Interpolation Attacks of the Block Cipher: SNAKE

Shiho Moriai[1]*, Takeshi Shimoyama[2]*, and Toshinobu Kaneko[3]

[1] NTT Laboratories
1-1 Hikari-no-oka, Yokosuka, 239-0847 Japan
shiho@isl.ntt.co.jp
[2] Fujitsu Laboratories LTD.
4-1-1, Kamikodanaka Nakahara-ku Kawasaki, 211-8588 Japan
shimo@flab.fujitsu.co.jp
[3] Science University of Tokyo
2641 Yamazaki, Noda, Chiba, 278-8510 Japan
kaneko@ee.noda.sut.ac.jp

Abstract. This paper presents an efficient interpolation attack using a computer algebra system. The interpolation attack proposed by Jakobsen and Knudsen was shown to be effective for attacking ciphers that use simple algebraic functions. However, there was a problem that the complexity and the number of pairs of plaintexts and ciphertexts required for the attack can be overestimated. We solve this problem by first, finding the actual number of coefficients in the polynomial (or rational expression) used in the attack by using a computer algebra system, and second, by finding the polynomial (or rational expression) with fewest coefficients by choosing the plaintexts. We apply this interpolation attack to the block cipher SNAKE proposed by Lee and Cha at JW-ISC'97. In the SNAKE family there are two types of Feistel ciphers, SNAKE(1) and SNAKE(2), with different round functions. Both of them use the inverse function in Galois Field GF(2^m) as S-box. We show that when the block size is 64 bits and $m = 8$, all round keys are recovered for SNAKE(1) and SNAKE(2) with up to 11 rounds. Moreover, when the block size is 128 bits and $m = 16$, all round keys are recovered for SNAKE(1) with up to 15 rounds and SNAKE(2) with up to 16 rounds.

1 Introduction

Since two powerful cryptanalyses on block ciphers, differential cryptanalysis[1] and linear cryptanalysis[6], were presented, some new block ciphers with provable security against these cryptanalyses have been proposed. On the other hand, Jakobsen and Knudsen raised the alarm that some of them are easy to cryptanalyze by algebraic attacks such as higher order differential attack and interpolation attack[3]. These attacks are effective for attacking ciphers that use simple algebraic functions. For example, there is the 6-round prototype Feistel cipher presented in [8], called the cipher $\mathcal{KN}$. It uses the cubing function in

* Most part of this work was done while the authors were with TAO, or Telecommunications Advancement Organization of Japan.

L. Knudsen (Ed.): FSE'99, LNCS 1636, pp. 275–289, 1999.

$\mathrm{GF}(2^{33})$ in the round function, and was broken by the higher order differential attack exploiting the low degree of polynomial expression over $\mathrm{GF}(2)$. A variant of the cipher, called the cipher $\mathcal{PURE}$, which uses the cubing function in $\mathrm{GF}(2^{32})$ as the round function, was broken by the interpolation attack up to 32 rounds by exploiting the low degree of polynomial expression over $\mathrm{GF}(2^{32})$. Moreover, a slightly modified version of the cipher SHARK[9], which uses the inverse function in $\mathrm{GF}(2^8)$ as S-box, was broken up to 5 rounds by an interpolation attack exploiting the low degree of rational expression over $\mathrm{GF}(2^8)$.

The principle of the interpolation attack is that, roughly speaking, if the ciphertext is represented as a polynomial or rational expression of the plaintext with N coefficients, the polynomial or rational expression can be constructed using N pairs of plaintexts and ciphertexts. Since N determines the complexity and the number of pairs required for the attack, it is important to find as small N as possible.

This paper shows two solutions to find a tighter upper bound of N. The first problem is that generally it is difficult to find the actual number of coefficients in the polynomial or rational expression. In [3] Jakobsen and Knudsen estimated it from the degree of the polynomial or rational expression. However, this method often overestimates it when we use a multivariate polynomial or rational expression, in particular. As the solution to this problem, we compute the actual polynomial or rational expression by using a computer algebra system and find the number of coefficients. The second problem is the number of coefficients (or the degree) of the polynomial or rational expression varies with the plaintexts chosen. If we use a computer algebra system, it is easy to compute the number of coefficients of the polynomial or rational expression in a few variables. We can find the polynomial or rational expression with the fewest coefficients by choosing the plaintexts.

We apply this interpolation attack to the block cipher SNAKE proposed by Lee and Cha at JW-ISC'97[5]. This cipher is not a prototype cipher and we don't modify it to simplify the cryptanalysis. The cipher SNAKE is a Feistel cipher with provable resistance against differential and linear cryptanalysis. In [5], it is also claimed that SNAKE is resistant against higher order differential attack and interpolation attack, though the rationale was not discussed enough. SNAKE(1) and SNAKE(2) have different round functions. To put it concretely, the structure of the round function is the same, the substitution-permutation network (SPN). Both of them use the same number of S-boxes in the round function, the function used as the S-box is the same, e.g., the inverse function in $\mathrm{GF}(2^m)$, but only the diffusion layer is different.

We apply to the cipher SNAKE the interpolation attack using *rational expressions*. If we represent the cipher SNAKE as a polynomial, the attack becomes impractical with only a few rounds, since the number of coefficients in the polynomial increases to the upper bound of the number of pairs we can obtain. This is because the degree of the inverse function in $\mathrm{GF}(2^m)$ in polynomial expression is very high as follows: $f(x) = x^{-1} = x^{2^m-2}$. Using a computer algebra system, we find the rational expression with the fewest coefficients by choosing

the plaintexts. As a result, both of the SNAKE ciphers with many rounds are broken. When the block size is 64 bit and $m = 8$, all round keys are recovered for SNAKE(1) and SNAKE(2) with up to 11 rounds. Moreover, when the block size is 128 bit and $m = 16$, all round keys are recovered for SNAKE(1) with up to 15 rounds and SNAKE(2) with up to 16 rounds.

This paper is organized as follows. In Section 2, we give a summary of the interpolation attack. Section 3 describes the specifications of the cipher SNAKE. In Sections 4 and 5, we apply the interpolation attack to the cipher SNAKE with blocksize 64 bits and 128 bits, respectively. In Section 6, we discuss some problems and make concluding remarks.

2 The Interpolation Attack

In this section, we describe the outline of the interpolation attack proposed by Jakobsen and Knudsen in [3] and explain the notations used in this paper. The target of the attack is an iterated cipher with block size $2n$ bits and R rounds. We denote a plaintext by x and a ciphertext by y. Let x be the concatenation of u subblocks $x_i \in \mathrm{GF}(2^m)$, where $2n = m \times u$. We define y similarly.

$$x = (x_u, x_{u-1}, \ldots, x_1) \in \mathrm{GF}(2^m)^u, \quad x_i \in \mathrm{GF}(2^m)$$
$$y = (y_u, y_{u-1}, \ldots, y_1) \in \mathrm{GF}(2^m)^u, \quad y_j \in \mathrm{GF}(2^m)$$

Moreover, we denote the i-th round key by $k^{(i)}$ and let the length of $k^{(i)}$ be l bits. Similarly let $k^{(i)}$ be the concatenation of t subblocks $k_j^{(i)}$, where $l = m \times t$.

$$k^{(i)} = (k_t^{(i)}, k_{t-1}^{(i)}, \ldots, k_1^{(i)}) \in \mathrm{GF}(2^m)^t \quad k_j^{(i)} \in \mathrm{GF}(2^m)$$

2.1 Global Deduction

If the key is fixed to k, a ciphertext subblock $y_j \in \mathrm{GF}(2^m)$ can be expressed as a polynomial in plaintext subblocks $\{x_u, x_{u-1}, \ldots, x_1\}$ as follows:

$$y_j = f_{jk}(x_u, x_{u-1}, \ldots, x_1) \in \mathrm{GF}(2^m)[x_u, x_{u-1}, \ldots, x_1],$$

where $\mathrm{GF}(2^m)[X]$ is the polynomial ring of $X = \{x_u, \ldots, x_1\}$ over $\mathrm{GF}(2^m)$. If the number of coefficients in $f_{jk}(x_u, x_{u-1}, \ldots, x_1)$ is N, the attacker can construct $f_{jk}(x_u, x_{u-1}, \ldots, x_1)$ from different N pairs of plaintexts and ciphertexts. If we define $\deg_{x_i} f_{jk}$ as the degree of $f_{jk}(x_u, x_{u-1}, \ldots, x_1)$ with respect to x_i, N is estimated as follows.

$$N \leq \prod_{1 \leq i \leq u} (\deg_{x_i} f_{jk} + 1) \tag{1}$$

Note that N can be overestimated when u is large and the polynomial is sparse.

Once the attacker constructs $f_{jk}(x_u, x_{u-1}, \ldots, x_1)$, (s)he can encrypt any plaintext into the corresponding ciphertext for key k, without knowing the key. This attack is called *global deduction* by Knudsen[4,3]. Similarly, by swapping ciphertexts and plaintexts, once the attacker can construct $x_i = f'_{ik}(y_u, y_{u-1}, \ldots, y_1)$ $\in \mathrm{GF}(2^m)[y_u, y_{u-1}, \ldots, y_1]$, (s)he can decrypt any ciphertext into the corresponding plaintext for key k, without knowing the key.

2.2 Instance Deduction

If some subblocks of plaintexts are fixed to some values as e.g., $x = (0, \ldots, 0, x_1)$, a ciphertext subblock $y_j \in \mathrm{GF}(2^m)$ can be expressed as a polynomial as follows:

$$y_j = f_{jk}(x_1) \in \mathrm{GF}(2^m)[x_1].$$

In this case, $f_{jk}(x_1)$ is a polynomial in one variable x_1. Generally, there are fewer coefficients in $f_{jk}(x_1)$ than in global deduction. Therefore, the attacker can construct $f_{jk}(x_1)$ from fewer chosen plaintexts and ciphertexts. Let N be the number of coefficient and let $\deg_{x_1} f_{jk} = d$, and N is estimated as $N \leq d + 1$. Once the attacker can construct $f_{jk}(x_1)$ from N pairs of plaintexts and ciphertexts, (s)he can encrypt a subset of all plaintexts, e.g., $x = (0, \ldots, 0, x_1)$, $^{\forall}x_1 \in \mathrm{GF}(2^m)$, into the corresponding ciphertexts for key k, without knowing the key. This attack is called *instance deduction* by Knudsen[4,3]. Similarly, by swapping ciphertexts and plaintexts, the attack where a subset of all ciphertexts are decrypted into the corresponding plaintexts is possible.

2.3 Key Recovery

The attacker recovers the last round key as follows. We denote the output of the $(R-1)$-th round by $\tilde{y} = (\tilde{y}_u, \tilde{y}_{u-1}, \ldots, \tilde{y}_1) \in \mathrm{GF}(2^m)^u$. A ciphertext subblock $\tilde{y}_j \in \mathrm{GF}(2^m)$ can be expressed as a polynomial in $\{x_u, x_{u-1}, \ldots, x_1\}$ as follows:

$$\tilde{y}_j = \tilde{f}(x_u, x_{u-1}, \ldots, x_1) \in \mathrm{GF}(2^m)[x_u, x_{u-1}, \ldots, x_1].$$

Let N' be the number of coefficients in $\tilde{f}(x_u, x_{u-1}, \ldots, x_1)$. On the other hand, $\tilde{y}_j$ can be also expressed using the ciphertext y and the last round key $k^{(R)}$. Therefore, if N' pairs of plaintexts x and ciphertexts y are available, the attacker can construct $\tilde{f}(x_u, x_{u-1}, \ldots, x_1)$ using $\tilde{y}_j$ which is computed using y and a guessed $k^{(R)}$.

$$\tilde{f}(x_u, x_{u-1}, \ldots, x_1) = \tilde{y}_j(y, k^{(R)}) \tag{2}$$

If Eq. (2) holds for another plaintext/ciphertext pair, the guessed $k^{(R)}$ is correct with high probability. From the procedure above, the last round key is recovered from any $N' + 1$ pairs of plaintexts and ciphertexts. The average of the required complexity for recovering the last round key is $(N' + 1)2^{l'-1}$, where l' is the number of last round key bits effective in Eq. (2). Repeating similar procedures, the attacker can find all round keys.

In the above, we showed only how to recover the last round key in the case of the global deduction attack, or known plaintext attack. Similarly the instance deduction attack, or chosen plaintext attack is also possible. In the instance deduction attack, the attacker can only use chosen plaintexts and ciphertexts, but fewer pairs are required than in the global deduction attack.

2.4 Meet-in-the-Middle Approach

The meet-in-the-middle approach in the interpolation attack was introduced by Jakobsen and Knudsen[3], which is effective for some attacks on block ciphers.

We denote the output of a certain internal round by $z = (z_u, z_{u-1}, \ldots, z_1) \in \mathrm{GF}(2^m)^u$. A subblock of z, $z_j \in \mathrm{GF}(2^m)$ can be expressed as a polynomial in $\{x_u, x_{u-1}, \ldots, x_1\}$ as follows:

$$z_j = f(x_u, x_{u-1}, \ldots, x_1) \in \mathrm{GF}(2^m)[x_u, x_{u-1}, \ldots, x_1]$$

On the other hand, z_j can be also expressed as a polynomial in $\{\tilde{y}_u, \tilde{y}_{u-1}, \ldots, \tilde{y}_1\}$ as follows:

$$z_j = g(\tilde{y}_u, \tilde{y}_{u-1}, \ldots, \tilde{y}_1) \in \mathrm{GF}(2^m)[\tilde{y}_u, \tilde{y}_{u-1}, \ldots, \tilde{y}_1].$$

Note that $\tilde{y}_j$ can be computed from the ciphertext y and a guessed $k^{(R)}$.

Therefore, Eq. (3) is constructed by guessing $k^{(R)}$.

$$f(x_u, x_{u-1}, \ldots, x_1) = g(\tilde{y}_u, \tilde{y}_{u-1}, \ldots, \tilde{y}_1) \tag{3}$$

The number of pairs required for constructing Eq. (3) is computed as follows. If f and g are represented as polynomials, the required number of pairs is

$$(\#\text{ of coefs. in } f) + (\#\text{ of coefs. in } g).$$

If f and g are represented as rational expressions $f = \frac{f_1}{f_2}$ and $g = \frac{g_1}{g_2}$, where $f_2 \neq 0$ and $g_2 \neq 0$, it is

$$\begin{aligned}&((\#\text{ of coefs. in } f_1) - 1) \times (\#\text{ of coefs. in } g_2)\\ &+ (\#\text{ of coefs. in } f_2) \times ((\#\text{ of coefs. in } g_1) - 1).\end{aligned}$$

Note that we subtract 1's because we can fix one of the coefficients in the rational expression to a certain value, e.g., 1. The attacker can judge whether $k^{(R)}$ is correct or not by examining if Eq. (3) holds for another plaintext/ciphertext pair.

3 SNAKE

The cipher SNAKE is a Feistel cipher, which has two types, SNAKE(1) and SNAKE(2), with different round functions. The general form is SNAKE$(i)(m, s, w, r)$, where

i – (= 1 or 2) the type of SNAKE described in the below,
m – the size of input and output of the S-box in bit,
s – the number of S-boxes used in the round function,
w – block size in bit ($w = 2sm$),
r – the number of rounds.

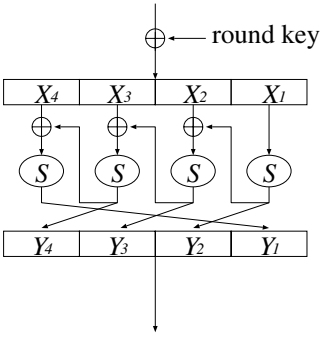

Fig. 1. Round function of SNAKE(1)

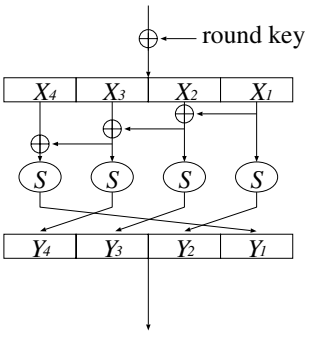

Fig. 2. Round function of SNAKE(2)

Figures 1 and 2 show the round functions of SNAKE(1) and SNAKE(2) for $s = 4$, which were demonstrated in [5]. For the S-box in the round function, the inverse function $S(x) = x^{-1}$ in $\mathrm{GF}(2^m)$ is used, because differential probability and linear probability of $S(x)$ are 2^{2-m} when m is even. In this paper we define the S-box as follows, though the output for input 0 is not defined in [5].

$$S(x) = \begin{cases} x^{-1} \text{ in } \mathrm{GF}(2^m) & x \neq 0 \\ 0 & x = 0 \end{cases}$$

Since SNAKE$(i)(8, 4, 64, 16)$ is given as an example in [5], we apply the interpolation attack to it in Section 4. Moreover, we also apply the interpolation attack to a 128-bit variant, SNAKE$(i)(\mathbf{16}, 4, \mathbf{128}, 16)$ in Section 5, since in [5] it is claimed that one of merits of the cipher SNAKE is that its encrypting data block length (=block size) is flexible.

4 Interpolation Attack of SNAKE$(i)(8, 4, 64, r)$

4.1 Rational Expression over $\mathrm{GF}(2^8)$ of SNAKE$(i)(8, 4, 64, r)$

In this section, we attack SNAKE$(i)(8, 4, 64, r)$ using the interpolation attack. If we represent the cipher SNAKE as a polynomial, the attack becomes impractical with only a few rounds, since the number of coefficients in the polynomial increases to the upper bound of the number of pairs we can obtain. Therefore, we represent SNAKE as a rational expression over $\mathrm{GF}(2^8)$.

Let the plaintext block and the ciphertext block be as follows.

$$x = (x_8, x_7, \ldots, x_1) \in \mathrm{GF}(2^8)^8, \quad x_i \in \mathrm{GF}(2^8)$$
$$y = (y_8, y_7, \ldots, y_1) \in \mathrm{GF}(2^8)^8, \quad y_j \in \mathrm{GF}(2^8)$$

We denote the i-th round key by

$$k^{(i)} = (k_4^{(i)}, k_3^{(i)}, k_2^{(i)}, k_1^{(i)}) \in \mathrm{GF}(2^8)^4, \quad k_j^{(i)} \in \mathrm{GF}(2^8).$$

Moreover, we denote the upper half (32 bits) of the output of the r-th round by

$$z^{(r)} = (z_4^{(r)}, z_3^{(r)}, z_2^{(r)}, z_1^{(r)}) \in \mathrm{GF}(2^8)^4, \quad z_j^{(r)} \in \mathrm{GF}(2^8).$$

Global deduction. In the global deduction, we represent a ciphertext subblock as a rational expression over $\mathrm{GF}(2^8)$ in $\{x_8, x_7, \ldots, x_1\}$. First of all, we show that the round functions of SNAKE(1) and SNAKE(2) can be represented as simple rational expressions as follows:

SNAKE(1)

$$Y_2 = \frac{1}{X_1}$$
$$Y_3 = \frac{1}{X_2 + \frac{1}{X_1}}$$
$$Y_4 = \frac{1}{X_3 + \frac{1}{X_2 + \frac{1}{X_1}}}$$
$$Y_1 = \frac{1}{X_4 + \frac{1}{X_3 + \frac{1}{X_2 + \frac{1}{X_1}}}}$$

SNAKE(2)

$$Y_2 = \frac{1}{X_1}$$
$$Y_3 = \frac{1}{X_1 + X_2}$$
$$Y_4 = \frac{1}{X_1 + X_2 + X_3}$$
$$Y_1 = \frac{1}{X_1 + X_2 + X_3 + X_4},$$

where variables $X_i, Y_j \in \mathrm{GF}(2^8)$ are shown in Figures 1 and 2.

Next, we extend the expressions of the round function to the entire cipher. In a Feistel cipher, there are XORs between 32-bit data in each round. These operations are regarded as four additions on $\mathrm{GF}(2^8)$. We'd like to find the rational expression over $\mathrm{GF}(2^8)$ of each subblock of the output of the r-th round, $z_j^{(r)} = \frac{f_{j1}^{(r)}}{f_{j2}^{(r)}}$, where $f_{j1}^{(r)}, f_{j2}^{(r)} (\neq 0) \in \mathrm{GF}(2^8)[x_8, \ldots, x_1, k_4^{(1)}, \ldots, k_1^{(1)}, \ldots, k_4^{(r)}, \ldots, k_1^{(r)}]$.

We use the computer algebra system Risa/Asir[7] to compute the rational expressions. It usually takes much time and space complexity to find them since the number of variables and the degree increases as the number of rounds increases. However, it is possible to find the rational expressions of the cipher SNAKE with only a few rounds. We show the *actual* numbers of coefficients in the rational expressions in Table 1. The number of coefficients we find here is very important and useful for evaluating the tighter upper bound of the complexity and the number of p/c pairs in the key-recovery attack that uses the meet-in-the-middle approach (see Section 5).

For estimating the number of coefficients in the rational expressions of SNAKE with more rounds, we use the following two techniques.

- decrease the number of variables by representing each round key $k_j^{(r)}$ as $\kappa^i \in \mathrm{GF}(2^8)$, i.e., a monomial in κ, where $\kappa \in \mathrm{GF}(2^8)$ and i is randomly chosen from $\mathrm{GF}(2^8) \setminus \{0, 255\}$.
- estimate the upper bound of the number of coefficients using Eq. (1), since it is easy to find the degree of the rational expression with respect to each variable.

Table 1. # of coef. in rational exp. over GF(2^8) of SNAKE(1) and SNAKE(2) (global deduction)

	SNAKE(1)				SNAKE(2)			
$z_4^{(1)}, z_3^{(1)}, z_2^{(1)}, z_1^{(1)}$	$\frac{(12)}{(8)}$,	$\frac{(6)}{(4)}$,	$\frac{(3)}{(2)}$,	$\frac{(24)}{(16)}$	$\frac{(5)}{(4)}$,	$\frac{(4)}{(3)}$,	$\frac{(3)}{(2)}$,	$\frac{(6)}{(5)}$
$z_4^{(2)}, z_3^{(2)}, z_2^{(2)}, z_1^{(2)}$	$\frac{(432)}{(352)}$,	$\frac{(108)}{(88)}$,	$\frac{(40)}{(32)}$,	$\frac{(1760)}{(1540)}$	$\frac{(85)}{(72)}$,	$\frac{(34)}{(27)}$,	$\frac{(14)}{(10)}$,	$\frac{(198)}{(185)}$

Note) (# of coefs. in the numerator)/(# of coefs. in the denominator)

We show the degrees of the rational expressions over GF(2^8) with respect to each variable in Table 2. Since for every subblock of every round $z_j^{(r)} \in \mathrm{GF}(2^8)$, the rational expressions of SNAKE(1) and SNAKE(2) are of the same degree with respect to each variable, we put them together in one table, Table 2.

Instance deduction. In the instance deduction, we fix some subblocks of the plaintexts $x = (x_8, x_7, \ldots, x_1)$ to a certain value. For example, we fix $\{x_7, \ldots, x_1\}$ to $\{0, \ldots, 0\}$, and represent a ciphertext subblock as a rational expression over GF(2^8) in x_8. If the number of coefficients in this rational expression in x_8, denoted by N, does not exceed $2^8 = 256$, we can construct the rational expression using N pairs of chosen plaintexts and ciphertexts. Therefore, it is desirable to find chosen p/c pairs such that the required number of pairs is as small as possible.

Chosen plaintexts useful for attacking SNAKE(1). We decided to find the rational expression with the fewest coefficients from the rational expressions in one variable. The reason for this is as follows. Let α and β be the numbers of variables. For the rational expression of a subblock $z_j^{(r)}$, if $\alpha > \beta$, the minimum value of the number of coefficients in the rational expression in α variables is larger than that in β variables.

It is easy to compute the rational expressions in one variable for all possible chosen plaintexts, since there are only 2^8 combinations. Our experimental results show that when we choose plaintexts s.t. $(x_8, 0, \ldots, 0)$ the number of coefficients in the rational expression in x_8 is the smallest for SNAKE(1). Table 3 shows the degrees of the rational expressions over GF(2^8) when we choose plaintexts s.t. $(x_8, 0, \ldots, 0)$ and $(0, x_7, 0, \ldots, 0)$, respectively. The figures in brackets are the numbers of coefficients in the numerator or denominator polynomials. From Table 3, we can see that these rational expressions are dense, or all coefficients are nonzero. Note that the degrees with respect to x_8 and x_7 in Table 2 are not always equivalent to those in Table 3, though you may conjecture that they are equivalent.

Chosen plaintexts useful for attacking SNAKE(2). For SNAKE(2), if we choose plaintexts s.t. $(x_8, x_8, 0, \ldots, 0)$, the degree of the rational expression in x_8 falls as Table 4 shows. This is because the input to the leftmost S-box in the 2-nd round function becomes constant. Our experimental results show that the plaintexts

Table 2. Degrees of rational exp. over GF(2^8) of SNAKE(1) and SNAKE(2) (global deduction)

$z_4^{(1)}, z_3^{(1)}$	1,0,0,0,0,1,1,1 / 0,0,0,0,0,1,1,1 ,	0,1,0,0,0,0,1,1 / 0,0,0,0,0,0,1,1 ,
$z_2^{(1)}, z_1^{(1)}$	0,0,1,0,0,0,0,1 / 0,0,0,0,0,0,0,1 ,	0,0,0,1,1,1,1,1 / 0,0,0,0,1,1,1,1
$z_4^{(2)}, z_3^{(2)}$	0,1,1,1,2,1,2,3 / 0,1,1,1,1,1,2,3 ,	0,0,1,1,1,2,1,2 / 0,0,1,1,1,1,1,2 ,
$z_2^{(2)}, z_1^{(2)}$	0,0,0,1,1,1,2,1 / 0,0,0,1,1,1,1,1 ,	1,1,1,1,1,2,3,5 / 1,1,1,1,1,2,3,4
$z_4^{(3)}, z_3^{(3)}$	2,1,2,3,3,6,7,9 / 1,1,2,3,3,6,7,9 ,	1,2,1,2,2,3,6,7 / 1,1,1,2,2,3,6,7 ,
$z_2^{(3)}, z_1^{(3)}$	1,1,2,1,1,2,3,6 / 1,1,1,1,1,2,3,6 ,	1,2,3,5,6,7,9,12 / 1,2,3,4,6,7,9,12
$z_4^{(4)}, z_3^{(4)}$	3,6,7,9,11,13,20,28 / 3,6,7,9,10,13,20,28 ,	2,3,6,7,8,11,13,20 / 2,3,6,7,8,10,13,20 ,
$z_2^{(4)}, z_1^{(4)}$	1,2,3,6,7,8,11,13 / 1,2,3,6,7,8,10,13 ,	6,7,9,12,13,20,28,39 / 6,7,9,12,13,20,28,38
$z_4^{(5)}, z_3^{(5)}$	11,13,20,28,31,45,59,81 / 10,13,20,28,31,45,59,81 ,	8,11,13,20,22,31,45,59 / 9,10,13,20,22,31,45,59 ,
$z_2^{(5)}, z_1^{(5)}$	7,8,11,13,14,22,31,45 / 7,8,10,13,14,22,31,45 ,	13,20,28,39,45,59,81,112 / 13,20,28,38,45,59,81,112
$z_4^{(6)}, z_3^{(6)}$	31,45,59,81,92,125,177,244 / 31,45,59,81,91,125,177,244 ,	22,31,45,59,67,91,125,177 / 22,31,45,59,67,91,125,177 ,
$z_2^{(6)}, z_1^{(6)}$	14,22,31,45,52,67,92,125 / 14,22,31,45,52,67,91,125 ,	45,59,81,112,125,177,244,255 / 45,59,81,112,125,177,244,255
$z_4^{(7)}, z_3^{(7)}$	92,125,177,244,255,255,255,255 / 91,125,177,244,255,255,255,255 ,	67,92,125,177,199,255,255,255 / 67,91,125,177,199,255,255,255 ,
$z_2^{(7)}, z_1^{(7)}$	52,67,92,125,139,199,255,255 / 52,67,91,125,139,199,255,255 ,	125,177,244,255,255,255,255,255 / 125,177,244,255,255,255,255,255

Note) Let $\deg_{x_i} f$ be the degree of f with respect to x_i, and the degrees in Table 2 are shown as follows.

$$\frac{\deg_{x_8} f_{j1}^{(r)}, \deg_{x_7} f_{j1}^{(r)}, \deg_{x_6} f_{j1}^{(r)}, \deg_{x_5} f_{j1}^{(r)}, \deg_{x_4} f_{j1}^{(r)}, \deg_{x_3} f_{j1}^{(r)}, \deg_{x_2} f_{j1}^{(r)}, \deg_{x_1} f_{j1}^{(r)}}{\deg_{x_8} f_{j2}^{(r)}, \deg_{x_7} f_{j2}^{(r)}, \deg_{x_6} f_{j2}^{(r)}, \deg_{x_5} f_{j2}^{(r)}, \deg_{x_4} f_{j2}^{(r)}, \deg_{x_3} f_{j2}^{(r)}, \deg_{x_2} f_{j2}^{(r)}, \deg_{x_1} f_{j2}^{(r)}}$$

s.t. $(x_8, x_8, 0, \ldots, 0)$ bring about the rational expression in one variable of the fewest coefficients for SNAKE(2). The plaintexts s.t. $(0, x_7, x_7, 0, \ldots, 0)$ bring about the second fewest one.

4.2 Key Recovery

In this subsection, we demonstrate how to recover the last round key by taking a simple example of a chosen plaintext attack of SNAKE(2) with 9 rounds, i.e. SNAKE(2)$(8, 4, 64, 9)$, (see also Figure 3 in Appendix). If we choose plaintexts s.t. $x = (x_8, x_8, 0, \ldots, 0)$, the second subblock from the right of the output of the 7-th round, $z_2^{(7)} \in \mathrm{GF}(2^8)$, is represented as the rational expression $z_2^{(7)} = \frac{f_1(x_8)}{f_2(x_8)}$, where both $f_1(x_8)$ and $f_2(x_8)$ have 16 coefficients (see Table 4). Therefore, if $16 + 15 = 31$ pairs of plaintexts s.t. $x = (x_8, x_8, 0, \ldots, 0)$ and corresponding ciphertexts are given, we can construct the rational expression. The attack equation is as follows.

$$\frac{f_1(x_8)}{f_2(x_8)} = y_6 + S(y_1 + k_1^{(9)}) \tag{4}$$

Table 3. Degrees of rational exp. over GF(2^8) of SNAKE(1).

when $x = (x_8, 0, \ldots, 0)$

$z_4^{(1)}, z_3^{(1)}, z_2^{(1)}, z_1^{(1)}$	$\frac{1}{0}\frac{(2)}{(1)}$,	$\frac{0}{0}\frac{(1)}{(1)}$,	$\frac{0}{0}\frac{(1)}{(1)}$,	$\frac{0}{0}\frac{(1)}{(1)}$
$z_4^{(2)}, z_3^{(2)}, z_2^{(2)}, z_1^{(2)}$	$\frac{0}{0}\frac{(1)}{(1)}$,	$\frac{0}{0}\frac{(1)}{(1)}$,	$\frac{0}{0}\frac{(1)}{(1)}$,	$\frac{0}{1}\frac{(1)}{(2)}$
$z_4^{(3)}, z_3^{(3)}, z_2^{(3)}, z_1^{(3)}$	$\frac{2}{1}\frac{(3)}{(2)}$,	$\frac{1}{1}\frac{(2)}{(2)}$,	$\frac{1}{1}\frac{(2)}{(2)}$,	$\frac{1}{1}\frac{(2)}{(2)}$
$z_4^{(4)}, z_3^{(4)}, z_2^{(4)}, z_1^{(4)}$	$\frac{3}{3}\frac{(4)}{(4)}$,	$\frac{2}{2}\frac{(3)}{(3)}$,	$\frac{1}{1}\frac{(2)}{(2)}$,	$\frac{5}{6}\frac{(6)}{(7)}$
$z_4^{(5)}, z_3^{(5)}, z_2^{(5)}, z_1^{(5)}$	$\frac{11}{10}\frac{(12)}{(11)}$,	$\frac{8}{8}\frac{(9)}{(9)}$,	$\frac{7}{7}\frac{(8)}{(8)}$,	$\frac{13}{13}\frac{(14)}{(14)}$
$z_4^{(6)}, z_3^{(6)}, z_2^{(6)}, z_1^{(6)}$	$\frac{31}{31}\frac{(32)}{(32)}$,	$\frac{22}{22}\frac{(23)}{(23)}$,	$\frac{14}{14}\frac{(15)}{(15)}$,	$\frac{44}{45}\frac{(45)}{(46)}$
$z_4^{(7)}, z_3^{(7)}, z_2^{(7)}, z_1^{(7)}$	$\frac{92}{91}\frac{(93)}{(92)}$,	$\frac{67}{67}\frac{(68)}{(68)}$,	$\frac{52}{52}\frac{(53)}{(53)}$,	$\frac{125}{125}\frac{(126)}{(126)}$

Note) degrees with respect to x_8

when $x = (0, x_7, 0, \ldots, 0)$

$z_4^{(1)}, z_3^{(1)}, z_2^{(1)}, z_1^{(1)}$	$\frac{0}{0}\frac{(1)}{(1)}$,	$\frac{1}{0}\frac{(2)}{(1)}$,	$\frac{0}{0}\frac{(1)}{(1)}$,	$\frac{0}{0}\frac{(1)}{(1)}$
$z_4^{(2)}, z_3^{(2)}, z_2^{(2)}, z_1^{(2)}$	$\frac{0}{1}\frac{(1)}{(2)}$,	$\frac{0}{0}\frac{(1)}{(1)}$,	$\frac{0}{0}\frac{(1)}{(1)}$,	$\frac{0}{1}\frac{(1)}{(2)}$
$z_4^{(3)}, z_3^{(3)}, z_2^{(3)}, z_1^{(3)}$	$\frac{1}{1}\frac{(2)}{(2)}$,	$\frac{2}{1}\frac{(3)}{(2)}$,	$\frac{1}{1}\frac{(2)}{(2)}$,	$\frac{2}{2}\frac{(3)}{(3)}$
$z_4^{(4)}, z_3^{(4)}, z_2^{(4)}, z_1^{(4)}$	$\frac{5}{6}\frac{(6)}{(7)}$,	$\frac{3}{3}\frac{(4)}{(4)}$,	$\frac{2}{2}\frac{(3)}{(3)}$,	$\frac{6}{7}\frac{(7)}{(8)}$
$z_4^{(5)}, z_3^{(5)}, z_2^{(5)}, z_1^{(5)}$	$\frac{13}{13}\frac{(14)}{(14)}$,	$\frac{11}{10}\frac{(12)}{(11)}$,	$\frac{8}{8}\frac{(9)}{(9)}$,	$\frac{20}{20}\frac{(21)}{(21)}$
$z_4^{(6)}, z_3^{(6)}, z_2^{(6)}, z_1^{(6)}$	$\frac{44}{45}\frac{(45)}{(46)}$,	$\frac{31}{31}\frac{(32)}{(32)}$,	$\frac{22}{22}\frac{(23)}{(23)}$,	$\frac{58}{59}\frac{(59)}{(60)}$
$z_4^{(7)}, z_3^{(7)}, z_2^{(7)}, z_1^{(7)}$	$\frac{125}{125}\frac{(126)}{(126)}$,	$\frac{92}{91}\frac{(93)}{(92)}$,	$\frac{67}{67}\frac{(68)}{(68)}$,	$\frac{177}{177}\frac{(178)}{(178)}$

Note) degrees with respect to x_7

The last round key $k_1^{(9)}$ is recovered as follows. For 31 plaintext/ciphertext pairs, we compute the right side of Eq. (4) guessing $k_1^{(9)}$. Thus all the coefficients in $\frac{f_1(x_8)}{f_2(x_8)}$ are determined. If the constructed Eq. (4) holds for the 32-nd pair of plaintext and ciphertext, we can judge that the guessed $k_1^{(9)}$ is correct with high probability. Since $k_1^{(9)}$ is 8 bits, the average of the required complexity of this attack is about $32 \times 2^8 \times \frac{1}{2} \sim 2^{12}$ times the computation of an S-box. Note that the required complexity for constructing the rational expression is negligible.

We apply similar key-recovery attacks to SNAKE with several rounds. We show some best attacks in Table 5, for which I mean that there is trade-off relations between the required number of p/c pairs and the complexity. The complexity is measured by the times of computation of the round function. In the column of strategy we show the attack strategies using simple symbols.

For example, the strategy "$7i + 1k$" means that the key-recovery attack uses the *instance deduction of* 7*-round* and recovers the last round key (m bits) as Figure 3 shows. The strategy "$7i + 2k$" means that the key-recovery attack uses the *instance deduction of* 7*-round* and recovers the last round key ($4m$ bits) and a subblock of the key of the second round from the bottom (m bits). The strategy "$11i + 2g + 1k$" means that the key-recovery attack uses the meet-in-the-middle

Table 4. Degrees of rational expression over GF(2^8) of SNAKE(2)

when $x = (x_8, x_8, 0, \ldots, 0)$

$z_4^{(1)}, z_3^{(1)}, z_2^{(1)}, z_1^{(1)}$	$\frac{1}{0}\frac{(2)}{(1)}$,	$\frac{1}{0}\frac{(2)}{(1)}$,	$\frac{0}{0}\frac{(1)}{(1)}$,	$\frac{0}{0}\frac{(1)}{(1)}$
$z_4^{(2)}, z_3^{(2)}, z_2^{(2)}, z_1^{(2)}$	$\frac{0}{1}\frac{(1)}{(2)}$,	$\frac{0}{0}\frac{(1)}{(1)}$,	$\frac{0}{0}\frac{(1)}{(1)}$,	$\frac{0}{0}\frac{(1)}{(1)}$
$z_4^{(3)}, z_3^{(3)}, z_2^{(3)}, z_1^{(3)}$	$\frac{1}{0}\frac{(2)}{(1)}$,	$\frac{1}{0}\frac{(2)}{(1)}$,	$\frac{0}{0}\frac{(1)}{(1)}$,	$\frac{1}{1}\frac{(2)}{(2)}$
$z_4^{(4)}, z_3^{(4)}, z_2^{(4)}, z_1^{(4)}$	$\frac{2}{3}\frac{(2)}{(4)}$,	$\frac{1}{1}\frac{(2)}{(2)}$,	$\frac{1}{1}\frac{(2)}{(2)}$,	$\frac{1}{1}\frac{(2)}{(2)}$
$z_4^{(5)}, z_3^{(5)}, z_2^{(5)}, z_1^{(5)}$	$\frac{4}{3}\frac{(5)}{(4)}$,	$\frac{3}{2}\frac{(4)}{(3)}$,	$\frac{1}{1}\frac{(2)}{(2)}$,	$\frac{7}{7}\frac{(8)}{(8)}$
$z_4^{(6)}, z_3^{(6)}, z_2^{(6)}, z_1^{(6)}$	$\frac{13}{14}\frac{(14)}{(15)}$,	$\frac{9}{9}\frac{(10)}{(10)}$,	$\frac{8}{8}\frac{(9)}{(9)}$,	$\frac{14}{14}\frac{(15)}{(15)}$
$z_4^{(7)}, z_3^{(7)}, z_2^{(7)}, z_1^{(7)}$	$\frac{35}{34}\frac{(36)}{(35)}$,	$\frac{25}{24}\frac{(26)}{(25)}$,	$\frac{15}{15}\frac{(16)}{(16)}$,	$\frac{52}{52}\frac{(53)}{(53)}$
$z_4^{(8)}, z_3^{(8)}, z_2^{(8)}, z_1^{(8)}$	$\frac{105}{106}\frac{(106)}{(107)}$,	$\frac{76}{76}\frac{(77)}{(77)}$,	$\frac{60}{60}\frac{(61)}{(61)}$,	$\frac{139}{139}\frac{(140)}{(140)}$

Note) degrees with respect to x_8

Table 5. Interpolation attacks of SNAKE(i)$(8, 4, 64, r)$

SNAKE(1)				
#rounds(r)	#pairs	complexity	chosen plaintexts	strategy
9	59	2^{37}	$(x_8, 0, \ldots, 0)$	$6i + 1g + 1k$
	106	2^{14}	$(x_8, 0, \ldots, 0)$	$7i + 1k$
10	106	2^{46}	$(x_8, 0, \ldots, 0)$	$7i + 2k$
	211	2^{39}	$(x_8, 0, \ldots, 0)$	$7i + 1g + 1k$
11	211	2^{47}	$(x_8, 0, \ldots, 0)$	$7i + 1g + 2k$
SNAKE(2)				
#rounds(r)	#pairs	complexity	chosen plaintexts	strategy
9	32	2^{12}	$(x_8, x_8, 0, \ldots, 0)$	$7i + 1k$
10	32	2^{43}	$(x_8, x_8, 0, \ldots, 0)$	$7i + 2k$
	63	2^{38}	$(x_8, x_8, 0, \ldots, 0)$	$7i + 1g + 1k$
	122	2^{14}	$(x_8, x_8, 0, \ldots, 0)$	$8i + 1k$
11	122	2^{46}	$(x_8, x_8, 0, \ldots, 0)$	$8i + 2k$

approach where the *instance deduction of* 11*-round* and the *global deduction of* 2*-round* are used, and recovers the last round key ($4m$ bits) as Figure 4 shows.

5 Interpolation Attack of SNAKE(i)$(16, 4, 128, r)$

We apply the interpolation attack to a 128-bit variant, SNAKE(i)$(16, 4, 128, r)$. When the block size is 128 bits and the size of input and output of the S-box is 16 bits, the maximum number of available p/c pairs for the attacker increases compared with the case when the block size is 64 bits. Thus, some attacks become possible that would be impractical when the block size was 64 bits.

For example, we demonstrate the interpolation attack of SNAKE(2) with 15 rounds, i.e. SNAKE(2)$(16, 4, 128, 15)$ (see also Figure 4 in Appendix). If we choose plaintexts s.t. $x = (x_8, x_8, 0, \ldots, 0)$, the second subblock from the

Table 6. Degrees of rational exp. over GF(2^{16}) of SNAKE(1)

when $x = (x_8, 0, \ldots, 0)$

$z_4^{(8)}, z_3^{(8)}, z_2^{(8)}, z_1^{(8)}$	$\frac{275}{275}$,	$\frac{199}{199}$,	$\frac{139}{139}$,	$\frac{380}{381}$
$z_4^{(9)}, z_3^{(9)}, z_2^{(9)}, z_1^{(9)}$	$\frac{811}{810}$,	$\frac{587}{587}$,	$\frac{433}{433}$,	$\frac{1119}{1119}$
$z_4^{(10)}, z_3^{(10)}, z_2^{(10)}, z_1^{(10)}$	$\frac{2414}{2414}$,	$\frac{1751}{1751}$,	$\frac{1258}{1258}$,	$\frac{3330}{3331}$
$z_4^{(11)}, z_3^{(11)}, z_2^{(11)}, z_1^{(11)}$	$\frac{7151}{7150}$,	$\frac{5176}{5176}$,	$\frac{3764}{3764}$,	$\frac{9873}{9873}$
$z_4^{(12)}, z_3^{(12)}, z_2^{(12)}, z_1^{(12)}$	$\frac{21227}{21227}$,	$\frac{15388}{15388}$,	$\frac{11131}{11131}$,	$\frac{29294}{29294}$
$z_4^{(13)}, z_3^{(13)}, z_2^{(13)}, z_1^{(13)}$	$-$,	$-$,	$\frac{33059}{33059}$,	$-$

Note) degrees with respect to x_8

Table 7. Degrees of rational exp. over GF(2^{16}) of SNAKE(2)

when $x = (x_8, x_8, 0, \ldots, 0)$

$z_4^{(9)}, z_3^{(9)}, z_2^{(9)}, z_1^{(9)}$	$\frac{310}{309}$,	$\frac{224}{223}$,	$\frac{154}{154}$,	$\frac{433}{433}$
$z_4^{(10)}, z_3^{(10)}, z_2^{(10)}, z_1^{(10)}$	$\frac{916}{917}$,	$\frac{663}{663}$,	$\frac{493}{493}$,	$\frac{1258}{1258}$
$z_4^{(11)}, z_3^{(11)}, z_2^{(11)}, z_1^{(11)}$	$\frac{2724}{2723}$,	$\frac{1975}{1974}$,	$\frac{1412}{1412}$,	$\frac{3764}{3764}$
$z_4^{(12)}, z_3^{(12)}, z_2^{(12)}, z_1^{(12)}$	$\frac{8067}{8068}$,	$\frac{5839}{5839}$,	$\frac{4257}{4257}$,	$\frac{11131}{11131}$
$z_4^{(13)}, z_3^{(13)}, z_2^{(13)}, z_1^{(13)}$	$\frac{23951}{23950}$,	$\frac{17363}{17362}$,	$\frac{12543}{12543}$,	$\frac{33059}{33059}$

Note) degrees with respect to x_8

right of the output of the 11-th round, $z_2^{(11)} \in \mathrm{GF}(2^{16})$, is represented as the rational expression $z_2^{(11)} = \frac{f_1(x_8)}{f_2(x_8)}$. According to Table 7, $\deg_{x_8} f_1 = 1412$ and $\deg_{x_8} f_2 = 1412$. On the other hand, $z_2^{(11)}$ is also represented using $\tilde{y}$, which can be computed from y and a guessed $k^{(15)}$: $z_2^{(11)} = \frac{g_1(\tilde{y})}{g_2(\tilde{y})}$. Using the meet-in-the-middle approach, we have the attack equation as follows.

$$\frac{f_1(x_8)}{f_2(x_8)} = \frac{g_1(\tilde{y}(y, k^{(15)}))}{g_2(\tilde{y}(y, k^{(15)}))} \tag{5}$$

From Table 1, the numbers of coefficients in g_1 and g_2 are 14 and 10, respectively. The numbers of coefficients in f_1 and f_2 are estimated to be at most 1413. Therefore, the required number of p/c pairs for constructing Eq. (5) is at most $(14-1) \times (1413-1) + 10 \times 1413 \sim 2^{15}$ for a guessed $k^{(15)}$. Since $k^{(15)}$ is 64 bits, the average of the required complexity of this attack is at most $2^{15} \times 2^{64} \times \frac{1}{2} \sim$ about 2^{78} times of computation of the round function.

If we didn't know the actual numbers of coefficients in g_1 and g_2, we would estimate them to be 48 and 32, respectively, from Eq. (1) and the degrees of $z_2^{(2)}$ in Table 1. Then, the attack would be considered as impossible because the required number of pairs exceeds 2^{16}.

We applied similar key-recovery attacks to SNAKE with the blocksize of 128 bits with several rounds. Similarly to Section 4, we show some best attacks in Table 9. As a practical attack of SNAKE(2)$(16, 4, 128, 16)$, we give the attack

Table 8. Degrees of rational expression over GF(2^{16}) of SNAKE(2)

when $x = (x_8, x_8 + x_7, x_7, \ldots, 0)$

$z_4^{(1)}, z_3^{(1)}, z_2^{(1)}, z_1^{(1)}$	$\frac{1,0}{0,0}$,	$\frac{1,1}{0,0}$,	$\frac{0,1}{0,0}$,	$\frac{0,0}{0,0}$
$z_4^{(2)}, z_3^{(2)}, z_2^{(2)}, z_1^{(2)}$	$\frac{0,0}{1,0}$,	$\frac{0,0}{0,1}$,	$\frac{0,0}{0,0}$,	$\frac{0,0}{0,0}$
$z_4^{(3)}, z_3^{(3)}, z_2^{(3)}, z_1^{(3)}$	$\frac{1,1}{0,1}$,	$\frac{1,1}{0,0}$,	$\frac{0,1}{0,0}$,	$\frac{1,1}{1,1}$
$z_4^{(4)}, z_3^{(4)}, z_2^{(4)}, z_1^{(4)}$	$\frac{2,1}{3,1}$,	$\frac{1,2}{1,3}$,	$\frac{1,1}{1,1}$,	$\frac{1,2}{1,2}$
$z_4^{(5)}, z_3^{(5)}, z_2^{(5)}, z_1^{(5)}$	$\frac{4,7}{3,7}$,	$\frac{3,4}{2,3}$,	$\frac{1,3}{1,2}$,	$\frac{7,8}{7,8}$
$z_4^{(6)}, z_3^{(6)}, z_2^{(6)}, z_1^{(6)}$	$\frac{13,14}{14,14}$,	$\frac{9,13}{9,14}$,	$\frac{8,9}{8,9}$,	$\frac{14,22}{14,22}$
$z_4^{(7)}, z_3^{(7)}, z_2^{(7)}, z_1^{(7)}$	$\frac{35,52}{34,52}$,	$\frac{25,35}{24,34}$,	$\frac{15,25}{15,24}$,	$\frac{52,67}{52,67}$
$z_4^{(8)}, z_3^{(8)}, z_2^{(8)}, z_1^{(8)}$	$\frac{105,139}{106,139}$,	$\frac{76,105}{76,106}$,	$\frac{60,76}{60,76}$,	$\frac{139,199}{139,199}$
$z_4^{(9)}, z_3^{(9)}, z_2^{(9)}, z_1^{(9)}$	$\frac{310,433}{309,433}$,	$\frac{224,310}{223,309}$,	$\frac{154,224}{154,223}$,	$\frac{433,587}{433,587}$
$z_4^{(10)}, z_3^{(10)}, z_2^{(10)}, z_1^{(10)}$	$\frac{916,1258}{917,1258}$,	$\frac{663,916}{663,917}$,	$\frac{493,663}{493,663}$,	$\frac{1258,1751}{1258,1751}$
$z_4^{(11)}, z_3^{(11)}, z_2^{(11)}, z_1^{(11)}$	$\frac{2724,3764}{2723,3764}$,	$\frac{1975,2724}{1974,2723}$,	$\frac{1412,1975}{1412,1974}$,	$\frac{3764,5176}{3764,5176}$
$z_4^{(12)}, z_3^{(12)}, z_2^{(12)}, z_1^{(12)}$	$\frac{8067,11131}{8068,11131}$,	$\frac{5839,8067}{5839,8068}$,	$\frac{4257,5839}{4257,5839}$,	$\frac{11131,15388}{11131,15388}$
$z_4^{(13)}, z_3^{(13)}, z_2^{(13)}, z_1^{(13)}$	$\frac{23951,33059}{23950,33059}$,	$\frac{17363,23951}{17362,23950}$,	$\frac{12543,17363}{12543,17362}$,	$\frac{33059,45602}{33059,45602}$
$z_4^{(14)}, z_3^{(14)}, z_2^{(14)}, z_1^{(14)}$	$-$,	$-$,	$\frac{37316,51441}{37316,51441}$,	$-$

Note) degrees with respect to x_8 and x_7

which requires $< 2^{32}$ p/c pairs and complexity of 2^{47} times the computation of the round function. It uses the chosen plaintexts s.t. $x = (x_8, x_8+x_7, x_7, 0, \ldots, 0)$. This brings about the rational expression in two variable of the fewest coefficients for SNAKE(2).

6 Discussion and Concluding Remarks

Division by 0. Here we discuss a problem in the interpolation attack using rational expressions, which wasn't pointed out in [3]. The problem is that we can't always construct correct rational expressions if at least one of the inputs of S-boxes are 0 in the encryption process. We can detect this by comparing the degree of the constructed rational expression with that in Table 2 etc. The degree often gets higher. If this happens, we may construct the rational expression again using different pairs of plaintexts and ciphertexts. In this case the required number of p/c pairs can be estimated by the cryptanalysis with probabilistic non-linear relations shown by Jakobsen [2]. This is based on Sudan's algorithm for decoding Reed-Solomon codes beyond the error-correction diameter. If we apply Jakobsen's result to this problem, when the rational expression holds with probability μ, the attack is possible with $\mathcal{N} = \frac{N}{\mu^2}$ p/c pairs in time polynomial in $\mathcal{N}$, where N is the number of coefficients in the rational expression. The probability μ is equal to the probability with which none of the inputs of S-boxes are zero in the encryption process. Therefore, $\mu = \left(\frac{2^m-1}{2^m}\right)^{4r}$ for SNAKE(i)$(m, 4, 8m, r)$, if we assume every input of the S-box is random and independent. For example,

Table 9. Interpolation attacks of SNAKE$(i)(16, 4, 128, r)$

SNAKE(1)				
#rounds(r)	#pairs	complexity	chosen plaintexts	strategy
13	2^{13}	2^{28}	$(x_8, 0, \ldots, 0)$	$11i + 1k$
14	2^{15}	2^{30}	$(x_8, 0, \ldots, 0)$	$12i + 1k$
15	2^{15}	2^{94}	$(x_8, 0, \ldots, 0)$	$12i + 2k$
	2^{16}	2^{79}	$(x_8, 0, \ldots, 0)$	$12i + 1g + 1k$
SNAKE(2)				
#rounds(r)	#pairs	complexity	chosen plaintexts	strategy
13	2^{11}	2^{74}	$(x_8, x_8, 0, \ldots, 0)$	$10i + 1g + 1k$
	2^{12}	2^{27}	$(x_8, x_8, 0, \ldots, 0)$	$11i + 1k$
14	2^{14}	2^{29}	$(x_8, x_8, 0, \ldots, 0)$	$12i + 1k$
15	2^{14}	2^{93}	$(x_8, x_8, 0, \ldots, 0)$	$12i + 2k$
	2^{15}	2^{30}	$(x_8, x_8, 0, \ldots, 0)$	$13i + 1k$
16	2^{15}	2^{94}	$(x_8, x_8, 0, \ldots, 0)$	$13i + 2k$
	2^{32}	2^{47}	$(x_8, x_8 + x_7, x_7, 0, \ldots, 0)$	$14i + 1k$

the attack for SNAKE$(i)(8, 4, 64, 11)$ is possible with $\mathcal{N} = \frac{N}{\mu^2} \sim 1.411N$ p/c pairs in time polynomial in $\mathcal{N}$, and the attack for SNAKE$(2)(16, 4, 128, 16)$ is possible with $\mathcal{N}' = \frac{N'}{\mu^2} \sim 1.002N'$ p/c pairs in time polynomial in $\mathcal{N}'$.

Diffusion layer. It is the plain diffusion layer that makes the interpolation attack on the cipher SNAKE(2) easier. The diffusion layer of the cipher SNAKE(2) keeps the outputs of some subblocks *constant* for some chosen plaintexts. We have to consider this in designing the diffusion layer.

Concluding remarks. We presented an efficient interpolation attack using a computer algebra system. We succeeded in attacking the block cipher SNAKE efficiently – with smaller complexity and fewer p/c pairs – 1) by finding the actual number of coefficients in the rational expression used in the attack and 2) by finding the rational expression with the fewest coefficients by choosing the plaintexts. We found some attacks feasible which we would consider as impossible by the interpolation attack described in [3]. When we evaluate the resistance of a block cipher to the interpolation attack, it is necessary to apply the interpolation attack described in this paper.

We showed that when the block size is 64 bits and $m = 8$, all round keys are recovered for SNAKE(1) and SNAKE(2) with up to 11 rounds. Moreover, when the block size is 128 bits and $m = 16$, all round keys are recovered for SNAKE(1) with up to 15 rounds and SNAKE(2) with up to 16 rounds.

References

1. E.Biham and A.Shamir, "Differential Cryptanalysis of DES-like Cryptosystems," Journal of Cryptology, Volume 4, Number 1, pp.3–72, Springer-Verlag, 1991.

2. T.Jakobsen, "Cryptanalysis of Block Ciphers with Probabilistic Non-Linear Relations of Low Degree," Advances in Cryptology – CRYPTO'98, Lecture Notes in Computer Science 1462, pp.212–222, Springer-Verlag, 1998.
3. T.Jakobsen and L.R.Knudsen, "The Interpolation Attack on Block Ciphers," Fast Software Encryption, FSE'97, Lecture Notes in Computer Science 1267, pp.28–40, Springer-Verlag, 1997.
4. L.R.Knudsen, "Block Ciphers – Analysis, Design and applications," phD thesis, Aarhus University, Denmark, 1994.
5. C.Lee and Y.Cha, "The Block Cipher : SNAKE with Provable Resistance against DC and LC attacks," In Proceedings of 1997 Korea-Japan Joint Workshop on Information Security and Cryptology (JW-ISC'97), pp.3–17, 1997.
6. M.Matsui, "Linear Cryptanalysis Method for DES Cipher," Advances in Cryptology – EUROCRYPT'93, Lecture Notes in Computer Science 765, pp.386–397, Springer-Verlag, 1994.
7. M.Noro and T.Takeshima, "Risa/Asir – a computer algebra system," Proceedings of ISSAC'92, pp.387–396, ACM Press, 1992.
8. K.Nyberg and L.R.Knudsen, "Provable Security Against a Differential Attack," Journal of Cryptology, Volume 8, Number 1, pp.27–37, Springer-Verlag, 1995.
9. V.Rijmen, J.Daemen, B.Preneel, A.Bosselaers, and E.De Win, "The cipher SHARK," Fast Software Encryption, FSE'96, Lecture Notes in Computer Science 1039, pp.99–112, Springer-Verlag, 1996.

Appendix

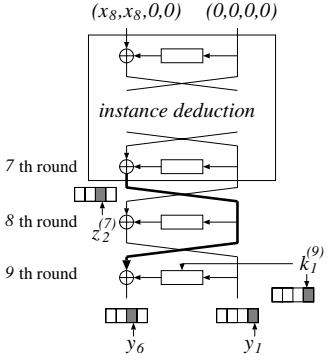

Fig. 3. A chosen plaintext attack of SNAKE(2)(8,4,64,9)

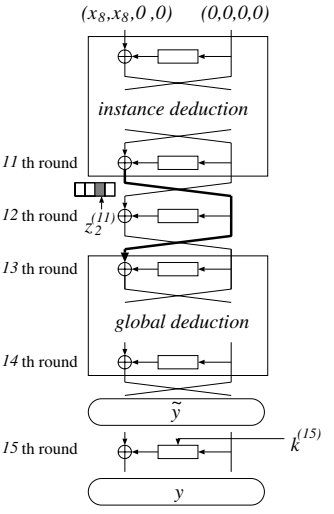

Fig. 4. A chosen plaintext attack of SNAKE(2)(16,4,128,15)