Des. Codes Cryptogr. (2012) 62:289–311
DOI 10.1007/s10623-011-9518-9

Fault analysis of Trivium

Yupu Hu · Juntao Gao · Qing Liu · Yiwei Zhang

Received: 3 October 2010 / Revised: 28 February 2011 / Accepted: 28 April 2011 /
Published online: 21 May 2011

Abstract As a hardware-oriented stream cipher, Trivium is on the edge of low cost and compactness. In this paper we discuss how brittle Trivium is under fault attack. Our fault model is based on the following two assumptions: (1) We can make fault injection on the state at a random time and (2) after each fault injection, the fault positions are from random one of three registers, and from a random area within eight neighboring bits. Our fault model has extremely weak assumptions for effective attack , and much weaker than that of Hojsík and Rudolf, in their fault attack on Trivium. We present a checking method such that, by observing original key-stream segment and fault injected key-stream segment, the injecting time and fault positions can be determined. Then, for several distributions of the injecting time, our random simulations always show that the attacker can break Trivium by a small number of repeated fault injections. For example, suppose that the injecting time has an uniform distribution over $\{0, 1, \ldots, 32\}$, then averagely no more than 16 repeated fault injection procedures will break Trivium, by averagely observing no more than 195×17 key-stream bits.

Keywords Trivium · Stream cipher · Side-channel attack · Fault analysis

Mathematics Subject Classification (2000) 94A60 · 94A55 · 11K45

Communicated by V. van Rijmen.

Y. Hu (✉) · J. Gao · Q. Liu
CNIS Laboratory, Xidian University, Xi'an 710071, China
e-mail: yphu@mail.xidian.edu.cn

J. Gao
e-mail: gjt_albert@163.com; jtgao@mail.xidian.edu.cn

Q. Liu
e-mail: baxiziliaoshi@126.com

Y. Zhang
ZTE IC Design Co., Ltd., Shenzhen 518057, China
e-mail: changdavid@163.com

1 Introduction

1.1 Background and results of our work

Trivium [1,2] is a hardware-oriented stream cipher designed in 2005 by Cannière and Preneel, and has been chosen as one of the final ciphers by eSTREAM project. It is well known that Trivium is on the edge of low cost and compactness, with a simple and elegant structure. Although Trivium has attracted a lot of interest [3–8], it remains strong enough against those known attacks, except for side-channel attacks. An obvious weakness of Trivium is that its non-linearization procedure is very slow, so that Trivium was guessed brittle under side-channel attacks.

Several side-channel attacks were presented for stream ciphers [9–15]. At FSE 2008 [16] and INDOCRYPT 2008 [17], Hojsík and Rudolf presented a side-channel attack on Trivium, named fault analysis. It uses fault floating and repeated fault injections to break Trivium. Their attack is successful, but their fault model is based on two strong assumptions, as follows.

Assumption 1 We can make fault injection on the state at a fixed time, especially at the initial time.

Assumption 2 After each 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 fault injection is made by laser or by magnetic disturbance or by some other brute forces. When a bit is corrupted, it is difficult to keep the neighbor bits not to be corrupted.

In this paper we discuss how brittle Trivium is under fault attack. That is, how weak the assumptions are needed for breaking Trivium by fault analysis.
Fault model of this paper Our assumptions are Assumptions 3 and 4.

Assumption 3 We can make fault injection on the state at a random time.

Assumption 4 After each fault injection, the fault positions are from random one of three registers, and from a random area within eight neighboring bits.

Here we explain our fault model in detail. The key-stream generator of Trivium has a state of 288 bits long, with state bits $(s_1, s_2, \dots, s_{288})$. The state is composed of three registers, with state bits $(s_1, s_2, \dots, s_{93})$, $(s_{94}, s_{95}, \dots, s_{177})$ and $(s_{177}, s_{178}, \dots, s_{288})$ respectively. In each register, state bits are positioned in natural ranking. At a random time M of the key-stream generator's driving procedure, the attacker injects faults at some state bits (that is, at time M, changes values of these state bits). The set of indices of fault bits is A. After such fault injection, the attacker does not know (M, A), the injecting time and fault positions. He only knows that A is a random area satisfying 2 restrictions in the follow.

(1) $A \subset \{1, \dots, 93\}$ or $A \subset \{94, \dots, 177\}$ or $A \subset \{178, \dots, 288\}$,
(2) $\max\{A\} - \min\{A\} \leq 7$.

Attack model of this paper Suppose that the attacker obtains an encryption machine, equipped with Trivium. He starts up this machine, and obtains original key-stream segment $(z_0 z_1 \dots z_N)$. Then he resets the machine, and simultaneously makes fault injection under Assumptions 3 and 4. So that he obtains the fault injected key-stream segment $(z'_0 z'_1 \dots z'_N)$, and the differential of the two segments $(\triangle z_0, \triangle z_1, \dots, \triangle z_N) = (z_0 + z'_0, z_1 + z'_1, \dots, z_N + z'_N)$. The attacker can repeat this resetting-injection procedure several times. He hopes to break Trivium by such information. In our attack model we neglect IV (initial vector), because we simply assume that the attacker uses same IV for each starting up.

Contributions of this paper First, we present a checking method such that, by observing original key-stream segment and fault injected key-stream segment, the injecting time and fault positions can be determined. Such determination is an important step for breaking Trivium. Only by this determination can the attacker obtain some additional linear equations of the state at some known time. Our checking method is based on our fault model, which is not only much weaker than that of Hojsík and Rudolf [16], but also extremely weak. Under weaker assumptions, we can not determine the injecting time and fault positions (For example, suppose $\max\{A\} - \min\{A\} \leq 8$, other than $\max\{A\} - \min\{A\} \leq 7$. We find that some different sets of fault positions will generate same key-stream segment. Some different sets of fault positions will generate different key-stream segments, but they are hard to be distinguished. So that we can only estimate the injecting time and fault positions with some credit degree). Our checking method is quite a new one, never similar to the checking method of Hojsík and Rudolf [16].

Second, we show how to break Trivium under our fault model. The attacker repeats the fault injection procedure several times, so as to accumulate enough number of linear equations of the state at a known time (Trivium is broken if the state at any known time is solved). To make the breaking more efficient, he can use fault floating technique, presented by Hojsík and Rudolf [17]. We suppose that the injecting time has an uniform distribution over $\{0, 1, \ldots, M_0\}$, and make random simulations. Our experimental results are as follows.

> For each fault injection procedure, averagely 195 fault injected key-stream bits are needed.
> For $M_0 = 0$, averagely 3.7 repeated fault injection procedures will break Trivium, by averagely observing 195×4.7 key-stream bits.
> For $M_0 = 1$, averagely 4.0 repeated fault injection procedures will break Trivium, by averagely observing 195×5.0 key-stream bits.
> For $M_0 = 2$, averagely 4.3 repeated fault injection procedures will break Trivium, by averagely observing 195×5.3 key-stream bits.
> For $M_0 = 4$, averagely 5.4 repeated fault injection procedures will break Trivium, by averagely observing 195×6.4 key-stream bits.
> For $M_0 = 8$, averagely 7.6 repeated fault injection procedures will break Trivium, by averagely observing 195×8.6 key-stream bits.
> For $M_0 = 16$, averagely 10.0 repeated fault injection procedures will break Trivium, by averagely observing 195×11.0 key-stream bits.
> For $M_0 = 32$, averagely no more than 16 repeated fault injection procedures will break Trivium, by averagely observing no more than 195×17.0 key-stream bits.

Although the practicality of fault attack is open to some debate, our fault model can relax the criticism against those transient fault models, pointed by Biham and Shamir [18]. We find that some durative fault model can be approached by our fault model. Besides, our Assumption 4 has a major difference with the assumption of cold boot attacks [19]. Their assumption only allows faults in single random direction, while our Assumption 4 allows faults in various random directions.

Fault floating technique The idea of floating fault analysis of Trivium [17] is to find an appropriate time e, such that the state at time e can be solved as easy as possible. In other words, it is to find a time e, such that as many as possible linear equations of the state at time e can be obtained. We will present a detailed explanation in Sects. 2 and 4.1.

Our principal insight Trivium is over simple so as to attract our interest in mathematically analyzing its weakness, especially in fault injection circumstance. We find that the work of Hojsík and Rudolf can be greatly improved, and their attack model can be greatly weakened.
Organization of this paper In Sect. 1.2 we review recent works related to 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 present a complete checking routine, through which the injecting time and fault positions can be determined. Section 4 is the procedure for breaking Trivium. In this section we make use of fault floating, presented by Hojsík and Rudolf [17], combining with repeated fault injections, and show that the attacker can accumulate enough number of linear equations of the state at a known time.

1.2 Recent works related to Trivium

Many previous results in Trivium cryptanalysis have been mentioned by Hojsík and Rudolf [16,17], and listed in our references. Here we only briefly mention four results obtained recently.

Priemuth-Schmid and 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. Pasalic [19] mainly considered the scenario where the key differential and/or IV differential influence the internal state of the cipher. They showed that under certain circumstances a chosen IV attack may be transformed into the key chosen attack. Based on the idea of cube attack proposed by Dinur and Shamir [20], Bedi and Pillai [21] presented cube attacks on Trivium.

2 Trivium model and Trivium features

The key-stream generator of Trivium has a state of 288 bits long, with state bits $(s_1, s_2, \ldots, s_{288})$. The state is composed of three registers. The first register is 93 bit long, with state bits $(s_1, s_2, \ldots, s_{93})$. The second register is 84 bit long, with state bits $(s_{94}, s_{95}, \ldots, s_{177})$. The third register is 111 bit long, with state bits $(s_{178}, s_{179}, \ldots, s_{288})$. Table 1 is an equivalent algorithm for the key-stream generation.

Table 1 The key-stream generation algorithm

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

for $i = 0$ to $N$ do
    $z_i \leftarrow s_{66} + s_{93} + s_{162} + s_{177} + s_{243} + s_{288}$
    $t_1 \leftarrow s_{66} + s_{91}s_{92} + s_{93} + s_{171}$
    $t_2 \leftarrow s_{162} + s_{175}s_{176} + s_{177} + s_{264}$
    $t_3 \leftarrow s_{243} + s_{286}s_{287} + s_{288} + s_{69}$
    $(s_1, \ldots, s_{93}) \leftarrow (t_3, s_1, \ldots, s_{92})$
    $(s_{94}, \ldots, s_{177}) \leftarrow (t_1, s_{94}, \ldots, s_{176})$
    $(s_{178}, \ldots, s_{288}) \leftarrow (t_2, s_{178}, \ldots, s_{287})$
end for
```

Table 2 The inner state renewal

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

In Table 1, step 2 is output of the key-stream bit, which is a linear function of the state. Step 3–8 is the state renewal, which is a non-linear-feedback-shift-register (NFSR) algorithm. In Appendix A, two figures illustrate Trivium algorithm. 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.

The state renewal is reversible. So that Trivium is broken if the state at any known time is revealed.

Suppose that the attacker obtains a key-stream segment

$$(z_t z_{t+1} z_{t+2} \ldots z_{t+N})$$

from time t to time $t + N$. Then he obtains $N + 1$ equations of

$$(s_{(t,1)}, s_{(t,2)}, \ldots, s_{(t,288)})$$

the state at time t. These equations are called original equations, and are respectively ranked Eq. 0, Eq. 1, . . ., Eq. N. 66 of these original equations are linear equations, ranked from Eqs. 0 to 65. 82 of these original equations are quadratic equations, ranked from Eqs. 66 to 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 structures, Eqs. 66–147 are also called pair quadratic equations (see [16]). 66 of these original equations are cubic equations, ranked from Eqs. 148 to 213. Equations 0–147 are presented in Appendix B.

Suppose that the attacker obtains not only the key-stream segment

$$(z_t z_{t+1} z_{t+2} \ldots z_{t+N})$$

from time t to time $t + N$, but also

(1) another key-stream segment $(z'_t z'_{t+1} z'_{t+2} \ldots z'_{t+N})$ from time t to time $t + N$, therefore the differential of two segments

$$(\triangle z_t, \triangle z_{t+1}, \ldots, \triangle z_{t+N}) = (z_t + z'_t, z_{t+1} + z'_{t+1}, \ldots, z_{t+N} + z'_{t+N})$$

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

$$(\triangle s_{(t,1)}, \triangle s_{(t,2)}, \ldots, \triangle s_{(t,288)}) = (s_{(t,1)} + s'_{(t,1)}, s_{(t,2)} + s'_{(t,2)}, \ldots, s_{(t,288)} + s'_{(t,288)})$$

Then he obtains another $N + 1$ equations of $(s_{(t,1)}, s_{(t,2)}, \ldots, s_{(t,288)})$. 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. Additional linear equations are most valuable for breaking Trivium.

It is clear that, by Table 2,

$$\begin{aligned}
&(\triangle s_{(t+1,1)}, \triangle s_{(t+1,2)}, \ldots, \triangle s_{(t+1,93)})\\
&\quad = (\triangle s_{(t,243)} + \triangle(s_{(t,286)}s_{(t,287)}) + \triangle s_{(t,288)} + \triangle s_{(t,69)}, \triangle s_{(t,1)}, \ldots, \triangle s_{(t,69)})\\
&\quad = (\triangle s_{(t,243)} + s_{(t,286)}\triangle s_{(t,287)} + s_{(t,287)}\triangle s_{(t,286)} + \triangle s_{(t,286)}\triangle s_{(t,287)}\\
&\qquad + \triangle s_{(t,288)} + \triangle s_{(t,69)}, \triangle s_{(t,1)}, \ldots, \triangle s_{(t,92)})
\end{aligned}$$

$$\begin{aligned}
&(\triangle s_{(t+1,94)}, \triangle s_{(t+1,95)}, \ldots, \triangle s_{(t+1,177)})\\
&\quad = (\triangle s_{(t,66)} + \triangle(s_{(t,91)}s_{(t,92)}) + \triangle s_{(t,93)} + \triangle s_{(t,171)}, \triangle s_{(t,94)}, \ldots, \triangle s_{(t,176)})\\
&\quad = (\triangle s_{(t,66)} + s_{(t,91)}\triangle s_{(t,92)} + s_{(t,92)}\triangle s_{(t,91)} + \triangle s_{(t,91)}\triangle s_{(t,92)} + \triangle s_{(t,93)}\\
&\qquad + \triangle s_{(t,171)}, \triangle s_{(t,94)}, \ldots, \triangle s_{(t,176)})
\end{aligned}$$

$$\begin{aligned}
&(\triangle s_{(t+1,178)}, \triangle s_{(t+1,179)}, \ldots, \triangle s_{(t+1,288)})\\
&\quad = (\triangle s_{(t,162)} + \triangle(s_{(t,175)}s_{(t,176)}) + \triangle s_{(t,177)} + \triangle s_{(t,264)}, \triangle s_{(t,178)}, \ldots, \triangle s_{(t,287)})\\
&\quad = (\triangle s_{(t,162)} + s_{(t,175)}\triangle s_{(t,176)} + s_{(t,176)}\triangle s_{(t,175)} + \triangle s_{(t,175)}\triangle s_{(t,176)}\\
&\qquad + \triangle s_{(t,177)} + \triangle s_{(t,264)}, \triangle s_{(t,178)}, \ldots, \triangle s_{(t,287)})
\end{aligned}$$

These formulae imply that, by knowing

$$(\triangle s_{(t,1)}, \triangle s_{(t,2)}, \ldots, \triangle s_{(t,288)})$$

and

$$\{\triangle(s_{(t,91)}s_{(t,92)}), \triangle(s_{(t,175)}s_{(t,176)}), \triangle(s_{(t,286)}s_{(t,287)})\}$$

we can induce $(\triangle s_{(t+1,1)}, \triangle s_{(t+1,2)}, \ldots, \triangle s_{(t+1,288)})$. This feature is called differential float, or fault float, presented by Hojsík and Rudolf [17].

3 Determination of the injecting time and fault positions

Suppose that the attacker has obtained original key-stream segment $(z_0 z_1 z_2 \ldots z_N)$ and fault injected key-stream segment $(z'_0 z'_1 z'_2 \ldots z'_N)$, according to Assumptions 3 and 4. So that he has obtained the differential of the two segments

$$(\triangle z_0, \triangle z_1, \ldots, \triangle z_N) = (z_0 + z'_0, z_1 + z'_1, \ldots, z_N + z'_N)$$

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.

A denotes the set of fault positions. $P_L = min\{A\}$ denotes the lowest position of injected faults. $P_H = max\{A\}$ denotes the highest position of injected faults. According to our Assumption 4, $0 \le P_H - P_L \le 7$. Again P_H and P_L are from same set of indices $\{1, \ldots, 93\}$ or $\{94, \ldots, 177\}$ or $\{178, \ldots, 288\}$.

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

M denotes the fault injecting time. T denotes the first time t such that $\triangle z_T = 1$. The attacker has already known T. He does not know M, but he does know that $T - 68 \leq M \leq T$.

$*$ denotes uncertain bit value.
n denotes the largest t such that $0 \leq t \leq 7$ and $\triangle z_{T+t} = 1$.
l denotes the smallest t such that $t > n$ and $\triangle z_{T+t} = 1$.
k denotes the largest t such that $l \leq t \leq l + 7$ and $\triangle z_{T+t} = 1$.

According to key-stream generation algorithm, A shifts rightward. When A passes across the positions

$$\{66, 69, 91, 92, 93, 162, 171, 175, 176, 177, 243, 264, 286, 287, 288\}$$

fault positions are diffused to the positions $\{1, 94, 178\}$. 6 positions

$$\{66, 69, 162, 171, 243, 264\}$$

are simple positions because, when A passes across them, faults are directly diffused to the positions $\{1, 94, 178\}$. 9 positions

$$\{91, 92, 93, 175, 176, 177, 286, 287, 288\}$$

are complicated positions because, when A passes across them, diffusion features are complicated.

Suppose (M, A) and (M', A') are two pairs of the fault injecting time and the set of fault positions, and $M' > M$. We say that (M, A) and (M', A') are equivalent, if (M, A) and (M', A') generate completely same fault injected key-stream, and they have same state value at time M'.

Lemma 1 *If* $A \cap \{66, 69, 91, 92, 93, 162, 171, 175, 176, 177, 243, 264, 286, 287, 288\} = \Phi$ *(the empty set),* (M, A) *and* $(M+1, A+1)$ *are equivalent, where* $(A+1) = \{a_1+1, \ldots, a_n+1\}$ *for* $A = \{a_1, \ldots, a_u\}$ *(in fact,* (M, A) *and* $(M + 1, A + 1)$ *have same state value at time* $M + 1$*).*

Lemma 2

(1) *In case* $1 \leq P_L \leq 66$*, we can equivalently take* $M = T$*, so that* $P_H \geq 66$ *and* $66 \in A$.
(2) *In case* $94 \leq P_L \leq 162$*, we can equivalently take* $M = T$*, so that* $P_H \geq 162$ *and* $162 \in A$.
(3) *In case* $178 \leq P_L \leq 243$*, we can equivalently take* $M = T$*, so that* $P_H \geq 243$ *and* $243 \in A$.
(4) *In case* $70 \leq P_L \leq 93$*, we can equivalently take* $T-2 \leq M \leq T$*, so that* $91 \leq P_H \leq 93$.
(5) *In case* $172 \leq P_L \leq 177$*, we can equivalently take* $T - 2 \leq M \leq T$*, so that* $175 \leq P_H \leq 177$.
(6) *In case* $265 \leq P_L \leq 288$*, we can equivalently take* $T - 2 \leq M \leq T$*, so that* $286 \leq P_H \leq 288$.
(7) *In case* $67 \leq P_L \leq 69$*, we can equivalently take* $\triangle s_{(M,69)} = 1$*, so that* $P_H \geq 69$ *and* $69 \in A$.
(8) *In case* $163 \leq P_L \leq 171$*, we can equivalently take* $\triangle s_{(M,171)} = 1$*, so that* $P_H \geq 171$ *and* $171 \in A$.
(9) *In case* $244 \leq P_L \leq 264$*, we can equivalently take* $\triangle s_{(M,264)} = 1$*, so that* $P_H \geq 264$ *and* $264 \in A$.

Lemma 3 *Suppose* $1 \leq P_L \leq 66$*. Equivalently take* $M = T$ *and* $P_H \geq 66$*. Then*

(1) $(\triangle z_{T+l}, \triangle z_{T+l+1}, \dots, \triangle z_{T+26}) = (1, *, \dots, *)$.
(2) $(\triangle z_{T+27}, \triangle z_{T+28}, \dots, \triangle z_{T+n+27})$
$=(\triangle z_T, \triangle z_{T+1}, \dots, \triangle z_{T+n})$
$=(1, *, \dots, *, 1)$.
(3) $(\triangle z_{T+n+28}, \triangle z_{T+n+29}, \dots, \triangle z_{T+65}) = (0, 0, \dots, 0)$
(4) $l \leq 27$
(5) $k - n = 27$.
(6) $A = \{t | 66 - n \leq t \leq 93 - l, \triangle z_{T-t+93} = 1\}$

Proof By the definition of l, (1) is true. According to Appendix B,

$$\begin{aligned}
&(\triangle z_T, \triangle z_{T+1}, \dots, \triangle z_{T+n})\\
&\quad = (\triangle s_{(T,66)}, \triangle s_{(T,65)}, \dots, \triangle s_{(T,66-n)})\\
&\quad = (1, *, \dots, *, 1),\\
&(\triangle z_{T+n+1}, \triangle z_{T+n+2}, \dots, \triangle z_{T+l-1}) = (0, 0, \dots, 0),\\
&(\triangle z_{T+l}, \triangle z_{T+l+1}, \dots, \triangle z_{T+26})\\
&\quad = (\triangle s_{(T,93-l)}, \triangle s_{(T,92-l)}, \dots, \triangle s_{(T,67)})\\
&\quad = (1, *, \dots, *),\\
&(\triangle z_{T+27}, \triangle z_{T+28}, \dots, \triangle z_{T+n+27})\\
&\quad = (\triangle s_{(T,66)}, \triangle s_{(T,65)}, \dots, \triangle s_{(T,66-n)})\\
&\quad = (1, * \dots, *, 1),\\
&(\triangle z_{T+n+28}, \triangle z_{T+n+29}, \dots, \triangle z_{T+65}) = (0, 0, \dots, 0).
\end{aligned}$$

All of the above deduce that (2) and (3) are true. By (2) and (3) and the definition of (n, l, k), (4) and (5) are true. (6) is a natural corollary of (1)–(5). Lemma 3 is proved. □

By similar proving procedure with Lemma 3, we can see that Lemmas 4 and 5 are true.

Lemma 4 *Suppose* $94 \leq P_L \leq 162$. *Equivalently take* $M = T$ *and* $P_H \geq 162$. *Then*

(1) $(\triangle z_{T+l}, \triangle z_{T+l+1}, \dots, \triangle z_{T+14}) = (1, * \dots, *)$.
(2) $(\triangle z_{T+15}, \triangle z_{T+16}, \dots, \triangle z_{T+n+15})$
$=(\triangle z_T, \triangle z_{T+1}, \dots, \triangle z_{T+n})$
$=(1, *, \dots, *, 1)$.
(3) $(\triangle z_{T+n+16}, \triangle z_{T+n+17}, \dots, \triangle z_{T+65}) = (0, 0, \dots, 0)$.
(4) $l \leq 15$.
(5) $k - n = 15$
(6) $A = \{t | 162 - n \leq t \leq 177 - l, \triangle z_{T-t+177} = 1\}$.

Lemma 5 *Suppose* $178 \leq P_L \leq 243$. *Equivalently take* $M = T$ *and* $P_H \geq 243$. *Then*

(1) $(\triangle z_{T+l}, \triangle z_{T+l+1}, \dots, \triangle z_{T+44}) = (1, *, \dots, *)$.
(2) $(\triangle z_{T+45}, \triangle z_{T+46}, \dots, \triangle z_{T+n+45})$
$=(\triangle z_T, \triangle z_{T+1}, \dots, \triangle z_{T+n})$
$=(1, *, \dots, *, 1)$.
(3) $(\triangle z_{T+n+46}, \triangle z_{T+n+47}, \dots, \triangle z_{T+65}) = (0, 0 \dots 0)$.
(4) $l \leq 45$.

(5) $k - n = 45$.
(6) $A = \{t|243 - n \leq t \leq 288 - l, \triangle z_{T-t+288} = 1\}$.

Lemma 6 *Suppose* $70 \leq P_L \leq 93$. *Equivalently take* $T - 2 \leq M \leq T$ *and* $91 \leq P_H \leq 93$. *Then*

(1) $(\triangle z_T, \triangle z_{T+1}, \ldots, \triangle z_{T+n})$
$=(\triangle s_{(T,93)}, \triangle s_{(T,92)}, \ldots, \triangle s_{(T,93-n)})$
$=(1, *, \ldots, *, 1)$.
(2) $\triangle z_{T+t} = 0$ *for* $n + 1 \leq t \leq 66$. *So that* $k - n \geq 60$.
(3) *If* $(\triangle z_{T+67}, \triangle z_{T+68}) = (1, *)$, *we can equivalently take* $M = T - 2$, *and* $A = \{t|91 - n \leq t \leq 91, \triangle z_{T-t+91} = 1\}$.
(4) *If* $(\triangle z_{T+67}, \triangle z_{T+68}) = (0, 1)$, *we can equivalently take* $M = T - 1$, *and* $A = \{t|92 - n \leq t \leq 92, \triangle z_{T-t+92} = 1\}$.
(5) *If* $(\triangle z_{T+67}, \triangle z_{T+68}) = (0, 0)$, *we can equivalently take* $M = T$, *and* $A = \{t|93 - n \leq t \leq 93, \triangle z_{T-t+93} = 1\}$.
(6) $(\triangle z_{T+67}, \triangle z_{T+68}, \ldots, \triangle z_{T+n+69})$
$=(\triangle z_{T+82}, \triangle z_{T+83}, \ldots, \triangle z_{T+n+84})$
$=(\triangle z_{T+133}, \triangle z_{T+134}, \ldots, \triangle z_{T+n+135})$.
$(\triangle z_{T+145}, \triangle z_{T+146}, \triangle z_{T+147}) = (\triangle z_{T+67}, \triangle z_{T+68}, \triangle z_{T+69})$,
$\triangle z_{T+t} = 0$ *for other* t *such that* $n + 1 \leq t \leq 147$.
(7) *If* $(\triangle z_{T+67}, \triangle z_{T+68}, \ldots, \triangle z_{T+n+69}) = (0, 0, \ldots, 0)$,
$(\triangle z_{T+n+1}, \triangle z_{T+n+2}, \ldots) = (0, 0, \ldots,)$ *is a zero stream.*

Proof First, we observe the state differential at time T.
$(\triangle s_{(T,93)}, \triangle s_{(T,92)}, \ldots, \triangle s_{(T,93-n)}) = (1, *, \ldots, *, 1)$,
If $M = T(P_H = 93)$, $\triangle s_{(T,j)} = 0$ for each $j \notin \{93 - n, 94 - n, \ldots, 93\}$.
If $M = T - 1(P_H = 92)$,
$\triangle s_{(T,94)} = \triangle(s_{(T-1,91)} s_{(T-1,92)} + s_{(T-1,93)}) = *$,
$\triangle s_{(T,j)} = 0$ for each $j \notin \{93 - n, 94 - n, \ldots, , 93, 94\}$.

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

Suppose $M = T - 2$ and $(\triangle s_{(T,95)}, \triangle s_{(T,94)}) = (0, 1)$. Then we can equivalently take $M = T - 1$.

Suppose $M \leq T - 1$ and $(\triangle s_{(T,95)}, \triangle s_{(T,94)}) = (0, 0)$. Then we can equivalently take $M = T$.

Second, we can obtain the state differential at time $T + 67$:

$$(\triangle s_{(T+67,162)}, \triangle s_{(T+67,161)} \ldots, \triangle s_{(T+67,160-n)})$$
$$= (\triangle s_{(T,95)}, \triangle s_{(T,94)}, \triangle(s_{(T,91)} s_{(T,92)} + s_{(T,93)}), \triangle(s_{(T,90)} s_{(T,91)} + s_{(T,92)}), \ldots,$$
$$\triangle(s_{(T,91-n)} s_{(T,92-n)} + s_{(T,93-n)}))$$

$\triangle s_{(T+67,j)}) = 0$ for other j.

Finally, by using Appendix B and the state differential at time $T+67$, it is easy to compute $(\triangle z_{T+67}, \triangle z_{T+68}, \ldots, \triangle z_{T+147})$. Lemma 6 is clear. □

By similar proving procedure with Lemma 6, we can see that Lemmas 7 and 8 are true.

Lemma 7 *Suppose* $172 \leq P_L \leq 177$. *Equivalently take* $T-2 \leq M \leq T$ *and* $175 \leq P_H \leq 177$. *Then*

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

(2) $\triangle z_{T+t} = 0$ *for* $n+1 \leq t \leq 63$. *So that* $k-n \geq 57$.

(3) *If* $(\triangle z_{T+64}, \triangle z_{T+65}) = (1, *)$, *we can equivalently take* $M = T-2$, *and* $A = \{t|175-n \leq t \leq 175, \triangle z_{T-t+175} = 1\}$.

(4) *If* $(\triangle z_{T+64}, \triangle z_{T+65}) = (0, 1)$, *we can equivalently take* $M = T-1$, *and* $A = \{t|176-n \leq t \leq 176, \triangle z_{T-t+176} = 1\}$.

(5) *If* $(\triangle z_{T+64}, \triangle z_{T+65}) = (0, 0)$, *we can equivalently take* $M = T$, *and* $A = \{t|177-n \leq t \leq 177, \triangle z_{T-t+177} = 1\}$.

(6) $(\triangle z_{T+64}, \triangle z_{T+65}, \ldots, \triangle z_{T+n+66})$
$=(\triangle z_{T+109}, \triangle z_{T+110}, \ldots, \triangle z_{T+n+111})$
$=(\triangle z_{T+130}, \triangle z_{T+131}, \ldots, \triangle z_{T+n+132})$.
$\triangle z_{T+t} = 0$ *for other* t *such that* $n+1 \leq t \leq 147$.

(7) *If* $(\triangle z_{T+64}, \triangle z_{T+65}, \ldots, \triangle z_{T+n+66}) = (0, 0, \ldots, 0)$, *then*
$(\triangle z_{T+n+1}, \triangle z_{T+n+2}, \ldots) = (0, 0, \ldots,)$ *is a zero stream.*

Lemma 8 *Suppose* $265 \leq P_L \leq 288$. *Equivalently take* $T-2 \leq M \leq T$ *and* $286 \leq P_H \leq 288$. *Then*

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

(2) $\triangle z_{T+t} = 0$ *for* $n+1 \leq t \leq 63$. *So that* $k-n \geq 57$.

(3) *If* $(\triangle z_{T+64}, \triangle z_{T+65}) = (1, *)$, *we can equivalently take* $M = T-2$, *and* $A = \{t|286-n \leq t \leq 286, \triangle z_{T-t+286} = 1\}$.

(4) *If* $(\triangle z_{T+64}, \triangle z_{T+65}) = (0, 1)$, *we can equivalently take* $M = T-1$, *and* $A = \{t|287-n \leq t \leq 287, \triangle z_{T-t+287} = 1\}$.

(5) *If* $(\triangle z_{T+64}, \triangle z_{T+65}) = (0, 0)$, *we can equivalently take* $M = T$, *and* $A = \{t|288-n \leq t \leq 288, \triangle z_{T-t+288} = 1\}$.

(6) $(\triangle z_{T+64}, \triangle z_{T+65}, \ldots, \triangle z_{T+n+66}) = (\triangle z_{T+91}, \triangle z_{T+92}, \ldots, \triangle z_{T+n+93})$,
$\triangle z_{T+t} = 0$ *for other* t *such that* $n+1 \leq t \leq 147$.

(7) *If* $(\triangle z_{T+64}, \triangle z_{T+65}, \ldots, \triangle z_{T+n+66}) = (0, 0, \ldots, 0)$, *then*
$(\triangle z_{T+n+1}, \triangle z_{T+n+2}, \ldots) = (0, 0, \ldots)$ *is a zero stream.*

Lemma 9 *Suppose* $67 \leq P_L \leq 69$. *Equivalently take* $\triangle s_{(M,69)} = 1$ *and* $P_H \geq 69$. *Then there is unique* m, $max\{0, n-2\} \leq m \leq n$, *such that*

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

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

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

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

(5) $k-n = 42$.

(6) $M = T - 24 + m$, *and the fault positions are of the set*

$$A = \{t | 69 - n + m \leq t \leq 69 + m, \triangle z_{T-t+m+69} = 1\}.$$

(7) $(\triangle z_{T+99}, \triangle z_{T+100}, \ldots, \triangle z_{T+125}) = (0, 0, \ldots, 0)$.

Proof Denote $m = P_H - 69$, then $n - m = 69 - P_L, max\{0, n-2\} \leq m \leq n \leq 7$. 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.

$$(\triangle s_{(M,69-n+m)}, \ldots, \triangle s_{(M,69+m)}) = (1, *, \ldots, *, 1), \quad \text{where } \triangle s_{(M,69)} = 1.$$
$$\triangle s_{(M,j)} = 0 \quad \text{for other } j.$$

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

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

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

$$(\triangle s_{(T,24-n)}, \ldots, \triangle s_{(T,24-m)}) = (\triangle s_{(M,69-n+m)}, \ldots, \triangle s_{(M,69)}) = (1, *, \ldots, *, 1).$$
$$(\triangle s_{(T,94)}, \triangle s_{(T,95)})$$
$$= (\triangle(s_{(M,68+m)} s_{(M,69+m)} + s_{(M,70+m)}), \triangle(s_{(M,69+m)} s_{(M,70+m)} + s_{(M,71+m)}))$$
$$= (*, *).$$
$$\triangle s_{(T,j)} = 0 \text{ for each } j \notin \{24-n, 25-n, \ldots, 24-m, 93-n, 94-n, \ldots, 93, 94, 95\}.$$

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

$$(\triangle z_T, \triangle z_{T+1}, \ldots, \triangle z_{T+n})$$
$$= (\triangle s_{(T,93)}, \triangle s_{(T,92)}, \ldots, \triangle s_{(T,93-n)})$$
$$= (1, *, \ldots, *, 1), \quad \text{where } \triangle z_{T+m} = 1.$$
$$(\triangle z_{T+n+1}, \triangle z_{T+n+2}, \ldots, \triangle z_{T+m+41}) = (0, \ldots, 0)$$
$$(\triangle z_{T+m+42}, \triangle z_{T+m+43}, \ldots, \triangle z_{T+n+42})$$
$$= (\triangle s_{(T,24-m)}, \triangle s_{(T,23-m)}, \ldots, \triangle s_{(T,24-n)})$$
$$= (1, *, \ldots, *, 1).$$
$$(\triangle z_{T+n+43}, \triangle z_{T+n+44}, \ldots, \triangle z_{T+66}) = (0, \ldots, 0).$$
$$(\triangle z_{T+99}, \triangle z_{T+100}, \ldots, \triangle z_{T+125}) = (0, \ldots, 0).$$

Lemma 9 is proved. □

Lemma 10 *Suppose* $163 \leq P_L \leq 171$. *Equivalently take* $\triangle s_{(M,171)} = 1$ *and* $P_H \geq 171$. *Then there is unique* m, $0 \leq m \leq n$, *such that*

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

(2) $(\triangle z_{T+n+1}, \triangle z_{T+n+2}, \ldots, \triangle z_{T+62}) = (0, 0 \ldots, 0)$. *So that* $k - n \geq 56$.

(3) $(\triangle z_{T+n+1}, \triangle z_{T+n+2}, \ldots, \triangle z_{T+140})$ *can be decomposed as*

$$(\triangle z_{T+n+1}, \triangle z_{T+n+2}, \ldots, \triangle z_{T+140})$$
$$=(\triangle u_{T+n+1}, \triangle u_{T+n+2}, \ldots, \triangle u_{T+140}) + (\triangle v_{T+n+1}, \triangle v_{T+n+2}, \ldots, \triangle v_{T+140}).$$

$(\triangle u_{T+n+1}, \triangle u_{T+n+2}, \ldots, \triangle u_{T+140})$ *is of the following shape.*

$$(\triangle u_{T+64}, \triangle u_{T+65}, \ldots, \triangle u_{T+n+66})$$
$$=(\triangle u_{T+109}, \triangle u_{T+110}, \ldots, \triangle u_{T+n+111})$$

$=(\triangle u_{T+130}, \triangle u_{T+131}, \ldots, \triangle u_{T+n+132})$
$=(*, \ldots, *)$,
$\triangle u_{T+j} = 0$ *for other* $j \in \{n+1, n+2, \ldots, 140\}$. $(\triangle v_{T+n+1}, \triangle v_{T+n+2}, \ldots, \triangle v_{T+140})$ *is of the following shape.*
$(\triangle v_{T+m+63}, \triangle v_{T+m+64}, \ldots, \triangle v_{T+n+63})$
$=(\triangle v_{T+m+78}, \triangle v_{T+m+79}, \ldots, \triangle v_{T+n+78})$
$=(\triangle v_{T+m+129}, \triangle v_{T+m+130}, \ldots, \triangle v_{T+n+129})$
$=(1, *, \ldots, *, 1)$,
$\triangle v_{T+j} = 0$ *for other* $j \in \{n+1, n+2, \ldots, 140\}$.

(4) $M = T - 6 + m$, *and* $A = \{t | 171 - n + m \le t \le 171 + m, \triangle z_{T-t+m+171} = 1\}$.
(5) m *is the smallest* t *such that* $0 \le t \le 7$ *and* $\triangle z_{T+t+78} = 1$.

Proof Denote $n = P_H - P_L$, $m = P_H - 171$, then $n - m = 171 - P_L$, $0 \le m \le n$. 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.

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

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

So that, at time $T + n + 1$, the state differential is the follow.

$$\begin{aligned}
&(\triangle s_{(T+n+1,178)}, \triangle s_{(T+n+1,179)}, \ldots, \triangle s_{(T+n+1,178+n)}, \triangle s_{(T+n+1,179+n)}, \triangle s_{(T+n+1,180+n)})\\
&\quad = (\triangle(s_{(T,175-n)}s_{(T,176-n)} + s_{(T,177-n)}), \triangle(s_{(T,176-n)}s_{(T,177-n)} + s_{(T,178-n)}), \ldots,\\
&\triangle(s_{(T,175)}s_{(T,176)} + s_{(T,177)}), \triangle(s_{(T-1,175)}s_{(T-1,176)} + s_{(T-1,177)}),\\
&\triangle(s_{(T-2,175)}s_{(T-2,176)} + s_{(T-2,177)}))\\
&\quad = (*, \ldots, *),\\
&(\triangle s_{(T+n+1,100)}, \ldots, \triangle s_{(T+n+1,100-m+n)})\\
&\quad = (\triangle s_{(M,171-n+m)}, \ldots, \triangle s_{(M,171)})\\
&\quad = (1, *, \ldots, *, 1).\\
&\triangle s_{(T+n+1,j)} = 0 foreachj \notin \{100, 101, \ldots, 100 - m + n, 178, 179, \ldots, 180 + n\}.
\end{aligned}$$

According to Appendix B and the state differential at time $T + n + 1$, we have completely proved Lemma 10. □

Lemma 11 *Suppose* $244 \le P_L \le 264$. *Equivalently take* $\triangle s_{(M,264)} = 1$ *and* $P_H \ge 264$. *Then there is unique* m, $0 \le m \le n$, *such that*

(1) $(\triangle z_T, \triangle z_{T+1}, \ldots, \triangle z_{T+n}) = (1, *, \ldots, *, 1)$, *where* $\triangle z_{T+m} = 1$.
(2) $(\triangle z_{T+n+1}, \triangle z_{T+n+2}, \ldots, \triangle z_{T+m+41}) = (0, 0, \ldots, 0)$.
(3) $(\triangle z_{T+m+42}, \triangle z_{T+m+43}, \ldots, \triangle z_{T+n+42})$
$=(\triangle z_{T+m}, \triangle z_{T+1+m}, \ldots, \triangle z_{T+n})$
$=(1, *, \ldots, *, 1)$.
(4) $(\triangle z_{T+n+43}, \triangle z_{T+n+44}, \ldots, \triangle z_{T+63}) = (0, 0, \ldots, 0)$.
(5) $k - n = 42$.
(6) $M = T - 24 + m$, *and* $A = \{t | 264 - n + m \le t \le 264 + m, \triangle z_{T-t+m+264} = 1\}$.
(7) $(\triangle z_{T+m+108}, \triangle z_{T+m+109}, \ldots, \triangle z_{T+n+108}) = (1, *, \ldots, *, 1)$.

Proof Denote $m = P_H - 264$, then $n - m = 264 - P_L$, $0 \le m \le n \le 7$. 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.

$$(\triangle s_{(M,264-n+m)}, \ldots, \triangle s_{(M,264+m)}) = (1, *, \ldots, *, 1), \quad \text{where} \triangle s_{(M,264)} = 1.$$
$$\triangle s_{(M,j)} = 0 \quad \text{for other} j.$$

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

$$\begin{aligned}
&(\triangle s_{(T,288-n)}, \ldots, \triangle s_{(T,288)})\\
&\quad = (\triangle s_{(M,264-n+m)}, \ldots, \triangle s_{(M,264+m)})\\
&\quad = (1, *, \ldots, *, 1), \quad \text{where}\\
&\triangle s_{(T,288-m)} = \triangle s_{(M,264)} = 1.\\
&(\triangle s_{(T,201-n)}, \ldots, \triangle s_{(T,201-m)})\\
&\quad = (\triangle s_{(M,264-n+m)}, \ldots, \triangle s_{(M,264)})\\
&\quad = (1, *, \ldots, *, 1).\\
&(\triangle s_{(T,1)}, \triangle s_{(T,2)})\\
&\quad = (\triangle(s_{(M,263+m)} s_{(M,264+m)} + s_{(M,265+m)}), \triangle(s_{(M,264+m)} s_{(M,265+m)} + s_{(M,266+m)}))\\
&\quad = (*, *).
\end{aligned}$$

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

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

$$\begin{aligned}
&(\triangle z_T, \triangle z_{T+1}, \ldots, \triangle z_{T+n})\\
&\quad = (\triangle s_{(T,288-n)}, \ldots, \triangle s_{(T,288)})\\
&\quad = (1, *, \ldots, *, 1), \quad \text{where } \triangle z_{T+m} = 1.\\
&(\triangle z_{T+n+1}, \triangle z_{T+n+2}, \ldots, \triangle z_{T+m+41}) = (0, \ldots, 0).\\
&(\triangle z_{T+m+42}, \triangle z_{T+m+43}, \ldots, \triangle z_{T+n+42})\\
&\quad = (\triangle s_{(T,201-m)}, \ldots, \triangle s_{(T,201-n)})\\
&\quad = (1, *, \ldots, *, 1).\\
&(\triangle z_{T+n+43}, \triangle z_{T+n+44}, \ldots, \triangle z_{T+63}) = (0, 0, \ldots, 0).\\
&(\triangle z_{T+m+108}, \triangle z_{T+m+109}, \ldots, \triangle z_{T+n+108})\\
&\quad = (\triangle s_{(T,201-m)}, \ldots, \triangle s_{(T,201-n)})\\
&\quad = (1, *, \ldots, *, 1).
\end{aligned}$$

Lemma 11 is proved. □

3.2 Case checking

By Lemmas 1–11 we know that, if the attacker knows which case it is from 9 cases $\{1 \le P_L \le 66, 67 \le P_L \le 69, 70 \le P_L \le 93, 94 \le P_L \le 162, 163 \le P_L \le 171, 172 \le P_L \le 177, 178 \le P_L \le 243, 244 \le P_L \le 264, 265 \le P_L \le 288\}$, the injection time and the fault positions (M, A) can be determined. So that we need only to check the cases.

Propositions 1–4 are clear by Lemmas 3–11.

Proposition 1

(1) *The value of* $k-n$ *comes from* $\{27, 15, 45, 42, [56, +\infty)\}$.
(2) *If* $k-n=27$, *the case is* $1 \le P_L \le 66$.
(3) *If* $k-n=15$, *the case is* $94 \le P_L \le 162$.
(4) *If* $k-n=45$, *the case is* $178 \le P_L \le 243$.
(5) *If* $k-n=42$, *the case is from* $\{67 \le P_L \le 69, 244 \le P_L \le 264\}$.
(6) *If* $k-n \in [56, +\infty)$, *the case is from* $\{70 \le P_L \le 93, 163 \le P_L \le 171, 172 \le P_L \le 177, 265 \le P_L \le 288\}$.

Proposition 2 *Suppose* $k-n=42$ *(so that the case is from* $\{67 \le P_L \le 69, 244 \le P_L \le 264\}$*). If* $(\triangle z_{T+108}, \triangle z_{T+109}, \ldots, \triangle z_{T+n+108}) = (0, 0, \ldots, 0)$, *the case is* $67 \le P_L \le 69$, *or else the case is* $244 \le P_L \le 264$.

Proposition 3 *Suppose* $k-n \in [56, +\infty)$ *(so that the case is from* $\{70 \le P_L \le 93, 163 \le P_L \le 171, 172 \le P_L \le 177, 265 \le P_L \le 288\}$*). If* $(\triangle z_{T+140}, \triangle z_{T+141}, \ldots, \triangle z_{T+147}) \ne (0, 0, \ldots, 0)$, *the case is from* $\{70 \le P_L \le 93, 163 \le P_L \le 171\}$, *or else the case is from* $\{70 \le P_L \le 93, 172 \le P_L \le 177, 265 \le P_L \le 288\}$.

Proposition 4 *Suppose* $k-n \in [56, +\infty)$ *and* $(\triangle z_{T+140}, \triangle z_{T+141}, \ldots, \triangle z_{T+147}) = (0, 0, \ldots, 0)$ *(so that the case is from* $\{70 \le P_L \le 93, 172 \le P_L \le 177, 265 \le P_L \le 288\}$.

(1) *If* $(\triangle z_{T+109}, \triangle z_{T+110}, \ldots, \triangle z_{T+118}) \ne (0, 0, \ldots, 0)$, *the case is* $172 \le P_L \le 177$.
(2) *If* $(\triangle z_{T+109}, \triangle z_{T+110}, \ldots, \triangle z_{T+118}) = (0, 0, \ldots, 0)$, *and*
$(\triangle z_{T+133}, \triangle z_{T+134}, \ldots, \triangle z_{T+147}) \ne (0, 0, \ldots, 0)$,
the case is$70 \le P_L \le 93$.
(3) *If* $(\triangle z_{T+109}, \triangle z_{T+110}, \ldots, \triangle z_{T+118}) = (0, 0, \ldots, 0)$,
$(\triangle z_{T+133}, \triangle z_{T+134}, \ldots, \triangle z_{T+147}) = (0, 0, \ldots, 0)$, *and*
$(\triangle z_{T+91}, \triangle z_{T+92}, \ldots, \triangle z_{T+100}) \ne (0, 0, \ldots, 0)$,
the case is $265 \le P_L \le 288$.
(4) *If* $(\triangle z_{T+109}, \triangle z_{T+110}, \ldots, \triangle z_{T+118}) = (0, 0, \ldots, 0)$,
$(\triangle z_{T+133}, \triangle z_{T+134}, \ldots, \triangle z_{T+147}) = (0, 0, \ldots, 0)$, *and*
$(\triangle z_{T+91}, \triangle z_{T+92}, \ldots, \triangle z_{T+100}) = (0, 0, \ldots, 0)$, *then*
$\triangle z_{T+n+1} \triangle z_{T+n+2} \ldots = 00\ldots$ *is a zero stream.*

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

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

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 $n+1 \le t \le 147$.

Lemma 12 *Suppose the case is* $163 \le P_L \le 171$, *and* $\triangle z_T \triangle z_{T+1} \triangle z_{T+2} \ldots \triangle z_{T+147}$ *possesses the features of the case* $70 \le P_L \le 93$. *Then we have*

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

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

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

Proof According to Lemma 10,
$(\triangle z_{T+n+1}, \triangle z_{T+n+2}, \ldots, \triangle z_{T+147}) =$
$(\triangle u_{T+n+1}, \triangle u_{T+n+2}, \ldots, \triangle u_{T+147}) + (\triangle v_{T+n+1}, \triangle v_{T+n+2}, \ldots, \triangle v_{T+147})$.
Because
$(\triangle v_{T+109}, \triangle v_{T+110}, \ldots, \triangle v_{T+n+111}) = (0, 0, \ldots, 0)$,
$(\triangle z_{T+109}, \triangle z_{T+110}, \ldots, \triangle z_{T+n+111}) = (\triangle u_{T+109}, \triangle u_{T+110}, \ldots, \triangle u_{T+n+111})$.
Again because
$(\triangle z_{T+109}, \triangle z_{T+110}, \ldots, \triangle z_{T+n+111}) = (0, 0, \ldots, 0)$,
$(\triangle u_{T+109}, \triangle u_{T+110}, \ldots, \triangle u_{T+n+111}) = (0, 0, \ldots, 0)$.
So that $(\triangle u_{T+n+1}, \triangle u_{T+n+2}, \ldots, \triangle u_{T+147})$ is a 0 string, and that
$(\triangle z_{T+n+1}, \triangle z_{T+n+2}, \ldots, \triangle z_{T+147}) = (\triangle v_{T+n+1}, \triangle v_{T+n+2}, \ldots, \triangle v_{T+147})$.
Notice that

$$(\triangle v_{T+m+63}, \triangle v_{T+m+64}, \ldots, \triangle v_{T+n+63}) = (1, *, \ldots, *, 1)$$

for some m such that $m \leq n \leq 7$. 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 $4 \leq m \leq n \leq 7$. By Lemma 10, Lemma 12 is proved. □

Proposition 5 *Suppose* $k - n \in [56, +\infty)$, *and* $(\triangle z_{T+140}, \triangle z_{T+141}, \ldots, \triangle z_{T+147}) \neq (0, 0, \ldots, 0)$ (*so that the case is from* $\{70 \leq P_L \leq 93, 163 \leq P_L \leq 171\}$).

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

(2) *If* $\triangle z_T \triangle z_{T+1} \triangle z_{T+2} \ldots \triangle z_{T+147}$ *possesses the features of case* $70 \leq P_L \leq 93$, *and at least one of the features of Lemma* 12 *does not hold, the case is* $70 \leq P_L \leq 93$.

(3) *If* $\triangle z_T \triangle z_{T+1} \triangle z_{T+2} \ldots \triangle z_{T+147}$ *possesses features of the case* $70 \leq P_L \leq 93$, *and all features of Lemma* 12 *hold, we can not check which case is from* $\{70 \leq P_L \leq 93, 163 \leq P_L \leq 171\}$. *But the state differential at time* $T + n + 1$ *can be uniquely determined as the follow,*

$$\begin{aligned}
&(\triangle s_{(T+n+1,100)}, \triangle s_{(T+n+1,101)}, \ldots, \triangle s_{(T+n+1,100-m+n)})\\
&\quad = (\triangle z_{63+n}, \triangle z_{62+n}, \ldots, \triangle z_{63+m})\\
&\quad = (1, *, \ldots, *, 1)\\
&\triangle s_{(T+n+1,j)} = 0 \quad for\ other\ j.
\end{aligned}$$

Proof (1) and (2) are clear.

Suppose the case is $163 \leq P_L \leq 171$, $\triangle z_T \triangle z_{T+1} \triangle z_{T+2} \ldots \triangle z_{T+147}$ possesses features of the case $70 \leq P_L \leq 93$, and all features of Lemma 12 hold. Then the state differential at time $T + n + 1$ is the follow,

$$\begin{aligned}
&(\triangle s_{(T+n+1,100)}, \triangle s_{(T+n+1,101)}, \ldots, \triangle s_{(T+n+1,100-m+n)})\\
&\quad = (\triangle z_{63+n}, \triangle z_{62+n}, \ldots, \triangle z_{63+m})\\
&\quad = (1, *, \ldots, *, 1)\\
&\triangle s_{(T+n+1,j)} = 0 \quad \text{for other } j.
\end{aligned}$$

Again suppose the case is $70 \leq P_L \leq 93$, and all features of Lemma 12 hold. Then the state differential at time $T+n+1$ can be determined, as the follow,

$$(\triangle s_{(T+n+1,94)}, \triangle s_{(T+n+1,95)}, \ldots, \triangle s_{(T+n+1,96+n)}) = (\triangle z_{69+n}, \triangle z_{68+n}, \ldots, \triangle z_{67})$$
$$\triangle s_{(T+n+1,j)} = 0 \quad \text{for other } j.$$

On the other hand, Lemma 12 tells us

$$(\triangle z_{69+n}, \triangle z_{68+n}, \ldots, \triangle z_{64+n}) = (0, 0, \ldots, 0)$$
$$(\triangle z_{63+n}, \triangle z_{62+n}, \ldots, \triangle z_{63+m}) = (1, *, \ldots, *, 1)$$
$$(\triangle z_{62+m}, \triangle z_{61+m}, \ldots, \triangle z_{67}) = (0, 0, \ldots, 0)$$

(3) is true.

Proposition 5 is proved. □

Up to now, we have presented a complete checking routine for determining the case. If the case is determined, the injecting time and fault positions are determined. On two occasions the case can not be determined. The first occasion is Proposition 4 (4), on which $\triangle z_{T+n+1} \triangle z_{T+n+2} \ldots = 00 \ldots$ is a zero string, implying an injecting failure. The second occasion is Proposition 5 (3), which must satisfy rigorous conditions. On the second occasion the state differential at time $T+n+1$ is determined, which is sufficient for our fault attack. Besides, these two occasions happen with extremely small probabilities.

4 Fault analysis under our assumptions

4.1 Fault floating

Suppose the attacker has determined (M, A), the injecting time and fault positions. In other words, he has obtained $(\triangle s_{(M,1)}, \triangle s_{(M,2)}, \ldots, \triangle s_{(M,288)})$, the state differential at time M. Then, from 82 original quadratic equations of the state at time M, he can obtain 82 additional equations. But most of these additional equations are identities, other than linear equations. The reason is that the state differential at time M is neither heavy (from point of Hamming weight) nor even (from point of distribution). The idea of floating fault analysis of Trivium, presented by Hojsík and Rudolf [17], is to find an appropriate later time e, such that $(\triangle s_{(e,1)}, \triangle s_{(e,2)}, \ldots, \triangle s_{(e,288)})$ is heavy enough and even enough, so that the attacker can obtain enough number of additional linear equations of the state at time e. Generally speaking, for $t \in \{M, M+1, \ldots, M+800\}$, the larger t is, the heavier and evener the state differential at time t is. A key problem is how to obtain the state differential at a later time from the state differentials at former times. In the follow we present a formal discussion (our new discussion, not presented by [17]).

Definition 1 Suppose the attacker has obtained

- Original key-stream segment $(z_0 z_1 z_2 \ldots z_N)$ and fault injected key-stream segment $(z'_0 z'_1 z'_2 \ldots z'_N)$.
- $(\triangle s_{(t,1)}, \triangle s_{(t,2)}, \ldots, \triangle s_{(t,288)})$.

We say the state differential is floatable at time t, if $(\triangle s_{(t+1,1)}, \triangle s_{(t+1,2)}, \ldots, \triangle s_{(t+1,288)})$ can be induced.

Proposition 6 *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*
$(\triangle s_{(t,76)}, \triangle s_{(t,77)}, \triangle s_{(t,157)}, \triangle s_{(t,158)}, \triangle s_{(t,268)}, \triangle s_{(t,269)}) = (0,0,0,0,0,0)$.

Proposition 6 is easy to be proved, by considering Eqs. 66, 69 and 84 of Appendix B, and by Sect. 2. For example, suppose $(\triangle s_{(t,286)}, \triangle s_{(t,287)}) = (0,0)$ and $(\triangle s_{(t,91)}, \triangle s_{(t,92)}) = (0,0)$.

First, we have $\triangle(s_{(t,286)} s_{(t,287)}) = 0$, $\triangle(s_{(t,91)} s_{(t,92)}) = 0$.

Second, by Eq. 66 of Appendix B, $\triangle(s_{(t,175)} s_{(t,176)})$ can be induced.

Finally, by Sect. 2, $(\triangle s_{(t+1,1)}, \triangle s_{(t+1,2)}, \ldots, \triangle s_{(t+1,288)})$ can be induced from known values of $\{\triangle(s_{(t,91)} s_{(t,92)}), \triangle(s_{(t,175)} s_{(t,176)}), \triangle(s_{(t,286)} s_{(t,287)}), (\triangle s_{(t,1)}, \triangle s_{(t,2)}, \ldots, \triangle s_{(t,288)})\}$.

Definition 2 We call e the floating end, if e is the smallest t such that, at time t, the two conditions of Proposition 6 can not be assured. (In fact, the state differential may still be floatable at or beyond the floating end, but the floatability is much more complicated to be analyzed on those occasions.)

Proposition 7 *By simple checking we have*

In case $1 \le P_L \le 66$, *the floating end is about* $T + 175$,
In case $94 \le P_L \le 162$, *the floating end is about* $T + 169$,
In case $178 \le P_L \le 243$, *the floating end is about* $T + 134$,
In case $70 \le P_L \le 93$, *the floating end is about* $T + 236$,
In case $172 \le P_L \le 177$, *the floating end is about* $T + 198$,
In case $1265 \le P_L \le 288$, *the floating end is about* $T + 227$,
In case $244 \le P_L \le 264$, *the floating end is about* $T + 195$,
In case $163 \le P_L \le 171$, *the floating end is about* $T + 161$,
In case $67 \le P_L \le 69$, *the floating end is not smaller than* $T + 130$.

4.2 Repeated fault injections

Besides their Assumptions 1 and 2, Hojsík and Rudolf [16,17] allowed repeated fault injection procedures. They had Assumption 5.

Assumption 5 The attacker can make such fault injection many times for the same initial state.

Hojsík and Rudolf then presented their result [17] under Assumptions 1, 2 and 5. Averagely 3.2 fault injections will break Trivium, by using averagely 800×4.2 key-stream bits. They guessed [17] the attack would be more effective if one-bit-fault-injection could be changed to multi-bit-fault-injection (that is, Assumption 2 could be changed, for example, to Assumption 4).

To break Trivium, our fault analysis also needs repeated fault injection procedures. Here we present our probabilistic assumptions, as a complement to our fault model. At initial time, the state is uniformly distributed. At time M, random faults appear in the positions $\{m, m+1, \ldots, m+7\}$, where m is uniformly distributed in the set $\{1, 2, \ldots, 86\} \cup \{94, 95, \ldots, 170\} \cup \{178, 179, \ldots, 281\}$. At each of 8 positions $\{m, m+1, \ldots, m+7\}$, 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.

In repeated fault injections, the attacker will obtain various floating ends from various fault injection procedures. But he does not want to obtain linear equations of the state at various floating ends. He hopes to accumulate enough linear equations of the state at such a common time, which is the minimum value of various floating ends. By this reason, the randomness of the injecting time M should be limited. So that we modify Assumption 3 into Assumption 6.

Assumption 6 We can make fault injection on the state at a random time M, where M has a uniform distribution over $\{0, 1, \dots, M_0\}$, M_0 is a fixed integer.

We set up our attack on Trivium under Assumptions 4, 5 and 6. We are only interested in accumulating enough number of linear equations of the state at some known time e, without caring how to solve the equations. If we obtain not less than 200 additional linear equations of the state at some known time e, we will say that Trivium can be broken. Notice that the state is a register including 288 bits. By considering 66 original linear equations, not less than 266 linear equations, about the state at time e, are obtained. There is a rank reduction in these linear equations, but they are enough for breaking Trivium, by careful solving, by a small number of guesses, and by combining with a large number of pair quadratic equations. 82 original equations are pair quadratic equations, as well as several additional equations. Special structures of pair quadratic equations make them quite helpful for solving the state. For example, if some bits could be solved out from linear equations, some pair quadratic terms are changed into linear terms. So that a pair quadratic equation can easily be changed into a linear equation, under some weak conditions. Now we take the known time e as the minimum value of various floating ends in various fault injection procedures. We repeat the fault injection procedure until we obtain not less than 200 additional linear equations of the state at such common time. Notice that such common time changes as the fault injection procedure repeats. This is a problem difficult to be theoretically analyzed, so that we use random simulations. We construct a random experiment, as the follow.

```
Step 1  Generate $(\triangle s_{(0,1)}, \dots, \triangle s_{(0,288)})$, the initial state, with uniform distribution.
Step 2  $N$:=0, $B_N$:=0, $e := +\infty$.
Step 3  If $B_N \geq 200$, output $N$.
Step 4  Start the state renewal procedure of Trivium by such initial state
        $(\triangle s_{(0,1)}, \dots, \triangle s_{(0,288)})$.
Step 5  Generate $M_{N+1}$, the injecting time, with uniform distribution over $\{0, 1, , \dots, M_0\}$.
Step 6  Generate $A_{N+1}$, the set of fault positions of the state at time $M_{N+1}$, with the distri-
        bution described in our probabilistic assumptions.
Step 7  Obtain $end_{N+1}$, the floating end of such injection $(M_{N+1}, A_{N+1})$.
Step 8  $e$ :=min$\{e, end_{N+1}\}$.
Step 9  $N$:=$N + 1$.
Step 10 Count $B_N$, the total number of additional linear equations of the state at time $e$, by
        $N$ injections $\{M_1, A_1\}, \{M_2, A_2\}, \dots, \{M_N, A_N\}$.
Step 11 Go to Step 3.
```

Step 10 can be specifically described as follows. Take $(\triangle s_{(e,1)}, \dots, \triangle s_{(e,288)})$, the state differential at time e. Take an original pair quadratic equation. If '1' entries of the state differential overlap quadratic terms' entries of the equation, the corresponding additional equation is a linear equation, or else the corresponding additional equation is an identity.

4.3 Results and comparisons

For fixed value of M_0, we repeat this random experiment 1,000 times, and compute $\overline{N}$, the average value of N. Our experiment results are as follows.

Under our probabilistic assumptions, the floating end has an expectation value 195. So that, for each fault injection procedure, averagely 195 fault injected key-stream bits are needed.

> For $M_0 = 0$, averagely 3.7 repeated fault injection procedures will break Trivium, by averagely observing 195×4.7 key-stream bits.
> For $M_0 = 1$, averagely 4.0 repeated fault injection procedures will break Trivium, by averagely observing 195×5.0 key-stream bits.
> For $M_0 = 2$, averagely 4.3repeated fault injection procedures will break Trivium, by averagely observing 195×5.3 key-stream bits.
> For $M_0 = 4$, averagely 5.4 repeated fault injection procedures will break Trivium, by averagely observing 195×6.4 key-stream bits.
> For $M_0 = 8$, averagely 7.6 repeated fault injection procedures will break Trivium, by averagely observing 195×8.6 key-stream bits.
> For $M_0 = 16$, averagely 10.0 repeated fault injection procedures will break Trivium, by averagely observing 195×11.0 key-stream bits.
> For $M_0 = 32$, averagely no more than 16 repeated fault injection procedures will break Trivium, by averagely observing no more than 195×17.0 key-stream bits.

Our result for $M_0 = 0$ is comparable with the result of Hojsík and Rudolf. Averagely 3.7 vs. 3.2 fault injections will break Trivium, by averagely observing 195×4.7 vs. 800×4.2 key-stream bits. From these comparisons, we can say that our model $M_0 = 0$ is similarly effective with the model of Hojsík and Rudolf, for fault attack.

We find that, 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.

5 Conclusion

The stream cipher Trivium is on the edge of low cost and compactness, but it can not resist the fault attack, under conditions as weak as in our paper. As a result, Trivium should be well protected against all types of micro-probing. Micro-probing is the physical basis of any fault analysis. The weaker the fault model, the easier the corresponding micro-probing.

Our attack model is only limited to Trivium. Fault attacks to other eSTREAM candidates need much stronger assumptions. Besides the interests of specialists, our work is valuable for practical micro-probing, because we present a practical method for solving the state.

Acknowledgments This paper is supported by the 973 project (No.2007CB311201), the Natural Science Foundation of China (No.60833008), the 111 project (No.B08038) and the Foundation of Guangxi Key Laboratory of Information and Communication (20902).

Appendix

A Trivium algorithm

See Figs. 1 and 2.

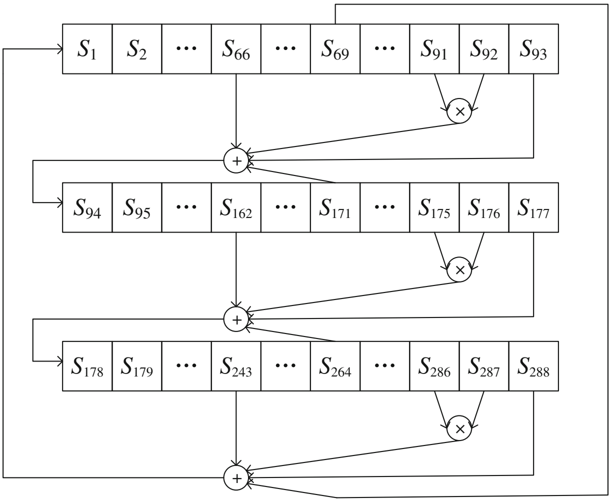

Fig. 1 State renewal

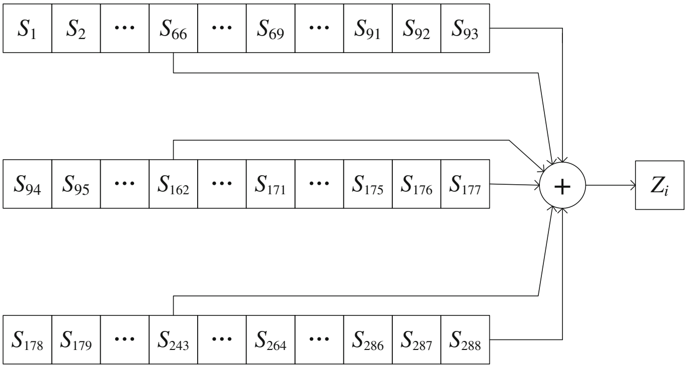

Fig. 2 Stream bits output

B Trivium original equations

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

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

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

$$\cdots \qquad \cdots$$

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

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

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

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

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

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

$$\dots \tag*{$\dots$}$$

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

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

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

$$\dots \tag*{$\dots$}$$

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

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

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

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

$$\dots \tag*{$\dots$}$$

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

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

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

$$\dots \tag*{$\dots$}$$

$$\begin{aligned} z_{131} &= s_{19} + s_{29}s_{30} + s_{44}s_{45} + s_{46} + s_{97} + s_{109} + s_{110}s_{111} + s_{112} + s_{124} + s_{142} + s_{155}s_{156} \\ &\quad + s_{157} + s_{178} + s_{199} + s_{205} + s_{221}s_{222} + s_{223} + s_{244} + s_{248}s_{249} + s_{250} \end{aligned} \tag{131}$$

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

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

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

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

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

$$\cdots \qquad \cdots$$

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

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

References

1. Cannière C.D., Preneel B.: Trivium: a stream cipher construction inspired by block cipher design principle. eSTREAM, ECRYPT Stream Cipher Project, Report 2005/30. http://www.ecrypt.eu.org/stream (2005). Accessed 30 June 2006.
2. Cannière C.D., Preneel B.: Trivium specifications. www.ecrypt.eu.org/stream/p3ciphers/trivium/trivium_p3.pdf (2007). Accessed 29 Apr 2007.
3. Raddum H.: Cryptanalytic results on Trivium. eSTREAM, ECRYPT Stream Cipher Project, Report 2006/039. http://www.ecrypt.eu.org/stream (2006). Accessed 3 Apr 2006.
4. Maximov A., Biryukov A.: Two trivial attacks on Trivium. eSTREAM, ECRYPT Stream Cipher Project, Report 2007/006. http://www.ecrypt.eu.org/stream (2007). Accessed 29 Apr 2007.
5. Babbage S.: Some thoughts on Trivium. eSTREAM, ECRYPT Stream Cipher Project, Report 2007/007. http://www.ecrypt.eu.org/stream (2007). Accessed 29 Apr 2007.
6. Turan M.S., Kara O.: Linear approximations for 2-round Trivium. eSTREAM, ECRYPT Stream Cipher Project, Report 2007/008. http://www.ecrypt.eu.org/stream (2007). Accessed 29 Apr 2007.
7. Hwang D., Chaney M., Karanam S., Ton N., Gaj K.: 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. http://www.ecrypt.eu.org/stream (2008). Accessed 10 Mar 2009.
8. Good T., Benaissa M.: 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. http://www.ecrypt.eu.org/stream (2008). Accessed 10 Mar 2009.
9. Biham E., Dunkelman O.: Differential cryptanalysis in stream ciphers. COSIC internal report (2007).
10. Rechberger C., Oswald E.: Stream ciphers and side-channel analysis. In: SASC 2004—The State of the Art of Stream Ciphers, Workshop Record, pp. 320–326. http://www.ecrypt.eu.org/stream (2004). Accessed 9 Apr 2005.

11. Fisher W., Gammel B.M., Kniffler O., Velten J.: Differential power analysis of stream ciphers. eSTREAM, ECRYPT Stream Cipher Project, Report 2007/014. http://www.ecrypt.eu.org/stream (2007). Accessed 29 Apr 2007.
12. Hoch J.J., Shamir A.: Fault analysis of stream ciphers. In: Joye M., Quisquater J.-J. (eds.) CHES 2004. LNCS, vol. 3156, pp. 240–253. Springer, Heidelberg (2004).
13. Biham E., Granboulan L., Nguyen P.: 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. http://www.ecrypt.eu.org/stream (2004). Accessed 9 Apr 2005.
14. Gierlichs B., Batina L., Clavier C., Eisenbarth T., Gouget A., Handschuh H., Kasper T., Lemke-Rust K., Mangard S., Moradi A., Oswald E.: Susceptibility of eSTREAM candidates towards side channel analysis. In: SASC 2008—The State of the Art of Stream Ciphers, Workshop Record, pp. 123–150. http://www.ecrypt.eu.org/stream (2008). Accessed 10 Mar 2009.
15. Fisher S., Khazaei S., Meier W.: 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. http://www.ecrypt.eu.org/stream (2008). Accessed 10 Mar 2009.
16. Hojsík M., Rudolf B.: Differential fault analysis of Trivium. In: Nyberg K. (ed.) FSE 2008. LNCS, vol. 5086, pp. 158–172. Springer, Heidelberg (2008).
17. Hojsík M., Rudolf B.: Floating fault analysis of Trivium. In: Chowdhury D.R., Rijmen V., Das A. (eds.) INDOCRYPT 2008. LNCS, vol. 5365, pp. 239–250. Springer, Heidelberg (2008).
18. Biham E., Shamir A.: Differential fault analysis of secret key cryptosystems. In: Advances in Cryptology-CRYPTO'97. LNCS, vol. 1294, pp. 513–525. Springer-Verlag, Berlin, Heidelberg (1997).
19. Pasalic E.: Key differentiation attacks on stream ciphers. Cryptology ePrint Archive. http://eprint.iacr.org/2008/443 (2008). Accessed 12 Dec 2008.
20. Dinur I., Shamir A. Cube attacks on tweakable black box polynomials. Cryptology ePrint Archive. http://eprint.iacr.org/2008/385 (2008). Accessed 12 Dec 2008.
21. Bedi S.S., Pillai N.R.: Cube attacks on Trivium. Cryptology ePrint Archive. http://eprint.iacr.org/2009/015 (2009). Accessed 10 Feb 2009.