A new chosen IV statistical distinguishing framework to attack symmetric ciphers, and its application to ACORN-v3 and Grain-128a

Vahid Amin Ghafari & Honggang Hu*

Key Laboratory of Electromagnetic Space Information, Chinese Academy of Sciences, University of Science and Technology of China, Hefei 230026*, China*

Abstract We propose a new attack framework based upon cube testers and d-monomial tests. The d-monomial test is a general framework for comparing the ANF of the symmetric cipher's output with ANF of a random Boolean function. In the d-monomial test, the focus is on the frequency of the special monomial in the ANF of Boolean functions, but in the proposed framework, the focus is on the truth table.

We attack ACORN-v3 and Grain-128a and demonstrate the efficiency of our framework. We show how it is possible to apply a distinguishing attack for up to 676 initialization rounds of ACORN-v3 and 171 initialization rounds of Grain-128a using our framework. The attack on ACORN-v3 is the best practical attack (and better results can be obtained by using more computing power).

One can apply distinguishing attacks to black box symmetric ciphers by the proposed framework, and we suggest some guidelines to make it possible to improve the attack by analyzing the internal structure of ciphers. The framework is applicable to all symmetric ciphers and hash functions. We discuss how it can reveal weaknesses that are not possible to find by other statistical tests. The attacks were practically implemented and verified.

Keywords chosen IV attack, distinguishing attack, statistical attack, cube testers, authenticated encryption

Citation Ghafari VA, Hu H. A new chosen IV statistical distinguishing framework to attack symmetric ciphers, and its application to ACORN-v3 and Grain-128a.

1 Introduction

ACORN-v3 has been accepted as an authenticated cipher candidate in the third-round of CAESAR (Competition for Authenticated Encryption: Security, Applicability, and Robustness) [1]. The CAESAR competition has been active since 2013 with 55 candidates [2]. Some attacks were applied to ACORN [3–8] in the first and second round of the competition, and the cipher was tweaked to ACORN-v3. A cube attack on 477 initialization rounds of ACORN-v2 was applied to recover the secret key with a time complexity of 2^{35} [8].

Two attacks on ACORN-v3 were published [9, 10]. The only passive attack on ACORN-v3 is cube attack [10]. Todo et al. (in [10]) claimed that cube attacks based on the division property on 704 and 649 initialization rounds of ACORN-v3 can recover one bit of the secret key with time complexities of 2^{122} and 2^{109}, respectively. These proposed attacks are impractical (because of the high time complexity) with unknown success probability [11].

* Corresponding author (email: hghu2005@ustc.edu.cn)

Our attack based on the new framework currently is the best practical attack (with regard to the time complexity on more initialization rounds) on ACORN-v3, to the best of our knowledge. Our framework distinguishes between random sequences and keystreams of ACORN-v3 for up to 676 initialization rounds with a time complexity of 200×2^{33}. One of the advantage of the proposed framework is that it is easy to adjust the accuracy of the test based on the available computing power. Therefore, better results (e.g., against up to 900 initialization rounds) can be obtained by more computational complexity.

Grain-v1 was introduced as a selected stream cipher in the hardware profile of the eSTREAM project [12,13] and Grain-128 was presented as a 128-bit security version in 2006 [14]. Some attacks were applied to Grain-128 [15–20], and Grain-128a was proposed as a stronger version of the Grain family with 128-bit security in 2011 [21]. Grain-128a has been standardized for radio frequency identification (RFID) devices by ISO/IEC [22]. The only type of passive single-key attack on Grain-128a is the conditional differential attack on the reduced version (the active fault attack [23] and related key chosen IV attack [24, 25] were applied to the cipher), but Grain-128a is considered secure from the practical point of view.

A distinguishing attack was mounted on Grain-128a with 177 initialization rounds in a conditional differential attack scenario, and also a nonrandomness was published on the 189 initialization rounds in a chosen key/IV conditional differential attack scenario [26]. In 2016, a key recovery attack was introduced on Grain-128a with 177 initialization rounds in a conditional differential attack scenario, and also a nonrandomness was presented for 195 initialization rounds in a chosen key/IV conditional differential attack scenario [27].

Our framework enables distinguishing between random sequences and keystreams of Grain-128a for up to 171 initialization rounds[1)] with a time complexity of 200×2^{28}. Better results can be obtained by more computational complexity.

The d-monomial test (or Statistical Möbius Analysis) was introduced by Filiol [28]. The number of monomials of degree d was considered in the Boolean function of the first bit of a keystream, and it was compared with the expected number in a random Boolean function. The test was done only on low degree monomials. The test was generalized and extended in [29,30]. In the extended version, instead of considering the number of monomials of a fixed degree, the numbers of monomials of several degrees are considered in the test. Another extended version of the test used a maximum degree monomial [30]. A greedy algorithm was proposed for finding a suitable subset of IV bits for finding the maximum degree monomial [31] and this algorithm was improved in 2017 [32].

Our attack is a new chosen IV statistical framework built upon d-monomial tests and cube testers. We consider some high degree monomials in the Boolean functions of the keystreams (by using cubes), and we propose a statistical test over the truth table outputs (TTs) of the functions. We consider some sets of TTs, and we compare the number of elements in every set with the expected numbers in random cases. It is expected that in a set of random Boolean functions; there exist Boolean functions with the specific numbers of ones in the TTs proportionally. A toy example of the proposed framework is as follows.

Suppose every cipher is a Boolean function with secret key and IV inputs and keystream output. We expect that in a set of 16 random Boolean functions in 2 variables, there should exist approximately one function with all zeros, four functions with 1 one, six functions with 2 ones, four functions with 3 ones, and one function with 4 ones in the set of TTs (see Table 1). We obtain the TT for two bits of the IV while other IV and secret key bits are fixed. Then we repeat this process under many different secret keys (e.g. 200 times) and we consider the numbers of TTs with 4 ones, 3 ones, 2 ones, 1 one, and all zeros. If there exists more than expected frequency of a type of TT, we can distinguish the input from a random set. For example, the probability that a random function has 3 ones in its TT is $4/16$. Hence, we expect $200 \times (4/16) = 50$ TTs with 3 ones. If there exists much difference between the expected and the observed values, we can distinguish the first bits of the keystreams of the cipher from random sequences.

In d-monomial tests (and in many statistical tests similar to it [33]), the focus is on the frequencies of the special monomials in the ANF of the Boolean function, but in the proposed framework, the focus is

1) An earlier result of this attack (i.e. a distinguishing attack for up to 169 initialization rounds of Grain-128a) was published in CyberC 2017 [34]. In this paper, we present our attack as a general framework, apply it to ACORN-v3, and extend our attack on Grain-128a up to 171 initialization rounds.

Table 1 The grouping of the 16 random Boolean functions in 2 variables based on the number of ones in TT

TT with all zeros	TTs with 1 one	TTs with 2 ones	TTs with 3 ones	TT with 4 ones
(0,0,0,0)	(1,0,0,0)	(1,1,0,0)	(1,1,1,0)	(1,1,1,1)
	(0,1,0,0)	(0,1,1,0)	(1,1,0,1)	
	(0,0,1,0)	(0,0,1,1)	(1,0,1,1)	
	(0,0,0,1)	(1,0,0,1)	(0,1,1,1)	
		(1,0,1,0)		
		(0,1,0,1)		

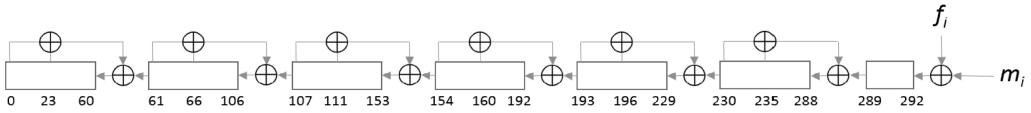

Figure 1 The block diagram of ACORN-v3 [1]

on the TTs. As our test is more general than d-monomial tests, it can reveal weaknesses that cannot be found by d-monomial tests.

The paper is organized as follows. ACORN-v3, Grain-128a, cube testers, and a statistical test are presented in Section 2. Then, the new framework is described in Section 3. In Section 4 and Section 5, we present our chosen IV statistical attack on ACORN-v3 and Grain-128a, respectively. Finally, we conclude the paper in Section 6.

2 Background

ACORN-v3, Grain-128a, cube testers, and the goodness-of-fit test are briefly described. As our attacks are on the reduced version of the ciphers and the authentication processes are effective after the initialization phase, we do not describe the authentication processes.

2.1 Brief description of ACORN-v3

Authenticated encryption ACORN-v3 accepts a 128-bit secret key $(k_0, ..., k_{127})$ and 128-bit IV $(v_0, ..., v_{127})$. The internal state of ACORN-v3 is 293 bits in the i^{th} round $(S_{i,0}, ..., S_{i,292})$. The internal state consists of six LFSRs and one buffer as shown in Figure 1. The maj and ch sub-functions are used in ACORN-v3 as follows.

$$maj(x; y; z) = (x \cdot y) \oplus (x \cdot z) \oplus (y \cdot z) \tag{1}$$

$$ch(x; y; z) = (x \cdot y) \oplus ((x \oplus 1) \cdot z) \tag{2}$$

The f_i function is the overall feedback bit for the i^{th} round and m_i is the message bit for the i^{th} round. f_i is computed as follows at each round. ca_i and cb_i are single bits which depend on the cipher phase.

$$f_i = S_{i,0} \oplus (S_{i,107} \oplus 1) \oplus maj(S_{i,244}; S_{i,23}; S_{i,160)} \oplus (ca_i \cdot S_{i,196}) \oplus (cb_i \cdot ks_i) \tag{3}$$

The feedback functions of the LFSRs are as follows.

$$S_{i,289} = S_{i,289} \oplus S_{i,235} \oplus S_{i,230} \tag{4}$$

$$S_{i,230} = S_{i,230} \oplus S_{i,196} \oplus S_{i,193} \tag{5}$$

$$S_{i,193} = S_{i,193} \oplus S_{i,160} \oplus S_{i,154} \tag{6}$$

$$S_{i,154} = S_{i,154} \oplus S_{i,111} \oplus S_{i,107} \tag{7}$$

$$S_{i,107} = S_{i,107} \oplus S_{i,66} \oplus S_{i,61} \tag{8}$$

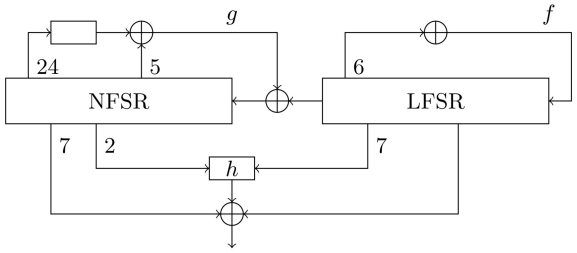

Figure 2 Grain-128a in the keystream generation phase [21]

$$S_{i,61} = S_{i,61} \oplus S_{i,23} \oplus S_{i,0} \tag{9}$$

The initialization phase consists of key/IV loading and 1792 rounds as follows.

- $S_{-1792,0} = S_{-1792,1} = ... = S_{-1792,292} = 0$
- $m_{1792+i} = k_i$ for $i = 0$ to 127
- $m_{1792+128+i} = IV_i$ for $i = 0$ to 127
- $m_{1792+256} = k_{i \ mod\ 128} \oplus 1$ for $i = 0$
- $m_{1792+256+i} = k_{i \ mod\ 128}$ for $i = 1$ to 1535
- $ca_{1792+i} = 1$ for $i = 0$ to 1791
- $cb_{1792+i} = 1$ for $i = 0$ to 1791
- 1792 initialization rounds

2.2 Brief description of Grain-128a

The Grain-128a cipher accepts a 128-bit secret key $(k_0, , k_{127})$ and 96-bit IV $(v_0, , v_{95})$. The internal state consists of a 128-bit LFSR $(l_0, , l_{127})$ and 128-bit NFSR $(n_0, , n_{127})$. The feedback functions are f and g for the LFSR and NFSR, respectively. The keystream is produced from some bits of the LFSR and NFSR as shown in Figure 2 [21].

The feedback function of the LFSR is as follows.

$$l_{(i+128)} = l_i \oplus l_{(i+7)} \oplus l_{(i+38)} \oplus l_{(i+70)} \oplus l_{(i+81)} \oplus l_{(i+96)} \tag{10}$$

The feedback function of the NFSR is as follows.

$$\begin{aligned} n_{(i+128)} = {} & l_i \oplus n_i \oplus n_{(i+26)} \oplus n_{(i+56)} \oplus n_{(i+91)} \cdot n_{(i+96)} \\ & \oplus n_{(i+3)} \cdot n_{(i+67)} \oplus n_{(i+11)} \cdot n_{(i+13)} \oplus n_{(i+17)} \cdot n_{(i+18)} \\ & \oplus n_{(i+27)} \cdot n_{(i+59)} \oplus n_{(i+40)} \cdot n_{(i+48)} \oplus n_{(i+61)} \cdot n_{(i+65)} \\ & \oplus n_{(i+68)} \cdot n_{(i+84)} \oplus n_{(i+88)} \cdot n_{(i+92)} \cdot n_{(i+93)} \cdot n_{(i+95)} \\ & \oplus n_{(i+22)} \cdot n_{(i+24)} \cdot n_{(i+25)} \oplus n_{(i+70)} \cdot n_{(i+78)} \cdot n_{(i+82)} \end{aligned} \tag{11}$$

The h function and output function are as follows.

$$h_i = n_{(i+12)} \cdot l_{(i+8)} \oplus l_{(i+13)} \cdot l_{(i+20)} \oplus n_{(i+95)} \cdot l_{(i+42)} \oplus l_{(i+60)} \cdot l_{(i+79)} \oplus n_{(i+12)} \cdot n_{(i+95)} \cdot l_{(i+94)} \tag{12}$$

$$z_i = h_i \oplus l_{(i+93)} \oplus n_{(i+2)} \oplus n_{(i+15)} \oplus n_{(i+36)} \oplus n_{(i+45)} \oplus n_{(i+64)} \oplus n_{(i+73)} \oplus n_{(i+89)} \tag{13}$$

In the initialization phase, the bits of the secret key are loaded into the NFSR, and the bits of the IV are loaded into the first 96 bits of the LFSR. The last bits of the LFSR are filled with 31-bit ones and one bit zero. Grain-128a is clocked 256 times without producing any keystream, and the output bits are fed to the cipher as shown in Figure 3. Thus, the first bit of the keystream is produced in the 257^{th} round [21].

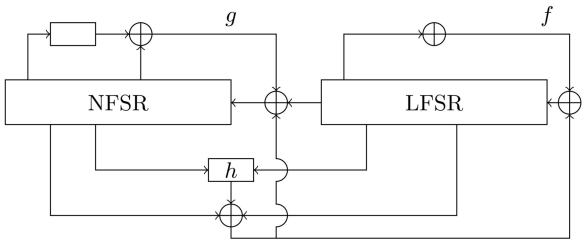

Figure 3 Grain-128a in the keystream generation phase [21]

2.3 Cube testers

Our framework is based upon cube testers [35]. A simple example of a cube tester is explained in the following. Suppose that the Boolean function of the first bit of a keystream is as follows.

$$f(x_1, x_2, x_3, x_4, x_5) = x_1 + x_2x_3 + x_1x_3(x_2 + x_4) + x_1x_5 \tag{14}$$

If we consider x_1 and x_3 as cube variables (CVs), the superpoly variables (SVs) are x_2 and x_4. The polynomial $x_2 + x_4$ is a superpoly of the CVs. It is known that

$$\begin{aligned}\sum_{x_1,x_3} f(x_1, x_2, x_3, x_4, x_5) &= f(0, x_2, 0, x_4, x_5) + f(0, x_2, 1, x_4, x_5) + f(1, x_2, 0, x_4, x_5) + f(1, x_2, 1, x_4, x_5) \\ &= x_2 + x_4.\end{aligned} \tag{15}$$

If one sums (XORs) the outputs of a Boolean function based on all possible values of a set of inputs (i.e. CVs), the superpoly of the CVs in the function can be obtained. It is possible to test a superpoly for various testable properties such as the presence of linear variables, constantness, and low degree [35].

2.4 Goodness-of-fit test

We use the goodness-of-fit test to determine whether a set of superpolys is random or not. The test is between the observed frequencies of occurrences and the expected frequencies as follows.

$$\chi^2 = \sum_{i=1}^{n} \frac{(o_i - e_i)^2}{e_i} \tag{16}$$

The χ^2 distribution is very close to the chi-square distribution with $v = n - 1$ degrees of freedom. The symbol o_i and e_i are the observed and expected frequency of the i^th occurrences, respectively. In our example (a set of 16 random Boolean functions in 2 variables), if we consider the number of TTs with only 1 one and 3 zeros, e_i is 4 (i.e. (1000, 0100, 0010, 0001).

The null hypothesis (H_0) is that distribution of observed and expected frequencies are consistent. If observed frequencies differ significantly from expected frequencies, the χ^2 will be large and the fit is weak. A good fit (i.e., small χ^2) states that we cannot reject H_0 based on the observed sample. The maximum value of χ^2 (based on the tolerable error) at which we cannot reject H_0, is χ^2_α. If $\chi^2 > \chi^2_\alpha$, we reject H_0 and the Boolean function set is nonrandom (i.e., it is related to a cipher). We suppose $\alpha = 0.05$, which means that the probability of rejecting H_0 when it is true is 5%.

3 New chosen IV statistical attack framework

Suppose that there are two resources that produce sequences: One is a cipher and other a random sequence generator. Attackers are interested in distinguishing between the sequences from the two resources. They can choose IV bits and obtain the first bits of the sequences. It is obvious that IV bits do not affect random sequence generators. We assume secret keys are random and unknown to the attackers.

Table 2 The expected frequencies of Boolean functions for the different numbers of ones in 200 random Boolean functions in 4 variables

0,1,2,3$^{\Delta}$	4	5	6	7	8	9	10	11	12	13,14,15,16$^{\Delta}$
2	5.5	13.3	24.4	34.9	39.3	34.9	24.4	13.3	5.5	2

$^{\Delta}$Note that low frequencies of ones are gathered together because at least the 80% expected frequencies should be more than 5, and all expected frequencies should be more than 1 in the goodness-of-fit test [36].

The first and most important part of the framework is choosing suitable SVs and CVs from the IV bits. The hardest part of the cube attacks is to find the best SVs and CVs. We propose some general guidelines for choosing the SVs and CVs so attackers to determine the best choice faster. The first guideline is to choose IV bits as SVs and CVs that are later combined with other bits and together. The second guideline is to select IV bits as SVs and CVs that later affect the states and keystreams. The last guideline is to choose as few bits as possible for the SVs (usually 4, 5, or 6 bits) and to choose as many bits as possible for the CVs. The focus of the attack will be on the higher degree monomials if more CVs are selected. Investigation of the structure of the cipher is very important, although it is also possible to apply the framework to black box structures.

Thus, an attacker chooses the SVs and CVs, and then sets the other IV bits to zero. He receives the first bits of the keystreams over all possible CVs. He sums these bits and obtains the superpoly [35]. He obtains TT of the superpoly by setting all possible values of the SVs. Then, he counts the number of ones in the TT (the counted values will be between 0 and 2^M while M is the number of SVs). In our attacks, we used 4 SVs, thus the number of the ones in the TT was between 0 and 16.

The attacker receives the first bits of the keystreams for many unknown secret keys (e.g., 200) and he repeats the process for every new secret key. He saves the frequencies of all possible numbers of ones in the TTs (e.g. with 4 SVs, he determines how many TTs out of the 200 cases have 0 ones, 1 one, 2 ones, , 16 ones). The attacker compares these frequencies with the expected frequencies. If the observed and expected frequencies are different enough, he has detected nonrandomness.

If the attacker can find suitable SVs and CVs in the offline phase of the attack, he can apply a distinguishing attack to the cipher in the online phase of the attack. Hence, if the attacker can detect the nonrandomness in the online phase, the source of bitstreams is the cipher and otherwise, the bitstreams are from random sequence generators.

We selected four variables as the SVs in the attacks. Thus, every TT consisted of 16 bits in its output. There are 2^{16} different TTs in this situation. In our framework, we consider TTs on the 17 separate sets. It is not possible to investigate all of the 2^{16} TTs and other statistical attacks only consider a very small part of them. The main difference between the proposed framework and other statistical attacks (like [28–33]) is that we focus on TTs while they focus on the limited numbers of monomials in the ANF. By using our framework, an attacker can apply a relatively comprehensive evaluation (although the evaluation is still limited by the time complexity). In other words, the proposed framework allows an attacker to succeed in finding distinguishing attacks on ciphers for which other statistical attacks fail.

For example, the expected frequency of Boolean functions with 1 one (and 15 zeros) in the TT is $\binom{16}{1} = 16$ in a set of 2^{16} random Boolean functions in 4 variables (i.e., there are 16 TTs with only 1 one in a set of all possible Boolean functions in 4 variables). The expected frequency of Boolean functions with r ones (and $16-r$ zeros) in TT is $m \times \binom{16}{r}/2^{16}$ in a set of m random Boolean functions in 4 variables. In Table 2, the expected numbers of Boolean functions for the different numbers of ones is presented for 200 random Boolean functions.

There are ten independent groups according to the grouping in Table 2. Hence, the degree of freedom is ten. Supposing $\alpha = 0.05$, we found $\chi^2_{0.05} = 18.3$ from the chi-square distribution table.

In the proposed framework, there are two criteria for identifying nonrandom sequences. The first criterion is that more than 5% of chi-square values are more than 18.3 (because with $\alpha = 0.05$, it is expected that in random sequences about 5% of chi-square values are more than 18.3). We used this criterion to identify the nonrandomness in the keystreams of Grain-128a with 171 initialization rounds.

The second criterion for identifying the nonrandom sequences is that the chi-square values are very

Table 3 SVs and CVs for the distinguishing attack on ACORN-v3 with up to 676 initialization rounds

	Number of bits	Position in IV
SVs	4	0, 1, 2, 3
CVs	29	99 - 127

Table 4 SVs and CVs for the distinguishing attack on Grain-128a with up to 171 initialization rounds

	Number of bits	Position in IV
SVs	4	0, 1, 2, 3
CVs	27	40 - 55, 117 - 127

large. The larger chi-square values show more nonrandomness in the TTs of superpolys. In our experiments, we found that in random sequences (e.g., the keystreams of Grain-128a with 2×256 initialization rounds) the chi-square values were always less than 40, whereas the maximum possible value for the chi-square is 18605 in the proposed framework. We used this criterion to identify the nonrandomness in the keystreams of ACORN-v3 with 676 initialization rounds.

One of the differences between the two criteria is the number of repetitions of the test. Although the numbers of repetitions are dependent on the chi-square values, generally the test needs to be repeated more when using the first criterion to make a correct final decision. For example, the test may need to be repeated at least 100 times when using the first criterion, but only about 5 times when using the second criterion. Note that it is possible to apply the framework to the one byte (instead of one bit) of keystreams, although this variation was not helpful for the attacks on ACORN-v3 and Grain-128a, and the order of computational complexity of the attack is 2^N while N is the number of cube and superpoly variables.

4 Chosen IV statistical attack on ACORN-v3

Our best distinguishing attack was obtained on ACORN-v3 up to 676 initialization rounds by the proposed framework. The best result was obtained with 4 SVs and 29 CVs according to Table 3.

We ran the attack many times according to the CVs and SVs of Table 3 on ACORN-v3 with 676 initialization rounds. The chi-square values were more than 1000, which means an attacker can easily distinguish between the keystreams of reduced ACORN-v3 and random sequences. As secret keys are random and unknown, one can apply a distinguishing attack under a chosen IV scenario in the real world on ACORN-v3 up to 676 initialization rounds. The time complexity of the attack is 200×2^{33} encryption of ACORN-v3 (each test contains 200 repeats). The data complexity is 200×2^{33} keystream bits and the memory complexity is negligible.

We ran the test over the keystream of ACORN-v3 with 2×1792 initialization rounds. As we expected, chi-square values were less than 18.3 in about 95% of the cases (because we chose $\alpha = 0.05$). This result means that the test can identify the keystreams of ACORN-v3 with 2×1792 initialization rounds as a random sequences, and this is a proof for the attack and shows that the attack can distinguish between random sequences and keystreams of reduced ACORN-v3.

5 Chosen IV statistical attack on Grain-128a

Our best distinguishing attack was obtained on Grain-128a up to 171 initialization rounds (we previously published a distinguishing attack for up to 169 initial rounds of Grain-128a in CyberC 2017 [34]). The better results (e.g., up to 200 initialization rounds) can be obtained by more CVs and testing different CVs and SVs. The best result was obtained with 4 SVs and 24 CVs according to Table 4.

We ran the attack 129 times according to CVs and SVs of Table 4 on Grain-128a with 171 initialization rounds. The chi-square values were more than 18.3 in 13 tests (i.e., about 10%). Thus, an attacker can distinguish between the keystreams of reduced Grain-128a and random sequences. Note that we ran the cipher 129×200 times with random keys (each test repeated 200 times). As secret keys are random and unknown, one can apply a distinguishing attack under a chosen IV scenario in the real world against up to 171 initialization rounds of Grain-128a. The time complexity of the attack is 200×2^{28} encryption of Grain-128a. The data complexity is 200×2^{28} keystream bits and the memory complexity is negligible.

We ran the test over the keystream of Grain-128a with 2×256 initialization rounds. As we expected, the chi-square values were less than 18.3 in about 95% of the cases, which means that the test can identify the keystreams of Grain-128a with 2×256 initialization rounds as a random sequences. This proves the attack can distinguish between random sequences and keystreams of reduced Grain-128a.

6 Conclusion

A new chosen IV statistical distinguishing attack framework against symmetric ciphers and hash functions is proposed in this work. The attack is based on the comparison of the truth tables (TTs) of a cipher and TTs of random Boolean functions. We applied the proposed framework practically to ACORN-v3 and Grain-128a. ACORN-v3 authenticated encryption is a candidate in third-round of CAESAR competition and Grain-128a is a well-known stream cipher. We showed how it is possible to succeed in a distinguishing attack against up to 676 initialization rounds of ACORN-v3 and 171 initialization rounds of Grain-128a by our framework with time complexities of 200×2^{33} and 200×2^{28}, respectively. The attack on ACORN-v3 is the best practical attack and the attack on Grain-128a is very close to the best previous attacks. The new attack technique can reveal weaknesses that are not found by other statistical tests and the approach is easily adaptable to get better results by utilizing more computational power. The framework is suitable for a systematic and general attack, so we propose the framework as a mandatory statistical test for every symmetric cipher. It is possible to apply the framework to black box symmetric ciphers and also to improve the framework if the internal structure is known. We are expanding the proposed framework to attack other ciphers.

Acknowledgements This work was supported by CAS-TWAS Presidents Fellowship for International PhD program.

References

1 Wu H. ACORN: A lightweight authenticated cipher (v3). CAESAR (Competition for Authenticated Encryption: Security, Applicability, and Robustness). 2016, Available at https://competitions.cr.yp.to/round3/acornv3.pdf
2 Abed F, Forler C, Lucks S. General overview of the authenticated schemes for the first round of the caesar competition. Cryptology ePrint Archive, Report 2014/792, 2014
3 Salam MI, Wong KK, Bartlett H, et al. Finding state collisions in the authenticated encryption stream cipher ACORN. In: Proceedings of Proceedings of the Australasian Computer Science Week Multiconference, Canberra, 2016. 36-37
4 Dalai DK, Roy D. A state recovery attack on ACORN-v1 and ACORN-v2. In: Proceedings of International Conference on Network and System Security, Helsinki, 2017, 332-345
5 Zhang X, Feng X, Lin D. Fault attack on the authenticated cipher ACORN-v2. Security and Communication Networks, 2017, 2017:16
6 Roy D, Mukhopadhyay S. Some results on ACORN. Cryptology ePrint Archive, Report 2016/1132, 2016
7 Dey P, Rohit RS, Adhikari A. Full key recovery of ACORN with a single fault. Journal of Information Security and Applications, 2016, 29:57-64
8 Salam MI, Bartlett H, Dawson E, et al. Investigating cube attacks on the authenticated encryption stream cipher acorn. In: Proceedings of International Conference on Applications and Techniques in Information Security, Cairns, 2016, 15-26
9 Siddhanti AA, Sarkar S, Maitra S, et al. Differential fault attack on Grain-v1, ACORN-v3 and Lizard. Cryptology ePrint Archive, Report 2017/678, 2017
10 Todo Y, Isobe T, Hao Y, et al. Cube attacks on non-blackbox polynomials based on division property. In: Proceedings of CRYPTO'17, Santa Barbara, 2017. 250-279

11 Liu M. Degree evaluation of NFSR-based cryptosystems. In: Proceedings of CRYPTO'17, Santa Barbara, 2017. 227-249

12 Hell M, Johansson T, Meier W. Grain: a stream cipher for constrained environments. International Journal of Wireless and Mobile Computing, 2007, 2: 86-93

13 Babbage S, Canniere C, Canteaut A, et al. The eSTREAM portfolio. eSTREAM. ECRYPT Stream Cipher Project. 2008, 44

14 Hell M, Johansson T, Maximov A, et al. A stream cipher proposal: Grain-128. In: Proceedings of Information Theory, 2006 IEEE International Symposium on. 2006, Seattle, 2016. 1614-1618

15 Lee Y, Jeong K, Sung J, et al. Related-key chosen IV attacks on Grain-v1 and Grain-128. In: Proceedings of Australasian Conference on Information Security and Privacy, Wollongong, 2008. 321-335

16 Dinur I, Shamir A. Breaking Grain-128 with dynamic cube attacks. In: Proceedings of FSE'11, Lyngby, 2011. 167-187

17 Dinur I, Gneysu T, Paar C, et al. An experimentally verified attack on full Grain-128 using dedicated reconfigurable hardware. In: Proceedings of ASIACRYPT'11, Seoul, 2011. 327-343

18 Mihaljevic M, Gangopadhyay S, Paul G, et al. Generic cryptographic weakness of k-normal Boolean functions in certain stream ciphers and cryptanalysis of Grain-128. Periodica Mathematica Hungarica, 2012, 65(2): 205-27

19 Aumasson JP, Dinur I, Henzen L, et al. Efficient FPGA implementations of high-dimensional cube testers on the stream cipher Grain-128. In: Proceedings of SHARCS09 Special-purpose Hardware for Attacking Cryptographic Systems, Washington, 2009. 147

20 Knellwolf S, Meier W, Naya-Plasencia M. Conditional differential cryptanalysis of NLFSR-based cryptosystems. In: Proceedings of ASIACRYPT'10, Singapore, 2010. 130-45

21 Ågren M, Hell M, Johansson T, et al. A new version of Grain-128 with authentication. In: Proceedings of Symmetric Key Encryption Workshop, Lyngby, 2011. 2011

22 ISO/IEC 29167-13:2015. Crypto suite Grain-128A security services for air interface communications. Information Technology - Automated Identification and Data Capture Techniques Part 13. 2015

23 Banik S, Maitra S, Sarkar S. A differential fault attack on Grain-128a using MACs. In: Proceedings of SPACE'12, Chennai, 2012. 111-25.

24 Ding L, Guan J. Related key chosen IV attack on Grain-128a stream cipher. IEEE Transactions on Information Forensics and Security, 2013, 8: 803-809

25 Banik S, Maitra S, Sarkar S, et al. A chosen IV related key attack on Grain-128a. In: Proceedings of Australasian Conference on Information Security and Privacy, Brisbane, 2013, 13-26

26 Lehmann M, Meier W. Conditional differential cryptanalysis of Grain-128a. In: Proceedings of International Conference on Cryptology and Network Security, Darmstadt, 2012, 1-11

27 Ma Z, Tian T, Qi WF. Conditional differential attacks on Grain-128a stream cipher. IET Information Security, 2016, 11: 139-45

28 Filiol E. A new statistical testing for symmetric ciphers and hash functions. In: Proceedings of International Conference on Information and Communications Security, Singapore, 2002. 342-353

29 Saarinen MJ. Chosen-IV statistical attacks on eStream stream ciphers. In: Proceedings of Stream Ciphers Revisited SASC, Leuven, 2006. 94-103

30 Englund H, Johansson T, Turan MS. A framework for chosen IV statistical analysis of stream ciphers. In: Proceedings of INDOCRYPT'07, Chennai, 2007. 268-281

31 Stankovski P. Greedy distinguishers and nonrandomness detectors. In: Proceedings of INDOCRYPT'10, Hyderabad, 2010. 210-226

32 Karlsson L, Hell M, Stankovski P. Improved greedy nonrandomness detectors for stream ciphers. In: Proceedings of ICISSP'17, Porto, 2017. 225-232

33 Fischer S, Khazaei S, Meier W. Chosen IV statistical analysis for key recovery attacks on stream ciphers. In: Proceedings of AFRICACRYPT'08, Casablanca, 2008. 236-45

34 Ghafari VA, Hu H. A new chosen IV statistical attack on Grain-128a cipher. In: Proceedings of cyberc'17, Nanjing, 2017. in press

35 Aumasson JP, Dinur I, Meier W, Shamir A. Cube testers and key recovery attacks on reduced-round MD6 and Trivium. In: Proceedings of FSE'09, Leuven, 2009. 1-22

36 Cochran WG. Some methods for strengthening the common χ^2 tests. Biometrics, 1954, 10: 417-451