Cryptography and the French Banking Cards: Past, Present, Future

Jacques Stern

Dépt d'Informatique, ENS – CNRS, 45 rue d'Ulm, 75230 Paris Cedex 05, France.
E-mail: Jacques.Stern@ens.fr
URL: http://www.di.ens.fr/users/stern

Abstract. This is a brief summary of the invited lecture delivered during the conference. The interested reader is referred to [2] for more information.

1 Introduction

In 1967, a group of French banks decided to offer a credit card service, under the form of a mere plastic card. The device was later enhanced with a magnetic stripe in 1971. Although magstripe cards display some cryptographic data, they are quite vulnerable: using rather simple equipment, it is possible to capture the encoded data and manufacture a fake card.

In 1990, it was decided to improve the security of the card by adding a chip. Since november 1992, all cards issued by the French banks are chip cards.

2 The cryptography of the French Banking cards

Based on the chip, several mechanisms were introduced:

1. PIN code verification,
2. RSA authentication,
3. (triple)-DES authentication.

The PIN code is a four digit sequence that the card holder enters. It is verified either from its enciphered version present on the magnetic stripe, in which case both need to be sent to a data center by means of an on-line connection, or else by the chip itself.

RSA authentication is based on an RSA signature of the card number and other related data. It is read from the chip and verified by the terminal at the point of sale.

DES authentication is based on the result of a CBC-MAC computation on the transaction data, by means of a triple DES key which the chip holds. Although simple DES was used when chip cards were launched in 1990, it has now been abandoned and replaced by triple DES. Since verification requires knowledge of the card's key, it can only be performed through an on-line connection.

In 1998, the "Humpich case" received wide coverage from the press, following an "experiment" demonstrating the use of a fake card at an off-line vending machine. Cryptographers will agree that the experiment did not show that its author was a genius: based on overoptimistic evaluations on the hardness of factoring (see e.g. [3]), the designers had originally chosen to use an RSA modulus of 320 bit only! RSA moduli now in use are over 768 bits, and quickly moving to 1024 bits.

Following the above, it was understood that the security offered by the chip card in an off-line scenario was hampered by more subtle versions of the "yes card" fraud. Such cards return a yes answer when a PIN code is submitted and display a card number and RSA signature captured form a legitimate card. To counter the fraud, it is necessary to replace the "static" authentication offered by RSA signatures by a dynamic version based an a challenge/response mechanism. Such mechanism is offered as an option in the EMV standard [1], under the acronym DDA (Dynamic Data Authentication). Taking advantage of the adoption of EMV, it has been decided to implement DDA in the French banking cards. The author believes this is an unprecedented effort of using public key cryptography in mass devices.

3 The Future

With triple DES, RSA, and DDA on board, the French banking cards are reaching a high level of cryptographic sophistication. French people are usually surprised to discover that in most countries, credit cards have no chip... It is expected however that chips will spread out, at least in Europe. Of course, the progress of the factoring algorithms is closely followed by the banks, and larger key sizes are bound to appear. Why not elliptic curves some day?

References

1. EMVCo EMV 4.0 Specifications available at `http://www.emvco.com/`
2. J. Patarin. La cryptographie des cartes bancaires. *Pour la Science*, Juillet/Oct 2002, 66–68.
3. R. Rivest, A. Shamir, and L. Adleman. A Method for Obtaining Digital Signatures and Public Key Cryptosystems. *Communications of the ACM*, 21(2):120–126, February 1978.