A New Class of Weak Keys for Blowfish

Orhun Kara and Cevat Manap

TÜBİTAK UEKAE, Gebze, Kocaeli, Turkey
{orhun, cmanap}@uekae.tubitak.gov.tr

Abstract. The reflection attack is a recently discovered self similarity analysis which is usually mounted on ciphers with many fixed points. In this paper, we describe two reflection attacks on r-round Blowfish which is a fast, software oriented encryption algorithm with a variable key length k. The attacks work successfully on approximately $2^{k+32-16r}$ number of keys which we call *reflectively weak keys*. We give an almost precise characterization of these keys. One interesting result is that 2^{34} known plaintexts are enough to determine if the unknown key is a reflectively weak key, for any key length and any number of rounds. Once a reflectively weak key is identified, a large amount of subkey information is revealed with no cost. Then, we recover the key in roughly $r \cdot 2^{16r+22}$ steps. Furthermore, it is possible to improve the attack for some key lengths by using memory to store all reflectively weak keys in a table in advance. The pre-computation phase costs roughly $r \cdot 2^{k-11}$ steps. Then the unknown key can be recovered in $2^{(k+32-16r)/64}$ steps. As an independent result, we improve Vaudenay's analysis on Blowfish for reflectively weak keys. Moreover, we propose a new success criterion for an attack working on some subset of the key space when the key generator is random.

Keywords: Blowfish, cryptanalysis, reflection attack, fixed point, key dependent S-Box, self similarity analysis, weak key.

1 Introduction

Self similarity attacks, such as slide attack [4, 5], related key attack [2], and a very recently discovered attack, reflection attack [10], generally work on ciphers with very simple key schedules. In this paper, we propose reflection attacks on full-round Blowfish which has a very complicated key schedule.

Blowfish is a widely used, unpatented, license-free, fast block cipher designed by Schneier in 1994 [16]. Blowfish is a 16-round Feistel network and uses a large number of subkeys. Security of the algorithm is particularly based on the key dependent S-boxes and the difficulty of recovering the key from a partial knowledge of some subkeys. No attacks have been published on a full version of Blowfish so far. Nevertheless, there have been a few studies on cryptanalysis of Blowfish. The analysis by Rijmen [14] is a second order differential attack against 4-round Blowfish. Another differential cryptanalysis is by Vaudenay [18] and uses $3 \cdot 2^{51}$ chosen plaintexts with the assumption that the round function

F is known and weak in the sense that some of its S-boxes are not one to one. The number of the keys producing the weak F functions is approximately 2^{k-15}. The slide attack by Biryukov and Wagner [4] uses only 2^{27} chosen plaintexts and works under the powerful assumption that all the P subkeys are equal to zero which happens with a probability of roughly 2^{-576}.

1.1 Our Contributions and Organization of the Paper

The notion of fixed points of weak DES keys is well known[9, 6, 12, 13][1]. These works focus on algebraic properties of DES permutations and their short cycles. In this paper, we also exploit permutations with many fixed points. However, we aim to identify weak keys and recover these keys in Blowfish.

We give two new models of description of Blowfish and deduce some reflection properties of Blowfish by utilizing these models. In particular, we show that certain keys produce $(r-2)$-round Blowfish encryption function with many fixed points. We call these keys as *reflectively weak keys*. The number of reflectively weak keys is approximately $2^{k+32-16r}$. We propose two reflection attacks on Blowfish with variable number of rounds. These attacks work on reflectively weak keys.

We identify a reflectively weak key using roughly 2^{34} known plaintexts for any number of rounds and any key length. Moreover, we characterize a reflectively weak key by certain equalities among its subkeys. The characterization is not precise, but it is true with a probability almost 1. Theorem 1 states the characterization in detail. The first attack is a guess-and-determine type attack utilizing this characterization. First, we determine whether the unknown key is a reflectively weak key. Once a reflectively weak key is identified, we obtain a large amount of subkey information with no cost. This information leads to a guess-and-determine attack. The time complexity of the attack is roughly $r \cdot 2^{16r+22}$ steps where each step is equal to one step of exhaustive search. In the second attack, we improve the time complexity of the first attack by using memory for some key lengths. We detect all reflectively weak keys and save them in a table in advance by checking all keys. The check mechanism deduced from the characterization of reflectively weak keys reduces the workload since we do not have to implement the whole key schedule, even though we check all the keys. The pre-computation phase costs roughly $r \cdot 2^{k-11}$ steps and we recover the key in $2^{(k+32-16r)/64}$ steps using $2^{k+32-16r}$ memory. Note that this is an improvement of the first attack when $k < 16r + 32$. Some interesting examples are given in Table 1 for $r = 8$ and $r = 16$.

Another result is a straightforward improvement of Vaudenay's attack. We reduce the number of chosen plaintexts from $3 \cdot 2^{51}$ to $3 \cdot 2^{44}$ on a set of keys of size roughly 2^{k-271}.

In addition, we propose a new success criterion for an attack working on some subset of the key space. We argue that such an attack is successful if the workload of determining that the unknown key is in the subset, is less than the

[1] We would like to thank the anonymous referees for pointing these references.

r	k	w	PC	M	T
8	128	2^{32}	$2^{120.6}$	2^{32}	-
	160	2^{64}	$2^{152.6}$	2^{64}	1
	192	2^{96}	$2^{184.6}$	2^{96}	2^{32}
	192	2^{96}	-	-	$2^{153.3}$
16	256	2^{32}	$2^{249.3}$	2^{32}	-
	288	2^{64}	$2^{281.3}$	2^{64}	1
	320	2^{96}	$2^{313.3}$	2^{96}	2^{32}
	384	2^{160}	-	-	$2^{282.1}$
	448	2^{224}	-	-	$2^{282.1}$

Table 1. Some Complexity Examples of The Attack. w is the average number of weak keys; PC is Pre-computation steps; M is Memory Space Used; T is Time Steps. Each step is equal to one step in exhaustive search. Data complexity is roughly 2^{34} known plaintexts. Complexities without memory are the examples of the first attack.

number of keys in the subset, and recovering it is less than that of exhaustive search.

The paper is organized as follows. Blowfish is described briefly in Section 2. Moreover, we give two new descriptions of the Blowfish algorithm. We state reflection properties of Blowfish in Section 3 as a preparation phase for the statements of the attacks. The notion of reflectively weak key and its characterization is introduced in this section. Then, we give the details of the attack and its improvement in Section 4. The improvement of Vaudenay's analysis for a subset of keys is given in Section 5. In the last section, we discuss the similarity degrees of the functions producing subkeys and the parameters of Blowfish, and give the argument about the success criterion for attacks working on some keys.

1.2 Notation

We use the following notation throughout the paper: k is the bit length of the key; r is the number of rounds; F is the key dependent round function of Blowfish; P is the array of 32 bit subkeys of Blowfish and P_i is its i-th component for $i = 1, .., r+2$; I is the array of hexadecimal digits of π XORed with the key bits; and $\oplus$ is the XOR operator.

2 High Level Descriptions of Blowfish

Blowfish is a 16-round Feistel network with 64 bit block length and a variable key length of at most 448 bits. It is also specified as an 8-round cipher with a key length of at most 192 bits [17]. Blowfish uses a large number of subkeys. The set of subkeys consists of two parts: The P array which contains $r+2$ number of 32-bit subkeys, $P_1, ..., P_{r+2}$, and four 8×32 key dependent S-boxes used in the F function. The encryption process starts after the P array and the S-boxes are generated. Let (x_1, y_1) be a plaintext for $x_1, y_1 \in GF(2)^{32}$. Then, i-th round of the encryption process is given as $(x_{i+1}, y_{i+1}) = (F(P_i \oplus x_i) \oplus y_i, P_i \oplus x_i)$. The corresponding ciphertext is defined as $(y_{r+1} \oplus P_{r+2}, x_{r+1} \oplus P_{r+1})$. We do not give the details of F function since we do not use it in the analyses. The high level description of Blowfish is depicted as Type I in Figure 1.

Generating the P array and the S-boxes is as follows:

- Initialize the I array and the S-boxes with hexadecimal digits of π.
- XOR I_1 with the first 32 bits of the key, I_2 with the second 32 bits of the key and so on for all bits of the key. Repeatedly cycle through the key bits until the entire I array has been XORed with key bits. Then copy the contents of the I array to the P array.
- Encrypt the all-zero string with the Blowfish algorithm, using the P array as subkeys. Replace P_1 and P_2 with the output.
- Repeat the last process, replacing all entries of P array, four S-boxes in order, with the output of continuously changing Blowfish algorithm.

2.1 New Models for Description

The XOR operator is commutative. Hence, an XOR operator of a subkey in Blowfish can be pushed through other XOR operators until a non-commutative operation such as an F operation is obtained. So, by moving certain subkeys we can obtain various descriptions of Blowfish. Two descriptions are depicted in Figure 1. We call them *the Type II description of Blowfish* and *the Type III description of Blowfish.* For example, in the Type II description we move the third round key through the second round to the first round and the fourth round key through the third round to the second round. So we consider the third round key as a part of the first round and the fourth round key as a part of the second round.

Repeating this process we obtain a new description of Blowfish where half of the rounds use two subkeys and the other half of the rounds use no subkey. The type III description can be obtained similarly. These descriptions facilitate the attack idea. Particularly, we treat two-round Blowfish as keyed or unkeyed:

Definition 1. *Two-rounds of Blowfish given as*

$$x' = F(P_{i_1} \oplus x) \oplus y \oplus P_{i_3} \oplus P_{i_4} \text{ and}$$
$$y' = F(F(P_{i_1} \oplus x) \oplus y \oplus P_{i_3}) \oplus P_{i_1} \oplus P_{i_2} \oplus x$$

is called a two-round keyed Blowfish function ($\mathcal{K}_2$ in short) and

$$x' = F(x) \oplus y \text{ and}$$
$$y' = F(F(x) \oplus y) \oplus x$$

is called a two-round unkeyed Blowfish function ($\mathcal{U}_2$ in short). Here (x, y) is an input and (x', y') is the corresponding output.

Two-round keyed/unkeyed Blowfish functions are depicted in Figure 2.

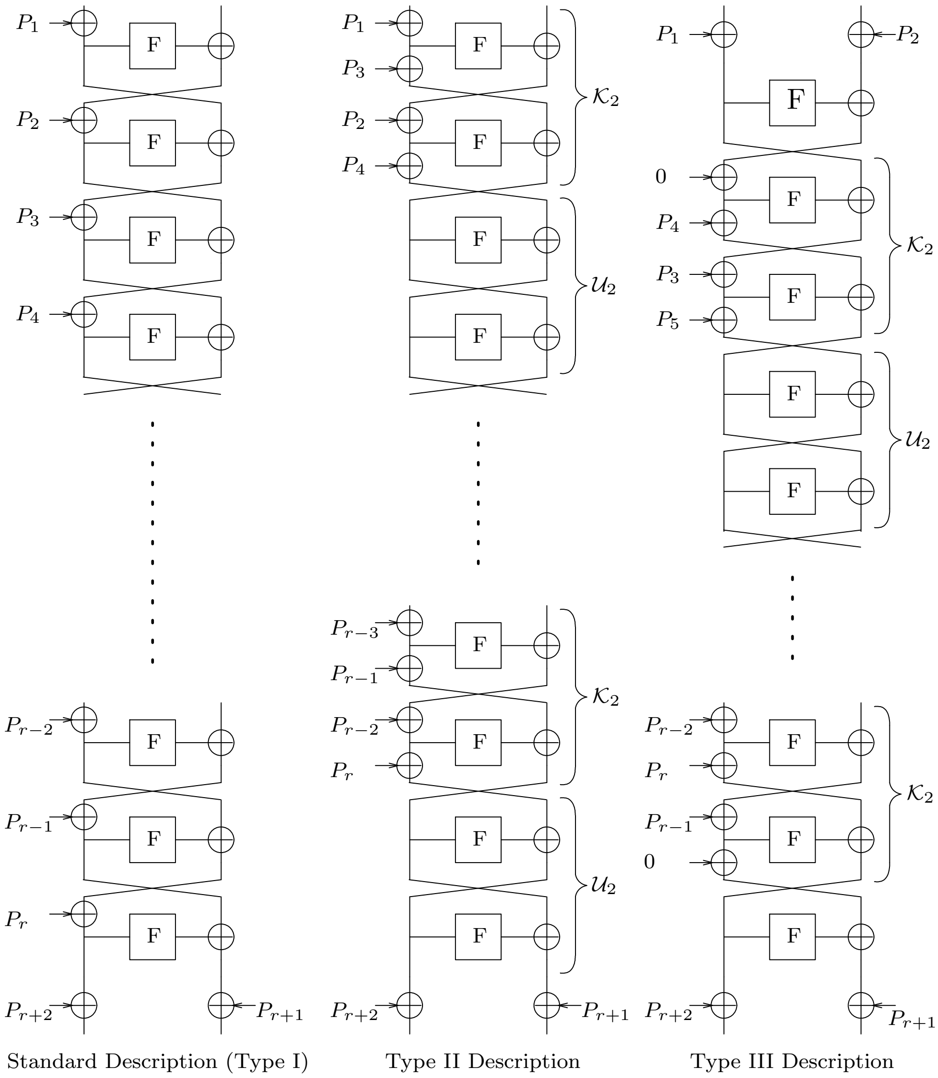

Fig. 1. Three different descriptions of r-round Blowfish

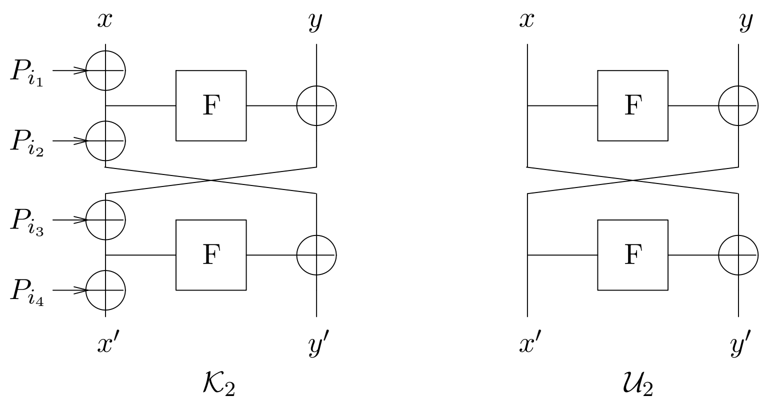

Fig. 2. General Description of $\mathcal{K}_2$ and $\mathcal{U}_2$

3 Reflection Properties of Blowfish

One of the very recent cryptanalysis methods is the reflection attack [10]. This attack exploits the similarities between the round functions of the encryption and the round functions of the decryption. It can be very powerful especially against product ciphers using involutions, such as Feistel networks. In general, self-similarity attacks are mounted on ciphers with simple key schedules. We apply reflection attack on Blowfish, as an exceptional example with a very complicated key schedule, and successfully recover the key in some special cases.

Let us note that Blowfish can be written as a composition of $\mathcal{K}_2$ and $\mathcal{U}_2$ functions (see Figure 1). The reflection attack exploits certain properties of these functions. $\mathcal{U}_2$ has many fixed points and so does $\mathcal{K}_2$ for some subkeys. Moreover, any $\mathcal{U}_2$ is an involution and $\mathcal{K}_2^{-1}$ has the same structure as $\mathcal{K}_2$.

Lemma 1. *Consider a two-round keyed Blowfish function given as*

$$x' = F(P_{i_1} \oplus x) \oplus y \oplus P_{i_3} \oplus P_{i_4} \text{ and}$$
$$y' = F(F(P_{i_1} \oplus x) \oplus y \oplus P_{i_3}) \oplus P_{i_1} \oplus P_{i_2} \oplus x$$

where (x, y) is the input and (x', y') is the corresponding output. If the subkeys $P_{i_1} = P_{i_4}$ and $P_{i_2} = P_{i_3}$, then the two-round keyed Blowfish function has 2^{32} fixed points.

Proof. Assume that $P_{i_1} = P_{i_4}$ and $P_{i_2} = P_{i_3}$. Then, (x, y) is encrypted to (x, y) if and only if $y = F(P_{i_1} \oplus x) \oplus x \oplus P_{i_1} \oplus P_{i_2}$. However, we have 2^{32} plaintexts of the form $(x, F(P_{i_1} \oplus x) \oplus x \oplus P_{i_1} \oplus P_{i_2})$. Therefore, the $\mathcal{K}_2$ has 2^{32} fixed points. □

A straightforward corollary of Lemma 1 is obtained when two-round Blowfish is unkeyed, i.e., $P_1 = P_2 = P_3 = P_4 = 0$. Hence, any two-round unkeyed Blowfish function ($\mathcal{U}_2$) has 2^{32} fixed points of the form $(x, F(x) \oplus x)$.

Definition 2. *A* $(4r'-2)$*-round function* $\mathcal{K}_2 S\mathcal{U}_2 S\mathcal{K}_2 S\mathcal{U}_2 S \cdots S\mathcal{U}_2 S\mathcal{K}_2$ *is called a* $(4r'-2)$*-round Blowfish function, where* S *is the swap operation of Feistel network.*

Note that, we have r' number of $\mathcal{K}_2$ and $r'-1$ number of $\mathcal{U}_2$ operations in a $(4r'-2)$-round Blowfish function.

We show that when there are certain relations among the round subkeys used in a $(4r'-2)$-round Blowfish function, then $(4r'-2)$-round Blowfish function has many fixed points.

Proposition 1. *Let* $\mathcal{B}$ *be a* $(4r'-2)$*-round Blowfish function. Assume that the* i*-th* $\mathcal{K}_2$ *of* $\mathcal{B}$ *is the inverse of the* $(r'-i+1)$*-th* $\mathcal{K}_2$ *of* $\mathcal{B}$ *for* $i = 1, ..., \lfloor \frac{r'}{2} \rfloor$ *where* $\lfloor \frac{r'}{2} \rfloor$ *is the integer part of* $\frac{r'}{2}$*. If* r' *is odd, then assume also that the* $(\frac{r'+1}{2})$*-th* $\mathcal{K}_2$ *has* 2^{32} *fixed points. Then the function* $\mathcal{B}$ *has* 2^{32} *fixed points.*

Proof. Let x be an input of $\mathcal{B}$. The intermediate two-round in the center of encryption is $(\frac{r'+1}{2})$-th $\mathcal{K}_2$ if r' is odd and $(\frac{r'}{2})$-th $\mathcal{U}_2$ if r' is even. $\mathcal{U}_2$ has 2^{32} fixed points by Lemma 1 and the $(\frac{r'+1}{2})$-th $\mathcal{K}_2$ also has 2^{32} fixed points by the assumption. Moreover, the i-th $\mathcal{K}_2$ is the inverse of $(r'-i+1)$-th $\mathcal{K}_2$ by the assumption. Then, the input of the i-th $\mathcal{K}_2$ is equal to the output of the $(r'-i+1)$-th $\mathcal{K}_2$ for any $i = 1, ..., \lfloor \frac{r'}{2} \rfloor$ corresponding to x means x is a fixed of $\mathcal{B}$. Hence, any fixed point of the central round produces a fixed point of $\mathcal{B}$ and any fixed point of $\mathcal{B}$ gives a fixed point of the central round. Therefore, $\mathcal{B}$ has 2^{32} fixed points.

□

Observe that, the i-th $\mathcal{K}_2$ is the inverse of the $(r'-i+1)$-th $\mathcal{K}_2$ if and only if their subkeys are equal in twist order. That is, if $P_{i_1}, P_{i_2}, P_{i_3}, P_{i_4}$ are the subkeys of i-th $\mathcal{K}_2$ and $P'_{i_1}, P'_{i_2}, P'_{i_3}, P'_{i_4}$ are the subkeys of $(r'-i+1)$-th $\mathcal{K}_2$ then we have $P_{i_1} = P'_{i_4}$, $P_{i_2} = P'_{i_3}$, $P_{i_3} = P'_{i_2}$ and $P_{i_4} = P'_{i_1}$. On the other hand, a sufficient condition for having 2^{32} fixed points of $(\frac{r'+1}{2})$-th $\mathcal{K}_2$ is given by Lemma 1.

Definition 3. *A key is called a reflectively weak key with respect to a* $(4r'-2)$*-round Blowfish function* $\mathcal{B}$ *if* $\mathcal{B}$ *has* 2^{32} *fixed points.*

Assumptions of Proposition 1 and Lemma 1 are satisfied when certain equalities among subkeys hold. In this case, we have many fixed points. In the following theorem, we prove that this is the only case resulting in many fixed points, by assuming that Blowfish is a random permutation when the assumptions do not hold.

Theorem 1. *Assume that a given key is reflectively weak with respect to an* $(r-2)$*-round Blowfish function* $\mathcal{B}$ *and also assume that* $\mathcal{B}$ *is a random permutation when the assumptions of Proposition 1 and Lemma 1 do not hold. Then, the subkeys of* $\mathcal{B}$ *satisfy the assumptions of Proposition 1 and Lemma 1 with a probability approximately*

$$1 - \frac{2^{16 \cdot r} - 1}{2^{32}! \cdot e + 2^{16 \cdot r} - 1}$$

where e is the Euler constant.

Proof. Let $X_{\mathcal{A}}$ be the event that $\mathcal{B}$ satisfies the assumptions of Proposition 1 and Lemma 1 and $X_{\mathcal{F}}$ be the event that $\mathcal{B}$ has 2^{32} fixed points. Assumptions of Proposition 1 and Lemma 1 imply that we have $\frac{r}{2}$ equalities between r subkeys of $\mathcal{B}$. Each equality holds with a probability approximately 2^{-32}. Hence, $\Pr(X_{\mathcal{A}}) = 2^{-16\cdot r}$. We have $\Pr(\ X_{\mathcal{F}} \mid X_{\mathcal{A}}\ ) = 1$ by Proposition 1. *The rencontres numbers,* i.e., the number $D(n, m)$ of permutations of n containing m fixed points, is given as

$$D(n, m) = \frac{n!}{m!} \sum_{k=0}^{n-m} \frac{(-1)^k}{k!}$$

which immediately implies that $\frac{D(n,m)}{n!} \approx \frac{e^{-1}}{m!}$ for large n (see [15] for details). Since $\mathcal{B}$ is a random permutation when the assumptions of Proposition 1 and Lemma 1 do not hold, we have $\Pr(\ X_{\mathcal{F}} \mid \overline{X_{\mathcal{A}}}\ ) = \frac{e^{-1}}{2^{32}!}$. Then,

$$\begin{aligned}\Pr(X_{\mathcal{F}}) &= \Pr(X_{\mathcal{A}}) \Pr(\ X_{\mathcal{F}} \mid X_{\mathcal{A}}\ ) + \Pr(\overline{X_{\mathcal{A}}}) \Pr(\ X_{\mathcal{F}} \mid \overline{X_{\mathcal{A}}}\ ) \\ &= 2^{-16\cdot r} + \frac{e^{-1}}{2^{32}!}(1 - 2^{-16\cdot r}).\end{aligned}$$

Now, applying Bayes Rule we get,

$$\Pr(\ X_{\mathcal{A}} \mid X_{\mathcal{F}}\ ) = \frac{\Pr(\ X_{\mathcal{F}} \mid X_{\mathcal{A}}\ ) \cdot \Pr(X_{\mathcal{A}})}{\Pr(X_{\mathcal{F}})} = 1 - \frac{2^{16r} - 1}{2^{32}! \cdot e + 2^{16r} - 1}$$

which is the probability that the assumptions of Proposition 1 and Lemma 1 hold, given that $\mathcal{B}$ has 2^{32} fixed points. □

Remark 1. Using Stirling's approximation, we have $2^{32}! \approx (2^{32})^{2^{32}} = 2^{2^{37}}$ and the probability given in Theorem 1 is almost 1 (roughly $1-2^{-2^{37}}$). Therefore, the converses of both Proposition 1 and Lemma 1 are true with a probability almost 1. This probability affects the success rate of the attacks. However, Theorem 1 implies that the false alarm probability is negligible. Hence, we can assume that we have $\frac{r}{2}$ equalities between r subkeys of $\mathcal{B}$ if $\mathcal{B}$ has 2^{32} fixed points.

Example 1. Let $r = 16$ and let $\mathcal{B}$ be the 14-round Blowfish function obtained by removing the first and the last rounds in Type III description of Blowfish. Then, loosely speaking, a key is a reflectively weak key with respect to $\mathcal{B}$ means that the following 7 equalities are satisfied: $P_4 = P_{15}$, $P_3 = P_{16}$, $P_5 = P_{14}$, $P_6 = P_{13}$, $P_7 = P_{12}$, $P_8 = P_{11}$ and $P_9 = P_{10}$. The eighth equality already holds (0=0) by the definition of Type III description of Blowfish.

4 Two Reflection Attacks

In this section, we introduce an attack and its improvement for some key lengths. The improvement has two phases: Reflectively weak keys are collected in the pre-computation phase, and the reflectively weak key is recovered during the on-line phase.

4.1 First Attack

The attack consists of two parts. In the first part, we identify if the key is reflectively weak. Subkeys of a reflectively weak key satisfies certain equalities and we utilize these equalities to recover the key in the second part.

We use several known plaintext-ciphertext pairs to identify a reflectively weak key . Let (x, y) denote plaintext and (x', y') denote the corresponding ciphertext. Assume that a reflectively weak key is used with respect to the $(r-2)$-round Blowfish function $\mathcal{B}$, obtained by removing the first and the last rounds in Type III description of Blowfish. Then, $\mathcal{B}$ will have 2^{32} fixed points by Proposition 1. Observe that, if $\mathcal{B}$ has a fixed point for (x, y), then we have $P_1 \oplus P_{r+2} = x \oplus x'$ and $P_2 \oplus P_{r+1} = y \oplus y'$. Hence, we expect the value $(P_1 \oplus P_{r+2}, P_2 \oplus P_{r+1})$ to occur with probability 2^{-32} and other values to occur with probability 2^{-64} when a reflectively weak key is used. On the other hand, we expect that each vector,$(x \oplus x', y \oplus y')$, occurs with probability 2^{-64} if the key is not a reflectively weak key. Consequently, we identify a reflectively weak key and obtain $(P_1 \oplus P_{r+2}, P_2 \oplus P_{r+1})$ with 2^{34} known plaintexts.

Once we identify a reflectively weak key, we can recover information on $\frac{r}{2}+1$ subkeys of P array since we have $\frac{r}{2}+1$ equalities between $r+2$ subkeys. $\frac{r}{2}-1$ of the equalities are deduced by Theorem 1 and two equalities are obtained while identifying the reflectively weak key. By guessing $\frac{r}{2}+1$ subkeys we can determine remaining $\frac{r}{2}+1$ subkeys and obtain the whole P array. One can recover the I array and the key by reversing the key schedule by the following Lemma.

Lemma 2. *Assume that the P array of a key is known. Then it is possible to recover the key by $\frac{r}{2}+1$ encryptions.*

Proof. For any $i = 1, ..., \frac{r}{2}+1$, (P_{2i-1}, P_{2i}) is the encryption of the all-zero string with the Blowfish algorithm with the subkeys

$$(P_1, P_2, \cdots, P_{2i-3}, P_{2i-2}, I_{2i-1}, I_{2i}, \cdots, I_{r+1}, I_{r+2})$$

and a publicly known F function.

We encrypt the all-zero string up to r rounds with subkeys $(P_1, P_2, \cdots, P_{r-1}, P_r)$ and obtain $(P_{r+1} \oplus I_{r+2}, P_{r+2} \oplus I_{r+1})$. Then, we can easily recover the subkeys (I_{r+1}, I_{r+2}). We need to recover (I_{r-1}, I_r) by using the P array and (I_{r+1}, I_{r+2}), and recover (I_{r-3}, I_{r-2}) by using the P array and $(I_{r-1}, I_r, I_{r+1}, I_{r+2})$. We repeat this process until the whole I array is obtained. So, the problem of reversing the key schedule and recovering the I array from the P array is reduced to the problem of recovering the value of (I_{2i-1}, I_{2i}) using $(P_1, P_2, \cdots, P_{2i-3}, P_{2i-2}, I_{2i+1}, I_{2i+2}, \cdots, I_{r+1}, I_{r+2})$ and (P_{2i-1}, P_{2i}). Observe that this problem is recovering the subkeys for two-round Blowfish given an input-output pair. The second subkey can be moved up to the first round and both subkeys can be considered as an initial whitening. Hence we can decrypt the output for two rounds, XOR the result with the input and obtain the subkeys (I_{2i-1}, I_{2i}). This process costs only one Blowfish encryption. Therefore we recover the whole I array with a cost of $\frac{r}{2}+1$ encryptions. Then the key is extracted from I with no cost. $\square$

Observe that repetition of 32 bit key words in the construction of the I array allows one to check whether the obtained I array is a valid array. Although several candidates may turn out to give valid I arrays, complexity of exhaustively searching these candidates is dominated by the complexity of the attack.

We guess $16r+32$ bits in total and each guess is checked in $\frac{r}{2}+1$ encryptions by Lemma 2. On the other hand, each step of exhaustive search costs $\frac{r}{2}+514$ encryptions. Therefore, the time complexity is $\frac{2^{16r+32}.(r+2)}{r+1028}$ exhaustive search steps. Hence we have the following theorem.

Theorem 2. *Let $\mathcal{B}$ be the $(r-2)$-round Blowfish function obtained by removing the first and the last rounds in the type* III *description of Blowfish. Then, one may determine if an unknown key is a reflectively weak key with respect to $\mathcal{B}$ by using approximately 2^{34} known plaintexts and then recover the key in $\frac{2^{16r+32}.(r+2)}{r+1028}$ steps if it is reflectively weak, where each step is a key loading time plus one encryption.*

Let us note that the time complexity of the attack is independent of the key length. On the other hand, a key is a reflectively weak key with respect to the $(r-2)$-round Blowfish function $\mathcal{B}$ in Type III description of Blowfish if $\frac{r}{2}-1$ equalities are satisfied among $r-2$ subkeys of $\mathcal{B}$ by Theorem 1. Therefore, assuming the Blowfish key schedule is random, the probability that a key is a reflectively weak key is 2^{32-16r}.

4.2 Second Attack

For some key lengths, the previous attack can be improved using memory. We search all the keys and collect reflectively weak keys in a table with their subkeys $(P_1 \oplus P_{r+2}, P_2 \oplus P_{r+1})$, sorted with respect to $(P_1 \oplus P_{r+2}, P_2 \oplus P_{r+1})$. A key is loaded to the key schedule and the P array is generated. Then, we check whether the subkeys $P_2, ..., P_r$ satisfy the equalities so as to satisfy the assumptions of Proposition 1. Note that the first check is the equality $P_{r/2+1} = P_{r/2+2}$ and most of the keys are eliminated in this step where it is enough to produce P arrays up to $P_{r/2+2}$ which costs $\frac{r}{4}+1$ encryptions. We need to produce P subkeys up to $P_{r/2+4}$ for only one in 2^{32} keys, up to $P_{r/2+6}$ for only one in 2^{64} keys and so on. Hence, the total time complexity is given as

$$\frac{2^{k-1}(r+4)}{r+1028} + \frac{2^{k-33}(r+8)}{r+1028} + \frac{2^{k-65}(r+12)}{r+1028} + \cdots \approx \frac{2^{k-1}(r+4)}{r+1028}$$

which seems to cost almost that of exhaustive search. However, it is done once and faster than exhaustive search.

The table of weak keys occupies $2^{k+32-16r}$ spaces in memory. The attack is now straightforward. First, we determine if the unknown key is reflectively weak with 2^{34} known plaintexts as in the first attack. If the key is a reflectively weak key, then we obtain $(P_1 \oplus P_{r+2}, P_2 \oplus P_{r+1})$. By searching the table sorted with respect to $(P_1 \oplus P_{r+2}, P_2 \oplus P_{r+1})$, we get approximately $2^{(k+32-16r)/64}$ candidates. The correct key can be recovered by searching these candidates. Therefore, the time complexity will be $2^{(k+32-16r)/64}$ steps.

5 Improvement of Vaudenay's Cryptanalysis on a Subset of Keys

In [18], Vaudenay proposes a differential attack on 16-round Blowfish with $3 \cdot 2^{51}$ chosen plaintexts with the assumption that the F function is known and weak in the sense that some of the S-boxes are not one to one. The attack works for approximately 2^{k-15} keys. The number of chosen plaintexts required for the attack can be generalized as $2^{2+7\cdot\lceil\frac{r-2}{2}\rceil}$ for $r \leq 10$ and $3 \cdot 2^{2+7\cdot\lceil\frac{r-2}{2}\rceil}$ for $r \geq 11$.

We improve Vaudenay's attack on 16-round Blowfish in a certain subset of Vaudenay's weak key class by reducing the amount of chosen plaintext required for the attack. The improved version has two steps: In the first step, we recover both whitening keys P_{17} and P_{18}, by a reflection attack to reduce the algorithm to 14 rounds. In the second step, we apply Vaudenay's differential attack to the 14-round algorithm.

Assume that F is known and weak. Assume also that a reflectively weak key with respect to the first 14 rounds of the Type II description of Blowfish is used. The latter assumption can be checked by collecting roughly 2^{34} vectors $(F(x) \oplus y \oplus x', F(F(x) \oplus y) \oplus x \oplus y')$ where (x, y) is a plaintext and (x', y') is the corresponding ciphertext. If a plaintext (x, y) is a fixed point of the first 14 rounds, then

$$(P_{18}, P_{17}) = (F(x) \oplus y \oplus x', F(F(x) \oplus y) \oplus x \oplus y').$$

Hence, we expect one of the vectors to occur approximately four times in the collection of approximately 2^{34} plaintexts, encrypted by a reflectively weak key. This vector is (P_{18}, P_{17}) since the probability that (P_{18}, P_{17}) occurs is slightly more than 2^{-32} whereas the probability that any arbitrary vector occurs is approximately 2^{-64}. Therefore, if a reflectively weak key with respect to the first 14 rounds of the Type II description is used, then we can identify it and recover the whitening keys (P_{18}, P_{17}) by using approximately 2^{34} known plaintexts. Then, we peel the last two rounds, obtaining 14-round Blowfish. Applying the differential attack in [18] to 14 round Blowfish requires $3 \cdot 2^{44}$ chosen plaintexts. Therefore, we reduce the number of chosen plaintexts from $3 \cdot 2^{51}$ to $3 \cdot 2^{44}$.

The attack works if the key is weak both in terms of Vaudenay's attack and reflectively. F is weak for 2^{-15} of key space. On the other hand, by Proposition 1 and Theorem 1, if a key is reflectively weak with respect to the first 14 rounds of the Type II description of Blowfish, then certain eight equalities between subkeys in these 14 rounds hold. Thus, the probability that a reflectively weak key is used is approximately 2^{-256} since each equation holds with probability 2^{-32}. Therefore, the attack works for a subset of key space of size 2^{k-271}.

6 Discussion of Attacks

A new definition of similarity degree between two functions is given in [10]. The definition is as follows:

Definition 4. *Let $F_1, F_2 : GF(2)^n \rightarrow GF(2)^m$ be two functions. Then, F_1 and F_2 are called similar of degree (d_1, d_2) with probability p if the number of $(x, x') \in GF(2)^n \times GF(2)^n$ satisfying*

$$HW(x \oplus x') \leq n - d_1 \Rightarrow HW(F_1(x) \oplus F_2(x')) \leq m - d_2$$

is $p \cdot 2^n \cdot \sum_{i=0}^{n-d_1} \binom{n}{i}$ where $HW()$ is the Hamming Weight of binary vectors.

It is argued in [10] that round functions should not be similar of large degrees with large probabilities. In Blowfish the functions producing round keys are given as

$$\phi_i : GF(2)^k \longrightarrow GF(2)^{32800}, \phi_i(K) = (P_i, F), \text{ for } i = 1, ..., r.$$

Hence, any two functions ϕ_i and ϕ_j are similar of degree $(k, 32768)$ with probability 1. In other words, they are similar of the full degree, $(k, 32800)$, with probability 2^{-32}. That is, the functions producing round keys are highly similar even though they are one way functions by themselves. We exploited this property to mount a reflection attack on Blowfish. This example indicates that ciphers having round functions which are similar of high degree with high probability, may be vulnerable to self similarity attacks even though they have very complicated key schedules. Moreover, we argue that the attacks presented here can be improved further by taking different degrees of similarity or by decreasing the number of pairs of the functions compared.

Another property that we exploited is the relatively short block length of Blowfish. Its key length can be as long as 448 bits whereas its block length is always 64 bits. We propose that block length of a block cipher should not be smaller than key length. This is also necessary to provide resistance to tradeoff attacks [8, 1, 7] when the cipher is operated in a stream mode.

By Lemma 2, it is easy to take inverse of the key schedule of Blowfish and deduce the key if one knows the P array . For example, if the P array were updated once more after the F function were constructed in the key schedule, then we could not recover the key from the P array. For 16-round Blowfish, this change makes the key schedule only 1.7% slower than the original key schedule.

Unlike typical Feistel structure, P_i's are XORed outside F. Adding the subkeys to left half of the Feistel network seems to hinder the self similarity attacks since it destroys the typical symmetry of Feistel network. However, we reconstructed the symmetry by describing Blowfish in different manners (see Figure 1). Moreover, one can push some of the subkey XORs to the whitening which allows to increase the number of weak keys.

A recent phenomenon is how to evaluate an attack mounted on some so called weak keys. Most conventional attacks such as differential cryptanalysis [3] or linear cryptanalysis [11] work generally on any key. On the other hand, the attacks working only on a subset of the keys form a new class. These attacks have two important parameters: The number of weak keys and the workload to identify that the unknown key is weak. For a given attack, let W be the workload of identifying a weak key and w be the number weak keys. Given a set of $\frac{2^k}{w}$ randomly generated keys, we expect one weak key on the average. To identify the weak key, we run the identification process on all $\frac{2^k}{w}$ keys with a cost of $W\frac{2^k}{w}$. So, a necessary condition for the success of the attack is $W\frac{2^k}{w} < 2^k$, i.e., $W < w$. This leads to the following criteria: Assuming that the keys are produced randomly, we propose that an attack on weak keys should be considered successful, if the workload of identification of a weak key is less than the number of weak keys, in addition to the widely adopted phenomenon that the workload of key recovery is less than that of exhaustive search.

Acknowledgments

We thank Hüseyin Demirci, Nezih Geçkinli, Atilla Hasekioğlu and Ali Aydın Selçuk for their comments.

References

1. S. Babbage, *Improved Exhaustive Search Attacks on Stream Ciphers*, European Convention on Security and Detection, IEE Conference publication No. 408, pp. 161-166, IEE, 1995
2. E. Biham, *New Types of Cryptanalytic Attacks Using Related Keys*, J. of Cryptology, Vol.7, pp.229-246, 1994.
3. E. Biham, A. Shamir, *Differential Cryptanalysis of Data Encryption Standard*, Springer Verlag, 1993.
4. A. Biryukov, D. Wagner, *Slide Attacks*, Proceedings of FSE'99, LNCS 1636, pp.245-259, Springer Verlag, 1999.
5. A. Biryukov, D. Wagner, *Advanced Slide Attacks*, Advances in Cryptology-EUROCRYPT 2000, LNCS 1807, pp.589-606, Springer Verlag, 2000.
6. D. Coppersmith, *The Real Reason for Rivest's Phenomenon*, Advances in Cryptology-CRYPTO'85, LNCS 218, pp.535, Springer Verlag, 1986.
7. J. Golić, *Cryptanalysis of Alleged A5 Stream Cipher,* Advances in Cryptology-EUROCRYPT'97, LNCS 1233, pp.239-255, Springer Verlag, 1997.
8. J. Hong, P. Sarkar, *Rediscovery of the Time Memory Tradeoff*, Cryptology ePrint Archive, Report 2005/090, 2005.
9. B. S. Kaliski, R. L. Rivest, A. T. Sherman, *Is DES a pure Cipher?(Results of More Cycling Experiments on DES)*, Advances in Cryptology-CRYPTO'85,LNCS 218, pp.212, Springer Verlag, 1986.
10. O. Kara, *Reflection Attacks on Product Ciphers*, Cryptology ePrint Archive, Report 2007/043, 2007.
11. M. Matsui, *Linear Cryptanalysis Method of DES Cipher*, Advances in Cryptology-EUROCRYPT'93, LNCS 765, pp. 386-397, Springer Verlag, 1994.
12. J. H. Moore, G. J. Simmons, *Cycle Structures of the DES with Weak and Semi-Weak Keys,* Advances in Cryptology-CRYPTO'86, LNCS 263, pp.9-32, Springer Verlag, 1987.
13. J. H. Moore, G. J. Simmons, *Cycle Structure of the DES for Keys Having Palindromic (or Antipalindromic) Sequences of Round Keys*, IEEE Transactions on Software Engineering, Vol.SE-13, pp.262-273, 1987.
14. V. Rijmen, *Cryptanalysis and Design of Iterated Block Ciphers,* Doctoral Dissertation, K.U. Leuven, 1997.

15. J. Riordan, *An Introduction to Combinatorial Analysis*, New York, Wiley, 1958.
16. B. Schneier, *Description of a New Variable - Length Key, 64 Bit Block Cipher (Blowfish),* Proceedings of FSE'94, LNCS 809, pp.191-204, Springer Verlag, 1994.
17. `http://www.schneier.com/blowfish.html`.
18. S. Vaudenay, *On the Weak Keys of Blowfish*, Proceedings of FSE'96, LNCS 1039, pp.27-32, Springer Verlag, 1996.