

# Certain Observations on ACORN v3 and the Implications to TMDTO Attacks

Akhilesh Anilkumar Siddhanti<sup>1</sup>(✉), Subhamoy Maitra<sup>2</sup>, and Nishant Sinha<sup>3</sup>

<sup>1</sup> BITS Pilani, Goa Campus, Goa, India  
akhileshsiddhanti@gmail.com

<sup>2</sup> Applied Statistics Unit, Indian Statistical Institute,  
203, B. T. Road, Kolkata 700108, India  
subho@isical.ac.in

<sup>3</sup> Department of Computer Science and Engineering,  
Indian Institute of Technology Roorkee, Roorkee 247667, India  
nishantsinha.iitr@gmail.com

**Abstract.** ACORN is a lightweight authenticated cipher which is one of the selected designs among the fifteen third round candidates. This is based on the underlying model of a stream cipher with 6 LFSRs of different lengths and three additional bits. In this paper we consider the scenario that certain amount of key stream bits and some portion of the state is known. Then we try to discover the rest of the state bits. For example, we show that the LFSR of length 47 can be recovered from 47 key stream bits and guessing the rest of the state bits. We also present the implication of such results towards mounting TMDTO attack on ACORN v3. We show that a TMDTO attack can be mounted with preprocessing complexity  $2^{171}$  and  $2^{180}$  (without and with the help of a SAT solver) and the maximum of online time, memory and data complexity  $2^{122}$  and  $2^{120}$  respectively. While our results do not refute any claim of the designer, these observations might be useful for further understanding of the cipher.

**Keywords:** ACORN v3 · Authenticated encryption · CAESAR · Cryptanalysis · Stream cipher

## 1 Introduction

A new competition CAESAR (Competition for Authenticated Encryption: Security, Applicability, and Robustness) [4] has been initiated recently with the first submission deadline in March 2014. The selected candidates of the third round are now available and ACORN v3 is one among those [10]. This is a lightweight authenticated stream cipher composed of 6 Linear Feedback Shift Registers (LFSRs) and four additional bits, making a state size of 293 bits. It promises a 128-bit security using a 128-bit secret key and IV.

Given that the present ciphers are designed with well informed efforts, refuting the designer's claim are quite challenging and sometimes even elusive. However, there are important observations discovered by the cryptanalysts that help

in providing more robust ciphers. This is the reason ACORN has been revised twice and the current version is ACORN v3. In this paper we concentrate on this cipher and try to see how well one can obtain certain portion of the state bits of ACORN v3 given some key stream bits and the rest of the bits of the state. This is related to sampling resistance as noted in [2,3]. In particular, we observe that the LFSR of length 47 ( $S_{107}, \dots, S_{153}$ ) can be recovered from 47 key stream bits and knowing the rest  $293 - 47 = 246$  state bits of ACORN v3. This is achieved by writing a set of several equations and feeding them to a SAT solver such as SAGE [8]. Similarly, the 60 bits ( $S_0, \dots, S_{59}$ ) of the LFSR having length 61 ( $S_0, \dots, S_{60}$ ) could be recovered from 72 key stream bits and the rest 233 state bits of the cipher. This is presented in Sect. 2. This kind of observation helps in mounting Time-Memory-Data-Trade-Off (TMDTO) attack on stream ciphers with varied parameters.

In TMDTO attack, we have four parameters, the preprocessing time  $P$ , the amount of Memory (table in secondary storage) required  $M$ , the amount of Data  $D$  (which is the key stream in case of a stream cipher) and the time  $T$  (the number of accesses to the table, i.e., the secondary storage). In case the key is of  $k$ -bits and all the parameters  $P, M, T, D$  are less than  $2^k$ , then it can be considered as a break. It has been pointed out in [10, Sect. 3.3.2] that as the state size ( $n = 293$ ) of ACORN v3 is more than twice the secret key size ( $k = 128$ ), such an attack is elusive. However, there is another implication of TMDTO attack, where we allow the preprocessing time to be more than the exhaustive key search and then try to minimize the maximum of the online parameters  $M, T, D$ . In case the online parameters are less than  $2^k$ , that attracts some interest in terms of cryptanalysis. In case of BG attack [1,5], the best situation is achieved when  $P = T = M = D = 2^{\frac{n}{2}}$  and  $M, D$  can be reduced at the cost of increasing  $P = T$ . Thus, achieving  $\max\{T, M, D\} < 2^{\frac{n}{2}}$  is not possible even when  $P > 2^{\frac{n}{2}}$ . Rather, we follow the idea of [2,3], where it is possible to reduce all three of the online parameters  $T, M, D$  less than  $2^{\frac{n}{2}}$  at the cost of increasing the preprocessing time  $P$  over  $2^{\frac{n}{2}}$ . In this regard, we obtain parameters like  $P = 2^{171}, M = T = D = 2^{120}$ , where all the online parameters are less than the complexity of exhaustive key search  $2^{128}$  in case of ACORN v3 [10]. This is presented in Sect. 3. Before proceeding further, let us describe the cipher first.

### 1.1 Description of ACORN v3

We briefly state here the description of ACORN v3 relevant to our work. We assume the plaintext message to be a stream of 0's and we concentrate only on the Pseudo Random Generation Algorithm (PRGA) that provides the key stream. We omit the Key Loading Algorithm (KLA) and the Key Scheduling Algorithm (KSA) of the cipher that are available at [10]. This is because the recovery of secret state bits during the PRGA and further the TMDTO attack can be studied irrespective of the initialization process. As stated before, ACORN v3 has 6 LFSRs and four additional bits concatenated to form the 293 bit state. The block diagram of ACORN is represented in Fig. 1 where  $f_t$  represents the feedback bit and  $m_t$  represents the message bit at  $t^{th}$  step [10]. We denote the

state of the cipher by  $\mathcal{S}_t$  and its respective bits as:  $S_{t+0} \dots S_{t+292}$ . The cipher has the following three functions.

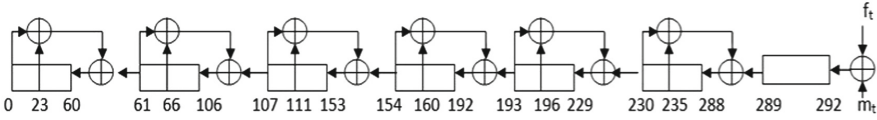


Fig. 1. The internal state of ACORN cipher.

**Output Function.** The output bit  $z_t$  for any state  $t$  is generated as:

$$z_t = S_{t+12} \oplus S_{t+154} \oplus maj(S_{t+235}, S_{t+61}, S_{t+193}) \oplus ch(S_{t+230}, S_{t+111}, S_{t+66}) \tag{1}$$

**Feedback Function.** The feedback bit  $f_t$  for any state  $t$  is generated as:

$$f_t = S_{t+0} \oplus (\sim S_{t+107}) \oplus maj(S_{t+244}, S_{t+23}, S_{t+160}) \oplus (ca_t \& S_{t+196}) \oplus (cb_t \& z_t) \tag{2}$$

**State Update Function.** Before performing the shift, the bits  $S_{t+289}, S_{t+230}, S_{t+193}, S_{t+154}, S_{t+107}, S_{t+61}$  are updated as follows:

$$S_{(t+289)} = S_{(t+289)} \oplus S_{(t+235)} \oplus S_{(t+230)} \tag{3}$$

$$S_{(t+230)} = S_{(t+230)} \oplus S_{(t+196)} \oplus S_{(t+193)} \tag{4}$$

$$S_{(t+193)} = S_{(t+193)} \oplus S_{(t+160)} \oplus S_{(t+154)} \tag{5}$$

$$S_{(t+154)} = S_{(t+154)} \oplus S_{(t+111)} \oplus S_{(t+107)} \tag{6}$$

$$S_{(t+107)} = S_{(t+107)} \oplus S_{(t+66)} \oplus S_{(t+61)} \tag{7}$$

$$S_{(t+61)} = S_{(t+61)} \oplus S_{(t+23)} \oplus S_{(t+0)} \tag{8}$$

And then the next bit is initialized with the feedback bit:

$$S_{t+293} = f_t \tag{9}$$

## 2 Methods to Recover Certain Bits of the State

The underlying motivation of BSW sampling [2,3] is the fact that certain bits of the state can be recovered by observing the key stream sequence  $z^t$  and guessing the remaining part of the state. This reduces the search space and offers a wider range of parameters to choose from in TMDTO attack. We consider two approaches here. The first one is using the SAT solver and the other one is by discovering the equations by hand using trial and error.

### 2.1 Using SAT Solver

Towards this we first form a family of equations and then feeding them into a SAT solver. While forming the equations, the degree of equations formed increases rapidly, which makes it very difficult to find solutions. Hence, we have to adopt a specific approach for formulating equations by introducing new variables. This is in line of [9]. Consider some PRGA round  $t$  of ACORN v3. The equations for the same round are:

1. 1 output bit equation,
2. 1 feedback bit equation, and
3. 6 state update equations.

At the beginning of PRGA, the adversary has 293 state variables  $S_0, S_1, \dots, S_{292}$ . The adversary has access to an  $\ell$ -length key stream  $z_0, z_1, \dots, z_{\ell-1}$ . We will now explain how the output equation is introduced into the system of equations. The output equation as mentioned in (1) is:

$$z_t = S_{t+12} \oplus S_{t+154} \oplus maj(S_{t+235}, S_{t+61}, S_{t+193}) \oplus ch(S_{t+230}, S_{t+111}, S_{t+66}) \tag{10}$$

To add an equation to the SAT solver, the equations are represented in a way such that it is zero in the ring of Boolean polynomials. That is, the output equation is written as

$$z_t \oplus S_{t+12} \oplus S_{t+154} \oplus maj(S_{t+235}, S_{t+61}, S_{t+193}) \oplus ch(S_{t+230}, S_{t+111}, S_{t+66}) \equiv 0, \tag{11}$$

for  $t = 0, 1, 2, \dots, \ell - 1$  and added to the system. Thus we have an array of output equations as:

$$\begin{aligned} z_0 \oplus S_{12} \oplus S_{154} \oplus maj(S_{235}, S_{61}, S_{193}) \oplus ch(S_{230}, S_{111}, S_{66}) &\equiv 0 \\ z_1 \oplus S_{13} \oplus S_{155} \oplus maj(S_{236}, S_{62}, S_{194}) \oplus ch(S_{231}, S_{112}, S_{67}) &\equiv 0 \\ \vdots & \\ z_{(\ell-1)} \oplus S_{(\ell-1+12)} \oplus S_{(\ell-1+154)} \oplus maj(S_{(\ell-1+235)}, S_{(\ell-1+61)}, S_{(\ell-1+193)}) & \\ \oplus ch(S_{(\ell-1+230)}, S_{(\ell-1+111)}, S_{(\ell-1+66)}) &\equiv 0 \end{aligned}$$

Next we discuss the inclusion of feedback bit equation into the system of equations. The equation as mentioned in (2) for PRGA is:

$$f_t = S_{t+0} \oplus (\sim S_{t+107}) \oplus maj(S_{t+244}, S_{t+23}, S_{t+160}) \oplus S_{t+196} \tag{12}$$

However, the feedback bit generated is not known. Thus directly substituting the state variable  $S_{t+293}$  by feedback equations increases non-linearity. Instead, the we introduce new variables  $f_0, f_1, \dots, f_{\ell-1}$  and add these equations to the SAT solver in the following manner:

$$\begin{aligned}
 f_0 \oplus S_0 \oplus (\sim S_{107}) \oplus maj(S_{244}, S_{23}, S_{160}) \oplus S_{196} &\equiv 0 \\
 f_1 \oplus S_1 \oplus (\sim S_{108}) \oplus maj(S_{245}, S_{24}, S_{161}) \oplus S_{197} &\equiv 0 \\
 \vdots \quad \dots \quad \dots \quad \dots \quad \dots \quad \dots \quad \dots \quad \dots \quad \dots & \\
 \vdots \quad \dots \quad \dots \quad \dots \quad \dots \quad \dots \quad \dots \quad \dots \quad \dots & \\
 f_{(\ell-1)} \oplus S_{(\ell-1)} \oplus (\sim S_{(\ell-1+107)}) & \\
 \oplus maj(S_{(\ell-1+244)}, S_{(\ell-1+23)}, S_{(\ell-1+160)}) \oplus S_{(\ell-1+196)} &\equiv 0
 \end{aligned}$$

By now,  $2\ell$  new equations and  $\ell$  new variables have been introduced into the system. The variables  $S_{t+289}, S_{t+230}, S_{t+193}, S_{t+154}, S_{t+107}, S_{t+61}$  are updated in Step 3 as mentioned earlier. For this, we introduce  $6\ell$  new variables  $a_1^0, a_2^0, a_3^0, a_4^0, a_5^0, a_6^0, \dots, a_1^{\ell-1}, a_2^{\ell-1}, a_3^{\ell-1}, a_4^{\ell-1}, a_5^{\ell-1}, a_6^{\ell-1}$  and add the following equations to the system (for  $t = 0, 1, \dots, \ell - 1$ ):

$$\begin{aligned}
 a_1^t \oplus S_{(t+289)} \oplus S_{(t+235)} \oplus S_{(t+230)} &\equiv 0 \\
 a_2^t \oplus S_{(t+230)} \oplus S_{(t+196)} \oplus S_{(t+193)} &\equiv 0 \\
 a_3^t \oplus S_{(t+193)} \oplus S_{(t+160)} \oplus S_{(t+154)} &\equiv 0 \\
 a_4^t \oplus S_{(t+154)} \oplus S_{(t+111)} \oplus S_{(t+107)} &\equiv 0 \\
 a_5^t \oplus S_{(t+107)} \oplus S_{(t+66)} \oplus S_{(t+61)} &\equiv 0 \\
 a_6^t \oplus S_{(t+61)} \oplus S_{(t+23)} \oplus S_{(t+0)} &\equiv 0
 \end{aligned}$$

Since new variables have been introduced, new equations need to be introduced to maintain consistency of the system. That is, the following equations are added to the system:

$$\begin{aligned}
 a_1^t \oplus S_{(t+288)} &\equiv 0 \\
 a_2^t \oplus S_{(t+229)} &\equiv 0 \\
 a_3^t \oplus S_{(t+192)} &\equiv 0 \\
 a_4^t \oplus S_{(t+153)} &\equiv 0 \\
 a_5^t \oplus S_{(t+106)} &\equiv 0 \\
 a_6^t \oplus S_{(t+60)} &\equiv 0
 \end{aligned}$$

for  $t = 0, 1, \dots, \ell - 1$ . Finally, we substitute the feedback bit into the state variable:

$$S_{293+t} = f_t \quad \forall t \in [0, \ell - 1].$$

Therefore, the number of variables used are  $293 + \ell + 6\ell = 293 + 7\ell$  and the number of equations formulated are  $\ell + \ell + 6\ell = 8\ell$  equations. All the equations are collected and fed to the SAT solver.

We set the SAT solver to find all possible solutions for the above system of equations. In this way, we are guaranteed that if the SAT solver returns only one solution, no other solution exists for the system of equations, and hence we are able to solve for the state. However, in few cases of our experiments we could not achieve that. For example, when we consider recovery of 60 bits with the help of 70 key stream bits, we sometimes obtain two solutions. The reason for the same is that the number of key stream bits is not enough and thus the SAT solver provides more solutions instead of a unique solution.

We use the SAT solver Cryptominisat-2.9.6 available with Sage-7.6 [8]. The experiments were performed on a laptop having hardware configuration Intel(R) Core(TM) i5-4200M CPU @ 2.50 GHz and 8 GB RAM running with Ubuntu-16.10. A few experimental data are provided where each row is based on  $2^{15}$  experiments.

**Table 1.** Experimental results for solving the equations. The time required to run the PRGA for 293 clocks is 0.088s on an average.

Key stream bits used	State bits recovered	Location of recovered bits	Proportion of multiple (two) solutions	Average time (sec)
47	47	$S_{107} \dots S_{153}$	0	0.076
43	43	$S_{12} \dots S_{54}$	0	0.067
72	60	$S_0 \dots S_{59}$	$1/2^{10}$	0.127
60	53	$S_{107} \dots S_{150}, S_{56}, \dots S_{64}$	$1/2^{14}$	0.097

### 2.2 Formation of Equations by Observation, not Using SAT Solver

In this section, we build the system of equations used to recover 49 bits of internal state by using first 49 bits of keystream. To perform this recovery, we need to fix 10 bits of internal state with a particular pattern and guess remaining state bits. The internal state bits to be recovered are represented by set  $\mathcal{R} = \mathcal{R}_1 \cup \mathcal{R}_2$ , where  $\mathcal{R}_1 = \{S_{(t+107)} : t = 0, \dots, 43\}$  and  $\mathcal{R}_2 = \{S_{(t+56)} : t = 0, \dots, 4\}$ . The Eq. (1) for generating keystream can be written as:

$$\begin{aligned}
 z_t = & S_{(t+12)} \oplus \overline{S_{(t+154)}} \oplus S_{(t+235)} \overline{S_{(t+61)}} \oplus S_{(t+235)} \overline{S_{(t+193)}} \oplus \overline{S_{(t+193)}} \overline{S_{(t+61)}} \\
 & \oplus \overline{S_{(t+230)}} \overline{S_{(t+111)}} \oplus \overline{S_{(t+230)}} \overline{S_{(t+66)}} \oplus S_{(t+66)}.
 \end{aligned}
 \tag{13}$$

Note that in the above equation, over-lined bits are feedback bits. The state bits are updated according to the following equations before generating the output bit:

$$\begin{aligned}
S_{(t+289)} &= S_{(t+289)} \oplus S_{(t+235)} \oplus S_{(t+230)} \\
S_{(t+230)} &= S_{(t+230)} \oplus S_{(t+196)} \oplus S_{(t+193)} \\
S_{(t+193)} &= S_{(t+193)} \oplus S_{(t+160)} \oplus S_{(t+154)} \\
S_{(t+154)} &= S_{(t+154)} \oplus S_{(t+111)} \oplus S_{(t+107)} \\
S_{(t+107)} &= S_{(t+107)} \oplus S_{(t+66)} \oplus S_{(t+61)} \\
S_{(t+61)} &= S_{(t+61)} \oplus S_{(t+23)} \oplus S_{(t+0)}
\end{aligned} \tag{14}$$

Thus, the Eq. (13) can be written as

$$\begin{aligned}
S_{(t+107)} &= z_t \oplus S_{(t+12)} \oplus S_{(t+154)} \oplus S_{(t+111)} \oplus S_{t+235}(S_{(t+61)} \oplus S_{(t+23)} \oplus S_{(t+0)}) \\
&\oplus S_{(t+235)}(S_{(t+193)} \oplus S_{(t+160)} \oplus S_{(t+154)}) \\
&\oplus (S_{(t+193)} \oplus S_{(t+160)} \oplus S_{(t+154)})(S_{(t+61)} \oplus S_{(t+23)} \oplus S_{(t+0)}) \\
&\oplus (S_{(t+230)} \oplus S_{(t+196)} \oplus S_{(t+193)})S_{(t+111)} \\
&\oplus (S_{(t+230)} \oplus S_{(t+196)} \oplus S_{(t+193)})S_{(t+66)} \oplus S_{(t+66)},
\end{aligned} \tag{15}$$

which makes the recovery simpler, because all the bits on the RHS of the equation are state bits (and not feedback bits) for  $t = 0, \dots, 32$ . However when we place  $t = 33, \dots, 48$  in Eq. (15), feedback bits are also involved and need to be calculated.

Now we use Eq. (15) to recover internal state bits of set  $\mathcal{R}_1$ . The recovery of state bits is done in a certain order. For example, if we attempt to recover  $S_{107}$  by placing  $t = 0$  in Eq. (15), then  $S_{111}$  appears on the RHS of the equation and requires the knowledge of  $S_{111}$ . Thus,  $S_{111}$  is recovered before performing the recovery of  $S_{107}$ .

We define four sets  $\mathcal{R}_3, \mathcal{R}_4, \mathcal{R}_5, \mathcal{R}_6$ , where

$$\begin{aligned}
\mathcal{R}_3 &= \{S_{(t+107)} : t = 40, 36, \dots, 0\} \\
\mathcal{R}_4 &= \{S_{(t+107)} : t = 41, 37, \dots, 1\} \\
\mathcal{R}_5 &= \{S_{(t+107)} : t = 42, 38, \dots, 2\} \\
\mathcal{R}_6 &= \{S_{(t+107)} : t = 43, 39, \dots, 3\}
\end{aligned}$$

and each  $\mathcal{R}_i \subset \mathcal{R}_1$ , for  $i = 3 \dots, 6$ . The order of recovery of state bits is  $\mathcal{R}_3, \mathcal{R}_4, \mathcal{R}_5, \mathcal{R}_6$  and  $\mathcal{R}_2$ , respectively, i.e. the state bits of  $\mathcal{R}_3$  are recovered first then  $\mathcal{R}_4$  and so on. For each set  $\mathcal{R}_i : i = 2 \dots, 6$ , the higher index elements are recovered first. We need not fix any internal state bits for recovering  $\mathcal{R}_1$ . However, to recover  $\mathcal{R}_2$ , the internal state bits are fixed according to Table 2. Let the set  $\mathcal{F}$  represent the internal state bits which are fixed according to Table 2.

Now we describe recovery of  $\mathcal{R}_3$ . The internal state bit  $S_{147}$  is recovered by substituting  $t = 40$  in Eq. (15). From this we have

$$\begin{aligned}
S_{147} &= z_{40} \oplus S_{52} \oplus \overline{S_{194}} \oplus S_{151} \oplus S_{275}(S_{101} \oplus \overline{S_{63}} \oplus S_{40}) \\
&\oplus S_{275}(\overline{S_{233}} \oplus \overline{S_{200}} \oplus \overline{S_{194}}) \oplus (\overline{S_{233}} \oplus \overline{S_{200}} \oplus \overline{S_{194}})(S_{101} \oplus \overline{S_{63}} \oplus S_{40}) \\
&\oplus (S_{270} \oplus \overline{S_{236}} \oplus \overline{S_{233}})S_{151} \oplus (S_{270} \oplus \overline{S_{236}} \oplus \overline{S_{233}})S_{106} \oplus S_{106}.
\end{aligned} \tag{16}$$

**Table 2.** State bits fixed.

Row no.	State bits and value
1	$S_{i+268} = 0 : i = 0 \dots, 4$
2	$S_{i+187} = S[i + 226] \oplus S[i + 193] \oplus S[i + 160] \oplus S[i + 154] : i = 0 \dots, 3$
3	$S_{191} = S[230] \oplus S[196] \oplus S[193] \oplus S[197] \oplus S[164] \oplus S[158]$

In Eq. (16), all the bits appearing on the RHS of the equation are guessed, except the over-lined bits. The over-lined bits are feedback bits, and not internal state bits due to Eq. (14). Thus, we need to guess more internal state bits to calculate the value of  $S_{63}, S_{194}, S_{200}, S_{233}$  and  $S_{236}$  using Eq. (14). In this way, we recover  $S_{147}$ .

Now the internal state bit of  $S_{143}$  is recovered by placing  $t = 36$  in Eq. (15) and we derive

$$\begin{aligned}
 S_{143} = & z_{36} \oplus S_{48} \oplus S_{190} \oplus S_{147} \oplus S_{271}(S_{97} \oplus S_{59} \oplus S_{36}) \\
 & \oplus S_{271}(S_{229} \oplus \overline{S_{196}} \oplus S_{190}) \oplus (S_{229} \oplus \overline{S_{196}} \oplus S_{190})(S_{97} \oplus S_{59} \oplus S_{36}) \quad (17) \\
 & \oplus (S_{266} \oplus \overline{S_{232}} \oplus S_{229})S_{147} \oplus (S_{266} \oplus \overline{S_{232}} \oplus S_{229})S_{102} \oplus S_{102}.
 \end{aligned}$$

Similarly, in Eq. (17), all the state bits appearing on the right side of equation need to be guessed, except  $S_{271}, S_{190}$  and the over-lined bits. The internal state bits  $S_{271}$  and  $S_{190}$  are fixed according to Table 2. The over-lined bits are calculated using Eq. (14). Thus, we need to guess more internal state bits to calculate the value of  $S_{196}, S_{232}$  and recover  $S_{143}$ .

The remaining state bits of  $\mathcal{R}_3$  i.e.  $S_{139}, S_{135}, \dots, S_{107}$  are recovered by substituting  $t = 32, 28, \dots, 0$ , respectively, in Eq. (15). While placing  $t = 32, 28, \dots, 0$  in Eq. (15), the internal state bits appearing on the RHS of the equation are guessed, except state bits belonging to  $\mathcal{R}$  and  $\mathcal{F}$ . Following the same methodology, the internal state bits of set  $\mathcal{R}_4, \mathcal{R}_5$  and  $\mathcal{R}_6$  are recovered.

To recover the state bits of set  $\mathcal{R}_2$ , all things are same as done earlier, except for Eq. (13) which is rewritten as

$$\begin{aligned}
 S_{t+12} = & z_t \oplus S_{(t+107)} \oplus S_{(t+154)} \oplus S_{(t+111)} \oplus S_{t+235}(S_{(t+61)} \oplus S_{(t+23)} \oplus S_{(t+0)}) \\
 & \oplus S_{t+235}(S_{(t+193)} \oplus S_{(t+160)} \oplus S_{(t+154)}) \\
 & \oplus (S_{(t+193)} \oplus S_{(t+160)} \oplus S_{(t+154)})(S_{(t+61)} \oplus S_{(t+23)} \oplus S_{(t+0)}) \\
 & \oplus (S_{(t+230)} \oplus S_{(t+196)} \oplus S_{(t+193)})S_{t+111} \\
 & \oplus (S_{(t+230)} \oplus S_{(t+196)} \oplus S_{(t+193)})S_{t+66} \oplus S_{t+66}. \quad (18)
 \end{aligned}$$

Thus, the internal state bits  $S_{56}, \dots, S_{60}$  are recovered by using  $t = 44, \dots, 48$  in Eq. (18), respectively. Another difference between recovery of  $\mathcal{R}_1$  and  $\mathcal{R}_2$  is that it is not necessary to recover the higher index elements first (as done before).

In this way, we recover 49 bits of  $\mathcal{R}$  by fixing the 10 internal state bits of set  $\mathcal{F}$  and guessing the remaining 234 state bits. However, there are nine



internal state bits i.e.  $S_{284}, \dots, S_{292}$  which are not appeared in the equations used for recovery. However these bits are also considered as guessed bits during application of TMDTO attack. In the Table 3, the details of equations are given used for recovery of state bits of set  $\mathcal{R}$ . The over-lined state bits and underlined state bits in Table 3 are feedback bits and fixed state bits (according to Table 2), respectively.

### 3 Complexity of TMDTO Attack

Now we will describe the TMDTO attack in complete detail. We have a state size of  $n = 293$  bits. Thus, the standard TMDTO formula [2,3] with a single table will be as follows:

- $TM^2D^2 = N^2$ , where  $N = 2^n$ ,
- $D^2 \leq T$ ,
- $P = \frac{N}{D}$ .

During the preprocessing phase, we will prepare a table with  $m$  rows and  $t$  columns, where  $mt^2 = N$  for a successful attack. The number of tables is  $\frac{t}{D}$  and given a single table we have  $t = D$ . Each row of the table contains a chain of  $t$  elements. Consider that a specific state of  $n = 293$  bits is  $\zeta$  and  $f$  is the one way function. Here by one way function  $f$ , we mean that the cipher with the state  $\zeta$  will be run for  $n$  times again to generate  $n$  many key stream bits. Those bits will be loaded as the new state, which is called  $\eta$ . That is  $\eta = f(\zeta)$ . We will start with a random state and then generate a row of  $t$  elements by this method. There will be  $m$  such rows. Thus, the total table size is  $mt$ . However, the complete row will not be saved. Only the starting and the final element will be saved. Thus, the storage requirement of the table will be  $O(m)$ , which is actually the memory parameter  $M$ .

#### 3.1 Knowledge of 47 Bits of State from 47 Key Stream Bits

Now consider the case when we are able to recover  $\psi$  bits of the state from  $\psi$  consecutive key stream bits and the rest of the state bits. In this case, we consider a fixed pattern for the key stream bits and only when that pattern is found in the key stream, we try to search the state in the table. Thus, in this case, we consider a state size of  $n - \psi$  bits and the parameters are referred as  $N' = 2^{n-\psi}$ ,  $P', M', T', D'$ . Let us now consider the exact parameters referring to Table 1, where  $\psi = 47$ . Thus,  $T'M'D'^2 = N'^2 = 2^{2(293-47)}$ . Let us consider  $D'^2 = T$ . Thus, we have  $T'M' = 2^{293-47} = 2^{246}$ . Now, one can consider,  $T' = M' = 2^{123}$  and  $D' = 2^{61.5}$ . However, as we have discussed that during the online phase, we can only mount the attack when a specific  $\psi$ -bit pattern comes, we have  $D = 2^\psi D'$ . Thus, finally, we will have the parameters  $T = T' = 2^{123}$ ,  $M = M' = 2^{123}$ ,  $D = 2^\psi D' = 2^{47} \cdot 2^{61.5} = 2^{108.5}$ ,  $P = P' = \frac{N'}{D'} = 2^{184.5}$ . This provides the maximum of online parameters as  $2^{123}$ , which is less than the exhaustive secret key search of complexity  $2^{128}$ . However, as expected, the pre-processing time is much larger than the exhaustive key search.

**Table 3.** Recovery of 49 bits of the internal state after fixing 10 bits

Steps	Equations used for recovery	Gussed bits
0	$S_{147} = z_{40} \oplus S_{52} \oplus \overline{S_{194}} \oplus S_{151} \oplus S_{275}(S_{101} \oplus \overline{S_{63}} \oplus S_{40})$ $\oplus S_{275}(\overline{S_{233}} \oplus \overline{S_{200}} \oplus \overline{S_{194}}) \oplus (\overline{S_{233}} \oplus \overline{S_{200}} \oplus \overline{S_{194}})$ $(S_{101} \oplus \overline{S_{63}} \oplus S_{40}) \oplus (\overline{S_{270}} \oplus \overline{S_{236}} \oplus \overline{S_{233}})S_{151}$ $\oplus (\overline{S_{270}} \oplus \overline{S_{236}} \oplus \overline{S_{233}})S_{106} \oplus S_{106}$	$S_{52}, S_{101}, S_{63}, S_{25}, S_2,$ $S_{40}, S_{275}, S_{233}, S_{199},$ $S_{196}, S_{200}, S_{167}, S_{161},$ $S_{194}, S_{155}, S_{236}, S_{202},$ $S_{151}, S_{106}$
1	$S_{143} = z_{36} \oplus S_{48} \oplus \overline{S_{190}} \oplus S_{147} \oplus \overline{S_{271}}(S_{97} \oplus S_{59} \oplus S_{36})$ $\oplus \overline{S_{271}}(S_{229} \oplus \overline{S_{196}} \oplus \overline{S_{190}}) \oplus (S_{229} \oplus \overline{S_{196}} \oplus \overline{S_{190}})$ $(S_{97} \oplus S_{59} \oplus S_{36}) \oplus (S_{266} \oplus \overline{S_{232}} \oplus S_{229})S_{147}$ $\oplus (S_{266} \oplus \overline{S_{232}} \oplus S_{229})S_{102} \oplus S_{102}$	$S_{48}, S_{97}, S_{36}, S_{229},$ $S_{163}, S_{157}, S_{266}, S_{232},$ $S_{198}, S_{195}, S_{102}$
2	$S_{139} = z_{32} \oplus S_{44} \oplus S_{186} \oplus S_{143} \oplus S_{267}(S_{93} \oplus S_{55} \oplus S_{32})$ $\oplus S_{267}(S_{225} \oplus S_{192} \oplus S_{186}) \oplus (S_{225} \oplus S_{192} \oplus S_{186})$ $(S_{93} \oplus S_{55} \oplus S_{32}) \oplus (S_{262} \oplus S_{228} \oplus S_{225})S_{143}$ $\oplus (S_{262} \oplus S_{228} \oplus S_{225})S_{98} \oplus S_{98}$	$S_{44}, S_{93}, S_{55}, S_{32},$ $S_{267}, S_{225}, S_{192}, S_{186}$ $S_{262}, S_{228}, S_{98}$
3	$S_{135} = z_{28} \oplus S_{40} \oplus S_{182} \oplus S_{139} \oplus S_{263}(S_{89} \oplus S_{51} \oplus S_{28})$ $\oplus S_{263}(S_{221} \oplus \overline{S_{188}} \oplus S_{182}) \oplus (S_{221} \oplus \overline{S_{188}} \oplus S_{182})$ $(S_{89} \oplus S_{51} \oplus S_{28}) \oplus (S_{258} \oplus S_{224} \oplus S_{221})S_{139}$ $\oplus (S_{258} \oplus S_{224} \oplus S_{221})S_{94} \oplus S_{94}$	$S_{89}, S_{51}, S_{28}, S_{263},$ $S_{221}, S_{182}, S_{258}, S_{224},$ $S_{94}$
4	$S_{131} = z_{24} \oplus S_{36} \oplus S_{178} \oplus S_{135} \oplus S_{259}(S_{85} \oplus S_{47} \oplus S_{24})$ $\oplus S_{259}(S_{217} \oplus S_{184} \oplus S_{178}) \oplus (S_{217} \oplus S_{184} \oplus S_{178})$ $(S_{85} \oplus S_{47} \oplus S_{24}) \oplus (S_{254} \oplus S_{220} \oplus S_{217})S_{135}$ $\oplus (S_{254} \oplus S_{220} \oplus S_{217})S_{90} \oplus S_{90}$	$S_{85}, S_{47}, S_{24}, S_{259},$ $S_{217}, S_{184}, S_{178}, S_{254},$ $S_{220}, S_{90}$
5	$S_{127} = z_{20} \oplus S_{32} \oplus S_{174} \oplus S_{131} \oplus S_{255}(S_{81} \oplus S_{43} \oplus S_{20})$ $\oplus S_{255}(S_{213} \oplus S_{180} \oplus S_{174}) \oplus (S_{213} \oplus S_{180} \oplus S_{174})$ $(S_{81} \oplus S_{43} \oplus S_{20}) \oplus (S_{250} \oplus S_{216} \oplus S_{213})S_{131}$ $\oplus (S_{250} \oplus S_{216} \oplus S_{213})S_{86} \oplus S_{86}$	$S_{81}, S_{43}, S_{20}, S_{255},$ $S_{213}, S_{180}, S_{174},$ $S_{250}, S_{216}, S_{86}$
6	$S_{123} = z_{16} \oplus S_{28} \oplus S_{170} \oplus S_{127} \oplus S_{251}(S_{77} \oplus S_{39} \oplus S_{16})$ $\oplus S_{251}(S_{209} \oplus S_{176} \oplus S_{170}) \oplus (S_{209} \oplus S_{176} \oplus S_{170})$ $(S_{77} \oplus S_{39} \oplus S_{16}) \oplus (S_{246} \oplus S_{212} \oplus S_{209})S_{127}$ $\oplus (S_{246} \oplus S_{212} \oplus S_{209})S_{82} \oplus S_{82}$	$S_{77}, S_{39}, S_{16}, S_{251},$ $S_{209}, S_{176}, S_{170}, S_{246},$ $S_{212}, S_{82}$
7	$S_{119} = z_{12} \oplus S_{24} \oplus S_{166} \oplus S_{123} \oplus S_{247}(S_{73} \oplus S_{35} \oplus S_{12})$ $\oplus S_{247}(S_{205} \oplus S_{172} \oplus S_{166}) \oplus (S_{205} \oplus S_{172} \oplus S_{166})$ $(S_{73} \oplus S_{35} \oplus S_{12}) \oplus (S_{242} \oplus S_{208} \oplus S_{205})S_{123}$ $\oplus (S_{242} \oplus S_{208} \oplus S_{205})S_{78} \oplus S_{78}$	$S_{73}, S_{35}, S_{12}, S_{247},$ $S_{205}, S_{172}, S_{166}, S_{242},$ $S_{208}, S_{78}$
8	$S_{115} = z_8 \oplus S_{20} \oplus S_{162} \oplus S_{119} \oplus S_{243}(S_{69} \oplus S_{31} \oplus S_8)$ $\oplus S_{243}(S_{201} \oplus S_{168} \oplus S_{162}) \oplus (S_{201} \oplus S_{168} \oplus S_{162})$ $(S_{69} \oplus S_{31} \oplus S_8) \oplus (S_{238} \oplus S_{204} \oplus S_{201})S_{119}$ $\oplus (S_{238} \oplus S_{204} \oplus S_{201})S_{74} \oplus S_{74}$	$S_{69}, S_{31}, S_8, S_{243},$ $S_{201}, S_{168}, S_{162}, S_{238},$ $S_{204}, S_{74}$
9	$S_{111} = z_4 \oplus S_{16} \oplus S_{158} \oplus S_{115} \oplus S_{239}(S_{65} \oplus S_{27} \oplus S_4)$ $\oplus S_{239}(S_{197} \oplus S_{164} \oplus S_{158}) \oplus (S_{197} \oplus S_{164} \oplus S_{158})$ $(S_{65} \oplus S_{27} \oplus S_4) \oplus (S_{234} \oplus S_{200} \oplus S_{197})S_{115}$ $\oplus (S_{234} \oplus S_{200} \oplus S_{197})S_{70} \oplus S_{70}$	$S_{65}, S_{27}, S_4, S_{239},$ $S_{197}, S_{164}, S_{158}, S_{234},$ $S_{70}$

(continued)

**Table 1.** (continued)

Steps	Equations used for recovery	Guessed bits
10	$S_{107} = z_0 \oplus S_{12} \oplus S_{154} \oplus S_{111} \oplus S_{235}(S_{61} \oplus S_{23} \oplus S_0)$ $\oplus S_{235}(S_{193} \oplus S_{160} \oplus S_{154}) \oplus (S_{193} \oplus S_{160} \oplus S_{154})$ $(S_{61} \oplus S_{23} \oplus S_0) \oplus (S_{230} \oplus S_{196} \oplus S_{193})S_{111}$ $\oplus (S_{230} \oplus S_{196} \oplus S_{193})S_{66} \oplus S_{66}$	$S_{61}, S_{23}, S_0, S_{235},$ $S_{193}, S_{160}, S_{154}, S_{230},$ $S_{66}$
11	$S_{148} = z_{41} \oplus S_{53} \oplus S_{195} \oplus S_{152} \oplus S_{276}(S_{102} \oplus \overline{S_{64}} \oplus S_{41})$ $\oplus S_{276}(\overline{S_{234}} \oplus \overline{S_{201}} \oplus \overline{S_{195}}) \oplus (S_{234} \oplus \overline{S_{201}} \oplus \overline{S_{195}})$ $(S_{102} \oplus \overline{S_{64}} \oplus S_{41}) \oplus (S_{271} \oplus \overline{S_{237}} \oplus \overline{S_{234}})S_{152}$ $\oplus (S_{271} \oplus \overline{S_{237}} \oplus \overline{S_{234}})\overline{S_{107}} \oplus \overline{S_{107}}$	$S_{53}, S_{64}, S_{26}, S_3,$ $S_{41}, S_{276}, S_{156}, S_{237},$ $S_{203}, S_{152}$
12	$S_{144} = z_{37} \oplus S_{49} \oplus \overline{S_{191}} \oplus S_{148} \oplus \overline{S_{272}}(S_{98} \oplus S_{60} \oplus S_{37})$ $\oplus \overline{S_{272}}(\overline{S_{230}} \oplus \overline{S_{197}} \oplus \overline{S_{191}}) \oplus (\overline{S_{230}} \oplus \overline{S_{197}} \oplus \overline{S_{191}})$ $(S_{98} \oplus S_{60} \oplus S_{37}) \oplus (S_{267} \oplus \overline{S_{233}} \oplus \overline{S_{230}})S_{148}$ $\oplus (S_{267} \oplus \overline{S_{233}} \oplus \overline{S_{230}})S_{103} \oplus S_{103}$	$S_{49}, S_{37}, S_{103}$
13	$S_{140} = z_{33} \oplus S_{45} \oplus \overline{S_{187}} \oplus S_{144} \oplus \overline{S_{268}}(S_{94} \oplus S_{56} \oplus S_{33})$ $\oplus \overline{S_{268}}(S_{226} \oplus \overline{S_{193}} \oplus \overline{S_{187}}) \oplus (S_{226} \oplus \overline{S_{193}} \oplus \overline{S_{187}})$ $(S_{94} \oplus S_{56} \oplus S_{33}) \oplus (S_{263} \oplus S_{229} \oplus S_{226})S_{144}$ $\oplus (S_{263} \oplus S_{229} \oplus S_{226})S_{99} \oplus S_{99}$	$S_{45}, S_{94}, S_{33},$ $S_{226}, S_{99}$
14	$S_{136} = z_{29} \oplus S_{41} \oplus S_{183} \oplus S_{140} \oplus S_{264}(S_{90} \oplus S_{52} \oplus S_{29})$ $\oplus S_{264}(S_{222} \oplus \overline{S_{189}} \oplus S_{183}) \oplus (S_{222} \oplus \overline{S_{189}} \oplus S_{183})$ $(S_{90} \oplus S_{52} \oplus S_{29}) \oplus (S_{259} \oplus S_{225} \oplus S_{222})S_{140}$ $\oplus (S_{259} \oplus S_{225} \oplus S_{222})S_{95} \oplus S_{95}$	$S_{29}, S_{264}, S_{222},$ $S_{183}, S_{95}$
15	$S_{132} = z_{25} \oplus S_{37} \oplus S_{179} \oplus S_{136} \oplus S_{260}(S_{86} \oplus S_{48} \oplus S_{25})$ $\oplus S_{260}(S_{218} \oplus S_{185} \oplus S_{179}) \oplus (S_{218} \oplus S_{185} \oplus S_{179})$ $(S_{86} \oplus S_{48} \oplus S_{25}) \oplus (S_{255} \oplus S_{221} \oplus S_{218})S_{136}$ $\oplus (S_{255} \oplus S_{221} \oplus S_{218})S_{91} \oplus S_{91}$	$S_{260}, S_{218}, S_{185},$ $S_{179}, S_{91}$
16	$S_{128} = z_{21} \oplus S_{33} \oplus S_{175} \oplus S_{132} \oplus S_{256}(S_{82} \oplus S_{44} \oplus S_{21})$ $\oplus S_{256}(S_{214} \oplus S_{181} \oplus S_{175}) \oplus (S_{214} \oplus S_{181} \oplus S_{175})$ $(S_{82} \oplus S_{44} \oplus S_{21}) \oplus (S_{251} \oplus S_{217} \oplus S_{214})S_{132}$ $\oplus (S_{251} \oplus S_{217} \oplus S_{214})S_{87} \oplus S_{87}$	$S_{21}, S_{256}, S_{214},$ $S_{181}, S_{175}, S_{87}$
17	$S_{124} = z_{17} \oplus S_{29} \oplus S_{171} \oplus S_{128} \oplus S_{252}(S_{78} \oplus S_{40} \oplus S_{17})$ $\oplus S_{252}(S_{210} \oplus S_{177} \oplus S_{171}) \oplus (S_{210} \oplus S_{177} \oplus S_{171})$ $(S_{78} \oplus S_{40} \oplus S_{17}) \oplus (S_{247} \oplus S_{213} \oplus S_{210})S_{128}$ $\oplus (S_{247} \oplus S_{213} \oplus S_{210})S_{83} \oplus S_{83}$	$S_{17}, S_{252}, S_{210},$ $S_{177}, S_{171}, S_{83}$
18	$S_{120} = z_{13} \oplus S_{25} \oplus S_{167} \oplus S_{124} \oplus S_{248}(S_{74} \oplus S_{36} \oplus S_{13})$ $\oplus S_{248}(S_{206} \oplus S_{173} \oplus S_{167}) \oplus (S_{206} \oplus S_{173} \oplus S_{167})$ $(S_{74} \oplus S_{36} \oplus S_{13}) \oplus (S_{243} \oplus S_{209} \oplus S_{206})S_{124}$ $\oplus (S_{243} \oplus S_{209} \oplus S_{206})S_{79} \oplus S_{79}$	$S_{13}, S_{248}, S_{206},$ $S_{173}, S_{79}$
19	$S_{116} = z_9 \oplus S_{21} \oplus S_{163} \oplus S_{120} \oplus S_{244}(S_{70} \oplus S_{32} \oplus S_9)$ $\oplus S_{244}(S_{202} \oplus S_{169} \oplus S_{163}) \oplus (S_{202} \oplus S_{169} \oplus S_{163})$ $(S_{70} \oplus S_{32} \oplus S_9) \oplus (S_{239} \oplus S_{205} \oplus S_{202})S_{120}$ $\oplus (S_{239} \oplus S_{205} \oplus S_{202})S_{75} \oplus S_{75}$	$S_9, S_{244}, S_{169}, S_{75}$

(continued)

Table 1. (continued)

Steps	Equations used for recovery	Gussed bits
20	$S_{112} = z_5 \oplus S_{17} \oplus S_{159} \oplus S_{116} \oplus S_{240}(S_{66} \oplus S_{28} \oplus S_5)$ $\oplus S_{240}(S_{198} \oplus S_{165} \oplus S_{159}) \oplus (S_{198} \oplus S_{165} \oplus S_{159})$ $(S_{66} \oplus S_{28} \oplus S_5) \oplus (S_{235} \oplus S_{201} \oplus S_{198})S_{116}$ $\oplus (S_{235} \oplus S_{201} \oplus S_{198})S_{71} \oplus S_{71}$	$S_5, S_{240}, S_{165},$ $S_{159}, S_{71}$
21	$S_{108} = z_1 \oplus S_{13} \oplus S_{155} \oplus S_{112} \oplus S_{236}(S_{62} \oplus S_{24} \oplus S_1)$ $\oplus S_{236}(S_{194} \oplus S_{161} \oplus S_{155}) \oplus (S_{194} \oplus S_{161} \oplus S_{155})$ $(S_{62} \oplus S_{24} \oplus S_1) \oplus (S_{231} \oplus S_{197} \oplus S_{194})S_{112}$ $\oplus (S_{231} \oplus S_{197} \oplus S_{194})S_{67} \oplus S_{67}$	$S_{62}, S_1, S_{231}, S_{67}$
22	$S_{149} = z_4 \oplus S_{54} \oplus S_{196} \oplus S_{153} \oplus S_{277}(S_{103} \oplus S_{65} \oplus S_{42})$ $\oplus S_{277}(\overline{S_{235}} \oplus \overline{S_{202}} \oplus \overline{S_{196}}) \oplus (\overline{S_{235}} \oplus \overline{S_{202}} \oplus \overline{S_{196}})$ $(S_{103} \oplus \overline{S_{65}} \oplus S_{42}) \oplus (\overline{S_{272}} \oplus \overline{S_{238}} \oplus \overline{S_{235}})S_{153}$ $\oplus (\overline{S_{272}} \oplus \overline{S_{238}} \oplus \overline{S_{235}})S_{108} \oplus \overline{S_{108}}$	$S_{54}, S_{42}, S_{277}, S_{153}$
23	$S_{145} = z_{38} \oplus S_{50} \oplus S_{192} \oplus S_{149} \oplus S_{273}(S_{99} \oplus \overline{S_{61}} \oplus \overline{S_{38}})$ $\oplus S_{273}(\overline{S_{231}} \oplus \overline{S_{198}} \oplus S_{192}) \oplus (\overline{S_{231}} \oplus \overline{S_{198}} \oplus S_{192})$ $(S_{99} \oplus \overline{S_{61}} \oplus \overline{S_{38}}) \oplus (\overline{S_{268}} \oplus \overline{S_{234}} \oplus \overline{S_{231}})S_{149}$ $\oplus (\overline{S_{268}} \oplus \overline{S_{234}} \oplus \overline{S_{231}})S_{104} \oplus S_{104}$	$S_{50}, S_{38}, S_{273}, S_{104}$
24	$S_{141} = z_{34} \oplus S_{46} \oplus \overline{S_{188}} \oplus S_{145} \oplus \overline{S_{269}}(S_{95} \oplus S_{57} \oplus S_{34})$ $\oplus \overline{S_{269}}(S_{227} \oplus \overline{S_{194}} \oplus \overline{S_{188}}) \oplus (S_{227} \oplus \overline{S_{194}} \oplus \overline{S_{188}})$ $(S_{95} \oplus S_{57} \oplus S_{34}) \oplus (S_{264} \oplus \overline{S_{230}} \oplus S_{227})S_{145}$ $\oplus (S_{264} \oplus \overline{S_{230}} \oplus S_{227})S_{100} \oplus S_{100}$	$S_{46}, S_{34}, S_{227}$ $S_{100}$
25	$S_{137} = z_{30} \oplus S_{42} \oplus S_{184} \oplus S_{141} \oplus S_{265}(S_{91} \oplus S_{53} \oplus S_{30})$ $\oplus S_{265}(S_{223} \oplus \overline{S_{190}} \oplus S_{184}) \oplus (S_{223} \oplus \overline{S_{190}} \oplus S_{184})$ $(S_{91} \oplus S_{53} \oplus S_{30}) \oplus (S_{260} \oplus S_{226} \oplus S_{223})S_{141}$ $\oplus (S_{260} \oplus S_{226} \oplus S_{223})S_{96} \oplus S_{96}$	$S_{30}, S_{265}, S_{223}, S_{96}$
26	$S_{133} = z_{26} \oplus S_{38} \oplus S_{180} \oplus S_{137} \oplus S_{261}(S_{87} \oplus S_{49} \oplus S_{26})$ $\oplus S_{261}(S_{219} \oplus S_{186} \oplus S_{180}) \oplus (S_{219} \oplus S_{186} \oplus S_{180})$ $(S_{87} \oplus S_{49} \oplus S_{26}) \oplus (S_{256} \oplus S_{222} \oplus S_{219})S_{137}$ $\oplus (S_{256} \oplus S_{222} \oplus S_{219})S_{92} \oplus S_{92}$	$S_{261}, S_{219}, S_{92}$
27	$S_{129} = z_{22} \oplus S_{34} \oplus S_{176} \oplus S_{133} \oplus S_{257}(S_{83} \oplus S_{45} \oplus S_{22})$ $\oplus S_{257}(S_{215} \oplus S_{182} \oplus S_{176}) \oplus (S_{215} \oplus S_{182} \oplus S_{176})$ $(S_{83} \oplus S_{45} \oplus S_{22}) \oplus (S_{252} \oplus S_{218} \oplus S_{215})S_{133}$ $\oplus (S_{252} \oplus S_{218} \oplus S_{215})S_{88} \oplus S_{88}$	$S_{22}, S_{257}, S_{215}, S_{88}$
28	$S_{125} = z_{18} \oplus S_{30} \oplus S_{172} \oplus S_{129} \oplus S_{253}(S_{79} \oplus S_{41} \oplus S_{18})$ $\oplus S_{253}(S_{211} \oplus S_{178} \oplus S_{172}) \oplus (S_{211} \oplus S_{178} \oplus S_{172})$ $(S_{79} \oplus S_{41} \oplus S_{18}) \oplus (S_{248} \oplus S_{214} \oplus S_{211})S_{129}$ $\oplus (S_{248} \oplus S_{214} \oplus S_{211})S_{84} \oplus S_{84}$	$S_{18}, S_{253}, S_{211}, S_{84}$
29	$S_{121} = z_{14} \oplus S_{26} \oplus S_{168} \oplus S_{125} \oplus S_{249}(S_{75} \oplus S_{37} \oplus S_{14})$ $\oplus S_{249}(S_{207} \oplus S_{174} \oplus S_{168}) \oplus (S_{207} \oplus S_{174} \oplus S_{168})$ $(S_{75} \oplus S_{37} \oplus S_{14}) \oplus (S_{244} \oplus S_{210} \oplus S_{207})S_{125}$ $\oplus (S_{244} \oplus S_{210} \oplus S_{207})S_{80} \oplus S_{80}$	$S_{14}, S_{249}, S_{207}, S_{80}$

(continued)

**Table 1.** (continued)

Steps	Equations used for recovery	Gussed bits
30	$S_{117} = z_{10} \oplus S_{22} \oplus S_{164} \oplus S_{121} \oplus S_{245}(S_{71} \oplus S_{33} \oplus S_{10})$ $\oplus S_{245}(S_{203} \oplus S_{170} \oplus S_{164}) \oplus (S_{203} \oplus S_{170} \oplus S_{164})$ $(S_{71} \oplus S_{33} \oplus S_{10}) \oplus (S_{240} \oplus S_{206} \oplus S_{203})S_{121}$ $\oplus (S_{240} \oplus S_{206} \oplus S_{203})S_{76} \oplus S_{76}$	$S_{10}, S_{245}, S_{76}$
31	$S_{113} = z_6 \oplus S_{18} \oplus S_{160} \oplus S_{117} \oplus S_{241}(S_{67} \oplus S_{29} \oplus S_6)$ $\oplus S_{241}(S_{199} \oplus S_{166} \oplus S_{160}) \oplus (S_{199} \oplus S_{166} \oplus S_{160})$ $(S_{67} \oplus S_{29} \oplus S_6) \oplus (S_{236} \oplus S_{202} \oplus S_{199})S_{117}$ $\oplus (S_{236} \oplus S_{202} \oplus S_{199})S_{72} \oplus S_{72}$	$S_6, S_{241}, S_{72}$
32	$S_{109} = z_2 \oplus S_{14} \oplus S_{156} \oplus S_{113} \oplus S_{237}(S_{63} \oplus S_{25} \oplus S_2)$ $\oplus S_{237}(S_{195} \oplus S_{162} \oplus S_{156}) \oplus (S_{195} \oplus S_{162} \oplus S_{156})$ $(S_{63} \oplus S_{25} \oplus S_2) \oplus (S_{232} \oplus S_{198} \oplus S_{195})S_{113}$ $\oplus (S_{232} \oplus S_{198} \oplus S_{195})S_{68} \oplus S_{68}$	$S_{68}$
33	$S_{150} = z_{43} \oplus S_{55} \oplus \overline{S_{197}} \oplus \overline{S_{154}} \oplus S_{278}(S_{104} \oplus \overline{S_{66}} \oplus S_{43})$ $\oplus S_{278}(\overline{S_{236}} \oplus \overline{S_{203}} \oplus \overline{S_{197}}) \oplus (\overline{S_{236}} \oplus \overline{S_{203}} \oplus \overline{S_{197}})$ $(S_{104} \oplus \overline{S_{66}} \oplus S_{43}) \oplus (S_{273} \oplus \overline{S_{239}} \oplus \overline{S_{236}})\overline{S_{154}}$ $\oplus (S_{273} \oplus \overline{S_{239}} \oplus \overline{S_{236}})\overline{S_{109}} \oplus \overline{S_{109}}$	$S_{278}$
34	$S_{146} = z_{39} \oplus S_{51} \oplus \overline{S_{193}} \oplus S_{150} \oplus S_{274}(S_{100} \oplus \overline{S_{62}} \oplus S_{39})$ $\oplus S_{274}(\overline{S_{232}} \oplus \overline{S_{199}} \oplus \overline{S_{193}}) \oplus (\overline{S_{232}} \oplus \overline{S_{199}} \oplus \overline{S_{193}})$ $(S_{100} \oplus \overline{S_{62}} \oplus S_{39}) \oplus (S_{269} \oplus \overline{S_{235}} \oplus \overline{S_{232}})S_{150}$ $\oplus (\overline{S_{269}} \oplus \overline{S_{235}} \oplus \overline{S_{232}})S_{105} \oplus S_{105}$	$S_{274}, S_{105}$
35	$S_{142} = z_{35} \oplus S_{47} \oplus \overline{S_{189}} \oplus S_{146} \oplus \overline{S_{270}}(S_{96} \oplus S_{58} \oplus S_{35})$ $\oplus \overline{S_{270}}(S_{228} \oplus \overline{S_{195}} \oplus \overline{S_{189}}) \oplus (S_{228} \oplus \overline{S_{195}} \oplus \overline{S_{189}})$ $(S_{96} \oplus S_{58} \oplus S_{35}) \oplus (S_{265} \oplus \overline{S_{231}} \oplus S_{228})S_{146}$ $\oplus (S_{265} \oplus \overline{S_{231}} \oplus S_{228})S_{101} \oplus S_{101}$	—
36	$S_{138} = z_{31} \oplus S_{43} \oplus S_{185} \oplus S_{142} \oplus S_{266}(S_{92} \oplus S_{54} \oplus S_{31})$ $\oplus S_{266}(S_{224} \oplus \overline{S_{191}} \oplus S_{185}) \oplus (S_{224} \oplus \overline{S_{191}} \oplus S_{185})$ $(S_{92} \oplus S_{54} \oplus S_{31}) \oplus (S_{261} \oplus S_{227} \oplus S_{224})S_{142}$ $\oplus (S_{261} \oplus S_{227} \oplus S_{224})S_{97} \oplus S_{97}$	—
37	$S_{134} = z_{27} \oplus S_{39} \oplus S_{181} \oplus S_{138} \oplus S_{262}(S_{88} \oplus S_{50} \oplus S_{27})$ $\oplus S_{262}(S_{220} \oplus \overline{S_{187}} \oplus S_{181}) \oplus (S_{220} \oplus \overline{S_{187}} \oplus S_{181})$ $(S_{88} \oplus S_{50} \oplus S_{27}) \oplus (S_{257} \oplus S_{223} \oplus S_{220})S_{138}$ $\oplus (S_{257} \oplus S_{223} \oplus S_{220})S_{93} \oplus S_{93}$	—
38	$S_{130} = z_{23} \oplus S_{35} \oplus S_{177} \oplus S_{134} \oplus S_{258}(S_{84} \oplus S_{46} \oplus S_{23})$ $\oplus S_{258}(S_{216} \oplus S_{183} \oplus S_{177}) \oplus (S_{216} \oplus S_{183} \oplus S_{177})$ $(S_{84} \oplus S_{46} \oplus S_{23}) \oplus (S_{253} \oplus S_{219} \oplus S_{216})S_{134}$ $\oplus (S_{253} \oplus S_{219} \oplus S_{216})S_{89} \oplus S_{89}$	—

(continued)

Table 1. (continued)

Steps	Equations used for recovery	Guessed bits
39	$  \begin{aligned}  S_{126} &= z_{19} \oplus S_{31} \oplus S_{173} \oplus S_{130} \oplus S_{254}(S_{80} \oplus S_{42} \oplus S_{19}) \\  &\oplus S_{254}(S_{212} \oplus S_{179} \oplus S_{173}) \oplus (S_{212} \oplus S_{179} \oplus S_{173}) \\  &(S_{80} \oplus S_{42} \oplus S_{19}) \oplus (S_{249} \oplus S_{215} \oplus S_{212})S_{130} \\  &\oplus (S_{249} \oplus S_{215} \oplus S_{212})S_{85} \oplus S_{85}  \end{aligned}  $	$S_{19}$
40	$  \begin{aligned}  S_{122} &= z_{15} \oplus S_{27} \oplus S_{169} \oplus S_{126} \oplus S_{250}(S_{76} \oplus S_{38} \oplus S_{15}) \\  &\oplus S_{250}(S_{208} \oplus S_{175} \oplus S_{169}) \oplus (S_{208} \oplus S_{175} \oplus S_{169}) \\  &(S_{76} \oplus S_{38} \oplus S_{15}) \oplus (S_{245} \oplus S_{211} \oplus S_{208})S_{126} \\  &\oplus (S_{245} \oplus S_{211} \oplus S_{208})S_{81} \oplus S_{81}  \end{aligned}  $	$S_{15}$
41	$  \begin{aligned}  S_{118} &= z_{11} \oplus S_{23} \oplus S_{165} \oplus S_{122} \oplus S_{246}(S_{72} \oplus S_{34} \oplus S_{11}) \\  &\oplus S_{246}(S_{204} \oplus S_{171} \oplus S_{165}) \oplus (S_{204} \oplus S_{171} \oplus S_{165}) \\  &(S_{72} \oplus S_{34} \oplus S_{11}) \oplus (S_{241} \oplus S_{207} \oplus S_{204})S_{122} \\  &\oplus (S_{241} \oplus S_{207} \oplus S_{204})S_{77} \oplus S_{77}  \end{aligned}  $	$S_{11}$
42	$  \begin{aligned}  S_{114} &= z_7 \oplus S_{19} \oplus S_{161} \oplus S_{118} \oplus S_{242}(S_{68} \oplus S_{30} \oplus S_7) \\  &\oplus S_{242}(S_{200} \oplus S_{167} \oplus S_{161}) \oplus (S_{200} \oplus S_{167} \oplus S_{161}) \\  &(S_{68} \oplus S_{30} \oplus S_7) \oplus (S_{237} \oplus S_{203} \oplus S_{200})S_{118} \\  &\oplus (S_{237} \oplus S_{203} \oplus S_{200})S_{73} \oplus S_{73}  \end{aligned}  $	—
43	$  \begin{aligned}  S_{110} &= z_3 \oplus S_{15} \oplus S_{157} \oplus S_{114} \oplus S_{238}(S_{64} \oplus S_{26} \oplus S_3) \\  &\oplus S_{238}(S_{196} \oplus S_{163} \oplus S_{157}) \oplus (S_{196} \oplus S_{163} \oplus S_{157}) \\  &(S_{64} \oplus S_{26} \oplus S_3) \oplus (S_{233} \oplus S_{199} \oplus S_{196})S_{114} \\  &\oplus (S_{233} \oplus S_{199} \oplus S_{196})S_{69} \oplus S_{69}  \end{aligned}  $	—
44	$  \begin{aligned}  S_{56} &= z_{44} \oplus S_{151} \oplus S_{198} \oplus S_{155} \oplus S_{279}(S_{105} \oplus S_{67} \oplus S_{44}) \\  &\oplus S_{279}(\overline{S_{237}} \oplus \overline{S_{204}} \oplus \overline{S_{198}}) \oplus (\overline{S_{237}} \oplus \overline{S_{204}} \oplus \overline{S_{198}}) \\  &(S_{105} \oplus S_{67} \oplus S_{44}) \oplus (S_{274} \oplus \overline{S_{240}} \oplus \overline{S_{237}})\overline{S_{155}} \\  &\oplus (S_{274} \oplus \overline{S_{240}} \oplus \overline{S_{237}})\overline{S_{110}} \oplus \overline{S_{110}}  \end{aligned}  $	$S_{279}$
45	$  \begin{aligned}  S_{57} &= z_{45} \oplus S_{152} \oplus S_{199} \oplus S_{156} \oplus S_{280}(S_{106} \oplus S_{68} \oplus S_{45}) \\  &\oplus S_{280}(\overline{S_{238}} \oplus \overline{S_{205}} \oplus \overline{S_{199}}) \oplus (\overline{S_{238}} \oplus \overline{S_{205}} \oplus \overline{S_{199}}) \\  &(S_{106} \oplus S_{68} \oplus S_{45}) \oplus (S_{275} \oplus \overline{S_{241}} \oplus \overline{S_{238}})\overline{S_{156}} \\  &\oplus (S_{275} \oplus \overline{S_{241}} \oplus \overline{S_{238}})\overline{S_{111}} \oplus \overline{S_{111}}  \end{aligned}  $	$S_{280}$
46	$  \begin{aligned}  S_{58} &= z_{46} \oplus S_{153} \oplus S_{200} \oplus S_{157} \oplus S_{281}(S_{107} \oplus S_{69} \oplus S_{46}) \\  &\oplus S_{281}(\overline{S_{239}} \oplus \overline{S_{206}} \oplus \overline{S_{200}}) \oplus (\overline{S_{239}} \oplus \overline{S_{206}} \oplus \overline{S_{200}}) \\  &(\overline{S_{107}} \oplus \overline{S_{69}} \oplus \overline{S_{46}}) \oplus (S_{276} \oplus \overline{S_{242}} \oplus \overline{S_{239}})\overline{S_{157}} \\  &\oplus (S_{276} \oplus \overline{S_{242}} \oplus \overline{S_{239}})\overline{S_{112}} \oplus \overline{S_{112}}  \end{aligned}  $	$S_{281}$
47	$  \begin{aligned}  S_{59} &= z_{47} \oplus S_{154} \oplus S_{201} \oplus S_{158} \oplus S_{282}(S_{108} \oplus S_{70} \oplus S_{47}) \\  &\oplus S_{282}(\overline{S_{240}} \oplus \overline{S_{207}} \oplus \overline{S_{201}}) \oplus (\overline{S_{240}} \oplus \overline{S_{207}} \oplus \overline{S_{201}}) \\  &(\overline{S_{108}} \oplus \overline{S_{70}} \oplus \overline{S_{47}}) \oplus (S_{277} \oplus \overline{S_{243}} \oplus \overline{S_{240}})\overline{S_{158}} \\  &\oplus (S_{277} \oplus \overline{S_{243}} \oplus \overline{S_{240}})\overline{S_{113}} \oplus \overline{S_{113}}  \end{aligned}  $	$S_{282}$
48	$  \begin{aligned}  S_{60} &= z_{48} \oplus S_{155} \oplus S_{202} \oplus S_{159} \oplus S_{283}(S_{109} \oplus S_{71} \oplus S_{48}) \\  &\oplus S_{283}(\overline{S_{241}} \oplus \overline{S_{208}} \oplus \overline{S_{202}}) \oplus (\overline{S_{241}} \oplus \overline{S_{208}} \oplus \overline{S_{202}}) \\  &(\overline{S_{109}} \oplus \overline{S_{71}} \oplus \overline{S_{48}}) \oplus (S_{278} \oplus \overline{S_{244}} \oplus \overline{S_{241}})\overline{S_{159}} \\  &\oplus (S_{278} \oplus \overline{S_{244}} \oplus \overline{S_{241}})\overline{S_{114}} \oplus \overline{S_{114}}  \end{aligned}  $	$S_{283}$

At this point, we like to explain about certain ‘unit’ cost related to exact complexity. Such unit cost may involve several computations related to the cipher operations. In a most generic way, given a  $k$ -bit secret key, the exhaustive attack asks for a complexity of  $2^k$  units, where each unit may require several CPU clocks. While mounting the TMDTO attack the same situation is valid. Thus, in our technique, we also consider all the operations as unit cost. However, we will point out a few cases when our calculations are most costly and that should be taken care of in the complexity analysis. For example, simply generating a 293-bit key stream (that will become the state  $\eta$ ) of ACORN v3 from a state  $\zeta$  requires 0.088s in our computing facility. However, to recover the 47 bits of the state from 47 bits of key stream and the remaining state bits requires a time of 0.076s, which is almost as same as the time taken to generate  $\zeta$ . Thus, no additional complexity is required for solving. Hence for this scenario our parameters are as follows. We can take  $T' = 2^{122}$ ,  $M' = 2^{124}$  and  $D' = 2^{61}$ . Then,  $T = T' \cdot 2^0 = 2^{122}$ ,  $M = M' = 2^{124}$ ,  $D = 2^\psi \cdot D' = 2^{47} \cdot 2^{61} = 2^{108}$ ,  $P = P' = \frac{N'}{D'} = 2^{185}$ .

### 3.2 Knowledge of 53 Bits of State from 60 Key Stream Bits

We follow a similar procedure as mentioned in Sect. 3.1. However, when the SAT solver is populated with equations and is set to find all possible solutions for 53 state bits using only 53 key stream bits, the SAT solver fails to find a unique solution. Instead, we get multiple solutions, where each solution provides the same 53-bit key stream pattern. To combat this problem, we involve a new idea. Instead of searching for a 53-bit pattern (say 53 continuous 0’s), we search for a 240-bit pattern where the first 53-bit sequence and the last 7-bit sequence are fixed (say to 0’s). This is based on the fact that the key stream sequence generated by all solutions are different. The SAT solver identifies the difference between the sequence of last 7 bits and removes all additional solutions. However, this gives us an additional Data complexity of  $2^7$ . Considering this constraint into the SAT solver in a similar fashion, (as explained in Sect. 2.1), we get the data mentioned in Table 1. However, in very few cases, two solutions sets are possible which generate the same keystream. Since the proportion is very small and our success probability is  $\frac{2^{14}-1}{2^{14}}$ , the time complexity should be multiplied by  $T' = T' \times \frac{2^{14}}{2^{14}-1} \approx T' \times 1 = T'$ . However, we still attempt to deal with this edge case scenario of two solutions. The idea is to simply discard the second solution during the offline phase and continue with the first solution set. The matrix stopping rule ensures the entire search space is covered with negligible collision. During the online phase, the adversary can access few more key stream bits following the fixed pattern in the key stream and hence conclude with the final solution. Our experiments show that 7 more key stream bits, i.e. 67 key stream bits in total are enough to find a unique solution.

Similar to Sect. 3.1 the time taken for solving equations is of the same order of generating  $\zeta$ , hence  $T = T'$ .

–  $T = T' = 2^{120}$  is the total time complexity of the attack,

- $M = M' = 2^{120}$  is the amount of memory required,
- $D = D' \times 2^{60} = 2^{120}$  where  $D' = 2^{60}$ , since the adversary must succeed in finding a 60-bit pattern,
- $P = \frac{N'}{D'} = 2^{180}$  is the preprocessing time for formulating tables.

### 3.3 Knowledge of 49 Bits of State from 49 Key Stream Bits and Fixing 10 State Bits

Here we consider the third approach which is similar to what has been recently considered in [7] for a TMDTO attack against Lizard [6]. We consider that  $\psi$  state bits can be recovered from  $\psi$  many key stream bits and rest of the state bits, but  $\tau$  many state bits has to be fixed to a specific pattern. This follows the idea mentioned in Sect. 2.2. In this case we go back to single preprocessing table. We will consider  $\psi = 49$  here, with  $\tau = 10$ . That is from  $\psi$  bits of key stream and the remaining  $(n - \psi)$  state bits (out of which  $\tau$  are fixed to a specific pattern), we will be able to solve for the  $\psi$  bits of the state. The initial table preparation goes as follows. We start with a  $(n - \psi - \tau)$  bit random pattern and then take a specific pattern for  $\psi$ . Also the fixed pattern of  $\phi$  is known. Now, using the equations as described in Sect. 2.2, we solve for the rest  $\psi$  bits of the state. This gives the complete state. Then we run the PRGA for  $n - \tau$  times. The initial  $\psi$  bits will be as fixed. The remaining  $(n - \psi - \tau)$  pseudorandom bits will be considered as the part of the next state bits. Thus, we have  $T'M' = 2^{n-\psi-\tau} = 2^{293-49-10} = 2^{234}$ . Let us take  $T' = 2^{112}$  and  $M' = 2^{122}$ , which also gives,  $D' = \sqrt{T'} = 2^{56}$ . Thus, we will now have the following parameters.

- $D = D' \cdot 2^{\psi+\tau} = 2^{56+49+10} = 2^{115}$ , as the specific pattern  $\psi$  should come towards consulting the table, and also for a good success rate to have the specific  $\tau$  bit pattern in the state we need to try  $2^\tau$  many times,
- $M = M' = 2^{122}$ ,
- $T = T' \cdot 2^\tau = 2^{112+10} = 2^{122}$ , as we only consult the preprocessing table when the specific  $\psi$  bit pattern appears in the key stream, but we need to try  $2^\tau$  times as we have that more data and here the solution time can be estimated from the operations in the equations and that can subsumed in the PRGA effort,
- $P = P' = \frac{N'}{D'} = 2^{234-56} = 2^{178}$ .

A similar online parameter in this respect can be obtained considering the equation  $5\psi + 2\tau = n$ . Here,  $\psi = 49$ , by fixing  $\tau = 10$ . However, we can easily increase  $\tau$  to 24 to satisfy the equation  $5\psi + 2\tau = 5 \cdot 49 + 2 \cdot 24 = 293 = n$ . That is we will fix 24 state bits to a specific pattern. In this case the online complexity becomes  $T = M = D = 2^{\frac{n-\psi}{2}} = 2^{\frac{293-49}{2}} = 2^{122}$ . However, the preprocessing becomes less, which is  $P = 2^{\frac{n+\psi}{2}} = 2^{\frac{293+49}{2}} = 2^{171}$ .

## 4 Conclusion

In this paper we have studied how certain portion of the state of ACORN v3 can be obtained from key stream and guessing or fixing the remaining state bits. We



attempt that problem by generating a set of equations and feeding that to SAT solver. At the same time, we try to consider the structure of the equations and solve a set of equations without using the SAT solver. Several examples with different parameters are presented. Based on those parameters, we note different time-memory-data trade-off for attacking ACORN v3. Indeed it is possible to mount the attack where the online complexity is less than the exhaustive key search. The pre-processing effort is higher than exhaustive search but it can be reduced further by increasing the amount of data or by recovering more internal state bits. While our observations do not refute any security claim of the cipher, the study adds certain insight towards the cryptanalysis and may lead to further research in this area.

**Acknowledgements.** The first author would like to thank Department of Science and Technology DST-FIST Level-1 Program Grant No. SR/FST/MSI-092/2013 for providing the computational facilities.

## References

1. Babbage, S.: A space/time tradeoff in exhaustive search attacks on stream ciphers. In: European Convention on Security and Detection. IEEE Conference Publication, no. 408, May 1995
2. Biryukov, A., Shamir, A., Wagner, D.: Real time cryptanalysis of A5/1 on a PC. In: Goos, G., Hartmanis, J., van Leeuwen, J., Schneier, B. (eds.) FSE 2000. LNCS, vol. 1978, pp. 1–18. Springer, Heidelberg (2001). [https://doi.org/10.1007/3-540-44706-7\\_1](https://doi.org/10.1007/3-540-44706-7_1)
3. Biryukov, A., Shamir, A.: Cryptanalytic time/memory/data tradeoffs for stream ciphers. In: Okamoto, T. (ed.) ASIACRYPT 2000. LNCS, vol. 1976, pp. 1–13. Springer, Heidelberg (2000). [https://doi.org/10.1007/3-540-44448-3\\_1](https://doi.org/10.1007/3-540-44448-3_1)
4. CAESAR. <http://competitions.cr.yt.to/caesar.html>
5. Golić, J.D.: Cryptanalysis of alleged A5 stream cipher. In: Fumy, W. (ed.) EUROCRYPT 1997. LNCS, vol. 1233, pp. 239–255. Springer, Heidelberg (1997). [https://doi.org/10.1007/3-540-69053-0\\_17](https://doi.org/10.1007/3-540-69053-0_17)
6. Hamann, M., Krause, M., Meier, W.: LIZARD - a lightweight stream cipher for power-constrained devices. In: FSE 2017. <http://eprint.iacr.org/2016/926>, <http://tosc.iacr.org/index.php/ToSC/article/view/584>
7. Maitra, S., Sinha, N., Siddhanti, A., Anand, R., Gangopadhyay, S.: A TMDTO attack against lizard (2017). <http://eprint.iacr.org/2017/647>
8. SAGE Mathematics Software. Free Software Foundation Inc. (2009). <http://www.sagemath.org>. (Open source project initiated by W. Stein and contributed by many)
9. Sarkar, S., Banik, S., Maitra, S.: Differential fault attack against grain family with very few faults and minimal assumptions. IEEE Trans. Comput. **64**(6), 1647–1657 (2015)
10. Wu, H.: ACORN: a lightweight authenticated cipher (v3). <https://competitions.cr.yt.to/round3/acornv3.pdf>