Floating Fault Analysis of Trivium under Weaker Assumptions[1]

Hu Yupu[1], Gao Juntao[1] and Liu Qing
[1] CNIS Laboratory, Xidian University, 710071 Xi'an, China
yphu@mail.xidian.edu.cn
jtgao@mail.xidian.edu.cn
baxiziliaoshi@126.com

Abstract. Trivium is a hardware-oriented stream cipher, and one of the finally chosen ciphers by eSTREAM project. Michal Hojsik and Bohuslav Rudolf presented an effective attack to Trivium, named floating fault analysis, at INDOCRYPT 2008. Their attack makes use of the fault injection and the fault float. In this paper, we present an improvement of this attack. Our attack is under following weaker and more practical assumptions.

- The fault injection can be made for the state at a random time.
- The positions of the fault bits are from random one of 3 NFSRs, and from a random area within 8 neighboring bits.

We present a checking method, by which either the injecting time and fault positions can be determined, or the state differential at a known time can be determined. Each of these two determinations is enough for floating attack. After the determination, the attacker can averagely obtain 67.167 additional linear equations from 82 original quadratic equations, and obtain 66 additional quadratic equations from 66 original cubic equations. A modification of our model is similarly effective with the model of Michal Hojsik and Bohuslav, for the floating attack.

Keywords: Trivium, stream cipher, differential fault analysis, fault injection, fault floating

1 Introduction

1.1 Background and Results of Our Work

Trivium [1, 2] is a hardware-oriented stream cipher designed in 2005 by De Cannière and Preneel for eSTREAM project, and has successfully been chosen as one of the final ciphers by eSTREAM. It has a simple and elegant structure that is composed of 3 non-linear feedback shift registers (NFSRs) and a linear output function. Although Trivium has attracted a lot of interest [3-8], it remains unbroken by passive attacks. An obvious weakness of Trivium is that its non-linearization procedure is over slow, so that the attacker can obtain a large number of low-degree equations of its initial state, by obtaining a key-stream segment. Such low-degree equations are strong enough against those passive attacks, but are weak against active attacks, for example, known-differential attack.

Several active attacks have been presented for stream ciphers [9-15]. Michal Hojsik and Bohuslav Rudolf presented an attack to Trivium, named differential fault analysis, at FSE 2008

[1] The work was supported in part by Nanural Science Fundation of China under Grant 60833008 and by 973 Project under Grant 2007CB311201

[16]. This attack is a known-differential attack, and makes use of the fault injection to obtain the state differential. After that, they presented a more effective attack to Trivium, named floating fault analysis, at INDOCRYPT 2008 [17]. Besides the fault injection, their attack makes use of fault floating, another powerful tool. This attack is no doubt successful, but under two strong assumptions, as the follow.

Assumption 1.1 The fault injection can be made for the state at a fixed time, especially at the initial time.

Assumption 1.2 After the fault injection, exactly one random bit is changed.

For any stream cipher, the state renewal is extremely fast, so that the attacker can hardly catch the state at a fixed time. On the other hand, the hardware-oriented stream ciphers are usually under protection against corruption. According to common comprehension, the fault injection is made by laser or by magnetic disturbance or by some other brute method. When a bit is corrupted, it is difficult to keep the neighbor bits not to be corrupted.

In this paper, we present an improvement of the floating fault attack. Our attack is under following weaker and more practical assumptions.

Assumption 2.1 The fault injection can be made for the state at a random time.

Assumption 2.2 The positions of the fault bits are from random one of 3 NFSRs, and from a random area within 8 neighboring bits.

We present a checking method, by which either the injecting time and fault positions can be determined, or the state differential at a known time can be determined. Each of these two determinations is enough for floating attack. After the determination, the attacker can averagely obtain 67.167 additional linear equations from 82 original quadratic equations, and obtain 66 additional quadratic equations from 66 original cubic equations. Then we make a modification to our model, that is, we preserve the floating attack model of Michal Hojsik and Bohuslav, allowing repeatedly faut injections, except that Assumption 1.2 is changed as Assumption 2.2. Averagely 4 fault injections and averagely 227×5 key-stream bits will break Trivium. This result is similarly effective with the primitive model of Michal Hojsik and Bohuslav Rudolf [17].

The contents are organized as follows. In subsection 1.2 we review related work recently about Trivium. Section 2 is a brief description of Trivium, emphasizing its differential feature and its differential floating feature. Section 3 is the checking method. In this section we first present, after the fault injection, the differential features in various cases. Then we present a complete checking routine, through which either the injecting time and fault positions can be determined, or the state differential at a known time can be determined. Section 4 is the floating analysis. We show that, till the time called “the floating end”, the attacker can averagely obtain 67.167 additional linear equations from 82 original quadratic equations, and obtain 66 additional quadratic equations from 66 original cubic equations. In section 5 we make a modification to our model, and compare with the primitive model of Michal Hojsik and Bohuslav Rudolf. We show that, for our modified model, averagely 4 fault injections and averagely 227×5 key-stream bits will break Trivium.

1.2 Related Work Recently about Trivium

Many previous results in Trivium cryptanalysis have been mensioned by Michal Hojsik and Bohuslav Rudolf [15, 16], and listed in our refferences. Here we only briefly mension 3 results obtained recently.

Deik Priemuth-schmid and Alex Biryukov [18] presented slid pairs in Trivium. They showed that initialization and key-stream generation of Trivium is slidable, that is, one can find distinct (Key, IV) pairs that produce identical (or closely related) key-streams. There are more than 2^{39} such pairs in Trivium. Enes Pasalic [19] mainly considered the scenario where the key differential and/or IV differential influence the internal state of the cipher. They show that under certain circumstances a chosen IV attack may be transformed in the key chosen attack. Based on the idea of cube attack proposed by Itai Dinur and Adi Shamir [20], S. S. Bedi and N. Rajesh Pillai [21] presented cube attacks on Trivium.

2 Trivium Model and Trivium Features

2.1 Trivium Key-Stream Generation and Original Equations

3 combined NFSRs (Non-linear Feedback Shift Registers) drive the key-stream of Trivium. The first NFSR is 93 bit long, denoted as $(s_1, \cdots, s_{93})$. The second NFSR is 84 bit long, denoted as $(s_{94}, \cdots, s_{177})$. The third NFSR is 111 bit long, denoted as $(s_{178}, \cdots, s_{288})$. Table 1 is an equivalent algorithm for the key-stream generation.

Table 1. The key-stream generation algorithm

```
Input: Trivium inner state $(s_1, \cdots, s_{288})$, number of output bits $N \leqslant 2^{64}$
Output: key-stream $(z_0 z_1 z_2 \cdots z_N)$

1: for $i$=0 to $N$ do
2:     $z_i \leftarrow s_{66}+s_{93}+s_{162}+s_{177}+s_{243}+s_{288}$
3:     $t_1 \leftarrow s_{66}+s_{91}s_{92}+s_{93}+s_{171}$
4:     $t_2 \leftarrow s_{162}+s_{175}s_{176}+s_{177}+s_{264}$
5:     $t_3 \leftarrow s_{243}+s_{286}s_{287}+s_{288}+s_{69}$
6:     $(s_1, \cdots, s_{93}) \leftarrow (t_3, s_1, \cdots, s_{92})$
7:     $(s_{94}, \cdots, s_{177}) \leftarrow (t_1, s_{94}, \cdots, s_{176})$
8:     $(s_{178}, \cdots, s_{288}) \leftarrow (t_2, s_{178}, \cdots, s_{287})$
4: end for
```

In Table 1, the step 2 is output of the key-stream bit, which is a linear function of the state. The step 3~8 is renewal of the inner state. Let $s_{(t,j)}$ denote the state bit at time t and position j, then Table 2 presents a clearer description for the state renewal.

Table 2. The inner state renewal

$(s_{(t+1,\ 1)}, s_{(t+1,\ 2)}, \cdots, s_{(t+1,\ 93)})$ $=(s_{(t,\ 243)}+s_{(t,\ 286)}s_{(t,\ 287)}+s_{(t,\ 288)}+s_{(t,\ 69)}, s_{(t,\ 1)}, \cdots, s_{(t,\ 92)})$
$(s_{(t+1,\ 94)}, s_{(t+1,\ 95)}, \cdots, s_{(t+1,\ 177)})$ $=(s_{(t,\ 66)}+s_{(t,\ 91)}s_{(t,\ 92)}+s_{(t,\ 93)}+s_{(t,\ 171)}, s_{(t,\ 94)}, \cdots, s_{(t,\ 176)})$
$(s_{(t+1,\ 178)}, s_{(t+1,\ 179)}, \cdots, s_{(t+1,\ 288)})$ $=(s_{(t,\ 162)}+s_{(t,\ 175)}s_{(t,\ 176)}+s_{(t,\ 177)}+s_{(t,\ 264)}, s_{(t,\ 178)}, \cdots, s_{(t,\ 287)})$

Suppose that the attacker obtains a key-stream segment ($z_t z_{t+1} z_{t+2} \cdots z_{t+N}$) from time t to time $t+N$. Then he obtains $N+1$ equations of ($s_{(t,\ 1)}$, $s_{(t,\ 2)}$,$\cdots$, $s_{(t,\ 288)}$), the state at time t. These equations are called original equations, and are respectively ranked equation (0), equation (1), $\cdots$, equation (N).

66 of these original equations are linear equations, ranked from equation (0) to equation (65). 82 of these original equations are quadratic equations, ranked from equation (66) to equation (147). In each of these quadratic equations, quadratic terms are the products of two neighbor bits $s_{(t\ j)}s_{(t,\ j+1)}$, and two quadratic terms do not have coincident bits. These quadratic terms are called pair quadratic terms. Because of such special features, equation (66) ~ equation (147) are also called pair quadratic equations (see [15]). 66 of these original equations are cubic equations, ranked from equation (148) to equation (213).

The equation (0) ~ equation (147) are presented in Appendix A.

2.2 Trivium Differential Features and Additional Equations

Suppose that the attacker obtains not only the key-stream segment ($z_t z_{t+1} z_{t+2} \cdots z_{t+N}$) from time t to time $t+N$, but also the following two objects.

(1) Another key-stream segment ($z_t' z_{t+1}' z_{t+2}' \cdots z_{t+N}'$) from time t to time $t+N$, therefore the differential of the two segments

$$(\triangle z_t,\ \triangle z_{t+1},\ \cdots,\ \triangle z_{t+N})=(z_t+z_t',\ z_{t+1}+z_{t+1}',\cdots,\ z_{t+N}+z_{t+N}').$$

(2) The differential value of two inner states at time t,

$$(\triangle s_{(t,\ 1)},\ \triangle s_{(t,\ 2)},\ \cdots,\ \triangle s_{(t,\ 288)})=(s_{(t,\ 1)}+s_{(t,\ 1)}',\ s_{(t,\ 2)}+s_{(t,\ 2)}',\cdots,\ s_{(t,\ 288)}+s_{(t,\ 288)}').$$

Then he obtains another $N+1$ equations of ($s_{(t,\ 1)}$, $s_{(t,\ 2)}$,$\cdots$, $s_{(t,\ 288)}$). These equations are called additional equations. From 66 original linear equations, he obtains 66 additional equations which are identities. From 82 original quadratic equations, he obtains 82 additional equations which are identities or linear equations. From 66 original cubic equations, he obtains 66 additional equations which are identities or linear equations or quadratic equations. And so on. Linear equations are most valuabale for breaking Trivium. Quadratic equations are much less valuabale.

2.3 Differential Floating Feature

It is clear that, by Appendix A,

$$(\triangle s_{(t+1,\ 1)},\ \triangle s_{(t+1,\ 2)},\ \cdots,\ \triangle s_{(t+1,\ 93)})$$

$=(\triangle s_{(t,243)}+\triangle(s_{(t,286)}s_{(t,287)})+\triangle s_{(t,288)}+\triangle s_{(t,69)},\ \triangle s_{(t,1)},\ \cdots,\ \triangle s_{(t,92)})$

$=(\triangle s_{(t,243)}+s_{(t,286)}\triangle s_{(t,287)}+s_{(t,287)}\triangle s_{(t,286)}+\triangle s_{(t,286)}\triangle s_{(t,287)}+\triangle s_{(t,288)}+\triangle s_{(t,69)},$
$\triangle s_{(t,1)},\ \cdots,\ \triangle s_{(t,92)}),$

$(\triangle s_{(t+1,94)},\ \triangle s_{(t+1,95)},\ \cdots,\ \triangle s_{(t+1,177)})$

$=(\triangle s_{(t,66)}+\triangle(s_{(t,91)}s_{(t,92)})+\triangle s_{(t,93)}+\triangle s_{(t,171)},\ \triangle s_{(t,94)},\ \cdots,\ \triangle s_{(t,176)})$

$=(\triangle s_{(t,66)}+s_{(t,91)}\triangle s_{(t,92)}+s_{(t,92)}\triangle s_{(t,91)}+\triangle s_{(t,91)}\triangle s_{(t,92)}+\triangle s_{(t,93)}+\triangle s_{(t,171)},$
$\triangle s_{(t,94)},\ \cdots,\ \triangle s_{(t,176)}),$

$(\triangle s_{(t+1,178)},\ \triangle s_{(t+1,179)},\ \cdots,\ \triangle s_{(t+1,288)})$

$=(\triangle s_{(t,162)}+\triangle(s_{(t,175)}s_{(t,176)})+\triangle s_{(t,177)}+\triangle s_{(t,264)},\ \triangle s_{(t,178)},\ \cdots,\ \triangle s_{(t,287)})$

$=(\triangle s_{(t,162)}+s_{(t,175)}\triangle s_{(t,176)}+s_{(t,176)}\triangle s_{(t,175)}+\triangle s_{(t,175)}\triangle s_{(t,176)}+\triangle s_{(t,177)}+\triangle s_{(t,264)},$
$\triangle s_{(t,178)},\ \cdots,\ \triangle s_{(t,287)}).$

It implies that, if the state differential at time t is known, the state differential at time t+1 is known under one of several weak conditions. This feature is called differential float, or fault float.

3 Determination of the Injecting Time and Fault Positions

Suppose that the attacker obtains an encryption machine. He starts up this machine, and obtains the key-stream segment ($z_0z_1z_2\cdots z_N$). Then he starts up the machine once again, and simultaneously makes fault injection under Assumption2.1 and Assumption2.2. So that he obtains the fault injected key-stream segment ($z_0'z_1'z_2'\cdots z_N'$), and the differential of the two segments ($\triangle z_0,\ \triangle z_1,\ \cdots,\ \triangle z_N$)=($z_0+z_0'$, z_1+z_1',$\cdots$, z_N+z_N'). He wants to determine the injecting time and fault positions.

3.1 Notations and Lemmas

$s_{(t,j)}$ denotes the state bit at time t and position j.

P_L denotes the lowest position of injected faults. P_H denotes the highest position of injected faults. According to our Assumption2.2, $1\leqslant P_H-P_L\leqslant 7$. Again P_H and P_L are from same set of indices {1, ⋯, 93} or {94, ⋯, 177} or {178, ⋯, 288}.

P_L is of 9 cases: $1\leqslant P_L\leqslant 66$, $67\leqslant P_L\leqslant 69$, $70\leqslant P_L\leqslant 93$, $94\leqslant P_L\leqslant 162$, $163\leqslant P_L\leqslant 171$, $172\leqslant P_L\leqslant 177$, $178\leqslant P_L\leqslant 243$, $244\leqslant P_L\leqslant 264$, $265\leqslant P_L\leqslant 288$.

T denotes the smallest time t such that $\triangle z_t=1$. M denotes the time when the faults are inserted. The attacker has already known T. He does not know M, but he does know that $T-68\leqslant M\leqslant T$.

Lemma 1 Suppose that

(1) $A=\{a_1,\ \cdots,\ a_n\}$ is a set of indices, max{A}-min{A}$\leqslant$7, and

$$A\subset\{1,\ \cdots,93\}\text{ or }A\subset\{94,\ \cdots,177\}\text{ or }A\subset\{178,\ \cdots,288\}.$$

(2) k is an integer.

(3) For j=0, 1, ⋯, k-1, $(A+j)\cap\{66, 69, 91, 92, 93, 162, 171, 175, 176, 177, 243, 264, 286, 287, 288\}=\Phi$ (the empty set), where (A+j)={a_1+j, ⋯, a_n+j}.

(4) $(A+k)\cap\{66, 69, 91, 92, 93, 162, 171, 175, 176, 177, 243, 264, 286, 287, 288\}\neq\Phi$.

(5) t is a time.

Then the following k+1 fault-injections are equivalent. That is, they generate k+1 fault injected key-streams which are completely same.

Injection 0: at time t, the bits at the positions of A are corrupted.

Injection 1: at time t+1, the bits at the positions of A+1 are corrupted.

…

Injection k: at time t+ k, the bits at the positions of A+k are corrupted.

Lemma 2

(1) In case $1\leqslant P_L\leqslant 66$, we can equivalently take M=T, so that $P_H\geqslant 66$.

(2) In case $94\leqslant P_L\leqslant 162$, we can equivalently take M=T, so that $P_H\geqslant 162$.

(3) In case $178\leqslant P_L\leqslant 243$, we can equivalently take M=T, so that $P_H\geqslant 243$.

(4) In case $70\leqslant P_L\leqslant 93$, we can equivalently take $T-2\leqslant M\leqslant T$, so that $91\leqslant P_H\leqslant 93$.

(5) In case $172\leqslant P_L\leqslant 177$, we can equivalently take $T-2\leqslant M\leqslant T$, so that $175\leqslant P_H\leqslant 177$.

(6) In the $265\leqslant P_L\leqslant 288$, we can equivalently take $T-2\leqslant M\leqslant T$, so that $286\leqslant P_H\leqslant 288$.

(7) In the $67\leqslant P_L\leqslant 69$, we can equivalently take $\triangle s_{(M,\,69)}=1$, so that $P_H\geqslant 69$.

(8) In the $163\leqslant P_L\leqslant 171$, we can equivalently take $\triangle s_{(M,\,171)}=1$, so that $P_H\geqslant 171$.

(9) In the $244\leqslant P_L\leqslant 264$, we can equivalently take $\triangle s_{(M,\,264)}=1$, so that $P_H\geqslant 264$.

3.2 Differential Features in Various Cases

Proposition 1 Suppose $1\leqslant P_L\leqslant 66$. Equivalently take M=T and $P_H\geqslant 66$. Then there are m and n, $0\leqslant m\leqslant n\leqslant 7$, such that

(1) $(\triangle z_T,\ \triangle z_{T+1},\ \cdots,\ \triangle z_{T+n-m})=(1, *\cdots *, 1)$.

(2) $(\triangle z_{T+n-m+1},\ \triangle z_{T+n-m+2},\ \cdots,\ \triangle z_{T-m+26})=(0, 0,\ \cdots, 0)$.

(3) $(\triangle z_{T-m+27},\ \triangle z_{T-m+28},\ \cdots,\ \triangle z_{T+26})=(1, *\cdots *)$.

(4) $(\triangle z_{T+27},\ \triangle z_{T+28},\ \cdots,\ \triangle z_{T+n-m+27})=(\triangle z_T,\ \triangle z_{T+1},\ \cdots,\ \triangle z_{T+n-m})=(1, *\cdots *, 1)$.

(5) $(\triangle z_{T+n-m+28},\ \triangle z_{T+n-m+29},\ \cdots,\ \triangle z_{T+65})=(0, 0,\ \cdots, 0)$.

(6) The fault positions are of the set $A=\{t|-n+m+66\leqslant t\leqslant m+66,\ \triangle z_{T-t+93}=1\}$.

Proof Denote $n=P_H-P_L$, $m=P_H-66$, then $n-m=66-P_L$, $0\leqslant m\leqslant n\leqslant 7$. According to Appendix A,

$(\triangle z_T,\ \triangle z_{T+1},\ \cdots,\ \triangle z_{T+n-m})=(\triangle s_{(T,\,66)},\ \triangle s_{(T,\,65)},\ \cdots,\ \triangle s_{(T,\,-n+m+66)})=(1, *\cdots *, 1)$,

$(\triangle z_{T+n-m+1},\ \triangle z_{T+n-m+2},\ \cdots,\ \triangle z_{T-m+26})=(0, 0,\ \cdots, 0)$,

$(\triangle z_{T-m+27},\ \triangle z_{T-m+28},\ \cdots,\ \triangle z_{T+26})=(\triangle s_{(T,\,m+66)},\ \triangle s_{(T,\,m+65)},\ \cdots,\ \triangle s_{(T,\,67)})=(1, *\cdots *)$,

$(\triangle z_{T+27},\ \triangle z_{T+28},\ \cdots,\ \triangle z_{T+n-m+27})=(\triangle s_{(T,\,66)},\ \triangle s_{(T,\,65)},\ \cdots,\ \triangle s_{(T,\,-n+m+66)})=(1, *\cdots *, 1)$,

$(\triangle z_{T+n-m+28},\ \triangle z_{T+n-m+29},\ \cdots,\ \triangle z_{T+65})=(0, 0,\ \cdots, 0)$.

Proposition 1 is proved.

Similar to Proposition 1, the following Proposition 2 and Proposition 3 are true.

Proposition 2 Suppose $94\leqslant P_L\leqslant 162$. Equivalently take M=T and $P_H\geqslant 162$. Then there are m and n, $0\leqslant m\leqslant n\leqslant 7$, such that

(1) $(\triangle z_T,\ \triangle z_{T+1},\ \cdots,\ \triangle z_{T+n-m})=(1, *\cdots *, 1)$.

(2) $(\triangle z_{T+n-m+1}, \triangle z_{T+n-m+2}, \cdots, \triangle z_{T-m+14})=(0, 0, \cdots, 0)$.

(3) $(\triangle z_{T-m+15}, \triangle z_{T-m+16}, \cdots, \triangle z_{T+14})=(1, *\cdots*)$.

(4) $(\triangle z_{T+15}, \triangle z_{T+16}, \cdots, \triangle z_{T+n-m+15})=(\triangle z_{T}, \triangle z_{T+1}, \cdots, \triangle z_{T+n-m})=(1, *\cdots*, 1)$.

(5) $(\triangle z_{T+n-m+16}, \triangle z_{T+n-m+17}, \cdots, \triangle z_{T+65})=(0, 0, \cdots, 0)$.

(6) The fault positions are of the set $A=\{t|-n+m+162\leqslant t\leqslant m+162, \triangle z_{T-t+177}=1\}$.

Proposition 3 Suppose $178\leqslant P_L\leqslant 243$. Equivalently take $M=T$ and $P_H\geqslant 243$. Then there are m and n, $0\leqslant m\leqslant n\leqslant 7$, such that

(1) $(\triangle z_{T}, \triangle z_{T+1}, \cdots, \triangle z_{T+n-m})=(1, *\cdots*, 1)$.

(2) $(\triangle z_{T+n-m+1}, \triangle z_{T+n-m+2}, \cdots, \triangle z_{T-m+44})=(0, 0, \cdots, 0)$.

(3) $(\triangle z_{T-m+45}, \triangle z_{T-m+46}, \cdots, \triangle z_{T+44})=(1, *\cdots*)$.

(4) $(\triangle z_{T+45}, \triangle z_{T+46}, \cdots, \triangle z_{T+n-m+45})=(\triangle z_{T}, \triangle z_{T+1}, \cdots, \triangle z_{T+n-m})=(1, *\cdots*, 1)$.

(5) $(\triangle z_{T+n-m+46}, \triangle z_{T+n-m+47}, \cdots, \triangle z_{T+65})=(0, 0, \cdots, 0)$.

(6) The fault positions are of the set $A=\{t|-n+m+243\leqslant t\leqslant m+243, \triangle z_{T-t+288}=1\}$.

Proposition 4 Suppose $70\leqslant P_L\leqslant 93$. Equivalently take T-$2\leqslant M\leqslant T$ and $91\leqslant P_H\leqslant 93$. Then there is n, $0\leqslant n\leqslant 7$, such that

(1) $(\triangle z_{T}, \triangle z_{T+1}, \cdots, \triangle z_{T+n})=(\triangle s_{(T, 93)}, \triangle s_{(T, 92)}, \cdots, \triangle s_{(T, 93-n)})=(1, *\cdots*, 1)$.

(2) If $M=T$-2 (P_H=91), $(\triangle z_{T+67}, \triangle z_{T+68})=(s_{(T-2, 92)}\triangle s_{(T, 93)}, \triangle(s_{(T, 92)}s_{(T, 93)}))$, and the fault positions are from the set $A=\{t|91-n\leqslant t\leqslant 91, \triangle z_{T-t+91}=1\}$.

(3) If $M=T$-1 (P_H=92), $(\triangle z_{T+67}, \triangle z_{T+68})=(0, \triangle(s_{(T, 92)}s_{(T, 93)}))$, and the fault positions are from the set A+1.

(4) If $M=T$ (P_H=93), $(\triangle z_{T+67}, \triangle z_{T+68})=(0, 0)$, and the fault positions are from the set A+2.

(5) $(\triangle z_{T+69}, \triangle z_{T+70}, \cdots, \triangle z_{T+n+69})=$
$(\triangle(s_{(T, 91)}s_{(T, 92)}+s_{(T, 93)}), \triangle(s_{(T, 90)}s_{(T, 91)}+s_{(T, 92)}), \cdots, \triangle(s_{(T, 91-n)}s_{(T, 92-n)}+s_{(T, 93-n)}))$.

(6) $(\triangle z_{T+67}, \triangle z_{T+68}, \cdots, \triangle z_{T+n+69})=(\triangle z_{T+82}, \triangle z_{T+83}, \cdots, \triangle z_{T+n+84})=(\triangle z_{T+133}, \triangle z_{T+134}, \cdots, \triangle z_{T+n+135})$.

(7) $(\triangle z_{T+145}, \triangle z_{T+146},\triangle z_{T+147})=(\triangle z_{T+67}, \triangle z_{T+68},\triangle z_{T+69})$.

(8) $\triangle z_{T+t}=0$ for other t such that $0\leqslant t\leqslant 147$.

(9) Whether $M=T$-2 or $M=T$-1 or $M=T$, the state differential at time T is the follow: $(\triangle s_{(T, 93-n)}, \triangle s_{(T, 94-n)}, \cdots, \triangle s_{(T, 93)})=(\triangle z_{T+n}, \triangle z_{T+n-1}, \cdots, \triangle z_{T})$, $(\triangle s_{(T, 94)}, \triangle s_{(T, 95)})= (\triangle z_{T+68}, \triangle z_{T+67})$, $\triangle s_{(T, j)}=0$ for other j.

Proof

If $M=T$ (P_H=93), $(\triangle s_{(T, 93)}, \triangle s_{(T, 92)}, \cdots, \triangle s_{(T, 93-n)})=(1, *\cdots*, 1)$, $\triangle s_{(T, j)}=0$ for other j.

If $M=T$-1 (P_H=92), $(\triangle s_{(T, 93)}, \triangle s_{(T, 92)}, \cdots, \triangle s_{(T, 93-n)})=(1, *\cdots*, 1)$, $\triangle s_{(T, 94)}=\triangle(s_{(T, 92)}s_{(T, 93)})$, $\triangle s_{(T, j)}=0$ for other j.

If $M=T$-2 (P_H=91), $(\triangle s_{(T, 93)}, \triangle s_{(T, 92)}, \cdots, \triangle s_{(T, 93-n)})=(1, *\cdots*, 1)$, $\triangle s_{(T, 94)}=\triangle(s_{(T, 92)}s_{(T, 93)})$, $\triangle s_{(T, 95)}=s_{(T-2, 92)}\triangle s_{(T, 93)}$, $\triangle s_{(T, j)}=0$ for other j.

According to Appendix A, Proposition 4 is clear.

Similar to Proposition 4, the following Proposition 5 and Proposition 6 are true.

Proposition 5 Suppose $172\leqslant P_L\leqslant 177$. Equivalently take T-$2\leqslant M\leqslant T$ and $175\leqslant P_H\leqslant 177$.

Then there is n, $0\leqslant n\leqslant 5$, such that

(1) $(\triangle z_{T}, \triangle z_{T+1}, \cdots, \triangle z_{T+n})=(\triangle s_{(T, 177)}, \triangle s_{(T, 176)}, \cdots, \triangle s_{(T, 177-n)})=(1, *\cdots*, 1)$.

(2) If $M=T$-2 (P_H=175), $(\triangle z_{T+64}, \triangle z_{T+65})=(s_{(T-2, 176)}\triangle s_{(T, 177)}, \triangle(s_{(T, 176)}s_{(T, 177)}))$, and the fault positions are from the set $A=\{t|175-n\leqslant t\leqslant 175, \triangle z_{T-t+175}=1\}$.

(3) If $M=T$-1 (P_H=176), $(\triangle z_{T+64}, \triangle z_{T+65})=(0, \triangle(s_{(T, 176)}s_{(T, 177)}))$, and the fault positions are from the set A+1.

(4) If $M=T$ (P_H=177), $(\triangle z_{T+64}, \triangle z_{T+65})=(0, 0)$, and the fault positions are from the set A+2.

(5) $(\triangle z_{T+66}, \triangle z_{T+67}, \cdots, \triangle z_{T+n+66})=$
$(\triangle(s_{(T, 175)}s_{(T, 176)}+s_{(T, 177)}), \triangle(s_{(T, 174)}s_{(T, 175)}+s_{(T, 176)}), \cdots, \triangle(s_{(T, 175-n)}s_{(T, 176-n)}+s_{(T, 177-n)}))$.

(6) $(\triangle z_{T+64}, \triangle z_{T+65}, \cdots, \triangle z_{T+n+66})=(\triangle z_{T+109}, \triangle z_{T+110}, \cdots, \triangle z_{T+n+111})=(\triangle z_{T+130}, \triangle z_{T+131}, \cdots, \triangle z_{T+n+132})$.

(7) $\triangle z_{T+t}=0$ for other t such that $0\leqslant t\leqslant 147$.

(8) Whether $M=T$-2 or $M=T$-1 or $M=T$, the state differential at time T is the follow: $(\triangle s_{(T, 177-n)}, \triangle s_{(T, 178-n)}, \cdots, \triangle s_{(T, 177)})=(\triangle z_{T+n}, \triangle z_{T+n-1}, \cdots, \triangle z_{T})$, $(\triangle s_{(T, 178)}, \triangle s_{(T, 179)})= (\triangle z_{T+65}, \triangle z_{T+64})$, $\triangle s_{(T, j)}=0$ for other j.

Proposition 6 Suppose $265\leqslant P_L\leqslant 288$. Equivalently take T-$2\leqslant M\leqslant T$ and $286\leqslant P_H\leqslant 288$. Then there is n, $0\leqslant n\leqslant 7$, such that

(1) $(\triangle z_{T}, \triangle z_{T+1}, \cdots, \triangle z_{T+n})=(\triangle s_{(T, 288)}, \triangle s_{(T, 287)}, \cdots, \triangle s_{(T, 288-n)})=(1, *\cdots*, 1)$.

(2) If $M=T$-2 (P_H=286), $(\triangle z_{T+64}, \triangle z_{T+65})=(s_{(T-2, 287)}\triangle s_{(T, 288)}, \triangle(s_{(T, 287)}s_{(T, 288)}))$, and the fault positions are from the set $A=\{t|286-n\leqslant t\leqslant 286, \triangle z_{T-t+286}=1\}$.

(3) If $M=T$-1 (P_H=287), $(\triangle z_{T+64}, \triangle z_{T+65})=(0, \triangle(s_{(T, 287)}s_{(T, 288)}))$, and the fault positions are from the set A+1.

(4) If $M=T$ (P_H=288), $(\triangle z_{T+64}, \triangle z_{T+65})=(0, 0)$, and the fault positions are from the set A+2.

(5) $(\triangle z_{T+66}, \triangle z_{T+67}, \cdots, \triangle z_{T+n+66})=$
$(\triangle(s_{(T, 286)}s_{(T, 287)}+s_{(T, 288)}), \triangle(s_{(T, 285)}s_{(T, 286)}+s_{(T, 287)}), \cdots, \triangle(s_{(T, 286-n)}s_{(T, 287-n)}+s_{(T, 288-n)}))$.

(6) $(\triangle z_{T+64}, \triangle z_{T+65}, \cdots, \triangle z_{T+n+66})=(\triangle z_{T+91}, \triangle z_{T+92}, \cdots, \triangle z_{T+n+93})$.

(7) $\triangle z_{T+t}=0$ for other t such that $0\leqslant t\leqslant 147$.

(8) Whether $M=T$-2 or $M=T$-1 or $M=T$, the state differential at time T is the follow: $(\triangle s_{(T, 288-n)}, \triangle s_{(T, 289-n)}, \cdots, \triangle s_{(T, 288)})=(\triangle z_{T+n}, \triangle z_{T+n-1}, \cdots, \triangle z_{T})$, $(\triangle s_{(T, 1)}, \triangle s_{(T, 2)})= (\triangle z_{T+65}, \triangle z_{T+64})$, $\triangle s_{(T, j)}=0$ for other j.

Proposition 7 Suppose $67\leqslant P_L\leqslant 69$. Equivalently take $\triangle s_{(M, 69)}=1$ and $P_H\geqslant 69$. Then there are m and n, $m\geqslant 0$, n-$2\leqslant m\leqslant n\leqslant 7$, such that

(1) $(\triangle z_{T}, \triangle z_{T+1}, \cdots, \triangle z_{T+n})=(1, *\cdots*, 1)$, where $\triangle z_{T+m}=1$.

(2) $(\triangle z_{T+n+1}, \triangle z_{T+n+2}, \cdots, \triangle z_{T+m+41})=(0, 0, \cdots, 0)$.

(3) $(\triangle z_{T+m+42}, \triangle z_{T+m+43}, \cdots, \triangle z_{T+n+42})=(\triangle z_{T+m}, \triangle z_{T+1+m}, \cdots, \triangle z_{T+n})=(1, *\cdots*, 1)$.

(4) $(\triangle z_{T+n+43}, \triangle z_{T+n+44}, \cdots, \triangle z_{T+66})=(0, 0, \cdots, 0)$.

(5) $(\triangle z_{T+92}, \triangle z_{T+m+109}, \cdots, \triangle z_{T+m+125})=(0, 0, \cdots, 0)$.

(6) $M=T$-24+m, where m is the smallest t such that $0\leqslant t\leqslant 7$ and $\triangle z_{T+t+42}=1$.

(7) The fault positions are of the set $A=\{t|69-n+m\leqslant t\leqslant 69+m, \triangle z_{T-t+m+69}=1\}$.

Proof Denote $n=P_H$-P_L, $m=P_H$-69, then n-m=69-P_L, $m\geqslant 0$, n-$2\leqslant m\leqslant n\leqslant 7$. According to the state renewal (Table 2) we know that, from time M to time T, position 69+m shifts to position 93.

So that T-M=24-m. We take close contact with differential floating feature.

At time M, the state differential is the follow.

$(\triangle s_{(M, 69-n+m)}, \cdots, \triangle s_{(M, 69+m)})=(1, *, \cdots *, 1)$, where $\triangle s_{(M, 69)}=1$.

$\triangle s_{(M, j)}=0$ for other j.

So that, at time $T=M+24-m$, the state differential is the follow.

$(\triangle s_{(T, 93-n)}, \cdots, \triangle s_{(T, 93)})=(\triangle s_{(M, 69-n+m)}, \cdots, \triangle s_{(M, 69+m)})=(1, *\cdots *, 1)$, where $\triangle s_{(T, 93-m)}=1$.

$(\triangle s_{(T, 24-n)}, \cdots, \triangle s_{(T, 24-m)})=(\triangle s_{(M, 69-n+m)}, \cdots, \triangle s_{(M, 69)})=(1, *, \cdots *, 1)$.

$(\triangle s_{(T, 94)}, \triangle s_{(T, 95)})=(\triangle(s_{(M, 68+m)}s_{(M, 69+m)}), \triangle(s_{(M, 69+m)}s_{(M, 70+m)}))$.

$\triangle s_{(T, j)}=0$ for each $j \notin \{24-n, 25-n, \cdots, 24-m, 93-n, 94-n, \cdots, 95\}$.

According to Appendix A and the state differential at time T, we can partly determine $(\triangle z_T, \triangle z_{T+1}, \triangle z_{T+2}, \cdots)$ as the follow.

$(\triangle z_T, \triangle z_{T+1}, \cdots, \triangle z_{T+n})=(\triangle s_{(T, 93)}, \triangle s_{(T, 92)}, \cdots, \triangle s_{(T, 93-n)})=(1, *\cdots *, 1)$, where $\triangle z_{T+m}=1$.

$(\triangle z_{T+n+1}, \triangle z_{T+n+2}, \cdots, \triangle z_{T+m+41})$ have no relation with $\{\triangle s_{(T, j)} | j \in \{24-n, 25-n, \cdots, 24-m, 93-n, 94-n, \cdots, 95\}\}$, so that $(\triangle z_{T+n+1}, \triangle z_{T+n+2}, \cdots, \triangle z_{T+m+41})=(0, \cdots, 0)$.

$(\triangle z_{T+m+42}, \triangle z_{T+m+43}, \cdots, \triangle z_{T+n+42})=(\triangle s_{(T, 24-m)}, \triangle s_{(T, 23-m)}, \cdots, \triangle s_{(T, 24-n)})=(1, *, \cdots *, 1)$.

$(\triangle z_{T+n+43}, \triangle z_{T+n+44}, \cdots, \triangle z_{T+66})$ have no relation with $\{\triangle s_{(T, j)} | j \in \{24-n, 25-n, \cdots, 24-m, 93-n, 94-n, \cdots, 95\}\}$, so that $(\triangle z_{T+n+43}, \triangle z_{T+n+44}, \cdots, \triangle z_{T+66})=(0, 0, \cdots, 0)$.

$(\triangle z_{T+92}, \triangle z_{T+m+109}, \cdots, \triangle z_{T+m+125})$ have no relation with $\{\triangle s_{(T, j)} | j \in \{24-n, 25-n, \cdots, 24-m, 93-n, 94-n, \cdots, 95\}\}$, so that $(\triangle z_{T+92}, \triangle z_{T+m+109}, \cdots, \triangle z_{T+m+125})=(0, 0, \cdots, 0)$.

Proposition 7 is proved.

Lemma 3 Suppose $163 \leqslant P_L \leqslant 171$. Equivalently take $\triangle s_{(M, 171)}=1$ and $P_H \geqslant 171$. Then there are m and n, $0 \leqslant m \leqslant 6$, $m \leqslant n \leqslant 7$, such that $M=T-6+m$. The fault positions are of the set $A=\{t | 171-n+m \leqslant t \leqslant 171+m, \triangle z_{T-t+m+171}=1\}$. The differential at time $T+n+1$ is the follow.

(1) $(\triangle s_{(T+n+1, 178)}, \triangle s_{(T+n+1, 179)}, \cdots, \triangle s_{(T+n+1, 178+n)})$

$=(\triangle(s_{(M, 169-n+m)}s_{(M, 170-n+m)}+s_{(M, 171-n+m)}), \triangle(s_{(M, 170-n+m)}s_{(M, 171-n+m)}+s_{(M, 172-n+m)}), \cdots, \triangle(s_{(M, 169+m)}s_{(M, 170+m)}+s_{(M, 171+m)}))$.

(2) If $M=T$ (m=6), $(\triangle s_{(T+n+1, 179+n)}, \triangle s_{(T+n+1, 180+n)})=(0, 0)$.

(3) If $M=T-1$ (m=5), $(\triangle s_{(T+n+1, 179+n)}, \triangle s_{(T+n+1, 180+n)})=(\triangle(s_{(M, 170+m)}s_{(M, 171+m)}), 0)$.

(4) If $M<T-1$ (m<5), $(\triangle s_{(T+n+1, 179+n)}, \triangle s_{(T+n+1, 180+n)})=(\triangle(s_{(M, 170+m)}s_{(M, 171+m)}), s_{(M, 172+m)}\triangle s_{(M, 171+m)})$.

(5) $(\triangle s_{(T+n+1, 100)}, \cdots, \triangle s_{(T+n+1, 100-m+n)})=(\triangle s_{(M, 171-n+m)}, \cdots, \triangle s_{(M, 171)})=(1, *, \cdots *, 1)$.

(6) $\triangle s_{(T+n+1, j)}=0$ for each $j \notin \{100, 101, \cdots, 100-m+n, 178, 179, \cdots, 180+n\}$.

Proof Denote $n=P_H-P_L$, $m=P_H-171$, then $n-m=171-P_L$, $0 \leqslant m \leqslant 6$, $m \leqslant n \leqslant 7$. According to the state renewal (Table 2) we know that, from time M to time T, position 171+m shifts to position 177. So that T-M=6-m. We take close contact with differential floating feature.

At time M, the state differential is the follow.

$(\triangle s_{(M, 171-n+m)}, \cdots, \triangle s_{(M, 171+m)})=(1, *, \cdots *, 1)$, where $\triangle s_{(M, 171)}=1$.

$\triangle s_{(M, j)}=0$ for other j.

At time $T+n+1$, the state differential is the follow.

$(\triangle s_{(T+n+1, 178)}, \triangle s_{(T+n+1, 179)}, \cdots, \triangle s_{(T+n+1, 178+n)})$

$=(\triangle(s_{(T, 175-n)}s_{(T, 176-n)}+s_{(T, 177-n)}), \triangle(s_{(T, 176-n)}s_{(T, 177-n)}+s_{(T, 178-n)}), \cdots, \triangle(s_{(T, 175)}s_{(T, 176)}+s_{(T, 177)}))$

$=(\triangle(s_{(M, 169-n+m)}s_{(M, 170-n+m)}+s_{(M, 171-n+m)}), \triangle(s_{(M, 170-n+m)}s_{(M, 171-n+m)}+s_{(M, 172-n+m)}), \cdots, \triangle(s_{(M,$

$_{169+m)}s_{(M,\,170+m)}+s_{(M,\,171+m)}))$.

If $M=T$ ($m=6$),

$$(\triangle s_{(T+n+1,\,179+n)},\ \triangle s_{(T+n+1,\,180+n)})=(\triangle s_{(T,\,178)},\ \triangle s_{(T,\,179)})=(0, 0).$$

If $M=T$-1 ($m=5$),

$$(\triangle s_{(T+n+1,\,179+n)},\ \triangle s_{(T+n+1,\,180+n)})=(\triangle s_{(T,\,178)},\ \triangle s_{(T,\,179)})=(\triangle(s_{(M,\,170+m)}s_{(M,\,171+m)}), 0).$$

If $M<T$-1 ($m<5$),

$$(\triangle s_{(T+n+1,\,179+n)},\ \triangle s_{(T+n+1,\,180+n)})=(\triangle s_{(T,\,178)},\ \triangle s_{(T,\,179)})$$
$$=(\triangle(s_{(M,\,170+m)}s_{(M,\,171+m)}),\ s_{(M,\,172+m)}\triangle s_{(M,\,171+m)}).$$

$(\triangle s_{(T+n+1,\,100)},\ \cdots,\ \triangle s_{(T+n+1,\,100\text{-}m+n)})=(\triangle s_{(M,\,171\text{-}n+m)},\ \cdots,\ \triangle s_{(M,\,171)})=(1, *, \cdots*, 1)$.

$\triangle s_{(T+n+1,\,j)}=0$ for each $j\notin\{100, 101, \cdots, 100\text{-}m+n, 178, 179, \cdots, 180+n\}$.

Lemma 3 is proved.

Proposition 8 Suppose $163\leqslant P_L\leqslant 171$. Equivalently take $\triangle s_{(M,\,171)}=1$ and $P_H\geqslant 171$. Then there are m and n, $0\leqslant m\leqslant 6$, $m\leqslant n\leqslant 7$, such that

(1) $M=T$-6+m.

(2) The fault positions are of the set $A=\{t|171\text{-}n+m\leqslant t\leqslant 171+m,\ \triangle z_{T\text{-}t+m+171}=1\}$.

(3) $(\triangle z_T,\ \triangle z_{T+1},\ \cdots,\ \triangle z_{T+n})=(\triangle s_{(M,\ 171+m)},\ \triangle s_{(M,\ 170+m)},\ \cdots,\ \triangle s_{(M,\ 171\text{-}n+m)},)=(1,\ *\cdots*,\ 1)$, where $\triangle z_{T+m}=1$.

(4) $(\triangle z_{T+n+1},\ \triangle z_{T+n+2},\ \cdots,\ \triangle z_{T+147})$ can be decomposed as

$$(\triangle z_{T+n+1},\ \triangle z_{T+n+2},\ \cdots,\ \triangle z_{T+147})=$$
$$(\triangle u_{T+n+1},\ \triangle u_{T+n+2},\ \cdots,\ \triangle u_{T+147})+(\triangle v_{T+n+1},\ \triangle v_{T+n+2},\ \cdots,\ \triangle v_{T+147}).$$

$(\triangle u_{T+n+1},\ \triangle u_{T+n+2},\ \cdots,\ \triangle u_{T+147})$ is of the following shape.

(u1)

$$(\triangle u_{T+64},\ \triangle u_{T+65},\ \cdots,\ \triangle u_{T+n+66})$$
$$=(\triangle u_{T+109},\ \triangle u_{T+110},\ \cdots,\ \triangle u_{T+n+111})$$
$$=(\triangle u_{T+130},\ \triangle u_{T+131},\ \cdots,\ \triangle u_{T+n+132})$$
$$=(\triangle s_{(T+n+1,\,180+n)},\ \triangle s_{(T+n+1,\,179+n)},\ \cdots,\ \triangle s_{(T+n+1,\,178)}).$$

(u2) $\triangle u_{T+j}=0$ for other $j\in\{n+1, n+2, \cdots, 147\}$.

$(\triangle v_{T+n+1},\ \triangle v_{T+n+2},\ \cdots,\ \triangle v_{T+147})$ is of the following shape.

(v1)

$$(\triangle v_{T+m+63},\ \triangle v_{T+m+64},\ \cdots,\ \triangle v_{T+n+63})$$
$$=(\triangle v_{T+m+78},\ \triangle v_{T+m+79},\ \cdots,\ \triangle v_{T+n+78})$$
$$=(\triangle v_{T+m+129},\ \triangle v_{T+m+130},\ \cdots,\ \triangle v_{T+n+129})$$
$$=(\triangle s_{(T+n+1,\,\text{-}m+n+100)},\ \triangle s_{(T+n+1,\,\text{-}m+n+99)},\ \cdots,\ \triangle s_{(T+n+1,\,100)})$$
$$=(1, *\cdots*, 1).$$

(v2) $(\triangle v_{T+m+141},\ \triangle v_{T+m+142},\ \cdots,\ \triangle v_{T+n+144})$ is some function of $\{\triangle s_{(T+n+1,\ 100)},\ \triangle s_{(T+n+1,\ 101)},\ \cdots,\ \triangle s_{(T+n+1,\,\text{-}m+n+100)}\}$, where $\triangle v_{T+m+141}=1$.

(v3) $\triangle v_{T+j}=0$ for other $j\in\{n+1, n+2, \cdots, 147\}$.

(5) m is the smallest t such that $0\leqslant t\leqslant 7$ and $\triangle z_{T+t+78}=1$.

Proof (1) and (2) have already been proved by Lemma 3. Again (3) is direct. From Lemma 3 we have already known the state differential at time $T+n+1$.

Now we take the stream differential $(\triangle u_{T+n+1},\ \triangle u_{T+n+2},\ \cdots,\ \triangle u_{T+147})$ as generated by such state differential at time $T+n+1$: respectively $\{\triangle s_{(T+n+1,\,178)},\ \triangle s_{(T+n+1,\,179)},\ \cdots,\ \triangle s_{(T+n+1,\,180+n)}\}$ at positions from $\{178, 179, \cdots, 180+n\}$, and 0 at other positions. Then $(\triangle u_{T+n+1}, \triangle u_{T+n+2}, \cdots, \triangle u_{T+147})$ is of the following shape.

$(\triangle u_{T+64}, \triangle u_{T+65}, \cdots, \triangle u_{T+n+66})$
$=(\triangle u_{T+109}, \triangle u_{T+110}, \cdots, \triangle u_{T+n+111})$
$=(\triangle u_{T+130}, \triangle u_{T+131}, \cdots, \triangle u_{T+n+132})$
$=(\triangle s_{(T+n+1, 180+n)}, \triangle s_{(T+n+1, 179+n)}, \cdots, \triangle s_{(T+n+1, 178)})$.

$\triangle u_{T+j}=0$ for other $j\in\{n+1, n+2, \cdots, 147\}$.

Again we take the stream differential $(\triangle v_{T+n+1}, \triangle v_{T+n+2}, \cdots, \triangle v_{T+147})$ as generated by such state differential at time $T+n+1$: respectively $\{\triangle s_{(T+n+1, 100)}, \triangle s_{(T+n+1, 101)}, \cdots, \triangle s_{(T+n+1, -m+n+100)}\}=\{1, *\cdots*, 1\}$ at positions from $\{100, 101, \cdots, 100-m+n\}$, and 0 at other positions. Then $(\triangle v_{T+n+1}, \triangle v_{T+n+2}, \cdots, \triangle v_{T+147})$ is of the following shape.

$(\triangle v_{T+m+63}, \triangle v_{T+m+64}, \cdots, \triangle v_{T+n+63})$
$=(\triangle v_{T+m+78}, \triangle v_{T+m+79}, \cdots, \triangle v_{T+n+78})$
$=(\triangle v_{T+m+129}, \triangle v_{T+m+130}, \cdots, \triangle v_{T+n+129})$
$=(\triangle s_{(T+n+1, -m+n+100)}, \triangle s_{(T+n+1, -m+n+99)}, \cdots, \triangle s_{(T+n+1, 100)})$
$=\{1, *\cdots*, 1\}$.

$\triangle v_{T+m+141}=\triangle s_{(T+n+1, 100+n-m)}=1$.

$(\triangle v_{T+m+142}, \triangle v_{T+m+143}, \cdots, \triangle v_{T+n+144})$ is some function of $\{\triangle s_{(T+n+1, 100)}, \triangle s_{(T+n+1, 101)}, \cdots, \triangle s_{(T+n+1, -m+n+100)}\}$.

$\triangle v_{T+j}=0$ for other $j\in\{n+1, n+2, \cdots, 147\}$.

In each equation of Appendix A, there is no the product of such two factors, one of which is from the position set $\{100, 101, \cdots, 100-m+n\}$, and another is from the position set $\{178, 179, \cdots, 180+n\}$. This implies that

$(\triangle z_{T+n+1}, \triangle z_{T+n+2}, \cdots, \triangle z_{T+147})=$
$(\triangle u_{T+n+1}, \triangle u_{T+n+2}, \cdots, \triangle u_{T+147})+(\triangle v_{T+n+1}, \triangle v_{T+n+2}, \cdots, \triangle v_{T+147})$.

So that

$(\triangle z_{T+78}, \triangle z_{T+79}, \cdots, \triangle z_{T+85})=(\triangle v_{T+78}, \triangle v_{T+79}, \cdots, \triangle v_{T+85})$,

and $\triangle v_{T+78}=\triangle v_{T+79}=\cdots=\triangle v_{T+m+77}=0$, $\triangle v_{T+m+78}=1$.

Proposition 8 is proved.

Proposition 9 Suppose $244\leqslant P_L\leqslant 264$. Equivalently take $\triangle s_{(M, 264)}=1$ and $P_H\geqslant 264$. Then there are m and n, $0\leqslant m\leqslant n\leqslant 7$, such that

(1) $(\triangle z_T, \triangle z_{T+1}, \cdots, \triangle z_{T+n})=(1, *\cdots*, 1)$, where $\triangle z_{T+m}=1$.

(2) $(\triangle z_{T+n+1}, \triangle z_{T+n+2}, \cdots, \triangle z_{T+m+41})=(0, 0, \cdots, 0)$.

(3) $(\triangle z_{T+m+42}, \triangle z_{T+m+43}, \cdots, \triangle z_{T+n+42})=(\triangle z_{T+m}, \triangle z_{T+1+m}, \cdots, \triangle z_{T+n})=(1, *\cdots*, 1)$.

(4) $(\triangle z_{T+n+43}, \triangle z_{T+n+44}, \cdots, \triangle z_{T+63})=(0, 0, \cdots, 0)$.

(5) $(\triangle z_{T+m+108}, \triangle z_{T+m+109}, \cdots, \triangle z_{T+n+108})=(\triangle z_{T+m}, \triangle z_{T+1+m}, \cdots, \triangle z_{T+n})=(1, *\cdots*, 1)$.

(6) $M=T-24+m$, where m is the smallest t such that $0\leqslant t\leqslant 7$ and $\triangle z_{T+t+42}=1$.

(7) The fault positions are of the set $A=\{t|264-n+m\leqslant t\leqslant 264+m, \triangle z_{T-t+m+264}=1\}$.

Proof Denote $n=P_H-P_L$, $m=P_H-264$, then $n-m=264-P_L$, $0\leqslant m\leqslant n\leqslant 7$. According to the state renewal (Table 2) we know that, from time M to time T, position $264+m$ shifts to position 288. So that $T-M=24-m$. We take close contact with differential floating feature.

At time M, the state differential is the follow.

$(\triangle s_{(M, 264-n+m)}, \cdots, \triangle s_{(M, 264+m)})=(1, *, \cdots *, 1)$, where $\triangle s_{(M, 264)}=1$.

$\triangle s_{(M, j)}=0$ for other j.

So that, at time $T=M+24-m$, the state differential is the follow.

$(\triangle s_{(T, 288-n)}, \cdots, \triangle s_{(T, 288)})=(\triangle s_{(M, 264-n+m)}, \cdots, \triangle s_{(M, 264+m)})=(1, *\cdots *, 1)$, where $\triangle s_{(T, 288-m)}=1$.

$(\triangle s_{(T, 201-n)}, \cdots, \triangle s_{(T, 201-m)})=(\triangle s_{(M, 264-n+m)}, \cdots, \triangle s_{(M, 264)})=(1, *, \cdots *, 1)$.

$(\triangle s_{(T, 1)}, \triangle s_{(T, 2)})=(\triangle(s_{(M, 263+m)}s_{(M, 264+m)}), \triangle(s_{(M, 264+m)}s_{(M, 265+m)}))$.

$\triangle s_{(T, j)}=0$ for each $j\notin\{1, 2, 201-n, 202-n, \cdots, 201-m, 288-n, 289-n, \cdots, 288\}$.

According to Appendix A and the state differential at time T, we can partly determine $(\triangle z_T, \triangle z_{T+1}, \triangle z_{T+2}, \cdots)$ as the follow.

$(\triangle z_T, \triangle z_{T+1}, \cdots, \triangle z_{T+n})=(\triangle s_{(T, 288-n)}, \cdots, \triangle s_{(T, 288)})=(1, *\cdots *, 1)$, where $\triangle z_{T+m}=1$.

$(\triangle z_{T+n+1}, \triangle z_{T+n+2}, \cdots, \triangle z_{T+m+41})=(0, \cdots, 0)$.

$(\triangle z_{T+m+42}, \triangle z_{T+m+43}, \cdots, \triangle z_{T+n+42})=(\triangle s_{(T, 201-m)}, \cdots, \triangle s_{(T, 201-n)})=(1, *, \cdots *, 1)$.

$(\triangle z_{T+n+43}, \triangle z_{T+n+44}, \cdots, \triangle z_{T+63})=(0, 0, \cdots, 0)$.

$(\triangle z_{T+m+108}, \triangle z_{T+m+109}, \cdots, \triangle z_{T+n+108})=(\triangle s_{(T, 201-m)}, \cdots, \triangle s_{(T, 201-n)})=(1, *, \cdots *, 1)$.

Proposition 9 is proved.

3.3 Case Checking

By Proposition 1~3 and Proposition 7~9 we know that, if the attacker knows which case is from $\{1\leqslant P_L\leqslant 66, 67\leqslant P_L\leqslant 69, 94\leqslant P_L\leqslant 162, 163\leqslant P_L\leqslant 171, 178\leqslant P_L\leqslant 243, 244\leqslant P_L\leqslant 264\}$, the injection time M and the fault positions can be determined. By Proposition 4~6 we know that, if the attacker knows which case is from $\{70\leqslant P_L\leqslant 93, 172\leqslant P_L\leqslant 177, 265\leqslant P_L\leqslant 288\}$, the injection time M has three possibilities, correspondingly the fault positions are of a floating set. But in each of these three cases the state differential at time T can be determined. This is enough for floating attack. So that we need only to check the cases by the key-stream differential $(\triangle z_T, \triangle z_{T+1},\triangle z_{T+2}, \cdots)$. We consider 10 cases $\{1\leqslant P_L\leqslant 66, 67\leqslant P_L\leqslant 69, 70\leqslant P_L\leqslant 93, 94\leqslant P_L\leqslant 162, 163\leqslant P_L\leqslant 171, 172\leqslant P_L\leqslant 177, 178\leqslant P_L\leqslant 243, 244\leqslant P_L\leqslant 264, 265\leqslant P_L\leqslant 288,$ Injection Failure$\}$, with an additional case called Injection Failure. Injection Failure is described as that $\triangle z_{T+8}\triangle z_{T+9}\cdots=00\cdots$ is a 0 sequence. Injection Failure has no help for breaking Trivium, because the attacker can not obtain any useful equation. The following facts, about Injection Failure, are easy to be proved. Injection Failure overlaps each one of 3 cases $\{70\leqslant P_L\leqslant 93, 172\leqslant P_L\leqslant 177, 265\leqslant P_L\leqslant 288\}$. Injection Failure does not overlap any one of 6 cases $\{1\leqslant P_L\leqslant 66, 67\leqslant P_L\leqslant 69, 94\leqslant P_L\leqslant 162, 163\leqslant P_L\leqslant 171, 178\leqslant P_L\leqslant 243, 244\leqslant P_L\leqslant 264\}$. If $\triangle z_{T+8}\triangle z_{T+9}\cdots\triangle z_{T+147}$ is a 0 string, the case is Injection Failure. If one is in case $70\leqslant P_L\leqslant 93$, he is not in case Injection Failure if and only if $(\triangle z_{T+82}, \triangle z_{T+83}, \cdots, \triangle z_{T+n+84})\neq(0, 0, \cdots, 0)$, according to Proposition 4. If one is in case $172\leqslant P_L\leqslant 177$, he is not in case Injection Failure if and only if $(\triangle z_{T+109}, \triangle z_{T+110}, \cdots, \triangle z_{T+n+111})\neq(0, 0, \cdots, 0)$, according to Proposition 5. If one is in case $265\leqslant P_L\leqslant 288$, he is not in case Injection Failure if and only if $(\triangle z_{T+91}, \triangle z_{T+92}, \cdots, \triangle z_{T+n+93})\neq(0, 0, \cdots, 0)$, according to Proposition 6.

In this subsection we use the following notations.

- n is the largest t such that $0\leqslant t\leqslant 7$ and $\triangle z_{T+t}=1$.
- l is the smallest t such that $t>n$ and $\triangle z_{T+t}=1$.

- k is the largest t such that $l \leqslant t \leqslant l+7$ and $\triangle z_{T+t}=1$.

By Proposition 1~9, the following Proposition 10 and Proposition 11 are clear.

Proposition 10

(1) The value of k-n comes from $\{27, 15, 45, 42, [55, +\infty]\}$.

(2) If k-n=27, the case is $1 \leqslant P_L \leqslant 66$.

(3) If k-n=15, the case is $94 \leqslant P_L \leqslant 162$.

(4) If k-n=45, the case is $178 \leqslant P_L \leqslant 243$.

(5) If k-n=42, the case is from $\{67 \leqslant P_L \leqslant 69, 244 \leqslant P_L \leqslant 264\}$.

(6) If k-$n \in [55, +\infty]$, the case is from $\{70 \leqslant P_L \leqslant 93, 163 \leqslant P_L \leqslant 171, 172 \leqslant P_L \leqslant 177, 265 \leqslant P_L \leqslant 288$, Injection Failure$\}$.

Proposition 11 Suppose the case is from $\{67 \leqslant P_L \leqslant 69, 244 \leqslant P_L \leqslant 264\}$. If $(\triangle z_{T+108}, \triangle z_{T+109}, \cdots, \triangle z_{T+n+108})=(0, 0, \cdots, 0)$, the case is $67 \leqslant P_L \leqslant 69$, or else $244 \leqslant P_L \leqslant 264$.

Proposition 12 Suppose the case is from $\{70 \leqslant P_L \leqslant 93, 163 \leqslant P_L \leqslant 171, 172 \leqslant P_L \leqslant 177, 265 \leqslant P_L \leqslant 288$, Injection Failure$\}$. If $(\triangle z_{T+140}, \triangle z_{T+141}, \cdots, \triangle z_{T+147}) \neq (0, 0, \cdots, 0)$, the case is from $\{70 \leqslant P_L \leqslant 93, 163 \leqslant P_L \leqslant 171\}$, or else the case is from $\{70 \leqslant P_L \leqslant 93, 172 \leqslant P_L \leqslant 177, 265 \leqslant P_L \leqslant 288$, Injection Failure$\}$.

Proof Consider Proposition 4, Proposition 5, Proposition 6 and Proposition 8. $(\triangle z_{T+140}, \triangle z_{T+141}, \cdots, \triangle z_{T+147}) \neq (0, 0, \cdots, 0)$ in case $163 \leqslant P_L \leqslant 171$. $(\triangle z_{T+140}, \triangle z_{T+141}, \cdots, \triangle z_{T+147})=(0, 0, \cdots, 0)$ in each case from $\{172 \leqslant P_L \leqslant 177, 265 \leqslant P_L \leqslant 288$, Injection Failure$\}$. It is not certain whether $(\triangle z_{T+140}, \triangle z_{T+141}, \cdots, \triangle z_{T+147})=(0, 0, \cdots, 0)$ in case $70 \leqslant P_L \leqslant 93$ (more detailed analysis shows that, in case $70 \leqslant P_L \leqslant 93$, $(\triangle z_{T+140}, \triangle z_{T+141}, \cdots, \triangle z_{T+147})=(0, 0, \cdots, 0)$ with small probability).

Proposition 13 Suppose the case is from $\{70 \leqslant P_L \leqslant 93, 172 \leqslant P_L \leqslant 177, 265 \leqslant P_L \leqslant 288$, Injection Failure$\}$.

(1) If $(\triangle z_{T+109}, \triangle z_{T+110}, \cdots, \triangle z_{T+118}) \neq (0, 0, \cdots, 0)$, the case is $172 \leqslant P_L \leqslant 177$.

(2) If $(\triangle z_{T+109}, \triangle z_{T+110}, \cdots, \triangle z_{T+118})=(0, 0, \cdots, 0)$, and $(\triangle z_{T+133}, \triangle z_{T+134}, \cdots, \triangle z_{T+147}) \neq (0, 0, \cdots, 0)$, the case is $70 \leqslant P_L \leqslant 93$.

(3) If $(\triangle z_{T+109}, \triangle z_{T+110}, \cdots, \triangle z_{T+118})=(0, 0, \cdots, 0)$, $(\triangle z_{T+133}, \triangle z_{T+134}, \cdots, \triangle z_{T+147})=(0, 0, \cdots, 0)$, and $(\triangle z_{T+91}, \triangle z_{T+92}, \cdots, \triangle z_{T+100}) \neq (0, 0, \cdots, 0)$, the case is $265 \leqslant P_L \leqslant 288$.

(4) If $(\triangle z_{T+109}, \triangle z_{T+110}, \cdots, \triangle z_{T+118})=(0, 0, \cdots, 0)$, $(\triangle z_{T+133}, \triangle z_{T+134}, \cdots, \triangle z_{T+147})=(0, 0, \cdots, 0)$, and $(\triangle z_{T+91}, \triangle z_{T+92}, \cdots, \triangle z_{T+100})=(0, 0, \cdots, 0)$, the case is Injection Failure.

Proof (1), (2), and (3) of Proposition 13 are clear. If the case is from $\{70 \leqslant P_L \leqslant 93, 172 \leqslant P_L \leqslant 177, 265 \leqslant P_L \leqslant 288$, Injection Failure$\}$, and all conditions of (4) of Proposition 13 hold, $(\triangle z_{T+n+1}, \triangle z_{T+n+2}, \cdots, \triangle z_{T+147})=(0, 0, \cdots, 0)$ is a 0 string. So that $(\triangle z_{T+n+1}, \triangle z_{T+n+2}, \cdots)=(0, 0, \cdots)$ is a 0 stream.

We say the string $\triangle z_T \triangle z_{T+1} \triangle z_{T+2} \cdots \triangle z_{T+147}$ possesses the features of the case $70 \leqslant P_L \leqslant 93$, if each of the following 3 conditions is true.

Condition 1: $(\triangle z_{T+67}, \triangle z_{T+68}, \cdots, \triangle z_{T+n+69})=(\triangle z_{T+82}, \triangle z_{T+83}, \cdots, \triangle z_{T+n+84})=(\triangle z_{T+133}, \triangle z_{T+134}, \cdots, \triangle z_{T+n+135})$.

Condition 2: $(\triangle z_{T+145}, \triangle z_{T+146}, \triangle z_{T+147})=(\triangle z_{T+67}, \triangle z_{T+68}, \triangle z_{T+69})$.

Condition 3: $\triangle z_{T+t}=0$ for other t such that $n+1\leqslant t\leqslant 147$.

Lemma 4 Suppose the case is $163\leqslant P_L\leqslant 171$, and $\triangle z_T\triangle z_{T+1}\triangle z_{T+2}\cdots\triangle z_{T+147}$ possesses the features of the case $70\leqslant P_L\leqslant 93$. Then we have

(1) $4\leqslant n\leqslant 7$.

(2) There is m, $4\leqslant m\leqslant n\leqslant 7$, such that $(\triangle z_{T+63+m}, \triangle z_{T+64+m}, \cdots, \triangle z_{T+63+n})=(\triangle z_{T+78+m}, \triangle z_{T+79+m}, \cdots, \triangle z_{T+78+n})=(\triangle z_{T+129+m}, \triangle z_{T+130+m}, \cdots, \triangle z_{T+129+n})=(1, *\cdots*, 1)$.

(3) $(\triangle z_{T+63+m}, \triangle z_{T+64+m}, \cdots, \triangle z_{T+69})=(\triangle z_{T+141+m}, \triangle z_{T+142+m}, \cdots, \triangle z_{T+147})=(1, *, *)$

(4) $\triangle z_{T+t}=0$ for other t such that $n+1\leqslant t\leqslant 147$.

Proof According to Proposition 8,

$$(\triangle z_{T+n+1}, \triangle z_{T+n+2}, \cdots, \triangle z_{T+147})=$$
$$(\triangle u_{T+n+1}, \triangle u_{T+n+2}, \cdots, \triangle u_{T+147})+(\triangle v_{T+n+1}, \triangle v_{T+n+2}, \cdots, \triangle v_{T+147}).$$

Because

$$(\triangle v_{T+109}, \triangle v_{T+110}, \cdots, \triangle v_{T+n+111}) =(0, 0, \cdots, 0),$$
$$(\triangle z_{T+109}, \triangle z_{T+110}, \cdots, \triangle z_{T+n+111})=(\triangle u_{T+109}, \triangle u_{T+110}, \cdots, \triangle u_{T+n+111}).$$

Again because

$$(\triangle z_{T+109}, \triangle z_{T+110}, \cdots, \triangle z_{T+n+111})=(0, 0, \cdots, 0),$$
$$(\triangle u_{T+109}, \triangle u_{T+110}, \cdots, \triangle u_{T+n+111})=(0, 0, \cdots, 0).$$

So that $(\triangle u_{T+n+1}, \triangle u_{T+n+2}, \cdots, \triangle u_{T+147})$ is a 0 string, and that

$$(\triangle z_{T+n+1}, \triangle z_{T+n+2}, \cdots, \triangle z_{T+147})=(\triangle v_{T+n+1}, \triangle v_{T+n+2}, \cdots, \triangle v_{T+147}).$$

Notice that $(\triangle v_{T+m+63}, \triangle v_{T+m+64}, \cdots, \triangle v_{T+n+63})=(1, *\cdots*, 1)$ for $m\leqslant n\leqslant 7$. Again notice that $(\triangle z_{T+63}, \triangle z_{T+64}, \triangle z_{T+65}, \triangle z_{T+66})=(0, 0, 0, 0)$. So that $4\leqslant m\leqslant n\leqslant 7$. By Proposition 8, Lemma 4 is proved.

Proposition 14 Suppose $(\triangle z_{T+140}, \triangle z_{T+141}, \cdots, \triangle z_{T+147})\neq(0, 0, \cdots, 0)$, so that the case is from $\{70\leqslant P_L\leqslant 93, 163\leqslant P_L\leqslant 171\}$.

(1) If $\triangle z_T\triangle z_{T+1}\triangle z_{T+2}\cdots\triangle z_{T+147}$ does not possess the features of case $70\leqslant P_L\leqslant 93$, the case is $163\leqslant P_L\leqslant 171$.

(2) If $\triangle z_T\triangle z_{T+1}\triangle z_{T+2}\cdots\triangle z_{T+147}$ possesses the features of the $70\leqslant P_L\leqslant 93$, and at least one of the features of Lemma 4 does not hold, the case is $70\leqslant P_L\leqslant 93$.

(3) If $\triangle z_T\triangle z_{T+1}\triangle z_{T+2}\cdots\triangle z_{T+147}$ possesses features of the case $70\leqslant P_L\leqslant 93$, and all features of Lemma 4 hold, we can not check which case is from $\{70\leqslant P_L\leqslant 93, 163\leqslant P_L\leqslant 171\}$. But the state differential at time $T+n+1$ can be uniquely determind as the follow: $(\triangle s_{(T+n+1, 100)}, \triangle s_{(T+n+1, 101)}, \cdots, \triangle s_{(T+n+1, 100-m+n)})=(\triangle z_{63+n}, \triangle z_{62+n}, \cdots, \triangle z_{63+m})=(1, *, \cdots*, 1)$, $\triangle s_{(T+n+1, j)}=0$ for other j.

Proof (1) and (2) of Proposition 14 are clear.

Suppose the case is $163\leqslant P_L\leqslant 171$, $\triangle z_T\triangle z_{T+1}\triangle z_{T+2}\cdots\triangle z_{T+147}$ possesses features of the case $70\leqslant P_L\leqslant 93$, and all features of Lemma 4 hold. Then the state differential at time $T+n+1$ is the follow: $(\triangle s_{(T+n+1, 100)}, \triangle s_{(T+n+1, 101)}, \cdots, \triangle s_{(T+n+1, 100-m+n)})=(\triangle z_{63+n}, \triangle z_{62+n}, \cdots, \triangle z_{63+m})=(1,$

, …, 1), $\triangle s_{(T+n+1, j)}=0$ for other j.

Again suppose the case is $70\leqslant P_L\leqslant 93$, and all features of Lemma 4 hold. Then the state differential at time $T+n+1$ can be determined, as the follow: $(\triangle s_{(T+n+1, 94)}, \triangle s_{(T+n+1, 95)}, \cdots, \triangle s_{(T+n+1, 96+n)})=(\triangle z_{69+n}, \triangle z_{68+n}, \cdots, \triangle z_{67})$, $\triangle s_{(T+n+1, j)}=0$ for other j. On the other hand, Lemma 4 tells us $(\triangle z_{69+n}, \triangle z_{68+n}, \cdots, \triangle z_{64+n})=(0, 0, \cdots, 0)$, $(\triangle z_{63+n}, \triangle z_{62+n}, \cdots, \triangle z_{63+m})=(1, *, \cdots *, 1)$, $(\triangle z_{62+m}, \triangle z_{61+m}, \cdots, \triangle z_{67})=(0, 0, \cdots, 0)$.

Proposition 14 is proved.

3.4 Summarization for Case Checking

Subsection 3.3 presents a complete checking routine for determining the case. If the case is determined, either the injecting time and fault positions are determined, or the state differential at time T is determined. The unique circumstance in which the case can not be determind is Proposition 14 (3). In this circumstance the state differential at time $T+n+1$ is determined. Each result of subsection 3.3 is sufficient for floating attack, except Injection Failure.

On the other hand, Injection Failure occurs with a small probability about 1/256.

4 Floating Fault Analysis Under Our Assumptions

4.1 Preparing for Floating

Michal Hojsik and Bohuslav Rudolf presented an effective attack to Trivium, named floating fault analysis. The idea of this attack is to find an appropriate time. At this time, the state differential is heavy enough (from point of Hamming weight) and even enough (from point of distribution). Generally speaking, the heavier and the more even the state differential is, the more additional equations will be linear equations, from 82 original quadratic equations. At fault injection time M, the state differential is only distributed within an 8 bits area. So that it needs to float the state differential. The weakness of Trivium makes such floating possible. Michal Hojsik and Bohuslav presented an algorithm for floating. The input of this algorithm is the follow.

- The two key-stream segments $(z_0z_1z_2\cdots z_N)$ and $(z_0'z_1'z_2'\cdots z_N')$.
- $(\triangle s_{(i, 1)}, \cdots, \triangle s_{(i, 288)})$, for each $i\in\{0, 1, \cdots, t\}$, where t is an integer, $t\geqslant 3$.
- $\{\triangle(s_{(i, 91)}s_{(i, 92)}), \triangle(s_{(i, 175)}s_{(i, 176)}), \triangle(s_{(i, 286)}s_{(i, 287)})\}$, for each $i\in\{0, 1, \cdots, t\text{-}1\}$.

The process of this algorithm is the follow.

Step 1: try to compute $\{\triangle(s_{(t, 91)}s_{(t, 92)}),\triangle(s_{(t, 175)}s_{(t, 176)}), \triangle(s_{(t, 286)}s_{(t, 287)})\}$.

Step 2: compute $(\triangle s_{(t+1, 1)}, \cdots, \triangle s_{(t+1, 288)})$.

It is said that the state differential is floatable at time t, if the algorithm can succeed. We know that Step 2 is immediate from the Step 1, by considering subsection 2.3. Step 1 is a computation which includes many cases, and needs many skills. For the sake of the simplicity of our analysis, we present two conditions, described in the following Lemma 5. The combination of these two conditions is sufficient for the floatablility.

Lemma 5 The state differential is floatable at time t, if each of the following two conditions holds.

(1) $(\triangle s_{(t,286)}, \triangle s_{(t,287)})=(0, 0)$ or $(\triangle s_{(t,175)}, \triangle s_{(t,176)})=(0, 0)$.

(2) $(\triangle s_{(t,91)}, \triangle s_{(t,92)})=(0, 0)$

or $(\triangle s_{(t,172)}, \triangle s_{(t,173)}, \triangle s_{(t,283)}, \triangle s_{(t,284)})=(0, 0, 0, 0)$

or $(\triangle s_{(t,76)}, \triangle s_{(t,77)}, \triangle s_{(t,157)}, \triangle s_{(t,158)}, \triangle s_{(t,268)}, \triangle s_{(t,269)})=(0, 0, 0, 0, 0, 0)$.

Proof Lemma 5 is clear by considering equation (66), equation (69) and equation (84) of Appendix A.

We call j the floating end, if j is the smallest t such that, at time t, the two conditions of Lemma 5 can not be assured. In fact, the state differential may still be floatable at or beyond the floating end, but it is much more complicated to analyze such floatability.

In next subsections we will make floating. Here are our assumptions. At each time, the state is uniformly distributed. At time M, random faults appear in the positions $\{m, m+1, \cdots, m+7\}$, where m is uniformly distributed in the set $\{1, 2, \cdots, 86\}\cup\{94, 95, \cdots, 170\}\cup\{178, 179, \cdots, 281\}$. At each of 8 positions$\{m, m+1, \cdots, m+7\}$, the fault value is uniformly distributed between 1 and 0. Faults at different positions are independent with each other. So that the average weight of the faults is 4.

Faults shift rightward as 3 NFSRs drive. When faults pass across the positions {66, 69, 91, 92, 93, 162, 171, 175, 176, 177, 243, 264, 286, 287, 288}, they are diffused to the positions {1, 94, 178}. 6 positions {66, 69, 162, 171, 243, 264} are simple positions because, when faults pass across them, these faults are directly diffused to the positions {1, 94, 178}. 9 positions {91, 92, 93, 175, 176, 177, 286, 287, 288} are key positions because, when faults pass across them, diffusion features are more complicated. Lemma 6 and Lemma 7 present diffusion features at these positions.

Lemma 6 Take n as a non-negative integer. Suppose that, at time t, the state differential possesses the following feature.

- At positions $\{91-n, 92-n, \cdots, 91\}$, the values are $\{X_{91-n}, X_{92-n}, \cdots, X_{91}\}$, where $\{X_{91-n}, X_{92-n}, \cdots, X_{91}\}$ are uniformly distributed, and independent with each other.
- At each position from $\{92, 93\}\cup\{64-n, 65-n,\cdots, 66\}\cup\{169-n, 170-n, \cdots, 171\}$, the value is 0.

$\{Y_{173-n}, Y_{174-n}, \cdots, Y_{175}\}$ denotes the state differential values at time $t+n+3$ and positions $\{94, 95, \cdots, 96+n\}$. Then

- Y_{175} has a biased distribution, taking 1 with the probability 0.25.
- Y_{174} has a biased distribution, taking 1 with the probability 0.375.
- $\{Y_{173-n}, Y_{174-n}, \cdots, Y_{173}\}$ are uniformly distributed and independent with each other.

Lemma 7 Take m as a non-negative integer, $m\leqslant n$. As a result of Lemma 6, at time $t+82$ and positions $\{173-m, 174-m, \cdots, 175\}$, the state differential values are such $\{Y_{173-m}, Y_{174-m}, \cdots, Y_{175}\}$. Suppose that, at time $t+82$, the state differential possesses the following feature.

- At each position from $\{176, 177\}\cup\{158-m, 159-m,\cdots, 162\}\cup\{260-m, 261-m, \cdots, 264\}$, the value is 0.

$\{Z_{282-m}, Z_{283-m}, \cdots, Z_{286}\}$ denotes the state differential values at time $t+m+87$ and positions $\{178, 179, \cdots, 182+m\}$. Then

- Z_{286} has a biased distribution, taking 1 with the probability 0.125.
- Z_{285} has a biased distribution, taking 1 with the probability 0.25.
- Z_{284} has a biased distribution, taking 1 with the probability 0.375.
- Z_{283} has a biased distribution, taking 1 with the probability 0.453125.
- $\{Z_{282-m}, Z_{283-m}, \cdots, Z_{282}\}$ are uniformly distributed and independent with each other.

Lemma 6 and Lemma 7 are easy to be verified by simple search. They describe such shift: faults firstly pass across the positions {91, 92, 93}, and secondly {175, 176, 177}. They imply some increase of average Hamming weight of differential. Symmetrical conclusion keeps true if we consider such shift: faults firstly pass across the positions {175, 176, 177}, and secondly {286, 287, 288}. Another symmetrical conclusion keeps true if we consider such shift: faults firstly pass across the positions {286, 287, 288}, and secondly {91, 92, 93}.

4.2 Floating Analysis for Case $1\leqslant P_L\leqslant 66$

In case $1\leqslant P_L\leqslant 66$, the floating end is about $T+163$. Let $(u_1, u_2, \cdots, u_{288})$ denote the state differential at the floating end. Then the major features of $(u_1, u_2, \cdots, u_{288})$ are the follow.

- Each of 141 entries $\{u_4\text{~}u_5, u_{29}\text{~}u_{83}, u_{92}\text{~}u_{93}, u_{101}, u_{110}, u_{119}\text{~}u_{143}, u_{163}\text{~}u_{170}, u_{194}, u_{203}\text{~}u_{221}, u_{234}\text{~}u_{236}, u_{247}\text{~}u_{248}, u_{259}\text{~}u_{263}, u_{272}\text{~}u_{288}\}$ is 0.
- Entry u_{233} takes 1 with the probability 0.125.
- Each of 5 entries $\{u_3, u_{162}, u_{232}, u_{246}, u_{258}\}$ takes 1 with the probability 0.25.
- Each of 7 entries $\{u_2, u_{14}, u_{152}, u_{161}, u_{231}, u_{245}, u_{257}\}$ takes 1 with the probability 0.375.
- Entry u_{230} takes 1 with the probability 0.453125.
- Each of other 133 entries is uniformly distributed. (But these 133 entries are not independent with each other)
- From these 133 entries, $\{u_{84}, u_{85}, \cdots, u_{91}\}$ are independent with each other.
- From these 133 entries, $(u_{84}, u_{85}, \cdots, u_{91})=(u_{102}, u_{103}, \cdots, u_{109})=(u_{111}, u_{112}, \cdots, u_{118})=(u_{195}, u_{196}, \cdots, u_{202})=(u_{264}, u_{265}, \cdots, u_{271})$.
- From these 133 entries, $(u_{85}, u_{86}, \cdots, u_{91})=(u_{16}, u_{17}, \cdots, u_{22})=(u_{94}, u_{95}, \cdots, u_{100})$.
- From these 133 entries, $(u_{86}, u_{87}, \cdots, u_{91})=(u_{23}, u_{24}, \cdots, u_{28})$.
- From these 133 entries, $(u_{88}, u_{89}, u_{90}, u_{91})=(u_{190}, u_{191}, u_{192}, u_{193})$.
- From these 133 entries, $(u_{84}, u_{85}, \cdots, u_{90})=(u_{171}, u_{172}, \cdots, u_{177})$.
- From these 133 entries, $(u_{144}, u_{145}, \cdots, u_{151})=(u_{237}, u_{238}, \cdots, u_{244})$.
- Average differential Hamming weights of 3 NFSRs are respectively 17.5, 24.5 and 30.453125.

By equation (66) of Appendix A, the additional equation is a linear equation (other than an identity) with the probability 0.75. Similarly by equation (67) of Appendix A, the additional equation is a linear equation (other than an identity) with the probability 0.75, etc. Table 3 presents each probability, with which the additional equation is a linear equation (other than an identity) by original quadratic equation. According to Appendix A, original quadratic equations are equation (66), equation (67), $\cdots$, equation (147). In Table 3, "Rank i" denotes equation (i) of Appendix A, i

∈{66, 67, ⋯, 147}, “Prob.” denotes corresponding probability with which the additional equation is a linear equation. Most probabilities in Table 3 are exact. A small number of these probabilities are conservative estimations, because we are not very clear what detailed correlation is between some entries of the state differential.

Table 3. The probability with which the additional equation is a linear equation

Rank	66	67	68	69	70	71	72	73	74	75
Prob.	0.75	0.75	0.75	0.875	0.938	0.875	0.75	0.75	0.75	0.75
Rank	76	77	78	79	80	81	82	83	84	85
Prob.	0.75	0.5	0	0.25	0.531	0.844	0.938	0.938	0.969	0.984
Rank	86	87	88	89	90	91	92	93	94	95
Prob.	0.984	0.984	0.984	0.938	0.922	0.938	0.875	0.75	0.875	0.938
Rank	96	97	98	99	100	101	102	103	104	105
Prob.	0.938	0.938	0.875	0.75	0.75	0.75	0.75	0.75	0.5	0
Rank	106	107	108	109	110	111	112	113	114	115
Prob.	0.25	0.531	0.844	0.938	0.938	0.984	0.984	0.984	0.984	0.984
Rank	116	117	118	119	120	121	122	123	124	125
Prob.	0.875	0	0	0.125	0.344	0.648	0.839	0.957	0.984	0.984
Rank	126	127	128	129	130	131	132	133	134	135
Prob.	0.984	0.984	0.984	0.984	0.984	0.969	0.969	0.984	0.984	0.984
Rank	136	137	138	139	140	141	142	143	144	145
Prob.	0.984	0.984	0.996	0.996	0.996	0.992	0.996	0.992	0.938	0.953
Rank	146	147								
Prob.	0.968	0.984								

According to Table 3 we can induce that, from 82 original quadratic equations, the attacker averagely obtains 66.6 additional equations, which are linear equations (other than identities).

4.3 Floating Analysis for Other 8 Cases

By the same procedure with subsection 4.2, we can obtain floating features in other 8 cases. In this subsection we omit the detailed discussion, and only present major results.

In case $94 \leqslant P_L \leqslant 162$, the floating end is about T+169. From 82 original quadratic equations, the attacker averagely obtains 70.6 additional equations which are linear equations.

In case $178 \leqslant P_L \leqslant 243$, the floating end is about T+134. From 82 original quadratic equations, the attacker averagely obtains 62.9 additional equations which are linear equations.

In case $70 \leqslant P_L \leqslant 93$, the floating end is about T+236. From 82 original quadratic equations, the attacker averagely obtains 74.9 additional equations which are linear equations.

In case $172 \leqslant P_L \leqslant 177$, the floating end is about T+198. Notice P_H-$P_L \leqslant 6$ in this case. So that, at the floating end, the differential is more sparsely distributed. From 82 original quadratic equations, the attacker averagely obtains 54.1 additional equations which are linear equations.

In case $265 \leqslant P_L \leqslant 288$, the floating end is about T+227. From 82 original quadratic equations, the attacker averagely obtains 72.9 additional equations which are linear equations.

In case $244 \leqslant P_L \leqslant 264$, the floating end is about T+195. From 82 original quadratic equations, the attacker averagely obtains 70.6 additional equations which are linear equations.

In case $163 \leqslant P_L \leqslant 171$, the floating end is about T+161. The analysis is much more complicated than other cases. We can still estimate that averagely no less than 50 additional equations are linear equations, from 82 original quadratic equations.

Case $67 \leqslant P_L \leqslant 69$ is another complicated case. We can only estimate that the floating end is not smaller than T+130, and that averagely no less than 40 additional equations are linear equations, from 82 original quadratic equations. Notice that the probability of this case is about 3/280, so that it can be neglected.

4.4 Summarization and Notes for Floating Analysis

From the discussion in last subsections we have the following result. At the floating end, averagely no less than 67.167 additional equations are linear equations, from 82 original quadratic equations. This result is quite satisfactory for the attacker.

These additional linear equations have a side function. Notice that 82 original quadratic equations are pair quadratic equations, and pair quadratic terms are sparsely distributed. 67.167 additional linear equations may combine with 66 original linear equations, to solve some bits of the state, so that some pair quadratic terms are changed into linear terms. This side function is helpful for Guess-and-Determine attack (see [15]).

There are 66 original equations which are cubic equations, and are not included in Appendix A. We call these equations equation (148), equation (149), ⋯, equation (213), respectively. From each of these 66 original cubic equations, the additional equation is almost certainly a quadratic equation (neither a linear equation nor an identity). In other words, almost 66 additional quadratic equations are obtained from 66 original cubic equations, at the floating end. It is hard to evaluate the power of these additional quadratic equations for breaking Trivium. If an additional quadratic equation is a pair quadratic equation, it is quite useful for Guess-and-Determine attack (see [15]).

5 A Comparison between Michal Hojsik's Model and Ours

5.1 Result and Guess of Michal Hojsik and Bohuslav

Besides their Assumption 1.1 and Assumption 1.2, Michal Hojsik and Bohuslav Rudolf [14, 15] allowed repeated fault injections. They had Assumption 1.3, as the follow.

Assumption 1.3 The attacker can make such fault injection many times for the same initial state.

Michal Hojsik and Bohuslav Rudolf then presented their result [15] under Assumption 1.1, Assumption 1.2 and Assumption 1.3. Averagely 3.2 fault injections will break Trivium, by using averagely 800×4.2 key-stream bits (they said they use averagely 800 original key-stream bits, so that they use averagely 800×3.2 fault-injected key-stream bits). They guessed [14] the attak would be more effective if one-bit-fault-injection could be changed as multi-bit-fault-injection (that is, Assumption 1.2 could be changed, for example, as Assumption 2.2).

5.2 Our Modified Model and Result

To compare Hojsik's model and ours, we must make some modification to our model. Assumption 1.3 is needed, that is, injection/floating procedure can be repeated. For different fault injections, we hope to solve the state at same time, other than to solve the states at various floating ends. By this reason, faults must be injected into initial state, and that floating must be started from the initial time. So that Assumption 1.1 is needed, other than Assumption 2.1. In a word, we make injection and floating under Assumption 1.1, Assumption 2.2 and Assumption 1.3. We try to solve the state at such time that is the minimal value of various floating ends.

Suppose the case is $1 \leqslant P_L \leqslant 66$. By subsection 4.2 we know that the floating end is about T+163. Now we can estimate the probabilistic distribution of T. T takes values from {0, 1, ⋯, 65}. T takes values from {0, 1, ⋯, 8} with descending probabilities. T takes any value from {8, 9, ⋯, 58} with the same probability. T takes values from {58, 59, ⋯, 65} with descending probabilities. A simple and approximate description is that T tends to be uniformly distributed in {0, 1, ⋯, 65}. So that the floating end tends to be uniformly distributed in {163, 164, ⋯, 228}.

Similarly, if the case is $94 \leqslant P_L \leqslant 162$, the floating end tends to be uniformly distributed in {169, 170, ⋯, 237}, ect. Lemma 8 presents approximately probabilistic distribution of the floating end in each of 9 cases, and presents the probability of each case.

Lemma 8 Let *end* denote the floating end.

(1) In case $1 \leqslant P_L \leqslant 66$, *end* tends to be uniformly distributed in {163, 164, ⋯, 228}. The probability of case $1 \leqslant P_L \leqslant 66$ tends to be 66/288.

(2) In case $94 \leqslant P_L \leqslant 162$, *end* tends to be uniformly distributed in {169, 170, ⋯, 237}. The probability of case $94 \leqslant P_L \leqslant 162$ tends to be 69/288.

(3) In case $178 \leqslant P_L \leqslant 243$, *end* tends to be uniformly distributed in {134, 135, ⋯, 199}. The probability of case $178 \leqslant P_L \leqslant 243$ tends to be 66/288.

(4) In case $70 \leqslant P_L \leqslant 93$, *end* tends to be uniformly distributed in {236, 237, ⋯, 259}. The probability of case $70 \leqslant P_L \leqslant 93$ tends to be 24/288.

(5) In case $172 \leqslant P_L \leqslant 177$, *end* has a biased distribution in {198, 199, ⋯, 203}, with descending probabilities. The probability of case $172 \leqslant P_L \leqslant 177$ tends to be 6/288.

(6) In case $265 \leqslant P_L \leqslant 288$, *end* tends to be uniformly distributed in {227, 228, ⋯, 250}. The probability of case $265 \leqslant P_L \leqslant 288$ tends to be 24/288.

(7) In case $67 \leqslant P_L \leqslant 69$, the distribution of *end* is complicated, but the probability of case $67 \leqslant P_L \leqslant 69$ is 3/288.

(8) In case $163 \leqslant P_L \leqslant 171$, *end* has a biased distribution in {161, 162, ⋯, 169}, with descending probabilities. The probability of case $172 \leqslant P_L \leqslant 177$ tends to be 9/288.

(9) In case $244 \leqslant P_L \leqslant 264$, *end* tends to be uniformly distributed in {195, 196, ⋯, 215}. The probability of case $244 \leqslant P_L \leqslant 264$ tends to be 21/288.

Lemma 8 implies that the expectation of the *end* is about 195. Now suppose that the injection/floating procedure is repeated 4 times, with the floating ends end_1, end_2, end_3 and end_4 respectively. Each of $\{end_1, end_2, end_3, end_4\}$ has an appropriate distribution as described in Lemma 8, and $\{end_1, end_2, end_3, end_4\}$ are independent each other. We try to solve the state at the time $min\{end_1, end_2, end_3, end_4\}$. It is easy to compute that the expectation of $min\{end_1, end_2, end_3, end_4\}$ is about 163.

For an injection/floating procedure, we consider the state at time 163. Let L denote the number of additional linear equations, about the state at time 163, obtained from 82 original quadratic equations. In the follow we list our analyzing results about L in 9 cases.

(1) In case $1\leqslant P_L\leqslant 66$, the average value of L is no less than 56.

(2) In case $94\leqslant P_L\leqslant 162$, the average value of L is no less than 59.

(3) In case $178\leqslant P_L\leqslant 243$, the average value of L is no less than 51.

(4) In case $70\leqslant P_L\leqslant 93$, the average value of L is no less than 63.

(5) In case $172\leqslant P_L\leqslant 177$, the average value of L is no less than 43.

(6) In case $265\leqslant P_L\leqslant 288$, the average value of L is no less than 61.

(7) In case $67\leqslant P_L\leqslant 69$, the average value of L is no less than 30.

(8) In case $163\leqslant P_L\leqslant 171$, the average value of L is no less than 40.

(9) In case $244\leqslant P_L\leqslant 264$, the average value of L is no less than 60.

In fact, these results are quite conservative from our analysis.

Then it is easy to compute that averagely no less than 55.823 additional equations are linear equations, about the state at time 163, obtained from 82 original quadratic equations. If injection/floating procedure is repeated 4 times, averagely no less than $55.823\times 4=223.292$ additional equations are linear equations, from 82 original quadratic equations. By considering 66 original linear equations, averagely no less than 289.292 linear equations, about the state at time 163, are obtained. There is a rank reduction in 289.292 linear equations, but these linear equations are enough for breaking Trivium, by careful soving skill, a small number of guesses, and a large number of pair quadratic equations (original and additional).

For obtaining $min\{end_1, end_2, end_3, end_4\}$, we must obtain $\{end_1, end_2, end_3, end_4\}$. So that, for each injection/floating procedure, the floating should be stoped at the same time $max\{end_1, end_2, end_3, end_4\}$. It is easy to compute that the expectation of $max\{end_1, end_2, end_3, end_4\}$ is about 227. This implies that 4 injection/floating procedures should be stoped at a same time, which is averagely 227. In other words, we need averagely 227×5 key-stream bits to obtain $min\{end_1, end_2, end_3, end_4\}$.

5.3 Comparison of Results and Notes

Under the model of Michal Hojsik and Bohuslav Rudolf, averagely 3.2 fault injections and averagely 800×4.2 key-stream bits will break Trivium. Under our modified model, averagely 4 fault injections and averagely 227×5 key-stream bits will break Trivium. From these comparison results, we can say that our modified model is similarly effective with the model of Michal Hojsik and Bohuslav Rudolf, for the floating attack.

Against their guess, our modified model is not more effective than the model of Michal Hojsik and Bohuslav Rudolf, for the floating attack. The follows are several reasons for that.

Our floating end is defined as “the smallest time when the two conditions of Lemma 5 can not be assured”, other than “the smallest time when the two conditions of Lemma 5 do not hold”. In fact, even in the circumstance “the two conditions of Lemma 5 do not hold”, there are some other methods for floatability. Our conservative definition reduces the difficulty of our analysis, but makes our modified model less effective.

In their model, Michal Hojsik and Bohuslav Rudolf seemed to make full use of skills for solving equations. We are not interested in how to solve the equations, and only try to obtain enough equations, especially linear equations. Therefore we can not present better result.

Multi-bit-fault-injection is never more effective than one-bit-fault-injection for floating attack. We find that, if the Hamming weight of the state differential is larger than 288/3, it is quite possible that the float has to be stoped soon. Therefore multi-bit-fault-injection can not generate more linear equations than one-bit-fault-injection. It can only reduce the number of needed key-stream bits.

6 Future Work

Trivium will lead us to continue our work. The first future work is the fault injection in larger scale. Advances in micro-electronics make the components smaller, so that fault positions should be in a larger scale. We find that, if the fault positions are from the area within 15 neighboring bits, a modified checking method will be valid. But the fault floating analysis seems more complicated.

The second future work is the combination of fault floating analysis and power analysis. A simple example will illustrate the function of such combination. Suppose that, after injection, the bit at position j is changed. Suppose $\{j-1, j, j+1\}\cap\{66, 69, 91, 92, 93, 162, 171, 175, 176, 177, 243, 264, 286, 287, 288\}=\Phi$ (the empty set). If the power consumed for the state renewal is larger, the bits at the positions j-1 and j+1 are equal to original bit at position j. If this power is smaller, the bits at the positions j-1 and j+1 are different with original bit at position j. If this power is equall, the bit at one position from $\{j-1, j+1\}$ is different with original bit at position j, and at another position is equal to original bit at position j.

The third future work is hard fault injection, that is, after the fault injection, bits at some positions of the state will be permanently 1 or 0. Hard fault injection may be considered a great reduction to the cipher, but there are still some problems, for example, how to determine the fault positions.

Acknowledgement

References

1. C. De Cannière, B. Preneel. Trivium: a stream cipher construction inspired by block cipher design principle. eSTREAM, ECRYPT Stream Cipher Project, Report 2005/30 (2005), http://www.ecrypt.eu.org/stream
2. C.De Cannière and Bart Preneel. Trivium Specifications.www.ecrypt.eu.org/stream/p3ciphers/trivium/trivium_p3.pdf
3. H. Raddum. Cryptanalytic results on Trivium. eSTREAM, ECRYPT Stream Cipher Project, Report 2006/039 (2006), http://www.ecrypt.eu.org/stream
4. A. Maximov, A. Biryukov. Two trivial attacks on Trivium. eSTREAM, ECRYPT Stream Cipher Project, Report 2007/006 (2007), http://www.ecrypt.eu.org/stream
5. S. Babbage. Some thoughts on Trivium. eSTREAM, ECRYPT Stream Cipher Project, Report 2007/007 (2007), http://www.ecrypt.eu.org/stream
6. M.S. Turan, O. Kara. Linear approximations for 2-round Trivium. eSTREAM, ECRYPT Stream Cipher Project, Report 2007/008 (2007), http://www.ecrypt.eu.org/stream
7. D. Hwang, et al. Comparison of FPGA – targeted hardware implementations of eSTREAM stream cipher candidates. In: SASC 2008 – The State of the Art of Stream Ciphers, Workshop Record, pp. 151-162 (2008), http://www.ecrypt.eu.org/stream
8. T. Good, M. Benaissa. Hardware performance of eSTREAM phase-III stream cipher candidates. In: SASC 2008 – The State of the Art of Stream Ciphers, Workshop Record, pp. 163-174 (2008), http://www.ecrypt.eu.org/stream
9. E. Biham, O. Dunkelman. Differential cryptanalysis in stream ciphers. COSIC internal report (2007)
10. C. Rechberger, E. Oswald. Stream ciphers and side-channel analysis. In: SASC 2004 – The State of the Art of Stream Ciphers, Workshop Record, pp. 320-326 (2004), http://www.ecrypt.eu.org/stream
11. W. Fisher, B.M. Gammel, O. Kniffler, J. Velten. Differential power analysis of stream ciphers. eSTREAM, ECRYPT Stream Cipher Project, Report 2007/014 (2007), http://www.ecrypt.eu.org/stream
12. J.J. Hoch, A. Shamir. Fault analysis of stream ciphers. In: M. Joye, J.-J. Quisquater (eds.) CHES 2004. LNCS, vol. 3156, pp. 240-253. Springer, Heidelberg (2004)
13. E. Biham, L. Granboulan, P. Nguyen. Impossible fault analysis of RC4 and differential fault analysis of RC4. In: SASC 2004 – The State of the Art of Stream Ciphers, Workshop Record, pp. 147-155 (2004), http://www.ecrypt.eu.org/stream
14. B. Gierlichs, et al. Susceptibility of eSTREAM candidates towards side channel analysis. In: SASC 2008 – The State of the Art of Stream Ciphers, Workshop Record, pp. 123-150 (2008), http://www.ecrypt.eu.org/stream
15. S. Fisher, S. Khazaei, W. Meier. Chosen IV statistical analysis for key recovery attacks on stream cipher. In: SASC 2008 – The State of the Art of Stream Ciphers, Workshop Record, pp. 31-41 (2008), http://www.ecrypt.eu.org/stream
16. M. Hojsik, B. Rudolf. Differential fault analysis of Trivium. In: K. Nyberg (ed.) FSE 2008. LNCS, vol. 5086, pp. 158-172. Springer, Heidelberg (2008)
17. M. Hojsik, B. Rudolf. Floating fault analysis of Trivium. In: D.R. Chowdhury, V. Rijmen, and A. Das (eds.) INDOCRYPT 2008. LNCS, vol. 5365, pp. 239-250, Springer, Heidelberg (2008)

18. Deik Priemuth-schmid, Alex Biryukov. Slid pairs in salsa20 and Trivium. In Proceedings of the 9th International Conference on Cryptology in India: Progress in Cryptology. LNCS 5365, pp.1-14, Springer, Heidelberg (2008).
19. Enes Pasalic. Key differentiation attacks on stream ciphers. Cryptology ePrint Archive. http://eprint.iacr.org/2008/443.
20. Itai Dinur and Adi Shamir. Cube Attacks on Tweakable Black Box Polynomials. Cryptology ePrint Archive. 2008. http://eprint.iacr.org/2008/385.
21. S. S. Bedi and N. Rajesh Pillai. Cube Attacks on Trivium. Cryptology ePrint Archive. http://eprint.iacr.org/2009/015.

Appendix

Appendix A Trivium Original Equations

By the key-stream ($z_0z_1z_2\cdots$), the attacker can obtain the original equations of the initial state (s_1, $\cdots$, s_{288}), described as following.

$$z_0=s_{66}+s_{93}+s_{162}+s_{177}+s_{243}+s_{288} \tag{0}$$

$$z_1=s_{65}+s_{92}+s_{161}+s_{176}+s_{242}+s_{287} \tag{1}$$

$$\cdots \qquad \cdots$$

$$z_{65}=s_1+s_{28}+s_{97}+s_{112}+s_{178}+s_{223} \tag{65}$$

$$z_{66}=s_{27}+s_{69}+s_{96}+s_{111}+s_{162}+s_{175}s_{176}+s_{177}+s_{222}+s_{243}+s_{264}+s_{286}s_{287}+s_{288} \tag{66}$$

$$z_{67}=s_{26}+s_{68}+s_{95}+s_{110}+s_{161}+s_{174}s_{175}+s_{176}+s_{221}+s_{242}+s_{263}+s_{285}s_{286}+s_{287} \tag{67}$$

$$z_{68}=s_{25}+s_{67}+s_{94}+s_{109}+s_{160}+s_{173}s_{174}+s_{175}+s_{220}+s_{241}+s_{262}+s_{284}s_{285}+s_{286} \tag{68}$$

$$z_{69}=s_{24}+s_{91}s_{92}+s_{93}+s_{108}+s_{159}+s_{171}+s_{172}s_{173}+s_{174}+s_{219}+s_{240}+s_{261}+s_{283}s_{284}+s_{285} \tag{69}$$

$$z_{70}=s_{23}+s_{90}s_{91}+s_{92}+s_{107}+s_{158}+s_{170}+s_{171}s_{172}+s_{173}+s_{218}+s_{239}+s_{260}+s_{282}s_{283}+s_{284} \tag{70}$$

$$z_{71}=s_{22}+s_{89}s_{90}+s_{91}+s_{106}+s_{157}+s_{169}+s_{170}s_{171}+s_{172}+s_{217}+s_{238}+s_{259}+s_{281}s_{282}+s_{283} \tag{71}$$

$$z_{72}=s_{21}+s_{88}s_{89}+s_{90}+s_{105}+s_{156}+s_{168}+s_{169}s_{170}+s_{171}+s_{216}+s_{237}+s_{258}+s_{280}s_{281}+s_{282} \tag{72}$$

$$z_{73}=s_{20}+s_{87}s_{88}+s_{89}+s_{104}+s_{155}+s_{167}+s_{168}s_{169}+s_{170}+s_{215}+s_{236}+s_{257}+s_{279}s_{280}+s_{281} \tag{73}$$

$$z_{74}=s_{19}+s_{86}s_{87}+s_{88}+s_{103}+s_{154}+s_{166}+s_{167}s_{168}+s_{169}+s_{214}+s_{235}+s_{256}+s_{278}s_{279}+s_{280} \tag{74}$$

$$z_{75}=s_{18}+s_{85}s_{86}+s_{87}+s_{102}+s_{153}+s_{165}+s_{166}s_{167}+s_{168}+s_{213}+s_{234}+s_{255}+s_{277}s_{278}+s_{279} \tag{75}$$

$$z_{76}=s_{17}+s_{84}s_{85}+s_{86}+s_{101}+s_{152}+s_{164}+s_{165}s_{166}+s_{167}+s_{212}+s_{233}+s_{254}+s_{276}s_{277}+s_{278} \tag{76}$$

$$z_{77}=s_{16}+s_{83}s_{84}+s_{85}+s_{100}+s_{151}+s_{163}+s_{164}s_{165}+s_{166}+s_{211}+s_{232}+s_{253}+s_{275}s_{276}+s_{277} \tag{77}$$

$$z_{78}=s_{15}+s_{82}s_{83}+s_{84}+s_{99}+s_{150}+s_{162}+s_{163}s_{164}+s_{165}+s_{210}+s_{231}+s_{252}+s_{274}s_{275}+s_{276} \tag{78}$$

$$z_{79}=s_{14}+s_{81}s_{82}+s_{83}+s_{98}+s_{149}+s_{161}+s_{162}s_{163}+s_{164}+s_{209}+s_{230}+s_{251}+s_{273}s_{274}+s_{275} \tag{79}$$

$$z_{80}=s_{13}+s_{80}s_{81}+s_{82}+s_{97}+s_{148}+s_{160}+s_{161}s_{162}+s_{163}+s_{208}+s_{229}+s_{250}+s_{272}s_{273}+s_{274} \tag{80}$$

$$z_{81}=s_{12}+s_{79}s_{80}+s_{81}+s_{96}+s_{147}+s_{159}+s_{160}s_{161}+s_{162}+s_{207}+s_{228}+s_{249}+s_{271}s_{272}+s_{273} \tag{81}$$

$$z_{82}=s_{11}+s_{78}s_{79}+s_{80}+s_{95}+s_{146}+s_{158}+s_{159}s_{160}+s_{161}+s_{206}+s_{227}+s_{248}+s_{270}s_{271}+s_{272} \tag{82}$$

$$z_{83}=s_{10}+s_{77}s_{78}+s_{79}+s_{94}+s_{145}+s_{157}+s_{158}s_{159}+s_{160}+s_{205}+s_{226}+s_{247}+s_{269}s_{270}+s_{271} \tag{83}$$

$$z_{84}=s_{9}+s_{66}+s_{76}s_{77}+s_{78}+s_{91}s_{92}+s_{93}+s_{144}+s_{156}+s_{157}s_{158}+s_{159}+s_{171}+s_{204}+s_{225}+s_{246}+s_{268}s_{269}+s_{270} \tag{84}$$

$$z_{85}=s_{8}+s_{65}+s_{75}s_{76}+s_{77}+s_{90}s_{91}+s_{92}+s_{143}+s_{155}+s_{156}s_{157}+s_{158}+s_{170}+s_{203}+s_{224}+s_{245}+s_{267}s_{268}+s_{269} \tag{85}$$

$$z_{86}=s_{7}+s_{64}+s_{74}s_{75}+s_{76}+s_{89}s_{90}+s_{91}+s_{142}+s_{154}+s_{155}s_{156}+s_{157}+s_{169}+s_{202}+s_{223}+s_{244}+s_{266}s_{267}+s_{268} \tag{86}$$

$$z_{87}=s_{6}+s_{63}+s_{73}s_{74}+s_{75}+s_{88}s_{89}+s_{90}+s_{141}+s_{153}+s_{154}s_{155}+s_{156}+s_{168}+s_{201}+s_{222}+s_{243}+s_{265}s_{266}+s_{267} \tag{87}$$

$$z_{88}=s_{5}+s_{62}+s_{72}s_{73}+s_{74}+s_{87}s_{88}+s_{89}+s_{140}+s_{152}+s_{153}s_{154}+s_{155}+s_{167}+s_{200}+s_{221}+s_{242}+s_{264}s_{265}+s_{266} \tag{88}$$

$$z_{89}=s_{4}+s_{61}+s_{71}s_{72}+s_{73}+s_{86}s_{87}+s_{88}+s_{139}+s_{151}+s_{152}s_{153}+s_{154}+s_{166}+s_{199}+s_{220}+s_{241}+s_{263}s_{264}+s_{265} \tag{89}$$

$$z_{90}=s_{3}+s_{60}+s_{70}s_{71}+s_{72}+s_{85}s_{86}+s_{87}+s_{138}+s_{150}+s_{151}s_{152}+s_{153}+s_{165}+s_{198}+s_{219}+s_{240}+s_{262}s_{263}+s_{264} \tag{90}$$

$$z_{91}=s_{2}+s_{59}+s_{69}s_{70}+s_{71}+s_{84}s_{85}+s_{86}+s_{137}+s_{149}+s_{150}s_{151}+s_{152}+s_{164}+s_{197}+s_{218}+s_{239}+s_{261}s_{262}+s_{263} \tag{91}$$

$$z_{92}=s_{1}+s_{58}+s_{68}s_{69}+s_{70}+s_{83}s_{84}+s_{85}+s_{136}+s_{148}+s_{149}s_{150}+s_{151}+s_{163}+s_{196}+s_{217}+s_{238}+s_{260}s_{261}+s_{262} \tag{92}$$

$$\begin{aligned}z_{93}=&s_{57}+s_{67}s_{68}+s_{82}s_{83}+s_{84}+s_{135}+s_{147}+s_{148}s_{149}+s_{150}+s_{162}\\&+s_{195}+s_{216}+s_{237}+s_{243}+s_{259}s_{260}+s_{261}+s_{286}s_{287}+s_{288}\end{aligned} \tag{93}$$

$$\begin{aligned}z_{94}=&s_{56}+s_{66}s_{67}+s_{81}s_{82}+s_{83}+s_{134}+s_{146}+s_{147}s_{148}+s_{149}+s_{161}\\&+s_{194}+s_{215}+s_{236}+s_{242}+s_{258}s_{259}+s_{260}+s_{285}s_{286}+s_{287}\end{aligned} \tag{94}$$

$$\begin{aligned}z_{95}=&s_{55}+s_{65}s_{66}+s_{80}s_{81}+s_{82}+s_{133}+s_{145}+s_{146}s_{147}+s_{148}+s_{160}\\&+s_{193}+s_{214}+s_{235}+s_{241}+s_{257}s_{258}+s_{259}+s_{284}s_{285}+s_{286}\end{aligned} \tag{95}$$

$$\begin{aligned}z_{96}=&s_{54}+s_{64}s_{65}+s_{79}s_{80}+s_{81}+s_{132}+s_{144}+s_{145}s_{146}+s_{147}+s_{159}\\&+s_{192}+s_{213}+s_{234}+s_{240}+s_{256}s_{257}+s_{258}+s_{283}s_{284}+s_{285}\end{aligned} \tag{96}$$

$$\begin{aligned}z_{97}=&s_{53}+s_{63}s_{64}+s_{78}s_{79}+s_{80}+s_{131}+s_{143}+s_{144}s_{145}+s_{146}+s_{158}\\&+s_{191}+s_{212}+s_{233}+s_{239}+s_{255}s_{256}+s_{257}+s_{282}s_{283}+s_{284}\end{aligned} \tag{97}$$

$$\begin{aligned}z_{98}=&s_{52}+s_{62}s_{63}+s_{77}s_{78}+s_{79}+s_{130}+s_{142}+s_{143}s_{144}+s_{145}+s_{157}\\&+s_{190}+s_{211}+s_{232}+s_{238}+s_{254}s_{255}+s_{256}+s_{281}s_{282}+s_{283}\end{aligned} \tag{98}$$

$$\begin{aligned}z_{99}=&s_{51}+s_{61}s_{62}+s_{76}s_{77}+s_{78}+s_{129}+s_{141}+s_{142}s_{143}+s_{144}+s_{156}\\&+s_{189}+s_{210}+s_{231}+s_{237}+s_{253}s_{254}+s_{255}+s_{280}s_{281}+s_{282}\end{aligned} \tag{99}$$

$$\begin{aligned}z_{100}=&s_{50}+s_{60}s_{61}+s_{75}s_{76}+s_{77}+s_{128}+s_{140}+s_{141}s_{142}+s_{143}+s_{155}\\&+s_{188}+s_{209}+s_{230}+s_{236}+s_{252}s_{253}+s_{254}+s_{279}s_{280}+s_{281}\end{aligned} \tag{100}$$

$$\begin{aligned}z_{101}=&s_{49}+s_{59}s_{60}+s_{74}s_{75}+s_{76}+s_{127}+s_{139}+s_{140}s_{141}+s_{142}+s_{154}\\&+s_{187}+s_{208}+s_{229}+s_{235}+s_{251}s_{252}+s_{253}+s_{278}s_{279}+s_{280}\end{aligned} \tag{101}$$

$$\begin{aligned}z_{102}=&s_{48}+s_{58}s_{59}+s_{73}s_{74}+s_{75}+s_{126}+s_{138}+s_{139}s_{140}+s_{141}+s_{153}\\&+s_{186}+s_{207}+s_{228}+s_{234}+s_{250}s_{251}+s_{252}+s_{277}s_{278}+s_{279}\end{aligned} \tag{102}$$

$$\begin{aligned}z_{103}=&s_{47}+s_{57}s_{58}+s_{72}s_{73}+s_{74}+s_{125}+s_{137}+s_{138}s_{139}+s_{140}+s_{152}\\&+s_{185}+s_{206}+s_{227}+s_{233}+s_{249}s_{250}+s_{251}+s_{276}s_{277}+s_{278}\end{aligned} \tag{103}$$

$$\begin{aligned}z_{104}=&s_{46}+s_{56}s_{57}+s_{71}s_{72}+s_{73}+s_{124}+s_{136}+s_{137}s_{138}+s_{139}+s_{151}\\&+s_{184}+s_{205}+s_{226}+s_{232}+s_{248}s_{249}+s_{250}+s_{275}s_{276}+s_{277}\end{aligned} \tag{104}$$

$$\begin{aligned}z_{105}=&s_{45}+s_{55}s_{56}+s_{70}s_{71}+s_{72}+s_{123}+s_{135}+s_{136}s_{137}+s_{138}+s_{150}\\&+s_{183}+s_{204}+s_{225}+s_{231}+s_{247}s_{248}+s_{249}+s_{274}s_{275}+s_{276}\end{aligned} \tag{105}$$

$$\begin{aligned}z_{106}=&s_{44}+s_{54}s_{55}+s_{69}s_{70}+s_{71}+s_{122}+s_{134}+s_{135}s_{136}+s_{137}+s_{149}\\&+s_{182}+s_{203}+s_{224}+s_{230}+s_{246}s_{247}+s_{248}+s_{273}s_{274}+s_{275}\end{aligned} \tag{106}$$

$$\begin{aligned}z_{107}=&s_{43}+s_{53}s_{54}+s_{68}s_{69}+s_{70}+s_{121}+s_{133}+s_{134}s_{135}+s_{136}+s_{148}\\&+s_{181}+s_{202}+s_{223}+s_{229}+s_{245}s_{246}+s_{247}+s_{272}s_{273}+s_{274}\end{aligned} \tag{107}$$

$$\begin{aligned}z_{108}=&s_{42}+s_{52}s_{53}+s_{67}s_{68}+s_{69}+s_{120}+s_{132}+s_{133}s_{134}+s_{135}+s_{147}\\&+s_{180}+s_{201}+s_{222}+s_{228}+s_{244}s_{245}+s_{246}+s_{271}s_{272}+s_{273}\end{aligned} \tag{108}$$

$$\begin{aligned}z_{109}=&s_{41}+s_{51}s_{52}+s_{66}s_{67}+s_{68}+s_{119}+s_{131}+s_{132}s_{133}+s_{134}+s_{146}\\&+s_{179}+s_{200}+s_{221}+s_{227}+s_{243}s_{244}+s_{245}+s_{270}s_{271}+s_{272}\end{aligned} \tag{109}$$

$$\begin{aligned}z_{110}=&s_{40}+s_{50}s_{51}+s_{65}s_{66}+s_{67}+s_{118}+s_{130}+s_{131}s_{132}+s_{133}+s_{145}\\&+s_{178}+s_{199}+s_{220}+s_{226}+s_{242}s_{243}+s_{244}+s_{269}s_{270}+s_{271}\end{aligned}\tag{110}$$

$$\begin{aligned}z_{111}=&s_{39}+s_{49}s_{50}+s_{64}s_{65}+s_{66}+s_{117}+s_{129}+s_{130}s_{131}+s_{132}+s_{144}+s_{162}+s_{175}s_{176}+s_{177}\\&+s_{198}+s_{219}+s_{225}+s_{241}s_{242}+s_{243}+s_{264}+s_{268}s_{269}+s_{270}\end{aligned}\tag{111}$$

$$\begin{aligned}z_{112}=&s_{38}+s_{48}s_{49}+s_{63}s_{64}+s_{65}+s_{116}+s_{128}+s_{129}s_{130}+s_{131}+s_{143}+s_{161}+s_{174}s_{175}+s_{176}\\&+s_{197}+s_{218}+s_{224}+s_{240}s_{241}+s_{242}+s_{263}+s_{267}s_{268}+s_{269}\end{aligned}\tag{112}$$

$$\begin{aligned}z_{113}=&s_{37}+s_{47}s_{48}+s_{62}s_{63}+s_{64}+s_{115}+s_{127}+s_{128}s_{129}+s_{130}+s_{142}+s_{160}+s_{173}s_{174}+s_{175}\\&+s_{196}+s_{217}+s_{223}+s_{239}s_{240}+s_{241}+s_{262}+s_{266}s_{267}+s_{268}\end{aligned}\tag{113}$$

$$\begin{aligned}z_{114}=&s_{36}+s_{46}s_{47}+s_{61}s_{62}+s_{63}+s_{114}+s_{126}+s_{127}s_{128}+s_{129}+s_{141}+s_{159}+s_{172}s_{173}+s_{174}\\&+s_{195}+s_{216}+s_{222}+s_{238}s_{239}+s_{240}+s_{261}+s_{265}s_{266}+s_{267}\end{aligned}\tag{114}$$

$$\begin{aligned}z_{115}=&s_{35}+s_{45}s_{46}+s_{60}s_{61}+s_{62}+s_{113}+s_{125}+s_{126}s_{127}+s_{128}+s_{140}+s_{158}+s_{171}s_{172}+s_{173}\\&+s_{194}+s_{215}+s_{221}+s_{237}s_{238}+s_{239}+s_{260}+s_{264}s_{265}+s_{266}\end{aligned}\tag{115}$$

$$\begin{aligned}z_{116}=&s_{34}+s_{44}s_{45}+s_{59}s_{60}+s_{61}+s_{112}+s_{124}+s_{125}s_{126}+s_{127}+s_{139}+s_{157}+s_{170}s_{171}+s_{172}\\&+s_{193}+s_{214}+s_{220}+s_{236}s_{237}+s_{238}+s_{259}+s_{263}s_{264}+s_{265}\end{aligned}\tag{116}$$

$$\begin{aligned}z_{117}=&s_{33}+s_{43}s_{44}+s_{58}s_{59}+s_{60}+s_{111}+s_{123}+s_{124}s_{125}+s_{126}+s_{138}+s_{156}+s_{169}s_{170}+s_{171}\\&+s_{192}+s_{213}+s_{219}+s_{235}s_{236}+s_{237}+s_{258}+s_{262}s_{263}+s_{264}\end{aligned}\tag{117}$$

$$\begin{aligned}z_{118}=&s_{32}+s_{42}s_{43}+s_{57}s_{58}+s_{59}+s_{110}+s_{122}+s_{123}s_{124}+s_{125}+s_{137}+s_{155}+s_{168}s_{169}+s_{170}\\&+s_{191}+s_{212}+s_{218}+s_{234}s_{235}+s_{236}+s_{257}+s_{261}s_{262}+s_{263}\end{aligned}\tag{118}$$

$$\begin{aligned}z_{119}=&s_{31}+s_{41}s_{42}+s_{56}s_{57}+s_{58}+s_{109}+s_{121}+s_{122}s_{123}+s_{124}+s_{136}+s_{154}+s_{167}s_{168}+s_{169}\\&+s_{190}+s_{211}+s_{217}+s_{233}s_{234}+s_{235}+s_{256}+s_{260}s_{261}+s_{262}\end{aligned}\tag{119}$$

$$\begin{aligned}z_{120}=&s_{30}+s_{40}s_{41}+s_{55}s_{56}+s_{57}+s_{108}+s_{120}+s_{121}s_{122}+s_{123}+s_{135}+s_{153}+s_{166}s_{167}+s_{168}\\&+s_{189}+s_{210}+s_{216}+s_{232}s_{233}+s_{234}+s_{255}+s_{259}s_{260}+s_{261}\end{aligned}\tag{120}$$

$$\begin{aligned}z_{121}=&s_{29}+s_{39}s_{40}+s_{54}s_{55}+s_{56}+s_{107}+s_{119}+s_{120}s_{121}+s_{122}+s_{134}+s_{152}+s_{165}s_{166}+s_{167}\\&+s_{188}+s_{209}+s_{215}+s_{231}s_{232}+s_{233}+s_{254}+s_{258}s_{259}+s_{260}\end{aligned}\tag{121}$$

$$\begin{aligned}z_{122}=&s_{28}+s_{38}s_{39}+s_{53}s_{54}+s_{55}+s_{106}+s_{118}+s_{119}s_{120}+s_{121}+s_{133}+s_{151}+s_{164}s_{165}+s_{166}\\&+s_{187}+s_{208}+s_{214}+s_{230}s_{231}+s_{232}+s_{253}+s_{257}s_{258}+s_{259}\end{aligned}\tag{122}$$

$$\begin{aligned}z_{123}=&s_{27}+s_{37}s_{38}+s_{52}s_{53}+s_{54}+s_{105}+s_{117}+s_{118}s_{119}+s_{120}+s_{132}+s_{150}+s_{163}s_{164}+s_{165}\\&+s_{186}+s_{207}+s_{213}+s_{229}s_{230}+s_{231}+s_{252}+s_{256}s_{257}+s_{258}\end{aligned}\tag{123}$$

$$\begin{aligned}z_{124}=&s_{26}+s_{36}s_{37}+s_{51}s_{52}+s_{53}+s_{104}+s_{116}+s_{117}s_{118}+s_{119}+s_{131}+s_{149}+s_{162}s_{163}+s_{164}\\&+s_{185}+s_{206}+s_{212}+s_{228}s_{229}+s_{230}+s_{251}+s_{255}s_{256}+s_{257}\end{aligned}\tag{124}$$

$$\begin{aligned}z_{125}=&s_{25}+s_{35}s_{36}+s_{50}s_{51}+s_{52}+s_{103}+s_{115}+s_{116}s_{117}+s_{118}+s_{130}+s_{148}+s_{161}s_{162}+s_{163}\\&+s_{184}+s_{205}+s_{211}+s_{227}s_{228}+s_{229}+s_{250}+s_{254}s_{255}+s_{256}\end{aligned}\tag{125}$$

$$\begin{aligned}z_{126}=&s_{24}+s_{34}s_{35}+s_{49}s_{50}+s_{51}+s_{102}+s_{114}+s_{115}s_{116}+s_{117}+s_{129}+s_{147}+s_{160}s_{161}+s_{162}\\&+s_{183}+s_{204}+s_{210}+s_{226}s_{227}+s_{228}+s_{249}+s_{253}s_{254}+s_{255}\end{aligned}\tag{126}$$

$$\begin{aligned}z_{127}=&s_{23}+s_{33}s_{34}+s_{48}s_{49}+s_{50}+s_{101}+s_{113}+s_{114}s_{115}+s_{116}+s_{128}+s_{146}+s_{159}s_{160}+s_{161}\\&+s_{182}+s_{203}+s_{209}+s_{225}s_{226}+s_{227}+s_{248}+s_{252}s_{253}+s_{254}\end{aligned}\tag{127}$$

$$\begin{aligned}z_{128}=&s_{22}+s_{32}s_{33}+s_{47}s_{48}+s_{49}+s_{100}+s_{112}+s_{113}s_{114}+s_{115}+s_{127}+s_{145}+s_{158}s_{159}+s_{160}\\&+s_{181}+s_{202}+s_{208}+s_{224}s_{225}+s_{226}+s_{247}+s_{251}s_{252}+s_{253}\end{aligned}\tag{128}$$

$$\begin{aligned}z_{129}=&s_{21}+s_{31}s_{32}+s_{46}s_{47}+s_{48}+s_{99}+s_{111}+s_{112}s_{113}+s_{114}+s_{126}+s_{144}+s_{157}s_{158}+s_{159}\\&+s_{180}+s_{201}+s_{207}+s_{223}s_{224}+s_{225}+s_{246}+s_{250}s_{251}+s_{252}\end{aligned}\tag{129}$$

$$\begin{aligned}z_{130}=&s_{20}+s_{30}s_{31}+s_{45}s_{46}+s_{47}+s_{98}+s_{110}+s_{111}s_{112}+s_{113}+s_{125}+s_{143}+s_{156}s_{157}+s_{158}\\&+s_{179}+s_{200}+s_{206}+s_{222}s_{223}+s_{224}+s_{245}+s_{249}s_{250}+s_{251}\end{aligned}\tag{130}$$

$$z_{131}=s_{19}+s_{29}s_{30}+s_{44}s_{45}+s_{46}+s_{97}+s_{109}+s_{110}s_{111}+s_{112}+s_{124}+s_{142}+s_{155}s_{156}+s_{157}$$

$$+s_{178}+s_{199}+s_{205}+s_{221}s_{222}+s_{223}+s_{244}+s_{248}s_{249}+s_{250} \tag{131}$$

$$\begin{aligned}z_{132}=&s_{18}+s_{28}s_{29}+s_{43}s_{44}+s_{45}+s_{96}+s_{108}+s_{109}s_{110}+s_{111}+s_{123}+s_{141}+s_{154}s_{155}+s_{156}+s_{162}\\&+s_{175}s_{176}+s_{177}+s_{198}+s_{204}+s_{220}s_{221}+s_{222}+s_{243}+s_{247}s_{248}+s_{249}+s_{264}\end{aligned} \tag{132}$$

$$\begin{aligned}z_{133}=&s_{17}+s_{27}s_{28}+s_{42}s_{43}+s_{44}+s_{95}+s_{107}+s_{108}s_{109}+s_{110}+s_{122}+s_{140}+s_{153}s_{154}+s_{155}+s_{161}\\&+s_{174}s_{175}+s_{176}+s_{197}+s_{203}+s_{219}s_{220}+s_{221}+s_{242}+s_{246}s_{247}+s_{248}+s_{263}\end{aligned} \tag{133}$$

$$\begin{aligned}z_{134}=&s_{16}+s_{26}s_{27}+s_{41}s_{42}+s_{43}+s_{94}+s_{106}+s_{107}s_{108}+s_{109}+s_{121}+s_{139}+s_{152}s_{153}+s_{154}+s_{160}\\&+s_{173}s_{174}+s_{175}+s_{196}+s_{202}+s_{218}s_{219}+s_{220}+s_{241}+s_{245}s_{246}+s_{247}+s_{262}\end{aligned} \tag{134}$$

$$\begin{aligned}z_{135}=&s_{15}+s_{25}s_{26}+s_{40}s_{41}+s_{42}+s_{66}+s_{91}s_{92}+s_{93}+s_{105}+s_{106}s_{107}+s_{108}+s_{120}+s_{138}+s_{151}s_{152}+s_{153}\\&+s_{159}+s_{171}+s_{172}s_{173}+s_{174}+s_{195}+s_{201}+s_{217}s_{218}+s_{219}+s_{240}+s_{244}s_{245}+s_{246}+s_{261}\end{aligned} \tag{135}$$

$$\begin{aligned}z_{136}=&s_{14}+s_{24}s_{25}+s_{39}s_{40}+s_{41}+s_{65}+s_{90}s_{91}+s_{92}+s_{104}+s_{105}s_{106}+s_{107}+s_{119}+s_{137}+s_{150}s_{151}+s_{152}\\&+s_{158}+s_{170}+s_{171}s_{172}+s_{173}+s_{194}+s_{200}+s_{216}s_{217}+s_{218}+s_{239}+s_{243}s_{244}+s_{245}+s_{260}\end{aligned} \tag{136}$$

$$\begin{aligned}z_{137}=&s_{13}+s_{23}s_{24}+s_{38}s_{39}+s_{40}+s_{64}+s_{89}s_{90}+s_{91}+s_{103}+s_{104}s_{105}+s_{106}+s_{118}+s_{136}+s_{149}s_{150}+s_{151}\\&+s_{157}+s_{169}+s_{170}s_{171}+s_{172}+s_{193}+s_{199}+s_{215}s_{216}+s_{217}+s_{238}+s_{242}s_{243}+s_{244}+s_{259}\end{aligned} \tag{137}$$

$$\begin{aligned}z_{138}=&s_{12}+s_{22}s_{23}+s_{37}s_{38}+s_{39}+s_{63}+s_{88}s_{89}+s_{90}+s_{102}+s_{103}s_{104}+s_{105}+s_{117}+s_{135}+s_{148}s_{149}+s_{150}\\&+s_{156}+s_{168}+s_{169}s_{170}+s_{171}+s_{192}+s_{198}+s_{214}s_{215}+s_{216}+s_{237}+s_{241}s_{242}+s_{243}+s_{258}\end{aligned} \tag{138}$$

$$\begin{aligned}z_{139}=&s_{11}+s_{21}s_{22}+s_{36}s_{37}+s_{38}+s_{62}+s_{87}s_{88}+s_{89}+s_{101}+s_{102}s_{103}+s_{104}+s_{116}+s_{134}+s_{147}s_{148}+s_{149}\\&+s_{155}+s_{167}+s_{168}s_{169}+s_{170}+s_{191}+s_{197}+s_{213}s_{214}+s_{215}+s_{236}+s_{240}s_{241}+s_{242}+s_{257}\end{aligned} \tag{139}$$

$$\begin{aligned}z_{140}=&s_{10}+s_{20}s_{21}+s_{35}s_{36}+s_{37}+s_{61}+s_{86}s_{87}+s_{88}+s_{100}+s_{101}s_{102}+s_{103}+s_{115}+s_{133}+s_{146}s_{147}+s_{148}\\&+s_{154}+s_{166}+s_{167}s_{168}+s_{169}+s_{190}+s_{196}+s_{212}s_{213}+s_{214}+s_{235}+s_{239}s_{240}+s_{241}+s_{256}\end{aligned} \tag{140}$$

$$\begin{aligned}z_{141}=&s_{9}+s_{19}s_{20}+s_{34}s_{35}+s_{36}+s_{60}+s_{85}s_{86}+s_{87}+s_{99}+s_{100}s_{101}+s_{102}+s_{114}+s_{132}+s_{145}s_{146}+s_{147}\\&+s_{153}+s_{165}+s_{166}s_{167}+s_{168}+s_{189}+s_{195}+s_{211}s_{212}+s_{213}+s_{234}+s_{238}s_{239}+s_{240}+s_{255}\end{aligned} \tag{141}$$

$$\begin{aligned}z_{142}=&s_{8}+s_{18}s_{19}+s_{33}s_{34}+s_{35}+s_{59}+s_{84}s_{85}+s_{86}+s_{98}+s_{99}s_{100}+s_{101}+s_{113}+s_{131}+s_{144}s_{145}+s_{146}\\&+s_{152}+s_{164}+s_{165}s_{166}+s_{167}+s_{188}+s_{194}+s_{210}s_{211}+s_{212}+s_{233}+s_{237}s_{238}+s_{239}+s_{254}\end{aligned} \tag{142}$$

$$\begin{aligned}z_{143}=&s_{7}+s_{17}s_{18}+s_{32}s_{33}+s_{34}+s_{58}+s_{83}s_{84}+s_{85}+s_{97}+s_{98}s_{99}+s_{100}+s_{112}+s_{130}+s_{143}s_{144}+s_{145}\\&+s_{151}+s_{163}+s_{164}s_{165}+s_{166}+s_{187}+s_{193}+s_{209}s_{210}+s_{211}+s_{232}+s_{236}s_{237}+s_{238}+s_{253}\end{aligned} \tag{143}$$

$$\begin{aligned}z_{144}=&s_{6}+s_{16}s_{17}+s_{31}s_{32}+s_{33}+s_{57}+s_{82}s_{83}+s_{84}+s_{96}+s_{97}s_{98}+s_{99}+s_{111}+s_{129}+s_{142}s_{143}+s_{144}\\&+s_{150}+s_{162}+s_{163}s_{164}+s_{165}+s_{186}+s_{192}+s_{208}s_{209}+s_{210}+s_{231}+s_{235}s_{236}+s_{237}+s_{252}\end{aligned} \tag{144}$$

$$\begin{aligned}z_{145}=&s_{5}+s_{15}s_{16}+s_{30}s_{31}+s_{32}+s_{56}+s_{81}s_{82}+s_{83}+s_{95}+s_{96}s_{97}+s_{98}+s_{110}+s_{128}+s_{141}s_{142}+s_{143}\\&+s_{149}+s_{161}+s_{162}s_{163}+s_{164}+s_{185}+s_{191}+s_{207}s_{208}+s_{209}+s_{230}+s_{234}s_{235}+s_{236}+s_{251}\end{aligned} \tag{145}$$

$$\begin{aligned}z_{146}=&s_{4}+s_{14}s_{15}+s_{29}s_{30}+s_{31}+s_{55}+s_{80}s_{81}+s_{82}+s_{94}+s_{95}s_{96}+s_{97}+s_{109}+s_{127}+s_{140}s_{141}+s_{142}\\&+s_{148}+s_{160}+s_{161}s_{162}+s_{163}+s_{184}+s_{190}+s_{206}s_{207}+s_{208}+s_{229}+s_{233}s_{234}+s_{235}+s_{250}\end{aligned} \tag{146}$$

$$\begin{aligned}z_{147}=&s_{3}+s_{13}s_{14}+s_{28}s_{29}+s_{30}+s_{54}+s_{66}+s_{79}s_{80}+s_{81}+s_{91}s_{92}+s_{93}+s_{94}s_{95}+s_{96}+s_{108}+s_{126}+s_{139}s_{140}+s_{141}\\&+s_{147}+s_{159}+s_{160}s_{161}+s_{162}+s_{171}+s_{183}+s_{189}+s_{205}s_{206}+s_{207}+s_{228}+s_{232}s_{233}+s_{234}+s_{249}\end{aligned} \tag{147}$$