Security in Electronic Payment Systems

Jan L. Camenisch[†], Jean-Marc Piveteau[‡], Markus A. Stadler[†]

[†]Institute for Theoretical Computer Science, ETH Zurich, CH-8092 Zurich
e-mail: {camenisch, stadler}@inf.ethz.ch

[‡]UBILAB, Union Bank of Switzerland, Bahnhofstrasse 45, CH-8021 Zurich
e-mail: piveteau@ubilab.ubs.ch

This paper describes a practical proposal for a secure electronic payment system protecting privacy. It uses the concept of anonymous accounts and offers payer's anonymity as an add-on feature to existing EFTPOS systems.

1 Introduction

The number of private and corporate financial transactions that are done electronically is growing rapidly. From a user's point of view, efficiency and flexibility are clear advantages of existing and emerging electronic payment systems. Due to technical progress (e.g. powerful smart cards) and new developments in cryptology, these systems offer also a high level of security.

The goal of this paper is to describe and discuss a new electronic payment system allowing a customer to pay anonymously without affecting the system's security. In Section 2 we introduce some basic concepts, and in Section 3 we present our proposal. Related systems are discussed in Section 4. The Appendix describes the novel methods in a concise mathematical notation.

2 Basic Concepts

The underlying model of an electronic payment system consists of three parties: a bank, a customer, and a shop. There are three different types of transactions within the system: withdrawal involving the bank and the customer, payment involving the customer and the shop, and deposit involving the shop and the bank. The customer's account is debited during withdrawal, and the shop is credited during deposit. The three transactions take place simultaneously or separately, depending on the payment system.

Customer, shop and bank have different security requirements. The shop, receiving a payment, wants to be sure that the bank will pay the amount into its account. The bank wants to prevent fraud, e.g. that an individual can deposit more money than he or she has withdrawn from another account or received during a payment. Finally, the customer does not want unauthorized persons to make payments debiting his or her account, or to lose money because of theft. Furthermore, the customer may wish to have the possibility to pay anonymously.

The work presented in this paper has been done in the context of a joint project of UBILAB and ETH Zurich. It was partly supported by the Swiss Federal Commission for the Advancement of Scientific Research (KWF), grant no. 2724.1. The Results described here will appear in [Cam94].

Not all of these security requirements have the same priority: prevention of forgery is essential, but there exist well-accepted payment systems that provide no protection against loss or theft, or that do not allow anonymous payments.

We now introduce two cryptologic concepts which will be used below.

The concept of digital signature has been introduced by W. Diffie and M. Hellman [Dif76]. A digital signature scheme is a public key algorithm that allows to authenticate a message by means of a piece of information, called the signature. The generation of the signature requires the knowledge of the signer's private key, while for the verification of the signature, only the knowledge of the corresponding public key is necessary. If the public key is publicly accessible, then everybody can verify the signature, while only the signer, who knows the private key, is able to sign.

D. Chaum introduced the concept of blind signature [Cha83], which is an extension of the concept of digital signatures. There are now two parties involved in the generation of the signature: a sender who chooses the message to be signed, and the signer who provides the sender with information allowing him or her to compute the signature. The main difference to ordinary digital signatures is that the signer does not receive any information, neither on the message nor on the resulting signature. More formally, the signer's information and the resulting message signature pair are statistically independent.

An example of a digital signature which can be extended to a blind signature is presented in the appendix.

3 Anonymous Electronic Payment Systems

Usually, the security of electronic payment systems is realized by a combination of physical measures and cryptologic methods. Physical security measures depend on the current technology; therefore, technological progress may threaten seriously the existing systems. It is therefore interesting to investigate systems whose security relies solely on cryptologic methods. In this section we propose an electronic payment system that provides payer's anonymity.

Electronic payment systems offering no anonymity can easily be realized. The simplest example is an EFTPOS-like[1] system in which payments are done by simultaneously debiting the payer's account and crediting the payee. The security of such a system is based on the authentication of the payer as the owner of the debited account; this means that the security does not need to rely on physical measures.

There also exist systems offering anonymity, for instance systems using numbered bank accounts, which have been introduced in some countries.

The basic idea of our proposal is to combine the two systems mentioned above in order to have the independence of physical security of the former and the anonymity of the latter. A customer has a regular account with the bank and is the owner of one or several anonymous accounts. Actually, anonymous accounts are similar to numbered bank accounts. The customer can pay with the regular account, if no anonymity is desired, and with an anonymous account, if the individual's identity should not be disclosed. However,

---

1 EFTPOS: Electronic Funds Transfer at the Point of Sale.

before an anonymous account can be used, some money has to be paid into it. How can this be done both digitally and anonymously?

Our solution is to split this transfer into two steps. In the first step, the customer withdraws money from the regular account and receives from the bank a digital attestation. Then he or she can use this attestation to pay the withdrawn money into the anonymous account.

The following properties of this attestation are fundamental for the security of the system.

- It must be impossible to forge an attestation because this is equivalent to forging money. For this reason, the bank signs the attestation with a digital signature.
- The attestation must not reveal the identity of the payer. This is possible if a blind signature is used instead of an ordinary digital signature: the customer acts as the sender and the bank as the signer.
- It must be impossible to use the attestation more than once to pay money into an account. This problem can be solved in the following way: the attestation consists essentially of the number of the customer's anonymous account and of the number of withdrawals that have been made using this anonymous account. Since the attestation is signed by the bank, the customer cannot change this information. The bank, counting for each anonymous account the number of valid transfers, accepts an attestation only if it indicates the correct account and if it contains the correct sequence number. After the money is paid into the anonymous account, the number of valid transfers is incremented by the bank. In this way, the attestation is automatically invalidated. Note that the customer has to take care that the attestations are used in the same order as they have been received.

Because the system does not rely on any physical security measure, it is possible to make backup-copies of all attestations. Therefore, if a smart card containing such attestations is lost, it is possible to restore the attestations in another card. Even if a thief obtains the attestations, he or she could only use them for the intended anonymous accounts.

This system can be realized as an extension of today's EFTPOS systems, since there is no significant difference between a payment involving an anonymous account and a regular account.

For legal reasons, the bank could be led to control the origin of money paid into an account. In the case of a regular account, this can be done with the usual assortment of administrative measures. For an anonymous account, the only fact known by the bank is that the money comes from some regular account, which means that its origin has previously been checked.

A more formal description of this payment system can be found in the Appendix.

4 Related Systems

The payment system described in Section 3 is not the first proposal of an anonymous electronic payment system. D. Chaum proposed a system that uses the attestation directly to pay the payee [Cha85]. Forgery is prevented and anonymity is assured with blind signatures as well. To prevent multiple use of attestations, the bank has to maintain a huge database storing all attestations already spent. Before the bank accepts an attestation, it searches the database for that specific attestation. This makes the system unpractical.

On the basis of Chaum's system, so called off-line systems have been proposed (see [Bra93], [Cha88]). They allow to pay with attestations without contacting the bank (respectively the database). Therefore, these systems cannot prevent that the same attestation is used more that once. However, the identity of cheaters can be determined later, thanks to the special structure of the attestations, while honest customers remain anonymous.

Payment systems based on value cards can also provide payer's anonymity. A value card is a smart card storing information that can be used as a means of payment. A phone card is a typical example of a value card: units are stored on the card and are debited when making a call. Some value cards can be reloaded and may be hence seen as an electronic purse (see e.g. [How94]).

Each value card contains a counter that indicates the amount of money stored in the electronic purse. When withdrawing money from the bank (i.e. when reloading the card), the counter is increased while the customer's account is debited with the same value. During a payment, the counter is decreased by the amount credited to the shop. For each transaction the card authenticates itself as a 'correct' card (i.e. a card issued by the bank) with a secret key and some cryptologic algorithms. The card is constructed in such a way that this secret key is not accessible from the outside. Additionally, the counter is protected against unauthorized manipulations. This means that the security of such a value card system essentially relies on physical security measures.

If the value card is lost then also the money stored in it is lost, because no backup copies can be made. If a user authentication mechanism is implemented (e.g. a password), the card is unusable for anyone who does not know the password, which may reduce the risk of theft. Anonymous payments are possible since no information about the owner or about the card is transmitted during a transaction.

5 Conclusion

We have presented and discussed a new electronic anonymous payment system. Compared to similar systems, it has the following advantages:

- It allows to combine payer's anonymity with the usual security requirements like protection against loss or theft of money, forgery, and overdraft.
- It permits to implement anonymity as an optional service which means that it is up to the payer to decide whether the particular payment will be anonymous or not.
- It is efficient and can be effectively managed. In particular, the size of the database that has to be maintained is reasonable.
- It can be realized as an extension of existing EFTPOS systems.

Acknowledgements

We would like to thank H.P. Frei, T. Kofler, and U. Maurer for valuable comments.

Appendix

A.1 Digital and Blind Signatures

This section describes the RSA signature algorithm [Riv78], and its blinded version proposed by Chaum in [Cha83].

We begin with the RSA algorithm. The signer's private key consists of two large prime numbers p and q, the corresponding public key is (n,e), with $n = p \cdot q$ and an integer e relatively prime to $(p-1)(q-1)$. The signer, knowing the factorization of n, is able to efficiently compute d with $e \cdot d = 1 \bmod (p-1)(q-1)$. To sign the message m (which is assumed to be an integer between 0 and $n-1$), the signer computes $s = m^d \bmod n$. The integer s is the signature of m. To verify the signature s, the receiver checks whether $m = s^e \bmod n$.

Chaum showed in [Cha83] how to generate blindly a valid RSA signature. Recall that in this case, the sender and the signer are different entities, and that only the sender knows the message m to be signed. The sender first selects a random number r and sends the blinded message $m' = mr^e \bmod n$ to the signer. The signer generates a valid RSA signature s' for m' and returns it to the sender, who then computes $s = s' \cdot r^{-1} \bmod n$. It is easy to check that s is a valid signature of m, and that (s,m) and (s',m'), considered as random variables, are statistically independent.

A.2 Formal description of the payment system

The objective of this section is to give a formal description of the system presented in section 3.2. We assume for simplicity that only a fixed amount v can be transferred from regular to anonymous accounts[2].

The system parameters are:

- H: one-way hash function.
- $(Bl(.,.), Sig(.), Ex(.,.), Ver(.,.))$: blind signature scheme. For a message m and a random value ρ, $Bl(\rho,m)$ is the blinded message, $s' = Sig(Bl(\rho,m))$ is the blinded signature, $Ex(\rho, Sig(Bl(\rho,m)))$ is the valid signature extracted from s' and ρ, while the predicate $Ver(.,.)$ is used to check the signature, which means that we have $Ver(m, Ex(\rho, Sig(Bl(\rho,m)))) = 1$ for every m and ρ.

The scheme is divided into four phases. The parties involved in the scheme are the customer *C* (payer), the shop *S* (payee) and the bank *B*.

Anonymous account opening phase

(1) *C* contacts *B* without showing its actual identifier (therefore *B* does not know anything about the true identity of *C* during this phase). The bank opens a new anonymous account *A* with account number acc_A and secret parameter k_A (e.g. a password), and sets $amount_A = 0$, and $counter_{AB} = 0$.

(2) *B* sends acc_A and k_A to *C*.

(3) *C* sets $counter_{AC} = 0$ and stores acc_A, k_A, $counter_{AC}$.

Withdrawal phase

(1) *C* identifies himself to *B*, randomly selects r and ρ, computes the message $m = H(acc_A, counter_{AC}, r)$, and sends the blinded message $m' = Bl(\rho,m)$ to *B*.

2 This assumption is necessary to prevent that a customer indicates in the attestation an amount larger than what has been actually withdrawn from his or her regular account. However, a modification of the scheme, using the technique explained in [Cha89], allows to consider any amount.

(2) B debits C's personal account with the amount v, and sends the blind signature $s' = Sig(m')$ back to C.
(3) C extracts a valid bank signature $s = Ex(\rho, s')$ of m.
(4) C increments $counter_{AC}$ by one.

Anonymous deposit phase

(1) C sends acc_A, r and s to B.
(2) B computes $m = H(acc_A, counter_{AB}, r)$ using $counter_{AB}$ stored in the account data of account A, and checks the validity of the signature s.
(3) B increases $amount_A$ by v.
(4) B increments $counter_{AB}$ by one.

Transaction phase

(1) C is identified by B through the knowledge of k_A if C wants to use the account acc_A, or C proves his or her identity to B when using the regular account. Then C gives the order to the bank B to transfer the amount p on S's account.
(2) B decreases the value $amount_A$ by p if C has been identified by his pseudonym, otherwise the value p is withdrawn from C's regular account.
(3) B credits S's account with the amount p.

References

[Bra93] Brands S: Untraceable Off-line Cash in Wallets with Observers, *Advances in Cryptology, Crypto ´93*. LNCS 773, Springer-Verlag, pp. 302-318

[Cha83] Chaum D: Blind Signature Systems. *Advances in Cryptology, Crypto '83*, Plenum, p. 153

[Cha85] Chaum D: Security without identification: transactions systems to make big brother obsolete. *Communications of the ACM*, 28, 1985, pp.1030-1044

[Cha88] Chaum D, Fiat A, Naor M: Untraceable Electronic Cash. *Advances in Cryptology, Crypto '88*, LNCS 403, Springer-Verlag, pp. 319-327

[Cha89] Chaum D: Online cash checks, *Advances in Cryptology, Eurocrypt '89*. LNCS 434, Springer-Verlag, pp. 289-293

[Cam94] Camenisch JL, Piveteau J-M, Stadler MA: An Efficient Electronic Payment System Protecting Privacy. To appear in: *Proceedings of ESORICS '94*

[Dif76] Diffie W, Hellman M: New Directions in Cryptography. *IEEE Trans. Info. Theory*, 1976, pp.644-654

[How94] Howes K: Mondex: An electronic cash system for the future. *EFMA's Newsletter*, n° 128, 1994, pp. 28-30

[Riv78] Rivest RL, Shamir A, Adleman L: A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21, 1978, pp.120-126