Tamper Resistance of AES

—

Models, Attacks and Countermeasures

Volker Krummel

December 27, 2007

Abstract

The block cipher Rijndael was selected as the Advanced Encryption Standard (AES) by the National Institute for Standards and Technology (NIST) in 2001. Since the beginning of the selection process in 1997 researchers all over the world analyzed several aspects of the security of AES.

In this thesis we focus on analyzing the so called tamper resistance of AES, i.e., the security of AES against side channel attacks - a major threat for the security of cryptographic algorithms. Firstly, we propose a general but strong model to analyze the security of cryptographic algorithms against side channel attacks. In our model we assume that an adversary is able to obtain the values of some of the intermediate results of AES encryptions with a secret key that is unknown to the adversary. An algorithm is called secure in our model if the values of intermediate results do not leak any information about the secret key. Hence, an algorithm that is secure in our model provides security against most side channel attacks. We propose a method to transform any algorithm that is defined over a finite field into an algorithm that is secure in our model. I.e., we present an algorithm for securely computing AES encryptions.

Secondly, we analyze a countermeasure called memory encryption that is widely used on todays high security smart cards. We develop a new class of fault attacks that is able to determine the secret key used in an AES encryption even in the presence of memory encryption. Our attack only needs a moderate number of fault inductions an hence shows that memory encryption used in a straightforward manner may not be an effective countermeasure.

In the last part of the thesis we analyze a special kind of side channel attacks, so called cache base attacks (CBA). In a CBA the adversary can exploit information about the cache behaviour of the processor during an AES encryption to determine information about the secret key. We show that a countermeasure based on random permutations as proposed in the literature is not an effective countermeasure against CBAs. To do so we present a CBA that determines the secret key efficiently. We improve the proposed countermeasure by introducing a new class of permutations called distinguished permutations. Using distinguished permuations instead of random permutations can provably protect at least parts of the secret key. Furthermore, we analyze the security of existing algorithms for computing AES encryptions against CBAs. We also present new algorithms that compute AES encryptions that provide a much better security against CBAs.