V International Conference on Mathematics and its Applications in Science and Engineering
(ICMASE 2024)

ICMASE 2024

FAULT INJECTION ATTACKS AGAINST RSA-CRT DIGITAL SIGNATURE

Fernando Contreras Alcalá[1,2,*], Miguel Ángel González de la Torre[2], Luis Hernández Encinas[2]

[1] *Centro Universitario de Tecnología y Arte Digital (U-TAD)*
(Fundación Max Mazin)
[2] *Instituto de Tecnologías Físicas y de la Información (ITEFI)*
Consejo Superior de Investigaciones Científicas (CSIC)
ferconalca@gmail.com, ma.gonzalez@csic.es, luis.h.encinas@csic.es

ABSTRACT

It is known that Cryptology has as objective to guarantee the confidentiality, integrity and authentication of information when it is stored or transmitted. Asymmetric cryptosystems are among the most used methods for encrypting the information, and one of their main applications is the digital signature. In this type of cryptosystems each user has two different keys: the public and the private one. The first one is publicly known and permits any user to encrypt information or verify the digital signature of the owner of the key; whereas the private key, which is secret, is used by the owner for decrypting the encrypted information or elaborating his digital signature.

The RSA cryptosystem is considered to be mathematically secure against the integer factorization methods, but there are other attacks whose objective is to obtain the private key [1]. In fact, Side Channel Attacks rely on analyzing certain information obtained from the device where an implementation of the algorithm runs; for example, measuring the execution time or the power consumption required by the algorithm, the electromagnetic field generated by the device, etc. On the other hand, Fault Injection (FI) Attacks deliberately induce a fault in the execution of the algorithm to get a wrong output, so that such output allows the attacker to make guesses based on the comparison of different results.

In this work, we explain the mathematical aspects of two FI attacks and analyze the security of the implementation of the RSA in a digital signature scenario, in particular when the RSA-CRT algorithm is considered. By using the Chipwhisperer platform, we simulate the Bellcore [2] and the Lenstra [3] attacks to factorize the RSA module and to obtain the private key. The first attack compares a fake signature and the real one, whereas the second one only uses a wrong signature.

***K*eywords** RSA-CRT digital signature · Fault injection attack · Chipwhisperer · Bellcore and Lenstra attacks

References

[1] Fúster Sabater A., Hernández Encinas L., Martín Muñoz A., Montoya Vitini F., and Muñoz Masqué J., Criptografía, protección de datos y aplicaciones. RA-MA, Madrid, 2012.

[2] Sidorenko A., van den Berg J., Foekema R., Grashuis M., and de Vos J., Bellcore attack in practice, Cryptology ePrint Archive 553, 2012.

[3] Paar C., Implementation of Cryptographic Schemes 1 Course, Ruhr-Universität Bochum (Germany), April 2015.

[*] *Corresponding Author's E-mail: ferconalca@gmail.com*