Fault Tolerant Infective Countermeasure for AES

Sikhar Patranabis, Abhishek Chakraborty, and Debdeep Mukhopadhyay

Department of Computer Science and Engg., IIT Kharagpur, India
{sikhar.patranabis,abhishek.chakraborty,debdeep}@cse.iitkgp.ernet.in

Abstract. Infective countermeasures have been a promising class of fault attack countermeasures. However, they have been subjected to several attacks owing to lack of formal proofs of security and improper implementations. In this paper, we first provide a formal information theoretic proof of security for one of the most recently proposed state of the art infective countermeasures against DFA, under the assumption that the adversary does not change the flow sequence or skip any instruction. Subsequently, we identify weaknesses in the infection mechanism of the countermeasure that could be exploited by attacks which change the flow sequence. Furthermore, we propose an augmented infective countermeasure scheme obtained by introducing suitable randomizations that reduce the success probabilities of such attacks. All the claims have been validated by supporting simulations and real life experiments on a SASEBO-W platform. We also compare the fault tolerance provided by our proposed countermeasure scheme against that provided by the existing scheme.

Keywords: Infective Countermeasure, AES, Randomization, Instruction Skip, Fault Attack, Fault Tolerant.

1 Introduction

With fault attacks now being an established threat to the security of cryptosystems, sound countermeasures are needed to protect them. Recent research has demonstrated two major flavors of countermeasures - detection based and infection based. Detection based countermeasures such as time and hardware redundancy [1, 2] are vulnerable against attacks to the comparison step itself and also against attacks using biased fault models [3]. Infective countermeasures, on the other hand, avoid the use of comparison by diffusing the effect of the fault to render the ciphertext unexploitable. However, deterministic diffusion based infective countermeasures are vulnerable to attacks as demonstrated by Lomné *et.al* [4]. A random variation of the infective countermeasure was proposed by Gierlichs *et.al* [5]. However, the infection method employed by this countermeasure has a number of shortcomings, as demonstrated by Battistello and Giraud [6], and in greater detail by Tupsamudre *et.al* [7]. Tupsamudre *et.al* have also proposed an improved infective countermeasure that avoids all the pitfalls of [5]

R.S. Chakraborty et al. (Eds.): SPACE 2015, LNCS 9354, pp. 190–209, 2015.
DOI: 10.1007/978-3-319-24126-5_12

and thwarts DFA. However, no formal proof of security has been provided for the proposed scheme. Moreover, fault attacks that allow an adversary to change the flow sequence of an algorithm by methods such as instruction skips have also not been considered.

Recent research on microcontrollers and embedded processors has revealed that fault models in which an adversary can skip one or more instructions is practically observable on various architectures [8, 9] using different fault injection techniques [10–12]. Hence, such a fault model is a realistic threat to embedded applications. We demonstrate in this paper that the instruction skip fault model weakens the infective countermeasure scheme proposed in [7] and allows easy key recovery. Thus, it is important to make infective countermeasure tolerant against attacks that change the flow sequence of the algorithm. This paper proposes an augmented infective countermeasure scheme with suitable randomizations that reduce the probability of occurrence such faults considerably.

Contributions: In this paper, we first present a formal information theoretic proof of security for the infective countermeasure scheme proposed by Tupsamudre *et.al* [7] against single and multiple fault injection models, under the assumption that an adversary cannot change the flow sequence or skip instructions. We then investigate in detail the threats posed to this countermeasure by the instruction skip fault model and formally analyze the information leakage as a result of the attack. We also examine in detail the drawbacks of the original scheme that makes it vulnerable to instruction skips, and then propose an augmented countermeasure scheme by incorporating necessary randomizations in the existing algorithm to reduce the probability of such attacks. All the claims have been validated by supporting simulations and real-life experiments on a SASEBO-W platform that compare the existing and augmented versions of the infective countermeasures both in terms of performance and security.

2 Preliminaries: The Infective Countermeasure

In this section, we briefly introduce the infective countermeasure scheme proposed by Tupsamudre *et.al* [7]. Table 1 summarizes the notations used in the rest of this paper. For the description of the countermeasure scheme, we use the same notations used in the original paper. Algorithm 1 depicts the infective countermeasure proposed in [7] for AES-128. In the event of a fault in any of the computation rounds (redundant or cipher), the algorithm detects the difference in values of R_0 and R_1 during the execution of the cipher round. The value of R_0 is then set to R_2 as described in step 11 of the algorithm. If, on the other hand, the adversary attacks the dummy round, $(R_2 \oplus \beta)$ evaluates to 1 and R_0 is once again set to R_2. In the event of undisturbed execution, the algorithm outputs the correct ciphertext. In the following section, we formally examine the security of the countermeasure scheme against single and multiple fault injections under the assumption that adversary cannot alter the flow of execution of the algorithm.