Square Attacks on Reduced-Round Variants of the Skipjack Block Cipher

Jorge Nakahara Jr*, Bart Preneel, Joos Vandewalle

Katholieke Universiteit Leuven, Dept. ESAT
Kasteelpark Arenberg 10, B–3001 Leuven–Heverlee, Belgium
{jorge.nakahara,bart.preneel,joos.vandewalle}@esat.kuleuven.ac.be

Version 1.11
Jan. 8, 2002

Abstract. This report surveys on a series of Square attacks on reduced-round versions of the Skipjack block cipher. **Skipjack** is an iterated block cipher encrypting 64-bit plaintext blocks into 64-bit ciphertext blocks, using an 80-bit key. Its design is based on a generalized Feistel Network making up 32 rounds of two different types. This cipher was developed by the National Security Agency for the Clipper chip and Fortezza PC card.

1 Introduction

This report is organized as follows: Sect.1 describes the Skipjack block cipher, the round structure, the encryption and decryption networks, and the key schedule. Sect.2 describes the main features used in a Square attack, and how it works. Sect.3 describes variants of the Square attack on reduced-round versions of Skipjack. Sect. 4 describes chosen-ciphertext attacks on reduced-round variants of Skipjack. Sect.6 summarizes the results in this report. Sect.7 contains ideas for further research.

Skipjack is an iterated 64-bit block cipher. Its design is based on an Unbalanced Feistel Network[2]. Skipjack iterates 32 rounds of two types called Rule-A and Rule-B.

Let $W^i = (w_1^i, w_2^i, w_3^i, w_4^i)$ be the input block to the i-th round, $0 \leq i \leq 31$. The round output block W^{i+1}, according to each rule, is computed according to Table 1. The plaintext block has index $i = 0$ and the ciphertext block has index $i = 32$. The main component of each kind of round is a non-linear keyed permutation G^i, where $0 \leq i \leq 31$ is the round number.

For encryption, the rounds are ordered as follows: first, eight Rule-A rounds, followed by eight Rule-B rounds, followed again by eight Rule-A rounds and finally eight more Rule-B rounds. Fig. 1 shows the Feistel Network of Skipjack and the untwisted network is presented in Fig. 2.

* sponsored in part by GOA project Mefisto 2000/06

Table 1. Description of Rule-A and Rule-B rounds and their inverses.

Rule-A round ($0 \leq i \leq 7; 16 \leq i \leq 23$)	Rule-B round ($8 \leq i \leq 15; 24 \leq i \leq 31$)
$w_1^{i+1} = \mathrm{G}^i(w_1^i) \oplus w_4^i \oplus (i+1)$	$w_1^{i+1} = w_4^i$
$w_2^{i+1} = \mathrm{G}^i(w_1^i)$	$w_2^{i+1} = \mathrm{G}^i(w_1^i)$
$w_3^{i+1} = w_2^i$	$w_3^{i+1} = w_1^i \oplus w_2^i \oplus (i+1)$
$w_4^{i+1} = w_3^i$	$w_4^{i+1} = w_3^i$
Rule-A^{-1} round ($0 \leq i \leq 7; 16 \leq i \leq 23$)	Rule-B^{-1} round ($8 \leq i \leq 15; 24 \leq i \leq 31$)
$w_1^{i-1} = \mathrm{G}^{-i}(w_2^i)$	$w_1^{i-1} = \mathrm{G}^{-i}(w_2^i)$
$w_2^{i-1} = w_3^i$	$w_2^{i-1} = \mathrm{G}^{-i}(w_2^i) \oplus w_3^i \oplus (i+1)$
$w_3^{i-1} = w_4^i$	$w_3^{i-1} = w_4^i$
$w_4^{i-1} = w_1^i \oplus w_2^i \oplus (i+1)$	$w_4^{i-1} = w_1^i$

It was observed by Biham et.al. in [5] that in Rule-A rounds the output of one G^i function is exclusive-ored with the input to the next round G^{i+1} function, similar to Rule-B^{-1} rounds. But, in Rule-B rounds the input to a G^i function does not depend on the output of the previous G^{i-1} function (only on the input of G^{i-4} function), and similarly for Rule-A^{-1} rounds. It means that Rule-A and Rule-B^{-1} rounds provide better diffusion and contribute more to the avalanche effect than Rule-A^{-1} and Rule-B rounds. Algebraic expressions of the four 16-bit output words after *eight* Rule-A or Rule-B^{-1} rounds confirm that all four outputs depend on all input words and key bytes through the G^i (or G^{-i}) functions. For Rule-B and Rule-A^{-1} rounds, though, *twelve* rounds at least are needed to achieve complete diffusion of every input block and key byte.

A fixed counter value, $i+1$, is exclusive-ored at round $i, 0 \leq i \leq 31$. It was observed by Biham et.al. in [5] that their presence protects against related-key attacks.

Another observation is that all operations in Skipjack can, ultimately, be carried out byte-wise, that is, there are neither bit-level operations, like in DES [9], nor cipher components which operate on quantities smaller than a byte.

1.1 The G^i Function

The $\mathrm{G}^i : \mathbb{Z}_2^{16} \times (\mathbb{Z}_2^8)^4 \rightarrow \mathbb{Z}_2^{16}$ function consists of a four-round balanced Feistel Network[2]. Each internal round of G^i uses a fixed permutation $\mathrm{F} : \mathbb{Z}_2^8 \rightarrow \mathbb{Z}_2^8$ called F-table. Let the concatenation of a pair of bytes, denoted $g_1||g_2$, be the input to G^i, and $(k_{4i \bmod 10}, k_{4i+1 \bmod 10}, k_{4i+2 \bmod 10}, k_{4i+3 \bmod 10})$ be the subkey bytes used in the i-th round, $0 \leq i \leq 31$. The four internal rounds of $\mathrm{G}^i(g_1||g_2)$ compute:

$$g_3 = \mathrm{F}(g_2 \oplus k_{4i \bmod 10}) \oplus g_1$$
$$g_4 = \mathrm{F}(g_3 \oplus k_{4i+1 \bmod 10}) \oplus g_2$$

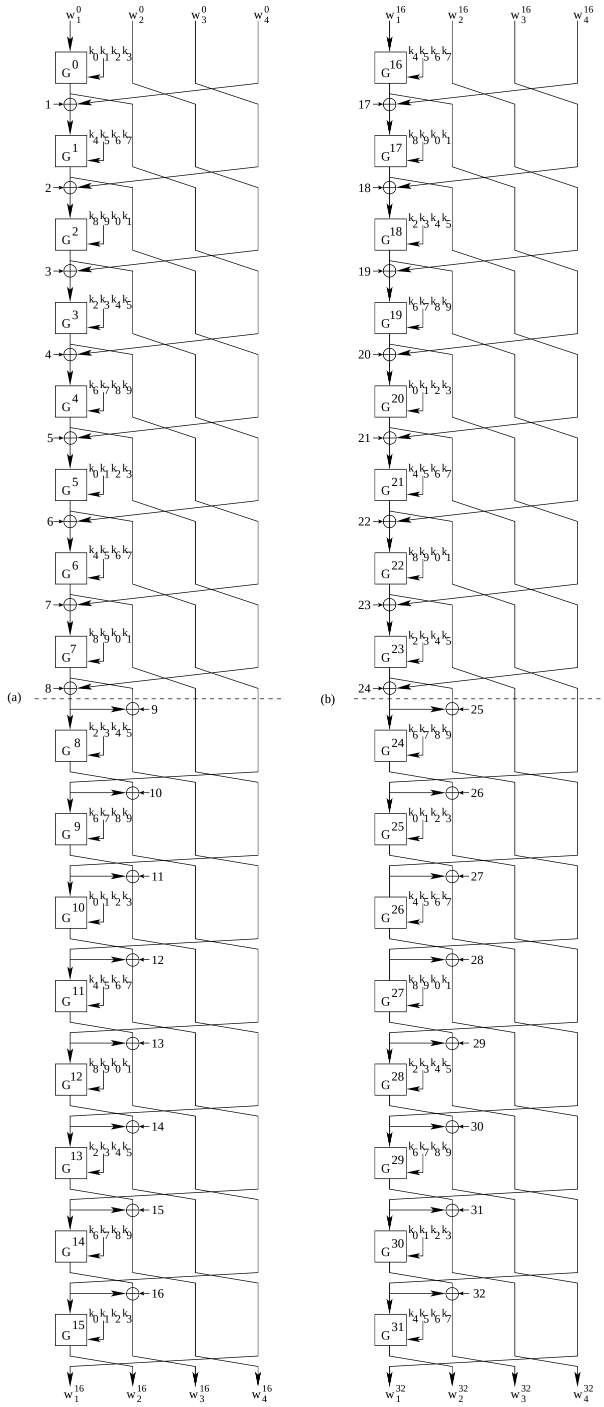

Fig. 1. Encryption mode of Skipjack: (a) first 16 rounds and (b) last 16 rounds.

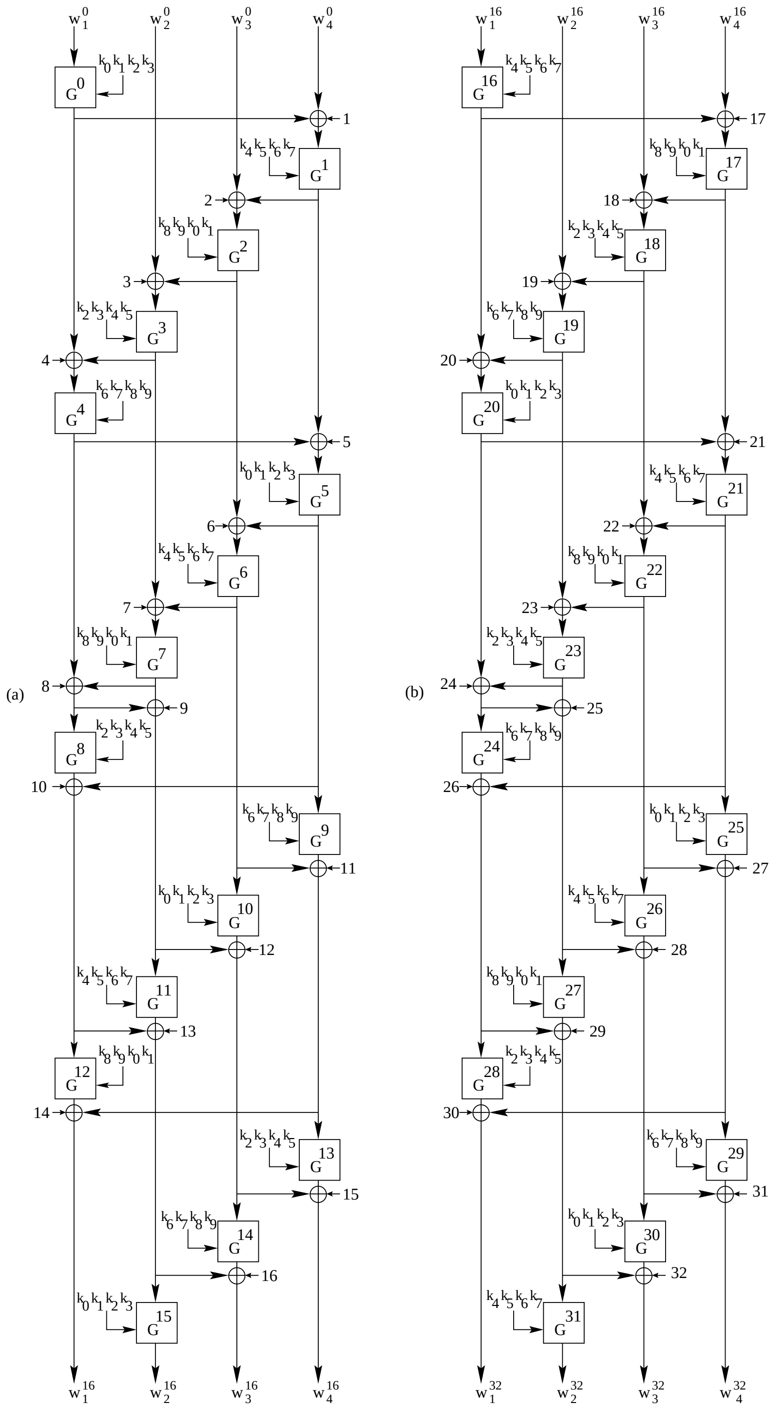

Fig. 2. Untwisted Skipjack network for encryption: (a) first 16 rounds, (b) last 16 rounds.

$g_5 = \mathrm{F}(g_4 \oplus k_{4i+2 \bmod 10}) \oplus g_3$
$g_6 = \mathrm{F}(g_5 \oplus k_{4i+3 \bmod 10}) \oplus g_4$

Therefore, $\mathrm{G}^i(g_1||g_2) = g_5||g_6$. Similarly, $\mathrm{G}^{-i}(g_5||g_6) = g_1||g_2$. Both schemes are depicted in Fig. 3.

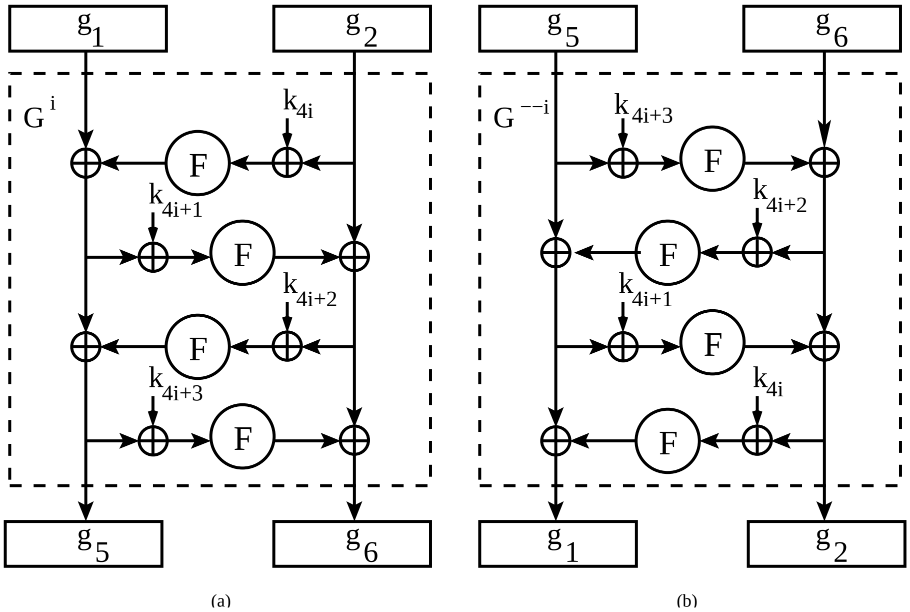

Fig. 3. Internal structure of: (a) permutation G^i and (b) its inverse G^{-i}.

The structure of G^i has asymetric diffusion: g_5 depends on g_1, g_2, $k_{4i \bmod 10}$, $k_{4i+1 \bmod 10}$ and $k_{4i+2 \bmod 10}$ but not on $k_{4i+3 \bmod 10}$, while g_6 depends on both inputs and on all four subkeys.

1.2 Decryption

Decryption in Skipjack consists of iterating the ciphertext through eight Rule-B^{-1} rounds, followed by eight Rule-A^{-1} rounds, followed by eight more Rule-B^{-1} rounds, and finally eight Rule-A^{-1} rounds, with the subkeys in reverse order. Although dissimilar to encryption, it was observed in [5] that decryption can be accomplished using the same structure as for encryption (Fig.1) with some appropriate byte reordering. If the plaintext block is denoted $P = (p_0, p_1, p_2, p_3, p_4, p_5, p_6, p_7)$, the user-key by $K = (k_0, k_1, k_2, k_3, k_4, k_5, k_6, k_7, k_8, k_9)$ and the corresponding ciphertext by $C = (c_0, c_1, c_2, c_3, c_4, c_5, c_6, c_7)$, then decryption consists in:

– reversing the order of the round counters, and
– encrypting the reordered ciphertext $C^* = (c_3, c_2, c_1, c_0, c_7, c_6, c_5, c_4)$, under the user-key $K^* = (k_7, k_6, k_5, k_4, k_3, k_2, k_1, k_0, k_9, k_8)$, resulting in the plaintext $P^* = (p_3, p_2, p_1, p_0, p_7, p_6, p_5, p_4)$

1.3 The Key Schedule

The key schedule of Skipjack uses four consecutive user-key bytes per round, in a cyclic fashion. Let $K = (k_0, k_1, k_2, k_3, k_4, k_5, k_6, k_7, k_8, k_9)$ be the 80-bit master key. Then, the i-th round subkey, $0 \leq i \leq 31$, is given by $(k_{4i \bmod 10}, k_{(4i+1) \bmod 10}, k_{(4i+2) \bmod 10}, k_{(4i+3) \bmod 10})$. As depicted in the left half of Table 2, the same set of four key bytes is repeated every five rounds. Besides, the key bytes which enter the G^i function can be distinguished as odd or even key bytes. If the internal rounds of G^i are numbered from 0 to 3, then the even-numbered key bytes $k_{4i \bmod 10}$, and $k_{(4i+2) \bmod 10}$ always enter the even-numbered rounds, while the odd-numbered key bytes $k_{(4i+1) \bmod 10}$, and $k_{(4i+3) \bmod 10}$ always enter the odd-numbered rounds. In order to simplify notation the reduction of the subkey index modulo 10 will be dropped from now on but it should be understood that the subkeys are taken as successive bytes of the master key taken in cyclic order.

An interesting observation about the key schedule is: if the key size were 72 bits or 9 bytes, and the key schedule were the same then the period of the subkeys would be 9. If the key size were 88 bits or 11 bytes, then the period would increase to 11.

Another observation is that, if all even-numbered key bytes were the same, as well as all odd-numbered key bytes then all round subkeys would be equal, for example, (k_0, k_1, k_0, k_1). There are only 2^{16} such keys that can be generated by the key schedule of Skipjack. These keys could allow a kind of slide attack [1], if it was not for the presence of two different kinds of rounds, which provides asymmetry in the cipher, independent of the round keys.

An interesting property, based on the bytewise structure of Skipjack, on the group operation used to mix the counter values (exclusive-or), and the fact that the counter values range from 1 to 32, is that an equivalent Feistel Network for Skipjack, with a more regular structure can be obtained, for example, by moving the counter values either upward till the plaintext, or downward till the ciphertext bytes.

Let the plaintext $P = (w_1^0, w_2^0, w_3^0, w_4^0)$, $w_i^0 \in \mathbb{Z}_2^{16}$ be encrypted, using Skipjack, to $C = (w_1^{32}, w_2^{32}, w_3^{32}, w_4^{32})$ under a key $K = (k_0, k_1, k_2, k_3, k_4, k_5, k_6, k_7, k_8, k_9)$, using the subkeys in the left half of Table 2. One equivalent network, which *moves* all the counters downward till the ciphertext, uses the transformed subkeys in the right half of Table 2, that is, the counters are mixed via exclusive-or with the original Skipjack key bytes. See Fig.4. Interestingly, only the even-numbered subkey bytes are affected. This equivalent transformation takes P to the ciphertext $C' = (w_0^{32}, w_1^{32}, w_2^{32} \oplus 3c_x, w_4^{32} \oplus 14_x)$. The subscript $_x$ denotes an hexadecimal value.

Table 2. Key schedule of Skipjack

Round	Subkey bytes					Equivalent Subkeys			
0	k_0	k_1	k_2	k_3		k_0	k_1	k_2	k_3
1	k_4	k_5	k_6	k_7	R	$k_4 \oplus 01_x$	k_5	$k_6 \oplus 01_x$	k_7
2	k_8	k_9	k_0	k_1	u	$k_8 \oplus 03_x$	k_9	$k_0 \oplus 03_x$	k_1
3	k_2	k_3	k_4	k_5	l	k_2	k_3	k_4	k_5
4	k_6	k_7	k_8	k_9	e	$k_6 \oplus 04_x$	k_7	$k_8 \oplus 04_x$	k_9
5	k_0	k_1	k_2	k_3		k_0	k_1	k_2	k_3
6	k_4	k_5	k_6	k_7	A	$k_4 \oplus 05_x$	k_5	$k_6 \oplus 05_x$	k_7
7	k_8	k_9	k_0	k_1		$k_8 \oplus 02_x$	k_9	$k_0 \oplus 02_x$	k_1
8	k_2	k_3	k_4	k_5		$k_2 \oplus 0e_x$	k_3	$k_4 \oplus 0e_x$	k_5
9	k_6	k_7	k_8	k_9	R	k_6	k_7	k_8	k_9
10	k_0	k_1	k_2	k_3	u	$k_0 \oplus 05_x$	k_1	$k_2 \oplus 05_x$	k_3
11	k_4	k_5	k_6	k_7	l	$k_4 \oplus 05_x$	k_5	$k_6 \oplus 05_x$	k_7
12	k_8	k_9	k_0	k_1	e	$k_8 \oplus 04_x$	k_9	$k_0 \oplus 04_x$	k_1
13	k_2	k_3	k_4	k_5		$k_2 \oplus 0e_x$	k_3	$k_4 \oplus 0e_x$	k_5
14	k_6	k_7	k_8	k_9	B	$k_6 \oplus 0c_x$	k_7	$k_8 \oplus 0c_x$	k_9
15	k_0	k_1	k_2	k_3		$k_0 \oplus 0c_x$	k_1	$k_2 \oplus 0c_x$	k_3
16	k_4	k_5	k_6	k_7		$k_4 \oplus 04_x$	k_5	$k_6 \oplus 04_x$	k_7
17	k_8	k_9	k_0	k_1	R	$k_8 \oplus 18_x$	k_9	$k_0 \oplus 18_x$	k_1
18	k_2	k_3	k_4	k_5	u	$k_2 \oplus 1a_x$	k_3	$k_4 \oplus 1a_x$	k_5
19	k_6	k_7	k_8	k_9	l	$k_6 \oplus 05_x$	k_7	$k_8 \oplus 05_x$	k_9
20	k_0	k_1	k_2	k_3	e	$k_0 \oplus 15_x$	k_1	$k_2 \oplus 15_x$	k_3
21	k_4	k_5	k_6	k_7		$k_4 \oplus 18_x$	k_5	$k_6 \oplus 18_x$	k_7
22	k_8	k_9	k_0	k_1	A	$k_8 \oplus 14_x$	k_9	$k_0 \oplus 14_x$	k_1
23	k_2	k_3	k_4	k_5		$k_2 \oplus 06_x$	k_3	$k_4 \oplus 06_x$	k_5
24	k_6	k_7	k_8	k_9		$k_6 \oplus 0b_x$	k_7	$k_8 \oplus 0b_x$	k_9
25	k_0	k_1	k_2	k_3	R	$k_0 \oplus 18_x$	k_1	$k_2 \oplus 18_x$	k_3
26	k_4	k_5	k_6	k_7	u	$k_4 \oplus 14_x$	k_5	$k_6 \oplus 14_x$	k_7
27	k_8	k_9	k_0	k_1	l	$k_8 \oplus 14_x$	k_9	$k_0 \oplus 14_x$	k_1
28	k_2	k_3	k_4	k_5	e	$k_2 \oplus 09_x$	k_3	$k_4 \oplus 09_x$	k_5
29	k_6	k_7	k_8	k_9		$k_6 \oplus 17_x$	k_7	$k_8 \oplus 17_x$	k_9
30	k_0	k_1	k_2	k_3	B	$k_0 \oplus 1c_x$	k_1	$k_2 \oplus 1c_x$	k_3
31	k_4	k_5	k_6	k_7		k_4	k_5	k_6	k_7

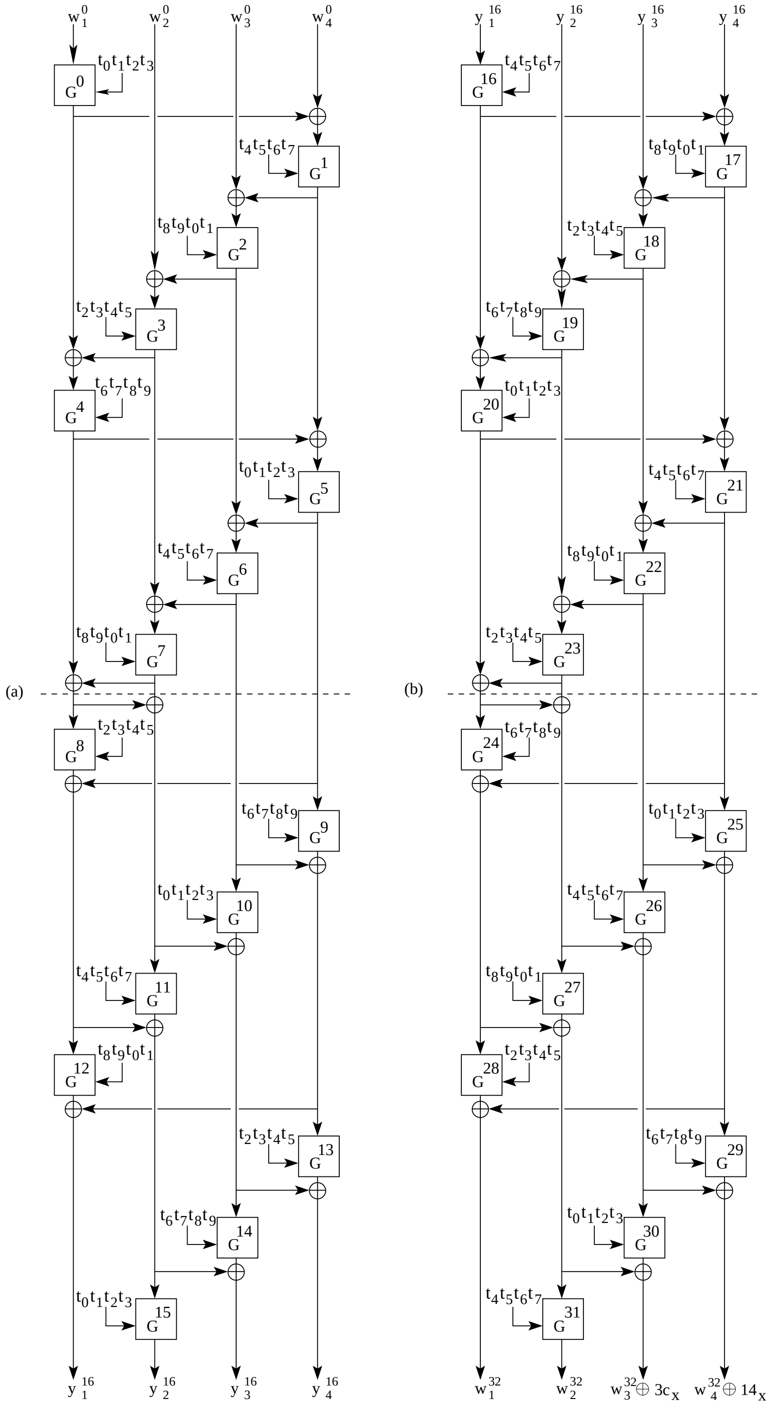

Fig. 4. An equivalent Skipjack network: (a) first 16 rounds, and (b) last 16 rounds.

2 The Square Attack: General Definitions

Former analyses of Skipjack were reported in [13, 12, 5, 14, **?**]. This report will focus on variants of the Square attack applied to Skipjack.

The Square attack is a *chosen-plaintext attack* originally applied against reduced-round versions of block ciphers of the *Square* family (see [10, 18, 3, 11]). This attack explores the structure of *Square*, but can also be used to analyse other block ciphers where the input block to a round is neatly partitioned into smaller, fixed-size component *words*.

Definition 1. *An* active *word is an n-bit quantity which assumes all 2^n possible values $0 \ldots 2^n - 1$. An active word contains, therefore, a permutation of 2^n values. Analogously, a* passive *word always assumes a fixed value. State bytes which are neither active not passive are termed* garbled.

Definition 2. *A Λ-set is a set of 2^n text blocks in which its n-bit words are either active or passive or garbled.*

Definition 3. *(Distinguishing Property in a Λ-set)*
Let x_i^j be the j-th value of the i-th word in a Λ-set. Assume words have n bits. If

$$\bigoplus_{j=0}^{2^n-1} x_i^j = 0$$

then the word x_i is said to be balanced *over the Λ-set.*

The number of text blocks in a Λ-set depends on the word size. For *Square*, where the cipher operations work on eight bits, a Λ-set consists typically of 2^8 blocks; for Skipjack, in attacks using 16-bit words, a Λ-set will consist of 2^{16} blocks. Although Skipjack is a byte-oriented cipher, the word size, for a Square attack, was chosen as $n = 16$ bits, because, smaller word sizes do not retain the distinguishing property for as many rounds as 16-bit words (see Fig. 5). Exhaustive analysis of all 256 patterns of plaintext Λ-sets consisting of 8-bit active/passive words indicate that the best (longer) pattern reaches six Rule-A rounds:

$$\begin{aligned}(P\ P\ A\ P\ P\ P\ P\ P) &\xrightarrow{\text{A}} (P\ P\ A\ P\ P\ P\ P\ P) \xrightarrow{\text{A}} (P\ P\ A\ P\ P\ P\ P\ P) \xrightarrow{\text{A}} \\ (P\ P\ A\ P\ P\ P\ P\ P) &\xrightarrow{\text{A}} (*\ ?\ *\ ?\ P\ P\ P\ P) \xrightarrow{\text{A}} \quad (?\ ?\ *\ ?\ P\ P\ ?\ ?) \xrightarrow{\text{A}} \\ (?\ ?\ *\ ?\ ?\ ?\ ?\ ?) &\xrightarrow{\text{A}} (?\ ?\ ?\ ?\ ?\ ?\ ?\ ?) \end{aligned} \tag{1}$$

Since F is an 8×8-bit permutation, and the exclusive-or with a fixed value also makes a permutation, the G^i and G^{-i} functions are 16×16-bit permutations for any 4-tuple of subkey bytes $(k_{4i \bmod 10},\ k_{4i+1 \bmod 10},\ k_{4i+2 \bmod 10},\ k_{4i+3 \bmod 10})$. Therefore, preliminary analyses indicate 16 bits to be an adequate word size

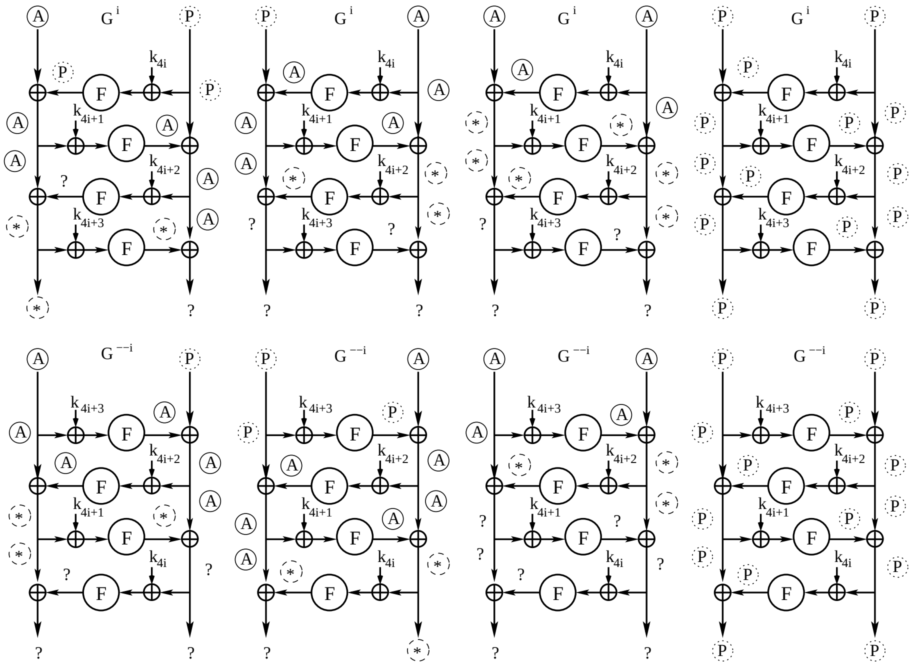

Fig. 5. Propagation of 8-bit active words in G^{i} and G^{-i}. See terminology in Sect.3.

for an initial Square attack. It is interesting to notice that the Square attack is independent of the F-table, or it inverse. All that is required is that it is an 8×8-bit permutation.

Both active and passive words satisfy the distinguishing criterium, although the active ones satisfy the property due to the fact that they form a permutation, while the passive words because all values are equal. Garbled words can also be balanced but usually they are not.

A typical attack starts by carefully choosing a Λ-set that propagates across the cipher until all words are garbled. By tracking the propagation of the active words through a round, it is possible to identify a pattern of active and passive words at the output of several rounds. This pattern contains a set of balanced words. The balanced words are subsequently used to distinguish subkeys in the outer rounds, either the first or the last round subkeys.

3 Square Attacks on Skipjack

Let $P^i = (P_1^i, P_2^i, P_3^i, P_4^i)$, with $P_j^i \in \mathbb{Z}_2^{16}$, $1 \leq j \leq 4$, $0 \leq i < 2^{16}$, be the plaintext blocks in a plaintext Λ-set, for 16-bit active words. A plaintext Λ-set is a set of inputs to Skipjack, and an ciphertext Λ-set is the corresponding set of ciphertext blocks. Let $C^i = (C_1^i, C_2^i, C_3^i, C_4^i)$ denote the ciphertext blocks in the Λ-set corresponding to P^i. Λ-sets will be identified only by the status of its component words: either *“A”* for *active*, *“P”* for *passive*, *“*”* for *balanced* or *“?”*

for garbled words. For example, the terminology $(A\ A\ A\ A) \stackrel{\mathrm{A}}{\to} (A\ A\ ?\ ?)$ will denote that the Λ-set $X = (A\ A\ A\ A)$ (with all of its words active) *results* in the Λ-set $Y = (A\ A\ ?\ ?)$ (with two active and two garbled words) after one Rule-A round. This one-round relationship holds with probability one.

Analogously, $(A\ A\ A\ A) \stackrel{\mathrm{B}}{\to} (A\ A\ ?\ ?)$ means that the Λ-set $X = (A\ A\ A\ A)$ results in the Λ-set $Y = (A\ A\ ?\ ?)$ after one Rule-B round. Multiple-round relations, in a chain, like for example, $X \stackrel{\mathrm{A}}{\to} Y \stackrel{\mathrm{A}}{\to} Z$ will denote a shortcut notation for $X \stackrel{\mathrm{A}}{\to} Y$ and $Y \stackrel{\mathrm{A}}{\to} Z$. This notation will also implicitly indicate where an attack actually starts in the Feistel Network of Skipjack. Usually, Λ-sets are applied to the first Rule-A round of Skipjack, but some variants may start at the second, third, or further rounds. These variant attacks aim at exploring the different diffusion properties of Rule-A and Rule-B rounds. The exact starting round for an attack should become clear from the notation.

Definition 4. *(nR-Attack)*
An nR-attack denotes, in the present context, a Square attack that discovers subkey(s) of n round(s), using Λ-set(s) and the distinguishing property to identify the correct subkeys.

The following is a list of the different Λ-sets that were analyzed, exhaustivelly, by making progressively more and more words active, starting from the first Rule-A round of Skipjack.

$$(A\ P\ P\ P) \stackrel{\mathrm{A}}{\to} (A\ P\ P\ A) \stackrel{\mathrm{A}}{\to} (A\ P\ A\ A) \stackrel{\mathrm{A}}{\to} (A\ A\ A\ A) \stackrel{\mathrm{A}}{\to} (*\ A\ A\ A) \stackrel{\mathrm{A}}{\to} (?\ A\ A\ ?) \stackrel{\mathrm{A}}{\to} (?\ A\ ?\ ?) \stackrel{\mathrm{A}}{\to} (?\ ?\ ?\ ?) \tag{2}$$

Although the chain of Λ-sets (2) covers the initial seven rounds of Skipjack, it is possible to do a 1R-attack on the initial eight rounds (see Fig.6). The ciphertext blocks $C^i = (C_1^i, C_2^i, C_3^i, C_4^i)$ are the outputs of the 8th Rule-A round. The attack guesses subkey bytes k_8, k_9, k_0, k_1 and checks if $\mathrm{G}^{-7}(C_2^i) \oplus C_3^i$ is an active word. A wrong 32-bit subkey candidate has probability of 2^{-16} of being balanced. To avoid false alarms, three plaintext Λ-sets are used. The chance that a wrong subkey passes the distinguishing test is $(2^{-16})^3 = 2^{-48}$ and thus, only the correct subkey is likely to remain. The passive plaintext words P_2^i, P_3^i, and P_4^i, and in all subsequent attacks, unless explicitly mentioned, are set to 0 (a fixed arbitrary value). The complexity of the attack is $2^{16} \cdot 2^{32} \cdot 2^{-5} + 2^{16} \cdot 2^{16} \cdot 2^{-5} + 2^{16} \cdot 2^{-5} \approx 2^{43}$ full Skipjack encryptions. The factor 2^{-5} corresponds to one evaluation of the G^i function which costs roughly 1/32 of the full Skipjack network evaluation.

$$(P\ A\ P\ P) \stackrel{\mathrm{A}}{\to} (P\ A\ P\ P) \stackrel{\mathrm{A}}{\to} (P\ A\ P\ P) \stackrel{\mathrm{A}}{\to} (P\ A\ P\ P) \stackrel{\mathrm{A}}{\to} (A\ A\ P\ P) \stackrel{\mathrm{A}}{\to} (A\ A\ P\ A) \stackrel{\mathrm{A}}{\to} (A\ A\ A\ A) \stackrel{\mathrm{A}}{\to} (A\ *\ A\ A) \stackrel{\mathrm{A}}{\to} (?\ ?\ A\ A) \stackrel{\mathrm{B}}{\to} (?\ A\ A\ A) \stackrel{\mathrm{B}}{\to} (?\ A\ A\ A) \stackrel{\mathrm{B}}{\to} (?\ A\ A\ *) \stackrel{\mathrm{B}}{\to} (?\ A\ *\ *) \stackrel{\mathrm{B}}{\to} (?\ ?\ *\ *) \stackrel{\mathrm{B}}{\to} (?\ ?\ *\ ?) \stackrel{\mathrm{B}}{\to} (?\ ?\ ?\ ?) \tag{3}$$

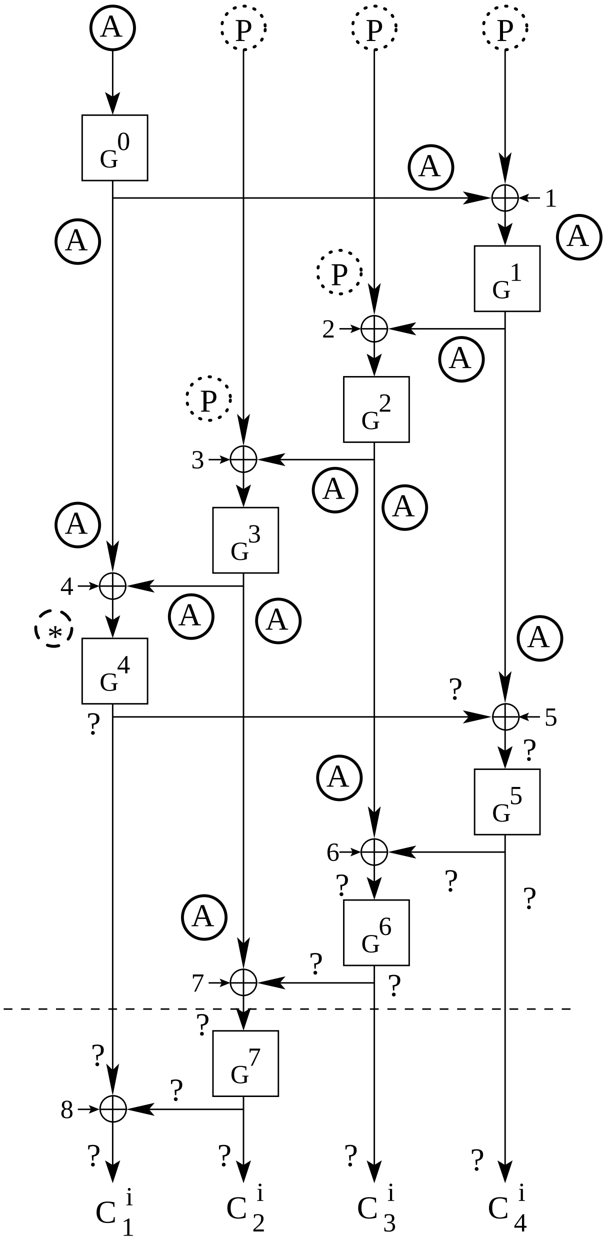

Fig. 6. Propagation of Λ-sets according to chain (2).

A 2R-attack on 16 rounds of Skipjack, using the chain (3) of Λ-sets, discovers subkey bytes k_0, k_1, k_2, k_3, k_6, k_7, k_8, k_9 by checking if $\mathrm{G}^{-14}(\mathrm{G}^{-15}(C_2^i) \oplus C_3^i)$ is balanced (see Fig. 7). One plaintext Λ-set gives only one 16-bit word to test for balance, and this attack in particular guesses 64 subkey bits at a time. To filter out false subkey candidates, five Λ-sets are used. The complexity is $2^{16} \cdot 2^{64} \cdot 2 \cdot 2^{-5} + 2^{16} \cdot 2^{48} \cdot 2 \cdot 2^{-5} + 2^{16} \cdot 2^{32} \cdot 2 \cdot 2^{-5} + 2^{16} \cdot 2^{16} \cdot 2 \cdot 2^{-5} + 2^{16} \cdot 2 \cdot 2^{-5} \approx 2^{76}$ full Skipjack encryptions.

A variant 1R-attack can be used to discover only k_6, k_7, k_8, k_9, covering 15 rounds. The attack discovers 32 key bits and verify if $\mathrm{G}^{-14}(C_3^i)$ is balanced. To filter out wrong 32-bit subkey candidates, three plaintext Λ-sets are used. The complexity is $2^{16} \cdot 2^{32} \cdot 2^{-5} + 2^{16} \cdot 2^{16} \cdot 2^{-5} + 2^{16} \cdot 2^{-5} \approx 2^{43}$ full Skipjack encryptions.

$$\begin{aligned}(P\ P\ A\ P) &\xrightarrow{\mathrm{A}} (P\ P\ A\ P) \xrightarrow{\mathrm{A}} (P\ P\ A\ P) \xrightarrow{\mathrm{A}} (P\ A\ A\ P) \xrightarrow{\mathrm{A}} (A\ A\ A\ P) \xrightarrow{\mathrm{A}} \\ &(A\ A\ A\ A) \xrightarrow{\mathrm{A}} (A\ A\ *\ A) \xrightarrow{\mathrm{A}} (A\ ?\ ?\ A) \xrightarrow{\mathrm{A}} (?\ ?\ ?\ A) \xrightarrow{\mathrm{B}} (?\ A\ ?\ A) \xrightarrow{\mathrm{B}} \\ &(?\ A\ ?\ A) \xrightarrow{\mathrm{B}} (?\ A\ ?\ ?) \xrightarrow{\mathrm{B}} (?\ A\ ?\ ?) \xrightarrow{\mathrm{B}} (?\ ?\ ?\ ?)\end{aligned} \tag{4}$$

A 1R-attack on 13 rounds (8 Rule-A and 5 Rule-B rounds), using the Λ-set chain (4), discovers subkeys k_8, k_9, k_0, k_1 and checks if $\mathrm{G}^{-12}(C_1^i) \oplus C_2^i$ is active (see Fig. 8). To filter out wrong 32-bit subkey candidates, three plaintex Λ-set are used. The complexity is $2^{16} \cdot 2^{32} \cdot 2^{-5} + 2^{16} \cdot 2^{16} \cdot 2^{-5} + 2^{16} \cdot 2^{-5} \approx 2^{43}$ full Skipjack encryptions.

$$\begin{aligned}(P\ P\ P\ A) &\xrightarrow{\mathrm{A}} (P\ P\ P\ A) \xrightarrow{\mathrm{A}} (P\ P\ A\ A) \xrightarrow{\mathrm{A}} (P\ A\ A\ A) \xrightarrow{\mathrm{A}} (A\ A\ A\ A) \xrightarrow{\mathrm{A}} \\ &(A\ A\ A\ *) \xrightarrow{\mathrm{A}} (A\ A\ ?\ ?) \xrightarrow{\mathrm{A}} (A\ ?\ ?\ ?) \xrightarrow{\mathrm{A}} (?\ ?\ ?\ ?) \xrightarrow{\mathrm{B}} (?\ A\ ?\ ?) \xrightarrow{\mathrm{B}} \\ &(?\ A\ ?\ ?) \xrightarrow{\mathrm{B}} (?\ A\ ?\ ?) \xrightarrow{\mathrm{B}} (?\ A\ ?\ ?) \xrightarrow{\mathrm{B}} (?\ ?\ ?\ ?)\end{aligned} \tag{5}$$

A 1R-attack on the initial 13 rounds of Skipjack using (5) is identical to the 1R-attack using (4). See Fig. 9.

$$\begin{aligned}(A\ A\ P\ P) &\xrightarrow{\mathrm{A}} (A\ A\ P\ A) \xrightarrow{\mathrm{A}} (A\ A\ A\ A) \xrightarrow{\mathrm{A}} (A\ *\ A\ A) \xrightarrow{\mathrm{A}} (?\ ?\ A\ A) \xrightarrow{\mathrm{A}} \\ &(?\ ?\ A\ ?) \xrightarrow{\mathrm{A}} (?\ ?\ ?\ ?) \xrightarrow{\mathrm{A}} (?\ ?\ ?\ ?) \xrightarrow{\mathrm{A}} (?\ ?\ ?\ ?) \xrightarrow{\mathrm{B}} (?\ ?\ ?\ ?)\end{aligned} \tag{6}$$

A 1R-attack on the initial nine rounds of Skipjack using (6) discovers subkey bytes k_4, k_5, k_6, k_7 by checking if $G^{-6}(C_3^i) \oplus C_4^i$ is active (see Fig. 10). To filter out wrong 32-bit subkey candidates three plaintext Λ-sets are used.

$$\begin{aligned}(A\ P\ A\ P) &\xrightarrow{\mathrm{A}} (A\ P\ A\ A) \xrightarrow{\mathrm{A}} (A\ P\ *\ A) \xrightarrow{\mathrm{A}} (A\ ?\ ?\ A) \xrightarrow{\mathrm{A}} (?\ ?\ ?\ A) \xrightarrow{\mathrm{A}} \\ &(?\ ?\ ?\ ?)\end{aligned} \tag{7}$$

A 1R-attack on the initial nine rounds of Skipjack using (7) discovers subkey bytes k_0, k_1, k_2, k_3 of the 6-th round and checks if $G^{-5}(C_4^i) \oplus C_1^i \oplus C_2^i$ is active.

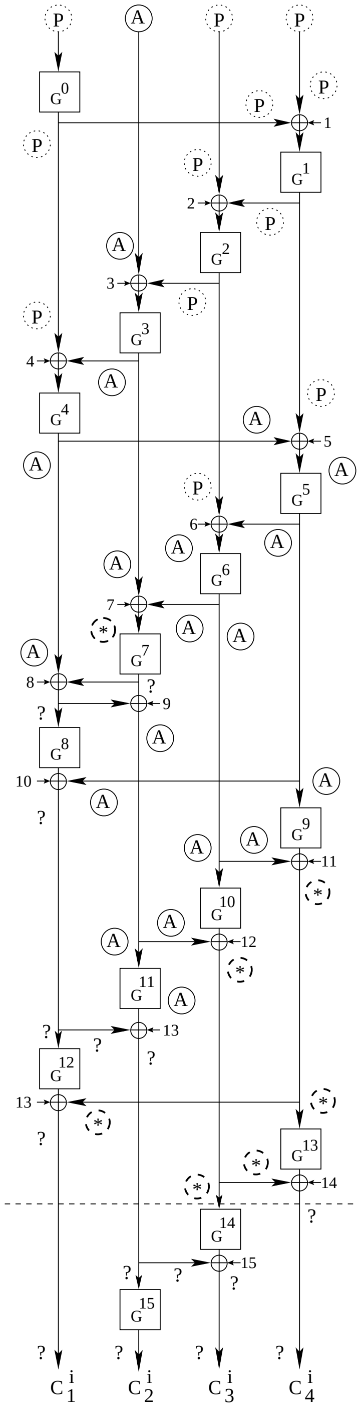

Fig. 7. Propagation of Λ-sets according to chain (3).

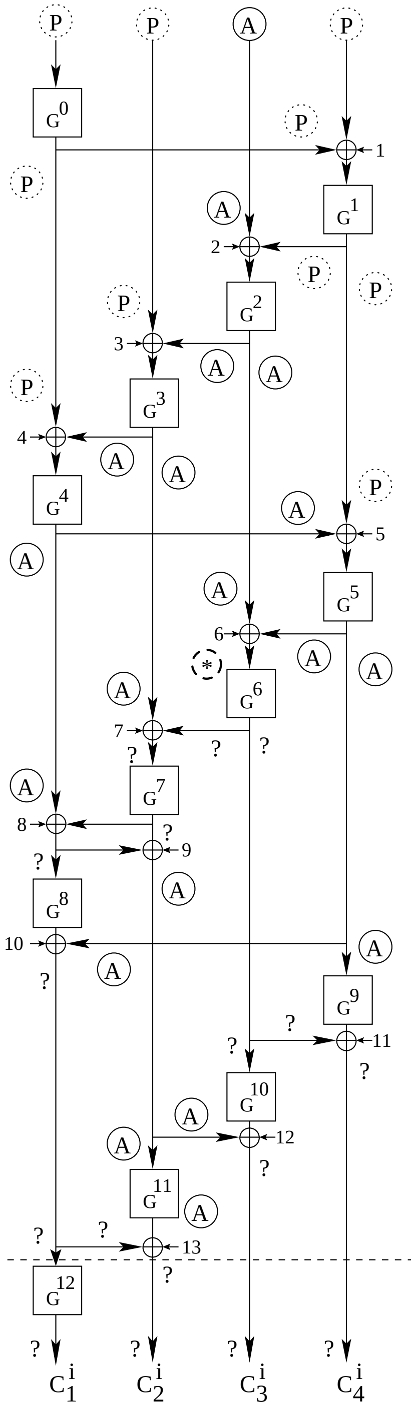

Fig. 8. Propagation of Λ-sets according to chain (4).

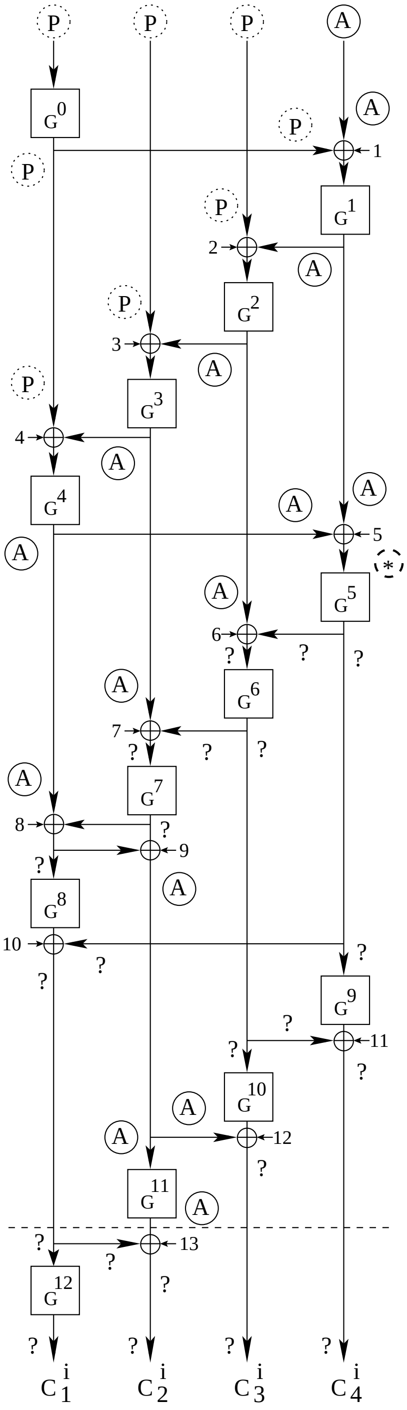

Fig. 9. Propagation of Λ-sets according to chain (5).

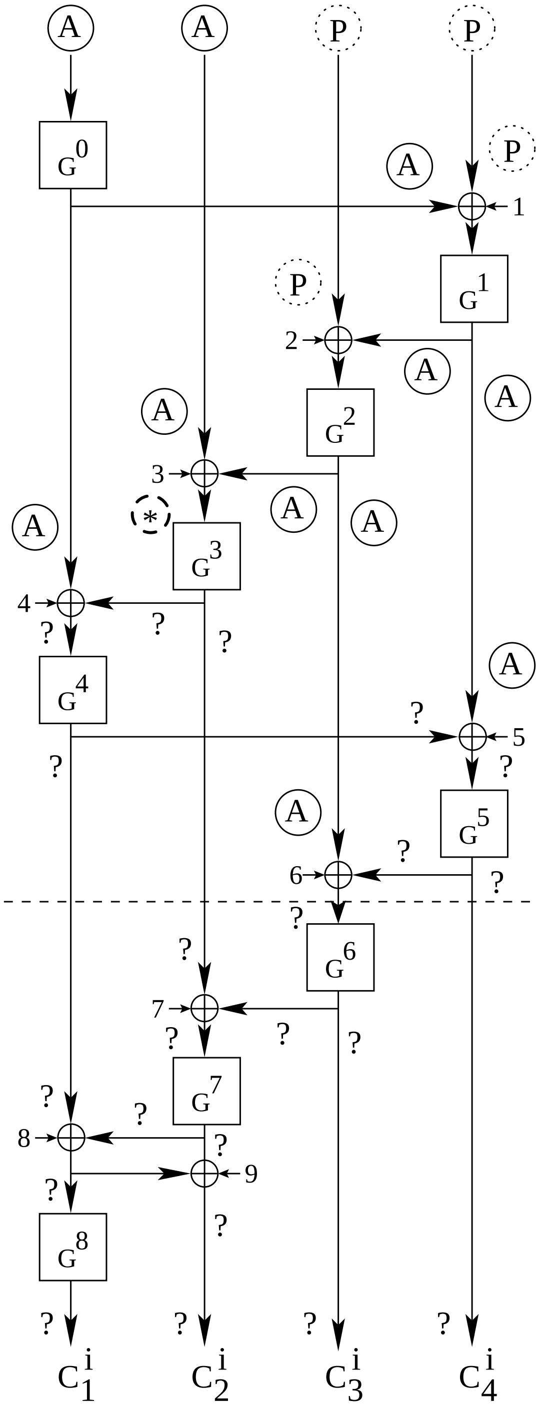

Fig. 10. Propagation of Λ-sets according to chain (6).

To filter out wrong 32-bit subkey candidates three plaintext Λ-sets are used. See Fig. 11.

$$\begin{aligned}(A\ P\ P\ A) \xrightarrow{\text{A}} (A\ P\ P\ *) \xrightarrow{\text{A}} (A\ P\ ?\ ?) \xrightarrow{\text{A}} (A\ ?\ ?\ ?) \xrightarrow{\text{A}} (?\ ?\ ?\ ?) \xrightarrow{\text{A}} \\ (?\ ?\ ?\ ?) \xrightarrow{\text{A}} (?\ ?\ ?\ ?) \xrightarrow{\text{A}} (?\ ?\ ?\ ?) \xrightarrow{\text{A}} (?\ ?\ ?\ ?)\end{aligned} \tag{8}$$

A 1R-attack can be made on the initial seven rounds of Skipjack, using (8), although the latter covers only four rounds. The attack discovers subkey bytes $k_6\ k_7\ k_8\ k_9$ of the 5-th round by checking if $G^{-4}(C_1^i) \oplus C_2^i \oplus C_3^i$ is active. To filter out wrong 32-bit subkey candidates three plaintext Λ-sets are used.

A 2R-attack on the first eight rounds of Skipjack using (8) discovers k_8, k_9, k_0, k_1 and compute $D_2^i = G^{-7}(C_2^i) \oplus C_3^i$ with complexity $\approx 2^{43}$. The attack proceeds to guess k_6, k_7 and checks if $G^{-4}(C_1^i \oplus C_2^i) \oplus D_2^i$ is active (see Fig. 12). The additional complexity is $2^{16} \cdot 2^{16} \cdot 2^{-5} + 2^{16} \cdot 2^{-5} \approx 2^{27}$. Four plaintext Λ-sets are used to filter out wrong 48-bit subkey candidates.

$$\begin{aligned}(P\ A\ A\ P) \xrightarrow{\text{A}} (P\ A\ A\ P) \xrightarrow{\text{A}} (P\ A\ A\ P) \xrightarrow{\text{A}} (P\ *\ A\ P) \xrightarrow{\text{A}} (?\ ?\ A\ P) \xrightarrow{\text{A}} \\ (?\ ?\ A\ ?) \xrightarrow{\text{A}} (?\ ?\ ?\ ?) \xrightarrow{\text{A}} (?\ ?\ ?\ ?) \xrightarrow{\text{A}} (?\ ?\ ?\ ?) \xrightarrow{\text{B}} (?\ ?\ ?\ ?)\end{aligned} \tag{9}$$

A 1R-attack on the nine initial rounds of Skipjack, using chain (9), discovers subkey bytes k_4, k_5, k_6, k_7 by checking if $G^{-6}(C_3^i) \oplus C_4^i$ is active (see Fig. 13). To filter out wrong 32-bit subkey candidates, three plaintext Λ-sets are used. Complexity is $\approx 2^{43}$, similar to previous attacks.

$$\begin{aligned}(P\ A\ P\ A) \xrightarrow{\text{A}} (P\ A\ P\ A) \xrightarrow{\text{A}} (P\ A\ A\ A) \xrightarrow{\text{A}} (P\ *\ A\ A) \xrightarrow{\text{A}} (?\ ?\ A\ A) \xrightarrow{\text{A}} \\ (?\ ?\ A\ ?) \xrightarrow{\text{A}} (?\ ?\ ?\ ?) \xrightarrow{\text{A}} (?\ ?\ ?\ ?) \xrightarrow{\text{A}} (?\ ?\ ?\ ?) \xrightarrow{\text{B}} (?\ ?\ ?\ ?)\end{aligned} \tag{10}$$

A 1R-attack on the nine initial rounds of Skipjack, using chain (10), discovers subkey bytes k_4, k_5, k_6, k_7 by checking if $G^{-6}(C_3^i) \oplus C_4^i$ is active (see Fig. 14). To filter out wrong 32-bit subkey candidates, three plaintext Λ-sets are used.

$$\begin{aligned}(P\ P\ A\ A) \xrightarrow{\text{A}} (P\ P\ A\ A) \xrightarrow{\text{A}} (P\ P\ *\ A) \xrightarrow{\text{A}} (P\ ?\ ?\ A) \xrightarrow{\text{A}} (?\ ?\ ?\ A) \xrightarrow{\text{A}} \\ (?\ ?\ ?\ ?) \xrightarrow{\text{A}} (?\ ?\ ?\ ?) \xrightarrow{\text{A}} (?\ ?\ ?\ ?) \xrightarrow{\text{A}} (?\ ?\ ?\ ?) \xrightarrow{\text{B}} (?\ ?\ ?\ ?)\end{aligned} \tag{11}$$

A 1R-attack on nine initial rounds of Skipjack, using chain (11), discovers subkeys k_0, k_1, k_2, k_3 by checking if $G^{-5}(C_4^i) \oplus C_2^i$ is active (see Fig.15). To filter out wrong 32-bit subkey candidates, three plaintext Λ-sets are used.

$$\begin{aligned}(A\ A\ A\ P) \xrightarrow{\text{A}} (A\ A\ A\ A) \xrightarrow{\text{A}} (A\ A\ *\ A) \xrightarrow{\text{A}} (A\ ?\ ?\ A) \xrightarrow{\text{A}} (?\ ?\ ?\ A) \xrightarrow{\text{A}} \\ (?\ ?\ ?\ ?) \xrightarrow{\text{A}} (?\ ?\ ?\ ?) \xrightarrow{\text{A}} (?\ ?\ ?\ ?) \xrightarrow{\text{A}} (?\ ?\ ?\ ?) \xrightarrow{\text{B}} (?\ ?\ ?\ ?)\end{aligned} \tag{12}$$

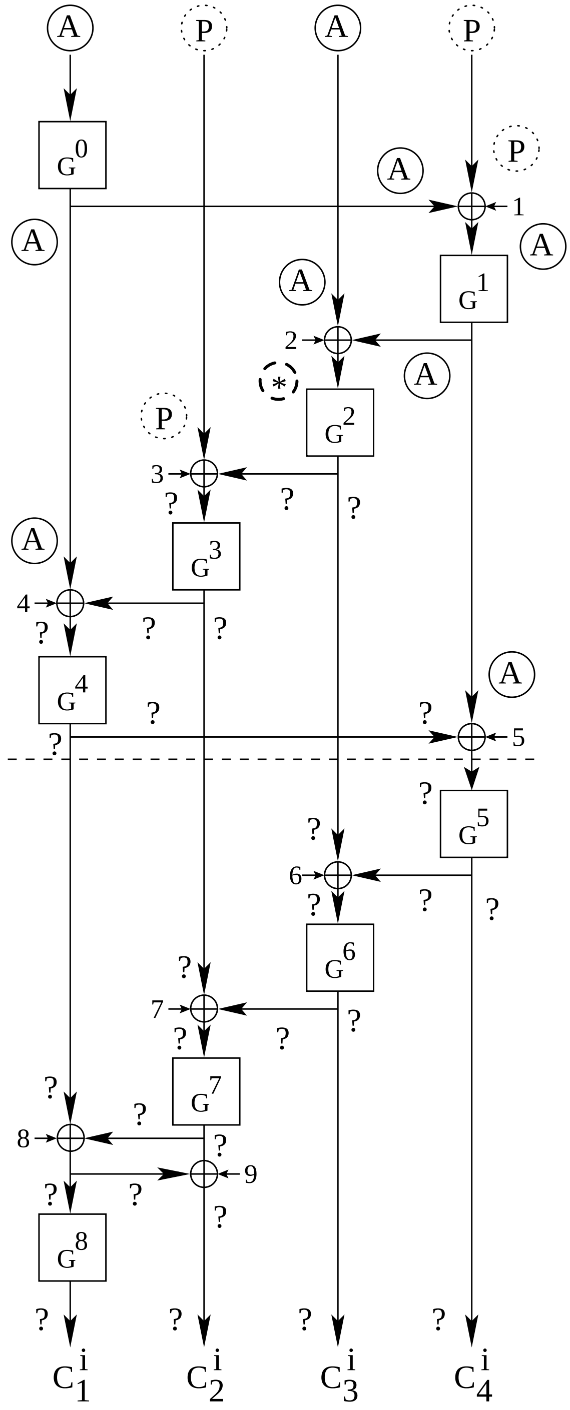

Fig. 11. Propagation of Λ-sets according to chain (7).

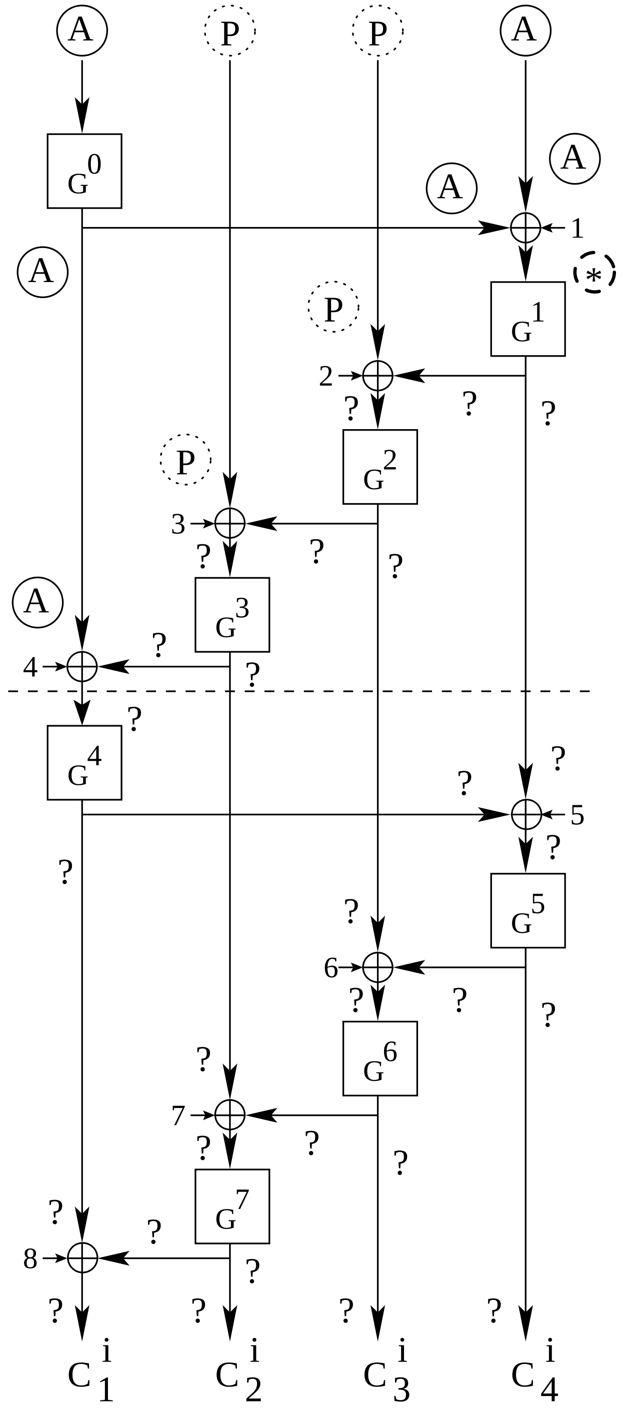

Fig. 12. Propagation of Λ-sets according to chain (8).

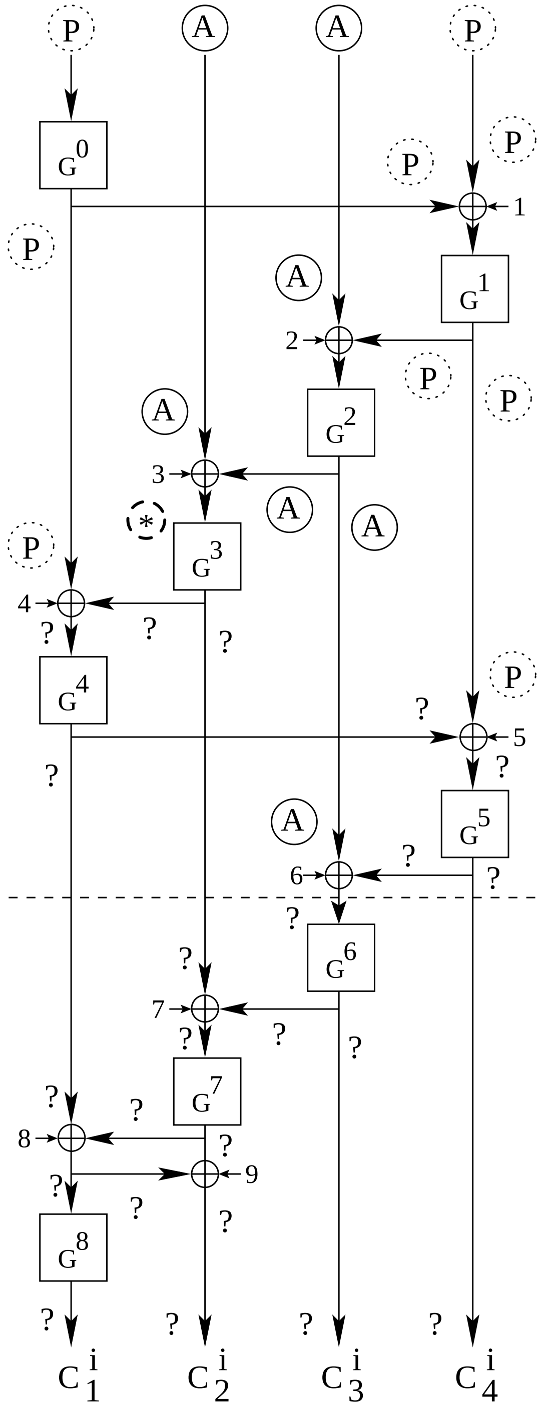

Fig. 13. Propagation of Λ-sets according to chain (9).

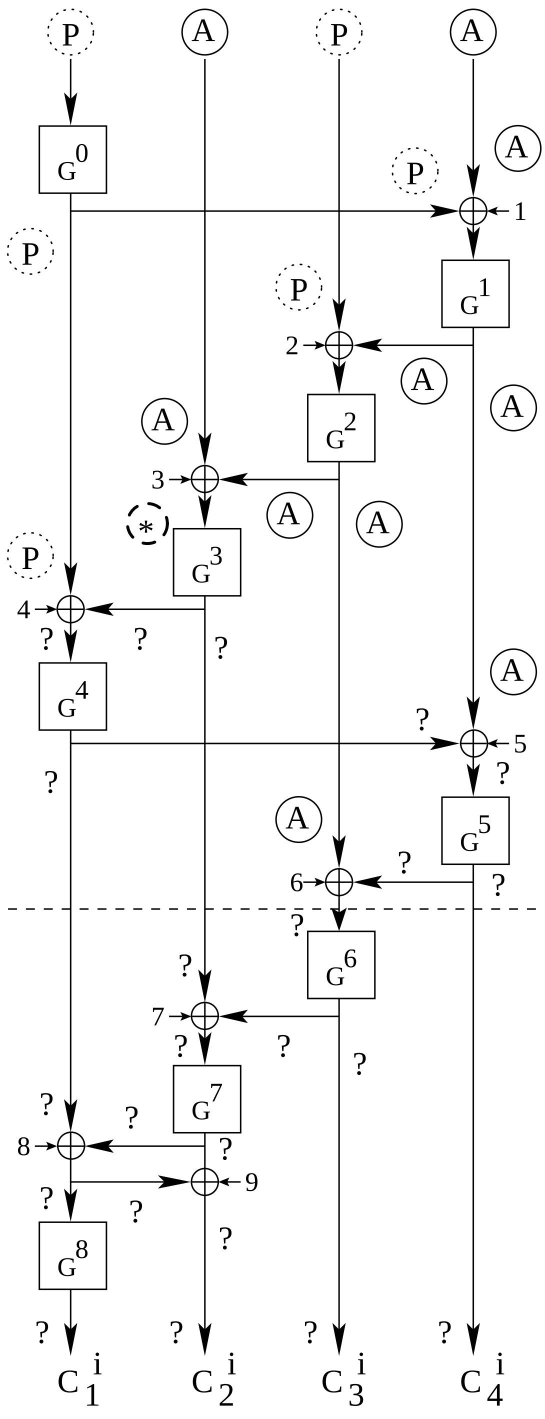

Fig. 14. Propagation of Λ-sets according to chain (10).

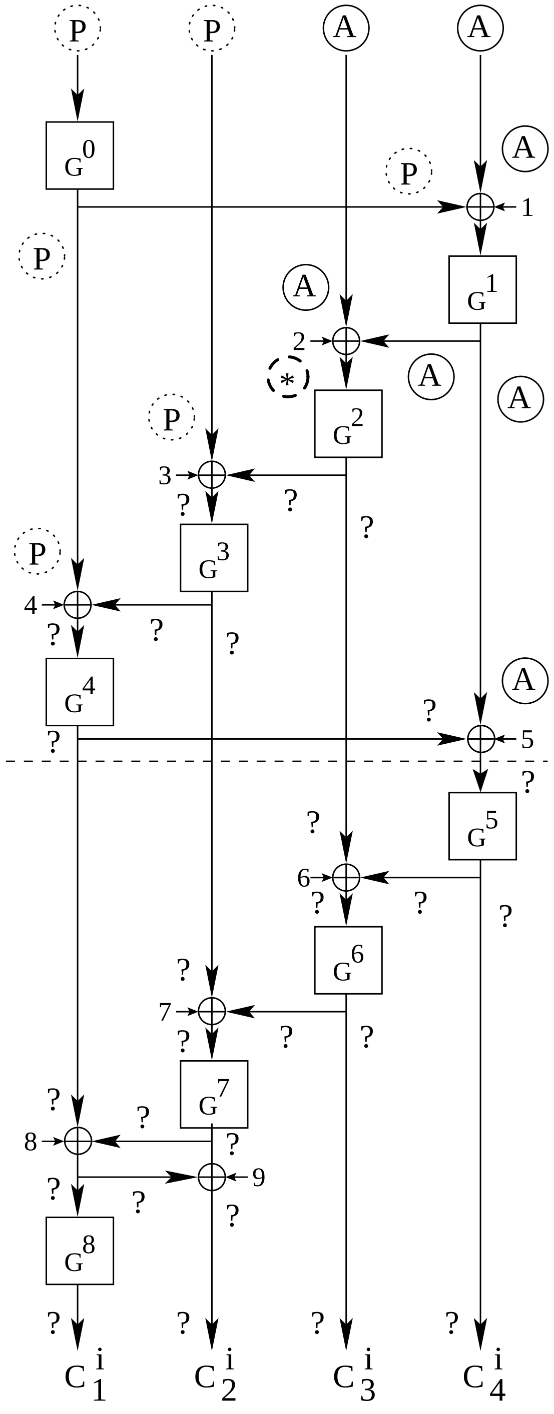

Fig. 15. Propagation of Λ-sets according to chain (11).

A 1R-attack on the first nine rounds of Skipjack, using (12), discovers subkey bytes k_0, k_1, k_2, k_3 by checking if $G^{-5}(C_4^i) \oplus C_2^i$ is active (see Fig. 16). To filter out wrong 32-bit subkey candidates, three plaintext Λ-sets are used. Complexity is $\approx 2^{43}$ full Skipjack encryptions, as previous attacks.

$$(A\ A\ P\ A) \xrightarrow{A} (A\ A\ P\ *) \xrightarrow{A} (A\ A\ ?\ ?) \xrightarrow{A} (A\ ?\ ?\ ?) \xrightarrow{A} (?\ ?\ ?\ ?) \xrightarrow{A} (?\ ?\ ?\ ?) \xrightarrow{A} (?\ ?\ ?\ ?) \xrightarrow{A} (?\ ?\ ?\ ?) \xrightarrow{A} (?\ ?\ ?\ ?) \tag{13}$$

A 2R-attack on eight rounds, using (13), discovers subkey bytes k_6, k_7, k_8, k_9, k_0, k_1 by checking if $G^{-4}(C_1^i \oplus C_2^i) \oplus G^{-7}(C_2^i) \oplus C_3^i$ is active (see Fig. 17). To filter out wrong 48-bit subkey candidates, four plaintext Λ-sets are used. Complexity is $2^{16} \cdot 2^{48} \cdot 2 \cdot 2^{-5} + 2^{16} \cdot 2^{32} \cdot 2 \cdot 2^{-5} + 2^{16} \cdot 2^{16} \cdot 2 \cdot 2^{-5} + 2^{16} \cdot 2 \cdot 2^{-5} \approx 2^{60}$ full Skipjack encryptions.

$$(A\ P\ A\ A) \xrightarrow{A} (A\ P\ A\ *) \xrightarrow{A} (A\ P\ ?\ ?) \xrightarrow{A} (A\ ?\ ?\ ?) \xrightarrow{A} (?\ ?\ ?\ ?) \xrightarrow{A} (?\ ?\ ?\ ?) \xrightarrow{A} (?\ ?\ ?\ ?) \xrightarrow{A} (?\ ?\ ?\ ?) \xrightarrow{A} (?\ ?\ ?\ ?) \tag{14}$$

A 2R-attack on the initial 8 rounds of Skipjack, using chain (14), is the same as the 2R-attack using chain (13). See Fig.18.

$$(P\ A\ A\ A) \xrightarrow{A} (P\ A\ A\ A) \xrightarrow{A} (P\ A\ *\ A) \xrightarrow{A} (P\ ?\ ?\ A) \xrightarrow{A} (?\ ?\ ?\ A) \xrightarrow{A} (?\ ?\ ?\ ?) \xrightarrow{A} (?\ ?\ ?\ ?) \xrightarrow{A} (?\ ?\ ?\ ?) \xrightarrow{A} (?\ ?\ ?\ ?) \xrightarrow{B} (?\ ?\ ?\ ?) \tag{15}$$

A 1R-attack on the initial 9 rounds of Skipjack, using (15), discovers subkey bytes k_0, k_1, k_2, k_3 by checking if $G^{-5}(C_4^i) \oplus C_2^i$ is active (see Fig.19). To filter out wrong 32-bit subkey candidates, three plaintext Λ-sets are used.

$$(A\ A\ A\ A) \xrightarrow{A} (A\ A\ A\ *) \xrightarrow{A} (A\ A\ ?\ ?) \xrightarrow{A} (A\ ?\ ?\ ?) \xrightarrow{A} (?\ ?\ ?\ ?) \xrightarrow{A} (?\ ?\ ?\ ?) \xrightarrow{A} (?\ ?\ ?\ ?) \xrightarrow{A} (?\ ?\ ?\ ?) \xrightarrow{A} (?\ ?\ ?\ ?) \tag{16}$$

A 2R-attack can be made using the chain (16) of Λ-sets, on eight rounds of Skipjack. The attack discovers subkey bytes k_6, k_7, k_8, k_9, k_0, k_1 by verifying if $\mathrm{G}^{-4}(C_1^i \oplus C_2^i) \oplus \mathrm{G}^{-7}(C_2^i) \oplus C_3^i$ is active. To filter out wrong 48-bit subkey candidates, four plaintext Λ-sets are used. See Fig.20.

Up to now all attack were made at the end of the cipher structure. In order to extend the propagation of Λ-set to further rounds, subkeys will be guessed at the top of cipher, and also the kind of permutation employed for the active input words will be carefully chosen.

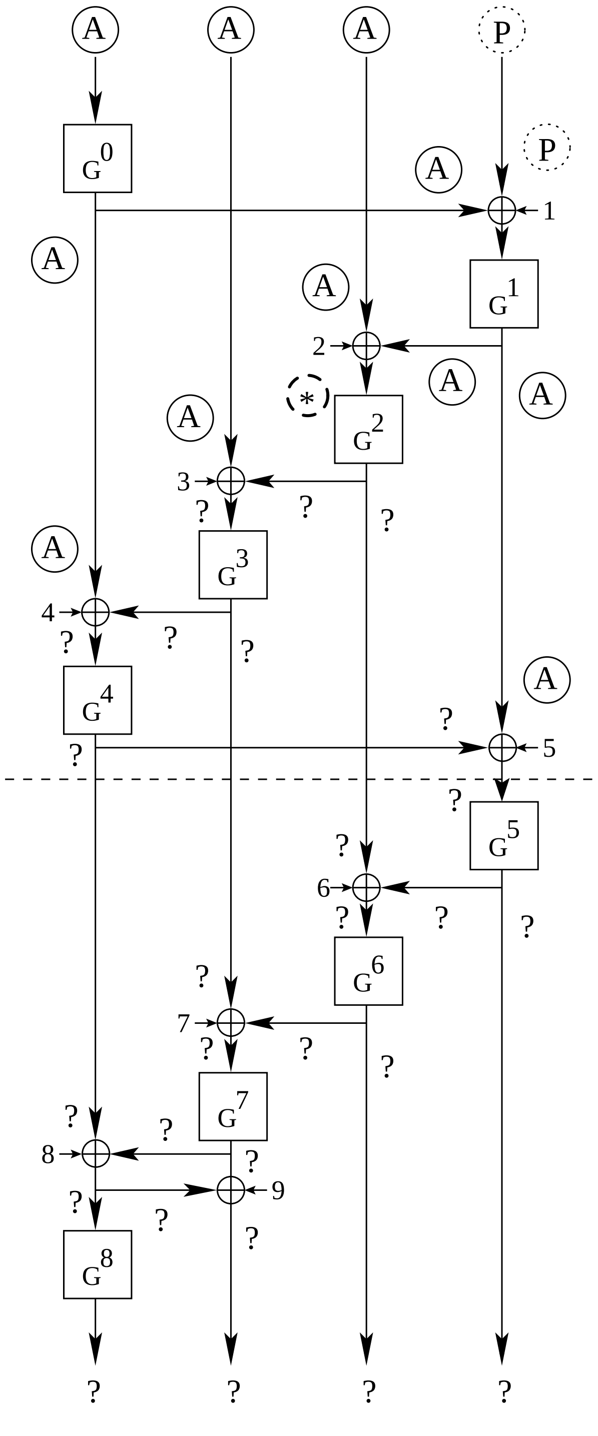

Fig. 16. Propagation of Λ-sets according to chain (12).

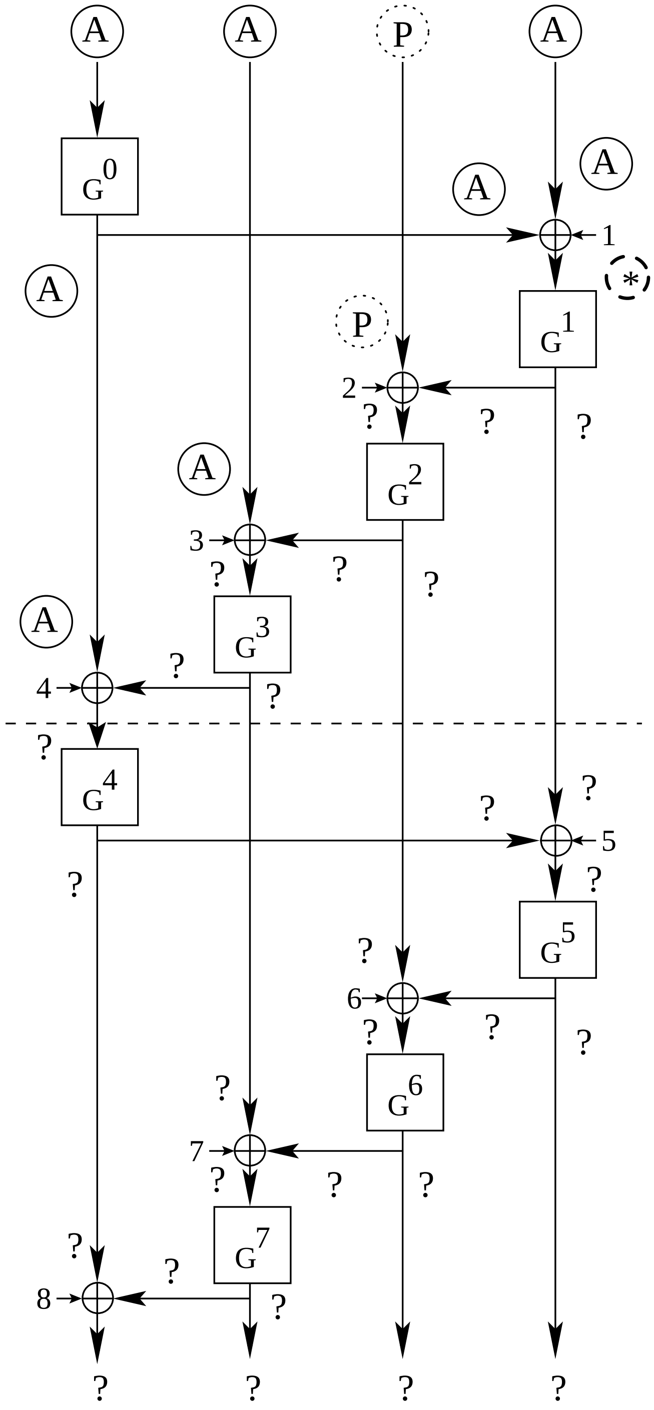

Fig. 17. Propagation of Λ-sets according to chain (13).

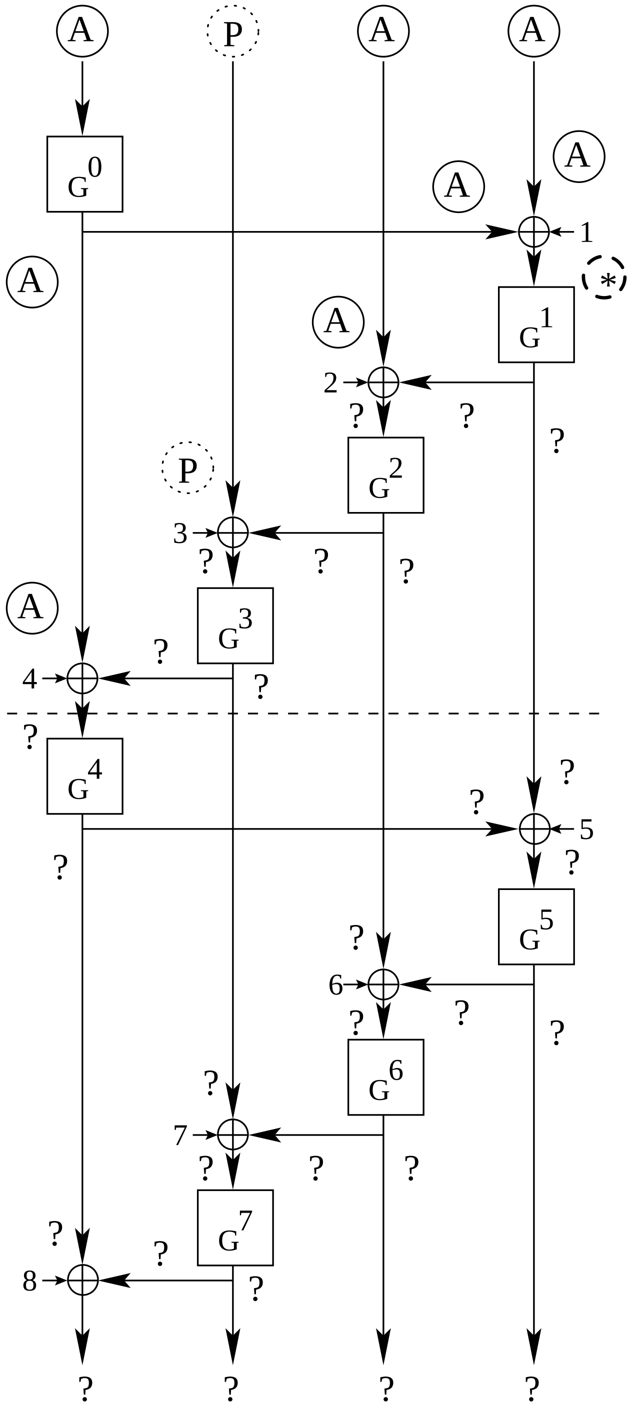

Fig. 18. Propagation of Λ-sets according to chain (14).

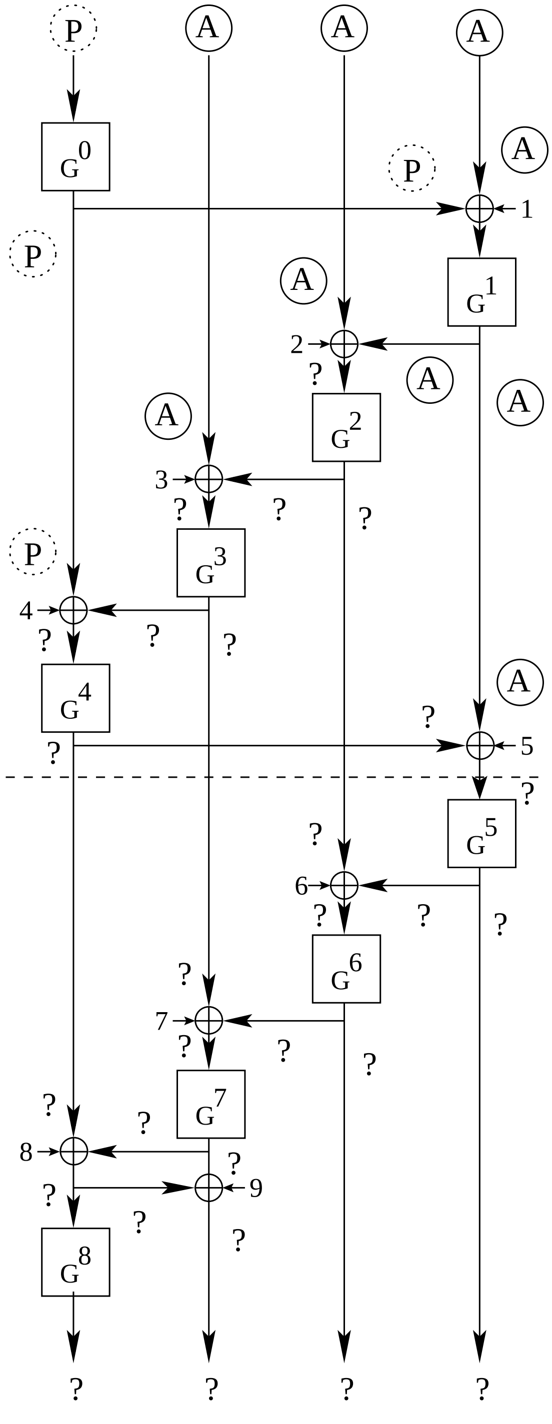

Fig. 19. Propagation of Λ-sets according to (15).

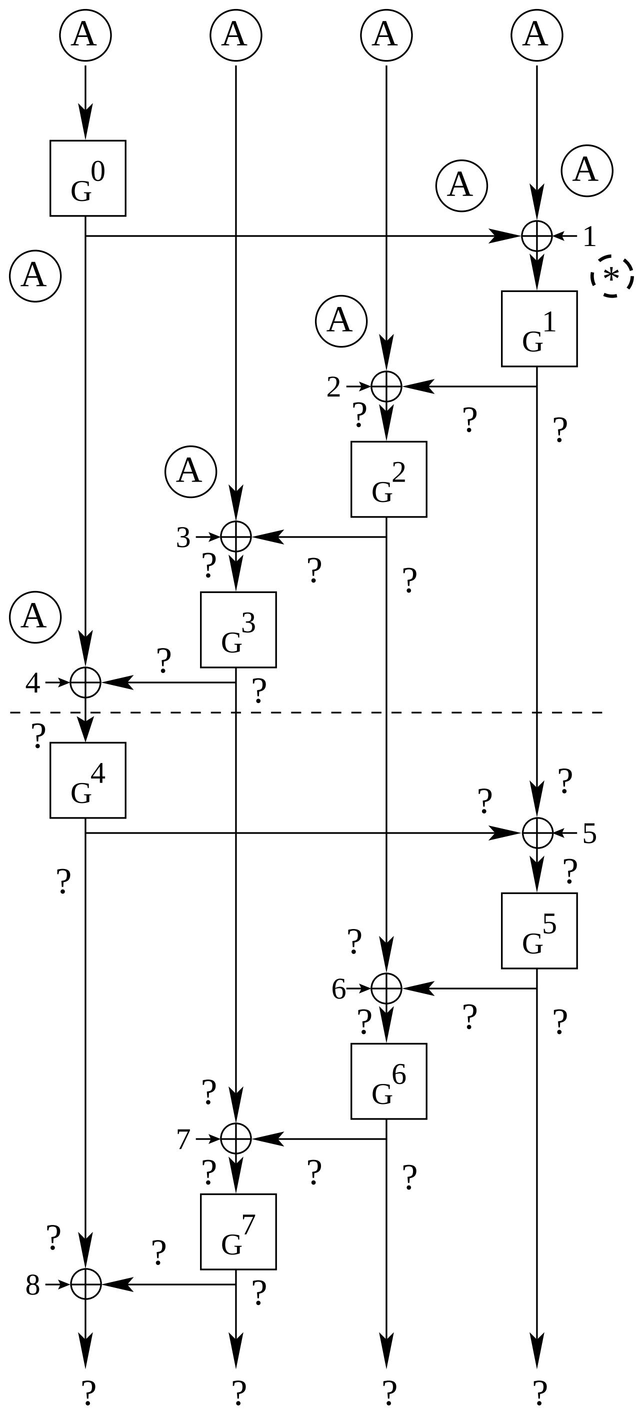

Fig. 20. Propagation of Λ-sets according to chain (16).

$$
\begin{aligned}
&(P\ P\ A\ A) \xrightarrow{\mathrm{A}} (P\ P\ A\ A) \xrightarrow{\mathrm{A}} (P\ P\ P\ A) \xrightarrow{\mathrm{A}} (P\ P\ P\ A) \xrightarrow{\mathrm{A}} (P\ P\ P\ A) \xrightarrow{\mathrm{A}} \\
&(P\ P\ P\ A) \xrightarrow{\mathrm{A}} (P\ P\ A\ A) \xrightarrow{\mathrm{A}} (P\ A\ A\ A) \xrightarrow{\mathrm{A}} (A\ A\ A\ A) \xrightarrow{\mathrm{B}} (A\ P\ A\ A) \xrightarrow{\mathrm{B}} \\
&(*\ P\ A\ A) \xrightarrow{\mathrm{B}} (*\ P\ A\ *) \xrightarrow{\mathrm{B}} (*\ P\ A\ *) \xrightarrow{\mathrm{B}} (?\ *\ A\ *) \xrightarrow{\mathrm{B}} (?\ *\ A\ ?) \xrightarrow{\mathrm{B}} \\
&(?\ *\ A\ ?) \xrightarrow{\mathrm{B}} (?\ ?\ *\ ?) \xrightarrow{\mathrm{B}} (?\ ?\ *\ ?) \xrightarrow{\mathrm{B}} (?\ ?\ ?\ ?)
\end{aligned}
\tag{17}
$$

Chain (17) of Λ-sets employ these two strategies. The plaintext Λ-set in (17) has two active words. Usually the kind of permutation in these words is arbitrary and unrelated, as in (11). An idea is to make both active words contain almost the same permutation. In P_3^i a permutation is input to an instance of G^1, which contains a guessed value for k_4, k_5, k_6, k_7. Since G^1 is a permutation, the output is always active: $P_3^i = \mathrm{G}^1(i)$. The same permutation to P_3^i is also input to P_4^i but exclusive-ored to a 16-bit guessed value, intended to match $\mathrm{G}^0(P_1^i)$. When the correct values for k_4, k_5, k_6, k_7 and for $\mathrm{G}^0(P_1^i)$ are chosen, the plaintext values have the form $P^i = (0, P_2^i, \mathrm{G}^1(i), i \oplus \mathrm{G}^0(0) \oplus 1)$, and the third output word of the second round will be $\mathrm{G}^1(i) \oplus 2 \oplus \mathrm{G}^1(i) = 2$ which is passive. The correct guesses for the four subkey bytes and $\mathrm{G}^0(0)$ can be verified by checking that $C_3^i \oplus C_4^i$ is balanced. This 1R-attack covers 18 rounds, and guesses 48 subkey bits and would require four plaintext Λ-sets. See Fig.21. The complexity is $2^{16} \cdot 2^{48} + 2^{16} \cdot 2^{32} + 2^{16} \cdot 2^{16} + 2^{16} \approx 2^{60}$ full Skipjack encryptions. A variant 2R-attack reaches 19 rounds. Additionally, subkey bytes k_2 and k_3 are to be found in order to decrypt the 19-th round, and check if $\mathrm{G}^{-18}(C_3^i) \oplus C_4^i$ is balanced. This attack at both extremes of the cipher discovers $32 + 16 = 48$ subkey bits, and will require five plaintext Λ-sets to filter avoid false subkeys. The complexity is $2^{16} \cdot 2^{48} \cdot 2^{-5} + 2^{16} \cdot 2^{32} \cdot 2^{-5} + 2^{16} \cdot 2^{16} \cdot 2^{-5} + 2^{16} \cdot 2^{-5} \approx 2^{59}$ full Skipjack encryptions.

$$
\begin{aligned}
&(A\ P\ A\ P) \xrightarrow{\mathrm{A}} (A\ P\ A\ A) \xrightarrow{\mathrm{A}} (A\ P\ P\ A) \xrightarrow{\mathrm{A}} (A\ P\ P\ A) \xrightarrow{\mathrm{A}} (A\ P\ P\ A) \xrightarrow{\mathrm{A}} \\
&(A\ P\ P\ *) \xrightarrow{\mathrm{A}} (A\ P\ ?\ ?) \xrightarrow{\mathrm{A}} (A\ ?\ ?\ ?) \xrightarrow{\mathrm{A}} (?\ ?\ ?\ ?) \xrightarrow{\mathrm{B}} (?\ A\ ?\ ?) \xrightarrow{\mathrm{B}} \\
&(?\ A\ ?\ ?) \xrightarrow{\mathrm{B}} (?\ A\ ?\ ?) \xrightarrow{\mathrm{B}} (?\ A\ ?\ ?) \xrightarrow{\mathrm{B}} (?\ ?\ ?\ ?) \xrightarrow{\mathrm{B}} (?\ ?\ ?\ ?) \xrightarrow{\mathrm{B}} \\
&(?\ ?\ ?\ ?) \xrightarrow{\mathrm{B}} (?\ ?\ ?\ ?) \xrightarrow{\mathrm{B}} (?\ ?\ ?\ ?) \xrightarrow{\mathrm{B}} (?\ ?\ ?\ ?)
\end{aligned}
\tag{18}
$$

The chain of Λ-sets (18) can be used in a 1R-attack on the initial 12 rounds of Skipjack. The attack discovers subkey bytes k_0, k_1, k_2, k_3, k_4, k_5, k_6, k_7 of the first two rounds, by applying key-dependent active words to two plaintext Λ-set words: $P_1^i = \mathrm{G}^{-0}(i)$, and $P_3^i = \mathrm{G}^1(i)$. For the passive words: $P_2^i = P_4^i = 0$. When all subkey bytes $k_0 \ldots k_7$ are guessed correctly, the 4-th output word of the first round might contain the same permutation as that applied to the two active plaintext words. Thus, the third output word of the second round will be passive as a result of the combination of $P_3^i = \mathrm{G}^1(i)$ and $\mathrm{G}^1(\mathrm{G}^0(\mathrm{G}^{-0}(i) \oplus 0)) = \mathrm{G}^1(i)$. The subsequent chain of Λ-sets allows the correct subkeys to be verified by checking that the second output word of the 12th round is active (see Fig. 22).

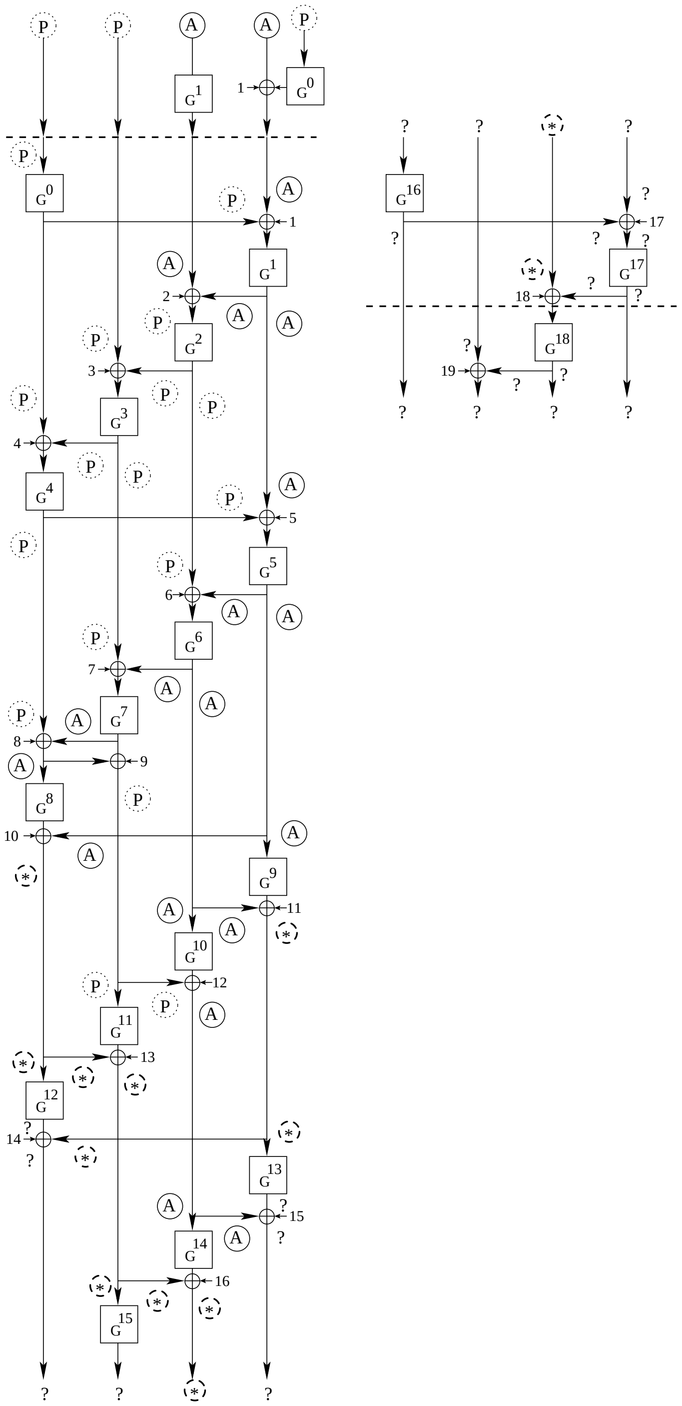

Fig. 21. Propagation of Λ-sets according to chain (17).

In total, 8*8=64 subkey bits are explored. In order to filter out wrong subkey candidates, four plaintext Λ-sets are used. The complexity is $2^{16} \cdot 2^{64} + 2^{16} \cdot 2^{48} + 2^{16} \cdot 2^{32} + 2^{16} \cdot 2^{16} + 2^{16} \approx 2^{80}$ full Skipjack computations, which is more than the effort of an exhaustive key search.

$$
\begin{gathered}
(P\ A\ A\ P) \xrightarrow{\mathrm{A}} (P\ A\ A\ P) \xrightarrow{\mathrm{A}} (P\ A\ A\ P) \xrightarrow{\mathrm{A}} (P\ P\ A\ P) \xrightarrow{\mathrm{A}} (P\ P\ A\ P) \xrightarrow{\mathrm{A}} \\
(P\ P\ A\ P) \xrightarrow{\mathrm{A}} (P\ P\ A\ P) \xrightarrow{\mathrm{A}} (P\ A\ A\ P) \xrightarrow{\mathrm{A}} (A\ A\ A\ P) \xrightarrow{\mathrm{B}} (A\ P\ A\ P) \xrightarrow{\mathrm{B}} \\
(A\ P\ A\ P) \xrightarrow{\mathrm{B}} (A\ P\ A\ A) \xrightarrow{\mathrm{B}} (A\ P\ A\ A) \xrightarrow{\mathrm{B}} (A\ A\ A\ A) \xrightarrow{\mathrm{B}} (*\ A\ A\ A) \xrightarrow{\mathrm{B}} \\
(*\ A\ A\ *) \xrightarrow{\mathrm{B}} (*\ A\ *\ *) \xrightarrow{\mathrm{A}} (?\ A\ *\ ?) \xrightarrow{\mathrm{A}} (?\ A\ ?\ ?) \xrightarrow{\mathrm{A}} (?\ ?\ ?\ ?) \xrightarrow{\mathrm{A}} \\
(?\ ?\ ?\ ?) \xrightarrow{\mathrm{A}} (?\ ?\ ?\ ?) \xrightarrow{\mathrm{A}} (?\ ?\ ?\ ?) \xrightarrow{\mathrm{A}} (?\ ?\ ?\ ?)
\end{gathered} \tag{19}
$$

The chain (19) of Λ-sets can be used in a 1R-attack on the first 18 rounds of Skipjack. The attack sets $P_2^i = \mathrm{G}^2(i) \oplus c$, $0 \leq i \leq 2^{16} - 1$, $c \in \{0,1\}^{16}$, $P_3^i = i$. The 16-bit value c is intended to match $\mathrm{G}^1(\mathrm{G}^0(0)) \oplus 2$. The passive words are set to: $P_1^i = 0$, $P_4^i = 1$. Subkeys k_8, k_9, k_0, k_1 and a 16-bit key related value $\mathrm{G}^1(\mathrm{G}^0(0)) \oplus 2$ are to be discovered, totaling 4*8+16=48 bits. When all these 48 subkey-related bits are discovered the second output word of the 18th round might be active (see Fig. 23). The complexity is $2^{16} \cdot 2^{48} \cdot 2^{-5} + 2^{16} \cdot 2^{32} \cdot 2^{-5} + 2^{16} \cdot 2^{16} \cdot 2^{-5} + 2^{16} \cdot 2^{-5} \approx 2^{59}$ full Skipjack encryptions. By guessing additionally, k_6, k_7, it is possible to make a 2R-attack on up to 23 rounds. When the correct values of k_6, k_7, k_8, k_9, k_0, k_1 and $\mathrm{G}^1(\mathrm{G}^0(0)) \oplus 2$ are found, $\mathrm{G}^{-19}(C_2^1 \oplus C_3^i)$ is guessed correctly, and the attacker can discover the second output word from the 18th round by computing $\mathrm{G}^{-19}(C_2^i \oplus C_3^i) \oplus \mathrm{G}^{-22}(C_3^i) \oplus C_4^i$ and check that it is active. In total, 64 subkey related bits have to be discovered. In order to filter out wrong subkey candidates, five plaintext Λ-sets are required. The complexity is $2^{16} \cdot 2^{64} \cdot 2 \cdot 2^{-5} + 2^{16} \cdot 2^{48} \cdot 2 \cdot 2^{-5} + 2^{16} \cdot 2^{32} \cdot 2 \cdot 2^{-5} + 2^{16} \cdot 2^{16} \cdot 2 \cdot 2^{-5} + 2^{16} \cdot 2 \cdot 2^{-5} \approx 2^{76}$ full Skipjack encryptions.

4 Chosen-Ciphertext Square Attacks

Since Skipjack uses two kinds of round structures: Rule-A and Rule-B, there is an asymmetry between encryption and decryption. The attacks to be described below assume that Skipjack is being used in decryption mode. Therefore, the Square attacks become chosen-ciphertext attacks. Let $C^i = (C_1^i, C_2^i, C_3^i, C_4^i)$ represent the chosen-ciphertext blocks in the ciphertext Λ-set, and P_i the corresponding plaintext blocks of the plaintext Λ-set. The number of rounds will be specified in each case.

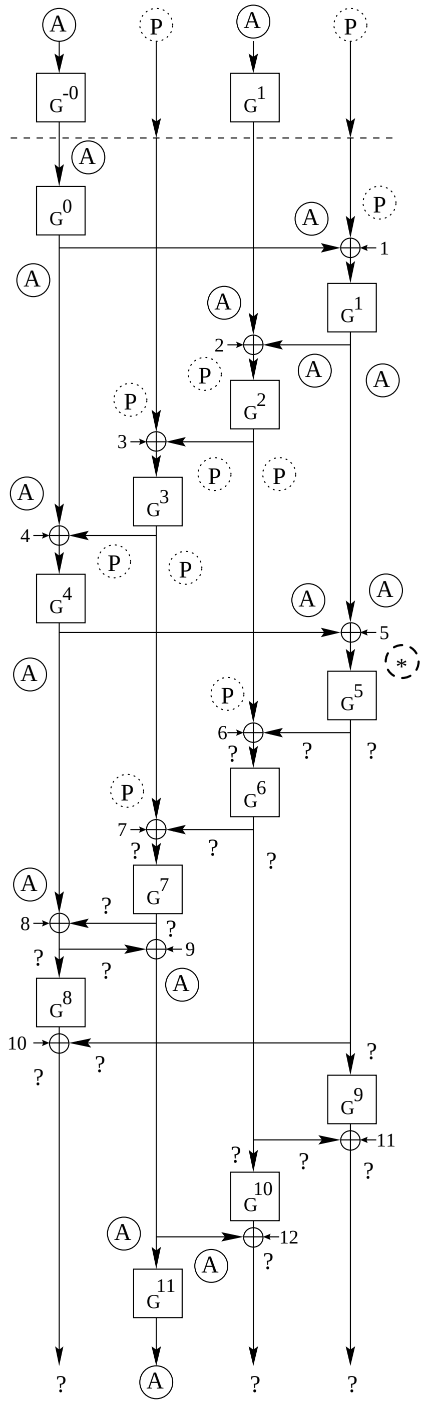

Fig. 22. Propagation of Λ-sets according to chain (18).

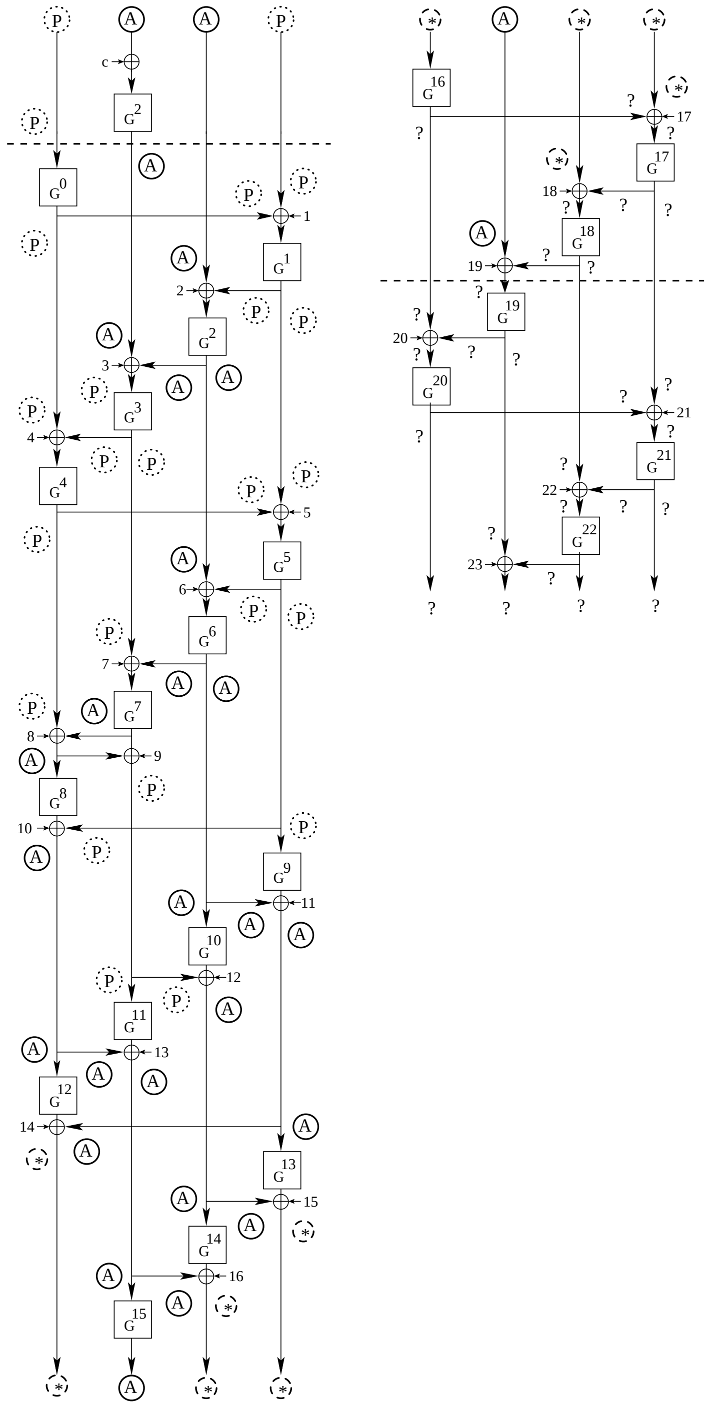

Fig. 23. Propagation of Λ-sets according to chain (19).

$$\begin{aligned}(A\ P\ P\ P) &\overset{B^{-1}}{\to} (A\ P\ P\ P) \overset{B^{-1}}{\to} (A\ P\ P\ P) \overset{B^{-1}}{\to} (A\ P\ P\ P) \overset{B^{-1}}{\to} (A\ A\ P\ P) \overset{B^{-1}}{\to} \\ (A\ A\ A\ P) &\overset{B^{-1}}{\to} (A\ A\ A\ A) \overset{B^{-1}}{\to} (*\ A\ A\ A) \overset{B^{-1}}{\to} (?\ ?\ A\ A) \overset{A^{-1}}{\to} (A\ ?\ A\ A) \overset{A^{-1}}{\to} \\ (A\ ?\ A\ A) &\overset{A^{-1}}{\to} (A\ ?\ *\ A) \overset{A^{-1}}{\to} (A\ ?\ *\ *) \overset{A^{-1}}{\to} (?\ ?\ *\ *) \overset{A^{-1}}{\to} (?\ ?\ *\ *) \overset{A^{-1}}{\to} \\ (?\ ?\ *\ ?) &\overset{A^{-1}}{\to} (?\ ?\ *\ ?) \overset{B^{-1}}{\to} (?\ ?\ ?\ ?) \overset{B^{-1}}{\to} (?\ ?\ ?\ ?) \overset{B^{-1}}{\to} (?\ ?\ ?\ ?) \overset{B^{-1}}{\to} \\ (?\ ?\ ?\ ?) &\overset{B^{-1}}{\to} (?\ ?\ ?\ ?) \end{aligned} \tag{20}$$

A 1R-attack can be done on 18 inverse rounds of Skipjack (eight Rule-B^{-1} rounds, eight Rule-A^{-1} rounds and two more Rule-B^{-1} rounds), using the first 17 rounds of the chain (20) of Λ-sets as a distinguisher. The attack discovers subkey bytes k_6, k_7, k_8, k_9 and verify if $\mathrm{G}^{-14}(P_3^i) \oplus P_2^i$ is balanced (see Fig. 24). To filter out false 32-bit subkey candidates, three ciphertext Λ-sets are used. The complexity of the attack is $2^{16} \cdot 2^{32} \cdot 2^{-5} + 2^{16} \cdot 2^{16} \cdot 2^{-5} + 2^{16} \cdot 2^{-5} \approx 2^{43}$ full Skipjack decryptions.

An extended 2R-attack on 21 inverse Skipjack rounds, using (20), discovers subkey bytes k_4, k_5, k_6, k_7, k_8, k_9, and checks if $P_1^i \oplus \mathrm{G}^{-11}(P_2^i) \oplus \mathrm{G}^{-14}(P_2^i \oplus P_3^i)$ is balanced. To filter out false 48-bit subkey candidates four ciphertext Λ-sets are used. The complexity is $2^{16} \cdot 2^{48} \cdot 2 \cdot 2^{-5} + 2^{16} \cdot 2^{32} \cdot 2 \cdot 2^{-5} + 2^{16} \cdot 2^{16} \cdot 2 \cdot 2^{-5} + 2^{16} \cdot 2 \cdot 2^{-5} \approx 2^{60}$ full Skipjack decryptions.

$$\begin{aligned}(P\ A\ P\ P) &\overset{B^{-1}}{\to} (P\ A\ A\ P) \overset{B^{-1}}{\to} (P\ A\ A\ A) \overset{B^{-1}}{\to} (A\ A\ A\ A) \overset{B^{-1}}{\to} (A\ *\ A\ A) \overset{B^{-1}}{\to} \\ (A\ ?\ ?\ A) &\overset{B^{-1}}{\to} (A\ ?\ ?\ ?) \overset{B^{-1}}{\to} (?\ ?\ ?\ ?) \overset{B^{-1}}{\to} (?\ ?\ ?\ ?) \end{aligned} \tag{21}$$

A 1R-attack can be done on eight Rule-B^{-1} rounds of Skipjack, using (21). The attack discovers subkey bytes k_6, k_7, k_8, k_9 by checking if $\mathrm{G}^{-24}(P_1^i) \oplus P_4^i$ is active (see Fig. 25). To filter out wrong 32-bit subkey candidates, three ciphertext Λ-sets are used. The complexity is $\approx 2^{43}$ full Skipjack decryptions.

$$\begin{aligned}(P\ P\ A\ P) &\overset{B^{-1}}{\to} (P\ P\ A\ P) \overset{B^{-1}}{\to} (P\ P\ A\ A) \overset{B^{-1}}{\to} (A\ P\ A\ A) \overset{B^{-1}}{\to} (A\ A\ A\ A) \overset{B^{-1}}{\to} \\ (A\ A\ *\ A) &\overset{B^{-1}}{\to} (A\ A\ ?\ ?) \overset{B^{-1}}{\to} (?\ A\ ?\ ?) \overset{B^{-1}}{\to} (?\ ?\ ?\ ?) \overset{A^{-1}}{\to} (A\ ?\ ?\ ?) \overset{A^{-1}}{\to} \\ (A\ ?\ ?\ ?) &\overset{A^{-1}}{\to} (A\ ?\ ?\ ?) \overset{A^{-1}}{\to} (A\ ?\ ?\ ?) \overset{A^{-1}}{\to} (?\ ?\ ?\ ?) \end{aligned} \tag{22}$$

A 1R-attack can be done on 13 inverse rounds of Skipjack, using (22). The attack discovers subkey bytes k_6, k_7, k_8, k_9 by verifying if $P_1^i \oplus \mathrm{G}^{-19}(P_2^i)$ is active (see Fig. 26). To filter out false 32-bit subkey candidates, three ciphertext Λ-sets are used. The complexity is $\approx 2^{43}$ full Skipjack decryptions.

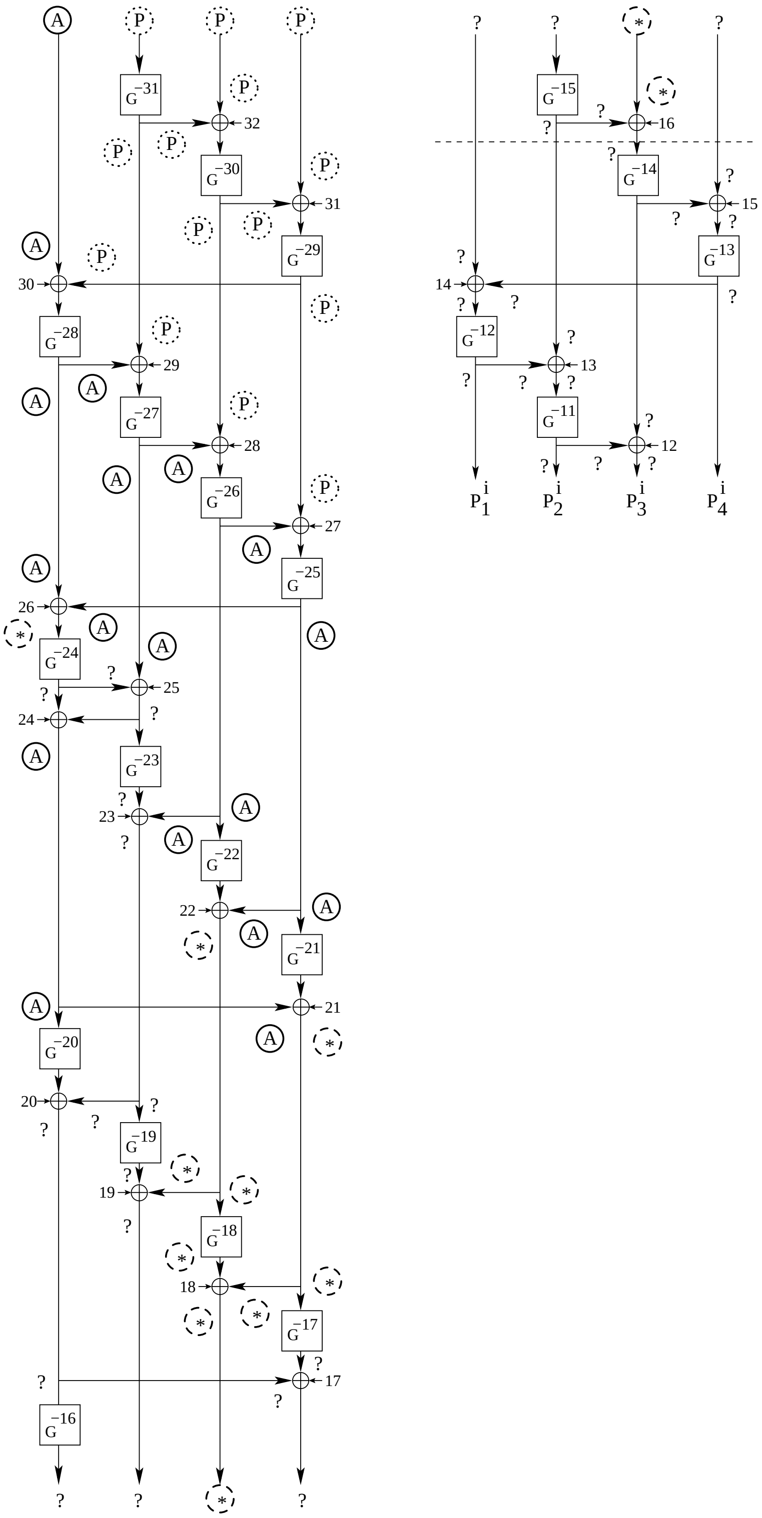

Fig. 24. Propagation of Λ-sets according to chain (20).

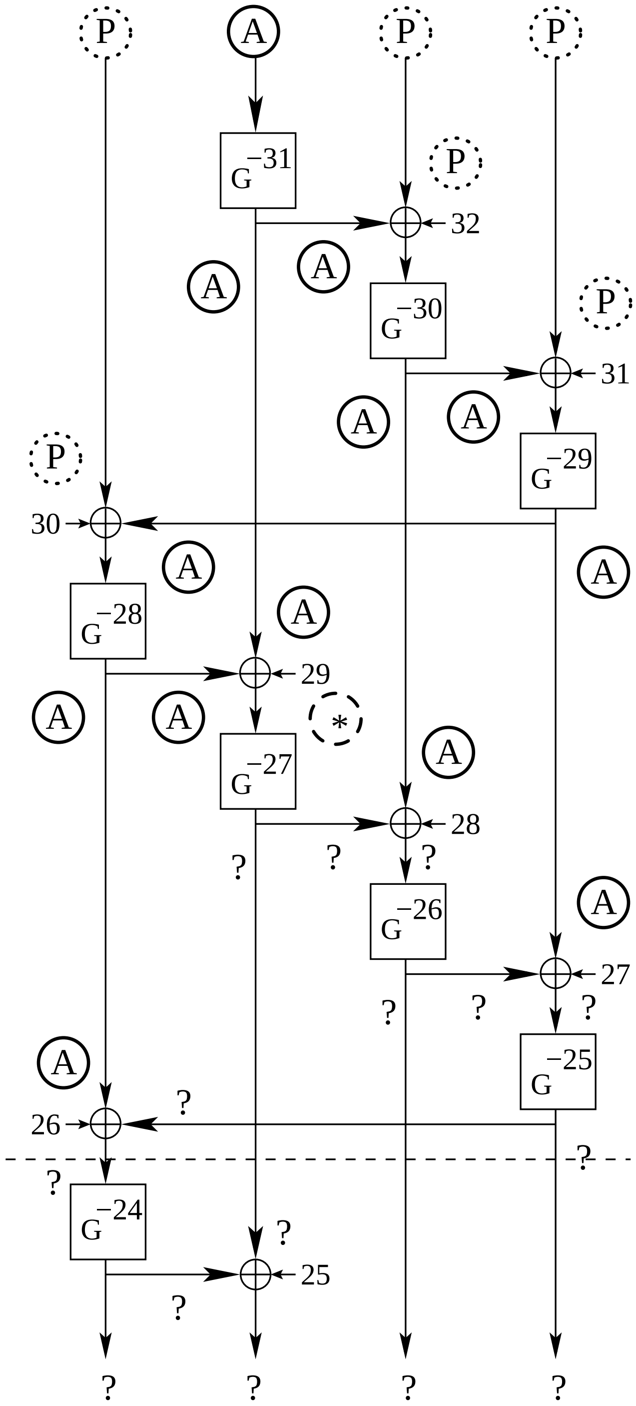

Fig. 25. Propagation of Λ-sets according to chain (21).

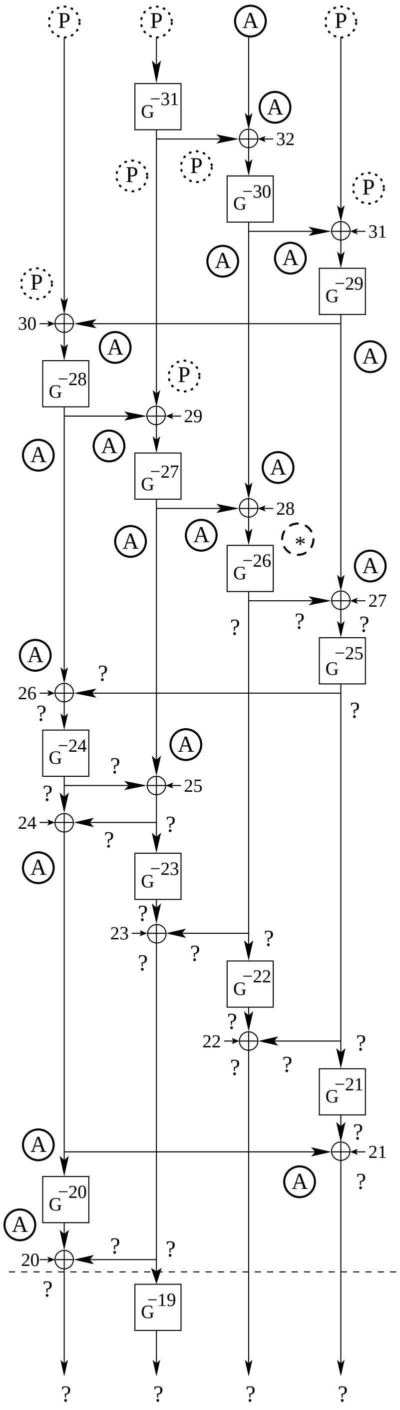

Fig. 26. Propagation of Λ-sets according to chain (22).

$$(P\ P\ P\ A) \overset{B^{-1}}{\to} (P\ P\ P\ A) \overset{B^{-1}}{\to} (P\ P\ P\ A) \overset{B^{-1}}{\to} (A\ P\ P\ A) \overset{B^{-1}}{\to} (A\ A\ P\ A) \overset{B^{-1}}{\to} (A\ A\ A\ A) \overset{B^{-1}}{\to} (A\ A\ A\ *) \overset{B^{-1}}{\to} (?\ A\ A\ ?) \overset{B^{-1}}{\to} (?\ ?\ A\ ?) \overset{A^{-1}}{\to} (A\ ?\ A\ ?) \overset{A^{-1}}{\to} (A\ ?\ A\ ?) \overset{A^{-1}}{\to} (A\ ?\ ?\ ?) \overset{A^{-1}}{\to} (A\ ?\ ?\ ?) \overset{A^{-1}}{\to} (?\ ?\ ?\ ?) \tag{23}$$

A 1R-attack on 13 inverse Skipjack rounds, using chain (23) is identical to the 1R-attack using chain (22). See Fig. 27.

$$(A\ A\ P\ P) \overset{B^{-1}}{\to} (A\ A\ A\ P) \overset{B^{-1}}{\to} (A\ A\ A\ A) \overset{B^{-1}}{\to} (*\ A\ A\ A) \overset{B^{-1}}{\to} (?\ ?\ A\ A) \overset{B^{-1}}{\to} (?\ ?\ ?\ A) \overset{B^{-1}}{\to} (?\ ?\ ?\ ?) \overset{B^{-1}}{\to} (?\ ?\ ?\ ?) \overset{B^{-1}}{\to} (?\ ?\ ?\ ?) \overset{A^{-1}}{\to} (?\ ?\ ?\ ?) \tag{24}$$

A 1R-attack on nine inverse Skipjack rounds, using (24), discovers subkey bytes k_0, k_1, k_2, k_3 by checking if $\mathrm{G}^{-25}(P_4^i) \oplus P_3^i$ is active (see Fig.30). To filter out false 32-bit subkey candidates, three ciphertext Λ-sets are used.

$$(A\ P\ A\ P) \overset{B^{-1}}{\to} (A\ P\ A\ P) \overset{B^{-1}}{\to} (A\ P\ A\ A) \overset{B^{-1}}{\to} (*\ P\ A\ A) \overset{B^{-1}}{\to} (?\ ?\ A\ A) \overset{B^{-1}}{\to} (?\ ?\ ?\ A) \overset{B^{-1}}{\to} (?\ ?\ ?\ ?) \overset{B^{-1}}{\to} (?\ ?\ ?\ ?) \overset{B^{-1}}{\to} (?\ ?\ ?\ ?) \overset{A^{-1}}{\to} (?\ ?\ ?\ ?) \tag{25}$$

A 2R-attack on ten inverse Skipjack rounds, using chain (25), discovers subkey bytes k_8, k_9, k_0, k_1, k_2, k_3 by checking if $\mathrm{G}^{-22}(P_3^i) \oplus \mathrm{G}^{-25}(P_4^i)$ is active (see Fig. 29). To filter out false 48-bit subkey candidates, four ciphertext Λ-sets are used. The complexity is $2^{16} \cdot 2^{48} \cdot 2 \cdot 2^{-5} + 2^{16} \cdot 2^{32} \cdot 2 \cdot 2^{-5} + 2^{16} \cdot 2^{16} \cdot 2 \cdot 2^{-5} + 2^{16} \cdot 2 \cdot 2^{-5} \approx 2^{60}$ full Skipjack decryptions.

$$(A\ P\ P\ A) \overset{B^{-1}}{\to} (A\ P\ P\ A) \overset{B^{-1}}{\to} (A\ P\ P\ A) \overset{B^{-1}}{\to} (*\ P\ P\ A) \overset{B^{-1}}{\to} (?\ ?\ P\ A) \overset{B^{-1}}{\to} (?\ ?\ ?\ A) \overset{B^{-1}}{\to} (?\ ?\ ?\ ?) \overset{B^{-1}}{\to} (?\ ?\ ?\ ?) \overset{B^{-1}}{\to} (?\ ?\ ?\ ?) \overset{A^{-1}}{\to} (?\ ?\ ?\ ?) \tag{26}$$

A 1R-attack on nine inverse Skipjack rounds, using (26) is identical to the 1R-attack using chain (24). See Fig. 30.

$$(P\ A\ A\ P) \overset{B^{-1}}{\to} (P\ A\ *\ A) \overset{B^{-1}}{\to} (P\ A\ ?\ ?) \overset{B^{-1}}{\to} (?\ A\ ?\ ?) \overset{B^{-1}}{\to} (?\ ?\ ?\ ?) \overset{B^{-1}}{\to} (?\ ?\ ?\ ?) \overset{B^{-1}}{\to} (?\ ?\ ?\ ?) \overset{B^{-1}}{\to} (?\ ?\ ?\ ?) \overset{B^{-1}}{\to} (?\ ?\ ?\ ?) \overset{A^{-1}}{\to} (?\ ?\ ?\ ?) \tag{27}$$

A 2R-attack on eight inverse Skipjack rounds, using (27), discovers subkey bytes k_6, k_7, k_8, k_9, k_0, k_1, by checking if $\mathrm{G}^{-24}(P_1^i) \oplus P_4^i \oplus \mathrm{G}^{-27}(P_1^i \oplus P_2^i)$ is active. To filter our false 48-bit subkey candidates, four ciphertext Λ-sets are used. Time complexity is $\approx 2^{60}$ full Skipjack decryptions.

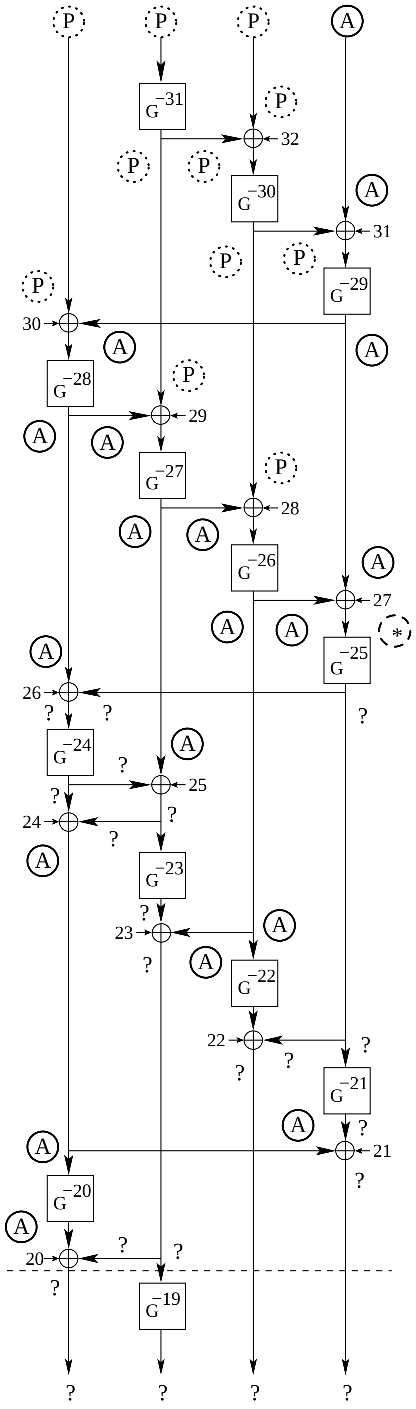

Fig. 27. Propagation of Λ-sets according to chain (23).

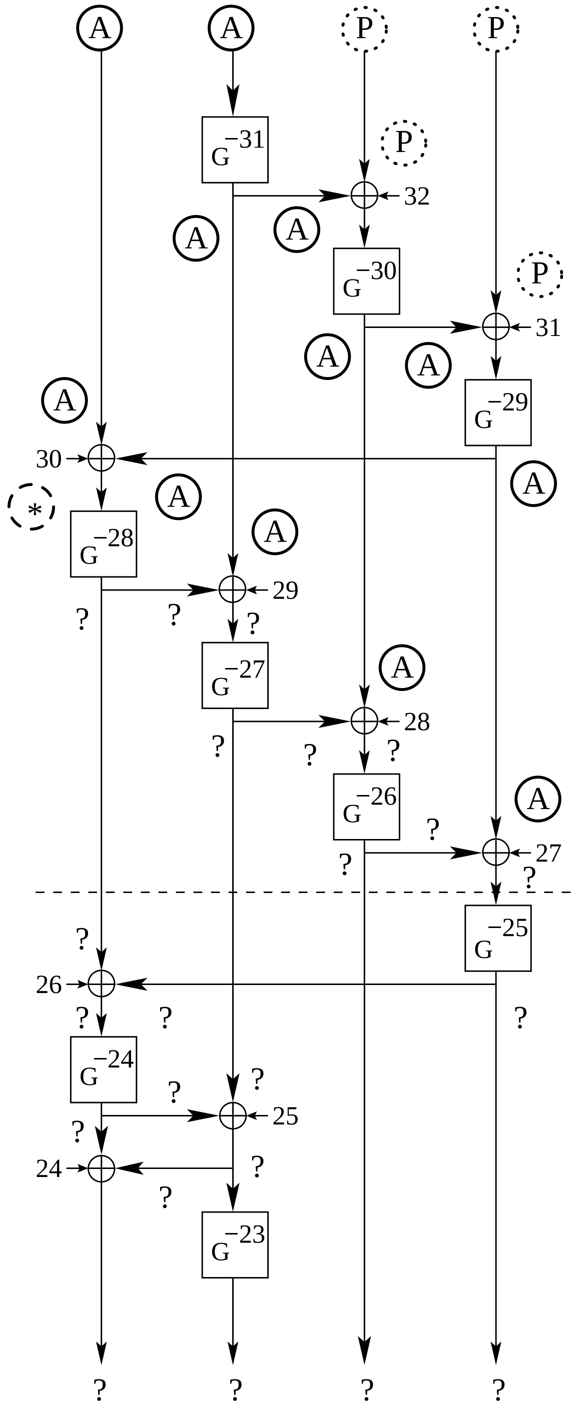

Fig. 28. Propagation of Λ-sets according to chain (24).

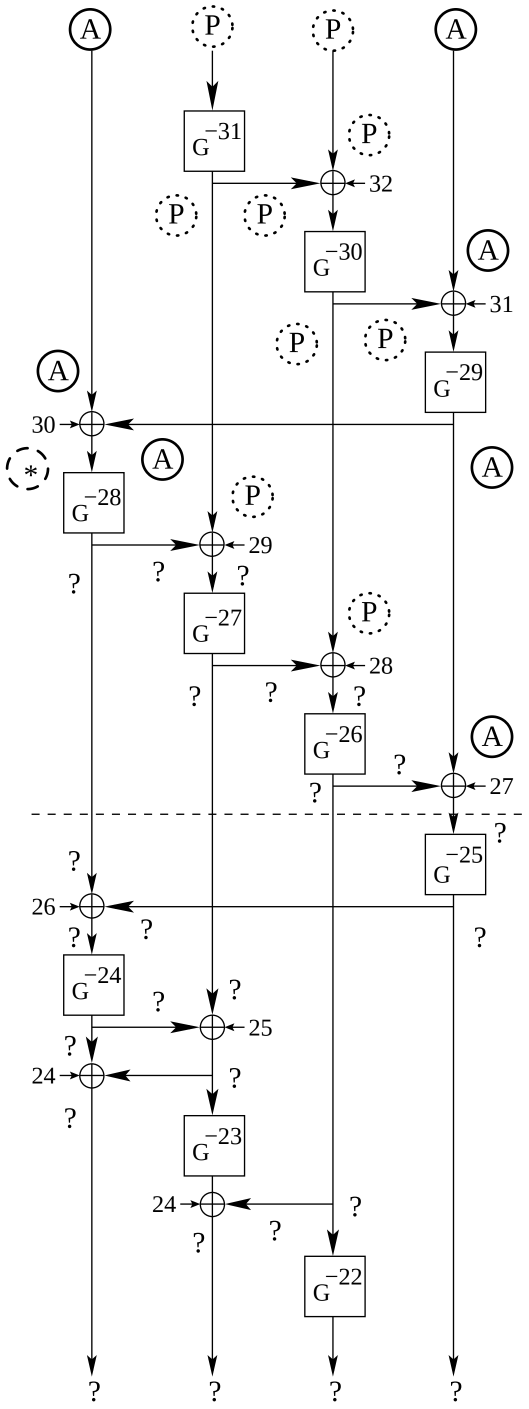

Fig. 29. Propagation of Λ-sets according to chain (25).

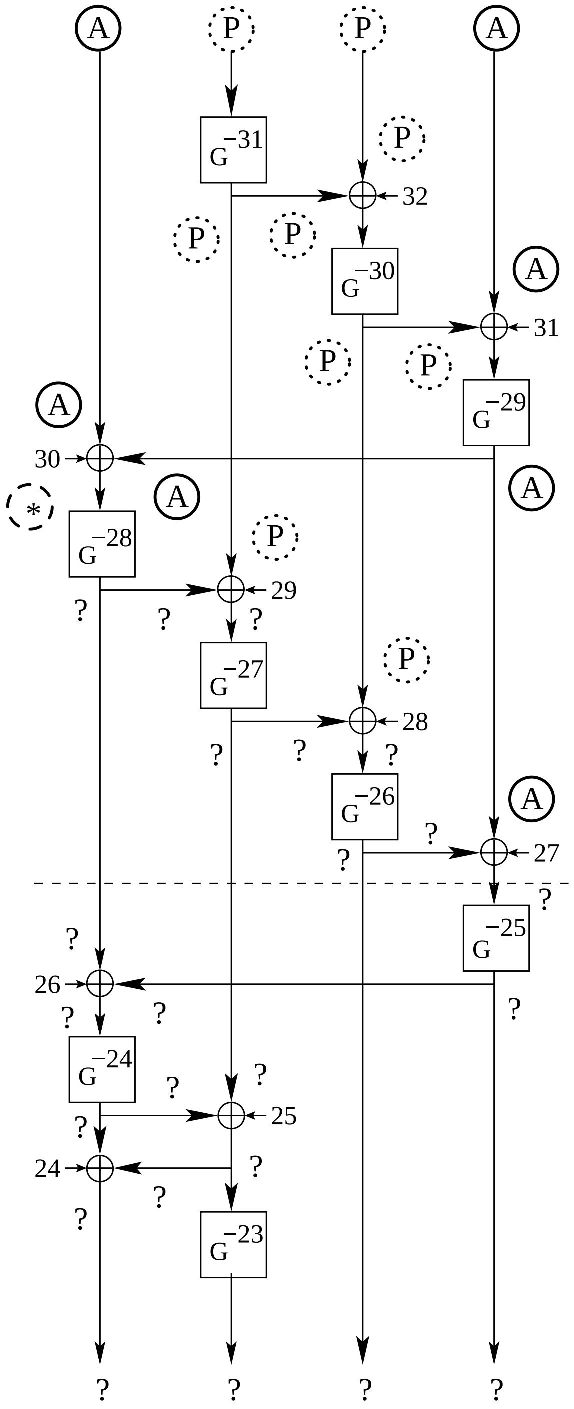

Fig. 30. Propagation of Λ-sets according to chain (26).

$$(P\ A\ P\ A) \overset{B^{-1}}{\rightarrow} (P\ A\ A\ A) \overset{B^{-1}}{\rightarrow} (P\ A\ A\ *) \overset{B^{-1}}{\rightarrow} (?\ A\ A\ ?) \overset{B^{-1}}{\rightarrow} (?\ ?\ A\ ?) \overset{B^{-1}}{\rightarrow} (?\ ?\ ?\ ?) \overset{B^{-1}}{\rightarrow} (?\ ?\ ?\ ?) \overset{B^{-1}}{\rightarrow} (?\ ?\ ?\ ?) \overset{B^{-1}}{\rightarrow} (?\ ?\ ?\ ?) \overset{A^{-1}}{\rightarrow} (?\ ?\ ?\ ?) \tag{28}$$

A 1R-attack on nine inverse Skipjack rounds, using chain (28), discovers subkey bytes k_4, k_5, k_6, k_7 by checking if $\mathrm{G}^{-26}(P_3^i) \oplus P_1^i$ is active. To filter our false 32-bit subkey candidates, three ciphertext Λ-sets are used.

$$(P\ P\ A\ A) \overset{B^{-1}}{\rightarrow} (P\ P\ A\ A) \overset{B^{-1}}{\rightarrow} (P\ P\ A\ *) \overset{B^{-1}}{\rightarrow} (?\ P\ A\ ?) \overset{B^{-1}}{\rightarrow} (?\ ?\ A\ ?) \overset{B^{-1}}{\rightarrow} (?\ ?\ ?\ ?) \overset{B^{-1}}{\rightarrow} (?\ ?\ ?\ ?) \overset{B^{-1}}{\rightarrow} (?\ ?\ ?\ ?) \overset{B^{-1}}{\rightarrow} (?\ ?\ ?\ ?) \overset{A^{-1}}{\rightarrow} (?\ ?\ ?\ ?) \tag{29}$$

A 1R-attack on nine inverse Skipjack rounds, using chain (29), is identical to the 1R-attack using chain (28).

$$(A\ A\ A\ P) \overset{B^{-1}}{\rightarrow} (A\ A\ *\ P) \overset{B^{-1}}{\rightarrow} (A\ A\ ?\ ?) \overset{B^{-1}}{\rightarrow} (?\ A\ ?\ ?) \overset{B^{-1}}{\rightarrow} (?\ ?\ ?\ ?) \overset{B^{-1}}{\rightarrow} (?\ ?\ ?\ ?) \overset{B^{-1}}{\rightarrow} (?\ ?\ ?\ ?) \overset{B^{-1}}{\rightarrow} (?\ ?\ ?\ ?) \overset{B^{-1}}{\rightarrow} (?\ ?\ ?\ ?) \overset{A^{-1}}{\rightarrow} (?\ ?\ ?\ ?) \tag{30}$$

A 2R-attack on eight inverse Skipjack rounds, using chain (30) is identical to the 2R-attack made using chain (27).

$$(A\ A\ P\ A) \overset{B^{-1}}{\rightarrow} (A\ A\ *\ P) \overset{B^{-1}}{\rightarrow} (A\ A\ ?\ ?) \overset{B^{-1}}{\rightarrow} (?\ A\ ?\ ?) \overset{B^{-1}}{\rightarrow} (?\ ?\ ?\ ?) \overset{B^{-1}}{\rightarrow} (?\ ?\ ?\ ?) \overset{B^{-1}}{\rightarrow} (?\ ?\ ?\ ?) \overset{B^{-1}}{\rightarrow} (?\ ?\ ?\ ?) \overset{B^{-1}}{\rightarrow} (?\ ?\ ?\ ?) \overset{A^{-1}}{\rightarrow} (?\ ?\ ?\ ?) \tag{31}$$

A 1R-attack on nine inverse Skipjack rounds, using chain (31), is identical to the 1R-attack using chain (28).

$$(A\ P\ A\ A) \overset{B^{-1}}{\rightarrow} (A\ P\ A\ A) \overset{B^{-1}}{\rightarrow} (A\ P\ A\ *) \overset{B^{-1}}{\rightarrow} (?\ P\ A\ ?) \overset{B^{-1}}{\rightarrow} (?\ ?\ A\ ?) \overset{B^{-1}}{\rightarrow} (?\ ?\ ?\ ?) \overset{B^{-1}}{\rightarrow} (?\ ?\ ?\ ?) \overset{B^{-1}}{\rightarrow} (?\ ?\ ?\ ?) \overset{B^{-1}}{\rightarrow} (?\ ?\ ?\ ?) \overset{A^{-1}}{\rightarrow} (?\ ?\ ?\ ?) \tag{32}$$

A 1R-attack on nine inverse Skipjack rounds, using chain (32), is identical to the 1R-attack using chain (28).

$$(A\ A\ A\ A) \overset{B^{-1}}{\rightarrow} (A\ A\ *\ A) \overset{B^{-1}}{\rightarrow} (A\ A\ ?\ ?) \overset{B^{-1}}{\rightarrow} (?\ A\ ?\ ?) \overset{B^{-1}}{\rightarrow} (?\ ?\ ?\ ?) \overset{B^{-1}}{\rightarrow} (?\ ?\ ?\ ?) \overset{B^{-1}}{\rightarrow} (?\ ?\ ?\ ?) \overset{B^{-1}}{\rightarrow} (?\ ?\ ?\ ?) \overset{B^{-1}}{\rightarrow} (?\ ?\ ?\ ?) \tag{33}$$

A 2R-attack on eight inverse Skipjack rounds, using (33) is identical to the 2R-attack made using chain (27).

5 Related-Key Square Attack

The chain consisting of only passive 16-bit words $(P\ P\ P\ P) \overset{\mathrm{A}}{\to} (P\ P\ P\ P)$ is the only iterative chain of Λ-sets found for Skipjack, that is, this chain can be concatenate with itself forever. But, our attacks do not work with it.

One idea, suggested by P.S.L.M. Barreto, is to make (some of) the subkey words active instead of the plaintext words [15]. This related-key Square attack would always operate with passive plaintext Λ-sets, but would assume that some subkey bytes(s) is(are) active.

An analysis of such attack indicate that, with only one subkey byte active, the longest chain of *key* Λ-sets covers the 6 (initial) rounds of Skipjack (a 6-round distinguisher). In this case, the Λ-sets need to be redefined as containing *8-bit words*. One example makes only subkey byte k_9 active and results in the chain:

$$\begin{aligned}(P\ P\ P\ P\ P\ P\ P\ P) &\overset{\mathrm{A}}{\to} (P\ P\ P\ P\ P\ P\ P\ P) \overset{\mathrm{A}}{\to} (P\ P\ P\ P\ P\ P\ P\ P) \overset{\mathrm{A}}{\to} \\ (P\ P\ A\ *\ A\ *\ P\ P) &\overset{\mathrm{A}}{\to} (?\ ?\ ?\ ?\ A\ *\ P\ P) \overset{\mathrm{A}}{\to} (?\ ?\ ?\ ?\ A * ?\ ?) \overset{\mathrm{A}}{\to} \\ (?\ ?\ ?\ ?\ ?\ ?\ ?\ ?) &\overset{\mathrm{A}}{\to} (?\ ?\ ?\ ?\ ?\ ?\ ?\ ?) \overset{\mathrm{A}}{\to} (?\ ?\ ?\ ?\ ?\ ?\ ?\ ?) \end{aligned} \tag{34}$$

Chain (34) allows a 3R-attack on the 9 initial rounds of Skipjack (see Fig. 31). The attack guess the key bytes k_4, k_5, k_6, and k_7, and determine if $\mathrm{G}^{-6}(C_3^i) \oplus C_4^i$ has the form $A*$, that is, the left-half is active and the right-half is balanced, to find out the correct 32-bit key of the 7th round. The complexity is 2^8 related-keys and $2^{16} \cdot 2^{32} \cdot 2^{-5} + 2^{16} \cdot 2^{16} \cdot 2^{-5} + 2^{16} \cdot 2^{-5} \approx 2^{43}$ full related-key Skipjack encryptions, i.e. using the same all-byte-passive plaintext, but with the last key byte active.

Another example, makes two key bytes simultaneously active (k_8, k_9), and uses 16-bit words. The Λ-set chain is :

$$\begin{aligned}(P\ P\ P\ P) &\overset{\mathrm{A}}{\to} (P\ P\ P\ P) \overset{\mathrm{A}}{\to} (P\ P\ P\ P) \overset{\mathrm{A}}{\to} (P\ A\ A\ P) \overset{\mathrm{A}}{\to} \\ (A\ A\ A\ P) &\overset{\mathrm{A}}{\to} (?\ A\ A\ ?) \overset{\mathrm{A}}{\to} (?\ A\ ?\ ?) \overset{\mathrm{A}}{\to} (?\ ?\ ?\ ?) \overset{\mathrm{A}}{\to} \\ &(?\ ?\ ?\ ?) \end{aligned} \tag{35}$$

The Λ-set chain (35) represents a 7-rounds distinguisher, and allows a 5R-attack on the initial 12 rounds of Skipjack to discover subkey bytes k_4, k_5, k_6,and k_7 (see Fig. 32). The plaintext Λ-set is composed of all passive 16-bit words $P^i = (P\ P\ P\ P)$. The key Λ-set has all key bytes fixed, except k_8, and k_9, which jointly range through all 2^{16} values $0 \ldots 2^{16} - 1$. The attack requires 2^{16} related-keys. The attack proceeds by guessing a 32-bit key value and checking is $\mathrm{G}^{-4}(\mathrm{G}^{-11}(C_2^i \oplus C_1^i))$ is active. The complexity is $2^{16} \cdot 2^{32} \cdot 2^{-4} + 2^{16} \cdot 2^{16} \cdot 2^4 + 2^{16} \cdot 2^4 \approx 2^{44}$ related-key full Skipjack encryptions.

6 Summary

The original chosen-plaintext Square attacks made for the Square block cipher [10] were adapted to the Skipjack block cipher, due to the similarity with which

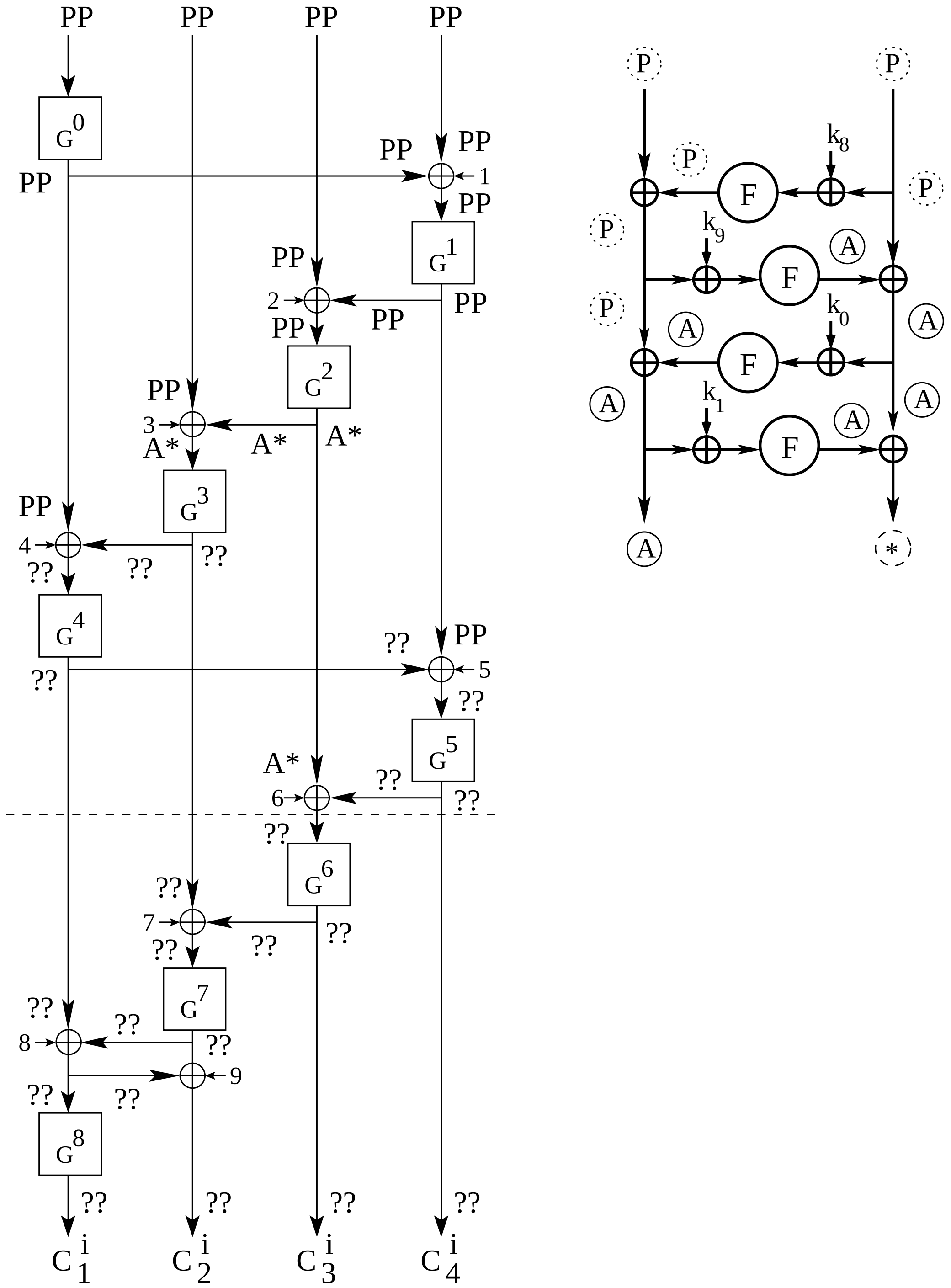

Fig. 31. Related-Key Square attack on 9 rounds of Skipjack.

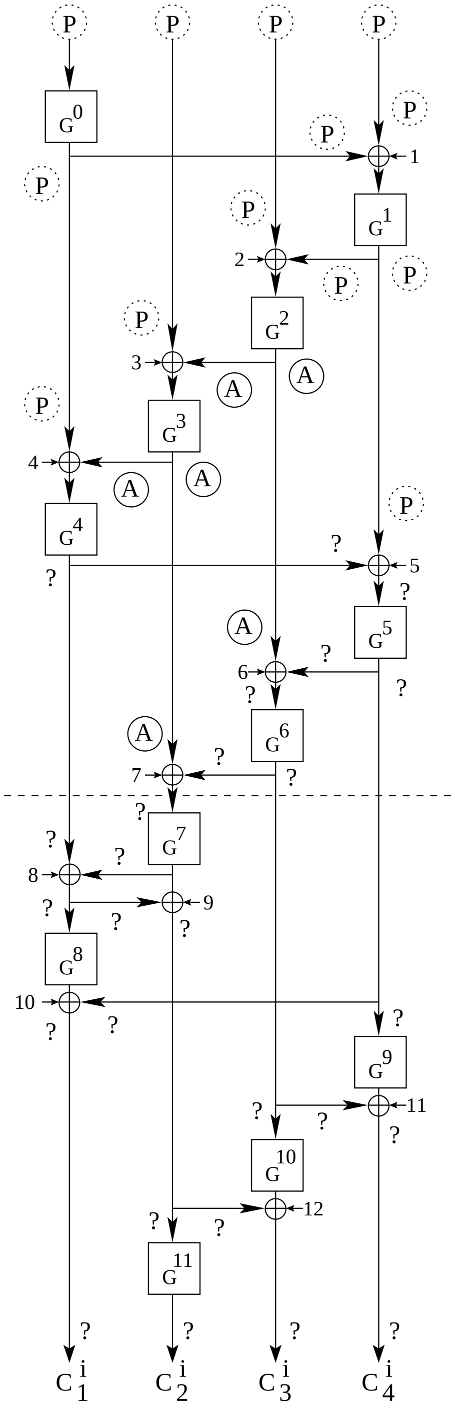

Fig. 32. Related-Key Square attack on 12 rounds of Skipjack.

each cipher breaks its input into fixed-sized sub-blocks, and operates throughout the enciphering/deciphering process with that fixed quantities.

Table 3 compares previous attacks made on Skipjack with the results obtained for the Square attacks.

Table 3. Complexity of different attacks on Skipjack

Rounds	Memory (chosen texts)	Time	Source	Attack Technique
16 ($1 \sim 16$)	2^{22}	2^{22}	[5]	Differential Attack
16 ($1 \sim 16$)	2^{17}	2^{16}	[5]	Yoyo game
31 ($2 \sim 32$)	2^{34}	2^{78}	[4]	Impossible Differential
31 ($1 \sim 31$)	2^{41}	2^{78}	[4]	Impossible Differential
16 ($1 \sim 16$)	2^{17}	$2^{34} \sim 2^{49}$	[13]	Truncated Differentials
16 ($9 \sim 24$)	2	2^{47}	[13]	Truncated Differentials
25 ($4 \sim 28$)	$2^{34.5}$	$2^{61.5}$	[13]	Boomerang Attack
28 ($4 \sim 32$)	2^{41}	2^{77}	[13]	Truncated Differentials
18 ($5 \sim 22$)	2^{17}	2^{44}	[16]	Saturation Attack
22 ($5 \sim 26$)	2^{18}	2^{76}	[16]	Saturation Attack
23 ($5 \sim 27$)	2^{18}	$3 \cdot 2^{75}$	[16]	Saturation Attack
22 ($1 \sim 22$)	2^{49}	2^{44}	[16]	Saturation Attack
26 ($1 \sim 27$)	2^{50}	2^{76}	[16]	Saturation Attack
27 ($1 \sim 27$)	2^{50}	$3 \cdot 2^{75}$	[16]	Saturation Attack
16 ($1 \sim 16$)	$3 * 2^{16}$	2^{76}	see chain (3)	Square Attack
19 ($1 \sim 19$)	$5 * 2^{16}$	2^{59}	see chain (17)	Square Attack
23 ($1 \sim 23$)	$5 * 2^{16}$	2^{76}	see chain (19)	Square Attack
13 ($19 \sim 32$)	$3 * 2^{16}$	2^{43}	see chain (22)	Square Attack
18 ($14 \sim 32$)	$3 * 2^{16}$	2^{43}	see chain (20)	Square Attack
21 ($11 \sim 32$)	$4 * 2^{16}$	2^{60}	see chain (20)	Square Attack
9 ($1 \sim 9$)	$3 \cdot 2^{16}$	2^{43}	see chain (34)	Related-Key Square Atack
12 ($1 \sim 12$)	$3 \cdot 2^{16}$	2^{44}	see chain (35)	Related-Key Square Atack

7 Further Work

A number of possibilities arise, that can lead to improved attacks on Skipjack. They include:

- All the attacks listed in this report started from either end of Skipjack, that is, either from the first Rule-A round or from the last Rule-B round. An idea would be to *insert* Λ-sets in some intermediate round of Skipjack and analyse how the different active-passive-garbled words propagate across each half of the cipher. That's the strategy used in [16], which actually led to better results than ours.

– Another idea, also suggested by P.S.L.M. Barreto is to analyse *residual traces* of balance, that is, instead of looking at full 16-bit words being active/passive or garbled, the intuition is to detect of l-bit amounts, $1 \leq l \leq 15$ are balaced.

8 Acknowledgements

The authors are grateful to Paulo S.L.M. Barreto for many fruitful discussions concerning previous drafts of this paper.

References

1. A. Biryukov, D. Wagner, *"Slide Attacks," Fast Software Encryption Workshop, LNCS 1636*, L.R. Knudsen, Ed., Springer-Verlag, 1999, pp. 245–259.
2. B. Schneier, J Kelsey, *"Unbalanced Feistel Networks and Block Cipher Design," Fast Software Encryption Workshop, LNCS 1039*, D. Gollmann, Ed., Springer-Verlag, 1996, pp. 121–144.
3. C. D'Halluin, G. Bijnens, V. Rijmen, B. Preneel, *"Attack on Six Rounds of Crypton," Fast Software Encryption Workshop, LNCS 1636*, L.R. Knudsen, Ed., Springer-Verlag, 1999, pp. 46–59.
4. E. Biham, A. Biryukov, A. Shamir, *"Cryptanalysis of Skipjack Reduced to 31 Rounds using Impossible Differentials,"* Technion, Computer Science Dept., Technical Report CS 0947, 1998, 12 pages.
5. E. Biham, A. Biryukov, O. Dunkelman, E. Richardson, A. Shamir, *"Initial observations on Skipjack: Cryptanalysis of Skipjack-3XOR,"* Technion, Computer Science Dept., Technical Report CS0946, 1998, 14 pages.
6. E. Biham, A. Shamir, *"Differential Cryptanalysis of the Data Encryption Standard,"* Springer-Verlag, 1993.
7. E.F. Brickell, D.E. Denning, S.T. Kent, D.P. Maher, W. Tuchman, *"Skipjack Review,"* Interim Report, The Skipjack Algorithm, July 28, 1993, available at *http://www.austinlinks.com/Crypto/skipjack-review.html*
8. *"Escrowed Encryption Standard (EES),"* Federal Information Processing Standards Publication 185, FIPS PUB 185, Feb. 9, 1994, available at *http://www.itl.nist.gov/fipspubs/fip185.htm*
9. FIPS 46, *"Data Encryption Standard,"* Federal Information Processing Standards Publication 46, US Department of Commerce/National Bureau of Standards, National Technical Information Service, Springfield, Virginia, 1977 (revised as FIPS 46-1:1988; FIPS 46-2:1993).
10. J. Daemen, L.R. Knudsen, V. Rijmen, *"The Block Cipher Square," Fast Software Encryption Workshop, LNCS 1267*, E. Biham, Ed., Springer-Verlag, 1997, pp. 149–165.
11. J. Daemen, V. Rijmen, *"AES Proposal: Rijndael,"* The First Advanced Encryption Standard Candidate Conference, NIST, 1998.
12. L. Granboulan, *"Flaws in Differential Cryptanalysis of Skipjack," Fast Software Encryption Workshop*, M. Matsui, Ed., Springer-Verlag, 2001, to appear.
13. L.R. Knudsen, M.J.B. Robshaw, D. Wagner, *"Truncated Differentials and Skipjack," Advances in Cryptology, Proceedings Crypto'99, LNCS 1666*, M. Wiener, Ed., Springer-Verlag, 1999, pp. 165–180.

14. L.R. Knudsen, D. Wagner, *"On the Structure of Skipjack,"* Discrete Applied Mathematics, Vol. 111, Issue 1–2, Jul. 15, 2001, pp. 103–116.
15. J. Nakahara Jr, B. Preneel, J. Vandewalle, *"Square Attacks on Reduced-Round PES and IDEA Block Ciphers",* Dept. of Electrical Enginnering (ESAT), COSIC Group, Internal Report, 2000.
16. H. Hwang, W. Lee, S. Lee, S. Lee, J. Lim, *"Saturation Attacks on Reduced Round Skipjack,"* to appear in the Proceedings of FSE'2002, Leuven, Belgium, Feb. 4–6, 2002.
17. *"Skipjack and KEA Specification,"* version 2.0, 29 May 1998, available at the National Institute of Standards and Technology Web site *http://csrc.nist.gov/encryption/skipjack–kea.htm*
18. V. Rijmen, J. Daemen, B. Preneel, A. Bosselaers, E. De Win, *"The Cipher SHARK," Fast Software Encryption Workshop, LNCS 1039*, D. Gollmann, Ed., Springer-Verlag, 1996, pp. 99–112.