Saturation Attacks on Reduced Round Skipjack

Kyungdeok Hwang[1], Wonil Lee[1], Sungjae Lee[2], Sangjin Lee[1], and Jongin Lim[1]

[1] Center for Information and Security Technologies(CIST),
Korea University, Anam Dong, Sungbuk Gu,
Seoul, KOREA
{ kdhwang, wonil, sangjin, jilim }@cist.korea.ac.kr
[2] Korea Information Security Agency(KISA)
sjlee@kisa.or.kr

Abstract. This paper describes saturation attacks on reduced-round versions of Skipjack. To begin with, we will show how to construct a 16-round distinguisher which distinguishes 16 rounds of Skipjack from a random permutation. The distinguisher is used to attack on 18(5∼22) and 23(5∼27) rounds of Skipjack. We can also construct a 20-round distinguisher based on the 16-round distinguisher. This distinguisher is used to attack on 22(1∼22) and 27(1∼27) rounds of Skipjack. The 80-bit user key of 27 rounds of Skipjack can be recovered with 2^{50} chosen plaintexts and $3 \cdot 2^{75}$ encryption times.

1 Introduction

In April 1993, the Clinton administration announced a proposed encryption technology that, according to the announcement "will bring the Federal Government together with industry in a voluntary program to improve the security and privacy of telephone communication while meeting the legitimate needs of law enforcement." Subsequently, in July 1993, a more formal announcement appeared in the Federal Register as a request for comments on a proposed Federal Information Processing Standard. The overall approach was initially referred to as Clipper, whereas the specific encryption algorithm is known as Skipjack.

Skipjack is a 64-bit block cipher and was first made public by the NSA in 1998[9, 10]. After the publication, several approaches to analysis of Skipjack have been made. The first analysis by Biham et al. [1] studied some of the detailed properties of G and in particular some of the properties of the substitution table S. This provided the first description of some differential and linear cryptanalytic attacks on reduced-round versions of Skipjack. They[2, 3] also considered the role of truncated differentials in Skipjack and some variants. Biham et al.[5] presented impossible differential attacks that are faster than exhaustive search for the user key if Skipjack is reduced by at least one round. So far, the attacks[5] are the best known attacks on Skipjack. Knudsen et al.[6] also published a range of attacks on reduced-round variants of Skipjack. They concentrate on the role of truncated differentials and demonstrated the effectiveness of boomerang attacks on Skipjack. But they could not improve on the impossible differential attacks on the 31 rounds of Skipjack. In addition, most recently Granboulan[7] found several flaws in the differential cryptanlysis of Knudsen et al.

In this paper, we describe saturation attacks on reduced-round versions of Skipjack. Saturation attack[8] is based on the idea of choosing a set of $k \times 2^w$ plaintexts such that each of the 2^w inputs for a w-bit permutation occurs exactly k times. The saturation attack exploits the fact that if the input set for the w-bit permutation is saturated then the output set of the permutation is saturated.

It should be emphasized that our attacks do not improve on the impossible differential attacks[5]. But this paper shows how to apply saturation attack to Skipjack for the first time.

The paper is organized as follows: In Section 2, preliminaries to the text of this paper is presented. The description of Skipjack is briefly given in Section 3. Section 4 explains how to construct a 16- and 20-round distinguisher. In Section 5, we show how to use the 16-round distinguisher to attack on 18(5∼22) and 23(5∼27) rounds of Skipjack. Moreover, using the 20-round distinguisher we also describe attacks on 22(1∼22) and 27(1∼27) rounds of Skipjack. Finally, in Section 6 we summarize this paper.

2 Preliminaries

We denote by I_n the set of all n-bit data. In this paper, a word always means a 16-bit data. We denote by $(\alpha^i, \beta^i, \gamma^i, \delta^i)$ an input data of the round i, where each of the Greek small letters is a constant word. By the notation, $(\alpha^{i+1}, \beta^{i+1}, \gamma^{i+1}, \delta^{i+1})$ means an output data of the round i. We denote by $(\mathbf{A}^i, \beta^i, \gamma^i, \delta^i)$ a set of input data of the round i, where $\mathbf{A}^i$ is a subset of I_{16} and each of the Greek small letters is a constant word (i.e.,$(\mathbf{A}^i, \beta^i, \gamma^i, \delta^i) = \{(\alpha^i, \beta^i, \gamma^i, \delta^i) \in I_{16}^4 | \alpha^i \in \mathbf{A}^i\}$). In a similar way, we can also define $(\mathbf{A}^i, \mathbf{B}^i, \gamma^i, \delta^i)$, $(\mathbf{A}^i, \mathbf{B}^i, \mathbf{C}^i, \delta^i)$, etc.

We will use the notion of a multiset to define a "saturated set". A multiset with $k \cdot 2^w$ entries in I_w is said to be "k-saturated " if every value in I_w is found exactly k times in the multiset. If $k = 1$, a saturated multiset is 1-saturated as I_w. From now on, "1-saturated" is shortly said to be "saturated". A set $M (\subseteq I_w)$ is said to be "balanced" if the following equation holds :

$$\bigoplus_{x_i \in M} x_i = 0.$$

Note that if M is a k-saturated multiset then M is balanced.

3 Skipjack

Skipjack[9] is a 64-bit iterated block cipher with 32 rounds of two types, called Rule A and Rule B. Each round is described in the form of a linear feedback shift register with additional non-linear keyed G permutation. Encryption with Skipjack consists of first applying eight rounds of Rule A, then eight rounds of Rule B, once again eight rounds of Rule A and finally eight rounds of Rule B.

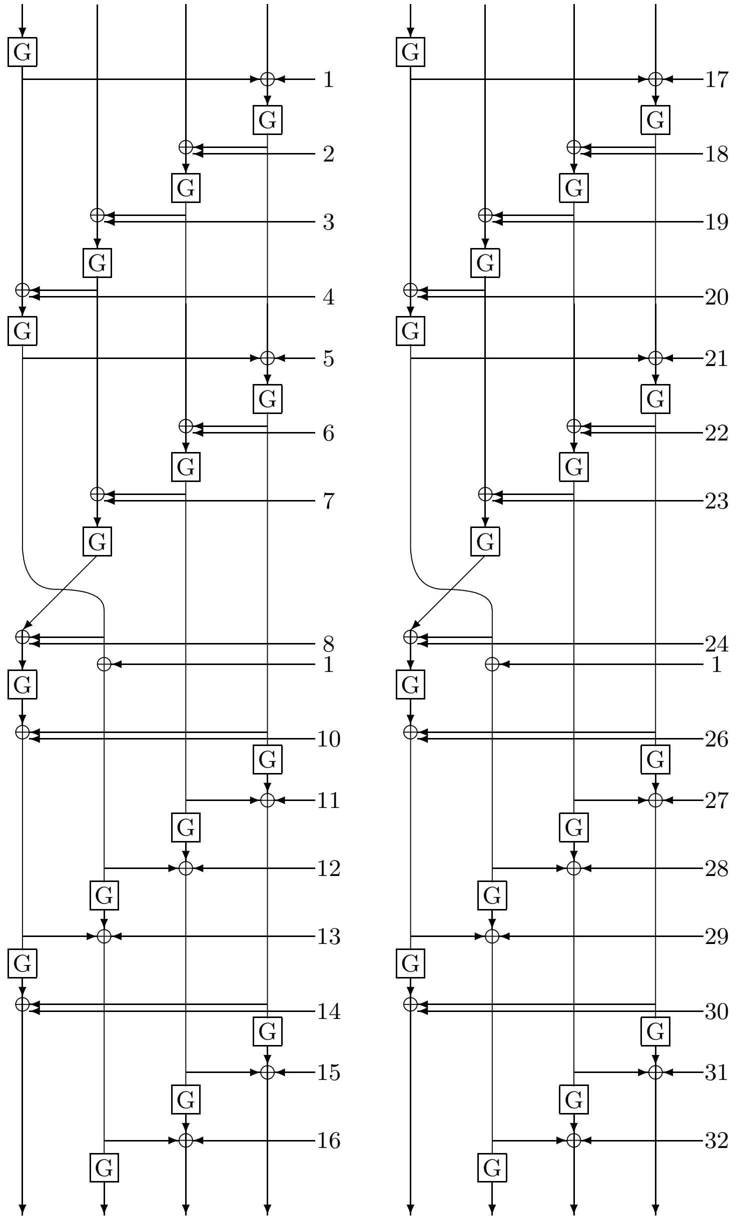

Fig. 1. Skipjack

Rule A	**Rule** B
$w_1^{k+1} = \mathrm{G}^k(w_1^k) \oplus w_4^k \oplus counter^k$	$w_1^{k+1} = w_4^k$
$w_2^{k+1} = \mathrm{G}^k(w_1^k)$	$w_2^{k+1} = \mathrm{G}^k(w_1^k)$
$w_3^{k+1} = w_2^k$	$w_3^{k+1} = w_1^k \oplus w_2^k \oplus counter^k$
$w_4^{k+1} = w_3^k$	$w_4^{k+1} = w_3^k$

Table 1. Rule A and B

The original definitions of Rule A and Rule B are given in table 1 where w_i is a word, *counter* is the round number and G is a four-round Feistel permutation whose F is defined as an 8 × 8-bit S box, and each round of G is keyed by eight bits of the key. The key scheduling of Skipjack takes a 10-byte key, and uses four of them at a time to key each G permutation. The first four bytes are used to key the first G permutation, and each additional G permutation is keyed by the next four bytes cyclically, with a cycle of five rounds.

The description of table 1 becomes simpler if we unroll the rounds, and keep the four words in the shift register stationary. Figure 1 describes this representation of Skipjack. In this paper, the existence of the *counter* is ignored since it has no cryptanalytic significance in our attack.

4 Distinguishers

It is well known that a good block cipher behaves like a random permutation. In this section, we describe distinguishers for Skipjack. In other words, given a well-chosen set of plaintexts, we will find properties in the corresponding set of ciphertexts, which are unlikely in the case of a random permutation. This holds for reduced-round versions of Skipjack under arbitrary keys. In the following, we describe how to construct a 16- and 20-round distinguisher.

4.1 A 16-round distinguisher

We describe how to construct a 16-round(5∼20) distinguisher. Using this distinguisher, we will show that Skipjack reduced from 32 to 18 rounds and to 23 rounds can be broken by an attack which is faster than exhaustive search.

We concentrate on the 16 rounds of Skipjack starting from round 5 and ending at round 20 (i.e., without the first four rounds and the last twelve rounds). For the sake of clarity, we use the original round numbers of the full Skipjack, i.e., from 5 to 20, rather than from 1 to 16. The 16-round distinguisher is shown in Figure 2.

Consider a set of 2^{16} plaintexts $(\alpha^5, \mathbf{B}^5, \gamma^5, \delta^5)$ where α^5, γ^5 and δ^5 are three arbitrary constant words and $\mathbf{B}^5$ is saturated. Then the corresponding data set after round 7 is $(\alpha^8, \mathbf{B}^8, \gamma^8, \delta^8)$ where α^8, γ^8 and δ^8 are new constant words and $\mathbf{B}^8$ is saturated. In addition, the corresponding data set after round 9 is $(\mathbf{A}^{10}, \beta^{10}, \gamma^{10}, \delta^{10})$ where $\mathbf{A}^{10}$ is saturated, and β^{10}, γ^{10} and δ^{10} are new constant words. We also observe that the set of output data of round 13 is $(\mathbf{A}^{14}, \mathbf{B}^{14}, \gamma^{14}, \delta^{14})$ where $\mathbf{A}^{14}, \mathbf{B}^{14}$ are saturated and the set of output data of round 17 is $(\mathbf{A}^{18}, \mathbf{B}^{18}, \mathbf{C}^{18}, \mathbf{D}^{18})$ where $\mathbf{A}^{18}$, $\mathbf{B}^{18}$, $\mathbf{C}^{18}$ and $\mathbf{D}^{18}$ are all saturated. Moreover, the set of output data of round 18 is $(\mathbf{A}^{19}, \mathbf{B}^{19}, \mathbf{C}^{19}, \mathbf{D}^{19})$ where $\mathbf{A}^{19}$, $\mathbf{B}^{19}$ and $\mathbf{D}^{19}$ are saturated, but $\mathbf{C}^{19}$ is generally not saturated since $\mathbf{C}^{19} = \{\gamma^{18} \oplus \delta^{19} | \gamma^{18} \in \mathbf{C}^{18}, \delta^{19} \in \mathbf{D}^{19}\}$ holds. However note that $\mathbf{C}^{19}$ is balanced.

The corresponding data set after round 19 is $(\mathbf{A}^{20}, \mathbf{B}^{20}, \mathbf{C}^{20}, \mathbf{D}^{20})$ where $\mathbf{A}^{20}$ and $\mathbf{D}^{20}$ are saturated, but neither $\mathbf{B}^{20}$ nor $\mathbf{C}^{20}$ is generally saturated. This fact is denoted by $(\mathbf{A}^{20}, \mathbf{?}, \mathbf{?}, \mathbf{D}^{20})$ in Figure 2. The corresponding data set after round 20 which is the last round in the distinguisher is $(\mathbf{A}^{21}, \mathbf{B}^{21}, \mathbf{C}^{21}\ , \mathbf{D}^{21})$ where $\mathbf{D}^{21}$ is saturated but $\mathbf{A}^{21}$, $\mathbf{B}^{21}$ and $\mathbf{C}^{21}$ are generally not saturated. This fact is denoted by $(\mathbf{?}, \mathbf{?}, \mathbf{?}, \mathbf{D}^{21})$ in figure 2. Note that $\mathbf{A}^{20}$, $\mathbf{D}^{21}$ is balanced.

As a result, given any set of 2^{16} plaintexts $(\alpha^5, \mathbf{B}^5, \gamma^5, \delta^5)$ where α^5, γ^5 and δ^5 are three arbitrary constant words and $\mathbf{B}^5$ is saturated, $\mathbf{A}^{20}$ and $\mathbf{D}^{21}$ are saturated and therefore balanced with probability 1. On the other hand, the probability that a random permutation satisfies the property is 2^{-32}. Therefore we can distinguish Skipjack from a random permutation with high probability.

The reason that a saturation attack works on the reduced-round versions of Skipjack can be explained by the fact that $\mathbf{A}^{20}$ and $\mathbf{D}^{21}$ are always balanced in this distinguisher.

4.2 An Extension to 20-round

We show how to extend the distinguisher from 16 to 20-round. Using the 20-round(1∼20) distinguihser, we will show that Skipjack reduced from 32 to 22 rounds and to 27 rounds can be broken by an attack which is faster than exhaustive search.

We concentrate on the 20 rounds of Skipjack starting from round 1 and ending at round 20 (i.e., without the last twelve rounds). The 20-round distinguisher is shown in Figure 3.

The result of this subsection will now be briefly summarized : Given any set of 2^{48} plaintexts $(\mathbf{A}^1, \mathbf{B}^1, \gamma^1, \mathbf{D}^1)$ where $\mathbf{A}^1$, $\mathbf{B}^1$ and $\mathbf{D}^1$ are saturated and γ^1 is a constant word, $\mathbf{A}^{20}$ and $\mathbf{D}^{21}$ are balanced with probability 1. On the other hand, the probability that a random permutation satisfies the property is 2^{-32}.

This result is derived from using the 16-round distinguisher. For the specific explanation of the result, we will partition the set of 2^{48} plaintexts into 2^{32} subsets with 2^{16} elements in the following paragraph. If we perform it, then each of the 2^{32} subsets turns into the form of the input set of the 16-round distinguisher after round 4. Accordingly, for each of the 2^{32} subsets, $\mathbf{A}^{20}$ and $\mathbf{D}^{21}$ are saturated and therefore balanced by the property of the 16-round distinguisher. For that reason, given the set of 2^{48} plaintexts $(\mathbf{A}^1, \mathbf{B}^1, \gamma^1, \mathbf{D}^1)$, $\mathbf{A}^{20}$ and $\mathbf{D}^{21}$ are always 2^{32}-saturated and therefore balanced.

Now we present that the set of the 2^{48} plaintexts can be partitioned. Let 2^{48} plaintexts $(\mathbf{A}^1, \mathbf{B}^1, \gamma^1, \mathbf{D}^1)$ be given as is stated above. We will concentrate on the data set after round 4 to partition the set of the 2^{48} plaintexts. Figure 3

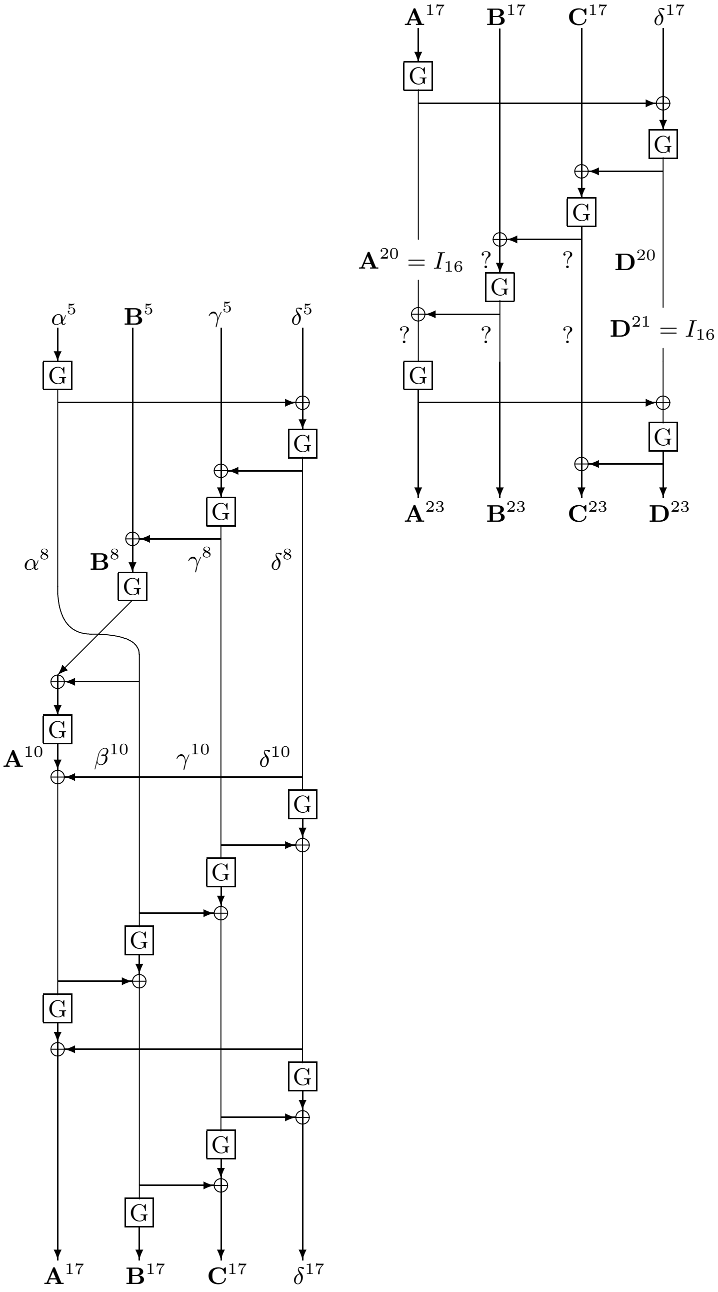

Fig. 2. 18-round(5∼22) Skipjack

describes this situation. At first, let $\alpha^5, \delta^5 \in I_{16}$ be fixed with any constant words and $\mathbf{B}^5 = I_{16}$(saturated set). Then γ^5 is determined by the equation $\mathrm{G}(\gamma^1 \oplus \delta^5) = \gamma^5$. In addition, for each $\beta_i^5 \in \mathbf{B}^5$, the corresponding tuple $(\alpha_i^1, \beta_i^1, \delta_i^1)$ is determined by the following equations.

$$\begin{aligned}\alpha_i^1 &= \mathrm{G}^{-1}(\alpha^5 \oplus \beta_i^5)\\ \beta_i^1 &= \mathrm{G}^{-1}(\beta_i^5) \oplus \gamma^5\\ \delta_i^1 &= (\alpha^5 \oplus \beta_i^5) \oplus \mathrm{G}^{-1}(\delta^5)\end{aligned}$$

If $i \neq j$ then $(\alpha_i^1, \beta_i^1, \delta_i^1) \neq (\alpha_j^1, \beta_j^1, \delta_j^1)$ holds since G is permutation. Therefore, if α^5 and $\delta^5 \in I_{16}$ are fixed and $\mathbf{B}^5$ is saturated then the number of the corresponding set $\{(\alpha_i^1, \beta_i^1, \gamma^1, \delta_i^1)|0 \leq i \leq 2^{16}-1\}$ is 2^{16}. Conversely, if the set $\{(\alpha_i^1, \beta_i^1, \gamma^1, \delta_i^1)|0 \leq i \leq 2^{16}-1\}$ is given, the corresponding set after round 4 is $(\alpha^5, \mathbf{B}^5, \gamma^5, \delta^5)$, where $\mathbf{B}^5$ is saturated, i.e., the input form of the 16-round distinguisher which is presented in section 4.1.

What's more, note that the fixed pair (α^5, δ^5) can be any one of 2^{32} elements. So, there are 2^{32} disjoint subsets of $\{(\alpha_i^1, \beta_i^1, \gamma^1, \delta_i^1)|\ 0 \leq i \leq 2^{16}-1\}_{0 \leq j \leq 2^{32}-1}$. By the explanation, we can easily obtain the fact that $(\mathbf{A}^1, \mathbf{B}^1, \gamma^1, \mathbf{D}^1)$ can be partitioned into the 2^{32} disjoint subsets of $\{(\alpha_i^1, \beta_i^1, \gamma^1, \delta_i^1)|\ 0 \leq i \leq 2^{16}-1\}_{0 \leq j \leq 2^{32}-1}$.

5 Saturation Attack

In this section, we use the distinguishers which is presented in section 4.1 and 4.2 to recover the user keys of the reduced-round versions of Skipjack.

5.1 Attack with the 16-round distinguisher

Attack on 18-round(5∼22) Skipjack It will be shown that we can recover K_{21} and K_{22} of the 18-round Skipjack(which is describe in Figure 2) using the 16-round distinguisher, where K_{21} and K_{22} are the subkeys of the round 21 and 22, respectively. Note that the attack is a chosen plaintext attack.

Let a set of 2^{16} plaintexts, $\mathsf{P} = (\alpha^5, \mathbf{B}^5, \gamma^5, \delta^5)(= \{(\alpha^5, \beta_i^5, \gamma^5, \delta^5)|0 \leq i \leq 2^{16}-1\})$ be chosen as required for the 16-round disginguisher. And ask for the corresponding set of ciphertexts, $\mathsf{C} = (\mathbf{A}^{23}, \mathbf{B}^{23}, \mathbf{C}^{23}, \mathbf{D}^{23})(= \{(\alpha_i^{23}, \beta_i^{23}, \gamma_i^{23}, \delta_i^{23})|\ 0 \leq i \leq 2^{16}-1\})$. Then the following equations hold with probability 1 by the property of the 16-round distinguisher.

$$\bigoplus_{0 \leq i \leq 2^{16}-1} \alpha_i^{20} = \bigoplus_{0 \leq i \leq 2^{16}-1} \mathrm{G}_{K_{21}}^{-1}(\alpha_i^{23}) \oplus \beta_i^{23} = 0, \quad K_{21} \in I_{32} \qquad (1)$$

$$\bigoplus_{0 \leq i \leq 2^{16}-1} \delta_i^{21} = \bigoplus_{0 \leq i \leq 2^{16}-1} \alpha_i^{23} \oplus \mathrm{G}_{K_{22}}^{-1}(\delta_i^{23}) = 0, \quad K_{22} \in I_{32} \qquad (2)$$

If K_{21} is the right subkey, it always satisfies the equation (1). While on the other, arbitrary subkey satisfies (1) with probability 2^{-16}. Since the length of

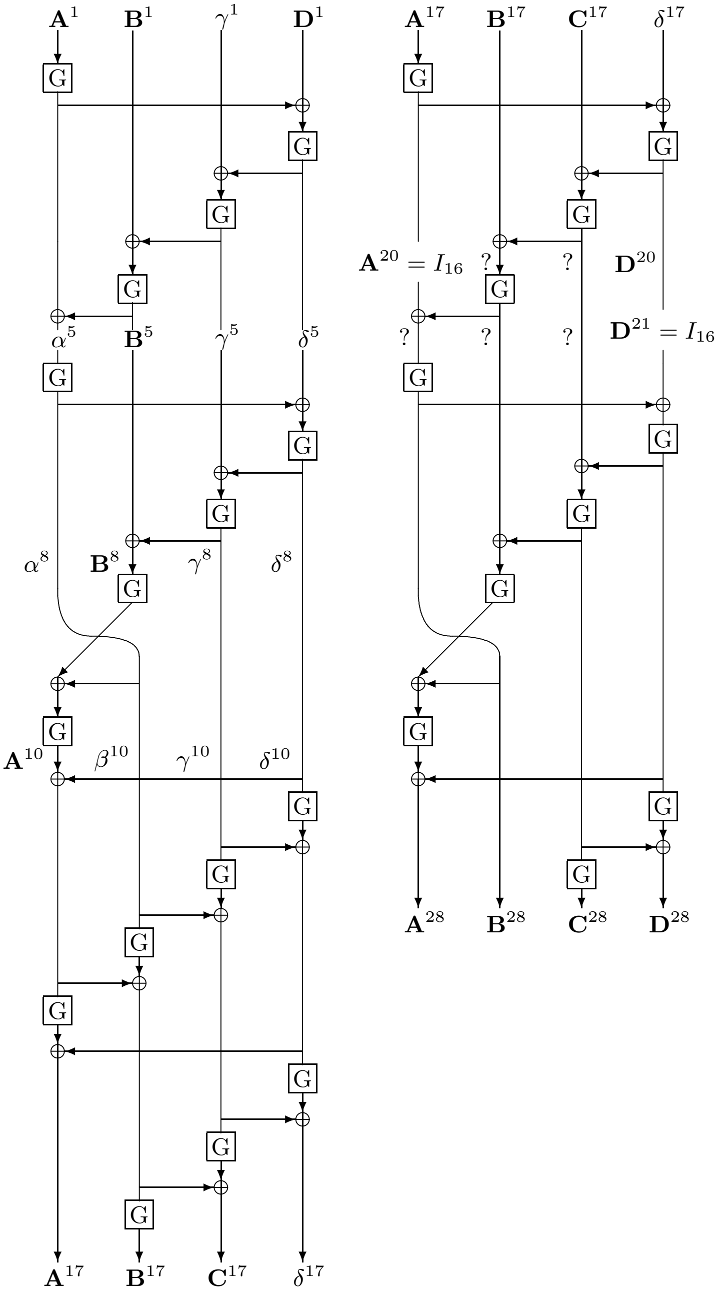

Fig. 3. 27-round(1∼27) Skipjack

the subkey is 32-bit, the number of subkeys satisfying (1) is about 2^{16}. Thus we need the other set of plaintexts to find the right subkey. For the about 2^{16} remaining candidate subkeys, if we perform the above process again with the other set of plaintexts, the only one candidate subkey remains with very high probability. Hence the subkey is almost the right key of the round 21. Also using the same way, we can find K_{22} with the equation (2). This attack can now be summarized in the following :

1. Choose two sets of 2^{16} plaintexts, $\mathsf{P}_1 = (\alpha_1^5, \mathbf{B}^5, \gamma_1^5, \delta_1^5)$, $\mathsf{P}_2 = (\alpha_2^5, \mathbf{B}^5, \gamma_2^5, \delta_2^5)$ as required for the 16-round distinguihser. Ask for the corresponding sets of ciphertexts, C_1 and C_2.
2. For each candidate subkey of K_{21}, calculate the equation (1) using P_1 and C_1.
3. For the remaining candidate subkeys after the process **2**, execute the process **2** again with P_2 and C_2.
4. Determine the remaining subkey after the process **3** as the right key.
5. Using the equation (2), find the right key K_{22} as in the previous process **2**, **3** and **4**.

The attack requires $2 \cdot 2^{16} = 2^{17}$ chosen plaintexts and the required work is about $2^{44} \simeq 2(2^{16} \cdot 2^{32} \cdot 2^{-5} + 2^{16} \cdot 2^{16} \cdot 2^{-5})$ encryption times where 2^{-5} means a G operation of Skipjack encryption. Using the simple key schedule of Skipjack, we can directly find 64 bits of all the user key bits. The remaining 16 bits can also be found by exhaustive search.

Attack on 23-round(5∼27) of Skipjack Using the 16-round distinguisher we can also recover K_{22}, K_{26} and K_{27} of the 23-round Skipjack where K_{22}, K_{26} and K_{27} are subkeys of the round 22, 26 and 27, respectively. Note that $K_{22} = K_{27}$ holds because of the simple key schedule of Skipjack.

Let a set of 2^{16} plaintexts, $\mathsf{P} = (\alpha^5, \mathbf{B}^5, \gamma^5, \delta^5)(= \{(\alpha^5, \beta_i^5, \gamma^5, \delta^5) | 0 \le i \le 2^{16}-1\})$ be chosen as required for the 16-round distinguisher. And ask for the corresponding set of ciphertexts, $\mathsf{C} = (\mathbf{A}^{28}, \mathbf{B}^{28}, \mathbf{C}^{28}, \mathbf{D}^{28})(= \{(\alpha_i^{28}, \beta_i^{28}, \gamma_i^{28}, \delta_i^{28})| \; 0 \le i \le 2^{16} - 1\})$. Then the following equation holds with probability 1 by the property of the 16-round distinguisher.

$$\bigoplus_{0 \le i \le 2^{16}-1} \delta_i^{21} = \bigoplus_{0 \le i \le 2^{16}-1} \beta_i^{28} \oplus \mathrm{G}_{K_{22}}^{-1}(\mathrm{G}_{K_{26}}^{-1}(\mathrm{G}_{K_{27}}^{-1}(\gamma_i^{28}) \oplus \delta_i^{28})) = 0 \qquad (3)$$

$$K_{22}, K_{26}, \text{ and } K_{27} \in I_{32} \quad (K_{22} = K_{27})$$

If (K_{22}, K_{26}) is the right subkey pair, it always satisfies the equation (3). Of course, K_{27} is determined by K_{22}. The probability that arbitrary subkey satisfies (3) is 2^{-16}. Since the length of the subkey pair is 64-bit at this time, the number of subkey pairs satisfying (3) is about 2^{48}. Thus we need other three sets of plaintexts to find the right subkey pair.

So, the attack requires $4 \cdot 2^{16} = 2^{18}$ chosen plaintexts and about $3 \cdot 2^{75} \simeq 2^{16} \cdot 2^{64} \cdot \frac{3}{2^5} + 2^{16} \cdot 2^{48} \cdot \frac{3}{2^5} + 2^{16} \cdot 2^{32} \cdot \frac{3}{2^5} + 2^{16} \cdot 2^{16} \cdot \frac{3}{2^5}$ encryption times. We can find 64 bits of all the user key bits using the key schedule of Skipjack. The remaining 16 bits can also be found by exhaustive search.

5.2 Attack with the 20-round distinguisher

Attack on 22-round(1∼22) of Skipjack If we use the 20-round distinguisher for attacking the 22-round Skipjack, we are able to recover K_{21} and K_{22} where K_{21} and K_{22} are the subkeys of the round 21 and 22, respectively.

Let a set of 2^{48} plaintexts, $\mathsf{P} = (\mathbf{A}^1, \mathbf{B}^1, \gamma^1, \mathbf{D}^1)(= \{(\alpha_i^1, \beta_i^1, \gamma^1, \delta_i^1) | 0 \le i \le 2^{48}-1\})$ be chosen as required for the 20-round distinguisher. And ask for the corresponding set of ciphertexts, $\mathsf{C} = (\mathbf{A}^{23}, \mathbf{B}^{23}, \mathbf{C}^{23}, \mathbf{D}^{23})(= \{(\alpha_i^{23}, \beta_i^{23}, \gamma_i^{23}, \delta_i^{23}) | 0 \le i \le 2^{48} - 1\})$. Then the following equations always hold by the property of the 20-round distinguisher. And subkey finding method is the same as in the attack on the 18-round(5∼22) Skipjack.

$$\bigoplus_{0 \le i \le 2^{48}-1} \alpha_i^{20} = \bigoplus_{0 \le i \le 2^{48}-1} \mathrm{G}_{K_{21}}^{-1}(\alpha_i^{23}) \oplus \beta_i^{23} = 0, \quad K_{21} \in I_{32} \tag{4}$$

$$\bigoplus_{0 \le i \le 2^{48}-1} \delta_i^{21} = \bigoplus_{0 \le i \le 2^{48}-1} \alpha_i^{23} \oplus \mathrm{G}_{K_{22}}^{-1}(\delta_i^{23}) = 0, \quad K_{22} \in I_{32} \tag{5}$$

Since the length of a word is 16-bit and the number of the set C is 2^{48}, for each 16-bit data channel, there must be words appeared repeatedly in the channel. For each possible word w, let the number of repetition that the word w appears in the channel be denoted by num. Then the following property holds.

$$\bigoplus_{num} w \triangleq \underbrace{w \oplus \cdots \oplus w}_{num} = \begin{cases} 0 & \text{if } num \text{ is even} \\ w & \text{if } num \text{ is odd} \end{cases} \tag{6}$$

In principle, for each candidate subkey, we need 2^{48} operations of G^{-1} function to calculate the equation (4). But using the property (6) we can reduce the complexity of the subkey finding method in the following way.

To begin with, for each possible α_i^{23}, we examine the number of repetition that the word α_i^{23} appears in the data channel. Then by this result and the property (6), we can calculate $\bigoplus_{0 \le i \le 2^{48}-1} \mathrm{G}_{K_{21}}^{-1}(\alpha_i^{23})$ with at most 2^{16} operations of G^{-1}. The summing up of this attack can be shown in the following :

1. Choose two sets of 2^{48} plaintexts, $\mathsf{P}_1 = (\mathbf{A}^1, \mathbf{B}^1, \gamma_1^1, \mathbf{D}^1)$, $\mathsf{P}_2 = (\mathbf{A}^1, \mathbf{B}^1, \gamma_2^1, \mathbf{D}^1)$ as required for the 20-round distinguisher. Ask for the corresponding sets of ciphertexts, C_1 and C_2.
2. For each candidate subkey of K_{21}, evaluate the equation (4) using P_1 and C_1 (At this time, use the property (6) to reduce the complexity of the calculation of the equation (4)).

3. For the remaining candidate subkeys after the process **2**, perform the process **2** again with P_2 and C_2.
4. Determine the remaining subkey after the process **3** as right key.
5. Using the equation (5), find the right key K_{22} as in the previous process **2**, **3** and **4**.

The attack requires $2 \cdot 2^{48} = 2^{49}$ chosen plaintexts and about $2(2^{16} \cdot 2^{32} \cdot 2^{-5} + 2^{16} \cdot 2^{16} \cdot 2^{-5}) \simeq 2^{44}$ encryption times. We can directly find 64 bits of all the user key bits using the key schedule. The remaining 16 bits can be found by exhaustive search.

Attack on 27-round(1∼27) of Skipjack Using the 20-round distinguisher we can also recover K_{22}, K_{26} and K_{27} of the 27-round Skipjack(which is describe in Figure 3) where K_{22}, K_{26} and K_{27} are subkeys of the round 22, 26 and 27, respectively. Note that $K_{22} = K_{27}$ holds.

Let a set of 2^{48} plaintexts, $\mathsf{P} = (\mathbf{A}^1, \mathbf{B}^1, \gamma^1, \mathbf{D}^1)(= \{(\alpha_i^1, \beta_i^1, \gamma^1, \delta_i^1) | 0 \le i \le 2^{48}-1\})$ be chosen as required for the 20-round distinguisher. And ask for the corresponding set of ciphertexts, $\mathsf{C} = (\mathbf{A}^{28}, \mathbf{B}^{28}, \mathbf{C}^{28}, \mathbf{D}^{28})(= \{(\alpha_i^{28}, \beta_i^{28}, \gamma_i^{28}, \delta_i^{28}) | 0 \le i \le 2^{48} - 1\})$. Then the following equation always holds by the property of the 20-round distinguisher. Subkey finding method is also the same as in the attack on the 23-round(5∼ 27) Skipjack.

$$\bigoplus_{0 \le i \le 2^{48}-1} \delta_i^{21} = \bigoplus_{0 \le i \le 2^{48}-1} \beta_i^{28} \oplus \mathrm{G}^{-1}_{K_{22}}(\mathrm{G}^{-1}_{K_{26}}(\mathrm{G}^{-1}_{K_{27}}(\gamma_i^{28}) \oplus \delta_i^{28})) = 0 \qquad (7)$$

$$K_{22}, K_{26}, \text{ and } K_{27} \in I_{32} \quad (K_{22} = K_{27})$$

The attack requires $4 \cdot 2^{48} = 2^{50}$ chosen plaintexts and about $2^{16} \cdot 2^{64} \cdot \frac{3}{2^5} + 2^{16} \cdot 2^{48} \cdot \frac{3}{2^5} + 2^{16} \cdot 2^{32} \cdot \frac{3}{2^5} + 2^{16} \cdot 2^{16} \cdot \frac{3}{2^5} \simeq 3 \cdot 2^{75}$ encryption times. Using the key schedule, we can find 64 bits of the user key. The remaining 16 bits can be found by exhaustive search.

rounds	plaintexts	running time
18(5∼22)	2^{17}	2^{44}
22(5∼26)	2^{18}	2^{76}
23(5∼27)	2^{18}	$3 \cdot 2^{75}$
22(1∼22)	2^{49}	2^{44}
26(1∼27)	2^{50}	2^{76}
27(1∼27)	2^{50}	$3 \cdot 2^{75}$

Table 2. Complexities of Saturation Attacks Against Reduced-Round Skipjack

6 Conclusion

In this paper we have described saturation attacks on reduced-round versions of Skipjack. We have showed how to construct a 16-round distinguisher. The distinguisher can be used to attack on 18(5∼22) and 23(5∼27) rounds of Skipjack. We could also construct a 20-round distinguisher based on the 16-round distinguisher. This distinguisher can be used to attack on 22(1∼22) and 27(1∼27) rounds of Skipjack. The complexities of these attacks are summarized in table 2. It should be emphasized that our attacks do not improve on the impossible differential attacks[5]. But this paper shows how to apply saturation attack to Skipjack for the first time.

Acknowledgment

We would like to thank Seokhie Hong and Jaechul Sung for many helpful discussions.

References

1. E. Biham, A. Biryukov, O. Dunkelmann, E. Richardson and A. Shamir, *Initial Observations on the Skipjack Encryption Algorithm*, June 25, 1998. Available at http://www.cs.technion.ac.il/ ∼biham/Reports/Skipjack/.
2. E. Biham, A. Biryukov, O. Dunkelmann, E. Richardson and A. Shamir, *Cryptanalysis of Skipjack-3XOR in* 2^{20} *time and using* 2^{9} *chosen plaintexts*, July 2, 1998. Available at http:// www.cs.technion.ac.il/∼biham/Reports/Skipjack/.
3. E. Biham, A. Biryukov, O. Dunkelmann, E. Richardson and A. Shamir, *Cryptanalysis of Skipjack-4XOR*, June 30, 1998. Available at http://www.cs.technion.ac.il/∼biham/Reports/Skipjack/.
4. E. Biham, A. Biryukov, and A. Shamir, *Initial Observations on the Skipjack : Cryptanalysis of Skipjack-3XOR*, SAC'98, 1998. Available at http://www.cs.technion.ac.il/∼biham/Reports/ Skipjack/.
5. Eli Biham, Alex Biryukov, and Adi Shamir, *Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials*, EUROCRYPT'99, LNCS 1592, Springer-Verlag, 1999 pp. 12–23. Available at http://www.cs.technion.ac.il/∼biham/Reports/Skipjack/.
6. Lars R. Knudsen, M.J.B. Robshaw, and David Wagner, *Truncated differentials and Skipjack*, CRYPTO'99, LNCS 1666, Springer-Verlag, August 1999 pp. 165–180.
7. Louis Granboulan, *Flaws in differential Cryptanalysis of Skipjack*, Fast Software Encryption Workshop 2001, LNCS 1039, Springer-Verlag April, 2001, pp. 341–346.
8. S. Lucks, *The Saturation Attack - a Bait for Twofish*, Fast Software Encryption Workshop 2001, LNCS 1039, Springer-Verlag, 2001, pp. 189–203
9. National Institute of Standards and Technology, *Skipjack and KEA Algorithm Specifications, version 2.0*, Available at http://crsc.nist.gov/encryption/skipjack-kea.htm.
10. National Institute of Standards and Technology, *NSA Releases Fortezza Algorithms*, Available at http://crsc.nist.gov/encryption/encryption/nsa-press.pdf.