	942
32	$8 \cdot 2^{-14}$	0.000000	0	0.014388	942
36	$9 \cdot 2^{-14}$	0.012636	828	0.014388	942
40	$10 \cdot 2^{-14}$	0.000000	0	0.001752	114
44	$11 \cdot 2^{-14}$	0.000000	0	0.001752	114
48	$12 \cdot 2^{-14}$	0.000000	0	0.001752	114
52	$13 \cdot 2^{-14}$	0.000000	0	0.001752	114
56	$14 \cdot 2^{-14}$	0.000000	0	0.001752	114
60	$15 \cdot 2^{-14}$	0.000000	0	0.001752	114
64	$16 \cdot 2^{-14}$	0.001580	103	0.001752	114
68	$17 \cdot 2^{-14}$	0.000000	0	0.000172	11
72	$18 \cdot 2^{-14}$	0.000000	0	0.000172	11
76	$19 \cdot 2^{-14}$	0.000000	0	0.000172	11
80	$20 \cdot 2^{-14}$	0.000000	0	0.000172	11
84	$21 \cdot 2^{-14}$	0.000000	0	0.000172	11
88	$22 \cdot 2^{-14}$	0.000000	0	0.000172	11
92	$23 \cdot 2^{-14}$	0.000000	0	0.000172	11
96	$24 \cdot 2^{-14}$	0.000000	0	0.000172	11
100	$25 \cdot 2^{-14}$	0.000158	10	0.000172	11
104	$26 \cdot 2^{-14}$	0.000000	0	0.000014	0
108	$27 \cdot 2^{-14}$	0.000000	0	0.000014	0
112	$28 \cdot 2^{-14}$	0.000000	0	0.000014	0
116	$29 \cdot 2^{-14}$	0.000000	0	0.000014	0
120	$30 \cdot 2^{-14}$	0.000000	0	0.000014	0
124	$31 \cdot 2^{-14}$	0.000000	0	0.000014	0
128	$32 \cdot 2^{-14}$	0.000000	0	0.000014	0
132	$33 \cdot 2^{-14}$	0.000000	0	0.000014	0
136	$34 \cdot 2^{-14}$	0.000000	0	0.000014	0
140	$35 \cdot 2^{-14}$	0.000000	0	0.000014	0
144	$36 \cdot 2^{-14}$	0.000013	0	0.000014	0

3 Differentials (Including One Repeated)
Double Poisson and Squared Double Poison Product
Parameter $\frac{1}{2}$

Differential Count	Differential Probability	Proportion of Subkeys	Expected No of 2^{16} Subkeys	Cumulative Proportion Subkeys	Cumulative No of 2^{16} Subkeys
0	$0 \cdot 2^{-21}$	0.845182	55389	1.000000	65536
8	$1 \cdot 2^{-21}$	0.091970	6027	0.154818	10146
16	$2 \cdot 2^{-21}$	0.022992	1506	0.062848	4118
24	$3 \cdot 2^{-21}$	0.003832	251	0.039856	2611
32	$4 \cdot 2^{-21}$	0.023471	1538	0.036024	2360
40	$5 \cdot 2^{-21}$	0.000048	3	0.012552	822
48	$6 \cdot 2^{-21}$	0.000004	0	0.012504	819
56	$7 \cdot 2^{-21}$	0.000000	0	0.012500	819
64	$8 \cdot 2^{-21}$	0.005748	376	0.012500	819
72	$9 \cdot 2^{-21}$	0.003832	251	0.006752	442
80	$10 \cdot 2^{-21}$	0.000000	0	0.002920	191
88	$11 \cdot 2^{-21}$	0.000000	0	0.002920	191
96	$12 \cdot 2^{-21}$	0.000958	62	0.002920	191
104	$13 \cdot 2^{-21}$	0.000000	0	0.001962	128
112	$14 \cdot 2^{-21}$	0.000000	0	0.001962	128
120	$15 \cdot 2^{-21}$	0.000000	0	0.001962	128
128	$16 \cdot 2^{-21}$	0.000599	39	0.001962	128
136	$17 \cdot 2^{-21}$	0.000000	0	0.001363	89
144	$18 \cdot 2^{-21}$	0.000958	62	0.001363	89
152	$19 \cdot 2^{-21}$	0.000000	0	0.000405	26
160	$20 \cdot 2^{-21}$	0.000012	0	0.000405	26
168	$21 \cdot 2^{-21}$	0.000000	0	0.000393	25
176	$22 \cdot 2^{-21}$	0.000000	0	0.000393	25
184	$23 \cdot 2^{-21}$	0.000000	0	0.000393	25
192	$24 \cdot 2^{-21}$	0.000001	0	0.000393	25
200	$25 \cdot 2^{-21}$	0.000048	3	0.000392	25
208	$26 \cdot 2^{-21}$	0.000000	0	0.000344	22
216	$27 \cdot 2^{-21}$	0.000160	10	0.000344	22
224	$28 \cdot 2^{-21}$	0.000000	0	0.000185	12
232	$29 \cdot 2^{-21}$	0.000000	0	0.000185	12
240	$30 \cdot 2^{-21}$	0.000000	0	0.000185	12
248	$31 \cdot 2^{-21}$	0.000000	0	0.000185	12
256	$32 \cdot 2^{-21}$	0.000120	7	0.000185	12
264	$33 \cdot 2^{-21}$	0.000000	0	0.000065	4
272	$34 \cdot 2^{-21}$	0.000000	0	0.000065	4
280	$35 \cdot 2^{-21}$	0.000000	0	0.000065	4
288	$36 \cdot 2^{-21}$	0.000024	1	0.000065	4

4 Differentials (Including One Repeated)
2-fold Double Poisson and Squared Double Poison Product
Parameter $\frac{1}{2}$

Differential Count	Differential Probability	Proportion of Subkeys	Expected No of 2^{16} Subkeys	Cumulative Proportion Subkeys	Cumulative No of 2^{16} Subkeys
0	$0 \cdot 2^{-28}$	0.939081	61543	1.000000	65536
16	$1 \cdot 2^{-28}$	0.027891	1827	0.060919	3992
32	$2 \cdot 2^{-28}$	0.013946	913	0.033027	2164
48	$3 \cdot 2^{-28}$	0.002324	152	0.019082	1250
64	$4 \cdot 2^{-28}$	0.009007	590	0.016757	1098
80	$5 \cdot 2^{-28}$	0.000029	1	0.007751	507
96	$6 \cdot 2^{-28}$	0.000583	38	0.007722	506
112	$7 \cdot 2^{-28}$	0.000000	0	0.007138	467
128	$8 \cdot 2^{-28}$	0.003559	233	0.007138	467
144	$9 \cdot 2^{-28}$	0.001211	79	0.003579	234
160	$10 \cdot 2^{-28}$	0.000007	0	0.002369	155
176	$11 \cdot 2^{-28}$	0.000000	0	0.002361	154
192	$12 \cdot 2^{-28}$	0.000594	38	0.002361	154
208	$13 \cdot 2^{-28}$	0.000000	0	0.001768	115
224	$14 \cdot 2^{-28}$	0.000000	0	0.001768	115
240	$15 \cdot 2^{-28}$	0.000001	0	0.001768	115
256	$16 \cdot 2^{-28}$	0.000654	42	0.001766	115
272	$17 \cdot 2^{-28}$	0.000000	0	0.001112	72
288	$18 \cdot 2^{-28}$	0.000581	38	0.001112	72
304	$19 \cdot 2^{-28}$	0.000000	0	0.000531	34
320	$20 \cdot 2^{-28}$	0.000007	0	0.000531	34
336	$21 \cdot 2^{-28}$	0.000000	0	0.000523	34
352	$22 \cdot 2^{-28}$	0.000000	0	0.000523	34
368	$23 \cdot 2^{-28}$	0.000000	0	0.000523	34
384	$24 \cdot 2^{-28}$	0.000146	9	0.000523	34
400	$25 \cdot 2^{-28}$	0.000015	0	0.000377	24
416	$26 \cdot 2^{-28}$	0.000000	0	0.000363	23
432	$27 \cdot 2^{-28}$	0.000097	6	0.000363	23
448	$28 \cdot 2^{-28}$	0.000000	0	0.000266	17
464	$29 \cdot 2^{-28}$	0.000000	0	0.000266	17
480	$30 \cdot 2^{-28}$	0.000000	0	0.000266	17
496	$31 \cdot 2^{-28}$	0.000000	0	0.000266	17
512	$32 \cdot 2^{-28}$	0.000091	5	0.000266	17
528	$33 \cdot 2^{-28}$	0.000000	0	0.000175	11
544	$34 \cdot 2^{-28}$	0.000000	0	0.000175	11
560	$35 \cdot 2^{-28}$	0.000000	0	0.000175	11
576	$36 \cdot 2^{-28}$	0.000098	6	0.000175	11

5 Differentials (Including One Repeated)
3-fold Double Poisson and Squared Double Poison Product
Parameter $\frac{1}{2}$

Differential Count	Differential Probability	Proportion of Subkeys	Expected No of 2^{16} Subkeys	Cumulative Proportion Subkeys	Cumulative No of 2^{16} Subkeys
0	$0 \cdot 2^{-35}$	0.976021	63964	1.000000	65536
32	$1 \cdot 2^{-35}$	0.008458	554	0.023979	1571
64	$2 \cdot 2^{-35}$	0.006344	415	0.015521	1017
96	$3 \cdot 2^{-35}$	0.001057	69	0.009177	601
128	$4 \cdot 2^{-35}$	0.003833	251	0.008120	532
160	$5 \cdot 2^{-35}$	0.000013	0	0.004287	280
192	$6 \cdot 2^{-35}$	0.000530	34	0.004274	280
224	$7 \cdot 2^{-35}$	0.000000	0	0.003744	245
256	$8 \cdot 2^{-35}$	0.001784	116	0.003744	245
288	$9 \cdot 2^{-35}$	0.000396	25	0.001960	128
320	$10 \cdot 2^{-35}$	0.000007	0	0.001563	102
352	$11 \cdot 2^{-35}$	0.000000	0	0.001557	102
384	$12 \cdot 2^{-35}$	0.000342	22	0.001557	102
416	$13 \cdot 2^{-35}$	0.000000	0	0.001215	79
448	$14 \cdot 2^{-35}$	0.000000	0	0.001215	79
480	$15 \cdot 2^{-35}$	0.000001	0	0.001215	79
512	$16 \cdot 2^{-35}$	0.000483	31	0.001214	79
544	$17 \cdot 2^{-35}$	0.000000	0	0.000731	47
576	$18 \cdot 2^{-35}$	0.000275	18	0.000731	47
608	$19 \cdot 2^{-35}$	0.000000	0	0.000456	29
640	$20 \cdot 2^{-35}$	0.000004	0	0.000456	29
672	$21 \cdot 2^{-35}$	0.000000	0	0.000451	29
704	$22 \cdot 2^{-35}$	0.000000	0	0.000451	29
736	$23 \cdot 2^{-35}$	0.000000	0	0.000451	29
768	$24 \cdot 2^{-35}$	0.000135	8	0.000451	29
800	$25 \cdot 2^{-35}$	0.000004	0	0.000316	20
832	$26 \cdot 2^{-35}$	0.000000	0	0.000312	20
864	$27 \cdot 2^{-35}$	0.000045	2	0.000312	20
896	$28 \cdot 2^{-35}$	0.000000	0	0.000267	17
928	$29 \cdot 2^{-35}$	0.000000	0	0.000267	17
960	$30 \cdot 2^{-35}$	0.000000	0	0.000267	17
992	$31 \cdot 2^{-35}$	0.000000	0	0.000267	17
1024	$32 \cdot 2^{-35}$	0.000083	5	0.000267	17
1056	$33 \cdot 2^{-35}$	0.000000	0	0.000184	12
1088	$34 \cdot 2^{-35}$	0.000000	0	0.000184	12
1120	$35 \cdot 2^{-35}$	0.000000	0	0.000184	12
1152	$36 \cdot 2^{-35}$	0.000083	5	0.000184	12

This article was processed using the LaTeX macro package with LLNCS style