Contactless Technology Security Issues

Dr. Helena Handschuh

Security Technologies Department
Gemplus

Introduction

Contactless smart cards appeared several years ago in the form of electronic tags. Today they are typically used in the fields of electronic ticketing, transport and access control. More recently they have started to be used for electronic payment transactions.

The main difference between contact and contactless cards is that the user does not need to insert his contactless card into the slot of a smart card reader. The communication takes place via a radio frequency link, over the air, rather than through electrical contacts located on the smart card module. An antenna providing inducted current to the embedded smart card chip powers the whole system. This is normally hidden between the front and the rear of the card body and is thus invisible to the user.

For a number of reasons contactless technology is erroneously believed to be less secure than contact technology. In this article the results of an investigation into the security of contactless card technology is presented. The research was carried out both within the framework of the European Project SINCE (*Secure and Interoperable Networking for Contactless in Europe*) [1] and internally in Gemplus' security labs.

Interestingly, the outcome of this investigation shows that contactless smartcards are not fundamentally less secure than contact cards. However some attacks are inherently facilitated. Therefore both the user and the issuer should be aware of these threats and take them into account when building or using the systems based on contactless smartcards.

Threats Specific to Contactless Technology

As pointed out before, the main difference between a contact card and a contactless card is the fact that a user of a contactless card does not need to insert his card into a reader, a considerable convenience. However, this feature opens the door to attacks which exploit over-the-air communication channels in an unwanted manner. In this section we provide a few examples users and issuers should consider when integrating contactless technology into their systems. These examples are taken from [1].

Eavesdropping

One of the major issues with contactless communication is the existence of easy ways to intercept and alter data being transmitted over the air. In particular, this enables local eavesdropping and provides insight into data being exchanged at a reduced cost. In the passive setting, an observer may learn useful and/or confidential information by triggering a response from the card at a distance, without the user being aware of it. This clearly implies an important privacy risk. For ex-

ample, digital passports could make use of contactless technology, but diplomats may not be enchanted by the fact that observers can interrogate their passport over-the-air to find out which countries they have been visiting before. In the active setting, so-called man-in-the-middle attacks are facilitated. Someone could cut out a few data blocks and replace them with other data to change for example transaction amounts.

For these reasons it is important to stress that encryption of the data being exchanged and mutual authentication (in which the reader authenticates the card and vice-versa) are mandatory in most cases.

Interruption of Operations
Another potential threat when using contactless technology is that the card moves in the electromagnetic field. Thus, the communication between the reader and the card may be interrupted at any time without notice. The user may move the card out of the field without being aware of it and the system and the application need to ensure that transactions come to a regular end. In any case, reliable backup mechanisms need to be put in place, and backtracking should always be possible. In ticketing applications for example, the system needs to ensure the user is not charged twice, but at least once.

Denial of Service
Taking the previous threat one step further, the user and the issuer should be aware of so-called denial of service attacks, in which, say, all monetary units could be debited from the card at a distance, thus denying the user access to the service he has paid for. Cards can be emptied or destroyed remotely using inappropriate electromagnetic waves. The user may even try to apply the attack to his own card, hoping to claim a new functional card from the issuer free of charge.

Covert Transactions
The most important difference between contact cards and contactless cards in terms of security lies in the fact that the user does not notice whether a fake reader is entering into a communication with the card he is holding. Therefore the biggest threat for contactless technology is represented by covert transactions in which fraudulent merchants communicate with the user's card, triggering fake transactions using fake readers. For example, such merchants could potentially process a number of transactions instead of only one, or hide a huge transaction amount by means of a second transaction with a smaller amount, or even from a distance debit all monetary units contained on the card. Several variants of this attack are possible in the context of contactless applications.

A sound approach to protect against this attack strategy is strong mutual authentication between the card, the reader and the user, possibly relying on certificates, and requiring some kind of user interaction. For example, whenever a transaction is performed, the user could be prompted to push a button on his card or to apply some similar mechanism. In any case, the system must assist the user to only accept legitimate transactions.

Communication Link and Dual Modes
Another potential risk is related to dual mode chip cards, i.e. cards that have both a module interface and a contactless communication link. These cards tend to share the underlying chip so that the only difference is the way the data is transmitted to the I/O buffer of the chip card. Hence it seems likely that an attacker would choose the less secure interface to attack the chip card. He might consider starting a communication on one interface, and then switching to the other. Typical security measures, such as side-channel countermeasures (see next section), should be efficiently implemented on both interfaces. Contact and contactless modes should be separated, not necessarily on separate cards, but certainly during card operation. In other words the communication channels should be used one at a time only.

Case Study: Comparing Side-Channel Attacks

In the previous section we have been investigating specific threats related to contactless technology.

However, it is worth mentioning that still more attacks exist, which apply to both contact and contactless cards. These include physical attacks on the chip hardware, for example by microelectronic probing (i.e. landing a needle on the chip surface and reading out bus traffic), as well as so-called side-channel attacks, in which the opponent simply monitors the electrical activity of the chip and tries to turn seemingly unrelated power, time or electromagnetic emanation measurements into meaningful information.

Our reason for addressing these kinds of attacks is that new types of side-channel attacks against contactless technology have recently emerged. These have proven quite successful in recovering secret information from the card, given very limited resources, if no specific countermeasures are implemented.

As a case study, let us compare *Power Analysis*, *Electromagnetic Analysis* and *Radio Frequency Analysis* attacks on a standard dual-mode chip card readily available on the market.

The RSA Signature Algorithm
Before we start, let us introduce some mathematical basics, which will clarify the subsequent analysis.

We consider a dual-mode chip card implementing a standard public key 1024-bit RSA signature

[2]. In signature mode, a message **m** is raised to some large secret power **d** modulo a composite number **n**, where n is the product of two large secret primes **p** and **q**. (In some implementations, the computations are first done modulo the secret prime p, then modulo the secret prime q and finally combined. This does not affect the result of our analysis in any way).

The target of the adversary is to recover the secret exponent d. In general, for RSA exponentiation, smartcard implementations use the well-known secure "square-and-multiply always" algorithm described in pseudo-code in figure 1. In case the current bit of the secret exponent d is set to zero, a dummy multiplication is inserted instead of the regular one, and the result is discarded. This way, the same operations are seemingly done both when the current bit of d is zero and when it is one.

```
Input:    message m to be signed
          public RSA modulus n
          secret RSA exponent d of size k bits

Let s = m
For i = k-2 down to 0
    Let s = s^2 mod n                    /* SQUARE */
    If (bit i of d is 1)
        Then s = s x m mod n             /* MULTIPLY */
        Else s' = s x m mod n            /* DUMMY MULTIPLY */
    End if
End for

Output:   public RSA signature s = m^d mod n
```

Figure 1 - **Secure Square and Multiply Modular Exponentiation Algorithm**

Example:	$s = m^{13} = m^{1101}$ (exponent in binary notation)
Init (MSB = 1):	$s = m$
i = k - 2 = 2 (bit = 1):	$s = m^2 \times m = m^3$
i = 1 (bit = 0):	$s = (m^3)^2 = m^6$
i = 0 (bit = 1):	$s = (m^6)^2 \times m = m^{13}$

Figure 2 - **Numerical Example of Square and Multiply Exponentiation**

A numerical example is given in figure 2.

Simple and Differential Power Analysis (SPA, DPA)

Using regular Power Analysis Techniques, the attacker either analyses the power consumption curve directly or applies statistical treatments to several power curves obtained from the execution of the RSA signature algorithm on different input messages, in order to recover the secret exponent d.

The measurements are performed by connecting a resistor to the electrical contacts of the chip and monitoring the power consumption while the card is processing a given signature operation. However, the dual mode chip card under study already features some protection against power analysis. On this combi-card, hardware countermeasures actually stop the attacker from reading out any kind of information about the secret key. The power curves observed reveal that a current stabilizer was implemented on the chip and that the power consumption does not depend on the data being processed by the card. Therefore, whatever the secret exponent and the input message, the power curves are constant and all look alike, as shown in figure 3. Even statistical analysis is useless in this case.

Electromagnetic Analysis (EMA)

The second step of our comparative analysis consists in applying so-called electromagnetic analysis techniques to the card. In this scenario, the attacker first de-capsulates the chip by removing the top layers protecting the chip from the outside world, without damaging it. Next, the surface of the chip is scanned to find the best location for electromagnetic measurements. These very fine measurements require a probe consisting of a tiny inductive coil linked to an oscilloscope, which transforms local electromagnetic emanations into measurable power curves. Once this equipment is set up, regular power and EM inducted curves appear on the oscilloscope's screen as shown in figure 4. The red power consumption curve is still completely flat

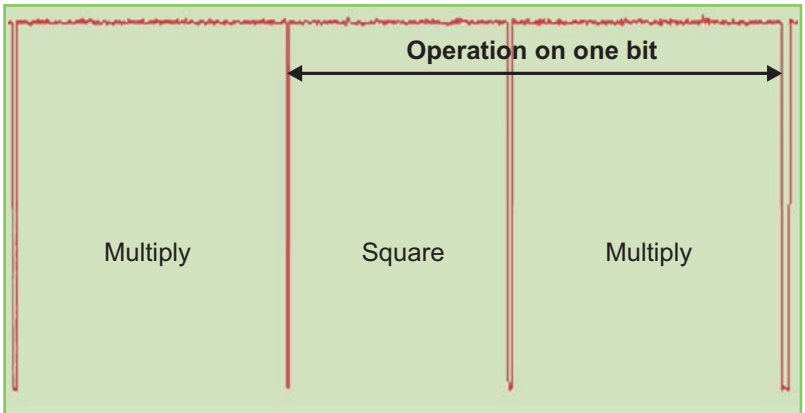

Figure 3 - **Curve Showing Power Consumption During a One-Bit Step of the Exponentiation**

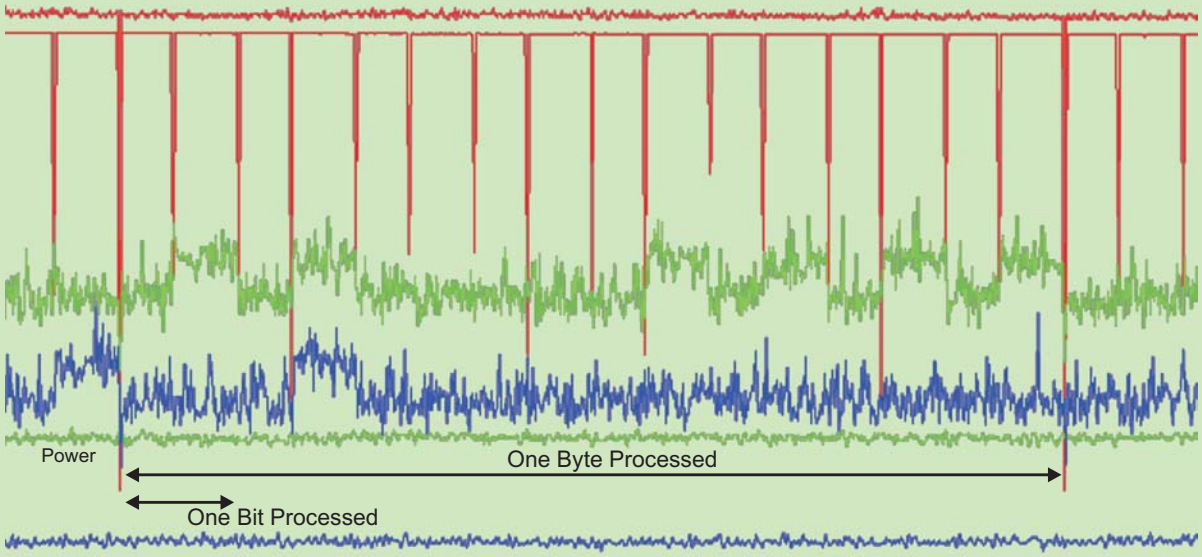

Figure 4 - **Power and Electromagnetic Analysis During a One-Bit Step of the Exponentiation**

while one starts to see variations in the green and blue EMA curves below it. Taking a closer look at these curves, a difference can clearly be identified between square and multiply operations corresponding to an exponent bit set to zero, and the same operations corresponding to an exponent bit set to one.

Radio Frequency Analysis (RFA)

Now let us introduce a new side-channel technique used exclusively in contactless technology: radio frequency analysis. This side-channel analysis is a mixture of both power and electromagnetic analysis. The idea is very simple: instead of de-capsulating the chip, consider measuring the electromagnetic field surrounding the chip card whilst in operation. The fact that the chip is powered via the radio frequency link implies that the magnetic field changes as a function of the current consumption of the card. Therefore, measuring the variations in the surrounding magnetic field should provide useful information to an attacker.

The equipment consists of a single magnetic loop made of copper wire, which captures the magnetic field and its variations, and transforms these measurements into power curves that can subsequently be monitored on the oscilloscope's screen. Figure 5 shows the set-up.

Figure 5 - **Equipment for Radio Frequency Analysis on a Contactless Card**

The contactless smart-card reader is implemented on the green plug board. The magnetic loop connected to an oscilloscope via claws is placed on top of the contactless smart card, which is itself separated from the reader by means of an empty plastic box.

In Figure 6, we show a power curve resulting from these measurements. It clearly appears that power consumption measured this way varies according to the data being processed. In Figure 7, we provide a close-up view of the previous curve. The secret exponent bits can now be identified one by one. These experiments reveal how powerful side-channel attacks can be, even in case the most obvious

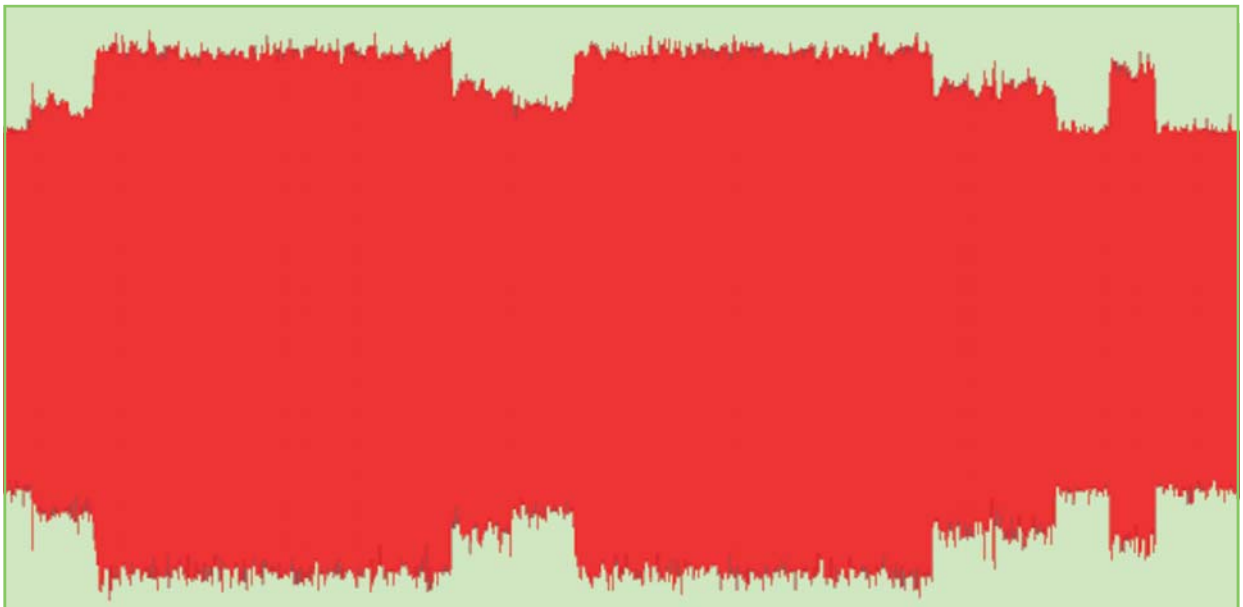

Figure 6 - **Radio Frequency Analysis Curve of an RSA Signature Computation**

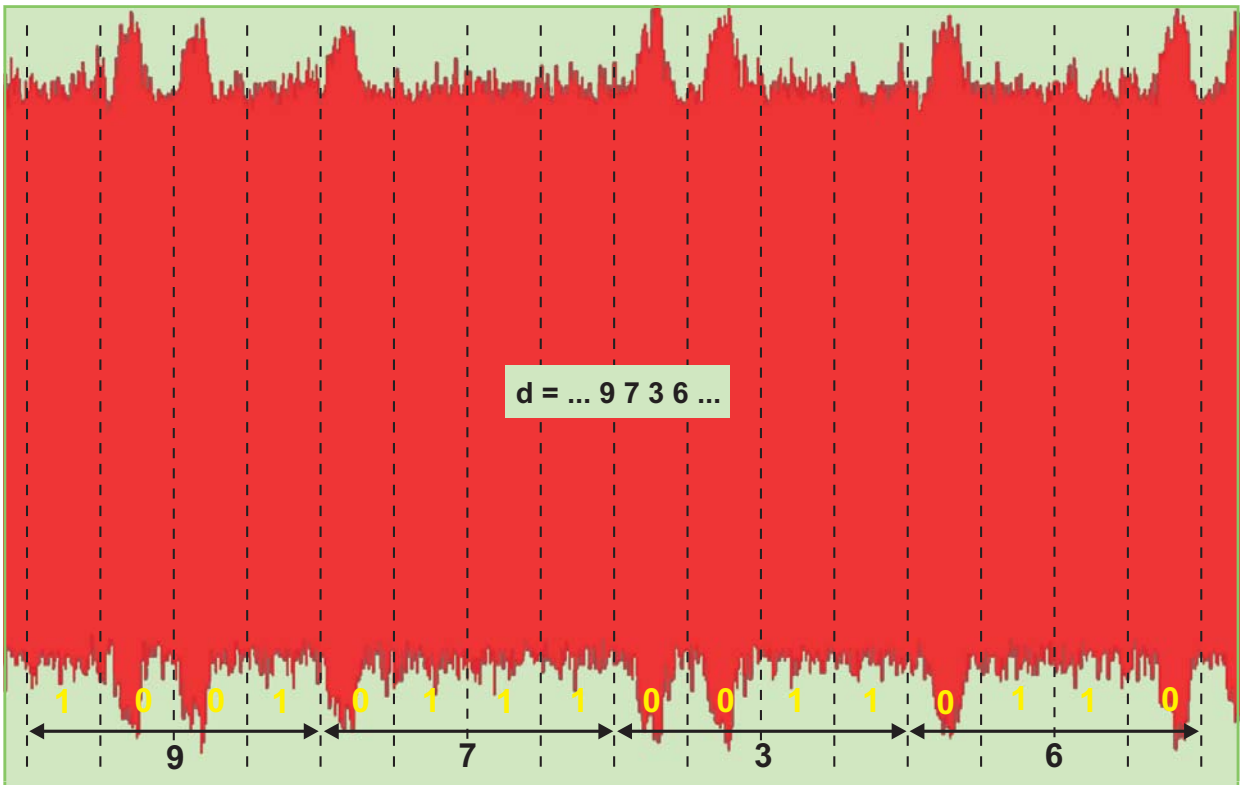

Figure 7 - **Close Up View of a Radio Frequency Analysis Curve During an RSA Signature Computation**

one (power analysis) has been taken into account by the chip manufacturer.

Conclusions Regarding Side-Channel Attacks

Our case study shows that hardware countermeasures (such as current stabilizers) against Power Attacks are necessary but not sufficient. Other side-channels have seriously to be taken into account. In the case of contactless technology, radio frequency analysis seems to be the most promising avenue of side-channel attacks. That needs to be addressed. It takes advantage of a weakness in contactless communication: the radio link is very easy to spy upon, and attacks go completely unnoticed. In addition, as opposed to electromagnetic analysis, radio fre-

quency analysis is a non-invasive technique. The chip card does not have to be tampered with. Therefore, more powerful security countermeasures such as message and exponent randomisation, need to be used when programming contactless smart cards. Fortunately, these techniques are already used to protect contact cards against general side-channel attacks and only need to be adapted to the contactless world.

Addressing Issues in Contactless Technology

Let us point out some issues that need to be taken into consideration when dealing with contactless technology.

First, contactless environments imply stringent timing and power constraints: public key cryptography and crypto-coprocessor sizes need to be optimised to fit in the card. Next we have seen that communication over the radio link implies some weaknesses from a security perspective: it is easier to attack using side-channel techniques, and also vulnerable to covert transactions. Typical countermeasures may be less cost-effective than in the contact world.

Users and issuers should be aware of the special properties of contactless technology and make sure these issues are addressed in a proper way. The right balance needs to be found between the cost of countermeasures in contactless cards, and the rest of the application. Contactless technology is not fundamentally more vulnerable than contact technology, but specific constraints and threats have to be taken into account and should be solved at the application level. Strong encryption and authentication should always be considered, and some kind of user interaction is required every step of the way. Security is always a trade-off.

Acknowledgements

The author would like to thank the security experts of Gemplus' Security Labs in La Ciotat for performing the above case study and for kindly providing the associated power curves and experimental results.

References

[1] SINCE Project, *Security and Threat Evaluation Relating to Contactless Cards*, eESC Common Specifications v2, volume 6, part 2, November 2002.

http://www.eurosmart.com/since/Download/SINCE_Secu_0103.pdf

[2] R.L. Rivest, A. Shamir, L. Adleman, *A method for obtaining digital signatures and public-key cryptosystems*, Communications of the ACM, Vol. 21, February 1978.

[3] W. Rankl and W. Effing, *Smart Card Handbook*, 2nd edition, New York, John Wiley & Sons, 2000.

[4] P. C. Kocher, *Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems*, in CRYPTO'96, Lecture Notes in Computer Science #1109, Springer Verlag, 1996.

[5] D. Boneh, R. DeMillo and R. Lipton, *On the Importance of Checking Cryptographic Protocols for Faults*, in EUROCRYPT'97, Lecture Notes in Computer Science #1233, Springer Verlag, 1997.

[6] J. Kelsey, B. Schneier, D. Wagner, C. Hall, *Side Channel Cryptanalysis of Product Ciphers*, in ESORICS'98, Lecture Notes in Computer Science #1485, Springer Verlag, 1998.

[7] P. Kocher, J. Jaffe, B. Jun, *Differential Power Analysis*, in CRYPTO'99, Lecture Notes in Computer Science #1666, Springer Verlag, 1999.

[8] L. Goubin, J. Patarin, *DES and Differential Power Analysis*, in CHES'99, Lecture Notes in Computer Science #1717, Springer Verlag, 1999.

[9] L. Goubin, J.-S. Coron, *On boolean and arithmetic masking against differential power analysis*, in CHES'00, Lecture Notes in Computer Science#1965, Springer Verlag, 2000.

[10] K. Gandolfi, C. Mourtel and F. Olivier, *Electromagnetic analysis: concrete results*, in CHES'01, Lecture Notes in Computer Science #2162, Springer Verlag, 2001.

[11] J.-J. Quisquater and D. Samyde, *ElectroMagnetic Analysis (EMA) Measures and Counter-Measures for Smart Cards*, in E-Smart Smartcard Programming and Security, Lecture Notes in Computer Science #2140, Springer Verlag, 2001.

About the Author

Dr. Helena Handschuh is Card Application Security Manager at Gemplus. She is actively involved in various information security and smart-card projects and has authored several papers and patents in cryptography.

Her current research focuses on secret-key cryptography, as well as mobile telecommunications security and security issues for contactless technology. Helena Handschuh is a Network and Communications engineer from the ENSTA.

She received a master's degree in Cryptography from the Ecole Polytechnique and holds a PhD in Cryptography from ENST in Paris.