Hindawi
Security and Communication Networks
Volume 2019, Article ID 7429320, 5 pages
https://doi.org/10.1155/2019/7429320

Research Article

Algebraic Degree Estimation of ACORN v3 Using Numeric Mapping

Lin Ding,[1,2] **Lei Wang**,[1,3] **Dawu Gu**,[1] **Chenhui Jin**,[2] **and Jie Guan**[2]

[1]*Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai 200240, China*
[2]*PLA SSF Information Engineering University, Zhengzhou 450001, China*
[3]*Westone Cryptologic Research Center, Beijing 100000, China*

Correspondence should be addressed to Lin Ding; dinglin_cipher@163.com

Received 6 May 2019; Accepted 24 October 2019; Published 20 November 2019

Guest Editor: Leonel Sousa

ACORN v3 is a lightweight authenticated encryption cipher, which was selected as one of the seven finalists of CAESAR competition in March 2018. It is intended for lightweight applications (resource-constrained environments). By using the technique numeric mapping proposed at CRYPTO 2017, an efficient algorithm for algebraic degree estimation of ACORN v3 is proposed. As a result, new distinguishing attacks on 647, 649, 670, 704, and 721 initialization rounds of ACORN v3 are obtained, respectively. So far, as we know, all of our distinguishing attacks on ACORN v3 are the best. The effectiveness and accuracy of our algorithm is confirmed by the experimental results.

1. Introduction

ACORN, which is known as ACORN v1 [1], is a lightweight authenticated encryption cipher which had been submitted to the CAESAR (Competition for Authenticated Encryption: Security, Applicability, and Robustness) competition [2] in 2014. The structure is based on nonlinear feedback shift register. Later, with minor modifications, it was updated as ACORN v2 [3] and ACORN v3 [4] by enhancing the security. In March 2018, ACORN v3 was selected as one of seven finalists of CAESAR competition. In February 2019, ACORN v3 was listed into the final CAESAR portfolio and recommended for the use case of lightweight applications (resource constrained environments). The state size of ACORN v3 is 293 bits. It uses a 128-bit key and a 128-bit initialization vector. The initialization of ACORN v3 consists of loading the key and IV into the state and running the cipher for 1792 steps.

1.1. Previous Attacks on ACORN. In 2014, Wu had submitted an authenticated encryption cipher, known as ACORN v1 to CAESAR competition. After then, some attacks on ACORN v1 and its tweaked version ACORN v2 were presented in [5–11]. Besides these attacks, a cube attack on 477 rounds of ACORN v2 was proposed in [12] to recover the 128-bit key with a total attack complexity of 2^{35}, and when the goal is to recover one bit of the secret key, 503 rounds of ACORN v2 were attacked. Later, the authenticated encryption cipher was updated as ACORN v3 with minor modifications by enhancing the security.

Until now, several attacks on ACORN v3 have been published in [13–16]. However, there are no attacks better than exhaustive key search on ACORN v3 so far. Based on cube testers and d-monomial test, Ghafari and Hu proposed a new attack framework in [17, 18] and presented a practical distinguishing attack on 676 rounds of ACORN v3 with time complexity of 200×2^{33}. This has been the best-known distinguishing attack on the round reduced variants of ACORN v3 so far. Recently, some key recovery attacks on ACORN v3 had been proposed. At CRYPTO 2017, Todo et al. [19] proposed possible key recovery attacks on 647, 649, and 704 rounds of ACORN v3, where no more than one bit of the secret key can be recovered with unknown probability in around 2^{78}, 2^{109}, and 2^{122}, respectively. The attack was improved by Wang et al. in [20, 21].

1.2. Numeric Mapping. At CRYPTO 2017, Liu [22] exploited a new technique, called *numeric mapping*, to iteratively estimate the upper bound on the algebraic degree of the internal states of an NFSR. Based on this new technique, he developed an algorithm for estimating the algebraic degree of NFSR-based cryptosystems and gave distinguishing attacks on Trivium-like ciphers, including Trivium, Kreyvium, and TriviA-SC as applications.

1.3. Our Contributions. In this paper, we focus on proposing an efficient algorithm for algebraic degree estimation of ACORN v3. By applying our algorithm, we investigate the mixing efficiency of ACORN v3. When taking all the key and IV bits as initial input variables, the result shows that the lower bound on the maximum number of initialization rounds of ACORN v3 such that the generated keystream bit does not achieve maximum algebraic degree is 669 (out of 1792). When taking all the IV bits as input variables, the result shows that the lower bound on the maximum number of initialization rounds of ACORN v3 such that the generated keystream bit does not achieve maximum algebraic degree is 708 (out of 1792). When taking a subset of all the IV bits as initial input variables, we apply our algorithm to ACORN v3 to exploit new distinguishing attacks. Some distinguishing attacks on round reduced variants of ACORN v3 we have obtained are listed in Table 1, and comparisons with previous works are made. As shown in Table 1, our results are the best-known distinguishing attacks on the cipher so far. Note that three key recovery attacks on the cipher in [19–21] are also listed in Table 1. In these attacks, the recovered secret variables are generally smaller than 1 bit, while the time complexities are significantly high. Because of the high time complexities, these attacks are impractical and cannot be verified by experiments, and the success probabilities of key recovery are difficult to estimate as they are based on some assumptions. Compared with them, our attacks have significantly better time complexities. Meanwhile, our attacks are deterministic rather than statistical, that is, our attacks hold with probability 1.

To verify these cryptanalytic results, we make an amount of experiments on round reduced variants of ACORN v3. The experimental results show that our distinguishing attacks are always consistent with our evaluated results. They are strong evidences of high accuracy of our algorithm.

This paper is organized as follows. Some notations are defined and the technique numeric mapping is introduced in Section 2. In Section 3, algebraic degree estimation of ACORN v3 is presented. The paper is concluded in Section 4.

2. Preliminaries

2.1. Notations. Let $\mathbb{F}_2 = \{0, 1\}$ be the finite field with two elements. Denote $\mathbb{F}_2^n$ the n-dimension vector space over the binary field $\mathbb{F}_2$. Let $\mathbb{B}_n$ be the set of all n-variable Boolean functions mapping from $\mathbb{F}_2^n$ into $\mathbb{F}_2$, and let $f \in \mathbb{B}_n$. The algebraic normal form (ANF) of the given Boolean function f over n variables $x_1, x_2, \ldots, x_n$ can be uniquely expressed as

$$f(x_1, x_2, \ldots, x_n) = \bigoplus_{c=(c_1,c_2,\ldots,c_n)\in\mathbb{F}_2^n} a_c \prod_{i=1}^{n} x_i^{c_i}, \quad (1)$$

where the coefficient a_c is a constant in $\mathbb{F}_2$ and c_i denotes the i-th digit of the binary encoding of c (and so the sum spans all monomials in $x_1, x_2, \ldots, x_n$). The algebraic degree of f, denoted by $\deg(f)$, is defined as $\max\{\mathrm{wt}(c) \mid a_c = 1\}$, where $\mathrm{wt}(c)$ is the Hamming weight of c. Thus, for a multivariate Boolean function, the degree of a term is the sum of the exponents of the variables in the term, and then the algebraic degree of the multivariate Boolean function is the maximum of the degrees of all terms in the Boolean function.

2.2. Cube Attack and Cube Tester. Almost any cryptographic scheme can be described by tweakable polynomials over the binary field $\mathbb{F}_2$, which contain both secret variables (e.g., key bits) and public variables (e.g., IV bits). Cube attack, proposed by Dinur and Shamir [23] at EUROCRYPT 2009, is one of general and powerful cryptanalytic techniques against symmetric-key cryptosystems. It treats the output bit of a stream cipher as an unknown Boolean polynomial $f(k_0, \ldots, k_{n-1}, v_0, \ldots, v_{m-1})$, where $k_0, \ldots, k_{n-1}$ are secret key variables and $v_0, \ldots, v_{m-1}$ are public IV variables. Given any monomial t_I which is the product of variables in $I = \{i_1, \ldots, i_d\} \subseteq \{0, 1, \ldots, m-1\}$, f can be represented as the sum of terms which are supersets of I and terms that miss at least one variable from I:

$$\begin{aligned} &f(k_0, \ldots, k_{n-1}, v_0, \ldots, v_{m-1}) \\ &\quad = t_I \cdot p_{S(I)} + q(k_0, \ldots, k_{n-1}, v_0, \ldots, v_{m-1}), \end{aligned} \quad (2)$$

where $p_{S(I)}$ is called the *superpoly* of I in f and the set $\{v_{i_1}, \ldots, v_{i_d}\}$ is called a *cube*. The idea behind cube attacks is that the sum of the Boolean polynomial $f(k_0, \ldots, k_{n-1}, v_0, \ldots, v_{m-1})$ over the cube which contains all possible values for the cube variables is exactly $p_{S(I)}$, while this is a random function for a random polynomial. In cube attacks, low-degree superpolys in secret variables are exploited to recover the key, while cube testers [24] work by distinguishing $p_{S(I)}$ from a random function. Especially, the superpoly $p_{S(I)}$ is equal to a zero constant, if the algebraic degree of f in the variables from I is smaller than the size of I. Thus, from the perspective of cube tester, estimation on algebraic degree of NFSR-based cryptosystems is an efficient way of constructing distinguishing attacks.

2.3. Numeric Mapping. At CRYPTO 2017, Liu [22] exploited a new technique, called *numeric mapping*, to iteratively estimate the upper bound on the algebraic degree of the internal states of an NFSR. Based on this new technique, he developed an algorithm for estimating the algebraic degree of NFSR-based cryptosystems. Let $f(x_1, x_2, \ldots, x_n) = \bigoplus_{c=(c_1,c_2,\ldots,c_n)\in\mathbb{F}_2^n} a_c \prod_{i=1}^{n} x_i^{c_i}$. The numeric mapping, denoted by **DEG**, is defined as

Table 1: Attacks on ACORN v3.

Cipher	# rounds	Attack	Time complexity	Reference
ACORN v3	647	Key recovery attack	2^{78}	[19]
	647	**Distinguishing attack**	2^{21}	**Sect. 4.3**
	649	Key recovery attack	2^{109}	[19]
	649	**Distinguishing attack**	2^{24}	**Sect. 4.3**
	676	Distinguishing attack	$200 \times 2^{33} \approx 2^{40.64}$	[17]
	676	**Distinguishing attack**	2^{36}	**Sect. 4.3**
	704	Key recovery attack	2^{122}	[19]
	704	Key recovery attack	$2^{77.88}$	[20]
	704	**Distinguishing attack**	2^{61}	**Sect. 4.3**
	721	**Distinguishing attack**	2^{95}	**Sect. 4.3**
	750	Key recovery attack	$2^{125.71}$	[21]
	750	Key recovery attack	$2^{120.92}$	[20]

$$\mathbf{DEG} : \mathbb{B}_n \times \mathbb{Z}^n \longrightarrow \mathbb{Z},$$
$$(f, D) \longmapsto \max_{a_c \neq 0} \left\{ \sum_{i=1}^{n} c_i d_i \right\}, \tag{3}$$

where $D = (d_1, d_2, \ldots, d_n)$, a_c's are coefficients of algebraic normal form of f as defined previously, and denote $\mathbb{Z}^n$ the n-dimension vector space over the integer field $\mathbb{Z}$. Let $g_i\,(1 \le i \le m)$ be Boolean functions on n variables and denote $\deg(G) = (\deg(g_1), \deg(g_2), \ldots, \deg(g_m))$ for $G = (g_1, g_2, \ldots, g_m)$. We call $\mathbf{DEG}(f, D)$ a *numeric degree* of h if $d_i \ge \deg(g_i)$ for all $1 \le i \le n$, where $D = (d_1, d_2, \ldots, d_n)$. The algebraic degree of h is always less than or equal to the numeric degree of h. The algebraic degrees of the output bits with respect to the internal states can be estimated iteratively for NFSR-based cryptosystems by using numeric mapping.

3. Algebraic Degree Estimation of ACORN v3

In this section, we first briefly give a description of ACORN v3 and then propose an efficient algorithm for algebraic degree estimation of ACORN v3 to exploit new distinguishing attacks on it.

3.1. Brief Description of ACORN v3. This section presents a brief description of the authenticated encryption cipher ACORN v3. The structure of ACORN v3 is shown in Figure 1. The state size of ACORN v3 is 293 bits, denoted by $S^{(t)} = (s_0^{(t)}, s_1^{(t)}, \ldots, s_{292}^{(t)})$ at t-th clock. It is constructed by using 6 LFSRs of different lengths 61, 46, 47, 39, 37, and 59 and one additional register of length 4. It supports a 128-bit key and a 128-bit initialization vector. As an authenticated encryption scheme, ACORN v3 passes through 4 procedures: initialization, processing the associated data, encryption, and finalization. In this paper, we only focus on the process of initialization, since the number of rounds we can attack is smaller than the 1792 initialization rounds. For more details about ACORN v3, we refer to [4].

The initialization of the authenticated encryption cipher ACORN v3 consists of loading the 128-bit key $(k_0, k_1, \ldots, k_{127})$ and 128-bit IV $(iv_0, iv_1, \ldots, iv_{127})$ into the state and running the cipher for 1792 steps.

(1) Initialize the state S_{-1792} to 0

(2) Let $m_{(-1792+t)} = k_t$ for $t = 0$ to 127
Let $m_{(-1792+128+t)} = iv_t$ for $t = 0$ to 127
Let $m_{(-1792+256)} = k_{(t \bmod 128)} \oplus 1$ for $t = 0$
Let $m_{(-1792+256+t)} = k_{(t \bmod 128)}$ for $t = 1$ to 1535

(3) For $t = -1792$ to $t = -1$, $S^{(t+1)} = \text{StateUpdate}\,128\,(S^{(t)}, m_t, ca_t, cb_t)$

At t-th clock, the cipher executes the state update function: $S^{(t+1)} = \text{State} - \text{Update}\,128\,(S^{(t)}, m_t, ca_t, cb_t)$, which is given as follows:

Step 1. Linear feedback update

$$s_{t,289} \longleftarrow s_{t,289} \oplus s_{t,235} \oplus s_{t,230}$$
$$s_{t,230} \longleftarrow s_{t,230} \oplus s_{t,196} \oplus s_{t,193}$$
$$s_{t,193} \longleftarrow s_{t,193} \oplus s_{t,160} \oplus s_{t,154}$$
$$s_{t,154} \longleftarrow s_{t,154} \oplus s_{t,111} \oplus s_{t,107}$$
$$s_{t,107} \longleftarrow s_{t,107} \oplus s_{t,66} \oplus s_{t,61}$$
$$s_{t,61} \longleftarrow s_{t,61} \oplus s_{t,23} \oplus s_{t,0}$$

Step 2. Generate keystream bit

$$z_t \longleftarrow s_{t,12} \oplus s_t\ , 154 \oplus s_{t,235} \cdot s_{t,61} \oplus s_{t,235} \cdot s_{t,193} \oplus s_{t,61} \cdot s_{t,193} \oplus\ s_{t,230} \cdot s_{t,111} \oplus (s_{t,230} \oplus 1) \cdot s_{t,66}$$

Step 3. Generate the nonlinear feedback bit

$$f_t \longleftarrow s_{t,0} \oplus s_{t,107} \oplus 1 \oplus s_{t,244} \cdot s_{t,23} \oplus s_{t,244} \cdot s_{t,160} \oplus\ s_{t,23} \cdot s_{t,160} \oplus s_{t,230} \oplus z_t$$

Step 4. Shift the 293-bit register with the feedback bit f_t

$$s_{t+1,i} \longleftarrow s_{t,i+1} \text{ for } i = 0, 1, \ldots, 291$$
$$s_{t+1,292} \longleftarrow f_t \oplus m_t$$

3.2. Algorithm for Algebraic Degree Estimation of ACORN v3. In this section, we will propose an efficient algorithm for algebraic degree estimation of ACORN v3 using numeric mapping, as depicted in Algorithm 1.

Algorithm 1 gives a numeric degree $\mathbf{DEG}(f, X)$ of the output function f after N rounds over initial input variables $X = (x_1, x_2, \ldots, x_{128})$ as output, which gives an upper bound on the algebraic degree of the first output bit after N rounds.

The time complexity of Algorithm 1 mainly depends on the values of N and the ANFs of the update function

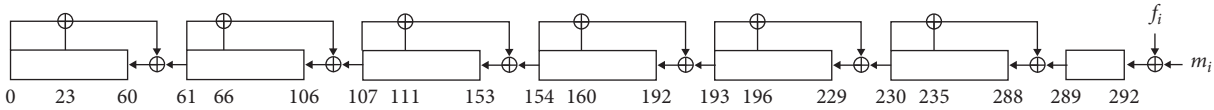

Figure 1: The structure of authenticated encryption cipher ACORN v3.

Require: Given the ANFs of the initial state $S^{(0)} = \{s_{0,0}, s_{0,1}, \ldots, s_{0,292}\}$, the ANFs of the update function State Update 128 and the keystream output function f, and the set of initial input variables $X = (x_1, x_2, \ldots, x_{128})$.
(1) Set $D^{(0)}$ to $\deg(S^{(0)}, X)$;
(2) For t from 1 to N do:
(3) $\quad D^{(t)} \longleftarrow \mathbf{DEG}(\text{State Update 128}(S^{(t-1)}), D^{(t-1)})$;
(4) Compute $\mathbf{DEG}(f, D^{(N)})$;
(5) Return $\mathbf{DEG}(f, D^{(N)})$.

Algorithm 1: Algebraic degree estimation of ACORN v3 using numeric mapping.

State Update 128. Since all of the update function State Update 128 are shifting operations except one quadratic function and six linear functions, Algorithm 1 has a time complexity of $\mathcal{O}(N)$. Algorithm 1 requires to store $D^{(t)}$ for $t = 1, 2, \ldots, N$. Since the number of initial input variables is constant for ACORN v3, it leads to a negligible memory complexity of $\mathcal{O}(N)$.

3.3. Experimental Results. By using Algorithm 1, we will investigate the mixing efficiency of ACORN v3 and exploit new distinguishing attacks on the cipher.

3.3.1. When Will the Initial Input Variables Be Sufficiently Mixed? By applying Algorithm 1, we investigate the mixing efficiency of ACORN v3. When taking all the key and IV bits as initial input variables, the result shows that the maximum number of initialization rounds of ACORN v3 such that the generated keystream bit does not achieve maximum algebraic degree is at least 669 (out of 1792). When taking all the IV bits as input variables, the result shows that the maximum number of initialization rounds of ACORN v3 such that the generated keystream bit does not achieve maximum algebraic degree is at least 708 (out of 1792). The results are listed in Table 2. Note that both of these two results are lower bounds on the maximum number of initialization rounds of ACORN v3 such that the generated keystream bit does not achieve maximum algebraic degree. In other words, the true maximum numbers of initialization rounds which do not achieve maximum algebraic degree could be higher.

Furthermore, we also take a subset of IV bits as initial input variables X and apply Algorithm 1 to ACORN v3. Since the IV bits are sequentially loaded into the internal state in the second 128 initialization rounds, it is a natural and reasonable idea that we select the latter IV bits into the cube. We consider an exhaustive search on the subset $\{iv_p, iv_{p+1}, \ldots, iv_{127}\}$ of all 128 IV bits for all $1 \le p \le 127$. Some results we have found are listed in Table 3. All these results are obtained on a common PC with 2.5 GHz Intel Pentium 4 processor within one second. In Table 3, the cube size d means that the cube $\{iv_{128-d}, iv_{128-(d-1)}, \ldots, iv_{127}\}$ is used in our attack. As for 676 rounds of ACORN v3, when $d = 36$, the best result $\mathbf{DEG}(f, X) = 35$ is found, which leads to a practical distinguishing attack on it with time complexity of 2^{36} and improves the previous distinguishing attack [17] by a factor of $2^{4.64}$. Furthermore, the distinguishing advantage of our attack is 1, while the attack of [17] is based on limited chi-square statistical test and its distinguishing advantage is certainly smaller than 1. As for 721 rounds of ACORN v3, when $d = 95$, the best result $\mathbf{DEG}(f, X) = 94$ is found, which leads to a distinguishing attack on it with time complexity of 2^{95}. This is the best result we have found. Clearly, our results are the best distinguishing attacks on round reduced variants of ACORN v3 so far. Note that all our attacks are deterministic rather than statistical, that is, our attacks hold with probability 1.

Table 2: Lower bound on the maximum number of rounds of not achieving maximum degree for ACORN v3 with initial input variables X.

Cipher	$X = (K, \text{IV})$		$X = \text{IV}$	
	(# key + # IV)	# rounds	# IV	# rounds
ACORN v3	256	669	128	708

Table 3: Our distinguishing attacks on round reduced variants of ACORN v3.

# rounds	Size of cube d	Cube	Time complexity
647	21	$\{iv_{107}, iv_{108}, \ldots, iv_{127}\}$	2^{21}
649	24	$\{iv_{104}, iv_{105}, \ldots, iv_{127}\}$	2^{24}
676	36	$\{iv_{92}, iv_{93}, \ldots, iv_{127}\}$	2^{36}
704	61	$\{iv_{67}, iv_{68}, \ldots, iv_{127}\}$	2^{61}
721	95	$\{iv_{33}, iv_{34}, \ldots, iv_{127}\}$	2^{95}

3.3.2. Experiments. Since 2^{21}, 2^{24}, and 2^{36} in Table 3 are practical, we verify these results by carrying out a test for random 100 keys within half a day on a common PC with 2.5 GHz Intel Pentium 4 processor. All outputs of 647, 649, and 670 rounds of

ACORN v3 over the cubes $\{iv_{107}, iv_{108}, \ldots, iv_{127}\}$, $\{iv_{104}, iv_{105}, \ldots, iv_{127}\}$ and $\{iv_{93}, iv_{94}, \ldots, iv_{127}\}$, respectively, always sum to 0. This clearly confirms the effectiveness and accuracy of our algorithm.

4. Conclusions

In this paper, we focus on proposing an efficient algorithm for algebraic degree estimation of ACORN v3. By applying our algorithm, we investigate the mixing efficiency of ACORN v3 and exploit distinguishing attacks on it. As a result, new distinguishing attacks on 647, 649, 670, 704, and 721 initialization rounds of ACORN v3 are obtained, respectively. So far as we know, all of our distinguishing attacks on ACORN v3 are the best. The effectiveness and accuracy of our algorithm is confirmed by the experimental results.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the National Natural Science Foundation of China under Grants 61602514, 61802437, 61272488, 61202491, 61572516, 61272041, and 61772547, National Cryptography Development Fund under Grant MMJJ20170125, and National Postdoctoral Program for Innovative Talents under Grant BX201700153.

References

[1] H. Wu, "ACORN: a lightweight authenticated cipher (v1). caesar first round submission," 2014, http://competitions.cr.yp.to/round1/acornv1.pdf.

[2] Caesar, "Competition for authenticated encryption: security, applicability, and robustness," http://competitions.cr.yp.to/index.html.

[3] H. Wu, "ACORN: a lightweight authenticated cipher (v2). caesar second round submission," 2015, http://competitions.cr.yp.to/round2/acornv2.pdf.

[4] H. Wu, "ACORN: a lightweight authenticated cipher (V3). CAESAR submission," 2016, http://competitions.cr.yp.to/round3/acornv3.pdf.

[5] L. Jiao, B. Zhang, and M. Wang, "Two generic methods of analyzing stream ciphers," in *ISC 2015. LNCS*, J. Lopez and C. J. Mitchell, Eds., vol. 9290, pp. 379–396, Springer, Cham, Switzerland, 2015.

[6] M. I. Salam, K. K. H. Wong, H. Bartlett, L. Simpson, E. Dawson, and J. Pieprzyk, "Finding state collisions in the authenticated encryption stream cipher acorn," Cryptology ePrint Archive, Report 2015/908, 2015, https://eprint.iacr.org/2015/908.

[7] F. Lafitte, L. Lerman, O. Markowitch, and D. Van Heule, "SAT-based cryptanalysis of ACORN," Cryptology ePrint Archive, Report 2016/521, 2016, https://eprint.iacr.org/2016/521.

[8] D. Roy and S. Mukhopadhyay, "Some results on ACORN," Cryptology ePrintArchive, Report 2016/1132, 2016, https://eprint.iacr.org/2016/1132.

[9] P. Dey, R. S. Rohit, and A. Adhikari, "Full key recovery of ACORN with a single fault," *Journal of Information Security and Applications*, vol. 29, pp. 57–64, 2016.

[10] D. K. Dalai and D. Roy, "A state recovery attack on ACORN-v1 and ACORN-v2," in *NSS 2017, LNCS*, Z. Yan, Ed., vol. 10394, pp. 332–345, Springer, Finland, 2017.

[11] X. Zhang, X. Feng, and D. Lin, "Fault attack on the authenticated cipher ACORN v2," *Security and Communication Networks*, vol. 2017, Article ID 3834685, 16 pages, 2017.

[12] M. I. Salam, H. Bartlett, E. Dawson, J. Pieprzyk, L. Simpson, and K. K.-H. Wong, "Investigating cube attacks on the authenticated encryption stream cipher ACORN," in *ATIS 2016. CCIS*, L. Batten and G. Li, Eds., vol. 651, pp. 15–26, Springer, Singapore, 2016.

[13] A. A. Siddhanti, S. Maitra, and N. Sinha, "Certain observations on ACORN v3 and the implications to TMDTO attacks," in *Space 2017. LNCS*, S. Ali, JL. Danger, and T. Eisenbarth, Eds., vol. 10662, pp. 264–280, Springer, Cham, Switzerland, 2017.

[14] X. Zhang and D. Lin, "Cryptanalysis of acorn in nonce-reuse setting," in *Inscrypt 2017. LNCS*, X. Chen, D. Lin, and M. Yung, Eds., vol. 10726, pp. 342–361, Springer, Cham, Switzerland, 2017.

[15] X. Zhang, X. Feng, and D. Lin, "Fault attack on ACORN v3," *The Computer Journal*, vol. 61, no. 8, pp. 1166–1179, 2018.

[16] A. Adomnicai, L. Masson, and J. J. A. Fournier, "Practical algebraic side-channel attacks against ACORN," in *ICISC 2018. LNCS*, K. Lee, Ed., vol. 11396, pp. 325–340, Springer, Cham, Switzerland, 2018.

[17] V. A. Ghafari and H. Hu, "A new chosen IV statistical distinguishing framework to attack symmetric ciphers, and its application to ACORN-v3 and Grain-128a," Cryptology ePrint Archive, Report 2017/1103, 2017, https://eprint.iacr.org/2017/1103.pdf.

[18] V. A. Ghafari and H. Hu, "A new chosen IV statistical distinguishing framework to attack symmetric ciphers, and its application to ACORN-v3 and Grain-128a," *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, no. 6, pp. 2393–2400, 2018, https://doi.org/10.1007/s12652-018-0897-x.

[19] Y. Todo, T. Isobe, Y. Hao, and W. Meier, "Cube attacks on non-blackbox polynomials based on division property," in *Crypto 2017. LNCS*, J. Katz and H. Shacham, Eds., vol. 10403, pp. 250–279, Springer, Cham, Switzerland, 2017.

[20] Q. Wang, Y. Hao, Y. Todo, C. Li, T. Isobe, and W. Meier, "Improved division property based cube attacks exploiting algebraic properties of superpoly," in *CRYPTO 2018, LNCS*, H. Shacham and A. Boldyreva, Eds., vol. 10991, pp. 275–305, Springer, Cham, Switzerland, 2018.

[21] Q. Wang, Y. Hao, Y. Todo, C. Li, T. Isobe, and W. Meier, "Improved division property based cube attacks exploiting algebraic properties of superpoly (full version)," Cryptology ePrint Archive, Report 2017/1063, 2017, https://eprint.iacr.org/2017/1063.

[22] M. Liu, "Degree evaluation of NFSR-based cryptosystems," in *CRYPTO 2017. LNCS*, J. Katz and H. Shacham, Eds., vol. 10403, pp. 227–249, Springer, Cham, 2017.

[23] I. Dinur and A. Shamir, "Cube attacks on tweakable black box polynomials," in *Eurocrypt 2009. LNCS*, A. Joux, Ed., vol. 5479, pp. 278–299, Springer, Heidelberg, Germany, 2009.

[24] J.-P. Aumasson, I. Dinur, W. Meier, and A. Shamir, "Cube testers and key recovery attacks on reduced-round MD6 and trivium," in *FSE 2009. LNCS*, O. Dunkelman, Ed., vol. 5665, pp. 1–22, Springer, Heidelberg, Germany, 2009.