Available online at www.sciencedirect.com
ScienceDirect

Computers and Electrical Engineering 33 (2007) 367–382

Computers and Electrical Engineering

www.elsevier.com/locate/compeleceng

Differential power and electromagnetic attacks on a FPGA implementation of elliptic curve cryptosystems

E. De Mulder [a], S.B. Örs [b,*], B. Preneel [a], I. Verbauwhede [a]

[a] *Katholieke Universiteit Leuven, Department of Electrical Engineering, SCD/COSIC, Belgium*
[b] *Istanbul Technical University, Department of Electronics and Communication Engineering, Turkey*

Available online 5 July 2007

Abstract

This paper describes the first differential power and electromagnetic analysis attacks performed on a hardware implementation of an elliptic curve cryptosystem. In the same time we also compared the metrics used in differential power and electromagnetic radiation attacks. We describe the use of the Pearson correlation coefficient, the distance of mean test and the maximum likelihood test. For each metric the number of measurements needed to get a clear idea of the right guess of the key-bit is taken as indication of the strength of the metric.

Keywords: FPGA; Power analysis; Electromagnetic analysis; Elliptic curve cryptosystems

1. Introduction

Elliptic curve cryptography (ECC) was proposed independently by Miller [13] and Koblitz [9] in the 80's. Since then a considerable amount of research has been performed on secure and efficient ECC implementations. The benefits of ECC, when compared with classical cryptosystems such as RSA [23], include: higher speed, lower power consumption and smaller certificates, which are especially useful for wireless applications.

There is a vast literature on differential power analysis (DPA) and differential electromagnetic radiation analysis (DEMA). This paper describes the first DPA and DEMA attack performed on a FPGA implementation of an elliptic curve cryptosystem over GF(p) [17]. The attacks in previous papers were performed on software implementations or were only simulations of attacks. With the start of differential power analysis in [10], followed by the differential electromagnetic analysis [8,22], several metrics were used to decide for the correct hypothesis. The literature mentions metrics such as the distance of mean test [10], the correlation analysis [18] and the maximum likelihood test [3], all explained in Section 2.2. As we wanted to know which of those yields the best results, we compare them based on the number of measurements needed to obtain the correct key. The number of measurements for the key guess to stabilize is representative for the quality of the metric.

[*] Corresponding author.
E-mail address: Siddika.Ors@itu.edu.tr (S.B. Örs).

0045-7906/$ - see front matter © 2007 Elsevier Ltd. All rights reserved.
doi:10.1016/j.compeleceng.2007.05.009

The paper is structured as follows: In Section 2, the theoretical background of elliptic curves, the power and electromagnetic radiation attacks and the different statistical methods for differential analysis are discussed. Section 3 gives an overview of the previous work in this area. This section is followed by a description of the measurement setup (Section 4). Section 5, describes differential power analysis attack and Section 6 describes differential electromagnetic analysis attack. Section 7 concludes the paper.

2. Theoretical background

2.1. Elliptic curves over GF(p)

An elliptic curve E is expressed in terms of the simplified Weierstrass equation: $y^2 = x^3 + ax + b$, where a, $b \in \mathrm{GF}(p)$ with $4a^3 + 27b^2 \neq 0 \pmod p$. The inverse of the point $P = (x_1, y_1)$ is $-P = (x_1, -y_1)$. The sum $P + Q$ of the points $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ (assume that $P, Q, \neq \mathcal{O}$, and $P \neq \pm Q$) is the point $R = (x_3, y_3)$ where: $x_3 = \lambda^2 - x_1 - x_2, y_3 = (x_1 - x_3)\lambda - y_1, \lambda = \frac{y_2 - y_1}{x_2 - x_1}$. For $P = Q$, the "doubling" formulae are: $x_3 = \lambda^2 - 2x_1, y_3 = (x_1 - x_3)\lambda - y_1, \lambda = \frac{3x_1^2 + a}{2y_1}$. The point at infinity $\mathcal{O}$ plays a role analogous to that of the number 0 in ordinary addition. Thus, $P + \mathcal{O} = P$ and $P + (-P) = \mathcal{O}$ for all points P. The points on an elliptic curve together with the operation of addition form an Abelian group. Then it is straightforward to introduce the point or scalar multiplication as main operation for elliptic curve cryptosystem (ECC). This operation can be calculated by with the always double-and-add algorithm as shown in Algorithm 1. For details see [13,9,4].

Algorithm 1. Elliptic curve point multiplication (ECPM)

```
Input: EC point $P = (x,y)$, integer $k$, $0 < k < M$, $k = (1, k_{l-2}, \ldots, k_0)_2$ and $M$
Output: $Q = [k]P = (x',y')$
Q ← P
for $i$ from $l - 2$ downto 0
    $Q_1 \leftarrow 2Q$
    $Q_2 \leftarrow Q_1 + P$
    if $k_i = 0$ then
        $Q \leftarrow Q_1$
    else
        $Q \leftarrow Q_2$
```

2.2. Power and electromagnetic analysis attacks

The power consumption of CMOS circuits is data-dependent. However, for the attacker, the relevant question is to know whether this data-dependent behavior is observable.

The first practical implementation of a power analysis attack on the DES was reported in [10] by Kocher et al. Since then, several organizations have developed the skills to conduct these measurements in practice; this now includes knowledge about statistics, the properties of the attacked cryptographic algorithms and the measurement setup.

The current that flows during the transition of the output of a CMOS gate, causes a variation of the electromagnetic field surrounding the chip that can be monitored by inductive probes which are particularly sensitive to the related impulse. The electromotive force across the sensor (Lentz' law) relates to the variation of magnetic flux as follows [25]:

$$V = -\frac{\mathrm{d}\phi}{\mathrm{d}t} \text{ and } \phi = \int\int \vec{B} \cdot \mathrm{d}\vec{A},$$

where V is the probe's output voltage, ϕ the magnetic flux sensed by probe, t is the time, $\vec{B}$ is the magnetic field and $\vec{A}$ is the area that it penetrates.