Protecting Smart Cards from Passive Power Analysis with Detached Power Supplies

Adi Shamir

Dept. of Applied Math.
The Weizmann Institute of Science
Rehovot 76100, Israel
shamir@wisdom.weizmann.ac.il

Abstract. Power analysis is a very successful cryptanalytic technique which extracts secret information from smart cards by analysing the power consumed during the execution of their internal programs. It is a passive attack in the sense that it can be applied in an undetectable way during normal interaction with the smart card without modifying the card or the protocol in any way. The attack is particularly dangerous in financial applications such as ATM cards, credit cards, and electronic wallets, in which users have to insert their cards into card readers which are owned and operated by potentially dishonest entities.
In this paper we describe a new solution to the problem, which completely decorrelates the external power supplied to the card from the internal power consumed by the chip. The new technique is very easy to implement, costs only a few cents per card, and provides perfect protection from passive power analysis.
Keywords: Smart cards, power analysis, SPA, DPA.

1 Introduction

Hundreds of millions of smart cards are used today in thousands of applications which include cellular telephony, pay TV, computer access control, storage of medical information, identification cards, stored value cards, credit cards, etc. These cards are typically used by executing cryptographic computations based on secret keys embedded in their non-volatile memories. The goal of an attacker is to extract these secret keys from the tamper resistant card in order to modify the card's contents, to create a duplicate card, or to generate an unauthorized transaction.

We distinguish between two types of attacks:

1. *An active attack*, in which the smart card chip can be extracted, modified, probed, partially destroyed, or used in unusual environments. Active attacks leave clearly visible signs of tampering, and thus they are usually applied to stolen cards, or in situations in which the owner of the smart card is interested in defeating its security (e.g., in pay TV or telephony applications). They include fault attacks [BDL], probing attacks [KK], chip microsurgery with focused ion beam (FIB) devices, etc. They typically require considerable amount of time, sophisticated equipment and detailed knowhow of

Ç.K. Koç and C. Paar (Eds.): CHES 2000, LNCS 1965, pp. 71–77, 2000.

the physical design of the chip. They are extremely powerful in extracting system-wide information about the smart card system, but are rarely used to extract individual user keys due to their cost and complexity.

2. *A passive attack*, in which the smart card can only be externally watched during its normal interaction with a (possibly modified) smart card reader. This is the preferred attack when the owner of the smart card is interested in preserving its security, e.g., in financial applications: An ATM card can be used to withdraw cash from a foreign cash dispensing machine operated by an unfamiliar financial institution, a credit card can be used to pay for merchandise in a mafia-affiliated store, and a mondex-like card can be used to transfer money to a purse owned by a dishonest taxi driver. In all these cases, smart cards which will be misused, retained, returned late, or returned damaged by active attacks will be immediately reported by the card owner to the card issuer, who will launch an investigation. Passive attacks include timing attacks [K], glitch attacks [KK], and power analysis [KJJ]. They require little sophistication and minimal investment, and can be carried out against a large number of individual cards by a small number of rogue card readers.

Timing and glitch attacks pose little risk to well designed smart card applications, since it is easy to protect the software and hardware elements of smart cards against them. However, power analysis is very easy to implement and very difficult to avoid. It is based on the observation that the detailed power consumption curve of a typical smart card (which describes how the externally supplied current changes over time) contains a huge amount of information about its operation. With sufficiently sensitive measuring devices, it is possible to watch the exact sequence of events (in the form of individual gates which switch on or off) during the execution of the microcode of each instruction. For example, the power consumption profiles of the addition and multiplication operations are completely different, the power consumed by writing 0..0 and 1..1 to memory are noticably different, and it is possible to visually extract the secret key of an RSA operation by determining which parts look like a modular squaring and which parts look like a modular multiplication.

In the Simple Power Analysis (SPA) variant of this attack, the attacker studies a single power consumption curve to obtain statistical information about the identity of the instructions and the Hamming weight of data words read from or written into memory at any given clock cycle. An example of the power consumed by a typical smart card during the execution of a DES encryption operation (at two time scales) is described in Fig. 1, which is taken from [KJJ]: at the top we can identify the 16 rounds of DES, the initial and final permutations, and other large scale structural details of the implementation; at the bottom, we can see the (noisy) details of the execution of a single round of DES.

The Differential Power Analysis (DPA) variant of this attack is even more powerful: the attacker studies multiple power consumption curves recorded from different executions with different inputs, and uses statistical differences between particular subsets of executions to find in an automated way particular key bits.

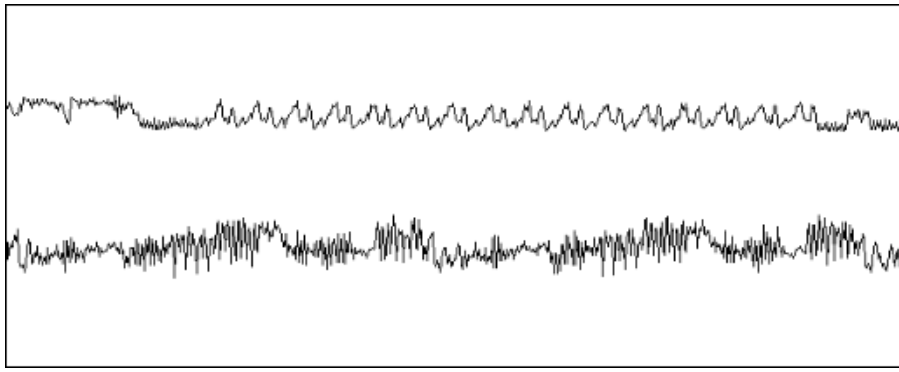

Fig. 1. The current supplied to standard smart cards

Kocher had publicly stated that with this DPA technique he managed to break essentially all the types of smart cards deployed so far by financial institutions.

Power analysis is usually a passive attack, since the smart card need not be modified in any way and cannot possibly know that its power supply is being monitored.

2 Previous Protective Techniques

After the publication of Kocher's SPA/DPA techniques, researchers and smart card manufacturers started looking for solutions. Attempts to make the power consumed by smart cards absolutely uniform by changing their physical design failed, since even small nonuniformity in the power consumption curve could be captured by sensitive digital oscilloscopes and analysed to reveal useful information. In addition, forcing all the instructions to switch the same number of gates on or off at the same points in time is a very unnatural requirement, which increases the area and total power consumption of the microprocessor, and slows it down.

Another proposed solution was to add a capacitor across the power supply lines on the smart card to smooth the power consumption curve. However, physical limitations restricted the size of the capacitor, and enough nonuniformity was left in the power consumption curve to make this a very partial solution, especially against DPA.

A related technique is to add to the smart card chip a sensor which measures the actual current supplied to the chip, and tries to actively equalize it by controling an additional current sink. However, the local changes in the power supply curve are so rapid that any compensation technique is likely to lag behind and leave many power spikes clearly visible.

Other proposed techniques include software-based randomization techniques, hardware-based random noise generators, unusual instructions, parallel execu-

tion of several instructions, etc. However, randomized software does not help if the attacker can follow individual instructions, and hardware noise can be eliminated by averaging multiple power consumption curves, and thus they provide only limited protection against a determined attacker with sensitive measuring devices.

A different solution is to replace the external power supply by an internal battery on the smart card. If the power pads on the smart card are not connected to the chip, the power consumption cannot be externally measured in a passive attack by the card reader. However, the thickness of a typical smart card is just 0.76 mm. Since such thin batteries are expensive, last a very short time, and are difficult to replace, this is not a practical solution.

An alternative solution is to use a rechargeable battery in each smart card. Such a battery can be charged by the external power supply whenever the card is inserted into a card reader, and thus we do not have to replace it so often. However, thin rechargeable batteries drain quickly even when they are not in use, and thus in normal intermittent use there is an unacceptably long charging delay before we can start powering the card from its internal battery. In addition, typical rechargeable batteries deteriorate after several hundred charging cycles, and thus the card has to be replaced after a relatively small number of intermittent transactions.

3 The New Proposal

In this paper we propose a new method which uses a simple "airgap" to completely decorrelate the power supplied to the card from the power consumed by the card. The basic idea is to use two capacitors as the power isolation element. During half the time capacitor 1 is (regularly) charged by the external power supply and capacitor 2 is (irregularly) discharged by supplying power to the smart card chip, and during the other half the roles of the two capacitors are reversed.

The behaviour of the capacitors is defined by a simple switch control unit and four power transistors which are added to the smart card chip (see Fig. 2). The preferred cyclic sequence of actions is:

1. The first capacitor is disconnected from external power.
2. The first capacitor is connected to the chip.
3. The second capacitor is disconnected from the chip.
4. The second capacitor is connected to the external power.

With this behaviour the smart card chip is always powered by at least one capacitor, but the external power supply is never connected directly to the internal chip. The supplied current has the uniform and predictable form described in Fig. 3, whereas the consumed current can continue to have the highly irregular shape of Fig. 1. The capacitors are connected via diodes to prevent leakage from the charged capacitor to the discharged capacitor during the brief moments in which they are connected in parallel to the chip.

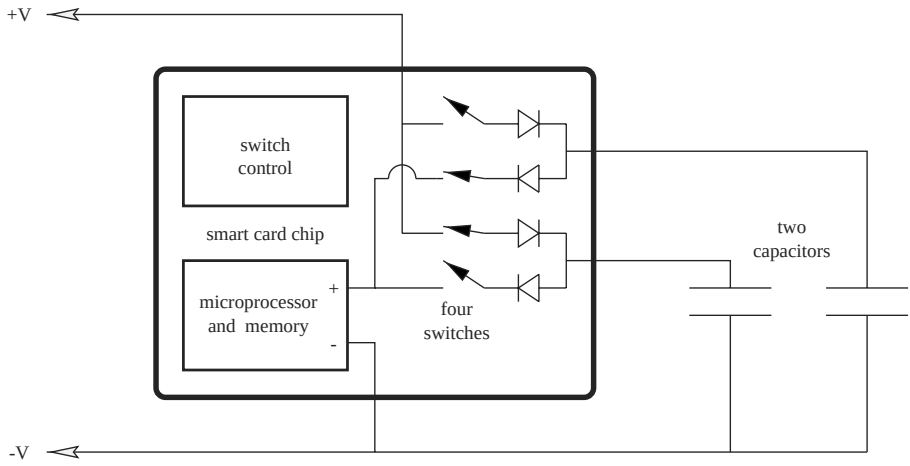

Fig. 2. Schematic diagram of a smart card with a detached power supply

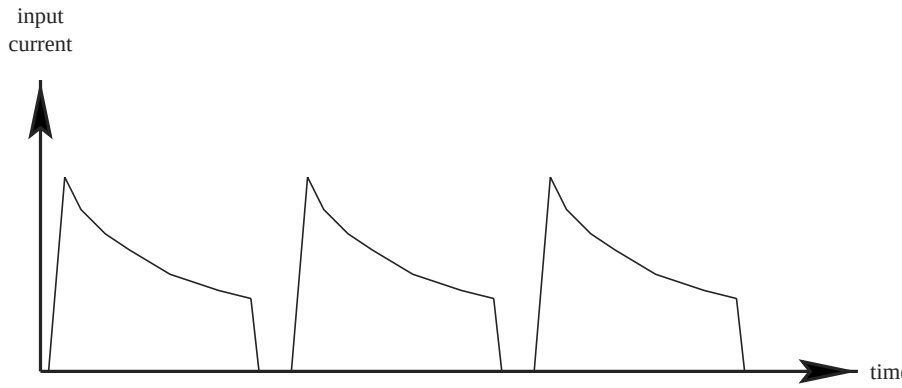

Fig. 3. The current supplied to smart cards with detached power supplies

The recommended size of each capacitor is about 0.1 microfarad. Low voltage capacitors of this type are commercially available in sizes as small as 2x2x0.4 mm, and thus they can be placed as external components next to the smart card chip in its plastic cavity. Alternatively, we can embed the capacitors in the card material itself by using alternate layers of plastic and aluminum in its 0.76 mm thickness and over its full surface area. Another possibility is to build the capacitors as extra metalic layers in the chip during its manufacturing process, but this would force the capacitor to be very small, and complicate the chip's manufacturing process. In large scale manufacturing, the addition of the two capacitors and the switch control adds just a few cents to the cost of the smart card.

An alternative design uses only one capacitor, which is alternately connected to the chip and to external power by two power transistors under the control of a simplified switch logic. The disadvantage of this approach is that the chip has to be halted and disconnected from power after each discharging cycle, which slows down its operation and can cause problems with some types of volatile on-chip memories.

The capacitor switchover should be triggered by counting a fixed number of instructions, rather than by comparing the dropping voltage of the discharging capacitor to some fixed threshold. The only information a passive attacker can infer is the total charge consumed by all the chip operations during the discharging period, which determines the initial current at the beginning of the next charging cycle. We can reduce this residual leakage by making the discharge period as long as possible. A simple calculation shows that a standard 0.1 microfarad capacitor can supply the 5 milliamperes required by a typical smart card chip for a period of 20 microseconds with a voltage drop of just 1 volt (say, from 6 volts to 5 volts). At the standard smart card clock rate of 5 megahertz, the chip performs about 100 instructions in this period, and thus the residual information which can be obtained by a passive attacker is the total power consumed by the chip during about 100 consecutive instructions. This is much less informative than the exact sequence of microcode events for each instruction, but it is still slightly vulnerable to DPA attacks on large numbers of sampled executions.

To make the smart card completely immune to passive power attacks, we have to add another simple element. Its role is to discharge the capacitor in an externally unobservable way to some fixed voltage after it is disconnected from the chip and before it is connected to the power supply (these are the intrapulse periods in Fig. 3). For example, the external power supply charges the capacitor from 4.5 to 6 volts, the chip discharges it during exactly 100 clock cycles to 5 ± 0.3 volts, and the switchover circuitry discharged it through an additional power transistor to exactly 4.5 volts during exactly 10 additional clock cycles before connecting it to the external power supply. In this case power measurements are completely useless, since the charging capacitors are always in exactly the same state at the same points in time regardless of the program executed or the data processed on the chip.

It is important to realize that power information can leak not only through the power lines, but also through the I/O line of the smart card chip which is used to send and receive data in a serial mode. This potential problem was ignored in most of the literature on power attacks, even though it can be used to attack chips whose power supplies were made immune to power attacks. In our proposed scheme, the voltage fluctuations of this line can leak information about the current power supplied by the capacitors. A simple solution to this problem is to disallow I/O operations (and temporarily ground or float the I/O line) during the execution of sensitive cryptographic subroutines.

The new capacitor approach is conceptually similar to the previously proposed battery approach, but it has the following important advantages:

- Capacitors are physically smaller than batteries, and are easier to embedded on the chip or in the plastic card next to the chip.
- Capacitors are cheaper than batteries, and cost just a few cents.
- Capacitors can be recharged an unlimited number of times, while batteries deteriorate after several hundred charging cycles.
- Capacitors do not have the memory effects of rechargeable batteries, and can be recharged without side effects even if they are not fully discharged.
- Capacitors can be charged in a fraction of a second, and thus intermittent use is not a problem.
- When we alternately charge and discharge capacitors, the average current consumed from the power supply is roughly equal to the average current consumed by the chip. Standard card readers may be unable to supply the large initial current needed if we want to charge the battery during the first second and then use it to power the chip for ten seconds.

The only disadvantage of the capacitor approach is that it can supply power to the chip only for several hundred clock cycles before its voltage becomes too low, and in each clock cycle the supplied voltage drops by about 0.01 volts. However, this voltage drop is not likely to interfere with the normal operation of the smart card chip, and we can repeatedly recharge the capacitors from the external power supply in order to execute an arbitrarily long computation.

Both the capacitor and the battery approaches are useless against an active attacker who can cut them off, replace them with other components, or measure the internal power consumption of the chip. However, the general problem of protecting smart cards in a cost effective way against active probing and microsurgery attacks seems to be currently unsolvable, and thus we do not try to address it in this paper.

References

BDL. D. Boneh, R. A. Demillo and R. J. Lipton, *On the Importance of Checking Cryptographic Protocols for Faults*, Proceedings of Eurocrypt 97, Springer-Verlag, 1997, pp 37-51.

K. P. Kocher, *Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems*, Proceedings of Crypto 96, Springer-Verlag, 1996, pp 104-113.

KK. O. Kommerling and M. Kuhn, *Design Principles for Tamper Resistant Smartcard Processors*, Proceedings of USENIX Workshop on Smartcard Technology, USENIX Association, pp. 9-20, 1999.
`http://www.cl.cam.ac.uk/~mgk25/sc99-tamper[-slides].pdf`.

KJJ. P. Kocher, J. Jaffe, and B. Jun, *Introduction to Differential Power Analysis and Related Attacks*, `http://www.cryptography.com/dpa/technical/index.html`, 1998.