Protecting Smart Cards from Power Analysis Attacks

S. Almanei
Department of Electrical & Computer Engineering,
Oregon State University, Corvallis, Oregon 97331.
E-mail:almanei@engr.orst.edu

May 28, 2002

Abstract— **As the demand on smart cards is increasing nowadays, a whole family of attacks are also present and can be a real threat on this technology future unless a solution can be implemented to safeguard it. In this paper I am presenting a new technique to protect smart cards from two main attacks, Differential Power Analysis (DPA) and Simple Power Analysis (SPA) Attacks. The two attacks allows the attacker to gain enough knowledge to know the secret key of the card's user.**

I. Introduction

Smart card users are increasing rapidly around the globe as shown in table 1. As a result, the security of smart cards must be examined and evaluated very carefully to insure a safe environment for its users.

Market	2001	2002	2003	Forecast
Mobile Comms	400	450	550	22%
Banking	145	181	220	22%
Others	196	263	357	36%

Table 1: Smart Card Market by Industry(Millions of Units).

Every smart card have a processing unit that will consume power to do the tasks specified. Most of the tasks are arithmetic calculations to insure the validity of the user. Verifying the correct PIN and encrypting the data so no one can use the card except the owner of the card. Our concerned here is to protect the secret key inside the card's memory. Since the card processor is digital it requires a very small amount of power to accomplish the encryption of the information. To measure the circuit's power consumption, a small (e.g., 50 ohm) resistor is inserted in series with the power or ground input. The voltage difference across the resistor divided by the resistance yields the current. Well-equipped electronics labs have equipment that can digitally sample voltage differences at extraordinarily high rates (over 1GHz) with excellent accuracy.[1] A figure showing the traces of a smart card's power consumption is illustrated below.

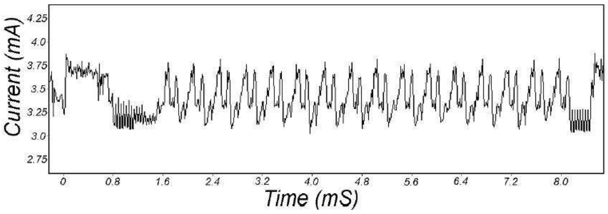

Figure 1: Power consumption for a 16 round DES key.

Unfortunately, the illustration in figure 1 is a real threat because it can be used to obtain the secret key from the card as we show next.

II. Power Attacks

In the recent years, there have been an extensive study on obtaining information (eg. secret keys) from smart cards. The very first announcement was made by Paul Kocher [1]. He review SPA attack and introduced DPA attack. The study was made specific against Digital Encryption Standard (DES). The techniques they used can be modified, hence, not limited to DES only.
The idea behind power analysis attacks is to exploit the differences in power consumption when the smart card processor process a logical zero or logical one.

- **SPA.**

SPA [1] on DES, could be used to reveal the Hamming weight of the key bytes which lead to the threat of a brute-force attack. Also RSA and Elliptic Curve Cryptosystem (ECC), are also vulnerable to an SPA attack on the Hamming weight of the individual key bytes. Its even possible that a stronger attack can be made directly against the square and multiply algorithm [2]. Illustration of the square and multiply algorithms are shown in figure 2.

```
exp1($M,\ e,\ N$) {
  $R\ =\ M$
   for ( $\imath = n-2\ downto\ 0$)
  {   $R = R^2\ mod\ N$
      if ($\imath\ bit\ of\ e\ is\ a\ 1$)
      $R = R \cdot M\ mod\ N$
  }
$return\ R$
}

exp1($M,\ e,\ N$) {
  $R\ =\ 1$
  $S\ =\ M$
  for ( $\imath\ =\ 0\ to\ n-1$)
  {   if ($\imath\ bit\ of\ e\ is\ a\ 1$)
      $R = R \cdot S\ mod\ N$
   }
$return\ R$
}
```

Figure 2: Square and multiply algorithms.

When the exponentiation is performed using one of the square and multiply algorithms shown in Figure 2, the outcome of the ”if statement” can be observed in the power signal whenever its executed, which leads to discovering every bit of the secret exponent. [2]

- **DPA.**

DPA [1] attacks are more advanced than SPA attacks in which they use statical methods and digital processing techniques on large number of power consumption signals to reduce noise and strengthen the differential signal so it will be obvious to distinguish between a logical zero and a logical one. SPA attacks on the other hand, would fail when differences in the power signals are so small that it is infeasible to directly observe them [3]. In case of DES, the attacker need to know the plain text to perform the attack on the first DES round or the ciphertext to perform the attack on the last DES round.[4] in another word, DPA analysis determine whether a key block k_s is correct. The attacker computes k-sample differential trace by finding the difference between the average of the traces. Figure 3 shows four different power traces that have been measured using DPA techniques in which the top is the normal power consumption of a smart card which uses DES. The rest are differential traces where the second from top is showing a correct guess of k_s. The last two traces from top are showing an incorrect value of k_s.[1]

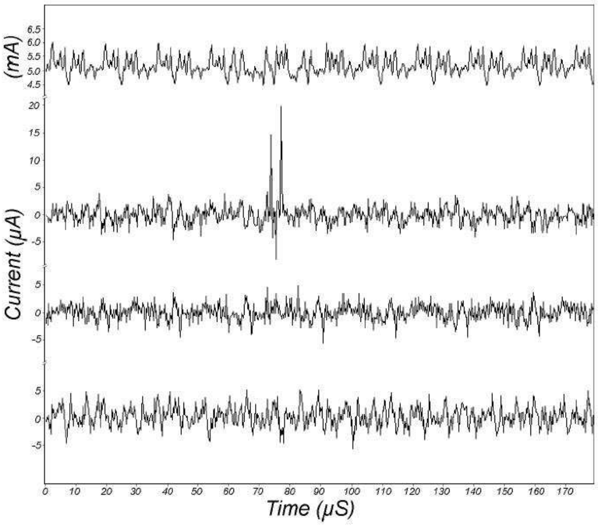

Figure 3: DPA traces with power reference.

III. Counter Measures

There have been some work on proposing a counter measure to prevent power analysis attacks on smart cards. One suggested solution to prevent DPA attacks is to add random calculations that increase the noise level enough to make the DPA bias spikes undetectable. The main goal is to add enough random noise to stop an attack, but to add minimal overhead.[5] However, there have to be a measurement done for every device ”almost” to calculate how much noise should be added.

Another proposal is to reduce signal sizes, such as by using constant execution path code, choosing operations that leak less information in their power consumption, balancing Hamming Weights and state transitions, and by physically shielding the device. Unfortunately such signal size reduction generally cannot reduce the signal size to zero, as an attacker with an infinite number of samples will still be able to perform DPA on the (heavily-degraded) signal. In practice, aggressive shielding can make attacks infeasible but adds significantly to a device’s size [1].

Another proposal to protect smart cards was proposed by Adi Shamir [6]. His idea was to use two capacitors to work as the power isolation element. During half the time capacitor 1 is charged by the external power supply and capacitor 2 is discharged by supplying power to the smart card chip, and during the other half the roles of the two capacitors are reversed. The behavior of the capacitors is defined by simple switch control unit and four power transistors which are added to the smart card chip. Applying this idea, the smart card chip will always be powered by at least one capacitor and the external power supply is never connected directly to the internal chip. The schematic of the proposal is shown in figure 4 and the graph of the supplied current will have a uniform and predictable form as shown in figure 5.

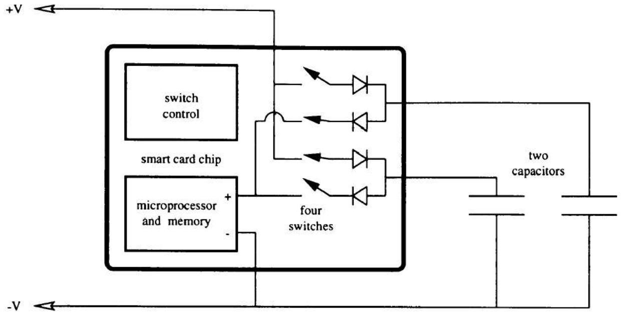

Figure 4: Smart card with detached power supply.

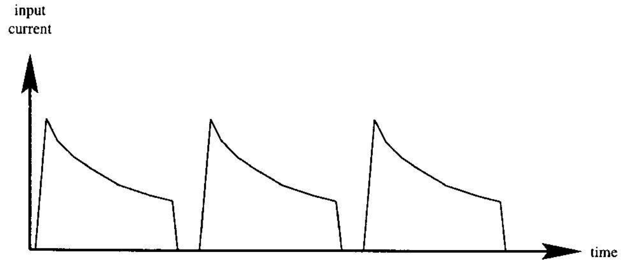

Figure 5: Current waveform of with detached power supply.

This idea; however, will make the manufacturing task very difficult because of the small size of the capacitors. [6]

My proposal here is to mask the power consumption by adding a Coprocessor to the smart card which contain a pseudo-random number generator which will trigger the power supply to ask for more current while the actual processor is verifying the input. in another word, it would act as another processor working on parallel with the actual processor. A diagram of the lay out of the proposed idea is shown in figure 6.

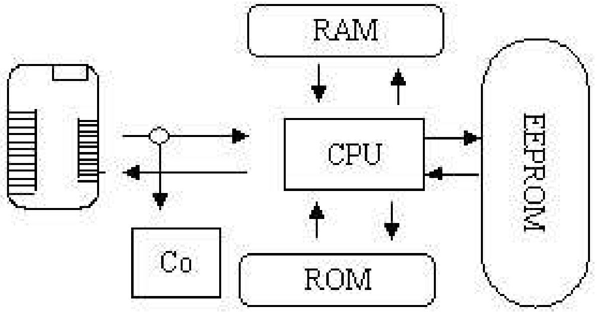

Figure 6: Impeded Coprocessor inside a smart card.

When the smart card is asked to verify a transaction, the Coprocessor is initialized with a request for current. There will be a multiplexer that will check for logical ones and zeros inside the Coprocessor block, when its a logical zero the pseudo-random number generator is then asked to generate a dummy number that will never be used just to suck some current from the power supply. Otherwise if its a logical one the cpu is asked to store the calculation in the memory and the start a dummy calculation which will be displayed to the attacker.

This approach will make the task of the attacker much more difficult to achieve because of the fact that the calculation of the dummy number is somewhat random and can't be really shown that an exact hit to the correct exponent is discovered. Unfortunately, the design of the Coprocessor and the timing between the CPU and the Coprocessor have to be really accurate because any missing gaps will lead to a total disaster to the accuracy of the calculation. also this will increase the production cost however the drawback of this proposal is the increasing time of the calculation and the need for more memory and power.

IV. Conclusion

With the described attacks, the task to insure safe and secure smart cards is very hard to achieve with the advances in signal processing and sophisticated equipments which can be very easily obtained by an attacker. I believe that in the near future it will be possible to increase the accuracy of this proposal by implementing it in a smart card. The need for secure smart cards is very important since we already know that the demand on this specific market is growing rapidly.

References

[1] Joshua Jaffe Paul Kocher and Benjamin Jun, "Differential power analysis," in *Advances in Cryptology — CRYPTO'99*, M. Wiener, Ed. 1999, Lecture Notes in Computer Science, No. 1666, pp. 388–397, Springer, Berlin, Germany.

[2] Ezzy A. Dabbish Thomas S. Messerges and Robert H. Sloan, "Power analysis attacks of modular exponentiation in smartcards," in *Cryptographic Hardware and Embedded Systems —CHES'99*, Ç. K. Koç and C. Paar, Ed. 1999, Lecture Notes in Computer Science No. 1717, pp. 144–157, Springer, Berlin, Germany.

[3] M. Anwar Hasan, "Power analysis attacks and algorithmic approaches to their countermeasures for koblitz curve cryptosystems," in *Cryptographic Hardware and Embedded Systems — CHES'00*, Ç. K. Koç and C. Paar, Ed. 2000, Lecture Notes in Computer Science, No. 1965, pp. 93–108, Springer, Berlin, Germany.

[4] Jean-Şbastien Coron and Louis Goubin, “Differential power analysis in the presenece of hardware countermeasures,” in *Cryptographic Hardware and Embedded Systems — CHES’00*, M. Wiener, Ed. 2000, Lecture Notes in Computer Science, No. 1965, pp. 252–263, Springer, Berlin, Germany.

[5] Ezzy A. Dabbish Thomas S. Messerges and Robert H. Sloan, “Investigations of power analysis attacks on smartcards,” in *Cryptographic Hardware and Embedded Systems*. 1999, USENIX Workshop on Smartcard Technology, USENIX, The Advanced Computing System Association.

[6] Adi Shamir, “Protecting smart cards from passive power analysis with detached power supplies,” in *Cryptographic Hardware and Embedded Systems*, ”Ç. K. Koç and C. Paar, Eds., Lecture Notes in Computer Science, No. 1965, pp. 71–77.