Open access • Proceedings Article • DOI:10.1109/WAC.2006.375739

Differential Electromagnetic Attack on an FPGA Implementation of Elliptic Curve Cryptosystems — Source link

E. De Mulder, S. B. Ors, Bart Preneel, Ingrid Verbauwhede

Institutions: Katholieke Universiteit Leuven, Istanbul Technical University

Published on: 24 Jul 2006 - World Automation Congress

Topics: Elliptic curve cryptography and Computational electromagnetics

Differential Electromagnetic Attack on an FPGA Implementation of Elliptic Curve Cryptosystems

E. De Mulder[1], S. B. Örs[2], B. Preneel[1], I. Verbauwhede[1]
[1]Katholieke Universiteit Leuven
Department of Electrical Engineering (ESAT), SCD/COSIC, Belgium
[2]Istanbul Technical University
Department of Electronics and Communication Engineering, Turkey

Abstract

This paper describes a differential electromagnetic analysis attack performed on a hardware implementation of an elliptic curve cryptosystem. We describe the use of the distance of mean test. The number of measurements needed to get a clear idea of the right guess of the key-bit is taken as indication of the success of the attack. We can find the right key-bit by using only 2000 measurements. Also we give a electromagnetic model for the FPGA we use in our experiments. The amplitude, the direction and the position of the current on the FPGA's lines with respect to the position of the antenna have an influence on the measured electromagnetic radiation in the FPGA's surrounding area.

Keywords: FPGA, Electromagnetic Analysis, Elliptic Curve Cryptosystems

1 Introduction

Elliptic Curve Cryptography (ECC) was proposed independently by Miller [12] 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 [18], include: higher speed, lower power consumption and smaller certificates, which are especially useful for wireless applications.

There is a vast literature on differential electromagnetic radiation analysis *(DEMA)*. This paper describes a DEMA attack performed on an FPGA implementation of an elliptic curve cryptosystem over $GF(p)$ [14, 15]. 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, 17], several metrics were used to decide for the correct hypothesis. We use the distance of mean test as our metric. The number of measurements for the key guess to stabilize is representative for the quality of the metric and the success of the DEMA attack. We can find the right key bit by using only 2000 measurements.

The paper is structured as follows: In Section 2 the theoretical background of elliptic curves, the electromagnetic radiation attacks and the distance of mean test 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) and by the electromagnetic model of the FPGA (Section 5). The DEMA attack is given in Section 6. 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 Weierstrass equation: $y^2 = x^3 + ax + b$, where $a, b \in GF(p)$ with $4a^3 + 27b^2 \neq 0 \pmod p$. The point at infinity $\mathcal{O}$ plays a role analogous to that of the number 0 in ordinary addition. The points on an elliptic curve together with the operation of addition form an Abelian group. Then it is straightforward to introduce the point 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 [12, 9, 5].

Algorithm 1 Elliptic curve point multiplication (ECPM)

```
Input: EC point $P = (x, y)$, integer $k$, $0 < k < M$, $k = (1, k_{l-2}, \cdots, k_0)_2$ 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 Electromagnetic Analysis Attacks

The current 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 current that flows during the switching of the CMOS gates, 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 [19]: $V = -\frac{\mathrm{d}\phi}{\mathrm{d}t}$ and $\phi = \iint \vec{B} \cdot d\vec{A}$, 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.

Maxwell's equation based on Ampère's law relates the magnetic field to their origin: $\vec{\nabla} \times \vec{B} = \mu\vec{J} + \epsilon\mu\frac{\delta\vec{E}}{\delta t}$, where $\vec{J}$ is the current density, $\vec{E}$ is the electrical field, ϵ is the dielectric permittivity and μ is the magnetic permeability.

Two types of electromagnetic analysis attacks are distinguished. In a *simple electromagnetic analysis* (SEMA) attack, an attacker uses the side-channel information from one measurement directly to determine (parts of) the secret key. In a *differential electromagnetic analysis* (DEMA) attack, many measurements are used in order to filter out noise.

2.2.1 Distance of Mean Test

. A distance of mean test begins by running the cryptographic algorithm for N random values of input. For each of the N inputs, I_i, a discrete time side-channel signal, $S_i[j]$, is collected and the corresponding output, O_i, may also be collected. The side-channel signal $S_i[j]$ is a sampled version of the side-channel output of the device during the execution of the algorithm that is being attacked. The index i corresponds to the I_i that produces the signal and the index j corresponds to the time of the sample. The $S_i[j]$ are split into two sets using a partitioning function, $D(\cdot)$: $S_0 = \{S_i[j]\,|D(\cdot) = 0\}$, $S_1 = \{S_i[j]\,|D(\cdot) = 1\}$.

The next step is to compute the average side-channel signal for each set: $A_0[j] = \frac{1}{|S_0|}\sum_{S_i[j]\in S_0} S_i[j]$, $A_1[j] = \frac{1}{|S_1|}\sum_{S_i[j]\in S_1} S_i[j]$ where $|S_0| + |S_1| = N$. By subtracting the two averages, a discrete time differential side-channel bias signal, $T[j]$, is obtained: $T[j] = A_0[j] - A_1[j]$.

Selecting an appropriate D function results in a differential side channel bias signal that can be used to verify guessed part of the secret key.

3 Previous Work

It is well known that the US government has been aware of electromagnetic leakage since the 1950's. The resulting standards are called TEMPEST; partially declassified documents can be found in [13]. The first published papers are work of Quisquater and Samyde [17] and the Gemplus team [8]. Quisquater and Samyde showed that it is possible to measure the electromagnetic radiation from a smart card. Quisquater also introduced the terms Simple EMA (SEMA) and Differential EMA (DEMA). The work of Gemplus deals with experiments on three algorithms: DES, RSA and COMP128.

According to Agrawal *et al.* there are 2 types of emanations: intentional and unintentional [2, 1]. The first type results from direct current flows. Th real advantage over other side-channel attacks lies in exploring unintentional emanations [2, 1]. More precisely, EM leakage consists of multiple channels.

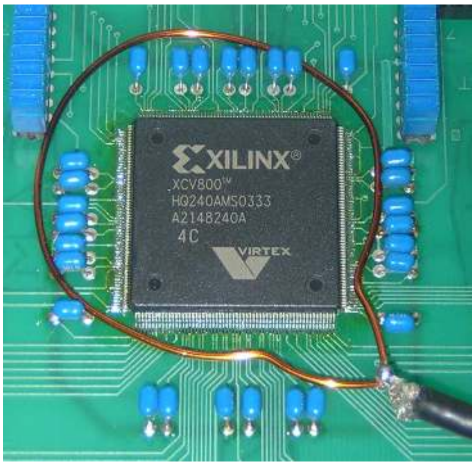


Figure 1: Measurement setup

Therefore, compromising information can be available even for DPA resistant devices which can be detached from the measurement equipment.

Besides carefully exploring all available EM emanations an attacker can also focus on a combination of two or more side-channels. Agrawal *et al.* defined these so-called multi-channel attacks in which the side-channels are not necessarily of a different kind [3].

Mangard also showed that near-field EM attacks can be conducted even with a simple hand-made coil in [11]. Besides that he showed that measuring the far-field emissions of a smart card connected to a power supply unit also suffices to determine the secret key used in the smart card.

Carlier *et al.* showed that EM side channels from an FPGA implementation of AES can be effectively used by an attacker to retrieve some secret information in [6].

De Mulder *et al.* presented a SEMA and a DEMA attack on an FPGA implementation of an elliptic curve processor in [7].

4 Measurement Setup

The measurement setup consists of the FPGA board with a Xilinx Virtex 800 FPGA presented in [16], an Tektronix TDS714L oscilloscope, a handmade loop antenna, a function generator and a power supply. The total power consumption and the electromagnetic radiation of the FPGA were measured simultaneously while it executes an elliptic curve point multiplication with the key and a point on the curve.

5 Electromagnetic Model of the FPGA

The following model gives an explanation of why we use a loop antenna and mentions some properties of the measured field which could be taken into account in the prediction phase of an attack. The current in an FPGA flows from the power source to the ground, in this way a loop is formed. At first approximation, the currents in an FPGA form small loops, that is why these currents could be modeled with a magnetic dipole as elementary building block. If the current loop is situated in the xy-plane and if we suppose that the medium where the loop is situated can be thought as free of loss; this suggests that $\sigma = 0$, then the electrical and magnetic field is defined by the following equations: $H_r = \frac{IA}{2\pi} jk_g \cos(\theta) e^{-jk_g r} r^{-2}(1 + (jk_g r)^{-1})$, $H_\theta = \frac{IA}{4\pi}(-k_g^2)\sin(\theta) e^{-jk_g r} r^{-1}(1 + (jk_g r)^{-1} + (jk_g r)^{-2})$, $E_\phi = \frac{IA}{4\pi} k_g^2 Z_c \sin(\theta) e^{-jk_g r} r^{-1}(1 + (jk_g r)^{-1})$, where Z_c is the characteristic impedance of the medium. In air this equals 120π and k_g the wavenumber, A is the surface of the loop, I is the current through the loop and r is the distance from the center of the loop untill the point where the field is calculated. Because we are measuring in the near field, only the near-field terms are important, this leaves:

$$H_r = \frac{IA}{2\pi} \cos(\theta) e^{-jk_g r} r^{-3} \qquad (1) \qquad\qquad H_\theta = -j\frac{IA}{4\pi} \sin(\theta) e^{-jk_g r} r^{-3} \qquad (2)$$

¿From this we can observe that in the near field, with the assumption of the magnetic dipole as elementary building block, only the magnetic field is important. To fully profit from this knowledge an inductive antenna should be used. We used this kind of antenna to measure the magnetic near field of the FPGA, more specific we used a circular loop antenna. They are more used to receive than to transmit, especially when the efficiency of the antenna is not more important than the signal-to-noise-ratio [4].

Our FPGA is divided into several banks each of which has one or more power pins and ground pins. So, if we use first order modeling we could imagine current flowing from the power pins in 1 bank, trough the bank, to the ground pins in the same bank. Figure 2 shows the explanation graphically and Fig. 3 shows the first order model of the current flow in the FPGA.

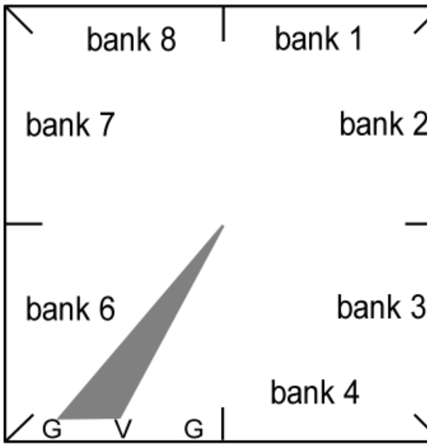


Figure 2: Area which is fed by one power pin

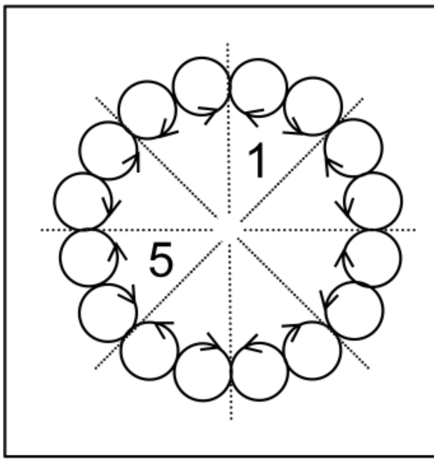


Figure 3: First order model of the current flow in an FPGA

Equations 1 and 2 show that the size of the current loop in the FPGA, the amplitude of the current, the direction of the current and the position of the current with respect to the position of the antenna have an influence on the measured field and hence should be taken into account in an EMA attack.

6 DEMA Attack on an FPGA Implementation of an Elliptic Curve Cryptosystem over $GF(p)$

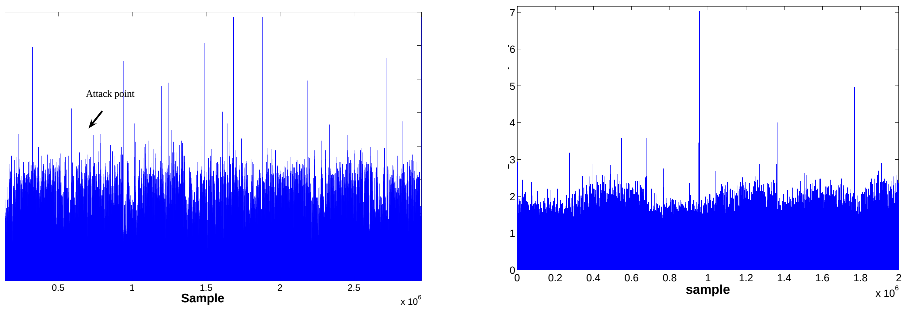
In this section, we conduct a DEMA attack on a FPGA implementation of an elliptic curve processor over $GF(p)$ [14, 15]. The electromagnetic radiation trace of one EC point multiplication is shown in Fig. 4.(a).

The target for our DEMA attack is the second most significant bit (MSB) of the key, k_{l-2}, in Algorithm 1. There are two temporary point registers in the design, Q_1 and Q_2. These temporary points and the output point Q are updated in the following order: $Q = P$, $Q_1 = 2P$, $Q_2 = 3P$, $Q = \begin{cases} 2P & \text{if} k_{l-2} = 0 \\ 3P & \text{if} k_{l-2} = 1 \end{cases}$, $Q_1 = \begin{cases} 4P & \text{if} k_{l-2} = 0 \\ 6P & \text{if} k_{l-2} = 1 \end{cases}$.

The first step of the DEMA attack is to find the point to measure. The electromagnetic radiation trace of an EC point multiplication is shown in Fig. 4.(a). Our choice for the measurement point is the fifth spike shown on Fig. 4.(a). This spike corresponds to the second update of Q_1 after the second EC point doubling.

We have produced a electromagnetic radiation file. For this purpose, we have chosen N random points on the EC and one fixed, but random key, k. The FPGA executes N point multiplications such that $Q_i = [k]P_i$ for $i = 1, 2, \cdots, N$. We have measured the electromagnetic radiation of the FPGA during 2400 clock cycles around the second update of Q_1. The clock frequency applied to the chip was around 300 kHz and the sampling frequency of the oscilloscope was 250 MHz. With these measurements, we have produced M_1, in which $M_1(i)$ is the *ith* measurement. The electromagnetic radiation trace of one of these measurements is shown in Fig. 4.(b).

We have applied a pre-processing technique to reduce the amount of measurement data in every clock cycle. We have found the maximum value of the measurement data in each clock cycle and taken the data in 20 clock cycles around the clock cycles that correspond to the five spikes in Fig. 4.(b).



(a) (b)

Figure 4: Electromagnetic radiation trace of a 160-bit ECPM over $GF(p)$ with Algorithm 1: (a) complete, (b) around the attack point

Thus, M_2 has 100 columns and N rows. We used the discrete Fourier transform to find the exact clock frequency and the number of samples per clock cycle.

We have implemented the EC point multiplication with Algorithm 1 in the C programming language. During the execution of the EC point multiplications, the C program computes the number of bits that change from 0 to 1 in some registers at the step corresponding to the fifth spike shown in Fig. 4.(b). The number of transitions is used as the electromagnetic radiation prediction.

We have produced two electromagnetic radiation prediction matrices, M_3 and M_4, for the $k_{l-2} = 0$ and $k_{l-2} = 1$ guesses, respectively. M_3 and M_4 have one column for the fifth spike and N rows for the N EC points.

We use the prediction matrices M_3 (for $k_{l-2} = 0$ guess) and M_4 (for $k_{l-2} = 1$ guess) in order to split the measurements in M_2 into sets. For each guess, we divide the N measurements into two sets. First we calculate the mean value of the prediction matrix M_3, $E(M_3)$. Measurement by measurement, we check if the predicted value is lower than the average value. If so, we put the measurement in set $S_{1,1}$, otherwise in set $S_{1,2}$. Then we calculate the mean value for each of the two sets and calculate the bias signal as $T_1 = E(S_{1,2}) - E(S_{1,1})$. We do the same for the prediction matrix M_4, the sets are now called $S_{2,1}$ and $S_{2,2}$ and the bias signal is T_2. The current consumption bias signals for $k_{l-2} = 0$ and $k_{l-2} = 1$ guesses are shown in Fig. 5. The figure shows a high peak on the expected spot on the trace for the $k_{l-2} = 1$ guess. Hence the decision for the right key-bit is equal to 1.

Figure 6 shows the change in the amplitude of all the clock cycles of the current consumption bias signals for the $k_{l-2} = 1$ guess. The number of measurements on these traces are the number of measurements in the sets $S_{2,1}$, $S_{2,2}$ described above. The number of measurements in these sets are nearly the same. Hence we should multiply the number of measurements seen in Fig. 6 by two in order to find the needed number of measurements. As it is shown in Fig. 6 2000 measurements are needed to distinguish the right clock cycle from the wrong ones.

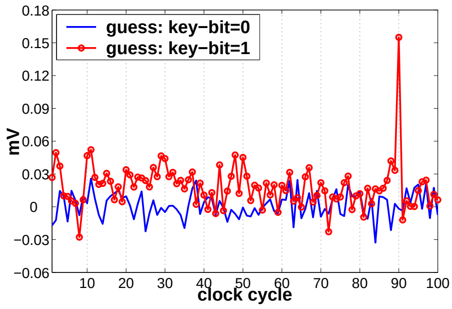


Figure 5: Electromagnetic radiation bias signals for the $k_{l-2} = 0$ and $k_{l-2} = 1$ guesses

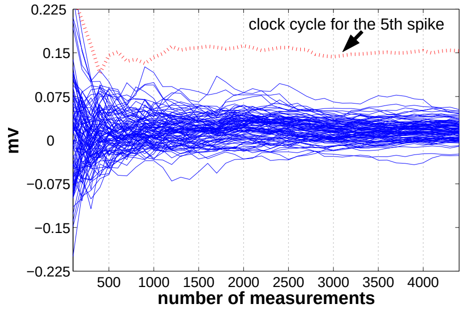


Figure 6: Change in the amplitude of the electromagnetic radiation bias signal for the $k_{l-2} = 1$ guess and all clock cycles

7 Conclusions

We have implemented a differential electromagnetic analysis attack on an FPGA implementation of elliptic curve cryptosystems over $GF(p)$. We use distance of mean test as the metric for the differential analysis. We conclude that it is possible to find the right key bit with 2000 measurements. The electromagnetic antenna model in this paper gives a first impression of the origin and properties of the field surrounding the FPGA. It explains the use of the loop antenna. In the future this model should be refined and checked with real measurements. From this it is already clear that the amplitude, the direction and the position of the current with respect to the position of the antenna have an influence on the measured electromagnetic radiation in the FPGA's surrounding area.

References

[1] D. Agrawal, B. Archambeault, S. Chari, J. R. Rao, and P. Rohatgi. Advances in side-channel cryptanalysis. *RSA Laboratories Cryptobytes*, 6(1):20–32, Spring 2003.

[2] D. Agrawal, B. Archambeault, J. R. Rao, and P. Rohatgi. The EM side-channel(s): Attacks and assessment methodologies. In B. S. Kaliski Jr., Ç. K. Koç, and C. Paar, editors, *Proceedings of the 4th International Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, volume 2523 of *Lecture Notes in Computer Science*, pages 29–45, Redwood Shores, CA, USA, August 13-15 2002. Springer-Verlag.

[3] D. Agrawal, J. R. Rao, and P. Rohatgi. Multi-channel attacks. In C. Walter, Ç. K. Koç, and C. Paar, editors, *Proceedings of the 5th International Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, volume 2779 of *Lecture Notes in Computer Science*, pages 2–16, Cologne, Germany, September 7-10 2003. Springer-Verlag.

[4] Constantine A. Balanis. *Antenna theory, analysis and design.* John Wiley & Sons, 1982.

[5] I. Blake, G. Seroussi, and N. P. Smart. *Elliptic Curves in Cryptography.* London Mathematical Society Lecture Note Series. Cambridge University Press, 1999.

[6] V. Carlier, H. Chabanne, E. Dottax, and H. Pelletier. Electromagnetic side channels of an FPGA implementation of AES. Cryptology ePrint Archive-2004/145, 2004. `http://eprint.iacr.org/`.

[7] E. De Mulder, P. Buysschaert, S. B. Ors, P. Delmotte, B. Preneel, G. Vandenbosch, and I. Verbauwhede. Electromagnetic analysis attack on a fpga implementation of an elliptic curve cryptosystem. In *Proceedings of the International Conference on "Computer as a tool (EUROCON)*, Sava Center, Belgrade, Serbia & Montenegro, November 21-24 2005. IEEE.

[8] K. Gandolfi, C. Mourtel, and F. Olivier. Electromagnetic analysis: Concrete results. In Ç. K. Koç, D. Naccache, and C. Paar, editors, *Proceedings of 3rd International Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, volume 2162 of *Lecture Notes in Computer Science*, pages 255–265, Paris, France, May 13-16 2001. Springer-Verlag.

[9] N. Koblitz. Elliptic curve cryptosystem. *Math. Comp.*, 48:203–209, 1987.

[10] P. Kocher, J. Jaffe, and B. Jun. Differential power analysis. In M. Wiener, editor, *Advances in Cryptology: Proceedings of CRYPTO'99*, volume 1666 of *Lecture Notes in Computer Science*, pages 388–397, Santa Barbara, CA, USA, August 15-19 1999. Springer-Verlag.

[11] S. Mangard. Exploiting radiated emissions - EM attacks on cryptographic ICs. In *Proceedings of Austrochip*, Linz, Austria, October 3 2003.

[12] V. Miller. Uses of elliptic curves in cryptography. In H. C. Williams, editor, *Advances in Cryptology: Proceedings of CRYPTO'85*, volume 218 of *Lecture Notes in Computer Science*, pages 417–426, Santa Barbara, CA, USA, August 18-22 1985. Springer-Verlag.

[13] NSA. NSA TEMPEST Documents, 2003. `http://www.cryptome.org/nsa-tempest.htm`.

[14] S. B. Ors, L. Batina, B. Preneel, and J. Vandewalle. Hardware implementation of an elliptic curve processor over $GF(p)$. In *IEEE 14th International Conference on Application-specific Systems, Architectures and Processors (ASAP)*, pages 433–443, The Hague, The Netherlands, June 24-26 2003.

[15] S. B. Ors, L. Batina, B. Preneel, and J. Vandewalle. Hardware implementation of an elliptic curve processor over $GF(p)$ with Montgomery modular multiplier. *International Journal of Embedded Systems*, February 2005.

[16] S. B. Ors, E. Oswald, and B. Preneel. Power-analysis attacks on an FPGA – first experimental results. In C. Walter, Ç. K. Koç, and C. Paar, editors, *Proceedings of the 5th International Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, volume 2779 of *Lecture Notes in Computer Science*, pages 35–50, Cologne, Germany, September 7-10 2003. Springer-Verlag.

[17] J.-J. Quisquater and D. Samyde. Electromagnetic analysis (EMA): Measures and counter-measures for smard cards. In I. Attali and T. Jensen, editors, *Proceedings of the International Conference on Research in Smart Cards: Smart Card Programming and Security (E-smart)*, volume 2140 of *Lecture Notes in Computer Science*, pages 200–210, Cannes, France, September 19-21 2001. Springer-Verlag.

[18] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[19] R. A. Serway. *Physics for scientists and engineers.* Saunders Golden sunburst series. Saunders college publishing, 1996.