A Differential Boomerang Attack Against 7-round Rijndael

Abbas Ghaemi Bafghi Babak Sadeghiyan

GhaemiB@ce.aut.ac.ir BaSadegh@ce.aut.ac.ir

Data Security Laboratory, Computer Engineering Department

Amirkabir University of Technology,Tehran , Iran , P.O.Box 15875-4413

Abstract. In this paper, we report on our design of a choosen plaintext attack with work factor 2^{252} to recover of the first and the last subkeys of a 7-round Rijndael, while differential cryptanalysis against Rijndael have been done for up to 6 rounds and reported in published papers. We found a 5-round boomerang characteristic for Rijndael, and designed a choosen plaintext attack based on this characteristic ,with work factor 2^{249} to recover the 32 bits of the 1^{st} round subkey and the 32 bits of the 7^{th} round subkey. We also designed some simmilar attacks to recover other bits of subkeys of the first round and the last round. Therefore the work factor of this choosen plaintext attack to recover all bits of the first and the last subkeys of a 7-round Rijndael will be 2^{252}, that is less than exhaustive search. It meanes that a 7-round Rijndael will be compromised with differential boomerang cryptanalysis.

Key words: Cryptography, Block Cipher, Differential Cryptanalysis, Differential Model, Rijndael, and Ant Colony Technique.

1. Introduction

Differential cryptanalysis of block ciphers was proposed by Biham and Shamir[2]. This method of cryptanalysis is done in two phases, which we call design and execution of attack. In the design phase, a cryptanalyser finds weaknesses of a cipher algorithm and applies them to find an appropriate differential characteristic for that cipher. In the execution phase, he must gather enough ciphertext pairs with the found characteristic and then identifies the effective bits of the key according to a counting scheme. These phases can be summarized as the following steps:

I. **Design of attack**

   1. Build the difference distribution table of S-boxes.
   2. Compute the probability of all possible one-round characteristics.
   3. Examine all combinations of one-round characteristics to find a suitable full-round characteristic.

II. **Execution of attack**

   1. Gather enough ciphertext pairs with the found characteristic.
   2. Identify effective bits of the key.

For an interested reader, we would like to elaborate that the bottleneck of the design phase is the step 3, i.e., examining all combinations of the one-round characteristics to find the best full-round characteristic. In [7], we described forward-backward method and applied dynamic programming and backtracking technique to used it to find suitable differential characteristics for Serpent. Although we managed to obtain suitable result, but one spend much time on it, as the examination of all combinations of one-round characteristics is a time consuming task. Then, in [8] we presented a model for finding suitable differential characteristics with applying intelligent techniques through forward-backward method. That model represents the problem of finding the best differential characteristic for a block cipher algorithm as the problem of finding the shortest path in a directed graph. Then, we applied ant-colony technique [6] for finding the shortest path in the directed graph. In this way, we reached two advantages. Firstly, by applying this technique, one can obtain a suitable result without examining the whole search space. Secondly, intelligent techniques such as ant-colony technique may reduce dependency of cryptanalysis from cryptanalyser.

Rijndael is a block cipher, which is selected as the Advanced Encryption Standard[1]. Differential cryptanalysis against Rijndael have been done for up to 6 rounds in [5], [3] and [4]. We found 8 5-round boomerang characteristics for Rijndael, and we designed a choosen plaintext attack based on these 5-round boomerang characteristics to recover of the first and the last subkeys of a 7-round Rijndael. The work factor of this attack is 2^{252}, that is less than exhustive search.

The remainder of this paper organized as follows: In section 2, we give a brief description of Rijndael(AES). In section 3, we review the boomerang attack. In section 4, we present our found characteristic and designed attack for a 7-round Rijndael. The last section is the conclusion of paper.

2. The description of Rijndael

Rijndael is a block cipher which is selected as the AES[1]. The AES requirements state that the length of the key can be specified to be 128, 192 or 256 bits while the length of the block is 128 bits. The designers of Rijndael cipher also allow the length of the block to be 128, 192 or 256 bits, independently of the length of the key. In this paper we deal with the variant in which the lengths of both are 256 bit. In this case the cipher consists of 14 rounds. The intermediate state is arranged in a 4×8 matrix of bytes. Every round except for the last consists of the following transformations:

1. **Byte Substitution:** This transformation is applied to each byte separately. Each byte is considered as representing coefficients of a polynomial of degree less than 8 over Z^2 (i.e., elements of $GF(2^8)$). The inverse of this polynomial modulo $(x^8 + x^4 + x^3 + x + 1)$ is calculated, the result is multiplied by a fixed

matrix and is added to a fixed polynomial. This transformation is the only non-linear transformation in the cipher.

2. **Shift:** The first row of the matrix remains constant, the second row is shifted one byte to the right, the third row is shifted three bytes to the right, and the last row is shifted four bytes to the right.
3. **Mix Column:** Each column of the matrix is considered as a polynomial of degree less than 4 over $GF(2^8)$ and this polynomial is multiplid by the polynomial $03_x.x^3+01_x.x^2+01_x.x+02_x$ (where a_x denotes hexadecimal value) modulo $(x^4 + 1)$. This transformation is linear.
4. **Add Round Key:** A 256-bit round key, which is derived from the key by the Key Expansion algorithm, is bytewise Xored to the state.

In the last round the MixColumn transformation is omitted and before the first round an Add Round Key transformation is performed, using the key itself as a round key.

The round key of each round is derived from the key using the Key Expansion algorithm. Each round key is of length 256 bit and by the design knowing a round key of any round is enough to recover the key. Let us denote the bytes of the expanded key by $K_0,K_1,K_2, \ldots$, where the key is $K_0,K_1, \ldots,K_{15}$. Then the expanded key is derived from the following formula:

$$K_n = \begin{cases} K_{n-1} \oplus K_{n-16} & \text{if } 16 \nmid n \\ K_{n-16} \oplus \text{ByteSubstitution}(\text{Shifted } K_{n-1}) \oplus \text{Rcon} & \text{othewise} \end{cases}$$

3. The boomerang attack

The boomerang attack is a differential attack that attempts to generate a quartet structure at an intermediate value halfway through the cipher[9]. The attack considers four plaintexts I1, I2, I'1, and I'2 along with their respective ciphertexts O1, O2, O'1 and O'2. Let E(.) represents the encryption operation, and decompose the cipher into E = E1oE0, where E0 represents the first half of the cipher and E1 represents the last half. We will use a differential characteristic for E0, say $\Delta \rightarrow \Delta^*$, as well as a differential characteristic for $E1^{-1}$ as $\nabla \rightarrow \nabla^*$.

We want to cover the pair (I1,I2) with the characteristic $\Delta \rightarrow \Delta^*$ for E0, and to cover the pairs (I1,I'1) and (I2,I'2) with the characteristic $\nabla \rightarrow \nabla^*$ for $E1^{-1}$. Then the pair (I'1,I'2) is perfectly set up to use the characteristic $\Delta \rightarrow \Delta^*$ for $E0^{-1}$ (figure 1). We define a right quartet as one where all four characteristics hold simultaneously.

Let's examine why this is so. Consider the intermediate value after half of the rounds. When the previous three characteristics hold, we have

$$\begin{aligned} E0(I'1) \oplus E0(I'2) &= E0(I1) \oplus E0(I2) \oplus E0(I1) \oplus E0(I'1) \oplus E0(I2) \oplus E0(I'2) \\ &= E0(I1) \oplus E0(I2) \oplus E1^{-1}(O1) \oplus E1^{-1}(O2) \oplus E1^{-1}(O'1) \oplus E1^{-1}(O'2) \\ &= \Delta^* \oplus \nabla^* \oplus \nabla^* = \Delta^*. \end{aligned}$$

Note that this is exactly the condition required to start the characteristic $\Delta \rightarrow \Delta^*$ for the inverse of the first half of the cipher. When this characteristic also holds, we will have the same difference in the plaintexts I'1 and I'2 as found in the original plaintexts I1 and I2. This is why it is called the boomerang attack: when you send it properly, it always comes back to you.

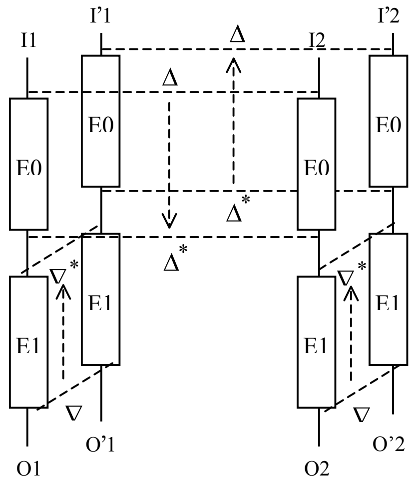

Figure1. A schematic of the basic boomerang attack.

The same attack works even if we do not predict the exact value of $\nabla *$ ahead of time, but instead merely require that the difference after decrypting by E1 is the same in the two pairs (I1,I'1) and (I2,I'2). A similar observation also holds for $\Delta *$. Therefore, we may sum over all values for $\Delta *$ and $\nabla *$ to obtain the probability of boomerang characterisitic as follows:

$$\Pr \approx \sum_{\Delta *} \Pr(\Delta \rightarrow \Delta * \text{ by E0})^2 \times \sum_{\nabla *} \Pr\left(\nabla \rightarrow \nabla * \text{ by } \mathrm{E1}^{-1}\right)^2$$

4. Design the boomerang attack against 7-round Rijndael

Differential cryptanalysis against Rijndael have been done for up to 6 rounds and is reported in [5], [3], and [4]. We found a two-round differential characteristic with probability of 2^{-30}, as shown in tabel 1, and a three-round differential characteristic with probability of 2^{-126}, as shown in tabel 2. Each row of these tables contains three columns. The first column gives the round number, the secound column gives the input difference or the output difference of the round substitution transformation, and the last column gives the probability of the one-round differential characteristic. Note that the input difference of each round is obtained by applying the shift and mix-column transformations to the output difference of the previous round.

We designed a boomerang attack based on these chararceristics for five round of Rijndael. If we call the first two rounds of this five rounds E0 and the final three rounds E1, the five-round Rijndael is E=E0oE1. Let

Tabel 1 : Two-round differential Characteristic for Rajndael

Round #	Differential Characteristic		Probability
1	Output	72000000004B000000000000000000020000000E2000000000000000000000000	
2	Input	D900000000000000000000000000000000000000000000000000000000000000	2^{-6}
	Output	5600000000000000000000000000000000000000000000000000000000000000	
3	Input	AC5656FA00000000000000000000000000000000000000000000000000000000	2^{-24}
	Output	F2D2D24E00000000000000000000000000000000000000000000000000000000	

Tabel 2 : Three-round differential Characteristic for Rajndael

Round #	Differential Characteristic		Probability
4	Input	A80000E7F2CB000000080000AE00E400ABACE7A6006800BE00005000000055CC	2^{-96}
	Output	A10000F7EA7C00000053000087000A0001F2F747002600CD0000300000009F28	
5	Input	9000000000830000000000000000006D000000004F000000000000000000000000	2^{-24}
	Output	030000000008F00000000000000005F00000000E7000000000000000000000000	
6	Input	3400000000000000000000000000000000000000000000000000000000000000	2^{-6}
	Output	7B00000000000000000000000000000000000000000000000000000000000000	
7	Input	F67B7B8D0000000000000000000000000000000000000000000000000000000	

$Input_i$ and $Output_i$ represent the input and output of i^{th} round , respectively. We use $Input_2 \rightarrow Output_3$ as our differential characteristice for E0 and $Output_6 \rightarrow Input_4$ as our differential characteristice for $E1^{-1}$. The probability of this five-round boomerang characteristic is $\left(2^{-30}\right)^2 \times \left(2^{-126}\right)^2 = 2^{-312}$.

As we mentioned earlier, we can design a similar characteristic even if we do not predict the exact values of $Output_3$ and $Input_4$. Therefore we may sum over all values for $Output_3$ and $Input_4$ in two-round characteristices of $Input_2 \rightarrow Output_3$ and in three-round characteristices of $Output_6 \rightarrow Input_4$ respectively. The number of active Sboxes in these characteristices is 5 and 21 respectively. According to the differential distribution table of the Sbox of Rijndael, the probability of each active Sbox is 2^{-6} and 2^{-7} in 1 and 127 cases respectively. The probability of five-round boomerang characteristic is calculated as follows:

$$\Pr = \sum_{i=0}^{5} \binom{5}{i} \times 127^{i} \times \left(\left(\frac{1}{2}\right)^{7\times i} \times \left(\frac{1}{2}\right)^{6\times(5-i)} \right)^2 \times \sum_{i=0}^{21} \binom{21}{i} \times 127^{i} \times \left(\left(\frac{1}{2}\right)^{7\times i} \times \left(\frac{1}{2}\right)^{6\times(21-i)} \right)^2 \cong 2^{-34.83} \times 2^{-146.30} \cong 2^{-182}$$

We extended above five-round boomerang characteristice to a seven-round attack to recover the 32 bits of the1^{st} round subkey and the 32 bits of the 7^{th} round subkey corresponding to the 4 active Sboxes of $Input_2$ and $Input_7$ respectively. This attack can be done in following steps(figure 2):

1- Set a counter corresponding to each of the probable values of the 32 bits of the 1^{st} round subkey and the 32 bits of the 7^{th} round subkey of Rijndael and initialize it by zero.

2- Gather enough pairs with difference of $Input_2$, denote such a pair as (I1,I2). Do step 3 to step 10 for each pair.

3- Apply the inverse of the first round for each of the pairs by employing all probable values of the 32 bits of 1^{st} round subkey to determine the bits of the pairs that are corresponding to the active sboxes, and determine the other bits of the pairs randomly. Denote such a resulted pair as (P1,P2).

4- Apply 7-round Rinjndael cipher to each of paintext pairs to obtain ciphertext pairs, Denote such a ciphertext pair as (C1,C2).

5- Peel off the last round for each of the ciphertext pairs corresponging to each of the probable values of the 128-bit subkey, Denote such a resulted pair as (O1,O2).

6- Compute $O'i = Oi \oplus \nabla$ for i=1,2, where $\nabla = Input_7$.

7- Re-encrypt the last round with the guessed 32-bit last round subkey, Denote such a resulted pair as (C'1,C'2).

8- Apply 7-round Rinjndael decipher to resulted pair, Denote such a resulted pair as (I'1,I'2).

9- Re-encrypt the first round with the guessed 32-bit first round subkey to obtain boomerang pairs, Denote such a boomerang pair as (Q1,Q2).

10- If deffernce of boomerang pair is equal $Input_2$ increase the counter corresponding to guessed subkeys.

11- The subkey corresponding to counter with maximum value is the right subkey.

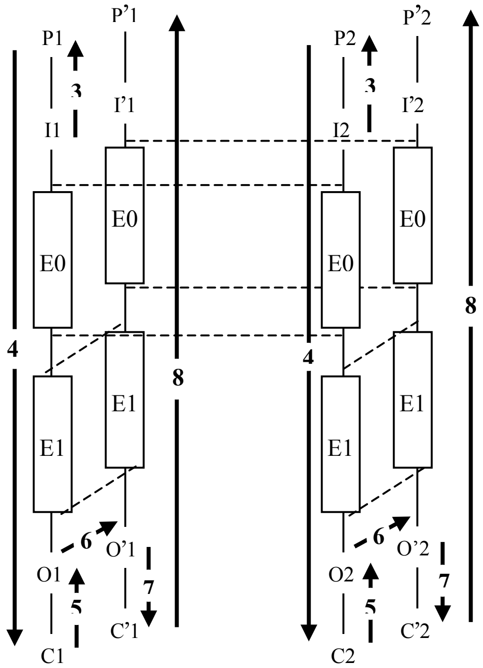

Fig 2. The schematic of a Boomerang attck for 7-round Rijndael.

The bold edges show the steps of the attack as above algorithm, where the label of each edge gives the step number.

We can identify all but approximately 2^{-228} of our boomerang pairs are wrong pairs, because their defferences of (I'1,I'2) can not be correspond to our desired difference $Input_2$. The signal to noise is calculated as follows:

$S/N=Pr\times2^{K}/\alpha\times\beta=2^{-182}\times2^{64}/1\times2^{-228}=2^{110}$

Therefore only 3 or 4 right pairs are required, then we need $4\times2^{182}=2^{184}$ pairs with our desired difference $Input_2$ in step 1 of above algorithm. The work factor is calculated as follows:

$WF= 2\times2^{184}\times2^{64}=2^{249}$

We found 7 other 5-round boomerang characteristics with probqability of 2^{-182} as shown in Appendix 1. We designed 7 attacks baseed on these characteristics similar to the above attack, such that each recover 32 bits of the first subkey and 32 bits of the last subkey in a 7-round Rijndael, while the work factor of each attack is 2^{249}. Therefor the work factor of attack to recover the first and the last subkeys of a 7-round Rijndael is 2^{252}.

5. Conclusion

In this paper we found a 5-round boomerang characteristic ,and designed a choosen plaintext attack based on this 5-round boomerang characteristic ,with work factor of 2^{249} to recover 32 bits of the first round subkey and 32 bits of the last round subkey of a 7-round Rijndael. Then we found 7 other 5-round boomerang characteristics with probqability of 2^{-182} that one can design 7 similar attacks to recover other bits of these subkeys. The work factor of this attack will be 2^{252}, that is less than exhaustive search. It meanes that 7-round Rijndael will be compromised with differential boomerang cryptanalysis.

References

[1] The Advanced Encryption Standard, http://csrc.nist.gov/encryption/aes/.

[2] E. Biham, A. Shamir, ”Differential Cryptanalysis of the Data Encryption Standard”, Springer-Verlag, 1993.

[3] E. Biham, N. Kellery, “Cryptanalysis of Reduced Variants of Rijndael”, http://csrc.nist.gov/encryption/aes/round2/conf3/papers/35-ebiham.pdf.

[4] J.H.Cheon and et.al. “Improved Impossible Differential Cryptanalysis of Rijndael and Crypto”.

[5] J. Daemen, V. Rijmen, “AES proposal: Rijndael”, http://csrc.nist.gov/encryption/aes/rijndael/.

[6] M. Dorigo, G. Di Caro, “Ant Colony Optimization: A New Meta-Heuristic”, IEEE Transactions on Systems, 1999.

[7] A. Ghaemi B., “Differential Cryptanalysis of Serpent”, 7th Annual Computer Society of Iran Computer Conference, I.R.Iran, Tehran, 2002.

[8] A. Ghaemi B. and B. Sadeghyian , “Differential Model of Block Ciphers with Ant Colony Technique”, accepted by Workshop on Coding, Cryptography, and Combinatorics, China, HuangShan, 2003.

[9] D. Wagner, “The Boomerang Attack”, Fast Software Encryption, 6th International Workshop, Springer-Verlag, 1990.

Appendix 1: Seven 5-round boomerang differential characteristics for Rijndael.

We found seven 5-round boomerang differential characteristics, as shown in the following tabels. Each row of these tables contains three columns. The first column gives the round number, the secound column gives the input difference or the output difference of the round substitution transformation, and the last column gives the probability of the one-round differential characteristic.

1.

Round #	Differential Characteristic		Probability
1	Output	0000000072000000004B000000000000000000200000000E2000000000000000	
2	Input	00000000D9000000000000000000000000000000000000000000000000000000	2^{-6}
	Output	0000000056000000000000000000000000000000000000000000000000000000	
3	Input	00000000AC5656FA000000000000000000000000000000000000000000000000	2^{-24}
	Output	00000000F2D2D24E000000000000000000000000000000000000000000000000	
4	Input	000055CCA80000E7F2CB000000080000AE00E400ABACE7A6006800BE00005000	2^{-96}
	Output	00009F28A10000F7EA7C0000005300087000A0001F2F747002600CD00003000	
5	Input	00000000900000000083000000000000000006D000000004F000000000000000	2^{-24}
	Output	0000000003000000008F00000000000000005F00000000E70000000000000000	
6	Input	0000000034000000000000000000000000000000000000000000000000000000	2^{-6}
	Output	000000007B000000000000000000000000000000000000000000000000000000	
7	Input	00000000F67B7B8D000000000000000000000000000000000000000000000000	

2.

Round #	Differential Characteristic		Probability
1	Output	000000000000000072000000004B00000000000000000200000000E200000000	
2	Input	0000000000000000D90000000000000000000000000000000000000000000000	2^{-6}
	Output	0000000000000000560000000000000000000000000000000000000000000000	
3	Input	0000000000000000AC5656FA0000000000000000000000000000000000000000	2^{-24}
	Output	0000000000000000F2D2D24E0000000000000000000000000000000000000000	
4	Input	00005000000055CCA80000E7F2CB000000080000AE00E400ABACE7A6006800BE	2^{-96}
	Output	0000300000009F28A10000F7EA7C00000053000087000A0001F2F747002600CD	
5	Input	000000000000000090000000008300000000000000006D000000004F00000000	2^{-24}
	Output	000000000000000003000000008F00000000000000005F00000000E700000000	
6	Input	0000000000000000340000000000000000000000000000000000000000000000	2^{-6}
	Output	00000000000000007B0000000000000000000000000000000000000000000000	
7	Input	0000000000000000F67B7B8D0000000000000000000000000000000000000000	

3.

Round #	Differential Characteristic		Probability
1	Output	00000000000000000000000072000000004B00000000000000000200000000E2	
2	Input	000000000000000000000000D900000000000000000000000000000000000000	2^{-6}
	Output	0000000000000000000000005600000000000000000000000000000000000000	
3	Input	000000000000000000000000AC5656FA00000000000000000000000000000000	2^{-24}
	Output	000000000000000000000000F2D2D24E00000000000000000000000000000000	
4	Input	006800BE00005000000055CCA80000E7F2CB000000080000AE00E400ABACE7A6	2^{-96}
	Output	002600CD0000300000009F28A10000F7EA7C00000053000087000A0001F2F747	
5	Input	00000000000000000000000090000000008300000000000000006D000000004F	2^{-24}
	Output	00000000000000000000000003000000008F00000000000000005F00000000E7	
6	Input	0000000000000000000000003400000000000000000000000000000000000000	2^{-6}
	Output	0000000000000000000000007B00000000000000000000000000000000000000	
7	Input	000000000000000000000000F67B7B8D00000000000000000000000000000000	

4.

Round #	Differential Characteristic		Probability
1	Output	000000E200000000000000000000000072000000004B00000000000000000200	
2	Input	00000000000000000000000000000000D9000000000000000000000000000000	2^{-6}
	Output	0000000000000000000000000000000056000000000000000000000000000000	
3	Input	00000000000000000000000000000000AC5656FA000000000000000000000000	2^{-24}
	Output	00000000000000000000000000000000F2D2D24E000000000000000000000000	
4	Input	ABACE7A6006800BE00005000000055CCA80000E7F2CB000000080000AE00E400	2^{-96}
	Output	01F2F747002600CD0000300000009F28A10000F7EA7C00000053000087000A00	
5	Input	0000004F00000000000000000000000090000000008300000000000000006D00	2^{-24}
	Output	000000E70000000000000000000000000300000000 8F00000000000000005F00	
6	Input	0000000000000000000000000000000034000000000000000000000000000000	2^{-6}
	Output	000000000000000000000000000000007B000000000000000000000000000000	
7	Input	00000000000000000000000000000000F67B7B8D000000000000000000000000	

5.

Round #	Differential Characteristic		Probability
1	Output	00000200000000E2000000000000000000000000720000000004B000000000000	
2	Input	0000000000000000000000000000000000000000D900000000000000000000000	2^{-6}
	Output	0000000000000000000000000000000000000000560000000000000000000000	
3	Input	0000000000000000000000000000000000000000AC5656FA0000000000000000	2^{-24}
	Output	0000000000000000000000000000000000000000F2D2D24E0000000000000000	
4	Input	AE00E400ABACE7A6006800BE000050000000055CCA80000E7F2CB000000080000	2^{-96}
	Output	87000A0001F2F747002600CD000030000000009F28A10000F7EA7C0000000530000	
5	Input	00006D000000004F0000000000000000000000009000000000830000000000000	2^{-24}
	Output	00005F00000000E70000000000000000000000000300000000008F000000000000	
6	Input	0000000000000000000000000000000000000000340000000000000000000000	2^{-6}
	Output	00000000000000000000000000000000000000007B0000000000000000000000	
7	Input	0000000000000000000000000000000000000000F67B7B8D0000000000000000	

6.

Round #	Differential Characteristic		Probability
1	Output	0000000000000200000000E2000000000000000000000000720000000004B0000	
2	Input	000000000000000000000000000000000000000000000000D900000000000000	2^{-6}
	Output	0000000000000000000000000000000000000000000000005600000000000000	
3	Input	000000000000000000000000000000000000000000000000AC5656FA00000000	2^{-24}
	Output	000000000000000000000000000000000000000000000000F2D2D24E00000000	
4	Input	00080000AE00E400ABACE7A6006800BE000050000000055CCA80000E7F2CB0000	2^{-96}
	Output	0053000087000A0001F2F747002600CD000030000000009F28A10000F7EA7C0000	
5	Input	0000000000006D000000004F000000000000000000000000900000000008300000	2^{-24}
	Output	0000000000005F00000000E700000000000000000000000003000000000 8F0000	
6	Input	0000000000000000000000000000000000000000000000003400000000000000	2^{-6}
	Output	0000000000000000000000000000000000000000000000007B00000000000000	
7	Input	000000000000000000000000000000000000000000000000F67B7B8D00000000	

7.

Round #	Differential Characteristic		Probability
1	Output	004B000000000000000000200000000E2000000000000000000000000072000000	
2	Input	00000000000000000000000000000000000000000000000000000000D9000000	2^{-6}
	Output	0000000000000000000000000000000000000000000000000000000056000000	
3	Input	00000000000000000000000000000000000000000000000000000000AC5656FA	2^{-24}
	Output	00000000000000000000000000000000000000000000000000000000F2D2D24E	
4	Input	F2CB000000080000AE00E400ABACE7A6006800BE000050000000055CCA80000E7	2^{-96}
	Output	EA7C00000000530000087000A0001F2F747002600CD000030000000009F28A10000F7	
5	Input	00830000000000000000006D000000004F0000000000000000000000090000000	2^{-24}
	Output	008F00000000000000005F00000000E7000000000000000000000000003000000	
6	Input	0000000000000000000000000000000000000000000000000000000034000000	2^{-6}
	Output	000000000000000000000000000000000000000000000000000000007B000000	
7	Input	00000000000000000000000000000000000000000000000000000000F67B7B8D	