On Comparing Side-Channel Preprocessing Techniques for Attacking RFID Devices

Thomas Plos, Michael Hutter, and Martin Feldhofer

Institute for Applied Information Processing and Communications (IAIK),
Graz University of Technology, Inffeldgasse 16a, 8010 Graz, Austria
{Thomas.Plos,Michael.Hutter,Martin.Feldhofer}@iaik.tugraz.at

Abstract. Security-enabled RFID tags become more and more important and integrated in our daily life. While the tags implement cryptographic algorithms that are secure in a mathematical sense, their implementation is susceptible to attacks. Physical side channels leak information about the processed secrets. This article focuses on practical analysis of electromagnetic (EM) side channels and evaluates different preprocessing techniques to increase the attacking performance. In particular, we have applied filtering and EM trace-integration techniques as well as Differential Frequency Analysis (DFA) to extract the secret key. We have investigated HF and UHF tag prototypes that implement a randomized AES implementation in software. Our experiments prove the applicability of different preprocessing techniques in a practical case study and demonstrate their efficiency on RFID devices. The results clarify that randomization as a countermeasure against side-channel attacks might be an insufficient protection for RFID tags and has to be combined with other proven countermeasure approaches.

Keywords: RFID, Differential Frequency Analysis, Side-Channel Analysis, Electromagnetic Attacks.

1 Introduction

During the last few years, Radio-Frequency Identification (RFID) has emerged from a simple identification technique to the enabler technology for buzzwords like “ambient intelligence” or the “Internet of things”. Additional features like sensors and actuators allow applications in many different fields apart from supply-chain management and inventory control. Sarma *et al.* [19] have been the first who addressed the importance of security for passive RFID tags. The introduction of security allows tags to prove their identity by means of cryptographic authentication. Furthermore, privacy issues could be solved and a protected access to the tag’s memory becomes possible.

In 2003, it was stated e.g. by Weis *et al.* [20] that strong cryptography is unfeasible on passive tags due to the fierce constraints concerning power consumption and chip area. Since then, many attempts have been made to implement standardized cryptographic algorithms in hardware complying with the

H.Y. Youm and M. Yung (Eds.): WISA 2009, LNCS 5932, pp. 163–177, 2009.

requirements of passive RFID tags. Among the most popular publications on that are realizations of the Advanced Encryption Standard (AES) [6], Elliptic-Curve Cryptography (ECC) [3,8], and GPS [9,15].

Unfortunately, having a crypto module of a secure algorithm in hardware on the tag is not sufficient for a secure RFID system. Due to the fact that an adversary always tries to break the weakest link in a system (and this is the RFID tag that is easily available for attacks), further attacks have to be considered. Side-channel attacks target at the implementation of a cryptographic device. They are very powerful in retrieving the secret key by measuring some physical property like power consumption, electromagnetic emanation, or timing behavior *etc.* Differential power analysis (DPA) [13] attacks and differential electromagnetic analysis (DEMA) [18,1] attacks gained a lot of attention during the last ten years.

In the findings of Hutter *et al.* [11] for HF tags as well as in the work of Oren *et al.* [16] and Plos [17] for the UHF frequency range, it has been shown that passive RFID tags are also susceptible to side-channel attacks. Even in the presence of the strong electromagnetic field of the reader DEMA attacks are possible. Hence, as far as a cryptographic algorithm is implemented on a tag, appropriate countermeasures have to be implemented. According to [14], countermeasures can principally be divided in either hiding or masking.

A very efficient way of implementing hiding, especially for low-resource devices like RFID tags, is to randomize the execution of the algorithm. This means that the performed operations of the algorithm occur at different moments in time in each execution. Randomization can be done by shuffling and by randomly inserting dummy cycles [14]. The reason why randomization is very cost efficient in terms of hardware resources is that the implementation is mainly done in the control logic. Moreover, spending additional clock cycles for randomizing the execution of the algorithm is convenient since the data rates used in RFID systems are rather low.

Differential Frequency Analysis (DFA)—not to confuse with differential fault analysis, which uses the same acronym—has been first mentioned by Gebotys *et al.* [7] in 2005. There, the authors successfully applied DFA to attack cryptographic algorithms running on a Personal Digital Assistant (PDA) device. The principle idea of DFA is to transform measured side-channel traces from the time domain to the frequency domain. The Fast Fourier Transform (FFT) is an operation that can be used for this transformation. Since the FFT is time-shift invariant, the time delays introduced by the side-channel analysis countermeasures are removed in the frequency domain. Further advantage of DFA especially for attacking RFID tags is that misaligned traces are of no concern. Misalignments do often occur due to the interfering reader field and difficulties in triggering appropriate events on the tag. Another approach that uses the frequency domain for handling misaligned traces has been presented by Homma *et al.* [10] in 2006. They have been able to diminish the displacement between traces by using a so-called phase-only correlation after transformation to the frequency domain.