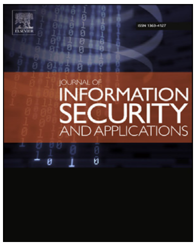
Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/jisa



Full key recovery of ACORN with a single fault

Prakash Dey [a], *Raghvendra Singh Rohit* [b], *Avishek Adhikari* [a,*]

[a] *Department of Pure Mathematics, University of Calcutta, Kolkata 700019, West Bengal, India*
[b] *Department of Mathematics & Statistics, Indian Institute of Science Education and Research, Kolkata, Nadia 741246, West Bengal, India*

ARTICLE INFO

Article history:
Available online 26 April 2016

Keywords:
Lightweight Authenticated Cipher
Cryptanalysis
CAESAR competition
ACORN
Fault analysis

ABSTRACT

The ongoing CAESAR competition launched in 2013, aimed to design authenticated encryption schemes for different applications and environments, attracted 57 submissions as candidates. Out of the 57 round 1 submissions, only 29 candidates were selected for round 2. Each of these candidates is to be analyzed carefully. Among these 29 candidates, ACORN is a family of Lightweight Authenticated Ciphers with Associated Data (AEAD). In this paper we propose a hard fault attack on both the versions of ACORN in a nonce-respecting scenario whereby a random bit of the fifth LFSR is permanently stuck at the value '1' before the driving procedure of the encryption device. Without the repetition of the same key–IV pair, this is the first work that we are aware of, where the secret key can be recovered fully with a computational complexity well below the limit of brute force search. With hard fault at a certain position the attack complexity reduces to $2^{55.85}$.

1. Introduction

CAESAR is an acronym for the "Competition for Authenticated Encryption: Security, Applicability and Robustness". The ongoing CAESAR competition (CAESAR, 2013) aims to identify a portfolio of authenticated encryption schemes that offer advantages over AES-GCM and are suitable for widespread adoption. On 27 January 2014, the final call for submissions was published. The submissions were due in March 2014. A total of 57 authenticated encryption schemes were submitted for this competition in round 1. The competition has 3 rounds. The CAESAR candidates are going through intense reviews, analyses and comparison processes by the cryptographic community. In round 2, out of 57 initial submissions, only 29 candidates are selected. ACORN, a family of Lightweight Authenticated Ciphers with Associated Data (AEAD), is one among them. It sequentially processes a message bit at a time, does not check the message length in decryption and authentication, requires no padding and allows parallel computation. These features benefit the hardware implementation of the ACORN. To the best of our knowledge, the only external analyses on ACORN that exist in literature are those of Chaigneau et al. (2015), Liu and Lin (2014), and Salam et al. (2015). The result by Liu and Lin (2014) shows the existence of slid pairs (key–IV pairs) that generate the same state up to a clock difference. They also proposed state recovering attacks using guess-and-determine and differential-algebraic techniques. However, the time complexity of their attack is more than that of the brute force search. Chaigneau et al. (2015) show that in nonce-reuse and unverified plaintext release setting, the full key of ACORN v1 can be recovered. Salam et al. (2015) identified weaknesses in the state update function of ACORN that results in the internal state collision in a chosen key and IV setting. However, their attack becomes infeasible when the secret key is unknown. Being more efficient in hardware, the cipher still has not received any analysis that targets its implementation. Also there is no key

* *Corresponding author.* Department of Pure Mathematics, University of Calcutta, Kolkata 700019, West Bengal, India. Tel.: +00919830794717.
E-mail addresses: pdprakashdey@gmail.com (P. Dey), iraghvendrarohit@gmail.com (R.S. Rohit), avishek.adh@gmail.com (A. Adhikari).

http://dx.doi.org/10.1016/j.jisa.2016.03.003

Table 1 – Attack summary on ACORN (with unknown key).

Existing works	Nonce repetition	Complexity
Liu and Lin (2014)	No	2^{180}
Chaigneau et al. (2015)	At least 4 times	2^{109}
Current work	No re-keying is required	Min. $2^{55.85}$

recovery attack with complexity less than that of brute force search in a nonce-respecting scenario (i.e., when the same key–IV pair is not reused). To focus on the same, we consider hard fault attack model in this paper. Table 1 provides a comparison between our result and the existing results when the key is assumed to be unknown.

Side channel attacks, such as power analysis, timing analysis and fault analysis, target the implementations of ciphers. Power and fault analyses are among the most explored types of side channel attacks.

The idea of Differential Fault Attack (DFA) was introduced by Biham and Shamir (1997). In literature, two types of fault attacks exist, namely, *soft fault attack* and *hard fault attack*. In *soft fault attacks*, the adversary injects soft faults i.e., she temporarily changes the register bit values and can reset the encryption machine multiple times. On the other hand, *hard fault attacks* are based on hard fault injection where some bits of the system are permanently set to 1 or 0 at some point of its operation cycle. Fault attacks generally study the robustness of a cryptosystem in a setting that is weaker than its original or expected mode of operation. In a DFA model, faults are injected during cipher operations. Since the faults flip the corresponding bits, the attack results in a difference in the state. The resulting faulty output, together with the fault free one, is analyzed to obtain full or a part of the secret information. This model of attack has been shown to be successful against both stream ciphers and block ciphers (Ali and Mukhopadhyay, 2011; Banik et al., 2012; Biham et al., 2005; Dey and Adhikari, 2014; Dey et al., 2015; Dutta and Paul, 2014; Hojsík and Rudolf, 2008a, 2008b; Hu et al., 2012, 2013; Karmakar and Chowdhury, 2011; Sarkar et al., 2015; Tunstall et al., 2011).

Hard fault analysis is a practical and powerful tool toward cryptanalysis of ciphers. The stream cipher RC4 and hardware oriented cipher TRIVIUM are susceptible to hard fault attack (Dutta and Paul, 2014; Hu et al., 2013; Maitra and Paul, 2008). The hard fault attack poses a serious threat to the cipher's security of implementation and hence analysis of ciphers under this attack model needs more attention.

1.1. *Our contribution*

In this paper, we propose a single bit hard fault key recovery attack on both the versions of ACORN. Acorn v1 design was modified to Acorn v2 so that the key cannot be recovered from the state by running the cipher backwards. However, unlike Chaigneau et al. (2015) and Liu and Lin (2014) this change in design has no effect on the current work. The proposed attack recovers the full key, without the internal state recovery and repetition of the key–IV pair, in a nonce-respecting scenario where a random bit of the fifth LFSR of ACORN is stuck at the value 1 before the driving procedure of the encryption device. In our attack we first uniquely identify the fault location by looking at the faulty keystream bits. Then a system of faulty keystream equations is generated. Experimental results suggest that, by Gaussian elimination and guessing some variables, the full key of ACORN can be recovered successfully with complexity less than that of a brute force search. With hard fault at a certain position the attack complexity reduces to $2^{55.85}$.

Organization of the paper: The rest of the paper is organized in the following way: In Section 2 we propose an alternative description of ACORN. The attack model considered in this paper is described in Section 3. Signature of a fault and fault location identification procedure are respectively described in Sections 4 and 5. Section 6 provides the key recovery procedure. Experimental results are provided in Section 7. Finally, Section 8 concludes the paper.

2. Description of ACORN

For the sake of simplicity of analysis we introduce an equivalent alternative description of ACORN. For the original descriptions of the two cipher versions, the reader may refer to Wu (2014) and Wu (2015).

Remark 1. *We abuse the '+' notation for Boolean XOR, i.e., GF(2) addition as well as standard arithmetic addition and that will be clear from the context. Also we use juxtaposition for Boolean AND i.e., GF(2) multiplication.*

ACORN is an AEAD algorithm. It uses 128-bit key $k = (k_0, \dots, k_{127})$, 128-bit initialization vector $IV = (IV_0, \dots, IV_{127})$ and *adlen* bit associated data $AD = (ad_0, \dots, ad_{adlen-1})$. The *pclen* bit length plaintext $P = (p_0, \dots, p_{pclen-1})$ is encrypted to the ciphertext $C = (ct_0, \dots, ct_{pclen-1})$ of the same bit length. After processing the plaintext bits, the authentication tag T (of length t-bits, $64 \le t \le 128$) is produced.

ACORN consists of 6 LFSRs respectively denoted by a, b, c, d, e, f and one NFSR denoted by g. At the i-th step, we denote the state of the registers a, b, c, d, e, f and g respectively by $(a_0^i, \dots, a_{60}^i)$, $(b_0^i, \dots, b_{45}^i)$, $(c_0^i, \dots, c_{46}^i)$, $(d_0^i, \dots, d_{38}^i)$, $(e_0^i, \dots, e_{36}^i)$, $(f_0^i, \dots, f_{58}^i)$ and $(g_0^i, \dots, g_3^i)$. The length of the registers a, b, c, d, e, f and g respectively being $\eta_a = 61$, $\eta_b = 46$, $\eta_c = 47$, $\eta_d = 39$, $\eta_e = 37$, $\eta_f = 59$ and $\eta_g = 4$. The ACORN state is shown in Fig. 1.

Thus at the beginning of the i-th step the 293-bit state of the cipher is given by (|| being the concatenation operator)

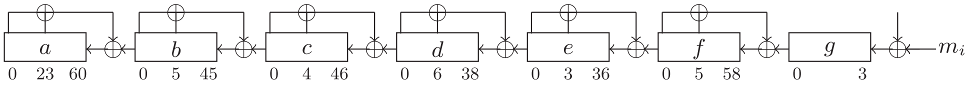


Fig. 1 – ACORN state.